L-007

PSD と機械学習による複数 DoS 攻撃パターンを考慮した攻撃検知
DoS Attack detection considering multiple patterns by PSD and machine learning

椙村 駿平† 関谷 勇司‡
Shumpei Sugimura Yuji Sekiya

1. はじめに

近年、ネットワークにつながるデバイスが増加するに伴い、サービスを妨害するための様々な攻撃が発生している。中でも、DoS 攻撃は組織的に行われ防御が難しいため、被害が拡大する傾向にある。DoS 攻撃には様々な種類があり、特に発見と防御が難しい攻撃として、低レート DoS 攻撃があげられる。この攻撃は通常の通信と判別がつきにくく、攻撃を検出することが難しい。また実際にセキュリティ対策を行う際には、やみくもに検出率を上げることだけを目指すのではなく、システム全体としての検出率と効率のバランスが求められる。

本研究では、閾値設定により攻撃の疑いのある通信を検出し、その通信を機械学習により精査することによって、実際のシステムに適用可能な複数種類の DoS 攻撃検出手法を提案する。

2. 先行研究

先行研究として、フーリエ変換を利用し 1 秒あたりの通信回数から PSD エントロピーを求め閾値として利用する手法[1]がある。この手法では、NSL-KDD[2]という攻撃データセットを利用している。NSL-KDD データセットは 1999 年に作成されたデータセットであり、現在では対策された攻撃や主流でない攻撃が多く含まれている。先行研究では DoS 攻撃の一種である smurf 攻撃について検知を行なっていた。

先行研究の手法について説明する。はじめに、通信回数から求められる PSD エントロピーによる閾値判別を行う。PSD(パワースペクトル密度)は、元のデータにフーリエ変換を行うことで求められる。以下に PSD の算出方法を示す。

$$PSD = \lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T} x(t)^2 dx$$

算出対象のデータに加え前後の 4 つのデータを使用し PSD の算出を行い、得られた PSD をエントロピー化し利用する。エントロピーの算出方法を以下に示す。

$$E = -\sum PSDk * \log(PSDk)$$

このように先行研究では、得られた PSD エントロピーに閾値を設定することによって、攻撃の疑いがある通信かどうかの判別を行っている。さらに、攻撃の疑いがあると判断された通信は機械学習での精査を行う。このように閾値を設定することで、機械学習に入力するデータを減らしながら効率よく攻撃の検知を行うことを提案している。

しかし前述の通り、先行研究では NSL-KDD の古いデータセットを用いて検証を行っている。そこで本研究では、まず始めに先行研究の手法が最新のデータセットに適応可能かを検証した。

2.1 データセット

適応するデータセットには CICIDS2017[3]を使用する。CICIDS2017 は 2017 年に作成されたデータセットであり様々な攻撃が含まれている。本研究ではその中でも DoS 攻撃についての検知を行う。以下に含まれている攻撃ツールについて表 1 に示す。

表 1 CICIDS2017 に含まれる DoS 攻撃の種類

Denial of service (DoS)			
slowloris	Slowhttptest	Hulk	GoldenEye

CICIDS2017 には 4 種類の DoS 攻撃が含まれている。これらについて先行研究の手法が適応できるかを確認する。

2.2 閾値設定

新しいデータセットである CICISD2017 を用いて、先行研究と同様の手法で PSD エントロピーを算出し、先行研究の手法が適応できるかを検証した。なお NSL-KDD データセットでは 2 秒あたりの通信回数から PSD を求めていたのに対し、CICIIDS2017 データセットには 1 秒あたりの通信回数が含まれているため、1 秒単位のデータの前後 4 つのデータを含め PSD エントロピーを算出した。算出した PSD エントロピーによって、通常の通信と攻撃を識別可能か検証した。箱ひげ図によって閾値設定可能かを検証した結果を図 1 に示す。

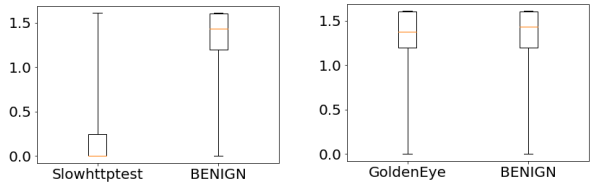

図 1 PSD エントロピーによる分布図

その結果、slowhttptest による攻撃は閾値によって識別可能であるが、GoldenEye による攻撃は閾値では判別できない可能性が高いことがわかった。よって先行研究による手法は、新しいデータセットにおいては特定の攻撃にしか適応できないことがわかった。そこで本研究では、新しいデータセットにも適用できるよう判別手法を改善した。

3. 提案手法

DoS 攻撃の判定に関しては、様々な要素が大きく影響していると考えられる。要素の一つとして、先行研究で扱われている通信回数があげられる。これは機械的な通信をする DoS 攻撃において重要な指標となる。そのほかにも通信容量に着目することができる。通信容量は DoS 攻撃において重要な要素であり、攻撃を行う際に大きな容量の方が効

† 東京大学大学院 工学系研究科
Graduate School of Engineering, The University of Tokyo.
‡ 東京大学大学院情報理工学系研究科
Graduate School of Information Science and Technology, The University of Tokyo

率的に攻撃を行えるなどの要素がある。しかし先行研究では通信容量を判定要素に導入していなかった。そこで本研究では、通信容量を PSD エントロピー算出に導入し、通常の通信と攻撃が分離できるかを検証した。図 2 に提案手法のフローチャートを示す。

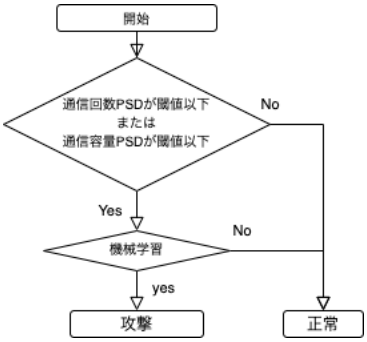

図 2　提案手法の流れ

まず閾値によるフィルタリングを行う。通信回数から求めた PSD エントロピーが閾値より小さい場合、または通信容量から求めた PSD エントロピーが閾値より小さい場合、その通信を攻撃の疑いがあると判定する。その後攻撃の疑いがあるとされた通信について機械学習での精査を行う。

3.1 閾値の設定

閾値の設定は、学習データから算出し設定した。今回提案する手法においては、閾値を通信回数から求めた PSD において正常な通信であるデータの第一四分位数（小さいデータのより 25%目）に設定した。同様に、通信容量から求めた PSD においては、通常の通信であるデータの第一四分位数を閾値として設定した。これらの設定より小さい値の通信について攻撃の疑いがあるとして機械学習での精査を行った。

3.2 機械学習

機械学習には NN(ニューラルネットワーク)を用いた。これは予備実験において、先行研究で利用されていた SVM よりも NN を利用した場合の方が優れた結果を示したため、NN を採用した。NN に入力する因子については先行研究[4]を参考に有効とされている 11 要素を選択した。また先行研究と同様に NN の構造は中間層 1 層の 10 ノードを持った 3 層とした。この NN により攻撃の疑いがある通信についての精査を行う。

4.　結果

47500 の通常通信のデータと 2500 の攻撃データをデータセット内からランダムに抽出し検証を行った。また検証方法には 5 回交差法を利用し、40000 の学習データと 10000 のテストデータに分割し検証した。この際学習データとテストデータそれぞれが 5%の攻撃データを含むように設計した。閾値設定が効果的に行われているかの実験結果を表 2、表 3 に示す。表 2 は本研究が提案する通信回数と通信容量から算出した PSD エントロピーを閾値としたもの、表 3 は通信回数のみから算出した PSD エントロピーを閾値としたものである。なおどちらも同じ検査対象数になるように設定し実験を行った。

表 2　通信回数と通信容量の PSD エントロピーによる閾値設定

	Suspected Attack	Suspected Normal
Actual Attack	435.2	64.8
Actual Normal	3230.6	6269.4

表 3　通信回数 PSD エントロピーによる閾値設定

	Suspected Attack	Suspected Normal
Actual Attack	397.0	103.0
Actual Normal	3326.4	6173.6

本研究が提案する手法では、87.04%の攻撃を攻撃の疑いがありと判定できている。対して先行研究の手法では、と 79.40%の攻撃が判定されている。このように通信回数だけではなく通信容量からも閾値を設定することで、攻撃検知の正確性が向上した。

また 機械学習によって判別した結果について、表 4 に示す。

表 4　提案手法での精度

	Predicted Attack	Predicted Normal
Actual Attack	3.75%	1.24%
Actual Normal	0.92%	94.90%

表に示すとおり、手法全体としての検知精度は 98.47%となった。NN に全ての通信を検査させた場合の精度は 98.85%である。閾値によるフィルタリングを設定した場合だと 75.16%の攻撃の通信が正しく検知できている。このように閾値設定を利用することで効率よく攻撃を検知できていることが確認できた。

5. おわりに

本研究では、PSD エントロピーを用いた閾値設定が多種の DoS 攻撃についても適応可能か検証を行った。その結果、限られた DoS 攻撃についての検知のみに有効であるとわかったため、通信容量を導入した PSD エントロピーを閾値する手法を提案した。その結果、複数の DoS 攻撃検知が可能になった。今後は閾値設定について、検知率と検査数のバランスが最適になる値の検証を行う。

参考文献

[1] N. Zhang, F. Jaafar and Y. Malik, "Low-Rate DoS Attack Detection Using PSD Based Entropy and Machine Learning", 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 59-62, 2019.

[2] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, “A Detailed Analysis of the KDD CUP 99 Data Set,” Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 2009.

[3] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018

[4] Osman Ali, Paul Cotae, “Towards DoS/DDoS Attack Detection Using Artificial Neural Networks”, 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2018.