L-027

不正アクセスポイントについての研究及び検知ソリューションの提案
Research on Rogue Access Point and The Proposal of Detection Solution

盧 仕斌† 大久保 隆夫†
Lu Shibin Okubo Takao

1. はじめに

無線技術の発展及びモバイル端末の普及に伴い、街中にある喫茶店、レストランなどの商業施設に多数の無線 LAN アクセスポイント（AP：Access Point）が設置されて、インターネットサービスを提供している。その一方で、多くのセキュリティ上の危険がある。電波の開放性のため、電波が届ける範囲内の端末は電波を傍受することで、通信内容が盗聴できる。更に 802.11 の管理フレームや制御フレームは認証と暗号化が提供されていないため、攻撃者が不正 AP（Rogue AP）を立ち上げ、フィッシングサイトに誘導し、正規 AP のサービス提供を妨害するなどの脅威がある。本稿ではクライアント端末側に使用できる不正 AP を検知するソリューションを提案する。

2. 従来の検知手法

不正 AP の検知手法について、以下の三種類が存在している：ネットワークの有線 LAN 側からの検出手法、端末の無線 LAN 側トラフィックの特徴を利用する検知手法、及び有線 LAN 側と無線 LAN 側の両方を用いるハイブリッド検知手法。

有線 LAN 側の検知手法は、ゲートウェイを通過するトラフィックを分析し、時間上の特徴によって不正 AP を検知する。例えば、トラフィックの到着時間の間隔時間の差異[1]、RTT のタイムスタンプの差異[2]を利用する。このような種類の検知手法は、無線 LAN の高速化、及びトラフィックの整形処理により適応が困難になる。

無線 LAN 側の検知手法は、無線 LAN エリア内に、多数のセンサーを設置して受動的にトラフィックを監視し、事前に認証されていない AP の MAC アドレス、メーカー、SSID と RSSI などの情報が発見されれば、不正 AP として検知する。この手法の例としては Motorala の AirDefense、Venustech の TianQing がある。その他、802.11 のフィンガープリントに基づく主動的な検知手法が提案されている。この手法は AP のチップ、ドライバーなどの攻撃者が偽装しにくいフィンガープリントを利用して不正 AP を検知する。例としては Bratus らは想定外の 802.11 管理フレームを AP に発送して反応によって不正 AP を検知する手法[3]を提案した。このような種類の検知手法は、事前に正規 AP のフィンガープリントの収集が必要のため管理コストがかかる。

有線 LAN 側と無線 LAN 側の検知手法を組み合わせるハイブリッド検知手法が、Ma らに提案された[4]。このような種類の検知手法は主動的な攻撃が発見でき、無線 LAN を監視するセンサーがいらず、将来システムの拡張に有利な、次世代の不正 AP 検知手法だとみられている。

†情報セキュリティ大学院大学 Institute of Information Security

3. 提案手法

個人利用者に対して、喫茶店などの商業施設に入って、初めて施設の無線 AP に接続する場合、正規 AP のフィンガープリントを持たないため、従来の不正 AP 検知手法は、利用できなくなる。そのため、本稿では利用者の端末に使用できるホワイトリストが不要の不正 AP を検知するソリューションを提案する。

3.1 ステップ 1

無線 LAN 側のクロックスキューに基づく検知手法[5]を利用して、接続したい SSID に所属する AP の数量、MAC アドレスとチャネル情報を取得する。

クロックスキューとは、電子回路において、クロック回路から送られるクロック信号が、AP に使われる時間計算用の水晶の周波数は差異があるため、802.11 ビーコンフレームが異なるタイミングで到着する現象である、AP ごとに違うため、この特徴は、攻撃者は改ざんが困難である。

オープンツールの Scapy を利用して、無線 AP から発送するビーコンの端末到着時間とビーコンに含むタイムスタンプを収集し、前の一つのビーコンの到着時間とタイムスタンプのそれぞれの差を算出すると、到着時間の差とタイムスタンプの差で直線が作られ、直線のスロープはクロックスキューとする。複数 AP の場合、複数の直線が作られる。これにより、攻撃者は不正 AP の SSID と MAC ドアレスを正規 AP と同じになっても検知できる。しかし施設に中継 AP がある場合、不正 AP を区別ができない。

3.2 ステップ 2

WindowsOS の WLANAPI を呼び出し、利用者のいる場所に接続したい SSID の RSSI を取得する。RSSI とは、受信側での受信された電波強度のインジケータである、端末のネットワークカード（NIC）に測定されるため、攻撃者は RSSI の偽造や改ざんが不可能となる。RSSI を取得した後で、RSSI により定位するロケーション技術を利用して，下記の公式（1）によって AP と端末の距離を算出する。

$$D = 10^{(ABS(RSSI)-A)/(10*n)} \quad (1)$$

公式中、n は電波の周波数が障害物によっての経路損失係数、範囲は 2～3.5、A は AP から 1M のところの RSSI の絶対値、いろいろな環境に測定して、n は 2.638 である、A は 28.926dBm である[6]。

三角定位法で AP の位置を算出するため、利用者は、以下のような間隔が 2M の三つ場所 A(2,0)、B(0,0)、C(0,2)から AP との距離を算出して、最終に AP の位置を取得する。取得した位置の AP が目測で施設所有のものかどうか確認する。

3.3 ステップ 3

Copyright © 2019 by Information Processing Society of Japan and
The Institute of Electronics, Information and Communication Engineers
All rights reserved.

ステップ１と２で取得する情報をまとめて、以下のフロー（図１）で不正 AP を判定する。

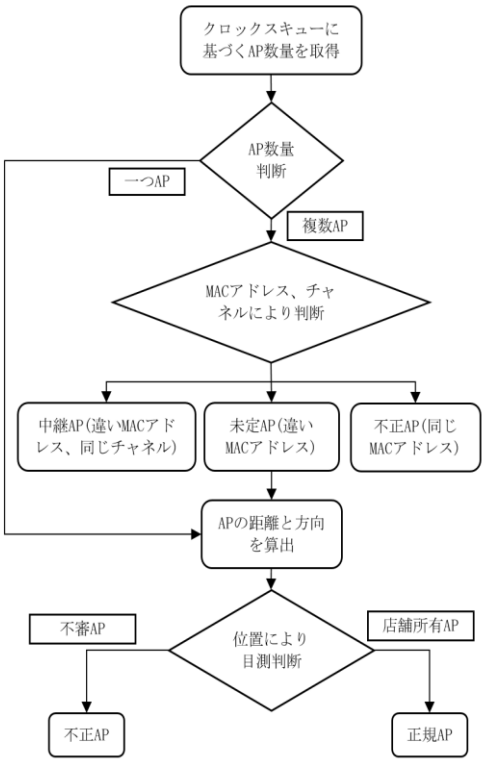

図 1　不正 AP 判定フロー

4. 評価実験

正規 AP が屋内に置く、提案のソリューションを用いて、ビーコンのクロックスキュー及び RSSI で算出した AP の位置は、不正 AP の実際の位置と比較してソリューションを評価する。

4.1 評価環境

Windows 環境に Scapy が入るノート PC が 1 台、正規 AP とするルータが 1 台、不正 AP とする USB 無線アダプタが 1 台と 802.11Beacon 収集する USB 無線アダプタが 1 台を用意する。正規 AP と不正 AP の SSID は“testAP”とする。

4.2 実験結果

不正 AP は正規 AP と同じ部屋に置いて、図２がステップ１によって算出した“testAP”のクロックスキューである、二つ線が二つ AP を証明できる、図３がステップ２によって、A、B と C の三つ点から算出した不正 AP の距離と大体の位置（※RSSI により算出した距離は誤差があるため確実な位置ではない）を示す。

5. おわりに

本稿は、不正 AP の検知手法の一つとして、接続したい AP の位置より不正かどうかを判断する手法である。実験結果によって、提案したソリューションで取得する AP 位置を利用して、利用者は自身で接続したい AP を確認することができるため、自分を守る一歩である。

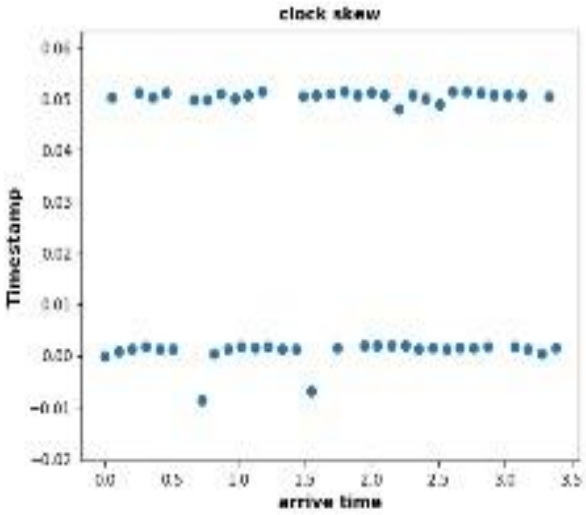

図 2　クロックスキュー

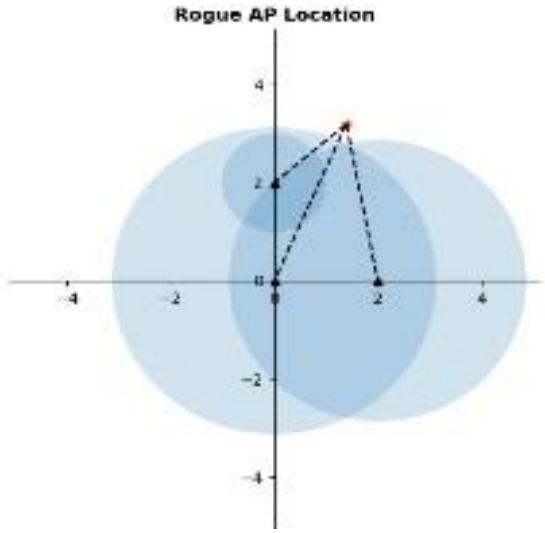

図 3　AP 位置

参考文献

[1] Beyah R, Kangude S, Yu G, et al. “Rogue Access Point Detection Using Temporal Traffic Characteristics”, IEEE Global Telecommunications Conference, GLOBECOM'04 (2004).
[2] Sheng B, TAN C C, Li Q, et al. “A timing-based scheme for rogue AP detection”, IEEE Transactions on Parallel and Distributed Systems, Vol.22, Issue.11 (2011).
[3] Bratus S, Cornelius C, Kotz D, et al. “Active behavioral fingerprinting of wireless devices”, WiSec'08 Proceedings of the first ACM conference on Wireless network security, Pages 56-61 (2008).
[4] Ma L R, Teymorian A Y, Cheng X Z, “A Hybrid Rogue Access Point Protection Framework for Commodity WiFi Networks”, IEEE INFOCOM 2008 - The 27th Conference on Computer Communications (2004).
[5] Jana S, Kasera S K, “On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skew”, IEEE Transactions on Mobile Computing, Vol.9, Issue.3 (2010).
[6] Wang P F, Luo Y F, et al. “Research on WiFi Indoor Location Algorithm Based on RSSI Ranging”, 2017 4th International Conference on Information Science and Control Engineering (ICISCE) (2017).

Copyright © 2019 by Information Processing Society of Japan and
The Institute of Electronics, Information and Communication Engineers
All rights reserved.