1ZA-06

異種無線 LAN 構成における バックボーン遅延利用 Rogue AP 検出の追跡調査

熊谷 僚太† 嶋田 創‡

名古屋大学大学院情報学研究科† 名古屋大学情報基盤センター‡

1．はじめに

近年の無線 LAN 利用の増加に伴って，無線 LAN 環境のセキュリティ侵害への懸念に強く関心がもたれている．代表的なセキュリティ侵害に Evil Twin 攻撃という攻撃手法が存在する．Evil Twin 攻撃では，攻撃者は正規のアクセスポイント(AP)と同様の SSID を持つ偽物の AP(Rogue AP)を設置する．SSID が同一の AP が複数存在する場合，一見すると見分けがつかないため，無線 LAN 利用者が意図せず Rogue AP に接続した場合もそれを察知される可能性が低く，悪意のある DNS による偽サーバへの誘導や Man-in-the-Middle 攻撃などが可能となる．そのため，2019 年度に同一 SSID による Rogue AP の検出を目的とした，インターネット定点サーバまでの通信遅延と無線 AP までの遅延の差分(バックボーン遅延)のヒストグラムのコサイン距離をもとに Rogue AP を検出する研究が実施された[1]．

2019 年度の実験後，文献[1]の実験に使用した学内ネットワークは大幅なアップデートが施され，AP やルータの更新など大規模な改修が行われたため，AP 内での遅延を含むバックボーン遅延が異なった値となる．

そこで，本論文では 2019 年度の実験と同様の実験を実施し，以前の評価時から識別制度に変化があるかを追跡調査することを実験の目的とする．さらに，今回の実験では，前回の実験時には存在しなかった新しい世代(802.11ax)の AP についてもその有効性を調査する．

2．評価実験

2．1 実験概要

アップデートされた学内ネットワーク内に，Rogue AP を想定した AP を新たに設置し，既存の各 AP および各 AP が提供する SSID に接続した時のバックボーン遅延(2.2 節参照)を測定する．評価は文献[1]と同様に，「以前にある SSID に接続した時のバックボーン遅延の測定結果を用いて，後日に接続した時に正規の同じ SSID か(Rogue AP)で無いかを判別する」形を取り，後日に別 SSID(Rogue AP を想定)に接続して取得したバックボーン遅延との類似度，以前の別の SSID で得られたバックボーン遅延との類似度よりも高ければ良いとする．

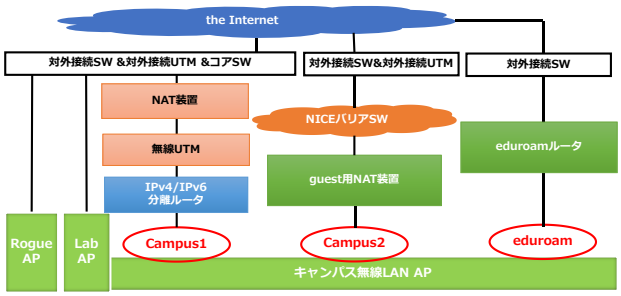

図 1 評価に用いたネットワーク構成

なお，文献[1]からの AP とネットワーク機器の変化は以下の通りである．

・Lab AP は 801.11n 世代から異機種の 802.11n 世代へ

・Rogue AP は 801.11a/g 世代から 802.11ax 世代へ

・Campus/eduroam の AP は 802.11a/g 世代から 802.11ac 世代へ，バックボーンのネットワーク機器にも更新あり

2．2 バックボーン遅延

文献[1]で提案された，バックボーン遅延による Rogue AP 識別方法とそれを利用した本追跡調査実験について説明する．

まず，AP からある定点サーバまでの遅延のことをバックボーン遅延と定義する(図 2)．本実験でのバックボーン遅延の測定には，図 2 のように端末から学外定点サーバまでの遅延(X)と，端末から AP までの遅延(Y)を同時に測定し，それらの差を計算するという方法を採用した．

バックボーン遅延は各 SSID ごとにそれぞれ 100 回ずつ測定し，バックボーン遅延から図 3 のグラフ部に示す遅延ヒストグラムを作成する．

Follow-up Survey of Backbone Delay Utilization Rogue AP Detection in Heterogeneous Wireless LAN Configurations

†Ryota KUMAGAI, Graduate School of Informatics, Nagoya University

‡Hajime SHIMADA, Nagoya University Information Technology Center

遅延ヒストグラムにおいてビンのサイズは可変としてあり，10ms 以下は 1ms 単位，10ms から 30ms は 2ms 単位，30ms から 50ms は 5ms 単位，50ms から 100ms は 10ms 単位としてある．これに 0ms 以下(測定誤差)と 100ms 以上を加えた 31 階級からなる遅延ヒストグラムを作成する．

最後に，得られた遅延ヒストグラムを 31 次元のベクトルとみなして異なる日や異なる SSID から得られた遅延ヒストグラム間のコサイン類似度を計算したものを，本実験の評価結果とした(図 2 中央の計算式部)．なお，コサイン類似度に用いたコサイン距離計算式を式(1)に示す．

$$\cos(a,b) = \frac{a \cdot b}{||a||||b||} = \frac{\sum_{i=1}^{n} a_i b_i}{\sqrt{\sum_{i=1}^{n} a_i^2}\sqrt{\sum_{i=1}^{n} b_i^2}} \quad (1)$$

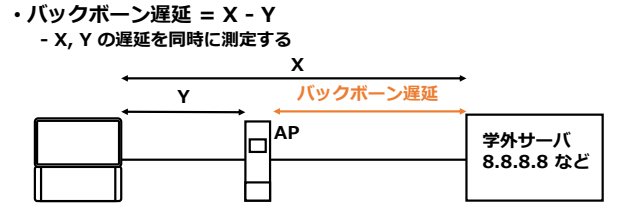

図２ バックボーン遅延

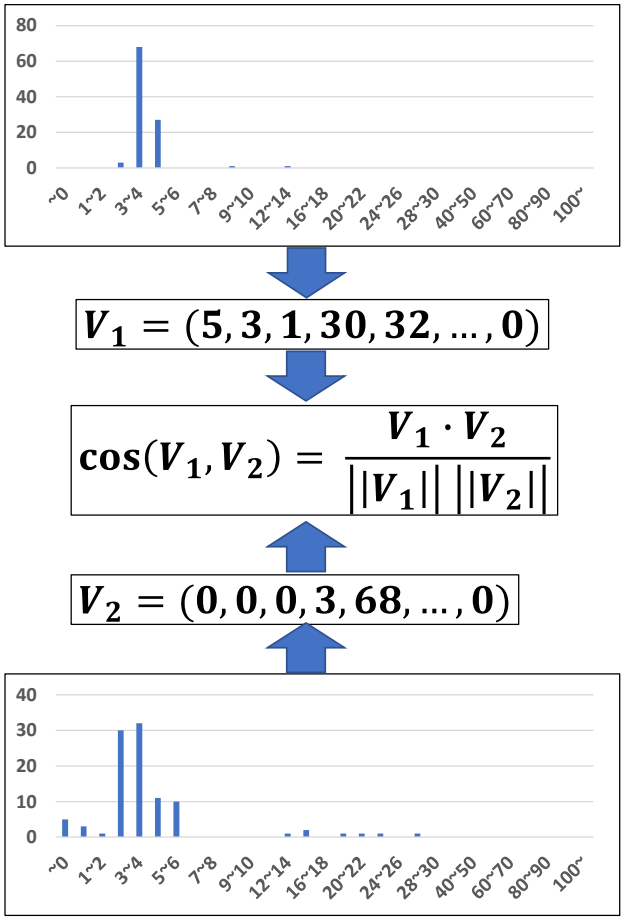

図３ 遅延ヒストグラムのコサイン類似度の算出

３．実験結果

実験結果を一部抜粋したものを図 4 に示す．図の各行は 1 月 10 日 13 時台に計測した遅延ヒストグラム，各列は 1 月 11 日 13 時台に計測したデータを示し，表中の値は各組合せにおけるコサイン距離の値を示す．表は縦方向に見て，ある SSID の遅延ヒストグラムが先行する日の同一 SSID の遅延ヒストグラムと最も高い場合，判別を成功することになる．表から，おおむね同一の SSID(対角成分)のコサイン類似度が最も大きい値を取ることが分かる．例外は Lab AP であり，Rogue AP との類似度が最も高くなってしまった．これは，図 1 に示すように，Lab AP と Rogue AP は同一の有線バックボーン上にある別体の AP から提供されているため，バックボーン遅延が似やすいためである．有線バックボーンを共有する別体の AP の類似性が高く判別が難しいことについては，文献[1]でも示されている．

	Lab AP	Rouge AP	Campus1	Campus2	eduroam
Lab AP	0.9466	0.8835	0.7682	0.9583	0.9152
Rouge AP	0.9950	0.9693	0.6048	0.9409	0.9023
Campus1	0.7998	0.7897	0.9126	0.8752	0.8688
Campus2	0.9521	0.8962	0.8185	0.9962	0.9715
eduroam	0.8832	0.8927	0.8580	0.9570	0.9902

図４ 実験結果

４．結論

本論文では，更新アップデートされたネットワークにおいても遅延ヒストグラムのコサイン類似度を用いて Rogue AP を検出可能かの追跡調査を行い，文献[1]と同様に Rogue AP の検出は可能であると言える結果を得た．以前の調査[1]に加え，環境が異なる今回の調査でも Rogue AP の検出は可能であったため，異種無線 LAN 構成において Rogue AP 検出のためにバックボーン遅延を利用する方法が有効である可能性がより高くなったと言える．

参考文献

[1] Ziwei Zhang, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada, ″Rogue AP Detection using Similarity of Backbone Delay Fluctuation Histogram,″ In Proceedings of the 34th International Conference on Information Networking *ICOIN2020*, pp. 239-244, January 2020.