

セキュアな無線リンクを形成するための 送受信ビームフォーミングによる分散伝送路形成法

山中 仁昭^{1,a)} 宮本 伸一² 三瓶 政一²

受付日 2013年5月11日, 採録日 2013年10月9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, 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. 本手法では, 送信ノードに搭載したアレーアンテナを用いて選択したパスの方向へ個別にビーム形成を行うことにより, 無線空間内に複数の伝送路を形成し, 分散伝送を実現する. 本稿では, 受信ノードへもアレーアンテナを搭載することにより, 送信ビームと協調して受信ビームを制御する送受信ビームフォーミング法を提案するとともに, こうしたビームフォーミング法に基づく分散伝送路形成法を提案する. 室内環境を模擬した計算機シミュレーションにより, 提案法は少ないアンテナ素子で分散性の高い伝送路を形成でき, 送信情報の秘匿性を向上させることができること, また, 従来法では十分な秘匿性を確保できない見通し外環境においても有効な対策となることを確認した.

キーワード: 分散伝送, 秘密分散法, アレーアンテナ, 送受信ビームフォーミング

Distributed Transmission for Secure Wireless Links by Joint Transmitter-receiver Beamforming

MASAAKI YAMANAKA^{1,a)} SHINICHI MIYAMOTO² SEIICHI SAMPEI²

Received: May 11, 2013, Accepted: October 9, 2013

Abstract: The authors have proposed a secure wireless link creation scheme based on a distributed transmission by providing multiple transmission routes to a destination. In this scheme, the transmitted information is divided into pieces of “shared information” by a secret sharing method and separately sent to a destination through different transmission routes with individually controlled antenna directivities. In this paper, the authors propose a joint receiver beamforming in accordance with the transmitter antenna directivity for the distributed transmission. Computer simulations clarify that the proposed scheme can enhance the degree of spatial distribution of the transmission routes. Therefore the secrecy of the transmitted information is greatly improved through the distributed transmission in wireless spaces including non-line-of sight environment from the sender.

Keywords: distributed transmission, secret sharing method, array antenna, joint transmitter-receiver beamforming

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 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. 従来, このよう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

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

的に導入が進められている。

一般に無線通信では、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、ユーザの利用に合わせた柔軟なネットワークの構築が可能である。その一方で、情報が周囲の広い範囲へ漏洩する危険に留意する必要がある。従来、こうしたセキュリティ対策としては、特定のアプリケーションやリンクごとに信号を暗号化して伝送することが一般的であり、比較的、通信の上位のレイヤで対策が施されてきた [1], [2]。しかしながら、近年、物理レイヤを中心に下位のレイヤにおいても多くの検討が積極的に行われている [3]。

物理レイヤは OSI 階層モデルにおいて、7 階層のうち最下層に位置するレイヤである。こうした下位のレイヤにおいてセキュリティ対策を施しておくことで、上位レイヤでの対策と合わせてより強固なセキュリティを達成できる。近年、物理レイヤでは、電波の伝搬特性を利用して暗号鍵を生成する検討 [4] や人工的な雑音の発生によりネットワークの秘匿性を向上させる検討 [5], [6] 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高いセキュリティ性能を達成できることが明らかになっている [7]。

著者らは、物理レイヤにおけるセキュリティ対策として、アンテナの指向性を制御することにより空間的に偏りのある複数の伝送路を形成し、こうした伝送路へ情報を分散して伝送することにより、送信情報が漏洩する危険性を軽減する方式を提案してきた [8]。提案法では、伝搬路のマルチパス性に着目し、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する。著者らは、このように選択したパスを中心に伝送路を形成することにより、パスの空間的な分散性を利用して分散伝送を実現できることを明らかにしてきた。

無線空間内に複数の伝送路を形成するうえでアンテナの指向性は重要な要素である。著者らは、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、アレーアンテナを用いた狭ビーム形成法を提案してきた。アンテナの指向性を「狭ビーム化」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、個々の伝送路の広がりを縮小でき、その分散性を高めることができる。そのため、狭ビームを形成することにより送信情報の秘匿性が向上する。しかしながら、秘匿性を十分に向上させるためには、ビーム幅をかなり狭く調整しなければならず、極度な狭ビーム化が必要となる。こうした狭ビームを形成するためには、非常に多くのアンテナ素子を必要とするため、実現性に課題が残る。

そこで、本稿では、一義的な狭ビーム化に頼らない分散伝送路形成法として、送信ノードだけではなく、受信ノードへもアレーアンテナを搭載し、送受信ノード間で協調してビーム制御を行う送受信ビームフォーミング法 (Joint transmitter-receiver beamforming) を提案する。一般に、無線 LAN 等のすべてのノードで同一周波数帯を使用する

無線ネットワークでは、ノード間の伝搬特性に可逆性が成立する。そのため、送信ノード、受信ノードの双方において、比較的少ない制御情報により互いのノードへの伝搬特性を把握し、選択する共通のパスに対してビームを向け合うことが可能である。送受信ビームフォーミングにより、受信ノードでは、所望信号に対する受信感度を高めることができる。それによって、送信ノードでは、送信電力を低減させて不要な電波の放射を抑圧でき、送受信ノード間に形成する伝送路の広がりを縮小できると考えられる。つまり、送受信ビームフォーミングによって無線空間内に形成する個々の伝送路の広がりを小さく抑え、分散性の高い伝送路を形成することが本稿の目的である。

本稿の構成は以下のとおりである。まず、2 章で分散伝送に基づくセキュアな無線リンクの形成法について述べ、送受信ビームフォーミングを導入する意義を説明する。続いて、3 章で、ビーム形成の具体的な手順を述べる。その後、4 章で、送受信ビームフォーミングの効果を計算機シミュレーションにより示し、最後に 5 章でまとめる。

2. セキュアな無線リンクの形成

2.1 分散伝送によるセキュリティの担保

情報量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 [9]。著者らは、このような考えに基づいて元情報を分散した後、無線伝搬路のマルチパス性を利用して分散し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を提案してきた。提案法では、まず、情報を振り分けて伝送するパスを有効パス (Effective path) 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て送信ビームを形成し、これら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。

送信情報の分散手法としては様々な手法が考えられるが、情報量的な考察に基づく手法として、秘密分散法がある [10]。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、その個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分散手法である。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 [11]。

図 1 は、こうした分散伝送の一例として、送信ノード (Source node : S) — 受信ノード (Destination node : D) 間で 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することにより、周囲に盗聴を試みる第三者の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、元情報の漏洩

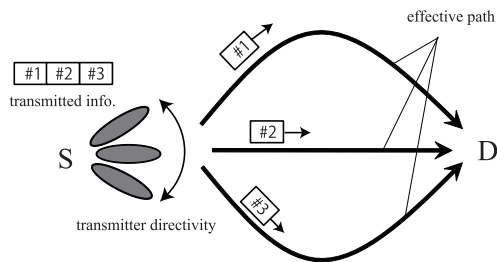


図 1 分散伝送のイメージ

Fig. 1 Realized image of the distributed transmission.

を抑制できる。

なお、通常、無線空間内においてパスの経路は複雑に重なり合うため、信号を完全に分散して伝送することは不可能である。しかしながら、指向性のあるアンテナを用い、その指向性をターゲットとするパスへ向けることで、空間内を伝搬する無線信号の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、信号を正しく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信号を復調することができず、正しく情報を伝達できないことを考慮すると、分散情報が伝達される領域（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で分散させておき、生成した分散情報ごとにアンテナの指向性を切り替えて伝送する。著者らはこうした分散伝送により、元情報が伝達されるエリアを狭く限定し、情報漏洩の危険性を軽減できることを明らかにしてきた。

2.2 送受信ビームフォーミング

前節で述べた分散伝送法により送信情報の秘匿性を高めるためには、無線空間内に形成する伝送路の分散性を高めることが必要であり、選択したパスに沿って伝送路の広がりを小さく抑えることが課題となる。こうした課題に対して、受信ノードへもアレーアンテナを設置し、送信ビームに協調して受信ビームを制御する、送受信ビームフォーミングが有効である。

図 2 に、本稿で提案する送受信ビームフォーミングについて示す。図 2 は、図 1 と同じ環境において、送受信ノード間で 3 つの有効パスを選択し、各パスへ情報を分散して伝送する様子を示している。提案法では、まず、送信ノード、受信ノードにおいて、互いのノードまでの伝搬特性を把握する。続いて、候補となる有効パスを選択し、互いに共通のパスに対してビームを向き合わせてたうえて、情報を分散して伝送する。

2.3 送受信ビームフォーミング導入の意義

送信情報の秘匿性を向上させるためには、個々の伝送路

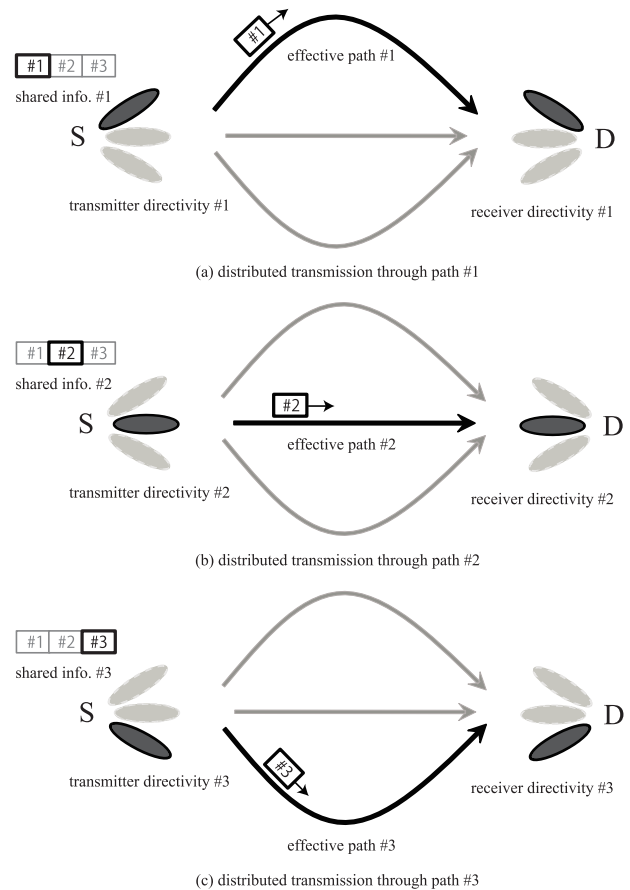


図 2 送受信ビームフォーミングによる分散伝送のイメージ

Fig. 2 Realized image of the distributed transmission with joint transmitter-receiver beamforming.

の広がりを小さく抑えることが必要である。送信ビームを狭ビーム化することによって電波の放射を制限し、伝送路の広がりを小さく抑えることができる。しかしながら、アレーアンテナでは、十分な狭ビームを形成するために非常に多くのアンテナ素子を必要とするという問題がある。

一般に伝送路の広がりを抑える手法として、電波の放射方向を制限することに加えて、放射電力を低減させることが有効である。放射電力を低減させることによって、ビーム制御のみでは制限しきれなかった不要な放射を抑圧し、伝送路の広がりを縮小できる。本稿では、こうした考えに基づき、送受信ビームフォーミングを導入する。送受信ビームフォーミングを導入し、送受信ノード間で互いにビームを向け合わせるにより、ノード間の伝搬利得を増幅することが可能であり、送信電力を低減させることができる。その結果、伝送路の広がりを縮小でき、狭ビーム化に頼らず、伝送路の分散性を向上させることができると考えられる。

2.4 関連研究

送信ノード、受信ノードに複数のアンテナを配置し、互いに協調してビーム制御を行う研究はすでに行われてい

る。送受信ノード双方に複数のアンテナを配置する伝送方式は Multiple-input multiple-output (MIMO) 伝送と呼ばれる [12]。一般に MIMO 伝送では、送信ノードに設置した各アンテナから異なる信号を送信するが、同じ信号を送信し、アンテナごとに信号の位相、振幅を制御することで、送信アンテナ全体の指向性を制御できる [13]。一方で、受信ノードにおいても、すべてのアンテナで同じ信号を受信したときは、アンテナごとに信号の位相、振幅を制御することで、受信アンテナ全体の指向性を制御できる。従来、こうしたビーム制御は通信リンクの品質を改善する目的で用いられてきた [14]。特に、複数のノードが同一空間内に存在する状況では、送受信ノード間で協調してビーム制御を行うことで、ネットワーク内で発生するノード間の干渉を抑圧しつつ、所望信号の受信特性を大きく改善でき、ネットワーク全体の通信品質を改善できる [15], [16]。

一方、本稿における送受信ビームフォーミングは、無線ネットワークのセキュリティの向上を目的としている。送受信ノード間でビームを互いに向け合うことにより、受信ノードでは所望信号に対する受信感度を向上させることができるため、より小さな電力の信号を復調することが可能となる。そのため、送信ノードでは、信号の送信電力を抑えることができ、不要な電波の放射を抑えて情報の拡散を防ぐことができる。本稿では、こうした考えに基づき、これまでは主に通信品質を改善する目的で提案されてきたアンテナのビーム制御法を応用し、無線空間内に複数の伝送路を形成することを目的とする。

3. 送受信ビームフォーミング法

送信ビームと協調して受信ビームを制御するためには、送受信ノードにおいて互いのノードへの伝搬特性を共通情報として把握し、両ノードにおいて事前に候補となる共通の有効パスを選択しておく必要がある。本章では、まず、こうした共有情報を通知し、送受信ビームフォーミングを行うためのノード間のアクセス手順について述べる。続いて、アレーアンテナを用いた送信ノード、受信ノードのビームフォーミング法について説明する。

3.1 送受信ノード間のアクセス手順

本手法では、IEEE802.11 系無線 LAN においてオプション規格として規格化されている RTS/CTS 制御 [18] を用いて、必要な情報を共有することを想定する。図 3 に本手法における端末間のアクセス手順を示し、送受信ビームフォーミングを行うための制御内容について図中の番号に合わせて以下に示す。なお、図中の両矢印は IEEE802.11 で定義されている短フレーム間隔 (Short inter frame space: SIFS) 示している。

(1) S ではキャリアセンスを行った後、D に対して RTS パケットを送信する。D では、受信した RTS パケッ

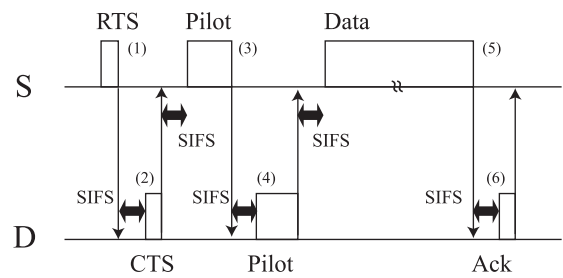


図 3 送受信ノード間のアクセス手順

Fig. 3 Access protocol between source and destination nodes.

トを基に S-D 間の伝搬路特性を推定し、候補となる有効パスを選択する。

(2) D では通信開始の可否に応じて CTS パケットを S に対して送信する。S では、受信した CTS パケットを基に D-S 間の伝搬路特性を推定し、候補となる有効パスを選択する。なお、本稿では、規定の RTS パケット、CTS パケットを基本として、こうしたパケット内に遅延プロファイルを推定するための PN (Pseudonoise) 系列 [17] 等の拡散系列を含めて伝送することにより、S, D の双方において伝搬路推定を行い、両ノード間に存在するパスを遅延プロファイルとして検出することを想定する。一般に無線 LAN 等のすべてのノードで同一の周波数帯を使用する無線ネットワークでは、ノード間の伝搬特性に可逆性が成立する。そのため、上記のように、伝搬路推定用の拡散系列をパケット内に含め、RTS, CTS パケットのように短い時間間隔で互いに交換するようなパケットに含めて伝送することで、S, D の双方においてほぼ同時刻に互いのノードへの遅延プロファイルを取得できる。また、こうしたパケットは S, D においてパケットの送信権を得ることを目的として、データパケットを送信する直前に行われるため非常に都合が良い。提案法では、S, D それぞれにおいて互いにノードまでの遅延プロファイルを推定した後、こうした遅延プロファイルを基に、パスの減衰量、およびパスの放射方向に関する情報を取得し、無線ネットワーク内で事前に共有する有効パスの選択基準に従って共通の有効パスを選択することを想定する。

(3) S では、まず、候補となる有効パスへ番号 (ID) 付けし、有効パスを順番に選択してビーム形成を行う。続いて、選択した有効パスの ID 情報を含めた Pilot パケットを D へ送信する。D では、S からの Pilot パケットにより S で選択された有効パスを把握し、選択されたパスに対してビーム形成を行う。

(4) D では送信電力制御を行うための制御情報として自身の送信電力レベルを Pilot パケットに含めて S へ通知する。

(5) S では受信した Pilot パケットの受信電力を推定した

後、D から制御情報として得た Pilot パケットの送信電力と比較して伝搬路の減衰量を推定する。そのうえで、推定した伝搬路の減衰量を基に D での目標受信レベルに対して送信電力制御を行い、Data パケットを D へ送信する。

- (6) D では Data パケットを受信後、受信の成否に応じて Ack/Nack パケットを S へ送信する。

3.2 有効パスの選択手順

本節では、推定した遅延プロファイルから有効パスを選択するための基準について述べるとともに、有効パスを選択する手順について説明する。無線空間内に分散性の高い複数の伝送路を形成するためには、その中心となる有効パスを適切に選択することが重要となる。提案法では、有効パスを選択するために下記の 2 つの条件を設け、これらの条件に基づいて有効パスを選択する。

角度条件 (W):

送信ノードからの放射角 (Angle of departure: AOD) が近いパスどうしは伝搬経路が似通るため、その周囲に形成される伝送路の重なりは大きく、形成される伝送路の分散性は低いと考えられる。そこで、有効パスの放射角は一定角度 (W) 以上離れていることとする条件を角度条件として設ける。

電力条件 (A):

一般に減衰量の大きいパスを用いて信号を伝送した場合、対象のノードに対して誤りなく信号を伝送するために、送信ノードにおいて送信電力を大きく増幅することが必要となる。このとき、送信電力を増大させることによって周囲への放射電力も増大するため、伝送路の広がりは大きくなり、伝送路間の分散性は低下すると考えられる。そこで、有効パスの減衰量は一定レベル (A) 以下であることとする条件を電力条件として設ける。

図 4 に上記の角度条件、電力条件に基づいて有効パス

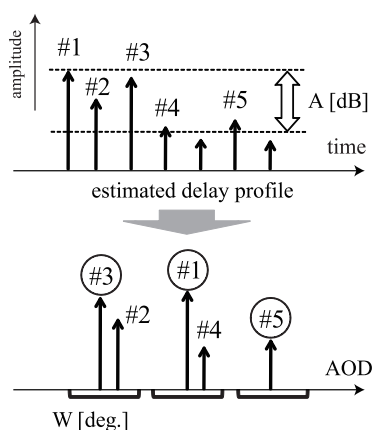


図 4 有効パス選択手順

Fig. 4 Effective path selection procedure.

を選択する様子を示す。図 4 は、まず、推定した遅延プロファイルを基に電力条件を満たす 5 つの候補となるパス (#1, #2, #3, #4, #5 パス) を抽出し、続いて、これらの候補のパスの中から、電力の高いパスの順に角度条件を満たす 3 つの有効パス (#1, #3, #5 パス) を選択する様子を示している。ここで、角度条件の W 、電力条件の A は有効パスを適切に選択するために重要なパラメータである。条件を厳しく (W を大きく、 A を小さく) し過ぎると必要なパスを見逃すこととなり、一方で、条件を緩和 (W を小さく、 A を大きく) し過ぎると無駄な分散につながる恐れがある。本稿では、これまでの著者らの経験により、本稿で想定する伝搬環境において、 A は第 1 パスを基準として 30 dB, W は各パスを中心に 30° とした。こうしたパラメータ設定はパスの伝搬特性に大きく依存し、周囲の伝搬環境に応じて適切に設定する必要があると考えられる。上記設定の最適性を含め、こうした検討は今後の検討課題である。なお、提案法では、有効パスを選択する手順において、遅延プロファイル内のすべてのパスに対して、その放射方向を推定する必要がある。本稿では指向性アンテナとしてアレーアンテナを用いることを前提に、Estimation of Signal Parameters via Rotational Invariance Techniques (ESPRIT) 法 [21] を適用し、推定する。

3.3 送信ビームフォーミング

送信ノードでは、電波の放射方向を制限するために、有効パスの方向に対して主ローブを向けるだけでなく、主ローブ以外のサイドローブを大きく抑圧する必要がある。著者らは、こうした送信ビームを形成するため、方向拘束付き出力最小化法 (Directionally constrained minimization of power: DCMP [19]) に基づくビームフォーミング法を提案してきた [20]。

図 5 にビーム形成の手順を示す。まず、パス選択部 (path selector) において、事前に割り振られた ID 情報に従って、1 つの有効パスを選択する。続いて、指向性制御部 (antenna directivity controller) において、選択した有

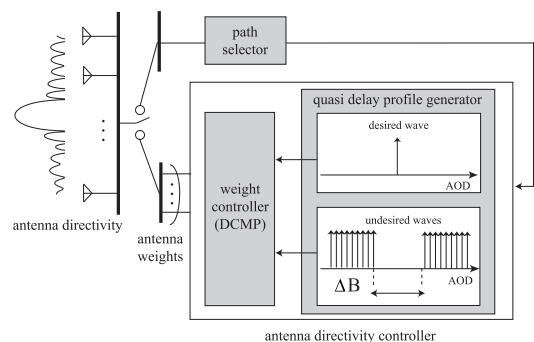


図 5 送信ビーム形成の手順

Fig. 5 Block diagram for the creation of transmitter directivity.

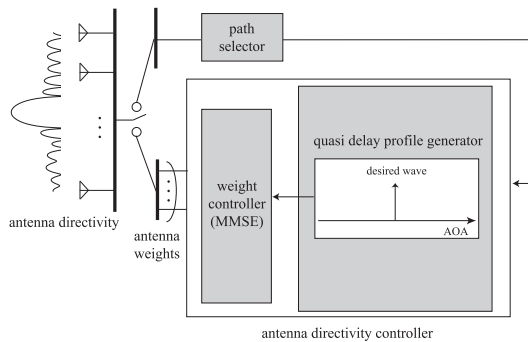


図 6 受信ビーム形成の手順

Fig. 6 Block diagram for the creation of receiver directivity.

効パスの放射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) を生成する. その後, DCMP 法に基づいてアンテナウエイトを算出し, 送信ビームを形成する. なお, 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る. ΔB を調整することにより主ローブのビーム幅をアンテナ自由度の範囲内で制御できる.

3.4 受信ビームフォーミング

受信ノードでは, 伝送路の広がりを見縮小させるため, 所望信号に対する受信感度を高めることが求められる. そのため, 主ローブの利得を大きく制御することが課題となる. 一方で, サイドローブを抑圧することは不要となる. このような要求に対して, MMSE 基準に基づくビーム制御が有効である. MMSE 基準では, 所望信号の SN 比を最大化するようビーム形成が行われるため, 所望方向へのアンテナ利得を最大化することができる [13]. 図 6 に受信ビーム形成の手順を示す. 本稿では, ノード間で送受信を交互に繰り返すことを考え, 受信ビーム形成の手順は, 送信ビーム形成の手順と基本的な構成を同一とした. 図 5 に示す手順と比較して, サイドローブを抑圧する必要がないため, 擬似干渉波の生成を行わない. また, 所望波に対する利得を最大化するため, MMSE 基準でアンテナウエイトを算出する点が異なる.

3.5 ビーム特性

アレーアンテナのビーム特性はアレーアンテナを構成する各素子アンテナのアンテナウエイトの値を基に数値計算によって求めることができる [13]. 3.3 節, 3.4 節の内容に基づいて送信ノード, 受信ノードに設置したアレーアンテナのアンテナウエイトを算出し, それぞれのビーム特性を評価した. 図 7 に送信ビーム特性, 図 8 に受信ビーム特性の一例を示す. ただし, 各図上部に示す “▽” は, 互いにビームを向け合う有効パスの放射方向, 到来方向 (Angle of arrival: AOA) を示している. なお, アレーアンテナの

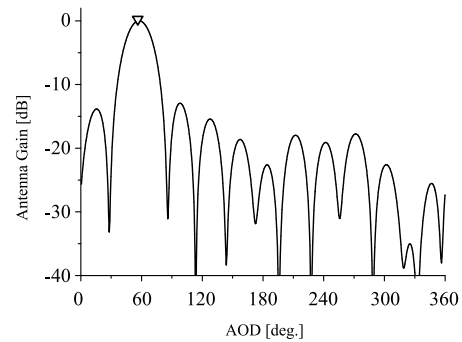


図 7 送信ビーム特性

Fig. 7 Transmitter directivity.

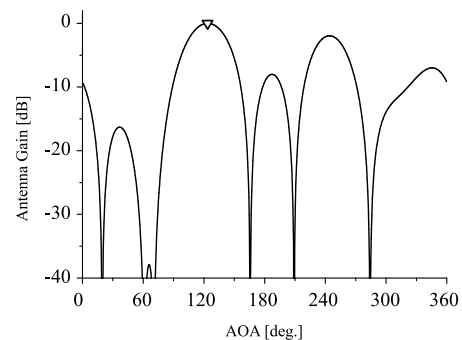


図 8 受信ビーム特性

Fig. 8 Receiver directivity.

アンテナ素子数は 12 素子とし, 各素子を半波長間隔で等間隔円状に配置した. 図 7 より, 有効パスの放射方向に対して主ローブを向け, サイドローブを大きく抑圧した送信ビームが形成できていることが分かる. また, 図 8 より, 有効パスの到来方向に対して主ローブを向けた受信ビームが形成できていることが分かる.

4. 計算機シミュレーション

受信ノードへもアレーアンテナを設置し, 送信ビームと協調した受信ビームを形成することによって, 伝送路の広がりを見縮小させることができる. また, こうした受信ビームの形成は, 見通し外環境等の送信ビームのみでは伝送路の広がりを見制御できない環境においてもその効果が期待できる. 本章では, 5 GHz 帯を用いた IEEE802.11a 無線 LAN による室内伝送を想定し, まず, 壁面のみで構成される簡易なモデル (伝搬路モデル I) を用いて, 送受信ビームフォーミングによって形成される伝送路の基本的な特性, および, 送信情報の秘匿性へ与える効果を明らかにする. 続いて, 伝搬路モデル I の拡張モデルとして, 送受信ノード間が見通し外環境となるモデル (伝搬路モデル II) を用い, 見通し外環境におけるその効果を明らかにする.

4.1 送受信ビームフォーミングの基本的効果

4.1.1 伝搬路モデル I

図 9 に伝搬路モデル I を示す. 伝搬路モデル I では, 壁

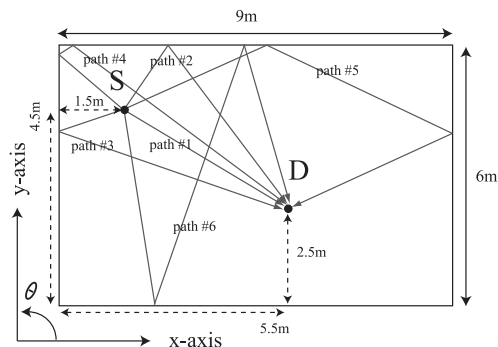


図 9 伝搬路モデル I
Fig. 9 Propagation model I.

表 1 有効パスの利得と放射角

Table 1 Propagation gain and angle of departure of effective path selected between source and destination nodes.

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

面のみの簡易な構成とし、伝搬路の特性を壁面での 2 回反射までを考慮したレイトレース法によりモデル化した [22]. レイトレース法を用いることで、パスが伝搬する経路を正確に求めることができ、その周囲に形成される伝送路の広がり进行评估できる. 本モデルにおいて選択した有効パスの特性として、図 9 にパスの経路、表 1 にパスの利得、送信ノードにおける放射角を示す. ただし、表中の利得は第 1 パスを基準とした正規化利得であり、放射角 (θ) 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.

4.1.2 評価方法

本評価では、無線 LAN [18] の伝送パラメータに基づき、規定の最小レートで情報を分散して伝送することを想定した. つまり、送信ノードは、規定の受信感度レベルを目標レベルとして受信ノードに対して送信電力制御を行うものとした. そのうえで、伝搬路モデル内で観測される無線信号の平均電力を基に伝送路の広がり求め、送信情報の秘匿化特性を評価した.

具体的には、まず、伝搬路モデル内を 0.5 m × 0.5 m のサブエリアに分割し、サブエリア内で観測される平均信号電力を求めた. 続いて、無線 LAN の受信感度レベル −82 dBm を基準に、平均受信電力 −85 dBm 以上を復調可能な閾値レベルとして設定し、閾値レベルを上回るサブエリアの集まりを伝送路としてその広がり求めた. そのうえで、満場一致型の秘分散法を適用することを想定し、伝送路の重なりから元の送信情報が漏洩するエリアの広がり进行评估した. 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、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. 通常、室内環境で

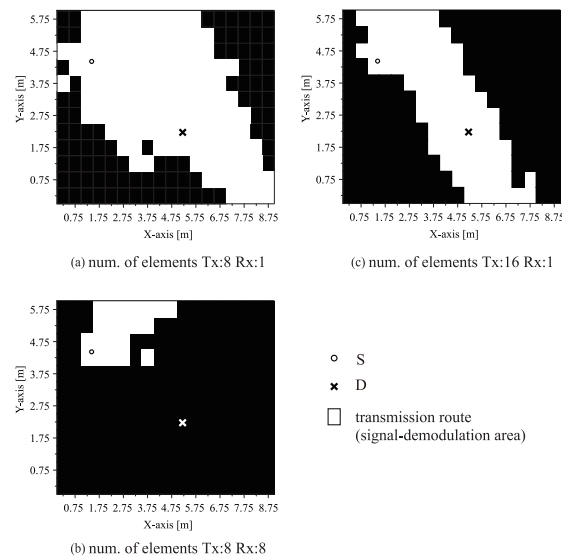


図 10 第 2 パスの周囲に形成される伝送路の様子

Fig. 10 Spatial distribution of the transmission route formed around path #2.

は様々な遮蔽物の影響により、受信電力がシャドウイングによって大きく変動する. しかしながら、本検討では伝搬路モデル内に細かい遮蔽物を配置しておらず、サブエリア内においてこうしたシャドウイングによる大きな受信電力の変化は生じることはないと考えられる. 本稿ではこうした伝搬環境を考慮し、サブエリア内での距離減衰による変動のみを考慮して上記 3 dB のマージンを設定した. 以下、閾値レベルを超えるサブエリアの集まりを「復調可能エリア (Signal-demodulation area)」と定義し、このエリアの広がり伝送路の広がりとして評価する.

4.1.3 伝送路の広がりを与える効果

図 10 に第 2 パスを対象に形成した伝送路の様子を示す. 図 10 (a), (b) は、ともにアンテナ素子数 8 素子で送信ビーム形成を行った結果を示しており、(a) は受信ビーム形成なし、(b) は受信ビーム形成あり (搭載アンテナ素子数 8 本) の結果である. これらの結果より、受信ビームを形成することにより、大きく伝送路の広がり縮小させることができることが分かる. これは、受信ビームによって所望信号に対する受信感度を高めることができたためであり、送信ノードにおいて送信電力を下げ、不要な電波の放射を抑制できたためであると考えられる. また、こうした効果は、アンテナ素子数を 16 素子として送信ビームの形成を行った結果 (図 10 (c)) と比較しても明らかであり、図 10 (b), (c) の結果より、同じアンテナ素子数の条件において、受信ビームを形成した方が伝送路の広がり大幅に制限できることが分かる. この結果は、送信ノードのみへアンテナ素子を集中して配置するよりも、受信ノードへも分散して配置し、相互にビーム形成を行う方が、少ないアンテナ素子で効率良く伝送路の広がり縮小させることができることを示している.

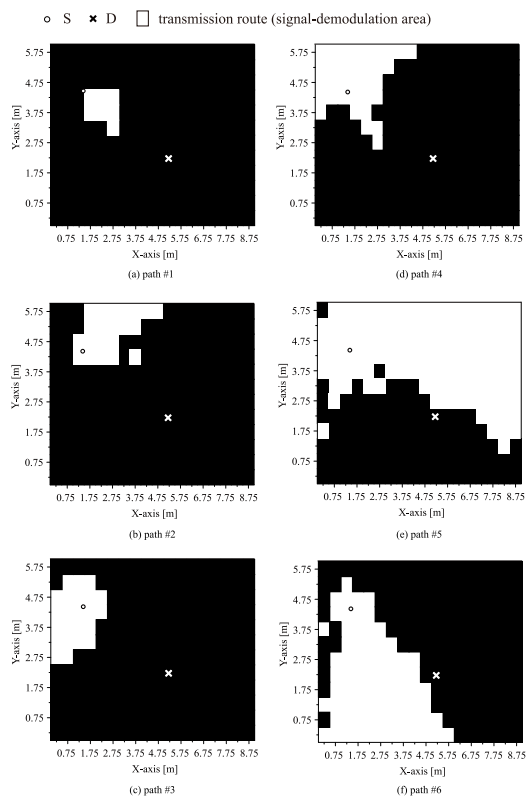


図 11 送受信ビームフォーミングにより形成される伝送路の分布
Fig. 11 Spatial distribution of the transmission route with joint transmitter-receiver beamforming.

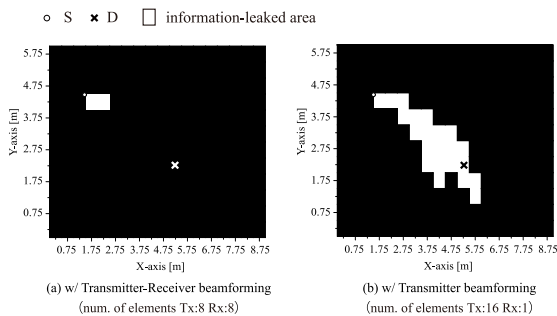


図 12 送信情報が漏洩するエリアの比較
Fig. 12 Information-leaked area of the original information.

4.1.4 送信情報の秘匿性に与える効果

表 1 にあげるすべてのパスを対象として伝送路を形成し、分散伝送を行うことにより、無線空間内にて達成する送信情報の秘匿性について検討を行った。図 11 に、各有効パスを対象として形成した伝送路の広がり性を示す。このような伝送路へ満場一致型の秘密分散法を基に生成した分散情報を伝送する。このとき、元の送信情報はすべての分散情報がなければ復元できないため、元情報が漏洩するエリアはすべての伝送路が重なったエリアとして評価できる。

図 12 (a) に結果を示す。図中の白いエリアが送信情報が漏洩するエリアを示している。(b) は比較対象として、受信ビームを形成せず、送信ビームのみで伝送路を形成し、分

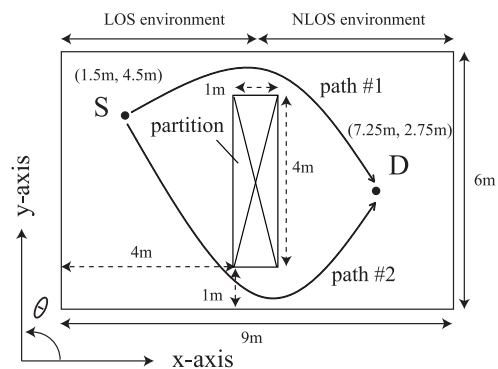


図 13 伝搬路モデル II
Fig. 13 Propagation model II.

表 2 有効パスの利得と放射角

Table 2 Propagation gain and angle of departure of effective path selected between source and destination nodes.

Path number	# 1	# 2
Gain (dB)	0	-1.8
AOD (deg.)	26.2	304.7

散伝送を行った結果である。ただし、アレーアンテナではアンテナ素子数が多いほど自由度の高いビーム制御が可能であり、伝送路の分散性を高めるうえで有利となる。そのため、こうしたビーム制御に関わる条件を揃えて評価するため、(a)、(b) ともに送受信ノードに設置したアレーアンテナの総アンテナ素子数は同一とした。図 12 の結果より、送受信ビームフォーミングを行うことで、送信情報が漏洩するエリアを大幅に縮小できていることが確認できる。これは、受信ビームによって、選択した有効パスに対して電力を集中して信号を伝送できたためであり、それにより伝送路の広がりを抑え、分散性の高い複数の伝送路を無線空間内に形成できたためであると考えられる。

4.2 見通し外環境における効果

4.2.1 伝搬路モデル II

図 13 に伝搬路モデル I の拡張モデルとして、部屋の中央に衝立を設置したモデルを示す。本モデルを伝搬路モデル II とし、見通し外環境における送受信ビームフォーミングの効果を確認する。部屋の中央に衝立を設置したことから、送信ノードにとって、衝立より左側の空間は見通し内 (Line of sight : LOS) 環境、衝立より右側の空間は見通し外 (Non line of sight : NLOS) 環境となる。見通し外環境では、回折による伝搬が支配的となり、電波がより広い範囲に拡散して伝搬することが考えられる。こうした回折の影響を含めた検討を行うため、モデル内の伝搬路特性は、反射に加え、回折を考慮したレイトレース法によりモデル化した。

送受信ノード間のパスの経路としては、衝立を回避する 2 本の経路が考えられる。図 13 にパスの経路、表 2 にパス

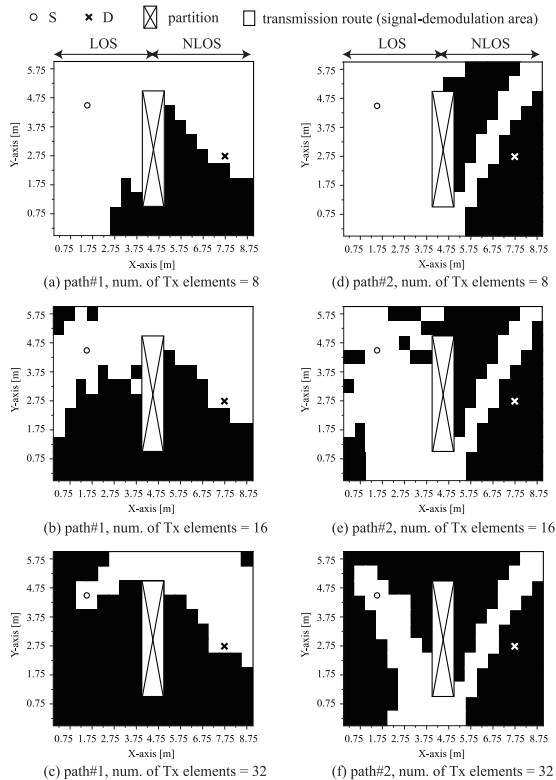


図 14 送信ビームフォーミングにより形成される伝送路の分布
Fig. 14 Spatial distribution of the transmission route with transmitter beamforming.

の特性として、パスの利得、送信ノードにおける放射角を示す。本節では、こうした2本のパスを対象に、送信ノードから見通し外となる環境において、送受信ビームフォーミングが伝送路の広がりを与える効果、および、送信情報の秘匿性を与える効果を検証する。

4.2.2 回折による伝搬が伝送路形成に与える影響

見通し外環境では、回折による伝搬が支配的となる。まず、回折による伝搬が伝送路の形成に与える影響を確認した。図 14 は、受信ビームを形成せず、送信ビームのみによって、伝搬路モデル II 内に形成される伝送路の様子を示している。図 14(a)–(c) はパス #1 の周囲に形成される伝送路、(d)–(f) はパス #2 の周囲に形成される伝送路を示しており、それぞれ、アンテナ素子数を 8, 16, 32 と変えて評価した結果である。図 14 の各図において、衝立より左側の見通し内環境に注目すると、アンテナ素子数の増大とともに、伝送路の広がりを縮小させることができていくことが分かる。一方で、衝立より右側の見通し外環境では、そうした変化は見られない。これは、見通し内環境では、アンテナ素子数を増やし、狭ビーム化を図ることにより、対象とするパスの周囲へ電力を集中して信号を送ることができるのに対し、見通し外環境では、回折によって電波が広範囲に拡散して伝搬するため、そうしたことが困難になるためであると考えられる。つまり、図 14 に示す結果は、送信ノードにとって見通し外となる環境において、送信ビーム

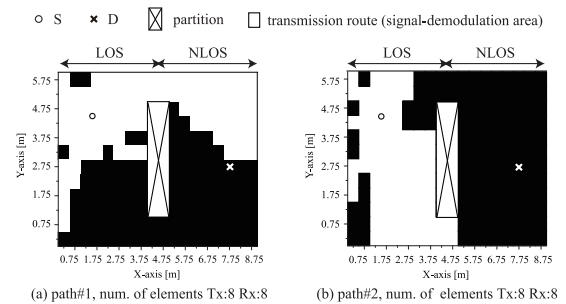


図 15 送受信ノード間に形成される伝送路の様子
Fig. 15 Spatial distribution of the transmission route with joint transmitter-receiver beamforming.

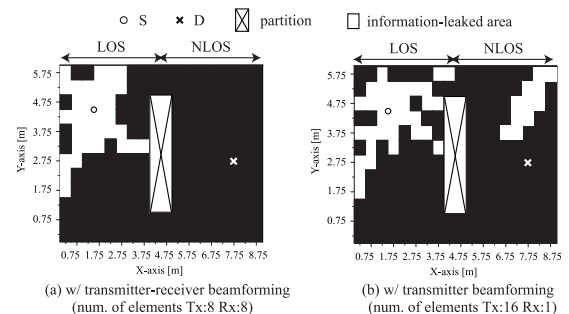


図 16 送信情報が漏洩するエリアの比較
Fig. 16 Information-leaked area of the original information.

のみでは伝送路の広がりを制御することが困難となることを示している。

4.2.3 伝送路の広がりを与える効果

前項で述べた問題に対して、送受信ビームフォーミングが有効である。図 15 は送受信ビームフォーミングによって、パス #1, #2 の周囲へ形成される伝送路の様子を示している。送信ノード、受信ノードに搭載するアンテナ素子数は 8 素子とした。図 15 と図 14 を比較すると、見通し外環境において、送受信ビームフォーミングを行うことで伝送路の広がりを縮小できていることが分かる。これは、受信ビームを形成することにより、有効パスの周囲へ電力を集中して信号を送ってきたためであり、送信ノードからの不要な電波の放射を抑制できたためである。

4.2.4 送信情報の秘匿性を与える効果

最後に、送受信ビームフォーミングが送信情報の秘匿性に与える効果を検証する。図 16(a) に、図 15 に示す 2 本の伝送路を用いた分散伝送により、送信情報が漏洩するエリアを示す。ただし、4.1.4 項での検討と同様に、送信情報は満場一致型の秘密分散法で分散させることを想定した。図 16(b) は比較対象として、受信ビームを形成せず、送信ビームのみで伝送路を形成し、分散伝送を行った結果である。ただし、(a), (b) ともに送受信ノードに設置したアレーアンテナの総アンテナ素子数は同一とした。両図より、送信ノードから見通し外となる環境において、(b) では送信情報が漏洩するエリアが存在するのに対し、(a) で

は完全に情報の漏洩を抑制できていることが分かる。この結果は、見通し外環境においても、送受信ビームフォーミングによって伝送路の分散性を高めることができ、本手法は送信情報の秘匿性を向上させるうえで有効な手法であることを示している。

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法において、狭ビーム化に頼らない分散伝送路形成法として、送信ビームと協調して受信ビームを制御する送受信ビームフォーミング法を提案した。受信ノードへもアレーアンテナを配置し、送信ビームに合わせて受信ビームを制御することで、所望信号に対する受信感度を向上させることができる。そのため、送信ノードでは、送信信号の信号電力を抑えることができ、個々の伝送路の広がりをも縮小して分散性の高い複数の伝送路を無線空間内に形成することができる。

室内環境を模擬した計算機シミュレーションの結果、まず、送受信ビームフォーミングによる基本的な効果として、送受信ノードへ搭載するアンテナ素子数を低減させつつ、無線空間内に形成する伝送路の広がりをも大幅に縮小できることを確認した。また、このような伝送路を用いることにより、空間内を伝搬する無線信号の分散性を高め、送信情報の秘匿性を向上できることを明らかにした。

続いて、送信ノードから見通し外となる環境において、送受信ビームフォーミングの効果を確認した。見通し外環境では、回折によって電波が広範囲に拡散して伝搬するため、送信ビームのみでは、伝送路の広がりをも十分に制御することが困難となる。こうした問題に対して、送受信ビームフォーミングの適用が有効であり、伝送路の広がりをも縮小させつつ、伝送路の分散性を高めることができること、またそれによって、送信情報の秘匿性を向上させることができ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] 難波誠一, 小口正人: インターネット・無線 LAN・放送における暗号化技術, 情報処理, Vol.45, No.11, pp.1143–1145 (2004).
- [3] Liu, R. and Trappe, W. (Eds.): *Securing Wireless Communications at the Physical Layer*, Springer (2010).
- [4] 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).
- [5] 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).
- [6] Lakshmanan, S., Tsao, C., Sivakumar, R. and Sundaresan, K.: Securing Wireless Data Networks

- against Eavesdropping using Smart Antennas, *Proc. ICDCS 2008*, pp.19–27 (2008).
- [7] Bloch, M. and Barros, J.: *Physical-Layer Security*, Cambridge University Press (2011).
- [8] 山中仁昭, 宮本伸一, 三瓶政一: 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, 研究報告マルチメディア通信と分散処理, 2012-DPS-152, pp.1–8 (2012).
- [9] Cover, T.M. and Thomas, J.A.: *Elements of Information Theory*, Wiley (1938).
- [10] Shamir, A.: How to Share a Secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (1979).
- [11] 尾形わか, 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).
- [12] Jankiraman, M.: *Space-time Codes and MIMO Systems*, Artech House Publishers (2004).
- [13] 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).
- [14] Lehne, P.H. and Pettersen, M.: An Overview of Smart Antenna Technology for Mobile Communications Systems, *IEEE Commun. Surveys & Tutorials*, Vol.2, No.4, pp.2–13 (1999).
- [15] Chang, J.H., Tassiulas, L. and Rashid-Farrokh, F.: Joint Transmitter Receiver Diversity for Efficient Space Division Multiaccess, *IEEE Trans. Wireless Commun.*, Vol.1, No.1, pp.16–27 (2002).
- [16] Chen, Z. and Manikas, A.: Joint Space-Time Transmitter-Receiver Beamforming, *Proc. Globecom 2010*, pp.1–5 (2010).
- [17] Sklar, B.: *Digital Communications (2nd ed.)*, Prentice Hall (2001).
- [18] IEEE Std 802.11-2007: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. (2007).
- [19] 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).
- [20] Yamanaka, M., Miyamoto, S., Sampei, S. and Morinaga, N.: A Study on a Transmit Antenna Directivity Control of Adaptive Array for Secure Wireless Transmission Based on the Multi-Path Routing, *Proc. VTC-Spring 2012*, pp.1–5 (2012).
- [21] Roy, R. and Kailath, T.: ESPRIT – Estimation of Signal Parameters via Rotational Invariance Techniques, *IEEE Trans. ASSP*, Vol.37, No.7, pp.984–995 (1989).
- [22] 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, 電子情報通信学会論文誌 B, Vol.J83-B, No.11, pp.1565–1576 (2000).



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。