2Y-4

SVM による IP 攻撃通信の判別法
Discriminating Malicious Traffic with SVM

千葉 大紀† 森 達哉†‡ 後藤 滋樹†

† 早稲田大学 基幹理工学部 情報理工学科
‡NTT サービスインテグレーション基盤研究所

概要

マルウェアの活動による被害が拡大・深刻化している．マルウェアによる悪意のある通信は複雑な難読化や暗号化を伴うため，シグネチャによるパターンマッチングでは解析の高速化が困難であり，リアルタイムな通信検出に課題がある．本研究は IP アドレスの構造的な特徴を利用することによって，悪意のある通信を高速かつ高精度に検出する手法を提案する．具体的には IP アドレスから抽出した特徴ベクトルに対して，教師あり機械学習法の一つである SVM (Support Vector Machine) を適用し，高精度な検出を実現する．統計的機械学習を用いるアプローチは，既知のパターンを利用するシグネチャベースの手法では検出が困難な未知の攻撃通信の判別において優位性がある．さらに，本手法で提案するアドレス構造の抽出に要する処理は軽量であるため，学習後の判定に要する演算コストが低い．したがって，本手法はリアルタイムの悪意のある通信の検出に応用可能である．本論文は提案手法を説明した後に，その有効性を実データを用いて検証した結果を報告する．

1 提案手法

本手法のアイディアは，悪意のある通信あるいは通常の通信を発信するホストの IP アドレスが，それぞれある一定のネットワークアドレス空間に集中しやすい性質を活用することである．はじめに悪性と通常を区別するラベル付きの IP アドレスリストを準備する．つぎに得られた IP アドレスから特徴ベクトルを抽出し，SVM の訓練アルゴリズムを適用することによって訓練モデルを構築する．通信の悪性を判定する時には，判定の対象となる未知の IP アドレスの特徴ベクトルに対して上述の訓練モデルから得られる判別式を適用して，その IP アドレス発の通信が悪性であるか通常であるかを二値判別する．単純なブラックリストやホワイトリストを用いる方法では既にリストにあるアドレスのみ判定可能であるのに対して，本アプローチは未知のアドレスに対する判定が出来る事が優れた点である．以下では IP アドレスから特徴ベクトルを抽出する方法について述べる．

■特徴ベクトル抽出手法 IP アドレスを構成するビット列の構造的な性質から，アドレスに固有な特徴ベクトルを抽出することが出来る．以下は IPv4 アドレスを例として抽出方法を記載するが，IPv6 アドレスでも同様に特徴ベクトルを抽出することができる．特徴ベクトルの抽出には様々な方法が可能であるが，本稿では紙面の都合上一つの方法のみに重点を置き，性能評価結果を報告する．IPv4 アドレスの上位 N $(1 \leq N \leq 4)$ オクテットを用いて，$M = 2^8 \times N$ 次元の特徴ベクトルを以下のようなスパースなバイナリビット列 $\{b_0, \ldots, b_{M-1}\}$ によって構成する．N は特徴ベクトルを構成する際のパラメタである．各ビットの初期値はすべて 0 であり，IPv4 アドレスの第 n $(1 \leq n \leq N)$ オクテットの 10 進表記が X $(0 \leq X \leq 2^8 - 1)$ であったら，$b_{2^8(n-1)+X} = 1$ とする．

2 性能評価

2.1 データ

悪性 IP アドレスのリストを，ある商用ネットワークに設置したハニーポット Dionaea [1] で収集した攻撃通信データ，およびパブリックな IP ブラックリストである Spamhaus DBL, PBL, SBL [2] を利用することで構築する．同様に通常 IP アドレスのリストを, 著名なドメインを集めたリストである Alexa Top Global Sites [3] を用いて抽出した IP アドレスリスト，パブリックな IP ホワイトリストである DNSWL [4]，および CDN のアドレスの一部や大学などの教育機関のアドレスを収集したリストを利用して構築する．表 1 に各 IP アドレスデータの内訳を示す．

表 1　収集した IP アドレスデータの内訳．数値はユニークな IP アドレス数．

悪性 IP アドレス				
Honeypot	DBL	PBL	SBL	計
3,097	508	628,042	4,233	635,880

通常 IP アドレス				
Alexa	DNSWL	CDN	Univ	計
10,869	136,500	67	125	147,561

表 2　ユニークな特徴ベクトルの数．

N	1	2	3	4
悪性	164	16,307	563,083	635,880
通常	173	9,176	37,213	147,561
和集合	179	21,085	600,027	783,441

2.2　評価方法

1 章で示した特徴ベクトル抽出法をデータに適用すると表 2 を得る．IP アドレスの上位のオクテット数 ($N = 1, 2$) のときは SVM への入力サンプル数が比較的小さいが，$N = 3, 4$ に対してはサンプル数が大きいことがわかる．そこで，本研究では IP アドレスの判別アルゴリズムとして線形 SVM および非線形 SVM を用いる．一般に非線形 SVM は線形 SVM よりも高精度な識別を実現可能であるが，データを高次元に写像する非線形関数を適用する演算により，訓練モデル作成の計算量が非常に大きくなることが知られている．本論文では $N = 1, \ldots, 4$ のすべてのケースについて軽量な線形 SVM を適用し，計算コストが高い非線形 SVM は特に次元数および入力数のいずれもが低い $N = 1, 2$ に対してのみ適用する．

表 2 に示すデータに対して 5 分割交差検定を行い，平均値をとることによって性能を評価する．ここで悪性，通常のそれぞれの特徴ベクトルは重複するものを除いているため，交差検定の結果は純粋に未知のアドレスに対する性能評価となる．本研究では線形 SVM および非線形 SVM の実装として LIBLINEAR [5] および LIBSVM [6] を用いた．カーネル関数としてガウスカーネルを採用し，精度を最適化するパラメタ値をグリッド探索によって求めた．

2.3　評価結果

各データの精度 (accuracy)，適合率 (precision)，再現率 (recall) を比較した結果を表 3，4 に示す．ここで精度とは正答率のことであり，判定したすべてのアドレスのうち，判定結果が正しかったアドレスの割合である．適合率とは，悪性と判定したアドレスのうち，実際に悪性であるものの割合である．再現率とは，実際に悪性であるアドレスのうち，正しく悪性と判定したアドレスの割合である．

全体としては，$N = 3$ のときに最も精度が高いことがわかる．これは多くのネットワークにおいて IP アドレスブロックが/24 を単位として運用されている事からも妥当な結果である．特に再現率が約 99% と非常に高く，悪性アドレスを見逃さない性能が高いことがわかる．ついで $N = 4$ の精度が良いが，アドレス全体を含んでしまうと未知のアドレスに対するロバスト性が失われる．$N = 3$ に対して $N = 4$ の性能が劣る．$N = 1, 2$ については，非線形 SVM の方が高い精度となるが，特に $N = 1$ の非線形 SVM では，すべての特徴ベクトルを通常と判定する識別モデルが精度を向上する為に最適であると判定されてしまい，期待するような結果を得る事は出来なかった．表 2 からもわかるように，第 1 オクテットのみでは悪性と通常で約半数の特徴ベクトルが重複するため，識別は困難である．

表 3　線形 SVM による識別結果．

N	1	2	3	4
精度 (accuracy)	9.82%	74.15%	94.70%	90.98%
適合率 (precision)	16.10%	77.52%	95.62%	93.15%
再現率 (recall)	20.12%	83.95%	98.87%	95.94%

表 4　非線形 SVM による識別結果．

N	1	2
精度 (accuracy)	51.34%	74.46%
適合率 (precision)	0.00%	78.13%
再現率 (recall)	0.00%	83.45%

3　まとめ

本研究では，IP アドレス構造の特徴を学習することによって悪意のある通信を判別する手法を提案した．性能評価の結果，未知の悪性 IP アドレスを高精度で検出できることを示した．特に強調したいことは，IP アドレスそのものが悪意のある通信の判断材料の 1 つとして利用することができる点である．今後の課題は特徴ベクトルの拡張や学習アルゴリズムの改善による更なる精度の向上，および提案手法を実ネットワークで動作させるための実装である．

参考文献

[1] Dionaea, http://dionaea.carnivore.it/

[2] The Spamhaus Project, http://www.spamhaus.org/

[3] Alexa Top Sites, http://www.alexa.com/topsites

[4] DNS Whitelist, http://www.dnswl.org/

[5] R.-E. Fan, K.-W. Chang, C.-J. Hsieh, X.-R. Wang, and C.-J. Lin. LIBLINEAR: A Library for Large Linear Classification, Journal of Machine Learning Research 9(2008), 1871-1874. Software available at http://www.csie.ntu.edu.tw/~cjlin/liblinear

[6] C. C. Chang and C. J. Lin, LIBSVM : a library for support vector machines, 2001. Software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm