(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 104541293 B
(45)授权公告日 2018.02.06

(21)申请号 201380024831.6

(22)申请日 2013.04.10

(65)同一申请的已公布的文献号
申请公布号 CN 104541293 A

(43)申请公布日 2015.04.22

(30)优先权数据
61/646,590 2012.05.14 US
61/683,274 2012.08.15 US
61/748,220 2013.01.02 US
13/776,414 2013.02.25 US

(85)PCT国际申请进入国家阶段日
2014.11.12

(86)PCT国际申请的申请数据
PCT/US2013/035963 2013.04.10

(87)PCT国际申请的公布数据
WO2013/173003 EN 2013.11.21

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚

(72)发明人 R·古普塔 X·魏 A·加塔拉 V·斯里哈拉

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张扬 王英

(51)Int.Cl.
G06N 5/04(2006.01)

(56)对比文件
CN 1961525 A,2007.05.09,
CN 1961525 A,2007.05.09,
US 2009/0239531 A1,2009.09.24,
US 2010/0128125 A1,2010.05.27,
US 6741974 B1,2004.05.25,

审查员 李梦芸

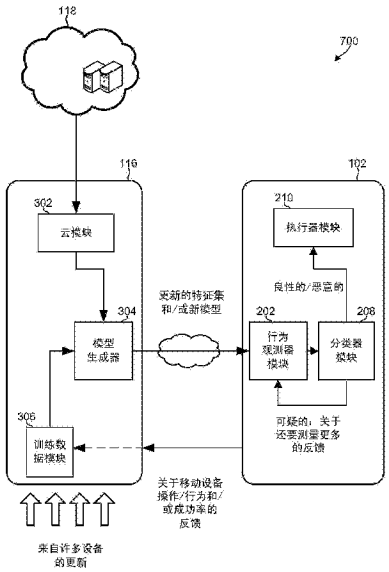
权利要求书6页 说明书22页 附图15页

(54)发明名称

用于客户端-云行为分析器的架构

(57)摘要

用于在客户端-云通信系统中生成数据模型的方法、系统和设备，其可以包括应用机器学习技术以生成描述行为向量的云语料库的第一族的分类器模型。可以对这些向量进行分析，以识别在所述第一族的分类器模型中具有最高可能性使移动设备能够决定性地确定移动设备行为是恶意的还是良性的因素。基于该分析，基于所确定的因素，可以生成第二族的分类器模型，该第二族的分类器模型将显著缩减的因素和数据点标识为与使所述移动设备能够决定性地确定所述移动设备行为是恶意的还是良性的有关。可以基于所述第二族的分类器模型生成移动设备分类器模块，并使其可以用于由移动设备下载，包括对行为向量做出贡献的设备。



CN 104541293 B

1.一种在客户端-云通信系统中生成数据模型的方法,包括:

将机器学习技术应用于从多个不同的移动设备收集的行为向量的云语料库,来生成第一族的健壮分类器模型,所述第一族的健壮分类器模型包括与对移动设备的移动设备行为进行分类有关的因素和数据点;

确定是否存在针对所述第一族的健壮分类器模型的足够的变化以保证生成新模型;

响应于确定存在针对所述第一族的健壮分类器模型的足够的变化,确定所述第一族的健壮分类器模型中哪些因素具有高可能性指示所述移动设备的所述移动设备行为是恶意的还是良性的;

基于所确定的因素,生成第二族的精简分类器模型,所述第二族的精简分类器模型包括与由所述移动设备用于确定所述移动设备的所述移动设备行为是恶意的还是良性的有关的数量缩减的因素和数据点,所述第二族的精简分类器模型中的每个精简分类器模型比其在所述第一族的健壮分类器模型中对应的健壮分类器模型少至少一个数量级;以及

基于所述第二族的精简分类器模型来生成移动设备分类器模块。

2.根据权利要求1所述的方法,其中,将机器学习技术应用于从多个不同的移动设备收集的行为向量的云语料库来生成第一族的健壮分类器模型包括:

在所述客户端-云通信系统的服务器上,从深度分类器生成所述第一族的健壮分类器模型。

3.根据权利要求1所述的方法,其中,生成第二族的精简分类器模型包括:

在所述客户端-云通信系统的服务器上,从精简分类器中生成所述第二族的精简分类器模型。

4.根据权利要求1所述的方法,其中,生成第二族的精简分类器模型包括:

在所述移动设备上,从精简分类器中生成所述第二族的精简分类器模型。

5.根据权利要求1所述的方法,其中,生成包括与在所述移动设备上用于确定所述移动设备的所述移动设备行为是恶意的还是良性的有关的数量缩减的因素和数据点的第二族的精简分类器模型包括:

通过将所确定的因素应用到所述行为向量的云语料库,来生成所述第二族的精简分类器模型。

6.一种客户端-云通信系统中的服务器,包括:

用于将机器学习技术应用于从多个不同的移动设备收集的行为向量的云语料库,来生成第一族的健壮分类器模型的单元,所述第一族的健壮分类器模型包括与对移动设备的移动设备行为进行分类有关的因素和数据点;

用于确定是否存在针对所述第一族的健壮分类器模型的足够的变化以保证生成新模型的单元;

用于响应于确定存在针对所述第一族的健壮分类器模型的足够的变化,确定所述第一族的健壮分类器模型中哪些因素具有高可能性指示所述移动设备的所述移动设备行为是恶意的还是良性的单元;

用于基于所确定的因素,生成第二族的精简分类器模型的单元,所述第二族的精简分类器模型包括与由所述移动设备用于确定所述移动设备的所述移动设备行为是恶意的还是良性的有关的数量缩减的因素和数据点,所述第二族的精简分类器模型中的每个精简分

类器模型比其在所述第一族的健壮分类器模型中对应的健壮分类器模型少至少一个数量级;以及

用于基于所述第二族的精简分类器模型来生成移动设备分类器模块的单元。

7.根据权利要求6所述的服务器,其中,用于将机器学习技术应用于从多个不同的移动设备收集的行为向量的云语料库来生成第一族的健壮分类器模型的单元包括:

用于从深度分类器生成所述第一族的健壮分类器模型的单元。

8.根据权利要求6所述的服务器,其中,用于生成第二族的精简分类器模型的单元包括:

用于从精简分类器中生成所述第二族的精简分类器模型的单元。

9.根据权利要求6所述的服务器,其中,用于生成第二族的精简分类器模型的单元包括:

用于向所述移动设备发送所述第一族的健壮分类器模型和所确定的因素的单元。

10.根据权利要求6所述的服务器,其中,用于生成包括与在所述移动设备上用于确定所述移动设备的所述移动设备行为是恶意的还是良性的有关的数量缩减的因素和数据点的第二族的精简分类器模型的单元包括:

用于通过将所确定的因素应用到所述行为向量的云语料库来生成所述第二族的精简分类器模型的单元。

11.一种分阶段评估移动设备行为的方法,包括:

监测移动设备行为以生成观测结果;

使用阈值以及关于将所述观测结果应用到初始的缩减的特征集模型的结果,来确定所述移动设备行为是使性能降级的、良性的、还是可疑的;

当确定所述移动设备行为是可疑的时,选择要监测的不同的移动设备行为,对所选择的不同的移动设备行为进行监测,以及基于对所选择的不同的移动设备行为的所述监测来生成细化的观测结果;以及

将所述细化的观测结果应用到随后的缩减的特征集模型,以确定所述移动设备行为是使性能降级的、还是良性的。

12.一种移动设备,包括:

用于监测移动设备行为以生成观测结果的单元;

用于使用阈值以及关于将所述观测结果应用到初始的缩减的特征集模型的结果,来确定所述移动设备行为是使性能降级的、良性的、还是可疑的单元;

用于当确定所述移动设备行为是可疑的时,选择要监测的不同的移动设备行为,对所选择的不同的移动设备行为进行监测,以及基于对所选择的不同的移动设备行为的所述监测来生成细化的观测结果的单元;以及

用于将所述细化的观测结果应用到随后的缩减的特征集模型,以确定所述移动设备行为是使性能降级的、还是良性的单元。

13.一种移动设备,包括:

处理器,其配置有处理器可执行指令以执行包括以下各项的操作:

监测移动设备行为以生成观测结果;

使用阈值以及关于将所述观测结果应用到初始的缩减的特征集模型的结果,来确定所

述移动设备行为是使性能降级的、良性的、还是可疑的；

当确定所述移动设备行为是可疑的时，选择要监测的不同的移动设备行为，对所选择的不同的移动设备行为进行监测，以及基于对所选择的不同的移动设备行为的所述监测来生成细化的观测结果；以及

将所述细化的观测结果应用到随后的缩减的特征集模型，以确定所述移动设备行为是使性能降级的、还是良性的。

14.一种在客户端-云通信系统中生成数据模型的方法，包括：

从多个移动设备接收观测信息；

基于从所述多个移动设备接收的所述观测信息，更新云网络的服务器中的行为分类的全局模型；

执行机器学习操作，以基于所述全局模型来生成第一族的分类器；

确定是否存在针对所生成的第一族的分类器的足够的变化以保证生成新的模型；

当确定存在针对所述第一族的分类器的足够的变化时，确定所生成的第一族的分类器中哪些特征是使移动设备处理器能够决定性地确定移动设备行为是恶意的还是良性的最佳特征；

基于所述最佳特征来生成第二族的分类器；

确定是否存在针对所生成的第二族的分类器的足够的变化以保证生成另外的新模型；

当确定存在针对所述第二族的分类器的足够的变化时，生成另外的分类器模型；以及

向所述移动设备处理器发送所生成的另外的分类器模型。

15.一种服务器，包括：

用于从多个移动设备接收观测信息的单元；

用于基于从所述多个移动设备接收的所述观测信息，更新行为分类的全局模型的单元；

用于执行机器学习操作，以基于所述全局模型来生成第一族的分类器的单元；

用于确定是否存在针对所生成的第一族的分类器的足够的变化以保证生成新的模型的单元；

用于当确定存在针对所述第一族的分类器的足够的变化时，确定所生成的第一族的分类器中哪些特征是使移动设备处理器能够决定性地确定移动设备行为是恶意的还是良性的最佳特征的单元；

用于基于所述最佳特征来生成第二族的分类器的单元；

用于确定是否存在针对所生成的第二族的分类器的足够的变化以保证生成另外的新模型的单元；

用于当确定存在针对所述第二族的分类器的足够的变化时，生成另外的分类器模型的单元；以及

用于向所述移动设备处理器发送所生成的另外的分类器模型的单元。

16.一种客户端-云通信系统中的服务器，包括：

处理器，其配置有处理器可执行指令以执行包括以下各项的操作：

将机器学习技术应用于从多个不同的移动设备收集的行为向量的云语料库，来生成第一族的健壮分类器模型，所述第一族的健壮分类器模型包括与对移动设备的移动设备行为

进行分类有关的因素和数据点；

确定是否存在针对所述第一族的健壮分类器模型的足够的变化以保证生成新模型；

响应于确定存在针对所述第一族的健壮分类器模型的足够的变化，确定所述第一族的健壮分类器模型中哪些因素具有高可能性指示所述移动设备的所述移动设备行为是恶意的还是良性的；

基于所确定的因素，生成第二族的精简分类器模型，所述第二族的精简分类器模型包括与由所述移动设备用于确定所述移动设备的所述移动设备行为是恶意的还是良性的有关的数量缩减的因素和数据点，所述第二族的精简分类器模型中的每个精简分类器模型比其在所述第一族的健壮分类器模型中对应的健壮分类器模型少至少一个数量级；以及

基于所述第二族的精简分类器模型来生成移动设备分类器模块。

17.根据权利要求16所述的服务器，其中，所述处理器配置有处理器可执行指令，以使得将机器学习技术应用于从多个不同的移动设备收集的行为向量的云语料库来生成第一族的健壮分类器模型包括：

从深度分类器生成所述第一族的健壮分类器模型。

18.根据权利要求16所述的服务器，其中，所述处理器配置有处理器可执行指令，以使得生成第二族的精简分类器模型包括：

从精简分类器中生成所述第二族的精简分类器模型。

19.根据权利要求16所述的服务器，其中，所述处理器配置有处理器可执行指令，以使得生成第二族的精简分类器模型包括：

向所述移动设备发送所述第一族的健壮分类器模型和所确定的因素。

20.根据权利要求16所述的服务器，其中，所述处理器配置有处理器可执行指令，以使得生成包括与在所述移动设备上用于确定所述移动设备的所述移动设备行为是恶意的还是良性的有关的数量缩减的因素和数据点的第二族的精简分类器模型包括：

通过将所确定的因素应用到所述行为向量的云语料库来生成所述第二族的精简分类器模型。

21.一种服务器，包括：

处理器，其配置有处理器可执行指令以执行包括以下各项的操作：

从多个移动设备接收观测信息；

基于从所述多个移动设备接收的所述观测信息，更新行为分类的全局模型；

执行机器学习操作，以基于所述全局模型来生成第一族的分类器；

确定是否存在针对所生成的第一族的分类器的足够的变化以保证生成新的模型；

当确定存在针对所述第一族的分类器的足够的变化时，确定所生成的第一族的分类器中哪些特征是使移动设备处理器能够决定性地确定移动设备行为是恶意的还是良性的最佳特征；

基于所述最佳特征来生成第二族的分类器；

确定是否存在针对所生成的第二族的分类器的足够的变化以保证生成另外的新模型；

当确定存在针对所述第二族的分类器的足够的变化时，生成另外的分类器模型；以及

向所述移动设备处理器发送所生成的另外的分类器模型。

22.一种非暂时性计算机可读存储介质，其具有被存储在其上的处理器可执行软件指

令，所述处理器可执行软件指令被配置为使处理器执行用于分阶段评估移动设备行为的操作，所述操作包括：

监测移动设备行为以生成观测结果；

使用阈值以及关于将所述观测结果应用到初始的缩减的特征集模型的结果，来确定所述移动设备行为是使性能降级的、良性的、还是可疑的；

当确定所述移动设备行为是可疑的时，选择要监测的不同的移动设备行为，对所选择的不同的移动设备行为进行监测，以及基于对所选择的不同的移动设备行为的所述监测来生成细化的观测结果；以及

将所述细化的观测结果应用到随后的缩减的特征集模型，以确定所述移动设备行为是使性能降级的、还是良性的。

23.一种非暂时性计算机可读存储介质，其具有被存储在其上的服务器可执行软件指令，所述服务器可执行软件指令被配置为使服务器处理器执行用于在客户端-云通信系统中生成数据模型的操作，所述操作包括：

将机器学习技术应用于从多个不同的移动设备收集的行为向量的云语料库，来生成第一族的健壮分类器模型，所述第一族的健壮分类器模型包括与对移动设备的移动设备行为进行分类有关的因素和数据点；

确定是否存在针对所述第一族的健壮分类器模型的足够的变化以保证生成新模型；

响应于确定存在针对所述第一族的健壮分类器模型的足够的变化，确定所述第一族的健壮分类器模型中哪些因素具有高可能性指示所述移动设备的所述移动设备行为是恶意的还是良性的；

基于所确定的因素，生成第二族的精简分类器模型，所述第二族的精简分类器模型包括与由所述移动设备用于确定所述移动设备的所述移动设备行为是恶意的还是良性的有关的数量缩减的因素和数据点，所述第二族的精简分类器模型中的每个精简分类器模型比其在所述第一族的健壮分类器模型中对应的健壮分类器模型少至少一个数量级；以及

基于所述第二族的精简分类器模型来生成移动设备分类器模块。

24.根据权利要求23所述的非暂时性计算机可读存储介质，其中，所存储的服务器可执行软件指令被配置为使所述服务器处理器执行操作，使得将机器学习技术应用于从多个不同的移动设备收集的行为向量的云语料库来生成第一族的健壮分类器模型包括：

在所述客户端-云通信系统的服务器上，从深度分类器生成所述第一族的健壮分类器模型。

25.根据权利要求23所述的非暂时性计算机可读存储介质，其中，所存储的服务器可执行软件指令被配置为使所述服务器处理器执行操作，使得生成第二族的精简分类器模型包括：

在所述客户端-云通信系统的服务器上，从精简分类器中生成所述第二族的精简分类器模型。

26.根据权利要求23所述的非暂时性计算机可读存储介质，其中，所存储的服务器可执行软件指令被配置为使所述服务器处理器执行操作，使得生成第二族的精简分类器模型包括：

在所述移动设备上，从精简分类器中生成所述第二族的精简分类器模型。

27.根据权利要求23所述的非暂时性计算机可读存储介质，其中，所存储的服务器可执行软件指令被配置为使所述服务器处理器执行操作，使得生成包括与在所述移动设备上用于确定所述移动设备的所述移动设备行为是恶意的还是良性的有关的数量缩减的因素和数据点的第二族的精简分类器模型包括：

通过将所确定的因素应用到所述行为向量的云语料库，来生成所述第二族的精简分类器模型。

28.一种非暂时性计算机可读存储介质，其具备被存储在其上的服务器可执行软件指令，所述服务器可执行软件指令被配置为使服务器处理器执行用于在客户端-云通信系统中生成数据模型的操作，所述操作包括：

从多个移动设备接收观测信息；

基于从所述多个移动设备接收的所述观测信息，更新云网络的服务器中的行为分类的全局模型；

执行机器学习操作，以基于所述全局模型来生成第一族的分类器；

确定是否存在针对所生成的第一族的分类器的足够的变化以保证生成新的模型；

当确定存在针对所述第一族的分类器的足够的变化时，确定所生成的第一族的分类器中哪些特征是使移动设备处理器能够决定性地确定移动设备行为是恶意的还是良性的最佳特征；

基于所述最佳特征来生成第二族的分类器；

确定是否存在针对所生成的第二族的分类器的足够的变化以保证生成另外的新模型；

当确定存在针对所述第二族的分类器的足够的变化时，生成另外的分类器模型；以及

向所述移动设备处理器发送所生成的另外的分类器模型。

用于客户端-云行为分析器的架构

[0001] 相关申请

[0002] 本申请要求享受于2013年1月2日提交的、题目为“Architecture for Client-Cloud Behavior Analyzer”的美国临时专利申请61/748,220、2012年5月14日提交的、题目为“System,Apparatus and Method for Adaptive Observation of Mobile Device Behavior”的美国临时专利申请No.61/646,590以及于2012年8月15日提交的、题目为“System,Apparatus and Method for Adaptive Observation of Mobile Device Behavior”的美国临时专利申请61/683,274的优先权的权益，故出于所有的目的以引用方式将这两个临时申请的全部内容并入本申请。

背景技术

[0003] 在过去的若干年里，蜂窝和无线通信技术已爆炸性增长。这种增长由更好的通信、硬件、更大的网络、以及更可靠的协议来推动。无线服务提供商现在能够向其客户提供不断扩展的一系列特征和服务，并向用户提供对信息、资源以及通信的前所未有的接入水平。为了与这些服务增强俱进，移动电子设备(例如，蜂窝电话、平板电脑、膝上型电脑等)已经变得比以往更强大和复杂。该复杂性已经为恶意软件、软件冲突、硬件错误、以及其它类似的错误或现象不利地影响移动设备的长期以及持续的性能和功率利用水平创造了新的机会。因此，对可能不利地影响移动设备的长期以及持续的性能和功率利用级别的条件和/或移动设备行为进行识别和校正对消费者而言是有益的。

发明内容

[0004] 各个方面包括在客户端-云通信系统中生成数据模型的方法，其可以包括应用机器学习技术以生成描述行为向量的云语料库的第一族的分类器模型，确定在所述第一族的分类器模型中哪些因素具有使移动设备能够决定性地确定移动设备行为是恶意的还是良性的较高可能性，基于所确定的因素生成将数量缩减的因素和数据点标识为与使所述移动设备能够决定性地确定所述移动设备行为是恶意的还是良性的有关的第二族的分类器模型，以及基于所述第二族的分类器模型生成移动设备分类器模块。

[0005] 在一方面，应用机器学习技术以生成描述行为向量的云语料库的第一族的分类器模型可以包括在云网络的服务器中的深度分类器中生成所述第一族的分类器模型。在另外的方面，生成第二族的分类器模型可以包括在网络服务器中的精简分类器中生成所述第二族的分类器模型。在另外的方面，生成第二族的分类器模型可以包括在所述移动设备网络中的精简分类器中生成所述第二族的分类器模型。在另外的方面，生成将数量缩减的因素和数据点标识为与使所述移动设备能够决定性地确定所述移动设备行为是恶意的还是良性的有关的第二族的分类器模型包括通过将所确定的因素应用到所述行为向量的云语料库来生成所述第二族的分类器模型。

[0006] 另外的方面包括一种服务器计算设备，其具有用于应用机器学习技术以生成描述行为向量的云语料库的第一族的分类器模型的单元，用于确定在所述第一族的分类器模型

中哪些因素具有使移动设备能够决定性地确定移动设备行为是恶意的还是良性的较高可能性的单元，用于基于所确定的因素生成将数量缩减的因素和数据点标识为与使所述移动设备能够决定性地确定所述移动设备行为是恶意的还是良性的有关的第二族的分类器模型的单元，以及用于基于所述第二族的分类器模型生成移动设备分类器模块的单元。

[0007] 在一方面，用于应用机器学习技术以生成描述行为向量的云语料库的第一族的分类器模型的单元可以包括用于在深度分类器中生成所述第一族的分类器模型的单元。在另外的方面，用于生成第二族的分类器模型的单元可以包括用于在精简分类器中生成所述第二族的分类器模型的单元。在另外的方面，用于生成第二族的分类器模型的单元可以包括用于向所述移动设备发送所述第一族的分类器模型和所确定的因素的单元。在另外的方面，用于生成将数量缩减的因素和数据点标识为与使所述移动设备能够决定性地确定所述移动设备行为是恶意的还是良性的有关的第二族的分类器模型的单元包括用于通过将所确定的因素应用到所述行为向量的云语料库来生成所述第二族的分类器模型的单元。

[0008] 另外的方面包括一种服务器计算设备，其具有处理器，该处理器配置具有用于执行操作的处理器可执行指令，所述操作可以包括应用机器学习技术以生成描述行为向量的云语料库的第一族的分类器模型，确定在所述第一族的分类器模型中哪些因素具有使移动设备能够决定性地确定移动设备行为是恶意的还是良性的较高可能性，基于所确定的因素生成将数量缩减的因素和数据点标识为与使所述移动设备能够决定性地确定所述移动设备行为是恶意的还是良性的有关的第二族的分类器模型，以及基于所述第二族的分类器模型生成移动设备分类器模块。

[0009] 在一方面，处理器可以配置具有处理器可执行指令使得应用机器学习技术以生成描述行为向量的云语料库的第一族的分类器模型可以包括在深度分类器中生成所述第一族的分类器模型。在另外的方面，处理器可以配置具有处理器可执行指令使得生成第二族的分类器模型可以包括在精简分类器中生成所述第二族的分类器模型。在另外的方面，处理器可以配置具有处理器可执行指令使得生成第二族的分类器模型可以包括向所述移动设备发送所述第一族的分类器模型和所确定的因素。在另外的方面，处理器可以配置具有处理器可执行指令使得生成将数量缩减的因素和数据点标识为与使所述移动设备能够决定性地确定所述移动设备行为是恶意的还是良性的有关的第二族的分类器模型可以包括通过将所确定的因素应用到所述行为向量的云语料库来生成所述第二族的分类器模型。

[0010] 另外的方面包括一种非暂时性计算机可读存储介质，其上存储有服务器可执行软件指令，所述软件指令配置成使服务器处理器执行用于在客户端-云通信系统中生成数据模型的操作。在一方面，所述操作可以包括应用机器学习技术以生成描述行为向量的云语料库的第一族的分类器模型，确定在所述第一族的分类器模型中哪些因素具有使移动设备能够决定性地确定移动设备行为是恶意的还是良性的较高可能性，基于所确定的因素生成将数量缩减的因素和数据点标识为与使所述移动设备能够决定性地确定所述移动设备行为是恶意的还是良性的有关的第二族的分类器模型，基于所述第二族的分类器模型生成移动设备分类器模块。

[0011] 在一方面，所存储的服务器可执行软件指令可以配置成使服务器处理器执行操作使得应用机器学习技术以生成描述行为向量的云语料库的第一族的分类器模型可以包括在云网络的服务器中的深度分类器中生成所述第一族的分类器模型。在另外的方面，所存

储的服务器可执行软件指令可以配置成使服务器处理器执行操作使得生成第二族的分类器模型可以包括在网络服务器中的精简分类器中生成所述第二族的分类器模型。在另外的方面，所存储的服务器可执行软件指令可以配置成使服务器处理器执行操作使得生成第二族的分类器模型可以包括向所述移动设备发送所述第一族的分类器模型和所确定的因素。在另外的方面，所存储的服务器可执行软件指令可以配置成使服务器处理器执行操作使得生成将数量缩减的因素和数据点标识为与使所述移动设备能够决定性地确定所述移动设备行为是恶意的还是良性的有关的第二族的分类器模型可以包括通过将所确定的因素应用到所述行为向量的云语料库来生成所述第二族的分类器模型。

[0012] 另外的方面包括一种客户端-云通信系统，其包括移动设备和服务器计算设备。服务器处理器可以配置具有服务器可执行指令以执行操作，所述操作包括应用机器学习技术以生成描述行为向量的云语料库的第一族的分类器模型，确定在所述第一族的分类器模型中哪些因素具有使移动设备能够决定性地确定移动设备行为是恶意的还是良性的较高可能性，以及向所述移动设备发送所述第一族的分类器模型和所确定的因素。移动设备处理器可以配置具有处理器可执行指令以执行操作，所述操作包括基于所确定的因素生成将数量缩减的因素和数据点标识为与使所述移动设备能够决定性地确定所述移动设备行为是恶意的还是良性的有关的第二族的分类器模型，以及基于所述第二族的分类器模型生成移动设备分类器模块。

[0013] 另外的方面包括用于分阶段评估移动设备行为的方法，包括监测移动设备行为以生成观测结果，将所述观测结果应用到初始的缩减的特征集模型，以确定所述移动设备行为是使性能降级的、良性的、还是可疑的，当确定所述移动设备行为是可疑的时，监测另外的或不同的移动设备行为以生成细化的观测结果，以及将所述细化的观测结果应用到随后的缩减的特征集模型，以确定所述移动设备行为是使性能降级的、使性能降级的还是良性的。

[0014] 另外的方面包括一种移动计算设备，其具有用于监测移动设备行为以生成观测结果的单元，用于将所述观测结果应用到初始的缩减的特征集模型，以确定所述移动设备行为是使性能降级的、良性的、还是可疑的单元，用于当确定所述移动设备行为是可疑的时，监测另外的或不同的移动设备行为以生成细化的观测结果的单元，以及用于将所述细化的观测结果应用到随后的缩减的特征集模型，以确定所述移动设备行为是使性能降级的、使性能降级的还是良性的单元。

[0015] 另外的方面包括一种移动计算设备，其具有配置具有处理器可执行指令的处理器以执行操作，所述操作包括监测移动设备行为以生成观测结果，将所述观测结果应用到初始的缩减的特征集模型，以确定所述移动设备行为是使性能降级的、良性的、还是可疑的，当确定所述移动设备行为是可疑的时，监测另外的或不同的移动设备行为以生成细化的观测结果，以及将所述细化的观测结果应用到随后的缩减的特征集模型，以确定所述移动设备行为是使性能降级的、使性能降级的还是良性的。

[0016] 另外的方面包括一种非暂时性计算机可读存储介质，其上存储有处理器可执行软件指令，所述软件指令配置成使处理器执行用于分阶段评估移动设备行为的操作。所述操作可以包括监测移动设备行为以生成观测结果，将所述观测结果应用到初始的缩减的特征集模型，以确定所述移动设备行为是使性能降级的、良性的、还是可疑的；当确定所述移动

设备行为是可疑的时，监测另外的或不同的移动设备行为以生成细化的观测结果；以及将所述细化的观测结果应用到随后的缩减的特征集模型，以确定所述移动设备行为是使性能降级的、使性能降级的还是良性的。

[0017] 另外的方面包括从多个移动设备接收观测信息，基于从所述多个移动设备接收的所述观测信息，更新在云网络的服务器中的行为分类的全局模型，基于所述全局模型，执行机器学习操作以生成第一族的分类器，确定针对所生成的第一族的分类器是否存在足够的变化以保证生成新的模型，当确定针对所述第一族的分类器存在足够的变化时，确定在所生成的第一族的分类器中哪些特征是使移动设备处理器能够决定性地确定移动设备行为是恶意的还是良性的最佳特征，基于所述最佳特征生成第二族的分类器，确定针对所生成的第二族的分类器是否存在足够的变化以保证生成另外的新模型，当确定针对所述第二族的分类器存在足够的变化时，生成另外的分类器模型，以及向所述移动设备处理器发送所生成的另外的分类器模型的方法。

[0018] 另外的方面包括一种服务器计算设备，其可以包括用于从多个移动设备接收观测信息的单元，用于基于从所述多个移动设备接收的所述观测信息，更新行为分类的全局模型的单元，用于基于所述全局模型，执行机器学习操作以生成第一族的分类器的单元，用于确定针对所生成的第一族的分类器是否存在足够的变化以保证生成新的模型的单元，用于当确定针对所述第一族的分类器存在足够的变化时，确定在所生成的第一族的分类器中哪些特征是使移动设备处理器能够决定性地确定移动设备行为是恶意的还是良性的最佳特征的单元，用于基于所述最佳特征生成第二族的分类器的单元，用于确定针对所生成的第二族的分类器是否存在足够的变化以保证生成另外的新模型的单元，用于当确定针对所述第二族的分类器存在足够的变化时，生成另外的分类器模型的单元，以及用于向所述移动设备处理器发送所生成的另外的分类器模型的单元。

[0019] 另外的方面包括一种服务器计算设备，其可以包括配置具有处理器可执行指令的处理器以执行操作，所述操作可以包括：从多个移动设备接收观测信息；基于从所述多个移动设备接收的所述观测信息，更新行为分类的全局模型；基于所述全局模型，执行机器学习操作以生成第一族的分类器；确定针对所生成的第一族的分类器是否存在足够的变化以保证生成新的模型；当确定针对所述第一族的分类器存在足够的变化时，确定在所生成的第一族的分类器中哪些特征是使移动设备处理器能够决定性地确定移动设备行为是恶意的还是良性的最佳特征；基于所述最佳特征生成第二族的分类器；确定针对所生成的第二族的分类器是否存在足够的变化以保证生成另外的新模型；当确定针对所述第二族的分类器存在足够的变化时，生成另外的分类器模型；以及向所述移动设备处理器发送所生成的另外的分类器模型。

[0020] 另外的方面包括一种非暂时性服务器可读存储介质，其上存储有处理器可执行软件指令，所述软件指令配置成使服务器计算设备执行操作，所述操作可以包括：从多个移动设备接收观测信息；基于从所述多个移动设备接收的所述观测信息，更新在云网络的服务器中的行为分类的全局模型；基于所述全局模型，执行机器学习操作以生成第一族的分类器；确定针对所生成的第一族的分类器是否存在足够的变化以保证生成新的模型；当确定针对所述第一族的分类器存在足够的变化时，确定在所生成的第一族的分类器中哪些特征是使移动设备处理器能够决定性地确定移动设备行为是恶意的还是良性的最佳特征；基于

所述最佳特征生成第二族的分类器；确定针对所生成的第二族的分类器是否存在足够的变化以保证生成另外的新模型；当确定针对所述第二族的分类器存在足够的变化时，生成另外的分类器模型；以及向所述移动设备处理器发送所生成的另外的分类器模型。

[0021] 另外的方面包括一种客户端-云通信系统，其包括移动设备和服务器。该服务器处理器可以配置具有服务器可执行指令，以执行操作，所述操作包括：从多个移动设备接收观测信息；基于从所述多个移动设备接收的所述观测信息，更新行为分类的全局模型；基于所述全局模型，执行机器学习操作以生成第一族的分类器；确定针对所生成的第一族的分类器是否存在足够的变化以保证生成新的模型；当确定针对所述第一族的分类器存在足够的变化时，确定在所生成的第一族的分类器中哪些特征是使移动设备处理器能够决定性地确定移动设备行为是恶意的还是良性的最佳特征；基于所述最佳特征生成第二族的分类器；确定针对所生成的第二族的分类器是否存在足够的变化以保证生成另外的新模型；当确定针对所述第二族的分类器存在足够的变化时，生成另外的分类器模型；以及向所述移动设备处理器发送所生成的另外的分类器模型作为初始的缩减的特征集模型。

[0022] 移动设备处理器可以配置具有处理器可执行指令，以执行操作，所述操作包括：从所述服务器接收所述初始的缩减的特征集模型；监测移动设备行为以生成观测结果；将所述观测结果应用到初始的缩减的特征集模型，以确定所述移动设备行为是使性能降级的、良性的、还是可疑的；当确定所述移动设备行为是可疑的时，监测另外的或不同的移动设备行为以生成细化的观测结果；将所述细化的观测结果应用到随后的缩减的特征集模型，以确定所述移动设备行为是使性能降级的、使性能降级的还是良性的；以及向所述服务器发送所述细化的观测结果和应用所述细化的观测结果的结果作为观测信息。

附图说明

[0023] 附图描绘了本发明的示例性方面，其被并入本申请中并构成该说明书的一部分，且其与上文给出的一般性描述以及下文给出的详细描述一起用于解释本发明的特征。

[0024] 图1是示出适合在各个方面中使用的示例性电信系统的网络组件的通信系统框图。

[0025] 图2是示出移动设备的一方面中的示例性逻辑组件和信息流的框图，该移动设备配置成确定特定的移动设备行为、软件应用、或进程是否是使性能降级的、可疑的、或良性的。

[0026] 图3是示出具有网络服务器的系统的一方面中的示例性组件和信息流的框图，该网络服务器配置成结合云服务/网络来工作以识别活动的恶意软件应用或写得不好的软件应用和/或可疑的或使性能降级的移动设备行为。

[0027] 图4是示出生成一个或多个缩减的特征模型的方法的一方面的过程流图，该缩减的特征模型包括来自全特征模型的特征和数据点的子集。

[0028] 图5A和5B是示出基于一个或多个缩减的特征模型来建立精简的移动设备分类器的系统方法的一方面的过程流图。

[0029] 图6是示出分阶段评估移动设备行为的渐进分析方法的一方面的过程流图。

[0030] 图7是示出包含网络服务器的系统的一方面中的示例性组件和信息流的框图，该网络服务器配置成从多个移动设备接收更新。

[0031] 图8A和8B是示出根据行为向量的云语料库建立精简的移动设备分类器的服务器/系统方法的一方面的过程流图，其中行为向量的云语料库是利用从多个移动设备接收的信息连续更新的。

[0032] 图9是根据一方面示出在配置成执行动态和自适应观测的观测器模块中示例性逻辑组件和信息流的框图。

[0033] 图10是根据另一方面示出在计算系统执行服务器守护进程中示例性逻辑组件和信息流的框图。

[0034] 图11是示出用于在移动设备上执行自适应观测的方法的一方面的过程流图。

[0035] 图12是适合在一方面中使用的移动设备的组件框图。

[0036] 图13是适合在一方面中使用的服务器设备的组件框图。

具体实施方式

[0037] 下面将参照附图详细描述各个方面。只要有可能，贯穿这些附图，将使用相同的附图标记来表示相同的或类似的部件。对特定示例和实现的引用是为了说明的目的，其不意在限制本发明或权利要求书的保护范围。

[0038] 在本申请中使用词语“示例性的”来指“充当示例、实例或例证”。本申请中被描述为“示例性的”任何实现不一定被解释为比其它的实现优选的或更优的。

[0039] 多个不同的蜂窝和移动通信服务和标准在未来是可用的或可预期的，其全部可以根据各方面或从各个方面受益。这样的服务和标准包括，例如第三代合作伙伴计划(3GPP)、长期演进(LTE)系统、第三代无线移动通信技术(3G)、第四代无线移动通信技术(4G)、全球移动通信系统(GSM)、通用移动电信系统(UMTS)、3GSM、通用分组无线服务(GPRS)、码分多址(CDMA)系统(例如，cdmaOne、CDMA1020TM)、用于GSM演进的增强型数据速率、增强型移动电话系统(AMPS)、数字AMPS(IS-136/TDMA)、演进数据优化(EV-DO)、数字增强型无绳电信(DECT)、微波存取全球互通(WiMAX)、无线局域网(WLAN)、Wi-Fi保护的访问I&II(WPA，WPA2)、以及集成的数字增强型网络(iden)。例如，这些技术中的每一个涉及发送和接收语音、数据、信令、和/或内容消息。应该理解的是，对与单个电信标准或技术相关的术语和/或技术细节的任何引用都仅是为了说明的目的，且其不意在将权利要求的保护范围限制到特定的通信系统或技术，除非在权利要求的语言中明确说明。

[0040] 在本申请中互换地使用词语“移动计算设备”和“移动设备”来指蜂窝电话、智能电话、个人或移动多媒体播放器、个人数据助理(PDA)、膝上型计算机、平板计算机、智能本、超级本、掌上计算机、无线电子邮件接收器、具有多媒体因特网功能的蜂窝电话、无线游戏控制器、以及包含存储器、对于其而言性能重要的可编程处理器、以及在电池电源下工作使得节能方法是有益的类似的个人电子设备中的任何一个或全部。虽然各个方面对于诸如智能电话之类的、具有有限处理功率且在电池上运行的移动计算设备尤其有用，但是这些方面在包含处理器并执行应用程序的任何电子设备中一般都有用。

[0041] 在本申请中使用术语“性能降级”来指各种各样不想要的移动设备操作和特征，例如较长的处理时间、较低的电池寿命、私人数据的丢失、恶意的经济活动(例如，发送未授权的高价SMS消息)、与强占移动设备或利用电话来进行监视或僵尸网络活动等有关的操作。

[0042] 在本申请中使用术语“片上系统”(SOC)是指包含在单个基板上集成的多个资源

和/或处理器的单个集成电路(IC)芯片。单个SOC可以包含用于数字、模拟、混合信号和射频功能的电路。单个SOC还可以包含任意数量的通用和/或专用处理器(数字信号处理器、调制解调器处理器、视频处理器等)、存储块(例如,ROM、RAM、闪存等)、以及资源(例如,定时器、电压调节器、振荡器等)。SOC还可以包含用于控制所集成的资源和处理器以及用于控制外围设备的软件。

[0043] 在本申请中使用术语“多核处理器”来指包含两个或更多个配置成读取和执行程序指令的独立的处理内核(例如,CPU内核)的单个集成电路(IC)芯片或芯片封装。SOC可以包含多个多核处理器,并且可以将SOC中的每一处理器称为内核。在本申请中使用术语“多处理器”来指包含配置成读取和执行程序指令的两个或多个处理单元的系统或设备。

[0044] 通常,移动设备的性能和功率效率随着时间而降级。近来,反病毒公司(例如,McAfee、Symantec等)已经开始销售旨在减慢这种降级的移动反病毒、防火墙、和加密产品。然而,这些解决方案中的许多依赖于计算密集型扫描引擎在移动设备上的周期性执行,这可能消耗了移动设备许多的处理和电池资源,使移动设备减慢或无用达延长的时间段,和/或以其它方式降低了用户体验。此外,这些解决方案典型地受限于检测已知的病毒和恶意软件,并且不能解决常常结合起来而导致移动设备随着时间的降级的多种复杂因素和/或交互(例如,当性能降级不是由病毒或恶意软件导致的时)。对于这些和其他原因,现有的抗病毒、防火墙、和加密产品未提供用于识别可能对移动设备随着时间降级起作用的多个因素、用于避免移动设备降级、或用于将老化的移动设备有效地恢复到其原始状况的胜任的解决方案。

[0045] 存在用于对在计算设备上执行的进程或应用程序的行为进行建模的各种解决方案,并且这些行为模型可以用于在计算设备上的恶意和良性进程/程序之间进行区分。然而,这些现有的建模解决方案不适合在移动设备上使用,这是因为这些解决方案通常需要执行计算密集型进程,这些进程消耗大量的处理、存储器和能量资源,而所有这些资源在移动设备上都是匮乏的。此外,这些解决方案通常受限于评估个别应用程序或进程的行为,而不对性能降级的移动设备行为提供准确的或完整的模型。由于这些或其他原因,现有的建模解决方案不适合识别对移动设备随着时间降级其作用的多个因素、防止移动设备降级、或将老化的移动设备有效地恢复到其原始的状况。

[0046] 存在用于通过使用机器学习技术来检测恶意软件的各种其他解决方案。这些解决方案通过在基于云的服务器中的应用来典型地分析软件应用或进程。这样的分析可能由数据变换组成,以提取软件应用的特征,并且然后在先前生成的机器学习模型上执行上述特征。执行模型允许通过利用从执行当前的应用获得的信息影响更新其来改进当前的模型。

[0047] 但是,这些解决方案中的许多由于其需要评估非常大量的数据,且其受限于评估单个的应用程序或进程、或需要在移动设备中执行计算密集型进程,因此其不适合在移动设备上使用。例如,现有的解决方案可以应用大量的训练数据导出将输入看作是特征向量的模型到个别软件应用,该特征向量是从数学变换的应用导出的。但是,这样的解决方案通常在一个时间仅分析单个软件应用,而不是使性能降级的移动设备行为的完整的模型。此外,这样的解决方案不应用机器学习技术来生成描述大量行为向量的第一族的分类器模型,确定在第一族的分类器模型中哪些因素最有可能使移动设备决定性地确定移动设备行为是恶意的还是良性的,以及基于所确定的因素生成第二族的分类器模型。此外,这样的解

决方案不确定对于第一和第二族的分类器是否存在足够的变化来保证生成新的或额外的数据/行为模型。由于这些和其他原因，现有的机器学习技术不适合在复杂的且资源受限的现代移动设备中使用。

[0048] 存在对移动设备随着时间在性能和功率利用级别方面的降级可能起作用的各种因素，包括设计很差的软件应用、恶意软件、病毒、零碎的存储器、后台处理等。但是，由于现代移动设备的复杂性，对于用户、操作系统、和/或应用程序(例如，抗病毒软件等)而言，准确且有效地识别这样的问题的源和/或对所识别的问题提供适当的补救措施日益困难。因此，目前移动设备用户具有较少的用于防止移动设备随着时间在性能和功率利用级别方面降级或用于将老化的移动设备恢复到其原始的性能和功率利用级别的补救措施。

[0049] 各个方面提供了用于有效地识别、分类、建模、防止、和/或校正经常使移动设备的性能和/或功率利用级别随着时间降级的条件和/或移动设备行为的网络服务器、移动设备、系统、和方法。通过将关于这样的状况和纠正措施存储在诸如“云”的中央数据库中并使移动设备访问并使用存储在该数据库中的信息，与独立地在每一移动设备中完成所有这样的分析相比，各个方面使得移动设备能够对性能限制和不理想的操作状况作出更快速的反应且具有更低的功耗。

[0050] 如上文所提及的，移动设备是具有相对受限的处理、存储器、和能量资源的资源受限系统。还如上文所提及的，现代的移动设备是复杂系统，并且可能存在需要分析以识别移动设备降级的原因或源的成千上万的特征/因素和数十亿的数据点。由于这些限制，因此对可能使现代移动设备的复杂且资源受限的系统在性能和/或功率利用级别方面降级的所有各种进程、行为、或因素(或其结合)进行评估经常是不可行的。

[0051] 鉴于这些事实，为了提供更好的性能，各种方面包括移动设备和网络服务器，其配置成与云服务或网络(例如，抗病毒合作方、安全合作方等)联合工作以智能且有效地识别可能使移动设备随着时间在性能和功率利用级别方面降级起作用的因素。各种方面可以在不消耗移动设备的过多的处理、存储器、或能量资源的情况下在移动设备上识别使性能降级的因素。

[0052] 在一方面，移动设备的主处理内核的主观测器进程、守护进程、模块、或子系统(在本申请中统称为“模块”)可以在移动设备系统的各个级别装备或协调各个应用程序接口(API)，并从装备的API收集行为信息。在一方面，移动设备还可以包含分析器模块，且分析器模块可以生成一个或多个分类器模块和/或包含一个或多个分类器的分类器模块。观测器模块可以向移动设备的分类器模块和/或分析器模块(例如，通过存储器写操作等)传送(例如，通过存储器写操作、函数调用等)所收集的行为信息，其可以对所收集的行为信息进行分析和/或分类，生成行为向量，基于行为向量和从各种其他的移动设备子系统收集的信息生成空间和/或时间相关，以确定特定的移动设备行为、软件应用、或进程是良性的、可疑的、或恶意的/使性能降级的。

[0053] 在一方面，分析器模块和/或分类器模块可以包含在移动设备的分析器模块中或作为移动设备的分析器模块的一部分。在一方面，一个或多个分类器可以被生成为训练数据集的函数，其可以包括成千上万的特征和数十亿的条目。在一方面，一个或多个分类器可以从缩减的训练数据集生成，该缩减的训练数据集仅包括与确定特定的移动设备行为、软件应用、或进程是良性的、可疑的、或恶意的/使性能退化的最相关的特征/条目。

[0054] 在一方面，移动设备的分析器模块和/或分类器模块可以配置成执行实时分析操作，其可以包括对通过观测器模块收集的行为信息应用数据、算法、和/或行为模式以确定移动设备行为是良性的、可疑的、还是恶意的/使性能退化的。当分类器没有足够的信息来分类或决定性地确定该行为良性还是恶意的时候，分类器模块可以确定移动设备行为是可疑的。

[0055] 在一方面，移动设备的分类器模块可以配置成当设备行为是可疑的时候，将其实时分析操作的结果传送至观测器模块。观测器模块可以调整其观测的粒度(即，观测移动设备行为的详细级别)和/或基于从分类器模块接收的信息(例如，实时分析操作的结果)改变所观测的行为，生成或收集新的或另外的行为信息，以及向分类器模块发送新的/另外的信息以进行进一步分析/分类。

[0056] 在观测器与分类器模块之间的这样的反馈传送(例如，分类器模块向观测器模块发送其实时分析操作的结果，且观测器模块向分类器模块发送更新的行为信息)可以使移动设备处理器递归地增加观测的粒度(即，进行更细化或更具体的观测)或改变所观测的特征/行为直到识别可疑的源或使性能降级的移动设备行为为止，或直到达到处理或电池消耗阈值为止，或直到移动设备处理器确定无法从对观测粒度的进一步增加来识别可疑的源或使性能降级的移动设备行为为止。这样的反馈通信还使得移动设备处理器在不消耗过多的移动设备的处理、存储器、或能量资源的情况下在移动设备中本地的调整或修改数据/行为模型。

[0057] 在各个方面，移动设备可以配置成与包含离线分类器和/或实时在线分类器的网络服务器通信。离线分类器可以基于从云服务/网络接收的信息生成健壮的数据/行为模型。实时在线分类器可以基于对从云服务/网络接收的信息所生成的更大且更复杂的行为模型的分析来生成精简的数据/行为模型。在线和离线分类器都可以生成包含云服务/网络使其可用于特定移动设备的信息的缩减的子集的数据/行为模型。在一方面，生成精简的数据/行为模型可以包括生成一个或多个缩减的特征模型(RFM)。

[0058] 网络服务器可以向移动设备发送所生成的精简的数据/行为模型。移动设备可以接收并实现、应用、或使用精简的数据/行为模型来识别可以的或使性能降级的移动设备行为、软件应用、进程等。由于精简的时间/行为模型包括与云服务/网络使其可用的相关信息的缩减的子集，因此移动设备可以使用精简的数据/行为模型在不消耗移动设备过多的处理、存储器、或能量资源的情况下确定移动设备行为是否是恶意的/使性能降级的或良性的。然后，移动设备可以校正或防止所识别的使性能降级的移动设备行为是使移动设备的性能和功率利用级别降级。

[0059] 在各个方面，网络服务器可以配置成通过执行、运行、和/或应用机器学习和/或上下文建模技术到行为信息和/或由许多移动设备提供的行为分析的结果来生成或更新精简的数据/行为模式。从而，网络服务器可以从许多移动设备接收大量的报告并分析、合并或将这样的群包(crowd-sourced)信息变成可用的信息，尤其是可以由所有移动设备使用或访问的精简数据集或所关注的行为模型。网络服务器可以在从移动设备接收新的行为/分析报告时连续地重新评估现有的精简的数据/行为模型，和/或基于历史数据(例如，从先前的执行中收集的、行为模型的先前应用等)、新信息、机器学习、上下文建模、以及在获得信息中所检测的变化、移动设备状态、环境状况、网络状况、移动设备性能、电池消耗级别等来

生成新的或更新的精简的数据/行为模型。

[0060] 在一方面，网络服务器可以配置成生成包含初始特征集(例如，初始的缩减的特征模型)和一个或多个随后的特征集(例如，随后的缩减的特征模型)精简的数据/行为模型。初始特征集可以包括被确定为具有使移动设备的分类器模块能够决定性地确定特定的移动设备行为、软件应用、或进程是恶意的/使性能降级的还是良性的最高可能性的信息。每一随后的特征集可以包括被确定为具有决定性地确定移动设备行为、软件应用、或进程是恶意的/使性能降级的还是良性的次高可能性的信息。每一随后的特征集可以包括比其前面的特征集更大的数据集，并且从而针对每一随后的特征集，与应用该数据/行为模型相关联的性能和功耗成本可能逐渐增加。

[0061] 在一方面，移动设备的分类器模块可以包括或实现使移动设备处理器能够分阶段评估移动设备行为的渐进的行为模型(或分类器)。例如，分类器模块可以配置成先应用包括初始特征集的精简的数据/行为模型，然后应用包括逐渐地更大的特征集直到分类器模块确定移动设备行为是良性的还是恶意的/使性能降级的。然后，分类器模块可以向网络服务器发送与每一模型的应用相关联的其操作的结果和/或成功率。网络服务器可以使用这样的结果来更新该精简的数据/行为模型(例如，在每一模型中包含的特征集等)，从而基于所有进行报告的移动设备的结果/成功率对模型进行精化。然后，网络服务器可以使更新的精简的数据/行为模型可用于移动设备，从而其可以使用该精简的数据/行为模型。以此方式，移动设备可以从其他移动设备的行为和结论立即受益。

[0062] 在一方面，网络服务器可以配置成连续地更新在线和离线分类器、模型生成器、和/或云模型。网络服务器可以配置成确定何时变化实质的足够保证生成新的模型以及何时变化可以被忽略。例如，网络服务器可以从许多不同的移动设备接收更新，执行机器学习操作以生成第一族的分类器，确定针对所生成的第一族的分类器是否存在足够的变化以保证生成新的模型，当确定针对第一族的分类器存在足够的变化时，确定在所生成的第一族的分类器中哪些特征是最好的特征(例如，通过特征选择算法)，基于上述最好的特征生成第二族的分类器，确定针对所生成的第二族的分类器是否存在足够的变化，以及当确定针对第二族的分类器存在足够的变化时，生成/更新移动设备分类器数据/行为模型。

[0063] 各个方面可以包括客户端-云系统和网络架构，其在云中包含深度分类器和用于在移动设备上进行在线实时的功率有效的实现的精简分类器。在一方面，精简分类器可以比深度分类器少一个数量级或少得多(例如，在所评估的因素的数量、处理时间等方面)。例如，客户端-云系统的一方面可以包括评估500个因素的深度分类器和评估50个因素的精简分类器。类似地，客户端-云系统的一方面包括评估5000亿数据点的深度分类器和评估500亿数据点的精简分类器。

[0064] 分类器的每一执行/应用或针对所收集的行为信息的数据/行为模型可以提供适合改进现有的和未来的分类器和数据/行为模型的信息。例如，如果将数据/行为模型应用到在移动设备上收集的行为信息的结果将超过1Mbps的网络使用识别为恶意的，且移动设备确定所监测的进程正在消耗1.5Mbps的网络资源，则系统可以将该进程标记为恶意的并在不改变实际模型的情况下加强所应用的模型(例如，增加给予模型准确性的权重等)。作为另一示例，如果移动设备确定消耗.5Mbps网络资源的应用是恶意的(由其他属性导致的)，则系统可以将阈值降低到0.9Mbps来修改原始的云模型、精简模型、或两者。

[0065] 各个方面可以包括配置成应用能够对移动设备行为进行分阶段评估的渐进的分类器模型的移动设备。

[0066] 各个方面可以包括适合基于新的观测更新云中的全局模型、以及当存在足够的/充分的变化时更新移动设备模型的系统。

[0067] 可以在诸如在图1中示出的示例性通信系统100之类的各种通信系统中实现各个方面。典型的小区电话网络104包括耦合到网络操作中心108的多个小区基站106，其操作成连接在移动设备102(例如，小区电话、膝上型电脑、平板电脑等)与其他网络目的地之间的语音电话和数据，例如通过电话陆地线(例如，POTS网络，未示出)和因特网110。移动设备102与电话网络104之间的通信可以通过诸如4G、3G、CDMA、TDMA、LTE和/或其他的小区电话通信技术之类的双向无线通信链路112来完成。电话网络104还可以包括耦合到向因特网110提供连接的网络操作中心108或在该网络操作中心108中的一个或多个服务器114。

[0068] 通信系统100还可以包括连接到电话网络104和因特网110的网络服务器116。网络服务器116和电话网络104之间的连接可以通过因特网110或通过专用网络(如由虚线箭头所示出的)。网络服务器116还可以实现成在云服务提供商网络118的网络架构中的服务器。可以通过电话网络104、因特网110、专用网络(未示出)、或其任何组合来实现网络服务器116与移动设备102之间的通信。

[0069] 网络服务器116可以向移动设备102发送精简的数据/行为模型，移动设备102可以接收并使用精简的数据/行为模型来识别可疑的或使性能降级的移动设备行为、软件应用、进程等。网络服务器116还可以向移动设备102发送分类和建模信息以替换、更新、创建和/或维护移动设备数据/行为模型。

[0070] 移动设备102可以收集设备102中的行为、状态、分类、建模、成功率、和/或统计信息，并向网络服务器116发送所收集的信息(例如，经由电话网络104)以进行分析。网络服务器116可以使用从移动设备102接收的信息来更新或精化精简的数据/行为模型或分类/建模以包含进一步针对的和/或缩减的特征的子集。

[0071] 图2示出了在配置成确定特定的移动设备行为、软件应用、或进程是恶意的/使性能降级的、可疑的、还是良性的移动设备102的一方面的示例性逻辑组件和信息流。在图2中示出的示例中，移动设备102包括行为观测器模块202、行为分析器模块204、外部上下文信息模块206、分类器模块208、以及执行器模块210。在一方面，分类器模块208可以作为行为分析器模块204的一部分来实现。在一方面，行为分析器模块204可以配置成生成一个或多个分类器模块208，其每一个可以包含一个或多个分类器。

[0072] 模块202-210中的每一个可以在软件、硬件、或其任何组合中实现。在各个方面，模块202-210可以在操作系统的一部分中(例如，在内核中、在内核空间中、在用户空间中等)、在单独的程序或应用中、在专用的硬件缓冲器或处理器、或其任意组合中实现。在一方面，模块202-210中的一个或多个可以被实现为在移动设备102的一个或多个处理器上执行的软件指令。

[0073] 行为观测器模块202可以配置成装备或协调移动设备的各个级别/模块处的应用程序接口(API)，以及经由所装备的API监测/观测各个级别/模块处的移动设备操作和事件(例如，系统事件、状态变化等)，收集与所观测到的操作/事件有关的信息，智能地对所收集的信息进行过滤，基于经过滤的信息生成一个或多个观测，并将所生成的观测结果存储在

存储器中(例如,在日志文件中等)和/或向行为观测器模块204发送(例如,经过存储器写、函数调用等)所生成的观测结果。

[0074] 行为观测器模块202可以通过收集与在应用框架或实时库中的库API调用、系统调用API、文件系统和联网子系统操作、设备(包括传感器设备)状态变化、以及其它类似的事件有关的信息来监测/观测移动设备操作和事件。行为观测器模块202还可以监测文件系统活动,该文件系统活动可以包括搜索文件名、文件访问的类别(个人信息或正常数据文件)、创建或删除文件(例如,exe、zip等类型)、文件读/写/查找操作、改变文件权限等。

[0075] 行为观测器模块202还可以监测数据网络活动,其可以包括连接类型、协议、端口号、设备所连接到的服务器/客户端、连接的数目、通信的体量或频率等。行为观测器模块202可以监测电话网络活动,这可以包括监测所发出的、接收到的、或拦截的电话或消息(例如,SMS等)的类型和数目(例如,所拨打的高价电话的数目)。

[0076] 行为观测器模块202还可以监测/观测系统资源使用,这可以包括监测分叉(fork)数目、存储器访问操作、打开的文件数目等。行为观测器模块202可以监测移动设备的状态,这可以包括监测各种因素,诸如显示器是打开的还是关闭的、设备是锁定的还是未锁定的、剩余的电池量、照相机的状态等。行为观测器模块202还可以通过例如监测关键服务(浏览器、合约提供方等)的意图、进程间通信的程度、弹出窗口等来监测进程间通信(IPC)。

[0077] 行为观测器模块202还可以监测/观测一个或多个硬件组件的驱动器统计和/或状态,该一个或多个硬件组件可以包括照相机、传感器、电子显示器、WiFi通信组件、数据控制器、存储器控制器、系统控制器、访问端口、定时器、外围设备、无线通信组件、外部存储器芯片、电压调节器、振荡器、锁相环、外围桥路、以及用于支持移动计算机设备上的处理器和客户端的其它类似组件。

[0078] 行为观测器模块202还可以监测/观测表示移动计算设备和/或移动设备子系统的状态或状况的一个或多个硬件计数器。硬件计数器可以包括处理器/内核的专用寄存器,其配置成存储在移动计算设备中发生的与硬件相关的活动或事件的计数或状态。

[0079] 行为观测器模块202还可以监测/观测软件应用的动作或操作、从应用下载服务器(例如,Apple® App商店服务器)的软件下载、软件应用所使用的移动设备信息、呼叫信息、文本消息传送信息(例如,SendSMS、BlockSMS、ReadSMS等)、媒体消息传送信息(例如,ReceiveMMS)、用户账户信息、位置信息、照相机信息、加速计信息、浏览器信息、基于浏览器的通信的内容、基于语音的通信的内容、短距离无线通信(例如,蓝牙、WiFi等)、基于文本的通信的内容、录制的音频文件的内容、电话簿或联系人信息、联系人列表等。

[0080] 行为观测器模块202可以监测/观测移动设备的传输或通信,包括包含语音邮件(VoiceMailComm)、设备标识符(DeviceIDComm)、用户账户信息(UserAccountComm)、日历信息(CalendarComm)、位置信息(LocationComm)、录制的音频信息(RecordAudioComm)、加速计信息(AccelerometerComm)等的通信。

[0081] 行为观测器模块202可以监测/观测对指南针信息、移动设备设置、电池寿命、陀螺仪信息、压力传感器、磁传感器、屏幕活动等的使用和更新/改变。行为观测器模块202可以监测/观测传送给软件应用传送及来自软件应用的通知(AppNotification)、应用更新等。行为观测器模块202可以监测/观测与请求对第二软件应用的下载和/或安装的第一软件应用相关的条件或事件。行为观测器模块202可以监测/观测与诸如密码的输入等之类的用户

认证相关的条件或事件。

[0082] 行为观测器模块202还可以监测/观测在移动设备的多个级别处的条件或事件，其中包括应用级别、无线电级别和传感器级别。应用级别观测可以包括经由面部识别软件观测用户、观测社交流、观测用户输入的备注、观测与PassBook/Google Wallet/Paypal等的使用有关的事件。应用级别观测还可以包括观测与虚拟私有网络(VPN)的使用有关的事件以及与同步、语音搜索、语音控制(例如，通过说一个词锁定/解锁电话)、语音翻译器、用于计算的数据卸载、视频流传送、在没有用户活动的情况下的照相机使用、在没有用户活动的情况下的麦克风使用等相关的事件。

[0083] 无线电级别观测可以包括确定以下各项中的任何一个或多个的出现、存在性或数量：在建立无线通信链路或发送信息之前与移动设备的用户交互、双/多SIM卡、因特网无线电、移动电话系留、卸载用于计算的数据、设备状态传送、作为游戏控制器或家庭控制器使用、车辆通信、移动设备同步等。无线电级别观测还可以包括监测用于定位、对等(p2p)通信、同步、车辆对车辆通信、和/或机器对机器(m2m)的无线电(WiFi、WiMax、蓝牙等)的使用。无线电级别观测还可以包括监测网络业务使用、统计或简档。

[0084] 传感器级别观测可以包括监测磁传感器或其它传感器以确定移动设备的使用和/或外部环境。例如，移动设备处理器可以配置成确定电话是在皮套中(例如，经由配置成感测皮套中的磁铁的磁传感器)还是在用户的口袋中(例如，经由通过照相机或光传感器检测到的光的量)。检测移动设备在皮套中可能与识别可疑行为有关，例如，这是因为在移动设备在皮套中时发生与用户的活动使用(例如，照相或录像、发送消息、进行语音电话、录音等)有关的活动和功能可能是在该设备上执行的恶意进程(例如，跟踪或监视用户)的标志。

[0085] 与使用或外部环境有关的传感器级别观测的其它示例可以包括检测近场通信(NFC)、从信用卡扫描仪、条形码扫描仪、或移动标签阅读器收集信息、检测USB充电源的存在、检测键盘或辅助设备已经耦合到移动设备、检测移动设备已经耦合到计算设备(例如，经由USB等)、确定LED、闪光灯、手电筒、或光源是否已经被修改或禁用(例如，恶意地禁用紧急信号应用等)、检测扬声器或麦克风已经被打开或上电、检测充电或电源事件、检测移动设备被用作游戏控制器等。传感器级别观测还可以包括从医疗或保健传感器或从扫描用户的身体收集信息、从插入到USB/音频插座的外部传感器收集信息、从触觉或触感传感器收集信息(例如，经由振动器接口等)、收集与移动设备的热状态相关的信息等。

[0086] 为了将所监测的因素的数量缩减到可管理的级别，在一方面，行为观测器模块202可以通过监测/观测行为或因素的初始集来执行粗观测，上述行为或因素的初始集是可能对移动设备的降级起作用的所有因素的较小的子集。在一方面，行为观测器模块202可以从网络服务器116和/或云服务或网络118中的组件接收行为和/或因素的初始集。在一方面，可以在从网络服务器116或云服务/网络118接收的数据/行为模型中指定行为/因素的初始集。在一方面，可以在缩减的特征模型(RFM)中指定行为/因素的初始集。

[0087] 行为分析器模块204和/或分类器模块208可以从行为观测器模块202接收观测结果，将所接收的信息(即观测结果)与从外部上下文信息模块206接收的上下文信息进行比较，并识别与所接收的、对设备随着时间的降级起作用(或可能起作用)、或可能导致设备上的问题的观测结果相关联的子系统、进程、和/或应用。

[0088] 在一方面，行为分析器模块204和/或分类器模块208可以包括用于利用有限的信

息集(例如,粗观测结果)来识别对设备随时间降级起作用(或可能起作用),或可能在设备上导致问题的行为、进程、或程序的智能。例如,行为分析器模块204可以配置成分析从各种模块(例如,行为观测器模块202、外部上下文信息模块206等)收集的信息(例如,具有观测结果的形式)、学习移动设备的正常操作行为、以及基于比较的结果生成一个或多个行为向量。行为分析器模块204可以向分类器模块208发送所生成的行为向量以进行进一步分析。

[0089] 分类器模块208可以接收行为向量并将其与一个或多个行为模块进行比较以确定特定的移动设备行为、软件应用、或进行时使性能降级的/恶意的、良性的、还是可疑的。

[0090] 当分类器模块208确定一行为、软件应用、或进程是恶意的或使性能降级的时,分类器模块208可以通知执行器模块210,执行器模块210可以执行各种动作或操作以校正被确定为是恶意的或使性能降级的移动设备行为和/或执行操作以修复、矫正、隔离、或解决所识别的问题。

[0091] 当分类器模块208确定一行为、软件应用、或进程是可疑的时,分类器模块208可以通知行为观测器模块202,行为观测器模块202可以调整其观测的粒度(即,观测移动设备行为的详细级别)和/或基于从分类器模块208接收的信息(例如,实时分析操作的结果)改变所观测的行为、生成或收集新的或另外的行为信息、并向行为分析器模块204和/或分类器模块208发送新的/另外的信息以进行进一步分析/分类。在行为观测器模块202与分类器模块208之间的这样的反馈通信使移动设备102递归地增加观测的粒度(即,进行更细化或更详细的观测)或改变所观测的特征/行为直到识别出可疑的源或使性能降级的移动设备行为为止、直到达到处理或电池消耗阈值为止、或直到移动设备处理器确定无法从进一步增加观测粒度来识别可疑的源或使性能降级的移动设备行为为止。这样的反馈通信还是的移动设备102能够在移动设备中本地调整或修改数据/行为模型,而不消耗过多的移动设备的处理、存储器、或能量资源。

[0092] 在一方面,行为观测器模块202和行为分析器模块204可以提供,单独地或集体地,对计算系统的行为的实时行为分析以从有限的或粗观测结果中识别可疑的行为,以动态地确定要更详细观测的行为,并且以动态地确定观测所需的详细级别。以此方式,行为观测器模块202使移动设备102能够在不需要设备上的大量的处理器、存储器、或电池资源的情况下,有效地识别并避免在移动设备上发生问题。

[0093] 图3示出了在包括网络服务器116的系统300的一方面中的示例性组件和信息流,其中网络服务器116配置成与云服务/网络118联合工作以智能且有效地识别移动设备102上活动地恶意的或写得不好的软件应用和/或可以的或使性能降级的移动设备行为,而不消耗移动设备过多的处理、存储器、或能量资源。在图3中示出的示例中,网络服务器116包括云模块302、模型生成器304、以及训练数据模块306,且移动设备102包括行为观测器模块202、分类器模块208以及执行器模块210。在一方面,分类器模块208可以包含在行为分析器模块204中或作为行为分析器模块204的一部分(在图2中示出)。在一方面,模型生成器304可以是实时在线的分类器。

[0094] 云模块302可以配置成从云服务/网络118接收大量的信息并生成包含可能对移动设备随着时间降级起作用的所有或大部分的特征、数据点、和/或因素的完整的或健壮的数据/行为模型。

[0095] 模型生成器304可以基于在云模块302中生成的完整模型生成精简的数据/行为模

型。在一方面，生成精简的数据/行为模型可以包括生成一个或多个缩减的特征模型(RFM)，其包含在由云模块302所生成的完整模型中包含的特征和数据点的子集。在一方面，模型生成器304可以生成包含初始特征集(例如，初始的缩减的特征模型)的精简的数据/行为模型，该初始特征集包含被确定为具有使分类器208能够决定性地确定特定移动设备行为是恶意的/使性能降级的还是良性的最高可能性的信息。模型生成器304可以向行为观测器模块202发送所生成的精简模型。

[0096] 行为观测器模块202可以基于所接收的模型监测/观测移动设备行为，生成观测结果，并向分类器模块208发送观测结果。分类器模块208可以执行实时分析操作，其可以包括将数据/行为模型应用到由行为观测器模块202所收集的行为信息，以确定移动设备行为是良性的、可疑的、还是恶意的/使性能降级的。分类器模块208可以当其没有足够的信息来分类或决定性地确定该行为是良性的还是恶意的时确定移动设备行为是可疑的。

[0097] 分类器模块208可以配置成当分类器模块208确定设备行为是可疑的时向行为观测器模块202传送其实时分析操作的结果。行为观测器模块202可以调整其观测的粒度(即，观测移动设备行为的详细级别)和/或基于从分类器模块208接收的信息(例如，基于实时分析操作的结果)改变所观测的行为，生成或收集新的或另外的行为信息，以及向分类器模块发送新的或另外的信息以进行进一步的分析/分类(例如，以新模型的形式)。以此方式，移动设备102可以递归地增加观测的粒度(即，进行更细化或更详细的观测)或改变所观测的特征/行为直到识别出可疑的源或使性能降级的移动设备行为为止，直到达到处理或电池消耗阈值为止，或直到移动设备处理器确定无法从进一步增加的观测粒度来识别出可疑的源或使性能降级的移动设备行为为止。

[0098] 移动设备102可以向网络服务器116发送与模型的应用相关联的其操作的结果和/或成功率。网络服务器116可以基于上述结果/成功率生成训练数据(例如，经由训练数据模块306)以由模型生成器304使用。模型生成器可以生成更新的模型，并向移动设备102发送更新的模型。

[0099] 图4示出了生成一个或多个缩减的特征模型(RFM)以包含在完整特征模型(例如，在云模块302中生成的模型等)中包含的特征和数据点的子集的方法400的一方面。在各个方面，方法400可以在云模块302、模型生成器304、分类器模块208、或其任何组合中执行。在框402中，处理器可以执行分类算法以根据从云服务/网络118接收的大量数据(例如，数十亿的数据点、成千上万的特征等)来建立决策树(或其他类似的结构)。在一方面，分类算法可以包括推进的决策树(BDT)算法或任何其它类似的分类或进行决策的算法。

[0100] 在框404中，处理器可以根据决策树或结构生成初始的缩减的特征集(例如，RFM0)。初始的缩减的特征集(例如，RFM0)可以包括被确定为具有使分类器模块能够决定性地确定特定移动设备行为是恶意的还是良性的最高可能性的信息。在框406中，处理器可以根据决策树或结构生成随后的缩减的特征集(例如，RFM1)，以包括被确定为具有使分类器模块能够决定性地确定特定移动设备行为是恶意的还是良性的次最高可能性的信息。在框408中，处理器可以根据决策树或结构生成另外的随后的特征集(例如，RFMn)。

[0101] 每一随后的特征集(例如，RFM1-RFMn)可以包括比其前一个特征集更大的数据集。例如，如果决策树或结构标识了一千(1000)个相关的因素，则初始的缩减的特征集(例如，RFM0)可以包括被确定为具有使移动设备的分类器模块能够决定性地确定移动设备行为是

恶意的还是良性的最高可能性的50个因素。第一随后的缩减的特征集(例如,RFM1)可以包括接下来的一百(100)个因素,且随后的缩减的特征集(例如,RFMn)可以包括剩下的八百五十(850)个因素。

[0102] 图5A示出了基于一个或多个缩减的特征模型(RFM)建立精简的移动设备分类器模型的系统方法500的一方面。在操作502中,网络服务器处理器可以应用机器学习技术以生成描述行为向量的云语料库512的第一族的分类器模型(例如,通过生成推进的决策树等)。行为向量的云语料库512可以包括从许多不同的移动设备(例如,一千万移动设备)收集的一大群行为向量(例如,十亿个行为向量)。

[0103] 在操作504中,网络服务器处理器可以对具有使移动设备的分类器/分析器模块能够决定性地确定特定移动设备行为是恶意的还是良性的最高可能性的特征进行识别并形成组。在操作506中,网络服务器处理器可以将所识别的最佳特征514应用到行为向量的云语料库512。在操作508中,网络服务器处理器可以生成与使分类器/分析器模块能够决定性地确定特定移动设备行为是恶意的还是良性的有关的明显缩减的特征的、新的族的缩减的特征模型。在操作510中,网络服务器处理器可以向移动设备102发送缩减的特征模块。

[0104] 图5B示出了基于一个或多个缩减的特征模型(RFM)建立精简的移动设备分类器模型的系统方法550的另一方面。在操作552中,网络服务器处理器可以应用机器学习技术来生成描述行为向量的语料库512的一族的分类器模型(例如,通过生成推进的决策树等)。在操作554中,网络服务器处理器可以对具有使移动设备的分类器/分析器模块能够决定性地确定移动设备行为是恶意的还是良性的最高可能性的特征进行识别并形成组。在操作556中,网络服务器处理器可以生成新的族的缩减的特征模型,该新的族的缩减的特征模型标识了与使分类器/分析器模块能够决定性地确定移动设备行为是恶意的还是良性的有关的明显缩减的特征。在一方面,网络服务器处理器可以基于所识别的最佳特征514来生成新的族的缩减的特征模块。在操作556中,网络服务器处理器可以向移动设备102发送缩减的特征模块。

[0105] 图6示出了在移动设备102中的示例性逻辑组件、信息流,该移动设备102配置成执行分阶段评估移动设备行为的渐进的分析方法600的一方面。在图6中示出的示例中,移动设备102包括行为分析器模块204,该行为分析器模块204包括初始的缩减的特征集(例如,RFM0)模块以及多个随后的缩减的特征集(例如,RFM1-RFMn),其每一个可以是分类器模块208。在操作602中,行为分析器模块202可以基于所接收的模型监测/观测移动设备行为,生成观测结果,并向初始的缩减的特征集(例如,RFM0)模块发送观测结果。

[0106] 初始的缩减的特征集(例如,RFM0)模块可以接收观测结果并确定特定的移动设备行为、软件应用、或进程是使性能降级的/恶意的、良性的、还是可疑的。当初始的缩减的特征集(例如,RFM0)模块确定一行为、软件应用、或进程是良性的、恶意的或使性能降级的时,在操作604a中,初始的缩减的特征集(例如,RFM0)模块可以通知执行器模块210,该执行器模块210可以执行各种动作或操作以校正被确定为是恶意的或使性能降级的移动设备行为和/或执行操作以修复、矫正、隔离、或解决所识别的问题。

[0107] 当初始的缩减的特征集(例如,RFM0)模块确定一行为、软件应用、或进程是可疑的时,在操作604b中,初始的缩减的特征集(例如,RFM0)模块可以向行为观测器模块202发送通知消息,行为观测器模块202可以调整其观测的粒度(即,观测移动设备行为的详细级别)

和/或基于从初始的缩减的特征集(例如,RFM0)模块接收的信息(例如,实时分析操作的结果)来改变行为,并生成或收集新的或另外的行为信息。在操作606中,行为分析器模块202可以向第一随后的缩减的特征集(例如,RFM1)模块发送新的/另外的信息以进行进一步的分析/分类。

[0108] 第一随后的缩减的特征集(例如,RFM1)模块可以接收上述另外的信息并确定特定的移动设备行为、软件应用、或进程是使性能降级的/恶意的、良性的、还是可疑的。当第一随后的缩减的特征集(例如,RFM1)模块确定一行为、软件应用、或进程是良性的、恶意的或使性能降级的时,在操作608a中,第一随后的缩减的特征集(例如,RFM1)模块可以通知执行器模块210,该执行器模块210可以执行各种动作或操作以校正被确定为是恶意的或使性能降级的移动设备行为和/或执行操作以修复、矫正、隔离、或解决所识别的问题。

[0109] 当第一随后的缩减的特征集(例如,RFM1)模块确定一行为、软件应用、或进程是可疑的时,在操作608b中,第一随后的缩减的特征集(例如,RFM1)模块可以向行为观测器模块202发送通知消息,行为观测器模块202可以调整其观测的粒度和/或基于从第一随后的缩减的特征集(例如,RFM1)模块接收的信息来改变行为,并生成或收集新的或另外的行为信息。在操作610中,行为分析器模块202可以向另一随后的缩减的特征集(例如,RFMn)模块发送新的/另外的信息以进行进一步的分析/分类。操作606-610可以重复地执行直到行为分析器模块204决定性地确定该行为、软件应用、或进程是良性的还是恶意的。

[0110] 图7示出了在包含网络服务器116的系统700的一方面中的示例性组件和信息流,该网络服务器116配置成从多个移动设备接收更新。

[0111] 图8A示出了根据行为向量的云语料库512建立精简的移动设备分类器模型的服务器/系统方法800的一方面,其中上述行为向量的云语料库512连续地从多个移动设备接收更新的信息。在操作802中,服务器处理器可以应用机器学习技术来生成描述行为向量的云语料库512的更新的第一族的分类器模型(例如,通过生成提升的决策树等)。在确定操作804中,服务器处理器可以确定针对第一族的分类器模型的改变是否显著。

[0112] 当确定第一族的分类器模型改变不显著(确定操作804=“否”)时,在操作816中,该方法800可以结束。当确定第一族的分类器模型改变显著(确定操作804=“是”)时,在操作806中,服务器处理器可以对被确定为具有使移动设备的分类器/分析器模块能够决定性地确定移动设备行为是恶意的还是良性的最高可能性的特征进行识别并形成组。

[0113] 在操作806中,服务器处理器可以将所识别的最佳特征应用到行为向量的云语料库512。在操作810中,服务器处理器可以生成第二族的分类器,其包括识别与使分类器/分析器模块能够决定性地确定移动设备行为是恶意的还是良性的有关的明显缩减的特征的缩减的特征模块。在确定操作812中,服务器处理器可以确定所生成的第二族的分类器是否包括与先前的模型明显不同的缩减的特征模块,以保证生成更新的移动设备分类器。当确定在第二族的分类器中没有足够的变化来保证生成更新的移动设备分类器(确定操作812=“否”)时,在操作816中,方法800可以结束。当确定在第二族的分类器中存在足够的变化来保证生成更新的移动设备分类器(确定操作812=“是”)时,在操作814中,系统可以生成包括缩减的特征模块中的一个或多个的更新的移动设备分类器,并向移动设备102发送移动设备分类器。

[0114] 图8B示出了根据行为向量的云语料库512建立精简的移动设备分类器模型的服务

器/系统方法850的另一方面，其中上述行为向量的云语料库512连续地从多个移动设备接收更新的信息。在操作852中，服务器处理器可以应用机器学习技术来生成描述行为向量的云语料库512的更新的第一族的分类器模型(例如，通过生成推进的决策树等)。在确定操作854中，服务器处理器可以确定针对第一族的分类器模型的改变是否显著。

[0115] 当确定第一族的分类器模型改变不显著(确定操作854＝“否”)时，在操作864中，该方法850可以结束。当确定第一族的分类器模型改变显著(确定操作854＝“是”)时，在操作856中，服务器处理器可以对被确定为具有使移动设备的分类器/分析器模块能够决定性地确定移动设备行为是恶意的还是良性的最高可能性的特征进行识别并形成组。在操作858中，服务器处理器可以生成第二族的分类器，其包括识别与使分类器/分析器模块能够决定性地确定移动设备行为是恶意的还是良性的有关的明显缩减的特征的缩减的特征模块。在确定操作860中，服务器处理器可以确定所生成的第二族的分类器是否包括与先前的模型明显不同的缩减的特征模块，以保证生成更新的移动设备分类器。

[0116] 当确定在第二族的分类器中没有足够的变化来保证生成更新的移动设备分类器(确定操作812＝“否”)时，在操作864中，方法850可以结束。当确定在第二族的分类器中存在足够的变化来保证生成更新的移动设备分类器(确定操作860＝“是”)时，在操作862中，系统可以生成包括缩减的特征模块中的一个或多个的更新的移动设备分类器，并向移动设备102发送移动设备分类器。

[0117] 图9示出了在配置成根据一方面执行动态且自适应的观测的计算系统的行为观测器模块202中的示例性逻辑组件和信息流。行为观测器模块202可以包括自适应过滤器模块902、抑制模块904、观测器模式模块906、高级别行为检测模块908、行为向量生成器910、以及安全缓冲器912。高级别行为检测模块908可以包括空间相关模块914和时间相关模块916。

[0118] 观测器模式模块906可以从各个源接收控制信息，其可以包括分析器单元(例如，上文参考图2描述的行为分析器模块204)和/或应用API。观测器模式模块906可以向自适应过滤器模块902和高级别行为检测模块908发送与各种观测器模式相关的控制信息。

[0119] 自适应过滤器模块902可以从多个源接收数据/信息，并对所接收的信息进行智能地过滤以生成从所接收的信息中选择的信息的较小子集。可以基于从分析器模块、或通过API传送的较高级别进程接收的信息或控制来调整该过滤器。可以向抑制模块904发送经过过滤的信息，抑制模块904可以负责控制从过滤器流出的信息量以确保高级别行为检测模块908不变得被请求或信息淹没或过载。

[0120] 高级别行为检测模块908可以从抑制模块904接收数据/信息，控制来自观测器模式模块906的信息以及来自移动设备的其他组件的上下文信息。高级别行为检测模块908可以使用所接收的信息来执行空间的或时间的相关以检测或识别可能导致设备以次优的级别执行的高级别行为。可以向行为向量生成器910发送空间和时间相关的结果，该行为向量生成器910可以接收该相关信息并生成描述特定进程、应用、或子系统的行为的行为向量。在一方面，行为向量生成器910可以生成行为向量，使得特定进程、应用、或子系统的每一高级别行为是行为向量的一个元素。在一方面，所生成的行为向量可以存储在安全缓冲器912中。高级别行为检测的示例可以包括检测特定事件的存在、另一事件的数量或频率、多个事件之间的关系、事件发生的顺序、特定事件的发生之间的时间差等。

[0121] 在各个方面，行为观测器模块202可以执行自适应观测以及控制观测粒度。即，行为观测器模块202可以动态地识别要观测的相关行为，并动态地确定要观测所识别的行为的详细级别。以此方式，行为观测器模块202使得系统能够在各个级别(例如，多个粗糙的和细化的级别)来监测移动设备的行为。行为观测器模块202可以使系统能够与正被观测内容的相适应。行为观测器模块202可以使系统能够基于可以从各种源获得的所关注的信息的子集来动态地改变正被观测的因素/行为。

[0122] 如上文所讨论的，行为观测器模块202可以基于从各种源接收的信息执行自适应观测技术和控制观测粒度。例如，高级别行为检测模块908可以从抑制模块904、观测器模块906接收信息，以及从移动设备的其他组件(例如，传感器)接收上下文信息。作为示例，执行时间相关的高级别行为检测模块908可能检测到照相机已经被使用且移动设备正试图将相片上载到服务器。高级别行为检测模块908还可以执行时间相关以确定移动设备上的应用是否在设备装在皮套中且系在用户的腰带上的同时在拍照。高级别行为检测模块908可以确定所检测的高级别行为(例如，在装在皮套中的同时使用照相机)是否为可接受的或常见的行为，这可以通过将当前的行为与该移动设备的过去的行为进行比较和/或访问从多个设备收集的信息(例如，从群包服务器接收的信息)来实现。由于当在皮套中时拍照并将照片上载到服务器是不寻常的行为(如根据在装在皮套中的背景下所观测到的正常行为所可以确定的)，在该情形下，高级别行为检测模块908可以将此识别为潜在的威胁行为并发起适当的响应(例如，关闭照相机、发出警报等)。

[0123] 在一方面，行为观测器模块202可以在多个部分中实现。

[0124] 图10示出了在实现观测器守护进程的一方面的计算系统1000中的逻辑组件和信息流。在图10中示出的示例中，计算系统1000包括行为检测器1002模块、数据库引擎1004模块、以及在用户空间中的行为分析器模块204、以及环形缓冲器1014、过滤器规则1016模块、抑制规则1018模块、以及在内核空间中的安全缓冲器1020。计算系统1000还可以包括观测器守护进程，该观测器守护进程包括在用户空间中的行为检测器1002以及数据库引擎1004，以及在内核空间中的安全缓冲器管理器1006、规则管理器1008、以及系统健康监测器1010。

[0125] 各个方面可以对包含webkit，、SDK、NDK、内核、驱动器以及硬件的移动设备上提供跨层观测，以描述系统行为的特征。可以实时进行上述行为观测。

[0126] 观测器模块可以执行自适应观测技术并控制观测粒度。如上文所讨论的，存在对移动设备的降级起作用的大量的(即，成千上万的)因素，并且对可能对设备的性能降级起作用的所有不同因素进行监测/观测是不可行的。为了克服这点，各个方面动态地识别要观测的有关行为，并动态地确定要以哪一详细级别来观测所识别的行为。

[0127] 图11示出了用于根据一方面执行动态且自适应观测的示例性方法1100。在框1102中，移动设备处理器可以通过监测/观测可能对移动设备的降级起作用的大量因素/行为的子集来执行粗观测。在框1103中，移动设备处理器可以生成描述粗观测和/或基于粗观测的移动设备行为的特征的行为向量。在框1104中，移动设备处理器可以识别与对移动设备的降级潜在起作用的粗观测相关联的子系统、进程、和/或应用。例如，这可以通过将从多个源接收的信息与从移动设备的传感器接收的上下文的信息进行比较来实现。在框1106中，移动设备处理器可以基于粗观测执行行为分析操作。在一方面，作为框1103和1104的一部分，

移动设备处理器可以执行上文参考图2-8B所讨论的操作中的一个或多个。

[0128] 在确定框1108中，移动设备处理器可以基于行为分析的结果来确定可疑的行为或潜在的问题是否可以被识别和校正。当移动设备处理器基于行为分析的结果确定可疑的行为或潜在的问题可以被识别和较正(即，确定框1108＝“是”)时，在框1118中，处理器可以发起用于校正行为的进程，并返回框1102以执行另外的粗观测。

[0129] 当移动设备处理器基于行为分析的结果确定可疑的行为或潜在的问题不能被识别和/或较正(即，确定框1108＝“否”)时，在确定框1109中，移动设备处理器可以确定是否存在有问题的可能性。在一方面，移动设备处理器可以通过计算移动设备遭遇潜在问题和/或进行可疑行为的概率以及确定所计算的概率是否大于预定的阈值来确定存在问题的可能性。当移动设备处理器确定所计算的概率不大于预定的阈值和/或没有存在可疑行为或潜在问题的可能性和/或没有可疑行为或潜在问题可检测的可能性(即，确定框1109＝“否”)时，处理器可以返回框1102以执行另外的粗观测。

[0130] 当移动设备处理器确定有存在可疑行为或潜在问题的可能性和/或有可疑行为或潜在问题可检测的可能性(即，确定框1109＝“是”)时，在框1110中，移动设备处理器可以对所识别的子系统、进程或应用执行更深的记录/观测或最后的记录。在框1112中，移动设备处理器可以对所识别的子系统、进程或应用执行更深入且更详细的观测。在框1114中，移动设备处理器可以基于上述更深入且更详细的观测来执行进一步的和/或更深的行为分析。在确定框1108中，移动设备处理器可以基于上述更深入的行为分析的结果再次确定是否可以识别并校正可疑行为或潜在问题。当移动设备处理器基于上述更输入行为分析的结果确定不能识别和校正可疑行为或潜在问题(即，确定框1108＝“否”)时，处理器可以重复在框1110-1114中的操作直到详细的级别细化地足够识别问题为止或直到确定利用另外的细节无法识别问题或不存在问题为止。

[0131] 当移动设备处理器基于上述更深入的行为分析的结果确定可以识别并校正可疑行为或潜在的问题(即，确定框1108＝“是”)时，在框1118中，移动设备处理器可以执行操作以校正问题/行为，且处理器可以返回框1102以执行另外的操作。

[0132] 在一方面，作为方法1100的框1102-1118的一部分，移动设备处理器可以执行系统行为的实时行为分析，以从有限且粗糙的观测中识别可疑的行为，以动态地确定要更详细观测的行为，以及动态地确定观测所需的精确的详细级别。这使得移动设备处理器能够有效地识别并避免问题发生，而无需使用设备上的大量处理器、存储器、或电池资源。

[0133] 各个方面可以在各种移动计算设备上实现，在图12中以智能电话的形式示出了其一示例。智能电话1202可以包括耦合到内部存储器1202、显示器1203、以及耦合到扬声器的处理器1201。另外，智能电话1202可以包括用于发送和接收电磁辐射的天线1204，天线1204可以连接到无线数据链路和/或耦合到处理器1301的蜂窝电话收发机1205。智能电话1202典型地还包括用于接收用户输入的菜单选择按钮或摇臂开关1206。

[0134] 典型的智能电话1202还包括声音编码/解码(编解码器)电路1212，其将从麦克风接收的声音数字化成适合无线传输的数据分组并将所接收的声音数据分组解码以生成提供给扬声器以生成声音的模拟信号。此外，处理器1201、无线收发机1205和编解码器1212中的一个或多个可以包括数字信号处理器(DSP)电路(未分别示出)。

[0135] 可以以客户端-服务器架构来实现方法的一方面的一部分，其中一些处理发生在

服务器中，例如维护正常操作行为的数据库，该数据库可以由移动设备处理器在执行本方面的方法时访问。这样的方面可以在诸如在图13中示出的服务器1300之类的各种市售的服务器设备中的任何一个上实现。这样的服务器1300典型地包括处理器1301，其耦合到易失性存储器1302和诸如磁盘驱动器1303之类的大容量非易失性存储器。服务器1300还可以包括耦合到处理器1301的软盘驱动器、压缩盘(CD)或DVD光盘驱动器13011。服务器1300还可以包括用于与网络1305建立数据连接的、耦合到处理器1301的网络访问端口1304，上述网络1305例如为耦合到其他广播系统计算机和服务器的局域网。

[0136] 处理器1201、1301可以是可以由软件指令(应用)配置成执行各种功能的任何可编程微处理器、微计算机或多处理器芯片，上述各种功能包括下文所描述的各个方面的功能。在一些移动设备中，可以提供多个处理器1201，例如一个处理器专用于无线通信功能以及一个处理器专用于运行其他应用。典型地，软件应用可以在其被访问并装载到处理器1201、1301中之前存储在内部存储器1202、1302、1303中。处理器1201、1301可以包括足够存储应用软件指令的内部存储器。

[0137] 用于在可编程处理器上执行的、以实现各个方面的操作的计算机程序代码或“程序代码”可以以诸如C、C++、C#、Smalltalk、Java、JavaScript、Visual Basic、结构化的查询语言(e.g.,Transact-SQL)、Perl之类的高级编程语言或以各种其他的编程语言来写。如在本申请中所使用的、存储在计算机可读存储介质上的程序代码或程序可以指其格式可以由处理器理解的机器语言代码(例如，对象代码)。

[0138] 许多移动计算设备操作系统内核被组织到用户空间(非特权代码在其中运行)以及内核空间(特权代码在其中运行)中。该分离在安卓®以及其他的通用公共授权(GPL)环境中是尤其重要的，在GPL环境中是内核空间的一部分的代码必需是GPL授权的，而在用户空间运行的代码可以不是GPL授权的。应该理解的是，除非明确表明，否则，在此讨论的各种软件组件/模块可以在内核空间或用户空间中实现。

[0139] 仅提供前述的方法描述和过程流图作为说明性示例，且其不意在需要或隐含必需按照所呈现的顺序来执行各个方面的步骤。如将由本领域的技术人员明白的，在前述方面中的步骤的顺序可以以任何顺序来执行。诸如“其后”、“然后”、“接下来”等之类的词不意在限制步骤的顺序；这些词仅用于指导读者浏览方法的描述。此外，任何对权利要求元素的单数引用，例如，使用冠词“一”、“一个”或“该”，不被解释为将该元素限制为单数。

[0140] 如在本申请中所使用的，术语“组件”、“模块”、“系统”、“引擎”、“生成器”、“管理器”等意在包括计算机相关的实体，例如但不限于硬件、固件、硬件和软件的组合、软件、或执行的软件，其配置成执行特定的操作或功能。例如，组件可以是但不限于在处理器上运行的进程、处理器、对象、可执行程序、执行的线程、程序、和/或计算机。通过说明的方式，在计算设备上运行的应用和计算设备可以被称为组件。一个或多个组件可以位于进程和/或执行的线程内，且组件可以位于一个处理器或内核上，和/或在两个或更多个处理器或内核之间分布。此外，这些组件可以从其上存储有各种指令和/或数据结构的各种非暂时性计算机可读介质执行。组件可以通过本地和/或远程进程、函数或过程调用、电子信号、数字分组、存储器读/写、以及其他已知的网络、计算机、处理器、和/或与进程相关的通信方法来进行通信。

[0141] 结合本申请中所公开的方面描述的各种示例性的逻辑框、模块、电路和算法步骤

均可以实现成电子硬件、计算机软件或其组合。为了清楚地表示硬件和软件之间的可交换性，上面对各种示例性的部件、框、模块、电路和步骤均围绕其功能进行了总体描述。至于这种功能是实现成硬件还是实现成软件，取决于特定的应用和对整个系统所施加的设计约束条件。熟练的技术人员可以针对每个特定应用，以变通的方式实现所描述的功能，但是，这种实现决策不应解释为背离本发明的保护范围。

[0142] 用于执行本申请所述功能的通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件或者其任意组合，可以实现或执行用于实现结合本申请中公开的方面所描述的各种示例性的逻辑、逻辑框、模块和电路的硬件。通用处理器可以是微处理器，或者，该处理器也可以是任何常规的处理器、控制器、微控制器或者状态机。处理器也可能实现为计算设备的组合，例如，DSP和微处理器的组合、多个微处理器、一个或多个微处理器与DSP内核的结合，或者任何其它此种结构。或者，一些步骤或方法可以由特定于给定功能的电路来执行。

[0143] 在一个或多个示例性的方面，所描述的功能可以用硬件、软件、固件或其任意组合的方式来实现。如果使用软件实现，则可以将这些功能存储在非暂时性计算机可读介质或非暂时性处理器可读介质上作为一个或多个指令或代码。本申请中公开的方法或算法的步骤可以包含在可以位于非暂时性计算机可读或处理器可读存储介质上的处理器可执行软件模块中。非暂时性计算机可读或处理器可读存储介质可以是可以由计算机或处理器存取的任何存储介质。通过示例的方式而不是限制的方式，这种非暂时性计算机可读或处理器可读介质可以包括RAM、ROM、EEPROM、闪速存储器、CD-ROM或其它光盘存储、磁盘存储介质或其它磁存储设备、或者能够用于存储具有指令或数据结构形式的期望的程序代码并可以由计算机进行存取的任何其它介质。如本申请中所使用的，磁盘和光盘包括压缩盘(CD)、激光盘、光盘、数字多功能光盘(DVD)、软盘和蓝光盘，其中磁盘通常磁性地复制数据，而光盘则用激光来光学地复制数据。上面的组合也包括在非暂时性计算机可读和处理器可读介质的保护范围之内。或者，方法或算法的操作可以位于非暂时性处理器可读介质和/或计算机可读介质上作为代码和/或指令中的一个或其任何组合或一组代码和/或指令，其可以并入到计算机程序产品中。

[0144] 为使本领域中的任何技术人员能够实现或者使用本发明，提供了对所公开的方面的上述描述。对于本领域技术人员来说，对这些方面的各种修改将是显而易见的，并且，本申请定义的总体原理也可以在不脱离本发明的精神或保护范围的基础上适用于其它方面。因此，本发明并不意在受限于本申请中示出的方面，而是与随后的权利要求书以及本申请中公开的原理和新颖性特征的最广范围相一致。

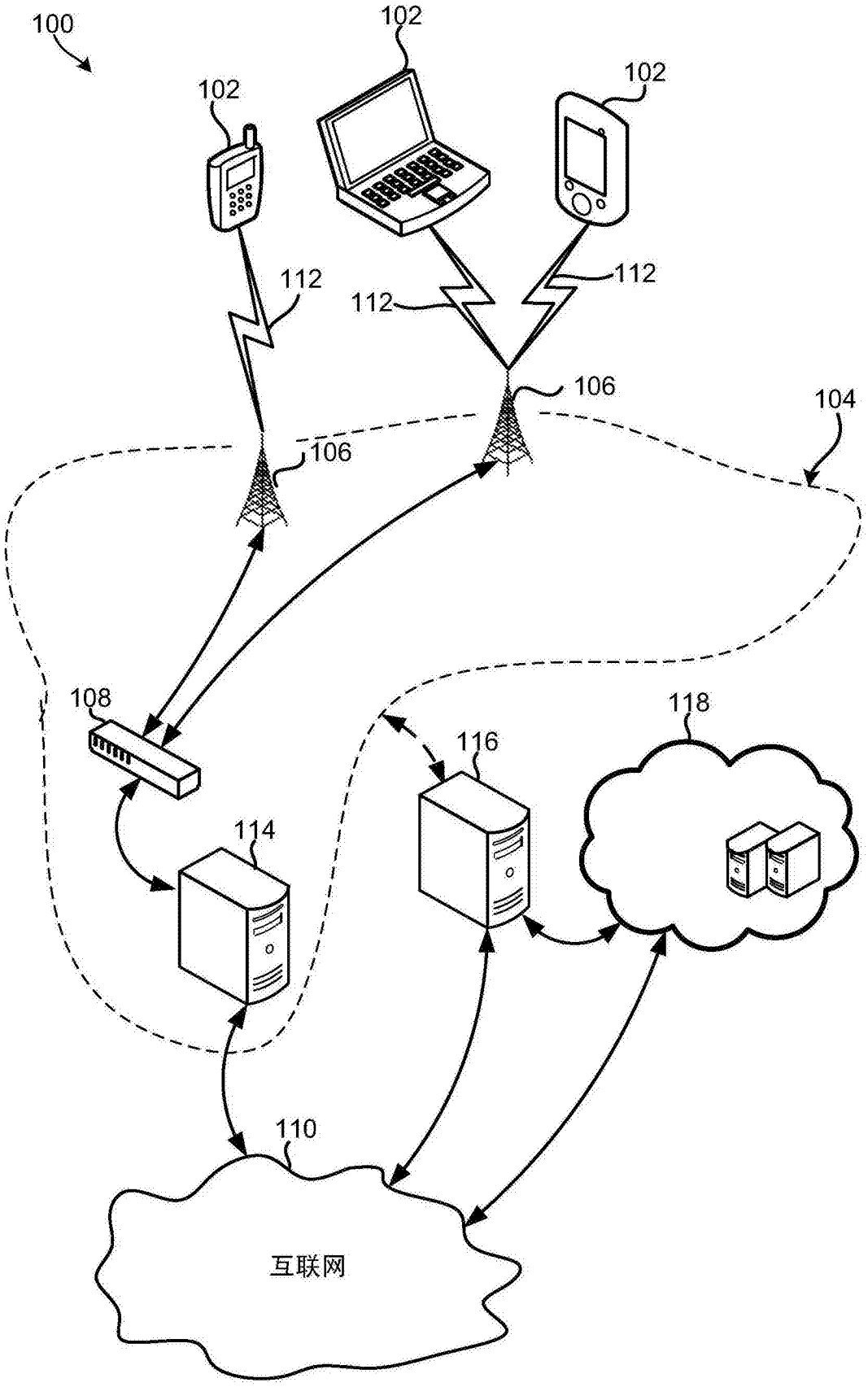


图1

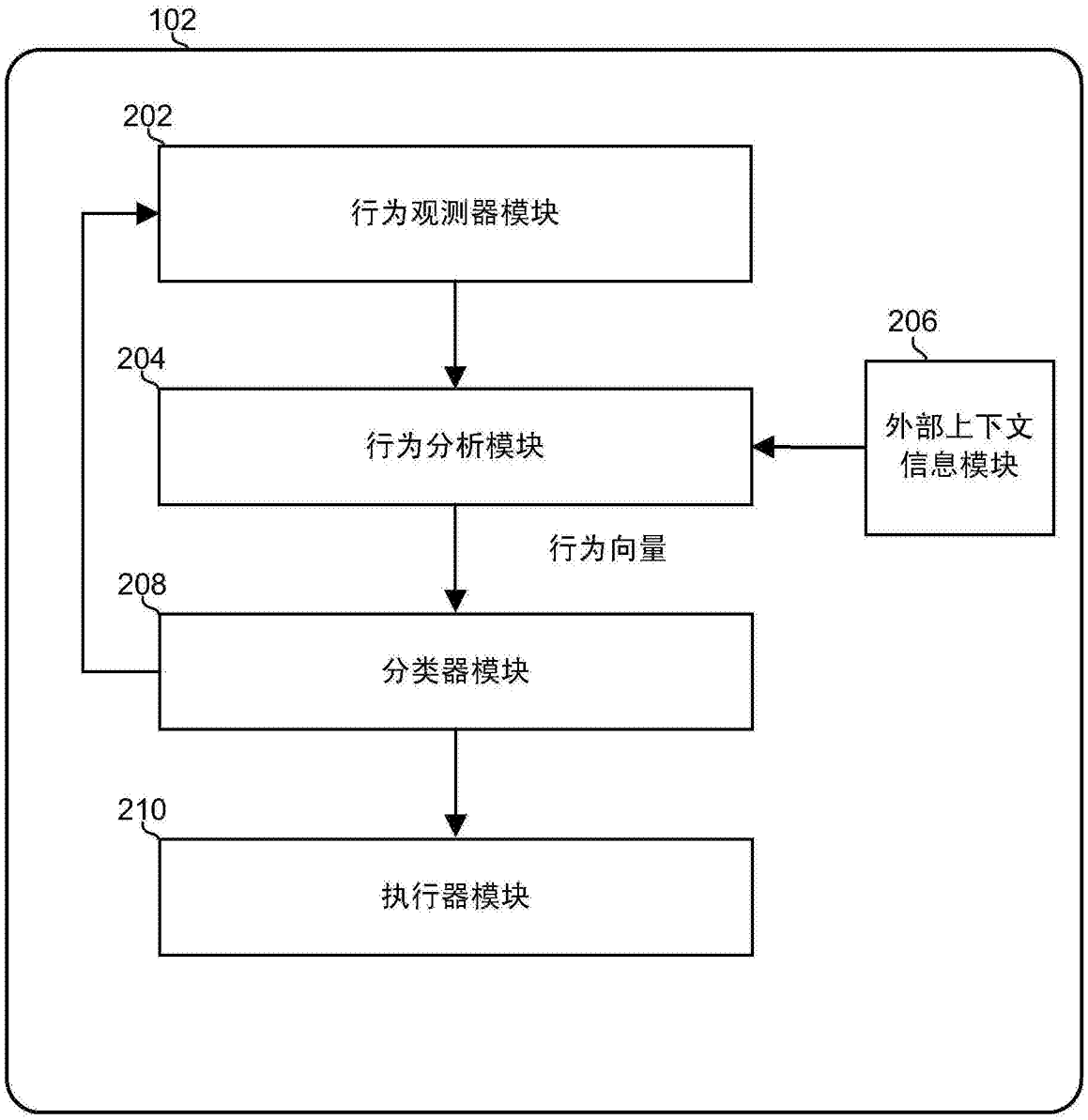

102
202
行为观测器模块
206
204
外部上下文
信息模块
行为分析模块
行为向量
208
分类器模块
210
执行器模块

图2

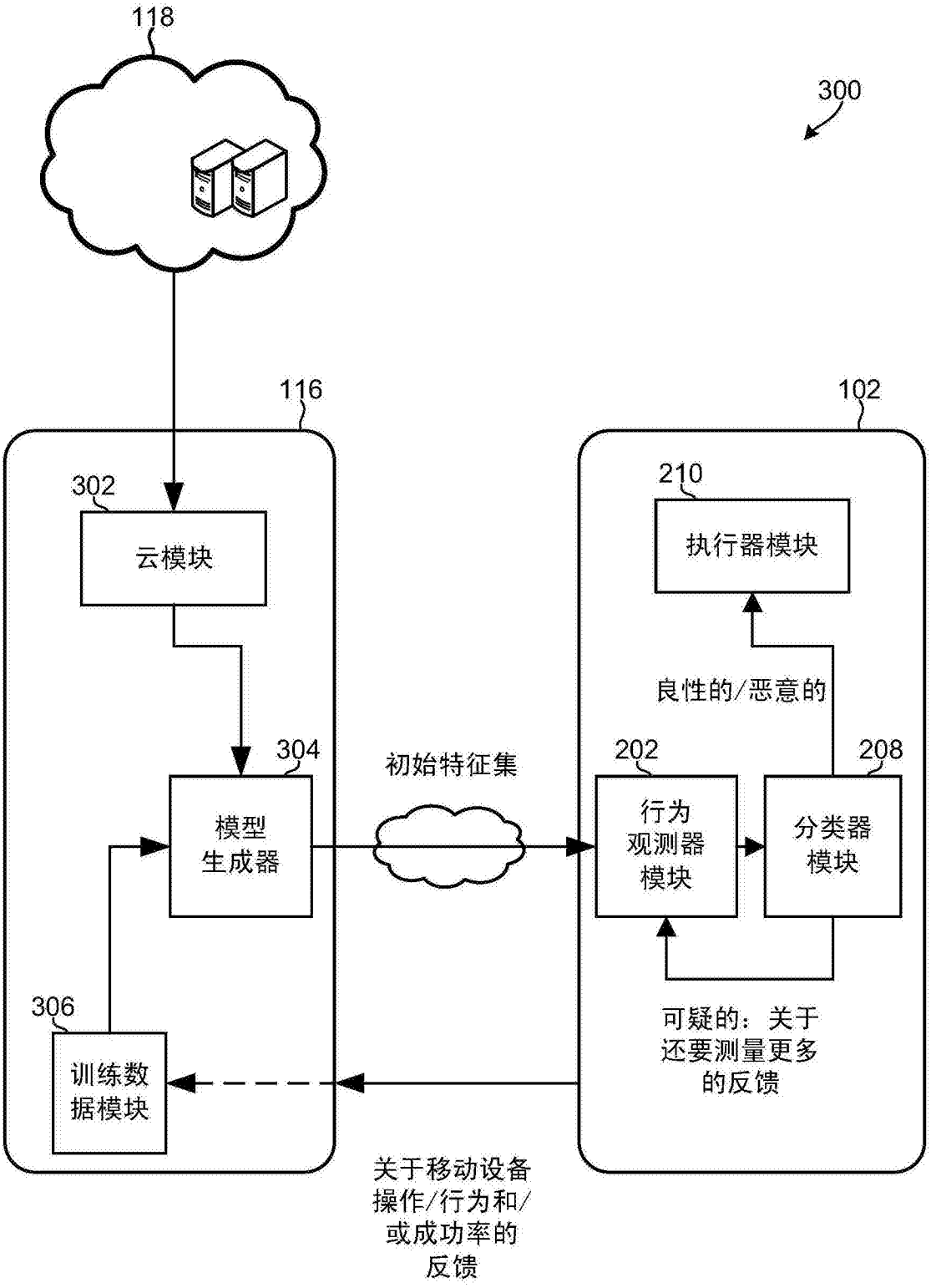

118
300
116
102
302
云模块
210
执行器模块
良性的/恶意的
304
初始特征集
202
208
模型
生成器
行为
观测器
模块
分类器
模块
306
训练数
据模块
可疑的：关于
还要测量更多
的反馈
关于移动设备
操作/行为和/
或成功率的
反馈

图3

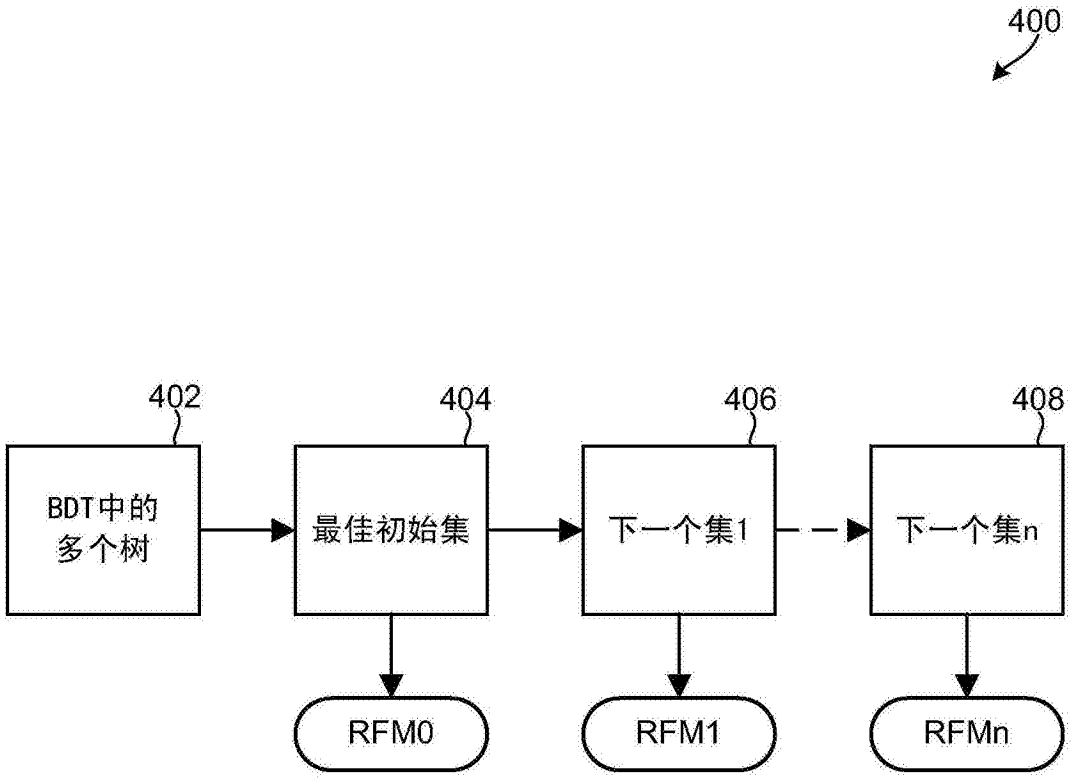

400
402
404
406
408
BDT中的
多个树
最佳初始集
下一个集1
下一个集n
RFM0
RFM1
RFMn

图4

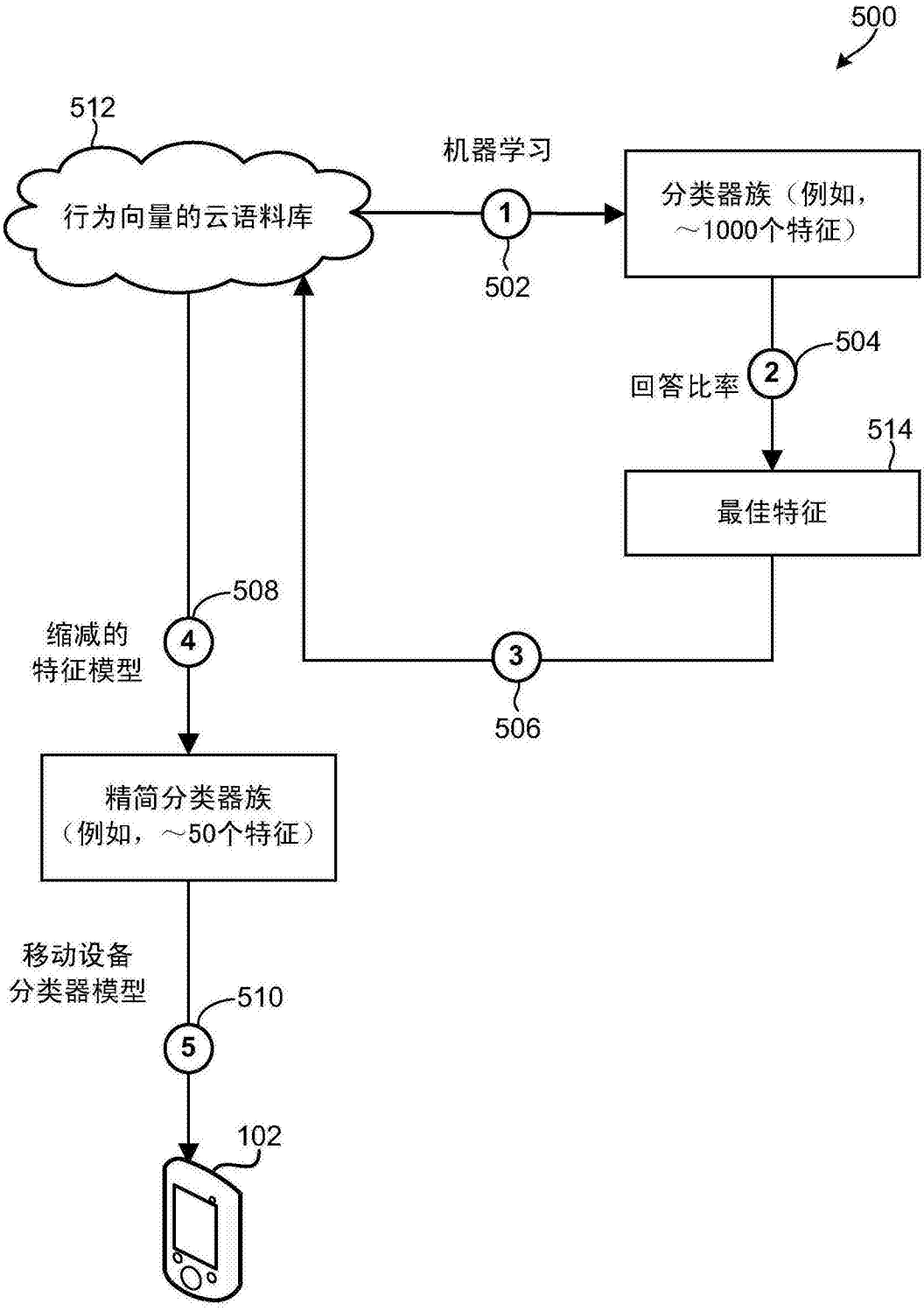

500
512
行为向量的云语料库
机器学习
1
502
分类器族（例如，
～1000个特征）
504
回答比率
2
514
最佳特征
508
缩减的
特征模型
4
3
506
精简分类器族
（例如，～50个特征）
移动设备
分类器模型
510
5
102

图5A

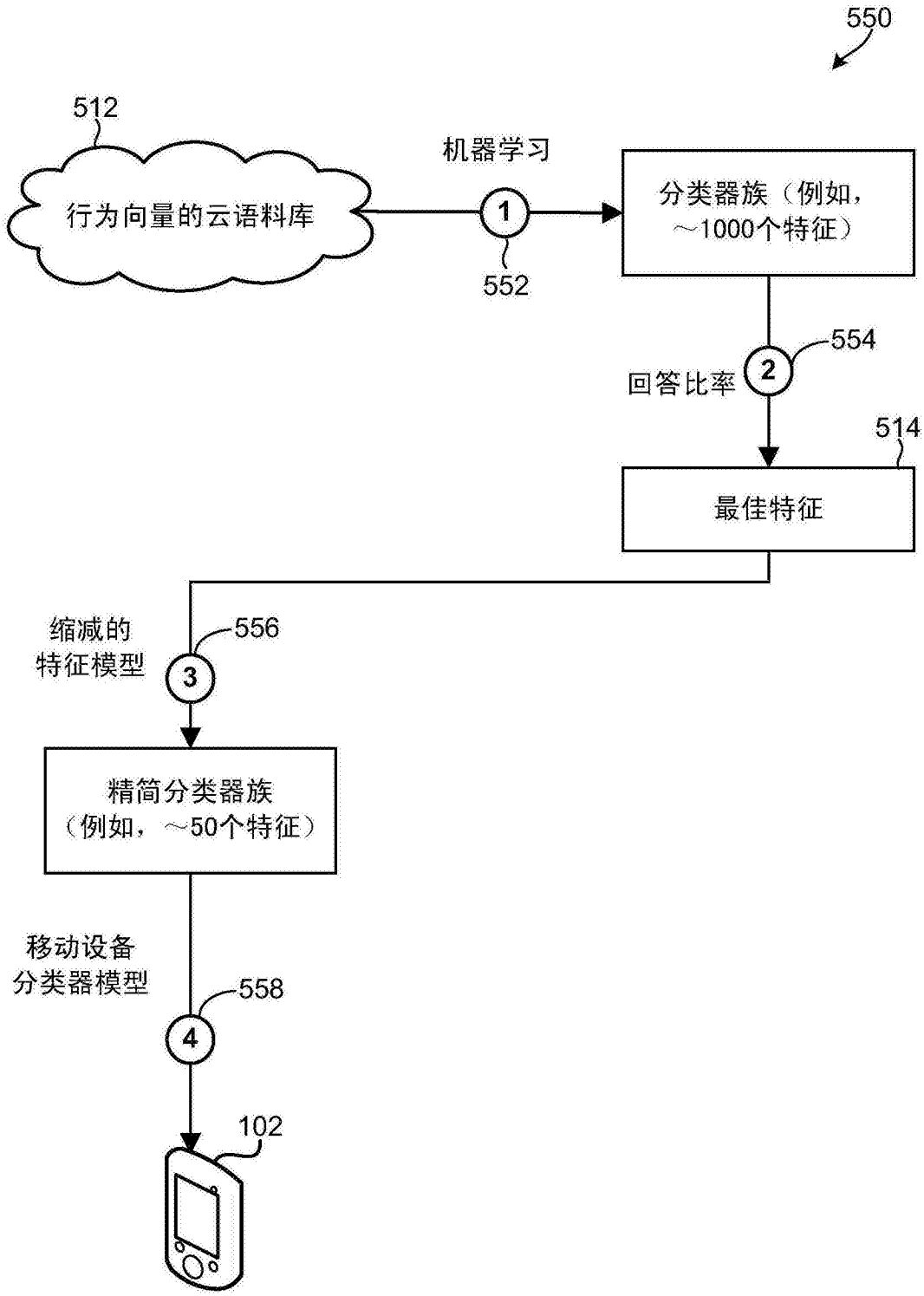

550
512
行为向量的云语料库
机器学习
1
552
分类器族（例如，
～1000个特征）
554
回答比率
2
514
最佳特征
缩减的
特征模型
556
3
精简分类器族
（例如，～50个特征）
移动设备
分类器模型
558
4
102

图5B

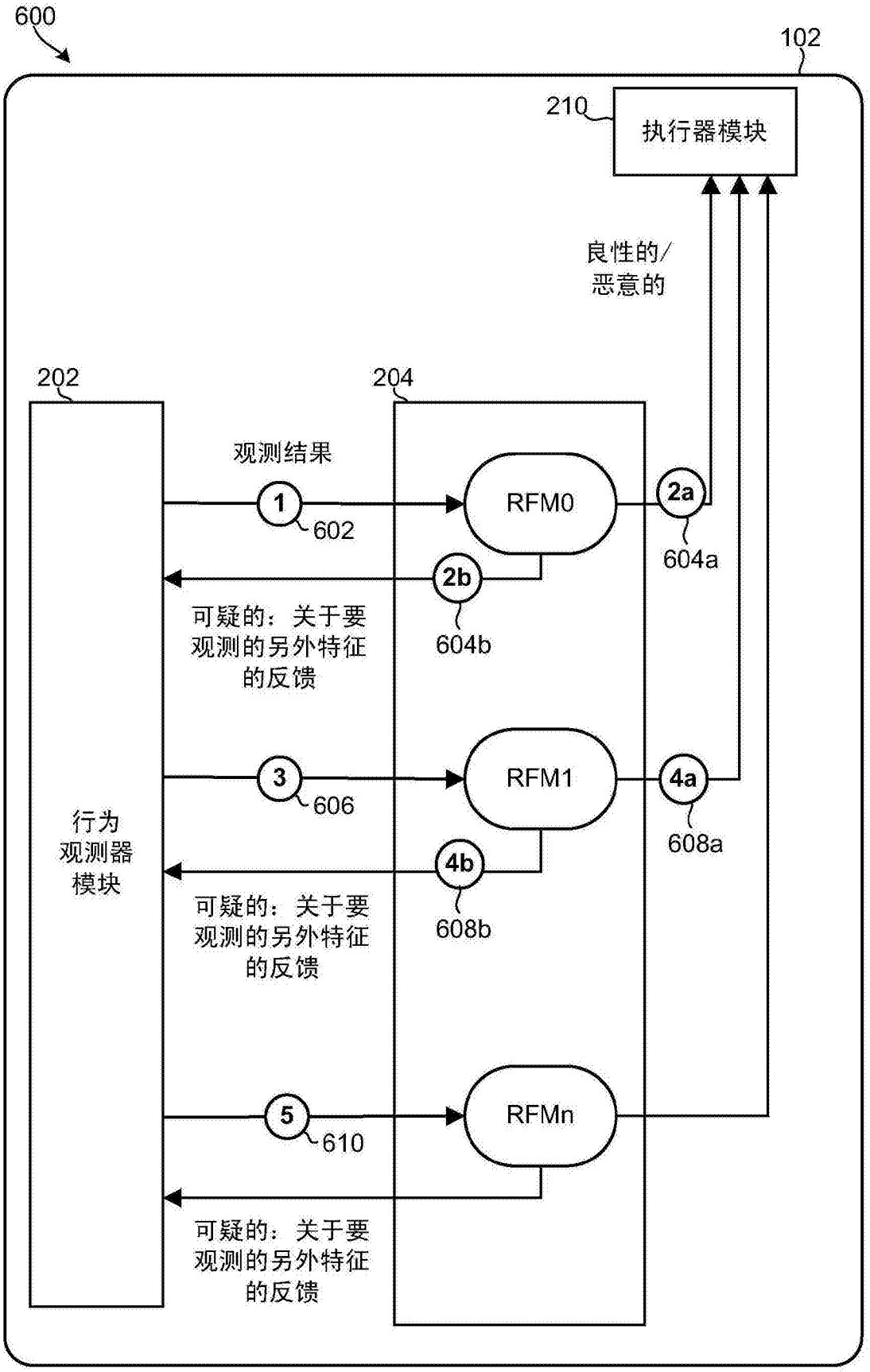

600
102
210
执行器模块
良性的/
恶意的
202
204
观测结果
1
602
RFM0
2a
604a
2b
604b
可疑的：关于要
观测的另外特征
的反馈
3
606
RFM1
4a
608a
行为
观测器
模块
4b
608b
可疑的：关于要
观测的另外特征
的反馈
5
610
RFMn
可疑的：关于要
观测的另外特征
的反馈

图6

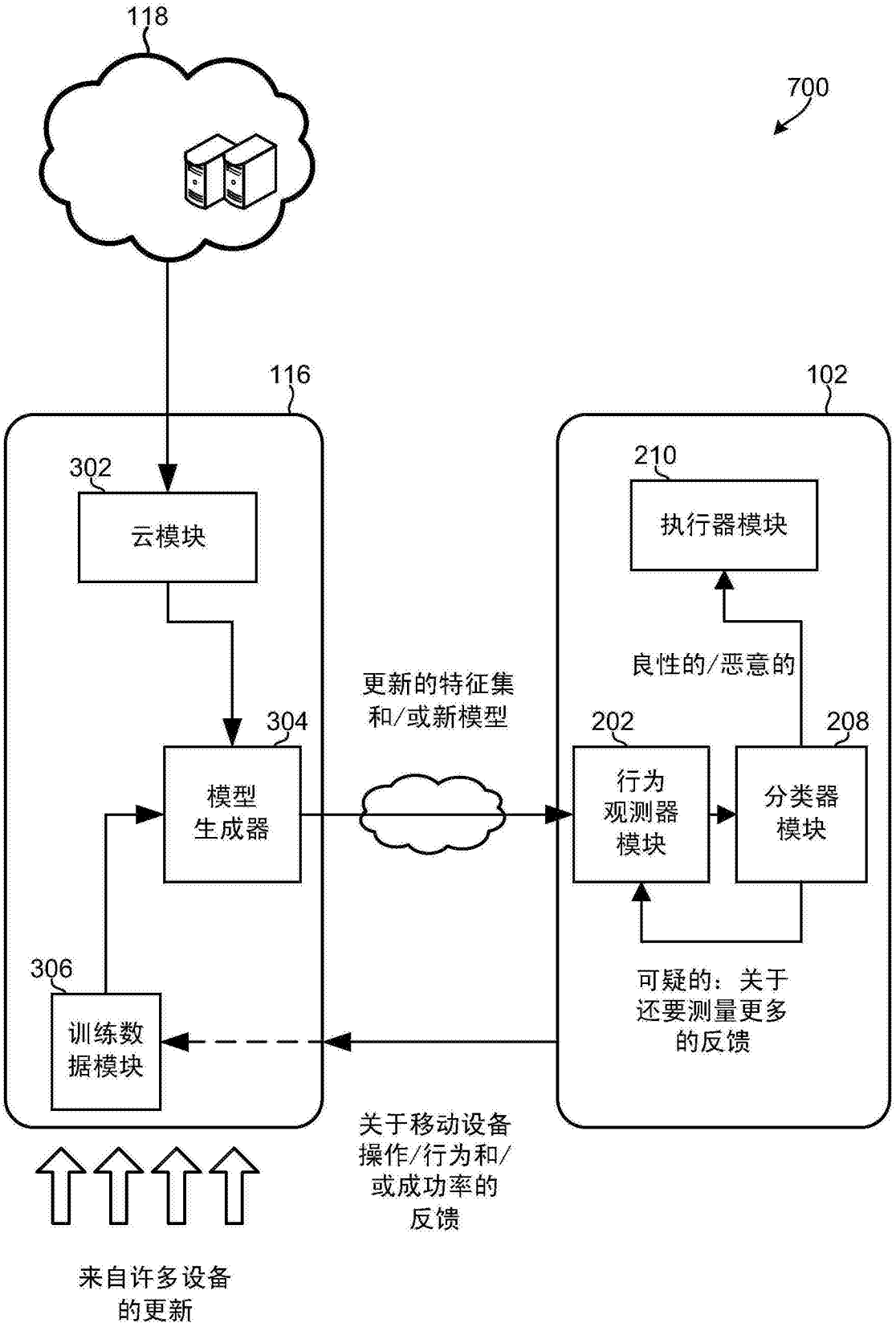

118
700
116
102
302
云模块
210
执行器模块
良性的/恶意的
更新的特征集
和/或新模型
304
202
208
模型
生成器
行为
观测器
模块
分类器
模块
306
训练数
据模块
可疑的：关于
还要测量更多
的反馈
关于移动设备
操作/行为和/
或成功率的
反馈
来自许多设备
的更新

图7

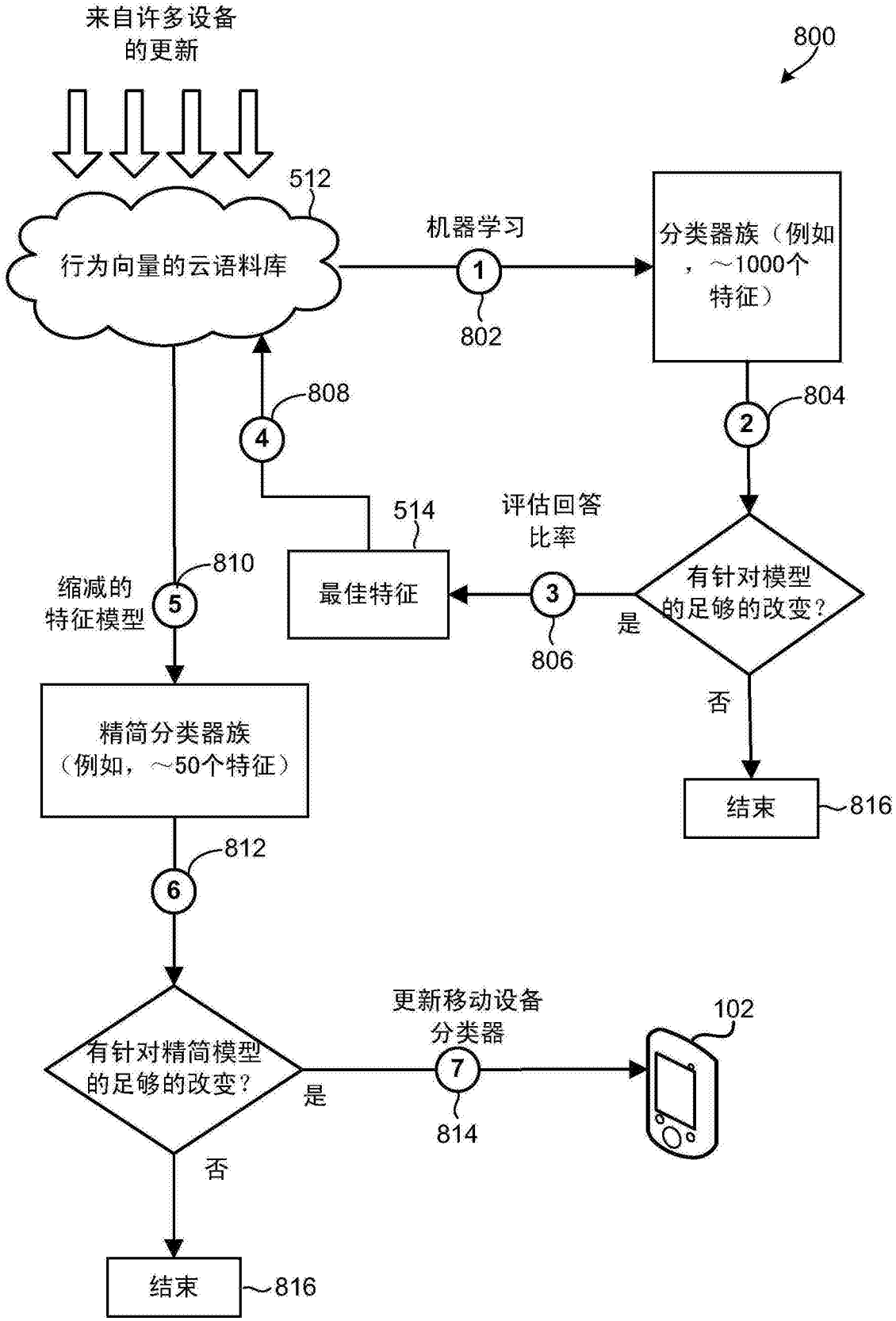

来自许多设备的更新
800
512
行为向量的云语料库
机器学习
1
802
分类器族（例如，～1000个特征）
804
2
808
4
514
评估回答比率
最佳特征
3
806
有针对模型的足够的改变？
是
否
结束
816
缩减的特征模型
810
5
精简分类器族（例如，～50个特征）
812
6
有针对精简模型的足够的改变？
是
更新移动设备分类器
7
814
102
否
结束
816

图8A

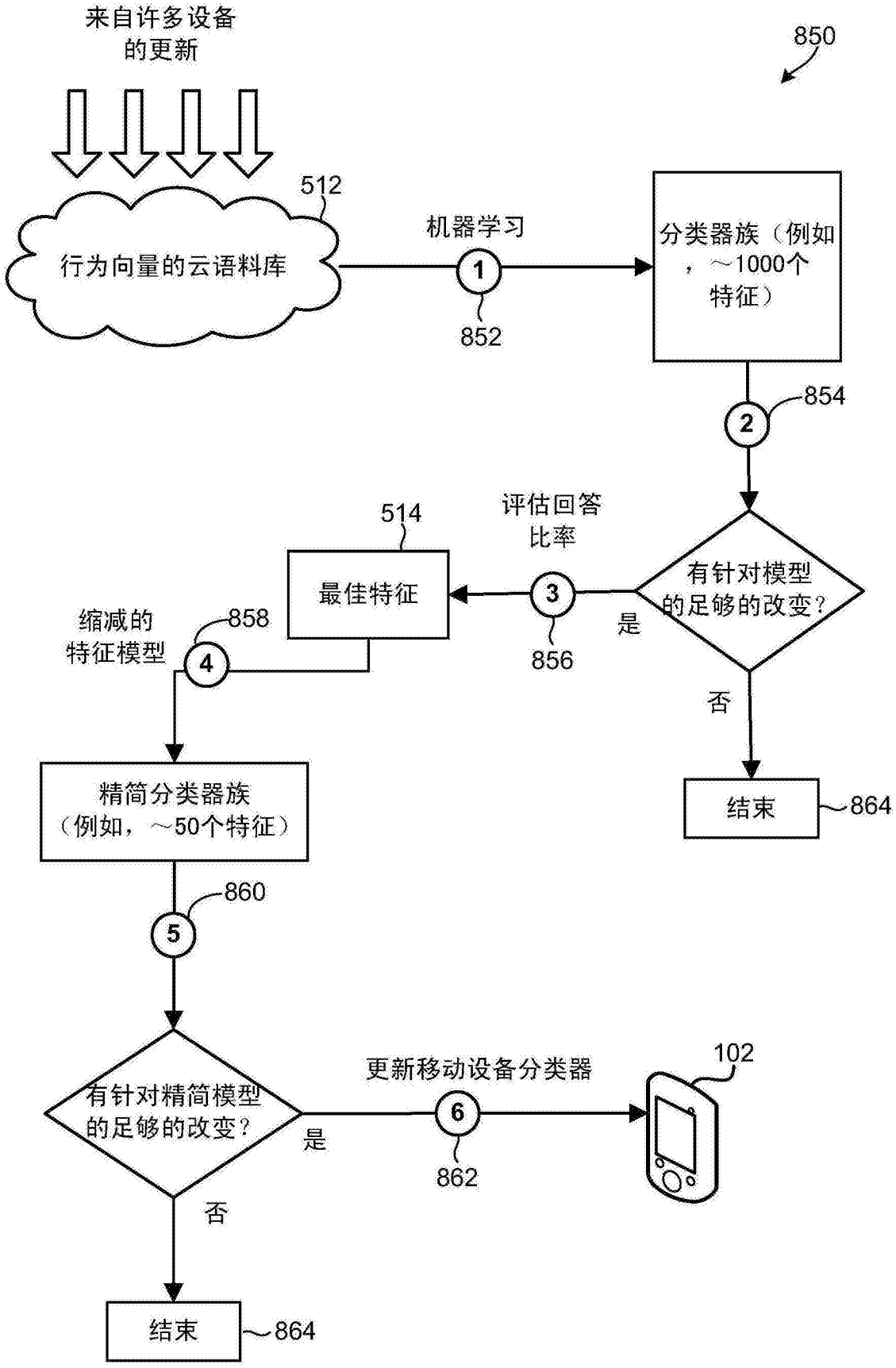

来自许多设备的更新
850
512
行为向量的云语料库
机器学习
1
852
分类器族（例如，～1000个特征）
854
2
评估回答比率
514
最佳特征
3
856
有针对模型的足够的改变？
是
否
缩减的特征模型
858
4
精简分类器族（例如，～50个特征）
结束
864
860
5
有针对精简模型的足够的改变？
是
更新移动设备分类器
6
862
102
否
结束
864

图8B

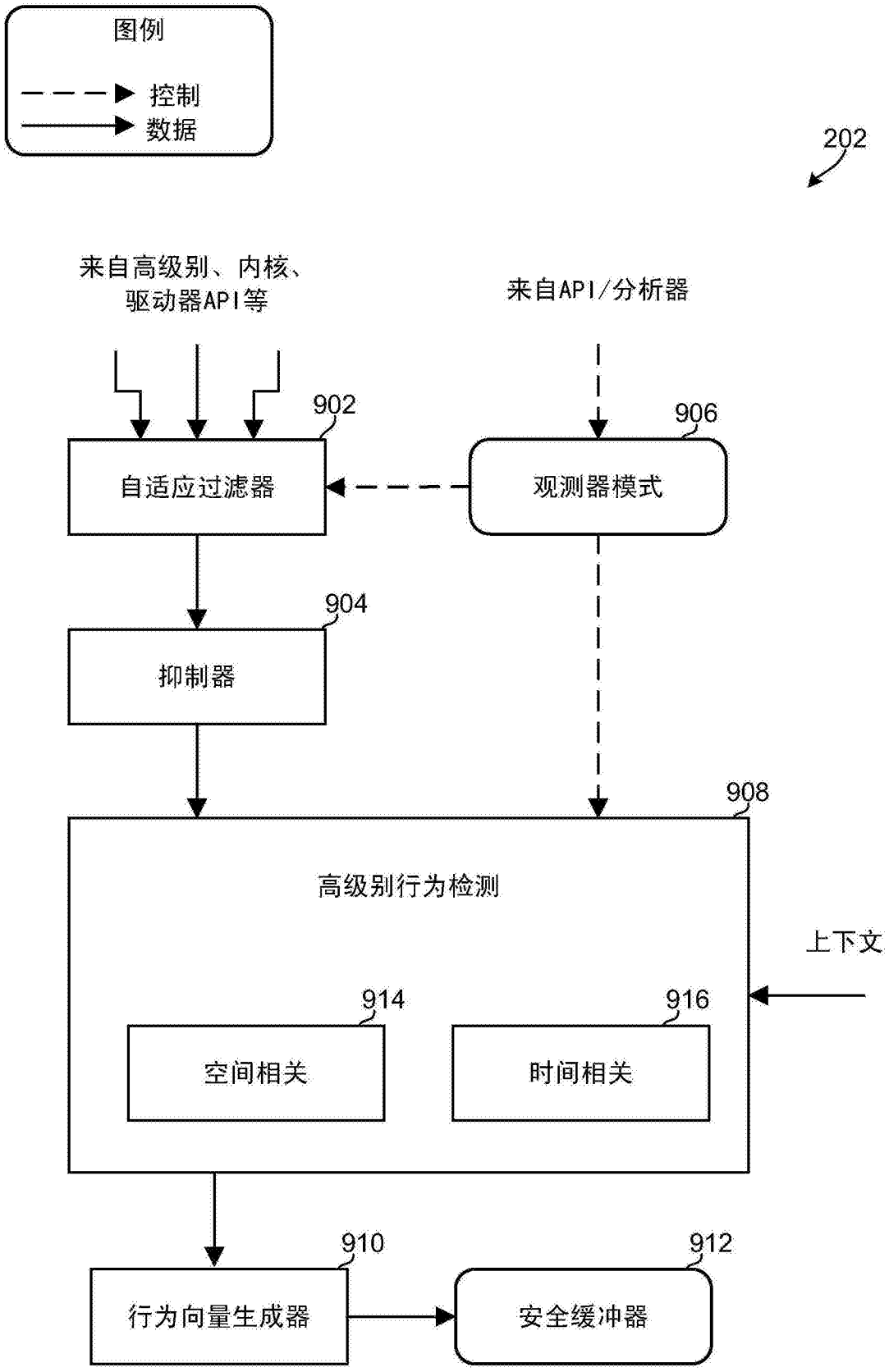

图例
控制
数据
202
来自高级别、内核、
驱动器API等
来自API/分析器
902
906
自适应过滤器
观测器模式
904
抑制器
908
高级别行为检测
上下文
914
916
空间相关
时间相关
910
912
行为向量生成器
安全缓冲器

图9

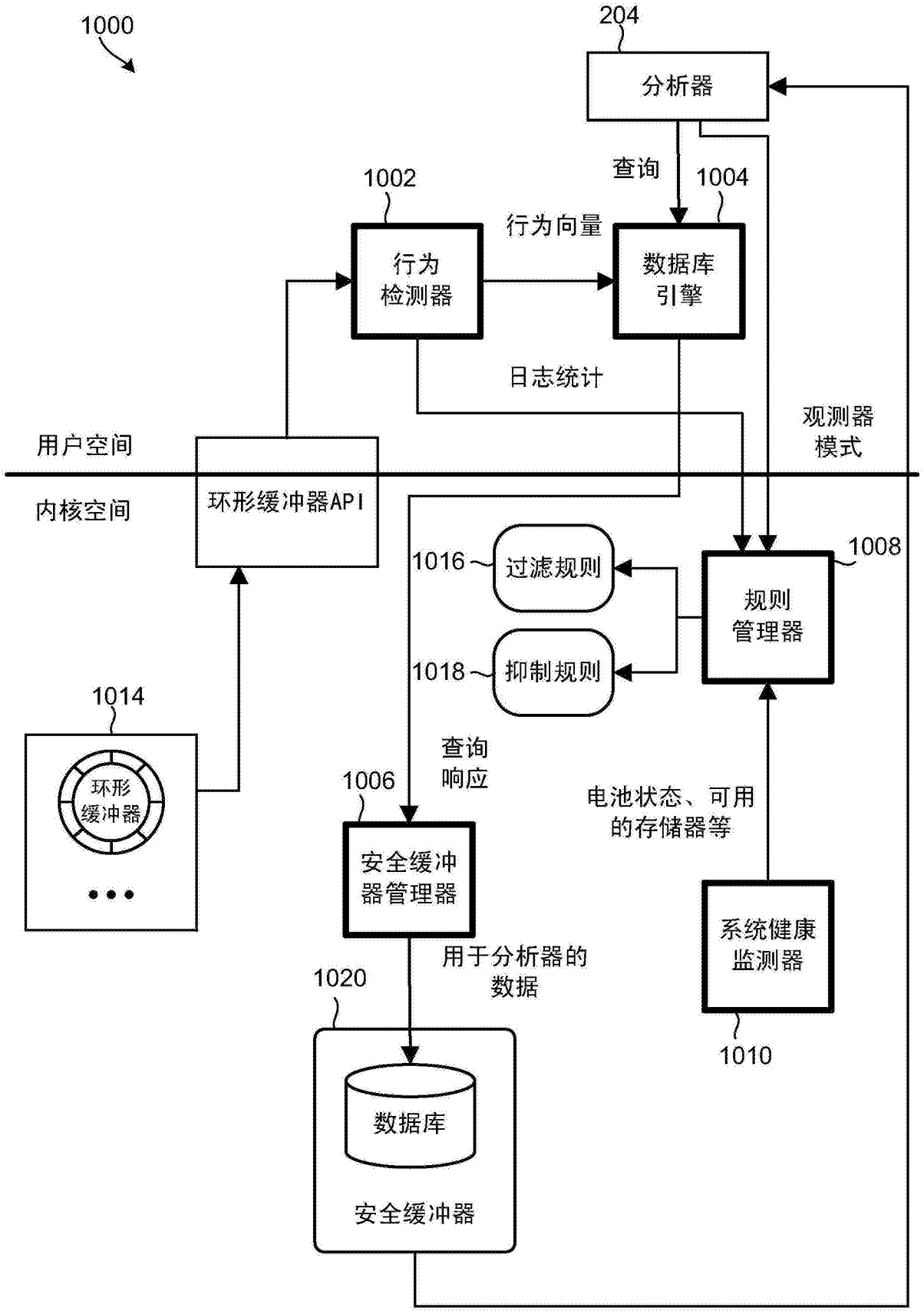

1000
204
分析器
查询
1004
1002
行为向量
行为
检测器
数据库
引擎
日志统计
观测器
模式
用户空间
内核空间
环形缓冲器API
1016
过滤规则
1008
规则
管理器
1018
抑制规则
1014
环形
缓冲器
查询
响应
1006
电池状态、可用
的存储器等
安全缓冲
器管理器
系统健康
监测器
用于分析器的
数据
1020
1010
数据库
安全缓冲器

图10

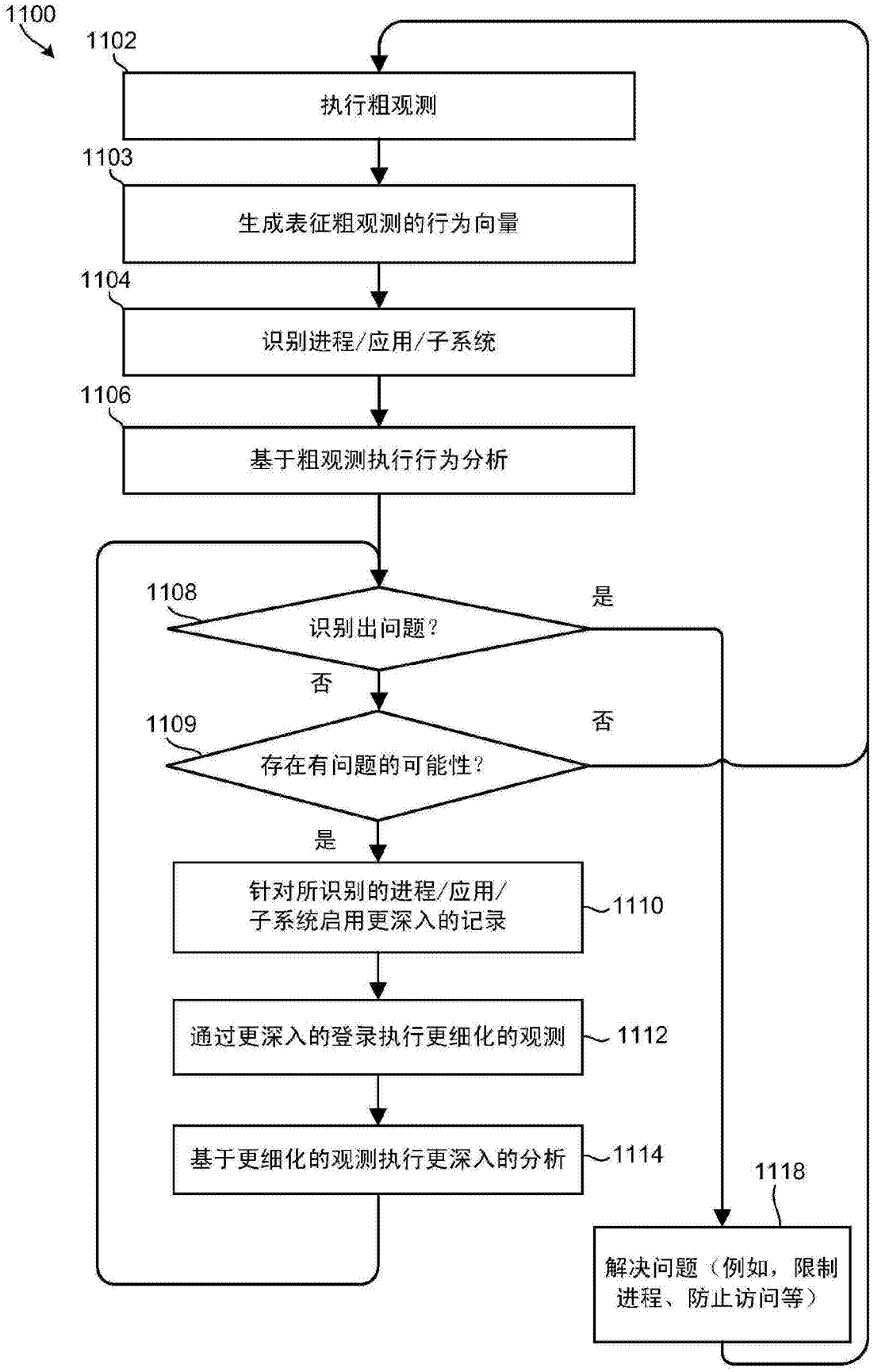

1100
1102
执行粗观测
1103
生成表征粗观测的行为向量
1104
识别进程/应用/子系统
1106
基于粗观测执行行为分析
1108
识别出问题？
是
否
1109
存在有问题的可能性？
否
是
针对所识别的进程/应用/
子系统启用更深入的记录
1110
通过更深入的登录执行更细化的观测
1112
基于更细化的观测执行更深入的分析
1114
1118
解决问题（例如，限制
进程、防止访问等）

图11

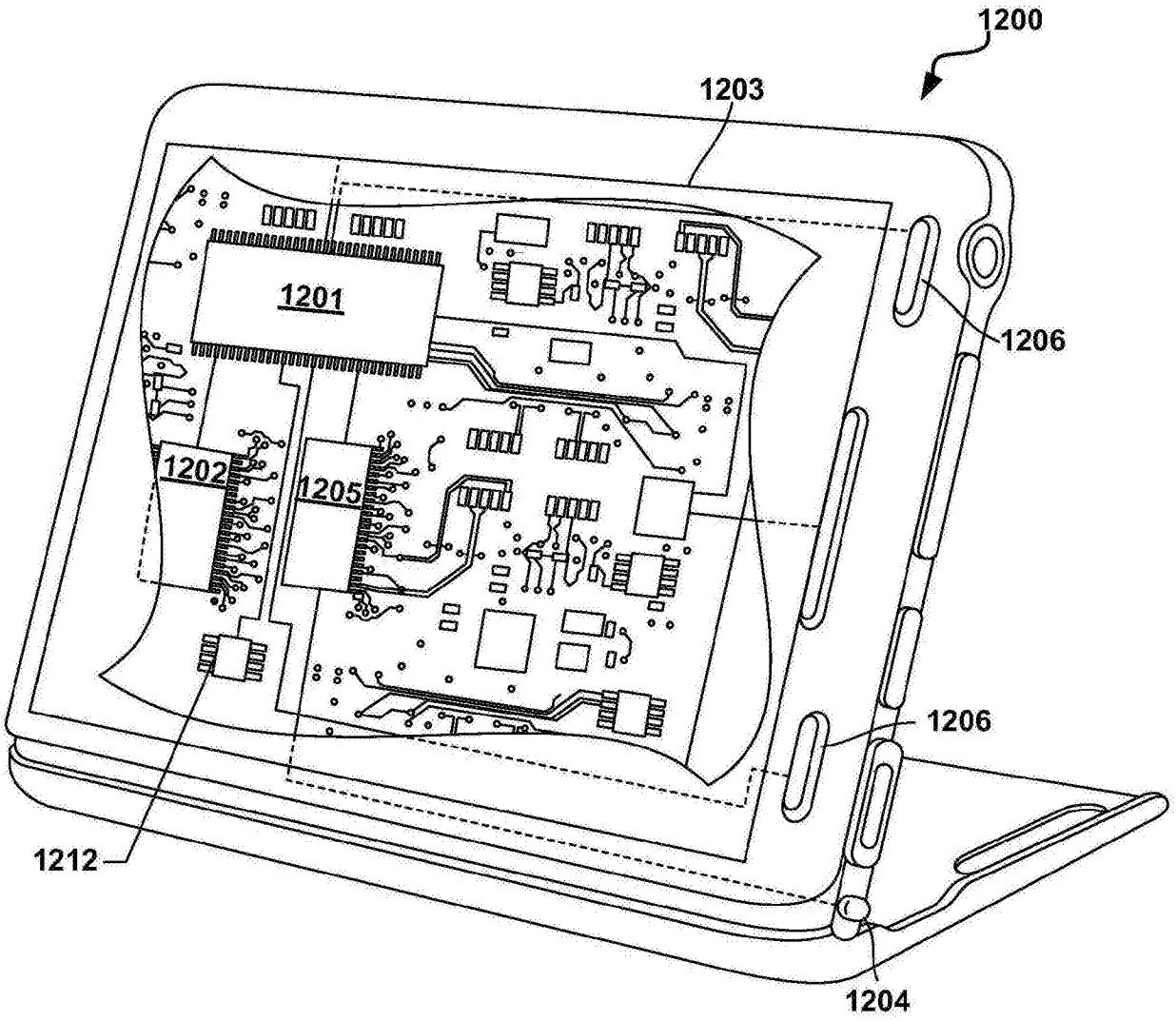


图12

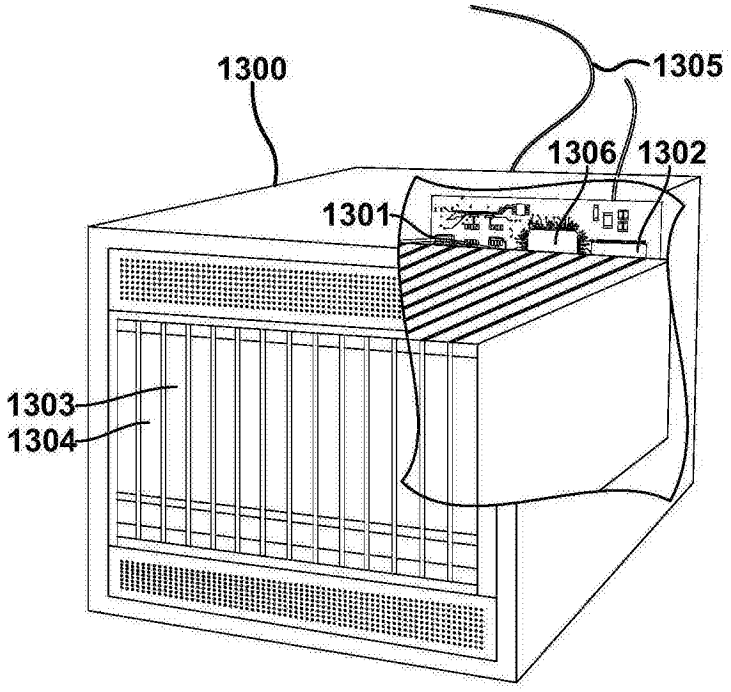


图13