1W-04

無線 LAN 内でキャプチャした無線フレームを利用した IoT 機器一覧表示システム

江川悠斗† 谷口義明† 井口信和†

近畿大学理工学部情報学科†

1. 序論

Wi-Fi を用いてネットワークに接続するデバイス（以下，Wi-Fi デバイス）は，ノート PC などのモバイル端末と AI スピーカーなどの IoT 機器に分類される．モバイル端末と比較し，IoT 機器は設置したことを忘れるなど監視が行き届きにくく [1]，十分なセキュリティ対策が行われずに放置される場合がある [2]．このような IoT 機器は，サイバー攻撃の被害を受けるだけでなく，他のデバイスに危害を加えることもある [3]．これを防ぐためには，まず，無線 LAN に接続された IoT 機器が何台存在するか把握する必要がある．

そこで本研究では，無線 LAN に接続された IoT 機器の把握を支援することを目的に，無線 LAN 内でキャプチャした無線フレームを利用した IoT 機器一覧表示システム（以下，本システム）を開発した．本システムは，無線フレームの取得や分析が可能な Tshark を用いる．本システム上でキャプチャした無線フレームを Tshark で解析することにより，アクセスポイント(以下，AP)に接続された Wi-Fi デバイスの IP アドレスと MAC アドレスを取得する．また，Wi-Fi デバイスの送受信する無線フレームの頻度や制御フレームの割合に基づき，Wi-Fi デバイスをモバイル端末と IoT 機器に分類することで，IoT 機器の台数を把握する．本システムにより，無線 LAN に接続された IoT 機器の把握を支援できる．

2. IoT 機器一覧表示システム

本システムの概要を図 1 に示す．本システムは，ノート PC 上で動作する．また，モバイル端末や IoT 機器とそれらが接続された AP から構成される無線 LAN 内で動作することを想定する．

本システムの GUI を図 2 に示す．最初に，ユーザはノート PC を AP に無線で接続する．次に，ユーザがシステム開始ボタンを押下すると，本システムは，アドレス取得機能を用いて，同じ AP に接続される Wi-Fi デバイスの IP アドレスと

IoT Device List Display System Based on Captured Frames in Wireless LAN

†Yuto EGAWA, Yoshiaki TANIGUCHI, Nobukazu IGUCHI, Faculty of Science and Engineering, Kindai University

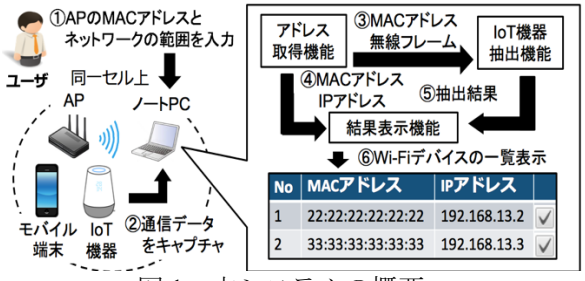

図 1：本システムの概要

図 2：本システムの GUI

MAC アドレスを取得する．そして，IoT 機器抽出機能を用いてモバイル端末と IoT 機器の分類を行う．最後に，結果表示機能を用いて，抽出した IoT 機器の接続数と IP アドレス，MAC アドレスを本システムの GUI の結果表示部に表示する．以下にそれぞれの機能について述べる．

2.1. アドレス取得機能

本機能は，Tshark でキャプチャした無線フレームを利用して AP に接続された Wi-Fi デバイスの IP アドレスと MAC アドレスを取得する機能である．本機能では，まず，airport コマンドと ifconfig コマンドを実行し，AP の MAC アドレスとネットワークの範囲を取得する．次に，送信元又は送信先 MAC アドレスが AP である無線フレームから，Wi-Fi デバイスの MAC アドレス一覧を取得する．そして，ネットワークの範囲に対して，ping コマンドと arp コマンドを実行し，ノート PC の ARP テーブルを取得する．ARP テーブルから，先に取得した MAC アドレスに対応する IP アドレスを取得する．本機能により，AP に接続された Wi-Fi デバイスの IP アドレスと

MACアドレスの一覧を取得できる．

2.2. IoT機器抽出機能

本機能は，Wi-Fiデバイスから IoT 機器を分類する機能である．本機能では，一定間隔毎の無線フレーム送受信回数を求め，その標準偏差，送受信のない期間の有無，管理フレームと制御フレームにおける種類毎のフレームの割合から，その Wi-Fi デバイスがモバイル端末か IoT 機器かを分類する．本機能により，APに接続されたIoT機器を抽出できる．

2.3. 結果表示機能

本機能は，APに接続されたIoT機器の接続数とIPアドレス，MACアドレス，チェックボックスを本システムのGUI上にある結果表示部に一覧表示する機能である．チェックボックスは，ユーザが各IoT機器を把握しているか確認するために用いる．本機能により，ユーザは把握していないIoT機器が存在するか確認できる．

3. 実験・考察

AP に接続された IoT 機器の情報をどれくらいの精度で取得可能か確認するために，性能評価実験を行った．実験環境として，実験用の AP とスマートプラグや AI スピーカーなどの IoT 機器 6 台，ノート PC やタブレット端末などのモバイル端末 14 台を用意した．実験で使用した PC のスペックは，OS:macOS Sierra(64bit)，CPU:Intel Core i5 1.6 GHz，メインメモリ:4GB である．

まず，本システムのアドレス取得機能を用いることにより，各 IoT 機器を個々に識別するために必要な IP アドレスと MAC アドレスをどれくらいの精度で取得可能か確認するために，IoT 機器とモバイル端末を AP に接続した状態で本システムを動作させ，各アドレスが正しく取得できるかを検証した．実験の結果，IP アドレスを 96.7%，MAC アドレスを 100%の確率で取得できることを確認した．この結果から，本システムは IoT 機器の各アドレスを高い精度で取得できることが分かった．しかし，一部の IoT 機器の IP アドレスを取得できないことが分かった．これは，本システムでは，一定期間フレームをキャプチャした後に，MAC アドレスに対応する IP アドレスを計測するのに対し，IoT 機器の中には，データ送信時のみ AP と接続を確立するものがあったためと考えられる．解決策として，無線フレームのキャプチャと並行して ping コマンドを発行することが挙げられる．これを行うことで，AP と IoT 機器が接続を確立した時に，IoT 機器の情報をノート PC の ARP テーブルに追加することができる．これにより，データ送信時のみ AP と接続を確立する IoT 機器の IP アドレスも取得できると考えられる．

表 1：IoT 機器 6 台とモバイル端末 14 台を AP に接続した場合の実験結果

回数		1	2	3	4	5	6	7	8	9	10
IoT 機器の表示台数		8	6	7	6	6	7	8	7	8	8
内訳	IoT 機器	6	6	6	6	6	6	6	6	6	6
	モバイル端末	2	0	1	0	0	1	2	1	2	2

また，本システムの IoT 機器抽出機能を用いることにより，AP に接続された IoT 機器をどれくらいの精度で抽出可能か確認するために，IoT 機器の抽出精度を計測した．IoT 機器 6 台とモバイル端末 14 台を AP に接続した状態で本システムを用いて 10 回の実験を行い，それぞれの実験で IoT 機器として分類された機器の台数を表 2 に示す．また IoT 機器として分類された機器のうち，実際に IoT 機器であったものとモバイル端末であったものの内訳をあわせて示す．表に示されるように，一部の実験でモバイル端末を IoT 機器として誤判定しているものの，全ての実験において AP に接続した IoT 機器を全て抽出できることを確認した．また AP に接続する機器数を変化させた場合も同様に，全ての IoT 機器を抽出できた．この結果から，本システムは 20 台までの Wi-Fi デバイスが接続された AP の場合，高い精度で IoT 機器を抽出できることが分かった．

4. 結論

本研究では，無線 LAN 内でキャプチャした無線フレームを利用した IoT 機器一覧表示システムを開発した．本システムは，APに接続されたIoT機器台数と IP アドレス，MAC アドレスを表示する．実験から，IoT 機器の一覧を高い精度で取得できることを確認した．これにより，無線 LAN に接続された IoT 機器の把握を支援できる．

今後は，IoT 機器の中で詳細な分類を行うことを可能とするために，IoT 機器抽出機能の拡張を行う予定である．

参考文献

1) 松井俊浩：IoT Security READY!! IoTのセキュリティの特性と人材育成，入手先<http://www.idec.or.jp/renkei/whats_new/6_iot_s_iwasaki_gakuen.pdf>(参照2018-11-8).
2) 半田富己男，矢野義博：IoTエッジ端末をボットネット化から防ぐ認証プラットホームの提案，情報処理学会研究報告，Vol.2017-CSEC-76，No.26，pp.1-3（2017）．
3) 中澤祐樹，佐々木良一，猪俣敦夫：野良IoTの地域特性の調査と分析，マルチメディア，分散協調とモバイルシンポジウム2017論文集，No.2017，pp.1138-1144（2017）．