Estimation of Fading Characteristics Based on Multiple Observed Signals at Remote Locations

Keisuke INOUE*, Hisato IWAI* and Hideichi SASAOKA*

(Received October 29, 2009)

Wireless communications have become popular and are used in various environments such as outdoor, offices, homes, etc. As the use of the wireless communications becomes common, security issues have become one of the most important technical subjects. In order to realize secure communications, a new wireless security technique based on wireless propagation characteristics has been proposed. The proposed technique is based on the reversibility and the locality of the wireless propagation characteristics to generate a common encryption key sequence between two wireless stations without pre-assignment and sharing of the key. The generated key can be used to realize secure secret wireless communications. The security performance of the technique has been analyzed in a viewpoint of encryption, however it has not been discussed from a viewpoint of radio propagation. The security of the technique relies on the fact that the received signal cannot be estimated from a remote point where the distance from the target point of the estimation is larger than the correlation length of the multipath fading environment. However it may be possible if an eavesdropper uses a higher performance receiving system such as directional antennas or multiple antenna systems, etc. In this paper, the possibility to break the locality is discussed. A method to estimate the received signal characteristics is presented based on the observed signals at multiple different points at a certain distance from the target and the estimation performance of the technique is evaluated quantitatively via computer simulations. The dependence of the estimation parameters on the estimation performance is analyzed. The mechanism of the estimation method is clarified through the analysis assuming a simpler propagation model. Based on the results of the analysis, a theoretical expression for the requirement to achieve successful estimation is derived.

Key words : Estimation of propagation characteristics, multipath fading, secret key agreement, theoretical analysis

キーワード : 伝搬特性推定，マルチパスフェージング，秘密鍵共有方式，理論検討

複数地点観測信号に基づく他地点伝搬路特性の推定

井上　恵輔，岩井　誠人，笹岡　秀一

1. まえがき

近年，無線通信の発展と需要の拡大に伴い，種々の新しい無線システムが提案，検討されている．しかし，無線通信は電波を利用しているため，不特定多数の第三者(盗聴局)が傍受可能であるという情報セキュリティ面での脆弱性が課題となる．これに対する無線通信のセキュリティ向上技術の一つとして，無線通信の伝搬路特性に基づく秘密鍵共有方式が検討されている [1-3]．これらの方式は，マルチパスフェージングの場所依存性及び電波伝搬の可逆

* Department of Electronics, Doshisha University, Kyotanabe, Kyoto, 610-0321, Japan
Telephone: +81-774-65-6355, Fax: +81-774-65-6801, E-mail: iwai@mail.doshisha.ac.jp

性により，伝搬路特性は送受信局間でのみ共有でき，ある程度距離が離れた他地点ではその情報を得ることができないという原理に基づいている．この方式は物理現象に基づいていることから情報理論的な安全性を有しており，対盗聴特性は盗聴局の計算資源に依存しないという特徴がある．

しかし，盗聴局が何らかの方法によって正規局間の伝搬路特性を推定できるとすれば，この方式より生成される秘密鍵の安全性は失われる．したがって，盗聴局による正規局の伝搬路特性の推定可能性を明確にすることは，伝搬路特性に基づく秘密鍵共有方式の安全性検討のうえで重要な課題となる．

そこで本研究では，秘密鍵共有方式の安全性検討に資するため，複数観測点の受信情報を用いて離れた地点の受信点の伝搬路特性を推定する方式について検討し，この手法による推定特性を詳細に分析する．マルチパス伝搬環境における推定メカニズムを明らかにするために，計算機シミュレーションにより単一波が到来する伝搬環境における推定特性を詳細に分析する．また，この推定特性の分析結果より推定が正確に行われる条件を導出する．

2. 伝搬路特性に基づく秘密鍵共有方式

現在，無線を利用した通信が広く用いられているが，無線を利用した通信は，その性質上，情報の盗聴が容易であり情報セキュリティー面での脆弱性が課題となるため，情報を暗号化する必要がある．一般に利用されている暗号方式として，公開鍵暗号方式と秘密鍵暗号方式がある [4, 5]．

公開鍵暗号方式は，公開された暗号化鍵を用いて暗号化を行い，復号の際には，秘密の復号鍵を用いて復号を行うという暗号である．公開された暗号化鍵(公開鍵)を知ることで，誰でも暗号化処理を行うことはできるが，復号処理を行うことができるのは，その復号鍵の持ち主である正規の利用者に限られる．また，暗号化用の鍵から復号用の鍵を導こうとすると莫大な計算量が必要なことから，復号鍵の解読は極めて困難である．このような方式は暗号方式として計算量的に安全であると言われる．しかし，復号鍵を用いて復号を行う場合も演算量が多くなるため，復号処理に必要な時間が多くなるなど，処理能力に制約のある移動通信端末に適用しにくいという問題がある [5]．

一方，秘密鍵暗号方式は，暗号化と復号で同じ鍵を用いる方式であり，その鍵を送受信者の間で共有する方式である．この方式では，情報の暗号化と復号で同じ鍵を用いるため，復号のための演算量が少なくなる．演算量が少なくてすむので，大量のデータを高速に伝送する場合に有効である．ただし，秘密鍵暗号方式の場合は，暗号通信を行いたい相手ごとに個別の秘密鍵を安全に共有し管理する必要があり，秘密鍵の配送や保管の際に秘密鍵が第三者に解読される危険性があるなどの問題がある．これらの問題を解決するため，鍵の配送を必要としない秘密鍵共有方式の一つとして，伝搬路特性に基づく秘密鍵共有方式が提案されている [1-3]．

伝搬路特性に基づく秘密鍵共有方式の概要を Fig. 1 に示す．

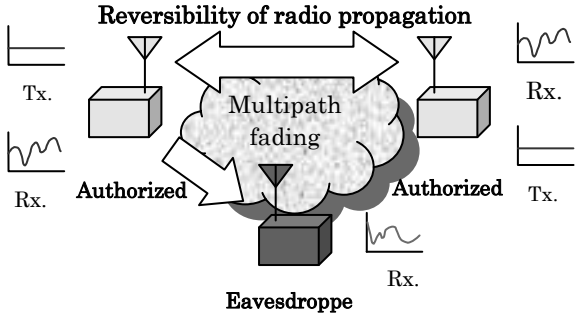


Fig. 1. Concept of wireless security technique based on wireless propagation characteristics.

電波伝搬において一般に送受信点間で可逆性が成り立つことから，正規の送受信者間で伝搬路の特性を共有することができる．Fig. 2 は単一アンテナを用いた場合のアンテナ変位に対するフェージングの相関特性を示している．同図から受信地点から 1/4 波長以上離れるとフェージング変動は相関が十分低くなり，無相関と考えてよい．したがって，フェージング環境における伝搬路の特性は，正規の送受信者間で第三者に秘密裏に共有することができる情報と考えることができる．これが，伝搬路特性

に基づく秘密鍵共有方式の基本原理である.

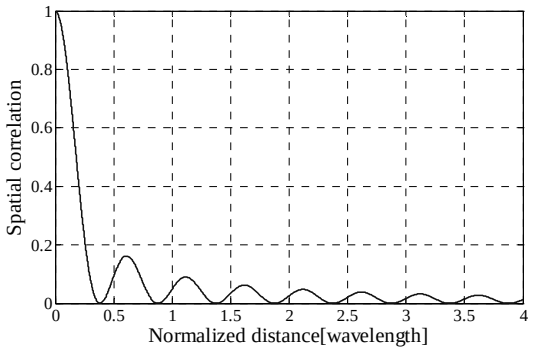


Fig. 2. Spatial correlation in multipath fading environment.

Fig. 3 は，電波伝搬路特性に基づいて秘密鍵(2 値系列)を生成する代表的な方法を概念的に示している. フェージング変動の強度分布からその中央値を求め, フェージングが変動する各時点の信号強度の大小を中央値をしきい値として判定し，0 または 1 に 2 値化する.

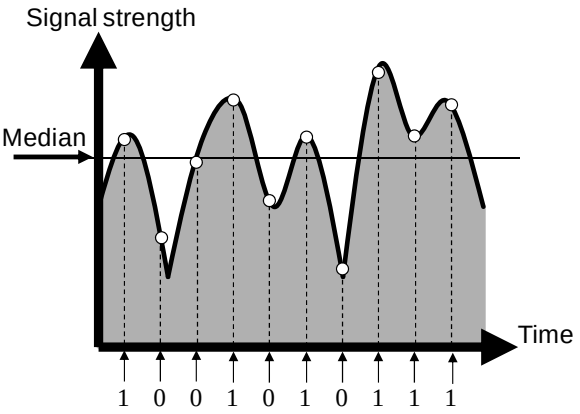


Fig. 3. Binarization by median value.

次に, 盗聴局が正規局のフェージング変動とある程度相関のある伝搬路特性を得たと考えた場合に, 盗聴局が正規局の秘密鍵とどの程度一致する鍵を得ることができるかを示す. フェージング変動の相関がρとなる二つのレイリーフェージングを考え, Fig. 3 に示した生成方法により 2 値系列をそれぞれ生成した場合の秘密鍵の一致特性を Fig. 4 に示す. 相関ρ=0.5 程度では一致率は無相関の場合と大差はない．また，たとえ相関ρ=0.9 でも一致率は 0.8 程度に収まることがわかる. 例えば 128 ビットの暗号鍵生成を考えると, 平均して 8 割程度の一致率では 128 ビット全てが完全に一致する確率はほぼ 0 である．ここで，Fig. 2 よりレイリーフェージング環境において相関値が 0.9 となる距離は 0.1 波長(800Hz において約 4cm, 2.4GHz において約 1.25cm)程度となり被盗聴側にほぼ隣接した状態となる. 盗聴行為は一般に被盗聴側から隠れて行うものであることを考慮すると, この方法により生成された秘密鍵を盗聴することは現実的には不可能であると言える.

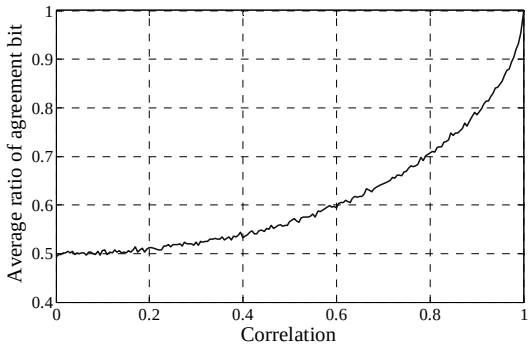


Fig. 4. Average agreement rate for variation of spatial correlation.

3. 他地点伝搬路特性の推定法と基本性能評価

3.1. 複数地点観測信号に基づく他地点伝搬路特性推定法 [6,7]

前章で示したように, 単一アンテナを用いた場合, フェージングの相関距離以上に受信点が離れると, 他地点の伝搬路特性を知ることは困難である. 本研究では, 秘密鍵共有方式の安全性検討という観点から盗聴者にとってより有利な状況(盗聴者が正規の受信局に比べてより性能・機能の高い受信システムを有している場合)を考える．例えば推定局が複数アンテナや指向性アンテナを用いている場合には, 他局の伝搬路特性の推定(これは秘密鍵共有方式では「盗聴」という行為にあたる)の可能性があると考えられる．そこで，本研究では盗聴者が正規受信局の周囲の複数地点で正規局と同時に受信するモデルを考え，電波干渉計の原理 [8]に類似した到来パスの方向検出(=仮想パス)及びその合成によって目的地点の伝搬特性を推定する方式を考える.

この推定方式の概念を Fig. 5 に示す．なお，本稿では二次元の問題を考える．推定を行う前提条件として，推定対象である正規受信局を中心とした半径 R(本論文では波長で正規化した正規化距離として表すこととする)の円周(これを観測円と呼ぶ)を考え，観測円周上に複数の観測点 P_n(n=1, …, N:N は観測点数)を等角度間隔で理想的に配置するものとする．また，推定対象局からの P_n の角度方向を γ_n と表す．さらに，P_n において観測される受信信号 Z_n は全て既知であるとし，これらの観測信号は推定対象局が受信するタイミングと同時に受信するものとする．

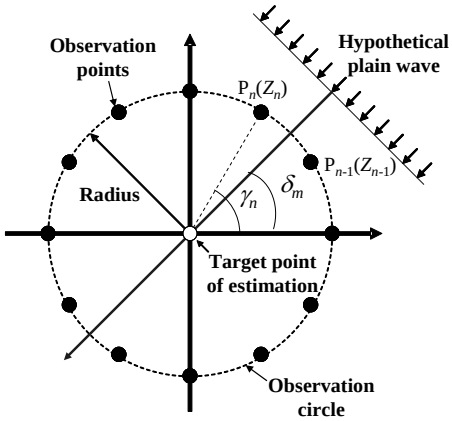


Fig. 5. Estimation model.

推定方法は以下の通りである．まず，実際の到来パスをある到来方向 δ_m の平面波とする仮想的なパス A_m(m=1, …, M:M は仮想パス数)を考え，それぞれの仮想パスごとに観測信号 Z_n を用いて推定対象局における受信信号の振幅・位相を推定する．本研究では δ_m は $2\pi m/M$ と等間隔に設定する．ここで，Z_n から推定される信号は $Z_n\exp(-j2\pi R\cos(\gamma_n-\delta_m))$ となる．さらに全ての観測点についてこの値を平均することにより，仮想パス A_m に対する推定対象局における推定信号 X_m は以下のように得られる．

$$X_m = \frac{1}{N}\sum_{n=0}^{N-1} Z_n \exp(-j2\pi R\cos(\gamma_n-\delta_m) \qquad (1)$$

ここで，X_m の値は，実際のパスの到来角度が仮想的な角度 δ_m と一致する場合は，n に対する各項がそれぞれ同位相となりその和(=$|X_m|$)の絶対値は大きくなる．それに対して一致しない場合は，各項の位相はランダムになりその和は位相が一致する場合に比べて小さくなる．ここで，すべての到来方向成分の寄与について考えるため，求めた X_m をすべての m について全周方向で平均し，以下のように推定対象局における推定受信信号 X を得る．

$$X = \frac{1}{M}\sum_{m=0}^{M-1} X_m \qquad (2)$$

3.2. シミュレーションによる基本性能評価

3.2.1. 信号強度変動の推定

前節で説明した検討手法の推定例を計算シミュレーションにより示す．ここでは，伝搬環境のモデルとして，複数の平面波が周囲一様の方向から到来する Jakes モデル[9]に類似する伝搬環境を仮定する．このモデルの概念を Fig. 6 に示す．到来マルチパスは平面波とし，その数を 5 とする．また，全ての到来マルチパスは等しい振幅(=1)をもつものとする．さらに，推定対象局における各パスの到来方向，受信位相は[0, 2π)の範囲で一様分布に従うランダム値であるとする．この伝搬環境モデルにおいて 3.1 節に示した推定手法を適用した場合の推定結果を示す．

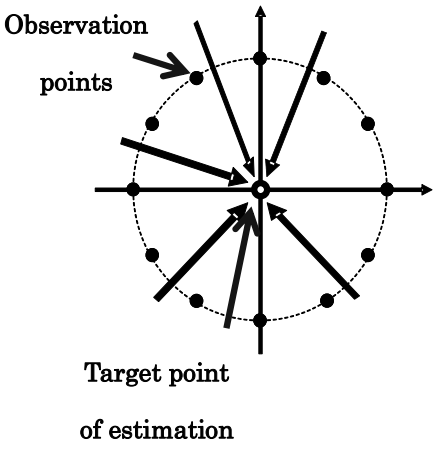


Fig. 6. Multipath model.

Fig. 7 及び Fig. 8 は信号強度の推定結果である．Fig. 7 は観測点数 N を 20 とした場合，Fig. 8 は 40 の場合の結果である．また，観測円半径 R=4 波長，仮想パス数 M=1000 と仮定している．本論文では秘

密鍵共有方式の安全性検討という立場で議論を行うため，仮想パスの数は十分に大きく設定することが適切である(仮想パス数の変化に対する特性については後に詳しく述べる)．したがってここでは，仮想パス数 M=1000 としている(後述のシミュレーション評価では特に断りがない限り M=1000 としている)．Fig. 7 および Fig. 8 の横軸は，フェージング環境(到来方向及び各到来波の位相)を変化させて異なるフェージング環境とした場合の試行回数を示している．また両図には，実際の受信信号強度，推定信号強度に加えて，これらの比を併せて示している．Fig. 7 では実際の値と推定値の比がフェージング環境を変化させるごとに変動しているが，Fig. 8 ではこの値が一定となっている．すなわち，実際の値と推定値が比例の関係であり，これよりフェージングによる信号強度変動を正確に推定できていることがわかる．

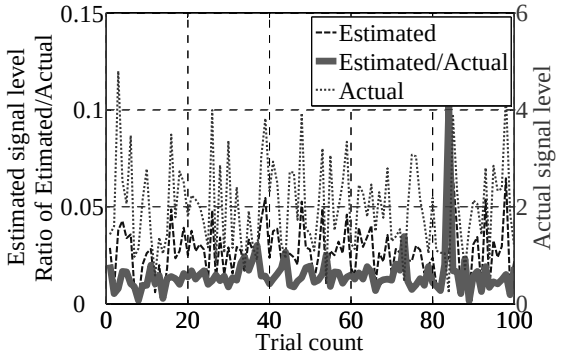


Fig. 7. Actual and estimated signal variations (N=20).

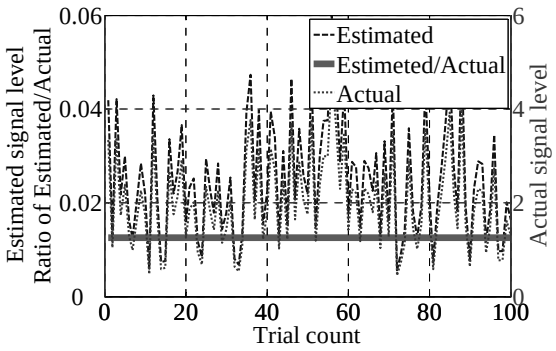


Fig. 8. Actual and estimated signal variations (N=40).

3. 2. 2. 相関値を用いた推定特性の定量化

次に，3.2.1 節の結果を踏まえ，Fig. 7 及び Fig. 8 に示されたようなフェージング環境の変化に伴う信号強度変動について，実際の値の変動と推定値の変動との間の相互相関係数を計算し，この相関を推定精度の指標として推定特性の定量化を行う．Fig. 8 のような状況では相関はほぼ 1 となり，Fig. 7 では相関値は 1 よりも小さくなる．この方法を用いて，観測円の半径，観測点数などを変化させた場合の推定特性の変化を示す．

Fig. 9 は観測円の半径 R を変化させた場合の相関特性を示している．ここでは観測点数 N=100 としている．N=100 の場合には観測円半径が 15 波長程度以下で目的の受信強度変動特性が正確に推定できることがわかる．

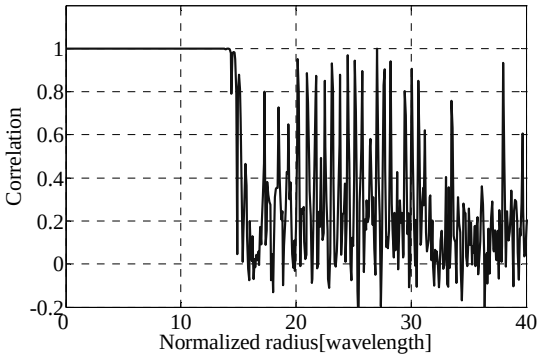


Fig. 9. Correlation characteristics when radius of observation circle is changed.

4. 推定特性に関する詳細検討

4. 1. 推定メカニズムと推定特性に関する分析

4. 1. 1. 仮想パスの到来方向に対する推定値の変化

Fig. 9 より観測円半径が 15 波長程度までほぼ正確な推定(相関の値がほぼ 1 となる)が実現されているが，観測円半径がそれ以上に大きくなると急に推定が不可能となる特性となることがわかる．本節では，このような推定特性が得られるメカニズムを詳しく分析するために Fig. 6 に示すモデルよりも簡易なモデルを考える．Fig. 10 に，ただ一つの平面波が Fig. 5 の 0[rad.]から到来する環境モデルを示す．観測点は 0[rad.]から配置しているので，一つ目の観測点の角度方向 γ_1 と平面波の到来方向との角度差はない．この環境において，仮想パスの到来方向 δ_m を変化させる場合について考える．なお，この到来波の推定対象局での受信位相を $\pi/2$ とする．

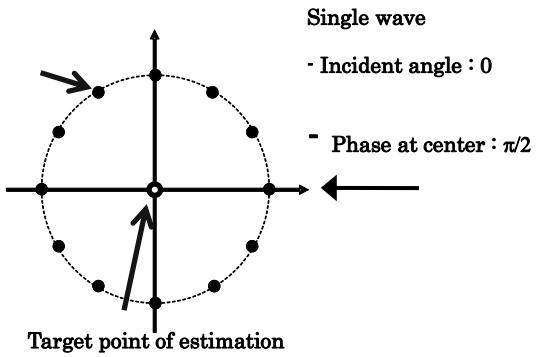
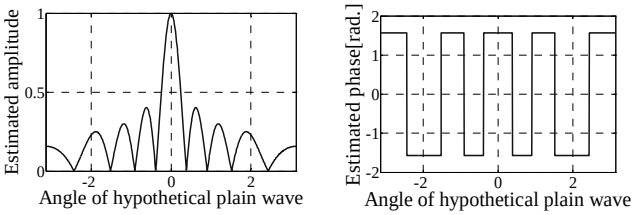
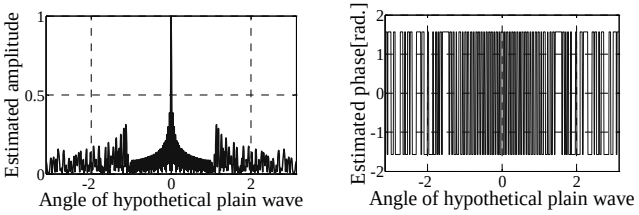


Fig. 10. Single wave model.

Fig. 11 は, Fig. 10 に示したモデルにおいて, N=100, M=1000 とし，観測円半径 R=1 波長，15 波長とした場合における，仮想パスの到来方向に対する式(1)で得られる推定値 X_m の振幅と位相の変化を示している．ここでは，この振幅特性がアンテナパターンに類似することから，たとえば Fig. 11(a)において,δ_m が±0.4[rad.]の範囲内の特性をメインローブ, その一つ外側の特性を第一サイドローブ, そのさらに外側を第二サイドローブなどと便宜的に呼ぶことにする.



(a)R=1[wavelength]



(b)R=15[wavelength]

Fig. 11. Estimated amplitude and phase when azimuth direction of hypothetical wave is changed (Arrival direction =0[rad.]).

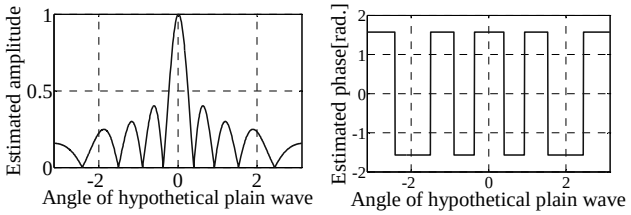
それぞれの位相特性から，推定位相は正しい位相と，それが反転した位相，の二つの場合しか存在し得ないことがわかる．これは，観測点の配置が推定対象局の周りに対称に配置されているためであり，後に理論的に検討する．

また, 最終的な推定値は各仮想パスに対する推定値 X_m を平均することによって得られるが，推定が可能な必要条件, つまりこの平均値が十分に大きくなる条件, としてメインローブの範囲内に少なくとも一つの仮想パスを考えることが必要と考えられる．Fig. 11 より，位相特性がメインローブに対して奇数番目のサイドローブが逆相, 偶数番目のサイドローブが同相であることから, その平均値は観測円半径の変化に対して振動的に変化することが予想される．また，観測円半径が大きくなるに伴い，平均値である推定値に対するメインローブ部分の寄与が小さくなり，平均値の振幅は小さくなる，または, 平均値が逆相になる可能性も生じると考えられる．

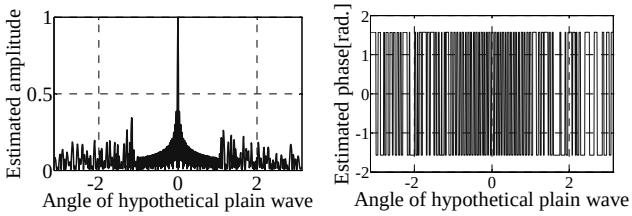
次に，γ_1 (0[rad.]方向)と実際に到来する平面波との間に角度差がある場合を考える. 平面波の到来方向を観測点間角度の 1/4 とした場合の Fig. 11 と同様の特性を Fig.12 に示す．ここでは N=100 としているので観測点間角度は 1/4×2π/100＝0.0157[rad.]である．また，M=1000 とし，観測半径 R=1 波長，15 波長の場合を考える．同図より，角度差がある場合にも, 角度差がない場合と同様に推定位相は正しい位相とそれが反転した位相, の二つしか存在しなく, 観測円半径が大きくなるに伴い, 平均値である推定値に対するメインローブ部分の寄与が小さくなることがわかる．なお，Fig. 12 において，観測点数 N=100 で正確な推定が不可能である観測半径 R=15 波長の場合には, パターンはわずかに非対称になっている．

これらの特性より, 観測点の推定対象局との角度方向γ_1 と平面波の到来方向との角度差がある場合でも，振幅・位相特性ともに，角度差がない場合とほぼ同様の特性を示すことがわかる(ただし, Fig. 12 の R=15 波長など正確な推定が行えない条件では, 振幅特性においてパターンがわずかに非対称なることから, 推定値 X の振幅値は角度方向γ_1 と平面波

の到来方向との角度差により変化することが考えられる). ここで得られた結果より，パスがランダム方向に到来する伝搬環境においてもここで示した考え方は一般に適用可能であり，以降の解析を簡易化することができると考えられる.



(a)R=1[wavelength]



(b)R=15[wavelength]

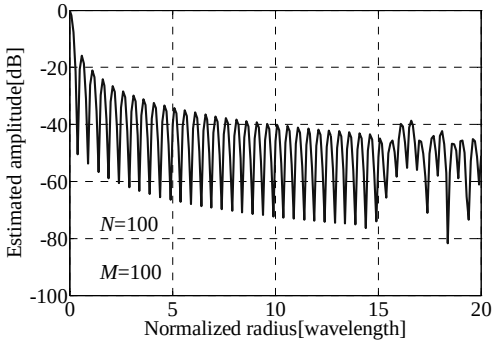
Fig. 12. Estimated amplitude and phase when azimuth direction of hypothetical wave is changed (Arrival direction =0.0157[rad.]).

4.1.2. 振幅及び位相推定確率の変化

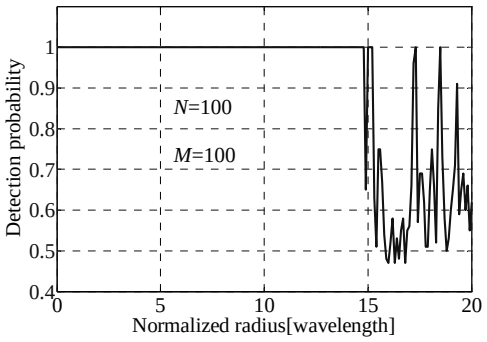
次に，前節の結果を踏まえ，観測円半径の変化に対する最終的な推定値 X の振幅及び位相推定確率の変化を Fig. 13 に示す.

前述のように，これは Fig. 11，Fig. 12 の特性を周方向に積分した値となる．ここで，(a)はただ一つの平面波の到来方向が[0, 2π)の範囲でランダムに到来する伝搬環境において 100 回試行した結果である(R=15 波長以下では推定精度は到来方向に依存せず 100 回試行したとしても一定値であるが，R=15 波長以上の場合は到来方向により推定振幅値が変化するので 100 試行の平均値を示している). (b)は位相推定確率である. 前節で示したように推定位相は正しい位相と逆相のみであることを考慮して，位相推定の指標として，正しい推定位相値を得た割合を用いている.

前節においても推測されたように，推定値の振幅は観測円半径の増加に伴って振動的に減少していくことがわかる．観測円半径が 15 波長程度までは振幅がかなり小さくなっても位相は正しく推定されている．しかし，Fig. 9 と同様に観測円半径が 15 波長程度を超えると，位相が逆転する可能性が生じ正確に推定できない場合が生じる．これは，メインローブの範囲が値が反転した位相部分に対して相対的に小さくなり，逆相部分を十分に補うだけの大きさを得ることができなくなったことによると考えられる.



(a)Amplitude



(b)Phase

Fig. 13. Estimated amplitude and probability of correct estimation of phase.

4.1.3. 雑音が存在する場合の推定特性

ここまでは雑音の影響を無視し，信号のみが存在する場合について議論してきた．しかしながら，実際の環境を考えた場合には雑音は必ず存在する．したがって，その影響を評価することは重要である.

ここでは Fig. 6 の伝搬環境モデルにおいて，雑音が存在する環境を想定する．Fig. 13(a)より推定値の振幅は観測円半径の変化に対して大きく振動しているので，雑音が存在する環境では推定特性は Fig. 9 よりも劣ることが考えられる.

Fig. 14 は, 信号対雑音電力比 SNR (Signal to Noise Ratio)=0dB，20dB，40dB とした場合の，Fig. 9 と同様な観測円半径の変化に対する相関特性を示している．ここで，SNR は一観測点における到来波の合成信号の平均電力と雑音平均電力の比である．Fig. 9 ではフラットであった観測円半径が 15 波長程度以下の部分においても，Fig. 13(a)に示す推定値の振幅の振動に伴って相関特性が大きく変動していることがわかる．ただし，SNR=40dB という SNR が大きい環境では，Fig. 9 の推定特性との差は大きくない．

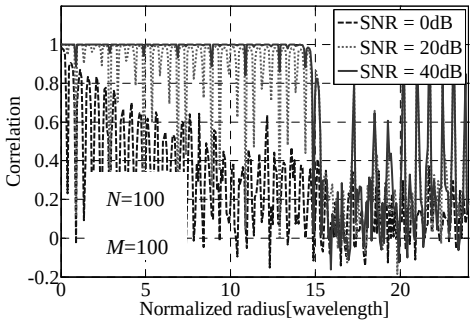


Fig. 14. Correlation characteristics in a noisy channel when radius of observation circle is changed.

4. 2. 推定特性に関する理論検討

4. 2. 1. 位相推定特性

以下では雑音が無い環境について考えるものとする．

ここでは，これまで示した推定特性が得られるメカニズムを理論的に検討する．4.1.1 節の特性分析により，単一の平面波が到来する伝搬環境では推定位相は正しい位相と，それが反転した位相，の二つの場合しか存在し得ないことがわかった．これは以下のように説明することができる．

まず，ある観測点 P_{n_1}(角度方向 γ_{n_1})に対して推定対象局を中心とした点対象な観測点 P_{n_2}($\gamma_{n_2}=\gamma_{n_1}+\pi$, $n_2=n_1+N/2$)を考える．ここで，到来波が平面波とすると式(1)の Z_n は以下の式で表すことができる．

$$Z_n = r\exp(\mathrm{j}(\omega + 2\pi R\cos(\gamma_n - \varphi))) \qquad (3)$$

ここで，r，ω，φは対象とする到来波の振幅，推定対象局における位相，到来角である．

式(1)と式(3)から仮想パス A_m に対する観測点 P_{n_1}, P_{n_2}における推定信号 X_{m,n_1}，X_{m,n_2}はそれぞれ以下の式で表すことができる．

$$\begin{aligned} X_{m,n_1} &= r\exp(\mathrm{j}(\omega + 2\pi R(\cos(\gamma_{n_1} - \varphi) - \cos(\gamma_{n_1} - \delta_m))) \\ X_{m,n_2} &= r\exp(\mathrm{j}(\omega + 2\pi R(\cos(\gamma_{n_2} - \varphi) - \cos(\gamma_{n_2} - \delta_m))) \end{aligned} \qquad (4)$$

$\gamma_{n_2}=\gamma_{n_1}+\pi$を用いると，以下の結果が得られる．

$$X_{m,n_1} + X_{m,n_2} = 2r\cos Q\exp(\mathrm{j}\omega) \qquad (5)$$

ここで，$Q = 2\pi R(\cos(\gamma_{n_1}-\varphi) - \cos(\gamma_{n_1}-\delta_m)$である．この結果から，ある観測点の信号情報の位相と点対象に位置する観測点の信号情報の位相を足し合わせると，互いの位相成分が相殺され正しい位相成分(ω)だけが残り，cos Q の値が正ならば推定位相は正しい位相，負ならばそれが反転した位相になる．さらに，式(5)の関係はすべての観測点において成り立ち，それらを全て加えた推定値の位相は到来平面波の位相や到来角などの伝搬環境や，観測点数や観測円半径などの推定手法のパラメータに依存せずに正しい位相と，それが反転した位相，の二つの場合しか存在し得ない．

4. 2. 2. 推定可能条件

次に，前節の検討を踏まえて，マルチパス伝搬環境における正確に推定が行える条件(推定可能条件)について考える．ここで，仮定するマルチパス伝搬環境における推定特性は単一到来波の伝搬環境の重ね合わせであるので，推定可能条件として単一到来波の伝搬環境において位相を正確に推定できる条件を考える．式(5)より cos Q の値が正になる場合，位相が正確に推定できる．したがって，推定可能条件は以下の式で表すことができる．

$$\frac{2}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N/2-1}\cos(2\pi R(\cos(\gamma_n - \phi) - \cos(\gamma_n - \delta_m))) \geq 0 \qquad (6)$$

ここで，推定可能な観測点数 N と観測円半径 R の関係について焦点を絞るものとする．N と R は推定システムの物理的な大きさや装置数によって限定されるものであるのに対して，仮想パス数 M は計算のプロセス内でのみ用いるものである．また，既に示したように M は大きい程推定能力の向上が得られるので，ある推定システムについての推定可

能条件を論じる場合には，M を理想的(無限大)に設定するのが適切である．この条件のもとで，式(6)左辺は以下のように表すことができる．

$$\begin{aligned}
&\frac{2}{NM}\sum_{m=0}^{M-1}\sum_{n=0}^{N/2-1}\cos(2\pi R(\cos(\gamma_n-\phi)-\cos(\gamma_n-\delta_m)))\\
&=\frac{1}{\pi N}\cdot\frac{2\pi}{M}\sum_{m=0}^{M-1}\sum_{n=0}^{N/2-1}\cos(2\pi R(\cos(\gamma_n-\phi)-\cos(\gamma_n-\frac{2\pi}{M}m)))\\
&=\frac{1}{\pi N}\sum_{n=0}^{N/2-1}\int_{-\pi}^{\pi}\cos(2\pi R(\cos(\gamma_n-\varphi)-\cos(\gamma_n-\delta))d\delta\quad\left(d\delta\equiv\frac{2\pi}{M}\right)\\
&=\frac{1}{\pi N}\sum_{n=0}^{N/2-1}\cos(2\pi R\cos(\gamma_n-\varphi))\int_{-\pi}^{\pi}\cos(2\pi R\cos(\gamma_n-\delta))d\delta\\
&+\frac{1}{\pi N}\sum_{n=0}^{N/2-1}\sin(2\pi R\cos(\gamma_n-\varphi))\int_{-\pi}^{\pi}\sin(2\pi R\cos(\gamma_n-\delta))d\delta\\
&=\frac{1}{\pi N}\int_{-\pi}^{\pi}\cos(2\pi R\cos(\gamma_n-\delta))d\delta\sum_{n=0}^{N/2-1}\cos(2\pi R\cos(\gamma_n-\varphi))\quad(7)
\end{aligned}$$

ここで，式(7)における積分は角度成分γ_nに対してδを全周方向で積分するので，$\delta'=\delta-\gamma_n$と置くと式(8)に示すようにγ_nは無視することができる．

$$\begin{aligned}
\int_{-\pi}^{\pi}\cos(2\pi R\cos(\gamma_n-\delta))d\delta&=\int_{-\pi}^{\pi}\cos(2\pi R\cos(\delta-\gamma_n))d\delta\\
&=\int_{-\pi-\gamma_n}^{\pi-\gamma_n}\cos(2\pi R\cos(\delta'))d\delta'\\
&=\int_{-\pi}^{\pi}\cos(2\pi R\cos(\delta'))d\delta'\quad(8)
\end{aligned}$$

ここで，シュレーフリの積分公式

$$J_m(z)=\frac{1}{\pi}\int_0^{\pi}\cos(m\theta-z\cdot\cos\theta)\cdot d\theta\qquad(9)$$

を用いると，式(6)は最終的に以下の形に変形される．

$$\begin{aligned}
&\frac{1}{\pi N}\int_{-\pi}^{\pi}\cos(2\pi R\cos(\gamma_n-\delta))d\delta\sum_{n=0}^{N/2-1}\cos(2\pi R\cos(\gamma_n-\varphi))\\
&=\frac{2}{\pi N}\int_{0}^{\pi}\cos(2\pi R\cos(\gamma_n-\delta))d\delta\sum_{n=0}^{N/2-1}\cos(2\pi R\cos(\gamma_n-\varphi))\\
&=\frac{2}{N}J_0(2\pi R)\sum_{n=0}^{N/2-1}\cos(2\pi R\cos(\gamma_n-\varphi))\qquad(10)
\end{aligned}$$

つまり，この式の値が推定可否の条件となる．Fig. 15に観測円半径Rの変化に対する式(10)の値の変化を示す．同図の結果から，R=15 波長程度以上になると式(10)の値が 0 以下になる場合があり，その結果として R=15 波長程度以上になると推定不可能になることがわかる．

また，式(10)において観測点数 N を無限大に仮定すると，式(7)-(9)と同様な結果な展開により，最終的に式(6)の左辺は以下となる．

$$\frac{2}{N}J_0(2\pi R)\sum_{n=0}^{N/2-1}\cos(2\pi R\cos(\gamma_n-\varphi))=\left(J_0(2\pi\cdot R)\right)^2\qquad(11)$$

ここで，式(11)は値が常に 0 以上であるので，観測円半径に依存することなく常に推定が可能なことがわかる．このことから観測点数 N を無限大にすると，観測円半径 R をどれだけ大きくしても推定可能となる．ただし，式(11)の値が 0 となる R がありその場合には，推定された信号が無限小にまで小さくなるので，雑音が存在すると推定特性は劣化する．

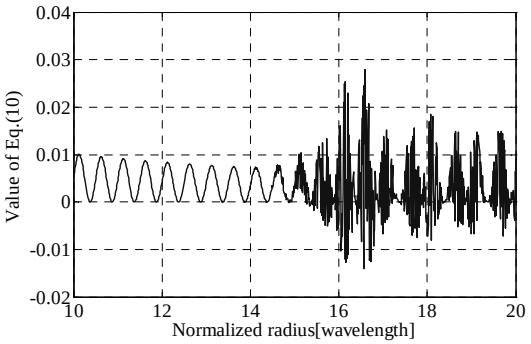


Fig. 15. Value of Eq.(10) when radius of observation circle is changed.

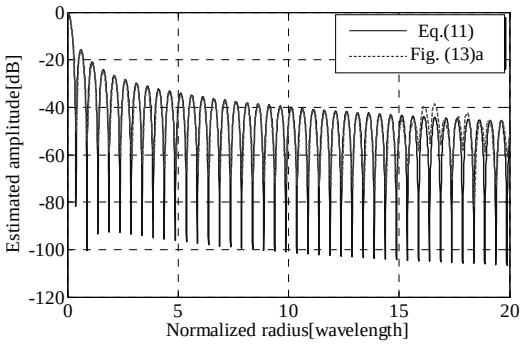


Fig. 16. Comparison of estimated amplitude, theory (Eq. (11)) and simulated (Fig. 13(a)).

式(11)を用いて計算した観測円半径の変化に対する推定振幅を Fig. 16 に示す．R=15 波長程度以下において，式(11)は，シミュレーションから得られた Fig. 13(a)の推定振幅特性に等しい特性を示すことがわかる．つまり，観測円半径の推定可能範囲では，振幅特性は第一種 0 次ベッセル関数の 2 乗に則する振動特性を示すことがわかる．また，この結果から雑音が存在する環境では，Fig. 14 に示す様に推定可

能なパラメータ環境においても相関値が観測円半径の変化に対して振動する.

4.2.3. 分析結果に基づく秘密鍵共有方式の鍵盗聴可能性に関する考察

前節までの分析から, 他地点を対象とした伝搬路特性の推定は理論的に可能であることが明らかとなった. この分析結果を基に 2 章で示した伝搬路特性に基づく秘密鍵共有式の鍵盗聴の可能性について考える. ここで, 伝搬環境は搬送周波数が 2.4GHz の周囲一様の方向からマルチパスが到来するレイリーフェージング環境とする. 例えば, 盗聴相手となる推定対象局から隠れて盗聴することを想定し, 対象局から 10m の半径の観測円半径を考えたとすると, 推定を正確に行うためには, 前節までの分析から, 最低でも 530 点程度の観測点が必要となる. この数の受信を推定対象局の受信信号と完全に時間同期させる必要がある. また, 位相推定精度を劣化させないためには盗聴局と推定対象局の位置関係も 1/10～1/100 波長の精度で既知でなければならない. つまり, 10m 離れた地点との距離を 1.25mm~12.5mm のオーダで正確に得ることが必要となる. このような伝搬路特性の推定は現実的には非常に困難である. 逆に, 時間的な同時受信が現実的に可能な数として例えば観測点数を 10 点とすると, 推定可能な推定対象局との距離は最長でも 18.8cm 程度となる. 盗聴行為は一般に被盗聴側から隠れて行うものであるので, この距離では盗聴行為を行うことは現実的に不可能である.

以上の考察より, 盗聴の観点において観測点数や推定対象との距離を変化させても他地点を対象とした伝搬路特性の推定は現実的に不可能であると結論づけることができる.

5. まとめ

秘密鍵共有方式の安全性検討に資するため, 複数地点での観測点の受信情報を用いて離れた地点の受信点の伝搬路特性を推定する方式について検討し, この手法による推定特性を詳細に分析した.

マルチパス伝搬環境における推定特性の推定メカニズムを明らかにするために, 単一到来波の伝搬環境における推定特性を詳細に分析した. 仮想パスのアジマス角に対する振幅特性と位相特性を分析し, 観測点および仮想パス数等の推定手法のパラメータに関する推定可否の条件を明らかにした. さらに, 観測円半径の増加に伴って推定値の振幅が振動的に変化することから, 雑音が存在する場合の特性についても結果を示した. また, この推定特性の分析結果に基づく, 推定可否の条件を理論式により表した. 最後に, 伝搬路特性に基づく秘密鍵共有式の鍵盗聴の可能性について検討した. 観測点数や推定対象との距離を変化させても, 現実的には他地点を対象とした伝搬路特性の推定は不可能であることを示した.

参考文献

1) 北浦明人, 笹岡秀一, “陸上移動通信における OFDM の伝搬路特性に基づく秘密鍵共有方式,” 信学論(A), vol. J87-A, no. 10, pp. 1320-1328, Oct., 2004.
2) T.Aono, K.Higuchi, T.Ohira, B.Komiyama and H.Sasaoka, “Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels,” IEEE Trans. Antennas & Propagt., vol. 53, no. 11, pp. 3776-3784, Nov. 2005.
3) 岩井誠人, 笹岡秀一, “電波伝搬特性を活用した秘密情報の伝送・共有技術,” 信学論(B), vol. J90-B, no. 9, pp. 770-783, Sep. 2007.
4) 岡本達明, 暗号と情報セキュリティ, 日経 BP 社, 1998.
5) 岡本龍明, 現代暗号, 産業図書株式会社, 1997.
6) K.Inoue, H.Iwai, and, H.Sasaoka, “Estimation of fading characteristics based on multiple observed signals at different locations,” Proc.2008 International Symposium on Antennas and Propagation (ISAP2008), TP-A05, Oct. 2008.
7) 井上恵輔, 丹後俊宏, 岩井誠人, 笹岡秀一, “他地点観測信号に基づく伝搬路特性推定の特性解析,”信学技報, AP2007-74, Sep. 2007.
8) 井口聖, 川口則幸, “超長基線干渉計(VLBI)における最適フィルタリング,” 信学論(B), Vol.J82-B, No.3, pp. 420-426, Mar, 1999.
9) W.C.Jakes, “Microwave Mobile Communications,” Wiley-IEEE Press, 1994.