テーマ番号	1EP17			
プロジェクトテーマ	和文	廉価で導入が容易な IoT 機器のセキュリティシステムに関する研究	指導教員	長田 茂美 教授
	英文	Research on security systems for IoT devices that are inexpensive and easy to implement		
プロジェクトメンバー	4EP3-71 村上 慧 (MURAKAMI Satoru)			

Abstract Since there are few inexpensive security services for IoT devices, and IoT devices often use their own protocols, it is difficult to install security software for each device. In addition, IoT devices infected with malware are likely to participate in DDoS attacks, and if we can detect IoT devices conducting DoS attacks, we can detect IoT devices suspected of being infected with malware. In this paper, we propose a DoS attack detection system that uses IPFIX to transform the communication flow of communication devices including IoT devices connected to an access point, and uses incremental learning to improve the accuracy of the learning model.

Keywords security, IoT, neural network, deep learning, CNN, LSTM.

1. はじめに

近年，IoT 機器の導入台数は急激な増加傾向にあり，世界に普及している IoT 機器が 2023 年には 340.9 億台になる見通しがなされている[1]. それに伴い，IoT 機器を狙ったサイバー攻撃も増加傾向にあり，1 年間に観測されたサイバー攻撃の回数は 2017 年から 2020 年にかけて約 3.3 倍になっている[2]. サイバー攻撃の一種である，マルウェア感染を受けた IoT 機器は，DDoS 攻撃などに利用され，二次被害が出てしまう可能性がある. そのため IoT 機器にセキュリティ対策を講じる必要があるが，IoT 機器はセキュリティソフトが対応していないものが多く，構造的に直接セキュリティソフトをインストールすることは難しい. また，セキュリティ製品の多くは高価で設置負荷が大きいため導入しにくい. そのため多くの IoT 機器は製造元のセキュリティ機構に依存したものとなっているが，製造元によっては，セキュリティ機構を施していない製品や，長期間のサポートがなされていない製品が多く，古いセキュリティ機構を使用している場合，脆弱性が突かれたときに個人情報が流出する恐れがある.

冒頭で述べたように IoT 機器がマルウェアに感染している時の 1 つの特徴として， DDoS 攻撃に参加するという挙動が多く見受けられる. そのため Access Point (AP)に接続されている機器の内，DoS 攻撃を行っている機器の存在が確認できればその AP 下の IoT 機器がマルウェアに感染している可能性が高いことがわかる.

そこで本論文では，導入を容易にする足掛かりとして，DoS 攻撃に対する IoT セキュリティシステムの作成を目的として，深層学習に基づく DoS 攻撃検知システムを提案する. また，システム稼働時にもデータの収集，学習を行えるようなシステムを設計することで，稼働するたびに DoS 攻撃に対する検知精度が上がっていくシステムを構築した.

2. 提案システム概要

図 1 に提案システムの全容を示す. 提案システムで使用する機器は赤枠で囲まれたレイヤ 2 スイッチと検知マシンである. レイヤ 2 スイッチにはポートフォワードという設定がされている. これはレイヤ 2 スイッチに接続されている AP の通信フローを検知マシンに中継するものである. レイヤ 2 スイッチで中継された通信フローは，検知マシン内で，yaf を用いて IPFIX 形式のパケット群を取得する. IPFIX とは通信フローを，分析が容易な形式に変換したものである. ここで IPFIX に変換されたパケット群は事前に学習されたモデルの増分学習に使用される. 増分学習とは学習済みのモデルの重みを初期値として，さらに学習を進める手法である.

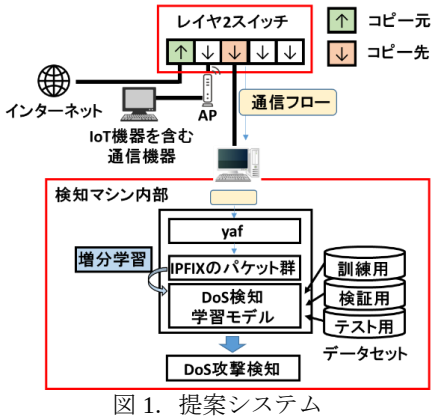

図 1. 提案システム
Fig.1 Proposed system

2.1 提案システムにおける学習モデルの構造

図 2 に提案システムにおける学習モデルの構造を示す. まず，一定量のパケット群(N 個)から「送信バイト数(標準化済み)」「受信バイト数(標準化済み)」「プロトコル」「パケットの送信時刻を 1 日で正規化した値(1)」の 4 つの要素を抜き出す. (1)の式の T は 0 時 00 分からパケットの総信時刻が経過した秒数を表しており，R は正規化された値を表している.

$$R = \frac{T}{(24 * 60 * 60) + (60 * 60) + 60} \quad (1)$$

ここで，4 つの要素を抜き出したパケット群の全体の個数が P 個となるように 0 パディングを行う. P の値は正常/異常データの N の値を見て常に P<N となるような値をユーザが決定する. 次に 0 パディングをしたパケット群に対して CNN で畳み込みを行い LSTM に入力し，その出力結果を全結合層に入力する. 全結合層の出力は活性化関数である sigmoid を用いて 0 から 1 の間の値で出力する. 正解ラベルは，正常は 0，異常は 1 である

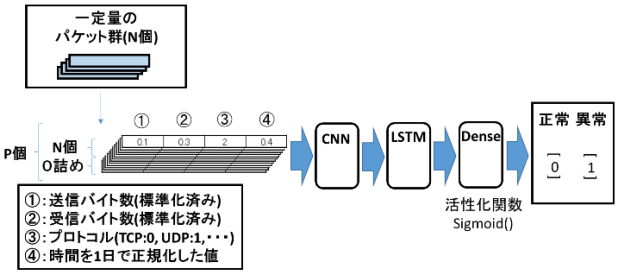

図 2. 学習モデルの構造
Fig.2 Structure of the learning model

3. データセットの収集

図 3 にデータセットの収集環境を示す．収集するデータはレイヤ 2 スイッチで観測される通信フローとする．その内, 正常データは監視カメラやその他通信機器のパケット群を観測したものであり, 異常データは攻撃用ラズベリーパイから DoS 攻撃用やられサーバに対して攻撃が行われている際のパケット群を観測したものである．

また，DoS 攻撃は SYN フラッド攻撃，FIN フラッド攻撃，ACK フラッド攻撃の 3 種類を用いる．これらは 10000 マイクロ秒(=0.01 秒)でパケットを送信しており，送信元はランダムな IP で偽造している．

収集したデータ量はそれぞれ SYN フラッド攻撃のデータが 3 日分，FIN/ACK フラッド攻撃のデータが 1 日分，正常データが 7 日分である．

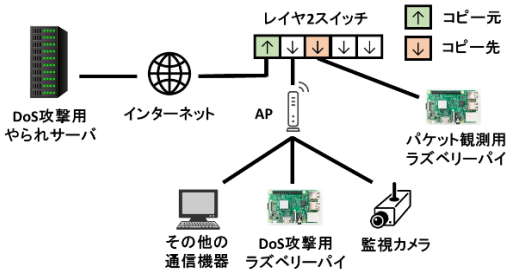

図 3. データセットの収集環境
Fig.3 Data set collection environment

4. 評価方法

図 4 に評価方法の概要を示す．事前学習には学習データとして，正常データと異常データである SYN フラッド攻撃のデータ 1 日分を用意する．また検証，評価データとして正常データと SYN フラッド攻撃のデータをそれぞれ半日分用いる. 増分学習には学習データとして正常データ 1 日分を、評価データとして正常データと異常データである SYN/FIN/ACK フラッド攻撃のデータ 1 日分用いる．増分学習の学習データは毎日異なるデータを用いる。評価データは同じデータを用いる．また，学習モデルの作成と増分学習はデスクトップパソコンを用いて行った．

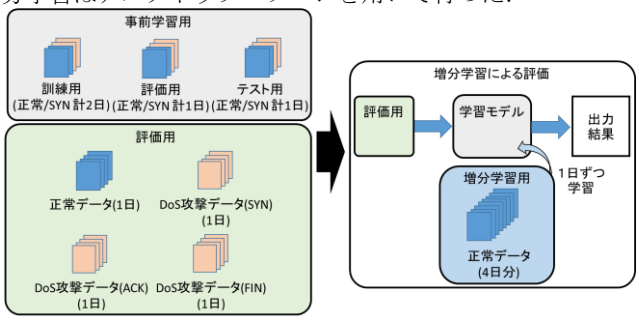

図 4. 評価方法の概要
Fig.4 Data set collection environmen

学習モデル作成の際に用いられる 3 つのデータは 4000 パケットごとに重複なく切り出されており, 深層学習の入力はこの切り出されたパケット群を用いて行う．さらに 2 日分の正常データと SYN フラッド攻撃のデータに含まれる送信バイト数と受信バイト数は標準化されており, 標準化パラメータは増分学習後の評価で使われる 3 種類の DoS 攻撃データと正常データにも使用する．

評価結果は正解率と再現率で評価しており，正常/異常の判断は閾値を用いて分類する. 評価に正解率と再現率を用いているのは, 全体としての DoS 攻撃の検知率と, 個々の正常/異常データの DoS 攻撃検知率を見るためである．

この評価は，実運用開始から 4 日間正常データのみ収集され, その正常データを全て増分学習に回したという状況を想定している．

4.1 評価結果

今回，増分学習を行うために作成した学習モデルは過学習がひどく，検証用データをすべて nan と判断した．nan とは未定義な値を表すものである．つまり今回作成した学習モデルは最低限の検知も行えないものであることが分かった．このような学習モデルが作成されてしまった原因は主に 2 つあると考えられる．

1 つ目の原因は特徴をうまく抽出できなかったことである．学習モデル作成時に損失関数の数値が動かないことが何度もあった．損失関数は正解からどれだけずれているかを表す関数であり，この値が変化してないということは，正解と異常の区別がついていないことが予測される．特徴をうまく抽出できていれば，このような区別がつかないという状況を防ぐことができる．得た情報から似たような情報を生成する GAN を用いて，異常データなどを疑似的に生成することができれば，生成する際に着目する特徴を抽出できるのではないかと考えた．

2 つ目の原因は学習用データが少なかったことである．学習モデルを作成する上で使用するデータセットの規模は検知精度に大きく影響する．今回用いたデータセットはとても少ないため，ただ学習させるだけでは検知精度が上がらないことは自明であり，データの前処理やニューラルネットワークの構造を工夫させる必要があった．また，複数の学習モデルを使用したアンサンブル学習などの手法は，少ないデータセットをより多角的な視点で判断することができ，検知精度を上げていくことができるのではないかと考えた．

5. おわりに

本論文では DoS 攻撃に対する IoT セキュリティシステムの作成を目的として，IPFIX に変換したパケット情報を活用し，深層学習に基づく DoS 攻撃検知システムを提案した. 今回の評価結果は学習モデルがうまく作成できなかったため，評価データの検証までできなかったが，4.1 で述べた GAN による特徴抽出や，アンサンブル学習を行うことで今回できなかった学習モデルの作成ができるようになるのではと期待される．また，今回の実験ではデスクトップパソコンで深層学習モデルの作成や DoS 攻撃の検知を行ったが, 今後はよりスペックの低いパソコンで学習や DoS 攻撃検知を行えるようなシステムへと改善していきたい．

参考文献

[1] 総務省，第 1 部　特集　デジタルで支える暮らしと経済，令和 3 年度版 情報通信白書，入手先 <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd105220.html> (参照 2022-1-10).

[2] サイバーセキュリティタスクフォース，ICT サイバーセキュリティ総合対策 2021，入手先 <https://www.soumu.go.jp/main_content/000761893.pdf>，(参照 2022-1-10).

[3] 阿久津　幹, 桑原剛希, 向井宏明, 横谷哲也，“サイバー攻撃検知を目的とした IoT ネットワークのトラフィック監視”，信学技報, vol. 118, no. 302, CQ2018-75, pp. 67-70

[4] 阿久津幹, 向井宏明, 横谷哲也, "制御ネットワークの異常検知に向けたトラフィック分析", 信学技報, vol. 119, no. 344, NS2019-159, pp. 133-138, (2019).

[5] Bifet, Albert, Ricard Gavaldá, Geoffrey Holmes, and Bernhard Pfahringer. Machine Learning for Data Streams with Practical Example in MOA. Cambridge, MA: The MIT Press, (2007).