情報処理学会論文誌 Vol.54 No.12 2440–2450 (Dec. 2013)

推薦論文

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] 三瓶 政一[2]

受付日 2013年3月16日, 採録日 2013年9月13日

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，選択した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．本稿では，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，空間的な分散性を高めて情報を伝送できるため，無線ネットワーク内における情報の秘匿性を向上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．計算機シミュレーションに基づく評価の結果，狭ビーム形成の効果として，個々の分散情報が伝達される領域の広がりを選択したパスの周囲に制限し，より分散性の高い複数の伝送路を無線空間内に形成できること，また，そのような伝送路を使用して分散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大幅に軽減できることを明らかにした．一方，その弊害として，受信ノードへの伝送品質の向上を目的としたビーム制御法と比較すると，狭ビームの度合いに比例して送信電力の増大が必要であることを明らかにした．

キーワード：アレーアンテナ，狭ビーム形成，分散伝送，秘密分散法

A Secure Wireless Link Creation Based on Distributed Transmission Using a Secret Sharing Method —Positive and Negative Effects of Narrow-beam Creation

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

Received: March 16, 2013, Accepted: September 13, 2013

Abstract: The authors have proposed a secure wireless link creation scheme based on a distributed transmission by providing multiple numbers of separated propagation routes to a destination. In the proposed scheme, at first, narrow-beam antenna directivities are created with an array antenna installed at the transmitter. Then, the transmitted information is divided into multiple numbers of "shared information" by a secret sharing method and sent to a destination separately through the propagation routes created with the individually controlled antenna-beam directivities. In this paper, we will clarify the positive and negative effects of the narrow-beam creation. By creating a narrow beam at the transmitter, as a positive effect, each shared piece of information is concentrated along the selected paths which will enhance the dispersibility of the distributed transmission. On the other hand, as a negative effect, the transmitted power of each shared piece of information is increased due to the deterioration of the propagation gain. Computer simulations clarify that the transmission routes are formed in a separated manner along the selected path with the narrow-beam creation, so that the secrecy of the transmitted information is greatly improved with the distributed transmission. On the other hand, the transmission power should be increased to maintain a wireless link as the antenna-beam width got narrowed with the narrow-beam creation.

Keywords: array antenna, narrow beam creation, distributed transmission, secret sharing method

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・空港のロビー等，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はらむことになる [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になる [3]．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，時間の経過ととも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，利用勝手が良く，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 [4], [5]．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いく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．秘密分散法は情報理論の分野で研究がさかんに進められている情報の分散管理手法の 1 つで，(k, n) 閾値法とも呼ばれる [6]．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できるが，k 個未満であれば，元情報に関する情報をいっさい得ることができないという特徴を有する．特に，$n = k$ の場合を満場一致型の秘密分散法 [7] と呼び，この場合はすべての分散情報がなければ元情報を復元できない．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できないため，送信者は第三者への情報漏洩を抑制できる．

アンテナの指向性は情報を空間的に分散して伝送するうえ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（Directional constrained minimization of power：DCMP）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．本稿では，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明らかにする．

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，無線空間内を伝搬する信号の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させることが必要となる．本稿では，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明らかにする．

本稿の構成は以下のとおりである．まず，2 章で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 章でアレーアンテナの構成を説明し，本稿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

[1] 広島国際大学工学部情報通信学科
Faculty of Engineering, Hiroshima International University, Kure, Hiroshima 737–0112, Japan
[2] 大阪大学大学院工学研究科電気電子情報工学専攻
Graduate School of Engineering, Osaka University, Suita, Osaka 565–0871, Japan
[a)] m-yamana@it.hirokoku-u.ac.jp

本論文の内容は 2012 年 9 月のマルチメディア通信と分散処理研究発表会にて報告され，同研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

で，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 章でまとめる．

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 [6]．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いっさい復元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できない手法を満場一致法と呼ぶ [7]．

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，送信ノード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 [8]．

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．

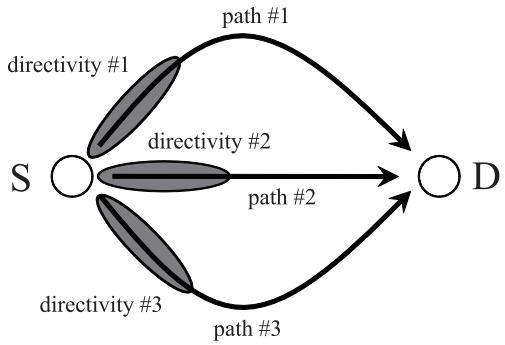


図 1 提案法による分散伝送のイメージ

Fig. 1 A realized image of the proposed distributed transmission.

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，無線空間全体において分散情報が伝達される領域を空間的に完全に分離する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，無線空間内を伝搬す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できず，正しく情報を伝達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できる．提案法では，このような考えに基づき，あらかじ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狭く限定し，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させる．

2.2 従来研究

従来，通信における盗聴対策としては，インターネットを介した通信を前提とし，IPsec や SSL を用いて情報を暗号化して送信する等，通信の比較的上位のレイヤにおいて対策が行われることが一般的であった．しかしながら，近年，1 章で述べたプライベートな無線ネットワークにおける鍵配送の問題に見られるように，通信路やネットワークの形態に起因する問題への対策として，より下位のレイヤにおける対策が注目されている [9]．

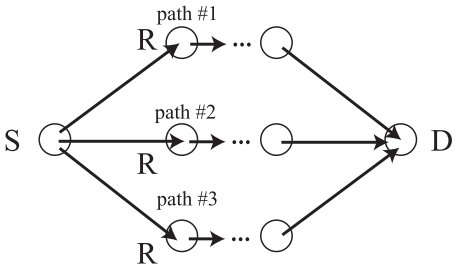
下位レイヤにおけるセキュリティ対策の 1 つに物理レイヤセキュリティがある．物理レイヤセキュリティとは，物理レイヤにおいて発生する物理現象を利用したセキュリティと定義できる．近年，こうした物理レイヤセキュリティとして，人工的に雑音を発生させたり，信号を広帯域に拡散したりすることにより，無線信号の復調を抑制する検討 [10], [11], [12] や，電波の伝搬特性を利用して暗号鍵を生成することにより，秘密通信を実現する検討 [13] 等，数多くの検討が行われており，情報理論に裏付けられた安全性の高いセキュリティを達成できる可能性が示されている [14]．しかしながら，これらのセキュリティ対策も受信側における対策という点では，従来の上位レイヤにおける対策と共通であり，信号波形として情報は第三者ノードへ漏洩しているため，雑音除去や拡散符号，暗号鍵の判明に

ともない，情報が漏洩する危険性がある．

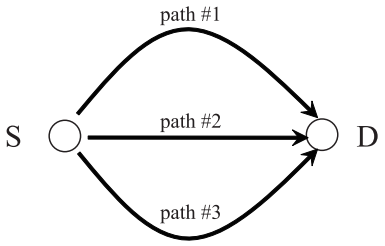
上記の課題に対し，指向性アンテナの適用が有効であり，同じく物理レイヤセキュリティとして，近年数多くの検討が行われている [15], [16]．送信ノードへ指向性アンテナを設置することで，送信側における対策が可能であり，電波の放射を制御することで，信号波形そのものの漏洩を未然に防ぐことができる．一方で，指向性アンテナを用いた対策では，アンテナの空間分解能が課題となる．従来の検討の多くは，1 つのアンテナビームにより電波の放射方向を制御する，単一ビームによる検討であった [15]．単一ビームでは情報の伝達方向を狭く制御できるものの，依然としてビーム方向への情報漏洩を許容することになる．こうした課題に対して，本稿において提案する複数ビームの形成が有効であり，2.1 節に述べるように，秘密分散法を適用することを前提に複数ビームを形成することにより，より広い範囲に対する情報漏洩の抑制が可能となる．

秘密分散法を通信へ適用し，分散伝送を行うことにより，送信情報の秘匿性を向上させる研究はすでに行われている．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 [17], [18], [19]．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どうし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 [17]，分散情報のルーティング手法の検討や [18]，指向性アンテナを用いた検討 [19] 等が行われている．

これに対し，本稿で述べる手法は，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させ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稿で対象とする分散伝送との違いを示す．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，本稿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．



(a) Multi-path 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 in the distributed transmission between the proposed method and the previous work.

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．本章では，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，本稿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させる．**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でき，選択したパスに沿って空間的な広がりの異なる複数の伝送路を形成できる．

ここで，アンテナのビーム幅は個々の分散情報が伝達されるエリアの広がりに大きく影響し，元情報が伝達されるエリアの広がりを左右する．そのため，ビーム幅は送信情報の秘匿性を大きく左右するパラメータである．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でき，

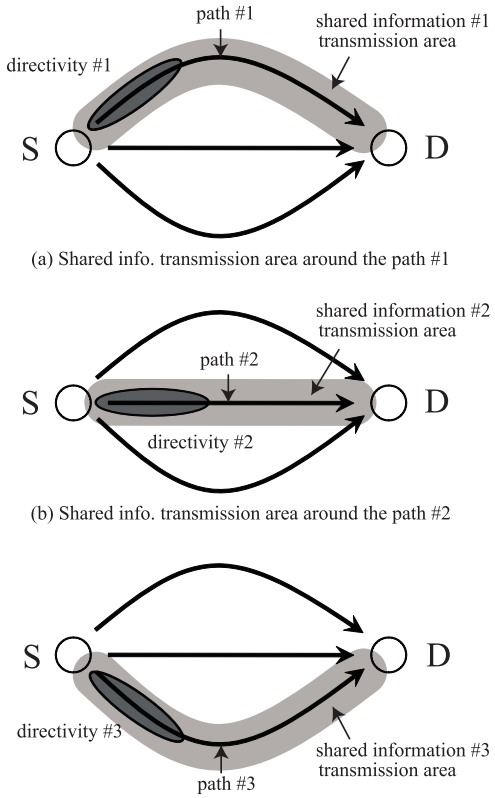


図 3 分散情報が伝達されるエリアの空間的な偏り

Fig. 3 Spatial distribution of the shared information transmission area.

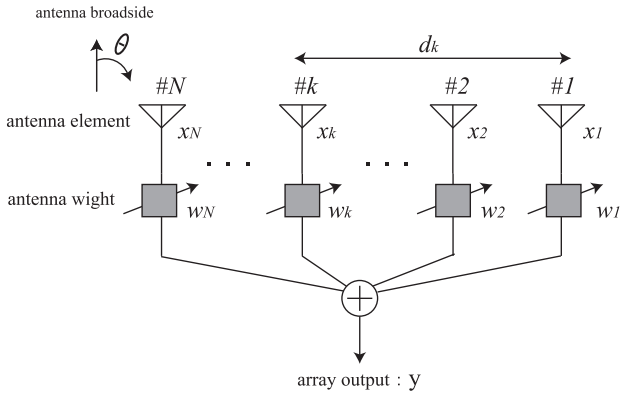


図 4 アレーアンテナの受信動作

Fig. 4 Reception behavior of the array antenna.

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，送信情報の秘匿性を向上させることができると考えられる．

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 [20]．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 に示す受信動作とまったく同じ原理で送信時のアンテナ指向性を制御できる．

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 は次式で表される．ただし，N はアンテナ素子数である．

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

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) のように表される．

$$x_k = x_1 \mathrm{v}_k(\theta) \tag{2}$$

ただし，$\mathrm{v}_k(\cdot)$ 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．

式 (1) は式 (2) を用いて以下のように変形できる．

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

ただし，

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

$\mathrm{D}(\theta)$ はアンテナ伝達関数と呼ばれ，その絶対量（$|\mathrm{D}(\theta)|$）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 $|\mathrm{D}(\theta)|$ はアンテナ指向性を表す．ここで，アレー応答（$\mathrm{v}_k(\theta)$）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できるアンテナウエイト制御法として 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を提案してきた [5]．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 1 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 [21], [22].

$$\min_{\mathbf{W}} \left(P_{out} = \frac{1}{2}\mathbf{W}^H \mathbf{R}_{xx} \mathbf{W} \right) \quad \text{subject to } C\mathbf{W}^* = \mathbf{H} \tag{5}$$

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．

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

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を提案してきた [5]．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（Angle of arrival：AOA）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，指向性制御部（antenna directivity controller）において，有効パスごと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 が大きいほどビーム幅が大きく，逆に ΔB が小さいほどビーム幅は小さくなる．次項では，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の影響を検証する．

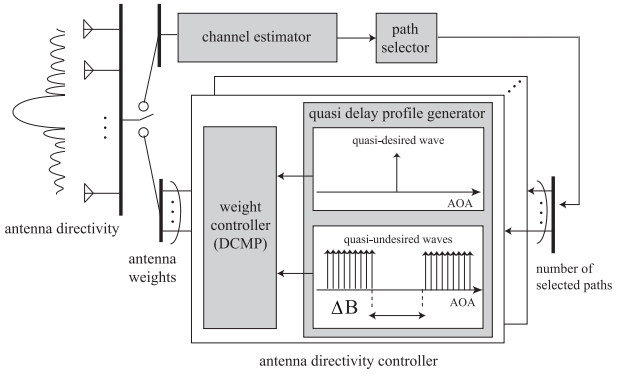


図 5 送信指向性制御手順

Fig. 5 Block diagram for creation of the transmit antenna directivity.

表 1 計算機シミュレーション諸元

Table 1 Simulation parameters.

carrier frequency	5 GHz
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 Relationship between the number of antenna elements and the beam width.

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

3.2.3 アンテナ指向性特性

アレーアンテナでは任意にビーム幅の狭い指向性を形成することはできず，指向性の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角度にアンテナ利得を抑圧し，ビーム幅の小さい狭ビームな指向性を形成できる．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（ΔS）は，アンテナ指向性の角度広がりとして，次式で定義した．θ_{target} は有効パスの放射方向である．

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

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

なお，本稿では，以後，アレーアンテナの諸元は表 1 に示すパラメータを適用し，アンテナ素子間干渉は発生しな

いと仮定した．本稿での議論は，こうした理想的な前提に基づいて提案法の有効性とその問題を明らかにすることにとどめることとする．アンテナ素子間干渉が提案法の特性に与える影響については，アンテナの設計手法によって大きく異なることから本稿での議論の対象外とし，以後のシミュレーション評価には考慮していないことにご注意いただきたい．

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させて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，分散情報が伝達されるエリアをパスに沿った狭い領域に制限し，すべての分散情報が得られる領域を狭く限定できる．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．本章では，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明らかにする．

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反射を考慮したレイトレース法に基づいてモデル化した．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 [23]．**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．

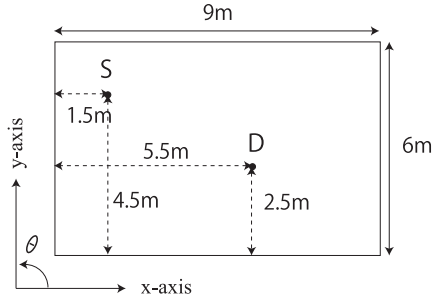


図 6 伝搬路モデル
Fig. 6 Propagation model.

表 3 有効パスの伝搬利得と放射角度
Table 3 Propagation gain and AOD of the effective path.

Path number	1	2	3	4	5	6
Gain（dB）	0	−9.5	−11.0	−16.1	−19.1	−20.5
AOD（deg.）	327.3	56.3	199.1	141.2	24.5	289.7

なお，本検討では，アンテナのビーム特性は水平面内の二次元特性とし，伝搬路モデルも壁面のみの反射を考慮した二次元モデルとした．一般に室内の伝搬特性を正確にモデル化するためには，三次元モデルを用いて三次元レイトレース法を適用する必要がある．しかしながら，室内環境において，二次元レイトレース法を用いて室内の伝搬特性を近似できる研究結果が報告されている [24]．文献 [24] では，正確な近似をするために，壁面における電波の反射係数や透過係数を伝搬路モデルに応じて調整する必要があることが述べられている．しかしながら，こうした報告は，二次元レイトレース法によって室内環境の基本的な伝搬路特性を推定できることを示している．本検討では，このような研究報告を基に，アンテナビーム特性，伝搬特性の両特性ともに二次元特性として条件を同一とし，二次元平面内の解析によって得られる特性を室内環境における基本的な傾向を示す特性として評価した．提案法の三次元的な解析，および，実空間へ適用したときの特性解析は今後の検討課題である．

また，**図 7** にこうした二次元レイトレース解析で考慮する最大反射回数の設定がモデル内における受信電力の推定特性へ与える影響を示す．図 7 は，図 6 に示す S 地点，D 地点にそれぞれ送信ノード，受信ノードを設置した際の，受信ノードで推定される受信電力をレイトレース解析で考慮した最大反射回数を変えて示している．ただし，送信ノードでの送信電力は 1 [mW] とした．図 7 より，まず，最大反射回数を 1 回と 4 回に設定した場合で，推定される受信電力の差は約 0.3 [dB] となっており，最大反射回数の違いによって大きな特性差が生じていないことが分かる．ただ，全体的な傾向として，最大反射回数を 1 回とした場合と 2 回以上では特性が異なっており，最大反射回数を 2 回以上とすることで受信電力特性が収束している．以後の検討では，こうした検討結果を基に，レイトレース解析に用いる最大反射回数の設定を 2 回とした．なお，レイトレース解析で設定される最大反射回数の設定は，推定す

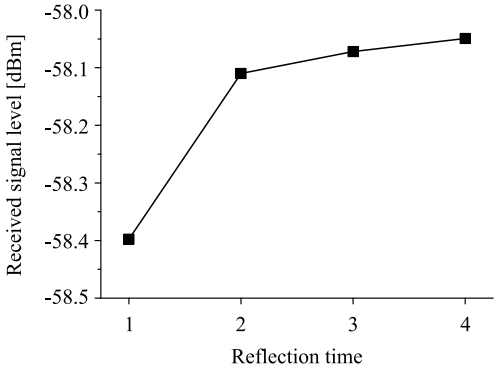


図 7 反射回数の設定が受信電力の推定特性へ与える影響
Fig. 7 Effect of the reflection time has on the estimated received signal level.

る伝搬特性の違いやその精度にも依存するが，4 回前後に設定した報告が多く見られる [25]．本検討において，最大反射回数を 2 回以上とすることで推定特性が収束した理由は，伝搬路モデルが簡易なモデルであることに加え，送受信ノード間が見通し内伝搬となるため，直接波や比較的反射回数の少ない反射波が支配的となったためであると考えられる．

以上の前提，および設定条件のもと，本検討では，図 6 に示す位置に送信ノード，受信ノードを配置し，送信ノードから受信ノードへ無線 LAN（IEEE802.11a）の伝送パラメータ [26] に基づき，規定された最小の伝送レートで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，伝搬路モデル内を 0.5 × 0.5 m のサブエリアに分割し，サブエリアごとの平均受信電力を算出した後，IEEE802.11a の受信感度レベルを基準に，受信感度レベルよりも 3 dB 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サブエリアごとに判断した．ただし，送信ノードでは，IEEE802.11a で規定された最小の伝送レートで伝送することを想定し，受信ノードでの受信電力が受信感度レベルとなるよう送信電力制御を行うものとした．IEEE802.11a で規定された受信感度は −82 dBm であることから，本検討で仮定した復調可能な閾値レベルは −85 dBm となる．なお，復調可能な閾値レベルを受信感度レベルよりも 3 dB 低く設定した理由は，本評価ではサブエリアごとに復調の可否を判断したためであり，サブエリア内における受信電力の変動を考慮したためである．以下，閾値レベルを超えるエリアを「復調可能エリア」と定義する．

4.3 秘匿性向上の効果

図 8 に有効パス ♯2（伝搬利得：−9.5 dB，放射角：56.3 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 8 より，アンテナ本数の増大とともに，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させることにより，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できているためであると考えられる．

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できる．一例として，**図 9** 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，**図 10** にこれらの復調可能エリアより算出した元情報が漏洩するエリアを示す．ただし，図 9 において，パス ♯1〜♯6 は表 3 の 6 本のパスを示

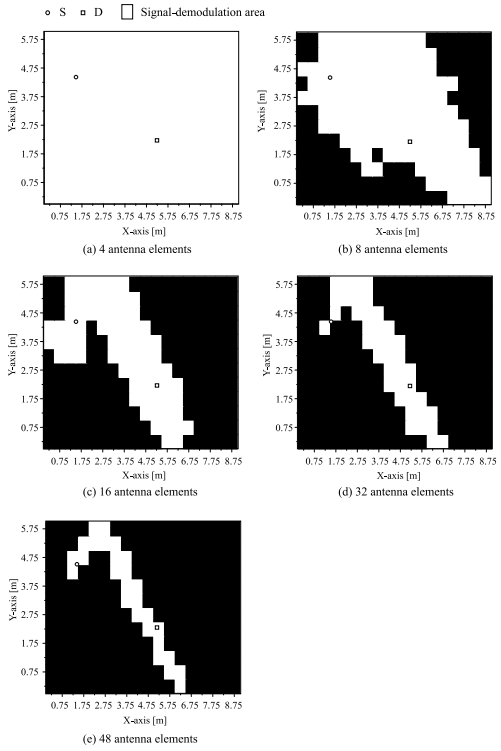


図 8 アンテナ素子数の変化にともなう復調可能エリアの変化
Fig. 8 Spatial distribution change of the signal-demodulation area in accordance with changes of the number of antenna elements.

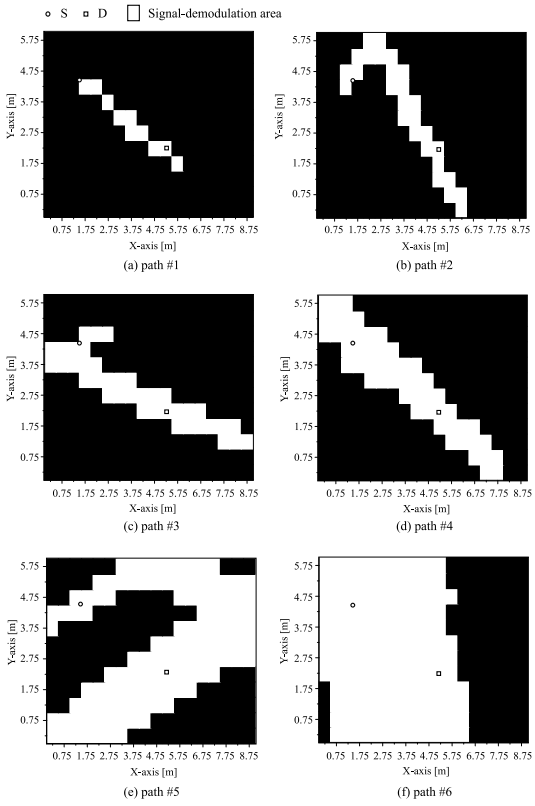


図 9 復調可能エリアの分布
Fig. 9 Spatial distribution of the signal-demodulation area.

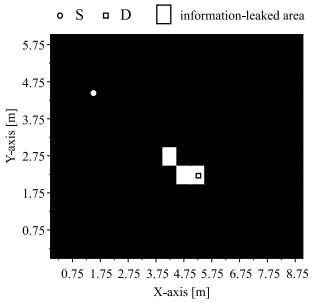


図 10 元情報が漏洩するエリアの分布
Fig. 10 Information-leaked area of the original information.

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 the information-leaked area.

Number of elements	4	8	16	32	48
Spatial ratio（%）	22.2	17.6	17.6	3.7	1.4

しており，図 10 に示す結果はこれら 6 本のパスへ満場一致型の秘密分散法に基づいて送信情報を分散して伝送した結果である．満場一致型の秘密分散法に基づく分散伝送を行うことにより，元情報の復元にはすべての分散情報が必要となる．そのため，元情報が漏洩するエリアは図 9 のすべての復調可能エリアが重なった領域として求めることができる．図 10 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．なお，図 9 において，パスの周囲に形成される復調可能エリアの広がりはパスごとに大きく異なっており，パス番号が大きくなるに従って，その広がりが増していることが分かる．これは表 3 に示すように，パス番号が大きくなるに従ってパスの伝搬利得が減少するためであり，本検討では，送信ノードにおいて受信ノードでの目標受信レベルを規定した送信電力制御を行っているために，送信ノードから放射される信号の電力が増大するためである．

表 4 に，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させるに従って，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．一方で，狭ビーム化とアンテナ利得の増幅の有無は無関係であり，所望方向へのアンテナ利得が増幅しなければ，狭ビーム化によって送受信ノード間のパスの数が制限され，送受信ノード間の伝搬利得が減少するため，場合によって送信電力が増大する弊害が生じる．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する際，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た送信指向性制御法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．

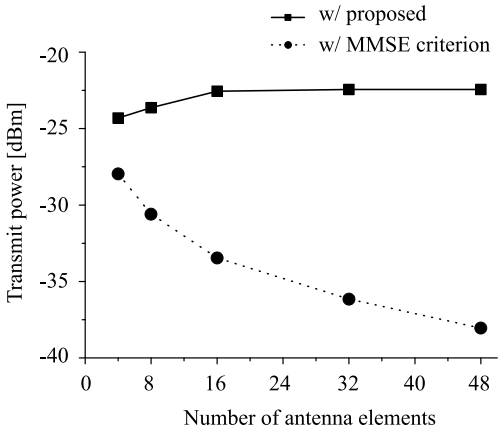


図 11 アンテナ素子数の増大に対する送信電力の変化
Fig. 11 Transmit power change against the number of antenna elements.

図 11 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 Minimum mean square error（MMSE）基準 [20] に基づく指向性制御法を用いた特性をあわせて示す．ただし，両特性において，送信ノードでは受信ノードに対して受信感度レベルを目標レベルとして送信電力制御を行っていることに注意していただきたい．

図 11 より，アンテナ素子数を増大させるに従って送信電力は約 3 dB 増大することを確認した．これは，上記の理由により，提案法では狭ビーム化を行ってもアンテナ利得は増幅されないため，狭ビーム化にともなって送受信ノード間の伝搬利得が減少したためであると考えられる．一方，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ともに広がっており，アンテナ素子数が 32 本の場合で比較すると約 10 dB 以上大きな送信電力が必要となることを確認した．これは，狭ビーム化を目的とする送信ビーム制御では自由度の増加がアンテナ利得の増幅に寄与しないため，MMSE 基準等の伝送品質の向上を目的とした送信指向性制御法と比較するとアンテナ素子数の増大とともに伝送効率の劣化が顕著に表れた結果であると考えられる．

5. おわりに

本稿では，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明らかにした．狭ビームを

形成し，送信情報を無線空間内で分散して伝送することにより，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，送信電力を増大させる必要がある．

本稿では，このような秘匿化の効果と電力面における弊害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 48 素子まで増大させることにより，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明らかにした．その一方で，アンテナ素子数を増大させることにより送信電力は最大約 3 dB 増大することを明らかにした．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 10 dB 以上の余分な送信電力が必要となることを明らかにした．

参考文献

[1] Yang, H., Ricciato, F., Lu, S. and Zhang, L.: Securing a Wireless World, *Proc. IEEE*, Vol.94, No.2, pp.442–454 (2006).

[2] Edney, J. and Arbaugh, W.A.: *Wi-Fi protected access and 802.11i*, Pearson Education (2004). 加藤聰彦（訳）：無線 LAN セキュリティ—次世代技術 IEEE802.11i と WPA の実際，構造計画研究所 (2006).

[3] Xiao, Y., Shen, X. and Du, D.-Z. (Eds.): *Wireless Network Security*, Springer (2007).

[4] 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 (2010).

[5] Yamanaka, M., Miyamoto, S., Sampei, S. and Morinaga, N.: A Study on a Transmit Antenna Directivity Conrol of Adaptive Array for Secure Wireless Transmission Based on the Multi-Path Routing, *Proc. VTC-Spring 2012*, pp.1–5 (2012).

[6] Shamir, A.: How to Share a Secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (1979).

[7] 尾形わかは，黒沢 馨：秘密分散共有法とその応用，電子情報通信学会誌，Vol.82, No.12, pp.1228–1236 (1999).

[8] Karnin, E.D., Greene, J. and Hellman, M.E.: On secret sharing systems, *IEEE Trans. Inform. Theory*, Vol.29, No.1, pp.35–41 (1983).

[9] Liu, R. and Trappe, W. (Eds.): *Securing Wireless Communications at the Physical Layer*, Springer (2010).

[10] Zhu, J., Mo, J. and Tao, M.: Cooperative Secret Communication with Artificial Noise in Symmetric Interference Channel, *IEEE Commun. Letters*, Vol.14, No.10, pp.885–887 (2010).

[11] Matsufuji, S. and Imamura, K.: A spread-spectrum communication system protecting information data from interception, *IEEE Trans. Inform. Theory*, Vol.46, No.4, pp.1691–1695 (2000).

[12] Valizadeh, A. and Wang, Z.J.: An Improved Multiplicative Spread Spectrum Embedding Scheme for Data Hiding, *IEEE Trans. Inform. Forensics and Security*, Vol.7, No.4, pp.1127–1143 (2012).

[13] 岩井誠人，笹岡秀一：電波伝搬特性を利用した秘密情報の伝送・共有技術，電子情報通信学会論文誌 B，Vol.J90-B, No.9, pp.770–783 (2007).

[14] Bloch, M. and Barros, J.: *Physical-Layer Security*, Cambridge University Press (2011).

[15] Goshi, D.S, Leong, K.M.K.H. and Itoh, T.: A secure high-speed retrodirective communication Link, *IEEE Trans. Microwave Theory and Tech.*, Vol.53, No.11, pp.3548–3556 (2005).

[16] Sun, Z. and Lu, J.: Improving the security performance in mobile wireless computing network using smart directional antenna, *Proc. CEEM 2003*, pp.47–50 (2003).

[17] Zhou, L. and Hass, Z.J.: Securing ad hoc networks, *IEEE Network*, Vol.13, No.6, pp.24–30 (1999).

[18] Lou, W. and Fang, Y.: A Multipath Routing Approach for Secure Data Delivery, *Proc. MILCOM 2001*, pp.1467–1473 (2001).

[19] Berman, V. and Mukherjee, B.: Data Security in MANETs using Multipath Routing and Directional Transmission, *Proc. ICC 2006*, pp.2322–2328 (2006).

[20] 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).

[21] Frost, O.L.: An algorithm for linearly constrained adaptive array processing, *Proc. IEEE*, Vol.60, No.8, pp.926–935 (1972).

[22] Takao, K., Fujita, M. and Nishi, T.: An Adaptive Antenna Array under Directional Constraint, *IEEE Trans. Antennas and Propagation*, Vol.24, No.5, pp.662–669 (1976).

[23] Seidel, S.Y. and Rappaport, T.S.: Site-specific propagation prediction for wireless in-building personal communication system design, *IEEE Trans. Veh. Technol.*, Vol.43, No.4, pp.879–891 (1994).

[24] 平館郁雄，矢野一人，太郎丸真：空間信号処理適用時の面的周波数利用効率評価へ向けた簡易二次元レイトレースによる伝搬路生成，電子情報通信学会技術報告，RCS2007-98 (2007).

[25] 杉浦貴志，本間尚樹，西森健太郎：MIMO センサ—屋内環境における侵入検出精度のレイトレース解析，電子情報通信学会技術報告，AP2010-76 (2010).

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

推薦文

無線 LAN 環境下におけるセキュリティ向上のために，秘密分散法の考え方に基づいた指向性アンテナを用いた狭ビーム形成方式を提案している．また，提案方式の導入にともない，目的ノードでの伝搬利得の減少を回避するための送信電力増大の弊害について評価も行っている．このように，提案方式の利点とあわせて弊害についても公平に評価を行った本論文は同研究分野において学術的に高い貢献が認められる．よって，本研究会からの推薦に値する．

（マルチメディア通信と分散処理研究会主査　勝本道哲）

山中 仁昭 （正会員）

平成 11 年大阪大学工学部通信工学科卒業．平成 14 年同大学大学院博士前期課程修了．同年広島国際大学社会環境科学部助手，平成 19 年同大学工学部助教，平成 23 年同講師，現在に至る．博士（工学）．これまで，無線干渉対策，Physical Layer Security に関する研究に従事．平成 14 年電気学会優秀論文発表賞受賞．電子情報通信学会，IEEE 各会員．

宮本 伸一

平成 2 年大阪大学工学部通信工学科卒業．平成 4 年同大学大学院博士前期課程修了．現在，同大学院工学研究科准教授．工学博士．これまで，無線通信方式，光通信方式，EMC に関する研究に従事．平成 13〜14 年米国・ヴァージニア州立工科大学客員研究員．平成 9 年電子情報通信学会学術奨励賞，平成 22 年および平成 25 年電子情報通信学会通信ソサイエティ活動功労賞受賞．電子情報通信学会，映像情報メディア学会，IEEE 各会員．

三瓶 政一

昭和 55 年東京工業大学工学部電気電子工学科卒業．昭和 57 年同大学大学院修士課程修了．同年郵政省電波研究所（現，独立行政法人情報通信研究機構）入所．以来，ディジタル陸上移動通信におけるフェージング対策，干渉対策，適応伝送方式の研究に従事．平成 3〜4 年米国・カリフォルニア大デービス校客員研究員．平成 5 年大阪大学工学部助教授．平成 16 年同大学大学院工学研究科教授．工学博士．昭和 60 年電子情報通信学会篠原記念学術奨励賞，平成 4 年および平成 20 年電気通信普及財団テレコムシステム技術賞，平成 13 年電子情報通信学会業績賞，平成 16 年ドコモ・モバイル・サイエンス賞，平成 21 年 Ericsson Telecommunication Award，平成 22 年電子情報通信学会通信ソサイエティ Best Paper Award 受賞．電子情報通信学会フェロー，映像情報メディア学会会員，IEEE Fellow．