3W-04

# Wi-Fi の受信信号強度を用いた位置推定によるデバイス認証方式に関する一検討

堀　孝浩† 朴　美娘† 岡崎　直宣‡
神奈川工科大学† 宮崎大学‡

## １．はじめに

近年，モバイル端末の普及と IoT(Internet of Things)機器の増加にともない，これらのデバイスを用いた近接情報に基づくサービスが注目されている．例えば，周辺交通情報，天気予報などのニュース通知，クーポン券の配布などがこれにあたる．これらのサービスを安全に提供するためには，デバイス認証が必要不可欠である．近接情報に基づくデバイス認証では，環境音や RFID センサなどが多く用いられる．しかしこれらの技術は，誤検知が多く，検出範囲も局所的である．一方，最近では，受信信号強度(RSS:Received Signal Strength)を用いた近接情報に基づく認証が注目を浴びている．図１に受信信号強度を用いた近接情報に基づく認証の例を示す．Alice と Bob は，同じ部屋でお互いに近接しているため，周辺の AP(Access Point)から受信した受信信号強度($RSS_A$, $RSS_B$, $RSS_C$)は，ほぼ等しくなる．しかし，Imposter デバイスは，部屋の外にいるため，壁と距離などにより電波は減衰され，取得できる受信信号強度は$RSS_A$のみである．このように，受信信号強度は，送受信器間の距離や電波伝搬環境により強度が変化する特徴があるため，第３者によるなりすましが難しいという特徴がある．

本研究は，認証を行いたいユーザと悪意のあるユーザがいると仮定し，悪意のあるユーザが認証するユーザの近接にいる場合にも高精度で認証可能にするための近接検出手法の検討を行う．

## ２．関連研究

Amigo[1]では，受信信号強度を用いた物理的な近接情報に基づく２つのデバイス間の認証・検証方式を提案している．無線デバイスのペアリングでは，Man-In-The-Middle(MITM)攻撃のような第３者によるペアリングデバイスの情報の漏れが問題である．既存の Bluetooth や Wi-Fi などの無線デバイス間のペアリングでは，ネットワークアドレスやデバイス名を用いてお互いに認証している．

しかしこのような情報は，固定的な情報であり，第３者がこの情報を知ってしまうと，実際に近接していなくても遠隔で認証できる可能性がある．そこで，この手法では，既存の Diffie-Hellman(DH)鍵交換方式に加え，２つのデバイスが共有する受信信号強度の特徴を用いてデバイス間認証を提案している．

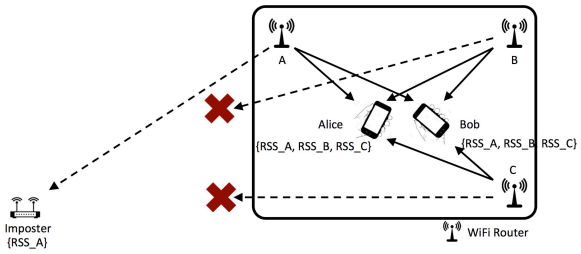


**図１．受信信号強度を用いた近接情報に基づく認証の例**

さらに本研究では，実験により，第３者の位置が認証を行う２つのデバイスと３m 以上離れていれば，その攻撃が検出でき，安全に認証ができることを確認している．もし，攻撃者が１m 程度で近距離にいる場合は，デバイス機器の周辺で手を振るなどの動作をすることで攻撃者のデバイスの受信信号強度と差別できるが，利便性が低くなる問題が考えられる．

## ３．予備実験

３つの PC(A,B,C)と AirPcap NX と Wireshark を用いて RSS の変化を測定する予備実験を研究室で行う．なお，悪意のあるユーザを C としている．実験のシナリオを下記に示す．

- A と B を研究室内に固定する
- C は A と B 付近から歩いての研究室のドアの前で静止する．
- C は研究室を出て廊下を２０～３０m 歩く．
- ラウンジに到着したら静止する．
- 測定を開始した位置に戻る．

実験結果を図２に示す．近接にある２つの PC の RSS パターンと，動いたり，遠い場所で静止したりした C の RSS のパターンは大きく違うことが分かった．また，A と B，B と C の RSS の差を比較したものを図３に示す．A と B の差は，ほぼ０に近いが，B と C の差は最大で 40dB まで違うことが分かった．さらに，３つの PC が同じ部屋にいる場合についても実験を行った．３台の PC が同じ部屋で静止しているため，RSS の差が見れないことが図４より分か

A Study on Device Authentication Method by Location Estimation Using Received Signal Strength of Wi-Fi
† Takahiro Hori, Mirang Park
Kanagawa Institute of Technology
‡Naonobu Okazaki
University of Miyazaki

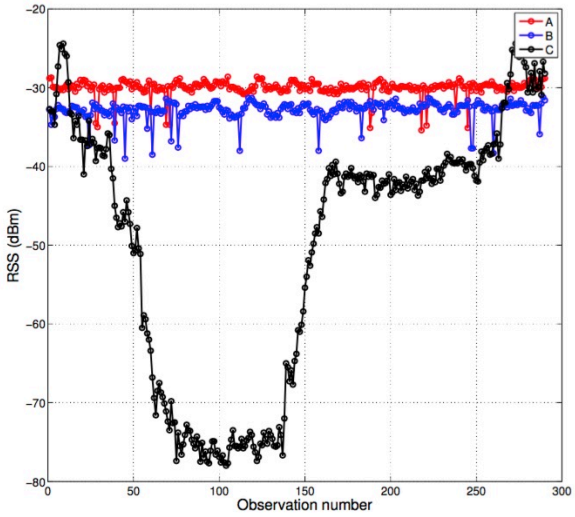


図２．A,B,C それぞれの RSS

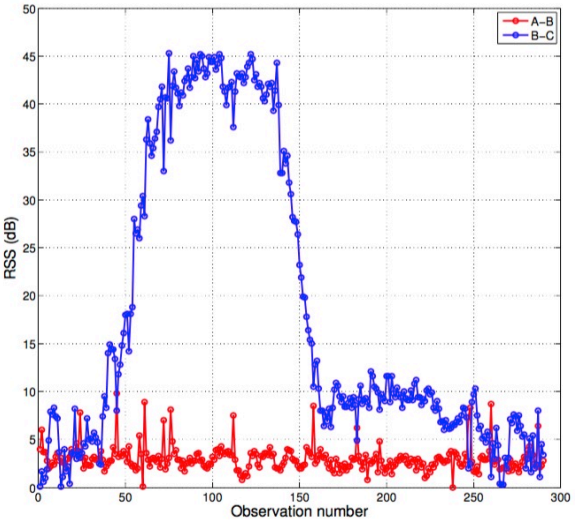


図３．A と B，B と C の RSS の差

った．

## ４．提案手法

本提案手法で想定しているケースは２つある．１つ目は，従来の受信信号強度を用いた認証手法[1]と同じように，認証を行うユーザはお互いに近接にある必要がある場合，２つ目は，悪意のあるユーザが認証をするユーザの近接にある場合である．２つ目の場合，誤認証率が高くなる問題がある．なお，認証範囲が狭く，悪意のあるユーザの位置による認証率の劣化の課題がある．

そこで本研究では，より広範囲で，悪意のあるユーザが認証するユーザと近接にある場合にも高い認証率を持つ手法を提案する．下記に提案手法の手順を示す．

① 認証を行うユーザは，周辺にある AP から beacon frame を受信し，受信信号強度を一定的な間隔で取得する．

② 事前に設定した時間に到達したら，取得した受信信号強度から特徴量(時間統計量)を抽出し， Proximity test を行う．

③ Proximity test で認証に成功したら，次の時刻に Sliding しながら繰り返し Proximity test を行う．

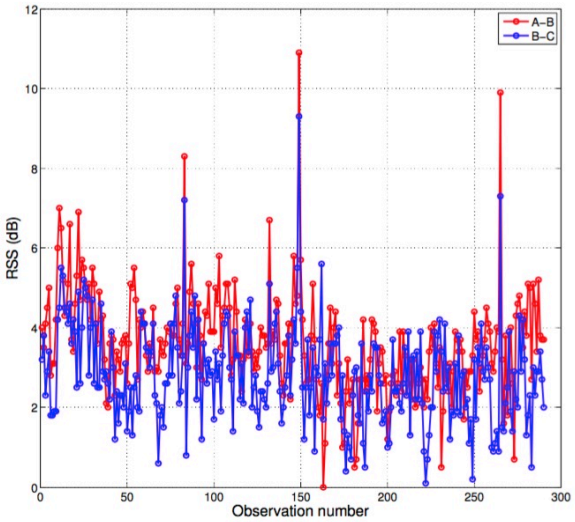


図４．同じ部屋にある場合の A と B，B と C の RSS の差

また，A と B は周辺の AP から RSS を取得すると同時に，お互いの RSS を取得する．A と B の送受出力が同じであれば，お互いの RSS の差はほぼ 0 に近くなる．もし，C が A の近接している場合，A と B の RSS の差と，A と C の差は 0 より大きくなる．これらのことを認証時に利用することにより，高精度の認証率が実現できると考えられる．

## ５．まとめ

本提案手法は，受信信号強度のパターンを比較すると同時に，認証を行うユーザ間の受信信号強度を確認することにより，悪意のあるユーザが近接である場合でもより高い認証率で認証できると考えられる．今後の課題として，どのくらいの間隔で受信信号強度から時間統計量を抽出するのか，RSS は雑音を含むため，雑音除去処理方法も検討する必要がある．また，Proximity test 時の閾値の検討，特徴量の検討も行う必要がある．

## 参考文献

[1] Varshavsky, Alex, et al. “Amigo:Proximity-based authentication of mobile devices.” International Conference on EddyUbiquitous Computing. Springer Berlin Heidelberg, 2007, pp. 253-270.