4D-04

大規模環境における悪意あるアクセスポイントの検知方式の検討

石倉禅 †　竹内格 †　大田幸由 †
†NTT セキュアプラットフォーム研究所

1　はじめに

公衆 Wi-Fi 環境整備が日本国内で推進されている。公衆 Wi-Fi は便利である一方で、セキュリティ上の問題が指摘されている。中でも、悪意のアクセスポイント (Rogue AP; RAP) による攻撃が懸念されており、IPA が昨年発行した公衆 Wi-Fi 利用者向けのガイドライン [1] をはじめ、多くのセキュリティ有識者が警戒が呼びかけている。RAP は、攻撃者が持ち込んだ AP から、攻撃者の NW に利用者の端末 (ユーザー端末) を誘導する AP であり、個人情報窃取やマルウェア配布といった脅威の前段である。また、RAP は正規に設置された実在する AP(Legitimate AP, LAP) と同一の SSID や暗号化キー等のプロファイルを設定 (詐称) することが可能である。ユーザー端末は過去に接続した AP の情報を記憶し、自動で再接続する設定となっている場合が多く、ユーザーが自覚しないうちに RAP と接続してしまう可能性がある。

2　RAP 対策の現状

RAP 対策は、WIPS(Wireless Intrusion Prevention System) の機能を搭載した無線 LAN コントローラが設置される一部の企業 NW では実施される一方で、公衆環境においては、RAP 対策が実施されている例は確認されていない。公衆無線 LAN サービス提供者向け [2] および利用者向け [3][4] に総務省が提供しているガイドラインには、「暗号化及び認証の情報セキュリティ方式に対応したアクセスポイントを設置すること (中略) など、適切な情報セキュリティ対策を講ずることが望ましい」と記述されている一方で、下位互換性の為にこれらの対策は実施されていない。また、AP の識別子として利用される SSID や BSSID は、攻撃者による詐称が容易であることから、利用者へ不審なアクセスポイントへの注意を呼びかけるだけでは、対策として不十分である。

Detecting Wi-Fi Rogue Access Point in Massive-Scale Environment
Zen ISHIKURA†, Kaku TAKEUCHI†　Yukiyoshi OTA †
†NTT Secure Platform Laboratories

3　目的および報告概要

本研究の目的は、どこでも安全に Wi-Fi を利用できるようにするために、公衆環境にも適用可能な RAP 対策技術を確立することである。本報告においては、先行技術を公衆環境に適用する上での問題点を整理し、LAN 内の L2 または L3 ローミングが可能である大規模な Wi-Fi 環境における RAP の検知方式を示す。

4　先行技術

4.1　機器指紋を用いた手法

Tien ら [6] は、一定時間 AP からビーコンを受信し、電波の周波数帯や時間的な揺らぎから KL 情報量を算出することで、AP 機器が使用している Wi-Fi のチップセットを同定する手法を示した。RAP が LAP と同時に存在していない状況下で本手法は有効であるが、RAP が LAP と同時に存在する場合、同定が困難となる。

4.2　電波分布を用いた手法

WIPS は、オフィス等で使用される無線 LAN セキュリティ対策製品のひとつである。無線 LAN コントローラ配下にあるアクセスポイントがアンテナとなり、周囲の電波分布をモニタする。モニタした電波分布は、オフィスのフロアマップに投影したモニタ画面として管理される。LAP の位置および LAP の電波分布を事前に正常状態として保持し、運用時に電波分布が正常状態と異なる場合、異常検知として NW 管理者に報告するものである。

WIPS を公衆環境で利用する上での問題点は、正常状態のデータ作成にあると考えた。

オフィス環境においては、特定の人物がある程度決まった通信機器を使用する一方で、公衆環境においては、不特定多数の人物が出入りするために、正常状態のデータ作成が困難である。(a) 正常時と運用時で電波分布が大きく変化すると、LAP のみが存在する環境であっても、LAP を RAP であると誤判定する可能性がある。(b) 運用時と同様の電波分布を正常状態を定義しようとした場合、その環境に RAP が混在していない、ということを保証できない。

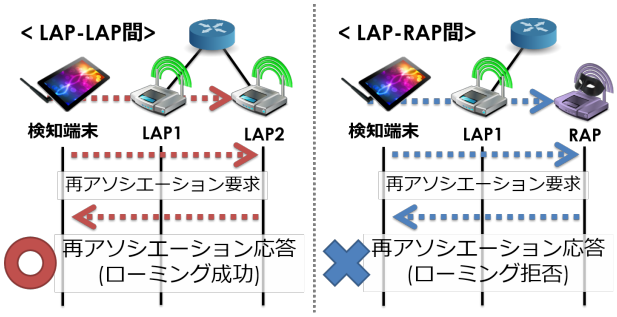

図 1: 再アソシエーションにおけるパケットシーケンス

4.3 RSSI-位置を用いた手法

Nazrul ら [5] は、LAP が発信するビーコンパケットの情報エレメント内に、RSSI と距離を変換するパラメータを挿入し、ビーコンパケットを受信したユーザー端末がそのパラメータを用いて AP の位置を算出することで、LAP と RAP を判別する手法を提案した。
本方式の問題点は、4.2 節と同様、事前に測定する正常時の電波環境と運用時の電波環境の違いにより、LAP を RAP であると誤判定する可能性があることである。

5 提案方式

5.1 要件とアプローチ

考案すべき方式の要件が少なくとも 2 点あると考えた。4.2 節で述べたように、正常状態の定義が困難であるから、データ参照することなく検知できることが第一の要件である。また、公衆 Wi-Fi は既に数多くの AP 機器が設置されているため、これらを更改することなく実施できることが第二の要件である。上記 2 点の要件を満たすのは、正常状態の定義が必要なく、また既設の AP 機器が使用している Wi-Fi 標準規格のパケットを用いる方式である。また、RAP は攻撃者が外部から持ち込まれるため、無線 NW で観測できない情報を模倣することはできない。したがって、複数の AP が有線 NW を介して実現するローミングを用いて、RAP 検知が可能であると考えた。

5.2 提案方式の概要

図 1 に、ローミングの手続きである再アソシエーションにおけるパケットシーケンスを示した。攻撃者が、LAP2 の BSSID を偽装すると仮定し、検知端末は LAP1 に接続しており、LAP2 の BSSID をもつ AP に対してローミングを行うものとする。LAP-LAP 間 (左) においては、検知端末が LAP2 に再アソシエーション要求を発信すると、LAP2 は応答として、検知端末へ再アソシエーション応答パケットを送信する。この再アソシエーション応答パケットの中には、状態コードが記載されており、ローミング可否、また拒否の場合は理由が記される。LAP 同士は、バックグラウンドで有線 NW で接続しており、検知端末が LAP1 で通信していたフレームを LAP2 に渡すことができるため、ローミングが成功する。一方、LAP-RAP 間 (右) の場合は、RAP は攻撃者による持ち込み型の AP であるため、有線 NW に属しておらず、ローミングの設定ももたないため、再アソシエーション応答パケットの中では再アソシエーション失敗の状態コードを応答することとなる。そして、再アソシエーションに失敗した AP を RAP として検知する。

6 おわりに

本報告においては、ローミング可能な環境における RAP 検知手法を提案した。提案手法は、現在主にオフィス環境で用いられている WIPS の方式が潜在的に抱える問題を回避しており、また既設の公衆 Wi-Fi 環境にも適用可能である。今後は、今回検討した RAP 検知方式を実装し、実際の公衆 Wi-Fi 環境で評価する予定である。先行研究例は確認されておらず、課題は下記の 2 点であると考えた。(1)RAP 検知技術評価指標の選定。LAP/RAP の判別率以外にも、利用チャネルの S/N 比に対する位置特定精度等、技術を評価する指標の選定が必要である。(2) 実際のフィールドでの検証方法の検討。被害や攻撃の傾向を把握する上でも、観測から着手する必要がある。

参考文献

[1] 野澤ら (IPA). 公衆無線ＬＡＮ利用に係る脅威と対策, March 2016.

[2] 総務省. 無線 lan ビジネスガイドライン第 2 版, Sep 2016.

[3] 総務省. Wi-fi 利用者向け 簡易マニュアル, Mar 2015.

[4] 総務省. 一般利用者が安心して無線ＬＡＮを利用するために, Nov 2014.

[5] Nazrul M. Ahmad and et al. A rssi-based rogue access point detection framework for wi-fi hotspots. *IEEE 2nd International Symposium on Telecommunication Technologies*, pp. 104–109, 2014.

[6] Tien Dang Vo-Huu, Triet Dang Vo-Huu, and Guevara Noubir. Fingerprinting wi-fi devices using software defined radios. *Proceedings of the 9th ACM Conference on Security; Privacy in Wireless and Mobile Networks*, pp. 3–14, 2016.