Vol.2015-IOT-28 No.42
2015/3/6

既知APの信号強度と位置情報を利用した組織内における未知AP探索システムの提案と評価

田原 義章[1,a)]　桝田 秀夫[2,b)]

概要：近年，無線技術の普及により多くの会社や大学などの組織で無線 LAN がインフラとして利用されている．しかしこれにより電波が届けば誰でも使えてしまうというセキュリティ面での問題や、無許可での無線 LAN AP の設置ができてしまうなどの問題も発生しており，有効なセキュリティ対策が必要となっている．そこで本研究では、組織で一元運用されており位置が判っている既知の無線 LAN AP の信号強度や位置情報を利用することで，問題のある未知の無線 LAN AP の位置を推定するシステムの提案と評価を行った．

Proposal of a System to Estimate the Location of Unknown Wireless APs by Utilizing the Signal Strength and Location Information of the Known APs

Yoshiaki Tahara[1,a)]　Hideo Masuda[2,b)]

Abstract: Recently, more organizations are using the wireless LAN infrastructure because of the widespread of the wireless technology. However, there are new problems about wireless LAN access points (AP) such as vulnerabilities in the security aspects or unauthorized establishments of access points at certain locations. Thus, there is a need to identify and address these problems before they occur. Therefore, in this study, I have proposed and evaluated a system to estimate the locations of the unknown or unauthorized wireless APs by utilizing the information obtained from the known or authorized establishments of wireless APs.

1. はじめに

無線 LAN は電波の届く範囲なら自由に動きながらデータ通信ができ，その手軽さゆえ職場や自宅，公共のスペースなど多くの場所で利用されている．しかし，無線 LAN の普及に伴い，新たな問題も発生している．例えば，安易なセキュリティ設定や無許可での AP の設置が挙げられる．AP は誰でも容易に入手でき，設置すれば初期設定の状態でも使用できるものが多い．しかし，初期設定の AP は暗号化や MAC アドレスの認証などのセキュリティが施されていないなど，セキュリティ対策が不十分である場合があり，そのことを知らずに AP を使用する場合がある．AP のセキュリティを疎かにすると，設置した AP の利用可能範囲にいる悪意のあるユーザが AP を無断使用したり，AP を利用している他のユーザの情報を盗聴するなどの問題が生じる可能性がある．また無許可で設置された AP は，近辺に設置してある他の AP と干渉して通信速度の低下の原因となったり，EvilTwin ホットスポット [2] と呼ばれるような公衆無線 LAN に見せかけた偽物の AP を設置しアカウントとパスワードを搾取するものもある．大学や企業に於いて，このような AP を放置するわけにはいかず，トラブルが生じる前に少しでも早くセキュリティ対策を施さなければならない，また無許可に設置された AP を発見し，対応することが求められる．

[1] 京都工芸繊維大学大学院 工芸科学研究科 情報工学専攻
Graduate School of Information Science, Kyoto Institute of Technology
[2] 京都工芸繊維大学 情報科学センター
Center for Information Science, Kyoto Institute of Technology
[a)] y-tahr14@dsm.cis.kit.ac.jp
[b)] h-masuda@kit.ac.jp

対応策としては，問題のある AP が設置されていることを当該機器管理者に指摘し，撤去やセキュリティを強化することが挙げられる．しかし，複雑な位置に設置された AP や，大学・企業などの AP を多く設置している場所では，問題のある AP の設置場所を特定するのは難しい．このため，問題のある AP の位置特定を補助する情報として AP の位置を推定するシステムがあれば有用であると考えられる．

そこで本研究では，ネットワーク管理者が可搬型の装置を持ち歩くことで，組織の管理下になく設置位置の不明な未知の AP(以下，未知 AP) の位置推定を支援する未知 AP 探索システムの試作と評価を行う．本システムは，ネットワーク管理者が既に運用しており，位置情報を持っている AP(以下，既知 AP) からの受信信号強度と観測場所の位置情報を元に位置推定を行えることを目指す．

以下，第二章において本研究に関連する研究について述べ，第三章で要求とそれに対する方針，第四章で未知 AP の位置推定を行うシステムの仕様，第五章で未知 AP の位置推定手順，第六章で行った実験とシステムの評価，最後に第七章で本研究の総括を行い，今後の課題について述べ，結言とする．

2. 関連研究

2.1 Air Patrol[1]

Air Patrol は Cirond 社が AP の位置推定を行うために開発したものである．AP を探索したい環境において Air Patrol Senser を複数の場所に設置する．設置した Air Patrol Senser は AP 情報を収集し，AP の位置や違法な帯域の無線電波の検知を行う．Air Patrol Senser で収集した AP 情報は位置情報の推定を行う Air Patrol Enterprise software へ自動的に送信される．複数の場所に設置された Air Patrol Senser の AP 情報をこのソフトウェアが解析し，無線 LAN AP の位置推定結果を表示する．

しかし，探索を行う場合 Air Patrol Senser を複数の場所にあらかじめ設置する必要がある．

2.2 Particle Filter[4] を用いた複数無線 LAN 基地局の位置推定手法

この手法は Wireless Search Assistant という探索支援システムを用いて情報収集と推定結果の提示を行う．

Wireless Search Assistant は機動性に優れた自走機に指向性アンテナ，無指向性アンテナ，GPS[3]，方向センサ，ノート PC，ヘッドマウントディスプレイ，推定ソフトウェアを搭載する．これにより，観測者は同時に運搬が難しい資材を運搬，使用することが可能になり，同時に迅速な移動が行えるようになる．

Wireless Search Assistant は GPS を用いて自走機の位置を取得し，方向センサによって自走機 (指向性アンテナ) の方向を取得する．AP の電波強度は指向性アンテナを用いて取得する．そしてヘッドマウントディスプレイを用いて観測者に AP の推定結果を逐次提示する．

Wireless Search Assistant によって探索する観測者の位置，指向性アンテナの方向，探索対象である AP からの受信電波強度を定期的に計測し，逐次推定を行う．蓄積されたデータと，距離と方向により決まる相対的な位置関係に関する受信電波強度のモデルを用いて AP の位置推定を行い，推定結果を観測者に逐次提示することで位置特定を支援する．

2.3 Place Engine[5]

PlaceEngine は，AP の電波を用いて無線 LAN 機器の現在位置を認識する技術である．GPS は GPS 衛星の見通せない屋内や地下では GPS 衛星の信号が受信できずに著しく精度が落ちたり使えないという弱点がある．それに対して PlaceEngine は，不特定の膨大な個数の AP から発信される MAC アドレスなどの情報を用いて位置認識を行うことで，地下や屋内でも位置推定を行うことができる．

PlaceEngine では，位置情報が必要になったときに以下の 3 つの情報を利用する．

- BSSID(MAC アドレス)
- SSID(ステーション名)
- RSSI(Received Signal Strength Indicator，受信信号強度)

PlaceEngine で推定を行うには，どの位置でどの AP が検出されるか，というデータベースが必要である．データベースは，ユーザによる位置検索や明示的な位置登録により更新され，それによって漸次的に発生する．

以下に PlaceEngine が，ユーザの位置を提示するまでの流れを以下に示す．

(1) ユーザは，近辺の AP から流れる電波を観測し，AP 情報 (MAC アドレス，電界強度などの情報) として取得する．
(2) ユーザは，AP 情報を PlaceEngine サーバーに送信する．
(3) PlaceEngine サーバーは，受け取った AP 情報と，あらかじめサーバーに蓄えられている AP 情報のデータベースとから，位置情報を推定し，その結果をユーザに送信する．

しかし，PlaceEngine の位置推定精度は，AP の密集度などユーザが位置を問い合わせた場所の AP 情報の状況や，その時点でのデータベースの状況により左右される．よって，AP が周囲にまったくないところでは位置推定は行えない．

3. 要求および方針

本章ではシステムに対する要求とその方針について述

べる．

3.1 要求

観測者が AP を探索するために必要な条件を以下に述べる．

- 観測のための専用装置を最小限にすること
  - 観測のために多数のセンサーを準備する必要がある場合，観測者の手間が問題となり，気軽に観測することができない．
  - 観測専用の機器ではなく，既存の設備を活用したり，通常の無線 LAN サービスにも使える構成が望ましい．
- 未知 AP の設置場所の推定精度は，部屋単位以下であること
  - 通常，部屋には管理責任者が割り当てられており，設置部屋まで特定できれば当該 AP の発見には十分と考えられる．

3.2 方針

- 既知 AP からの受信信号強度を元に位置推定を行う
  - 組織で既に運用している AP であれば，機器名，場所，識別信号 (SSID) が事前に判る．
  - 新規に観測専用装置を敷設する必要がない．
  - 新規に AP を増設すれば，推定に使える AP としてだけではなく，組織内無線 LAN 利用範囲の拡大にもなる．
- 無線 LAN アダプタと GPS が付いた機器を持ち歩いて位置推定結果を表示する
  - 推定した場所には最終的には訪問して現物を目視できる必要がある
  - 測定場所の移動は建屋内外と多岐にわたる

4. 未知 AP 探索システムの仕様

本章では前章にあげた要求を満たす未知 AP 探索システムの仕様について述べる．本システムは scan プログラム，scan データベース，search プログラムで構成される．scan プログラムによって周囲の AP の情報を取得し，この情報と既知 AP や観測者の位置情報を scan データベースに保存，保存したデータを search プログラムの入力として未知 AP の推定位置を出力するというのが未知 AP 位置推定の流れである．

システムの構成を図 1 に示す．次に scan プログラムの具体的な動作について述べる．

4.1 scan プログラム

scan プログラムは観測者の周辺に存在する AP を探索し，未知 AP の位置推定に必要な情報を得るためのプログラムである．観測者には周囲の無線 LAN AP に関する以下の情報の一覧を提示する．

- MAC アドレス
- チャンネル
- 信号品質
- 信号強度
- ESSID
- ビットレート

AP の情報取得方法として，周辺に存在する AP の情報を収集する「iwlist scan」コマンドを用いる．「iwlist scan」コマンドを使用することで図 2 のような形で周囲の AP の情報が得られる．

4.2 search プログラム

search プログラムは scan プログラムから得た観測者の周囲の AP の情報と，既知 AP や観測者の位置情報から未知 AP の位置推定を行うプログラムである．

以下に search プログラムの動作を示す．

(1) scan プログラムで作成されたファイルと，ファイルを作成した際の観測者の位置を読み込む
(2) 4.2.2 節の判別法によりファイル内の周囲の AP 情報を既知 AP，未知 AP に分け，既知 AP と未知 AP の受信信号強度を抽出
(3) 4.2.3 節の方法により未知 AP の位置を推定する

4.2.1 観測者の位置情報の取得

本システムでは観測者は任意の地点で周辺の AP の情報収集を行い，未知 AP の位置を推定する．その際，観測者がどの地点で情報を収集したかという情報が必要になる．これに対しては、GPS ユニットからの測位情報を使用する．また，組織内であれば別途地図を用いた位置情報の決定方法も利用できると想定している．

4.2.2 MAC アドレスによる既知 AP，未知 AP の判別機能

本システムでは AP の情報を収集した際，既知 AP と未知 AP を判別して情報を格納する必要がある．PC 内に既知 AP の MAC アドレスと設置座標のデータをあらかじめ保管しておく．search プログラム起動時にそのデータを読み込む．

観測した AP の MAC アドレスが，

データに記録された MAC アドレスと一致する場合
　観測した AP は既知 AP である
データに記録された MAC アドレスと一致しない場合
　観測した AP は未知 AP である

と判別する．

4.2.3 未知 AP の位置推定方法

既知 AP が複数ある場合，収集した既知 AP と未知 AP の受信信号強度を比較して，

・未知 AP ＜観測した全既知 AP の時
　観測者と最強信号強度の既知 AP を半径とした円の内側

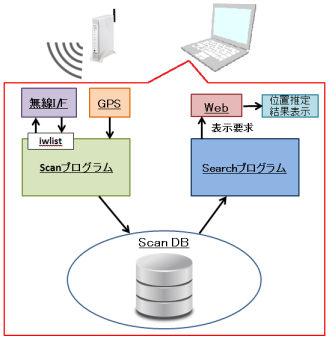

図 1　位置推定システム構成図

```
Cell 07 - Address: 08:1F:F3:XX:XX:XX↓
          Channel:6↓
          Frequency:2.437 GHz (Channel 6)↓
          Quality=36/70  Signal level=-74 dBm  ↓
          Encryption key:on↓
          ESSID:"KITnet"↓
          Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s↓
                    11 Mb/s; 12 Mb/s; 18 Mb/s↓
          Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s↓
          Mode:Master↓
```

図 2　iwlist scan 例

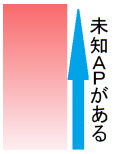

図 3　未知 AP がある可能性の高さの色

・既知 AP(A) 信号強度＜未知 AP 信号強度
かつ 未知 AP 信号強度＜既知 AP(B) 信号強度 の時
観測者と既知 AP(A) 間を半径とする円 A と，観測者と既知 AP(B) 間を半径とする円 B の中間と推測
・未知 AP 信号強度＜受信した全既知 AP 信号強度
または 未知 AP が観測不可能 の時
観測者と最弱信号強度の既知 AP 間を半径とした円の外側と推測

という判定を全てのファイルに対して行い，複数の結果を重ねあわせることで位置推定に用いる分布図を作成する．

5. 未知 AP の位置推定手順

本章では位置推定の流れについて述べる．未知 AP を位置推定する際には以下の操作を順番に行う

手順 1　：事前に決めた観測位置に移動
手順 2　：scan プログラムにより周囲の AP の情報一覧を取得
手順 3　：MAC アドレスから既知 AP，未知 AP に分別し，ファイルに保存
手順 4　：search プログラムにより未知 AP があると考えられる分布図の更新
手順 5　：次の観測位置に移動し，2-4 を行う

全ての観測箇所での操作が終了した時点で位置推定完了とする．

図 4　実験毎の未知 AP の位置

図 5　既知 AP と 38 箇所の観測箇所

6. 評価実験

本章では実装したシステムを用いて，大学内で未知 AP の位置推定を行う．scan プログラムを行う箇所，つまり観測箇所数や未知 AP の位置を変化させることによって位置推定の精度を評価する．なお，今回は方式を評価するため，観測者の位置情報は別途地図を用いて事前に計測しておくこととする．

6.1 実験環境

作成したシステムを評価するために 3 つの実験を行った．実験毎の未知 AP の位置は図 4 であり，それぞれの実験で観測箇所数を”16 箇所”，”38 箇所”，”38 箇所中 4 箇所”と変化させて位置推定を行う．”38 箇所中 4 箇所”では 38 箇所で AP を観測した後，4 箇所のみのデータを位置推定に用いる．選択する 4 箇所は未知 AP の信号強度が強かった観測箇所の上位 4 箇所とする．位置推定に用いた既知 AP や観測箇所の位置は図 5 で，観測者の位置情報にはまたこれ以降の位置推定結果の図では，図 3 のように白から濃い赤にかけて 100 段階のグラデーションで未知 AP がある可能性を示しており，赤色が強くなるほど未知 AP がある可能性が高いと考える．

実験に用いた機器は次の通りである．

表 1　実験に用いた機器

	機器名
ノート PC	Aspire V5 V5-131-N14D
無線 LAN	broadcom 802.11n network adapter
実験 1 の未知 AP	BUFFALO 製 WZR-AMPG300NH/P
実験 2 の未知 AP	Cisco 製 Aironet 1130AG
実験 3 の未知 AP	Cisco 製 Aironet 1130AG
既知 AP	Cisco 製 Aironet 1130AG Cisco 製 Aironet 1142N Cisco 製 Aironet 2602I

推定時の設定としては，緯度経度の 0．000001 度四方を

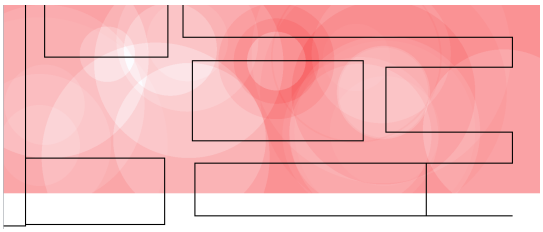

図 6　実験 1 16 箇所

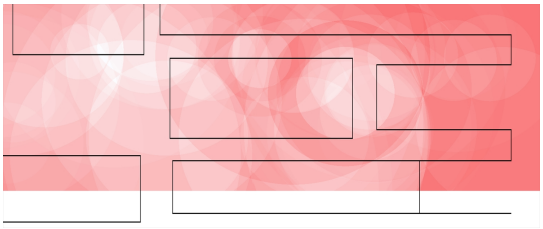

図 7　実験 1 38 箇所

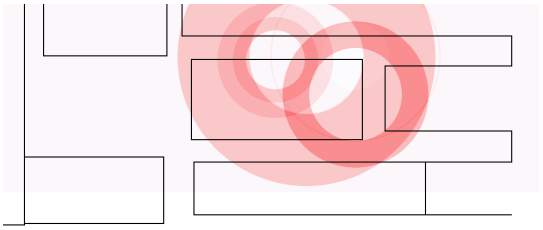

図 8　実験 1 38 箇所中 4 箇所

未知 AP の候補位置の最小単位とした．

6.2　実験結果

位置推定精度を評価するために 3 つの実験を行った．実験 1 の結果はそれぞれ図 6，図 7，図 8．実験 2 の結果はそれぞれ図 9，図 10，図 11．実験 3 の結果はそれぞれ図 12，図 13，図 14 である．

6.3　評価

得られた実験結果を位置推定精度の観点から評価する．図 6，9，12 と図 7，10，13 を比較すると，観測箇所の増加による推定精度の変化は小さいことが分かる．また図 7，10，13 と図 8，11，14 を比較すると，位置推定に用いるデータの厳選によって推定精度の向上が見られた．これらの結果から，位置推定精度の向上には観測箇所数の増加ではなく推定に用いる観測データの検討が必要であると考えられた．最も精度が高かった 38 箇所中 4 箇所を位置推定に用いた結果である図 8，11，14 では未知 AP があると考えられる候補の範囲は約半径 15m の円内であった．候補範囲を部屋単位以下にするには，更なる精度の向上が必要である．

7.　まとめ

本論文では既知 AP の位置情報と受信信号品質，またから取得した位置情報を用いて未知 AP の位置推定を行うシステムの提案と評価を行った．6.3 節の比較，評価では 38

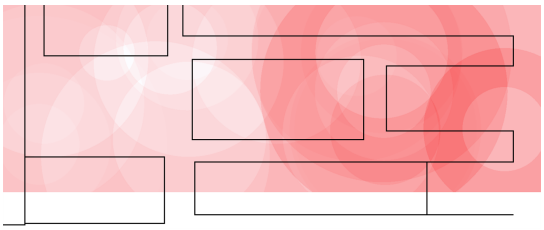

図 9　実験 2 16 箇所

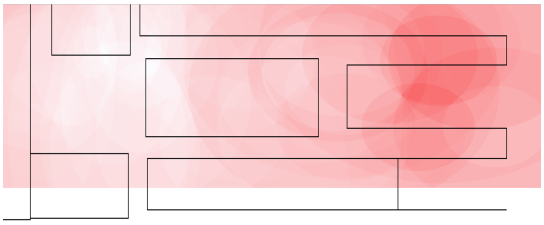

図 10　実験 2 38 箇所

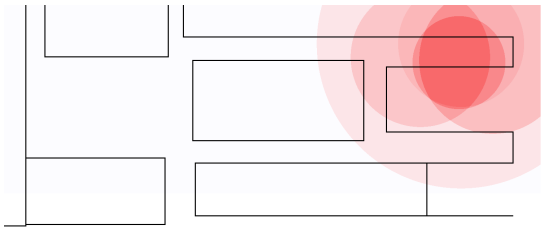

図 11　実験 2 38 箇所中 4 箇所

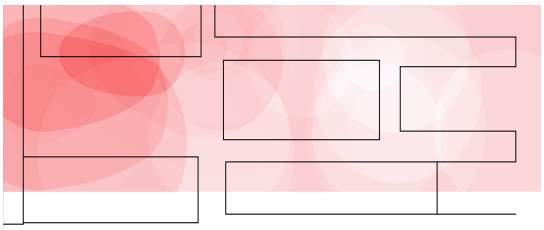

図 12　実験 3 16 箇所

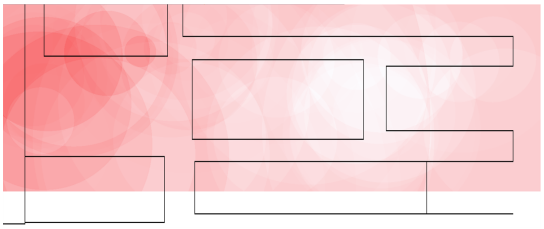

図 13　実験 3 38 箇所

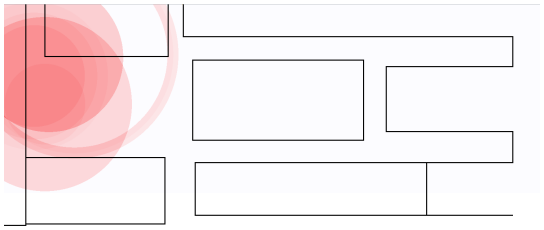

図 14　実験 3 38 箇所中 4 箇所

箇所の観測データを全てを推定に用いたものより 4 箇所のみを用いた結果の方が精度が良かった．今後は位置推定に使う観測データの選別を検討し，位置推定精度をより向上させる．またこのシステムは観測者の位置を自動で取得しリアルタイムに位置推定を行うことを目指している．タブレット端末などを持って，未知 AP が近いと考えられる方向に移動しながら同時に位置推定を行うためにも iOS や Android 上で動作するシステムを目指す．

謝辞

本研究の一部は，JSPS 科研費 26330104 の助成を受けたものである．

参考文献

[1] : AirPatrol, http://www.cirond.com/.
[2] Litner, H., Keeler, B. and Serotte, L.: AirDefense Discovers New Version of 'Evil Twin' At-tack at Interop 2005, http://www.airdefense.net/newsandpress/01_24_05.shtm (2005).
[3] 明生安田：GPS 技術の展望 (GPS 論文小特集)，電子情報通信学会論文誌. B, 通信，Vol. 84, No. 12, pp. 2082–2091 (2001).
[4] 鈴木啓之，伊藤誠悟，河口信夫：Particle Filter を用いた複数無線 LAN 基地局の位置推定手法 (セッション 1:位置検出)，情報処理学会研究報告. MBL, [モバイルコンピューティングとユビキタス通信研究会研究報告]，pp. 15–22 (2006).
[5] 暦本純一，塩野崎敦，末吉隆彦：PlaceEngine–実世界集合知に基づく WiFi 位置情報基盤，インタ-ネットコンファレンス論文集，pp. 95–104 (2006).