GRU를 활용한 악성코드 탐지의 관한 연구*)

류경근, 최용철, 이덕규**

**서원대학교 정보보안학과

ryu8340@gmail.com cho6nt@gmail.com, deokgyulee@gmail.com

A Study on Malicious Code Detection Using GRU**

Ryu Kyeong Geun, Yong cheol Choi, Deok Gyu Lee

**Dept. of information Security, Seowon University

요 약

최근 악성코드에 의한 피해사례가 매년 증가하고 있다. 전통적인 시그니처 기반 안티바이러스 솔루션은 제로데이 공격이나 랜섬웨어처럼 전례가 없는 새로운 위협에 속수무책일 정도로 취약하다. 그럼에도 불구하고 많은 기업이 다중 엔드포인트 보안 전략의 일환으로 시그니처 기반 안티바이러스 솔루션을 유지하고 있다. 이에 응하고자 다양한 악성코드 분석기술이 출현해왔으며, 최근의 연구들은 부분 머신러닝을 이용하여 기존에 진행했던 시그니쳐 기반의 한계를 보완하고 노력하고 있다. 본 논문은 머신러닝을 이용한 바이러스 분석 모델과 머신러닝 알고리즘 중 GRU를 이용한 솔루션 시스템을 제안한다. 기존 DB Server를 통해 머신러닝을 학습 시키며 다양한 샘플과 형식을 이용하여 머신러닝을 학습하고 이를 이용해 새로운 악성코드, 변조된 악성코드의 탐지율을 높일 수 있다.

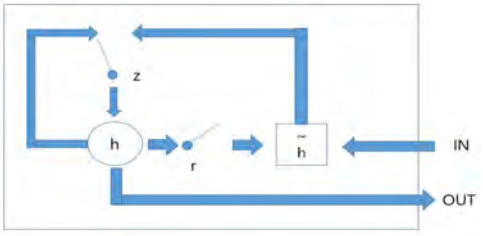
1. 서론

최근 기업 사용자는 데스크톱 PC뿐만 아니라, 노트북, 태블릿, 스마트폰, 그리고 수많은 이동식 저장장치를 사용한다. 또한 최근에는 IoT, 클라우딩 컴퓨터등이 실사용화 되면서 새로운 악성코드들이 대량 발생하며 신종 악성코드는 20% 미만이라고 한다. 나머지는 기존에 있던 악성코드들이 변형되어 사용된다. 진화하는 악성코드와 취약점은 주로 이런 엔드포인트 기기들을 노리고 있어 보안 상태는 나날이 위험해지고 있다. 카스퍼스키 통계에 따르면, 2018년에 탐지된 전체 신종 악성 파일 중에서 백도어로 밝혀진 악성 파일의 수는 44% 증가했으며 랜섬웨어의 규모도 43% 증가했다고 발표 했다. 이는 사이버상에서 심각한 위협이 되며, 이러한 악성코드는 나날히 발전하여 더욱 정교해지고 복잡해지고 있다. 50% 이상의 악성코드가 안티바이러스 제품에 탐지되지 않는 경우가 발생한다.[1] 기계 학습 방법은 데이터로부터 알고리즘을 지속적으로 학습하여 갱신할 수 있기 때문에 변칙적인 침입에 유연하게 대응할 수 있는 장점을 가지고 있다.[2] 이러한 측면에서 바이러스 발생 초반 바이러스에 대한 적은 데이터로 머신러닝을 학습시켜 초기 데이터로도 변종 악성코드를 탐지할 수 있도록 하는 GRU를 활용한 머신러닝 탐지 모델을 제안한다.

*) 본 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2019-0-00326, 블록체인 기반 물류정보의 실시간 트래킹을 통한 스마트 항만 응용 플랫폼 개발)

2. 관련연구

2.1 GRU(Gated Recurrent Unit)

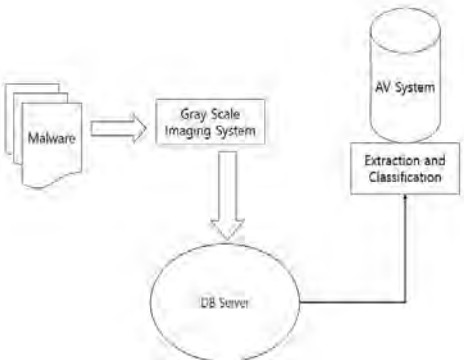


(그림 1) GRU 모델 구조

GRU(Gated Recurrent Unit)는 2014년 발표된 모델로 LSTM의 구조를보다 단순하게 처리한 LSTM 변형모델의 하나이다. GRU의 구조는 LSTM과 마찬가지로 gate를 이용하여 정보의 양을 조절하는 것은 같지만, gate의 제어 방식에는 차이가 있음을 알 수 있다. GRU는 LSTM의 forget gate와 input gate를 update gate로 통합하고, 이를 기준으로 상호작용하는 네 개의 층이 존재한다. 입력데이터를 선택적으로 학습시키기 위해 세 개의 셀 상태의 게이트에서 정보를 더하거나 지우는 구조를 가지고 있다.[3] 셀 상태와 은닉 상태를 하나로 통합하였다. LSTM보다 단순한 구조로 가중치 수가 작으므로 또한 학습이 더 빠르지만, LSTM과 거의 같은 성능을 보인다.[4]

3. 제안방식

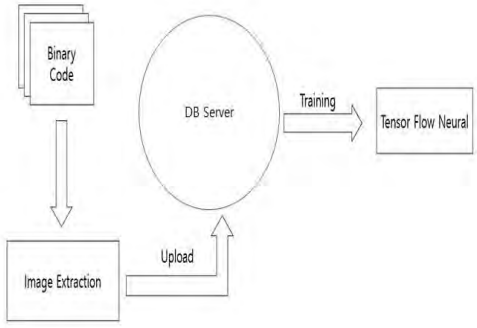
3.1 시스템 구성



(그림 2) 시스템 흐름도

이 그림은 본 논문에서 제안할 방식 시스템의 흐름과 AV(Anti-Virus) System의 분류하여 학습하는 과정을 나타낸다. 먼저 DB Server에는 이미지가 등록된다. 사용자들이 파일의 그레이스케일을 추출해주는 모듈에서 파일에 특정 특징을 배열화 시켜 DB Server에 등록 하면 머신러닝을 통하여 그레이스케일 화 된 이미지를 가져오고 이미지 파일에서 배열을 추출하여, 분류 작업을 통하여 악성코드와 정상파일 등을 분류한다. 본 논문에서 사용한 머신러닝은 LSTM의 한 종류인 GRU를 사용하며 제안하는 방식은 기존 머신러닝 모델보다 게이트 수가 적으며 구조가 간단하여[5] 빠르고 많은 데이터를 실시간성으로 추가할 수 있고, 다양한 데이터셋을 통해 더 수준 높은 기계학습이 가능하여, 기존 Deep Learning 방식의 전수조사의 다양성 또한 보장 할 수 있다.

3.2 악성코드 분류 및 탐지



(그림 3) 악성코드 이미지화

악성코드를 이미지화 시키는 분류 시스템의 흐름은 [그림 3.]과 같다. 먼저, 악성코드 바이트코드를 이미지화 하는 작업을 수행한다. 이 과정을 통해 일정크기의 이미지로 변환시키고, 이미지의 크기에 따라 분류정확도가 영향을 받는다. 이미지화 된 악성코드의 이미지를 학습시킨다.

3.3 데이터 전처리

기계학습을 하기 위해서는 데이터 분석이 필요하다. 데이터 분석을 통해 불필요한 정보를 제

거하고 기계학습의 효과를 최대한으로 할 수 있다. 수집 데이터로서는 악성코드 분석에 사용되는 Feature들은 PE header, Strings, Sequences, DLL/API, Entropy, Instructions, Visualization , Memory 정보, File 정보, Registry 정보, CPU Register, Network 속정보, Anti-Virus 분석정보[6]등 다양하지만, 그 중 분석에 주요한 정보를 가진 5가지인 PE Header, Printable Strings, Sequences, DLL/API, Entropy에 관한 데이터를 수집할 것이고 이 정보와 그 파일이 악성코드인지 여부를 통해 배열을 만들어 머신러닝으로 학습을 시킨다.

3.4 머신러닝의 비정상 행위 탐지

학습 행위를 마치면 각각의 파일들에 대한 정상파일에 대한 출력 시퀀스를 가지고 있다. 이를 이용해 가중치를 계산한다.[7] 또한 이 가중치를 임계치로 설정하여 후에 다른 파일로부터의 정보를 계속 받아와 분석을 하여 분석 정보을 추출하고 가지고 있던 정상파일과 비교하여 이를 정상파일과 동일하거나 유사한 패턴의 형태를 가지면 가중치가 임계치를 넘지않으니 평소와 비슷함으로 정상파일로 간주하며 비정상 패턴이면 가중치가 정상패턴과 크게 다르게 되므로 임계치를 초과하여 비정상파일로 탐지한다.

3.5 Dropout 적용에 따른 성능 차이

인공신경망의 학습은 가중치를 일정 범위 내에서 골고루 분포하도록 초기화 할 경우 좋은 결과를 보이며 Dropout 기법을 통해 과다학습을 방지할 수 있다.[7] 일반적인 신경망 모델에서는 Dropout을 적용할 때 더 좋은 성능을 보인다. 하지만 RNN 계열의 모델들을 정규화 하는 방법은 많이 적용되지 않고 RNN 모델을 확장하고 보완하여 만든 GRU 모델 역시 Dropout을 적용하면 오히려 성능이 떨어진다. [9]

3.6 머신러닝 모델 비교

<표 1> 머신 러닝 모델 비교

	데이터 의존도	정확도	과적합 빈도
RNN	○	△	○
LSTM	○	○	△
GRU	△	○	X

<표 1> 은 기존에 있던 RNN과 LSTM을 활용하여 만든 사용자 행위 분석과 본 논문에서 제안하는 시스템간의 비교를 나타내고 있다. 데이터 의존도 측면에서는 기존의 RNN과 LSTM은 사용자 분석의 데이터 의존도는 매우 높다. 이에 반해 GRU는 LSTM에서 데이터 의존도를 낮추어 제안된 모델로서 데이터가 부족한 경우에도 기존 방식보다 빠르게 이상 행동을 유추해낼 수 있다. 정확도 측면에선 RNN과 GRU 모델에 큰 차이는 없다. 하지만 GRU 모델에선 적은 데이터로와 짧은 학습 시간으로도 높은 정확도를 얻을 수 있다. LSTM은 적은 데이터에선 GRU보단 낮은 정확도를 가지지만 충분한 수의 데이터가 있을시 우수한 결과를 보여주었다. 과적합 빈도 측면에서 보자면 RNN은 히든 노드가 순환하는 방식으로 망각 게이트가 없어 과적합이 일어나기 쉽다. LSTM은 RNN에서 메모리셀을 더한 구조로서 과적합 비율을 줄였다. 여기서 GRU는 셀상태와 은닉상태를 통합하여서 더욱 메모리에 적재를 줄이고 과적합 빈도를 낮췄다. 분석한 내용을 보자면 RNN을 이용한 사용자 행위 분석보단 다른 LSTM과 GRU를 사용한 사용자 행위 분석이 월등한 성능을 갖고 있다. 여기서 LSTM은 많은 데이터를 가질 시 더욱 높은 정확도를 보여주었고 GRU는 많은 데이터를 학습할 시 LSTM보단 낮은 정확도를 가지게 되지만 GRU는 적은 데이터와 짧은 시간으로 단기간에 높은 정확도를 보여주었다. 제로데이 공격 이후 초반 적은 데이터에 대한 학습에 더 유용하다. 초기 보안 측면을 위해 본 논문에선 GRU 방식을 제안한다.

4. 결론

최근 악성코드에 의한 피해사례가 매년 증가하고 있다. 전통적인 시그니처 기반 안티바이러스 솔루션은 제로데이 공격이나 랜섬웨어처럼 전례가 없는 새로운 위협에 속수무책일 정도로 취약하다. 본 논문에서는 차세대 안티바이러스 솔루션 대책으로 머신러닝 알고리즘 중 GRU를 이용한 솔루션 시스템을 제안한다. 기존 머신러닝을 사용한 안티바이러스 소프트웨어와 비교하며 변종 악성코드를 탐지할 때 더욱 적은 데이터를 사용해서 탐지 할 수 있을 것이다. 탐지하는 부분에서 다양한 샘플과 형식을 이용하여 머신러닝을 학습하고 이를 이용해 새로운 악성코드 및 변조 악성코드의 탐지율을 높일 수 있고 또한 기존의 Deep Learning 방식의 다양한 학습 및 전수조사가 필요한 부분을 GRU 알고리즘으로 보완 할 수 있지만 현재 실험 데이터가 없으며 명확한 성능을 기대하기 어렵고 적용시에도 머신러닝의 문제점인 높은 오탐률에 대한 개선해야한다. 최근 CNN과 GRU를 함께 사용하여 이미지에 대한 학습도를 향상 시키는 연구도 이루어지고 있으니 이에 맞춰 적용할 여지도 충분히 있다.

[참고문헌]

[1] M. Sharif, A. Lanzi, J. Giffin, W. Lee,'Automatic Reverse Engineering of Malware Emulators', 2009 30th IEEE Symposium on Security and Privacy, pp. 94-109.

[2] Joe cheolhee "Research on An efficient Insider Threat Detectionbased on LSTM Autoencoder using user attribute information",Sungkyunkwan University Doctor's Thesis, Aply 2018

[3] Seo Jihye, Yong hawnseung, 'EPerformance Evaluation of LSTM and GRU using TensorFlow,' 2014. Korea Information Science Society 2016 Winter Conference, 2016, pp. 211 - 213 (3 pages)

[4] J. Chung, C. Gulcehre, K. H. Cho, and Y. Bengio, 'Empirical evaluation of gated recurrent neural networks on sequence modeling,' 2014.

[5] Junyoung Chung and Çaglar Gülçehr, 'Empirical Evaluation of Gated Recurrent Neural Networks on Sequnce Modeling',

Newyork Univ. ArXiv, December 2014

[6] Tae-jin Lee, 'Trend of Intelligent Malware Analysis Technology Using Machine Learning, KIISC review v.28 no.2, April 2018

[7] Dong-wook Ha, 'A Study on a Machine Learning Model for Detecting Insider Anomaly Behaviour', February 2018

[8] hoe-hyeon KIM, 'Forecasting Time-se ries Data Using LSTM/GRU Recurrent Neural Networks', Korea National Open University Master's Thesis, July 2017

[9] Ye-seul Lee, 'The Judgement System for the Risk Classification of Internal Data Leakage using GRU Model', soongsil University Master's Thesis,

December 2017