[Work in Progress] 研究報告

無線 LAN 環境における遅延ゆらぎに着目した不正アクセスポイントの検知の初期検討

張紫薇[†1]　長谷川皓一[†1]　山口由紀子[†1]　嶋田創[†1]

Initial Study of Rogue Access Point Detection using Delay Fluctuation in Wireless Network

近年，無線 LAN の利用拡大に伴い，そのセキュリティに対するニーズが高まっている．例えば，公衆無線 LAN 環境で，正規のアクセスポイント(AP)になりすまし，通信の盗聴や改ざんを行う不正 AP の脅威がある．不正 AP は正規 AP と同じ SSID と MAC アドレスを持ち，正規 AP より強い電波を送信するか，Deauthentication 攻撃を行い，クライアントと正規 AP との接続を強制的に中断させることで，クライアントを不正 AP に接続させる．この手法は Evil Twin 攻撃と呼ばれており，非常に容易に実行可能である．また，本物の AP であると利用者に信じ込ませるためには，クライアントにインターネット接続を提供する必要がある．これには,「正規の AP に中継する」「異なる回線を使う」などの方法がある[1].

不正 AP の検知に関する既存の研究は，管理者側での検知を目的として行われているものが多い．そこで，本研究では，クライアント側での検知を目的とする．

不正 AP は，正規 AP の振る舞いを模擬しているが，バックボーンネットワークや認証サーバのスペック(WPA-E AP の場合)まで全く同じ設定にすることはできない．そのため，正規 AP と不正 AP では，AP から先の通信の過程で遅延や遅延ゆらぎの差が生じ，過去の正規 AP への接続時の遅延情報をもとに，不正 AP を識別できると考える．今回は図 3-1 に示すように，「異なる回線を使う」形の不正 AP が存在する環境において実験を行った．

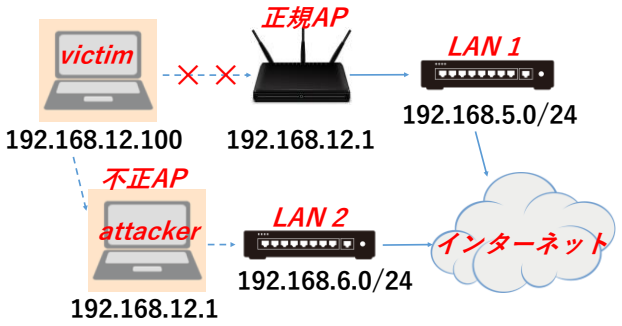

図 1 実験環境の構成

不正 AP は，Ubuntu 環境で構築し，正規 AP とは異なる LAN に接続した．正規 AP 側の LAN は PC ルータによって学内ネットワークに接続され，不正 AP 側の LAN は Cisco 製ルータにて学内ネットワークに接続される．また，不正 AP は正規 AP と同じ IP アドレス，SSID また異なる MAC アドレスを設定した．クライアント(victim)では Wireshark を利用して通信遅延を測定した．

インターネット上での遅延測定用の定点サーバとして Google のウェブサーバを選定し，正規 AP と不正 AP のそれぞれに接続した場合について，HTTP 通信のパケットを各 100 回キャプチャした．

評価する遅延時間は，TCP 3-way handshake でクライアントが SYN を送った後，サーバ側から SYN/ACK が返って来るまでの時間としている．今回は予備評価の段階のため，AP までの遅延の差分は取っていない．

評価結果を表 1 に示す．不正 AP 経由の場合の平均遅延が，正規 AP 経由の場合より大きかった．これは，836ms と 284ms という 2 つの異常値が平均と分散を押し上げたためである．なお，正規 AP および不正 AP の双方から大きい方から 5 個の遅延を覗いた平均値においても，正規 AP 側が 11ms に対して不正 AP 側が 15ms となり，明確な差異が出た．

表 1 遅延の測定結果

	正規 AP	不正 AP
平均(ms)	12	28
分散	0.032	7.528

現段階では，電波干渉などによる遅延の変動が少ない無線 LAN 環境においてクライアントからインターネット上の定点サーバまで遅延で評価しているが，実環境では，無線 LAN 側での遅延変動が大きくなると考える．そのため，クライアントから定点サーバまでの遅延より，クライアントから AP までの遅延の差分を取り，AP から先のバックボーン遅延をもとに，正規 AP と不正 AP の判別を試みる．

また，異なる時間帯やインターネットの利用者数など実験結果に影響を及ぼす要素を考慮するため，より大規模な無線 LAN 基盤にて長期的な評価を行う．

参考文献

[1] 保要隆明，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，法政大学大学院理工学・工学研究科紀要，Vol. 57, pp. 1-8, 2016 年 3 月.

†1 名古屋大学