物理層セキュリティに注目した準情報理論的安全な第５世代移動通信システム

代表研究者　　高野 泰洋　　神戸大学　大学院工学研究科　助教

【概要】

第５世代以降の移動通信システムにおいて，大規模 MIMO 伝送のチャネル・レシプロシティを用いた情報理論的安全な無線通信の実現が期待されている．多くの先行研究ではチャネルを既知と想定しているが，無線通信ではチャネルは推定すべきパラメータである．特に，セキュア伝送では，Artificial Noise (AN) を用いた安全性向上が想定されている．このため，近隣システムから漏洩した AN 等に起因する未知干渉を含む MIMO チャネル推定は必須である．このような背景のもと，本研究は第１フェーズとして，チャネル推定の高精度化を検討し，従来法を凌駕する推定法を提案した．引き続き，これまで得られた知見を活用し，第２フェーズとして，従来の暗号化と情報理論的安全性を併用したアプローチを検討していく．

1.　はじめに

無線通信の安全性は，これまで，上位層における通信データの暗号化により担保されてきた．しかし，計算量的安全性を保証する暗号化は，攻撃者の計算能力向上に加え，サイドチャネルの情報漏洩量に応じてその安全性が劣化する恐れがある．一方，第５世代移動通信システムは，大規模 MIMO 伝送やミリ波帯域を利用して 10Gbps 以上の伝送速度を目指している．しかし，電磁波の性質上，無線信号は拡散および反射され，常に正規ユーザ Bob のみに情報伝達することは難しい．従って，伝送帯域が増加するにつれ，傍聴ユーザ Eve へ漏洩する情報量も増加しうる．このような背景のもと，従来の暗号化に加えて，伝搬路の性質を活用した物理層セキュリティ[1]による安全性の強化が望まれている．具体的には，大規模 MIMO 伝送システムを想定し，チャネル・レシプロシティ[2]による情報理論的安全な無線伝送が期待されている．

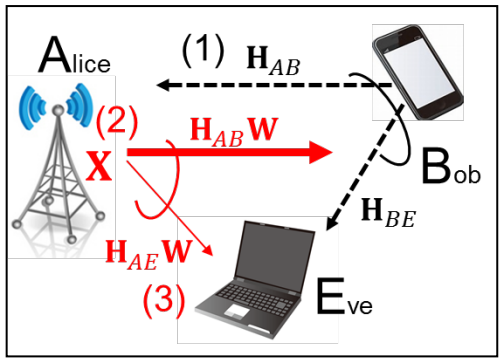

図 1 チャネル・レシプロシティ

チャネル・レシプロシティ(図 1)は，(1)上り伝送のチャネル推定結果から算出された下り送信重み$\mathbf{W}$により，(2)正規受信者 Bob の下りチャネル推定を不要にする信号処理である．Alice はパイロット信号を伝送しないため，Bob 以外の受信者は十分な精度でチャネル推定ができない．従って，(3)傍聴者 Eve には下りデータ$\mathbf{X}$の復調が困難となり，Alice-Bob 間でチャネルパラメータ$\mathbf{H}_{\mathrm{AB}}$を利用した情報理論的安全な無線伝送が実現できる．送信重み$\mathbf{W}$の算出技法として，Matrix Pencil$(\mathbf{H}_{\mathrm{AB}},\mathbf{H}_{\mathrm{AE}})$に関する Generalized singular value decomposition (GSVD)に基づく送信プリコーディング法([3]等)などが知られている．しかし，チャネル・レシプロシティは，[*9]で議論した通り，上り/下り伝送フレームのタイムラグに応じて，その伝送性能が劣化してしまう．また仮に，何らかの方法で Eve がチャネル$\mathbf{H}_{\mathrm{AE}}$を高精度に推定できるとする．これら対策として，$\mathbf{H}_{\mathrm{AB}}$の直行空間もしくは傍聴者 Eve に対し Artificial Noise を伝送することで，傍聴者の正常受信を妨げる対策法([4]等)も提案されている．ところが，先行研究の多くは，チャネルパラメータが既知であると前提している．しかし，大規模 MIMO チャネルでは，Pilot 汚染[5]等，克服すべき問題が残されている．特に，近隣システムから漏洩しうる AN 等の未知干渉を想定した高精度なチャネル推定法はまだ十分に議論されていない．そこで，本研究は，まず大規模 MIMO システムにおけるチャネル推定向上を目指した．そして，高精度なチャネル推定法，および，当該研究から得られる伝搬路の特性を活用し，現実的な伝送シナリオにおいて，暗号化と物理層セキュリティを併用した準情報理論的安全な無線伝送の検討を計画した．

公益財団法人電気通信普及財団
研究調査助成報告書　第35号　2020年度

2. 大規模 MIMO 伝送におけるチャネル推定性能向上

2.1. ターボ受信を想定したチャネル推定精度の向上

チャネル推定は，一般的に，送受信者間で共有された既知の Pilot 系列の受信信号を用いて実現される．大規模 MIMO では送信ストリーム数に応じた直交系列の組み合わせが必要である．任意の直交系列の組み合わせを設計する手段として，Gold 系列等を用いてもよい．しかし，限られた無線スペクトラムを有効利用するために，Pilot 系列はできるだけ短く設計されるべきである．ところが，有限長の Pilot 信号は，Gold 系列であっても，ストリーム数増加に伴い直交性が損なわれる．この問題の解決策として，ターボ受信を想定したチャネル推定法が考えられる．ターボ受信は，チャネル復号器からフィードバックされたデータ信号の対数尤度比をもとに送信信号のレプリカを生成することができる．つまり，ターボチャネル推定法は，短い Pilot と長いレプリカ信号を併用することで Pilot 汚染問題を改善することができる．ここで，無線伝送フォーマットは，通常，Pilot 信号の他にも Inter-block interference(IBI)を回避するために Guard interval (GI) 等の制御信号を有する．しかし，このような制御信号は，やはりスペクトラム利用効率を低下させる．ターボチャネル推定は，十分な繰り返し受信実行後，IBI 問題を解決できる．しかし，レプリカ信号を生成できない初回の繰り返し受信時には Mean square error (MSE)フロアが発生してしまう課題がある．

本研究は，MIMO 伝送における Pilot 汚染および IBI 問題への解決策として，研究成果[*2]において，条件付き ℓ1 正規化 MMSE 推定法を提案した．具体的には，初回の繰り返し受信時，チャネル長制約 (ℓ1 正規化) により IBI 回避を行う．そして，２回目以降の繰り返し受信時はレプリカ信号を用いた IBI キャンセルを実施する．さらに，当該チャネル推定を条件付き ℓ1 正規化 MMSE 問題として形式化し，チャネルの部分空間が ℓ1MMSE 法と通常の ℓ2MMSE 法とで同一であることに注目し，その解決策を Adaptive IBI-managed (AIM-)MMSE 法として提案した．計算機シミュレーションにより，提案法を用いた受信機は，スペクトラム利用効率を高めるのと同時にターボ繰り返し受信の Bit error rate (BER) 収束性能を向上させることを検証した．(図 2)

さらに，[*8]において，チャネル長とチャネル推定精度が Secrecy Capacity に及ぼす影響を議論し，当該 AIM-MMSE 法の物理層セキュリティへの応用を検討した．

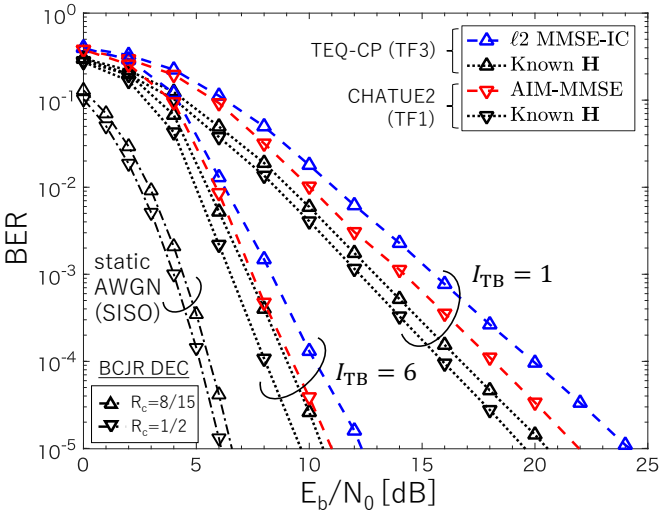

図 2 Pedestrian-B 3km/h (PB3)シナリオにおける BER 性能 [*2, Fig. 8]

2.2. 大規模 MIMO システムにおけるターボチャネル推定法の高速化

前述の通り，ターボチャネル推定法は，大規模 MIMO システムにおいて Pilot 汚染問題を解決すると共に，Secrecy Capacity を向上させることができる． Pilot とレプリカ信号を利用したターボチャネル推定は，Joint-maximum likelihood (ML)問題として形式化される．Gaussian Elimination に基づく逆行列計算を実行する従来の解法は，送信,受信アンテナ数(N_T, N_R)とシステム定数κに対し，計算量オーダー $\mathcal{O}(\kappa^3 N_T^3 N_R^3)$ を必要とする．しかし，大規模 MIMO システムでは，アンテナ数増加に伴い，この演算を実行することが困難である．そこで，本研究は，研究成果[*3]において，Joint ML 問題における共分散行列の代数的特徴を利用し，推定性能を損なうことなく受信アンテナ数と独立な演算量$\mathcal{O}(\kappa^3 N_T^3)$で実行可能なターボチャネル推定法を提案した．また，高い学術的成果が認められた本研究は国際会議 IEEE Global SIP 2018 [*4] に招待された．また，2018 年電子情報通信学会ソサイエティ大会において関連研究者と情報共有，意見交換を行った．

2.3. 時空間部分空間法を用いた未知干渉 MIMO チャネル推定の精度の向上

前述のとおり，セキュア伝送システムでは，近隣システムから漏洩した AN を想定したうえで高精度なチャネル推定の実現が不可欠である．近年，mmWave を想定した MIMO チャネル推定([6, 7]等)が広く研究されている．しかし，多くの先行研究では，送受信機双方向のビームフォーミングが実施可能で，かつ，長期間のチ

ャネル・コヒーレント時間を想定している．しかし，安価なシングルアンテナ端末ノードを有する IoT ネットワーク等では必ずしも送受信ビームフォーミングが実施できるとは限らない．しかも，“massive MIMO チャネル推定”と題した先行研究の中には，[*6]で概説したとおり，下りの MISO チャネル推定や時分割された SIMO チャネル推定を議論しており，未知干渉 MIMO チャネル推定問題は十分に議論されていない．

そこで，本研究は，研究成果[*1]にて，ℓ1 正規化時空間部分空間法を用いたチャネル推定法を提案した．時空間部分空間法は，[8]にて，Principal component analysis (PCA) に基づく解法が示されていた．しかし，PCA に基づく推定法は未知干渉信号を効果的に抑圧できない．そこで，[*1]では，Independent component analysis (ICA)の概念に基づき，Resolvable Path 毎に時空間部分空間を解析することで，従来法より推定性能を改善できることを行列代数的に証明した．次に，提案法は，具体的には，時空間部分空間法[8]に ℓ1 正規化を付与した ℓ1 MMSE 推定問題であり，Expectation-Maximization (EM)アルゴリズムとして形式化される．ところが，この ℓ1MMSE 推定問題では，厳密に MMSE 規範に従って最適解を導くために，有意な信号がどこに位置するかを示す Active-set が事前に決定されている必要がある．一方，未知干渉信号や端末移動のため，通信中に Active-set が変化しうる．[*1]では，チャネル共分散行列の算出法を工夫し，事後に決定された Active-set に対し厳密に EM アルゴリズムを実行可能な ℓ1MMSE 推定法(*ℓ1iST*)を提案した．図 3 に示すとおり，提案法が未知干渉 MIMO チャネルにおいて性能限界 Normalized adaptive Cramer-Rao Bound (NaCRB)に漸近する推定性能を達成することを検証した．

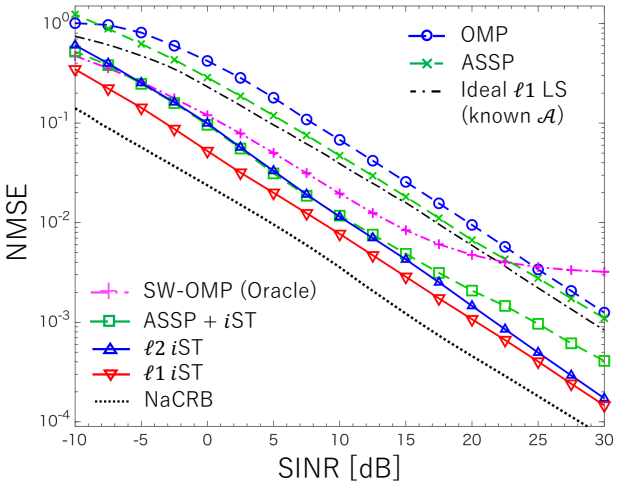

図 3　6×12 MIMO 系における NMSE 性能 (PB3, INR=0dB) [*1, Fig. 6]

3.　まとめ

本研究は，第 1 フェーズとして，チャネル推定を想定した現実的な物理層セキュリティの実現を目指し，未知干渉を含む大規模 MIMO システムでの高精度なチャネル推定法を提案した．また，チャネル推定精度が Secrecy Capacity へ及ぼす影響を議論した．そして，第 2 フェーズとして，これらの新たな知見に基づき，現実的な伝送シナリオにおけるセキュア伝送法を検討中である．検討結果の一部を国際会議に投稿し，現在，査読審査中である[*10]．引き続き，従来の暗号化と情報理論的安全性を併用したアプローチの検討を進め，Beyond 5G 通信システムの安全性向上を目指す．

【参考文献】

[1] A. D. Wyner, “The wire-tap channel,” *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang and H. H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66-74, April 2011.

[3] M. Jilani and T. 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.

[4] P. H. Lin, S. H. Lai, S. C. Lin, and H. J. Su, “On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, September 2013.

[5] Y. Takano, M. Juntti, and T. Matsumoto, “Performance of an ℓ1 regularized subspace-based MIMO channel estimation with random sequences,” *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 112–115, Feb 2016.
[6] J. Lee, G. Gil, and Y. H. Lee, “Channel estimation via orthogonal matching pursuit for hybrid MIMO systems in millimeter wave communications,” *IEEE Trans. Commun.,* vol. 64, no. 6, pp. 2370–2386, June 2016.
[7] J. Rodriguez-Fernandez, N. Gonzalez-Prelcic, K. Venugopal, and R. W. Heath, “Frequency-domain compressive channel estimation for frequency-selective hybrid millimeter wave MIMO systems,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, pp. 2946–2960, May 2018.
[8] M. Nicoli, O. Simeone, and U. Spagnolini, “Multislot estimation of fast-varying space-time communication channels,” *IEEE Trans. Signal Process.*, vol. 51, no. 5, pp. 1184 – 1195, may 2003.

〈発　表　資　料〉

	題　　名	掲載誌・学会名等	発表年月
[*1]	A Spatial–Temporal Subspace-Based Compressive Channel Estimation Technique in Unknown Interference MIMO Channels	IEEE Trans. on Signal Proc.	2020 年 1 月
[*2]	A Conditional ℓ1 Regularized MMSE Channel Estimation Technique for IBI Channels	IEEE Trans. on Wireless Commun.	2018 年 10 月
[*3]	A low-complexity LS turbo channel estimation technique for MU-MIMO systems	IEEE Signal Proc. Lett.	2018 年 5 月
[*4]	A low-complexity LS turbo channel estimation technique for MU-MIMO systems （招待ポスター発表）	IEEE Global SIP 2018. https://sigport.org/documents/globalsip-2018-poster-low-complexity-ls-turbo-channel-estimation-technique-mu-mimo-systems	2018 年 11 月
[*5]	時空間-部分空間圧縮チャネル推定を利用した MIMO 伝送性能	信学技報	2020 年 3 月
[*6]	圧縮チャネル推定の研究動向	信学技報	2020 年 1 月
[*7]	条件付き L1 正規化チャネル推定法を用いた物理層セキュリティの検討	信学技報	2019 年 1 月
[*8]	秘匿伝送を想定した大規模 MIMO システムにおけるターボチャネル推定法の高速化	信学ソ大	2018 年 9 月
[*9]	無線物理層セキュリティを用いた IoT ネットワークの検討	コンピュータセキュリティシンポジウム(CSS) 2017	2017 年 10 月
[*10]	A Joint SLNR-MMSE-based Adaptive Secure Transmission Technique for Broadband IoT Systems	*Submitted to IEEE Globecom 2020*	査読審査中 (2020/06 現在)

以上.