(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101909711 B
(45)授权公告日 2014.12.24

(21)申请号 200880122998.5
(22)申请日 2008.10.20
(30)优先权数据
11/925570 2007.10.26 US
11/927357 2007.10.29 US
11/929617 2007.10.30 US
11/932863 2007.10.31 US
(85)PCT国际申请进入国家阶段日
2010.06.25
(86)PCT国际申请的申请数据
PCT/US2008/080527 2008.10.20
(87)PCT国际申请的公布数据
WO2009/055342 EN 2009.04.30
(73)专利权人 美国索尼电脑娱乐公司
地址 美国加利福尼亚州
(72)发明人 G·扎列夫斯基 A·哈里斯
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 王岳 李家麟
(51)Int.Cl.
A63F 9/24(2006.01)
(56)对比文件
US 2003216962 A1,2003.11.20,
CN 1558574 A,2004.12.29,
CN 1783068 A,2006.06.07,
US 2007105624 A1,2007.05.10,
审查员 楚大顺

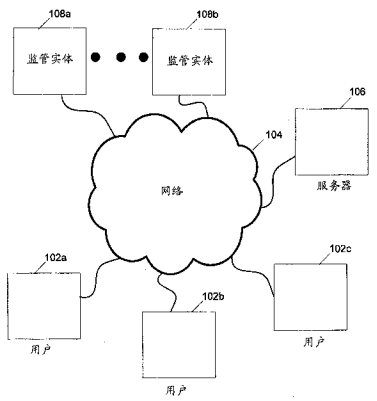
权利要求书3页 说明书19页 附图18页

(54)发明名称

资源的在线监控

(57)摘要

描述有用于监管在线社区中的活动的方法、装置和技术。一些方面包括:由社区成员响应于另外的社区成员的不当活动而激活触发机构。接收在激活触发机构的时间左右的社区成员的活动的基于时间的历史记录。根据所述基于时间的历史记录来重建所述社区活动。评估所述社区成员的活动以确定是否存在不当活动,并且如果存在引起问题的社区成员的不当活动,则对所述引起问题的社区成员采取适当行动。



CN 101909711 B

1. 一种监管在线会话的方法，其特征在于，该方法包括：

由在线社区中的第一在线用户观察所述在线社区中的第二在线用户的不当行为；

响应于所述不当行为而激活触发机构；所述触发机构的激活发起对在线社区活动的基于时间的历史的存储，所述基于时间的历史覆盖如下的时间段：该时间段在激活触发机构以前延长所期望的持续时间以及在激活触发机构以后延长所期望的持续时间；以及

当观察到所述不当行为时捕获所述在线会话的基于时间的历史，其包括捕获虚拟角色的景观和声音以监控受到在线用户控制的虚拟角色的不当行为，以及评估所述基于时间的历史以确定所述在线用户是否已经进行了不当行为；

将所述基于时间的历史传输给监管实体，所述监管实体接收所述基于时间的历史并且重建所述在线活动以确定是否存在所述用户之一的不当活动，并且如果存在所述用户之一的不当活动，则对所述用户采取适当行动；以及

对引起问题的在线用户采取适当行动包括以下之中的至少一个：向所述引起问题的在线用户发出警告；限制所述引起问题的在线用户的可用在线选项；以及约束所述引起问题的在线用户对所述在线社区的访问。

2. 根据权利要求 1 所述的方法，其特征在于捕获基于时间的历史包括将特定在线用户的标识与所述特定在线用户的在线活动相关联。

3. 根据权利要求 1 所述的方法，其特征在于包括在所述基于时间的历史中的活动类型包括：文字聊天、音频聊天、所有人物的状态、它们的位置、以及在重新创建在线会话中有用的数据。

4. 根据权利要求 1 所述的方法，其特征在于所述在线会话的基于时间的历史被存储在缓冲器中作为滑动的在线活动窗口。

5. 根据权利要求 1 所述的方法，其特征在于对引起问题的用户采取适当行动包括禁用所述引起问题的在线用户的通信能力。

6. 一种监管在线会话的系统，其特征在于，所述系统包括：

至少两个在在线社区中通信的用户，

其中在线社区中的第一用户观察所述在线社区中的第二用户的不当行为以响应于所述不当行为按下应急按钮，

应急按钮的按下发起对在线社区活动的基于时间的历史的存储，

其中当观察到所述不当行为时捕获基于时间的历史，其包括捕获虚拟角色的景观和声音以监控受到在线用户控制的虚拟角色的不当行为，以及评估所述基于时间的历史以确定所述在线用户是否已经进行了不当行为；

所述基于时间的历史覆盖如下的时间段：该时间段从按下应急按钮以前的第一期望的持续时间延伸到按下应急按钮以后的第二期望的持续时间；以及

监管实体，其接收所述基于时间的历史并且重建所述在线活动以确定是否存在所述用户之一的不当活动，并且如果存在所述用户之一的不当活动，则对该一个用户采取适当行动，采取适当行动包括以下项之中的至少一个：向引起问题的社区成员发出警告；限制所述引起问题的社区成员的可用在线选项；以及约束所述引起问题的社区成员对所述在线社区的访问。

7. 一种在在线社区中使用的支持网络的设备，其特征在于，该支持网络的设备包括：

触发机构，其在由网络用户基于包括网络用户的认知和网络社区标准的因素观察到不当在线活动时被该网络用户激活；所述触发机构的激活发起对在线社区活动的基于时间的历史的存储，所述基于时间的历史覆盖如下的时间段：该时间段在激活所述触发机构以前延长所期望的持续时间以及在激活所述触发机构以后延长所期望的持续时间；

处理器，其在触发机构被激活时捕获在线社区中的网络用户的在线活动的基于时间的历史，其包括捕获虚拟角色的景观和声音以监控受到在线用户控制的虚拟角色的不当行为，以及评估所述基于时间的历史以确定所述在线用户是否已经进行了不当行为；以及

网络接口，其将所述基于时间的历史传输给监管实体，

其中所述监管实体接收所述基于时间的历史并且重建所述在线活动以确定是否存在所述用户之一的不当活动，并且如果存在所述用户之一的不当活动，则对所述用户采取适当行动；其中所述适当行动包括以下项之中的至少一个：向引起问题的在线用户发出警告；限制所述引起问题的在线用户的可用在线选项；以及约束所述引起问题的在线用户对所述在线社区的访问。

8. 一种分配在线资源以监控已经被识别为进行不当行为的在线用户的方法，其特征在于，该方法包括：

接收在线用户可能正在进行不当行为的指示，

其中在另一个在线用户采取行动以发起存储所述在线用户的在线社区活动的基于时间的历史时发送所述指示，所述基于时间的历史覆盖如下时间段，该时间段在采取所述行动之前延长期望的持续时间并且在采取所述行动之后延长期望的持续时间；

捕获包括所述在线用户的在线社区活动的在线会话的基于时间的历史；

重建所述在线社区活动并且确定是否存在引起问题的在线用户的不当活动；

针对所述引起问题的在线用户的监控的所希望等级分配在线资源。

9. 根据权利要求 8 所述的方法，其特征在于捕获所述基于时间的历史包括：将在线用户标识与其在线活动相关联。

10. 根据权利要求 8 所述的方法，其特征在于针对引起问题的在线用户的监控的所希望等级分配在线资源包括：指派在线资源以跟踪引起问题的在线用户的活动。

11. 根据权利要求 8 所述的方法，其特征在于，所述方法进一步包括：捕获所述基于时间的历史的网络资源分配实体。

12. 根据权利要求 8 所述的方法，其特征在于，所述方法进一步包括：监管实体，该监管实体捕获所述基于时间的历史，重建所述在线社区活动，并且把引起问题的用户的监控的所期望等级传递给网络资源分配实体，所述网络资源分配实体分配网络资源。

13. 根据权利要求 8 所述的方法，其特征在于基于所述基于时间的历史的多个数据来进行重建所述在线社区活动，所述多个数据包括：文字聊天、音频聊天、所有人物的状态、它们的位置、以及与所述基于时间的历史相关的任何其他数据。

14. 一种分配在线资源以监控已经被识别为进行不当行为的在线用户的方法，其特征在于，该方法包括：

接收由在线用户响应于另一个在线用户的有嫌疑的不当行为而激活触发机构的指示；

其中在所述在线用户采取行动以发起存储另一个在线用户的在线社区活动的基于时

间的历史时发送所述指示，所述基于时间的历史覆盖如下时间段，该时间段在采取所述行动之前延长期望的持续时间并且在采取所述行动之后延长期望的持续时间；

接收在激活触发机构的时间左右的用户的在线社区活动的基于时间的历史；

根据所述基于时间的历史来重建所述在线活动；以及

评估所述用户的活动以确定是否存在引起问题的社区成员的不当行为，并且如果存在不当行为，则分配在线资源以监控已经被识别为进行不当行为的用户。

15. 根据权利要求 14 所述的方法，其特征在于基于所述基于时间的历史的多个数据来进行重建所述在线社区活动，所述多个数据包括：文字聊天、音频聊天、所有人物的状态、它们的位置、以及与所述基于时间的历史相关的任何其他数据。

16. 一种监管在线会话的系统，具有被分配以监控在线社区的成员的在线资源，其特征在于，所述系统包括：

至少两个在所述在线社区中通信的用户，其中所述在线社区中的第一用户观察所述在线社区中的一个或多个其它用户的有嫌疑的不当行为，第一用户响应于所述不当行为采取行动，

其中采取所述行动以发起存储在线社区活动的基于时间的历史，所述基于时间的历史覆盖如下的时间段：该时间段在采取所述行动之前延长期望的持续时间以及在采取所述行动之后延长期望的持续时间；

监管实体，接收所述基于时间的历史并且重建所述在线社区活动以根据目前用以度量不当行为的标准来确定是否存在所述用户之一的不当行为，并且如果存在所述用户之一的不当行为，则确定监控的所期望等级以跟踪引起问题的用户的在线社区活动；

网络资源分配实体，分配在线资源以跟踪引起问题的用户的活动。

17. 根据权利要求 16 所述的系统，其特征在于，基于所述基于时间的历史的多个数据来进行重建所述在线社区活动，所述多个数据包括：文字聊天、音频聊天、所有人物的状态、它们的位置、以及与所述基于时间的历史相关的任何其他数据。

资源的在线监控

技术领域

[0001] 本发明涉及在线会话、更具体而言涉及：对在线会话的基于社区的监管(moderation)；对在线会话中的作弊(cheating)的监管；基于在线会话的基于社区的监管而进行在线资源的分配；以及改善应用诚实性(integrity)。

背景技术

[0002] 在典型的在线会话（比如虚拟实现会话、游戏、以及其它应用）中，用户可以与在线社区中的其它在线用户交互和通信。在该交互期间，在线社区的成员可能易遭受来自该社区的其它成员的不当或冒犯性的行为。

[0003] 例如，一个社区成员可能开始给该社区的其它成员发送包括不良语言或其它不当语言的聊天消息。同样，该社区的一个成员可能作出对其它社区成员可见的不文雅的手势或绘图。

[0004] 另外，社区成员可能进行非法活动。例如，在虚拟现实环境中，社区成员之一可能发布色情内容或者进行其它非法活动。所述非法活动可能对该社区的其它成员是冒犯性的。

[0005] 在其它例子中，在线社区的成员可能进行在线游戏。在所述在线游戏期间，一人或多人、或者游戏玩家可能进行作弊以获得相对于其它游戏玩家的不公平的优势。所述作弊活动可能导致其它在线玩家对所述在线游戏不满。

[0006] 特定社区成员的冒犯性行动、非法行动、作弊或者其它不当行动可能降低其它社区成员的在线会话的乐趣。因此，需要改善在线会话中的监管。

发明内容

[0007] 本发明的实施例提供用于监管在线会话的方法、系统、装置、以及程序。在一个实施例中，一种用于在线会话的社区监管的方法包括：由第二在线用户观察第一在线用户的不当行为。第二在线用户响应于所述不当行为而激活或按下触发机构。所述在线会话的基于时间的历史记录被捕获。然后，所述基于时间的历史记录被传输给监管实体。

[0008] 在一个实施例中，所述在线会话的基于时间的历史记录包括在激活或按下触发机构以前发生达预先确定的时间量的在线会话活动。所述基于时间的历史记录的持续时间可以由用户来设置、或者其可以是预先确定的时间段、或者由网络实体或由其它技术来设置。所述基于时间的历史记录可以包括将在线用户标识与其在线活动相关联的信息。在一个实施例中，可以给观察到不当行为并且激活或按下触发机构的用户颁发奖励。触发机构的例子是应急按钮。

[0009] 在一种用于监管在线社区中的活动的方法的另一实施例中，该方法包括：接收由社区成员响应于另外的社区成员的不当活动而激活触发机构的指示。然后，接收在激活触发机构的时间左右的社区成员的活动的基于时间的历史记录。根据所述基于时间的历史记录来重建(recreate)所述社区活动。然后评估所述社区成员的活动以确定是否存在不当

活动，并且如果存在引起问题的 (offending) 社区成员的不当活动，则对所述引起问题的社区成员采取适当行动。

[0010] 在一种在线社区的又一实施例中，存在至少两个在该在线社区中通信的用户，其中该在线社区中的第一用户观察该在线社区中的第二用户的不当行为并且响应于所述不当行为按下应急按钮，应急按钮的按下发起对在线社区活动的基于时间的历史记录的存储，所述基于时间的历史记录覆盖如下的时间段：该时间段在按下应急按钮以前延长 (extend) 达所期望的持续时间以及在按下应急按钮以后延长达所期望的持续时间。所述在线社区还包括监管实体，所述监管实体接收所述基于时间的历史记录并且重建所述在线活动以确定是否存在所述用户之一的不当活动，并且如果存在所述用户之一的不当活动，则对所述用户采取适当行动。

[0011] 在又一实施例中，一种支持网络的设备包括触发机构。该设备还包括处理器，所述处理器捕获在线社区中的用户的在线活动的基于时间的历史记录。另外，存在将所述基于时间的历史记录传输给监管实体的网络接口，所述监管实体确定是否曾存在所述在线用户之一的不当在线活动。

[0012] 在一个实施例中，对引起问题的社区成员采取适当行动包括以下项之中的一个或多个：向所述引起问题的社区成员发出警告；限制所述引起问题的成员的可用在线选项；以及约束所述引起问题的社区成员对所述在线社区的访问。触发机构被激活可以是按下应急按钮。

[0013] 本发明的实施例还提供有用于检测和阻止在线游戏会话中的作弊的方法、系统、装置、以及程序。一些方面包括玩在线游戏。在该游戏的玩的期间，玩家之一检测另外的在线游戏玩家的有嫌疑的作弊行为。关于该在线游戏中的所有玩家的活动的游戏信息被收集，所述游戏信息包括在其期间发生有嫌疑的作弊行为的游戏时间段。所述游戏信息被传递给游戏作弊监控实体，所述游戏作弊监控实体评估所述游戏信息以确定是否存在作弊活动，并且如果存在作弊活动则采取适当行动。

[0014] 在一个实施例中，捕获在线游戏会话的游戏信息包括：捕获在检测到有嫌疑的作弊行为以前发生达预先确定的时间量的在线游戏会话活动。在一个实施例中，捕获所述游戏信息包括：将在线游戏玩家的标识与该玩家的在线活动相关联。在一个实施例中，给观察到作弊行为并且将所述游戏信息传递给所述游戏作弊监控实体的游戏玩家提供奖励。也可以存在由玩家响应于检测到有嫌疑的作弊活动而激活的触发机构。

[0015] 在另一实施例中，一种用于监管在线游戏社区中的作弊活动的方法包括：接收在线游戏会话中的玩家怀疑该游戏会话中的另外的玩家进行作弊行为的指示。接收所述有嫌疑的作弊行为的时间左右的游戏活动的游戏信息。根据所述游戏信息重建所述游戏活动。评估所述游戏中的玩家的活动以确定是否存在作弊行为，并且如果存在所述游戏玩家之一的作弊行为，则对作弊游戏玩家采取适当行动。适当活动的一个例子包括约束作弊游戏玩家对所述在线游戏的访问。

[0016] 在另一实施例中，一种在线游戏会话包括至少两个在该在线游戏会话中通信的玩家，其中该在线游戏会话中的第一玩家检测该在线游戏会话中的第二玩家的有嫌疑的作弊行为，第一用户将存在有嫌疑的作弊行为的指示传递给游戏作弊监控实体。所述游戏作弊监控实体在接收存在作弊行为的指示以后收集该在线游戏会话中的所有玩家的玩的游戏

信息，所述游戏信息包括如下的时间段：该时间段在接收所述指示之前和之后延长达所期望的持续时间，所述游戏作弊监控实体使用所述游戏信息来重建所述玩家的在线游戏活动，以确定是否存在所述玩家之一的作弊活动，并且如果存在所述玩家之一的作弊活动，则所述游戏作弊监控实体采取适当行动。适当行动的例子包括约束作弊玩家对所述在线游戏会话的访问。

[0017] 在又一实施例中，一种游戏作弊监控实体包括接收存在作弊行为的指示的网络接口。所述游戏作弊监控实体还包括收集该在线游戏会话中的所有玩家的游戏信息的处理器，所述游戏信息包括如下的时间段：该时间段在接收所述指示之前和之后延长达所期望的持续时间，所述处理器使用所述游戏信息来重建该游戏会话中的玩家的在线游戏活动，以确定是否存在所述玩家之中的一个或多个的作弊活动，并且如果存在一个或多个所述玩家的作弊活动，则所述游戏作弊监控实体采取适当行动。

[0018] 本发明的实施例还提供用于分配在线或其它网络资源以监控在线社区的方法、系统、装置、以及程序。在一个实施例中，一种分配在线资源以监控已经被识别为进行不当行为的在线社区成员的方法包括：接收在线用户可能进行不当行为的指示。捕获包括所述用户的行为的在线会话的基于时间的历史记录。重建所述在线活动并且确定是否存在引起问题的在线用户的不当活动。

[0019] 针对引起问题的在线用户的监控的所希望等级分配在线资源。在一个实施例中，在线会话的基于时间的历史记录包括：捕获在接收在线用户可能进行不当行为的指示以前发生达预先确定的时间量的在线会话活动。在另一实施例中，捕获所述基于时间的历史记录包括：将在线用户标识与其在线活动相关联。在一个实施例中，针对引起问题的在线用户的监控的所希望等级分配在线资源包括：指派在线资源以跟踪引起问题的在线用户的活动。另一实施例包括捕获基于时间的历史记录的网络资源分配实体。在一个实施例中，监管实体捕获所述基于时间的历史记录，重建所述在线活动并且把引起问题的用户的监控的所期望等级传递给网络资源分配实体，所述网络资源分配实体分配网络资源。

[0020] 在另一实施例中，一种用于分配在线资源以监控已经被识别为进行不当行为的在线社区成员的方法包括：接收由在线社区成员响应于另外的在线社区成员的有嫌疑的不当活动而激活触发机构的指示。接收在激活触发机构的时间左右的社区成员的在线活动的基于时间的历史记录。根据所述基于时间的历史记录来重建所述社区活动。评估所述社区成员的活动以确定是否存在不当活动，并且如果存在引起问题的社区成员的不当活动，则分配在线资源以监控已经被识别为进行不当行为的社区成员。

[0021] 在另一实施例中，一种具有被分配以监控在线社区的成员的在线资源的在线社区包括至少两个在该在线社区中通信的用户，其中该在线社区中的第一用户观察该在线社区中的一个或多个其它用户的有嫌疑的不当行为，第一用户响应于所述不当行为按下应急按钮，应急按钮的按下发起对在线社区活动的基于时间的历史记录的存储，所述基于时间的历史记录覆盖如下的时间段：该时间段在按下应急按钮以前延长达所期望的持续时间和在按下应急按钮以后延长达所期望的持续时间。监管实体，接收所述基于时间的历史记录并且重建所述在线活动以确定是否存在所述用户之一的不当活动，并且如果存在所述用户之一的不当活动，则确定监控的所期望等级以跟踪引起问题的用户的活动。网络分配资源分配实体，其分配在线资源以跟踪引起问题的用户的活动。

[0022] 在一个实施例中，一种网络实体包括接收在线用户可能进行不当活动的指示的网络接口。处理器，在所述指示被接收时捕获在线社区中的用户在线活动的基于时间的历史记录，重建该在线社区的在线活动并且确定是否曾存在所述在线用户之中的一个或多个的不当在线活动，并且如果存在不当活动，则分配在线资源以实现引起问题的用户的监控的所期望等级。

[0023] 在实施例中，所述在线会话的基于时间的历史记录包括在按下触发机构以前发生达预先确定的时间量的在线会话活动。所述基于时间的历史记录的持续时间可以由用户来设置、或者其可以是预先确定的时间段、或者由网络实体或由其它技术来设置。所述基于时间的历史记录可以包括将在线用户标识与其在线活动相关联的信息。在实施例中，可以给观察到不当行为并且按下触发机构的用户颁发奖励。触发机构的例子是应急按钮。

[0024] 本发明的实施例还提供有用于改善应用诚实性的方法、系统、装置、以及程序。在一个实施例中，一种用于改善应用的诚实性的方法包括：与该应用交互。观察该应用的意外的操作。响应于所述意外的操作激活触发机构。捕获所述应用会话的基于时间的历史记录。将所述基于时间的历史记录传递给网络实体以用于评估。

[0025] 在一个实施例中，该应用包括测试在线游戏，并且捕获所述基于时间的历史记录包括捕获在按下触发机构以前发生达预先确定的时间量的在线游戏会话活动。

[0026] 在一个实施例中，激活触发机构包括：按下应急按钮。在实施例中，观察该应用的意外操作包括观察该应用的操作中的假信号 (glitch)。在一个实施例中，该网络实体包括服务器、或者监管实体、或者其它网络实体。在另一实施例中，传递所述基于时间的历史记录包括：通过局域网、或者广域网（比如因特网）、或者网络的任意组合传输所述基于时间的历史记录。

[0027] 在另一实施例中，一种用于测试在线游戏的方法包括：接收触发机构响应于在线游戏的意外操作而被激活的指示。接收在激活触发机构的时间左右的在线游戏活动的基于时间的历史记录。根据所述基于时间的历史记录来重建所述游戏活动。评估所述游戏活动以确定是否存在该游戏的操作中的失常 (malfunction)。在另一实施例中，测试该在线游戏包括对该游戏的操作中的失常进行故障诊断。

[0028] 在又一实施例中，一种在线游戏测试单元包括触发机构。该测试单元还包括处理器，所述处理器在触发机构被激活时捕获游戏活动的基于时间的历史记录。该测试单元包括网络接口，所述网络接口将所述基于时间的历史记录传输给网络实体，所述网络实体确定是否存在该在线游戏的操作中的失常。

[0029] 在阅读下面的详细描述和附图以后，本发明的其它特征和优点将更容易地变得对于领域的技术人员而言显而易见。

附图说明

[0030] 图 1 是示出了用于监管在线用户活动的示例性体系结构的框图。

[0031] 图 2 是用于监管在线用户活动的网络体系结构的另一实施例的框图。

[0032] 图 3A 是示出社区监管方面的对等通信网络的框图。

[0033] 图 3B 是示出了由图 3A 的网络中的另一用户指示存在不当行为的框图。

[0034] 图 3C 是图 3A 的对等网络的框图，其示出了监管实体 108 采取预防行动。

[0035] 图 4A 是示出了社区监管方面的客户端服务器通信网络的框图。

[0036] 图 4B 示出了图 4A 的网络，其中服务器将音频聊天消息从第一用户传输到其它用户。

[0037] 图 4C 示出了图 4A 的网络，其中用户发送不当消息。

[0038] 图 4D 示出了图 4A 的网络，其示出了服务器对用户所发送的不当消息采取适当行动。

[0039] 图 5 是示出了检测和防止不当在线活动的方法的流程图。

[0040] 图 6 是检测不当在线行为的另一实施例的流程图。

[0041] 图 7 是示出响应于不当活动而采取适当行动的方面的流程图。

[0042] 图 8 是示出了使用社区监管来防止在线视频游戏中的作弊的实施例的流程图。

[0043] 图 9 是示出了监管在线行为方面的流程图。

[0044] 图 10 是评估用户在线活动的另一实施例的流程图。

[0045] 图 11 是测试环境的框图。

[0046] 图 12A 是图 12A 中所示的在线测试环境的流程图。

[0047] 图 12B 是图 11 中所示的测试环境的实施例的流程图。

[0048] 图 13 是示出了可以响应于用户的不当行为而采取的不同类型的行动的例子的表。

[0049] 图 14 是示出了可以结合在此所示各个实施例使用的示例性支持网络的设备 1450 的框图。

[0050] 图 15 是示出了可以结合在此所示各个实施例使用的示例性游戏作弊监控实体的框图。

[0051] 图 16 是示出了检测在线环境中的作弊的实施例的流程图。

[0052] 图 17 是示出了检测在线环境中的作弊的另一实施例的流程图。

[0053] 图 18 是可以分配资源的监管实体的另一实施例的框图。

[0054] 图 19 是示出了在线或其它网络资源分配方面的流程图。

[0055] 图 20 是示出了分配在线或其它网络资源的附加方面的流程图。

具体实施方式

[0056] 在阅读下面的描述以后，将变得对于本领域的技术人员而言显而易见的是：如何在各个可替代的实施例和可替代的应用中实施本发明。然而，尽管在此将描述本发明的各个实施例，但是应当理解，这些实施例仅仅是以例子的方式而不是约束的方式被提供的。因此，不应当将对各个实施例的所述详细描述解释成约束本发明的范围或外延。

[0057] 图 1 是示出了用于监管在线用户活动的示例性体系结构的框图。如图 1 所示，一个或多个用户或客户端 102a-c 与网络 104 通信。在一个实施例中，用户 102a-c 通过该网络在自组织 (ad-hoe) 通信网络中彼此通信。在另一实施例中，所述用户通过该网络与服务器 106 通信。用户 102 可以使用支持网络的设备、比如游戏控制台（比如 Sony play station 3)、膝上型计算设备、便携式游戏设备（比如play station portable)、台式计算设备、蜂窝电话、或者任意其它的能够与通信网络 104 对接的设备。

[0058] 在一个实施例中，所述体系结构包括监管实体 108，所述监管实体 108 也与网络

104 通信。监管实体 108 可以用于在用户 102a-c 之一进行不当或者不可接受的行为的情况下采取适当行动。例如，如后面将要讨论的样，监管实体 108 可以中断从一个用户到另一用户的通信或者可以在所期望的时间段内约束引起问题的用户对网络的访问。

[0059] 在一个实施例中，监管实体 108 是单独的网络节点。在其它实施例中，监管实体 108 可以并入其它网络节点（比如用户 102a-c 之中的一个或多个、或者服务器 106、或者其它网络实体）内。应当理解，对用户 102a-c 和服务器 106 以及监管实体 108 的参考仅仅是为了便于理解各个实施例。例如，可以在对等网络、客户端服务器网络的情形下或者在对等体组 (peer group) 内实施本发明的实施例。因此，在一些实例中，根据数据交换的定时和性质，客户端或用户可以充当服务器或监管实体并且反之亦然。例如，对等网络中的各个客户端可以每个都包括在线活动（比如虚拟现实）的一部分，并且可以发送和接收与所述在线活动相关的数据。因此，除非由特定的约束另行作出规定，对用户或服务器或监管实体的任何参考都意图包括由所述操作实体之中的一个或任意操作实体执行的操作。在一些实例中，可以以通用名称（比如网络节点、计算节点、或者网络设备）来指代具有用户 / 服务器功能的设备。就这一点而言，用户、服务器、以及监管实体每个都可以被认为是网络计算节点或网络设备。

[0060] 在一个示例性实施例中，一个用户 102c 可以在其它在线用户 102a 和 102b 在在线环境下交互时监控所述其它在线用户的活动。当用户 102c 之一认为用户 102a 和 102b 之一进行针对该在线环境的不当行为时，所述用户可以例如按下应急按钮或表示正在发生不当活动的一些其它指示。尽管该讨论描述了一个用户 102c 监控其它用户 102a-b，但是在其它实施例中，所有用户都监控所有其它用户的活动。在其它实施例中，可以授权所选用户或用户组监控其它在线用户。

[0061] 当应急按钮被按下时，该在线环境的快照 (snapshot) 被捕获并且被发送给监管实体 108 以用于评估。在线活动的快照包括当应急按钮被按下时以及应急按钮被按下之前的所期望的时间段内发生的活动。换言之，监控在线活动的每个用户设备 102 都包括缓冲器或其它类型的存储器，在那里存储在该在线环境下被监控的所有用户的某个持续时间的活动。通过这种方式，当应急按钮被按下时，缓冲器的内容（其包括在按下应急按钮以前的时间段以及在按下应急按钮之后的所期望的时间段）被发送给监管实体 108 以用于评估。所述基于时间的历史记录的持续时间可以由用户来设置、或者其可以是预先确定的时间段、或者由网络实体或由其它技术来设置。

[0062] 所述监管实体接收所存储的用户在线活动。然后，监管实体 108 对照一组已经被预先建立的标准或规则来评估所述在线活动。如果监管实体 108 确定所述用户行为之一不当，则监管实体 108 可以采取适当行动。例如，如果用户使用冒犯性语言，则监管实体 108 可以禁用该用户的麦克风。在另一个实施例中，监管实体 108 可以警告所述用户停止使用冒犯性语言，或者监管实体 108 可以约束所述用户并且仅仅允许所述用户访问该在线环境的可以接受所述语言的部分、比如该环境的仅限成人的部分，或者所述用户可以被完全禁止访问该在线环境。在另外的例子中，如果用户在游戏中作弊，则监管实体 108 可以警告所述用户停止作弊活动，或者监管实体 108 可以约束所述用户并且不允许该进行作弊的用户参与该游戏。

[0063] 在一个实施例中，可以奖励识别出不当行为的用户。例如，如果用户识别出游戏中

的作弊者，则可以给予所述用户奖励。奖励鼓励用户识别不当行为、比如作弊，并且由于采取适当行动，因此所有其它用户的在线体验被改善。当然，用户可能通过识别未涉及不当行为的其它用户来滥用所述奖励特性。为了阻止这些类型的错误识别，用户可以因作出虚假识别受到记过。

[0064] 图 2 是用于监管在线用户活动的网络体系结构的另一实施例的框图。如图 2 所示，多个用户 102a、102b、以及 102c 与网络 104 通信。与该网络通信的还有服务器 106。在图 2 的实施例中，存在多个监管实体 108a 至 108n。在该实施例中，每个监管实体都被配置为评估特定类型的不当行为。例如，一个监管实体可以被配置为评估在线环境中的冒犯性语言。某个不同的监管实体可以被配置为评估在线游戏中的作弊活动。另一监管实体被配置为评估在线非法活动、比如散布色情或其它非法材料。在其它实施例中，其它监管实体被配置为评估其它类型的不当在线行为。类似于图 1 的通信网络，一旦不当在线活动已经被监管实体确定，则可以采取适当行动。

[0065] 图 3A 是示出社区监管方面的对等通信网络的框图。如图 3A 所示，该社区包括通过通信网络 104 彼此通信的 3 个用户 102a、102b、以及 102c。与网络 104 通信的还有监管实体 108。在图 3A 所示的例子中，第一用户 102a 通过给其它用户 102b 和 102c 发送语音消息进行通信。在图 3A 的例子中，由第一用户 102a 发送的语音消息包括不当的或不良的语言。

[0066] 图 3B 是示出了由图 3A 的网络中的另一用户指示存在不当行为的框图。在一个实施例中，用户 102c 按下应急按钮以指示存在不当行为。图 3B 中所示，第三用户 102c 在从第一用户 102a 听到所述不当和不良消息以后按下应急按钮或者其它触发设备以指示正在或已经发生不当行为。当进行在线活动时，所述用户的支持网络的设备一直在缓冲在线活动的时段或基于时间的历史记录，由此记录该社区中的所有被监控用户的在线活动。换言之，第三用户的设备 102c 中的缓冲器具有滑动的存储窗口，所述滑动的存储窗口总是记录所述用户的以前的在线活动的一部分。当应急按钮被按下时，该网络上的所述以前的活动以及当前的活动和在所期望的持续时间内的将来活动被保存。然后，所述整个缓冲器可以被发送给监管实体 108。除了发送所记录的在线活动，被发送给监管实体 108 的消息可以包括对第三用户 102c 所报告的冒犯性或不当行为的类型的指示。可以被缓冲的在线活动的类型的例子包括对诸如下列在线活动的基于时间的历史记录：文字聊天、音频聊天、人物和 / 或在线参与者的状态、以及其它类型的在线活动。

[0067] 在另一实施例中，进行在线游戏的虚拟角色的景观和声音可以被捕获并且存储在基于时间的历史记录中。然后，监管实体 108 可以评估用户的在线活动的基于时间的历史记录，并且确定第一用户 102a 的行为是否不当、比如第一用户是否进行作弊。

[0068] 图 3C 是图 3A 的对等网络的框图，其示出了监管实体 108 采取预防行动。如图 3C 的例子中所示，在确定第一用户 102a 的活动不当以后，监管实体 108 可以采取预防行动。例如，监管实体 108 可以给第一用户 102a 发送指示其行为不当并且将来不要进行这样的行为的警告。还可以采取其它类型的预防行动。例如，监管实体 108 可以给第一用户 102a 的设备发送命令并且禁用第一用户 102a 的通信能力、比如禁用第一用户的麦克风。

[0069] 在其它实施例中，监管实体 108 可以采取诸如下列行动：中止引起问题的用户的签约 (subscription)，使得其不再能够进行所述在线活动。监管实体 108 还可以添加或增

加对已经进行不当活动的特定用户的监控。在其它实施例中，可以单独地或以任意组合使用这些类型的纠正行动。

[0070] 尽管图 3A-C 中所示的例子示出了 3 个用户，但是在其它实施例中，可以存在不同数目的用户。而且在其它实施例中，不同数目的用户或用户组可以监控和被监控。

[0071] 图 4A 是示出了社区监管方面的客户端服务器通信网络的框图。如图 4A 中所示，3 个用户 102a、102b、以及 102c 在进行在线活动时使用支持网络的设备通过服务器 106 通信。在图 4A 中，第一用户 102a 与第二和第三用户 102b、102c 进行音频聊天。来自 102a 的音频消息被路由到服务器 106。

[0072] 图 4B 示出了图 4A 的网络，其中该服务器将音频聊天消息从第一用户传输到其它用户。在图 4B 的例子中，服务器 106 将音频聊天消息从第一用户 102a 传输到第二和第三用户 102b、102c。在其它例子中，在该网络中可以存在多个其它用户。例如，第一用户的消息可以被传输给一个其它用户或任意数目的其它用户。

[0073] 图 4C 示出了图 4A 的网络，其中用户发送不当消息。在该例中，第一用户 102a 发送针对第二和第三用户 102b、102c 的音频聊天消息，并且所述消息包括不当内容。

[0074] 图 4D 示出了图 4A 的网络，其示出了服务器对用户所发送的不当消息采取适当行动。如图 4D 中所示，服务器 106 检测由第一用户 102a 所发送的音频消息并且确定其为不当。由于所述消息包括不当材料，因此服务器 106 不将其传输给第二和第三用户 102b、102c。服务器 106 还可以采取其它行动、比如警告第一用户 102a 其音频消息和行为不当、中止第一用户的签约、以及附加或增加地监控第一用户、以及其它类型的行动。

[0075] 在图 4A 至 4D 所示的实施例中，监控实体的功能被并入服务器 106 中。在其它实施例中，监控实体的功能可以被并入其它网络实体、比如用户设备、或其它网络设备中。

[0076] 尽管图 4A-D 中所示的例子示出了 3 个用户，但是在其它实施例中，可以存在不同数目的用户。而且在其它实施例中，不同数目的用户或用户组可以监控和被监控。

[0077] 图 5 是示出了用于检测和防止不当在线活动的方法的流程图。流程在框 502 中开始，其中在线用户观察冒犯性或不当行为。被认为是冒犯性或不当的行为的类型可以基于各个用户对不当行为的认知，或者基于关于什么是适当行为和不当行为的社区标准。在于 2006 年 8 月 9 日提交的名称为“Dynamic Rating of Content”的美国专利申请号 11/502,265 中公开有用于确定什么是适当行为和不当行为的各种技术，所述专利申请的全部内容通过引用并入本申请。

[0078] 流程继续进行到框 504，其中用户按下应急按钮或者执行另外的行动以指示或者响应于观察到冒犯性或不当的在线行为。然后，流程继续进行到框 506，其中所有社区成员的活动的基于时间的历史记录被捕获。所述基于时间的历史记录可以被存储在用户的设备中，并且包括滑动的在线活动窗口。换言之，过去的在线活动的一部分被连续地记录在缓冲器中，使得当应急按钮被按下时，以前的在线活动、以及当前的在线活动和将来时间段的在线活动的一部分被存储。通过这种方式，指示用户的不当或冒犯性在线活动的证据被捕获在基于时间的历史记录中。

[0079] 流程继续进行到框 508。在框 508 中，基于时间的历史记录被发送给监管实体。除了基于时间的历史记录，对冒犯性行为的类型的可选指示也可以被发送给监管实体。例如，可以发送如下指示：其示出用户认为该不当活动是冒犯性语言或非法活动、比如在线色情

内容、或者玩家在游戏中作弊、或者其它不当活动。

[0080] 然后，流程继续进行到框 510。在框 510 中，该监管实体评估所述基于时间的历史记录以确定所述活动是否是冒犯性或不当的。可选地，如果对冒犯性行为的类型的指示被包括在被发送给该监管实体的消息中，则所述基于时间的历史记录可以基于活动类型而被路由到该监管实体内的特定引擎、或者被路由到适当的监管实体。换言之，一个监管实体或监管实体内的引擎可以被优化为识别特定类型的不当活动、比如不良语言并且对其采取适当行动。不同的引擎或监管实体可以被优化为检测其它类型的不当活动、例如非法在线活动或游戏作弊等并且对其采取行动。

[0081] 然后，流程继续进行到框 512，其中该监管实体采取适当行动。在评估期间，如果该监管实体确定所述活动不是不当的，则其可以不采取行动。如果该监管实体确定所述行为是冒犯性或不当的，则该监管实体可以采取适当行动。例如，该监管实体可以警告该用户注意其行为，或者该监管实体可以中止该用户的签约，或者增加或添加监控以跟踪引起问题的用户的在线活动。

[0082] 可选地，如果确定存在有不当活动，则报告所述活动的用户可以受到奖赏。如果确定不存在不当活动，则报告所述活动的用户可以受到记过。通过这种方式，用户被鼓励报告不当活动，同时被阻止作出错误报告。

[0083] 图 6 是检测不当在线行为的另一实施例的流程图。流程在框 602 中开始，其中用户加入在线社区活动。例如，用户可以加入在线游戏活动，或者其可以进行在线虚拟现实会话或其它在线活动、比如SonyHome®环境。流程继续进行到框 604，其中该用户与该在线社区的其它成员交互。然后，流程继续进行到框 606，其中该用户意识到其它社区成员之一的不当活动。然后，流程继续进行到框 608，其中该用户按下应急按钮或者以其它方式指示已经观察到不当活动。然后，流程继续进行到框 610，其中该在线环境的不当活动的基于时间的历史记录被捕获并且被发送给监管实体。如前面所述的那样，所述基于时间的历史记录包括滑动窗口，所述滑动窗口记录在按下应急按钮以前以及按下应急按钮以后的活动。通过这种方式，在发生冒犯性行为时的在线活动被捕获并且被发送给该监管实体。可选地，报告不当活动的用户可以受到奖励，而作出错误报告的用户可以受到记过。

[0084] 图 7 是示出响应于不当活动而采取适当行动的方面的流程图。在一个实施例中，可以由网络实体、比如图 1 和 2 中的监管实体 108 或服务器 106 来采取所述行动。流程在框 702 中开始，其中对发生不当活动的指示、比如对应急按钮的按下被接收。然后，流程继续进行到框 704，其中该在线社区成员的活动的基于时间的历史记录被接收。然后，流程继续进行到框 706。在框 706 中，该在线社区成员的活动被评估。在框 708 中，在该在线社区的基于时间的历史记录中所记录的任何不当活动都被识别。然后，流程继续进行到框 710，其中采取适当行动。如果在框 708 中没有不当活动被识别出，则在框 710 中不采取行动。如果在框 708 中识别出不当活动，则在框 710 中采取适当行动。例如，可以给引起问题的用户发出警告，或者引起问题的用户可以被中止签约，或者可以存在对引起问题的用户的附加或增加的监控。可选地，报告不当活动的用户可以受到奖励，而作出错误报告的用户可以受到记过。

[0085] 图 8 是示出了使用社区监管来防止在线视频游戏中的作弊的实施例的流程图。在一个实施例中，可以由网络实体、比如图 1 和 2 中的监管实体 108 或服务器 106 来实现防止

在线视频游戏中的作弊。流程在框 802 中开始，其中在线游戏用户观察其它参与者之一的可疑的游戏活动。流程继续进行到框 804，其中观察可疑游戏活动的用户例如通过按下应急按钮、或者触发机构、或者其它类型的指示来指示其认为另外的玩家可能在作弊。然后，流程继续进行到框 806，其中该在线游戏成员的活动的基于时间的历史记录被捕获。所述基于时间的历史记录包括已经在按下应急按钮以前被存储的某个持续时间的游戏活动、以及在按下应急按钮之后的某个时间段的游戏活动。通过这种方式，环绕按下应急按钮的滑动时间窗口已经被记录。可以被包括在基于时间的历史记录中的活动的类型包括文字聊天、音频聊天、所有人物的状态、其位置、以及将会有助于重建该在线环境的任意其它数据。然后，流程继续进行到框 810。在框 810 中，该历史记录被发送给监管实体。在一个实施例中，对所观察到的不当行为的类型的可选指示也被包括在内。例如，如果玩家已经观察到有嫌疑的作弊玩家消失、具有异常的力量、或者对来自其它玩家的攻击有抵抗力，则所述信息可以被包括在内并且与基于时间的历史记录一起被发送。

[0086] 然后，流程继续进行到框 812。在框 812 中，该监管实体评估所述游戏参与者的在线行为。使用所述基于时间的历史记录，该监管实体可以回放导致按下应急按钮的场景。通过这种方式，可以确定是否有人进行作弊。在下列文献中描述有用于检测在线游戏中的作弊的各种技术：于 2006 年 3 月 20 日提交的名称为“Active Validation of Network Devices”的未决美国专利申请序列号 11/386,039；于 2006 年 5 月 1 日提交的名称为“Passive Validation of Network Devices”的序列号 11/415,881；于 2006 年 6 月 7 日提交的名称为“Game Metrics”的序列号 11/449,141；于 2007 年 3 月 16 日提交的名称为“Maintaining Community Integrity”序列号 11/725,175，所述全部专利申请的全部内容被并入本申请。

[0087] 在框 812 中评估在线行为以后，流程继续进行到框 814。在框 814 中，该监管实体可以基于所述不当行为的严重性采取适当行动。在一个实施例中，如果未检测到不当行为，则该监管实体将不采取行动。在其它实施例中，如果检测到不当行为，则该监管实体可以采取适当行动范围内的任何行动、包括警告、中止用户的签约、添加增加的监控、或者上述项的任意组合。可选地，报告作弊的用户可以受到奖励，而作出错误报告的用户可以受到记过。

[0088] 尽管图 3 至 7 描述了与不当在线活动、比如冒犯性语言相关联的实施例，但是所述相同的技术可以被用于防止在线游戏中的作弊。例如，在图 3A-C 中，替代用户检测冒犯性语言并且报告给监管实体，用户可以检测在线游戏环境中的有嫌疑的作弊，并且将其报告给监管实体，其中将采取适当行动。同样在图 4A-D 中，在基于客户端 / 服务器的体系结构中，服务器可以检测用户的有嫌疑的在线作弊，并且采取适当行动。同样在图 5 至 7 中，冒犯性或不当的行为可以是在线游戏环境中的作弊。

[0089] 图 9 是示出了监管在线行为的方面的流程图。在一个实施例中，图 9 的方面可以由图 1 和 2 中所示的监管实体或服务器来实施。流程在框 902 中开始，其中表示已经观察到不当行为（比如按钮已经被按下）的指示被接收。流程继续进行到框 904，其中在按钮被按下的时间左右的社区成员活动的基于时间的历史记录被接收。然后在框 906 中，社区成员的活动被评估以确定其是否为不当活动，不当活动可以包括不良或不当的语言、向其它在线用户散布或展示色情内容、在线游戏中的作弊等等。如果在框 906 中确定所述活动不

是不当的，则流程继续进行到框 910。在框 910 中，针对所述用户的投诉被记载在用户的文件中。该用户文件可以被维持以记录其它用户认为存在由该嫌疑用户执行的不当活动的指示的数目。

[0090] 然后，流程继续进行到框 912。在框 912 中，投诉的数目被与预先确定的值或阈值相比较。如果确定针对该用户的投诉数目未超过所述阈值水平，则流程继续进行而回到框 902，并且该系统等待对应急按钮的下次处理。回到框 912，如果确定投诉的数目超过所述阈值，则流程继续进行到框 914。由于投诉的数目已经超过所述阈值，因此认为可能存在一些不当的行为、或者至少由嫌疑用户实施的对该社区的其它成员而言为冒犯性的某些类型的行为。因此在框 914 中，可以采取适当行动。所述行动可以仅仅是警告或通知嫌疑用户该社区的其它成员认为其行为不可接受，或者所述行动可以更严厉、比如中止签约。另外，可以由于该社区的其它成员认为用户的行为为冒犯性的而对该用户进行增加的监控。回到框 906，如果确定该用户的活动不当，则流程继续进行到框 914，并且采取适当行动。再次地，所述行动的范围可以是从警告该用户其活动不当到中止签约再到添加增加的监控等等。

[0091] 然后，流程继续进行到框 916。在框 916 中，该用户的文件被更新，从而指示存在不当活动或已经采取行动。例如，该用户文件可以指示已经对该用户发出注意其活动的警告。当在 916 对同一用户采取之后的行动时，可以响应于以前采取的行动增加行动的严厉程度。

[0092] 如图 9 中所示，如果多个用户按下应急按钮，从而指示特定类型的活动对该社区的其它成员是不可接受的，则即使被监管实体当前用于评估不当行为的标准指示该行为不是不当的，仍然可以将针对特定类型的行为所记载的投诉的数目用于修改由该监管实体在评估行为时所使用的标准和规则集合。例如，如果特定类型的行为本来未被认为是不当的，但是如针对该活动的大量投诉所指示的那样，大多数其它在线用户认为特定活动是不当的，则监管实体可以修改其评估活动所对照的标准，并且将所述新活动设置成不当的。通过这种方式，随着社区随时间变化和发展，认为活动不当所依据的标准将随着该社区一起发展。

[0093] 图 10 是评估用户在线活动的另一实施例的流程图。在一个实施例中，图 10 的方面可以由图 1 和 2 中所示的监管实体或服务器来实施。流程在框 1002 中开始，其中表示已经发生不当活动、比如已经按下应急按钮的指示被接收。流程继续进行到框 1004，并且在按钮被按下的时间左右的社区成员活动的基于时间的历史记录被接收。所述基于时间的历史记录可以包括如下数据 :其用于重建在应急按钮被按下的时间左右的在线活动，使得监管者可以评估特定用户的在线活动是否不当。

[0094] 流程继续进行到框 1006，并且基于时间的历史记录被评估以获悉是否存在不当活动。如果不当活动超过阈值，则流程继续进行到框 1008。在框 1006 中，所述阈值可以被设置为使得第一次进行特定的不当活动时采取适当行动。例如，如果存在非法活动、比如色情或其它一些非法行为，则流程将继续进行到框 1008，其中由于所述活动的严重性而立即采取适当行动。除了采取适当行动，可以调整对特定用户的监控等级。例如，监控等级可以被增加，使得所述引起问题的特定用户的在线活动随时被监管实体监控。该用户的文件也被更新以指示其不当活动。

[0095] 监控等级的调整允许具有有限资源的系统更有效地跨社区成员分配那些资源。例

如，如果存在具有许多成员的大社区，则监管实体可以能够监控所有成员的在线活动。通过增加已经被识别成进行不当行为的所识别出的特定个体的监控等级，有限的系统资源可以被更加有效地使用。

[0096] 然后，流程继续进行到框 1002，并且在线活动继续被监控。回到框 1006，如果不当活动未超过阈值，则流程继续进行到框 1010。在框 1010 中，该成员的文件被评估以获悉是否存在针对该特定成员的以前的投诉。流程继续进行到框 1012，并且累计的不当活动被评估获悉其是否超过阈值。如果该特定成员的累计不当活动未超过所述阈值，则流程继续进行到框 1014。

[0097] 在框 1014 中，该用户的监控等级可以被调整。例如，监控等级可以被增加以更密切地监控该特定成员的活动。另外，该成员的文件被更新，以指示存在可能的不当行为。然后，流程继续进行到框 1002 并且继续监控是否存在对不当活动的指示、比如按下应急按钮。回到框 1012，如果累计的不当活动超过所述阈值，则流程继续进行到框 1016，并且该特定用户的监控等级将根据已经累计的实例的数目和严重性而被调整。例如，监控等级可以由于其它成员已经对该特定用户的活动进行投诉的实例数目而被增加。该成员的文件也被更新，并且流程继续进行到框 1002，其中继续监控网络活动。

[0098] 图 11 是测试环境的框图。例如，图 11 可以是用于测试在线游戏或其它在线应用的测试环境。如图 11 中所示，可以存在多个测试器 1102A、1102B、以及 1102C。在其它实施例中，可以存在任意所期望数目的测试器、例如一个、两个、或任意数目的测试器。这些在线测试器与网络 1104 和服务器 1106 通信。随着所述测试器交互和评估在线活动，他们将发现他们希望报告给该服务器以用于对该应用进行故障诊断和更新的缺陷和假信号。当所述测试器之一遇到假信号时，其可以触发指示、比如按下应急按钮，这将记录按下应急按钮的时间左右的持续时间内的在线环境。例如，该持续时间可以从按下按钮以前延长到按下该按钮以后达所期望的时间段为止。通过这种方式，该在线环境可以被捕获以对假信号的原因进行评估。

[0099] 在图 11 的另一实施例中，测试器与网络 1104 通信。网络 1104 可以是局域网、广域网（比如因特网）、或者其它类型的网络。与该网络通信的还有其它网络实体。例如，服务器 1106、或者监管实体 1108、或者其它网络实体的任意组合可以与网络 1104 通信。在一个实施例中，测试器 1102a 包括网络接口 1110、处理器 1112、以及触发机构 1114（比如应急按钮）。在一个实施例中，当触发机构 1114 被激活时，所述触发机构可以被按下并且处理器 1112 捕获活动（比如游戏活动）的基于时间的历史记录。基于时间的历史记录可以通过网络接口 1110 被传递给另外的网络实体。例如，基于时间的历史记录可以被传递给服务器 1106、或者监管实体 1108、或者其它网络实体。

[0100] 在一个实施例中，随着测试器交互并且评估该应用、比如在线游戏、非在线游戏、或者其它应用，所述测试器将发现他们希望报告给该服务器以用于对该应用进行故障诊断和更新的缺陷和假信号。当所述测试器遇到假信号时，其可以触发机构、比如按下应急按钮，以提供对所述假信号的指示。对测试环境的基于时间的历史记录在激活触发机构的时间左右的持续时间内被记录。例如，该持续时间可以从激活触发机构以前延长到激活触发机构以后的某个时间段为止。通过这种方式，活动和该应用的参数可以被捕获以对假信号的原因进行评估。

[0101] 图 12A 是图 11 中所示的在线测试环境的流程图。流程在框 1202 中开始，其中测试器进行对在线环境或应用的测试。流程继续进行到框 1204，其中测试器在测试期间识别出感兴趣的实例。例如，所述测试器可能识别出应用中的其希望报告的假信号或某种不连续性。流程继续进行到框 1206，其中所述测试器在感兴趣的时刻按下应急按钮。然后，流程继续进行到框 1208，其中该在线环境在测试活动期间的基于时间的历史记录被捕获。在一个实施例中，所述基于时间的历史记录是滑动的存储窗口，该存储窗口在按下应急按钮以前开始、经过并直到按下应急按钮以后。然后，流程继续进行到框 1210，其中所述基于时间的历史记录被存储以用于对该应用进行评估和故障诊断。

[0102] 图 12B 是图 11 中所示的测试环境的另一实施例的流程图。流程在框 1212 中开始，其中测试器进行对应用的测试。例如，该应用可以是非在线游戏、在线游戏、或者其它应用。流程继续进行到框 1214，其中测试器在测试期间识别出感兴趣的实例。例如，所述测试器可能识别出应用中的其希望报告的假信号或某种不连续性。流程继续进行到框 1216，其中所述测试器激活触发机构。例如，所述测试器可以按下应急按钮、或者其它类型的机构，以指示感兴趣的时刻。然后，流程继续进行到框 1218，其中该在线环境在测试活动期间的基于时间的历史记录被捕获。在一个实施例中，所述基于时间的历史记录是滑动的存储窗口，其在激活触发机构以前开始、经过并直到激活触发机构以后。然后，流程继续进行到框 1220，其中所述基于时间的历史记录被评估。在一个实施例中，所述基于时间的历史记录通过局域网被传递给服务器。在另一实施例中，所述基于时间的历史记录通过广域网（比如因特网）被传递给服务器。在一个实施例中，所述基于时间的历史记录被用于对该应用进行故障诊断。

[0103] 图 13 是示出了可以由于用户的不当行为而对用户采取的可能行动的例子的表。图 13 中所示的表具有：第一列 1302，其列出不同类型的不当行为；以及第二列 1304，其列出可以对每种类型的行为采取的不同的可能行动。例如，第一种不当行为 1306 是超出预先确定的社区标准的范围的行为。这种行为的例子可以是使用不良语言、种族或人种歧视、手势类型、以及其它类型的已经被该社区识别为不可接受的行为。可以响应于这些类型的行为而采取的可能行动 1308 的例子包括：发出警告、中止语音消息收发能力、中止用户对该在线活动的签约、增加对引起问题的用户的监控、约束对该在线活动的一部分的访问（比如约束对儿童倾向于访问的在线环境的部分的访问）等等。

[0104] 图 13 中所列出的第二种不当行为 1310 是在线游戏中的作弊。可以响应于在线游戏中的作弊而采取的可能行动 1312 的例子包括：发出警告、降低玩家在该游戏中的能力、惩罚该玩家（比如降低其分数）、约束玩家对游戏选项的访问（比如不让玩家使用特定的游戏选项）、中止该玩家对该在线游戏的签约、增加对作弊者的监控等等。

[0105] 图 13 中所列出的第三种行为 1314 是可疑行为。这种行为包括如下行为：其可能不违反社区标准，但是该社区的许多成员可能对该行为投诉。这种行为的例子可以包括贬损性语言、或者有嫌疑的、有疑问的行为。可以响应于可疑行为而采取的可能行动 1316 的例子包括：发出警告、增加对所述用户的监控等等。

[0106] 图 13 中所列出的第四种不当行为 1318 是非法活动。这种活动的例子包括对在线的儿童显示色情内容。可以响应于非法在线活动而采取的可能行动 1320 的例子包括：中止所述玩家对该在线游戏的签约、向合适当局报告所述活动、增加对作弊者的监控等等。

[0107] 图 14 是示出了可以结合在此所示各个实施例使用的示例性的支持网络的设备 1450 的框图。支持网络的设备 650 可以包括一个或多个处理器、比如处理器 1452。可以提供附加的处理器、比如 :用于管理输入 / 输出的辅助处理器、用于执行浮点数学运算的辅助处理器、具有适于快速执行信号处理算法的体系结构的专用微处理器 (比如数字信号处理器)、从属于主处理系统的从处理器 (比如后端处理器)、用于双或多处理器系统的附加的微处理器或控制器、或者例如在要实施并行处理的情况下的协处理器。这样的辅助处理器或协处理器可以是分立的处理器,或者与处理器 1452 相集成。

[0108] 处理器 1452 可以连接到通信总线 1454。通信总线 1454 可以包括用于促进计算机系统 1450 的存储设备与其它外围部件之间的信息传送的数据通道。通信总线 1454 可以进一步提供用于与处理器 1452 之间的通信的信号集、包括数据总线、地址总线、以及控制总线 (未示出)。通信总线 1454 可以包括任意的标准和非标准总线体系结构、比如符合下列标准的总线体系结构 :工业标准体系结构 (“ISA”)、扩展工业标准体系结构 (“EISA”)、微通道体系结构 (“MCA”)、外围部件互连 (“PCI”) 局部总线、或者由电气电子工程师协会 (“IEEE”) 发布的标准、包括 IEEE 488 通用接口总线 (“GPIB”)、IEEE 690/S-100 等等。

[0109] 支持网络的设备 1450 还可以包括主存储器 1456 并且还可以包括辅助存储器 1458。主存储器 148 可以提供缓冲器以存储在线会话期间的在线活动。例如,该缓冲器可以提供存储在线会话中的用户的在线活动的滑动存储窗口。所存储的在线会话的持续时间可以被预先确定、由用户来设置、在程序控制下或者由其它技术来调整。主存储器 1456 还可以提供对处理器 1452 上所执行的程序的指令和数据的存储。主存储器 1456 通常是基于半导体的存储器、比如动态随机存取存储器 (“DRAM”)、和 / 或静态随机存取存储器 (“SRAM”)。其它的基于半导体的存储器类型例如包括 :同步动态随机存取存储器 (“SDRAM”)、Rambus 动态随机存取存储器 (“RDRAM”)、铁电随机存取存储器 (“FRAM”) 等等、包括只读存储器 (“ROM”)。

[0110] 辅助存储器 1458 可以可选地包括硬盘驱动器 1460 和 / 或可移动存储驱动器 1462、例如软盘驱动器、磁带驱动器、光盘 (“CD”) 驱动器、数字多用光盘 (“DVD”) 驱动器、记忆棒 (memory stick) 等等。可移动存储驱动器 1462 以公知的方式从可移动存储介质 1464 读取和 / 或写入可移动存储介质 1464。可移动存储介质 1464 例如可以是 CD、DVD、闪存驱动器、记忆棒等等。

[0111] 可移动存储介质 1464 通常是上面存储有计算机可执行代码 (即软件) 和 / 或数据的计算机可读介质。存储在可移动存储介质 1464 上的计算机软件或数据可以作为电通信信号 1478 被读入到计算机系统 1450 中。

[0112] 在可替代的实施例中,辅助存储器 1458 可以包括其它类似的用于允许将计算机程序或者其它数据或指令加载到计算机系统 1450 中的装置。这样的装置例如可以包括外部存储介质 1472 和接口 1470。外部存储介质 1472 的例子例如可以包括外部硬盘驱动器、或者外部光驱动器、或者外部磁光驱动器。

[0113] 辅助存储器 1458 的其它例子可以包括基于半导体的存储器、比如可编程只读存储器 (“PROM”)、可擦除可编程只读存储器 (“EPROM”)、电可擦除只读存储器 (“EEPROM”)、或者闪存 (类似于 EEPROM 的面向块的存储器)。还包括有任意其它可移动存储单元 1472 和接口 1470,其允许将软件和数据从可移动存储单元 1472 传送到支持网络的设备 1450。

[0114] 支持网络的设备 1450 还可以包括通信接口 1474。通信接口 1474 允许在支持网络的设备 450 与外部设备、网络、或者信息源之间传送软件和数据。例如，计算机软件或可执行代码可以通过通信接口 1474 从网络实体传送到支持网络的设备 1450。另外，通信接口 1474 可以建立和维持到外部网络（比如因特网）的有线和无线通信二者。通信接口 1474 的例子举几个例子来说包括调制解调器、网络接口卡（“NIC”）、通信端口、PCMCIA 插槽和卡、红外接口、IEEE 1394 火线、无线 LAN、IEEE 802.11 接口、IEEE 802.16 接口、蓝牙接口、网状网络接口。

[0115] 通信接口 1474 通常可以实施工业发布的协议标准、比如以太网 IEEE 802 标准、光纤通道、数字用户线（“DSL”）、异步数字用户线（“ADSL”）、帧中继、异步传输模式（“ATM”）、集成数字服务网络（“ISDN”）、个人通信服务（“PCS”）、传输控制协议 / 因特网协议（“TCP/IP”）、串行线路因特网协议 / 点对点协议（“SLIP/PPP”）等等，但是也可以实施定制的或非标准的接口协议。

[0116] 通过通信接口 1474 所传送的软件和数据一般为电通信信号 1478 的形式。这些信号 1478 可以通过通信通道 1480 被提供给通信接口 1474。通信通道 1480 承载信号 1478 并且可以使用多种有线或无线通信装置而被实施、所述通信装置举几个例子来说包括 :导线或电缆、光纤、常规电话线、蜂窝电话链路、无线数据通信链路、射频 (RF) 链路、或者红外链路。

[0117] 计算机可执行代码（即计算机程序或软件）可以被存储在主存储器 1456 和 / 或辅助存储器 1458 中。计算机程序还可以通过通信接口 1474 被接收并且被存储在主存储器 1456 和 / 或辅助存储器 1458 中。这样的计算机程序在被执行时可以使得计算机系统 1450 能够执行本发明的前面所述的各个功能。

[0118] 在本说明书中，术语“计算机可读介质”用于指被用于存储数据和 / 或给支持网络的设备 1450 提供计算机可执行代码（例如软件和计算机程序）的任意介质。这些介质的例子包括 :主存储器 1456、辅助存储器 1458（包括硬盘驱动器 1460、可移动存储介质 1464、以及外部存储介质 1472）、以及与通信接口 1474 通信地耦合的任何外围设备（包括其它网络设备）。这些计算机可读介质是用于提供可执行代码、编程指令、以及软件、或者将数据存储和 / 或记录到支持网络的设备 1450 的装置。

[0119] 支持网络的设备 1450 还包括触发机构 1476。所述触发机构可以被用户激活以指示事件的发生。例如，如果用户观察到另外的在线用户的不当行为，则触发机构可以被激活。触发机构的激活可以导致支持网络的设备的各种操作。例如，如果用户激活触发机构，则在线会话的基于时间的历史记录可以被存储。在一个实施例中，触发机构是应急按钮。

[0120] 在一个实施例中，图 15 是示出了可以结合在此所示各个实施例使用的示例性游戏作弊监控实体的框图。如图 15 所示，游戏作弊监控实体 1500 包括网络接口 1502，所述网络接口 1502 接收存在作弊行为的指示。例如，在线游戏中的玩家可以发送表示在线游戏中的另外的玩家在作弊的指示。游戏作弊监控实体 1500 还包括处理器 1504，所述处理器 1504 收集至少嫌疑作弊玩家的游戏活动的游戏信息。在另一实施例中，游戏作弊监控实体 1500 收集该在线游戏会话中的所有玩家的游戏活动的游戏信息。所述游戏信息可以包括如下的时间段 :该时间段在接收指示之前延长达所期望的持续时间和在接收指示以后延长达所期望的持续时间。例如，在一个实施例中，游戏作弊监控实体可以是在玩家玩游戏时收集游戏

信息的游戏服务器。在另一实施例中，所述游戏作弊监控实体可以是单独的网络实体，或者可以与另外的网络实体一起被包括在内。在又一实施例中，作弊监控实体可以从另外的网络实体（比如游戏服务器、或者游戏中的玩家、或者其它来源）接收游戏信息。

[0121] 处理器 1504 使用所述游戏信息来重建游戏会话中的玩家的在线游戏活动，以确定是否存在所述玩家之中的一个或多个的作弊活动。如果存在一个或多个玩家的作弊，则游戏作弊监控实体可以采取适当行动。例如，游戏作弊监控实体可以约束已经被识别为“作弊者”的玩家访问该在线游戏会话或者其它游戏会话、或者限制已经被识别为作弊者的玩家的可用游戏选项、或者其它类型的行动。

[0122] 在另一实施例中，图 15 是可以分配资源、比如在线资源或其它网络资源的监管实体的框图。所述监管实体（亦称网络分配监管实体）可以是与网络（比如图 1-4 中所示的网络 104）通信的单独的实体，或者网络资源分配监管实体的操作可以被实施在另外的网络实体、（比如图 1 中所示的监管实体 108、服务器 106、用户 102、或者其它网络实体）中。如图 15 中所示，网络实体 1500 包括网络接口 1502。网络实体 1500 可以接收在线用户可能进行不当活动的指示。

[0123] 网络实体 1500 还包括如下处理器：其可以在指示被接收时捕获在线社区中的用户的在线活动的基于时间的历史记录。所述网络实体重建该在线社区的在线活动，并且确定是否曾存在所述在线用户之中的一个或多个的不当在线活动，并且如果存在不当活动，则分配在线资源以实现对引起问题的用户的监控的所希望等级。

[0124] 在另一实施例中，网络实体 1500 的功能可以被实施在其它实体中、或者通过若干网络实体而实施。例如，监管实体 108、或者服务器 106、或者用户 102 可以实施网络实体 1500 的操作。例如，监管实体可以接收对不当活动的指示并且捕获所述活动的基于时间的历史记录。然后，所述监管实体可以把对所期望的期望监控等级的指示发送给如下的网络实体：所述网络实体调整被分配用于监控引起问题的用户的网络资源的水平。

[0125] 图 16 是示出了检测在线环境中的作弊的实施例的流程图。流程在框 1602 中开始，并且在线游戏会话中的玩家检测另外的在线游戏玩家的有嫌疑的作弊行为。流程继续进行到框 1604，并且关于该在线游戏中的玩家的玩游戏活动的游戏信息被收集。所述游戏信息可以包括有嫌疑的作弊玩家、或者所有玩家、或者任意所期望数目的玩家的游戏活动。在一个实施例中，所述游戏信息包括在其期间发生有嫌疑的作弊行为的某时间段的游戏。所述游戏信息可以包括游戏玩家的行动。例如，他们移动到何处、他们多快地移动、他们是否看上去比通常情况具有更多能力或力量等等。

[0126] 然后，流程继续进行到框 1606。在框 1606 中，所述游戏信息被传递给游戏作弊监控实体。流程继续进行到框 1608，并且所述游戏作弊监控实体评估所述游戏信息以确定是否存在作弊活动。如果存在作弊活动，则所述游戏作弊监控实体可以采取适当行动。在一个实施例中，给观察到作弊行为并且将游戏信息传递给所述游戏作弊监控实体的游戏玩家提供奖励。也可以存在由玩家响应于检测到有嫌疑的作弊活动而激活的触发机构。

[0127] 在一个实施例中，捕获在线游戏会话的游戏信息包括：捕获在检测到有嫌疑的作弊行为以前发生达预先确定的时间量的在线游戏会话活动。在一个实施例中，捕获所述游戏信息包括：将在线游戏玩家的标识与该玩家的在线活动相关联。

[0128] 图 17 是示出了检测在线环境中的作弊的另一实施例的流程图。流程在框 1702 中

开始，其中表示如下内容的指示被接收：在线游戏会话中的玩家怀疑该游戏会话中的另外的玩家进行作弊行为。例如，游戏作弊监控实体可以接收该指示。流程继续进行到框 1704，其中所述游戏作弊监控实体收集有嫌疑的作弊行为的时间左右的游戏活动的游戏信息。例如，所述游戏作弊监控实体可以是游戏服务器并且收集游戏信息。在另一实施例中，所述游戏作弊监控实体接收所述游戏信息。例如，所述游戏作弊监控实体可以从游戏服务器、或者从该在线游戏的玩家、或者其它网络实体、或者实体的任意组合接收游戏信息。流程继续进行到框 1706，并且所述游戏作弊监控实体根据所述游戏信息重建所述游戏活动。

[0129] 流程继续进行到框 1708，并且所述游戏作弊监控实体评估该游戏中的玩家的活动以确定是否存在作弊行为。如果存在所述游戏玩家之中的一个或多个的作弊行为，则所述游戏作弊监控实体可以对作弊游戏玩家采取适当行动。适当活动的一个例子包括约束作弊游戏玩家对该在线游戏的访问。

[0130] 图 18 是可以分配资源、比如在线资源或其它网络资源的监管实体的另一实施例的框图。所述监管实体（亦称网络分配监管实体）可以是与网络（比如图 1-4 中所示的网络 104）通信的单独的实体，或者网络资源分配监管实体的操作可以被实施在另外的网络实体（比如图 1 中所示的监管实体 108、服务器 106、用户 102、或者其它网络实体）中。如图 18 中所示，网络实体 1800 包括网络接口 1802。网络接口 1800 可以接收在线用户可能进行不当活动的指示。

[0131] 网络实体 1800 还包括处理器 1804，所述处理器 1804 可以在指示被接收时捕获在线社区中的用户的在线活动的基于时间的历史记录。所述网络实体重建该在线社区的在线活动，并且确定是否曾存在所述在线用户之中的一个或多个的不当活动，并且如果存在不当活动，则分配在线资源以实现对引起问题的用户的监控的所希望等级。

[0132] 在另一实施例中，网络实体 180 的功能可以被实施在其它实体中、或者通过若干网络实体而实施。例如，监管实体 108、或者服务器 106、或者用户 102 可以实施网络实体 1800 的操作。例如，监管实体可以接收对不当活动的指示并且捕获所述活动的基于时间的历史记录。然后，所述监管实体可以发送对所期望的期望监控等级的指示，以调整被分配用于监控引起问题的用户的网络资源的水平。

[0133] 图 19 是示出了在线或其它网络资源分配的方面的流程图。流程在框 1902 中开始，并且在线用户可能进行不当行为的指示被接收。然后，流程继续进行到框 1904，并且包括所述用户的行为的在线会话的基于时间的历史记录被捕获。流程继续进行到框 1906，其中该会话的在线活动被重建。在框 1906 中确定是否存在引起问题的在线用户的不当活动。然后，流程继续进行到框 1908。在框 1908 中，针对引起问题的在线用户的监控的所希望等级分配在线资源。

[0134] 在一个实施例中，捕获在线会话的基于时间的历史记录包括：捕获在接收在线用户可能进行不当行为的指示以前发生达预先确定的时间量的在线游戏会话活动。在另一实施例中，捕获所述基于时间的历史记录包括：将在线用户标识与其在线活动相关联。

[0135] 在一个实施例中，针对引起问题的成员的监控的所希望等级分配在线资源包括：指派在线资源以跟踪引起问题的成员的活动。在一个实施例中，网络资源分配实体捕获基于时间的历史记录。在另一实施例中，监管实体捕获基于时间的历史记录，重建所述在线活动并且把引起问题的用户的监控的所期望等级传递给网络资源分配实体，所述网络资源分

配实体分配网络资源。在又一实施例中，所述基于时间的历史记录被从另外的网络实体接收。

[0136] 图 20 是示出了分配在线或其它网络资源的附加方面的流程图。流程在框 2002 中开始，触发机构被在线社区成员激活的指示被接收，其指示另外的在线社区成员的有嫌疑的不当行为。流程继续进行到框 2004，其中社区成员在线活动的基于时间的历史记录被接收。流程继续进行到框 2006，其中所述社区活动被根据所述基于时间的历史记录来重建。流程继续进行到框 2008，其中所述社区成员的活动被评估以确定是否存在不当行为，并且如果存在引起问题的社区成员的不当行为，则在线资源被分配，以监控已经被识别为进行不当行为的社区成员。

[0137] 还可以使用诸如下列部件主要以硬件来实施各个实施例：专用集成电路（“ASIC”）、或者现场可编程门阵列（“FPGA”）。能够执行在此所述功能的硬件状态机的实施方式对于相关领域的技术人员而言也将是显而易见的。还可以使用硬件和软件二者的组合来实施各个实施例。

[0138] 在此所使用的术语“模块”是指、但不限于：执行某些任务的软件或硬件部件、比如 FPGA 或 ASIC。模块可以被有利地配置为处于可寻址的存储介质上，并且被有利地配置为在一个或多个支持网络的设备或处理器上执行。因此，举例来说，模块可以包括部件、过程、功能、属性、进程、子例程、程序代码段、驱动器、固件、微码、电路、数据、数据库、数据结构、表、阵列、变量等等。所述部件和模块中所提供的功能可以被组合到更少的部件和模块中或者被进一步分离到附加的部件或模块中。附加地，所述部件和模块可以被有利地实施为在一个或多个支持网络的设备或计算机上执行。

[0139] 此外，本领域的技术人员能够理解，结合上述附图和在此公开的实施例所描述的各个说明性的逻辑块、模块、电路、以及方法步骤常常可以被实施成电子硬件、计算机软件、或者二者的组合。为了清楚地示出硬件与软件的互换性，各个说明性的部件、块、模块、电路、以及步骤通常已经在上面关于其功能予以描述。这样的功能是被实施成硬件还是软件取决于特定应用以及对整个系统施加的设计约束。技术人员可以以不同的方式针对每个特定的应用实施所述功能，但是这样的实施方式决策不应当被解释成导致偏离本发明的范围。另外，功能在模块、块、电路、或者步骤内的分组是为了易于说明。特定的功能或步骤可以在不偏离本发明的情况下从一个模块、块、或者电路中移动到另外的模块、块、或者电路中。

[0140] 此外，结合在此公开的实施例所描述的各个说明性的逻辑块、模块、以及方法可以利用下列项来实施或执行：被设计为执行在此所述的功能的通用处理器、数字信号处理器（“DSP”）、ASIC、FPGA 或其它可编程逻辑设备、分立门或晶体管逻辑、分立硬件部件、或者其任意组合。通用处理器可以是微处理器，但是可替代地，该处理器可以是任意的处理器、控制器、微控制器、或者状态机。处理器还可以被实施成计算设备的组合、例如 DSP 与微处理器的组合、多个微处理器、一个或多个结合 DSP 核的微处理器、或者任意其它这样的配置。

[0141] 附加地，结合在此公开的实施例所描述的方法或过程的步骤可以直接体现为硬件、由处理器执行的软件模块、或者二者的组合。软件模块可以处于 RAM 存储器、闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可移动盘、CD-ROM、或者任意其它形式的存储介（包括网络存储介质）中。示例性的存储介质可以耦合到处理器使得这样的处理

器可以从所述存储介质读取信息以及将信息写入所述存储介质。可替代地，所述存储介质可以是处理器的一部分。所述处理器和存储设备也可以处于 ASIC 中。

[0142] 尽管上面是对本发明优选实施例的完整描述，但是可以使用各个替代方案、修改方案、以及等价方案。因此，不应当参考上面的描述、而是相反应当参考所附权利要求书连同等效物的其全部范围来确定本发明范围。无论是否优选，在此所述的任何特征都可以与在此所述的任意其它特征相组合，而无论所述其它特征是否优选。因此，本发明不是旨在受限于在此所示的实施例，而是旨在被给予与在此所公开的主要特征和新颖性特征一致的最大范围。

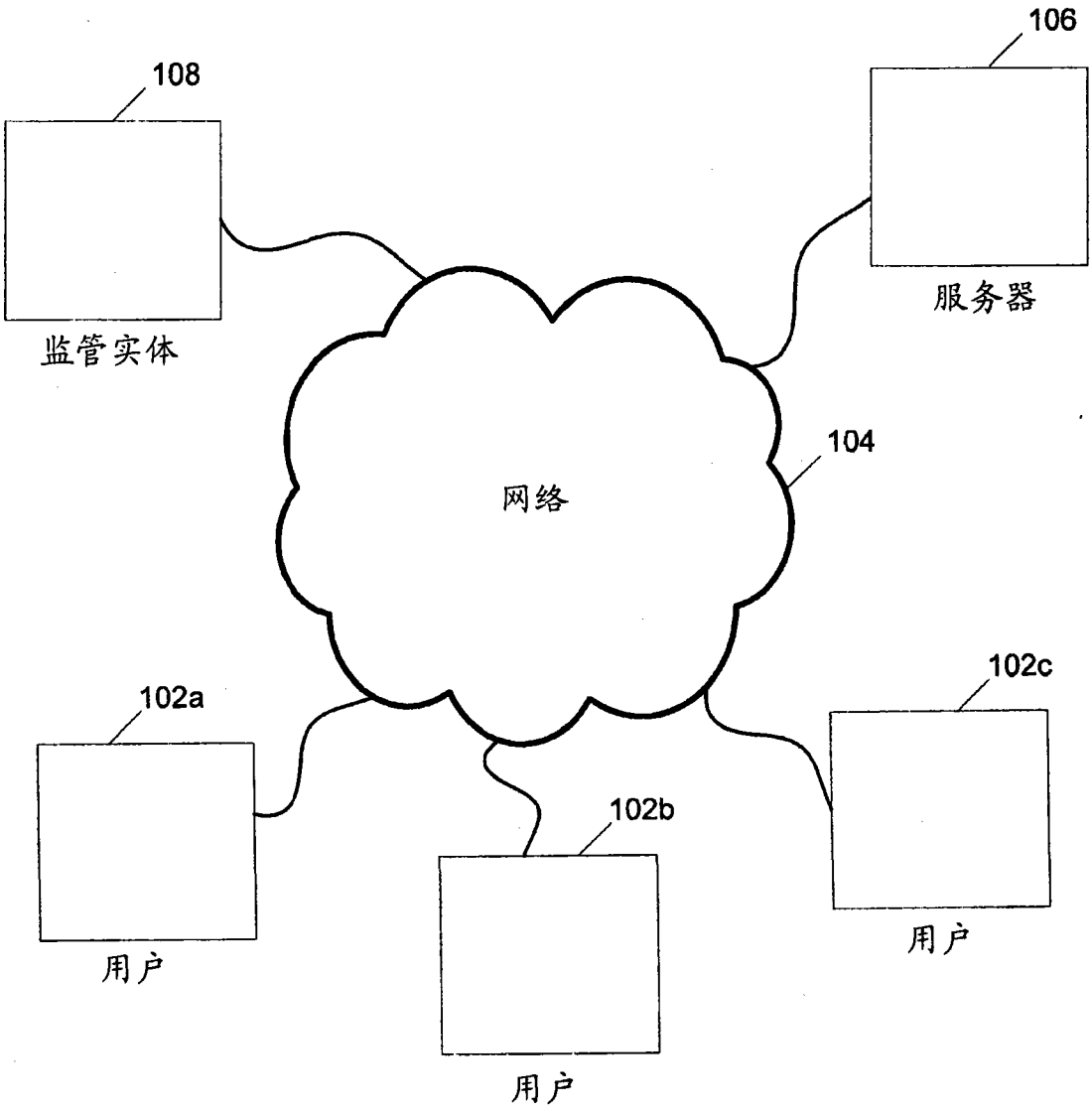


图 1

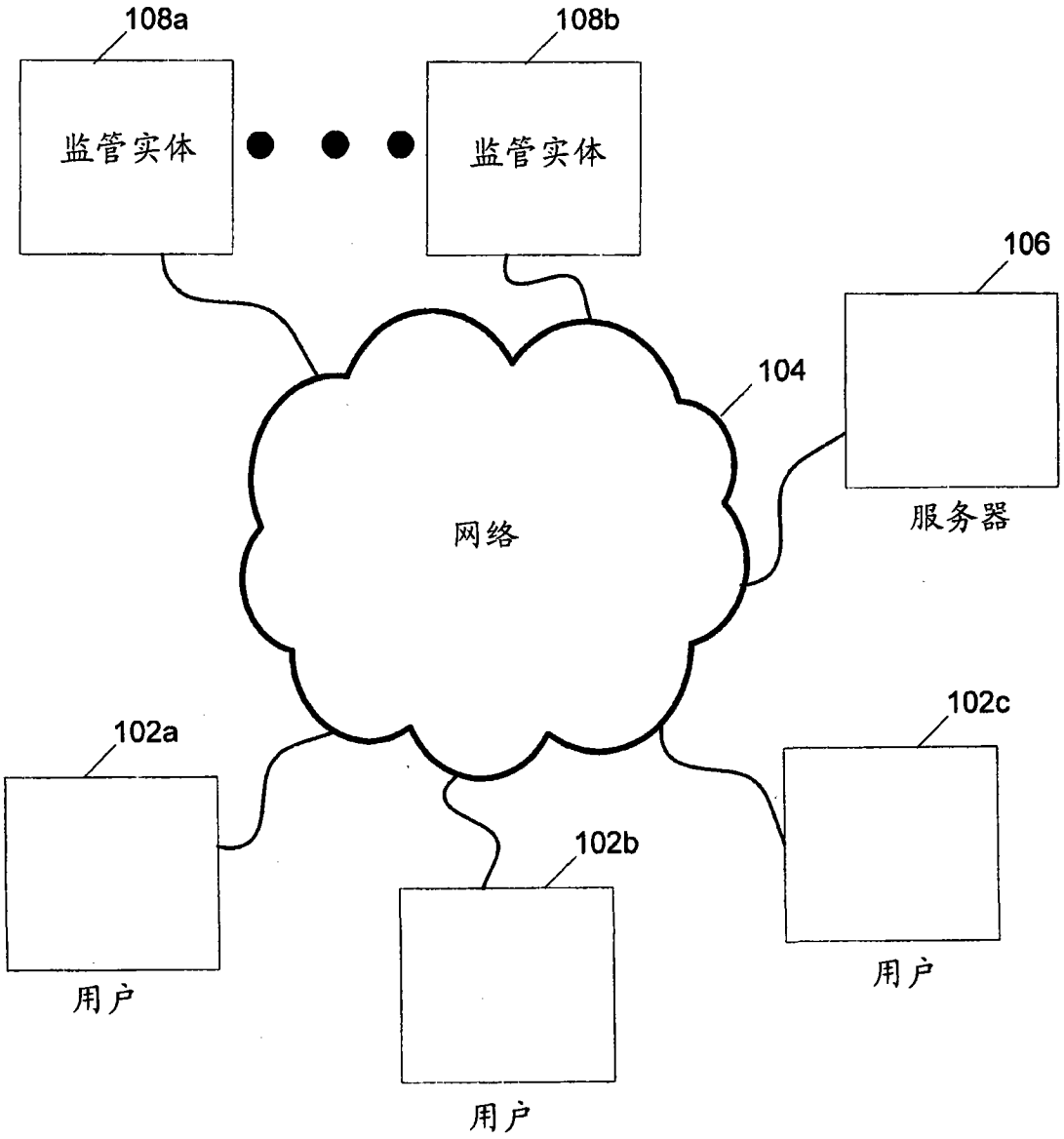


图 2

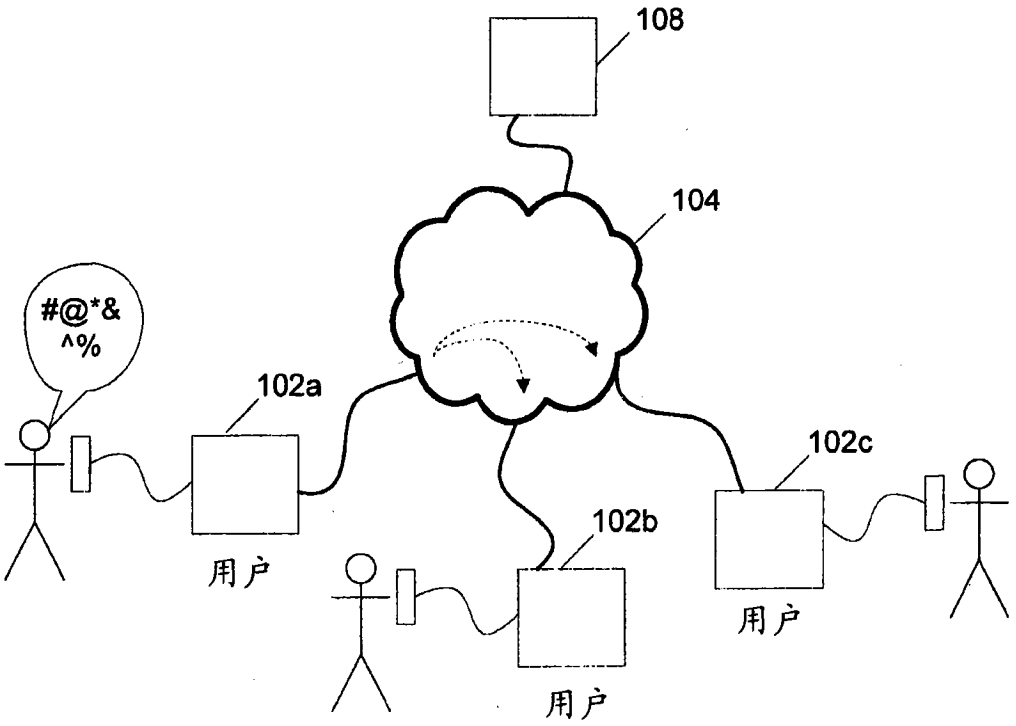


图 3A

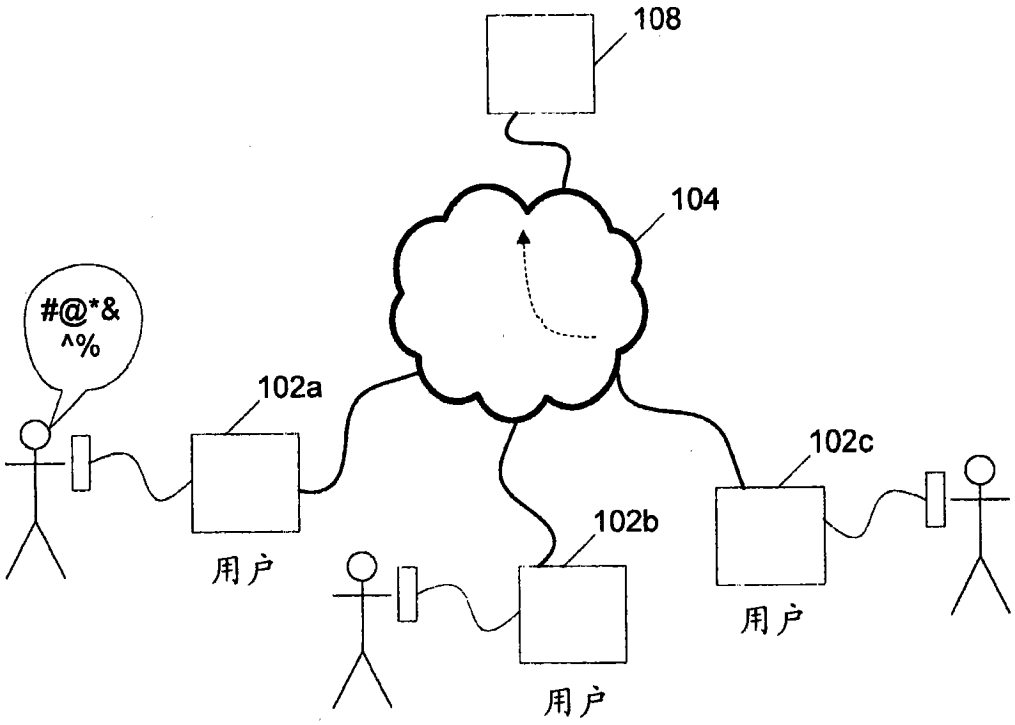


图 3B

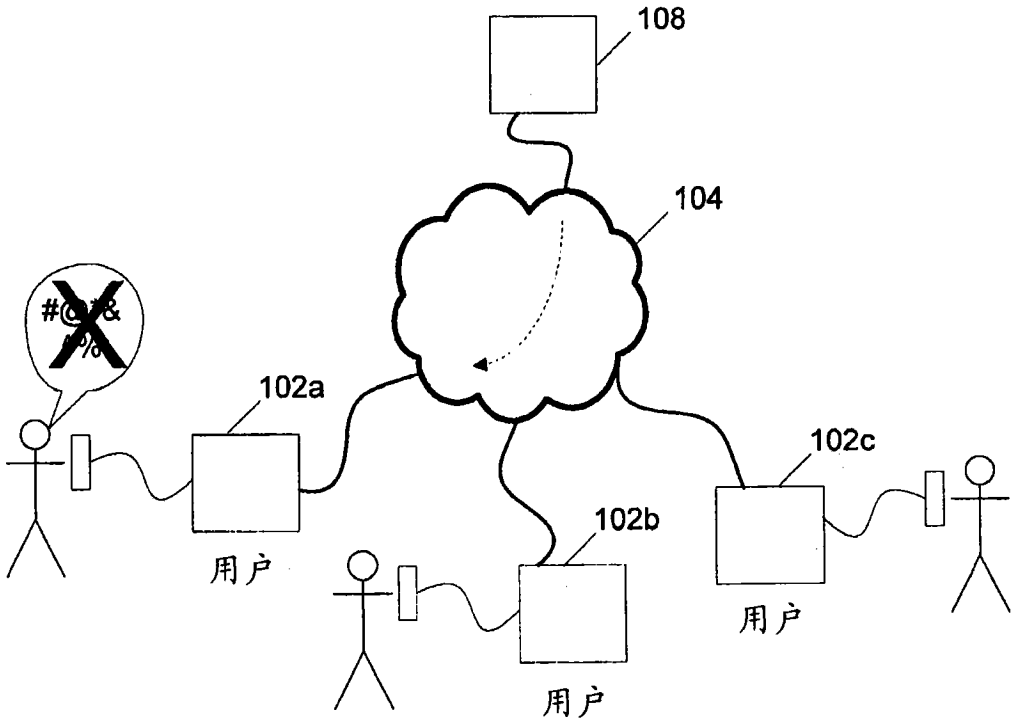

108
104
#@%&
102a
102c
102b
用户
用户
用户

图 3C

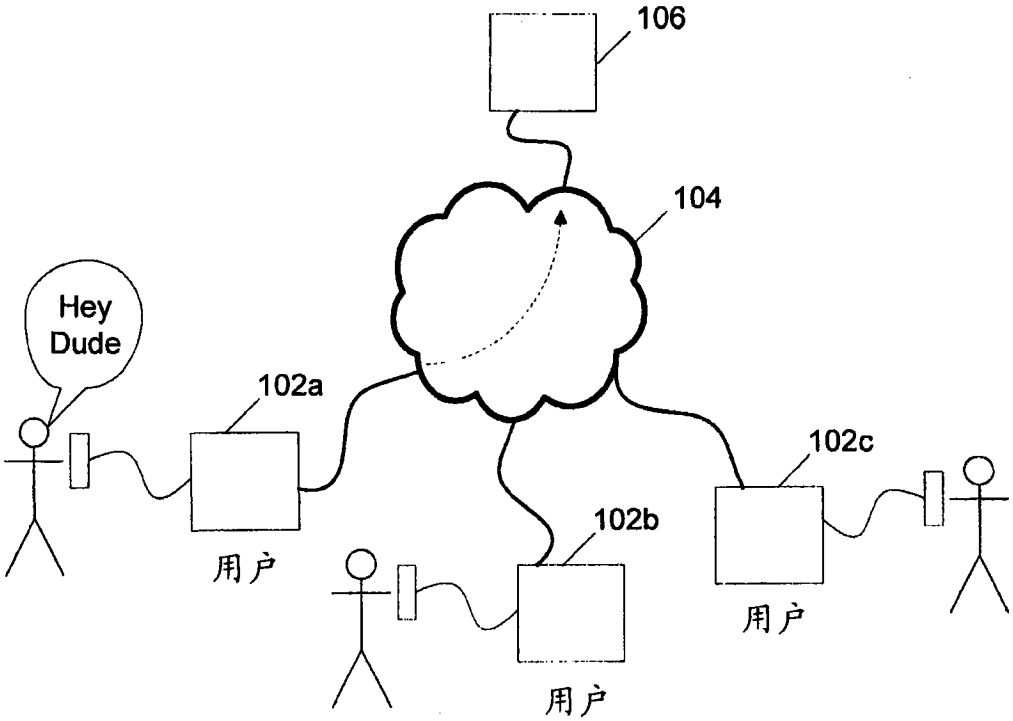

106
104
Hey
Dude
102a
102c
102b
用户
用户
用户

图 4A

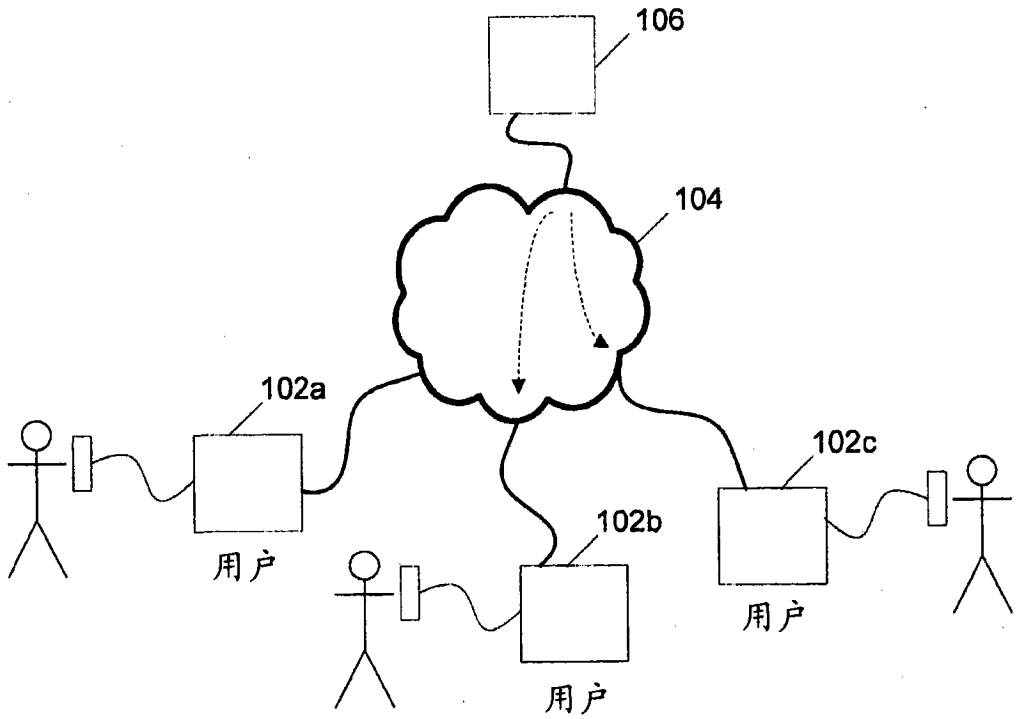


图 4B

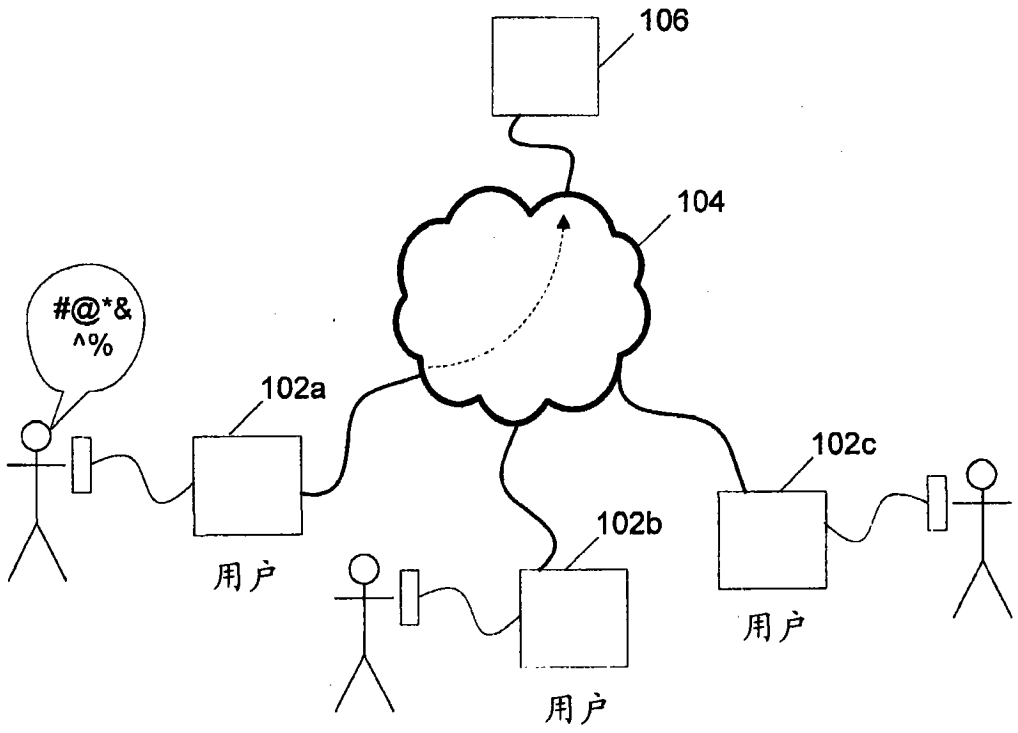


图 4C

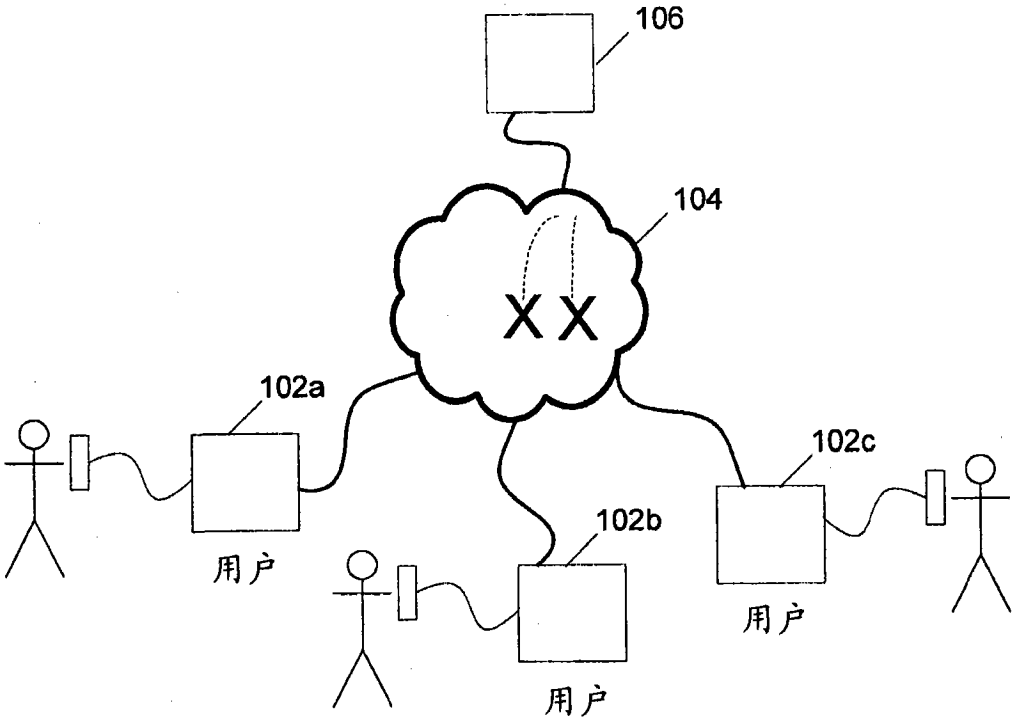


图 4D

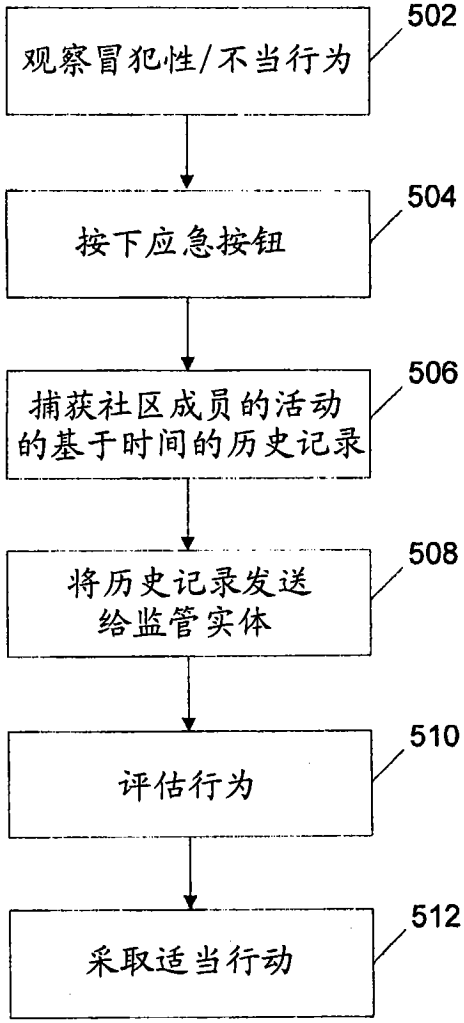

观察冒犯性/不当行为
502
按下应急按钮
504
捕获社区成员的活动的基于时间的历史记录
506
将历史记录发送给监管实体
508
评估行为
510
采取适当行动
512

图 5

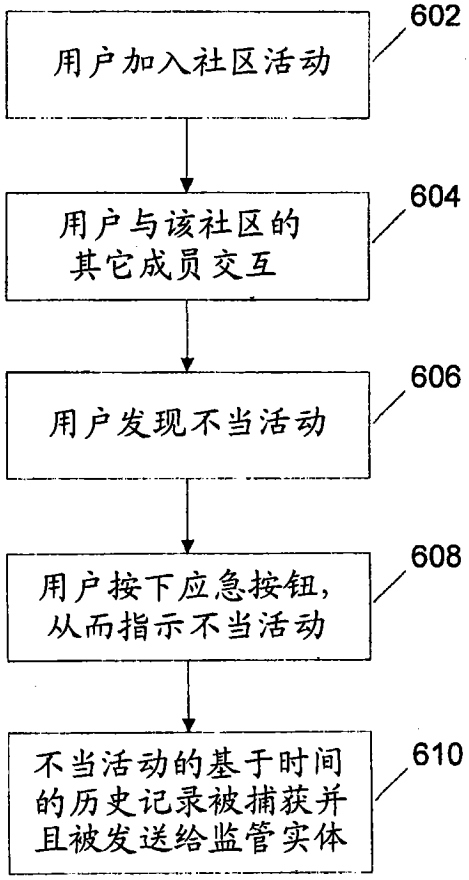

用户加入社区活动
602
用户与该社区的其它成员交互
604
用户发现不当活动
606
用户按下应急按钮，从而指示不当活动
608
不当活动的基于时间的历史记录被捕获并且被发送给监管实体
610

图 6

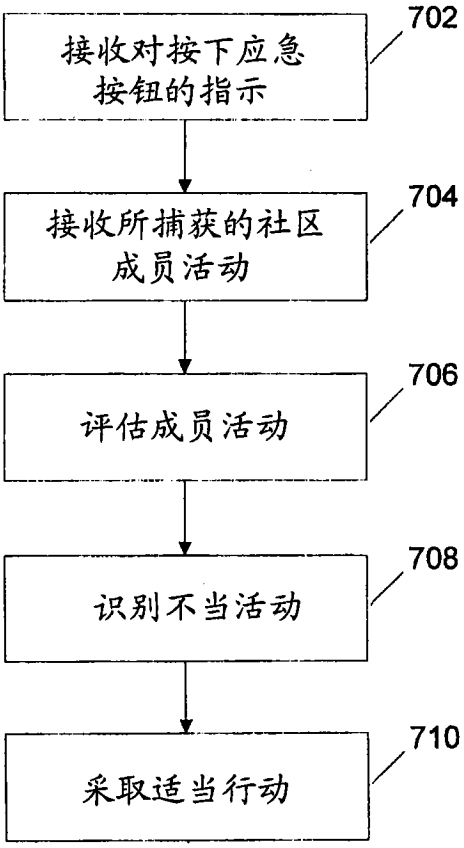

接收对按下应急按钮的指示
702
接收所捕获的社区成员活动
704
评估成员活动
706
识别不当活动
708
采取适当行动
710

图 7

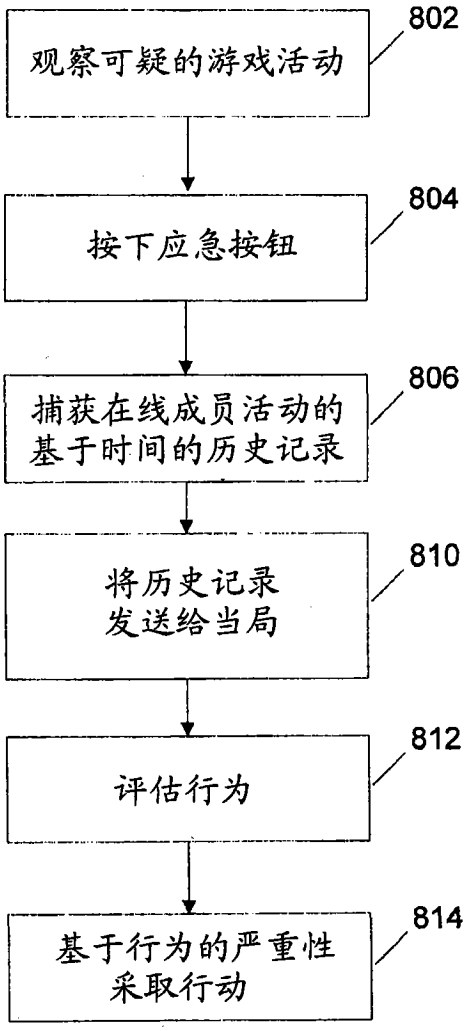

观察可疑的游戏活动
802
按下应急按钮
804
捕获在线成员活动的基于时间的历史记录
806
将历史记录发送给当局
810
评估行为
812
基于行为的严重性采取行动
814

图 8

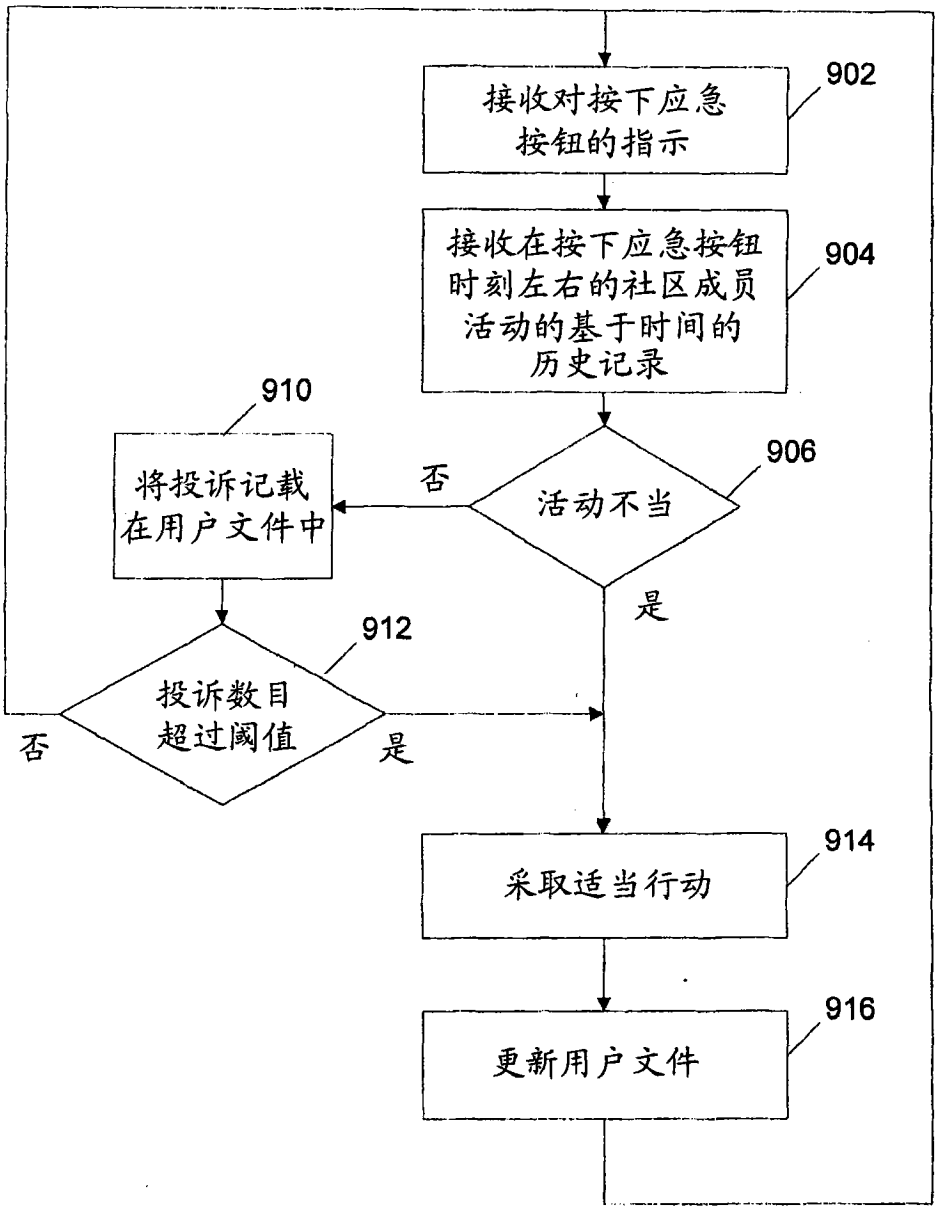

接收对按下应急按钮的指示
902
接收在按下应急按钮时刻左右的社区成员活动的基于时间的历史记录
904
活动不当
906
否
将投诉记载在用户文件中
910
是
投诉数目超过阈值
912
否
是
采取适当行动
914
更新用户文件
916

图 9

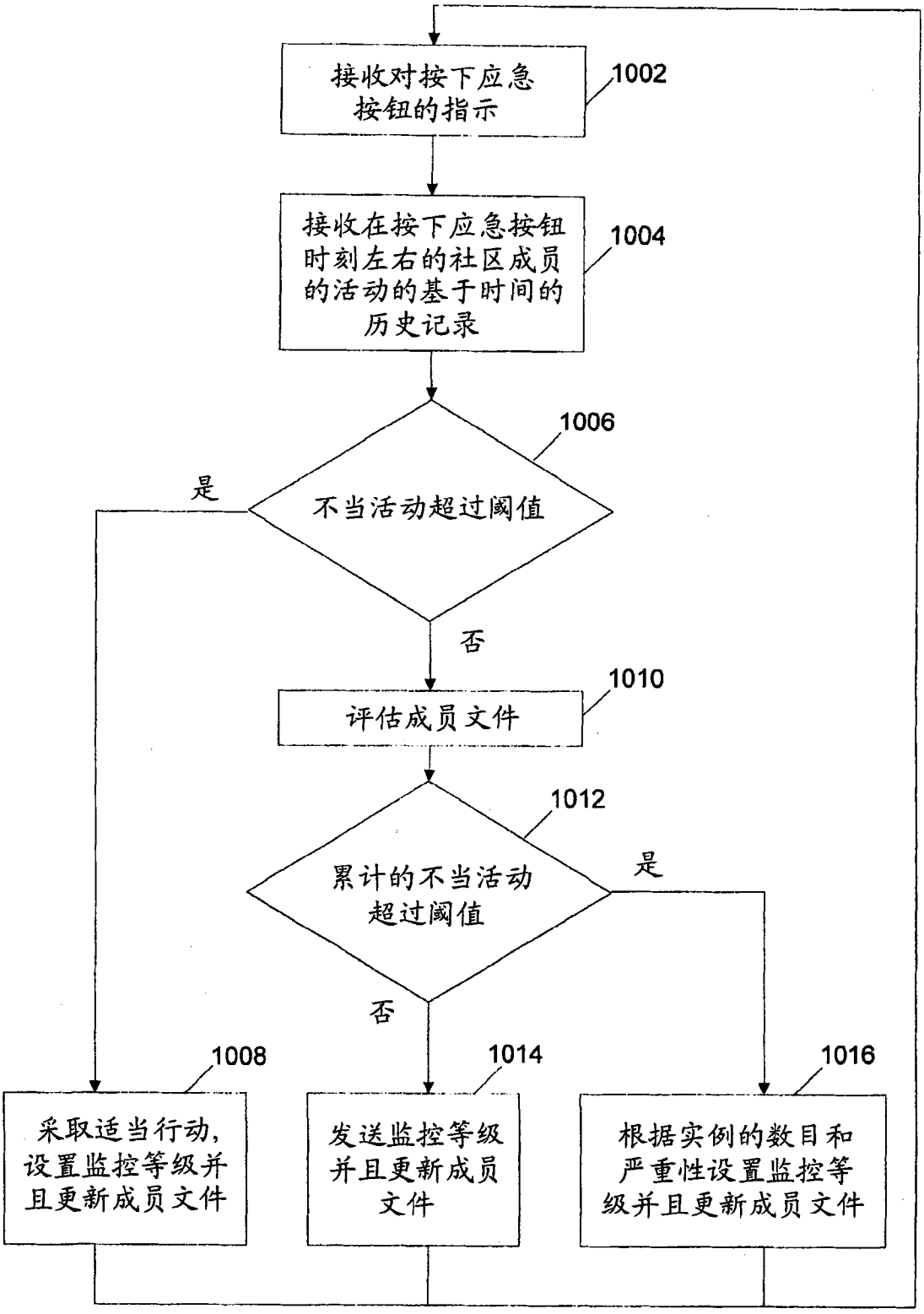

接收对按下应急按钮的指示
1002
接收在按下应急按钮时刻左右的社区成员的活动的基于时间的历史记录
1004
1006
不当活动超过阈值
是
否
1010
评估成员文件
1012
累计的不当活动超过阈值
是
否
1008
采取适当行动，设置监控等级并且更新成员文件
1014
发送监控等级并且更新成员文件
1016
根据实例的数目和严重性设置监控等级并且更新成员文件

图 10

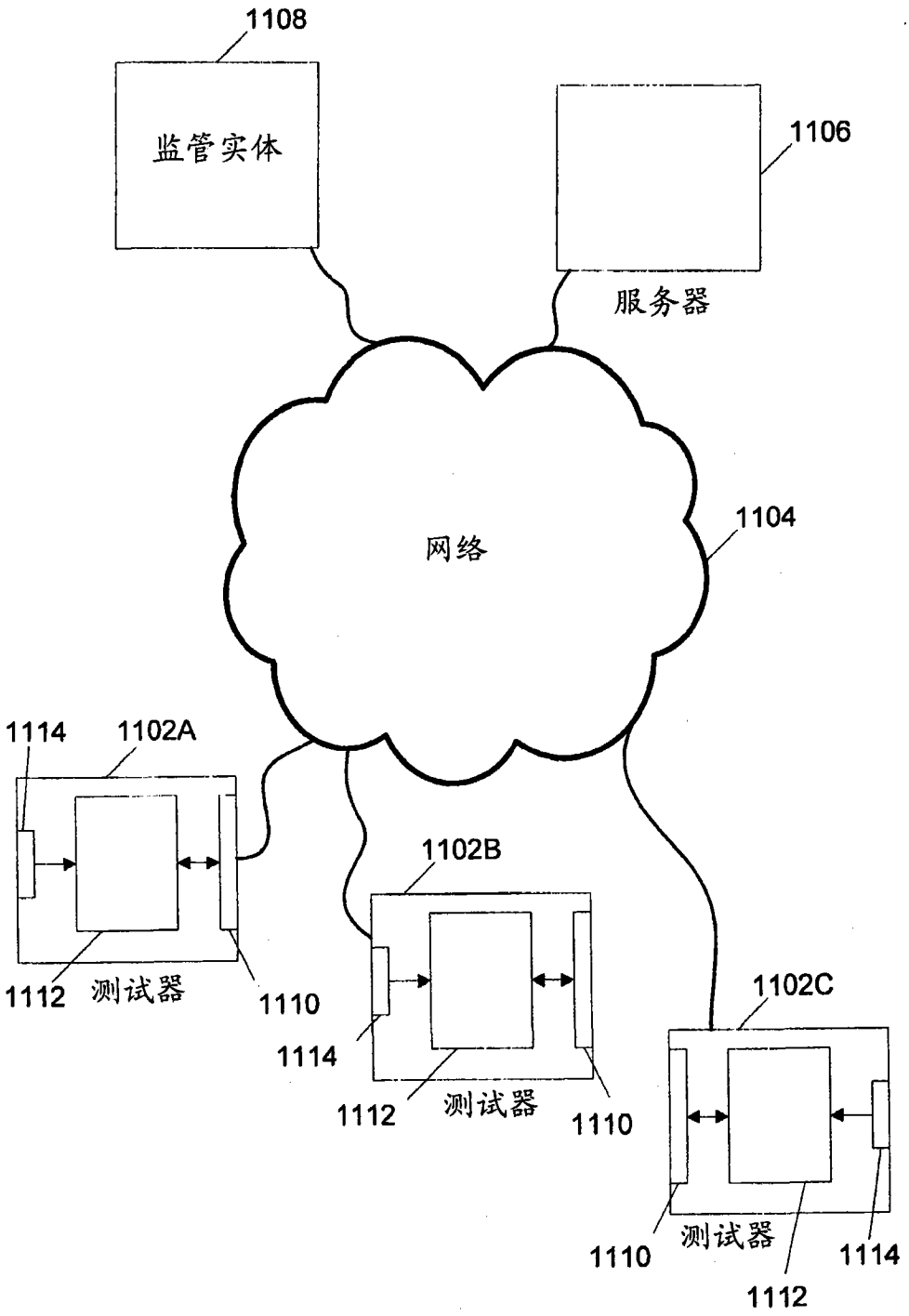

1108
监管实体
1106
服务器
网络
1104
1114
1102A
1112
测试器
1110
1102B
1114
1112
测试器
1110
1102C
1110
测试器
1114
1112

图 11

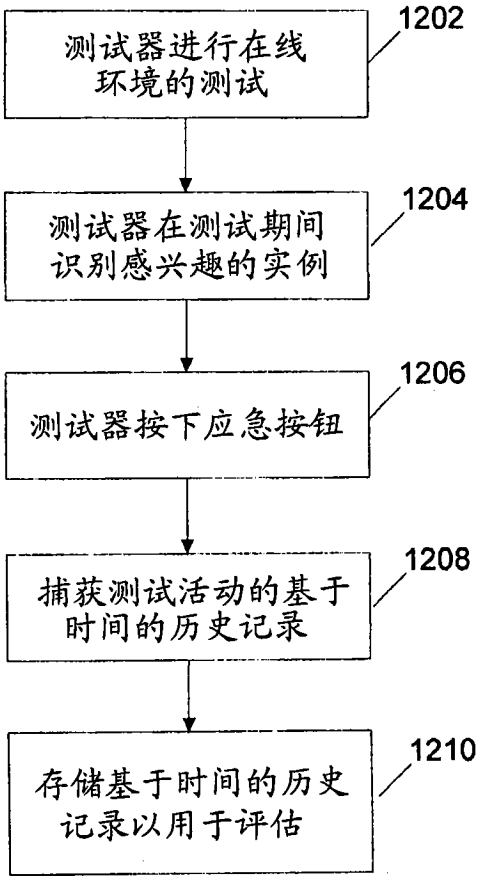

测试器进行在线环境的测试
1202
测试器在测试期间识别感兴趣的实例
1204
测试器按下应急按钮
1206
捕获测试活动的基于时间的历史记录
1208
存储基于时间的历史记录以用于评估
1210

图 12A

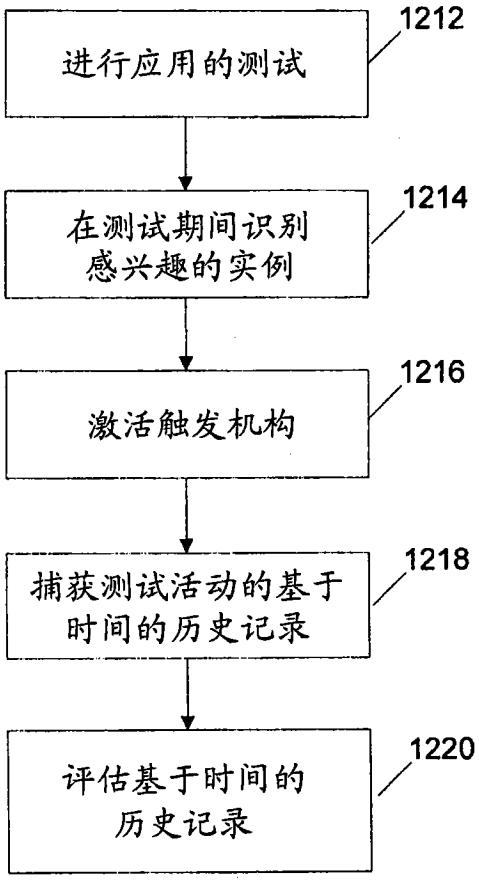
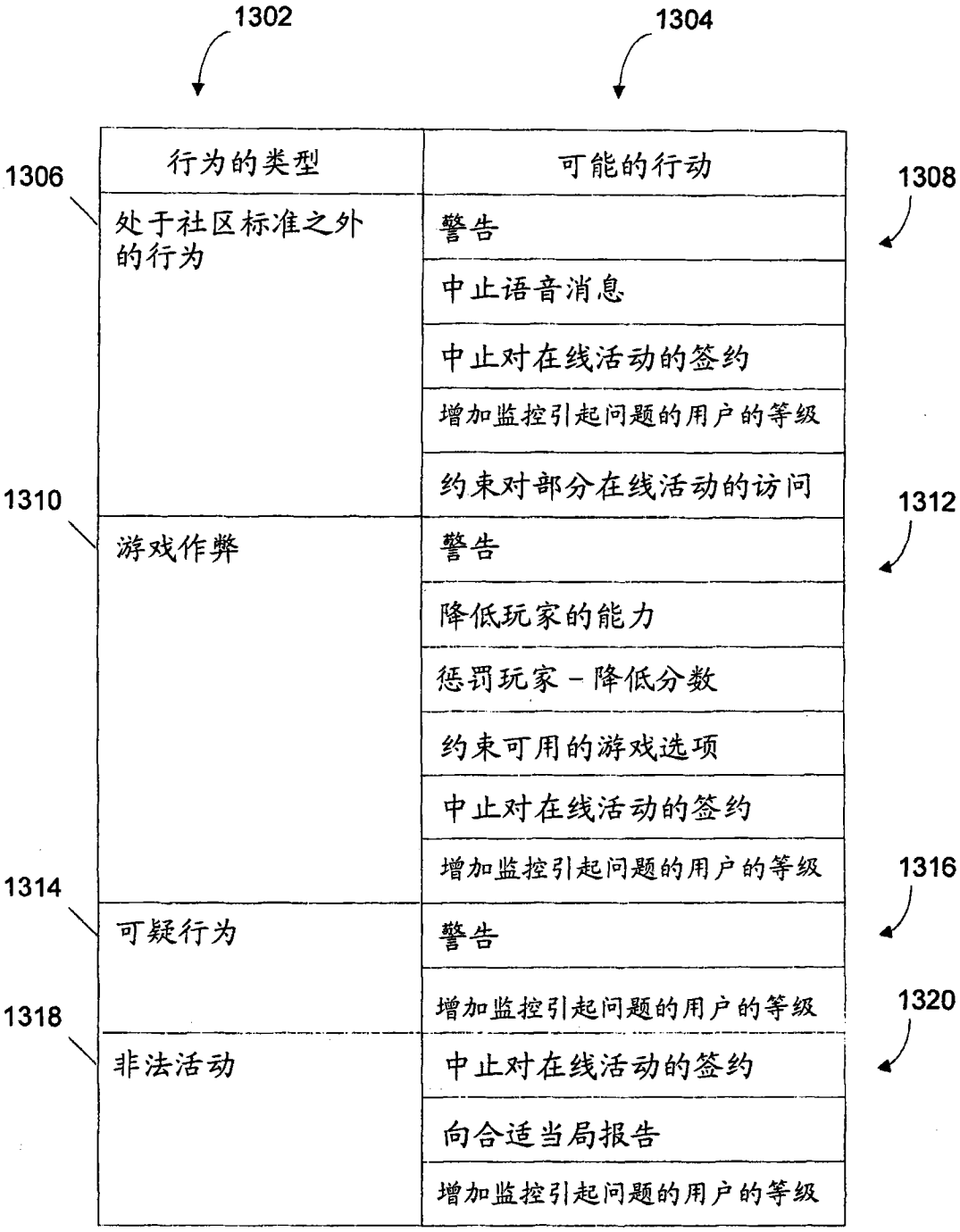

进行应用的测试
1212
在测试期间识别感兴趣的实例
1214
激活触发机构
1216
捕获测试活动的基于时间的历史记录
1218
评估基于时间的历史记录
1220

图 12B



行为的类型	可能的行动
处于社区标准之外的行为	警告
	中止语音消息
	中止对在线活动的签约
	增加监控引起问题的用户的等级
	约束对部分在线活动的访问
游戏作弊	警告
	降低玩家的能力
	惩罚玩家 - 降低分数
	约束可用的游戏选项
	中止对在线活动的签约
	增加监控引起问题的用户的等级
可疑行为	警告
	增加监控引起问题的用户的等级
非法活动	中止对在线活动的签约
	向合适当局报告
	增加监控引起问题的用户的等级

图 13

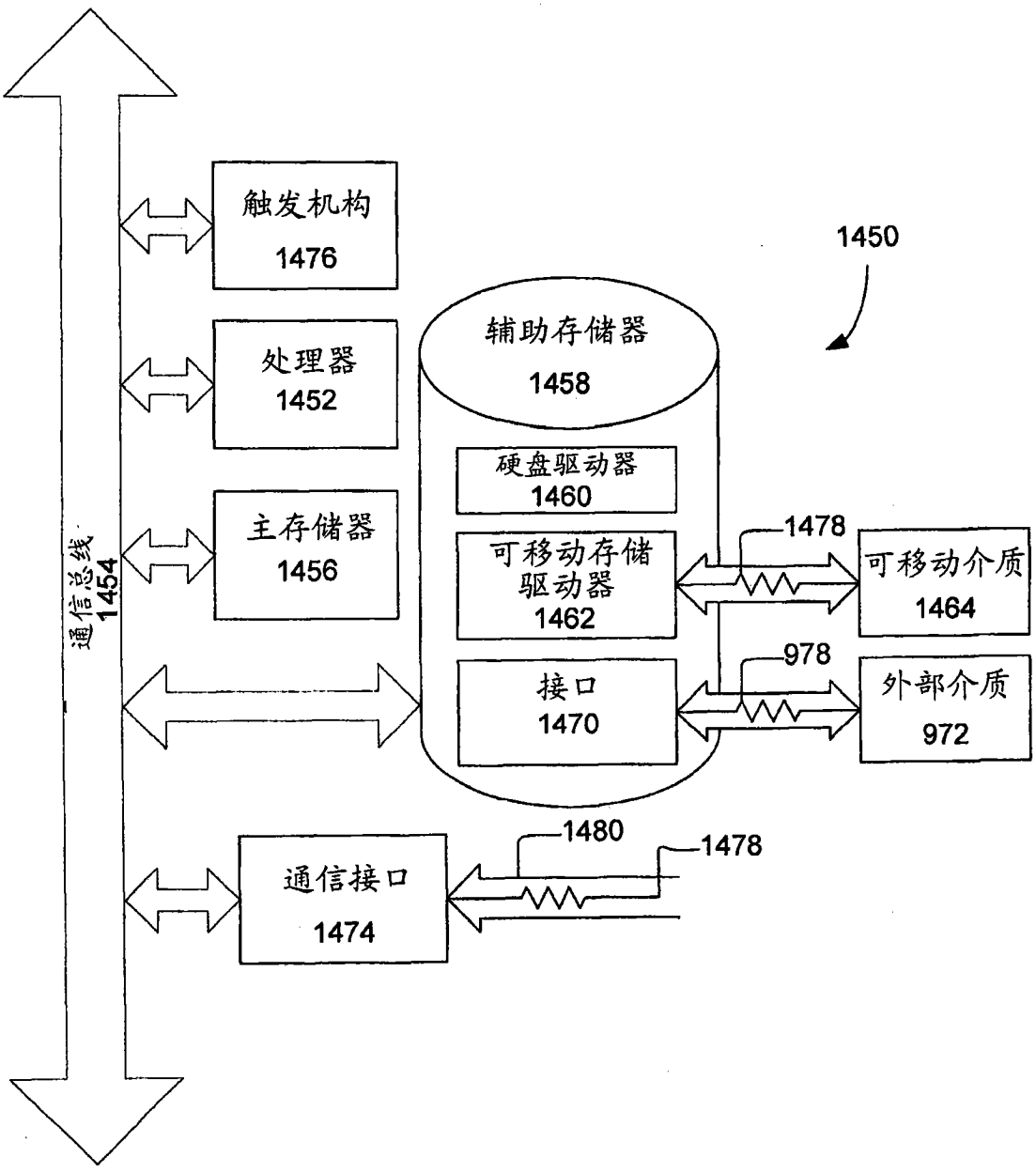

触发机构
1476
处理器
1452
主存储器
1456
通信总线
1454
辅助存储器
1458
1450
硬盘驱动器
1460
可移动存储
驱动器
1462
1478
可移动介质
1464
接口
1470
978
外部介质
972
通信接口
1474
1480
1478

图 14

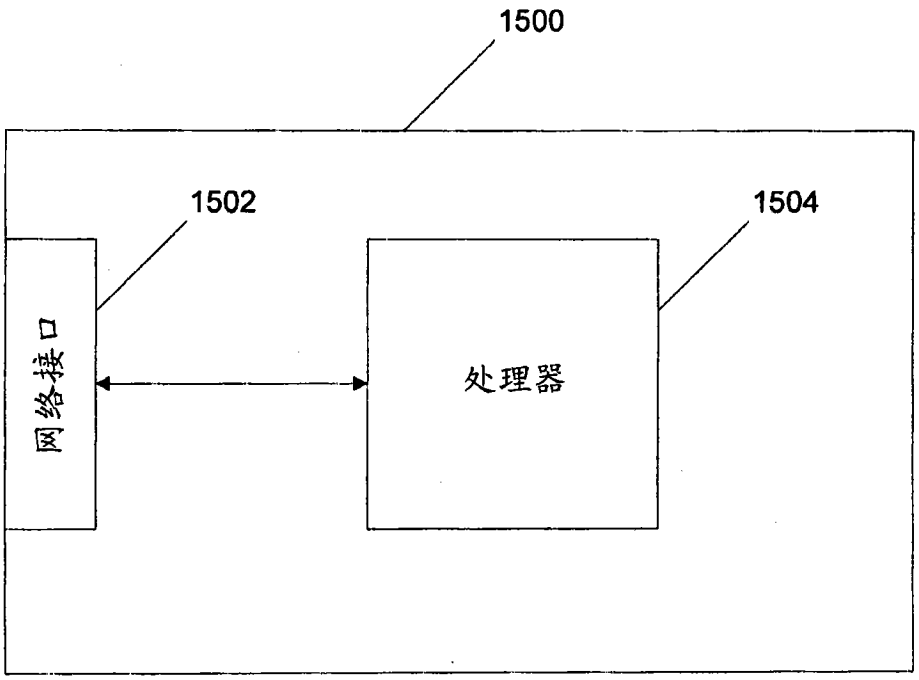


图 15

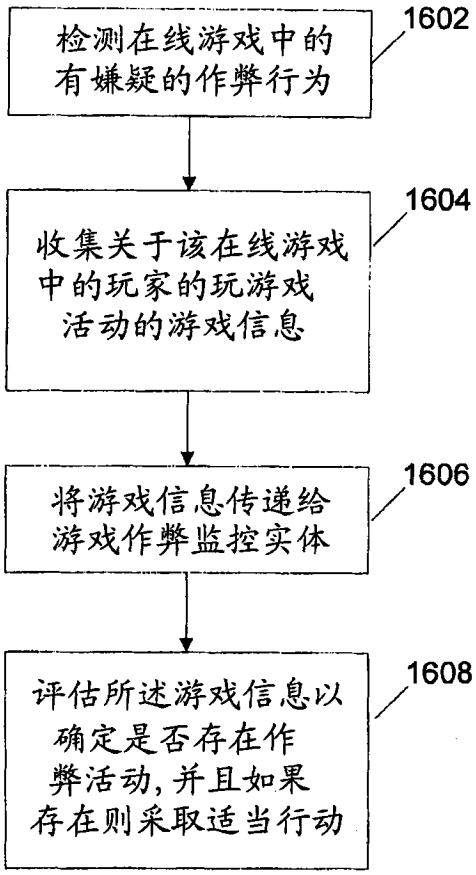

检测在线游戏中的有嫌疑的作弊行为
1602
收集关于该在线游戏中的玩家的玩游戏活动的游戏信息
1604
将游戏信息传递给游戏作弊监控实体
1606
评估所述游戏信息以确定是否存在作弊活动，并且如果存在则采取适当行动
1608

图 16

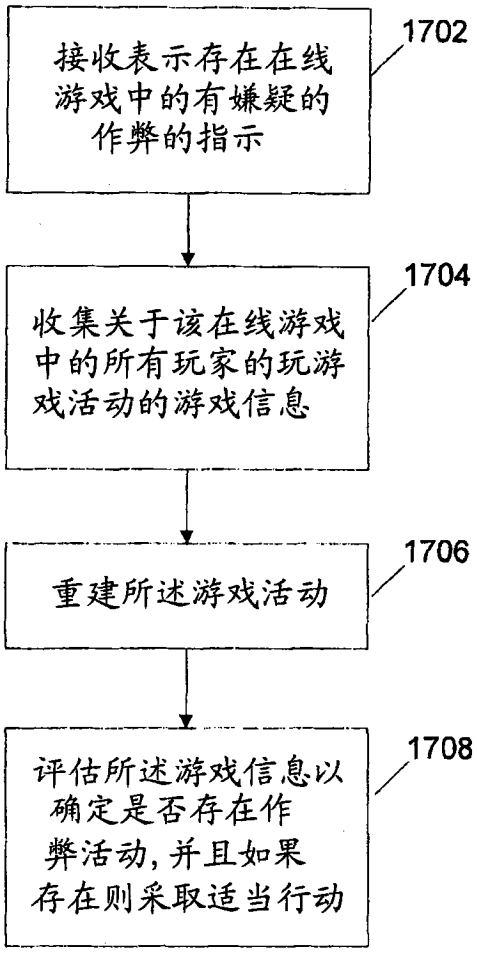

接收表示存在在线游戏中的有嫌疑的作弊的指示
1702
收集关于该在线游戏中的所有玩家的玩游戏活动的游戏信息
1704
重建所述游戏活动
1706
评估所述游戏信息以确定是否存在作弊活动，并且如果存在则采取适当行动
1708

图 17

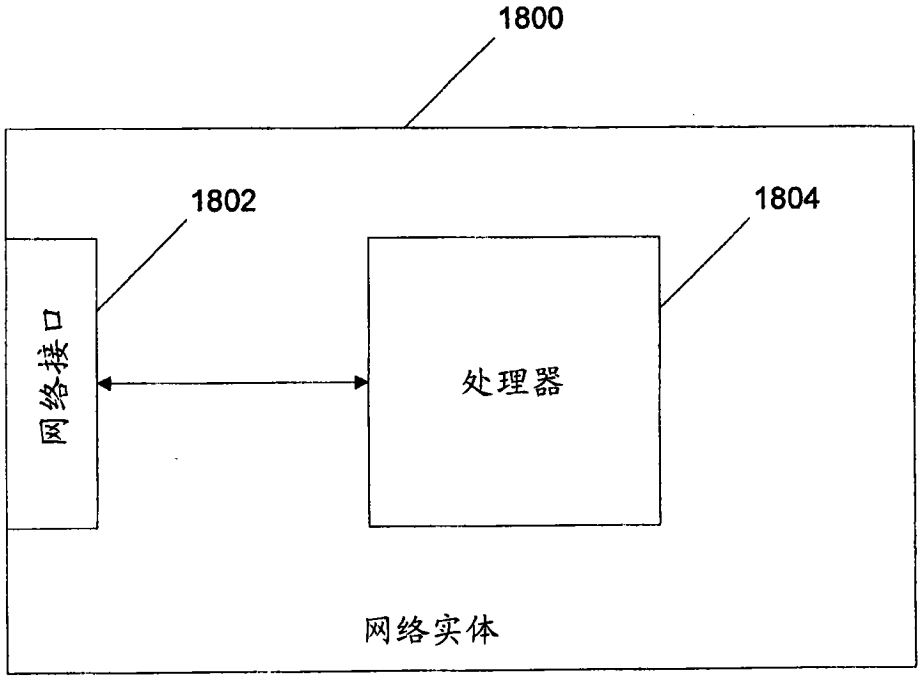


图 18

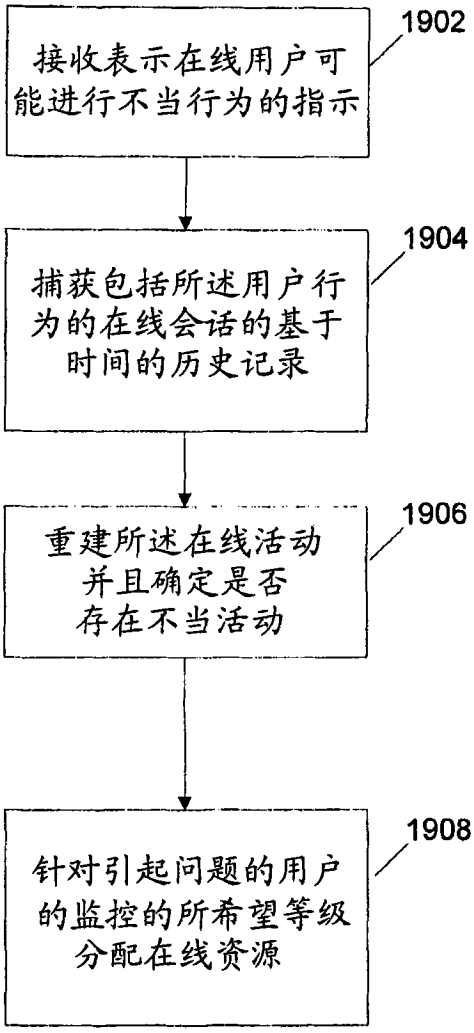

接收表示在线用户可能进行不当行为的指示
1902
捕获包括所述用户行为的在线会话的基于时间的历史记录
1904
重建所述在线活动并且确定是否存在不当活动
1906
针对引起问题的用户的监控的所希望等级分配在线资源
1908

图 19

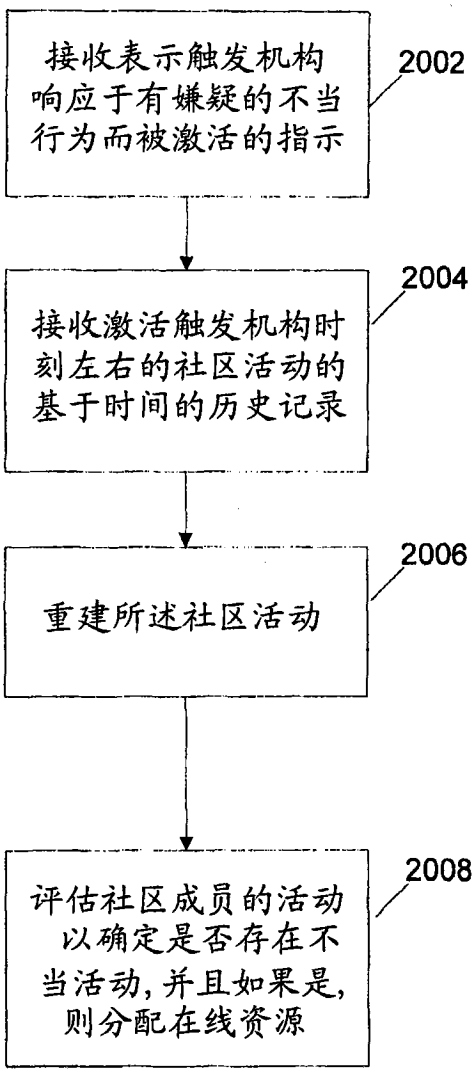

接收表示触发机构响应于有嫌疑的不当行为而被激活的指示
2002
接收激活触发机构时刻左右的社区活动的基于时间的历史记录
2004
重建所述社区活动
2006
评估社区成员的活动以确定是否存在不当活动，并且如果是，则分配在线资源
2008

图 20