無線セキュア伝送の研究動向調査

高野 泰洋[1]　白石 善明[1]　森井 昌克[1]

概要：Beyond 5G (B5G) システムにて，情報理論的安全性に基づくセキュア伝送が検討されている．セキュア伝送は，Massive-MIMO チャネルの空間自由度を活用した Spatial-division multiple access (SDMA) を応用した送信プリコーディング技術の一つで，その送信重みの算出は Signal-to-leak-and-noise ratio (SLNR) 最大化規範に基づく Generalized eigenvalue decomposition (GED) や，リンク行列から構成された Matrix Pencil の Generalized singular value decomposition (GSVD) により算出される．本稿は，IoT システム等を想定し，比較的長い伝送間隔の通信シナリオにおいて，２つの方式のセキュア伝送性能を調査する．シミュレーション結果，当該想定シナリオでは GSVD 法に比べ GED 法は Secrecy Capacity を向上することを確認した．

キーワード：セキュア伝送，Signal-to-leak-and-noise ratio (SLNR)，Internet of Things (IoT)，物理層セキュリティ，情報理論的安全性．

A Survey on Wireless Secure-Transmission Techniques

Yasuhiro TAKANO[1]　Yoshiaki SHIRAISHI[1]　Masakatsu MORII[1]

Abstract: In Beyond 5G (B5G) systems, secure transmission (Tx) methods based on Information-theoretic security are studied. The secure Tx methods are Tx precoding techniques based the spatial-division multiple access (SDMA) exploiting spatial degree of freedoms (DoFs) of massive-multiple-input multiple output (MIMO) channels. The Tx weights can be computed by using the generalized eigenvalue decomposition (GED) under maximum signal-to-leak-and-noise ratio (SLNR) criterion, or by using the generalized singular value decomposition (GSVD) for a matrix pencil composed from link matrixes. This paper investigates, by assuming IoT systems, secure Tx performance of the two methods in communication scenarios having long Tx intervals. Simulation results verified that the GED method improves secrecy capacity over the GSVD technique in the assumed scenarios.

Keywords: Secure transmission, Signal-to-leak-and-noise ratio (SLNR), Internet of Things (IoT), physical layer security, information-theoretic security.

1. はじめに

無線通信の安全性は，従来，上位層での暗号化により保証されてきた．多くのプロトコルで利用されている Advanced encryption standard (AES) [1] は，現在，十分な計算量的安全性を持つと考えられている．しかし，一度設置した後，10 年間メンテナンスフリーで稼働する Internet of Things (IoT) システムにおいて，10 年後も当該 AES が現在と同様に安全であるとは限らない．

また，無線システムの進化が伝送レートの増加に応える一方，漏洩情報量もそれに比例して増加しうる懸念がある．しかし，Massive-multiple-input multiple-output (MIMO) を想定する Beyond 5th generation (B5G) システムでは，高い空間自由度を活用し，特定のユーザのみに情報伝送するセキュア伝送の実現が検討されている．セキュア伝送はリンク間のチャネル容量差を活用するため，チャネルの状態に依存し，常に実行可能とは限らない．しかし，セキュア伝送を既存の暗号化技術と併用して安全性の向上を図る

[1] 神戸大学
Kobe University

ことが期待されている．

セキュア伝送の実現方法として，複数チャネル行列で構成された Matrix Pencil の Generalized singular value decomposition (GSVD)([2] 等) による送信重みの算出法が提案されている．GSVD 法は高 Signal-to-noise ratio (SNR) において最適性能を達成することが知られている．しかし，中低 SNR 領域においては Signal-to-leakage-and-noise ratio (SLNR) 規範に基づく Generalized eigenvalue decomposition (GED) 法の方が好ましいという研究事例 [3] もある．本稿では，一部の IoT システムには通信頻度が低いものがあることに注目し，送信間隔の長いシナリオでの GSVD 法と GED 法のセキュア伝送性能を比較する．

本稿の構成は次の通りである．第 2 章は本稿の想定するシステムを述べる．第 3 章は，セキュア伝送問題を形式化し，GED 法および GSVD 法を概説する．第 4 章は数値例により，両者の性能を比較する．第 5 章は，本稿の結論をまとめる．

表記: タイミング l から過去 L 件の観測値に対し間隔 Δ でサンプルした系列 $\mathbf{X}(j)$ の平均行列を $\mathbb{E}_{j=l}^{L,\Delta}[\mathbf{X}(j)] = \frac{1}{L}\sum_{j=1}^{L}\mathbf{X}(l-(L-j)\Delta)$ と記す．簡潔のため，誤解の無い範囲で，サンプル区間を省略して $\mathbb{E}[\mathbf{X}(j)]$ と記す．また，Column- と row-wise の共分散行列を，それぞれ，$\mathbb{K}[\mathbf{X}(j)] = \mathbb{E}[\mathbf{X}^{\mathsf{H}}(j)\mathbf{X}(j)]$ と $\mathbb{R}[\mathbf{X}(j)] = \mathbb{E}[\mathbf{X}(j)\mathbf{X}^{\mathsf{H}}(j)]$ と表記する．

2. システムモデル

本稿は，Time division duplex (TDD) 通信システムを想定し，Artificial noise (AN) を併用した送信プリコーディングにより MIMO-multiple-antenna eavesdropper (MIMO-ME) シナリオにおけるセキュア伝送を検討する．具体的には，Alice は N_{A} 本のアンテナから，$M_{\mathrm{B}} = 1$ 本アンテナの Bob へ秘密情報を伝送する．M_{E} 本のアンテナを持つ傍聴者 Eve は，Alice と正規に通信するのと同時に，Bob へ伝送された秘密情報を取得を企てている．また，図 1 に示すとおり，Uplink (UL) 伝送タイミング $\mathcal{T}_{\mathrm{u}}$ 中，Bob と Eve は Δ_{u2u} スロット間隔で Alice へ参照信号を送る．これにより，Alice は該当ユーザーとのチャネルを [4] 等のアルゴリズムにより推定する．そして，Alice は，Downlink (DL) 伝送タイミング $\mathcal{T}_{\mathrm{d}}$ 時に，最新の参照信号受信から Δ_{u2d} スロット後に当該ユーザへ秘密情報を伝送する．

チャネルは，Winner II model [5] に従って生成されたマルチパス伝搬路を仮定する．本稿では，LoRa 等の IoT システムを考慮し，スロット長 L_D に比べて，信号伝送間隔 Δ_{u2u} や Δ_{u2d} が長い状況を想定する．従って，低速な端末移動であっても，最新の DL チャネルを最後に受信した UL チャネルで近似することは必ずしも正確でないことに注意されたい．

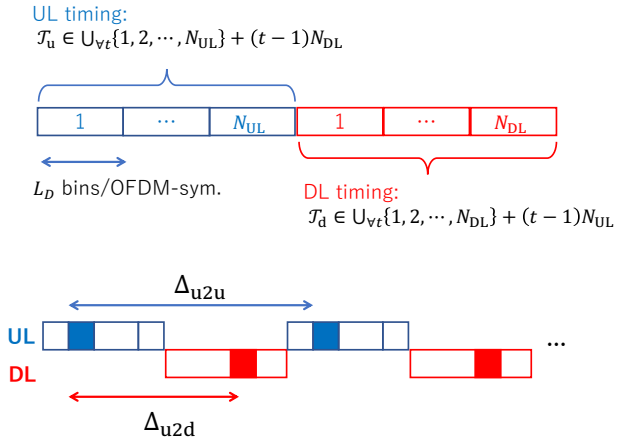

図 1　スロットフォーマット．

2.1 DL Receive (Rx) 信号

DL スロット $l \in \mathcal{T}_{\mathrm{d}}$ における Bob と Eve の第 f-bin の受信信号は，それぞれ，

$$\mathbf{y}_{\mathrm{B}}(f,l) = \mathbf{H}_{\mathrm{B}}(f,l)\mathbf{x}(f,l) + \mathbf{z}_{\mathrm{B}}(f,l) \quad \in \mathbb{C}^{M_{\mathrm{B}}\times 1}, \quad (1)$$

$$\mathbf{y}_{\mathrm{E}}(f,l) = \mathbf{H}_{\mathrm{E}}(f,l)\mathbf{x}(f,l) + \mathbf{z}_{\mathrm{E}}(f,l) \quad \in \mathbb{C}^{M_{\mathrm{E}}\times 1} \quad (2)$$

と書ける．ここで，$\mathbf{H}_{\mathrm{B}}(f,l) \in \mathbb{C}^{M_{\mathrm{B}}\times N_{\mathrm{A}}}$ と $\mathbf{H}_{\mathrm{E}}(f,l) \in \mathbb{C}^{M_{\mathrm{E}}\times N_{\mathrm{A}}}$ は，それぞれ，Bob-Alice 間，Eve-Alice 間，のチャネル行列である．熱雑音ベクトル $\mathbf{z}_{\mathrm{B}}(f,l)$ と $\mathbf{z}_{\mathrm{E}}(f,l)$ は，ノイズ分散を σ_{z}^2 とし，それぞれ $\mathcal{CN}(\mathbf{0},\sigma_{\mathrm{z}}^2\mathbf{I}_{M_{\mathrm{B}}})$ and $\mathcal{CN}(\mathbf{0},\sigma_{\mathrm{z}}^2\mathbf{I}_{M})$ に従う．Alice から送信される長さ N_{A} の信号ベクトルは

$$\begin{aligned}\mathbf{x}(f,l) = {} & \mathbf{W}_{\mathrm{B}}(f,l)\sigma_{\mathrm{b}}(l)\mathbf{b}(f,l) \quad (3)\\ & + \mathbf{W}_{\mathrm{E}}(f,l)\sigma_{\mathrm{E}}(l)\mathbf{a}_{\mathrm{E}}(f,l) + \mathbf{W}_{\perp}(f,l)\sigma_{\perp}(l)\mathbf{a}_{\perp}(f,l)\end{aligned}$$

により与えられる．ここで，$\mathbf{b}(f,l)$ は Bob へ伝送する秘密信号である．また，AN ベクトル $\mathbf{a}_{\mathrm{E}}(f,l) \in \mathbb{C}^{M_{\mathrm{E}}}$ と $\mathbf{a}_{\perp}(f,l) \in \mathbb{C}^{N_{\mathrm{A}}}$ は，それぞれ，Eve および (正規チャネル $\mathbf{H}_{\mathrm{B}}(f,l)$ との直行空間に存在しうる) 未知の傍聴者の受信を阻害を目的としている．これらの信号は，$\mathbb{E}[\|\mathbf{b}(f,l)\|^2] = \mathbb{E}[\|\mathbf{a}_{\mathrm{E}}(f,l)\|^2] = \mathbb{E}[\|\mathbf{a}_{\perp}(f,l)\|^2] = 1$ を満たすように生成する．それぞれの信号の電力比は，正の係数 $\sigma_{\mathrm{b}}(l)$, $\sigma_{\mathrm{E}}(l)$, $\sigma_{\perp}(l)$ により定めるが，これらは

$$\sigma_{\mathrm{b}}^2(l) + \sigma_{\mathrm{a}}^2(l) + \sigma_{\perp}^2(l) = 1, \quad (4)$$

を満たすように正規化する．送信重み行列 $\mathbf{W}_{\mathrm{B}}(f,l) \in \mathbb{C}^{N_{\mathrm{A}}\times M_{\mathrm{B}}}$, $\mathbf{W}_{\mathrm{E}}(f,l) \in \mathbb{C}^{N_{\mathrm{A}}\times M_{\mathrm{E}}}$ と $\mathbf{W}_{\perp}(f,l) \in \mathbb{C}^{N_{\mathrm{A}}\times N_{\mathrm{A}}}$ も

$$\begin{aligned}&\tfrac{1}{L_{\mathrm{D}}}\textstyle\sum_{f=1}^{L_{\mathrm{D}}}\|\mathbf{W}_{\mathrm{B}}(f,l)\|^2 = \quad (5)\\ &\tfrac{1}{L_{\mathrm{D}}}\textstyle\sum_{f=1}^{L_{\mathrm{D}}}\|\mathbf{W}_{\mathrm{E}}(f,l)\|^2 = \tfrac{1}{L_{\mathrm{D}}}\textstyle\sum_{f=1}^{L_{\mathrm{D}}}\|\mathbf{W}_{\perp}(f,l)\|^2 = 1.\end{aligned}$$

となるように算出する．しかし，最新の DL slot $l \in \mathcal{T}_{\mathrm{d}}$ に対応するチャネル行列を $\{\mathbf{H}_{\mathrm{B}}(f,l), \mathbf{H}_{\mathrm{E}}(f,l)\}$ 正確に推定することは困難である．送信重み行列は過去の UL チャネル行列の推定値を用いて計算しなければならないことに注意されたい．

3. セキュア伝送法

3.1 問題形式化

本稿の対象とするセキュア伝送問題は，過去の UL スロットタイミングで求めた UL チャネル推定値

$$\left\{\hat{\mathbf{H}}_{\mathrm{B}}^{\mathsf{T}}(f,l),\hat{\mathbf{H}}_{\mathrm{E}}^{\mathsf{T}}(f,l)\mid\forall l_{\mathrm{u}}\in\mathcal{T}_{\mathrm{u}}(l)\right\}_{\forall f} \tag{6}$$

を用いて，チャネル容量制約

$$\begin{cases}\mathbb{E}\left[\mathtt{C}_{\mathrm{B}}(\Theta(l)\mid\sigma_{\mathrm{z}}^2)\right]>\mathtt{C}_0+\Delta\mathtt{C}_{\mathrm{B}} & (7)\\ \mathbb{E}\left[\mathtt{C}_{\mathrm{E}}(\Theta(l)\mid\sigma_{\mathrm{z}}^2)\right]<\mathtt{C}_0+\Delta\mathtt{C}_{\mathrm{E}}, & (8)\end{cases}$$

のもと，Ergodic Secrecy Capacity

$$\max\mathbb{E}\left[\mathtt{C}_{\mathrm{S}}\left(\Theta(l)\right)\right] \tag{9}$$

を最大にするパラメータ集合

$$\Theta(l)=\left\{\sigma_{\mathrm{b}}^2(l),\sigma_{\mathrm{E}}^2(l),\{\mathbf{W}_{\mathrm{B}}(f,l),\mathbf{W}_{\mathrm{E}}(f,l),\mathbf{W}_{\perp}(f,l)\}_{\forall f},\right\} \tag{10}$$

を求めることである．ここで，定数 $\{\mathtt{C}_0,\Delta\mathtt{C}_{\mathrm{B}},\Delta\mathtt{C}_{\mathrm{E}}\}$ は所望の伝送レートを達成するために必要なチャネル容量 $\mathtt{C}_0$，および，秘匿チャネル容量を確保するためのオフセット $(\Delta\mathtt{C}_{\mathrm{B}},\Delta\mathtt{C}_{\mathrm{E}})$ である．Ergodic capacity (9) は，

$$\begin{aligned}\mathbb{E}\left[\mathtt{C}_{\mathrm{S}}\left(\Theta(l)\right)\right] &= \mathbb{E}\left[\mathtt{C}_{\mathrm{B}}\left(\Theta(l_{\mathrm{u}}),\{\mathbf{T}_{\mathrm{B}}(f,l_{\mathrm{u}})\}_{\forall f}\right)\right]\\ &\quad-\mathbb{E}\left[\mathtt{C}_{\mathrm{E}}\left(\Theta(l_{\mathrm{u}}),\{\mathbf{T}_{\mathrm{E}}(f,l_{\mathrm{u}})\}_{\forall f}\right)\right],\end{aligned}$$

により定義する．ただし，チャネルコヒーレント定数 L_C と UL 伝送間隔 Δ_{u2u} スロットに対し，

$$\mathbf{T}_{\mathrm{E}}(f,l)\stackrel{\mathrm{def}}{=}\mathbb{E}_{j=l}^{L_C,\Delta_{\mathrm{u2u}}}[\mathbf{H}_{\mathrm{E}}^{*}(f,j)\otimes\mathbf{H}_{\mathrm{E}}(f,j)]. \tag{11}$$

$\otimes$ はクロネッカー積である．テンソル $\mathbf{T}_{\mathrm{B}}(f,l)$ も同様に定める．Eve の平均チャネル容量は，

$$\mathbb{E}\left[\mathtt{C}_{\mathrm{E}}\left(\Theta(l),\{\mathbf{T}_{\mathrm{E}}(f,l)\}_{\forall f}\right)\right]=\sum_{f=1}^{L_{\mathrm{D}}}\bar{\mathtt{C}}_{M_{\mathrm{E}}}\left(\Theta(l),\mathbf{T}_{\mathrm{E}}(f,l)\right) \tag{12}$$

により算出する．ここで，簡単のため (l,f) を省略するが，

$$\begin{aligned}\bar{\mathtt{C}}_{M_{\mathrm{E}}}\left(\Theta(l),\mathbf{T}_{\mathrm{E}}\right)\stackrel{\mathrm{def}}{=}\log_2\big\{&\mathbf{I}_{M_{\mathrm{E}}}+\sigma_{\mathrm{b}}^2\mathbb{R}[\mathbf{H}_{\mathrm{E}}\mathbf{W}_{\mathrm{B}}]\cdot\\ &\left\{\sigma_{\mathrm{E}}^2\mathbb{R}[\mathbf{H}_{\mathrm{E}}\mathbf{W}_{\mathrm{E}}]+\sigma_{\perp}^2\mathbb{R}[\mathbf{H}_{\mathrm{E}}\mathbf{W}_{\perp}]+\sigma_{\mathrm{z}}^2\mathbf{I}_{M_{\mathrm{E}}}\right\}^{-1}\Big\}.\end{aligned} \tag{13}$$

ただし，共分散行列 $\mathbb{R}_{j=l}^{L_C,\Delta_{\mathrm{u2u}}}[\mathbf{H}_{\mathrm{E}}\mathbf{W}_{\mathrm{B}}]$ はベクトル化: $\mathtt{vec}\{\mathbb{R}[\mathbf{H}_{\mathrm{E}}\mathbf{W}_{\mathrm{B}}]\}=\mathbf{T}_{\mathrm{E}}\mathtt{vec}\{\mathbf{W}_{\mathrm{B}}\mathbf{W}_{\mathrm{B}}^{\mathsf{H}}\}$ を通じて算出する．$\mathbb{E}[\mathtt{C}_{\mathrm{B}}(\cdot)]$ も (12) と同様に定義する．

パラメータセット (10) のうち，信号電力 $(\sigma_{\mathrm{b}}^2,\sigma_{\mathrm{E}}^2)$ は [6], Algorithm 1 に準じて算出可能である．以下，送信重み行列 $(\mathbf{W}_{\perp},\mathbf{W}_{\mathrm{B}},\mathbf{W}_{\mathrm{E}})$ の解法に関し概説する．

3.2 $\mathbf{W}_{\perp}$ の解

[4] 等で議論した部分空間法を利用してもよい．簡単のため係数 (l,f) を省略するが，$\mathbf{H}_{\mathrm{B}}$ の部分空間は，$\mathbb{R}[\mathbf{H}_{\mathrm{B}}]$ の Rank $r\leq M_{\mathrm{B}}$ の固有空間ベクトル $\mathbf{U}_{\mathrm{B,r}}$ である．従って，その直行送信重み行列は，制約 (5) のもと，$\mathbf{W}_{\perp}\propto\mathbf{I}_{N_{\mathrm{A}}}-\mathbf{U}_{\mathrm{B,r}}\mathbf{U}_{\mathrm{B,r}}^{\mathsf{H}}$ に従って計算する．

3.3 $(\mathbf{W_B},\mathbf{W_E})$ の解: GED 法

[6] で詳述したとおり，3.1 節の問題は，Maximum SLNR 規範により解くことができる．本稿では，SLNR 規範の重み行列 $\mathbf{W}_{\mathrm{B}}$ が共分散行列 $(\mathbb{R}_{j=l_u}^{L_C}[\mathbf{H}_{\mathrm{B}}],\mathbb{R}_{j=l_u}^{L_C}[\mathbf{H}_{\mathrm{E}}]+\kappa^2\mathbf{I})$ の GED により算出される[*1]ことから，この解法を GED 法と呼ぶ．ここで，共分散行列算出における移動平均窓長を $L_C>1$ にすることで，チャネルパラメータの 2 次統計量が考慮される．つまり，送信間隔がチャネルコヒーレント時間より短い場合，当該 GED 法はチャネルモデルの時間的な統計的不変量を活用し，送信重みの算出精度を向上させる．

3.4 $(\mathbf{W_B},\mathbf{W_E})$ の解: GSVD 法

[2], [7] 等で提案されている通り，セキュア伝送問題解決する送信重みは Matrix Pencil $(\mathbf{H}_{\mathrm{B}},\mathbf{H}_{\mathrm{E}})$ の GSVD により算出してもよい．広帯域伝送を想定した 3.1 節の問題は，各 f-bin 毎に GSVD を用いて送信重みを計算すればよい．

4. 数値例

4.1 パラメータ設定

チャネルパラメータは，Winner II モデルの Urban micro-cell (B1: line-of-sight (LoS) clustered delay line) [5] により生成される．キャリア周波数 2.4 GHz の Industrial, scientific and medical (ISM) バンドを想定し，伝送帯域 3 MHz とする．また，1 slot の長さは，$L_D=256$ bins/OFDM-symbol とする．Alice, Bob, Eve はそれぞれ $(N_{\mathrm{A}},M_{\mathrm{B}},M_{\mathrm{E}})=(32,1,2)$ 本の Uniform circular array (UCA) アンテナを持つ．端末の移動移動速度は，Bob，Eve 共に 5 km/h とする．

更に，[6] と同様，符号化率 1/3 での Binary phase shift keyed (BPSK) $\sim$ 256 Quadrature amplitude modulation (QAM) の適応変調と，$\mathtt{C}_0$ に対し ±3 dB のマージンを考慮する．従って，(7) と (8) は $(\mathtt{C}_0+\Delta\mathtt{C}_{\mathrm{B}},\mathtt{C}_0+\Delta\mathtt{C}_{\mathrm{E}})=(5.4,0.2)$ [bps] と設定する．また，スロット伝送間隔は $(\Delta_{\mathrm{u2u}},\Delta_{\mathrm{u2d}})=(10,9)$ slots とした．

図 2 に示すとおり，Alice と Bob はそれぞれ原点 (0,0) と (0,100) [m] に固定する．Eve の位置は，$d_{\mathrm{E}}=80$[m] に対し，$\mathbf{p}_{\mathrm{E}}=d_{\mathrm{E}}(\cos\phi_E,\sin\phi_E)$, $\phi_E\in[0,\pi]$ [rad] により与えられる．

[*1] κ^2 は受信 signal-to-interference-puls-noise ratio (SINR) に応じて決まるパラメータである [6].

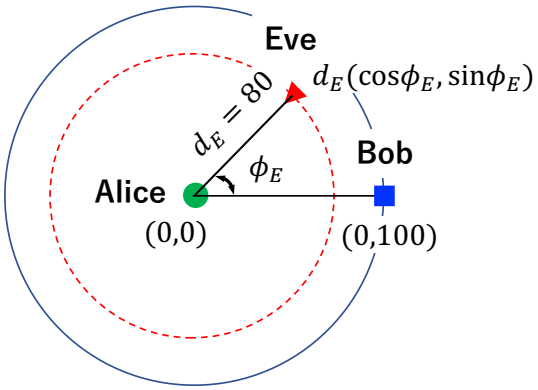

図 2　ユーザー位置.

4.2　SNR に対するセキュア伝送性能

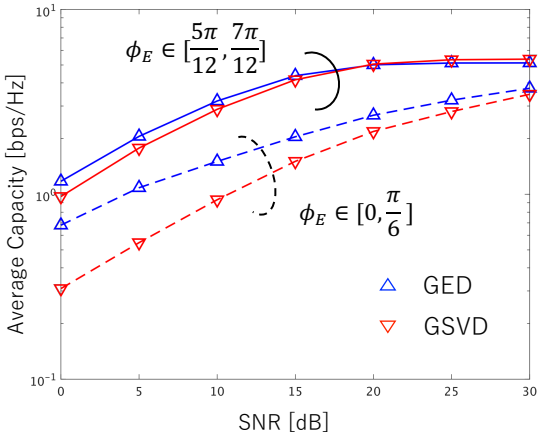

図 3　SNR に対するセキュア伝送性能.

図 3 に SNR に対する GED と GSVD 法の Secrecy Capacity 性能を示す．$\phi_{\mathrm{E}} \in [\frac{5}{12}\pi, \frac{7}{12}\pi]$ のとき，つまり，Eve が Bob から十分離れている場合，どちらの方式も $\mathtt{C}_{\mathrm{S}} > 1$ [bps/Hz] を達成している．しかし，$\phi_{\mathrm{E}} \in [0, \frac{1}{6}\pi]$ のとき，つまり，Eve が Bob の近くにいるとき，GSVD 法は低 SNR において Secrecy Capacity が大きく劣化している．一方，GED 法は，3.3 節に述べた通り，$L_C = 10$ として算出した 2 次元統計量を活用してこの問題を改善している．

4.3　Bob と Eve の位置に対するセキュア伝送性能

図 4 に GSVD 法の伝送性能を示す．SNR = 10 dB において，$\phi_E = 0$ に Eve が位置するとき，$\mathtt{C}_{\mathrm{B}} = 0.1$ [bps/Hz] となるため，GSVD 法は BPSK 変調による低速伝送も実行できない．また，$\forall\phi_{\mathrm{E}}$ に対し，GSVD 法は Eve の Ergodic capacity $\mathbb{E}[\mathtt{C}_{\mathrm{E}}]$ を過大評価してしまい，Eve への AN 電力 σ_{E}^2 が増加していることがわかる．

一方，GED 法は，図 5 に示す通り，SNR = 10 dB の時，$\forall\phi_E$ に対し，$\mathbb{E}[\mathtt{C}_{\mathrm{E}}]$ を適切な精度で評価し，σ_{E}^2 を減少させている．また，GED 法は $0.5 < \mathtt{C}_{\mathrm{B}} < 4$ [bps] かつ $\mathtt{C}_{\mathrm{E}} \leq 0.1$ [bps] を達成している．つまり，想定したシナリオにおいて，Alice は，GED 法と適応的変調法を併用して，Bob へのセキュア伝送を常に実現できる．

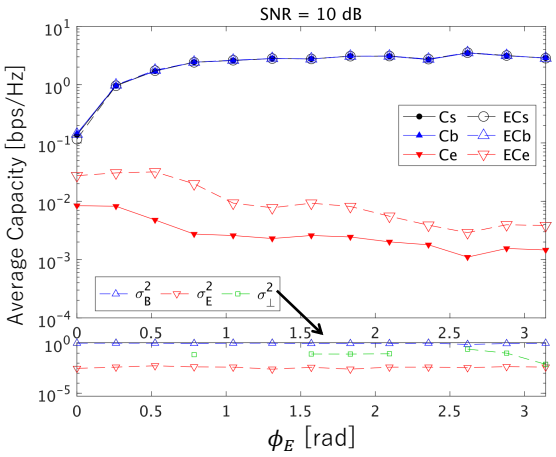

図 4　GSVD 法のセキュア伝送性能.

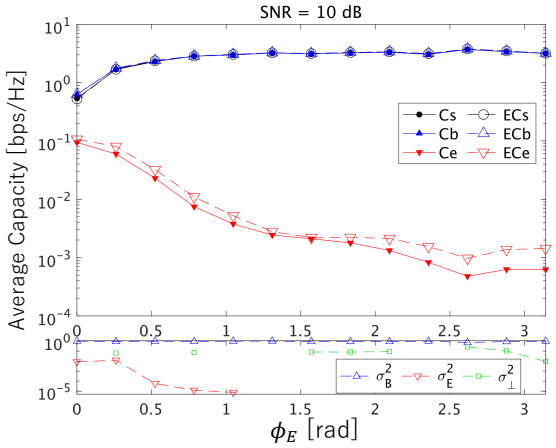

図 5　GED 法のセキュア伝送性能.

5.　まとめ

本稿は，TDD-MIMO 伝送において，比較的長い UL/DL の伝送間隔のシナリオを想定し，GED 法と GSVD 法によるセキュア伝送性能を比較した．このようなシナリオでは，GSVD 法は Ergodic capacity の推定精度が劣化してしまう．一方，GED 法は，チャネルの時間的 2 次統計量を考慮した共分散行列から送信重みを算出するため，Ergodic capacity の推定精度を改善可能なことを確認した．今後の課題として，本研究は，[6] の提案法を拡張し，Passive eavesdroppers を含むシナリオでのセキュア伝送性能の向上を目指す．

謝辞　本研究は JSPS 科研費 17K06423 および 20K04463 の助成を受けたものである．

参考文献

[1] Joan Daemen and Vincent Rijmen. *The design of Rijndael: AES-the advanced encryption standard.* Springer

Science & Business Media, 2013.

[2] S. A. A. Fakoorian and A. L. Swindlehurst. Optimal power allocation for GSVD-based beamforming in the MIMO gaussian wiretap channel. In *2012 IEEE International Symposium on Information Theory Proceedings*, pp. 2321–2325, 2012.

[3] Kun Wang, Xiyuan Wang, and Xianda Zhang. SLNR-based transmit beamforming for MIMO wiretap channel. *Wireless personal communications*, Vol. 71, No. 1, pp. 109–121, 2013.

[4] Y. Takano, H.-J. Su, Y. Shiraishi, and M. Morii. A spatial–temporal subspace-based compressive channel estimation technique in unknown interference MIMO channels. *IEEE Trans. Signal Process.*, Vol. 68, pp. 300–313, 2020.

[5] Juha Meinilä, Pekka Kyösti, Tommi Jämsä, and Lassi Hentilä. Winner II channel models. *Radio Technologies and Concepts for IMT-Advanced*, pp. 39–92, 2009.

[6] Y. Takano and H.-J. Su. A joint SLNR–MMSE-based adaptive secure transmission technique for broadband IoT systems. *to be presented in IEEE Globecom 2020, accepted on Aug. 17th 2020.*

[7] Marouen Jilani and Tomoaki Ohtsuki. Joint SVD-GSVD precoding technique and secrecy capacity lower bound for the MIMO relay wire-tap channel. *EURASIP Journal on Wireless Communications and Networking*, Vol. 2012, No. 1, p. 361, 2012.