



(10) 申请公布号 CN 104903918 A

(43) 申请公布日 2015.09.09

(21) 申请号 201380069436.X

(72) 发明人 维纳伊·斯里达拉 拉贾什·古普塔
卡塞姆·法瓦兹

(22) 申请日 2013.12.30

(30) 优先权数据

(74) 专利代理机构 北京律盟知识产权代理有限公司 11287

61/748,217 2013.01.02 US

61/748, 220 2013. 01. 02 US

61/874, 109 2013. 09. 05 US

61/874, 129 2013. 09. 05 US

14/091,707 2013. 11. 27 US

代理人 宋献涛

(51) Int. Cl.

G06N 5/04(2006.01)

(85) PCT国际申请进入国家阶段日

2015. 06. 30

(86) PCT国际申请的申请数据

PCT/US2013/078350 2013. 12. 30

(87) PCT国际申请的公布数据

W02014/107438 EN 2014. 07. 10

(71) 申请人 高通股份有限公司

地址 美国加利福尼亚州

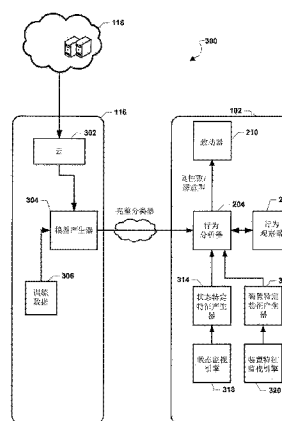
权利要求书7页 说明书32页 附图11页

(54) 发明名称

动态地产生和使用装置特定及装置状态特定的分类器模型以高效分类移动装置行为的方法及系统

(57) 摘要

各种方面提供移动装置和施用于所述移动装置上以用于修改行为模型以考虑到装置特定或装置状态特定特征的方法。在所述各种方面中,行为分析器模块可利用从网络服务器接收的行为模型的完整特征集合(即,大型分类器模型)以建立供用于监视所述移动装置上的恶意行为的精实分类器模型,且所述行为分析器模块可动态地修改这些精实分类器模型以包括所述移动装置和/或所述移动装置的当前配置特有的特征。因此,所述各种方面可通过考虑特定移动装置及其当前配置来增强所述移动装置的总体安全性,且可通过仅监视与所述移动装置相关的特征来改善总体性能。



1. 一种在移动装置中产生数据模型的方法,其包括:

在所述移动装置的处理器中接收识别多个测试条件的完整分类器模型;

使用所述移动装置的装置特定信息来识别所述多个测试条件中的与分类所述移动装置的行为相关的移动装置特定测试条件;

在所述移动装置中产生仅包含所述所识别的移动装置特定测试条件的精实分类器模型;以及

在所述移动装置中使用所述所产生的精实分类器模型来分类所述移动装置的所述行为。

2. 根据权利要求 1 所述的方法,其中:

接收识别所述多个测试条件的所述完整分类器模型包括接收包含适合于转换多个决策节点的信息的有限状态机,所述多个决策节点中的每一者评估所述多个测试条件中的一者;以及

产生仅包含所述所识别的移动装置特定测试条件的所述精实分类器模型包括产生所述精实分类器模型以仅包含评估与所述移动装置的当前操作状态或配置相关的移动装置特征的所述决策节点。

3. 根据权利要求 2 所述的方法,其中产生所述精实分类器模型以仅包含评估与所述移动装置的所述当前操作状态或配置相关的移动装置特征的所述决策节点包括:

确定在不消耗所述移动装置的过多量的处理、存储器或能量资源的情况下应加以评估以分类所述行为的独特测试条件的数目;

通过顺序地遍历所述完整分类器模型中的所述多个测试条件且将与分类所述移动装置的所述行为相关的那些测试条件插入到测试条件列表中直至所述测试条件列表包含所述所确定的数目的独特测试条件来产生所述测试条件列表;以及

产生所述精实分类器模型以包含所述完整分类器模型中的测试被包含于所述所产生的测试条件列表中的所述测试条件中的一者的所述决策节点。

4. 根据权利要求 2 所述的方法,其中在所述移动装置中使用所述所产生的精实分类器模型来分类所述移动装置的所述行为包括通过以下步骤来使用所述精实分类器模型以将所述行为分类为良性型或非良性型:

将所收集的行为信息应用到所述精实分类器模型中的每一决策节点;

计算将所述所收集的行为信息应用到所述精实分类器模型中的每一决策节点的结果的加权平均值;以及

将所述加权平均值与阈值相比较。

5. 根据权利要求 1 所述的方法,其进一步包括:

监视所述移动装置以检测以下各者中的一者的改变:所述移动装置的状态、所述移动装置的配置、所述移动装置的能力及所述移动装置的功能性;

响应于检测到所述而修改所述精实分类器模型以包含一组更新的测试条件;以及

使用所述经修改的精实分类器模型来分类所述移动装置的所述行为。

6. 根据权利要求 5 所述的方法,其中监视所述移动装置及响应于检测到所述改变而修改所述精实分类器模型以包含所述组更新的测试条件包括:

识别与所述所检测到的改变相关联的被添加的移动装置特征;

确定所述所识别的被添加的移动装置特征是否被包含于所述所产生的精实分类器模型中 ; 以及

响应于确定所述所识别的特征未被包含于所述所产生的精实分类器模型中而将所述所识别的特征添加到所述所产生的精实分类器模型。

7. 根据权利要求 5 所述的方法, 其中监视所述移动装置及响应于检测到所述改变而修改所述精实分类器模型以包含所述组更新的测试条件包括 :

通过检测辅助组件被添加到所述移动装置来检测所述移动装置的所述能力的所述改变 ;

确定所述精实分类器模型是否包含评估所述辅助组件的任何测试条件 ;

响应于确定所述精实分类器模型不包含评估所述辅助组件的任何测试条件而确定所述完整分类器模型是否包含用于所述辅助组件的任何测试条件 ; 以及

响应于确定所述完整分类器模型包含用于所述辅助组件的测试条件而将与所述辅助组件相关联的测试条件添加到所述精实分类器模型。

8. 根据权利要求 5 所述的方法, 其中监视所述移动装置及响应于检测到所述改变而修改所述精实分类器模型以包含所述组更新的测试条件包括 :

检测所述移动装置的所述功能性的所述改变 ;

确定所述所检测到的功能性改变表示被添加或被去除的功能性 ;

响应于确定所述所检测到的功能性改变表示被添加的功能性而确定所述精实分类器模型是否包含评估受所述所检测到的功能性改变影响的移动装置特征的任何测试条件 ;

响应于确定所述精实分类器模型不包含评估所述移动装置特征的任何测试条件而确定所述完整分类器模型是否包含评估所述移动装置特征的任何测试条件 ; 以及

响应于确定所述完整分类器模型包含评估所述移动装置特征的测试条件而将评估受所述所检测到的改变影响的所述移动装置特征的测试条件添加到所述精实分类器模型。

9. 根据权利要求 5 所述的方法, 其中监视所述移动装置及响应于检测到所述改变而修改所述精实分类器模型以包含所述组更新的测试条件包括 :

确定在所述移动装置上是否已存在所述状态改变 ;

响应于确定在所述移动装置上已存在所述状态改变而识别与所述移动装置的先前状态相关且与所述移动装置的当前状态不相关的特征 ; 以及

从所述精实分类器模型去除与所述所识别的特征相关联的测试条件。

10. 一种移动装置, 其包括 :

经配置有处理器可执行指令以执行操作的处理器, 所述操作包括 :

接收识别多个测试条件的完整分类器模型 ;

使用所述移动装置的装置特定信息来识别所述多个测试条件中的与分类所述移动装置的行为相关的移动装置特定测试条件 ;

产生仅包含所述所识别的移动装置特定测试条件的精实分类器模型 ; 以及

在所述移动装置中使用所述所产生的精实分类器模型来分类所述移动装置的所述行为。

11. 根据权利要求 10 所述的移动装置, 其中所述处理器经配置有处理器可执行指令以执行操作使得 :

接收识别所述多个测试条件的所述完整分类器模型包括接收包含适合于转换多个决策节点的信息的有限状态机,所述多个决策节点中的每一者评估所述多个测试条件中的一者;以及

产生仅包含所述所识别的移动装置特定测试条件的所述精实分类器模型包括产生所述精实分类器模型以仅包含评估与所述移动装置的当前操作状态或配置相关的移动装置特征的所述决策节点。

12. 根据权利要求 11 所述的移动装置,其中所述处理器经配置有处理器可执行指令以执行操作,使得产生所述精实分类器模型以仅包含评估与所述移动装置的所述当前操作状态或配置相关的移动装置特征的所述决策节点包括:

确定在不消耗所述移动装置的过多量的处理、存储器或能量资源的情况下应加以评估以分类所述行为的独特测试条件的数目;

通过顺序地遍历所述完整分类器模型中的所述多个测试条件且将与分类所述移动装置的所述行为相关的那些测试条件插入到测试条件列表中直至所述测试条件列表包含所述所确定的数目的独特测试条件来产生所述测试条件列表;以及

产生所述精实分类器模型以包含所述完整分类器模型中的测试被包含于所述所产生的测试条件列表中的所述测试条件中的一者的所述决策节点。

13. 根据权利要求 11 所述的移动装置,其中所述处理器经配置有处理器可执行指令以执行操作,使得在所述移动装置中使用所述所产生的精实分类器模型来分类所述移动装置的所述行为包括通过以下步骤来使用所述精实分类器模型以将所述行为分类为良性型或非良性型:

将所收集的行为信息应用到所述精实分类器模型中的每一决策节点;

计算将所述所收集的行为信息应用到所述精实分类器模型中的每一决策节点的结果的加权平均值;以及

将所述加权平均值与阈值相比较。

14. 根据权利要求 10 所述的移动装置,其中所述处理器经配置有处理器可执行指令以执行操作,所述操作进一步包括:

监视所述移动装置以检测以下各者中的一者的改变:所述移动装置的状态、所述移动装置的配置、所述移动装置的能力及所述移动装置的功能性;

响应于检测到所述而修改所述精实分类器模型以包含一组更新的测试条件;以及

使用所述经修改的精实分类器模型来分类所述移动装置的所述行为。

15. 根据权利要求 14 所述的移动装置,其中所述处理器经配置有处理器可执行指令以执行操作,使得监视所述移动装置及响应于检测到所述改变而修改所述精实分类器模型以包含所述组更新的测试条件包括:

识别与所述所检测到的改变相关联的被添加的移动装置特征;

确定所述所识别的被添加的移动装置特征是否被包含于所述所产生的精实分类器模型中;以及

响应于确定所述所识别的特征未被包含于所述所产生的精实分类器模型中而将所述所识别的特征添加到所述所产生的精实分类器模型。

16. 根据权利要求 14 所述的移动装置,其中所述处理器经配置有处理器可执行指令以

执行操作,使得监视所述移动装置及响应于检测到所述改变而修改所述精实分类器模型以包含所述组更新的测试条件包括:

通过检测辅助组件被添加到所述移动装置来检测所述移动装置的所述能力的所述改变;

确定所述精实分类器模型是否包含评估所述辅助组件的任何测试条件;

响应于确定所述精实分类器模型不包含评估所述辅助组件的任何测试条件而确定所述完整分类器模型是否包含用于所述辅助组件的任何测试条件;以及

响应于确定所述完整分类器模型包含用于所述辅助组件的测试条件而将与所述辅助组件相关联的测试条件添加到所述精实分类器模型。

17. 根据权利要求 14 所述的移动装置,其中所述处理器经配置有处理器可执行指令以执行操作,使得监视所述移动装置及响应于检测到所述改变而修改所述精实分类器模型以包含所述组更新的测试条件包括:

检测所述移动装置的所述功能性的所述改变;

确定所述所检测到的功能性改变表示被添加或被去除的功能性;

响应于确定所述所检测到的功能性改变表示被添加的功能性而确定所述精实分类器模型是否包含评估受所述所检测到的功能性改变影响的移动装置特征的任何测试条件;

响应于确定所述精实分类器模型不包含评估所述移动装置特征的任何测试条件而确定所述完整分类器模型是否包含评估所述移动装置特征的任何测试条件;以及

响应于确定所述完整分类器模型包含评估所述移动装置特征的测试条件而将评估受所述所检测到的改变影响的所述移动装置特征的测试条件添加到所述精实分类器模型。

18. 根据权利要求 14 所述的移动装置,其中所述处理器经配置有处理器可执行指令以执行操作,使得监视所述移动装置及响应于检测到所述改变而修改所述精实分类器模型以包含所述组更新的测试条件包括:

确定在所述移动装置上是否已存在所述状态改变;

响应于确定在所述移动装置上已存在所述状态改变而识别与所述移动装置的先前状态相关且与所述移动装置的当前状态不相关的特征;以及

从所述精实分类器模型去除与所述所识别的特征相关联的测试条件。

19. 一种非暂时性计算机可读存储媒体,其上存储有处理器可执行软件指令,所述软件指令经配置以使移动装置的处理器执行操作,所述操作包括:

接收识别多个测试条件的完整分类器模型;

使用所述移动装置的装置特定信息来识别所述多个测试条件中的与分类所述移动装置的行为相关的移动装置特定测试条件;

产生仅包含所述所识别的移动装置特定测试条件的精实分类器模型;以及

在所述移动装置中使用所述所产生的精实分类器模型来分类所述移动装置的所述行为。

20. 根据权利要求 19 所述的非暂时性计算机可读存储媒体,其中所述所存储的处理器可执行软件指令经配置以使处理器执行操作使得:

接收识别所述多个测试条件的所述完整分类器模型包括接收包含适合于转换多个决策节点的信息的有限状态机,所述多个决策节点中的每一者评估所述多个测试条件中的一

者 ; 以及

产生仅包含所述所识别的移动装置特定测试条件的所述精实分类器模型包括产生所述精实分类器模型以仅包含评估与所述移动装置的当前操作状态或配置相关的移动装置特征的所述决策节点。

21. 根据权利要求 20 所述的非暂时性计算机可读存储媒体, 其中所述所存储的处理器可执行软件指令经配置以使处理器执行操作, 使得产生所述精实分类器模型以仅包含评估与所述移动装置的所述当前操作状态或配置相关的移动装置特征的所述决策节点包括:

确定在不消耗所述移动装置的过多量的处理、存储器或能量资源的情况下应加以评估以分类所述行为的独特测试条件的数目;

通过顺序地遍历所述完整分类器模型中的所述多个测试条件且将与分类所述移动装置的所述行为相关的那些测试条件插入到测试条件列表中直至所述测试条件列表包含所述所确定的数目的独特测试条件来产生所述测试条件列表; 以及

产生所述精实分类器模型以包含所述完整分类器模型中的测试被包含于所述所产生的测试条件列表中的所述测试条件中的一者的所述决策节点。

22. 根据权利要求 20 所述的非暂时性计算机可读存储媒体, 其中所述所存储的处理器可执行软件指令经配置以使处理器执行操作, 使得在所述移动装置中使用所述所产生的精实分类器模型来分类所述移动装置的所述行为包括通过以下步骤来使用所述精实分类器模型以将所述行为分类为良性型或非良性型:

将所收集的行为信息应用到所述精实分类器模型中的每一决策节点;

计算将所述所收集的行为信息应用到所述精实分类器模型中的每一决策节点的结果的加权平均值; 以及

将所述加权平均值与阈值相比较。

23. 根据权利要求 19 所述的非暂时性计算机可读存储媒体, 其中所述所存储的处理器可执行软件指令经配置以使处理器执行操作, 所述操作进一步包括:

监视所述移动装置以检测以下各者中的一者的改变: 所述移动装置的状态、所述移动装置的配置、所述移动装置的能力及所述移动装置的功能性;

响应于检测到所述而修改所述精实分类器模型以包含一组更新的测试条件; 以及

使用所述经修改的精实分类器模型来分类所述移动装置的所述行为。

24. 根据权利要求 23 所述的非暂时性计算机可读存储媒体, 其中所述所存储的处理器可执行软件指令经配置以使处理器执行操作, 使得监视所述移动装置及响应于检测到所述改变而修改所述精实分类器模型以包含所述组更新的测试条件包括:

识别与所述所检测到的改变相关联的被添加的移动装置特征;

确定所述所识别的特征是否被包含于所述所产生的精实分类器模型中; 以及

响应于确定所述所识别的特征未被包含于所述所产生的精实分类器模型中而将所述所识别的特征添加到所述所产生的精实分类器模型。

25. 根据权利要求 23 所述的非暂时性计算机可读存储媒体, 其中所述所存储的处理器可执行软件指令经配置以使处理器执行操作, 使得监视所述移动装置及响应于检测到所述改变而修改所述精实分类器模型以包含所述组更新的测试条件包括:

通过检测辅助组件被添加到所述移动装置来检测所述移动装置的所述能力的所述改

变；

确定所述精实分类器模型是否包含评估所述辅助组件的任何测试条件；

响应于确定所述精实分类器模型不包含评估所述辅助组件的任何测试条件而确定所述完整分类器模型是否包含用于所述辅助组件的任何测试条件；以及

响应于确定所述完整分类器模型包含用于所述辅助组件的测试条件而将与所述辅助组件相关联的测试条件添加到所述精实分类器模型。

26. 根据权利要求 23 所述的非暂时性计算机可读存储媒体，其中所述所存储的处理器可执行软件指令经配置以使处理器执行操作，使得监视所述移动装置及响应于检测到所述改变而修改所述精实分类器模型以包含所述组更新的测试条件包括：

检测所述移动装置的所述功能性的所述改变；

确定所述所检测到的功能性改变表示被添加或被去除的功能性；

响应于确定所述所检测到的功能性改变表示被添加的功能性而确定所述精实分类器模型是否包含评估受所述所检测到的功能性改变影响的移动装置特征的任何测试条件；

响应于确定所述精实分类器模型不包含评估所述移动装置特征的任何测试条件而确定所述完整分类器模型是否包含评估所述移动装置特征的任何测试条件；以及

响应于确定所述完整分类器模型包含评估所述移动装置特征的测试条件而将评估受所述所检测到的改变影响的所述移动装置特征的测试条件添加到所述精实分类器模型。

27. 根据权利要求 23 所述的非暂时性计算机可读存储媒体，其中所述所存储的处理器可执行软件指令经配置以使处理器执行操作，使得监视所述移动装置及响应于检测到所述改变而修改所述精实分类器模型以包含所述组更新的测试条件包括：

确定在所述移动装置上是否已存在所述状态改变；

响应于确定在所述移动装置上已存在所述状态改变而识别与所述移动装置的先前状态相关且与所述移动装置的当前状态不相关的特征；以及

从所述精实分类器模型去除与所述所识别的特征相关联的测试条件。

28. 一种移动装置，其包括：

用于接收识别多个测试条件的完整分类器模型的装置；

用于使用所述移动装置的装置特定信息来识别所述多个测试条件中的与分类所述移动装置的行为相关的移动装置特定测试条件的装置；

用于产生仅包含所述所识别的移动装置特定测试条件的精实分类器模型的装置；以及

用于在所述移动装置中使用所述所产生的精实分类器模型来分类所述移动装置的所述行为的装置。

29. 根据权利要求 28 所述的移动装置，其中：

用于接收识别所述多个测试条件的所述完整分类器模型的装置包括用于接收包含适合于转换多个决策节点的信息的有限状态机的装置，所述多个决策节点中的每一者评估所述多个测试条件中的一者；以及

用于产生仅包含所述所识别的移动装置特定测试条件的所述精实分类器模型的装置包括用于产生所述精实分类器模型以仅包含评估与所述移动装置的当前操作状态或配置相关的移动装置特征的所述决策节点的装置。

30. 根据权利要求 29 所述的移动装置，其中用于产生所述精实分类器模型以仅包含评

估与所述移动装置的所述当前操作状态或配置相关的移动装置特征的所述决策节点的装置包括：

用于确定在不消耗所述移动装置的过多量的处理、存储器或能量资源的情况下应加以评估以分类所述行为的独特测试条件的装置的数目；

用于通过顺序地遍历所述完整分类器模型中的所述多个测试条件且将与分类所述移动装置的所述行为相关的那些测试条件插入到测试条件列表中直至所述测试条件列表包含所述所确定的数目的独特测试条件来产生所述测试条件列表的装置；以及

用于产生所述精实分类器模型以包含所述完整分类器模型中的测试被包含于所述所产生的测试条件列表中的所述条件中的一者的所述决策节点的装置。

动态地产生和使用装置特定及装置状态特定的分类器模型 以高效分类移动装置行为的方法及系统

[0001] 相关申请案

[0002] 本申请案主张以下各案的优先权的权利：2013 年 9 月 5 日申请的题目为“动态装置特定及装置状态特定分类器 (Dynamic Device-Specific and Device-State-Specific Classifier)”的美国临时申请案第 61/874,109 号；2013 年 9 月 5 日申请的题目为“使用加速决策树桩和联合特征选择及剪除算法以用于对移动装置行为进行高效分类的方法和系统 (Methods and Systems of Using Boosted Decision Stumps and Joint Feature Selection and Pruning Algorithms for the Efficient Classification of Mobile Device Behaviors)”的美国临时申请案第 61/874,129 号；2013 年 1 月 2 日申请的题目为“装置上实时行为分析器 (On-Device Real-Time Behavior Analyzer)”的美国临时专利申请案第 61/748,217 号；以及 2013 年 1 月 2 日申请的题目为“客户端 - 云行为分析器的架构 (Architecture for Client-Cloud Behavior Analyzer)”的美国临时专利申请案第 61/748,220 号，所有以上各案的全部内容特此以引用的方式并入本文中。

背景技术

[0003] 蜂窝式及无线通信技术已在过去若干年中突飞猛进。这种成长受到更好的通信、硬件、较大的网络及较可靠的协议助力。结果，无线服务提供商现能够向其客户提供前所未有的程度的对信息、资源及通信的存取。

[0004] 为了跟上这些服务增强，移动电子装置（例如，蜂窝式电话、平板计算机、膝上型计算机等）已变得越发强大及复杂。这种复杂性已为恶意软件、软件冲突、硬件故障及其它类似的错误或现象负面地影响移动装置的长期及持续性能与功率利用水平创造了新的机会。因此，识别及校正可负面地影响移动装置的长期及持续性能与功率利用水平的条件和/或移动装置行为是有益于消费者的。

发明内容

[0005] 各种方面包含在移动装置中产生数据模型的方法，所述方法包含：在移动装置的处理器中接收识别多个测试条件的完整分类器模型；使用移动装置的装置特定信息来识别所述多个测试条件中的与分类移动装置的行为相关的移动装置特定测试条件；在移动装置中产生仅包含所识别的移动装置特定测试条件的精实分类器模型；以及在移动装置中使用所产生的精实分类器模型来分类移动装置的行为。

[0006] 在方面中，接收识别多个测试条件的完整分类器模型可包含接收包含适合于转换多个决策节点的信息的有限状态机，所述多个决策节点中的每一者评估所述多个测试条件中的一者，且产生仅包含所识别的移动装置特定测试条件的精实分类器模型包含产生精实分类器模型以仅包含评估与移动装置的当前操作状态或配置相关的移动装置特征的决策节点。在另外的方面中，产生精实分类器模型以仅包含评估与移动装置的当前操作状态或配置相关的移动装置特征的决策节点可包含：确定在不消耗移动装置的过多量的处理、存

存储器或能量资源的情况下应加以评估以分类所述行为的独特测试条件的数目 ;通过顺序地遍历完整分类器模型中的多个测试条件且将与分类移动装置的行为相关的那些测试条件插入到测试条件列表中直至所述测试条件列表包含所述已确定的数目的独特测试条件来产生所述测试条件列表 ;以及产生精实分类器模型以包含完整分类器模型中的测试被包含于所产生的测试条件列表中的条件中的一者的决策节点。

[0007] 在另外的方面中,在移动装置中使用所产生的精实分类器模型来分类移动装置的行为可包含通过以下步骤来使用精实分类器模型以将行为分类为良性型或非良性型 :将所收集的行为信息应用到精实分类器模型中的每一决策节点 ;计算将所收集的行为信息应用到精实分类器模型中的每一决策节点的结果的加权平均值 ;以及将所述加权平均值与阈值相比较。在另外的方面中,所述方法可包含 :监视移动装置以检测移动装置的状态、移动装置的配置、移动装置的能力及移动装置的功能性中的一者的改变 ;响应于检测到所述而修改精实分类器模型以包含一组更新的测试条件 ;以及使用经修改的精实分类器模型来分类移动装置的行为。

[0008] 在另外的方面中,监视移动装置以检测改变及响应于检测到所述改变而修改精实分类器模型以包含一组更新的测试条件可包含 :识别与所检测到的改变相关联的阈值被添加的移动装置特征 ;确定所识别的特征是否被包含于所产生的精实分类器模型中 ;以及响应于确定所识别的特征未被包含于所产生的精实分类器模型中而将所识别的特征添加到所产生的精实分类器模型。

[0009] 在另外的方面中,监视移动装置以检测改变及响应于检测到所述改变而修改精实分类器模型以包含一组更新的测试条件可包含 :通过检测辅助组件被添加到移动装置来检测移动装置的能力的改变 ;确定精实分类器模型是否包含评估被添加的组件的任何测试条件 ;响应于确定精实分类器模型不包含评估被添加的组件的任何测试条件而确定完整分类器模型是否包含用于被添加的组件的任何测试条件 ;以及响应于确定完整分类器模型包含用于被添加的组件的测试条件而将用于被添加的组件的测试条件添加到精实分类器模型。

[0010] 在另外的方面中,监视移动装置以检测改变及响应于检测到所述改变而修改精实分类器模型以包含一组更新的测试条件可包含 :检测移动装置的功能性的改变 ;确定所检测到的功能性改变表示被添加或被去除的功能性 ;响应于确定所检测到的功能性改变表示被添加的功能性而确定精实分类器模型是否包含评估受所检测到的功能性改变影响的移动装置特征的任何测试条件 ;响应于确定精实分类器模型不包含评估移动装置特征的任何测试条件而确定完整分类器模型是否包含评估移动装置特征的任何测试条件 ;以及响应于确定完整分类器模型包含评估移动装置特征的测试条件而将评估受所检测到的改变影响的移动装置特征的测试条件添加到精实分类器模型。

[0011] 在另外的方面中,监视移动装置以检测改变及响应于检测到所述改变而修改精实分类器模型以包含一组更新的测试条件可包含 :确定在移动装置上是否已存在状态改变 ;响应于确定在移动装置上已存在状态改变而识别与移动装置的先前状态相关但与移动装置的当前状态不相关的特征 ;以及从精实分类器模型去除与所识别的特征相关联的测试条件。

[0012] 另外的方面包含移动装置,其包含经配置有处理器可执行指令以执行操作的处理器,所述操作包含 :接收识别多个测试条件的完整分类器模型 ;使用移动装置的装置特定

信息来识别所述多个测试条件中的与分类移动装置的行为相关的移动装置特定测试条件 ; 产生仅包含所识别的移动装置特定测试条件的精实分类器模型 ; 以及在移动装置中使用所产生的精实分类器模型来分类移动装置的行为。

[0013] 在方面中, 所述处理器可经配置有处理器可执行指令以执行操作, 使得接收识别多个测试条件的完整分类器模型可包含接收包含适合于转换多个决策节点的信息的有限状态机, 所述多个决策节点中的每一者评估所述多个测试条件中的一者, 且产生仅包含所识别的移动装置特定测试条件的精实分类器模型包含产生精实分类器模型以仅包含评估与移动装置的当前操作状态或配置相关的移动装置特征的决策节点。

[0014] 在另外的方面中, 所述处理器可经配置有处理器可执行指令以执行操作, 使得产生精实分类器模型以仅包含评估与移动装置的当前操作状态或配置相关的移动装置特征的决策节点可包含 : 确定在不消耗移动装置的过多量的处理、存储器或能量资源的情况下应加以评估以分类所述行为的独特测试条件的数目 ; 通过顺序地遍历完整分类器模型中的多个测试条件且将与分类移动装置的行为相关的那些测试条件插入到测试条件列表中直至所述测试条件列表包含已确定的数目的独特测试条件来产生所述测试条件列表 ; 以及产生精实分类器模型以包含完整分类器模型中的测试被包含于所产生的测试条件列表中的条件中的一者的决策节点。

[0015] 在另外的方面中, 所述处理器可经配置有处理器可执行指令以执行操作, 使得在移动装置中使用所产生的精实分类器模型来分类移动装置的行为可包含通过以下步骤来使用精实分类器模型以将所述行为分类为良性型或非良性型 : 将所收集的行为信息应用到精实分类器模型中的每一决策节点 ; 计算将所收集的行为信息应用到精实分类器模型中的每一决策节点的结果的加权平均值 ; 以及将所述加权平均值与阈值相比较。

[0016] 在另外的方面中, 所述处理器可经配置有处理器可执行指令以执行操作, 所述操作进一步包含 : 监视移动装置以检测移动装置的状态、移动装置的配置、移动装置的能力及移动装置的功能性中的一者的改变 ; 响应于检测到所述而修改精实分类器模型以包含一组更新的测试条件 ; 以及使用经修改的精实分类器模型来分类移动装置的行为。

[0017] 在另外的方面中, 所述处理器可经配置有处理器可执行指令以执行操作, 使得监视移动装置以检测改变及响应于检测到所述改变而修改精实分类器模型以包含一组更新的测试条件可包含 : 识别与所检测到的改变相关联的被添加的移动装置特征 ; 确定所识别的特征是否被包含于所产生的精实分类器模型中 ; 以及响应于确定所识别的特征未被包含于所产生的精实分类器模型中而将所识别的特征添加到所产生的精实分类器模型。

[0018] 在另外的方面中, 所述处理器可经配置有处理器可执行指令以执行操作, 使得监视移动装置以检测改变及响应于检测到所述改变而修改精实分类器模型以包含一组更新的测试条件可包含 : 通过检测辅助组件被添加到移动装置来检测移动装置的能力的改变 ; 确定精实分类器模型是否包含评估被添加的组件的任何测试条件 ; 响应于确定精实分类器模型不包含评估被添加的组件的任何测试条件而确定完整分类器模型是否包含用于被添加的组件的任何测试条件 ; 以及响应于确定完整分类器模型包含用于被添加的组件的测试条件而将用于被添加的组件的测试条件添加到精实分类器模型。

[0019] 在另外的方面中, 所述处理器可经配置有处理器可执行指令以执行操作, 使得监视移动装置以检测改变及响应于检测到所述改变而修改精实分类器模型以包含一组更新

的测试条件可包含 :检测移动装置的功能性的改变 ;确定所检测到的功能性改变表示被添加或被去除的功能性 ;响应于确定所检测到的功能性改变表示被添加的功能性而确定精实分类器模型是否包含评估受所检测到的功能性改变影响的移动装置特征的任何测试条件 ;响应于确定精实分类器模型不包含评估移动装置特征的任何测试条件而确定完整分类器模型是否包含评估移动装置特征的任何测试条件 ;以及响应于确定完整分类器模型包含评估移动装置特征的测试条件而将评估受所检测到的改变影响的移动装置特征的测试条件添加到精实分类器模型。

[0020] 在另外的方面中,所述处理器可经配置有处理器可执行指令以执行操作,使得监视移动装置以检测改变及响应于检测到所述改变而修改精实分类器模型以包含一组更新的测试条件可包含 :确定在移动装置上是否已存在状态的改变 ;响应于确定在移动装置上已存在状态的改变而识别与移动装置的先前状态相关但与移动装置的当前状态无关的特征 ;以及从精实分类器模型去除与所识别的特征相关联的测试条件。

[0021] 另外的方面包含非暂时性计算机可读存储媒体,其上存储有处理器可执行软件指令,所述处理器可执行软件指令经配置以使移动装置的处理器执行操作,所述操作包含 :在移动装置的处理器中接收识别多个测试条件的完整分类器模型 ;使用移动装置的装置特定信息来识别所述多个测试条件中的与分类移动装置的行为相关的移动装置特定测试条件 ;在移动装置中产生仅包含所识别的移动装置特定测试条件的精实分类器模型 ;以及在移动装置中使用所产生的精实分类器模型来分类移动装置的行为。

[0022] 在方面中,所存储的处理器可执行软件指令可经配置以使处理器执行操作,使得接收识别多个测试条件的完整分类器模型可包含接收包含适合于转换多个决策节点的信息的有限状态机,所述多个决策节点中的每一者评估所述多个测试条件中的一者,且产生仅包含所识别的移动装置特定测试条件的精实分类器模型包含产生精实分类器模型以仅包含评估与移动装置的当前操作状态或配置相关的移动装置特征的决策节点。

[0023] 在另外的方面中,所存储的处理器可执行软件指令可经配置以使处理器执行操作,使得产生精实分类器模型以仅包含评估与移动装置的当前操作状态或配置相关的移动装置特征的决策节点可包含 :确定在不消耗移动装置的过多量的处理、存储器或能量资源的情况下应加以评估以分类所述行为的独特测试条件的数目 ;通过顺序地遍历完整分类器模型中的多个测试条件且将与分类移动装置的行为相关的那些测试条件插入到测试条件列表中直至所述测试条件列表包含已确定的数目的独特测试条件来产生所述测试条件列表 ;以及产生精实分类器模型以包含完整分类器模型中的测试被包含于所产生的测试条件列表中的条件中的一者的决策节点。

[0024] 在另外的方面中,所存储的处理器可执行软件指令可经配置以使处理器执行操作,使得在移动装置中使用所产生的精实分类器模型来分类移动装置的行为可包含通过以下步骤来使用精实分类器模型以将所述行为分类为良性型或非良性型 :将所收集的行为信息应用到精实分类器模型中的每一决策节点 ;计算将所收集的行为信息应用到精实分类器模型中的每一决策节点的结果的加权平均值 ;以及将所述加权平均值与阈值相比较。在另外的方面中,所存储的处理器可执行软件指令可经配置以使处理器执行操作,所述操作进一步包含 :监视移动装置以检测移动装置的状态、移动装置的配置、移动装置的能力及移动装置的功能性中的一者的改变 ;响应于检测到所述而修改精实分类器模型以包含一组更新

的测试条件 ; 以及使用经修改的精实分类器模型来分类移动装置的行为。

[0025] 在另外的方面中, 所存储的处理器可执行软件指令可经配置以使处理器执行操作, 使得监视移动装置以检测改变及响应于检测到所述改变而修改精实分类器模型以包含一组更新的测试条件可包含 : 识别与所检测到的改变相关联的被添加的移动装置特征 ; 确定所识别的特征是否被包含于所产生的精实分类器模型中 ; 以及响应于确定所识别的特征未被包含于所产生的精实分类器模型中而将所识别的特征添加到所产生的精实分类器模型。

[0026] 在另外的方面中, 所存储的处理器可执行软件指令可经配置以使处理器执行操作, 使得监视移动装置以检测改变及响应于检测到所述改变而修改精实分类器模型以包含一组更新的测试条件可包含 : 通过检测辅助组件被添加到移动装置来检测移动装置的能力的改变 ; 确定精实分类器模型是否包含评估被添加的组件的任何测试条件 ; 响应于确定精实分类器模型不包含评估被添加的组件的任何测试条件而确定完整分类器模型是否包含用于被添加的组件的任何测试条件 ; 以及响应于确定完整分类器模型包含用于被添加的组件的测试条件而将用于被添加的组件的测试条件添加到精实分类器模型。

[0027] 在另外的方面中, 所存储的处理器可执行软件指令可经配置以使处理器执行操作, 使得监视移动装置以检测改变及响应于检测到所述改变而修改精实分类器模型以包含一组更新的测试条件可包含 : 检测移动装置的功能性的改变 ; 确定所检测到的功能性改变表示被添加或被去除的功能性 ; 响应于确定所检测到的功能性改变表示被添加的功能性而确定精实分类器模型是否包含评估受所检测到的功能性改变影响的移动装置特征的任何测试条件 ; 响应于确定精实分类器模型不包含评估移动装置特征的任何测试条件而确定完整分类器模型是否包含评估移动装置特征的任何测试条件 ; 以及响应于确定完整分类器模型包含评估移动装置特征的测试条件而将评估受所检测到的改变影响的移动装置特征的测试条件添加到精实分类器模型。

[0028] 在另外的方面中, 所存储的处理器可执行软件指令可经配置以使处理器执行操作, 使得监视移动装置以检测改变及响应于检测到所述改变而修改精实分类器模型以包含一组更新的测试条件可包含 : 确定在移动装置上是否已存在状态的改变 ; 响应于确定在移动装置上已存在状态的改变而识别与移动装置的先前状态相关但与移动装置的当前状态无关的特征 ; 以及从精实分类器模型去除与所识别的特征相关联的测试条件。

[0029] 另外的方面包含移动装置, 所述移动装置具有用于执行上文所描述的方法的功能的装置。所述移动装置可包含 : 用于接收识别多个测试条件的完整分类器模型的装置 ; 用于使用移动装置的装置特定信息来识别所述多个测试条件中的与分类移动装置的行为相关的移动装置特定测试条件的装置 ; 用于产生仅包含所识别的移动装置特定测试条件的精实分类器模型的装置 ; 以及用于在移动装置中使用所产生的精实分类器模型来分类移动装置的行为的装置。

[0030] 在方面中, 用于接收识别多个测试条件的完整分类器模型的装置可包含用于接收包含适合于转换多个决策节点的信息的有限状态机的装置, 所述多个决策节点中的每一者评估所述多个测试条件中的一者。在另外的方面中, 用于产生仅包含所识别的移动装置特定测试条件的精实分类器模型的装置可包含用于产生精实分类器模型以仅包含评估与移动装置的当前操作状态或配置相关的移动装置特征的决策节点的装置。

[0031] 在方面中,用于产生精实分类器模型以仅包含评估与移动装置的当前操作状态或配置相关的移动装置特征的决策节点的装置可包含:用于确定在不消耗移动装置的过多量的处理、存储器或能量资源的情况下应加以评估以分类所述行为的独特测试条件的数目的装置;用于通过顺序地遍历完整分类器模型中的多个测试条件且将与分类移动装置的行为相关的那些测试条件插入到测试条件列表中直至所述测试条件列表包含已确定的数目的独特测试条件来产生所述测试条件列表的装置;用于产生精实分类器模型以包含完整分类器模型中的测试被包含于所产生的测试条件列表中的条件中的一者的决策节点的装置。

附图说明

[0032] 被并入本文中且构成此说明书的部分的所附图式说明了本发明的实例方面,且与上文所给出的一般描述及下文所给出的详细描述一起用来解释本发明的特征。

[0033] 图 1 为说明实例电信系统的网络组件的通信系统框图,所述实例电信系统适合于与各种方面一起使用。

[0034] 图 2 为说明方面移动装置中的实例逻辑组件及信息流的框图,所述移动装置经配置以确定特定移动装置行为是恶意型、性能降级型、可疑型还是良性型。

[0035] 图 3 为说明方面系统中的实例组件及信息流的框图,所述系统包含经配置以结合移动装置来工作的网络服务器,所述移动装置经配置以:从完整分类器模型产生目标精实分类器模型;以及使用所述精实分类器模型来确定特定移动装置行为是恶意型、性能降级型、可疑型还是良性型。

[0036] 图 4 为进程流程图,其说明一种在移动装置中产生精实分类器模型以包含被包含于从网络服务器接收的完整分类器模型中的特征及数据点的子集的方面方法。

[0037] 图 5 为进程流程图,其说明根据各种方面的一种通过选择移动装置的装置特定特征并将其添加到精实分类器模型来在移动装置中产生或修改精实分类器模型的方法。

[0038] 图 6 为进程流程图,其说明根据各种方面的一种通过从完整分类器模型去除移动装置的装置特定特征来在移动装置中产生或修改精实分类器的方法。

[0039] 图 7 为进程流程图,其说明根据各种方面的另一种通过将移动装置的装置特定及装置状态特定特征添加到分类器模型来在移动装置中产生或修改精实分类器模型的方法。

[0040] 图 8 为进程流程图,其说明根据各种方面的另一种用于通过将移动装置的装置状态特定特征添加到分类器模型来在移动装置中产生或修改精实分类器模型的方法。

[0041] 图 9 为进程流程图,其说明根据各种方面的另一种用于通过将移动装置的装置状态特定特征添加到分类器模型来在移动装置中产生或修改精实分类器模型的方法。

[0042] 图 10 为适合于在方面中使用的移动装置的组件框图。

[0043] 图 11 为适合于在方面中使用的服务器装置的组件框图。

具体实施方式

[0044] 将参看所附图式来详细描述各种方面。在任何可能的地方,将贯穿图式而使用相同参考数字以指代相同或相似部分。对特定实例和实施方案所做的参考是用于说明性目的且并不打算限制本发明或权利要求书的范围。

[0045] 当前,存在用于将在计算装置上执行的应用程序的行为模型化的各种解决方案,

且可将这些解决方案与机器学习技术一起使用以确定软件应用程序是恶意型还是良性型的。但是,这些解决方案并不适合于在移动装置上使用,因为所述解决方案需要评估非常大的行为信息库 (corpus),不动态地产生行为模型,不考虑计算装置的装置特定特征或装置状态特定特征,不智能地对行为模型中的特征进行优先级排序,被限制到评估个别应用程序或进程,和 / 或需要在移动装置中执行计算密集型进程。因而,在移动装置中实施或执行这些现有解决方案可对移动装置的响应性、性能或功率消耗特性具有显著的负面和 / 或用户可察觉的影响。

[0046] 举例来说,计算装置可经配置以:使用现有的基于机器学习的解决方案来存取及使用训练数据的大型库;导出将特征向量作为输入的模型;以及使用此模型来确定计算装置的软件应用程序是恶意型还是良性型。但是,此解决方案不产生完整分类器模型(即,强健的数据或行为模型),所述完整分类器模型以可供移动装置使用以快速地产生精实分类器模型的格式或信息结构(例如,有限状态机等)来描述大的行为信息库。至少出于这个原因,此类解决方案不允许移动装置产生包含、测试或考虑装置特定或装置状态特定特征的精实分类器模型。另外,这个解决方案不允许移动装置产生精实分类器模型,所述精实分类器模型根据特征与分类特定移动装置(在所述特定移动装置中使用所述模型)中的特定行为的相关性来智能地识别所述特征或对所述特征进行优先级排序。出于这些及其它原因,此类解决方案无法在不对移动装置的响应性、性能或功率消耗特性具有显著的负面或用户可察觉的影响的情况下由移动装置处理器使用以快速地且高效地识别、分析或分类复杂的移动装置行为。

[0047] 除现有解决方案的上述限制之外,许多行为模型化解决方案还实施“一刀切”方法以将计算装置的行为模型化,且因此不适合于在移动装置中使用。也就是说,这些解决方案通常产生行为模型,使得所述行为模型为泛用的且可用于许多计算装置中和 / 或与多种不同硬件及软件配置一起使用。因而,这些泛用的行为模型常常包含 / 测试非常大数目的特征,所述特征中的许多特征与识别、分析或分类特定计算装置(在所述特定计算装置中实际使用所述行为模型)中的行为不相关(且因此不能用于识别、分析或分类特定计算装置中的行为)。另外,这些解决方案并不基于特征与分类特定移动装置(在所述特定移动装置中使用所述模型)中的特定行为的相关性来将相对优先级指派给所述特征。因此,这些解决方案通常需要计算装置应用包含大量无组织、经不恰当地优先级排序或不相关的特征的行为模型。这些模型不适合于在资源受约束的移动装置中使用,这是因为所述模型可使移动装置处理器分析对识别移动装置随时间的过去而降级的原因或来源无用的大量特征。因而,这些现有解决方案不适合于在复杂却又资源受约束的移动装置中使用。

[0048] 现代移动装置为非常可配置及复杂的系统。因而,对确定特定移动装置行为是良性型还是非良性型(例如,恶意型或性能降级型)最为重要的特征在每一移动装置中可为不同的。另外,不同特征组合可需要在每一移动装置中进行监视和 / 或分析以便使那个移动装置快速地且高效地确定特定行为是良性型还是非良性型。但是,可常常仅使用从特定移动装置(将在所述特定移动装置中监视或分析行为)获得的装置特定信息来确定需要监视及分析的特征的精确组合及每一特征或特征组合的相对优先级或重要性。出于这些及其它原因,在不同于特定装置(在所述特定装置中使用行为模型)的任何计算装置中所产生的行为模型无法包含识别对分类那个装置中的行为最为重要的特征的精确组合的信息。

[0049] 举例来说,如果第一移动装置经配置以使用其生物测定传感器(例如,指纹读取器、语音识别子系统、视网膜扫描仪等)来授权金融交易,那么测试与对所述生物测定传感器的存取及使用有关的条件的特征很可能与确定所观察到的存取金融软件的行为在彼移动装置中是恶意型还是良性型的过程相关。举例来说,对第一移动装置中的生物测定传感器的存取及使用可指示恶意应用程序正在用户不知道或不同意的情况下授权金融交易。另一方面,测试与对这些传感器的存取及使用有关的条件的特征不太可能与确定所观察到的存取金融软件的行为在第二移动装置(其未经配置成使用其生物测定传感器来授权金融交易)中是恶意型还是良性型的过程相关。也就是说,由于第一装置及第二装置可在除其使用其生物测定传感器的配置之外的所有方面均相同(即,为相同类型、型号、操作系统、软件等),所以产生准确地识别评估两个装置的与对生物测定传感器的存取及使用有关的条件的特征的泛用行为模型将具挑战性。产生测试数十万(或数百万)个经类似地配备却又可独立地配置的移动装置上的复杂得多的条件或特征的泛用模型将甚至更具挑战性。

[0050] 概言之,各种方面通过将网络服务器及移动装置配置成彼此结合地工作以高效地识别、分类、模型化、防止和/或校正常常使移动装置的性能和/或功率利用水平随时间的过去而降级的条件和/或移动装置行为来克服当前解决方案的这些限制。网络服务器可经配置以:从中心数据库(例如,“云”)接收关于各种条件、特征、行为及校正动作的信息;以及使用此信息来产生完整分类器模型(即,数据或行为模型),所述完整分类器模型以可被移动装置快速地转换为一或多个精实分类器模型的格式或结构(例如,有限状态机等)来描述大的行为信息库。

[0051] 在方面中,完整分类器模型可为大的行为信息库的有限状态机描述或表示。在方面中,有限状态机可包含适合于表现为多个节点、加速确定树或决策树桩(stump)(每一者测试一或多个特征)的信息。举例来说,有限状态机可为可被表现为一系列加速决策树桩的信息结构,所述加速决策树桩共同地识别、描述、测试或评估与确定移动装置行为是良性型还是促成那个移动装置的性能随时间的过去而降级相关的特征及数据点中的所有或许多特征及数据点。网络服务器可接着将完整分类器模型(即,包含有限状态机和/或加速决策树桩的系列的信息结构等)发送到移动装置。

[0052] 移动装置可经配置以接收及使用完整分类器模型来产生装置特定和/或装置状态特定的精实分类器模型或具不同等级的复杂性(或“精实性”)的精实分类器模型的系列。为了实现此,移动装置可剪除或淘汰被包含于从网络服务器接收的完整分类器模型中的强健的加速确定树系列(本文中为“完整加速确定树分类器模型”)以产生精实分类器模型,所述精实分类器模型包含减少的数目的加速确定树和/或评估有限数目的测试条件或特征。移动装置可接着使用此本地地产生的装置特定和/或装置状态特定分类器模型来执行实时行为监视及分析操作,且识别不合意或使性能降级的移动装置行为的来源或原因。

[0053] 通过产生将大的行为信息库描述或表现为有限状态机、决策节点、确定树或可加以修改、淘汰、扩充或以其它方式使用以产生精实分类器模型的其它类似的信息结构的完整分类器模型,各种方面允许移动装置快速地、高效地且在不存取训练数据或另外与网络服务器、中心数据库或云网络/服务器通信的情况下产生精实分类器模型。此显著地减小了移动装置对网络的依赖性,且改善了移动装置的性能及功率消耗特性。

[0054] 另外,通过在移动装置中本地地产生精实分类器模型以考虑装置特定或装置状态

特定特征, 各种方面允许移动装置将其监视操作集中于对识别不合意或破坏性能的移动装置行为的来源或原因最为重要的特征或因素。此允许移动装置在不引起所述移动装置的响应性、性能或功率消耗特性方面的显著负面或用户可察觉的改变的情况下识别并响应于不合意或使性能降级的移动装置行为。

[0055] 数个不同蜂窝式及行动通信服务与标准在未来是可用的或预期的, 所有所述蜂窝式及行动通信服务与标准可实施各种方面并受益于各种方面。这些服务及标准包含 (例如) 第三代合作伙伴计划 (3GPP)、长期演进 (LTE) 系统、第三代无线行动通信技术 (3G)、第四代无线行动通信技术 (4G)、全球行动通信系统 (GSM)、通用行动电信系统 (UMTS)、3GSM、通用分组无线电服务 (GPRS)、码分多址 (CDMA) 系统 (例如, cdmaOne、CDMA1020TM)、GSM 演进增强数据速率 (EDGE)、进阶移动电话系统 (AMPS)、数字 AMPS (IS-136/TDMA)、演进数据优化 (EV-DO)、数字增强无线电信 (DECT)、微波存取全球互通 (WiMAX)、无线局域网 (WLAN)、Wi-Fi 保护存取 I&II (WPA、WPA2) 及集成数字增强网络 (iden)。这些技术中的每一者涉及 (例如) 语音、数据、信令和 / 或内容消息的传输及接收。应理解, 除非在权利要求书语言中具体叙述, 否则对与个别电信标准或技术有关的术语和 / 或技术细节的任何参考是仅用于说明性目的且并不意欲将权利要求书的范围限制到特定通信系统或技术。

[0056] 术语“移动计算装置”及“移动装置”在本文中可互换地使用以指以下各者中的任一者或全部: 蜂窝式电话、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、智能笔记本电脑计算机、轻量级笔记本电脑计算机、掌上计算机、无线电子邮件接收器、多媒体具因特网能力的蜂窝式电话、无线游戏控制器, 及包含存储器、可程序化处理器 (对于所述可程序化处理器来说, 性能是重要的) 且由电池供电而操作 (使得省电方法有益处) 的类似的个人电子装置。尽管各种方面对于具有有限资源且依靠电池供电而执行的例如智能电话等移动计算装置特别有用, 但所述方面一般来说在包含处理器且执行应用程序的任何电子装置中有用。

[0057] 一般来说, 移动装置的性能及功率效率随时间的过去而降级。近年来, 防毒公司 (例如, McAfee、Symantec 等) 已开始销售旨在减缓此降级的行动防毒、防火墙及加密产品。但是, 许多这些解决方案依赖于在移动装置上周期性地执行计算密集型扫描引擎, 此可消耗移动装置的许多处理及电池资源, 在延长的时间周期中减缓移动装置或使移动装置不能使用和 / 或以其它方式使用用户体验降级。另外, 这些解决方案通常被限制到检测已知的病毒及恶意软件, 且未解决常常相组合以促成移动装置随时间的过去而降级的多个复杂因素和 / 或互动 (例如, 当性能降级并非由病毒或恶意软件引起时)。出于这些及其它原因, 现有的防毒、防火墙及加密产品不提供适当解决方案来识别可促成移动装置随时间的过去而降级的众多因素, 防止移动装置降级或高效地使老化的移动装置恢复到其原始条件。

[0058] 移动装置为具有相对有限的处理、存储器及能量资源的资源受约束的系统。现代移动装置也是复杂系统, 其具有可促成移动装置的性能及功率利用水平随时间的过去而降级的各种各样的因素。可促成性能降级的因素的实例包含拙劣设计的软件应用程序、恶意软件、病毒、片断的存储器及背景进程。归因于这些因素的数目、多样性及复杂性, 评估可使现代移动装置的复杂却又资源受约束的系统的性能和 / 或功率利用水平降级的所有各种组件、行为、进程、操作、条件、状态或特征 (或其组合) 常常是不可行的。因而, 用户、操作系统或应用程序 (例如, 防病毒软件等) 难以准确且高效地识别这些问题的来源。结果, 移

动装置用户当前几乎不具有用于防止移动装置的性能及功率利用水平随时间的过去而降级或用于使老化的移动装置恢复到其原始的性能及功率利用水平的补救法。

[0059] 各种方面还包含综合性行为监视及分析系统,其用于智能地且高效地识别、防止和 / 或校正常常使移动装置的性能和 / 或功率利用水平随时间的过去而降级的条件、因素和 / 或移动装置行为。在方面中,移动装置的观察器进程、精灵协助程序、模块或子系统(本文中统称作“模块”)可检测(instrument)或协调在移动装置系统的各种层级处的各种应用程序编程接口(API)、寄存器、计数器或其它组件(本文中统称作“被检测组件”)。观察器模块可通过从被检测组件收集行为信息来持续地(或接近持续地)监视移动装置行为。移动装置还可包含分析器模块,且观察器模块可将所收集的行为信息传达(例如,经由存储器写入操作、函数调用等)到所述分析器模块。分析器模块可接收并使用行为信息来产生行为向量,基于行为向量来产生空间和 / 或时间相关,且使用此信息来确定特定移动装置行为、条件、子系统、软件应用程序或进程是良性型、可疑型还是非良性型(即,恶意型或性能降级型)。移动装置可接着使用此分析的结果来消除、补救、隔离或以其它方式修复或响应于所识别的问题。

[0060] 分析器模块还可经配置以执行实时行为分析操作,所述实时行为分析操作可包含实行、执行数据、算法、分类器或模型(本文中统称作“分类器模型”)和 / 或将数据、算法、分类器或模型应用到所收集的行为信息以确定移动装置行为是良性型还是非良性型(例如,恶意型或性能降级型)。每一分类器模型可为行为模型,其包含可供移动装置处理器使用以评估移动装置的行为的特定特征或方面的数据和 / 或信息结构(例如,特征向量、行为向量、组件列表等)。每一分类器模型还可包含用于监视移动装置中的数个特征、因素、数据点、输入项、API、状态、条件、行为、应用程序、进程、操作、组件等(本文中统称为“特征”)的决策准则。分类器模型可被预安装于移动装置上,从网络服务器下载或接收,在移动装置中产生,或其任何组合。可通过使用群众外包(crowd sourcing)解决方案、行为模型化技术、机器学习算法等来产生分类器模型。

[0061] 可将每一分类器模型归类为完整分类器模型或精实分类器模型。完整分类器模型可为经产生作为大型训练数据集的函数的强健数据模型,其可包含数千个特征及数十亿个输入项。精实分类器模型可为从精简数据集产生的较集中的数据模型,其仅包含 / 测试对于确定特定移动装置行为是良性型还是非良性型(例如,恶意型或性能降级型)最为相关的特征 / 输入项。

[0062] 如上文所提到,可存在需要分析以恰当地识别移动装置的降级的原因或来源的数千个特征 / 因素及数十亿个数据点。因此,可对非常大数目的特征来训练分类器模型以便支持所有款式及型号的移动装置,且使每一移动装置做出关于特定移动装置行为是良性型还是非良性型(例如,恶意型或性能降级型)的准确决策。但是,由于移动装置为资源受约束的系统,所以对于移动装置来说评估所有这些特征常常是不可行的。此外,移动装置呈现许多不同配置及种类,但很少有移动装置(如果有的话)包含可在完整分类器模型中提到的每一特征或功能性。各种方面产生精实分类器模型,分析器模块可应用所述精实分类器模型以评估与移动装置最为相关的特征的目标子集,从而限制在分类移动装置行为时使用完整分类模式的情况下原本会执行的测试条件及分析的数目。

[0063] 各种方面包含移动装置及网络服务器,所述移动装置及网络服务器经配置成彼此

结合地工作以智能地且高效地识别与确定移动装置行为是良性型还是非良性型（例如，恶意型或性能降级型）最为相关的特征、因素及数据点。通过在移动装置中本地地产生考虑到装置特定特征和 / 或装置状态特定特征的精实分类器模型，各种方面允许移动装置处理器在不引起移动装置的响应性、性能或功率消耗特性方面的显著负面或用户可察觉的改变的情况下应用集中的分类器模型以快速且高效地识别、分析或分类复杂的移动装置行为（例如，经由观察器模块及分析器模块等）。

[0064] 可通过网络服务器来产生完整分类器模型，所述网络服务器经配置以从云服务 / 网络接收关于移动装置行为及在那些行为期间或特征化那些行为的状态、特征及条件的大量信息。此信息可呈移动装置行为向量的非常大的云库的形式。网络服务器可使用此信息来产生准确地描述行为向量的非常大云库的完整分类器模型（即，强健数据 / 行为模型）。网络服务器可产生完整分类器模型以包含可促成数个不同款式、型号及配置的移动装置中的任一者随时间的过去而降级的特征、数据点和 / 或因素中的所有或大部分特征、数据点和 / 或因素。

[0065] 在方面中，网络服务器可产生完整分类器模型以包含有限状态机表现或表示，例如可被快速且高效地淘汰、修改或转换为适合于在移动装置处理器中使用或执行的精实分类器模型的加速确定树 / 树桩或加速确定树 / 树桩的系列等。所述有限状态机表现或表示可为包含测试条件、状态信息、状态转变规则及其它类似信息的信息结构。在方面中，有限状态机表现或表示可为包含大型或强健的加速决策树桩系列的信息结构，所述加速决策树桩中的每一者评估或测试移动装置行为的特征、条件或方面。

[0066] 移动装置可经配置以：从网络服务器接收完整分类器模型；以及使用所接收的完整分类器模型来产生特定用于移动装置的特征及功能性的精实分类器模型（即，数据 / 行为模型）。

[0067] 在各种方面中，移动装置可使用行为模型化及机器学习技术来智能地且动态地产生精实分类器模型，使得所述精实分类器模型：考虑到移动装置的装置特定和 / 或装置状态特定特征（例如，与移动装置配置、功能性、所连接 / 所包含硬件等相关的特征）；包含、测试或评估经确定为对于识别移动装置随时间的过去而降级的原因或来源重要的特征的集中且目标子集；和 / 或基于识别特征对于成功地分类特定移动装置（在所述特定移动装置中使用 / 评估所述特征）中的行为的相对重要性的机率或信赖度值来对特征的目标子集进行优先级排序。

[0068] 通过在移动装置（在所述移动装置中使用分类器模型）中产生分类器模型，各种方面允许移动装置准确地识别在确定那个特定移动装置上的行为是良性型还是促成彼装置性能降级的过程中最为重要的特定特征。这些方面还允许移动装置根据精实分类器模型中的特征对分类那个特定移动装置中的行为的相对重要性来准确地对所述特征进行优先级排序。

[0069] 装置特定或装置状态特定信息的使用允许移动装置快速地识别应被包含于精实分类器模型中的特征且对所述特征进行优先级排序，以及识别应从精实分类器模型排除的特征。举例来说，移动装置可经配置以识别被包含于完整模型中的特征 / 节点 / 树 / 树桩且从精实分类器模型排除所述特征 / 节点 / 树 / 树桩，所述特征 / 节点 / 树 / 树桩测试基于移动装置的特定特征集合而不存在于或不能存在于所述移动装置中的条件且因此与所

述移动装置不相关。举例来说,不包含生物测定传感器的移动装置可从精实分类器模型排除测试或评估与生物测定传感器的使用有关的条件的所有特征 / 节点 / 树桩。

[0070] 另外,由于精实分类器模型包含必须加以评估的状态、特征、行为或条件的精简子集(即,与完整分类器模型相比较),所以观察器模块和 / 或分析器模块可在不消耗移动装置的过多量的处理、存储器或能量资源的情况下使用精实分类器模型来快速地且准确地确定移动装置行为是良性型还是非良性型(例如,恶意型或性能降级型)。

[0071] 在方面中,移动装置可经配置以使用完整分类器模型来产生具不同等级的复杂性(或“精实性”)的精实分类器模型的系列。可常规地应用精实分类器模型的最精实系列(即,基于最少数目的测试条件的精实分类器模型)直至遇到所述模型不能归类为良性型或恶意型(且因此由所述模型归类为可疑型)的行为为止,此时,可应用较强健(即,较不精实)的精实分类器模型以尝试将所述行为归类为良性型或恶意型。可应用所产生的精实分类器模型的系列内的愈发强健的精实分类器模型直至达成对行为的明确分类为止。以此方式,观察器模块和 / 或分析器模块可通过将对最完全但为资源密集的精实分类器模型的使用限制到需要强健分类器模型来明确地分类行为的那些情形而在效率与准确度之间达到平衡。

[0072] 在各种方面中,移动装置可经配置以通过以下步骤来产生一或多个精实分类器模型:将有限状态机表示 / 表现转换为加速决策树桩;基于移动装置特定状态、特征、行为、条件或配置来剪除或淘汰所述组完整的加速决策树桩以包含被包含于完整分类器模型中的加速决策树桩的一或多个子集;以及使用加速决策树桩的所述一或多个子集来智能地监视、分析和 / 或分类移动装置行为。

[0073] 加速决策树桩的使用允许观察器模块和 / 或分析器模块在不与云或网络通信的情况下产生及应用精实数据模型以重新训练数据,这样显著地减少移动装置对网络服务器及云的依赖性。此消除了移动装置与网络服务器之间的反馈通信,从而进一步改善了移动装置的性能及功率消耗特性。

[0074] 加速决策树桩是具有正好一个节点(及因此一个测试问题或测试条件)及权值的一级确定树,且因此非常适合于用于数据 / 行为的二进制分类中。也就是说,将行为向量应用到加速决策树桩产生了二进制回答(例如,是或否)。举例来说,如果由加速决策树桩所测试的问题 / 条件为“短信服务(SMS)传输的频率小于每分钟 x 次?”,那么将值“3”应用到加速决策树桩将产生“是”回答(对于“小于 3 次”SMS 传输来说)或“否”回答(对于“3 或大于 3 次”SMS 传输来说)。

[0075] 加速决策树桩是高效的,这是因为其非常简单且原始(且因此不需要显著的处理资源)。加速决策树桩还是非常可并行化的,且因此可并行 / 同时应用或测试许多树桩(例如,通过移动装置中的多个核心或处理器)。

[0076] 如下文所描述,网络服务器(或另一计算装置)可从移动装置行为的另一更复杂模型(诸如,加速确定树模型)产生加速决策树桩型完整分类器模型。这些复杂模型可使特征化尖端分类系统中的移动装置行为的装置状态、操作及受监视节点间的互动的完整(或接近完整)集合相关。如上文所提到,服务器或其它计算装置可通过应用机器学习技术以产生描述从大量移动装置收集的移动装置行为向量的云库的模型来产生完整、复杂的分类器模型。作为实例,加速确定树分类器模型可追踪穿过可测试条件的决策节点而实现对当

前移动装置行为是恶意型还是良性型的确定的数百条路径。可使用许多已知的学习及相关模型化技术在服务器中产生这些复杂模型。尽管这些复杂模型可通过向来自成百上千个移动装置的数据学习而在准确地辨识恶意行为方面变得非常有效,但将所述复杂模型应用到特定移动装置的配置及行为可能需要显著处理(尤其是在模型涉及复杂、多级确定树的情况下)。由于移动装置通常在资源方面受限制,所以使用这些模型可影响装置性能及电池寿命。

[0077] 为了提供更有利于供移动装置使用的强健分类器模型,服务器(例如,云服务器或网络服务器)或另一计算装置(例如,移动装置或将耦合到移动装置的计算机)可将复杂的分类器模型变换为大型加速决策树桩模型。决策树桩中所涉及的较简单确定及在并行进程中应用这些分类器模型的能力可使得移动装置能够更好地受益于由网络服务器执行的分析。又,如下文所论述,可由移动装置使用加速决策树桩完整分类器模型来产生精实分类器模型以基于装置特定或装置状态特定信息而包含(或排除)特征。此可通过配置移动装置处理器以执行下文所描述的方面方法来实现。

[0078] 在另外的方面中,移动装置可包含各种组件,所述组件经配置以将特定针对移动装置或移动装置的当前状态的特征并入到用以检测移动装置上的恶意行为的精实分类器模型或一组精实分类器模型中。

[0079] 在方面中,移动装置可经配置以产生精实分类器模型以包含被包含于完整分类器模型中的分类器准则的子集,且仅包含对应于与移动装置配置、功能性及所连接/所包含硬件相关的特征的那些分类器准则。移动装置可使用这(这些)精实分类器模型来仅监视存在的或与装置相关的那些特征及功能。移动装置可接着周期性地修改或重新产生所述精实分类器模型以基于移动装置的当前状态及配置来包含或去除各种特征及相对应的分类器准则。

[0080] 作为实例且在方面中,操作于移动装置上的行为分析器模块可接收大型加速决策树桩分类器模型(其中决策树桩与行为模型的完整特征集合相关联),且所述行为分析器模块可通过以下步骤而从大型分类器模型导出一或多个精实分类器模型:仅选择来自所述大型分类器模型的与移动装置的当前配置、功能性、操作状态和/或所连接/所包含硬件相关的特征;以及将对应于所述所选特征的加速决策树桩的子集包含于精实分类器模型中。在此方面中,对应于与移动装置相关的特征的特征的分类器准则可为被包含于大型分类器模型中的测试所选特征中的至少一者的那些加速决策树桩。在方面中,行为分析器模块可接着周期性地修改或重新产生加速决策树桩精实分类器模型以基于移动装置的当前状态及配置而包含或去除各种特征,使得精实分类器模型继续包含装置特定特征加速决策树桩。

[0081] 在方面中,操作于移动计算装置上的装置状态监视引擎可持续地监视移动装置以发现移动装置的配置和/或状态的改变。在另外的方面中,装置状态监视引擎可寻找可能影响行为分析器模块(或分类器模块)检测恶意行为的性能或有效性的配置和/或状态改变。举例来说,装置状态监视引擎可监视移动装置的行为直至检测到“低电池状态”为止,此时行为分析器模块可改变精实分类器模型以分析移动装置上的较少特征来发现恶意行为,以便节省能量。

[0082] 在另一方面中,当装置状态监视引擎检测到状态改变时,所述装置状态监视引擎可通知装置状态特定特征产生器,且装置状态特定特征产生器可向行为分析器模块传信以

基于移动装置的状态改变而添加或去除某些特征。

[0083] 在另一方面中,移动装置可包含经配置以确定与移动装置自身有关的特征的装置特定特征产生器。举例来说,装置特定特征产生器可确定移动装置包含近场通信、Wi-Fi 及 Bluetooth®能力。在另外的方面中,装置特定特征产生器可向行为分析器传信以基于与移动装置自身有关的特征而在精实分类器模型中包含或去除特征。因此,移动装置上的各种组件可修改精实分类器模型以反映特定针对移动装置的配置和 / 或移动装置的当前状态的特征,此可使得各种组件能够通过基于移动装置的当前状态对受监视的特征进行优先级排序来更好地检测恶意行为或改善移动装置的总性能。

[0084] 如上文所提到,可由移动装置处理以产生用于监视行为的精实分类器模型的一种类型的大型分类器模型的一个实例是加速决策树桩分类器模型。在以下的详细描述中,可参考加速决策树桩分类器模型;但是,除非技术方案明确叙述加速决策树桩分类器模型,否则这些参考是用于实例目的,且并不意欲限制权利要求书的范围。

[0085] 可将各种方面实施于例如图 1 中所说明的实例通信系统 100 等多种通信系统内。典型蜂窝式电话网络 104 包含耦合到网络操作中心 108 的多个蜂窝式基地台 106,所述网络操作中心 108 操作以连接移动装置 102(例如,蜂窝式电话、膝上型计算机、平板计算机等)与其它网络目的地之间的语音通话及数据(例如,经由电话陆线(例如,POTS 网络,未图标)及因特网 110 等)。可经由双向无线通信链路 112(例如,4G、3G、CDMA、TDMA、LTE 和 / 或其它蜂窝式电话通信技术等)来实现移动装置 102 与电话网络 104 之间的通信。电话网络 104 还可包含耦合到网络操作中心 108 或位于网络操作中心 108 内的一或多个服务器 114,所述一或多个服务器 114 提供到因特网 110 的连接。

[0086] 通信系统 100 可进一步包含连接到电话网络 104 及因特网 110 的网络服务器 116。网络服务器 116 与电话网络 104 之间的连接可经由因特网 110 或经由专用网络(如由虚线箭头说明)来达成。还可将网络服务器 116 实施为云服务提供商网络 118 的网络基础架构内的服务器。可经由电话网络 104、因特网 110、专用网络(未说明)或其任何组合来达成网络服务器 116 与移动装置 102 之间的通信。

[0087] 网络服务器 116 可将完整分类器模型发送到移动装置 102,所述移动装置 102 可接收及使用完整分类器模型以识别可疑型或性能降级型移动装置行为、软件应用程序、进程等。网络服务器 116 还可将分类及模型化信息发送到移动装置 102 以代替、更新、建立和 / 或维持移动装置分类模型。移动装置 102 可接收及使用完整分类器模型以产生适合于用于识别可疑型或性能降级型移动装置行为、软件应用程序、进程等的精实分类器模型。网络服务器 116 还可将分类及模型化信息发送到移动装置 102 以代替、更新、建立和 / 或维持移动装置数据 / 行为模型。

[0088] 在方面中,移动装置 102 可经配置以使用所收集的行为、状态、分类、模型化、成功率和 / 或统计信息来产生、更新或改进精实分类器模型(或数据 / 行为模型),所述精实分类器模型包含移动装置 102 中的特征的另一目标和 / 或精简的子集。此减少了移动装置与网络服务器 116 之间的反馈通信量,且改善了移动装置 102 的性能及功率消耗特性。

[0089] 图 2 说明方面移动装置 102 中的实例逻辑组件及信息流,所述移动装置 102 经配置以确定特定移动装置行为、软件应用程序或进程是恶意型 / 性能降级型、可疑型还是良性型。在图 2 中所说明的实例中,移动装置 102 包含行为观察器模块 202、行为分析器模块

204、分类器模块 208 及致动器模块 210。在方面中,可将分类器模块 208 实施为行为分析器模块 204 的部分。在方面中,行为分析器模块 204 可经配置以产生一或多个分类器模块 208,所述一或多个分类器模块 208 中的每一者可包含一或多个分类器。

[0090] 可将模块 202 到 210 中的每一者实施于软件、硬件或其任何组合中。在各种方面中,可将模块 202 到 210 实施于操作系统的部分内(例如,在内核内、在内核空间中、在用户空间中等)、分开的程序或应用程序内、特殊化硬件缓冲器或处理器中,或其任何组合。在方面中,可将模块 202 到 210 中的一或多者实施为执行于移动装置 102 的一或多个处理器上的软件指令。

[0091] 行为观察器模块 202 可经配置以检测或协调在移动装置的各种层级/模块处的应用程序编程接口(API),且经由经检测 API 来监视/观察在各种层级/模块处的移动装置操作及事件(例如,系统事件、状态改变等)、收集关于所观察到的操作/事件的信息、智能地过滤所收集的信息、基于经过滤的信息来产生一或多个观察及将所产生的观察存储于存储器中(例如,在记录档案等中)和/或将所产生的观察发送(例如,经由存储器写入、函数调用等)到行为分析器模块 204。

[0092] 行为观察器模块 202 可通过收集关于以下各者的信息来监视/观察移动装置操作及事件:应用程序构架或运行时间库中的库应用程序编程接口(API)呼叫、系统呼叫 API、文件系统及网络连接符系统操作、装置(包含传感器装置)状态改变及其它类似的事件。行为观察器模块 202 还可监视文件系统活动,其可包含搜寻文件名、档案存取类别(个人信息或普通数据文件)、建立或删除档案(例如,类型 exe、zip 等)、档案读取/写入/搜寻操作、改变档案权限等。

[0093] 行为观察器模块 202 还可监视数据网络活动,其可包含连接类型、协议、端口号、装置所连接到的服务器/客户端、连接数目、通信的量或频率等。行为观察器模块 202 可监视电话网络活动,其可包含监视被发出、接收或截获的通话或消息(例如, SMS 等)的类型及数目(例如,所拨打的高阶电话的数目)。

[0094] 行为观察器模块 202 还可监视系统资源使用率,其可包含监视分支(fork)的数目、存储器存取操作、开启的档案的数目等。行为观察器模块 202 可监视移动装置的状态,其可包含监视各种因素,例如显示器是接通还是关断、装置被锁定还是被解锁、剩余的电池电量、相机状态等。行为观察器模块 202 还可通过(例如)监视对关键性服务(浏览器、合同提供者等)的意图、进程间通信的程度、弹出窗口等来监视进程间通信(IPC)。

[0095] 行为观察器模块 202 还可监视/观察驱动程序统计数据 and / 或一或多个硬件组件的态势,所述一或多个硬件组件可包含相机、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、存取端口、定时器、外围装置、无线通信组件、外部存储器芯片、电压调节器、振荡器、锁相回路、外围网桥及用以支持执行于移动计算装置上的处理器及客户端的其它类似组件。

[0096] 行为观察器模块 202 还可监视/观察一或多个硬件计数器,所述一或多个硬件计数器表示移动计算装置和/或移动装置子系统的状态或态势。硬件计数器可包含处理器/核心的专用寄存器,所述专用寄存器经配置以存储发生于移动计算装置中的与硬件有关的活动或事件的计数或状态。

[0097] 行为观察器模块 202 还可监视/观察以下各者的动作或操作:软件应用程序、从应

用程序下载服务器（例如，Apple® App Store 服务器）的软件下载、由软件应用程序使用的移动装置信息、通话信息、文字消息传递信息（例如，SendSMS、BlockSMS、ReadSMS 等）、媒体消息传递信息（例如，ReceiveMMS）、用户帐户信息、位置信息、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、短程无线电通信（例如，Bluetooth®、WiFi 等）、基于文字的通信的内容、所记录的音频档案的内容、电话簿或联系人信息、联系人列表等。

[0098] 行为观察器模块 202 可监视 / 观察移动装置的传输或通信，其包含包含以下各者的通信：语音邮件 (VoiceMailComm)、装置识别符 (DeviceIDComm)、用户帐户信息 (UserAccountComm)、日历信息 (CalendarComm)、位置信息 (LocationComm)、所记录的音频信息 (RecordAudioComm)、加速计信息 (AccelerometerComm) 等。

[0099] 行为观察器模块 202 可监视 / 观察对罗盘信息、移动装置设定、电池寿命、陀螺仪信息、压力传感器、磁体传感器、屏幕活动等的使用及更新 / 改变。行为观察器模块 202 可监视 / 观察被传达到软件应用程序及从软件应用程序传达的通知 (AppNotifications)、应用程序更新等。行为观察器模块 202 可监视 / 观察关于第一软件应用程序请求下载和 / 或安装第二软件应用程序的条件或事件。行为观察器模块 202 可监视 / 观察关于用户验证的条件或事件（例如，密码的键入等）。

[0100] 行为观察器模块 202 还可监视 / 观察在移动装置的多个层级（包含应用层级、无线电层级及传感器层级）处的条件或事件。应用层级观察可包含：经由面部辨识软件来观察用户、观察社交串流 (social stream)、观察由用户键入的笔记、观察关于 PassBook/Google Wallet/Paypal 的使用的事件等。应用层级观察还可包含观察关于虚拟专用网络 (VPN) 的使用的事件，及关于同步、语音搜寻、语音控制（例如，通过说一个词来锁定 / 解锁电话）、语言翻译器、供计算的数据的卸除、视频串流传输、在无用户活动的情况下的相机使用、在无用户活动的情况下的麦克风使用等的事件。

[0101] 无线电层级观察可包含确定以下各者中的任何一或多者的出现、存在或量：在建立无线电通信链路或传输信息之前用户与移动装置的互动、双 / 多用户身分模块 (SIM) 卡、因特网无线电、移动电话系留、卸除供计算的数据、装置状态通信、作为游戏控制器或家用控制器的使用、车辆通信、移动装置同步等。无线电层级观察还可包含监视用于定位、对等式 (p2p) 通信、同步、车辆至车辆通信和 / 或机器至机器 (m2m) 的无线电 (WiFi、WiMax、Bluetooth®等) 的使用。无线电层级观察可进一步包含监视网络业务使用率、统计数据或配置文件。

[0102] 传感器层级观察可包含监视磁体传感器或其它传感器以确定移动装置的使用和 / 或外部环境。举例来说，移动装置处理器可经配置以确定电话是在护套中（例如，经由经配置以感测护套内的磁体的磁体传感器）还是在用户口袋中（例如，经由由相机或光传感器检测到的光的量）。检测到移动装置是在护套中可与辨识可疑行为相关，例如，因为当移动装置被放入护套中时发生与用户的有效使用有关的活动及功能（例如，拍摄照片或视频、发送消息、进行语音通话、记录声音等）可为有恶意的进程在装置上执行（例如，以追踪或暗中监视用户）的征兆。

[0103] 与使用或外部环境有关的传感器层级观察的其它实例可包含：检测近场通信

(NFC) ;收集来自信用卡扫描仪、条形码扫描仪或行动卷标读取器的信息 ;检测通用串行总线 (USB) 充电源的存在 ;检测到键盘或辅助装置已耦合到移动装置 ;检测到移动装置已耦合到计算装置 (例如,经由USB等) ;确定LED、闪光、闪光灯或光源是否已被修改或停用 (例如,恶意地停用紧急传信应用程序等) ;检测到扬声器或麦克风已被接通或通电 ;检测充电或供电事件 ;检测到移动装置正被用作游戏控制器,等。传感器层级观察还可包含收集来自医学或保健传感器或来自扫描用户身体的信息、收集来自被塞到USB/ 音频插孔中的外部传感器的信息、收集来自触感或触觉传感器的信息 (例如,经由振动器接口等)、收集关于移动装置的热状态的信息,等。

[0104] 为了将受监视的因素的数目减小到可管理水平,在方面中,行为观察器模块 202 可通过监视 / 观察一组初始的行为或因素来执行粗略观察,所述行为或因素是可促成移动装置降级的所有因素的小子集。在方面中,行为观察器模块 202 可从网络服务器 116 和 / 或云服务或网络 118 中的组件接收所述组初始行为和 / 或因素。在方面中,可在从网络服务器 116 或云服务 / 网络 118 接收的数据 / 行为模型中指定所述组初始的行为 / 因素。在方面中,可在精简特征模型 (RFM) 中指定所述组初始的行为 / 因素。

[0105] 行为分析器模块 204 和 / 或分类器模块 208 可从行为观察器模块 202 接收观察、将所接收的信息 (即,观察) 与从外部模块接收的内容脉络信息相比较,及识别与所接收的观察相关联的正促成 (或很可能促成) 装置随时间的过去而降级或可以其它方式引起装置上的问题的子系统、进程和 / 或应用程序。

[0106] 在方面中,行为分析器模块 204 和 / 或分类器模块 208 可包含用于利用一组有限的信息 (即,粗略观察) 来识别正促成 (或很可能促成) 装置随时间的过去而降级或可以其它方式引起装置上的问题的行为、进程或程序的智能。举例来说,行为分析器模块 204 可经配置以分析从各种模块 (例如,行为观察器模块 202、外部模块等) 收集的信息 (例如,呈观察的形式)、学习移动装置的正常操作行为,及基于比较的结果来产生一或多个行为向量。行为分析器模块 204 可将所产生的行为向量发送到分类器模块 208 以供进一步分析。

[0107] 分类器模块 208 可接收所述行为向量且将其与一或多个行为模块相比较以确定特定移动装置行为、软件应用程序或进程是性能降级型 / 恶意型、良性型还是可疑型。

[0108] 当分类器模块 208 确定行为、软件应用程序或进程为恶意型或性能降级型时,分类器模块 208 可通知致动器模块 210,所述致动器模块 210 可执行各种动作或操作以校正经确定为恶意型或性能降级型的移动装置行为和 / 或执行操作以消除、补救、隔离或以其它方式修复所识别的问题。

[0109] 当分类器模块 208 确定行为、软件应用程序或进程为可疑型时,分类器模块 208 可通知行为观察器模块 202,所述行为观察器模块 202 可调整其观察的粒度 (即,观察移动装置行为的详细级别) 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) 来改变所观察到的行为、产生或收集新的或额外的行为信息及将所述新的 / 额外信息发送到行为分析器模块 204 和 / 或分类器模块 208 以供进一步分析 / 分类。行为观察器模块 202 与分类器模块 208 之间的此反馈通信使得移动装置 102 能够递归地增加观察的粒度 (即,进行较精细或较详细的观察) 或改变所观察到的特征 / 行为直至识别可疑型或性能降级型移动装置行为的来源为止、直至达到处理或电池消耗阈值为止,或直至移动装置处理器确定不能从观察粒度的进一步增加来识别可疑型或性能降级型移动装置行为的来源为

止。此反馈通信还使得移动装置 102 能够在不消耗移动装置的过多量的处理、存储器或能量资源的情况下在移动装置中本地地调整或修改数据 / 行为模型。

[0110] 在方面中,行为观察器模块 202 及行为分析器模块 204 可提供(个别地或共同地)对计算系统的行为的实时行为分析以从有限及粗略的观察识别可疑型行为、动态地确定有待于更详细地观察的行为,及动态地确定进行所述观察所需的详细程度。以此方式,行为观察器模块 202 使得移动装置 102 能够在不需要装置上的大量处理器、存储器或电池资源的情况下高效地识别问题并防止在移动装置上发生所述问题。

[0111] 图 3 说明方面系统 300 中的实例组件及信息流,所述系统 300 包含移动装置 102,所述移动装置 102 经配置以结合网络服务器 116 来工作从而在不消耗移动装置的过多量的处理、存储器或能量资源的情况下智能地且高效地识别移动装置 102 上的有恶意或拙劣地撰写的软件应用程序和 / 或可疑型或性能降级型移动装置行为。

[0112] 在图 3 中所说明的实例中,网络服务器 116 包含云模块 302、模型产生器 304 模块及训练数据模块 306。移动装置 102 包含行为观察器模块 202、分析器模块 204、致动器模块 210、状态监视引擎 312、状态特定特征产生器 314、装置特定特征产生器 316 及装置特征监视引擎 318。在各种方面中,可包含以下各者或可将以下各者实施为行为分析器模块 204 的部分或分类器模块 208(图 3 中未说明)的部分:状态监视引擎 312、状态特定特征产生器 314、装置特定特征产生器 316 和 / 或装置特征监视引擎 318。

[0113] 云模块 302 可经配置以从云服务 / 网络 118 接收大量信息,所述信息包含可促成移动装置随时间的过去而降级的特征、数据点和 / 或因素中的所有或大部分特征、数据点和 / 或因素。

[0114] 模型产生器 304 可使用在云模块 302 中所接收的信息及训练数据(例如,经由训练数据模块 306)来产生完整或强健分类器模型,所述完整或强健分类器模型包含或识别可促成移动装置随时间的过去而降级的特征、数据点和 / 或因素中的所有或大部分特征、数据点和 / 或因素。

[0115] 在各种方面中,网络服务器 116 可经配置以通过实行、执行机器学习和 / 或内容脉络模型化技术和 / 或将机器学习和 / 或内容脉络模型化技术应用到行为信息和 / 或由许多移动装置提供的行为分析的结果或从云服务 / 网络 118 接收的其它信息来产生完整分类器模型。因此,网络服务器 116 可从许多移动装置接收大量报告且分析、合并此群众外包的信息或以其它方式将此群众外包的信息变成可用信息(尤其是可供所有移动装置使用或存取的行为模型)。网络服务器 116 可在从移动装置接收到新的行为 / 分析报告时持续地重新评估现有的行为模型,和 / 或基于历史信息(例如,从先前执行所收集、行为模型的先前应用等)、新信息、机器学习、内容脉络模型化及在可用信息、移动装置状态、环境条件、网络条件、移动装置性能、电池消耗级别等方面的所检测到的改变来产生新的或更新的行为模型。

[0116] 在方面中,模型产生器 304 可产生完整分类器模型以包含有限状态机表示,例如可被快速地且高效地淘汰、修改或被转换为适合于在移动装置处理器中使用或执行的精实分类器模型的加速决策树桩或加速决策树桩的系列。所述有限状态机表现或表示可为包含测试条件、状态信息、状态转变规则及其它类似的信息的信息结构。在方面中,有限状态机表现或表示可为包含加速决策树桩的大型或强健系列的信息结构,所述加速决策树桩中的

每一者评估或测试移动装置行为的条件、特征、因素或方面。

[0117] 模型产生器 304 模块可将完整分类器模块发送到移动装置 102, 所述移动装置 102 可经配置以基于在云模块 302 中所产生的完整模型来产生精实数据 / 行为模型。在方面中, 移动装置 102 可经配置以使用完整分类器模型来产生具不同等级的复杂性 (或“精实性”) 的精实分类器模型的系列。

[0118] 在方面中, 产生精实数据 / 行为模型可包含产生一或多个精简特征模型 (RFM), 所述一或多个 RFM 包含被包含于在网络服务器 112 中所产生的完整模型中的特征及数据点的子集。在方面中, 移动装置可产生精实数据 / 行为模型, 所述精实数据 / 行为模型包含初始特征集合 (例如, 初始精简特征模型), 所述初始特征集合包含经确定为具有使得行为分析器模块 204 能够结论性地确定特定移动装置行为是良性型还是恶意型 / 性能降级型的最高机率的信息。

[0119] 在方面中, 移动装置 102 可经配置以淘汰被包含于从网络服务器 112 接收的完整分类器模型中的加速决策树桩的系列, 从而产生精实分类器模型, 所述精实分类器模型包含减少的数目的加速决策树桩和 / 或评估有限数目的测试条件。可通过以下步骤来实现对完整加速决策树桩分类器模型的此淘汰: 选择加速决策树桩; 识别与所选的决策树桩取决于相同的移动装置特定状态、特征、行为或条件 (及因此可基于一个确定结果加以应用) 的所有其它加速决策树桩; 将取决于相同的移动装置特定状态、特征、行为或条件的所选的加速决策树桩及所有所识别的其它加速决策树桩包含于精实分类器模型中; 以及针对尚未被包含于精实分类器模型中的有限数目的所选的加速决策树桩而重复所述进程。以此方式, 可产生包含取决于有限数目的不同移动装置特定状态、特征、行为或条件的所有加速决策树桩的精实分类器模型。移动装置可接着在不消耗其过多量的处理、存储器或能量资源的情况下使用此本地地产生的精实分类器模型来快速地分类移动装置行为。

[0120] 加速决策树桩是具有正好一个节点 (及因此一个测试问题或测试条件) 及权值的一级确定树, 且因此非常适合于用于数据 / 行为的二进制分类中。也就是说, 将行为向量应用到加速决策树桩产生了二进制回答 (例如, 是或否)。举例来说, 如果由加速决策树桩所测试的问题 / 条件为“SMS 传输的频率小于每分钟 x 次?”, 那么将值“3”应用到加速决策树桩将产生“是”回答 (对于“小于 3 次”SMS 传输来说) 或“否”回答 (对于“3 或大于 3 次”SMS 传输来说)。

[0121] 树桩是高效的, 因为其非常简单且是原始的 (及因此不需要显著的处理资源)。树桩还是非常可并行化的, 且因此可并行 / 同时应用许多树桩 (例如, 通过移动装置中的多个核心或处理器)。

[0122] 在方面中, 移动装置 102 的行为分析器模块 204 可在不存取网络服务器 116 上的训练数据 (例如, 来自训练数据模块 306) 的情况下以决策树桩的形式产生精实分类器模型, 借此消除对移动装置 102 与网络服务器 116 之间的反馈通信的需求。换句话说, 行为分析器模块 204 可在不与云或网络通信以重新训练数据的情况下产生及应用精实分类器模型, 这样显著地减少了移动装置对云的依赖性 (及因此改善了移动装置的性能及功率消耗特性)。行为分析器模块 204 还可使用加速决策树桩来分类计算装置行为以识别恶意软件或恶意行为。

[0123] 在方面中, 移动装置可经配置以执行“联合特征选择及剪除”操作, 所述操作允

许移动装置；在无需存取云训练数据的情况下在运作中产生精实分类器模型、每应用程序动态地重新配置所述分类器以增强分类准确度，及指定每一分类器的确定复杂性（例如， $O(\text{树桩的数目})$ ）。

[0124] 在方面中，“联合特征选择及剪除”操作可包含执行特征选择操作。举例来说，行为分析器模块 204 可确定其需要产生测试 2 个独特特征（例如，F1 及 F3）的精实分类器模型，在这种情况下，特征选择操作可包含遍历 100 个加速决策树桩的列表直至发现最初 2 个独特特征（例如，F1 及 F3）为止。

[0125] 行为分析器模块 204 可接着仅测试由特征选择操作所识别的特征（例如，F1 及 F3），此可通过遍历 100 个加速决策树桩的整个列表且删除测试不同特征 / 条件（例如，F5）的任何树桩来实现。可在不重新训练数据的情况下将剩余的加速决策树桩（即，测试条件“F1”及“F3”的树桩）用作精实分类器模型。行为分析器模块 204 可将行为信息（例如，呈行为向量的形式）应用到剩余的加速决策树桩中的每一者、计算从剩余树桩接收的所有回答的加权平均值，及使用所述加权平均值来确定移动装置行为是恶意型还是良性型。

[0126] 一旦已经由特征选择及剪除进程产生了加速决策树桩，行为分析器模块 204 便可将所选的决策树桩用作行为模型，行为分析器模块 204 可将所述行为模型与当前装置状态、设定及行为相比较。由于决策树桩是独立的二进制测试，所以行为分析器模块 204 可并行地执行将所观察到的行为（其可被概述于行为向量中）与模型相比较的行为分析进程。而且，由于树桩非常简单（基本上为二进制），所以用以执行每一树桩的处理可非常简单且因此可以较少的处理额外耗用而快速地实现。由于每一决策树桩产生具有权值的回答，所以可将行为分析器模块 204 的关于行为是恶意型还是良性型的最终决策确定为所有结果的加权总和，这也可以是简单计算。

[0127] 因此，在方面中，行为分析器模块 204 可从移动装置 102 上的正在进行的行为的观察（从行为观察器模块 202 接收）而产生行为向量，且行为分析器模块 204 可将所述行为向量应用到加速决策树桩以确定移动装置 102 上的正在进行的行为是恶意型还是良性型。

[0128] 在另外的方面中，行为分析器模块 204 可修改由于执行联合特征选择及剪除操作所产生的精实分类器模型以并有移动装置 102 特有和 / 或移动装置 102 特有的当前状态 / 配置的特征。在方面中，行为分析器模块 204 从大型分类器模型（从网络服务器 116 接收）产生的精实分类器模型可不充分地表示移动装置 102 的特征及当前行为。举例来说，从网络服务器 116 接收的大型分类器模型可仅包含与近场通信有关的少量行为向量 / 模型，因此如果行为分析器模块 204 在不顾被包含于移动装置上的特征的情况下产生精实分类器模型，那么其可能会省略与近场通信有关的少数特征。但是，考虑到近场通信在实行某些金融交易（例如，Google Wallet）中的重要性，可十分需要将近场通信特征包含于精实分类器模型中以便检测可具有显著金融意义的恶意活动（例如，将信用卡信息发送到黑客）。作为另一实例，如果移动装置 102 连接到不安全的无线接入点，那么由于未授权存取或其它恶意活动的风险增加，移动装置可受益于对 Wi-Fi 行为的增加的警惕性。各种方面通过在将全局模型剪除直至用以监视移动装置行为及状态的精实分类器模型时考虑被包含于移动装置上或连接到移动装置的所有特征及功能来解决这些顾虑。

[0129] 另外，如果精实分类器模型包含不再与移动装置 102 相关的特征（归因于移动装置 102 的配置或状态改变），那么所述模型监视恶意行为的有效性可变得低于原本可能的

程度。举例来说,如果移动装置被置于“飞航模式”,从而切断无线连接,那么与调制解调器活动及消息传输有关的特征变得不相关。作为另一实例,如果 WiFi 收发器被停用,那么与 WiFi 通信活动有关的特征变得不相关。

[0130] 在方面中,通过在移动装置的状态及配置发生改变及演进时修改或更新从大型分类器模型导出的精实分类器模型,行为分析器模块 204 可确保与移动装置和 / 或移动装置的当前状态有关的重要特征被包含于精实分类器模型中,而不相关特征被去除。通过包含重要特征,行为分析器模块 204 可以较高信赖度来检测恶意行为,因为移动装置的更多相关特征正受监视。

[0131] 行为分析器模块 204 可从操作于移动装置 102 上的状态特定特征产生器 314 和 / 或装置特定特征产生器 316 获悉有待于添加到精实分类器模型或从其去除的特征。在方面中,状态特定特征产生器 314 和 / 或装置特定特征产生器 316 可被分开地实施或实施为行为分析器模块 204 的一部分。

[0132] 在方面中,状态特定特征产生器 314 可与状态监视引擎 318 通信。状态监视引擎 318 可持续地监视移动装置 102 上的配置和 / 或状态改变。这些配置和 / 或状态改变可与移动装置 102 的各种特征或组件有关。举例来说,状态监视引擎 318 可检测移动装置 102 何时连接到新的无线网络、移动装置 102 的电池电量何时下降到阈值以下(例如,低电池电量状态)、移动装置 102 何时漫游及与无线外围装置(例如,无线键盘或游戏控制器)建立 Bluetooth® 连接。在另一方面中,状态监视引擎可仅监视移动装置 102 上的显著改变 / 事件(例如,启用移动装置 102 上的“飞航模式”)。

[0133] 在检测到配置和 / 或状态改变之后,状态监视引擎 318 可通知状态特定特征产生器 314。状态特定特征产生器 314 可识别与配置和 / 或状态改变有关的一或多个特征,且可将信号发送到行为分析器模块 204 以添加这些特征或从精实分类器模型去除这些特征。举例来说,当状态监视引擎 318 通知状态特定特征产生器 314 移动装置 102 已进入“飞航模式”时(即,已关断其无线通信能力),状态特定特征产生器 314 可确定当前在精实分类器模型中不需要与移动装置的 Wi-Fi 有关的特征。

[0134] 基于从状态特定特征产生器 314 接收的反馈,行为分析器模块 204 可修改精实分类器模型以添加或去除特征,借此增强行为分析器模块 204 的检测恶意行为的总体能力且确保仅与移动装置有关的特征受监视。

[0135] 在另一方面中,装置特定特征产生器 316 可与装置特征监视引擎 320 通信,所述装置特征监视引擎 320 经配置以监视移动装置的功能性 / 能力的改变。换句话说,装置特征监视引擎 320 可检测移动装置 102 何时添加或去除特定功能,例如键盘、鼠标或另一外围装置等。

[0136] 回应于检测到新的或被去除的能力,装置特征监视引擎 320 可向装置特定特征产生器 314 警告移动装置 102 的功能性的改变。装置特定特征产生器 314 可确定与功能性改变相关联的特征且可向行为分析器单元 204 传信以添加或去除与所述改变相关联的特征。

[0137] 在另一方面中,装置特定特征产生器 314 可确定精实分类器模型中的不相关的特征,或确定从精实分类器模型遗漏且与移动装置 102 相关的特征。举例来说,行为分析器模块 204 的初始精实分类器模型可不包含与 Bluetooth® 无线电的行为有关的特征,所述行为可使移动装置易受在其 Bluetooth® 无线电上的恶意行为的攻击,这是因为 Bluetooth® 上

的活动不在精实分类器模型中且因此被忽略 / 未受监视。在此实例中,行为分析器模块 204 可在从服务器接收的大型分类器模型中探寻 Bluetooth® 特征且可将那些 Bluetooth® 特征添加到精实分类器模型,借此确保可适当监视移动装置的 Bluetooth® 无线电以发现恶意为。因此,装置特定特征产生器 314 可确定精实分类器模型中的遗漏或多余的特征且将反馈发送到行为分析器模块 204 以添加或去除那些特征。

[0138] 图 4 说明一种考虑到移动装置的装置特定及装置状态特定特征的产生精实分类器的方面方法 400。可通过移动装置中的处理核心来执行方法 400。

[0139] 在方面中,方法 400 可包含:在移动装置的处理核心中接收识别多个测试条件的完整分类器模型(例如,包含适合于转换多个决策节点(所述多个决策节点中的每一者评估所述多个测试条件中的一者)的信息的有限状态机,等);使用移动装置的装置特定信息来识别多个测试条件中的与分类移动装置的行为相关的移动装置特定测试条件;在移动装置中产生仅包含所识别的移动装置特定测试条件(例如,仅包含评估与移动装置的当前操作状态或配置相关的移动装置特征的决策节点)的精实分类器模型;以及在移动装置中使用所产生的精实分类器模型来分类移动装置的行为。

[0140] 返回到图 4,在框 402 中,处理核心可接收包含或识别大量特征和 / 或与所述特征相关联的多个测试条件的完整分类器模型。在方面中,完整分类器模型可包含多个加速确定树或树桩,所述多个加速确定树或树桩适合于供移动装置用于将行为分类为良性型或恶意型,例如,通过将行为向量值作为输入而应用到加速决策树桩 / 树以测试与移动装置的特征有关的条件等。

[0141] 将行为向量值应用到大量树桩 / 树以测试大型分类器模型中的多个特征可使移动装置 102 承受沉重负担。举例来说,这些操作可占用处理器及存储器功能,以致于对移动装置的其它进程的执行造成危害。这些操作还可耗尽移动装置 102 的电池电力。为了帮助减少对移动装置 102 的性能的这些不利影响,移动装置 102 可实施联合特征选择及剪除算法以从大型分类器模型产生精实分类器模型。

[0142] 在框 404 中,在处理核心中操作的行为分析器模块 204 可从大型分类器模型选择有待于监视及评估以便分类有关的移动装置行为的特征。各种准则可用以从大型分类器模型选择特征及加速决策树桩。举例来说,联合特征选择及剪除算法的规则可指定选择被认为对移动装置 102 的恰当操作至关重要的特征(如处理器、存储器及通信特征)。在以从最重要或最常用移动装置特征到最不重要或最不常用移动装置特征的方式对大型分类器模型排序时,所述规则还可指定可为适当的最初数目个特征(例如,最初 50、100、200、1,000 等)。

[0143] 在框 406 中,在处理核心中操作的行为分析器模块 204 可从所选特征产生精实分类器模型以测试移动装置 102 的至少一个特征的行为。在方面中,行为分析器模块 204 可扫描被包含于大型分类器模型中的加速决策树桩列表且将测试所选特征中的至少一者或由所选特征中的至少一者回答的每一加速决策树桩并入到精实分类器模型中。因此,在方面中,精实分类器模型可包含所选特征与和那些所选特征相关联的加速决策树桩两者。

[0144] 在框 408 中,在处理核心中操作的行为分析器模块 204 可基于装置特定特征 / 功能性和 / 或装置状态特定特征来修改精实分类器模型。由于网络服务器 116 使用来自各种类型的移动装置的信息来建立大型分类器模型,所以精实分类器模型(其是从大型分类器

模型导出)可包含与移动装置无关的众多特征(即,与其它类型的移动装置有关的特征)或可不包含一些极端重要的特征(即,在大型分类器模型中未被选择的特征)。由于不相关特征的存在或重要特征的缺乏,所以精实分类器模型可在前一种情况下浪费资源(例如,电池电力、CPU 循环等)来监视不相关特征,或在后一种情况下由于不监视关键性特征而提供无效的安全性。因此,移动装置的总体安全性及性能可受益于修改精实分类器模型以更密切地反映移动装置的特征及与移动装置的当前状态有关的特征。下文参看图 5 到 8 来进一步描述修改精实分类器模型的进程。

[0145] 在方面中,在处理核心中操作的行为分析器模块 204 可在无需联系网络服务器 116 的情况下通过并有由移动装置 102 所识别的未选特征且从所接收的大型分类器模型并入有有关的加速决策树桩来修改精实分类器模型以反映移动装置 102 的特定特征及状态的改变。还可通过基于装置特定及装置状态特定信息而从精实分类器模型去除不必要的特征及加速决策树桩来修改精实分类器模型。排除对联系网络服务器 116 以重新训练由移动装置的改变产生的信息的需求可节约移动装置的电力、处理及通信资源。去除不必要的特征及加速决策树桩还可通过避免处理过多或不相关信息来节约电力及处理资源。

[0146] 在框 410 中,在处理核心中操作的行为观察器 202 可监视/观察由精实分类器模型指示的移动装置特征的行为。行为观察器 202 可记录与特征有关的数据,如上文参看图 2 所描述。

[0147] 在框 412 中,行为分析器模块 204 可产生被包含于精实分类器模型中的移动装置特征的行为的行为向量。在方面中,所述行为向量可利用从行为观察器 202 接收的观察以产生行为向量,如上文参看图 2 所描述。

[0148] 在框 414 中,在处理核心中操作的分类器 208 和/或行为分析器模块 204 可将所产生的行为向量应用到加速决策树桩。在方面中,分类器 208 和/或行为分析器模块 204 可将表示特定特征的行为向量中的值应用到测试那个特定特征的一或多个加速决策树桩。将行为向量值应用到加速决策树桩的结果是例如“是”或“否”等二进制结果,其中每一结果被指派有指示特征的行为是良性型或恶意型的信赖度因素的加权机率。举例来说,行为分类器 208 可通过将移动装置 102 的行为向量值(例如,表示在最近十分钟中所发送的 SMS 消息的数目的值)用于短信服务(SMS)来测试移动装置 102 上的 SMS 特征以解析与所述 SMS 特征有关的加速决策树桩。与所述 SMS 特征相关联的加速决策树桩可包含对以下各者的测试:“在最近十分钟中是否发送 150 个或 150 个以下的 SMS 消息”、“在最近十分钟中是否发送 100 个或 100 个以下的 SMS 消息”、“在最近十分钟中是否发送 50 个或 50 个以下的 SMS 消息”等。加速决策树桩测试的每一解析可产生移动装置 102 的 SMS 特征的行为为恶意型或良性型的某种加权机率,且行为分类器 208 可将加权机率相组合以确定移动装置 102 的当前配置是恶意型还是良性型及那个结论的某种信赖度(例如,当前配置是良性型且具有 35%信赖度)。

[0149] 在确定框 416 中,分类器模块 208 和/或行为分析器模块 204 可基于将所产生的行为向量应用到精实分类器模型中的加速决策树桩的结果来确定移动装置是否正经历恶意行为。

[0150] 当分类器模块 208 确定移动装置正经历恶意行为时(即,确定框 416 =“是”),致动器 210 可在框 418 中终止恶意行为。为了终止恶意行为,致动器可限制对具有违法行为

的有关特征的存取,或识别造成所述行为的组件且隔离或删除所述组件。当分类器 208 确定移动装置未正经历恶意行为时(即,确定框 416 =“否”),因为行为观察器 202 可通过在框 410 中监视/观察由精实分类器模型所指示的移动装置特征的行为而继续,所以所述进程可在循环中继续。

[0151] 一般来说,移动装置共享多种常用组件/特征;但是,对于某些组件/特征来说,在移动装置之间存在广泛差异。制造商可在其产品范围的高端或接近高端的移动装置中提供如近场通信的特征。所开发的供政府或商业使用的特制装置可包含例如安全通信或生物测定用户识别能力等特征。这些特征可以是通常未被包含于其它移动装置中的装置特定特征。

[0152] 类似地,外围装置及软件可将移动装置的特征扩充超出其原始特征集合。举例来说,具Bluetooth®功能的耳机或键盘、经由音频插孔所连接的磁条读取器、所连接的医学装置(例如,起搏器)或HDMI连接的外部显示器(例如,电视、监视器或投影仪)是现在常用的外围装置,以上各者在被连接时扩充移动装置的特征集合。所有这些特征可为十分依赖且特定针对特定移动装置(在所述特定移动装置中实施、包含、监视和/或评估所述特征)的装置特定特征。

[0153] 图5说明一种修改分类器模型以包含移动装置(在所述移动装置中使用所述模型)的装置特定特征的方面方法500。可在移动装置102的处理核心中执行方法500。

[0154] 在框502中,在处理核心中操作的装置特征监视引擎320可辨识与移动装置的功能性有关的特征。在初始化了移动装置或恶意行为监视应用程序时和/或在初始化了特征时,就可辨识所述特征。举例来说,装置特征监视引擎320可在启动移动装置时进行确定以识别移动装置的功能性/能力,例如Bluetooth®、一或多个WAN无线电、输入/输出装置(例如,相机、扬声器、鼠标、键盘等)等。在另一实例中,装置特征监视引擎320可辨识与和移动装置通信或受移动装置控制的例如远程处理装置等外围装置有关的其它功能性/能力。

[0155] 在确定框504中,在处理核心中操作的装置特定特征产生器316可确定已辨识特征是否被包含于选自大型分类器模型以供包含于精实分类器模型中的特征当中。在方面中,装置特定特征产生器316可从装置特征监视引擎320接收关于当前存在于移动装置上的功能性/能力的通知。举例来说,装置特定特征产生器316可辨识出移动装置包含Bluetooth®无线电且可向装置特定特征产生器316警告此能力。作为响应,装置特定特征产生器316可确定与Bluetooth®无线电有关的特征是否被或应被包含于精实分类器模型中。

[0156] 当装置特定特征产生器316确定已辨识特征为被包含于精实分类器模型中的特征中的一者时(即,确定框504 =“是”),处理核心可确定将不做出精实分类器模型的改变且在处理核心中操作的行为观察器模块202可继续在框410中通过收集关于由精实分类器模型指示的特征的信息来监视/观察移动装置的行为。换句话说,装置特定特征产生器316可确定不需要另外的动作,这是因为精实分类器模型业已包含所辨识特征。

[0157] 当装置特定特征产生器316确定所辨识特征非为被包含于精实分类器模型中的特征中的一者时(即,确定框 =“否”),在框506中,行为分析器模块204可将由装置特定特征产生器316所识别的特征连同来自大型分类器模型的有关的对应加速决策树桩一起添加到精实分类器模型。在方面中,行为分析器模块204可添加所辨识特征以便确保精实

分类器模型充分表示移动装置的能力及功能性（即，以确保移动装置的装置特定特征 / 功能性受到充分监视 / 保护）。

[0158] 行为观察器 202 可接着继续在框 410 中监视 / 观察由经更新的精实分类器模型指示的移动装置特征的行为。

[0159] 将特征添加到精实分类器可帮助使精实分类器不会落后于移动装置的配置及操作状态改变。如上文所提到，具有最新的精实分类器可改善行为分析器模块 204 监视移动装置 102 上的恶意行为的能力，这是因为可监视一组较完整的作用中特征。在方面中，一些特征（当在作用中时）对监视来说变得日益重要，这是因为所述特征可提供对敏感信息（诸如，金融信息）的存取。举例来说，近场通信与电子商务密切相关。此特征常常能存取信用卡信息及例如 Google Wallet 及 PayPal 帐户信息等电子商务帐户信息。因此，添加具有对敏感信息的存取权的作用中特征对于保护此信息免遭恶意行为侵害来说可为重要的。

[0160] 图 6 说明一种可实施于移动装置上的用于通过去除移动装置的装置特定特征来修改精实分类器模型的方面方法 600。当移动装置 102 的特征发生改变时（例如，从移动装置去除外围装置），所述特征可不再被包含于移动装置 102 上但可仍寻址于精实分类器模型中。这样会将不必要的复杂性添加到行为向量的处理，这是因为移动装置现可包含对于监视移动装置的行为来说无用或与监视移动装置的行为不相关（因为不存在的特征不可能为恶意的）的信息。一个残留特征可能对移动装置 102 的资源及能力不具有太多影响。但是，随时间的过去，所去除的特征的数目可增加且引起行为监视进程的明显劣化。因此，当特征不再与移动装置的当前配置或操作状态相关时，从精实分类器模型去除所述特征及相对应的加速决策树桩可为有益的。

[0161] 在框 602 中，装置特征监视引擎 320 可辨识与移动装置 102 的功能性有关的特征列表。所述列表可含有与移动装置的功能性有关的例如其近场通信能力、外围装置、WAN 无线电等每一特征。

[0162] 在确定框 604 中，装置特定特征产生器 316 可确定被包含于精实分类器模型中的与装置特定能力有关的特征是否被包含于与移动装置的功能性有关的特征列表中。换句话说，特定特征产生器 316 可确定精实分类器模型中的任何特征（例如，Bluetooth®、近场通信或其它装置特定功能）是否因为那些特征或有关功能性并不存在于移动装置上而过剩。当装置特定特征产生器 316 确定精实分类器模型中的所有特征是在列表上时（即，确定框 604 = “是”），可不做出精实分类器模型的改变且行为观察器 202 可继续在框 410 中监视 / 观察由精实分类器模型指示的移动装置特征的行为。

[0163] 当装置特定特征产生器 316 确定在精实分类器模型中的与移动装置能力 / 功能性有关的一或多个特征不在移动装置能力 / 功能性的列表上时（即，确定框 604 = “否”），行为分析器模块 204 可在框 606 中从精实分类器模型去除不相关或过剩的特征及相对应的加速决策树桩。举例来说，当 Bluetooth® 无线电在移动装置上被去启动时，行为分析器模块 204 可从精实分类器模型去除与 Bluetooth® 无线电有关的特征。行为观察器 202 可接着继续在框 410 中使用经更新的精实分类器模型来监视 / 观察移动装置特征的行为。

[0164] 图 7 说明一种可实施于移动装置上的用于修改精实分类器模型以考虑到移动装置的装置特定特征的改变的方面方法 700。可在移动装置的处理核心中执行方法 700。在移动装置 102 的特征为静态的方面中，使处理核心（例如，在整个移动装置 102 首次被通电

时)检查移动装置 102 的特征一次可能已足够。在特征可被间歇地改变的其它方面中,检查移动装置 102 的特征可发生于(例如)当移动装置 102 执行更新程序或用于监视移动装置 102 的行为的软件被初始化时。但是,在移动装置 102 的特征为动态(即,其中可在移动装置 102 的正常操作期间添加及去除功能性和/或特征)的方面中,识别所述改变且在发生所述改变时使精实分类器模型适应所述特征可为有利的。连接及断开连接外围装置(类似于先前所提到的外围装置)可引发装置功能性和/或特征的这些改变。

[0165] 在确定框 702 中,在移动装置的处理核心中操作的装置特征监视引擎 320 可监视移动装置以确定是否存在或是否已存在移动装置的状态、配置、能力或功能性的任何改变。在方面中,特征监视引擎 320 可经配置以不断地监视移动装置 102,从而确定何时已添加或去除与移动装置的装置特定特征有关的功能性。在另一方面中,装置特征监视引擎 320 可经配置以接收在添加或去除功能性和/或特征时通知装置特定特征产生器 320 的提示。举例来说,在内核空间中接收到中断以从移动装置 102 连接或断开连接外围装置时,可通知装置特定特征产生器 320。

[0166] 当装置特征监视引擎 320 确定已不存在移动装置 102 的功能性改变时(即,确定框 702 = “否”),那么可不做出精实分类器模型的改变且行为观察器 202 可继续在框 410 中监视/观察由精实分类器模型指示的移动装置特征的行为。当装置特征监视引擎 320 确定存在或已存在移动装置 102 的功能性改变时(即,确定框 702 = “是”),在框 704 中,装置特定特征产生器 316 可辨识或识别与所检测到的功能性改变相关联的移动装置特征。多个特征可共享给定功能性或与给定功能性有关。在方面中,装置特定特征产生器 316 可从装置特征监视引擎 320 接收已改变的功能性的指示。装置特定特征产生器 316 可使所述功能性与一或多个特征相关且识别所述特征中的哪一者受所述功能性改变影响。举例来说,连接至移动装置 102 的不同外围装置可经由无线连接(如 Bluetooth®)从移动装置 102 串流传输媒体。一个此外围装置可为一组无线扬声器,而另一外围装置可为无线连接的电视。两个外围装置都可在功能上允许串流传输媒体;但是,装置特定特征产生器 316 可区分出扬声器可提供用以串流传输音频媒体的特征且电视可提供用以串流传输音频媒体、视频媒体及音频/视频多媒体的特征。因此,仅在串流传输音频的功能性方面的改变可导致装置特定特征产生器 316 做出以下结论:受所述改变影响的特征是到无线扬声器而非到无线电视的音频串流。

[0167] 在确定框 706 中,装置特定特征产生器 316 可确定移动装置的功能性改变是功能性的添加还是功能性的去除。也就是说,在确定框 706 中,处理核心可确定所检测到的功能性改变是表示被添加的功能性还是被去除的功能性。此确定可帮助维持最新的精实分类器模型。如先前所论述,维持精实分类器模型可改善监视恶意行为的性能且减小监视对移动装置 102 的性能的影响。

[0168] 当装置特定特征产生器 316 确定改变是功能性的添加时(即,确定框 706 = “添加(Addition)”),在确定框 708 中,装置特定特征产生器 316 可确定与所改变的功能性相关联的已辨识特征是否被包含于精实分类器模型中。举例来说,处理核心可在确定框 708 中响应于确定所检测到的功能性改变表示被添加的功能性而确定精实分类器模型是否包含评估受所述所检测到的功能性改变影响的移动装置特征的任何测试条件。当装置特定特征产生器 316 确定已辨识特征被包含于精实分类器模型的特征中时(即,确定框 708 = “是”),

处理核心可确定将不对精实分类器模型做出改变,且行为观察器 202 可继续在框 410 中监视 / 观察由精实分类器模型指示的移动装置特征的行为。

[0169] 当装置特定特征产生器 316 确定移动装置的已辨识特征未被包含于精实分类器模型中时 (即,确定框 708 = “否”),在框 710 中,行为分析器模块 204 可将由装置特定特征产生器 316 识别的特征及其有关加速决策树桩从大型分类器模型添加到精实分类器模型。也就是说,在框 710 中,处理核心可响应于确定精实分类器模型不包含评估移动装置特征的任何测试条件而确定完整分类器模型是否包含评估移动装置特征的任何测试条件,且响应于确定完整分类器模型包含评估移动装置特征的测试条件而将评估受所检测到的改变影响的移动装置特征的测试条件添加到精实分类器模型。当新功能性被添加到移动装置时将新特征添加到精实分类器使得能够在移动装置 102 的配置改变时对移动装置 102 的所有特征及功能性进行有效的恶意行为监视。行为观察器 202 可继续在框 410 中监视 / 观察由经更新的精实分类器模型指示的移动装置特征的行为。

[0170] 当装置特定特征产生器 316 确定改变是涉及功能性和 / 或特征的去除时 (即,确定框 708 = “去除”),在确定框 712 中,装置特定特征产生器 316 可确定已辨识特征是否被包含于精实分类器模型中。当装置特定特征产生器 316 确定所述特征是在精实分类器模型中时 (即,确定框 712 = “是”),在框 714 中,行为分析器模块 204 可从精实分类器模型去除那个 (那些) 特征及有关加速决策树桩。去除不再与移动装置 102 相关的特征及加速决策树桩可减少用以监视恶意行为所需的资源,因此减小对移动装置 102 的性能的影响。行为观察器 202 可继续在框 410 中监视 / 观察由精实分类器模型指示的移动装置特征的行为。当装置特定特征产生器 316 确定所述已辨识特征不在精实分类器模型中时 (即,确定框 714 = “否”),可不做出精实分类器模型的改变且行为观察器 202 可继续在框 410 中监视 / 观察由精实分类器模型指示的移动装置特征的行为。

[0171] 图 8 说明一种用于通过添加与移动装置的状态有关的移动装置特征来修改精实分类器模型的方面方法 800。移动装置的状态可正不断地改变;且发生于移动装置 102 上的每一事件可改变与特征有关的状态。举例来说,当移动装置 102 变为在作用中或闲置、产生通信连接或结束连接,及被塞到充电器中或被拔去插塞使得其由电池供电时,状态可发生改变。状态可如此频繁地改变以致于在每一状态改变时识别特征可为繁重的,这是因为将不得不从网络服务器 116 获得特征信息或甚至获得所接收的大型分类器模型。状态还可非常快速地改变,且如果针对每一状态改变来更新特征,那么到发生更新的时候所述更新可能已过时,这是因为有关状态再次改变。因此,移动装置 102 可要求:在识别有待于添加到精实分类器模型或从精实分类器模型去除的功能之前,状态改变应为实质的。实质状态改变可包含断开连接所有无线连接 (如当启动“飞航模式”时)、在连接到安全网络接入点时减小安全协议级别,或进入及退出蜂窝式通信的漫游模式。

[0172] 在确定框 802 中,状态监视引擎 318 可确定在移动装置上是否已存在状态改变。状态监视引擎 318 可监视移动装置的所有状态或状态的子集。在方面中,可不将移动装置的一些状态视为指示可促成或涉及恶意行为的特征,且因此无需监视所述状态。在另外的方面中,可不断地监视受状态监视引擎 318 监视的状态以发现状态改变。当状态监视引擎 318 确定已不存在状态改变时 (即,确定框 802 = “否”),那么可不做出精实分类器模型的改变,且行为观察器 202 可继续在框 410 中监视 / 观察由精实分类器模型指示的移动装置

特征的行为。

[0173] 如上文所论述,可不将所有状态改变视为重要的,且许多状态改变发生得如此快速和 / 或频繁以致于基于状态改变来监视 (或停止监视) 有关特征可并非有效的。当状态监视引擎 318 确定存在状态改变时 (即,确定框 802 = “是”),在确定框 806 中,状态监视引擎 318 可确定移动装置的一或多个状态改变是否为实质的。当状态监视引擎 318 确定移动装置的所述 / 所述状态改变并非实质时 (即,确定框 806 = “否”),行为观察器 202 可继续在框 410 中监视 / 观察由精实分类器模型指示的移动装置特征的行为。当状态监视引擎 318 确定移动装置的所述 / 所述状态改变为实质时 (即,确定框 806 = “是”),在框 808 中,状态监视引擎 318 可辨识移动装置的当前状态及先前状态。在方面中,可预先确定是什么使状态改变为实质的,且可通过由状态监视引擎 318 存取的规则来识别实质状态改变。

[0174] 在框 810 中,状态特定特征产生器 314 可辨识与当前状态及先前状态有关的特征。在方面中,状态特定特征产生器 314 可从状态监视引擎 318 接收实质状态改变的通知,这可触发状态特定特征产生器 314 以使特征与所述实质状态改变相关或辨识具有所述实质状态改变的特征。在方面中,特征与实质状态改变之间的相关可为直接相关。举例来说,正经由 WiFi 建立的无线连接的状态可与移动装置 102 的 WiFi 特征直接有关。在另一方面中,特征与实质状态改变之间的相关可为切向相关。举例来说,指示快速网络连接的状态可指示与云服务器的较好互动,这可涉及移动装置 102 上的例如将信息卸除到云服务器等恶意行为。在另一方面中,所述相关可为间接相关。举例来说,可使移动装置 102 的电池状态与各组特征相关。在高电池电量状态期间,当移动装置 102 具有用以处置对范围广的一组特征 (包含高及低优先级特征) 的监视的足够电力资源时,可监视范围广的所述组特征以发现恶意行为。类似地,在低电池电量状态期间,当移动装置 102 不具有用以处置对范围广的所述组特征的监视的足够电力资源时,可监视范围窄的一组特征 (包含高优先级特征) 以发现恶意行为。

[0175] 在框 812 中,行为分析器模块 204 可将由状态特定特征产生器 314 所识别的与当前状态有关但与先前状态无关的任何特征 (即,新近相关特征) 连同添加到精实分类器模型。可从大型分类器模型获得被添加到精实分类器模型的所述特征及所述相关联的加速决策树桩。在框 814 中,行为分析器模块 204 可从精实分类器模型去除经辨识为与先前状态有关但与当前状态无关 (即,不再相关) 的任何特征及相关联的加速决策树桩。行为观察器 202 可继续在框 410 中监视 / 观察由精实分类器模型指示的移动装置特征的行为。以此方式添加及去除与实质状态改变有关的特征及加速决策树桩可使精实分类器保持不落伍,如上文所论述。

[0176] 图 9 说明一种产生精实或集中的分类器 / 行为模型的方面方法 900,所述精实或集中的分类器 / 行为模型考虑到移动装置的装置特定及装置状态特定特征。可由移动装置中的处理核心来执行方法 900。

[0177] 在方法 900 的框 902 中,处理核心可接收完整分类器模型,所述完整分类器模型是以下各者或包含以下各者:有限状态机、加速确定树的列表、加速决策树桩的列表或识别多个测试条件的其它类似信息结构。在方面中,完整分类器模型包含有限状态机,所述有限状态机包含适合于表现多个加速决策树桩的信息和 / 或包含适合于由移动装置转换为多个加速决策树桩的信息。在方面中,有限状态机可以是 (或可包含) 加速决策树桩的有序或

经优先级排序的列表。所述加速决策树桩中的每一者可包含测试条件及权值。

[0178] 如上文所论述,加速决策树桩是具有正好一个节点(及因此一个测试问题或测试条件)及权值的一级确定树,且因此非常适合于用于数据/行为的二进制分类中。此意谓将特征向量或行为向量应用到加速决策树桩会产生二进制回答(例如,是或否)。举例来说,如果由加速决策树桩测试的问题/条件为“SMS 传输的频率小于每分钟 x 次?”,那么将值“3”应用到加速决策树桩将产生“是”回答(对于“小于 3 次”SMS 传输来说)或“否”回答(对于“3 或大于 3 次”SMS 传输来说)。

[0179] 返回到图 9,在方法 900 的框 904 中,处理核心可确定在不消耗移动装置的过多量的处理、存储器或能量资源的情况下应加以评估以将移动装置行为准确地分类为恶意型或良性型的独特测试条件的数目。此可包含确定在移动装置中可用的处理、存储器和/或能量资源的量、移动装置的测试条件所需的处理、存储器或能量资源的量;确定(由于测试条件)与有待于在移动装置中加以分析或评估的行为或条件相关联的优先级和/或复杂性;以及选择/确定独特测试条件的数目以便在移动装置的可用处理、存储器或能量资源的消耗、待自测试条件达成的行为分类的准确度以及由所述条件测试的行为的重要性或优先级之间达到平衡或折中。

[0180] 在框 906 中,处理核心可使用装置特定或装置状态特定信息来快速地识别应被包含或从精实分类器模型排除的特征和/或测试条件。举例来说,处理核心可识别归因于移动装置的当前硬件或软件配置、操作状态等而不可能存在于移动装置中的测试条件、特征或因素。作为另一实例,处理核心可识别及从精实分类器模型排除被包含于完整模型中的特征/节点/树桩及不可能存在于移动装置中和/或与移动装置不相关的测试条件。

[0181] 在方面中,在框 908 中,处理核心可自开始遍历加速决策树桩的列表以用已确定数目的独特测试条件来填入所选测试条件的列表,及排除框 906 中所识别的测试条件。举例来说,处理核心可跳过、忽略或删除其测试条件归因于移动装置的当前硬件或软件配置而不可能存在于移动装置中的被包含于完整分类器模型中的特征。在方面中,处理核心还可确定所选测试条件中的每一者的绝对或相对优先级值,且将所述绝对或相对优先级值存储成与在所选测试条件的列表中的其对应测试条件相关联。

[0182] 在方面中,在框 908 中,处理核心可通过顺序地遍历完整分类器模型中的多个测试条件且将与分类移动装置的行为相关的那些测试条件插入到测试条件列表中直至所述测试条件列表包含已确定的数目的独特测试条件来产生所述测试条件列表。在另外的方面中,产生测试条件列表可包含:顺序地遍历完整分类器模型的决策节点;忽略与和分类移动装置的行为不相关的测试条件相关联的决策节点;以及将与未被忽略的每一顺序地遍历的决策节点相关联的测试条件插入到测试条件列表中直至所述测试条件列表包含已确定的数目的独特测试条件。

[0183] 在框 910 中,处理核心可产生精实分类器模型,所述精实分类器模型包含被包含于完整分类器模型中的测试在所产生的测试条件列表中所识别的所选测试条件中的一者(及因此排除在框 906 中所识别的测试条件)的所有加速决策树桩。在方面中,处理核心可产生精实分类器模型以按加速决策树桩的重要性或优先级值的次序来包含或表现所述加速决策树桩。

[0184] 在任选框 912 中,可增加独特测试条件的数目以便通过重复以下操作来产生另一

较强健（即，较不精实）的精实分类器模型；在框 908 中针对较大数目的测试条件来遍历加速决策树桩的列表；以及在框 910 中产生另一精实分类器模型。可重复这些操作以产生精实分类器模型的系列。

[0185] 各种方面可实施于多种移动计算装置中的任一者中，所述移动计算装置的实例说明于图 10 中。移动计算装置 1000 可包含耦合到触控屏幕控制器 1004 及内部存储器 1006 的处理器 1002。所述处理器 1002 可为经指定用于一般或特定处理任务的一或多个多核心集成电路。内部存储器 1006 可为易失性或非易失性存储器，且还可为安全和 / 或加密的存储器，或不安全和 / 或未加密的存储器，或其任何组合。触控屏幕控制器 1004 及处理器 1002 还可耦合到例如电阻性感测触控屏幕、电容性感测触控屏幕、红外线感测触控屏幕等触控屏幕面板 1012。另外，移动计算装置 1000 的显示器无需具有触控屏幕能力。

[0186] 移动计算装置 1000 可具有彼此耦合和 / 或耦合到处理器 1002 的一或多个无线电信号收发器 1008（例如，Peanut、Bluetooth®、Zigbee、Wi-Fi、射频无线电）及天线 1010，以用于发送及接收通信。可将所述收发器 1008 及天线 1010 与上述电路一起使用以实施各种无线传输协议堆栈及接口。移动计算装置 1000 可包含蜂窝式网络无线调制解调器芯片 1016，所述蜂窝式网络无线调制解调器芯片 1016 允许实现经由蜂窝式网络的通信且耦合到处理器。

[0187] 移动计算装置 1000 可包含耦合到处理器 1002 的外围装置连接接口 1018。所述外围装置连接接口 1018 可被特殊地配置以接受一种类型的连接，或可经配置以接受各种类型的实体及通信连接（普通或专属）（例如，USB、FireWire、Thunderbolt 或 PCIe 等）。外围装置连接接口 1018 还可耦合到经类似地配置的外围装置端口（未图标）。

[0188] 移动计算装置 1000 还可包含用于提供音频输出的扬声器 1014。移动计算装置 1000 还可包含外壳 1020，所述外壳 1020 由塑料、金属或材料的组合建构，且用于含有本文中所论述的组件中的所有或一些组件。移动计算装置 1000 可包含耦合到处理器 1002 的例如抛弃式或可再充电型电池等电源 1022。可再充电型电池还可耦合到外围装置端口以从位于移动计算装置 1000 外部的源接收充电电流。移动计算装置 1000 还可包含用于接收用户输入的物理按钮 1024。移动计算装置 1000 还可包含用于接通及关断移动计算装置 1000 的电源按钮 1026。

[0189] 上文所描述的各种方面还可实施于例如图 11 中所说明的膝上型计算机 1100 等多种移动计算装置内。许多膝上型计算机包含触摸板型触控表面 1117，所述触摸板型触控表面 1117 充当计算机的指针装置，且因此可接收拖曳、卷动及拨动示意动作（类似于被实施于配备有触控屏幕显示器及上文所描述的移动计算装置上的那些示意动作）。膝上型计算机 1100 将通常包含耦合到易失性存储器 1112 及大容量非易失性存储器（例如，闪存的碟机 1113 等）的处理器 1111。另外，计算机 1100 可具有耦合到处理器 1111 的一或多个天线 1108 和 / 或蜂窝式电话收发器 1116，所述一或多个天线 1108 用于发送及接收可连接到无线数据链路的电磁辐射。计算机 1100 还可包含耦合到处理器 1111 的软性磁盘驱动器 1114 及紧密光盘 (CD) 机 1115。在笔记本计算机配置中，计算机外壳包含触摸板 1117、键盘 1118 及显示器 1119，以上各者都耦合到处理器 1111。计算装置的其它配置可包含如为熟知的耦合到处理器（例如，经由 USB 输入）的计算机鼠标或轨迹球，所述计算机鼠标或轨迹球亦可结合各种方面加以使用。

[0190] 可以高阶编程语言（例如，C、C++、C#、Smalltalk、Java、JavaScript、Visual Basic、结构化查询语言（例如，Transact-SQL）、Perl 等）或以各种其它编程语言来撰写供执行于可编程处理器上以用于实行各种方面的操作的计算机程序码或“程序代码”。如本申请案中所使用，存储于计算机可读存储媒体上的程序代码或程序可指机器语言码（例如，目标码等），所述机器语言码的格式可被处理器理解。

[0191] 许多移动计算装置操作系统内核被组织成用户空间（其中执行非特权程序代码）及内核空间（其中执行特权程序代码）中。此分开在 Android 及作为内核空间的部分的程序代码必须经通用公共授权（general public license, GPL）授权而执行于用户空间中的程序代码可不经 GPL 授权的其它 GPL 环境中尤为重要。应理解，除非另有明确阐述，否则此处所论述的各种软件组件 / 模块可实施于内核空间或用户空间中。

[0192] 上述方法描述及进程流程图是仅仅被提供作为说明性实例且并不意欲要求或暗示必须以所呈现的次序来执行各种方面的步骤。如由熟习此项技术者将了解，可以任何次序来执行上述方面中的步骤的次序。例如“其后”、“接着”、“接下来”等的词语并不意欲限制步骤的次序；这些词语仅用以引导读者阅读所述方法的描述。另外，对呈单数（例如，使用冠词“一”或“所述”）的技术方案组件的任何参考不应被解释为将所述组件限制到单数。

[0193] 如此申请案中所使用，术语“组件”、“模块”、“系统”、“引擎”、“产生器”、“管理器”及其类似者意欲包含计算机有关实体，例如（但不限于）经配置以执行特定操作或功能的硬件、韧体、硬件与软件的组合、软件或执行中的软件等。举例来说，组件可为（但不限于）执行于处理器上的进程、处理器、对象、可执行程序、执行线绪、程序和 / 或计算机。借助于说明，可将执行于计算装置上的应用程序与计算装置两者称作组件。一或多个组件可驻留于进程和 / 或执行线绪内，且一组件可被区域化于一个处理器或核心上和 / 或分布于两个或两个以上的处理器或核心中。另外，这些组件可从各种非暂时性计算机可读媒体来执行，所述非暂时性计算机可读媒体具有存储于其上的各种指令和 / 或数据结构。组件可借助于本地和 / 或远程进程、函式或程序调用、电子信号、数据包、存储器读取 / 写入及其它已知的与网络、计算机、处理器和 / 或进程有关的通信方法来通信。

[0194] 结合本文中所揭示的方面而描述的各种说明性逻辑块、模块、电路及算法步骤可经实施为电子硬件、计算机软件或两者的组合。为了清楚地说明硬件与软件的此可互换性，上文已大体在功能性方面描述了各种说明性组件、块、模块、电路及步骤。此功能性经实施为硬件还是软件取决于特定应用及强加于整个系统的设计约束而定。熟习此项技术者可针对每一特定应用而以变化的方式来实施所描述的功能性，但这些实施决策不应解释为导致背离本发明的范围。

[0195] 可由通用处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、现场可编程门阵列（FPGA）或其它可程序化逻辑装置、离散闸或晶体管逻辑、离散硬件组件或其经设计以执行本文中所描述的功能的任何组合来实施或执行用以实施结合本文中所揭示的方面而描述的各种说明性逻辑、逻辑块、模块及电路的硬件。通用处理器可以是多处理器；但在替代例中，处理器可以是任何常规的处理器、控制器、微控制器或状态机。还可将处理器实施为计算装置的组合，例如 DSP 与多处理器的组合、多个多处理器、结合 DSP 核心的一或多个多处理器，或任何其它此配置。替代地，可由特定针对给定功能的电路来执行一些步骤或方法。

[0196] 可将一或多个方面中所描述的功能实施于硬件、软件、固件或其任何组合中。如果实施于软件中,那么所述功能可作为一或多个指令或程序代码而存储于非暂时性计算机可读媒体或非暂时性处理器可读媒体上。本文中所揭示的方法或算法的步骤可体现于可驻留于非暂时性计算机可读或处理器可读存储媒体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媒体可为可由计算机或处理器存取的任何存储媒体。借助于实例但非限制,这些非暂时性计算机可读或处理器可读媒体可包含 RAM、ROM、EEPROM、闪存、CD-ROM 或其它光盘存储器、磁盘存储器或其它磁性存储装置或可用以以指令或数据结构的形式来存储所要程序代码且可由计算机存取的任何其它媒体。如本文中所使用,磁盘及光盘包含紧密光盘 (CD)、激光光盘、光盘、数字激光视盘 (DVD)、软性磁盘及蓝光光盘,其中磁盘通常以磁性方式再生数据,而光盘通过激光以光学方式再生数据。以上各物的组合也被包含于非暂时性计算机可读及处理器可读媒体的范围内。另外,方法或算法的操作可作为程序代码和 / 或指令中的一者或任一组合或集合而驻留于非暂时性处理器可读媒体和 / 或计算机可读媒体上,可将所述非暂时性处理器可读媒体和 / 或计算机可读媒体并入到计算机程序产品中。

[0197] 提供对所揭示方面的上述描述以使得任何熟习此项技术者能够制造或使用本发明。对这些方面的各种修改将容易为所属领域的技术人员所显而易见,且可在不背离本发明的精神或范围的情况下将本文中所定义的一般原理应用到其它方面。因此,本发明并不意欲受限于本文中所展示的方面,而是应符合与所附权利要求书及本文中所揭示的原理及新颖特征一致的最广范围。

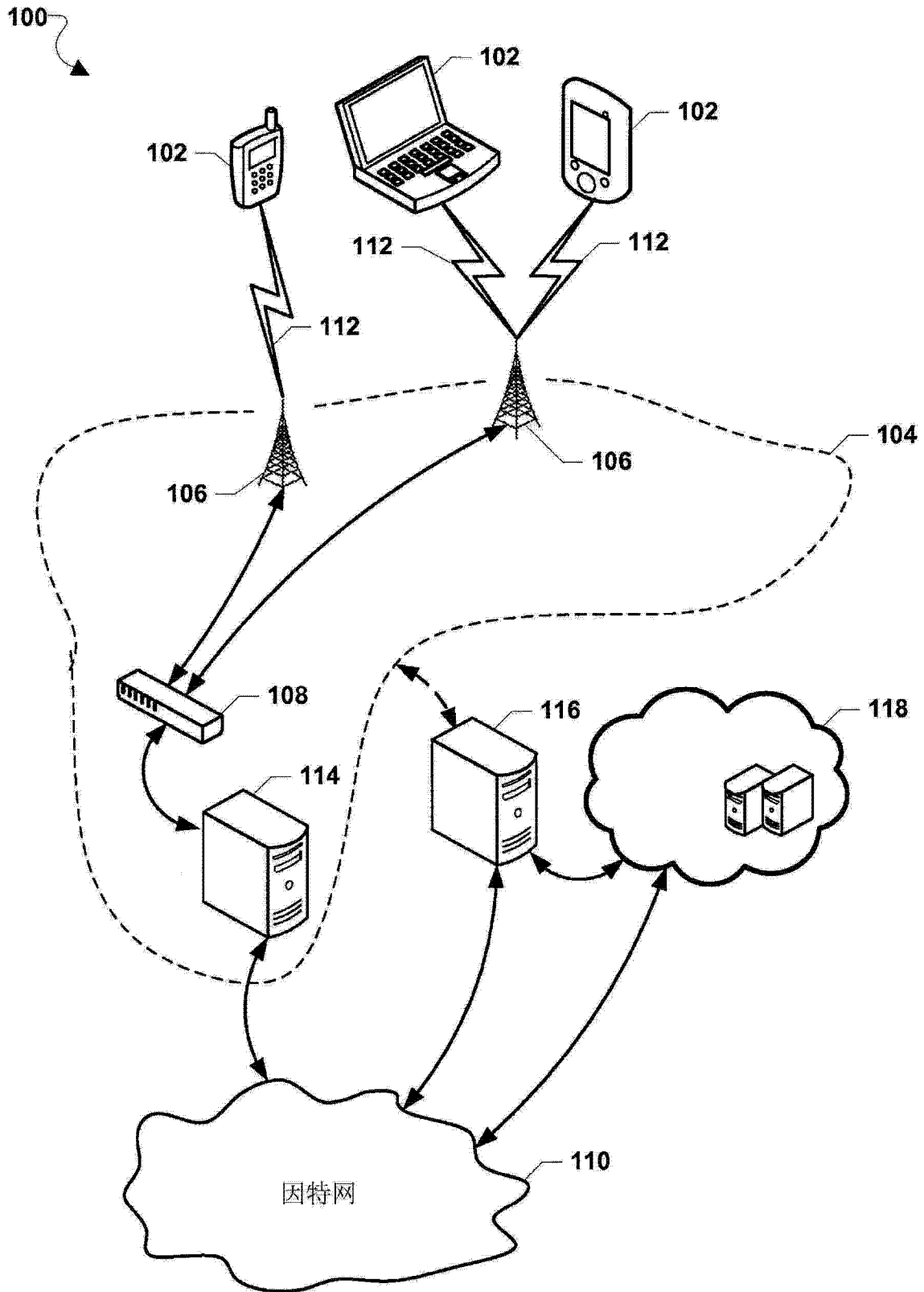


图 1

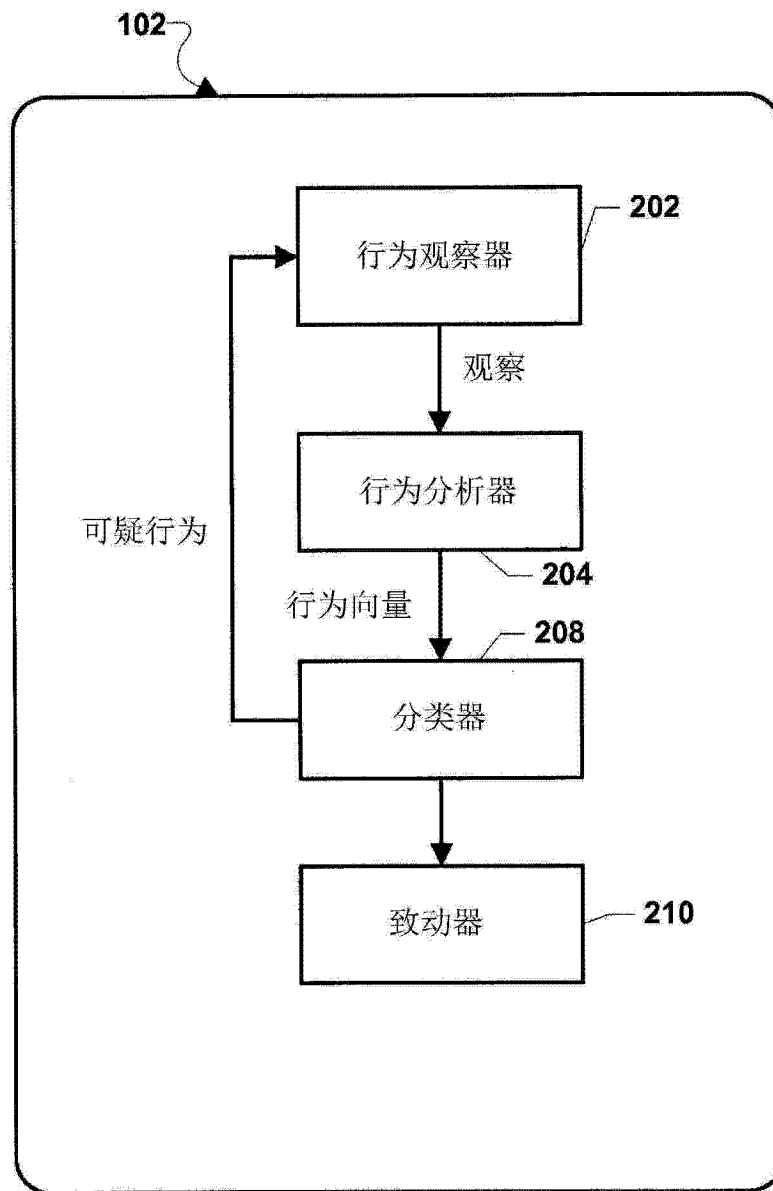


图 2

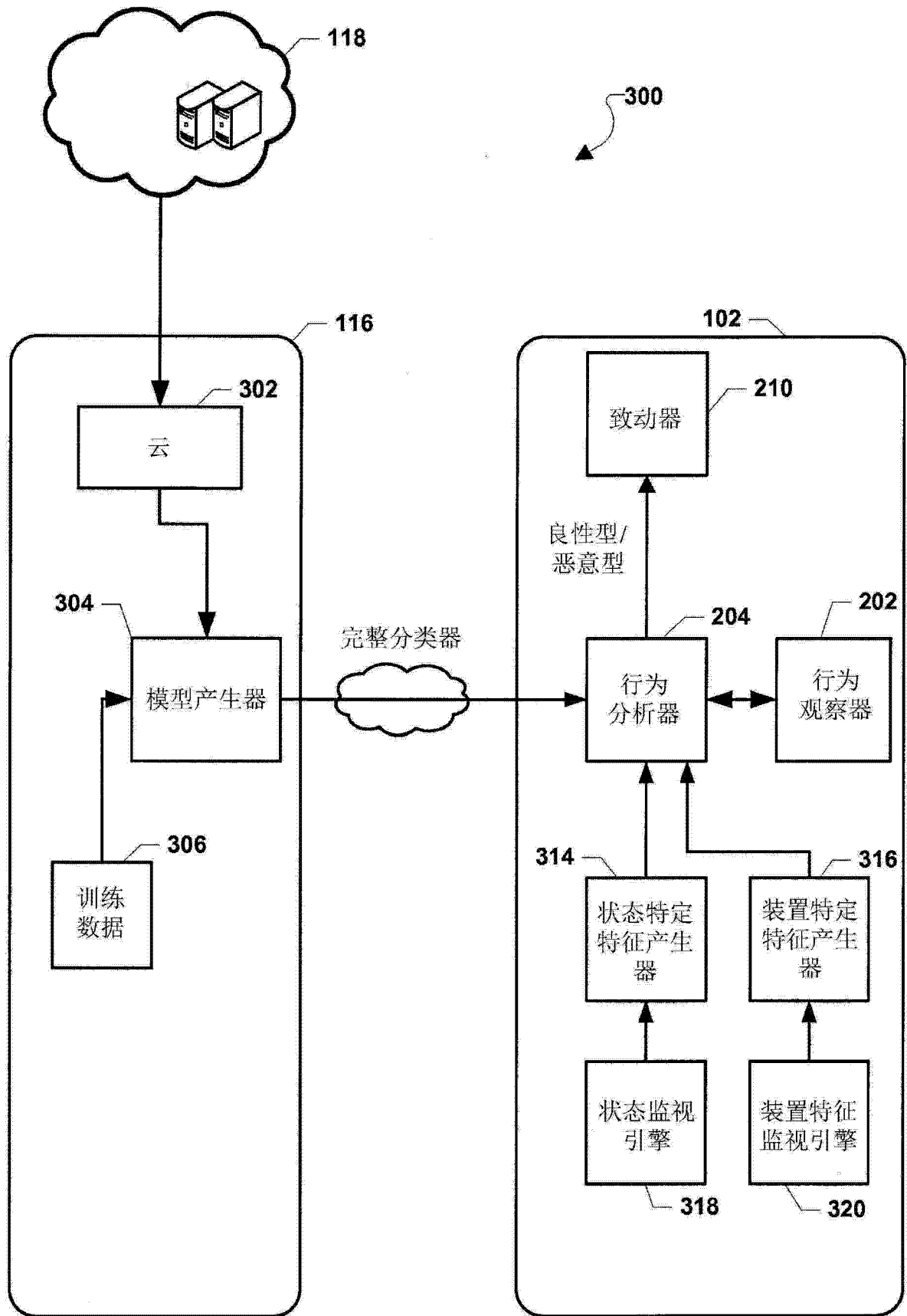


图 3

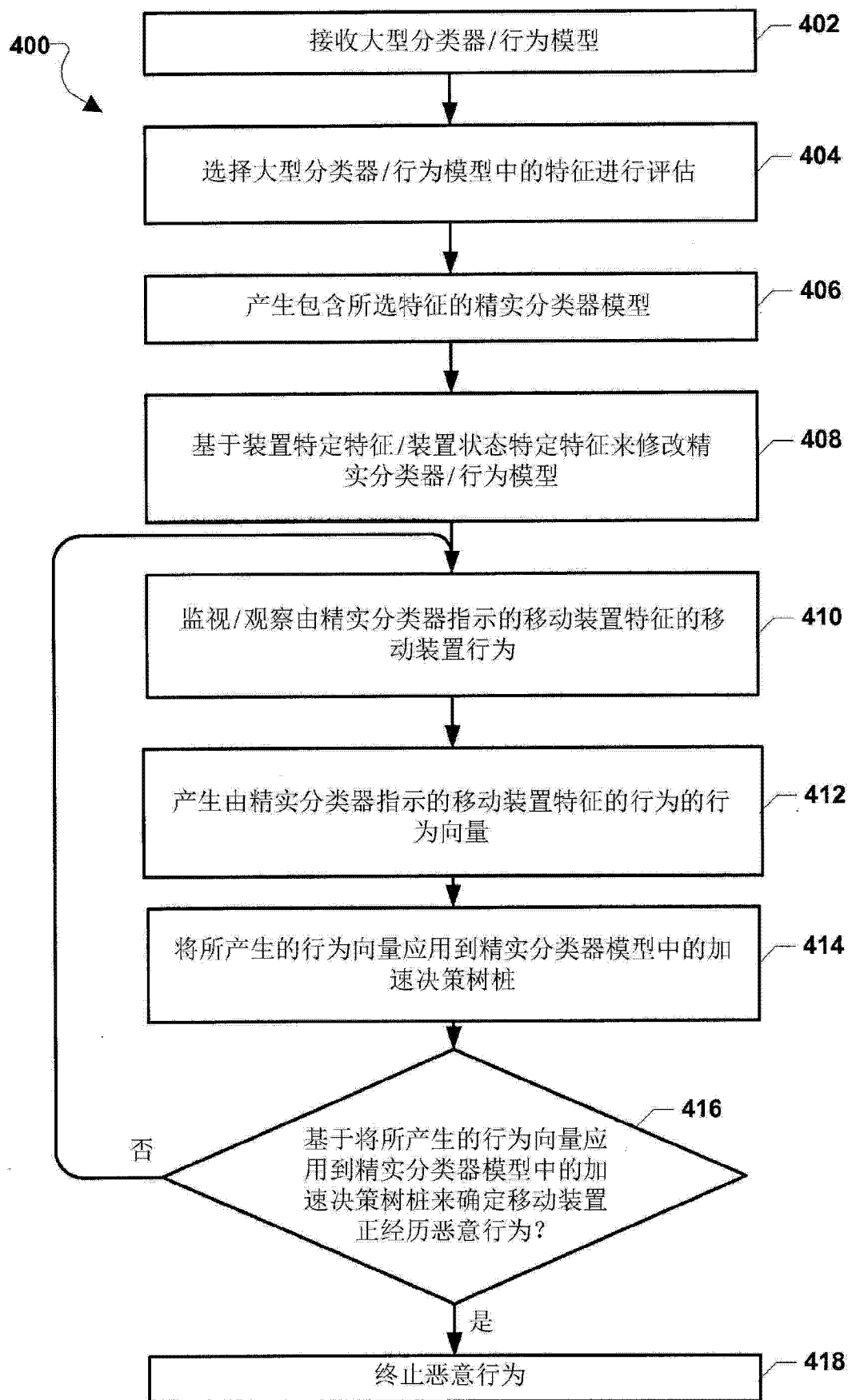


图 4

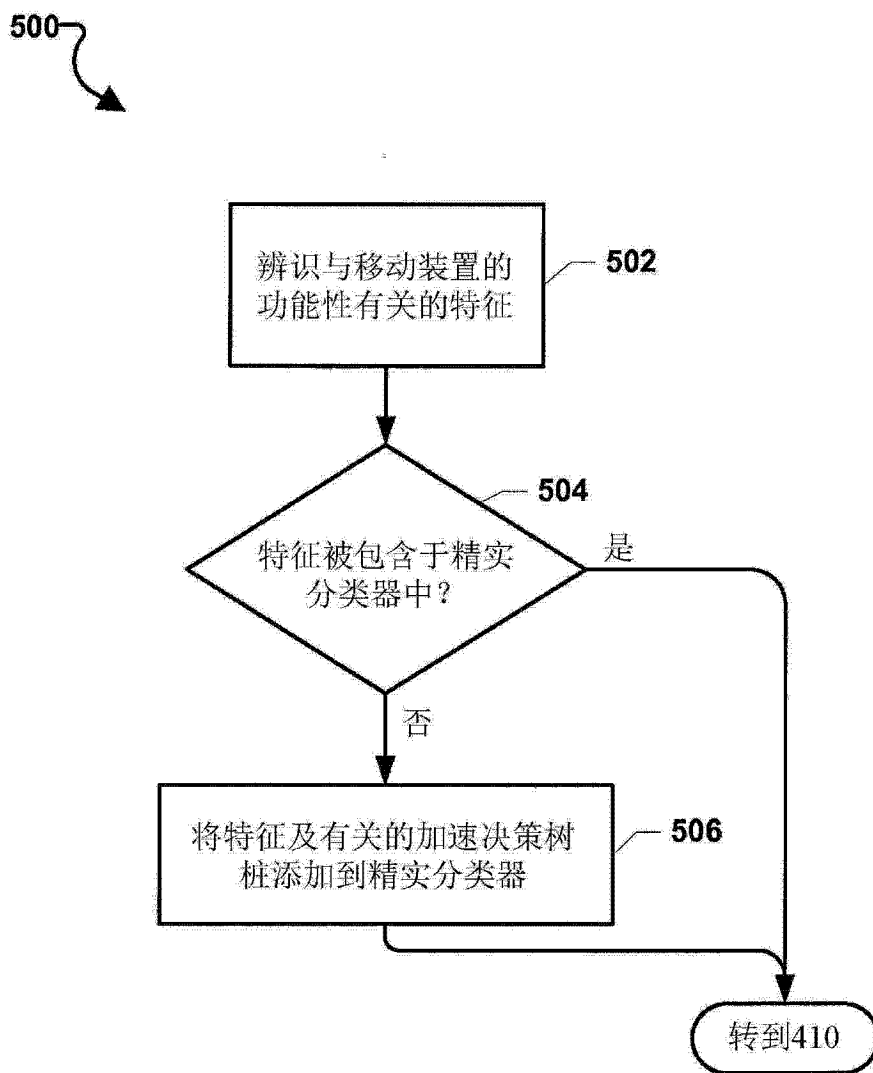


图 5

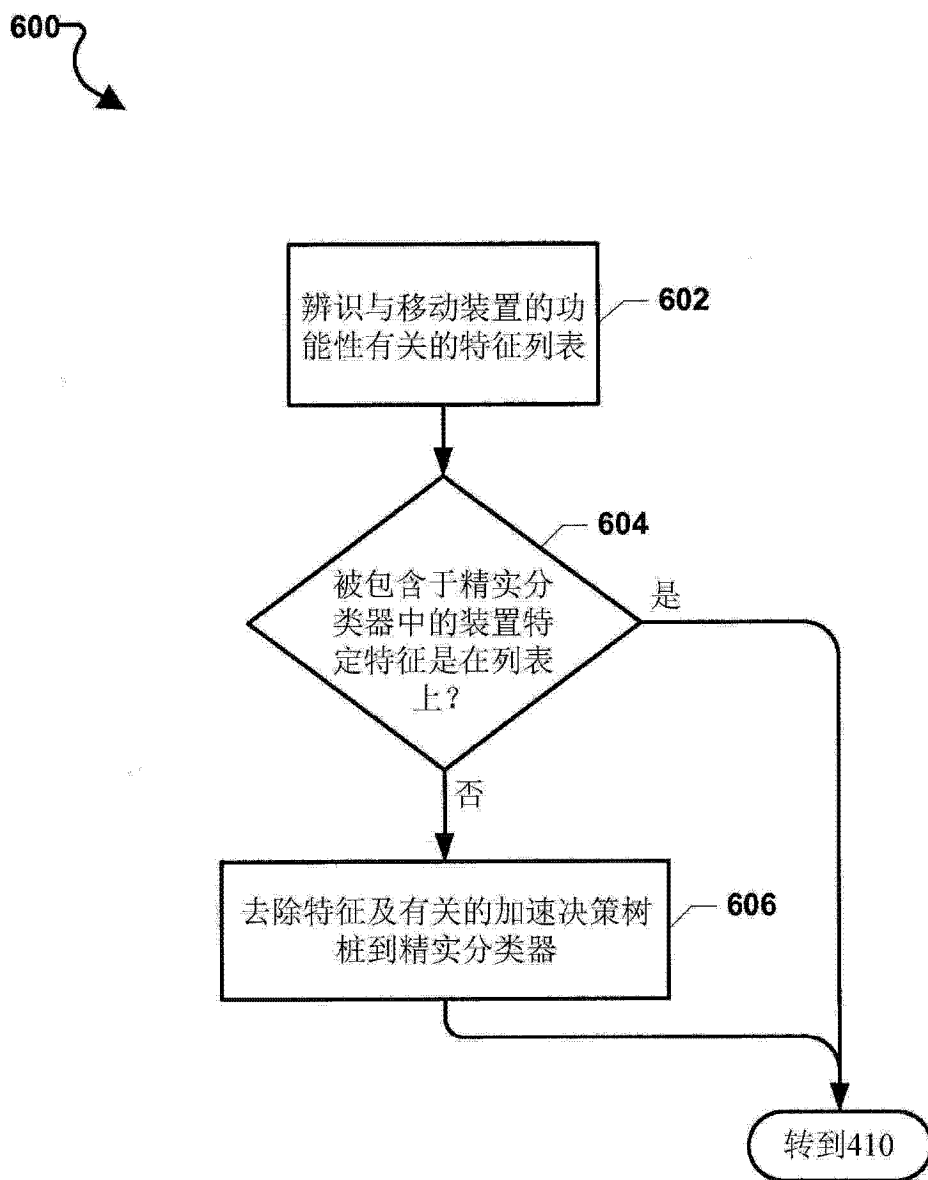


图 6

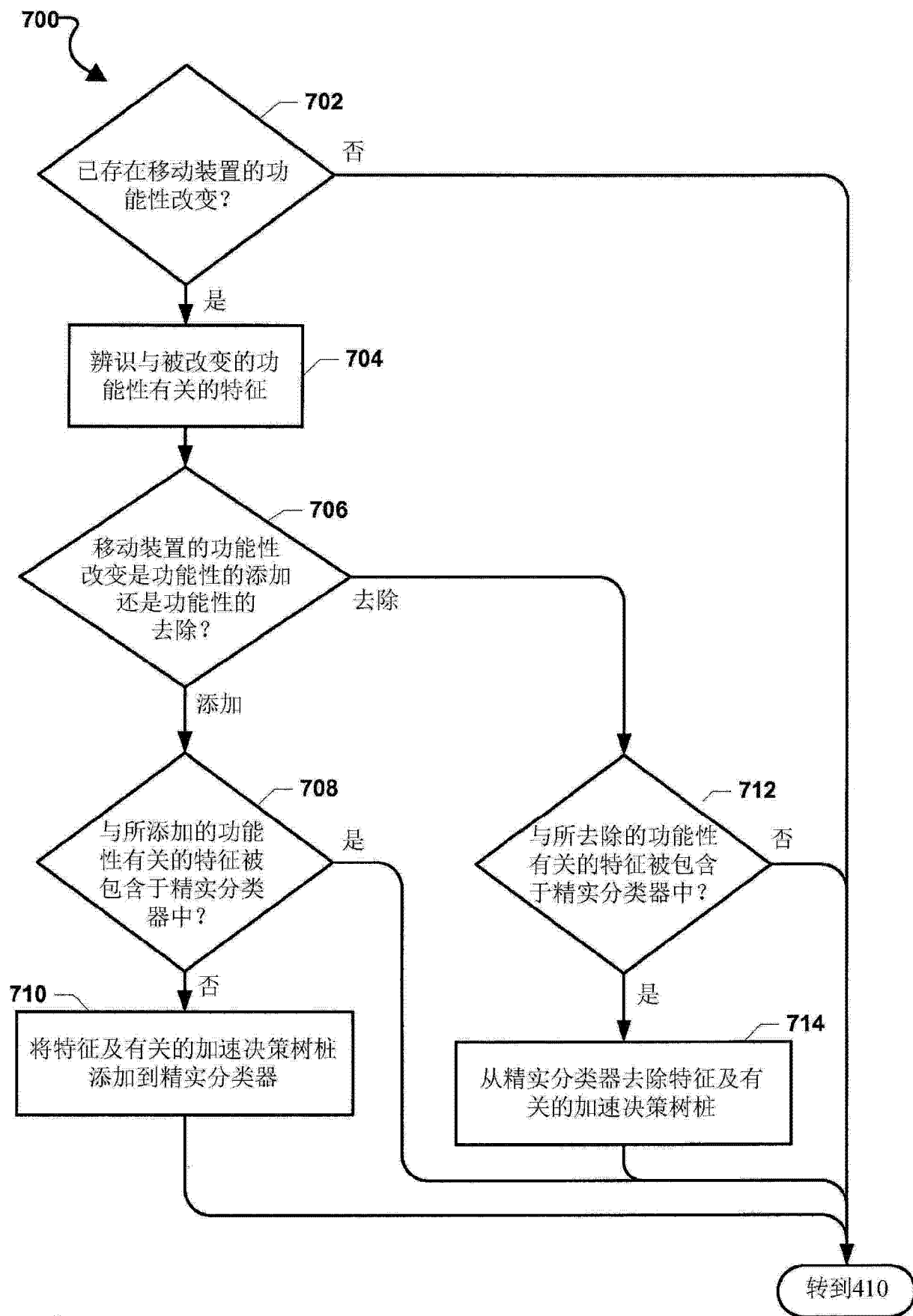


图 7

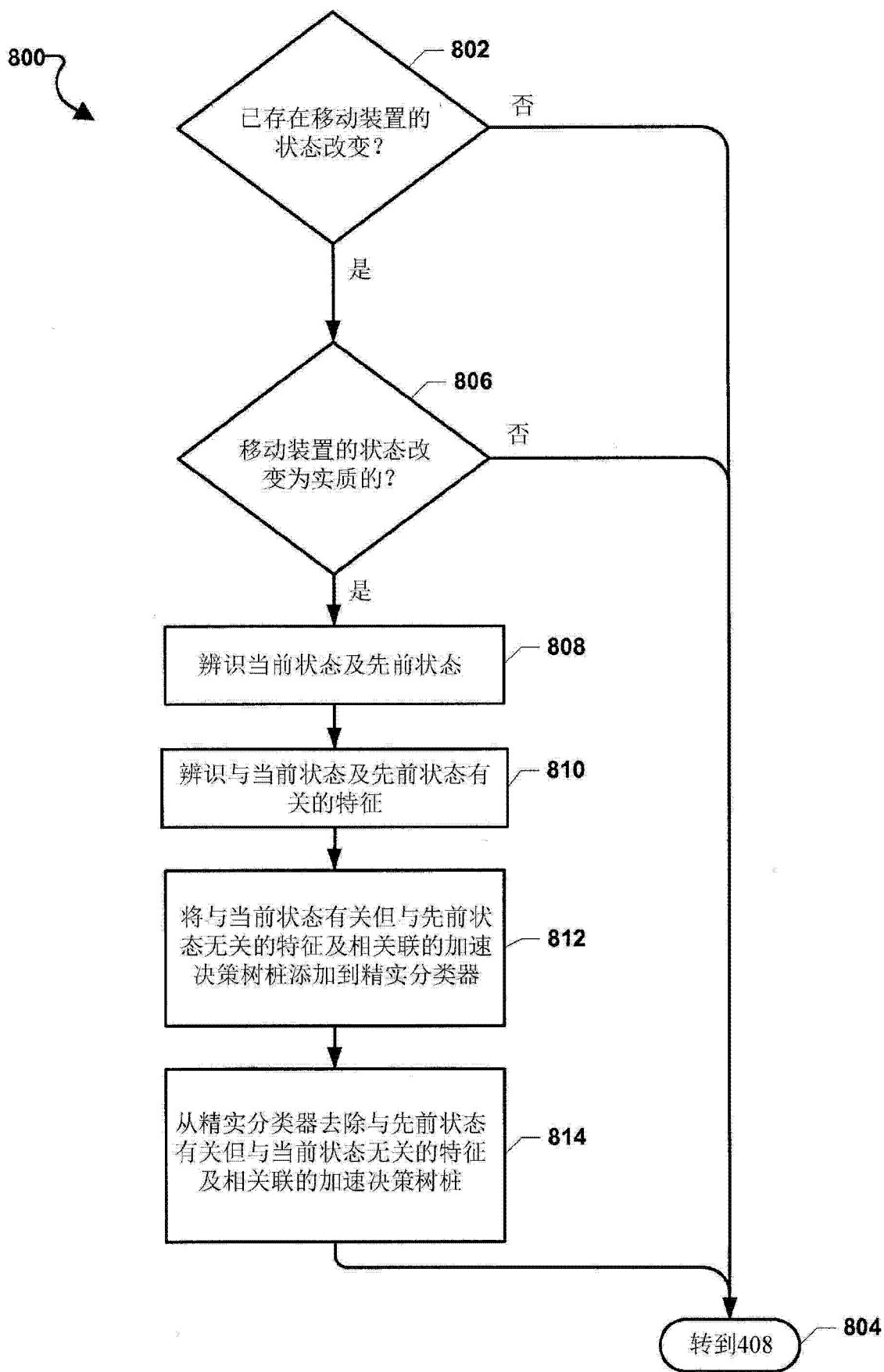


图 8

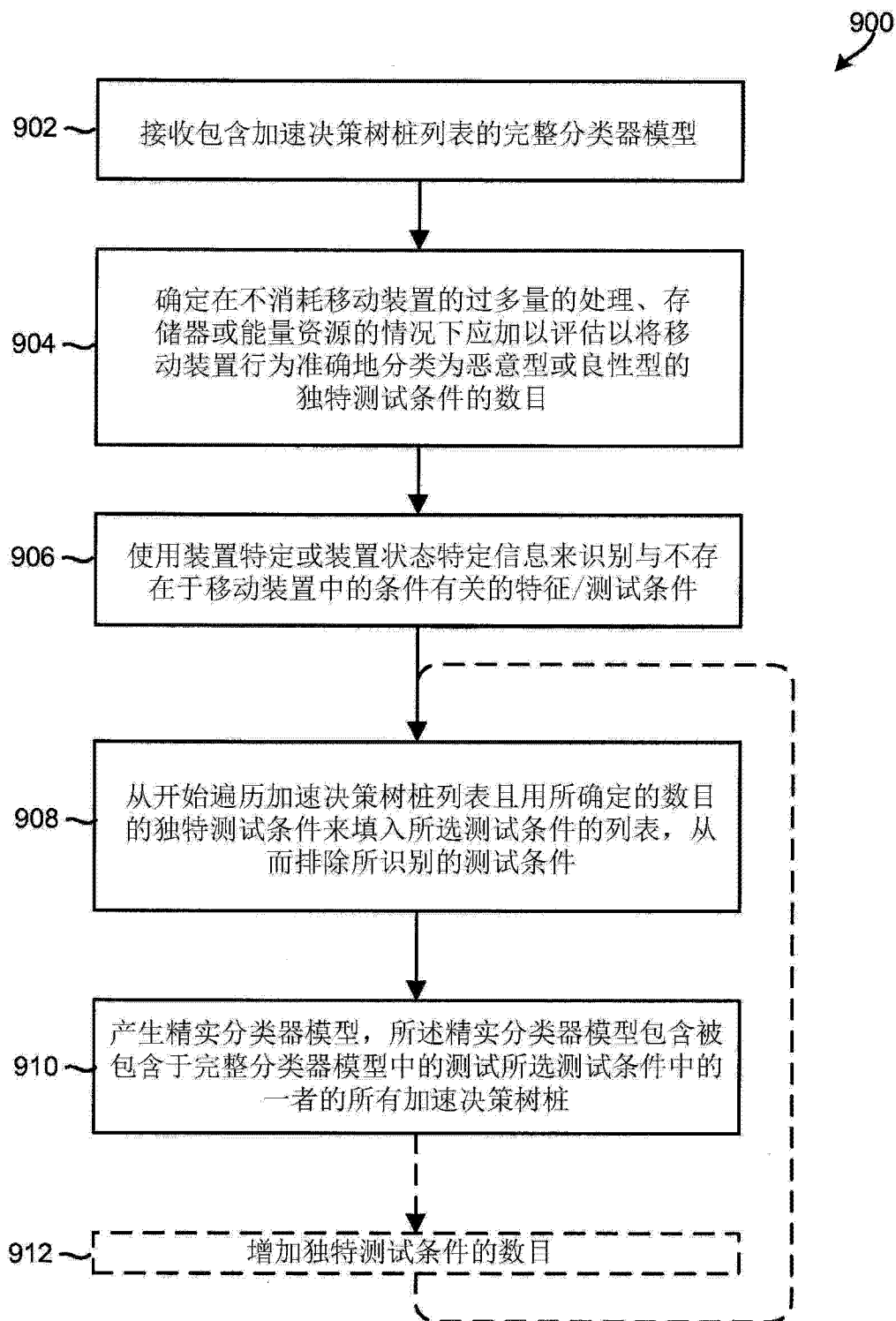


图 9

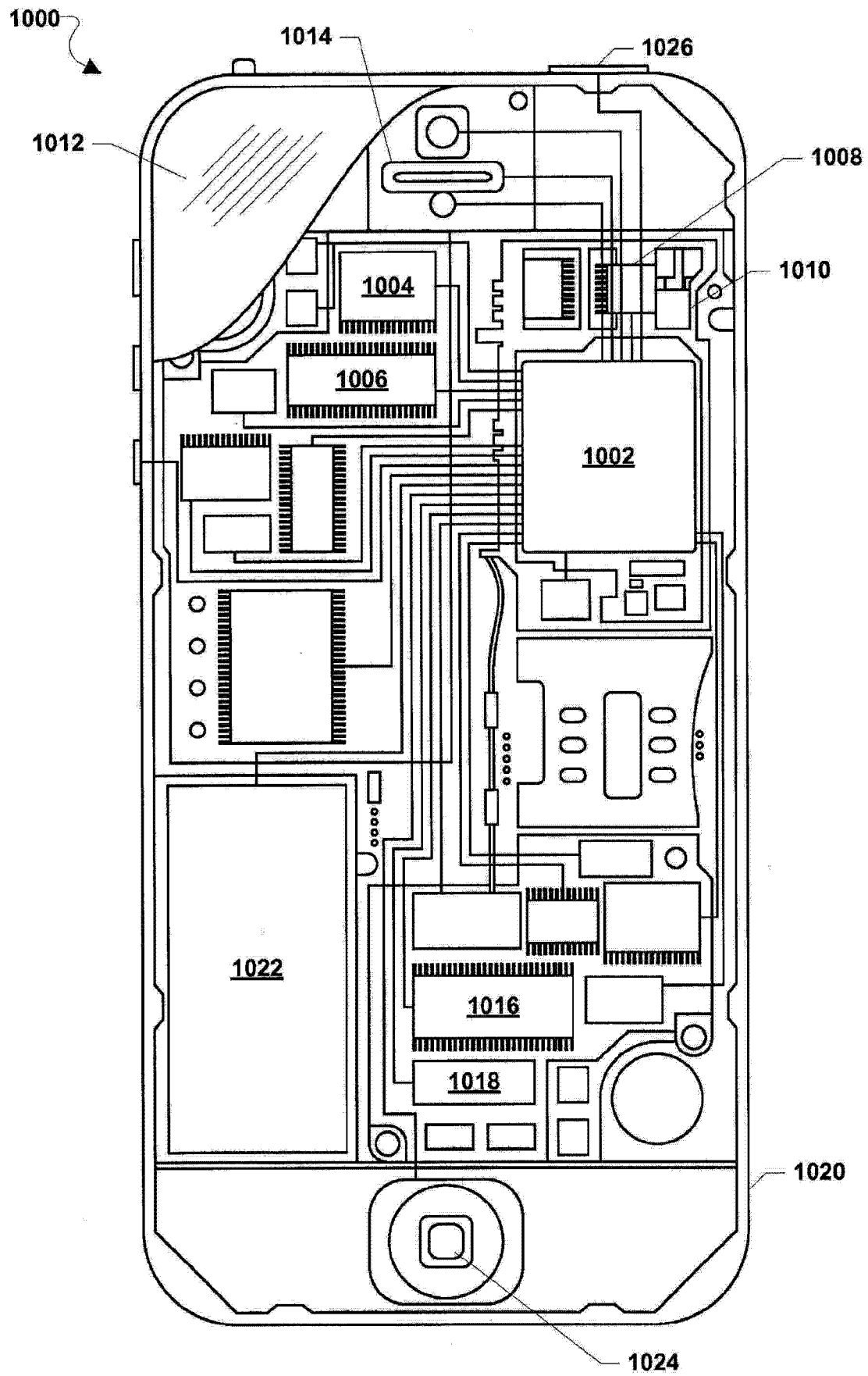


图 10

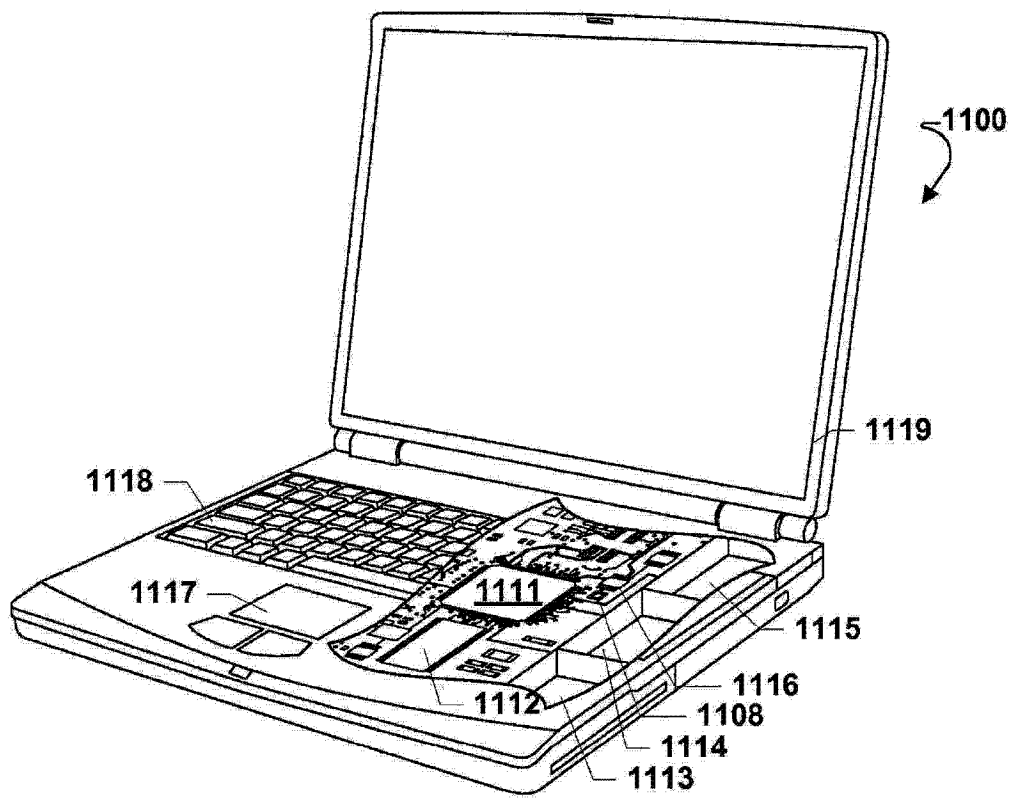


图 11