MIMO 固有ビーム空間分割多重伝送における秘密情報伝送

北野　隆康[†]　　岩井　誠人[†]　　笹岡　秀一[†]

Secret Information Transmission in MIMO Eigenbeam-Space Division Multiplexing

Takayasu KITANO[†], Hisato IWAI[†], and Hideichi SASAOKA[†]

あらまし　無線通信におけるセキュリティ技術の一つとして，MIMO 固有ビーム空間分割多重伝送のシステム構成に基づく秘密情報伝送方式を提案する．提案方式は，固有ビーム空間分割多重伝送において，固有値の大きいパスを用いて秘密情報伝送を行い，固有値の小さいパスを盗聴局での受信を妨害する用途に用いることで秘密情報伝送を実現する．提案方式は，受信局には通常の固有ビーム空間分割多重伝送の受信機を使用することが可能であり，システム全体としては送信局の構成のみを変更するだけで秘密情報伝送が実現可能であるという利点がある．この方式について計算機シミュレーションを行って性能を評価したところ，秘密情報伝送が可能であることが確認できた．

キーワード　情報セキュリティ，秘密情報伝送，MIMO，固有ビーム空間分割多重

1. まえがき

近年の無線通信の普及に伴い，無線通信のセキュリティ対策が重要となっている．無線通信における盗聴対策としては，共通鍵暗号方式を用いて暗号通信を行うことが一般的である．共通鍵暗号方式は，第三者には秘密の情報（以下，秘密情報と呼ぶ）に対して，送信局と受信局で同じ秘密鍵を用いて暗号化と復号を行う方式で，暗号化した情報を伝送することで秘密情報の安全性を保つことができる．この方式は，秘密通信が容易であるという利点がある一方で，秘密鍵を第三者に知られないように共有し，管理する必要がある．秘密鍵の共有手法として，現在は公開鍵暗号方式を用いた秘密鍵の直接配送により共有することが一般的であるが，公開鍵暗号方式は計算量の複雑性に基づく方式であるため，消費電力に制限のある移動通信に適用するには計算量の点で課題が残る．

この課題を解決する一手法として，電波伝搬特性に基づいた秘密鍵共有 [1]〜[14] が提案されている．電波伝搬に基づく秘密鍵共有手法には，大きく分けて，秘密鍵を二つの無線局において何らかの共有情報に基づいて個別に生成する方法 [1]〜[5] と，秘密通信方式により秘密鍵を安全に配送する方法 [7]〜[14] の 2 種類が提案されている．前者は，電波伝搬特性に基づく秘密鍵共有方式として提案されているように，電波伝搬の可逆性と電波伝搬の場所依存性といった電波伝搬の特徴 [15], [16] に基づいて，秘密情報の送信局と受信局で電波伝搬特性に基づいた秘密鍵を生成し共有する方式である．一方，秘密通信方式は，Wyner の盗聴モデル [7] や放送型盗聴通信路モデル [8] などに代表されるように，伝送特性を活用して，安全に秘密情報を伝送する方法である．

電波伝搬特性に基づく秘密鍵共有方式では，電波伝搬特性に基づいて秘密鍵を生成するという観点で実用化が容易であるが，秘密情報をそのまま伝送できないという課題がある．これに対して，秘密通信方式は，秘密情報をそのまま伝送できる利点があるが，無線通信における自然現象に基づくだけでは実現が困難である [17]．本論文では，秘密通信方式に分類される方式を対象とする．

秘密通信方式に関して，筆者らは以前に，複数アンテナからの干渉波送信制御を用いた秘密通信方式を提案した [14]．この方式は，送信局が複数アンテナを有するシステムにおいて，秘密情報信号と干渉信号を同時に送信し，盗聴局での盗聴を妨害することで秘密情

[†] 同志社大学，京田辺市
Doshisha University, 1–3 Tatara Miyako-dani, Kyotanabe-shi, 610–0321 Japan

報伝送を実現する．ただし，干渉信号をそのまま送信するだけでは秘密情報の受信局に対しても干渉する可能性があるため，この方式では干渉信号の送信時に，受信局において複数の干渉信号を同時に受信することで干渉信号成分を打ち消すような制御を行う．これにより，受信局では秘密情報信号のみが受信され，盗聴局では秘密情報信号と干渉信号が合成された信号を受信することになるため，秘密情報伝送が実現できる．この方式については，文献 [14] において有効性を確認したが，1 系列の秘密情報信号を伝送するために多数のアンテナが必要であり，安全性を高めるためには，干渉信号により多くの電力を割り当てる必要があるなどの課題があった．

一方，複数アンテナを用いたシステムとして，近年 MIMO (Multi-Input Multi-Output) 伝送がよく用いられている．MIMO における秘密情報伝送方式に関する研究 [11]〜[13] もなされてはいるが，理論的な実現の可能性に関するものが多く，実際のシステムに適用する具体的な方法については示されていない，あるいは，システム全体を秘密情報伝送専用のものに変更する必要があるなど，実際のシステムに適用するには課題もあった．

本論文では，MIMO 伝送に着目し，MIMO 固有ビーム空間分割多重伝送 (Eigenbeam-Space Division Multiplexing; E-SDM) [18] のシステム構成に基づく秘密情報伝送方式を提案する．提案方式は，固有ビーム空間分割多重伝送において，固有値の大きなパスで秘密情報を伝送し，固有値の小さなパスでは盗聴を妨害するよう作用させることで秘密情報伝送を実現する．更に提案方式では，送信局が秘密情報信号を送信する際に受信処理を考慮した制御を行って信号を送信するため，受信局にハードウェアの追加や改造をすることなく秘密情報伝送が実現できるという利点をもつ．

本論文では，計算機シミュレーションにより提案方式の性能を評価し，その有効性を示す．

2. 固有ビーム空間分割多重伝送における盗聴通信路

2.1 放送型盗聴通信路モデル

秘密情報伝送の最も基本的な形として，図 1 のような放送型の盗聴通信路モデル [8] がある．放送型盗聴通信路モデルは，送信局と受信局が情報伝送を行うシステムにおいて盗聴局が存在する場合に，送信局と受信局の間での秘密情報伝送の理論的実現性を示すものである．送信局と受信局との間のチャネルの容量 C が盗聴局でのチャネル容量 C_w を上回る場合に，送信局が $C \geq R > C_w$ を満たす伝送レート R で情報伝送を行うと，その情報が盗聴局に盗聴されることなく秘密情報伝送が可能となる．

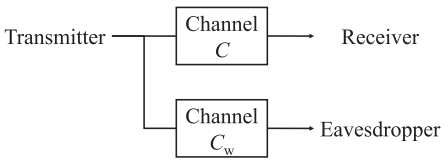


図 1 放送型盗聴通信路モデル
Fig. 1 Tapping model in wireless system.

これにより秘密情報伝送が理論的に可能であることは示されるが，無線通信における雑音やフェージングなどの自然現象に依存するだけでは常に $C > C_w$ になるとは限らず，そのままでは秘密情報伝送が十分であるとはいえない．無線通信において秘密情報伝送を実現するためには，$C > C_w$ の実現性を高める補助的な要素を加える必要がある．

2.2 固有ビーム空間多重伝送における盗聴モデル

無線通信における秘密情報伝送の実現法の一つとして，送信局でチャネル情報が既知であるシステムを想定し，受信局に有利となるようチャネルに応じた送信制御を行うことで秘密情報伝送を実現することが考えられる．そこで，MIMO 伝送において送受信局でチャネル情報が既知であるという前提でビームフォーミングを行う固有ビーム空間分割多重伝送に着目し，固有ビーム空間分割多重伝送構成に基づく秘密情報伝送の実現に関する基本的な特性を調べる．

まず，通常の固有ビーム空間分割多重伝送を用いる場合のチャネル容量を示し，その場合における秘密情報の伝送性能を評価する．固有ビーム空間分割多重伝送において盗聴局が存在するモデルとして，図 2 に示すように，送信局と受信局の他に盗聴局が存在する環境を想定する．なお，送信アンテナと受信アンテナはそれぞれ N，M 本であるとし，N と M の小さい方の値を $K(K = \min(M, N))$ とする．

ここで，送信局と受信局の間のチャネルを $\mathbf{H}$ とし，その相関行列 $\mathbf{H}^{\mathrm{H}} \cdot \mathbf{H}$ を固有値分解すると，固有ベクトル $\mathbf{e}$ が得られる．

$$\mathbf{H}^{\mathrm{H}} \cdot \mathbf{H} = \mathbf{e} \cdot \mathbf{\Lambda} \cdot \mathbf{e}^{\mathrm{H}} \tag{1}$$

ただし，$\mathbf{\Lambda}$ は次式のように固有値 $\lambda_1, \lambda_2, \cdots, \lambda_K (\lambda_1 \geq$

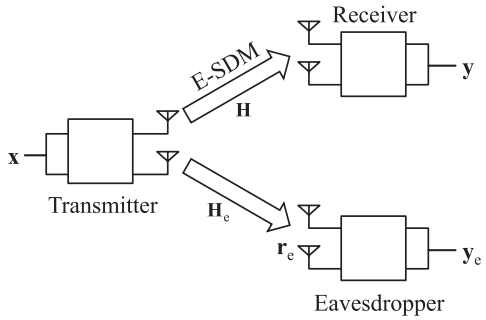


図 2　固有ビーム空間分割多重伝送における盗聴モデル
Fig. 2　Tapping model in MIMO E-SDM system.

$\lambda_2 \geq \cdots \geq \lambda_K$) を対角要素にもつ対角行列とする．

$$\mathbf{\Lambda} = \begin{bmatrix} \lambda_1 & & & \mathbf{0} \\ & \lambda_2 & & \\ & & \ddots & \\ \mathbf{0} & & & \lambda_K \end{bmatrix} \tag{2}$$

一般的な固有ビーム空間分割多重伝送では，固有ベクトルに基づいた重み付けによりビームフォーミングを行う．つまり，送信信号系列を $\mathbf{x}$，受信信号系列を $\mathbf{y}$ とし，雑音が発生しないような環境を想定すると，固有ビーム空間分割多重伝送は次式のように表される．

$$\begin{aligned} \mathbf{y} &= (\mathbf{H} \cdot \mathbf{e})^{\mathrm{H}} \cdot \mathbf{H} \cdot \mathbf{e} \cdot \mathbf{x} \\ &= \mathbf{\Lambda} \cdot \mathbf{x} \end{aligned} \tag{3}$$

一方，盗聴局では，受信信号を $\mathbf{r}_{\mathrm{e}}$ とすると，チャネル $\mathbf{H}_{\mathrm{e}}$ が受信局でのチャネル $\mathbf{H}$ とは異なる ($\mathbf{H}_{\mathrm{e}} \neq \mathbf{H}$) ため，

$$\mathbf{r}_{\mathrm{e}} = \mathbf{H}_{\mathrm{e}} \cdot \mathbf{e} \cdot \mathbf{x} \tag{4}$$

となり，盗聴局はこの受信信号をもとに $\mathbf{y}_{\mathrm{e}}$ を取り出し，情報の盗聴を試みるものとする．

本論文では，盗聴に対する性能の評価のため，盗聴局に有利な条件を仮定する．すなわち，盗聴局でも自身のチャネル $\mathbf{H}_{\mathrm{e}}$ と，受信局でのチャネル $\mathbf{H}$ を知っており，送信重みである固有ベクトル $\mathbf{e}$ を算出することが可能であるとする．盗聴局はこの条件の下で受信信号に対して MLD (Maximum Likelihood Detection) を行うことで盗聴を試みる．具体的には，盗聴局では，$\mathbf{e}$ を含めた送信信号系列候補 $\hat{\mathbf{x}}$ のレプリカ $\mathbf{e} \cdot \hat{\mathbf{x}}$ と受信信号系列とのメトリック μ を次式のように計算し，メトリック μ が最小となる送信信号系列の候補 $\hat{\mathbf{x}}$ を送信された系列として採用する．

$$\mu = ||\mathbf{r}_{\mathrm{e}} - \mathbf{H}_{\mathrm{e}} \cdot \mathbf{e} \cdot \hat{\mathbf{x}}|| \tag{5}$$

盗聴局で受信局でのチャネル $\mathbf{H}$ を知っているという前提は，固有ビーム空間分割多重におけるチャネル情報を，暗号化しないで公開通信路を用いて共有する場合に十分に想定される．

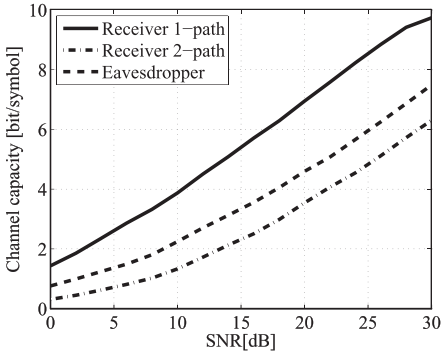


図 3　パスごとのチャネル容量
Fig. 3　Channel capacity per path.

2.3　固有パスごとのチャネル容量

ここでは，一般的な固有ビーム空間分割多重伝送におけるパスごとのチャネル容量から，固有ビーム空間分割多重伝送において秘密情報を伝送する場合の秘密情報の安全性を示す．

まず送信局と受信局との間において，式 (3) のような一般的な固有ビーム空間分割多重伝送により情報伝送を行い，盗聴局が MLD によりその情報の盗聴を試みることを想定する．伝送環境は，送受信アンテナ数がそれぞれ 2 本ずつの 2×2 MIMO チャネルとし，チャネル行列 $\mathbf{H}, \mathbf{H}_{\mathrm{e}}$ の要素である各チャネルがそれぞれ独立なレイリー分布に従う i.i.d. チャネル (independent identically distributed channel) であると仮定する．以上の環境において，受信局での固有パスごとの平均チャネル容量と，盗聴局での平均チャネル容量を図 3 に示す．盗聴局では MLD を用いることを想定しているため，第 1 パスと第 2 パスには区別がなく同じ特性となる．ここで，SNR (Signal-to-Noise Ratio) はアンテナ 1 本当りの受信電力に対する雑音電力比で定義し，平均チャネル容量 C は，変調方式に QAM を用いて，その変調多値数に応じて 1 シンボル当りに送信されるビット数 b_t と，そのビット誤り率 $p_e(b_t)$ により次式で表されるものを用いる．

$$C = \max_{b_t}(b_t \cdot (1 - p_e(b_t))) \tag{6}$$

なお，図 3 は平均チャネル容量を示しており，瞬時的なチャネル容量特性ではない．しかし，チャネルのフェージング変動が十分に豊富である場合や長時間にわたって秘密情報伝送を行う場合を想定すると，その特性は平均特性に収束する [10]．秘密情報伝送の基本的な特性の評価のため，本論文では平均特性を用いることにする．

図 3 より，固有値の大きい第 1 パスでは，受信局と盗聴局の SNR が同じ場合には，盗聴局のチャネル容量に比べて受信局のチャネル容量が大きくなることが分かる．一方，固有値の小さい第 2 パスでは，受信局のチャネル容量が盗聴局での容量を下回っている．この結果は，受信局と盗聴局が同じ SNR である場合に，第 1 パスを用いて伝送を行うと，**2.1** に示した $C > C_w$ の条件が満たされ，秘密情報伝送が可能であることを示している．しかし，実際の無線伝送環境を考慮すると，必ずしも受信局と盗聴局が同じ SNR とはならず，盗聴局の SNR が受信局での SNR を大きく上回ることは十分にあり得ることである．図 3 においても，盗聴局の SNR が受信局の SNR に比べて約 8 dB 以上良好な場合は，$C \leq C_w$ となり，このような環境下では秘密情報伝送が不可能である．そこで，秘密情報伝送を実現するためには，盗聴局での SNR にかかわらず秘密情報伝送が可能であることが必要である．

なお，図 3 では 2×2 MIMO チャネルにおける結果を示したが，アンテナ本数を増やした $(M \times N)$ 場合も同様に，同じ SNR の環境では，固有値が相対的に大きいパス（その数：1 または複数）で受信局のチャネル容量が盗聴局のチャネル容量を上回り，固有値が小さいパスでは盗聴局のチャネル容量を下回ると考えられる．

3. 固有ビーム空間分割多重伝送システムに基づく秘密情報伝送

3.1 固有ビーム空間分割多重伝送システムに基づく秘密情報伝送の概要

前章に示したように，送信局と受信局の間で通常の固有ビーム空間分割多重伝送を行う場合，固有値の大きいパスでは盗聴局に比べて大きいチャネル容量を得ることができるが，盗聴局の SNR が大きい場合を想定すると秘密情報伝送が困難である．そこで，本論文では，固有値の大きいパスを用いて秘密情報伝送を行い，固有値の小さいパスでは，盗聴局における MIMO 受信の直交性を崩すような処理を行うことで盗聴局での受信を妨害するような制御を同時に行う秘密情報伝送方式を提案する．これを実現するために，本提案方式では，固有ビーム空間分割多重伝送における送信重みに注目して，これまでとは異なる送信重みを用いる．

一般の形である $M \times N$ MIMO チャネルを想定し，秘密情報伝送に用いる送信重み行列を $\mathbf{w}_{\mathrm{t}}$ とすると，受信局での受信信号 $\mathbf{y}$ は，

$$\mathbf{y} = (\mathbf{H} \cdot \mathbf{e})^{\mathrm{H}} \cdot \mathbf{H} \cdot \mathbf{w}_{\mathrm{t}} \cdot \mathbf{x} \tag{7}$$

となる．ここで，式の簡易化のため，チャネル行列 $\mathbf{H}$ と受信側での処理をまとめて

$$\mathbf{A} = (\mathbf{H} \cdot \mathbf{e})^{\mathrm{H}} \cdot \mathbf{H} \tag{8}$$

と表す．このとき，固有値の大きいパスでのみ情報伝送を行うには，送信重み $\mathbf{w}_{\mathrm{t}}$ が

$$\mathbf{A} \cdot \mathbf{w}_{\mathrm{t}} = \begin{bmatrix} \mathbf{\Lambda_1} & \mathbf{0} \\ \mathbf{P} & \mathbf{Q} \end{bmatrix} \tag{9}$$

を満たすようにすればよい．なお，式 (9) 中の $\mathbf{\Lambda_1}$ は，秘密情報伝送に使用するパスの固有値行列であり，また，$\mathbf{P}, \mathbf{Q}$ は，盗聴局による盗聴を妨害するために作用させることを目的とする要素である．式 (9) を満たす送信重み $\mathbf{w}_{\mathrm{t}}$ を用いて送信信号系列 $\mathbf{x}$ を送信し，受信局では一般的な固有ビーム空間分割多重伝送と同じ方法で受信するものとする．この場合の受信信号 $\mathbf{y}$ は，

$$\begin{aligned} \mathbf{y} &= (\mathbf{H} \cdot \mathbf{e})^{\mathrm{H}} \cdot \mathbf{H} \cdot \mathbf{w}_{\mathrm{t}} \cdot \mathbf{x} \\ &= \begin{bmatrix} \mathbf{\Lambda_1} & \mathbf{0} \\ \mathbf{P} & \mathbf{Q} \end{bmatrix} \cdot \mathbf{x} \end{aligned} \tag{10}$$

となる．これより，$\mathbf{\Lambda_1}$ に相当するパスでは，一般的な固有ビーム空間分割多重伝送と同じような伝送が可能であることが分かる．一方，それ以外の固有値の小さいパスに該当するパスでは，受信局でも復調が困難であるが，これらのパスの情報は盗聴妨害用途で使用することが前提であり秘密情報伝送には用いないため，正しく受信する必要はない．つまり，式 (9) の送信重み $\mathbf{w}_{\mathrm{t}}$ を用いる場合，システム全体としては送信局での重みのみを変更するだけでよく，受信局では一般的な固有ビーム空間分割多重伝送と同じ受信機で受信可能である．

送信重みを決定する際には式 (9) のみを満たせばよいため，本論文では，式 (9) を送信重みが満たす条件と呼ぶ．なお，盗聴対策としては，式 (9) の要素 $\mathbf{P}$ のみで盗聴を妨害する効果が得られるが，本論文ではより一般的な表現を考慮し，式 (9) のように $\mathbf{P},\mathbf{Q}$ の二つの要素を用いた形で表す．

3.2 送信重み

送信重みの候補として，式 (8) の逆行列に相当する行列を求め，それに基づいて送信重みを生成すると，式 (9) の条件を満たすことができると考えられる．このような送信重みの候補として，次式のものが挙げられる．

$$\mathbf{w}_{\mathrm{t}} = (\mathbf{H}^{\mathrm{H}} \cdot \mathbf{H})^{-1} \cdot \mathbf{e} \cdot \mathbf{L} \tag{11}$$

式 (11) の送信重み $\mathbf{w}_{\mathrm{t}}$ を式 (9) の左辺に代入すると，

$$\begin{aligned}\mathbf{A} \cdot \mathbf{w}_{\mathrm{t}} &= (\mathbf{H} \cdot \mathbf{e})^{\mathrm{H}} \cdot \mathbf{H} \cdot \mathbf{w}_{\mathrm{t}} \\ &= \mathbf{e}^{\mathrm{H}} \cdot \mathbf{H}^{\mathrm{H}} \cdot \mathbf{H} \cdot (\mathbf{H}^{\mathrm{H}} \cdot \mathbf{H})^{-1} \cdot \mathbf{e} \cdot \mathbf{L} \\ &= \mathbf{e}^{\mathrm{H}} \cdot \mathbf{e} \cdot \mathbf{L} \\ &= \mathbf{L}\end{aligned} \tag{12}$$

となる．ただし，式 (12) では，固有ベクトルの特徴である，$\mathbf{e}^{\mathrm{H}} \cdot \mathbf{e}$ が単位行列になることを利用した．

ここで，式 (12) が式 (9) の条件を満たすには，$\mathbf{L}$ を

$$\mathbf{L} = \begin{bmatrix} \boldsymbol{\Lambda_1} & \mathbf{0} \\ \mathbf{P} & \mathbf{Q} \end{bmatrix} \tag{13}$$

と設定すればよい．

以上より，送信重み $\mathbf{w}_{\mathrm{t}}$ は，

$$\mathbf{w}_{\mathrm{t}} = (\mathbf{H}^{\mathrm{H}} \cdot \mathbf{H})^{-1} \cdot \mathbf{e} \begin{bmatrix} \boldsymbol{\Lambda_1} & \mathbf{0} \\ \mathbf{P} & \mathbf{Q} \end{bmatrix} \tag{14}$$

と表される．

式 (14) の送信重み $\mathbf{w}_{\mathrm{t}}$ は，行列 $\mathbf{P},\mathbf{Q}$ の各要素の値によらず式 (9) が成り立つ．行列 $\mathbf{P},\mathbf{Q}$ は，送信局と受信局との間で共有しておく必要がなく，送信局が任意に設定可能な値を要素にもつ行列である．ただし，実際にこの重みを使用して情報伝送を行う場合は，$\mathbf{P},\mathbf{Q}$ の値の変化に伴って送信電力が大きく変化してしまう．そのため，実際の伝送時には，$\mathbf{w}_{\mathrm{t}}$ のノルム $||\mathbf{w}_{\mathrm{t}}||$ が一定になるように正規化して伝送する必要がある．ただし，本章では原理的な説明のため，$\mathbf{w}_{\mathrm{t}}$ を正規化しない形で議論を進める．

3.3 盗聴局での受信と盗聴耐性の向上

式 (14) の重みを用いて情報伝送を行う場合に，盗聴局での受信信号 $\mathbf{r}_{\mathrm{e}}$ は次式のようになる．

$$\begin{aligned}\mathbf{r}_{\mathrm{e}} &= \mathbf{H}_{\mathrm{e}} \cdot \mathbf{w}_{\mathrm{t}} \cdot \mathbf{x} \\ &= \mathbf{H}_{\mathrm{e}} \cdot (\mathbf{H}^{\mathrm{H}} \cdot \mathbf{H})^{-1} \cdot \mathbf{e} \cdot \begin{bmatrix} \boldsymbol{\Lambda_1} & \mathbf{0} \\ \mathbf{P} & \mathbf{Q} \end{bmatrix} \cdot \mathbf{x}\end{aligned} \tag{15}$$

ここで，式の簡易化のため，

$$\mathbf{B} = \begin{bmatrix} \mathbf{B}_{11} & \mathbf{B}_{12} \\ \mathbf{B}_{21} & \mathbf{B}_{22} \end{bmatrix} = \mathbf{H}_{\mathrm{e}} \cdot (\mathbf{H}^{\mathrm{H}} \cdot \mathbf{H})^{-1} \cdot \mathbf{e} \tag{16}$$

とし，送信信号系列 $\mathbf{x}$ を $\mathbf{x} = [\mathbf{x}_1 \quad \mathbf{x}_2]^{\mathrm{T}}$ とすると，受信信号は，

$$\begin{aligned}\mathbf{r}_{\mathrm{e}} &= \begin{bmatrix} \mathbf{B}_{11} & \mathbf{B}_{12} \\ \mathbf{B}_{21} & \mathbf{B}_{22} \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{\Lambda_1} & \mathbf{0} \\ \mathbf{P} & \mathbf{Q} \end{bmatrix} \cdot \mathbf{x} \\ &= \begin{bmatrix} \mathbf{B}_{11} \cdot \boldsymbol{\Lambda}_1 + \mathbf{B}_{12} \cdot \mathbf{P} & \mathbf{B}_{12} \cdot \mathbf{Q} \\ \mathbf{B}_{21} \cdot \boldsymbol{\Lambda}_1 + \mathbf{B}_{22} \cdot \mathbf{P} & \mathbf{B}_{22} \cdot \mathbf{Q} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} \\ &= \begin{bmatrix} (\mathbf{B}_{11} \cdot \boldsymbol{\Lambda}_1 + \mathbf{B}_{12} \cdot \mathbf{P}) \cdot \mathbf{x}_1 + \mathbf{B}_{12} \cdot \mathbf{Q} \cdot \mathbf{x}_2 \\ (\mathbf{B}_{21} \cdot \boldsymbol{\Lambda}_1 + \mathbf{B}_{22} \cdot \mathbf{P}) \cdot \mathbf{x}_1 + \mathbf{B}_{22} \cdot \mathbf{Q} \cdot \mathbf{x}_2 \end{bmatrix}\end{aligned} \tag{17}$$

と表される．

このとき，式 (17) の $\boldsymbol{\Lambda}_1$ と $\mathbf{B}$ の各要素 $\mathbf{B}_{ij}(i,j = 1,2)$ は，送信局と受信局のチャネル $\mathbf{H}$，あるいは，$\mathbf{H}$ と盗聴局でのチャネル $\mathbf{H}_{\mathrm{e}}$ によって一意に決まるものであり，盗聴局でも知ることができる．しかし，$\mathbf{P},\mathbf{Q}$ の各要素は送信局で独自に決定でき，受信局を含めた他局には公開されないため，盗聴局ではこれらの値を知ることができない．盗聴局で $\mathbf{P},\mathbf{Q}$ を知ることができない場合は，盗聴局が行う MLD が困難になり，秘密情報の安全性が保たれると考えられる．

しかし，常に $\mathbf{P},\mathbf{Q}$ の各要素に同じ値を設定して情報伝送を行うと，盗聴局でも長期にわたって同じ重みを掛けられた信号を受信することになるため，盗聴局が受信した系列を詳細に分析することにより $\mathbf{P},\mathbf{Q}$ の値が推測できる可能性がある．これに対しては，$\mathbf{P},\mathbf{Q}$ の各要素の値を送信局が任意に決定できることを活用し，一定時間ごとに異なる値を設定することで対策を行う．例えば，情報 1 シンボルごとに $\mathbf{P},\mathbf{Q}$ に異なる値を用いて伝送すると，盗聴局でこれらの値を推測することが困難になり，MLD による盗聴も，より困難

なものとなる．これは，文献 [14] で使用されている盗聴耐性向上手法と同様の手法である．

4. 計算機シミュレーション

4.1 シミュレーションシステム

提案方式の有効性を計算機シミュレーションにより確認する．シミュレーションモデルは，図 2 と同様に，送信局と受信局間で提案方式による情報伝送を行い，盗聴局が MLD によりその情報の盗聴を試みているとする．このとき，盗聴局は自身のチャネル $\mathbf{H}_{\mathrm{e}}$ だけでなく，送信局と受信局との間のチャネル $\mathbf{H}$，及びその結果として得られる固有ベクトル $\mathbf{e}$ も知っているものとして，式 (5) の MLD を行う．

ここでは，固有ビーム空間分割多重伝送における秘密情報伝送の有効性を基本的な環境で評価するため，送受信アンテナ数がそれぞれ 2 本ずつの 2×2 MIMO チャネルで，各チャネルは相互に独立に変動するレイリー分布に従う i.i.d. チャネルであるとする．また，変調方式には QPSK を用いる．なお，本論文ではシングルキャリヤ伝送を想定したシミュレーションにより提案方式を評価するが，OFDM などのマルチキャリヤ伝送においても各サブキャリヤごとに提案方式を適用することで同じ結果が得られると考えられる．

ここで，2×2 MIMO チャネルを想定する場合に，式 (14) の送信重み $\mathbf{w}_{\mathrm{t}}$ は，

$$\mathbf{w}_{\mathrm{t}} = (\mathbf{H}^{\mathrm{H}} \cdot \mathbf{H})^{-1} \cdot \mathbf{e} \cdot \begin{bmatrix} \lambda_1 & 0 \\ p & q \end{bmatrix} \tag{18}$$

と表される．p, q の値の設定は任意であるが，本論文では，p, q の値に複素数を想定し，その値を 1 シンボルごとに変化させるものとする．また，p, q の実部と虚部には，それぞれ平均が 0 で標準偏差が σ の互いに独立な正規乱数を用いる．

4.2 相互情報量

提案方式の安全性を相互情報量 [19] を用いて評価する．ここでは，評価指標としての相互情報量について述べる．

2 値の送信情報を $X = \{0, 1\}$，受信情報を $Y = \{0, 1\}$ とし，それぞれのエントロピーを $H(X)$, $H(Y)$ とする．また，Y を知っているという条件で依然として残る X のエントロピーが条件付きエントロピーであり，$H(Y|X)$ と表される．このとき，受信局で得ることができる情報量が相互情報量 $I(X;Y)$ であり，次式のように表される．

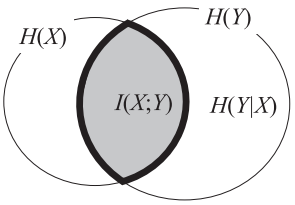


図 4 相互情報量
Fig. 4 Concept of mutual information.

$$I(X;Y) = H(Y) - H(Y|X) \tag{19}$$

これらの概念を図示すると図 4 のように表される．相互情報量 $I(X;Y)$ は，X と Y の符号に偏りがない場合には，X と Y のビット誤り率 P_{e} により

$$I(X;Y) = 1 + P_{\mathrm{e}} \log_2(P_{\mathrm{e}}) + (1 - P_{\mathrm{e}}) \log_2(1 - P_{\mathrm{e}}) \tag{20}$$

と表される [14], [19]．

相互情報量は，送信情報に対して受信局が得られる情報量を示しており，送信情報がすべて正しく受信された場合に 1 となるものである．つまり，秘密情報伝送の性能評価として相互情報量を用いる場合は，受信局では 1 に近づくことが望ましく，盗聴局での受信（傍受）の場合は 0 に近い値であることが望ましい．なお，盗聴局で相互情報量が 1 になる場合は，盗聴局ですべての送信情報が得られることになり，秘密情報伝送を行う上で不適である．一方，受信局では，相互情報量が 1 にならない場合でも，各種誤り訂正技術を用いることで正確な情報伝送を行うことができる．ただし，この場合は，盗聴局でも誤り訂正のために公開された情報の利用が可能であるため，盗聴局で得られる情報量も多くなる．そのため，秘密情報伝送の評価に相互情報量を用いる場合は，受信局と盗聴局の相互情報量の差が重要となる．

本論文では，具体的な変調方式を想定し，式 (20) で示されるようなビット誤り率から算出される相互情報量を用いて耐盗聴性能を評価する．

4.3 送信重みのパラメータと安全性の評価

ここでは，式 (18) の送信重み $\mathbf{w}_{\mathrm{t}}$ における任意の値 p, q と，受信局と盗聴局で得られる相互情報量との関係を示し，提案方式の送信重みのパラメータと秘密情報の安全性の関係を調査する．ここでのシミュレーションでは，受信局で SNR が 10 dB，20 dB，30 dB の雑音が発生し，盗聴局では雑音が発生しないという

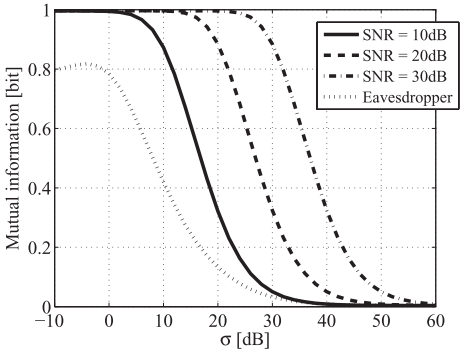
環境を想定する．なお，盗聴局で雑音が発生しない環境を想定しているが，これは，耐盗聴性能の下限を評価するという目的のため，盗聴局に有利な環境を設定している．

ここで，$||\mathbf{w}_t|| = 1$ となるように重みの大きさを制御することを想定する．この条件における，p, q の標準偏差 σ に対する受信局と盗聴局での相互情報量特性を図 5 (a) に示す．なお，σ は，p の絶対値の平均 $|\bar{p}|$ と q の絶対値の平均 $|\bar{q}|$ の和がチャネルの第 2 固有値 λ_2 と等しくなる場合，すなわち，$|\bar{p}| + |\bar{q}| = \lambda_2$ となる場合を基準 (0 dB) とする．図 5 (a) より，受信局での相互情報量は盗聴局での相互情報量を上回っていることが確認できる．また，σ が小さい値では受信局と盗聴局でともに相互情報量が大きくなり，σ が大きい領域では受信局と盗聴局の両方で相互情報量が小さくなっていることから，受信局での受信性能と盗聴局に対する盗聴耐性はトレードオフの関係であるといえる．なお，図 5 (a) では，σ が一定以上になると受信局の相互情報量も小さくなるが，これは送信重み $\mathbf{w}_t$ が $||\mathbf{w}_t|| = 1$ で一定となるよう設定されているため，σ が大きくなるにつれて第 2 パスに割り当てられる電力が大きくなり，結果として第 1 パスに割り当てられる電力が小さくなることが影響している．

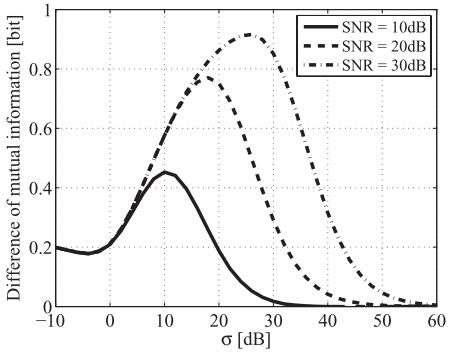
図 5 (b) に，受信局と盗聴局での相互情報量の差を示す．図 5 (b) より，SNR が小さい場合と SNR が比較的大きい場合を比較すると，SNR が小さい環境ほど相互情報量の差が最大になる σ の値も小さくなっている．SNR に応じて適切な σ の値が存在するが，SNR が 10〜30 dB の環境では，σ を 10 dB に設定すると 0.4 以上の相互情報量差が得られることを確認できる．

4.4 相互情報量による安全性の評価

最後に p, q の正規化標準偏差 σ を 10 dB，20 dB，30 dB で固定する場合の，SNR に対する受信局の相互情報量特性と盗聴局での相互情報量特性，受信局と盗聴局の相互情報量差を図 6 に示す．なお，アンテナ 1 本当りの受信電力に対する雑音電力比を SNR としており，ここでも盗聴局で雑音が発生しない環境を想定している．



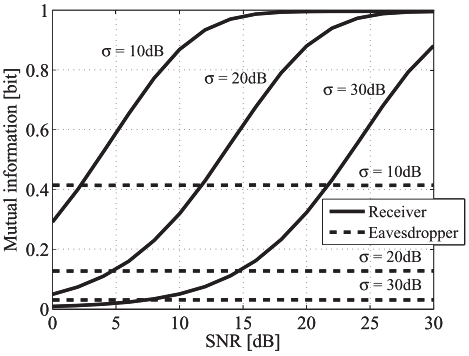
(a) 受信局と盗聴局での特性



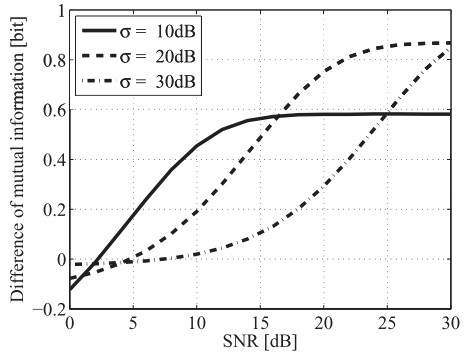
(b) 受信局と盗聴局での相互情報量の差

図 5　σ に対する相互情報量特性

Fig. 5　Mutual information as a function of σ.



(a) 受信局と盗聴局での特性



(b) 受信局と盗聴局での相互情報量の差

図 6　SNR に対する相互情報量特性

Fig. 6　Mutual information as a function of SNR.

図 6 (a) より，受信局での相互情報量特性は，σ を小さい値に設定するほど低 SNR 環境でも大きい相互情報量が確保できることが分かる．例えば，相互情報量が 0.9 の場合で比較すると，σ が 10 dB と 20 dB の場合で，SNR にして約 10 dB の差がある．受信局と盗聴局の相互情報量差は，図 6 (b) に示すように σ の値が大きいほど高 SNR 環境での差が広がっている．一方，低 SNR 環境で σ の値が小さい場合は，受信局での相互情報量が確保できないため，相互情報量の差が小さくなっている．

実際の秘密情報伝送を考えると，伝送する秘密情報が盗聴されないことを優先すべきである．秘密情報を安全に伝送するという観点では，通信環境が，秘密情報伝送を確実に保証するような状況である場合は秘密情報伝送を行い，必ずしも保証されないような状況下では秘密情報伝送を中止するような制御を行うことが望ましい．つまり，秘密情報の安全な伝送という観点では，以下のような制御を行うことが適切であると考えられる．

受信局と盗聴局での相互情報量差と情報伝送に用いる誤り訂正の性能を考慮して，受信局での相互情報量が 1 となり，盗聴局では 1 にはならないような SNR のしきい値を求める．そして，実際に伝送を行う環境での SNR がしきい値以上である場合は秘密情報伝送を行い，しきい値以下になる場合は秘密情報伝送を行わないというような送信制御を行うことで，安全な秘密情報伝送が実現可能となると考えられる．

5. むすび

無線通信におけるセキュリティ対策として，MIMO 固有ビーム空間分割多重伝送のシステム構成に基づく秘密情報伝送を提案し，その性能を評価した．提案方式では，固有値の大きいパスで秘密情報伝送を行い，固有値の小さいパスを用いて盗聴を妨害することで秘密情報の安全性を向上させている．また，提案方式は，一般的な固有ビーム空間分割多重伝送方式の受信機構成を考慮した送信重みを用いているため，固有ビーム空間分割多重伝送の送信重みを変更するだけで秘密情報伝送が可能になるという利点がある．

本論文では，送信重みがもつパラメータを変化させる場合の性能を比較し，秘密情報伝送に適した重みを用いることで秘密情報伝送が可能になることを示した．今回想定した MIMO 環境は，送信アンテナ，受信アンテナとも 2 本ずつの環境を想定して評価を行ったが，より多くの送受信アンテナを有する環境に適した重みについては，今後の課題である．

また，本論文では MLD が最適な盗聴手法であるとして提案方式を評価したが，空間フィルタリングなど他の受信方法を用いる場合や，独立成分分析などを用いて能動的な盗聴を試みる場合についても評価する必要がある．これらの盗聴手法の提案，及び，安全性評価も今後の課題である．

謝辞 本研究は科学研究費補助金基盤研究 (C)（課題番号 22560397）の助成を受けたものである．

文　献

[1] J.E. Hershey, A.A. Hassan, and R. Yarlagadda, “Unconventional cryptographic key variable management,” IEEE Trans. Commun., vol.43, no.1, pp.3–6, Jan. 1995.

[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 Propag., vol.53, no.11, pp.3776–3784, Nov. 2005.

[3] 青野智之，樋口啓介，大平　孝，小宮山牧兒，笹岡秀一，“エスパアンテナを用いた IEEE802. 15.4 無線秘密鍵共有システム，” 信学論（B），vol.J88-B, no.9, pp.1801–1812, Sept. 2005.

[4] 北浦明人，笹岡秀一，“陸上移動通信における OFDM の伝送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.

[5] 清水崇之，岩井誠人，笹岡秀一，“エスパアンテナを用いた秘密鍵共有方式における盗聴耐性の高い鍵生成法，” 信学論（B），vol.J92-B, no.9, pp.1348–1361, Sept. 2009.

[6] 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, Sept. 2007.

[7] A.D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol.54, no.8, pp.1334–1387, Oct. 1975.

[8] I. Csiszar and J. Korner, “Broadcast channels with confidential message,” IEEE Trans. Inf. Theory, vol.24, no.3, pp.339–348, May 1978.

[9] H. Yamamoto, “Information theory of cryptology,” IEICE Trans., vol.E74, no.9, pp.2456–2465, Sept. 1991.

[10] H. Koorapaty, A.A. Hassan, and S. Chennakeshu, “Secure information transmission for mobile radio,” IEEE Commun. Lett., vol.4, no.2, pp.52–55, Feb. 2000.

[11] A. Khisti, G. Womell, A. Wiesel, and Y. Eldar, “On the Gaussian MIMO wiretap channel,” IEEE International Symposium on Information Theory (ISIT2007), pp.2471–2475, 2007.

[12] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” IEEE International Symposium on Information Theory (ISIT2008),

pp.524–528, 2008.
[13] X. Li and E.P. Ratazzi, “MIMO Transmissions with information-theoretic secrecy for secret-key agreement in wireless networks,” Proc. IEEE Military Communications Conference (MILCOM’2005), vol.3, pp.1353–1359, Oct. 2005.
[14] 北野隆康，岩井誠人，笹岡秀一，“複数アンテナからの干渉波送信制御を用いた秘密通信方式,” 信学論（B），vol.J92-B, no.9, pp.1362–1372, Sept. 2009.
[15] W.C. Jakes, Microwave mobile communications, John Wiley & Sons, 1974.
[16] 唐沢好男，ディジタル移動通信の電波伝搬基礎，コロナ社，東京，2003.
[17] 今井秀樹，花岡吾一郎，“情報量的安全性に基づく暗号技術,” 信学論（A），vol.J87-A, no.6, pp.721–733, June 2004.
[18] 大鐘武雄，西村寿彦，小川恭孝，“MIMO チャネルにおける空間分割多重方式とその基本特性,” 信学論（B），vol.J87-B, no.9, pp.1162–1173, Sept. 2004.
[19] N. Abramson, Information Theory and Coding, McGraw-Hill, New York, 1963.

（平成 22 年 5 月 25 日受付，9 月 14 日再受付）

北野　隆康　（学生員）

平 18 同志社大・工・電気卒．平 20 同大大学院博士前期課程了．現在，同大学院博士後期課程在学中．ディジタル無線通信方式の研究に従事．IEEE 学生員．

岩井　誠人　（正員）

昭 62 京大・工・電気 II 卒．平元同大大学院修士課程了．同年国際電信電話（株）（KDD，現 KDDI（株））入社．衛星通信・陸上移動通信におけるアンテナ・伝搬及び無線伝送方式，ソフトウェア無線の研究に従事．平 8 米国 Univercity of California, San Diego (UCSD) Visiting Scholar．平 11 トヨタ自動車（株），米国 Telcordia Technologies 社 Visiting Researcher．平 13（株）トヨタ IT 開発センター．平 15 国際電気通信基礎技術研究所 (ATR) 適応コミュニケーション研究所．平 16 同志社大・工・助教授．無線通信における電波伝搬，ソフトウェア無線，アドホックネットワークに関する研究に従事．平 6 本会学術奨励賞，平 17，平 19 及び平 21 本会通ソ活動功労賞，平 20 本会論文賞受賞．情報学博士．IEEE 会員．

笹岡　秀一　（正員：フェロー）

昭 46 京都工繊大・工・電気卒，昭 48 京大大学院修士課程了．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．衛星通信方式，陸上移動通信の研究に従事．平 10 大阪電通大・工・教授．平 12 同志社大・工・教授．次世代陸上移動通信システム，ディジタル無線通信方式，変復調・符号化の研究に従事．平 20 本会論文賞受賞．工博．IEEE 会員．