(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년04월07일
(11) 등록번호 10-1508577
(24) 등록일자 2015년03월30일

(51) 국제특허분류(Int. Cl.)
*G06F 21/56* (2013.01)
(21) 출원번호 10-2013-0120032
(22) 출원일자 2013년10월08일
심사청구일자 2013년10월08일
(56) 선행기술조사문헌
KR1020120070016 A
KR1020130076266 A
KR1020130071617 A

(73) 특허권자
**고려대학교 산학협력단**

(72) 발명자
**이희조**
**이제현**
**이수연**

(74) 대리인
**특허법인엠에이피에스**

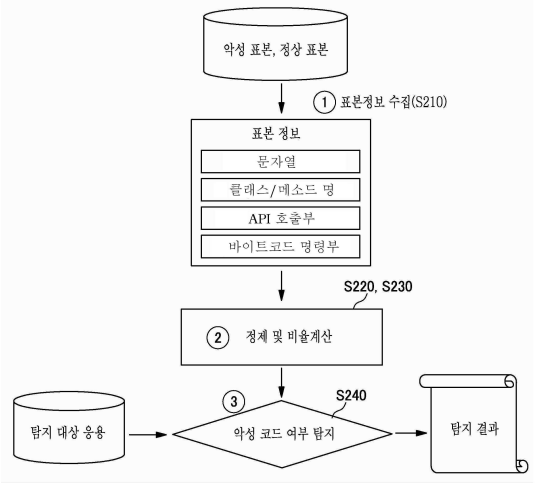
전체 청구항 수 : 총 10 항 심사관 : 구본재

(54) 발명의 명칭 **악성코드 탐지장치 및 방법**

## (57) 요 약

악성코드 탐지장치는, 기저장된 또는 입력된 악성표본 및 정상표본으로부터 표본정보를 수집하는 정보추출부, 하나 이상의 악성표본의 하나 이상의 표본정보 및 하나 이상의 정상표본의 하나 이상의 표본정보에 공통으로 존재하는 코드정보를 악성표본 및 정상표본에서 제거하여 악성표본 및 정상표본의 고유정보를 생성하는 표본정보 정제부, 각 고유정보를 포함하는 악성표본 종의 비율 및 각 고유정보를 포함하는 정상표본 종의 비율을 산출하여 각 고유정보에 비율을 부여하는 가중치 계산부, 및 비율을 기초로 탐지 대상 응용이 하나 이상의 악성표본 종 중 어느 악성표본 종과 유사한지 판단하여 탐지 대상 응용이 악성 코드임을 탐지하는 탐지부를 포함한다.

*대 표 도* - 도2



# 명 세 서

## 청구범위

### 청구항 1

악성코드 탐지장치에 있어서,

기저장된 또는 입력된 악성코드 및 정상코드로부터 악성표본 및 정상표본을 수집하는 정보추출부;

상기 수집된 악성표본 및 정상표본에 공통으로 존재하는 코드정보를 상기 악성표본 및 상기 정상표본에서 제거하여 상기 악성표본 및 상기 정상표본의 고유정보를 생성하는 표본정보 정제부;

상기 악성표본의 종 및 상기 정상표본의 종에 포함된 각각의 고유정보의 가중치를 계산하는 가중치 계산부; 및

상기 계산된 가중치 및 탐지 대상 응용에 포함된 하나 이상의 고유정보의 확률에 기초하여 상기 탐지 대상 응용이 대응되는 악성표본의 종에 해당하는 악성코드임을 탐지하는 탐지부를 포함하되,

상기 악성표본 및 상기 정상표본은 각각 하나 이상의 악성표본의 종 및 정상표본의 종으로 분류되고,

상기 고유정보의 확률은 상기 하나 이상의 악성표본의 종 및 정상표본의 종에 포함된 각각의 고유정보의 가중치에 기초하여 계산되는 것인, 악성코드 탐지장치.

### 청구항 2

제 1 항에 있어서,

상기 가중치 계산부는,

상기 악성표본에 포함된 하나 이상의 고유정보 중 어느 하나의 고유정보가 포함되는 악성표본의 수 대비 상기 악성표본의 종 내의 상기 어느 하나의 고유정보가 포함된 악성표본의 비율에 기초하여 상기 악성표본의 종에 포함된 각각의 고유정보에 대한 가중치를 계산하고,

상기 정상표본에 포함된 하나 이상의 고유정보 중 어느 하나의 고유정보가 포함되는 정상표본의 수 대비 상기 정상표본의 종 내의 상기 어느 하나의 고유정보가 포함된 정상표본의 비율에 기초하여 상기 정상표본의 종에 포함된 각각의 고유정보에 대한 가중치를 계산하는 악성코드 탐지장치.

### 청구항 3

제 1 항에 있어서,

상기 탐지부는,

상기 탐지 대상 응용에 포함된 하나 이상의 고유정보, 및 상기 악성표본의 종 및 상기 정상표본의 종에 포함된 각각의 고유정보의 가중치에 기초하여 상기 탐지 대상 응용이 상기 악성표본의 종에 포함될 확률 및 상기 정상표본의 종에 포함되지 않을 확률을 산출하여 상기 탐지 대상 응용이 어느 악성표본 종과 유사한지 판단하는 악성코드 탐지장치.

### 청구항 4

제 1 항에 있어서,

상기 탐지부는,

하기 수학식을 이용하여 상기 탐지 대상 응용이 어느 악성표본 종과 유사한지 판단하는 악성코드 탐지장치.

[수학식]

$$S(\alpha, F_i) = \frac{\sum\{p_k \mid k \in \alpha \,\&\, k \in F_i\}}{\sum\{p_k \mid k \in F_i\}} * \left(1 - \frac{\sum\{p_k \mid k \in \alpha \,\&\, k \in W\}}{\sum\{p_k \mid k \in W\}}\right)$$

a는 탐지 대상 응용, Fi는 i번째 악성표본 종에 포함된 표본정보의 합집합, k는 고유정보, $p_k$는 고유정보k를 포함한 악성표본 종의 비율 또는 정상표본 종의 비율, W는 하나 이상의 정상표본에 포함된 표본정보의 합집합, S(a, Fi)는 상기 탐지 대상 응용과 상기 i번째 악성표본 종의 유사도임.

**청구항 5**

제 4 항에 있어서,

상기 탐지부는,

상기 유사도가 일정한 임계치 이상인 때, 상기 탐지 대상 응용이 상기 i번째 악성표본 종에 속하는 악성코드임을 탐지하는 악성코드 탐지장치.

**청구항 6**

악성코드 탐지방법에 있어서,

기저장된 또는 입력된 악성코드 및 정상코드로부터 악성표본 및 정상표본을 수집하는 단계;

상기 수집된 악성표본 및 정상표본에 공통으로 존재하는 코드정보를 상기 악성표본 및 상기 정상표본에서 제거하여 상기 악성표본 및 상기 정상표본의 고유정보를 생성하는 단계;

상기 악성표본의 종 및 상기 정상표본의 종에 포함된 각각의 고유정보의 가중치를 계산하는 단계; 및

상기 계산된 가중치 및 탐지 대상 응용에 포함된 하나 이상의 고유정보에 기초하여 상기 탐지 대상 응용이 대응되는 악성표본의 종에 해당하는 악성코드임을  탐지하는 단계를 포함하되,

상기 악성표본과 상기 정상표본은 각각 하나 이상의 악성표본의 종 및 정상표본의 종으로 분류되고,

상기 고유정보의 확률은 상기 하나 이상의 악성표본 종 및 정상표본의 종에 포함된 각각의 고유정보의 가중치에 기초하여 계산되는 것인, 악성코드 탐지방법.

**청구항 7**

제 6 항에 있어서,

상기 가중치를 산출하는 단계는,

상기 악성표본에 포함된 하나 이상의 고유정보 중 어느 하나의 고유정보가 포함되는 악성표본의 수 대비 상기 악성표본의 종 내의 상기 어느 하나의 고유정보가 포함된 악성표본의 비율에 기초하여 상기 악성표본의 종에 포함된 각각의 고유정보에 대한 가중치를 계산하고,

상기 정상표본에 포함된 하나 이상의 고유정보 중 어느 하나의 고유정보가 포함되는 정상표본의 수 대비 상기 정상표본의 종 내의 상기 어느 하나의 고유정보가 포함된 정상표본의 비율에 기초하여 상기 정상표본의 종에 포함된 각각의 고유정보에 대한 가중치를 계산하는 악성코드 탐지방법.

**청구항 8**

제 6 항에 있어서,

상기 탐지하는 단계는,

상기 탐지 대상 응용에 포함된 하나 이상의 고유정보, 및 상기 악성표본의 종 및 상기 정상표본의 종에 포함된 각각의 고유정보의 가중치에 기초하여 상기 탐지 대상 응용이 상기 악성표본의 종에 포함될 확률 및 상기 정상표본의 종에 포함되지 않을 확률을 산출하여 상기 탐지 대상 응용이 어느 악성표본 종과 유사한지 판단하는 악성코드 탐지방법.

**청구항 9**

제 6 항에 있어서,

상기 탐지하는 단계는,

하기 수학식을 이용하여 상기 탐지 대상 응용이 어느 악성표본 종과 유사한지 판단하는 악성코드 탐지방법.

[수학식]

$$S(\alpha, F_i) = \frac{\sum\{p_k \mid k \in \alpha \,\&\, k \in F_i\}}{\sum\{p_k \mid k \in F_i\}} * \left(1 - \frac{\sum\{p_k \mid k \in \alpha \,\&\, k \in W\}}{\sum\{p_k \mid k \in W\}}\right)$$

a는 탐지 대상 응용, Fi는 i번째 악성표본 종에 포함된 표본정보의 합집합, k는 고유정보, $p_k$는 고유정보k를 포함한 악성표본 종의 비율 또는 정상표본 종의 비율, W는 하나 이상의 정상표본에 포함된 표본정보의 합집합, S(a, Fi)는 상기 탐지 대상 응용과 상기 i번째 악성표본 종의 유사도임.

**청구항 10**

제 9 항에 있어서,

상기 탐지하는 단계는,

상기 유사도가 일정한 임계치 이상인 때, 상기 탐지 대상 응용이 상기 i번째 악성표본 종에 속하는 악성코드임을 탐지하는 악성코드 탐지방법.

## *발명의 설명*

### *기 술 분 야*

[0001] 본 발명은 악성코드 탐지장치 및 방법에 관한 것으로서, 보다 상세하게는, 악성코드의 고유정보와의 유사도를 이용하여 악성코드를 탐지하는 장치 및 방법에 관한 것이다.

### *배 경 기 술*

[0002] 안드로이드(Android)는 휴대 전화를 비롯한 휴대용 장치를 위한 운영 체제와 미들웨어, 사용자 인터페이스 그리고 표준 응용 프로그램(예를 들어, 웹 브라우저, 이메일 클라이언트, 단문 메시지 서비스(SMS), 멀티미디어 메시지 서비스(MMS)등)을 포함하고 있는 소프트웨어 스택(STACK)이자 모바일 운영 체제로서, 전 세계 모바일 운영 체제 시장에서 큰 비중을 차지하고 있다. 안드로이드를 사용하는 휴대용 장치의 사용이 증가하면서 이를 대상으로 하는 악성코드 역시 빠르게 증가하여 모바일 장치에서의 악성코드의 주요 구동환경으로 지목되고 있다.

[0003] 안드로이드 환경에서 구동되는 악성코드는 휴대용 장치에 저장된 사용자의 개인정보에 접근하여 변조, 삭제 또

는 장치의 네트워크 기능을 이용하여 외부로 유출 시킬 수 있으며, 사용자의 허가 없이 금전적 이득을 취하거나, 휴대용 장치의 저장장치, 연산장치, 통신장치를 임의로 유용하여 다른 네트워크나 컴퓨터를 공격하는데 사용해 중대한 문제가 되고 있다.

[0004] 알려진 안드로이드 악성코드들의 대부분은 서로 유사성을 가진 종으로 밝혀지고 있으며, 새로이 발견되고 있는 악성코드들의 상당 수가 알려진 종에 속한 변종으로 보고되고 있다. 안드로이드 악성코드 제작자는 다수의 변종을 빠르게 생성, 갱신하여 악성코드를 탑재한 응용의 탐지 효율을 떨어뜨리는데, 이를 위해 한 번 사용한 코드를 재사용하거나, 기능 또는 구조의 일부만을 수정, 삭제, 또는 추가하거나, 리패키징 기술을 사용하여 악성코드를 탑재한 응용만을 변경하는 방법으로 다량의 변종을 제작한다. 따라서 안드로이드 악성코드에 효율적으로 대응하기 위해서는 악성코드 여부를 판단할 때 기존에 알려진 종과 유사성을 가지는지를 우선 판단하는 것이 효율적 접근방법이며 이를 위한 기술들이 연구, 제안되어왔다.

[0005] 대표적인 기존 안드로이드 악성코드 탐지 기술은 데스크탑 환경과 동일한 접근방법을 사용하여 특정 종을 판단하는 기준이 되는 대표 고유정보를 전문가의 분석으로부터 도출하여 정의하고, 이를 기준으로 탐지하는 기술이 있다. 변종에 대응하기 위해 제안된 기술로는 기준 고유정보의 정의 없이 응용 간 유사성을 비교하여 변종 여부를 탐지하는 방식이 있다.

[0006] 상용 장치 또는 응용에서 일반적으로 사용되는 안드로이드 악성코드 탐지 기술은 특정 종을 판단하는 기준이 되는 대표 고유정보가 포괄하는 범위가 매우 좁아 고도의 변종을 탐지하지 못하거나, 과도하게 넓은 범위를 포괄하는 정보를 사용하거나, 기준 고유정보의 정의 없이 응용 간 유사성 비교방식을 사용하여 오탐률이 높고 시간/공간적 효율이 떨어지는 단점이 있다.

[0007] 이와 관련하여 대한민국 공개특허공보 제 10-2010-0069135호(발명의 명칭: 악성코드 분류 시스템)에는 악성코드의 유사도를 측정함으로써, 기존의 악성코드와 새로운 악성코드의 유형 및 관련 정도를 쉽게 파악할 수 있는 악성코드 분류 시스템에 대하여 기술하고 있다.

## *발명의 내용*

### *해결하려는 과제*

[0008] 본 발명은 전술한 종래 기술의 문제점을 해결하기 위한 것으로서, 악성표본과 탐지 대상 응용의 유사성을 판단하기 위해 고유정보를 정의하고, 고유정보를 통계적 기법으로 선별하여 악성 코드를 탐지하는 악성코드 탐지장치 및 방법을 제공한다.

[0009] 또한, 본 발명은 전술한 종래 기술의 문제점을 해결하기 위한 것으로서, 악성표본과 탐지 대상 응용의 고유정보 간의 비교를 통해 유사도를 검출하여 악성 코드를 탐지하는 악성코드 탐지장치 및 방법을 제공한다.

### *과제의 해결 수단*

[0010] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 제 1 측면에 따른 악성코드 탐지장치는, 기저장된 또는 입력된 악성표본 및 정상표본으로부터 표본정보를 수집하는 정보추출부, 하나 이상의 악성표본의 하나 이상의 표본정보 및 하나 이상의 정상표본의 하나 이상의 표본정보에 공통으로 존재하는 코드정보를 악성표본 및 정상표본에서 제거하여 악성표본 및 정상표본의 고유정보를 생성하는 표본정보 정제부, 각 고유정보를 포함하는 악성표본 종의 비율 및 각 고유정보를 포함하는 정상표본 종의 비율을 산출하여 각 고유정보에 비율을 부여하는 가중치 계산부, 및 비율을 기초로 탐지 대상 응용이 하나 이상의 악성표본 종 중 어느 악성표본 종과 유사한지 판단하여 탐지 대상 응용이 악성 코드임을 탐지하는 탐지부를 포함한다.

[0011] 또한, 본 발명의 제 2 측면에 따른 악성코드 탐지방법은, 기저장된 또는 입력된 악성표본 및 정상표본으로부터 표본정보를 수집하는 단계, 하나 이상의 악성표본의 하나 이상의 표본정보 및 하나 이상의 정상표본의 하나 이상의 표본정보에 공통으로 존재하는 코드정보를 악성표본 및 정상표본에서 제거하여 악성표본 및 정상표본의 고유정보를 생성하는 단계, 각 고유정보를 포함하는 악성표본 종의 비율 및 각 고유정보를 포함하는 정상표본 종의 비율을 산출하여 각 고유정보에 비율을 부여하는 단계, 및 비율을 기초로 탐지 대상 응용이 하나 이상의 악성표본 종 중 어느 악성표본 종과 유사한지 판단하여 탐지 대상 응용이 악성 코드임을 탐지하는 단계를 포함한다.

### *발명의 효과*

[0012] 전술한 본 발명의 과제 해결 수단에 의하면, 정상표본의 고유정보가 정제된 악성표본의 고유정보를 추출하여 탐지 대상 응용의 악성표본 종을 정의할 수 있다.

[0013] 또한, 전술한 본 발명의 과제 해결 수단에 의하면, 추출된 고유정보를 이용하여 탐지 대상 응용이 어떤 종과 유사한지 확률적으로 산출하여 유사도를 검출하고, 유사도를 기반으로 악성표본 종을 정의할 수 있다.

[0014] 또한, 전술한 본 발명의 과제 해결 수단에 의하면, 악성코드 탐지장치는 악성코드 고유정보의 유사성을 이용하여, 코드 재사용, 리패키징, 코드의 일부 변경과 같이 의도된 변종 악성코드 또는 코드 구현단계에서 일부 고유정보를 이용하는 신종 악성코드를 탐지할 수 있다.

## *도면의 간단한 설명*

[0015] 도 1은 본 발명의 일 실시예에 따른 악성코드 탐지장치의 블록도이다.

도 2는 본 발명의 일 실시예에 따른 악성코드 탐지장치가 악성코드를 탐지하는 방법의 순서도이다.

도 3은 표본정보의 정제 및 비율 산출의 과정을 상세하게 도시한다.

도 4는 표본정보의 정제 및 비율 산출의 과정에 대하여 설명하기 위한 일 예에 대하여 도시한다.

도 5는 악성코드 탐지장치가 산출된 비율을 이용하여 탐지 대상 응용과 유사한 악성 표본을 탐지하는 방법에 대한 일 예이다.

도 6은 본 발명의 일 실시예에 따른 악성코드 탐지장치를 이용하여 평균 탐지 성공률, 평균 오탐율을 산출한 성능 도표이다.

## *발명을 실시하기 위한 구체적인 내용*

[0016] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0017] 본원 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함" 한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다. 본원 명세서 전체에서 사용되는 정도의 용어 "~(하는) 단계" 또는 "~의 단계"는 "~ 를 위한 단계"를 의미하지 않는다.

[0018] 본 발명의 일 실시예에 따르면 악성 코드 탐지장치는 안드로이드 악성표본 및 정상표본을 초기에 저장할 수 있고, 표본정보 추출, 표본정보의 정제 및 고유정보의 비율 계산, 악성코드 탐지의 세 단계를 거친다. 악성표본은 악성 코드를 종류별로 분류한 표본으로, 일정 기준에 따라 각각 "종"으로 그룹화될 수 있다. 정상표본(White list)은 악성표본이 될 수 없는 정상적인 코드를 종류별로 분류한 표본이고 마찬가지로 일정 기준에 따라 각각 "종"으로 그룹화될 수 있다. 단, 정상표본은 일 예에 의하면 모든 표본이 하나의 종을 형성한다.

[0019] 도 1은 본 발명의 일 실시예에 따른 악성코드 탐지장치의 블록도이다.

[0020] 상술한 과정을 수행하기 위한 본 발명의 일 실시예에 따른 악성코드 탐지장치는, 정보추출부(110), 표본정보 정제부(120), 가중치 계산부(130), 및 탐지부(140)를 포함한다.

[0021] 우선, 정보추출부(110)는 기저장된 또는 입력된 악성표본 및 정상표본으로부터 그들의 표본정보를 수집한다.

[0022] 표본정보 정제부(120)는 하나 이상의 악성표본의 하나 이상의 표본정보 및 하나 이상의 정상표본의 하나 이상의 표본정보에 공통으로 존재하는 코드정보를 악성표본 및 정상표본에서 제거하여 악성표본 및 정상표본의 고유정보를 생성한다. 즉, 악성표본과 정상표본이 모두 포함하고 있는 코드정보는 악성표본 또는 정상표본을 구분하는 명확한 기준이 될 수 없기 때문에 하나 이상의 정상표본의 모든 표본정보와 하나 이상의 악성표본의 모든 표본정보를 비교하여 공통으로 존재하는 코드정보가 제거되고, 이러한 코드정보가 제거된 결과 고유정보가 생성된다.

[0023] 가중치 계산부(130)는 정제된 악성표본 또는 정제된 정상표본의 각 고유정보를 포함하는 악성표본 종의 비율 또는 정상표본 종의 비율을 산출한다. 본 발명의 일 실시예에 따르면, 가중치 계산부(130)는 전체 악성표본 종 내 어느 한 고유정보를 포함하는 악성표본 수 대비 어느 한 악성표본 종 내 어느 한 고유정보를 포함하는 악성

표본 수를 구하여 비율을 산출할 수 있다. 정상표본에 대해서도 마찬가지로 비율을 산출할 수 있다. 일 예에 따라 모든 정상표본이 하나의 종을 형성하는 경우, 비율은 전체 정상표본의 수 대비 전체 정상표본 내 어느 한 고유정보를 포함하는 정상표본 수일 수 있다. 이러한 비율은 각 고유정보에 대한 '가중치'로 표현될 수 있고, 이러한 비율 또는 가중치는 각 고유정보에 부여될 수 있다.

[0024] 탐지부(140)는 탐지 대상 응용이 하나 이상의 악성표본 종 중 어느 악성표본 종과 유사한지 판단하여 탐지 대상 응용이 악성 코드인지 탐지한다. 이때, 탐지부(140)는 가중치 계산부(130)에서 산출한 비율을 기초로 유사한지 판단할 수 있다. 본 발명의 일 실시예에 따르면, 탐지부(140)는 탐지 대상 응용 및 어느 한 악성표본 종이 공통으로 포함하고 있는 고유정보가 해당 악성표본 종에 존재할 확률, 및 탐지 대상 응용 및 정상표본이 공통으로 포함하고 있는 고유정보가 해당 정상표본에 존재하지 않을 확률을 이용하여 탐지 대상 응용이 어느 한 악성표본 종과 유사한지 판단할 수 있다. 이러한 탐지부(140)의 확률 계산 방법을 식으로 나타내면 수학식 1과 같이 나타낼 수 있다.

*수학식 1*

[0025]
$$S(\alpha, F_i) = \frac{\sum\{p_k \mid k \in \alpha \,\&\, k \in F_i\}}{\sum\{p_k \mid k \in F_i\}} * \left(1 - \frac{\sum\{p_k \mid k \in \alpha \,\&\, k \in W\}}{\sum\{p_k \mid k \in W\}}\right)$$

[0026] 이때, a는 탐지 대상 응용, Fi는 i번째 악성표본 종에 포함된 표본정보의 합집합, k는 고유정보, $p_k$는 고유정보 k를 포함한 악성표본 종의 비율 또는 정상표본 종의 비율, W는 하나 이상의 정상표본에 포함된 표본정보의 합집합, S(a, Fi)는 탐지 대상 응용과 i번째 악성표본 종의 유사도를 의미한다. 수학식 1과 관련된 상세한 설명은 도 5와 관련하여 후술한다.

[0027] 본 발명의 또 다른 실시예에 따르면 탐지부(140)는 이러한 유사도가 일정한 임계치 이상인 때, 탐지 대상 응용이 해당 악성표본 종에 속하는 악성 코드임을 탐지할 수 있고, 임계치는 보안 상태에 따라 다르게 조정할 수 있다.

[0028] 이하, 도 2 내지 도 5와 관련하여 악성코드 탐지장치가 악성코드를 탐지하는 방법에 대하여 설명한다.

[0029] 도 2는 본 발명의 일 실시예에 따른 악성코드 탐지장치가 악성코드를 탐지하는 방법의 순서도이다.

[0030] 먼저, 악성코드 탐지장치가 악성표본 및 정상표본으로부터 종 표본정보를 수집한다(S210). 예를 들어, 악성코드 탐지장치는 악성표본 또는 정상표본으로부터 문자열, 클래스(Class)명, 메소드(Method)명, API 호출부, 및 바이트코드 명령부의 네 가지 정보를 악성코드 탐지를 위한 표본정보로써 수집한다. 이는, 안드로이드에서 사용되는 응용의 실행코드 파일(Dalvik Executable (DEX)) 이 일반적으로 압축된 "응용 이름.apk" 파일 내 "classes.dex"의 형식으로 존재하는 표준구조 정보를 이용하여, 수집된 악성표본 또는 정상표본에서 "1) ASCII 문자열, 2) 클래스(Class), 메소드(Method) 명 문자열, 3) API 호출 이진문자열, 4) 메소드 구현 이진문자열"을 이진문자열의 형태로 수집하는 것을 의미한다.

[0031] 이어서, 악성코드 탐지장치는 표본정보를 정제하고 고유정보의 비율을 계산(산출)한다(S220, S230). 이때, 악성코드 탐지장치는 기저장된 또는 입력된 하나의 악성표본 또는 정상표본에서 발견된 하나 이상의 표본정보에 대하여 같은 종류의 표본정보가 여러 개인 경우 한 개의 표본정보로 보고, 모든 정상표본은 한 개의 종으로 본다.

[0032] 도 3은 이러한 표본정보의 정제 및 비율 계산의 과정을 더욱 상세하게 도시한다.

[0033] 표본 정보를 정제하는 경우(S220), 예를 들어, 종 1에 포함된 악성표본이 네 개인 때, 종 1에 포함된 표본 1 내지 표본 4에서 정상표본에 포함된 모든 표본정보를 제거한다. 즉, 하나 이상의 정상표본이 포함하는 표본정보의 합집합 및 하나 이상의 악성표본이 포함하는 표본정보의 합집합이 공통으로 포함하는 표본정보를 제거한다. 더욱 상세한 설명은 도 4와 관련하여 후술한다. 이러한 공통 표본정보를 제거한 악성표본은 고유정보를 포함하고 있다. 정상표본에 대해서도 마찬가지로 수행된다.

[0034] 이어서, 각 고유정보를 포함하는 악성표본 종의 비율 및 각 고유정보를 포함하는 정상표본 종의 비율을 계산한다(S230). 즉, 전체 악성표본 종 내 어느 한 고유정보를 포함하는 악성표본 수 대비 어느 한 악성표본 종 내에서 고유정보를 포함하는 악성표본 수를 이용하여 비율을 산출한다(비율 = (종 내 정보 A가 존재하는 표본 수) / (전체 표본 내 정보 A가 존재하는 표본 수)). 정상표본에 대해서는, 모든 정상표본이 하나의 종을 형성하는 경우, 비율은 전체 정상표본의 수 대비 전체 정상표본 내 어느 한 고유정보를 포함하는 정상표본 수일 수 있다. 이때, 비율은 한 종의 각 고유정보에 대한 가중치를 의미할 수 있다. 그리고, 이와 같이 산출된 비율(또는, 가중치)은 각 고유정보에 부여된다.

[0035] 도 4는 표본정보의 정제 및 비율 계산의 과정에 대하여 설명하기 위한 일 예에 대하여 도시한다.

[0036] 하나 이상의 악성표본 종(종 1, 종 2, 종 3)은 각 종에 속한 악성표본(악성표본1, 악성표본 2)을 포함하고, 정상표본(정상표본 1, 정상표본 2)은 한 표본이 하나의 종을 형성한다. 악성표본 및 정상표본은 표본 정보(A, B, C, D, E, F, G, H, I, J, K)를 포함한다.

[0037] 악성 코드 탐지장치가 하나 이상의 정상표본1 또는 정상표본 2에 존재하는 모든 표본 정보(E, F, I, J, K)를 악성표본에서 제거하여 악성표본의 고유 정보를 생성한다(S220). 따라서, 모든 악성표본 종에 존재하는 표본정보(A, B, C, D, E, F, G, H)에서 정상표본에 존재하는 표본정보(E, F)를 제거한다. 마찬가지로 하나 이상의 악성표본 종에 존재하는 모든 표본 정보(A, B, C, D, E, F, G, H)를 정상표본에서 제거하여 정상표본의 고유 정보를 생성한다. 따라서, 모든 정상표본 종에 존재하는 표본정보(E, F, I, J, K)에서 정상표본에 존재하는 표본정보(E, F)를 제거한다. 즉, 모든 악성표본 및 모든 정상표본에 공통으로 존재하는 코드정보를 각 종에서 제거한다. 그 결과, 악성표본 종1은 고유정보(A, D, G), 악성표본 종 2는 고유정보(B, D, H), 악성표본 종 3은 고유정보(C, G, H), 정상표본 종은 고유정보(I, J, K)를 포함한다.

[0038] 이어서, 각 악성표본 종에 존재하는 각 고유정보에 대하여 악성표본의 비율을 계산하는데(S230), 악성표본 종 1의 고유정보 D에 대하여 일 예를 들면, 전체 악성표본 종 중에서 고유정보 D를 포함하는 악성표본의 수는 3이고(악성표본 종1의 표본 1 및 표본 2, 악성표본 종 2의 표본 1), 악성표본 종 1에서 고유정보 D를 포함하는 악성표본의 수는 2이다(악성표본 종 1의 표본 1 및 표본 2). 따라서 비율은 2/3으로 산출된다. 악성표본 종 2의 고유정보 H에 대하여 다른 예를 들면, 전체 악성표본 종 중에서 고유정보 H를 포함하는 악성표본의 수는 2이고(악성표본 종 2의 표본 2, 악성표본 종 3의 표본 1), 악성표본 종 2에서 고유정보 H를 포함하는 악성표본의 수는 1이다(악성표본 종 2의 표본 2). 나머지, 악성표본 종 1의 고유정보 A, G, 악성표본 종 2의 고유정보 B, D, 악성표본 종 3의 고유정보 C, G, H에 대해서도 동일한 방법으로 산출된다. 그리고 이러한 비율(또는 가중치)이 각 고유정보에 부여된다.

[0039] 정상표본은 표본에 관계없이 하나의 종을 형성할 수 있다. 따라서 악성표본과 달리 정상표본의 비율 계산시, 고유정보 J에 대하여, 전체 정상표본의 수는 2(정상표본 1, 정상표본 2)이고, 고유정보 J를 포함하는 정상표본의 수는 1(정상표본 1)인바, 고유정보 J에 대한 비율은 1/2로 계산된다. 나머지 고유정보 I, K에 대해서도 동일한 방법으로 산출된다. 그리고 이러한 비율(또는 가중치)이 각 고유정보에 부여된다.

[0040] 그리고 각 고유정보에 대해 부여된 비율을 기초로 탐지 대상 응용이 어느 악성 표본 종과 유사한지 판단하여 탐지대상 응용이 해당 악성표본 종으로 분류되는 악성코드임을 탐지할 수 있게 된다(S240).

[0041] 본 발명의 일 실시예에 따르면 악성코드 탐지장치는 탐지 대상 응용 및 어느 한 악성표본 종이 공통으로 포함하고 있는 고유정보가 악성표본 종에 존재할 확률, 및 탐지 대상 응용 및 어느 한 정상표본이 공통으로 포함하고 있는 고유정보가 정상표본에 존재하지 않을 확률을 이용하여 탐지 대상 응용이 어느 악성표본 종과 유사한지 판단할 수 있다.

[0042] 또한 본 발명의 다른 실시예에 따르면, 수학식 1을 이용하여 유사도를 산출하고 유사도에 기반해 어느 악성표본 종과 유사한지 판단할 수 있다.

[0043] 또한 본 발명의 또 다른 실시예에 따르면, 산출된 유사도가 특정 임계치 이상일 때, 탐지 대상 응용이 해당 유사도가 산출된 악성표본 종에 속하는 악성코드임을 탐지할 수 있다. 이와 관련하여 도 5에서 상세히 후술한다.

[0044] 도 5는 악성코드 탐지장치가 이와 같이 산출된 비율을 이용하여 탐지 대상 응용과 유사한 악성 표본을 탐지하는 방법에 대한 일 예이다.

[0045] 본 발명의 일 실시예에 따르면 탐지대상 응용에 대해서도, 상술한 바와 같이 정상표본 및 악성표본 공통으로 포함하는 표본정보(E, F)를 제거하고, 나머지 표본정보(즉, 고유정보)를 기초로 각 악성표본 종과의 유사성을 탐

지한다. 예를 들어, 수학식 1을 이용한 경우, 악성표본 종 2와의 유사성을 탐지함에 있어서, 고유정보 B에 대하여 악성표본 종 2는 2/2(=1)의 비율을, 고유정보 D에 대하여 종 2는 1/3(=0.33)의 비율을, 고유정보 H에 대하여 악성표본 종 2는 1/2(=0.5)의 비율을 부여한다. 비율의 총합은 1.83이 된다. 탐지대상 응용(a)이 포함하는 고유정보는 A, D, G, J 인바, 이 중 고유정보 2와 공통되는 고유정보 D의 비율은 0.33이다. 그리고, 정상표본과 탐지대상 응용(a)간의 비유사성을 수학식 1에서 이용하기 위해, 정상표본에 존재하는 고유정보(I, J, K)의 비율의 총합은 2이고, 탐지대상 응용(a)에 공통으로 존재하는 고유정보는 J인바, J에 대한 정상표본의 비율은 0.5이다. 이를 수학식 1에 대입한 경우, 다음과 같이 0.14의 결과가 도출된다( $S(a,F2)=\frac{0.33}{1.83}*\left(1-\frac{0.5}{2}\right)=0.14$ ). 악성표본 종 1 및 종 3에 대해서도 이와 같이 유사도를 산출하면, 종 1에 대해서는 0.75, 종 3에 대해서는 0.19의 유사도가 산출된다. 따라서, 탐지대상 응용(a)은 이 중 가장 높은 유사도를 보이는 종 1로 탐지될 수 있다. 다만, 본 발명의 다른 실시예에 따르면, 유사도에 대하여 임계치를 기설정할 수 있고, 유사도가 일정 임계치를 초과한 경우에 대하여 탐지대상 응용(a)이 해당 악성표본 종으로 분류되는 악성코드임을 탐지할 수 있게 된다.

[0046] 도 6은 본 발명의 일 실시예에 따른 악성코드 탐지장치를 이용하여 평균 탐지 성공률, 평균 오탐율을 계산한 성능 도표이다.

[0047] 도 6의 성능 도표는 공개된 안드로이드 악성표본 4개의 종, 79개의 표본과 1,680개의 정상표본을 사용하여 각 종에서 난수적으로 선택한 20%를 고유정보 생성표본으로, 나머지 80%를 검사 표본으로하여 10회 실험한 결과의 평균값이다.

[0048] 표 1의 성능 비교표는 동일 기술분야의 해외 선행 연구에서 공개된 동일 성능지표와 본 기법의 실험에서 도출된 성능의 비교표이다. Accuracy, Precision, Recall의 3개 성능지표에서 모두 진보된 성능을 보일 뿐 아니라 Precision과 Recall의 종합평가지표인 F-Measure, 구체적으로 F1 Score평가에서도 높은 수치를 보였다.

*표 1*

[0049]

| Method | Accuracy | Recall | Precision | F-measure |
|---|---|---|---|---|
| AndroGuard | 93.04% | 49.58% | 99.16% | 66.11% |
| DroidMat | 97.87% | 87.39% | 96.74% | 91.83% |
| Proposed | **99.89%** | **97.73%** | **99.74%** | **98.73%** |

[0050] 본 발명은 이와 같이 다수의 응용 중에서 악성코드를 탐지하여야 할 때, 알려진 악성코드의 표본과 그 변종을 사전에 수집하여 정제한 종의 고유정보를 이용하여 정확하고 효율적으로 악성코드를 탐지함으로서 전문가가 직접 분석하여야 하는 대상을 대폭 감소시키고, 최종적으로 모바일 장치의 사용자를 악성코드로의 감염 위험으로부터 보호함과 동시에 악성코드에 감염된 모바일 장치에 의해 발생할 수 있는 이차적 피해를 방지하는 효과가 있다.

[0051] 참고로, 본 발명의 실시예에 따른 도 1에 도시된 구성 요소들은 소프트웨어 또는 FPGA(Field Programmable Gate Array) 또는 ASIC(Application Specific Integrated Circuit)와 같은 하드웨어 구성 요소를 의미하며, 소정의 역할들을 수행한다.

[0052] 그렇지만 '구성 요소들'은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니며, 각 구성 요소는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다.

[0053] 따라서, 일 예로서 구성 요소는 소프트웨어 구성 요소들, 객체지향 소프트웨어 구성 요소들, 클래스 구성 요소들 및 태스크 구성 요소들과 같은 구성 요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다.

[0054] 구성 요소들과 해당 구성 요소들 안에서 제공되는 기능은 더 작은 수의 구성 요소들로 결합되거나 추가적인 구성 요소들로 더 분리될 수 있다.

[0055] 한편, 도 1에서 도시된 각각의 구성요소는 일종의 '모듈'로 구성될 수 있다. 상기 '모듈'은 소프트웨어 또는 Field Programmable Gate Array(FPGA) 또는 주문형 반도체(ASIC, Application Specific Integrated Circuit)

과 같은 하드웨어 구성요소를 의미하며, 모듈은 어떤 역할들을 수행한다. 그렇지만 모듈은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. 모듈은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 실행시키도록 구성될 수도 있다. 구성요소들과 모듈들에서 제공되는 기능은 더 작은 수의 구성요소들 및 모듈들로 결합되거나 추가적인 구성요소들과 모듈들로 더 분리될 수 있다.

[0056] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0057] 상술한 본 발명에 따른 악성코드 탐지방법은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로서 구현되는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체로는 컴퓨터 시스템에 의하여 해독될 수 있는 데이터가 저장된 모든 종류의 기록 매체를 포함한다. 예를 들어, ROM(Read Only Memory), RAM(Random Access Memory), 자기 테이프, 자기 디스크, 플래쉬 메모리, 광 데이터 저장장치 등이 있을 수 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 통신망으로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 읽을 수 있는 코드로서 저장되고 실행될 수 있다.

[0058] 본 발명의 방법 및 시스템은 특정 실시예와 관련하여 설명되었지만, 그것들의 구성 요소 또는 동작의 일부 또는 전부는 범용 하드웨어 아키텍쳐를 갖는 컴퓨터 시스템을 사용하여 구현될 수 있다.

## *부호의 설명*

[0059] S210: 고유정보 수집

S220, S230: 정제 및 비율 계산

S240: 악성코드 여부 탐지

110: 정보추출부

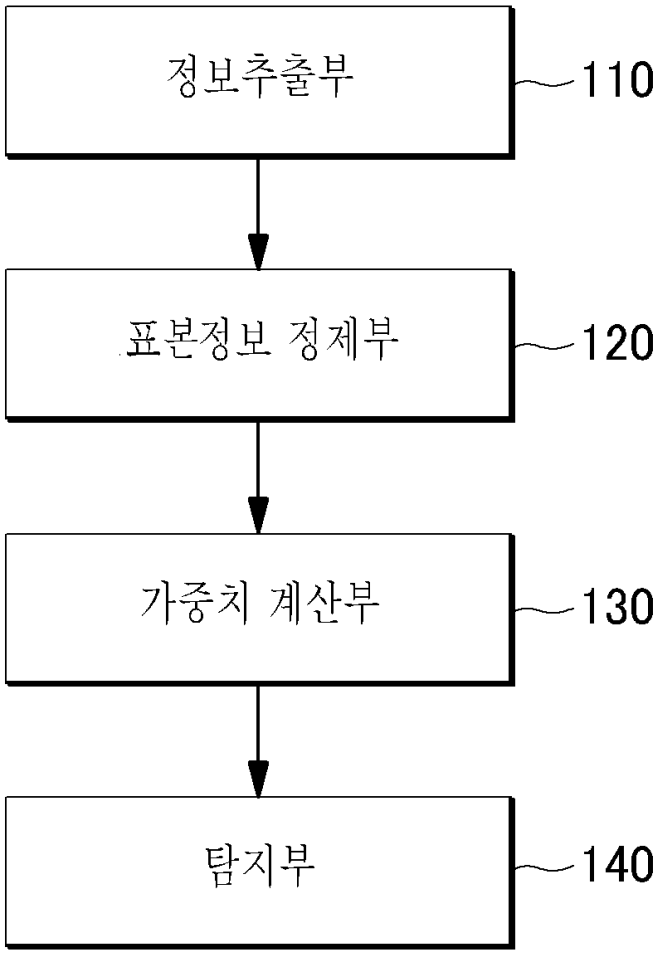
120: 표본정보 정제부

130: 가중치 계산부

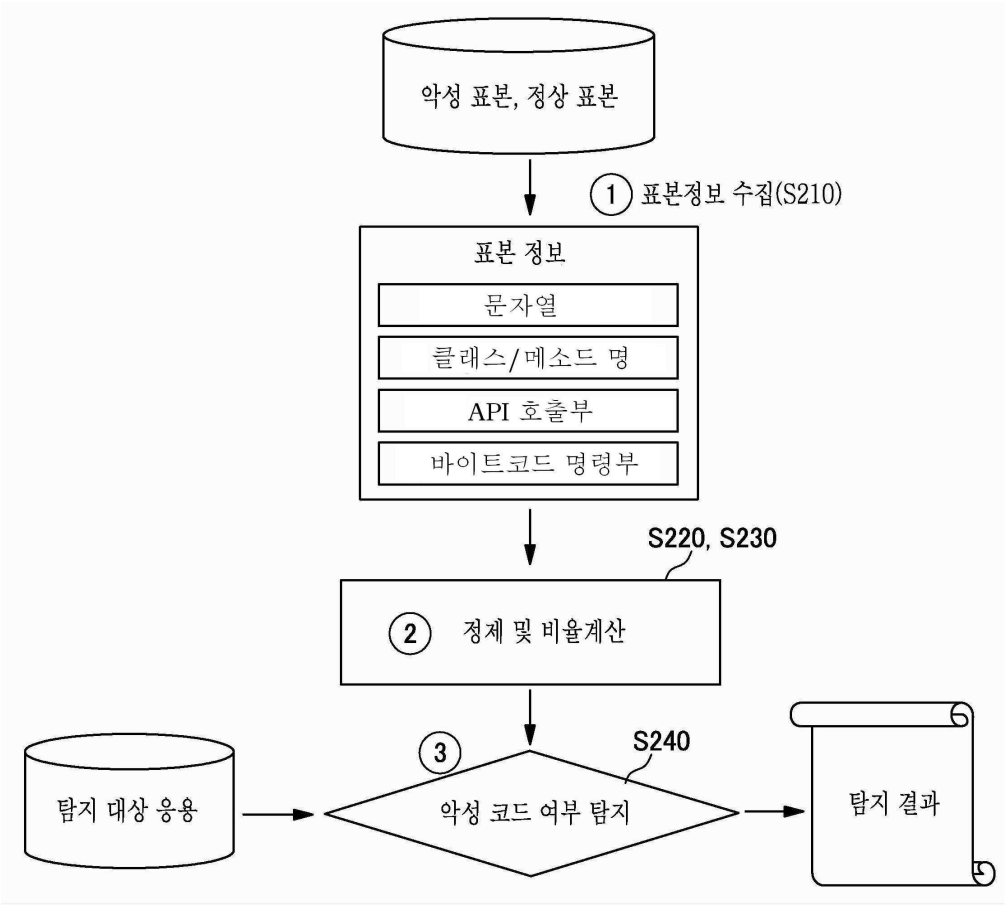
140: 탐지부

도면

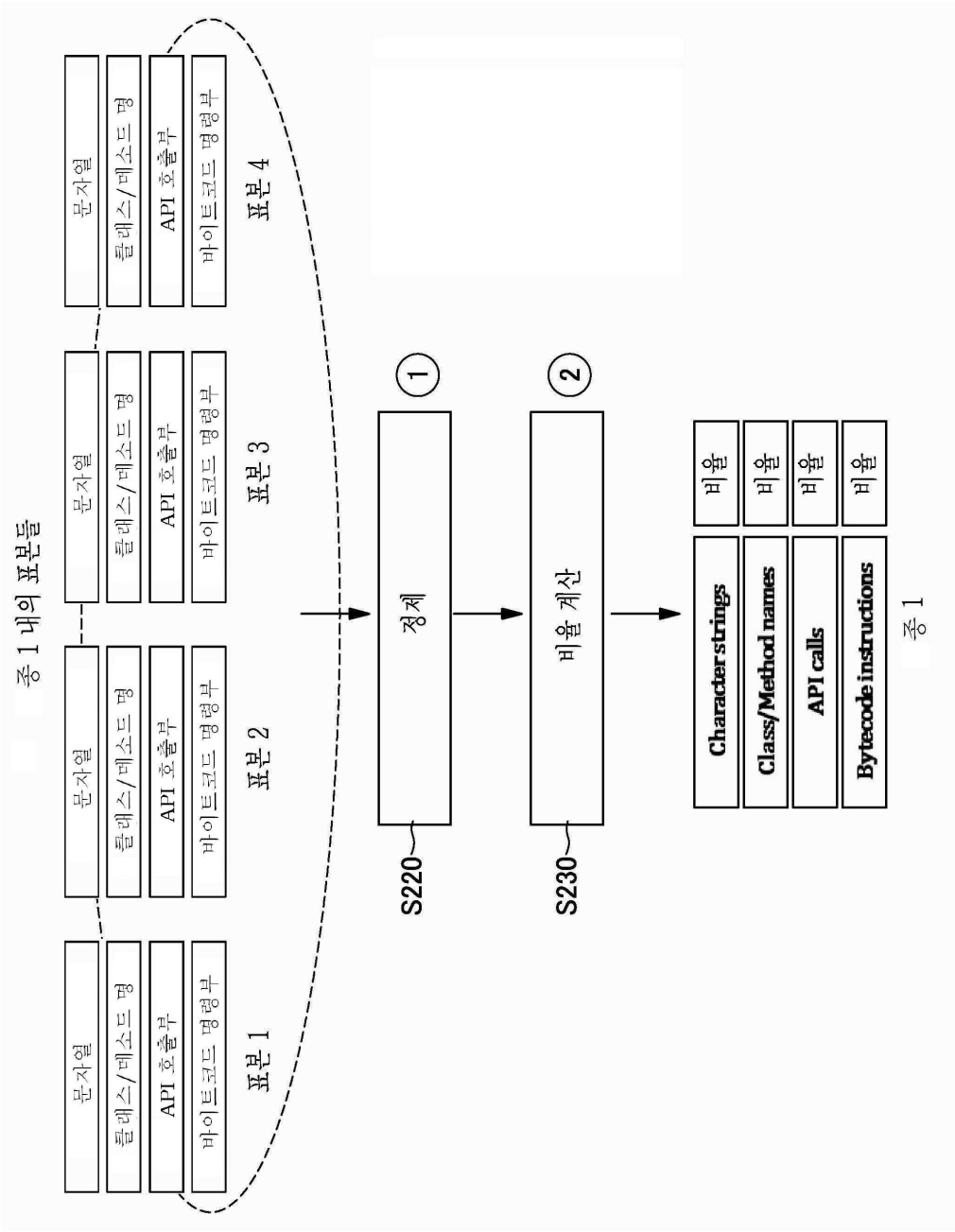
도면1



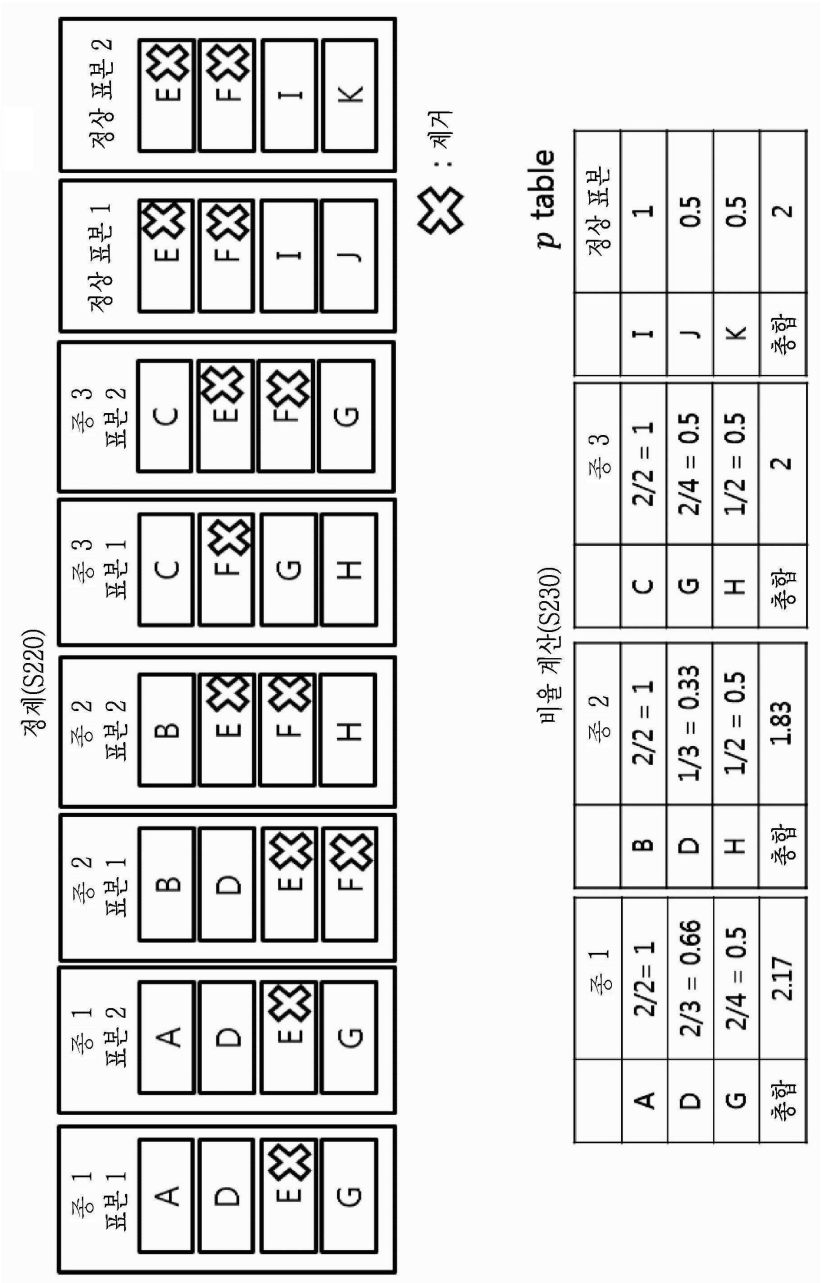
도면2


악성 표본, 정상 표본
① 표본정보 수집(S210)
표본 정보
문자열
클래스/메소드 명
API 호출부
바이트코드 명령부
S220, S230
② 정제 및 비율계산
③
S240
탐지 대상 응용
악성 코드 여부 탐지
탐지 결과

도면3


종 1 내의 표본들
표본 1
문자열
클래스/메소드 명
API 호출부
바이트코드 명령부
표본 2
문자열
클래스/메소드 명
API 호출부
바이트코드 명령부
표본 3
문자열
클래스/메소드 명
API 호출부
바이트코드 명령부
표본 4
문자열
클래스/메소드 명
API 호출부
바이트코드 명령부
①
정제
S220
②
비율 계산
S230
Character strings
Class/Method names
API calls
Bytecode instructions
비율
비율
비율
비율
종 1

도면4




비율 계산(S230)

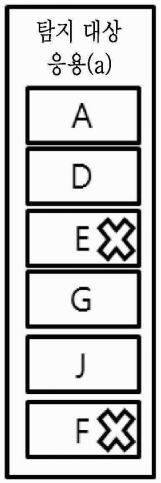
*p* table

| | 종 1 |
|---|---|
| A | 2/2= 1 |
| D | 2/3 = 0.66 |
| G | 2/4 = 0.5 |
| 총합 | 2.17 |

| | 종 2 |
|---|---|
| B | 2/2 = 1 |
| D | 1/3 = 0.33 |
| H | 1/2 = 0.5 |
| 총합 | 1.83 |

| | 종 3 |
|---|---|
| C | 2/2 = 1 |
| G | 2/4 = 0.5 |
| H | 1/2 = 0.5 |
| 총합 | 2 |

| | 정상 표본 |
|---|---|
| I | 1 |
| J | 0.5 |
| K | 0.5 |
| 총합 | 2 |




| | 종 1 | | 종 2 | | 종 3 | | 정상 표본 |
|---|---|---|---|---|---|---|---|
| A | 2/2= 1 | B | 2/2 = 1 | C | 2/2 = 1 | I | 1 |
| D | 2/3 = 0.66 | D | 1/3 = 0.33 | G | 2/4 = 0.5 | J | 0.5 |
| G | 2/4 = 0.5 | H | 1/2 = 0.5 | H | 1/2 = 0.5 | K | 0.5 |
| 총합 | 2.17 | 총합 | 1.83 | 총합 | 2 | | 2 |

$p$ table

$$S(\alpha, F1) = \frac{1 + 0.66 + 0.5}{2.17} * \left(1 - \frac{0.5}{2}\right) = 0.75$$

$$S(\alpha, F2) = \frac{0.33}{1.83} * \left(1 - \frac{0.5}{2}\right) = 0.14$$

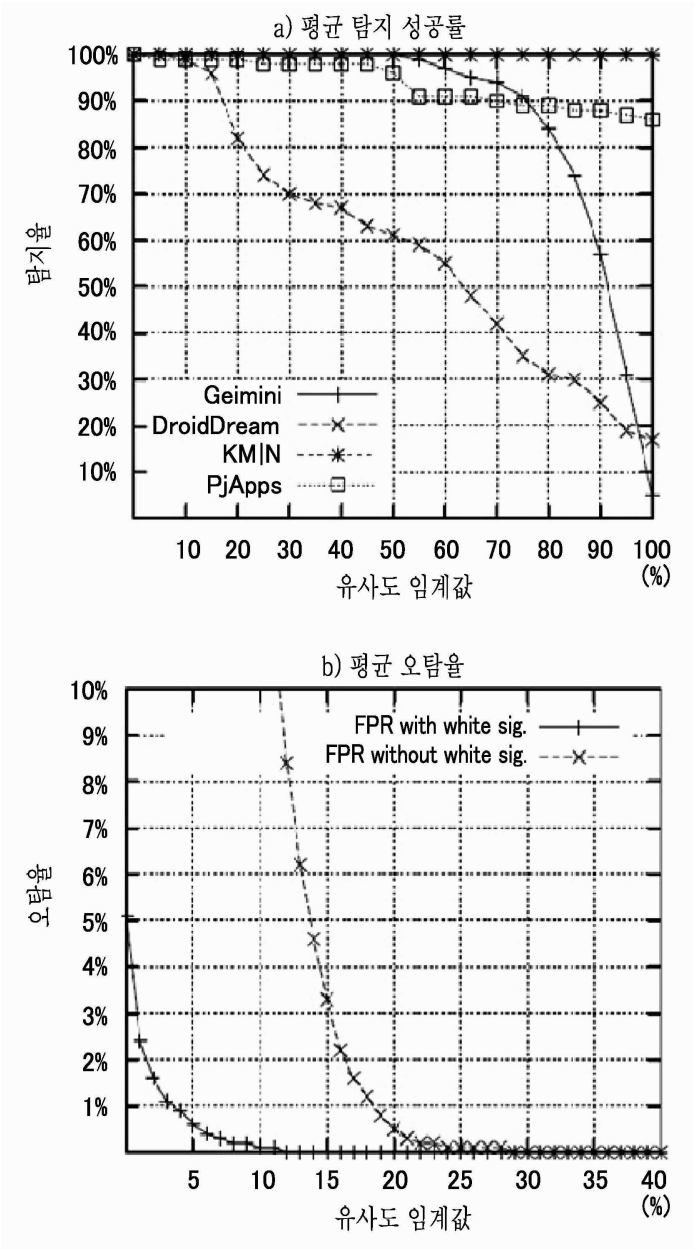
$$S(\alpha, F3) = \frac{0.5}{2} * \left(1 - \frac{0.5}{2}\right) = 0.19$$

$$t = 0.5,\ S(\alpha, F1) = 0.75, S(\alpha, F2) = 0.14,\ S(\alpha, F3) = 0.19$$
$$\therefore \alpha \in F1$$



등록특허 10-1508577

도면6


a) 평균 탐지 성공률
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
탐지율
Geimini
DroidDream
KM|N
PjApps
10 20 30 40 50 60 70 80 90 100
(%)
유사도 임계값
b) 평균 오탐율
10%
9%
8%
7%
6%
5%
4%
3%
2%
1%
오탐율
FPR with white sig.
FPR without white sig.
5 10 15 20 25 30 35 40
(%)
유사도 임계값