7ZC-07

軽量化 DenseNet を用いたマルウェア分類

ダオ　ヴァン　トゥアン†　　佐藤　浩†　久保　正男†

防衛大学校情報工学科†

1．　はじめに

マルウェアは日々進化している。インターネットは私たちの生活に欠かせないものになると同時に、優れたサービスを提供するが、多くのセキュリティ上の脅威も起こっている。攻撃者はマルウェアを利用してインターネット上でリモート管理ツールとして間接的に標的に侵入、妨害、および制御を行うことでサイバーセキュリティに大きな影響を与え、個人、社会、国への脅威を引き起こす。ウィルス対策ソフト及び侵入検知システムを出し抜くため、マルウェアの作成者は、ユーザインタラクション、環境認識、難読化、コード圧縮、コード暗号化などのさまざまな回避手法を組み合わせて、既存のマルウェアを一部変更する。その結果、新しい亜種には、元のマルウェアと同じ悪意と特性を持つ傾向がある。

機械学習は、各分野で遭遇する問題のほとんどを解決する優れたアルゴリズムの開発により、ますます強力になっている。マルウェア分類のための機械学習ベースの方法の一つに、ビジョンベースのアプローチがある。攻撃者は難読化技術を使用するため、同じファミリのマルウェアの亜種では、同じ場所に同一のコードが表示されない可能性があるが、全体としてある程度類似したコードとデータの順序は維持されている。機械学習の手法である畳み込みニューラルネットワーク（CNN）は、マルウェアのファミリから共通の機能を抽出できる。

既存研究では、複雑なニューラルネットを構築することが多いが、その実行には高性能なコンピュータと長い処理時間が必要である。本究では Densnet を軽量化したモデルにより、画像化されたデータセットに対しマルウェアの分類を行った。本手法は、短い時間で高い精度を得ただけでなく、人間の目には判別できない類似のマルウェアファミリーを識別することもできた。

2.　マルウェアの画像化

マルウェアのサンプルを画像として視覚化するには、各バイトを画像の 1 ピクセルとして解釈する必要がある。マルウェアのバイナリファイルを 16 進数で表したものを図 1 に示す。最初の行はメモリアドレスのオフセットであり、2 行目以降は、16 進数のペアを表す。各 16 進数のペアは、画像のピクセル値として機能する 1 つの 10 進数として扱わる。その値をグレースケールと対応付けて画像に変換する。

```
00000000`00400000: 4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00
00000000`00400010: B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00
00000000`00400020: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000000`00400030: 00 00 00 00 00 00 00 00  00 00 00 00 20 01 00 00
00000000`00400040: 0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68
00000000`00400050: 69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F
00000000`00400060: 74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20
00000000`00400070: 6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00
00000000`00400080: 4F BD E6 37 0B DC 88 64  0B DC 88 64 0B DC 88 64
00000000`00400090: BF 40 79 64 08 DC 88 64  BF 40 7B 64 BB DC 88 64
00000000`004000A0: BF 40 7A 64 16 DC 88 64  95 7C 4F 64 0A DC 88 64
00000000`004000B0: 30 82 8B 65 1C DC 88 64  30 82 8C 65 28 DC 88 64
00000000`004000C0: 99 82 81 65 0A DC 88 64  D6 23 59 64 0A DC 88 64
00000000`004000D0: D6 23 46 64 09 DC 88 64  D6 23 43 64 12 DC 88 64
00000000`004000E0: 0B DC 89 64 29 DD 88 64  30 82 8D 65 36 DC 88 64
00000000`004000F0: 99 82 8D 65 22 DC 88 64  99 82 77 64 0A DC 88 64
00000000`00400100: 0B DC 1F 64 0A DC 88 64  99 82 8A 65 0A DC 88 64
00000000`00400110: 52 69 63 68 0B DC 88 64  00 00 00 00 00 00 00 00
00000000`00400120: 50 45 00 00 4C 01 0A 00  5E 4B 87 5F 00 00 00 00
00000000`00400130: 00 00 00 00 E0 00 03 01  0B 01 01 00 00 C0 09 00
00000000`00400140: 00 10 07 00 00 00 00 00  00 A0 0F 00 00 10 00 00
00000000`00400150: 00 C0 09 00 00 00 40 00  00 10 00 00 00 02 00 00
```

図 1　マルウェアバイナリファイルの構造

3.　提案手法

画像から特徴を抽出するモデルは様々あるが、その中で、近年 DenseNet[1]が注目を集めている。DenseNet では図 2 に示したように各 DenseBlock で、それ以前の層の結果を結合する。Dense Block を用いることで離れた層の情報をそのまま加味することができる。

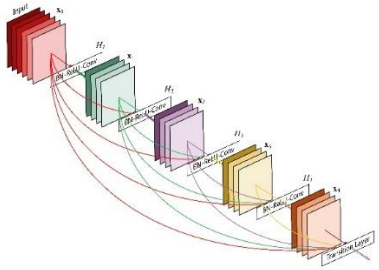

図 2　DensNet の構造[1]

DenseBlock のフィルタを一定の値（成長率 k）でコントロールするため、通常の CNN より、パラメータの数が少なくなり、計算量も減少できる。最後の層で全結合化するときに Flatten ではなく Global Average Pooling（GAP）で平均を取って分類するが、本研究では Global Max Pooling (GMP)も導入することで、各フィルタの重要値を捉えることを狙う。更に、本研究では学習率を以下の(1)式のように調整する：

Using Light-weight DenseNet for Image-based Malware Classification

† Computer Science, National Defense Academy

$$learning\_rate *= \frac{1}{1 + decay * epoch} \quad (1)$$

引数 Decay が 0 の場合、学習率の変更に影響を与えない。Decay が指定されている場合、指定された固定量だけ前のエポックからの学習率が減少する。 Decay の値は次のように実装される。

$$decay = \frac{initial\_learning\_rate}{number\ of\ epoches} \quad (2)$$

本研究では Adam 最適化を利用するため、$initial\_learning\_rate$ = 0.001. Epoch 数は 50 とする。モデルをコンパクトにするため、成長率 k は 32 とした。Dense Block は重複することなく、DenseNet の深さは 13、パラメータは 197,673 である。

4. 実験

本研究では Malimg データセット[2]を用いて実験を行い。データセットは 25 の異なるマルウェアファミリーの 9,339 のサンプルで構成されている。図 3 に示すように、学習率を調整することによって Epoch 32 以降で学習の安定が見られた。また、既存研究との比較を表 1 に示す。提案手法は Accuracy が 1% 程度上がり、学習時間に関しては Awan らの VGG19 モデル[4]より 18 倍以上時間を短縮することができた。

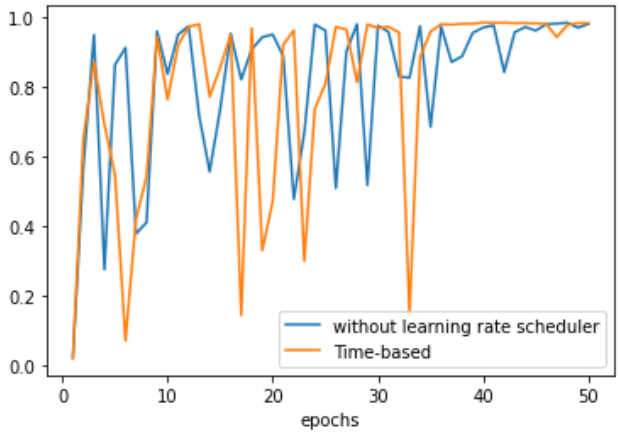

図 3　学習率の調整が有りと無しとの比較

表 1　既存研究との比較

モデル	Accuracy (%)	Time(s)
CNN [2]	97.18	6140
DenseNet-201[3]	98.23	1941
VGG19[4]	97.68	5363
DenseNet-13 学習率調整なし	98.61	327
DenseNet-13 学習率調整あり	**98.64**	**285**

図 4 に Confusion matrix を示す。Autorun.K 及び Yuner. A の 2 つファミリーは人間の目で区別が非常に困難（図 5）だが、本モデルでは 100%の分類精度が得られた。

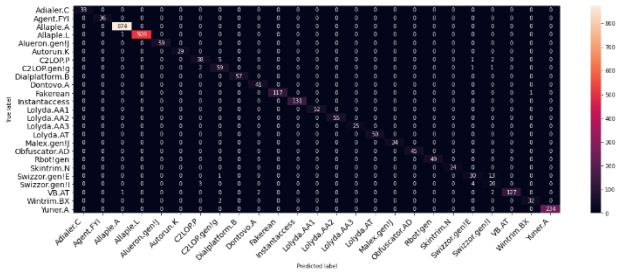

図 4　Confusion matrix

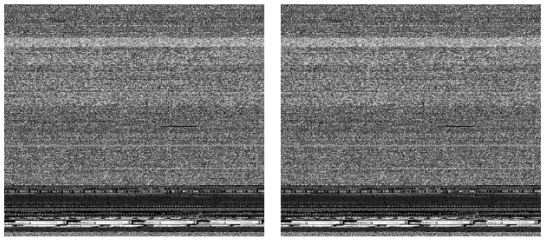

図 5　類似のマルウェアファミリー

5. まとめ

本研究では、軽量化 DenseNet を用いてマルウェア分類した。提案モデルは、深いネットワークを使った既存研究より高い精度を短い時間で得ることができる。また、類似のマルウェアファミリーも高い精度で分類できる。今後は新マルウェア及び Benign を Malimg データセットに追加し、検出及び分類タスクを同時に実施する。

6. 参考文献

[1] G.Huang, Z. Liu, K. Weinberger, “Densely Connected Convolutional Networks”, in Project “Efficient Deep Learning”, Aug. 2016.
[2] L. Nataraj, S. Karthikeyan, G. Jacob and B.S. Manjunath, “Malware images: visualization and automatic classification”, Proceedings of the 8th International Symposium on Visualization for Cyber Security, 2011.
[3] J. Hemalatha, S.A. Roseline, S. Geetha, S. Kadry and R. Damaševičius, “An Efficient DenseNet-Based Deep Learning Model for Malware Detection”, in Entropy 23(3):344, Mar.2021.
[4] M. Awan, M. Mohoammed, A. Yasin, A. Zain, “Image-Based Malware Classification Using VGG19 Network and Spatial Convolutional Attention”, in Electronics, vol. 10, no. 19, Oct. 2021.