(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년04월12일
(11) 등록번호 10-1848576
(24) 등록일자 2018년04월06일

(51) 국제특허분류(Int. Cl.)
G06F 21/52 (2013.01) *G06F 11/36* (2006.01)
G06F 21/44 (2013.01) *G06F 21/55* (2013.01)
G06F 21/56 (2013.01) *G06N 5/04* (2006.01)
G06N 99/00 (2010.01)
(52) CPC특허분류
G06F 21/52 (2013.01)
G06F 11/3612 (2013.01)
(21) 출원번호 10-2016-7017189
(22) 출원일자(국제) 2014년12월05일
심사청구일자 2017년06월28일
(85) 번역문제출일자 2016년06월27일
(65) 공개번호 10-2016-0094387
(43) 공개일자 2016년08월09일
(86) 국제출원번호 PCT/US2014/068944
(87) 국제공개번호 WO 2015/085265
국제공개일자 2015년06월11일
(30) 우선권주장
61/912,624 2013년12월06일 미국(US)
14/259,501 2014년04월23일 미국(US)
(56) 선행기술조사문헌
US20130247187 A1
US20100281248 A1
US8266698 B1
US20060085854 A1

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
굽타 라자르시
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
간트만 알렉산더
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
스리드하라 비나이
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인코리아나

전체 청구항 수 : 총 16 항 심사관 : 구대성

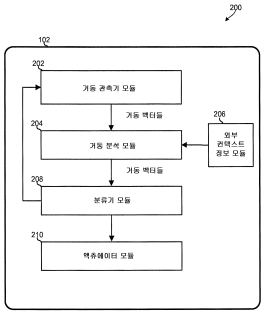
(54) 발명의 명칭 **이동 디바이스 거동들의 효율적인 분류를 위한 애플리케이션-특정 및 애플리케이션-타입-특정 모델들을 이용하는 방법들 및 시스템들**

(57) 요 약

방법들과, 방법들을 구현하는 이동 디바이스들은 소프트웨어 애플리케이션이 바람직하지 않거나 성능 열화하는 거동을 야기시키고 있는지 여부를 예측하는 포괄적인 거동 모니터링 및 분석 시스템의 효율 및 성능을 개선시키기 위하여 애플리케이션-특정 및/또는 애플리케이션-타입 특정 분류기를 이용한다. 애플리케이션-특정 및 애

(뒷면에 계속)

대 표 도



플리케이션-타입 특정 분류기 모델들은 이동 디바이스에서 수신되거나 생성될 수도 있는 전체 또는 더욱 완전한 분류기 모델 내에 포함되는 판단 노드들의 감소되고 더욱 포커싱된 서브세트를 포함할 수도 있다. 국소적으로 생성된 애플리케이션-특정 및/또는 애플리케이션-타입 특정 분류기 모델들은 애플리케이션-기반 분류기 모델들을, 이동 디바이스 거동을 모니터링함으로써 생성된 거동/특징 벡터에 적용함으로써 실시간 거동 모니터링 및 분석 동작들을 수행하기 위하여 이용될 수도 있다. 다양한 양태들은 소프트웨어 애플리케이션의 동작들이 바람직하지 않거나 성능 열화하는 거동에 기여하는지 여부를 결정하기 위해 가장 중요한 작은 수의 특징들에 대해 모니터링 및 분석 동작들을 포커싱한다.

(52) CPC특허분류
G06F 21/44 (2013.01)
G06F 21/552 (2013.01)
G06F 21/562 (2013.01)
G06F 21/566 (2013.01)
G06N 5/04 (2013.01)
G06N 5/043 (2013.01)
G06N 99/005 (2013.01)
G06F 2221/034 (2013.01)

명 세 서

청구범위

청구항 1

별개의 특성들을 가지는 애플리케이션 타입들에 기초하여 이동 디바이스에서 분류기 모델들을 생성하고 사용하는 방법으로서,

상기 이동 디바이스의 프로세서에서, 복수의 부스팅된 판단 스텀프들로의 변환에 적합한 정보를 포함하는 유한 상태 머신을 수신하는 단계로서, 상기 복수의 부스팅된 판단 스텀프들의 각각은 복수의 테스트 조건들 중 하나를 평가하는, 상기 유한 상태 머신을 수신하는 단계;

수신된 상기 유한 상태 머신에 포함된 상기 정보를, 상기 복수의 테스트 조건들 중의 하나를 각각 평가하는 상기 복수의 부스팅된 판단 스텀프들로 변환하는 단계;

상기 복수의 부스팅된 판단 스텀프들에 기초하여 상기 이동 디바이스에서 희박 분류기 모델들의 패밀리를 생성하는 단계;

상기 이동 디바이스의 상기 프로세서를 통해, 상기 복수의 테스트 조건들에서 테스트 조건들의 서브세트를 평가하는 상기 복수의 부스팅된 판단 스텀프들에서의 부스팅된 판단 스텀프들을 포함하고 우선순위화하는 애플리케이션-타입-특정 분류기 모델을 생성하는 단계로서, 상기 테스트 조건들의 서브세트는 소프트웨어 애플리케이션의 하나의 타입에 의해 사용되는 이동 디바이스 특징 (feature) 들을 평가하도록 결정되고, 상기 소프트웨어 애플리케이션의 하나의 타입은 상기 이동 디바이스에 실행하는데 적합한 것으로 결정되는, 상기 애플리케이션-타입-특정 분류기 모델을 생성하는 단계;

상기 희박 분류기 모델들의 패밀리로부터 희박 분류기 모델을 선택하는 단계; 및

수집된 거동 정보를 생성된 상기 애플리케이션-타입-특정 분류기 모델 및 선택된 상기 희박 분류기 모델에 병렬로 적용하여 상기 이동 디바이스의 거동을 분류하는 단계를 포함하는, 이동 디바이스에서 분류기 모델들을 생성하고 사용하는 방법.

청구항 2

제 1 항에 있어서,

이동 디바이스 컴포넌트로부터 거동 정보를 수집함으로써 시간의 주기 동안에 상기 거동을 모니터링하는 단계를 더 포함하고,

상기 수집된 거동 정보를 생성된 상기 애플리케이션-타입-특정 분류기 모델 및 선택된 상기 희박 분류기 모델에 병렬로 적용하여 상기 이동 디바이스의 거동을 분류하는 단계는,

특징 벡터를 생성하기 위하여 상기 거동 정보를 이용하는 단계;

생성된 상기 특징 벡터를 상기 애플리케이션-타입-특정 분류기 모델에 적용함으로써 상기 애플리케이션-타입-특정 분류기 모델 내에 포함된 각각의 테스트 조건을 평가하는 단계;

상기 애플리케이션-타입-특정 분류기 모델에서 테스트 조건들을 평가하는 각각의 결과의 가중화된 평균을 연산하는 단계; 및

연산된 상기 가중화된 평균에 기초하여 상기 거동이 양성 (benign) 인지 여부를 결정하는 단계를 포함하는, 이동 디바이스에서 분류기 모델들을 생성하고 사용하는 방법.

청구항 3

제 1 항에 있어서,

상기 애플리케이션-타입-특정 분류기 모델을 생성하는 단계는,

조건을 테스트하기 위하여 요구되는 상기 이동 디바이스에서 이용 가능한 자원의 양을 초과하는 이동 디바이스

자원들의 양을 소비하지 않으면서, 상기 거동을 분류하기 위하여 평가되어야 하는 다수의 고유한 테스트 조건들을 결정하는 단계를 더 포함하는, 이동 디바이스에서 분류기 모델들을 생성하고 사용하는 방법.

청구항 4

제 1 항에 있어서,

소프트웨어 애플리케이션의 상태, 상기 소프트웨어 애플리케이션의 구성, 상기 소프트웨어 애플리케이션의 동작, 및 상기 소프트웨어 애플리케이션의 기능성 중의 하나에 있어서의 변경을 검출하기 위하여 상기 소프트웨어 애플리케이션을 모니터링하는 단계를 더 포함하는, 이동 디바이스에서 분류기 모델들을 생성하고 사용하는 방법.

청구항 5

제 4 항에 있어서,

검출된 상기 변경과 연관된 특징을 식별하는 단계;

식별된 상기 특징이 상기 애플리케이션-타입-특정 분류기 모델 내에 포함되는지 여부를 결정하는 단계; 및

식별된 상기 특징이 상기 애플리케이션-타입-특정 분류기 모델 내에 포함되지 않는 것으로 결정하는 것에 응답하여, 식별된 상기 특징을 평가하는 상기 복수의 테스트 조건들에서의 테스트 조건을 식별하고, 식별된 상기 테스트 조건을 상기 애플리케이션-타입-특정 분류기 모델에 추가하는 단계를 더 포함하는, 이동 디바이스에서 분류기 모델들을 생성하고 사용하는 방법.

청구항 6

제 1 항에 있어서,

거동 정보의 코퍼스를 서버에서 수신하는 것;

상기 거동 정보의 코퍼스에 기초하여 상기 유한 상태 머신을 생성하는 것; 및

상기 유한 상태 머신을 상기 이동 디바이스로 전송하는 것에 의해, 상기 서버에서 상기 유한 상태 머신을 생성하는 단계를 더 포함하는, 이동 디바이스에서 분류기 모델들을 생성하고 사용하는 방법.

청구항 7

이동 컴퓨팅 디바이스로서,

메모리; 및

상기 메모리에 커플링되고, 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성된 프로세서를 포함하고,

상기 동작들은,

복수의 부스팅된 판단 스텀프들로의 변환에 적합한 정보를 포함하는 유한 상태 머신을 수신하는 것으로서, 상기 복수의 부스팅된 판단 스텀프들의 각각은 복수의 테스트 조건들 중 하나를 평가하는, 상기 유한 상태 머신을 수신하는 것;

수신된 상기 유한 상태 머신에 포함된 상기 정보를, 상기 복수의 테스트 조건들 중의 하나를 각각 평가하는 상기 복수의 부스팅된 판단 스텀프들로 변환하는 것;

상기 복수의 부스팅된 판단 스텀프들에 기초하여 희박 분류기 모델들의 패밀리를 생성하는 것;

상기 복수의 테스트 조건들에서 테스트 조건들의 서브세트를 평가하는 상기 복수의 부스팅된 판단 스텀프들에서의 부스팅된 판단 스텀프들을 포함하고 우선순위화하는 애플리케이션-타입-특정 분류기 모델을 생성하는 것으로서, 상기 테스트 조건들의 서브세트는 소프트웨어 애플리케이션의 하나의 타입에 의해 사용되는 이동 디바이스 특징들을 평가하도록 결정되고, 상기 소프트웨어 애플리케이션의 하나의 타입은 상기 이동 디바이스에 실행하는데 적합한 것으로 결정되는, 상기 애플리케이션-타입-특정 분류기 모델을 생성하는 것;

상기 희박 분류기 모델들의 패밀리로부터 희박 분류기 모델을 선택하는 것; 및

수집된 거동 정보를 생성된 상기 애플리케이션-타입-특정 분류기 모델 및 선택된 상기 희박 분류기 모

델에 병렬로 적용하여 상기 이동 디바이스의 거동을 분류하는 것

을 포함하는, 이동 컴퓨팅 디바이스.

청구항 8

제 7 항에 있어서,

상기 프로세서는, 이동 디바이스 컴포넌트로부터 거동 정보를 수집함으로써 시간의 주기 동안에 상기 거동을 모니터링하는 것을 더 포함하는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되고; 그리고

상기 프로세서는, 상기 수집된 거동 정보를 생성된 상기 애플리케이션-타입-특정 분류기 모델 및 선택된 상기 희박 분류기 모델에 병렬로 적용하여 상기 이동 디바이스의 거동을 분류하는 것이,

특징 벡터를 생성하기 위하여 상기 거동 정보를 이용하는 것;

생성된 상기 특징 벡터를 상기 애플리케이션-타입-특정 분류기 모델에 적용함으로써 상기 애플리케이션-타입-특정 분류기 모델 내에 포함된 각각의 테스트 조건을 평가하는 것;

상기 애플리케이션-타입-특정 분류기 모델에서 테스트 조건들을 평가하는 각각의 결과의 가중화된 평균을 연산하는 것; 및

연산된 상기 가중화된 평균에 기초하여 상기 거동이 양성인지 여부를 결정하는 것을 포함하도록 하는

동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되는, 이동 컴퓨팅 디바이스.

청구항 9

제 7 항에 있어서,

상기 프로세서는,

상기 애플리케이션-타입-특정 분류기 모델을 생성하는 것이 조건을 테스트하기 위하여 요구되는 상기 이동 디바이스에서 이용 가능한 자원의 양을 초과하는 이동 디바이스 자원들의 양을 소비하지 않으면서, 상기 거동을 분류하기 위하여 평가되어야 하는 다수의 고유한 테스트 조건들을 결정하는 것을 포함하도록 하는

동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되는, 이동 컴퓨팅 디바이스.

청구항 10

프로세서-실행가능 소프트웨어 명령들을 저장한 비-일시적 컴퓨터 판독가능 저장 매체로서,

상기 프로세서-실행가능 소프트웨어 명령들은, 이동 디바이스의 프로세서로 하여금, 동작들을 수행하게 하도록 구성되고, 상기 동작들은,

복수의 부스팅된 판단 스텀프들로의 변환에 적합한 정보를 포함하는 유한 상태 머신을 수신하는 것으로서, 상기 복수의 부스팅된 판단 스텀프들의 각각은 복수의 테스트 조건들 중 하나를 평가하는, 상기 유한 상태 머신을 수신하는 것;

수신된 상기 유한 상태 머신에 포함된 상기 정보를, 상기 복수의 테스트 조건들 중의 하나를 각각 평가하는 상기 복수의 부스팅된 판단 스텀프들로 변환하는 것;

상기 복수의 부스팅된 판단 스텀프들에 기초하여 상기 이동 디바이스에서 희박 분류기 모델들의 패밀리를 생성하는 것;

상기 복수의 테스트 조건들에서 테스트 조건들의 서브세트를 평가하는 상기 복수의 부스팅된 판단 스텀프들에서의 부스팅된 판단 스텀프들을 포함하고 우선순위화하는 애플리케이션-타입-특정 분류기 모델을 생성하는 것으로서, 상기 테스트 조건들의 서브세트는 소프트웨어 애플리케이션의 하나의 타입에 의해 사용되는 이동 디바이스 특징들을 평가하도록 결정되고, 상기 소프트웨어 애플리케이션의 하나의 타입은 상기 이동 디바이스에 실행하는데 적합한 것으로 결정되는, 상기 애플리케이션-타입-특정 분류기 모델을 생성하는 것;

상기 희박 분류기 모델들의 패밀리로부터 희박 분류기 모델을 선택하는 것; 및

수집된 거동 정보를 생성된 상기 애플리케이션-타입-특정 분류기 모델 및 선택된 상기 희박 분류기 모델에 병렬

로 적용하여 상기 이동 디바이스의 거동을 분류하는 것

을 포함하는, 비-일시적 컴퓨터 판독가능 저장 매체.

청구항 11

제 10 항에 있어서,

상기 저장된 프로세서-실행가능 소프트웨어 명령들은, 프로세서로 하여금, 이동 디바이스 컴포넌트로부터 거동 정보를 수집함으로써 시간의 주기 동안에 상기 거동을 모니터링하는 것을 더 포함하는 동작들을 수행하게 하도록 구성되고; 그리고

상기 저장된 프로세서-실행가능 소프트웨어 명령들은, 프로세서로 하여금, 상기 수집된 거동 정보를 생성된 상기 애플리케이션-타입-특정 분류기 모델 및 선택된 상기 희박 분류기 모델에 병렬로 적용하여 상기 이동 디바이스의 거동을 분류하는 것이,

특징 벡터를 생성하기 위하여 상기 거동 정보를 이용하는 것;

생성된 상기 특징 벡터를 상기 애플리케이션-타입-특정 분류기 모델에 적용함으로써 상기 애플리케이션-타입-특정 분류기 모델 내에 포함된 각각의 테스트 조건을 평가하는 것;

상기 애플리케이션-타입-특정 분류기 모델에서 테스트 조건들을 평가하는 각각의 결과의 가중화된 평균을 연산하는 것; 및

연산된 상기 가중화된 평균에 기초하여 상기 거동이 양성인지 여부를 결정하는 것을 포함하도록 하는

동작들을 수행하게 하도록 구성되는, 비-일시적 컴퓨터 판독가능 저장 매체.

청구항 12

제 10 항에 있어서,

상기 저장된 프로세서-실행가능 소프트웨어 명령들은, 프로세서로 하여금,

상기 애플리케이션-타입-특정 분류기 모델을 생성하는 것이 조건을 테스트하기 위하여 요구되는 상기 이동 디바이스에서 이용 가능한 자원의 양을 초과하는 이동 디바이스 자원들의 양을 소비하지 않으면서, 상기 거동을 분류하기 위하여 평가되어야 하는 다수의 고유한 테스트 조건들을 결정하는 것을 더 포함하도록 하는

동작들을 수행하게 하도록 구성되는, 비-일시적 컴퓨터 판독가능 저장 매체.

청구항 13

이동 컴퓨팅 디바이스로서,

복수의 부스팅된 판단 스텀프들로의 변환에 적합한 정보를 포함하는 유한 상태 머신을 수신하기 위한 수단으로서, 상기 복수의 부스팅된 판단 스텀프들의 각각은 복수의 테스트 조건들 중 하나를 평가하는, 상기 유한 상태 머신을 수신하기 위한 수단;

수신된 상기 유한 상태 머신에 포함된 상기 정보를, 상기 복수의 테스트 조건들 중의 하나를 각각 평가하는 상기 복수의 부스팅된 판단 스텀프들로 변환하기 위한 수단;

상기 복수의 부스팅된 판단 스텀프들에 기초하여 희박 분류기 모델들의 패밀리를 생성하기 위한 수단;

상기 복수의 테스트 조건들에서 테스트 조건들의 서브세트를 평가하는 상기 복수의 부스팅된 판단 스텀프들에서의 부스팅된 판단 스텀브들을 포함하고 우선순위화하는 애플리케이션-타입-특정 분류기 모델을 생성하기 위한 수단으로서, 상기 테스트 조건들의 서브세트는 소프트웨어 애플리케이션의 하나의 타입에 의해 사용되는 이동 디바이스 특징들을 평가하도록 결정되고, 상기 소프트웨어 애플리케이션의 하나의 타입은 상기 이동 디바이스에 실행하는데 적합한 것으로 결정되는, 상기 애플리케이션-타입-특정 분류기 모델을 생성하기 위한 수단;

상기 희박 분류기 모델들의 패밀리로부터 희박 분류기 모델들을 선택하기 위한 수단; 및

수집된 거동 정보를 생성된 상기 애플리케이션-타입-특정 분류기 모델 및 선택된 상기 희박 분류기 모델에 병렬로 적용하여 상기 이동 디바이스의 거동을 분류하기 위한 수단을 포함하는, 이동 컴퓨팅 디바이스.

청구항 14

제 13 항에 있어서,

이동 디바이스 컴포넌트로부터 거동 정보를 수집함으로써 시간의 주기 동안에 상기 거동을 모니터링하기 위한 수단을 더 포함하고,

상기 수집된 거동 정보를 생성된 상기 애플리케이션-타입-특정 분류기 모델 및 선택된 상기 희박 분류기 모델에 병렬로 적용하여 상기 이동 디바이스의 거동을 분류하기 위한 수단은,

특징 벡터를 생성하기 위하여 상기 거동 정보를 이용하기 위한 수단;

생성된 상기 특징 벡터를 상기 애플리케이션-타입-특정 분류기 모델에 적용함으로써 상기 애플리케이션-타입-특정 분류기 모델 내에 포함된 각각의 테스트 조건을 평가하기 위한 수단;

상기 애플리케이션-타입-특정 분류기 모델에서 테스트 조건들을 평가하는 각각의 결과의 가중화된 평균을 연산하기 위한 수단; 및

연산된 상기 가중화된 평균에 기초하여 상기 거동이 양성인지 여부를 결정하기 위한 수단을 포함하는, 이동 컴퓨팅 디바이스.

청구항 15

제 13 항에 있어서,

상기 애플리케이션-타입-특정 분류기 모델을 생성하기 위한 수단은, 조건을 테스트하기 위하여 요구되는 상기 이동 디바이스에서 이용 가능한 자원의 양을 초과하는 이동 디바이스 자원들의 양을 소비하지 않으면서, 상기 거동을 분류하기 위하여 평가되어야 하는 다수의 고유한 테스트 조건들을 결정하기 위한 수단을 더 포함하는, 이동 컴퓨팅 디바이스.

청구항 16

제 13 항에 있어서,

소프트웨어 애플리케이션의 상태, 상기 소프트웨어 애플리케이션의 구성, 상기 소프트웨어 애플리케이션의 동작, 및 상기 소프트웨어 애플리케이션의 기능성 중의 하나에 있어서의 변경을 검출하기 위하여 상기 소프트웨어 애플리케이션을 모니터링하기 위한 수단을 더 포함하는, 이동 컴퓨팅 디바이스.

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

발명의 설명

기 술 분 야

[0001] 관련된 출원들

[0002] 이 출원은, 그 전체 내용들이 모든 목적들을 위한 참조에 의해 본원에 편입되는, 2013 년 12 월 6 일자로 출원된 "Methods and Systems of Using Application-Specific and Application-Type-Specific Models for the Efficient Classification of Mobile Device Behaviors" 라는 명칭의 미국 가출원 제 61/912,624 호에 대한 우선권의 이익을 주장한다.

배 경 기 술

[0003] 셀룰러 및 무선 통신 기술들은 과거 몇 년에 걸쳐 폭발적인 성장을 보였다. 이 성장은 더욱 양호한 통신들, 하드웨어, 더욱 대형의 네트워크들, 및 더욱 신뢰성 있는 프로토콜들에 의해 추진되었다. 그 결과, 무선 서비스 제공자들은 이제 그들의 고객들에게 정보, 자원들, 및 통신들에 대한 전례없는 레벨들의 액세스를 제공할 수 있다.

[0004] 이 서비스 개량들과 보조를 맞추기 위하여, 이동 전자 디바이스들 (예컨대, 셀룰러 전화들, 태블릿들, 랩톱들 등) 은 이전보다 더욱 강력하고 복잡하게 되었다. 이 복잡성은 악성 (malicious) 소프트웨어, 소프트웨어 충돌들, 하드웨어 고장들, 및 이동 디바이스의 장기간 그리고 계속된 성능 및 전력 사용 레벨들에 부정적으로 영향을 주기 위한 다른 유사한 에러들 또는 현상들에 대한 새로운 기회들을 만들었다. 따라서, 이동 디바이스의 장기간 그리고 계속된 성능 및 전력 사용 레벨들에 부정적으로 영향을 줄 수도 있는 조건들 및/또는 이동 디바이스 거동 (behavior) 들을 식별하고 정정하는 것은 소비자들에게 유익하다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0005] 다양한 양태들은, 복수의 테스트 조건들을 포함하는 전체 분류기 모델 (full classifier model) 을 이동 디바이스의 프로세서에서 수신하는 것, 이동 디바이스의 소프트웨어 애플리케이션에 의해 이용된 이동 디바이스 특징들, 또는 이동 디바이스 상에 실행할 수 있는 소프트웨어 애플리케이션의 타입을 식별하는 것, 식별된 이동 디바이스 특징들을 평가하는 복수의 테스트 조건들에서 테스트 조건들을 식별하는 것, 식별된 테스트 조건들을 우선순위화하는 애플리케이션-기반 분류기 모델 (애플리케이션-기반 분류기 모델은 애플리케이션-특정 분류기 모델 또는 애플리케이션-타입-특정 분류기 모델임) 을 생성하는 것, 및 이동 디바이스의 거동을 분류하기 위하여 이동 디바이스에서 생성된 애플리케이션-기반 분류기 모델을 이용하는 것에 의해 이동 디바이스에서 데이터 모델들을 생성하는 방법들을 포함한다.

[0006] 일 양태에서, 이동 디바이스 특징들을 식별하는 것은 소프트웨어 애플리케이션에 의해 이용된 이동 디바이스 특징들을 식별하는 것을 포함할 수도 있고, 애플리케이션-기반 분류기 모델을 생성하는 것은 애플리케이션-특정 분류기 모델을 생성하는 것을 포함할 수도 있다. 추가의 양태에서, 이동 디바이스 특징들을 식별하는 것은 이동 디바이스 상에 실행할 수 있는 소프트웨어 애플리케이션의 하나의 타입에 의해 이용된 이동 디바이스 특징들을 식별하는 것을 포함할 수도 있고, 애플리케이션-기반 분류기 모델을 생성하는 것은 애플리케이션-타입-특정 분류기 모델을 생성하는 것을 포함할 수도 있다.

[0007] 추가의 양태에서, 방법은 이동 디바이스 컴포넌트로부터 거동 정보를 수집함으로써 시간의 주기 동안에 거동을 모니터링하는 것을 포함할 수도 있다. 추가의 양태에서, 이동 디바이스의 거동을 분류하기 위하여 이동 디바이스에서 애플리케이션-기반 분류기 모델을 이용하는 것은 특징 벡터를 생성하기 위하여 거동 정보를 이용하는 것, 생성된 특징 벡터를 애플리케이션-기반 분류기 모델에 적용함으로써 애플리케이션-기반 분류기 모델 내에 포함된 각각의 테스트 조건을 평가하는 것, 애플리케이션-기반 분류기 모델에서 테스트 조건들을 평가하는 각각의 결과의 가중화된 평균을 연산하는 것, 및 가중화된 평균에 기초하여 거동이 악성인지 또는 양성 (benign) 인지 여부를 결정하는 것을 포함할 수도 있다.

[0008] 추가의 양태에서, 복수의 테스트 조건들을 식별하는 전체 분류기 모델을 수신하는 것은 복수의 테스트 조건들 중의 하나를 각각 평가하는 복수의 판단 노드들로의 변환에 적합한 정보를 포함할 수도 있는 유한 상태 머신 (finite state machine) 을 수신하는 것을 포함할 수도 있다. 일 양태에서, 식별된 테스트 조건들을 우선순위화하는 애플리케이션-기반 분류기 모델을 생성하는 것은 소프트웨어 애플리케이션에 관련되는 이동 디바이스 특징, 및/또는 소프트웨어 애플리케이션의 타입에 관련되는 이동 디바이스 특징 중의 하나를 평가하는 판단 노드들을 포함하기 위하여 애플리케이션-기반 분류기 모델을 생성하는 것을 포함할 수도 있다.

[0009] 추가의 양태에서, 식별된 테스트 조건들을 우선순위화하는 애플리케이션-기반 분류기 모델을 생성하는 것은 이동 디바이스 자원들 (예컨대, 메모리, 프로세싱, 및 배터리 자원들) 의 과도한 양을 소비하지 않으면서, 거동을 분류하기 위하여 평가되어야 하는 다수의 고유한 테스트 조건들을 결정하는 것, 전체 분류기 모델에서 복수의 테스트 조건들을 순차적으로 트래버싱함으로써 테스트 조건들의 리스트를 생성하고, 테스트 조건들의 리스트가 결정된 수의 고유한 테스트 조건들을 포함할 때까지, 소프트웨어 애플리케이션에 의해 액세스되고 이용될 수도 있는 특징들에 관련되는 그 테스트 조건들을 테스트 조건들의 리스트 내로 삽입하는 것, 및 전체 분류기 모델 내에 포함되고, 테스트 조건들 중의 생성된 리스트 내에 포함된 테스트 조건들 중의 하나를 테스트하는 판단 노드들을 포함하기 위하여 애플리케이션-기반 분류기 모델을 생성하는 것을 포함할 수도 있다.

[0010] 추가의 양태에서, 복수의 테스트 조건들을 식별하는 전체 분류기 모델을 수신하는 것은 유한 상태 머신을 수신하는 것을 포함할 수도 있다. 추가의 양태에서, 방법은 유한 상태 머신을, 복수의 테스트 조건들 중의 하나를 각각 평가하는 부스팅된 판단 스텀프 (boosted decision stump) 들로 변환하는 것, 부스팅된 판단 스텀프들에 기초하여 이동 디바이스에서 희박 분류기 모델 (lean classifier model) 들의 패밀리 (family) 를 생성하는 것, 희박 분류기 모델들의 패밀리로부터 희박 분류기 모델들을 선택하는 것, 및 수집된 거동 정보를 애플리케이션-기반 분류기 모델 및 선택된 희박 분류기 모델에 병렬로 적용하는 것을 포함한다.

[0011] 추가의 양태에서, 이동 디바이스 특징들을 식별하는 것은 소프트웨어 애플리케이션에 의해 이용된 이동 디바이스 특징들을 식별하는 것을 포함할 수도 있다. 추가의 양태에서, 방법은 소프트웨어 애플리케이션의 상태, 소프트웨어 애플리케이션의 구성, 소프트웨어 애플리케이션의 동작, 및 소프트웨어 애플리케이션의 기능성 중의 하나에 있어서의 변경을 검출하기 위하여 소프트웨어 애플리케이션을 모니터링하는 것을 포함할 수도 있다. 추가의 양태에서, 방법은 변경을 검출하는 것에 응답하여 테스트 조건들의 업데이트된 세트를 포함하기 위하여

애플리케이션-기반 분류기 모델을 수정하는 것, 및 이동 디바이스의 거동을 재분류하기 위하여 수정된 애플리케이션-기반 분류기 모델을 이용하는 것을 포함할 수도 있다.

[0012] 추가의 양태에서, 소프트웨어 애플리케이션을 모니터링하는 것과, 변경을 검출하는 것에 응답하여 테스트 조건들의 업데이트된 세트를 포함하기 위하여 애플리케이션-기반 분류기 모델을 수정하는 것은 검출된 변경과 연관된 특징을 식별하는 것, 식별된 특징이 애플리케이션-기반 분류기 모델 내에 포함되는지 여부를 결정하는 것, 식별된 특징을 평가하는 복수의 테스트 조건들에서 테스트 조건을 식별하는 것, 식별된 특징이 애플리케이션-기반 분류기 모델 내에 포함되지 않는 것으로 결정하는 것에 응답하여 식별된 테스트 조건을 애플리케이션-기반 분류기 모델에 추가하는 것을 포함할 수도 있다. 추가의 양태에서, 방법은 거동 정보의 코퍼스 (corpus) 를 서버에서 수신하는 것, 복수의 부스팅된 판단 스텀프들로의 변환에 적합한 데이터를 포함하기 위하여 거동 정보의 코퍼스에 기초하여 유한 상태 머신을 생성하는 것, 및 유한 상태 머신을 전체 분류기 모델로서 이동 디바이스로 전송하는 것에 의해, 서버에서 전체 분류기 모델을 생성하는 것을 포함할 수도 있다.

[0013] 추가의 양태들은, 복수의 테스트 조건들을 포함하는 전체 분류기 모델을 수신하는 것, 이동 컴퓨팅 디바이스의 소프트웨어 애플리케이션 중의 하나에 의해 이용된 이동 디바이스 특징들과, 이동 컴퓨팅 디바이스 상에서 실행될 수도 있는 소프트웨어 애플리케이션의 타입을 식별하는 것, 식별된 이동 디바이스 특징들을 평가하는 복수의 테스트 조건들에서 테스트 조건들을 식별하는 것, 식별된 테스트 조건들을 우선순위화하는 애플리케이션-기반 분류기 모델 (즉, 애플리케이션-특정 분류기 모델 또는 애플리케이션-타입-특정 분류기 모델) 을 생성하는 것, 및 이동 컴퓨팅 디바이스의 거동을 분류하기 위하여 생성된 애플리케이션-기반 분류기 모델을 이용하는 것을 포함할 수도 있는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성된 프로세서를 가지는 이동 컴퓨팅 디바이스를 포함한다.

[0014] 일 양태에서, 프로세서는, 이동 디바이스 특징들을 식별하는 것이 소프트웨어 애플리케이션에 의해 이용된 이동 디바이스 특징들을 식별하는 것을 포함할 수도 있고, 애플리케이션-기반 분류기 모델을 생성하는 것이 애플리케이션-특정 분류기 모델을 생성하는 것을 포함할 수도 있도록 하는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성될 수도 있다. 추가의 양태에서, 프로세서는, 이동 디바이스 특징들을 식별하는 것이 이동 컴퓨팅 디바이스 상에서 실행될 수도 있는 소프트웨어 애플리케이션의 하나의 타입에 의해 이용된 이동 디바이스 특징들을 식별하는 것을 포함할 수도 있고, 애플리케이션-기반 분류기 모델을 생성하는 것이 애플리케이션-타입-특정 분류기 모델을 생성하는 것을 포함할 수도 있도록 하는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성될 수도 있다.

[0015] 추가의 양태에서, 프로세서는 이동 디바이스 컴포넌트로부터 거동 정보를 수집함으로써 시간의 주기 동안에 거동을 모니터링하는 것을 더 포함할 수도 있는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성될 수도 있다. 추가의 양태에서, 프로세서는, 거동을 분류하기 위하여 애플리케이션-기반 분류기 모델을 이용하는 것이 특징 벡터를 생성하기 위하여 거동 정보를 이용하는 것, 생성된 특징 벡터를 애플리케이션-기반 분류기 모델에 적용함으로써 애플리케이션-기반 분류기 모델 내에 포함된 각각의 테스트 조건을 평가하는 것, 애플리케이션-기반 분류기 모델에서 테스트 조건들을 평가하는 각각의 결과의 가중화된 평균을 연산하는 것, 및 가중화된 평균에 기초하여 거동이 악성인지 또는 양성인지 여부를 결정하는 것을 포함할 수도 있도록 하는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성될 수도 있다.

[0016] 추가의 양태에서, 프로세서는, 복수의 테스트 조건들을 식별하는 전체 분류기 모델을 수신하는 것이 복수의 테스트 조건들 중의 하나를 각각 평가하는 복수의 판단 노드들로의 변환에 적합한 정보를 포함하는 유한 상태 머신을 수신하는 것을 포함할 수도 있고, 식별된 테스트 조건들을 우선순위화하는 애플리케이션-기반 분류기 모델을 생성하는 것이 소프트웨어 애플리케이션에 관련되는 이동 디바이스 특징과, 소프트웨어 애플리케이션의 타입에 관련되는 이동 디바이스 특징 중의 하나를 평가하는 판단 노드들을 포함하기 위하여 애플리케이션-기반 분류기 모델을 생성하는 것을 포함할 수도 있도록 하는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성될 수도 있다.

[0017] 추가의 양태에서, 프로세서는, 식별된 테스트 조건들을 우선순위화하는 애플리케이션-기반 분류기 모델을 생성하는 것이 이동 디바이스 자원들의 과도한 양을 소비하지 않으면서, 거동을 분류하기 위하여 평가되어야 하는 다수의 고유한 테스트 조건들을 결정하는 것, 전체 분류기 모델에서 복수의 테스트 조건들을 순차적으로 트래버싱함으로써 테스트 조건들의 리스트를 생성하고, 테스트 조건들의 리스트가 다수의 고유한 테스트 조건들을 포함할 때까지, 소프트웨어 애플리케이션에 의해 액세스되고 이용될 수도 있는 특징들에 관련되는 그 테스트 조건들을 테스트 조건들의 리스트 내로 삽입하는 것, 및 테스트 조건들의 생성된 리스트 내에 포함된 테스트 조건들

중의 하나를 테스트하는 전체 분류기 모델에서의 판단 노드들을 포함하기 위하여 애플리케이션-기반 분류기 모델을 생성하는 것을 더 포함할 수도 있도록 하는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성될 수도 있다.

[0018] 추가의 양태들은, 프로세서로 하여금, 복수의 테스트 조건들을 포함하는 전체 분류기 모델을 수신하는 것, 소프트웨어 애플리케이션 중의 하나에 의해 이용된 이동 디바이스 특징들과, 이동 디바이스 상에 실행할 수 있는 소프트웨어 애플리케이션의 타입을 식별하는 것, 식별된 이동 디바이스 특징들을 평가하는 복수의 테스트 조건들에서 테스트 조건들을 식별하는 것, 식별된 테스트 조건들을 우선순위화하는 애플리케이션-기반 분류기 모델(예컨대, 애플리케이션-특정 분류기 모델 또는 애플리케이션-타입-특정 분류기 모델)을 생성하는 것, 및 이동 디바이스의 거동을 분류하기 위하여 생성된 애플리케이션-기반 분류기 모델을 이용하는 것을 포함하는 동작들을 수행하게 하도록 구성된 프로세서-실행가능 소프트웨어 명령들을 저장한 비-일시적인 컴퓨터 판독가능 저장 매체를 포함한다.

[0019] 일 양태에서, 저장된 프로세서-실행가능 소프트웨어 명령들은, 프로세서로 하여금, 이동 디바이스 특징들을 식별하는 것이 소프트웨어 애플리케이션에 의해 이용된 이동 디바이스 특징들을 식별하는 것을 포함할 수도 있고, 애플리케이션-기반 분류기 모델을 생성하는 것이 애플리케이션-특정 분류기 모델을 생성하는 것을 포함할 수도 있도록 하는 동작들을 수행하게 하도록 구성될 수도 있다. 추가의 양태에서, 저장된 프로세서-실행가능 소프트웨어 명령들은, 프로세서로 하여금, 이동 디바이스 특징들을 식별하는 것이 이동 디바이스 상에 실행할 수 있는 소프트웨어 애플리케이션의 하나의 타입에 의해 이용된 이동 디바이스 특징들을 식별하는 것을 포함할 수도 있고, 애플리케이션-기반 분류기 모델을 생성하는 것이 애플리케이션-타입-특정 분류기 모델을 생성하는 것을 포함할 수도 있도록 하는 동작들을 수행하게 하도록 구성될 수도 있다.

[0020] 추가의 양태에서, 저장된 프로세서-실행가능 소프트웨어 명령들은, 프로세서로 하여금, 이동 디바이스 컴포넌트로부터 거동 정보를 수집함으로써 시간의 주기 동안에 거동을 모니터링하는 것을 더 포함할 수도 있는 동작들을 수행하게 하도록 구성될 수도 있다. 추가의 양태에서, 저장된 프로세서-실행가능 소프트웨어 명령들은, 프로세서로 하여금, 이동 디바이스의 거동을 분류하기 위하여 애플리케이션-기반 분류기 모델을 이용하는 것이 특징 벡터를 생성하기 위하여 거동 정보를 이용하는 것, 생성된 특징 벡터를 애플리케이션-기반 분류기 모델에 적용함으로써 애플리케이션-기반 분류기 모델 내에 포함된 각각의 테스트 조건을 평가하는 것, 애플리케이션-기반 분류기 모델에서 테스트 조건들을 평가하는 각각의 결과의 가중화된 평균을 연산하는 것, 및 가중화된 평균에 기초하여 거동이 악성인지 또는 양성인지 여부를 결정하는 것을 포함할 수도 있도록 하는 동작들을 수행하게 하도록 구성될 수도 있다.

[0021] 추가의 양태에서, 저장된 프로세서-실행가능 소프트웨어 명령들은, 프로세서로 하여금, 복수의 테스트 조건들을 식별하는 전체 분류기 모델을 수신하는 것이 복수의 테스트 조건들 중의 하나를 각각 평가하는 복수의 판단 노드들로의 변환에 적합한 정보를 포함하는 유한 상태 머신을 수신하는 것을 포함할 수도 있고, 식별된 테스트 조건들을 우선순위화하는 애플리케이션-기반 분류기 모델을 생성하는 것이 소프트웨어 애플리케이션 또는 소프트웨어 애플리케이션의 타입에 관련되는 이동 디바이스 특징을 평가하는 판단 노드들을 포함하기 위하여 애플리케이션-기반 분류기 모델을 생성하는 것을 포함할 수도 있도록 하는 동작들을 수행하게 하도록 구성될 수도 있다.

[0022] 추가의 양태에서, 저장된 프로세서-실행가능 소프트웨어 명령들은, 프로세서로 하여금, 식별된 테스트 조건들을 우선순위화하는 애플리케이션-기반 분류기 모델을 생성하는 것이 이동 디바이스 자원들의 과도한 양을 소비하지 않으면서, 거동을 분류하기 위하여 평가되어야 하는 다수의 고유한 테스트 조건들을 결정하는 것, 전체 분류기 모델에서 복수의 테스트 조건들을 순차적으로 트래버싱함으로써 테스트 조건들의 리스트를 생성하고, 테스트 조건들의 리스트가 다수의 고유한 테스트 조건들을 포함할 때까지, 소프트웨어 애플리케이션에 의해 액세스되고 이용될 수도 있는 특징들에 관련되는 그 테스트 조건들을 테스트 조건들의 리스트 내로 삽입하는 것, 및 테스트 조건들의 생성된 리스트 내에 포함된 테스트 조건들 중의 하나를 테스트하는 전체 분류기 모델에서의 판단 노드들을 포함하기 위하여 애플리케이션-기반 분류기 모델을 생성하는 것을 더 포함할 수도 있도록 하는 동작들을 수행하게 하도록 구성될 수도 있다.

[0023] 추가의 양태들은, 복수의 테스트 조건들을 포함하는 전체 분류기 모델을 수신하기 위한 수단, 소프트웨어 애플리케이션에 의해 이용된 이동 디바이스 특징들, 또는 이동 컴퓨팅 디바이스 상에서 실행될 수도 있는 소프트웨어 애플리케이션의 타입을 식별하기 위한 수단, 식별된 이동 디바이스 특징들을 평가하는 복수의 테스트 조건들에서 테스트 조건들을 식별하기 위한 수단, 식별된 테스트 조건들을 우선순위화하는 애플리케이션-기반 분류기 모델을 생성하기 위한 수단, 및 이동 컴퓨팅 디바이스의 거동을 분류하기 위하여 생성된 애플리케이션-기반 분

류기 모델을 이용하기 위한 수단을 포함할 수도 있는 컴퓨팅 디바이스를 포함한다.

[0024] 일 양태에서, 이동 디바이스 특징들을 식별하기 위한 수단은 소프트웨어 애플리케이션에 의해 이용된 이동 디바이스 특징들을 식별하기 위한 수단을 포함할 수도 있다. 추가의 양태에서, 애플리케이션-기반 분류기 모델을 생성하기 위한 수단은 애플리케이션-특정 분류기 모델을 생성하기 위한 수단을 포함할 수도 있다. 일 양태에서, 이동 디바이스 특징들을 식별하기 위한 수단은 이동 컴퓨팅 디바이스 상에서 실행될 수도 있는 소프트웨어 애플리케이션의 하나의 타입에 의해 이용된 이동 디바이스 특징들을 식별하기 위한 수단을 포함할 수도 있고, 애플리케이션-기반 분류기 모델을 생성하기 위한 수단은 애플리케이션-타입-특정 분류기 모델을 생성하는 것을 포함할 수도 있다.

[0025] 추가의 양태에서, 컴퓨팅 디바이스는 이동 디바이스 컴포넌트로부터 거동 정보를 수집함으로써 시간의 주기 동안에 거동을 모니터링하기 위한 수단을 포함할 수도 있다. 추가의 양태에서, 이동 컴퓨팅 디바이스의 거동을 분류하기 위하여 애플리케이션-기반 분류기 모델을 이용하기 위한 수단은 특징 벡터를 생성하기 위하여 거동 정보를 이용하기 위한 수단, 생성된 특징 벡터를 애플리케이션-기반 분류기 모델에 적용함으로써 애플리케이션-기반 분류기 모델 내에 포함된 각각의 테스트 조건을 평가하기 위한 수단, 애플리케이션-기반 분류기 모델에서 테스트 조건들을 평가하는 각각의 결과의 가중화된 평균을 연산하기 위한 수단, 및 가중화된 평균에 기초하여 거동이 악성인지 또는 양성인지 여부를 결정하기 위한 수단을 포함할 수도 있다.

[0026] 추가의 양태에서, 복수의 테스트 조건들을 식별하는 전체 분류기 모델을 수신하기 위한 수단은 복수의 테스트 조건들 중의 하나를 각각 평가하는 복수의 판단 노드들로의 변환에 적합한 정보를 포함하는 유한 상태 머신을 수신하기 위한 수단을 포함할 수도 있고, 식별된 테스트 조건들을 우선순위화하는 애플리케이션-기반 분류기 모델을 생성하기 위한 수단은 소프트웨어 애플리케이션에 관련되는 이동 디바이스 특징, 또는 소프트웨어 애플리케이션의 타입에 관련되는 이동 디바이스 특징을 평가하는 판단 노드들을 포함하기 위하여 애플리케이션-기반 분류기 모델을 생성하기 위한 수단을 포함할 수도 있다.

[0027] 추가의 양태에서, 식별된 테스트 조건들을 우선순위화하는 애플리케이션-기반 분류기 모델을 생성하기 위한 수단은 이동 디바이스 자원들의 과도한 양을 소비하지 않으면서, 거동을 분류하기 위하여 평가되어야 하는 다수의 고유한 테스트 조건들을 결정하기 위한 수단, 전체 분류기 모델에서 복수의 테스트 조건들을 순차적으로 트래버싱함으로써 테스트 조건들의 리스트를 생성하고, 테스트 조건들의 리스트가 다수의 고유한 테스트 조건들을 포함할 때까지, 소프트웨어 애플리케이션에 의해 액세스되고 이용될 수도 있는 특징들에 관련되는 그 테스트 조건들을 테스트 조건들의 리스트 내로 삽입하기 위한 수단, 및 테스트 조건들의 생성된 리스트 내에 포함된 테스트 조건들 중의 하나를 테스트하는 전체 분류기 모델에서의 판단 노드들을 포함하기 위하여 애플리케이션-기반 분류기 모델을 생성하기 위한 수단을 더 포함할 수도 있다.

[0028] 추가의 양태에서, 복수의 테스트 조건들을 식별하는 전체 분류기 모델을 수신하기 위한 수단은 유한 상태 머신을 수신하기 위한 수단을 포함할 수도 있다. 추가의 양태에서, 이동 컴퓨팅 디바이스는 유한 상태 머신을, 복수의 테스트 조건들 중의 하나를 각각 평가하는 부스팅된 판단 스텀프들로 변환하기 위한 수단, 부스팅된 판단 스텀프들에 기초하여 희박 분류기 모델들의 패밀리를 생성하기 위한 수단, 희박 분류기 모델들의 패밀리로부터 희박 분류기 모델들을 선택하기 위한 수단, 및 수집된 거동 정보를 애플리케이션-기반 분류기 모델 및 선택된 희박 분류기 모델에 병렬로 적용하기 위한 수단을 더 포함할 수도 있다.

[0029] 추가의 양태에서, 이동 디바이스 특징들을 식별하기 위한 수단은 소프트웨어 애플리케이션에 의해 이용된 이동 디바이스 특징들을 식별하기 위한 수단을 포함할 수도 있다. 추가의 양태에서, 이동 컴퓨팅 디바이스는 소프트웨어 애플리케이션의 상태, 소프트웨어 애플리케이션의 구성, 소프트웨어 애플리케이션의 동작, 및 소프트웨어 애플리케이션의 기능성 중의 하나에 있어서의 변경을 검출하기 위하여 소프트웨어 애플리케이션을 모니터링하기 위한 수단을 더 포함할 수도 있다. 추가의 양태에서, 컴퓨팅 디바이스는 변경을 검출하는 것에 응답하여 테스트 조건들의 업데이트된 세트를 포함하기 위하여 애플리케이션-기반 분류기 모델을 수정하기 위한 수단, 및 거동을 재분류하기 위하여 수정된 애플리케이션-기반 분류기 모델을 이용하기 위한 수단을 포함할 수도 있다.

도면의 간단한 설명

[0030] 본원에 편입되며 이 명세서의 일부를 구성하는 첨부한 도면들은 발명의 예시적인 양태들을 예시하고, 위에서 주어진 일반적인 설명 및 이하에서 주어진 상세한 설명과 함께, 발명의 특징들을 설명하도록 작용한다.

도 1 은 다양한 양태들과 함께 이용하는데 적합한 일 예의 통신 시스템의 네트워크 컴포넌트들을 예시하는 통신

시스템 블록도이다.

도 2 는 특정한 이동 디바이스 거동이 악성인지, 성능-열화 (performance-degrading) 인지, 의심스러운지 (suspicious), 또는 양성인지 여부를 결정하도록 구성된 일 양태의 이동 디바이스들에서 일 예의 논리적 컴포넌트들 및 정보 흐름들을 예시하는 블록도이다.

도 3 은 특정 이동 디바이스 거동이 악성인지, 성능-열화인지, 의심스러운지, 또는 양성인지 여부를 결정하기 위하여 이동 디바이스와 함께 작동하도록 구성된 네트워크 서버를 포함하는 일 양태의 시스템에서 일 예의 컴포넌트들 및 정보 흐름들을 예시하는 블록도이다.

도 4 는 데이터, 거동 벡터들, 또는 분류기 모델들을 재트레이닝 (re-train) 하지 않으면서 애플리케이션-기반 분류기 모델들을 생성하도록 구성된 이동 디바이스를 포함하는 일 양태의 시스템에서 일 예의 컴포넌트들 및 정보 흐름들을 예시하는 블록도이다.

도 5a 는 복수의 소프트웨어 애플리케이션들에 맵핑된 일 예의 분류기 모델의 예시도이다.

도 5b 는 이동 디바이스에서 국소적으로 애플리케이션-기반 분류기 모델들을 생성하는 또 다른 양태의 이동 디바이스 방법을 예시하는 프로세스 흐름도이다.

도 6 은 이동 디바이스에서 국소적으로 애플리케이션-기반 분류기 모델들을 생성하는 또 다른 양태의 이동 디바이스 방법을 예시하는 또 다른 프로세스 흐름도이다.

도 7 은 이동 디바이스에서 애플리케이션-기반 또는 희박 분류기 모델들을 생성하는 또 다른 양태의 이동 디바이스 방법을 예시하는 프로세스 흐름도이다.

도 8 은 희박 분류기 모델들을 생성하기 위하여 일 양태의 서버 프로세서에 의해 생성될 수도 있으며 이동 디바이스 프로세서에 의해 이용될 수도 있는 일 예의 부스팅된 판단 스텀프들의 예시도이다.

도 9 는 양태에 따라 동적 및 적응적 관측들을 수행하도록 구성된 관측기 모듈에서 일 예의 논리적 컴포넌트들 및 정보 흐름들을 예시하는 블록도이다.

도 10 은 또 다른 양태에 따라 관측기 데몬 (observer daemon) 들을 구현하는 컴퓨팅 시스템에서 논리적 컴포넌트들 및 정보 흐름들을 예시하는 블록도이다.

도 11 은 이동 디바이스들에 관한 적응적 관측들을 수행하기 위한 일 양태의 방법을 예시하는 프로세스 흐름도이다.

도 12 는 일 양태에서 이용하는데 적합한 이동 디바이스의 컴포넌트 블록도이다.

도 13 은 일 양태에서 이용하는데 적합한 서버 디바이스의 컴포넌트 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0031] 다양한 양태들은 첨부한 도면들을 참조하여 상세하게 설명될 것이다. 가능한 경우마다, 동일한 참조 번호들은 동일하거나 유사한 부분들을 지칭하기 위하여 도면들의 전반에 걸쳐 이용될 것이다. 특정한 예들 및 구현예들에 대해 행해진 참조들은 예시적인 목적들을 위한 것이고, 발명 또는 청구항들의 범위를 제한하도록 의도된 것은 아니다.

[0032] 개요에서, 다양한 양태들은 포괄적인 거동 모니터링 및 분석 시스템의 효율 및 성능을 개선시키고, 이동 디바이스가 소프트웨어 애플리케이션이 이동 디바이스의 바람직하지 않거나 성능 열화하는 거동의 소스 (source) 또는 원인인지 여부를 더욱 양호하게 예측하는 것을 가능하게 하기 위하여, 애플리케이션-특정 및/또는 애플리케이션-타입 특정 분류기 모델들 (즉, 데이터 또는 거동 모델들) 을 이용하는 방법들과, 방법들을 구현하도록 구성된 이동 디바이스들을 포함한다. 참조의 용이함을 위하여, 용어 "애플리케이션-기반 분류기 모델들" 은 이하에서 설명된 바와 같은 애플리케이션-특정 및 애플리케이션-타입 특정 분류기 모델들 중의 어느 하나 또는 양자를 지칭하기 위하여 본원에서, 그리고 청구항들에서 이용된다.

[0033] 포괄적인 거동 모니터링 및 분석 시스템은 시간 경과에 따라 이동 디바이스의 성능 및/또는 전력 사용 레벨들을 종종 열화시키는 조건들 및/또는 이동 디바이스 거동들을 지능적으로 그리고 효율적으로 식별하고, 분류하고, 모델링하고, 방지하고, 및/또는 정정하기 위하여 서로 함께 작동하도록 구성된 네트워크 서버 및 이동 디바이스를 포함할 수도 있다. 네트워크 서버는, 중앙 데이터베이스 (예컨대, "클라우드 (cloud)") 로부터 다양한

조건들, 특징들, 거동들, 및 정정 액션들에 대한 정보를 수신하고, 이동 디바이스에 의해 하나 이상의 희박 분류기 모델들로 신속하게 변환될 수 있는 포맷 또는 구조인 정보 (예컨대, 거동 정보) 의 대형 코퍼스를 설명하는 전체 또는 로버스트 (robust) 분류기 모델 (예컨대, 데이터/거동 모델) 을 생성하기 위하여 이 정보를 이용하도록 구성될 수도 있다. 예를 들어, 네트워크 서버는, 이동 디바이스의 특징을 각각 평가하거나 테스트하고, 희박 분류기 모델 내에 포함될 수도 있는 복수의 판단 노드들 (예컨대, 부스팅된 판단 트리들, 부스팅된 판단 스텀프들 등) 포함하기 위하여 전체 분류기 모델을 생성할 수도 있다.

[0034] 네트워크 서버는 전체 분류기를 이동 디바이스로 전송할 수도 있다. 이동 디바이스는 변동되는 레벨들의 복잡성 (또는 "희박성 (leanness)") 의 희박 분류기 모델 또는 희박 분류기 모델들의 패밀리를 생성하기 위하여 전체 분류기 모델을 수신하고 이용하도록 구성될 수도 있다. 이것을 달성하기 위하여, 이동 디바이스는, 감소된 수의 판단 노드들을 포함하고 및/또는 제한된 수의 테스트 조건들을 평가하는 희박 분류기 모델들을 생성하기 위하여 전체 분류기 모델 내에 포함된 판단 노드들을 트리밍 (trim), 컬링 (cull), 또는 프루닝 (prune) 할 수도 있다.

[0035] 게다가, 이동 디바이스는 또한, 특정 소프트웨어 애플리케이션 (Google® 지갑) 및/또는 소프트웨어 애플리케이션의 특정 타입 (예컨대, 게임들, 내비게이션, 금융, 뉴스, 생산성 등) 에 관련되는 조건들 또는 특징들을 식별하고 테스트하는 애플리케이션-특정 및/또는 애플리케이션-타입 특정 분류기 모델들을 동적으로 생성할 수도 있다. 일 양태에서, 이 애플리케이션-기반 분류기 모델들 (즉, 애플리케이션-특정 및 애플리케이션-타입 특정 분류기 모델들) 은, 수신된 전체 분류기 모델 내에 포함되는 판단 노드들, 또는 수신된 전체 분류기 모델로부터 생성된 희박 분류기 모델 내에 포함된 것들의 감소되고 더욱 포커싱된 (focused) 서브세트를 포함하기 위하여 생성될 수도 있다.

[0036] 다양한 양태들에서, 이동 디바이스는 시스템에서의 각각의 소프트웨어 애플리케이션에 대해, 및/또는 시스템에서의 소프트웨어 애플리케이션의 각각의 타입에 대해 애플리케이션-기반 분류기 모델들을 생성하도록 구성될 수도 있다. 이동 디바이스는 또한, 높은 위험이 있거나 남용하기 쉬운 소프트웨어 애플리케이션들 및/또는 애플리케이션 타입들 (예컨대, 금융 애플리케이션들, 포인트-오브-세일 (point-of-sale) 애플리케이션들, 생체인식 센서 애플리케이션들 등) 을 동적으로 식별하고, 높은 위험이 있거나 남용하기 쉬운 것으로서 식별되는 소프트웨어 애플리케이션들 및/또는 애플리케이션 타입들만을 위한 애플리케이션-기반 분류기 모델들을 생성하도록 구성될 수도 있다. 다양한 양태들에서, 이동 디바이스는 애플리케이션-기반 분류기 모델들을 동적으로, 반응적으로, 사전적으로, 및/또는 새로운 애플리케이션이 설치되거나 업데이트될 때마다 생성하도록 구성될 수도 있다.

[0037] 이동 디바이스는 실시간 거동 모니터링 및 분석 동작들을 수행하기 위하여 국소적으로 생성된 희박 및/또는 애플리케이션-기반 분류기 모델들을 이용하도록 구성될 수도 있다. 일 양태에서, 이동 디바이스는 다수의 분류기 모델들을 병렬로 이용하거나 적용하도록 구성될 수도 있다. 다양한 양태들에서, 이동 디바이스는 특정 소프트웨어 애플리케이션을 평가할 때, 동일하거나 상이한 거동/특징 벡터에 대해 더욱 일반적인 희박 분류기 모델을 이용/적용하는 것으로부터 생성된 결과들에 비해, 거동/특징 벡터에 대해 애플리케이션-기반 분류기 모델들을 이용하거나 적용하는 것으로부터 생성된 결과들에 대해 선호도 또는 우선순위를 부여하도록 구성될 수도 있다. 다양한 양태들에서, 이동 디바이스는 소프트웨어 애플리케이션, 프로세서, 또는 복잡한 이동 디바이스 거동이 양성인지, 또는 이동 디바이스의 성능 또는 전력 소비 특성들의 열화에 기여하는지 여부를 예측하기 위하여 분류기 모델들을 적용하는 결과들을 이용할 수도 있다.

[0038] 분류기 모델들이 포커싱되거나 애플리케이션-특정 또는 애플리케이션-타입-특정 특징들에 기초하도록 이동 디바이스에서 국소적으로 분류기 모델들을 동적으로 생성함으로써, 다양한 양태들은 이동 디바이스가, 특정 소프트웨어 애플리케이션의 동작들이 이동 디바이스의 바람직하지 않거나 성능 열화하는 거동에 기여하는지 여부를 결정하기 위하여 가장 중요한 작은 수의 특징들에 대해 그 모니터링 및 분석 동작들을 포커싱하도록 한다. 이것은 이동 디바이스의 성능 및 전력 소비 특성들을 개선시키고, 이동 디바이스가 이동 디바이스 자원들 (예컨대, 프로세싱, 메모리, 또는 에너지 자원들) 의 과도한 양을 소비하지 않으면서, 연속적으로 또는 거의 연속적으로 실시간 거동 모니터링 및 분석 동작들을 수행하도록 한다.

[0039] 단어 "예시적" 은 "예, 사례, 또는 예시로서 작용함" 을 의미하기 위하여 본원에서 이용된다. "예시적" 으로서 본원에서 설명된 임의의 구현예는 다른 구현예들에 비해 바람직하거나 유리한 것으로서 반드시 해석되어야 하는 것은 아니다.

[0040] 어구 "애플리케이션-기반 분류기 모델" 은 애플리케이션-특정 분류기 모델 및 애플리케이션-타입-특정 분류기

모듈의 양자를 집합적으로 그리고 대안적으로 지칭하기 위하여 본원에서 일반적으로 이용된다. 즉, 애플리케이션-기반 분류기 모델은 애플리케이션-특정 분류기 모델 또는 애플리케이션-타입-특정 분류기 모델일 수도 있다. 애플리케이션-특정 분류기 모델은, 개별적인 소프트웨어 애플리케이션을 평가하기 위하여 이용될 수도 있는 데이터, 정보 구조들 (예컨대, 특징 벡터들, 거동 벡터들, 컴포넌트 리스트들 등), 및/또는 판단 기준들을 식별하거나 포함하는 분류기 모델일 수도 있다. 애플리케이션-타입-특정 분류기 모델은 소프트웨어 애플리케이션 (예컨대, 금융 애플리케이션들, 생산성 애플리케이션들 등) 의 특정한 클래스, 범주, 또는 타입을 평가하는 것에 관련 있는 데이터, 정보 구조들, 및/또는 판단 기준들을 식별하거나 포함하는 분류기 모델일 수도 있다.

[0041] 용어들 "이동 컴퓨팅 디바이스" 및 "이동 디바이스" 는 셀룰러 전화들, 스마트폰들, 개인용 또는 이동 멀티미디어 플레이어들, 개인 정보 단말 (personal data assistant; PDA) 들, 랩톱 컴퓨터들, 태블릿 컴퓨터들, 스마트북 (smartbook) 들, 울트라북 (ultrabook) 들, 팜톱 (palm-top) 컴퓨터들, 무선 전자 메일 수신기들, 멀티미디어 인터넷 가능형 셀룰러 전화들, 무선 게임용 제어기들과, 메모리, 성능이 중요한 프로그래밍가능한 프로세서를 포함하며 전력 절감 방법들이 유익하도록 배터리 전력 하에서 동작하는 유사한 개인용 전자 디바이스들 중의 임의의 하나 또는 전부를 지칭하기 위하여 본원에서 상호 교환가능하게 이용된다. 다양한 양태들은 제한된 자원들을 가지며 배터리로 작동되는 스마트폰들과 같은 이동 컴퓨팅 디바이스들을 위해 특히 유용하지만, 양태들은 일반적으로, 프로세서를 포함하며 애플리케이션 프로그램들을 실행하는 임의의 전자 디바이스에서 유용하다.

[0042] 일반적으로, 이동 디바이스의 성능 및 전력 효율은 시간 경과에 따라 열화된다. 최근에는, 안티-바이러스 (anti-virus) 회사들 (예를 들어, McAfee, Symantec 등) 이 이 열화를 늦추는 것을 목적으로 하는 이동 안티-바이러스, 방화벽, 및 암호화 제품들을 판매하기 시작하였다. 그러나, 이 솔루션들 중의 다수는 이동 디바이스 상에서의 연산-집약적 스캐닝 엔진 (computationally-intensive scanning engine) 의 주기적 실행에 의존하고, 이것은 이동 디바이스의 프로세싱 및 배터리 자원들 중의 다수를 소비할 수도 있고, 연장된 시간 주기들 동안에 이동 디바이스를 느리게 하거나 이동 디바이스를 쓸모없게 할 수도 있고, 및/또는 이와 다르게 사용자 경험을 열화시킬 수도 있다. 게다가, 이 솔루션들은 알려진 바이러스들 및 멀웨어 (malware) 를 검출하는 것으로 전형적으로 제한되고, (예컨대, 성능 열화가 바이러스들 또는 멀웨어에 의해 야기되지 않을 때) 시간 경과에 따른 이동 디바이스의 열화에 기여하기 위하여 종종 조합되는 다수의 복잡한 인자들 및/또는 상호작용들을 다루지는 않는다. 이러한 그리고 다른 이유들로 인해, 기존의 안티-바이러스, 방화벽, 및 암호화 제품들은 시간 경과에 따른 이동 디바이스의 열화에 기여할 수도 있는 많은 인자들을 식별하거나, 이동 디바이스 열화를 방지하거나, 또는 노후화한 이동 디바이스를 그 원래의 조건으로 효율적으로 복원시키기 위한 적절한 솔루션들을 제공하지 않는다.

[0043] 현재, 컴퓨팅 디바이스 상에서 실행되는 애플리케이션 프로그램 거동을 모델링하기 위한 다양한 솔루션들이 존재하고, 이 솔루션들은 소프트웨어 애플리케이션이 악성인지 또는 양성인지 여부를 결정하기 위하여 머신 학습 기법들과 함께 이용될 수도 있다. 그러나, 이 솔루션들은 이동 디바이스들 상에서의 이용을 위해 적당하지 않은데, 이는 이들이 거동 정보의 매우 대형 코퍼스를 평가하는 것을 요구하고, 컴퓨팅 디바이스의 애플리케이션-특정 또는 애플리케이션-타입-특정 특징들을 참작하기 위하여 거동 모델들을 동적으로 생성하지 않고, 거동 모델에서 특징들을 지능적으로 우선순위화하지 않고, 개별적인 애플리케이션 프로그램 또는 프로세스를 평가하는 것으로 제한되고, 및/또는 이동 디바이스에서 연산-집약적 프로세스들의 실행을 요구하기 때문이다. 이와 같이, 이동 디바이스에서 이 기존의 솔루션들을 구현하거나 수행하는 것은 이동 디바이스의 응답성, 성능, 또는 전력 소비 특성들에 상당히 부정적 및/또는 사용자-지각가능한 영향을 가질 수도 있다.

[0044] 예를 들어, 컴퓨팅 디바이스는 트레이닝 데이터의 대형 코퍼스를 액세스 및 이용하고, 특징 벡터를 입력으로서 취하는 모델을 유도하고, 컴퓨팅 디바이스의 소프트웨어 애플리케이션이 악성인지 또는 양성인지 여부를 결정하기 위해 이 모델을 이용하기 위하여 기존의 머신 학습-기반 솔루션을 이용하도록 구성될 수도 있다. 그러나, 이러한 솔루션은 희박 분류기 모델을 신속하게 생성하기 위하여 이동 디바이스에 의해 이용될 수도 있는 포맷 또는 정보 구조 (예컨대, 유한 상태 머신 등) 인 거동 정보의 대형 코퍼스를 설명하는 전체 분류기 모델 (즉, 로버스트 데이터 또는 거동 모델) 을 생성하지 않는다. 적어도 이 이유 때문에, 이러한 솔루션은 이동 디바이스가 개별적인 애플리케이션 또는 애플리케이션 타입에 특정적인 조건들 또는 특징들에 포커싱하거나 이러한 조건들 또는 특징들을 우선순위화하는 판단 노드들을 포함하는 희박 분류기 모델을 생성하도록 하지 않는다. 게다가, 이 솔루션은 이동 디바이스가, 특정 거동, 소프트웨어 애플리케이션, 또는 모델이 이용되는 특정 이동 디바이스에서의 소프트웨어 애플리케이션 타입을 분류하는 것에 대한 그 관련성에 따라 특징들을

지능적으로 식별하거나 우선순위화하는 희박 분류기 모델을 생성하도록 하지 않는다. 이러한 그리고 다른 이유들 때문에, 이러한 솔루션은 소프트웨어 애플리케이션을, 이동 디바이스의 응답성, 성능, 또는 전력 소비 특성들에 상당히 부정적인 또는 사용자-지각가능한 영향을 가지는 복잡한 이동 디바이스 거동에 기여하는 것으로서 신속하고 효율적으로 식별하거나, 분석하거나, 분류하기 위하여 이동 디바이스 프로세서에 의해 이용될 수 없다.

[0045] 기존의 솔루션들의 상기 언급된 제한들에 추가하여, 많은 거동 모델링 솔루션들은 컴퓨팅 디바이스의 거동들을 모델링하는 것에 대한 "일률적인 (one-size-fits-all)" 접근법을 구현한다. 즉, 이 솔루션들은, 거동 모델들이 일반적이며 많은 컴퓨팅 디바이스들에서, 및/또는 다양한 상이한 하드웨어 및 소프트웨어 구성들과 함께 이용될 수도 있도록 거동 모델들을 전형적으로 생성한다. 이와 같이, 이 일반적인 거동 모델들은 매우 많은 수의 특징들을 종종 포함/테스트하고, 이 특징들의 많은 것은 특정 소프트웨어 애플리케이션의 거동, 또는 이들이 실제적으로 이용되는 특정 컴퓨팅 디바이스에서의 애플리케이션 타입을 식별하거나, 분석하거나, 분류하는 것에 관련되지 않는다 (그리고, 이에 따라 이를 위해 이용될 수 없음). 게다가, 이 솔루션들은 모델이 이용되는 특정 이동 디바이스에서의 특정 거동을 분류하는 것에 대한 그 관련성에 기초하여 상대적인 우선순위들을 특징들에 배정하지 않는다. 그러므로, 이 솔루션들은 컴퓨팅 디바이스가 많은 수의 오조직 (disorganize) 되거나, 부적당하게 우선순위화되거나, 또는 무관한 특징들을 포함하는 거동 모델들을 적용할 것을 전형적으로 요구한다. 이러한 모델들은 이동 디바이스 프로세서로 하여금, 시간 경과에 따른 이동 디바이스의 열화의 원인 또는 소스를 식별하기 위해 유용하지 않은 많은 수의 특징들을 분석하게 할 수도 있기 때문에, 이러한 모델들은 자원-제약된 이동 디바이스들에서의 이용을 위해 적당하지 않다. 이와 같이, 이 기존의 솔루션들은 아직 복잡한 자원-제약된 이동 디바이스들에서의 이용을 위해 적당하지 않다.

[0046] 최신 이동 디바이스들은 고도로 구성가능하고 복잡한 시스템들이다. 이와 같이, 특정한 이동 디바이스 거동이 양성인지 또는 양성이 아닌지 (예컨대, 악성 또는 성능-열화) 여부를 결정하기 위하여 가장 중요한 특징들은 각각의 이동 디바이스에서 상이할 수도 있다. 또한, 특징들의 상이한 조합은 그 이동 디바이스가 특정한 거동이 양성인지 또는 양성이 아닌지 여부를 신속하고 효율적으로 결정하도록 하기 위하여, 각각의 이동 디바이스에서 모니터링 및/또는 분석을 요구할 수도 있다. 그렇지만, 모니터링 및 분석을 요구하는 특징들의 정확한 조합과, 각각의 특징 또는 특징 조합의 상대적인 우선순위 또는 중요도는 거동이 모니터링되거나 분석되어야 하는 특정 이동 디바이스로부터 획득된 애플리케이션-특정, 애플리케이션-타입 특정, 및/또는 디바이스-특정 정보를 이용하여 종종 결정되기만 할 수 있다. 이러한 그리고 다른 이유들 때문에, 거동 모델들이 이용되는 특정 디바이스 이외의 임의의 컴퓨팅 디바이스에서 생성된 거동 모델들은 그 디바이스에서의 소프트웨어 애플리케이션 또는 이동 디바이스 거동을 분류하기 위해 가장 중요한 특징들의 정밀한 조합을 식별하는 정보를 포함할 수 없다.

[0047] 예를 들어, 제 1 이동 디바이스가 금융 거래들을 인가 (authorize) 하기 위하여 그 생체인식 센서들 (예컨대, 지문 판독기, 음성 인식 서브시스템, 홍채 스캐너 등) 을 이용하도록 구성될 경우, 생체인식 센서들의 액세스 및 이용에 관한 조건들을 테스트하는 특징들은 금융 소프트웨어를 액세스하는 관측된 거동이 그 이동 디바이스에서 악성인지 또는 양성인지 여부를 결정하는 것에 관련될 가능성이 있다. 예를 들어, 제 1 이동 디바이스에서의 생체인식 센서들의 액세스 및 이용은 악성 애플리케이션이 사용자의 지식 또는 동의 없이 금융 거래를 인가하고 있음을 표시할 수도 있다. 다른 한편으로, 이 센서들의 액세스 및 이용에 관한 조건들을 테스트하는 특징들은 금융 소프트웨어를 액세스하는 관측된 거동이 금융 거래들을 인가하기 위하여 그 생체인식 센서들을 이용하도록 구성되지 않은 제 2 이동 디바이스에서 악성인지 또는 양성인지 여부를 결정하는 것에 관련될 가능성이 없다. 즉, 제 1 및 제 2 디바이스들은 그 생체인식 센서들의 이용을 위한 그 구성을 제외하고는 모든 양태들에서 동일 (즉, 동일한 타입, 모델, 오퍼레이팅 시스템 (operating system), 소프트웨어 등임) 할 수도 있으므로, 양자의 디바이스들을 위한 생체인식 센서들의 액세스 및 이용에 관한 조건들을 평가하는 특징들을 정확하게 식별하는 일반적인 거동 모델을 생성하는 것은 도전적일 것이다. 수 십만 (또는 수 백만) 개의 유사한 장비이지만 독립적으로 구성가능한 이동 디바이스들 상에서 훨씬 더 복잡한 조건들 또는 특징들을 테스트하는 일반적인 모델을 생성하는 것은 훨씬 더 도전적일 것이다.

[0048] 게다가, 이동 디바이스들은 상대적으로 제한된 프로세싱, 메모리, 및 에너지 자원들을 가지는 자원 제약된 시스템들이다. 최신 이동 디바이스들은 또한, 시간 경과에 따라 이동 디바이스의 성능 및 전력 사용 레벨들에 있어서의 열화에 기여할 수도 있는 여러 다양한 인자들을 가지는 복잡한 시스템들이다. 성능 열화에 기여할 수도 있는 인자들의 예들은 열악하게 설계된 소프트웨어 애플리케이션들, 멀웨어, 바이러스들, 프래그먼트화된 메모리 (fragmented memory), 및 배경 프로세스들을 포함한다. 이 인자들의 수, 다양성, 및 복잡성으로 인

해, 최신 이동 디바이스들의 복잡하지만 자원-제약된 시스템들의 성능 및/또는 전력 사용 레벨들을 열화시킬 수도 있는 다양한 컴포넌트들, 거동들, 프로세스들, 동작들, 조건들, 상태들, 또는 특징들 (또는 그 조합들) 의 전부를 평가하는 것은 종종 실현가능하지 않다. 이와 같이, 사용자들, 오퍼레이팅 시스템들, 또는 애플리케이션 프로그램들 (예컨대, 안티-바이러스 소프트웨어 등) 은 이러한 문제들의 근원들을 정확하고 효율적으로 식별하는 것이 어렵다. 그 결과, 이동 디바이스 사용자들은 시간 경과에 따른 이동 디바이스의 성능 및 전력 사용 레벨들에서의 열화를 방지하거나, 노후화한 이동 디바이스를 그 원래의 성능 및 전력 사용 레벨들로 복원시키기 위한 몇몇 방안들을 현재 가지고 있다.

[0049] 다양한 양태들은 시간 경과에 따라 이동 디바이스의 성능 및/또는 전력 사용 레벨들을 종종 열화시키는 조건들, 인자들, 및/또는 이동 디바이스 거동들을 지능적으로 그리고 효율적으로 식별하고, 방지하고, 및/또는 정정하기 위한 포괄적인 거동 모니터링 및 분석 시스템을 포함한다. 일 양태에서, 이동 디바이스의 관측기 프로세스, 데몬, 모듈, 또는 서브-시스템 (본원에서는 집합적으로 "모듈" 로서 지칭됨) 은 이동 디바이스 시스템의 다양한 레벨들에서 다양한 애플리케이션 프로그래밍 인터페이스 (application programming interface; API) 들, 레지스터 (register) 들, 카운터들, 또는 다른 이동 디바이스 컴포넌트들 (본원에서 집합적으로 "장치화된 컴포넌트들") 을 구현하거나 조직화할 수도 있다. 관측기 모듈은 장치화된 컴포넌트로부터 거동 정보를 수집함으로써 이동 디바이스 거동들을 연속적으로 (또는 거의 연속적으로) 모니터링할 수도 있다. 이동 디바이스는 분석기 모듈을 또한 포함할 수도 있고, 관측기 모듈은 (예컨대, 메모리 기록 동작, 함수 호출 등을 통해) 수집된 거동 정보를 분석기 모듈로 통신할 수도 있다. 분석기 모듈은, 특징 또는 거동 벡터들을 생성하고, 특징/거동 벡터들에 기초하여 공간적 및/또는 시간적 상관들을 생성하고, 특정한 이동 디바이스 거동, 조건, 서브-시스템, 소프트웨어 애플리케이션, 또는 프로세스가 양성인지, 의심스러운지, 또는 양성이 아닌지 (즉, 악성 또는 성능-열화) 여부를 결정하기 위해 이 정보를 이용하기 위하여 거동 정보를 수신하고 이용할 수도 있다. 다음으로, 이동 디바이스는 식별된 문제들을 치유하거나, 고치거나, 격리시키거나, 또는 이와 다르게 해결 또는 응답하기 위하여 이 분석의 결과들을 이용할 수도 있다.

[0050] 분석기 모듈은 또한, 소프트웨어 애플리케이션 또는 이동 디바이스 거동이 양성인지 또는 양성이 아닌지 (예컨대, 악성 또는 성능-열화) 여부를 결정하기 위하여 데이터, 알고리즘들, 분류기들, 또는 모델들 (본원에서는 "분류기 모델들" 로서 집합적으로 지칭됨) 을 수집된 거동 정보에 대해 수행하는 것, 실행하는 것, 및/또는 적용하는 것을 포함할 수도 있는 실시간 거동 분석 동작들을 수행하도록 구성될 수도 있다. 각각의 분류기 모델은 이동 디바이스의 거동의 특정 특징 또는 양태를 평가하기 위하여 이동 디바이스 프로세서에 의해 이용될 수도 있는 데이터 및/또는 정보 구조들 (예컨대, 특징 벡터들, 거동 벡터들, 컴포넌트 리스트들 등) 을 포함하는 거동 모델일 수도 있다. 각각의 분류기 모델은 또한, 이동 디바이스에서 다수의 특징들, 인자들, 데이터 포인트들, 엔트리들, API 들, 상태들, 조건들, 거동들, 애플리케이션들, 프로세스들, 동작들, 컴포넌트들 등 (본원에서 집합적으로 "특징들") 을 모니터링하기 위한 판단 기준들을 포함할 수도 있다. 분류기 모델들은 이동 디바이스 상에서 사전설치될 수도 있거나, 네트워크 서버로부터 다운로딩되거나 수신될 수도 있거나, 이동 디바이스에서 생성될 수도 있거나, 그 임의의 조합일 수도 있다. 분류기 모델들은 크라우드 소싱 (crowd sourcing) 솔루션들, 거동 모델링 기법들, 머신 학습 알고리즘들 등을 이용함으로써 생성될 수도 있다.

[0051] 각각의 분류기 모델은 전체 분류기 모델 또는 희박 분류기 모델로서 범주화될 수도 있다. 전체 분류기 모델은 수 천 개의 특징들 및 수 백만 개의 엔트리들을 포함할 수도 있는 대형 트레이닝 데이터세트의 함수로서 생성되는 로버스트 데이터 모델일 수도 있다. 희박 분류기 모델은 특정한 이동 디바이스 거동이 양성인지 또는 양성이 아닌지 (예컨대, 악성 또는 성능-열화) 여부를 결정하기 위하여 가장 관련되는 특징들/엔트리들에 대한 테스트들을 포함하거나 우선순위화하는 감소된 데이터세트로부터 생성되는 더욱 포커싱된 데이터 모델일 수도 있다.

[0052] 국소적으로 생성된 희박 분류기 모델은 이동 디바이스에서 생성되는 희박 분류기 모델이다. 애플리케이션-기반 분류기 모델은 애플리케이션 특정 분류기 모델 또는 애플리케이션-타입-특정 분류기 모델일 수도 있다. 애플리케이션 특정 분류기 모델은 특정한 소프트웨어 애플리케이션이 양성인지 또는 양성이 아닌지 (예컨대, 악성 또는 성능-열화) 여부를 결정하기 위하여 가장 관련되는 특징들/엔트리들에 대한 테스트들을 포함하거나 우선순위화하는 포커싱된 데이터 모델을 포함하는 분류기 모델이다. 애플리케이션-타입 특정 분류기 모델은 소프트웨어 애플리케이션의 특정한 타입이 양성인지 또는 양성이 아닌지 (예컨대, 악성 또는 성능-열화) 여부를 결정하기 위하여 가장 관련되는 특징들/엔트리들에 대한 테스트들을 포함하거나 우선순위화하는 포커싱되거나 우선순위화된 데이터 모델을 포함하는 분류기 모델이다.

[0053] 위에서 언급된 바와 같이, 이동 디바이스의 열화의 원인 또는 소스를 적당하게 식별하기 위한 분석을 요구하는

수 천 개의 특징들/인자들 및 수 백만 개의 데이터 포인트들이 있을 수도 있다. 그러므로, 분류기 모델들은 이동 디바이스들의 모든 제품들 및 모델들을 지원하기 위하여, 그리고 각각의 이동 디바이스가 특정한 이동 디바이스 거동이 양성인지 또는 양성이 아닌지 (예컨대, 악성 또는 성능-열화) 여부에 관한 정확한 판단들을 행하기 위하여, 매우 많은 수의 특징들에 대해 트레이닝될 수도 있다. 그렇지만, 이동 디바이스들은 자원 제약된 시스템들이므로, 이동 디바이스가 모든 이러한 특징들을 평가하는 것이 종종 실현가능하지 않다. 또한, 이동 디바이스들은 많은 상이한 구성들 및 다양성들로 제공되고, 많은 수의 상이한 소프트웨어 애플리케이션들 또는 애플리케이션 타입들을 포함할 수도 있다. 그렇지만, 약간의 이동 디바이스들은 (만약 있다면) 전체 분류기 모델들에서 어드레싱될 수도 있는 모든 특징 또는 기능성을 포함한다. 다양한 양태들은, 분석기 모듈이 특정 이동 디바이스의 소프트웨어 애플리케이션들에 가장 관련되는 특징들의 타겟화된 서브세트를 평가하기 위하여 적용할 수도 있는 희박 애플리케이션-기반 분류기 모델들을 생성하여, 이동 디바이스 거동을 분류할 때에 일반적인 또는 전체 분류기 모델이 이용되었을 경우에 이와 다르게 수행될 테스트 조건들 및 분석들의 수를 제한한다.

[0054] 다양한 양태들은 이동 디바이스 거동이 양성인지 또는 양성이 아닌지 (예컨대, 악성 또는 성능-열화) 여부를 결정하는 것에 가장 관련되는 특징들, 인자들, 및 데이터 포인트들을 지능적으로 그리고 효율적으로 식별하기 위하여 서로 함께 작동하도록 구성된 이동 디바이스들 및 네트워크 서버들을 포함한다. 디바이스-특정 특징들 및/또는 디바이스-상태-특정 특징들을 참조하여 이동 디바이스에서 국소적으로 희박 분류기 모델들을 생성함으로써, 다양한 양태들은 이동 디바이스 프로세서가, 이동 디바이스의 응답성, 성능, 또는 전력 소비 특성들에서의 상당히 부정적인 또는 사용자-지각각능한 변경을 야기시키지 않으면서, (예컨대, 관측기 및 분석기 모듈들 등을 통해) 복잡한 이동 디바이스 거동을 신속하고 효율적으로 식별하거나, 분석하거나, 또는 분류하기 위하여 포커싱된 분류기 모델들을 적용하도록 한다.

[0055] 전체 분류기 모델은 클라우드 서비스/네트워크로부터, 이동 디바이스 거동들 및 상태들, 특징들, 및 그 거동들 동안의, 또는 그 거동들을 특징화하는 조건들에 관한 다량의 정보를 수신하도록 구성된 네트워크 서버에 의해 생성될 수도 있다. 이 정보는 이동 디바이스 거동 벡터들의 매우 대형 클라우드 코퍼스의 형태로 되어 있을 수도 있다. 네트워크 서버는 거동 벡터들의 매우 대형 클라우드 코퍼스를 정확하게 설명하는 전체 분류기 모델 (즉, 로버스트 데이터/거동 모델) 을 생성하기 위하여 이 정보를 이용할 수도 있다. 네트워크 서버는 이동 디바이스들의 다수의 상이한 제품들, 모델들, 및 구성들 중의 임의의 것의 시간 경과에 따른 열화에 기여할 수 있는 특징들, 데이터 포인트들, 및/또는 인자들의 전부 또는 대부분을 포함하기 위하여 전체 분류기 모델을 생성할 수도 있다.

[0056] 일 양태에서, 네트워크 서버는, 이동 디바이스 프로세서에서의 이용 또는 실행에 적합한 희박 분류기 모델들로 신속하고 효율적으로 컬링되거나, 수정되거나, 변환될 수 있는 부스팅된 판단 트리/스텀프 또는 부스팅된 판단 트리들/스텀프들의 패밀리를 포함하는 정보 구조일 수도 있는 유한 상태 머신 표현 또는 표시를 포함하기 위하여 전체 분류기 모델을 생성할 수도 있다. 유한 상태 머신 표현 또는 표시 ("유한 상태 머신" 으로 축약됨) 은 테스트 조건들, 상태 정보, 상태-천이 (state-transition) 규칙들, 및 다른 유사한 정보를 포함하는 정보일 수도 있다. 일 양태에서, 유한 상태 머신은 이동 디바이스 거동의 특징, 조건, 또는 양태를 각각 평가하거나 테스트하는 부스팅된 판단 스텀프들의 대형 또는 로버스트 패밀리를 포함하는 정보 구조일 수도 있다.

[0057] 이동 디바이스는, 네트워크 서버로부터 전체 분류기 모델을 수신하고, 이동 디바이스의 특징들 및 기능성들에 대해 특정적인 희박 분류기 모델들 (즉, 데이터/거동 모델들) 을 생성하기 위하여 수신된 전체 분류기 모델을 이용하도록 구성될 수도 있다.

[0058] 다양한 양태들에서, 이동 디바이스는, 희박 분류기 모델들이 이동 디바이스의 디바이스-특정 및/또는 디바이스-상태-특정 특징들 (예컨대, 이동 디바이스 구성, 기능성, 접속된/포함된 하드웨어 등에 관련된 특징들) 을 참작하도록 희박 분류기 모델들을 지능적으로 그리고 동적으로 생성하기 위하여, 시간 경과에 따른 이동 디바이스의 열화의 원인 또는 소스를 식별하기 위하여 중요한 것으로 결정되는 특징들의 포커싱된 그리고 타겟화된 서브세트를 포함하거나, 테스트하거나, 또는 평가하기 위하여, 및/또는 특징들이 이용/평가되는 특정 이동 디바이스에서의 거동을 성공적으로 분류하기 위한 그 상대적인 중요도를 식별하는 확률 또는 신뢰성 값들에 기초하여 특징들의 타겟화된 서브세트를 우선순위화하기 위하여, 거동 모델링 및 머신 학습 기법들을 이용할 수도 있다.

[0059] 모델들이 이용되는 이동 디바이스에서 분류기 모델들을 생성함으로써, 다양한 양태들은 이동 디바이스가, 그 특정 이동 디바이스 상에서의 거동이 양성인지, 또는 성능에 있어서의 그 디바이스 열화에 기여하는지 여부를 결정함에 있어서 가장 중요한 특정 특징들을 정확하게 식별하도록 한다. 이 양태들은 또한, 이동 디바이스가

그 특정 이동 디바이스에서의 거동들을 분류하는 것에 대한 그 상대적인 중요도에 따라 희박 분류기 모델들에서 특징들을 정확하게 우선순위화하도록 한다.

[0060] 애플리케이션-특정, 애플리케이션-타입 특정, 디바이스-특정 및/또는 디바이스-상태-특정 정보의 이용은 이동 디바이스가 희박 분류기 모델들 내에 포함되어야 하는 특징들을 신속하게 식별하고 우선순위화할 뿐만 아니라, 희박 분류기 모델들로부터 제외되어야 하는 특징들을 식별하도록 한다. 예를 들어, 이동 디바이스는, 그 특정 특징 세트에 기초하여 이동 디바이스 상에서 실행되는 소프트웨어 애플리케이션에 속하지 않고, 그러므로, 이동 디바이스에 관련되지 않는 조건들을 테스트하는 전체 모델 내에 포함된 특징들/노드들/트리들/스텀프들을 식별하고 희박 분류기 모델들로부터 이러한 특징들/노드들/트리들/스텀프들을 제외하도록 구성될 수도 있다. 예를 들어, 생체인식 센서를 포함하지 않는 이동 디바이스는 소프트웨어 애플리케이션에 의해 생체인식 센서의 이용에 관한 조건들을 테스트하거나 평가하는 모든 특징들/노드들/스텀프들을 희박 분류기 모델들로부터 제외할 수도 있다.

[0061] 또한, 희박 분류기 모델들은 평가되어야 하는 (즉, 전체 분류기 모델과 비교되는) 상태들, 특징들, 거동들, 또는 조건들의 감소된 서브세트를 포함하므로, 관측기 및/또는 분석기 모듈들은 이동 디바이스의 과도한 양의 프로세싱, 메모리, 또는 에너지 자원들을 소비하지 않으면서, 이동 디바이스 거동이 양성인지 또는 양성이 아닌지 (예컨대, 악성 또는 성능-열화) 여부를 신속하고 정확하게 결정하기 위하여 희박 분류기 모델을 이용할 수도 있다.

[0062] 일 양태에서, 이동 디바이스는 변동되는 레벨들의 복잡성 (또는 "희박성") 의 희박 분류기 모델들의 패밀리를 생성하기 위하여 전체 분류기 모델을 이용하도록 구성될 수도 있다. 희박 분류기 모델들의 가장 희박한 패밀리 (즉, 가장 적은 수의 테스트 조건들에 기초한 희박 분류기 모델) 는, 모델이 양성 또는 악성의 어느 하나로서 범주화할 수 없는 거동이 조우 (encounter) 될 때까지 일상적으로 적용될 수도 있고, 이때, 더욱 로버스트 (즉, 덜 희박한) 희박 분류기 모델은 거동을 양성 또는 악성의 어느 하나로서 범주화하기 위한 시도로 적용될 수도 있다. 생성된 희박 분류기 모델들의 패밀리 내의 훨씬 더 로버스트 희박 분류기 모델의 애플리케이션은 거동의 확정적인 분류가 달성될 때까지 적용될 수도 있다. 이러한 방식으로, 관측기 및/또는 분석기 모듈들은, 가장 완전하지만, 자원-집약적 희박 분류기 모델들의 이용을, 거동을 확정적으로 분류하기 위하여 로버스트 분류기 모델이 필요하게 되는 그러한 상황들로 제한함으로써, 효율성과 정확성 사이의 균형을 유지할 수 있다.

[0063] 다양한 양태들에서, 이동 디바이스는, 유한 상태 머신 표시/표현을 부스팅된 판단 스텀프들로 변환함으로써, 전체 분류기 모델 내에 포함된 부스팅된 판단 스텀프들의 서브세트 또는 서브세트들을 포함하기 위하여 특정한 애플리케이션 또는 애플리케이션의 타입, 특징들, 거동들, 조건들, 또는 구성들에 특정적인 애플리케이션 상태들에 기초하여 부스팅된 판단 스텀프들의 전체 세트를 프루닝하거나 컬링함으로써, 그리고 이동 디바이스 거동을 지능적으로 모니터링하고, 분석하고, 및/또는 분류하기 위하여 부스팅된 판단 스텀프들의 서브세트 또는 서브세트들을 이용함으로써, 하나 이상의 희박 분류기 모델들을 생성하도록 구성될 수도 있다.

[0064] 부스팅된 판단 스텀프들의 이용은 관측기 및/또는 분석기 모듈들이 데이터를 재트레이닝하기 위하여 클라우드 또는 네트워크와 통신하지 않으면서, 희박 데이터 모델들을 생성하고 적용하도록 하고, 이것은 네트워크 서버 및 클라우드에 대한 이동 디바이스의 종속성을 상당히 감소시킨다. 이것은 이동 디바이스와 네트워크 서버 사이의 피드백 통신들을 제거하고, 이것은 이동 디바이스의 성능 및 전력 소비를 추가로 개선시킨다.

[0065] 부스팅된 판단 스텀프들은, 정확하게 하나의 노드 (그리고 이에 따라, 하나의 테스트 질문 또는 테스트 조건) 및 가중 값을 가지는 1 레벨 판단 트리들이고, 이에 따라, 데이터/거동들의 이진 분류 (binary classification) 에서의 이용을 위해 양호하게 적합하다. 즉, 거동 벡터를 부스팅된 판단 스텀프에 적용하는 것은 이진 답변 (예컨대, 예 또는 아니오) 으로 귀착된다. 예를 들어, 부스팅된 판단 스텀프에 의해 테스팅된 질문/조건이 "단문 서비스 (Short Message Service; SMS) 송신들의 빈도가 분 당 x 미만인가" 일 경우, "3" 의 값을 부스팅된 판단 스텀프에 적용하는 것은 ("3 미만" SMS 송신들에 대해) "예" 답변, 또는 ("3 이상" SMS 송신들에 대해) "아니오" 답변의 어느 하나로 귀착될 것이다.

[0066] 부스팅된 판단 스텀프들은 이들이 매우 간단하고 원시적이기 때문에 (그리고 이에 따라, 상당한 프로세싱 자원들을 요구하지 않음) 효율적이다. 부스팅된 판단 스텀프들은 또한 매우 병렬화가능하고, 이에 따라, 많은 스텀프들은 (예컨대, 이동 디바이스에서의 다수의 코어들 또는 프로세서들에 의해) 병렬로/동시에 적용되거나 테스팅될 수도 있다.

[0067] 이하에서 설명된 바와 같이, 네트워크 서버 (또는 또 다른 컴퓨팅 디바이스) 는 부스팅된 판단 트리 모델과 같이, 이동 디바이스 거동들의 또 다른 더욱 복잡한 모델로부터의 부스팅된 판단 스텀프-타입 전체 분류기 모델을 생성할 수도 있다. 이러한 복잡한 모델들은 복잡한 분류 시스템에서 이동 디바이스 거동을 특징화하는 디바이스 상태들, 동작들, 및 모니터링된 노드들 사이에서 상호작용들의 전체 (또는 거의 전체) 세트를 상관시킬 수도 있다. 위에서 언급된 바와 같이, 서버 또는 다른 컴퓨팅 디바이스는 많은 수의 이동 디바이스들로부터 수집된 이동 디바이스들의 거동 벡터들의 클라우드 코퍼스를 설명하는 모델들을 생성하기 위하여 머신 학습 기법들을 적용함으로써, 전체의 복잡한 분류기 모델을 생성할 수도 있다. 예로서, 부스팅된 판단 트리 분류기 모델은 현재의 이동 디바이스 거동이 악성인지 또는 양성인지 여부의 결정에 도달하기 위하여 테스팅가능한 조건들의 판단 노드들을 통해 수 백 개의 경로들을 추적할 수도 있다. 이러한 복잡한 모델들은 다수의 알려진 학습 및 상관 모델링 기법들을 이용하여 서버에서 생성될 수도 있다. 이러한 복잡한 모델들은 많은 수 백 개의 이동 디바이스들로부터의 데이터로부터 학습함으로써 악성 거동들을 정확하게 인식함에 있어서 상당히 효과적으로 될 수 있지만, 특정한 이동 디바이스의 구성 및 거동들에 대한 그 적용은 특히, 모델이 복잡한 멀티레벨 판단 트리들을 수반할 경우에 상당한 프로세싱을 요구할 수도 있다. 이동 디바이스들은 전형적으로 자원 제한되므로, 이러한 모델들을 이용하는 것은 디바이스 성능 및 배터리 수명에 영향을 줄 수도 있다.

[0068] 이동 디바이스들에 의한 이용에 더욱 도움이 되는 로버스트 분류기 모델들을 만들기 위하여, 서버 (예컨대, 클라우드 서버 또는 네트워크 서버) 또는 또 다른 컴퓨팅 디바이스 (예컨대, 이동 디바이스 또는 이동 디바이스에 결합할 컴퓨터) 는 복잡한 분류기 모델들을 대형의 부스팅된 판단 스텀프 모델들로 변환할 수도 있다. 판단 스텀프들 내에 수반된 더욱 간단한 결정들과, 병렬 프로세스들에서 이러한 분류기 모델들을 적용하기 위한 능력은 이동 디바이스들이 네트워크 서버에 의해 수행된 분석들로부터 더욱 양호하게 이익을 얻는 것을 가능하게 할 수도 있다. 또한, 이하에서 논의된 바와 같이, 부스팅된 판단 스텀프 전체 분류기 모델은 디바이스-특정 또는 디바이스-상태-특정 정보에 기초하여 특징들을 포함 (또는 제외) 하기 위해 희박 분류기 모델을 생성하기 위하여, 이동 디바이스들에 의해 이용될 수도 있다. 이것은 이하에서 설명된 양태의 방법들을 수행하도록 이동 디바이스 프로세서를 구성함으로써 달성될 수도 있다.

[0069] 추가의 양태들에서, 이동 디바이스는 이동 디바이스 또는 이동 디바이스의 현재의 상태에 특정적인 특징들을, 이동 디바이스 상에서 악성 거동을 검출하기 위하여 이용된 희박 분류기 모델 또는 희박 분류기 모델들의 세트 내로 편입하도록 구성된 다양한 컴포넌트들을 포함할 수도 있다.

[0070] 일 양태에서, 이동 디바이스는 이동 디바이스 구성, 기능성, 및 접속된/포함된 하드웨어에 관련된 특징들에 대응하는 분류기 기준들을 우선순위화하는 전체 분류기 모델 내에 포함된 분류기 기준들의 서브세트를 포함하기 위하여 희박 분류기 모델을 생성하도록 구성될 수도 있다. 이동 디바이스는 디바이스에 존재하거나 관련된 그 특징들 및 기능들을 우선적으로 또는 배타적으로 모니터링하기 위하여 이 희박 분류기 모델(들)을 이용할 수도 있다. 다음으로, 이동 디바이스는 이동 디바이스의 현재의 상태 및 구성에 기초하여 다양한 특징들 및 대응하는 분류기 기준들을 포함하거나 제거하기 위하여 희박 분류기 모델(들)을 주기적으로 수정하거나 재생성할 수도 있다.

[0071] 예로서, 그리고 일 양태에서, 이동 디바이스 상에서 동작하는 거동 분석기 모듈은 거동 모델들의 전체 특징 세트와 연관된 판단 스텀프들을 갖는 대형의 부스팅된 판단 스텀프들 분류기 모델을 수신할 수도 있고, 거동 분석기 모듈은 이동 디바이스의 현재의 구성, 기능성, 동작 상태, 및/또는 접속된/포함된 하드웨어와 관련되는 대형 분류기 모델(들)로부터 특징들을 선택하거나 우선순위화함으로써, 그리고 선택된 특징들에 대응하는 부스팅된 판단 스텀프들의 서브세트를 희박 분류기 모델 내에 포함함으로써, 대형 분류기 모델들로부터 하나 이상의 희박 분류기 모델들을 유도할 수도 있다. 이 양태에서, 이동 디바이스에 관련된 특징들에 대응하는 분류기 기준들은 선택된 특징들 중의 적어도 하나를 테스트하는 대형 분류기 모델 내에 포함된 그 부스팅된 판단 스텀프들일 수도 있다. 일 양태에서, 다음으로, 거동 분석기 모듈은 희박 분류기 모델이 디바이스-특정 특징 부스팅된 판단 스텀프들을 포함하는 것을 계속하도록, 이동 디바이스의 현재의 상태 및 구성에 기초하여 다양한 특징들을 포함하거나 제거하기 위하여 부스팅된 판단 스텀프들 희박 분류기 모델(들)을 주기적으로 수정하거나 재생성할 수도 있다.

[0072] 일 양태에서, 이동 컴퓨팅 디바이스 상에서 동작하는 디바이스 상태 모니터링 엔진은 이동 디바이스의 구성 및/또는 상태에서의 변경들에 대해 이동 디바이스를 계속적으로 모니터링할 수도 있다. 추가의 양태에서, 디바이스 상태 모니터링 엔진은 악성 거동을 검출하기 위하여 거동 분석기 모듈 (또는 분류기 모듈) 의 성능 또는 유효성에 영향을 줄 수도 있는 구성 및/또는 상태 변경들을 찾을 수도 있다. 예를 들어, 디바이스 상태 모니터링 엔진은 "로우 배터리 상태" 가 검출될 때까지 이동 디바이스의 거동들을 모니터링할 수도 있고, 이때,

거동 분석기 모듈은 에너지를 절감하기 위하여 악성 거동에 대하여 이동 디바이스 상의 더 적은 특징들을 분석하기 위하여 희박 분류기 모델을 변경할 수도 있다.

[0073] 또 다른 양태에서, 디바이스 상태 모니터링 엔진은 디바이스 상태 모니터링 엔진이 상태 변경을 언제 검출하는지를 디바이스 상태 특정 특징 생성기에 통지할 수도 있고, 디바이스 상태 특정 특징 생성기는 이동 디바이스의 상태 변경에 기초하여 어떤 특징들을 추가하거나 제거할 것을 거동 분석기 모듈에 시그널링할 수도 있다.

[0074] 또 다른 양태에서, 이동 디바이스는 이동 디바이스 자체에 관련된 특징들을 결정하도록 구성된 디바이스 특정 특징 생성기를 포함할 수도 있다. 예를 들어, 디바이스-특정 특징 생성기는 이동 디바이스가 근접장 (near-field) 통신, Wi-Fi, 및 Bluetooth® 기능들을 포함하는 것으로 결정할 수도 있다. 추가의 양태에서, 디바이스-특정 특징 생성기는 이동 디바이스 자체에 관련된 특징들에 기초하여 희박 분류기 모델들에서 특징들을 포함하거나 제거할 것을 거동 분석기에 시그널링할 수도 있다. 이에 따라, 이동 디바이스 상의 다양한 컴포넌트들은 이동 디바이스의 구성 및/또는 이동 디바이스의 현재의 상태에 특정적인 특징들을 반영하기 위하여 희박 분류기 모델을 수정할 수도 있고, 이것은 다양한 컴포넌트들이 이동 디바이스의 현재의 상태에 기초하여 모니터링된 특징들을 우선순위화함으로써 악성 거동을 더욱 양호하게 검출하거나 이동 디바이스의 전체적인 성능을 개선시키는 것을 가능하게 할 수도 있다.

[0075] 위에서 주목된 바와 같이, 거동을 모니터링함에 있어서의 이용을 위한 희박 분류기 모델을 생성하기 위하여 이동 디바이스에 의해 프로세싱될 수도 있는 대형 분류기 모델의 타입의 하나의 예는 부스팅된 판단 스텀프들 분류기 모델이다. 뒤따르는 상세한 설명들에서는, 부스팅된 판단 스텀프들 분류기 모델들에 대해 참조들이 행해질 수도 있지만, 이러한 참조들은 일 예의 목적들을 위한 것이고, 청구항이 부스팅된 판단 스텀프들 분류기 모델을 명시적으로 인용하지 않으면, 청구항들의 범위를 제한하도록 의도된 것은 아니다.

[0076] 일 양태에서, 이동 디바이스는, 네트워크 서버로부터 복수의 테스트 조건들을 포함하는 전체 분류기 모델을 수신함으로써, 이동 디바이스의 소프트웨어 애플리케이션에 의해 (또는 이동 디바이스 상에 실행할 수 있는 소프트웨어 애플리케이션의 타입에 의해) 이용되는 이동 디바이스 특징들을 식별함으로써, 식별된 이동 디바이스 특징들 중의 하나를 평가하는 전체 분류기 모델에서 테스트 조건들을 식별함으로써, 식별된 테스트 조건들의 우선순위, 중요도, 또는 성공률들을 결정함으로써, 그 중요도 또는 성공률들에 따라 식별된 테스트 조건들을 우선순위화하거나 순서화함으로써, 그리고 식별된 테스트 조건들이 그 결정된 우선순위들, 중요도, 또는 성공률들에 따라 순서화되도록 식별된 테스트 조건들을 포함하는 분류기 모델을 생성함으로써, 애플리케이션-기반 분류기 모델을 생성하도록 구성될 수도 있다.

[0077] 이동 디바이스는 실시간 거동 모니터링 및 분석 동작들을 수행하기 위하여 국소적으로 생성된 희박 및/또는 애플리케이션-기반 분류기 모델들을 이용하도록 구성될 수도 있다. 예를 들어, 이동 디바이스는, 이동 디바이스로부터 거동 정보를 수집함으로써, 특징 벡터를 생성하기 위하여 수집된 거동 정보를 이용함으로써, 애플리케이션-기반 분류기 모델 내에 포함된 각각의 테스트 조건을 평가하기 위하여 생성된 특징 벡터를 애플리케이션-기반 분류기 모델에 적용함으로써, 대응하는 애플리케이션을 실행하는 이동 디바이스의 거동을 분류하기 위하여 애플리케이션-기반 분류기 모델을 이용할 수도 있다. 이동 디바이스는 또한, 애플리케이션-기반 분류기 모델에서 테스트 조건들을 평가하는 각각의 결과의 가중화된 평균을 연산할 수도 있고, 이동 디바이스 거동이 악성인지 또는 양성인지 여부를 결정하기 위하여 가중화된 평균을 이용할 수도 있다.

[0078] 다양한 양태들은 도 1 에서 예시된 일 예의 통신 시스템 (100) 과 같은 다양한 통신 시스템들 내에서 구현될 수도 있다. 전형적인 셀 전화 네트워크 (104) 는 예컨대, 전화 지상 라인들 (예컨대, 도시되지 않은 POTS 네트워크) 및 인터넷 (110) 을 통해, 이동 디바이스들 (102) (예컨대, 셀 전화들, 랩톱들, 태블릿들 등) 과 다른 네트워크 목적지들 사이에서 음성 호출들 및 데이터를 접속하도록 동작하는, 네트워크 동작 센터 (108) 에 결합된 복수의 셀 기지국들 (106) 을 포함한다. 이동 디바이스들 (102) 과 전화 네트워크 (104) 사이의 통신들은 4G, 3G, CDMA, TDMA, LTE, 및/또는 다른 셀 전화 통신 기술들과 같은 양방향 무선 통신 링크들 (112) 을 통해 달성될 수도 있다. 전화 네트워크 (104) 는 또한, 인터넷 (110) 으로의 접속을 제공하는 네트워크 동작 센터 (108) 에 결합되거나 네트워크 동작 센터 (108) 내의 하나 이상의 서버들 (114) 을 포함할 수도 있다.

[0079] 통신 시스템 (100) 은 전화 네트워크 (104) 및 인터넷 (110) 에 접속된 네트워크 서버들 (116) 을 더 포함할 수도 있다. 네트워크 서버들 (116) 과 전화 네트워크 (104) 사이의 접속은 인터넷 (110)을 통하거나, (점선 화살표들에 의해 예시된 바와 같은) 사설 네트워크를 통한 것일 수도 있다. 네트워크 서버 (116) 는 또한, 클라우드 서비스 제공자 네트워크 (118) 의 네트워크 기반구조 내의 서버로서 구현될 수도 있다. 네트워크 서버 (116) 와 이동 디바이스들 (102) 사이의 통신은 전화 네트워크 (104), 인터넷 (110), 사설 네트워크 (예시

되지 않음), 또는 그 임의의 조합을 통해 달성될 수도 있다.

[0080] 네트워크 서버 (116) 는 중앙 데이터베이스 또는 클라우드 서비스 제공자 네트워크 (118) 로부터 다양한 조건들, 특징들, 거동들, 및 정정 액션들에 관한 정보를 수신하고, 컴퓨팅 디바이스의 거동의 특정 양태를 평가하기 위하여 컴퓨팅 디바이스의 프로세서에 의해 이용될 수도 있는 데이터 및/또는 정보 구조들 (예컨대, 특징 벡터들, 거동 벡터들, 컴포넌트 리스트들 등) 을 포함하는 데이터, 알고리즘들, 분류기들, 또는 거동 모델들 (본원에서는 집합적으로 "분류기 모델들") 을 생성하기 위하여 이 정보를 이용할 수도 있다.

[0081] 일 양태에서, 네트워크 서버 (116) 는 전체 분류기 모델을 생성하도록 구성될 수도 있다. 전체 분류기 모델은 수 천 개의 특징들 및 수 백만 개의 엔트리들을 포함할 수도 있는 대형 트레이닝 데이터세트의 함수로서 생성되는 로버스트 데이터 모델일 수도 있다. 일 양태에서, 네트워크 서버 (116) 는 이동 디바이스들 (102) 의 다수의 상이한 제품들, 모델들, 및 구성들 중의 임의의 것의 열화에 기여할 수 있는 특징들, 데이터 포인트들, 및/또는 인자들의 전부 또는 대부분을 포함하기 위하여 전체 분류기 모델을 생성하도록 구성될 수도 있다.

다양한 양태들에서, 네트워크 서버는 더욱 희박한 분류기 모델들을 신속하고 효율적으로 생성하기 위하여 수정될 수 있거나, 컬링될 수 있거나, 증강될 수 있거나, 또는 이와 다르게 이용될 수 있는 유한 상태 머신, 판단 노드들, 판단 트리들로서, 또는 임의의 정보 구조로, 거동 정보의 대형 코퍼스를 설명하거나 표현하기 위하여 전체 분류기 모델을 생성하도록 구성될 수도 있다.

[0082] 게다가, 이동 디바이스 (102) 는 네트워크 서버 (116) 로부터 전체 분류기 모델을 수신하도록 구성될 수도 있다. 이동 디바이스는 이동 디바이스 (102) 의 소프트웨어 애플리케이션들의 특정 특징들 및 기능성들을 참작하는 더욱 포커싱된 분류기 모델들을 생성하기 위하여 전체 분류기 모델을 이용하도록 추가로 구성될 수도 있다. 예를 들어, 이동 디바이스 (102) 는, 이동 디바이스 (102) 상에서 설치되거나 디바이스의 메모리 내에 저장되는 특정 소프트웨어 애플리케이션 또는 소프트웨어 애플리케이션의 특정 타입 (예컨대, 게임들, 내비게이션, 금융 등) 에 관련되는 이동 디바이스의 조건들 또는 특징들을 우선적으로 또는 배타적으로 식별하거나 평가하는 애플리케이션-특정 및/또는 애플리케이션-타입-특정 분류기 모델들 (즉, 데이터 또는 거동 모델들) 을 생성할 수도 있다. 이동 디바이스 (102) 는 실시간 거동 모니터링 및 분석 동작들을 수행하기 위하여 국소적으로 생성된 분류기 모델들을 이용할 수도 있다.

[0083] 도 2 는 특정한 이동 디바이스 거동, 소프트웨어 애플리케이션, 또는 프로세스가 악성/성능-열화인지, 의심스러운지, 또는 양성인지 여부를 결정하기 위하여 실시간 거동 모니터링 및 분석 동작들 (200) 을 수행하도록 구성된 일 양태의 이동 디바이스 (102) 에서 일 예의 논리적 컴포넌트들 및 정보 흐름들을 예시한다. 이 동작들 (200) 은 이동 디바이스의 프로세싱, 메모리, 또는 에너지 자원들의 과도한 양을 소비하지 않으면서, 이동 디바이스 (102) 에서의 하나 이상의 프로세싱 코어들에 의해 연속적으로 (또는 거의 연속적으로) 수행될 수도 있다.

[0084] 도 2 에서 예시된 예에서, 이동 디바이스 (102) 는 거동 관측기 모듈 (202), 거동 분석기 모듈 (204), 외부 컨텍스트 정보 모듈 (206), 분류기 모듈 (208), 및 액츄에이터 모듈 (210) 을 포함한다. 일 양태에서, 분류기 모듈 (208) 은 거동 분석기 모듈 (204) 의 일부로서 구현될 수도 있다. 일 양태에서, 거동 분석기 모듈 (204) 은 하나 이상의 분류기 모듈들 (208) 을 생성하도록 구성될 수도 있고, 하나 이상의 분류기 모듈들의 각각은 소프트웨어 애플리케이션의 특정 특징들 또는 이동 디바이스 거동을 평가하기 위하여 이동 디바이스 프로세서에 의해 이용될 수도 있는 데이터 및/또는 정보 구조들 (예컨대, 판단 노드들 등) 을 포함하는 하나 이상의 분류기 모델들 (예컨대, 데이터/거동 모델들) 을 포함할 수도 있다.

[0085] 모듈들 (202 내지 210) 의 각각은 소프트웨어, 하드웨어, 또는 그 조합으로 구현되는 스레드 (thread), 프로세스, 데몬, 모듈, 서브-시스템, 또는 조합일 수도 있다. 다양한 양태들에서, 모듈들 (202 내지 210) 은 오퍼레이팅 시스템의 일부들 내에서 (예컨대, 커널 (kernel) 내에서, 커널 공간에서, 사용자 공간에서 등), 별도의 프로그램들 또는 애플리케이션들 내에서, 특화된 하드웨어 버퍼들 또는 프로세서들에서, 또는 그 임의의 조합에서 구현될 수도 있다. 일 양태에서, 모듈들 (202 내지 210) 중의 하나 이상은 이동 디바이스 (102) 의 하나 이상의 프로세서들 상에서 실행되는 소프트웨어 명령들로서 구현될 수도 있다.

[0086] 거동 관측기 모듈 (202) 은 이동 디바이스 시스템의 다양한 레벨들에서 다양한 API 들, 레지스터들, 카운터들, 또는 다른 컴포넌트들 (본원에서는 집합적으로 "장치화된 컴포넌트들") 을 구현하거나 조직화하고, 장치화된 컴포넌트들로부터 거동 정보를 수집함으로써 시간의 주기 동안에, 그리고 실시간으로 이동 디바이스 거동들을 연속적으로 (또는 거의 연속적으로) 모니터링하도록 구성될 수도 있다. 예를 들어, 거동 관측기 모듈 (202) 은 이동 디바이스 (102) 의 메모리 내에 저장된 로그 파일들 (예컨대, API 로그들 등) 로부터 정보를 판독함으로써 라이브러리 API 호출들, 시스템 호출 API 들, 드라이버 API 호출들, 및 다른 장치화된 컴포넌트들을 모니

터링할 수도 있다.

[0087] 거동 관측기 모듈 (202) 은 또한, 장치화된 컴포넌트들을 통해 이동 디바이스 동작들 및 이벤트들 (예컨대, 시스템 이벤트들, 상태 변경들 등) 을 모니터링/관측하고, 관측된 동작들/이벤트들에 속하는 정보를 수집하고, 수집된 정보를 지능적으로 필터링하고, 필터링된 정보에 기초하여 하나 이상의 관측들 (예컨대, 거동 벡터들 등) 을 생성하고, 생성된 관측들을 메모리 내에 (예컨대, 로그 파일 등의 내에) 저장하고, 및/또는 (예컨대, 메모리 기록들, 함수 호출들 등을 통해) 생성된 관측들 또는 수집된 거동 정보를 거동 분석기 모듈 (204) 로 전송하도록 구성될 수도 있다. 다양한 양태들에서, 생성된 관측들은 거동 벡터로서, 및/또는 API 로그 파일 또는 구조에서 저장될 수도 있다.

[0088] 거동 관측기 모듈 (202) 은 애플리케이션 프레임워크 또는 실행-시간 (run-time) 라이브러리 (library) 들에서의 라이브러리 API 호출들, 시스템 호출 API 들, 파일-시스템, 및 네트워킹 서브-시스템 동작들, (센서 디바이스들을 포함하는) 디바이스 상태 변경들, 및 다른 유사한 이벤트들에 속하는 정보를 수집함으로써, 이동 디바이스 동작들 및 이벤트들을 모니터링/관측할 수도 있다. 거동 관측기 모듈 (202) 은 또한, 파일명들을 검색하는 것, 파일 액세스들의 범주들 (개인 정보 또는 정상 데이터 파일들), 파일들 (예를 들어, 타입 exe, zip 등) 을 생성하거나 삭제하는 것, 파일 판독/기록/탐색 동작들, 파일 허가 (file permission) 들을 변경하는 것 등을 포함할 수도 있는 파일 시스템 활동을 모니터링할 수도 있다.

[0089] 거동 관측기 모듈 (202) 은 또한, 접속들의 타입들, 프로토콜들, 포트 번호들, 디바이스가 접속되는 서버/클라이언트, 접속들의 수, 통신들의 용량 또는 주파수 등을 포함할 수도 있는 데이터 네트워크 활동을 모니터링할 수도 있다. 거동 관측기 모듈 (202) 은, 송출되거나, 수신되거나, 또는 차단된 호출들 또는 메시지들 (예컨대, SMS 등) 의 수 (예컨대, 통화된 고급 호출들의 수) 및 타입을 모니터링하는 것을 포함할 수도 있는 전화 네트워크 활동을 모니터링할 수도 있다.

[0090] 거동 관측기 모듈 (202) 은 또한, 포크 (fork) 들의 수, 메모리 액세스 동작들, 개방된 파일들의 수 등을 모니터링하는 것을 포함할 수도 있는 시스템 자원 사용을 모니터링할 수도 있다. 거동 관측기 모듈 (202) 은, 디스플레이가 온 (on) 또는 오프 (off) 인지 여부, 디바이스가 잠금 (locking) 되거나 잠금해제 (unlocking) 되는지 여부, 남아 있는 배터리의 양, 카메라의 상태 등과 같은 다양한 인자들을 모니터링하는 것을 포함할 수도 있는 이동 디바이스의 상태를 모니터링할 수도 있다. 거동 관측기 모듈 (202) 은 또한, 예를 들어, 중대한 서비스들 (브라우저, 계약들 제공자 등) 에 대한 의향들, 인터-프로세스 (inter-process) 통신들의 정도, 팝-업 (pop-up) 윈도우들 등을 모니터링함으로써 인터-프로세스 통신들 (inter-process communications; IPC) 을 모니터링할 수도 있다.

[0091] 거동 관측기 모듈 (202) 은 또한, 카메라들, 센서들, 전자 디스플레이들, WiFi 통신 컴포넌트들, 데이터 제어기들, 메모리 제어기들, 시스템 제어기들, 액세스 포트들, 타이머들, 주변 디바이스들, 무선 통신 컴포넌트들, 외부 메모리 칩들, 전압 레귤레이터들, 발진기 (oscillator) 들, 위상-고정 루프 (phase-locked loop) 들, 주변 브릿지들, 및 이동 컴퓨팅 디바이스 상에서 실행되는 프로세서들 및 클라이언트들을 지원하기 위하여 이용된 다른 유사한 컴포넌트들을 포함할 수도 있는 하나 이상의 하드웨어 컴포넌트들의 드라이버 통계들 및/또는 스테이터스 (status) 를 모니터링/관측할 수도 있다.

[0092] 거동 관측기 모듈 (202) 은 또한, 이동 컴퓨팅 디바이스 및/또는 이동 디바이스 서브-시스템들의 상태 또는 스테이터스를 나타내는 하나 이상의 하드웨어 카운터들을 모니터링/관측할 수도 있다. 하드웨어 카운터는 이동 컴퓨팅 디바이스에서 발생하는 하드웨어-관련된 활동들 또는 이벤트들의 카운트 (count) 또는 상태를 저장하도록 구성되는 프로세서들/코어들의 특수-목적 레지스터를 포함할 수도 있다.

[0093] 거동 관측기 모듈 (202) 은 또한, 소프트웨어 애플리케이션들의 액션 (action) 들 또는 동작들, 애플리케이션 다운로드 서버 (예컨대, Apple® App Store (앱 스토어) 서버) 로부터의 소프트웨어 다운로드들, 소프트웨어 애플리케이션들에 의해 이용된 이동 디바이스 정보, 호출 정보, 텍스트 메시징 정보 (예컨대, SendSMS, BlockSMS, ReadSMS 등), 미디어 메시징 정보 (예컨대, ReceiveMMS), 사용자 계정 정보, 위치 정보, 카메라 정보, 가속도계 정보, 브라우저 정보, 브라우저-기반 통신들의 컨텐츠, 음성-기반 통신들의 컨텐츠, 단거리 라디오 통신들 (예컨대, Bluetooth®, WiFi 등), 텍스트-기반 통신들의 컨텐츠, 레코딩된 오디오 파일들의 컨텐츠, 전화번호부 또는 연락처 정보, 연락처 리스트들 등을 모니터링/관측할 수도 있다.

[0094] 거동 관측기 모듈 (202) 은 음성메일 (VoiceMailComm), 디바이스 식별자들 (DeviceIDComm), 사용자 계정 정보 (UserAccountComm), 달력 정보 (CalendarComm), 위치 정보 (LocationComm), 레코딩된 오디오 정보

(RecordAudioComm), 가속도계 정보 (AccelerometerComm) 등을 포함하는 통신들을 포함하는, 이동 디바이스의 송신들 또는 통신들을 모니터링/관측할 수도 있다.

[0095] 거동 관측기 모듈 (202) 은 나침반 정보, 이동 디바이스 세팅들, 배터리 수명, 자이로스코프 정보, 압력 센서들, 자석 센서들, 스크린 활동 등의 사용 및 업데이트들/변경들을 모니터링/관측할 수도 있다. 거동 관측기 모듈 (202) 은 소프트웨어 애플리케이션으로 그리고 이로부터 통신된 통지들 (AppNotifications), 애플리케이션 업데이트들 등을 모니터링/관측할 수도 있다. 거동 관측기 모듈 (202) 은 제 2 소프트웨어 애플리케이션의 다운로딩 및/또는 설치를 요청하는 제 1 소프트웨어 애플리케이션에 속하는 조건들 또는 이벤트들을 모니터링/관측할 수도 있다. 거동 관측기 모듈 (202) 은 패스워드의 입력 등과 같은 사용자 검증에 속하는 조건들 또는 이벤트들을 모니터링/관측할 수도 있다.

[0096] 거동 관측기 모듈 (202) 은 또한, 애플리케이션 레벨, 라디오 레벨, 및 센서 레벨을 포함하는, 이동 디바이스의 다수의 레벨들에서 조건들 또는 이벤트들을 모니터링/관측할 수도 있다. 애플리케이션 레벨 관측들은 안면 인식 소프트웨어를 통해 사용자를 관측하는 것, 소셜 스트림 (social stream) 들을 관측하는 것, 사용자에 의해 입력된 메모들을 관측하는 것, PassBook, Google® 지갑, 및 PayPal 과 같은 금융 애플리케이션들의 이용에 속하는 이벤트들을 관측하는 것, 소프트웨어 애플리케이션의 액세스 및 보호된 정보의 이용을 관측하는 것 등을 포함할 수도 있다. 애플리케이션 레벨 관측들은 또한, 가상 사설 네트워크 (virtual private network; VPN) 들의 이용에 관한 이벤트들과, 동기화, 음성 검색들, 음성 제어 (예컨대, 하나의 단어를 말함으로써 전화를 잠금/잠금해제), 언어 번역기들, 통신들을 위한 데이터의 오프로딩 (offloading), 비디오 스트리밍, 사용자 활동 없는 카메라 사용, 사용자 활동 없는 마이크로폰 사용 등에 속하는 이벤트들을 관측하는 것을 포함할 수도 있다. 애플리케이션 레벨 관측은 또한, 금융 거래들을 허가하기 위한 생체인식 센서들 (예컨대, 지문 판독기, 음성 인식 서브시스템, 망막 스캐너 등) 의 소프트웨어 애플리케이션의 이용과, 생체인식 센서들의 액세스 및 이용에 관한 조건들을 모니터링하는 것을 포함할 수도 있다.

[0097] 라디오 레벨 관측들은 라디오 통신 링크들을 확립하거나 정보를 송신하기 전의 이동 디바이스와의 사용자 상호작용, 이중/다중 가입자 식별 모듈 (subscriber identity module; SIM) 카드들, 인터넷 라디오, 이동 전화 테더링, 연산들을 위한 오프로딩 데이터, 디바이스 상태 통신들, 게임 제어기 또는 홈 제어기로서의 이용, 차량 통신들, 이동 디바이스 동기화 등 중의 임의의 것 이상의 존재, 실존 또는 양을 결정하는 것을 포함할 수도 있다. 라디오 레벨 관측들은 또한, 위치결정, 피어-투-피어 (peer-to-peer; p2p) 통신들, 동기화, 차량 대 차량 통신들, 및/또는 머신-대-머신 (machine-to-machine; m2m) 을 위한 라디오들 (WiFi, WiMax, 블루투스 등) 의 이용을 모니터링하는 것을 포함할 수도 있다. 라디오 레벨 관측들은 네트워크 트래픽 사용, 통계들, 또는 프로파일들을 모니터링하는 것을 더 포함할 수도 있다.

[0098] 센서 레벨 관측들은 이동 디바이스의 사용 및/또는 외부 환경을 결정하기 위하여 자석 센서 또는 다른 센서를 모니터링하는 것을 포함할 수도 있다. 예를 들어, 이동 디바이스 프로세서는 전화가 (예컨대, 수납주머니 (holster) 내의 자석을 감지하도록 구성된 자석 센서를 통해) 수납주머니 내에 있는지, 또는 (예컨대, 카메라 또는 광 센서에 의해 검출된 광의 양을 통해) 사용자의 포켓 내에 있는지 여부를 결정하도록 구성될 수도 있다.

이동 디바이스가 수납주머니 내에 있는 것을 검출하는 것은 의심스러운 거동들을 인식하는 것에 관련될 수도 있는데, 예를 들어, 이는 이동 디바이스가 수납되는 동안에 발생하는 사용자에 의한 능동적인 사용 (예컨대, 사진들 또는 비디오들의 촬영, 메시지들의 전송, 음성 호출을 행함, 사운드들을 레코딩 등) 에 관련된 활동들 및 기능들이 (예컨대, 사용자에 관해 추적하거나 정찰하기 위하여) 디바이스 상에서 실행되는 범죄적 프로세스들의 징후들일 수 있기 때문이다.

[0099] 사용 또는 외부 환경들에 관련된 센서 레벨 관측들의 다른 예들은 근접장 통신 (near-field communication; NFC) 들을 검출하는 것, 신용 카드 스캐너, 바코드 스캐너, 또는 이동 태그 판독기로부터 정보를 수집하는 것, 범용 직렬 버스 (universal serial bus; USB) 전력 충전 소스의 존재를 검출하는 것, 키보드 또는 보조 디바이스가 이동 디바이스에 결합된 것을 검출하는 것, 이동 디바이스가 (예컨대, USB 등을 통해) 컴퓨팅 디바이스에 결합된 것을 검출하는 것, LED, 플래시, 플래시라이트, 또는 광원이 수정되었거나 디스에이블되었는지 여부 (예컨대, 긴급 시그널링 앱을 악의적으로 디스에이블하는 것 등) 를 결정하는 것, 스피커 또는 마이크로폰이 턴온 (turn on) 되거나 급전된 것을 검출하는 것, 충전 또는 전력 이벤트를 검출하는 것, 이동 디바이스가 게임 제어기로서 이용되고 있는 것을 검출하는 것 등을 포함할 수도 있다. 센서 레벨 관측들은 또한, 의료용 또는 건광관리 센서들로부터 또는 사용자의 신체를 스캐닝하는 것으로부터 정보를 수집하는 것, USB/오디오 잭으로 플러깅된 외부 센서로부터 정보를 수집하는 것, (예컨대, 진동기 인터페이스 등을 통해) 촉각 또는 햅틱 센서로부터 정보를 수집하는 것, 이동 디바이스의 열 상태에 속하는 정보를 수집하는 것, 지문 판독기, 음성 인식 서브

시스템, 망막 스캐너로부터 정보를 수집하는 것 등을 포함할 수도 있다.

[0100] 거동 관측기 모듈 (202) 은 관측된 거동들의 간결한 정의를 포함하는 거동 벡터들을 생성하도록 구성될 수도 있다. 각각의 거동 벡터는 이동 디바이스, 소프트웨어 애플리케이션, 또는 프로세스의 관측된 거동을 값 또는 벡터 데이터-구조로 (예컨대, 수들의 스트링의 형태 등으로) 간단 명료하게 설명할 수도 있다. 거동 벡터는 또한, 이동 디바이스 시스템이 이동 디바이스 거동들을 신속하게 인식하고, 식별하고, 및/또는 분석하는 것을 가능하게 하는 식별자로서 기능할 수도 있다. 일 양태에서, 거동 관측기 모듈 (202) 은 일련의 수들을 포함하는 거동 벡터를 생성할 수도 있고, 이러한 수들의 각각은 이동 디바이스의 특징 또는 거동을 나타낸다. 예를 들어, 거동 벡터 내에 포함된 수들은 이동 디바이스의 카메라가 이용 중인지 여부 (예컨대, 카메라가 오프일 때에 제로 (zero) 이고 카메라가 활성화될 때에 1), 이동 디바이스로부터 송신되었거나 이동 디바이스에 의해 생성되었던 네트워크 트래픽의 양 (예컨대, 20 KB/sec 등), 통신되었던 인터넷 메시지들의 수 (예컨대, SMS 메시지들의 수 등) 등을 나타낼 수도 있다.

[0101] 열악하게 설계된 소프트웨어 애플리케이션들, 멀웨어, 바이러스들, 프래그먼트화된 메모리, 및 배경 프로세스들을 포함하는, 시간 경과에 따라 이동 디바이스의 성능 및 전력 사용 레벨들에 있어서의 열화에 기여할 수도 있는 많은 다양한 인자들이 있을 수도 있다. 이 인자들의 수, 다양성, 및 복잡성으로 인해, 최신 이동 디바이스들의 복잡하지만 자원-제약된 시스템들의 성능 및/또는 전력 사용 레벨들을 열화시킬 수도 있는 다양한 컴포넌트들, 거동들, 프로세스들, 동작들, 조건들, 상태들, 또는 특징들 (또는 그 조합들) 의 전부를 동시에 평가하는 것은 종종 실현가능하지 않다. 관리가능한 레벨로 모니터링된 인자들의 수를 감소시키기 위하여, 일 양태에서, 거동 관측기 모듈 (202) 은 이동 디바이스의 열화에 기여할 수 있었던 모든 인자들의 작은 서브세트인 거동들 또는 인자들의 초기 또는 감소된 세트를 모니터링/관측하도록 구성될 수도 있다.

[0102] 일 양태에서, 거동 관측기 모듈 (202) 은 네트워크 서버 (116) 및/또는 클라우드 서비스 또는 네트워크 (118) 에서의 컴포넌트로부터 거동들 및/또는 인자들의 초기 세트를 수신할 수도 있다. 일 양태에서, 거동들/인자들의 초기 세트는 네트워크 서버 (116) 로부터 수신된 전체 분류기 모델에서 특정될 수도 있다. 또 다른 양태에서, 거동들/인자들의 초기 세트는 전체 분류기 모델에 기초하여 이동 디바이스에서 생성되는 희박 분류기 모델에서 특정될 수도 있다. 일 양태에서, 거동들/인자들의 초기 세트는 전체 또는 희박 분류기 모델에 기초하여 이동 디바이스에서 생성되는 애플리케이션-기반 분류기 모델에서 특정될 수도 있다. 다양한 양태들에서, 애플리케이션-기반 분류기 모델은 애플리케이션-특정 분류기 모델 또는 애플리케이션-타입-특정 분류기 모델일 수도 있다.

[0103] 거동 관측기 모듈 (202) 은 (예컨대, 메모리 기록 동작, 함수 호출 등을 통해) 수집된 거동 정보를 거동 분석기 모듈 (204) 로 통신할 수도 있다. 거동 분석기 모듈 (204) 은, 거동 벡터들을 생성하고, 거동 벡터들에 기초하여 공간적 및/또는 시간적 상관들을 생성하고, 특정한 이동 디바이스 거동, 조건, 서브-시스템, 소프트웨어 애플리케이션, 또는 프로세스가 양성인지, 의심스러운지, 또는 양성이 아닌지 (즉, 악성 또는 성능-열화) 여부를 결정하기 위해 이 정보를 이용하기 위하여 거동 정보를 수신하고 이용할 수도 있다.

[0104] 거동 분석기 모듈 (204) 및/또는 분류기 모듈 (208) 은, 이동 이동 디바이스 거동이 양성인지 또는 양성이 아닌지 (예컨대, 악성 또는 성능-열화) 여부를 결정하기 위하여 데이터, 알고리즘들, 분류기들, 또는 모델들 (집합적으로 "분류기 모델들" 로서 지칭됨) 을 수집된 거동 정보에 대해 수행하는 것, 실행하는 것, 및/또는 적용하는 것을 포함할 수도 있는 실시간 거동 분석 동작들을 수행하도록 구성될 수도 있다. 각각의 분류기 모델은 이동 디바이스 거동의 특정 특징 또는 양태를 평가하기 위하여 이동 디바이스 프로세서에 의해 이용될 수도 있는 데이터 및/또는 정보 구조들 (예컨대, 특징 벡터들, 거동 벡터들, 컴포넌트 리스트들 등) 을 포함하는 거동 모델일 수도 있다. 각각의 분류기 모델은 또한, 이동 디바이스 (102) 에서 다수의 특징들, 인자들, 데이터 포인트들, 엔트리들, API 들, 상태들, 조건들, 거동들, 애플리케이션들, 프로세스들, 동작들, 컴포넌트들 등 (집합적으로 "특징들" 로서 지칭됨) 을 모니터링하기 위한 판단 기준들을 포함할 수도 있다. 분류기 모델들은 이동 디바이스 (102) 상에서 사전설치될 수도 있거나, 네트워크 서버 (116) 로부터 다운로딩되거나 수신될 수도 있거나, 이동 디바이스 (102) 에서 생성될 수도 있거나, 그 임의의 조합일 수도 있다. 분류기 모델들은 또한, 크라우드 소싱 솔루션들, 거동 모델링 기법들, 머신 학습 알고리즘들 등을 이용함으로써 생성될 수도 있다.

[0105] 각각의 분류기 모델은 전체 분류기 모델 또는 희박 분류기 모델로서 범주화될 수도 있다. 전체 분류기 모델은 수 천 개의 특징들 및 수 백만 개의 엔트리들을 포함할 수도 있는 대형 트레이닝 데이터세트의 함수로서 생성되는 로버스트 데이터 모델일 수도 있다. 희박 분류기 모델은 특정한 이동 디바이스 거동이 양성인지 또

는 양성이 아닌지 (예컨대, 악성 또는 성능-열화) 여부를 결정하기 위하여 가장 관련되는 특징들/엔트리들에 대한 테스트들을 포함하거나 우선순위화하는 감소된 데이터세트로부터 생성되는 더욱 포커싱된 데이터 모델일 수도 있다.

[0106] 거동 분석기 모듈 (204) 및/또는 분류기 모듈 (208) 은 거동 관측기 모듈 (202) 로부터 관측들 또는 거동 정보를 수신할 수도 있고, 수신된 정보 (즉, 관측들) 를 외부 컨텍스트 정보 모듈 (206) 로부터 수신된 컨텍스트 정보와 비교할 수도 있고, 시간 경과에 따른 디바이스의 열화에 기여하고 있거나 (또는 기여할 가능성이 있음), 또는 이와 다르게 디바이스에 관한 문제들을 야기시킬 수도 있는 수신된 관측들과 연관된 서브시스템들, 프로세스들, 및/또는 애플리케이션들을 식별할 수도 있다.

[0107] 일 양태에서, 거동 분석기 모듈 (204) 및/또는 분류기 모듈 (208) 은 시간 경과에 따른 디바이스의 열화에 기여하고 있거나 (또는 기여할 가능성이 있거나), 또는 이와 다르게 디바이스에 관한 문제들을 야기시킬 수도 있는 거동들, 프로세스들, 또는 프로그램들을 식별하기 위하여 정보의 제한된 세트 (즉, 대략적인 관측들) 를 사용하기 위한 지능 (intelligence) 을 포함할 수도 있다. 예를 들어, 거동 분석기 모듈 (204) 은 다양한 모듈들 (예컨대, 거동 관측기 모듈 (202), 외부 컨텍스트 정보 모듈 (206) 등) 로부터 수집된 (예컨대, 관측들의 형태인) 정보를 분석하고, 이동 디바이스의 정상 동작 거동들을 학습하고, 비교들의 결과들에 기초하여 하나 이상의 거동 벡터들을 생성하도록 구성될 수도 있다. 거동 분석기 모듈 (204) 은 추가의 분석을 위하여, 생성된 거동 벡터들을 분류기 모듈 (208) 로 전송할 수도 있다.

[0108] 일 양태에서, 분류기 모듈 (208) 은, 특정한 이동 디바이스 거동, 소프트웨어 애플리케이션, 또는 프로세스가 성능-열화/악성인지, 양성인지, 또는 의심스러운지 여부를 결정하기 위하여 거동 벡터들을 분류기 모델에 적용하거나 거동 벡터들을 분류기 모델과 비교하도록 구성될 수도 있다. 분류기 모듈 (208) 이 거동, 소프트웨어 애플리케이션, 또는 프로세스가 악성이거나 성능-열화인 것으로 결정할 때, 분류기 모듈 (208) 은 액츄에이터 모듈 (210) 에 통지할 수도 있고, 이 액츄에이터 모듈 (210) 은 악성이거나 성능-열화인 것으로 결정된 이동 디바이스 거동들을 정정하기 위한 다양한 액션들 또는 동작들을 수행할 수도 있고, 및/또는 식별된 문제를 치유하거나, 고치거나, 격리하거나, 또는 이와 다르게 해결하기 위한 동작들을 수행할 수도 있다.

[0109] 분류기 모듈 (208) 이 거동, 소프트웨어 애플리케이션, 또는 프로세스가 의심스러운 것으로 결정할 때, 분류기 모듈 (208) 은 거동 관측기 모듈 (202) 에 통지할 수도 있고, 이 거동 관측기 모듈 (202) 은 그 관측들의 입도 (granularity) (즉, 이동 디바이스 거동들이 관측되는 상세함의 레벨) 를 조절할 수도 있고 및/또는 분류기 모듈 (208) 로부터 수신된 정보 (예컨대, 실시간 분석 동작들의 결과들) 에 기초하여 관측되는 거동들을 변경시킬 수도 있고, 새로운 또는 추가적인 거동 정보를 생성하거나 수집할 수도 있고, 추가의 분석/분류를 위하여 새로운/추가적인 정보를 거동 분석기 모듈 (204) 및/또는 분류기 모듈 (208) 로 전송할 수도 있다. 거동 관측기 모듈 (202) 과 분류기 모듈 (208) 사이의 이러한 피드백 통신들은 이동 디바이스 (102) 가 관측들의 입도를 재귀적으로 증가시키는 것 (즉, 더 미세하거나 더욱 상세한 관측들을 행함) 을 가능하게 하거나, 의심스러운 또는 성능-열화인 이동 디바이스 거동의 소스가 식별될 때까지, 프로세싱 또는 배터리 소비 임계점에 도달될 때까지, 또는 이동 디바이스 프로세서가 의심스러운 또는 성능-열화인 이동 디바이스 거동의 소스가 관측 입도에 있어서의 추가의 증가들로부터 식별될 수 없는 것으로 결정할 때까지 관측되는 특징들/거동들을 변경하는 것을 가능하게 한다. 이러한 피드백 통신은 또한, 이동 디바이스의 프로세싱, 메모리, 또는 에너지 자원들의 과도한 양을 소비하지 않으면서, 이동 디바이스 (102) 가 이동 디바이스에서 국소적으로 데이터/거동 모델들을 조절하거나 수정하는 것을 가능하게 한다.

[0110] 일 양태에서, 거동 관측기 모듈 (202) 및 거동 분석기 모듈 (204) 은 제한된 그리고 대략적인 관측들로부터 의심스러운 거동을 식별하기 위하여, 더욱 상세하게 관측하기 위한 거동들을 동적으로 결정하기 위하여, 그리고 관측들에 대해 요구된 상세함의 레벨을 동적으로 결정하기 위하여, 개별적으로 또는 집합적으로 중의 어느 하나로, 컴퓨팅 시스템의 거동들의 실시간 거동 분석을 제공할 수도 있다. 이러한 방식으로, 거동 관측기 모듈 (202) 은 이동 디바이스 (102) 가 디바이스 상에서 다량의 프로세서, 메모리, 또는 배터리 자원들을 요구하지 않으면서, 문제들을 효율적으로 식별하고 문제들이 이동 디바이스들 상에서 발생하는 것을 방지하는 것을 가능하게 한다.

[0111] 다양한 양태들에서, 거동 관측기 모듈 (202) 및/또는 거동 분석기 모듈 (204) 은 근접 모니터링을 요구하는 임계 데이터 자원 (critical data resource) 을 식별함으로써, 임계 데이터 자원과 연관된 중간 자원을 식별함으로써, 임계 데이터 자원 및 중간 자원을 액세스할 때에 소프트웨어 애플리케이션에 의해 행해진 API 호출들을 모니터링함으로써, API 호출들에 의해 소비되거나 생성되는 이동 디바이스 자원들을 식별함으로써, API 호출들

의 패턴을 소프트웨어 애플리케이션에 의한 악성 활동을 표시하는 것으로서 식별함으로써, API 호출들의 식별된 패턴 및 식별된 이동 디바이스 자원들에 기초하여 경량 거동 시그니처 (light-weight behavior signature) 를 생성함으로써, 거동 분석 동작들을 수행하기 위하여 경량 거동 시그니처를 이용함으로써, 그리고 거동 분석 동작들에 기초하여 소프트웨어 애플리케이션이 악성인지 또는 양성인지 여부를 결정함으로써, 이동 디바이스 거동들을 분석하도록 구성될 수도 있다.

[0112] 다양한 양태들에서, 거동 관측기 모듈 (202) 및/또는 거동 분석기 모듈 (204) 은 이동 디바이스 상에서 실행되는 소프트웨어 애플리케이션들에 의해 가장 빈번하게 이용되는 API 들을 식별함으로써, 이동 디바이스의 메모리 내의 API 로그에서 식별된 핫 API (hot API) 들의 사용에 관한 정보를 저장함으로써, 그리고 정상 동작 패턴들과 부합하지 않는 이동 디바이스 거동들을 식별하기 위하여 API 로그에서 저장된 정보에 기초하여 거동 분석 동작들을 수행함으로써, 이동 디바이스 거동들을 분석하도록 구성될 수도 있다. 일 양태에서, API 로그는, API 의 소환 (invocation) 들에 걸쳐 동일하게 유지되는 일반적인 필드들의 값들이 API 의 각각의 소환에 특정적인 특정 필드들의 값들로서 별도의 테이블에서 저장되도록 API 로그가 편성되게 생성될 수도 있다. API 로그는 또한, 특정 필드들의 값들이 일반적인 필드들의 값들을 저장하는 별도의 테이블에 대한 해시 키 (hash key) 들과 함께 테이블에서 저장되도록 생성될 수도 있다.

[0113] 다양한 양태들에서, 거동 관측기 모듈 (202) 및/또는 거동 분석기 모듈 (204) 은 복수의 부스팅된 판단 스텀프들로서의 변환 또는 표현에 적합한 유한 상태 머신을 포함하는 전체 분류기 모델을 수신함으로써, 전체 분류기에 기초하여 이동 디바이스에서 희박 분류기 모델을 생성함으로써, 그리고 이동 디바이스의 거동을 양성 또는 양성이 아닌 것 (즉, 악성, 성능 열화 등) 중의 어느 하나인 것으로서 분류하기 위하여 이동 디바이스에서 희박 분류기 모델을 이용함으로써, 이동 디바이스 거동들을 분석하도록 구성될 수도 있다. 일 양태에서, 전체 분류기 모델에 기초하여 희박 분류기 모델을 생성하는 것은 이동 디바이스의 프로세싱, 메모리, 또는 에너지 자원들의 과도한 양을 소비하지 않으면서, 이동 디바이스 거동을 분류하기 위하여 평가되어야 하는 다수의 고유한 테스트 조건들을 결정하는 것, 부스팅된 판단 스텀프들의 리스트를 순차적으로 트래버싱함으로써 테스트 조건들의 리스트를 생성하고 테스트 조건들의 리스트가 결정된 수의 고유한 테스트 조건들을 포함할 수도 있을 때까지, 각각의 순차적으로 통과된 부스팅된 판단 스텀프와 연관된 테스트 조건을 테스트 조건들의 리스트 내로 삽입하는 것, 및 테스트 조건들의 생성된 리스트 내에 포함된 복수의 테스트 조건들 중의 하나를 테스트하는 그 부스팅된 판단 스텀프들을 포함하거나 우선순위화하기 위하여 희박 분류기 모델을 생성하는 것을 포함할 수도 있다.

[0114] 다양한 양태들에서, 거동 관측기 모듈 (202) 및/또는 거동 분석기 모듈 (204) 은 이동 디바이스의 거동을 분류하는 것에 관련되는 복수의 테스트 조건들에서 이동 디바이스-특정, 애플리케이션-특정, 또는 애플리케이션-타입 특정 테스트 조건들을 식별하기 위하여 이동 디바이스의 디바이스-특정 정보를 이용하고, 식별된 이동 디바이스-특정, 애플리케이션-특정, 또는 애플리케이션-타입 특정 테스트 조건들을 포함하거나 우선순위화하는 희박 분류기 모델을 생성하고, 이동 디바이스의 거동을 분류하기 위하여 이동 디바이스에서 생성된 희박 분류기 모델을 이용하도록 구성될 수도 있다. 일 양태에서, 희박 분류기 모델은 이동 디바이스의 현재의 동작 상태 또는 구성에 관련되는 이동 디바이스 특징을 평가하는 판단 노드들을 포함하거나 우선순위화하기 위하여 생성될 수도 있다. 추가의 양태에서, 희박 분류기 모델을 생성하는 것은 이동 디바이스의 자원들 (예컨대, 프로세싱, 메모리, 또는 에너지 자원들) 의 과도한 양을 소비하지 않으면서, 거동을 분류하기 위하여 평가되어야 하는 다수의 고유한 테스트 조건들을 결정하는 것, 전체 분류기 모델에서 복수의 테스트 조건들을 순차적으로 트래버싱함으로써 테스트 조건들의 리스트를 생성하고, 테스트 조건들의 리스트가 결정된 수의 고유한 테스트 조건들을 포함할 때까지, 이동 디바이스의 거동을 분류하는 것에 관련되는 그 테스트 조건들을 테스트 조건들의 리스트 내로 삽입하는 것, 및 테스트 조건들의 생성된 리스트 내에 포함된 조건들 중의 하나를 테스트하는 전체 분류기 모델 내에 포함된 판단 노드들을 포함하기 위하여 희박 분류기 모델을 생성하는 것을 포함할 수도 있다.

[0115] 다양한 양태들에서, 거동 관측기 모듈 (202) 및/또는 거동 분석기 모듈 (204) 은 소프트웨어 애플리케이션 또는 프로세스의 활동을 모니터링함으로써, 소프트웨어 애플리케이션/프로세스의 오퍼레이팅 시스템 실행 상태를 결정함으로써, 그리고 활동이 모니터링되었던 소프트웨어 애플리케이션 또는 프로세스의 활동 및/또는 오퍼레이팅 시스템 실행 상태에 기초하여 활동이 양성인지 여부를 결정함으로써, 이동 디바이스의 정상 동작 패턴들과 부합하지 않는 이동 디바이스 거동들을 인식하도록 구성될 수도 있다. 추가의 양태에서, 거동 관측기 모듈 (202) 및/또는 거동 분석기 모듈 (204) 은 소프트웨어 애플리케이션 또는 프로세스의 오퍼레이팅 시스템 실행 상태가 활동에 관련되는지 여부를 결정할 수도 있고, 활동이 모니터링되었던 소프트웨어 애플리케이션 또는 프로세스의 오퍼레이팅 시스템 실행 상태를 식별하는 섀도우 특징 값 (shadow feature value) 을 생성할 수도 있

고, 활동을 오퍼레이팅 시스템 실행 상태를 식별하는 섀도우 특징 값과 연관시키는 거동 벡터를 생성할 수도 있고, 활동이 양성인지, 의심스러운지, 또는 양성이 아닌지 (즉, 악성 또는 성능-열화) 여부를 결정하기 위하여 거동 벡터를 이용할 수도 있다.

[0116] 위에서 논의된 바와 같이, 이동 디바이스 프로세서는 다양한 특징들을 평가하는데 적합한 복수의 테스트 조건들을 포함하는 분류기 모델을 수신하거나 생성할 수도 있고, 특정 소프트웨어 애플리케이션 또는 소프트웨어 애플리케이션-타입에 의해 이용된 이동 디바이스 특징들을 식별할 수도 있고, 식별된 이동 디바이스 특징들을 평가하는 수신된/생성된 분류기 모델에서의 테스트 조건들을 식별할 수도 있고, 식별된 테스트 조건들을 포함하거나 우선순위화하는 애플리케이션-특정 및/또는 애플리케이션-타입 특정 분류기 모델들을 생성할 수도 있다. 특정 소프트웨어 애플리케이션 또는 특정 소프트웨어 애플리케이션-타입에 의해 이용된 특징들은 이동 디바이스 동작들, 이동 디바이스 이벤트들, 데이터 네트워크 활동, 시스템 자원 사용, 이동 디바이스 상태, 인터-프로세스 통신들, 드라이버 통계들, 하드웨어 컴포넌트 스테이터스, 하드웨어 카운터들, 소프트웨어 애플리케이션들의 액션들 또는 동작들, 소프트웨어 다운로드들, 디바이스 또는 컴포넌트 세팅들에 대한 변경들, 애플리케이션 레벨에서의 조건들 및 이벤트들, 라디오 레벨에서의 조건들 및 이벤트들, 센서 레벨에서의 조건들 및 이벤트들, 위치 하드웨어, 개인 영역 네트워크 하드웨어, 마이크로폰 하드웨어, 스피커 하드웨어, 카메라 하드웨어, 스크린 하드웨어, 범용 직렬 버스 하드웨어, 동기화 하드웨어, 위치 하드웨어 드라이버들, 개인 영역 네트워크 하드웨어 드라이버들, 근접장 통신 하드웨어 드라이버들, 마이크로폰 하드웨어 드라이버들, 스피커 하드웨어 드라이버들, 카메라 하드웨어 드라이버들, 자이로스코프 하드웨어 드라이버들, 브라우저 지원 하드웨어 드라이버들, 배터리 하드웨어 드라이버들, 범용 직렬 버스 하드웨어 드라이버들, 저장 하드웨어 드라이버들, 사용자 상호작용 하드웨어 드라이버들, 동기화 하드웨어 드라이버들, 라디오 인터페이스 하드웨어 드라이버들과, 위치 하드웨어, 근접장 통신 (NFC) 하드웨어, 스크린 하드웨어, 브라우저 지원 하드웨어, 저장 하드웨어, 가속도계 하드웨어, 동기화 하드웨어, 이중 SIM 하드웨어, 라디오 인터페이스 하드웨어, 및 임의의 특정 하드웨어에 대한 관련되지 않은 특징들을 모니터링하거나 평가함으로써 결정될 수도 있다.

[0117] 예를 들어, 다양한 양태들에서, 이동 디바이스 프로세서는 관성 센서 (inertia sensor) 컴포넌트, 배터리 하드웨어 컴포넌트, 브라우저 지원 하드웨어 컴포넌트, 카메라 하드웨어 컴포넌트, 가입자 식별 모듈 (SIM) 하드웨어 컴포넌트, 위치 하드웨어 컴포넌트, 마이크로폰 하드웨어 컴포넌트, 라디오 인터페이스 하드웨어 컴포넌트, 스피커 하드웨어 컴포넌트, 스크린 하드웨어 컴포넌트, 동기화 하드웨어 컴포넌트, 저장 컴포넌트, 범용 직렬 버스 하드웨어 컴포넌트, 사용자 상호작용 하드웨어 컴포넌트, 관성 센서 드라이버 컴포넌트, 배터리 하드웨어 드라이버 컴포넌트, 브라우저 지원 하드웨어 드라이버 컴포넌트, 카메라 하드웨어 드라이버 컴포넌트, SIM 하드웨어 드라이버 컴포넌트, 위치 하드웨어 드라이버 컴포넌트, 마이크로폰 하드웨어 드라이버 컴포넌트, 라디오 인터페이스 하드웨어 드라이버 컴포넌트, 스피커 하드웨어 드라이버 컴포넌트, 스크린 하드웨어 드라이버 컴포넌트, 동기화 하드웨어 드라이버 컴포넌트, 저장 드라이버 컴포넌트, 범용 직렬 버스 하드웨어 드라이버 컴포넌트, 범용 직렬 버스를 통해 접속된 하드웨어 컴포넌트, 및 사용자 상호작용 하드웨어 드라이버 컴포넌트와 같은 하나 이상의 장치화된 컴포넌트들로부터 정보를 수집함으로써 특정 소프트웨어 애플리케이션 (또는 특정 소프트웨어 애플리케이션 타입) 에 의해 이용된 이동 디바이스 특징들을 식별할 수도 있다.

[0118] 다양한 양태들에서, 이동 디바이스 프로세서는 애플리케이션 프레임워크 또는 실행-시간 라이브러리에서의 라이브러리 애플리케이션 프로그래밍 인터페이스 (API) 호출들, 시스템 호출 API 들, 파일-시스템 및 네트워킹 서브-시스템 동작들, 파일 시스템 활동, 파일명들 검색들, 파일 액세스들의 범주들, 파일 허가들의 변경, 파일들의 생성 또는 삭제에 관한 동작들, 및 파일 판독/기록/탐색 동작들 중의 하나 이상을 모니터링하거나 분석함으로써 특정 소프트웨어 애플리케이션 (또는 특정 소프트웨어 애플리케이션 타입) 에 의해 이용된 이동 디바이스 특징들을 식별할 수도 있다.

[0119] 다양한 양태들에서, 이동 디바이스 프로세서는 접속 타입들, 프로토콜들, 포트 번호들, 디바이스가 접속되는 서버/클라이언트, 접속들의 수, 통신들의 용량 또는 주파수, 전화 네트워크 활동, 전송된 호출들/메시지들의 타입 및 수, 수신된 호출들/메시지들의 타입 및 수, 차단된 호출들/메시지들의 타입 및 수, 호출 정보, 텍스트 메시징 정보, 미디어 메시징, 사용자 계정 정보, 송신들, 음성메일, 및 디바이스 식별자들 중의 하나 이상을 모니터링하거나 분석함으로써 특정 소프트웨어 애플리케이션 (또는 특정 소프트웨어 애플리케이션 타입) 에 의해 이용된 이동 디바이스 특징들을 식별할 수도 있다.

[0120] 다양한 양태들에서, 이동 디바이스 프로세서는 포크 (fork) 들의 수, 메모리 액세스 동작들, 및 소프트웨어 애플리케이션에 의해 개방된 파일들의 수 중의 하나 이상을 모니터링하거나 분석함으로써 특정 소프트웨어 애플리케이션 (또는 특정 소프트웨어 애플리케이션 타입) 에 의해 이용된 이동 디바이스 특징들을 식별할 수도 있다.

다양한 양태들에서, 이동 디바이스 프로세서는, 디스플레이 온/오프 상태, 잠금/잠금해제된 상태, 배터리 충전 상태, 카메라 상태, 및 마이크로폰 상태를 포함하는, 소프트웨어 애플리케이션에 의해 야기된 상태 변경들을 모니터링하거나 분석함으로써, 특정 소프트웨어 애플리케이션 (또는 특정 소프트웨어 애플리케이션 타입) 에 의해 이용된 이동 디바이스 특징들을 식별할 수도 있다.

[0121] 다양한 양태들에서, 이동 디바이스 프로세서는 중대한 서비스들, 인터-프로세스 통신들의 정도, 및 소프트웨어 애플리케이션에 의해 생성된 팝-업 윈도우들을 모니터링하거나 분석함으로써 특정 소프트웨어 애플리케이션 (또는 특정 소프트웨어 애플리케이션 타입) 에 의해 이용된 이동 디바이스 특징들을 식별할 수도 있다. 다양한 양태들에서, 이동 디바이스 프로세서는 카메라들, 센서들, 전자 디스플레이들, WiFi 통신 컴포넌트들, 데이터 제어기들, 메모리 제어기들, 시스템 제어기들, 액세스 포트들, 주변 디바이스들, 무선 통신 컴포넌트들, 및 외부 메모리 칩들 중의 하나 이상에 대한 드라이버들로부터의 통계들을 모니터링하거나 분석함으로써 특정 소프트웨어 애플리케이션 (또는 특정 소프트웨어 애플리케이션 타입) 에 의해 이용된 이동 디바이스 특징들을 식별할 수도 있다.

[0122] 다양한 양태들에서, 이동 디바이스 프로세서는 카메라들, 센서들, 전자 디스플레이들, WiFi 통신 컴포넌트들, 데이터 제어기들, 메모리 제어기들, 시스템 제어기들, 액세스 포트들, 타이머들, 주변 디바이스들, 무선 통신 컴포넌트들, 외부 메모리 칩들, 전압 레귤레이터들, 발진기들, 위상-고정 루프들, 주변 브릿지들, 및 이동 컴퓨팅 디바이스 상에서 실행되는 프로세서들 및 클라이언트들을 지원하기 위하여 이용된 다른 유사한 컴포넌트들의 액세스 또는 이용을 모니터링하거나 분석함으로써 특정 소프트웨어 애플리케이션 (또는 특정 소프트웨어 애플리케이션 타입) 에 의해 이용된 이동 디바이스 특징들을 식별할 수도 있다.

[0123] 다양한 양태들에서, 이동 디바이스 프로세서는 이동 컴퓨팅 디바이스 및/또는 이동 디바이스 서브-시스템들 및/또는, 하드웨어-관련된 활동들 또는 이벤트들의 카운트 또는 상태를 저장하도록 구성되는 프로세서들/코어들의 특수-목적 레지스터들의 상태 또는 스테이터스를 나타내는 하드웨어 카운터들의 액세스 또는 이용을 모니터링하거나 분석함으로써 특정 소프트웨어 애플리케이션 (또는 특정 소프트웨어 애플리케이션 타입) 에 의해 이용된 이동 디바이스 특징들을 식별할 수도 있다.

[0124] 다양한 양태들에서, 이동 디바이스 프로세서는, 위치 정보, 카메라 정보, 가속도계 정보, 브라우저 정보, 브라우저-기반 통신들의 컨텐츠, 음성-기반 통신들의 컨텐츠, 단거리 라디오 통신들, 텍스트-기반 통신들의 컨텐츠, 레코딩된 오디오 파일들의 컨텐츠, 전화번호부 또는 연락처 정보, 연락처들 리스트들, 달력 정보, 위치 정보, 레코딩된 오디오 정보, 가속도계 정보, 소프트웨어 애플리케이션으로, 그리고 소프트웨어 애플리케이션으로부터 통신된 통지들, 사용자 검증들, 및 사용자 패스워드를 포함하는, 소프트웨어 애플리케이션에 의해 이용된 정보의 타입들을 모니터링하거나 분석함으로써 특정 소프트웨어 애플리케이션 (또는 특정 소프트웨어 애플리케이션 타입) 에 의해 이용된 이동 디바이스 특징들을 식별할 수도 있다.

[0125] 다양한 양태들에서, 이동 디바이스 프로세서는 애플리케이션 다운로드 서버로부터의 소프트웨어 다운로드들 중의 하나 이상을 모니터링하거나 분석함으로써 특정 소프트웨어 애플리케이션 (또는 특정 소프트웨어 애플리케이션 타입) 에 의해, 및 제 2 소프트웨어 애플리케이션의 다운로딩 및/또는 설치를 요청하는 제 1 소프트웨어 애플리케이션에 의해 이용된 이동 디바이스 특징들을 식별할 수도 있다.

[0126] 도 3 은 이동 디바이스 (102) 의 프로세싱, 메모리, 또는 에너지 자원들의 과도한 양을 소비하지 않으면서, 이동 디바이스 (102) 상에서 성능-열화하는 이동 디바이스 거동들을 지능적으로 그리고 효율적으로 식별하기 위하여 이동 디바이스 (102) 와 함께 작동하도록 구성된 네트워크 서버 (116) 를 포함하는 시스템 (300) 에서의 일 예의 컴포넌트들 및 정보 흐름들을 예시한다. 도 3 에서 예시된 예에서, 이동 디바이스 (102) 는 특징 선택 및 컬링 모듈 (304), 희박 분류기 모델 생성기 모듈 (306), 및 애플리케이션-기반 분류기 모델 생성기 모듈 (308) 을 포함하고, 애플리케이션-기반 분류기 모델 생성기 모듈 (308) 은 애플리케이션-특정 분류기 모델 생성기 모듈 (310) 및 애플리케이션-타입-특정 분류기 모델 생성기 모듈 (312) 을 포함할 수도 있다. 네트워크 서버 (116) 는 전체 분류기 모델 생성기 모듈 (302) 을 포함한다.

[0127] 모듈들 (304 내지 312) 중의 임의의 것 또는 전부는 실시간 온라인 분류기 모듈일 수도 있고, 및/또는 도 2 에서 예시된 거동 분석기 모듈 (204) 또는 분류기 모듈 (208) 내에 포함될 수도 있다. 일 양태에서, 애플리케이션-기반 분류기 모델 생성기 모듈 (308) 은 희박 분류기 모델 생성기 모듈 (306) 내에 포함될 수도 있다. 다양한 양태들에서, 특징 선택 및 컬링 모듈 (304) 은 애플리케이션-기반 분류기 모델 생성기 모듈 (308) 또는 희박 분류기 모델 생성기 모듈 (306) 내에 포함될 수도 있다.

[0128] 네트워크 서버 (116) 는 클라우드 서비스/네트워크 (118) 로부터 다양한 조건들, 특징들, 거동들, 및 정정 액션들에 관한 정보를 수신하고, 이동 디바이스 (102) 에 의해 하나 이상의 희박 분류기 모델들로 신속하게 변환될 수 있는 포맷 또는 구조인 거동 정보의 대형 코퍼스를 설명하는 전체 분류기 모델을 생성하기 위하여 이 정보를 이용하도록 구성될 수도 있다. 예를 들어, 네트워크 서버 (116) 에서의 전체 분류기 모델 생성기 모듈 (302) 은 거동 정보의 대형 코퍼스의 유한 상태 머신 설명 또는 표시를 포함할 수도 있는 전체 분류기 모델을 생성하기 위하여, 클라우드 서비스/네트워크 (118) 로부터 수신된 거동 벡터들의 클라우드 코퍼스를 이용할 수도 있다. 유한 상태 머신은, 이동 디바이스 거동을 분류하는 것에 관련되는 특징들 및 데이터 포인트들의 전부 또는 다수를 집합적으로 식별하거나, 설명하거나, 테스트하거나, 또는 평가하는 부스팅된 판단 스텀프들의 패밀리와 같은 하나 이상의 판단 노드들로서 표현될 수도 있는 정보 구조일 수도 있다.

[0129] 네트워크 서버 (116) 는 전체 분류기 모델을 이동 디바이스 (102) 로 전송할 수도 있고, 이동 디바이스 (102) 는 감소된 특징 분류기 모델 또는 변동되는 레벨들의 복잡성 또는 희박성의 분류기 모델들의 패밀리를 생성하기 위하여 전체 분류기 모델을 수신하고 이용할 수도 있다. 다양한 양태들에서, 감소된 특징 분류기 모델들은 특징 선택 및 컬링 모듈 (304), 희박 분류기 모델 생성기 모듈 (306), 애플리케이션-기반 분류기 생성기 모듈 (308), 또는 그 임의의 조합에서 생성될 수도 있다. 즉, 이동 디바이스 (102) 의 특징 선택 및 컬링 모듈 (304), 희박 분류기 모델 생성기 모듈 (306), 및/또는 애플리케이션-기반 분류기 생성기 (308) 모듈들은 전체 분류기 모델 내에 포함된 특징들 및 데이터 포인트들의 서브세트를 포함하는 하나 이상의 감소된 특징 분류기 모델들을 생성하기 위하여, 집합적으로 또는 개별적으로, 네트워크 서버로부터 수신된 전체 분류기 모델 내에 포함된 정보를 이용할 수도 있다.

[0130] 예를 들어, 희박 분류기 모델 생성기 모듈 (306) 및 특징 선택 및 컬링 모듈 (304) 은 감소된 수의 부스팅된 판단 스텀프들을 포함하고 및/또는 제한된 수의 테스트 조건들을 평가하는 감소된 특징 분류기 모델을 생성하기 위하여, 네트워크 서버 (116) 로부터 수신된 전체 분류기 모델의 유한 상태 머신 내에 포함된 부스팅된 판단 스텀프들의 로버스트 패밀리를 집합적으로 컬링할 수도 있다. 부스팅된 판단 스텀프들의 로버스트 패밀리의 컬링은 부스팅된 판단 스텀프를 선택함으로써, 선택된 판단 스텀프와 동일한 이동 디바이스 특징을 테스트하거나 이러한 이동 디바이스 특징에 종속되는 모든 다른 부스팅된 판단 스텀프들을 식별함으로써, 그리고 선택된 스텀프와, 동일한 이동 디바이스 특징을 테스트하거나 이에 종속되는 모든 식별된 다른 부스팅된 판단 스텀프들을 정보 구조에 추가함으로써 달성될 수도 있다. 다음으로, 이 프로세스는 제한된 수의 스텀프들 또는 디바이스 특징들에 대해 반복될 수도 있어서, 정보 구조는 작은 또는 제한된 수의 상이한 특징들 또는 조건들을 테스트하거나 이러한 특징들 또는 조건들에 종속되는 전체 분류기 모델에서 모든 부스팅된 판단 스텀프들을 포함한다. 다음으로, 이동 디바이스는 이동 디바이스의 제한된 수의 상이한 특징들 또는 조건들을 테스트하기 위하여, 그리고 그 프로세싱, 메모리, 또는 에너지 자원들의 과도한 양을 소비하지 않으면서 이동 디바이스 거동을 신속하게 분류하기 위하여, 이 정보 구조를 희박 분류기 모델로서 이용할 수도 있다.

[0131] 희박 분류기 모델 생성기 모듈 (306) 은 이동 디바이스와, 이동 디바이스 상에 실행할 수 있는 특정한 소프트웨어 애플리케이션 또는 프로세스에 특정적인 분류기 모델들을 생성하도록 추가로 구성될 수도 있다. 이러한 방식으로, 이동 디바이스에 속하며 소프트웨어 애플리케이션에 대한 특정한 관련성이 있는 특징들 또는 엘리먼트들을 우선적으로 또는 배타적으로 테스트하는 하나 이상의 희박 분류기 모델들이 생성될 수도 있다. 이 디바이스-특정 및 애플리케이션-특정/애플리케이션 타입-특정 희박 분류기 모델들은 애플리케이션에 관련되며 이동 디바이스에 속하는 테스트 조건들을 선택함으로써 하나의 패스 (pass) 에서 희박 분류기 모델 생성기 모듈 (306) 에 의해 생성될 수도 있다. 대안적으로, 희박 분류기 모델 생성기 모듈 (306) 은 이동 디바이스에 속하는 테스트 조건들을 포함하는 디바이스-특정 희박 분류기 모델을 생성할 수도 있고, 이 희박 분류기 모델로부터, 애플리케이션에 관련되는 그 테스트 조건들을 포함하거나 우선순위화하는 추가의 세분화된 모델을 생성할 수도 있다. 추가의 대안으로서, 희박 분류기 모델 생성기 모듈 (306) 은 애플리케이션에 관련되는 희박 분류기 모델을 생성할 수도 있고, 그 다음으로, 이동 디바이스에 관련되지 않는 테스트 조건들을 제거할 수도 있다. 설명의 용이함을 위하여, 디바이스-특정 희박 분류기 모델을 생성하는 프로세스들이 먼저 설명되고, 그 다음으로, 애플리케이션-특정 또는 애플리케이션-타입 특정 희박 분류기 모델을 생성하는 프로세스들이 설명된다.

[0132] 희박 분류기 모델 생성기 모듈 (306) 은 그 특정 이동 디바이스 (102) 의 거동을 분류하는 것에 관련되거나 속하는 이동 디바이스-특정 특징들 (또는 테스트 조건들) 을 식별하기 위하여, 이동 디바이스 (102) 의 디바이스-특정 정보를 이용함으로써 디바이스-특정 분류기 모델들을 생성하도록 구성될 수도 있다. 희박 분류기 모델 생성기 모듈 (306) 은 식별된 이동 디바이스-특정 특징들 또는 테스트 조건들을 우선적으로 또는 배타적으로 포

함하거나, 테스트하거나, 또는 이에 종속되는 희박 분류기 모델들을 생성하기 위하여 이 정보를 이용할 수도 있다. 이동 디바이스 (102) 는 그 프로세싱, 메모리, 또는 에너지 자원들의 과도한 양을 소비하지 않으면서, 이동 디바이스의 거동을 분류하기 위하여 이 국소적으로 생성된 희박 분류기 모델들을 이용할 수도 있다. 즉, 디바이스-특정 또는 디바이스-상태-특정 특징들을 참작하기 위하여 이동 디바이스 (102) 에서 국소적으로 희박 분류기 모델들을 생성함으로써, 다양한 양태들은 이동 디바이스 (102) 가 그 특정 이동 디바이스 (102) 에서의 바람직하지 않은 거동의 소스 또는 원인을 식별하기 위해 가장 중요한 특징들 또는 인자들에 대한 그 모니터링 동작들에 대해 포커싱하도록 한다.

[0133] 희박 분류기 모델 생성기 모듈 (306) 은 또한, 소프트웨어 애플리케이션/프로세스의 오퍼레이팅 시스템 실행 상태가 모니터링된 이동 디바이스 거동들 중의 임의의 것이 악성인지 또는 의심스러운지 여부를 결정하는 것에 관련되는지 여부를 결정하고, 오퍼레이팅 시스템 실행 상태들을 참작하는 특징들 또는 거동들을 포함하거나, 식별하거나, 또는 평가하는 희박 분류기 모델을 생성하도록 구성될 수도 있다. 다음으로, 이동 디바이스 (102) 는 이러한 결정들이 관련되는 소프트웨어 애플리케이션들의 오퍼레이팅 시스템 실행 상태들을 우선적으로 또는 배타적으로 모니터링하기 위하여 이 국소적으로 생성된 희박 분류기 모델들을 이용할 수도 있다. 이것은 이동 디바이스 (102) 가 거동이 양성인지 여부를 더욱 양호하게 예측하기 위하여 그 동작들을 애플리케이션의 가장 중요한 특징들 및 기능들에 포커싱하도록 한다. 즉 선택된 소프트웨어 애플리케이션들 (또는 프로세스들, 스레드들 등) 의 오퍼레이팅 시스템 실행 상태들을 모니터링함으로써, 다양한 양태들은 이동 디바이스 (102) 가 거동이 양성인지 또는 악성인지 여부를 더욱 양호하게 예측하도록 한다. 또한, 소프트웨어 애플리케이션의 오퍼레이팅 시스템 실행 상태가 거동이 양성인지 또는 악성인지 여부의 결정에 관련되는지 여부를 지능적으로 결정 (그리고 이러한 결정들이 관련되는 소프트웨어 애플리케이션들 (또는 프로세스들, 스레드들 등) 을 모니터링하기 위하여 선택) 함으로써, 다양한 양태들은 이동 디바이스 (102) 가 이동 디바이스의 프로세싱, 메모리, 또는 에너지 자원들의 과도한 양을 소비하지 않으면서, 그 동작들을 더욱 양호하게 포커싱하고 성능-열화 거동들/인자들을 식별하도록 한다.

[0134] 일 양태에서, 특징 선택 및 컬링 모듈 (304) 은 "온 더 플라이 (on the fly)" 로, 그리고 이동 디바바이스 (102) 가 재트레이닝을 위하여 클라우드 데이터를 액세스할 것을 요구하지 않으면서, 분류기 모델들의 특징 선택 및 생성을 허용하도록 구성될 수도 있다. 이것은 애플리케이션-기반 분류기 모델 생성기 모듈 (308) 이, 이동 디바이스 (102) 가 특정 소프트웨어 애플리케이션들, 또는 소프트웨어 애플리케이션들의 특정 타입들, 클래스들, 또는 범주들에 관련 있는 특징들을 평가하는 것에 그 동작들을 포커싱하도록 하는 이동 디바이스 (102) 에서의 분류기 모델들을 생성/작성하도록 한다.

[0135] 즉, 애플리케이션-기반 분류기 모델 생성기 모듈 (308)은 이동 디바이스 (102) 가, 특정 소프트웨어 애플리케이션의 동작, 또는 소프트웨어 애플리케이션들의 어떤 타입, 클래스, 또는 범주에 의해 전형적으로 수행되는 동작들과 연관되는 이동 디바이스의 특징들을 우선적으로 또는 배타적으로 테스트하거나 평가하는 고도로 포커싱되고 희박한 분류기 모델들을 생성하고 이용하도록 한다. 이것을 달성하기 위하여, 애플리케이션-기반 분류기 모델 생성기 모듈 (308) 은 남용에 대한 높은 위험이 있고 및/또는 보안에 대한 특수한 필요성을 가지는 소프트웨어 애플리케이션들을 지능적으로 식별할 수도 있고, 이 식별된 애플리케이션들의 각각에 대하여, 애플리케이션이 이 실행 동안에 수행할 수 있거나 수행할 활동들을 결정할 수도 있다. 다음으로, 애플리케이션-특정 모델 생성기 모듈 (308) 은 개별적인 소프트웨어 애플리케이션이 이동 디바이스 (102) 의 성능 열화 거동에 기여하고 있는지, 또는 기여할 가능성이 있는지 여부를 결정함에 있어서 이동 디바이스에 의한 이용을 위해 양호하게 적합한 분류기 모델들을 생성하기 위하여, 이 활동들을 이동 디바이스의 데이터 중심 특징들과 연관시킬 수도 있다.

[0136] 애플리케이션-특정 분류기 모델 생성기 모듈 (308) 은 새로운 애플리케이션이 이동 디바이스에서 설치되거나 업데이트될 때마다 애플리케이션-특정 및/또는 애플리케이션-타입-특정 분류기 모델들을 생성하도록 구성될 수도 있다. 이것은 애플리케이션 특정 모델 생성기 모듈 (310) 및/또는 애플리케이션-타입-특정 모델 생성기 모듈 (312) 을 통해 달성될 수도 있다.

[0137] 애플리케이션-타입-특정 분류기 모델 생성기 모듈 (312) 은 그 소프트웨어 애플리케이션 (예컨대, 게임, 내비게이션, 금융 등) 의 범주, 타입, 또는 분류에 기초하여 특정 소프트웨어 애플리케이션에 대한 분류기 모델을 생성하도록 구성될 수도 있다. 애플리케이션-타입-특정 분류기 모델 생성기 모듈 (312) 은 소프트웨어 애플리케이션과 연관된 애플리케이션 스토어 라벨 (application store label) 을 판독함으로써, 통계 분석 동작들을 수행함으로써, 및/또는 소프트웨어 애플리케이션을 다른 유사한 소프트웨어 애플리케이션들과 비교함으로써, 소

프트웨어 애플리케이션의 범주, 타입, 또는 분류를 결정할 수도 있다.

[0138] 예를 들어, 애플리케이션-타입-특정 분류기 모델 생성기 모듈 (312) 은 제 1 소프트웨어 애플리케이션의 허가들 (예컨대, 오퍼레이팅 시스템, 파일, 액세스 등) 및/또는 API 사용 패턴들을 평가할 수도 있고, 제 1 소프트웨어 애플리케이션이 제 2 소프트웨어 애플리케이션의 것과, 동일한 세트의 허가들을 포함하거나 동일한 세트의 API 들을 사용하는지 여부를 결정하기 위하여, 이 정보를 제 2 소프트웨어 애플리케이션의 허가들 또는 API 사용 패턴과 비교할 수도 있고, 제 1 소프트웨어 애플리케이션이 제 2 소프트웨어 애플리케이션의 것과, 동일한 세트의 허가들을 포함하거나 동일한 세트의 API 들을 사용할 때에 제 1 소프트웨어 애플리케이션에 대한 소프트웨어 애플리케이션 타입 (예컨대, 금융 소프트웨어, 뱅킹 애플리케이션 등) 을 결정하기 위하여 제 2 소프트웨어 애플리케이션의 라벨링 정보 (labeling information) 를 이용할 수도 있다. 다음으로, 애플리케이션-타입-특정 분류기 모델 생성기 모듈 (312) 은 결정된 소프트웨어 애플리케이션 타입에 기초하여 제 1 소프트웨어 애플리케이션을 평가하는데 적합한 분류기 모델을 생성하거나, 업데이트하거나, 또는 선택할 수도 있다. 일 양태에서, 이것은 결정된 소프트웨어 애플리케이션 타입에 기초하여 네트워크 서버 (116) 로부터 수신된 전체 분류기 모델 내에 포함된 판단 노드들을 컬링함으로써 달성될 수도 있다.

[0139] 애플리케이션-특정 분류기 모델 생성기 모듈 (310) 은 라벨링 정보, 정적 분석, 설치 시간 분석에 기초하여, 또는 소프트웨어 애플리케이션의 오퍼레이팅 시스템, 파일, 및/또는 액세스 허가들을 결정함으로써, 특정 소프트웨어 애플리케이션에 대한 분류기 모델을 생성하도록 구성될 수도 있다. 예를 들어, 이동 디바이스는 소프트웨어 애플리케이션이 업데이트될 때마다 소프트웨어 애플리케이션의 정적 분석을 수행할 수도 있고, 이 분석의 결과들을 이동 디바이스의 메모리 내에 저장할 수도 있고, 그 애플리케이션이 의심스러운 이동 디바이스 거동에 기여하고 있는지 여부를 결정하기 위해 가장 중요한 이동 디바이스 조건들 또는 인자들을 결정하기 위하여 이 정보를 이용할 수도 있고, 가장 중요한 조건들 또는 인자들을 테스트하는 노드들을 포함하기 위하여 전체 분류기 모델 내에 포함된 판단 노드들을 컬링할 수도 있다.

[0140] 도 4 는 이동 디바이스 (102) 에서 애플리케이션-특정 및/또는 애플리케이션-타입-특정 분류기 모델들을 생성하는 일 양태의 방법 (400) 을 예시한다. 방법 (400) 은 이동 디바이스 (102) 의 프로세싱 코어에 의해 수행될 수도 있다.

[0141] 블록 (402) 에서, 프로세싱 코어는, 이동 디바이스 거동이 시간 경과에 따른 이동 디바이스 (102) 의 성능에 있어서의 열화 또는 전력 소비 특성들에 양성인지 또는 이에 기여하고 있는지 여부를 결정하는 것에 관련되는 특징들 및 데이터 포인트들의 전부 또는 다수를 집합적으로 식별하거나, 설명하거나, 테스트하거나, 또는 평가하는 많은 수의 판단 노드들 (448) 을 생성하기 위하여 전체 분류기 모델 (452) 내에 포함된 정보를 이용할 수도 있다. 예를 들어, 블록 (402) 에서, 프로세싱 코어는 사십 (40) 개의 고유한 조건들을 테스트하는 백 (100) 개의 판단 노드들 (448) 을 생성할 수도 있다.

[0142] 일 양태에서, 판단 노드들 (448) 은 판단 스텀프들 (예컨대, 부스팅된 판단 스텀프들 등) 일 수도 있다. 각각의 판단 스텀프는 하나의 조건 또는 이동 디바이스 특징을 테스트하는 정확하게 하나의 노드를 가지는 1 레벨 판단 트리일 수도 있다. 판단 스텀프에는 하나의 노드만이 있으므로, 특징 벡터를 판단 스텀프에 적용하는 것은 이진 답변 (예컨대, 예 또는 아니오, 악성 또는 양성 등) 으로 귀착된다. 예를 들어, 판단 스텀프 (448b) 에 의해 테스팅된 조건이 "SMS 송신들의 빈도가 분 당 x 미만인가" 일 경우, "3" 의 값을 판단 스텀프 (448b) 에 적용하는 것은 ("3 미만" SMS 송신들에 대해) "예" 답변, 또는 ("3 이상" SMS 송신들에 대해) "아니오" 답변의 어느 하나로 귀착될 것이다. 다음으로, 이 이진 "예" 또는 "아니오" 답변은 결과를 거동이 악성 (M) 또는 양성 (B) 의 어느 하나인 것을 표시하는 것으로서 분류하기 위하여 이용될 수도 있다. 이 스텀프들은 매우 간단한 평가들 (기본적으로 이진) 이므로, 각각의 스텀프를 수행하기 위한 프로세싱은 매우 간단하고, 적은 프로세싱 오버헤드 (overhead) 로 신속하게 및/또는 병렬로 달성될 수 있다.

[0143] 일 양태에서, 각각의 판단 노드 (448) 는 얼마나 많은 지식이 테스트 질문에 답변하는 것으로부터 얻어지는지를 표시하는 가중 값, 및/또는 테스트 조건에 답변하는 것이 프로세싱 코어가 이동 디바이스 거동이 양성인지 여부를 결정하는 것을 가능하게 할 가능성과 연관될 수도 있다. 판단 노드 (448) 와 연관된 가중은 이동 디바이스 거동들, 소프트웨어 애플리케이션들, 또는 이동 디바이스에서의 프로세스들의 이전의 관측들 또는 분석으로부터 수집된 정보에 기초하여 연산될 수도 있다. 일 양태에서, 각각의 판단 노드 (448) 와 연관된 가중은 또한, 데이터의 코퍼스 (예컨대, 데이터 또는 거동 벡터들의 클라우드 코퍼스) 의 얼마나 많은 유닛들이 노드를 구축하기 위하여 이용되는지에 기초하여 연산될 수도 있다. 일 양태에서, 가중 값들은 이전의 데이터/거동 모델들 또는 분류기들의 실행/적용으로부터 수집된 정확성 또는 성능 정보에 기초하여 생성될 수도 있다.

[0144] 도 4 를 참조하면, 블록 (404) 에서, 프로세싱 코어는 전체 분류기 모델 (452) 내에 포함된 판단 노드들 (448) 의 포커싱된 서브세트를 포함하는 희박 분류기 모델 (454) 을 생성할 수도 있다. 이것을 달성하기 위하여, 프로세싱 코어는, 전체 분류기 모델 (452) 내에 포함된 판단 노드들 (448) 의 순서화되거나 우선순위화된 리스트를 생성하는 것, 이동 디바이스 (102) 의 프로세싱, 메모리, 또는 에너지 자원들의 과도한 양을 소비하지 않으면서, 이동 디바이스 거동을 분류하기 위하여 평가되어야 하는 다수의 고유한 테스트 조건들을 결정하는 것, 판단 노드들 (448) 의 순서화된/우선순위화된 리스트를 순차적으로 트래버싱함으로써 테스트 조건들의 리스트를 생성하고, 테스트 조건들의 리스트가 결정된 수의 고유한 테스트 조건들을 포함할 때까지, 각각의 순차적으로 통과된 판단 노드 (448) 와 연관된 테스트 조건을 테스트 조건들의 리스트 내로 삽입하는 것, 및 테스트 조건들의 생성된 리스트 내에 포함된 복수의 테스트 조건들 중의 하나를 테스트하는 판단 노드들 (448) 을 우선적으로 또는 배타적으로 포함하는 정보 구조를 생성하는 것을 포함할 수도 있는 특징 선택 동작들을 수행할 수도 있다.

일 양태에서, 프로세싱 코어는, 분류기 모델들의 패밀리에서의 각각의 모델 (454) 이 상이한 수의 고유한 테스트 조건들을 평가하고 및/또는 상이한 수의 판단 노드들을 포함하도록 패밀리 분류기 모델들을 생성할 수도 있다.

[0145] 블록 (406) 에서, 프로세싱 코어는, 예컨대, API 들을 어드레싱하는 판단 노드들, 또는 애플리케이션에 의해 호출되거나 소환되지 않는 함수들을 누락할 뿐만 아니라, 애플리케이션에 의해 액세스되거나 수정되지 않는 디바이스 자원들에 관한 판단 노드들을 누락함으로써, 특정 소프트웨어 애플리케이션 (즉, Google® 지갑) 에 관련되는 조건들 또는 특징들을 테스트하거나 평가하는 희박 분류기 모델 (454) 에서의 판단 노드들을 우선적으로 또는 배타적으로 포함하는 애플리케이션-특정 분류기 모델 (456) 을 생성하기 위하여, 희박 분류기 모델들 (454) 중의 하나 내에 포함된 판단 노드들 (즉, 부스팅된 판단 스텀프들) 을 트리밍하거나, 컬링하거나, 또는 프루닝할 수도 있다. 일 양태에서, 프로세싱 코어는 특징 선택 및 컬링 동작들을 수행함으로써 애플리케이션-특정 분류기 모델 (456) 을 생성할 수도 있다. 다양한 양태들에서, 프로세싱 코어는 소프트웨어 애플리케이션과 연관된 라벨링 정보, 애플리케이션 상에서의 정적 분석 동작들을 수행하는 결과들, 애플리케이션의 설치 시간 분석을 수행하는 결과들에 기초하여, 소프트웨어 애플리케이션의 오퍼레이팅 시스템, 파일, 및/또는 액세스 허가들을 평가함으로써, 애플리케이션의 API 사용을 평가함으로써 등에 의해, 애플리케이션-특정 분류기 모델 (456) 내에 포함하기 위한 판단 노드들 (448) 을 식별할 수도 있다.

[0146] 일 양태에서는, 블록 (406) 에서, 프로세싱 코어가 복수의 애플리케이션-특정 분류기 모델들 (456) 을 생성할 수도 있고, 애플리케이션-특정 분류기 모델들 (456) 의 각각은 상이한 소프트웨어 애플리케이션을 평가한다.

일 양태에서, 프로세싱 코어는 시스템에서의 모든 소프트웨어 애플리케이션에 대하여, 및/또는 이동 디바이스 상에서 실행되는 모든 애플리케이션이 그 자신의 능동적인 분류기를 가지도록, 애플리케이션-특정 분류기 모델 (456) 을 생성할 수도 있다. 일 양태에서는, 블록 (406) 에서, 프로세싱 코어가 애플리케이션-특정 분류기 모델들 (456) 의 패밀리를 생성할 수도 있다. 애플리케이션-특정 분류기 모델들 (456) 의 패밀리에서의 각각의 애플리케이션-특정 분류기 모델 (456) 은 단일 소프트웨어 애플리케이션에 관련되는 상이한 조합 또는 수의 특징들을 평가할 수도 있다.

[0147] 블록 (408) 에서, 프로세싱 코어는 애플리케이션-타입-특정 분류기 모델들 (458) 을 생성하기 위하여, 희박 분류기 모델들 (454) 중의 하나 내에 포함된 판단 노드들 (즉, 부스팅된 판단 스텀프들) 을 트리밍하거나, 컬링하거나, 또는 프루닝할 수도 있다. 생성된 애플리케이션-타입 특정 분류기 모델들 (458) 은 소프트웨어 애플리케이션들 (예컨대, 게임, 내비게이션, 금융 등) 의 특정 타입, 범주, 또는 클래스에 관련되는 조건들 또는 특징들을 테스트하거나 평가하는 전체 또는 희박 분류기 모델들 (452, 454) 내에 포함되는 판단 노드들을 우선적으로 또는 배타적으로 포함할 수도 있다. 일 양태에서, 프로세싱 코어는 특징 선택 및 컬링 동작들을 수행함으로써 애플리케이션-타입 특정 분류기 모델 (458) 내에 포함하기 위한 판단 노드들을 식별할 수도 있다. 일 양태에서, 프로세싱 코어는 각각의 소프트웨어 애플리케이션의 범주, 타입, 또는 분류를 결정할 수도 있고, 및/또는 소프트웨어 애플리케이션과 연관된 애플리케이션 스토어 라벨을 판독함으로써, 정적 분석 동작들을 수행함으로써, 및/또는 소프트웨어 애플리케이션을 다른 유사한 소프트웨어 애플리케이션들과 비교함으로써, 애플리케이션-타입-특정 분류기 모델 (456) 내에 포함되어야 하는 판단 노드들 (448) 을 식별할 수도 있다.

[0148] 블록 (410) 에서, 프로세싱 코어는 실시간 거동 모니터링 및 분석 동작들을 수행하기 위하여 국소적으로 생성된 분류기 모델들 (454, 456, 458) 중의 하나 또는 임의의 조합을 이용할 수도 있고, 복잡한 이동 디바이스 거동이 양성인지, 또는 이동 디바이스의 성능의 열화 또는 전력 소비 특성들에 기여하는지 여부를 예측할 수도 있다.

일 양태에서, 이동 디바이스는 다수의 분류기 모델들 (454, 456, 458) 을 병렬로 이용하거나 적용하도록 구성될 수도 있다. 일 양태에서, 프로세싱 코어는 특정 소프트웨어 애플리케이션을 평가할 때에 희박 분류기

모델 (454) 을 적용/이용하는 것으로부터 생성된 결과들에 비해, 애플리케이션-기반 분류기 모델들 (456, 458) 을 적용하거나 이용하는 것으로부터 생성된 결과들에 선호도 또는 우선순위를 부여할 수도 있다. 프로세싱 코어는 복잡한 이동 디바이스 거동이 양성인지, 시간 경과에 따른 이동 디바이스의 성능의 열화 또는 전력 소비 특성들에 기여하는지 여부를 예측하기 위하여, 분류기 모델들을 적용하는 결과들을 이용할 수도 있다.

[0149] 애플리케이션-특정 또는 애플리케이션-타입-특정 특징들 및/또는 기능성을 참작하기 위하여 이동 디바이스에서 국소적으로 애플리케이션-기반 분류기 모델들 (456, 458) 을 동적으로 생성함으로써, 다양한 양태들은 이동 디바이스 (102) 가 그 모니터링 동작들을, 특정 소프트웨어 애플리케이션의 동작들이 이동 디바이스의 바람직하지 않거나 성능 열화하는 거동에 기여하고 있는지 여부를 결정하기 위해 가장 중요한 작은 수의 특징들에 대해 포커싱하도록 한다. 이것은 이동 디바이스 (102) 의 성능 및 전력 소비 특성들을 개선시키고, 이동 디바이스가 그 프로세싱, 메모리, 또는 에너지 자원들의 과도한 양을 소비하지 않으면서, 연속적으로 또는 거의 연속적으로 실시간 거동 모니터링 및 분석 동작들을 수행하도록 한다.

[0150] 도 5a 는 거동 벡터를 다수의 애플리케이션-기반 분류기 모델들에 병렬로 적용하기 위하여 일 양태의 이동 디바이스 (102) 에 의해 이용될 수도 있는 일 예의 분류기 모델 (500) 을 예시한다. 분류기 모델 (500) 은 전체 분류기 모델 또는 국소적으로 생성된 희박 분류기 모델일 수도 있다. 분류기 모델 (500) 은 하나 이상의 소프트웨어 애플리케이션들 App1 내지 App5 와 연관되는 복수의 판단 노드들 (502 내지 514) 을 포함할 수도 있다. 예를 들어, 도 5a 에서, 판단 노드 (502) 는 소프트웨어 애플리케이션들 App1, App2, App4, 및 App5 와 연관되고, 판단 노드 (504) 는 App1 과 연관되고, 판단 노드 (506) 는 App1 및 App2 와 연관되고, 판단 노드 (508) 는 소프트웨어 애플리케이션들 App1, App2, App4, 및 App5 와 연관되고, 판단 노드 (510) 는 소프트웨어 애플리케이션들 App1, App2, 및 App5 와 연관되고, 판단 노드 (512) 는 소프트웨어 애플리케이션들 App1 과 연관되고, 판단 노드 (514) 는 소프트웨어 애플리케이션들 App1, App2, App4, 및 App5 와 연관된다.

[0151] 일 양태에서, 이동 디바이스에서의 프로세싱 코어는 분류기 모델 (500) 을 복수의 애플리케이션-기반 분류기 모델들로 파티셔닝하기 위하여 판단 노드들 (502 내지 514) 과 소프트웨어 애플리케이션들 App1 내지 App5 사이의 맵핑 (mapping) 들을 이용하도록 구성될 수도 있다. 예를 들어, 프로세서는, App1 에 대한 애플리케이션-기반 분류기가 판단 노드들 (502 내지 514) 을 포함해야 하는 반면, App2 에 대한 애플리케이션-기반 분류기가 판단 노드들 (502, 506, 508, 510, 및 514) 을 포함해야 하는 것으로 결정하기 위하여 맵핑들을 이용할 수도 있다. 즉, 각각의 소프트웨어 애플리케이션에 대해 상이한 분류기 모델을 생성하고 실행하는 것이 아니라, 프로세싱 코어는 모든 분류기들에 대해 판단 노드들 (502 내지 514) 의 동일한 세트를 실행하기 위하여 거동 벡터를 분류기 모델 (500) 내에 포함된 모든 판단 노드들 (502 내지 514) 에 적용할 수도 있다. 각각의 애플리케이션 App1 내지 App5 에 대하여, 이동 디바이스는, 애플리케이션 App1 내지 App5 에 관련되는 판단 노드들 (502 내지 514) 이 그 애플리케이션이 실행되고 있을 때에 디바이스 거동들을 평가하기 위하여 이용되거나 우선순위화되도록, 마스크 (예컨대, 0-1 (zero-one) 마스크) 를 분류기 모델 (500) 에 적용할 수도 있다.

[0152] 일 양태에서, 이동 디바이스는 그 대응하는 애플리케이션 App1 내지 App5 에 대한 그 관련성에 기초하여 판단 노드들 (502 내지 514) 에 대한 상이한 가중 값들 또는 상이한 가중화된 평균들을 계산할 수도 있다. 멀웨어/양성 값에 대한 이러한 신뢰성을 연산하는 것은 다수의 판단 노드들 (502 내지 514) 을 평가하는 것과, 그 가중 값들의 가중화된 평균을 취하는 것을 포함할 수도 있다. 일 양태에서, 이동 디바이스는 동일하거나 상이한 희박 분류기들에 대해 신뢰성 값을 연산할 수도 있다. 일 양태에서, 이동 디바이스는 분류기를 구성하는 판단 노드들 (502 내지 514) 의 각각의 조합에 대한 상이한 가중화된 평균들을 연산할 수도 있다.

[0153] 도 5b 는 이동 디바이스의 애플리케이션-특정 및 애플리케이션-타입-특정 특징들을 참작하는 분류기 모델들을 생성하는 일 양태의 방법 (510) 을 예시한다. 방법 (510) 은 이동 디바이스에서의 프로세싱 코어에 의해 수행될 수도 있다.

[0154] 블록 (512) 에서, 프로세싱 코어는 감소된 수의 판단 노드들 및 특징들/테스트 조건들을 포함하는 희박 분류기 모델을 생성하기 위하여 합동 특징 선택 및 컬링 (joint feature selection and culling; JFSP) 동작들을 수행할 수도 있다. 블록 (518) 에서, 프로세싱 코어는 이동 디바이스의 거동을 분류하는 것에 대한 그 관련성에 따라 특징들/테스트 조건들을 우선순위화하거나 등급화 (rank) 할 수도 있다.

[0155] 블록 (514) 에서, 프로세싱 코어는 그 애플리케이션의 허가 세트 {Fper} 를 평가함으로써 소프트웨어 애플리케이션에 대한 특징/테스트 조건들을 유도하거나 결정할 수도 있다. 블록 (516) 에서, 프로세싱 코어는 그 애플리케이션 상에서 정적 또는 설치 시간 분석을 수행하는 결과들을 평가함으로써 소프트웨어 애플리케이션에 대한 특징들 또는 테스트 조건들의 세트 {Finstall} 를 결정할 수도 있다. 블록 (520) 에서, 프로세싱 코어는

이동 디바이스의 거동을 분류하는 것에 대한 그 관련성에 따라 각각의 애플리케이션에 대한 특징들/테스트 조건들을 우선순위화하거나 등급화할 수도 있다. 일 양태에서, 이것은 공식을 통해 달성될 수도 있다:

[0156] {Fapp} = {Fper} U {Finstall}

[0157] 블록 (522) 에서, 프로세싱 코어는 JFSP 를 순서화 함수로서 이용함으로써 애플리케이션 특징들 {Fapp} 마다 우선순위화하거나 등급화할 수도 있다. 예를 들어, 프로세싱 코어는 블록 (518) 에서 생성된 희박 분류기에 대한 JFSP 동작들을 수행할 수도 있다. 블록 (524) 에서, 프로세싱 코어는 애플리케이션 특징들 {Fapp} 마다의 등급화된 리스트를 생성할 수도 있다. 블록 (526) 에서, 프로세싱 코어는 관심 있는 특징들을 선택하기 위하여 JFSP 를 적용할 수도 있다. 블록 (528) 에서, 프로세싱 코어는 관심 있는 특징들을 포함하기 위하여 애플리케이션 마다 희박 분류기 모델을 생성할 수도 있다.

[0158] 도 6 은 이동 디바이스의 애플리케이션-특정 및 애플리케이션-타입-특정 특징들을 참작하는 희박 또는 포커싱된 분류기/거동 모델들을 생성하는 일 양태의 방법 (600) 을 예시한다.

[0159] 방법 (600) 의 블록 (602) 에서, 프로세싱 코어는, 유한 상태 머신, 부스팅된 판단 트리들의 리스트, 복수의 테스트 조건들을 식별하는 스텀프들 또는 다른 유사한 정보 구조이거나 이를 포함하는 전체 분류기 모델을 수신할 수도 있다. 일 양태에서, 전체 분류기 모델은, 복수의 부스팅된 판단 스텀프들을 표현하는데 적합한 정보를 포함하고, 및/또는 복수의 부스팅된 판단 스텀프들로의 이동 디바이스에 의한 변환에 적합한 정보를 포함하는 유한 상태 머신을 포함한다. 일 양태에서, 유한 상태 머신은 부스팅된 판단 스텀프들의 순서화된 또는 우선순위화된 리스트일 수도 있다 (또는 이를 포함할 수도 있음). 부스팅된 판단 스텀프들의 각각은 테스트 조건 및 가중 값을 포함할 수도 있다.

[0160] 블록 (604) 에서, 프로세싱 코어는 이동 디바이스의 프로세싱, 메모리, 또는 에너지 자원들의 과도한 양을 소비하지 않으면서, 이동 디바이스 거동을 악성 또는 양성의 어느 하나인 것으로서 정확하게 분류하기 위하여 평가되어야 하는 다수의 고유한 테스트 조건들을 결정할 수도 있다. 이것은 이동 디바이스에서 이용가능한 프로세싱, 메모리, 및/또는 에너지 자원들의 양으로서, 조건을 테스트하기 위하여 요구되는 이동 디바이스의 프로세싱, 메모리, 또는 에너지 자원들의 양을 결정하는 것, 조건을 테스트함으로써 이동 디바이스에서 분석되거나 평가되어야 하는 거동 또는 조건과 연관된 우선순위 및/또는 복잡성을 결정하는 것, 및 이동 디바이스의 이용가능한 프로세싱, 메모리, 또는 메모리 자원들의 소비, 조건을 테스트하는 것으로부터 달성되어야 하는 거동 분류의 정확성, 및 조건에 의해 테스트되는 거동의 중요도 또는 우선순위 사이의 균형 또는 절충을 유지하도록 다수의 고유한 테스트 조건들을 선택/결정하는 것을 포함할 수도 있다.

[0161] 블록 (606) 에서, 프로세싱 코어는 희박 분류기 모델들에 포함되거나 이로부터 제외되어야 하는 특징들 및/또는 테스트 조건들을 신속하게 식별하기 위하여 디바이스-특정 또는 디바이스-상태-특정 정보를 이용할 수도 있다. 예를 들어, 프로세싱 코어는 이동 디바이스의 현재의 하드웨어 또는 소프트웨어 구성, 동작 상태 등으로 인해 이동 디바이스에서 존재할 수 없는 조건들, 특징들, 또는 인자들을 테스트하는 테스트 조건들을 식별할 수도 있다. 또 다른 예로서, 프로세싱 코어는 전체 모델 내에 포함되는 특징들/노드들/스텀프들과, 이동 디바이스에서 존재할 수 없고 및/또는 이동 디바이스에 관련되지 않는 테스트 조건들을 식별할 수도 있고 이들을 희박 분류기 모델들로부터 제외할 수도 있다.

[0162] 일 양태에서는, 블록 (608) 에서, 프로세싱 코어가 선택된 테스트 조건들의 리스트를 결정된 수의 고유한 테스트 조건들로 파퓰레이팅 (populate) 하기 위하여, 그리고 블록 (606) 에서 식별된 테스트 조건들을 제외하기 위하여 초반부로부터 부스팅된 판단 스텀프들의 리스트를 통과할 수도 있다. 예를 들어, 프로세싱 코어는 소프트웨어 애플리케이션에 의해 이용될 수 없는 조건들을 테스트하는 전체 분류기 모델 내에 포함된 특징들을 스킵 (skip) 하거나, 무시하거나, 또는 삭제할 수도 있다. 일 양태에서, 프로세싱 코어는 또한, 선택된 테스트 조건들의 각각에 대한 절대적 또는 상대적 우선순위 값을 결정할 수도 있고, 선택된 테스트 조건들의 리스트에서 그 대응하는 테스트 조건들과 연관하여 절대적 또는 상대적 우선순위들 값을 저장할 수도 있다.

[0163] 일 양태에서는, 블록 (608) 에서, 프로세싱 코어가 전체 분류기 모델에서 복수의 테스트 조건들을 순차적으로 트래버싱함으로써 테스트 조건들의 리스트를 생성하고 테스트 조건들의 리스트가 결정된 수의 고유한 테스트 조건들을 포함할 때까지, 이동 디바이스의 거동을 분류하는 것에 관련되는 그 테스트 조건들을 테스트 조건들의 리스트 내로 삽입할 수도 있다. 추가의 양태에서, 테스트 조건들의 리스트를 생성하는 것은 전체 분류기 모델의 판단 노드들을 순차적으로 통과하는 것, 소프트웨어 애플리케이션에 관련되지 않는 테스트 조건들과 연관된 판단 노드들을 무시하는 것, 및 테스트 조건들의 리스트가 결정된 수의 고유한 테스트 조건들을 포함할 때까

지, 무시되지 않는 각각의 순차적으로 통과된 판단 노드와 연관된 테스트 조건들을 테스트 조건들의 리스트 내로 삽입하는 것을 포함할 수도 있다.

[0164] 블록 (610) 에서, 프로세싱 코어는 테스트 조건들의 생성된 리스트에서 식별된 선택된 테스트 조건들 중의 하나를 테스트하는 (그리고 이에 따라, 블록 (606) 에서 식별된 테스트 조건들을 제외함) 전체 분류기 모델 내에 포함된 모든 부스팅된 판단 스텀프들을 포함하는 희박 분류기 모델을 생성할 수도 있다. 일 양태에서, 프로세싱 코어는 부스팅된 판단 스텀프들을 그 중요도 또는 우선순위 값의 순서로 포함하거나 표현하기 위하여 희박 분류기 모델을 생성할 수도 있다. 일 양태에서는, 블록 (610) 에서, 프로세싱 코어가 블록 (608) 에서 더 많은 수의 테스트 조건들에 대한 부스팅된 판단 스텀프들의 리스트를 통과하고 또 다른 희박 분류기 모드를 생성하는 동작들을 반복함으로써 또 다른 더욱 로버스트 (즉, 덜 희박한) 희박 분류기 모델을 생성하기 위하여 고유한 테스트 조건들의 수를 감소시킬 수도 있다. 이 동작들은 희박 분류기 모델들의 패밀리를 생성하기 위하여 반복될 수도 있다.

[0165] 블록 (612) 에서, 프로세싱 코어는, 희박 분류기 모델 내에 포함되고, 소프트웨어 애플리케이션이 이동 디바이스의 성능 열화 거동에 기여하고 있는지 여부를 결정하는 것에 관련되는 특징들 또는 테스트 조건들을 식별하기 위하여, 애플리케이션-특정 정보 및/또는 애플리케이션-타입 특정 정보를 이용할 수도 있다. 블록 (614) 에서, 프로세싱 코어는 희박 분류기 모델에서 부스팅된 판단 스텀프들을 통과할 수도 있고 소프트웨어 애플리케이션에 의해 이용되는 특징 또는 조건을 테스트하는 판단 스텀프들을 선택하거나 그 소프트웨어 애플리케이션에 맵핑할 수도 있고, 선택되거나 맵핑된 판단 스텀프들을 애플리케이션-특정 분류기 모델 또는 애플리케이션-타입-특정 분류기 모델로서 이용할 수도 있다.

[0166] 도 7 은 이동 디바이스의 거동을 분류하기 위하여 희박 분류기 모델을 이용하는 일 양태의 방법 (700) 을 예시한다. 방법 (700) 은 이동 디바이스에서의 프로세싱 코어에 의해 수행될 수도 있다.

[0167] 블록 (702) 에서, 프로세싱 코어는 이동 디바이스 시스템의 다양한 레벨들에서 장치화되는 다양한 컴포넌트들로부터 거동 정보를 수집하기 위하여 관측들을 수행할 수도 있다. 일 양태에서, 이것은 도 2 를 참조하여 위에서 논의된 거동 관측기 모듈 (202) 을 통해 달성될 수도 있다. 블록 (704) 에서, 프로세싱 코어는 관측들, 수집된 거동 정보, 및/또는 이동 디바이스 거동을 특징화하는 거동 벡터를 생성할 수도 있다. 또한, 블록 (704) 에서, 프로세싱 코어는 변동되는 레벨들의 복잡성 (또는 "희박성") 의 희박 분류기 모델 또는 희박 분류기 모델들의 패밀리를 생성하기 위하여 네트워크 서버로부터 수신된 전체 분류기 모델을 이용할 수도 있다. 이것을 달성하기 위하여, 프로세싱 코어는, 감소된 수의 부스팅된 판단 스텀프들을 포함하고 및/또는 제한된 수의 테스트 조건들을 평가하는 희박 분류기 모델들을 생성하기 위하여 전체 분류기 모델 내에 포함된 부스팅된 판단 스텀프들의 패밀리를 컬링할 수도 있다.

[0168] 블록 (706) 에서, 프로세싱 코어는 이동 디바이스에 의해 아직 평가되거나 적용되지 않았던 희박 분류기 모델들의 패밀리에서의 가장 희박한 분류기 (즉, 가장 적은 수의 상이한 이동 디바이스 상태들, 특징들, 거동들, 또는 조건들에 기초한 모델) 를 선택할 수도 있다. 일 양태에서, 이것은 분류기 모델들의 순서화된 리스트에서 제 1 분류기 모델을 선택하는 프로세싱 코어에 의해 달성될 수도 있다.

[0169] 블록 (708) 에서, 프로세싱 코어는 수집된 거동 정보 또는 거동 벡터들을 선택된 희박 분류기 모델에서의 각각의 부스팅된 판단 스텀프에 적용할 수도 있다. 부스팅된 판단 스텀프들은 이진 판단들이고 희박 분류기 모델은 동일한 테스트 조건에 기초하는 다수의 이진 판단들을 선택함으로써 생성되므로, 거동 벡터를 희박 분류기 모델에서 부스팅된 판단 스텀프들에 적용하는 프로세스는 병렬 동작으로 수행될 수도 있다. 대안적으로, 블록 (530) 에서 적용된 거동 벡터는 희박 분류기 모델 내에 포함된 제한된 수의 테스트 조건 파라미터들을 단지 포함하기 위하여 절단되거나 필터링될 수도 있음으로써, 모델을 적용함에 있어서 연산 노력을 추가로 감소시킬 수도 있다.

[0170] 블록 (710) 에서, 프로세싱 코어는 수집된 거동 정보를 희박 분류기 모델에서 각각의 부스팅된 판단 스텀프에 적용하는 결과들의 가중화된 평균을 연산하거나 결정할 수도 있다. 블록 (712) 에서, 프로세싱 코어는 연산된 가중화된 평균을 임계 값과 비교할 수도 있다. 결정 블록 (714) 에서, 프로세싱 코어는 이 비교의 결과들 및/또는 선택된 희박 분류기 모델을 적용함으로써 생성된 결과들이 의심스러운지 여부를 결정할 수도 있다.
예를 들어, 프로세싱 코어는 이 결과들이 높은 신뢰성의 정도로 거동을 악성 또는 양성의 어느 하나로서 분류하기 위하여 이용될 수도 있는지 여부를 결정할 수도 있고, 그렇지 않을 경우, 거동을 의심스러운 것으로서 취급할 수도 있다.

[0171] 프로세싱 코어가 결과들이 의심스러운 것으로 결정할 경우 (예컨대, 결정 블록 (714) = "예"), 프로세싱 코어는 거동이 높은 신뢰성의 정도로 악성 또는 양성으로서 분류될 때까지 더 많은 디바이스 상태들, 특징들, 거동들, 또는 조건들을 평가하는 더 강력한 (즉, 덜 희박한) 분류기 모델을 선택하고 적용하기 위하여, 블록들 (706 내지 712) 에서의 동작들을 반복할 수도 있다. 프로세싱 코어가 예컨대, 거동이 높은 신뢰성의 정도로 악성 또는 양성의 어느 하나로서 분류될 수 있는 것으로 결정함으로써, 결과들이 의심스럽지 않은 것으로 결정할 경우 (예컨대, 결정 블록 (714) = "아니오"), 블록 (716) 에서, 프로세싱 코어는 이동 디바이스의 거동을 양성 또는 잠재적으로 악성으로서 분류하기 위하여 블록 (712) 에서 생성된 비교의 결과를 이용할 수도 있다.

[0172] 대안적인 양태의 방법에서, 위에서 설명된 동작들은 이미 희박 분류기 모델에 있지 않은 부스팅된 판단 스텀프를 순차적으로 선택함으로써; 선택된 판단 스텀프와 동일한 이동 디바이스 상태, 특징, 거동, 또는 조건에 종속되는 (그리고 이에 따라, 하나의 결정 결과에 기초하여 적용될 수 있는) 모든 다른 부스팅된 판단 스텀프들을 식별함으로써; 동일한 이동 디바이스 상태, 특징, 거동, 또는 조건에 종속되는 선택된 그리고 모든 식별된 다른 부스팅된 판단 스텀프들을 희박 분류기 모델에서 포함함으로써; 그리고 결정된 수의 테스트 조건들과 동일한 횟수 동안 프로세스를 반복함으로써 달성될 수도 있다. 선택된 부스팅된 판단 스텀프와 동일한 테스트 조건에 종속되는 모든 부스팅된 판단 스텀프들이 그때마다 희박 분류기 모델에 추가되므로, 이 프로세스가 수행되는 횟수를 제한하는 것은 희박 분류기 모델 내에 포함된 테스트 조건들의 수를 제한할 것이다.

[0173] 도 8 은 다양한 양태들에 따라 이용하는데 적합한 부스팅된 판단 트리/분류기를 생성하는데 적합한 일 예의 부스팅 방법 (800) 을 예시한다. 동작 (802) 에서, 프로세서는 판단 트리/분류기를 생성 및/또는 실행할 수도 잇고, 판단 트리/분류기의 실행으로부터 트레이닝 샘플 (training sample) 을 수집할 수도 있고, 트레이닝 샘플에 기초하여 새로운 분류기 모델 (h1(x)) 을 생성할 수도 있다. 트레이닝 샘플은 이동 디바이스에서의 이동 디바이스 거동들, 소프트웨어 애플리케이션들, 또는 프로세스들의 이전의 관측들 또는 분석으로부터 수집된 정보를 포함할 수도 있다. 트레이닝 샘플 및/또는 새로운 분류기 모델 (h1(x)) 은 이전의 분류기들 내에 포함된 질문 또는 테스트 조건들의 타입들에 기초하여, 및/또는 거동 분석기 모듈 (204) 의 분류기 모듈 (208) 에서의 이전의 데이터/거동 모델들 또는 분류기들의 실행/적용으로부터 수집된 정확성 또는 성능 특성들에 기초하여 생성될 수도 있다. 동작 (804) 에서, 프로세서는 제 2 의 새로운 트리/분류기 (h2(x)) 를 생성하기 위하여, 생성된 판단 트리/분류기 (h1(x)) 에 의해 오분류 (misclassify) 되었던 엔트리들의 가중을 부스팅 (또는 증가) 할 수도 있다. 일 양태에서, 트레이닝 샘플 및/또는 새로운 분류기 모델 (h2(x)) 은 분류기의 이전의 실행 또는 이용 (h1(x)) 의 오류 레이트에 기초하여 생성될 수도 있다. 일 양태에서, 트레이닝 샘플 및/또는 새로운 분류기 모델 (h2(x)) 은 분류기의 이전의 실행 또는 이용에서 데이터 포인트들의 오류 레이트 또는 오분류에 기여되었던 것을 가지는 것으로 결정된 속성들에 기초하여 생성될 수도 있다.

[0174] 일 양태에서, 오분류된 엔트리들은 그 상대적 정확성 또는 유효성에 기초하여 가중화될 수도 있다. 동작 (806) 에서, 프로세서는 제 3 의 새로운 트리/분류기 (h3(x)) 를 생성하기 위하여, 생성된 제 2 트리/분류기 (h2(x)) 에 의해 오분류되었던 엔트리들의 가중을 부스팅 (또는 증가) 할 수도 있다. 동작 (808) 에서, 804 내지 806 의 동작들은 "t" 개의 새로운 트리/분류기들 ($h_t(x)$) 을 생성하기 위하여 반복될 수도 있다.

[0175] 제 1 판단 트리/분류기 (h1(x)) 에 의해 오분류되었던 엔트리들의 가중을 부스팅 또는 증가시킴으로써, 제 2 트리/분류기 (h2(x)) 는 제 1 판단 트리/분류기 (h1(x)) 에 의해 오분류되었던 엔티티들을 더욱 정확하게 분류할 수도 있지만, 또한, 제 1 판단 트리/분류기 (h1(x)) 에 의해 올바르게 분류되었던 엔티티들의 일부를 오분류할 수도 있다. 유사하게, 제 3 트리/분류기 (h3(x)) 는 제 2 판단 트리/분류기 (h2(x)) 에 의해 오분류되었던 엔티티들을 더욱 정확하게 분류할 수도 있고, 제 2 판단 트리/분류기 (h2(x)) 에 의해 올바르게 분류되었던 엔티티들의 일부를 오분류할 수도 있다. 즉, 트리 분류기들 h1(x) 내지 $h_t(x)$ 의 패밀리를 생성하는 것은 전체적으로 수렴하는 시스템으로 귀착되지 않을 수도 있지만, 병렬로 실행될 수도 있는 다수의 판단 트리들/분류기들로 귀착된다.

[0176] 도 9 는 일 양태에 따라 동적 및 적응적 관측들을 수행하도록 구성된 컴퓨팅 시스템의 거동 관측기 모듈 (202) 에서의 일 예의 논리적 컴포넌트들 및 정보 흐름들을 예시한다. 거동 관측기 모듈 (202) 은 적응적 필터 모듈 (902), 스로틀 모듈 (throttle module; 904), 관측기 모드 모듈 (906), 하이-레벨 거동 검출 모듈 (908), 거동 벡터 생성기 (910), 및 보안 버퍼 (912) 를 포함할 수도 있다. 하이-레벨 거동 검출 모듈 (908) 은 공간적 상관 모듈 (914) 및 시간적 상관 모듈 (916) 을 포함할 수도 있다.

[0177] 관측기 모드 모듈 (906) 은, 분석기 유닛 (예컨대, 도 2 를 참조하여 위에서 설명된 거동 분석기 모듈 (204)) 및/또는 애플리케이션 API 를 포함할 수도 있는 다양한 소스들로부터 제어 정보를 수신할 수도 있다. 관측

기 모드 모듈 (906) 은 다양한 관측기 모드들에 속하는 제어 정보를 적응적 필터 모듈 (902) 및 하이-레벨 거동 검출 모듈 (908) 로 전송할 수도 있다.

[0178] 적응적 필터 모듈 (902) 은 다수의 소스들로부터 데이터/정보를 수신할 수도 있고, 수신된 정보로부터 선택된 정보의 더 작은 서브세트를 생성하기 위하여 수신된 정보를 지능적으로 필터링할 수도 있다. 이 필터는 분석기 모듈, 또는 API 를 통해 통신하는 하이-레벨 프로세스로부터 수신된 정보 또는 제어에 기초하여 적응될 수도 있다. 필터링된 정보는 스로틀 모듈 (904) 로 전송될 수도 있고, 이 스로틀 모듈 (904) 은 하이-레벨 거동 검출 모듈 (908) 이 요청들 또는 정보로 플러딩 (flood) 또는 오버로딩 (overload) 되지 않는 것을 보장하기 위하여 필터로부터 흐르는 정보의 양을 제어하는 것을 담당할 수도 있다.

[0179] 하이-레벨 거동 검출 모듈 (908) 은 스로틀 모듈 (904) 로부터 데이터/정보를, 관측기 모드 모듈 (906) 로부터 제어 정보를, 그리고 이동 디바이스의 다른 컴포넌트들로부터 컨텍스트 정보를 수신할 수도 있다. 하이-레벨 거동 검출 모듈 (908) 은, 디바이스로 하여금 차선의 (sub-optimal) 레벨들에서 수행하게 할 수도 있는 하이 레벨 거동들을 검출하거나 식별하기 위한 공간적 및 시간적 상관들을 수행하기 위하여 수신된 정보를 이용할 수도 있다. 공간적 및 시간적 상관들의 결과들은 거동 벡터 생성기 (910) 로 전송될 수도 있고, 이 거동 벡터 생성기 (910) 는 상관 정보를 수신할 수도 있고, 특정한 프로세스, 애플리케이션, 또는 서브-시스템의 거동들을 설명하는 거동 벡터를 생성할 수도 있다. 일 양태에서, 거동 벡터 생성기 (910) 는 특정한 프로세스, 애플리케이션, 또는 서브-시스템의 하이-레벨 거동이 거동 벡터의 엘리먼트일 수도 있도록 거동 벡터를 생성할 수도 있다. 일 양태에서, 생성된 거동 벡터는 보안 버퍼 (912) 내에 저장될 수도 있다. 하이-레벨 거동 검출의 예들은 특정한 이벤트의 실존의 검출, 또 다른 이벤트의 양 또는 빈도, 다수의 이벤트들 사이의 관계, 이벤트들이 발생하는 순서, 어떤 이벤트들의 발생 사이의 시간 차이들 등을 포함할 수도 있다.

[0180] 다양한 양태들에서, 거동 관측기 모듈 (202) 은 적응적 관측들을 수행할 수도 있고 관측 입도 (observation granularity) 를 제어할 수도 있다. 즉, 거동 관측기 모듈 (202) 은 관측되어야 할 관련된 거동들을 동적으로 식별할 수도 있고, 식별된 거동들이 관측되어야 하는 상세함의 레벨을 동적으로 결정할 수도 있다. 이러한 방식으로, 거동 관측기 모듈 (202) 은 시스템이 다양한 레벨들 (예컨대, 다수의 대략적인 그리고 미세한 레벨들) 에서 이동 디바이스의 거동들을 모니터링하는 것을 가능하게 한다. 거동 관측기 모듈 (202) 은 시스템이 관측되고 있는 것에 적응하는 것을 가능하게 할 수도 있다. 거동 관측기 모듈 (202) 은 시스템이 광범위한 소스들로부터 획득될 수도 있는 정보의 포커싱된 서브세트에 기초하여 관측되고 있는 인자들/거동들을 동적으로 변경시키는 것을 가능하게 할 수도 있다.

[0181] 위에서 논의된 바와 같이, 거동 관측기 모듈 (202) 은 적응적 관측 기법들을 수행할 수도 있고, 다양한 소스들로부터 수신된 정보에 기초하여 관측 입도를 제어할 수도 있다. 예를 들어, 하이-레벨 거동 검출 모듈 (908) 은 스로틀 모듈 (904), 관측기 모드 모듈 (906) 로부터의 정보와, 이동 디바이스의 다른 컴포넌트들 (예컨대, 센서들) 로부터 수신된 컨텍스트 정보를 수신할 수도 있다. 예로서, 시간적 상관들을 수행하는 하이-레벨 거동 검출 모듈 (908) 은, 카메라가 이용되었고 이동 디바이스가 사진 (picture) 을 서버에 업로딩하는 것을 시도하고 있음을 검출할 수도 있다. 하이-레벨 거동 검출 모듈 (908) 은 또한, 디바이스가 사용자의 벨트에 채워졌거나 부착된 동안에 이동 디바이스 상의 애플리케이션이 사진을 촬영하였는지 여부를 결정하기 위하여 공간적 상관들을 수행할 수도 있다. 하이-레벨 거동 검출 모듈 (908) 은 이 검출된 하이-레벨 거동 (예컨대, 채워진 동안의 카메라의 사용) 이, 현재의 거동을 이동 디바이스의 과거의 거동들과 비교함으로써, 및/또는 복수의 디바이스들로부터 수집된 정보 (예컨대, 크라우드-소싱 서버로부터 수신된 정보) 를 액세스함으로써 달성될 수도 있는 수용가능하거나 보편적인 거동인지 여부를 결정할 수도 있다. 채워져 있는 동안에 사진들을 촬영하고 이들을 서버에 업로딩하는 것은 (채워져 있는 전후상황에서 관측된 정상적인 거동들로부터 결정될 수도 있는 바와 같이) 통상적이지 않은 거동이므로, 이 상황에서, 하이-레벨 거동 검출 모듈 (908) 은 이것을 잠재적으로 위협하는 거동으로서 인식할 수도 있고, 적합한 응답 (예컨대, 카메라를 멈추는 것, 경보를 울리는 것 등) 을 개시할 수도 있다.

[0182] 일 양태에서, 거동 관측기 모듈 (202) 은 다수의 부분들로 구현될 수도 있다.

[0183] 도 10 은 일 양태의 관측기 데몬을 구현하는 컴퓨팅 시스템 (1000) 에서 논리적 컴포넌트들 및 정보 흐름들을 더욱 상세하게 예시한다. 도 10 에서 예시된 예에서, 컴퓨팅 시스템 (1000) 은 사용자 공간에서의 거동 검출기 (1002) 모듈, 데이터베이스 엔진 (1004) 모듈, 및 거동 분석기 모듈 (204) 과, 커널 공간에서의 링 버퍼 (1014), 필터 규칙들 (1016) 모듈, 스로틀링 규칙들 (1018) 모듈, 및 보안 버퍼 (1020) 를 포함한다. 컴퓨팅 시스템 (1000) 은, 사용자 공간에서의 거동 검출기 (1002) 및 데이터베이스 엔진 (1004) 과, 커널 공간에서

의 보안 버퍼 관리기 (1006), 규칙들 관리기 (1008), 및 시스템 건전성 모니터 (1010) 를 포함하는 관측기 데몬을 더 포함할 수도 있다.

[0184] 다양한 양태들은 시스템 거동을 특징화하기 위하여 웹키트 (webkit), SDK, NDK, 커널, 드라이버들, 및 하드웨어를 망라하는 이동 디바이스들에 관한 교차-계층 관측들을 제공할 수도 있다. 거동 관측들은 실시간으로 행해질 수도 있다.

[0185] 관측기 모듈은 적응적 관측 기법들을 수행할 수도 있고 관측 입도를 제어할 수도 있다. 위에서 논의된 바와 같이, 이동 디바이스의 열화에 기여할 수도 있는 많은 수 (즉, 수 천 개의) 인자들이 있고, 디바이스의 성능의 열화에 기여할 수도 있는 상이한 인자들의 전부를 모니터링/관측하는 것이 실현가능하지 않을 수도 있다. 이것을 극복하기 위하여, 다양한 양태들은 관측되어야 할 관련 있는 거동들을 동적으로 식별하고, 식별된 거동들이 관측되어야 하는 상세함의 레벨을 동적으로 결정한다.

[0186] 도 11 은 일 양태에 따라 동적 및 적응적 관측들을 수행하기 위한 일 예의 방법 (1100) 을 예시한다. 블록 (1102) 에서, 이동 디바이스 프로세서는 이동 디바이스의 열화에 기여할 수도 있는 많은 수의 인자들/거동들의 서브세트를 모니터링/관측함으로써 대략적인 관측들을 수행할 수도 있다. 블록 (1103) 에서, 이동 디바이스 프로세서는 대략적인 관측들에 기초하여 대략적인 관측들 및/또는 이동 디바이스 거동을 특징화하는 거동 벡터를 생성할 수도 있다. 블록 (1104) 에서, 이동 디바이스 프로세서는 이동 디바이스의 열화에 잠재적으로 기여할 수도 있는 대략적인 관측들과 연관된 서브시스템들, 프로세스들, 및/또는 애플리케이션들을 식별할 수도 있다. 이것은 예를 들어, 다수의 소스들로부터 수신된 정보를 이동 디바이스의 센서들로부터 수신된 컨텍스트 정보와 비교함으로써 달성될 수도 있다. 블록 (1106) 에서, 이동 디바이스 프로세서는 대략적인 관측들에 기초하여 거동 분석 동작들을 수행할 수도 있다. 일 양태에서, 블록들 (1103 및 1104) 의 일부로서, 이동 디바이스 프로세서는 도 2 내지 도 10 을 참조하여 위에서 논의된 동작들 중의 하나 이상을 수행할 수도 있다.

[0187] 결정 블록 (1108) 에서, 이동 디바이스 프로세서는 의심스러운 거동들 또는 잠재적인 문제들이 거동 분석의 결과들에 기초하여 식별되고 정정될 수 있는지 여부를 결정할 수도 있다. 이동 디바이스 프로세서가 의심스러운 거동들 또는 잠재적인 문제들이 거동 분석의 결과들에 기초하여 식별되고 정정될 수 있는 것으로 결정할 때 (즉, 결정 블록 (1108) = "예"), 블록 (1118) 에서, 프로세서는 거동을 정정하기 위하여 프로세스를 개시할 수도 있고, 추가의 대략적인 관측들을 수행하기 위하여 블록 (1102) 으로 복귀할 수도 있다.

[0188] 이동 디바이스 프로세서가 의심스러운 거동들 또는 잠재적인 문제들이 거동 분석의 결과들에 기초하여 식별 및/또는 정정될 수 없는 것으로 결정할 때 (즉, 결정 블록 (1108) = "아니오"), 결정 블록 (1109) 에서, 이동 디바이스 프로세서는 문제의 가능성이 있는지 여부를 결정할 수도 있다. 일 양태에서, 이동 디바이스 프로세서는 이동 디바이스가 잠재적인 문제들을 조우하고 및/또는 의심스러운 거동들에 관여할 확률을 연산함으로써, 그리고 연산된 확률이 미리 결정된 문턱치보다 더 큰지 여부를 결정함으로써, 문제의 가능성이 있는 것으로 결정할 수도 있다. 이동 디바이스 프로세서가 연산된 확률이 미리 결정된 문턱치보다 더 크지 않은 것, 및/또는 의심스러운 거동들 또는 잠재적인 문제들이 존재하고 및/또는 검출가능할 가능성이 없는 것으로 결정할 때 (즉, 결정 블록 (1109) = "아니오"), 프로세서는 추가의 대략적인 관측들을 수행하기 위하여 블록 (1102) 으로 복귀할 수도 있다.

[0189] 이동 디바이스 프로세서가 의심스러운 거동들 또는 잠재적인 문제들이 존재하고 및/또는 검출가능할 가능성이 있는 것으로 결정할 때 (즉, 결정 블록 (1109) = "예"), 블록 (1110) 에서, 이동 디바이스 프로세서는 식별된 서브시스템들, 프로세스들, 또는 애플리케이션들에 관한 더 심도 있는 로깅/관측들 또는 최종적인 로깅 (logging) 을 수행할 수도 있다. 블록 (1112) 에서, 이동 디바이스 프로세서는 식별된 서브시스템들, 프로세스들, 또는 애플리케이션들에 관한 더 심도 있고 더욱 상세한 관측들을 수행할 수도 있다. 블록 (1114) 에서, 이동 디바이스 프로세서는 더 심도 있고 더욱 상세한 관측들에 기초하여 추가의 및/또는 더 심도 있는 거동 분석을 수행할 수도 있다. 결정 블록 (1108) 에서, 이동 디바이스 프로세서는 의심스러운 거동들 또는 잠재적인 문제들이 더 심도 있는 거동 분석의 결과들에 기초하여 식별되고 정정될 수 있는지 여부를 다시 결정할 수도 있다. 이동 디바이스 프로세서가 의심스러운 거동들 또는 잠재적인 문제들이 더 심도 있는 거동 분석의 결과들에 기초하여 식별되고 정정될 수 없는 것으로 결정할 때 (즉, 결정 블록 (1108) = "아니오"), 프로세서는 상세함의 레벨이 문제를 식별할 정도로 충분하게 미세할 때까지, 또는 문제가 추가적인 상세함으로 식별될 수 없거나 문제가 존재하지 않는 것으로 결정될 때까지 블록들 (1110 내지 1114) 에서의 동작들을 반복할 수도 있다.

[0190] 이동 디바이스 프로세서가 의심스러운 거동들 또는 잠재적인 문제들이 더 심도 있는 거동 분석의 결과들에 기초하여 식별되고 정정될 수 있는 것으로 결정할 때 (즉, 결정 블록 (1108) = "예"), 블록 (1118) 에서, 이동 디바이스 프로세서는 문제/거동을 정정하기 위한 동작들을 수행할 수도 있고, 추가적인 동작들을 수행하기 위하여 블록 (1102) 으로 복귀할 수도 있다.

[0191] 일 양태에서, 방법 (1100) 의 블록들 (1102 내지 1118) 의 일부로서, 이동 디바이스 프로세서는 제한된 그리고 대략적인 관측들로부터 의심스러운 거동들을 식별하기 위하여, 더욱 상세하게 관측하기 위한 거동들을 동적으로 결정하기 위하여, 그리고 관측들을 대해 요구된 상세함의 정밀한 레벨을 동적으로 결정하기 위하여, 시스템의 거동들의 실시간 거동 분석을 수행할 수도 있다. 이것은 이동 디바이스 프로세서가, 디바이스 상에서 다량의 프로세서, 메모리, 또는 배터리 자원들의 이용을 요구하지 않으면서, 문제들을 효율적으로 식별하고 문제들이 발생하는 것을 방지하는 것을 가능하게 한다.

[0192] 다양한 양태들은 다양한 컴퓨팅 디바이스들 상에서 구현될 수도 있고, 그 예는 도 12 에서 스마트폰의 형태로 예시되어 있다. 스마트폰 (1200) 은 내부 메모리 (1204), 디스플레이 (1212), 및 스피커 (1214) 에 결합된 프로세서 (1202) 를 포함할 수도 있다. 추가적으로, 스마트폰 (1200) 은, 무선 데이터 링크, 및/또는 프로세서 (1202) 에 결합된 셀룰러 전화 트랜시버 (1208) 에 접속될 수도 있는, 전자기 복사를 전송하고 수신하기 위한 안테나를 포함할 수도 있다. 스마트폰들 (1200) 은 또한 전형적으로, 사용자 입력들을 수신하기 위한 메뉴 선택 버튼들 또는 록커 스위치 (rocker switch) 들 (1220) 을 포함한다.

[0193] 전형적인 스마트폰 (1200) 은 또한, 마이크로폰으로부터 수신된 사운드를, 무선 송신에 적합한 데이터 패킷들로 디지털화하고, 사운드를 생성하기 위한 스피커에 제공되는 아날로그 신호들을 생성하기 위하여 수신된 사운드 데이터 패킷들을 디코딩하는 사운드 인코딩/디코딩 (encoding/decoding; CODEC) 회로 (1206) 를 포함한다. 또한, 프로세서 (1202), 무선 트랜시버 (1208) 및 CODEC (1206) 중의 하나 이상은 디지털 신호 프로세서 (digital signal processor; DSP) 회로 (별도로 도시되지 않음) 를 포함할 수도 있다.

[0194] 일 양태의 방법들의 부분들은, 일 양태의 방법들을 실행하면서 이동 디바이스 프로세서에 의해 액세스될 수도 있는 정상적인 동작 거동들의 데이터베이스들을 유지하는 것과 같은, 서버에서 발생하는 프로세싱의 일부를 갖는 클라이언트-서버 아키텍처에서 달성될 수도 있다. 이러한 양태들은 도 13 에서 예시된 서버 (1300) 와 같은, 다양한 상업적으로 입수가능한 서버 디바이스들 중의 임의의 것 상에서 구현될 수도 있다. 이러한 서버 (1300) 는 전형적으로, 휘발성 메모리 (1302) 및, 디스크 드라이브 (disk drive; 1303) 와 같은 대용량 비휘발성 메모리에 결합된 프로세서 (1301) 를 포함한다. 서버 (1300) 는 또한, 프로세서 (1301) 에 결합된 플로피 디스크 드라이브 (floppy disc drive), 컴팩트 디스크 (compact disc; CD) 또는 DVD 디스크 (disc) 드라이브 (1304) 를 포함할 수도 있다. 서버 (1300) 는 또한, 다른 브로드캐스트 시스템 컴퓨터들 및 서버들에 결합된 로컬 영역 네트워크와 같은 네트워크 (1305) 와의 데이터 접속들을 구축하기 위하여 프로세서 (1301) 에 결합된 네트워크 액세스 포트들 (1306) 을 포함할 수도 있다.

[0195] 프로세서들 (1202, 1301) 은, 이하에서 설명된 다양한 양태들의 기능들을 포함하는 다양한 기능들을 수행하기 위하여 소프트웨어 명령들 (애플리케이션들) 에 의해 구성될 수 있는 임의의 프로그래밍가능한 마이크로프로세서, 마이크로컴퓨터 또는 다중 프로세서 칩 또는 칩들일 수도 있다. 일부의 이동 디바이스들에서는, 무선 통신 기능들에 전용인 하나의 프로세서 및 다른 애플리케이션들을 실행하는 것에 전용인 하나의 프로세서와 같은, 다중 프로세서들 (1202) 이 제공될 수도 있다. 전형적으로, 소프트웨어 애플리케이션들은, 이들이 액세스되고 프로세서 (1202, 1301) 로 로딩되기 전에 내부 메모리 (1204, 1302, 1303) 내에 저장될 수도 있다. 프로세서 (1202, 1301) 는 애플리케이션 소프트웨어 명령들을 저장하기에 충분한 내부 메모리를 포함할 수도 있다.

[0196] 다수의 상이한 셀룰러 및 이동 통신 서비스들 및 표준들은 미래에 이용가능하거나 구상되고, 이들 모두는 다양한 양태들을 구현하고 이 다양한 양태들로부터 이익을 얻을 수도 있다. 이러한 서비스들 및 표준들은 예를 들어, 3 세대 파트너십 프로젝트 (third generation partnership project; 3GPP), 롱텀 에볼루션 (long term evolution; LTE) 시스템들, 제 4 세대 무선 이동 통신 기술 (4G), 이동 통신들을 위한 글로벌 시스템 (global system for mobile communications; GSM), 범용 이동 통신 시스템 (universal mobile telecommunications system; UMTS), 3GSM, 일반 패킷 라디오 서비스 (general packet radio service; GPRS), 코드 분할 다중 액세스 (code division multiple access; CDMA) 시스템들 (예를 들어, cdmaOne, CDMA1020TM), GSM 진화를 위한 개량형 데이터 레이트들 (enhanced data rates for GSM evolution; EDGE), 진보된 이동 전화 시스템 (advanced mobile phone system; AMPS), 디지털 AMPS (IS-136/TDMA), 진화-데이터 최적화 (evolution-data optimized;

EV-DO), 디지털 개량형 코드리스 통신 (digital enhanced cordless telecommunications; DECT), 마이크로파 액세스를 위한 전세계적 상호운용성 (Worldwide Interoperability for Microwave Access; WiMAX), 무선 로컬 영역 네트워크 (wireless local area network; WLAN), Wi-Fi 보호된 액세스 I & II (WPA, WPA2), 및 통합된 디지털 개량형 네트워크 (integrated digital enhanced network; iden) 를 포함한다. 이 기술들의 각각은 예를 들어, 음성, 데이터, 시그널링, 및/또는 컨텐츠 메시지들의 송신 및 수신을 포함한다. 산업적 통신 표준 또는 기술에 관련된 용어 및/또는 기술적 세부사항들에 대한 임의의 참조들은 오직 예시적인 목적들을 위한 것이고, 청구항 언어에서 구체적으로 인용되지 않으면, 청구항들의 범위를 특정한 통신 시스템 또는 기술로 제한하도록 의도된 것은 아니다.

[0197] 용어 "성능 열화" 는 더 긴 프로세싱 시간들, 더 느린 실시간 응답성, 더 낮은 배터리 수명, 사적 데이터의 손실, 악의적인 경제적 활동 (예를 들어, 인가되지 않은 고급 SMS 메시지의 전송), 서비스 거부 (denial of service; DoS), 이동 디바이스를 멋대로 사용하는 것 또는 스파이 (spy) 또는 봇넷 (botnet) 활동들을 위하여 폰을 사용하는 것과 관련된 동작들 등과 같은, 광범위한 바람직하지 않은 이동 디바이스 동작들 및 특성들을 지칭하기 위하여 이 출원에서 이용된다.

[0198] 다양한 양태들의 동작들을 수행하기 위한 프로그래밍가능한 프로세서 상에서의 실행을 위한 컴퓨터 프로그램 코드 또는 "프로그램 코드" 는 C, C++, C#, 스몰토크 (Smalltalk), 자바 (Java), 자바스크립트 (JavaScript), 비쥬얼 베이직 (Visual Basic), 구조화 질의어 (예컨대, 트랜잭트-SQL (Transact-SQL)), 펄 (Perl), 또는 다양한 다른 프로그래밍 언어들과 같은 하이 레벨 프로그래밍 언어로 기재될 수도 있다. 이 출원에서 이용된 바와 같은 컴퓨터 판독가능 저장 매체 상에 저장된 프로그램 코드 또는 프로그램들은 그 포맷이 프로세서에 의해 이해가능한 (오브젝트 코드와 같은) 머신 언어 코드를 지칭할 수도 있다.

[0199] 시스템 커널들을 동작시키는 다수의 이동 컴퓨팅 디바이스들은 사용자 공간 (비-특권부여된 (non-privileged) 코드가 실행됨) 및 커널 공간 (특권부여된 코드가 실행됨) 으로 편성된다. 이 분리는, 커널 공간의 일부인 코드가 GPL 라이센싱되어야 하는 반면, 사용자-공간에서 실행되는 코드는 GPL 라이센싱되지 않을 수도 있는 Android® 및 다른 일반 공중 라이선스 (general public license; GPL) 환경들에서 특별히 중요하다. 여기에서 논의된 다양한 소프트웨어 컴포넌트들/모듈들은 이와 다르게 명시적으로 기재되지 않으면, 커널 공간 또는 사용자 공간의 어느 하나에서 구현될 수도 있다는 것이 이해되어야 한다.

[0200] 상기한 방법 설명들 및 프로세스 흐름도들은 예시적인 예들에 불과한 것으로서 제공되고, 다양한 양태들의 단계들이 제시된 순서로 수행되어야 하는 것을 요구하거나 암시하도록 의도된 것이 아니다. 당해 분야의 숙련자에 의해 인식되는 바와 같이, 상기한 양태들에서의 단계들의 순서는 임의의 순서로 수행될 수도 있다. "그 다음", "다음으로", "다음" 등과 같은 단어들은 단계들의 순서를 제한하도록 의도된 것이 아니고; 이 단어들은 방법들의 설명을 통해 독자를 안내하기 위하여 간단하게 이용된다. 또한, 예를 들어, 관사들 "a", "an", 또는 "the" 를 이용하는 단수인 청구항 구성요소들에 대한 임의의 참조는 구성요소를 단수로 제한하는 것으로 해석되지 않아야 한다.

[0201] 이 출원에서 이용된 바와 같이, 용어들 "컴포넌트", "모듈", "시스템", "엔진", "생성기", "관리기" 등은 하드웨어, 펌웨어, 하드웨어 및 소프트웨어의 조합, 소프트웨어, 또는 특정한 동작들 또는 기능들을 수행하도록 구성되는 실행 중인 소프트웨어와 같지만, 이것으로 제한되지 않는 컴퓨터-관련 엔티티를 포함하도록 의도된다. 예를 들어, 컴포넌트는 프로세서 상에서 실행되는 프로세스, 프로세서, 오브젝트, 실행가능물 (executable), 실행 스레드 (thread of execution), 프로그램, 및/또는 컴퓨터일 수도 있지만, 이것으로 제한되지 않는다. 예시로서, 컴퓨팅 디바이스 상에서 실행되는 애플리케이션 및 컴퓨팅 디바이스 양자는 컴포넌트로서 지칭될 수도 있다. 하나 이상의 컴포넌트들은 프로세스 및/또는 실행 스레드 내에서 상주할 수도 있고, 컴포넌트는 하나의 프로세서 상에서 로컬라이즈 (localize) 될 수도 있고 및/또는 2 개 이상의 프로세서들 또는 코어들 사이에서 분산될 수도 있다. 게다가, 이 컴포넌트들은 그 위에 저장된 다양한 명령들 및/또는 데이터 구조들을 가지는 다양한 비-일시적인 (non-transitory) 컴퓨터 판독가능 매체들로부터 실행될 수도 있다. 컴포넌트들은 로컬 및/또는 원격 프로세스들, 함수 또는 프로시저 (procedure) 호출들, 전자 신호들, 데이터 패킷들, 메모리 판독/기록들, 및 다른 알려진 네트워크, 컴퓨터, 프로세서, 및/또는 프로세스 관련 통신 방법론들을 통해 통신할 수도 있다.

[0202] 본원에서 개시된 양태들과 관련하여 설명된 다양한 예시적인 논리적 블록들, 모듈들, 회로들, 및 알고리즘 단계들은 전자 하드웨어, 컴퓨터 소프트웨어, 또는 양자의 조합들로서 구현될 수도 있다. 하드웨어 및 소프트웨어의 이 교환가능성을 명확하게 예시하기 위하여, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들, 및 단

계들은 일반적으로 그 기능성의 측면에서 위에서 설명되었다. 이러한 기능성이 하드웨어 또는 소프트웨어로 구현되는지 여부는 특정한 애플리케이션과, 전체 시스템에 부과된 설계 제약들에 종속된다. 숙련된 기술자들은 각각의 특정 애플리케이션을 위한 다양한 방법들로 설명된 기능성을 구현할 수도 있지만, 이러한 구현 판정들은 본 발명의 범위로부터의 이탈을 야기시키는 것으로 해석되지 않아야 한다.

[0203] 본원에서 개시된 양태들과 관련하여 설명된 다양한 예시적인 로직들, 논리적 블록들, 모듈들, 및 회로들을 구현하기 위하여 이용된 하드웨어는 범용 프로세서, 디지털 신호 프로세서 (DSP), 주문형 집적 회로 (application specific integrated circuit; ASIC), 필드 프로그래밍가능 게이트 어레이 (field programmable gate array; FPGA) 또는 다른 프로그래밍가능 로직 디바이스, 개별 게이트 또는 트랜지스터 로직, 개별 하드웨어 컴포넌트들, 또는 본원에서 설명된 기능들을 수행하도록 설계된 그 임의의 조합으로 구현되거나 수행될 수도 있다. 범용 프로세서는 멀티프로세서일 수도 있지만, 대안적으로, 프로세서는 임의의 기존의 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수도 있다. 프로세서는 또한, 컴퓨팅 디바이스들의 조합, 예를 들어, DSP 및 멀티프로세서, 복수의 멀티프로세서들, DSP 코어와 함께 하나 이상의 멀티프로세서들, 또는 임의의 다른 이러한 구성의 조합으로서 구현될 수도 있다. 대안적으로, 일부의 단계들 또는 방법들은 주어진 기능에 특정한 회로부에 의해 수행될 수도 있다.

[0204] 하나 이상의 예시적인 양태들에서는, 설명된 기능들이 하드웨어, 소프트웨어, 펌웨어, 또는 그 임의의 조합으로 구현될 수도 있다. 소프트웨어로 구현될 경우, 기능들은 비-일시적인 컴퓨터-판독가능 저장 매체 또는 비-일시적인 프로세서-판독가능 저장 매체 상에서 하나 이상의 프로세서-실행가능 명령들 또는 코드로서 저장될 수도 있다. 본원에서 개시된 방법 또는 알고리즘의 단계들은 비-일시적인 컴퓨터-판독가능한 또는 프로세서-판독가능한 저장 매체 상에서 상주할 수도 있는 프로세서-실행가능 소프트웨어 모듈에서 구체화될 수도 있다.

비-일시적인 컴퓨터-판독가능 또는 프로세서-판독가능 저장 매체들은 컴퓨터 또는 프로세서에 의해 액세스될 수도 있는 임의의 저장 매체들일 수도 있다. 제한이 아닌 예로서, 이러한 비-일시적인 컴퓨터-판독가능 또는 프로세서-판독가능 매체들은 RAM, ROM, EEPROM, FLASH 메모리, CD-ROM 또는 다른 광학 디스크 저장, 자기 디스크 저장, 또는 다른 자기 저장 디바이스들, 또는 명령들 또는 데이터 구조들의 형태로 희망하는 프로그램 코드를 저장하기 위해 이용될 수 있으며 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다.

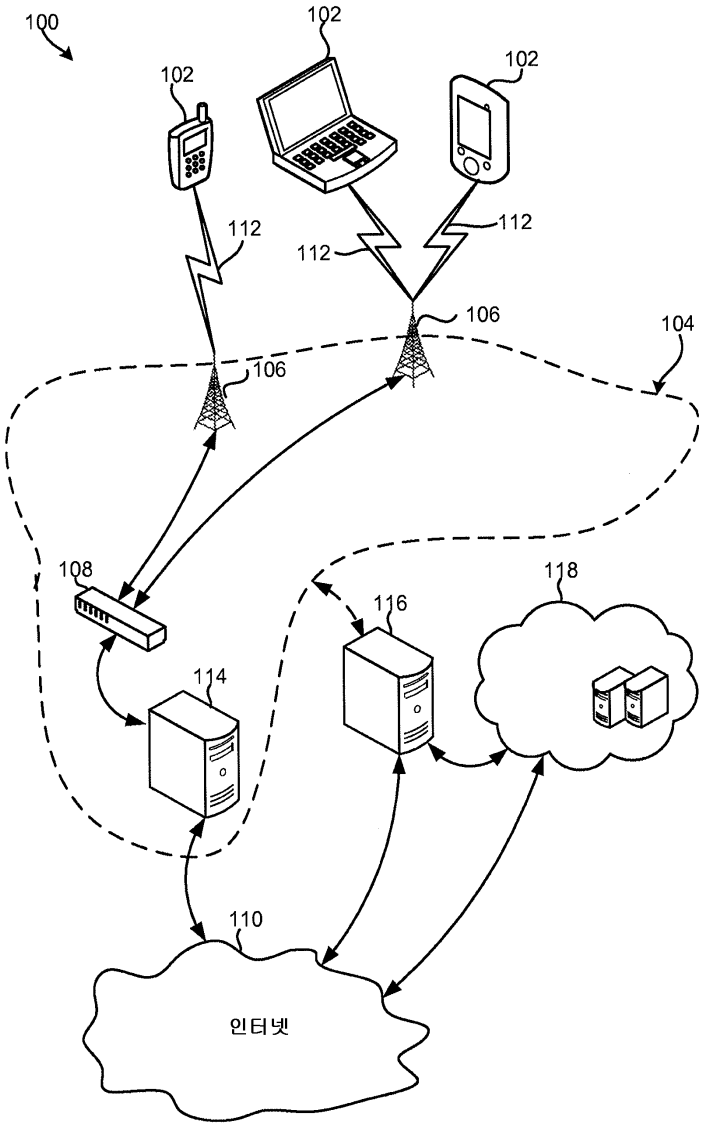
본원에서 이용된 바와 같은 디스크 (disk) 및 디스크 (disc) 는 컴팩트 디스크 (compact disc; CD), 레이저 디스크 (laser disc), 광학 디스크 (optical disc), 디지털 다기능 디스크 (digital versatile disc; DVD), 플로피 디스크 (floppy disk) 및 블루레이 디스크 (blu-ray disc) 를 포함하고, 여기서, 디스크 (disk) 들은 통상 데이터를 자기적으로 재생하는 반면, 디스크 (disc) 들은 데이터를 레이저들로 광학적으로 재생한다. 상기의 조합들은 또한, 비-일시적인 컴퓨터-판독가능 및 프로세서-판독가능 매체들의 범위 내에 포함된다. 추가적으로, 방법 또는 알고리즘의 동작들은, 컴퓨터 프로그램 제품 내로 편입될 수도 있는 비-일시적인 프로세서-판독가능 매체 및/또는 컴퓨터-판독가능 매체 상에 코드들 및/또는 명령들 중의 하나 또는 임의의 조합 또는 세트로서 상주할 수도 있다.

[0205] 개시된 양태들의 선행하는 설명은 당해 분야의 당업자가 본 발명을 제조하거나 이용하는 것을 가능하게 하도록 제공된다. 이 양태들에 대한 다양한 수정들은 당해 분야의 당업자들에게 용이하게 명백할 것이고, 본원에서 정의된 일반적인 원리들은 발명의 사상 또는 범위로부터 이탈하지 않으면서 다른 양태들에 적용될 수도 있다.

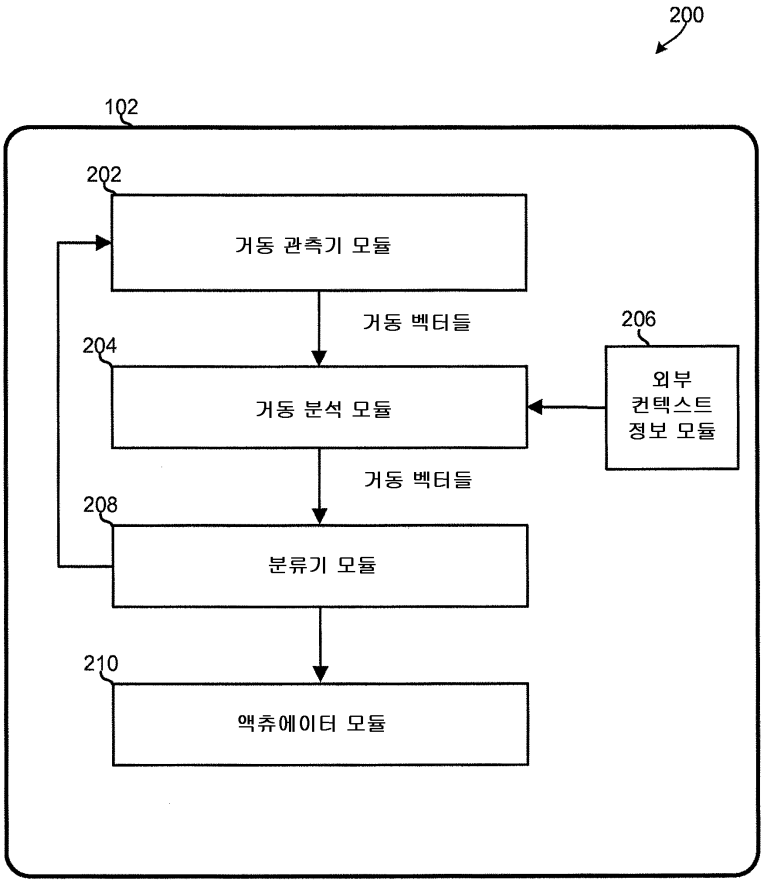
따라서, 본 발명은 본원에서 도시된 양태들에 제한되도록 의도된 것이 아니라, 다음의 청구항들 및 본원에서 개시된 원리들 및 신규한 특징들과 일관되는 가장 넓은 범위를 따르도록 하기 위한 것이다.

도면

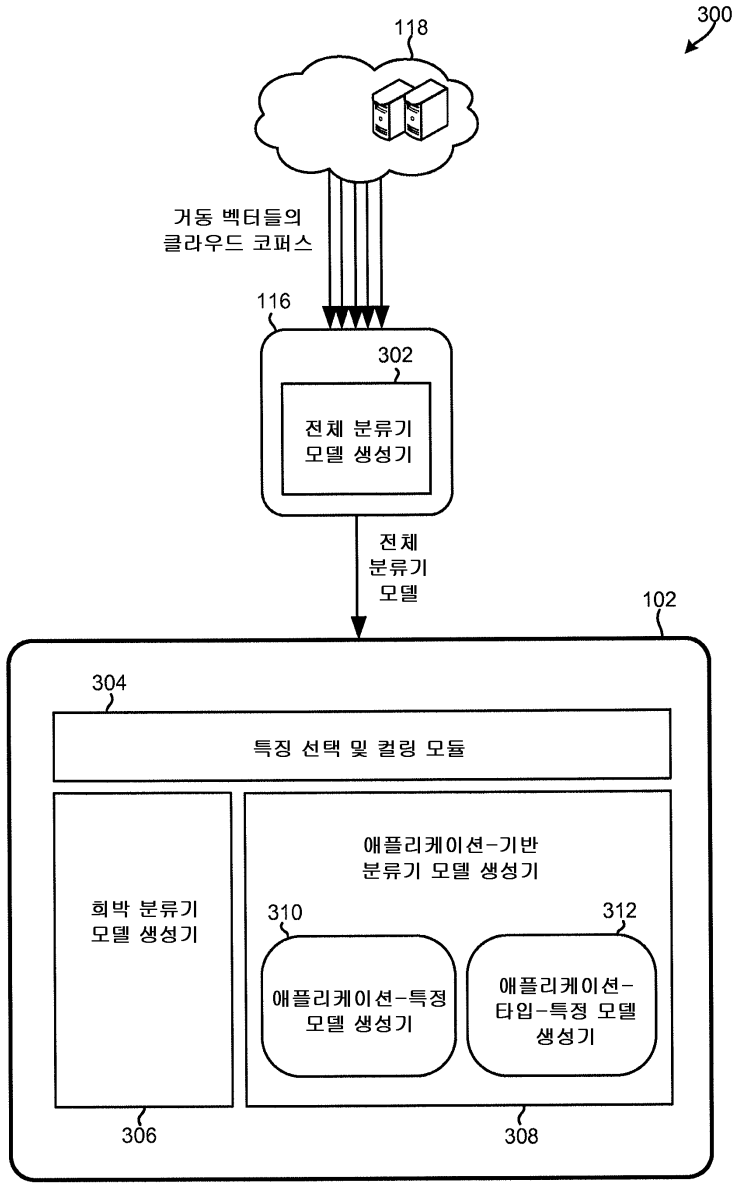
도면1



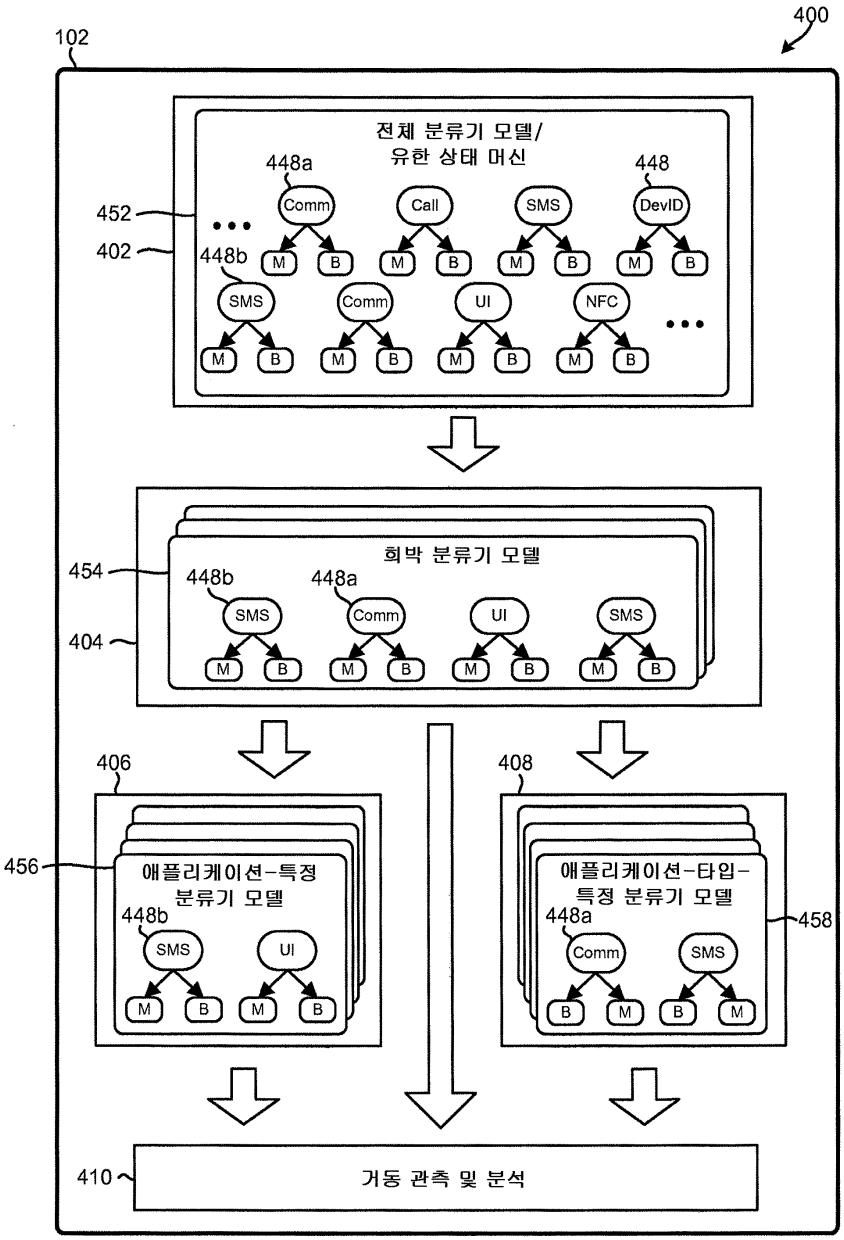
도면2


200
102
202
거동 관측기 모듈
거동 벡터들
206
204
외부
컨텍스트
정보 모듈
거동 분석 모듈
거동 벡터들
208
분류기 모듈
210
액츄에이터 모듈

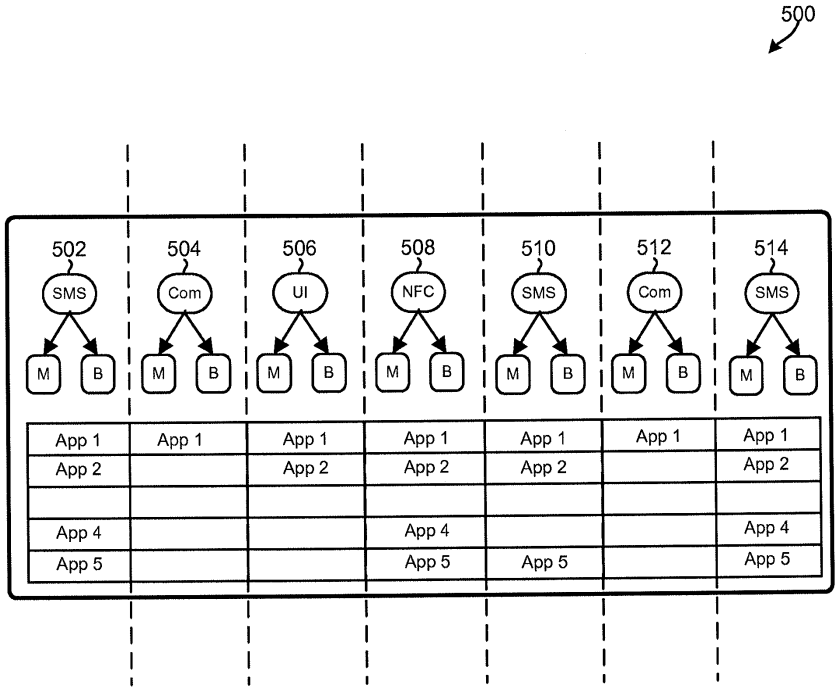
도면3


300
118
거동 벡터들의
클라우드 코퍼스
116
302
전체 분류기
모델 생성기
전체
분류기
모델
102
304
특징 선택 및 컬링 모듈
희박 분류기
모델 생성기
애플리케이션-기반
분류기 모델 생성기
310
312
애플리케이션-특정
모델 생성기
애플리케이션-
타입-특정 모델
생성기
306
308

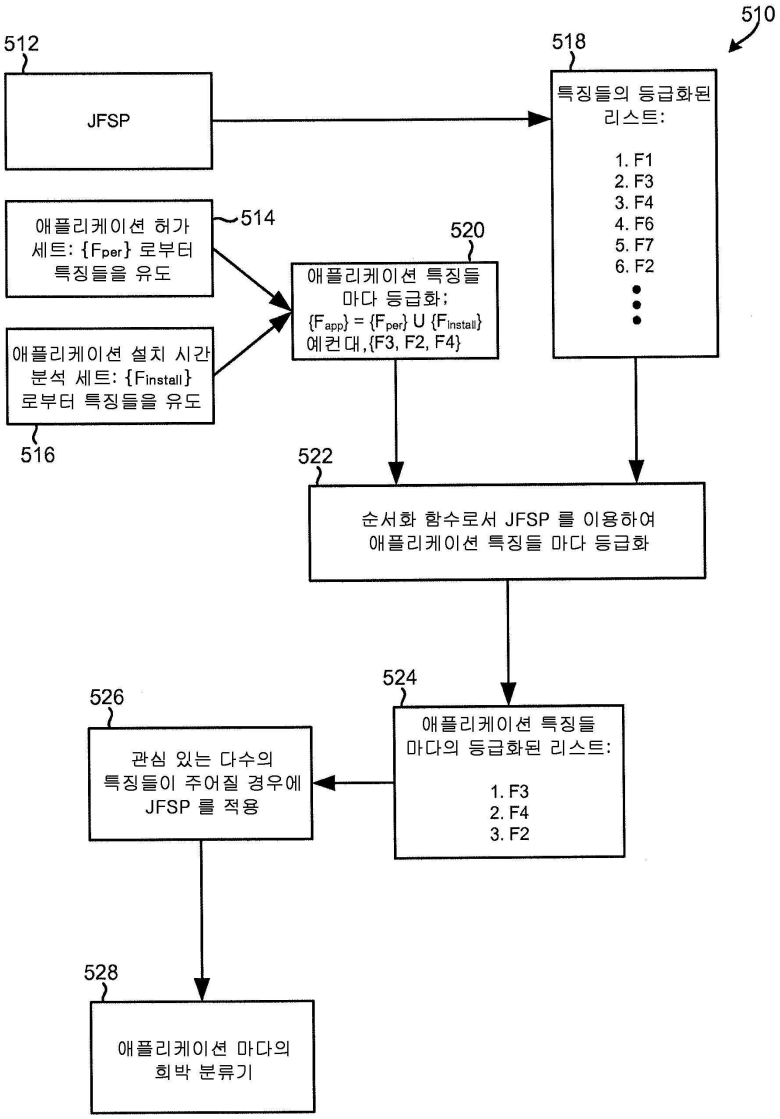
도면4


400
102
전체 분류기 모델/
유한 상태 머신
448a
448
452
402
448b
Comm
Call
SMS
DevID
SMS
Comm
UI
NFC
M
B
454
희박 분류기 모델
404
406
408
456
애플리케이션-특정
분류기 모델
애플리케이션-타입-
특정 분류기 모델
458
410
거동 관측 및 분석

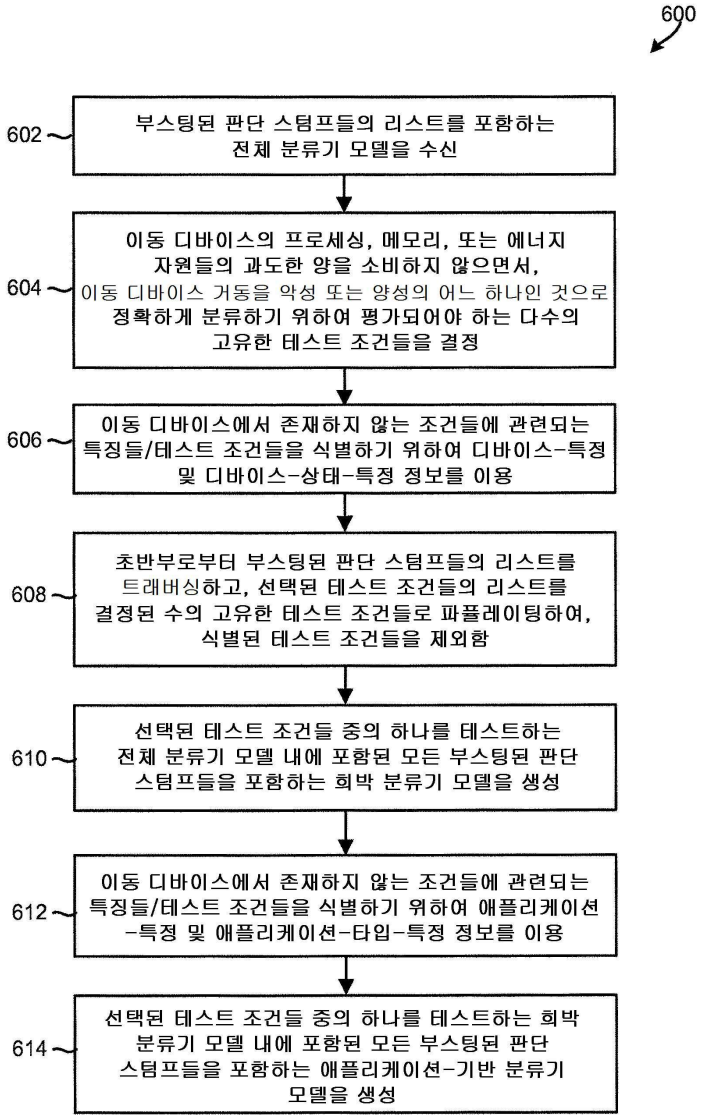
도면5a


500
502
504
506
508
510
512
514
SMS
Com
UI
NFC
SMS
Com
SMS
M
B
App 1
App 2
App 4
App 5

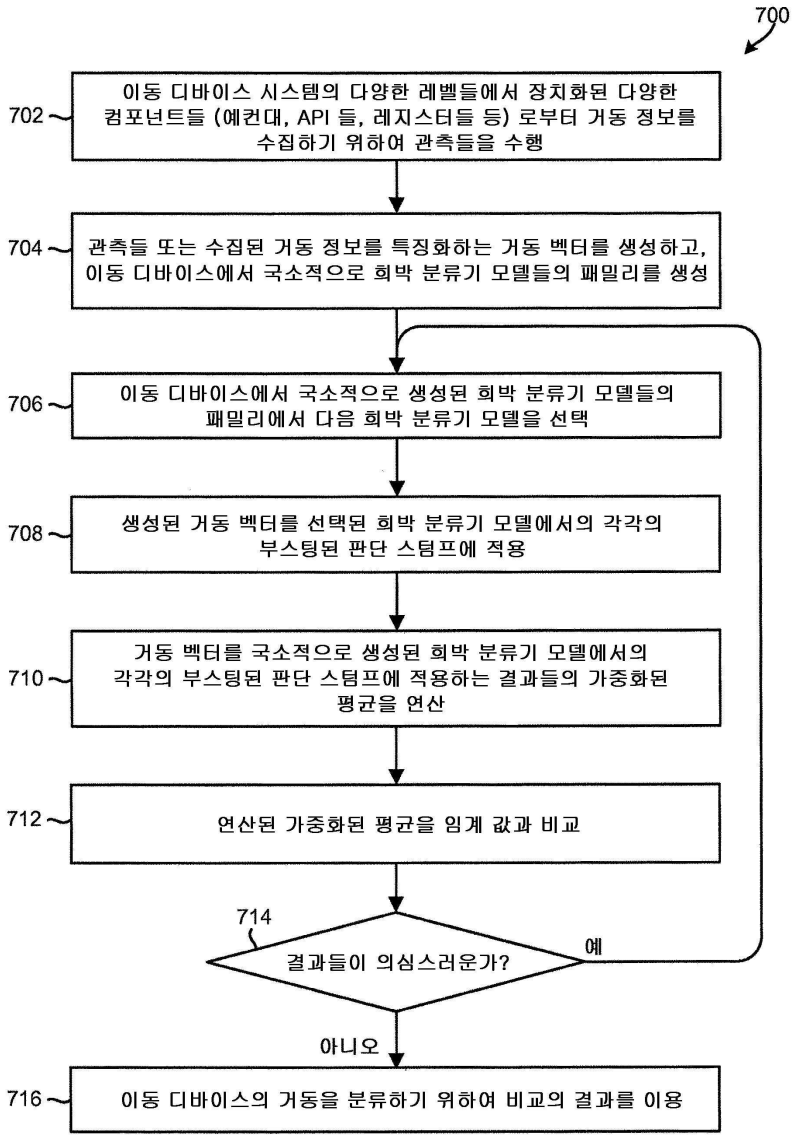
도면5b


510
512
JFSP
518
특징들의 등급화된 리스트:
1. F1
2. F3
3. F4
4. F6
5. F7
6. F2
애플리케이션 허가 세트: {Fper} 로부터 특징들을 유도
514
520
애플리케이션 특징들 마다 등급화: {Fapp} = {Fper} U {Finstall} 예컨대,{F3, F2, F4}
애플리케이션 설치 시간 분석 세트: {Finstall} 로부터 특징들을 유도
516
522
순서화 함수로서 JFSP 를 이용하여 애플리케이션 특징들 마다 등급화
524
애플리케이션 특징들 마다의 등급화된 리스트:
1. F3
2. F4
3. F2
526
관심 있는 다수의 특징들이 주어질 경우에 JFSP 를 적용
528
애플리케이션 마다의 희박 분류기

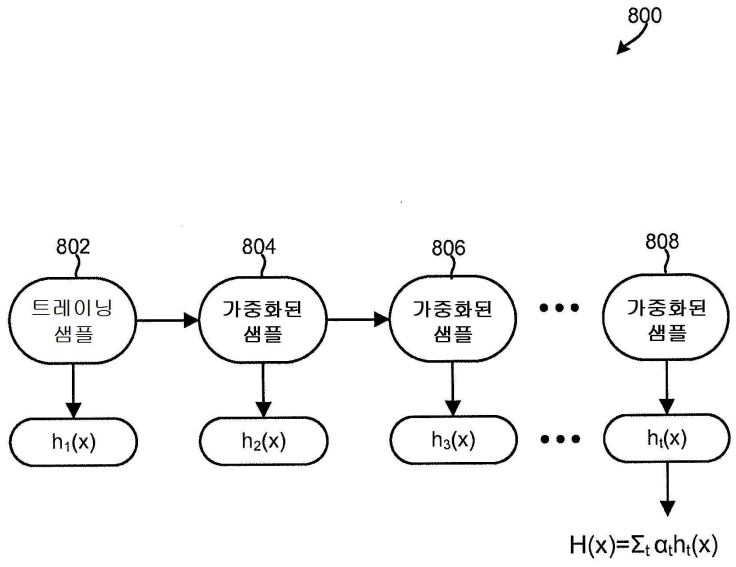
도면6


600
602
부스팅된 판단 스텀프들의 리스트를 포함하는 전체 분류기 모델을 수신
604
이동 디바이스의 프로세싱, 메모리, 또는 에너지 자원들의 과도한 양을 소비하지 않으면서, 이동 디바이스 거동을 악성 또는 양성의 어느 하나인 것으로 정확하게 분류하기 위하여 평가되어야 하는 다수의 고유한 테스트 조건들을 결정
606
이동 디바이스에서 존재하지 않는 조건들에 관련되는 특징들/테스트 조건들을 식별하기 위하여 디바이스-특정 및 디바이스-상태-특정 정보를 이용
608
초반부로부터 부스팅된 판단 스텀프들의 리스트를 트래버싱하고, 선택된 테스트 조건들의 리스트를 결정된 수의 고유한 테스트 조건들로 파플레이팅하여, 식별된 테스트 조건들을 제외함
610
선택된 테스트 조건들 중의 하나를 테스트하는 전체 분류기 모델 내에 포함된 모든 부스팅된 판단 스텀프들을 포함하는 희박 분류기 모델을 생성
612
이동 디바이스에서 존재하지 않는 조건들에 관련되는 특징들/테스트 조건들을 식별하기 위하여 애플리케이션-특정 및 애플리케이션-타입-특정 정보를 이용
614
선택된 테스트 조건들 중의 하나를 테스트하는 희박 분류기 모델 내에 포함된 모든 부스팅된 판단 스텀프들을 포함하는 애플리케이션-기반 분류기 모델을 생성

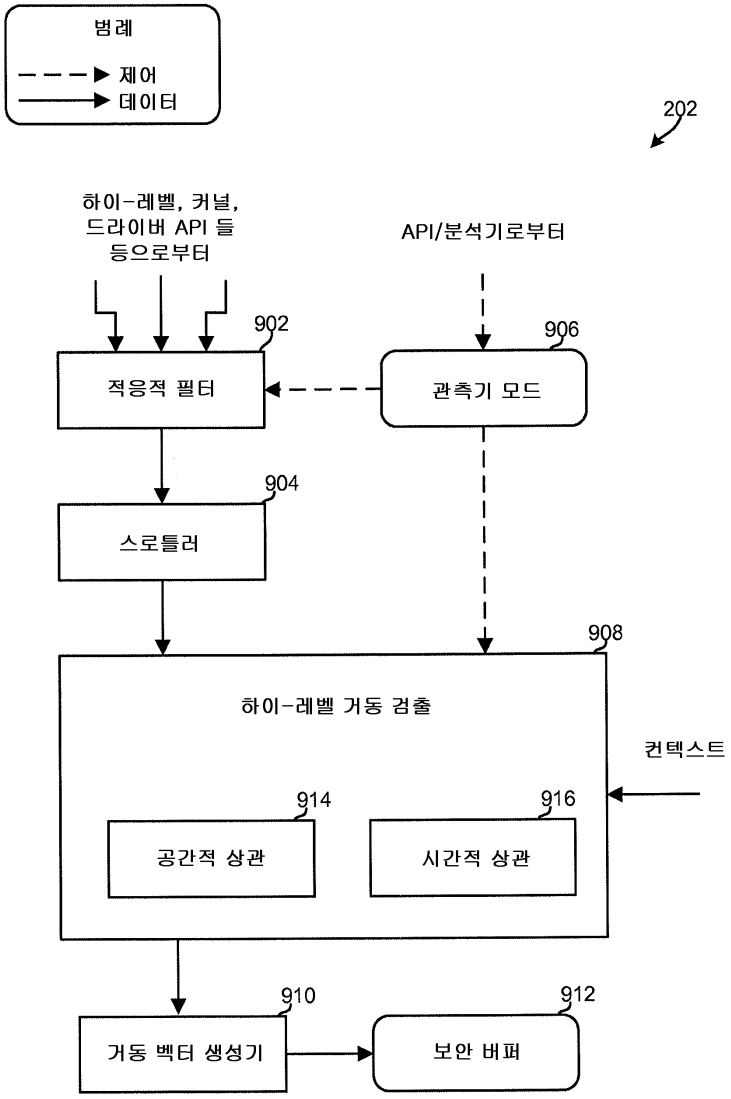
도면7


700
702
이동 디바이스 시스템의 다양한 레벨들에서 장치화된 다양한 컴포넌트들 (예컨대, API 들, 레지스터들 등) 로부터 거동 정보를 수집하기 위하여 관측들을 수행
704
관측들 또는 수집된 거동 정보를 특징화하는 거동 벡터를 생성하고, 이동 디바이스에서 국소적으로 희박 분류기 모델들의 패밀리를 생성
706
이동 디바이스에서 국소적으로 생성된 희박 분류기 모델들의 패밀리에서 다음 희박 분류기 모델을 선택
708
생성된 거동 벡터를 선택된 희박 분류기 모델에서의 각각의 부스팅된 판단 스텀프에 적용
710
거동 벡터를 국소적으로 생성된 희박 분류기 모델에서의 각각의 부스팅된 판단 스텀프에 적용하는 결과들의 가중화된 평균을 연산
712
연산된 가중화된 평균을 임계 값과 비교
714
결과들이 의심스러운가?
예
아니오
716
이동 디바이스의 거동을 분류하기 위하여 비교의 결과를 이용

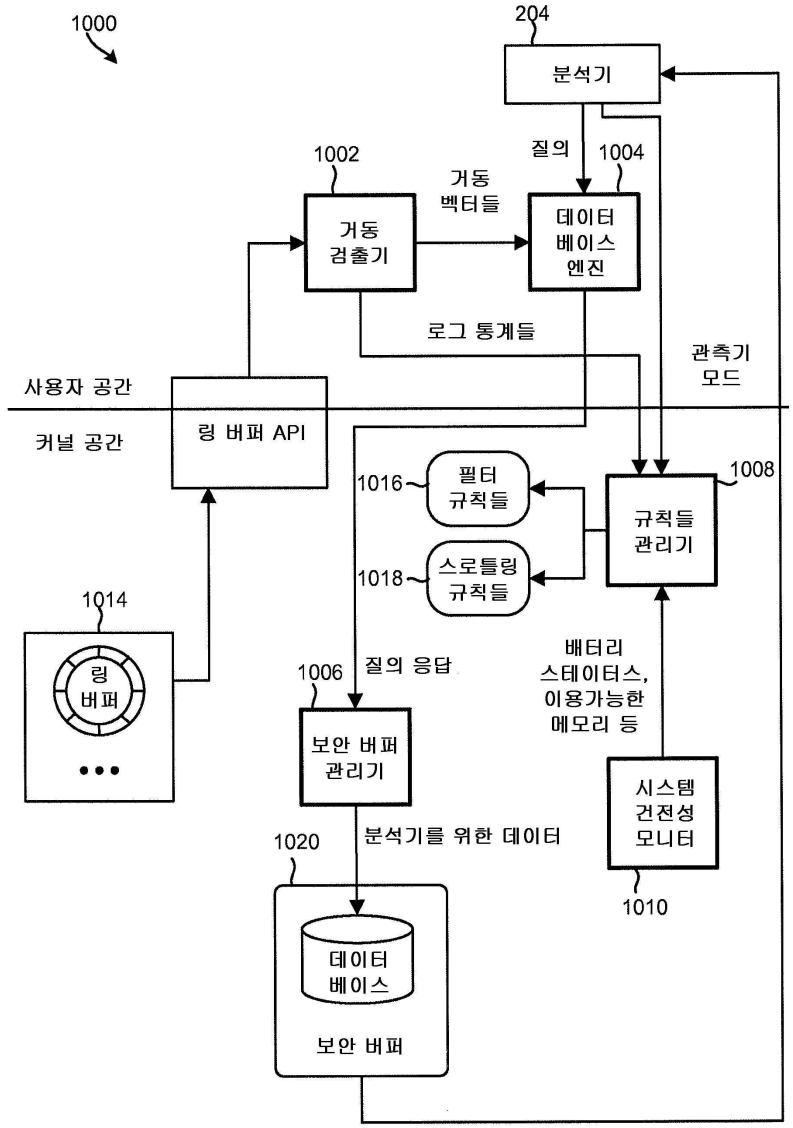
도면8


800
802
804
806
808
트레이닝 샘플
가중화된 샘플
가중화된 샘플
가중화된 샘플
h1(x)
h2(x)
h3(x)
ht(x)
H(x)=Σt αthtt(x)

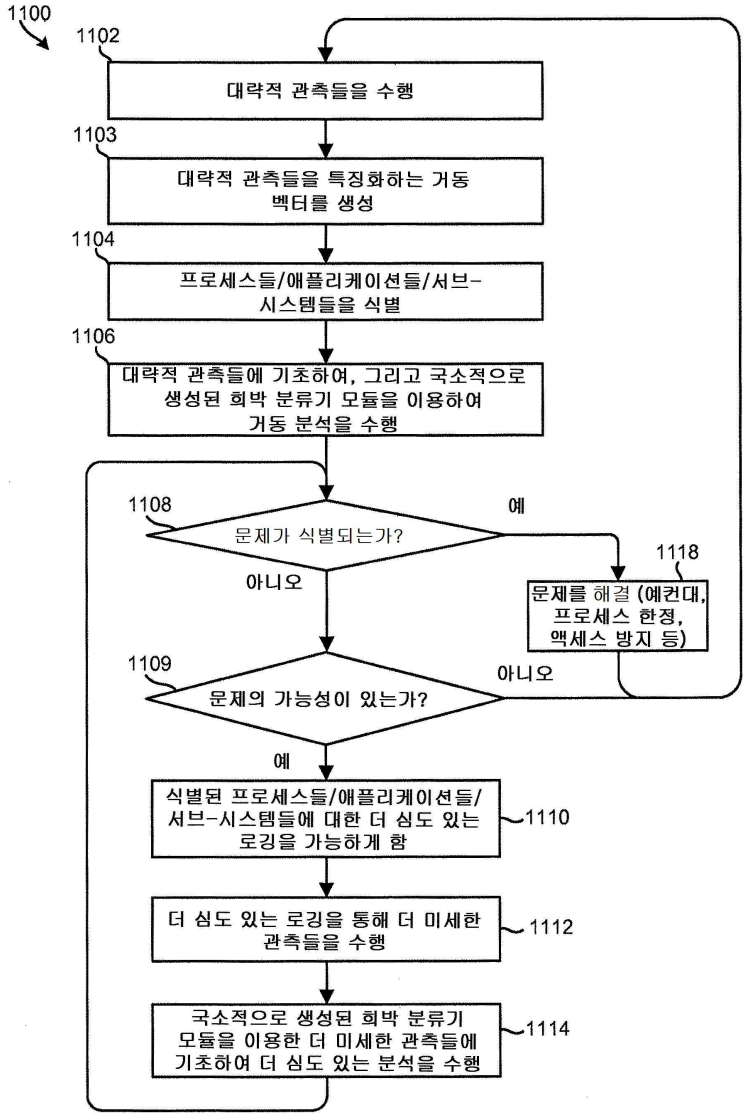
도면9


범례
제어
데이터
202
하이-레벨, 커널, 드라이버 API 들 등으로부터
API/분석기로부터
902
906
적응적 필터
관측기 모드
904
스로틀러
908
하이-레벨 거동 검출
컨텍스트
914
916
공간적 상관
시간적 상관
910
912
거동 벡터 생성기
보안 버퍼

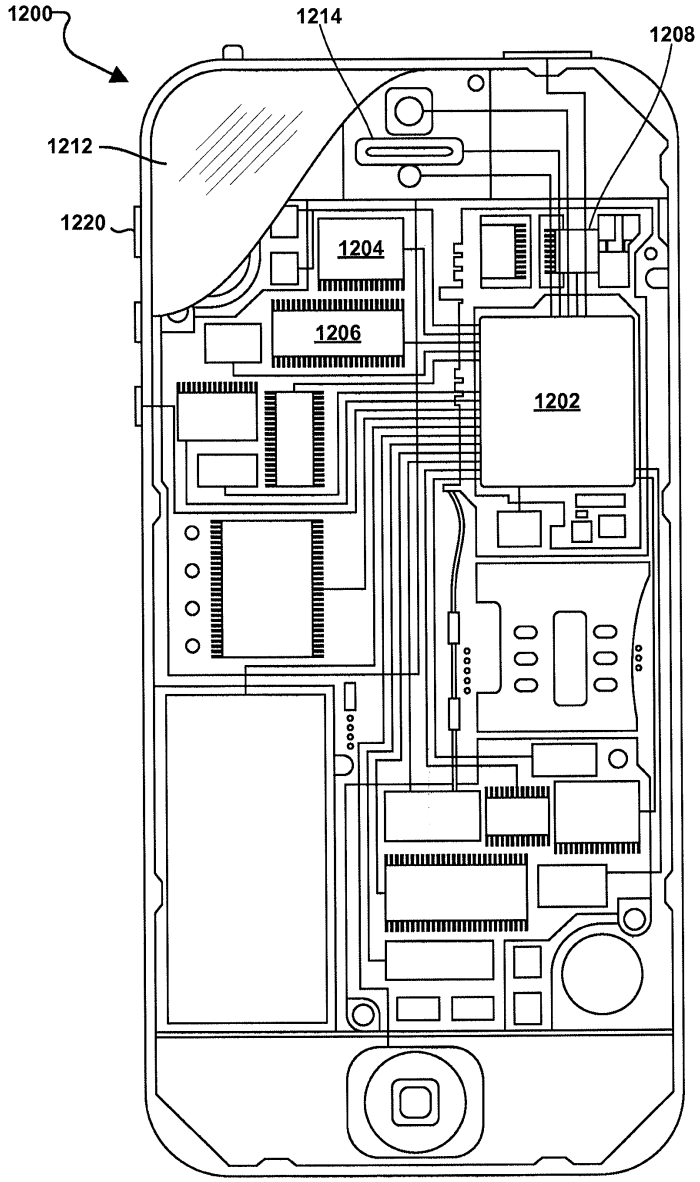
도면10


1000
204
분석기
질의
1004
1002
거동
벡터들
거동
검출기
데이터
베이스
엔진
로그 통계들
관측기
모드
사용자 공간
커널 공간
링 버퍼 API
1016
필터
규칙들
1008
규칙들
관리기
1018
스로틀링
규칙들
1014
링
버퍼
1006
질의 응답
배터리
스테이터스,
이용가능한
메모리 등
보안 버퍼
관리기
시스템
건전성
모니터
1010
1020
분석기를 위한 데이터
데이터
베이스
보안 버퍼

도면11


1100
1102
대략적 관측들을 수행
1103
대략적 관측들을 특징화하는 거동 벡터를 생성
1104
프로세스들/애플리케이션들/서브-시스템들을 식별
1106
대략적 관측들에 기초하여, 그리고 국소적으로 생성된 희박 분류기 모듈을 이용하여 거동 분석을 수행
1108
문제가 식별되는가?
예
아니오
1118
문제를 해결 (예컨대, 프로세스 한정, 액세스 방지 등)
1109
문제의 가능성이 있는가?
아니오
예
식별된 프로세스들/애플리케이션들/서브-시스템들에 대한 더 심도 있는 로깅을 가능하게 함
1110
더 심도 있는 로깅을 통해 더 미세한 관측들을 수행
1112
국소적으로 생성된 희박 분류기 모듈을 이용한 더 미세한 관측들에 기초하여 더 심도 있는 분석을 수행
1114

도면12



도면13