[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/32 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利说明书

专利号 ZL 01807069.8

[45] 授权公告日 2006 年 4 月 12 日

[11] 授权公告号 CN 1251534C

[22] 申请日 2001.3.20 [21] 申请号 01807069.8
[30] 优先权
[32] 2000.3.24 [33] FI [31] 20000695
[86] 国际申请 PCT/FI2001/000279 2001.3.20
[87] 国际公布 WO2001/078432 英 2001.10.18
[85] 进入国家阶段日期 2002.9.23
[71] 专利权人 斯麦脱信托系统有限公司
地址 芬兰赫尔辛基
[72] 发明人 M·马托 J·柳科伦
H·皮耶蒂莱伦 V·莱赫托宁
审查员 王国梅

[74] 专利代理机构 上海专利商标事务所有限公司
代理人 洪 玲

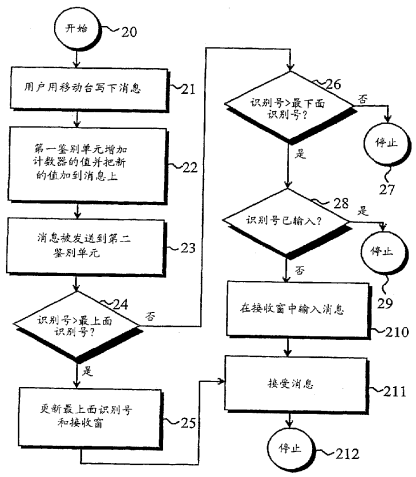
权利要求书 2 页 说明书 5 页 附图 6 页

[54] 发明名称

消息处理

[57] 摘要

本发明涉及一种在电信系统中识别数字签名消息的方法和系统，该通信系统包括通信网络（MCN）、连接于电信网络（MCN）并包含用户识别模块（SIM）的移动台（MS）、连接于电信网络（MCN）的网络服务器（NS），以及连接于网络服务器（NS）并包含移动台识别号清单的数据库（DB），这个方法中，在移动台（MS）和网络服务器（NS）之间建立连接，并且把消息保存到移动台（MS）。在这个方法中，在第一鉴别单元（FCU）中增加消息识别号，把来自第一鉴别单元（FCU）的消息识别号加到消息上，把消息发送到第二鉴别单元（SCU），在识别号中检查是否在较早已接收到此消息，并且如果还没有接收这个消息就接受它。



1．一种在电信系统中对数字签名消息进行识别的方法，该系统包括：

电信网络（MCN）；

连接于所述电信网络（MCN）并包含用户识别模块（SIM）的移动台（MS）；

连接于所述电信网络（MCN）的网络服务器（NS）；以及

连接于所述网络服务器（NS）并包含识别号清单的数据库（DB），在这个方法中：

在所述移动台（MS）和所述网络服务器（NS）之间建立连接；并且

把所述消息保存到所述移动台（MS），

其特征在于该方法包含的步骤有：

在第一鉴别单元（FCU）中增加所述消息识别号；

把来自所述第一鉴别单元（FCU）的所述消息识别号加到所述消息上；

把所述消息发送到第二鉴别单元（SCU）；

在所述识别号中检查是否在较早已经接收所述消息；以及

如果还没有接收所述消息就接受它，以及

如果所述消息的识别号超过定位在所述网络服务器（NS）中的所述识别号清单最上面的识别号，那么就接受所述消息。

2．按权利要求 1 所述的方法，其特征在于如果所述第二鉴别单元（SCU）定位在所述网络服务器（NS）中，那么把所述第一鉴别单元（FCU）安置在所述移动台（MS）中或所述用户识别模块（SIM）中。

3．按权利要求 1 所述的方法，其特征在于如果所述第二鉴别单元（SCU）定位在所述移动台（MS）中，那么把所述第一鉴别单元（FCU）安置在所述网络服务器（NS）中。

4．按权利要求 1、2 或 3 所述的方法，其特征在于如果所述消息的识别号超过所述识别号清单所述最上面的识别号，那么就移动所述识别号清单以使所述消息的识别号成为新的识别号清单的最上面的识别号。

5．按权利要求 1、2 或 3 所述的方法，其特征在于如果所述消息识别号低于所述识别号清单的所述最上面的识别号，并超过所述识别号清单的最下面的识别号，而且所述消息还没有输入而接收在所述识别号清单中，那么就接受所述消息。

6．按权利要求 1、2 或 3 所述的方法，其特征在于如果接受了所述消息，那

么就更新接收的所述识别号清单。

7．按权利要求 1、2 或 3 所述的方法，其特征在于是在移动通信的全球系统（GSM）中发送所述消息。

8．按权利要求 1、2 或 3 所述的方法，其特征在于是通过短消息服务（SMS）作为短消息传输所述消息。

9．按权利要求 1、2 或 3 所述的方法，其特征在于在数据传输期间对所述消息进行数字签名。

10．按权利要求 1、2 或 3 所述的方法，其特征在于对所述第一鉴别单元（FCU）进行编程，以致如果所述识别号增长得太大就停止操作。

11．按权利要求 1、2 或 3 所述的方法，其特征在于把所述第一鉴别单元（FCU）安置在所述用户识别模块（SIM）中。

12．一种在电信系统中对数字签名消息进行识别的系统，该系统包括：

电信网络（MCN）；

连接于所述电信网络（MCN）并包含用户识别模块（SIM）的移动台（MS）；

连接于所述电信网络（MCN）的网络服务器（NS）；以及

连接于所述网络服务器（NS）并包含移动台识别号清单的数据库（DB），在这个系统中：

在所述移动台（MS）和所述网络服务器（NS）之间建立连接；并且

把所述消息保存到所述移动台（MS），

其特征在于该系统包括：

第一鉴别单元（FCU），它包括产生所述消息识别号并把它加到所述消息上的发生器；以及

第二鉴别单元（SCU），它包括识别数字签名消息并更新所述识别号清单的鉴别器。

消 息 处 理

本发明涉及电信系统。尤其，本发明涉及一种方法和系统，其中，把识别号加到消息上以从移动台或网络服务器发送，在这之后，把消息传输到网络服务器或移动台，它的识别号清单和消息识别号帮助人们来判别是否能接受该消息。

现有技术

短消息的数字签名正变得普遍。数字签名是使人们明确识别消息发送者的电子签名。还可以使用数字签名来弄清楚发送的消息是否在数据传输期间变化的事实并可用来在消息中自动标记时间。通常数字签名的消息不是加密的，因此如果消息包括了敏感的信息，那么消息就要使用例如公共密钥方法（RSA，Rivest-Shamir-Asleman）进行加密。

短消息服务使人们能发送通常包含多达 160 个字符的短消息。消息的发送不需要接通移动台。如果不能到达移动台，则可以把该消息被保存到短消息服务中心。短消息服务中心把消息保存几天，并且如果在移动网络区域中启动了接收此消息的移动台，那么就把消息发送到移动台。或在相同小区区域中发送消息或通过移动台的漫游特点把消息发送到其他小区。当把短消息从发送者传输到接收者时，就通过通信网络的几个部件发送短消息，它们会引起在短消息行进过程中的延迟、使相互顺序消失和变化。也可以把短消息发送到其他设备，比如数字电话或电子邮件消息。

会以四种不同的方式发生电信系统中要传输的消息的交换：服务器通知、移动台通知、PUSH 或 PULL 服务。在服务器通知中，服务器把消息发送到移动台，而不期待有此消息的回答。相应地，在移动台通知中，移动台把消息发送到服务器，而不期待有此消息的回答。相反，在 PUSH 服务中，服务器把消息发送到移动台，而服务器期待对于此消息的回答。PUSH 服务可以仍旧继续由服务器发送的消息。在 PULL 服务中，移动台把消息发送到服务器，而移动台期待对于此消息的回答。在 PUSH 服务以及在 PUSH 服务中，通过发送新消息可以继续 PULL 服务。

当在移动通信系统中发送消息时，人们不得不指出所使用的消息信道已经变成很低的带宽和速率。此外，消息的发送者和接收者两者都没有一可靠的公共时

钟。

一个特定的问题是消息的识别以及注意到复本或发送或接收的消息都太迟。通常，诸如付账之类的单一交易使用数字签名的消息。在那种情况下，有一个风险就是一些外来的实体保存此消息并在想要得到经济利益的较晚时候重新发送它。把以上提到的方法称作为重复攻击。另一方面，有可能在数据发送期间使消息加倍，虽然数据发送系统工作十分正常。当发送数据的时间使消息加倍，消息到达目的地就更明显了。也可以根据几个消息的发送进行消息的纠错。

先前已知的是解决以上提到问题的方法。在数字签名之前，在消息上加上时间标记，使用所述时间标记来识别消息的发送时刻。当把消息的时间标记与接收者的时钟比较时，消息的接收者就注意消息是否是复本以及首先是否接收得达迟。拒收太迟到达的复本和消息。在移动台中这个方法相当麻烦，这是因为这个方法需要发送者和接收者两者的时钟精确同步。如果有非常迅速产生的复本，那么时间标记也是不可靠的。非常迅速产生的消息可能接收相同的时间标记，在这种情况下，没有人可以知道什么是消息的正确发送顺序。

本发明的目的是消除或至少缓和以上涉及的不足。本发明一个进一步的目的是在具有有限存储量和计算能力的移动台中以及在定位于电信网络中的服务器中提供了一种消息识别的非常简单的方法。

发明简述

本发明使人们能注意由于包括其中的信息可能不正确而会被拒绝的复本或太迟到达的数字签名消息。

本发明涉及首先保存消息的方法。在消息发送消息之前，在第一鉴别单元增加了识别号，消息标识符，并且把识别号加到消息上，通过这样使消息表现区别。对消息和消息识别号进行数字签名，并把它们通过通信网络传输到第二鉴别单元。在第二鉴别单元中，把消息识别号与在识别号清单中最上面的识别号比较。如果此消息识别号超过了识别号清单中的最上面识别号，那么就更新识别号清单，并接收此消息。如果此消息识别号低于识别号清单中最下面的识别号，那么人们知道消息接收得太迟了，在这种情况下，就拒收此消息。如果此消息识别号落在了识别号清单中最下面和最上面识别号之间，那么就通过查询识别号清单检查是否已经接收这个消息。识别号清单包括已接收的消息识别号。如果根据识别号清单还未接收消息，那么就更新识别号清单，并接收此消息。否则就拒收此消息。

为了消息的识别，在产生识别号及在接近发送的时候把它加于消息上的移动台或网络服务器中都需要第一鉴别单元。如果消息识别号增长太大，那么第一鉴别单元就注意这个情况并停止进程，例如以如此的方法使第一鉴别单元不再增加要附加到要发送的消息上的识别号。在移动通信系统的服务器中或在移动台中，需要第二鉴别单元，其中，通过把识别号与识别号的移动台特定的表现区别的识别号清单比较而识别此消息。

在一个实施例中，移动台的用户通过由他或她的移动台发送数字签名的以及已加上识别号的短消息付账。就本发明所示出的，用户在短消息中写上付账需要的信息，并把此短消息发送到识别消息的服务器。

就如与现有技术比较，本发明提供了这样的优点，它使人们能迅速容易地在数字签名消息中识别加倍的消息以及接收太迟的消息。在这样的情况下，可以使用本发明，例如用于在使用中的只有有限存储量和处理能力的移动台。本发明也可用于防止重复攻击。

附图简述

在以下部分，将参照附图借助本发明的实施例的几个例子来描述本发明，其中

图 1 表示依照本发明的一个系统；

图 2 是说明依照本发明方法的流程图；

图 3 表示依照本发明的一个实施例；

图 4 表示依照本发明的一个识别号清单；以及

图 5 表示依照本发明的一个实施例。

发明详述

图 1 表示依照本发明的一个系统。移动台 MS 包括第一鉴别单元 FCU，通常把它被安置在移动台的用户识别模块（SIM，Subscriber Identity Module）中。通过电信网络 MCN 把移动台 MS 连接于网络服务器 NS。网络服务器 NS 包括连接于数据库 DB 的第二鉴别单元 SCU。在数据库 DB 中有对于每个移动台表现区别的已接收消息的识别号清单。第二鉴别单元处理由移动台发送的消息并通过查询识别号清单而检查消息的可靠性。如果消息到达太迟或如果它是复本，那么消息就是错误的。

图 2 是表示依照本发明方法的一个示意图。首先在块 21，用户在移动电话中写下消息。在块 22，在发送这个消息之前，第一鉴别单元 FCU 在移动台中增加识别号并把新的识别号加在消息上。在块 23，对消息进行数字签名并把它发送到第二鉴别单元 SCU。在块 24，把消息的识别号 MC 与定位于网络服务器中的识别号清单的最上面的识别号 NUMC 进行比较。如果消息的识别号大于识别号清单的最上面的识别号，那么就更新识别号清单。识别号清单的一种实施是使用位寄存器，其中，使用一单独位来消息是否已经接受标志。在块 26 及 27，如果消息的识别号 MC 低于识别号清单最下面的识别号 NLWC，那么它是关于消息太迟到达而被拒收的问题。在块 28，如果此消息识别号落在了识别号清单中最下面和最上面的识别号之间，那么为了查出是否已经接收消息，查询识别号清单。在块 210 及 211，如果还没有把消息输入识别号清单，那么就把它输入识别号清单并接收消息。

图 3 表示依照本发明的一个实施例。用户在移动台中写下付账所需的信息，在图 3a 中有移动台信息显示的说明。在图 3b，在消息数字签名之前，询问该用户是否打算表现消息的区别。在图 3c，如本发明所示出，用户接受表现区别，因此把表现消息区别的标识符加于消息。对消息进行数字签名，并通过数据传输网把它发送到网络服务器。在图 3d，在成功发送消息的情况下通知用户。

图 4 表示依照本发明的一个识别号清单。在图中的线段表示消息的识别号。消息 A 的识别号与识别号清单的位置比较，消息 A 已经到达得太迟了，因此就拒收消息 A。消息 B 的识别号指向识别号清单中最下面的识别号，并因此是消息的第一可接受的识别号。消息 C 的识别号在识别号清单区域内，但不接受这个消息，因为消息的识别号已在识别号清单上了，因此较早已经接收了该消息。在识别号清单中标有 X 的点指的是已接收消息的识别号。消息 D 的识别号在识别号清单中指向最上面的可接受的消息。消息 E 的识别号超过了识别号清单，因此就移动识别号清单以使消息 E 的识别号将是新的识别号清单的最上面识别号。在移动识别号清单时，会从识别号清单中除去那些已接收消息的太低的识别号。

图 5 表示依照本发明的一个实施例。电信系统包括移动台 NID1、NID2、NID3 和数据库 NID4、NID5。保存到移动台 NID1 的是一数据库，它包括网络标识符（Network ID）、呼出消息标识符、进入消息标识符和所接受消息识别号清单。网络标识符是明确的号码，使用它来识别在电信网络中的上述设备。在图中，呼出标识符是要加到消息上的标识符，并且相应地，进入标识符是进入消息的识别号。例如，识别号包括 16 比特。在通信网络的服务器上也有类似移动台数据库的

数据库，使用它来识别发送到服务器的消息。必须注意，系统是对称的，因此如本发明所示，既识别从移动台发送到服务器的消息又识别从服务器发送到移动台的消息是可能的。

图 6 表示依照本发明的一个实施例。对于消息的识别，每个网络元件都包括信息。在移动台 MS 有 a 比特的识别号 Cs，它包含最后发送的消息的标识符值。数字签名的消息 DSM 本身包括消息 M 的内容以及识别号 Mnc。在服务器 DS 中有 a 比特的识别号 Cr，它包含这以前接收的最大识别号，以及 b 比特的识别号清单 W，在它上面存储了 B 的先前识别号的状态。可以以如此方法实现 B 比特的识别号清单 W 作为比特字段，致使 1 就表示已接收了消息。相应地，比特 0 就表示还没有接收此消息。

仅在以上提到的实施例没有限制本发明，而在权利要求书所定义的本发明理念的范围内许多变化是可能的。

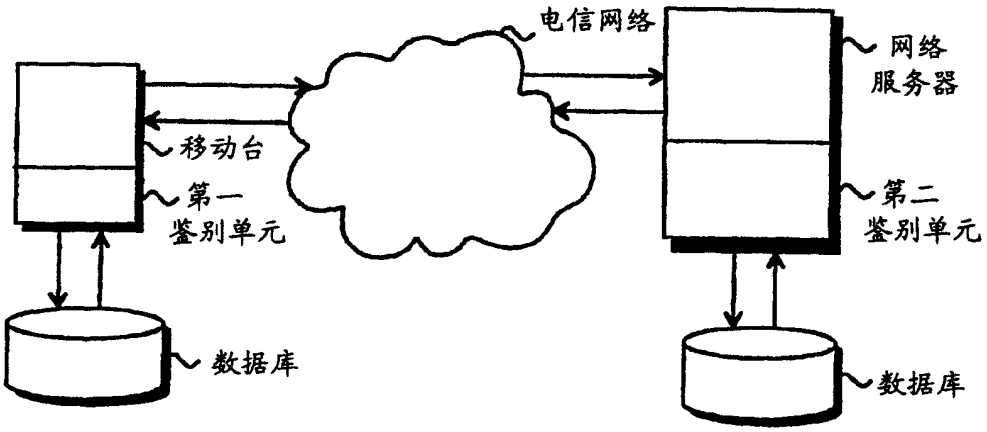


图 1

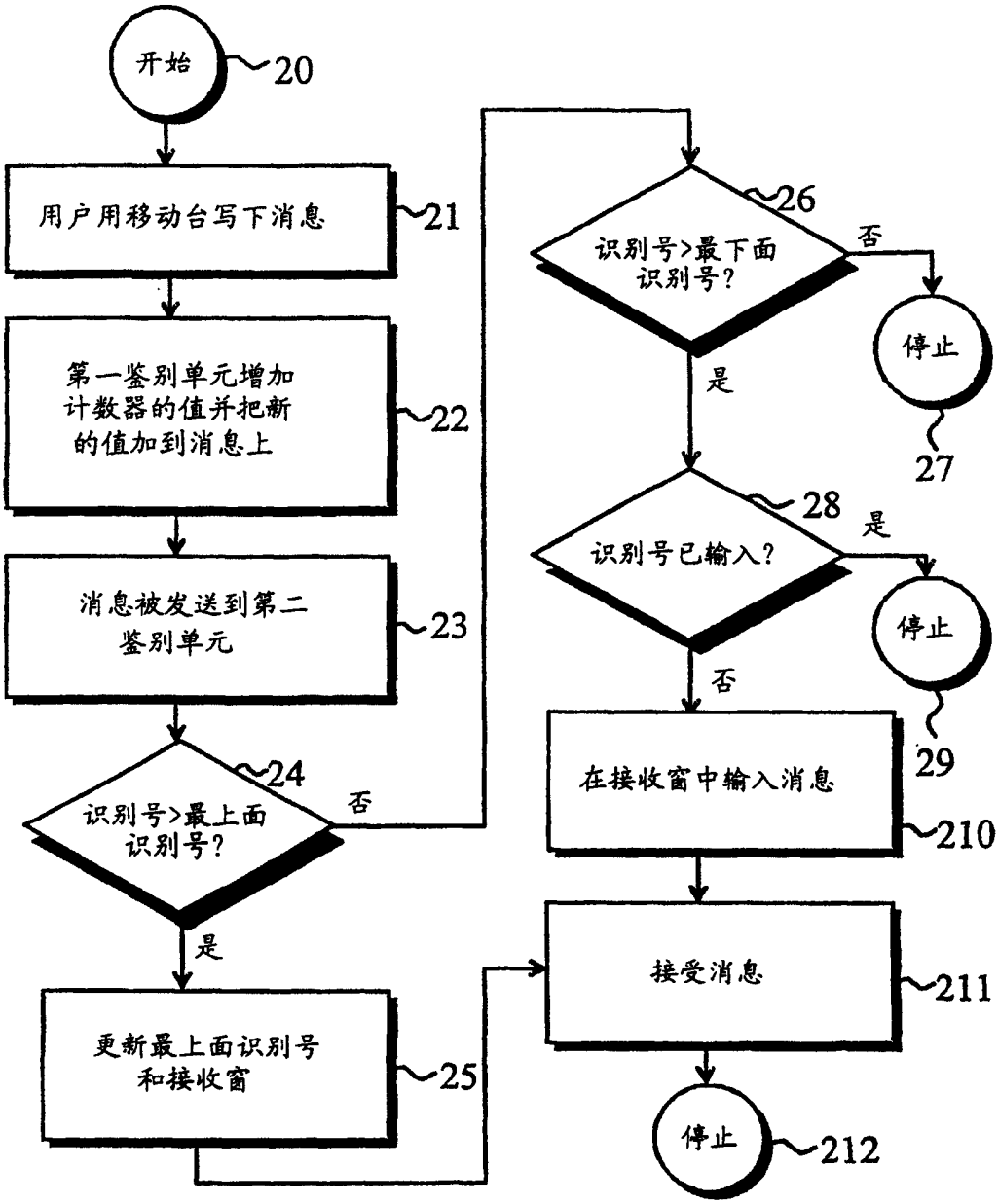

开始
20
用户用移动台写下消息
21
第一鉴别单元增加计数器的值并把新的值加到消息上
22
消息被发送到第二鉴别单元
23
识别号>最上面识别号?
24
否
是
更新最上面识别号和接收窗
25
识别号>最下面识别号?
26
否
停止
27
是
识别号已输入?
28
是
停止
29
否
在接收窗中输入消息
210
接受消息
211
停止
212

图 2

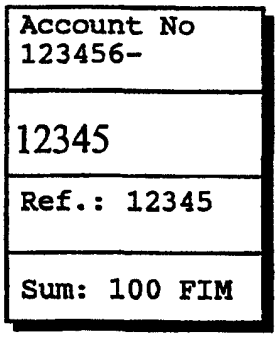


图 3a

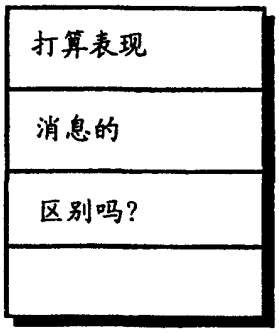


图 3b

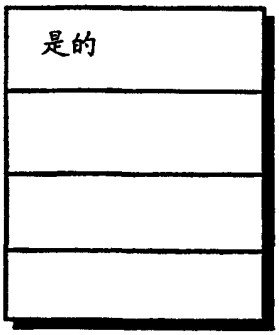


图 3c

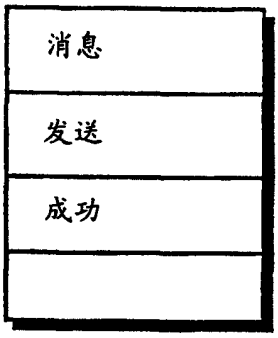


图 3d

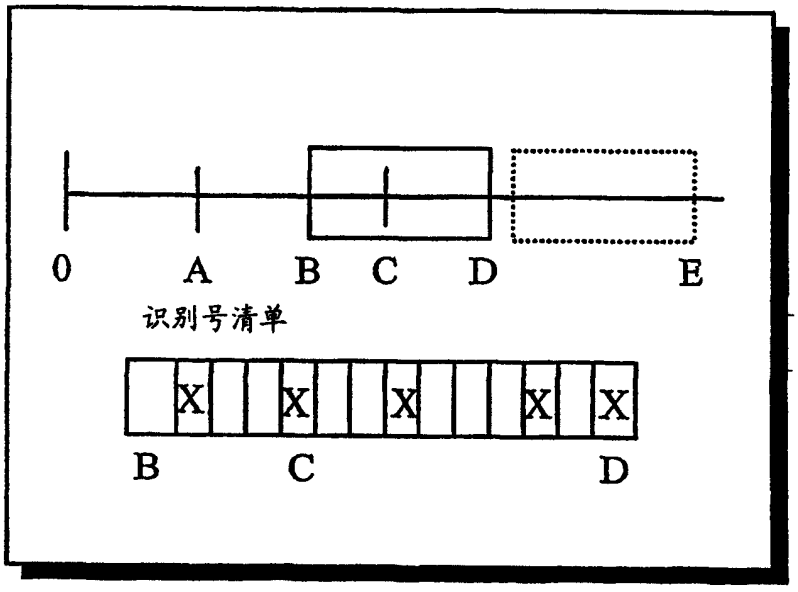


图 4

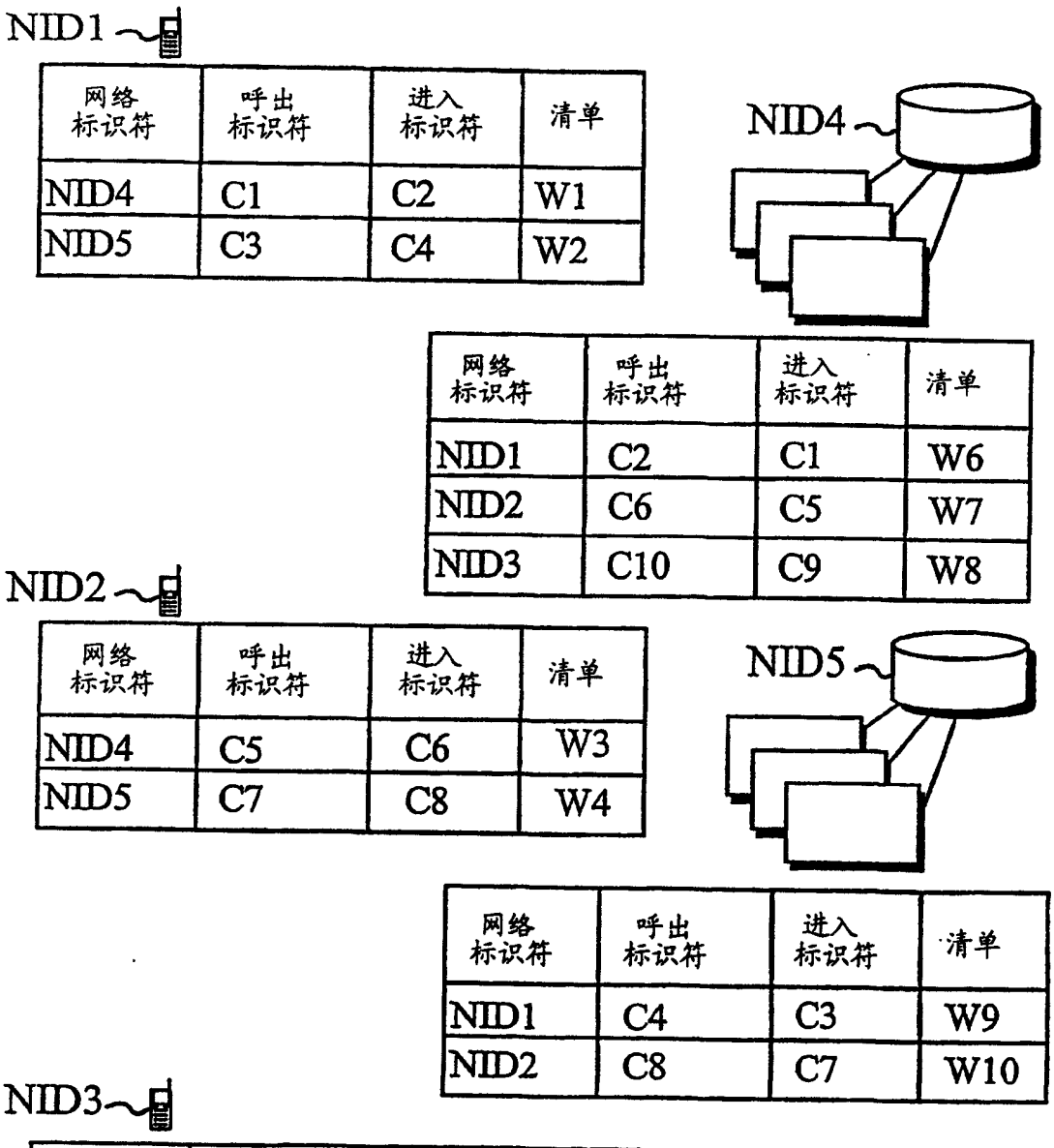

NID1
网络标识符
呼出标识符
进入标识符
清单
NID4 C1 C2 W1
NID5 C3 C4 W2
NID4
网络标识符
呼出标识符
进入标识符
清单
NID1 C2 C1 W6
NID2 C6 C5 W7
NID3 C10 C9 W8
NID2
网络标识符
呼出标识符
进入标识符
清单
NID4 C5 C6 W3
NID5 C7 C8 W4
NID5
网络标识符
呼出标识符
进入标识符
清单
NID1 C4 C3 W9
NID2 C8 C7 W10
NID3
Network id
Outgoing id
Incoming id
List
NID4 C9 C10 W5

图 5

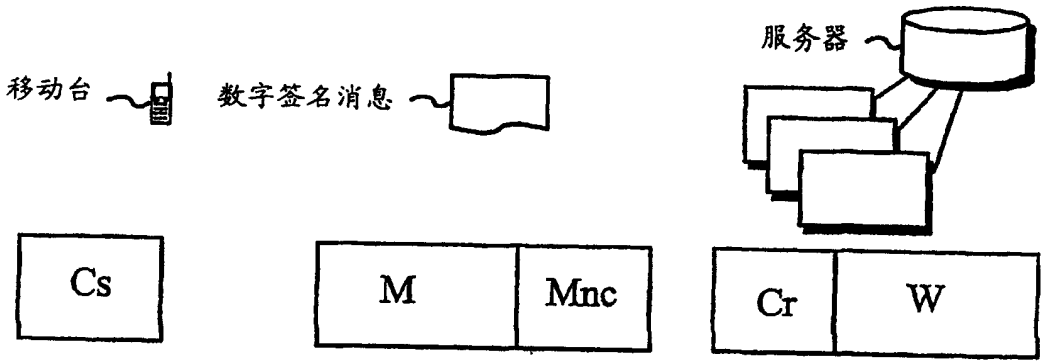


图 6