Entity Authentication Scheme for Wireless Terminal Based on Location Identification Using ESPAR Antenna

Naoki OTANI, Hisato IWAI and Hideichi SASAOKA*

(Received January 9, 2014)

As a measure against spoofing in wireless communications, there is entity authentication of radio terminal based on location identification. In this entity authentication, location identification is performed by a technique similar to location estimation of a radio terminal based on location fingerprint in multipath environment. One of proposed systems of entity authentication based on location identification generates the received signal strength variation related to multipath arrival directions by antenna pattern change. However, the characteristic evaluation under real environment is not fully performed. This paper estimates both basic characteristic in a computer simulation and experiment under real environment for the system using ESPAR antenna. Moreover, this paper shows feasibility of the proposed system under real environment.

key words : information security, entity authentication, ESPAR antenna, location fingerprint

キーワード : 情報セキュリティ，相手認証，エスパアンテナ，位置指紋

エスパアンテナを用いた位置識別に基づく無線端末の相手認証方式

尾谷 尚宣，岩井 誠人，笹岡 秀一

1．まえがき

無線通信は，開かれた空間を通して電波の送受信を行うため，盗聴や不正アクセスなどその脆弱性が問題となっている．ここで，盗聴対策としては，共通鍵暗号方式や公開鍵暗号方式など，計算量的な複雑性を根拠にする暗号技術を使用するのが一般的である．これに対して，電波伝搬特性を用いた秘密鍵共有[1-2]と秘密情報伝送[3]が提案されている．ここで，無線秘密鍵共有は，電波伝搬の可逆性と場所依存性を活用した方式であり，マルチパス環境における電波伝搬特性の複雑性を安全性の根拠にしている．

一方，「なりすまし」による不正アクセスの対策としては，暗号技術を用いた相手認証が一般的であるが，電波伝搬特性を用いた位置識別に基づいて無線端末の相手認証を行う方式が提案されている[4-6]．この方式は，無線端末の位置固定を前提とし，各無線端末を識別するための特徴量を事前に取得しておき，相手認証時に取得した特徴量と比較することで位置識別を行う．この方式の一つに電波の到来時間差に関連する周波数特性を観測する方式がある[4]．また，この方式の別のものに，可変指向性アンテナ

*Department of Electronics, Doshisha University, Kyoto
Telephone: +81-774-65-6355, Fax: +81-774-65-6801, E-mail: hsasaoka@mail.doshisha.ac.jp

の指向性パターンを変化させ，電波到来方向に関係する受信信号強度変動の時系列を特徴量として用いる方式がある[5-6]．これらの方式は，位置推定を目的としないが，電波の位置指紋に基づく位置推定と類似の手法である[7-9]．

これまで，著者達は電波を用いた秘密鍵共有方式の研究を理論やシミュレーションで実施するばかりでなく，実験装置を開発して実験的研究を実施してきた[10-13]．この秘密鍵共有方式は，電波伝搬の可逆性を活用して共有した位置指紋から秘密鍵を生成しているとみなせる．そこで，既に開発済みのアレーアンテナを用いた秘密鍵共有装置を用いて，位置指紋に基づく位置識別およびそれに基づく相手認証がどの程度の性能で実現できるかを実験的に検討してきた[6,14,15]．

本論文では，アレーアンテナでなくエスパアンテナを用いアンテナの指向性パターンを変化させて，電波到来方向に関係したRSSI 変動の時系列を特徴量として相手認証を行う方式を対象とし，計算機シミュレーションと実環境での実験により基本特性の評価を行った．

２．電波伝搬特性に基づく位置識別と相手認証

電波伝搬特性を用いた相手認証方式は単独で相手認証を実施するのではなく，事前に無線端末間（例えば，アクセスポイント (AP: Access point) とユーザ端末 (UT: User Terminal) 間で情報セキュリティ技術等を用いた相手認証が確立していることが前提となる．そして，無線端末の位置が固定されている前提のもと，位置識別による簡易な相手認証に基づき，通常の相手認証を毎回実施することなく，悪意の第三者による「なりすまし」を防止することを目的としている．

2.1 電波伝搬特性に基づく位置識別

本方式は，電波伝搬特性の場所依存性に基づいている．この場所依存性は，電波が広範囲の角度から到来するマルチパス伝搬環境で顕著となり，移動通信環境では信号受信点が数波長程度離れるとフェージング変動がほぼ無相関となることが知られている．この特性は，マルチパス伝搬の特徴量を位置指紋とした位置推定にも用いられている．

位置識別に用いる特徴量としては，マルチパスの到来時間差に関係する周波数特性の標本値[4]，アンテナの指向性パターンの変化による電波到来方向に関係するRSSI 変動の時系列[5]等がある．これらのデータを事前（初期の相手認証時）に取得しておき，次に簡易な相手認証時に取得したデータと事前データ比較することで，同一地点から発射された電波か否かの位置識別を実施する．ここで，周波数特性に基づく位置識別は，室内環境など遅延時間差が小さく観測可能な周波数帯域幅が限定される場合に，十分に多様な特徴量を取得することが難しい．これに対して，アンテナの指向性パターンを変化させて取得した RSSI 変動の時系列（以下，RSSI プロファイルと呼ぶ．）は，マルチパス伝搬環境において電波の到来方向とその振幅・位相に依存した多様性・複雑性に関係しているため，十分に多様な特徴量を取得できる可能性がある．

ここで，マルチパス伝搬環境の多様性・複雑性を最大限に活用した位置識別法，および各種の位置識別法の特徴が，アレーアンテナを用いた場合について検討されている[6]．それによると，RSSI プロファイルを用いる方式は，必ずしも優れた方式ではないが，秘密鍵共有と相手識別を同一装置で実現できるところに特徴がある．

RSSI プロファイルを用いる方式において，受信信号強度は，送信電力の時間変動，受信増幅器利得の時間変動の他に伝送路上の変動要因などの影響をうける．このため，RSSI プロファイルの平均値からの差分を標準偏差で正規化した値を特徴量とする．また，事前データと相手認証時のデータとの比較（類似度の評価）は，相関係数を求めることで行う．当然ながら，相関係数は [1,-1] の範囲にある．

また，RSSI プロファイルを用いた位置識別では，その性能が指向性パターンの設定に依存する．特に，RSSI 系列長が短く指向性パターンの種類が限定されると，使用した指向性パターンの偏りにより，複数電波の到来方向とその振幅・位相などマルチパス伝搬路の多様性・複雑性に関する十分な情報を取得

できない懸念がある[6]．このため，最適な指向性パターンの設定が重要となる．一方，RSSI プロファイルの系列長を適当に長く設定すれば，指向性パターンを実現可能な範囲でランダムに設定しても，指向性パターンの偏りが減少するためマルチパス伝搬路の多様性・複雑性に関する十分な情報が取得できるとも考えられる[6]．しかし，理論的に検討は本論文の範囲を超えるので計算機シミュレーションと実環境下での実験で評価する．

2.2 エスパアンテナを用いた相手認証

Fig .1 にエスパアンテナを用いた位置識別システムの構成を示す．Fig. 1 に示すようにAP には７素子エスパアンテナを，UT にはオムニアンテナを使用している．7素子エスパアンテナは，中央に給電素子が１本，その周囲に無給電素子が６本配置された構造となっている．それぞれの無給電素子に装荷されたリアクタンスの値を変化させることで，アンテナの指向性を多様に制御することができる．リアクタンス値をランダムにすることで，RSSI プロファイルを取得することが可能となる．このシステムの構成と方式諸元は，秘密鍵共有実験のために開発したエスパアンテナを用いた装置[10-11]と同様である．

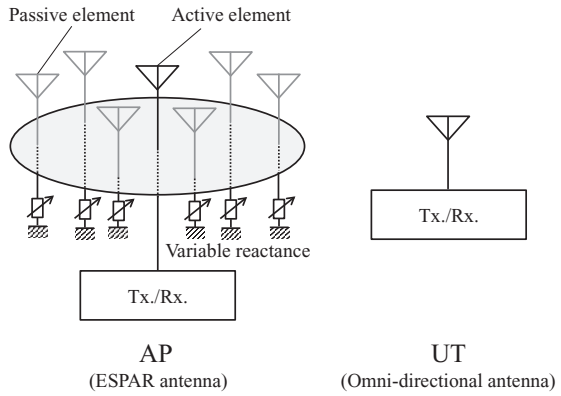


Fig. 1. Location identification system using ESPAR antenna.

位置識別に基づく無線端末の相手認証は，既に述べたように事前に相手認証が確立していることを前提としている．また，無線端末の位置が固定されている前提の下で，位置識別による簡易な相手認証を実施する．相手認証の可否は，相手方の無線端末の位置が同一か否かで判定することになる．

Fig. 2 にエスパアンテナを用いた無線端末の相手認証の手順を示す．Fig. 2 に示すようにフェーズ１では，ステップ１で従来手法による相手認証が確立した直後に，ステップ２でRSSI プロファイルの事前データを取得する．ステップ２では，AP が長さnのアンテナの指向性パターン系列 $\boldsymbol{L}_1$ を生成し，APがUTに対して測定用信号を送信するよう要求する．要求を受けたUTは測定用信号をAP に対してn 回送信する．AP は $\boldsymbol{L}_1$ の各指向性を用いてこの信号を順次受信することで，長さn のRSSI プロファイル $\boldsymbol{p}_1 = (p_{11}, p_{12}, \cdots, p_{1n})$ を生成する．

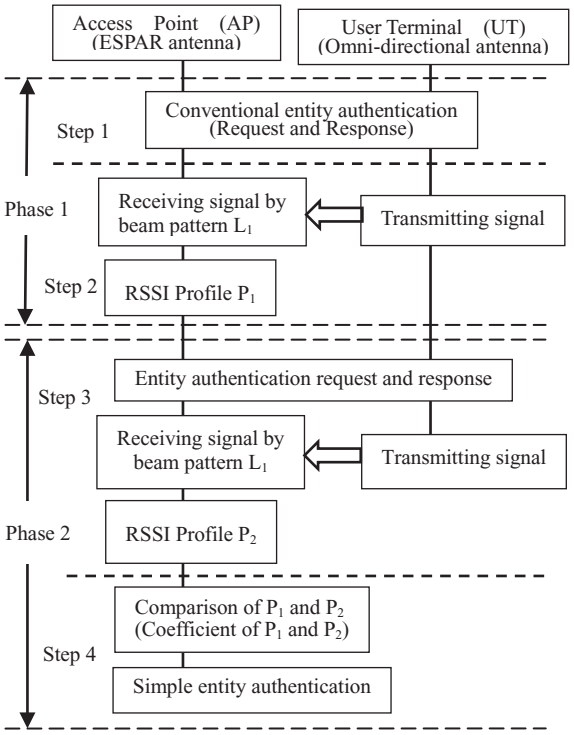


Fig. 2. Procedure of entity authentication using ESPAR antenna.

次に，無線端末の位置が固定されている前提の下で，一定時間が経過後にフェーズ２の簡易な相手認証を行う．フェーズ２のステップ３では，ステップ１で用いたアンテナ指向性パターン系列 $\boldsymbol{L}_1$ と同じパターン系列を用いて同様な処理を行い，RSSI プロファイル $\boldsymbol{p}_2 = (p_{21}, p_{22}, \cdots, p_{2n})$ を生成する．ステ

ップ４では，$\boldsymbol{p}_1$ と$\boldsymbol{p}_2$ の類似度を評価し，それを認証の指標とする．

ここで，受信信号強度データ$\boldsymbol{p}_1$ と$\boldsymbol{p}_2$ そのものは，既に述べたように送信電力の時間変動，受信増幅器利得の時間変動の他に伝送路上の変動要因などの影響をうけるため類似度が減少する．このため，RSSI プロファイルの平均値からの差分を標準偏差で正規化した値をX_1, X_2 を用いる．

$$X_1 = \left(\frac{p_{11}-\bar{p}_1}{\sigma_1},\ \frac{p_{12}-\bar{p}_1}{\sigma_1}, \cdots, \frac{p_{1n}-\bar{p}_1}{\sigma_1}\right),$$

$$\bar{p}_1 = \frac{1}{n}\sum_{i=1}^{n} p_{1i}\ ,\ \sigma_1 = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(p_{1i}-\bar{p}_1)^2} \qquad (1)$$

$$X_2 = \left(\frac{p_{21}-\bar{p}_2}{\sigma_2},\ \frac{p_{22}-\bar{p}_2}{\sigma_2}, \cdots, \frac{p_{2n}-\bar{p}_1}{\sigma_2}\right),$$

$$\bar{p}_2 = \frac{1}{n}\sum_{i=1}^{n} p_{2i}\ ,\ \sigma_2 = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(p_{2i}-\bar{p}_2)^2} \qquad (2)$$

また，類似度はX_1 とX_2 の相関で評価する．X_1 とX_2 の相関は，

$$R_{X_1,X_2} = \frac{1}{n}\sum_{i=1}^{n}\frac{p_{1i}-\bar{p}_1}{\sigma_1} \times \frac{p_{2i}-\bar{p}_2}{\sigma_2} \qquad (3)$$

と表される．なお，式(3)で表される相関は$\boldsymbol{p}_1$ と$\boldsymbol{p}_2$ の相関係数（正規化共分散）C_{p_1,p_2}と同じであり，

$$C_{p_1,p_2} = R_{X_1,X_2} = \frac{\sum_{i=1}^{n}(p_{1i}-\bar{p}_1)(p_{2i}-\bar{p}_2)}{\sqrt{\sum_{i=1}^{n}(p_{1i}-\bar{p}_1)^2}\sqrt{\sum_{i=1}^{n}(p_{2i}-\bar{p}_2)^2}} \qquad (4)$$

を用いて，$\boldsymbol{p}_1$ と$\boldsymbol{p}_2$ から直接に算出できる．この相関係数は，[−1, 1] の範囲の値をとり，類似度が高いと１に近づく．

位置識別に基づく相手認証は，類似度（相関係数）の大小で判定する．あらかじめ設定した閾値より相関係数が大きければ正規のユーザ端末と相手認証を行い，相関係数が小さければ「なりすまし」端末(SP: Spoofing point)と判断する．

３．計算機シミュレーションによる評価

3.1 システムモデル・システム諸元

Fig. 3 にシミュレーションに用いる室内環境と各端末の配置を示す．想定する室内環境はコンクリート材質の壁に囲まれた縦(y)・横(x) が6.2m×8.6m の障害物のない２次元の部屋とする．レートレース法による電波伝搬解析の容易さを考慮して，実際の部屋と異なり，窓，ドア，什器などのない部屋を想定している．各端末の配置（座標(x, y)）は，部屋中央のAP を部屋中央の(0.0m, 0.0m)，UTを(1.5m, 1.0m)に固定する．一方，SP は，任意の場所に存在することを想定して，Fig. 3 に示すように部屋全体を0.05m 間隔で移動させる．

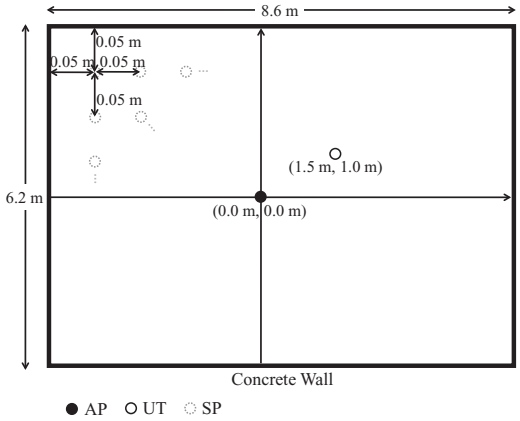


Fig. 3. Simulation environment and terminal positions.

Table 1. にシミュレーション諸元を示す．伝搬路特性は６回までの反射を考慮した２次元レイトレーシング法を用いて計算する．RSSI プロファイル$\boldsymbol{p}_1$, $\boldsymbol{p}_2$ は，Fig. 2 に示される無線端末の相手認証手順に従って取得する．また，SP を想定した別の場所からの送信に対し，RSSI プロファイル$\boldsymbol{p}_3$ を取得する．RSSI プロファイルを生成する際，雑音による影響を軽減するために同一の指向性パターンで 32回の測定を行い，その測定サンプルの同相加算を行ってRSSI を得る．RSSI は後に示す実験装置の仕様に合わせ，1 dB 刻みの値とする．また，搬送波周波数は実験に用いた周波数と同じ2.480 GHz とし，RSSI プロファイルの長さを 32, 64, 128, 256 と変化させる．信号対雑音電力比 SNR (Signal -to- Noise Ratio) は，0 dB, 10 dB, 20 dB とする．なお，SNRの設定において信号電力は，AP・UT の両方にオムニアンテナを用いた場合の受信信号電力を基準とする．したがって，指向性アンテナを使用した場合の瞬時のSNR は，受信信号電力の変化に比例して変化する．また，SP のSNR は，UTでの信号電力を基準として，レイトレーシング法により求められた各地点の信号強度に

比例して，UTでの基準のSNR から変化させている．レイトレーシング法において，３次元モデルではなく２次元モデルとしている．この理由は，数値計算を容易にする目的からでなく，SP により有利な環境を想定して安全性を評価する目的からである．３次元モデルの場合は，２次元モデルの場合よりもマルチパスが増えることにより，UT とSP とのRSSIプロファイルの相関係数が低下する推定されるので，２次元モデルでの評価の方がSP にとって有利になる．

Table 1. Simulation parameters.

Room size	6.2m×8.6m
Wall material	Concrete (μ_r=6.76, Ã=0.0023 S/m)
Terminal positions	AP: (0.0 m, 0.0 m) UT: (1.5 m, 1.0 m) SP: placed 0.05 m intervals
Channel model	2D Ray-tracing Reflection: up to 6 times Vertical polarization
Carrier frequency	2.480 GHz
Averaging	32 sample
Length of RSSI profile	32, 64, 128, 256
SNR	0 dB, 10 dB, 20 dB

3.2 シミュレーション結果

はじめに，SP が(-1.5m, -1.5m) に存在し，SNR = 20 dB，n= 256 の場合のRSSIプロファイル$\boldsymbol{p}_1$，$\boldsymbol{p}_2$，$\boldsymbol{p}_3$をFig. 4 に示す．$\boldsymbol{p}_3$ はSP が測定用信号をAP に送信した場合にAP で得られるRSSI プロファイルである．Fig. 4 より$\boldsymbol{p}_1$ と$\boldsymbol{p}_2$ のRSSI プロファイルは同様の傾向がみられるが，$\boldsymbol{p}_1$ と$\boldsymbol{p}_3$ のRSSI プロファイルは電波伝搬特性の場所依存性により，まったく異なっている．この電波伝搬特性の相違を利用して位置識別が可能となり，それに基づいて相手認証が行える．なお，この場合，$\boldsymbol{p}_1$　$\boldsymbol{p}_2$ 間の相関係数は0.98，$\boldsymbol{p}_1$　$\boldsymbol{p}_3$ 間の相関係数は0.13 となっている．$\boldsymbol{p}_1$−$\boldsymbol{p}_2$間の相関係数が1にならないのは，RSSI プロファイルを１dB 刻みで量子化しているため，受信機雑音の影響で場合により $\boldsymbol{p}_1$, $\boldsymbol{p}_2$ の値に1dB刻みの相違が発生するためと考えられる．

Fig. 5 にSP の位置を変化させた場合の $\boldsymbol{p}_1$−$\boldsymbol{p}_2$間と$\boldsymbol{p}_1$−$\boldsymbol{p}_3$ 間の相関係数の空間的な累積分布（CDF: Cumulative Distribution Function）を示す．

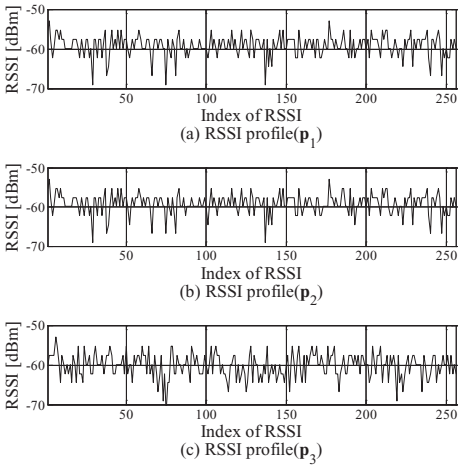


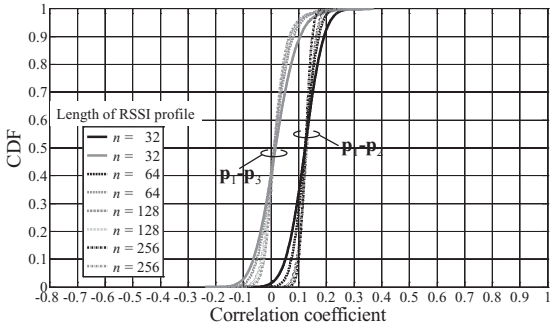
Fig. 4. RSSI profiles, where SP was placed at (-1.5 m, -1.5 m).

Fig. 5 (a) に示されるSNR=0dB の場合，$\boldsymbol{p}_1$−$\boldsymbol{p}_3$ 間の相関係数は0.0 付近に集中し，系列長n が増加するに伴いより集中する傾向がある．また，$\boldsymbol{p}_1$−$\boldsymbol{p}_2$ 間の相関係数は0.12付近に集中し，系列長nが増加するに伴いより集中する傾向がある．ここで，系列長の増加に伴う特性の変化は，相関係数に大きく影響する受信器雑音の確率的な偏りが減少するためと考えられる．Fig. 5 (b) に示されるSNR=10dB の場合，$\boldsymbol{p}_1$−$\boldsymbol{p}_2$ 間の相関係数は0.78付近に集中する一方，$\boldsymbol{p}_1$−$\boldsymbol{p}_3$ 間の相関係数は0.1を中央値として-0.3 から0.8の範囲に分布している．

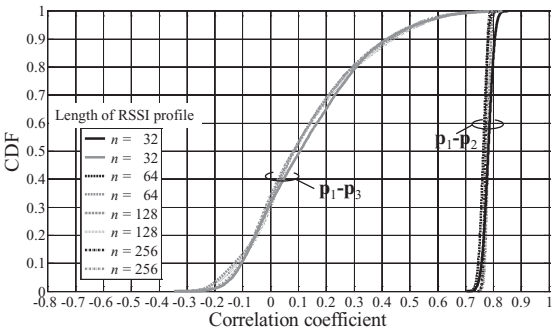
Fig. 5 (c) に示されるSNR=20dB の場合，$\boldsymbol{p}_1$−$\boldsymbol{p}_2$間の相関係数は0.95 付近に集中する一方，$\boldsymbol{p}_1$−$\boldsymbol{p}_3$ 間の相関係数は0.13 を中央値として-0.35 から0.9 の範囲に分布している．また，系列長の増加に伴う変化が比較的少ない．このことは，指向性パターンをランダムに設定することに起因する確率的な偏りが，n=32 程度でほぼ無くなっていることを意味している．また，Fig. 5 (a), (b), (c) を比較すると，系列長を増加させてもSNR を実効的に改善する効果がないことが分かる．

位置識別を誤りなく実施するためには，$\boldsymbol{p}_1$−$\boldsymbol{p}_2$ 間の相関係数と$\boldsymbol{p}_1$−$\boldsymbol{p}_3$ 間の相関係数の累積分布の範囲に重なりがないことが必要となる．SNR が20dB の場合，n の大きさによらず，$\boldsymbol{p}_1$−$\boldsymbol{p}_2$ 間の相関係数が0.91 以下になる累積確率は0であり，$\boldsymbol{p}_1$−$\boldsymbol{p}_3$ 間の

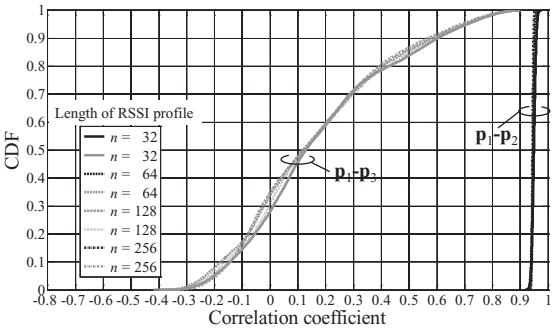
相関係数が0.91以下になる累積確率は１である．そのため，判定閾値をたとえば0.91 に設定すれば，ほぼ完全にUTの位置識別が可能となり，UTの相手認証ができるため，SP の「なりすまし」を排除できる．しかし，SNR が10dB の場合は，p_1－p_2 間の相関係数の最大値が小さくなり，そのような判定閾値は設定できない．位置識別に基づく相手認証を誤りなく実施するには, ある程度のSNR を確保する必要があることが分かる．



(a) SNR=0 dB



(b) SNR=10 dB



(c) SNR=20 dB

Fig. 5. CDF of RSSI correlation coefficient (simulation).

Fig. 6 にSNR = 20 dB，$n = 256$ の場合におけるSP位置に対するp_1－p_3 間の相関係数の空間分布を示す．Fig. 6 より，高い相関係数を示す位置は，AP(0.0m, 0.0m) とUT(1.5m, 1.0m) を結ぶ直線上およびその周辺に多く存在することがわかる. これが, Fig. 5 においてp_1－p_3 間の相関係数の累積分布において相関係数が高い部分と関係しており, 位置識別による相手認証の特性を劣化させる原因となっている. このような相関係数が高くなる場所が存在ことは, 電波を用いた秘密鍵共有方式で既に報告されており, 直接波の影響であることが指摘されている[16]．なお，電波を用いた秘密鍵共有方式に対しては, 直接波の影響を低減させる手法が提案されている[17]．位置識別による相手認証においても，同様の手法を用いることで, 位置識別の性能向上が期待できる．

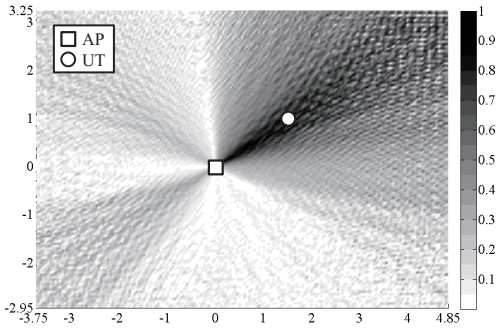


Fig. 6. Spatial distribution of RSSI correlation coefficient (simulation).

４．実環境下における実験による評価

4.1 実験環境と装置のシステム諸元

エスパアンテナを用いた装置の構成と方式諸元は，秘密鍵共有実験のために開発した装置と同様である[10-11]．Fig. 7 に実験を行った部屋と各端末の配置を示す．実験は，縦(x)・横(y)・高さ(z) が6.2m×8.6m×3.0m の部屋で行った．部屋の壁はコンクリートであり，金属ドアと窓ガラスが含まれる．また，室内には机や什器などがいくつか配置されている．なお，装置の操作は部屋内で行ったが，操作者の存在が測定結果に与える影響が少なくなるよう

に壁際で測定を行った．ここで，実験を行う部屋の縦・横の大きさ，AP の座標 (x, y, z) = (0.0m, 0.0m, 0.7m) とUT の座標 (1.5m, 1.0m, 0.7m) の内で(x, y) 座標は計算機シミュレーションと同じである．

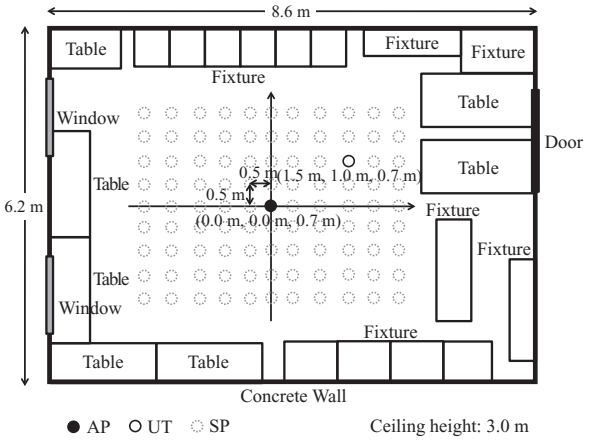


Fig. 7. Experimental environment and configuration of terminals.

この状態で，Fig. 2 に示される無線端末の相互認証手順の第一段階を実行し，RSSI プロファイル$\boldsymbol{p}_1$を取得する．次に，アンテナの指向性パターンを同じ状態に設定してRSSI プロファイル$\boldsymbol{p}_2$ を 98個取得する．複数回の測定を行うのは，電波伝搬特性や装置特性の変動，受信雑音などの影響を，$\boldsymbol{p}_1$－$\boldsymbol{p}_2$ 間の相関係数の累積分布で表すためである．この回数は後で述べるように，$\boldsymbol{p}_1$－$\boldsymbol{p}_3$ 間の相関係数の累積分布を求めるのに必要なSPの測定点数と同数に設定している．なお，$\boldsymbol{p}_1$ の生成完了から$\boldsymbol{p}_2$ の生成開始までの間隔は約10秒であり，98個すべての$\boldsymbol{p}_2$ の測定を終了するまでには，さらに約50秒程度の所要時間であった．次に，SP を想定した別の場所からの送信に対し，アンテナ指向性パターンなどの設定を同じ状態でRSSI プロファイル$\boldsymbol{p}_3$ を取得する．SP は0.5m間隔の格子上に配置し，測定点数は98個となる．

また，RSSI プロファイルの系列長さn は 32, 64, 128, 256 と変化させる．なお，計算機シミュレーションと同様に，RSSI プロファイルを生成する際に同一指向性パターンで 32回の測定を行い，その測定値を同相加算してRSSI を得る．

4.2 実験結果

Fig. 8 に$\boldsymbol{p}_1$－$\boldsymbol{p}_2$ 間と$\boldsymbol{p}_1$－$\boldsymbol{p}_3$ 間の相関係数の累積分布を示す．図より$\boldsymbol{p}_1$－$\boldsymbol{p}_2$ 間の相関係数が，0.96 近傍（ほぼ0.93から0.99）に分布する一方，$\boldsymbol{p}_1$－$\boldsymbol{p}_3$ 間の相関係数が，-0.05 を中央値として-0.85 から0.95の範囲に分布している．また，両者の相関関数の分布には重なる部分があるため，UT とSP をほぼ完全に識別する判定閾値が設定できない．また，系列長nを変化させても相関係数の累積分布はほとんど変化しない．このことは，アンテナの指向性パターンをランダムに設定することに起因する確率的な偏りが，n=32 程度でほぼ無くなっていることを意味している．

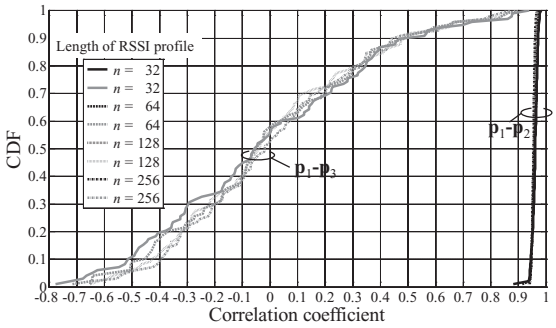


Fig. 8. CDF of RSSI correlation coefficient (experiment).

実環境下における実験結果は，$\boldsymbol{p}_1$－$\boldsymbol{p}_3$ 間の相関係数が負となる割合が多く，計算機シミュレーション結果と大きく相違している．一方，系列長に対する相関係数の累積分布は，実験結果もシミュレーション結果も同様の傾向でほとんど変化しない．また，$\boldsymbol{p}_1$－$\boldsymbol{p}_2$ 間の相関係数の実験結果をFig. 7 のシミュレーション結果と比較すると，Fig. 7 (c)のSNR=20dBの結果に近いことから，実験結果はおおよそSNR=20dB 相当の結果であると考えられる．

Fig. 9 にn=256 の場合における$\boldsymbol{p}_1$－$\boldsymbol{p}_3$ 間の相関係数の空間分布を示す．Fig. 9 より，相関係数が高い場所は，計算機シミュレーションと同様にAP(0.0m, 0.0m) とUT(1.5m, 1.0m) を結ぶ直線上およびその周辺に多く存在することがわかる．なお，Fig. 9 において相関係数が負となるものは，その絶対値をとって表示している．AP から見てUT と逆

方向に相関係数が高い部分があるのは，相関係数が負側に小さくなっている部分であり，相関係数が負の部分の累積分布に関係している．

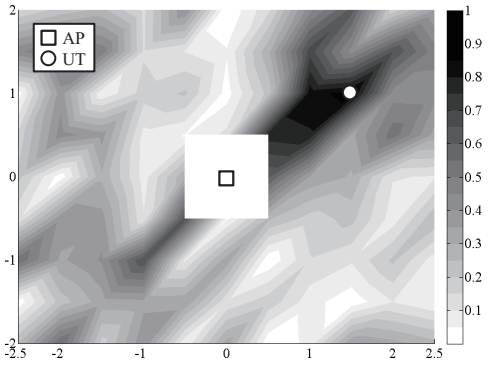


Fig. 9. Spatial distribution of RSSI correlation coefficient (experiment).

5．むすび

本論文では，アンテナの指向性パターンを変化させて取得した受信信号強度(RSSI)変動の時系列を用いた無線端末の相手認証方式の原理を示すとともに，エスパアンテナを用いた場合について，位置識別のためのRSSI プロファイルの類似度を示す相関係数を計算機シミュレーションと実環境下の実験により評価した．

計算機シミュレーションの結果，RSSI プロファイルの系列長の増加に伴う特性変化が比較的少ないことが分かった．一方，実験結果は相関係数の累積分布の負の部分が増加するなど計算機シミュレーション結果と相違することが明らかとなった．計算機シミュレーション結果と実験結果の相違は，シミュレーションにおける電波伝搬環境モデルが実際と相違していることが一因と考えられるが，今後さらに詳細な検討が必要である．今回の評価は，特定の環境のみであったので，異なる環境での評価も重要である．

文　献

1) J. E. Hershey, A. A. Hassan, and R. Yarlagadda, “Unconventional cryptographic keying variable management,” IEEE Trans. Commni., **43**, 3-6, (1995).

2) A.A. Hassan, W.E. Stark, J.E. Hershey, and S. Chennakeshu, “Cryptographic key agreement for mobile radio,” Digital Signal Processing, **6**, 207-212, (1996).

3) H. Koorapaty, A.A.Hassan, and S. Chennakeshu, “Secure information transmission for mobile radio,” **4**, 52-55, (2000).

4) L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, “Using the physical layer for wireless authentication in time-variant channels,” IEEE Trans. Wireless Commun., **7**, 2571-2579, (2008).

5) 尾谷尚宣，川村俊一，岩井誠人，笹岡秀一，“電波伝搬特性に基づく端末認証方式の基礎検討”，電子情報通信学会技術研究報告，RCS2010-**42**，145-150，(2010)．

6) 笹岡秀一，尾谷尚宣，岩井誠人，“電波伝搬特性を用いた位置識別に基づく相手認証方式の特性評価”，電子情報通信学会論文誌(B)，**96**，831-841，(2013)．

7) 辻宏之，“アレーアンテナを用いた屋内外の無線局位置推定の実験的検証”，電子情報通信学会論文誌(B)，**90**，784-796，(2007)．

8) 池田昇平，辻宏之，大槻知明，“部分空間マッチングを用いた屋内位置推定における信号部分空間相関の影響”，電子情報通信学会技術研究報告，RCS2007-**99**，13-17，(2007)．

9) 黒崎雄太，山田寛喜，山内芳雄，“近似信号部分空間を用いた屋内無線端末位置推定に関する検討”，電子情報通信学会技術研究報告，A･P2009-**35**，141-146，(2009)．

10) 青野智之，樋口啓介，大平孝，小宮山牧兒，笹岡秀一，“エスパアンテナを用いたIEEE802.15.4無線秘密鍵共有システム”，電子情報通信学会論文誌(B)，**88**，1801-1812，(2005)．

11) T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, “Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channel,” IEEE Trans. on Antennas Propag., **53**, 3776-3784, (2005).

12) 尾谷尚宣，北野隆康，清水崇之，岩井誠人，笹岡秀一，“アレーアンテナを用いた電波伝搬特性に基づく秘密鍵共有・無線機識別装置の開発”，電子情報通信学会技術研究報告，A･P2010-**138**，31-36，(2011)．

13) T. Shimizu, N. Otani, T. Kitano, H. Iwai, and H. Sasaoka, “Experimental validation of wireless secret key agreement using array antennas,” Proc. The XXX General Assembly and Scientific Symposium of the International Union of Radio Science (URSI GASS’11), 1–4, (2011).

14) 尾谷尚宣，岩井誠人，笹岡秀一，“電波伝搬特性に基づく無線端末認証方式の実験的評価”，電子情報通信学会技術研究報告，A･P2011-**80**，19-24，(2011)．

15) 尾谷尚宣，岩井誠人，笹岡秀一，“電波伝搬特性に基づく無線端末認証方式の基礎特性評価”，電子情報通信学会技術研究報告，A・P2011-187，13-18，(2012).
16) 樋口啓介，青野智弘，大平孝，笹岡秀一，“エスパアンテナを用いた無線秘密鍵共有方式における共有秘密鍵の空間相関特性シミュレーション”，電子情報通信学会技術研究報告，A・P2004-42，7-12，(2004).
17) 清水崇之，岩井誠人，笹岡秀一，“エスパアンテナを用いた秘密鍵共有方式における盗聴耐性の高い鍵生成法”，電子情報通信学会論文誌(B)，92，1348-1361，(2009).