Secret Information Transmission Scheme in MIMO System Using Time-variant Pre-coding

Hideichi SASAOKA*, Takuma TAKIMURA* and Hisato IWAI*

(Received December 28, 2015)

Recently, physical layer security technology such as secret key agreement and secret information transmission using radio propagation attracts attention in wireless communications. The authors proposed a MIMO system which applied signal dispersion and noise addition method as a secret information transmission scheme. However, this scheme is weak for the attack of the eavesdropper using independent component analysis (ICA). This paper generalized the earlier proposed method and derived the equivalent system using time-variant precoding. This paper also proposed the improvement method using the multi-level modulation and the update of reception antenna weight as a measure for the attack using ICA. As a result of computer simulation, it become clear that the proposed scheme has a satisfactory performance of bit error rate between authorized users and that the proposed scheme has a sufficient tolerance for the attack from eavesdropper.

Key words : secret information transmission, MIMO, precoding, ICA, physical layer security

キーワード：秘密情報伝送，MIMO，プリコーディング，独立成分分析，物理層セキュリティ

MIMO における時変化プリコーディングを用いた秘密情報伝送方式

笹岡秀一，瀧村拓馬，岩井誠人

１．はじめに

近年，携帯電話や無線 LAN など無線通信が広く普及し，利用者はその利便性を享受している．しかし，無線通信は開かれた空間を通して電波の送受を行うため，盗聴や不正アクセスなど情報セキュリティ面の脆弱性が問題となっている．この盗聴対策として，計算量的な複雑性を安全性の根拠とする暗号技術を使用することが一般的である．これに対して情報量的な複雑性を安全性の根拠とする暗号技術の理論的研究が行われている[1,2]．また，これより少し現実的な技術として，無線通信路特性を用いた秘密鍵共有[3,4]と秘密情報伝送[5]が提案されている．さらに，ここ数年，電波（物理層）における情報セキュリティ（所謂，Physical layer security）に対する関心が高まっている．

電波を用いた物理層セキュリティ技術としては，無線通信路特性を用いた秘密鍵共有と秘密情

*Department of Electronics, Doshisha University, Kyoto
Telephone: +81-774-65-6355, FAX: +81-774-65-6801, E-mail: hsasaoka@mail.doshisha.ac.jp

報伝送が代表的なものであり，各種の研究が行われている [6]．ここで，秘密鍵共有においては，電波伝搬特性の可逆性により得られた相関情報に基づき正規者間で秘密鍵を共有する一方，電波伝搬の場所依存性により盗聴者に対する安全性を確保している．一方，秘密情報伝送の研究は，Wyner の盗聴通信路モデル [7]や放送型盗聴通信路モデル [8]に始まるが，その原理は正規者間と正規者・盗聴者間の通信容量に格差をつけることである．しかし，より積極的には，通信路歪みや干渉等を活用して盗聴者に対して情報の正常受信が難しい状態に設定する一方，通信路歪みや干渉の場所依存性を活用して正規者間でそれらを軽減する制御を行うことで実現する．なお，秘密情報伝送の具体的な実現法は，通信システムと通信路に依存して各種のものがある [6]．そこで，以下では無線通信で広く用いられている MIMO (Multi-Input Multi-Output) システムなど複数アンテナを用いたシステムに対象を絞る．

MIMO システムでは，伝搬路において複数ストリーム（チャネル）間の干渉が発生するが，これを活用した秘密情報伝送の研究が行われている [9-11]．その原理は，チャネル間干渉により盗聴局の正常受信を困難とする一方，正規局間では空間分割多重化(Space Division Multiplexing)など送受信アンテナの重み付けにより各チャネルを直交化して高品質伝送を実現することである．これらの研究は，理論的な実現可能性に関するものが多く，実際のシステムに適用する場合の具体的な方法が十分に示されていない．これに対して，MIMO 固有ビーム空間分割多重 (Eigenbeam SDM: E-SDM) において，秘密情報伝送に用いないチャネルに積極的に盗聴を妨害する信号（時間変化する信号）を伝送する方式が提案されている [12]．一方，MIMO システムと異なるが類似点・共通点のあるものとして，複数ユーザや複数アンテナからの干渉波送信を用いた秘密情報伝送の研究が行われている [13-15]．

MIMO システムを用いたディジタルの秘密情報伝送の盗聴法とその盗聴耐性は，システムの設定条件に依存する．例えば，MIMO E-SDM を採用すると，プリコーディングが行われるが，その送信重みが盗聴局に未知の場合，盗聴者は最尤判定(MLD)受信などの高性能な受信方式を採用できない．しかし，プリコーディングが時間的に一定で変調諸元が既知の前提の下で，ブラインドでの空間フィルタリングによる受信が可能であり，多少の特性劣化があるものの秘密情報が得られる．このため，正規局と盗聴局の通信容量に大きな格差をつけることが難しい．これに対して，秘密信号を時変化する重み付けを行った後に各チャネルに分散させると共に，各チャネルにダミー信号（雑音）を付加して伝送し，受信側で秘密信号のみを取り出す秘密情報伝送方式が提案されている [16]．しかし，この方式は，受信処理を簡単化するために受信重みを時間的に一定に設定しているため，独立成分分析 (ICA: Independent Component Analysis) によるブラインド信号合成・干渉分離の攻撃を受け易い [16]．この問題は，受信重みを一定時間ごとに更新する手法を採用することで改善されると考えられる．しかし，この件について十分な検討が行われていない．

そこで本論文では，MIMO システムにおいて正規局間で各チャネルの直交関係を保ったままで，送信重みおよび受信重みを時間的に変化させて守秘性を向上させた秘密情報伝送方式を提案した．提案方式では，送信重みを短時間で（例えば，１シンボル単位で）変化させると共に，受信重みを一定時間毎（例えば，数シンボルから数十シンボル毎）に変更している．この提案方式は，既存方式 [16]と類似点が多いが，既存方式の構成法の改良と一般化を行っている．また，多様なシミュレーション結果を用いて総合的な検討を行っている．

２．MIMO システムにおける秘密情報伝送方式

2.1 チャネル間干渉を活用した従来方式の課題

MIMO システムにおける秘密情報伝送は，チャ

ネル間干渉を活用するものが多い．ここで，正規局間で各チャネル間に干渉がない方式を採用するのが一般的である．具体的には，送受信間での電波伝搬特性の共有に基づくMIMO E-SDMを用いる．一方，秘密情報伝送を行うチャネルのみを干渉なしとする方式も考えられる．しかし，この方式は，複数アンテナを用い干渉波を送信する方式と類似である．また，MIMOシステムに特徴的な方式と必ずしも言えない．そこで，今回の検討対象外とする．

MIMO E-SDMの場合，何らかの手段で送信側と受信側の双方で電波伝搬特性の情報を共有する必要がある．ここで，電波伝搬路特性の情報を受信側から公開通信路を介して送信側に帰還する場合，正規局の送信重み情報が盗聴局に既知となる．また，正規局・盗聴局間の電波伝搬特性が既知を十分な妥当性をもって想定できる．この場合には，盗聴局においてMLD受信が可能となるため，正規局間と正規局・盗聴局間の伝送品質（又は通信容量）の差異が少ない．なお，このようにMLD受信が可能となる一因は，送信重み付け前の各チャネル入力信号が独立なディジタル信号となっているためである．

一方，電波伝搬特性の情報を電波伝搬路の可逆性により送信側及び受信側で独自に取得する場合には，送信重みを盗聴局に未知にできる．この場合には，正規局・盗聴局間の電波伝搬特性が既知を前提としても，それのみでは空間フィルタリングを実施できない．しかし，送信重みを含めて伝搬路特性が未知の条件の下でブラインドの信号分離を実施すれば，特性劣化が多少起こっても信号の抽出が可能となる．ここで，盗聴局における特性劣化（又は通信容量の減少）の程度が問題となる．

2.2 信号分散を用いた伝送方式の構成と課題

2.2.1 基本構成

ここでは，MIMO E-SDMにおいて直交化のための送信重みが盗聴局に既知の場合でも適用可能な秘密情報伝送方式を検討する．このためには，送信重み入力が通常のディジタル信号と異なる必要がある．そのような発想から，信号分散を用いた秘密情報伝送方式が提案されている[16]．

MIMO E-SDMを用いた秘密情報伝送方式の基本構成をFig. 1 に示す. 図は一例として送受信アンテナが３本ずつの場合を示している．図において送信重み入力 (x_1, x_2, x_3) は, 秘密情報を伝送する信号 $s(t)$ に複素の重み付け $a_i(t)$ を行った後，複素の雑音 $n_i(\mathrm{t})$ を付加したものである．それゆえ，

$$x_i(\mathrm{t}) = a_i(t)s(t) + n_i(t),\quad i = 1,2,3 \tag{1}$$

と表される．ここで，$a_i(t)$ と $n_i(\mathrm{t})$ は受信処理を容易にするため，

$$a_1(t) + a_2(t) + a_3(t) = 1 \tag{2-1}$$

$$n_1(t) + n_2(t) + n_3(t) = 0 \tag{2-2}$$

の関係を満たすように設定する．

送信および受信のアンテナ重み W_{T} と W_{R} は，E-SDMを実現するために，

$$W_T = U\,,\ W_R = (HU)^H \tag{3-1}$$

$$W_R H W_T = (HU)^H HU = \Lambda \tag{3-2}$$

の関係がある．ここで，Uはチャネル行列 Hの相関行列 $\mathrm{G} = H^H H$ を対角化するユニタリ行列で $\Lambda = U^H GU = \mathrm{diag}(\lambda_1, \lambda_2, \lambda_3)$ である．図において，$\boldsymbol{\eta} = (\eta_1, \eta_2, \eta_3)$ は，受信機雑音である．ここで，送信重み入力 $\boldsymbol{x} = (x_1, x_2, x_3)$ と受信重み出力 $\boldsymbol{y} = (y_1, y_2, y_3)$ は，

$$\boldsymbol{y} = W_R(HW_T\boldsymbol{x} + \boldsymbol{\eta}) = \Lambda\boldsymbol{x} + W_R\boldsymbol{\eta} \tag{4}$$

の関係にある．ここで，$\boldsymbol{y}$ の信号成分 $\hat{\boldsymbol{y}} = (\hat{y}_1, \hat{y}_2, \hat{y}_3)$ は，$\hat{y}_i = \lambda_i x_i\ (i = 1,2,3)$ となる．この受信重み出力に各チャネルの利得 λ_{i} の逆数を掛けて合成信号 $r(t)$ を得る． ここで，r(t)の信号成分を $\hat{r}(\mathrm{t})$ とすると，式(2)を用いて，

$$\begin{aligned}\hat{r}(t) &= \textstyle\sum_{i=1}^{3} \hat{y}_i/\lambda_i = \sum_{i=1}^{3} x_i \\ &= \textstyle\sum_{i=1}^{3}\{a_i(t) + n_i(t)\} = s(t)\end{aligned} \tag{5}$$

となり，送信信号が取り出せる．また，受信雑音の項も含めたr(t)は，

$$r(t) = s(t) + [1/\lambda_1\,, 1/\lambda_2\,, 1/\lambda_3]W_R\boldsymbol{\eta} \tag{6}$$

となる．

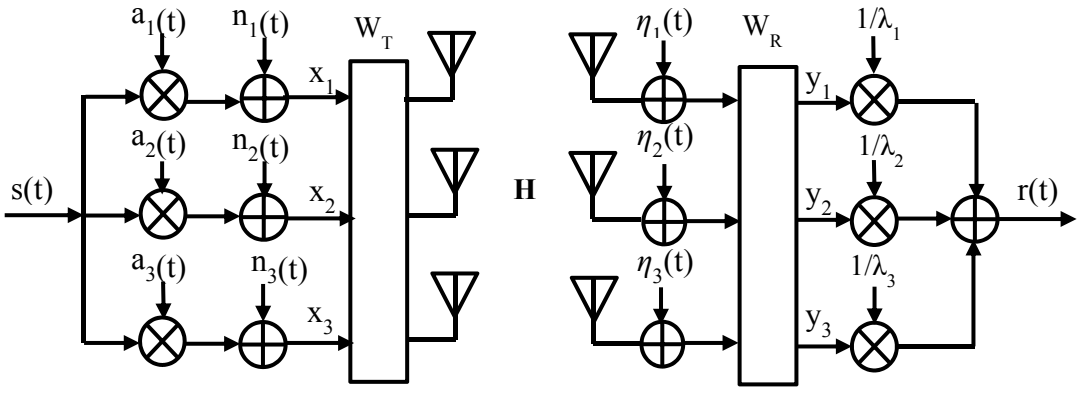


Fig. 1. Configuration of the secret information transmission using MIMO E-SDM.

2.2.2 基本構成の課題と対処法

上記の方式は，秘密情報を伝送する信号とダミー信号（雑音）に時変化する送信重みを付加していることに相当するので，MLD 受信が困難となっていることが分かる．

しかし，この基本構成のままでは安全性に欠陥がある．盗聴局が，正規局・盗聴局間の電波伝搬特性と正規局の送信重みを既知とすると，盗聴局が３本以上のアンテナで信号を受信すれば，正規局の各アンテナ出力を取得し，次に送信重み入力 (x_1, x_2, x_3) を容易に取得できる．これらを単に合成することで，秘密情報を伝送する信号が簡単に得られる．この欠陥を除くためには，送信重み入力の前でさらに重み付けを行うこと，その重み付けの値を正規局間で秘密裏に共有できることが望ましい．このような変更を行った方式の例を Fig. 2 に示す．図において付加的な送信および受信重みは，MIMO E-SDM 方式の場合に正規局間で秘密裏に共有可能である．図において合成信号 r(t)は，

$$r(t) = s(t) + \left(1/\sqrt{\lambda_1}, 1/\sqrt{\lambda_2}, 1/\sqrt{\lambda_3}\right) W_R \boldsymbol{\eta} \quad (7)$$

となる．式(6)と式(7)は，雑音の項が異なっている．

2.3 時変化プリコーディングの適用方式の提案

2.3.1 提案方式の基本形

上記の信号分散を用いた秘密情報伝送方式を一般化すると Fig. 3 の構成となる．図において，受信重み出力 $\boldsymbol{y}$ は送信重み入力 $\boldsymbol{x}$ と受信機雑音 $\boldsymbol{\eta}$ を用いて，式(3)で表される．

送信重み入力 $\boldsymbol{x}$ と受信重み出力 $\mathbf{y}$ の信号成分 $\hat{\boldsymbol{y}}$ は，

$$x_i(t) = B_i\{a_i(t)s(t) + n_i(t)\} \quad (8\text{-}1)$$

$$y_i(t) = \lambda_i B_i\{a_i(t)s(t) + n_i(t)\} \quad (8\text{-}2)$$

と表される．また，$\boldsymbol{y}$ に $C_i\lambda_i B_i = 1,\ (i = 1,2,3)$ となる重み C_i を掛けて $\boldsymbol{z}$ を得る．ここで，$\boldsymbol{z}$ の信号成分 $\hat{\boldsymbol{z}}$ と $r(t)$ の信号成分 $\hat{r}(t)$ は，$C_i = 1/(\lambda_i B_i)$ を用いて，

$$\hat{z}_i(t) = C_i y_i(t) = a_i(t)s(t) + n_i(t) \quad (9)$$

$$\hat{r}(t) = \sum_{i=1}^{3}\left(a_i s(t) + n_i(t)\right) = s(t) \quad (10)$$

となり，送信信号が得られる．また，雑音の項を含む r(t)は，

$$r(t) = s(t) + [C_1, C_2, C_3] W_R \boldsymbol{\eta} \quad (11)$$

と表される．

2.3.2 提案方式の等価変換

ここで，Fig. 3 のシステムをさらに一般化することを考える．なお，以下では簡単化のために受信雑音の項を検討対象外とし，信号系の数式を導出する．はじめに，式(8)の $x_i(t)$ は，信号 $s(t)$ と雑音 $n_1(t), n_2(t), n_3(t)$ の線形結合であるが，独立な雑音が二つであることを用いて行列表現すると式(12)となる．また，式(9)の $\hat{z}_i$ は式(13)となる．ここで，信号 $s(t)$ ばかりでなく，雑音 $n_1(t)$, $n_2(t)$ を取り出すことを考える．信号と雑音を分離するためには，式(11)に含まれる行列の逆行列を掛ければ良い．逆行列が，式(14) となることを用いると，信号出力と雑音出力を $r(t)$ と $\mu_1(t)$, $\mu_2(t)$ は，式(15) と表される．

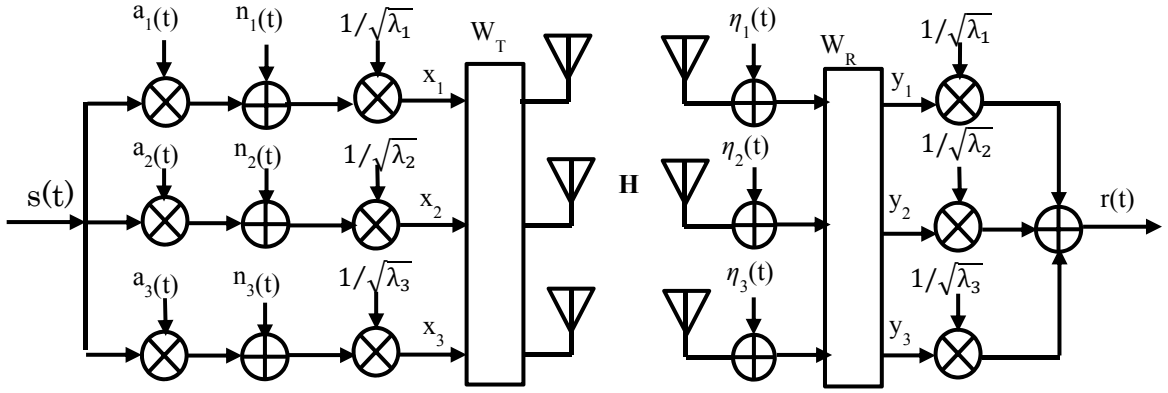


Fig. 2. Revised configuration of the secret information transmission system using MIMO E-SDM.

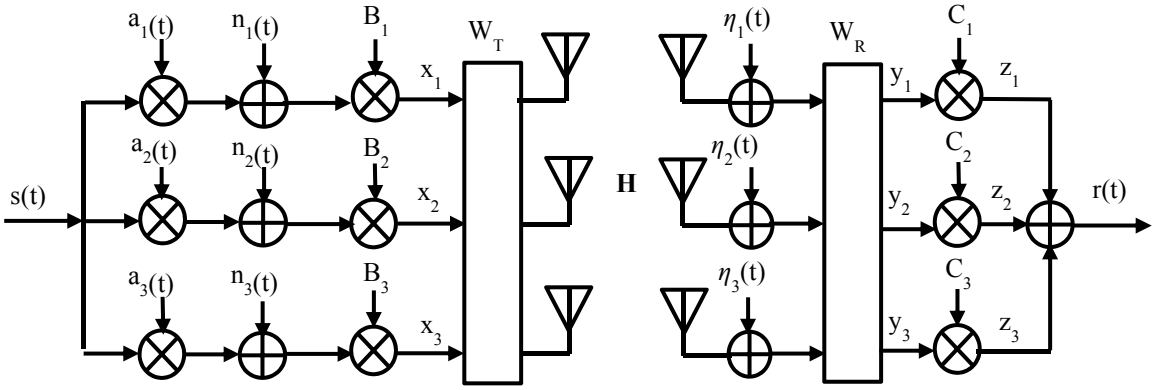


Fig. 3. The basic configuration of the proposed system. This is generalization of the secret information transmission system using MIMO E-SDM.

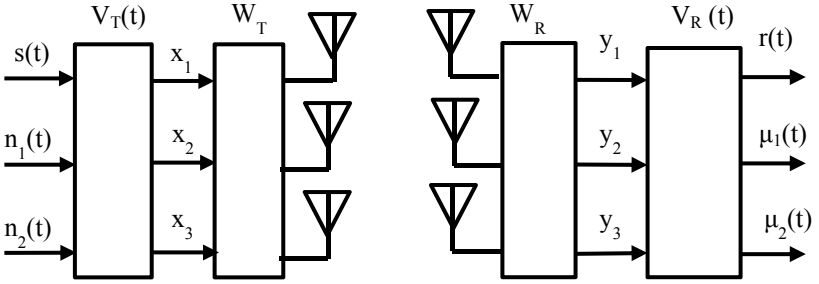
$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} B_1 & 0 & 0 \\ 0 & B_2 & 0 \\ 0 & 0 & B_3 \end{bmatrix} \begin{bmatrix} a_1(t) & 1 & 0 \\ a_2(t) & 0 & 1 \\ a_3(t) & -1 & -1 \end{bmatrix} \begin{bmatrix} s(t) \\ n_1(t) \\ n_2(t) \end{bmatrix} = \begin{bmatrix} B_1 a_1(t) & B_1 & 0 \\ B_2 a_2(t) & 0 & B_2 \\ B_3 a_3(t) & -B_3 & -B_3 \end{bmatrix} \begin{bmatrix} s(t) \\ n_1(t) \\ n_2(t) \end{bmatrix} \tag{12}$$

$$\begin{bmatrix} \hat{z}_1 \\ \hat{z}_2 \\ \hat{z}_3 \end{bmatrix} = \begin{bmatrix} a_1(t) & 1 & 0 \\ a_2(t) & 0 & 1 \\ a_3(t) & -1 & -1 \end{bmatrix} \begin{bmatrix} s(t) \\ n_1(t) \\ n_2(t) \end{bmatrix} \tag{13}$$

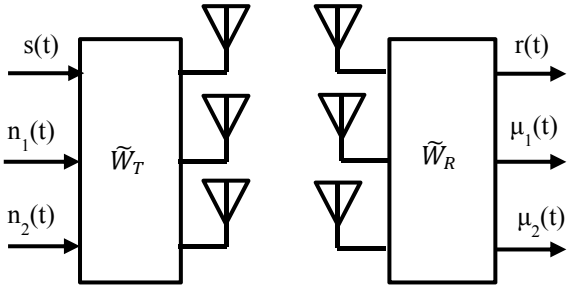
$$\begin{bmatrix} a_1(t) & 1 & 0 \\ a_2(t) & 0 & 1 \\ a_3(t) & -1 & -1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ a_2(t) + a_3(t) & -a_1(t) & -a_1(t) \\ -a_2(t) & a_1(t) + a_3(t) & -a_2(t) \end{bmatrix} \tag{14}$$

$$\begin{bmatrix} r(t) \\ \mu_1(t) \\ \mu_2(t) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ a_2(t) + a_3(t) & -a_1(t) & -a_1(t) \\ -a_2(t) & a_1(t) + a_3(t) & -a_2(t) \end{bmatrix} \begin{bmatrix} C_1 & 0 & 0 \\ 0 & C_2 & 0 \\ 0 & 0 & C_3 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}$$

$$= \begin{bmatrix} C_1 & C_2 & C_3 \\ C_1(a_2(t)+a_3(t)) & -C_2a_1(t) & -C_3a_1(t) \\ -C_1a_2(t) & C_2(a_1(t)+a_3(t)) & -C_3a_2(t) \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} \tag{15}$$



(a) Modified configuration of proposed system



(b) Generalized configuration of proposed system

Fig. 4. Configuration of the proposed system.

$$V_T(t) = \begin{bmatrix} B_1a_1(t) & B_1 & 0 \\ B_2a_2(t) & 0 & B_2 \\ B_3a_3(t) & -B_3 & -B_3 \end{bmatrix} \tag{16}$$

$$V_R(t) = \begin{bmatrix} C_1 & C_2 & C_3 \\ C_1(a_2(t)+a_3(t)) & -C_2a_1(t) & -C_3a_1(t) \\ -C_1a_2(t) & C_2(a_1(t)+a_3(t)) & -C_3a_2(t) \end{bmatrix} \tag{17}$$

次に，この等価変換に基づくシステムの構成を Fig. 4 の (a) に示す. 図は直交化のための送信重み W_T と受信重み W_R をもつ MIMO システムに，時変化する送信重み $V_T(t)$ と受信重み $V_R(t)$ を付加したものになっている．ここで，$V_T(t)$ と $V_R(t)$ は，式(16)と式(17)となる.

また，送信重みを一体化したものを $\widetilde{W}_T(t) = W_TV_T(t)$ とし，受信重みを一体化したものを $\widetilde{W}_R(t) = V_R(t)W_R$ とすると，Fig. 4 の (b) に示すように時変化プリコーディング MIMO と等価となる．なお，Fig. 4 の (a) 構成は，時変化する部分としない部分を分離した構成となっているところに特徴がある.

3．盗聴局による攻撃モデルとその対策

3.1 独立成分分析を用いたブラインド信号分離

独立成分分析(ＩＣＡ)は，独立な確率変数 $s_1, \cdots, s_n$ の線形結合により確率変数 $x_1, \cdots, x_n$ が

$$x_i = a_{i1}s_1 + a_{i2}s_2 + \cdots + a_{in}s_n, \ i = 1, \cdots, n \tag{18}$$

で生成されるとのモデルの下で，観測できる確率

変数 $x_1, \cdots, x_n$ から結合係数 a_{ij} と直接観測できない潜在変数 $s_1, \cdots, s_n$ の両方を推定する手法である [17]. 一つの独立成分を推定するため，観測量 $\boldsymbol{x} = \boldsymbol{As}$ に対し $y = \boldsymbol{b}^T\boldsymbol{x} = \boldsymbol{b}^T\boldsymbol{As}$ とすると，$\boldsymbol{b}$ が A の逆行列の一つの行であれば，y が一つの独立成分 s_i と等しくなる．また，このとき非ガウス性が最大となる．逆に，$\boldsymbol{b}$ を変化させて y の非ガウス性を最大とすれば，一つの独立成分が得られる．結局，独立成分分析は，非ガウス性が最大となる方向を探索する問題として定式化される [17].

複数アンテナから送信された電波信号が空間で多重され，それを複数アンテナで受信して，結合前の元の信号を分離するシステムを考える．ここで，各送受信アンテナ間の電波伝搬特性が既知の場合は，その特性を用いて各信号の直交化が可能となる．また，送信信号の変調諸元等が既知であれば，信号の分離がある程度可能となることも考えられる．しかし，信号と伝搬路の情報が未知の場合は，未知の状態（ブラインド）で信号を分離するしかない．一般に複数の電波信号は独立で非ガウス分布であるので，独立成分分析によりブラインド信号分離が可能となる．なお，電波信号に対しては，複数の独立成分の推定と複素数への拡張が必要となる．複数成分の推定には，各成分の直交化が必要であり，その一つに対称的直交化がある [17].

独立成分分析には，各種のアルゴリズムがあるが，比較的特性が良く高速演算が可能な観点から，複素確率変数に対する不動点アルゴリズムを用いた高速独立成分分析が有力な手法である．この独立成分分析のアルゴリズムを Table 1 に示す [17]．表において期待値としては，実際に使えるデータ標本を平均化したものを推定値とする．また，表において，$\mathrm{g(y)} = \mathrm{y}$ の場合には，

$$\boldsymbol{w} \leftarrow \mathrm{E}\{\boldsymbol{z}(\boldsymbol{w}^H\boldsymbol{z})^*|\boldsymbol{w}^H\boldsymbol{z}|^2\} - \mathrm{E}\{2|\boldsymbol{w}^H\boldsymbol{z}|^2\}\boldsymbol{w} \quad (19)$$

となる．

Table 1. Algorithm for first independent component analysis.

1. データの平均値を 0 にする中心化を行う．
2. データを白色化したものを $\boldsymbol{z}$ とする．
3. 独立成分の数を m と決め，カウンター p を 1 とする．
4. $\boldsymbol{w}_\mathrm{i}$ $(i = 1, \cdots, m)$ の初期値を決める．それぞれのノルムは 1 とする．行列 W の第 6 ステップにより直交化する．
5. $\boldsymbol{w}_\mathrm{i} \leftarrow \mathrm{E}\{\boldsymbol{z}(\boldsymbol{w}_\mathrm{i}{}^H\boldsymbol{z})^*\mathrm{g}(|\boldsymbol{w}_\mathrm{i}{}^H\boldsymbol{z}|^2)\}$ $-\mathrm{E}\{\mathrm{g}(|\boldsymbol{w}_\mathrm{i}{}^H\boldsymbol{z}|^2) + |\boldsymbol{w}_\mathrm{i}{}^H\boldsymbol{z}|^2\mathrm{g}'(|\boldsymbol{w}_\mathrm{i}{}^H\boldsymbol{z}|^2)\}\boldsymbol{w}_\mathrm{i}$ とする．ここで，$\mathrm{g}()$ は関数である．
6. $\mathrm{W} = (w_1, \cdots, w_\mathrm{m})^T$ の対称的直交化を $\mathrm{W} \leftarrow (WW^T)^{-1/2}W$ で行う．
7. 収束していなければ，5. へ戻る．

3.2 独立成分分析による信号分離特性

ここでは，独立成分分析のブラインド信号分離の特性評価の例を示す．Fig. 5 は，独立成分分析の性能評価システムである．ここで，送信信号としては，(a) 両方が QPSK の場合，(b) 両方が 16QAM の場合，(c) QPSK とガウス雑音の場合を対象とした．なお，(a),(b) は独立成分数の数を 2，(c)は独立成分の数を 1 として独立成分分析を行っている．性能評価の一指標として，独立成分分析を適用するブロック長（シンボル数）に対する信号再生確率を用いた．なお，信号再生の判定は，送信信号と受信側での再生信号との正規化された相関が 0.95 以上とした．また，信号対雑音電力比（SN 比）を 20dB とし，伝搬路はブロック内で定常なレイリーフェージングとしている．

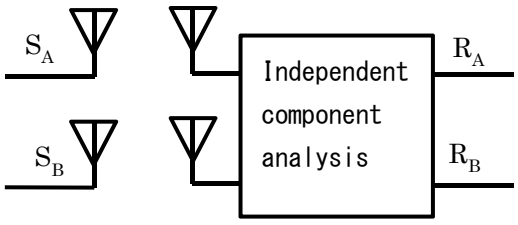
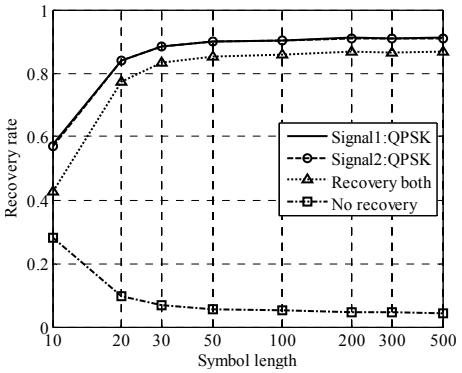
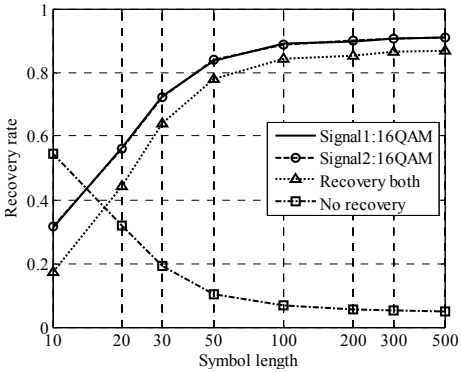


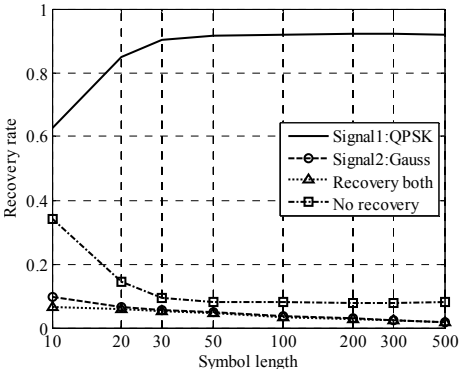
Fig. 5. Signal separation model using independent component analysis.



(a) QPSK and QPSK



(b) 16QAM and 16QAM



(c) QPSK and Gauss noise

Fig. 6. Provability of signal separation by using independent component analysis.

Fig. 6 にシミュレーション結果を示す．(a) の場合, シンボル数 30 程度で特性の増加が飽和し，両方の信号が共に再生される確率は約 90%となっている．(b) の場合，シンボル数 100 程度で特性の増加が飽和し，両方の信号が共に再生される確率は約 90%となっている. 変調多値数の増加に伴って独立成分分析の性能が若干低下していることが分かる．(c) の場合，シンボル数 30 程度で特性の増加が飽和し，QPSK 信号の再生確率は約 90%となっている．なお，独立成分数を 2 としてOPSK信号とガウス性雑音の場合に独立成分分析を適用すると，良好な分離が行われておらず動作が変になることを確かめている．このことから，ガウス性雑音と非ガウス性信号の混合の場合には，一成分の独立成分分析の方が有効であることが分かる．

3.3 提案方式に対する攻撃のモデルとその対策

盗聴局による提案方式に対する攻撃のモデルを Fig. 7 に示す．図において，提案方式の送信部は信号と二種類のガウス雑音の時変化する線形結合であり, 受信アンテナの出力値 $(\tilde{y}_1, \tilde{y}_2, \tilde{y}_3)$ も時変化する線形結合である．しかし，Fig.3 に示される提案方式において, B_i と C_i がある区間内で一定の場合，信号成分を抽出するための重みは一定となるので，その区間内で独立成分分析の適用が可能となる．

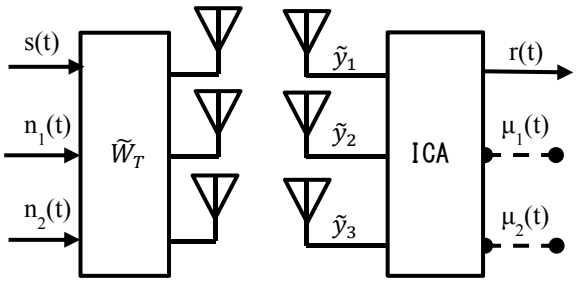


Fig. 7. Attack model for proposed system.

盗聴局による攻撃の対策は，一言で言うと有力な攻撃法である独立成分分析が効果的でないようにすることである．その一方法は，信号をガウス分布に近づける観点から，多値変調等の採用である．別の方法は，付加的な送受信重み B_i, C_i が一定の区間（時間長）を変化させて，独立成分分析を適用可能な区間を制限し，独立成分分析が十分に収束しないようにすることである．このような手法の有効性が，独立成分分析によるブライン

ド信号分離の特性評価結果からも推測できる．

4．計算機シミュレーション結果

4.1 シミュレーションシステム

4.1.1 提案方式の構成と方式諸元

シミュレーションに用いた提案方式の構成は，Fig.3 に示すようである．固有ビーム空間分割多重のための送信重み W_T と受信重み W_R の他に，付加的な送信重み B_i と受信重み C_i を設定している．この付加的な重みは，ある区間内（区間長が例えば数十シンボル）で一定としている．この区間をプリコーディングブロックと呼ぶことにする．さらに，シンボル毎に時間変化する $a_i(t)$ で重み付けを行っている．このシステムは，Fig.4 (a) に示すように時変化する送信重み $V_T(t)$ と受信重み $V_R(t)$ とが付加されたシステムと等価となる．方式諸元を Table 2 に示す．

Table 2. Parameter for proposed system.

MIMO system	E-SDM, Antenna: 3×3
Pre-coding of MIMO	Time variant pre-coding, Pre-coding block length : 10, 20, 50, 100 symbol
Modulation	QPSK，16QAM
Radio propagation	Rayleigh fading, Solid fading

4.1.2 攻撃モデルの構成と諸元

シミュレーションに用いた攻撃モデルの構成は，Fig. 7 に示すようである．提案方式では，信号と二種の雑音の線形結合が送信される．それを独立成分分析に用いてブラインド信号分離を実施し，信号成分を取り出す．雑音成分の取り出しは必ずしも必要ない．独立成分分析には，複素確率変数を対象にした不動点アルゴリズムを用いた高速独立成分分析の手法を採用している．方式諸元を Table 3 に示す．ここで，独立成分分析のデータ長は，特性劣化が生じないようにプリコーディングブロック長と対応させている．

Table 3. Parameter for attack system.

Signal separation	Received antenna: 3 Independent component analysis
ICA	Algorithm: First ICA, Complex data Data length:10,20,50,100 symbol Repetition time : 5
Demodulation	Ideal phase compensation, Coherent detection

4.2 シミュレーション結果

4.2.1 基本システムのビット誤り率特性

提案システムの SN 比対ビット誤り特性のシミュレーション結果を Fig. 8 に示す．ここで，変調は QPSK としている．また，プリコーディングブロック長は，50, 100 シンボルに設定している．さらに，送受信の付加的な重みを $B_i = 1/\sqrt{\lambda_i}$, $C_i = 1/\sqrt{\lambda_i}$ としている．図から正規局間のビット誤り率特性に比べ正規局・盗聴局間の特性は大きく劣化しているが，SN 比が高くなると規局・盗聴局間のビット誤り率特性が十分小さく（例えば，10^{-2} 以下）なるため，秘密情報伝送が十分でない．見方を変えると独立成分分析が有力な攻撃手法であることが分かる．

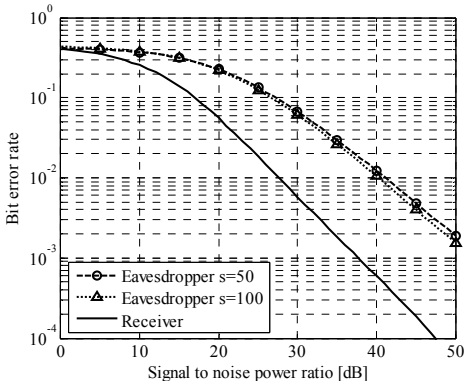


Fig. 8. Bit error rate (BER) performance vs. signal-to-noise power ration (SNR) .

4.2.2 多値変調による対策の効果

プリコーディングブロック長を 50 symbol に設

定し，QAM の変調多値数を変化させて，盗聴局の SN 比対ビット誤り率特性求めた結果を Fig. 9 に示す．図から変調多値数の増加とともにビット誤り率が 10^{-1} 以上に急激に増加している．独立成分分析による攻撃に対して多値変調が有効であることが分かる．

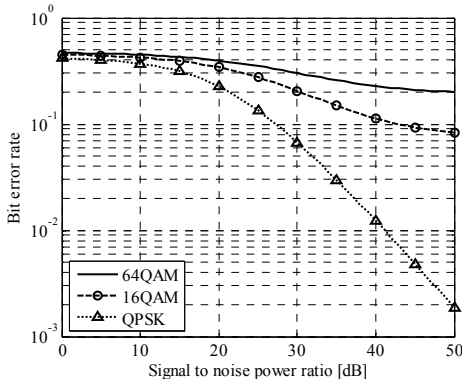


Fig. 9. BER performance vs. SNR for multi-level modulation.

4. 2. 3 付加的な送受信重みの時間変化の効果

変調方式を QPSK と 16QAM とし, プリコーディングブロック長（独立成分分析のデータ長）を 10, 20, 50 symbol と変化させて, 盗聴局の SN 比対ビット誤り率特性求めた結果を Fig. 10 に示す. 図からプリコーディングブロック長の短縮とともにビット誤り率が 10^{-1} 付近まで急激に増加している．独立成分分析による攻撃に対してプリコーディングブロック長の短縮が有効であることが分かる．

このようにビット誤り率が増加するとブロック内の誤り個数も大きくなることが予想されるが，誤り発生に偏りがあるとブロック内で誤りがない場合が発生することも考えられる．そこで，QPSK 変調および 16QAM 変調で，プリコーディングブロック長を 10 symbol とした場合に, ブロック内誤り個数の分布を調べた結果を Fig. 11 に示す．(a) の QPSK の場合，ブロック内のビット誤り個数が零となる確率がある．このことは，平均のビット誤り率が大きくなり平均的な秘密性が十分であっても，一部ブロックに秘密性が不十分となる場合があることを意味している．一方，(b) の 16QAM 変調の場合，ブロック内ビット誤り個数が零となる確率がほとんどないことが分かる．この結果は，独立成分分析の攻撃に耐えて

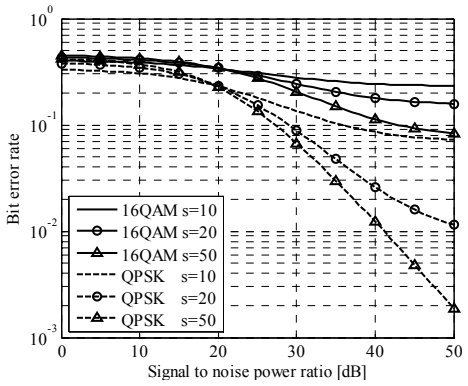
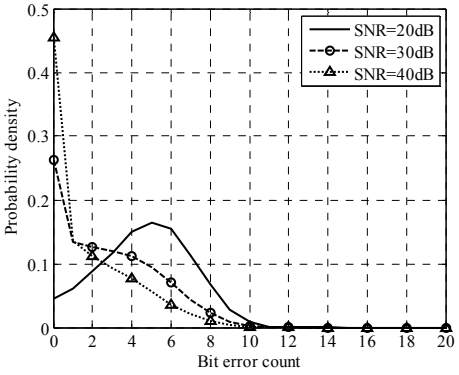
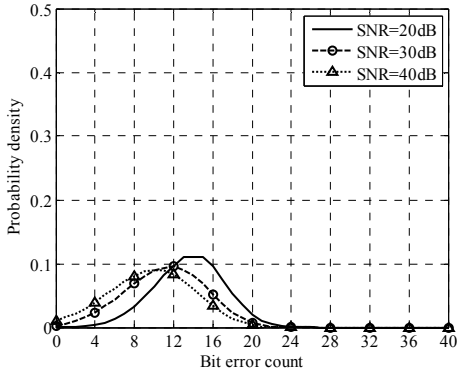


Fig. 10. BER performance vs. SNR for various pre-coding block length.



(a) QPSK in 10 symbol block



(b) 16QAM in 10 symbol block

Fig. 11. Distribution of error number in a symbol block.

秘密情報伝送が可能なことを示している．

５．まとめ

MIMO システムにおける秘密情報分散伝送方式の課題を検討し，時変化プリコーディングを用いた秘密情報伝送方式を提案した．また，独立成分分析を用いた盗聴局による提案方式への攻撃モデルとその対策を検討した．計算機シミュレーションにより提案方式の特性評価を行った結果，正規局間で良好な情報伝送特性が得られることが分かった．また，多値変調の採用とプリコーディングブロック長を短縮により，独立成分分析による盗聴局の攻撃の下でも十分な守秘性が確保できることが分かった．

今回は，独立成分分析による攻撃を対象としたが，他に有力な攻撃法とその対策を検討することは，今後の課題である．また，提案方式が独立成分分析の攻撃に少し弱い原因は，MIMO システムで伝送した複数信号の線形和で元の信号を得る手法に一因がある．複数の伝送信号の非線形処理で元の信号を得る手法の検討も今後の課題である．

参考文献

1) H.Yamamoto, “Information Theory of Cryptology,” *IEICE Trans*., **E74**[9], 2456-2464, (1991).
2) 今井秀樹，花岡悟一郎，“情報量的安全性に基づく暗号技術，”電子情報通信学会論文誌(A), **J87-A**[6], 721-733，(2004).
3) J. E. Hershey, A. A. Hassan and R. Yarlagadda, “Unconventional Cryptographic Keying Variable Management,” *IEEE Trans. Commni.*, **43**[1], 3-6, (1995).
4) A. A. Hassan, W. E. Stark, J. E. Hershey and S. Chennakeshu, “Cryptographic Key Agreement for Mobile Radio,” *Digital Signal Processing*, **6**, 207-212, (1996).
5) H. Koorapaty, A. A. Hassan and S. Chennakeshu, “Secure Information Transmission for Mobile Radio,” *IEEE Communication Letters*, **4**[2], 52-55, (2000).
6) 笹岡秀一，“電波を用いた無線通信セキュリティ技術，”電子情報通信学会技術研究報告，WBS2010-**51**, 31-36，(2011).
7) A. D. Wyner, “The Wire-tap Channel,” *Bell Sys. Tech. J*., **54**, 1355-1387, (1975).
8) I. Csiszar and J. Korner, “Broadcast Channel with Confidential Message,” *IEEE Trans. Inform. Theory*, IT-**24**[3], 339-348, (1978).
9) X. Li, and E. P. Ratazzi, “MIMO Transmission with Information-theoretic Secrecy for Secret-key Agreement in Wireless Networks,” *Proc. IEEE Military Communication Conference* (*MILCOM’ 2005*), **3**, 1353-1359, (2005).
10) A. Khisti, G. Womell, A. Wiesel, and Y. Eldar, “On the Gaussian MIMO Wiretap Channel,” *IEEE International Symposium on Information Theory* (*ISIT2007*), 2471-2475, (2007).
11) F. Oggier and B. Hassibi, “The Secrecy Capacity of the MIMO Wiretap Channel,” *IEEE International Symposium on Information Theory* (*ISIT2007*), 524-528, (2008).
12) 北野隆康，岩井誠人，笹岡秀一，“MIMO 固有ビーム空間分割多重伝送における秘密情報伝送，”電子情報通信学会論文誌(B)，**J94-B**[2]，85-93，(2011).
13) R. Liu, I. Maric, P. Spasojevic, and R. D. Yares, “Discrete Memoryless Interference and Broadcast Channels with Confidential Messages: Secrecy Rate Regions,” *IEEE Trans. Inf. Theory*, **54**[6], 2493-2507, (2008).
14) X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, “The Gaussian Wiretap Channel with a Helping Interference,” *IEEE International Symposium on Information Theory* (*ISIT2008*), 389-393, (2008).
15) 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，”電子情報通信学会論文誌(B)，**J92-B**[9]，1362-1372，(2009).
16) 田中智，清水崇之，北野隆康，岩井誠人，笹岡秀一，“MIMO システムにおける信号分散を用いた秘密情報伝送方式，”電子情報通信学会技術研究報告，RCS2000-**282**，195-200，(2011).
17) A. Hyvarinen, J. Karhunen and E. Oja, *Independent Component Analysis*, (John Wiley and Sons, Inc. , 2001).