Vol.2012-DPS-152 No.13
Vol.2012-GN-85 No.13
Vol.2012-EIP-57 No.13
2012/9/13

秘密分散法に基づくセキュアな無線通信リンクの形成 -狭ビーム形成の効果とその弊害-

山中 仁昭[1,a)]　宮本 伸一[2,b)]　三瓶 政一[2,c)]

概要：著者らは，プライベートな無線ネットワークにおいて第三者への情報漏洩の危険性を軽減する手法として，送信ノードから受信ノードへ至る複数のパスを選択した後，秘密分散法の考えに基づき，これらのパスへ情報を分散して伝送する手法を提案してきた．提案方式では，送信ノードにアレーアンテナを搭載することを前提に，選択したパスに対して個別に鋭い指向性（狭ビーム）を形成し，これらの指向性を時間的に切り替えることにより送受信ノード間における分散伝送を実現する．本報告では，アレーアンテナのアンテナ本数を増大させ狭ビームを形成することの効果とその弊害について明らかにする．狭ビームを形成することにより，情報を無線空間内で大きく分散して伝送することができるため，情報の秘匿性を向上することができると考えられる．その一方で狭ビームを形成することにより，送受信ノード間の伝搬利得が減少するため，送信電力が増大する等の電力面における弊害が生じることが懸念される．本報告では，著者らがこれまでに提案してきた指向性制御法を対象に，このような狭ビーム形成の効果とその弊害について計算機シミュレーションによる評価に基づき検証する．

A Study on Secure Wireless Links Based on Distributed Transmission Using a Secret Sharing Method -Positive and Negative Effects of Narrow Beam Creation-

Masaaki Yamanaka[1,a)]　Shinichi Miyamoto[2,b)]　Seiichi Sampei[2,c)]

Abstract: The authors have proposed a secure wireless link creation scheme based on a distributed transmission by providing a plural number of separated propagation routes to a destination. In the proposed scheme, the transmitted information is divided into a plural number of "shared information" by a secret sharing method and sent to the destination separately through the different propagation routes with individually controlled antenna directivities. In this article the positive and negative effects of narrow beam creation at the transmitter will be discussed. By creating a narrow beam at the transmitter, as a positive effect, each shared piece of information will be transmitted to a limited area around each selected path which will improve the secrecy of the original information. On the other side, as a negative effect, the transmitted power of each shared signal will be increased. Both effects are evaluated quantitatively and discussed based on a computer simulation.

1. はじめに

ユーザ周辺の情報伝達を支える通信ネットワークとして無線 LAN 等に代表されるプライベートな無線ネットワークが広く普及している．これまでこのようなプライベートな無線ネットワークは家庭やオフィス等，主に特定の人物が出入りするプライベートな場所で用いられることが一般的であった．しかしながら，近年，駅の構内やビル・空港のロビーなど，不特定の第三者が自由に出入りする公共性の高い場所においても，無線ネットワークの特徴である，配線が不要であり，容易にかつ柔軟に通信エリアを形成で

[1] 広島国際大学工学部情報通信学科
広島県呉市広古新開 5-1-1，737–0112.
[2] 大阪大学大学院工学研究科電気電子情報工学専攻
大阪府吹田市山田丘 2-1，565–0871.
[a)] m-yamana@it.hirokoku-u.ac.jp
[b)] miyamoto@comm.eng.osaka-u.ac.jp
[c)] sampei@comm.eng.osaka-u.ac.jp

Vol.2012-DPS-152 No.13
Vol.2012-GN-85 No.13
Vol.2012-EIP-57 No.13
2012/9/13

きる点を理由に積極的に導入が進められている．

無線 LAN 等の無線ネットワークではマイクロ波帯の電波を使用するため，複雑で遮蔽の多い環境においても，電波が反射や回折を繰り返して伝搬する特徴を利用して，安定した通信リンクを形成することが可能である．一方で，不特定の第三者が自由に出入りするような空間では，第三者によって信号が傍受されやすく，通信内容を盗聴される危険性を含むことになる [1]．

従来，無線通信では送信情報の秘匿性を確保するために，送信信号を暗号化して伝送する手法が広く用いられてきた．送信信号を暗号化して伝送することにより，たとえ無線信号が傍受され，正しく復調されたとしても，暗号鍵を秘密にしておくことで送信情報の秘匿性を保つことができる．しかしながら，このような暗号化に基づく手法では，鍵の管理手法によってその秘匿性が大きく左右される [2]．特に，プライベートな無線ネットワークでは各ノードでの自律分散制御が基本となることから暗号鍵の管理が難しく，複雑な鍵配送の手続きなしには鍵の秘匿性が大きく低下することが知られている．また，近年，個人が所有する PC 等の処理速度が高速化し，正しく鍵配送を行ったとしても，鍵の候補を総当たりに確認することにより，時間の経過と伴に鍵の秘匿性が低下し，暗号が解読される危険性が指摘されている．今後，公共性の高い場所においても，利用勝手がよく，かつ安心して利用できる無線ネットワークを構築するためには，このようなセキュリティ上の課題を克服する必要がある．

著者らは，これまで，送信情報を無線空間内において分散して伝送することにより，送信情報が第三者へ漏洩する危険性を軽減する方式について提案してきた [3][4]．提案法では，無線伝搬路のマルチパス性に着目し，まず，秘密分散法に基づいて元情報をそれ単独では意味をなさない情報へ分散する．続いて，送信ノードから受信ノードへ至る幾つかのパスを選択した後，送信ノードのアンテナ指向性を制御し，選択したパスへ情報を空間的に分散して伝送することにより，第三者への情報漏洩を抑制する．秘密分散法は情報理論の分野で研究が盛んに進められている情報の分散管理手法の一つで，(k,n) 閾値法とも呼ばれる [5]．元情報を n 個の情報に分散して管理し，これら n 個の分散情報のうち k 個以上あれば，元情報を誤りなく復元することができるが，k 個未満であれば，元情報に関する情報を一切得ることができない特徴を有する．特に $n = k$ の場合を満場一致型の秘密分散法と呼び [6]，この場合はすべての分散情報がなければ元情報を復元することができない．このような満場一致型の秘密分散法を適用し，送信情報を無線空間内で分散して伝送することにより，盗聴を試みる第三者はすべての分散情報を集めない限り元情報を復元することができないため，送信者は第三者への情報漏洩を抑制することができる．

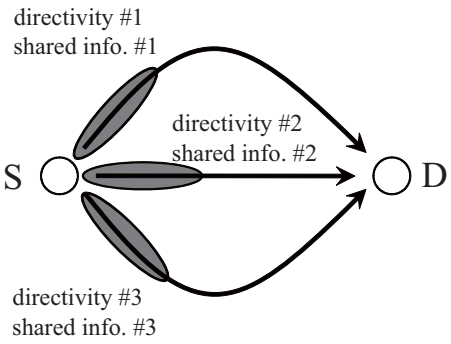


図 1 提案法による情報伝達の流れ
Fig. 1 Information flow of the proposed method

アンテナの指向性は情報を空間的に分散して伝送する上で重要な要素である．著者らは，これまで，アンテナ指向性制御法として送信ノードにアレーアンテナを搭載することを前提に，選択した伝搬パスの放射方向を推定し，その方向に対して鋭い指向性を形成する指向性制御法を提案してきた．提案法では方向拘束付き出力最小化（DCMP：Directional Constrained Minimization of Power）基準に基づき，選択したパスの放射方向に対する拘束条件の下，アンテナ出力を最小とするアンテナウエイトを求めることで，目標とする方向に対してのみ利得を有する鋭い指向性を形成する．本報告ではこのような特定の方向のみに鋭い利得を有する指向性を「狭ビーム」と定義し，ビーム幅を狭める狭ビーム化が送信情報の秘匿性に与える効果とそれによる弊害について検証する．

アンテナのビーム幅を狭くすることで選択したパスへ電力を集中して信号を送信することができるため，信号が伝搬する領域をパスに沿った狭い範囲に制限し，無線空間内での信号の空間的な分散性を高めることができる．そのため，狭ビーム化により送信情報の秘匿性は向上すると考えられる．一方で，このような狭ビーム化による弊害として，送受信ノード間の伝搬利得は減少するため，送信情報を誤りなく受信ノードへ伝達するには送信電力を増大することが必要となる．本報告では，このような狭ビーム化による秘匿性向上の効果と送信電力への影響について，計算機シミュレーションによる評価に基づき検証する．

本報告の構成は以下の通りである．まず，2 章にて秘密分散法を用いたセキュアな無線リンク形成法について述べる．また，3 章にてアレーアンテナの構成を説明し，本報告で対象とする狭ビーム形成法について述べる．続いて，4 章にて，狭ビーム化が送信情報の秘匿性に与える効果と送信電力特性へ与える弊害について検証する．最後に，5 章にてまとめる．

Vol.2012-DPS-152 No.13
Vol.2012-GN-85 No.13
Vol.2012-EIP-57 No.13
2012/9/13

2. 秘密分散法を用いた情報分散伝送による セキュアな無線リンクの形成法

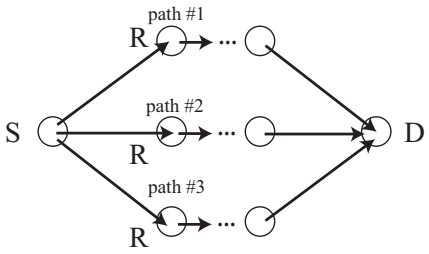
2.1 提案法の概要

情報理論的な観点から情報伝達のメカニズムを見直すと，送信情報を復元するために十分な情報量を与えなければ，一部の情報が漏洩したとしても元情報の伝達を抑制することができる．このような情報伝達の管理手法として秘密分散法に基づく手法がある [5]．秘密分散法とは元情報をそれ単独では意味を持たない情報に分散した後，そのうち定められた個数以上の分散情報があれば元情報を復元することができるが，分散情報の個数がそのような数に満たなければ元情報を一切復元することができないという情報の管理手法である．特に，すべての分散情報がなければ元情報を復元することができない手法を満場一致法と呼ぶ [6]．

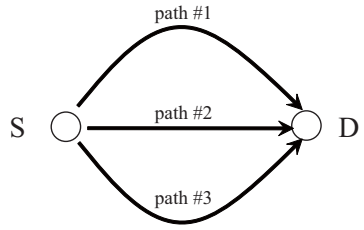
著者らは，このような満場一致型の秘密分散法に基づいて元情報を分散した後，無線伝搬路が固有に有するマルチパス性を利用し，分散情報を重なりの小さいパスに振り分けて伝送することにより，伝搬途中における情報漏洩の危険性を軽減する手法について提案してきた．提案法では，まず，送受信ノード間において情報を伝送するパスを有効パスとして選択し，選択した有効パスと同数の分散情報を生成する．続いて，それぞれの有効パスの放射方向を中心とした狭ビームを形成し，これらの狭ビームを時間的に切り替えながら，分散情報を異なる方向／タイミングで送信する．このとき，秘密分散法に基づいて送信情報を生成することにより，送信情報全体の情報量は増大するため，伝送効率は低下するが，このような伝送効率の低下と引き換えに，伝送中の情報漏洩の危険性を軽減することができる [7]．

図 1 は，一例として，送信ノード（Source node：S）－受信ノード（Destination node：D）間において 3 つの有効パスを選択し，送信情報をこれらのパスに分散して伝送する様子を示している．図 1 に示すように，情報を複数のパスへ分散させて伝送することにより，周囲に盗聴を試みる第三者ノードが存在したとしても，このようなノードがすべての分散情報を獲得することを防ぎ，元情報が漏洩する危険性を軽減できる．

なお，通常，無線空間内においてパスは複雑に重なり合うため，図 1 に示すように無線空間全体において信号の伝送路を完全に離すことは不可能である．しかしながら，指向性アンテナを用いることにより，無線信号の電力をターゲットとするパスに集中させ，無線空間内で得られる信号電力に空間的な偏りを生じさせることができる．このとき，無線信号を復調するには一定の電力が必要となること，また，そのような電力に満たない場合は無線信号を正しく復調することができず，正しく情報を伝達することができないことを考慮すると，図 1 に示すような動作により，分散



(a) multipath routing in ad-hoc network (previous work)



(b) distributed transmission in wireless space (proposed)

図 2 提案法と従来手法との分散伝送の違い
Fig. 2 Difference between our proposal and the previous work

情報が伝達される空間的な領域（エリア）に信号電力と同様の空間的な偏りを生じさせることができ，すべての分散情報が伝達されるエリアを小さく限定することができる．提案法では，このような考えに基づき，予め送信情報を満場一致型の秘密分散法にて分散しておき，生成した分散情報を異なるアンテナ指向性に振り分けて伝送することにより，元情報が伝達されるエリアを無線空間内において小さく限定し，送受信ノード間の広い範囲に対して情報漏洩の危険性を軽減する．

2.2 従来研究

秘密分散法を通信へ適用し，送信情報の秘匿性を向上する研究は既に行われている．これまでは主に，複数のノードが同一無線空間内に存在し，ノード間の通信路がメッシュ状に構築されるアドホックな無線ネットワークを対象として検討が進められてきた [8]-[10]．通常，アドホックな無線ネットワークでは，携帯電話システムに代表されるのセルラーネットワークとは異なり，バックボーンとなる有線ネットワークがないため，距離的に離れたノード同士が通信を行うためには，ネットワーク内の他のノードを中継するマルチホップ通信を行う必要がある．このとき，送信ノードから受信ノードへ至るマルチホップな通信路は中継ノードの選び方によって複数の通信路が考えられるため，これらの通信路へ送信情報を分散して伝送することにより，無線ネットワーク内での秘匿性を高めることができる．このような考えは Multi-path Routing 法として提案され [8]，分散情報のルーティング手法の検討や [9]，指向性アンテナを用いた検討等 [10] が行われている．

これに対し，本報告で述べる手法は，送信ノードから受信ノードまでのシングルホップな伝送を対象とし，無線伝

Vol.2012-DPS-152 No.13
Vol.2012-GN-85 No.13
Vol.2012-EIP-57 No.13
2012/9/13

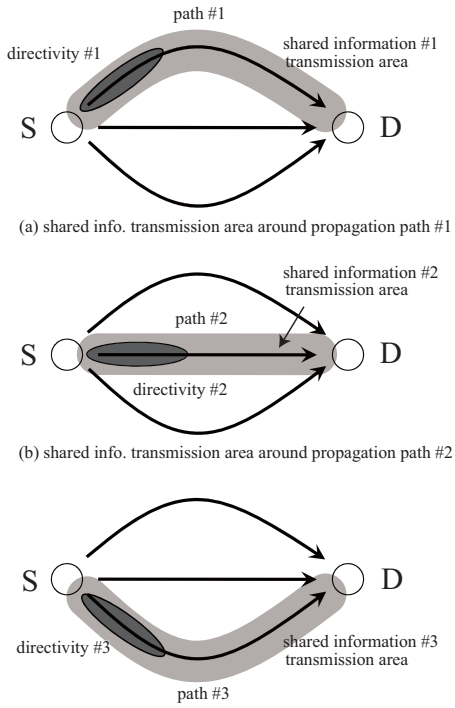


図 3 分散情報が伝達されるエリアの空間的な偏り
Fig. 3 Spatial distribution of the shared information transmission area

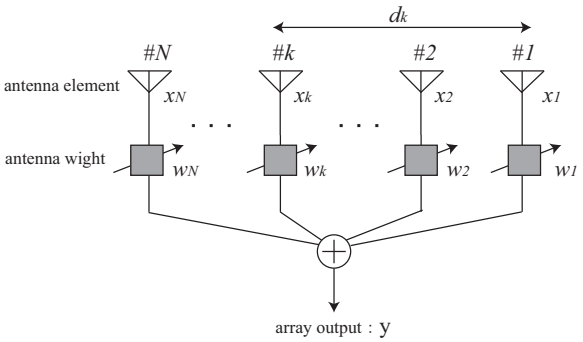


図 4 アレーアンテナの受信動作
Fig. 4 Receiving behavior of adaptive array

送路が固有に有するマルチパス性を利用して分散伝送することにより，送受信ノード周囲の無線空間内で送信情報の秘匿性を向上することを目的としている．図 2 に従来のアドホックな無線ネットワークを対象とした分散伝送と本報告で対象とする分散伝送との違いを示す．上記のようなアドホックな無線ネットワーク環境を対象とした場合には，図 2（a）に示すように中継ノード（Relay node：R）を含めて分散伝送を行うことで大規模な無線ネットワークにおいても送信情報の秘匿性を保つことができる．一方，本報告で対象とする分散伝送では，図 2（b）に示すように無線伝送路が固有に有するマルチパス性を利用して分散伝送を行うことで，プライベートな環境等，必ずしも中継ノードが存在しない状況においても適用することが可能である．

3. 狭ビーム形成法

アンテナ指向性は提案法における送信情報の秘匿性を左右する重要な要素となる．本節では，まず，アンテナ指向性が送信情報の秘匿性に与える影響について述べる．続いて，送信ノードへアレーアンテナを搭載することを前提に，本報告で対象とするアレーアンテナを用いた狭ビームの形成手法について説明する．

3.1 アンテナ指向性が送信情報の秘匿性へ与える影響

提案法では送信ノードにおいてビーム幅の小さい狭ビームを形成し，分散情報が伝達されるエリアに空間的な偏りを生じさせることで，すべての分散情報が伝達されるエリアを小さく限定し，伝搬途中における情報漏洩の危険性を軽減する．図 3 に狭ビームを形成することにより，分散情報が伝達されるエリア間に空間的な偏りが生じる様子を示す．通常，無線信号を正しく復調するためには，受信感度以上の信号レベルが必要となる．そのため，狭ビームを形成し，有効パスの放射方向へ電力を集中して伝送することにより，分散情報が伝達されるエリアを各有効パスを中心に制限することができる．このとき，アンテナのビーム幅はパスの周囲に形成される信号の伝搬領域の広がりに大きく影響し，ビーム幅が大きいほど分散情報が伝達されるエリアは広くなる．個々の分散情報が伝達されるエリアが広がることにより，元情報が伝達されるエリアも広がるため，アンテナのビーム幅は送信情報の秘匿性へ大きく影響する．すなわち，アンテナのビーム幅が小さいほど，元情報が漏洩するエリアを小さく制限することができ，逆に，ビーム幅が大きくなるほど，元情報が漏洩する危険性が増すことになる．つまり，狭ビーム化を図ることにより，元情報が漏洩するエリアを小さく制限でき，情報の秘匿性を向上することができる．

3.2 アレーアンテナ

アレーアンテナは複数のアンテナ素子から構成され，各素子のアンテナウエイトを制御することによりその指向性を制御することのできる，適応制御型の指向性アンテナである．図 4 にアレーアンテナを用いた受信動作を示し，受信信号の式表現を用いてアレーアンテナの指向性制御の原理について述べる．なお，提案法では，送信時に指向性制御を行うため，提案法における信号の流れは図 4 に示すそれとは逆の流れになる．しかしながら，図 4 に示す受信動作と全く同じ原理で送信時のアンテナ指向性を制御することができる．

アレーアンテナの k 番目のアンテナ素子における受信信号を x_k，アンテナウエイトを w_k とするとアレー出力 y は次式で表わされる．ただし，N はアンテナ素子数である．

Vol.2012-DPS-152 No.13
Vol.2012-GN-85 No.13
Vol.2012-EIP-57 No.13
2012/9/13

$$y = \sum_{k=1}^{N} x_k w_k \tag{1}$$

ここで，受信信号がアンテナ素子間距離（d_k）に対して十分に狭帯域であり，Δf を受信信号の帯域幅，c を光速として，$2\pi\Delta f \frac{d_k}{c} \ll 1$ が成り立つと仮定すると，k 番目のアンテナ素子における受信信号は 1 番目のアンテナ素子を基準素子として式（2）のように表わされる．ただし，$v_k(\cdot)$ は基準素子に対する受信位相の変動量を表す項目であり，アレー応答と呼ばれる．なお，θ は電波の到来方向であり，アレー応答は θ の関数となる．

$$x_k = x_1 v_k(\theta) \tag{2}$$

式（1）は式（2）を用いて以下のように変形できる．

$$\begin{aligned} y &= \sum_{k=1}^{N} x_1 v_k(\theta) w_k \\ &= x_1 \sum_{k=1}^{N} v_k(\theta) w_k \\ &= x_1 D(\theta) \end{aligned} \tag{3}$$

ただし，

$$D(\theta) = \sum_{k=1}^{N} v_k(\theta) w_k \tag{4}$$

$D(\theta)$ はアンテナ伝達関数と呼ばれ，その絶対量（$|D(\theta)|$）は電波の到来方向（θ）に対するアンテナ利得を示す．つまり $|D(\theta)|$ はアンテナ指向性を表す．ここで，アレー応答（$v_k(\theta)$）はアンテナ素子配置の形状によって定まる関数であることに注意すると，式（4）より，アレーアンテナの指向性はアンテナウエイトによって一意に定まることが分かる．

著者らは，所望方向へのアンテナ利得を制御することのできるアンテナウエイト制御法として，方向拘束付出力電力最小化法（Directionally Constrained Minimization of Power 法：DCMP 法）に着目し，DCMP 法を基本として所望方向に対して利得を向けつつ，他の方向に対して利得を大幅に抑制することで，狭ビームを形成する手法について提案してきた．続いて，DCMP 法に基づくアンテナウエイト制御法について述べ，DCMP 法を基本とした狭ビーム形成法について説明する．

3.2.1 DCMP 法に基づくアンテナウエイト制御法

ある特定の一方向を所望方向とし，その方向に対して利得を向け，他の方向への放射を抑圧するアンテナウエイト制御は，単一方向拘束の DCMP 法に相当する．単一方向拘束の DCMP 法に基づくアンテナウエイト $\mathbf{W}$ は，以下の条件付き最小化問題を解くことにより求めることができる [11]．

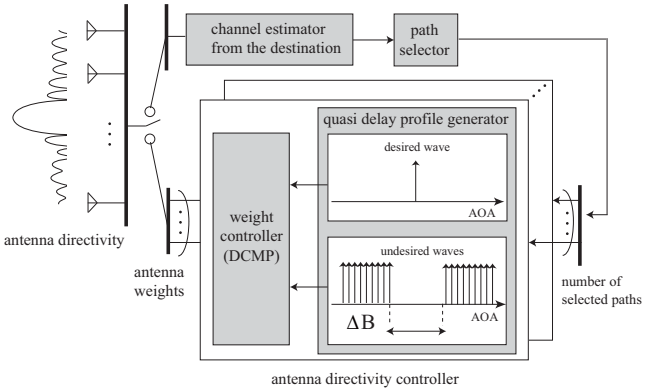


図 5 送信指向性制御手順

Fig. 5 Block diagram of the antenna directivity control procedure

$$\begin{aligned} &\underset{\mathbf{W}}{min} \left(P_{out} = \frac{1}{2} \mathbf{W}^H \mathbf{R}_{xx} \mathbf{W} \right) \\ &\text{subject to } C\mathbf{W}^* = \mathbf{H} \end{aligned} \tag{5}$$

ただし，$\mathbf{R}_{xx}$ はアレーアンテナを構成するアンテナ素子間の相関行列である．また，C は拘束応答値，$\mathbf{H}$ は拘束方向に対するアレー応答ベクトルである．$(\cdot)^*$ は複素共役を表す．

ここで，式（5）で示される最小化問題は Lagrange の未定係数法を用いて解くことができ，最適アンテナウエイト $\mathbf{W_{opt}}$ は次式で与えられる．

$$\begin{aligned} \mathbf{W_{opt}} &= \gamma \mathbf{R}_{xx}^{-1} C \\ \gamma &= \frac{\mathbf{H}^*}{C^* \mathbf{R}_{xx}^{-1} C} \end{aligned} \tag{6}$$

3.2.2 狭ビーム形成法

DCMP 法をアンテナウエイト制御法に用いたアレーアンテナでは，拘束方向に対する拘束条件の下，アレーの出力電力を最小化するようウエイト制御が行われ，不要波成分が抑圧される．著者らはこの特徴を利用し，ウエイト制御上仮想的に，ターゲットとする有効パスの放射方向に対して擬似的な所望波を，それ以外の方向に対して擬似的な干渉波を生成し，ターゲットとする有効パスの放射方向に対して狭ビームを形成する手法について提案してきた．ただし，提案法ではネットワーク内のすべてのノードが同一周波数帯を共有して使用し，ノード間の送受信リンクにおいて伝搬特性に可逆性が成り立つことを前提とした．このような前提の下，ターゲットとする有効パスの放射方向は直前の受信リンクにて到来方向として推定することを想定した．

図 5 に指向性制御の手順を示す．まず，アンテナから接続されるスイッチを上側に切り替え，チャネル推定部（channel estimator）において伝搬路推定を行う．続いて，パス選択部（path selector）において，得られた遅延プロファイルを基に有効パスを選択する．その後，指向性制御

Vol.2012-DPS-152 No.13
Vol.2012-GN-85 No.13
Vol.2012-EIP-57 No.13
2012/9/13

表 1 計算機シミュレーション諸元
Table 1 Simulation parameters

carrier frequency	5GHz
array configuration	circular
antenna element separation	half wavelength

表 2 アンテナ素子数とビーム幅の関係
Table 2 Reraltionship between the number of antenna elements and the beam width

Num. of elements	4	8	16	32	48	64
Beam width（deg.）	70.9	43.5	14.8	9.7	9.6	10.5

部（antenna directivity controller）において，有効パス毎にパスの到来方向に対して擬似的な所望波（quasi-desired wave：擬似所望波）を，それ以外の方向に擬似的な干渉波（quasi-undesired wave：擬似干渉波）を生成し，DCMP 法に基づいて送信ウエイトを算出する．

ここで，図 5 において，ΔB は擬似所望波を中心とした擬似干渉波を生成しない空白の角度幅であり，形成される狭ビームのビーム幅の目安となる．ΔB が大きいほど幅の広いビームが形成され，逆に ΔB が小さいほど幅の狭いビームが形成される．本報告では ΔB を調整することにより狭ビーム化を図り，狭ビーム化による送信情報秘匿化の効果と送信電力増大への影響について検証する．

3.2.3 アンテナ指向性特性

アレーアンテナでは任意に幅の狭いビームを形成することはできず，ビーム幅はアンテナ素子数に大きく依存する．アンテナ素子数が多いほど広い角度に対してアンテナ利得を抑圧し，より幅の小さい狭ビームな指向性を形成することができる．アンテナ素子数と調整可能な最小のビーム幅の関係を明らかにするために計算機シミュレーションにより評価を行った．表 1 にシミュレーション諸元を示し，表 2 にアンテナ素子数とビーム幅の関係を示す．ただし，ビーム幅（ΔW）は，アンテナ指向性の角度広がりの標準偏差として，次式にて定義した．

$$\Delta W = \sqrt{\int_0^{360} (\theta - \theta_{target})^2 |D_{norm}(\theta)| d\theta} \qquad (7)$$

$$D_{norm}(\theta) = \frac{D(\theta)}{\int_0^{360} D(\theta) d\theta} \qquad (8)$$

ただし，$\theta_{tareget}$ は有効パスの放射方向である．

4. 秘匿性向上の効果と電力面における弊害

アンテナ素子数を増大し狭ビーム化を図ることで，選択した有効パスへ電力を集中して信号を送信することができるため，分散信号が伝達されるエリアをパスに沿った狭い領域に制限し，すべての分散信号が得られる領域を狭く限定することができる．そのため，狭ビーム化により送信情報の秘匿性は向上すると考えられる．一方でこのような狭ビーム化による弊害として，送受信ノード間の伝搬利得は減少するため，送信情報を正しく受信ノードへ伝達するためには信号電力を増幅する必要がある．本節では，このような狭ビーム化による秘匿性向上の効果と送信電力増大の影響について計算機シミュレーションに基づき検証する．

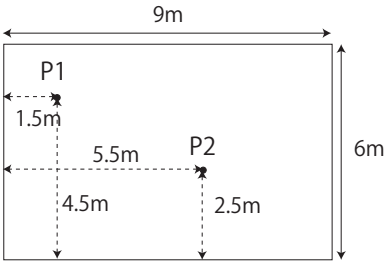


図 6 伝搬路モデル
Fig. 6 Propagation model

表 3 有効パスの伝搬利得と放射角度
Table 3 Propagation gain and angle of departure of effective path detected between source and destination nodes

Path number	1	2	3	4	5	6
Gain（dB）	0	-9.4	-11.1	-11.3	-17.6	-19.2
AOD（deg）	330.3	55.0	299.1	197.1	227.1	23.5

4.1 伝搬路モデル

図 6 に本検討で用いた伝搬路モデルを示す．本検討では，図 6 に示すような長方形の室内環境を想定し，伝搬エリア内の伝搬路は壁面での 2 回反射を考慮したレイトレース法に基いてモデル化した．レイトレース法に基づいてモデル化することにより，パスがモデル内を伝搬する経路を正確に求めることができる [12]．表 3 にレイトレース法に基づいて算出した，送受信ノード間における有効パスの特性を示す．ただし，表中の伝搬利得（Gain）は第 1 パスを基準とした正規化伝搬利得，放射角（Angle of departure：AOD）はアレーアンテナのブロードサイド方向を基準とした水平面内の方位角である．

本検討では，このような伝搬路モデルを使用し，図 6 に示す P1 地点，P2 地点にそれぞれ送信ノード，受信ノードを配置した．その上で，送信ノードから受信ノードへ IEEE802.11a 無線 LAN の伝送パラメータ [13] に基づき，規定された最小の伝送レートにて情報を分散して伝送することを想定した．

4.2 評価方法

一般に無線通信では，送信信号を復調するためには受信感度以上の受信電力が必要である．本検討では，このような受信感度レベルを基準に，受信感度レベルよりも 3dB 低いレベルを復調可能な閾値レベルとして，送信情報が漏洩する可能性を判断する．具体的には，閾値レベルを超えるエリアを「復調可能エリア」と定義し，そのようなエリア

Vol.2012-DPS-152 No.13
Vol.2012-GN-85 No.13
Vol.2012-EIP-57 No.13
2012/9/13

を分散情報が正しく伝達されるエリアとして，元情報が漏洩するエリアを評価する．

なお，信号電力や信号の変調方式等の伝送パラメータは，IEEE802.11a 無線 LAN の標準規格に基づいて設定した．IEEE802.11a 無線 LAN の受信感度は −82dBm であることから復調可能な閾値レベルは −85dBm となる．

4.3 秘匿性向上の効果

図 7 に有効パス ♯2（伝搬利得：−9.4 dB，放射角：55.0 deg）を対象に，アンテナ素子数をパラメータとしてその周囲に形成される復調可能エリアの空間的な分布特性を示す．図中の白いエリアが復調可能エリアを示している．図 7 より，アンテナ本数の増大と伴に，復調可能エリアが狭く制限されていることが分かる．これは，アンテナ素子数を増大することにより，狭ビーム化が図られ，無線信号の電力をパスに沿った狭い領域に集中して受信ノードへ伝送することが出来ているためである．このように分散情報が伝達されるエリアを狭く制限できれば，元情報が漏洩するエリアを狭く制限することができる．すなわち，狭ビーム化を図ることで元情報の秘匿性を向上することができる．

一例として，図 8 にアンテナ素子数を 48 本とした場合の各分散信号の復調可能エリアを示し，これら復調可能エリアより算出される元情報が漏洩するエリアを図 9 に示す．ただし，図 8 においてパス ♯1〜♯6 は表 3 の 6 本のパスを示しており，図 9 に示す結果は，これら 6 本のパスへ送信情報を分散して伝送した結果である．図 9 より，元情報が漏洩するエリアを受信ノードの周囲に限定し，漏洩の危険性を大きく低減できていることが分かる．

表 4 に，このような元情報が漏洩するエリアが伝搬路モデル全エリア内に占める割合をアンテナ素子数をパラメータにして示す．表 4 より，アンテナ素子数を増大するに従って，元情報が漏洩するエリアは縮小し，送信情報の秘匿性が向上していることが分かる．

4.4 電力面における弊害

狭ビーム化を図ることにより，送信情報の秘匿性は向上する．しかしながら，送受信ノード間の伝搬利得は減少するため，送信電力が増大する弊害が生じる．また特に，提案法では，DCMP 法に基づき有効パスの放射方向に対してアンテナ利得を形成しつつも，余った自由度を他方向の干渉抑圧に積極的に活用する指向性制御を行っているため，アンテナ素子数の増大による自由度の増加がアンテナ利得の増幅に寄与しない．このため，伝送品質の向上を目的としてアンテナ素子数を増大した場合と比較すると著しく受信ノードへの電力効率が劣化する．

図 10 にアンテナ素子数に対する送信電力の変化を示す．比較対象として，受信ノードへの伝送品質の向上を目的として MMSE（Minimum Mean Square Error）基準に基づく指向性制御法を用いた特性を合わせて示す．ただし，比較する都合上，両手法での送信電力は受信ノードでの受信電力が IEEE802.11a 無線 LAN の受信感度（−82dBm）となるよう設定した．

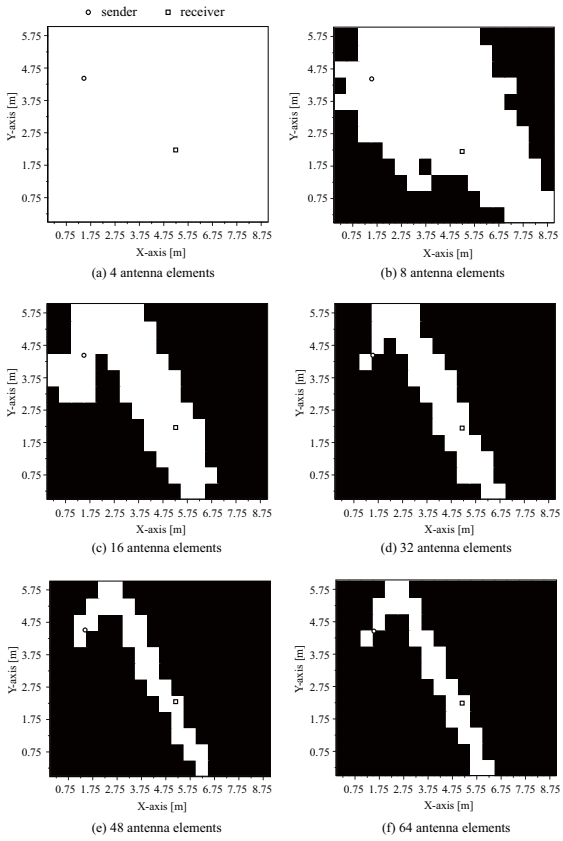


図 7 アンテナ素子数の変化に伴う復調可能エリアの変化
Fig. 7 Spatial distribution change of the area where the transmitted signals can be well received and demodulated

表 4 元情報漏洩エリアが全評価エリアに占める割合
Table 4 Spatial ratio of information leaked area

Num. of elements	4	8	16	32	48	64
Spatial ratio（%）	22.2	17.6	17.6	3.7	1.4	0.9

図 10 より，アンテナ素子数を増大するに従って送信電力は約 3dB 増大することを確認した．また，アンテナ素子数が 16 素子を超えると送信電力の増大は見られないものの，MMSE 基準を用いた特性と比較すると，送信電力の差はアンテナ素子数の増大と伴に広がっており，アンテナ素子数が 32 本の場合で比較すると約 10dB 以上大きな送信電力が必要となることを確認した．

5. おわりに

本報告では，著者らがこれまでに提案してきた秘密分散法に基づくセキュアな無線リンクの形成手法において，狭ビームを形成することによる送信情報秘匿化の効果と送信電力面における弊害について検証した．狭ビームを形成し，送信情報を無線空間内にて分散して伝送することにより，

Vol.2012-DPS-152 No.13
Vol.2012-GN-85 No.13
Vol.2012-EIP-57 No.13
2012/9/13

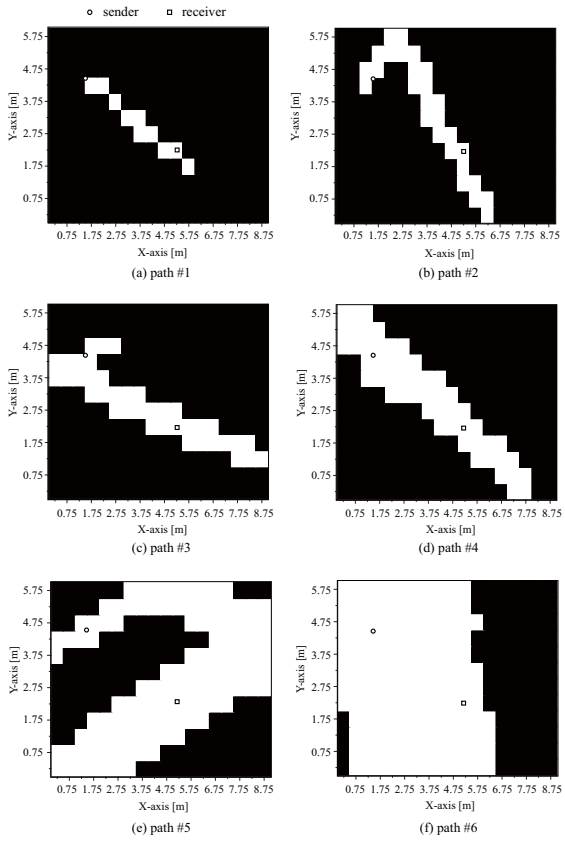


図 8 復調可能エリアの分布

Fig. 8 Spatial distribution of the area where the transmitted signals can be well received and demodulated

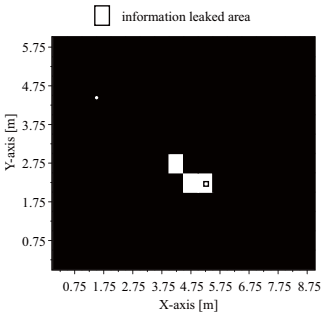


図 9 元情報漏洩エリア

Fig. 9 Information leaked area

送信情報が周囲へ漏洩する危険性を大幅に軽減することが可能である．その一方で，狭ビーム化により送受信ノード間の伝搬利得が減少するため，送信電力を増大する必要がある．

本報告では，このような秘匿化の効果と電力面における弊害をを定量的に検証するために，著者らがこれまでに提案を行ってきたアレーアンテナを用いた狭ビーム形成法を評価対象として，計算機シミュレーションに基づく評価を行った．その結果，アンテナ素子数を最大 64 素子まで増大することにより，送信情報の伝達エリアを受信ノードのごく周辺に限定することができ，伝搬途中における情報漏洩の危険性を大幅に低減できることを確認した．その一方で，アンテナ素子数を増大することにより送信電力は最大約 3dB 増大することを確認した．また，MMSE 基準に基づく指向性制御法等のように受信ノードへの受信品質の向上を目的とした指向性制御法と比較すると大幅に電力効率が劣化し，アンテナ素子数が 32 本の場合に約 10dB 以上の送信電力が必要となることを確認した．

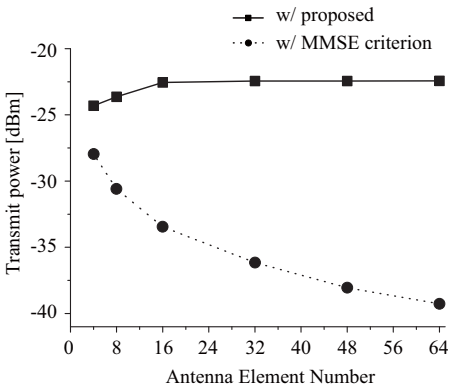


図 10 アンテナ素子数の増大に対する送信電力の変化

Fig. 10 Transmit power change against the number of antenna elements

参考文献

[1] J. Edney, W. Arbaugh（加藤聰彦監訳）, 無線 LAN セキュリティ ー次世代技術 IEEE802.11i と WPA の実際ー, 共立出版，2006.

[2] H. Yang, F. Ricciato, S. Lu, L. Zhang, “Securing a Wireless World, ” Proceedings of the IEEE, Vol. 94, No. 2, pp. 442-454 , Feb. 2006.

[3] 山中仁昭，宮本伸一，三瓶政一，森永規彦，“秘密分散法に基づくセキュアな無線通信リンクの形成に関する一検討，” 信学ソ大会，B-5-127, Sept. 2010.

[4] M. Yamanaka, et al., “A Study on a Transmit Antenna Directivity Conrol of Adaptive Array for Secure Wireless Transmission Based on the Multi-Path Routing,” in Proc. of IEEE VTC-Spring 2012, May 2012.

[5] A. Shamir, “How to Share a Secret,” Communications of the ACM, Vol. 22, No. 11, pp. 612-613, Nov. 1979.

[6] 尾形わかは，黒沢馨，“秘密分散共有法とその応用，” 信学誌，Vol. 82, No. 12, pp. 1228-1236, Dec. 1999.

[7] E. Karnin, J. Greene, M. Hellman, “On Secret Sharing Systems, ” IEEE Trans. on Info., Vol. 29, No. 1, pp. 35-41, Jan. 1983.

[8] L. Zhou, Z. J. Hass, “Securing Ad Hoc Networks,” IEEE Network, Vol. 13, No. 6, pp. 24-30, Aug. 2002.

[9] W. Lou, Y. Fang, “A Multipath Approach for Secure Data Delivery, ” in Proc. of MILCOM 2001, Aug. 2001.

[10] V. Berman, B. Mukherjee, “Data Security in MANETs using Multipath Routing and Directional Transmission, ” in Proc. of IEEE ICC 2006, Jun. 2006.

[11] 菊間信良，アレーアンテナによる適応信号処理，科学技術出版，1999.

[12] 今井哲朗．犬飼裕一郎，藤井輝也，“レイトレースを用いた屋内エリア推定システム，” 信学論，Vol. J83-B, No. 11, pp. 1565-1576, Nov. 2000.

[13] IEEE Std 802.11-2007, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” IEEE Std, 2007.