J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

공격자 그룹 특징 추출 프레임워크 : 악성코드 저자 그룹 식별을 위한 유전 알고리즘 기반 저자 클러스터링☆

The attacker group feature extraction framework : Authorship Clustering based on Genetic Algorithm for Malware Authorship Group Identification

신 건 윤[1] 김 동 욱[1] 한 명 묵[1]*
Gun-Yoon Shin Dong-Wook Kim Myung-Mook Han

요 약

최근 악성코드를 활용한 APT(Advanced Persistent Threat) 공격의 수가 점차 증가하면서 이를 예방하고 탐지하기 위한 연구가 활발히 진행되고 있다. 이러한 공격들은 공격이 발생하기 전에 탐지하고 차단하는 것도 중요하지만, 발생 공격 사례 또는 공격 유형에 대한 정확한 분석과 공격 분류를 통해 효과적인 대응을 하는 것 또한 중요하며, 이러한 대응은 해당 공격의 공격 그룹을 분석함으로써 정할 수 있다. 따라서 본 논문에서는 공격자 그룹의 특징을 파악하고 분석하기 위한 악성코드를 활용한 유전 알고리즘 기반 공격자 그룹 특징 추출 프레임워크를 제안한다. 해당 프레임워크에서는 수집된 악성코드를 디컴파일러와 디셈블러를 통해 관련 코드를 추출하고 코드 분석을 통해 저자와 관련된 정보들을 분석한다. 악성코드에는 해당 코드만이 가지고 있는 고유한 특징들이 존재하며, 이러한 특징들은 곧 해당 악성코드의 작성자 또는 공격자 그룹을 식별할 수 있는 특징이라고 할 수 있다. 따라서 우리는 저자 클러스터링 방법을 통해 바이너리 및 소스 코드에서 추출한 다양한 특징들 중에 특정 악성코드 작성자 그룹만이 가지고 있는 특징들을 선별하고, 정확한 클러스터링 수행을 위해 유전 알고리즘을 적용하여 주요 특징들을 유추한다. 또한 각 악성코드 저자 그룹들이 가지고 있는 특성들을 기반으로 각 그룹들만을 표현할 수 있는 특징들을 찾고 이를 통해 프로필을 작성하여 작성자 그룹이 정확하게 군집화 되었는지 확인한다. 본 논문에서는 실험을 통해 유전 알고리즘을 활용하여 저자가 정확히 식별되는 지와 유전 알고리즘을 활용하여 주요 특징 식별이 가능한지를 확인 할 것이다. 실험 결과, 86%의 저자 분류 정확도를 보이는 것을 확인하였고 유전 알고리즘을 통해 추출된 정보들 중에 저자 분석에 사용될 특징들을 선별하였다.

☞ 주제어 : 저자 특성, 공격자 그룹, 유전 알고리즘, 악성코드, 저자 클러스터링

ABSTRACT

Recently, the number of APT(Advanced Persistent Threats) attack using malware has been increasing, and research is underway to prevent and detect them. While it is important to detect and block attacks before they occur, it is also important to make an effective response through an accurate analysis for attack case and attack type, these respond which can be determined by analyzing the attack group of such attacks. Therefore, this paper propose a framework based on genetic algorithm for analyzing malware and understanding attacker group's features. The framework uses decompiler and disassembler to extract related code in collected malware, and analyzes information related to author through code analysis. Malware has unique characteristics that only it has, which can be said to be features that can identify the author or attacker groups of that malware. So, we select specific features only having attack group among the various features extracted from binary and source code through the authorship clustering method, and apply genetic algorithm to accurate clustering to infer specific features. Also, we find features which based on characteristics each group of malware authors has that can express each group, and create profiles to verify that the group of authors is correctly clustered. In this paper, we do experiment about author classification using genetic algorithm and finding specific features to express author characteristic. In experiment result, we identified an author classification accuracy of 86% and selected features to be used for authorship analysis among the information extracted through genetic algorithm.

☞ keyword : Authorship Attribution, Attacker Group, Genetic Algorithm, Malware, Authorship Clustering

[1] Graduate School of IT Convergence Engineering Dept., Gachon University, Seongnam, 13120, Korea.
* Corresponding Author(mmhan@gachon.ac.kr)
[Received 30 October 2019, Reviewed 11 November 2019(R2 26 December 2019), Accepted 3 January 2020]

☆ 이 논문은 2019년도 한국인터넷정보학회 춘계학술대회 우수 논문 추천에 따라 확장 및 수정된 논문임.
☆ 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2018R1D1A1B07050864).

1. 서 론

인터넷의 발달로 인하여 사회 전반적으로 다양한 정보들을 인터넷을 통해 빠르게 주고받고 있으며, 이러한 기술들은 다양한 산업, 기업 및 국가에서 사용되고 있고, 어떤 분야를 막론하든지 간에 인터넷이 사용되지 않는 곳이 없을 정도로 현재 보급되어 있다. 하지만 인터넷을 통해 정보를 주고받는 다는 것은 항상 보안에 대한 위협을 가지고 있다는 것을 의미하며, 실제로 인터넷 환경을 활용한 공격의 수가 점차 증가하고 있다[1].

대표적인 예로 APT 공격을 들 수 있으며, 해당 공격은 특정 프로그램 혹은 특정 시스템에 대한 취약점을 분석하고 공격을 통해 정보를 탈취하거나 시스템을 마비시키는 등의 공격을 수행한다. 또한 APT 공격에서는 악성코드들이 주로 사용되며, 이를 통해 시스템 등을 장악하고 정보를 탈취한다. 해당 공격 방식은 짧은 시간에 이루어지는 것이 아닌, 취약점을 찾고 침투 경로를 설정하는 등의 긴 시간을 두고 수행하는 공격 방식이기 때문에 공격자들은 자신들이 주로 사용하는 악성코드 종류, 공격 방식, 침입 루트, 타겟 정보 분석 방식 등을 가지고 있다. 따라서 인터넷에 존재하는 공격자와 관련된 이러한 정보들을 정확히 분석하고 식별하면 공격에 대한 피해를 좀 더 줄일 수 있을 것이다.

본 논문에서는 최근 자주 발생하는 공격들에 대한 공격자나 공격 그룹의 정보를 분석하고 식별하기 위하여 그들이 사용하는 악성코드를 분석할 것이다. 해당 악성코드를 분석하게 되면, 악성코드 공격자들이 가지고 있는 고유한 특징들을 식별할 수 있다[2]. 이를 통해 악성코드 공격자 혹은 유포자들을 그룹화 할 수 있는 정보를 얻을 수 있으며, 이는 곧 공격자 및 유포자가 가지고 있는 고유한 특징을 식별하는 것을 의미한다. 이처럼 악성코드 공격자 혹은 작성자를 식별할 수 있는 고유 특징들은 악성코드를 디컴파일러 및 디셈블러를 통해 얻은 바이너리 코드와 소스 코드 등을 통해 얻을 수 있으며, 관련 특징들로는 N-gram, PE, Opcode, 패킹, 파일 구조, 함수, 레지스터, idiom, graphlet, super graphlet, call graphlet, N-gram, 단어 빈도, 어휘 표현력 등이 있다.

이러한 특징들을 중에서 악성코드 공격자 그룹이 가지고 있는 고유한 특징을 식별하고 해당 그룹만이 가지고 있는 특별한 특징(정보)들을 파악한다. 또한 파악된 악성코드 공격자 그룹의 고유 특징들을 가지고 그룹 프로파일을 생성하여 새로운 악성코드 분석을 수행할 때, 어떠한 유형의 그룹에 속하는 지도 확인 할 것이다.

따라서 본 논문에서는 유전 알고리즘 기반 악성코드 공격자 그룹 특징 추출 프레임워크를 제안한다. 해당 프레임워크를 통해 악성코드의 바이너리 및 소스 코드 등을 추출하고 해당 코드에서 저자와 관련된 정보를 추출한다. 그리고 추출된 정보들을 가지고 클러스터링을 통한 공격자 그룹을 생성하고 각 그룹마다 가지고 있는 특별한 특정(정보)들을 파악한다. 또한 파악된 정보를 가지고 그룹 프로파일을 생성하여, 새로운 악성코드가 유입되었을 때 해당 악성코드가 어떠한 유형의 공격에 속하는 지 혹은 어떤 공격자 그룹에 속하는 지를 파악하여 능동적인 보안 대책 선정과 신속한 대응이 가능하도록 할 것이며, 그룹별 고유 특징들을 통해 그룹 클러스터링 정확도를 향상시킬 것이다[3].

논문의 순서는 다음과 같다. 2장에서는 Authorship Attribution과 유전 알고리즘에 대해서 소개하며, 3장에서는 제안하는 악성코드 공격자 그룹 식별을 위한 유전 알고리즘 기반 특징 추출 프레임워크에 대해 소개한다. 4장에서는 관련 연구를 수행하며, 5장에서 결론을 내린다.

2. 관련 연구

2.1 Authorship Attribution

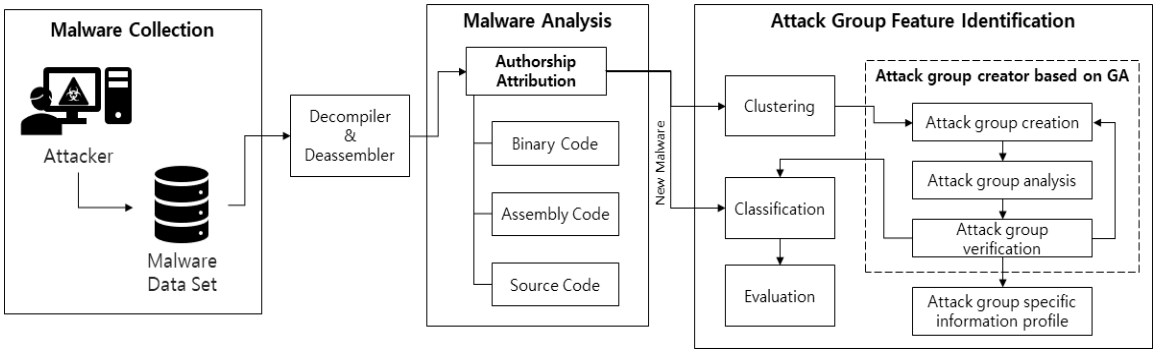
Authorship Attribution은 바이너리, 어셈블리어 및 소스 코드와 같은 프로그램 코드들이나 워드, 한글, 액셀 등과 같은 문서들을 분석하여 코드나 문서 안에 존재하는 저자를 유추할 수 있는 정보들을 찾아내는 방법을 의미한다. 분석을 통해 작성자의 특성을 파악하거나 프로필을 생성하기도 하며, 크게 3가지 방법으로 나뉜다[4][5].

2.1.1 Authorship Identification

특정한 저자에 의해 작성된 여러 코드, 메시지 혹은 문서 등을 분석하여 작성자의 특징을 식별하는 방식을 의미하며, 이를 통해 특정 저자를 식별할 수 있는 특징들을 선별한다. 새로 분석하는 문서에서 특징들을 추출하고 비교 분석하는 방법을 주로 사용한다.

2.1.2 Authorship Characterization

특정한 저자의 특성을 파악하고, 해당 저자만을 식별할 수 있는 특징들을 찾아 저자의 프로필을 만드는 방법을 의미하며, 저자의 성별, 프로그램 언어 교육 수준, 문



(그림 1) 유전 알고리즘 기반 악성코드 공격자 그룹 특징 추출 프레임워크
(Figure 1) Malware Attacker group feature extraction framework based on Genetic Algorithm

화, 배경지식 등을 기반으로 프로필을 작성한다.

2.1.3 Similarity Detection

다양한 코드나 메시지를 분석 및 비교하여 각 문서별 유사도를 측정하는 방식으로 모방이 아닌 한 저자에 의해서 작성되었는지를 확인하는 방법을 말한다. 어휘, 기능, 구문 특징, 내용 등을 가지고 특징들을 추출한다. 주로 저작권과 관련된 문제를 해결하고자 할 때 사용한다.

Authorship Attribution에 사용되는 특징들로는 어휘적, 문자적, 구문록적, 의미론적 특징들이 있으며, N-gram, 토큰, 빈도수 등의 방법을 적용하여 관련 특징을 추출한다. 이는 일반적인 문서뿐만 아니라, 바이너리 코드, 소스 코드 및 어셈블리 코드 등과 같은 유형의 문서에도 사용할 수 있으며, 코드에서는 추가적으로 코드만이 가지고 있는 정보들(데이터, 프로그램 언어적 특징, 코드 흐름 등)을 가지고 특징을 생성한다.

2.2 Genetic Algorithm

유전 알고리즘은 생물의 유전학적 진화 메커니즘을 기반으로 한 공학 모델로 최적화 탐색 문제에 적합한 알고리즘이다. 유전 진화를 모델로 사용하였기 때문에 유전자 돌연변이(mutation), 선택(selection), 교차(crossover) 등의 방법이 적용된다[6].

특정 문제를 해결하기 위한 최적의 해를 찾기 위해 사용하며, 일반적으로 해를 염색체(chromosome)으로 나타낸다. 일반적으로 염색체를 이진수로 표현하나, 이는 어떠한 문제를 해결하느냐에 따라 다양한 표현방법이 존재한다. 또한 각 염색체들이 특정 문제에 대해서 얼마만큼의 가치(value)를 가지고 있는지를 적합 함수(fitness function)을 통해 평가한다[7][8].

유전 알고리즘은 보통 지역 최적화(local optimization)에 사용되며, 특징 공간에서 일부 지역에 대한 최적화를 수행하여 여러 개의 최적화된 해를 산출하지만 해당 값들이 전체 특징 공간에서의 최적의 값이라고 정의할 수 없다. 따라서 유전 알고리즘과 추가적으로 전역 최적화(global optimization) 알고리즘을 사용하여 최적의 해를 찾는 것이 좋다.

염색체 선택 방식에는 룰렛휠, 토너먼트, 순위 기반 선택 등이 있으며, 교차 방식에는 일점, 다점, 균등, 싸이클, PMX 교차 등이 있고, 변이 방식에는 전형적, 비 균등 변이 등의 방식이 존재한다. 다양한 방식들 중에서 특정 문제에 맞는 방식을 선택하여 유전 알고리즘을 구성해야한다.

3. 악성코드 공격자 특징 추출 프레임워크

본 논문에서는 authorship attribution과 유전 알고리즘 기반 악성코드 공격자 식별을 위한 공격자 특징 추출 프래임워크를 제안한다. 제안 하는 프레임워크는 그림 1과 같으며, 4가지 단계(악성코드 수집, 악성코드 분석, 악성코드 공격 그룹 클러스터링, 평가)를 거쳐 진행되고, 이와 관련된 상세한 내용은 다음과 같다.

먼저 악성코드 수집 단계에서는 실제 필드에서 발생하는 악성코드들을 수집하고, 악성코드 데이터 셋에 저장한다. 그리고 두 번째 단계인 악성코드 분석에서는 디컴파일러와 디셈블러를 통해 수집된 악성코드로부터 관련 코드들(바이너리, 어셈블리, 소스 코드 등)을 추출한다. 그리고 Authorship Attribution 기반의 악성코드 분석을 통해

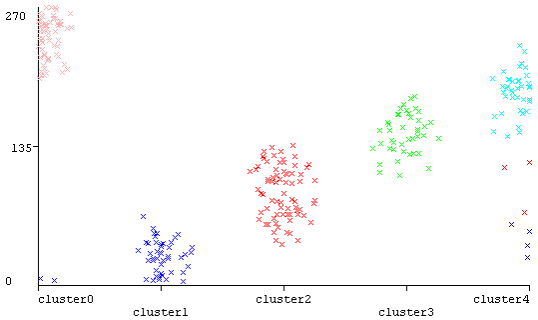
서 저자와 관련된 함수, 레지스터, idiom, graphlet, super graphlet, call graphlet, N-gram, 단어 빈도 등과 같은 특징들을 추출하고, 데이터 셋을 구축한다. Authorship Attribution을 통한 작성자 분석에서 사용하는 바이너리, 소스, 어셈블리 등과 같은 코드부분이 악성코드 분석에 사용되는 코드가 동일하기 때문에 이를 통한 악성코드 분석이 가능하며[9], 해당 방식은 일반적으로 악성코드 탐지 및 분석을 수행하기 위해 분석하는 것보다 다양한 측면에서 악성코드를 분석하기 때문에 보다 다양한 특징들이 추출되고, 이러한 특징들 중에는 악성코드의 공격자, 저자 혹은 유포자와 관련된 특징들이 존재한다[10]. 그 다음 악성코드 공격 그룹 클러스터링 단계에서는 유전 알고리즘을 적용하여 악성코드 공격 그룹 분류를 위한 특징들을 선별하고, 선별된 특징들을 가지고 클러스터링을 수행한다. 이때, 각각의 악성코드 그룹이 가지고 있는 특별한 특징(정보)를 식별하게 되고 이를 기반으로 악성코드 공격 그룹 프로필을 생성하게 된다. 또한 유전 알고리즘 기반의 클러스터링 방식을 적용함으로써 식별되지 않은 그룹의 수를 유추하고 이를 통한 군집화 정확도 향상에 기여한다[11]. 그 후, 유전 알고리즘을 통해 선별한 악성코드 공격 그룹 분류에 유효한 특징들을 가지고 분류(classification)에 적용하여 실제로 악성코드 공격 그룹 분류에 효과적인지를 확인한다.

4. 실 험

본 장에서는 앞서 제안한 프레임워크를 검증하기 위한 연구를 진행하며, 악성코드 공격자 그룹으로 넘어가기 이전 단계인 정상 실행파일 데이터 셋을 가지고 연구 수행한다. 이를 통해 본 논문에서 제안한 Authorship Attribution 기반 저자 특징들과 유전 알고리즘을 활용한 코드 저자 식별에 알맞은 특징을 선택하는 지에 대해서 확인하고, 관련 연구들과의 비교 분석을 수행한다.

연구에 사용한 데이터 셋은 Google Gode Jam[12]을 통해 수집한 코드를 사용하였으며, 이를 실행파일로 변형한 후에 디컴파일러와 디셈블러를 사용하여 여러 코드들을 수집하였다. 실험에 사용된 데이터 셋은 총 5명의 저자로 구성되어 있으며, 저자마다 평균 50개 이상의 실행파일을 가지고 있다. 해당 데이터 셋을 통해 추출한 특징은 총 12개의 특징으로 실행 파일에 디컴파일러 및 디셈블러를 적용하여 해당 특징들을 추출하였다. 실험 환경으로 CPU는 Intel Core i7-8700 3.20GHz, RAM은 16.0 GB, OS는 Window 10 64bit를 사용하였다.

먼저 클러스터링 알고리즘을 통해 각 실행파일마다 어떠한 라벨에 속하는 지를 확인하였다. 그림 2는 해당 연구에 대한 실험 결과로, X축은 클러스터링을 통해 산출한 클러스터를 의미하고 Y축은 실행파일의 번호를 의미한다. 즉, Y축은 데이터 셋에 포함된 실행파일의 수를 나타낸다고 볼 수 있다. 또한 표현된 색은 실행파일의 실제 라벨을 나타낸 것이다. 그림에서 보이는 바와 같이 대체적으로 클러스터마다 하나의 저자만이 포함되어있는 것을 확인할 수 있다. 따라서 authorship attribution을 가지고 추출한 특징들이 실행파일의 저자를 분석하고 분류하는데 있어 사용될 수 있다는 것을 확인할 수 있었다.



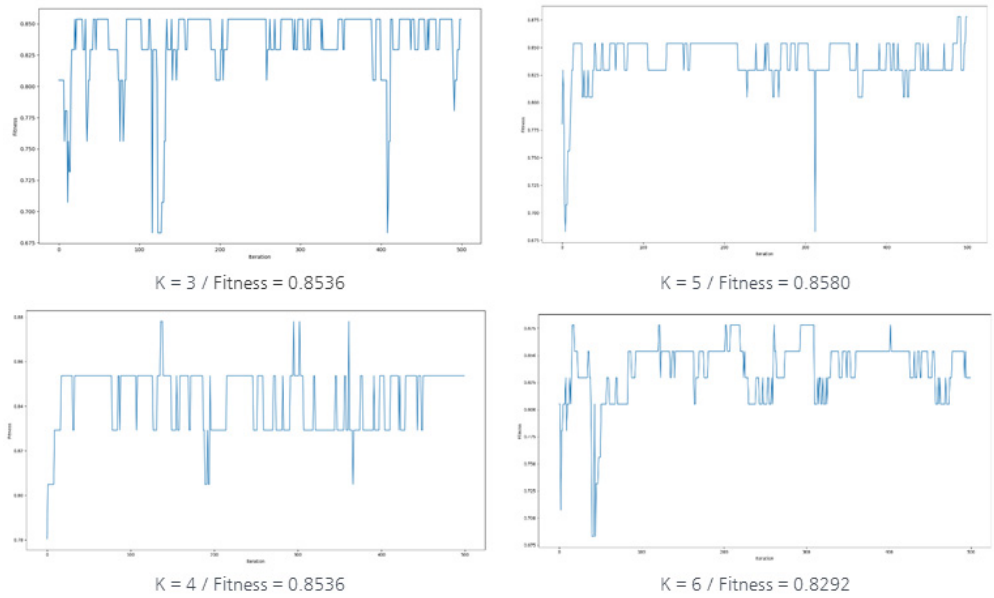
(그림 2) Authorship Attribution 기반 특징 데이터 분포 확인 결과

(Figure 2) Result of feature data distribution based on Authorship Attribution

4.1 염색체 다양성 확보를 위한 염색체 선택 방법 연구

유전 알고리즘의 경우 적합 함수는 저자 식별 정확도를 사용하였다. 그리고 각각의 개별 특징을 하나의 유전으로 설정하고, 염색체의 특정 유전자의 값이 0이면 해당 특징을 사용하지 않고 1이면 해당 특징을 사용하였다. 선택은 룰렛 휠 방법을 적용하였고, 변이는 다중 포인트(multi-point) 방법을 적용하였다. 룰렛 휠 선택 방식은 대표적인 선택 방식 중 하나로, 적합 함수를 통해 각 염색체의 적합 함수 결과값을 산출하고 결과값이 좋을수록 선택될 확률을 높게 하는 방식이다. 룰렛 휠 선택은 식 (1)과 같이 표현할 수 있다.

$$f_i = (C_w - C_i) + \frac{(C_w - C_b)}{(k-1)}, \quad k > 1 \qquad (1)$$



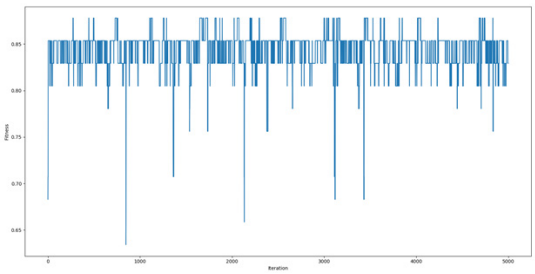
(그림 3) k값에 따른 룰렛 휠 선택 방식의 적합 함수 결과값
(Figure 3) The fitness function result of roulette wheel approach according to k value

C_w는 한 세대에서 가장 좋지 않은 적합 함수 결과값을 나타내고 C_b는 한 세대에서 가장 좋은 적합 함수 결과값을 나타낸다. C_i는 i번째 염색체의 적합 함수 결과값을 나타낸다. 일반적으로 k의 값이 증가하면 selection pressure가 증가하며, 염색체 다양성에 문제가 생기게 된다. 일반적으로 k값은 3~4사이의 값을 가지며, 데이터 셋에 맞는 최적의 k값을 찾아야 염색체 다양성을 확보할 수 있다.

본 연구에서는 최적의 k값을 산출하기위해 k의 값을 1씩 증가시키면서 유전 알고리즘을 수행하였으며, 세대별 염색체 수는 50으로 설정하였다. 그리고 구조는 안전 상태(steady-state) 유전 알고리즘을 적용하였다. 그림 3은 이에 대한 결과로 X축은 적합 함수 결과값을 의미하고, X축은 반복한 세대 수를 의미한다. 해당 실험에서는 최대 500 세대까지 반복하였으며, 실험 결과 k의 값이 5일 때 가장 좋은 저자 식별 정확도를 보인다는 것을 확인 할 수 있었다.

4.2 저자 그룹 분류에 유용한 특징 선택 연구

해당 연구에서는 앞선 연구와는 다르게 세대는 수렴이 될 때까지 최대 5,000세대를 반복하였다. 실험 결과 최종적으로 0.8670의 저자 식별 정확도에서 수렴하는 것이 나타났으며, 5,000세대를 반복하면서 나타난 결과는 그림 4와 같다. X축은 반복된 세대 수를 의미하며 1,000세대를 단위로 표현하였으며 최대 5,000세대를 반복하였다. Y축은 해당 세대에서의 최대 적합 함수 결과값을 나타낸다.



(그림 4) 유용한 특징 선택 실험 결과
(Figure 4) Experiment Result of useful feature selection

약 100세대를 거친 후부터 0.8670의 최대 적합 함수 결과값을 가진다는 것을 확인할 수 있다. 추가적으로 유전 알고리즘을 통해 산출한 저자 식별에 유용한 특징 부분 집합을 확인하였으며, 연구 결과 염색체 배열이 (1,1,0,1,1,

1,1,1,1,1,1,0,0)과 같을 때, 가장 높은 저자 식별 정확도를 보인다는 것을 확인하였으며, 즉 12개의 유전자 중에서 3, 11, 12번째 유전자를 제외한 나머지 특징들은 저자를 식별하는데 유용하다는 것을 확인할 수 있었다.

4.3 관련 연구 비교 분석

본 연구에서는 이전에 연구된 논문들[2][5]과의 비교를 통해 본 프레임워크에 대한 평가를 수행하였다. 비교 결과는 표 1과 같으며, Alrabaee et al[2]에서는 Authorship Attribution 방법을 적용한 저자 식별을 위한 OBA2 프레임워크를 제안하였으며, Google Gode Jam[12]을 통해 수집한 데이터 셋을 사용하였다. 해당 연구에서는 저자의 수를 늘려가면서 정확도를 측정하였으며, 본 연구와 같이 저자가 5명일 때, 약 84%의 저자 분류 정확도를 보였다. Rosenblum et al[5]에서도 마찬가지로 Authorhsip Attribution 기반 소스 코드 및 바이너리 특징들을 추출하여 저자를 식별하는 연구를 수행하였으며, 연구 결과 약 77%의 저자 분류 정확도를 보인 것을 확인할 수 있었다. 이를 통해 본 연구에서 제안한 방식이 기존에 제안한 방법들보다 저자를 식별하는데 있어서 높은 정확도를 보인다는 것을 확인할 수 있었다.

(표 1) Alrabaee et al(2) and Rosenblum et al(5)과의 authorship attribution 정확도 비교 결과
(Table 1) Accuracy comparison results of authorship attribution obtained by Alrabaee et al(2) and Rosenblum et al(5)

System	number of author	accuracy
Alrabaee et al[2]	5+	84%
Rosenblum et al[5]	50+	78%
Our proposed Framwork	5	86%

5. 결 론

본 연구에서는 악성코드 공격 그룹과 관련된 특징을 추출하기 위한 프레임워크를 제안하였다. 해당 프레임워크를 통해서 디컴파일러와 디셈블러를 사용하여 악성코드 혹은 실행파일에 대한 코드 데이터를 추출하고 이를 바탕으로 Authorship Attribution 기반 특징들을 생성한다. 생성된 특징들을 가지고 클러스터링을 수행하여, 악성코드 공격 그룹이 정확히 식별되는지 확인한다. 그리고나서 유전 알고리즘 기반 공격 그룹 생성기를 통해 나눠진 클러스터마다 분석을 수행하여, 각각의 클러스터가 가지고 있는 특성을 파악한다. 이를 통해 각 악성코드 그룹이 가지고 있는, 그룹을 나타내고 표현할 수 있는 특징들을 선별하고 이를 가지고 공격 그룹 프로필을 생성한다. 마지막으로 유전 알고리즘을 통해 선별한 악성코드 공격 그룹을 분류하는데 유용한 특징 서브 집합을 가지고 분류 알고리즘에 적용하여 해당 특징들이 실제로 악성코드 공격 그룹을 분류하는데 있어서 효과적인지를 확인 할 수 있다.

실험을 통해서는 디컴파일러 및 디셈블러를 통해 생성한 코드들을 Authorship Attribution 기반 특징 추출 방법을 적용하였을 때, 공격 그룹 혹은 저자를 정확하게 분류할 수 있는 지와 유전 알고리즘 기반 선별된 특징들이 실제로 악성코드 공격 그룹 분류 또는 저자를 분류하는데 있어 유용한 특징들을 선별해 내는 지를 확인하였다. 실험 결과 Authorship Attribution 기반 특징 추출을 통해 생성한 특징들은 실제로 저자 라벨을 정확히 나눠준다는 것을 확인하였으며 이는 해당 특징들이 저자나 공격 그룹을 분류하는데 유용하다는 것을 보여주었다. 또한 유전 알고리즘 기반 선별된 특징들도 실험 결과 약 86%의 저자 식별 정확도를 보였다. 또한 이전에 제안된 연구들과의 비교 분석을 통해 본 연구에서 제안하는 Authoship Attribution 기반 저자 특징 추출 프레임워크의 성능을 확인하였으며, 연구 결과 이전 제안한 연구들보다 높은 저자 분류 정확도를 보인 것을 확인하였다. 이를 통해 유전 알고리즘이 저자를 분류하는데 있어 효과적인 특징들을 선별해 준다는 것을 확인 할 수 있었다.

현재까지 진행된 연구를 통해 정상적인 실행 파일을 분석하고 특징을 추출하여, 저자 식별이 가능한지를 확인해보았다. 향후 추가적인 연구를 통해 실제 악성코드를 분석하여 공격 그룹을 찾고, 그룹별 중요 특징을 식별하는 방법에 대한 연구를 수행할 것이며, 부족 데이터 셋을 더 확보하여 연구를 진행할 것이다.

참고문헌(Reference)

[1] Sungho Kim and Suchul Lee, "Automatic Malware Detection Rule Generation and Verification System", Journal of Internet Computing and Services, Vol. 20, No. 2, pp. 9-19, 2019.
http://doi.org/10.7472/jksii.2019.20.2.9

[2] Alrabaee, Saed, et al. "OBA2: An onion approach to binary code authorship attribution", Digital Investigation,

Vol.11, pp. 94-103, 2014.
https://doi.org/10.1016/j.diin.2014.03.012

[3] C. Wang, “A malware variants detection methodology with an opcode based feature method and a fast density based clustering algorithm”, Fuzzy systems and knowledge discovery, pp. 233-245, 2016.
https://doi.org/10.1109/fskd.2016.7603221

[4] Kalgutkar, Vaibhavi, et al. ″Code Authorship Attribution: Methods and Challenges″, ACM Computing Surveys, 2019.
https://dl.acm.org/citation.cfm?id=3292577

[5] Rosenblum, Nathan, Xiaojin Zhu, and Barton Miller. ″Who wrote this code? identifying the authors of program binaries″, ESORICS, pp. 172-189, 2011.
https://doi.org/10.1007/978-3-642-23822-2_10

[6] David E. Goldberg, ″Genetic Algorithms in Search, Optimization and Machine Learning″, Addison-Wesley Longman Publishing Co., 1989
https://dl.acm.org/citation.cfm?id=534133

[7] Jung-Ho Kim, Joo-Ho In and Soo-Hoan Chae. ″Semantic-based Genetic Algorithm for Feature Selection″, Journal of Internet Computing and Services, Vol. 13, No. 4, pp. 1-10, 2012.
http://doi.org/10.7472/jksii.2012.13.4.1

[8] Sung-Sam Hong, Dong-Wook Kim and Myung-Mook Han. ″Feature-selection algorithm based on genetic algorithms using unstructured data for attack mail identification″, Journal of Internet Computing and Services, Vol. 20, No. 1, pp. 1-10, 2019.
http://doi.org/10.7472/jksii.2019.20.1.01

[9] I. Krsul, H. Spafford, ″Authorship Analysis: identifying the author of a program″, Computer & Security, pp. 233-257, 1997.
https://doi.org/10.1016/0167-4048(96)81683-x

[10] S. Burrows, M. Tahaghoghi, “Source Code Authorship Attribution using n-grams”, In Proc. of the Australasian Document Computing Symposium, 2007.
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.68.5920

[11] Yuan, Xiaohui, et al. ″A genetic algorithm-based, dynamic clustering method towards improved WSN longevity″, Journal of Network and Systems Management, pp. 21-46, 2017.
https://link.springer.com/article/10.1007/s10922-016-9379-7

[12] Google Code Jam, “https://code.google.com/codejam/”

◐ 저 자 소 개 ◑

신 건 윤(Gun-Yoon Shin)
2017년 가천대학교 인터랙티브 미디어 융합학과 학사
2018년 가천대학교 일반대학원 컴퓨터공학과(공학석사)
2018년~현재 가천대학교 컴퓨터공학과 박사과정
관심분야 : 기계 학습, 악성코드 분석, 공격자 식별, 저자 분석, 인공지능
E-mail : tlsrjsdbs@gmail.com

김 동 욱 (Dong-Wook Kim)
2015년 가천대학교 컴퓨터공학과(공학사)
2017년 가천대학교 일반대학원 컴퓨터공학과(공학석사)
2017년~현재 가천대학교 컴퓨터공학과 박사과정
관심분야 : Data Mining, AI, Data fusion, Anomaly Detection
E-mail : kog7306@naver.com

한 명 묵(Myung-Mook Han)
1980년 연세대학교 공과대학(공학사)
1987년 뉴욕공과대학교 대학원 컴퓨터공학과(공학석사)
1997년 오사카시립대학교 대학원 정보공학부(이학박사)
1998년~현재 가천대학교 소프트웨어학과 교수
관심분야 : 정보보호, 알고리즘, 데이터 마이닝, 기계 학습
E-mail : mmhan@gachon.ac.kr