



[12] 发明专利说明书

[21] ZL 专利号 01800288.9

[45] 授权公告日 2005 年 7 月 13 日

[11] 授权公告号 CN 1210920C

[22] 申请日 2001.2.20 [21] 申请号 01800288.9

[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

[30] 优先权

代理人 吴丽丽

[32] 2000.2.22 [33] FI [31] 20000407

[32] 2000.2.25 [33] FI [31] 20000444

[86] 国际申请 PCT/FI2001/000165 2001.2.20

[87] 国际公布 WO2001/063853 英 2001.8.30

[85] 进入国家阶段日期 2001.10.22

[71] 专利权人 诺基亚公司

地址 芬兰埃斯波

[72] 发明人 朱卡·维伦 瓦尔特里·奈米

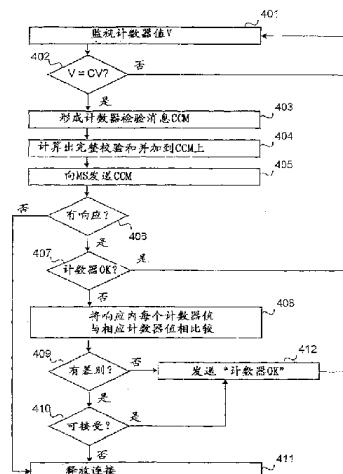
审查员 戴磊

[54] 发明名称 检验发送数据量的方法

权利要求书 3 页 说明书 16 页 附图 3 页

[57] 摘要

在网络基础设施与用户设备之间的连接期间，在网络基础设施内维护一个与通过连接发送的数据量有关的第一指示，而在用户设备内维护一个与发送的数据量有关的第二指示。对出现一个预定检验值作出响应(402)，触发一个检验过程。这个检验过程应用完整性受到保护的信令。在检验过程期间，将第一指示与第二指示相比较。这个检验过程可以很容易发现通过在网络基础设施与移动台之间的合法连接发送和/或接收数据、使数据传输费用由移动台承担的入侵者。



1. 一种检验在一个包括至少一个用户设备和一个网络基本设施的通信系统中通过一个连接发送的数据量的方法，

其特征是所述方法包括下列步骤：

在网络基本设施内维护一个与通过所述连接发送的数据量有关的第一指示；

在用户设备内维护一个与通过所述连接发送的数据量有关的第二指示；

对遇到一个预定的检验值作出响应，触发一个检验过程，所述检验过程应用完整性受到保护的信令消息；以及

在检验过程期间将第一指示与第二指示相比较。

2. 一种按照权利要求1所述的方法，其特征是所述方法还包括下列步骤：

如果第一指示与第二指示相同，继续所述连接和对第一指示和第二指示的维护。

3. 一种按照权利要求2所述的方法，其特征是所述方法还包括下列步骤：

在网络基本设施内触发检验过程；

向用户设备发送第一指示；

在用户设备内将第一指示与第二指示相比较；以及

如果第一指示与第二指示不同：

- 将第二指示从用户设备发送给网络基本设施；

- 再检验第一指示；

- 将再检验的第一指示与接收的第二指示相比较；以及

- 如果再检验的第一指示与接收的第二指示不同，释放所述连接。

4. 一种按照权利要求2所述的方法，其特征是所述方法还包括下列步骤：

在网络基本设施内触发检验过程；

向用户设备发送第一指示；
在用户设备内将第一指示与第二指示相比较；以及
如果第一指示与第二指示不同：
- 将第二指示从用户设备发送给网络基本设施；
- 再检验第一指示；
- 将再检验的第一指示与接收的第二指示相比较；以及
- 如果再检验的第一指示与接收的第二指示不同：
- 检验在再检验的第一指示与接收的第二指示之间的差别是否可接受；以及
- 只有在所述差别是不可接受的时候才释放所述连接。

5. 一种按照权利要求4所述的方法，其特征是所述方法还包括下列步骤：

如果在再检验的第一指示与接收的第二指示之间的差别是可接受的，减小所述检验值。

6. 一种按照权利要求2、3、4或5所述的方法，其特征是所述方法还包括下列步骤：

在用户设备内触发检验过程；
向网络基本设施发送第二指示；
在网络基本设施内将第一指示与第二指示相比较；以及
如果第一指示与第二指示不同：
- 将第一指示从网络基本设施发送给用户设备；
- 再检验第二指示；
- 将再检验的第二指示与接收的第一指示相比较；以及
- 如果再检验的第二指示与接收的第一指示不同，释放所述连接。

7. 根据权利要求6所述的方法，其特征在于包括以下步骤：

在用户设备中，在一段预定时间内等待一个来自网络基本设施的消息，所述消息包括第一指示；以及

仅当在所述预定的时间中没有接收到消息时在用户设备中触发检验过程。

8. 一种按照权利要求2、3、4或5所述的方法，其特征是所述方法还包括下列步骤：

在用户设备内触发检验过程；

向网络基本设施发送第二指示；

在网络基本设施内将第一指示与第二指示相比较；以及
如果第一指示与第二指示不同：

- 将第一指示从网络基本设施发送给用户设备；

- 再检验第二指示；

- 将再检验的第二指示与接收的第一指示相比较；以及

- 如果再检验的第二指示与接收的第一指示不同，所述方法还包括

下列步骤：

检验在再检验的第二指示与接收的第一指示之间的差别是否可接受；以及

只有在所述差别是不可接受的时候才释放所述连接。

9. 一种按照权利要求8所述的方法，其特征是所述方法还包括下列步骤：

在用户设备内，在一段预定时间内等待一个来自网络基本设施的消息，所述消息含有第一指示；以及

只有在预定时间内没有接收到所述消息的时候才在用户设备内触发检验过程。

10. 一种按照权利要求1至5中任一所述的方法，其特征是以现有技术的完整性受到保护的信令消息改变在用户设备与网络基本设施之间的检验过程中所需的信息。

11. 一种按照权利要求1至5中任一所述的方法，其特征是所述预定检验值确定在两个相继的检验过程之间发送的数据量。

12. 一种按照权利要求1至5中任一所述的方法，其特征是所述预定检验值确定在两个相继的检验过程之间发送的数据分组数。

13. 一种按照权利要求1至5中任一所述的方法，其特征是所述预定检验值确定在两个相继的检验过程之间的时间间隔。

检验发送数据量的方法

发明领域

本发明涉及检验在通信系统中特别是在可以通过空中接口发送非加密用户数据的无线电通信系统中发送的数据量的技术。

发明背景

无线电通信系统通常是指任何能在用户与网络之间进行无线通信的电信系统。在移动通信系统中，用户能在网络的覆盖区域内移动。典型的移动通信系统是公共陆地移动网(PLMN)。本发明可以用于不同的移动通信系统，例如通用移动通信系统(UMTS)和IMT-2000 (国际移动远程通信2000)。下面，本发明以UMTS，具体地说是以在第三代合作项目3GPP中所规范的UMTS系统，为例进行说明，但这并不是限制性的。

诸如控制信令和用户数据之类的信息，通过数据分组在移动台与网络基本设施之间交换。每个数据分组包括至少一个头标和一个数据部分。头标可以包括一个为数据分组进行路由选择的地址。在数据非加密发送时，地址可以被改变，特别是在地址呈IP(因特网协议)型和数据传输涉及一定的安全问题时。

图1例示了一个第三方MiM (“介入者”) 干涉移动台MS2与网络基本设施之间通过空中接口进行无线电通信的情况。在本申请中，第三方称为入侵者。这个称呼涵盖了各种非法干扰通过空中接口通信的情况，不论这干涉是为了窃听，还是用修改、删除、重排、重放、电子欺骗或任何其他普通操作来扰乱通信。入侵者例如可以用发送通过无线电连接发送的消息的非法拷贝干涉非加密无线电通信，改变移动台MS2发送的

数据分组的地址，滤去数据分组或发送虚假消息，干扰通信的完整性。

入侵者MiM对于移动台MS2(目标用户)代表网络基本设施(基站BS2和RNC2, 即RNS2, 见下面图1中所示), 同时对于网络基本设施(真正的基站BS2 (和RNC2))代表一个移动台MS2。入侵者MiM可以被动地只是窃听消息。主要问题是非加密的连接使入侵者MiM能修改头标, 允许入侵者通过MS2的连接发送和/或接收它自己的数据而不会被移动台MS2(和网络方)察觉。入侵者MiM只要让所有来自MS2的分组通过和修改这些分组的头标(主要是协议数据单元PDU号码)就可以在MS2发送的分组之间发送它自己的分组。对于下行链路分组, 入侵者MiM可以从数据流中滤出它自己的分组, 而让给MS2的分组带着经修改的头标通过。因此, MS2的用户察觉不到入侵者, 不知道他必须还要为入侵者的分组付费。MS2的用户只有在以后他的帐单中可以发现这种情况。

解决这个主要问题的一种方案是通过检验数据分组的完整性来验证每个数据分组(消息)。这种验证通常称为完整性保护, 一般不包括保护发送的数据分组的机密性。为了保护一个数据分组的完整性, 发送方按照一个预定算法计算出一个消息验证码MAC-I的值, 附加到数据分组上发送。MAC-I通常是一个比较短的比特串, 取决于附加到的数据分组(消息)和发送方和接收方都知道的密钥。接收方(通常)根据消息和密钥按照预定算法重算出一个XMAC-I值, 再将接收到的MAC-I与计算出的XMAC-I相比较。如果它们匹配, 接收方可以相信数据分组(消息)是完整(未被触动)的, 由所设想的那方发送。

完整性保护的问题是增大了通信的开销。通常, 为了将可以正确推测出MAC-I值的概率减小到使成功假冒无利可图的程度, MAC-I值应该足够长。例如, 采用32比特的MAC-I值可以将正确推测的概率减小到 $1/2^{294\ 967\ 296}$, 这对于大多数的应用来说是足够小了。然而, 在空中接口上, 每个分组有32个附加比特可以认为是相当大的开销, 应该尽可能避免。这就是为什么例如在UMTS中这种添加MAC-I的完整性保护只用于信令(在控制面上)。在完整性保护只用于信令时, 入侵者可以修改用户数据, 特别是头标, 发送/接收他自己的数据, 使得费用由合法的目标用户

MS2承担。在任何能以空中接口进行非加密数据传输的电信系统中可以出现类似的问题。

发明概述

本发明的一个目的是提供一种早期察觉通过连接发送和/或接收他自己的数据的入侵者的方法和实现这种方法的设备。这个目的是用特征如分别在独立权利要求中所述的方法、系统、网络部件和用户设备实现的。在各从属权利要求中给出了本发明的一些优选实施例。

本发明的基本思想是在网络方和用户设备(移动台)对发送的数据量计数，周期性地检验双方所计的数据量是否相同。“发送的数据”在这里指的是接收和/或发送的数据。在用户设备(移动台)与网络之间，在完整性受到保护的消息中改变在检验过程中所需的信息。本发明表明，甚至在用户面不用完整性保护的情况下，也可以利用控制面的完整性保护来对抗入侵者。本发明的一个优点是可以早期揭露通过连接发送和/或接收他自己数据的入侵者。另一个优点是用户设备(移动台)和网络节点可以由本机周期性地根据在连接期间发送的数据量相互验证。本发明也使运营商可以使合法用户只负担他自己的数据通信的费用而不负担入侵者的数据通信的费用。

在本发明的一个优选实施例中，根据比较结果推断是否释放连接。这样做的优点是，如果比较结果揭示有入侵者，这个入侵者就不能再使用这个连接。

在本发明的另一个优选实施例中，检验过程在网络基本设施内触发。这样做的优点是，不需要将检验值发送给用户设备(移动台)。

在本发明的又一个优选实施例中，检验过程可以在用户设备(移动台)内触发。这样做的优点是，如果入侵者只向用户设备(移动台)发送数据和/或用户设备(移动台)例如运行一个为一个合法的远程用户服务的应用软件，检验过程仍然可以触发。

在本发明的又一个优选实施例中，在用户设备(移动台)遇到检验值

后，用户设备(移动台)在一段预定时间内等待一个表示检验过程在网络基本设施内触发的消息，只有在用户设备(移动台)在这段预定时间内没有接收到这消息的时候它才触发检验过程。这样做的优点是，检验过程不会同时触发两次。

附图简要说明

下面将结合附图通过优选实施例对本发明进行详细说明，在这些附图中：

图1示出了一个简化的UMTS体系结构；

图2例示了一些协议组；

图3为例示按照本发明实现的用户设备和网络基本设施的功能的流程图；

图4为例示在本发明的第一优选实施例中网络内的检验过程的流程图；以及

图5为例示在本发明的第一优选实施例中用户设备内的检验过程的流程图。

发明详细说明

下面将在第三代移动系统UMTS中实现为例说明本发明的这些优选实施例。然而，目的并不是将本发明限制于这些实施例。本发明可用于可以通过空中接口发送非加密用户数据的任何电信系统。这样的系统的例子有IMT-2000、IS-41、GSM(全球移动通信系统)或相应的移动系统，诸如PCS(个人通信系统)、DCS 1800(1800兆赫数字蜂窝系统)之类。一般移动通信系统的规范，特别是IMT-2000和UMTS系统的规范，发展很快。这种发展可能需要本发明作一些附加的改变。因此，所有的措词和表示方式应该尽可能广义地予以理解，它们只是说明性的，并不是对本发明有所限制。对本发明来说，功能是实质性的，而不论是由哪个网

络部件或设备执行的。

图1示出了一个简化的UMTS体系结构，其中只例示了对本发明是必需的部分，当然，一个通常的移动电话系统还包括一些其他功能和结构，对于所属技术领域的专业人员来说，这些都是显而易见的，不需要在这里详细说明。UMTS的主要部分有：核心网CN，UMTS陆地无线电接入网UTRAN，以及也称为用户设备UE的移动台MS1、MS2。核心网与UTRAN之间的接口称为Iu接口，而UTRAN与移动台MS之间的空中接口称为Uu接口。Uu接口是一个空中接口。

UTRAN包括一组无线电网子系统RNS1、RNS2（也称为无线电接入网），通过Iu接口连接到核心网CN上。每个RNS负责它的小区的资源。一个无线电网子系统RNS包括一个无线电网控制器RNC和多个基站BS。两个无线电网子系统RNS之间的接口称为Iur接口。无线电网控制器RNC与基站BS之间的接口称为Iub接口。

无线电网控制器RNC1、RNC2是负责控制UTRAN无线电资源的网络节点。它连接到核心网CN上，终止限定移动台与UTRAN之间的消息和过程的RRC(无线电资源控制)协议。它在逻辑上相当于GSM系统内的一个基站控制器。在每个在一个移动台MS1与UTRAN之间的连接上，有一个RNC是服务RNC。如图1所示，RNC连接到两个CN节点(MSC/VLR 和SGSN)上。在一些网络拓扑结构中，一个RNC可以连接到一个或两个以上的可以是相同或不同类型的CN节点上。将来，一个RNC例如可以连接到几个SGSN上。

基站BS1、BS2也称为B节点。基站BS的主要功能是执行空中接口层1的处理(信道编码和交织，速率适配，扩频等)。它也执行一些基本无线电资源管理操作，如内部回路功率控制。逻辑上，它相当于在GSM系统内的一个基站收发信台。

核心网CN可以连接到一些外部网络EN上，这些外部网络可以是电路交换(CS)网(例如PLMN，PSTN，ISDN)，也可以是分组交换(PS)网(例如因特网)。核心网CN包括一个归属位置寄存器HLR、一个移动业务交换中心/访问位置寄存器MSC/VLR、一个网关MSC GMSC、一个服务

GPRS(通用分组无线电业务)支持节点SGSN和一个网关GPRS支持节点GGSN。在这里描述的核心网基于第二代GSM/GPRS网。其他类型的核心网，例如IS-41，可能包括其他一些网络部件。

移动台MS可以是一个简化的只用于语音的终端，或者可以是一个充当一个业务平台、支持与业务有关的各种功能的装载和执行的各种业务的终端。移动台MS包括实际的移动设备ME和一个可拆卸连接的标识卡USIM（也称为用户标志模块）。在这种情况下，一个移动台MS（即用户设备）通常意味着是由用户标志模块和实际移动设备形成的实体。用户标志模块USIM是一个保存用户身份、执行验证算法和存储验证、加密密钥和移动台所需的一些预订信息的智能卡。移动设备ME是用来通过移动台MS与UTRAN之间的Uu接口进行无线电通信的无线电终端。移动设备可以是任何能在移动通信系统内进行通信的设备，或者是若干件设备的组合，例如一个接有提供移动连接的Nokia卡电话的多媒体计算机。

实现本发明的功能的系统不仅包括按照现有技术发送数据和信令所需的装置，而且还包括在网络方维护一个与发送的数据量有关的第一指示的装置、在用户设备(移动台)内维护一个与发送的数据量有关的第二指示的装置、触发一个得出第一指示与第二指示的值是否相同的检验过程的装置。系统还可以包括在第一指示与第二指示不同时再检验发送数据量的值的装置。系统还可以包括判决这些值之间的差别是否可接受的装置和响应不能接受的差别而释放连接的装置。在系统的结构上不需要改变硬件。它包括一些处理器和存储器，用来实现本发明的这些功能。实现本发明所需改变的只是补充或更新一些软件程序和/或在参与检验过程的网络节点和用户设备(移动台)内添加一些专用集成电路(ASIC)。

为了实现图3、4和5详细示出的本发明的功能，要对包括按照现有技术从用户设备(移动台)发送数据或向用户设备发送数据的装置的网络节点进行一些修改。网络节点的硬件配置和基本操作不必改变。这些改变可以通过更新或添加一些软件程序和/或专用集成电路(ASIC)实现。虽然最好修改网络节点在图4和5的功能配合下实现图3所示功能，但是发明也可以在图3的功能配合下实现图4所示功能或图5所示功能。

可以对包括按照现有技术发送和接收数据的装置的用户设备(移动台),进行一些修改,实现图3、4和5较为详细示出的本发明的这些功能。用户设备(移动台)的硬件配置和基本操作不必改变。这些改变可以通过更新或添加一些软件程序和/或专用集成电路(ASIC)实现。虽然最好修改用户设备(移动台)在图4和5的功能配合下实现图3所示功能,但是发明也可以在图3的功能配合下实现图4所示功能或图5所示功能。

由于实现本发明涉及这些功能和对在空中接口中所用的协议的处理,下面将研究怎样能贯彻必需的协议组的一个例子。图2例示了一个遵从3GPP规范的空中接口协议组。这里所示的这些协议实体将在移动台与基站BS或无线电网控制器RNC之间起作用。这里没有示出BS与RNC之间的协议层划分,因为这与本发明无关。

空中接口协议可以分成一个控制面CP和一个用户面UP。控制面用于MS与RNC之间以及MS与CN之间的所有信令。用户面承载实际用户数据。一些空中接口协议只在一个面起作用,一些协议在两个面都起作用。

这些协议组被分成一些层:也称为物理层的第一层L1,也称为数据链路层的第二层L2,以及也称为网络层的第三层L3。一些层只含有一个协议,一些层含有几个不同的协议。每个单元,例如移动台和RNC RNC,各有一个层与另一个单元的一个层进行逻辑通信。这种通信称为对等通信。只有最低的物理层直接相互通信。其他层总是应用由下一个较低的层提供的服务。因此,消息必须在垂直方向上在这些层之间物理地传送,而只有在最低层信息才在这些层之间水平地传送。

物理层包括所有使通信在无线电信道得以进行的方式和机制。这些机制例如包括调制、功率控制、编码和定时。宽带CDMA(WCDMA)和时分CDMA(TD-CDMA)是可用于空中接口的多址接入方法的两个例子。物理层通过以传送表征数据为特征的传送信道为媒体接入控制(MAC)协议提供服务。

移动台MS与RNC或BS之间的数据链路层L2使用无线电链路控制RLC协议和媒体接入控制MAC。无线电链路控制RLC在无线电通路上提供一个取决于无线电解决方案的可靠链路。RLC通过描述RLC怎样处理

数据分组和例如是否使用自动重发请求(ARQ)功能的业务接入点(SAP)为更高的层提供服务。在控制面上，RLC服务由RRC协议用来进行信令传送。通常最少有三个RLC实体用于信令传送：一个透明模式实体，一个非证实模式实体，以及一个证实模式实体。在用户面上，RLC服务由业务专用协议层PDCP或BMC或者由其他较高层用户面功能(例如语音编解码器)使用。对于不用PDCP或BMC协议的业务，RLC服务在控制面上称为信令无线电承载业务，而在用户面上称为无线电承载业务。

MAC协议通过逻辑信道为RLC协议提供服务。逻辑信道由所发送的数据类型表征。在MAC层内，这些逻辑信道映射为一些传送信道。

只是对于PS范围的业务(通过SGSN路由的业务)才存在分组数据会聚协议(PDCP)，它的主要功能是头标压缩，这意味着在发送实体压缩冗余的协议控制信息(例如TCP/IP和RTP/UDP/IP头标)，而在接收实体解压缩。由PDCP提供的服务称为无线电承载业务。

只是对于SMS小区广播业务才存在广播多点传送控制协议(BMC)，这起源于GSM。BMC协议提供的服务也称为无线电承载业务。

RRC协议通过业务接入点为高层(非接入层)提供服务。所有在MS与CN之间的高层信令(移动性管理，呼叫控制，会话管理等等)都封装在RRC消息内，通过空中接口传输。

在RRC与所有下层协议之间的控制接口由RRC协议用来配置下层协议实体的特性(包括物理、传送和逻辑信道的参数)。同样的控制接口由RRC层用来例如命令下层协议执行一定类型的测量和由下层协议用来向RRC报告测量结果和差错情况。

入侵者必须以“被动方式”监视RRC信令，这样他就可以在一个合法的移动台与无线电网之间出现改变时修改他自己的协议组。在入侵者利用一个存在的无线电承载业务发送了他的第一个数据分组后，他必须采取较为积极的态度对待以这个无线电承载业务发送的数据。具体地说，他必须修改在合法的对等实体之间的所有数据分组(PDCP和RLC)的头标(主要是数据PDU号码)。

图3例示了按照本发明设计的在一个空中接口非加密传输连接期间

用户设备(移动台)和网络基本设施的工作情况。假设网络基本设施的功能是以RNC实现的。

图3开始于在MS与RNC之间已经建立了RRC连接。在步骤301，为这个连接建立一个无线电承载业务。根据业务情况，在UMTS内的信息通常可以使用一个或多个无线电承载业务（即在一个连接期间建立的一个或多个无线电承载业务）发送。无线电承载业务的数量也可以改变，因为可以在用户设备(移动台)与RNC之间的RRC连接期间释放或建立一些无线电承载业务。

在建立无线电承载业务的同时，在步骤302，使一些计数器进行工作。在图3所示的这个例子中，对于一个无线电承载业务有两个计数器：一个计数器用于上行链路方向，一个计数器用于下行链路方向。在步骤303，维护这些计数器的值，只要这个无线电承载业务有效（没有释放）。也就是说，在网络基本设施从MS（或者从装作MS的入侵者）接收到一个分组或者向MS发送一个分组（虽然入侵者可以滤去它）时，就在网络基本设施内更新相应计数器的值。相应，在MS发送或接收到一个分组时，就在MS内更新相应计数器的值。

在本发明的另一个实施例中，对于一个连接只有一个计数器。这个计数器可以用上述用于无线电承载业务的计数器作为子计数器。

在本发明的又一个实施例中，对于一个连接有两个计数器：一个计数器用于下行链路方向，一个计数器用于上行链路方向。这些计数器可以用上述用于无线电承载业务的计数器作为子计数器。

在本发明的第一优选实施例中，对于每个无线电承载业务有两个计数器。每个计数器包括一个作为最低有效部分的消息序号和一个作为最高有效部分的超帧号码HFN。消息序号取决于协议层。最好，消息序号是一个RLC PDU序号。使用RLC PDU序号和HFN的优点是它们已经在MS和RNC内实现，因为它们用于RLC层的ARQ功能，而且也作为加密算法的输入。

计数器(或子计数器)也可以对其他计数，例如发送的总数据量、在上一个“计数器检验”消息(示于图4)后发送的数据量、发送的分组数或

PDU号码。计数器可以使用模运算。重要的是计数器值应足以可靠地表示发送的数据量(或数据分组数)。也就是说，在用户设备(移动台)内的计数器值与在网络方的计数器值之间的差别应能充分反映出来，入侵者是否在“合法”分组之间发送他自己的分组。

在图4和5中比较详细地示出了在本发明的第一优选实施例中的检验过程。在检验过程中发送和接收的消息是信令消息。例如在UMTS内，所有的信令消息都受到完整性保护。为了清晰起见，可以认为在图4和5中一个信令消息如果完整性保护检验没有通过(即如果入侵者已经试图修改了消息)就不能作为一个接收消息。当然，如果入侵者滤去这些信令消息，它们就不能被这些合法实体(在第一优选实施例中为一个移动台MS和一个无线电网控制器RNC)接收。

图4例示了在本发明的第一优选实施例中为移动台服务的RNC的功能。在本发明的第一优选实施例中，在RNC中触发周期性的检验过程。RNC在第一优选实施例中表示网络基本设施，即网络方。在本发明的其他实施例中，其他的网络节点，例如基站或SGSN，可以执行下面描述为RNC功能的那些功能。

在步骤401，RNC监视连接的每个计数器值。在本发明的第一优选实施例中，每个有效的无线电承载业务具有两个计数器(上行链路和下行链路)，因此每个无线电承载业务有两个计数器值需监视。在监视期间，即在一个计数器的值改变时，在步骤402，RNC检验出现的是否为一个预定的检验值CV。在第一优选实施例中，检验值表示在两个相继的检验过程之间发送的分组数。在其他实施例中，检验值可以是一个门限。这个门限可以表示在上次检验过程触发后计数器值可以增大多少。检验值例如可以是一个RLC PDU号码范围。检验值可以在网络方自由规定，甚至在监视期间可以改变。在监视计数器值的这些实施例中，适当检验值的选择通常受所用的计数器的类型以及例如PDU长度、比特率、业务质量等的影响。

如果没有出现检验值CV(步骤402)，RNC就继续进行监视。

如果出现检验值，在步骤403，RNC形成一个“计数器检验”消息

CCM。在本发明的第一优选实施例中“计数器检验”消息含有每个计数器的计数器值的最高有效部分，即HFN。在本发明的其他实施例中，“计数器检验”消息只含有一个校验和，或某个按计数器值（即按一个由每个有效无线电承载业务的计数器值形成的比特串）计算出来的其他相应的“总和”。校验和最好是利用完整性保护算法计算出的消息验证码MAC-I。

在“计数器检验”消息就绪时，在步骤404，RNC计算出完整性校验和。在本发明的第一优选实施例中，完整性算法是f9，其输入参数是一个在验证和密钥协商过程期间得出的完整性密钥；一个方向比特(上行链路或下行链路)；一个是由网络选择的随机值的开始值；RRC消息本身(即在这种情况下的计数器检验消息)；以及一个是在利用同样的完整性密钥IK进行完整性保护的不同连接之间由MS维护的序号的COUNT值。COUNT值包括超帧号码(HFN-I)和RRC消息序号。完整性算法也可以需要一个“无线电承载业务”专用输入参数，例如一个无线电承载业务标识符。在计算完整性校验和时，RNC在步骤404将完整性校验和添加到“计数器检验”消息上，在步骤405发送给移动台MS。

在发送“计数器检验”消息后，在步骤406，RNC在一段协议标准中规定的预定时间内等待一个响应。如上所述，在RNC接收到一个信令消息时，它按此计算出一个完整性校验和，再将计算出的校验和与添加在消息内的校验和相比较，只有在它们匹配的时候，RNC才将这个信令消息认为是一个接收的信令消息。然而，这些步骤在图4中没有示出。

如果接收到响应(步骤406)，RNC就在步骤407检验，如果这个响应是一个“计数器ok”消息，即一个表示在MS内的计数器值与在RNC内的相同的消息，RNC就继续监视计数器值(步骤401)。

如果这个响应不是一个“计数器ok”消息(步骤407)，它在本发明的第一优选实施例中是一个含有在MS内为连接而维护的所有计数器值。这些计数器值最好在响应消息内由每个计数器的计数器值的最高有效部分即HFN表示。在步骤408，RNC将响应内的每个计数器值与它所维护的相应的计数器值相比较。因此RNC再检验它的计数器值。如果没有差别(步

骤409), RNC在步骤412向MS发送一个“计数器ok”信令消息, 再继续监视计数器值(步骤401)。计数器ok消息是一个完整性受到保护的消息。

如果有差别(步骤409), RNC必须判定这个差别是否可接受(步骤410)。计数器值有少许差别可能是由于同步引起的: 在对各方的计数器值检验之间会有一个小的时间差。也就是说, 一方可能已经发送了一个分组, 而另一方却还没有接收到。在这段时间内某个计数器值的最高有效部分可能改变。如果这个差别是可接受的(步骤410), 过程就进至步骤412, RNC发送“计数器ok”消息。如果这个差别是不可接受的, 就在步骤411, RNC释放这个连接。最好连接通过完整性受到保护的信令消息释放, 或者, 至少第一个表示必须释放连接的消息必须是完整性受到保护的。也可以不用信令就中断这个连接。

如果RNC在预定时间内没有接收到任何响应(步骤406), 就也释放连接。这样, 如果入侵者滤去了“检验计数器”消息, 连接也将释放。

在本发明的第二优选实施例中, 也可以在MS内触发周期性的检验过程。在周期性的检验过程在MS内触发时, MS执行RNC的上述功能(并向RNC发送这些消息)。在本发明的第二优选实施例中, 在MS注意到出现检验值时(步骤402), MS在一段预定时间内等待一个来自RNC的“计数器检验”消息。如果MS在这段预定时间内没有接收到“计数器检验”消息, MS就自己形成“计数器检验”消息来触发检验过程(步骤403)。在某些其他实施例中, MS在步骤402与403之间不执行这个辅助步骤。

在MS可以触发周期性的检验过程的一些实施例中, 网络最好在连接开始就向MS发送检验值的信号。这个信令必须是完整性受到保护的。检验值也可以是一个在MS内已设定的固定值。

在本发明的一些其他实施例中, 每个无线电承载业务可以作为一个整体来进行监视, 也就是说, 不是分别监视上行链路和下行链路方向。也可以将连接作为一个整体来监视, 也就是说, 不是分别监视各个无线电承载业务。这后一种情况也可以通过分别监视上行链路和下行链路来实现。

本发明的其他实施例中, 不是监视计数器值, 而是监视从发送上个

“计数器检验”消息或者从触发检验过程以来所经过的时间。在这些实施例中，检验值表示在两个检验过程之间的时间间隔。这个时间间隔不必是恒定的，它也可以例如由一个随机数产生器或者由一些其他产生非恒定值的方法产生。时间间隔也可以是一些固定而非恒定的时间间隔。在过了这段时间间隔时，就形成“计数器检验”消息(步骤403)。

在本发明的一个实施例中，可以在有可接受的差别时减小检验值，从而在那些可能有一个入侵者的“可疑”情况下可以较早地触发检验过程，而在MS和RNC内维护的计数器值之间没有差别时，恢复检验值。

图5例示了在本发明的第一优选实施例中在RNC触发周期性的检验过程时移动台MS的工作情况。

在步骤501，MS接收到一个来自RNC的“计数器检验”消息。如上所述，在MS接收到一个诸如“计数器检验”消息之类的信令消息时，它按这个信令消息计算出一个完整性校验和，再将计算出的校验和与添加在这消息内的校验和相比较，而只有在它们匹配的时候MS才将这个信令消息作为一个接收的信令消息。然而，在图5中没有示出这些步骤。

在本发明的第一优选实施例中，“计数器检验”消息含有每个由RNC维护的计数器的计数器值的最高有效部分。在步骤502，MS将“计数器检验”消息内的每个计数器值与由MS维护的相应计数器值相比较。

如果这些值相同(步骤503)，就在步骤507，MS向RNC发送一个“计数器ok”消息。“计数器ok”消息是一个完整性受到保护的消息。

如果一个或多个值不与相应的值相同(步骤503)，就在步骤504，MS形成一个响应。这个响应含有MS为这个连接维护的每个计数器的计数器值的最高有效部分。

在这个响应就绪时，MS在步骤505如上面在图4中所示那样计算出一个完整性校验和，在步骤505将它添加到响应上，再在步骤506将消息发送给RNC。

在发送了响应后，在步骤507，MS在一段预定时间内等待来自RNC的响应。这段时间在协议标准中规定。来自RNC的响应也是一个完整性受到保护的信令消息。如果接收到来自RNC的响应(步骤507)，就在步骤

508, MS检验这个响应是否为一个“计数器ok”消息(即表示在MS内的计数器值与在RNC内的相同的消息)。如果这个消息是一个“计数器ok”消息, MS就继续监视计数器值(步骤509)。

如果这个响应不是一个“计数器ok”消息(步骤507), 而是一个释放连接消息, 就在步骤510, MS释放这个连接。释放过程可以包括在实际释放操作前从MS向RNC发送一个响应消息。

如果MS在预定时间内没有接收到来自RNC的响应(步骤507), MS就本机释放这个连接(步骤508)。

在一些其他实施例中, 在步骤504形成的响应只含有那些不相同的计数器的计数器值。

在一些其他实施例中, 在步骤504形成的响应含有完整的计数器值(不只是那些最高有效比特)。

在计数器检验消息含有校验和或相应的总和的实施例中, MS计算出一个相应的校验和或总和, 在步骤502将它与消息内的相比较。

在本发明的另一个实施例中, 在计数器值不同时(步骤503), MS就释放这个连接。也就是说, 跳过步骤504-509。在这个实施例中, 还跳过图4中的步骤408-410和412。

在MS可以触发检验过程的实施例中, RNC执行图5中所示的MS的功能。

在本发明的一些实施例中, 在检验过程期间, 在各个信令消息内不改变信息或部分信息, 如图4和5中的情况。在这些实施例中, 计数器值(或相应的指示符)和/或比较结果添加到现有技术的在MS与RNC之间发送的完整性受到保护的信令消息上。

在基于以上这个利用现有技术的完整性受到保护的信令消息的实施例的本发明的一个实施例中, RNC(或MS)在出现检验值后等待RNC(或MS)在其中添加了计数器值的完整性受到保护的信令消息。等待下一个完整性受到保护的信令消息的等待时间可以由一个独立的定时器控制。这个独立的定时器规定了在出现检验值后、必须发送一个现有技术的完整性受到保护的信令消息前的最大允许等待时间。如果在这段允许等待

时间内不发送现有技术的完整性受到保护的信令消息，就使用在图4和5中示出的这些独立的信令消息。在这个实施例中，要发送的计数器值(或相应的指示符)和/或比较结果是在发送实际的完整性受到保护的信令消息时存在的那些值(而不是在出现检验值时存在的这些值)。在这个实施例中还可以不用独立的定时器而用一个辅助计数器。辅助计数器的触发值更可取地规定了在出现检验值后、必须发送一个现有技术的完整性受到保护的信令消息前的最多允许发送的数据分组数。因此，可以改变允许的等待时间。这个辅助计数器的触发值还可以例如规定在出现检验值后必须发送一个现有技术的信令消息前的最多允许接收(或发送)的数据分组数。或者，辅助计数器和独立定时器也可以一起使用，而在这样情况下由较早计满的规定最大等待时间。

现有技术的信令消息在这里涵盖了所有由于除只发送在检验过程中所需的信息以外的某些其他原因发送的信令消息。

图3、4和5中所示的这些步骤不是绝对按时间顺序的，一些步骤可以同时执行或者按与所给出的不同的次序。在这些步骤之间还可以执行其他功能。一些步骤也可以省去。例如，在本发明的一些实施例中，在计数器值有差别时，不检验这差别是否可接受(图4中的步骤410)，而是直接导致释放连接。这些信令消息只是示范性的，为发送同样的信息甚至可以包括几个独立的消息。此外，这些消息也可以含有其他信息。而且，消息的名称可以与上面所提到的不同。

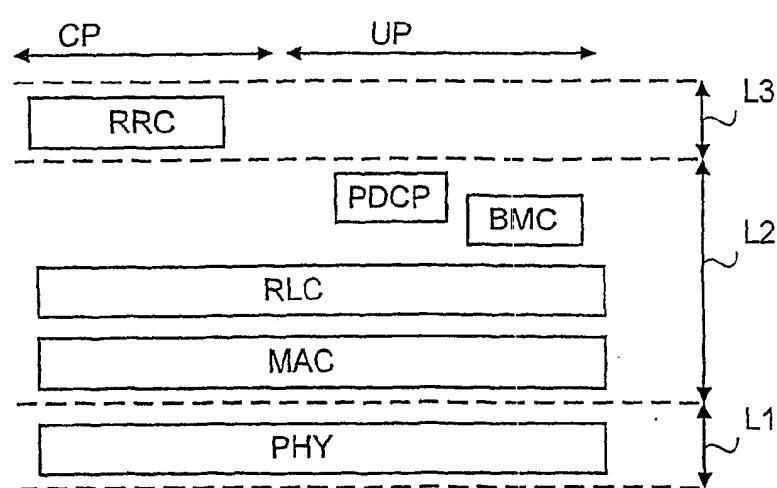
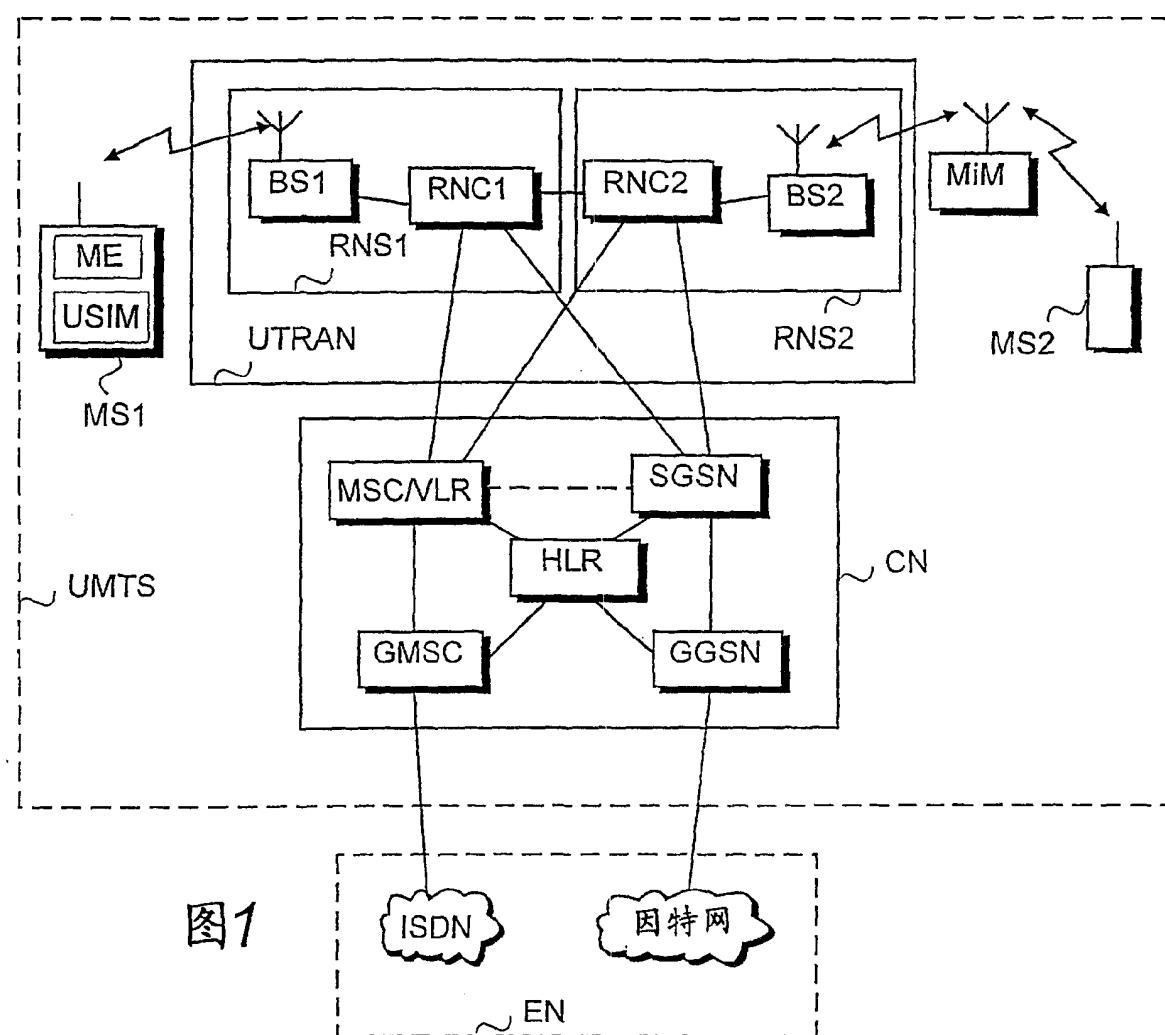
上面所说明的这些实施例或这些实施例的一些部分可以自由地加以组合，形成本发明的新的实施例。

上面通过一些使用重发协议RLC的不透明模式（这是大多数分组数据业务的情况）的实施例对本发明作了说明。然而，本发明也可以配合其他协议和配合电路交换连接实施。

在上面对本发明的说明中假设空中接口在网络基本设施与用户设备之间。然而，空中接口也可以在两个网络节点之间。

虽然上面是以无线电通信系统对本发明进行说明，但是本发明也可以应用于固定系统。

可以理解，以上说明和有关附图只是用来例示本发明。对于所属技术领域的专业人员来说，显然本发明可以在不背离在所附权利要求书中所揭示的本发明的范围和精神的情况下以不同的方式加以修改。



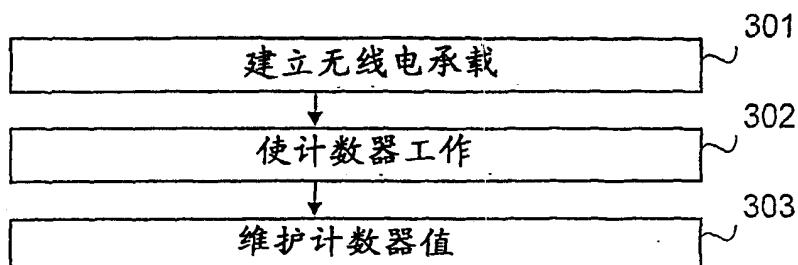


图3

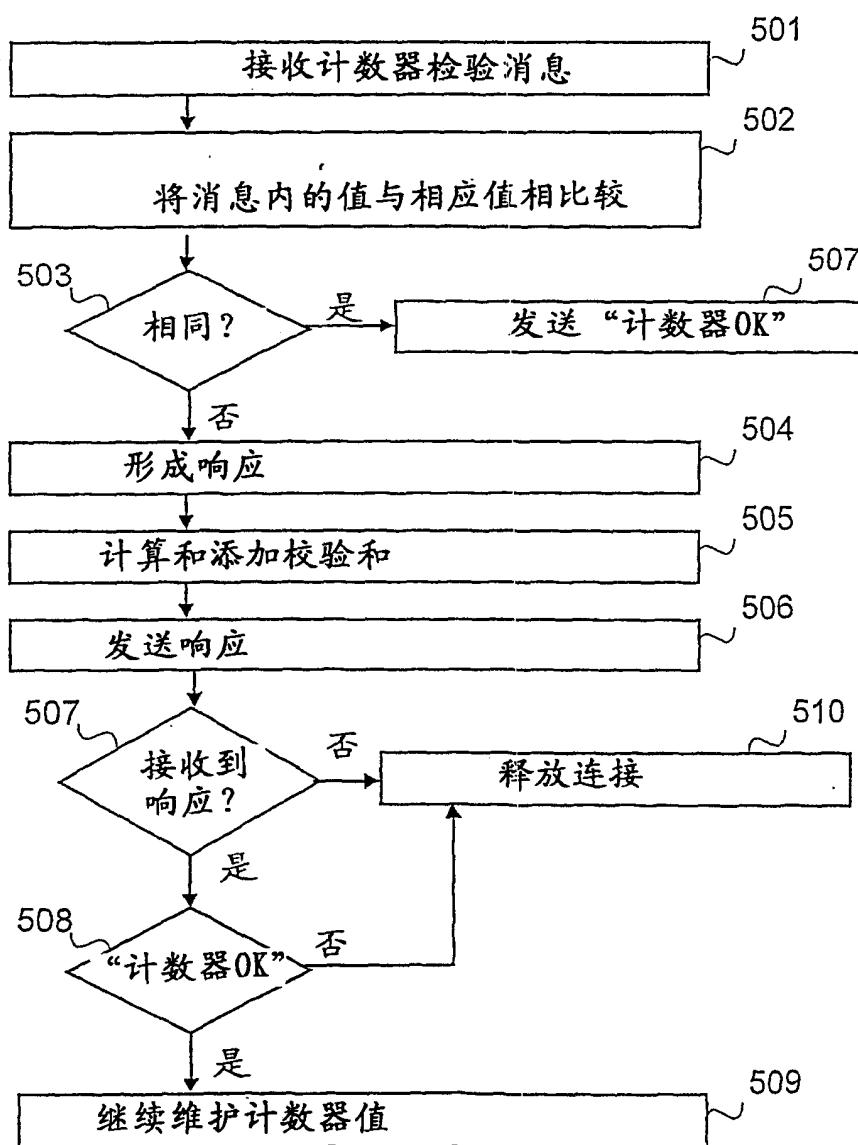


图5

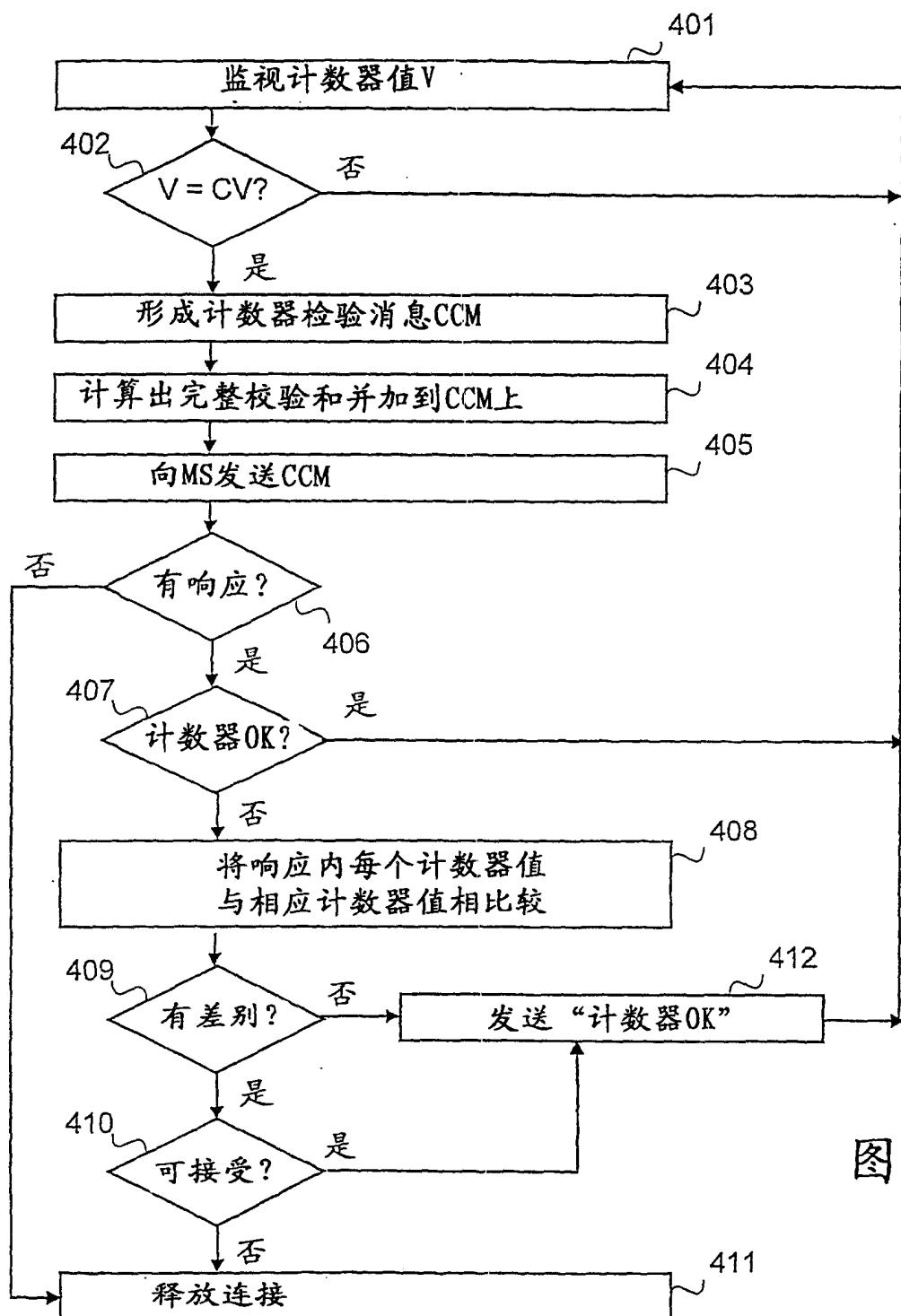


图 4