Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.3, Jun. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.3.549

악성코드 분석의 Ground-Truth 향상을 위한 Unified Labeling과 Fine-Grained 검증*

오 상 진,† 박 래 현, 권 태 경‡
연세대학교 정보대학원 정보보호연구실

Unified Labeling and Fine-Grained Verification for Improving Ground-Truth of Malware Analysis*

Sang-Jin Oh,† Leo-Hyun Park, Tae-Kyoung Kwon‡
Information Security Lab., Graduation School of Information, Yonsei University

요 약

최근 AV 벤더들의 악성코드 동향 보고서에 따르면 신종, 변종 악성코드의 출현 개수가 기하급수적으로 증가하고 있다. 이에 따라 분석 속도가 떨어지는 수동적 분석방법을 대체하고자 기계학습을 적용하는 악성코드 분석 연구가 활발히 연구되고 있다. 하지만 지도학습기반의 기계학습을 이용할 때 많은 연구에서 AV 벤더가 제공하는 신뢰성이 낮은 악성코드 패밀리명을 레이블로 사용하고 있다. 이와 같이 악성코드 레이블의 낮은 신뢰성 문제를 해결하기 위해 본 논문에서는 새로운 레이블링 기법인 "Unified Labeling"을 소개하고 나아가 Fine-grained 방식의 특징 분석을 통해 악성 행위 유사성을 검증한다. 본 연구의 검증을 위해 다양한 기반의 클러스터링 알고리즘을 이용하여 기존의 레이블링 기법과 비교하였다.

ABSTRACT

According to a recent report by anti-virus vendors, the number of new and modified malware increased exponentially. Therefore, malware analysis research using machine learning has been actively researched in order to replace passive analysis method which has low analysis speed. However, when using supervised learning based machine learning, many studies use low-reliability malware family name provided by the antivirus vendor as the label. In order to solve the problem of low-reliability of malware label, this paper introduces a new labeling technique, "Unified Labeling", and further verifies the malicious behavior similarity through the feature analysis of the fine-grained method. To verify this study, various clustering algorithms were used and compared with existing labeling techniques.

Keywords: Malware, Labeling, Machine Learning, Clustering

I. 서 론

최근 Anti-Virus(AV) 벤더들의 악성코드 동향 보고서에 따르면 신종, 변종 악성코드의 출현 개수가 기하급수적으로 증가하고 있다. Kaspersky security bulletin에 따르면 2017년 새로 등장한 악

Received(02. 12. 2019), Modified(04. 30. 2019), Accepted(04. 30. 2019)
* 본 논문은 2018년도 한국정보보호학회 동계학술대회에 발표한 우수논문을 개선 및 확장한 것임.
* 이 논문은 2019년도 정부 (과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원(No. 2017-0-00380, 차세대 인증 기술 개발)과 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 지원을 받아 수행된 연구임 (IITP-2019-2016-0-00304).
† 주저자, dhtkdwls537@gmail.com
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

성코드는 약 천5백만 개에 달했다[1]. Symantec ISTR report가 보고한 연간 변종 악성코드 수는 해마다 증가하여 2017년 한 해 동안 약 6.6억 개의 변종 악성코드가 등장했다[2]. G Data Software Blog에 따르면 2018년 상반기 출현한 신규 악성코드 유형은 약 2백만 개에 달했다[3]. 악성코드 분석 전문가들의 기존 수동적 분석 방법의 분석속도는 최근 악성코드의 출현 속도보다 현저히 느리기 때문에 기하급수적으로 증가하는 악성코드를 분석하기에는 분석 속도에 대한 한계가 있다. 이러한 기존 방법의 한계를 보완하고 대체하기 위해 최근 기계학습 알고리즘을 활용한 악성코드 탐지 및 분류에 대한 연구가 활발히 진행되고 있다[7].

지도학습 기반의 기계학습 알고리즘은 학습 데이터에 대한 레이블이 필수적이다. 이러한 레이블은 ground-truth가 높을수록 연구 결과의 신뢰성이 높아진다. 기존의 악성코드 분류 연구는 AV 벤더에서 제공하는 악성코드 패밀리명을 레이블로 사용해왔다. AV 벤더는 악성코드의 패밀리정보를 수동적인 접근 방식으로 추출한다. 또한 AV 벤더마다 세분화된 패밀리명의 추출 기준이 다르며, 그 기준이 명확하지 않다. 따라서 단일 AV 벤더의 패밀리명은 일관성과 신뢰성이 낮다[4]. 하지만 레이블링에 사용할 수 있는 정보가 부족한 악성코드 분석 전문가들은 단일 AV 벤더의 레이블에 의존할 수밖에 없다.

기존 연구인 AVclass는 AV 벤더의 레이블들 중에서 가장 가능성 있는 레이블을 투표를 통해 샘플에 지정하였다[4]. 이에 따라 최근 많은 연구들이 이를 활용해 신뢰성을 확보하고 있다. 하지만, 샘플에 단일 레이블만을 지정하기 때문에 지정되지 않은 다른 레이블의 정보는 무시되는 문제가 있다. 뿐만 아니라 최다득표를 한 레이블이 복수일 경우 동일한 두 샘플의 레이블이 서로 다르게 지정될 가능성이 있다. 따라서 레이블링의 신뢰성과 일관성 문제는 완전히 해결되지 않은 상태이다.

본 논문은 기존의 문제를 해결하기 위해 Oh et al. [9] 기반의 unified labeling을 제안한다. AV 벤더의 레이블 중 하나만 지정하는 AVclass와 달리 본 기법은 모든 AV 벤더의 레이블을 통합함으로써 신뢰성과 일관성을 향상시킨다. 이를 통해 높은 ground-truth를 가진 레이블 기반의 분류 연구가 가능할 것으로 기대된다. 본 논문은 real world에서 수집한 5,045개 샘플 데이터 셋으로 연구를 진행하였다. 또한 fine-grained 방식 기반으로 특징을 분석하여 레이블마다 악성 행위 유사성의 신뢰도를 측정했다. 본 논문에서 제안하는 레이블링을 평가하기 위해 단일 AV 벤더에서 제공하는 패밀리명 및 기존 연구의 레이블링과의 비교를 통해 악성코드 레이블의 ground-truth를 검증하였다. 검증 평가를 위해 세 가지 클러스터링 알고리즘을 이용하였다. 결과적으로 기존 기법보다 제안하는 기법을 통한 레이블에서 악성 행위의 유사성 이 더 높게 나타남을 확인하였다.

II. 기반 기술 소개

2.1 Clustering Algorithm

클러스터링 알고리즘은 비지도 학습 기반의 기계학습 알고리즘이며, 이는 레이블이 없이 주어진 샘플의 특성을 이용하여 유형을 군집하는 알고리즘이다. 거리 기반, 계층 기반 등 기반에 따라 클러스터링 알고리즘을 다양하게 적용할 수 있다. Agglomerative clustering은 단일 클러스터를 상향 병합하는 계층 기반 알고리즘이다. K-Means는 클러스터 간 거리 차이의 분산을 최소화하는 거리 기반의 알고리즘이다. Birch clustering은 CF tree를 이용한 통합된 계층 군집화 기법의 알고리즘이다.

2.2 Forward Stepwise Selection Algorithm

기계학습에서 특징 선택은 차원의 저주를 해결하고 과적합의 위험을 줄여줄 뿐만 아니라 훈련 시간을 감소시켜 준다. Forward stepwise selection은 이러한 특징 선택 알고리즘 중 하나이다. 이는 단일 특징 정보들의 정확도를 측정하고, 높은 정확도를 갖는 특징을 특징 조합에 점차 추가시켜 최적의 특징 조합을 찾는 알고리즘이다. 이 알고리즘은 best subset selection 알고리즘과 비교하면 유사한 성능을 보이고 보다 적은 특징을 이용하기 때문에 시간상 효율적이다[8].

III. 시스템 설계

본 연구에서 제안하는 unified labeling의 시스템 개요를 소개한다. 나아가 unified labeling의 ground-truth를 평가하기 위해 forward stepwise selection 알고리즘을 활용하여 fine-grained 특징 분석을 통해 특징 선정 모델을

제안한다.

3.1 Unified labeling 시스템 설계

본 논문에서 제안하는 unified labeling의 시스템 개요는 Fig 1.과 같다. 이는 크게 Parsing phase, Filtering phase, Unifying phase 순으로 구분된다.

Parsing phase는 AV 벤더에서 제공하는 악성코드 샘플의 패밀리명을 파싱한다. 본 연구는 저명한 AV 벤더인 Symantec, AhnLab, Kaspersky에서 제공하는 패밀리명과 Virus total과 cuckoo sandbox를 연동하여 추출한 패밀리명을 활용하였다.

악성코드 패밀리명의 규칙은 AV 벤더마다 다르기 때문에 AV 벤더에 적합한 규칙을 이용하여 토큰을 파싱한다. 파싱은 공통적으로 '@', '!', '.' 등 구분자를 이용하여 토큰을 분류하며, AhnLab의 v3는 추가로 'Win32', 'Win-Trojan', 'Win-PUP', 'Win-95' 등을 구분자로 지정하여 토큰화 작업을 진행한다.

Filtering phase는 제네릭 토큰으로 이루어진 generic list에 파싱된 토큰의 포함 여부를 확인하여 필터링을 한다. 제네릭 토큰은 행위가 다른 악성코드들을 같은 행위로 판단하여 군집하는 위험성을 가진다. 본 연구의 generic list는 'generic', 'agent', 'heur', 'gen', 'gen1', 'worm' 등 13개의 제네릭 토큰이 포함되어 있다.

Unifying phase는 이전 단계를 거친 AV 벤더의 토큰을 하나의 레이블로 통합하는 과정이다. Unifying phase는 기존의 클러스터링 방식의 병합 매커니즘을 활용하지만 numeric한 데이터가 아닌 문자열인 토큰을 이용하여 병합한다. Unifying phase는 Fig 2.와 같이 Setting step, Grouping step 두 가지 단계로 진행한다. 첫 번째 단계인 Setting step에서는 구분자를 '.'으로 지정하여 한 샘플에 대해 제공하는 각 AV 벤더의 토큰들을 하나의 레이블로 병합한다. 또한 병합된 레이블에서 중복 토큰이 존재한다면 중복된 토큰을 제거한다. 이 후 Grouping step 단계에서는 샘플 간 레이블의 토큰이 중복한다면 해당 샘플들을 그룹화하고 레이블을 병합 후에 중복 토큰을 제거한다. Grouping step은 샘플 간 그룹화가 불가능할 때까지 이 단계를 반복한다.

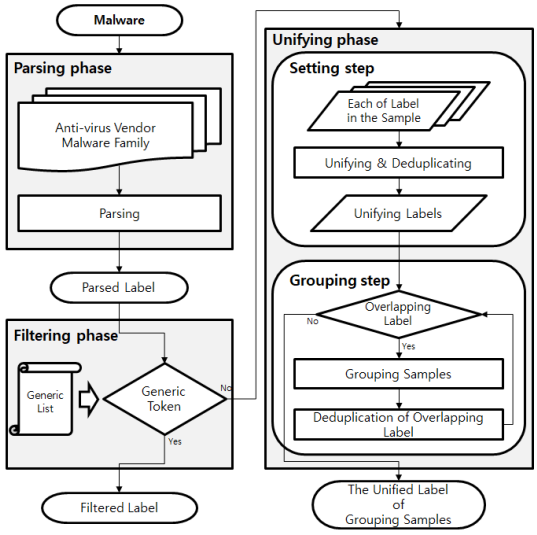


Fig. 1. Unified Labeling System Overview

3.2 특징 선정 시스템 설계

특징 선정 시스템을 통해 unified labeling의 신뢰성을 평가 및 검증한다. 본 연구에서는 agglomerative clustering과 k-means, birch cluster-

Name of Sample	Kaspersky	Symantec	V3	Cuckoo
Sample 1	A	B	A	A
Sample 2	B	B	B	C
Sample 3	D	D	E	F

Setting step

Name of Sample	Label of Setting phase
Sample 1	A.B
Sample 2	B.C
Sample 3	D.E.F

Grouping step

Group Number	Involved label	Involved sample
Group 0	A.B.C	Sample 1, Sample 2
Group 1	D.E.F	Sample 3

Setting step

$Sample_1 = [AV_1, AV_2, AV_3, AV_4]$
...
$Sample_n = [AV_1, AV_2, AV_3, AV_4]$
$SampleSet = \{Sample_1, \dots, Sample_n\}$
For i :=1 to n do
  For j :=1 to 4 do
    IF $AV_j \in genericList$ *then*
      remove AV_j
ELSE
  PASS
ENDIF
JOIN $AV_1, \dots, AV_m$ *of* $Sample_i$ *to '.'*
IF duplication in $Sample_i$ *then*
  deduplicate label in $Sample_i$
ELSE
  PASS
ENDIF

Grouping step

$g = 0$
REPEAT
  create $Group_g$
  FOR i:=1 to n-1 do
    FOR j:=i+1 to n do
      IF $Sample_i \cap Sample_j$ *then*
        append $Sample_{i,j}$ *to* $Group_g$
        deduplicate label in $Group_g$
ELSE
  PASS
ENDIF
$g = g + 1$
UNTIL no duplicate label between Samples

Fig. 2. Detailed Steps in Unifying Phase

ing 3가지 클러스터링 알고리즘을 활용하였다. 또한, 특징 선정에 forward stepwise selection 알고리즘을 이용하였으며, 두 번의 forward stepwise selection 과정을 거친다. 전체적인 특징 선정 시스템의 개요는 Fig 3.와 같다. 카테고리 특징 후보를 이용하여 첫 번째 forward stepwise selection 단계를 진행한다. 이 단계는 optimal feature set과 optimal score를 초기화한다. 초기화 후에 특징 테스트를 한다.

특징 테스트는 클러스터링 알고리즘을 통해 특징들의 f1-score를 산출하여 최적의 특징 조합을 찾는 프로세스이다. 이는 f1-score가 가장 높은 특징 조합을 선정하고 optimal feature set에 추가한다. 이때의 f1-score가 optimal score가 된다. 기존의 feature set에서 optimal feature set에 추가된 특징을 제거한 후 이를 반복한다.

결과적으로 최적의 카테고리 특징 조합을 찾고, 카테고리 특징 조합을 서브 카테고리 특징 후보 조합으로 변환한다.

변환된 서브 카테고리 특징 후보 조합을 활용하여 두 번째 forward stepwise selection을 진행한다. 결과적으로 최적의 서브 카테고리 특징 조합을 찾는다. 이러한 특징 선정 시스템은 모든 서브 카테고리 특징을 후보로 할 필요 없이 첫 번째 특징 선정을 통하여 서브 카테고리 특징 후보를 줄일 수 있다. 이를 통해 시간적인 효율성을 얻을 수 있다. 또한 서브 카테고리 특징 조합은 fine-grained 특징 분석을 통해 얻은 세밀한 악성 행위 특징이 되며, 높은 신뢰성 검증의 필수 요소이다.

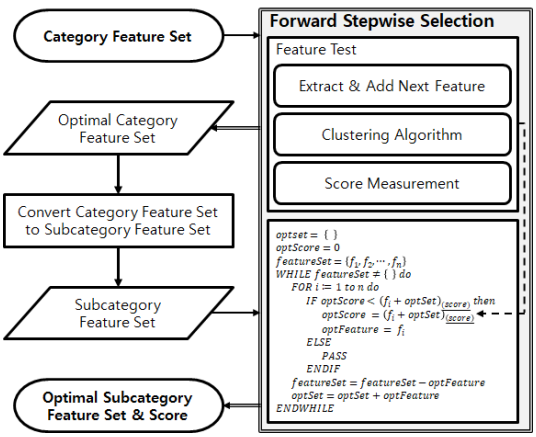


Fig. 3. Feature Selection System Overview

IV. 실험 설계 및 결과

4.1 실험 환경 및 데이터 셋

모든 실험은 Intel (R) Xeon(R) Gold 6134 CPU @ 3.20 GHz, 190 GB RAM and Ubuntu 18.04.1 LTS 환경에서 python 2.7 및 머신러닝 모듈 scikit-learn을 활용하여 실험을 수행했다. 또한, 실험을 위해 Virus total에서 수집한 5,045개의 악성코드 샘플 데이터 셋을 활용하였다.

악성코드 샘플의 특징은 다양한 python의 라이브러리와 cuckoo sandbox를 통해 정적/동적 특징을 추출하였다. 정적 특징 중 opcode는 바이트 시퀀스를 bigram하였고, pesection은 pesection의 섹션 비율을 이용하였다. 동적 특징의 API function은 악성코드 샘플의 첫 번째 프로세스의 API 시퀀스를 bigram하여 활용하였다. 악성코드의 군집화를 위해 모든 악성코드 특징을 후보로 forward stepwise selection 알고리즘에 적용하였다. 활용된 악성코드 특징의 후보는 Table 1.과 같으며 서브 카테고리 특징들은 해당 카테고리 특징에 속한다.

4.2 Unified Labeling

5,045개의 악성코드 샘플의 Unified label을 생성하기 위해 AV 3사와 Cuckoo Sandbox의 패밀리명을 활용하였으며, 각각의 패밀리명 개수는 Symantec 85개, AhnLab 198개, Kaspersky 149개, Cuckoo Sandbox 87개이다. 또한 AVclass [4]을 이용한 결과 106개의 레이블을 생성했다. Unified labeling을 하기 위해서 각 패밀리명을 이용하여 Fig.1의 시스템 흐름에 따라 Setting step을 통해 각 레이블에서 제공하는 패밀리명의 파싱을 통합하여 757개의 레이블을 생성했다. 이후 Grouping step을 통해 그룹을 병합해 최종적으로 41개의 레이블을 생성했다.

4.3 Clustering을 활용한 레이블링 검증 평가

본 연구에서 제안한 unified labeling과 기존 연구 AVclass의 레이블링, 각 AV 벤더 3사, cuckoo sandbox의 레이블의 비교를 위해 agglomerative clustering, k-means, birch clustering 3개의 알고리즘을 활용하였다.

Table 1. Category Feature Set & Subcategory Feature Set

Category	opcode	pesection	compile	api	command	droppedfile	registry	service	mutex
Subcategory	opcode	pesection	compile	api	command	name, size, ssdeep	access, delete, read, write	created, started	mutex
Category	network								
Subcategory	host, dnsAnswer, dnsRequest, dnsType, domainIP, domainName, icmpdst, icmpsrc, icmptype, pcapSHA256, pcapSorted, udpDstIP, udpDstPort, udpOffset, udpSrcIP, udpSrcPort, udpTime								

각 레이블링 방법에 따른 precision과 recall은 Table 2.와 같으며 이를 통해 산출한 f1-score는 Fig 4.와 같다. 최적의 서브 카테고리 특징 조합 관점에서 기존의 AVclass는 단일 AV 벤더 레이블에 비해 f1-score의 근소한 향상을 보였다. 반면 최적의 카테고리 특징 조합 관점에서 AVclass의 agglomerative clustering의 f1-score는 Kaspersky에 비해 1.67% 낮았고, birch clustering의 f1-score는 Kaspersky와 Cuckoo에 비해 각각 1.7%, 0.35% 낮았다. 이는 AVclass가 기반에 따른 클러스터링 알고리즘에 유연하지 못하다는 것을 뜻한다. 또한 전체적으로 AVclass 레이블과 단일 AV 벤더의 레이블의 f1-score는 모든 알고리즘과 특징 조합에 대해 80%에 미치지 못했다.

첫 번째 특징 선정 단계에서 카테고리 특징 조합을 후보로 최적의 카테고리 특징 조합을 선정하였고, 이를 이용한 unified label의 성능 측정 결과는 k-means와 agglomerative clustering, birch clustering의 f1-score가 각각 89.02%, 88.66%, 88.66%였다. 이 중 가장 높은 성능을 보인 k-means의 최적의 카테고리 특징 조합은 'mutex', 'service', 'compile', 'api', 'network', 'registry', 'droppedfile', 'command' 이였다.

Table 2. Clustering Algorithm Results

Alg.	Type of Label	Category Feature Set		Sub Category Feature Set	
		Pre.	Rec.	Pre.	Rec.
K.C.	Symantec	78.00%	65.26%	75.41%	68.59%
	V3	76.65%	70.88%	85.27%	70.74%
	Kaspersky	81.97%	70.28%	82.87%	70.91%
	Cuckoo	82.08%	67.01%	87.14%	66.49%
	AVclass	86.12%	70.85%	85.99%	70.75%
	Unified Label	**96.06%**	**82.93%**	**95.85%**	**87.59%**
A.C.	Symantec	76.23%	67.69%	76.23%	67.69%
	V3	79.96%	70.52%	83.38%	75.39%
	Kaspersky	83.41%	71.84%	83.41%	71.84%
	Cuckoo	86.05%	66.99%	86.05%	66.99%
	AVclass	83.07%	69.23%	88.48%	72.69%
	Unified Label	**97.88%**	**81.02%**	**96.01%**	**83.31%**
B.C.	Symantec	76.65%	64.53%	85.56%	65.15%
	V3	79.96%	70.52%	80.75%	75.19%
	Kaspersky	82.47%	72.96%	82.48%	72.96%
	Cuckoo	82.41%	70.64%	82.77%	71.36%
	AVclass	83.11%	69.55%	88.04%	71.42%
	Unified Label	**97.88%**	**81.02%**	**96.91%**	**83.41%**

Alg.: Algorithms, Pre.: Precision, Rec.: Recall
K.C.: K-means clustering, A.C.: Agglomerative clustering, B.C.: Birch clustering

두 번째 특징 선정 단계에서는 첫 번째 특징 선정 단계에서 얻은 최적의 카테고리 특징 조합을 서브 카테고리 특징 조합 후보로 변환하여 최적의 서브 카테고리 특징 조합을 선정하였다. 이를 이용한 unified label의 성능 측정 결과는 k-means와 agglomerative clustering, birch clustering의 f1-score가 각각 91.53%, 89.21%, 89.66%였다. 이 중 가장 높은 성능을 보인 k-means의 최적의 서브 카테고리 특징 조합은 'dnsType', 'mutex', 'icmpsrc', 'pcapSorted', 'udpSrcPort', 'icmpdst', 'udpSrcIP' 였다.

종합적으로 unified label의 모든 클러스터링 알고리즘의 f1-score는 타 레이블에 비해 약 10% 이상 높은 성능을 보임으로써 다양한 클러스터링 알고리즘에서 보다 유연함을 확인하였다.

Unified label이 가장 높은 성능을 보인 k-means의 경우 최적의 서브 카테고리 특징 조합은 최적의 카테고리 특징 조합에 비해 f1-score가 약 2.5% 증가하였다. 이외에도 agglomerative clustering과 birch clustering에서 각각 0.55%, 1% 증가하였다. 이는 최적의 카테고리 특징 조합보다 fine-grained 기반의 특징 분석을 통한 최적의 서브 카테고리 특징 조합이 그룹 내 악성 행위의 유사도와 레이블링의 신뢰도를 더욱 향상했음을 나타낸다.

V. 관련 연구

레이블의 높은 ground-truth을 위해 레이블링 관련 연구와 레이블링에 대한 평가 검증 관련 연구가 많이 진행되고 있다.

Sebastian et al. [4]는 AV 벤더가 제공하는 패밀리명을 이용하여 악성코드 레이블을 추출하는 AVclass를 개발하였다. AVClass는 AV 벤더의 패

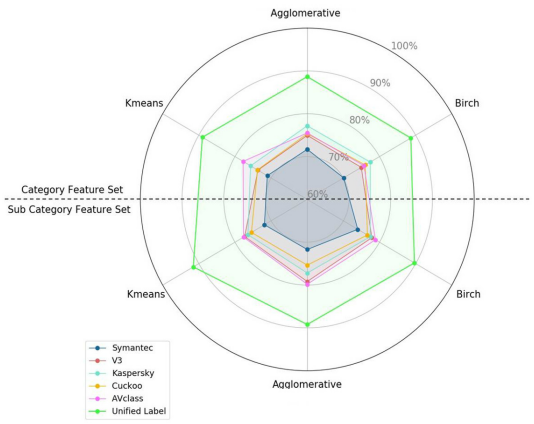


Fig. 4. F1-score results of Clustering Algorithms

밀리명을 처리하기 위해 정규화, 일반 토큰 제거, 별칭 탐지 단계를 진행하여 가장 득표수가 많은 레이블 하나를 선택하여 악성코드 샘플에 지정하였다. 하지만, 레이블의 득표수가 동표가 나올 경우에 하나의 레이블을 선택하기 때문에 악성코드 레이블의 유사한 악성 행위를 파악하기에 한계가 있다. Kantchellian et al. [5]은 AV 벤더가 제공하는 패밀리명을 가중치 할당을 통해 신뢰성 있는 레이블링 방법을 제안했다. 이 연구는 낮은 false positive 보였지만, 높은 false negative에 대한 한계가 있다. 즉, recall의 성능이 비교적 낮다는 것을 나타낸다. Hurier et al. [6]은 ground truth를 평가하기 위해 정량적인 방법을 이용한 새로운 측정 기준을 제안했다. 하지만 레이블이 정규화되지 않았으며, 악성코드 샘플에 레이블 지정 한계가 있다.

본 논문은 단일 패밀리명이 아닌 AV 벤더에서 제공하는 다양한 패밀리명을 정규화 및 통합하여 레이블링하였다. 이를 통해 일관성 문제를 해결하였으며, precision뿐만 아니라 recall 성능도 향상했다.

본 논문은 fine-grained 검증 기법을 통해 보다 세밀한 행위 특징을 분석하였고, 다양한 기반의 클러스터링 알고리즘을 통해 신뢰도 평가 검증을 하였다. 이를 통해 기존 기법 대비 그룹 별 악성 행위 유사도를 향상시킬 수 있었다.

VI. 결 론

본 연구는 ground-truth가 높은 레이블을 만들기 위해서 새로운 레이블링 기법인 unified labeling을 제안했다. 이를 통해 지도학습 기반의 기계학습알고리즘을 활용할 때 발생하는 학습 데이터 셋 레이블의 신뢰성 저하에 대한 문제를 해결할 수 있다. 또한 fine-grained 분석 기법을 활용함으로써 최적의 서브카테고리 특징 조합을 찾았고 이를 통해 악성 행위의 유사성에 대한 결과도 더 높게 나왔다.

한편, 본 논문에서 사용한 단일 AV 벤더의 레이블을 통한 unified label의 더 이상의 성능 향상은 한계가 있었다. 신뢰도가 높은 단일 AV 벤더를 다수 선별하여 레이블을 재구성하면 보다 향상된 성능을 기대할 수 있다. 또한, 기준이 명확하지 않은 과도한 세분화는 악성 행위가 유사한 샘플에 대한 재현율이 낮다. 하지만 패밀리 분류를 위해서는 명확한 기준을 통한 적당한 세분화가 필요하다. Unified labeling의 통합 기준을 바꾼다면 보다 세분화된 레이블링이 가능하다. 마지막으로, fine-grained 방식으로 얻어낸 데이터 셋 단위의 특징 조합뿐만 아니라 각 악성코드 그룹의 악성 행위 특징을 조합을 fine-grained 방식으로 찾을 수 있을 것으로 기대한다.

References

[1] Kaspersky, “Overall Statistics For 2017”, https://securelist.com/ksb-overall-statistics-2017/83453, Dec. 2018

[2] Symantec, “Internet Security Threat Report (ISTR)”, https://www. symantec.com/security-center/threat-report, Dec, 2018

[3] G DATA SECURITY BLOG, https://www.gdatasoftware.com/blog, Dec, 2018

[4] Sebastián, Marcos, et al. ″Avclass: A tool for massive malware labeling.″ International Symposium on Research in Attacks, Intrusions, and Defenses. Springer, pp. 230-253, Sep. 2016.

[5] Kantchelian, Alex, et al. ″Better malware ground truth: Techniques for weighting anti-virus vendor labels.″ Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security. pp. 45-56, Oct. 2015.

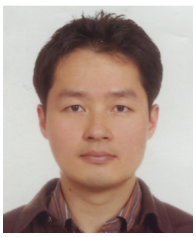
[6] Hurier, Médéric, et al. ″On the lack of consensus in anti-virus decisions: Metrics and insights on building

ground truths of android malware." International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment(DIMVA). pp.142-162, Jul. 2016.
〔7〕 Li, Jin, et al. "Significant Permission Identification for Machine Learning Based Android Malware Detection." IEEE Transactions on Industrial Informatics, 14(7), pp.3216-3225, Jan. 2018.
〔8〕 M Ahmadi, D. Ulyanov, S. Semenov, M. Trofimov, and G. Giacinto. "Novel feature extraction, selection and fusion for effective malware family classification," In Proc. Data and Application Security and Privacy (CODASPY), pp. 183 - 194, Mar. 2016.
〔9〕 Oh Sangjin, Park Laehyun, Park Jun-hyung and Kwon Taekyoung, "A Study of Labeling for Ground-Truth of Malware Family Names." Conference on Information Security and Cryptography-Winter, pp 66-69, Dec. 2018.

〈저자소개〉

오 상 진 (Sang jin Oh) 학생회원
2018년 2월: 을지대학교 의료IT마케팅학과 졸업
2018년 3월~현재: 연세대학교 정보보호 연구실 석사 과정
〈관심분야〉 정보보호, 악성코드 탐지, 기계학습, Adversarial Machine Learning 등

박 래 현 (Leo Hyun Park) 학생회원
2017년 2월: 광운대학교 컴퓨터공학 졸업
2017년 3월~현재: 연세대학교 정보보호 연구실 통합 과정
〈관심분야〉 악성코드 탐지, 유저블 시큐리티, 기계학습, Adversarial Machine Learning 등



권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년~2000년: U.C. Berkely Post-Doc
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년: Univ. Maryland at College Park 교환 교수
2013년 9월~현재: 연세대학교 정보대학원 교수
〈관심분야〉 암호 프로토콜, 인증, 유저블 시큐리티, 사물인터넷 보안, 소프트웨어 보안, 펌웨어 보안 등