(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년02월07일
(11) 등록번호 10-1826865
(24) 등록일자 2018년02월01일

(51) 국제특허분류(Int. Cl.)
G06N 5/04 (2006.01) *G06F 9/44* (2018.01)
(52) CPC특허분류
G06N 5/043 (2013.01)
G06F 9/4498 (2018.02)
(21) 출원번호 10-2015-7020512
(22) 출원일자(국제) 2013년12월30일
심사청구일자 2017년08월02일
(85) 번역문제출일자 2015년07월28일
(65) 공개번호 10-2015-0103173
(43) 공개일자 2015년09월09일
(86) 국제출원번호 PCT/US2013/078352
(87) 국제공개번호 WO 2014/107439
국제공개일자 2014년07월10일
(30) 우선권주장
61/748,217 2013년01월02일 미국(US)
(뒷면에 계속)

(56) 선행기술조사문헌
US20080127336 A1
Schmidt, A-D., et al. "Static analysis of executables for collaborative malware detection on android." Communications, 2009. ICC'09. IEEE International Conference on. IEEE, 2009.
Faddoul, Jean Baptiste, et al. "Boosting multi-task weak learners with applications to textual and social data." Machine Learning and Applications (ICMLA), 9th International Conference on. IEEE, 2010.

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
파와즈, 카셈
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
스리다라, 비나이
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
굽타, 라자쉬
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

전체 청구항 수 : 총 25 항 심사관 : 서광훈

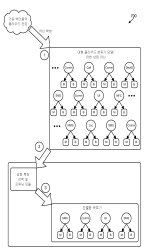
(54) 발명의 명칭 **모바일 디바이스 거동들의 효율적인 분류를 위해 부스트 결정 그루터기들 및 공동의 특징 선택 및 선별 알고리즘들을 사용하는 방법들 및 시스템들**

(57) 요 약

모바일 디바이스 거동을 분류하기 위한 방법들 및 시스템들은, 부스트 결정 그루터기들로의 변환에 적합한 유한 상태 머신을 포함하고 및/또는 모바일 디바이스 거동이 양성인지 또는 시간에 걸쳐 모바일 디바이스의 열화에 기여하는지를 결정하는 것에 관련된 특징들 중 많은 것 또는 전부를 기술하는 풀 분류기 모델을 생성하기 위해, 모

(뒷면에 계속)

대 표 도



바일 디바이스 거동들의 대형 전집을 사용하도록 서버를 구성하는 것을 포함한다. 모바일 디바이스는 풀 분류기 모델을 수신하고, 그 모델을 사용하여 부스트 결정 그루터기들의 풀 세트를 생성할 수 있고, 풀 세트를 모바일 디바이스 거동이 양성인지를 효율적으로 결정하기에 적합한 서브세트로 선별함으로써, 부스트 결정 그루터기들의 풀 세트로부터 더 포커싱된 또는 간결한 분류기 모델이 생성된다. 부스트 결정 그루터기들은, 테스트 조건들의 제한된 세트에 의존하는 모든 부스트 결정 그루터기들을 선택함으로써 선별될 수 있다.

(30) 우선권주장

61/748,220 2013년01월02일 미국(US)

61/874,129 2013년09월05일 미국(US)

14/090,261 2013년11월26일 미국(US)

명 세 서

청구범위

청구항 1

모바일 디바이스에서 모델들을 생성하는 방법으로서,

유한 상태 머신(finite state machine)을 포함하는 풀(full) 분류기 모델을 서버 컴퓨팅 디바이스로부터 상기 모바일 디바이스의 프로세서에서 수신하는 단계 - 상기 유한 상태 머신은 복수의 부스트 결정 그루터기(boosted decision stump)들로서의 표현에 적합한 정보를 포함하고, 각각의 부스트 결정 그루터기는 테스트 조건 및 가중값을 포함함 -;

상기 모바일 디바이스의 상기 프로세서에 의해, 상기 수신된 풀 분류기 모델에 포함된 상기 유한 상태 머신을 상기 복수의 부스트 결정 그루터기들로 변환함으로써 부스트 결정 그루터기들의 정렬된 리스트를 생성하는 단계;

상기 모바일 디바이스의 상기 프로세서에 의해, 상기 모바일 디바이스에서 간결한(lean) 분류기 모델을 생성하기 위해 상기 생성된 부스트 결정 그루터기들의 정렬된 리스트를 선별(cull)하는 단계 - 상기 선별하는 단계는:

상기 모바일 디바이스의 에너지 자원들에 기초하여 모바일 디바이스 거동을 분류하기 위해 상기 모바일 디바이스에서 평가할 상이한 테스트 조건들의 수를 결정하는 단계;

테스트 조건들의 리스트가 상기 결정된 수의 상이한 테스트 조건들을 포함할 때까지, 상기 생성된 부스트 결정 그루터기들의 정렬된 리스트를 순차적으로 횡단(traverse)하고 그리고 각각의 순차적으로 횡단된 부스트 결정 그루터기와 연관된 테스트 조건을 상기 테스트 조건들의 리스트에 삽입함으로써, 상기 결정된 수의 상이한 테스트 조건들을 포함하는 상기 테스트 조건들의 리스트를 생성하는 단계; 및

상기 생성된 테스트 조건들의 리스트에 포함된 복수의 테스트 조건들 중 하나를 테스트하는 부스트 결정 그루터기들을 포함하도록 상기 간결한 분류기 모델을 생성하는 단계를 포함함 -;

상기 모바일 디바이스의 상기 프로세서에 의해, 결과들을 생성하기 위해 상기 생성된 간결한 분류기 모델에 모바일 디바이스 거동 벡터를 적용하는 단계; 및

상기 모바일 디바이스의 상기 프로세서에 의해, 상기 모바일 디바이스 거동을 분류하기 위해 상기 생성된 결과들을 사용하는 단계를 포함하는,

모바일 디바이스에서 모델들을 생성하는 방법.

청구항 2

제 1 항에 있어서,

상기 모바일 디바이스 거동을 분류하기 위해 상기 생성된 결과들을 사용하는 단계는 상기 모바일 디바이스 거동을 비-양성(non benign)으로서 분류하기 위해 상기 생성된 결과들을 사용하는 단계를 포함하는,

모바일 디바이스에서 모델들을 생성하는 방법.

청구항 3

제 1 항에 있어서,

상기 결과들을 생성하기 위해 상기 생성된 간결한 분류기 모델에 상기 모바일 디바이스 거동 벡터를 적용하는 단계는:

상기 모바일 디바이스 거동 벡터에 포함된 수집된 거동 정보를 상기 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용하는 단계;

상기 수집된 거동 정보를 상기 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용하는 것의 결과들

의 가중된 평균을 계산하는 단계; 및

상기 가중된 평균을 임계값과 비교하는 단계를 포함하는,

모바일 디바이스에서 모델들을 생성하는 방법.

청구항 4

제 1 항에 있어서,

상기 간결한 분류기 모델을 생성하는 단계는 상기 생성된 부스트 결정 그루터기들의 정렬된 리스트에 포함된 부스트 결정 그루터기들에 기초하여 간결한 분류기 모델들의 패밀리(family)를 생성하는 단계를 포함하고;

상기 생성된 간결한 분류기 모델들의 패밀리는 상기 간결한 분류기 모델 및 복수의 부가적인 간결한 분류기 모델들을 포함하고; 그리고

상기 복수의 부가적인 간결한 분류기 모델들 각각은 상이한 수의 상이한 테스트 조건들을 포함하는,

모바일 디바이스에서 모델들을 생성하는 방법.

청구항 5

제 1 항에 있어서,

상기 간결한 분류기 모델을 생성하는 단계는:

상이한 가중값 및 상이한 임계값을 사용하여 제 1 조건을 테스트하는 결정 그루터기를 각각 포함하는 복수의 간결한 분류기 모델들을 생성하는 단계를 포함하는,

모바일 디바이스에서 모델들을 생성하는 방법.

청구항 6

제 1 항에 있어서,

상기 수신된 풀 분류기 모델에 기초하여 상기 모바일 디바이스에서 생성되는 복수의 간결한 분류기 모델들 내의 부스트 결정 그루터기들과 연관된 임계값들을 재계산하는 단계를 더 포함하는,

모바일 디바이스에서 모델들을 생성하는 방법.

청구항 7

제 1 항에 있어서,

상기 수신된 풀 분류기 모델에 기초하여 상기 모바일 디바이스에서 생성되는 복수의 간결한 분류기 모델들 내의 부스트 결정 그루터기들과 연관된 가중값들을 재계산하는 단계를 더 포함하는,

모바일 디바이스에서 모델들을 생성하는 방법.

청구항 8

제 1 항에 있어서,

모바일 디바이스 거동들에 대한 정보의 전집(corpus)을 서버에서 수신하고; 그리고

상기 복수의 부스트 결정 그루터기들로의 변환에 적합한 데이터를 포함하도록 상기 정보의 전집에 기초하여 상기 유한 상태 머신을 생성함으로써,

상기 서버에서 상기 풀 분류기 모델을 생성하는 단계; 및

상기 풀 분류기 모델로서 상기 유한 상태 머신을 상기 모바일 디바이스에 전송하는 단계를 더 포함하는,

모바일 디바이스에서 모델들을 생성하는 방법.

청구항 9

제 8 항에 있어서,

각각의 테스트 조건은 확률 값과 연관되고;

각각의 확률 값은 상기 각각의 확률 값과 연관된 테스트 조건이 상기 모바일 디바이스로 하여금 상기 모바일 디바이스 거동이 양성인지 여부를 결정하는 것을 가능하게 할 가능성(likelyhood)을 식별하고; 그리고

상기 방법은:

상기 풀 분류기 모델로서 상기 유한 상태 머신을 상기 모바일 디바이스에 전송하기 전에, 확률 값들에 기초하여 상기 유한 상태 머신에서 상기 복수의 부스트 결정 그루터기들을 정렬하는 단계를 더 포함하는,

모바일 디바이스에서 모델들을 생성하는 방법.

청구항 10

모바일 컴퓨팅 디바이스로서,

동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성된 프로세서를 포함하고, 상기 동작들은:

유한 상태 머신을 포함하는 풀 분류기 모델을 수신하는 것 - 상기 유한 상태 머신은 복수의 부스트 결정 그루터기들로서의 표현에 적합한 정보를 포함하고, 각각의 부스트 결정 그루터기는 테스트 조건 및 가중값을 포함함 -;

상기 수신된 풀 분류기 모델에 포함된 상기 유한 상태 머신을 상기 복수의 부스트 결정 그루터기들로 변환함으로써 부스트 결정 그루터기들의 정렬된 리스트를 생성하는 것;

간결한 분류기 모델을 생성하기 위해 상기 생성된 부스트 결정 그루터기들의 정렬된 리스트를 선별하는 것 - 상기 선별하는 것은:

에너지 자원들에 기초하여 모바일 디바이스 거동을 분류하기 위해 평가할 상이한 테스트 조건들의 수를 결정하는 것;

테스트 조건들의 리스트가 상기 결정된 수의 상이한 테스트 조건들을 포함할 때까지, 상기 생성된 부스트 결정 그루터기들의 정렬된 리스트를 순차적으로 횡단하고 그리고 각각의 순차적으로 횡단된 부스트 결정 그루터기와 연관된 테스트 조건을 상기 테스트 조건들의 리스트에 삽입함으로써, 상기 결정된 수의 상이한 테스트 조건들을 포함하는 상기 테스트 조건들의 리스트를 생성하는 것; 및

상기 생성된 테스트 조건들의 리스트에 포함된 복수의 테스트 조건들 중 하나를 테스트하는 부스트 결정 그루터기들을 포함하도록 상기 간결한 분류기 모델을 생성하는 것을 포함함 -;

결과들을 생성하기 위해 상기 생성된 간결한 분류기 모델에 모바일 디바이스 거동 벡터를 적용하는 것; 및

상기 모바일 디바이스 거동을 분류하기 위해 상기 생성된 결과들을 사용하는 것을 포함하는,

모바일 컴퓨팅 디바이스.

청구항 11

제 10 항에 있어서,

상기 프로세서는,

상기 결과들을 생성하기 위해 상기 생성된 간결한 분류기 모델에 상기 모바일 디바이스 거동 벡터를 적용하는 것이:

상기 모바일 디바이스 거동 벡터에 포함된 수집된 거동 정보를 상기 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용하는 것;

상기 수집된 거동 정보를 상기 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용하는 것의 결과들의 가중된 평균을 계산하는 것; 및

상기 가중된 평균을 임계값과 비교하는 것을 포함하도록

동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되는,

모바일 컴퓨팅 디바이스.

청구항 12

제 10 항에 있어서,

상기 프로세서는,

상기 간결한 분류기 모델을 생성하는 것이:

상기 생성된 부스트 결정 그루터기들의 정렬된 리스트에 포함된 부스트 결정 그루터기들에 기초하여 간결한 분류기 모델들의 패밀리를 생성하는 것을 포함하도록

동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되고,

상기 간결한 분류기 모델들의 패밀리는 상기 간결한 분류기 모델 및 복수의 부가적인 간결한 분류기 모델들을 포함하고, 상기 복수의 부가적인 간결한 분류기 모델들 각각은 상이한 수의 상이한 테스트 조건들을 포함하는,

모바일 컴퓨팅 디바이스.

청구항 13

제 10 항에 있어서,

상기 프로세서는,

간결한 분류기 모델을 생성하는 것이:

상이한 가중값 및 상이한 임계값을 사용하여 제 1 조건을 테스트하는 결정 그루터기를 각각 포함하는 복수의 간결한 분류기 모델들을 생성하는 것을 포함하도록

동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되는,

모바일 컴퓨팅 디바이스.

청구항 14

제 10 항에 있어서,

상기 프로세서는,

상기 수신된 풀 분류기 모델에 기초하여 생성되는 복수의 간결한 분류기 모델들 내의 부스트 결정 그루터기들과 연관된 임계값들 및 가중값들을 재계산하는 것을 추가로 포함하는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되는,

모바일 컴퓨팅 디바이스.

청구항 15

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

상기 프로세서-실행가능 소프트웨어 명령들은 모바일 디바이스 내의 프로세서로 하여금 동작들을 수행하게 하도록 구성되고, 상기 동작들은:

유한 상태 머신을 포함하는 풀 분류기 모델을 수신하는 것 – 상기 유한 상태 머신은 복수의 부스트 결정 그루터기들로서의 표현에 적합한 정보를 포함하고, 각각의 부스트 결정 그루터기는 테스트 조건 및 가중값을 포함함 –;

상기 수신된 풀 분류기 모델에 포함된 상기 유한 상태 머신을 상기 복수의 부스트 결정 그루터기들로 변환함으로써 부스트 결정 그루터기들의 정렬된 리스트를 생성하는 것;

간결한 분류기 모델을 생성하기 위해 상기 생성된 부스트 결정 그루터기들의 정렬된 리스트를 선별하는 것 – 상기 선별하는 것은:

에너지 자원들에 기초하여 모바일 디바이스 거동을 분류하기 위해 평가할 상이한 테스트 조건들의 수를 결정하는 것;

테스트 조건들의 리스트가 상기 결정된 수의 상이한 테스트 조건들을 포함할 때까지, 상기 생성된 부스트 결정 그루터기들의 정렬된 리스트를 순차적으로 횡단하고 그리고 각각의 순차적으로 횡단된 부스트 결정 그루터기와 연관된 테스트 조건을 상기 테스트 조건들의 리스트에 삽입함으로써, 상기 결정된 수의 상이한 테스트 조건들을 포함하는 상기 테스트 조건들의 리스트를 생성하는 것; 및

상기 생성된 테스트 조건들의 리스트에 포함된 복수의 테스트 조건들 중 하나를 테스트하는 부스트 결정 그루터기들을 포함하도록 상기 간결한 분류기 모델을 생성하는 것을 포함함 -;

결과들을 생성하기 위해 상기 생성된 간결한 분류기 모델에 모바일 디바이스 거동 벡터를 적용하는 것; 및

상기 모바일 디바이스 거동을 분류하기 위해 상기 생성된 결과들을 사용하는 것을 포함하는,

비-일시적 컴퓨터 판독가능 저장 매체.

청구항 16

제 15 항에 있어서,

상기 저장된 프로세서-실행가능 소프트웨어 명령들은,

상기 결과들을 생성하기 위해 상기 생성된 간결한 분류기 모델에 상기 모바일 디바이스 거동 벡터를 적용하는 것이:

상기 모바일 디바이스 거동 벡터에 포함된 수집된 거동 정보를 상기 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용하는 것;

상기 수집된 거동 정보를 상기 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용하는 것의 결과들의 가중된 평균을 계산하는 것; 및

상기 가중된 평균을 임계값과 비교하는 것을 포함하도록

상기 모바일 디바이스 내의 프로세서로 하여금 동작들을 수행하게 하도록 구성되는,

비-일시적 컴퓨터 판독가능 저장 매체.

청구항 17

제 15 항에 있어서,

상기 저장된 프로세서-실행가능 소프트웨어 명령들은,

상기 간결한 분류기 모델을 생성하는 것이:

상기 생성된 부스트 결정 그루터기들의 정렬된 리스트에 포함된 부스트 결정 그루터기들에 기초하여 간결한 분류기 모델들의 패밀리를 생성하는 것을 포함하도록

상기 모바일 디바이스 내의 프로세서로 하여금 동작들을 수행하게 하도록 구성되고,

상기 간결한 분류기 모델들의 패밀리는 상기 간결한 분류기 모델 및 복수의 부가적인 간결한 분류기 모델들을 포함하고, 상기 복수의 부가적인 간결한 분류기 모델들 각각은 상이한 수의 상이한 테스트 조건들을 포함하는,

비-일시적 컴퓨터 판독가능 저장 매체.

청구항 18

제 15 항에 있어서,

상기 저장된 프로세서-실행가능 소프트웨어 명령들은,

간결한 분류기 모델을 생성하는 것이:

상이한 가중값 및 상이한 임계값을 사용하여 제 1 조건을 테스트하는 결정 그루터기를 각각 포함하는 복수의 간결한 분류기 모델들을 생성하는 것을 포함하도록

상기 모바일 디바이스 내의 프로세서로 하여금 동작들을 수행하게 하도록 구성되는,

비-일시적 컴퓨터 판독가능 저장 매체.

청구항 19

제 15 항에 있어서,

상기 저장된 프로세서-실행가능 소프트웨어 명령들은 상기 모바일 디바이스 내의 프로세서로 하여금,

상기 수신된 풀 분류기 모델에 기초하여 생성되는 복수의 간결한 분류기 모델들 내의 부스트 결정 그루터기들과 연관된 임계값들 및 가중값들을 재계산하는 것을 추가로 포함하는 동작들을 수행하게 하도록 구성되는,

비-일시적 컴퓨터 판독가능 저장 매체.

청구항 20

시스템으로서,

디바이스 프로세서를 포함하는 모바일 디바이스; 및

동작들을 수행하기 위한 서버-실행가능 명령들로 구성된 서버를 포함하고,

상기 동작들은:

모바일 디바이스 거동들에 대한 정보의 전집을 수신하는 것;

상기 정보의 전집에 기초하여, 테스트 조건 및 가중값을 각각 포함하는 복수의 부스트 결정 그루터기들로의 변환에 적합한 데이터를 포함하는 유한 상태 머신을 생성하는 것; 및

풀 분류기 모델로서 상기 유한 상태 머신을 상기 모바일 디바이스에 전송하는 것을 포함하고,

상기 모바일 디바이스 내의 상기 디바이스 프로세서는:

상기 풀 분류기 모델을 수신하는 것;

상기 수신된 풀 분류기 모델에 포함된 상기 유한 상태 머신을 상기 복수의 부스트 결정 그루터기들로 변환함으로써 부스트 결정 그루터기들의 정렬된 리스트를 생성하는 것;

간결한 분류기 모델을 생성하기 위해 상기 생성된 부스트 결정 그루터기들의 정렬된 리스트를 선별하는 것 - 상기 선별하는 것은:

상기 모바일 디바이스의 에너지 자원들에 기초하여 모바일 디바이스 거동을 분류하기 위해 평가할 상이한 테스트 조건들의 수를 결정하는 것;

테스트 조건들의 리스트가 상기 결정된 수의 상이한 테스트 조건들을 포함할 때까지, 상기 생성된 부스트 결정 그루터기들의 정렬된 리스트를 순차적으로 횡단하고 그리고 각각의 순차적으로 횡단된 부스트 결정 그루터기와 연관된 테스트 조건을 상기 테스트 조건들의 리스트에 삽입함으로써, 상기 결정된 수의 상이한 테스트 조건들을 포함하는 상기 테스트 조건들의 리스트를 생성하는 것; 및

상기 생성된 테스트 조건들의 리스트에 포함된 복수의 테스트 조건들 중 하나를 테스트하는 부스트 결정 그루터기들을 포함하도록 상기 간결한 분류기 모델을 생성하는 것을 포함함 -;

결과들을 생성하기 위해 상기 생성된 간결한 분류기 모델에 모바일 디바이스 거동 벡터를 적용하는 것; 및

상기 모바일 디바이스 거동을 분류하기 위해 상기 생성된 결과들을 사용하는 것

을 포함하는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되는,

시스템.

청구항 21

제 20 항에 있어서,

상기 디바이스 프로세서는,

상기 결과들을 생성하기 위해 상기 생성된 간결한 분류기 모델에 상기 모바일 디바이스 거동 벡터를 적용하는 것이:

상기 모바일 디바이스 거동 벡터에 포함된 수집된 거동 정보를 상기 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용하는 것;

상기 수집된 거동 정보를 상기 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용하는 것의 결과들의 가중된 평균을 계산하는 것; 및

상기 가중된 평균을 임계값과 비교하는 것을 포함하도록

동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되는,

시스템.

청구항 22

제 20 항에 있어서,

상기 디바이스 프로세서는,

상기 간결한 분류기 모델을 생성하는 것이:

상기 생성된 부스트 결정 그루터기들의 정렬된 리스트에 포함된 부스트 결정 그루터기들에 기초하여 간결한 분류기 모델들의 패밀리를 생성하는 것을 포함하도록

동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되고,

상기 간결한 분류기 모델들의 패밀리는 상기 간결한 분류기 모델 및 복수의 부가적인 간결한 분류기 모델들을 포함하고, 상기 복수의 부가적인 간결한 분류기 모델들 각각은 상이한 수의 상이한 테스트 조건들을 포함하는,

시스템.

청구항 23

제 20 항에 있어서,

상기 디바이스 프로세서는,

상기 간결한 분류기 모델을 생성하는 것이:

상이한 가중값 및 상이한 임계값을 사용하여 제 1 조건을 테스트하는 결정 그루터기를 각각 포함하는 복수의 간결한 분류기 모델들을 생성하는 것을 포함하도록

동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되는,

시스템.

청구항 24

제 23 항에 있어서,

상기 디바이스 프로세서는,

상기 수신된 풀 분류기 모델에 기초하여 상기 모바일 디바이스에서 생성되는 상기 복수의 간결한 분류기 모델들 내의 부스트 결정 그루터기들과 연관된 임계값들 및 가중값들을 재계산하는 것을 추가로 포함하는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되는,

시스템.

청구항 25

제 20 항에 있어서,

상기 서버는,

상기 유한 상태 머신을 생성하는 것이:

각각의 테스트 조건이 확률 값과 연관되고;

각각의 확률 값이, 상기 각각의 확률 값과 연관된 테스트 조건이 상기 모바일 디바이스로 하여금 상기 모바일 디바이스 거동이 양성인지 여부를 결정하는 것을 가능하게 할 가능성을 식별하게

상기 유한 상태 머신을 생성하는 것을 포함하도록 동작들을 수행하기 위한 서버-실행가능 명령들로 구성되고, 그리고

상기 서버는,

상기 풀 분류기 모델로서 상기 유한 상태 머신을 상기 모바일 디바이스에 전송하기 전에, 확률 값들에 기초하여 상기 유한 상태 머신에서 상기 복수의 부스트 결정 그루터기들을 정렬하는 것을 추가로 포함하는 동작들을 수행하기 위한 서버-실행가능 명령들로 구성되는,

시스템.

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

발명의 설명

기 술 분 야

[0001] [0001] 본 출원은, 2013년 9월 05일자로 출원된 "Methods and Systems of Using Boosted Decision Stumps and Joint Feature Selection and Pruning Algorithms for the Efficient Classification of Mobile Device Behaviors"란 명칭의 미국 가출원 제 61/874,129 호, 2013년 1월 2일자로 출원된 "On-Device Real-Time Behavior Analyzer"란 명칭의 미국 가특허 출원 제 61/748,217 호, 및 2013년 1월 2일자로 출원된 "Architecture for Client-Cloud Behavior Analyzer"란 명칭의 미국 가특허 출원 제 61/748,220 호에 대해 우선권의 이익을 주장하고, 상기 가출원들 모두의 전체 내용들은 이로써 인용에 의해 통합된다.

배 경 기 술

[0002] [0002] 셀룰러 및 무선 통신 기술들은 과거 수년에 걸쳐 폭발적인 성장을 보여왔다. 이러한 성장은 더 양호한 통신들, 하드웨어, 더 큰 네트워크들, 및 더 신뢰할 수 있는 프로토콜들에 의해 뒷받침되었다. 결과적으로, 무선 서비스 제공자들은 이제 그들의 고객들에게 정보, 자원들, 및 통신들에 대한 전례 없는 레벨들의 액세스를

제공할 수 있다.

[0003] [0003] 이들 서비스 강화들과 보조를 맞추기 위해, 모바일 전자 디바이스들(예를 들어, 셀룰러 폰들, 태블릿들, 랩톱들 등)은 한층 더 강력하고 복잡하게 되었다. 이러한 복잡성은 악성 소프트웨어, 소프트웨어 충돌들, 하드웨어 결함들, 및 다른 유사한 에러들 또는 현상들이 모바일 디바이스의 장기 및 계속적인 성능 및 전력 이용 레벨들에 부정적으로 영향을 미치는 새로운 기회들을 형성하였다. 따라서, 모바일 디바이스의 장기 및 계속적인 성능 및 전력 이용 레벨들에 부정적으로 영향을 미칠 수 있는 조건들 및/또는 모바일 디바이스 거동들(behaviors)을 식별 및 정정하는 것이 소비자들에게 유익하다.

발명의 내용

[0004] [0004] 다양한 양상들은 모바일 디바이스에서 간결한 거동 분류기 모델들을 생성하는 방법들을 포함하고, 상기 방법은 유한 상태 머신을 포함하는 풀 분류기 모델을 모바일 디바이스의 프로세서에서 수신하는 단계, 및 모바일 디바이스에서 간결한 분류기 모델을 생성하기 위해 풀 분류기 모델을 사용하는 단계를 포함할 수 있다. 유한 상태 머신은 복수의 부스트 결정 그루터기들로서의 표현 또는 변환에 적합한 정보를 포함할 수 있고, 부스트 결정 그루터기들 각각은 테스트 조건 및 가중값을 포함할 수 있다. 일 양상에서, 상기 방법은 모바일 디바이스의 거동을 양성(benign) 또는 양성이 아닌 것(즉, 악성, 성능 열화 등) 중 어느 하나로 분류하기 위해 모바일 디바이스에서 간결한 분류기 모델을 사용하는 단계를 더 포함할 수 있다.

[0005] [0005] 일 양상에서, 풀 분류기 모델에 기초하여 간결한 분류기 모델을 생성하는 단계는, 풀 분류기 모델에 포함된 유한 상태 머신을 부스트 결정 그루터기들의 리스트로 변환하는 단계, 및 부스트 결정 그루터기들의 리스트에 포함된 부스트 결정 그루터기들에 기초하여 간결한 분류기 모델을 생성하는 단계를 포함할 수 있다.

[0006] [0006] 일 양상에서, 풀 분류기 모델에 기초하여 간결한 분류기 모델을 생성하는 단계는, 모바일 디바이스의 과도한 양의 프로세싱, 메모리 또는 에너지 자원들을 소비하지 않고서, 모바일 디바이스 거동을 분류하기 위해 평가되어야 하는 고유한 테스트 조건들의 수를 결정하는 단계, 테스트 조건들의 리스트가 결정된 수의 고유한 테스트 조건들을 포함할 때까지, 부스트 결정 그루터기들의 리스트를 순차적으로 횡단(traversing)하고, 각각의 순차적으로 횡단된 부스트 결정 그루터기와 연관된 테스트 조건을 테스트 조건들의 리스트에 삽입함으로써, 테스트 조건들의 리스트를 생성하는 단계, 및 생성된 테스트 조건들의 리스트에 포함된 복수의 테스트 조건들 중 하나를 테스트하는 그러한 부스트 결정 그루터기들만을 포함하기 위한 간결한 분류기 모델을 생성하는 단계를 더 포함할 수 있다.

[0007] [0007] 일 양상에서, 상기 방법은, 수집된 거동 정보를 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용하고, 수집된 거동 정보를 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용하는 것의 결과들의 가중된 평균을 계산하고, 그리고 가중된 평균과 임계값을 비교함으로써, 모바일 디바이스의 거동을 양성 또는 양성이 아닌 것 중 어느 하나로 분류하기 위해 모바일 디바이스에서 간결한 분류기 모델을 사용하는 단계를 포함할 수 있다.

[0008] [0008] 일 양상에서, 풀 분류기 모델에 기초하여 간결한 분류기 모델을 생성하는 단계는, 풀 분류기 모델에 포함된 유한 상태 머신을 부스트 결정 그루터기들의 리스트로 변환하는 단계, 및 부스트 결정 그루터기들의 리스트에 포함된 부스트 결정 그루터기들에 기초하여 간결한 분류기 모델들의 패밀리(family)를 생성하는 단계를 포함할 수 있고, 간결한 분류기 모델들의 패밀리는 간결한 분류기 모델 및 복수의 부가적인 간결한 분류기 모델들을 포함하고, 복수의 부가적인 간결한 분류기 모델들 각각은 상이한 수의 고유한 테스트 조건들을 포함한다.

[0009] [0009] 일 양상에서, 간결한 분류기 모델을 생성하는 단계는, 상이한 가중값 및 상이한 임계값을 사용하여 제 1 조건을 테스트하는 결정 그루터기를 각각 포함하는 복수의 간결한 분류기 모델들을 생성하는 단계를 포함할 수 있다. 일 양상에서, 상기 방법은 풀 분류기 모델에 기초하여 모바일 디바이스에서 생성된 복수의 간결한 분류기 모델들 내의 부스트 결정 그루터기들과 연관된 임계값들을 재계산하는 단계를 더 포함할 수 있다. 일 양상에서, 상기 방법은 풀 분류기 모델에 기초하여 모바일 디바이스에서 생성된 복수의 간결한 분류기 모델들 내의 부스트 결정 그루터기들과 연관된 가중값들을 재계산하는 단계를 포함할 수 있다.

[0010] [0010] 일 양상에서, 상기 방법은 모바일 디바이스 거동들에 대한 정보의 전집(corpus)을 서버에서 수신하고, 그리고 복수의 부스트 결정 그루터기들로의 변환에 적합한 데이터를 포함하기 위해 모바일 디바이스 거동들에 대한 정보의 전집에 기초하여 상기 유한 상태 머신을 생성함으로써, 서버에서 풀 분류기 모델을 생성하는 단계, 및 풀 분류기 모델로서 유한 상태 머신을 모바일 디바이스로 전송하는 단계를 포함할 수 있다. 일 양상에서, 복수의 테스트 조건들 각각은, 가능성의 연관된 테스트 조건이 모바일 디바이스가 모바일 디바이스 거동이 양성

인지를 결정하는 것을 가능하게 할 가능성을 식별하는 확률 값과 연관되고, 상기 방법은, 풀 분류기 모델로서 유한 상태 머신을 모바일 디바이스로 전송하기 전에, 확률 값들에 기초하여 유한 상태 머신에서 복수의 부스트 결정 그루터기들을 조직하는 단계를 더 포함한다.

[0011] [0011] 추가의 양상들은 앞서 설명된 방법들의 동작들을 수행하기 위한 프로세서-실행 가능 명령들로 구성된 프로세서를 갖는 모바일 컴퓨팅 디바이스를 포함한다.

[0012] [0012] 추가의 양상들은 모바일 디바이스 내의 프로세서로 하여금 앞서 설명된 방법들의 동작들을 수행하게 하도록 구성된 프로세서-실행 가능 소프트웨어 명령들이 저장된 비일시적인 컴퓨터 판독 가능 저장 매체를 포함한다.

[0013] [0013] 추가의 양상들은, 디바이스 프로세서를 포함하는 모바일 디바이스, 및 동작들을 수행하기 위한 서버-실행 가능 명령들로 구성된 서버를 포함하고, 상기 동작들은, 모바일 디바이스 거동들에 대한 정보의 전집(corpus)을 수신하는 동작, 테스트 조건 및 가중값을 각각 포함하는 복수의 부스트 결정 그루터기들로의 변환에 적합한 데이터를 포함하는 유한 상태 머신을 상기 정보의 전집에 기초하여 생성하는 동작, 및 풀 분류기 모델로서 상기 유한 상태 머신을 상기 모바일 디바이스로 전송하는 동작을 포함한다. 일 양상에서, 디바이스 프로세서는 동작들을 수행하기 위한 프로세서-실행 가능 명령들로 구성될 수 있고, 상기 동작들은, 풀 분류기 모델을 수신하는 동작, 수신된 풀 분류기 모델에 기초하여 상기 모바일 디바이스에서 간결한 분류기 모델을 생성하는 동작, 및 상기 모바일 디바이스의 거동을 양성 또는 양성이 아닌 것 중 어느 하나로 분류하기 위해 상기 간결한 분류기 모델을 사용하는 동작을 포함한다.

[0014] [0014] 일 양상의 시스템에서, 디바이스 프로세서는, 상기 풀 분류기 모델에 기초하여 간결한 분류기 모델을 생성하는 동작이, 상기 풀 분류기 모델에 포함된 상기 유한 상태 머신을 부스트 결정 그루터기들의 리스트로 변환하는 동작, 상기 모바일 디바이스의 과도한 양의 프로세싱, 메모리 또는 에너지 자원들을 소비하지 않고서, 상기 모바일 디바이스의 거동을 분류하기 위해 평가되어야 하는 고유한 테스트 조건들의 수를 결정하는 동작, 테스트 조건들의 리스트가 결정된 수의 고유한 테스트 조건들을 포함할 때까지, 상기 부스트 결정 그루터기들의 리스트를 순차적으로 횡단하고, 각각의 순차적으로 횡단된 부스트 결정 그루터기와 연관된 테스트 조건을 상기 테스트 조건들의 리스트에 삽입함으로써, 상기 테스트 조건들의 리스트를 생성하는 동작, 및 생성된 테스트 조건들의 리스트에 포함된 복수의 테스트 조건들 중 하나를 테스트하는 상기 부스트 결정 그루터기들의 리스트에 포함된 부스트 결정 그루터기들을 포함하기 위한 상기 간결한 분류기 모델을 생성하는 동작을 포함하도록, 동작들을 수행하기 위한 프로세서-실행 가능 명령들로 구성될 수 있다.

[0015] [0015] 일 양상의 시스템에서, 디바이스 프로세서는, 상기 모바일 디바이스의 거동을 분류하기 위해 상기 간결한 분류기 모델을 사용하는 동작이, 수집된 거동 정보를 상기 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용하는 동작, 상기 수집된 거동 정보를 상기 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용하는 것의 결과들의 가중된 평균을 계산하는 동작, 및 상기 가중된 평균과 임계값을 비교하는 동작을 포함하도록, 동작들을 수행하기 위한 프로세서-실행 가능 명령들로 구성될 수 있다. 일 양상의 시스템에서, 디바이스 프로세서는, 상기 풀 분류기 모델에 기초하여 간결한 분류기 모델을 생성하는 동작이, 상기 풀 분류기 모델에 포함된 상기 유한 상태 머신을 부스트 결정 그루터기들의 리스트로 변환하는 동작, 및 상기 부스트 결정 그루터기들의 리스트에 포함된 부스트 결정 그루터기들에 기초하여 간결한 분류기 모델들의 패밀리를 생성하는 동작을 포함하도록, 동작들을 수행하기 위한 프로세서-실행 가능 명령들로 구성될 수 있고, 상기 간결한 분류기 모델들의 패밀리는 상기 간결한 분류기 모델 및 복수의 부가적인 간결한 분류기 모델들을 포함하고, 상기 복수의 부가적인 간결한 분류기 모델들 각각은 상이한 수의 고유한 테스트 조건들을 포함한다.

[0016] [0016] 일 양상의 시스템에서, 디바이스 프로세서는, 상기 풀 분류기 모델에 기초하여 간결한 분류기 모델을 생성하는 동작이, 상이한 가중값 및 상이한 임계값을 사용하여 제 1 조건을 테스트하는 결정 그루터기를 각각 포함하는 복수의 간결한 분류기 모델들을 생성하는 동작을 포함하도록, 동작들을 수행하기 위한 프로세서-실행 가능 명령들로 구성될 수 있다. 일 양상의 시스템에서, 디바이스 프로세서는, 복수의 간결한 분류기 모델들 내의 부스트 결정 그루터기들과 연관된 임계값들 및 가중값들을 재계산하는 동작을 더 포함하는 동작들을 수행하기 위한 프로세서-실행 가능 명령들로 구성될 수 있다.

[0017] [0017] 일 양상의 시스템에서, 서버는, 복수의 테스트 조건들 각각이 가능성의 연관된 테스트 조건이 모바일 디바이스 거동이 양성인지를 상기 모바일 디바이스가 결정하는 것을 가능하게 할 상기 가능성을 식별하는 확률 값과 연관되도록 동작들을 수행하기 위한 서버-실행 가능 명령들로 구성될 수 있다. 일 양상의 시스템에서, 서버는, 풀 분류기 모델로서 상기 유한 상태 머신을 상기 모바일 디바이스로 전송하기 전에, 상기 확률 값들에 기초

하여 상기 유한 상태 머신에서 상기 복수의 부스트 결정 그루터기들을 조직하는 동작을 더 포함하는 동작들을 수행하기 위한 서버-실행 가능 명령들로 구성될 수 있다.

도면의 간단한 설명

[0018] [0018] 본 명세서에 통합되고 본 명세서의 일부를 구성하는 첨부된 도면들은, 본 발명의 예시적인 양상들을 예시하고, 앞서 주어진 일반적인 설명 및 아래에서 주어지는 상세한 설명과 함께 본 발명의 특징들을 설명하도록 기능한다.

[0019] 도 1은, 다양한 양상들에서 사용하기에 적합한 예시적인 원격통신 시스템의 네트워크 컴포넌트들을 예시한 통신 시스템 블록도이다.

[0020] 도 2는, 특정 모바일 디바이스 거동이 악성인지, 성능-열화적인지, 의심스러운지 또는 양성인지를 결정하도록 구성된 일 양상의 모바일 디바이스에서의 예시적인 논리 컴포넌트들 및 정보 흐름들을 예시한 블록도이다.

[0021] 도 3은, 특정 모바일 디바이스 거동이 악성인지, 성능-열화적인지, 의심스러운지 또는 양성인지를 결정하기 위해 모바일 디바이스와 관련하여 작동하도록 구성된 네트워크 서버를 포함하는 일 양상의 시스템에서의 예시적인 컴포넌트들 및 정보 흐름을 예시한 블록도이다.

[0022] 도 4는, 데이터, 거동 벡터들 또는 분류기 모델들을 재-트레이닝하지 않고서, 풀(full) 분류기 모델로부터 타겟팅된 및 간결한(lean) 분류기 모델을 생성하도록 구성된 모바일 디바이스를 포함하는 일 양상의 시스템에서의 예시적인 컴포넌트들 및 정보 흐름들을 예시한 블록도이다.

[0023] 도 5a는, 네트워크 서버로부터 수신된 풀 분류기 모델에 포함되는 데이터 포인트들 및 특징들의 서브세트를 포함하는 간결한 분류기 모델을 모바일 디바이스에서 생성하는 일 양상의 모바일 디바이스 방법을 예시한 프로세스 흐름도이다.

[0024] 도 5b는, 모바일 디바이스에서 로컬적으로 간결한 분류기 모델을 생성하는 다른 양상의 모바일 디바이스 방법을 예시한 프로세스 흐름도이다.

[0025] 도 5c는, 모바일 디바이스의 거동을 분류하기 위해 로컬적으로 생성된 간결한 분류기 모델을 사용하는 일 양상의 모바일 디바이스 방법을 예시한 프로세스 흐름도이다.

[0026] 도 5d는, 모바일 디바이스에서 간결한 분류기 모델을 생성하는 또 다른 양상의 모바일 디바이스 방법을 예시한 프로세스 흐름도이다.

[0027] 도 6a는, 더 포커싱된 간결한 분류기 모델들을 생성하는데 있어서 모바일 디바이스에 의해 사용하기에 적합한 부스트 결정 그루터기들을 포함하는 풀 분류기 모델을 네트워크 서버에서 생성하는 일 양상의 네트워크 서버 방법을 예시한 프로세스 흐름도이다.

[0028] 도 6b는, 다양한 양상들에 따른, 부스트 결정 그루터기 분류기를 생성하기에 적합한 예시적인 방법을 예시한 프로세스 흐름도이다.

[0029] 도 7은 일 양상에 따른, 부스트 결정 그루터기들을 포함하는 분류기 모델들을 생성하는 예시적인 방법의 프로세스 흐름도이다.

[0030] 도 8은, 간결한 분류기 모델들을 생성하기 위해 모바일 디바이스 프로세서에 의해 사용되고 일 양상의 서버 프로세서에 의해 생성될 수 있는 예시적인 부스트 결정 그루터기들의 예시이다.

[0031] 도 9는, 일 양상에 따른, 동적 및 적응적 관측들을 수행하도록 구성된 관측기 모듈에서의 예시적인 논리 컴포넌트들 및 정보 흐름들을 예시한 블록도이다.

[0032] 도 10은, 다른 양상에 따른, 관측기 데몬들을 구현하는 컴퓨팅 시스템에서의 논리 컴포넌트들 및 정보 흐름들을 예시한 블록도이다.

[0033] 도 11은 모바일 디바이스들 상에서 적응적 관측들을 수행하기 위한 일 양상의 방법을 예시한 프로세스 흐름도이다.

[0034] 도 12는 일 양상에서 사용하기에 적합한 모바일 디바이스의 컴포넌트 블록도이다.

[0035] 도 13은 일 양상에서 사용하기에 적합한 서버 디바이스의 컴포넌트 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0019] [0036] 다양한 양상들은 첨부된 도면들을 참조하여 상세히 설명될 것이다. 가능한 경우에는 항상, 동일한 참조 번호들은 도면들 전반에 걸쳐 동일하거나 유사한 부분들을 지칭하도록 이용될 것이다. 특정한 예들에 대해 참조가 행해지고, 구현들은 예시적인 목적들이고, 본 발명 또는 청구항들의 범위를 제한하려는 의도가 아니다.

[0020] [0037] 단어 "예시적인"은 본 명세서에서 "예, 예증 또는 예시로서 기능하는"을 의미하도록 사용된다. 본 명세서에서 "예시적인" 것으로 설명되는 임의의 구현은 반드시 다른 구현들에 비해 선호되거나 유리한 것으로 해석될 필요는 없다.

[0021] [0038] 개요에서, 다양한 양상들은 시간에 걸쳐 모바일 디바이스의 성능 및/또는 전력 이용 레벨들을 종종 열화시키는 조건들 및/또는 모바일 디바이스 거동들을 효율적으로 식별, 분류, 모델링, 방지 및/또는 정정하기 위한 네트워크 서버들, 모바일 디바이스들, 시스템들 및 방법들을 포함한다. 네트워크 서버는 중앙 데이터베이스(예를 들면, "클라우드")로부터 다양한 조건들, 특징들, 거동들 및 교정 동작들에 대한 정보를 수신하고, 모바일 디바이스에 의해 하나 이상의 간결한 분류기 모델들로 빠르게 변환될 수 있는 포맷 또는 구조의 큰 전집의 거동 정보를 설명하는 풀 분류기 모델(즉, 데이터 또는 거동 모델)을 생성하기 위해 이러한 정보를 사용하도록 구성될 수 있다.

[0022] [0039] 일 양상에서, 풀 분류기 모델은 큰 전집의 거동 정보의 유한 상태 머신 디스크립션 또는 표현일 수 있다. 일 양상에서, 유한 상태 머신은 복수의 부스트 결정 그루터기들로서의 표현에 적합한 정보를 포함할 수 있다. 예를 들면, 유한 상태 머신은, 모바일 디바이스 거동이 양성인지 또는 시간에 걸쳐 그 모바일 디바이스의 성능 열화에 기여하는지를 결정하는 것에 관련된 특징들 및 데이터 포인트들 중 전부 또는 많은 것을 총괄적으로 식별, 설명, 테스트 또는 평가하는 부스트 결정 그루터기들의 패밀리로서 표현될 수 있는 정보 구조일 수 있다. 이어서, 네트워크 서버는 풀 분류기 모델(즉, 유한 상태 머신 및/또는 부스트 결정 그루터기들의 패밀리 등을 포함하는 정보 구조)을 모바일 디바이스로 전송할 수 있다.

[0023] [0040] 모바일 디바이스는, 다양한 레벨들의 복잡성(또는 "간결함(leanness)")의 간결한 분류기 모델 또는 간결한 분류기 모델들의 패밀리를 생성하기 위해 풀 분류기 모델을 수신 및 사용하도록 구성될 수 있다. 이를 달성하기 위해, 모바일 디바이스는, 감소된 수의 부스트 결정 그루터기들을 포함하고 및/또는 제한된 수의 테스트 조건들을 평가하는 간결한 분류기 모델을 생성하기 위해, 네트워크 서버로부터 수신된 풀 분류기 모델(본원에서 "풀 부스트 결정 그루터기 분류기 모델")에 포함된 강인한 부스트 결정 그루터기들의 패밀리를 선별할 수 있다. 풀 부스트 결정 그루터기 분류기 모델의 이러한 선별은: 부스트 결정 그루터기를 선택하고; 선택된 결정 그루터기와 동일한 모바일 디바이스 상태, 특징, 거동 또는 조건에 의존하는(그리고 따라서 하나의 결정 결과에 기초하여 적용될 수 있는) 모든 다른 부스트 결정 그루터기들을 식별하고; 동일한 모바일 디바이스 상태, 특징, 거동 또는 조건에 의존하는 선택된 및 모든 식별된 다른 부스트 결정 그루터기들을 간결한 분류기 모델에 포함시키고; 그리고 간결한 분류기 모델에 이미 포함되지 않은 제한된 수의 선택된 부스트 결정 그루터기들에 대해 프로세스를 반복함으로써 달성될 수 있다. 이러한 방식으로, 제한된 수의 상이한 모바일 디바이스 상태들, 특징들, 거동들 또는 조건들에 의존하는 모든 부스트 결정 그루터기들을 포함하는 간결한 분류기 모델이 생성될 수 있다. 이어서, 모바일 디바이스는, 과도한 양의 자신의 프로세싱, 메모리 또는 에너지 자원들을 소비하지 않고서, 모바일 디바이스 거동을 빠르게 분류하기 위해, 이러한 로컬적으로 생성된 간결한 분류기 모델을 사용할 수 있다.

[0024] [0041] 일 양상에서, 모바일 디바이스는, 상이한 간결함의 정도들의 간결한 분류기 모델들의 패밀리를 생성하기 위해, 상이한 수들의 상이한 모바일 디바이스 상태들, 특징들, 거동들 또는 조건들을 여러 번 사용하여 풀 부스트 결정 그루터기 분류기 모델을 선별하는 동작들을 수행할 수 있다. 간결한 분류기 모델을 생성하는데 사용되는 상이한 모바일 디바이스 상태들, 특징들, 거동들 또는 조건들의 수가 더 많을수록, 모델이 악성 또는 의심스러운 거동을 정확하게 식별할 가능성이 더 높을 것이지만, 더 많은 프로세싱 전력이 소비될 것이다. 따라서, 일 양상에서, 모바일 디바이스는 일상적으로 일군의 간결한 분류기 모델들 중 가장 간결한 것을 적용하도록 구성될 수 있다(즉, 모델은 가장 적은 수의 상이한 모바일 디바이스 상태들, 특징들, 거동들 또는 조건들에 기초함). 가장 간결한 분류기 모델에 의해 생성된 결과들이 의심스러운 경우에, 모바일 디바이스 프로세서는, 거동이 악성 또는 양성으로서 식별될 수 있는지를 결정하기 위해 더 많은 디바이스 상태들, 특징들, 거동들 또는 조건들을 평가하는 더 강한(즉, 덜 간결한) 분류기 모델을 적용할 수 있다. 그러한 덜 간결한 분류기 모델을 적

용함으로써 생성된 결과들이 여전히 의심스러운 경우에, 거동이 악성 또는 양성으로서 명확하게 분류될 때까지, 훨씬 더 강한(훨씬 덜 간결한) 분류기 모델이 적용될 수 있고, 기타 등등이다.

[0025] [0042] 그러한 거동들 및 교정 동작들에 대한 정보를 중앙 데이터베이스(예를 들면, "클라우드")에 저장하고, 시간에 걸쳐 각각의 모바일 디바이스의 성능 및 전력 이용 레벨들의 열화에 기여하는 요인들을 지능적으로 및 효율적으로 식별하기 위해 중앙 데이터베이스에 저장된 정보를 사용하도록 서로 협력하여 작동하도록 모바일 디바이스들 및 네트워크 서버들을 구성함으로써, 다양한 양상들은 모바일 디바이스가 모바일 디바이스의 성능-제한 및 원하지 않는 동작 조건들을 더 정확히 및 효율적으로 식별하고 이에 응답하는 것을 가능하게 한다.

[0026] [0043] 또한, 네트워크 서버에서 부스트 결정 그루터기들을 포함하는 분류기 모델들을 생성하고, 이러한 분류기들/모델들을 모바일 디바이스로 전송함으로써, 다양한 양상들은, 트레이닝 데이터를 액세스하거나 네트워크 서버, 중앙 데이터베이스, 또는 클라우드 네트워크/서버와 추가로 통신하지 않고서, 모바일 디바이스가 앞서 설명된 방식으로 부스트 결정 그루터기들의 수를 선별함으로써 모바일 디바이스에서 간결한(또는 더 포커싱된) 분류기 모델들을 빠르고 효율적으로 생성하도록 허용한다. 이것은 네트워크에 대한 모바일 디바이스의 의존성을 상당히 감소시키고, 모바일 디바이스의 성능 및 전력 소비 특성들을 추가로 개선한다.

[0027] [0044] 다수의 상이한 셀룰러 및 모바일 통신 서비스들 및 표준들이 장래에 이용가능하거나 고려되고, 이들 모두는 다양한 양상들을 구현할 수 있고 그로부터 이점이 있을 수 있다. 이러한 서비스들 및 표준들은, 예를 들어, 3세대 파트너쉽 프로젝트(3GPP), 롱 텀 에볼루션(LTE) 시스템들, 3세대 무선 모바일 통신 기술(3G), 4세대 무선 모바일 통신 기술(4G), GSM(global system for mobile communications), UMTS(universal mobile telecommunications system), 3GSM, GPRS(general packet radio service), CDMA(code division multiple access) 시스템들(예를 들어, cdmaOne, CDMA1020TM), EDGE(enhanced data rates for GSM evolution), AMPS(advanced mobile phone system), 디지털 AMPS(IS-136/TDMA), EV-DO(evolution-data optimized), DECT(digital enhanced cordless telecommunications), WiMAX(worldwide interoperability for microwave access), WLAN(wireless local area network), WPA A, WPA2(Wi-Fi Protected Access I & II), 및 iden(integrated digital enhanced network)을 포함한다. 이러한 기술들 각각은, 예를 들면, 음성, 데이터, 시그널링 및/또는 콘텐츠 메시지들의 송신 및 수신을 수반한다. 개별적인 원격통신 표준 또는 기술과 관련된 용어 및/또는 기술적 세부사항들에 대한 임의의 참조들이, 오직 예시의 목적이며, 문언 청구항에서 특별히 달리 언급되지 않으면, 청구항들의 범위를 특정 통신 시스템 또는 기술로 제한하려는 의도가 아님을 이해해야 한다.

[0028] [0045] "모바일 컴퓨팅 디바이스" 및 "모바일 디바이스"라는 용어들은, 셀룰러 전화기들, 스마트폰들, 퍼스널 또는 모바일 멀티-미디어 플레이어들, 개인 휴대 정보 단말기(PDA)들, 랩톱 컴퓨터들, 태블릿 컴퓨터들, 스마트북들, 울트라북들, 팜-톱 컴퓨터들, 무선 전자 메일 수신기들, 멀티미디어 인터넷 가능 셀룰러 전화기들, 무선 게이밍 제어기들, 및 성능이 중요한 프로그래머블 프로세서, 메모리를 포함하고 전력 보존 방법들이 유익하도록 배터리 전력 하에서 동작하는 유사한 퍼스널 전자 디바이스들 중 어느 하나 또는 전부를 지칭하기 위해 본 명세서에서 상호교환가능하게 사용된다. 다양한 양상들은 배터리 전력 상의 제한된 자원 및 실행을 갖는 스마트폰들과 같은 모바일 컴퓨팅 디바이스들에 특히 유용하지만, 양상들은 일반적으로 프로세서를 포함하고 애플리케이션 프로그램들을 실행하는 임의의 전자 디바이스에서 유용하다.

[0029] [0046] 일반적으로, 모바일 디바이스의 성능 및 전력 효율은 시간에 걸쳐 열화한다. 최근에, 안티-바이러스 회사들(예를 들어, McAfee, Symantec 등)은 이러한 열화를 늦추는 것을 목적으로 하는 모바일 안티-바이러스, 파이어월, 및 암호화 제품들을 마케팅하기 시작하였다. 그러나, 이들 솔루션들의 많은 것들은 모바일 디바이스 상에서의 계산 집약적인 스캐닝 엔진의 주기적 실행에 의존하고, 이는 모바일 디바이스의 프로세싱 및 배터리 자원을 많이 소모할 수 있고, 연장된 시간 기간들 동안 모바일 디바이스를 느리게 하거나 쓸모 없게 할 수 있고, 및/또는 그렇지 않다면 사용자 경험을 열화시킬 수 있다. 또한, 이들 솔루션들은 통상적으로 알려진 바이러스들 및 멀웨어(malware)를 검출하는 것에 한정되고, (예를 들면, 성능 열화가 바이러스들 또는 멀웨어에 의해 야기되지 않을 때) 시간에 걸쳐 모바일 디바이스의 열화에 기여하는데 종종 결합되는 다수의 복잡한 요인들 및/또는 상호작용을 해결하지 못한다. 이들 및 다른 이유들로 인해, 기존의 안티-바이러스, 파이어월, 및 암호화 제품들은, 시간에 걸친 모바일 디바이스의 열화에 기여할 수 있는 수많은 요인들을 식별하거나, 모바일 디바이스의 열화를 방지하거나, 노화하는 모바일 디바이스를 그것의 원래 상태로 효율적으로 복원하기 위한 적당한 솔루션들을 제공하지 않는다.

[0030] [0047] 컴퓨팅 디바이스 상에서 실행되는 애플리케이션 프로그램들 또는 프로세스들의 거동을 모델링하거나 머신 학습 기술들을 사용함으로써 악성 소프트웨어를 검출하기 위한 다양한 다른 솔루션들이 존재한다. 그러나,

이들 솔루션들 중 많은 것들은, 이러한 솔루션들이 매우 큰 전집의 데이터를 평가하는 것을 요구하거나, 개별적인 애플리케이션 프로그램 또는 프로세스를 평가하는 것으로 제한되거나, 모바일 디바이스에서 계산 집약적 프로세스들의 실행을 요구하기 때문에, 모바일 디바이스 상에서의 사용에 적합하지 않다. 이로써, 모바일 디바이스에서 그러한 솔루션들을 구현 또는 수행하는 것은 모바일 디바이스의 응답성, 성능 또는 전력 소비 특성들에 대한 상당한 부정적인 및/또는 사용자-지각 가능한 영향을 가질 수 있다. 이들 및 다른 이유들로 인해, 기존의 모델링 및 머신 학습 솔루션들은 현대 모바일 디바이스들의 복잡하고 여전히 자원-제한된 시스템들에서 사용하기에 매우 적합하지 않다.

[0031] [0048] 예를 들면, 기존의 머신 학습-기반 솔루션은, 특징 벡터를 입력으로서 취하는 모델을 도출하기 위해 트레이닝 데이터의 전집을 사용하도록 컴퓨팅 디바이스를 구성하는 것을 포함할 수 있다. 그러나, 그러한 솔루션은, 테스트 조건 및 가중값을 각각 포함하는 복수의 부스트 결정 그루터기들로의 변환 또는 부스트 결정 그루터기들로서의 표현에 적합한 유한 상태 머신(또는 다른 유사한 정보 구조)을 포함하는 풀 분류기 모델(또는 분류기 모델들의 패밀리)을 생성하지 않는다. 적어도 이러한 이유로, 그러한 솔루션들은, 모바일 디바이스의 응답성 또는 성능 또는 전력 소비 특성들에 상당한, 부정적인 또는 사용자 지각 가능한 영향을 갖지 않으면서, 모바일 디바이스 거동들을 빠르고 효율적으로 식별, 분석 및/또는 분류하는데 사용될 포커싱된 부스트 결정 그루터기들의 세트를 포함하는 간결한 분류기 모델을 빠르고 효율적으로 생성하기 위해 모바일 디바이스 프로세서에 의해 사용되지 않을 수 있다.

[0032] [0049] 모바일 디바이스들은 비교적 제한된 프로세싱, 메모리, 및 에너지 자원들을 갖는 자원 제약된 시스템들이다. 현대의 모바일 디바이스들은 또한 복잡한 시스템들이고, 악성이거나 그렇지 않다면 모바일 디바이스의 성능 열화에 기여할 수 있는 다양한 데이터 흐름들, 데이터 동작들(판독, 기록, 데이터 인코딩, 데이터 전송들 등), 프로세스들, 컴포넌트들, 거동들 또는 요인들(또는 이들의 조합들) 모두를 평가하는 것은 종종 실현 가능하지 않다. 이들 및 다른 이유들로, 사용자들, 운영 시스템들, 및/또는 애플리케이션 프로그램들(예를 들면, 안티-바이러스 소프트웨어 등)이 문제점들의 소스들을 정확하고 효율적으로 식별하고 및/또는 식별된 문제점들에 적절한 해결책들을 제공하는 것이 점점 더 어렵다. 결과적으로, 모바일 디바이스 사용자들은 현재, 시간에 걸쳐 모바일 디바이스의 성능 및 전력 이용 레벨들의 열하를 방지하기 위한 몇몇의 해결책들을 갖는다.

[0033] [0050] 다양한 양상들은, 모바일 디바이스의 성능 및/또는 전력 이용 레벨들을 시간에 걸쳐 종종 열화시키는 조건들 및/또는 모바일 디바이스 거동들을 효율적으로 식별, 분류, 모델링, 방지, 및/또는 정정하기 위한 네트워크 서버들, 모바일 디바이스들, 시스템들, 및 방법들을 포함한다.

[0034] [0051] 일 양상에서, 모바일 디바이스의 관측기 프로세스, 데몬, 모듈 또는 서브-시스템(본 명세서에서는 "모듈"로서 총칭됨)은 모바일 디바이스 시스템의 다양한 레벨들에서 다양한 API들, 레지스터들, 카운터들 또는 다른 컴포넌트들(본 명세서에서 총괄적으로 "설치된 컴포넌트들")을 설치 또는 조정할 수 있다. 관측기 모듈은, 설치된 컴포넌트들로부터 거동 정보를 수집함으로써 모바일 디바이스 거동들을 계속해서(또는 거의 계속해서) 모니터링할 수 있다. 모바일 디바이스는 또한 분석기 모듈을 포함할 수 있고, 관측기 모듈은 수집된 거동 정보를 (예를 들면, 메모리 기록 동작, 함수 호출 등을 통해) 모바일 디바이스의 분석기 모듈로 통신할 수 있다. 분석기 모듈은 거동 정보를 수신하고, 거동 벡터들을 생성하기 위해 거동 정보를 사용하고, 거동 벡터들에 기초하여 공간적 및/또는 시간적 상관들을 생성하고, 특정 모바일 디바이스 거동, 서브-시스템, 소프트웨어 애플리케이션, 또는 프로세스가 양성인지, 의심스러운지, 악성인지 또는 성능 열화적인지를 결정하기 위해 이러한 정보를 사용할 수 있다.

[0035] [0052] 분석기 모듈은, 모바일 디바이스 거동이 양성인지 또는 양성이 아닌지(예를 들면, 악성 또는 성능-열화)를 결정하기 위해 수집된 거동 정보에 대해 데이터, 알고리즘들, 분류기들 또는 거동 모델들(본 명세서에서 총괄적으로 "분류기 모델")을 수행, 실행 및/또는 적용하는 것을 포함하는 실시간 거동 분석 동작들을 수행하도록 구성될 수 있다. 각각의 분류기 모델은, 모바일 디바이스 거동의 특정 양상을 평가하기 위해 모바일 디바이스 프로세서에 의해 사용될 수 있는 정보를 포함하는 거동 모델일 수 있다. 분류기 모델들은 모바일 디바이스 상에 미리 설치되거나, 다운로딩되거나, 네트워크 서버로부터 수신되거나, 모바일 디바이스에서 생성되거나 이들의 임의의 조합일 수 있다. 분류기 모델은 머신 학습 및 다른 유사한 기술들을 사용함으로써 생성될 수 있다.

[0036] [0053] 각각의 분류기 모델은 풀 분류기 모델 또는 간결한 분류기 모델로서 카테고리화될 수 있다. 풀 분류기 모델은, 수천개의 특징들 및 수십억개의 엔트리들을 포함할 수 있는 대형 트레이닝 데이터세트의 기능으로서 생성된 강인한 데이터 모델일 수 있다. 간결한 분류기 모델은, 특정 모바일 디바이스 거동이 양성인지 또는 양성

이 아닌지(예를 들면, 악성 또는 성능-열화)를 결정하는 것에 가장 관련된 특징들/엔트리들만을 포함하는 감소된 데이터세트로부터 생성된 더 포커싱된 데이터 모델일 수 있다.

[0037] [0054] 앞서 언급된 바와 같이, 모바일 디바이스의 열화의 원인 또는 소스를 적절히 식별하기 위한 분석을 요구하는 수천개의 특징들/요인들 및 수십억개의 데이터 포인트들이 존재할 수 있다. 따라서, 분석기 모듈에 의해 사용되는 각각의 분류기 모델은, 특정 모바일 디바이스 거동이 양성인지 또는 양성이 아닌지(예를 들면, 악성 또는 성능-열화)에 관하여 모바일 디바이스가 정확히 결정할 수 있도록 하기 위해 매우 많은 수의 특징들, 요인들 및 데이터 포인트들에 대해 트레이닝되어야 한다. 하지만, 모바일 디바이스들이 자원 제한된 시스템들이기 때문에, 분석기 모듈이 이러한 특징들, 요인들 및 데이터 포인트들 모두를 평가하는 것은 종종 실현 가능하지 않다. 따라서, 분석기 모듈이, 모바일 디바이스 거동을 분류할 때 (간결한 분류기 모델이 아닌 경우) 분석을 요구할 모든 특징들, 요인들 및 데이터 포인트들 중 타겟팅된 서브세트를 평가하는 것을 포커싱한 간결한 분류기 모델들을 적용하는 것이 중요하다.

[0038] [0055] 다양한 양상들은, 특정 모바일 디바이스 거동이 양성인지 또는 양성이 아닌지(예를 들면, 악성 또는 성능-열화)를 결정하는 것에 가장 관련된 특징들, 요인들 및 데이터 포인트들을 지능적으로 및 효율적으로 식별하기 위해 서로 협력하여 작동하도록 구성된 모바일 디바이스들 및 네트워크 서버들을 포함한다. 네트워크 서버에서 부스트 결정 그루터기들을 포함하는 분류기 모델들을 생성하고, 이들 분류기들/모델들을 모바일 디바이스로 전송함으로써, 다양한 양상들은 모바일 디바이스가 모바일 디바이스에서 간결한 분류기 모델들을 빠르고 효율적으로 생성하도록 허용한다.

[0039] [0056] 다양한 양상들에서, 네트워크 서버는 모바일 디바이스 거동들 동안에 그러한 거동들 및 상태들, 특징들, 및 조건들에 관한 또는 그러한 거동들을 특징화하는 대량의 정보를 클라우드 서비스/네트워크로부터 수신하도록 구성될 수 있다. 이러한 정보는 모바일 디바이스 거동 벡터들의 매우 큰 클라우드 전집 형태일 수 있다. 네트워크 서버는, 거동 벡터들의 매우 큰 클라우드 전집을 정확히 설명하는 풀 분류기 모델(즉, 강인한 데이터/거동 모델)을 생성하기 위해 이러한 정보를 사용할 수 있다. 네트워크 서버는, 시간에 걸쳐 다수의 상이한 모바일 디바이스들 중 임의의 것의 열화에 기여할 수 있는 특징들, 데이터 포인트들 및/또는 요인들 중 대부분 또는 전부를 포함하기 위해 풀 분류기 모델을 생성할 수 있다.

[0040] [0057] 일 양상에서, 네트워크 서버는 부스트 결정 그루터기 또는 부스트 결정 그루터기의 패밀리와 같은 유한 상태 머신 표현 또는 표시를 포함하기 위해 풀 분류기 모델을 생성할 수 있다. 이러한 유한 상태 머신 표현 또는 표시는, 모바일 디바이스 프로세서에서의 선별 알고리즘들의 애플리케이션을 통해 모바일 디바이스에서 사용 또는 실행에 적합한 간결한 분류기 모델들로 빠르고 효율적으로 선별, 수정 또는 변환될 수 있다. 유한 상태 머신 표현 또는 표시는, 테스트 조건들, 상태 정보, 상태-전환 규칙들 및 다른 유사한 정보를 포함하는 정보 구조일 수 있다. 일 양상에서, 유한 상태 머신 표현 또는 표시는, 모바일 디바이스의 거동의 조건, 특징, 요인 또는 양상을 각각 평가 또는 테스트하는 부스트 결정 그루터기들의 대형 또는 강인한 패밀리를 포함하는 정보 구조일 수 있다.

[0041] [0058] 모바일 디바이스는 네트워크 서버로부터 풀 분류기 모델을 수신하고, 모바일 디바이스에서 로컬적으로 간결한 분류기 모델들(즉, 데이터/거동 모델들)을 생성하기 위해 수신된 풀 분류기 모델을 사용하도록 구성될 수 있다. 모바일 디바이스는, 수신된 풀 분류기 모델에 포함된 부스트 결정 그루터기들의 세트를, 감소 또는 제한된 수의 상이한 모바일 디바이스 상태들, 특징들, 거동들 또는 조건들을 식별, 테스트, 평가 및/또는 의존하는 부스트 결정 그루터기들의 서브세트로 선별함으로써 이들 로컬 간결한 분류기 모델들을 생성할 수 있다. 부스트 결정 그루터기들의 풀 세트의 이러한 선별은: 부스트 결정 그루터기를 선택하고; 동일한 모바일 디바이스 상태, 특징, 거동 또는 조건에 의존하는 모든 다른 부스트 결정 그루터기들을 선택된 결정 그루터기에 의존하는(그리고 따라서 하나의 결정 결과에 기초하여 적용될 수 있는) 모든 다른 부스트 결정 그루터기들을 식별하고; 동일한 모바일 디바이스 상태, 특징, 거동 또는 조건에 의존하는 선택된 및 모든 식별된 다른 부스트 결정 그루터기들을 간결한 분류기 모델에 포함시키고; 그리고 간결한 분류기 모델에 이미 포함되지 않은 감소된/제한된 수의 선택된 부스트 결정 그루터기들에 대해 프로세스를 반복함으로써 달성될 수 있다. 테스트되는 상이한 수들의 모바일 디바이스 상태들, 특징들, 거동들 또는 조건들을 사용하여 프로세스를 반복함으로써, 간결한 분류기 모델들의 패밀리는 평가되는 상태들, 특징들, 거동들 또는 조건들의 수에 의해 결정된 다양한 간결함의 정도로 생성될 수 있다. 또한, 이들 간결한 분류기 모델들 각각은, 평가된 테스트 결과들, 특징들 또는 조건들의 중요성에 할당된 상이한 가중치들 및/또는 상이한 임계값들을 사용하지만, 다른 간결한 분류기 모델과 동일한 특징들 또는 조건들 중 일부 또는 전부를 테스트 또는 평가할 수 있다. 이로써, 간결한 분류기 모델들을 생성 또는 재생성하는 프로세스는 결정 그루터기들과 연관된 임계값들 및/또는 가중치들을 재계산하는 것을 포함할

수 있다.

[0042] [0059] 이들 간결한 분류기 모델들이 (풀 분류기 모델과 비교하여) 테스트되어야 하는 감소된 상태들, 특징들, 거동들 또는 조건들의 서브세트를 포함하기 때문에, 관측기 및/또는 분석기 모듈들은, 모바일 디바이스의 과도한 양의 프로세싱, 메모리 또는 에너지 자원들을 소비하지 않고서, 모바일 디바이스 거동이 양성인지 모바일 디바이스의 성능 열화에 기여하는지를 빠르고 정확하게 결정하기 위해 이들을 사용할 수 있다. 앞서 언급된 바와 같이, 간결한 분류기 모델들의 패밀리 중 가장 간결한 분류기 모델(즉, 가장 적은 수의 테스트 조건들에 기초한 간결한 분류기 모델)은, 그 모델이 양성 또는 악성 중 어느 하나로서 카테고리화할 수 없는(그리고 따라서 모델에 의해 의심스러운 것으로 카테고리화된) 거동이 조우(encounter)될 때까지, 일상적으로 적용될 수 있고, 이때에, 거동을 양성 또는 악성 중 어느 하나로부터 카테고리화하기 위한 시도로 더 강인한(즉, 덜 간결한) 간결한 분류기 모델이 적용될 수 있다. 생성된 간결한 분류기 모델들의 패밀리 내의 훨씬 더 강인한 간결한 분류기 모델들의 적용은, 거동의 명확한 분류가 달성될 때까지 적용될 수 있다. 이러한 방식으로, 관측기 및/또는 분석기 모듈들은, 가장 완벽하지만 자원-집약적인 간결한 분류기 모델들의 사용을 강인한 분류기 모델이 거동을 명백히 분류하는데 필요로 되는 그러한 상황들로 제한함으로써, 효율성과 정확성 사이에서 절충(strike a balance)할 수 있다.

[0043] [0060] 다양한 양상들에서, 모바일 디바이스는, 유한 상태 머신 표시/표현을 부스트 결정 그루터기들로 변환하고, 풀 분류기 모델에 포함된 부스트 결정 그루터기들의 풀 세트를 제한된 수의 상이한 모바일 디바이스 상태들, 특징들, 거동들 또는 조건들에 의존하는 부스트 결정 그루터기들의 서브세트 또는 서브세트들로 선별하고, 그리고 모바일 디바이스 거동을 지능적으로 모니터링, 분석 및/또는 분류하기 위해 부스트 결정 그루터기들의 서브세트 또는 서브세트들을 사용함으로써 하나 이상의 간결한 분류기 모델들을 생성하도록 구성될 수 있다. 부스트 결정 그루터기들의 사용은 관측기 및/또는 분석기 모듈들이, 데이터를 재-트레이닝하기 위해 클라우드 또는 네트워크와 통신하지 않고서, 간결한 분류기 모델들을 생성 및 적용하도록 허용하고, 이것은 네트워크 서버 및 클라우드에 대한 모바일 디바이스의 의존성을 상당히 감소시킨다. 이것은 모바일 디바이스와 네트워크 서버 사이의 피드백 통신들을 제거하고, 이것은 또한 모바일 디바이스의 성능 및 전력 소비 특성들을 개선한다.

[0044] [0061] 부스트 결정 그루터기들은, 정확히 하나의 노드(및 따라서 하나의 테스트 질문 또는 테스트 조건) 및 가중값을 갖는 하나의 레벨 결정 트리들이고, 따라서 데이터/거동들의 이진(binary) 분류에서 사용하기에 매우 적합하다. 즉, 거동 벡터를 부스트 결정 그루터기에 적용하는 것은 이진 대답(예를 들면, 예 또는 아니오)을 발생시킨다. 예를 들면, 부스트 결정 그루터기에 의해 테스트되는 질문/조건이 "단문 메시지 서비스(SMS) 전송들의 빈도가 분 당 x 미만인가"인 경우에, "3"의 값을 부스트 결정 그루터기에 적용하는 것은 ("3 미만"의 SMS 전송들에 대해) "예" 대답 또는 ("3 이상"의 SMS 전송들에 대해) "아니오" 대답 중 어느 하나를 발생시킬 것이다.

[0045] [0062] 부스트 결정 그루터기들이 매우 간단하고 근본적이기(그리고 따라서 상당한 프로세싱 자원들을 요구하지 않기) 때문에, 부스트 결정 그루터기들이 효율적이다. 부스트 결정 그루터기들은 또한 매우 병행화 가능(parallelizable)하고, 따라서 많은 그루터기들이 (예를 들면, 모바일 디바이스 내의 다수의 코어들 또는 프로세서들에 의해) 동시에/동일한 시간에 적용 또는 테스트될 수 있다.

[0046] [0063] 아래에 설명되는 바와 같이, 네트워크 서버(또는 다른 컴퓨팅 디바이스)는 부스트 결정 트리 모델과 같이, 모바일 디바이스 거동들의 다른 더 복잡한 모델로부터 부스트 결정 그루터기-타입의 풀 분류기 모델을 생성할 수 있다. 그러한 복잡한 모델들은, 정교한 분류 시스템에서 모바일 디바이스 거동을 특징화하는 디바이스 상태들, 동작들 및 모니터링되는 노드들 사이의 상호작용들의 풀(또는 거의 풀) 세트를 상관시킬 수 있다. 앞서 언급된 바와 같이, 서버 또는 다른 컴퓨팅 디바이스는, 많은 수의 모바일 디바이스들로부터 수집된 모바일 디바이스들의 거동 벡터들의 클라우드 전집을 설명하는 모델들을 생성하기 위해 머신 학습 기술들을 적용함으로써, 풀, 복잡한 분류기 모델을 생성할 수 있다. 예로서, 부스트 결정 트리 분류기 모델은, 현재 모바일 디바이스 거동이 악성인지 또는 양성인지의 결정에 도달하기 위해 테스트 가능한 조건들의 결정 노드들을 통한 수백개의 경로들을 추적할 수 있다. 그러한 복잡한 모델들은 다수의 알려진 학습 및 상관 모델링 기술들을 사용하여 서버에서 생성될 수 있다. 그러한 복잡한 모델들이 많은 수백개의 모바일 디바이스들로부터의 데이터로부터 학습함으로써 악성 거동들을 정확하게 인식하는데 있어서 매우 효과적으로 될 수 있지만, 특정 모바일 디바이스의 구성 및 거동들에 대한 복잡한 모델들의 적용은, 특히 그 모델이 복잡한 다중레벨 결정 트리들을 수반하는 경우에, 상당한 프로세싱을 요구할 수 있다. 모바일 디바이스들이 통상적으로 자원 제한적이기 때문에, 그러한 모델들을 사용하는 것은 디바이스 성능 및 배터리 수명에 영향을 줄 수 있다.

[0047] [0064] 모바일 디바이스들에 의한 사용에 더 좋은 강인한 분류기 모델들을 렌더링하기 위해, 서버(예를 들면, 클라우드 서버 또는 네트워크 서버) 또는 다른 컴퓨팅 디바이스(예를 들면, 모바일 디바이스 또는 모바일 디바이스에 연결될 컴퓨터)는 복잡한 분류기 모델들을 대형 부스트 결정 그루터기 모델들로 변환할 수 있다. 결정 그루터기들에 수반된 더 간단한 결정들 및 병렬 프로세스들에서 그러한 분류기 모델들을 적용하기 위한 능력은, 모바일 디바이스들이 네트워크 서버에 의해 수행되는 분석들로부터 더 양호하게 이익을 얻는 것을 가능하게 할 수 있다. 또한, 아래에 논의되는 바와 같이, 부스트 결정 그루터기 풀 분류기 모델은, 아래에 설명되는 양상의 방법들을 사용하여 간결한 분류기 모델을 생성하기 위해 모바일 디바이스들에 의해 사용될 수 있다.

[0048] [0065] 일 양상에서, 부스트 결정 그루터기 풀 분류기 모델을 생성하는 서버 또는 다른 컴퓨팅 디바이스는, 아래에 더 상세히 설명되는 양상의 프로세스를 따름으로써 그렇게 할 수 있다. 요약하면, 서버 또는 다른 컴퓨팅 디바이스는 풀 복잡한 분류기 모델(예를 들면, 부스트 결정 트리 모델) 내에서 노드를 선택하고, 노드가 악성 거동을 예측하는 시간의 퍼센티지를 결정하기 위해 그 모델을 적용할 수 있다. 다시 말해서, 서버 또는 다른 컴퓨팅 디바이스는 노드의 하나의 브랜치를 선택하고, 브랜치가 악성 거동의 결정으로 유도되는 시간의 부분을 결정하기 위해 그 브랜치에 접속된 모든 후속 노드들 및 경로들을 따를 수 있다. 일 양상에서, 이러한 시간의 부분은 노드에 대한 "가중치" 요인을 계산하는데 사용될 수 있다. 예를 들면, 후속 경로가 시간의 80 %의 악성 거동 결론을 발생시키는 하나의 브랜치를 갖는 결정 노드는 0.8의 가중 계수와 연관될 수 있어서, 이러한 단일 결정 노드가 잠재적인 악성(및 따라서 의심스러운) 거동의 신뢰할 수 있는 표시자인 것을 나타낸다. 다른 예로서, 브랜치들이 악성 거동 결론으로 동일하게 유도될 수 있는 복잡한 분류기 모델 내의 결정 노드는, 악성 거동을 인식하는데 있어서 더 적은 도움을 제공할 것이고, 따라서 매우 낮은 가중 계수 또는 우선권이 제공될 수 있다.

[0049] [0066] 각각의 결정 노드로부터의 결과들을 추적하는 프로세스에서, 서버 또는 다른 컴퓨팅 디바이스는, 결정 노드가 이진(즉, "예" 또는 "아니오")이 아닌 경우에, 다양한 테스트 조건들을 각각의 노드에 적용할 수 있다. 예를 들면, 복잡한 분류기 모델은 다양한 값들(예를 들면, 분당 전송되는 SMS 메시지들의 수)을 수용할 수 있고, 궁극적인 결론은 그 값에 의존한다. 그러나, 값들의 범위들은 결정 그루터기들의 이진 성질과 불일치한다. 그래서, 서버 또는 다른 컴퓨팅 디바이스는, 값들에 의해 특징화된 조건들에 도움이 되는 그러한 노드들에 대한 다양한 이진 결정들 또는 테스트들을 개발할 수 있다. 예를 들면, 서버 또는 다른 컴퓨팅 디바이스는 복잡한 분류기 모델을 통해 "하나보다 더 많은", "십보다 더 많은" 및 "100보다 더 많은"과 같은 다수의 임계치 테스트들 또는 조건들을 생성 및 테스트할 수 있다. 그러한 임계치 테스트들은, 서버가 복잡한 모델을 연구하여 도달할 수 있는 결론들에 기초하여 서버에 의해 식별 또는 선택될 수 있다. 이어서, 각각의 그러한 임계치-기반 테스트는, 그의 예측값 및 따라서 그의 부스팅 요인을 결정하도록 테스트될 수 있는 단일 결정 그루터기로서 처리될 수 있다.

[0050] [0067] 복잡한 분류기 모델에서 모든 결정 노드들을 통해 이러한 프로세스를 따름으로서, 서버 또는 다른 컴퓨팅 디바이스는 복잡한 다중-계층 결정 모델을 매우 많은 수의 부스트 결정 그루터기들의 단일 계층 모델로 변환할 수 있다. 이어서, 서버 또는 다른 컴퓨팅 디바이스는, 매우 적은 예측 또는 분류 이득을 제공하는 테스트 조건들(예를 들면, "파워 온인가?")을 제거하기 위해, 값이 임계값 미만인 결정 그루터기들을 제거함으로써 모델을 손질할 수 있다.

[0051] [0068] 결과적인 그러한 그루터기들의 수가 풀 분류기 모델에서 클 수 있지만, 그루터기들의 이진 성질은 특히 자원 제약된 프로세서들에서 그들의 애플리케이션을 용이하게 할 수 있다. 일 양상에서, 서버 또는 다른 컴퓨팅 디바이스는 부스트 결정 그루터기 풀 분류기 모델을 모바일 디바이스들의 사용을 위해 모바일 디바이스들에 제공할 수 있다.

[0052] [0069] 부스트 결정 그루터기들의 대형 분류기 모델을 생성하는 프로세스는, 많은 모바일 디바이스들로부터의 입력들을 분석하고 풀, 복잡한 거동 분류기 모델을 생성하는 클라우드 서버에 의해 생성될 수 있는데, 왜냐하면 그러한 서버들이 분석을 완료하기 위한 프로세싱 자원 및 프로세싱 시간을 가질 것이기 때문이다. 그러나, 앞서 언급된 바와 같이, 양상의 방법들은 또한 심지어 모바일 디바이스를 비롯해서 다른 컴퓨팅 디바이스에 의해 수행될 수 있다. 이러한 양상에서, 서버(예를 들면, 클라우드 또는 네트워크 서버)는 풀, 복잡한 거동 분류기 모델을 다른 컴퓨팅 디바이스로 전달할 수 있고, 이어서, 다른 컴퓨팅 디바이스는, 앞서 서술되고 아래에 더 상세히 서술되는 바와 같이, 그 모델을 부스트 결정 그루터기 모델로 변환하기 위해 모델을 프로세싱할 수 있다. 예를 들면, 사용자가 사용자의 모바일 디바이스에 연결한 개인용 컴퓨터는 풀, 복잡한 거동 분류기 모델을 다운로딩하고, 이어서, 개인용 컴퓨터가 (예를 들면, 유선 또는 무선 데이터 링크를 통해) 모바일 디바이스에 대해 이용 가능하게 하는 대형 부스트 결정 그루터기 모델을 생성하기 위해 양상의 방법들을 수행할 수 있다. 다른

예로서, 모바일 디바이스는 풀, 복잡한 거동 분류기 모델을 다운로딩하고, 이어서, 모바일 디바이스가 메모리에 저장하는 대형 부스트 결정 그루터기 모델을 생성하기 위해, 가령, 모바일 디바이스가 충전되고 사용중이지 않은 늦은 밤 시간 동안에, 양상의 방법들을 수행할 수 있다. 서버 또는 다른 컴퓨팅 디바이스에 의해 구현되는 프로세스들이 매우 유사하기 때문에, 양상의 방법들은 서버에 의해 수행되는 것으로 아래에 더 상세히 설명된다. 그러나, 그러한 설명은 예시적인 목적이며, 청구항들에서 그렇게 구체적으로 언급되지 않는다면, 양상의 방법들을 서버 상에서 수행되는 것으로 제한하도록 의도되지 않는다.

[0053] [0070] 추가의 양상에서, 모바일 디바이스들은, 트레이닝 데이터를 액세스하지 않고서 그리고 모바일 디바이스의 과도한 양의 프로세싱, 메모리 또는 에너지 자원들을 소비하지 않고서, 결정 그루터기들에서 테스트되는 제한된 수의 요인들을 선택함으로써 간결한 분류기 모델들을 구축하기 위해 부스트 결정 그루터기들의 수신된 또는 자체-생성된 대형 분류기 모델을 사용하도록 구성될 수 있다. 분석기 모듈은, 멀웨어를 식별하고 디바이스 거동을 악성 또는 양성으로서 분류하기 위해 선택된 부스트 결정 그루터기들의 간결한 분류기 모델을 사용할 수 있다. 아래에 더 완전히 설명되는 바와 같이, 모바일 디바이스들은, 테스트될 모니터링할 특징들의 수(예를 들면, 15)를 결정하고, 제 1 특징을 선택하고, 그 특징의 테스트를 포함하는 부스트 결정 그루터기들 모두(예를 들면, 모니터링되는 특징으로부터 획득된 값에 기초한 임계치 테스트들을 갖는 모든 그루터기들)를 간결한 분류기에 통합하고, 그리고 간결한 분류기 모델에서 어드레싱되는 특징들의 수가 결정된 수일 때까지 이러한 프로세스를 반복함으로써 간결한 분류기 모델들을 생성할 수 있다. 그러한 간결한 분류기 모델 내의 부스트 결정 그루터기들의 수가 특징들의 수보다 상당히 더 클 수 있다는 것이 주목할 만하다.

[0054] [0071] 일 양상에서, 모바일 디바이스는, 복수의 부스트 결정 그루터기들로의 변환에 적합한 유한 상태 머신을 포함하는 풀 분류기 모델을 수신하도록 구성될 수 있다. 모바일 디바이스는 풀 분류기 모델에 기초하여 간결한 분류기 모델을 생성할 수 있고, 이것은 풀 분류기 모델의 유한 상태 머신을 부스트 결정 그루터기들로 변환하고 이들 부스트 결정 그루터기들을 간결한 분류기 모델로서 사용함으로써 달성될 수 있다.

[0055] [0072] 다양한 양상들은, 도 1에 예시된 예시적인 통신 시스템(100)과 같은 다양한 통신 시스템들 내에서 구현될 수 있다. 통상적인 셀 전화 네트워크(104)는, 가령, 전화 지상 라인들(예를 들어, POTS 네트워크, 미도시) 및 인터넷(110)을 통해, 모바일 디바이스들(102)(예를 들어, 셀 전화기들, 랩톱들, 태블릿들 등)과 다른 네트워크 목적지들 사이에 음성 호들 및 데이터를 연결하도록 동작하는, 네트워크 운영 센터(108)에 연결된 복수의 셀 기지국들(106)을 포함한다. 모바일 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 수 있다. 전화 네트워크(104)는 또한, 인터넷(110)에 대한 접속을 제공하는 네트워크 운영 센터(108) 내의 또는 네트워크 운영 센터(108)에 연결된 하나 이상의 서버들(114)을 포함할 수 있다.

[0056] [0073] 통신 시스템(100)은 전화 네트워크(104) 및 인터넷(110)에 연결된 네트워크 서버들(116)을 더 포함할 수 있다. 네트워크 서버(116)와 전화 네트워크(104) 사이의 연결은 인터넷(110)을 통해서 또는(점선 화살표에 의해 도시된 바와 같이) 사설 네트워크를 통한 것일 수 있다. 네트워크 서버(116)는 또한, 클라우드 서비스 제공자 네트워크(118)의 네트워크 인프라구조 내의 서버로서 구현될 수 있다. 네트워크 서버(116)와 모바일 디바이스들(102) 사이의 통신은 전화 네트워크(104), 인터넷(110), 사설 네트워크(예시되지 않음), 또는 이들의 임의의 조합을 통해 달성될 수 있다.

[0057] [0074] 네트워크 서버(116)는 간결한 데이터/거동 모델들을 모바일 디바이스(102)로 전송할 수 있고, 모바일 디바이스(102)는, 의심스러운 또는 성능-열화하는 모바일 디바이스 거동들, 소프트웨어 애플리케이션들, 프로세스 등을 식별하기 위해 간결한 데이터/거동 모델들을 수신 및 사용할 수 있다. 네트워크 서버(116)는 또한, 모바일 디바이스 데이터/거동 모델들을 대체, 업데이트, 생성 및/또는 유지하기 위해 분류 및 모델링 정보를 모바일 디바이스들(102)로 전송할 수 있다.

[0058] [0075] 모바일 디바이스(102)는 모바일 디바이스(102)에서 거동, 상태, 분류, 모델링, 성공률 및/또는 통계 정보를 수집하고, 분석을 위해 수집된 정보를 (예를 들면, 전화 네트워크(104)를 통해) 네트워크 서버(116)로 전송할 수 있다. 네트워크 서버(116)는, 추가로 타겟팅된 및/또는 감소된 특징들의 서브세트를 포함시키도록 간결한 데이터/거동 모델들 또는 분류/모델링 정보를 업데이트 또는 개선(refine)하기 위해, 모바일 디바이스(102)로부터 수신된 정보를 사용할 수 있다.

[0059] [0076] 일 양상에서, 모바일 디바이스(102)는, 모바일 디바이스(102)에서 추가로 타겟팅된 및/또는 감소된 특징들의 서브세트를 포함하는 간결한 분류기 모델들(또는 데이터/거동 모델들)을 생성, 업데이트 또는 개선하기 위해, 수집된 거동, 상태, 분류, 모델링, 성공률 및/또는 통계 정보를 사용하도록 구성될 수 있다. 이것은 모바

일 디바이스와 네트워크 서버(116) 사이의 피드백 통신들의 양을 감소시키고, 모바일 디바이스(102)의 성능 및 전력 소비 특성들을 개선한다.

[0060] [0077] 도 2는, 특정 모바일 디바이스 거동, 소프트웨어 애플리케이션, 또는 프로세스가 악성/성능-열화적, 의심스러운, 또는 양성인지 여부를 결정하도록 구성된 일 양상의 모바일 디바이스(102)에서의 예시적인 논리 컴포넌트들 및 정보 흐름들을 나타낸다. 도 2에 예시된 예에서, 모바일 디바이스(102)는 거동 관측기 모듈(202), 거동 분석기 모듈(204), 외부 컨텍스트 정보 모듈(206), 분류기 모듈(208) 및 작동기(actuator) 모듈(210)을 포함한다. 일 양상에서, 분류기 모듈(208)은 거동 분석기 모듈(204)의 부분으로서 구현될 수 있다. 일 양상에서, 거동 분석기 모듈(204)은 하나 이상의 분류기 모듈들(208)을 생성하도록 구성될 수 있고, 이들 각각은 하나 이상의 분류기들을 포함할 수 있다.

[0061] [0078] 모듈들(202-210) 각각은 소프트웨어, 하드웨어, 또는 이들의 임의의 조합으로 구현될 수 있다. 다양한 양상들에서, 모듈들(202-210)은 운영 시스템의 부분들 내에서(예를 들어, 커널 내에서, 커널 공간에서, 사용자 공간에서 등), 별개의 프로그램들 또는 애플리케이션들 내에서, 특수화된 하드웨어 버퍼들 또는 프로세서들에서, 또는 이들의 임의의 조합에서 구현될 수 있다. 일 양상에서, 모듈들(202-210)의 하나 이상은 모바일 디바이스(102)의 하나 이상의 프로세서들 상에서 실행되는 소프트웨어 명령들로서 구현될 수 있다.

[0062] [0079] 거동 관측기 모듈(202)은, 모바일 디바이스의 다양한 레벨들/모듈들에서 애플리케이션 프로그래밍 인터페이스들(API들)을 설치 또는 조정하고, 그리고 설치된 API들을 통해 다양한 레벨들/모듈들에서 모바일 디바이스 동작들 및 이벤트들(예를 들어, 시스템 이벤트들, 상태 변화들 등)을 모니터링/관측하고, 관측된 동작들/이벤트들에 관한 정보를 수집하고, 수집된 정보를 지능적으로 필터링하고, 필터링된 정보에 기초하여 하나 이상의 관측들을 생성하며, 생성된 관측들을 메모리에(예를 들어, 로그 파일 등에) 저장하고, 및/또는 생성된 관측들을 (예를 들어, 메모리 기록들, 함수 호출들 등을 통해) 거동 분석기 모듈(204)로 전송하도록 구성될 수 있다.

[0063] [0080] 거동 관측기 모듈(202)은, 애플리케이션 프레임워크 또는 런-타임 라이브러리들에서의 라이브러리 애플리케이션 프로그래밍 인터페이스(API) 호들, 시스템 호 API들, 파일-시스템 및 네트워킹 서브-시스템 동작들, (센서 디바이스들을 포함하는) 디바이스 상태 변화들, 및 다른 유사한 이벤트들에 관한 정보를 수집함으로써, 모바일 디바이스 동작들 및 이벤트들을 모니터링/관측할 수 있다. 거동 관측기 모듈(202)은 파일 명칭들, 파일 액세스들의 카테고리들(개인용 정보 또는 정규 데이터 파일들)을 검색하는 것, 파일들(예를 들어, exe, zip 타입 등)을 생성 또는 삭제하는 것, 파일 읽기/쓰기/탐색 동작들, 파일 허가들을 변경하는 것 등을 포함할 수 있는 파일 시스템 활동을 또한 모니터링할 수 있다.

[0064] [0081] 거동 관측기 모듈(202)은 또한, 연결들의 유형들, 프로토콜들, 포트 넘버들, 디바이스가 접속되는 서버/클라이언트, 접속들의 수, 통신들의 볼륨 또는 주파수 등을 포함할 수 있는 데이터 네트워크 활동을 모니터링할 수 있다. 거동 관측기 모듈(202)은, 전송되어 나간, 수신된, 또는 차단된 호들 또는 메시지들(예를 들어, SMS 등)의 유형 및 수(예를 들어, 배치된 프리미엄 호들의 수)를 모니터링하는 것을 포함할 수 있는, 전화 네트워크 활동을 모니터링할 수 있다.

[0065] [0082] 거동 관측기 모듈(202)은 또한, 시스템 자원 사용을 모니터링할 수 있고, 이는 포크들(forks)의 수, 메모리 액세스 동작들, 파일 개방의 수 등을 모니터링하는 것을 포함할 수 있다. 거동 관측기 모듈(202)은 모바일 디바이스의 상태를 모니터링할 수 있고, 이는 디스플레이가 온 또는 오프에 있는지 여부, 디바이스가 잠겨(lock) 있는지 또는 잠금해제(unlock)되어 있는지 여부, 잔여 배터리 양, 카메라의 상태 등과 같은 다양한 요인들을 모니터링하는 것을 포함할 수 있다. 거동 관측기 모듈(202)은 또한, 예를 들어, 중대한 서비스들(브라우저, 계약 제공자 등)에 대한 의도들, 인터-프로세스 통신들의 정도, 팝-업 윈도우들 등을 모니터링함으로써, 인터-프로세스 통신(inter-process communications; IPC)들을 모니터링할 수 있다.

[0066] [0083] 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 조정기들, 발진기들, 위상-동기 루프들, 주변 브릿지들, 및 모바일 컴퓨팅 디바이스 상에서 실행되는 프로세서들 및 클라이언트들을 지원하는데 사용되는 다른 유사한 컴포넌트들을 포함할 수 있는 하나 이상의 하드웨어 컴포넌트들의 드라이버 통계들 및/또는 상태를 모니터링/관측할 수 있다.

[0067] [0084] 거동 관측기 모듈(202)은 또한, 모바일 컴퓨팅 디바이스 및/또는 모바일 디바이스 서브-시스템들의 상태 또는 상황을 나타내는 하나 이상의 하드웨어 카운터들을 모니터링/관측할 수 있다. 하드웨어 카운터는, 모바일 컴퓨팅 디바이스에서 발생하는 하드웨어 관련 활동들 또는 이벤트들의 카운트 또는 상태를 저장하도록 구성된,

프로세서들/코어들의 특수 목적 레지스터를 포함할 수 있다.

[0068] [0085] 거동 관측기 모듈(202)은 또한 소프트웨어 애플리케이션들의 작동들 또는 동작들, 애플리케이션 다운로드 서버(예를 들면, Apple® App 스토어 서버)로부터의 소프트웨어 다운로드들, 소프트웨어 애플리케이션들에 의해 사용되는 모바일 디바이스 정보, 호 정보, 텍스트 메시징 정보(예를 들면, SendSMS, BlockSMS, ReadSMS 등), 미디어 메시징 정보(예를 들면, ReceiveMMS), 미디어 메시징 정보(예를 들면, ReceiveMMS), 사용자 어카운트 정보, 위치 정보, 카메라 정보, 가속도계 정보, 브라우저 정보, 브라우저-기반 통신들의 콘텐츠, 음성-기반 통신들의 콘텐츠, 단거리 라디오 통신들(예를 들면, 블루투쓰, WiFi 등), 텍스트-기반 통신들의 콘텐츠, 기록된 오디오 파일들의 콘텐츠, 폰북 또는 연락처 정보, 연락처 리스트들 등을 모니터링/관측할 수 있다.

[0069] [0086] 거동 관측기 모듈(202)은, 음성메일(VoicemailComm), 디바이스 식별자들(DeviceIDComm), 사용자 어카운트 정보(UserAccountComm), 캘린더 정보(CalendarComm), 위치 정보(LocationComm), 기록된 오디오 정보(RecordAudioComm), 가속도계 정보(AccelerometerComm) 등을 포함하는 통신들을 비롯해서, 모바일 디바이스의 전송들 또는 통신들을 모니터링/관측할 수 있다.

[0070] [0087] 거동 관측기 모듈(202)은 컴파스 정보, 모바일 디바이스 설정들, 배터리 수명, 자이로스코프 정보, 압력 센서들, 자석 센서들, 스크린 활동 등의 사용 및 이들에 대한 업데이트들/변화들을 모니터링/관측할 수 있다. 거동 관측기 모듈(202)은 소프트웨어 애플리케이션(AppNotification), 애플리케이션 업데이트들 등으로 및 등으로부터 통신되는 통지들을 모니터링/관측할 수 있다. 거동 관측기 모듈(202)은 제 2 소프트웨어 애플리케이션의 다운로딩 및/또는 설치를 요청하는 제 1 소프트웨어 애플리케이션에 관한 조건들 및/또는 이벤트들을 모니터링/관측할 수 있다. 거동 관측기 모듈(202)은 패스워드 입력 등과 같은 사용자 검증에 관한 조건들 또는 이벤트들을 모니터링/관측할 수 있다.

[0071] [0088] 거동 관측기 모듈(202)은 또한 애플리케이션 레벨, 라디오 레벨 및 센서 레벨을 비롯해서, 모바일 디바이스의 다수의 레벨들에서의 조건들 또는 이벤트들을 모니터링/관측할 수 있다. 애플리케이션 레벨 관측들은 안면 인식 소프트웨어를 통한 사용자의 관측, 소셜 스트림들의 관측, 사용자에 의해 입력된 노트들의 관측, 패스북/구글 월릿/페이팔의 사용에 관한 이벤트들의 관측 등을 포함할 수 있다. 애플리케이션 레벨 관측들은 또한 VPN들(virtual private networks)의 사용에 관련된 이벤트들 및 동기화, 음성 탐색들, 음성 제어(예를 들면, 하나의 단어를 얘기함으로써 폰을 잠금/잠금해제), 언어 번역기들, 계산들을 위한 데이터의 오프로딩, 비디오 스트리밍, 사용자 활동이 없는 카메라 사용, 사용자 활동이 없는 마이크로폰 사용 등에 관한 이벤트들의 관측을 포함할 수 있다.

[0072] [0089] 라디오 레벨 관측들은, 라디오 통신 링크들을 설정하거나 정보를 전송하기 전에 모바일 디바이스와의 사용자 상호 작용, 듀얼/다수의 SIM(subscriber identity module) 카드들, 인터넷 라디오, 모바일 폰 테더링, 계산들을 위한 데이터의 오프로딩, 디바이스 상태 통신들, 게임 제어기 또는 홈 제어기로서의 사용, 차량 통신들, 모바일 디바이스 동기화 등 중 임의의 것 또는 그 이상의 존재, 실재 또는 양을 결정하는 것을 포함할 수 있다. 라디오 레벨 관측들은 또한 포지셔닝을 위한 라디오들(WiFi, WiMax, 블루투쓰 등)의 사용, 피어-투-피어(p2p) 통신들, 동기화, 차량 대 차량 통신들 및/또는 머신-투-머신(m2m)의 모니터링을 포함할 수 있다. 라디오 레벨 관측들은 네트워크 트래픽 사용, 통계들 또는 프로파일들의 모니터링을 더 포함할 수 있다.

[0073] [0090] 센서 레벨 관측들은, 모바일 디바이스의 사용 및/또는 외부 환경을 결정하기 위해 자석 센서 또는 다른 센서를 모니터링하는 것을 포함할 수 있다. 예를 들면, 모바일 디바이스 프로세서는, 폰이 (예를 들면, 홀스터(holster) 내의 자석을 감지하도록 구성된 자석 센서를 통해) 홀스터 내에 있는지 또는 (예를 들면, 카메라 또는 광 센서에 의해 검출된 광의 양을 통해) 사용자의 포켓 내에 있는지를 결정하도록 구성될 수 있다. 모바일 디바이스가 홀스터 내에 있다는 것을 검출하는 것은, 예를 들면, 의심스러운 거동들을 인식하는 것에 관련될 수 있는데, 왜냐하면 모바일 디바이스가 홀스터에 있는 동안에 발생한 사용자에 의한 활성 사용에 관련된 활동들 및 기능들(예를 들면, 사진들 또는 비디오들의 촬영, 메시지들의 전송, 음성 호출의 실시, 사운드들의 기록 등)이 (예를 들면, 사용자를 추적하거나 스파이 활동을 하기 위해) 디바이스 상에서 실행되는 범죄의 프로세스들의 사인들일 수 있기 때문이다.

[0074] [0091] 사용 또는 외부 환경들에 관련된 센서 레벨 관측들의 다른 예들은 근거리장 통신들(NFC)을 검출하는 것, 신용 카드 스캐너, 바코드 스캐너 또는 모바일 태그 판독기로부터 정보를 수집하는 것, USB(universal serial bus) 전력 충전 소스의 존재를 검출하는 것, 키보드 또는 보조 디바이스가 모바일 디바이스에 연결되었다는 것을 검출하는 것, 모바일 디바이스가 (예를 들면, USB 등을 통해) 컴퓨팅 디바이스에 연결되었다는 것을 검출하는 것, LED, 플래시, 손전등 또는 광원이 수정 또는 디스에이블(예를 들면, 긴급 시그널링 앱 등을 악성으로 디

스에이블)되었는지를 결정하는 것, 스피커 또는 마이크로폰이 턴 온 또는 전력 공급된다는 것을 검출하는 것, 충전 또는 전력 이벤트를 검출하는 것, 모바일 디바이스가 게임 제어기로서 사용되고 있다는 것을 검출하는 것 등을 포함할 수 있다. 센서 레벨 관측들은 또한 의료 또는 건강관리 센서들로부터 또는 사용자의 신체를 스캐닝하는 것으로부터 정보를 수집하는 것, USB/오디오 잭에 플러깅된 외부 센서로부터 정보를 수집하는 것, (예를 들면, 진동 인터페이스 등을 통해) 촉각 또는 햅틱 센서로부터 정보를 수집하는 것, 모바일 디바이스의 열 상태에 관한 정보를 수집하는 것 등을 포함할 수 있다.

[0075] [0092] 모니터링되는 요인들의 수를 관리가능한 레벨로 감소시키기 위해, 일 양상에서, 거동 관측기 모듈(202)은, 모바일 디바이스의 열화에 기여할 수 있는 모든 요인들 중 작은 서브세트인 거동들 또는 요인들의 초기 세트를 모니터링/관측함으로써 코스(coarse) 관측들을 수행할 수 있다. 일 양상에서, 거동 관측기 모듈(202)은 네트워크 서버(116) 및/또는 클라우드 서비스 또는 네트워크(118) 내의 컴포넌트로부터 거동들 및/또는 요인들의 초기 세트를 수신할 수 있다. 일 양상에서, 거동들 및/또는 요인들의 초기 세트는 네트워크 서버(116) 또는 클라우드 서비스/네트워크(118)로부터 수신된 데이터/거동 모델들에 지정될 수 있다. 일 양상에서, 거동들 및/또는 요인들의 초기 세트는 RFM(reduced feature model)들에 지정될 수 있다.

[0076] [0093] 거동 분석기 모듈(204) 및/또는 분류기 모듈(208)은 거동 관측기 모듈(202)로부터 관측들을 수신하고, 수신된 정보(즉, 관측들)와 외부 컨텍스트 정보 모듈(206)로부터 수신된 컨텍스트 정보를 비교하고, 시간에 걸친 디바이스의 열화에 기여하는 (또는 기여할 가능성이 있는), 또는 그렇지 않으면 디바이스 상에서 문제들을 야기할 수 있는 수신된 관측들과 연관된 서브시스템들, 프로세스들 및/또는 애플리케이션들을 식별할 수 있다.

[0077] [0094] 일 양상에서, 거동 분석기 모듈(204) 및/또는 분류기 모듈(208)은 시간에 걸친 디바이스의 열화에 기여하는 (또는 기여할 가능성이 있는), 또는 그렇지 않으면 디바이스 상에서 문제들을 야기할 수 있는 거동들, 프로세스들, 또는 프로그램들을 식별하기 위해 제한된 세트의 정보(즉, 코스 관측들)를 이용하기 위한 지능을 포함할 수 있다. 예를 들어, 거동 분석기 모듈(204)은 다양한 모듈들(예를 들어, 거동 관측기 모듈(202), 외부 컨텍스트 정보 모듈(206) 등)로부터 수집된 (예를 들어, 관측들의 형태의) 정보를 분석하고, 모바일 디바이스의 정규 동작 거동들을 학습하고, 비교의 결과들에 기초하여 하나 이상의 거동 벡터들을 생성하도록 구성될 수 있다. 거동 분석기 모듈(204)은 추가의 분석을 위해 생성된 거동 벡터들을 분류기 모듈(208)로 전송할 수 있다.

[0078] [0095] 분류기 모듈(208)은 거동 벡터들을 수신하고, 특정 모바일 디바이스 거동, 소프트웨어 애플리케이션 또는 프로세스가 성능-열화/악성, 양성 또는 의심스러운지를 결정하기 위해 거동 벡터들과 하나 이상의 거동 모듈들과 비교할 수 있다.

[0079] [0096] 분류기 모듈(208)이 거동, 소프트웨어 애플리케이션 또는 프로세스가 악성이거나 성능-열화적이라고 결정할 때, 분류기 모듈(208)은 작동기 모듈(210)에 통지할 수 있고, 작동기 모듈(210)은, 악성 또는 성능-열화적인 것으로 결정된 모바일 디바이스 거동들을 정정하기 위한 다양한 작동들 또는 동작들을 수행하고 및/또는 식별된 문제를 치유, 치료, 격리 또는 그렇지 않다면 고치기 위한 동작들을 수행할 수 있다.

[0080] [0097] 분류기 모듈(208)이 거동, 소프트웨어 애플리케이션 또는 프로세스가 의심스러운 것으로 결정할 때, 분류기 모듈(208)은 거동 관측기 모듈(202)에 통지할 수 있고, 거동 관측기 모듈(202)은 자신의 관측들의 입도(granularity)(즉, 모바일 디바이스 거동들이 관측되는 세부 레벨)을 조정하고 및/또는 분류기 모듈(208)로부터 수신된 정보(예를 들면, 실시간 분석 동작들의 결과들)에 기초하여 관측된 거동들을 변경하고, 새로운 또는 부가적인 거동 정보를 생성 또는 수집하고, 추가의 분석/분류를 위해 새로운/부가적인 정보를 거동 분석기 모듈(204) 및/또는 분류기 모듈(208)로 전송할 수 있다. 거동 관측기 모듈(202)과 분류기 모듈(208) 사이의 그러한 피드백 통신들은 모바일 디바이스(102)가 관측들의 입도를 재귀적으로(recursively) 증가(즉, 더 미세하거나 더 상세한 관측들을 하거나)시키거나, 의심스러운 또는 성능-열화적인 모바일 디바이스 거동의 소스가 식별될 때까지, 프로세싱 또는 배터리 소비 임계치가 도달될 때까지, 또는 모바일 디바이스 프로세서가 의심스러운 또는 성능-열화적인 모바일 디바이스 거동의 소스가 관측 입도의 추가의 증가들로부터 식별될 수 없다고 결정할 때까지, 관측되는 특징들/거동들을 변경하는 것을 가능하게 한다. 그러한 피드백 통신은 또한 모바일 디바이스(102)가 모바일 디바이스의 과도한 양의 프로세싱, 메모리 또는 에너지 자원들을 소비하지 않고서 모바일 디바이스에서 로컬적으로 데이터/거동 모델들을 조정 또는 수정하는 것을 가능하게 한다.

[0081] [0098] 일 양상에서, 거동 관측기 모듈(202) 및 거동 분석기 모듈(204)은, 제한된 코스 관측들로부터 의심스러운 거동을 식별하고, 더 상세히 관측할 거동들을 동적으로 결정하고, 관측들을 위해 요구된 세부 레벨을 동적으

로 결정하기 위해, 개별적으로 또는 총괄적으로, 컴퓨팅 시스템의 거동들의 실시간 거동 분석을 제공할 수 있다. 이러한 방식으로, 거동 관측기 모듈(202)은 모바일 디바이스(102)가 디바이스에 대한 많은 양의 프로세서, 메모리 또는 배터리 자원들을 요구하지 않고서 모바일 디바이스들 상에서 발생하는 문제들을 효율적으로 식별 및 방지하는 것을 가능하게 한다.

[0082] [0099] 도 3 및 도 4는, 모바일 디바이스의 과도한 양의 프로세싱, 메모리 또는 에너지 자원들을 소비하지 않고서, 모바일 디바이스(102) 상의 활동적으로 악성 또는 열악하게 기록된 소프트웨어 애플리케이션들 및/또는 의심스러운 또는 성능-열화적인 모바일 디바이스 거동들을 지능적으로 및 효율적으로 식별하기 위해, 클라우드 서비스/네트워크(118)와 협력하여 작동하도록 구성된 네트워크 서버(116)를 포함하는 일 양상의 시스템(300) 내의 예시적인 컴포넌트들 및 정보 흐름들을 예시한다. 도 3에 예시된 예에서, 네트워크 서버(116)는 클라우드 모듈(302), 모델 생성기(304) 모듈 및 트레이닝 데이터 모듈(306)을 포함한다. 모바일 디바이스(102)는 거동 관측기 모듈(202), 분류기 모듈(208) 및 작동기 모듈(210)을 포함한다. 일 양상에서, 분류기 모듈(208)은 (도 2에 예시된) 거동 분석기 모듈(204)에 포함되거나 거동 분석기 모듈(204)의 부분일 수 있다. 일 양상에서, 모델 생성기(304) 모듈은 실시간 온라인 분류기일 수 있다.

[0083] [0100] 클라우드 모듈(302)은 클라우드 서비스/네트워크(118)로부터 대량의 정보를 수신하고, 시간에 걸쳐 모바일 디바이스의 열화에 기여할 수 있는 특징들, 데이터 포인트들 및/또는 요인들 중 대부분 또는 전부를 포함하는 풀 또는 강인한 데이터/거동 모델을 생성하도록 구성될 수 있다.

[0084] [0101] 모델 생성기(304) 모듈은 클라우드 모듈(302)에서 생성된 풀 모델에 기초하여 간결한 데이터/거동 모델들을 생성하도록 구성될 수 있다. 일 양상에서, 간결한 데이터/거동 모델들을 생성하는 것은, 클라우드 모듈(302)에 의해 생성된 풀 모델에 포함된 특징들 및 데이터 포인트들의 서브세트를 포함하는 하나 이상의 RFM들(reduced feature models)을 생성하는 것을 포함할 수 있다. 일 양상에서, 모델 생성기(304)는, 분류기 모듈(208)이 특정 모바일 디바이스 거동이 양성 또는 악성/성능-열화적인지를 결정적으로 결정하는 것을 가능하게 하는 최고의 가능성을 갖는 것으로 결정된 정보를 포함하는 초기 특징 세트(예를 들면, 초기의 감소된 특징 모델)를 포함하는 간결한 데이터/거동 모델을 생성할 수 있다. 모델 생성기(304)는 생성된 간결한 모델들을 거동 관측기 모듈(202)로 전송할 수 있다.

[0085] [0102] 거동 관측기 모듈(202)은 수신된 모델에 기초하여 모바일 디바이스 거동을 모니터링/관측하고, 관측들을 생성하고, 관측들을 분류기 모듈(208)로 전송할 수 있다. 분류기 모듈(208)은 실시간 분석 동작들을 수행할 수 있고, 실시간 분석 동작들은, 모바일 디바이스 거동이 양성인지, 의심스러운지 또는 악성/성능-열화적인지를 결정하기 위해 거동 관측기 모듈(202)에 의해 수집된 거동 정보에 데이터/거동 모델들을 적용하는 것을 포함할 수 있다. 분류기 모듈(208)은, 분류기 모듈(208)이 거동이 양성 또는 악성 중 어느 하나라고 분류 또는 결정적으로 결정하기에 충분한 정보를 갖지 않을 때, 모바일 디바이스 거동이 의심스럽다고 결정할 수 있다.

[0086] [0103] 분류기 모듈(208)은, 디바이스 거동이 의심스럽다고 분류기 모듈(208)이 결정할 때, 자신의 실시간 분석 동작들의 결과들을 거동 관측기 모듈(202)로 통신하도록 구성될 수 있다. 거동 관측기 모듈(202)은 자신의 관측들의 입도(즉, 모바일 디바이스가 관측되는 세부 레벨)를 조정하고 및/또는 분류기 모듈(208)로부터 수신된 정보에 기초하여(예를 들면, 실시간 분석 동작들의 결과들에 기초하여) 관측되는 거동들을 변경하고, 새로운 또는 부가적인 거동 정보를 생성 또는 수집하고, (예를 들면, 새로운 모델들의 형태의) 추가의 분석/분류를 위해 새로운/부가적인 거동 정보를 분류기 모듈로 전송할 수 있다. 이러한 방식으로, 모바일 디바이스(102)는 관측들의 입도를 재귀적으로 증가(즉, 더 미세하거나 더 상세한 관측들을 하거나)시키거나, 의심스러운 또는 성능-열화적인 모바일 디바이스 거동의 소스가 식별될 때까지, 프로세싱 또는 배터리 소비 임계치가 도달될 때까지, 또는 모바일 디바이스 프로세서가 의심스러운 또는 성능-열화적인 모바일 디바이스 거동의 소스가 관측 입도의 추가의 증가들로부터 식별될 수 없다고 결정할 때까지, 관측되는 특징들/거동들을 변경할 수 있다.

[0087] [0104] 모바일 디바이스(102)는, 자신의 동작들의 결과들 및/또는 모델들의 적용과 연관된 성공률들을 네트워크 서버(116)로 전송할 수 있다. 네트워크 서버(116)는 모델 생성기(304)에 의한 사용을 위해 결과들/성공률들에 기초하여 (예를 들면, 트레이닝 데이터 모듈(306)을 통해) 트레이닝 데이터를 생성할 수 있다. 모델 생성기는 트레이닝 데이터에 기초하여 업데이트된 모델들을 생성하고, 업데이트된 모델들을 모바일 디바이스(102)로 전송할 수 있다.

[0088] [0105] 도 4에 예시된 예에서, 모바일 디바이스(102)와 네트워크 서버(116) 사이에 어떠한 피드백 통신들도 존재하지 않는다. 오히려, 모바일 디바이스(102)는, 풀 모델 생성기(404)에서 생성되고 네트워크 서버(116)로부터 수신된 풀 또는 더 강인한 모델들에 기초하여 포커싱된/타겟팅된 거동 모델들 또는 분류기들을 생성하도록

구성된 간결한 모델 생성기 모듈(402)을 포함한다. 즉, 네트워크 서버(116)는 풀 분류기 모델들을 모바일 디바이스(102)로 전송하도록 구성될 수 있고, 모바일 디바이스(102)는 풀 분류기 모델에 기초하여 간결한 분류기 모델들을 생성하도록 구성될 수 있다. 이것은, 분류기 모델들에서 부스트 결정 그루터기들의 사용(또는 포함)으로 인해 모바일 디바이스의 과도한 양의 프로세싱 또는 배터리 자원들을 소비하지 않고서, 달성될 수 있다. 즉, 네트워크 서버(116)에서 부스트 결정 그루터기들을 포함하는 분류기 모델들을 생성하고, 이들 분류기들/모델들을 모바일 디바이스(102)로 전송함으로써, 다양한 양상들은, 간결한 모델 생성기 모듈(402)이, 트레이닝 데이터를 액세스하거나 네트워크 서버(116) 또는 클라우드 네트워크/서버(118)와 추가로 통신하지 않고서, 풀 분류기 모델에 포함된 부스트 결정 그루터기들의 수를 선별함으로써 모바일 디바이스(102)에서 간결한(또는 더 포커싱된) 분류기 모델들을 빠르고 효율적으로 생성하도록 허용한다. 이것은 네트워크 통신들에 대한 모바일 디바이스의 의존성을 상당히 감소시키고, 모바일 디바이스(102)의 성능 및 전력 소비 특성들을 추가로 개선한다.

[0089] [0106] 도 5a는 모바일 디바이스에서 간결한 또는 포커싱된 분류기/거동 모델(예를 들면, 모델 생성기 모듈(402)에 의해 생성된 모델 등)을 생성하는 일 양상의 방법(500)을 예시한다. 방법(500)은 모바일 디바이스 내의 프로세싱 코어에 의해 수행될 수 있다.

[0090] [0107] 방법(500)의 블록(502)에서, 프로세싱 코어는, 유한 상태 머신, 부스트 결정 그루터기들의 리스트 또는 다른 유사한 정보 구조인 또는 이들을 포함하는 풀 분류기 모델을 수신할 수 있다. 일 양상에서, 풀 분류기 모델은, 복수의 부스트 결정 그루터기들을 표현하기에 적합한 정보를 포함하고 및/또는 모바일 디바이스에 의한 복수의 부스트 결정 그루터기들로의 변환에 적합한 정보를 포함하는 유한 상태 머신을 포함한다. 일 양상에서, 유한 상태 머신은 정렬된 또는 우선 순위화된 부스트 결정 그루터기들의 리스트일 수 있다(또는 이를 포함할 수 있다). 부스트 결정 그루터기들 각각은 테스트 조건 및 가중값을 포함할 수 있다.

[0091] [0108] 앞서 논의된 바와 같이, 부스트 결정 그루터기들은, 정확히 하나의 노드(및 따라서 하나의 테스트 질문 또는 테스트 조건) 및 가중값을 갖고, 따라서 데이터/거동들의 이진 분류에 사용하기에 매우 적합한 하나의 레벨 결정 트리들이다. 이것은, 특징 벡터 또는 거동 벡터를 부스트 결정 그루터기에 적용하는 것이 이진 대답(예를 들면, 예 또는 아니오)을 발생시킨다는 것을 의미한다. 예를 들면, 부스트 결정 그루터기에 의해 테스트되는 질문/조건이 "SMS 전송들의 빈도가 분당 x 개 미만인가"이면, "3"의 값을 부스트 결정 그루터기에 적용하는 것은 ("3 개 미만"의 SMS 전송들에 대해) "예" 대답 또는 ("3 개 이상"의 SMS 전송들에 대해) "아니오" 대답 중 어느 하나를 발생시킬 것이다.

[0092] [0109] 도 5a로 복귀하면, 방법(500)의 블록(504)에서, 프로세싱 코어는, 모바일 디바이스의 과도한 양의 프로세싱, 메모리 또는 에너지 자원들을 소비하지 않고서, 모바일 디바이스 거동을 악성 또는 양성 중 어느 하나인 것으로 정확히 분류하기 위해 평가되어야 하는 고유한 테스트 조건들의 수를 결정할 수 있다. 이것은, 모바일 디바이스에서 이용 가능한 프로세싱, 메모리 및/또는 에너지 자원들의 양, 조건을 테스트하는데 요구된 모바일 디바이스의 프로세싱, 메모리 또는 에너지 자원들의 양을 결정하는 것, 조건을 테스트함으로써 모바일 디바이스에서 분석 또는 평가되는 거동 또는 조건과 연관된 우선순위 및/또는 복잡성을 결정하는 것, 및 모바일 디바이스의 이용 가능한 프로세싱, 메모리 또는 에너지 자원들의 소비, 조건을 테스트하는 것으로부터 달성되는 거동 분류의 정확성 및 조건에 의해 테스트되는 거동의 중요성 또는 우선순위 사이를 절충하거나 트레이드오프하기 위해 고유한 테스트 조건들의 수를 선택/결정하는 것을 포함할 수 있다.

[0093] [0110] 블록(506)에서, 프로세싱 코어는, 결정된 수의 고유한 테스트 조건들을 갖는 선택된 테스트 조건들의 리스트를 파퓰레이팅하기 시작하는 것으로부터 부스트 결정 그루터기들의 리스트를 횡단(traverse)할 수 있다. 일 양상에서, 프로세싱 코어는 또한 선택된 테스트 조건들 각각에 대한 절대 또는 상대적인 우선순위 값을 결정하고, 그들의 대응하는 테스트 조건들과 연관된 절대 또는 상대적인 우선순위 값을 선택된 테스트 조건들의 리스트에 저장할 수 있다.

[0094] [0111] 블록(508)에서, 프로세싱 코어는 선택된 테스트 조건들 중 하나를 테스트하는 풀 분류기 모델에 포함되는 모든 부스트 결정 그루터기들을 포함하는 간결한 분류기 모델을 생성할 수 있다. 일 양상에서, 프로세싱 코어는, 부스트 결정 그루터기들을 포함하거나 이들을 중요성 또는 우선순위 값의 순서로 표현하기 위해 간결한 분류기 모델을 생성할 수 있다.

[0095] [0112] 선택적인 블록(510)에서, 블록(506)에서 더 많은 수의 테스트 조건들에 대해 부스트 결정 그루터기들의 리스트를 횡단하는 동작들을 반복하고, 블록(508)에서 다른 간결한 분류기 모델을 생성함으로써, 다른 더 강인한(즉, 덜 간결한) 간결한 분류기 모델을 생성하기 위해, 고유한 테스트 조건들의 수가 증가될 수 있다. 이러

한 동작들은 간결한 분류기 모델들의 패밀리를 생성하기 위해 반복될 수 있다.

[0096] [0113] 도 5b는 모바일 디바이스에서 데이터 모델들을 생성하는 다른 양상의 방법(511)을 예시한다. 방법(511)은 모바일 디바이스 내의 프로세싱 코어에 의해 수행될 수 있다. 방법(511)의 블록(512)에서, 프로세싱 코어는 유한 상태 머신을 포함하는 풀 분류기 모델을 수신할 수 있다. 유한 상태 머신은, 복수의 부스트 결정 그루터기들로의 변환에 적합한 정보를 포함하는 정보 구조일 수 있다. 블록(514)에서, 프로세싱 코어는, 풀 분류기 모델에 포함된 유한 상태 머신을, 테스트 조건 및 가중값을 포함하는 부스트 결정 그루터기들로 변환할 수 있다.

[0097] [0114] 일 양상에서, 프로세싱 코어는 또한, 블록(512)에서 유한 상태 머신으로부터 생성되는 부스트 결정 그루터기들 각각에 대한 우선순위 값들을 계산 또는 결정할 수 있다. 프로세싱 코어는, 모바일 디바이스의 프로세싱, 메모리 또는 에너지 자원들의 소비, 거동 분류의 정확성 등 사이의 트레이드오프들을 밸런싱하기 위해 부스트 결정 그루터기들의 우선순위들을 결정할 수 있다. 프로세싱 코어는 또한, 부스트 결정 그루터기들의 연관된 가중값들, 거동을 정확히 분류하기 위한 테스트 조건들의 상대적인 또는 예측된 중요성 등에 기초하여 부스트 결정 그루터기들의 우선순위들을 결정할 수 있다.

[0098] [0115] 또한, 블록(512)에서, 프로세싱 코어는, 부스트 결정 그루터기들의 우선순위들에 따라 및/또는 그들의 중요성의 순서로 유한 상태 머신으로부터 생성되는 부스트 결정 그루터기들을 포함, 참조, 식별 및/또는 조직하는 제 1 리스트(또는 다른 정보 구조)를 생성할 수 있다. 예를 들면, 프로세싱 코어는, 제 1 아이템으로서 최고의 우선순위를 갖는 그루터기, 다음에 제 2 최고의 우선순위 값을 갖는 그루터기 등을 포함하는 정렬된 리스트인 제 1 리스트를 생성할 수 있다. 이러한 중요성의 순서는 또한 클라우드 전집으로부터 수집된 정보뿐만 아니라 선별 알고리즘이 실행되는 디바이스에 특정된 정보를 고려할 수 있다.

[0099] [0116] 블록(516)에서, 프로세싱 코어는, 간결한 분류기 모델을 적용할 때 평가되어야 하는 고유한 테스트 조건들(즉, 모바일 디바이스 상태들, 특징들, 거동들 또는 부스트 결정 그루터기들에서 테스트될 수 있는 조건들)의 수를 계산 또는 결정할 수 있다. 이러한 고유한 테스트 조건들의 수를 계산 또는 결정하는 것은 모델을 적용하는데 요구되는 모바일 디바이스의 프로세싱, 메모리 또는 에너지 자원들의 소비, 및 간결한 분류기 모델에서 달성되는 거동 분류의 정확성 사이를 절충 또는 트레이드오프하는 것을 수반할 수 있다. 그러한 결정은, 모바일 디바이스에서 이용 가능한 프로세싱, 메모리 및/또는 에너지 자원들의 양을 결정하는 것, 분석될 거동과 연관된 우선순위 및/또는 복잡성을 결정하는 것, 및 거동의 우선순위 및/또는 복잡성과 이용 가능한 자원들을 밸런싱하는 것을 포함할 수 있다.

[0100] [0117] 블록(518)에서, 프로세싱 코어는, 부스트 결정 그루터기들의 제 1 리스트를 순차적으로 횡단하고 각각의 횡단된 부스트 결정 그루터기와 연관된 테스트 조건 값들을 제 2 리스트에 삽입함으로써, 제 2 리스트를 생성할 수 있다. 프로세싱 코어는, 제 2 리스트의 길이가 고유한 테스트 조건들의 결정된 수와 동일할 때까지 또는 제 2 리스트가 결정된 수의 고유한 테스트 조건들 모두를 포함할 때까지, 계속해서 제 1 리스트를 횡단하고 값들을 제 2 리스트에 삽입할 수 있다.

[0101] [0118] 블록(520)에서, 프로세싱 코어는, 제 1 리스트에 포함된 부스트 결정 그루터기들에 기초하여 간결한 분류기 모델을 생성할 수 있다. 일 양상에서, 프로세싱 코어는, 제 2 리스트(즉, 블록(518)에서 생성된 테스트 조건들의 리스트)에 포함되는 테스트 조건들 중 하나를 테스트하는 부스트 결정 그루터기들만을 포함하기 위한 간결한 분류기 모델을 생성할 수 있다.

[0102] [0100] 선택적인 블록(522)에서, 블록(518)에서 더 많은 수의 테스트 조건들에 대한 부스트 결정 그루터기들의 리스트를 횡단하는 동작들을 반복하고, 블록(520)에서 다른 간결한 분류기 모델을 생성함으로써, 다른 더 강인한(즉, 덜 간결한) 간결한 분류기 모델을 생성하기 위해, 고유한 테스트 조건들의 수가 증가될 수 있다. 이들 동작들은 간결한 분류기 모델들의 패밀리를 생성하기 위해 반복될 수 있다.

[0103] [0119] 도 5c는 모바일 디바이스의 거동을 분류하기 위한 간결한 분류기 모델을 사용하는 일 양상의 방법(524)을 예시한다. 방법(524)은 모바일 디바이스 내의 프로세싱 코어에 의해 수행될 수 있다.

[0104] [0120] 방법(524)의 블록(526)에서, 프로세싱 코어는, 모바일 디바이스 시스템의 다양한 레벨들에서 설치된 다양한 컴포넌트들로부터 거동 정보를 수집하기 위해 관측들을 수행할 수 있다. 일 양상에서, 이것은 도 2를 참조하여 앞서 논의된 거동 관측기 모듈(202)을 통해 달성될 수 있다. 블록(528)에서, 프로세싱 코어는 관측들, 수집된 거동 정보 및/또는 모바일 디바이스 거동을 특징화하는 거동 벡터를 생성할 수 있다. 또한, 블록(528)에서, 프로세싱 코어는 간결한 분류기 모델 또는 다양한 레벨들의 복잡성(또는 "간결함")의 간결한 분류기 모델

들의 패밀리를 생성하기 위해 네트워크 서버로부터 수신된 풀 분류기 모델을 사용할 수 있다. 이를 달성하기 위해, 프로세싱 코어는, 감소된 수의 부스트 결정 그루터기들을 포함하고 및/또는 제한된 수의 테스트 조건들을 평가하는 간결한 분류기 모델들을 생성하기 위해 풀 분류기 모델에 포함된 부스트 결정 그루터기들의 패밀리를 선별할 수 있다.

[0105] [0121] 블록(529)에서, 프로세싱 코어는, 모바일 디바이스에 의해 아직 평가 또는 적용되지 않은 가장 간결한 분류기(즉, 가장 적은 수의 상이한 모바일 디바이스 상태들, 특징들, 거동들 또는 조건들에 기초한 모델)를 간결한 분류기 모델들의 패밀리에서 선택할 수 있다. 일 양상에서, 이것은, 프로세싱 코어가 분류기 모델들의 정렬된 리스트에서 제 1 분류기 모델을 선택함으로써 달성될 수 있다.

[0106] [0122] 블록(530)에서, 프로세싱 코어는 수집된 거동 정보 또는 거동 벡터들을 선택된 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용할 수 있다. 부스트 결정 그루터기들이 이진 결정들이고, 간결한 분류기 모델이 동일한 테스트 조건에 기초하는 많은 이진 결정들을 선택함으로써 생성되기 때문에, 거동 벡터를 간결한 분류기 모델 내의 부스트 결정 그루터기들에 적용하는 프로세스는 병렬 동작으로 수행될 수 있다. 대안적으로, 블록(530)에서 적용된 거동 벡터는, 간결한 분류기 모델에 포함된 제한된 수의 테스트 조건 파라미터들만을 포함하기 위해 트렁케이트(truncate) 또는 필터링될 수 있고, 이로써 모델을 적용하는데 있어서 계산 노력을 추가로 감소시킨다.

[0107] [0123] 블록(532)에서, 프로세싱 코어는, 수집된 거동 정보를 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용한 것의 결과들의 가중된 평균을 계산 또는 결정할 수 있다. 블록(534)에서, 프로세싱 코어는 계산된 가중된 평균과 임계값을 비교할 수 있다. 결정 블록(535)에서, 프로세싱 코어는, 이러한 비교의 결과들 및/또는 선택된 간결한 분류기 모델을 적용함으로써 생성된 결과들이 의심스러운지를 결정할 수 있다. 예를 들면, 프로세싱 코어는, 높은 신뢰도로 이들 결과들이 거동을 악성 또는 양성 중 어느 하나로 분류하고, 그렇지 않다면, 거동을 의심스러운 것으로 처리는데 사용될 수 있는지를 결정할 수 있다.

[0108] [0124] 결과들이 의심스러운 것으로 프로세싱 코어가 결정하면(예를 들면, 결정 블록(535) = "예"), 프로세싱 코어는, 거동이 높은 신뢰도로 악성 또는 양성으로서 분류될 때까지, 더 많은 디바이스 상태들, 특징들, 거동들 또는 조건들을 평가하는 더 강한(즉, 덜 간결한) 분류기 모델을 선택 및 적용하기 위해 블록들(529-534)의 동작들을 반복할 수 있다. 가령, 거동이 높은 신뢰도로 악성 또는 양성 중 어느 하나인 것으로 분류될 수 있다고 결정함으로써, 결과들이 의심스럽지 않다고 프로세싱 코어가 결정하면(예를 들면, 결정 블록(535) = "아니오"), 블록(536)에서, 프로세싱 코어는 모바일 디바이스의 거동을 양성 또는 잠재적으로 악성인 것으로 분류하기 위해 블록(534)에서 생성된 비교의 결과를 사용할 수 있다.

[0109] [0125] 도 5d에 예시된 대안적인 양상의 방법(540)에서, 블록들(518 및 520)을 참조하여 앞서 설명된 동작들은, 간결한 분류기 모델에 이미 존재하지 않는 부스트 결정 그루터기를 순차적으로 선택하고; 선택된 결정 그루터기와 동일한 모바일 디바이스 상태, 특징, 거동 또는 조건에 의존하는 (그리고 따라서 하나의 결정 결과에 기초하여 적용될 수 있는) 모든 다른 부스트 결정 그루터기들을 식별하고; 동일한 모바일 디바이스 상태, 특징, 거동 또는 조건에 의존하는 선택되고 식별된 모든 다른 부스트 결정 그루터기들을 간결한 분류기 모델에 포함시키고; 그리고 결정된 수의 테스트 조건들과 동일한 횟수로 프로세스를 반복함으로써 달성될 수 있다. 선택된 부스트 결정 그루터기와 동일한 테스트 조건에 의존하는 모든 부스트 결정 그루터기들이 매번 간결한 분류기 모델에 부가되기 때문에, 이러한 프로세스가 수행되는 횟수를 제한하는 것은 간결한 분류기 모델에 포함되는 테스트 조건들의 수를 제한할 것이다.

[0110] [0126] 도 5d를 참조하면, 블록(542)에서, 프로세싱 코어는, 간결한 분류기 모델에서 평가되어야 하는 고유한 테스트 조건들(즉, 모바일 디바이스 상태들, 특징들, 거동들, 또는 부스트 결정 그루터기에서 테스트될 수 있는 조건들)의 수(N)를 계산 또는 결정할 수 있다. 이러한 고유한 테스트 조건들의 수를 계산 또는 결정하는 것은 모델을 적용하는데 요구되는 모바일 디바이스의 프로세싱, 메모리 또는 에너지 자원들의 소비, 및 간결한 분류기 모델에 의해 달성되는 거동 분류의 정확성 사이를 절충 또는 트레이드오프하는 것을 수반할 수 있다. 그러한 결정은 모바일 디바이스에서 이용 가능한 프로세싱, 메모리 및/또는 에너지 자원들의 양을 결정하는 것, 분석될 거동과 연관된 우선순위 및/또는 복잡성을 결정하는 것, 및 거동의 우선순위 및/또는 복잡성과 이용 가능한 자원들을 밸런싱하는 것을 포함할 수 있다.

[0111] [0127] 블록(544)에서, 프로세싱 코어는 루프 카운트 변수의 값을 제로(0)와 동일하도록 설정하거나, 그렇지 않다면 결정된 횟수(N)로 수행될 루프를 개시할 수 있다. 블록(546)에서, 프로세싱 코어는, 부스트 결정 그루터기들의 풀 세트에 포함되거나 이로부터 생성되고 간결한 분류기 모델 리스트에 포함되지 않는 부스트 결정 그루

터기를 선택할 수 있다. 첫 회에, 루프를 통해, 간결한 분류기 모델 리스트에 어떠한 부스트 결정 그루터기들도 존재하지 않을 것이고, 그래서, 제 1 부스트 결정 그루터기가 선택될 것이다. 본 명세서에 언급된 바와 같이, 풀 분류기 모델은, 풀 세트 내의 제 1 부스트 결정 그루터기가 악성 또는 양성 거동을 인식할 최고의 가능성을 갖도록 구성될 수 있다. 블록(548)에서, 프로세싱 코어는 선택된 결정 그루터기와 연관된 테스트 조건을 결정할 수 있다. 블록(550)에서, 프로세싱 코어는, 선택된 결정 그루터기의 테스트 조건과 동일한 테스트 조건에 의존하거나 이를 포함 또는 테스트하는 풀 분류기 모델에 포함되거나 이로부터 생성되는 결정 그루터기들 모두를 식별할 수 있다. 블록(552)에서, 프로세싱 코어는, 동일한 테스트 조건에 의존하거나, 이를 포함 또는 테스트하는 식별된 부스트 결정 그루터기들 모두 및 선택된 부스트 결정 그루터기를 간결한 분류기 모델 리스트에 부가할 수 있다.

[0112] [0128] 블록(554)에서, 프로세싱 코어는 루프 카운트 변수의 값을 증분할 수 있다. 결정 블록(556)에서, 프로세싱 코어는, 루프 카운트 변수의 값이 블록(542)에서 결정된 고유한 테스트 조건들 중 수(N)보다 크거나 이와 동일한지를 결정할 수 있다. 루프 카운트 변수의 값이 고유한 테스트 조건들의 수보다 크거나 동일하지 않다고 프로세싱 코어가 결정하면(즉, 결정 블록(556) = "아니오"), 프로세싱 코어는 블록들(546-554)의 동작들을 반복할 수 있다. 루프 카운트 변수의 값이 고유한 테스트 조건들의 수보다 크거나 동일하다고 프로세싱 코어가 결정하면(즉, 결정 블록(556) = "예"), 블록(558)에서, 프로세싱 코어는, 모든 부스트 결정 그루터기들을 간결한 분류기 모델 리스트에 포함하기 위한 간결한 분류기 모델을 생성할 수 있다.

[0113] [0129] 이러한 방법(540)은, 간결한 분류기 모델 내의 고유한 테스트 조건들의 수(N)를 변경함으로써 다양한 강인함 또는 간결함의 정도의 간결한 분류기 모델들의 패밀리를 생성하기 위해 여러 번 사용될 수 있다. 예를 들면, 선택적인 블록(560)에서, 모바일 디바이스 프로세서는, 더 많은 테스트 조건들을 통합하는 다른 간결한 분류기 모델을 생성하기 위해, 블록(542)에서 결정된 고유한 테스트 조건들의 수(N)를 증가시킬 수 있다. 선택적인 결정 블록(562)에서, 프로세서는, 증가된 수(N)가 테스트 조건들의 최대수(max N)를 초과하는지를 결정할 수 있다. 테스트 조건들의 최대수는, 분류하기 어려운 거동들을 평가하는데 요구된 자원 투자 또는 최대 성능 패널티에 기초하여 (예를 들면, 개발자, 서비스 제공자, 사용자에 의해 또는 알고리즘을 통해) 결정될 수 있다. 증가된 수(N)가 최대 수(max N) 미만이면(즉, 결정 블록(562) = "아니오"), 앞서 설명된 블록들(544 내지 560)의 동작들은 다른 간결한 분류기 모델을 생성하기 위해 반복될 수 있다. 일단 최대수의 고유한 테스트 조건들이 간결한 분류기 모델에 포함되면(즉, 결정 블록(562) = "예"), 간결한 분류기 모델들을 생성하는 프로세스가 종료될 수 있다.

[0114] [0130] 도 5a, 도 5b 및 도 5d가 부스트 결정 그루터기들의 풀 세트를 횡단하는 전체 프로세스를 반복함으로써 간결한 분류기 모델들의 패밀리를 생성하는 것을 설명하지만, 생성된 간결한 분류기 모델(즉, 블록들(508, 520 및 558) 중 임의의 블록에서 생성된 모델)로 시작하여, 생성된 간결한 분류기 모델에 이미 포함되지 않은 테스트 조건에 의존하는 부스트 결정 그루터기들을 그 모델에 부가되는 부가된 수의 테스트 조건들에 대한 부스트 결정 그루터기들의 풀 세트를 횡단함으로써, 유사한 결과가 달성될 수 있다.

[0115] [0131] 또한, 도 5a, 도 5b 및 도 5d가 가장 간결한 것으로부터 가장 강인한 것까지 간결한 분류기 모델들의 패밀리를 생성하는 것을 설명하지만, 간단히 최대수(예를 들면, N = max N)의 테스트 조건들로 시작하여 매번 수를 감소시킴으로써, 가장 강인한 것으로부터 가장 간결한 것까지 간결한 분류기 모델들이 또한 생성될 수 있다.

[0116] [0132] 도 6a는 서버 또는 클라우드에서 풀 분류기를 생성하는 일 양상의 방법(600)을 예시한다. 방법(600)은, 클라우드 네트워크에 연결된 서버 컴퓨팅 디바이스 내의 프로세싱 코어에 의해 수행될 수 있다.

[0117] [0133] 블록(602)에서, 프로세싱 코어는, 많은 수의 디바이스 상태들, 구성들 및 거동뿐만 아니라, 악성 거동이 검출되었는지에 관한 정보를 비롯해서, 거동 데이터의 전집을 많은 모바일 디바이스들로부터 수집할 수 있다. 블록(604)에서, 프로세싱 코어는, 거동 데이터의 전집으로부터 디바이스 상태들, 구성들 및 거동 내에서 테스트될 수 있는 특정 이진 질문들/테스트 조건들을 식별할 수 있다. 디바이스 상태들, 구성들 및 거동들 전부를 특징화하기 위해, 많은 수의 그러한 이진 질문들/테스트 조건들이 통상적으로 식별될 것이다. 이어서, 블록(606)에서, 각각의 식별된 이진 질문에 대해, 프로세싱 코어는, 악성 거동이 이진 질문에 대한 대답들 중 하나 또는 다른 것에 대응하는 시간들의 부분 또는 퍼센티지를 결정하기 위해, 데이터베이스를 테스트할 수 있다. 블록(608)에서, 프로세싱 코어는 악성 거동에 대한 최고의 대응성을 갖는 이진 질문을, 대응성 퍼센티지에 기초하여 결정된 가중값을 갖는 제 1 결정 그루터기로서 선택할 수 있다. 블록(610)에서, 프로세싱 코어는, 도 6b를 참조하여 아래에 설명되는 바와 같이, 부정확하게 분류된 샘플들/테스트 조건들의 가중치를 부스팅할 수 있다.

[0118] [0134] 이어서, 서버의 프로세싱 코어는, 이러한 경우에 악성 거동에 대한 최고의 대응성을 갖는 질문을 식별하기 위해, 제 1 질문의 대답이 악성 거동과 연관되지 않은 값(예를 들면, "아니오")이라고 가정하는 이진 질문을 스캐닝하는 프로세스를 반복할 수 있다. 이어서, 그 질문은 모델에서 제 2 이진 질문으로서 설정되고, 그의 가중값은 그의 대응성 퍼센티지에 기초하여 결정된다. 이어서, 서버는, 이러한 경우에 악성 거동에 대한 최고의 대응성을 갖는 다음 질문/테스트 조건을 식별하기 위해, 이진 질문 - 제 1 질문들/테스트 조건들의 대답들이 악성 거동과 연관되지 않은 값들(예를 들면, "아니오")이라고 가정함 - 을 스캐닝하는 프로세스를 반복한다. 이어서, 그 질문/테스트 조건은 모델에서 제 3 이진 질문/테스트 조건이고, 그의 가중값은 그의 대응성 퍼센티지에 기초하여 결정된다. 이러한 프로세스는 완전한 세트를 구축하기 위해 식별된 이진 질문들/테스트 조건들 모두를 통해 계속된다.

[0119] [0135] 이진 질문/테스트 조건들을 생성하는 프로세스에서, 서버는 통신들의 빈도, 또는 이전 시간 간격 내의 통신들의 수와 같이 범위를 갖는 데이터를 평가하고, 거동들을 분류하는 것을 돕는 방식으로 범위를 포함하는 일련의 이진 질문/테스트 조건들을 공식화할 수 있다. 따라서, 하나의 이진 질문/테스트 조건은, 디바이스가 이전의 5 분 내에 0보다 더 많은 데이터 전송들을 전송하였는지일 수 있고(낮은 상관관계를 가질 수 있음), 제 2 이진 질문/테스트 조건은 디바이스가 이전의 5 분 내에 10보다 더 많은 데이터 전송들을 전송하였는지일 수 있고(중간 상관관계를 가질 수 있음), 제 3 질문/테스트 조건은 디바이스가 이전 5 분 내에 100보다 더 많은 데이터 전송들을 전송하였는지일 수 있다(높은 상관관계를 가질 수 있음).

[0120] [0136] 최종 세트의 질문/테스트 조건들의 일부 선별은, 가령, 악성 거동에 대한 결정된 가중치 또는 상관관계가 임계값 미만(예를 들면, 통계적으로 유의미한 것 미만)인 그러한 질문들/테스트 조건들을 제거하기 위해, 풀 분류기 세트가 모바일 디바이스들로 전송되기 전에 서버에 의해 이루어질 수 있다. 예를 들면, 악성 거동에 대한 상관관계가 대략 50/50인 경우에, 어떠한 대답도 현재 거동이 악성인지 또는 양성인지의 질문을 대답하는 것에 도움되지 않기 때문에, 그 결정 그루터기를 사용하는데 있어서 적은 이점이 존재할 수 있다.

[0121] [0137] 도 6b는, 다양한 양상들에 따라 사용하기에 적합한 부스트 결정 트리/분류기를 생성하기에 적합한 예시적인 부스팅 방법(620)을 예시한다. 동작(622)에서, 프로세서는 결정 트리/분류기를 생성 및/또는 실행하고, 결정 트리/분류기의 실행으로부터 트레이닝 샘플을 수집하고, 트레이닝 샘플에 기초하여 새로운 분류기 모델(h1(x))을 생성할 수 있다. 트레이닝 샘플은 모바일 디바이스 거동들, 소프트웨어 애플리케이션들 또는 모바일 디바이스 내의 프로세스들의 이전 관측들 또는 분석으로부터 수집된 정보를 포함할 수 있다. 트레이닝 샘플 및/또는 새로운 분류기 모델(h1(x))은 이전 분류기들에 포함된 질문 또는 테스트 조건들의 타입들에 기초하여 및/또는 거동 분석기 모듈(204)의 분류기 모듈(208) 내의 이전의 데이터/거동 모델들 또는 분류기들의 실행/적용으로부터 수집된 정확성 또는 성능 특성들에 기초하여 생성될 수 있다. 동작(624)에서, 프로세서는, 제 2 새로운 트리/분류기(h2(x))를 생성하기 위해, 생성된 결정 트리/분류기(h1(x))에 의해 잘못 분류된 엔트리들의 가중치를 부스팅(또는 증가)할 수 있다. 일 양상에서, 트레이닝 샘플 및 새로운 분류기 모델(h2(x))은 분류기의 이전 실행 또는 사용(h1(x))의 실수율(mistake rate)에 기초하여 생성될 수 있다. 일 양상에서, 트레이닝 샘플 및 새로운 분류기 모델(h2(x))은 분류기의 이전 실행 또는 사용 시에 데이터 포인트들의 오분류(misclassification) 또는 실수율에 기여한 것으로 결정된 속성들에 기초하여 생성될 수 있다.

[0122] [0138] 일 양상에서, 잘못 분류된 엔트리들은 자신들의 상대적인 정확성 또는 유효성에 기초하여 가중될 수 있다. 동작(626)에서, 프로세서는, 제 3 새로운 트리/분류기(h3(x))를 생성하기 위해, 생성된 제 2 트리/분류기(h2(x))에 의해 잘못 분류된 엔트리들의 가중치를 부스팅(또는 증가)할 수 있다. 동작(628)에서, 숫자 "t"의 새로운 트리/분류기들($h_t(x)$)을 생성하기 위해 (624-626)의 동작들이 반복될 수 있다.

[0123] [0139] 제 1 결정 트리/분류기(h1(x))에 의해 잘못 분류된 엔티티들의 가중치를 부스팅 또는 증가시킴으로써, 제 2 트리/분류기(h2(x))는 제 1 결정 트리/분류기(h1(x))에 의해 잘못 분류된 엔티티들을 더 정확하게 분류할 수 있지만, 또한 제 1 결정 트리/분류기(h1(x))에 의해 정확히 분류된 엔티티들 중 일부를 잘못 분류할 수 있다. 마찬가지로, 제 3 트리/분류기(h3(x))는 제 2 결정 트리/분류기(h2(x))에 의해 잘못 분류된 엔티티들을 더 정확하게 분류하지만, 제 2 결정 트리/분류기(h2(x))에 의해 정확히 분류된 엔티티들 중 일부를 잘못 분류할 수 있다. 즉, 트리/분류기들($h1(x)-h_t(x)$)의 패밀리는, 전체적으로 수렴하는 시스템을 발생시키지 않지만, 동시에 실행될 수 있는 다수의 결정 트리들/분류기들을 발생시킬 수 있다.

[0124] [0140] 도 7은, 모바일 디바이스의 과도한 양의 프로세싱, 메모리 또는 에너지 자원들을 소비하지 않고서, 모바일 디바이스(102)에 대한 활동적으로 악성 또는 열악하게 기록된 소프트웨어 애플리케이션들 및/또는 의심스러운 또는 성능-열화적인 모바일 디바이스 거동들을 지능적으로 및 효율적으로 식별하는데 사용될 수 있고 부스트

결정 그루터기들을 포함하는 분류기 모델들을 생성하는 예시적인 방법(700)을 예시한다. 방법(700)의 동작(1)에서, 네트워크 서버 내의 오프라인 분류기는 클라우드 서비스/네트워크로부터 수신된 정보에 기초하여 풀 또는 강인한 분류기 모델을 생성할 수 있다. 예를 들면, 풀 분류기는, 사십(40) 개의 고유한 조건들을 테스트하는 100 개의 부스트 결정 그루터기들을 포함할 수 있다. 방법(700)의 동작(2)에서, 풀 분류기 모델들은 모바일 디바이스(102) 내의 분석기/분류기 모듈(208)로 전송될 수 있다. 방법(700)의 동작(3)에서, 분석기/분류기 모듈(208)은 풀 분류기 모델을 분석한 것에 기초하여 부스트 결정 그루터기들의 형태의 간결한 데이터/거동 모델들 분류기들의 세트를 생성할 수 있다. 이것은 "공동의 특징 선택 및 선별" 동작들을 수행함으로써 달성될 수 있고, 상기 동작들은 모바일 디바이스가 클라우드 트레이닝 데이터에 대한 액세스를 필요로 하지 않고 온-디-플라이(on-the-fly) 방식으로 간결한 모델들 생성하고; 분류 정확성을 개선하기 위해 애플리케이션마다 분류기들을 동적으로 재구성하고; 그리고 각각의 분류기에 대한 결정적인 복잡성(예를 들면, O(그루터기들의 #))을 특정하도록 허용한다. "공동의 특징 선택 및 선별" 동작들은 또한 특징 선택 동작들을 수행하는 것을 포함할 수 있다.

[0125] [0141] 도 8은, 모바일 디바이스에서 간결한 분류기 모델들을 생성하기 위해 디바이스 프로세서에 의해 사용되고 일 양상의 서버 프로세서에 의해 생성될 수 있는 예시적인 부스트 결정 그루터기들(800)을 예시한다. 도 8에 예시된 예에서, 부스트 결정 그루터기들(800)은, 각각 질문 또는 테스트 조건(예를 들면, F1, F3, F5)을 포함하고, 프로세서에 의해 실행 또는 수행될 때, 확정적인 이진 대답(예를 들면, 참 또는 거짓, 악성 또는 양성 등) 중 어느 하나를 발생시킬 수 있는 복수의 결정 노드들(W1-W4)을 포함한다. 각각의 결정 노드들(W1-W4)은 또한 가중값과 연관될 수 있다.

[0126] [0142] 도 8은 또한 도 7을 참조하여 앞서 논의된 "공동의 특징 선택 및 선별" 동작들을 수행하는 방법(802)을 예시한다. 방법(802)은, 모바일 디바이스의 분석기 모듈이 자신이 2 개의 고유한 조건들을 테스트하는 간결한 분류기를 생성할 필요가 있다고 결정하는 것을 포함할 수 있고, 이러한 경우에, 특징 선택 동작들은, 첫 번째 2 개의 고유한 조건들(예를 들면, 도 8의 F1 및 F3)이 발견될 때까지 100 개의 부스트 결정 그루터기들의 리스트를 횡단하는 것을 포함할 수 있다. 이어서, 분석기/분류기 모듈(208)은 특징 선택 동작들에 의해 식별된 조건들(예를 들면, F1 및 F3)만을 테스트할 수 있고, 이것은, 100 개의 부스트 결정 그루터기들의 전체 리스트를 횡단하고 상이한 조건(예를 들면, F5)을 테스트하는 임의의 그루터기를 삭제함으로써 달성될 수 있다. 남아있는 부스트 결정 그루터기들(즉, 조건들("F1" 및 "F3")을 테스트하는 그루터기들)은, 데이터를 재트레이닝하지 않고서 간결한 분류기로서 사용될 수 있다. 분석기/분류기 모듈(208)은 거동 정보를 남아있는 부스트 결정 그루터기들(즉, 조건들("F1" 및 "F3")을 테스트하는 그루터기들) 각각에 적용하고, 남아있는 그루터기들로부터 수신된 대답들 모두의 가중된 평균을 계산하고, 모바일 디바이스 거동이 악성인지 또는 양성인지를 결정하기 위해 가중된 평균을 사용할 수 있다.

[0127] [0143] 일단 부스트 결정 그루터기들이 특징 선택 및 선별 프로세스를 통해 생성되면, 선택된 결정 그루터기들은, 현재 디바이스 상태들, 설정들 및 거동들에 대해 비교될 수 있는 분류기 또는 거동 모델로서 사용될 수 있다. 결정 그루터기들이 독립적인 이진 테스트들이기 때문에, 거동 벡터로 요약될 수 있는 관측된 거동들과 그 모델을 비교하는 거동 분석 프로세스는 동시에 수행될 수 있다. 또한, 그루터기들이 매우 간단하기 때문에(기본적으로 이진), 각각의 그루터기를 수행하기 위한 프로세싱은 매우 간단하고, 따라서 더 적은 프로세싱 오버헤드로 빠르게 달성될 수 있다. 각각의 결정 그루터기는 가중값을 갖는 대답을 산출하고, 거동들이 악성 또는 양성인지에 관한 궁극적인 결정은 모든 결과들의 가중된 합산으로서 결정될 수 있고, 이것이 간단한 계산이다.

[0128] [0144] 노드와 연관된 가중치는 모바일 디바이스 거동들, 소프트웨어 애플리케이션들 또는 모바일 디바이스 내의 프로세스들의 이전의 관측들 또는 분석으로부터 수집된 정보에 기초하여 계산될 수 있다. 각각의 노드와 연관된 가중치는 또한, 데이터의 전집(예를 들면, 데이터 또는 거동 벡터들의 클라우드 전집)의 얼마나 많은 단위들이 부스트 결정 그루터기들을 구축하는데 사용되는지에 기초하여 계산될 수 있다.

[0129] [0145] 도 9는 일 양상에 따라 동적 및 적응적 관측들을 수행하도록 구성된 컴퓨팅 시스템의 거동 관측기 모듈(202)에서의 예시적인 논리 컴포넌트들 및 정보 흐름들을 예시한다. 거동 관측기 모듈(202)은 적응형 필터 모듈(902), 스로틀 모듈(904), 관측기 모드 모듈(906), 하이-레벨 거동 검출 모듈(908), 거동 벡터 생성기(910), 및 보안 버퍼(912)를 포함할 수 있다. 하이-레벨 거동 검출 모듈(908)은 공간적 상관 모듈(914) 및 시간적 상관 모듈(916)을 포함할 수 있다.

[0130] [0146] 관측기 모드 모듈(906)은, 분석기 유닛(예를 들어, 도 2를 참조하여 전술한 거동 분석기 모듈(204)) 및/또는 애플리케이션 API를 포함할 수 있는 다양한 소스들로부터 제어 정보를 수신할 수 있다. 관측기 모드 모듈

(906)은 다양한 관측기 모드들에 관한 제어 정보를 적응형 필터 모듈(902) 및 하이-레벨 거동 검출 모듈(908)에 전송할 수 있다.

[0131] [0147] 적응형 필터 모듈(902)은 다수의 소스들로부터 데이터/정보를 수신하고, 수신된 정보를 지능적으로 필터링하여 수신된 정보로부터 선택된 정보의 더 작은 서브세트를 생성할 수 있다. 이 필터는, API를 통해 통신하는 상위-레벨 프로세스, 또는 분석기 모듈로부터 수신된 정보 또는 제어에 기초하여 적응될 수 있다. 필터링된 정보는 스로틀 모듈(904)에 전송될 수 있고, 이 스로틀 모듈은, 하이-레벨 거동 검출 모듈(908)이 요청들 또는 정보로 넘치거나 과부하되지 않도록 보장하기 위해 필터로부터 흐르는 정보의 양을 제어하는 것을 담당할 수 있다.

[0132] [0148] 하이-레벨 거동 검출 모듈(908)은, 스로틀 모듈(904)로부터의 데이터/정보, 관측기 모드 모듈(906)로부터의 제어 정보, 및 모바일 디바이스의 다른 컴포넌트들로부터의 컨텍스트 정보를 수신할 수 있다. 하이-레벨 거동 검출 모듈(908)은, 디바이스로 하여금 차선의 레벨들에서 수행하게 할 수 있는 하이 레벨 거동들을 검출 또는 식별하기 위해 공간적 및 시간적 상관들을 수행하기 위해 수신된 정보를 이용할 수 있다. 공간적 및 시간적 상관들의 결과들은 거동 벡터 생성기(910)에 전송될 수 있고, 이 거동 벡터 생성기는, 상관 정보를 수신하고, 특정 프로세스, 애플리케이션, 또는 서브-시스템의 거동들을 기술하는 거동 벡터를 생성할 수 있다. 일 양상에서, 거동 벡터 생성기(910)는, 특정 프로세스, 애플리케이션, 또는 서브-시스템의 각각의 하이-레벨 거동이 거동 벡터의 요소이도록 하는 거동 벡터를 생성할 수 있다. 일 양상에서, 생성된 거동 벡터는 보안 버퍼(912)에 저장될 수 있다. 하이-레벨 거동 검출의 예들은, 특정 이벤트의 존재, 다른 이벤트의 양 또는 빈도, 다수의 이벤트들 사이의 관계, 이벤트들이 발생하는 순서, 어떤 이벤트들의 발생 사이의 시간 차이들 등의 검출을 포함할 수 있다.

[0133] [0149] 다양한 양상들에서, 거동 관측기 모듈(202)은 적응적 관측들을 수행하고 관측 입도를 제어할 수 있다. 즉, 거동 관측기 모듈(202)은 관측될 관련 거동들을 동적으로 식별하고, 식별된 거동들이 관측되어야 하는 세부 레벨을 동적으로 결정할 수 있다. 이러한 방식으로, 거동 관측기 모듈(202)은 시스템이 다양한 레벨들(예를 들어, 다수의 코스 및 미세 레벨들)에서 모바일 디바이스의 거동들을 모니터링하는 것을 가능하게 한다. 거동 관측기 모듈(202)은 시스템이 관측되고 있는 것에 적응하는 것을 가능하게 할 수 있다. 거동 관측기 모듈(202)은 시스템이, 매우 다양한 소스들로부터 획득될 수 있는 정보의 포커싱된 서브세트에 기초하여 관측되고 있는 요인들/거동들을 동적으로 변화하게 하는 것을 가능하게 할 수 있다.

[0134] [0150] 앞서 논의된 바와 같이, 거동 관측기 모듈(202)은 적응적 관측 기법들을 수행하고, 다양한 소스들로부터 수신된 정보에 기초하여 관측 입도를 제어할 수 있다. 예를 들어, 하이-레벨 거동 검출 모듈(908)은 스로틀 모듈(904), 관측기 모드 모듈(906)로부터의 정보, 및 모바일 디바이스의 다른 컴포넌트들(예를 들어, 센서들)로부터 수신된 컨텍스트 정보를 수신할 수 있다. 일 예로서, 시간적 상관들을 수행하는 하이-레벨 거동 검출 모듈(908)은, 카메라가 사용되었고 모바일 디바이스가 화상을 서버에 업로드하기를 시도하고 있다는 것을 검출할 수 있다. 하이-레벨 거동 검출 모듈(908)은 또한, 모바일 디바이스가 홀스터에 넣어져서 사용자의 벨트에 부착되어 있는 동안 모바일 디바이스 상의 애플리케이션이 사진을 촬영하였는지 여부를 결정하기 위해 공간적 상관들을 수행할 수 있다. 하이-레벨 거동 검출 모듈(908)은, 이 검출된 하이-레벨 거동(예를 들어, 홀스터에 넣어져 있는 동안의 카메라의 사용)이 수용가능한 또는 통상적인 거동인지 여부를 결정할 수 있고, 이는 모바일 디바이스의 과거 거동과 현재 거동을 비교하고 및/또는 복수의 디바이스들로부터 수집된 정보(예를 들면, 크라우드-소싱(crowd-sourcing) 서버로부터 수신된 정보)를 액세싱함으로써 달성될 수 있다. 홀스터에 넣어져 있는 동안 화상들을 촬영하는 것 및 그것들을 서버에 업로드하는 것이(홀스터에 넣어져 있는 상황에서 관측된 정규 거동들로부터 결정될 수 있는 바와 같이) 통상적이지 않은 거동이기 때문에, 이러한 상황에서, 하이-레벨 거동 검출 모듈(908)은 이것을 잠재적으로 위협적인 거동으로서 인식하고, 적절한 반응(예를 들어, 카메라를 끄는 것, 경고음을 내는 것 등)을 개시할 수 있다.

[0135] [0151] 일 양상에서, 거동 관측기 모듈(202)은 다수의 부분들에서 구현될 수 있다.

[0136] [0152] 도 10은, 일 양상의 관측기 데몬(daemon)을 구현하는 컴퓨팅 시스템(1000)에서의 논리적 컴포넌트들 및 정보 흐름들을 더 상세히 예시한다. 도 10에 예시된 예에서, 컴퓨팅 시스템(1000)은 사용자 공간에서 거동 검출기(1002) 모듈, 데이터베이스 엔진(1004) 모듈, 및 거동 분석기 모듈(204), 그리고 커널 공간에서 링 버퍼(1014), 필터 규칙(1016) 모듈, 스로틀링 규칙(1018) 모듈, 및 보안 버퍼(1020)를 포함한다. 컴퓨팅 디바이스(1000)는 사용자 공간에서 거동 검출기(1002) 및 데이터베이스 엔진(1004), 및 커널 공간에서 보안 버퍼 관리기(1006), 규칙 관리기(1008), 및 시스템 건강(health) 모니터(1010)를 포함하는 관측기 데몬을 추가로 포함할 수

있다.

[0137] [0153] 다양한 양상들은, 시스템 거동을 특징화하기 위해 웹키트(webkit), SDK, NDK, 커널, 드라이버들, 및 하드웨어를 포함하는 모바일 디바이스들 상의 크로스-레이어 관측들을 제공할 수 있다. 거동 관측들은 실시간으로 이루어질 수 있다.

[0138] [0154] 관측기 모듈은 적응적 관측 기술들을 수행하고, 관측 입도를 제어할 수 있다. 앞서 논의된 바와 같이, 모바일 디바이스의 열화에 기여할 수 있는 많은 수의(즉, 수천개의) 요인들이 존재하고, 디바이스의 성능의 열화에 기여할 수 있는 상이한 요인들 전부를 모니터링/관측하는 것은 실현가능하지 않을 수 있다. 이를 극복하기 위해, 다양한 양상들은, 관측될 관련 거동들을 동적으로 식별하고, 식별된 거동들이 관측될 세부 레벨을 동적으로 결정한다.

[0139] [0155] 도 11은 일 양상에 따라 동적 및 적응적 관측들을 수행하는 예시적인 방법(1100)을 나타낸다. 블록(1102)에서, 모바일 디바이스 프로세서는 모바일 디바이스의 열화에 기여할 수 있는 많은 수의 요인들/거동들의 서브세트를 모니터링/관측함으로써 코스 관측들을 수행할 수 있다. 블록(1103)에서, 모바일 디바이스 프로세서는 코스 관측들에 기초하여 코스 관측들 및/또는 모바일 디바이스 거동을 특징화하는 거동 벡터를 생성할 수 있다. 블록(1104)에서, 모바일 디바이스 프로세서는, 모바일 디바이스의 열화에 잠재적으로 기여할 수 있는 코스 관측들과 연관된 서브시스템들, 프로세스들 및/또는 애플리케이션들을 식별할 수 있다. 이는, 예를 들어, 다중 소스들로부터 수신된 정보와 모바일 디바이스의 센서들로부터 수신된 상황적 정보를 비교함으로써 달성될 수 있다. 블록(1106)에서, 모바일 디바이스 프로세서는 코스 관측들에 기초하여 거동 분석 동작들을 수행할 수 있다. 일 양상에서, 블록들(1103 및 1104)의 일부로서, 모바일 디바이스 프로세서는 도 2 내지 도 10을 참조하여 앞서 논의된 동작들 중 하나 이상을 수행할 수 있다.

[0140] [0156] 결정 블록(1108)에서, 모바일 디바이스 프로세서는, 의심스러운 거동들 또는 잠재적인 문제들이 거동 분석의 결과들에 기초하여 식별되고 정정될 수 있는지 여부를 결정할 수 있다. 모바일 디바이스 프로세서가, 의심스러운 거동들 또는 잠재적인 문제들이 거동 분석의 결과들에 기초하여 식별되고 정정될 수 있다고 결정하는 경우(즉, 결정 블록(1108) = "예"), 블록(1118)에서, 프로세서는 거동을 정정하기 위한 프로세스를 개시하고, 블록(1102)으로 돌아가 추가적인 코스 관측들을 수행할 수 있다.

[0141] [0157] 모바일 디바이스 프로세서가, 의심스러운 거동들 또는 잠재적인 문제들이 거동 분석의 결과들에 기초하여 식별 및/또는 정정될 수 없다고 결정하는 경우(즉, 결정 블록(1108) = "아니오"), 결정 블록(1109)에서, 모바일 디바이스 프로세서는 문제의 가능성이 존재하는지 여부를 결정할 수 있다. 일 양상에서, 모바일 디바이스 프로세서는, 모바일 디바이스가 잠재적인 문제들에 맞닥뜨리는 것 및/또는 의심스러운 거동들에 연루될 가능성을 계산하고, 그 계산된 가능성이 미리 결정된 임계치보다 큰지 여부를 결정함으로써, 문제의 가능성이 존재한다고 결정할 수 있다. 모바일 디바이스 프로세서가, 계산된 가능성이 미리 결정된 임계치보다 크지 않고, 및/또는, 의심스러운 거동들 또는 잠재적인 문제들이 존재 및/또는 검출가능할 가능성이 없다고 결정하는 경우(즉, 결정 블록(1109) = "아니오"), 프로세서는 추가적인 코스 관측들을 수행하기 위해 블록(1102)으로 복귀할 수 있다.

[0142] [0158] 모바일 디바이스 프로세서가, 의심스러운 거동들 또는 잠재적인 문제들이 존재 및/또는 검출가능할 가능성이 있다고 결정하는 경우(즉, 결정 블록(1109)= "예"), 블록(1110)에서, 모바일 디바이스 프로세서는 식별된 서브시스템들, 프로세스들 또는 애플리케이션들에 대해 더 깊은 로깅(logging)/관측들 또는 최종 로깅을 수행할 수 있다. 블록(1112)에서, 모바일 디바이스 프로세서는 식별된 서브시스템들, 프로세스들 또는 애플리케이션들에 대해 더 깊고 더 상세한 관측들을 수행할 수 있다. 블록(1114)에서, 모바일 디바이스 프로세서는 더 깊고 더 상세한 관측들에 기초하여 추가의 및/또는 더 깊은 거동 분석을 수행할 수 있다. 결정 블록(1108)에서, 모바일 디바이스 프로세서는, 의심스러운 거동들 또는 잠재적인 문제들이 더 깊은 거동 분석의 결과들에 기초하여 식별되고 정정될 수 있는지 여부를 다시 결정할 수 있다. 모바일 디바이스 프로세서가, 의심스러운 거동들 또는 잠재적인 문제들이 더 깊은 거동 분석의 결과들에 기초하여 식별 및 정정될 수 없다고 결정하는 경우(즉, 결정 블록(1108) = "아니오"), 프로세서는, 세부 레벨이 문제를 식별하기에 충분하게 미세하게 될 때까지 또는 문제들이 추가적인 세부사항으로 식별될 수 없다거나 아무런 문제도 존재하지 않는다고 결정될 때까지, 블록들(1110-1114)의 동작들을 반복할 수 있다.

[0143] [0159] 모바일 디바이스 프로세서가, 의심스러운 거동들 또는 잠재적인 문제들이 더 깊은 거동 분석의 결과들에 기초하여 식별 및 정정될 수 있다고 결정하는 경우(즉, 결정 블록(1108) = "예"), 블록(1118)에서, 모바일 디바이스 프로세서는 문제/거동을 정정하기 위한 동작들을 수행할 수 있고, 프로세서는 추가적인 동작들을 수행하기

위해 블록(1102)으로 복귀할 수 있다.

[0144] [0160] 일 양상에서, 방법(1100)의 블록들(1102-1118)의 일부로서, 모바일 디바이스 프로세서는 제한된 및 코스 관측들로부터 의심스러운 거동을 식별하기 위해, 더 상세하게 관측할 거동들을 동적으로 결정하기 위해, 및 관측들에 필요한 정확한 세부 레벨을 동적으로 결정하기 위해, 시스템의 거동들의 실시간 거동 분석을 수행할 수 있다. 이는 모바일 디바이스 프로세서가, 디바이스 상의 대량의 프로세서, 메모리, 또는 배터리 자원을 사용할 필요 없이, 문제들을 효율적으로 식별 및 발생 방지하는 것을 가능하게 한다.

[0145] [0161] 다양한 양상들은 다양한 컴퓨팅 디바이스들 상에서 구현될 수 있고, 그 일 예가 스마트폰의 형태로 도 12에서 예시된다. 스마트폰(1200)은 내부 메모리(1204), 디스플레이(1212), 그리고 스피커(1214)에 연결된 프로세서(1202)를 포함할 수 있다. 추가적으로, 스마트폰(1200)은 프로세서(1202)에 연결된 무선 데이터 링크 및/또는 셀룰러 전화 트랜시버(1208)에 접속될 수 있는, 전자기적 방사를 전송 및 수신하는 안테나를 포함할 수 있다. 스마트폰들(1200)은 통상적으로 사용자 입력들을 수신하기 위한 메뉴 선택 버튼들 또는 로커(rocker) 스위치들(1220)을 또한 포함한다.

[0146] [0100] 통상적인 스마트폰(1200)은 또한, 마이크로폰으로부터 수신된 사운드를 무선 송신에 적합한 데이터 패킷들로 디지털화하고, 사운드를 생성하기 위해 스피커에 제공되는 아날로그 신호들을 생성하기 위해 수신된 사운드 데이터 패킷들을 디코딩하는 사운드 인코딩/디코딩(CODEC) 회로(1206)를 포함한다. 또한, 프로세서(1202), 무선 트랜시버(1208) 및 CODEC(1206) 중 하나 이상은 디지털 신호 프로세서(DSP) 회로를 포함할 수 있다(개별적으로 도시되지 않음).

[0147] [0162] 양상 방법들의 부분들은, 그 양상 방법들을 실행하는 동안 모바일 디바이스 프로세서에 의해 액세스될 수 있는, 정규 동작 거동들의 데이터베이스들을 유지하는 것과 같은, 서버에서 일어나는 프로세싱의 일부로 클라이언트-서버 아키텍처에서 달성될 수 있다. 이러한 양상들은 도 13에서 도시된 서버(1300)와 같은 다양한 상업적으로 이용가능한 서버 디바이스들 중 임의의 것 상에서 구현될 수 있다. 이러한 서버(1300)는 통상적으로, 휘발성 메모리(1302), 및 디스크 드라이브(1303)와 같은 대용량의 비휘발성 메모리에 연결된 프로세서(1301)를 포함한다. 서버(1300)는 또한, 프로세서(1301)에 연결된 플로피 디스크 드라이브, 컴팩트 디스크(CD) 또는 DVD 디스크 드라이브(1304)를 포함할 수 있다. 서버(1300)는 또한, 다른 브로드캐스트 시스템 컴퓨터들 및 서버들에 연결된 로컬 영역 네트워크와 같은 네트워크(1305)와 데이터 접속들을 확립하기 위한, 프로세서(1301)에 연결된 네트워크 액세스 포트들(1306)을 포함할 수 있다.

[0148] [0163] 프로세서들(1202, 1301)은, 이하 설명되는 다양한 양상들의 기능들을 포함하는 다양한 기능들을 수행하도록 소프트웨어 명령들(애플리케이션들)에 의해 구성될 수 있는 임의의 프로그래머블 마이크로프로세서, 마이크로컴퓨터 또는 다중 프로세서 칩 또는 칩들일 수 있다. 일부 모바일 디바이스들에서, 무선 통신 기능들에 전용되는 하나의 프로세서 및 다른 애플리케이션들을 실행되도록 전용되는 하나의 프로세서와 같이 다중 프로세서들(1202)이 제공될 수 있다. 통상적으로, 소프트웨어 애플리케이션들은, 그들이 액세스되고 프로세서(1202, 1301) 내로 로딩되기 전에 내부 메모리(1204, 1302, 1303)에 저장될 수 있다. 프로세서(1202, 1301)는 애플리케이션 소프트웨어 명령들을 저장하기에 충분한 내부 메모리를 포함할 수 있다.

[0149] [0164] "성능 열화(performance degradation)"라는 용어는, 더 긴 프로세싱 시간들, 더 느린 실시간 응답, 더 낮은 배터리 수명, 개인 데이터의 손실, 악성 경제적 활동(예를 들어, 허가되지 않은 프리미엄 SMS 메시지를 전송하는 것), 서비스 거부(DoS), 스파이 또는 봇네트(botnet) 활동들 등을 위해 모바일 디바이스를 징발(commandeering)하는 것 또는 전화기를 이용하는 것에 관련된 동작들과 같은 아주 다양한 바람직하지 않은 모바일 디바이스 동작들 및 특성들을 지칭하기 위해 본 출원에서 사용된다.

[0150] [0165] 다양한 양상들의 동작들을 수행하기 위해 프로그래머블 프로세서 상에서 실행하기 위한 컴퓨터 프로그램 코드 또는 "프로그램 코드"는 C, C++, C#, Smalltalk, Java, JavaScript, Visual Basic, 구조화된 쿼리 언어(예를 들어, Transact-SQL), Perl과 같은 하이 레벨 프로그래밍 언어에서, 또는 다양한 다른 프로그래밍 언어들로 기록될 수 있다. 본 출원에 사용된 바와 같이, 컴퓨터 판독가능 저장 매체 상에 저장된 프로그램 코드 또는 프로그램들은, 포맷이 프로세서에 의해 이해 가능한 (오브젝트 코드와 같은) 기계 언어 코드를 지칭할 수 있다.

[0151] [0166] 많은 모바일 컴퓨팅 디바이스들 운영 시스템 커널들은 (비특권(non-privileged) 코드가 실행되는) 사용자 공간 및 (특권(privileged) 코드가 실행되는) 커널 공간으로 조직화된다. 이러한 분리는, 커널 공간의 일부인 코드는 GPL 허가되어야 하는 한편, 사용자-공간에서 실행되는 코드는 GPL 허가되지 않을 수 있는 Android®

및 다른 GPL(general public license) 환경들에서 특히 중요하다. 본원에서 논의된 다양한 소프트웨어 컴포넌트들/모듈들은, 다르게 명시적으로 진술되지 않는 한, 커널 공간 또는 사용자 공간 중 어느 하나에서 구현될 수 있다는 것을 이해하여야 한다.

[0152] [0167] 상기 방법 설명들 및 프로세스 흐름도들은 단지 예시적인 예들로서 제공되고, 다양한 양상들의 단계들이 제시된 순서로 수행되어야 함을 요구하거나 의미하도록 의도되지 않는다. 당업자에 의해 인식될 바와 같이, 상기 양상들의 단계들의 순서는 임의의 순서로 수행될 수 있다. "그 후", "그 다음", "다음" 등과 같은 단어들은 단계들의 순서를 제한하도록 의도되지 않고; 이 단어들은 단순히, 방법들의 설명에 걸쳐 독자를 안내하기 위해 사용된다. 추가로, 예를 들어, 관사들("a", "an" 또는 "the")을 이용한 단수인 청구항 엘리먼트들에 대한 임의의 참조는 그 엘리먼트를 단수로 제한하는 것으로 해석되어서는 안된다.

[0153] [0168] 본 출원에 사용된 바와 같이, 용어들 "컴포넌트", "모듈", "시스템", "엔진", "생성기", "관리기" 등은, 이에 제한되지 않지만, 하드웨어, 펌웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어, 또는 실행중인 소프트웨어와 같은 컴퓨터-관련 엔티티를 포함하도록 의도되고, 이들은 특정 동작들 또는 기능들을 수행하도록 구성된다. 예를 들면, 컴포넌트는, 이에 제한되지 않지만, 프로세서 상에서 실행되는 프로세스, 프로세서, 오브젝트, 실행 가능한 것, 실행 스레드, 프로그램 및/또는 컴퓨터일 수 있다. 예시로서, 컴퓨팅 디바이스 상에서 실행되는 애플리케이션 및 컴퓨팅 디바이스 둘 모두는 컴포넌트로 지칭될 수 있다. 하나 이상의 컴포넌트들은 프로세스 및/또는 실행 스레드 내에 상주할 수 있고, 컴포넌트는 하나의 프로세서 또는 코어 상에서 로컬화되고 및/또는 2 개 이상의 프로세서들 또는 코어들 사이에서 분배될 수 있다. 또한, 이러한 컴포넌트들은 다양한 명령들 및/또는 데이터 구조들이 저장된 다양한 비일시적인 컴퓨터 판독 가능 매체들로부터 실행될 수 있다. 컴포넌트들은 로컬 및/또는 원격 프로세스들, 기능 또는 절차 호들, 전자 신호들, 데이터 패킷들, 메모리 판독/기록들 및 다른 알려진 네트워크, 컴퓨터, 프로세서 및/또는 통신 방법들에 관련된 프로세스에 의해 통신할 수 있다.

[0154] [0169] 본 명세서에 개시된 양상들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들 및 알고리즘 단계들은 전자 하드웨어, 컴퓨터 소프트웨어 또는 둘 모두의 조합들로 구현될 수 있다. 하드웨어 및 소프트웨어의 이러한 상호 교환가능성을 명확히 예시하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 일반적으로 그들의 기능적 관점에서 앞서 설명되었다. 이러한 기능이 하드웨어로 구현되는지 또는 소프트웨어로 구현되는지 여부는 특정 애플리케이션, 및 전체 시스템에 대해 부과된 설계 제한들에 의존한다. 당업자들은 설명된 기능을 각각의 특정 애플리케이션에 대해 다양한 방식들로 구현할 수 있지만, 이러한 구현 결정들이 본 발명의 범위를 벗어나는 것을 야기하는 것으로 해석되어서는 안 된다.

[0155] [0170] 본 명세서에서 개시되는 양상들과 관련하여 설명된 다양한 예시적인 논리들, 논리 블록들, 모듈들 및 회로들을 구현하는데 이용되는 하드웨어는 범용 프로세서, 디지털 신호 프로세서(DSP), 주문형 집적 회로(ASIC), 필드 프로그래머블 게이트 어레이(FPGA) 또는 다른 프로그래머블 논리 디바이스, 이산 게이트 또는 트랜지스터 논리, 이산 하드웨어 컴포넌트들, 또는 본 명세서에서 설명된 기능들을 수행하도록 설계된 이들의 임의의 조합에 의해 구현 또는 수행될 수 있다. 범용 프로세서는 멀티프로세서일 수 있지만, 대안적으로, 프로세서는 임의의 종래의 프로세서, 제어기, 마이크로제어기 또는 상태 머신일 수 있다. 또한, 프로세서는 컴퓨팅 디바이스들의 조합, 예를 들어, DSP 및 멀티프로세서의 조합, 복수의 멀티프로세서들, DSP 코어와 결합된 하나 이상의 멀티프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수 있다. 대안적으로, 몇몇 단계들 또는 방법들은, 주어진 기능에 특정된 회로에 의해 수행될 수 있다.

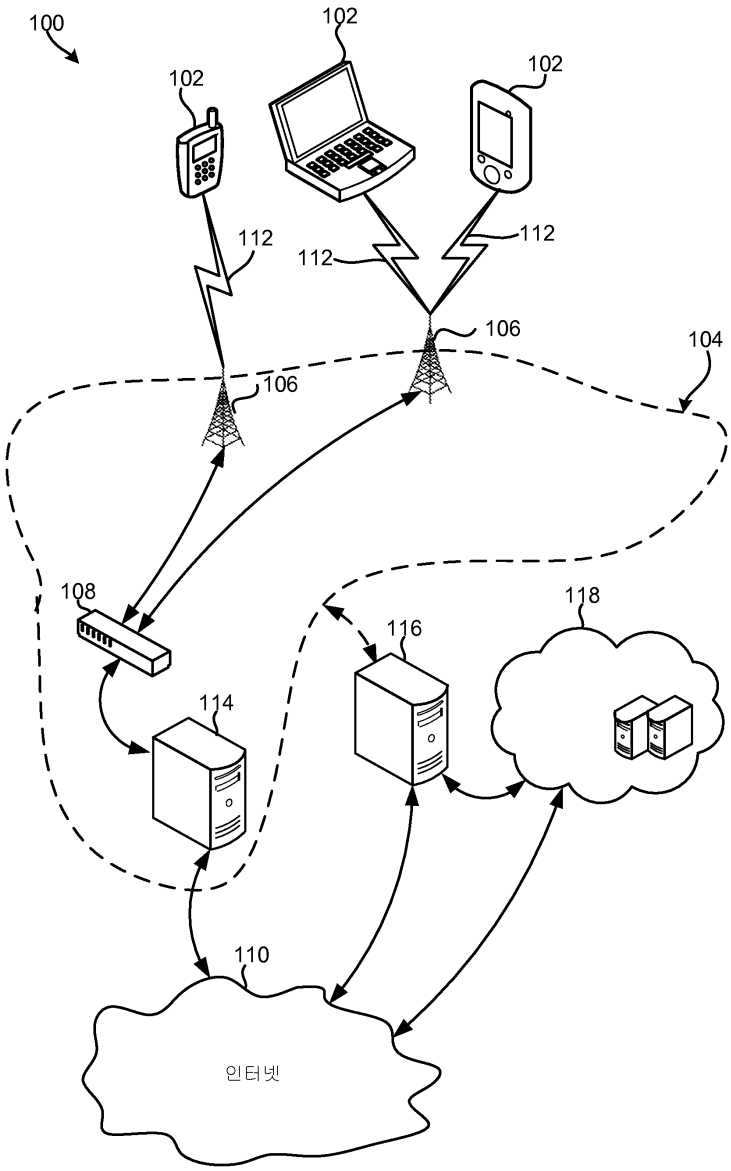
[0156] [0171] 하나 이상의 예시적인 양상들에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어 또는 이들의 임의의 조합으로 구현될 수 있다. 소프트웨어로 구현되면, 상기 기능들은 비일시적 컴퓨터 판독 가능 저장 매체 또는 비일시적인 프로세서 판독 가능 저장 매체 상에 하나 이상의 프로세서 실행가능 명령들 또는 코드로서 저장될 수 있다. 본 명세서에 개시된 알고리즘 또는 방법의 단계들은, 비일시적 컴퓨터 판독 가능 또는 프로세서 판독 가능 저장 매체 상에 상주할 수 있는 프로세서 실행가능 소프트웨어 모듈에서 구현될 수 있다. 비일시적 컴퓨터 판독 가능 또는 프로세서 판독 가능 저장 매체들은 컴퓨터 또는 프로세서에 의해 액세스될 수 있는 임의의 저장 매체들일 수 있다. 비제한적인 예로서, 그러한 비일시적 컴퓨터 판독 가능 또는 프로세서 판독 가능 저장 매체들은 RAM, ROM, EEPROM, 플래시 메모리, CD-ROM 또는 다른 광학 디스크 저장소, 자기 디스크 저장소 또는 다른 자기 저장 디바이스들 또는 명령들 또는 데이터 구조들의 형태로 요구되는 프로그램 코드를 저장하는데 이용될 수 있고, 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 본 명세서에서 사용되는 디스크(disk) 및 디스크(disc)는 컴팩트 디스크(disc)(CD), 레이저 디스크(disc), 광 디스크(disc), 디지털 다기능 디스크(DVD), 플로피 디스크(disk), 및 블루-레이 디스크(disc)를 포함하며, 여기서 디스크(disk)들은 보

통 데이터를 자기적으로 재생하지만, 디스크(disc)들은 레이저들로 데이터를 광학적으로 재생한다. 상기한 것의 조합들은 또한 비일시적 컴퓨터 판독 가능 및 프로세서 판독 가능 매체들의 범위 내에 포함된다. 추가적으로, 방법 또는 알고리즘의 동작들은, 컴퓨터 프로그램 물건에 통합될 수 있는 비일시적 프로세서 판독 가능 매체 및/또는 컴퓨터-판독 가능 매체 상에 코드들 및/또는 명령들 중 하나 또는 임의의 조합 또는 세트로서 상주할 수 있다.

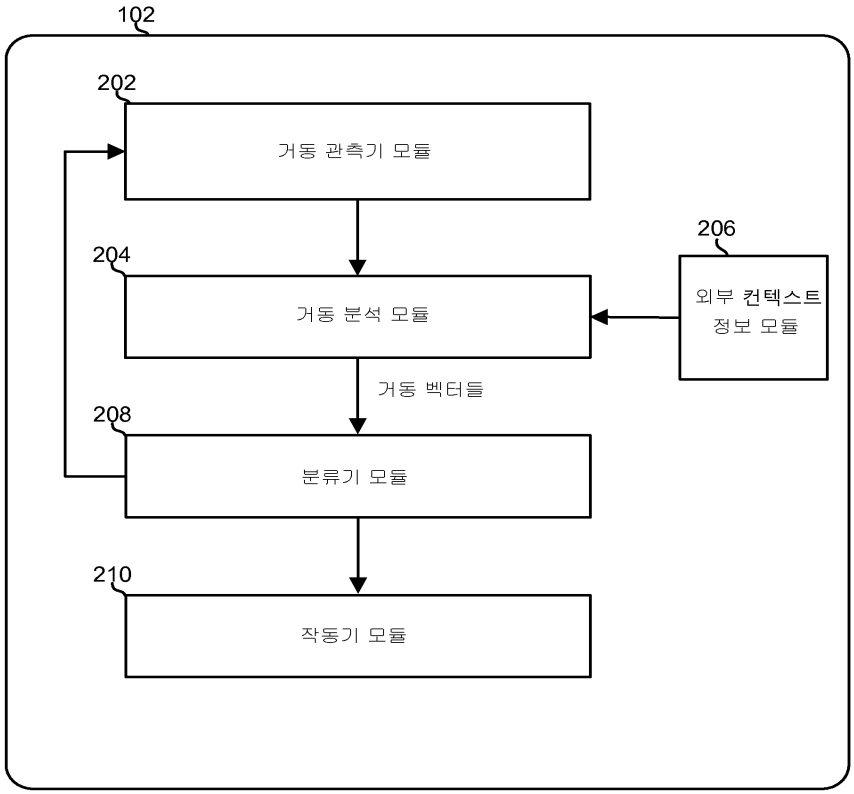
[0157] [0172] 개시된 양상들의 이전 설명은 임의의 당업자가 본 발명을 이용하거나 또는 실시할 수 있도록 제공된다. 이 양상들에 대한 다양한 변형들은 당업자들에게 쉽게 명백할 것이며, 본 명세서에 정의된 일반적인 원리들은 본 발명의 사상 또는 범위를 벗어남이 없이 다른 양상들에 적용될 수 있다. 따라서, 본 발명은 본 명세서에 제시된 양상들로 한정되는 것으로 의도되지 않고, 본 명세서에 개시된 하기 청구항들 및 원리들 및 신규한 특징들과 부합하는 가장 넓은 범위에 따라야 한다.

도면

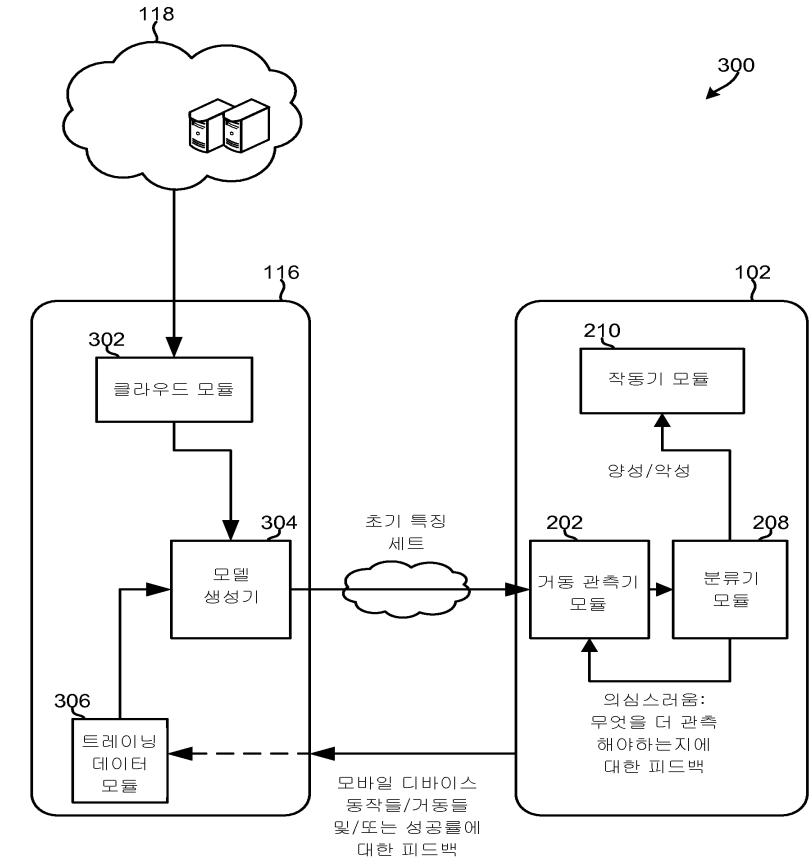
도면1



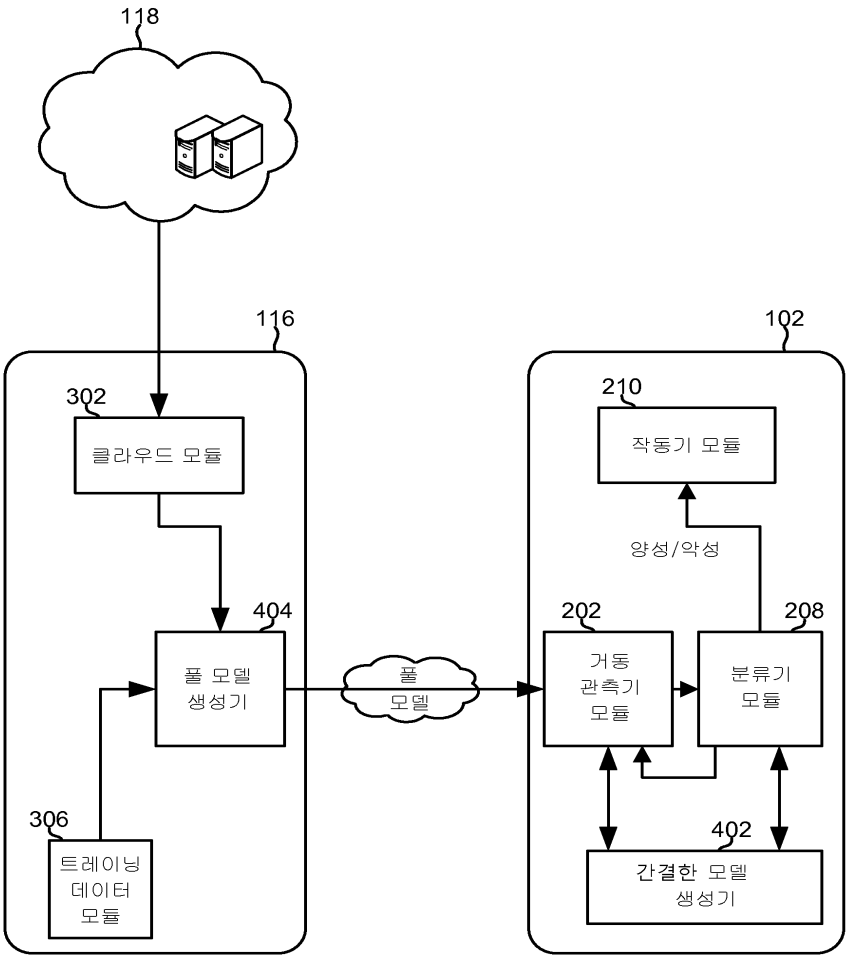
도면2


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

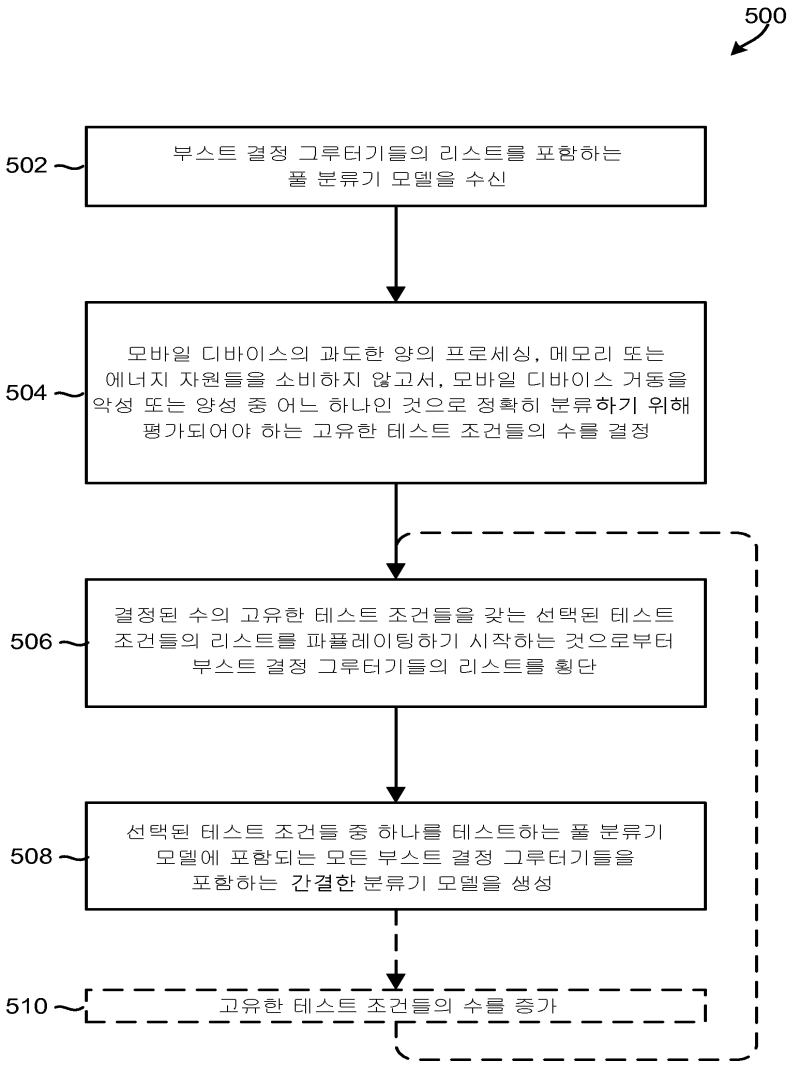
도면3


118
300
116
102
302
클라우드 모듈
210
작동기 모듈
양성/악성
304
초기 특징 세트
202
208
모델 생성기
거동 관측기 모듈
분류기 모듈
306
의심스러움: 무엇을 더 관측해야하는지에 대한 피드백
트레이닝 데이터 모듈
모바일 디바이스 동작들/거동들 및/또는 성공률에 대한 피드백

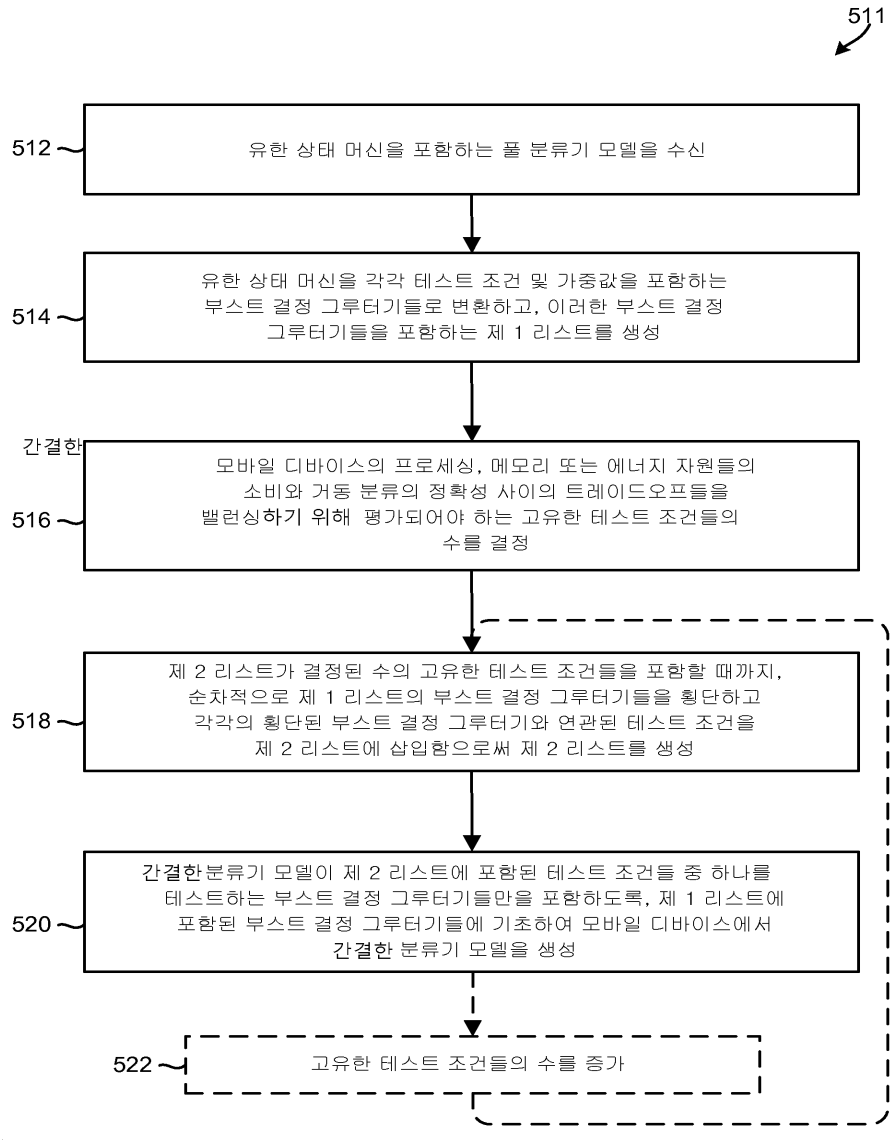
도면4


118
116
102
302
클라우드 모듈
210
작동기 모듈
양성/악성
404
202
208
풀 모델
생성기
풀
모델
거동
관측기
모듈
분류기
모듈
306
402
트레이닝
데이터
모듈
간결한 모델
생성기

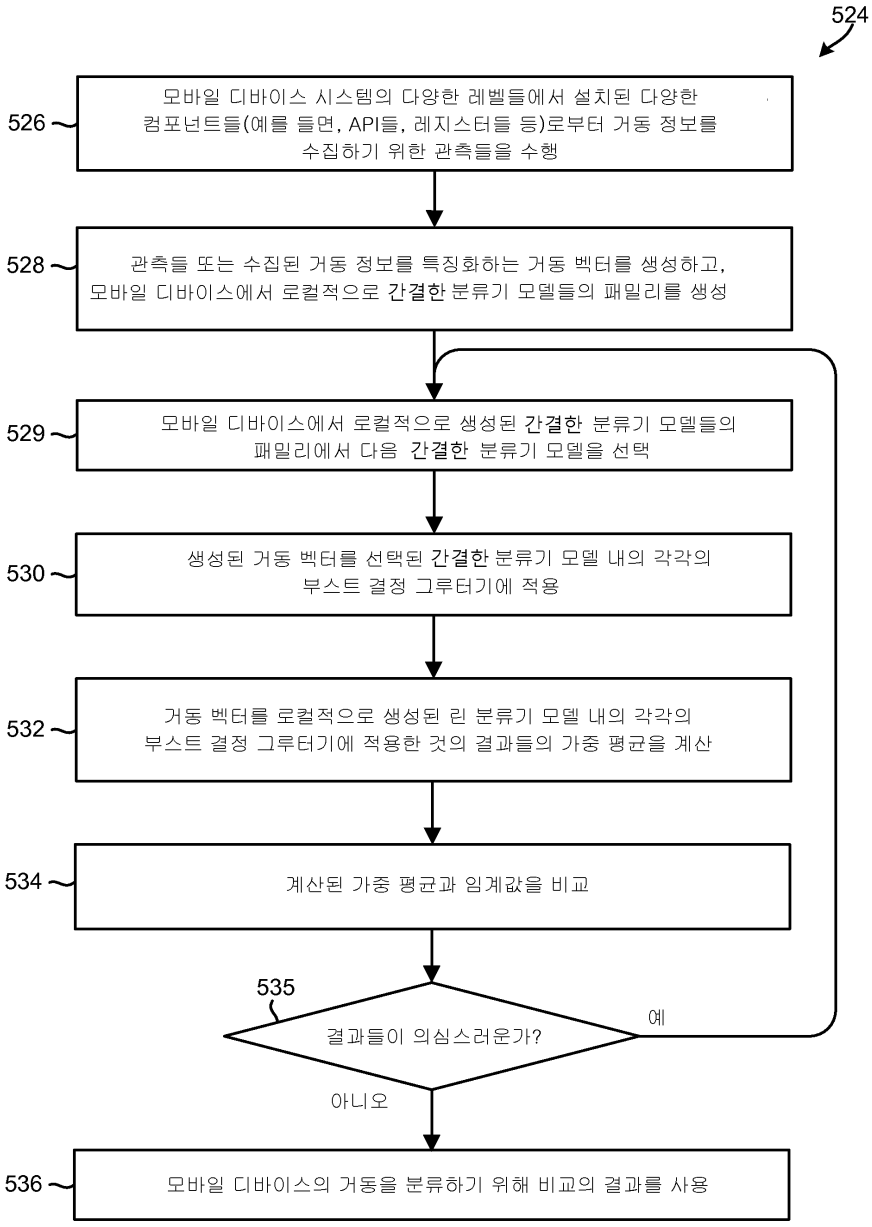
도면5a


500
502
부스트 결정 그루터기들의 리스트를 포함하는 풀 분류기 모델을 수신
504
모바일 디바이스의 과도한 양의 프로세싱, 메모리 또는 에너지 자원들을 소비하지 않고서, 모바일 디바이스 거동을 악성 또는 양성 중 어느 하나인 것으로 정확히 분류하기 위해 평가되어야 하는 고유한 테스트 조건들의 수를 결정
506
결정된 수의 고유한 테스트 조건들을 갖는 선택된 테스트 조건들의 리스트를 파퓰레이팅하기 시작하는 것으로부터 부스트 결정 그루터기들의 리스트를 횡단
508
선택된 테스트 조건들 중 하나를 테스트하는 풀 분류기 모델에 포함되는 모든 부스트 결정 그루터기들을 포함하는 간결한 분류기 모델을 생성
510
고유한 테스트 조건들의 수를 증가

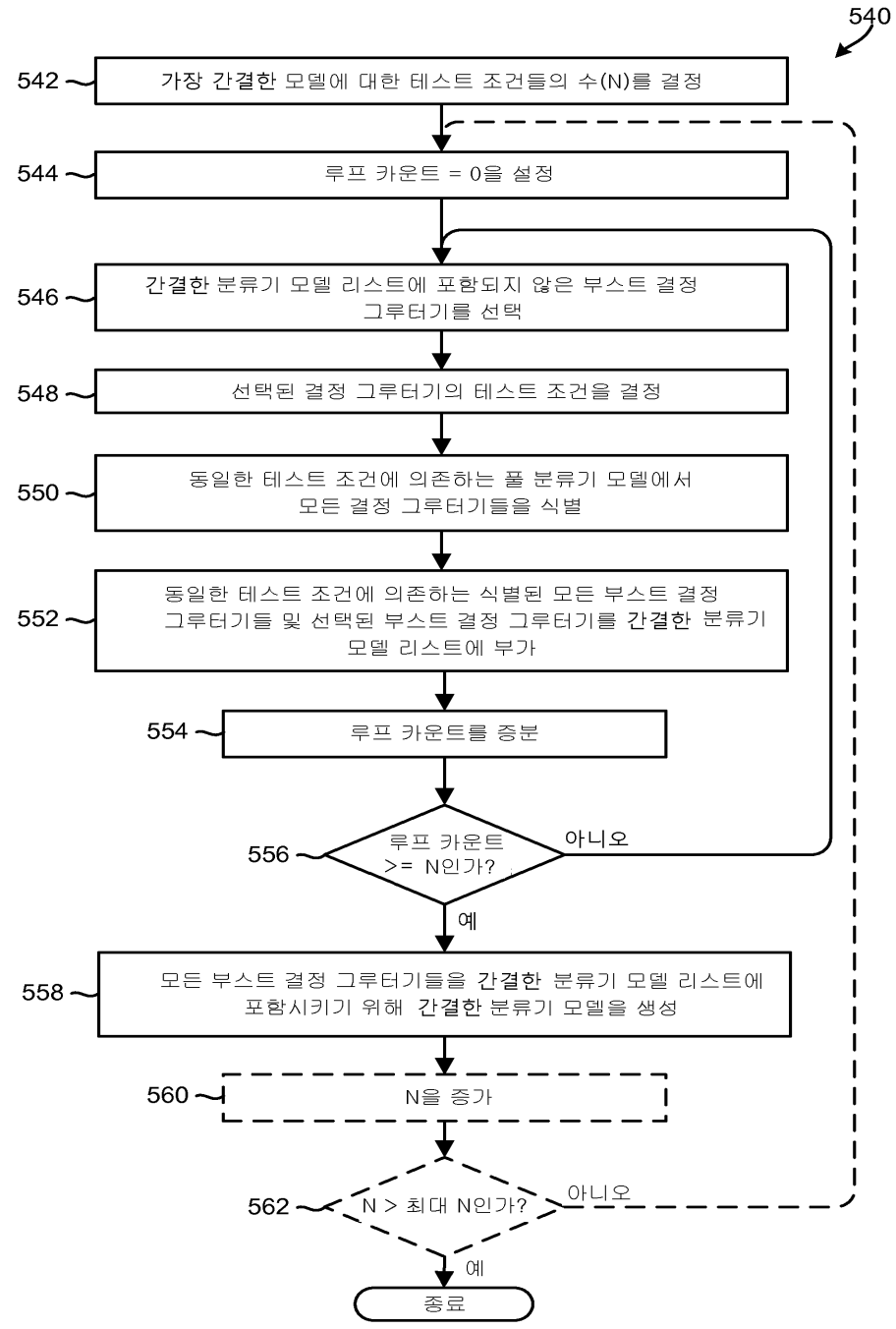
도면5b


511
512
유한 상태 머신을 포함하는 풀 분류기 모델을 수신
514
유한 상태 머신을 각각 테스트 조건 및 가중값을 포함하는 부스트 결정 그루터기들로 변환하고, 이러한 부스트 결정 그루터기들을 포함하는 제 1 리스트를 생성
간결한
516
모바일 디바이스의 프로세싱, 메모리 또는 에너지 자원들의 소비와 거동 분류의 정확성 사이의 트레이드오프들을 밸런싱하기 위해 평가되어야 하는 고유한 테스트 조건들의 수를 결정
518
제 2 리스트가 결정된 수의 고유한 테스트 조건들을 포함할 때까지, 순차적으로 제 1 리스트의 부스트 결정 그루터기들을 횡단하고 각각의 횡단된 부스트 결정 그루터기와 연관된 테스트 조건을 제 2 리스트에 삽입함으로써 제 2 리스트를 생성
520
간결한 분류기 모델이 제 2 리스트에 포함된 테스트 조건들 중 하나를 테스트하는 부스트 결정 그루터기들만을 포함하도록, 제 1 리스트에 포함된 부스트 결정 그루터기들에 기초하여 모바일 디바이스에서 간결한 분류기 모델을 생성
522
고유한 테스트 조건들의 수를 증가

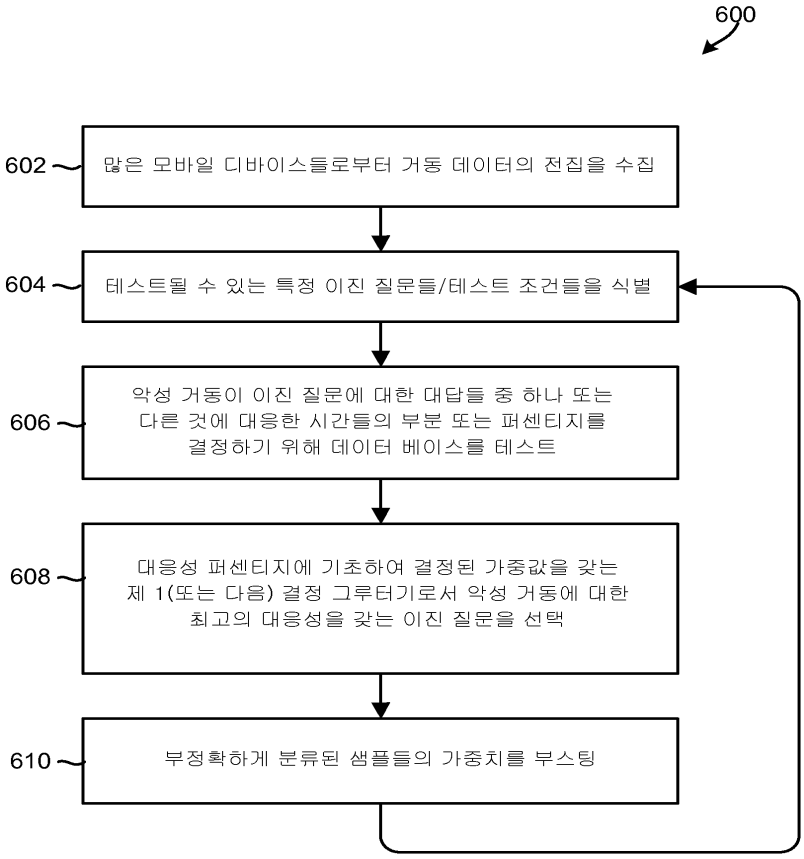
도면5c


524
526
모바일 디바이스 시스템의 다양한 레벨들에서 설치된 다양한 컴포넌트들(예를 들면, API들, 레지스터들 등)로부터 거동 정보를 수집하기 위한 관측들을 수행
528
관측들 또는 수집된 거동 정보를 특징화하는 거동 벡터를 생성하고, 모바일 디바이스에서 로컬적으로 간결한 분류기 모델들의 패밀리를 생성
529
모바일 디바이스에서 로컬적으로 생성된 간결한 분류기 모델들의 패밀리에서 다음 간결한 분류기 모델을 선택
530
생성된 거동 벡터를 선택된 간결한 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용
532
거동 벡터를 로컬적으로 생성된 린 분류기 모델 내의 각각의 부스트 결정 그루터기에 적용한 것의 결과들의 가중 평균을 계산
534
계산된 가중 평균과 임계값을 비교
535
결과들이 의심스러운가?
예
아니오
536
모바일 디바이스의 거동을 분류하기 위해 비교의 결과를 사용

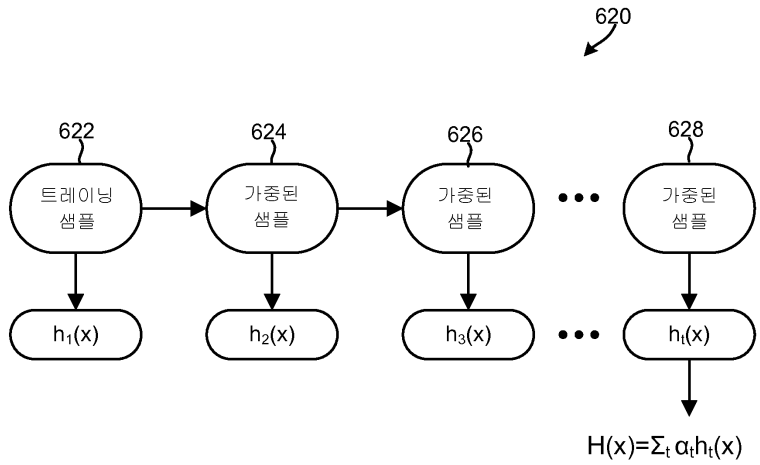
도면5d


540
542
가장 간결한 모델에 대한 테스트 조건들의 수(N)를 결정
544
루프 카운트 = 0을 설정
546
간결한 분류기 모델 리스트에 포함되지 않은 부스트 결정 그루터기를 선택
548
선택된 결정 그루터기의 테스트 조건을 결정
550
동일한 테스트 조건에 의존하는 풀 분류기 모델에서 모든 결정 그루터기들을 식별
552
동일한 테스트 조건에 의존하는 식별된 모든 부스트 결정 그루터기들 및 선택된 부스트 결정 그루터기를 간결한 분류기 모델 리스트에 부가
554
루프 카운트를 증분
556
루프 카운트 >= N인가?
아니오
예
558
모든 부스트 결정 그루터기들을 간결한 분류기 모델 리스트에 포함시키기 위해 간결한 분류기 모델을 생성
560
N을 증가
562
N > 최대 N인가?
아니오
예
종료

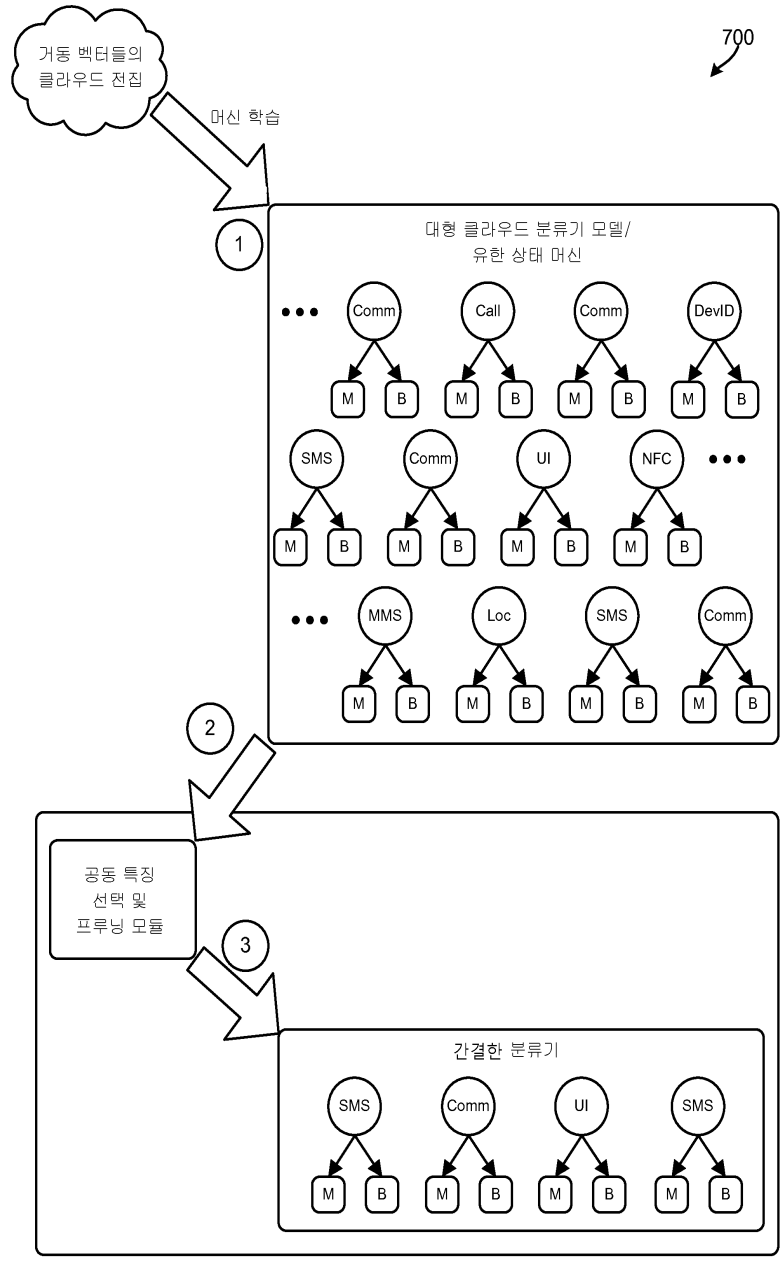
도면6a


600
602
많은 모바일 디바이스들로부터 거동 데이터의 전집을 수집
604
테스트될 수 있는 특정 이진 질문들/테스트 조건들을 식별
606
악성 거동이 이진 질문에 대한 대답들 중 하나 또는 다른 것에 대응한 시간들의 부분 또는 퍼센티지를 결정하기 위해 데이터 베이스를 테스트
608
대응성 퍼센티지에 기초하여 결정된 가중값을 갖는 제 1(또는 다음) 결정 그루터기로서 악성 거동에 대한 최고의 대응성을 갖는 이진 질문을 선택
610
부정확하게 분류된 샘플들의 가중치를 부스팅

도면6b

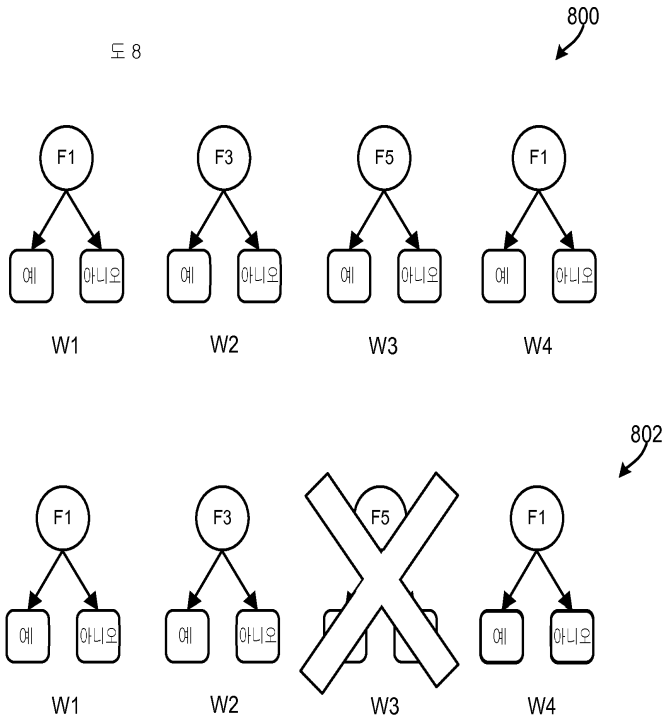

620
622
624
626
628
트레이닝 샘플
가중된 샘플
가중된 샘플
가중된 샘플
h1(x)
h2(x)
h3(x)
ht(x)
H(x)=Σt αtht(x)

도면7

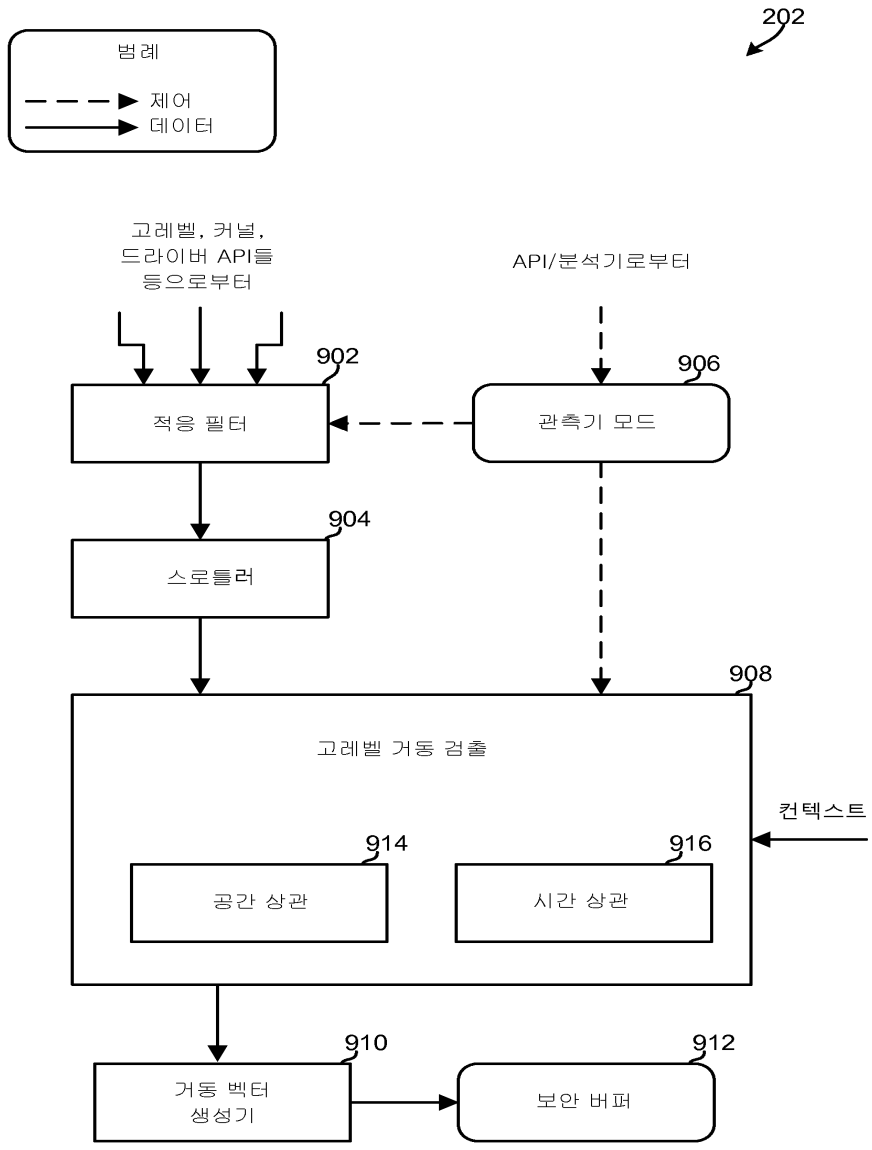

700
거동 벡터들의
클라우드 전집
머신 학습
1
대형 클라우드 분류기 모델/
유한 상태 머신
Comm
Call
Comm
DevID
SMS
Comm
UI
NFC
MMS
Loc
SMS
Comm
M
B
2
공동 특징
선택 및
프루닝 모듈
3
간결한 분류기
SMS
Comm
UI
SMS

도면8

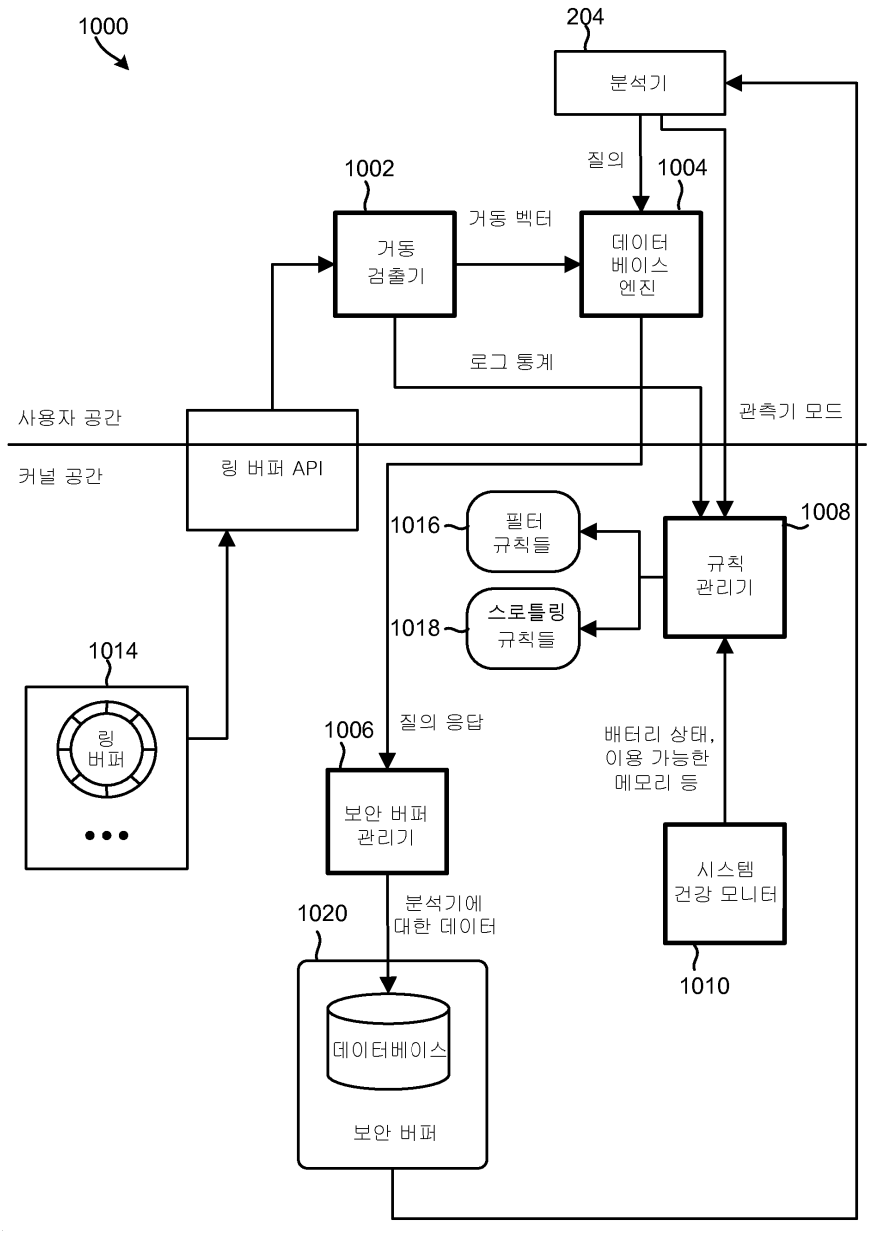
도 8


800
F1
F3
F5
F1
예
아니오
예
아니오
예
아니오
예
아니오
W1
W2
W3
W4
802
F1
F3
F5
F1
예
아니오
예
아니오
예
아니오
W1
W2
W3
W4

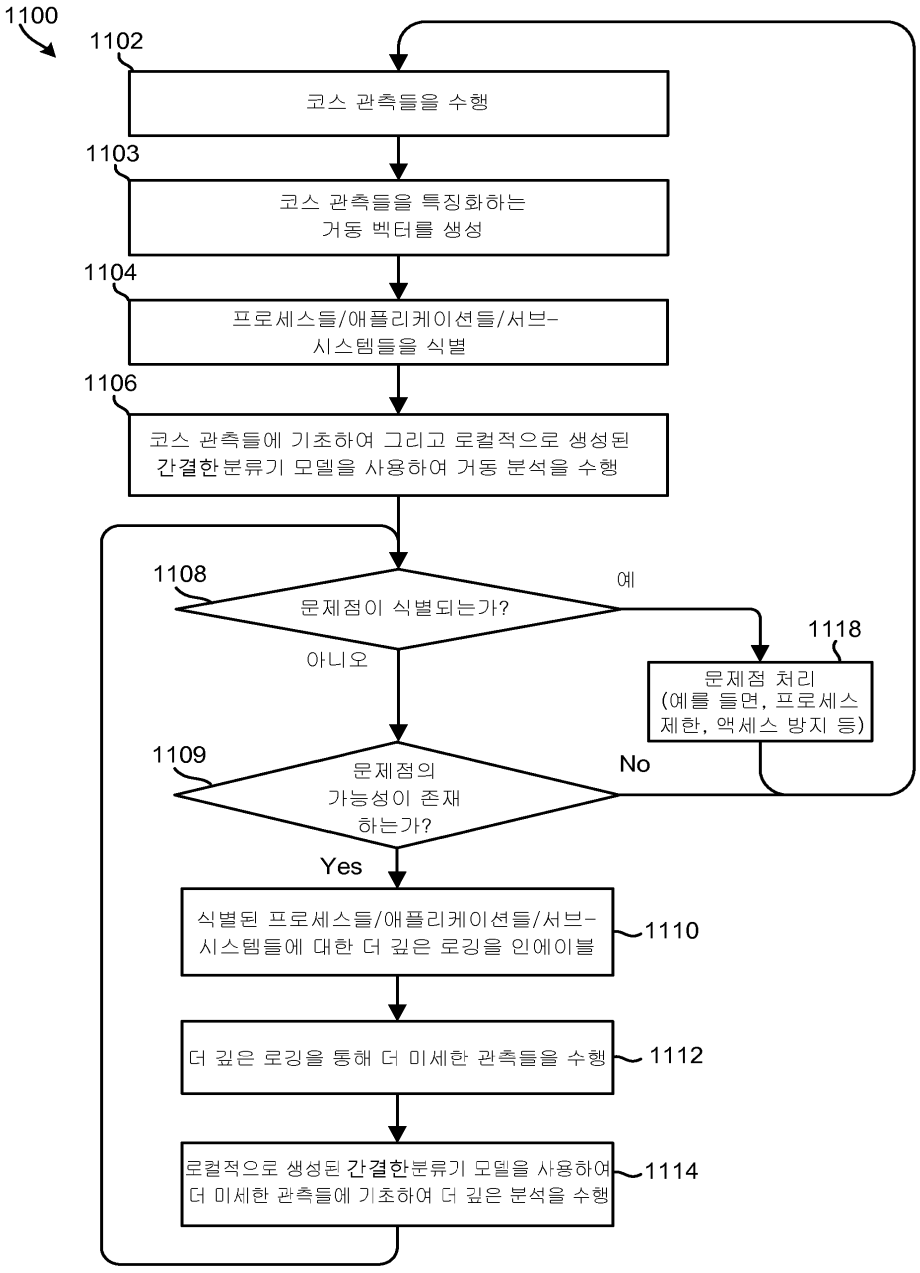
도면9


202
범례
제어
데이터
고레벨, 커널,
드라이버 API들
등으로부터
API/분석기로부터
902
906
적응 필터
관측기 모드
904
스로틀러
908
고레벨 거동 검출
컨텍스트
914
916
공간 상관
시간 상관
910
912
거동 벡터
생성기
보안 버퍼

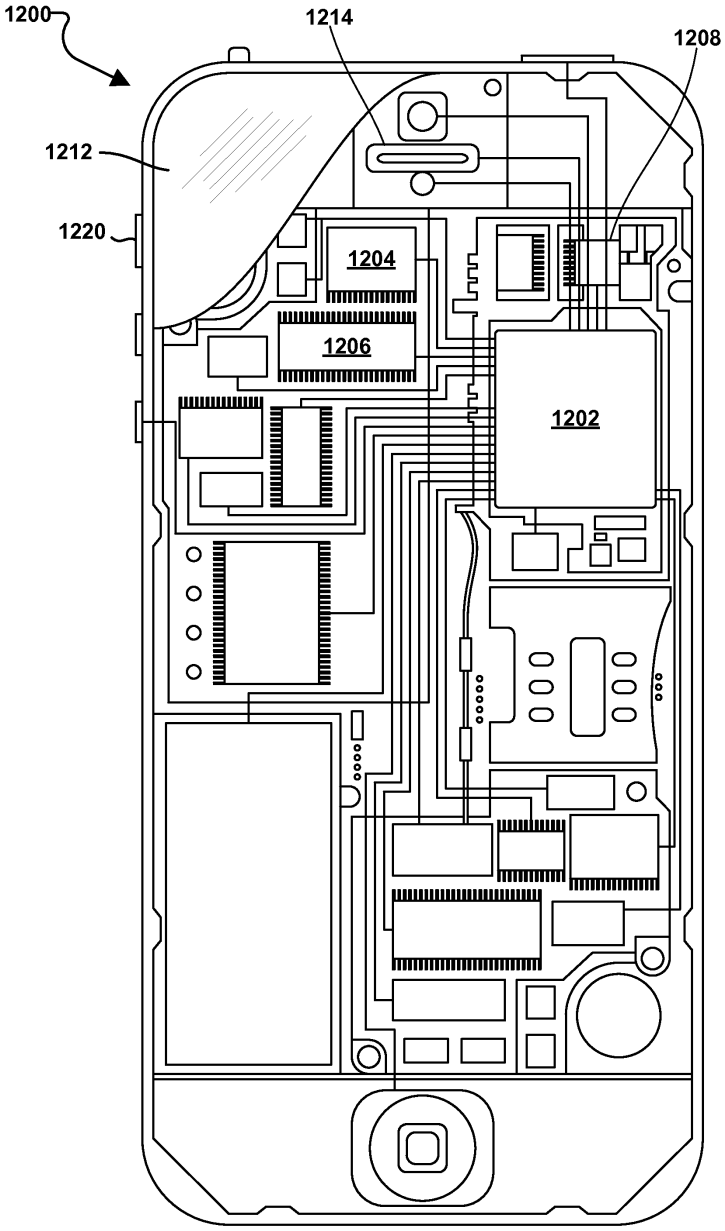
도면10


1000
204
분석기
질의
1004
1002
거동 벡터
거동
검출기
데이터
베이스
엔진
로그 통계
사용자 공간
관측기 모드
커널 공간
링 버퍼 API
1016
필터
규칙들
1008
규칙
관리기
1018
스로틀링
규칙들
1014
링
버퍼
1006
질의 응답
배터리 상태,
이용 가능한
메모리 등
보안 버퍼
관리기
시스템
건강 모니터
1020
분석기에
대한 데이터
1010
데이터베이스
보안 버퍼

도면11


1100
1102
코스 관측들을 수행
1103
코스 관측들을 특징화하는
거동 벡터를 생성
1104
프로세스들/애플리케이션들/서브-
시스템들을 식별
1106
코스 관측들에 기초하여 그리고 로컬적으로 생성된
간결한분류기 모델을 사용하여 거동 분석을 수행
1108
문제점이 식별되는가?
예
아니오
1118
문제점 처리
(예를 들면, 프로세스
제한, 액세스 방지 등)
1109
문제점의
가능성이 존재
하는가?
No
Yes
식별된 프로세스들/애플리케이션들/서브-
시스템들에 대한 더 깊은 로깅을 인에이블
1110
더 깊은 로깅을 통해 더 미세한 관측들을 수행
1112
로컬적으로 생성된 간결한분류기 모델을 사용하여
더 미세한 관측들에 기초하여 더 깊은 분석을 수행
1114

도면12



도면13