受信信号強度を用いたデバイス認証における異常値除去手法に関する検討

堀 孝浩[1] 朴 美娘[2] 岡崎 直宣[3]

概要：無線デバイスにおける近接検出技術には，環境音や RFID センサを用いたものがある．しかし，近接検出可能な範囲が局所的なことや，なりすましが容易なことが問題である．そこで近年では，受信信号強度 (RSS) を用いた近接情報に基づくデバイス認証方式が注目されている．RSS は，数百 m の範囲で受信が可能なため，認証範囲が広くなることが期待されている．しかし，電波受信環境により RSS が連続的に異常値になることも考えられ，この異常値を除去せず近接検出を行った場合，近接検出の精度が低下することが考えられる．本論文では，10m 四方程度の会議室で認証したいデバイスが，室内・室外のどちらにあるのかを，デバイスの RSS 情報と，部屋に設置したサーバが受信する RSS 情報のコサイン類似度を比較し，近接検出することを想定する．RSS の異常値除去手法として，スミルノフの棄却検定を利用する手法を提案し，その有効性を実験で確認した．実験の結果，2.4GH z 帯において，棄却検定を行い異常値除去した場合のコサイン類似度が 0.99 となり，異常値除去を行わない場合より，コサイン類似度が 0.05 向上した．これにより，同じ部屋にいるにも関わらず，室外にいると判定される可能性が低くなり，近接検出の精度が向上すると考えられる．しかし，5GHz 帯においては，有意な結果は得られなかった．

A study on Noise Removal Method in Device Authentication using RSS

TAKAHIRO HORI[1] MIRANG PARK[2] NAONOBU OKAZAKI[3]

1. はじめに

近年，IoT (Internet of Things) 機器の増加に伴い，これらのデバイスを用いた近接情報に基づくデバイス認証やサービスが注目されている [1]．例えば，ユーザとサービス提供者が近くにいるかを判定し，クーポンを配布するなどのサービスを提供するものがあり，これを近接検出と呼ぶ．ここでの近接の定義は，アプリケーションによって数 mm から数 km まで様々である．近接情報には，デバイスの正確な位置情報を用いないため，位置情報の偽造による不正な認証などのセキュリティ上の問題や，位置情報が公開された場合のプライバシー侵害の問題はない．近接情報技術では，環境音 [2], [3] や RFID(Radio Frequency IDentifier)[4] センサが多く用いられている．しかし，これらの技術は誤検知が多く，また，検出範囲も 1-2m と局所的である．また，一般的な IoT 機器には，これらのセンサが含まれていない場合が多く，購入費用の増加や多様なサービスは提供できないといった問題もある．そこで近年では，Bluetooth[5] や Wi-Fi[6], [7], [8], [9], [10] などの受信信号強度 (RSS:Received Signal Strength) を用いた近接検出に基づく認証に注目が集まっている．RSS は，ほとんどのデバイスで取得が可能であり，送受信機器間の距離や電波伝達環境により減衰する特徴がある．また，Wi-Fi は，広範囲で受信することが可能なため，より広範囲で近接検出が可能だと考えられる．

本論文では，これらの技術を，データベースへのアクセス権に応用することを考える．例えば，会議資料などが保存されているデータベースが設置されている会議室があるとする．この部屋にはアクセスポイント（AP）があり，その AP に接続されていると，データベースにアクセスできるとする．会議室等に設置されている AP は，不特定多数

1 神奈川工科大学 大学院
Kanagawa Institute of Technology Graduate School
2 神奈川工科大学
Kanagawa Institute of Technology
3 宮崎大学
Univercity of Miyazaki

Copyright (c) 2017 by the Information Processing Society of Japan

の人が接続することが想定され，一度接続をすると，電波の範囲内に入ると自動的に接続されるのが一般的である．この状態だと，AP のある部屋の室内にいなくても，室外からデータベースにアクセスできる可能性は十分に考えられる．これを悪用し，攻撃者は，部屋の外部でから AP にアクセスをし，データベースに接続し，会議資料等を盗むことが可能だと考えられる．AP の設定で MAC アドレスなどでフィルタリングを行うことは可能だが，AP 利用者が変わる度に手動で設定しなければならず利便性が低い．これらを防ぐために，AP から発信されている beacon frame の RSS 情報を利用し近接検出を行い，AP のある部屋の室内，室外を識別し，室外判定された場合は，アクセス拒否をする，ということを本論文では考える．

縣ら [10] は，部屋レベルの Proximity 検出において，2.4GHz 帯と 5GHz 帯の両方の信号を用いて，高精度な部屋レベルの Proximity 検出を実現する手法を提案している．実験の結果，識別正答率は，88%を達成し，高精度で近接検出が行えている．RSS は，電波伝達環境などにより，突然ノイズ（異常値）が発生することが考えられる．縣らの研究では，この異常値を，平均 RSS を算出することで，近接検出に与える影響を低減している．しかし，異常値が連続的に発生した場合，RSS の平均を算出するだけでは，精度が低下してしまうことが考えられる．

筆者らは，RSS を利用した近接検出において，RSS に異常値が発生した場合の異常値除去手法として，データ全体の平均値と標準偏差を元に統計学的に異常値を棄却する，スミルノフの棄却検定が有効だと考えた．本論文では，異常値除去手法として，スミルノフの棄却検定を利用する事を提案し，実験を行いその有効性について確認する．本論文が想定するシステムは，10m 四方程度の会議室において，認証を行いたいデバイスが会議室の室内・室外のどちらにあるのかを，Wi-Fi の RSS を利用し，近接検出するシステムを想定する．また，使用する AP は，室内の 1 か所とし，近接検出は，コサイン類似度を利用する．実験では，スミルノフの棄却検定においての有意水準を 0.05 に設定し，異常値除去を行い，異常値除去を行う場合と，行わない場合の近接検出のコサイン類似度を比較し，提案手法の有効性について確認する．

以下 2 章では，関連研究を紹介し，3 章では提案手法について説明する．4 章で実験について示し，5 章でまとめを行う．

2. 関連研究

2.1 環境音を利用した近接検出

環境音を利用した近接検出 [2], [3] では，環境音の周波数スペクトルの類似度などを用いている．これらの手法は，RFID[4] や Bluetooth[5] などを利用した手法に比べ，近接検出範囲が広いのが特徴である．また，Schurmann ら [2] の方式では，精度が 90%に近く，高精度な近接検出も実現している．しかし，環境音は，異なる場所でも類似してしまう可能性があり，誤検知することが考えられる．

2.2 RSS 強度を利用した認証

一般的に，無線通信における RSS と，送信機と受信機間の物理的な距離は比例するため，RSS をデバイスの認証情報として用いることができる．一般に，電波の減衰は次のようなフリスの伝達公式にて表現される．

$$\frac{P_{tr}}{T_t} = G_t G_r (\frac{\lambda}{4\pi D_{tr}})^2 \quad (1)$$

ここで t は送信機，r は受信機を示し，P_{tr} は，r が t より受け取った電力 [W]，T_t は，t より送られてきた電力，G_t，G_r は，t, r のゲイン，D_{tr} は，tr 間の距離である．藤井ら [6] は，上記の式を使い，2 つの受信機の RSS の比を

$$R = (\frac{D_{t2}}{D_{t1}})^2 \quad (2)$$

と定式化している．これは，RSS によって送信機が存在する空間を定めることができることを意味する．ただし，得られる情報は，2 つの受信機から送信機までの距離の比のみであり，受信側は送信機の正確な位置を特定できるわけではない．しかしながら，空間が限定できれば，ある信号を受信したとき，送信機の位置が限定された空間に存在するかどうかを調べることで，認証が可能になる．

2.3 Wi-Fi の RSS を利用した近接検出

Wi-Fi の RSS を利用した近接検出では，RSS の類似度やユーザ間の RSS のユークリッド距離などを用いて近接検出を行うものが一般的である [7], [8], [9], [10]．

Amigo[7] では，受信信号強度を用いた近接情報に基づくデバイス間の認証・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，MITM (Man-In-The-Middle) 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など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 者にこの情報が知られた場合，なりすましで認証されてしまう可能性がある．そこで，この手法では，既存の DH (Diffie-Hellman) 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，デバイス間認証を行う方式を提案している．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．しかし，これは，認証を行う 2 つのデバイスが近接 (5cm) と非常に近い場合である．2 つのデバイスが近接 (1m) の場合も，認証を行うことは可能だが，安全な認証を行うには，長い時間 (20 秒) 測定をする必要がある．

縣ら [10] は，部屋レベルの Proximity 検出において，

Copyright (c) 2017 by the Information Processing Society of Japan

2.4GHz 帯と 5GHz 帯の両方の信号を用いて，高精度な部屋レベルの Proximity 検出を実現する手法を提案している．Wi-Fi の beacon frame を受信し，RSS の類似度を表 2 つの特徴量を 2.4GHz 帯と 5GHz 帯の両方で抽出している．5GHz 帯は，壁などの伝達環境による減衰に 2.4GHz 帯と差があり，これを利用することにより高精度化を実現している．また，電波伝達環境により一時的に発生する RSS の変化に対応するために，特徴量に RSS の平均を利用している．実験により，2 つのデバイスが同じ部屋にいるかどうかを識別し，想定したすべてのケースにおいて 88 %の識別正答率を達成した．これにより，従来法 [9] と比べ環境への影響に強くなり，10-15m の部屋レベルでの Proximity 検出を高精度で実現した．

Wi-Fi を利用した近接検出に関する研究は盛んに行われているが，電波伝達環境などにより，RSS が異常値になった場合の異常値除去に関する研究は少ない．筆者らは，この異常値を，スミルノフ棄却検定を行い除去することにより高精度に近接検出が可能だと考える．

2.4 スミルノフ棄却検定

スミルノフ棄却検定とは，データ中に他のデータとかけ離れている異常値がある場合，それを棄却するべきかどうかを全体の平均値と標準偏差を元に統計的に検定する手法である [11]．スミルノフ棄却検定の手順は，まず，帰無仮説と対立仮説を立てる．帰無仮説では，他のデータとかけ離れた値は異常値ではないと仮説を立てる．対立仮説では，他のデータとかけ離れた値は異常値であると仮説を立てる．次に，有意水準 α を決め，データ数 n 個のときの有意点 k を得る．なお，一般的に，有意水準 α は，0.05，0.1 で設定することが多い．有意点 k は，自由度 $n-2$ の t 分布の α /n × 100 パーセンタイルを t として，下記の式で計算できる．

$$k = \frac{(n-1)^t}{\sqrt{n(n-2)+nt^2}} \tag{3}$$

検定統計量を T，標本分散を S^2，標本平均を $\overline{x}$，検定したい値を x_i とした時，検定統計量 T を下記の式で計算する．

$$T = \frac{|x_i - \overline{x}|}{S} \tag{4}$$

なお，S は標準偏差である．そして，$T > k$ のとき，検定した値 x は異常値とみなし，棄却する．

3. 提案手法

本論文では，RSS を利用した，近接検出における RSS の異常値除去手法として，スミルノフ棄却検定を利用する手法を提案する．本提案手法では，10m 四方程度の会議室にある Wi-Fi のアクセスポイント (AP) から発信される beacon frame の RSS を利用し，認証を行いたいデバイスが室内・室外にあるかを近接検出し，デバイス認証を行う場面を想定する．

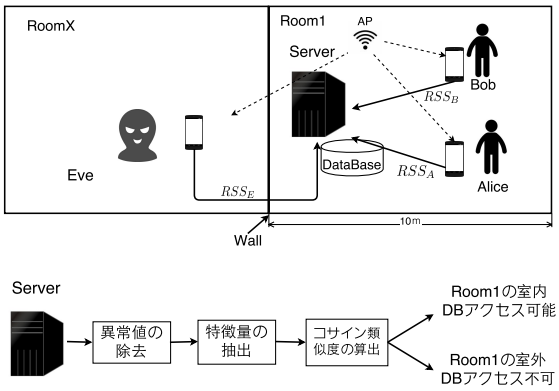

図 1 システムモデル

3.1 システムモデル

図 1 に，認証するデバイス（ユーザ）を Alice と Bob，攻撃者を Eve とした，本論文におけるシステムモデルを示す．本論文のシステムは，会議資料などが保存されているサーバが設置されている 10m 四方程度の会議室があるとする．この部屋にはアクセスポイント（AP）とサーバとデータベースがあり，その AP に接続されていると，データベースにアクセスできるとする．フィルタリング等の設定を行わない場合，この状態では，AP のある部屋の室内にいなくても，室外からデータベースにアクセスされる可能性は十分に考えられる．これを悪用し，攻撃者は，部屋の外部でから AP にアクセスし，データベースから会議資料等を盗むことが可能だと考えられる．これを防ぐために，AP から発信されている beacon frame の RSS 情報を利用し近接検出を行い，そのデバイスが，AP のある部屋の室内，室外にあるかを識別し，室外と判定された場合は，アクセス拒否をする．システムモデルの構築手順を以下に示す．

(1) Alice と Bob が持つデバイスは，部屋にある 1 つの AP から送信されている beacon frame を受信する．
(2) Alice と Bob が持つデバイスは，受信した beacon frame の RSS 情報をサーバに送信する．
(3) サーバで受信した RSS 情報から異常値を検出し，異常値除去を行う．異常値除去は，スミルノフの棄却検定を利用する．
(4) RSS 情報から特徴量の抽出を行う．
(5) (4) で得た，認証を行いたいデバイスの特徴量と，サーバの特徴量のコサイン類似度を算出し，算出された結果に応じて，デバイスの位置を室内・室外かに識別する．

3.2 異常値除去アルゴリズム

図 2 に異常値除去の提案アルゴリズムを示す．

Copyright (c) 2017 by the Information Processing Society of Japan

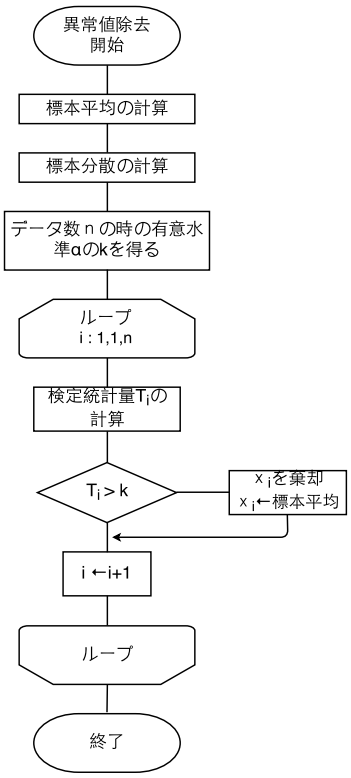

図 2 異常値除去アルゴリズム

【Step1】

RSS 情報の標本平均を計算する．RSS 情報の標本平均 $\overline{x}$ は，下記の式で計算される．

$$\overline{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{5}$$

n は,RSS 値の個数，i 番目の RSS 値を x_i とする．

【Step2】

RSS 情報の標本分散を求める．標本分散を S^2 とすると下記の式で計算される．

$$S^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \overline{x})^2 \tag{6}$$

【Step3】

式 (3) により，有意点 k を計算する．

【Step4】

式 (4) により，検定統計量 T を求める．$T_i > k$ となった場合，その値を異常値として棄却し，標本平均 $\overline{x}$ を代入する．$T_i < k$ と場合は，そのままにする．全ての RSS 値の検定が終了したらスミルノフの棄却検定が終了し異常値除去が完了する．

3.3 特徴量の定義とコサイン類似度の算出

本論文では，認証するデバイスが，AP のある部屋の室内・室外にあるかを近接検出するために，下記で定義する特徴量のコサイン類似度を用いる．

- RSS の平均値
- RSS の標準偏差
- RSS の最大値
- RSS の最小値
- RSS の中央値

これらを採用した理由は，平均値や標準偏差は，壁などによる減衰の影響を受け，ばらつきが発生しやすいと考えたためである．また，最大値，最小値，中央値は，AP までの距離による影響を大きく受けると考えたためである．

コサイン類似度とは，ベクトル空間モデルにおいて文書同士の類似度を比較する際に用いられる類似度計算手法である．コサイン類似度は，0 から 1 の範囲で類似度が表され，1 に近ければ類似しており，0 に近ければ類似していないことになる．2 つのベクトル $\vec{a}$ と $\vec{b}$ の類似度は下記の式で計算できる．

$$cos(\vec{a},\vec{b}) = \frac{\sum_{i=0}^{|V|} a_i b_i}{\sqrt{\sum_{i=1}^{|V|} a_i^2} \cdot \sqrt{\sum_{i=1}^{|V|} b_i^2}} \tag{7}$$

認証を行いたいデバイスとサーバが，同じ室内にいる場合，室内での場所や広さにより多少の減衰はあるが，基本的には，同等の RSS 情報を測定することが可能である．つまり，認証を行いたいデバイスとサーバの RSS 情報は類似したものになると考えられる．本論文の近接検出では，これらを利用し，認証を行いたいデバイスとサーバの RSS 情報のコサイン類似度を算出し，近接検出を行う．

表 1 実験諸元

アクセスポイント	WSR-2533DHP-CB
Beacon Frame を受信する時間	20 秒
棄却検定時の有意水準 α	0.05
使用する周波数帯	2.4GHz , 5GHz

4. 実験評価

提案アルゴリズムの効果を確認するために実験を行う．異常値除去を行う場合と行わない場合でのコサイン類似度を比較し，その有効性について確認する．

4.1 実験諸元

図 3 に実験を行った部屋の環境を示す．ここで，認証を行いたい部屋を Room1，攻撃者が攻撃をする部屋を Room2，廊下とし，認証するデバイス，攻撃者は動かないものとする．Room1 は，12 階建てのビルの 2 階にあり，周辺には，10 個前後の AP が存在する．また，部屋と部屋の間にあるコンクリート製の壁は約 28cm，ドアはガラス製で厚さは約 5cm である．

実験で使用する機器や，使用する識別器に関しては表 1 に示す．RSS を測定するにあたり，AirPcap NX[12] と Wireshark[13] がインストールされているノート PC を用

Copyright (c) 2017 by the Information Processing Society of Japan

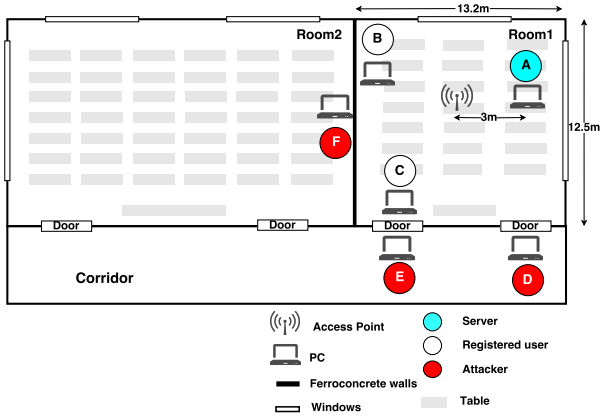

図 3　実験環境

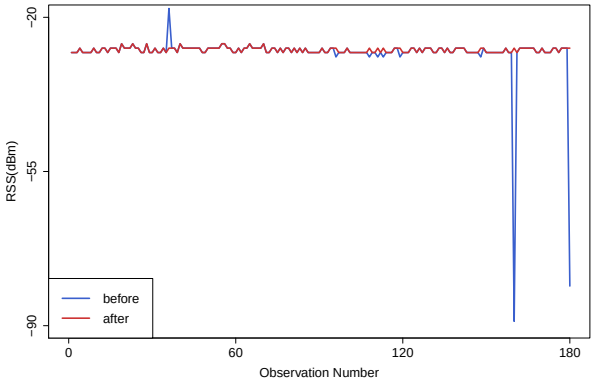

図 4　2.4GHz 帯においての検定結果

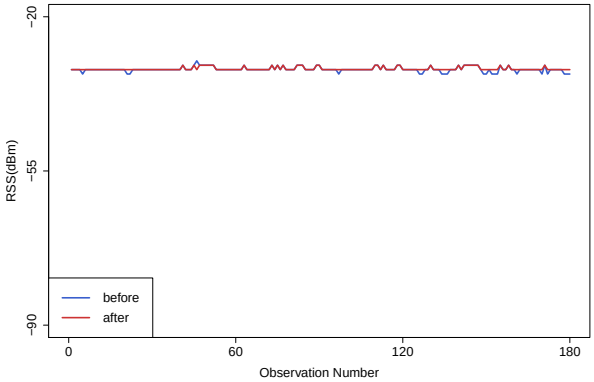

図 5　5GHz 帯においての検定結果

意した．RSS の測定は，認証を行いたい部屋と，攻撃者が攻撃を行う場所の合計 6 か所で，人の出入りがないときに行った．今回は，図 3 にある A から F の場所で行った．なお，サーバの設置位置は A とした．

4.2　異常値除去

異常値除去は，3.2 節で提案した手法を適応する．スミルノフ棄却検定の有意水準 α は，一般的な 0.05 で行う．図 4 は，2.4GHz 帯においてスミルノフ棄却検定を行う前の RSS 情報と棄却検定を行ったときのグラフである．水色の線を見ると，RSS は，周辺環境などにより，突発的に非常に弱い RSS が発生している．デバイスは静止状態にあり，RSS が突発的に急激に変化するとは考えにくいため，これは，異常値だと考えられる．これを除去せず，近接検出を行った場合，このデバイスは，AP から離れた場所にあると近接検出され，正確に近接検出ができないことが考えられる．橙色の線は，スミルノフ棄却検定を行い，異常値除去を行った結果である．スミルノフ棄却検定を行うことで，突発的に発生する RSS の異常値を除去できていることがわかる．図 5 は，5GHz 帯においてスミルノフ棄却検定を行う前の RSS 情報と行ったときのグラフである．水色の線が異常値除去を行う前の RSS である．5GHz 帯では，大幅な RSS の変化がないことがわかる．橙色の線が異常値除去後の RSS で，所々で発生している，比較的小さな異常値を除去できていることがわかる．

表 2　各箇所での平均 RSS

	A	B	C	D	E	F
2.4GHz(dBm)	-28.3	-39.1	-32.2	-40.4	-39.4	-37.5
5GHz(dBm)	-31.9	-34.1	-35.9	-42.4	-47.5	-41.9

4.3　各箇所での平均 RSS

表 2 に各箇所での平均 RSS を周波数帯別に示す．AP ポイントから数 m 離れただけでも RSS に変化が表れていることがわかる．地点 B と F は，壁を挟んでほぼ同じ距離にいるが，2.4GHz 帯では地点 F の方が平均 RSS が高くなっている．しかし，5GHz 帯では，大幅な減衰が見られる．地点 C と E はドアを挟んでほぼ同じ距離にいるが，AP がある部屋の外の方が RSS が減衰していることがわかる．特に，5GHz 帯の方が大幅に減衰していることがわかる．このように，周波数帯によって差はあるものの，壁やドアを通すことにより，室内と室外では RSS に差があることがわかる．

4.4　コサイン類似度による近接検出

コサイン類似度は，A とのコサイン類似度を比較し，A と B〜F のそれぞれの場所で算出する．表 3 に，算出されたコサイン類似度を示す．まず，2.4GHz 帯も 5GHz 帯もコサイン類似度が，室内と室外で大きく差が出たことがわかる．これは，壁やガラスなどを挟み，室外の RSS は，室内の RSS と比べ弱くなったからだと考える．次に，棄却検定を行わない場合と行う場合を比較する．棄却検定を行った場合，2.4GHz 帯では，同じ室内あるデバイスとのコサイン類似度が，B の場所において 0.04 向上がったこたが確認できる．これは，棄却検定を行い異常値が除去され，最大値や最小値，中央値が類似するようになったためだと考える．これにより，室内にあるデバイスが，室外と判定され

Copyright (c) 2017 by the Information Processing Society of Japan

表 3　コサイン類似度算出結果

		A と B	A と C	A と D	A と E	A と F
2.4Ghz	棄却検定なし	0.940	0.707	0.575	0.499	0.412
	棄却検定あり	0.999	0.707	0.577	0.500	0.447
5Ghz	棄却検定なし	0.999	0.707	0.577	0.500	0.447
	棄却検定あり	0.999	0.707	0.577	0.500	0.447

る可能性が低くなり，近接検出の精度が向上することが考えられる．しかし，室外のコサイン類似度も，若干向上している．これは，異常値除去をすることにより，標準偏差が類似するようになったためだと考える．コサイン類似度が向上したが，元々のコサイン類似度の差が大きく，コサイン類似度の向上も若干である．そのため，室外にあるデバイスを室内にあると近接検出される可能性は低く，近接検出の精度が低下することは考えにくい．ただし，5GHz 帯では，棄却検定を行うことによる変化は見られなかった．

5. おわりに

本論文では，10m 四方程度の会議室での近接検出を想定し，受信信号強度の異常値除去手法として，スミルノフの棄却検定を用いた手法を提案し，その有効性を実験で確認した．実験の結果，部屋の室内と室外で電波強度の差があることがわかった．異常値除去の効果は，異常値除去した場合のコサイン類似度が 0.99 となり，異常値除去を行わない場合より，コサイン類似度が 0.05 向上した．これにより，同じ部屋にいるにも関わらず，室外にいると判定される可能性が低くなり，近接検出の精度が向上すると考えられる．ただし，5GHz 帯においては，有意な結果は得られなかった．

今後の課題として，まず，人の出入りのある時間での RSS の測定をし，異常値除去を行い，近接検出を行うことが挙げられる．その他に，近接検出に掛かる所要時間の検討や，複数の AP の RSS 情報を利用することによる高精度化などについても検討する必要があると考える．

参考文献

[1] “米国における IoT（モノのインターネット）に関する取り組みの現状,” IPA 情報処理推進機構, ニューヨークだより, 2015.

[2] D. Schurm ann and S. Sigg,“Secure communication based on ambient audio,” IEEE Transactions on Mobile Computing, vol. 12, no.2, pp.358-370, 2013.

[3] N. Karapanos, C. Marforio, and C. Soriente,,“Soundproof : Usable two-factor authentication based on ambient sound,” in Proc. 24th USENIX security symposium, pp. 483-498, 2015.

[4] M. Bolic, M. Rostamian, and P. M. Djuric,“Proximity detection with RFID : A step toward the Internet of Things,” Pervasive Computing, IEEE, vol. 14, no. 2, pp. 70-76, 2015.

[5] S. Liu, Y. Jiang, and A. Striegel,“Face-to-face proximity estimation using bluetooth on smartphones,” IEEE Trans. Mobile Comput, vol. 13, no. 3, pp. 811-823, Apr. 2014.

[6] 藤井 達也, 小野 貴継, 金谷 晴一, 井上 弘士, “受信真奥強度を用いたデバイスに認証方式における攻撃可能条件の定式化,” 信学技報, vol. 116, no. 178, DC2016-19, pp. 15-22, 2016.

[7] A. Varshavsky, A. Scannell, A. LaMarca, and E. de Lara, “Amigo:Proximity-based authentication of mobile devices.” International Conference on EddyUbiquitous Computing. Springer Berlin Heidelberg, 2007, pp.253-270.

[8] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, “Ensemble : Cooperative proximity-based authentication.” in Proc. ACM Int. Conf. Mobile Syst. (Mobisys), Appl. Services, pp. 331-334, 2010.

[9] Y. Agata, J. Hong, and T. Ohtsuki,“Room-Level Proximity Detection Using Beacon Frame From Multiple Access Point ,” in Proc. Asia-Pacific Signal and Infomation Processing Association (APSIPA), pp. 941-945, 2015.

[10] 縣 侑吾, 洪 志勲, 大槻 知明,“複数アクセスポイントからのデュアルバンド信号の受信信号強度に基づく部屋レベルの Proximity 検出,” 信学技報, vol. 115, no. 437, ASN2015-82, pp. 15-20, 2016.

[11] 石村 貞夫 : すぐわかる統計解析, 東京図書株式会社, 東京, 1997.

[12] AirPcap “https://www.riverbed.com/index.html”

[13] Wireshark “https://www.wireshark.org/”

Copyright (c) 2017 by the Information Processing Society of Japan