Précodage sécurisé pour les réseaux massivement MIMO non-cellulaires

Steve SAWADOGO[1,2] Vincent SAVAUX[1] Luc LE MAGOAROU[2] Matthieu CRUSSIÈRE[2] Patrick SAVELLI[1]

[1]Institut de Recherche Technologique b<>com, 1219 avenue des Champs Blancs, 35510 Cesson-Sévigné, France

[2]INSA Rennes, CNRS, IETR - UMR 6164, F-35000, Rennes, France

Résumé – Dans cet article, nous proposons des précodages par projection pour sécuriser les transmissions massivement MIMO pour les communications non-cellulaires. Nous dérivons trois précodages sécurisés basés sur le précodeur zéro-forcing (ZF). Le premier annule le signal transmis dans la direction non-désirée, le second sécurise d'abord le canal légitime avant le précodage ZF, et le troisième, minimise l'érreur quadratique moyenne sous contrainte de sécurité. Avec une révision de la définition usuelle du débit secret (*secrecy rate*), les résultats de simulations confirment la suppression totale du signal reçu par l'utilisateur illégitime, améliorant significativement la sécurité sans injection de bruit artificiel.

Abstract – In this paper, we introduce projection-based precoding to secure cell-free Massive MIMO systems. We derive three secure precoding based on the zero-forcing (ZF) precoder. The first one cancels the transmit signal in the undesired direction, the second one first secures the legitimate channel before ZF precoding, and the third one minimises the mean square error under secrecy constraints. With a revision of the usual definition of the secrecy rate, the simulation results show total suppression of the signal received by eavesdroppers, significantly improving secrecy without injection of artificial noise.

1 Introduction

Le MIMO massif est une technologie clé pour les réseaux sans fil futurs, offrant un débit accru, une meilleure efficacité énergétique et une fiabilité améliorée par rapport au MIMO classique. Parmi ses architectures, le MIMO massif non cellulaire (*CF-mMIMO*) est essentiel pour la 6G, reposant sur des points d'accès distribués et coordonnés par une unité centrale [2, 13]. Toutefois, cette distribution expose les réseaux aux écoutes malveillantes, nécessitant des solutions de sécurité robustes.

La sécurité des réseaux sans fil repose entre autres sur des approches cryptographiques ou des techniques de sécurité physique (Physical Layer Security, PLS). Bien que le chiffrement soit efficace, il pose des défis en gestion des clés et en complexité. Les approches classiques de sécurisation physique en MIMO massif, comme le précodage par décomposition en valeurs singulières généralisée (GSVD) [6, 7], maximisent la capacité secrète mais restent inadaptées aux systèmes non-cellulaire massivement MIMO, notamment en raison de leur dépendance à des combinaisons spécifiques (ou post-codage) du côté des utilisateurs légitimes (appellés Bob). Une approche alternative, l'injection de bruit artificiel [4], consiste à transmettre simultanément le signal utile et un bruit artificiel destiné à perturber l'interception par les utilisateurs malveillants (appelés Ève). Cependant, cette méthode nécessite une puissance d'émission plus élevée due à la transmission du bruit. La maximisation du débit secret dans les réseaux massivement MIMO, définis comme la différence entre le débit de Bob et celui d'Ève, a été étudiée via des schémas de précodage linéaire et d'allocation de puissance dans [3, 12]. Toutefois, maximiser le débit secret total ne minimise pas nécessairement la puissance reçue par Ève, et la nature non-convexe de ces problèmes d'optimisation implique un coût computationnel élevé.

Dans cet article, nous introduisons des méthodes de précodages sécurisés par projection. S'inscrivant dans le cadre général de la projection sur le noyau (Null-Space Projection, NSP) [10, 7], la méthode proposée diffère du NSP classique car elle ne nécéssite pas de décomposition en valeurs singulières (SVD), pour la construction d'une base du noyau. Nous construisons un projecteur sur le complément orthogonal au canal d'Ève, directement à l'aide de ce dernier. Deux approches sont ainsi introduites : la méthode du précodeur projeté, où le signal transmis est projeté sur le complément orthogonal au canal d'Ève et la méthode du canal projeté où la matrice de canal légitime est d'abord projeté sur le complément orthogonal du canal d'Ève, avant d'appliquer un précodage sur ce canal nouvellement obtenu. Ces deux approches sont moins complexes que celles reposant sur des problèmes d'optimisation et ne nécéssitent pas de SVD, contrairement aux méthodes de la littérature. De plus, nous introduisons un précodeur MMSE sous contrainte d'orthogonalité au canal d'Ève et montrons qu'il s'agit également d'un précodeur MMSE projeté. Ainsi, contrairement aux méthodes qui maximisent le débit secret, ces trois méthodes assurent l'orthogonalité du signal transmis au canal d'Ève, ce qui annule le débit sur Ève. Les simulations sur des environnements intérieurs à trajets multiples comme proposé par l'organisme 3GPP [1], démontrent des améliorations significatives du débit secret, métrique que reformulons pour explicitement prendre en compte la capacité d'Ève à décoder le signal intercepté.

Le reste de cet article est organisé comme suit : la section 2 présente le modèle du système d'étude, la section 3 présente le précodage sécurisé par projection, les métriques de performance sont présentées en section 4, puis les analyses et résultats de simulations en section 5, et enfin la section 6 conclut cet article.

Notations : Les lettres minuscules en gras $\mathbf{a}$ et normales a représentent respectivement les vecteurs et scalaires. Les lettres majuscules $\mathbf{A}$ représentent les matrices. $\mathbf{A}^H$ indique la transposée conjuguée de la matrice $\mathbf{A}$. $\|.\|_F$ et $\mathbb{E}[.]$ représentent respectivement la norme de Frobenius et l'espérance mathématique. Les matrices $\mathbf{0}_N$ and $\mathbf{I}_N$ sont respectivement les matrices nulles et identités de taille N.

2 Modèle du Système d'Étude

Considérons un système massivement MIMO non-cellulaire où L points d'accès, chacun équipé de réseaux d'antennes planaires de M éléments, desservent conjointement $K = K_b + K_e$

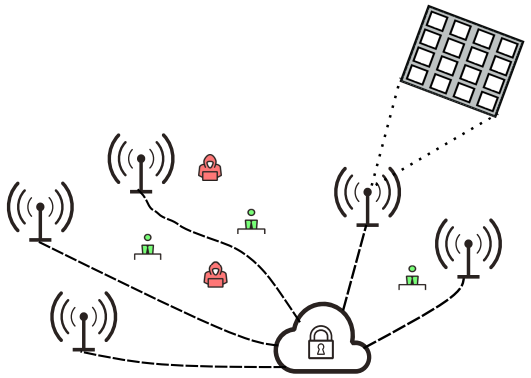

FIGURE 1 : Réseaux massivement MIMO non-cellulaire

utilisateurs mono-antennes, comme illustrés dans la Figure 1. Les K_b premiers, appelés Bob, sont légitimes, tandis que les K_e restants, appelés Eve, sont malveillants. Le canal entre un utilisateur k et tous les points d'accès est noté $\mathbf{h}_k \in \mathbb{C}^{ML}$. En supposant la connaissance parfaite des canaux, nous construisons les vecteurs de précodage $\mathbf{w}_k \in \mathbb{C}^{ML}$ pour chaque utilisateur légitime. Le signal reçu par les utilisateurs est donné par :

$$\mathbf{y} = \mathbf{HWs} + \mathbf{n} \tag{1}$$

où $\mathbf{H} = [\mathbf{h}_0, \cdots, \mathbf{h}_{K-1}]^T \in \mathbb{C}^{K \times ML}$ et $\mathbf{W} = [\mathbf{w}_0, \cdots, \mathbf{w}_{K-1}]^T \in \mathbb{C}^{ML \times K_b}$ sont les matrices de canaux et de précodage, $\mathbf{s} \in \mathbb{C}^{K_b}$ contient les symboles transmis, et $\mathbf{n} \in \mathbb{C}^K$ représente le bruit blanc gaussien de variance σ^2 sur chaque utilisateur. La puissance totale de transmission disponible pour l'ensemble du système est limitée à P.

Nous définissons les matrices de canaux $\mathbf{H}_b \in \mathbb{C}^{Kb \times ML}$ pour Bob et $\mathbf{H}_e \in \mathbb{C}^{Ke \times ML}$ pour Eve. Contrairement à [10], nous adoptons une projection sécurisée sans décomposition SVD. Le signal confidentiel est projeté sur le complément orthogonal de $\mathbf{H}_e$, noté $\mathbb{H}_{e\perp}$, annulant ainsi toute interception par Eve. La matrice de projection associée est :

$$\mathbf{P}_{e^\perp} = \mathbf{I}_{ML} - \mathbf{H}_e^H (\mathbf{H}_e \mathbf{H}_e^H)^{-1} \mathbf{H}_e. \tag{2}$$

Deux techniques de précodage sécurisé basées sur le précodeur zéro-forcing sont développées : le précodeur projeté et le canal projeté. Bien que nous choisissions ici le précodeur ZF [2], d'autres précodeurs pourraient être utilisés avec les techniques de précodage ci-dessous.

3 Précodage Sécurisé par Projection

3.1 Méthode du Précodeur Projeté

La méthode du précodeur projeté (PP) consiste à projeter le signal précodé (avec un précodeur conventionnel, sans contraintes de sécurité) dans le complement orthogonal à l'espace d'Eve, avec la matrice $\mathbf{P}_{e^\perp}$. Le précodeur obtenu avec cette méthode et noté $\mathbf{W}_{pp}$, s'écrit :

$$\mathbf{W}_{pp} = \frac{1}{\beta_{pp}} \mathbf{P}_{e^\perp} \mathbf{H}_b^H \left(\mathbf{H}_b \mathbf{H}_b^H\right)^{-1}, \tag{3}$$

où $\beta_{pp} = \sqrt{\frac{\|\mathbf{P}_{e^\perp} \mathbf{H}_b^H \left(\mathbf{H}_b \mathbf{H}_b^H\right)^{-1}\|_F^2}{P}}$ est le facteur de normalisation de la puissance transmise. Le signal transmis $\mathbf{W}_{pp}\mathbf{s}$ est donc orthogonal à $\mathbf{H}_e$ ($\mathbf{H}_e \mathbf{W}_{pp} \mathbf{s} = \mathbf{0}$). Cela est soutenu par des résultats expérimentaux dans la Section 5.2

3.2 Méthode du canal projeté

Cette approche se décline en deux étapes : sécuriser le canal de Bob en le projetant sur le complément orthogonal à l'espace d'Ève, puis appliquer un précodage conventionnel sur le canal obtenu. L'expression du précodeur obtenu avec cette méthode, noté $\mathbf{W}_{pc}$, s'écrit :

$$\mathbf{W}_{pc} = \frac{1}{\beta_{pc}} \mathbf{P}_{e^\perp} \mathbf{H}_b^H \left(\mathbf{H}_b \mathbf{P}_{e^\perp} \mathbf{H}_b^H\right)^{-1}, \tag{4}$$

où $\beta_{pc} = \sqrt{\frac{\|\mathbf{P}_{e^\perp} \mathbf{H}_b^H \left(\mathbf{H}_b \mathbf{P}_{e^\perp} \mathbf{H}_b^H\right)^{-1}\|_F^2}{P}}$ est le facteur de normalisation. Comme avec (3), le signal transmis est orthogonal à $\mathbf{H}_e$.

proposition 1 *Le précodeur décrit dans (4) peut être réécrit sous une forme plus intuitive et directe. Plus précisement, on peut montrer :*

$$\mathbf{W}_{pc} = \frac{1}{\beta_{pc}} \mathbf{H}^H \left(\mathbf{H}\mathbf{H}^H\right)^{-1} \mathbf{M}, \tag{5}$$

où $\mathbf{M} = \left[\mathbf{I}_{K_b}^T, \mathbf{O}_{K_e \times K_b}^T\right]^T$.

La preuve, omise ici pour concision, repose sur l'inversion par blocs de $\mathbf{HH}^H$, suivie de l'extraction du premier bloc-colonne via une multiplication par $\mathbf{M}$.

L'expression (5) montre que la méthode du canal projeté appliquée au ZF diagonalise les canaux de Bob et Ève (par inversion de canal), puis oriente le signal confidentiel vers Bob tout en supprimant les faisceaux dirigés vers Ève.

3.3 Méthode du MMSE contraint

L'approche consiste à minimiser l'erreur quadratique moyenne sur Bob [2] tout en annulant le signal intercepté par Eve. Le précodeur est solution du problème d'optimisation suivant :

$$\mathrm{O}_1 : \begin{cases} \underset{\mathbf{W}}{\operatorname{argmin}}\ \mathbb{E}\left\{\|\mathbf{y}_b - \mathbf{s}\|_F^2\right\} \\ s.t. \quad \mathbb{E}\left\{\|\mathbf{Ws}\|_F^2\right\} = P \quad (\mathrm{C_P}) \\ s.t. \quad \mathbf{H}_e \mathbf{Ws} = \mathbf{0} \quad (\mathrm{C_S}) \end{cases} . \tag{6}$$

Le problème O_1 est convexe et peut etre résolu par la technique des multiplieurs de Lagrange, qui donne la solution suivante noté $\mathbf{W}_{sc}^{MMSE}$:

$$\begin{aligned} &\mathbf{W}_{sc}^{MMSE} \\ &= \underbrace{\left(\mathbf{H}_b^H \mathbf{H}_b + \lambda_P \mathbf{I}_{ML}\right)^{-1}}_{\mathbf{G'}_b^{-1}} \mathbf{H}^H \left[\mathbf{I}_{K_b}, -\mathbf{A}_{ee}^{-1} \mathbf{A}_{eb}\right]^T \\ &= \underbrace{\mathbf{G}_b^{-1} \mathbf{H}_b^H}_{\mathbf{W}^{MMSE}} - \mathbf{G}_b^{-1} \mathbf{H}_e^H \left(\mathbf{H}_e \mathbf{G}_b^{-1} \mathbf{H}_e^H\right)^{-1} \mathbf{H}_e \underbrace{\mathbf{G}_b^{-1} \mathbf{H}_b^H}_{\mathbf{W}^{MMSE}} \\ &= \underbrace{\left[\mathbf{I}_{ML} - \mathbf{G}_b^{-1} \mathbf{H}_e^H \left(\mathbf{H}_e \mathbf{G}_b^{-1} \mathbf{H}_e^H\right)^{-1} \mathbf{H}_e\right]}_{\overline{\mathbf{P}}_{e^\perp}} \underbrace{\mathbf{G}_b^{-1} \mathbf{H}_b^H}_{\mathbf{W}^{MMSE}} \end{aligned} \tag{7}$$

où λ_P est le multiplieur de Lagrange associé à la contrainte C_P et $\mathbf{A}_{xy} \triangleq \mathbf{H}_x \mathbf{G}_b^{-1} \mathbf{H}_y^H$, $\forall x, y \in \{b, e\}$. Le précodeur MMSE secrètement contraint s'obtient en soustrayant du précodeur MMSE conventionnel la contribution responsable de la fuite d'énergie vers Ève. De plus, la matrice $\overline{\mathbf{P}}_{e^\perp}$ étant une projection sur $\mathbb{H}_{e^\perp}$ selon le produit scalaire induit par $\mathbf{G}_b^{-1}$, fait du MMSE contraint un MMSE projeté.

Ici, la sécurité des transmissions repose sur l'orthogonalité au canal d'Ève. Pour évaluer la performance des précodeurs, des métriques de sécurité sont employées.

4 Métriques de Performance

4.1 Débit Secret Usuel

Le débit secret, noté R_s est définis comme [3] :

$$\mathrm{R}_s = |\mathrm{R}_b - \mathrm{R}_e|^+, \tag{8}$$

où $|.|^+ = \max(.,0)$ et, R_b et R_e représentent respectivement les débits de Bob et Eve, donnés par :

$$\mathrm{R}_b = \sum_{k=0}^{K_b-1} \log_2\left(1+\frac{\alpha_k P_t}{\gamma_k P_t+\sigma^2}\right), \tag{9}$$

$$\mathrm{R}_e = \sum_{k'=K_b}^{K_b+K_e-1} \log_2\left(1+\frac{\nu_{k'} P_t}{\sigma^2}\right), \tag{10}$$

avec les α_k, γ_k et ν'_k représentant respectivement les gains normalisés du canal de Bob, des interférences entre utilisateurs légitimes, et du canal d'Ève. Le débit secret, largement étudié en sécurité de la couche physique [3, 12], ne reflète pas directement la capacité d'Ève à décoder le message. En effet, une valeur de R_s peut masquer un débit élevé pour Ève lorsque $\mathrm{R}_b > \mathrm{R}_e$, lui permettant ainsi d'intercepter l'information. Pour pallier cette limite, nous redéfinissons cette métrique en intégrant explicitement la capacité d'Ève à intercepter le signal.

4.2 Débit Secret Proposé

Supposons que le système puisse injecter du bruit artificiel sur Ève [4], afin de limiter son débit à une valeur cible ε, en prélevant la puissance nécessaire notée P_n de la puissance totale P_t. Un compromis doit alors être trouvé entre l'allocation au bruit artificiel et au signal utile. Le débit secret proposé, noté R_s^*, est défini comme le débit de Bob lorsque celui d'Ève est maintenu à ε :

$$\mathrm{R}_s^* = \sum_{k=0}^{K_b-1} \log_2\left(1+\frac{\alpha_k |P_t-P_n|^+}{\gamma_k |P_t-P_n|^+ +\sigma^2}\right) \tag{11}$$

$$\text{s.t. } \mathrm{R}^e_{k'} \le \varepsilon, \forall k' \in \{K_b,\cdots,K_b+K_e-1\},$$

où $\mathrm{R}^e_{k'}$ est le débit sur le k'-ième utilisateurs illégitimes, soumis à l'injection de bruit artificiel. La puissance de bruit minimale nécéssaire à remplir la condition de sécurité dans (11) notée $P_n^{\min}$ est :

$$P_n^{\min} \triangleq \max_{k'} \frac{|\nu_{k'} P_t - \sigma^2(2^\varepsilon-1)|^+}{\nu_{k'}+\omega_{k'}(2^\varepsilon-1)}, \tag{12}$$

où $\omega_{k'}$ représente l'atténuation du bruit artificiel sur Ève. Dans la suite de l'article, on considère que $P_n = P_n^{\min}$.

Des résultats de simulations sont proposés dans la section suivante, permettant d'évaluer les méthodes proposées et de les comparer avec des méthodes classiques.

5 Simulation et Discussion

5.1 Paramètres de Simulations

La simulation modélise un bâtiment industriel à un seul étage, basé sur le modèle 3GPP [1], avec des dimensions de 120 m $\times$50 m $\times$10 m. Six points d'accès multi-antennes ($L = 6$, $M = 16$), avec un espacement inter-éléments équivalent à une demi-longueur d'onde, sont installés au plafond à une hauteur de 9,5 m et fonctionnent à une fréquence porteuse de $f_c = 28$GHz (communications en ondes millimétriques). Bob et Eve sont modélisés comme des récepteurs mono-antennes positionnés à 1,5m du sol.

Trois scénarios de propagation sont simulés : faible corrélation, corrélation moyenne, forte corrélation, correspondant aux configurations 1, 2 et 3 de la Figure 2, respectivement. La génération des canaux est réalisée à l'aide de Sionna Ray-Tracing [5], une bibliothèque basée sur TensorFlow pour la simulation des communications sans fil et optiques. Matlab est utilisé pour la génération des figures.

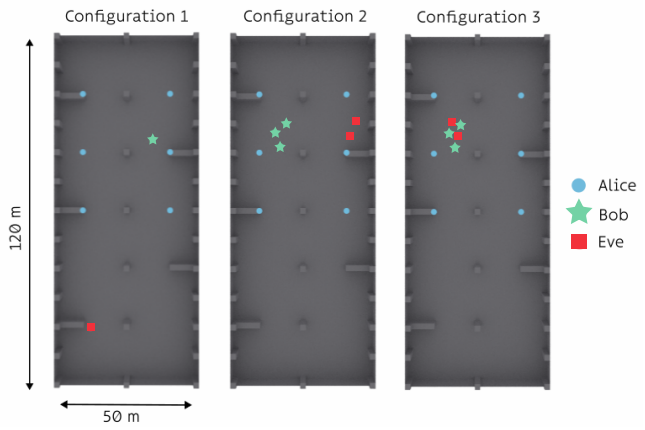

FIGURE 2 : Environnement de simulation

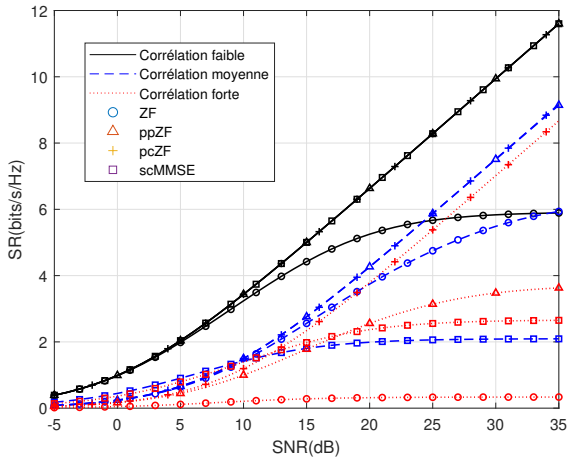

FIGURE 3 : Débit secret usuel

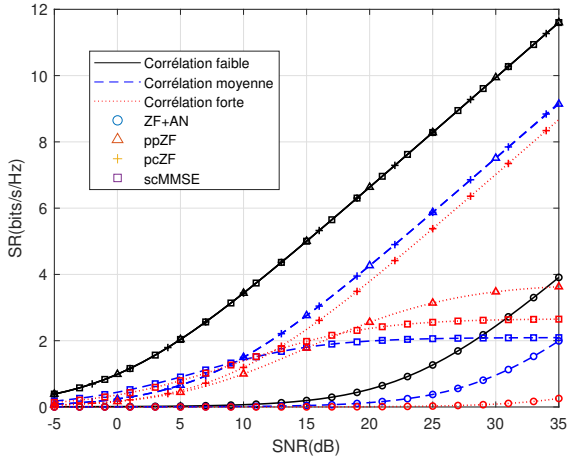

FIGURE 4 : Débit secret proposé

5.2 Résultats de Simulations

La figure 3 illustre les débits secrets (bits/s/Hz) définis dans (8) en fonction du SNR (dB). Pour une comparaison équitable, les débits de Bob et Ève sont normalisés par K_b et K_e, respectivement. Les préfixes "pp", "pc" et "sc" sur la figure 3 repésentent respectivement les méthodes précodeur projeté, canal projeté et MMSE secrètement contraint. On observe que les courbes du ZF conventionnel atteignent un palier, car

le débit d'Ève atteint celui de Bob. Ce comportement des trajectoires du ZF conventionnel dans chaque configuration de corrélation soutient davantage l'introduction de la métrique proposée dans (11), illustrée en figure 4 avec $\varepsilon = 10^{-4}$.

Sur la figure 4, les précodeurs sécurisés (ppZF, pcZF, scMMSE) conservent leurs performances en comparaison à la figure 3, sans nécessiter d'injection de bruit artificiel, car garantissant l'orthogonalité au canal d'Ève même lorsque ce dernier est proche de Bob. Cela corrobore les résultats théoriques de la section 3 sur l'orthogonalité des précodeurs au canal d'Ève. La nouvelle métrique permet une comparaison plus juste avec les méthodes basées sur l'injection de bruit. Ainsi, le ZF conventionnel avec bruit artificiel présente un faible débit secret, car la majorité de la puissance est principalement allouée au bruit artificiel.

La méthode du canal projeté surpasse celle du précodeur projeté, notamment en cas de forte corrélation des canaux. En effet, le précodeur projeté appliqué au ZF introduit des interférences entre utilisateurs légitimes, conduisant à la perte de performance. À l'inverse, le canal projeté maintient l'orthogonalité entre utilisateurs légitimes (typique du ZF) et au canal d'Ève, garantissant un débit secret non borné. Enfin, le précodeur MMSE contraint excelle à faible SNR (≈ 5dB), tandis que le ZF devient plus performant à fort SNR (≈ 25 dB), conformément aux attentes théoriques : le MMSE atténue le bruit à bas SNR, alors que le ZF supprime les interférences inter-utilisateurs, qui domine à SNR élevé.

5.3 Discussion

Les résultats présentés dans cet article reposent sur l'hypothèse forte d'une connaissance de canaux (CSI) parfaite, notamment celle d'Eve. Des travaux comme [8, 11] montrent qu'une estimation partielle reste possible, même pour un espion passif, à travers des techniques de détection. Cela motive une analyse de robustesse à la CSI imparfaite, menée dans [9], où les précodeurs proposés, se révèlent résistants aux erreurs gaussiennes de CSI, notamment pcZF qui permet une atténuation notable des interférences due aux erreurs de CSI, confirmée par simulations.

La complexité computationnelle des solutions proposées reste aussi un enjeu, car ces méthodes reposent sur des opérations matricielles couteuses lorsque $ML \gg K_b, K_e$, comme dans les systèmes massivement MIMO. Une version étendue de cet article devrait établir une analyse comparative de la complexité computationnellle des précodeurs proposés avec celle de précodeurs existants, tel que le GSVD.

6 Conclusion

Cet article propose de nouvelles techniques de précodage par projection pour sécuriser les communications en réseaux massivement MIMO non-cellulaires. Deux approches sont développées : le précodeur projeté, qui annule la fuite d'information vers Ève en projetant le signal transmis sur l'orthogonal de son canal, et le canal projeté, qui sécurise d'abord le canal de Bob avant le précodage, améliorant ainsi la confidentialité. Un précodeur MMSE avec une contrainte additionnelle de sécurité est également introduit, garantissant l'orthogonalité du signal transmis au canal d'Ève. Les simulations confirment des gains substantiels en sécurité, même lorsque Bob et Ève sont proches, sans nécessiter d'injection de bruit artificiel. Les recherches futures exploreront l'efficacité énergétique secrète sous des contraintes d'allocation de puissance des points d'accès.

Références

[1] 3GPP : Study on Channel Model for Frequencies from 0.5 to 100 GHz (Release14). Rapport technique, ETSI 3rd Generation Partnership Project (3GPP), Sophia Antipolis, France, May 2017.

[2] Emil BJÖRNSON, Jakob HOYDIS et Luca SANGUINETTI : Massive MIMO Networks : Spectral, Energy, and Hardware Efficiency. *Foundations and Trends® in Signal Processing*, 11(3–4):154–655, 2017.

[3] Jinseok CHOI et Jeonghun PARK : Sum Secrecy Spectral Efficiency Maximization in Downlink MU-MIMO : Colluding Eavesdroppers. *IEEE Transactions on Vehicular Technology*, 70(1):1051–1056, 2021.

[4] S. GOEL et R. NEGI : Secret communication in presence of colluding eavesdroppers. *In MILCOM 2005 - 2005 IEEE Military Communications Conference*, pages 1501–1506 Vol. 3, 2005.

[5] Jakob HOYDIS, Faycal Ait AOUDIA, Sebastian CAMMERER, Merlin NIMIER-DAVID, Nikolaus BINDER, Guillermo MARCUS et Alexander KELLER : Sionna RT : Differentiable Ray Tracing for Radio Propagation Modeling. *In 2023 IEEE Globecom Workshops (GC Wkshps)*, pages 317–321, 2023.

[6] Ashish KHISTI et Gregory W. WORNELL : Secure Transmission With Multiple Antennas I : The MISOME Wiretap Channel. *IEEE Transactions on Information Theory*, 56(7):3088–3104, 2010.

[7] Ashish KHISTI et Gregory W. WORNELL : Secure Transmission With Multiple Antennas—Part II : The MIMOME Wiretap Channel. *IEEE Transactions on Information Theory*, 56(11):5515–5532, 2010.

[8] Amitav MUKHERJEE et A. Lee SWINDLEHURST : Detecting passive eavesdroppers in the MIMO wiretap channel. *In 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 2809–2812, 2012.

[9] Steve SAWADOGO, Vincent SAVAUX, Luc Le MAGOAROU, Matthieu CRUSSIÈRE et Patrick SAVELLI : Robust Precoding design for Secure MIMO Communication with Imperfect CSI. mai 2025.

[10] Shabnam SODAGARI, Awais KHAWAR, T. Charles CLANCY et Robert MCGWIER : A projection based approach for radar and telecommunication systems coexistence. *In 2012 IEEE Global Communications Conference (GLOBECOM)*, pages 5010–5014, 2012.

[11] Nanchi SU, Fan LIU et Christos MASOUROS : Sensing-Assisted Eavesdropper Estimation : An ISAC Breakthrough in Physical Layer Security. *IEEE Transactions on Wireless Communications*, 23(4):3162–3174, 2024.

[12] Dong WANG, Bo BAI, Wenbo ZHAO et Zhu HAN : A Survey of Optimization Approaches for Wireless Physical Layer Security. *IEEE Communications Surveys and Tutorials*, 21(2):1878–1911, 2019.

[13] Jiayi ZHANG, Shuaifei CHEN, Yan LIN, Jiakang ZHENG, Bo AI et Lajos HANZO : Cell-Free Massive MIMO : A New Next-Generation Paradigm. *IEEE Access*, 7:99878–99888, 2019.