ネットワーク情報を利用した無線LAN不正アクセスポイント判定手法

保安, 隆明 / HOYO, Takaaki

(出版者 / Publisher)
法政大学大学院理工学・工学研究科
(雑誌名 / Journal or Publication Title)
法政大学大学院紀要. 理工学・工学研究科編 / 法政大学大学院紀要. 理工学・工学研究科編
(巻 / Volume)
57
(開始ページ / Start Page)
1
(終了ページ / End Page)
8
(発行年 / Year)
2016-03-24
(URL)
https://doi.org/10.15002/00013288

ネットワーク情報を利用した 無線 LAN 不正アクセスポイント判定手法

Rouge access point detection method using network information

保要隆明
Takaaki Hoyo
指導教員　金井敦

法政大学大学院理工学研究科応用情報工学専攻修士課程

Wireless LAN access points are installed everywhere. Although such access point is a convenient, it is present many of the security problems. Among them, it is not progressing countermeasure of rogue access point. Then, urgent solutions are required. In this study, we propose a method for detecting the rogue access point by much collected information of the wireless LAN access point and network. Also, rouge access point detection using the proposed network information has shown to be useful through the evaluation experiments on the feasibility of this method.
***Key Words** : Wi-Fi, Security, EvilTwin, RougeAP*

１．はじめに

スマートデバイスやモバイルノート PC の発展やこれらの端末を使ったニーズの増加に伴い，会社や学校などの PC を使うユーザが多い場所のみならず，街中にあるカフェや駅など至るところに無線 LAN アクセスポイントが設置されている．これまでは外出先で通信を行うためには，3G や LTE などの携帯電話回線によってインターネット接続を行うことが主だった．しかし，無線 LAN アクセスポイントが利用できる環境の整備によりインターネットへの接続が容易となってきている．

無線でのネットワークへの接続は，電波を使って通信を行うため場所を選ばずに接続できて便利である．一方で，電波が届く範囲内であれば誰でも通信を行うことが可能であるため，他ユーザが行っている無線通信の盗聴や無線 LAN アクセスポイントの不正利用など，セキュリティ上の問題が多数存在する．このような問題の多くは，具体的な対策が提案されている．例えば，無線通信の盗聴であれば，暗号強度が高いアルゴリズムを用いて無線 LAN クライアント（子機）と無線 LAN アクセスポイント（親機）間を暗号化することで盗聴を防ぎ，アクセスポイントの不正利用であれば，利用者認証を行うことで不正利用を防いでいる．

しかし，この中でも明確な対策が提案されていない問題がある．それが，悪意のある第三者による不正アクセスポイントの設置である．このようなアクセスポイントは，無線 LAN の仕組みを悪用して，アクセスポイントに接続してきた利用者を接続させている．利用者がこのようなアクセスポイントに接続してしまった場合，クライアントとアクセスポイント間で暗号化されていても，攻撃者が設置したアクセスポイントで通信を盗聴されてしまう脅威や，さらに不正なサイトへ誘導されマルウェアに感染させられる脅威がある．

この問題への対策として，管理者側で不正なアクセスポイントを検知する方法がいくつか提案されている．しかし，暗号化機能と異なり，実装されている製品は僅かである．また、アクセスポイントを管理する側の対策だけでなく，無線 LAN アクセスポイントを利用する側で検知する技術の研究も行われているが，特殊なハードウェアが必要であることや確実に検知できる手法がないことにより，決定的な対策が未だ発案されていない．

従来の研究では，ネットワークの様々な情報を収集し，不正アクセスポイントであるか判定する手法は提案されてきたが，利用する情報が少なかった．また，過去に接続した正規のアクセスポイントの情報を保存しておき不正アクセスポイントの検知に利用する手法もなかった．

本稿では，特殊なハードウェアを使わずに従来の精度より検知の精度を向上させるために，アクセスポイントやアクセスポイントが接続しているネットワークの情報など，より多くの情報を収集し，過去に接続した正規のアクセスポイントの情報と比較することで不正アクセス

ポイントの判定を行う手法を提案する．また，本手法が実際に有用な手法であるか評価を行い，実現可能性を考察する．

２．背景

攻撃者は不正アクセスポイントに利用者接続させるために，無線 LAN の接続方法を悪用する．また，不正アクセスポイントはインターネットへの接続を提供するため，様々な方法を使って通信をインターネットに中継する．そこで本章では，無線 LAN に接続する仕組み，それを悪用した攻撃，さらにインターネットへの中継方法について述べる．

（１）無線 LAN アクセスポイントへの接続

無線 LAN には，BSSID (Basic Service Set Identification) と ESSID (Extended Service Set Identification) の２つのネットワーク識別子がある．BSS は，１つの無線 LAN アクセスポイントとそこに接続している無線 LAN デバイスで構成されるネットワークで，その識別子である BSSID は基本的に無線 LAN アクセスポイントの MAC アドレスが使用される．また ESS は，複数の BSS で構成される無線 LAN のネットワークであり，ESSID は基本的に任意の 32 文字であり，一般的に SSID と呼ばれるものである． この SSID は，無線 LAN クライアントは，SSID を指定して同じ SSID を持つ最も電波が強いアクセスポイントに接続する．

また，無線 LAN を利用している端末は，持ち運んで利用することが多いため，同じ SSID 内の異なるアクセスポイントの電波の範囲に移動した際も，自動で接続を切り替えるローミングと呼ばれる機能がある．よって，複数のアクセスポイントで同じ SSID を設定しておくことで，あるアクセスポイントの電波が届く範囲を外れた時に，同じ SSID の別のアクセスポイントに自動で再接続され，通信を維持することが可能である．

（２）EvilTwin 攻撃

EvilTwin 攻撃とは，攻撃者が正規のアクセスポイントになりすました不正なアクセスポイントを設置して，利用者を接続する攻撃である．これは（１）で紹介した無線 LAN アクセスポイントの仕組みを悪用することで成立する． [1]では，攻撃が成立すると考えられるシナリオを次のように定義している．

① アクセスポイントのすり替え

正規のアクセスポイントをシャットダウンし，同じ設定にした不正なアクセスポイントに置き換える．

② 正規アクセスポイントとの共存

攻撃者は，正規のアクセスポイントと同じ SSID を持ち，なおかつ正規のものより電波の強い不正なアクセスポイントを設置する．無線 LAN クライアントは，接続したいワイヤレスネットワークの SSID を選択すると，電波が最も強いアクセスポイントに自動で接続するため，利用者は気づかずに不正なアクセスポイントへ接続させられる．

③異なる場所への設置

攻撃者は，不正なアクセスポイントを正規の無線 LAN アクセスポイントと同じ設定にしたものを用意する．設置する場所は，正規のアクセスポイントの電波が届かない異なる場所である．無線 LAN クライアントは，アクセスポイントへの接続情報を保持しているため，そこへ自動で接続される．

④プローブ要求による不正アクセスポイントの生成

無線 LAN クライアントは効率よく過去に利用したアクセスポイントを発見するため，SSID の情報をプローブ要求として送信する．これを不正アクセスポイントで拾うことで，クライアントが使用したことのある SSID のアクセスポイントを自動で生成する．

①の手法は，アクセスポイントを物理的に交換する必要があるので，攻撃者と管理者の結託や特別な状況でなければ成立するのは難しい．よって，本研究では②～④の状況を考慮する．

（３）インターネットへの接続

不正アクセスポイントの多くは，接続してきた利用者の通信を盗聴するために，インターネット接続を提供する．不正アクセスポイントが接続してきた利用者にインターネットを提供する方法は，次のように考えられる．

① 正規のアクセスポイントに中継する方法

通信を正規のアクセスポイントに中継させる方法である．（図１） 不正アクセスポイントはルータのような振る舞いをする．この接続方法は，（２）で紹介した攻撃シナリオⅢの場合，近くに正規のアクセスポイントがないことを想定しているため不可能である．

②直接 LAN に接続する方法

正規のアクセスポイントが属するネットワークが，有線でのアクセスやターゲットとは異なる SSID のアクセスポイントを提供している場合に利用できる方法である．（図２） この場合，正規のアクセスポイントを経由せずにインターネットへ接続することが可能である．

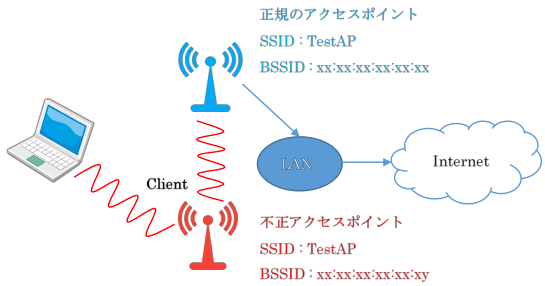

図 1　正規のアクセスポイントに中継する方法

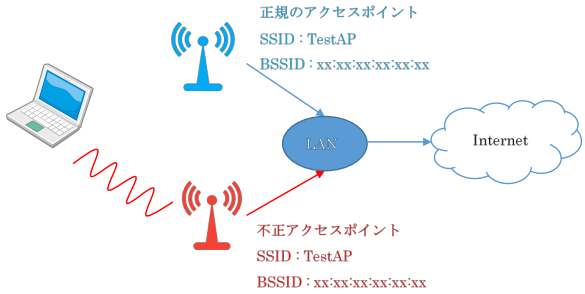

図 2　直接 LAN に接続する方法

③ 異なる回線を使う方法

正規のアクセスポイントは経由せず，他の回線を利用してインターネット接続を提供する方法である．（図３）この時，他の回線に利用されるのは，攻撃者が用意したモバイルルータや携帯電話の回線が考えられる．

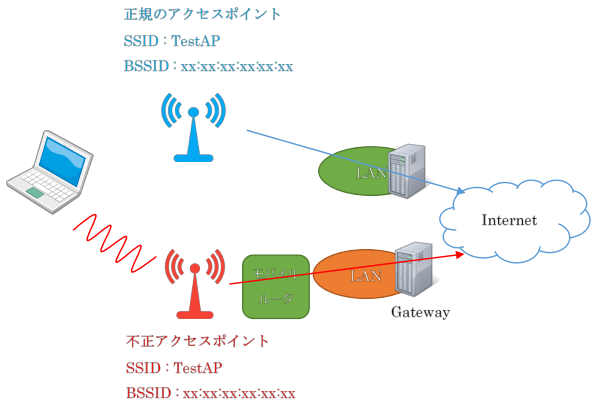

図 3　異なる回線を使用する方法

（４）不正アクセスポイント接続後の脅威

利用者が不正なアクセスポイントへ接続してしまった場合，次のような脅威が考えられる．

・通信内容の盗聴
・中間者攻撃による SSL 通信の復号
・フィッシングサイトなどの不正なサイトへの誘導

このような脅威から守るためにも，不正なアクセスポイントに接続された際に検知し，すぐに切断することが重要である．

３．関連研究

“A Novel Approach for Rogue Access Point Detection on the Client-Side” [2]では，SSID と MAC アドレス（BSSID）が正規のアクセスポイントと同じであるパターンの不正アクセスポイントの検知手法について提案している．

この手法では，まず 2 つのアクセスポイントから取得した IP アドレスを比較する．安全なネットワークである場合，二つの IP アドレスが異なるが，同じネットワークアドレスであるとしている．

また，2 つの IP アドレスが同じであるか 2 つの IP アドレスのネットワークアドレスが異なる場合，危険なネットワークとしている．さらに，後者の場合は，ネットワークの経路を調査する traceroute コマンドを 2 つのアクセスポイントに実行して結果を比較する．この時，片方の結果よりも余分なホップが含まれている場合は最も危険であると判断する．

この手法の問題点は，2(3)で紹介したインターネットに接続する方法によっては，安全と判断したネットワークでも不正なアクセスポイントである場合があることと，traceroute に使われる ICMP や UDP のパケットを禁止にしているネットワークもあることである．よって，この情報のみでは正しく判定出来ない場合があると考えられる．

“CETAD: Detecting Evil Twin Access Point Attacks in Wireless Hotspots” [3]では，アクセスポイントが利用している ISP (Internet Service Provider) の情報，グローバル IP アドレスの情報，クライアントとサーバの RTT(Round Trip Time)から不正なアクセスポイントの検知をする手法を提案している．

ISP とグローバル IP アドレスの情報は，2 (3)で紹介した「異なる回線を使う方式」であれば，正規のアクセスポイントと別の回線を使うので，異なる ISP，異なるグローバル IP アドレスとなると考えられる．よって，この方法でインターネットに接続された不正アクセスポイントであれば，ほぼ確実に検知することが可能である．

一方，RTT を使った検知は 2 (3)で紹介した「正規のアクセスポイントに中継する方式」を対象としている．これは不正アクセスポイントが正規のアクセスポイントに比べて多くホップすることで，RTT が正規のアクセスポイントよりも増加すると考えられているからである．しかし，RTT は様々な要因で変わるため，この手法での検知は不安定になると考えられる．

“User-Side Wi-Fi Evil Twin Attack Detection Using SSL/TCP Protocols” [4]でも 2(3)の「異なる回線を使う方式」の不正アクセスポイントを検知するための手法を提案している．この研究の場合，グローバル IP アドレスや ISP の情報を用いて検知をするのではなく，異なるアクセ

スポイントにローミングされた時に，TCP/SSL コネクションが切断されないかどうかで検知をしている．同じ ISP のバックボーンネットワークに接続されたアクセスポイントであれば，ローミングした時に通信を切断せずに継続させることが可能である．しかし，異なる ISP のバックボーンネットワークに繋がった場合，グローバル IP アドレスとポート番号が変化するため，接続を継続するのは困難である．このことを利用して検知を行っている．

４．提案手法

関連研究で提案されている手法に共通して言えることは，すべての不正アクセスポイント設置のシナリオに対応できておらず，確実に検知できる手法も存在していない．また，関連研究ではネットワークの情報を収集して不正アクセスポイントの判定を行っていたが，収集するネットワーク情報が少なかった．

そこで，本研究ではより多くのネットワーク情報を収集して不正アクセスポイントの判定に使用することによって，多くの設置シナリオに対応し，確実に不正アクセスポイントの判定を行うことを目的とする．

（１）提案手法の前提条件

提案手法では，次の環境で不正アクセスポイントを判定できることを前提とする．

・汎用的なコンピュータ，OS
・特殊なハードウェアは使用しない

また，クライアントが初めてアクセスポイントに接続する時には，不正アクセスポイントが設置されていない前提とする．これは，不正なアクセスポイントが設置されている状況はほとんどなく，最初に不正アクセスポイントに接続される可能性は極めて低いと考えたためである．

（２）提案手法の概要

提案する手法では大きく分けて，「情報収集フェーズ」と「不正アクセスポイント判定フェーズ」の二つに分かれる．

「情報収集フェーズ」では，無線 LAN クライアントでネットワークやアクセスポイントの情報を収集する．ここで収集する情報の種類と特徴については，（３）で述べる．

そして，「不正アクセスポイント判定フェーズ」では，収集した情報を用いて不正アクセスポイントであるかを判定する．判定方法や判定のタイミングについては（４）で述べる．

（３）判定に利用する情報

本節では，判定に用いる情報の種類と特徴を述べる．ここで用いる情報は前提条件で示した環境で収集できるものである．

a）無線 LAN アクセスポイントの識別情報

２（１）でも述べたように，無線 LAN アクセスポイントの識別子には，SSID と BSSID (MAC アドレス)が使用される．

Evil Twin 攻撃を行うためには，正規のアクセスポイントと同じ SSID を不正アクセスポイントに設定しなければならない．そのため，SSID は正規のアクセスポイントと不正アクセスポイントで必ず一致している．

一方，BSSID は基本的には一致しない．これは，BSSID はアクセスポイントとなるインターフェースの MAC アドレスの値が通常は使われるからである．しかし，MAC アドレスは偽装が簡単にできる．そのため，不正アクセスポイントが設置される場合，BSSID の設定パターンは２つ考えられる．

一つは，正規のアクセスポイントの BSSID と重複しないアドレスの場合である．無線 LAN は一つの SSID で複数のアクセスポイントを運用されることがある．そのため，一つの SSID で複数の BSSID のアクセスポイントを検出することも多い．

もう一つは，正規のアクセスポイントの BSSID と重複するアドレスとなる場合である．この場合，不正アクセスポイントが正規のアクセスポイントよりも強い電波を送信すると，不正なアクセスポイントに接続されてしまう．

いずれの場合にしても，SSID と BSSID のみで不正アクセスポイントを判断することは難しいため，これらの情報をキーにして他の情報と比較する必要がある．

b）DHCP 情報

一般的な無線 LAN アクセスポイントでは，接続を行うと自動で DHCP (Dynamic Host Configuration Protocol) を用いてネットワーク情報が自動で設定される．

２（３）の「正規のアクセスポイントに中継する」場合，不正アクセスポイントではルータのような役割をしているため，正規のアクセスポイントとは異なるネットワークに接続される．よって，DHCP で配布される IP 通信を行うための IP アドレスに関連する情報や DHCP サーバの IP アドレスは異なる．

また，２（４）で紹介したように，利用者を不正なサイトに誘導する攻撃も考えられる．その場合，攻撃者が用意した DNS サーバで名前解決させることが考えられるので，DNS サーバの IP アドレスも変化する可能性がある．

以上の理由から，不正アクセスポイントを経由した場合，DHCP 情報が変わる可能性がある．正規のアクセスポイントの管理者がこれらの情報変化させることは少な

い．したがって，DHCP の情報は不正アクセスポイントを判定するために有用な情報であると考えられる．

しかし，この情報が一致していても不正アクセスポイントである場合があるので，完全な判定はできない．例えば，インターネットへの接続が「異なる回線を使用する方法」であった場合，正規のアクセスポイントと同じような環境を再現することも可能であるので，そのような場合は判定が不可能となる．

c）認証ページの情報

大学やオフィス，公衆無線 LAN など不特定多数が利用する無線 LAN では，接続に必要なパスフレーズを公開して運用されていることが多く，WPA など無線 LAN が提供するセキュリティ方式では認証がほとんど出来ていない．そのため，不正利用を防止するために，無線 LAN アクセスポイントに接続後インターネットを利用しようとすると，利用者認証を行うページへリダイレクトされる．そして．そのページで ID やパスワードを入力して不正に公衆無線 LAN が利用されないようにしている．

攻撃者は，このようなサービスでの認証情報を持っていないことが多く，それを手に入れるために偽の認証ページを作成し，利用者から認証情報を搾取する手口を行うことがある．したがって，このような不正な認証ページに気づくことが出来れば判定情報の一つとして利用可能であると考えられる．

このような目的で使われる認証ページでは，ID やパスワードなど機密性が高い情報を送信する必要があるため，信頼できる認証局によって電子署名された SSL サーバ証明書を使った HTTPS で通信されていることが多い．もし攻撃者がこのようなサイトを偽装する場合，証明書を使わない HTTP で情報を送信するページ，もしくは攻撃者が自己署名した証明書などを用いて HTTPS 通信を行う認証ページが考えられる．そのため，認証ページの URL や証明書の情報を収集する．また，正しい DNS サーバから認証ページの URL を IP アドレスに変換する名前解決を行うと，認証ページの IP アドレス変化しないはずなので，この情報も収集する．

d）グローバル IP アドレス

IP アドレスには，組織内で使用できるプライベート IP アドレスとインターネットで利用される重複しないグローバル IP アドレスがある．一般的に，無線 LAN アクセスポイントに接続すると，プライベート IP アドレスが割り当てられる．しかし，プライベート IP アドレスのままではインターネットでは使えないので，インターネット上のサーバにアクセスする際は，NAPT(Network Address Port Translation) などにより，プライベート IP アドレスが ISP(Internet Service Provider)などが管理するグローバル IP アドレスに変換される．したがって，サーバにアクセスした際の IP アドレスを確認すると，アドレス変換後の ISP のグローバル IP アドレスとなっている．

不正アクセスポイントのインターネットへの接続方法が「異なる回線を使う方法」の場合，正規のアクセスポイントが使っているネットワークを利用しないため，インターネットに出るときの ISP も異なるはずである．正規のアクセスポイントは頻繁に ISP が変わることはないため，異なる ISP が管理するグローバル IP アドレスからのアクセスであれば，「異なる回線を使う方法」でインターネットに接続している不正アクセスポイントを判定することが可能である．

e）経路情報とホップ数

TCP/IP を使った通信で目的のホストに接続するとき，通信パケットは様々なルータを経由する．経路情報は，目的のホストに通信が到達するまでにどのルータを経由するのかという情報である．また，ホップ数とはこの時経由したルータの数である．

不正アクセスポイントを経由し，インターネットに接続されると異なる経路を通ることがある．例えば，不正アクセスポイントへ接続していない通信であれば直接正規のアクセスポイントを通る経路となるが，インターネットの接続方法が，「正規のアクセスポイントを中継する方法」であれば，不正アクセスポイントを経由する経路に変わる．この時，通常の場合と経路に差異が発生するので，それを用いて判定ができると考えられる．

これらの経路情報は traceroute コマンドを使用して調査することが可能であるが，環境によっては正しく結果が出力されないことがある．その場合にも対応するために，IP の TTL(Time To Live)を確認することでホップ数を調べる．TTL は，ルータでパケットがルーティングされる度に減少し，パケットがループすることを防ぐ用途で用いられる．

TTL のデフォルトの値は OS 毎に決まっている（例えば，Linux のデフォルトの TTL は 64）．よって，クライアントとサーバとの通信をパケットキャプチャし，IP のヘッダ情報の TTL を確認することで，ホップ数を確認することが出来る．基本的に同じネットワークであれば一定のホップ数でサーバまで辿り着くため，ホップ数に変化があれば途中で異なる経路を通っていることが推定できる．したがたって，この情報も，不正なアクセスポイントの判定に利用できると考えられる．

f）RTT

RTT(Round Trip Time)は，あるホストにデータを発信してから応答が返ってくるまでの時間である．サーバへ複数回通信を行い，その時間を測定する．

不正アクセスポイントを通る場合，RTT は不安定になると考えられる．これは，「正規のアクセスポイントに中継する場合」や「異なる回線を使用する場合」，通信が正規のアクセスポイントと異なる経路を通るからであ

る．また，無線は有線と比較して通信が遅延することが多い．ゆえに，インターネットに接続方法が異なるアクセスポイントに中継する場合には，この特徴が顕著になると考えられる．このような性質から，RTT の平均値と標準偏差は判定に利用できると考えられる．このことを踏まえて，RTT 測定時に平均値，最大値，最小値，標準偏差を収集する．

ただし，正規のアクセスポイントを用いても，インターネット側の回線の使用率が高い場合やRTTを測定するサーバの負荷が高い場合など，不正アクセスポイントに関連しない要因でRTTが不安定になることも考えられる．そのため，この情報のみでは不十分であり，他の情報と組み合わせて判定に利用する必要がある．

（4）不正アクセスポイントの判定手順

提案手法では，（3）で示した情報を収集して，同じ SSID を持つアクセスポイントに過去に接続した時の情報と比較することで，不正アクセスポイントの判定を行う．判定の手順を，図 4 に示す．

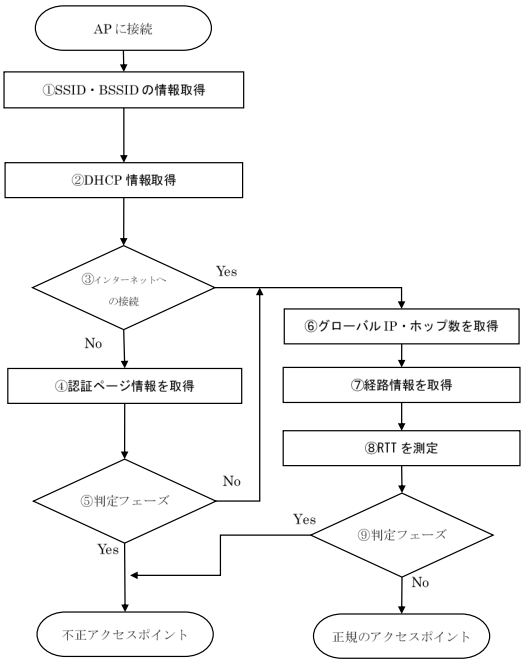

図 4　不正アクセスポイント判定手順

まず，無線 LAN アクセスポイントに接続すると，DHCP でネットワーク情報が与えられるので，それを収集する．

次に，インターネットへの接続の可否を確認する．これは，判定のフェーズで利用する一部の情報がインターネットに接続しなければ取得できないためである．

インターネットへの接続が出来ない時，認証ページがあると考えられる．この場合，そのページへリダイレクトされるので，まずそのページの URL,と IP アドレス，証明書の情報を収集し，その情報のみで不正アクセスポイントの判定を行う．表 1 に不正アクセスポイントを判定する基準を示す．

表 1　認証がある場合の判定基準

収集する情報	判定基準
IP アドレス	異なる
サブネットマスク	異なる
ネットワークアドレス	異なる
デフォルトゲートウェイ	異なる
DNS サーバの IP アドレス	異なる
DHCP サーバの IP アドレス	異なる
認証ページの URL	異なる
認証ページの IP アドレス	異なる
証明書の Common Name	異なる
証明書のシグネチャ	異なる

この基準に当てはまらなければ，不正な認証ページではないと判断し,認証ページにID,パスワードを入力し，インターネットへの接続を可能にする．

インターネット接続が可能になると，インターネット上のグローバルIPアドレスの情報や経路情報の取得が行える．ここでアクセスするのは，グローバル IP アドレスを入手するための専用のプライベートのサーバである．また，そのサーバに対して HTTP プロトコルを使って RTT を測定する．

ここで収集した情報を表 2 に示した基準で判定する．そして，この基準に当てはまらなければ，不正アクセスポイントではないと判定する．

表 2　インターネット接続が可能な場合の判定基準

収集する情報	判定基準
IP アドレス	異なる
サブネットマスク	異なる
ネットワークアドレス	異なる
デフォルトゲートウェイ	異なる
DNS サーバの IP アドレス	異なる
DHCP サーバの IP アドレス	異なる
グローバル IP アドレス	異なる
組織	異なる
TTL	異なる
経路情報	異なる
RTT 平均値	しきい値よりも大きい
RTT 最大値	しきい値よりも大きい
RTT 最小値	しきい値よりも大きい
RTT 標準偏差	しきい値よりも大きい

５．提案手法の評価

本章では，４で提案した手法を用いて不正アクセスポイントを判定可能であるか評価実験を行う．評価実験は，実験室に不正アクセスポイントを使った Evil Twin 攻撃が実験できるネットワーク環境を用意して行った．

（１）実験環境

実験を行う環境を図 5 に示す．

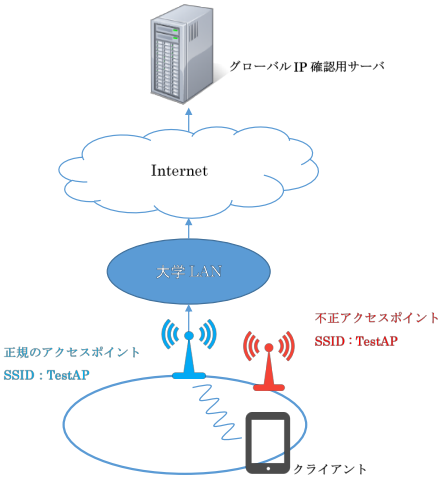

図 5　実験環境

不正アクセスポイントは，ノート PC に Linux で動作するアクセスポイントを作成できるソフトウェアをインストールして実現した．表 3 にそのアクセスポイントの設定を示す．

表 3　不正アクセスポイントの設定

項目	内容
SSID	TestAP
BSSID	00:1D:73:42:5C:31
channel	8
LAN 側 IP アドレス	状況により変化
その他	・DHCP サーバによる LAN 側ネットワーク情報の配布 ・NAPT によるアドレス変換 ・DNS は大学のものを使用

正規のアクセスポイントには，市販されている無線 LAN ルータを使用した．表 4 にそのアクセスポイントの設定を示す．

アクセスポイントに接続するクライアントには Android タブレットを使用し，表 5 に示すネットワーク情報を収集するツールをインストールした．

表 4 正規のアクセスポイントの設定

項目	内容
SSID	TestAP
BSSID	00:1D:73:42:5C:30
channel	1
LAN 側 IP アドレス	192.168.11.1/24
その他	・DHCP サーバによる LAN 側ネットワーク情報の配布 ・NAPT によるアドレス変換 ・DNS サーバは AP が持つものを使用

表 5 収集に使用するツール

アプリ名	内容
WiFiInfoChecker	オリジナルの情報収集ツール
Httping	HTTP で RTT を測定するツール
Traceroute	Traceroute を行うツール

WiFiInfoChecker は今回の評価のために実装したツールで，Android API 経由で WiFi 情報と DHCP 情報，インターネット上に構築したグローバル IP 確認用サーバと通信して，グローバル IP アドレス，IP アドレスが割り当てられている組織，サーバでパケットキャプチャした IP パケットの TTL を確認することが可能である．

（２）実験方法

不正アクセスポイントの攻撃パターンを作成する．表 5 に実験した攻撃パターンを示す．なお，２（２）で述べた攻撃シナリオはすべてのパターンで「正規のアクセスポイントとの共存」をしている場合とし，ネットワークの認証はないものとする．

表 6　攻撃パターン

パターン	インターネット接続方法
1	正規のアクセスポイントに中継
2	異なる SSID を持つ AP に接続
3	有線接続
4	異なる回線を使う方法

この攻撃パターンにおいて，次の方法で実験を行い，判定に使用する情報を収集した．

① タブレットで SSID “TestAP” を選択して接続
② WiFiInfoChecker を起動して収集した結果を保存
③ Traceroute を実行して，グローバル IP 確認サーバへの経路情報を保存
④ Httping でグローバル IP 確認サーバへ 100 回リクエストを送信し，RTT の各値を保存．その後，平均値，最大値，最小値，標準偏差を計算した．

表 7　実験結果

タイプ	項目	パターン 1	パターン 2	パターン 3	パターン 4
DHCP	IP アドレス	異なる	異なる	異なる	異なる
	サブネットマスク	一致	一致	一致	一致
	ネットワークアドレス	異なる	一致	一致	一致
	デフォルトゲートウェイ	一致	一致	一致	一致
	DNS サーバ	異なる	異なる	異なる	異なる
	DHCP サーバ	異なる	一致	一致	一致
グローバル IP	グローバル IP	一致	一致	一致	異なる
	組織	一致	一致	一致	異なる
経路・ホップ数	TTL	異なる	一致	一致	異なる
	経路情報	異なる	一致	一致	異なる
RTT	RTT 平均値 (65.62ms)	98.6ms	130.88ms	60.74ms	290.48ms
	RTT 最大値 (243ms)	1067.0301ms	1098ms	94ms	2595ms
	RTT 最小値 (45ms)	45.0ms	47ms	43ms	160ms
	RTT の標準偏差 (20.79)	154.57956	231.7549	8.3613	358.0201

（３）実験結果と考察

この実験の結果を表 7 に示す．RTT 以外の項目は，正規のアクセスポイントに接続した時に取得した情報と不正アクセスポイントに接続した時の結果である．RTT は計算した値である．

DHCP 情報による判定は，パターン 1 の場合で最も有効である．これは，正規のアクセスポイントを中継する場合，必ず異なるネットワークとなるため，配布されるネットワーク情報に差異が出来るためである．なお，他のパターンでは，DHCP で配布された情報は正規のアクセスポイントと一致していたので，この情報で判定を行うのは難しい．しかし，実際に不正アクセスポイントが設置される環境では，ネットワーク設定を同じにするとは限らない．例えば，今回不正アクセスポイントの起動スクリプトには，DNS サーバを使用する設定はなかったため，外部の DNS サーバを使用した．その結果として，DNS の設定に差異が生じた．もし同じように設定を怠る攻撃者がいれば，この情報でも不正アクセスポイントの判定が可能であると考えられる．

グローバル IP アドレス情報による判定は，異なる回線を使った時のみに有効であった．正規のアクセスポイントでグローバル IP アドレスが変わることはほとんどないため，確実に判定出来ると考えられる．

RTT の統計値による違いは，1,2,4 で顕著に見られた．これは無線区間がパターン 3 に比べて多かったためである．この結果から，RTT は無線 LAN を中継してインターネットに接続する場合の判定に有効だと考えられる．しかし，今回の実験ではネットワークの他の区間での遅延を考慮してない．そのため，この値だけでなく，複数の情報を用いて判定を行うことは有用であると考えられる．

６． 結論

本稿では，ネットワークの情報を利用して不正アクセスポイントを判定する手法を提案した．また，評価実験によって提案手法を用いて限定的ではあるが不正アクセスポイントを判定することが確認出来た．それにより，本手法を用いて不正アクセスポイントを判定することが実現可能であることを示すことが出来た．

今後は，今回実験を行わなかったさらに多くの攻撃パターンで実験を行うことでより多くの場合で示す必要がある．また，実際に無線 LAN が運用されている環境でも本手法が実現可能であるかも示す必要がある．

参考文献

1) Fabian Lanze, Andriy Panchenko, Igancio Ponce-Alcaide, Thomas Engel, "Undesired Relatives: Protection Mechanisms Against The Evil Twin Attack in IEEE 802.11," 2014.

2) Somayeh Nikbakhsh, Azizah Bt Abdul Manaf, Mazdak Zamani, Maziar Janbeglou, "A Novel Approach for Rogue Access Point Detection on the Client-Side," 2012.

3) Hossen Mustafa, Wenyuan Xu, "CETAD: Detecting Evil Twin Access Point Attacks in Wireless Hotspots," 2014.

4) Omar Nakhila, Erich Dondyk, Muhammad Faisal Amjad, Cliff Zou, "User-Side Wi-Fi Evil Twin Attack Detection Using SSL/TCP Protocols," 2015.