機械学習を用いた未知 IoT デバイスの検出

Unknown IoT Device Detection Using Machine Learning

本山　潤　　三好　匠　　山崎　託　　シルバーストン　トーマス
Jun MOTOYAMA　　Takumi MIYOSHI　　Taku YAMAZAKI　　Thomas SILVERSTON
芝浦工業大学大学院理工学研究科
Graduate School of Engineering and Science, Shibaura Institute of Technology

1. まえがき

稼働中の IoT（Internet of things）デバイスを自動的に認識することはセキュリティの観点から非常に重要であり，複数のデバイスに対して機械学習を用いてデバイス分類を行う手法が多く提案されている．しかし，得られた学習モデルを用いて未知のデバイスを予測したり発見したりする手法は少ない．本稿では，多数の IoT デバイスが接続されているネットワークを想定し，機械学習を用いて未知 IoT デバイスの種類を分類する手法を提案する．

2. 従来手法

文献 [1] では，機械学習を用いて IoT デバイスを自動的に分類する手法が提案されている．本研究では，スマートスピーカー（Spk）1 台，室内カメラ（Cam）1 台，スマート電球（Blb）1 台，スマートプラグ（Plg）2 台の計 4 種目 5 種類の IoT デバイスのトラヒックを収集した．各デバイスが送受信するパケットの IP アドレスやポート番号，パケットサイズなどの分布からエントロピーを算出し，これらを特徴量として機械学習を用いることで，ランダムフォレストにより 94%の精度で分類できることを示している．

ここで，文献 [1] で使用されたデバイスのトラヒックデータを使用し，機械学習を用いて予測確率を求め時系列順に並べた結果を図 1，図 2 に示す．予測確率とは，機械学習の分類結果として出力される各ラベルに対して算出される確率である．実験に使用するすべてのデバイスを訓練データとして使用することで，図 1 のように該当するデバイスの予測確率がほぼ 100%となる．一方，訓練に用いなかったデバイスを分類しようとすると，図 2 のように予測確率にばらつきが生じ，未知デバイスの認識が難しいことが分かる．

3. 提案手法

本稿では，多数の IoT デバイスを含むネットワークにおいて，機械学習を用いて未知のデバイスを検知する手法を検討する．まず，あるデバイスから生成された時点 t $(t = 0,\ 1,\ 2\ ...)$ のトラヒックに対して，機械学習を用いて各出力ラベル l に対する予測確率 $P_l(t)$ を求める．時系列データの予測確率 $P_l(t)$ の変動を抑えるため，加重移動平均 $\hat{P}_l(t)$ を式 (1) により算出する．

$$\hat{P}_l(t) = \begin{cases} P_l(t) & (t = 0) \\ \alpha P_l(t) + (1-\alpha)\hat{P}_l(t-1) & (t > 0) \end{cases} \quad (1)$$

l に対する $\hat{P}_l(t)$ の最大値が閾値 φ 以上の場合は時点 t の出力ラベルを「l」とし，それ以外の場合は「未知デバイス」とする．これを所定の時間繰り返し，出力ラベルの個数を数える．個数が θ 以上で，かつ最大となる出力ラベルのデバイスを最終的な分類結果とし，それが存在しない場合は未知のデバイスとして分類する．

4. 提案手法の評価

提案手法の評価を行うために，実データによる分類実験を行った．実験では，Spk 1 台，Cam 1 台，Blb 1 台，Plg 4 台の計 4 種目 7 種類のデバイスを使用し，出力ラベルはデバイスの種目ごとに設定する．各デバイスのトラヒックデータを 24 時間分取得し，5 分ごとに分割して時系列データを作成した後，[1] と同様にエントロピーを算出したものを特徴量とする．前半の 70%（16.8 時間分）を訓練データとして使用し，Plg データの後半 30%（7.2 時間分）のみをテストデータとして使用する．学習モデルの作成には，ロジスティック回帰を使用する．訓練に用いる Plg デバイスの数を 1〜4 とし，$\alpha = 0.1$，$\varphi = 0.95$，$\theta = 10$ とした．

結果を図 3 に示す．図では，訓練に用いた Plg の数におけるすべての組合せに対して，Plg 4 台分のテストデータの分類結果の割合を示している．図 3 より，訓練に用いる Plg 数が増加すると，「Plg」と分類される割合が増加することが分かる．一方，訓練に用いる Plg 数が少ない場合には，Plg に属するデバイスのトラヒックが十分に学習されていないため，未知デバイスと分類される割合が高くなる．

5. むすび

本稿では機械学習を用いた未知 IoT デバイスの分類手法を提案し，評価を行った．今後は各デバイスの分析を行い，分類精度を向上させる予定である．

文献

[1] H. Nguyen-An, T. Silverston, T. Yamazaki, and T. Miyoshi, “IoT traffic: modeling and measurement experiments,” IoT, vol. 2, no. 1, pp. 140-162, Feb. 2021.

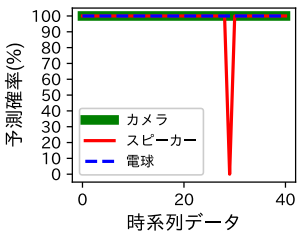

図 1　各デバイスに対応した予測確率の変化

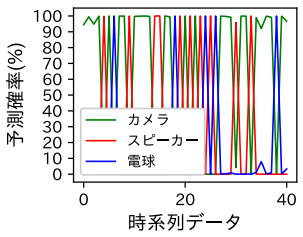

図 2　訓練されていないデバイスの予測確率の変化

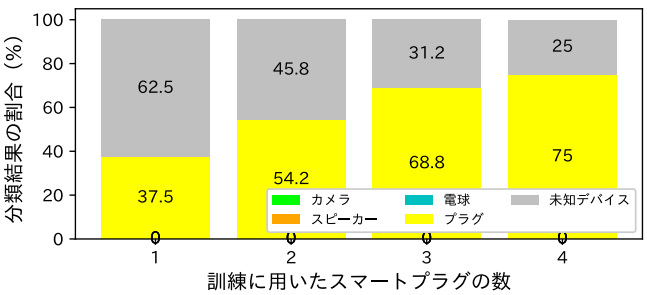

図 3　訓練に用いたスマートプラグの数に対する分類結果の割合