7S-04

インターネット到達性確認パケットの推定・追跡を用いた不正アクセスポイント検出手法

竹田智洋† 大平健司‡ 谷岡広樹‡ 佐野雅彦‡ 松浦健二‡ 上田哲史‡
徳島大学 工学部† 徳島大学 情報センター‡

1. はじめに

無線 LAN を利用する機会の増加にともない，セキュリティ上の課題が増加している．無線 LAN は電波を用いて通信を行っており，電波が届く範囲であれば傍受や妨害電波による攻撃が可能である．セキュリティ上の課題の 1 つとして，組織内に許可を得ず設置したアクセスポイント(以下 AP)や正規の AP を装った AP（以下不正 AP）に関する問題が存在する．これらの AP は不正アクセスの入り口となることが多く，情報漏洩等のセキュリティリスクを高めている．よって本稿では，不正 AP に関する脅威を取り除くため，不正 AP の検出手法について提案する．

2. 従来手法

不正 AP の検出手法としては，大別してネットワーク上流の有線 LAN 側から検出する方法，末端の無線 LAN による通信を傍受し検出する方法，有線 LAN と無線 LAN の双方を用いて検出する方法の 3 種類存在する．

有線 LAN 側での推定方法として，無線 LAN のアクセス遅延が大きい特徴を利用し，無線 LAN で接続されている機器を推定する手法[1]があるが，現在では無線 LAN の高速化により適用できない場合が増加している．

無線 LAN 側での検出方法として，事前に正規 AP の SSID や BSSID，使用チャネル等を登録しておき，特定対象の AP の発する情報と比較する事により，不正 AP を検出する手法[2]が存在する．この手法は事前に情報を作成せねばならず，多大な管理コストが発生する．

有線/無線 LAN の双方を用いて検出する手法として，トラヒックの相関から両者のフローが一致するかどうかを識別することにより不正 AP を検出する手法[3]がある．こちらの手法は LAN 内のクライアント同士の通信の割合が多いと正しく検知できないデメリットが存在する．

A Rogue Access Point Detection Method with Estimation and Trace of Internet Reachability Check Packets
†Tomohiro Takeda
†Tokushima University

3. 提案手法

無線 LAN 側と有線 LAN 側の双方を観測し，無線 LAN 接続直後に流れるインターネット到達性確認パケットが流れたと思われる時刻を比較することにより，管理対象有線ネットワークに対象 AP が接続されているかの判定を行う．

有線 LAN 側から流れるパケットは暗号化されていないが，通信量が膨大である可能性が高いので，インターネット到達性確認パケットの GET リクエストを検知し取得する．

無線 LAN の通信は暗号化されていることが多いため通信内容を解析することは出来ないが，インターネット到達性確認パケットの HTTP レスポンス（以下 HTTP レスポンス）のパケット長が OS 毎に一定である特性を利用し，無線 LAN 通信のパケットの暗号化されたフレーム長から HTTP レスポンスを推定する．また，このパケットはクライアントが無線 LAN に接続した直後に流れるため，クライアントの無線 LAN 認証パケットも取得し推定の材料とする．

OS 毎にインターネット到達性を確認する URL が異なるため，有線側・無線側の双方のパケットを解析することにより，インターネット到達性確認パケットを流したクライアントの OS も特定が可能である．よって，有線 LAN 側からのパケットと，無線 LAN 側からパケットに関して，それぞれに OS 並びに流れた時刻が解る．したがって，無線 LAN 側で観測された HTTP レスポンスと推定されるパケットの流れた時刻を基準に，有線側から観測できるインターネット到達性確認パケットの GET リクエストの中で，OS が同じでかつ最も時刻が近いパケットを選択し，基準にしたパケットとの時間差を求め，一定の範囲に集中するかどうかで判定を行う．ただし各観測機器の時刻は同期されているものとする．

検査対象の AP が監視している有線ネットワークに接続されていた場合は，有線 LAN 側と無線 LAN 側で観測したパケットの時間差はインターネット到達性確認パケットの送受信に掛かる時間に対応するため，一定の範囲に集中する．

4. 評価実験

NAPT を兼ねた 2 つの AP を実験ネットワーク内に設置し，実験ネットワーク上流の有線ネットワークを流れる通信と無線 LAN を用いた通信のパケットを取得し，提案手法を用いて推定・比較を行うことで，上流の有線ネットワークから見た IP アドレスと無線 LAN の通信を行っている AP の紐付けが可能かどうかを確認した．なお本実験では，HTTP レスポンスの推定にあたり，認証パケットが流れてから 10 秒以内に流れたパケットに範囲を絞り推定を行った．

4.1 評価環境

Windows 並びに Android の OS が入った無線 LAN クライアントを各 2 台用意し，NAPT を兼ねた AP に接続した．短時間に大量のインターネット到達性確認パケットを取得するため，Windows では無線 LAN の接続・切断を繰り返すバッチファイルを実行し，Android では手動で無線 LAN 接続の ON/OFF を行い，約 20 分間測定した．

有線ネットワークを流れるパケットは，実験ネットワーク上流に設置したソフトウェアルータで tcpdump を用いて取得した．無線 LAN フレームについては，Raspbian を導入した RaspberryPi B+と Planex GW-900D を用い，モニターモードで取得した．

4.2 評価結果

上流の有線ネットワークから見た，ある IP アドレスが送受信先である通信のダンプデータと，対応する AP が送受信先である無線通信のダンプデータを元に提案手法を用いて 312 パケットを HTTP レスポンスであると推定した．また，対応しない AP が送受信先である無線通信のダンプデータを元に 119 パケットを HTTP レスポンスであると推定した．それぞれの時間差をヒストグラムとして表したものが図 1，図 2 である．

5. 考察

図 1 では-1.5 秒から 2.0 秒の範囲に時間差が集中した．時間差として負の値が算出されている．これは，短い間隔で複数のインターネット到達性確認パケットが送受信された場合，推定した HTTP レスポンスに最も近い HTTP GET リクエストとの時間差を求めているため，リクエストとレスポンスの対応関係に差異が生じ，誤差が生じたものと考えられる．

図 2 では，-4.0 秒から 4.0 秒の範囲に時間差が集中せず表示された．これは評価実験にて約 10 秒毎に無線 LAN の再接続を行ったためであると考えられる．

6. まとめ

本稿では不正 AP の対策の 1 つとして，検査対象 AP が管理対象有線ネットワークに接続されているかどうかを確認する手法を提案した．

評価実験を行い，検査対象 AP の送受信データが暗号化されている場合でも，インターネット到達性確認パケットを推定・追跡することにより，当該 AP が管理対象有線ネットワークに接続されているか否かを識別できることを確認した．

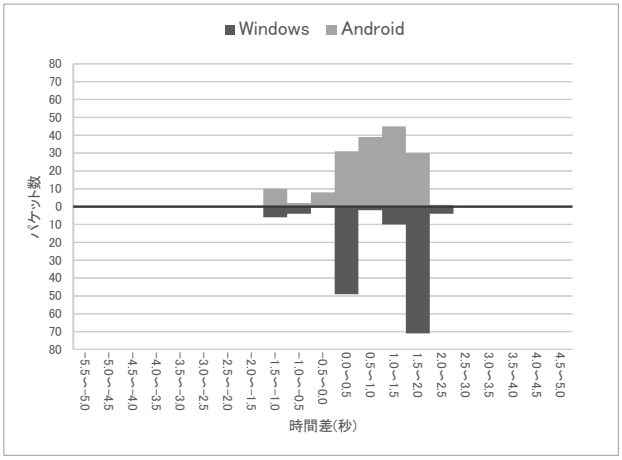

図 1 対応する組み合わせの時間差

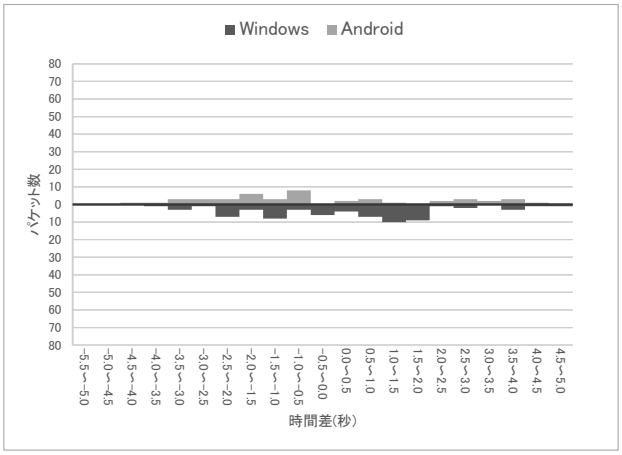

図 2 対応しない組み合わせの時間差

参考文献

[1] R. Beyah, S. Kangude, G. Yu, B. Strickland and J. Copeland : Rogue Access Point Detection using Temporal Traffic Characteristics, IEEE GLOBECOM (2004).
[2]S. Thakur and B. Abhijit : RAPD Algorithm: Detection of Rogue Access Point in Wireless Network, Vol. 3, No. 6, pp. 85-89 (2013).
[3] 川田 丈浩, 矢田 健 : 無線/有線 LAN トラヒック分析による不正アクセスポイント検出法の提案, 信学技報, vol. 114, No. 373, pp. 1-4 (2014).