IoTマルウェア検知精度向上のためのGridSearchCVによるOCSVMのパラメータ最適化

IoT マルウェア検知精度向上のための GridSearchCV による OCSVM のパラメータ最適化

村中　弘樹 [a)]・後藤　修斗 [b)]・油田　健太郎 [c)]・山場　久昭 [d)]・岡崎　直宣 [e)]

Parameter Optimization of OCSVM by GridSearchCV for Improving IoT Malware Detection Accuracy

Hiroki MURANAKA, Shuto GOTO, Kentaro ABURADA, Hisaaki YAMABA, Naonobu OKAZAKI

Abstract

Abstract is written in 200-300 words. In recent years, the Internet of Things (IoT) has been playing an increasingly important role in our lives. It has enabled us to form new services and business models, and to automate and improve the efficiency of our work. However, at the same time, security vulnerabilities have become an issue: according to NICT, more than half of the observed cyber attack-related communications targeted the IoT [3].In this study, we propose a system that combines n-gram analysis and OCSVM to discriminate between normal communication of IoT devices and communication after malware infection, and a system that uses GridSearchCV to calculate the best parameters for the parameters arbitrarily set by humans when applying OCSVM. The system is proposed to calculate the best parameters using GridSearchCV. For the evaluation, we conducted an experiment to compare the detection accuracy of 25 sets of parameters conventionally used and the detection accuracy using GridSearchCV, and showed good detection accuracy. However, in some cases, the detection accuracy decreased in the process of increasing the total number of data given to GridSearchCV. As a future subject, it is necessary to change the ratio and the total number of normal data and more than normal data, to observe the change of detection accuracy, and to study the cause.

Keywords: IoT, Malware detection, OCSVM, GridSearchCV

1. はじめに

今日、我々の身の回りの生活において「モノ」と「インターネット」を繋げた「モノのインターネット (Internet of Things)」、通称 IoT の活躍が著しいものとなっている。従来ではインターネットに接続されていなかった様々な「モノ」がネットワークを通じることで、新たなサービスやビジネスモデルを形成し、仕事の自動化や効率化を図ることが可能となった。IoT の導入は私生活や事業場に留まらず、国家プロジェクトとして行政サービスにも導入されつつある。政府が「Society5.0」と掲げた「質の高い生活が出来る人間中心の世界」構想は、IoT 技術を行政サービスに組み込み、国民生活の利便性の向上を図るものとなっており、今後は国単位での IoT デバイスの導入が伺え、より活躍の場が広がっていくことが予想される。

普及が進んでいく一方で、IoT 機器のセキュリティ面での脆弱性が問題となっている。2016 年 10 月に米国の DNS サービスプロバイダである Dyn が史上最大規模の DDoS 攻撃を受けたことで、IoT 機器のセキュリティの脆弱性が注目された。この DDoS 攻撃では Amazon、Google、Netflix、Twitter など大手ウェブサービスへのアクセスを約 6 時間に渡り妨害され、120 万人以上のユーザーが被害を受けた。調査の結果、この DDoS 攻撃は「Mirai」と呼ばれるマルウェアに感染した 50 万台にも及ぶ IoT デバイスによって構築されたボットネットによる攻撃であることが判明した [1)]。IoT デバイスの特質上、機器の電源は切らずに稼働したままにすることが多く、また、PC やスマートフォンに比べて IoT 機器はセキュリティに対する関心や意識が低く、ID やパスワードが簡易な文字列に設定されることが多いため「Mirai」の感染拡大を引き起こした要因であると考える。同年 10 月ではネットに突如現れた、「Mirai」の制作者がソースコードを公開したことが発端となり、「Mirai」の亜種である IoT マルウェアは 2016 年-2018 年の間だけで約 37 倍と爆発的に増加した [2)]。

また、情報通信研究機構 (NICT) が公表した「NICTER 観測レポート 2018」では、NICTER の構築したダークネット観測網にて観測したサイバー攻撃関連通信のうち、約半数以上が IoT 機器が標的とされ、特に Web カメラ、Web 管理画面、ルータ等が狙われたことが示されている [3)]。

以上の現状から、IoT 技術が様々な分野で導入され、新たな生活・働き方・ビジネスが形成されている一方で、近年は IoT 機器がサイバー攻撃者から魅力的な標的とされていることが判明した。今後行政サービスにも IoT 技術が導入されることを鑑みると、IoT デバイスのセキュリティ面での改善が

[a)] 工学専攻機械・情報系コース大学院生
[b)] 情報システム工学科学部生
[c)] 情報システム工学科准教授
[d)] 情報システム工学科助教
[e)] 情報システム工学科教授

早急に必要である。

本研究では、IoT デバイスがマルウェアに感染した際に、その感染の有無を検出するシステムとして、n-gram 解析と One-Class Support Vector Machine(以下 OCSVM) を組み合わせた IoT マルウェア検知技術を提案する。さらに、本システムの検知精度を向上させるため、本来人間の手によって任意に設定される OCSVM のパラメータを GridSearchCV(Python のオープンソース機械学習ライブラリ scikit-learn の一部) を用いて、自動で最適なパラメータを算出するシステムを提案する。

2. 関連研究

文献 [4] では PAYL というマルウェア検知システムが提案された。PAYL はパケットからの特徴量の抽出に n-gram 解析を用い、学習フェーズでは、各ホストに対するパケットのポート、ペイロード長ごとに n-gram の出現回数の平均と標準偏差を計算しモデルとして記録する。テストフェーズでも同様に、検知対象のパケットのペイロードにおける n-gram の出現回数を計算し、そのパケットのポート、ペイロード長に該当するモデルとのマハラノビス距離を測定し、閾値以上であれば異常として検出する。

文献 [5] ではマルウェアに感染した機器が C&C サーバとの通信を行う際のパケットのペイロード情報が正常通信の場合と異なる特徴を持つことが述べられている。その異なる特徴の一つとしてペイロード内の ASCII 文字コードの出現頻度が挙げられており、n-gram 解析によるペイロードからの特徴量を抽出することはマルウェア検知に有効であると結論付けている。本研究の提案システムにおける特徴量の抽出にはこの n-gram 解析を採用した。

文献 [6] では、n-gram を改良した 2v-gram 法によって特徴量の抽出を行い、その特徴量を教師なし機械学習手法である OCSVM を用いて学習し検知を行うシステムを提案している。同文献では、ペイロードの解析と OCSVM を組み合わせることで良好な結果が得られており、当研究においても n-gram 解析と OCSVM を組み合わせた特徴量の抽出方法を採用した。

3. 提案手法

本研究では、n-gram 解析と OCSVM を組み合わせ、IoT デバイスの正常通信とマルウェア感染後の異常通信を識別するシステムを提案する。また、OCSVM を適用する際に、人間の手によって任意に設定されるパラメータを、今回は GridSearchCV を用いて最良のパラメータを算出するシステムを提案する。

3.1 実装環境の想定

IoT 機器は、一般的に低コストかつ省電力であり、機器には最小限のハードウェアリソースしか搭載されていないことが多い。そのため、セキュリティ対策のために機器個別にシステムを実装するのではなく、ゲートウェイなどの中継機器や、クラウド上に実装することが現実的であると考える。図 1 に、本研究で想定する IoT ネットワークを示す。

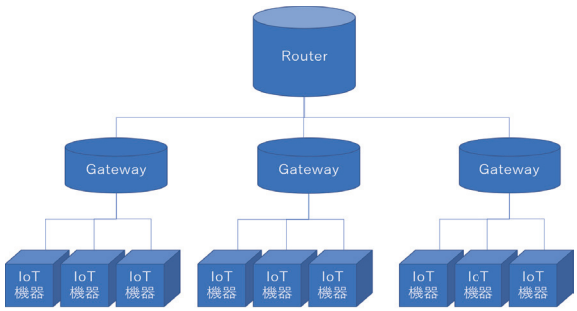

図 1. 想定する IoT ネットワーク

3.2 提案システム

3.2.1 アノマリ型検知システム

近年「Mirai」の亜種である IoT マルウェアが急増している背景を鑑みて、今回は未知のマルウェアにも対応が可能なアノマリ型検知を採用する。

3.2.2 n-gram 解析による特徴量抽出

本研究では、機械学習に用いる特徴量を n-gram 解析によって行う。n-gram 解析による文字列の分割例を以下に示す。

文字列: 太郎はご飯を食べた

$N = 2$**(2-gram):** 「太郎」「郎は」「はご」「ご飯」「飯を」「を食」「食べ」「べた」

$N = 3$**(3-gram):** 「太郎は」「郎はご」「はご飯」「ご飯を」「飯を食」「を食べ」「食べた」

n-gram 解析は任意のテキストから n 個の単語を切り出し、切り出した文字列・単語の出現頻度を求めることで、テキスト中の任意の文字列の出現頻度パターンを得られる。

文献 [5] の通り、n-gram 解析によって通信パケットのペイロード情報から特徴量を抽出することの有効性が示されていることから、n-gram 解析を採用した。具体的には、パケットのペイロード内の n 個の連続したバイト列の出現頻度から出現回数の総和・平均・標準偏差を計算し、この 3 つを機械学習における入力データとする。n-gram 解析の特性上、N の値を大きくするほど計算量の増加と精度の低下が見られることから、提案手法では 2-gram 法により特徴量を抽出する。

3.2.3 One-ClassSupportVectorMachine

OCSVM は、テキスト分類において n-gram 解析と組み合わせると良好な精度を示すことが文献 [6] でも証明されていたため、今回は OCSVM を採用して異常トラフィックを検出する。

OCSVM は教師無し学習による 1 クラス分類手法であり、正常データのみを用いて 1 つのクラス分の学習を行う点が Support Vector Machine(以下 SVM) と大きく異なる。OCSVM では、学習に用いた正常データをクラスタ “1” に分類し、原点のみを “-1” に属するカーネルトリックと呼ばれる手法を用いて、高次元の特徴空間へデータを写像する。学習した正常データは原点 (クラスタ “-1”) から遠くに配置され、学習した正常データと類似しないデータは原点近くに配置されるため、この性質を用いて正常・異常データの区別を行うものとなっている [7]。カーネルトリックによる写像を図 2 に示す。

通常の SVM では複数クラスのデータを学習データとして用いることから、分類器としての役割を強く持つのに対して、

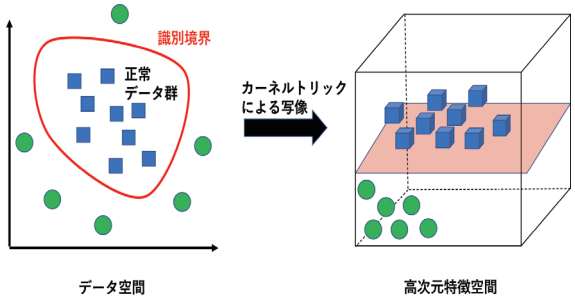

図 2. カーネルトリックによる高次元特徴空間への写像

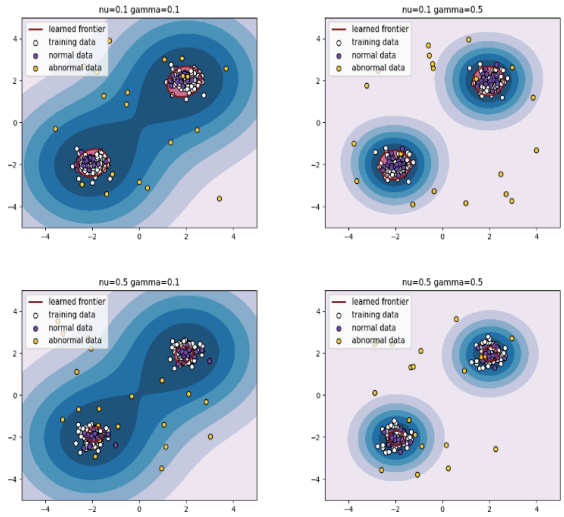

図 3. パラメータ変動

正常データのみ学習して識別境界を生成する OCSVM は、正常・異常データを識別する外れ値検知手法としての役割を強く持つ。

3.2.4 GridSearchCV によるパラメータ選定

本研究では、人間の手で任意に設定されるハイパーパラメータを scikit-Learn の標準ライブラリとして備えられている GridSearchCV を使い、機械学習によって自動で最適なパラメータの算出が可能か検証する。検知精度の向上を図る上で、OCSVM のパラメータである γ 値と ν 値は検知精度を左右する重要な要素となる。γ 値はサポートベクトルの識別境界の複雑さを決め、ν 値は外れ値の割合の下限を決めるパラメータである。scikit-learn 公式 [8] を参考にして作成した γ 値と ν 値のパラメータによる変動を図 3 に示す。良好な結果を得るためにはハイパーパラメータをその都度設定し直してモデルの学習・予測を行う必要があるため、試行回数が多くなるほど時間消費が激しくなり、作業効率が悪くなる。また、OCSVM のパラメータチューニングについては文献等が見当たらず、一般的には γ 値、ν 値共に 0.001、0.01、0.05、0.1、0.5 といった値で 5*5 の 25 組でチューニングすることが慣例である。今回は、OCSVM に GridSearchCV を適用し、自動で得られたパラメータを設定することで検知精度の向上が見られたか検証する。

3.3 提案システムの流れ

提案システムの流れは、特徴ベクトル抽出・パラメータ選定・学習・テストの 4 つのフェーズに分割される。

表 1. 良性シナリオ詳細

データセット名	キャプチャ期間	パケット数	デバイス名
CTU-Honeypot Capture-7-1	1.4(hrs)	8,276	SomfyDoorLock
CTU-Honeypot Capture-4-1	24(hrs)	21,000	PhilipsHUE
CTU-Honeypot Capture-5-1	5.4(hrs)	398,000	AmazonEcho

3.4 特徴ベクトル抽出

データの前処理として、n-gram 解析による特徴量抽出を行う。最初にペイロード内のバイト列を文字列として見なし、2-gram を生成する。その後、2-gram の出現頻度をカウントし、出現回数の総和・平均・標準偏差の 3 つを 1 パケットの特徴ベクトルとして抽出する。抽出した特徴ベクトルを元に、以降のフェーズへ移る。

3.5 パラメータ選定

GridSearchCV 関数に引数として、モデル (OCSVM) とパラメータ (γ 値と ν 値) の探索範囲、前フェーズで抽出した特徴ベクトルの中から任意の数のデータと正解ラベル (正常 “1”、異常 “-1”) を渡してグリッドサーチを実行する。実行後、返ってきたパラメータをモデルにセットし、次段階のフェーズへ移行する。

3.6 学習フェーズ

OCSVM の学習フェーズでは、正常データの特徴ベクトルのみを学習する。この段階の学習により、正常値と異常値を区別するための識別境界を生成し、正常クラスの領域を設定する。

3.7 テストフェーズ

テストフェーズでは、正常・異常データ両方の特徴ベクトルを用いて予測を行う。予測した特徴ベクトルが正常クラスの領域内に分類された場合、そのパケットは正常と判定され、領域外に分類された場合は異常と判定する。

4. 評価実験

4.1 実験目的

GridSearchCV により算出したパラメータを設定し、慣例的なパラメータを設定した際の OCSVM と比較して、検知精度が向上したかを検証する。

4.2 データセット

IoT 通信トラフィックのデータセットは StratosphereLab より IoT-23[9] を使用した。このうち、良性 3 種 (表 1)、悪性 1 種 (表 2) のシナリオを用いて検証を行う。良性シナリオはモデルの学習用とテスト用に分割する必要があるため、今回は良性シナリオのうち、8 割を学習データとして学習させる。そして、検知精度を測定する際には、残りの 2 割の良性シナリオと全悪性シナリオをテストデータとしてモデルに予測させる。

4.3 パラメータチューニング

本研究でのパラメータチューニングは、グリッドサーチ法を採用した。グリッドサーチ法では、指定した範囲内のハイ

表 2. 悪性シナリオ詳細

データセット名	キャプチャ期間	パケット数	マルウェア名
CTU-Malware Capture-34-1	1.4(hrs)	8,276	Mirai

表 3. 評価指標の詳細

指標		説明
TP	真陽性	異常を異常と判別
FP	偽陽性	正常を異常と判別
TN	真陰性	正常を正常と判別
FN	偽陰性	異常を正常と判別

表 4. 慣例のパラメータによる検知精度

γ 値	ν 値	ACC	TPR	FPR
0.01	0.1	92.56%	93.29%	8.72%
0.01	0.001	90.78%	89.12%	8.49%
0.1	0.01	88.83%	90.99%	16.23%
0.01	0.01	85.44%	85.81%	14.01%
0.1	0.05	84.26%	89.76%	16.87%

表 5. 導出したパラメータによる検知精度

γ 値	ν 値	ACC	TPR	FPR	与データ総数
0.093	0.16	89.16%	87.93%	12.12%	5100(正:5000)
0.079	0.05	93.78%	91.40%	8.92%	4100(正:4000)
0.007	0.02	93.01%	90.45%	9.34%	3100(正:3000)
0.03	0.05	87.38%	75.89%	7.69%	2100(正:2000)
0.006	0.02	77.94%	70.57%	22.50%	1100(正:1000)

パーパラメータの全ての組み合わせに対して学習を行い、最も良い精度 (汎化性能) を示したパラメータを採用する。パラメータの選定方法としては他にも、チューニングするパラメータとそのパラメータが従う分布・探索を行う回数を指定してランダムに探索を行うランダムサーチ [10] や、少量のデータでもガウス回帰に従ってパラメータを導出可能なベイズ探索 [11] などがあるが、今回はモデルに学習させる為の大量のデータを準備出来た点、探索範囲の調整が容易な点を加味してグリッドサーチ法を採用する。

4.4 評価

4.4.1 評価指標

本実験では正常を Negative、異常を Positive とし、以下の指標を用いて評価を行う。評価指標の詳細については表 3 にて示す。

$$Accuracy(ACC) = \frac{TP + TN}{TP + FP + TN + FN} \quad (1)$$

$$TruePositiveRate(TPR) = \frac{TP}{TP + FN} \quad (2)$$

$$FalsePositiveRate(FPR) = \frac{FP}{FP + TN} \quad (3)$$

4.4.2 実験結果

慣例的な γ 値・ν 値 25 組の検知精度を図り、その中から高い検知精度を示した 5 組を表 4 に示す。

一方、提案手法で得られた値で検知した結果を表 5 に示す。今回のパラメータ探索では、GridSearchCV に渡すデータのうち異常データを 100 個で固定し、正常データを 1000 個ずつ増やして 5 回検証を行った。

最初の 4 回は GridSearchCV に与えるデータの数が多くなるほど検知精度の向上が見られ、与データの総数が 4100 個 (正常データ 4000 個、異常データ 100 個) のとき、ACC が 93.78%と最も良い精度を示した。

表 4 と表 5 を比較すると、慣例のパラメータを設定した際の最良の検知精度が 92.56%なのに対し、GridSearchCV により導出したパラメータを設定した際の最良の検知精度が 93.78%と精度の向上を確認出来た。

4.5 考察

総データ数 4100 個から正常データを 1000 個増やして 5100 個 (正常:5000 個、異常:100 個) で探索し、導出したパラメータを扱うと検知精度の低下が確認された。これは、GridSearchCV に渡す異常データの数を 100 個で固定したまま正常データの数を増やしたことから、データの割合が偏り、検知精度の低下を引き起こしたと推察する。本実験では、チューニングしたパラメータによる検知精度の測定回数が僅か 5 回と少なかったことから、GridSearchCV に与えるデータの総数・割合と検知精度の因果関係については詳しく追求出来なかったため、本研究の今後の課題といえる。

5. まとめ

本研究では、n-gram 解析と OCSVM を組み合わせた IoT マルウェア検知システムを提案した。さらに、提案システムの検知精度を向上させるため、OCSVM のパラメータである γ 値と ν 値を自動で最適化するための手法として、GridSearchCV による OCSVM のパラメータチューニングを提案した。

実験では、慣例的に用いられるパラメータ 25 組による検知精度と、GridSearchCV を用いてチューニングしたパラメータによる検知精度の比較を行った。実験の結果、慣例的な値を使った場合よりも、提案手法でチューニングした値の方が良好な検知精度を示した。しかし、GridSearchCV に与えるデータの総数を増やしていく過程で、かえって検知精度が低下した場面があった。今後の課題として、GridSearchCV に渡す正常・異常データの割合・総数を変更して検知精度の向上・低下を観察し、検知精度が低下した原因を追究する必要があると考える。

参考文献

1) OracleNewsConnect:https://dyn.com/blog/dyn-analysis-summaryof-friday-october-21-attack/, (2021/01/17 閲覧)

2) Q.D.Ngo, H.T.Nguyen, V.H.Le, D.H.Nguyen: A survey of IoT malware and detection methods based on static features、ICTExpress、Volume6、Issue4、pp。280-286、2020.

3) https://www.nict.go.jp/press/2019/02/06-1.html, (2021/01/20 閲覧)

4) Wang, Ke. and S. J. Stolfo: Anomalous payload based network intrusion detection、RAID, Vol. 4, 2004.

5) 大月優輔, 市野将嗣, 川元研治, 畑田充弘, 吉浦裕: マルウェア感染検知のためのトラヒックデータにおけるペイロード情報の特徴量評価, ComputerSecuritySymposium, 2012.

6) R. Perdisci, G. Gu. W. Lee：Using an Ensemble of One-ClassSVM Classifiers to Harden Payload-based Anomaly Detection Systems、Proceedings of the 6th IEEE International Conference on Data Mining(ICDM2006), pp. 488-498, 2006.

7) https://hktech.hatenablog.com/entry/2018/10/11/235312, (2021/01/25 閲覧)

8) https://scikit-learn.org/0.19/auto_examples/svm/plot_oneclass.html, (2021/01/26 閲覧)

9) https://www.stratosphereips.org/datasets-iot23, (2020/12/18 閲覧)

10) https://aizine.ai/glossary-gridsearch/, (2021/01/22 閲覧)

11) https://wak-tech.com/archives/1775, (2021/01/23 閲覧)