[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/32 (2006.01)
H04M 11/04 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710000620.5

[43] 公开日 2008 年 7 月 16 日

[11] 公开号 CN 101222692A

[22] 申请日 2007.1.9
[21] 申请号 200710000620.5
[71] 申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦
[72] 发明人 刘 轶 史幸川 陈 刚

[74] 专利代理机构 北京康信知识产权代理有限责任公司
代理人 李 伟 吴孟秋

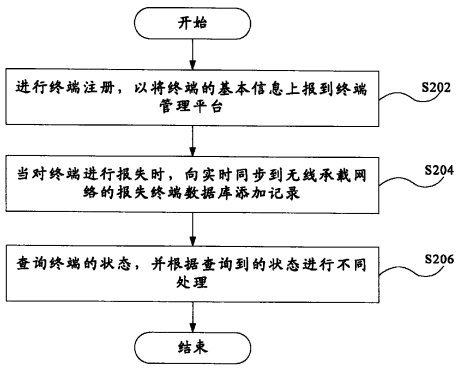
权利要求书 3 页 说明书 13 页 附图 6 页

[54] 发明名称

基于终端管理业务的终端防盗方法

[57] 摘要

本发明公开了一种终端防盗方法，用于基于终端管理业务进行终端防盗，该方法包括以下步骤：步骤 S202，进行终端注册，以将终端的基本信息上报到终端管理平台；步骤 S204，当对终端进行报失时，向实时同步到无线承载网络的报失终端数据库添加记录；以及步骤 S206，查询终端的状态，并根据查询到的状态进行不同处理。 因此，最大限度的保护了私人数据，增加了用户重新获得丢失终端的可能性。



1. 一种终端防盗方法，用于基于终端管理业务进行终端防盗，其特征在于，包括以下步骤：

步骤 S202，进行终端注册，以将所述终端的基本信息上报到终端管理平台；

步骤 S204，当对所述终端进行报失时，向实时同步到无线承载网络的报失终端数据库添加记录；以及

步骤 S206，查询所述终端的状态，并根据查询到的所述状态进行不同处理。

2. 根据权利要求 1 所述的终端防盗方法，其特征在于，所述步骤 S206 包括以下步骤：

步骤 A，查询所述终端的 SIM/USIM 卡的状态，如果所述 SIM/USIM 卡处于开机状态，则判断所述 SIM/USIM 卡是否与所述终端配合使用，并根据判断结果进行不同处理；

步骤 B，如果所述 SIM/USIM 卡没有处于开机状态，则查询终端管理数据库中是否有关于所述终端的 IMEI/IMSI 的变更记录，并根据查询结果进行相应处理；以及

步骤 C，如果所述步骤 A 和所述步骤 B 失败，则终端管理服务器实时监测，当监测到所述终端时，进行相应处理。

3. 根据权利要求 2 所述的终端防盗方法，其特征在于，在所述步骤 A 中，如果判断结果为是，则通知终端业务服务器触发第一防盗软件，如果判断结果为否，则通知使用所述 SIM/USIM

卡的终端，所述SIM/USIM卡为报失卡，并禁止所述SIM/USIM卡的业务。

4. 根据权利要求2所述的终端防盗方法，其特征在于，在所述步骤B中，如果所述终端管理数据库中有所述变更记录，则查询新的SIM/USIM卡的状态，如果所述终端处于开机状态，则所述终端管理服务器触发所述第一防盗软件。

5. 根据权利要求2所述的终端防盗方法，其特征在于，在所述步骤C中，当检测到所述终端时，还包括以下步骤：

判断所述终端是否使用所述SIM/USIM卡开机，当判断结果为是时，由所述无线承载网络通知所述终端管理服务器触发所述第一防盗软件；以及

当判断结果为否时，在所述终端更换新SIM/USIM卡第一次开机时，所述终端管理服务器根据所述终端的注册信息监测到所述终端，并通过查询注册的IMEI/IMSI对应关系，对所述终端应用所述第一防盗软件。

6. 根据权利要求5所述的终端防盗方法，其特征在于，还包括以下步骤：

如果所述终端管理服务器对所述终端应用所述第一防盗软件失败，则在所述终端每次开机注册时，所述无线网络都通知所述终端管理服务器所述终端为报失终端，所述终端管理服务器将重新对所述终端应用第一防盗软件。

7. 根据权利要求1至6任一项所述的终端防盗方法，其特征在于，还包括以下步骤：

步骤S208，以预定方式通知所述终端的使用用户，所述终端为报失终端，并在指定时间内返回营业厅进行相应处理；

步骤 S210，如果在所述指定时间内返回营业厅，则利用 FOTA 功能对所述终端进行版本恢复；以及

步骤 S212，如果在所述指定时间内没有返回营业厅，则在检测到所述终端处于开机状态时，则对所示终端应用第二防盗软件。

8. 根据权利要求 7 所述的终端防盗方法，其特征在于，在所述步骤 S208 中，还包括以下步骤：永久删除用户数据。

9. 根据权利要求 7 所述的终端防盗方法，其特征在于，在所述步骤 S212 中，还包括以下步骤：永久删除用户数据。

10. 根据权利要求 3 至 6 任一项所述的终端防盗方法，其特征在于，所述第一防盗软件用于封闭所有可以查看私人用户数据的 UI 接口，并且不允许用户主动发起任何操作，只允许专用号码对其进行呼叫或发送信息，并在所述 UI 接口上提示用户所述终端为报失终端。

11. 根据权利要求 7 所述的终端防盗方法，其特征在于，所述第二防盗软件用于使所述终端的内部程序无法正常运行。

12. 根据权利要求 7 所述的终端防盗方法，其特征在于，所述预定方式包括以下至少一种：短消息、以及语音电话。

基于终端管理业务的终端防盗方法

技术领域

本发明涉及通信领域，更具体地，涉及一种用于基于终端管理（OMA Device Management，简称DM）业务进行终端防盗的终端防盗方法。

背景技术

DM业务是管理用户终端的新业务，开放移动联盟（OMA）组织已经对该业务制定了标准规范。该业务使得运营商实现了通过无线方式对移动终端进行远程管理的能力。

DM目前比较成熟的功能可以归纳如下：

（1）参数采集；

（2）参数配置；以及

（3）固件升级（FOTA）。

如果终端出现软件故障或参数配置问题，则用户无须前往维修中心进行诊断和软件更新，而是通过DM平台提供的服务进行远程终端诊断，通过无线方式下载终端软件补丁或执行自动远程设置即可解决终端软件故障和参数配置问题。使用终端管理业务平台，终端业务参数设置和终端软件版本的下载升级也可通过DM平台的用

户自服务门户，由用户自行完成相关参数设置和软件升级，极大的方便了用户对终端的使用。

而随着 3G 网络的运营，数据传输速度的大幅提高，一些新的应用也已经开始被规划，例如:

（1）增值型固件更新/软件升级;

（2）UI 更新；以及

（3）网络优化支持。

对于运营商来讲，可以利用该业务完成未来新业务的部署工作，可以通过在原有终端上推送新版本来完成软件的升级，避免了过去为了支持新业务给运营商和用户带来的各种不便，从而可以更方便的迅速推广新业务。使用 DM 平台，运营商还可以对终端的界面进行更新，辅助用户实现个性化终端设置。这将有助于树立运营商的品牌形象，提升用户满意度。DM 平台的业务分析统计功能，通过分析终端厂商上传的终端能力信息和无线方式收集的终端其他信息，可用于运营商的业务分析和经营决策。

移动用户可以通过多种方式使用终端管理服务。网络可对终端进行批量参数设置、参数收集、软件除错、和功能升级；用户通过登录用户自服务网站，通过 DM 平台触发终端管理业务；移动用户通过 DM 无线应用协议（Wireless Application Protocol，简称 WAP）入口，触发终端管理业务；以及通过终端侧发起 DM 服务。

目前的终端防盗技术虽然很多，但其可靠性及可实施性都存在着很多不足。尤其是通过系统的端到端的解决方案，大多仅仅是对国际移动设备识别码（International Mobile Equipment Identification

Number，简称 IMEI）的控制，并且需要针对终端防盗建立专用的数据库。尤其是对终端上的私人数据的保护，都需要终端做特殊的配合，通用性比较差。所以目前多种终端的防盗方案并没有得到真正的应用。

因此，需要一种用于基于终端管理业务进行终端防盗的终端防盗方法，以解决上述问题。

发明内容

为了解决上述问题，本发明提供了一种用于基于终端管理业务进行终端防盗的终端防盗方法，利用现有的 OMA DM 业务，实现对被盗终端的私人数据内容保护，对被盗终端的限制操作等功能。并且如果被盗终端成功被追回并且返还失主后，可以恢复所有私人数据和使用功能。

为了实现上述目的，本发明提供了一种用于基于终端管理业务进行终端防盗的终端防盗方法，该方法包括以下步骤：步骤 S202，进行终端注册，以将终端的基本信息上报到终端管理平台；步骤 S204，当对终端进行报失时，向实时同步到无线承载网络的报失终端数据库添加记录；以及步骤 S206，查询终端的状态，并根据查询到的状态进行不同处理。

根据本发明的一个方面，步骤 S206 包括以下步骤：步骤 A，查询终端的 SIM/USIM 卡的状态，如果 SIM/USIM 卡处于开机状态，则判断 SIM/USIM 卡是否与终端配合使用，并根据判断结果进行不同处理；步骤 B，如果 SIM/USIM 卡没有处于开机状态，则查询终端管理数据库中是否有关于终端的 IMEI/IMSI 的变更记录，并根据查询结果进行相应处理；以及步骤 C，如果步骤 A 和步骤 B 失败，则终端管理服务器实时监测，当监测到终端时，进行相应处理。

另外，根据本发明的一个方面，在步骤 A 中，如果判断结果为是，则通知终端业务服务器触发第一防盗软件，如果判断结果为否，则通知使用 SIM/USIM 卡的终端，SIM/USIM 卡为报失卡，并禁止 SIM/USIM 卡的业务。

根据本发明的一个方面，在步骤 B 中，如果终端管理数据库中有变更记录，则查询新的 SIM/USIM 卡的状态，如果终端处于开机状态，则终端管理服务器触发第一防盗软件。

根据本发明的一个方面，在步骤 C 中，当检测到终端时，还包括以下步骤：判断终端是否使用 SIM/USIM 卡开机，当判断结果为是时，由无线承载网络通知终端管理服务器触发第一防盗软件；以及当判断结果为否时，在终端更换新 SIM/USIM 卡第一次开机时，终端管理服务器根据终端的注册信息监测到终端，并通过查询注册的 IMEI/IMSI 对应关系，对终端应用第一防盗软件。

根据本发明一个方面的终端防盗方法还包括以下步骤：如果终端管理服务器对终端应用第一防盗软件失败，则在终端每次开机注册时，无线网络都通知终端管理服务器终端为报失终端，终端管理服务器将重新对终端应用第一防盗软件。

此外，终端防盗方法还包括以下步骤：步骤 S208，以预定方式通知终端的使用用户，终端为报失终端，并在指定时间内返回营业厅进行相应处理；步骤 S210，如果在指定时间内返回营业厅，则利用 FOTA 功能对终端进行版本恢复；以及步骤 S212，如果在指定时间内没有返回营业厅，则在检测到终端处于开机状态时，则对所示终端应用第二防盗软件。

在步骤 S208 中，还包括以下步骤：永久删除用户数据，在步骤 S212 中，还包括以下步骤：永久删除用户数据。

第一防盗软件用于封闭所有可以查看私人用户数据的UI接口，并且不允许用户主动发起任何操作，只允许专用号码对其进行呼叫或发送信息，并在 UI 接口上提示用户终端为报失终端；第二防盗软件用于使终端的内部程序无法正常运行。

根据本发明的一个方面，预定方式包括以下至少一种：短消息、以及语音电话。

基于 DM 的终端防盗方案，不需要运营商增加额外的服务器等设施，只需要在 DM 服务器上做很小的修改，就可以兼容终端防盗功能。而且不需要终端做额外的配合，只要支持 DM 功能即可。

因此，本发明实现了以下技术效果：利用 DM 业务固件更新等特性，向运营商提供了一种可靠、稳定、低成本的终端防盗系统。对于用户来讲，则可以最大限度的保护私人数据，并且也极大地增加了用户重新获得丢失终端的可能性。最后在无法获得被盗终端的情况下，可以将被盗终端报废，从而从源头杜绝终端被盗。

本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

附图用来提供对本发明的进一步理解，并且构成说明书的一部分，与本发明的实施例一起用于解释本发明，并不构成对本发明的限制。在附图中：

图 1 是 DM 业务的结构框图；

图 2 是根据本发明的用于基于终端管理业务进行终端防盗的终端防盗方法的流程图;

图 3 是终端向 DM 系统自注册流程图;

图 4 是 DM 防盗至用户报失的流程图;

图 5 是查询被盗终端状态的过程的流程图; 以及

图 6 是 DM 防盗至终端开机的流程图。

具体实施方式

以下结合附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明。

在本实施例中，基于 DM 的终端防盗系统需要结合终端的锁网锁卡功能共同使用，在未来的 3G 运营中，运营商对终端进行定制已经是一个大的趋势，而锁网锁卡是定制终端的必选功能。也就是说运营商定制的终端只能使用该运营商提供的卡和网络。这样就有效的保证了被盗终端不能到其它网络使用，从而必须接收 DM 的防盗管理。

图 1 是 DM 业务的结构框图。如图 1 所示，基于 DM 业务的终端防盗系统的装置包括以下组成部分:

无线承载网络 **102**: 在本实施例中，对于无线网络并没有具体要求，只要承载的速率可以支持 DM 的业务要求即可。无线网络可以是 2G/2.5G 网络，也可以是 3G 网络。网络制式可以包括 GSM，WCDMA，TDSCDMA，CDMA 等;

移动终端 **104**，要求终端本身支持 DM 功能；

DM 业务操作平台 **106**，是运营商操作人员的操作窗口，可以利用该平台发起 DM 的相关业务；以及

DM 业务平台 **108**，具备各种终端的数据，如终端对应的静态数据表、反映 DM 树结构的 DDF 文件、固件升级包、升级包描述文件和升级包策略文件等。

此外，对于 DM 业务本身还需要 WAP 网关 **110** 和 SMS 网关 **112** 等，主要用于接收 DM 相关操作的状态信息。

从硬件的角度讲，基于 DM 的终端防盗系统不需要增加任何硬件配置，而需要增加的软件模块包括：在 DM 业务操作平台 **106** 需要增加操作员对于被盗终端的处理窗口；以及在 DM 业务平台 **108** 需要增加终端防盗软件版本。

终端防盗软件版本需要两个版本，防盗版本 1 的主要功能是封闭所有可以查看私人用户数据的 UI 接口，并且不允许用户主动发起任何操作，只有局方（或者警方）专用号码可以对其进行呼叫，并且在 UI 上提示用户该终端为遗失终端，请马上同运营商联系。防盗版本 2 的主要功能则是彻底破坏终端软件，导致机器无法运行。

以下将结合图 3-5 详细描述图 2 中本实施例的终端防盗方法，其中，图 2 是根据本发明的用于基于终端管理业务进行终端防盗的终端防盗方法的流程图，如图 2 所示的终端防盗方法的流程图示出了完成本发明的需要进行的基本步骤：

步骤 S202，进行终端注册，以将终端的基本信息上报到终端管理平台；

步骤 S204，当对终端进行报失时，向实时同步到无线承载网络的报失终端数据库添加记录；以及

步骤 S206，查询终端的状态，并根据查询到的状态进行不同处理。

图 3 是终端向 DM 系统自注册流程图，如图 2 所示的上述步骤 S202 终端注册的具体过程如图 3 所示。

如图 3 所示，对于防盗方案来说最主要的是 IMEI 和国际移动客户识别码（International Mobile Subscriber Identification Number，简称 IMSI）的对应关系。在本实施例中，终端的注册可以通过短消息实现，注册的主要内容包括：终端 IMEI，厂商名称，终端型号，软件版本。

为了保证终端软件的统一性，注册功能可以集成在 SIM/USIM 上，开机后有卡内相关应用自动完成注册功能。当然也可以由终端本身完成注册功能。

符合 DM 平台规范要求的终端，第一次开机时，终端必须将终端的 IMEI 及其他 DM 平台需要的基础信息以短信的方式发送到 DM 平台。平台侧负责解析该消息，并在平台侧建立终端 IMEI 和终端号码的对应关系列表。如果用户更换 SIM/USIM 卡，开机时终端应将新的对应关系上传到 DM 终端管理平台。对于因为更换 SIM/USIM 卡而引发的终端注册，考虑到终端防盗的需要，对于原来的 SIM/USIM 卡同 IMEI 的对应关系，需要保留一段时间（如 6 个月）。

如果终端收到来自 DM 平台特服号码的注册成功确认短信，则终端记录此次注册成功的 SIM/USIM 卡的 IMSI 信息到终端某个预

先确定的位置（如果使用卡内应用，则是读取终端的 IMEI，并且将此数据保存在卡内），以便终端可以在下次开机的时候检测此IMSI（IMEI）。此后，每次终端重新启动，都应检测 SIM 卡的 IMSI 与保存的 IMSI 是否一致，如果不一致，则终端应重新向平台侧发送自注册信息并且更新 IMEI/IMSI 配对信息。

上面注册流程除了有助于 DM 服务器了解用户的终端使用信息，从而加快终端固件升级（FOTA）的速度外，对于终端防盗也有着重大的意义。当被盗终端换了该运营商的其它 SIM/USIM 时，DM服务器可以在第一时间掌握终端的动态，并且利用 DM 的 FOTA 功能，向终端发起防盗版本 1 的升级，封闭该终端所有可以查看私人用户数据的 UI 接口，并且不允许用户主动发起任何操作。

图 4 是 DM 防盗至用户报失的流程图，以下将继续参照图 4 详细描述如图 2 所示的用户报失过程 S204 的具体步骤。如图 4 所示，其具体步骤包括:

步骤 1，用户报失，需要提供能够证明用户身份的相关措施。例如，用户可以凭借身份证到营业厅报失，也可以电话报失，但是需要提供用户密码或者回答相关问题。在确认用户身份后，将被盗终端的信息输入被盗数据库中保存;

步骤 2，查询被盗终端的 SIM/USIM 卡状态，如果被盗终端的 SIM/USIM 卡处于开机状态，则进行步骤 3，如果被盗终端的 SIM/USIM 卡处于关机状态，则进行步骤 6;

步骤 3，查询 DM 服务器中记录的 IMEI/IMSI 记录，判断处于开机状态的被盗 SIM/USIM 卡是否正在与被盗终端配合使用，如果被盗 SIM/USIM 是同被盗终端配合使用，则进行步骤 4，如果被盗 SIM/USIM 卡更换其它终端使用，则进行步骤 5;

步骤4，通过DM平台完成防盗版本1的升级，升级后用户将不能访问被盗终端的所有私人数据，不能发起任何主动操作。为了避免防盗版本1升级失败，在网络侧同时禁止该被盗SIM/USIM卡的所有业务，只允许局方（或者警方）专用号码可以对其进行呼叫或者发送消息。而运营商通过网络发送消息，或者向用户发起呼叫，通知用户该终端为被盗终端，请在N天内上交给营业厅；

步骤5，如果被盗SIM/USIM更换的终端为非被盗终端（注意因为有终端开机流程的保证，所以此种情况不会有被盗卡配合其它被盗终端的情况出现），则通知用户该SIM/USIM卡为被盗卡，停止该被盗SIM/USIM卡的所有业务；以及

步骤6，如果被盗SIM/USIM卡处于关机状态，则查询DM服务器侧是否有近期的关于被盗终端的IMEI/IMSI的变更记录（由终端的DM自注册信息上报）。

需要指出的是，如果没有变更记录说明被盗终端没有更换其它SIM/USIM卡进行操作，则用户报失流程结束。将会在用户开机流程中处理后续事务；如果有近期的变更记录，则说明被盗终端可能更换SIM/USIM卡正在使用，通过DM服务器查询到最新的IMEI/IMSI对应关系，并且更新到被盗数据库中，则进行步骤4。

综上所述，用户在发现终端丢失后，首先向运营商的服务部门进行口头挂失，运营商可以根据预留的用户密码对用户身份进行鉴别。如果没有密码或者密码不对，则失主必须携带有效证件到营业厅进行挂失。

运营商接受挂失后，则通过DM业务操作平台向被盗终端数据库添加记录，该数据库需要实时同步到无线承载侧。防止被盗终端使用原来的SIM/USIM卡进行操作。

图 5 是查询被盗终端状态的过程的流程图，如图 5 所示，包括以下步骤:

步骤 A，当被盗终端数据被同步到无线承载网络侧后，则首先查询被盗 SIM/USIM 卡的状态。如果被盗的 SIM/USIM 处于开机状态，这里面又可以分为两种情况。

一种情况是被盗终端仍然同被盗 SIM/USIM 卡配合使用，对于此种情况则立刻通知 DM 服务器触发防盗版本 1 的升级。

另外一种情况是被盗 SIM/USIM 卡同其它终端配合使用，对于此种情况网络侧发送短消息通知终端，此 SIM/USIM 卡为被盗卡，并且由网络侧禁止该 SIM/USIM 的所有业务。

步骤 B，如果经过查询原来的 SIM/USIM 卡并没有处于开机状态，则查询 DM 服务器中的被盗终端的 IMEI，是否有同新的 SIM/USIM 卡的变更记录。如果有，则查询新的 SIM/USIM 卡的状态，如果处于开机状态，DM 服务器立刻对该终端发起防盗版本 1 的升级。

步骤 C，如果上面两种方式都没有发现被盗终端，则说明被盗终端还没有在运营商的网络中使用。DM 服务器将实时监控被盗终端，如果一旦监测到被盗终端开机，则 DM 服务器立刻触发对该被盗终端的防盗版本 1 的升级。

当被盗终端使用原 SIM/USIM 卡开机时，由无线承载网络即时通知 DM 服务器，发起防盗版本 1 的升级。如果被盗终端更换 SIM/USIM 卡第一次开机时，DM 服务器根据终端注册消息(IMEI)，将会监测出被盗终端，通过查询注册的最新 IMEI/IMSI 对应关系，DM 服务器可以即时对该终端发起防盗版本 1 的升级，假设此次防

盗版本 1 更新失败，在以后每次开机注册时，无线网络都将通知 DM 服务器该终端为被盗终端，DM 服务器将重新对其发起防盗版本 1 的更新。

图 6 是 DM 防盗至终端开机的流程图，以下将参照图 6 描述如图 5 所示的终端开机的具体步骤。如图 6 所示，终端开机包括以下步骤：

步骤 1，网络侧接收到终端的注册消息，并且从中提取出 IMEI 和 IMSI 信息；

步骤 2，在被盗终端数据库中查询该终端的 IMEI，确定该终端是否是被盗终端。如果是被盗终端则通知 DM 服务器，并且将对应的 IMEI/IMSI 参数传递给 DM 服务器，进行步骤 3，如果不是被盗终端，则结束流程；

步骤 3，查询该被盗终端是否已经进行过防盗版本 1 的升级，如果已经进行过防盗版本 1 的升级，则进行步骤 4，如果还没有进行防盗版本 1 的升级，则发起防盗版本 1 的升级，并且通知用户该终端为被盗终端，请在 N 天内上交给营业厅，其中，防盗版本 1 升级的主要功能是：封闭所有可以查看私人用户数据的 UI 接口，并且不允许用户主动发起任何操作，只有局方（或者警方）专用号码可以对其进行呼叫或者发送消息，并且在 UI 上提示用户该终端为遗失终端，请马上同运营商联系；以及

步骤 4，判断已经进行过防盗版本 1 升级的被盗终端，是否已经超过规定的返还给营业厅的规定期限。

如果还没有超过期限，则通过消息或者语音再次提醒用户该终端为被盗终端，请尽快返还营业厅，N 天之内被盗终端返还营业厅

后，运营商将通知失主到营业厅领取终端，因此可以保证用户仍然使用原号码。此时终端仍然是防盗版本1，不能进行任何主动操作。通过DM用户操作平台，利用FOTA功能发起对该终端的版本恢复。版本恢复成功后，用户可以正常使用，并且所有私人数据依然保留。

如果已经超过规定的返还期限，被盗终端仍然没有返还营业厅，则基本可以认为被盗终端无返回希望。如果一旦检测到终端处于激活状态，则采取如下措施:

（1）永久性删除用户数据，终端本身一般都是支持对内存的完全格式化的，所以可以利用短消息，或者对DM参数配置等功能的扩展，通知终端永久性的擦除终端内的所有用户数据。

（2）防盗版本2升级，利用DM的FOTA功能，对被盗终端进行防盗版本2的升级。终端在完成防盗版本2的升级后，则终端内部程序将无法正常运行，对网络也不会有任何的影响，该终端基本作废。

此外，如果在对终端升级到防盗版本1后，在规定的时间内，被盗终端被返回到营业厅，则可以利用DM重新恢复终端版本，失主可以领回终端重新使用。

以上仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

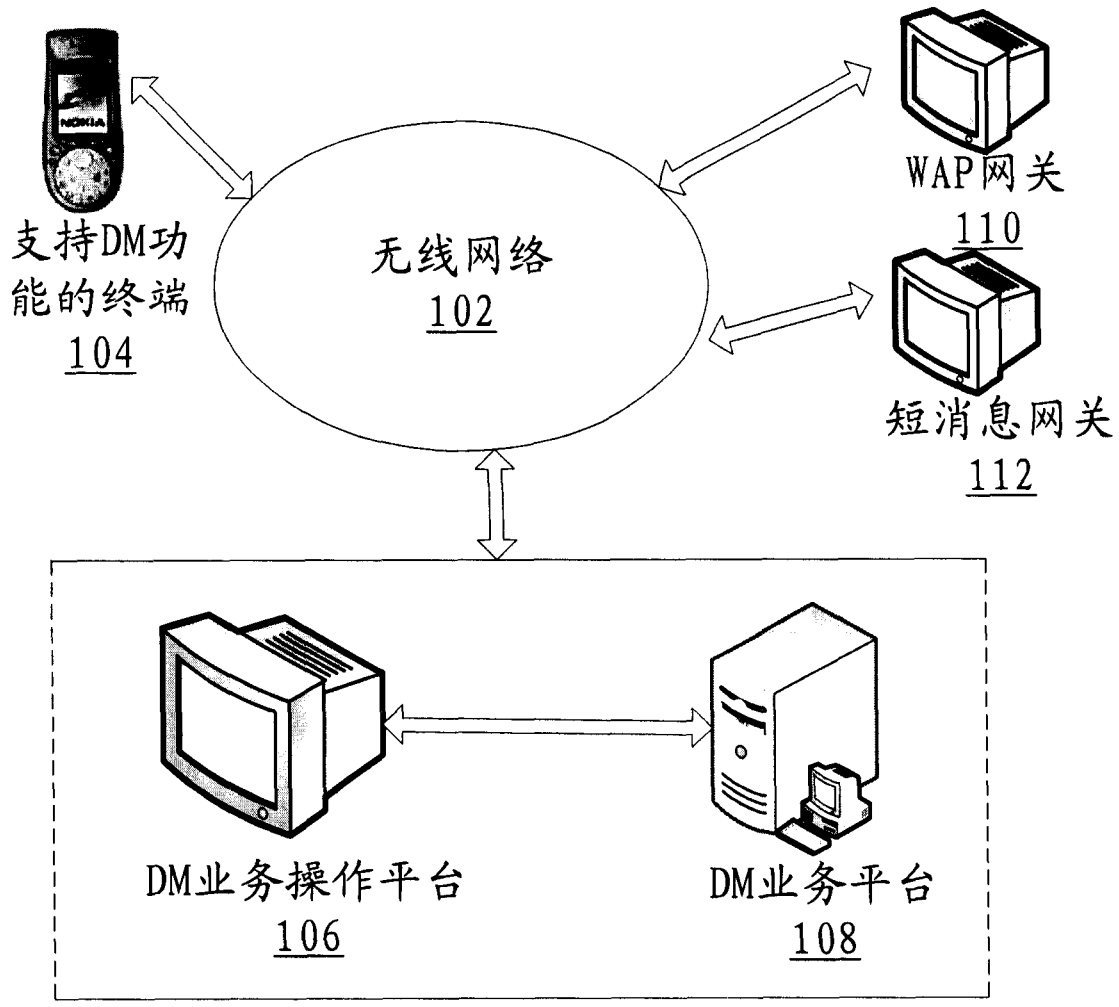

支持DM功能的终端
104
无线网络
102
WAP网关
110
短消息网关
112
DM业务操作平台
106
DM业务平台
108

图 1

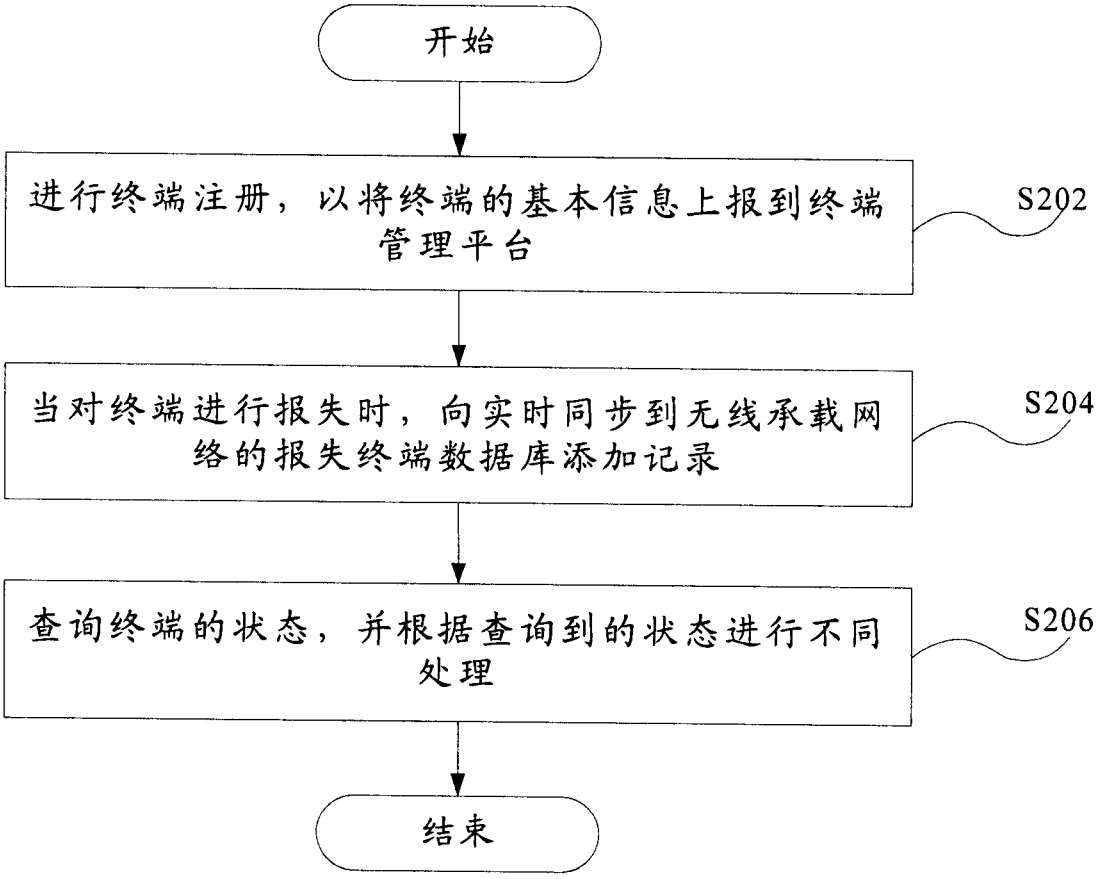

开始
进行终端注册，以将终端的基本信息上报到终端管理平台
S202
当对终端进行报失时，向实时同步到无线承载网络的报失终端数据库添加记录
S204
查询终端的状态，并根据查询到的状态进行不同处理
S206
结束

图 2

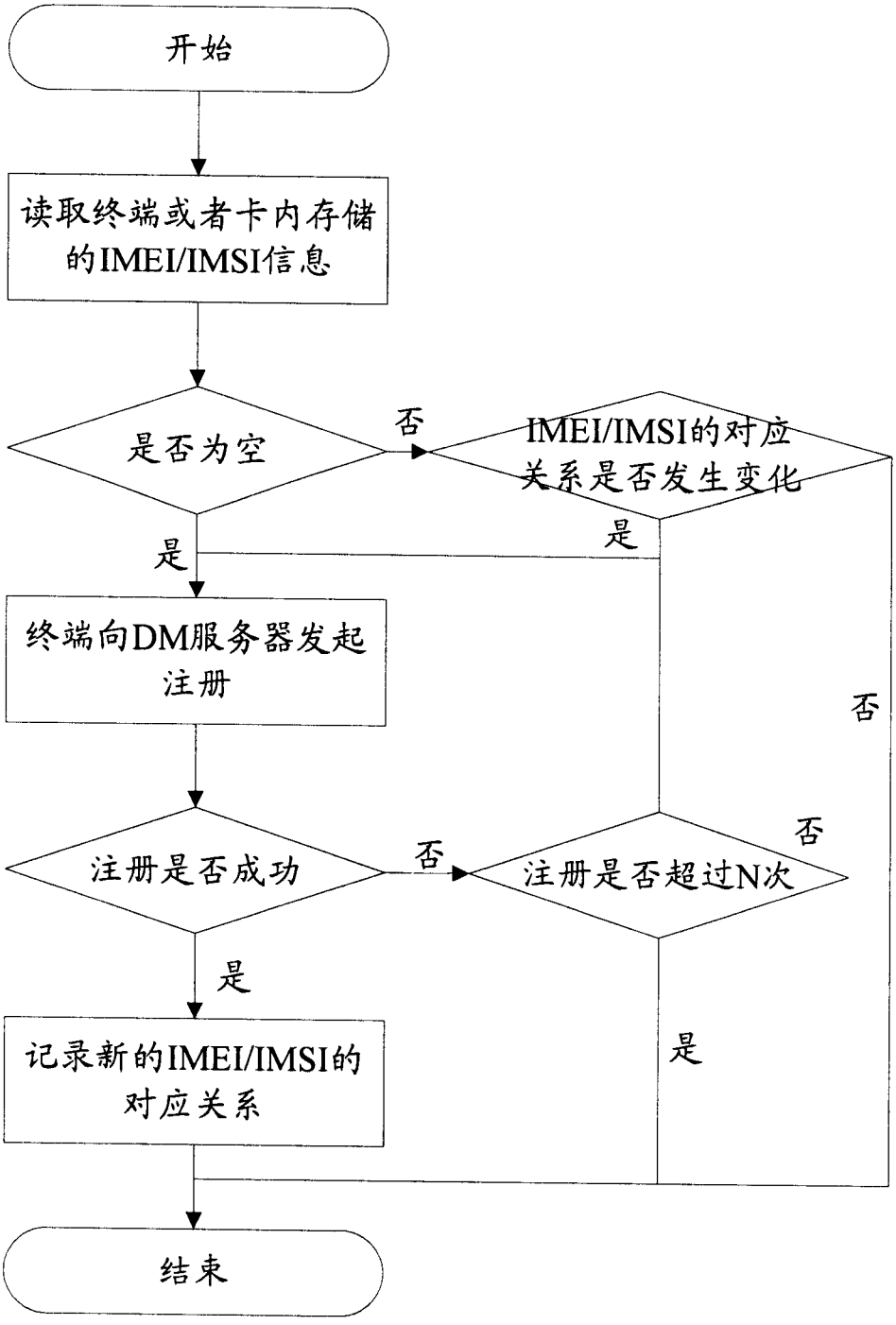

开始
读取终端或者卡内存储的IMEI/IMSI信息
是否为空
否
IMEI/IMSI的对应关系是否发生变化
是
是
否
终端向DM服务器发起注册
注册是否成功
否
注册是否超过N次
否
是
是
记录新的IMEI/IMSI的对应关系
结束

图 3

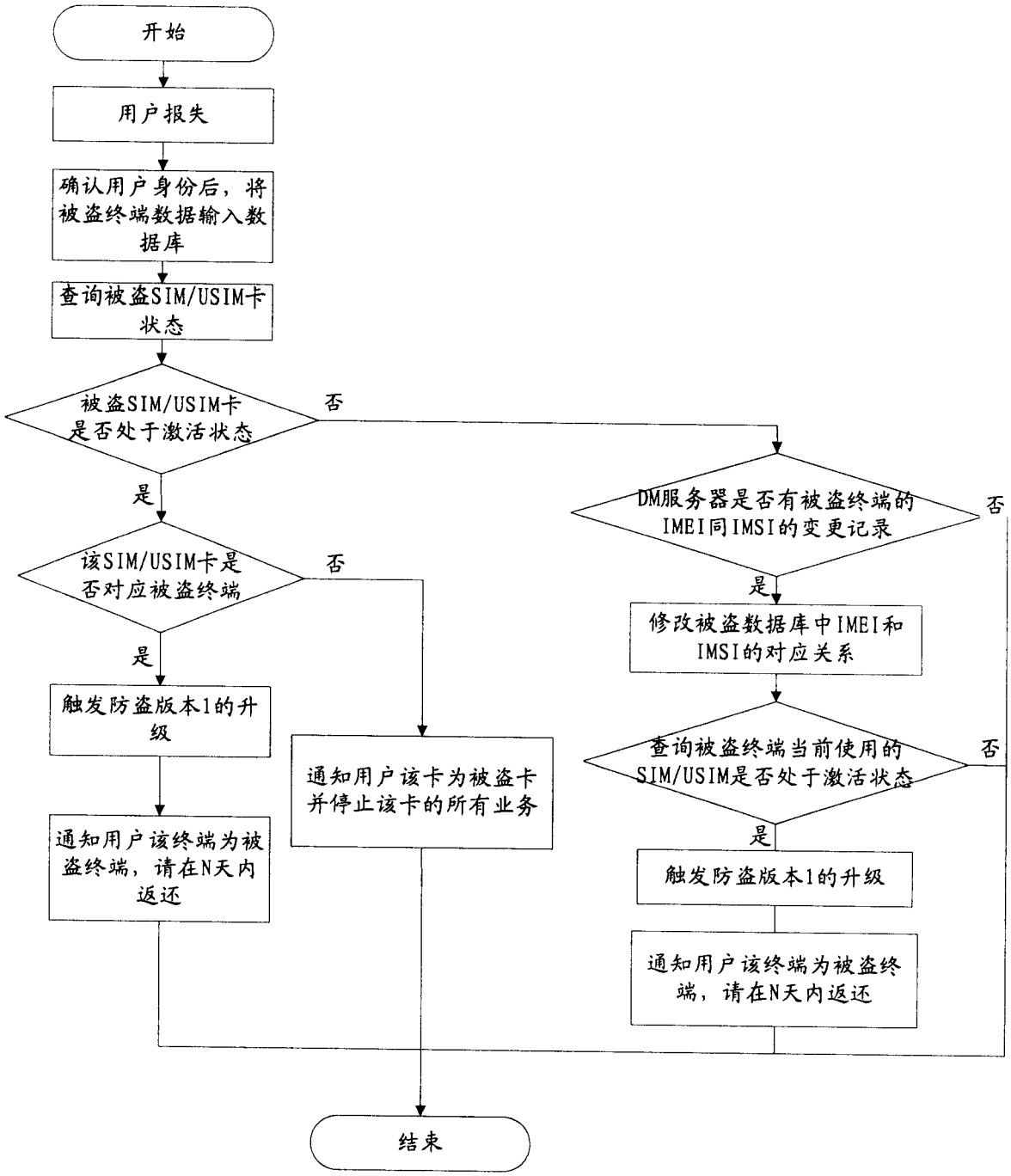

开始
用户报失
确认用户身份后，将被盗终端数据输入数据库
查询被盗SIM/USIM卡状态
被盗SIM/USIM卡是否处于激活状态
否
是
该SIM/USIM卡是否对应被盗终端
否
是
触发防盗版本1的升级
通知用户该终端为被盗终端，请在N天内返还
通知用户该卡为被盗卡并停止该卡的所有业务
DM服务器是否有被盗终端的IMEI同IMSI的变更记录
否
是
修改被盗数据库中IMEI和IMSI的对应关系
查询被盗终端当前使用的SIM/USIM是否处于激活状态
否
是
触发防盗版本1的升级
通知用户该终端为被盗终端，请在N天内返还
结束

图 4

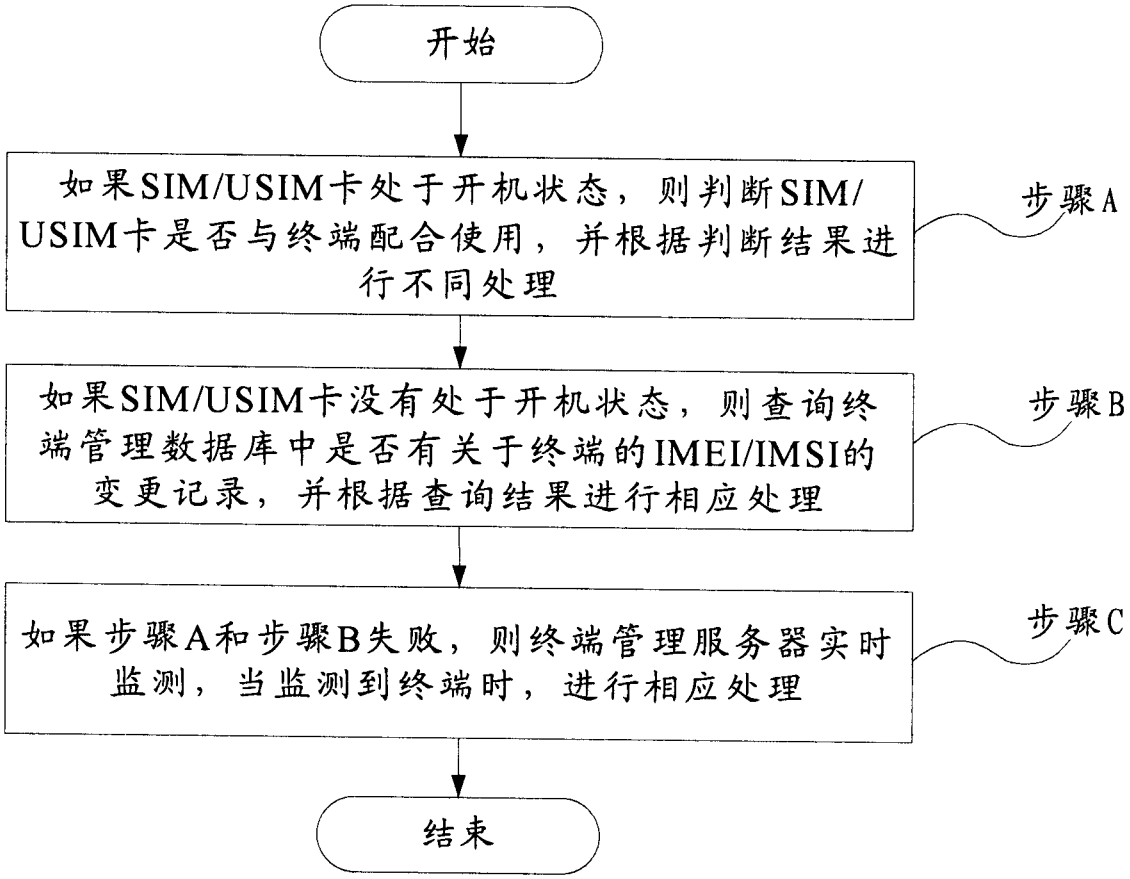

开始
如果SIM/USIM卡处于开机状态，则判断SIM/USIM卡是否与终端配合使用，并根据判断结果进行不同处理
步骤A
如果SIM/USIM卡没有处于开机状态，则查询终端管理数据库中是否有关于终端的IMEI/IMSI的变更记录，并根据查询结果进行相应处理
步骤B
如果步骤A和步骤B失败，则终端管理服务器实时监测，当监测到终端时，进行相应处理
步骤C
结束

图 5

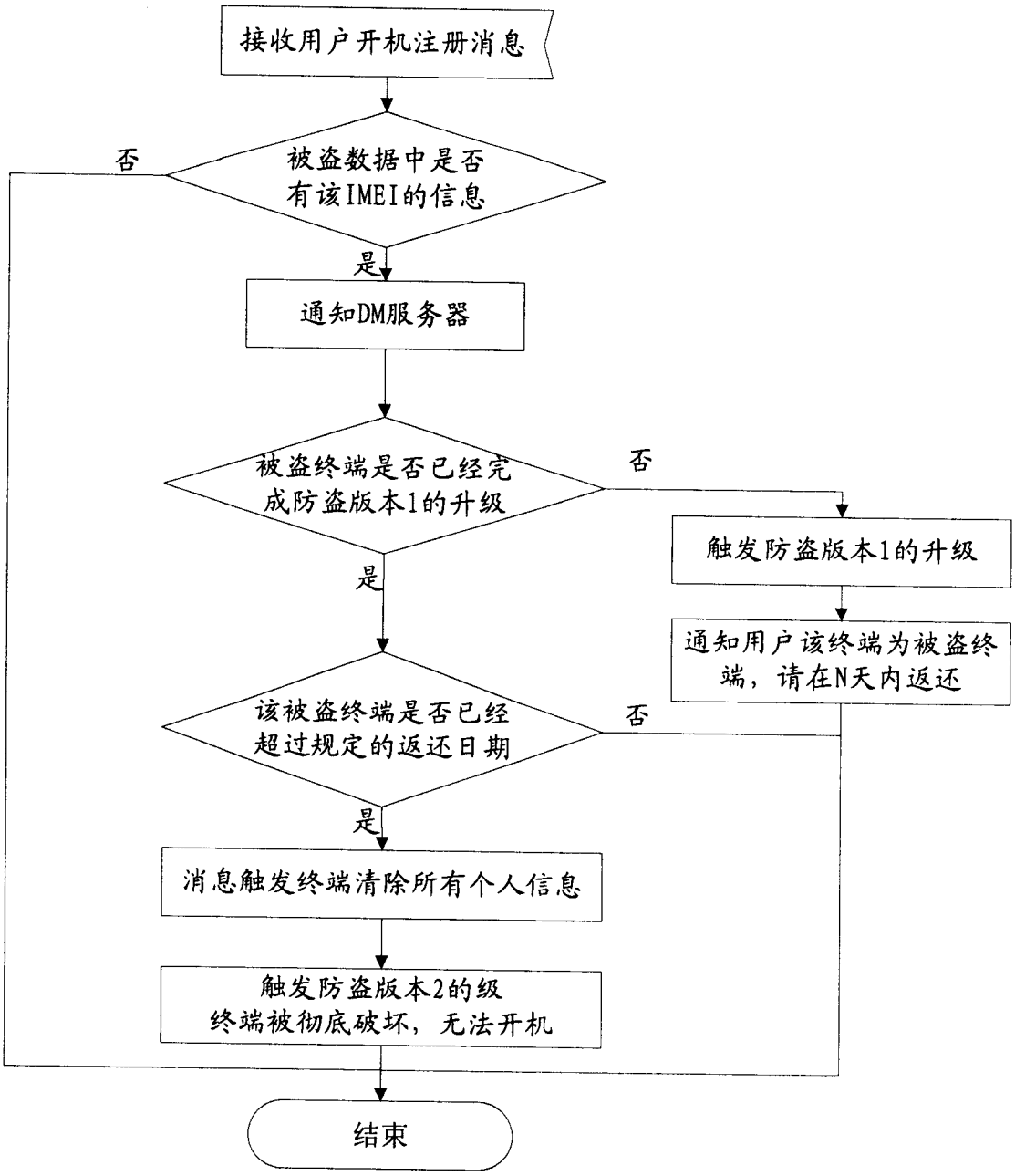

接收用户开机注册消息
被盗数据中是否有该IMEI的信息
否
是
通知DM服务器
被盗终端是否已经完成防盗版本1的升级
否
触发防盗版本1的升级
是
通知用户该终端为被盗终端，请在N天内返还
该被盗终端是否已经超过规定的返还日期
否
是
消息触发终端清除所有个人信息
触发防盗版本2的级
终端被彻底破坏，无法开机
结束

图 6