マルウェア検知におけるオンライン機械学習アルゴリズムの比較研究

中 村 燎 太† 大 山 恵 弘†

1. はじめに

近年では，マルウェア特有の挙動を検知するビヘイビア法に，バッチ学習という機械学習技術と組み合わせたマルウェア検知手法が盛んに研究されている．ところが，バッチ学習では新たなマルウェアが発見される度に全既知検体を再学習させる手間が生じるため，増加するマルウェアの検知用途として実用性に欠ける．

一方で，オンライン学習という機械学習技術を用いたビヘイビア法は，マルウェアを容易に追加学習させることが可能であり，マルウェア検知用途との親和性が高い．但し，本手法を実用する際には「処理が低速であっても，検知精度を優先したい」といった状況別のニーズに適するオンライン学習アルゴリズムを都度選択することが望まれる．従って，マルウェア検知用途における各アルゴリズムの特性評価は，アルゴリズム選択の指標を示すために有意である．そこで本研究では，4 系統 7 パターンのオンライン学習アルゴリズムの各々について，マルウェア検知における「信頼性」と「処理速度」を始めとする特性を実験にて示す．

2. マルウェア検知機構

本研究では，**図 1** に示す機構の下でオンライン機械学習アルゴリズムを利用し，Windows OS に対応したマルウェアを検知することを想定する．

まず，未知検体がマルウェアであるか否かを識別し，マルウェアを検知するための根拠として，本機構では素性 (ラベル) が判明している複数の学習用検体の API コール列及びラベルと，ラベルが判明していない識別用検体の API コール列を利用する．API コール列は，検体が利用した Win32 API，Native API, システムコールのシーケンス列より構成される．本情報を利用した既存のマルウェア検知技術は数多く存在し，例えば Ahmed ら[1] は未知マルウェアを 97% の精度で検知することに成功している．

次に，前処理として各検体の API コール列に N-gram を適用する．N-gram とは「一塊の情報を，先頭から順番に N 個の要素群に分割する処理」のことで，分割後の要素群は「セグメント」と表記する．例えば，“ABCD” という API コール列に 2-gram を適用すると “AB”，“BC”，“CD” というセグメントが生成される．この際に，類似した挙動を示す API をマージすることで API コール列の特徴量を削減し，生成されるセグメントの総数を最小化することで処理時間やメモリ消費量の増大を防いでいる．そして，検体毎に各セグメントの内包数 (セグメント数) を集計する．

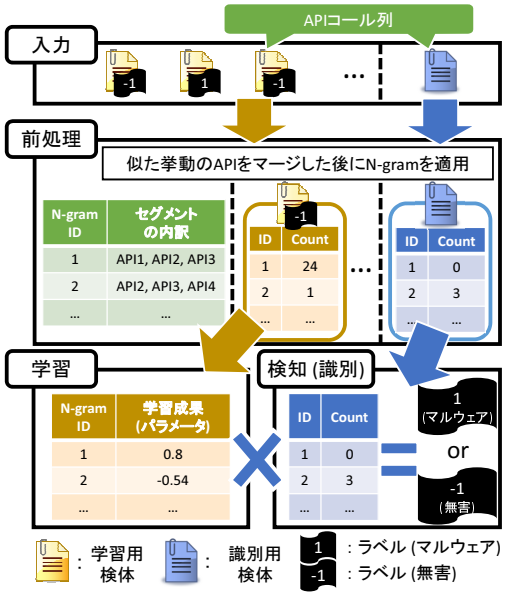

図 1 マルウェア検知機構の概要図

最後に，各検体のセグメント数をオンライン学習アルゴリズムにて学習し，その成果 (パラメータ) を用いて識別用検体のラベルを出力する．本機構にて利用するアルゴリズムとしては，Passive-Aggressive (PA)，Adaptive Regularization of Weight Vectors (AROW)，Normal HERD (NHERD)，Soft Confidence-Weighted (SCW) の 4 系統を想定する．NHERD を除く 3 系統には複数の亜系統が存在するが，本研究では API コール列のような線形分離可能性が保証されていないデータにも対応する PA-I, PA-II[2], AROW[3], NAROW[5], NHERD[4], SCW-I, SCW-II[6] の 7 パターンを比較対象とする．

† 電気通信大学 情報理工学研究科 総合情報学専攻
Dept. of Informatics, Graduate School of Informatics and Engineering, The University of Electro-Communications.

3. 実　　験

実験の主目的は，各アルゴリズムに対応するマルウェア検知機構を実装し，実検体に対して検知実験を行うことで，マルウェア検知における各アルゴリズムの特性を「信頼性☆」・「処理速度☆☆」を始めとする複数の側面から示すことである．また，本研究ではマルウェア検知機構の利用様態に即した評価を行うべく，「通常実験」と「リアルタイム検知実験」という 2 種類の実験を独立に実施した．紙面の都合上，本稿では両実験の概要を述べるに止め，実験結果及びアルゴリズムの評価概要はポスター発表にて提示する．

3.1 通 常 実 験

本実験は，識別用検体の API コール列を十分な分量に達するまで収集することが可能で，かつ API コール列の収集が完了するまで識別を留保できるケースに見合ったデータを得るためのものである．具体例としては，アンチウイルスソフトウェアベンダーにおいて，未知検体の自動的な初期スクリーニング用途として本機構を利用するケース等が挙げられる．API コール列等の動的解析情報を利用したマルウェア検知研究では，暗黙的に本想定が利用されているものが多く，一例として村上ら[8] による研究が挙げられる．

本実験では，FFRI Datasets 2015[7] に収録されたマルウェアと，独自に収集・解析した無害バイナリの API コール列を実験対象とした．そして，全検体を 7 : 3 の割合で無作為に分割し，学習用検体群と識別用検体群の組 (検体セット) を複数生成した．次に，セグメントサイズ N 及び学習アルゴリズムを変えつつ，各検体セットに対して測定を行った．なお，各検体セットの測定前には分割交差検証を実施して各アルゴリズムの調整を行うと同時に，検体セットの妥当性を確認した．最後に，各検体セットに対応する測定結果の平均値を，N 及びアルゴリズム毎に算出した．

なお，本実験では，識別用検体を学習に再利用した場合の信頼性も併せて算出した．これは,「オンライン学習の利点である追加学習機構を利用して，学習成果の更新を図る」ケースに対応するための措置である．

更に，マルウェア検知機構への入力情報として，2 章にて述べた「N-gram のセグメント数」を入力する標準的なケースに代えて,「セグメントの比重」を入力したケースにおける信頼性も併せて算出した．本結果は，学習アルゴリズムが N-gram セグメントの数に影響されるか否かの判断に有用である．

3.2 リアルタイム検知実験

本実験は，識別用検体の API コール列が収集途中であっても，定期的に識別が行われるケースに見合ったデータを得るためのものである．例えば，本研究と同様の検知機構を搭載したアンチウイルスソフトウェアでは，マルウェアの動作を早急に停止させるべく、未知検体を定期的に識別する機構が必要となる．

本実験では，識別用検体の API コール列を 300 の倍数毎に識別し，最後までマルウェアと判定されなかった検体を無害バイナリ，そうでないものをマルウェアとして扱った．他の諸条件は通常実験と同様である．

4. 本稿のまとめと今後の課題

オンライン学習を用いたマルウェア検知機構の利点及び構造と，マルウェア検知用途における各アルゴリズムの特性を評価するための実験手法を示した．今後は，誤ったラベル付きの学習用検体を混入させたケースに対応する実験を行い，より多様な観点から学習アルゴリズムの特性を評価する．

☆ 本稿では，正解率, 精度, 検出率, 特異度, 偽陽性率, 偽陰性率, F 値の 7 指標の総称として本単語を定義する．

☆☆ 学習用検体 1 つあたりの学習速度と，識別用検体 1 つあたりの識別速度を指す．

参　考　文　献

1) Faraz Ahmed, Haider Hameed, M. Zubair Shafiq, and Muddassar Farooq. Using Spatio-temporal Information in API Calls with Machine Learning Algorithms for Malware Detection. In *Proceedings of the 2nd ACM Workshop on Security and Artificial Intelligence*, AISec '09, pp. 55–62, 2009.
2) Koby Crammer, Ofer Dekel, Joseph Keshet, Shai Shalev-Shwartz, and Yoram Singer. Online Passive-Aggressive Algorithms. *Journal of Machine Learning Research*, Vol. 7, pp. 551–585, 2006.
3) Koby Crammer, Alex Kulesza, and Mark Dredze. Adaptive Regularization of Weight Vectors. In *Advances in Neural Information Processing Systems 22*, pp. 414–422, 2009.
4) Koby Crammer and Daniel D. Lee. Learning via gaussian herding. In *Advances in Neural Information Processing Systems 23*, pp. 451–459, 2010.
5) Francesco Orabona and Koby Crammer. New adaptive algorithms for online classification. In *Advances in Neural Information Processing Systems 23*, pp. 1840–1848. 2010.
6) Jialei Wang, Peilin Zhao, and Steven C. Hoi. Exact Soft Confidence-Weighted Learning. In *Proceedings of the 29th International Conference on Machine Learning (ICML-12)*, pp. 121–128, 2012.
7) 神薗雅紀, 秋山満昭, 笠間貴弘, 村上純一, 畑田充弘, 寺田真敏. マルウェア対策のための研究用データセット〜MWS Datasets 2015〜. 情報処理学会 研究報告コンピュータセキュリティ（CSEC）, No. 6, pp. 1–8, Jun 2015.
8) 村上純一, 鵜飼裕司. 類似度に基づいた評価データの選別によるマルウェア検知精度の向上. コンピュータセキュリティシンポジウム 2013 論文集, No. 4, pp. 870–876, Oct 2013.