[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04W 8/18 (2006.01)
H04W 12/02 (2009.01)
H04W 88/02 (2009.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200780021319.0

[43] 公开日 2009 年 8 月 5 日

[11] 公开号 CN 101502146A

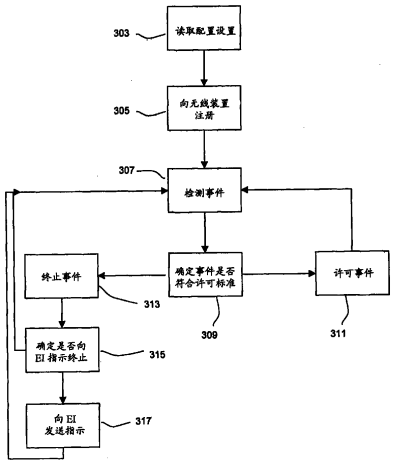
[22] 申请日 2007.6.8
[21] 申请号 200780021319.0
[30] 优先权
[32] 2006. 6. 8 [33] US [31] 60/804,221
[86] 国际申请 PCT/IB2007/001105 2007.6.8
[87] 国际公布 WO2007/141607 英 2007.12.13
[85] 进入国家阶段日期 2008.12.8
[71] 申请人 夏兰·布莱德里
地址 爱尔兰都柏林
[72] 发明人 夏兰·布莱德里
[74] 专利代理机构 北京康信知识产权代理有限责任公司
代理人 余 刚 尚志峰
权利要求书 7 页 说明书 17 页 附图 6 页

[54] 发明名称

基于 SIM 的防火墙的方法和设备

[57] 摘要

一种使用基于 SIM 的防火墙来对无线装置或 SIM 中可能发生的事件进行过滤和管理的方法，该方法可以包括：读取配置设置；向无线装置注册，并且启动计时器；检测事件；确定该事件是否符合许可标准；并且，如果事件符合，则许可该事件。如果不许可该事件，则该方法还包括：终止该事件；确定是否指示外部界面；并且潜在地向外部界面发送指示。 这些指示也可以被发送到检测该事件和/或阻止该事件的远程系统。



1. 一种用于操作移动装置中的基于 SIM 的防火墙的方法，所述方法包括:

（a）由 SIM 接收发生的、与包括所述 SIM 的移动装置有关的事件的指示;

（b）由所述 SIM 确定所述事件满足至少一个条件；以及

（c）由所述 SIM 阻止所述事件。

2. 根据权利要求 1 所述的方法，其中，所述事件包括出话呼叫。

3. 根据权利要求 1 所述的方法，其中，所述事件包括来话呼叫。

4. 根据权利要求 1 所述的方法，其中，所述事件包括输入文本消息。

5. 根据权利要求 1 所述的方法，其中，所述事件包括输出文本消息。

6. 根据权利要求 1 所述的方法，其中，所述事件包括 MMS 消息、SMS 消息、或 USSD 消息中的一个。

7. 根据权利要求 1 所述的方法，其中，所述事件包括视频呼叫、一键呼叫、VOIP 呼叫、电子邮件、小区广播、即时通讯消息、GPRS、蓝牙、网络通信、或数据连接起动中的至少一个。

8. 根据权利要求 1 所述的方法，其中，所述至少一个条件包括所述事件的源的电话号码。

9. 根据权利要求 1 所述的方法，其中，所述至少一个条件包括所述事件的源的电话号码的一部分。

10. 根据权利要求 1 所述的方法，其中，所述至少一个条件包括所述事件的源的地理区域。

11. 根据权利要求 1 所述的方法，其中，所述至少一个条件包括所述事件发生的时间。

12. 根据权利要求 1 所述的方法，其中，所述至少一个条件包括所述事件发生的日期。

13. 根据权利要求 1 所述的方法，其中，所述至少一个条件包括在给定时间周期期间通过所述移动装置预先处理的呼叫的总量。

14. 根据权利要求 1 所述的方法，其中，所述至少一个条件包括在给定时间周期期间通过所述移动装置预先处理的文本消息的总量。

15. 根据权利要求 1 所述的方法，其中，所述至少一个条件包括在给定时间周期期间通过所述移动装置预先处理的 MMS 的总量。

16. 根据权利要求 1 所述的方法，其中，所述至少一个条件包括在给定时间周期期间通过所述移动装置预先处理的数据的总量。

17. 根据权利要求 1 所述的方法，其中，所述至少一个条件包括在给定时间周期期间通过所述移动装置预先处理的事件的总量。

18. 根据权利要求 1 所述的方法，其中，所述至少一个条件包括所述事件的源地址的属性。

19. 根据权利要求 18 所述的方法，其中，所述源地址是 IP 地址、URL、SS 服务代码、或 USSD 服务代码中的一个。

20. 根据权利要求 1 所述的方法，其中，步骤（c）包括由所述 SIM 阻止通过所述移动装置的用户界面来指示事件。

21. 根据权利要求 1 所述的方法，其中，步骤（c）包括由所述 SIM 阻止所述移动装置发送涉及所述事件的信息。

22. 根据权利要求 1 所述的方法，还包括由所述 SIM 注册以接收预定的事件组的指示。

23. 根据权利要求 1 所述的方法，还包括由所述移动装置从远程源接收所述至少一个条件。

24. 根据权利要求 23 所述的方法，还包括：通过网站来接收用于阻止的所述至少一个条件；以及向所述移动装置发送所述至少一个条件。

25. 根据权利要求 1 所述的方法，还包括：通过语音识别或自动电话应答系统中的一个来接收用于阻止的所述至少一个条件；以及向所述移动装置发送所述至少一个条件。

26. 根据权利要求 1 所述的方法，还包括：通过交互式 TV、或互联网协议 TV（IPTV）中的一个来接收用于阻止的所述至少一个条件；以及向所述移动装置发送所述至少一个条件。

27. 根据权利要求 1 所述的方法，还包括：通过移动互联网网站来接收用于阻止的所述至少一个条件；以及向所述移动装置发送所述至少一个条件。

28. 根据权利要求 1 所述的方法，还包括：通过第二移动装置来接收用于阻止的所述至少一个条件；以及向所述移动装置发送所述至少一个条件。

29. 根据权利要求 1 所述的方法，还包括以下步骤：向远程系统发送检测到所述事件的指示。

30. 根据权利要求 29 所述的方法，还包括向所述远程系统发送所述事件被阻止的指示。

31. 一种在移动装置中用作防火墙的 SIM，所述 SIM 包括：

接收装置，用于由 SIM 接收发生的、与包括所述 SIM 的移动装置有关的事件的指示；

确定装置，用于由所述 SIM 确定所述事件满足至少一个条件；以及

阻止装置，用于由所述 SIM 阻止所述事件。

32. 根据权利要求 31 所述的方法，其中，所述事件包括出话呼叫。

33. 根据权利要求 31 所述的方法，其中，所述事件包括来话呼叫。

34. 根据权利要求 31 所述的方法，其中，所述事件包括输入文本消息。

35. 根据权利要求 31 所述的方法，其中，所述事件包括输出文本消息。

36. 根据权利要求 31 所述的方法，其中，所述事件包括 MMS 消息、SMS 消息、或 USSD 消息中的一个。

37. 根据权利要求 31 所述的方法，其中，所述事件包括视频呼叫、一键呼叫、VOIP 呼叫、电子邮件、小区广播、即时通讯消息、GPRS、蓝牙、网络通信、或数据连接起动中的至少一个。

38. 根据权利要求 31 所述的方法，其中，所述至少一个条件包括所述事件的源的电话号码。

39. 根据权利要求 31 所述的方法，其中，所述至少一个条件包括所述事件的源的电话号码的一部分。

40. 根据权利要求 31 所述的方法，其中，所述至少一个条件包括所述事件的源的地理区域。

41. 根据权利要求 31 所述的方法，其中，所述至少一个条件包括所述事件发生的时间。

42. 根据权利要求 31 所述的方法，其中，所述至少一个条件包括所述事件发生的日期。

43. 根据权利要求 31 所述的方法，其中，所述至少一个条件包括在给定时间周期期间通过所述移动装置预先处理呼叫的总量。

44. 根据权利要求 31 所述的方法，其中，所述至少一个条件包括在给定时间周期期间通过所述移动装置预先处理的文本消息的总量。

45. 根据权利要求 31 所述的方法，其中，所述至少一个条件包括在给定时间周期期间通过所述移动装置预先处理的 MMS 的总量。

46. 根据权利要求 31 所述的方法，其中，所述至少一个条件包括在给定时间周期期间通过所述移动装置预先处理的数据的总量。

47. 根据权利要求 31 所述的方法，其中，所述至少一个条件包括在给定时间周期期间通过所述移动装置预先处理的事件的总量。

48. 根据权利要求 31 所述的方法，其中，所述至少一个条件包括所述事件的源地址的属性。

49. 根据权利要求 48 所述的方法，其中，所述源地址是 IP 地址、URL、SS 服务代码、或 USSD 服务代码中的一个。

50. 根据权利要求 31 所述的方法，其中，所述 SIM 包括用于阻止通过所述移动装置的用户界面来指示事件的装置。

51. 根据权利要求 31 所述的方法，其中，所述 SIM 包括用于阻止所述移动装置发送涉及所述事件的信息的装置。

52. 根据权利要求 31 所述的方法，还包括用于由所述 SIM 注册以接收预定的事件组的指示的装置。

53. 根据权利要求 31 所述的方法，还包括用于由所述 SIM 从远程源接收所述至少一个条件的装置。

54. 根据权利要求 31 所述的方法，还包括用于由所述 SIM 从数据中接收所述至少一个条件的装置，通过以下中的至少一个输入所述数据：网站、语音识别或自动电话应答系统、交互式 TV、互联网协议 TV（IPTV）、移动互联网网站、或第二移动装置。

55. 根据权利要求 31 所述的方法，还包括用于向远程系统发送检测所述事件的指示的装置。

56. 根据权利要求 55 所述的方法，还包括用于向所述远程系统发送所述事件被阻止的指示的装置。

57. 一种用于操作移动装置中的基于 SIM 的防火墙的方法，所述方法包括:

（a）由移动装置中的 SIM 检测所述 SIM 的部分内存的修改;

（b）由所述 SIM 接收发生的、与所述移动装置有关的事件的指示；以及

（c）由所述 SIM 至少部分地基于所述修改的检测来阻止所述事件。

58. 根据权利要求 57 所述的方法，其中，步骤（a）包括从所述移动装置的操作系统中接收关于所述 SIM 的部分内存已经修改的指示。

59. 根据权利要求 57 所述的方法，其中，步骤（a）包括从所述 SIM 的操作系统中接收关于所述 SIM 的部分内存已经修改的指示。

60. 根据权利要求 57 所述的方法，其中，步骤（a）包括确定所述部分内存的内容与前一时刻的部分内存的内容不同。

基于 SIM 的防火墙的方法和设备

相关申请

本申请要求于 2006 年 6 月 8 号提交的、题为“METHODS AND APPARATUS FOR A SIM-BASED FIREWALL”的美国临时专利申请序列号 60/804,221 的优先权。

技术领域

本发明涉及采用用户识别模块的无线装置，以及涉及对在这种装置上输入和输出的通信、数据以及事件进行过滤和管理的装置。

背景技术

在很多情况下，都期望具有在无线装置上有效过滤输入和输出的事件的能力。然而，现有技术可以并未涉及对可以由无线电话网络中的现代无线装置发送和接收的多个数据和通信进行细致的控制。

例如，全球移动通信系统（GSM）和通用移动电信系统（UMTS）的固定拨号号码（FDN）服务可以对出话呼叫、承载业务以及远程服务进行限制，但不能对可由现代无线装置接收的多个数据和通信进行控制。GSM 和 UMTS 限制拨号号码（BDN）服务能够阻止向预定电话号码出话呼叫，但不能控制来话呼叫，也不能控制可由现代无线装置发送和接收的多个数据和通信。

使用移动网络增强定制应用逻辑（CAMEL）的智能网（IN）或在无线电话网络中使用的无线智能网（WIN）技术可以提供对可由无线电话网络中的现代无线装置发送和接收的数据及通信进行一定程度地控制，但它们使用起来复杂、昂贵、耗时。

因此，需要一种对可由无线电话网络中的无线装置发送和接收的多个数据、通信以及事件提供高效细致的控制的解决方案。

发明内容

本发明涉及一种对可由网络中的无线装置发送和接收的多个数据、通信及事件提供细致的控制的系统和方法。

一方面，本发明是一种使用基于 SIM 的防火墙来对在无线装置或 SIM 中可能发生的事件进行过滤和管理的方法。简言之，该方法包括：读取配置设置；向无线装置注册，并启动计时器；检测事件；确定事件是否符合许可标准；并且，如果事件符合，则许可该事件。如果不许可该事件，则该方法还可以包括：终止该事件；确定是否指示外部界面；并且潜在地向外部界面发送指示。该方法还可以包括向远程系统发送该事件被检测和/或阻止的指示。

另一方面，本发明是一种用于远程管理基于 SIM 的防火墙的方法。简言之，该方法包括：接收来自网络的远程管理事件。该远程管理事件可以包括以下中的一个或多个：命令基于 SIM 的防火墙停止；命令基于 SIM 的防火墙重新启动；修改基于 SIM 的防火墙的配置设置；保存基于 SIM 的防火墙的经修改的配置设置；修改基于 SIM 的防火墙的可执行文件和可执行库（library）；以及保存基于 SIM 的防火墙的经修改的可执行文件和可执行库。

另一方面，本发明是用于执行上述任意方法的一个或多个数字电子系统。

附图说明

通过参考结合附图的以下描述，本发明的前述和其他目的、方面、特征、以及优点会更加显而易见和易于理解，其中：

图 1A 是示出了连接到网络的、结合有基于 SIM 的防火墙的无线装置的一个实施例的框图；

图 1B 是示出网络的一个实施例的框图；

图 2A 和图 2B 是示出由基于 SIM 的防火墙处理的事件的不同实施例的流程图；

图 3 是示出由基于 SIM 的防火墙执行的用于过滤事件的方法的一个实施例的流程图；以及

图 4 是示出用于远程管理基于 SIM 的防火墙的一个实施例的流程图。

具体实施方式

现在参照图 1A，示出了连接到网络的、结合有基于 SIM 的防火墙的无线装置的一个实施例的框图。简言之，无线装置 **101** 包括：中央处理单元（CPU）**103**、用户识别（Subscriber Identity）模块（SIM）**107**、基于 SIM 的防火墙（**109**）、无线电收发信机（**115**）和外部界面（EI）**111**。该无线装置可以与一个或多个网络 **105** 进行通信，也可以与一个或多个发射机/接收机站 **113** 进行通信。

现在更详细地参照图 1A，其示出了无线装置 **101**。此处，术语“无线装置”指不使用电线、电缆或其他有形传输介质而能够向网络发送语音和/或数据（非语音）信息以及接收来自网络的声音和/或数据（非语音）信息的任意装置。在一个实施例中，无线装置 **101** 可以包括移动电话。在其他实施例中，无线装置可以包括蜂窝电话、智能电话、固定移动融合电话（fixed-mobile convergence phone）、卫星电话、无线数据卡、无线个人数字助理（PDA）、无线调制解调器或计算机、以及无线地进行通信的电子系统。

在所示实施例中，无线装置 **101** 包括 SIM **107**。SIM **107** 可以是包括以下中的一个或多个的智能卡：CPU、密码处理器、只读存储器（ROM）、随机存取存储器（RAM）、电可擦除可编程只读存储器（EEPROM）、以及输入/输出电路。

SIM **107** 可以用于存储关于 SIM **107** 的所有者、允许与 SIM **107** 连接的网络、SIM **107** 可以在网络上获得的服务、以及电话号码的地址簿的唯一定制和认证信息。SIM **107** 可以包括一个或多个增值应用。这些应用可以包括：银行、生物、医学、安全、生产力、身份管理、数字签名、公钥基础结构（PKI）、多媒体、票务、数字权利管理、博弈、忠诚（loyalty）应用。SIM 应用可以采用 SIM 应用工具箱（SAT）技术或其他智能卡应用技术。

在另一个实施例中，无线装置可以包括取代 SIM 的通用集成电路卡（UICC）。UICC 可以包括以下识别模块（IM）技术中的一种或多种：GSM 用户识别模块（SIM）、UMTS 互联网协议多媒体服务识别模块（ISIM）、CDMA 可移动（removable）用户识别模块（R-UIM）、以及增值应用。UICC 应用可以使用以下技术中的一种或多种：USAT（通用 SIM 应用工具箱）、CCAT（CDMA 卡应用工具箱）、CAT（卡应用工具箱）、UATK（UIM 应用工具箱）或其他

智能卡技术。在本文中，SIM **107** 一般地用于表示 SIM 卡和具有 USIM、或其他 IM（存在于 UICC 上的应用）的 UICC。

在示出的实施例中，SIM **107** 可以包括基于 SIM 的防火墙应用程序 **109**，这里称为 SIM 防火墙。SIM 防火墙 **109** 可以包括可编程逻辑，其检测、过滤和管理在网络 **105**、无线装置 **101**、无线装置的 SIM **107** 和外部界面 **111** 之间的任一方向上传递的数据、通信及事件。SIM 防火墙 **109** 可以对照一个或多个可配置标准来评估数据、通信和事件。如果该数据、通信和事件符合特定的标准，则可以拒绝、或允许它们在网络 **105**、无线装置 **101**、无线装置的 SIM **107** 和外部界面 **111** 之间的任一方向上继续传输。

在一个实施例中，作为 SIM **107** 的制造过程的一部分，使用含 SMS 或蜂窝广播（CB）消息的无线电（Over The Air）（OTA）管理、使用承载独立协议（BIP）、使用 Java 远程方法调用（RMI）、使用支持 J2ME 安全和信任服务（SATSA）说明书的 Java2 微型版（J2ME）midlet、使用无线装置的操作系统、使用无线装置上的应用程序、使用信用卡适用器（CAD）或其他物理地连接到 SIM 的智能读卡器、使用能够通过短距离射频技术与 SIM 进行通信的无接触智能卡技术，可以将 SIM 防火墙 **109** 传输并安装到 SIM **107** 上。

在所示实施例中，可以使用以下中的一个或多个来在网络上远程管理 SIM 防火墙 **109**：SMS 消息、小区广播消息、BIP、Java RMI、支持 SATSA 说明书或其他远程管理技术的 J2ME midlet、无线装置的操作系统、无线装置上的应用程序。这些实施例可以使个人管理 SIM 防火墙 **109**，而不必物理地连接到 SIM **107**。

在一个实施例中，可以使用信用卡适用器（CAD）或其他物理地连接到 SIM 的智能读卡器、使用能够通过短距离射频技术与 SIM 进行通信的无接触智能卡技术来本地管理 SIM 防火墙 **109**。

在所示实施例中，SIM 防火墙当移动装置开机时可以自动启动，而当移动装置关机时可以停止。也可以通过这里描述的任意一个或所有的本地和远程管理技术来停止和启动 SIM 防火墙。

在示出的实施例中，无线装置 **101** 可以包括外部界面（EI）**111**。外部界面可以包括以下中的一个或多个：人-机界面（MMI）和机器到机器界面（M2M）。MMI 可以包括允许人作用于或操作无线装置的任意装置，包括但不限于以下：屏幕、照相机、指纹读取器、键盘、小键盘、话筒、光传感器、声音传感器、动作传感器、扬声器。M2M 可以包括允许另一装置与无线装置交换数据或操作无线装置的任意装置，包括但不限于以下：RS-232 串行通信数据端口、厂商的私有通信数据端口、通用串行总线（USB）数据端口、蓝牙收发信机数据端口、超宽带（UWB）收发信机数据端口、红外线数据端口、其他的短距离射频技术数据端口、或使无线装置与另一装置进行通信的其他数据端口。

在所示实施例中，无线装置 **101** 可以与网络 **105** 进行通信。网络 **105** 可以包括任意已知的能够接收无线传输的网络。

参照图 1B，其示出了实例网络 **105**。网络 **105** 可以包括以下中的一个或多个、以及任一或所有：本领域中描述为移动站（MS）的无线装置 **101**；基站收发台（BTS）**113**、基站控制器（BSC）**147**、移动交换中心（MSC）**117**、归属位置寄存器（HLR）**119**、认证中心（AuC）**121**、访问位置寄存器（VLR）**123**、网关移动交换中心（GMSC）**125**、公共交换电信网络（PSTN）**127**、短消息服务中心（SMSC）**129**、设备识别寄存器（EIR）**131**、非结构化补充业务数据（USSDGW）网关 **133**、互联网应用服务器（IAS）**135**、网关通用分组无线业务（GPRS）支持节点（GGSN）**137**、服务 GPRS 支持节点（SGSN）**139**、分组数据网络（PDN）**141**、SIM OTA 服务

器（OTA）**143**、以及 SMS 网关 MSC（SMS GMSC）**145**。可以以使用任意互连技术的拓扑布局来连接网络 **105** 的组件。

此处描述的网络 **105** 可以包括一般化的 GSM/GPRS 网络，虽然本领域的技术人员应当理解，本发明也可以用于采用不同载体、协议、技术、结构和拓扑的其他网络。在其他实施例中，网络 **105** 可以采用以下中的一个或多个：通用移动电信业务（UMTS）、码分多址（CDMA 包括 CDMA2000 1x、CDMA2000 1xEV-DO、CDMA2000 1xEV-DV、CDMA TIA/EIA/ANSI-95A/B）、GPRS、增强型数据速率 GSM 演进技术（EDGE）、宽带码分多址（W-CDMA）、个人数字蜂窝（PDC）、集成数字增强网络（iDEN）、高速上行链路分组接入（HSUPA）UMTS、高速下行链路分组接入（HSDPA）UMTS、自由移动的多媒体接入（FOMA）、时分同步码分多址（TD-SCDMA）、时分码分多址（TD-CDMA）、UMTS 时分双工（UMTS-TDD）、UMTS 长期演进（LTE）、频分复用（FDM）、频分双工（FDD）、直接序列（Direct Sequence）超宽带（DS-UWB）、网络协议多媒体子系统（IMS）、会话初始协议（SIP）、正交频分复用（OFDM）、正交频分多址（OFDMA）、软件定义无线电（SDR）、个人通信服务（PCS）、高速电路交换数据（HSCSD）、超宽度（UWB）、宽带综合调度增强网络（WiDEN）、非授权移动接入（UMA）、WiMax IEE 802.16、WiFi IEE 802.11、无线局域网（WLAN）、电路交换数据（CSD）、无线广域网（WWAN）、网络语音电话（VOIP）、时分多址（TDMA）、无线宽带（WiBro）、时分 CDMA（TD-CDMA）、无线局域网语音电话（VoWLAN）、多输入多输出（Multiple-input multiple-output）（MIMO）、可变扩频因子扩频正交频分复用、一键呼叫（PTT）、七号信令系统（SS7）、IP 七号信令系统、信息传输部分-第 2 级对等（Peer-to-Peer）适配层（M2PA）、信息传输部分-第 3 级用户适配层（M3UA）、公共信道七号信令系统（CCS7）、传

输控制协议/网络协议（TCP/IP）、超文本传输协议（HTTP）、安全超文本传输协议（HTTPS）、用户数据报（Datagram）协议（UDP）。

现在参照图 2A，示出了由基于 SIM 的防火墙处理的事件的一个实施例的流程图。简言之，网络 **105** 对无线装置接收的事件进行初始化（步骤 **201**）。在无线装置 **101** 内运行的基于 SIM 的防火墙 **109** 检测该事件（步骤 **203**），并评估该事件（步骤 **205**）。基于 SIM 的防火墙允许该事件（步骤 **207**），则该事件继续（步骤 **209**），从而传递到 EI **111**。然后可以通过从 EI **111** 到无线装置的传输来完成该事件（步骤 **211**），在这之后传输到网络（步骤 **213**）。

现在更详细地参照图 2A，在所示实施例中，网络 **105** 对无线装置接收的事件进行初始化（步骤 **201**）。该事件可以包括以下中的一个或多个：语音电话、视频电话、PTT 电话、小区广播消息、SMS 消息、即时通讯消息、无线应用协议（WAP）推（push）消息、多媒体消息服务（MMS）通知、SIM 更新消息、增强型短消息服务（EMS）消息、电子邮件通知、电子邮件消息、输入的加密/不加密数据连接指示、输入的加密/不加密数据连接、移动电视数据、无线装置的标注/查询（paging/polling）、输入的无线电、视频或其他多媒体内容、无线装置操作系统更新、无线装置应用程序更新、无线装置硬件更新、新的无线装置应用程序的安装。

在所示实施例中，然后，运行在无线装置中的 SIM 上的基于 SIM 的防火墙应用程序检测该事件（步骤 **203**）。在一些实施例中，SIM 防火墙可能以前已经向无线装置或无线装置操作系统（一个或多个可从网络接收的事件要指示给该无线装置或无线装置操作系统）进行了注册。在一个实施例中，在无线装置接收了该事件之后，关于该事件的信息和对于输入事件的控制可以从无线装置传递到 SIM 防火墙。在其他实施例中，SIM 可以主动地检测一个或多个事件。

在所示实施例中，然后，SIM 防火墙可以对照可配置标准来评估该事件（步骤 **205**），可配置标准可以存储在 SIM 或无线装置上。标准可以包括以下中的一个或多个：事件类型、输入或输出的事件、数据类型、数据内容、应用程序类型、协议、载体、源地址、目的地址、事件、日期、以前的使用量、以及以前的事件量。

在一个实施例中，SIM 防火墙可以通过部分和/或全部符合（match）来评估源地址和目的地址。SIM 防火墙可以评估寻址方案，寻址方案可以包括以下中的一个或多个：网络协议（IPv4 和/或 IPv6）地址和/或端口号、统一资源定位符地址、电子邮件地址、GPRS APN（接入点名称）、MSISDN（移动站综合服务数字网络）号、USSD 服务代码、小区 ID、IMEI（国际移动设备识别）、IMSI（国际移动用户识别）、SMS 端口号、无线装置端口号、无线装置支持的其他寻址方案。

在另一个实施例中，SIM 防火墙可以通过一个或多个时间分量的任意组合来评估事件。例如，父母可以指定孩子在上学时间不能使用移动电话来给朋友打电话或接听朋友的电话。或者，例如，公司经理可以指定公司的移动电话只可以在工作日的工作时间期间使用。SIM 防火墙也可以基于可配置的时间来评估事件，例如，它可以每隔 10 秒对条件进行评估。

在所示实施例中，如果配置的标准不禁止该事件，则基于 SIM 的防火墙会使该事件继续（步骤 **207**），从而该事件的控制从 SIM 传递到无线装置，然后传递到无线装置的外部界面（步骤 **209**）。

在所示实施例中，无线装置的外部界面继而可以处理该事件（步骤 **209**）。该事件可由以下中的一个或多个处理：外部界面的 M2M 或 MMI 界面。

在所示实施例中，通过从外部界面 **111** 到无线装置的传送来完成该事件（步骤 **211**），然后传递到网络（步骤 **213**）。

虽然在所示实施例中，在基于 SIM 的防火墙使事件继续进行（步骤 **207**）之后，该事件的控制从 SIM 传递到无线装置，然后传递到无线装置的外部界面（步骤 **209**），但是在其他实施例中，该事件的控制可以传递到以下实体中的一个或多个以处理：无线装置、无线装置上的应用程序、无线装置的操作系统、无线装置的硬件、SIM、SIM 上的应用程序。通过从接收实体发送，然后传递到网络，该事件完成（步骤 **213**）。

现在参照图 2B，其是示出了由基于 SIM 的防火墙处理的事件的另一实施例的流程图。简言之，网络 **105** 对无线装置接收的事件进行初始化（步骤 **201**）。运行在无线装置 **101** 内的基于 SIM 的防火墙检测该事件（步骤 **203**），并且评估该事件（步骤 **205**）。基于 SIM 的防火墙禁止该事件，从而该事件终止（步骤 **219**）。通过从无线装置传送到网络，该事件完成（步骤 **221**）。

现在更详细地参照图 2B，在示出的实施例中，网络 **105** 对无线装置接收的事件进行初始化（步骤 **201**）。可以如对图 2A 所描述的那样来执行这个步骤。

在所示实施例中，可以由运行在 SIM 上的基于 SIM 的防火墙应用程序检测该事件（步骤 **203**）。可以如对图 2A 所描述的那样来执行这个步骤。

在所示实施例中，基于 SIM 的防火墙应用程序会对照可以存储在 SIM 或无线装置上的可配置标准来评估该事件（步骤 **205**）。可以根据此处描述的任一实施例来执行这个步骤。在所示实施例中，

由配置的标准禁止该事件，因而 SIM 防火墙阻止了该事件继续进行。

事件继而终止（步骤 **219**），而控制被传递到无线装置。在一些实施例中，事件的终止可以通过从无线装置到网络的传输来完成（步骤 **221**）。

虽然在图 2A 和图 2B 示出的实施例中，由网络来初始化事件（步骤 **201**），但是在其他实施例中，基于 SIM 的防火墙可以检测和评估可由无线装置（**101**）、SIM（**107**）、SIM 上的应用程序、无线装置（**111**）的外部界面来初始化的其他事件，或者可以检测和评估可由基于 SIM 的防火墙（**109**）推断（infer）的事件。

由无线装置初始化的事件可以包括但不限于以下：由计时器（timer）产生的事件、由外部或内部读卡器产生的事件、涉及访问或修改无线装置的文件系统或存储的事件、涉及访问或修改访问外部存储技术（诸如 SD（安全数字）闪存、MMC（多媒体卡）闪存、压缩闪速存储器、存储棒、闪存 RAM/ROM、EPROM（可擦除可编程只读存储器）、EEPROM（电可擦除可编程只读存储器）、固态存储器、硬盘驱动、NAND 闪速存储器）的事件、涉及启动或终止在无线装置上执行的应用程序或服务的事件、由无线装置的操作系统产生的事件、涉及开始或终止无线装置上的数据会话的事件、涉及从另一装置接收蓝牙通信的事件、涉及从另一装置接收红外线通信的事件、以及涉及使用短距离射频技术从另一装置接收通信的事件。

由无线装置的外部界面初始化的事件可以包括：涉及用户操作无线装置的按钮的事件、涉及用户操作无线装置上的操纵杆的事件、涉及用户操作用户输入机制（包括无线装置的语音控制）的事件、涉及用户发送 SMS 消息的事件、涉及用户发送 MMS 消息的事

件、涉及 USSD 消息的事件、涉及用户发送即时消息的事件、涉及用户开始或终止语音呼叫的事件、涉及用户开始或终止视频呼叫的事件、涉及用户开始或终止 VOIP 呼叫的事件、涉及用户开始或终止 PTT 呼叫的事件、涉及用户开始或终止蓝牙数据会话的事件、涉及用户开始或终止红外线数据会话的事件、涉及用户开始或终止数据会话的事件、涉及用户开始或终止无线装置或 SIM 的服务的事件、以及涉及用户开始或终止无线装置或 SIM 上的应用程序的事件、通过 M2M 发送到无线装置的 AT 命令、通过 M2M 发送到 SIM 的 AT 命令、通过 M2M 发送到无线装置或 SIM 的其他编程命令。

由 SIM 初始化的事件可以包括：由 SIM 上的应用程序产生的事件、涉及访问或修改 SIM 的文件系统或存储的事件、涉及访问或修改 SIM 的加密或其他保护文件或存储、以及涉及适用于 SIM 的文件或内存的密码操作的事件。

现在参照图 3，示出了由 SIM 防火墙执行的用于过滤事件的方法的一个实施例的流程图。简言之，该方法包括：读取配置设置（步骤 **303**）；向无线装置注册（步骤 **305**），以及；检测事件（步骤 **307**）；确定该事件是否符合许可标准（criteria for allowance）（步骤 **309**）；并且，如果事件符合，则许可该事件（步骤 **311**）。如果不许可该事件，则该方法还包括：终止该事件（步骤 **313**）；确定是否指示 EI（步骤 **315**）；以及潜在地向 EI 发送指示（步骤 **317**）。

现在更详细地参照图 3，在示出的实施例中，SIM 防火墙读取配置设置（步骤 **303**）。在一个实施例中，防火墙从在 SIM 上存储的文件中读取配置设置。在其他实施例中，防火墙从 SIM 的内存中读取配置设置。在另外的实施例中，防火墙从在无线装置上存储的其他文件中读取配置设置。

在一个实施例中，配置设置包括无线装置或 SIM 上的存储文件或存储区。存储文件或存储区包括以下中的一个或多个：源地址、目的地址、协议、载体、时间类型、输入或输出方向、数据类型、数据内容、应用程序、资源、期间事件允许或禁止的时间、如果事件禁止是否应该指示外部界面、以及符合这些标准中的一个或多个的事件是否应该允许或禁止。

在基于 SIM 的防火墙读取了配置设置（步骤 **303**）之后，就可以向无线装置注册，并且可以启动任意所需的计时器（步骤 **305**）。应该由无线装置指示的 SIM 防火墙向无线装置注册在配置设置中指定的所有事件。

在一个实施例中，SIM 防火墙可以启动一个或多个计时器，用于在配置设置中指定的时间停止。在其他实施例中，SIM 防火墙可以向无线装置请求启动一个或多个计时器，用于在配置设置中定义的期间停止。当计时器停止时，无线装置向 SIM 防火墙指示该事件。

在所示出的实施例中，当 SIM 防火墙检测到事件时（步骤 **307**），SIM 防火墙确定该事件是否符合允许标准（步骤 **309**）。如果事件符合允许标准，则许可该事件（步骤 **311**），于是 SIM 防火墙准备检测另一事件（步骤 **307**）。可以使用此处描述的任何标准和信息来作出所述确定。在其他的实施例中，SIM 防火墙可以确定事件是否符合拒绝标准。在另外的实施例中，SIM 防火墙可以基于允许标准和拒绝标准两者来确定是否允许事件。在一个实施例中，SIM 防火墙可以包括等级标准。例如，SIM 防火墙可以包括拒绝所有至给定区代码的出话呼叫、而允许来自所述区代码内的特定号码的呼叫的标准。

如果事件不符合允许标准，则终止该事件（步骤 **313**），然后，SIM 防火墙准备检测另一事件（步骤 **307**）。在一些实施例中，SIM

防火墙访问配置设置，以确定是否应该向外部界面指示禁止事件已经终止（步骤 **315**），然后，SIM 防火墙准备检测另一事件（步骤 **307**）。

在其他实施例中，SIM 防火墙可以向网络发送终止事件（步骤 **313**）、或许可事件（步骤 **311**）的指示。传送可以使用以下中的一种或多种：SMS 消息、USSD、BIP、HTTP/HTTPS、GPRS、TCP/IP、UDP 或任意其他的通信技术。

在一些实施例中，网络或无线装置可以顺序地向个人、无线装置、计算机、服务器、或任意其他的电子系统发送检测事件和/或终止事件的指示。使用交互式语音应答（IVR）、语音可扩展标记语言（VXML）和文本到语音（TTS）技术、HTTP/S、TCP/IP、UDP、可扩展标记语言（XML）或其他通信技术的网络或无线装置利用电子邮件、SMS、EMS、MMS、即时消息、语音呼叫、视频呼叫、VOIP 呼叫、PTT 呼叫或语音呼叫来发送指示。例如，网络可以向父母的电子邮件地址发送来自给定电话号码的呼叫被阻止而不能到达孩子的电话的指示。或者，例如，无线装置可以向公司的会计经理可访问的日志发送阻止了该装置的用户向给定区代码打电话的指示。或者例如，无线装置可以向父母的移动装置发送孩子的移动电话正在访问给定的互联网网址或 IP 地址的文本消息。

现在参照图 4，示出了由 SIM 防火墙执行的、用于处理远程管理事件的方法的一个实施例的流程图。简言之，该方法包括：从网络中接收远程管理事件（步骤 **407**）。远程管理事件可以包括以下中的一个或多个：命令 SIM 防火墙停止（步骤 **409**）；命令 SIM 防火墙重新启动；修改 SIM 防火墙的配置设置（步骤 **411**）；保存 SIM 防火墙的经修改的配置设置（步骤 **413**）；修改 SIM 防火墙的可执行文件和可执行库（步骤 **415**）；保存 SIM 防火墙的经修改的可执行文件和可执行库（步骤 **417**）；以及重启 SIM 防火墙（步骤 **419**）。

在其他的实施例中，SIM 防火墙可以执行用于处理本地管理事件的上述方法。可以根据此处描述的任意实施例来执行该方法。在另外的实施例中，远程管理事件可以由无线装置、或无线装置的操作系统上的应用程序来接收，并且在某些情况下被修改，然后被传递到 SIM 防火墙或 SIM。

现在更加详细地参照图 4，在示出的实施例中，SIM 防火墙从网络中接收远程管理事件（步骤 **407**）。可以根据此处描述的任意实施例来执行这个步骤。

在示出的实施例中，SIM 防火墙可以接收包括 SIM 防火墙停止运行的命令的远程管理事件（步骤 **409**）。SIM 防火墙停止运行的命令可以包括：永久停止运行的命令；在无线装置开机之前停止运行、在无线装置开机时重新启动的命令；或停止运行直到指示再次启动的命令。一旦接收到所述命令，SIM 防火墙就可以相应地停止运行。

在示出的实施例中，SIM 防火墙、或 SIM 操作系统可以接收包括修改配置设置的命令的远程管理事件（步骤 **411**）。修改配置设置的命令可以包含：利用新的配置设置来重写现有的配置设置、或删除现有的配置设置并使用新的配置设置数据来代替它们的命令和数据。

在示出的实施例中，SIM 防火墙、或 SIM 操作系统保存新的配置设置，以在 SIM、或无线装置上保持存储（步骤 **413**）。SIM 防火墙可以立即使用配置设置，或者可以重启（步骤 **419**）并读取配置设置。

在示出的实施例中，SIM 防火墙、或 SIM 操作系统可以接收包括修改 SIM 防火墙应用程序的库和文件的命令的远程管理事件（步骤 **415**）。修改 SIM 防火墙应用程序的库和文件的命令可以包含：

需要删除库和文件并使用新的库和文件来代替它们、或利用新的库和文件来重写库和文件的命令和数据。在其他实施例中，修改 SIM 防火墙的库和文件的命令可以包含从网络的某位置下载新的库和文件的命令。

然后，SIM 防火墙、或 SIM 操作系统保存文件和库，以在 SIM、或无线装置上保持存储（步骤 **417**）。之后，SIM 防火墙立即使用新的库和文件，或者可以重启（步骤 **419**）以使用新的库和文件。

在一些实施例中，个人、无线装置、计算机或电子系统可以使用所描述的方法以远程地设置 SIM 防火墙的配置设置。在一个实施例中，使用互联网网络浏览器的人连接到允许授权用户修改 SIM 防火墙的配置设置的网站。然后，该网站连接到网络并向 SIM 防火墙发送配置设置。然后，网络将终止或许可事件的指示发送给网站、或无线装置或电子系统。在其他实施例中，个人可以使用 SMS、MMS、EMS、即时消息、无线应用协议（WAP）、i-mode 模式、IVR 或其他的通信技术以远程地设置配置设置。在一些实施例中，配置设置可以由使用 IPTV、交互式 TV、移动网站、语音识别系统、或语音自动系统中的一个或多个的用户来远程设置。在一些实施例中，配置设置可以由使用第二移动装置的用户来远程设置。在这些实施例之一中，可以（例如）通过蓝牙连接，从第二移动装置将配置设置直接发送至待配置的装置。

例如，最近为孩子买了移动电话的父母可以登陆网站，该网站允许父母指定电话可以将呼叫发送到的号码和电话可以接收呼叫的号码、以及任意其他的防火墙设置。然后，网站可以将已配置的设置发送到孩子的电话，电话以这些设置激活。或者，例如，公司可以使用网站来配置分发给公司员工的多个无线装置。经理可以访问网站来设置这些装置使用的最大分钟数。然后，该网站可以向公司指定的所有装置发送已配置的设置。

尽管本文中描述了多个实施例，但是应该理解，本领域技术人员可以想到多种其他修改和实施例，他们都将落入本公开的原则的精神和范围内。更具体地，在本公开、附图、以及所附权利要求的范围内，可以在主题结合排列的排列方式和/或组成部分方面进行各种修改和改变。除了组成部分和/或排列方面的修改和改变以外，可选的使用对本领域技术人员来说是显而易见的选择。

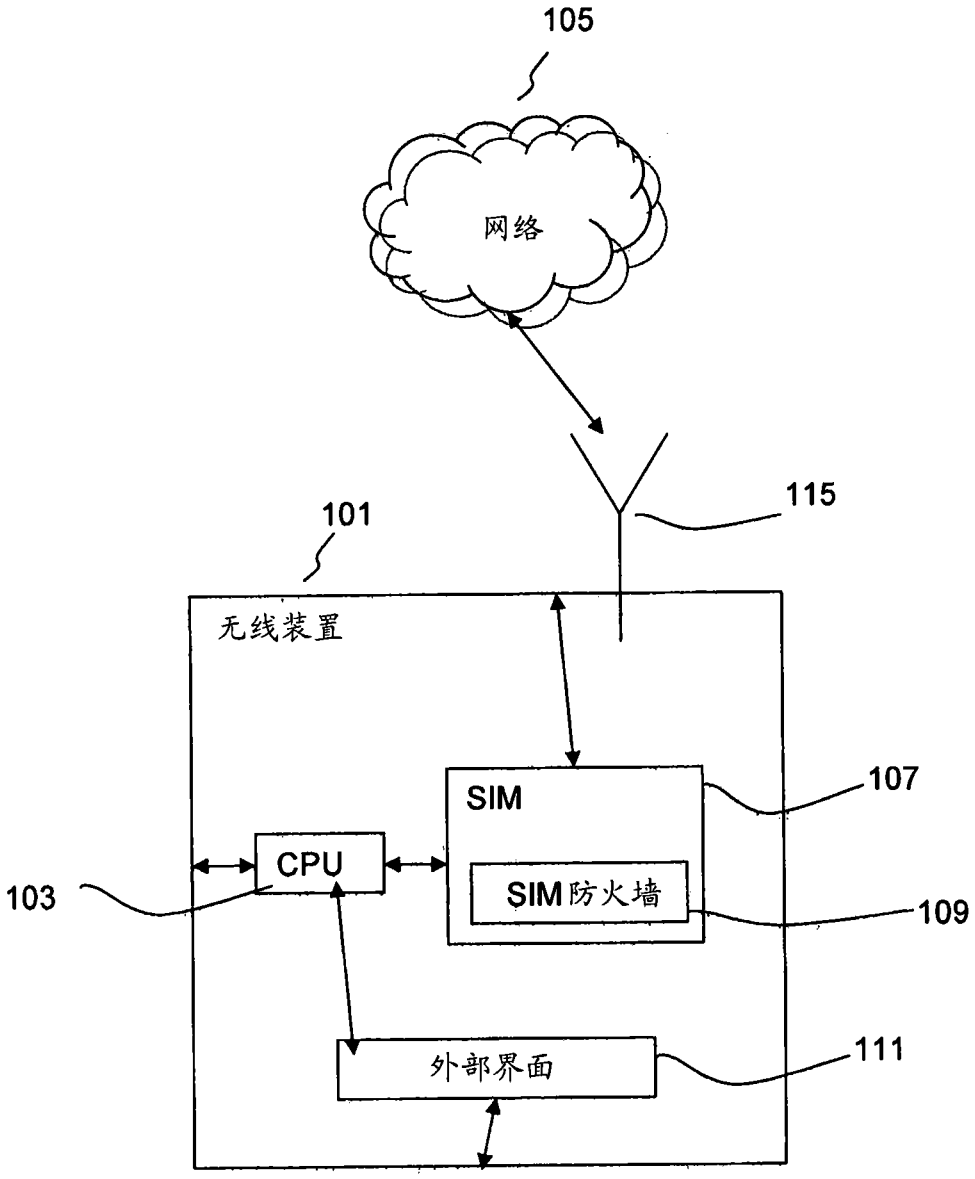


图 1A

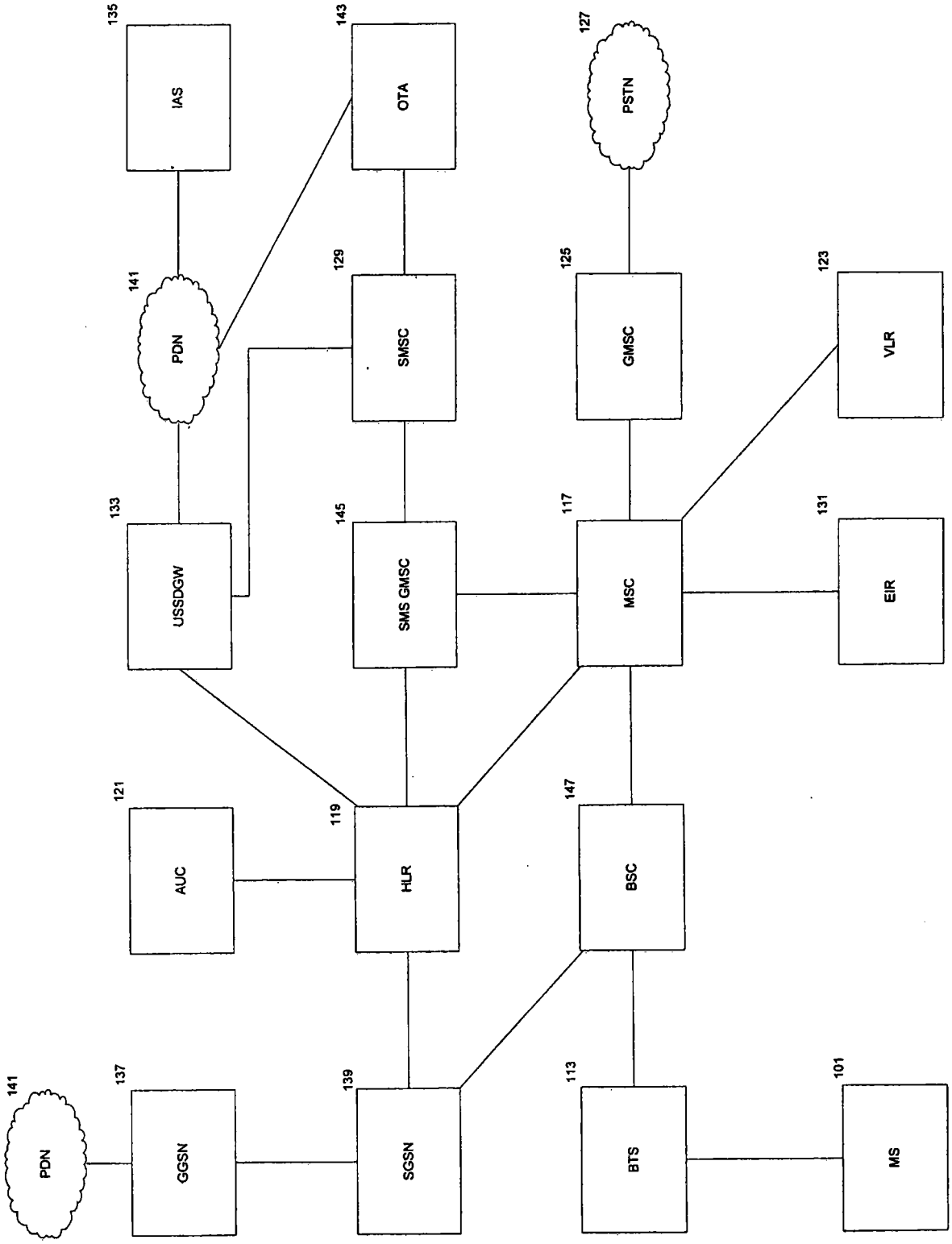

135
IAS
143
OTA
127
PSTN
141
PDN
129
SMSC
125
GMSC
123
VLR
133
USSDGW
145
SMS GMSC
117
MSC
131
EIR
121
AUC
119
HLR
147
BSC
141
PDN
137
GGSN
139
SGSN
113
BTS
101
MS

图 1B

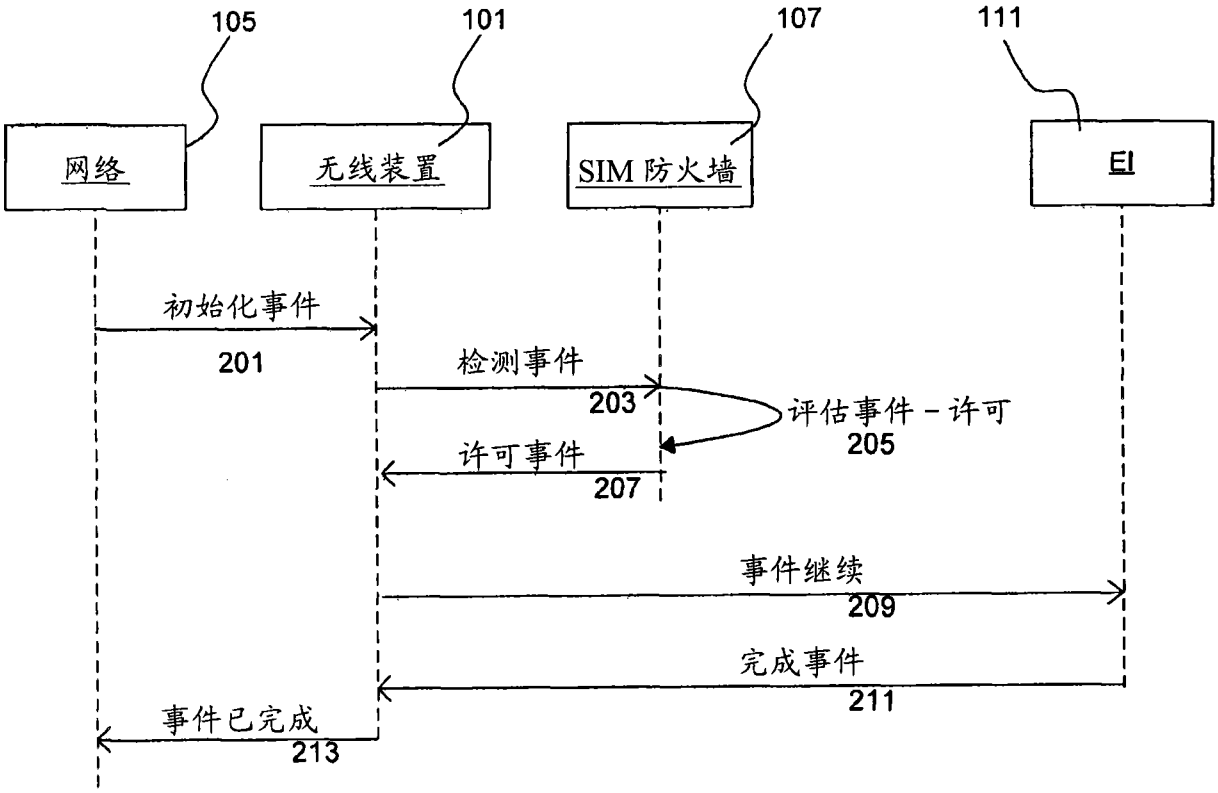

105
101
107
111
网络
无线装置
SIM 防火墙
EI
初始化事件
201
检测事件
203
评估事件 - 许可
205
许可事件
207
事件继续
209
完成事件
211
事件已完成
213

图 2A

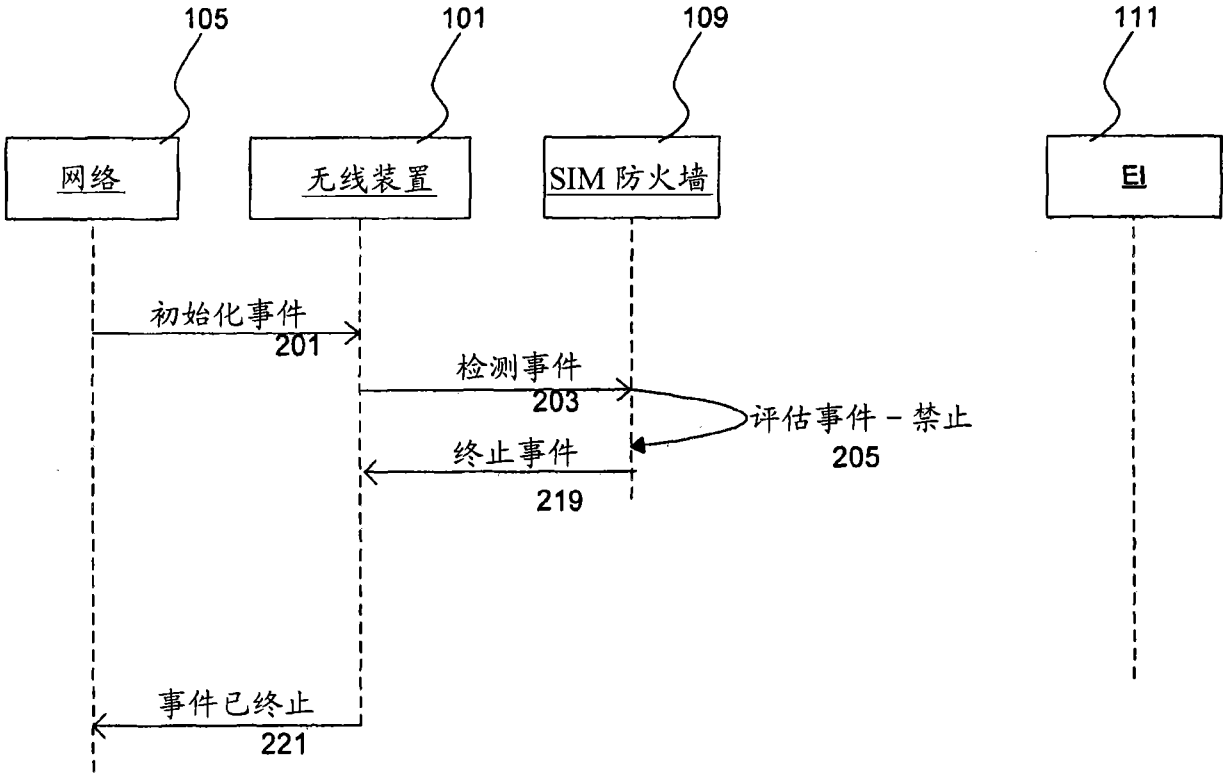

105
101
109
111
网络
无线装置
SIM 防火墙
EI
初始化事件
201
检测事件
203
评估事件 - 禁止
205
终止事件
219
事件已终止
221

图 2B

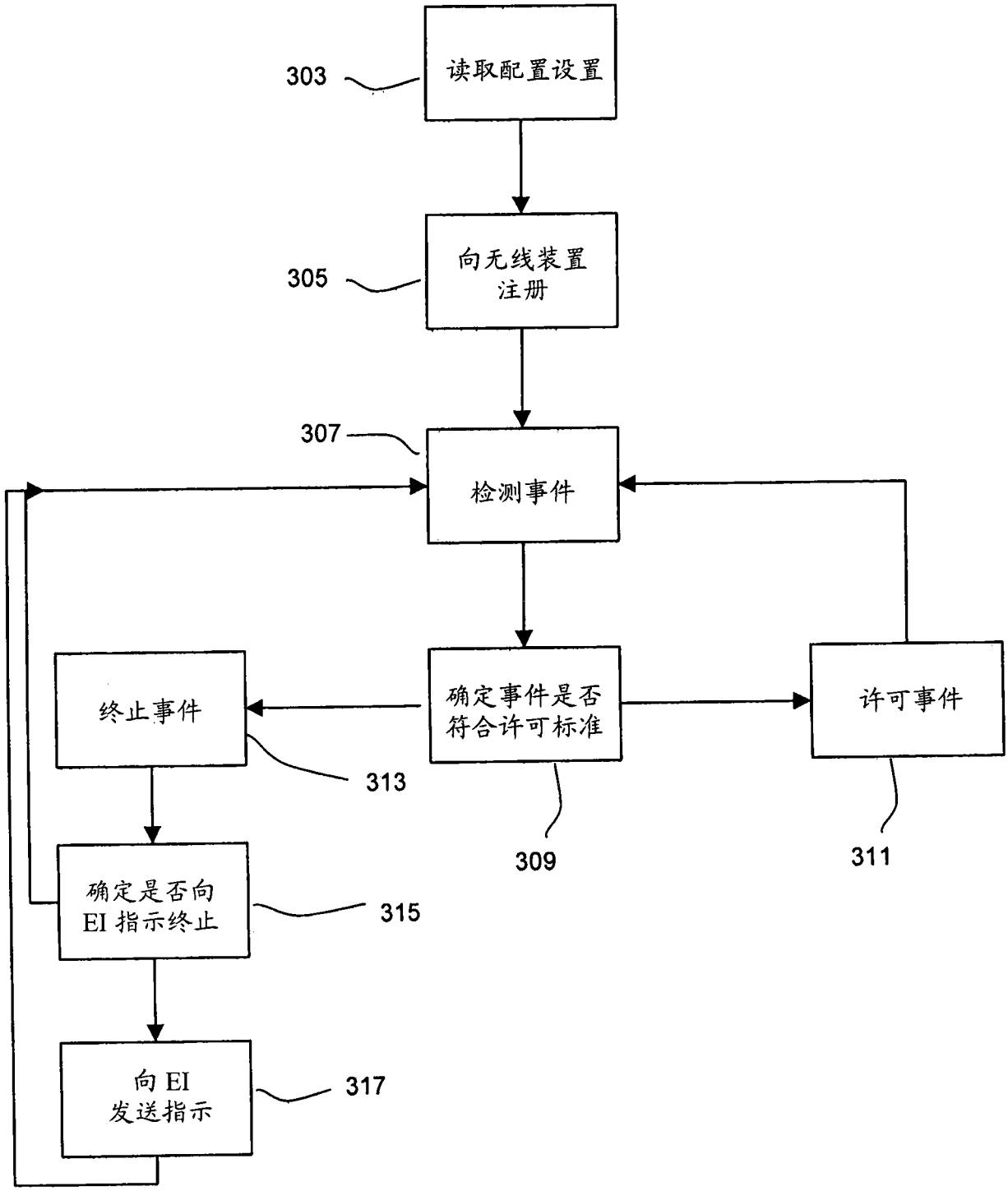

303
读取配置设置
305
向无线装置
注册
307
检测事件
终止事件
确定事件是否
符合许可标准
许可事件
313
309
311
确定是否向
EI 指示终止
315
向 EI
发送指示
317

图 3

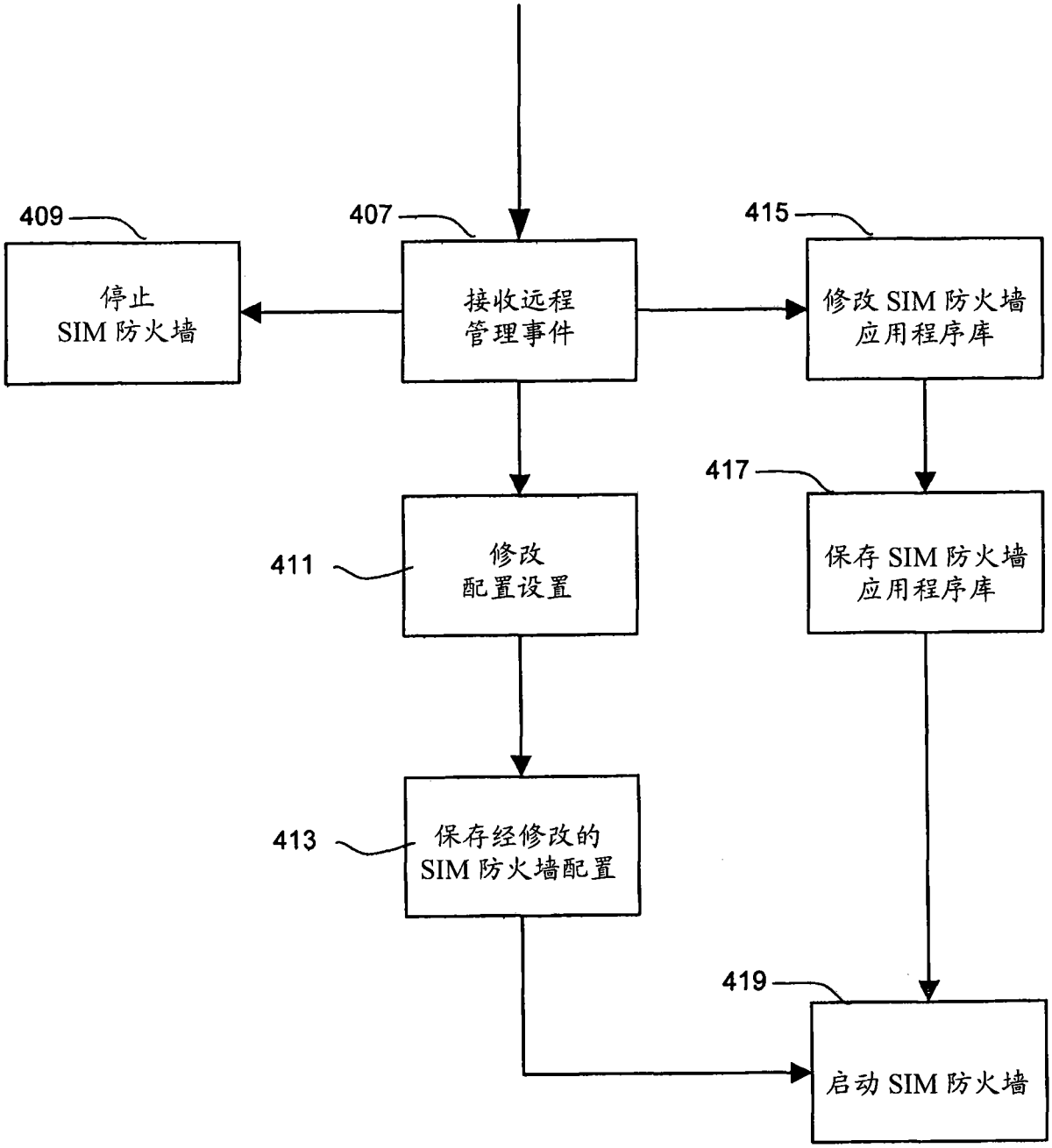

409
停止
SIM 防火墙
407
接收远程
管理事件
415
修改 SIM 防火墙
应用程序库
411
修改
配置设置
417
保存 SIM 防火墙
应用程序库
413
保存经修改的
SIM 防火墙配置
419
启动 SIM 防火墙

图 4