

ユーザアクセス情報を用いた Evil Twin 攻撃検出手法

森田 雅也^{1,a)} 金井 敦^{2,b)} 谷本 茂明^{3,c)}

概要：スマートデバイスが普及し、近年では公衆無線 LAN 環境の整備も進んでいる。多くの場所で無料で Wi-Fi に接続できるのは便利である反面、様々なセキュリティ上の問題を伴う。正規の無線 LAN アクセスポイントを偽装して、誤って接続したユーザに対して様々な攻撃を行う Evil Twin 攻撃はその問題のひとつである。現在、Evil Twin 攻撃を検出する手法がいくつか提案されているが、完全な対策は確立されていない。本研究では、導入が簡単な新たな Evil Twin 攻撃検出手法として、RTT 分布に着目する方法と、GPS と RSSI の関係を利用した方法の 2 つ指標を組み合わせた手法を提案する。本手法の実現性について検討するためにそれぞれ実験を行った。RTT 分布の方は検出精度が 0.861 となり、GPS と RSSI の方では検出可能となる条件を見つけた。実験の結果はどちらも一定の有用性を示す結果が得られた。

キーワード： Evil Twin 攻撃, RTT, GPS, RSSI

Evil Twin Attack Detection Method Using User Access Information

MASAYA MORITA^{1,a)} ATSUSHI KANAI^{2,b)} SHIGEAKI TANIMOTO^{3,c)}

Abstract: In recent years, public wireless LAN environment has been improved. Although free Wi-Fi in a city is convenient, it comes with various security problems. One of the problems is Evil Twin Attack, which spoofs a legitimate wireless LAN access point and carries out various attacks against users who are mistakenly connected. Many methods for detecting Evil Twin Attack have been proposed. However, there are still no perfect methods. In this study, we propose a method for detecting Evil Twin Attack that is easy to deploy. It is a combination of two indicators: a method that focuses on RTT distribution and a method that uses GPS & RSSI relationships. We did experiments to examine feasibility. The accuracy of detection by RTT was 0.861, whereas I found the condition that can be detected by GPS & RSSI. Both results showed certain utility.

Keywords: Evil Twin Attack, RTT, GPS, RSSI

1. はじめに

スマートフォンやタブレットをはじめとするスマートデバイス（端末）の普及は続いている。当初、2020 年に予

定されていた東京オリンピックに伴って訪日外国人が増加し、公衆無線 LAN の利用もさらに高まると予測されていた。そこで総務省は数年前から地方の観光名所や博物館などを中心に無料 Wi-Fi を導入し公衆無線 LAN 環境の増強を進めている [1]。

例えば、駅、カフェ、ホテルといった場所で、無料で Wi-Fi に接続できるのは当たり前になった。Wi-Fi の利用は 4G や LTE などの携帯キャリア回線での通信量を気にせずに使えたりと便利であるが、様々なセキュリティ上の問題を伴う。正規の無線 LAN アクセスポイント（AP）に偽装し、誤って接続したユーザに対して様々な攻撃を行う Evil Twin 攻撃はその問題のひとつである。この問題

¹ 法政大学大学院 理工学研究科 応用情報工学専攻
Major of Applied Informatics, Graduate School of Science and Engineering, Hosei University

² 法政大学 理工学部
Faculty of Science and Engineering, Hosei University

³ 千葉工業大学 社会システム科学部
Faculty of Social Systems Science, Chiba Institute of Technology

a) masaya.morita.2p@stu.hosei.ac.jp

b) yoikana@hosei.ac.jp

c) shigeaki.tanimoto@it-chiba.ac.jp

への対策として認証サーバ (RADIUS サーバ) を用いる IEEE802.1X 認証の EAP 方式が考えられるが、コストが多くかかるなどの理由のため公衆無線 LAN にはあまり普及していない。時間や費用といったコスト的な問題で対策を講じていない無線 LAN も多く存在する。

現在では、コストが低い対策として、ユーザの端末から得られる情報のみで Evil Twin 攻撃を検出する手法が既にいくつか提案されている。しかし、汎用的な検出手法でない、ルータに制約がある時には適用できない、などの理由によりそれぞれ問題も残っていると思われる。本研究では、ユーザの端末のみで検出するという制限を無くし、Web アプリケーションのような形での検出手法を新たに提案する。この手法は導入が容易で、ルータの制約などに左右されない方法である。ここでの検出方法は、RTT 分布、GPS と RSSI の関係を利用する 2 つの指標があり、この 2 つを組み合わせる事もできる。この方法での検出が実現可能であるか調べるためにそれぞれ実験を行ったのでその結果を報告する。

2. 関連研究

Evil Twin 攻撃検出手法は既にいくつか提案されている。これらの検出手法を大別すると管理者側と利用者側に分けられる。AP などで攻撃を検出をする管理者側対策の多くはコストがかかる。対してユーザの端末のみで完結する利用者側対策はコストが低く抑えられる可能性が高く近年研究が進んでいる。ここでは主に利用者側での検出手法の関連研究について述べる。

Nikbakhsh らは文献 [2] で、SSID と MAC アドレスが同じ AP にそれぞれ接続し、その時のプライベート IP アドレスと traceroute の結果から Evil Twin 攻撃を検出する手法を提案した。しかし、例えば AP で ICMP パケットを禁止されている場合には動作しないなどの問題がある。Mustafa らは文献 [3] で、同じ SSID を持つ AP にそれぞれ接続し、まず始めにそれぞれの ISP 情報を得る。それが同じであれば Google などの公のサーバへ HTTPS 接続にかかる時間から RTT 値を 10 個ずつ得る。それらをウィンドウサイズ $h = 30\text{ ms}$ として MSC アルゴリズムというクラスタリングを適用する。この結果に 2 つ以上のクラスタがあった時に Evil Twin 攻撃と判定する検出手法を提案している。しかし、誤差も大きい RTT に対してウィンドウサイズを固定してクラスタリングするので汎用性があるのかなどの疑問が残る。Nakhila らは文献 [4] で、同じ SSID を持つ AP のひとつで SSL/TCP socket 通信を開始して、Web ページのダウンロード中に別の AP に切り替えた時にダウンロードが進行するかどうかで Evil Twin 攻撃を判定する検出手法を提案している。しかし、これだけだと複数の AP を同じ SSID で運用している場合は誤検出になってしまう。Song らは文献 [6] で、パケット間到着時間に着目

したアルゴリズムによる検出手法を 2 つ提案している。その一方の HDT アルゴリズムは検出精度が高く、かつ汎用性もある手法であるが、無線 LAN 規格ごとに事前学習が必要になる。その他には文献 [5][7][8] で、データフレーム流量、TCP termination での遅延時間、多量のネットワーク情報収集による Evil Twin 攻撃検出の可能性を示している。

以上の利用者側での対策は認証リストなどの事前情報を持たないで検出を実現させる必要があるといった制約が多く非常に難しい。本研究では、そのような制約をいくつか無くしたいと考え、Web サーバに AP 情報を事前に登録し、その情報を元にサーバ側で検出する Web アプリケーションを想定した検出手法を提案する。

3. Evil Twin 攻撃

Evil Twin 攻撃とは、攻撃者が正規 AP に偽装した不正 AP を設置し、ユーザに誤ってその不正 AP に接続させる攻撃である。その後、攻撃者はそのユーザの通信を盗聴したり、ユーザを不正サイトへ誘導してマルウェアに感染させたりする。ここでは Evil Twin 攻撃の仕組みについて説明する。

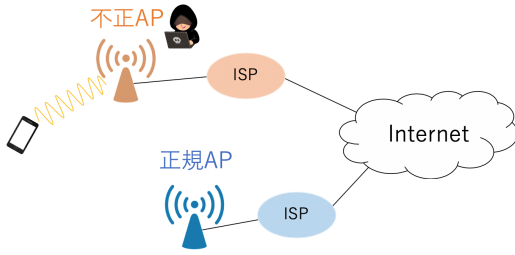
3.1 攻撃シナリオ

無線 LAN には、BSSID (Basic Service Set Identifier) と ESSID (Extended Service Set Identifier) の 2 つのネットワーク識別子を持つ。BSSID は基本的に AP の MAC アドレスが使用される。ESSID は任意の 32 文字以下の英数字で設定でき、これが無線ネットワークの識別名となる。一般に SSID と言われると ESSID を指す。無線 LAN クライアントは SSID を指定することで接続したい AP を選択できる。同じ SSID を持つ AP が複数ある場合はその中で最も電波が強い AP に接続する。Evil Twin 攻撃はこの性質を悪用してユーザを不正 AP に接続させることが多い。

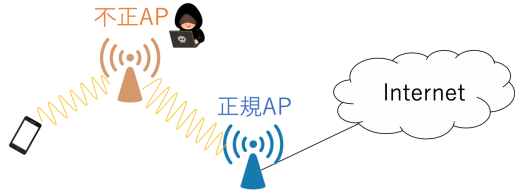
Evil Twin 攻撃シナリオにもいくつかのパターンがあるが、本研究では図 1 の 2 つの攻撃シナリオに絞って進める。図 1(a) は、攻撃者がモバイルルータや携帯回線などの独自回線を利用するシナリオである。これをタイプ 1 とする。図 1(b) は、通信を正規 AP に中継させるシナリオである。これをタイプ 2 とする。この時に不正 AP はルータまたはブリッジのような振る舞いをする。また当然この時に不正 AP は、正規 AP の電波が届く範囲に設置する必要がある。

3.2 RTT 分布について

タイプ 2 の攻撃シナリオの時、正規 AP と不正 AP で接続時の RTT (Round-Trip Time) に違いが生じることは既に指摘されている [3], [8]。実際にこれを調べるために Web サーバを用意して、不正 AP と正規 AP にそれぞれ端末を接続させて、それぞれの端末から Web サーバに HTTP



(a) 独自回線を使用する場合（タイプ 1）



(b) 正規 AP を中継する場合（タイプ 2）

図 1 Evil Twin 攻撃シナリオ

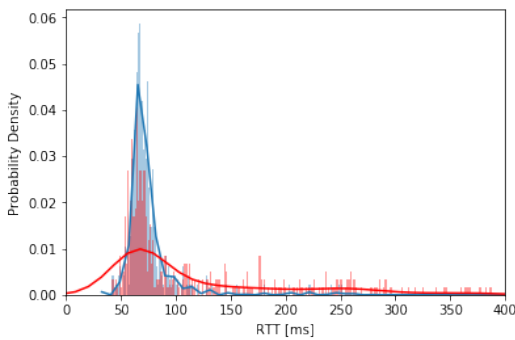


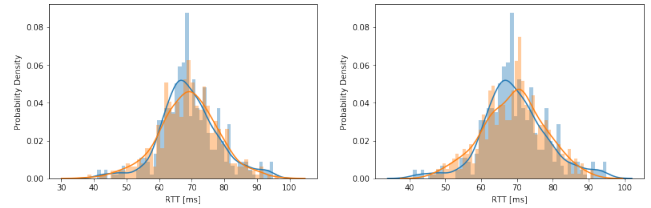
図 2 RTT 分布（タイプ 2）
（青：正規 AP、赤：不正 AP）

GET を実行して RTT を計測するのを 10 秒間隔で 1 時間続けた。この時の RTT 分布をヒストグラムで図 2 に示す。青は正規 AP に接続している時の RTT 分布で、赤は不正 AP に接続している時の RTT 分布である。ただし、図 2 では 400 ms 以上はカットされている。ここでの曲線はカーネル密度推定によって得られたものである。図 2 から明らかに不正 AP に接続している時は RTT 値が大きい値の割合が多いことが分かる。そして特に注目すべきは、正規 AP に接続している時の RTT 分布の形状である。正規分布に似た形であることが分かる。しかし、RTT には誤差が生じる事が多いので、RTT 値が大きくなる割合をゼロにすることはできない。図 2 の正規 AP への接続時の分布も右に裾野が僅かに伸びている。

実際に図 2 の正規 AP と接続時の RTT 分布が正規分布と似ているかどうか統計的に調べる。右の裾野を無くすために、第 3 四分位数を Q_3 、四分位範囲を IQR として、閾値 $Q_3 + IQR \times 1.5$ 以上の外れ値を削除したデータと、そのデータの平均と標準偏差を元に正規分布に従う乱数（正

表 1 RTT 分布と正規乱数とのコルモゴロフ・スミルノフ検定結果

p 値	$p < 0.05$	$p \geq 0.05$
合計	307	693



(a) p 値 = 0.389 のとき

(b) p 値 = 0.0422 のとき

図 3 分布の比較
（青：RTT 分布、橙：正規乱数）

規乱数）を同じデータ数だけ発生させたデータ、この 2 つのデータでコルモゴロフ・スミルノフ検定を行って p 値が 0.05 未満かどうかを確認するのを 1000 回繰り返した。その結果を表 1 に示す。コルモゴロフ・スミルノフ検定とは、統計学における仮説検定の一種である。帰無仮説を 2 つの標本の分布は等しいとして、対立仮説を 2 つの標本の分布は異なると定義されている。有限個の標本に基づいて 2 つの母集団の確率分布が異なるかどうかを判定する。p 値が大きいような場合には 2 つの標本の母集団の確率分布は近いとすることができる。また、p 値が 0.05 未満の時と 0.05 以上の時の正規乱数との分布の比較の一例をそれぞれ図 3 にそれぞれ示す。

図 3 の (a) と (b) には大きな差がないように見える。正規乱数の僅かな違いが p 値に大きな影響を与えていることが分かる。実際に図 3 の (a) と (b) の 2 つを見比べるとどちらも分布は似ている。表 1 で p 値が 0.05 未満の割合が少ない事も考えると、正規 AP に接続時の RTT 分布は正規分布と見なす事ができる。無線ネットワークの低遅延環境での RTT 分布が正規分布と見なせると文献 [10] でも述べられている。

4. 提案手法

本研究で提案する手法は、Web アプリケーションを想定している。ここでは、その提案手法に必要な前提と Evil Twin 攻撃を検出するための 2 つの指標について説明する。

4.1 前提

最も重要なのは Web サーバの準備である。この Web サーバの主な役割は、AP を識別、その AP 毎のデータ収集、収集したデータを元に Evil Twin 攻撃の検出である。例えば、AP 毎に一意的 URL を用意しておき、その URL 先へのアクセスからユーザアクセス情報を集める。常に Evil Twin 攻撃を受けている AP はなく、正規 AP に接続している時の正しい情報（基準データ）を蓄積するのは容

易だと考えられる．ある程度の基準データが集まれば，そのデータを元にアクセスしたユーザに対して Evil Twin 攻撃判定をして，その結果を返すことができる．もし基準データにグローバル IP アドレスなどの ISP 情報が含まれていたら，タイプ 1 の Evil Twin 攻撃を検出することができる [3], [8]．実際に運用するとしたら HTTPS 通信も前提として必要である．

4.2 RTT 分布

タイプ 2 の Evil Twin 攻撃の時，不正 AP と正規 AP のどちらに接続しているかで RTT 分布が違うことは既に述べた．また，正規 AP に接続時の RTT 分布は正規分布と見なせる事も確認した．これらを Evil Twin 攻撃検出に利用する．ここでの RTT とは HTTP GET での取得にかかる時間のことである．基準データとして短い時間間隔である程度の数の RTT 値が集められたら，例えば検出時前の 30 分間の RTT 値データを正規 AP に接続されている時の RTT 分布（正規分布）と見なして，Evil Twin 攻撃判定をしたい端末で数回分 RTT 値を取得して，それら RTT 値の平均がその正規分布からズレているかどうかで攻撃を判定する．タイプ 2 の Evil Twin 攻撃であれば正規 AP を中継する無駄なホップがあり，基準データの RTT 値平均よりも大きな平均値になる可能性が高い．それにより基準データから得られた正規分布からズレているはずなのでそれを攻撃と判断し，ズレていると判断できない場合は正常通信と判断する．ズレの判定は z 検定や t 検定という仮説検定で行う．有意水準を設定して得られた統計量から判断する． z 検定は (1) の式での統計量が標準正規分布に従うのを利用し， t 検定は (2) の式での統計量が自由度 $m - 1$ の t 分布に従うのを利用する．

$$z = \frac{\bar{x} - \mu}{\frac{\sigma}{\sqrt{n}}} \sim N(0, 1^2) \quad (1)$$

$$t = \frac{\bar{x} - \mu}{\frac{\bar{\sigma}}{\sqrt{m}}} \sim t(m - 1) \quad (2)$$

ここで， μ は基準データの RTT 値の平均， σ は基準データの RTT 値の標準偏差， n は基準データの RTT 値のデータ数， $\bar{\sigma}$ は端末から取得した RTT 値の不偏標準偏差， m は端末から取得した RTT 値のデータ数である．

4.3 GPS & RSSI 関係

本論文で GPS (Global Positioning System) とは経度・緯度の位置情報のことで，RSSI (Received Signal Strength Indication) とはクライアントが AP などからどれくらいの強さの電波を受信しているかを表したものである．RSSI は Android の Wifinfo では [dBm] 単位で表示されるため，本論文では RSSI の単位を [dBm] として扱う．

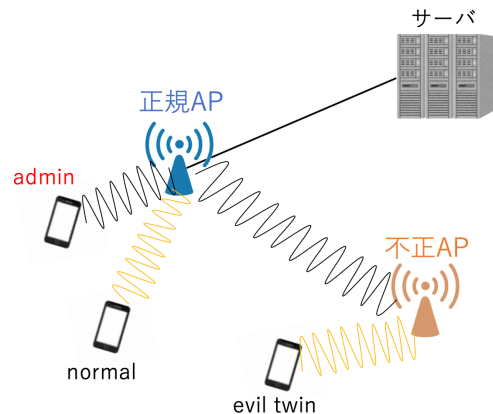


図 4 実験構成イメージ図

Evil Twin 攻撃は，正規 AP と同じ SSID に設定して偽装した不正 AP に接続させる事で成立すると述べた．同じ SSID を持つ AP が複数ある場合は電波が強い方が優先され，その仕組みを悪用する事が多い．実際の状況を考えて正規 AP の電波が弱い所に不正 AP が設置される事が多いはずである．基準データに GPS データとその地点での RSSI データが含まれており，正規 AP の通信範囲で満遍なく，つまり正規 AP 付近から電波が届く限界まで距離間隔が短いデータしかないくらいに基準データを持っていると仮定する．そうすると攻撃判定をしたい端末から近い基準データを GPS データから求めて，それらの RSSI 値平均との差異が大きければ Evil Twin 攻撃と判断できる．ただし，不正 AP に接続していたとしても近くの基準データの RSSI との差異が小さい場合は Evil Twin 攻撃を検出できない．これは電波の強度がちょうど同じくらいという状況である．例えば，正規 AP と不正 AP が非常に近くにあり，その両方の AP に近い位置で端末が AP に接続しようとする．この時，どちらの AP も高い電波強度である可能性が高いため RSSI 値がどちらの AP に接続しても近い値になり，こういった場合には近くの基準データとの RSSI 値に差異がないため検出できないと考えられる．ただ実際に Evil Twin 攻撃を成功させるためには正規 AP より電波強度を高くする必要があるので，このような状況での攻撃成功率は低いと思われる．

5. 実験

4 章の提案手法で，RTT 分布と GPS & RSSI 関係の 2 つの指標による Evil Twin 攻撃検出の仕組みをそれぞれ説明した．ここでは，それらの指標による検出が実現可能であるか調べるための実験について述べる．今回，実験のために Web サーバを VPS に構築し，Android アプリも特別に実装した．

5.1 RTT 分布

RTT 分布による検出実験の構成イメージを図 4 に示す．Evil Twin 攻撃シナリオのタイプ 2 を想定しているので，

表 2 z 検定による Evil Twin 攻撃検出結果

z 検定	真陽性率	真陰性率	偽陽性率	偽陰性率	精度
片側 5%	90 %	80 %	20 %	10 %	0.861
片側 1%	89 %	82 %	18 %	11 %	0.861

表 3 t 検定による Evil Twin 攻撃検出結果

t 検定	真陽性率	真陰性率	偽陽性率	偽陰性率	精度
片側 5%	49 %	92 %	51 %	0.08 %	0.672
片側 1%	34 %	92 %	66 %	0.08 %	0.582

不正 AP は正規 AP を中継するようにしている．図 4 の中にある admin 端末は基準データをサーバに蓄積する役割で，normal 端末は正規 AP に接続した時のテスト用で，evil twin 端末は不正 AP に接続した時のテスト用である．admin 端末は 10 秒間隔で RTT 値を取得してサーバに送るのを繰り返してサーバに基準データを蓄積させる．以下に normal 端末と evil twin 端末のテスト端末が行う実験手順を説明する．

- (1) 20 個分の RTT 値を取得して，まとめてサーバへ送信
- (2) サーバが受信した時刻以前の 60 個分の基準データを正規分布と考え，z 検定や t 検定の片側検定で有意水準を 5%や 1%に設定して仮説検定を繰り返す

この時，RTT 値のデータに対して細かな外れ値操作をする．まず，それぞれのデータ毎に第 3 四分位数を Q_3 ，四分位範囲を IQR として，閾値 $Q_3 + IQR \times \alpha$ 以上の RTT 値を外れ値とする．60 個分の基準データに対しては $\alpha = 1.5$ として外れ値の RTT 値データは全て削除する．20 個分のテスト端末から得た RTT 値データに対しては $\alpha = 2.5$ として外れ値の数が 1 または 2 個の時は全て削除し，3 個以上の時は最大 RTT 値のみを削除する．なぜこのような操作をするかというと，もし Evil Twin 攻撃があった場合には外れ値が多くなると予想されるためである．

合計 122 回これらを繰り返した．z 検定による検出結果は表 2，t 検定による検出結果は表 3 にそれぞれ示す．Evil Twin 攻撃を正しく検出できた数を TP，正規 AP に接続している正常通信を正しく判断できた数を TN，Evil Twin 攻撃であるが見逃してしまった数を FP，正規 AP に接続しているのに Evil Twin 攻撃と誤って検出してしまった数を FN とする．真陽性率，真陰性率，偽陽性率，偽陰性率は以下のように計算している．

$$\text{真陽性率} = \frac{TP}{TP + FN} \quad (3)$$

$$\text{真陰性率} = \frac{TN}{TN + FP} \quad (4)$$

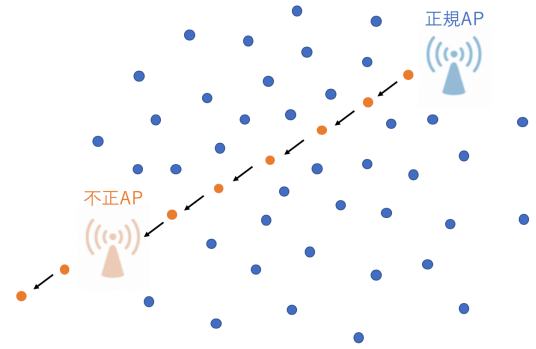


図 5 GPS&RSSI 関係の実験イメージ図

$$\text{偽陽性率} = \frac{FP}{TN + FP} \quad (5)$$

$$\text{偽陰性率} = \frac{FN}{TP + FN} \quad (6)$$

$$\text{精度} = \frac{TP + TN}{TP + FP + TN + FN} \quad (7)$$

5.2 GPS & RSSI 関係

GPS&RSSI 関係による検出実験の構成イメージも図 4 とほとんど同じである．こちらは Evil Twin 攻撃シナリオのタイプ 1 とタイプ 2 の両方に対応していると考えているが，ここではタイプ 2 を想定して実験を行った．ただし図 4 にある normal 端末は使わず，admin 端末が基準データを集める役割で，evil twin 端末がテスト用という役割で利用した．実験内容は，まず初めに admin 端末で正規 AP の通信範囲全体で満遍なくデータを取得する．このときの取得データは GPS と RSSI の 2 つのデータが少なくとも必要である．その後に不正 AP に接続した evil twin 端末を正規 AP 付近からデータを取得しながら不正 AP に近づいて行く．この実験イメージを図 5 に示す．図 5 の青点は事前に集めた基準データの取得地点，橙点は不正 AP に接続している evil twin 端末からのデータ取得地点の例である．evil twin 端末を持って正規 AP から不正 AP にデータを取得しながら近づいて行き，不正 AP もある程度超えたらデータ取得を止める．図 5 ではその移動イメージも図で表している．実際の正規 AP から不正 AP の距離は 16m であった．evil twin 端末で得られたデータに近い上位 6 つの基準データを GPS データから求めて，それらの基準データの RSSI 値の平均と自身の RSSI をグラフに表したものを図 6 に示す．図 6 の緑の波線は基準データの最大値である．正規 AP から不正 AP に向かって進んでいたが，この緑線が正規 AP の通信範囲の限界とも考えられる．橙線は Evil Twin 攻撃を受けているので不正 AP に近づくと RSSI 値が高くなっていて，さらに進むことで不正 AP から離れることになり RSSI 値は落ちている．青線は近くの基準データの RSSI 値平均なので正規 AP から離れるほ

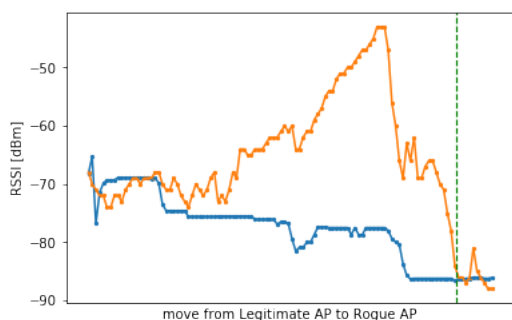


図 6 正規 AP から不正 AP に近付いた時の RSSI 値変動
(青：近くの基準データの RSSI 値平均、
橙：evil twin 端末の RSSI 値変動)

ど小さくなっている。2 つに大きな差が現れるタイミングがあり、この差は検出に十分な大きさだと思われる。橙線のピークが最も不正 AP に近い位置だと考えられる。その時の近くの基準データの RSSI 値平均との差は 34.5[dBm] であった。

6. 考察

本研究ではユーザアクセス情報を元に Evil Twin 攻撃を検出する手法を提案した。実現方法として Web アプリケーション型の検出システムを想定し、Web サーバに AP の情報を登録してあるシナリオを考えた。また、これによって実現できる 2 つの指標を用いた Evil Twin 攻撃検出の実験を行った。RTT 分布の検出実験では z 検定による検出で精度 0.861 が得られた。真陽性率は 90% と高いのだが、真陰性率が 80% と少し低くなった。t 検定による検出だと精度自体は非常に低いが、真陰性率が 92% と高いのが注目である。式 (2) の分母の標準偏差は基準データではなく、取得した RTT 値データのものが利用される。これにより誤差の大きい RTT 値があった時でも統計量が抑えられるので誤って Evil Twin 攻撃と判断することが少なくなったのだと考えられる。しかし、Evil Twin 攻撃があった時にも同様の効果が現れるので真陽性率が大きく落ちてしまうのが問題である。また、実験環境が低遅延環境であった事が結果に影響を与えている可能性があり、高遅延環境であった時に同様の検出率となる保証はない。

GPS&RSSI 関係の方の実験では、最終的に図 6 のグラフが結果として得られた。図 6 の左側は正規 AP 付近であるので、本来であれば青線の RSSI 値が高いはずである。しかし、今回の実験で使った正規 AP の電波出力が弱く、不正 AP が比較的に電波出力が高かったため差が見られなくなっている。それでも不正 AP に近づくと橙線の RSSI 値が高くなり、その近くの基準データの RSSI 値平均との差が大きくなり最大で 34.5 [dBm] であった。ちょうど橙線の RSSI 値がピークの位置である。そのピーク前後も 10 [dBm] 以上の差があるのを確認できた。緑の波線は基準

データの最大値であり、正規 AP の通信範囲の限界とも言えるが、実際に実験をしていた時の感覚だともう少し左にあるはずだった。これは誤差に起因するズレだと思われる。当然、GPS や RSSI の測定値にも誤差が含まれているのでそういったことまで考える必要がある。しかし、正規 AP と不正 AP の両方で同じくらいの RSSI 値となる所では検出はできない。図 6 で言う左側の差がない状況のことである。このような検出できない状況のときは RTT 分布による攻撃検出を行うなどの組み合わせが可能である。本論文で述べた 2 つの指標は対立するものではなく相補的な関係であると考えている。この 2 つの指標以外の追加もできる。さらに Web アプリケーションを想定しているので、AP で HTTP や HTTPS の通信が許可されていれば適用可能であるのもメリットである。

7. 今後の課題

本論文で提案する手法は、既存の研究も容易に組み合わせることができる可能性が高い。原田らは文献 [11] で、都内無線 LAN の実態調査の結果を報告しており、実際に駅や空港などで提供される公衆無線 LAN のほとんどは認証あり AP であると分かった。AP での認証の手順や仕組みを調べることでその AP が不正であるかを検出できる可能性も指摘している [8], [11]。正しい認証プロセスが事前に分かっていたら確実な検出が可能になる。提案する手法に認証プロセスを登録情報として保存すれば実現できると思われる。

しかし、本手法には問題も残っている。AP の正しい情報を一定間隔で収集する必要がある事と、偽の情報が登録されない仕組みが必要である事は解決されるべき問題である。対策としては AP 毎に最低 1 つは一定間隔でサーバに AP 情報を送信する端末を用意しておく。その情報を確実に正しい情報と判断してサーバに蓄積し、その情報と違ったものは登録されない仕組みにする。ただし、この対策だと AP 毎に端末を準備して稼働させ続ける必要があるのもその分のコストがかかってしまう。また、実際に運用する事を考えると、攻撃を検出できるだけの情報が登録されているかどうかを把握したい。例えば、GPS&RSSI 関係による検出手法だと前提として、AP の通信範囲で満遍なくデータを取得する必要があるがどれくらいのデータが必要なのかを把握したい。このような問題を一つずつ解決していく事が今後の課題である。

8. おわりに

本研究は、Web アプリケーションを想定した、2 つの指標による Evil Twin 攻撃検出手法を提案した。Web サーバを用意してサービスとして提供する事も可能である。AP で HTTP や HTTPS の通信を禁止することはほとんど無いので、多くの AP で適用が可能であると思われる。本論

文で述べた 2 つの指標による攻撃検出はそれぞれ一定の有用性を示した。それらはお互いを補い合う事ができると考えていて、既存研究などから他の指標を追加する事も考えられる。今後はシステムから検出方法までをもう少し実用的にまとめてあげて、残った問題の対策を考えて行きたい。

謝辞 本研究は JSPS 科研費 JP19H04098 の助成を受けたものです。

参考文献

- [1] 独立行政法人情報処理推進機構 (IPA) : 令和元年版 情報通信白書 (ICT 白書), pp.372-373, 総務省 (2019).
- [2] S. Nikbakhsh, A.B.A. Manaf, M. Zamai, et al.: A Novel Approach for Rogue Access Point Detection on the Client-Side, *Proc. Advanced Information Networking and Applications Workshops (AINA)*, IEEE Computer Society (2012).
- [3] H. Mustafa and W. Xu: CETAD: Detecting Evil Twin Access Point Attacks in Wireless Hotspots, *Proc. Communications and Network Security (CNS)*, IEEE (2014).
- [4] O. Nakhila, E. Dondyk, M. Faisal, et al.: User-Side Wi-Fi Evil Twin Attack Detection Using SSL/TCP Protocols, *Proc. Consumer Communications and Networking Conference (CCNC)*, IEEE (2015).
- [5] Q. Lu, H. Qu, Y. Zhuang, et al.: A Passive Client-based Approach to Detect Evil Twin Attacks, *Proc. TrustCom/BigDataSE/ICSS*, IEEE Computer Society (2017).
- [6] Y. Song, C. Yand and G. Gu: Who Is Peeping at Your Passwords at Starbucks? - To Catch an Evil Twin Access Point, *Proc. Dependable Systems & Networks (DSN)*, IEEE (2010).
- [7] E. Kuo, M. Chang and D. Kao: User-Side Evil Twin Attack Detection Using Time-Delay Statistics of TCP Connection Termination, *Proc. Advanced Communications Technology (ICACT)*, IEEE (2018).
- [8] 保要隆明, 金井敦: 無線 LAN 不正アクセスポイント判定手法の検討, 信学技報, 電子情報通信学会 (2015).
- [9] T. Elteto and S. Molnar: On the distribution of round-trip delays in TCP/IP networks, *Proc. Local Computer Networks (LCN)*, IEEE (1999).
- [10] 田行里衣, 池上大介: LTE 環境下の実測データに基づく RTT 分布モデリング, 信学技報, 電子情報通信学会 (2018).
- [11] 原田敏明, 森達哉, 後藤滋樹: その無線アクセスポイント安全ですか? 不正な無線 AP の分類とフィールド調査, *Proc. Computer Security Symposium (CSS)*, 情報処理学会 (2015).