

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.



[12] 发明专利说明书

H04Q 7/38 (2006.01)

H04Q 7/34 (2006.01)

H04M 3/22 (2006.01)

专利号 ZL 00818904.8

[45] 授权公告日 2008年4月9日

[11] 授权公告号 CN 100381006C

[22] 申请日 2000.2.11 [21] 申请号 00818904.8

[86] 国际申请 PCT/EP2000/001126 2000.2.11

[87] 国际公布 WO2001/060098 英 2001.8.16

[85] 进入国家阶段日期 2002.8.9

[73] 专利权人 诺基亚公司

地址 芬兰埃斯波

[72] 发明人 加纳·易洛安塔

[56] 参考文献

US5974309A 1999.10.26

WO99/39492A1 1999.8.5

CN1209709A 1999.3.3

审查员 张宏伟

[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 董莘

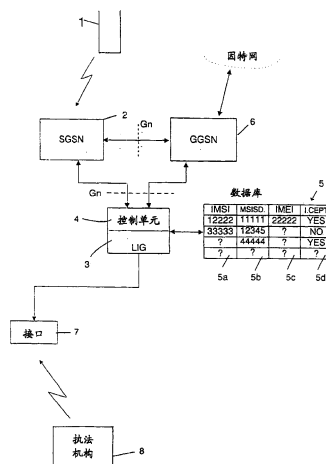
权利要求书 3 页 说明书 12 页 附图 3 页

[54] 发明名称

用于获得通信网络中被监控用户的识别信息的方法和系统

[57] 摘要

本发明提供了一种用于获得通信网络中被监控用户的识别信息的方法，在所述方法中为截接用户提供数据库，当被监控用户发起或接收到通信时，所述网络提供标识符数据以识别数据库中的用户，所述接收的标识符数据按照与对应用户的相互关系而存储在所述数据库中，以便为每个对应用户提供包含多个标识符数据的索引表。



1、一种用于获得通信网络中被监控用户的识别信息的方法，在所述方法中

为截接用户提供数据库，

当被监控用户发起或接收到通信时，所述网络提供标识符数据以识别数据库中的用户，

所述接收的标识符数据按照与对应用户的相互关系而存储在所述数据库中，以便为每个对应用户提供包含多个标识符数据的索引表；

当开始监控用户时，所述截接用户向所述数据库输入关于用户的目标标识符、用户的识别数据或用户的设备识别数据的标识符数据；

其中当所述被监控用户执行新的通信时，由支持节点生成的标识符数据，

将所述生成的标识符数据与已经存储在所述数据库中的标识符数据进行比较，

在所述被监控用户的数据库中没有包含标识符数据，或者包含的标识符数据与所述生成的标识符数据不同时，存储所述生成的标识符数据到所述数据库中。

2、根据权利要求1的方法，其中所述标识符数据是用户的目标标识符、用户的识别数据或者用户的设备识别数据。

3、根据权利要求2的方法，其中所述用户的目标标识符是用户的IP地址，所述识别数据是国际移动用户身份IMSI、用户的移动目标标识符MSISDN或3G的国际移动用户身份IMUI、或者所述设备识别是国际移动台设备身份IMEI。

4、根据权利要求1的方法，其中当开始或结束对用户的监控时，所述截接用户向所述数据库输入关于监控或不监控用户的数据。

5、一种在通信网络中监控用户的方法，包括：

为截接用户提供数据库，

当被监控用户发起或接收到通信时，所述网络提供标识符数据以识别数据库中的用户，

所述接收的标识符数据按照与对应用户的相互关系而存储在所述数据库中，以便为每个对应用户提供包含多个标识符数据的索引表；

其中监控设备在用户发起或接收通信时，检测由支持节点生成的标识符数据的出现，

将这个数据与数据库中存储的数据作比较，以及

在所述标识符数据对应于所述数据库存储中的被监控用户的目标标识符、用户的识别数据或用户的设备识别数据时，开始对所述用户进行监控；

当开始监控用户时，所述截接用户向所述数据库输入关于用户的目标标识符、用户的识别数据或用户的设备识别数据的标识符数据。

6、一种用于获得通信网络中被监控用户的识别信息的系统，其中为截接用户提供数据库，当所述被监控用户发起或收到通信时，所述网络提供标识符数据以识别数据库中的用户，

所述系统包括控制装置，用于在所述数据库中存储接收的信息，以便为每个对应用户提供包含多个标识符数据的索引表；

所述截接用户提供关于用户的目标标识符、用户的识别数据或用户的设备识别数据的标识符数据，所述控制装置在开始监控用户时将这些数据输入到所述数据库中；

其中所述控制装置比较在所述被监控用户执行新的通信时由支持节点生成的标识符数据与已经存储在所述数据库中的标识符数据，在所述被监控用户的数据库中没有包含标识符数据，或者包含的标识符数据与所述生成的标识符数据不同时，存储所述生成的标识符数据到所述数据库中。

7、根据权利要求6的系统，其中所述标识符数据是用户的目标标识符、用户的识别数据或者用户的设备识别数据。

8、根据权利要求7的系统，其中所述用户的目标标识符是用户的IP地址，所述识别数据是国际移动用户身份IMSI、用户的移动目标标识符MSISDN或3G的国际移动用户身份IMUI、或者所述设备识别是国际移动台设备身份IMEI。

9、根据权利要求6的系统，其中所述截取用户提供关于监控或不监控用户的数据，所述控制装置在开始或结束对用户的监控时将这些数据输入到所述数据库中。

10、一种在通信网络中监控用户的系统，

其中为截取用户提供数据库，当所述被监控用户发起或收到通信时，所述网络提供标识符数据以识别数据库中的用户，

所述系统包括控制装置，用于在所述数据库中存储接收的信息，以便为每个对应用户提供包含多个标识符数据的索引表；

其中所述控制装置检测在用户发起或接收通信时生成的标识符数据的出现，将所述数据与存储在数据库中的数据作比较，在所述数据对应于存储在所述数据库中的标识符数据且对应于被监控用户时，开始对所述用户进行监控；

所述截取用户提供关于用户的目标标识符、用户的识别数据或用户的设备识别数据的标识符数据，所述控制装置在开始监控用户时将这些数据输入到所述数据库中。

用于获得通信网络中被监控用户的 识别信息的方法和系统

技术领域

本发明一般针对包括移动通信或固定通信在内的通信领域，例如移动通信和通过诸如固定数据网的固定网络的通信。本发明尤其针对一种用于获得被合法截接（监控）的个人或设备的识别信息的方法和系统，以及用于监控这种个人或设备的方法和系统。

背景技术

美国 5974309 公开了一种用于通过执法机构监控蜂窝电话呼叫的方法和装置。这里，当有电话呼叫被监控用户时，执法机构检查帐单识别号，或主叫线路识别信息用以识别主叫用户。

通常，当监控由诸如 GSM 系统（全球移动通信系统），或诸如 GPRS（通用分组无线电业务）的分组交换网络，或 UMTS（通用移动通信系统）中的被监控用户发出或接收的通信时，在正确追踪待监控用户上将出现问题。官方已知的监控（截接）标准通常为被监控用户的移动目标标识符（MSISDN，用户的移动目标标识符）（如电话号码）。因此截接激活通常是基于 MSISDN 的。然而，当罪犯知道了截接激活后，他们可例如使用预付费 SIM（用户身份模块）卡，这样基于 MSISDN 的截接变得相当困难。或许有人考虑使用 IMEI（国际移动台设备身份）作为截接激活的标准，因为被监控用户更换他们的设备而不是更换通常免费的 SIM 卡要更麻烦和昂贵。在 GSM 中，存在附加信息 IMSI（国际移动用户身份），它能以唯一方式在内部识别用户。然而，激活该截接的管理机构（通常为执法机构，但最终也可以是经官方许可的私人机构或类似机构）并不知道 IMSI，因此在实际应用中 MSISDN 更为方便。

通常，MSISDN 和 IMSI 具有一一对应关系，其映射信息储存在 HLR（归属位置寄存器）中。尽管在理论上因此可利用 HLR 信息将 MSISDN 映射为 IMSI，但这种映射需要耗费时间的过程，因此如果可能的话应予以避免。此外，HLR 定期被更新，这使得在截接设备中保存正确的映射信息很费力。此外，IMEI 并不是 HLR 信息的一部分，因为用户到 IMEI 的映射通常只在短时间内有效，可能仅对一个移动连接有效。

因此需要一种方法和系统能够提供有用于监控的信息，或者以可靠和简单的方式实现这种监控。

发明内容

本发明旨在提供一种方法和系统，其中不用访问诸如 HLR 的大容量存储器就能自动分配关于一个或多个被监控用户的若干识别信息。

根据本发明的一个方面，提供了一种用于获得通信网络中被监控用户的识别信息的方法，在所述方法中

为截接用户提供数据库，

当被监控用户发起或接收到通信时，所述网络提供标识符数据以识别数据库中的用户，

所述接收的标识符数据按照与对应用户的相互关系而存储在所述数据库中，以便为每个对应用户提供包含多个标识符数据的索引表；

当开始监控用户时，所述截接用户向所述数据库输入关于用户的目标标识符、用户的识别数据或用户的设备识别数据的标识符数据。

根据本发明的另一个方面，提供了一种在通信网络中监控用户的方法，包括：

为截接用户提供数据库，

当被监控用户发起或接收到通信时，所述网络提供标识符数据以识别数据库中的用户，

所述接收的标识符数据按照与对应用户的相互关系而存储在所述

数据库中，以便为每个对应用户提供包含多个标识符数据的索引表；

其中监控设备在用户发起或接收通信时，检测由支持节点生成的标识符数据的出现，

将这个数据与数据库中存储的数据作比较，以及

在所述标识符数据对应于所述数据库存储中的被监控用户的目标标识符、用户的识别数据或用户的设备识别数据时，开始对所述用户进行监控；

当开始监控用户时，所述截接用户向所述数据库输入关于用户的目标标识符、用户的识别数据或用户的设备识别数据的标识符数据。

根据本发明的再一个方面，提供了一种用于获得通信网络中被监控用户的识别信息的系统，其中为截接用户提供数据库，当所述被监控用户发起或收到通信时，所述网络提供标识符数据以识别数据库中的用户，

所述系统包括控制装置，用于在所述数据库中存储接收的信息，以便为每个对应用户提供包含多个标识符数据的索引表；

所述截接用户提供关于用户的目标标识符、用户的识别数据或用户的设备识别数据的标识符数据，所述控制装置在开始监控用户时将这些数据输入到所述数据库中。

根据本发明的再一个方面，提供了一种在通信网络中监控用户的系统，

其中为截接用户提供数据库，当所述被监控用户发起或收到通信时，所述网络提供标识符数据以识别数据库中的用户，

所述系统包括控制装置，用于在所述数据库中存储接收的信息，以便为每个对应用户提供包含多个标识符数据的索引表；

其中所述控制装置检测在用户发起或接收通信时生成的标识符数据的出现，将所述数据与存储在数据库中的数据作比较，在所述数据对应于存储在所述数据库中的标识符数据且对应于被监控用户时，开始对所述用户进行监控；

所述截接用户提供关于用户的目标标识符、用户的识别数据或用

户的设备识别数据的标识符数据，所述控制装置在开始监控用户时将这些数据输入到所述数据库中。

例如，不用 HLR 就能映射 MSISDN 和/或 IMEI 到 IMSI。这就带来了诸多方便。首先，映射更新的识别信息非常有效。其次，当更新 HLR 时无需更新映射信息，这样就可避免一致性问题。第三，所提出的解决方案也适合于使用由不同制造商生产的 HLR 的移动网络。由于在 HLR 和执法机构的截接设备之间没有定义标准化接口，做到截接设备与不同 HLR 之间兼容很困难，实际上可能甚至做不到。另外，避免了截接设备访问 HLR 时出现的困难，如不同的通信协议和接口，在 HLR 中必需用于截接的补充业务，信息转换效率低下，以及需要大存储量的 HLR 来存储关于大量用户记录的数据。此外，不需要修改 HLR，而且截接设备和 HLR 之间不必有特定接口。

此外，提供存储了指向被监控用户的不同识别信息之间的对应表（索引表）的数据库使得截接也可基于通常不能被利用的信息。例如，截接基于 IMEI 也是可能的。对于与其归属网络没有签订漫游合同的来访用户（在这种情况下，无法访问来访用户网络的 HLR），基于这种信息（例如 IMEI 和/或 MSISDN）的截接也是可能的。存储为达到监控目的所必需的识别信息的小型数据库就足够了。与 HLR 相比这种做法的处理和管理很容易。如果允许当前有效连接的截接数据丢失，那么在截接设备中就不再需要对应数据库。同样，如果由于出错丢失了这个数据库，那么只丢失当前有效连接的截接数据，当监控被监控用户执行的下一次通信时，还有重建对应数据库的可能性。

用户的目标标识符可以是用户的 IP 地址，识别数据可以是 IMSI，MSISDN 或 IMUI（国际移动用户身份），而设备识别可以是 IMEI。

附图说明

图 1 是根据本发明的系统的实施例的基本结构，

图 2 是本发明的方法的实施例的流程图，及

图 3 是用于开始截接的方法的流程图。

具体实施方式

图 1 示出了移动台 1，它以一种已知方式通过无线电波与支持节点 2 通信。本发明适用于所有类型的网络，如包含电路交换的 GSM 系统，或诸如 UMTS 或 GPRS 的分组交换系统。本发明当然也适用于实现移动或固定通信的任何其他通信网络。此外本发明也适用于纯分组交换的类似未来全 IP 网络。下面将重点参考 GPRS 系统为例描述本发明，但发明并不局限于此。在 GPRS 系统中，支持节点可以是正服务 GPRS 支持节点(SGSN)，通过诸如 Gn 指示的接口与网关 GPRS 支持节点(GGSN) 6 通信。网关节点 6 也可与其他网络通信，如图 1 所示的因特网。

为达到监控目的，该系统包括合法截接网关(LIG) 3，其中包含有控制单元 4。网关 3 另外包括，或者说与存储用以识别用户(例如用户或网络的来访者)的识别数据的数据库 5 合作。网关 3 借助接口 7 从诸如执法机构 8 的截接用户接收信息，并将信息发送给截接用户。接口 7 可以是类似于支持节点 2 的支持节点。在此使用的术语“执法机构”代表可对某个设备或个人，如在本例中使用移动台 1 的罪犯，的通信进行合法监控(截接)的任何类型的官方或私人机构或个人。在此使用的术语通信并不局限于传统的电话呼叫，而是也指 SMS(短信息业务)或 WAP(无线应用协议)连接或任何其他类型的连接。

本发明允许基于识别信息，即，每次激活新连接时由支持节点 2 和/或网关节点 6 通过接口 Gn 向合法截接网关 3 发送的标识符数据(优选 MSISDN, IMEI, IMSI)，激活合法截接。网关 3 在数据库 5 中存储该识别信息。因此，数据库 5 最终为一个或多个被监控用户存储了识别信息之间的对应关系的索引表，如 MSISDN-IMEI-IMSI。这使得截接可基于数据库 5 中存储的任何一个参数。

合法截接网关 3 可以是例如通常在 GPRS 系统中使用的普通网关，具有管理数据库 5(借助控制单元 4)，接收从支持节点 2 或 6 发送的识别信息以及将所述识别信息输入到数据库中的正确位置的附加功

能。

在本例中，数据库 5 具有二维的类似矩阵的结构，包括 5a 到 5d 四列和依赖于所列条目数的任意行数。5a 列存储唯一的用户识别信息 IMSI（国际移动用户身份）。5b 列包含用户的目标标识符，在此为 MSISDN（移动用户 ISDN 号）。5c 列用于存储设备识别信息，在此为 IMEI（国际移动台设备身份）。第四列 5d 包含用于决定截接或不截接用户的数据。在本例中，将监控在数据库的第一和第三行注册的用户，而不（或不再）截接第二行列出的用户。数据库 5 由此在各行存储了一张索引表，表示指向同一个人或设备的个体识别信息之间的对应关系。

一般来说，一旦支持节点 2 和蜂窝电信网络的所有其他支持节点被激活，它们就会通知合法截接网关 3 出现新的连接。支持节点发出从用户（移动台 1）接收到的识别信息，例如，如果是 SGSN 则识别信息为 IMSI，MSISDN 和 IMEI，或如果是 GGSN 则识别信息为 MSISDN 和 IMSI。因此，截接设备（网关 3）能在用户使用网络时了解 IMSI-MSISDN 和 IMSI-IMEI 之间的对应关系，网关 3 存储这个识别信息 MSISDN-IMEI-IMSI，因而在之后的激活截接时能方便使用它。由网关 3 和数据库 5 构成的截接设备在认识到最近一次用户活动后诸如 IMEI 的一些信息发生了改变，就会更新数据库 5。

详细地说，支持移动台 1 的各个支持节点 2 或网关节点 6，在每次用户激活会话或隧道时通知网关 3。一旦收到关于会话或隧道激活的通知，网关 3 就检查在其数据库 5 中是否已经有相应信息。如果数据库 5 中没有包含匹配条目，网关 3 向数据库 5 中添加该可用信息。如果数据库 5 对于一个或多个 IMSI 识别信息，包含不同于发出的 MSISDN 或 IMEI 信息的 MSISDN 和/或 IMEI 信息，网关 3 更新数据库 5 以便包括该新信息。

因此支持节点 2，6 适合于一开始激活就向网关 3 发送识别信息。除此之外，不必修改支持节点。网关 3 通过参考数据库 5 并读出相应数据转换发送的 MSISDN 和 IMEI 信息为 IMSI 识别信息。如果数据

库 5 在某些情况下，当前没有对应激活截接的 IMSI 信息的关于 MSISDN 或 IMEI 的任何信息，这意味着被监控用户没有启动任何通信，因为截接设备（网关 3）已经连接到该网络。被监控用户一拨打电话，就可获得对应 IMSI 信息的 MSISDN 和/或 IMEI 识别信息，这样就可以开始截接。因此截接总是在被监控用户实际传送任何数据之前被激活。

可以对网关 3 的数据库 5 进行管理，以便仅对在列 5d 截接决定被设为“yes”的行注册识别信息。在可选结构中，截接设备也可适合于在数据库 5 中为自开始激活截接设备以来变得有效的所有主叫注册所有识别信息 IMSI, MSISDN, IMEI。在此情况下，随着每个附加用户变得有效，数据库的容量变得越来越大。后面这种情况具备的优点是，拥有过去变得有效的所有用户的所有可用识别信息的索引表。因此，当重新开始截接用户时，通常数据库已经包括了各个用户的全部或者至少一些识别信息。当检测到一个表征被监控用户开始进行通信的识别信息时，就可立即开始截接。

如果数据库变得过大，总是存在简单地全部清空或者至少清空所有包含截接命令为“no”的行的可能性。这样做也有助于容易从错误状态中恢复，因为数据库 5 根本不需要恢复或仅有部分需要恢复，而且对于在清空或错误恢复后变得有效的任何用户来说，数据库 5 总是能被重新填满。

根据一个可选实施例，可对网关 3 编程以便总是从数据库 5 中删除当前无效，即不实施呼叫的所有用户。该可选实施例适用于网关 3 仅需要关于有效用户的信息时。在此情况下，支持节点 2 通知截接设备，即网关 3，何时连接结束。在此情况下，数据库 5 总是储存当前有效用户的列表。如果执法机构 8 应通过发送用户的目标标识符通知网关 3 监控用户的新请求时，例如，网关 3 通过参考数据库 5 可很容易检查这个用户当前是否正在进行通信，而且能够立即开始接收和存储往返相应的目标标识符发送的消息。

另一可能性是将数据库 5 的尺寸限制到一个固定值，这样就能简

化其实现。在此情况下，应尽可能从数据库 5 中删除关于非监控用户的任何信息，以避免因空闲容量过小而导致的任何存储问题。

下面提供对数据库 5 内容变化的详细描述。

假设

1. 每当激活隧道/会话时，截接设备 3 都将从节点 2 得到“开始”的通知。这些消息总是包含 IMSI，还可选择地包含 MSISDN 和/或 IMEI。
2. IMEI 检查能否在 SGSN 节点 2 触发。
3. 截接设备 3 采集数据库 5 中的 IMSI-MSISDN-IMEI 三元组（MSISDN 或 IMEI 可以省略）。
4. 截接设备 3 只在非永久性存储器存储数据库 5，而且每当数据库 5 变得过大就删除三元组（行）。然而截接设备 3 不会删除当前有效的用户的三元组。
5. 数据库 5 包含关于是否激活截接的信息。
6. 每当终止隧道/会话时，截接设备 3 就会从节点 2 得到“结束”的通知。这些消息包括至少 IMSI。

起初数据库 5 是空的。当管理机构（机构 8）对 MSISDN=11111 激活截接时，数据库被更新为：

数据库：（IMSI=?，MSISDN=11111，IMEI=?，Intercept=Yes）

机构 8 对 IMEI=22222 激活另一截接，数据库 5 被更新为：

数据库：（IMSI=?，MSISDN=11111，IMEI=?，Intercept=Yes）

（IMSI=?，MSISDN=?，IMEI=22222，Intercept=Yes）

当机构 8 对 IMSI=33333 激活截接时，数据库 5 被更新为：

数据库：（IMSI=?，MSISDN=11111，IMEI=?，Intercept=Yes）

（IMSI=?，MSISDN=?，IMEI=22222，Intercept=Yes）

（IMSI=33333，MSISDN=?，IMEI=?，Intercept=Yes）

当从 GGSN (节点 2) 到达开始 (IMSI=33333, MSISDN=12345) 通知时, 数据库被更新如下:

数据库: (IMSI=?, MSISDN=11111, IMEI=?, Intercept=Yes)
(IMSI=?, MSISDN=?, IMEI=22222, Intercept=Yes)
(IMSI=33333, MSISDN=12345, IMEI=?, Intercept=Yes)

对 IMSI=33333 使用常规过程来激活截接。之后, 接收到来自 SGSN(节点 2)的开始通知(IMSI=12222, MSISDN=11111, IMEI=?)。数据库 5 被更新为:

数据库: (IMSI=12222, MSISDN=11111, IMEI=? , Intercept=Yes)
(IMSI=?, MSISDN=?, IMEI=22222, Intercept=Yes)
(IMSI=33333, MSISDN=12345, IMEI=?, Intercept=Yes)

尽管管理机构已经对 MSISDN=11111 激活了截接, 但对 IMSI=12222 仍可激活截接。这是正确的做法是因为 IMSI 和 MSISDN 具有一一对应关系。

接着从 SGSN 节点 2 接收到开始通知 (IMSI=12222, MSISDN=11111, IMEI=22222)。数据库 5 被更新同时执行常规截接激活过程。在此情况下, 由于 IMSI 和 MSISDN 映射, 头两行合并。

数据库 5:

(IMSI=12222, MSISDN=11111, IMEI=22222, Intercept=Yes)
(IMSI=33333, MSISDN=12345, IMEI=?, Intercept=Yes)

接下来, 从 SGSN 节点 2 接收到开始通知 (IMSI=88888, MSISDN=?, IMEI=22222)。现在从数据库 5 就可找到 IMEI, 但 IMSI 并不映射到当前的 IMEI。这表明该 IMEI 目前正被另外一个 SIM 卡使用。旧的 IMEI 信息被清除并向数据库 5 中添加一个新条目。

IMSI-MSISDN 的对应关系仍然有效并且无需清除。

IMI: (IMSI=12222, MSISDN=11111, IMEI=?, Intercept=Yes)
(IMSI=33333, MSISDN=12345, IMEI=?, Intercept=Yes)
(IMSI=88888, MSISDN=?, IMEI=22222, Intercept=Yes)

现在对 **IMSI=88888** 来说截接被激活。接下来，机构 8 对 **IMSI=33333** 去活截接同时更新数据库 5；然而，该记录并不从数据库 5 中删除，因为如果需要的话，现在对 **MSISDN=12345** 激活截接更为有效。此外，如果对于该截接存在有效的隧道或会话，则不能清除该记录（因为接下来的再激活将释放当前有效的隧道或会话的其余部分）。

数据库 5:

(IMSI=12222, MSISDN=11111, IMEI=?, Intercept=Yes)
(IMSI=33333, MSISDN=12345, IMEI=?, Intercept=No)
(IMSI=88888, MSISDN=?, IMEI=22222, Intercept=Yes)

接下来，截接设备接收“结束 (IMSI=33333)”。为节省空间，数据库的第三行被删除。应指出，之所以能删除这一行是因为该 **IMSI** 没有有效的会话，而且该 **IMSI**（或相关的 **MSISDN/IMSI**）不处于截接状态。

数据库: (IMSI=12222, MSISDN=11111, IMEI=?, Intercept=Yes)
(IMSI=88888, MSISDN=?, IMEI=22222, Intercept=Yes)

通常情况下，为了不释放任何截接数据，数据库 5 总是必须为当前有效的会话/隧道保存信息。然而，如果尽管截接变得有效也允许忽略当前有效的连接，那么在数据库 5 中只需保存当前有效并且处于截接状态的记录。这里所有处于截接状态的记录都保存在数据库 5 中，因为在本例中数据库 5 也用做目标数据库。

一些门限可基于数据库 5 更新设置。一个例子是按照 **IMEI** 存储在一些时段内使用的不同 **SIM 卡 (IMSI)** 的数量。通过这种方法，

可警告管理机构有“可疑的”IMEI；还可能将所使用的 IMEI 和 MSISDN 传送给管理机构。

图 2 示意性地给出了一种用于获得识别信息和更新数据库 5 的方法的流程图。在步骤 S1，执法机构 8 向网关 3 发送与被监控用户相关的数据。网关 3 中的控制单元 4 将这个数据（例如目标标识符）输入到数据库 5 中，并将对应行的截接标志（5d 列）设为“yes”（步骤 S2）。在步骤 S3，网络检查是否有一个新用户开始通信。如果没有，系统保持在等待状态。如果有，支持节点 2 将与主叫相关的目标标识符、用户识别数据和/或设备识别数据的可用数据发送给合法截接网关 3（步骤 S4）。此后，合法截接网关 3 检查这个数据是否已经包含在数据库 5 中或者是否为新数据。如果是新的，将这个识别数据存储到数据库 5 中（步骤 S5）。

图 3 是用于决定截接或不截接呼叫的流程图。当一方（用户或来访者）开始启动通信时（步骤 S6）该过程开始。处理这次通信的支持节点向合法截接网关 3 发送信息，通知它用户开始通信（步骤 S7）。这个信息在此称为“开始”，并且包括可能得到的所有用户识别信息（MSISDN, IMSI 和/或 IMEI）。网关 3 的控制单元 4 选择在“开始”通知中包含的这个识别信息，并将它与在包含“interception: YES”指示的数据库行中出现的识别信息作比较（步骤 S8）。因此，即使在对于被监控用户仅有部分识别信息，如“IMSI”，出现在数据库 5 中时，控制单元 4 也能检测该 IMSI 信息与“开始”通知中包含的信息的一致性，并且即使在执法机构 8 根本不知道该 IMSI 信息并因此无法向数据库 5 提供相应信息的情况下，开始截接该呼叫（步骤 S9）。因此成功截接被监控呼叫的可能性提高了。如果在步骤 S8 的判断为“no”，截接程序转到步骤 S10，不执行截接就结束了。

尽管上面对本发明的描述主要是关于 GPRS 的，但本发明也可应用于其他网络标准，例如 UMTS，或一般来说应用于移动通信网络。此外，本发明也可应用于固定网络，如有线约束的电信网，或者分组或电路交换的固定数据网。

本发明也可用于全 IP 交换网,其中目标地址可以是在截接系统的数据库注册的 IP 地址。

图 1

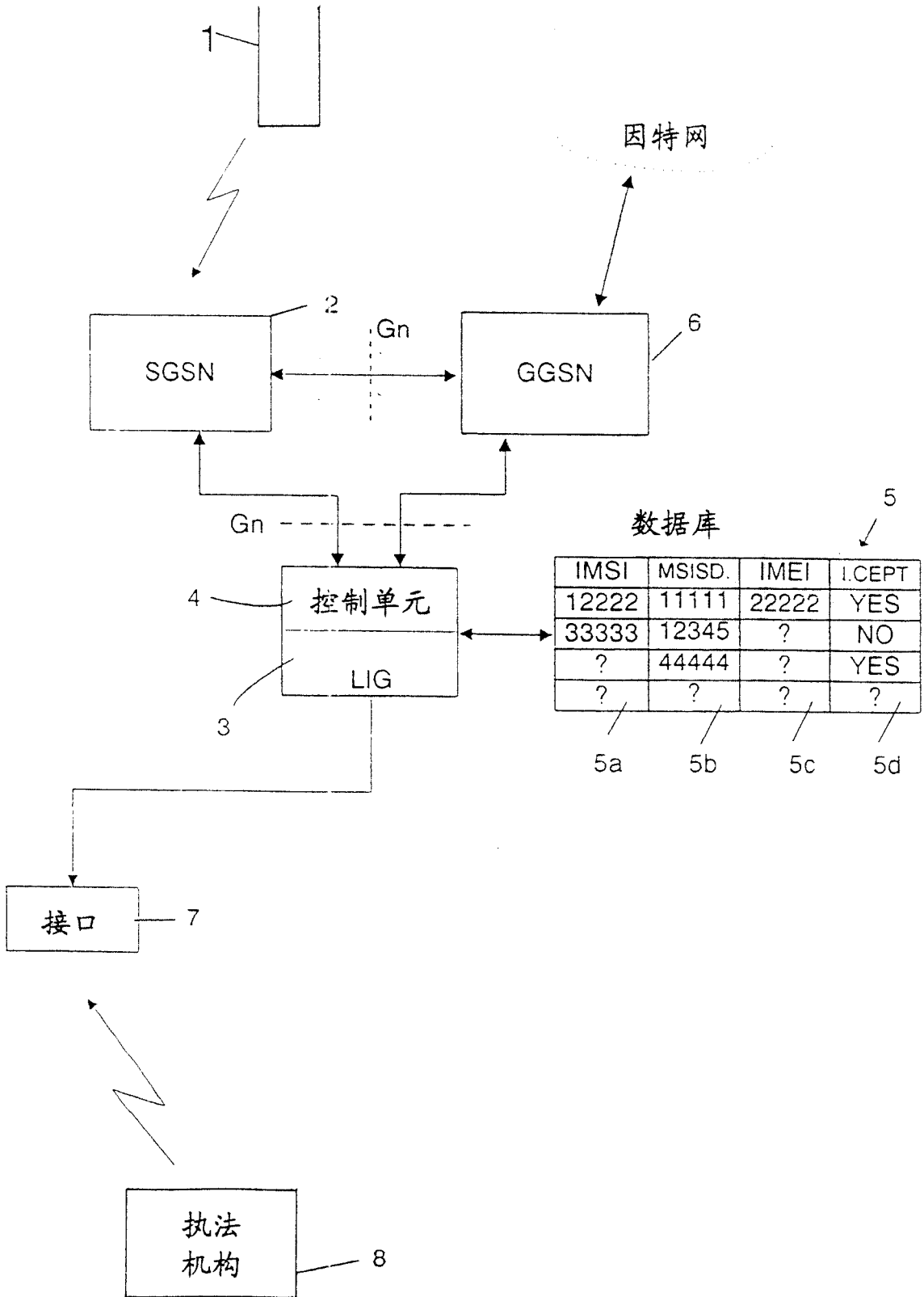


图 2

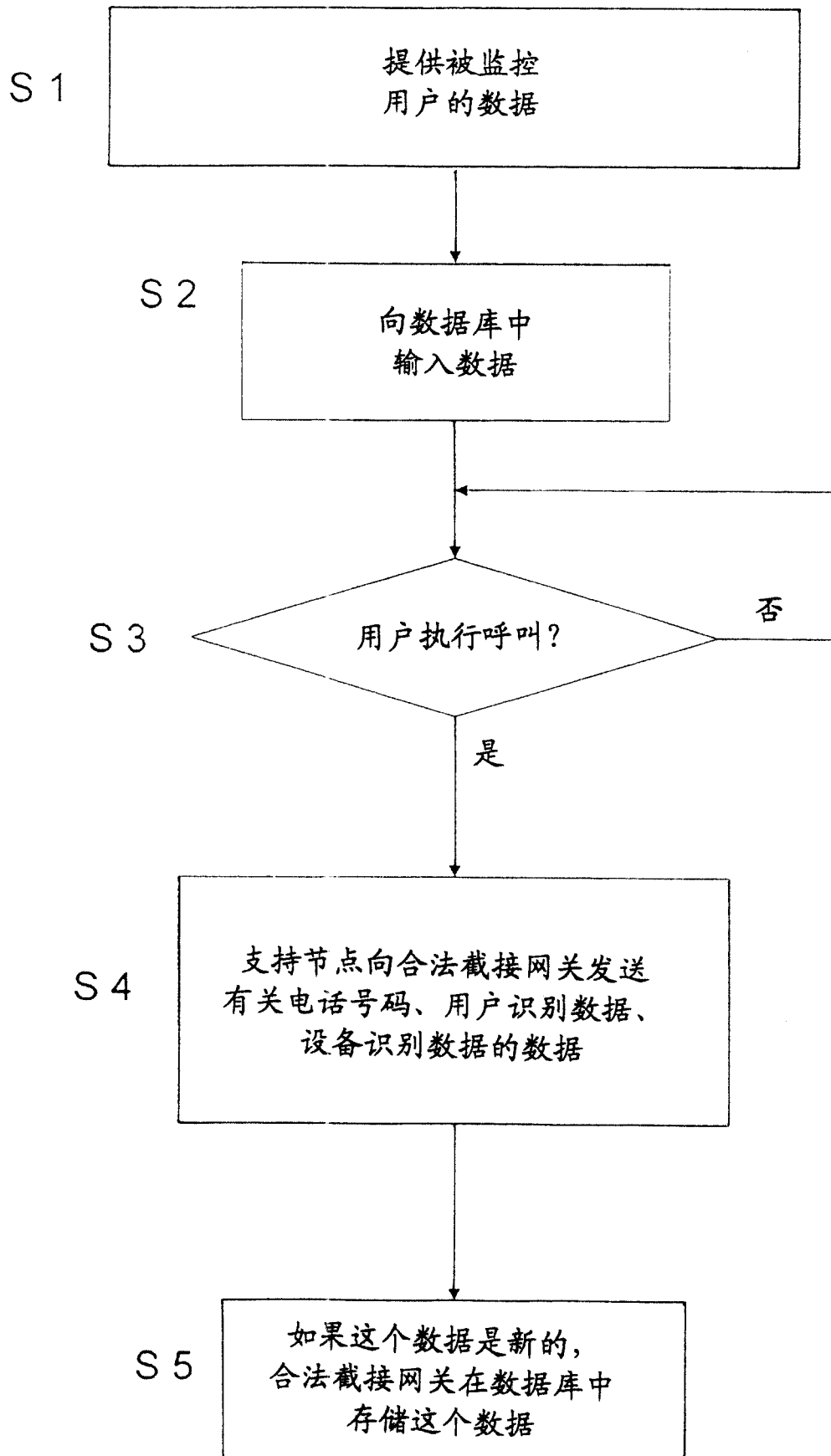


图 3

