Enhanced Physical Layer Security through Frequency and Spatial Diversity

Idowu Iseoluwa Ajayi

SORBONNE UNIVERSITÉ

École Doctorale Informatique, Télécommunications et Electronique

Laboratoire d'Informatique, Signal et Image, Électronique et Télécommunications

THÈSE

présentée par : **Idowu Iseoluwa AJAYI**
soutenue le : **26 juin 2023**

pour obtenir le grade de : **Docteur de Sorbonne Université**

préparée au : **École Doctorale Informatique, Télécommunications et Electronique**

Enhanced Physical Layer Security through Frequency and Spatial Diversity

THÈSE dirigée par :

[**Mme Lina MROUEH**] Professeure, ISEP

et co-encadrée par :

[**M. Yahia MEDJAHDI**] Maître de Conférences, IMT Nord-Europe

[**Mme Fatima KADDOUR**] Ingénieure de Recherche, ANFR

Jury

M. Yves LOUET	Professeur, CentraleSupélec	Président
M. Didier LE RUYET	Professeur, CNAM	Rapporteur
M. Sebastien HOUCKE	Professeur, IMT-Atlantique	Rapporteur
Mme Nour EL MADHOUN	Associate Professor, ISEP	Examinatrice
M. Aissa IKHLEF	Associate Professor, Durham University	Examinateur

Acknowledgements

I would like to give all the glory to God Almighty for giving me the grace to successfully complete this thesis, and receive awards for it. I want to convey my deepest appreciation to Prof. Lina Mroueh, my supervisor, for her invaluable guidance and support during the course of my research. Her willingness and readiness to pay attention to all details of my research work was a real blessing. I am truly grateful for her guidance and supervision. I would also like to specially say a big thank you to Dr. Yahia Medjahdi, my Co-Supervisor during the thesis. His level of commitment, zeal, and passion was admirable. He was always available and never stopped bringing up ideas to make the thesis more impactful. For his constructive feedback and suggestions, which have not only enhanced the quality of my research but also provided me with a broader understanding of the world of research, thank you. Dr. Fatima Kaddour was my industrial supervisor, and she certainly contributed massively to the success of the thesis. Her contributions were nothing short of excellent and made the thesis much better. Indeed, I was blessed with a wonderful supervisory team.

To my beautiful wife, Oluwatosin Ajayi, she is indeed an invaluable support system for me. She gave me her full support throughout my thesis and celebrated all my big and small wins with me. Her listening ears, advice, prayers, and sacrifices mean the world to me. To my parents, it gives me joy to see how proud they are of me. I am deeply thankful for the knowledge they have imparted, their unwavering support, encouraging words, and the unending motivation they offered throughout my research journey. My siblings also never made me feel alone and were a support system whose impact cannot be over-emphasized.

Throughout my Ph.D. journey, I have been privileged to meet many friends and individuals who have made this journey extremely memorable for me. I would like to extend my heartfelt thanks to each of them.

Abstract

Physical layer security (PLS) is an emerging paradigm that focuses on using the properties of wireless communication, such as noise, fading, dispersion, interference, diversity, etc., to provide security between legitimate users in the presence of an eavesdropper. Since PLS uses signal processing and coding techniques, it takes place at the physical layer and hence can guarantee secrecy irrespective of the computational power of the eavesdropper. This makes it an interesting approach to complement legacy cryptography whose security premise is based on the computational hardness of the encryption algorithm that cannot be easily broken by an eavesdropper. The advancements in quantum computing has however shown that attackers have access to super computers and relying on only encryption will not be enough. In addition, the recent rapid advancement in wireless communication technologies has seen the emergence and adoption of technologies such as Internet of Things, Ultra-Reliable and Low Latency Communication, massive Machine-Type Communication, Unmanned Aerial Vehicles, etc. Most of these technologies are decentralized, limited in computational and power resources, and delay sensitive. This makes PLS a very interesting alternative to provide security in such technologies.

To this end, in this thesis, we study the limitations to the practical implementation of PLS and propose solutions to address these challenges. First, we investigate the energy efficiency challenge of PLS by artificial noise (AN) injection in massive Multiple-Input Multiple-Output (MIMO) context. The large precoding matrix in massive MIMO also contributes to a transmit signal with high Peak-to-Average Power Ratio (PAPR). This motivated us to propose a novel algorithm , referred to as PAPR-Aware-Secure-mMIMO. In this scheme, instantaneous Channel State Information (CSI) is used to design a PAPR-aware AN that simultaneously provides security while reducing the PAPR. This leads to energy efficient secure massive MIMO. The performance is measured in terms of secrecy capacity, Symbol Error Rate (SER), PAPR, and Secrecy Energy Efficiency (SEE). Next, we consider PLS by channel adaptation. These PLS schemes depend on the accuracy of the instantaneous CSI and are

ineffective when the CSI is inaccurate. However, CSI could be inaccurate in practice due to such factors as noisy CSI feedback, outdated CSI, etc. To address this, we commence by proposing a PLS scheme that uses precoding and diversity to provide PLS. We then study the impact of imperfect CSI on the PLS performance and conclude with a proposal of a low-complexity autoencoder neural network to denoise the imperfect CSI and give optimal PLS performance. The proposed autoencoder models are referred to as DenoiseSecNet and HybDenoiseSecNet respectively. The performance is measured in terms of secrecy capacity and Bit Error Rate (BER).

Finally, we study the performance of PLS under finite-alphabet signaling. Many works model performance assuming that the channel inputs are Gaussian distributed. However, Gaussian signals have high detection complexity because they take a continuum of values and have unbounded amplitudes. In practice, discrete channel inputs are used because they help to maintain moderate peak transmission power and receiver complexity. However, they introduce constraints that significantly affect PLS performance, hence, the related contribution in this thesis. We propose the use of dynamic keys to partition modulation spaces in such a way that it benefits a legitimate receiver and not the eavesdropper. These keys are based on the independent main channel and using them to partition leads to larger decision regions for the intended receiver but smaller ones for the Eavesdropper. The scheme is referred to as Index Partitioned Modulation (IPM). The performance is measured in terms of secrecy capacity, mutual information and BER.

Keywords : Physical layer security, massive MIMO, artificial noise, peak-to-average power ratio, secrecy energy efficiency, index-partitioned modulation, artificial intelligence, channel adaptation, autoencoder, precoding.

Résumé

La sécurité de la couche physique (PLS) est un paradigme émergent qui se concentre sur l'utilisation des propriétés de la communication sans fil, telles que le bruit, l'évanouissement, la dispersion, l'interférence, la diversité, etc. pour assurer la sécurité entre les utilisateurs légitimes en présence d'un espion. Comme le PLS utilise des techniques de traitement du signal et de codage, il intervient au niveau de la couche physique et peut donc garantir le secret quelle que soit la puissance de calcul de l'espion. Cela en fait une approche intéressante pour compléter la cryptographie traditionnelle dont le principe de sécurité est basé sur la dureté informatique de l'algorithme de cryptage qui ne peut pas être facilement cassé par un espion. Les progrès de l'informatique quantique ont toutefois montré que les attaquants ont accès à des superordinateurs et qu'il ne suffira pas de s'appuyer sur le seul cryptage. En outre, les récents progrès rapides des technologies de communication sans fil ont permis l'émergence et l'adoption de technologies telles que l'internet des objets, les communications ultra-fiables et à faible latence, les communications massives de type machine, les véhicules aériens sans pilote, etc. La plupart de ces technologies sont décentralisées, limitées en ressources de calcul et de puissance, et sensibles aux délais. La plupart de ces technologies sont décentralisées, limitées en ressources de calcul et de puissance, et sensibles aux délais. Cela fait du PLS une alternative très intéressante pour assurer la sécurité dans ces technologies.

À cette fin, dans cette thèse, nous étudions les limites de la mise en œuvre pratique de la PLS et proposons des solutions pour relever ces défis. Tout d'abord, nous étudions le défi de l'efficacité énergétique du PLS par l'injection de bruit artificiel (AN) dans un contexte massif d'entrées multiples et de sorties multiples (MIMO). La grande matrice de précodage dans le contexte MIMO massif contribue également à un signal d'émission avec un rapport élevé entre la puissance de crête et la puissance moyenne (PAPR). Cela nous a incités à proposer un nouvel algorithme, appelé PAPR-Aware-Secure-mMIMO. Dans ce schéma, les informations instantanées sur l'état du canal (CSI) sont utilisées pour

concevoir un AN conscient du PAPR qui assure simultanément la sécurité tout en réduisant le PAPR. Il en résulte un MIMO massif sécurisé et économe en énergie. Les performances sont mesurées en termes de capacité de secret, de taux d'erreur de symbole (SER), de PAPR et d'efficacité énergétique du secret (SEE). Ensuite, nous considérons le PLS par adaptation de canal. Ces schémas PLS dépendent de la précision de la CSI instantanée et sont inefficaces lorsque la CSI est imprécise. Cependant, la CSI peut être inexacte dans la pratique en raison de facteurs tels qu'un retour d'information bruyant, une CSI périmée, etc. Pour résoudre ce problème, nous commençons par proposer un schéma PLS qui utilise le précodage et la diversité pour fournir le PLS. Nous étudions ensuite l'impact Les modèles d'autoencodeurs proposés sont appelés DenoiseSecNet et HybDenoiseSecNet respectivement. Les modèles d'autoencodeur proposés sont appelés respectivement DenoiseSecNet et HybDenoiseSecNet. Les performances sont mesurées en termes de capacité de secret et de taux d'erreur binaire (TEB).

Enfin, nous étudions les performances de la PLS dans le cadre d'une signalisation à alphabet fini. De nombreux travaux modélisent les performances en supposant que les entrées du canal sont distribuées de manière gaussienne. Cependant, les signaux gaussiens ont une grande complexité de détection car ils prennent un continuum de valeurs et ont des amplitudes non limitées. Dans la pratique, on utilise des entrées de canal discrètes parce qu'elles permettent de maintenir une puissance de transmission de crête et une complexité de réception modérées. Cependant, elles introduisent des contraintes qui affectent de manière significative la performance du PLS, d'où la contribution de cette thèse. Nous proposons d'utiliser des clés dynamiques pour partitionner les espaces de modulation de manière à ce qu'ils profitent à un récepteur légitime et non à un espion. Ces clés sont basées sur le canal principal indépendant et leur utilisation pour la partition conduit à des régions de décision plus grandes pour le récepteur prévu et plus petites pour l'espion. Ce système est appelé modulation partitionnée par index (IPM). Les performances sont mesurées en termes de capacité de secret, d'information mutuelle et de TEB.

Mots clés : Sécurité de la couche physique, MIMO massif, bruit artificiel, rapport de puissance crête-moyenne, efficacité énergétique du secret, modulation indexée, intelligence artificielle, adaptation du canal, autoencodeur, précodage.

Résumé des travaux de thèse

Chapitre 1 - Introduction

Motivation

Au cours de la dernière décennie, la société et l'économie ont évolué vers une forte dépendance aux réseaux de communication sans fil et à l'accès à l'internet. Cette évolution a vu le web passer du web statique des années 1990 au web social (web 2.0), au web sémantique (web 3.0) et plus récemment au web des objets (web 4.0) [1]. Cependant, cette connectivité accrue a également exposé les utilisateurs aux cyberattaques, à l'espionnage et au vol de données, mettant ainsi en danger la vie privée et les informations personnelles.

La sécurité des communications a traditionnellement reposé sur la cryptographie, mais elle présente des limites en termes de ressources informatiques et de complexité. De plus, l'avènement de l'informatique quantique remet en question son efficacité [2]. C'est pourquoi la sécurité de la couche physique (PLS) est devenue un nouveau paradigme pour améliorer la sécurité des communications sans fil. La PLS est rapide, légère et utilise les caractéristiques des canaux sans fil pour empêcher les espions de décoder les données, sans imposer de contraintes sur leurs capacités de calcul ni nécessiter de gestion de clés [3, 4].

Objectifs de la thèse

Cette thèse apporte des contributions dans les principales catégories de PLS. Dans toutes ces catégories, l'objectif est de proposer une nouvelle solution pour répondre à une limitation dans l'application pratique de la PLS. En termes généraux, nous aimerions faire ce qui suit :

- Relever simultanément le défi de l'efficacité énergétique dans les systèmes massifs à entrées et sorties multiples (MIMO) et de la PLS par injection de bruit artificiel (AN).

- Étudier l'impact d'une information instantanée imparfaite sur l'état du canal (CSI) dans une approche PLS d'adaptation au canal qui utilise le précodage et la diversité pour la sécurité.

- Proposer une solution au problème de l'imperfection de l'ICS instantanée dans l'application de la PLS par l'adaptation du canal à l'aide de techniques d'intelligence artificielle (IA).

- Étendre les travaux sur la PLS non seulement à la signalisation d'entrée gaussienne, mais aussi à la signalisation d'alphabet fini, qui est une réalité pratique dans les scénarios de déploiement.

- Proposer un nouveau schéma PLS dans le cadre des techniques PLS basées sur les clés avec des contraintes d'entrée à alphabet fini.

Chapitre 2 - Principes fondamentaux de la PLS et autres concepts clés de la thèse

La sécurité de la couche physique

Le paradigme de la sécurité de la couche physique (PLS) suscite un grand intérêt récemment [3,4]. Il exploite les caractéristiques des canaux sans fil pour assurer la confidentialité des communications entre un émetteur (Alice) et un récepteur légitime (Bob), tout en protégeant contre un espion puissant (Eve), illustré à la figure 1. La PLS présente des avantages tels qu'une complexité de calcul réduite par rapport à la cryptographie traditionnelle et une sécurité potentielle sur le plan quantique.

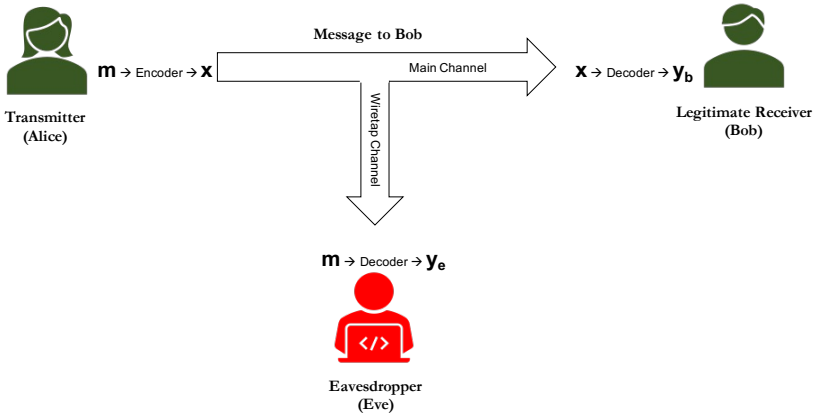


Figure 1: Modèle de canal d'écoute.

La PLS devient de plus en plus pertinente en raison de la croissance exponentielle de technologies

telles que l'internet des objets (IoT), la communication d'appareil à appareil (D2D), les drones (UAV), la communication ultra-fiable et à faible latence (URLLC), les communications massives de type machine (mMTC), les ondes millimétriques (mmWave), la communication térahertz, etc. Ces technologies sont souvent décentralisées, limitées en ressources et sensibles à la latence, ce qui nécessite des solutions de sécurité adaptées, telles que la PLS, en complément de la cryptographie traditionnelle [5].

Métriques PLS

Il existe plusieurs mesures dans la littérature, telles que la capacité de secret, la probabilité d'interruption du secret, le débit de secret, l'écart de sécurité mesuré en termes de taux d'erreur sur les bits (TEB), etc. [4]. Le choix des mesures est basé sur l'approche PLS considérée et, dans cette thèse, nous utiliserons la capacité de secret et le TEB pour quantifier les gains de sécurité des différents schémas.

Capacité de secret

La présente thèse adopte le canal filaire à évanouissement, et un type fondamental est celui qui prend en compte les antennes uniques d'Alice, de Bob et d'Eve. Dans ce cas, à un intervalle de temps donné, pour un message, m, transmis sous la forme x, Bob reçoit $y_b = h_b x + z_b$, et Eve reçoit $y_e = h_e x + z_e$, où h_b et h_e sont des variables gaussiennes complexes à moyenne nulle, à évanouissement de Rayleigh, avec une variance unitaire pour les canaux principaux et les canaux d'écoute. z_b et $z_e \sim \mathcal{N}_{\mathbb{C}}(0, \sigma^2)$ sont les bruits blancs gaussiens additifs (AWGN) indépendants avec des variances σ_b^2 et σ_e^2 respectivement chez Bob et Eve. La capacité de secret est la mesure PLS la plus répandue et elle est définie comme le débit de transmission maximal auquel l'espion ne peut décoder aucune information [6]. Avec une contrainte de puissance de P, elle est égale à la différence positive entre la capacité du canal principal et la capacité du canal d'écoute. Une valeur positive signifie que le secret est réalisable et un zéro implique qu'il n'y a pas de garantie de secret. Nous mesurons la capacité de secret en b/s/Hz (ou bits/utilisation du canal).

À l'origine, dans [6], la capacité de secret est calculée à l'aide de la capacité du canal de Shannon qui donne la capacité maximale du canal en supposant une signalisation gaussienne. Si l'on considère la formulation pour la signalisation à alphabet fini, la capacité du canal est mesurée en termes d'information mutuelle. Ainsi, pour les contributions des chapitres 3 et 4 de cette thèse, nous adoptons

le premier calcul de la capacité de secret, tandis que dans la contribution finale du chapitre 5, nous adoptons le second. Par conséquent, l'expression générale de la capacité de secret dans cette thèse est la suivante:

$$C_s = \begin{cases} \left[\log_2\left(1+\gamma_b\right) - \log_2\left(1+\gamma_e\right)\right]^+ & \text{si signalisation gaussienne,} \\ \left[\mathrm{I}_b(m,y_b) - \mathrm{I}_e(m,y_e)\right]^+, & \text{si Signalisation alphabétique finie.} \end{cases} \tag{1}$$

où γ est le rapport signal/bruit (RSB) dans un canal à évanouissement est donné par $\gamma = P|h|^2/\sigma^2$.

Taux d'erreur binaire

Dans cette thèse, nous évaluons la sécurité en comparant le RSB requis par Bob et Eve pour atteindre des TEB cibles. Un système atteignant un faible RSB pour un TEB donné est considéré plus sûr que ceux nécessitant un RSB élevé. Nous calculons numériquement le TEB comme la moyenne des erreurs binaires par unité pour toutes les réalisations du canal, et vérifions également théoriquement certaines contributions de la thèse.

Plusieurs approches ont été adoptées dans le cadre du PLS et sont généralement classées comme suit : L'injection d'AN, l'adaptation du canal et les techniques de clé de canal. Toutes ces approches PLS ont leurs avantages et leurs inconvénients. Par conséquent, le choix de l'approche PLS optimale à utiliser dépend des particularités de la transmission et des exigences de l'utilisateur.n, and channel key techniques. All of these PLS approaches have their merits and demerits. Hence, the choice of an optimal PLS approach to employ depends on the peculiarities of the transmission and the user requirements.

Chapitre 3 - Efficacité énergétique dans la MIMO massive sécurisée

Dans ce chapitre, nous étudions la relation importante entre la fourniture de PLS par l'utilisation de l'injection d'AN et l'efficacité énergétique du système qui en résulte. Le schéma PLS par injection d'AN exploite les degrés de liberté spatiaux excédentaires entre l'émetteur et le récepteur. Par conséquent, le grand nombre d'antennes d'émission par rapport au récepteur dans le MIMO massif offre la possibilité de déployer l'injection d'AN. Cependant, le MIMO massif souffre de signaux d'émission ayant un rapport puissance de crête/puissance moyenne (PAPR) élevé en raison de la grande taille de sa matrice

de précodage. Il est important de noter que le PAPR élevé du signal d'émission dans la MIMO massive peut être accentué par la superposition en phase entre le signal d'information et les sous-espaces AN. Par conséquent, si la conception n'est pas soignée, nous risquons d'assurer la sécurité au détriment de l'efficacité énergétique.

Modèle de système

Transmission MIMO massive en liaison descendante

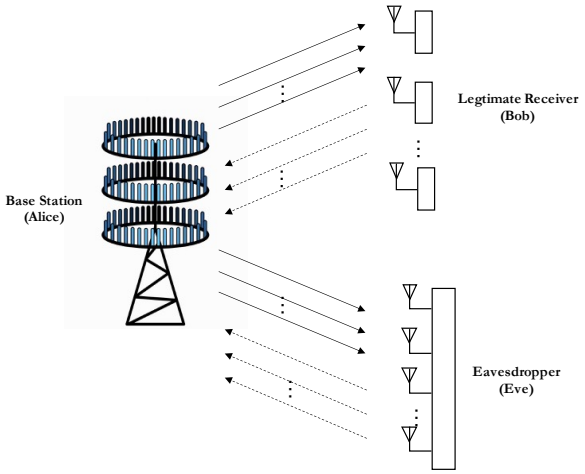


Figure 2: Modèle de système de transmission MIMO massive en liaison descendante précodée AN avec N_t antennes à la station de base, N_r récepteurs légitimes à antenne unique et $N_{r,e}$ antennes à l'espion, où $N_t \gg N_r, N_{r,e}$.

Nous considérons une transmission MIMO massive unicellulaire en liaison descendante entre une station de base (Alice) dotée de N_t antennes et N_r terminaux récepteurs légitimes à antenne unique en présence d'un espion passif (Eve) équipé de $N_{r,e}$ antennes de réception, comme le montre la figure 2. Eve peut être perçue soit comme un espion doté de plusieurs antennes, soit comme plusieurs espions à antenne unique qui peuvent collaborer et effectuer une détection coopérative. Dans notre étude, nous considérons la situation dans laquelle tous les espions collaborent pour espionner les informations transmises à un seul terminal légitime. En fait, dans cette thèse, Bob représente un terminal parmi les N_r terminaux disponibles. Notons que N_t est significativement plus grand que N_r et $N_{r,e}$ ($N_t \gg N_r, N_{r,e}$).

Nous partons de l'hypothèse d'un environnement de diffusion riche en visibilité directe et, à ce titre, nous modélisons tous les canaux comme des canaux de Rayleigh à évanouissement plat non corrélés. On suppose que le canal principal, $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$, peut être parfaitement estimé et est disponible à la

station de base en utilisant la réciprocité des canaux en mode TDD. Cette propriété est couramment utilisée dans la littérature relative au MIMO massif en mode TDD [7–10]. Nous supposons qu'Alice ne connaît pas le CSI d'Eve, $\mathbf{H}_e \in \mathbb{C}^{N_{r,e} \times N_t}$. Les entrées de $\mathbf{H}$ et $\mathbf{H}_e$ sont des variables gaussiennes complexes indépendantes et identiquement distribuées (i.i.d.) à moyenne nulle et à variance unitaire.

Deux méthodes de précodage ont été envisagées dans ce travail : ZF et MF. Le précodage MF, plus facile à mettre en œuvre, maximise simplement le SNR au niveau du récepteur légitime uniquement, tandis que le précodage ZF vise à annuler les interférences multi-utilisateurs (MUI) entre les récepteurs légitimes. La complexité de calcul du précodage ZF est examinée dans [11,12]. Le vecteur de précodage, $\mathbf{F} \in \mathbb{C}^{N_t \times N_r}$, peut être écrit comme suit

$$\mathbf{F} = \begin{cases} \mathbf{H}^\dagger (\mathbf{H}\mathbf{H}^\dagger)^{-1}, & \text{si Précodage ZF,} \\ \left[\frac{\mathbf{h}_1^\dagger}{\|\mathbf{h}_1\|}, \ldots, \frac{\mathbf{h}_{N_r}^\dagger}{\|\mathbf{h}_{N_r}\|} \right], & \text{si Précodage MF.} \end{cases} \tag{2}$$

Ainsi, le signal d'émission précodé, $\boldsymbol{v} \in \mathbb{C}^{N_t \times 1}$ pour un vecteur de données, $\boldsymbol{s} \in \mathbb{C}^{N_r \times 1}$ avec N_r valeurs complexes, peut être exprimé comme suit

$$\boldsymbol{v} = \sqrt{\frac{1}{\psi}} \mathbf{F} \boldsymbol{s}, \tag{3}$$

où ψ est la norme de Frobenius de $\mathbf{F}$ qui est incluse pour la normalisation (dérivation donnée dans la section 3.11) et s'exprime simplement comme suit

$$\psi = \begin{cases} \frac{N_r}{N_t - N_r}, & \text{si Précodage ZF,} \\ N_r, & \text{si Précodage MF.} \end{cases} \tag{4}$$

Bruit artificiel Transmission précodée

Pour un système précodé AN avec une puissance totale disponible P, le budget de puissance est respecté en répartissant la puissance entre le signal d'information et l'AN. La puissance allouée au signal d'information est représentée par θP tandis que le reste du budget de puissance, $(1-\theta)P$, est consacré à l'AN, où $0 < \theta \leq 1$.

Nous calculons la matrice de l'espace nul, $\mathbf{V} \in \mathbb{C}^{N_t \times N_t}$, pour $\mathbf{H}$ en utilisant la pseudo-inverse de Moore-Penrose [13]:

$$\mathbf{V} = \mathbf{I}_{N_t} - \mathbf{H}^\dagger (\mathbf{H}\mathbf{H}^\dagger)^{-1} \mathbf{H}. \tag{5}$$

Nous adoptons une répartition égale de la puissance entre toutes les antennes d'émission. Ainsi, lorsqu'un AN aléatoire est injecté dans l'espace nul du canal principal, le signal d'émission, $\boldsymbol{x} \in \mathbb{C}^{N_t \times 1}$ pour un vecteur de données, $\boldsymbol{s} \in \mathbb{C}^{N_r \times 1}$ avec N_r valeurs complexes, peut être exprimé comme suit

$$\boldsymbol{x} = \sqrt{\frac{\theta}{\psi}}\mathbf{F}\boldsymbol{s} + \sqrt{\frac{1-\theta}{\xi}}\mathbf{V}\boldsymbol{k}, \tag{6}$$

où $\boldsymbol{k} \in \mathbb{C}^{N_t \times 1}$ est l'AN généré aléatoirement avec une matrice de covariance $\sigma_k^2\mathbf{I}_{N_t}$, tandis que ξ est la norme de Frobenius de $\mathbf{V}$ (dérivation donnée dans la section 3.11) qui est incluse pour la normalisation et s'exprime simplement comme suit

$$\xi = N_t - N_r. \tag{7}$$

Pour le m-ième terminal légitime, le symbole reçu est donné comme suit

$$y_{b_m} = \begin{cases} \sqrt{\frac{\theta}{\psi}}s_m + z_b, & \text{if Précodage ZF,} \\ \sqrt{\frac{\theta}{\psi}}\mathbf{h}_m\mathbf{f}_m s_m + \sum\limits_{\substack{i=1 \\ i\neq m}}^{N_r}\sqrt{\frac{\theta}{\psi}}\mathbf{h}_m\mathbf{f}_i s_i + z_b, & \text{if Précodage MF,} \end{cases} \tag{8}$$

où s_m est le m-ième élément du vecteur de données d'émission $\boldsymbol{s}$, et le s_i restant est le i-ième élément du vecteur de données transmis à d'autres récepteurs dans la même cellule, et $z_b \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_b^2)$ est la composante AWGN complexe au terminal légitime avec une variance σ_b^2 qui n'est pas corrélée avec s_m. Le premier terme du signal précodé MF dans (8) est le signal désiré dont le SNR est maximisé en raison du précodage MF, et le second terme indique le MUI intracellulaire. C'est la principale différence avec le précodage ZF dont le MUI est nul, ce qui garantit une excellente qualité de transmission pour les utilisateurs légitimes. Toutefois, cela se fait au détriment de la complexité de calcul.

Le signal reçu par l'espion, $\boldsymbol{y}_{e_1} \in \mathbb{C}^{N_{r,e} \times 1}$, est le suivant

$$\boldsymbol{y}_{e_1} = \sqrt{\frac{\theta}{\psi}}\mathbf{H}_e\mathbf{F}\boldsymbol{s} + \sqrt{\frac{1-\theta}{\xi}}\mathbf{H}_e\mathbf{V}\boldsymbol{k} + \boldsymbol{z}_e, \tag{9}$$

où $\boldsymbol{z}_e \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_e^2\mathbf{I}_{N_{r,e}})$ est l'échantillon AWGN i.i.d. avec une matrice de covariance $\sigma_e^2\mathbf{I}_{N_{r,e}}$.

PAPR-Aware-Secure-mMIMO ALGORITHM

Dans le PAPR-Aware-Secure-mMIMO, nous commençons par appliquer un précodage linéaire au signal qui donne une haute qualité de transmission (3). Nous appliquons ensuite un algorithme itératif

pour évaluer les signaux d'atténuation des crêtes. Cela permet de réduire le rapport PAPR du signal de transmission et d'améliorer la sécurité.

Pour obtenir le PAPR optimal, les fortes amplitudes du signal d'émission sont itérativement écrêtées jusqu'à un seuil optimal avant la transmission. Le seuil d'écrêtage, λ_ℓ, pour chaque itération est la puissance moyenne du signal à l'itération multipliée par le PAPR cible (PAPR_0), en substance

$$\lambda_\ell = \mathbb{E}[|\boldsymbol{\upsilon}_\ell|^2] \times \text{PAPR}_0. \tag{10}$$

Nous représentons le signal écrêté par $\boldsymbol{d}$ et le signal excédentaire après écrêtage par $\boldsymbol{z}$ dont l'amplitude et la phase de $\boldsymbol{z}$ sont telles que $|\boldsymbol{z}_\ell| = [|\boldsymbol{\upsilon}_\ell| - \sqrt{\lambda}_\ell]^+$ et $\text{phase}(\boldsymbol{z}_\ell) = \text{phase}(\boldsymbol{\upsilon}_\ell)$. Sous une autre forme, l'excès de signal après écrêtage peut être exprimé comme suit :

$$\boldsymbol{z} = [\boldsymbol{\upsilon} - \boldsymbol{d}]^+. \tag{11}$$

Pour chaque réalisation de canal, le signal excédentaire optimal à chaque étape d'itération de l'algorithme est celui qui représente notre AN ($\boldsymbol{\omega}$) tenant compte du PAPR, projeté dans l'espace nul. Essentiellement, le signal excédentaire optimal est donné par la formule suivante

$$\boldsymbol{z}_\ell = \mathbf{V}\boldsymbol{\omega}_\ell. \tag{12}$$

Cependant, le signal d'annulation de crête est à peine égal à $\boldsymbol{z}$. Pour relever ce défi, nous utilisons le problème d'optimisation convexe (13) ci-dessous.

$$\begin{aligned} &\text{Find } \arg\min_{\boldsymbol{\omega}} \|\mathbf{V}\boldsymbol{\omega} - \boldsymbol{z}\|_2^2, \\ &\text{subject to } \begin{cases} \boldsymbol{z} = [\boldsymbol{\upsilon} - \boldsymbol{d}]^+ \\ \text{PAPR}(\boldsymbol{d}) \leq \text{PAPR}_0. \end{cases} \end{aligned} \tag{13}$$

La première contrainte garantit que seul le signal excédentaire après l'écrêtage est utilisé pour concevoir l'AN tenant compte du PAPR. La deuxième contrainte garantit que le PAPR du signal écrêté ne dépasse pas le PAPR cible. Le problème d'optimisation ci-dessus peut être résolu à l'aide de la méthode SGD [14, 15]. Les directions de recherche du gradient le plus raide à chaque étape d'itération de l'algorithme sont données par le gradient négatif de $\boldsymbol{G}$ à $\boldsymbol{\omega}_\ell$ dénoté par

$$\nabla_{\omega_\ell} \boldsymbol{G}(\boldsymbol{\omega}_\ell) = \frac{2}{\mathcal{L}_\omega} \mathbf{V}^\dagger (\mathbf{V}\boldsymbol{\omega}_\ell - \boldsymbol{z}_\ell), \tag{14}$$

où $\mathcal{L}_e = 2\sigma^2_{\mathbf{max}}(\mathbf{V})$ est la constante de Lipschitz [16] pour $\|\mathbf{V}\boldsymbol{\omega} - \boldsymbol{z}\|_2^2$. D'après (14), à chaque étape d'itération, le PAPR-aware an est mis à jour comme suit

$$\boldsymbol{\omega}_{\ell+1} = \boldsymbol{\omega}_\ell - \nabla_{\omega_\ell}\boldsymbol{G}(\boldsymbol{\omega}_\ell), \tag{15}$$

et le signal pour l'étape suivante de l'algorithme est mis à jour comme suit

$$\boldsymbol{\upsilon}_{\ell+1} = \boldsymbol{\upsilon}_\ell + p_\ell \mathbf{V}\boldsymbol{\omega}_\ell, \tag{16}$$

où p est un facteur de régularisation calculé à l'aide de l'approximation des moindres carrés (LSA) [17]. En utilisant ce facteur de régularisation, l'amplitude des signaux d'annulation de crête générés par LSA est presque égale à celle du bruit d'écrêtage original. Elle peut être exprimée comme suit

$$p_\ell = \frac{|\ \mathbf{V}\boldsymbol{\omega}_\ell\ |^{\mathrm{T}} |\ \boldsymbol{z}_\ell\ |}{\|\mathbf{V}\boldsymbol{\omega}_\ell\|^2}. \tag{17}$$

Comme nous l'avons décrit précédemment, l'AN final tenant compte du PAPR pour chaque réalisation de canal est la somme normalisée des $p_\ell \mathbf{V}\boldsymbol{\omega}_\ell$ pour chaque étape de l'itération. Par conséquent, à l'étape finale de l'algorithme, nous obtenons le signal précodé AN tenant compte du rapport PAPR, $\ddot{\boldsymbol{x}} \in \mathbb{C}^{N_t \times 1}$, qui s'écrit comme suit

$$\ddot{\boldsymbol{x}} = \sqrt{\frac{\theta}{\psi}}\mathbf{F}\boldsymbol{s} + \sqrt{\frac{(1-\theta)}{\xi}}\mathbf{V}\frac{\ddot{\boldsymbol{\omega}}}{\sigma_{\ddot{\omega}}}, \tag{18}$$

where

$$\ddot{\boldsymbol{\omega}} = \sum p_\ell \mathbf{V}_{\boldsymbol{\ell}}\boldsymbol{\omega}_{\boldsymbol{\ell}},$$

and $\sigma_{\ddot{\boldsymbol{\omega}}}$ is the standard deviation of the total injected AN $\ddot{\boldsymbol{\omega}}$.

La capacité du canal principal reste la même que dans le cas de l'injection aléatoire d'un AN, puisque cet AN reste transparent pour Bob et n'a pas d'impact sur le canal principal. En outre, grâce à la normalisation de l'AN tenant compte du PAPR, $\ddot{\boldsymbol{\omega}}$, et au respect de la condition d'attribution de puissance égale, la capacité du canal d'écoute électronique restera la même que lorsque nous injectons un AN aléatoire. Par conséquent, la condition d'attribution d'une puissance égale est remplie pour l'AN réduisant le PAPR lorsque

$$\psi\sigma_s^2 + \sigma_{\ddot{\omega}}^2 = P. \tag{19}$$

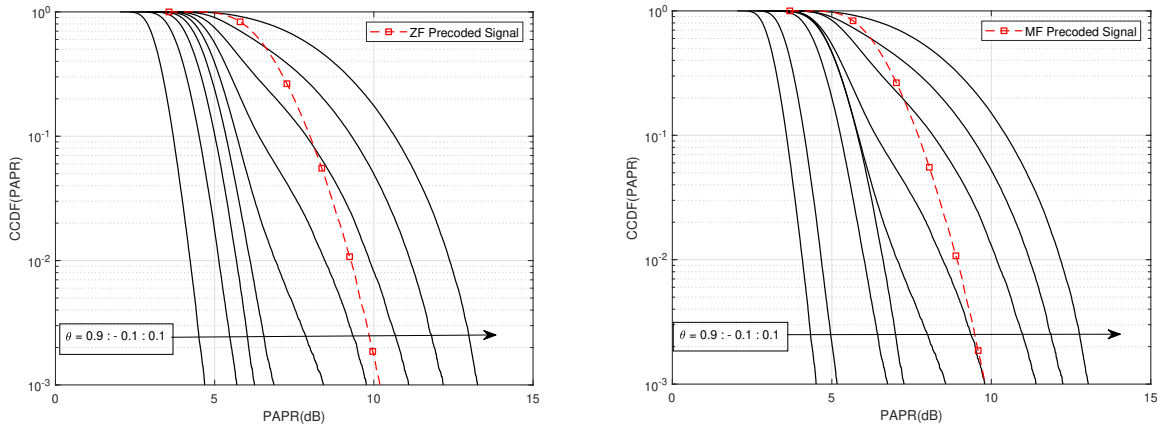
Intuitivement, nous nous attendons à ce que les capacités de secret soient les mêmes puisque les covariances de l'AN aléatoire et de l'AN tenant compte du PAPR sont les mêmes. En substance, le gain de secret dû à l'injection d'AN reste le même,

$$C_{s_2} = C_{s_1}. \tag{20}$$

Performance du PAPR-Aware-Secure-mMIMO en cas d'évanouissement de Rayleigh non corrélé

Dans cette section, nous présentons les résultats de la simulation pour le schéma PAPR-Aware-Secure-mMIMO proposé pour l'amélioration de la sécurité et la réduction du PAPR. Dans toutes les simulations, 40 itérations de l'algorithme sont effectuées pour chaque réalisation de canal. Nous considérons $N_t = 70$ antennes à la station de base (Alice), $N_r = 10$ récepteurs légitimes à antenne unique tandis que Bob est 1 sur les 10, et $N_{r,e} = 10$ antennes coopératives d'écoute clandestine. Nous utilisons la fonction de distribution cumulative complémentaire (FDCC) pour évaluer la performance de la réduction du PAPR, qui désigne la probabilité que le PAPR du signal estimé dépasse un seuil donné.

Allocation optimale de la puissance

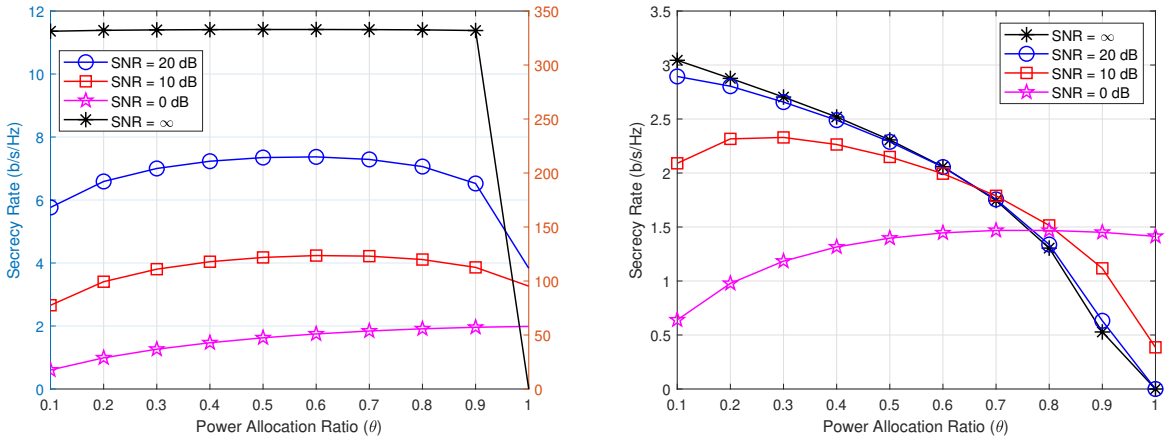


(a) Zero-Forcing. (b) Matched Filter.

Figure 3: Performance PAPR en fonction du rapport d'allocation de puissance : $\theta = 0.9$ correspond à la courbe la plus à gauche et $\theta = 0,.$ correspond à la courbe la plus à droite.

Pour connaître l'allocation optimale de puissance pour le schéma PAPR-Aware-Secure-mMIMO, nous examinerons son impact sur les performances en termes de PAPR et de capacité de secret. La

figure 3 montre l'impact de θ sur les performances en matière de PAPR. Il existe un compromis entre le rapport PAPR atteint et le pourcentage de la puissance allouée à l'AN. Il convient de noter que $\theta \in]0, 1]$ où $\theta = 1$ correspond au cas du précodage ZF/MF sans injection d'AN. Lorsque $\theta = 0$, le signal utile est nul et il n'est pas nécessaire de concevoir un AN tenant compte du PAPR. Plus la puissance allouée à l'AN est importante (c'est-à-dire lorsque θ diminue), plus le PAPR augmente de manière significative. Nous observons que lorsque la puissance allouée à l'AN est trop importante, l'algorithme n'est plus efficace, ce qui se traduit par un PAPR égal ou supérieur au PAPR sans injection d'AN (précodage ZF/MF uniquement). En fait, nous observons un PAPR très élevé allant jusqu'à 13,3 dB lorsque θ = 0,1 et on peut en déduire que le PAPR élevé est l'effet combiné de l'augmentation du PAPR due au précodage MIMO massif et à l'injection d'AN. Comme moins de puissance est allouée à l'AN conscient du PAPR, nous observons une diminution constante du PAPR atteint et nous obtenons un PAPR de 4,6 dB lorsque $\theta = 0,9$ pour le précodage ZF et un PAPR de 6,50 dB lorsque $\theta = 0,6$ pour le précodage MF.



(a) Zero-Forcing. (b) Matched Filter.

Figure 4: Performances en matière de capacité de confidentialité du système AN-assisté proposé par rapport au ratio d'allocation de puissance (θ) à différents régimes de SNR.

L'étape suivante de la proposition d'un θ optimal consiste à étudier son effet sur la capacité de secret du système, comme le montre la figure 4a. Différents régimes de RSB sont pris en compte : faible RSB ($\overline{\gamma}$ = 0 dB), RSB moyen ($\overline{\gamma}$ = 10 dB), RSB élevé ($\overline{\gamma}$ = 20 dB) et RSB très élevé ($\overline{\gamma} = \infty$). Pour les deux schémas de précodage, dans le régime de faible RSB, la capacité de secret augmente à mesure que l'on attribue plus de puissance au signal utile. Ceci est évident du fait que la capacité de secret est significativement affectée par le bruit thermique dans cette région. Pour les régions à

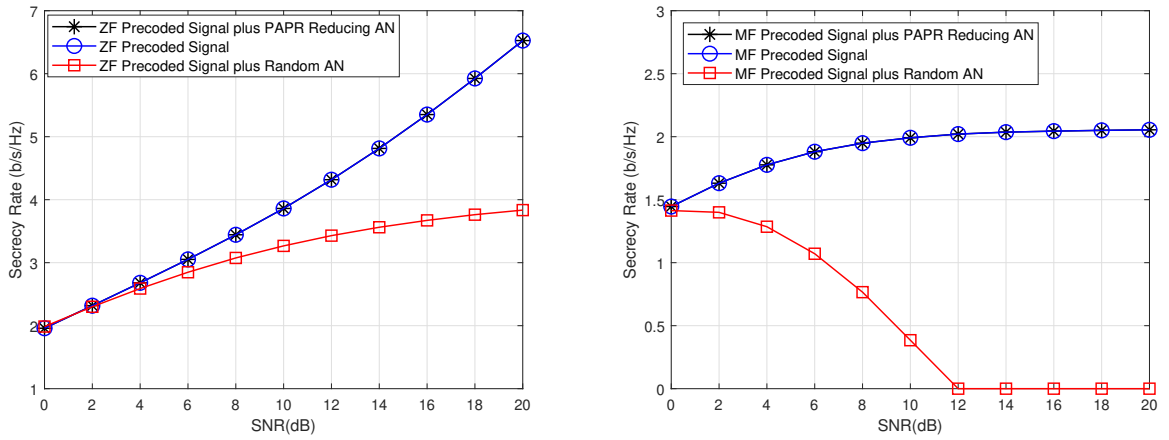
RSB plus élevé avec précodage ZF (figure 4a), la capacité de secret devient plus élevée et atteint ses valeurs maximales lorsque θ est compris entre 0,5 et 0,6. Cela correspond approximativement à une répartition égale de la puissance entre le signal utile et l'AN. Toutefois, lorsque $\theta = 0,9$, la capacité de secret n'est que légèrement inférieure à la valeur maximale, mais le PAPR à une CCDF de 0,1% est le plus faible à ce stade. Par conséquent, $\theta = 0,9$ est un rapport d'attribution de puissance optimal pour le précodage ZF. Il s'agit d'un argument en faveur d'un rapport optimal dérivé numériquement et non d'un point optimal mathématique. Il convient de noter que le côté gauche de l'axe des y de la figure 3.4a correspond aux $\overline{\gamma} = 0, 10, \text{et } 20dB$, tandis que l'échelle de l'axe des y de droite correspond à $\overline{\gamma} = \infty$.

En revanche, sur la figure 4b, pour les trois régions à SNR plus élevé avec précodage MF, nous observons des pentes négatives pour les trois. Plus la puissance allouée au signal utile est importante, plus la capacité de secret diminue. Cela indique que l'injection d'AN est nécessaire pour les régimes à SNR élevé, car sans AN, la capacité de Bob à antenne unique sera plus affectée par le MUI que la capacité de l'espion coopératif. Toutefois, nous devons veiller à attribuer un rapport de puissance optimal à l'AN, car une augmentation de la puissance de l'AN entraîne une augmentation du PAPR. Par conséquent, la simulation montre qu'un choix de θ=0,6 est un rapport d'allocation optimal pour le schéma PAPR-Aware-Secure-mMIMO avec précodage MF [1]. Avec un CCDF de 0,1

Capacité de cryptage et taux d'erreur des symboles atteints

Dans la figure 5, les performances en matière de capacité de secret du système assisté par AN sont représentées en fonction du RSB moyen. Nous supposons que le RSB moyen est le même pour Bob et Eve. Avec 70 antennes de station de base et un rapport d'attribution de puissance θ=0,9/0,6 pour le précodage ZF et MF respectivement, nous considérons la capacité d'un terminal légitime unique sur 10 utilisateurs légitimes et la capacité d'une Eve coopérative composée de 10 antennes de réception. Pour Eve, nous examinons la capacité par rapport à la réception d'un seul symbole transmis. Nous pouvons observer sur la figure 5a que lorsque nous transmettons le signal précodé ZF sans injection d'AN, la capacité de secret est de 2 b/s/Hz à SNR = 0 dB. Avec l'augmentation du SNR, ce taux augmente légèrement pour atteindre une limite de 4 b/s/Hz. Ce résultat est conforme aux travaux réalisés dans [18] où les auteurs ont montré qu'en considérant un seul terminal, la transmission sécurisée peut

[1] En outre, il s'agit d'un argument pour un rapport optimal qui est dérivé numériquement et non d'un point optimal mathématique



(a) Zero-Forcing à $\theta = 0.9$.

(b) Matched Filter à $\theta = 0.6$.

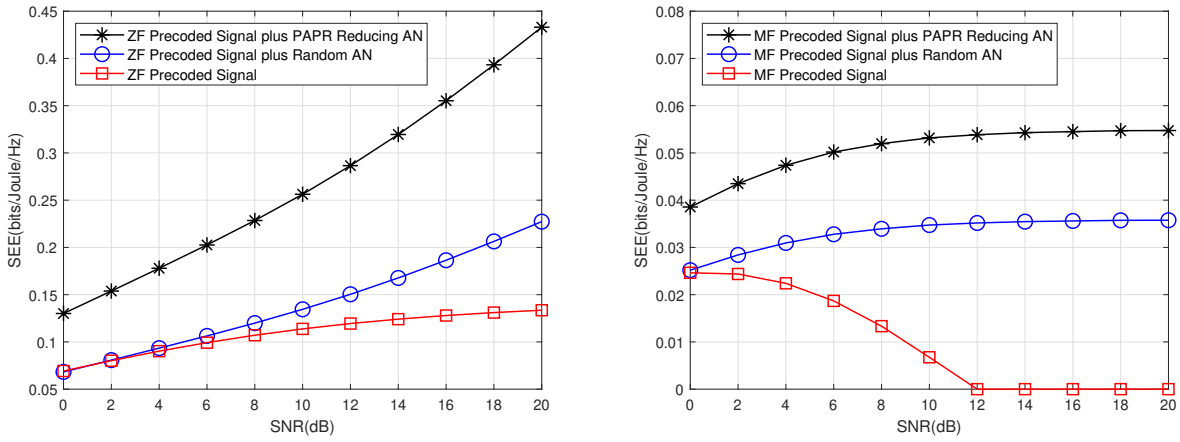
Figure 5: Performance de la capacité de sécurité du système assisté par AN proposé par rapport à la capacité avec injection aléatoire d'AN et sans injection d'AN.

être limitée en MIMO massive avec écoute passive si le nombre d'antennes d'écoute est trop important. Toutefois, avec l'injection d'AN, le schéma de transmission permet une amélioration continue de la capacité de secret réalisable à mesure que le RSB augmente. Essentiellement, la capacité de secret C_s augmente puisque C_e est limitée par la variance de l'AN dans un régime de RSN élevé, tandis que C_b continue d'augmenter. Il convient de noter que les graphiques ont été simulés en supposant que Bob et Eve ont le même RSB, ce qui n'est pas toujours le cas dans la pratique. Il est possible qu'Eve ait un avantage de position par rapport à Bob et donc un meilleur RSB. En substance, l'injection de la technique AN reste une technique de sécurité utile pour la MIMO massive. Toutefois, cette capacité de secret est la même dans les deux cas, lorsque nous injectons un AN aléatoire, comme dans les travaux sur l'AN traditionnels, et lorsque nous injectons l'AN de réduction du PAPR que nous proposons. C'est là l'avantage du système que nous proposons, car nous obtenons le secret offert par les anciens systèmes AN, mais avec un PAPR réduit, ce qui le rend moins coûteux et plus facile à mettre en œuvre dans la pratique.

De même, pour le signal précodé MF transmis avec AN dans la figure 5b, la capacité de secret commence à 1,5 b/s/Hz dans la région de faible SNR et augmente lentement jusqu'à une valeur stable d'environ 2 b/s/Hz dans les régions de SNR plus élevé. Toutefois, sans l'injection d'AN, la capacité de secret diminue fortement et le secret est complètement perdu à partir d'un RSB moyen de 12 dB. C'est l'effet du MUI dans les régions à SNR élevé qui fait que le Bob à antenne unique a une capacité

inférieure à celle du Eve à 10 antennes coopératives.

Gain d'efficacité énergétique



(a) Zero-Forcing à $\theta = 0.9$.

(b) Matched Filter à $\theta = 0.6$.

Figure 6: Performance en matière de sécurité et d'efficacité énergétique du système assisté par AN proposé par rapport à la capacité avec injection aléatoire d'AN et sans injection d'AN.

Nos systèmes proposés avec un PAPR de 4,6 dB/6,5 dB pour le précodage ZF/MF auront des HPA avec de meilleures efficacités que les anciens systèmes avec un PAPR de 10,1 dB. Ainsi, pour que nos systèmes proposés et les anciens systèmes atteignent une linéarité complète, nous introduisons des IBO de -4,6 dB/-6,5 dB et de -10,1 dB respectivement. Ces chiffres sont basés sur les valeurs du PAPR à une CCDF de 0,1%, comme le montre la figure 3. Le choix d'un niveau de 0,1% implique qu'après l'introduction de l'IBO, 99,9 % du signal se situera dans la région linéaire de la HPA. Il a été démontré dans [19] que 100mW/200mW par antenne est une puissance d'émission optimale dans une liaison descendante MIMO massive utilisant le précodage ZF/MF. À mesure que l'IBO augmente, l'efficacité de l'APH diminue, ce qui entraîne une augmentation de la consommation totale d'énergie. La consommation d'énergie plus élevée pour la même capacité de secret entraîne une baisse de la SEE. Nous observons donc sur la figure 6 que le schéma que nous proposons présente les meilleures performances en termes de SEE, surpassant les schémas avec ou sans injection d'AN. Pour l'option de précodage ZF de la figure 6a, le gain SEE du schéma proposé est significativement le plus élevé et présente une pente positive à mesure que le RSB moyen augmente. Le schéma avec injection aléatoire d'AN est légèrement plus performant que le schéma sans injection d'AN. Cela est dû au fait que les deux consomment la même énergie, mais que le premier a une capacité de secret plus élevée.

Dans la figure 6b, nous observons que pour l'option de précodage MF, la performance SEE pour le schéma proposé augmente jusqu'à la valeur stable la plus élevée à mesure que le RSB moyen augmente. Ensuite, le schéma avec injection aléatoire d'AN est plus performant que le schéma sans injection d'AN. Dans ce dernier cas, la SEE passe à zéro à partir de 12 dB. Cela indique que la capacité de secret dans les régimes de SNR élevés pour ce schéma est nulle parce que l'IUM limite davantage le Bob à antenne unique que l'espion coopératif. Les systèmes MIMO massifs permettent de remédier à ce problème en augmentant le nombre d'antennes d'émission, mais le champ d'application du présent travail est limité à un système MIMO massif avec 70 antennes de station de base seulement.

Chapitre 4 - Sécurité de la couche physique grâce à la diversité et au précodage

Introduction

Dans ce chapitre, nous commençons par proposer un schéma PLS qui combine le précodage MF et la diversité de fréquence dans un schéma de transmission OFDM. L'objectif de ce système est de réduire les performances de l'espion tout en conservant les performances attendues de Bob. Pour assurer une communication sécurisée en présence d'un espion, le précodeur MF adaptatif garantit que seul Bob conserve le gain de diversité fourni par le schéma de répétition. Étant donné que les signaux écoutés sont précodés à l'aide de l'ICS de l'utilisateur légitime, Eve perdra le gain de diversité et connaîtra un TEB plus élevé et une capacité de canal plus faible que Bob. Cette dégradation d'Eve par rapport à Bob garantit la sécurité des communications en présence d'Eve, car Bob peut décoder les symboles transmis à un RSB supérieur à celui d'Eve. Le schéma de répétition est adopté pour fournir un gain de diversité à Bob, mais le précodeur MF garantit qu'Eve perd le gain de diversité. L'écart de sécurité entre Bob et Eve est mesuré en termes de TEB et de capacité de secret. Cette étude est réalisée en modes FDD et TDD. En mode FDD, il y a un retour d'information entre Alice et Bob et cette information est transmise à Eve. Dans ce mode, nous supposons qu'Eve est passive mais parfaitement consciente de la CSI des canaux d'écoute et des canaux principaux. C'est le pire cas pour la sécurité. La réciprocité des canaux est adoptée en mode TDD et Eve n'effectue qu'une égalisation aveugle.

System Model

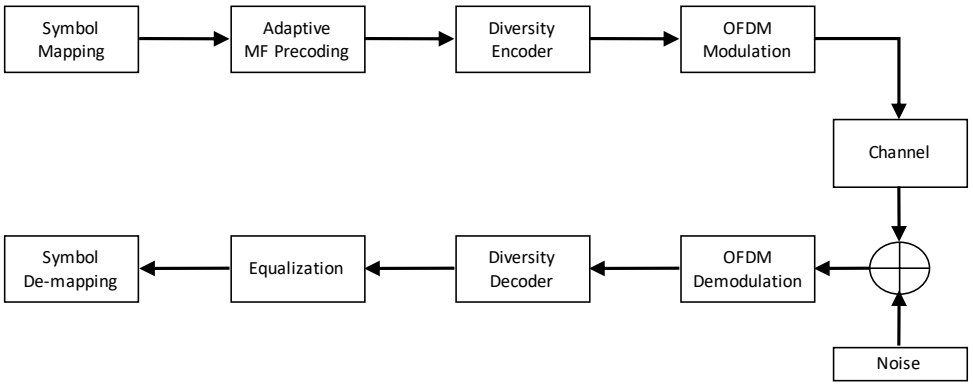


Figure 7: Modèle de système OFDM utilisant la diversité et la technique PLS adaptative.

Nous considérons une transmission OFDM avec N sous-porteuses fonctionnant en mode FDD. Les entrées du canal principal entre Alice et Bob, $\boldsymbol{h}^{(b)}$, sont des variables gaussiennes complexes à moyenne nulle, à évanouissement de Rayleigh et à variance unitaire. Il en va de même pour le canal d'écoute électronique entre Alice et Eve, $\boldsymbol{h}^{(e)}$. Pour chaque paire de sous-porteuses non corrélées dans le même bloc OFDM ($h_{n_1}^{(b)}$ et $h_{n_2}^{(b)}$), Alice transmet à Bob des symboles précodés MF x_{n_1} et x_{n_2}. Pour garantir la non-corrélation entre les paires de sous-porteuses, toutes les paires sont choisies comme suit:

$$h|_{n_1,n_2} = \begin{cases} h_{n_1}, & \text{where } 1 \leq n_1 \leq N/2, \\ h_{n_2}, & \text{where } n_2 = n_1 + N/2. \end{cases} \tag{21}$$

Le CSI instantané du canal principal est utilisé pour concevoir le précodeur qui maximise le SNR dans la direction de Bob uniquement. La diversité des fréquences est également ajoutée pour améliorer la fiabilité. Les étapes de la transmission de bout en bout sont illustrées à la figure 7. Eve connaît le CSI du canal principal grâce à la rétroaction du CSI en mode FDD. Bob et Eve sont situés à des endroits différents. Par conséquent, leurs canaux présentent une propagation non corrélée dans un environnement riche en diffusion [20]. Cela garantit que le signal précodé de la MF d'émission interceptée n'est pas optimal pour Eve. Il perd le gain de diversité car le précodage a été effectué avec un CSI non corrélé au sien. Bob bénéficie ainsi d'un gain de secret et d'erreur par rapport à Eve.

Pour chaque paire de sous-porteuses, les signaux reçus par Bob sont tels que

$$y_{n_1}^{(b)} = h_{n_1}^{(b)} x_{n_1} + z_{n_1}^{(b)}, \tag{22}$$

$$y_{n_2}^{(b)} = h_{n_2}^{(b)} x_{n_2} + z_{n_2}^{(b)}, \tag{23}$$

où $z_{n_1}^{(b)} \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_{n_1}^2)$ et $z_{n_2}^{(b)} \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_{n_2}^2)$ sont la composante AWGN complexe au niveau du récepteur prévu.

The received signals at Eve are expressed as

$$y_{n_1}^{(e)} = h_{n_1}^{(e)} x_{n_1} + z_{n_1}^{(e)}, \tag{24}$$

$$y_{n_2}^{(e)} = h_{n_2}^{(e)} x_{n_2} + z_{n_2}^{(e)}. \tag{25}$$

De même, $z_{n_1}^{(e)} \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_{n_1}^2)$ et $z_{n_2}^{(e)} \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_{n_2}^2)$ sont la composante AWGN complexe au niveau de l'espion.

Les signaux précodés en MF sont exprimés comme suit

$$x_{n_1} = P_{n_1} s, \quad x_{n_2} = P_{n_2} s \tag{26}$$

où

$$P_{n_1} = \frac{\sqrt{2} h_{n_1}^{(b)^*}}{\sqrt{|h_{n_1}^{(b)}|^2 + |h_{n_2}^{(b)}|^2}}, \quad P_{n_2} = \frac{\sqrt{2} h_{n_2}^{(b)^*}}{\sqrt{|h_{n_1}^{(b)}|^2 + |h_{n_2}^{(b)}|^2}}. \tag{27}$$

En substituant (26) et (27) dans (23) et en additionnant simplement les signaux reçus sur les deux sous-porteuses non corrélées, le signal reçu par Bob peut être écrit sous la forme suivante

$$\tilde{s}^{(b_1)} = \sqrt{2(|h_{n_1}^{(b)}|^2 + |h_{n_2}^{(b)}|^2)} s + z_{n_1}^{(b)} + z_{n_2}^{(b)}. \tag{28}$$

D'après (28), le rapport signal/bruit (SNR) instantané à Bob est donné comme suit

$$\gamma^{(b_1)} = (|h_{n_1}^{(b)}|^2 + |h_{n_2}^{(b)}|^2) \bar{\gamma}, \tag{29}$$

où $\bar{\gamma}$ est le SNR moyen au niveau du récepteur.

Le calcul du TEB pour la constellation QPSK est facilement disponible dans la littérature lorsque les variables de décision sont des variables aléatoires gaussiennes [21]

$$\mathrm{BER}(\mathrm{SNR}) = \frac{1}{2} \mathrm{erfc}\left(\sqrt{\frac{\mathrm{SNR}}{2}} \right) \tag{30}$$

Par conséquent, en conditionnant l'ensemble des variables h_{n_1} et h_{n_2}, nous pouvons obtenir la probabilité d'erreur MDPQ conditionnelle correspondant à la paire de sous-porteuses à Bob

$$\mathrm{BER}^{(\mathrm{b}_1)}\big|_{h_{n_1}^{(b)}, h_{n_2}^{(b)}} = \frac{1}{2} \mathrm{erfc}\left(\sqrt{\frac{\gamma^{(\mathrm{b}_1)}}{2}} \right), \tag{31}$$

Le TEB final est obtenu en faisant la moyenne du TEB conditionnel sur les variables h_{n_1} h_{n_2} pour toutes les paires de sous-porteuses dans N.

De même, lorsque le CSI est parfait, le signal reçu à Eve, le SNR instantané et le BER QPSK conditionnel peuvent s'écrire respectivement comme suit

$$\tilde{s}^{(e_1)} = \sqrt{2}\left(\frac{h_{n_1}^{(e)}h_{n_1}^{(b)^*} + h_{n_2}^{(e)}h_{n_2}^{(b)^*}}{\sqrt{(|h_{n_1}^{(b)}|^2 + |h_{n_2}^{(b)}|^2)}}\right)s + z_{n_1}^{(e)} + z_{n_2}^{(e)}. \tag{32}$$

$$\gamma^{(e_1)} = \left(\frac{\alpha\alpha^*}{|h_{n_1}^{(b)}|^2 + |h_{n_2}^{(b)}|^2}\right)\bar{\gamma} \tag{33}$$

$$\mathrm{BER}^{(\mathrm{e_1})}\Big|_{h_{n_1}^{(e)},h_{n_2}^{(e)}} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\gamma^{(\mathrm{e_1})}}{2}}\right), \tag{34}$$

where

$$\alpha = h_{n_1}^{(e)}h_{n_1}^{(b)^*} + h_{n_2}^{(e)}h_{n_2}^{(b)^*} \tag{35}$$

La capacité de secret est la différence positive entre la capacité du canal principal et la capacité du canal de l'espion [6]. Une valeur positive signifie que le secret est réalisable et un zéro implique qu'il n'y a pas de garantie de secret. Nous mesurons la capacité de secret en bps/Hz (ou bits/utilisation du canal). Comme pour le TEB, la capacité de secret finale est obtenue en calculant la moyenne des capacités conditionnelles des variables h_{n_1} h_{n_2} pour toutes les paires de sous-porteuses dans N. Les capacités conditionnelles des canaux de Bob et d'Eve et la capacité conditionnelle de secret s'expriment respectivement comme suit

$$\mathrm{C}^{(\mathrm{b_1})}\Big|_{h_{n_1}^{(b)},h_{n_2}^{(b)}} = \frac{1}{2}\log_2(1+\gamma^{(b_1)}), \tag{36}$$

$$\mathrm{C}^{(\mathrm{e_1})}\Big|_{h_{n_1}^{(e)},h_{n_2}^{(e)}} = \frac{1}{2}\log_2(1+\gamma(e_1)), \tag{37}$$

$$\mathrm{C}_{\mathrm{s}}^{(1)}\Big|_{h_{n_1}^{(b)},h_{n_2}^{(b)},h_{n_1}^{(e)},h_{n_2}^{(e)}} = [\mathrm{C}^{(\mathrm{b_1})} - \mathrm{C}^{(\mathrm{e_1})}]^+ \tag{38}$$

Le facteur de moitié dans (36) et (37) s'explique par le fait que seule la moitié de la largeur de bande disponible est utilisée pour la transmission. Pour N sous-porteuses disponibles, N/2 symboles uniques sont transmis.

Débruitage d'un CSI imparfait à l'aide d'un autoencodeur de débruitage - Structure et fonctionnement de DenoiseSecNet

Les performances du système proposé dépendent de la précision de la CSI instantanée. Lorsque la variance de l'erreur CSI augmente, la capacité de secret diminue et le TEB augmente de manière significative, ce qui entraîne une dégradation du système. C'est pourquoi un algorithme de débruitage par réseau neuronal, employé au niveau de l'émetteur pour débruiter la CSI imparfaite, est introduit. La CSI débruitée est ensuite utilisée pour le précodage MF et permet à Bob de conserver les gains de sécurité escomptés par rapport à Eve.

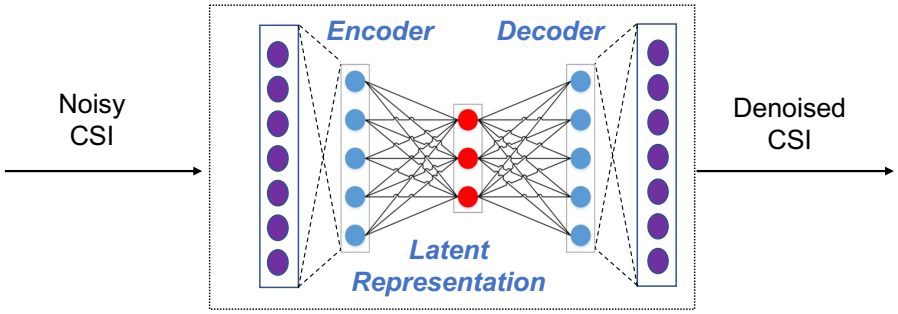


Figure 8: Algorithme DAE DenoiseSecNet proposé.

La première partie de cette section explique la structure et le fonctionnement du système DenoiseSecNet proposé. Dans la deuxième sous-section, nous proposons une version hybride de DenoiseSecNet qui est plus optimale en termes de performances et de complexité de calcul.

Dans ce travail, nous avons utilisé l'autoencodeur feed-forward de l'apprentissage profond, un modèle très connu de l'apprentissage profond, pour débruiter le CSI imparfait au niveau de l'émetteur [22]. DenoiseSecNet est un bloc autoencodeur à 5 couches composé d'une couche d'entrée, d'une couche de sortie et de 3 couches cachées, comme le montre la figure 8. Nous définissons $f(.)$ et $g(.)$ comme les opérations d'encodage et de décodage de l'autoencodeur respectivement. Dans DenoiseSecNet, nous définissons l'entrée comme le CSI bruité, $\tilde{\boldsymbol{h}}$. Les sorties du codeur et du décodeur seront donc respectivement $f(\tilde{\boldsymbol{h}})$ et $g(f(\tilde{\boldsymbol{h}}))$. Les opérations de codage et de décodage ont toutes deux lieu chez Alice. Ensuite, la sortie du bloc de décodage est utilisée pour précoder le signal d'émission. De la

première couche cachée à la couche de sortie, nous avons des couches entièrement connectées (FC) et une couche d'activation qui fournit une non-linéarité au modèle. Pour la ℓ-ième couche du modèle, l'activation linéaire peut être écrite comme suit:

$$\boldsymbol{m}_\ell = \boldsymbol{W}_\ell \boldsymbol{a}_{\ell-1} + \boldsymbol{b}_\ell, \tag{39}$$

où $\boldsymbol{a}_{\ell-1}$ est l'activation de la $(\ell-1)$-ième couche précédente, $\boldsymbol{W}_\ell$ représente le poids de la ℓ-ième couche actuelle et $\boldsymbol{b}_\ell$ sont les biais de la couche. Il convient de noter que le CSI bruité est l'entrée de la première couche, c'est-à-dire $\boldsymbol{a}_0 = \tilde{\boldsymbol{h}}$.

Ensuite, nous introduisons la non-linéarité dans le modèle. Celle-ci est nécessaire pour développer des représentations complexes capables de modéliser correctement la fonction. La non-linéarité est obtenue par l'utilisation de l'AF et l'AF de choix est l'unité linéaire rectifiée paramétrique (PReLU). Cette AF améliore l'ajustement du modèle avec un coût de calcul supplémentaire quasi nul et un faible risque d'overfitting [23]. La raison du choix de PReLU est expliquée dans la section **??**. PReLU est évalué comme suit :

$$\phi(m) = \begin{cases} m, & \text{si } m \geq 0, \\ \xi m, & sinon. \end{cases}, \tag{40}$$

où ξ est un paramètre pouvant être appris. La sortie de la section codeur du modèle, étiquetée "Représentation latente" sur la figure 8, est donnée ci-dessous :

$$f(\tilde{\boldsymbol{h}}) = \phi_\ell(\boldsymbol{W}_\ell(\phi_{\ell-1}(...\phi_1(\boldsymbol{W}_1\tilde{\boldsymbol{h}} + \boldsymbol{b}_1))) + \boldsymbol{b}_\ell), \tag{41}$$

où $\phi(.)$ représente l'activation non linéaire. Après le codage, le décodeur prend les données codées et génère une sortie qui correspond de manière optimale à la version sans bruit de l'entrée bruyante. La section du décodeur est représentée ci-dessous :

$$g(f(\tilde{\boldsymbol{h}})) = \phi_L(\boldsymbol{W}_L(\phi_{\ell-1}(...\phi_1(\boldsymbol{W}_1 f(\tilde{\boldsymbol{h}}) + \boldsymbol{b}_1))) + \boldsymbol{b}_L). \tag{42}$$

Pour entraîner le modèle, les hyperparamètres ont été optimisés à l'aide de ray tune [24]. Il s'agit du nombre de couches, du nombre de nœuds par couche, de la taille du lot et du choix de l'AF. La perte, $\mathcal{L}(h, g(f(\tilde{h})))$, est évaluée à l'aide de la perte MSE comme suit:

$$\mathcal{L}(\boldsymbol{h}, g(f(\tilde{\boldsymbol{h}}))) = \frac{1}{N}\sum_{i=1}^{N} \|\hat{\boldsymbol{h}} - \boldsymbol{h}\|_2^2, \tag{43}$$

où $hat\boldsymbol{h}$ est la sortie de l'autoencodeur. Dans le présent document, la MSE est préférée à l'erreur absolue moyenne (MAE) et à l'erreur logarithmique quadratique moyenne (MSLE), car nous voulons nous assurer que les erreurs importantes sont nettement plus pénalisées que les petites erreurs. Pour optimiser le système et mettre à jour itérativement les paramètres en conséquence, nous avons utilisé l'optimiseur SGD. Il est plus performant que d'autres optimiseurs tels que Adam, RMSprop, Adagrad, AdaDelta, etc. dans notre travail.

Option hybride de DenoiseSecNet

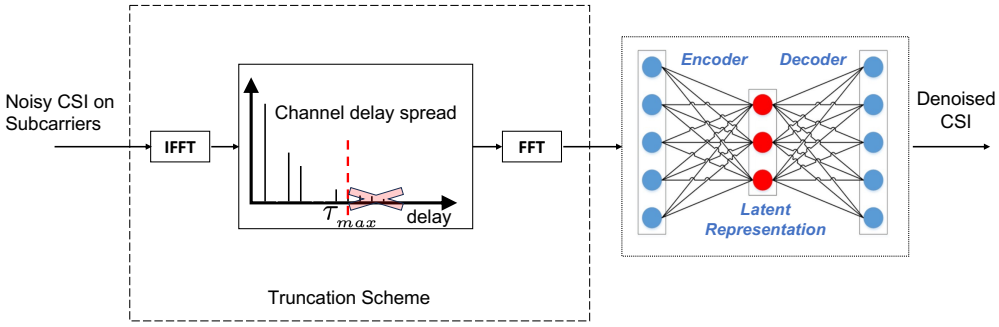


Figure 9: Algorithme DAE HybDenoisedSecNet proposé.

Pour des raisons de complexité, nous proposons une option hybride pour dénaturer le CSI bruyant, HybDenoiseSecNet. La principale motivation ici est d'obtenir des gains de performance en termes de TEB et de capacité de secret similaires à ceux de DenoiseSecNet, mais avec une complexité réduite. Pour ce faire, la CSI imparfaite est d'abord débruitée à l'aide de la méthode de troncature mentionnée. Nous supposons que la longueur du canal est connue d'Alice grâce à la rétroaction en mode FDD. Dans l'hypothèse de N sous-porteuses et d'une longueur de canal connue de T, la rétroaction CSI bruitée ($\tilde{\boldsymbol{h}}$) est d'abord transformée du domaine des fréquences au domaine temporel (TD), comme $\tilde{\boldsymbol{h}}^{TD}$, à l'aide d'une opération IFFT d'une taille de N. La troncature a ensuite lieu dans le domaine temporel, comme indiqué dans (4.39).

$$\ddot{h}_t^{TD} = \begin{cases} \tilde{h}_t^{TD}, & \text{if } 0 \leq t \leq T-1, \\ 0, & \text{if } T \leq t \leq N. \end{cases}, \tag{44}$$

Les prises du canal au-delà de la prise significative connue de T sont supposées être causées par le bruit et sont ignorées. La CSI tronquée est ensuite transformée dans le domaine fréquentiel sous la forme $\ddot{\boldsymbol{h}}$, à l'aide de la FFT. Cette CSI débruitée est ensuite passée par l'autoencodeur du réseau neuronal artificiel (ANN) pour une opération de débruitage supplémentaire. Étant donné qu'il est déjà partiellement

Table 1: Hyperparameters

DenoiseSecNet Structure	128-64-16-64-128
HybDenoiseSecNet Structure	128-16-128
DNNet-NEU Structure	128-1024-128
Training Sample Size	7×10^5
Validation Sample Size	2×10^5
Test Sample Size	1×10^5
Batch size	20
Learning rate	0.01
Optimizer	SGD
CSI Error Variance	0.1
Loss Function	MSE

débruité, l'autoencodeur ANN permet d'obtenir une réduction supplémentaire significative du bruit avec moins de calculs que l'option complète de DenoiseSecNet. En fait, nous n'avons pas besoin d'un réseau neuronal profond et un réseau neuronal peu profond peut produire des résultats optimaux.

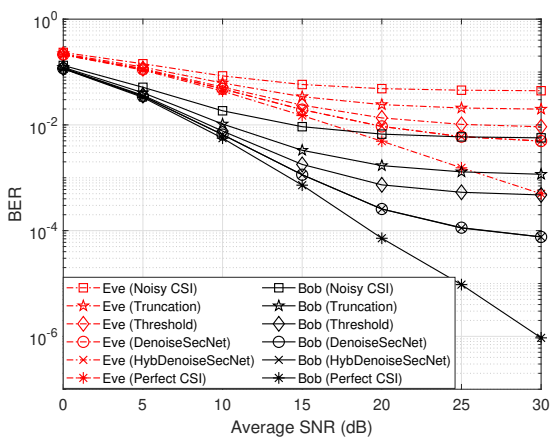
$$g(f(\ddot{\boldsymbol{h}})) = \phi_L(\boldsymbol{W}_L(\phi_{\ell-1}(...\phi_1(\boldsymbol{W}_1 f(\ddot{\boldsymbol{h}}) + \boldsymbol{b}_1))) + \boldsymbol{b}_L). \tag{45}$$

La version hybride proposée est présentée à la figure 9. Les autres hyperparamètres restant similaires, le changement dans le modèle hybride est le nombre de couches cachées et de neurones, et donc la complexité du modèle.

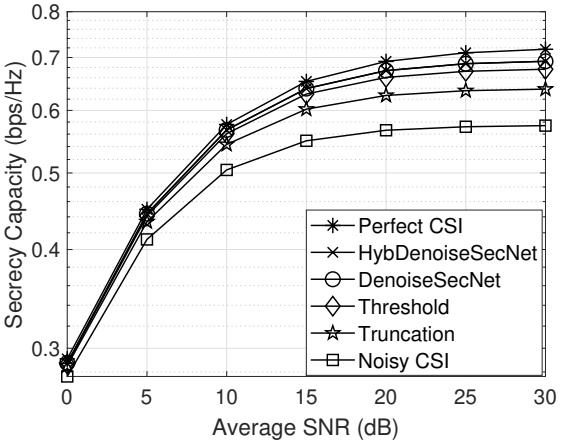
Analyse des performances avec CSI débruité

Dans cette section, nous présentons les performances des systèmes DenoiseSecNet et HybDenoiseSecNet que nous proposons et nous les comparons aux systèmes de débruitage existants. Nous considérons un système OFDM avec $N = 64$ sous-porteuses et une constellation QAM. Les couches cachées de la version complète de DenoiseSecNet sont de 64-16-64 tandis que la version hybride n'a qu'une couche cachée de 16 neurones. L'entrée CSI bruyante de 64 sous-porteuses avec 64 nombres complexes chacune est séparée en composantes réelles et imaginaires à l'entrée et à la sortie du modèle. Les couches d'entrée et de sortie ont donc chacune une longueur de 128. Les hyperparamètres utilisés dans la simulation sont résumés dans le tableau 1. Pour le schéma DNNet-NEU, nous considérons les hyperparamètres proposés par les auteurs dans [25].

Dans la figure 10a, le TEB de Bob et d'Eve est représenté en fonction du RSB moyen pour différents scénarios. Lorsque la CSI est parfaite ($\epsilon = 0$), Bob bénéficie d'un gain de diversité de 2, mais Eve



(a) Performance du TEB avec DenoiseSecNet.



(b) Performances en matière de sécurité avec DenoiseSecNet.

Figure 10: Performance avec l'ICS débruitée.

perd ce gain. Le TEB plus élevé d'Eve entraîne un écart de sécurité entre Bob et Eve. Avec un CSI bruité ($\epsilon = 0,1$), les performances de Bob et Eve sont complètement dégradées, et tous deux présentent des planchers d'erreur à partir d'un RSB moyen de 20 dB. De toute évidence, le système PLS est très sensible à la précision de l'ICS. Nous analysons ensuite les performances en termes de TEB des modèles d'autoencodeur proposés (complet et hybride), de DNNet-NEU et de deux schémas de débruitage conventionnels à base de réseaux non neuronaux : les schémas à seuil universel et les schémas de troncature. Nous observons que les schémas basés sur les réseaux neuronaux sont plus performants que les schémas conventionnels. Les schémas de troncature et de seuil universel présentent un plancher d'erreur de 10^{-3} et 5 fois 10^{-3} respectivement autour d'un RSB moyen de 30 dB. Lorsque DenoiseSecNet, HybDenoiseSecNet et DNNet-NEU sont utilisés pour débruiter le CSI bruyant, on constate une amélioration significative du TEB. Les deux modèles proposés atteignent le même niveau de TEB inférieur à 10^{-4} à $SNR = 30dB$. Le TEB de DNNet-NEU est à peu près le même que celui des modèles proposés.

La figure 10b montre les performances de la capacité de secret pour les schémas. Comme on pouvait s'y attendre, la capacité de secret est la plus élevée dans des conditions de CSI parfaite et la plus faible lorsque la variance de l'erreur CSI est la plus élevée ($\epsilon = 0,1$). Les schémas proposés et DNNet-NEU ont une capacité de secret légèrement inférieure au scénario le plus favorable. Là encore, les versions hybride et complète de DenoiseSecNet ont les mêmes performances. Vient ensuite le schéma de seuil universel, et le schéma de troncature était le schéma de débruitage CSI le moins efficace. Il convient de

noter que la capacité de secret est positive dans tous les cas. Cela montre que malgré la dégradation des performances due à la CSI bruyante, la capacité du canal de Bob reste supérieure à celle du canal d'Eve dans des conditions similaires.

Chapitre 5 - Index Modulation partitionnée

Introduction et motivations

Jusqu'à présent, les contributions de cette thèse, comme de nombreux schémas PLS dans la littérature, ont supposé que les entrées du canal étaient distribuées de manière gaussienne. La complexité de détection des signaux gaussiens est élevée car elle prend un continuum de valeurs. En outre, l'amplitude des signaux gaussiens n'étant pas limitée, la signalisation gaussienne n'est généralement pas utilisée dans la pratique. Dans la pratique, les entrées de canal sont généralement tirées d'une constellation de signaux discrets tels que QPSK, QAM, etc. Ces entrées de canal discrètes permettent de maintenir une puissance de transmission de crête et une complexité de réception modérées. Toutefois, les contraintes d'entrée à alphabet fini ont un impact significatif sur les performances PLS réalisables et cet impact doit être pris en compte dans la conception de schémas PLS pratiques.

Pour améliorer la PLS, nous proposons dans ce chapitre une nouvelle approche appelée modulation partitionnée par index (IPM). Cette modulation partitionne l'espace de constellation total utilisé par un canal principal en sous-espaces distincts et disjoints de manière à maximiser la distance euclidienne pour la transmission du canal principal. L'index est dérivé d'un index de clé sans fil dynamique qui est unique pour le canal légitime. Nous tirons parti du caractère aléatoire du canal qui existe dans les domaines temporel et spectral pour générer des clés qui sont uniques pour le canal principal. En supposant une décorrélation spatiale entre le canal principal et le canal d'écoute, ce qui implique des réponses indépendantes et non corrélées, l'index dynamique obtenu à partir de la clé sans fil n'est pas disponible pour Eve. Par conséquent, Eve utilisera tous les points de l'espace de constellation pour décoder le signal transmis, ce qui entraînera une dégradation significative du décodage. En l'absence de connaissance de l'index, le décodage au niveau de l'espion est dégradé en raison d'un choix adéquat de l'étiquetage des bits. Ce dernier garantit que la distance euclidienne entre les images de la même information est maximisée et que la distance de Hamming entre les étiquettes de bits des symboles voisins dans l'ensemble de la constellation est au moins égale à un.

Modulation partitionnée par index (IPM) : concept général et illustration

Wireless wiretap channel

Nous considérons un canal sans fil dans lequel un émetteur (Alice) transmet des symboles normalisés 2^q-QAM x_n à un récepteur légitime (Bob) sur N sous-porteuses dans un système TDD OFDM avec une taille FFT de $N_c \geq N$. Les signaux transmis sont interceptés par un espion (Eve) situé à proximité du récepteur légitime. Toutefois, le canal de Bob est indépendant de celui d'Eve, ce qui est le cas lorsqu'ils sont séparés par au moins une demi-longueur d'onde [20,26]. Sur chaque sous-porteuse de fréquence $0 \leq n \leq N-1$, les coefficients de canal $h_n^{(b)}$ et $h_n^{(e)}$ sont calculés comme la FFT du canal de prise aléatoire en fonction du profil de retard de puissance du canal (PDP). Les signaux reçus des deux côtés (Bob et Eve) sont tels que,

$$y_n^{(b)} = h_n^{(b)} x_n + z_n^{(b)}, \tag{46}$$

$$y_n^{(e)} = h_n^{(e)} x_n + z_n^{(e)}. \tag{47}$$

Le vecteur transmis à Alice est désigné par $\mathbf{x}$, celui reçu par Bob par $\mathbf{y}^{(b)}$ et par Eve par $\mathbf{y}^{(e)}$. Les bruits aléatoires $z_n^{(b)}$ et $z_n^{(e)}$ sont des variables complexes gaussiennes aléatoires i.i.d. $\mathcal{CN}(0, \sigma^2)$ avec pdf,

$$p(z_n) = p(y_n|h_n, x_n) = \frac{1}{\pi\sigma^2} e^{-\frac{1}{\sigma^2}|y_n - h_n x_n|^2}. \tag{48}$$

Pour garantir une comparaison équitable, les PDP représentant les atténuations du signal σ_t^2 aux écarts de retard τ_s, des canaux entre Alice $\rightarrow$ Bob et Alice $\rightarrow$ Eve sont supposés être identiques. Les coefficients de canal aléatoires sont générés à l'aide du modèle de canal de Jakes [26] et sont pondérés par l'atténuation correspondante d'un écart de délai donné. Nous supposons que ces coefficients sont parfaitement connus de chaque côté du récepteur.

Concept général de l'IPM

Le schéma IPM que nous proposons est illustré à la figure 11 et consiste à partitionner la modulation 2^q-QAM (désignée par Ω_c avec $|\Omega_c| = 2^q$) en 2^ℓ espaces multiples disjoints (désignés par $\Lambda_m \subset \Omega_c$, avec $1 \leq m \leq 2^\ell$), de manière à ce que : $\bigcap_m \Lambda_m = \emptyset$, $\bigcup_m \Lambda_m = \Omega_c$ et $|\Lambda_m| = 2^{q-\ell}$. Chaque sous-espace Λ_m est indexé par un index basé sur le canal d'une longueur de ℓ, partagé entre Alice et Bob. Une

séquence de bits d'information donnée de $(q-\ell)$ aura des images différentes dans Ω_c en fonction de la valeur de l'index et réduira le nombre de bits d'information par symbole à $(q-\ell)$ plutôt qu'à q. Dans tout l'espace, l'étiquetage des bits des symboles est effectué de telle sorte que la distance euclidienne entre les symboles voisins d'une partition donnée soit maximisée. En effet, cela devrait garantir que la distance euclidienne entre les images de la séquence de bits d'information est maximisée. Chez Alice, l'index partagé détermine le sous-espace réduit Λ_m dans lequel se trouve le symbole MAQ 2^q. Sur la base de cet index, Bob décode le symbole QAM bruité dans Λ_m avec des symboles voisins plus éloignés que Ω_c. Comme Eve n'a pas connaissance de l'indice partagé par Alice et Bob en fonction du canal, Eve décode le symbole QAM bruité dans l'espace entier Ω_c avec des symboles voisins moins éloignés que Λ_m, ce qui induit une faible information mutuelle. Ce schéma IPM est appelé ci-après IPM sans bruit.

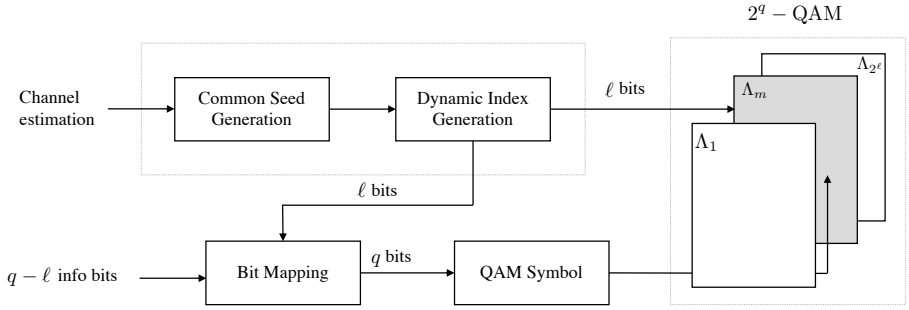


Figure 11: Modulation partitionnée de l'indice

IPM bruyant

Dans le régime de rapport signal/bruit élevé, les distances euclidiennes entre les points voisins sont relativement importantes dans les deux treillis Λ_m ou Ω_c. Dans ce cas, le gain de secret devient insignifiant car les symboles bruyants peuvent être distingués aussi bien par Bob que par Eve. Afin d'induire une plus grande confusion chez l'espion, nous proposons d'injecter un AN uniforme aléatoire dans le symbole QAM généré par l'IPM. Pour ce faire, nous ajoutons l'AN généré au symbole QAM tout en conservant la puissance totale chez Alice, ce qui est appelé IPM bruyant. La fonction de distribution de probabilité (pdf) de cet AN uniforme aléatoire sera examinée plus en détail dans la sous-section 5.2.5.2.

Résultats numériques

Nous considérons un système OFDM qui fonctionne dans une bande de $1,4$ MHz divisée en sous-porteuses de $\Delta f = 15$ kHz avec une FFT de taille $N_c = 128$ où seulement $N = 72$ sous-porteuses sont utilisées. La fréquence d'échantillonnage est de $F_s = N_c \Delta f = 1,92$ MHz. Le modèle urbain type étendu (ETU), correspondant à un environnement radioélectrique hautement sélectif avec les PDP décrits dans le tableau 2, est pris en compte.

Table 2: PDP pour ETU : τ = propagation du retard et σ_t^2 = puissance

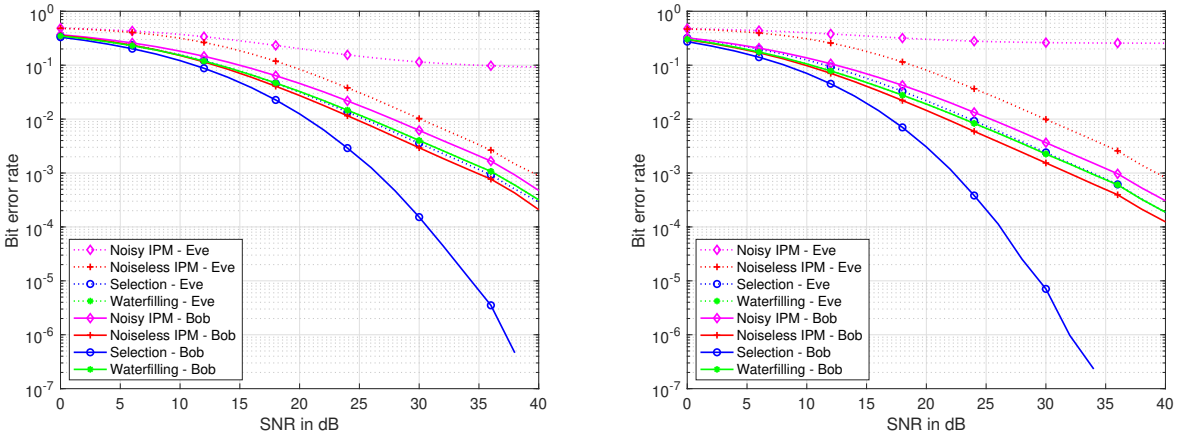
$\tau[ns]$	0	50	120	200	230	500	1600	2300	5000
$\sigma_t^2[dB]$	-1	-1	-1	0	0	0	-3	-5	-7

Nous comparons les performances des schémas IPM bruyants et silencieux proposés ($\beta = 0,7$) avec un schéma qui utilise l'évitement de l'évanouissement par la sélection de l'index de la sous-porteuse et un autre schéma où l'algorithme de remplissage d'eau hérité est utilisé pour favoriser le canal principal puisqu'il est indépendant du canal d'écoute électronique. Nous comparons les performances en termes d'information mutuelle, de capacité de secret et de TEB. Pour garantir une comparaison équitable, nous avons fixé les paramètres du système (taille de la constellation et nombre de sous-porteuses actives) de manière à obtenir la même efficacité spectrale maximale que le système IPM, comme le montre le tableau 3. Avec le schéma de sélection des sous-porteuses, la puissance totale est répartie uniformément entre toutes les sous-porteuses actives.

Table 3: Efficacité spectrale des différents systèmes pour une comparaison équitable

IPM		64QAM ($\ell = 1$)	64QAM ($\ell = 2$)	16QAM ($\ell = 1$)	16QAM ($\ell = 2$)
	No of bpcu	5	4	3	2
Selection	**No of Active SCs**	60	48	54	36
Selection	**Constellation**	64QAM	64QAM	16QAM	16QAM
Water-filling	**No of Active SCs**	72	72	72	72
Water-filling	**Constellation**	32QAM	16QAM	8PSK	QPSK

En utilisant la distribution de bruit équivalente, nous avons montré que le critère MAP est équivalent à la minimisation de la distance euclidienne entre le signal reçu et le signal transmis atténué. Nous avons ainsi caractérisé les courbes de TEB de notre système par rapport à celles de la littérature dans la figure 12. La sécurité fournie est mesurée en termes d'écart de RSB entre Bob et Eve pour différentes valeurs de TEB. En raison de la sélection de sous-porteuses à gain élevé dans le schéma



(a) 16-QAM(3bpcu

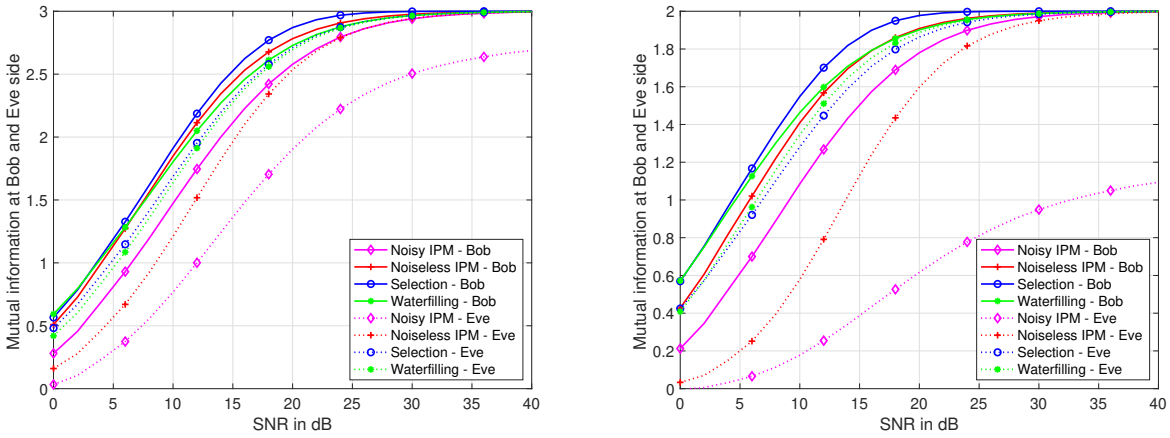
(b) 16-QAM(2bpcu)

Figure 12: Taux d'erreur binaire pour Eve et Bob à $\beta = 0.7$.

de sélection, nous constatons que le TEB de Bob a un gain de diversité supérieur à 1, mais qu'Eve a un TEB relativement bon avec un gain de diversité de 1 et donc un écart de sécurité minime. L'utilisation de l'algorithme de remplissage d'eau n'apporte aucun gain de sécurité car, à des valeurs de RSB élevées, l'attribution de puissance devient la même que l'attribution de puissance uniforme et il n'y a pas de gain pour Bob par rapport à Eve. Pour le schéma IPM sans bruit, Bob est plus performant qu'Eve, mais avec des écarts de RSB entre les deux pour certaines valeurs de TEB. Cependant, le MIP bruyant a donné les meilleures performances car nous constatons que le bruit uniforme n'affecte que légèrement le TEB de Bob mais dégrade complètement le TEB d'Eve avec une apparition précoce du plancher d'erreur dans toutes les constellations et tous les bits par canal utilisés (bpcu) considérés. La dégradation minimale de la qualité du décodage sur le canal principal peut être compensée par une augmentation de l'énergie, qui ne profitera qu'à Bob et non à Eve.

La figure 13 illustre la variation de l'information mutuelle en fonction du RSB obtenu avec la MAQ-16 (3bpcu et 2bpcu). On constate que pour les schémas considérés, l'information mutuelle de Bob converge vers l'efficacité spectrale maximale. Comme pour le TEB, cette convergence est plus rapide pour le schéma de sélection que pour les autres schémas. Sur l'écoute électronique, seul le schéma IPM bruyant n'atteint pas l'efficacité spectrale maximale. Cette réduction est d'autant plus efficace avec un partitionnement sur 2 bits que sur 1 bit.

Nous voyons dans la figure 14 la capacité de secret entre pour tous les schémas. Il s'agit simplement de la différence d'information mutuelle entre Bob et Eve. On constate que les schémas IPM sont



(a) 16-QAM(3bpcu

(b) 16-QAM(2bpcu)

Figure 13: Performance en matière d'information mutuelle pour Eve et Bob à $\beta = 0,7$.

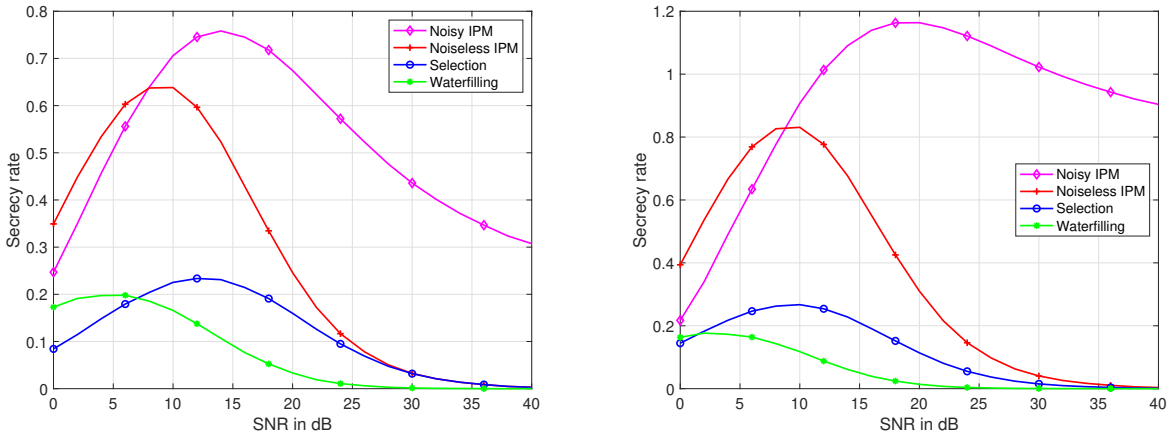
nettement plus performants que les schémas de sélection et de remplissage d'eau dans les régimes de faible RSB, mais que tous les schémas, à l'exception du schéma IPM bruyant, tombent à zéro dans le régime de RSB élevé. Cela confirme une fois de plus les performances optimales en matière de secret du schéma IPM bruyant. Dans le régime de RSB très élevé, l'AN uniforme continue à dégrader Eve mais pas Bob. Pour la constellation 16-QAM, le gain de sécurité est de 0,3 et 0,9 bpcu dans le cas d'un partitionnement avec 1 et 2 bit(s) d'index respectivement.

Conclusion

Le titre de cette thèse est "Amélioration de la sécurité de la couche physique grâce à la diversité de fréquence et spatiale". Le premier chapitre présente les motivations de la recherche et le contexte des contributions. Le deuxième chapitre explique les concepts fondamentaux tels que PLS, Massive MIMO, OFDM et AI. Les chapitres 3 à 5 contiennent les contributions principales.

Dans le chapitre 3, il est démontré que l'injection d'AN aléatoire augmente le PAPR du signal d'émission en raison de la superposition en phase du signal d'information et de l'AN. Un nouvel algorithme, "PAPR-Aware-Secure-mMIMO", est proposé pour minimiser conjointement le PAPR et maximiser la sécurité en utilisant le CSI instantané. Les simulations montrent des améliorations en termes de PAPR, SER, capacité de secret et SEE par rapport aux systèmes existants.

Le chapitre 4 se concentre sur l'adaptation du canal dans la PLS en utilisant le CSI instantané



(a) 16-QAM(3bpcu

(b) 16-QAM(2bpcu)

Figure 14: Performance de la capacité de secret pour Eve et Bob à $\beta = 0.7$.

pour concevoir un précodeur adaptatif. L'indépendance des canaux entre Bob et Eve conduit à un écart de sécurité. L'impact de la CSI imparfaite est étudié, et un autoencodeur de débruitage est proposé pour améliorer les performances en matière de secret.

Enfin, la thèse présente un système PLS à alphabet fini appelé "IPM", qui utilise une constellation de signaux discrets pour l'entrée du canal. L'IPM est évalué en termes d'information mutuelle, de taux de secret et de TEB, montrant des performances supérieures par rapport aux autres schémas existants grâce à l'injection d'AN.

En résumé, cette thèse explore diverses techniques pour améliorer la sécurité de la couche physique, en se concentrant sur la réduction du PAPR, l'adaptation du canal, et l'utilisation d'entrées à alphabet fini pour renforcer la sécurité des communications.

Contents

List of Tables

List of Figures

List of acronyms

5G	Fifth Generation
AF	Activation Function
AI	Adaptive Interleaving
AN	Artificial Noise
ANN	Artificial Neural Network
ASD	Angular Standard Deviation
AWGN	Additive White Gaussian Noise
BS	Base Station
BER	Bit Error Rate
bpcu	bits per channel use
CCDF	Complementary Cumulative Distribution Function
CDF	Cumulative Distribution Function
CFO	Carrier Frequency Offset
CIR	Channel Impulse Response
CoMP	Coordinated Multi-Point
CNN	Convolutional Neural Networks
CP	Cyclic Prefix
CSI	Channel State Information
D2D	Device-to-Device
DAE	Denoising Autoencoder
DFT	Discrete Fourier Transform
DoF	Degree of Freedom
EM	Electromagnetic
ETU	Extended Typical Urban
FDD	Frequency Division Duplex
FFT	Fast Fourier Transform
HPA	High Power Amplifier
IBO	Input Back-Off

IDFT Inverse Discrete Fourier Transform
FC Fully Connected
GD Gradient Descent
IFFT Inverse Fourier Fourier Transform
ICI Inter-Carrier Interference
IoT Internet of Things
i.i.d. independent and identically distributed
IPM Indexed Partitioned Modulation
IRS Intelligent Reflecting Surface
ISI Inter-Symbol Interference
LTE Long-Term Evolution
MAC Media Access Control
MAE Mean Absolute Error
MF Matched Filter
ML Machine Learning
MLP Multilayer Perceptron
MIMO Multiple-Input Multiple-Output
MISO Multiple-Input Single-Output
MMSE Minimum Mean-Squared Error
mMTC Massive Machine Type Communication
mmWave Millimeter Wave
MRC Maximum Ratio Combining
MSE Mean Squared Error
MSLE Mean Squared Logarithmic Error
MU Multi-User
MUI Multi-User Interference
NEU Noise Extraction Unit
NMSE Normalized Mean Squared Error
NOMA Non-Orthogonal Multiple Access
OBO Output Back-Off
OFDM Orthogonal Frequency Division Multiplexing
PAPR Peak-to-Average Power Ratio
PLS Physical Layer Security
PReLU Parametric Rectified Linear Unit
P/S Parallel-to-Serial
QAM Quadrature Amplitude Modulation
QoS Quality of Service

QPSK Quadrature Phase Shift Keying
ReLU Rectified Linear Unit
RNN Recurrent Neural Networks
RSSI Received Signal Strength Indicator
SDMA Space Division Multiple Access
SE Spectral Efficiency
SEE Secrecy Energy Efficiency
SELU Scaled Exponential Linear Unit
SER Symbol Error Rate
SGD Stochastic Gradient Descent
SINR Signal-to-Interference plus Noise Ratio
SIS Subcarrier Index Selection
SISO Single-Input Single-Output
SOP Secrecy Outage Probability
SNR Signal-to-Noise Ratio
S/P Serial-to-Parallel
TD Time Domain
TDD Time Division Duplex
UAV Unmanned Aerial Vehicles
UE User Equipment
URLLC Ultra Reliable and Low Latency Communication
w.r.t. with respect to
ZF Zero-Forcing

Chapter 1

Introduction

Contenu

1.1 Research Context

The last decade has been marked by an unprecedented shift in society and economy towards a heavy reliance on wireless communication networks and unlimited access to the Internet. The traditional web of the 1990s with static content has undergone several evolutions from the social web (web 2.0), to the semantic web (web 3.0) and lately to the web of objects (web 4.0) [1]. This evolution of the web could only be done thanks to the great technological advances that have been made in parallel in all areas of digital technology: electronics, telecommunications, computing and massive data processing. This ability of the internet to connect devices, people and objects at the same time has a double facet.

Though the web offers an unprecedented environment for collaboration, coordination, and co-production, all web users are vulnerable to cyber attacks, espionage, hacking of information, and consequently the invasion of privacy and personal data. Traditionally, communication security has been provided using cryptography [5]. Although cryptography has been a huge success, it has its limi-

tations in terms of high resource requirements and computational complexity. Cryptographic security measures thrive under the assumption that the legitimate receiver has more computational resources than the eavesdropper, a condition that is not necessarily true anymore due to recent advances in quantum computing [2]. Furthermore, many of the devices that use wireless connections are limited by power and computational resources, highly sensitive to delays and overheads, and may be deployed in a decentralized network.

To this end, Physical Layer Security (PLS) is a new paradigm used to enhance the security of wireless communication systems. PLS is quantum secure, fast, and light to implement. Its advantages over cryptography are lower computational complexity and resource requirement. PLS techniques take advantage of the characteristics of wireless channels such as noise, fading, interference, diversity, dispersion, etc. to ensure an intended receiver (Bob) successfully decodes transmitted data from a transmitter (Alice) while preventing an eavesdropper (Eve) from doing so [3, 4]. The main design goal of PLS is to increase the performance difference between the link of the legitimate receiver and that of the eavesdropper by using well-designed transmission schemes. Dissimilar to encryption based methods, no constraint is placed on the computational ability of the eavesdropper and no key distribution/management is required in PLS.

1.2 Thesis Objectives

This thesis makes contributions in the major categories of PLS. In all of these categories, the objective is to propose a novel solution to address a limitation in the practical application of PLS. In broad terms, we would like to do the following:

- Simultaneously address the challenge of energy efficiency in massive Multiple-Input Multiple-Output (MIMO) systems and PLS by Artificial Noise (AN) injection.
- Study the impact of imperfect instantaneous Channel State Information (CSI) in a channel adaptation PLS approach that used precoding and diversity for security.
- Propose a solution to the challenge of imperfect instantaneous CSI in the application of PLS through channel adaptation by using Artificial Intelligence (AI) techniques.
- Extend the work on PLS to not only Gaussian input signaling but also finite-alphabet signaling

which is a practical reality in deployment scenarios.

- Propose a novel PLS scheme under key-based PLS techniques with finite-alphabet input constraints.

1.3 Thesis Outline

- **Chapter 2 - Fundamentals of PLS and Other Key Concepts of the Thesis**
  Chapter 2 is devoted to introducing the background and the state-of-the-art related to the different concepts used throughout this thesis. We commence by explaining the concept of PLS which is the central theme of the thesis. Next, we look at three popular PLS approaches in the literature: AN Injection, Channel Adaptation, and Key-based approaches, along with relevant works in the literature. Afterward, the overview, fundamental principles, system model, and challenges of Massive MIMO were given. A major contribution of the thesis was centered on a massive MIMO context and hence the need for a solid introduction to its operations. The other contributions in this thesis adopt frequency-selective fading and this motivated the introduction to the concept of Orthogonal Frequency Division Multiplexing (OFDM). We introduced the fundamental principle, the system model, implementation, and other relevant properties. Finally, in this chapter, we gave a brief overview of the use of deep learning in wireless communication and more importantly, the use of autoencoder. A vital contribution in this thesis used an autoencoder model to improve PLS and thus a need for a clear understanding of the concept.

- **Chapter 3 - Energy Efficiency in Secure Massive MIMO**
  Energy efficiency is an important factor in the deployment of massive MIMO systems in practice. One major factor contributing to poor energy efficiency is the high Peak-to-Average Power Ratio (PAPR) of transmit signals. This high PAPR is due to the high-dimensional precoding matrix in massive MIMO caused by the large number of transmit antennas. In addition, the injection of random AN to provide PLS also suffers from high PAPR due to the in-phase superposition of the information signal and the AN sub-space. Based on this, we propose an interesting approach to security in massive MIMO using AN injection in the third chapter. The proposed AN simultaneously reduces the PAPR of the transmit signal while ensuring secure communication between legitimate users in the presence of an eavesdropper.

- **Chapter 4 - Frequency Diversity in Physical Layer Security**

  Chapter 4 is devoted to another PLS approach known as channel adaptation. We commence by proposing a PLS scheme that makes use of the instantaneous CSI. However, since instantaneous CSI is imperfect in practice due to factors such as noisy CSI feedback, delayed feedback, etc., we then study the impact of imperfect CSI on the performance of the PLS scheme. We conclude the chapter by proposing the use of AI to denoise the noisy CSI that is used for the PLS.

- **Chapter 5 - Index Partitioned Modulation**

  In this chapter, we consider the practical case of having PLS with finite-alphabet input signaling. This last contribution chapter considers yet another approach in PLS that makes use of channel keys in reciprocity-based communication. A novel PLS scheme uses these dynamic keys, which are unique to the main channel users, to partition the modulation space intelligently in such a way that it favors the legitimate user only. Since the eavesdropper's channel is independent of the main channel, the eavesdropper is unable to know the unique keys of the main channel users. The partitioned modulation will ensure that the total constellation space is separated into distinct and disjoint subspaces in such a way that it maximizes Euclidean distance for the main channel transmission. The eavesdropper on the other hand will have smaller decision regions with less distant neighboring symbols and thus lower mutual information compared to the legitimate user.

- **Chapter 6 - Conclusion and Perspectives**

  This chapter draws the final conclusions by highlighting the main contributions of this dissertation. Possible future research are provided at the end.

1.4 List of Publications

The publications listed below are published, accepted for publication and submitted. We have also added ongoing articles.

1.4.1 Journals

- **I. Ajayi**, Y. Medjahdi, R. Zayani, L. Mroueh and F. Z. Kaddour, "PAPR-Aware Artificial Noise for Secure Massive MIMO Downlink," in IEEE Access, vol. 10, pp. 68482-68490, 2022, doi:

10.1109/ACCESS.2022.3186695.

- L. Mroueh and **I. Ajayi**, "Noisy and Dynamic-Index Partitioned Modulation for Physical Layer Security," in IEEE Transactions on Information Forensics and Security, Submitted.

1.4.2 Conference Papers

- **I. Ajayi**, Y. Medjahdi, F. Kaddour and L. Mroueh, "Impact of Imperfect Channel State Information on Physical Layer Security by Precoding and Diversity," 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Semarang, Indonesia, 2021, pp. 322-327, doi: 10.23919/EECSI53397.2021.9624230.

- **I. Ajayi**, Y. Medjahdi, L. Mroueh and F. Kaddour, "Physical Layer Security by Interleaving and Diversity: Impact of Imperfect Channel State Information," 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Semarang, Indonesia, 2021, pp. 299-304, doi: 10.23919/EECSI53397.2021.9624293.

- **I. Ajayi**, Y. Medjahdi, L. Mroueh, R. Zayani and F. Kaddour, "Secrecy Energy Efficiency in PAPR-Aware Artificial Noise Scheme for Secure Massive MIMO," 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Gothenburg, Sweden, 2023, pp. 42-47, doi: 10.1109/EuCNC/6GSummit58263.2023.10188263.

- **I. Ajayi**, Y. Medjahdi, L. Mroueh, O. Okubadejo and F. Kaddour, "Low-Complexity Neural Networks for Denoising Imperfect CSI in Physical Layer Security," 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Gothenburg, Sweden, 2023, pp. 48-53, doi: 10.1109/EuCNC/6GSummit58263.2023.10188372.

1.4.3 Ongoing Papers

- **I. Ajayi** and Y. Medjahdi, "Performance Optimization of PAPR-Aware Artificial Noise Scheme for Secure Massive MIMO under Correlated Rayleigh Fading,", Ongoing.

- **I. Ajayi** and Y. Medjahdi, "Deep Learning Approach to PAPR-Aware Secure Massive MIMO Algorithm", Ongoing.

Chapter 2

Fundamentals of PLS and Other Key Concepts of the Thesis

Contenu

2.1 Introduction

This chapter provides an overview of the key aspects of this thesis. The discussions in this chapter are pivotal to having a full understanding of the contributions of the thesis which will be seen in the chapters that follow. Section 2.2 explains different aspects of the PLS paradigm: secrecy notions, secrecy metrics, major categories of PLS schemes in the literature, and their limitations. Massive MIMO, a key technology for Fifth Generation (5G) and Beyond, is introduced in section 2.3. In section 2.4, the principles behind OFDM are introduced. Finally, section 2.5 gives a brief introduction to deep learning in wireless communication.

2.2 Physical Layer Security

PLS is an emerging paradigm that has gained a lot of attention in recent times [3, 4]. It is based on the pivotal idea of turning wireless channel characteristics such as noise, fading, dispersion, diversity, and interference into a source of security. It is considered a promising technique that exploits the channel properties to send confidential messages from a transmitter (Alice) to the legitimate receiver (Bob) in the presence of a powerful eavesdropper (Eve). It is a field that is gaining more attention in recent times because it offers the advantages of lower computational complexity and lower resource requirement compared to legacy cryptography and it is potentially quantum secure. The ease of implementing a security solution is more important now than ever before. Technologies such as Internet of Things (IoT), Device-to-Device Communication(D2D), Unmanned Aerial Vehicles (UAV), Ultra-Reliable and Low Latency Communication (URLLC), Massive Machine-Type Communications (mMTC), millimeter wave (mmWave), terahertz communication, etc are in a phase of exponential growth. Despite the prospects of using these technologies, the security of the communication remains a very crucial talking point. Traditional cryptographic key management security approaches are not necessarily suitable for some of these newer communication technologies. Cryptography relies on computational complexity and it is resource intensive [5]. However, the earlier-mentioned technologies are mostly decentralized, limited in computational and power resources, and highly sensitive to latency. Hence, there is a need for a security solution that can complement cryptography solutions: PLS.

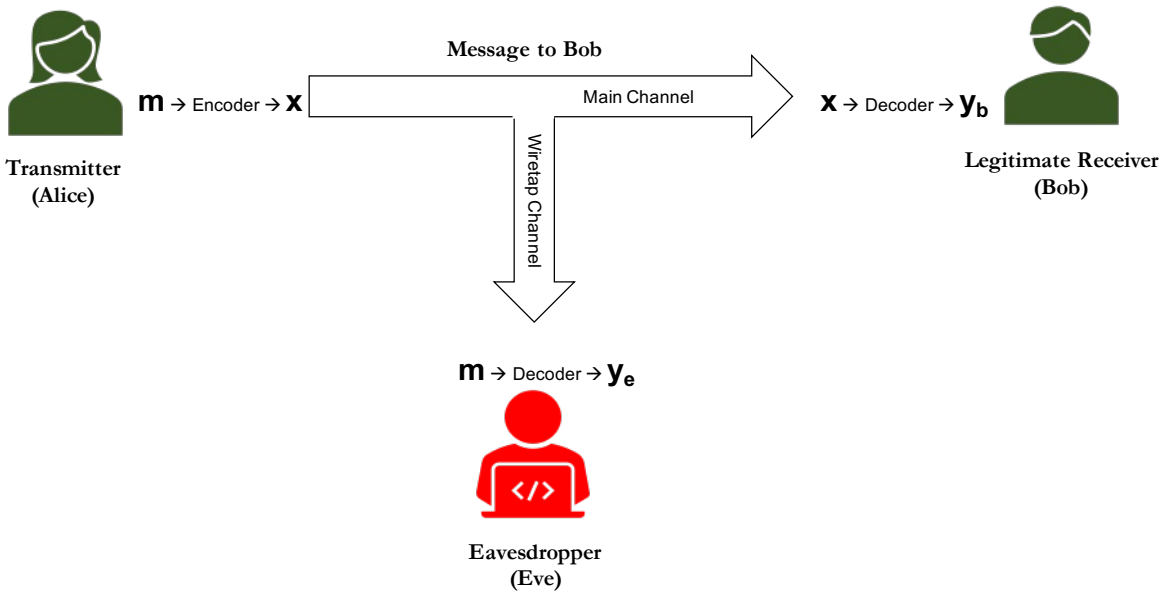


Figure 2.1: Wiretap channel model.

2.2.1 PLS Secrecy Notions

The foundation of the research on PLS was done by Wyner in his seminal work in [30]. Fig. 2.1 shows the wiretap channel model proposed by Wyner. He established that secure communication is possible between legitimate users as long as the eavesdropper's channel (wiretap channel) is more degraded than the legitimate users' channel (main channel). Thus, random secrecy codes based on channel realizations were used to achieve confidentiality without using shared secret keys. In this setup, Alice sends a message m that is encoded to x of length n before transmission. The received signals at Bob and Eve are indicated by y_b and y_e, respectively. The entropy of the source information is given by $H(m)$, whereas the residual uncertainty (conditional entropy) for the eavesdropper's obseration is denoted by $H(m|y_e)$. Popular secrecy notions in PLS are perfect, strong, and weak secrecies [31]. For there to be perfect secrecy as seen in (2.1), the mutual information leakage to Eve is zero regardless of the computational power. This is the most stringent secrecy measure as it ensures an almost unity decoding error probability at Eve.

$$\mathrm{I}(m; y_e) = 0. \tag{2.1}$$

For two variables A and B, the mutual information quantifies the amount of information shared

between the two variables. It is defined as follows:

$$\begin{aligned} \mathrm{I}(A;B) &= H(B) - H(B|A) \\ &= H(A) - H(A|B), \end{aligned} \tag{2.2}$$

where $H(B|A)$(resp.$(HA|B)$ denotes the conditional entropy, which expresses the average amount of uncertainty in B(resp.A) given that the value of A(resp.B) is known.

The next secrecy notion is the strong secrecy and the requirement for this is that asymptotic mutual information goes to zero as the codeword length n goes to infinity, (2.3).In essence the mutual information leakage is zero on each channel use.

$$\lim_{n\to\infty} \mathrm{I}(m; y_e) = 0. \tag{2.3}$$

Finally, Wyner's work adopts the notion of weak secrecy, (2.4). The fundamental requirement here is that the asymptotic mutual information rate goes to zero as the codeword length goes to infinity. This means that the mutual information per channel use is not zero but the average mutual information.

$$\lim_{n\to\infty} \frac{1}{n}\mathrm{I}(m; y_e) = 0. \tag{2.4}$$

2.2.2 PLS Metrics

Now that we have established the secrecy notions of PLS, the next big task is to quantify how much information Alice can securely and reliably transmit to Bob in the presence of Eve. This brings us to the important topic of "**PLS Metrics**". There are several metrics in the literature such as secrecy capacity, secrecy outage probability, secrecy throughput, security gap measured in terms of bit error rate (BER), etc. [4]. The choice of metrics is based on the PLS approach being considered and in this thesis, we will be using the secrecy capacity and the BER to quantify the security gains of the various schemes.

2.2.2.1 Secrecy Capacity

The fading wiretap channel is adopted in this thesis, and a fundamental type is one that considers single antennas at Alice, Bob, and Eve as shown in Fig. 2.2. In this case, at a particular time slot,

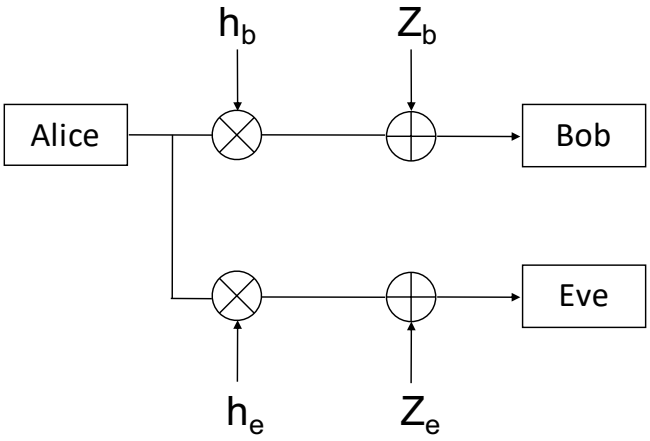


Figure 2.2: Fading wiretap channel model.

for a message, m, transmitted as x, Bob receives

$$y_b = h_b x + z_b, \tag{2.5}$$

and Eve receives

$$y_e = h_e x + z_e, \tag{2.6}$$

where h_b and h_e, are i.i.d. Rayleigh fading zero-mean complex Gaussian variables with unit variance for the main and wiretap channels. z_b and $z_e \sim \mathcal{N}_{\mathbb{C}}(0, \sigma^2)$ are the independent Additive White Gaussian Noise (AWGN) with variances σ_b^2 and σ_e^2 at the Bob and Eve respectively. Secrecy capacity is the most popular PLS metric and it is defined as the maximum transmission rate at which the eavesdropper is unable to decode any information [6]. GIven a power constraint of P, it is equal to the positive difference between the main channel capacity and the capacity of the wiretap channel as seen in (2.7). A positive value means secrecy is achievable and a zero implies there is no secrecy guarantee. We measure secrecy capacity in b/s/Hz (or bits/channel use).

$$C_s = \left[\log_2\left(1 + \frac{P|h_b|^2}{\sigma_b^2}\right) - \log_2\left(1 + \frac{P|h_e|^2}{\sigma_e^2}\right)\right]^+ \tag{2.7}$$

Note that the Signal-to-Noise Ratio (SNR), γ, in a fading channel is given as $\gamma = P|h|^2/\sigma^2$. This is the ratio of the power of the useful signal to the power of the thermal noise, taking into account the

effect of channel fading. In essence, the secrecy capacity is rewritten as:

$$C_s = \left[\log_2\left(1+\gamma_b\right) - \log_2\left(1+\gamma_e\right)\right]^+ \tag{2.8}$$

Originally in [6], secrecy capacity is calculated using the Shannon channel capacity which gives the maximum capacity of the channel assuming Gaussian signaling. If we consider the formulation for finite-alphabet signaling, the capacity of the channel is measured in terms of the mutual information. As such, for the contributions in Chapters 3 and 4 of this thesis, we adopt the former computation of secrecy capacity while in the final contribution Chapter 5, we adopt the latter. Hence, the general expression for secrecy capacity in this thesis is:

$$C_s = \begin{cases} \left[\log_2\left(1+\gamma_b\right) - \log_2\left(1+\gamma_e\right)\right]^+ & \text{if Gaussian signaling,} \\ \left[\mathrm{I}_b(m,y_b) - \mathrm{I}_e(m,y_e)\right]^+, & \text{if Finite-alphabet signaling.} \end{cases} \tag{2.9}$$

2.2.2.2 Bit Error Rate

In this thesis, we also measure security by comparing the SNR needed by Bob and Eve to attain targeted BER values. This gives the security gap between the legitimate receiver and the eavesdropper. The system that attains a target BER at a low SNR value is classified as more reliable and secure than a system which needs a much higher SNR to attain the same BER or never attains certain BER values due to error floors. Numerically, the BER is calculated as the average number of received bit errors per unit for all channel realizations. We also verify the BER values theoretically in some of the contributions of the thesis.

Several approaches have been adopted in PLS and are broadly categorized as follows: AN injection, channel adaptation, and channel key techniques. All of these PLS approaches have their merits and demerits. Hence, the choice of an optimal PLS approach to employ depends on the peculiarities of the transmission and the user requirements.

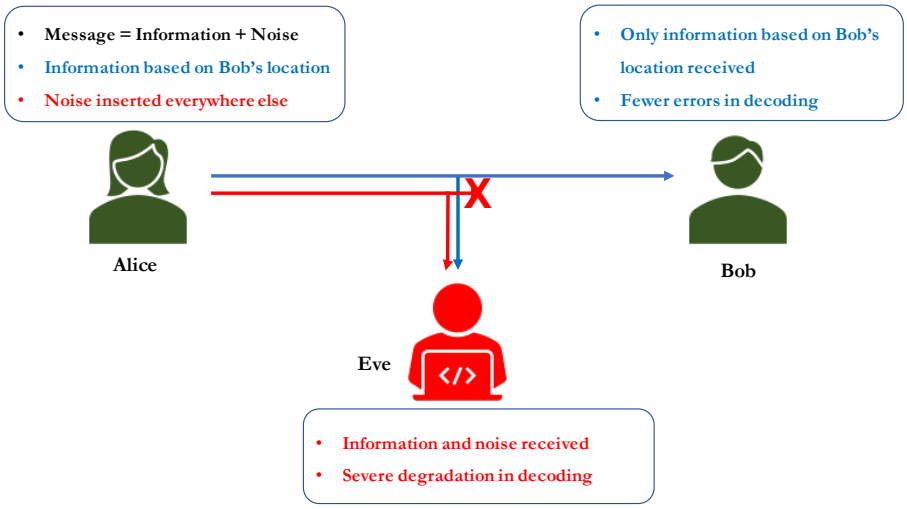


Figure 2.3: Artificial noise injection.

2.2.3 Artificial Noise Injection Approach

The use of AN injection to provide security is a well-established concept in PLS and was introduced in [32]. It is classified as a channel enhancing technique [3]. The main idea is that when a transmitter has a higher spatial Degree of Freedom (DoF) than an eavesdropper, it can exploit it by using the available power to transmit AN in the null space of the legitimate receiver but range space of the eavesdropper. This AN will be transparent to Bob but it will degrade the channel of Eve, hence secrecy is provided, shown in Fig. 2.3. To this end, we assume the main and the wiretap channels are independent. This is possible if there is a minimum separation of half a wavelength between the channels. A condition that is usually true when the environment is rich scattering [20].

In [33], AN injection was used in a MIMO scheme and further enhanced by using the advanced Intelligent Reflecting Surface (IRS). In order to maximize the secrecy rate, the transmit precoding matrix at the Base Station (BS), covariance of the AN and the phase shifts of the IRS were jointly optimized subject to the constraints of transmit power limit and unit modulus of the IRS phase shifts. The authors in [34] proposed an AN scheme for single antenna scenarios, where there is no spatial diversity advantage. With a long enough coherence block, the transmission is broken down into two phases. In the first phase, Bob transmits random AN and in the second phase, Alice sends back the random AN and useful signal back to Bob. It is assumed that Eve is unaware of the instantaneous CSI of the main channel but Bob is aware of it. The authors demonstrated that a secrecy gain was

achievable in such a scenario.

In [35], a relay-aided secure AN MIMO system was proposed. The transmitter sends signals to the destination via an amplify and forward relay in the presence of a passive eavesdropper. The system was designed as a non-convex stochastic optimization problem with a source transmission power constraint and a non-convex relay transmission power constraint. Using exact penalty function method, the non-convex relay transmission power constraint was appended to the objective function. This led to a simpler stochastic optimization problem with a non-convex objective function and convex constraints. Finally, parallel stochastic decomposition algorithm was introduced to solve this new optimization problem. The solution provided the optimal power allocation at the source and relay nodes for transmitting the AN and the useful signal to maximize the expected value of the system secrecy rate. In [36], a transmit filter and AN design for secure MIMO-OFDM systems was proposed. The transmit filter destroys the orthogonality of the signal received by the eavesdropper while the time-domain AN further improves the security of the legitimate transmission.

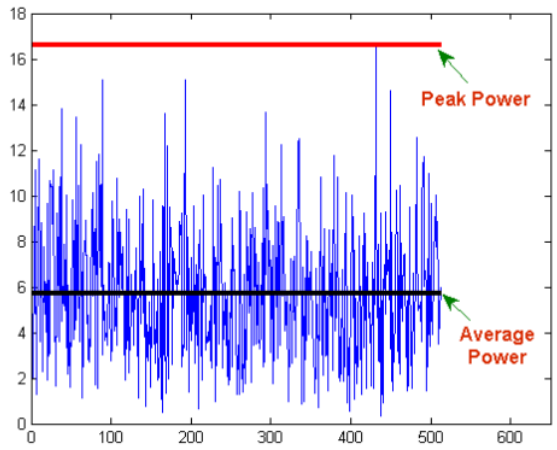


Figure 2.4: Peak-to-average power ratio (PAPR) [27].

Evidently, there have been many works on the use of AN for PLS. However, a challenge that is yet to receive enough attention in the literature is the high PAPR caused by this PLS approach. This high PAPR is caused by the in-phase superposition of the useful signal and the AN. PAPR is the ratio of the highest (peak) signal power to the average power of the signal. A high PAPR means that there is a wide gap between the signal's peak power and its average value as seen in Fig. 2.4. A high PAPR is undesirable in communication and more details are given in Section 2.3.4. Evidently, the limitation

to the use of AN for PLS in practice is the negative impact on energy efficiency. This is a crucial factor in practical deployment and deserves to be studied and optimized. More details on some of the works that address this high PAPR challenge in the literature and our contribution in this thesis are given in Section 3.1. The PAPR for a transmit signal $\boldsymbol{x}$ is calculated as:

$$\text{PAPR} = \frac{\max_{n=1,2,\ldots,N_t} \left[|x_n|^2\right]}{\mathbb{E}[\|\boldsymbol{x}\|^2]} = \frac{\|\boldsymbol{x}\|_\infty^2}{\|\boldsymbol{x}\|_2^2}, \tag{2.10}$$

where the numerator gives the peak signal power for the n-th transmit antenna out of all N_t transmit antennas while the denominator is the average signal power of all n antennas.

2.2.4 Channel Adaptation Approach

The basic idea in this category of PLS techniques is that, as long as Bob and Eve experience independent and uncorrelated fading, secure communication remains possible between Alice and Bob even when the average SNR is higher at Eve than at Bob. This can be achieved by adapting the transmission parameters to favor Bob based on its instantaneous CSI. In these techniques, there is no need for additional processing at Bob to decode the information. With independent fading, Bob will achieve a higher SNR than Eve, since the transmission parameters for Bob will be optimized, but will appear random to Eve or degrade Eve's performance. The earliest research works on this PLS technique can be found in [37–39]. The technique requires that Alice knows the instantaneous CSI of Bob. It is applicable in both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes. Most of the signal processing is done at the transmitter side and the receiver usually does not require any extra processing. This makes this PLS approach ideal for many new communication technologies that have devices with limited processing complexities. In TDD mode, the uplink and downlink are separated in time but make use of the same transmission frequency. If the uplink and downlink are separated in frequency but transmit at the same time, it is referred to as FDD. These two duplexing modes are shown in Fig. 2.5.

Several works have been done in this domain of PLS and we take a look at some of the works that are relevant to this thesis. In [40], the authors proposed the concept of fade-avoiding sub-channel usage in a frequency selective transmission scheme. The application of a channel adaptation technique in 5G URLLC was presented in [41]. Beamforming, a technique that involves adjusting the signal amplitudes and phases to form a strong beam towards a direction of interest, has also been used

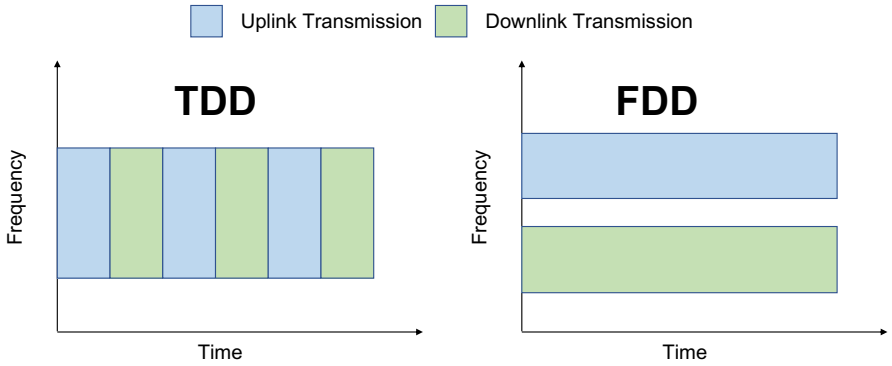


Figure 2.5: Transmission duplexing modes.

for PLS [42–44]. The use of channel coding techniques for security is addressed in [45, 46]. Optimal power allocation as a PLS technique was worked on in [11, 47]. In wireless communications, diversity techniques are based on the principle that a receiver gets several signals bearing the same information, through independently fading channels [48–50]. It is used to mitigate the effects of multipath fading. Some works in the literature address the use of diversity in providing PLS [51–53].

Precoding is a transmitter side signal processing that is employed to improve transmission performance and spectral efficiency. Usually, transmit signal preprocessing requires the CSI to be known at the transmitter. Interestingly, precoding can be used as a channel adaptation PLS technique to provide security in a transmission system. We take a look at some of the research works in this direction. In [54], the authors proposed the use of Zero-Forcing (ZF) and Minimum Mean-Squared Error (MMSE) precoders for PLS in a wiretap system where there is spatial decorrelation between the main channel and the wiretap channel. The performance of the eavesdropper is completely degraded because it carries out blind equalization as there is no CSI leakage to it. A precoded orthogonal space-time block coding in a Multiple-Input Single-Output (MISO) setup that minimizes the error rate only at the legitimate receiver was investigated in [55]. In the paper, the authors also proposed a new technique called "Precoding along with Partial Pre-Equalizing" that further improves the security of the system. This is achieved by using a new precoder design that is composed of both the original precoder and a newly designed unitary matrix. In [56], a precoder that incorporates the CSI of the eavesdropper in a mmWave UAV system was proposed. Symbol-level precoding to counteract learning-assisted eavesdropping in downlink multiuser-MISO system was proposed in [57]. The authors in [58] studied the impact of imperfect CSI on the Mean Squared Error (MSE) performance of a downlink MISO OFDM

systems using a Matched Filter (MF) precoder. Some of the works in the literature that employ MF precoding in multi-antenna scenarios can be seen in [59–61].

From the above, it is clear that channel adaptation techniques require knowledge of instantaneous CSI. However, the instantaneous CSI is not usually perfect due to factors such as noisy feedback, outdated CSI, etc. This means that under imperfect CSI conditions, the performance of the PLS scheme deteriorates. This is a limitation to the application of PLS in practice that is worthy of study. Several denoising strategies have been considered in the literature. More details on this and our contribution in this thesis will be given in Section 4.4.

2.2.5 Channel Key Approach

Finally for this Section 2.2 on PLS approaches in the literature, we will see an overview of the PLS schemes that offer security based on the secret sequences extracted from the wireless channel. This domain of PLS was introduced in [62] and elaborated by [63–65]. The fundamental approach is that Alice and Bob extract secret keys which are random sequences (vectors) or random matrices from the main/legitimate channel between them. This random key is then used to manipulate the data that is sent from Alice to Bob. Bob uses the same approach to recover the transmitted information. To make this scheme successful, the following assumptions are required to be true:

- There is spatial decorrelation between the main channel and the wiretap channel. This means they will experience independent channel responses. It is possible when there is a minimum distance of half a wavelength between Bob and Eve.
- Channel reciprocity in TDD mode holds. Reciprocity implies that the channel responses in the uplink are identical to the channel responses in the downlink. This property holds as long as the uplink and downlink transmissions happen within the channel coherence time. It is also important to mention that reciprocity is true after the proper calibration of the transmission chainset Eve reçoit.
- Channel randomness (variation) exists in the temporal, frequency and spatial domains due to rich scattering environments that cause fading and multipath reflections.

Majority of the PLS schemes under this category use one of the following channel metrics to

generate the random sequence: Received Signal Strength Indicator (RSSI), channel frequency-phase, and channel diversity methods. There are five steps employed in key generation [66]. They are:

1. Channel probing at Alice and Bob using sounding techniques to obtain random correlated measurements at both sides.
2. Extraction of channel features to use them as common random variables.
3. Quantization based on thresholds to generate secret random keys.
4. Privacy reconciliation which is the process of finding and correcting mismatch bits of the quantization outputs generated at Alice and Bob.
5. Privacy amplification to enhance the security and amplify the difficulty for Eve to guess the shared key.

2.3 Massive Multiple-Input Multiple-Output

2.3.1 Overview

In wireless communication, the electromagnetic (EM) waves carry information signal from the transmitter(s) to the receiver(s). The broadcast nature of wireless communication means that the EM wave is propagated in all directions. The signal energy is spread out and less energy reaches the receiver as the distance increases. To ensure that the receivers over a large coverage area receive a sufficient signal energy, cellular network topology was proposed and improved on in various works [67, 68]. The central idea is that the coverage area is split into cells and each cell has a BS that facilitates the communication between devices or User Equipment (UE) within the network. To simplify the discussion, each UE is connected to a BS which provides service to it. A downlink communication refers to communication from the BS to UE and a communication from the UE to the BS is referred to as uplink communication as shown in Fig. 2.6.

In recent times, the demand for wireless services has grown from wireless voice communications to heavier wireless data transmissions with services such as online video calls, online gaming, etc becoming highly desired. This means there is an urgent need to increase the area throughput in cellular communication. This is the data rate available per area and is measured in $b/s/km^2$. There

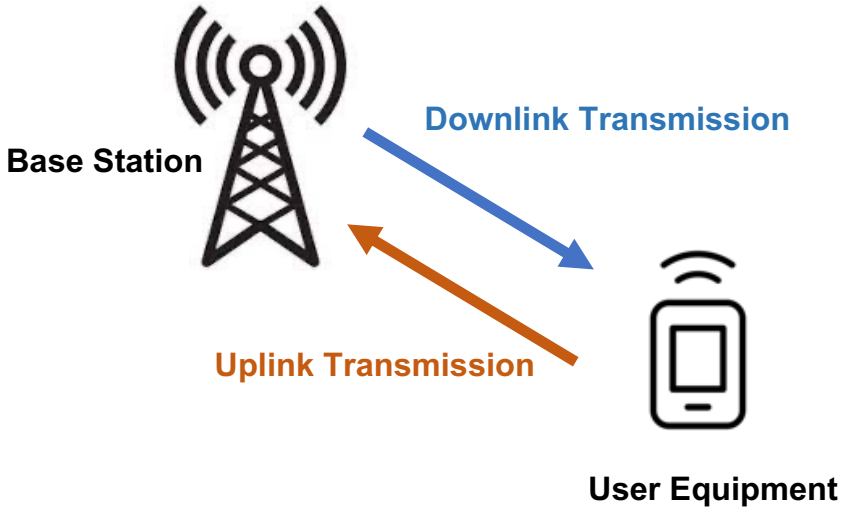


Figure 2.6: Uplink and downlink transmission.

are three ways to achieve this increase: allocating more bandwidth, densifying the network by installing more BSs per coverage area and improving the Spectral Efficiency (SE) per cell. Historically, the first two methods have been very well explored and are now at a saturation point with little to no potential for improvement in the foreseeable future [69]. The challenges of increasing these factors beyond the current state include increased risk of deep shadow (leading to reduced coverage), high deployment costs, inter-cell interference issues, limitation in range and service reliability, etc. Evidently, the most viable approach will be to improve the SE. In other words, increase the throughput by using the BS and bandwidth that are already in place in a more intelligent way through new modulation and multiplexing techniques. By definition, the SE is the amount of information that can be transferred per second over one Hz of bandwidth. It is measured in $b/s/Hz$ and expressed as:

$$SE = \log_2(1 + \gamma) \tag{2.11}$$

where γ is the Signal-to-Interference plus Noise Ratio (SINR). The following are some of the ways to improve SE include:

1. Increase in transmit power
2. Obtain an array gain
3. Uplink and downlink Space Division Multiple Access (SDMA)

4. Acquiring CSI

The first two methods above increase the SE by increasing the SINR. This means that the increase in SE will only be a logarithmic increase and that gives a slow increase in SE as seen in (2.11). To achieve greater increase in SE, a more interesting approach will be to increase the number of UE served simultaneously by the multiple antennas at the BS, and this is done with an intelligent CSI estimation method that limits the number of pilots used. The methods 3 and 4 above are the core concepts behind massive MIMO, a hot topic today that promises a bright future for wireless communication technology.

2.3.2 Fundamental Principle of Massive MIMO

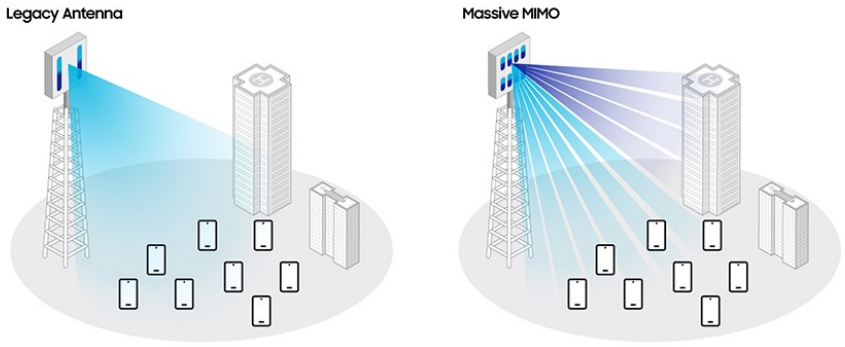


Figure 2.7: Illustration of the downlink massive MIMO [28].

Massive MIMO is widely seen as a key technology in the next generation wireless technology because it offers of the advantages of significant improvement in throughput, better radiated energy efficiency, reduced latency, simplification of the Media Access Control (MAC) layer, and robustness to intentional jamming. It was introduced in [7] and popularly studied in [70, 71]. In massive MIMO systems, the BS is equipped with a very large number of antennas as illustrated in Fig. 2.7 in comparison to legacy antenna deployment. It has great potential for 5G and beyond services such as URLLC and mMTC. Massive MIMO is highly spectrally efficient and it achieves this by adopting the following:

- It uses SDMA to achieve multiplexing gain by serving multiple UE using the same time-frequency

resources.

- It has a significantly larger number of BS antennas than the number of UE ($N_t \gg N_r$). This ensures that it benefits from the law of large numbers and is able to obtain good interference suppression. Note that N_t, grows in proportion to increase in N_r [71].
- Usually, it operates in TDD mode to limit CSI acquisition overhead due to the high number of BS antennas [8].

It is worth noting that there are now research works exploring massive MIMO in FDD mode [72–75] but the TDD massive MIMO is more common and seen in practical deployments today [7–10].

2.3.3 System Model for Downlink Transmission in Massive MIMO

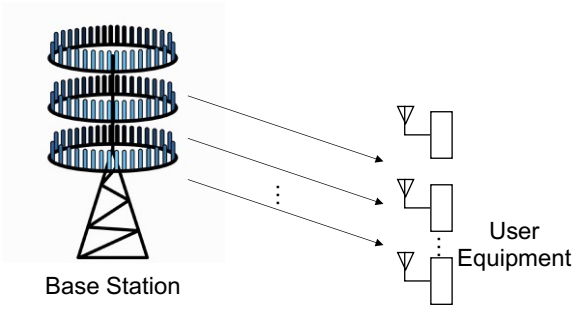


Figure 2.8: Model for downlink massive MIMO studied in the thesis.

In this thesis, we consider a single-cell massive MIMO system with a focus on the downlink communication from the BS to the UE, as shown in 2.8. Using its N_t antennas, the BS transmits the following downlink signal to the N_r single antenna UE:

$$\boldsymbol{x} = \mathbf{F}\boldsymbol{s}, \tag{2.12}$$

where $\mathbf{F} \in \mathbb{C}^{N_t \times N_r}$ is the precoding matrix for the data vector, $\boldsymbol{s} \in \mathbb{C}^{N_r \times 1}$. Equation (2.12) can be rewritten as

$$\boldsymbol{x} = \sum_{i=1}^{N_r} \mathbf{f}_i s_i. \tag{2.13}$$

where s_i is the data intended for the i-th UE and P_i is the signal power. This signal is assigned to a transmit precoding vector $\mathbf{f}_i \in \mathbb{C}^{N_t \times 1}$ that determines the spatial directivity of the transmission. The

precoding vector satisfies $\mathbb{E}\{\|\mathbf{f}_i\|\}^2 = 1$ such that $\mathbb{E}\{\|\mathbf{f}_i s_i\|\}^2 = P_i$ is the transmit power allocated to this UE.

The m-th intended UE gets the following signal:

$$\begin{aligned} y_m &= \mathbf{h}_m \boldsymbol{x} + z_m \\ &= \sum_{i=1}^{N_r} \mathbf{h}_m \mathbf{f}_i s_i + z_m \\ &= \mathbf{h}_m \mathbf{f}_m s_m + \sum_{\substack{i=1 \\ i \neq m}}^{N_r} \mathbf{h}_m \mathbf{f}_i s_i + z_m, \end{aligned} \tag{2.14}$$

where $\mathbf{h}_m$ represents the Rayleigh fading zero-mean complex Gaussian variables with unit variance for the m-th downlink channel, and $z_m \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_m^2)$ is the independent AWGN with variance σ_m^2 at the receiver. The first term in (2.14) is the desired signal while the second term represents the intra-cell interference. The channels are constant within a coherence block, while the signals and noise take new realization at every sample. The derivations of the precoding normalizations and SE at the receiver are given in details in the next chapter.

2.3.4 PAPR Challenge in Massive MIMO

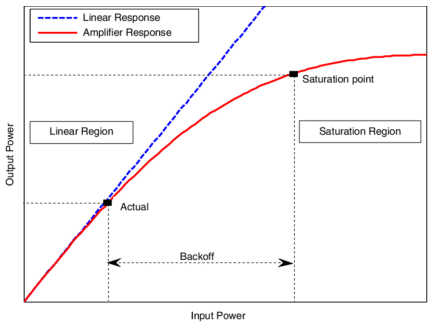


Figure 2.9: Transfer function of a High Power Amplifier (HPA) [29].

Despite numerous benefits of massive MIMO in terms of spectral and energy efficiencies, increased throughput, reduced latency, etc., one of the key areas that still remains a challenge in practical deployment is the high PAPR of its transmit signal. In as much as we can use simple linear signal processing approaches such as MF, MMSE, ZF, etc., the huge size of massive MIMO results in high dimensional precoding matrix leading to transmit signals with high PAPR. The negative effect of a high PAPR is observed in the operation of the High Power Amplifiers (HPA). HPAs increase the power

of its input signal before transmission. They are the highest power consuming unit at the BS as they account for up to 70% of the power consumption during transmission [76]. A high PAPR induces non-linearity in the radio frequency HPA. In other words, the HPA is forced to operate in the non-linear region. Consequently, there will be problems such as non-linear in-band distortion, out-of-band radiation which causes signal distortion, phase rotation and adjacent channel interference [77]. To mitigate these heavy distortions, Input Back-Off (IBO) is introduced. Such back-off forces the HPA to operate in the linear region where the transfer characteristics are sufficiently linear, see Fig. 2.9. To put it in other words, the HPA's operating point is reduced to accommodate the high signal peaks in the linear region of the HPA.

However, the disadvantage of introducing IBO is that the HPAs will have lower energy efficiency. Most of the power supplied to the HPA will be wasted as heat. This is highly undesirable, especially in massive MIMO systems where improved energy efficiency is an important goal. In addition, operating at lower power levels reduces the power efficiency, which would result in huge operational expenditure for large-scale BS having hundreds of antennas. This is not a practical solution for 5G networks since the target energy efficiency improvement is 100x with respect to (w.r.t.) 4G Long-Term Evolution (LTE). It is important to note that massive MIMO precoders exhibit transmit signals with high PAPR regardless of whether it is a single-carrier or OFDM transmission [78]. Hence, the scope of the first contribution of this thesis, to be seen in Chapter 3 is single-carrier massive MIMO.

2.4 Orthogonal Frequency Division Multiplexing

2.4.1 Fundamental Principle of OFDM

OFDM is a multi-carrier modulation technique that is useful in frequency selective transmissions. It was introduced in [79]. Bandwidth is the number of complex-valued samples that describes a signal per second. Therefore, the time interval between two samples is inversely proportional to the bandwidth. In other words, one decreases when the other increases. It is worth mentioning that wireless channels have a dispersive nature. This means that the signal energy that is transmitted over a given interval will naturally spread out and be received for a duration that is longer than the transmit duration. The implication of this is interference between successively transmitted symbols.

OFDM proffers an effective solution to this by subdividing the available channel bandwidth into a

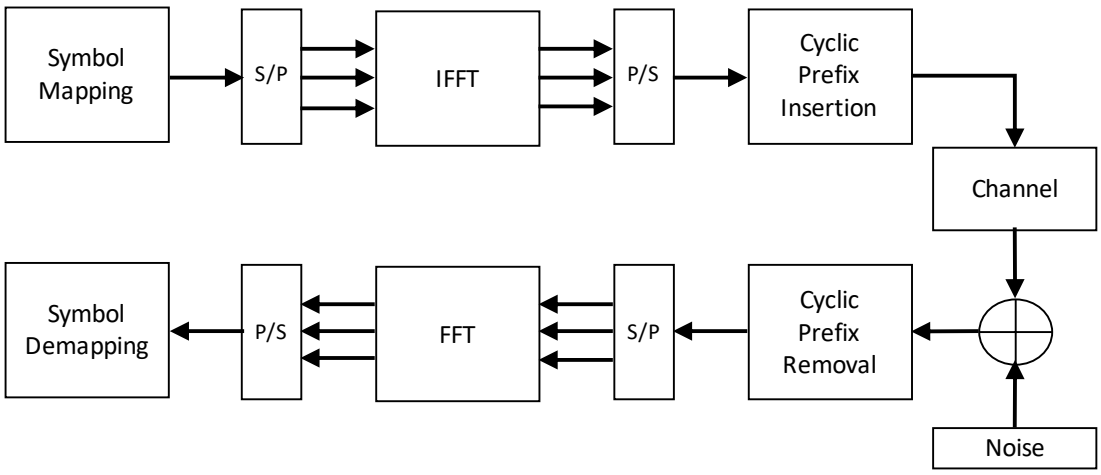


Figure 2.10: Block diagram of OFDM transmission.

number of equal-bandwidth subchannels with one subcarrier per subchannel. The bandwidth of the subchannel will be low enough to ensure that each subchannel experience a nearly constant frequency response. This means that the time interval between two successive samples will be longer than the channel dispersion. In other words, each subcarrier will experience flat fading, even in a frequency selective environment. For a channel bandwidth, B, K subcarriers are created such that $K = B/\Delta f$, where Δf is the equal spacing between the subcarriers. If the total symbol rate for an OFDM block is T, then by setting the symbol rate on each subcarrier, $1/T$ to be equal to Δf, there will be complete orthogonality between the subcarriers over the entire symbol duration, independently of the relative phase between the subcarriers.

In this section, we briefly discuss the steps in an OFDM communication from the transmitter to the receiver shown in Fig. 2.10. The first step at the transmitter is the data mapping which means mapping generated bit streams to corresponding symbols based on the adopted modulation techniques such as Quadrature Phase Shift Keying (QPSK), Quadrature Amplitude Modulation (QAM), etc. The high bit-rate data stream is split into K parallel low-rate data streams by using a simple Serial-to-Parallel (S/P) conversion to prepare the data conversion into the OFDM waveform. It is important to mention that K corresponds to the number of subcarriers and the Fast Fourier Transform (FFT) size. After this, K-point Inverse Fast Fourier Transform (IFFT) operation is applied to the blocks of K data symbols. This corresponds to modulating K orthogonal subcarriers. The obtained samples are now in the time domain and are then reconverted to a serial stream using a simple parallel-to-serial

(P/S) converter. The final step at the transmitter before transmission is the insertion of CP which should be greater than the maximum delay spread of the channel. After this, the signal is sent to the receiver. At the receiver, the first step is the CP removal. Afterwards a S/P conversion takes place to reconstruct the separate OFDM blocks. Next, K-size FFT operation and a simple equalization take place respectively. Finally, symbol demapping to recover the sent symbol is done.

2.4.2 FFT Implementation of OFDM

From above, the transmitted OFDM symbol is the Inverse Discrete Fourier Transform (IDFT) of the transmit data sequence between $0 \leq k \leq K$. Hence, the transmit signal is simply the concatenation of blocks obtained by performing the IDFT on blocks of K data symbols. In addition, the receiver performs Discrete Fourier Transform (DFT) operation to transform the signal back to the frequency domain for equalization. It is important to state that for an improvement in complexity, K is usually chosen to be a power of 2 so that the fast and more efficient IFFT can be used at the transmitter and FFT at the receiver [80], see Fig. 2.11. This has a complexity of only $K \log K$ as compared with DFT/IDFT with a complexity of K^2.

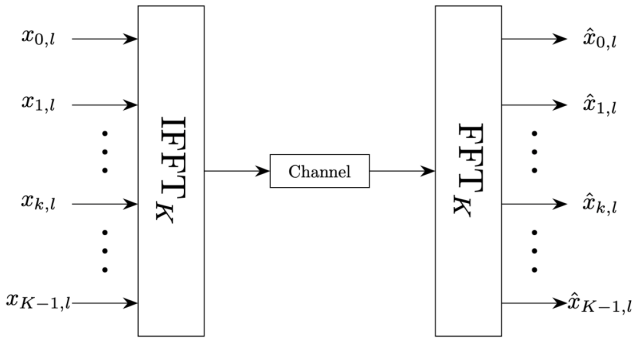


Figure 2.11: OFDM implementation using IFFT/FFT.

2.4.3 Cyclic Prefix

To completely remove the effect of Inter-Symbol Interference (ISI) and maintain the orthogonality between subcarriers, a CP is inserted between consecutive OFDM symbols. Due to the CP insertion, the transmitted signal becomes periodic and the effect of the time-dispersive multipath channel is equivalent to a cyclic convolution. In other words, the CP transforms the linear convolution channel to a cyclic convolution channel. This means that after the FFT operation, the equalization becomes

the simply task of removing the scalar gain per subcarrier. To insert the CP, we copy a portion of the OFDM block of length Δ at the end of the block and introduce it in the front of the block as shown in Fig. 2.12. The length is carefully chosen to ensure that its addition to T will guarantee that the overall length will accommodate the longest delay spread expected on the frequency selective channel, thereby eliminating ISI.

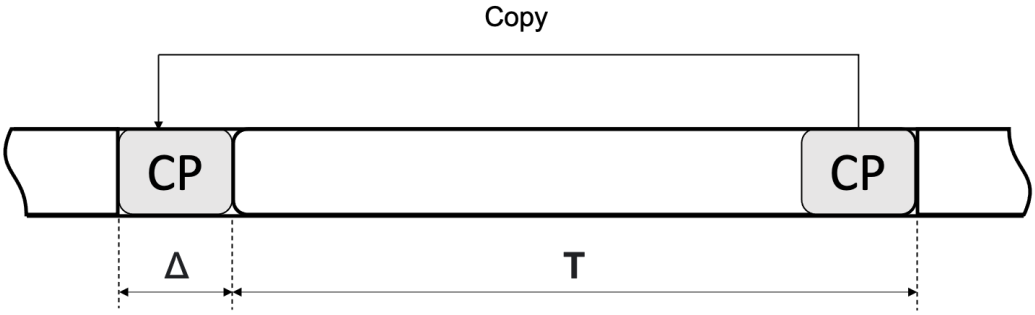


Figure 2.12: An OFDM symbol consisting of a useful part prepended with a CP.

2.5 Artificial Intelligence

2.5.1 Overview

AI is defined as a computation paradigm that gives intelligence to a machine with the goal of teaching the machine to learn, react and work like humans. Generally speaking, there are numerous AI techniques, such as Machine Learning (ML), Expert Systems, Evolutionary Algorithms, etc. ML techniques encompass the body of algorithms that extract knowledge from data to make decisions without being explicitly programmed. In terms of the learning mechanism, ML techniques are broadly categorized as Supervised Learning [81, 82], Unsupervised Learning [83], and Reinforcement Learning [84].

Deep learning is a subset of ML which is in turn a subset of AI, see Fig. 2.13. Deep learning allows computational models that consists of multiple layers to learn the representations of data with multiple levels of abstraction, from low to high level features. Some of the major advantages of deep learning over ML are feature engineering and capability to better handle large amount of data. A very important step in traditional ML is feature engineering which consists of feature extraction and/or feature selection. Feature selection is the process of reducing the number of dimensions in the raw data by removing less useful features and keeping only significant features. Feature extraction, on the other

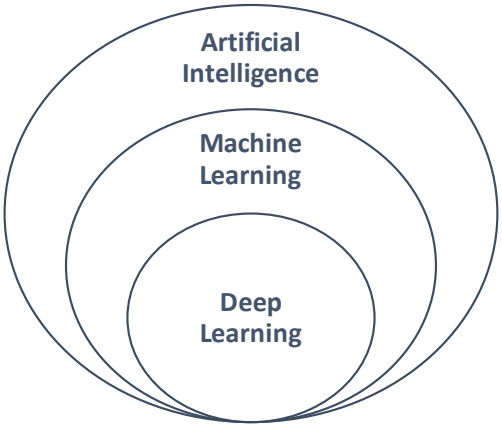


Figure 2.13: Venn diagram of the relation between deep learning, ML, and AI.

hand, is the process of transforming the raw data into a processed data with lower dimensions. In essence, feature engineering involves using domain knowledge to extract the most important features in a raw data that have a significant consequence on the ML model design. Usually, when feature engineering is properly done, it improves the performance of the ML algorithm. However, it is well known that feature extraction is time consuming and very costly [85]. It requires detailed engineering and good domain expertise. Interestingly, human interaction is not needed for feature extraction in deep learning. Deep learning falls under the category of Representation Learning. By using the multiple processing layers, high level features and inner correlations are extracted from the data without any prior feature handling [86]. The low level features are represented at the earlier layers and high level features are represented as we go deeper into the model.

In addition, some traditional ML algorithms typically load all data in memory during the training of the algorithm. This could become cumbersome in big data scenarios, which is typical in mobile and wireless systems. In contrast, Stochastic Gradient Descent (SGD) which is used in deep learning training only requires a batch of the overall data at every step of the training. This makes deep learning highly scalable with big data. More so, increasing the data size provides limited increase in legacy ML algorithms unlike in deep learning algorithms where the performance significantly grows with large volumes of data.

2.5.2 Deep Learning in Wireless Communication

The breakthroughs of deep learning are very well established in some domains such as image processing [23, 87], natural language processing [88], etc. Similarly, in recent times, research works have been done on the application of deep learning in wireless communications. All layers of the wireless communication stack have been addressed but we take a look at the applications of deep learning to the PHY layer. The authors in [89, 90] proposed the use of deep learning for automatic modulation classification. Channel estimation and signal detection in OFDM systems was presented in [91]. The use of Multilayer Perceptron (MLP), Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) for channel decoding in 5G systems was proposed in [92]. The use of deep learning for Rayleigh channel prediction for massive MIMO, PLS, Non-Orthogonal Multiple Access (NOMA), and Coordinated Multi-Point (CoMP) contexts was proposed in [93]. These are but a few of the applications of deep learning at the PHY layer. A survey of more related works can be seen in [94–96].

2.5.3 Autoencoder

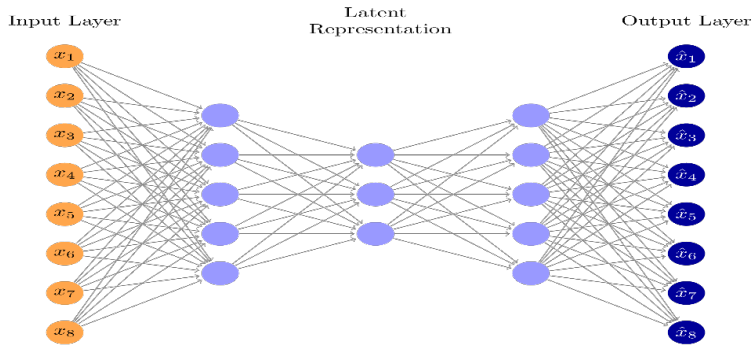


Figure 2.14: Autoencoder architecture.

There are many deep learning architectures available today but of interest to this thesis is the autoencoder architecture. Autoencoders learn an encoder function from the input to representation and a decoder function back from the representation to the input space as shown in Fig. 2.14. The goal is to find a low-dimensional representation of its input to at some intermediate layer and then reconstruct the output with minimal error. The closer the output is to the input, the more effective the autoencoder model is. It uses the neural network framework of deep learning. There are, basically 7 types of autoencoders: Denoising Autoencoder (DAE), Sparse Autoencoder, Deep Autoencoder, Contractive Autoencoder, Undercomplete Autoencoder, Convolutional Autoencoder, and Variational

Autoencoder. In this thesis, the DAE will be used to achieve optimal PLS performance in the proposed channel adaptation PLS scheme to be seen in Section 4.2.

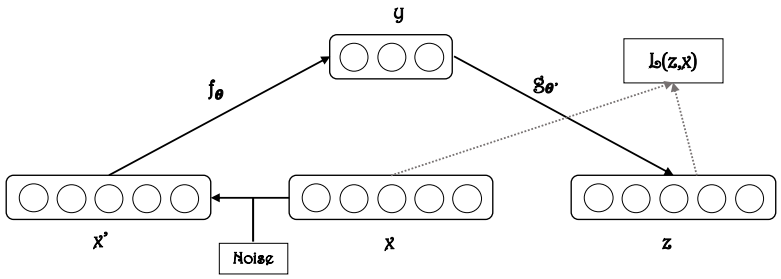


Figure 2.15: Denoising autoencoder architecture.

The approach in the DAE is shown in Fig. 2.15. Instead of simply reconstructing the input, it attempts to reconstruct a noisy version of the input. In essence, the encoder operation (f_θ) generates the latent representation from a noisy input while the decoder operation (g'_θ) attempts to recover a noiseless version of the input from the latent representation of a noisy input. The system is forced to learn the hidden representation of the input and will not carry out a simply copy/paste operation. The noise that corrupts the input can be a Gaussian noise and more details about the proposed DAE solution in our proposed PLS scheme will be given in Section 4.4.

2.6 Conclusion

In this chapter, some fundamental concepts of major aspects of this thesis was discussed. The knowledge of these key areas are pivotal for the appreciation of the contributions of the thesis. A discussion of some of the state-of-the art techniques were also addressed. In the next chapter, the first contribution of the thesis will be presented. It covers the use of AN in an energy efficient way in massive MIMO.

Chapter 3

Energy Efficiency in Secure Massive MIMO

Contenu

3.1 Introduction

In this chapter, we study the important relationship between providing PLS by the use of AN injection and the resulting energy efficiency of the system. As mentioned in Section 2.5.1, the AN injection PLS scheme exploits the excess spatial DoFs between the transmitter and the receiver. Therefore, the large number of transmit antennas compared to the receiver in massive MIMO creates an opportunity to deploy AN injection. Important to note is the fact that the high transmit signal PAPR in massive MIMO can be accentuated by in-phase superposition between the information signal and the AN sub-spaces. Hence, if not carefully designed, we risk providing security at the expense of energy efficiency. To address this high PAPR challenge, we take a look at the few related works in the literature. The authors in [97] showed that the famous AN-based technique proposed in [32] causes high PAPR in the antenna domain for a MISO model. This was compared with traditional OFDM signal in the time domain. To solve this problem, an angle rotation based technique was proposed to reduce the PAPR, while maintaining the secrecy capacity performance as that of the original AN-aided method. In [98], the authors proposed to either change the distribution of the added AN from Gaussian to uniform in flat fading environments or use an optimized AN. This does not only avoid PAPR increase but also helps reduce the PAPR of OFDM signal transmission in a Single-Input Single-Output (SISO) model. In [99], the authors proposed a power allocation algorithm for AN subspaces to solve the non-convex optimization problem of PAPR. It is based on fractional programming, the difference between convex functions programming and non-convex quadratic equality constraint relaxation.

3.2 System Model

3.2.1 Downlink Massive MIMO Transmission

We consider a single-cell massive MIMO downlink transmission between a BS (Alice) with N_t antennas and N_r legitimate single-antenna receiver terminals in the presence of passive eavesdropper (Eve) equipped with $N_{r,e}$ receive antennas as shown in Fig. 3.1. Eve can be perceived either as an eavesdropper with multiple antennas or several single antenna eavesdroppers that can collaborate and carry out cooperative detection. In our study, we consider the situation in which all eavesdroppers collaborate to eavesdrop on the information transmitted to only one legitimate terminal. In essence, in this thesis, Bob signifies one terminal out of the available N_r terminals. Note that N_t is significantly

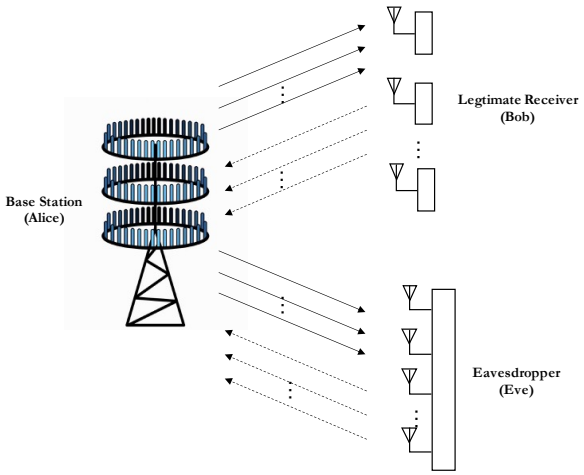


Figure 3.1: System model of the AN precoded single-carrier massive MIMO downlink transmission with N_t antennas at the BS, N_r single antenna legitimate receivers and $N_{r,e}$ antennas at the eavesdropper where $N_t \gg N_r, N_{r,e}$.

larger than N_r and $N_{r,e}$ ($N_t \gg N_r, N_{r,e}$).

We assume a non-line-of-sight rich scattering environment and, as such, model all channels as uncorrelated flat-fading Rayleigh channels. It is assumed that the main channel, $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$, can be perfectly estimated and is available at the BS using channel reciprocity in TDD mode. The property is commonly used in the literature related to massive MIMO with TDD mode [7–10]. We assume that Alice is unaware of Eve's CSI, $\mathbf{H}_e \in \mathbb{C}^{N_{r,e} \times N_t}$. The entries of $\mathbf{H}$ and $\mathbf{H}_e$ are independent and identically distributed (i.i.d.) zero-mean complex Gaussian variables with unit variance.

Two precoding methods have been considered in this work; ZF and MF. The easier to implement MF precoding simply maximizes the SNR at the legitimate receiver only while ZF precoding aims to cancel out Multi-User Interference (MUI) between the legitimate receivers. The computational complexity of ZF precoding is discussed in [11,12]. The precoding vector, $\mathbf{F} \in \mathbb{C}^{N_t \times N_r}$, can be written as

$$\mathbf{F} = \begin{cases} \mathbf{H}^\dagger(\mathbf{H}\mathbf{H}^\dagger)^{-1}, & \text{if ZF Precoding,} \\ \left[\frac{\mathbf{h}_1^\dagger}{\|\mathbf{h}_1\|}, \ldots, \frac{\mathbf{h}_{N_r}^\dagger}{\|\mathbf{h}_{N_r}\|}\right], & \text{if MF Precoding.} \end{cases} \tag{3.1}$$

Thus, the precoded transmit signal, $\boldsymbol{v} \in \mathbb{C}^{N_t \times 1}$ for a data vector, $\boldsymbol{s} \in \mathbb{C}^{N_r \times 1}$ with N_r complex values, can be expressed as

$$\boldsymbol{v} = \sqrt{\frac{1}{\psi}}\mathbf{F}\boldsymbol{s}, \tag{3.2}$$

where ψ is the Frobenius norm of $\mathbf{F}$ that is included for normalization (derivation given in Section 3.11) and is simply expressed as

$$\psi = \begin{cases} \frac{N_r}{N_t - N_r}, & \text{if ZF Precoding,} \\ N_r, & \text{if MF Precoding.} \end{cases} \tag{3.3}$$

3.2.2 Artificial Noise Precoded Transmission

For an AN-precoded system with a total available power P, the power budget is respected by distributing the power between the information signal and AN. The power allocated to the information signal is represented as θP while the rest of the power budget, $(1-\theta)P$, is dedicated to the AN, where $0 < \theta \leq 1$.

We calculate the null space matrix, $\mathbf{V} \in \mathbb{C}^{N_t \times N_t}$, for $\mathbf{H}$ using the Moore–Penrose Pseudoinverse [13]:

$$\mathbf{V} = \mathbf{I}_{N_t} - \mathbf{H}^{\dagger}(\mathbf{H}\mathbf{H}^{\dagger})^{-1}\mathbf{H}. \tag{3.4}$$

We adopt equal power allocation across all transmit antennas. Thus, when a random AN is injected into the null space of the main channel, the transmit signal, $\boldsymbol{x} \in \mathbb{C}^{N_t \times 1}$ for a data vector, $\boldsymbol{s} \in \mathbb{C}^{N_r \times 1}$ with N_r complex values, can be expressed as

$$\boldsymbol{x} = \sqrt{\frac{\theta}{\psi}}\mathbf{F}\boldsymbol{s} + \sqrt{\frac{1-\theta}{\xi}}\mathbf{V}\boldsymbol{k}, \tag{3.5}$$

where $\boldsymbol{k} \in \mathbb{C}^{N_t \times 1}$ is the randomly generated AN with a covariance matrix $\sigma_k^2 \mathbf{I}_{N_t}$, while ξ is the Frobenius norms of $\mathbf{V}$ (derivation given in the Section 3.11) that is included for normalization and simply expressed as

$$\xi = N_t - N_r. \tag{3.6}$$

For the m-th legitimate terminal, the received symbol is given as

$$y_{b_m} = \begin{cases} \sqrt{\frac{\theta}{\psi}} s_m + z_b, & \text{if ZF Precoding,} \\ \sqrt{\frac{\theta}{\psi}} \mathbf{h}_m \mathbf{f}_m s_m + \sum\limits_{\substack{i=1 \\ i \neq m}}^{N_r} \sqrt{\frac{\theta}{\psi}} \mathbf{h}_m \mathbf{f}_i s_i + z_b, & \text{if MF Precoding,} \end{cases} \tag{3.7}$$

where s_m is the m-th element in the transmit data vector $\boldsymbol{s}$, and the remaining s_i is the i-th element in the data vector transmitted to other receivers in the same cell, and $z_b \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_b^2)$ is the complex AWGN component at the legitimate terminal with variance σ_b^2 which is uncorrelated with s_m. The first term for the MF precoded signal in (3.7) is the desired signal whose SNR is maximized due to the MF precoding, and the second term shows the intra-cell MUI. This is the major difference with ZF precoding whose MUI is zero, thus guaranteeing excellent transmission quality for legitimate users. However, this comes at the expense of computational complexity [11, 12].

The received signal at the eavesdropper, $\boldsymbol{y}_{e_1} \in \mathbb{C}^{N_{r,e} \times 1}$, is

$$\boldsymbol{y}_{e_1} = \sqrt{\frac{\theta}{\psi}}\mathbf{H}_e\mathbf{F}\boldsymbol{s} + \sqrt{\frac{1-\theta}{\xi}}\mathbf{H}_e\mathbf{V}\boldsymbol{k} + \boldsymbol{z}_e, \tag{3.8}$$

where $\boldsymbol{z}_e \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_e^2\mathbf{I}_{N_{r,e}})$ is the i.i.d. AWGN sample with covariance matrix $\sigma_e^2\mathbf{I}_{N_{r,e}}$.

3.3 Performance Metrics

In this section, we present the performance metrics needed to study the security and energy efficiency performance of this system. With these metrics, we are able to propose an optimal power allocation ratio for the scheme, and highlight the energy efficiency gains. The metrics adopted are PAPR, secrecy capacity, SER, SEE, and HPA efficiency.

3.3.1 Peak-to-average Power Ratio (PAPR)

Recall that PAPR is defined as the ratio of the highest (peak) signal power to its average power value, Section 2.3.4. For the transmit signal (3.5), it can be written as

$$\text{PAPR}_1 = \frac{\max_{n=1,2,\ldots,N_t}\left[|x_n|^2\right]}{\mathbb{E}[\|\boldsymbol{x}\|^2]} = \frac{\|\boldsymbol{x}\|_\infty^2}{\|\boldsymbol{x}\|_2^2}. \tag{3.9}$$

3.3.2 Secrecy Capacity

From (3.7), the channel capacity when we consider only one legitimate receiver is written as

$$C_{b_m} = \begin{cases} \log_2\left(1+\frac{\theta}{\psi}\overline{\gamma}\right), & \text{if ZF Precoding,} \\ \log_2\left(1+\dfrac{\dfrac{\theta\overline{\gamma}\|\mathbf{h}_m\|^2}{\psi}}{\dfrac{\theta\overline{\gamma}}{\psi}\sum\limits_{\substack{n=1\\n\neq m}}^{N_r}\dfrac{|\,\mathbf{h}_m\mathbf{h}_n^\dagger\,|^2}{\|\mathbf{h}_n\|^2}+1}\right), & \text{if MF Precoding,} \end{cases} \tag{3.10}$$

where $\overline{\gamma}$ is the average SNR at the legitimate receiver given as

$$\overline{\gamma} = \frac{\mathbb{E}\{|\,s\,|^2\}}{\sigma_b^2} = \frac{\sigma_s^2}{\sigma_b^2}, \tag{3.11}$$

and σ_s^2 is the variance of the transmit data symbol, s_m.

Inspired by [100], we show the channel capacity for Eve when a Gaussian random AN is injected in the null space of the main channel with equal power allocation,

$$\psi\sigma_s^2 + \xi\sigma_k^2 = P. \tag{3.12}$$

For notational convenience, we represent

$$\mathbf{A} = \mathbf{H}_e\mathbf{F}\mathbf{F}^\dagger\mathbf{H}_e^\dagger, \text{ and } \mathbf{B} = \mathbf{H}_e\mathbf{V}\mathbf{V}^\dagger\mathbf{H}_e^\dagger. \tag{3.13}$$

By letting $\sigma_s^2 = \theta P/\psi$ and $\sigma_k^2 = (1-\theta)P/\xi$, the wiretap channel capacity for a cooperative eavesdropper attempting to intercept a single symbol out of all the transmitted symbols can be written as

$$\begin{aligned} C_e = \frac{1}{N_{r,e}}\Bigg(&\log_2\det\left(\mathbf{I}_{N_{r,e}} + \frac{\theta\overline{\gamma}}{\psi}\mathbf{A} + \frac{(1-\theta)\overline{\gamma}}{\xi}\mathbf{B}\right) \\ &- \log_2\det\left(\mathbf{I}_{N_{r,e}} + \frac{(1-\theta)\overline{\gamma}}{\xi}\mathbf{B}\right)\Bigg). \end{aligned} \tag{3.14}$$

From (3.10) and (3.14), considering a model in which the symbol sent to a single terminal is intercepted by collaborating eavesdroppers, the secrecy capacity when a Gaussian random AN is injected is given as

$$C_{s_1} = [C_{b_m} - C_e]^+. \tag{3.15}$$

3.3.3 Secrecy Energy Efficiency (SEE)

Energy efficiency refers to the total number of bits successfully transmitted by consuming a Joule of energy [19]. Similarly, Secrecy Energy Efficiency (SEE) is the total number of confidential information bits transmitted by consuming a Joule of energy. The total power consumption at the BS is the combined HPA power across all antennas and the circuit power consumption which is also proportional to the number of active antennas, N_t [19]. It can be written as

$$P_{\text{total}} = \sum_{a \in N_t} \frac{P_a^{out}}{\eta_a} + N_t P_{cir}, \tag{3.16}$$

where P_{cir} denotes the circuit power consumption. From (3.15) and (3.16), the SEE is evaluated as

$$\text{SEE} = \frac{C_s}{P_{\text{total}}}. \tag{3.17}$$

3.3.4 High Power Amplifier Efficiency

For the a-th transmit antenna, the HPA efficiency denoted η_a, is modeled according to [10] as

$$\eta_a = \left(\frac{P_a^{out}}{P_{a,max}^{out}} \right)^{\beta} \eta_{max}, \tag{3.18}$$

where P_a^{out} is the operating point of the antenna HPA and $P_{a,max}^{out}$ is the maximum HPA output power. This ratio represents, on a linear scale, the Output Back-Off (OBO) of the HPA. The maximal HPA efficiency is η_{max} and $\beta \in [0, 1]$ is the efficiency exponent depending on the type of HPA. The value of β is 0.5 and 1 for non-ideal class B and A HPAs, respectively. In this work, we consider class B HPA because they are more efficient and do not have the heating problems associated with class A HPAs. Class B amplifier uses two complimentary transistors for each half of the waveform, so that each transistor device amplifies only half of the output waveform. Hence, it has a significantly better efficiency than class A HPA. Due to its zero bias, its OBO is equal to the IBO [101]. Hence, the HPA efficiency can be rewritten in terms of IBO as

$$\eta_a = \left(\frac{P_a^{in}}{P_{a,max}^{in}} \right)^{\beta} \eta_{max}, \tag{3.19}$$

where P_a^{in} is the input operating point of the antenna HPA and $P_{a,max}^{in}$ is the maximum HPA input power. For the proposed scheme and the legacy schemes to achieve complete linearity, we introduce

an IBO that is equal to the magnitude of the PAPR. This guarantees that the peak signal points still fall within the linear region of the HPA. On a linear scale, the IBO will be the inverse of the PAPR. The HPA efficiency is then rewritten as

$$\eta_a = \left(\frac{1}{\text{PAPR}}\right)^{\beta} \eta_{max}. \tag{3.20}$$

3.4 PAPR-Aware Artificial Noise

To jointly minimize the PAPRs associated with all antennas in (3.9) results in a non-convex problem that is complicated to solve and, to the best of our knowledge, there is no efficient solution for such a non-convex problem. Inspired by the work in [102], our proposed transmission scheme transforms the PAPR reduction and AN generation challenge into an iterative online algorithm. At every iteration of the algorithm, an updated transmit signal, $\boldsymbol{\upsilon} \in \mathbb{C}^{N_t \times 1}$, is clipped based on a clipping threshold (λ_ℓ) that is dependent on the PAPR target (PAPR_0). The excess signal at every iteration, $\boldsymbol{z} \in \mathbb{C}^{N_t \times 1}$, is then used to generate a PAPR-aware AN, $\boldsymbol{\omega} \in \mathbb{C}^{N_t \times 1}$, which is added to the current iteration transmit signal. The combination of the current iteration transmit signal and PAPR-aware AN are then used as the transmit signal of the next iteration. At the last step of the algorithm, the final PAPR-aware AN is the normalized summation of all ANs generated at each step of the algorithm. This is then added to the ZF/MF precoded signal, with power allocation constraints obeyed. The algorithm is shown diagrammatically in Figure 3.2 below:

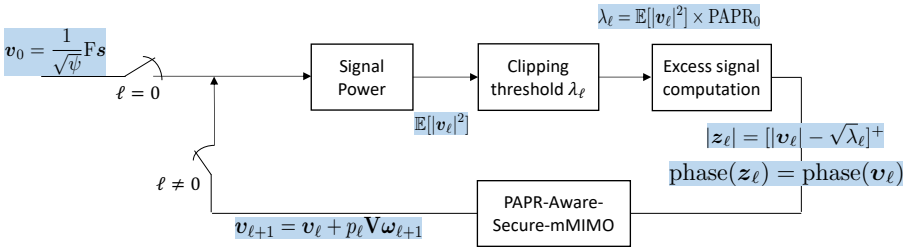


Figure 3.2: Algorithm Flow.

Our goal is to exploit the null space provided by massive MIMO in the design of the PAPR-aware AN. Similar to other AN injection schemes, this PAPR-aware noise is injected into the null space of the main channel, $\mathbf{H}$. This means that the AN will remain transparent to Bob but will degrade the wiretap channel, $\mathbf{H}_e$, since it is in its range space. Indeed, the majority of the literature with passive eavesdroppers considered that Bob's channel is independent of Eve in wireless environments, which

can be satisfied when they are separated apart by at least half a wavelength [20, 26]. Note that this is only true in rich scattering environments.

The main contributions can be summarized as follows:

- We propose an iterative online algorithm, referred to as PAPR-Aware-Secure-mMIMO algorithm. It has the advantage of providing security due to AN injection while reducing the PAPR of the transmit signal. At each iteration step, excess signal after clipping is used to design a PAPR-aware AN. The two objectives at each iteration step are that PAPR-aware AN is constrained to the null-space and the PAPR of the transmit signal at that point is less than or equal to the target PAPR. This becomes a convex optimization problem and we showed that it can be solved online by Gradient Descent (GD) approach, using the instantaneous information . The proposed AN achieves the same secrecy capacity as legacy AN aided schemes employing random AN [32] but with the additional advantage of a reduced PAPR. Using numerical simulations, we validate the performance of our proposed scheme in a downlink massive MIMO transmission exposed to passive eavesdropping.

- We study the impact of the ratio of the power distribution between the useful signal and the AN on the secrecy capacity, SEE, PAPR and SER in our proposed transmission scheme. We analyze the PAPR performance of the transmission scheme w.r.t. the number of transmit antennas at the BS and target PAPRs.

- We study the impact of correlation on these performance metrics. The degree of correlation is evaluated in terms of Angular Standard deviation (ASD). In addition, using numerical simulation, we show the gain in SEE for our proposed scheme compared to the legacy schemes.

3.5 PAPR-Aware-Secure-mMIMO ALGORITHM

In the PAPR-Aware-Secure-mMIMO, we commence by applying linear precoding to signal that gives high transmission quality (3.2). We then apply an iterative algorithm to evaluate the peak-canceling signals. This reduces the PAPR of the transmit signal and enhances security.

To obtain the optimal PAPR, the high amplitudes of the transmit signal is iteratively clipped to an optimal threshold before transmission. The clipping threshold, λ_ℓ, for every iteration is the average

signal power at the iteration multiplied by the PAPR target (PAPR_0), in essence

$$\lambda_\ell = \mathbb{E}[|\boldsymbol{\upsilon}_\ell|^2] \times \text{PAPR}_0. \tag{3.21}$$

We represent the clipped signal as $\boldsymbol{d} \in \mathbb{C}^{N_t \times 1}$ and the excess signal after clipping as $\boldsymbol{z}$ whose magnitude and phase of $\boldsymbol{z}$ are such that $|\boldsymbol{z}_\ell| = [|\boldsymbol{\upsilon}_\ell| - \sqrt{\lambda}_\ell]^+$ and $\text{phase}(\boldsymbol{z}_\ell) = \text{phase}(\boldsymbol{\upsilon}_\ell)$. In another form, the excess signal after clipping can be expressed as:

$$\boldsymbol{z} = [\boldsymbol{\upsilon} - \boldsymbol{d}]^+. \tag{3.22}$$

For every channel realization, the optimal excess signal at each iteration step on the algorithm is the one which represents our PAPR-aware AN ($\boldsymbol{\omega}$) projected into the null-space. In essence, the optimal excess signal is given as

$$\boldsymbol{z}_\ell = \mathbf{V}\boldsymbol{\omega}_\ell. \tag{3.23}$$

However the peak canceling signal hardly equals $\boldsymbol{z}$. To address this challenge, we employ the convex optimization problem (3.24) below.

$$\begin{aligned} &\text{Find } \arg\min_{\boldsymbol{\omega}} \|\mathbf{V}\boldsymbol{\omega} - \boldsymbol{z}\|_2^2, \\ &\text{subject to } \begin{cases} \boldsymbol{z} = [\boldsymbol{\upsilon} - \boldsymbol{d}]^+ \\ \text{PAPR}(\boldsymbol{d}) \leq \text{PAPR}_0. \end{cases} \end{aligned} \tag{3.24}$$

In the first constraint, we ensure that only the excess signal after clipping is used to design the PAPR-aware AN. The second constraint ensures that the PAPR of the clipped signal does not exceed the target PAPR. The optimization problem above can be solved using the SGD method [14, 15]. The search directions of the steepest gradient at every iteration step in the algorithm is given by the negative gradient of $\boldsymbol{G}$ at $\boldsymbol{\omega}_\ell$ denoted as

$$\nabla_{\omega_\ell} \boldsymbol{G}(\boldsymbol{\omega}_\ell) = \frac{2}{\mathcal{L}_\omega} \mathbf{V}^\dagger (\mathbf{V}\boldsymbol{\omega}_\ell - \boldsymbol{z}_\ell), \tag{3.25}$$

where $\mathcal{L}_e = 2\sigma^2_{\mathbf{max}}(\mathbf{V})$ is the Lipschitz constant [16] for $\|\mathbf{V}\boldsymbol{\omega} - \boldsymbol{z}\|_2^2$. From (3.25), at each iteration step, the PAPR-aware an is updated as

$$\boldsymbol{\omega}_{\ell+1} = \boldsymbol{\omega}_\ell - \nabla_{\omega_\ell} \boldsymbol{G}(\boldsymbol{\omega}_\ell), \tag{3.26}$$

and the signal for the next step of the algorithm is updated as

$$\boldsymbol{\upsilon}_{\ell+1} = \boldsymbol{\upsilon}_{\ell} + p_{\ell}\mathbf{V}\boldsymbol{\omega}_{\ell}, \tag{3.27}$$

where p is a regularization factor calculated using Least Squares Approximation (LSA) [17]. By using this regularization factor, the amplitude of peak canceling signals generated by LSA is almost equal to those of the original clipping noise. It can be expressed as

$$p_{\ell} = \frac{\mid \mathbf{V}\boldsymbol{\omega}_{\ell} \mid^{\mathrm{T}} \mid \boldsymbol{z}_{\ell} \mid}{\|\mathbf{V}\boldsymbol{\omega}_{\ell}\|^2}. \tag{3.28}$$

As earlier described, the final PAPR-aware AN for every channel realization is the normalized summation of the $p_{\ell}\mathbf{V}\boldsymbol{\omega}_{\ell}$ for every step of the iteration. Hence, at the final step of the algorithm, we obtain the PAPR-aware AN precoded signal, $\ddot{\boldsymbol{x}} \in \mathbb{C}^{N_t \times 1}$, written as

$$\ddot{\boldsymbol{x}} = \sqrt{\frac{\theta}{\psi}}\mathbf{F}\boldsymbol{s} + \sqrt{\frac{(1-\theta)}{\xi}}\mathbf{V}\frac{\ddot{\boldsymbol{\omega}}}{\sigma_{\ddot{\omega}}}, \tag{3.29}$$

where

$$\ddot{\boldsymbol{\omega}} = \sum p_{\ell}\mathbf{V}_{\ell}\boldsymbol{\omega}_{\ell},$$

and $\sigma_{\ddot{\omega}}$ is the standard deviation of the total injected AN $\ddot{\boldsymbol{\omega}}$.

3.6 Algorithm Summary

In this section, we sequentially itemize the steps employed in the proposed PAPR-Aware-Secure-mMIMO. As stated, the algorithm achieves both security enhancement and PAPR reduction simultaneously. The algorithm steps are shown in Tab. **Algorithm 1**.

The received signal for Bob, a single terminal, remains identical to (3.7). This is because, similar to the random AN, the AN is also constrained to the null space of the main channel and is therefore transparent to Bob. The received signal at the eavesdropper is expressed as follows:

$$\boldsymbol{y}_{e_2} = \sqrt{\frac{\theta}{\psi}}\mathbf{H}_e\mathbf{F}\boldsymbol{s} + \sqrt{\frac{1-\theta}{\xi}}\mathbf{H}_e\frac{\ddot{\boldsymbol{\omega}}}{\sigma_{\ddot{\omega}}} + \boldsymbol{n}_e, \tag{3.30}$$

where $\ddot{\boldsymbol{\omega}}$ is the PAPR-aware AN designed by the algorithm. Now the PAPR of the signal when the PAPR-aware AN is injected will be significantly lower than the PAPR when random AN is injected.

Algorithm 1 PAPR-Aware-Secure-mMIMO

Initialization: $\boldsymbol{\omega} = 0_{N_t \times 1}$, $\boldsymbol{z} = 0_{N_t \times 1}$, $\ddot{\boldsymbol{\omega}} = 0_{N_t \times 1}$, $\boldsymbol{\upsilon}_0 = \sqrt{\frac{1}{\psi}}\mathbf{F}\boldsymbol{s}$, $\mathcal{L}_\omega = 2\sigma^2_{max}(\mathbf{V})$
for ℓ = 0,...,L-1 **do**
  $\lambda_\ell = \mathbb{E}[|\boldsymbol{\upsilon}_\ell|^2] \times \text{PAPR}_0$
  $|\boldsymbol{z}_\ell| = [|\boldsymbol{\upsilon}_\ell| - \sqrt{\lambda}_\ell]^+$
  $\text{phase}(\boldsymbol{z}_\ell) = \text{phase}(\boldsymbol{\upsilon}_\ell)$
  $p^\ell = \frac{\sum|\mathbf{V}\boldsymbol{\omega}_\ell||\boldsymbol{z}_\ell|}{\sum|\mathbf{V}\boldsymbol{\omega}_\ell|^2}$
  $\boldsymbol{\omega}_{\ell+1} = \boldsymbol{\omega}_\ell - \frac{2}{\mathcal{L}_\omega}\mathbf{V}^\dagger(\mathbf{V}\boldsymbol{\omega}_\ell - \boldsymbol{z}_\ell)$
  $\boldsymbol{\upsilon}_{\ell+1} = \boldsymbol{\upsilon}_\ell + p_\ell\mathbf{V}\boldsymbol{\omega}_{\ell+1}$
  $\ddot{\boldsymbol{\omega}}_{\ell+1} = \ddot{\boldsymbol{\omega}}_\ell + p_\ell\mathbf{V}\boldsymbol{\omega}_{\ell+1}$
  if ℓ == L-1 **then**
    $\ddot{\boldsymbol{x}} = \sqrt{\frac{\theta}{\psi}}\mathbf{F}\boldsymbol{s} + \sqrt{\frac{(1-\theta)}{\xi}}\mathbf{V}\frac{\ddot{\omega}}{\sigma_{\ddot{\omega}}}$
  end if
end for
return $\ddot{\boldsymbol{x}}$

The PAPR expression is seen below and the results are validated through simulations in the next section,

The main channel capacity remains the same as (3.10) since this AN remains transparent to Bob and has no impact on the main channel. Also, by normalization of the PAPR-aware AN, $\ddot{\boldsymbol{\omega}}$, and respecting the equal power allocation condition described in (3.12), the wiretap channel capacity will remain the same as when we inject a random AN. Hence, the equal power allocation condition is fulfilled for the PAPR reducing AN when

$$\psi\sigma_s^2 + \xi\sigma_{\ddot{\omega}}^2 = P. \tag{3.31}$$

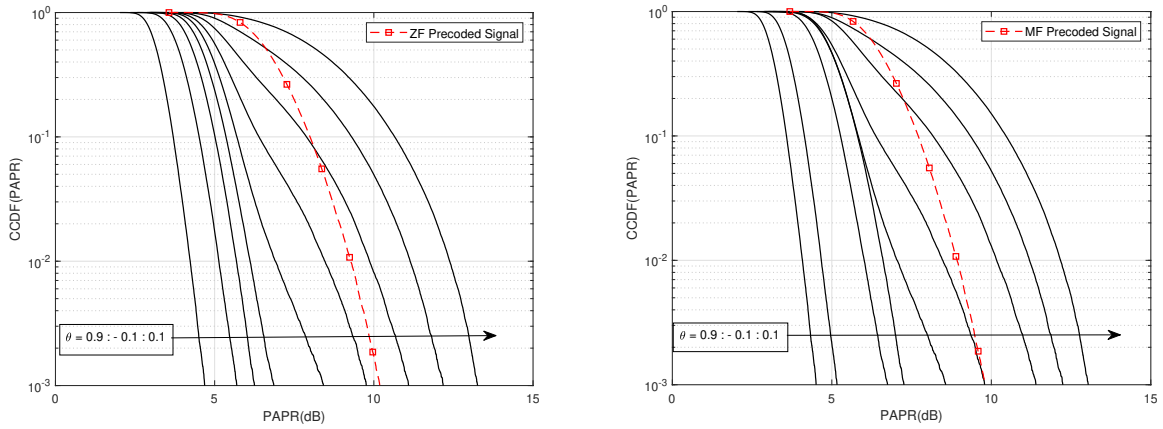
Intuitively, we expect the secrecy capacities to be the same since the covariances of the random AN and PAPR-aware AN are the same. In essence, the secrecy gain due to AN injection remains the same,

$$C_{s_2} = C_{s_1}. \tag{3.32}$$

3.7 Performance of PAPR-Aware-Secure-mMIMO under Uncorrelated Rayleigh Fading

In this section, we present the simulation results for the proposed PAPR-Aware-Secure-mMIMO scheme for security enhancement and PAPR reduction. In all simulations, 40 iterations of the algorithm are carried out for every channel realization. We consider $N_t = 70$ antennas at the BS (Alice), $N_r = 10$ single antenna legitimate receivers while Bob is 1 out of the 10, and $N_{r,e}$ =10 cooperative eavesdropper antennas. We use the Complementary Cumulative Distribution Function (CCDF) to evaluate the PAPR reduction performance, which denotes the probability that the PAPR of the estimated signal exceeds a given threshold.

3.7.1 Optimal Power Allocation



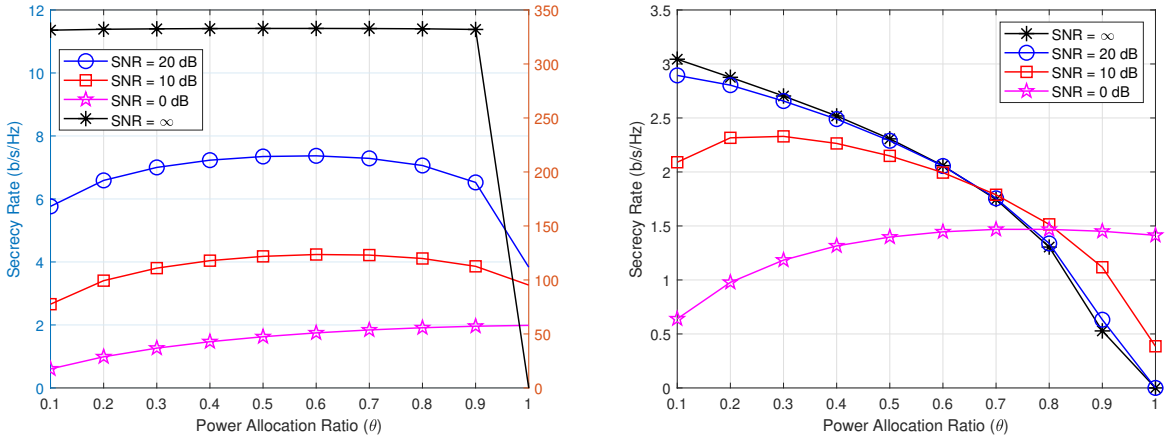
(a) Zero-Forcing.

(b) Matched Filter.

Figure 3.3: PAPR performance w.r.t. power allocation ratio: $\theta = 0.9$ corresponds to the leftmost curve and $\theta = 0.1$ corresponds to the rightmost curve.

To know the optimal power allocation for the PAPR-Aware-Secure-mMIMO scheme, we will consider its impact on PAPR and secrecy capacity performances. In Fig 3.3, we see the impact of θ on the PAPR performance. There is a trade-off between the attained PAPR and the percentage of the power allocated to AN. Note that $\theta \in]0, 1]$ where $\theta = 1$ corresponds to ZF/MF precoding case without AN injection. When $\theta = 0$, the useful signal is null and there is no need to design a PAPR-aware AN. As more power is allocated to the AN (i.e., with θ decrease), the PAPR significantly increases. We observe that when too much power is allocated to the AN, the algorithm is no longer effective,

resulting in a PAPR equal to or greater than the PAPR without AN injection (ZF/MF precoding only). In fact, we observe a very high PAPR of up to 13.3 dB when $\theta = 0.1$ and it can be deduced that the high PAPR is the combined effect of the PAPR increase due to both massive MIMO precoding and AN injection. As less power is allocated to the PAPR-aware AN, we observe a constant decrease in the attained PAPR and we obtain a 4.6 dB PAPR when $\theta = 0.9$ for ZF precoding and 6.50 dB PAPR when $\theta = 0.6$ for MF precoding.



(a) Zero-Forcing.

(b) Matched Filter.

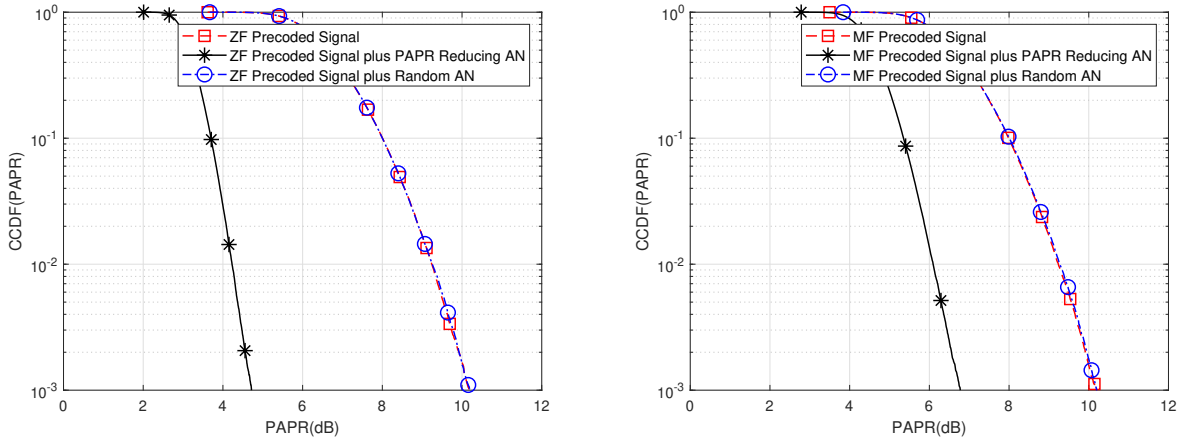
Figure 3.4: Secrecy capacity performance of the proposed AN-aided scheme compared to the power allocation ratio (θ) at different SNR regimes.

The next step in proposing an optimal θ is to study its effect on the secrecy capacity of the system as shown in Fig. 3.4. Different SNR regimes are considered: low SNR ($\overline{\gamma} = 0$ dB), medium SNR ($\overline{\gamma} =$ 10 dB), high SNR ($\overline{\gamma} = 20$ dB), and very high SNR ($\overline{\gamma} = \infty$) regimes. For both precoding schemes, in the low SNR regime, the secrecy capacity increases as more power is allocated to the useful signal. This is evident from the fact that the secrecy capacity is significantly affected by the thermal noise in this region. For the higher SNR regions with ZF precoding (Fig. 3.4a), the secrecy capacity becomes higher reaching its maximum values when θ is between 0.5 and 0.6. This approximately corresponds to equal power allocation between the useful signal and the AN. However, when $\theta = 0.9$, the secrecy capacity is only slightly lower than the maximum value but the PAPR at a CCDF of 0.1% is lowest at this point. Hence, $\theta = 0.9$ is an optimal power allocation ratio for ZF precoding. [1]. Note that the left side of the y-axis in Fig. 3.4a is for the $\overline{\gamma} = 0, 10,$ and $20dB$ while the right y-axis scale is for $\overline{\gamma} = \infty$.

[1]This is an argument for an optimal ratio that is derived numerically and not a mathematical optimal point

On the other hand in Fig. 3.4b, for the three higher SNR regions with MF precoding, we observe negative slopes for all three. As more power is allocated to the useful signal, the secrecy capacity decreases. This indicates that AN injection is necessary for the higher SNR regimes because without AN, the capacity of the single antenna Bob will be more affected by the MUI than the capacity of the cooperative eavesdropper. However, we must pay attention to allocating an optimal power ratio to the AN since an increase in the AN power leads to an increase in PAPR. Therefore, the simulation shows that a choice of θ=0.6 is an optimal allocation ratio for the PAPR-Aware-Secure-mMIMO scheme with MF precoding [2]. At a CCDF of 0.1%, we obtain a PAPR of 6.5 dB and a secrecy capacity greater than 2 bps/Hz in higher SNR regimes ($\overline{\gamma}$ = 10, 20, and ∞ dB).

3.7.2 Achieved PAPR, Secrecy Capacity and Symbol Error Rate Performances



(a) Zero-Forcing.

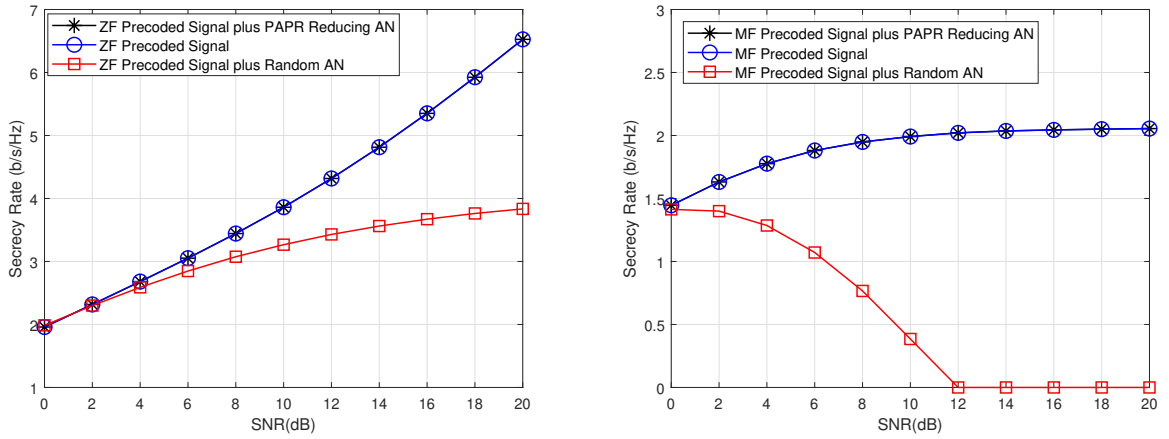
(b) Matched Filter.

Figure 3.5: CCDFs of the PAPR of the proposed AN-aided scheme compared with signal with random AN and signal without added AN.

In Fig. 3.5, we compare the PAPR of the transmit signal using our algorithm to the PAPR of the transmit signal when a random AN is employed. The simulation was carried out at the optimal power allocation ratios θ = 0.9 and 0.6 for ZF and MF precoding respectively as proposed in Section 3.7.1. It can be seen that our algorithm provides a substantial PAPR reduction (shown by the solid line) compared to the PAPR for the signal with ZF/MF precoding only and the signal with random AN injection, shown by the dash and dash-dot lines respectively in Fig. 3.5. At CCDF of 0.1%, we observe a gain of 4.6 dB/6.5 dB for ZF/MF precoding respectively. Another point to note is that even without

[2]Also, this is an argument for an optimal ratio that is derived numerically and not a mathematical optimal point

AN injection, massive MIMO has a high PAPR due to the precoding schemes. We observe that with these simulation parameters, the random AN, which is also known for its high PAPR challenges, does not accentuate the PAPR in the massive MIMO scheme. This is evident from the fact that the PAPR for both the precoding scheme without any AN injection and the scheme with random AN injection is 10.1 dB at a CCDF of 0.1%. This implies that the high PAPR is due to the massive MIMO precoding and is not accentuated by the AN injection.



(a) Zero-Forcing at $\theta = 0.9$.

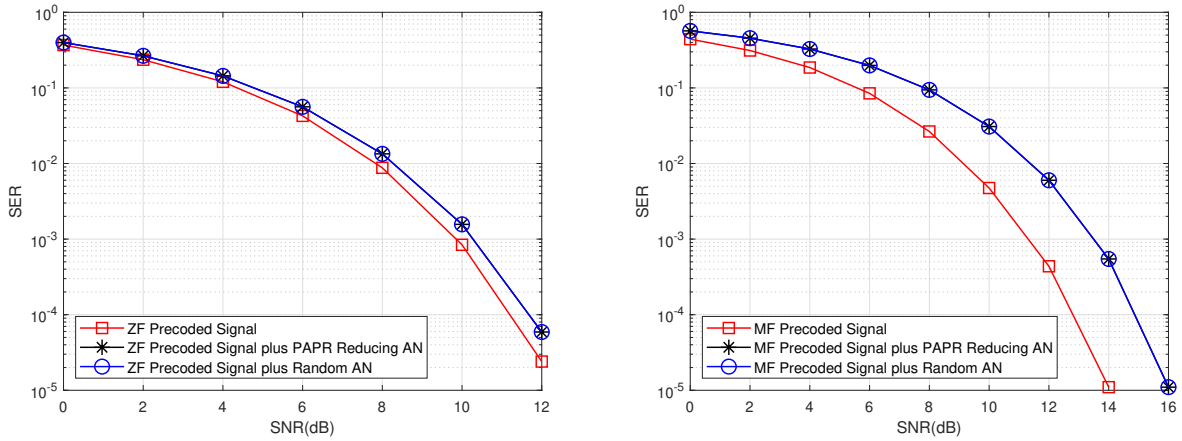
(b) Matched Filter at $\theta = 0.6$.

Figure 3.6: Secrecy capacity performance of the proposed AN-aided scheme compared to the capacity with random AN injection and no AN injection

In Fig. 3.6, the secrecy capacity performance of the AN-aided scheme is plotted against the average SNR. We assume the same average SNR for Bob and Eve. With 70 BS antennas and a power allocation ratio θ=0.9/0.6 for ZF and MF precoding respectively, we consider the capacity of a single legitimate terminal out of 10 legitimate users and the capacity of a cooperative Eve consisting of 10 receive antennas. For Eve, we look at the capacity in relation to a single transmitted symbol received. We can observe in Fig. 3.6a that when we transmit the ZF-precoded signal without any AN injection, the secrecy capacity is 2 b/s/Hz at SNR = 0 dB. With the increase in SNR, this rate slightly grows to reach a limit of 4 b/s/Hz. This is in agreement with the work done in [18] where the authors showed that considering a single terminal, the secure transmission may be limited in massive MIMO with passive eavesdropping if the number of eavesdropper antennas is too large. However, with the injection of AN, the transmission scheme provides a continuous enhancement of the achievable secrecy capacity as the SNR increases. In essence, the secrecy capacity C_s becomes larger since C_e is limited by the variance of the AN in a high SNR regime while C_b keeps rising. Note that the plots have been simulated with

the assumption of the same SNR at Bob and Eve, a condition that is not necessarily always true in practical scenarios. It is possible that Eve has a positional advantage over Bob and therefore a better SNR. In essence, the injection of the AN technique remains a useful security technique for massive MIMO. However, this secrecy capacity is the same for both cases when we inject random AN as in legacy AN works and when we inject our proposed PAPR reducing AN. This is the benefit of our proposed scheme, as we obtain the secrecy offered by legacy AN schemes but with a reduced PAPR, thereby making this less expensive and more feasible for practical deployments.

Similarly, for MF precoded signal transmitted with AN in Fig. 3.6b, the secrecy capacity starts at 1.5 b/s/Hz in the low SNR region and slowly grows to a steady value of about 2 b/s/Hz at the higher SNR regions. However, without AN Injection, there is a sharp roll off in the secrecy capacity and secrecy is completely lost from 12 dB average SNR. This is the effect of the MUI in the higher SNR regions which leads to the single antenna Bob having a lower capacity than the 10 antenna cooperative antenna Eve.



(a) Zero-Forcing at $\theta = 0.9$.

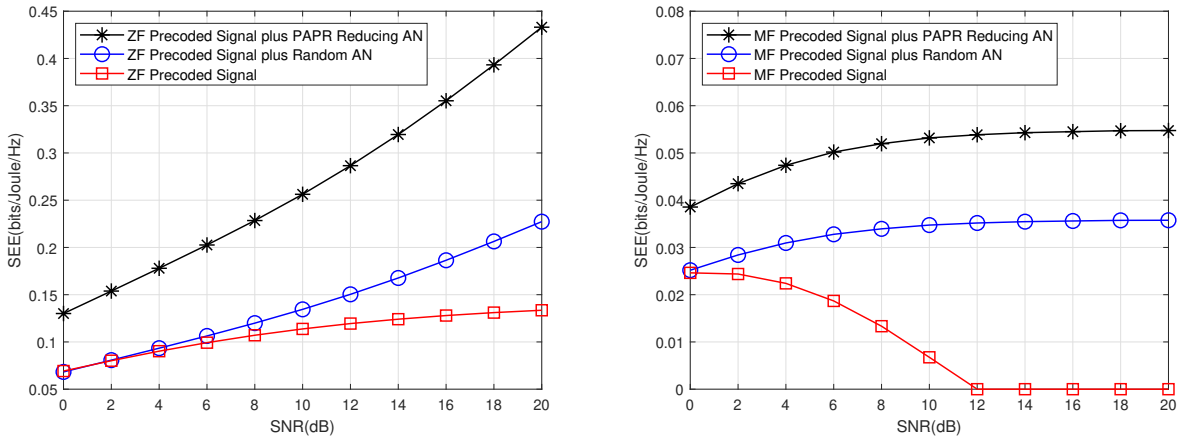
(b) Matched Filter at $\theta = 0.6$.

Figure 3.7: Symbol error rate performance for 16 QAM constellation size with power allocation ratio.

In Fig. 3.7, we analyze the Symbol Error Rate (SER) performance of the proposed scheme in comparison to the cases when random AN is injected and when no AN is injected using the 16-QAM constellation size. For ZF precoding at a power allocation ratio of $\theta = 0.9$, it can be observed that at an SER value of 10^{-4}, there is about 0.5 dB of SNR loss for our scheme, compared to the ZF precoding without any AN injection scheme. Expectedly, the SER performance is the same in our scheme and for the scheme with random AN injection. It is obvious that the added signal related to

PAPR reduction and secrecy does not affect the quality of transmission. For MF precoding at a power allocation ratio of $\theta = 0.6$, at the SER value of 10^{-4}, there is about 2 dB of SNR loss for our scheme, compared to the MF precoding without any AN injection scheme. Similarly, the SER performance is the same for our scheme and the scheme with random AN injection. This is expected since the variance of the ANs is the same for both. We can conclude that the 2 dB loss in SNR in this case is acceptable in transmission quality for the gains in energy efficiency and secrecy.

3.7.3 Energy Efficiency Gain



(a) Zero-Forcing at $\theta = 0.9$.

(b) Matched Filter at $\theta = 0.6$.

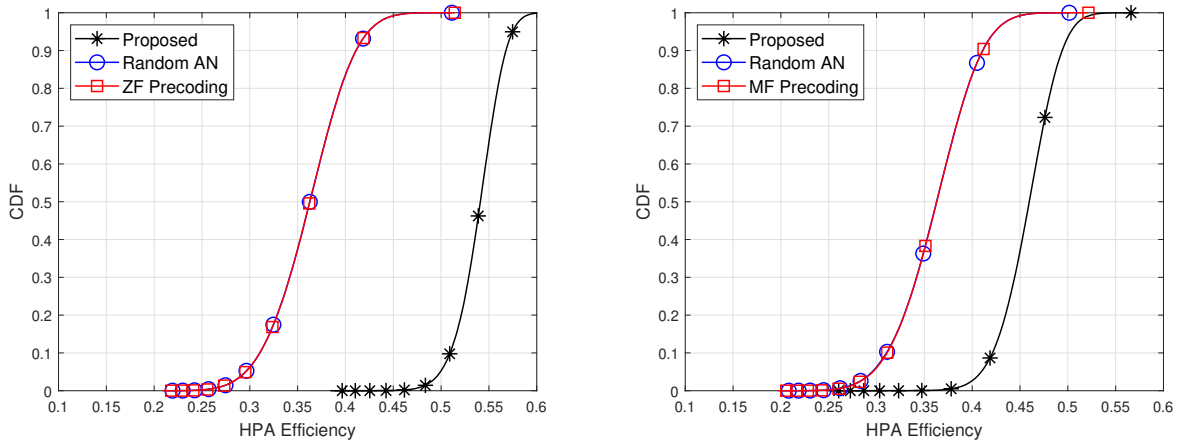
Figure 3.8: Secrecy energy efficiency performance of the proposed AN-aided scheme compared to the capacity with random AN injection and no AN injection

Our proposed schemes with a PAPR of 4.6 dB/6.5 dB for ZF/MF precoding will have HPAs with better efficiencies than legacy schemes with a PAPR of 10.1 dB. Thus, for our proposed schemes and the legacy schemes to achieve complete linearity, we introduce IBOs of -4.6 dB/-6.5 dB and -10.1dB respectively[3]. This is based on the PAPR values at a CCDF of 0.1% as shown in Fig. 3.3. The choice of a level of 0.1% implies that after introducing the IBO, 99.9% of the signal will lie in the linear region of the HPA. It has been shown in [19] that 100mW/200mW per antenna is an optimal transmit power in massive MIMO downlink using ZF/MF precoding. It is evident from (3.19) and (3.16) that as the IBO increases, the HPA efficiency decreases leading to higher total power consumption. Consuming higher power for the same secrecy capacity leads to lower SEE. Hence, we observe in Fig. 3.8, that

[3]It is important to note that equations (3.10), (3.14), and (3.15) are only valid when the transmit signal is linearly amplified by the HPA

our proposed scheme shows the highest SEE performance, outperforming the schemes with or without AN injection. For the ZF precoding option in Fig. 3.8a, the SEE gain of the proposed scheme is significantly highest and has a positive slope as the average SNR increases. The scheme with random AN injection slightly outperforms the scheme without AN injection. This is owing to both consuming the same energy but the former having a higher secrecy capacity.

In Fig. 3.8b, we observe that for the MF precoding option, the SEE performance for the proposed scheme increases to the highest steady value as the average SNR increases. Next, the scheme with random AN injection outperforms the scheme without any AN injection. For the latter, the SEE goes to zero from 12 dB. This indicates that the secrecy capacity in the higher SNR regimes for this scheme is zero because the MUI limits the single antenna Bob more than the cooperative eavesdropper. Massive MIMO schemes combat this by increasing the number of transmit antennas but the scope of this work is limited to a massive MIMO system with 70 BS antennas only.



(a) Zero-Forcing at $\theta = 0.9$.

(b) Matched Filter at $\theta = 0.6$.

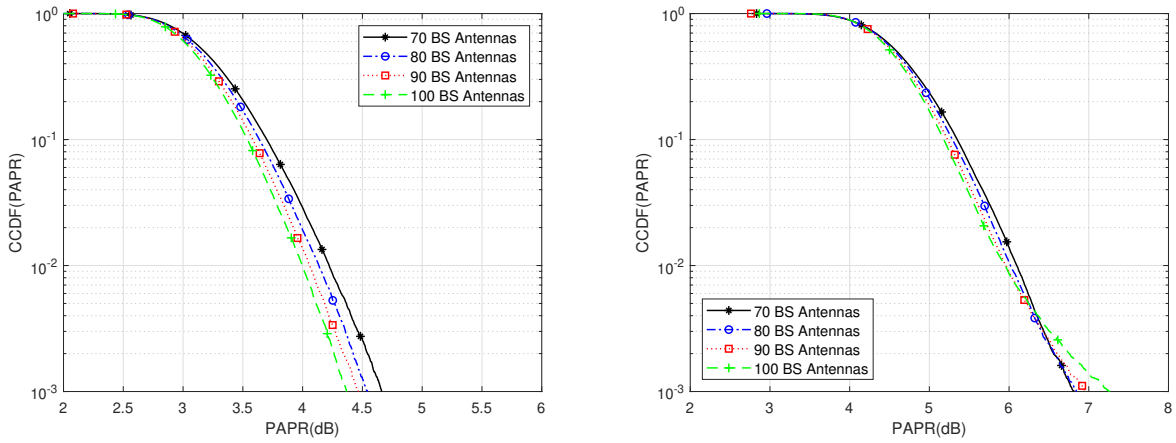
Figure 3.9: CDFs of the HPA efficiency of the proposed AN-aided scheme.

In Fig. 3.9, we compare the cumulative distribution function (CDF) of the HPA efficiencies for PAPR-Aware-Secure-mMIMO with the legacy schemes. In this simulation we adopted class B HPAs with efficiency exponent, $\beta = 0.5$ and maximal HPA efficiency, $\eta_{max} = 0.78$. The HPA efficiency is inversely proportional to PAPR which means that they are related by a decreasing function. Our proposed scheme with a PAPR of 4.6 dB/6.5 dB for ZF/MF precoding will have HPAs with better efficiency than legacy schemes with a PAPR of 10.1 dB. For ZF precoding, the range of HPA efficiencies goes from 0.4 when the PAPR is 4.6 dB at a CCDF of 0.1% to values as high as 0.6 when the CCDF is

1. This corresponds to about 78% of the maximum HPA efficiency. When MF precoding is adopted, the range of HPA efficiencies goes from 0.3 when the PAPR is 6.5 dB at a CCDF of 0.1% to values as high as 0.57 when the CCDF is 1. In contrast, the HPA efficiency is much lower for the scheme with random AN and the scheme without any AN injection. Evidently, by adopting our proposed scheme, we can improve the energy consumption efficiency of our HPA.

3.7.4 Further Studies on Sensitivity of PAPR Performance of PAPR-Aware-Secure-mMIMO

For a more robust study, we analyze the PAPR performance of the proposed PAPR-Aware-Secure-mMIMO scheme w.r.t. other transmission parameters. First we consider the sensitivity of the scheme to the number of transmit antennas. This is followed by an analysis w.r.t. the PAPR target in the algorithm.



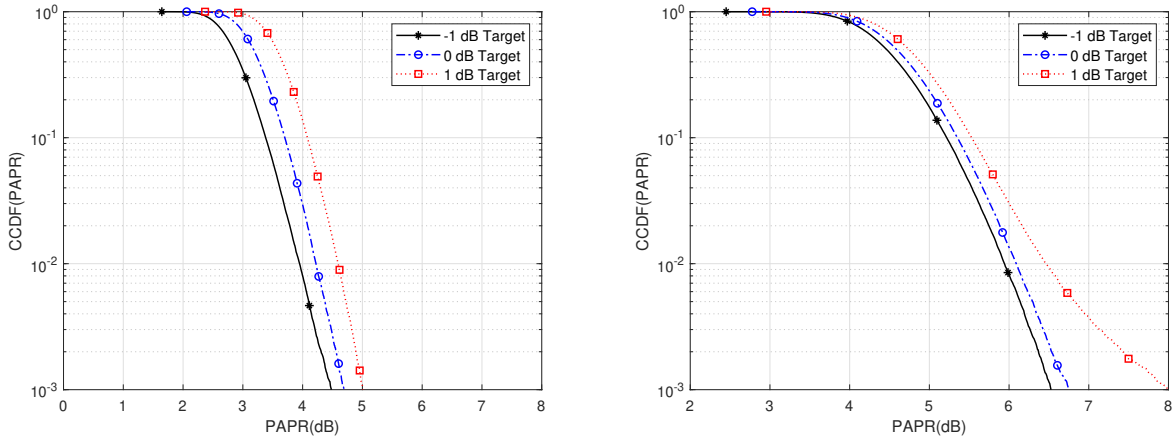
(a) Zero-Forcing.

(b) Matched Filter.

Figure 3.10: PAPR gain performance of the proposed AN-aided scheme w.r.t. the number of BS antennas.

The impact of the number of transmit antennas N_t on the PAPR reduction gain is analyzed in Fig. 3.10. We consider the range of $N_t \in [70, 100]$, $N_r = 10$ and $\theta = 0.9/0.6$ for ZF/MF precoding respectively. For ZF precoding, we observe that for a fixed number of legitimate users, the PAPR gain shows marginal improvement (less than 0.3 dB) when the number of BS antennas goes from 70 to 100. The PAPR performance is even less sensitive to the change in the number of transmit antennas when MF precoding is adopted. However, it is worth using more BS antennas if the number of legitimate terminals becomes higher.

Fig. 3.11 shows the performance of the proposed algorithm w.r.t. various target PAPR levels. For



(a) Zero-Forcing at $\theta = 0.9$..

(b) Matched Filter at $\theta = 0.6$.

Figure 3.11: Comparison of the CCDF of the PAPR of proposed AN-aidded scheme for different PAPR targets.

ZF precoding, we observe that for a target PAPR of -1 dB, we achieve a PAPR of 4.4 dB that is 5.4 dB higher than the target PAPR. When the target is 1 dB, the achieved PAPR is 5 dB which is 4 dB above the target. Similarly for MF precoding, the PAPR performance is closer to target as the target value increases. Consequently, we can conclude that the algorithm is more effective when the target PAPR is less strict.

3.8 Effect of Spatial Correlation on PAPR-Secure-mMIMO

Of major significance is the impact of spatial correlation on the performance of massive MIMO systems. A fading channel is considered spatially uncorrelated if the channel gains and direction are independent random variables, and the channel direction is uniformly distributed over the unit-sphere [69]. This is at best an ideal assumption because practical channels are usually spatially correlated. This is also known as space-selective fading [103]. The antennas have a non-uniform radiation pattern and due to this irregularity in the propagation environment, higher power levels are received from some spatial directions more than other directions [104]. There are different approaches to modeling the spatial correlated propagation. We have adopted the Local Scattering Spatial Correlation Model in this work [105]. In light of these, in this thesis work, we study the performance of PAPR-Aware-Secure-mMIMO under correlated Rayleigh fading conditions. We consider both ZF and MF linear precoding methods. Performance analysis is also done in terms of SEE, HPA efficiency, PAPR, secrecy capacity,

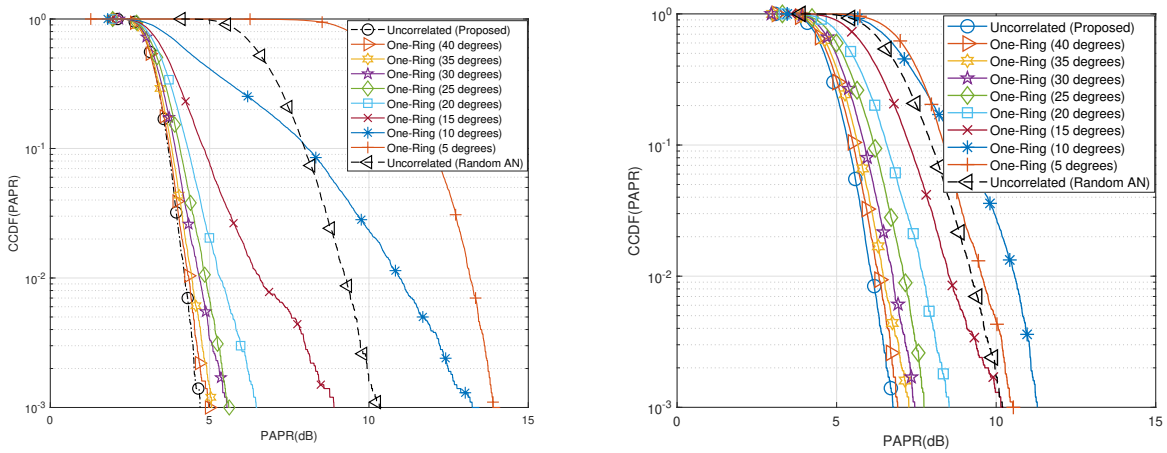
and SER. We study the impact of correlation on these performance metrics. The degree of correlation is evaluated in terms of Angular Standard deviation (ASD).

The main channel, $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$, is modeled as a correlated Rayleigh flat fading channel, and each channel vector for each receiver follows $\mathbf{h} \rightarrow \mathcal{N}_{\mathbb{C}}(\mathbf{0}_{N_t}, \mathbf{R})$, where $\mathbf{R} \in \mathbb{C}^{N_t \times N_t}$ is the channel correlation matrix which is a Toeplitz matrix. Uncorrelated Rayleigh Fading is a special case when $\mathbf{R}$ is a scaled identity matrix, i.e. $\mathbf{R} = \aleph \mathbf{I}_{N_t}$. In that case, all diagonal elements are equal and all non-diagonal elements are zero. There is no dominant spatial directivity. It is assumed that the wiretap channel, $\mathbf{H}_e \in \mathbb{C}^{N_{r,e} \times N_t}$, is unknown to Alice but experiences identical spatial correlation like the main channel. We suppose that the BS is elevated such that there is no scattering in its near field but there is a localized scattering around the receivers. In essence, all multipath components are due to this scattering and $\bar{\varphi}$ represents the angle of an arbitrary multipath component. Note that $\bar{\varphi} = \varphi + \delta$, where φ is the deterministic nominal angle and δ is the random deviation from the nominal angle with ASD represented as σ_φ. We assume that the deviations are uniformly distributed $\delta \sim \mathcal{U}[-\sqrt{3}\sigma_\varphi, \sqrt{3}\sigma_\varphi]$. This is referred to in the literature as one-ring local scattering model. All scatterers are assumed to lie on a circle centered at the receiver terminal.

3.9 Performance Analysis for Correlated Rayleigh Fading

In this section, we present the simulation results for the proposed PAPR-Aware-Secure-mMIMO scheme under correlated Rayleigh fading. The nominal angle, $\varphi = 30°$, and angular standard deviation $\sigma_\varphi \in [5°, 40°]$. In all simulations, 40 iterations of the algorithm are carried out for every correlated channel realization. We consider $N_t = 70$ antennas at the BS (Alice), $N_r = 10$ legitimate receivers while Bob is 1 out of the 10, and $N_{r,e} = 10$ cooperative eavesdropper antennas.

In Fig 3.12, we study the effect of different values of σ_φ on the PAPR performance of the PAPR-Aware-Secure-mMIMO algorithm under correlated Rayleigh fading. For the considered range, the correlation is highest when $\sigma_\varphi = 5°$ and lowest when $\sigma_\varphi = 40°$. This is also compared to the cases of uncorrelated fading when our proposed PAPR-Aware AN or random AN is injected. For ZF and MF precoding, the PAPR is lowest when there is no spatial correlation. As the magnitude of correlation increases, the PAPR increases. The scheme with ZF precoding is significantly more sensitive to the correlation as we observed a PAPR of 4.6 dB at a CCDF of 0.1% without correlation and a PAPR as

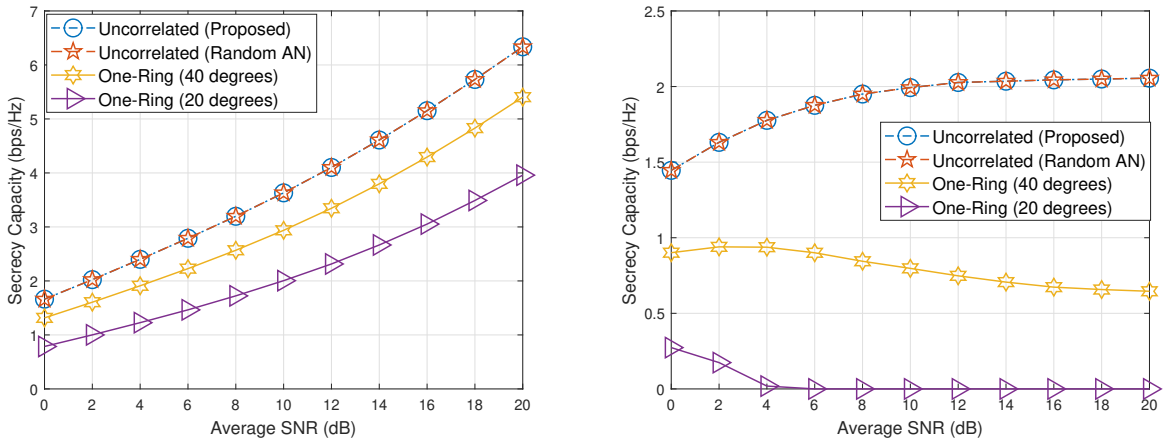


(a) Zero-Forcing at $\theta = 0.9$.

(b) Matched Filter at $\theta = 0.6$.

Figure 3.12: PAPR performance w.r.t. degree of correlation: leftmost curve shows uncorrelation and the rightmost curve shows maximum correlation with $\sigma_\varphi = 5°$.

high as 14 dB with a strong correlation of $\sigma_\varphi = 5°$. The range is reduced with MF precoding. For both precoding schemes, the PAPR performance when the correlation is high ($\sigma_\varphi = 5°\&10°$) is worse than the PAPR performance for random AN injection with uncorrelated fading.



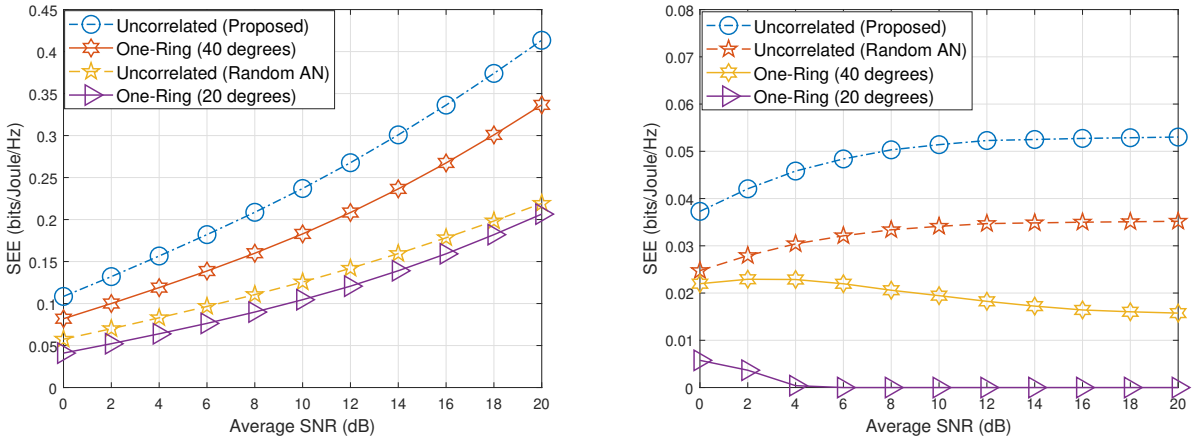
(a) Zero-Forcing at $\theta = 0.9$.

(b) Matched Filter at $\theta = 0.6$.

Figure 3.13: Secrecy capacity performance w.r.t. degree of correlation.

To study the secrecy capacity performance as seen in Fig. 3.13, we consider the same average SNR at Bob and Eve. For emphasis, we restate that Bob is one out of the 10 legitimate receivers while Eve is represented by the 10 cooperative single antenna terminals. As expected, the secrecy capacity is the same for uncorrelated fading when the proposed PAPR-Aware AN or random AN is injected.

We consider two ASDs of $\sigma_\varphi = 20°\&40°$. For both precoding schemes, the secrecy capacity reduces as the correlation level increases. However, the ZF precoding option maintained a positive slope as the average SNR increased. There is a complete loss of secrecy in the MF precoding option at an average SNR of 4 dB when $\sigma_\varphi = 20°$. Our scheme with MF precoding is more sensitive to channel correlation than when ZF precoding is adopted.



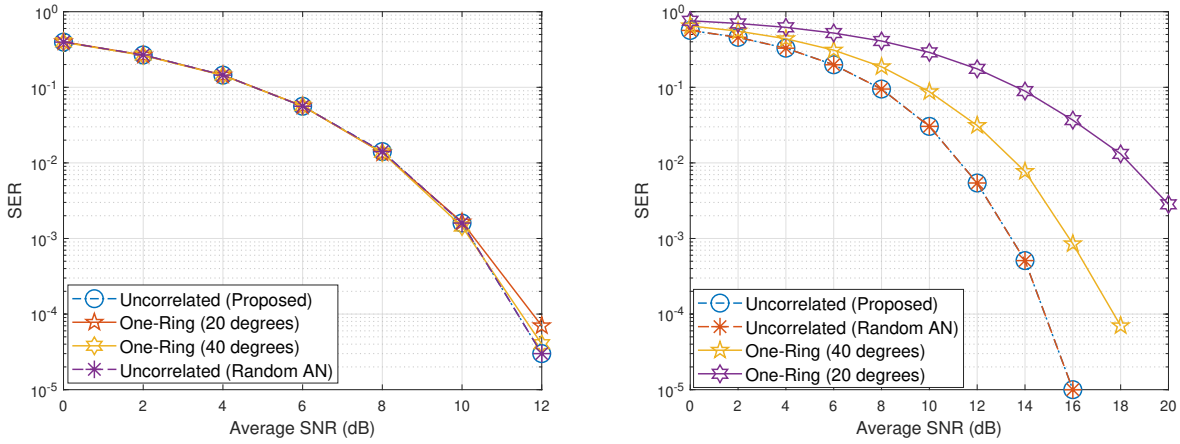
(a) Zero-Forcing at $\theta = 0.9$.

(b) Matched Filter at $\theta = 0.6$.

Figure 3.14: SEE performance w.r.t. degree of correlation.

It is important to restate that the secrecy capacity performance in Fig. 3.13 is only achievable when the transmit signal is linearly amplified by the HPA. This linearity is possible by introducing a back-off of the same magnitude as the PAPR. Our proposed scheme with a PAPR of 4.6 dB and 6.5 dB for ZF and MF precoding with uncorrelated fading respectively will have HPAs with better efficiency than legacy schemes with a PAPR of 10.1 dB. Similarly, as seen in Fig. 3.12, correlation increases the PAPR performance and that reduces the efficiency of the HPA. Thus, to achieve complete linearity, we introduce IBOs equivalent to the PAPR performances. As correlation increases, secrecy capacity decreases PAPR increases, HPA efficiency decreases, and thus SEE decreases. At $\sigma_\varphi = 20°$, the scheme with random AN has a slightly better SEE. MF precoding in Fig. 3.14b shows smaller absolute SEE values but similar performance variations, with the uncorrelated fading of our proposed scheme having the highest SEE and the SEE reducing with correlation increase.

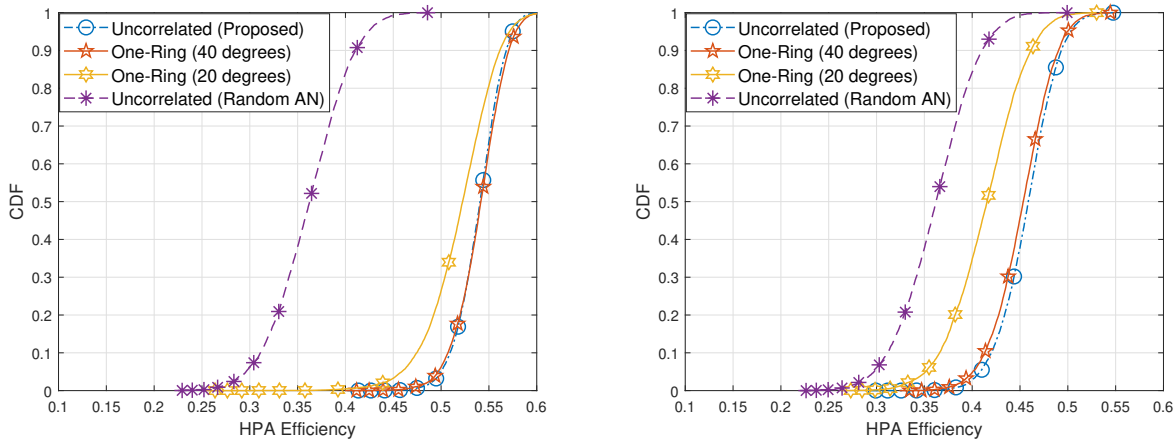
The fourth metric studied is the SER. In Fig. 3.15, we compare the SER performance of the proposed algorithm with various correlation levels and when random AN is injected. 16-QAM constellation size is considered and $\theta = 0.9$ and 0.6 for ZF and MF precoding respectively. The SER with



(a) Zero-Forcing (b) Matched Filter

Figure 3.15: SER performance w.r.t. degree of correlation.

ZF precoding is approximately the same in all cases. This further demonstrates the MUI cancellation in ZF precoding. It is not sensitive to the correlation. For MF precoding, at SER value of 10^{-3}, there is about 2 dB of SNR loss for our scheme without correlation compared to when there is a correlation of $\sigma_\varphi = 40°$. This SER loss increases as the correlation increases.



(a) Zero-Forcing (b) Matched Filter

Figure 3.16: CDFs of the HPA efficiency of the proposed AN-aided scheme with correlated Rayleigh fading.

In Fig. 3.16, we study the effect of correlation on the CDF of the HPA efficiencies for PAPR-Aware-Secure-mMIMO. In this simulation we adopted class B HPAs with efficiency exponent, $\beta = 0.5$ and maximal HPA efficiency, $\eta_{max} = 0.78$. The HPA efficiency is inversely proportional to PAPR which means that they are related by a decreasing function. Intuitively, for ZF precoding, HPA efficiency

is highest without correlation with a range from 0.4 when the PAPR is 4.6 dB at a CCDF of 0.1% to values as high as 0.6 when the CCDF is 1. For MF precoding with a PAPR of 6.5 dB, the range of HPA efficiencies goes from 0.3 when the PAPR is 6.5 dB at a CCDF of 0.1% to values as high as 0.57 when the CCDF is 1. In contrast, the HPA efficiency is much lower for the scheme with random AN. The efficiency is 0.2 when the PAPR is 10.1 dB at CCDF of 0.1% and has peak values of 0.45 at CCDF of 1. As the correlation increases the HPA efficiency decreases.

3.10 Conclusion

In this chapter, we studied an important category of PLS that focuses on the use of AN injection for security and its impact on energy efficiency. A method to design a PAPR-aware AN that significantly reduces PAPR and enhances security in a massive MIMO downlink transmission was proposed as a convex optimization problem. This optimization was solved by an iterative online algorithm, referred to as PAPR-Aware-Secure-mMIMO, that makes use of instantaneous information using the GD approach. The proposed transmission scheme is easy to implement and offers a solution to the high PAPR challenge in massive MIMO. A study of the PAPR, secrecy capacity, and SER performances of the scheme in relation to the power allocation ratio (θ) showed that an optimal point is achieved when θ = 0.9/0.6 for ZF/MF precoding respectively. It implies allocating 90%/60% of the available power to the useful signal and the remaining 10%/40% to the AN.

In the next chapter, we study another category of PLS techniques referred to as channel adaptation techniques in Section 2.2.4 and the impact of imperfect CSI on the PLS performance metrics. We considered flat fading in this chapter but in the next, we move on to consider the case of frequency selective fading.

3.11 Appendix

3.11.1 The proof that the Frobenius norm of the ZF precoder (3.1 on page 39) is as given in (3.3 on page 40)

$\mathbf{F} = \mathbf{H}^{\dagger}(\mathbf{H}\mathbf{H}^{\dagger})^{-1}$

$\mathbf{F}^{\dagger} = (\mathbf{H}\mathbf{H}^{\dagger})^{-1}\mathbf{H}$

$\|\mathbf{F}\|_F^2 = \mathrm{Tr}(\mathbf{F}^{\dagger}\mathbf{F})$

$$\|\mathbf{F}\|_F^2 = \mathrm{Tr}\left[(\mathbf{H}\mathbf{H}^\dagger)^{-1}\mathbf{H}\mathbf{H}^\dagger(\mathbf{H}\mathbf{H}^\dagger)^{-1}\right]$$

$$\|\mathbf{F}\|_F^2 = \mathrm{Tr}\left[(\mathbf{H}\mathbf{H}^\dagger)^{-1}\right]$$

Using the derivations of the expectation of trace of complex inverse Wishart matrices as shown in [106, 107] $\|\mathbf{F}\|_F^2 = \frac{N_r}{N_t - N_r}$.

3.11.2 The proof that the normalization of the null space matrix (3.4 on page 40) is as given in (3.6 on page 40)

$$\mathbf{V} = \mathbf{I}_{N_t} - \mathbf{H}^\dagger(\mathbf{H}\mathbf{H}^\dagger)^{-1}\mathbf{H}$$

$$\|\mathbf{V}\|_F^2 = \mathrm{Tr}(\mathbf{V}\mathbf{V}^\dagger)$$

$$\|\mathbf{V}\|_F^2 = \mathrm{Tr}(\mathbf{I}_{N_t} - \mathbf{H}^\dagger(\mathbf{H}\mathbf{H}^\dagger)^{-1}\mathbf{H})$$

$$\|\mathbf{V}\|_F^2 = \mathrm{Tr}(\mathbf{I}_{N_t} - (\mathbf{H}\mathbf{H}^\dagger)(\mathbf{H}\mathbf{H}^\dagger)^{-1})$$

$$\|\mathbf{V}\|_F^2 = \mathrm{Tr}(\mathbf{I}_{N_t}) - \mathrm{Tr}(\mathbf{I}_{N_r})$$

$$\|\mathbf{V}\|_F^2 = N_t - N_r.$$

Chapter 4

Frequency Diversity in Physical Layer Security

Contenu

4.1 Introduction

In this chapter, we begin by proposing a PLS scheme that combines MF precoding and frequency diversity in an OFDM transmission scheme. The goal in this scheme is to degrade the performance of the eavesdropper while keeping the performance of Bob as expected. To achieve secure communication in the presence of an eavesdropper, the adaptive MF precoder ensures that only Bob maintains the diversity gain provided by repetition scheme. Since the eavesdropped signals are precoded using the legitimate user's CSI, Eve will lose the diversity gain and experience a higher BER and lower channel

capacity than Bob. This degradation of Eve compared to Bob guarantees secure communication in the presence of Eve as Bob can decode transmitted symbols at a higher SNR compared to Eve. Repetition scheme is adopted to provide diversity gain to Bob but the MF precoder ensures that Eve loses the diversity gain. The security gap between Bob and Eve is measured in terms of BER and secrecy capacity. This study is done under FDD and TDD modes. In FDD mode, there is CSI feedback between Alice and Bob and this CSI leaks to Eve. In this mode, we assume that Eve is passive but fully aware of the CSI of the wiretap and main channels. This is the worst case for security. Channel reciprocity is adopted in TDD mode and Eve only carries out blind equalization. We summarize our major contributions in this chapter as follows:

- We study the use of adaptive MF precoding in a single-antenna multi-carrier transmission mode, combined with repetition diversity. Numerical results show the BER and secrecy capacity performance improvement of the proposed schemes over legacy denoising schemes.
- We provide an analysis of this imperfect CSI on the security performance of the system. We derive the expressions for the received signals, conditional secrecy capacity and conditional QPSK BER for Bob and Eve under imperfect CSI conditions. These derivations are verified numerically and theoretically.
- We propose a DAE model referred to as DenoiseSecNet. This model accepts noisy CSI as input and gives denoised CSI that are nearly accurate estimates of the noiseless CSI. We propose a hybrid model (HybDenoiseSecNet) that combines a conventional denoising scheme with a shallow DAE. This achieved the same performance as DenoiseSecNet but at a much-reduced complexity. We also show the significant reduction in complexity of our proposed scheme compared to another neural network scheme in the literature.

4.2 Physical Layer Security through Diversity and Precoding

4.2.1 System Model

We consider an OFDM transmission with N subcarriers operating in FDD mode. The entries of the main channel between Alice and bob, $\boldsymbol{h}^{(b)}$, are i.i.d. Rayleigh fading zero-mean complex Gaussian variables with unit variance. The same applies to the wiretap channel between Alice and Eve, $\boldsymbol{h}^{(e)}$.

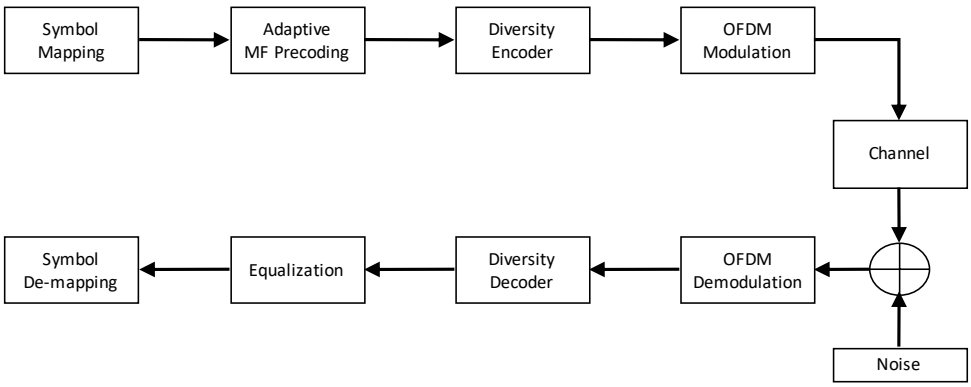


Figure 4.1: OFDM system model employing diversity and adaptive PLS technique.

For every pair of uncorrelated subcarrier in the same OFDM block ($h_{n_1}^{(b)}$ and $h_{n2}^{(b)}$), Alice transmits MF precoded symbols x_{n_1} and x_{n_2} to Bob. To ensure the uncorrelation between subcarrier pairs, all pairs are chosen as follows:

$$h|_{n_1,n_2} = \begin{cases} h_{n_1}, & \text{where } 1 \leq n_1 \leq N/2, \\ h_{n_2}, & \text{where } n_2 = n_1 + N/2. \end{cases} \tag{4.1}$$

The instantaneous CSI of the main channel is used to design the precoder which maximizes SNR in the direction of Bob only. Frequency diversity is also added to improve reliability. The end-to-end transmission steps are shown in Fig. 4.1.

Eve is aware of the main channel CSI due to CSI feedback in FDD mode. Bob and Eve are located at separate locations. Hence, their channels exhibit uncorrelated propagation in a rich scattering environment [20]. This ensures that the intercepted transmit MF precoded signal is not optimal for Eve. It loses the diversity gain because the precoding was done with a CSI uncorrelated to its own. This provides secrecy and error gain for Bob over Eve.

For each pair of subcarriers, the received signals at Bob are such that

$$y_{n_1}^{(b)} = h_{n_1}^{(b)} x_{n_1} + z_{n_1}^{(b)}, \tag{4.2}$$

$$y_{n_2}^{(b)} = h_{n_2}^{(b)} x_{n_2} + z_{n_2}^{(b)}, \tag{4.3}$$

where $z_{n_1}^{(b)} \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_{n_1}^2)$ and $z_{n_2}^{(b)} \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_{n_2}^2)$ are the complex AWGN component at the intended receiver.

The received signals at Eve are expressed as

$$y_{n_1}^{(e)} = h_{n_1}^{(e)} x_{n_1} + z_{n_1}^{(e)}, \tag{4.4}$$

$$y_{n_2}^{(e)} = h_{n_2}^{(e)} x_{n_2} + z_{n_2}^{(e)}. \tag{4.5}$$

Similarly, $z_{n_1}^{(e)} \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_{n_1}^2)$ and $z_{n_2}^{(e)} \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_{n_2}^2)$ are the complex AWGN component at the eavesdropper.

The MF-precoded signals are expressed as

$$x_{n_1} = P_{n_1} s, \quad x_{n_2} = P_{n_2} s \tag{4.6}$$

where

$$P_{n_1} = \frac{\sqrt{2} h_{n_1}^{(b)^*}}{\sqrt{|h_{n_1}^{(b)}|^2 + |h_{n_2}^{(b)}|^2}}, \quad P_{n_2} = \frac{\sqrt{2} h_{n_2}^{(b)^*}}{\sqrt{|h_{n_1}^{(b)}|^2 + |h_{n_2}^{(b)}|^2}}. \tag{4.7}$$

By substituting (4.6) and (4.7) in (4.3) and simply summing the received signals on the two uncorrelated subcarriers, the received signal at Bob can be written as

$$\tilde{s}^{(b_1)} = \sqrt{2(|h_{n_1}^{(b)}|^2 + |h_{n_2}^{(b)}|^2)} s + z_{n_1}^{(b)} + z_{n_2}^{(b)}. \tag{4.8}$$

From (4.8), the instantaneous signal to noise ratio (SNR) at Bob is given as

$$\gamma^{(b_1)} = (|h_{n_1}^{(b)}|^2 + |h_{n_2}^{(b)}|^2) \bar{\gamma}, \tag{4.9}$$

where $\bar{\gamma}$ is the average SNR at the receiver.

The calculation of the BER for QPSK constellation is readily available in the literature when the decision variables are Gaussian random variables [21]

$$\mathrm{BER}(\mathrm{SNR}) = \frac{1}{2} \mathrm{erfc}\left(\sqrt{\frac{\mathrm{SNR}}{2}} \right) \tag{4.10}$$

Therefore, by conditioning on the set of variables h_{n_1} and h_{n_2}, we can obtain the conditional QPSK error probability corresponding the subcarrier pair at Bob

$$\mathrm{BER}^{(\mathrm{b}_1)}\big|_{h_{n_1}^{(b)}, h_{n_2}^{(b)}} = \frac{1}{2} \mathrm{erfc}\left(\sqrt{\frac{\gamma^{(\mathrm{b}_1)}}{2}} \right), \tag{4.11}$$

The final BER is obtained by averaging the conditional BER on the variables h_{n_1} h_{n_2} for all subcarrier pairs in N.

Similarly, when the CSI is perfect, the received signal at Eve, the instantaneous SNR and conditional QPSK BER can be respectively written as

$$\tilde{s}^{(e_1)} = \sqrt{2}\left(\frac{h_{n_1}^{(e)}h_{n_1}^{(b)^*} + h_{n_2}^{(e)}h_{n_2}^{(b)^*}}{\sqrt{(|h_{n_1}^{(b)}|^2 + |h_{n_2}^{(b)}|^2)}}\right)s + z_{n_1}^{(e)} + z_{n_2}^{(e)}. \tag{4.12}$$

$$\gamma^{(e_1)} = \left(\frac{\alpha\alpha^*}{|h_{n_1}^{(b)}|^2 + |h_{n_2}^{(b)}|^2}\right)\bar{\gamma} \tag{4.13}$$

$$\mathrm{BER}^{(\mathrm{e}_1)}\Big|_{h_{n_1}^{(e)},h_{n_2}^{(e)}} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\gamma^{(\mathrm{e}_1)}}{2}}\right), \tag{4.14}$$

where

$$\alpha = h_{n_1}^{(e)}h_{n_1}^{(b)^*} + h_{n_2}^{(e)}h_{n_2}^{(b)^*} \tag{4.15}$$

Secrecy capacity is the positive difference between the main channel capacity and eavesdropper's channel capacity [6]. A positive value means secrecy is achievable and a zero implies there is no secrecy guarantee. We measure secrecy capacity in bps/Hz (or bits/channel use). Similar to the BER performance, the final secrecy capacity is obtained by averaging the conditional ones on the variables h_{n_1} h_{n_2} for all subcarrier pairs in N. The conditional channel capacities of Bob and Eve and the conditional secrecy capacity are respectively expressed as

$$\mathrm{C}^{(\mathrm{b}_1)}\Big|_{h_{n_1}^{(b)},h_{n_2}^{(b)}} = \frac{1}{2}\log_2(1+\gamma^{(b_1)}), \tag{4.16}$$

$$\mathrm{C}^{(\mathrm{e}_1)}\Big|_{h_{n_1}^{(e)},h_{n_2}^{(e)}} = \frac{1}{2}\log_2(1+\gamma(e_1)), \tag{4.17}$$

$$\mathrm{C}_{\mathrm{s}}^{(1)}\Big|_{h_{n_1}^{(b)},h_{n_2}^{(b)},h_{n_1}^{(e)},h_{n_2}^{(e)}} = [\mathrm{C}^{(\mathrm{b}_1)} - \mathrm{C}^{(\mathrm{e}_1)}]^+ \tag{4.18}$$

The factor of half in (4.16) and (4.17) is because only half of the available bandwidth is used for the transmission. For N available subcarriers, N/2 unique symbols are transmitted.

4.2.2 Performance Analysis with Perfect CSI

In this section, we present the BER and secrecy capacity performances of our proposed PLS scheme. We adopt an OFDM system with a total of $N = 64$ subcarriers. The symbols are QPSK modulated. For a fair comparison, we compare the BER and secrecy capacity performances of Bob and Eve under the assumptions of the same average SNR at both of them. Due to spatial decorrelation and rich scattering, the main channel and wiretap channel are uncorrelated. BER is a Quality of Service (QoS) related metric that can also be used to analyse the security of a system. The channel with higher BER is less secure and more degraded compared to the channel with lower BER under similar conditions and the same information signal. The difference in the BER is a measure of the security gap in the system [4]. The Vehicular A model corresponding to a highly frequency selective radio environment with power delay profiles (PDPs) described in Table 4.1 is considered. From Table 4.1, the coherence bandwidth, calculated as the inverse of multipath delay spread, is 2.7MHz [108]. From (4.1), this means there is a gap of 5MHz between subcarrier pairs and compared to a coherence bandwidth of 2.7MHz, uncorrelation between subcarriers is guaranteed. We present the numerical and theoretical results.

Table 4.1: PDP for Vehicular-A with 10MHz bandwidth: τ = delay spread and σ_t^2 = power

$\tau[ns]$	0	300	700	1100	1700	2500
$\sigma_t^2[dB]$	0	-1	-9	-10	-15	-20

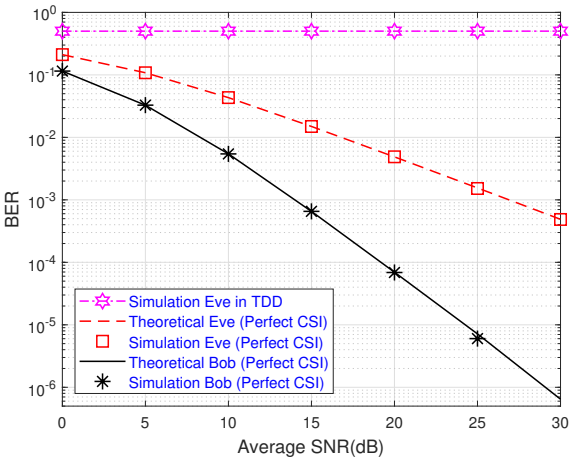


Figure 4.2: BER performance with perfect CSI.

With a perfect CSI as seen in Fig. 4.2, it can be observed that Bob outperforms Eve. Bob

maintains a diversity gain of 2 but Eve loses the diversity gain in FDD mode and is fully degraded in TDD mode. In FDD mode, Eve is aware of the main channel instantaneous CSI and is able to use this instantaneous CSI for equalization. However, since the eavesdropped symbols have been precoded with an uncorrelated CSI, it leads to loss of diversity gain compared to Bob. The higher BER for Eve compared to Bob is an indication of the security gap in the system. In TDD mode, the main channel CSI is not available to Eve, Eve carries out blind equalization and is completely degraded.

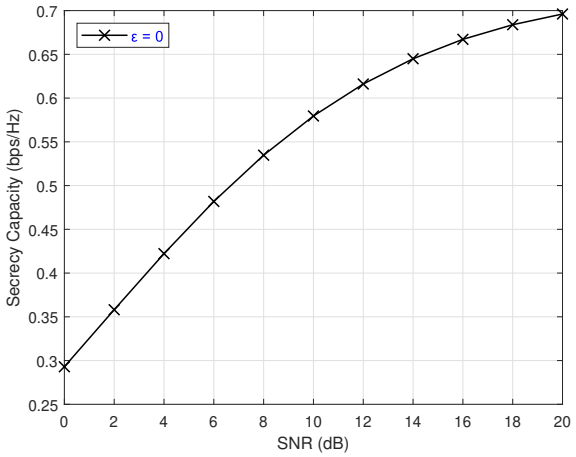


Figure 4.3: Secrecy capacity performance with perfect CSI.

In Fig. 4.3, we see a positively increasing secrecy capacity at all average SNRs. This confirms that the capacity of Bob is higher than Eve's capacity at all SNRs.

4.3 Impact of Imperfect Channel State Information

Studies on the impact of imperfect CSI in different PLS schemes can be seen in [109–113]. The authors in [111] studied secure communications in a Multi-User (MU) massive MIMO system with imperfect CSI due to outdated CSI and channel estimation errors. The obtained results showed a significant reduction in secrecy capacity due to imperfect CSI. In [112], the impact of imperfect CSI in an MU-MIMO system that combines selection transmission at the transmitter and Maximum Ratio Combining (MRC) at the receivers was studied. It was observed that PLS performance in terms of probability of non zero secrecy capacity and secrecy outage probability degrades with a rise in imperfect CSI. In [113], the authors analysed the secrecy performance of a MIMO relay system under imperfect CSI. They concluded that the saturated minimum secrecy outage probability and maximum

secrecy capacity depends on the severity of the imperfect CSI.

To study the impact of imperfect CSI on this adaptive PLS scheme, we assume a noisy analog feedback channel between Alice and Bob. The imperfect CSI has equal estimation noise variance at Alice, Bob and Eve. We model the imperfect CSI on the n-th subcarrier as given in [114]:

$$\boldsymbol{h}^{(b)} = \sqrt{1-\epsilon}\hat{\boldsymbol{h}}^{(b)} + \sqrt{\epsilon}\boldsymbol{\psi}, \tag{4.19}$$

where $\boldsymbol{h}^{(b)}$ is the actual channel gain without errors and $\hat{\boldsymbol{h}}^{(b)}$ is the imperfect channel gain with errors. The estimation error $\boldsymbol{\psi}$ is a zero-mean unit variance complex Gaussian random variable $C\mathcal{N}(0,1)$, The case $\epsilon = 0$ corresponds to the perfect CSI scenario while $\epsilon = 1$ corresponds to completely noisy CSI.

The received signals at Bob under imperfect CSI condition are expressed as

$$\hat{y}_{n_1}^{(b)} = h_{n_1}^{(b)}\hat{x}_{n_1} + z_{n_1}^{(b)}, \quad \hat{y}_{n_2}^{(b)} = h_{n_2}^{(b)}\hat{x}_{n_2} + z_{n_2}^{(b)}. \tag{4.20}$$

where

$$\hat{x}_{n_1} = \hat{P}_{n_1}s, \quad \hat{x}_{n_2} = \hat{P}_{n_2}s \tag{4.21}$$

and $\hat{P}$, the adaptive MF precoder that is designed according to the imperfect instantaneous CSI

$$\hat{P}_{n_1} = \frac{\sqrt{2}\hat{h}_{n_1}^{(b)^*}}{\sqrt{|\hat{h}_{n_1}^{(b)}|^2 + |\hat{h}_{n_2}^{(b)}|^2}}, \quad P_{n_2} = \frac{\sqrt{2}\hat{h}_{n_2}^{(b)^*}}{\sqrt{|\hat{h}_{n_1}^{(b)}|^2 + |\hat{h}_{n_2}^{(b)}|^2}}. \tag{4.22}$$

By substituting (4.19), (4.21) and (4.22) in (4.20), the received signal at Bob is shown in (4.23) below

$$\tilde{s}^{(b_2)} = \sqrt{2(1-\epsilon)\left(|\hat{h}_{n_1}^{(b)}|^2 + |\hat{h}_{n_2}^{(b)}|^2\right)}s + \frac{\sqrt{2\epsilon}(\psi_{n_1}^{(b)}\hat{h}_{n_1}^{(b)^*} + \psi_{n_2}^{(b)}\hat{h}_{n_2}^{(b)^*})}{\sqrt{\left(|\hat{h}_{n_1}^{(b)}|^2 + |\hat{h}_{n_2}^{(b)}|^2\right)}}s + z_{n_1}^{(b)} + z_{n_2}^{(b)}. \tag{4.23}$$

From (4.23), the instantaneous SNR at Bob can be written as

$$\gamma^{(b_2)} = \frac{(1-\epsilon)(|\hat{h}_{n_1}^{(b)}|^2 + |\hat{h}_{n_2}^{(b)}|^2)\bar{\gamma}}{\epsilon\bar{\gamma} + 1}. \tag{4.24}$$

Similar to earlier derivations, the conditional QPSK BER at Bob is given as

$$\mathrm{BER}^{(\mathrm{b}_2)}\Big|_{h_{n_1}^{(b)},h_{n_2}^{(b)}} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\gamma^{(\mathrm{b}_2)}}{2}}\right). \tag{4.25}$$

For asymptotic analysis, we consider the instantaneous SNR with imperfect CSI when $\bar{\gamma} \to \infty$. The asymptotic limit is given as

$$\lim_{\bar{\gamma}\to\infty} \gamma^{(b)} = \frac{(1-\epsilon)}{\epsilon}(|\tilde{h}_{n_1}^{(b)}|^2 + |\tilde{h}_{n_2}^{(b)}|^2). \tag{4.26}$$

The instantaneous SNR in this region is no longer dependent on the average SNR but is now limited by the CSI error variance. The implication of this is an error floor as will be seen in Section 4.3.1.

Following the same convention, the received signal, instantaneous SNR and conditional QPSK BER at Eve are respectively expressed as

$$\tilde{s}^{(e_2)} = \frac{\sqrt{2(1-\epsilon)}(\hat{h}_{n_1}^{(e)}\hat{h}_{n_1}^{(b)^*} + \hat{h}_{n_2}^{(e)}\hat{h}_{n_2}^{(b)^*}) + \sqrt{2\epsilon}(\psi_{n_1}^{(e)}\hat{h}_{n_1}^{(b)^*} + \psi_{n_2}^{(e)}\hat{h}_{n_2}^{(b)^*})}{\sqrt{\left(|\hat{h}_{n_1}^{(b)}|^2 + |\hat{h}_{n_2}^{(b)}|^2\right)}}s + z_{n_1}^{(e)} + z_{n_2}^{(e)} \tag{4.27}$$

$$\gamma^{(e_2)} = \frac{(1-\epsilon)(\beta\beta^*)\bar{\gamma}}{(\epsilon\bar{\gamma}+1)(|\hat{h}_{n_1}^{(b)}|^2 + |\hat{h}_{n_2}^{(b)}|^2)} \tag{4.28}$$

$$\mathrm{BER}^{(\mathrm{e}_2)}\Big|_{h_{n_1}^{(e)},h_{n_2}^{(e)}} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\gamma^{(\mathrm{e}_2)}}{2}}\right), \tag{4.29}$$

where

$$\beta = \hat{h}_{n_1}^{(e)}\hat{h}_{n_1}^{(b)^*} + \hat{h}_{n_2}^{(e)}\hat{h}_{n_2}^{(b)^*} \tag{4.30}$$

In this case, the conditional channel capacities for Bob and Eve and the conditional secrecy capacity can be respectively expressed as

$$\mathrm{C}^{(\mathrm{b}_2)}\Big|_{h_{n_1}^{(b)},h_{n_2}^{(b)}} = \frac{1}{2}\log_2(1+\gamma^{(b_2)}), \tag{4.31}$$

$$\mathrm{C}^{(\mathrm{e}_2)}\Big|_{h_{n_1}^{(e)},h_{n_2}^{(e)}} = \frac{1}{2}\log_2(1+\gamma^{(e_2)}), \tag{4.32}$$

$$\mathrm{C}_{\mathrm{s}}^{(2)}\Big|_{h_{n_1}^{(b)},h_{n_2}^{(b)},h_{n_1}^{(e)},h_{n_2}^{(e)}} = [\mathrm{C}^{(\mathrm{b}_2)} - \mathrm{C}^{(\mathrm{e}_2)}]^{+} \tag{4.33}$$

The system will no longer be optimal for Bob because the precoded symbols do not maximize the SNR anymore as is expected in MF precoding. As this estimation error variance increases, the intersymbol interference increases and Bob loses the diversity gain and thus the security gap over Eve decreases.The effect of this is that Alice precodes the symbol using a noisy CSI and thus the SNR for the legitimate user is no longer maximized.

4.3.1 Performance Analysis with Imperfect CSI Estimation

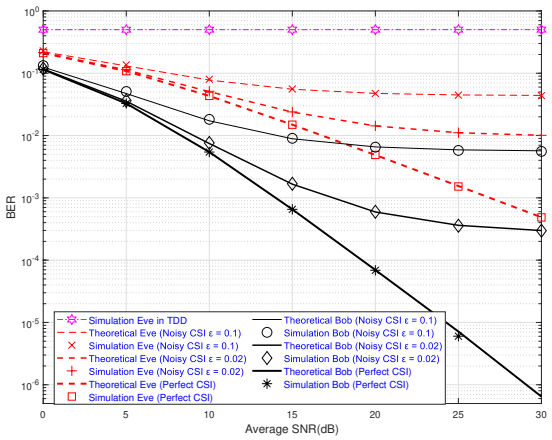


Figure 4.4: BER performance with imperfect CSI.

Next, we look at the impact of imperfect CSI on the BER performance at three CSI error variances (ϵ = [0, 0.02, 0.1]). In Fig. 4.4, when ϵ= 0.02, we observe a slight increase in the BER of Bob and Eve. However, the system is still secure as the gap between Bob and Eve remains significant. As the CSI error variance increases to ϵ = 0.1, the BER significantly increases at both Bob and Eve. Bob completely loses the diversity gain. They both begin to exhibit an error floor around an average SNR of 20dB. The system is highly sensitive to increase in CSI error variance.

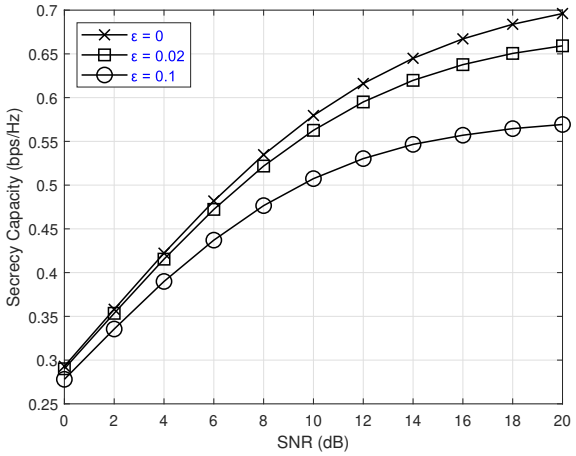


Figure 4.5: Secrecy capacity performance with imperfect CSI.

In Fig. 4.5, we plot the secrecy capacity of the system against the average SNR. As expected, we see that the secrecy capacity is highest when there is no CSI error (ϵ =0), an ideal assumption. However, when the CSI is imperfect, the secrecy capacity reduces as the CSI error variance increases. The higher the magnitude of the variance, the lower the overall secrecy capacity in the system. This is in agreement with the BER performance. At all CSI error variances studied, the secrecy capacity remains positive. This means that although the imperfect CSI causes performance degradation at Bob and Eve, the channel capacity of Bob remains higher than the channel capacity of Eve.

4.4 Denoising Imperfect CSI using Denoising AutoEncoder

Denoising is the process of removing noise from a noisy signal. In [115], the use of the truncation technique to denoise the noisy CSI was presented. In this method, the authors assumed that the channel length is known and only the Channel Impulse Response (CIR) taps below the channel length are considered significant. The CIR is truncated at this point and all other taps beyond this are discarded. It was shown to give a better MSE compared to the no truncation case. More popular is the noisy CSI denoising using the threshold approach. Several works have been done in this area as seen in [116,117]. An iterative threshold method using convolutional code for channel estimation in an OFDM transmission was proposed in [116]. The results showed that higher transmit diversity gains and better BER performances were achieved compared to legacy estimation schemes that are more susceptible to noise. In [117], an efficient time-domain threshold-based channel estimation technique

was proposed in OFDM systems. The threshold, referred to as the universal threshold, can be applied without prior knowledge of the channel statistics and the standard deviation of the noise.

Recently, deep learning has been adopted in many fields such as natural language processing [118], computer vision [119], etc. Similarly, researchers have started working on the use of deep learning for CSI prediction (in the case of outdated CSI [120]) or CSI denoising (in the case of noisy CSI [25,121]). The authors in [25] proposed an autoencoder to reduce CSI feedback in a massive MIMO system operating in FDD mode. The CSI is encoded after CSI estimation and then transmitted as a low-dimensional codeword. At the receiver, the received codeword is decoded to recover the original CSI. A Noise Extraction Unit (NEU) was then used to extract the noise in the codeword. The model predicts the noise and then subtracts the predicted noise from the noisy codeword to get the denoised codeword. This scheme is hereafter referred to as DNNet-NEU.

The conclusion from Section 4.3 is that as the CSI error variance increases, the secrecy capacity reduces and BER significantly increases leading to system degradation. Hence, a neural network denoising algorithm that is employed at the transmitter to denoise the imperfect CSI is introduced. The denoised CSI is then used for the MF precoding and ensures Bob retains the intended security gains over Eve.

4.4.1 Structure and Operation of DenoiseSecNet

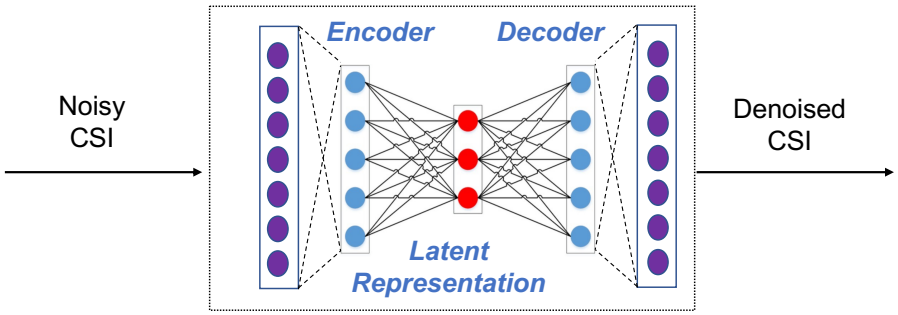


Figure 4.6: Proposed DenoiseSecNet DAE algorithm.

The first part of this section explains the structure and operation of the proposed DenoiseSecNet. In the second subsection, we propose a hybrid version of DenoiseSecNet which is more optimal in terms of performance and computational complexity.

In this work, to denoise the imperfect CSI at the transmitter, we have used the feed-forward

autoencoder of deep learning, a very well-known model in deep learning [22]. DenoiseSecNet is a 5-layer autoencoder block consisting of the input layer, output layer, and 3 hidden layers as shown in Fig. 4.6. We define $f(.)$ and $g(.)$ as the encoder and decoder operations of the autoencoder respectively. In DenoiseSecNet, we define the input as the noisy CSI, $\tilde{\boldsymbol{h}}$. Thus the encoder and decoder outputs will be $f(\tilde{\boldsymbol{h}})$ and $g(f(\tilde{\boldsymbol{h}}))$ respectively. The encoding and decoding operations both take place at Alice. Afterward, the output of the decoding block is used to precode the transmit signal.

Starting from the first hidden layer to the output layer, we have Fully Connected (FC) layers and an activation layer that provides non-linearity to the model. For the ℓ-th layer of the model, the linear activation can be written as:

$$\boldsymbol{m}_\ell = \boldsymbol{W}_\ell \boldsymbol{a}_{\ell-1} + \boldsymbol{b}_\ell, \tag{4.34}$$

where $\boldsymbol{a}_{\ell-1}$ is the activation of the previous $(\ell-1)$-th layer, $\boldsymbol{W}_\ell$ represents the weight of the current ℓ-th layer and $\boldsymbol{b}_\ell$ are the biases for the layer. Note that the noisy CSI is the input for the first layer, i.e. $\boldsymbol{a}_0 = \tilde{\boldsymbol{h}}$.

Next, we introduce non-linearity into the model. This is needed to develop complex representations that can properly model the function. Non-linearity is achieved by the use of AF and the AF of choice is the Parametric Rectified Linear Unit (PReLU). This AF improves model fitting with nearly zero extra computational cost and little overfitting risk [23]. The rationale behind choosing PReLU is explained in Section 4.4.3. PReLU is evaluated as:

$$\phi(m) = \begin{cases} m, & \text{if } m \geq 0, \\ \xi m, & otherwise. \end{cases}, \tag{4.35}$$

where ξ is a learnable parameter. The output of the encoder section of the model, labeled as "Latent Representation" in Fig. 4.6, is given below:

$$f(\tilde{\boldsymbol{h}}) = \phi_\ell(\boldsymbol{W}_\ell(\phi_{\ell-1}(...\phi_1(\boldsymbol{W}_1\tilde{\boldsymbol{h}} + \boldsymbol{b}_1))) + \boldsymbol{b}_\ell), \tag{4.36}$$

where $\phi(.)$ represents the non-linear activation. After encoding, the decoder takes the encoded data and generates an output that is an optimal match of the noiseless version of the noisy input. The decoder section is represented below:

$$g(f(\tilde{\boldsymbol{h}})) = \phi_L(\boldsymbol{W}_L(\phi_{\ell-1}(...\phi_1(\boldsymbol{W}_1 f(\tilde{\boldsymbol{h}}) + \boldsymbol{b}_1))) + \boldsymbol{b}_L). \tag{4.37}$$

To train the model, the hyperparameters were optimized using ray tune [24]. These include the number of layers, the number of nodes per layer, the batch size, and the choice of the AF. The loss, $\mathcal{L}(h, g(f(\tilde{h})))$, is evaluated using MSE loss as:

$$\mathcal{L}(\boldsymbol{h}, g(f(\tilde{\boldsymbol{h}}))) = \frac{1}{N}\sum_{i=1}^{N}\|\hat{\boldsymbol{h}} - \boldsymbol{h}\|_2^2, \tag{4.38}$$

where $\hat{\boldsymbol{h}}$ is the output of the autoencoder. In this paper, MSE is preferred to Mean Absolute Error (MAE) and Mean Squared Logarithmic Error (MSLE) because we want to ensure that the large errors are significantly more penalized than the smaller errors. To optimize the system and iteratively update the parameters accordingly, we used the SGD optimizer. It outperforms other optimizers such as Adam, RMSprop, Adagrad, AdaDelta, etc. in our work.

4.4.2 Hybrid Option of DenoiseSecNet

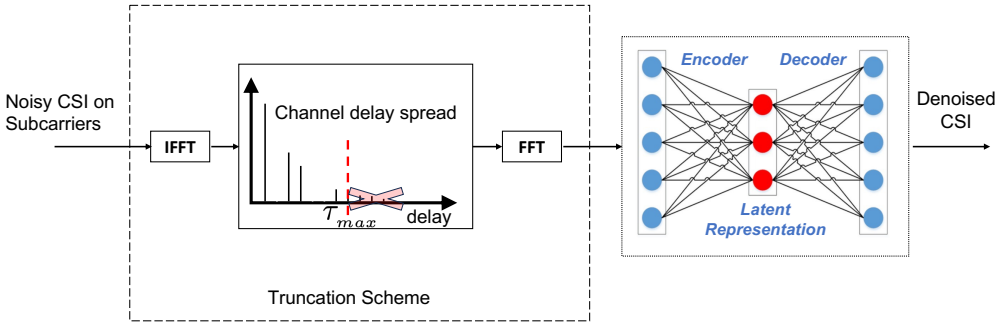


Figure 4.7: Proposed HybDenoisedSecNet DAE algorithm.

For complexity considerations, we propose a hybrid option to denoise the noisy CSI, HybDenoiseSecNet. The major motivation here is to obtain similar BER and secrecy capacity performance gains to DenoiseSecNet but at reduced complexity. To achieve this, the imperfect CSI is first denoised using the legacy scheme, truncation method, mentioned in Section 4.4. We assume that the channel length is known at Alice due to feedback in FDD mode. Assuming N subcarriers and a known channel tap length of T, the noisy CSI feedback ($\tilde{\boldsymbol{h}}$) is first transformed from frequency domain to time domain (TD), as $\tilde{\boldsymbol{h}}^{TD}$, using IFFT operation of size N. The truncation then takes place in the time domain as seen in (4.39).

$$\ddot{h}_t^{TD} = \begin{cases} \tilde{h}_t^{TD}, & \text{if } 0 \le t \le T-1, \\ 0, & \text{if } T \le t \le N. \end{cases}, \tag{4.39}$$

Channel taps beyond the known significant tap of T are assumed to be caused by the noise and are ignored. Then the truncated CSI is transformed to the frequency domain as, $\ddot{\boldsymbol{h}}$, using the FFT. This denoised CSI is then passed through the Artificial Neural Network (ANN) autoencoder for further denoising operation as seen in (4.40). Since already partially denoised, the ANN autoencoder can achieve a significant further reduction in noise with fewer computations as compared to the full option of DenoiseSecNet. In fact, we do not need a deep neural network and a shallow neural network can produce optimal results.

$$g(f(\ddot{\boldsymbol{h}})) = \phi_L(\boldsymbol{W}_L(\phi_{\ell-1}(...\phi_1(\boldsymbol{W}_1 f(\ddot{\boldsymbol{h}}) + \boldsymbol{b}_1))) + \boldsymbol{b}_L). \tag{4.40}$$

The proposed hybrid version is shown in Fig. 4.7. With other hyperparameters remaining similar, the change in the hybrid model is the number of hidden layers and neurons, and thus the model complexity.

4.4.3 Performance Analysis with Denoised CSI

In this section, we present the performance of our proposed DenoiseSecNet and HybDenoiseSecNet and compare them to legacy denoising schemes. We consider an OFDM system with $N = 64$ subcarriers and a QAM constellation. The hidden layers for the full version of DenoiseSecNet are 64-16-64 while the hybrid version has only one 16-neuron hidden layer. The noisy CSI input of 64 subcarriers with 64 complex numbers each is separated into the real and imaginary components at the input and output of the model. Hence, the input and output layers are each 128 in length. The hyperparameters used in the simulation are summarized in Table 4.2. For the DNNet-NEU scheme, we consider the hyperparameters as proposed by the authors in [25].

In Fig. 4.8, the BER of Bob and Eve are plotted against the average SNR for different scenarios. When the CSI is perfect ($\epsilon = 0$), Bob has a diversity gain of 2 but Eve loses the diversity gain. The higher BER at Eve leads to a security gap between Bob and Eve. With a noisy CSI ($\epsilon = 0.1$), the performances of Bob and Eve are completely degraded, and both exhibit error floors from an average SNR of 20 dB as explained in Section 4.3. Evidently, the PLS scheme is highly sensitive to CSI accuracy. We then analyze the BER performance for the proposed autoencoder models (full and hybrid), DNNet-NEU, and two conventional non-neural network denoising schemes; universal threshold and truncation schemes. We observe that the neural network-based schemes outperform

Table 4.2: Hyperparameters

DenoiseSecNet Structure	128-64-16-64-128
HybDenoiseSecNet Structure	128-16-128
DNNet-NEU Structure	128-1024-128
Training Sample Size	7×10^5
Validation Sample Size	2×10^5
Test Sample Size	1×10^5
Batch size	20
Learning rate	0.01
Optimizer	SGD
CSI Error Variance	0.1
Loss Function	MSE

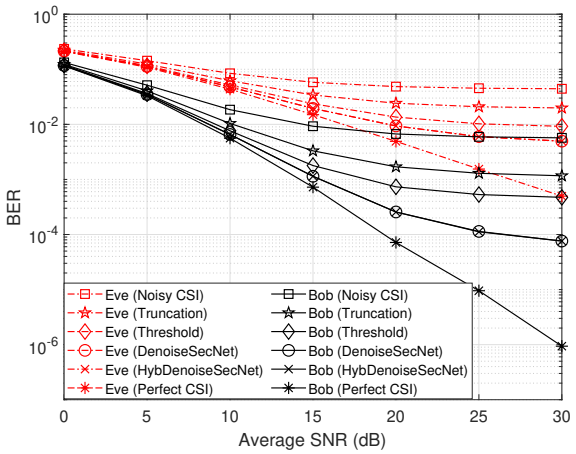


Figure 4.8: BER performance with DenoiseSecNet.

the conventional schemes. Truncation and universal threshold schemes exhibit an error floor of 10^{-3} and 5×10^{-3} respectively around 30 dB average SNR. When DenoiseSecNet, HybDenoiseSecNet, and DNNet-NEU are used to denoise the noisy CSI, we can see a significant enhancement in BER performance. The two proposed models achieve the same level of BER less than 10^{-4} at SNR = 30 dB. The BER performance of DNNet-NEU is approximately the same as that of the proposed models.

In Fig. 4.9, we see the secrecy capacity performance for the schemes. Expectedly, the secrecy capacity is highest under perfect CSI conditions and lowest when the CSI error variance is highest (ϵ = 0.1). The proposed schemes and DNNet-NEU have a secrecy capacity slightly below the best-case scenario. Again, the hybrid and full versions of DenoiseSecNet have the same performance. Next to this is the universal threshold scheme, and the truncation scheme was the least effective CSI denoising scheme. It should be noted that the secrecy capacity was positive in all the cases. This shows that

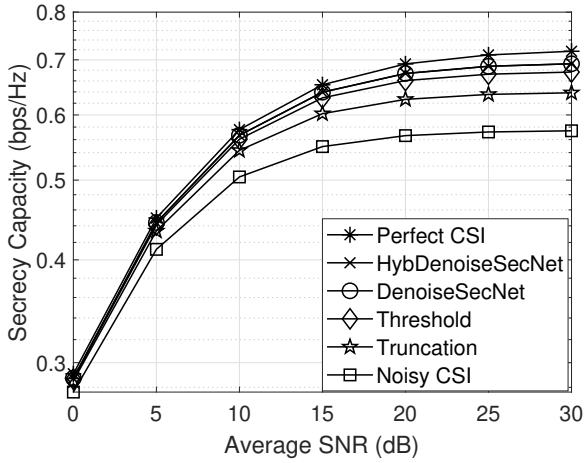


Figure 4.9: Secrecy performance with DenoiseSecNet.

despite the performance degradation due to the noisy CSI, the channel capacity of Bob remains higher than the channel capacity of Eve under similar conditions.

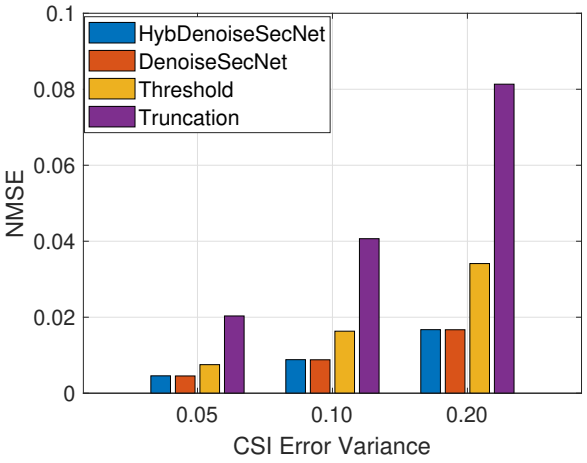


Figure 4.10: NMSE performance with DenoiseSecNet.

The performances of the denoising schemes are compared at three CSI error variance levels ($\epsilon = 0.05$, 0.1, and 0.2) in Fig. 4.10. Again, DenoiseSecNet and its hybrid version had the lowest Normalized Mean Squared Error (NMSE) after denoising. The truncation scheme had the highest NMSE. The schemes remained equally effective in terms of the percentage reduction in error irrespective of the error variance. Compared to the initial CSI error variances, a 91% error reduction was achieved with full and hybrid versions of DenoiseSecNet, while DNNet-NEU, threshold, and truncation schemes achieved 90%, 85%, and 60% reductions respectively.

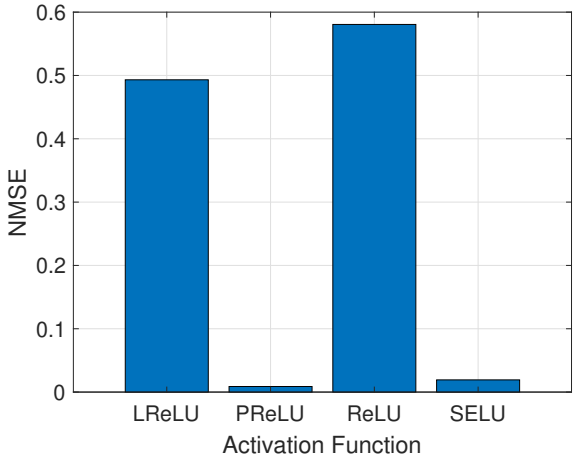


Figure 4.11: NMSE performance with DenoiseSecNet.

Table 4.3: Computational complexity in terms of real-valued operations

Denoising Scheme	**No of Multiplications**	**No of Summations**
Truncation	1,152	1,536
Universal Threshold	1,152	2,304
DenoiseSecNet	18,432	18,432
HybDenoiseSecNet	5,248	5,632
DNNet-NEU	262,144	262,144

We compare the performance of HybDenoiseSecNet at ϵ=0.1 w.r.t. different AFs in Fig. 4.11. We have chosen to use non-saturated AFs that have the advantage of solving the vanishing/exploding gradient problems while improving the convergence speed. Rectified Linear Unit (ReLU) had the highest NMSE, this can be explained by the fact that it only considers the positive part of the linear activation and ignores the negative. The CSI on the other hand has a distribution of positive and negative components. The second-highest NMSE of 0.49 was observed with leaky ReLU. By default, this AF assigns a gradient of 0.01 to the negative component of the linear activation but this does not optimally model our CSI distribution. Scaled Exponential Linear Unit (SELU), a self-normalizing AF suitable for ANNs to enable high-level abstract representation [122] was also considered. Finally, the best performance was observed with PReLU. This is explained by the fact that the AF can learn the gradient for the negative region of the CSI. Hence, it properly captures the entire positive and negative ranges of the CSI.

4.4.4 Computational Analysis

Inspired by [123], the computational complexity analysis is done in terms of the number of real-valued mathematical operations (multiplication/division and summation/subtraction) needed to denoise the noisy CSIs.

For the truncation scheme, most of the complexity is from the IFFT operation before truncation and the FFT operation afterward. It is well known that the complexity of a single FFT operation is $(N/2)\log N$ complex multiplications and $N\log N$ complex summations. A complex multiplication is equivalent to 3 real-valued multiplications and 2 real-valued summations and a complex summation is equivalent to 2 real-valued summations. In essence, for the truncation scheme, the complexity is broken down to $3N\log N$ real-valued multiplications and $4N\log N$ real-valued summations. In the universal threshold denoising scheme, in addition to truncation, we have the two median calculations and signal clipping operations. This introduces an additional $2N\log N$ to make a total of $6N\log N$ real-valued operations [1]

For the neural network schemes, the focus is on the number of real-valued multiplications and summations required to activate all neurons in the hidden and output layers of the network. Moving from the ℓ-th to the $(\ell+1)$-th layer will require $J_\ell J_{\ell+1}$ multiplications/summations for the linear transformation, where J signifies the number of neurons in the layer. The extra operations are the bias summation and vector product in the activation. In summary, the real-valued multiplication and summation in DenoiseSecNet are given as:

$$\mathcal{N}_{MUL} = \mathcal{N}_{SUM} = \sum_{\ell=1}^{L} J_{\ell-1}J_\ell \tag{4.41}$$

Table 4.3 gives a summary of the number of real-valued operations for all the considered denoising schemes. From this table, we see that for both multiplication and summation operations, HybDenoiseSecNet requires only about 30% of the processing resources used by DenoiseSecNet. In other words, the full option uses 3.3 times more resources than the hybrid option. As expected, the hybrid option is more complex than the threshold and truncation schemes but the significant secrecy and BER performance gains are valid motivations to employ this scheme. However, DNNet-NEU requires the most amount of computational complexity and is 14 times the complexity of DenoiseSecNet and 50 times

[1] Recall that median calculation involves sorting and the best sorting algorithms are at $N\log(N)$ complexity.

that of HybDenoiseSecNet. This significant reduction in complexity is what makes HybDenoiseSecNet an interesting alternative.

4.5 Conclusion

In this chapter, we studied the impact of imperfect CSI on a system that combines the popular MF precoding and repetition scheme to provide PLS. Since this scheme depends on instantaneous CSI, imperfect CSI has a significant impact on the secrecy capacity and BER performance of the system. Next, we proposed two denoising autoencoder models (DenoiseSecNet and HybDenoiseSecNet) that are used to denoise the imperfect CSI before applying the adaptive PLS scheme. Through simulations, we showed that our scheme significantly outperforms conventional schemes in terms of BER, secrecy capacity, and NMSE. We also studied the reduced complexity of our proposed schemes compared to another neural network scheme in the literature. An interesting extension of this work will be to consider the multi-antenna scenario and cases where the noise variance is not uniform across subcarriers. In the next chapter, we will consider yet another crucial aspect of PLS that focuses on key-based PLS and channel coding under frequency selective transmission.

Chapter 5

Index Partitioned Modulation

Contenu

5.1 Introduction and Motivations

So far, the contributions in this thesis, like many PLS schemes in the literature, have assumed that the channel inputs are Gaussian distributed. The detection complexity of Gaussian signals is high as it takes a continuum of values. In addition to this, the amplitude of Gaussian signals are unbounded, so Gaussian signaling is typically not used in practice [124]. Typically, the channel inputs in practice are drawn from a discrete signal constellation such as QPSK, QAM, etc. These discrete channel inputs help to maintain moderate peak transmission power and receiver complexity. However, finite-alphabet input constraints have a significant impact on the achievable PLS performance and this impact should be taken into account in designing practical PLS schemes.

We begin by taking a look at related works in the literature that focus on finite-alphabet signaling in OFDM systems. It is well known that the performance of OFDM systems is very sensitive to frequency synchronization errors and that Carrier Frequency Offset (CFO) leads to Inter-Carrier Interference (ICI) [125]. The authors in [126] used this drawback to provide PLS in an OFDM system by exploiting channel reciprocity available in TDD mode. Bob generates a signal with an induced CFO which Alice can estimate and compensate for. The downlink communication is then pre-compensated using the CFO in such a way that Bob receives it without ICI but Eve suffers the ICI and is degraded. This is possible due to channel independence between the main and wiretap channels. In [127], the authors proposed an eavesdropping-resilient OFDM system using sorted subcarrier interleaving. Alice interleaves each subcarrier in each OFDM signal according to the instantaneous CSI of the main channel for a system operating in TDD mode. Since there is no CSI feedback in TDD mode, Bob derives the interleaving pattern initiated by Alice through its local channel estimate, and then de-interleave the received signals. Eve is however unaware of this interleaving pattern and is significantly degraded.

The authors in [128] worked on power allocation and TD AN design for wiretap OFDM with discrete inputs. It was proven that the secrecy capacity of any discrete channel inputs with a finite number of possible values (finite entropy) is a non-concave function w.r.t. the transmit power. A low-complexity power allocation algorithm based on Lagrange dual optimization was then proposed for discrete channel inputs. The temporal DoF provided by CP insertion in OFDM was exploited to insert AN that further enhances security. PLS improvements were shown in terms of mutual information and

secrecy capacity. In [41], a PLS scheme referred to as OFDM with Subcarrier Index Selection (OFDM-SIS) was proposed for safeguarding the transmission of OFDM-based waveforms against eavesdropping in 5G and beyond wireless networks. Subcarrier indices that maximize the SNR at only the legitimate receivers were selected. This is then combined with an adaptive interleaving performed based on the legitimate user's channel that is different from that of the eavesdropper. The numerical results showed PLS improvements in terms of Secrecy Outage Probability (SOP) and BER. Signal space diversity, a technique to increase reliability of detection over fading channels, was explored to provide security in [129]. The in-phase and quadrature components of PSK and QAM constellations are interleaved and sent independently over the main channel which is independent from the wiretap channel. This leads to both security and reliability gains measured in terms of BER security gap.

The work in [130] proposed the combination of two TD ANs in MIMO-OFDM. The first is a conventional AN that takes advantage of the temporal DoF provided by CP insertion and the second is a TD AN which is generated to be canceled out at the legitimate receiver in the frequency domain. The advantage of the scheme is that it does not depend on the spatial DoF that conventional AN methods rely on. The paper [131] studied the information theoretic secrecy capacitys that are achievable in a wiretap OFDM channel when transmitting QAM constellation symbols. The loss with respect to the secrecy capacity obtained with Gaussian distributed inputs was evaluated for both finite constellation cardinalities and in the asymptotic approximation of arbitrarily high cardinality. Bit-loading strategies to efficiently allocate the appropriate number of bits in each subchannel, by considering the two-fold objective of minimizing the loss with respect to the Gaussian input secrecy capacity and minimizing the total bit load was then proposed. Some other works that consider PLS with finite alphabets can be seen in [132–138].

To improve the PLS, we propose in this chapter a new approach referred to as Index Partitioned Modulation (IPM). This modulation partitions the total constellation space used by a main channel into distinct and disjoint subspaces in such a way that it maximizes euclidean distance for the main channel transmission. The index is derived from a dynamic wireless key index that is unique to the legitimate channel. We take advantage of the channel randomness that exists in the temporal and spectral domains to generate keys that are unique to the main channel. Assuming spatial decorrelation between the main and wiretap channels, which implies independent and uncorrelated channel responses, the dynamic index obtained from the wireless key is unavailable to Eve. Hence, Eve will

use all points in the constellation space to decode the transmitted signal, leading to a significantly degraded decoding. In the absence of the index knowledge, the decoding at the Eavesdropper is degraded due to an adequate choice of a bit labelling. This latter guarantees that the Euclidian distance between the images of the same information is maximized and the Hamming distance between the bits labels of neighboring symbols in the whole constellation is at least equal to one.

5.2 Index Partitioned Modulation (IPM): general concept and illustration

In this section, we present our proposed IPM scheme. The wireless wiretap system model is first presented in Subsection 5.2.1. Next, we describe in Subsection 5.2.2 and 5.2.3 the main concepts of noiseless IPM and noisy IPM. Both cases rely on a dynamic index that changes in time and is known at the transmitter and legitimate receiver, but not at the eavesdropper. The generation of this wireless channel dependent dynamic index is presented in 5.2.4. Finally, toy examples illustrating noiseless and noisy IPM concepts are provided in Subsection 5.2.5.

5.2.1 Wireless wiretap channel

We consider a wireless channel in which a transmitter (Alice) transmits normalized 2^q-QAM symbols x_n to a legitimate receiver (Bob) over N subcarriers in a TDD OFDM system with an FFT size of $N_c \geq N$. The transmitted signal are intercepted by an eavesdropper (Eve) situated in the vicinity of the legitimate receiver. However, Bob's channel is independent of Eve, and this can be satisfied when they are separated by at least half a wavelength [20,26]. On each frequency subcarrier $0 \leq n \leq N-1$, the channel coefficients $h_n^{(b)}$ and $h_n^{(e)}$ are computed as the FFT of random tap channel depending on the channel Power Delay Profile (PDP). The received signal at both sides (Bob and Eve) are such that,

$$y_n^{(b)} = h_n^{(b)} x_n + z_n^{(b)}, \tag{5.1}$$

$$y_n^{(e)} = h_n^{(e)} x_n + z_n^{(e)}. \tag{5.2}$$

The transmitted vector at Alice is denoted by $\mathbf{x}$, the received one at Bob by $\mathbf{y}^{(b)}$ and at Eve by $\mathbf{y}^{(e)}$. The random noise $z_n^{(b)}$ and $z_n^{(e)}$ are i.i.d. random Gaussian complex variables $\mathcal{CN}(0,\sigma^2)$ with pdf[1],

$$p(z_n) = p(y_n|h_n,x_n) = \frac{1}{\pi\sigma^2} e^{-\frac{1}{\sigma^2}|y_n - h_n x_n|^2}. \tag{5.3}$$

[1] the subscript $^{(b)}$ and $^{(e)}$ are dropped in (5.3)

To ensure a fair comparison, the PDP representing the signal attenuations σ_t^2 at the delay spreads τ_s, of the channels between Alice $\rightarrow$ Bob and Alice $\rightarrow$ Eve are assumed to be identical. The random tap channel coefficients are generated using the Jakes channel model [26] and are weighted by the corresponding attenuation of a given delay spread. We assume that these coefficients are perfectly known at each receiver side.

5.2.2 General IPM concept

Our proposed IPM scheme is illustrated in Figure 5.1 and consists of partitioning the 2^q-QAM modulation (denoted by Ω_c with $|\Omega_c| = 2^q$) into 2^ℓ multiple disjoint spaces (denoted by $\Lambda_m \subset \Omega_c$, with $1 \leq m \leq 2^\ell$), such that: $\bigcap_m \Lambda_m = \emptyset$, $\bigcup_m \Lambda_m = \Omega_c$ and $|\Lambda_m| = 2^{q-\ell}$. Each sub-space Λ_m is indexed by a channel-based index with length ℓ, shared between Alice and Bob. A given $(q-\ell)$ information bits sequence will have different images in Ω_c depending on the value of the index and will reduce the number information bit per symbol to $(q-\ell)$ rather than q. In the whole space, the symbol bit labeling is performed in such a way that the Euclidean distance between neighboring symbols of a given partition is maximized. Indeed, it should guarantee that the Euclidean distance between image of the information bit sequence is maximized. At Alice, the shared index will dictate the reduced sub-space Λ_m in which the 2^q-QAM symbol lies. Based on this index, Bob decodes the noisy QAM symbol in Λ_m with more distant neighboring symbols than Ω_c. As Eve is not aware of the shared channel-dependent index between Alice and Bob, Eve decodes the noisy QAM symbol in the whole space Ω_c with less distant neighboring symbols than Λ_m, which induces low mutual information. This IPM scheme is hereafter referred to as noiseless IPM.

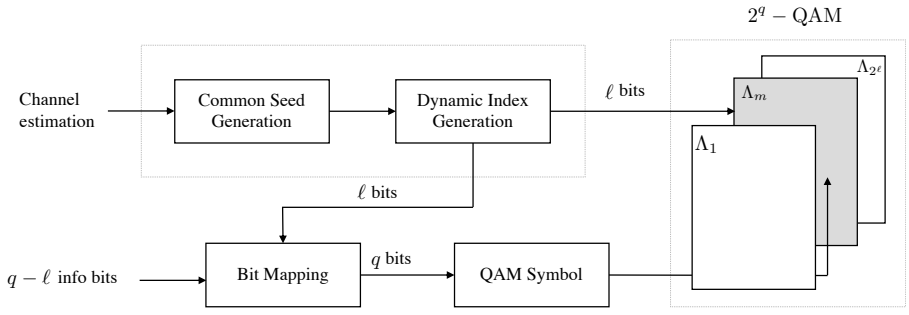


Figure 5.1: Index partitioned modulation

5.2.3 Noisy IPM

In the high SNR regime, the Euclidean distances between neighboring points are relatively large in both lattices Λ_m or Ω_c. In this case, the secrecy gain becomes non-significant as the noisy symbols become distinguishable at Bob as well as at Eve. In order to induce more confusion at the eavesdropper, we propose to inject a random uniform AN into the QAM symbol generated by the IPM. This is performed by adding the generated AN to the QAM symbol while conserving the total power at Alice, it is referred to as noisy IPM. The probability distribution function (pdf) of this random uniform AN will be further discussed in Subsection 5.2.5.2.

5.2.4 Dynamic shared index generation

IPM relies essentially on a dynamic index that indicates, for Alice and Bob, in which partition the QAM symbol lies. This index should change dynamically in each subcarrier to guarantee that it is not intercepted at the eavesdropper. To perform this, a common seed $0 \leq \alpha_0 \leq 1$ is generated at the beginning of the transmission based on the impulse response of the TDD channel between Alice and Bob. The key establishment technique based on channel reciprocity-based has been widely investigated in literature aiming to generate a shared key at Alice and Bob [66]. The key generation will not be addressed in this paper and we refer the reader to [139] for more information. To generate the dynamic key, we use the chaotic sequence [140] that critically depends on its initial value and the μ-value with $\mu \in [0, 4]$. Note that the chaotic behavior of the sequence depends on the initial of μ that should be such that $\mu > 3.85$. The main steps of the dynamic key generation are illustrated in Algorithm2. A quantization of the channel between Alice and Bob is required to generate this common seed over a large number bits, to say 128 bits or 256 bits as in [141]. We assume that this common seed is not available at Eve, and that 2^{128} or 2^{256} trials are required to know the exact initial seed. Moreover, this common seed is not sent on the wireless interface, and a congruential pseudo-random number generator is used to generate a bit corresponding to each real number generated by the chaotic sequence (line 7 in Algorithm 2). This operation is not reversible and it will not be possible to find the values of α_n in the algorithm from the index k_n. Using a numerical simulation, we have shown that this chaotic-sequence algorithm provides an equal probability to generate a bit equal to 1 or 0.

Algorithm 2 Generation of dynamic index

Require: At each subcarrier n, the length of the index ℓ

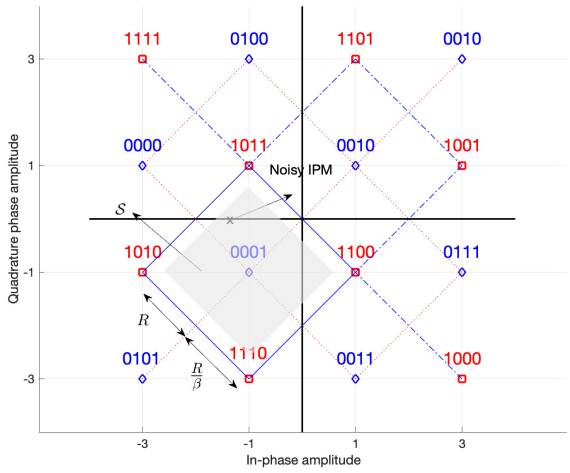
1: Set the precision parameter to $p = 16$
2: Set $\mu_0 = 3.85$
3: **if** n $= 1$ **then**
4: $\quad \alpha_0 = \text{INITIALIZE LOGISTIC MAP}(\mathbf{h}^{(b)})$
5: **end if**
6: $\alpha_n = \mu\alpha_{n-1}(1 - \alpha_{n-1})$
7: Compute $\bar{\alpha}_n = \text{round}(\alpha_n \times 10^p) \pmod{2^\ell}$
8: Convert $\bar{\alpha}_n$ to binary: $\mathbf{k}_n = \text{decimal to binary}(\bar{\alpha}_n, \ell)$
9: Save the value of α_n

5.2.5 Toy example illustrating the IPM concept

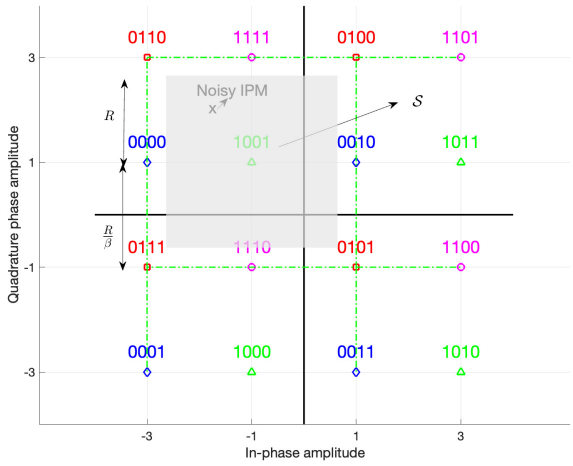
To illustrate our proposed schemes, we provide the following examples of one-bit and two-bits partitioning with noiseless IPM and noisy IPM.

5.2.5.1 Noiseless IPM

We consider a 16-QAM constellation with 2 partitions in Figure 5.2a and 4 partitions in Figure 5.2b. The three (resp. the two) last bits in Figure 5.2a (resp. Figure 5.2b) are the information bits and the first (resp. the first two) bits corresponds to the shared dynamic index between Alice and Bob. We let $\psi(\mathbf{b}|\mathbf{k})$ denote the image of an information sequence $\mathbf{b}$ knowing $\mathbf{k}$. As an example in Figure 5.2a, the image of the information sequence 101 is $\psi(101|0) = -3 - 3i$ if the index is 0, and is equal to $\psi(101|1) = 1 + 3i$ if the index is 1. This means that the sequence 101 has two distinct images in the constellation of Eve Ω_c. To ensure confusion at Eve, the bit labeling should guarantee that the Euclidean distance between these two images is maximized. Indeed, the Hamming distance between the neighboring bit sequences in Ω_c should be at least equal to one. This observation is identical in Figure 5.2b where the bit labeling should guarantee that the Euclidean distance between $\psi(\mathbf{b}|k_1k_2)$ is maximized. As an example in Figure 5.2b, $\psi(00|00) = -3 + 1i$, $\psi(00|01) = 1 + 3i$, $\psi(00|10) = -1 - 3i$ and $\psi(00|11) = 3 - 1i$.



(a) Noisy IPM: one-bit partitioning $\Lambda_0 \rightarrow \diamond$ and $\Lambda_1 \rightarrow \square$.



(b) Noisy IPM: two-bit partitioning $\Lambda_{00} \rightarrow \diamond$, $\Lambda_{01} \rightarrow \square$, $\Lambda_{10} \rightarrow \triangle$ and $\Lambda_{11} \rightarrow \circ$.

Figure 5.2: 16QAM-noisy IPM with symbol label $[\mathbf{k}, \mathbf{b}]$

5.2.5.2 Noisy IPM

Figure 5.2a illustrates Bob detection zones (or the Voronoï regions around each symbol) of a 16-QAM with two partitions: the blue lines delimit the detection zones in the partition with index 0 and the red ones for the case of an index 1. The symbol detection is performed without error as far as the received symbol remains in the detection zone around the transmitted QAM symbol, to say $\psi(001|0) = -1 - 1i$. To induce more confusion at Eve, we propose to transmit instead of the IPM QAM symbol $\psi(001|0) = -1 - 1i$, a random complex number uniformly chosen in the gray square $\mathcal{S}$ (that is included in the Voronoï region) centered around this transmitted symbol. In the high SNR regime, the reception of the noisy IPM symbol in the square will be the one that will ensure the most confusion at the eavesdropper. We can intuitively observe that, at Eve, depending on the position of the received symbol, there is an equal probability that this noisy IPM symbol stems from two neighboring symbols in the 16-QAM constellation. This means that there is an equal probability that the AN stems from $-1 - 1i$ or $-1 + 1i$ when the received symbol is situated in the upper small part of the gray square of Figure 5.2a. In a similar way, Figure 5.2b illustrates Bob's detection zones with 4 partitions. Here again, instead of transmitting a QAM symbol (to say $\psi(01|10) = -1 + 1i$), we add to this latter a random uniform AN chosen in the square detection zone $\mathcal{S}$ around this point (in gray). As in the previous case, at Eve, depending on the position of the transmitted point there is an equal probability that this point stems from one of the four neighboring points $-3 + 3i$, $-1 + 3i$, $-3 + 1i$ or

$-1+1i$.

5.3 Mathematical Representation of IPM and Noisy IPM

In this section, we provide a mathematical framework to describe the noiseless IPM and noisy IPM. We detail in Subsections 5.3.1 and 5.3.2 how the IPM partitioning and bit mapping, referred as cross-labeling, are performed. Then, we characterize in Subsection 5.3.3 the IPM input signal and we show how to split the power between the random injected AN and the useful signal.

5.3.1 2^q-QAM partitioning

The partition concept is known since the seminal work on mapping by set partitions of Ungerboëck in [142]. It involves partitioning the 2^q-QAM constellation into disjoint subsets to increase the Euclidean distance between neighboring symbols in each partition. A systematic procedure described in [142] is used to form encoded bits in the 2^q-QAM symbols. Unlike the mapping by set partitioning, our proposed IPM scheme assumes that the partition index is *fully known* at the legitimate receiver and transmitter, but not at the eaveesdropper. Moreover, the objective of the bit labeling in IPM scheme is different from the mapping by set partitioning. It aims to induce more error at the eavesdropper, and to minimize the error at the legitimate receiver. This will be further described in Subsection 5.3.2.

The main idea of the partitioning is to recursively divide the symbols in the 2^q-QAM constellation into disjoint groups of symbols. In each group of symbol, the Euclidean distance between the neighboring points is increased. For an IPM with 2 (resp. 4) partitions corresponding to an index-length of $\ell=1$ (resp. $\ell=2$), the minimal Euclidian distance in Figure 5.3 (resp. Figure 5.4) is $d_{\min}\sqrt{2}$ (resp. $2d_{\min}$) where $d_{\min}$ is the minimal distance in the normalized QAM constellation with

$$d_{\min}=\frac{2}{\sqrt{E_s}}, \tag{5.4}$$

and the symbol energy $E_s=\frac{2(2^q-1)}{3}$. To easily generate the partitions for $\ell=1$ and $\ell=2$, one can consider the 2^q-QAM constellation as the set of points generated by $4\mathbb{Z}[i]-(2+2i)+(\pm1\pm1i)$ inside the constellation bounds. Note that in each case $(\pm1\pm1i)$ generates shifts with 4 orientations $\swarrow\nearrow\nwarrow\searrow$ around of $4\mathbb{Z}[i]-(2+2i)$-points. For the two partitions case, Λ_0 (resp. Λ_1) are then generated considering $\swarrow\nearrow$ (resp.$\nwarrow\searrow$) orientations shifts. For the 4 partitions case, the partitions Λ_{00}, Λ_{01}, Λ_{10}

and Λ_{11} are generated considering respectively $\swarrow, \nearrow, \nwarrow, \searrow$ orientations. The same procedure can be recursively performed to generate deeper partitions.

5.3.2 Cross-labeling: bit mapping in the partitioned 2^q-QAM

Let $\mathbf{b}$ be the information bit vector on each subcarrier carrying $(q-\ell)$ bits and $\mathbf{k}$ be the index partition of $1 \leq \ell \leq 2$ bits. Each symbol in the 2^q-QAM constellation is labeled by the binary sequence $[\mathbf{k}, \mathbf{b}]$. Knowing $\mathbf{k}$, the bit mapping is a bijection, and $\mathbf{b}$ has a unique image denoted $\psi(\mathbf{b}|\mathbf{k})$. However, when $\mathbf{k}$ is not known, $\mathbf{b}$ has 2^ℓ images in Ω_c with $\vec{\psi}(\mathbf{b}) = \Big(\psi(\mathbf{b}|\mathbf{k}_1), \ldots, \psi(\mathbf{b}|\mathbf{k}_{2^\ell})\Big)$. For the ℓ-bit length index k, the bit labeling is performed to guarantee that: (C1) the Euclidean distance between all the images of $\psi(\mathbf{b})$ is maximized; (C2) the Hamming distance between the information sequence (the $q-\ell$ last bits) considering two neighboring symbols in Ω_c is at least equal to 1; (C3) the Hamming distance between the information sequence in Λ_k is minimized. The first two conditions will increase the confusion at the eavesdropper when attempting to decode the sequence $\mathbf{b}$ in Ω_c. The last condition will minimize the BER at the legitimate receiver.

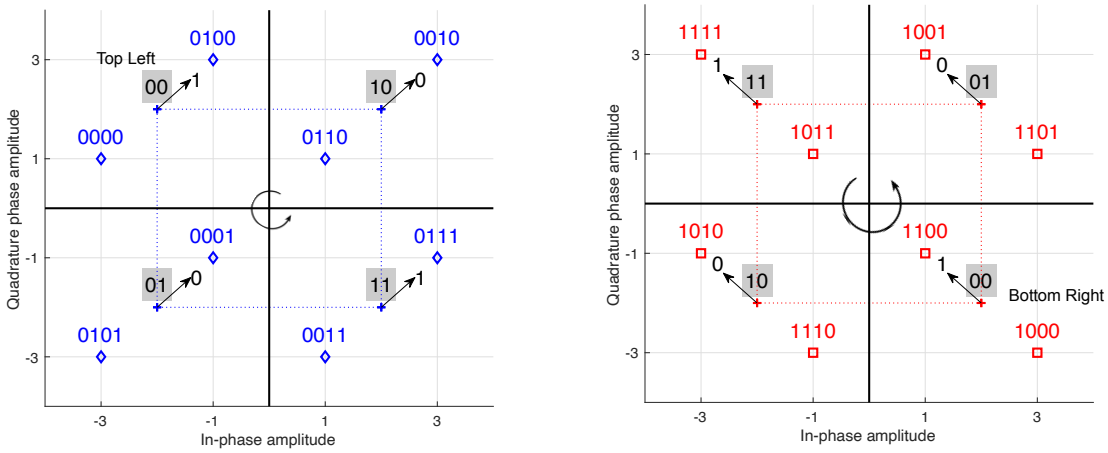
5.3.2.1 Cross-labeling for one-bit index partitioning

For the one-bit index partitioning, we need to label the points generated by shifted $4\mathbb{Z}[i] - (2+2i)$ with a shift orientation of $\swarrow\nearrow$ for $k=0$, and $\nwarrow\searrow$ for $k=1$. The information sequence consists of $(q-1)$ bits. Our proposed cross-labeling is performed in 4 steps: (S1) Identify inside each partition Λ_k, the virtual points generated by $4\mathbb{Z}[i] - (2+2i)$, situated inside the constellation and indicate the shift orientation. These virtual points are identical to both partitions but their bit labeling is different. (S2) To label these virtual points, a Gray mapping is used with a sense $\mathcal{O}_1(k)$ defined with respect to k and the all-zero sequence of $(q-2)$ bits as,

$$\mathcal{O}_1(k) = \begin{cases} \text{top-left } \vec{0} \text{ ; anti-clockwise Gray map,} & k=0, \\ \text{bottom-right } \vec{0} \text{ ; anti-clockwise Gray map,} & k=1. \end{cases} \tag{5.5}$$

(S3) In each partition, a bit changes from 1 to 0 or 0 to 1 in the direction $\nearrow$ with $k=0$ (resp. $\nwarrow$ with $k=1$). (S4) In each partition, the combination of the bit affected by the shift direction and virtual points form the QAM symbols. Our proposed bit labeling is illustrated in Figure 5.3. The virtual points are indicated in Figure 5.3a and 5.3b and are labelled according to (5.5). This labeling corresponds to the last two bits of the constellation points of Λ_0 and Λ_1. The shift orientation $\nearrow$ in

Λ_0 (resp. $\nwarrow$ in Λ_1) is alternatively labelled by 1 and 0. The leftmost bit corresponds to the partition index. The average Hamming distance in Λ_1 (or Λ_2) is $\frac{8}{9} \times 1 + \frac{1}{9} \times 3 = 1.22$. We can also observe that the Hamming distance between the information bit in Ω_c is at least equal to one. The average number of neighboring symbols in Λ_0 or Λ_1 is equal to $\frac{1}{8}(2 \times 1 + 4 \times 2 + 2 \times 4) = 2.25$.



(a) IPM: $\Lambda_0 \rightarrow \diamond$

(b) IPM: $\Lambda_1 \rightarrow \square$.

Figure 5.3: Binary mapping with respect to $\mathcal{O}_1(k)$ in (5.5)

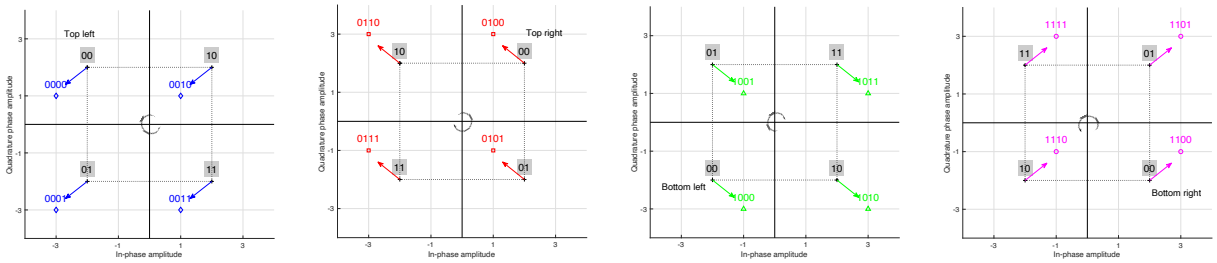
5.3.2.2 Cross-labeling for two-bits index partitioning

In this case, the partition is determined based on the shift orientation $00 = \swarrow$, $01 = \nearrow$, $11 = \nwarrow$, $10 = \searrow$. As previously, the virtual points are identified and are labelled with respect to the position of the $(q-2)$-length zero sequence and the sense of the gray mapping $\mathcal{O}(\mathbf{k})$ as,

$$\mathcal{O}_2(\mathbf{k}) = \begin{cases} \text{top-left } \vec{0}\text{; anti-clockwise Gray map,} & \mathbf{k} = 00, \\ \text{top-right } \vec{0}\text{; clockwise Gray map,} & \mathbf{k} = 01, \\ \text{bottom-left } \vec{0}\text{; clockwise Gray map,} & \mathbf{k} = 10, \\ \text{bottom-right } \vec{0}\text{; anti-clockwise Gray map,} & \mathbf{k} = 11. \end{cases} \tag{5.6}$$

Figure 5.4 illustrates the 16-QAM bit labeling with a bit index of length 2. The virtual points are identified and labeled according to (5.6). The first two bits correspond to the index. We can observe that the Hamming distance between the information bits of neighboring points in $\Lambda_{\mathbf{k}}$ is equal to 1. The average number of neighboring symbols in $\Lambda_{\mathbf{k}}$ is equal to 2 compared to 3 in Ω_c.

The binary mapping for one-bit partitioning and two-bits partitioning for a 64-QAM constellation is illustrated in Figures 5.5a and 5.5b. The colors are used to distinguish the different partitions. We



(a) IPM: $\Lambda_{00} \to \diamond$ (b) IPM: $\Lambda_{01} \to \square$. (c) IPM: $\Lambda_{10} \to \triangle$ (d) IPM: $\Lambda_{11} \to \circ$.

Figure 5.4: Binary mapping with respect to $\mathcal{O}_2(k)$ in (5.6)

can observe that for one bit partitioning in Figure 5.5a, the Hamming distance is equal to one with probability of 40/49. The average Hamming distance is equal to $\frac{40}{49} \times 1 + \times \frac{9}{49} \times 3 \approx 1.37$. The average number of neighboring symbols in Λ_0 (or Λ_1) is $\bar{N}_1^{(b)} \approx 3$, compared to 3.5 at the eavesdropper. We can also notice that the Hamming distance in Ω_c is at least equal to one. For the two bits partitioning in Figure 5.5b, the average number of neighboring symbols is $\bar{N}_2^{(b)} = 3$ compared to 3.5 symbols in Ω_c.

At the eavesdropper, the average number of neighboring symbol $\bar{N}^{(e)}$ in Ω_c computed in one quadrant is,

$$\bar{N}^{(e)} = \frac{1}{2^{q-2}} \left(4(2^{\frac{q-2}{2}} - 1)^2 + 3 \times 2(2^{\frac{q-2}{2}} - 1) + 2 \right) = 4(1 - 2^{-q/2}). \tag{5.7}$$

For the general 2^q-QAM constellation with one-bit partitioning, the average number of neighboring symbols at the legitimate receiver is,

$$\bar{N}_1^{(b)} = \frac{1}{2^{q-1}} (2 \times 4(2^{q/2-1} - 1) + 2 + 4(2^{q-1} - 4(2^{q/2-1} - 1) - 2)) = 4(1 - 2^{-q/2})^2. \tag{5.8}$$

For the two-bits partitioning, the average number of neighboring symbol is

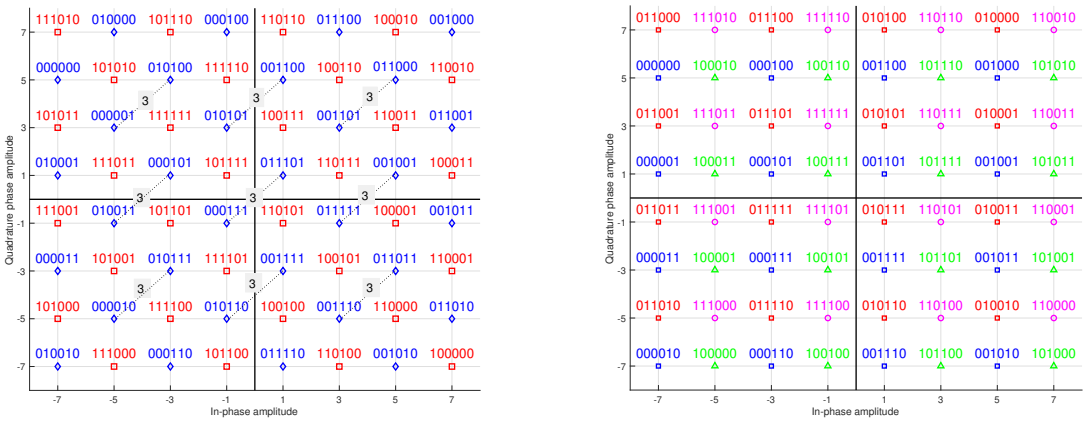
$$\bar{N}_2^{(b)} = 4(1 - 2^{-(q-2)/2}). \tag{5.9}$$

The average Hamming distance and the number of neighboring symbols are summarized in Table 5.1.

5.3.3 IPM signal constitution

At the transmitter, the input signal is,

$$x = \sqrt{\theta P} s_0 + u, \tag{5.10}$$



(a) Cross-labeling with one-bit partitioning

(b) Cross-labeling with two-bits partitioning

Figure 5.5: Binary mapping of 64-QAM constellation

Table 5.1: Cross-labeling: average Hamming distance

		64-QAM		16QAM		QPSK
	ℓ	1	2	1	2	1
Bob	$d_{\mathbb{H}}$	1.37	1	1.23	1	1
	$\bar{N}$	3.06	3	2.25	2	1
Eve	$d_{\mathbb{H}}$	2.65	1.43	2.17	1.34	0.5
	$\bar{N}$	3.5	3.5	3	3	2

where $s_0 = \frac{1}{\sqrt{E_s}}\psi(\mathbf{b}|\mathbf{k}) \in \Lambda_{\mathbf{k}}$ is the normalized symbol, $u \in \mathcal{S}$ the uniform AN with pdf,

$$f(u) = \begin{cases} \frac{1}{|\mathcal{S}|} & u \in \mathcal{S} \\ 0 & \text{otherwise} \end{cases} \tag{5.11}$$

and $0 < \theta \leq 1$ is a scaling factor that guarantees that the power constraint is satisfied *i.e.* $\mathbb{E}[|x|^2] = P$, and

$$\mathbb{E}[|u|^2] = \mathbb{E}[|x|^2] - \theta P\,\mathbb{E}[|s_0|^2] = (1-\theta)P. \tag{5.12}$$

The minimal Euclidean distance in the partitioned scaled constellation is denoted by $d_{\mathbb{E}}(\Lambda_k) = \sqrt{\theta P}2^{\ell/2}d_{\min}$, whereas the scaled minimal Euclidean distance in Ω_c is $d_{\mathbb{E}}(\Omega_c) = \sqrt{\theta P}d_{\min}$. The space $\mathcal{S}$ of the random uniform AN is a subspace of the Voronoï region, denoted $\mathcal{V}(o)$, such that $\mathcal{S} \subseteq \mathcal{V}(o)$. This space $\mathcal{S}$ is illustrated in Figure 5.2a for the case with $\ell = 1$ and Figure 5.2b in the case of $\ell = 2$. This space is parametrized by a factor $0 < \beta \leq 1$ that adjusts the size of the square $\mathcal{S}$ to remain inside

the Voronoï region. In both cases of one-bit index or two-bits index, $\mathcal{S}$ corresponds to a square in the $\pi/4$-**rotated coordinate system** for $\ell = 1$, and in the **Cartesian coordinate system** for $\ell = 2$, *i.e.*,

$$\mathcal{S} = \{u \in \mathbb{C} : -R \leq \Re(u), \Im(u) \leq R\}, \tag{5.13}$$

where $R = \beta d_{\mathbb{E}}(\Lambda_k)/2$, is the half of the scaled minimal distance that ensures that $\mathcal{S} \subseteq \mathcal{V}(o)$ with $0 \leq \beta \leq 1$ a scaling factor that adjust the size of $\mathcal{S}$ to remain inside the Voronoï region, such that,

$$R = \sqrt{\theta P} 2^{\ell/2-1} \beta d_{\min}. \tag{5.14}$$

The square area is $|\mathcal{S}| = 4R^2$. The power of the random uniform noise is,

$$\mathbb{E}[|u|^2] = \frac{1}{|\mathcal{S}|} \int_{-R}^{R} \int_{-R}^{R} |u|^2 du = \frac{2R^2}{3}. \tag{5.15}$$

Using (5.15), the power constraint in (5.12) is satisfied for

$$\theta = \frac{3E_s}{3E_s + 2^{\ell+1}\beta^2}. \tag{5.16}$$

5.4 Secrecy Metrics Evaluation: Secrecy capacity, Symbol Error Probability and Average BER

In this section, we characterize the secrecy performance of our scheme in terms of secrecy capacity, symbol error probability (same as SER), and average BER. For this, we compute first in Subsection 5.4.1 the probability of the received signal conditioned by the transmitted information sequence. We evaluate then the secrecy capacity in Subsection 5.4.2 and the pairwise symbol error probability in Subsection 5.4.3. To simplify the notation, we drop, all the superscripts relative to Bob and Eve $^{(b)}$ and $^{(e)}$ from the output, the input and channels. The model in (5.1), (5.2) and (5.10) for each subcarrier becomes,

$$y_n = \sqrt{\theta P} h_n s_0 + (h_n u + z_n), \tag{5.17}$$

The random value SNR_{h_n} and the average SNR are defined as,

$$\mathrm{SNR}_{h_n} \triangleq \frac{\theta P |h_n|^2}{E_s \sigma^2}, \tag{5.18}$$

$$\mathrm{SNR} \triangleq \frac{\theta P}{E_s 2\sigma^2}. \tag{5.19}$$

5.4.1 Channel conditional probabilities

Given the channel model in (5.17), the conditional probabilities of y given s_0, denoted as $\omega(y|s_0,h)$ are computed considering different domain space variations of u (*i.e.* for both the noiseless IPM case and noisy IPM with square region).

Lemma 5.1 (General noisy IPM case) *For the noisy IPM case, the conditional probability $\omega(y_n|s_0,h_n)$ on each subcarrier is such that,*

$$\omega(y_n|s_0,h_n)=\frac{1}{|\mathcal{S}|}\frac{1}{2\pi\sigma_{h_n}^2}\iint_{u\in\mathcal{S}} e^{-\frac{1}{2\sigma_{h_n}^2}|u-u_z|^2}du, \tag{5.20}$$

where $\sigma_{h_n}=\sigma/|h_n|$ and

$$u_z=\frac{1}{|h_n|^2}\Big(y_n-\sqrt{\theta P}\,h_n s_0\Big)h_n^*, \qquad |h_n|\neq 0. \tag{5.21}$$

Proof: The proof is provided in Appendix 5.7.1. □

Lemma 5.2 (Square region) *For the noisy IPM case with square region, the conditional probability $\omega(y_n|s_0,h_n)$ on each subcarrier is*

$$\omega(y_n|s_0,h_n)=\frac{1}{4R^2}\prod_{k=1}^{2}\left[\Phi\Big(\frac{R-u_{z,k}^{(\ell)}}{\sigma_{h_n}}\Big)-\Phi\Big(-\frac{R+\nu_{z,k}^{(\ell)}}{\sigma_{h_n}}\Big)\right] \tag{5.22}$$

with $(u_{z,1}^{(1)},u_{z,2}^{(1)})$ are the coordinates of u_z in the $\pi/4$-rotated coordinate system, and $(u_{z,1}^{(2)},u_{z,2}^{(2)})$ are the coordinates of u_z in the Cartesian coordinate system, such that, $u_{z,1}^{(2)}=\Re(u_z)$, $u_{z,2}^{(2)}=\Im(u_z)$ and $u_{z,1}^{(1)}=\cos(\pi/4)u_{z,1}+\sin(\pi/4)u_{z,2}$ and $u_{z,2}^{(1)}=-\sin(\pi/4)u_{z,1}+\cos(\pi/4)u_{z,2}$.

Proof: The proof is provided in Appendix 5.7.2. □

5.4.2 Secrecy capacity evaluation

In this subsection, we compute in Theorem 5.1 the secrecy capacity defined as the difference of mutual information between the main channel and the wiretap channel. The main difference between both channels stems from the knowledge of the dynamic index at Bob but not at Eve.

Theorem 5.1 (Mutual information) *At a given subcarrier, the mutual information between Alice and Bob is,*

$$I_b(\psi(\mathbf{b}_n|\mathbf{k}_n), y_n^{(b)}) = (q-\ell) - \mathbb{E}_{h_n,\mathbf{b}_n,\mathbf{k}_n}\left[\log_2 \frac{\sum_{s_0\in\Lambda_{\mathbf{k}}} \omega(y_n^{(b)}|s_0, h_n^{(b)})}{\omega(y_n^{(b)}|\psi(\mathbf{b}_n|\mathbf{k}_n), h_n^{(b)})}\right], \tag{5.23}$$

and the average mutual information for the main channel is given as

$$I_b(\psi(\mathbf{b}|\mathbf{k}), y^{(b)}) = \frac{1}{N}\sum_{n=1}^{N} I_b(\psi(\mathbf{b}_n|\mathbf{k}_n), y_n^{(b)}). \tag{5.24}$$

The mutual information between Alice and Eve on each subcarrier is,

$$I_e(\psi(\mathbf{b}_n), y_n^{(e)}) = (q-\ell) - \mathbb{E}_{h_n,\mathbf{b}_n}\left[\log_2 \frac{\sum_{s_0\in\Omega_c} \omega(y_n^{(e)}|s_0, h_n^{(e)})}{\sum_{\mathbf{k}_n} \omega(y_n^{(e)}|\psi(\mathbf{b}_n|\mathbf{k}_n), h_n^{(e)})}\right], \tag{5.25}$$

and the average mutual information for the wiretap channel is given as

$$I_e(\psi(\mathbf{b}), y^{(e)}) = \frac{1}{N}\sum_{n=1}^{N} I_e(\psi(\mathbf{b}_n), y_n^{(e)}). \tag{5.26}$$

The secrecy capacity is computed using (5.23) and (5.25). as,

$$C_s = I_b(\psi(\mathbf{b}|\mathbf{k}), y^{(b)}) - I_e(\psi(\mathbf{b}), y^{(e)}).$$

Proof: The proof is provided in Appendix 5.7.3. □

A Monte-Carlo simulation is performed to compute the mutual information of Bob and Eve. First, the IPM signal corresponding to a random binary sequence $\mathbf{b}_n$ and a random binary index $\mathbf{k}_n$ is formed at Alice using (5.10). The corresponding received signal $y_n^{(b)}$ and $y_n^{(e)}$ are then generated at Bob and Eve using (5.1) and (5.2). Using Lemmas 5.1 to 5.2 and given the values of $y_n^{(b)}$ and $y_n^{(e)}$ and the fading channels $h_n^{(b)}$ and $h_n^{(e)}$, the expressions of $\omega(y_n^{(b)}|s, h_n^{(b)})$ and $\omega(y_n^{(e)}|s, h_n^{(e)})$ are respectively computed.

corollary-t 5.1 (secrecy capacity asymptotic behavior) *In the high SNR regime, the asymptotic mutual information of the main channel between Alice and Bob is,*

$$\lim_{\sigma\to 0} I_b(\psi(\mathbf{b}|\mathbf{k}), y^{(b)}) = q - \ell. \tag{5.27}$$

The asymptotic mutual information of the Eavedropper channel between Alice and Eve is,

$$\lim_{\sigma\to 0} I_e(\psi(\mathbf{b}), y^{(e)}) = (q-\ell) - C_s(\beta) \tag{5.28}$$

with $C_s(\beta) = 0$ *if* $0 < \beta \leq \frac{1}{2}$. *Otherwise, for the* 2^q*-QAM constellation with* $q \neq 2$,

$$C_s(\beta) = \begin{cases} \bar{N}^{(e)} \left(1 - \frac{1}{2\beta}\right)^2, & \ell = 1 \\ \bar{N}^{(e)} \left(1 - \frac{1}{2\beta}\right) - \frac{1}{2^{q-2}} \left(1 - \frac{1}{2\beta}\right)^2 & \ell = 2, \end{cases} \tag{5.29}$$

with $\bar{N}^{(e)}$ *being the average number of neighbors around each constellation point in* Ω_c *defined in (5.7). For the case of QPSK with* $\ell = 1$*-bit partitioning,*

$$C_s(\beta) = \left(1 - \frac{1}{2\beta}\right)^2.$$

Proof: The proof is detailed in Appendix 5.7.4. □

5.4.3 Error rate evaluation

In this subsection, we convey first the Maximum A-Posteriori (MAP) decoding criterion into a Euclidean distance minimization. Based on this, we compute the symbol error probability at the legitimate receiver and the eavesdropper.

5.4.3.1 MAP criterion and detection zone

Theorem 5.3 summarizes the IPM decoding rules obtained by applying the MAP criterion to conditional probabilities in Lemmas 5.1 and 5.2.

Lemma 5.3 (MAP detection) *For the noiseless IPM and the noisy IPM case with square noisy region, the MAP detection* $\max \omega(y_n|s, h_n)$ *is equivalent to finding the constellation point that minimizes the Euclidean distance such that:*

- *At the legitimate receiver with full k-index knowledge,*

$$\hat{s}_n = \arg \min_{s \in \Lambda_k} |y_n - \sqrt{\theta P} h_n s|^2. \tag{5.30}$$

- *At the eavesdropper without k-index knowledge,*

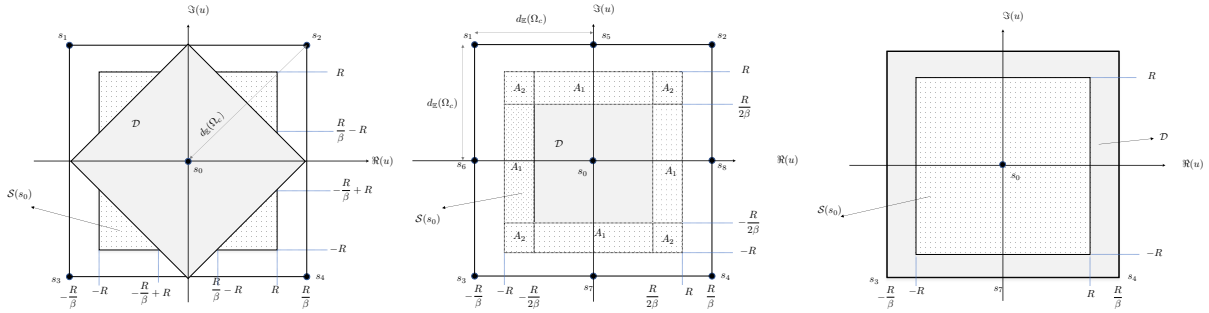
$$\hat{s}_n = \arg \min_{s \in \Omega_c} |y - \sqrt{\theta P} h_n s|^2. \tag{5.31}$$

Proof: The proof is provided in Appendix 5.7.5. □

Using the MAP criterion in Lemma 5.3, the correct detection zone $\mathcal{D}$ around a given constellation point s_0 is

$$\mathcal{D}(\mathcal{L}) = \{v \in \mathbb{C} : |s_0 - v| \leq |s - v|, \forall s \in \mathcal{L}\} \tag{5.32}$$

with $\mathcal{L} = \Lambda_k$ at Bob and $\mathcal{L} = \Omega_c$ at Eve. The detection region bounds depend on the scaled minimal Euclidean distance where $d_{\mathbb{E}}(\Lambda_k) = \frac{R}{\beta}$ and is equal to $d_{\mathbb{E}}(\Omega_c) = \frac{R}{2^{\ell/2}\beta}$.



(a) Eve with $\ell = 1$, $\mathcal{S} \cap \mathcal{D} \neq \mathcal{S}$ (b) Eve with $\ell = 2$, $\mathcal{D} \subseteq \mathcal{S}$ (c) Bob with $\ell = 1, 2$, $\mathcal{S} \subseteq \mathcal{D}$

Figure 5.6: Error detection zones: the detection $\mathcal{D}$ zone is in gray and the uniform noise domain space $\mathcal{S}$ is filled with a dot pattern

With respect to the geometry of the figure, we can distinguish between two cases: (i) the detection zone and the uniform noise domain space $\mathcal{S}$ have similar geometric shape in the Cartesian coordinate system at Bob or Eve with $\ell = 2$ or in the rotated $\pi/4$-coordinate system for Bob case with $\ell = 1$ and Eve case with $\ell = 2$ as illustrated in Figures 5.6b and 5.6c. (ii) the correct detection zone $\mathcal{D}$ and the uniform noise domain space $\mathcal{S}$ have different geometric shape (case of Eve with $\ell = 1$) in the rotated $\pi/4$-coordinate system as illustrated in Figure 5.6a; In all cases, the symbol error probability is,

$$\mathbb{P}_e = \text{Prob}\{u_z = (u + h_n^{-1} z) \notin \mathcal{D}(\mathcal{L})\}, \tag{5.33}$$

where $\mathcal{D}(\mathcal{L})$ is the detection zone specified in Figure 5.6 and u_z is the random noise with coordinates in the rotated $\frac{\pi}{4}$- system for $\ell = 1$ or the Cartesian system for $\ell = 2$, having as pdf distribution,

$$f(u_z) = \frac{1}{4R^2} \prod_{k=1}^{2} \left[\Phi\Big(\frac{R - u_{z,k}}{\sigma_{h_n}}\Big) - \Phi\Big(-\frac{R + u_{z,k}}{\sigma_{h_n}}\Big) \right],$$

with $u_{z,1} = \Re(u_z)$ and $u_{z,2} = \Im(u_z)$. In the high SNR regime, the average BER can be deduced from the most dominant error event computed in (5.33) as,

$$\text{BER}^{(b),(e)}(\text{SNR}) = \frac{\bar{d}_{\mathbb{H}}^{(b),(e)}}{q - \ell} \mathbb{P}_e^{(b),(e)}(\text{SNR}), \tag{5.34}$$

with $\bar{d}_{\mathbb{H}}^{(b)}$ (resp. $\bar{d}_{\mathbb{H}}^{(e)}$) being the average Hamming distance in Λ_k (resp. Ω_c) that are summarized in Table 5.1.

5.4.3.2 Error rate evaluation at Eve

At the eavesdropper, the SER is computed from (5.33) where the detection zone with one-bit partitioning is such that,

$$\mathcal{D}_1(\Omega_c) = \{u_z \in \mathbb{C} : |\Re(u_z)| < \frac{R}{\beta} \text{ and } -\frac{R}{\beta} + |\Re(u_z)| < \Im(u_z)| < \frac{R}{\beta} - |\Re(u_z)|\}, \tag{5.35}$$

and for two-bits partitioning,

$$\mathcal{D}_2(\Omega_c) = \{u_z \in \mathbb{C} : |\Re(u_z)| < \frac{R}{2^{\ell/2}\beta} \text{ and } |\Im(u_z)| < \frac{R}{2^{\ell/2}\beta}\}.$$

We can notice from Figure 5.6a, that if the detection zone $\mathcal{D}_1(\Omega_c) \cap \mathcal{S} = \mathcal{S}$, the symbol error probability becomes negligible in the high SNR regime. However, $\mathcal{D}_1(\Omega_c) \cap \mathcal{S} \neq \mathcal{S}$, requires that $\frac{1}{2} \leq \beta \leq 1$. Similarly, $\mathcal{D}_2(\Omega_c) \cap \mathcal{S} \neq \mathcal{S}$ if $\frac{1}{2} \leq \beta \leq 1$. The expansion of these symbol error probability expressions show that in the high SNR regime, the SER achieves a constant high SER floor as detailed in Theorem 5.2.

Theorem 5.2 (eavesdropper error rate) *For $\frac{1}{2} \leq \beta \leq 1$, the SER at the eavesdropper for and 2^q-QAM constellation ($q \neq 2$) achieves a constant error floor :*

1. *For the one-bit partitioning ($\ell = 1$):*

$$\mathbb{P}_e^{(e,1)} \approx 2(1 - 2^{-q/2}) \left(1 - \frac{1}{2\beta}\right)^2 + o(\mathrm{SNR}^0). \tag{5.36}$$

2. *For the two-bit partitioning ($\ell = 2$):*

$$\mathbb{P}_e^{(e,2)} \approx (1 - 2^{-q})\Big(1 - \frac{1}{2\beta}\Big) \left(1 + \frac{1 - 2^{-q/2}}{1 + 2^{-q/2}} \frac{1}{2\beta}\right) + o(\mathrm{SNR}^0), \tag{5.37}$$

which is approximately equal to $\mathbb{P}_e^{(e,2)} \approx 1 - \frac{1}{4\beta^2}$ for high modulation order. A correction term should be added to the symbol error probability when attempting to decode two symbols carrying the same information binary sequence, as,

$$\mathbb{P}_{e,c}^{(e,2)} = \mathbb{P}_e^{(e,2)} - 2^{-q} \left(1 - \frac{1}{2\beta}\right)^2.$$

For the case of QPSK constellation with one-bit partitioning,

$$\mathbb{P}_e^{(e,1)} \approx \left(1 - \frac{1}{2\beta}\right)^2.$$

Proof: The proof is provided in Appendix 5.7.6. □

5.4.3.3 Error rate evaluation at Bob

At the legitimate receiver, the error rate is computed from (5.33) where

$$\mathcal{D}^{(\ell=1,2)}(\Lambda_k) = \{u_z \in \mathbb{C} : |\Re(u_z)| < \frac{R}{\beta} \text{ and } |\Im(u_z)| < \frac{R}{\beta}\}.$$

The expansion of this expression is detailed in Theorem 5.3 given a subcarrier $|h_n|$.

Theorem 5.3 (General case) *Let $\hat{s}$ be the decoded symbol at the receiver side and s_0 being the transmitted one. Considering the general noisy IPM, the symbol error probability at Bob is,*

$$\mathbb{P}_e(\text{SNR}) \approx \frac{\bar{N}_a^{(b)}}{2^{\ell/2}\beta}\mathbb{E}_{h_n}\Big[\mathbb{P}_{e,1}(\text{SNR}_{h_n}) + \mathbb{P}_{e,2}(\text{SNR}_{h_n})\Big], \tag{5.38}$$

where

$$\mathbb{P}_{e,1} = 2\eta_p Q(\eta_p\sqrt{\text{SNR}_{h_n}}) - 2\eta_m Q(\eta_m\sqrt{\text{SNR}_{h_n}}), \tag{5.39}$$

$$\mathbb{P}_{e,2} = \sqrt{\frac{2}{\pi\,\text{SNR}_{h_n}}}\left[\exp\left(\frac{-\eta_m^2}{2}\,\text{SNR}_{h_n}\right) - \exp\left(\frac{-\eta_p^2}{2}\,\text{SNR}_{h_n}\right)\right], \tag{5.40}$$

and,

$$\eta_m = 2^{\ell/2}(1-\beta), \tag{5.41}$$

$$\eta_p = 2^{\ell/2}(1+\beta). \tag{5.42}$$

with

$$\bar{N}_a^{(b)} = \frac{1}{4}\bar{N}^{(b)} = \begin{cases}(1-2^{-\frac{q}{2}})^2 & \ell = 1,\\ (1-2^{-\frac{q-2}{2}}) & \ell = 2,\end{cases}$$

and $\bar{N}^{(b)}$ being defined in (5.8) and (5.9).

The final BER is obtained by averaging the conditional BER on the variable h_n for all subcarriers.

Proof: The proof is provided in Appendix 5.7.7. □

5.5 Numerical results

We consider an OFDM system that operates in a band of 1.4 MHz divided into subcarrier of $\Delta f = 15$ kHz with an FFT of size $N_c = 128$ where only $N = 72$ subcarriers are used. The sampling frequency is $F_s = N_c \Delta f = 1.92$ MHz. The Extended Typical Urban model (ETU) , corresponding to a highly selective radio environment with PDPs described in Table 5.2 is considered.

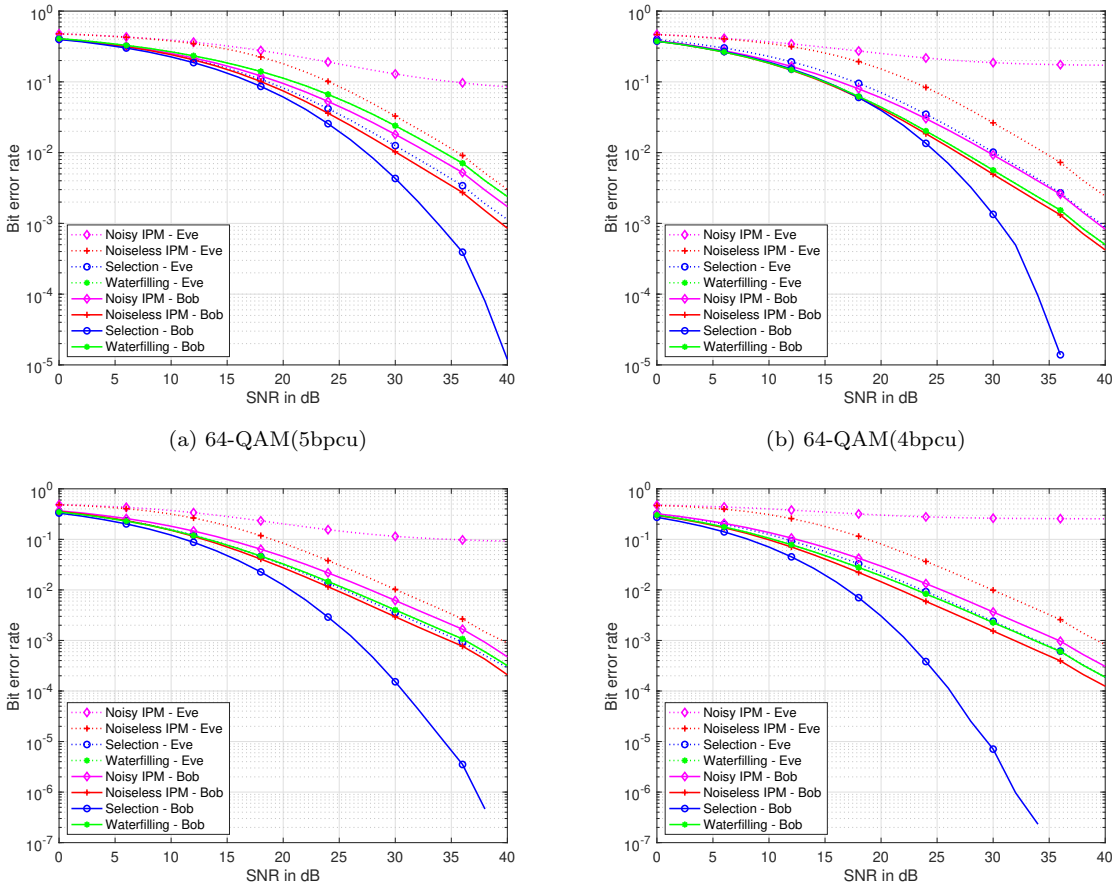
Table 5.2: PDP for ETU: τ = delay spread and σ_t^2 = power

$\tau[ns]$	0	50	120	200	230	500	1600	2300	5000
$\sigma_t^2[dB]$	-1	-1	-1	0	0	0	-3	-5	-7

We compare the performance of the proposed noiseless and noisy IPM ($\beta = 0.7$) schemes with a scheme that employs fade avoidance through subcarrier index selection [40] and another scheme where legacy water-filling algorithm is employed to favor the main channel since it is independent from the wiretap channel. We compare the performance in terms of mutual information, secrecy capacity and BER. To ensure a fair comparison, we set the system parameters (constellation size and number of active subcarriers) to achieve the same maximum spectral efficiency as the IPM system as shown in Table 5.3. With the subcarrier selection scheme, the total power is distributed evenly among all active subcarriers.

Table 5.3: Spectral efficiency of various schemes for fair comparison

IPM		64QAM ($\ell = 1$)	64QAM ($\ell = 2$)	16QAM ($\ell = 1$)	16QAM ($\ell = 2$)
	No of bpcu	5	4	3	2
Selection	**No of Active SCs**	60	48	54	36
Selection	**Constellation**	64QAM	64QAM	16QAM	16QAM
Water-filling	**No of Active SCs**	72	72	72	72
Water-filling	**Constellation**	32QAM	16QAM	8PSK	QPSK



(a) 64-QAM(5bpcu)

(b) 64-QAM(4bpcu)

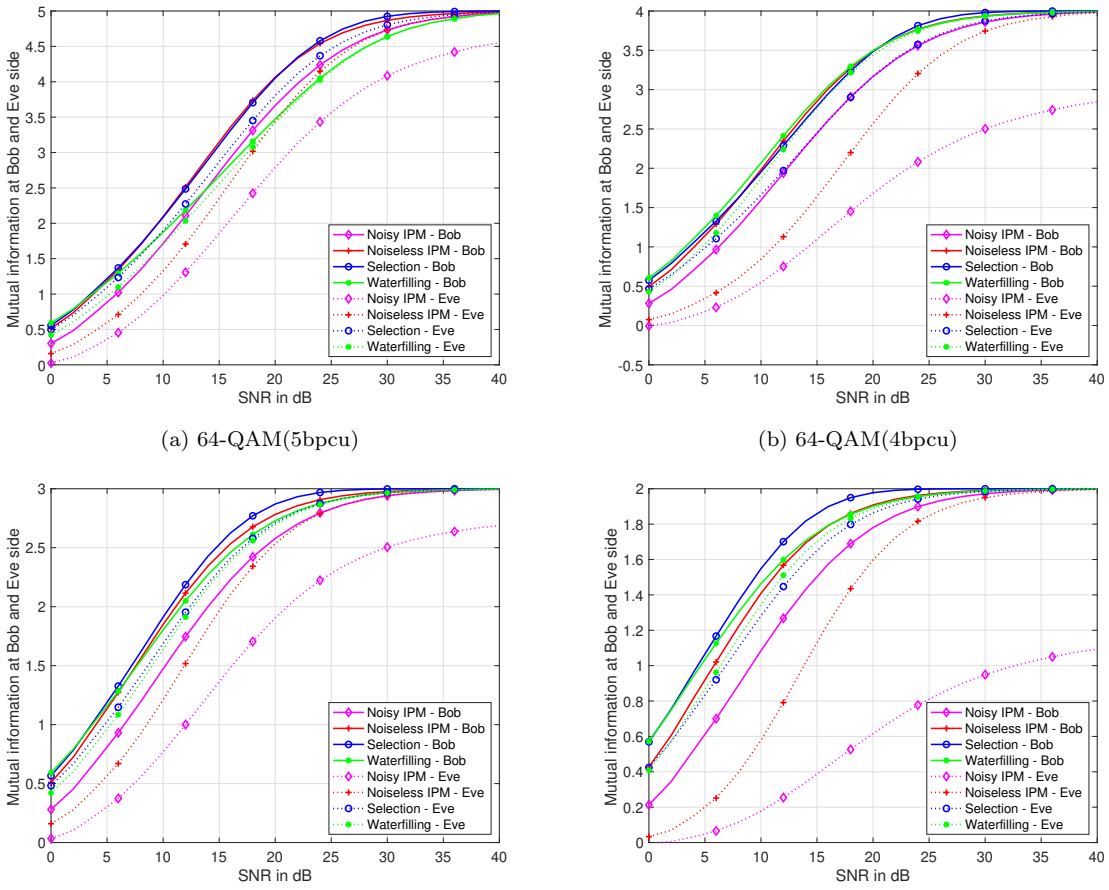
(c) 16-QAM(3bpcu)

(d) 16-QAM(2bpcu)

Figure 5.7: Bit error rate performance for Eve and Bob at $\beta = 0.7$

Using the equivalent noise distribution, we have shown that the MAP criterion is equivalent to the minimization of the Euclidean distance between the received signal and the attenuated transmitted signal. We have thus characterized the BER curves of our scheme in comparison with those of the literature in Figure 5.7. The security provided is measured in terms of the SNR gap between Bob and Eve at different BER values. Due to the selection of only high gain subcarriers in the selection scheme, we see Bob's BER performance with a diversity gain more than 1 but Eve has a relatively good BER with a diversity gain of 1 and thus minimal security gap. There is no security gain when using the water-filling algorithm because at high SNR values, the power allocation becomes the same as uniform power allocation and there is no gain for Bob over Eve. For the noiseless IPM scheme, Bob outperforms Eve but with SNR gaps between both at certain BER values. However, the noisy IPM gave the best performance as we see that the uniform noise only slightly affects the BER performance

of Bob but completely degrades the BER performance of Eve with an early onset of error floor in all considered constellations and bits per channel use (bpcu). The minimal degradation in decoding quality on the main channel can be compensated by an increase in energy, which will only benefit Bob and not Eve.



(a) 64-QAM(5bpcu)

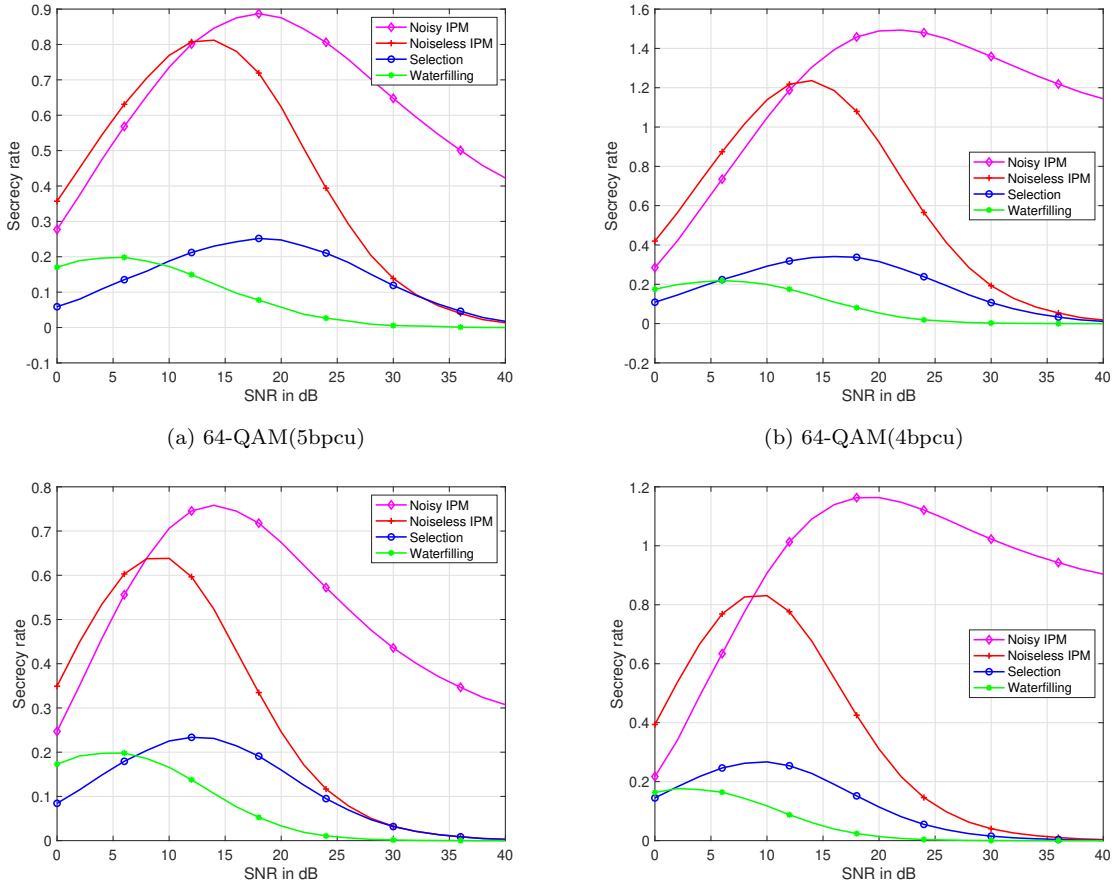
(b) 64-QAM(4bpcu)

(c) 16-QAM(3bpcu)

(d) 16-QAM(2bpcu)

Figure 5.8: Mutual information performance for Eve and Bob at $\beta = 0.7$

Figure 5.8 illustrates the variation of the mutual information as a function of the SNR obtained with 64-QAM (5bpcu and 4bpcu) and 16-QAM (3bpcu and 2bpcu). We can see that for the considered schemes, Bob's mutual information converges towards the maximum spectral efficiency. Similar to the BER performance this convergence is fastest for the selection scheme than the other schemes. On the wiretap, only the noisy IPM scheme does not reach the maximum spectral efficiency. This reduction is all the more efficient with a partitioning on 2 bits than on 1 bit.



(a) 64-QAM(5bpcu)

(b) 64-QAM(4bpcu)

(c) 16-QAM(3bpcu)

(d) 16-QAM(2bpcu)

Figure 5.9: Secrecy capacity performance for Eve and Bob at $\beta = 0.7$

We see in Figure 5.9 the secrecy capacity between for all the schemes. This is simply the difference in mutual information between Bob and Eve. It can be seen that the IPM schemes clearly outperforms the selection and water-filling schemes at the low SNR regimes but all except the noisy IPM goes to zero at the high SNR regime. This confirms again the optimal secrecy performance of the noisy IPM scheme. In the very high SNR regime, the uniform AN continues to degrade Eve but not Bob. For the 16-QAM constellation, the gain in security is 0.3 and 0.9 bpcu in the case of partitioning with 1 and 2 index bit(s) respectively. For the 64-QAM constellation, the gain in security is 0.42 and 1.18 bpcu in the case of partitioning with 1 and 2 index bit(s) respectively.

5.6 Conclusion

In this chapter, we proposed a new PLS scheme called noisy and dynamic IPM. IPM uses dynamic keys (known only by Alice and Bob) to select, in the partitioned constellation, a unique image for a given information bit sequence. We defined a cross-labeling to map the information bits into symbols with two-fold objectives. The cross-labeling maximizes the BER at the eavesdropper while minimizing the same at Bob. At the eavesdropper, the absence of the index's knowledge decreases the size of the detection zone compared to the legitimate receiver. For this, we inject a random uniform noise in a domain space scaled by a parameter β that ensures that this region is fully included in the large Bob's Voronoï region. We analytically show that the secrecy capacity and the symbol error probability at the eavesdropper achieve a plateau value independent of SNR, when the domain space of the injected random uniform noise exceeds the eavesdropper detection area. The random uniform noise domain space is wider when considering deeper partitioning, and induces confusion in the constellation states at the eavesdropper while conserving the states of the legitimate receiver in the different partitions as separate. Numerical results are provided to assess the theoretical results and they showed that our proposed scheme outperforms other known literature schemes.

5.7 Appendix

5.7.1 Proof of Lemma 5.1 on page 98

The proof of this Lemma is obtained by considering the marginalization of the joint probability,

$$\begin{aligned} \omega(y_n|s_0,h_n) &= \iint_{u\in\mathcal{S}} f(y_n,u|s_0,h_n)du \\ &= \iint_{u\in\mathcal{S}} f(y_n|s_0,h_n,u)f(u)du. \end{aligned}$$

Note that $f(y_n|s_0,h_n,u) = f(z)$ with $z = y_n - \sqrt{\theta P}\ h_n s_0 - h_n u$ being a Gaussian random random variable.

5.7.2 Proof of Lemma 5.2 on page 98

For the index of length 1, the square region inside the Voronoï region is rotated with an angle of $\pi/4$. As the rotation does not change the Gaussian distribution of the complex random noise, in

both cases of 1-bit or 2-bits of index length, the random uniform noise u varies in a square region $\mathcal{S}$ defined in the $\pi/4$-rotated coordinate system for $\ell = 2$ and in the Cartesian coordinate system for $\ell = 2$. The conditional probability distribution in Lemma 5.1 is equivalent to the computation of the CDF of two independent random Gaussian variable $\mathcal{N}(\Re(u_z), \sigma_{h_n})$ and $\mathcal{N}(\Im(u_z), \sigma_{h_n})$.

5.7.3 Proof of Theorem 5.1 on page 99

The average mutual information between the transmitted information signal at Alice and the received one $\mathbf{y}^{(b)}$ at Bob knowing the dynamic index $\mathbf{k}$ is,

$$\begin{aligned} \mathrm{I}_b(\psi(\mathbf{b}), \mathbf{y}_n^{(b)_n} | \mathbf{k}_n) &= \mathrm{I}_b(s_0, y_n^{(b)} | \mathbf{k}_n); && (5.43) \\ &= \mathbb{E}\big[\mathrm{H}(y_n^{(b)} | \mathbf{k}_n) - \mathrm{H}(y_n^{(b)} | s_0, \mathbf{k}_n)\big], && (5.44) \end{aligned}$$

where s_0 is the normalized corresponding symbol in Λ_k and H(.) is the entropy of a random variable, such that,

$$\begin{aligned} \mathrm{H}(y_n^{(b)} | h_n^{(b)}, \mathbf{k}_n) &= -\log_2 f(y_n^{(b)} | h_n^{(b)}, \mathbf{k}_n), && (5.45) \\ \mathrm{H}(y_n^{(b)} | s_0, h_n^{(b)}) &= -\log_2 f(y_n^{(b)} | s_0, h_n^{(b)}, \mathbf{k}_n). && (5.46) \end{aligned}$$

The conditional probability in (5.45) is computed by marginalizing over all the possibilities of $s_0 \in \Lambda_k$,

$$\begin{aligned} f(y_n^{(b)} | h_n^{(b)}, \mathbf{k}_n) &= \sum_{s_0 \in \Lambda_k} f(s_0) f(\mathbf{y}_n^{(b)} | s_0, h_n^{(b)}), \\ &= \frac{1}{2^{q-\ell}} \sum_{s_0 \in \Lambda_k} f(\mathbf{y}_n^{(b)} | s_0, h_n^{(b)}). && (5.47) \end{aligned}$$

Combining (5.44) and (5.47), the average mutual information in (5.23) is deduced.

Unlike Bob, Eve is not aware of the value of the key index. The mutual information at Eve side is,

$$\mathrm{I}_e(\psi(\mathbf{b}_n), y_n^{(e)}) = \mathbb{E}\big[\mathrm{H}(y_n^{(e)}) - \mathrm{H}(y_n^{(e)} | \psi(\mathbf{b}_n)\big], \quad (5.48)$$

where

$$\begin{aligned} \mathrm{H}(y_n^{(e)} | h_n^{(e)}) &= -\log_2 f(y_n^{(e)} | h_n^{(e)}), && (5.49) \\ \mathrm{H}(y_n^{(e)} | \psi(\mathbf{b}_n), h_n^{(e)}) &= -\log_2 f(y_n^{(e)} | \psi(\mathbf{b}_n), h_n^{(e)}). && (5.50) \end{aligned}$$

At Eve side, $\mathbf{k}_n$ is not known and the probability in (5.49) is the marginalization over all the values of $s_0 \in \Omega_c$,

$$\begin{aligned} f(y_n^{(e)}|h_n^{(e)}) &= \sum_{s_0 \in \Omega_c} f(s_0) f(y_n^{(e)}|s_0, h_n^{(e)}), \\ &= \frac{1}{2^q} \sum_{s_0 \in \Omega_c} f(y_n^{(e)}|s_0, h_n^{(e)}). \end{aligned} \tag{5.51}$$

Indeed, the information bit vector $\mathbf{b}_n$ has multiple image in Ω_c, and the conditional probability in (5.50) is computed,

$$\begin{aligned} f(y_n^{(e)}|\psi(\mathbf{b}_n), h_n^{(e)}) &= \sum_{\mathbf{k}_n} \mathrm{p}(k_n) f(y_n^{(e)}|\psi(\mathbf{b}_n), h_n^{(e)}, \mathbf{k}_n) \\ &= \frac{1}{2^\ell} \sum_{\mathbf{k_n}} f(y_n^{(e)}|\psi(\mathbf{b}_n|\mathbf{k}_n), h_n^{(e)}) \end{aligned} \tag{5.52}$$

By combining (5.48), (5.51) and (5.52), the average mutual information in (5.25) is deduced.

5.7.4 Proof of Corollary 5.1 on page 100

Let s_0 be the transmitted symbol and $y_n^{(b)}$ (resp. $y_n^{(e)}$) the noisy received signal at Bob side (resp. Eve side) with $\sigma_{h_n} \to 0$. The mutual information in Theorem 5.1 depends on the conditional probability $\omega(y_n|s, h_n)$ given in Lemma 5.1. For $\sigma_{h_n} \to 0$, the value of u_z in Lemma 5.1 is

$$u_z = \sqrt{\theta P}(s_0 - s) + u. \tag{5.53}$$

The variation set of s is provided in Theorem 5.1 where $s \in \Lambda_k$ at Bob side and $s \in \Omega_c$ at Eve side. The limit of $\omega(y_n|s, h_n)$ in Lemma 5.1 is,

$$\lim_{\sigma_{h_n} \to 0} \omega(y_n|s, h_n) = \frac{1}{|\mathcal{S}|} \iint_{\mathcal{S}} \lim_{\sigma_{h_n} \to 0} \frac{1}{2\pi\sigma_{h_n^2}} e^{-\frac{1}{\sigma_h^2}|u-u_z|^2} du, \tag{5.54}$$

$$= \frac{1}{|\mathcal{S}|} \iint_{\mathbb{R}^2} \mathbb{1}(u \in \mathbb{S}) \delta(u - u_z) du, \tag{5.55}$$

$$= \frac{1}{|\mathcal{S}|} \mathbb{1}(u_z \in \mathbb{S}). \tag{5.56}$$

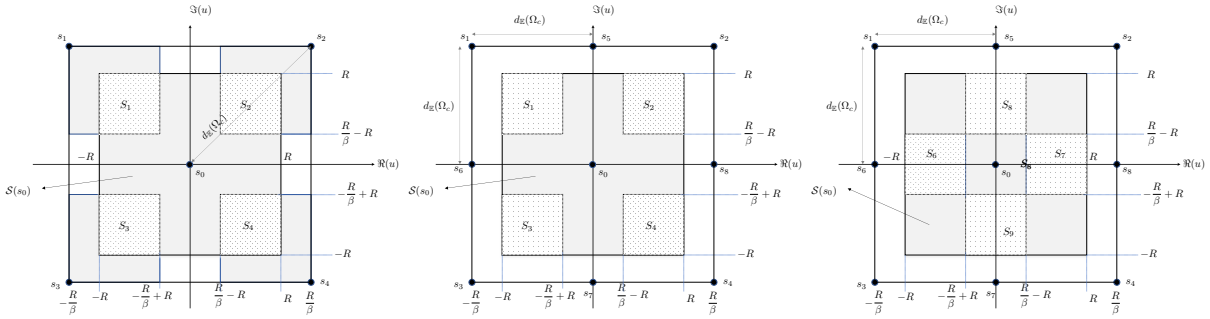
Let $\mathcal{N}_s$ be the set of symbols verifying that $u_z \in \mathcal{S}$. Given $s \in \mathcal{N}_s$, the condition $\mathbb{1}(u_z \in \mathcal{S})$ is equivalent to $\mathbb{1}(u_z \in \mathcal{S}_{(s,s_0)})$ with

$$\mathcal{S}_{(s,s_0)} = \{u_{r,\min} \leq \Re(u) \leq u_{r,\max}; u_{i,\min} \leq \Im(u) \leq u_{i,\max}\} \tag{5.57}$$

with $u_{r,\min} = \max\big(-R; -R - \sqrt{\theta P}\Re(s_0 - s)\big)$, $u_{r,\max} = \min\big(R; R - \sqrt{\theta P}\Re(s_0 - s)\big)$, $u_{i,\min} = \max\big(-R; -R - \sqrt{\theta P}\Im(s_0 - s)\big)$, $u_{i,\max} = \min\big(R; R - \sqrt{\theta P}\Im(s_0 - s)\big)$. These conditions are feasible if $\sqrt{\theta P}|\Re(s_0 - s)| < 2R$ and $\sqrt{\theta P}|\Im(s_0 - s)| < 2R$. Consequently,

$$\mathcal{N}_s = \{s : \Re(s) < \Re(s_0) \pm 2^{\ell/2}\beta d_{\min}, \Im(s) < \Im(s_0) \pm 2^{\ell/2}\beta d_{\min}, \}. \tag{5.58}$$

At the legitimate receiver, the computation of the mutual information $\mathrm{I}_b(\psi(\mathbf{b}_n), \mathbf{y}_n^{(b_n)}|\mathbf{k}_n)$ requires to



(a) $\ell = 1 : \mathcal{A}_r^{(\pm)} \cap \mathcal{A}_i^{(\pm)}$ (b) $\ell = 2 : \mathcal{A}_r^{(\pm)} \cap \mathcal{A}_i^{(\pm)}$ (c) $(\mathcal{A}_r^{(\pm)} \cap \overline{\mathcal{A}_i^{(\pm)}}) \cup (\overline{\mathcal{A}_r^{(\pm)}} \cap \mathcal{A}_i^{(\pm)})$

Figure 5.10: Eavesdropper decoding in Ω_c: Feasible region of u_z

compute:

$$\sum_{s\in\Lambda_{k_n}} \frac{\omega(y_n^{(b)}|s, h_n^{(b)})}{\omega(y_n^{(b)}|s_0, h_n^{(b)})} = 1 + \sum_{s\neq s_0 : s\in\Lambda_{k_n}} \mathbb{1}(u_z \in \mathbb{S}).$$

Given a partition Λ_{k_n} and $\forall s \neq s_0 \in \Lambda_{k_n}$, the set of potential symbols s that ensure that $u_z \in \mathcal{S}$ is empty as the closest points to s_0 are $s_0 - s = \pm 2^{\ell/2} d_{\min}$ or $s_0 - s = \pm(2^{\ell/2} d_{\min})1i$ with $2^{\ell/2} d_{\min} \geq \beta 2^{\ell/2} d_{\min}$. Consequently, $\sum_{s\neq s_0 : s\in\Lambda_{k_n}} \mathbb{1}(u_z \in \mathbb{S}) = 0$. The mutual information at the legitimate receiver is then,

$$\lim_{\sigma_h \to 0} \mathrm{I}_b(\psi(\mathbf{b}_n), \mathbf{y}_n^{(b)}|\mathbf{k}_n) \to (q - \ell)$$

At the eavesdropper receiver, the computation of the mutual information requires to compute:

$$F = \frac{\sum_{s\in\Omega_c} \omega(y_n^{(e)}|s, h_n^{(e)})}{\omega(y_n^{(e)}|s_0, h_n^{(e)}) + \sum_{k:\psi(\mathbf{b}_n|\mathbf{k}_n)\neq s_0} \omega(y_n^{(e)}|\psi(\mathbf{b}_n|\mathbf{k}_n), h_n^{(e)})}$$

Note first that due to (5.56)

$$\sum_{\mathbf{k}_n : \psi(\mathbf{b}_n|\mathbf{k}_n)\neq s_0} \omega(y_n^{(e)}|\psi(\mathbf{b}_n|\mathbf{k}_n), h_n^{(e)}) = \frac{1}{|\mathcal{S}|} \sum_{\mathbf{k}_n : \psi(\mathbf{b}_n|\mathbf{k}_n)\neq s_0} \mathbb{1}(u_{z,\mathbf{k}_n} \in \mathcal{S})$$

with $u_{z,\mathbf{k}_n} = \sqrt{\theta P}(\psi(\mathbf{b}_n|\mathbf{k}_n) - s_0) + u$. The bit labeling in Subsection 5.3.2 guarantees that $\sqrt{\theta P}|(\psi(\mathbf{b}_n|\mathbf{k}_n) - s_0)| > 2R$ for all cases except some particular cases that will be separately studied in the following.

In all the other cases, $\sum_{k_n:\psi(\mathbf{b}_n|\mathbf{k}_n)\neq s_0}\omega(y_n^{(e)}|\psi(\mathbf{b}_n|\mathbf{k}_n),h_n^{(e)})=0$ and

$$F=\sum_{s\in\Omega_c}\frac{\omega(y_n^{(e)}|s,h_n^{(e)})}{\omega(y_n^{(e)}|s_0,h_n^{(e)})}=1+\sum_{s\neq s_0:s\in\Omega_c}\mathbb{1}(u_z\in\mathbb{S}) \tag{5.59}$$

where $u_z=\sqrt{\theta P}(s_0-s)+u$. As in the previous case, we need to identify the set $\mathcal{N}_s$ of feasible symbols $s\in\Omega_c$ defined in (5.58) ensuring $u_z\in\mathcal{S}$. If $0\leq 2\beta<1$, then $\mathcal{N}_s=\emptyset$ as the distance between two symbols is at least $d_{\min}$. $\mathcal{N}_s$ is a non-empty set if $2\beta>1$. For $\ell=1$, the set of $s\in\Omega_c$ satisfying (5.58) is $\mathcal{N}_s=\{s_0+d_{\min}2^{-\frac{1}{2}}(\pm 1\pm 1i)\}$. For each $s\in\mathcal{N}_s$, we need to determine the area of variation of u according to (5.57). The corresponding regions are disjoint and are illustrated in Figure 5.10a and have identical area,

$$|S_i|=\left(2R-\frac{R}{\beta}\right)^2,\quad 1\leq i\leq 4$$

The value of F in (5.59) is then equal to 1 or 2, and can be written as,

$$F=\begin{cases}1 & u\notin\bigcup_{s\in\mathcal{N}_s}S_i,\\ 2 & u\in\bigcup_{s\in\mathcal{N}_s}S_i,\end{cases}$$

where $\bigcup_{s\in\mathcal{N}_s}R_i$ depends on the number of neighboring symbols around s_0, *i.e.*

$$\text{Prob}\left\{u\in\bigcup S_i\right\}=\sum_{s_0\in\Omega_c}\frac{1}{2^q}|\mathcal{N}(s_0)||S_i|=\mathbb{E}[|\mathcal{N}(s_0)|]\left(1-\frac{1}{2\beta}\right)^2 \tag{5.60}$$

where $N_a^{(e)}=\mathbb{E}[|\mathcal{N}_s(s_0)|]$ is the average number of neighbors around a point in Ω_c. It follows that,

$$\begin{aligned}\mathbb{E}(\log_2(F)) &= \log_2(2)\,\text{Prob}\left\{u\in\bigcup_{s\in\mathcal{N}_s}S_i\right\},\\ &= N_a^{(e)}\left(1-\frac{1}{2\beta}\right)^2,\end{aligned}$$

For the QPSK partitioned with one bit, the symbols around the origin, map the same information bit 0 or 1. This means that, $\sqrt{\theta P}|\psi(0|0)-\psi(0|1)|<2R$. In this case, $\sum_{k:\psi(\mathbf{b}_n|\mathbf{k}_n)}\omega(y_n^{(e)}|\psi(\mathbf{b}_n|\mathbf{k}_n),h_n^{(e)})=\frac{2}{|\mathcal{S}|}$. By repeating similar step as before,

$$\mathbb{E}[\log_2(F)]=\left(1-\frac{1}{2\beta}\right)^2. \tag{5.61}$$

For $\ell=2$, the set of $s\in\Omega_c$ satisfying (5.58) is:

$$\mathcal{N}_s=\{\pm d_{\min},\pm d_{\min}\times 1i,d_{\min}(\pm 1\pm 1i)\}.$$

As previously, the conditions in (5.57) are illustrated in Figure 5.10. In Figure 5.10a, the values of $s \in \mathcal{N}_s$ for which the conditions S_1 are satisfied are $s_0 + d_{\min}, s_0 + d_{\min}(1-1i), s_0 - d_{\min}1i$. In this case, $\sum_{s \neq s_0 : s \in \Omega_c} \mathbb{1}(u_z \in \mathbb{S}) = 3$ if the three neighbors are $\in \Omega_c$. In Figure 5.10b, the values of $s \in \mathcal{N}_s$ for which the conditions S_6 is satisfied for $s = s_0 + d_{\min}$. This means that $\sum_{s \neq s_0 : s \in \Omega_c} \mathbb{1}(u_z \in \mathbb{S}) = 1$. The value of F is then equal to 2 or 4. In the following, we identify the regions where $F = 2$ or $F = 4$ depending on the number of neighboring points. Let $\mathcal{N}_s$ denotes the set of neighbors around a given symbols s_0.

1. Case of $|\mathcal{N}_s| = 2$ (consider the right-lower quadrant) : The probability $\text{Prob}\{|\mathcal{N}_s| = 2\} = \frac{1}{2^{q-2}}$. In this case,
$$F = \begin{cases} 4 & u \in S_4 \\ 2 & u \in (S_3 \cup S_9) \cup (S_2 \cup S_7) \\ 1 & \text{otherwise} \end{cases}$$

2. Case of $|\mathcal{N}_s| = 3$ (consider the lower half in Figures 5.10b and 5.10c). The probability $\text{Prob}\{|\mathcal{N}_s| = 3\} = \frac{2(2^{\frac{q-2}{2}}-1)}{2^{q-2}}$. In this case,
$$F = \begin{cases} 4 & u \in (S_3 \cup S_4) \\ 2 & u \in (S_1 \cup S_6) \cup (S_9) \cup (S_3 \cup S_9) \cup (S_2 \cup S_7) \\ 1 & \text{otherwise} \end{cases}$$

3. Case of $|\mathcal{N}_s| = 4$. The probability $\text{Prob}\{|\mathcal{N}_s| = 4\} = \frac{(2^{\frac{q-2}{2}}-1)^2}{2^{q-2}}$. In this case,
$$F = \begin{cases} 4 & u \in S_1 \cup S_2 \cup S_3 \cup S_4 \\ 2 & u \in S_5 \cup S_6 \cup S_7 \cup S_8 \\ 1 & \text{otherwise} \end{cases}$$

By replacing the values of the disjoint surfaces by their values as, $|S_1| = |S_2| = |S_3| = |S_4| = (1 - \frac{1}{2\beta})^2$ and $|S_6| = |S_7| = |S_8| = |S_9| = 4R^2(\frac{1}{\beta} - 1)(1 - \frac{1}{2\beta})$ we can deduce that,

$$\mathbb{E}[\log_2(F)] = \bar{N}_a(1 - \frac{1}{2\beta}). \tag{5.62}$$

A correction term should be added to take into account the bit labeling, as there exist in the constellation 4 symbols in Ω_c around the origin $\pm 1 \pm 1i$ for which $\sqrt{\theta P}|(\psi(\mathbf{b}_n|\mathbf{k}_n) - s_0)| < 2R$. This can be observed for the 16QAM constellation in Figure 5.3b where $\sqrt{\theta P}|(\psi(10|11) - \psi(10|00))| < 2R$ and also $\sqrt{\theta P}|(\psi(01|10) - \psi(01|01))| < 2R$. This is also the case for a 64-QAM in Figure 5.5b where

$\sqrt{\theta P}|(\psi(1101|11)-\psi(1101|00))|<2R$ and also $\sqrt{\theta P}|(\psi(0111|10)-\psi(0111|01))|<2R$. In this case, $\sum_{k:\psi(\mathbf{b}|\mathbf{k})}\omega(y_n^{(e)}|\psi(\mathbf{b}_n|\mathbf{k}_n),h_n^{(e)})=\frac{2}{|\mathcal{S}|}$ and $F=\frac{1}{2}\sum_{s\neq s_0:s\in\Omega_c}\mathbb{1}(u_z\in\mathbb{S})$ on a single quadrant of Figure 5.10b. For this particular constellation symbol,

$$F=\begin{cases}4 & u\in S_1\cup S_2\cup S_3\\ 2 & u\in S_5\cup S_6\cup S_7\cup S_8\cup S_4\\ 1 & \text{otherwise}\end{cases}$$

When averaging over all constellation points in (5.62), a correction term should be added as,

$$\mathbb{E}[\log_2(F)]=\bar{N}_a\left(1-\frac{1}{2\beta}\right)-\frac{1}{2^{q-2}}\left(1-\frac{1}{2\beta}\right)^2$$

5.7.5 Proof of Lemma 5.3 on page 101

The variation of $\omega(y_n|s_0,h_n)$ in Lemma 5.2 as a function of $\nu=|u_z|$ is deduced from the derivative of $\omega(.)$ with respect to ν,

$$\frac{\partial\omega}{\partial\nu}=\frac{\partial\omega}{\partial u_{z,r}}\frac{\partial u_{z,r}}{\partial\nu}+\frac{\partial\omega}{\partial u_{z,i}}\frac{\partial u_{z,i}}{\partial\nu}.$$

By computing the partial derivatives,

$$\begin{aligned}\frac{\partial\omega}{\partial u_{z,r}} &= \frac{p_i}{4R^2}\Big(e^{-\frac{(R+\nu_r)^2}{\sigma_{h_n}^2}}-e^{-\frac{(R-u_{z,r})^2}{\sigma_{h_n}^2}}\Big),\\ p_i &= \Phi\left(\frac{R-u_{z,i}}{\sigma_{h_n}}\right)-\Phi\left(-\frac{R+u_{z,i}}{\sigma_{h_n}}\right),\\ \frac{\partial u_{z,r}}{\partial\nu} &= \frac{\nu}{u_{z,r}}.\end{aligned}$$

Note first that p_i is the probability that a Gaussian value to be bounded by two values and is then $0\leq p_i\leq 1$. If $u_{z,r}>0$, then, $\frac{\partial\omega}{\partial u_{z,r}}<0$ and $\frac{\partial u_{z,r}}{\partial\nu}>0$. If $u_{z,r}>0$, then, $\frac{\partial\omega}{\partial u_{z,r}}>0$ and $\frac{\partial u_{z,r}}{\partial\nu}<0$. This means that in both case cases $\frac{\partial\omega}{\partial u_{z,r}}\frac{\partial u_{z,r}}{\partial\nu}<0$. In a similar manner, $\frac{\partial\omega}{\partial u_{z,i}}\frac{\partial u_{z,i}}{\partial\nu}$ is also negative. Consequently, $\frac{\partial\omega}{\partial\nu}<0$. Maximizing the function $\omega(y_n|s_0,h_n)$ is then equivalent to minimize ν. At the legitimate receiver, the index k_n is assumed to be perfectly known. The MAP estimation is then performed within the alphabet Λ_{k_n}. At the eavesdropper, the estimated symbol resulting from the MAP decoding is

$$\hat{s}=\arg\min_k\min_{s\in\Lambda_k}|y-\sqrt{\theta P}h_n s|^2.$$

This is equivalent to search for the minimal distance in Ω_c.

5.7.6 Proof of Theorem 5.2 on page 103

The error probability at the eavesdropper can be written as,

$$\text{Prob}\{u_z \notin \mathcal{D}\} = \text{Prob}\{u_z \in \mathcal{S} \cap \bar{\mathcal{D}}\} + \text{Prob}\{u_z \in \bar{\mathcal{S}} \cap \bar{\mathcal{D}}\}.$$

In the high SNR regime, the uniform random noise is dominant and the error probability reduces to,

$$\lim_{\sigma \to 0} \text{Prob}\{u_z \notin \mathcal{D}\} = \text{Prob}\{u_z \in \mathcal{S} \cap \bar{\mathcal{D}}\} = \frac{|\mathcal{S} \cap \bar{\mathcal{D}}|}{|\mathcal{S}|},$$

where $|\mathcal{S}| = 4R^2$ and the area $|\mathcal{S} \cap \bar{\mathcal{D}}|$ is deduced from Figures 5.6a and 5.6b.

For $\ell = 1$, the average area depends on the average number of neighboring symbols in Ω_c and $|\mathcal{S} \cap \bar{\mathcal{D}}| = 2\bar{N}_a R^2 \left(1 - \frac{1}{2\beta}\right)^2$. Then, $\text{Prob}\{u_z \notin \mathcal{D}\} = \frac{2\bar{N}^{(e)} R^2 \left(1 - \frac{1}{2\beta}\right)^2}{4R^2}$ with $\bar{N}^{(e)}$ being the average number of neighbors in (5.7). The case of $\ell = 2$ is more complexe as the number of neighbors affects the area of $|\mathcal{S} \cap \bar{\mathcal{D}}|$ (not in a proportional way as for the previous case), as following:

$$|\mathcal{S} \cap \bar{\mathcal{D}}| = \begin{cases} A & \text{if } |\mathcal{N}(s_0)| = 4 \\ A - A_1 & \text{if } |\mathcal{N}(s_0)| = 3 \\ A - 2A_1 - A_2 & \text{if } |\mathcal{N}(s_0)| = 2. \end{cases}$$

with $A = R^2(4 - \frac{1}{\beta^2})$, $A_1 = \frac{R^2}{\beta}(1 - \frac{1}{2\beta})$ and $A_2 = R^2(1 - \frac{1}{2\beta})^2$. It follows that,

$$\mathbb{E}[|\mathcal{S} \cap \bar{\mathcal{D}}|] = A - A_1 \frac{2(2^{\frac{q-2}{2}} - 1)}{2^{q-2}} - 2A_1 \frac{1}{2^{q-2}} - A_2 \frac{1}{2^{q-2}}. \tag{5.63}$$

The strict symbol error probability is then,

$$\mathbb{P}_e^{(e,2)} = (1 - 2^{-q}) \left(1 - \frac{1}{2\beta}\right) \left(1 + \frac{1 - 2^{-q/2}}{1 + 2^{-q/2}} \frac{1}{2\beta}\right)$$

We should note that due to the proposed mapping in Figure 5.5b where $\sqrt{\theta P}|(\psi(1101|11) - \psi(1101|00))| < 2R$ and also $\sqrt{\theta P}|(\psi(0111|10) - \psi(0111|01))| < 2R$, the symbol error probability expression will not detect that these two symbols correspond to the same binary information sequence. To take into account this event, we should include this particular case that arises with probability $1/2^{q-2}$, for which $|\mathcal{S} \cap \bar{\mathcal{D}}| = A - A2$. By updating this expression,

$$\mathbb{E}[|\mathcal{S} \cap \bar{\mathcal{D}}|] = A - A_1 \frac{2(2^{\frac{q-2}{2}} - 1)}{2^{q-2}} - 2A_1 \frac{1}{2^{q-2}} - A_2 \frac{2}{2^{q-2}}.$$

A correction term should be then added to the symbol error probability as,

$$\mathbb{P}_{e,c} = \mathbb{P}_e^{(e,2)} - 2^{-q} \left(1 - \frac{1}{2\beta}\right)^2$$

5.7.7 Proof of Theorem 5.3 on page 103

Assuming that the number of neighbors is equal to 4, the correct decision probability is,

$$\mathrm{P}_c = \left(\frac{1}{2R} \int_{-\frac{R}{\beta}}^{+\frac{R}{\beta}} \left[\Phi\Big(\frac{R - u_{z,1}}{\sigma_h} \Big) - \Phi\Big(-\frac{R + u_{z,1}}{\sigma_h} \Big) \right] du_{z,1} \right)^2 .$$

The expansion of this integral leads to,

$$\mathrm{P}_c = \left(\frac{1}{2^{\ell/2+1}\beta} (\mathrm{P}_{c,1} + P_{c,2}) \right)^2$$

with

$$\mathrm{P}_{c,1} = \left[-\eta_m \operatorname{erf}\left(\eta_m \sqrt{\frac{\mathrm{SNR}_{h_n}}{2}} \right) + \eta_p \operatorname{erf}\left(\eta_p \sqrt{\frac{\mathrm{SNR}_{h_n}}{2}} \right) \right],$$

and

$$\mathrm{P}_{c,2} = \sqrt{\frac{2}{\pi\,\mathrm{SNR}}} \left[\exp\left(-\frac{\mu_p^2}{2} \mathrm{SNR}_{h_n} \right) - \exp\left(-\frac{\mu_m^2}{2} \mathrm{SNR}_{h_n} \right) \right].$$

This expression can be rewritten as,

$$\mathrm{P}_c = \Big(1 - (1 - \frac{1}{2^{\ell/2+1}\beta} (P_{c,1} + P_{c,2}) \Big)^2 = \Big(1 - \frac{1}{2^{\ell/2+1}\beta} (P_{e,1} + P_{e,2}) \Big)^2 \tag{5.64}$$

with $P_{e,1} = 2^{\ell/2+1}\beta - \mathrm{P}_{c,1}$ and $\mathrm{P}_{e,2} = -\mathrm{P}_{c,2}$ such that,

$$\begin{aligned} P_{e,1} =& 2^{\ell/2+1}\beta + \eta_m \operatorname{erf}\left(\eta_m \sqrt{\frac{\mathrm{SNR}}{2}} \right) - \eta_p \operatorname{erf}\left(\eta_p \sqrt{\frac{\mathrm{SNR}}{2}} \right) \\ =& \eta_p - \eta_m + \eta_m \operatorname{erf}\left(\eta_m \sqrt{\frac{\mathrm{SNR}}{2}} \right) - \eta_p \operatorname{erf}\left(\eta_p \sqrt{\frac{\mathrm{SNR}}{2}} \right) \\ =& 2\eta_p \mathcal{Q}(\eta_p \sqrt{\mathrm{SNR}}) - 2\eta_m \mathcal{Q}(\eta_m \sqrt{\mathrm{SNR}}). \end{aligned}$$

Finally, the error probability can be then rewritten as,

$$\mathrm{P}_e = 1 - \mathrm{P}_c = 1 - \Big(1 - \frac{1}{2^{\ell/2+1}\beta} (P_{e,1} + P_{e,2}) \Big)^2 .$$

This expression can be closely approximated by

$$\mathrm{P}_e \approx \frac{2}{2^{\ell/2+1}\beta} (P_{e,1} + P_{e,2}).$$

Due to the symmetry of the distribution function of u_z in Lemma 5.2, the average error probability considering the number of neighbors $|\mathcal{N}_s|$ is $\mathbb{P}_e = \mathrm{P}_e \times \mathrm{Prob}\{|\mathcal{N}_s| = 4\} + \frac{3}{4}\mathrm{P}_e \times \mathrm{Prob}\{|\mathcal{N}_s| = 3\} + \frac{2}{4}\mathrm{P}_e \times \mathrm{Prob}\{|\mathcal{N}_s| = 2\} + \frac{1}{4}\mathrm{P}_e \times \mathrm{Prob}\{|\mathcal{N}_s| = 1\} = \frac{\bar{N}^{(b)}}{4}\mathrm{P}_e$.

Chapter 6

Conclusion and Perspectives

Contenu

6.1 Conclusion

The title of this thesis is "**Enhanced Physical Layer Security through Frequency and Spatial Diversity**". In the first chapter of the thesis, we have presented the research motivations and the background that resulted in the different contributions of this dissertation. In the second chapter, we gave detailed explanations of the fundamental concepts of this thesis - PLS, Massive MIMO, OFDM and AI. Chapters 3 to 5 are the contribution chapters of this thesis.

In Chapter 3, we showed that injection of random AN leads to increase in the PAPR of the transmit signal. This is caused by the in-phase superposition of the information signal and the AN sub-spaces. More so, the large number of transmit antennas in massive MIMO leads to high-dimensional precoding matrix also leads to high-PAPR transmit signals. To address these limitations, we proposed in this thesis a novel algorithm referred to as "**PAPR-Aware-Secure-mMIMO**". In this scheme, instantaneous CSI is used to design a PAPR-Aware AN that jointly minimizes PAPR and maximizes security. The proposed transmission scheme transforms the PAPR reduction problem into a convex optimization problem which can be solved by an algorithm using real-time data via the GD approach. The clipping signals in the algorithm are used to design a PAPR-aware AN signal, thereby achieving both PAPR reduction and security enhancement. Using numerical simulations, we showed the performance gain

of our proposed scheme compared to legacy schemes with or without random AN injection in terms of PAPR, SER, secrecy capacity, and SEE. The proposed scheme achieved the same secrecy capacity as legacy scheme with random AN but at a significantly reduced PAPR performance and better SEE. We also showed that our proposed scheme is sensitive to the degree of spatial in a spatially correlated system.

The Chapter 4 of this thesis focused on channel adaption in PLS. We proposed a PLS scheme that uses instantaneous CSI to design an adaptive MF precoder and diversity that is suited for the legitimate receiver and not the eavesdropper. The channel independence between the main and wiretap channel leads to a security gap between Bob and Eve since Bob maintains the intended diversity gain and Eve loses the diversity gain. However, instantaneous CSI is difficult to obtain in practice due to such factors such as noisy CSI feedback, delayed CSI feedback, etc. Thus, we subsequently studied the impact of imperfect CSI due to noisy feedback on the secrecy performance of the PLS scheme. Finally, we proposed the use of a low-complexity denoising autoencoder to denoise the noisy CSI and the denoised CSI is then use for the PLS scheme. Secrecy gains of the scheme was shown in terms of BER and secrecy capacity. We showed that the hybrid version of the proposed autoencoder, referred to as "**HybDenoiseSecNet**" had a significantly reduced computational complexity compared to the deep autoencodder ('**DenoiseSecNet**") and other legacy denoising schemes such as truncation and universal threshold schemes.

Most PLS schemes adopt Gaussian input signaling. However, the detection complexity of Gaussian signals is high as it takes a continuum of values. In addition to this, the amplitude of Gaussian signals are unbounded, so Gaussian signaling is typically not used in practice. Typically, the channel inputs in practice are drawn from a discrete signal constellation such as QPSK, QAM, etc. To this end, we proposed a finite-alphabet PLS scheme referred to as **IPM**. IPM selects a unique image in a partitioned constellation based on dynamic keys known only to Alice and Bob. In order to map the information bits into symbols, we defined a cross-labelling. As the eavesdropper is unaware of the index, it decreases the size of the detection zone compared to the legitimate receiver. To further cause confusion at the eavesdropper, we inject uniform AN that keeps the received symbol within the detection zones of Bob but induce more confusion at the already smaller detection zones of Eve. Performance evaluation is done in terms of mutual information, secrecy rate and BER and it was established that compared to the noiseless IPM scheme and other legacy schemes, the noisy IPM outperformed all others.

6.2 Suggestions for Future Work

PLS is an emerging topic which still presents numerous challenges and research potentials. The adoption of PLS in emerging areas such as massive MIMO [143], IRS [144], AI [145], terahertz communications [146] etc. remains open to contributions. Distance from users is a major drawback of conventional massive MIMO, since different users experience large variations of received signal strength [143]. Typically, an expensive massive MIMO BS is placed in an elevated location to increase the cell radius and cover a large number of UE. Cell-free comes to the rescue by having antennnas, which are controlled by a central processing unit, distributed among different locations and eliminating the need for the cell-based deployment. An important aspect of the contribution in Chapter 3 is the optimal power allocation ratio between information signal and AN. However, if the UE do not receive the same signal strength, this could have a direct impact on the optimal power allocation from the BS. It will be interesting to study the PAPR-Aware-Secure-mMIMO in a cell-free massive MIMO deployment. Again, as shown in Chapter 3, the proposed PAPR-Aware-Secure-AN is sensitive to spatial correlation. Spatial correlation is also a known challenge in massive MIMO. In essence, it is expedient to optimize either the precoding technique or the algorithm itself to account for correlated fading and ensure that the performance of Bob remains immune to the effects of correlation.

AI in PLS is a topic with numerous potentials for breakthroughs in PLS. We considered noisy CSI of equal variance across all subcarriers in Chapter 4. It is possible in practice to have variable noise variance across spectral or temporal domains. This will increase the approach to learning of the proposed deep learning model. It will also important to develop a deep learning model for the PAPR-Aware-Secure-mMIMO algorithm. A comparative study of the performance and complexity of both conventional and AI approaches is suggested. In Chapter 5, the injection of uniform AN in noisy IPM optimized the secrecy performance but could have an effect on the PAPR performance of the scheme. It is interesting to study the effect of the power allocation ratio on the PAPR performance which will result in a proposal of a modified scheme that achieves optimal secrecy and energy efficiency simultaneously.

Bibliography

[1] H. J. Patil et Y. P. Surwades, "Web technologies from web 2.0 to web 4.0," *International Journal for Science and Advance Research In Technology*, vol. 4, n°. 4, p. 810–814, 2018.

[2] L. Gyongyosi et S. Imre, "A survey on quantum computing technology," *Computer Science Review*, vol. 31, p. 51–71, 2019.

[3] P. Angueira, I. Val, J. Montalbán, O. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari et A. Arriola, "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Communications Surveys and Tutorials*, vol. 24, n°. 2, p. 810–838, 2022.

[4] J. M. Hamamreh, H. M. Furqan et H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 21, n°. 2, p. 1773–1828, 2019.

[5] O. G. Abood et S. K. Guirguis, "A survey on cryptography algorithms," *International Journal of Scientific and Research Publications*, vol. 8, n°. 7, p. 495–516, 2018.

[6] J. Barros et M. R. D. Rodrigues, "Secrecy capacity of wireless channels," dans *2006 IEEE International Symposium on Information Theory*, 2006, p. 356–360.

[7] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Transactions on Wireless Communications*, vol. 9, n°. 11, p. 3590–3600, 2010.

[8] J. Tan et L. Dai, "Channel feedback in TDD massive MIMO systems with partial reciprocity," *IEEE Transactions on Vehicular Technology*, vol. 70, n°. 12, p. 12 960–12 974, 2021.

[9] Q. Qin, L. Gui, B. Gong et S. Luo, "Sparse channel estimation for massive MIMO-OFDM systems over time-varying channels," *IEEE Access*, vol. 6, p. 33 740–33 751, 2018.

[10] X. Jiang et F. Kaltenberger, "Channel reciprocity calibration in TDD hybrid beamforming massive MIMO systems," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, n°. 3, p. 422–431, 2018.

[11] G. Chen, Q. Zeng, X. Xue et Z. Li, "A low complexity precoding algorithm based on parallel conjugate gradient for massive MIMO systems," *IEEE Access*, vol. 6, p. 54 010–54 017, 2018.

[12] C. Zhang, Z. Li, L. Shen, F. Yan, M. Wu et X. Wang, "A low-complexity massive MIMO precoding algorithm based on chebyshev iteration," *IEEE Access*, vol. 5, p. 22 545–22 551, 2017.

[13] J. C. A. Barata et M. S. Hussein, "The moore–penrose pseudoinverse: A tutorial review of the theory," dans *Brazilian Journal of Physics*, vol. 42, n°. 1-2, 2012, p. 146–165.

[14] X. Qin, Z. Yan et G. He, "A near-optimal detection scheme based on joint steepest descent and Jacobi method for uplink massive MIMO systems," *IEEE Communications Letters*, vol. 20, n°. 2, p. 276–279, 2016.

[15] W. Wan, "Implementing online natural gradient learning: problems and solutions," *IEEE Transactions on Neural Networks*, vol. 17, n°. 2, p. 317–329, 2006.

[16] G. Golub et C. van Loan, *Matrix Computations*. 3rd ed. Stockholm, Sweden: Johns Hopkins Univ, 2012.

[17] H. Li, T. Jiang et Y. Zhou, "An improved tone reservation scheme with fast convergence for PAPR reduction in OFDM systems," *IEEE Transactions on Broadcasting*, vol. 57, n°. 4, p. 902–906, 2011.

[18] J. Zhu, R. Schober et V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 13, n°. 9, p. 4766–4781, 2014.

[19] M. A. Rao, A. Jehangir, S. Mustafa, M. N. Sohail et U. R. Ateeq, "Energy efficiency augmentation in massive MIMO systems through linear precoding schemes and power consumption modeling," *Wireless Communications and Mobile Computing*, p. 1–13, 2020.

[20] F. Pan, Z. Pang, M. Luvisotto, M. Xiao et H. Wen, "Physical-layer security for industrial wireless control systems: Basics and future directions," *IEEE Industrial Electronics Magazine*, vol. 12, n°. 4, p. 18–27, 2018.

[21] K. Cho et D. Yoon, "On the general BER expression of one- and two-dimensional amplitude modulations," *IEEE Transactions on Communications*, vol. 50, n°. 7, p. 1074–1080, 2002.

[22] Y. Bengio, L. Yao, G. Alain et P. Vincent, "Generalized denoising auto-encoders as generative models," dans *26th International Conference on Neural Information Processing Systems*, ser. NIPS'13, vol. 1, 2013, p. 899–907.

[23] K. He, X. Zhang, S. Ren et J. Sun, "Deep residual learning for image recognition," dans *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, p. 770–778.

[24] R. Liaw, E. Liang, R. Nishihara, P. Moritz, J. E. Gonzalez et I. Stoica, "Tune: A research platform for distributed model selection and training," *arXiv preprint arXiv:1807.05118*, 2018.

[25] H. Ye, F. Gao, J. Qian, H. Wang et G. Y. Li, "Deep learning-based denoise network for CSI feedback in FDD massive MIMO systems," *IEEE Communications Letters*, vol. 24, n°. 8, p. 1742–1746, 2020.

[26] W. J. Jr., "Microwave mobile communications," dans *Wiley-Interscience, New York*, 1974.

[27] Techplayon, "What is PAPR (peak to average power ratio), why it matters to power amplifier ?" Techplayon, Rapport technique, 2017.

[28] Samsung, "Massive MIMO, key technology for enhancing 5G network capacity and user experiences, will continue to be essential driver for 5g build-out," Samsung, Rapport technique, 2020.

[29] R. A. Bakr, E. S. Hassan, G. A. Hussein, I. M. Eldokany, S. El-Dolil, O. Oraby et F. E. A. El-Samie, "Continuous phase modulation with chaotic interleaving for optical OFDM systems," *Optical and Quantum Electronics*, vol. 47, n°. 8, p. 2489–2506, 2015. [En ligne]. Disponible: https://doi.org/10.1007/s11082-015-0130-5

[30] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, n°. 8, p. 1335–1387, 1975.

[31] A. Subramanian, A. T. Suresh, S. Raj, A. Thangaraj, M. Bloch et S. McLaughlin, "Strong and weak secrecy in wiretap channels," dans *2010 6th International Symposium on Turbo Codes & Iterative Information Processing*, 2010, p. 30–34.

[32] S. Goel et R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, n°. 6, p. 2180–2189, 2008.

[33] S. Hong, C. Pan, H. Ren, K. Wang et A. Nallanathan, "Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface," *IEEE Transactions on Communications*, vol. 68, n°. 12, p. 7851–7866, 2020.

[34] B. He, Y. She et V. K. N. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Transactions on Vehicular Technology*, vol. 66, n°. 10, p. 9577–9581, 2017.

[35] B. Li, M. Zhang, Y. Rong et Z. Han, "Artificial noise-aided secure relay communication with unknown channel knowledge of eavesdropper," *IEEE Transactions on Wireless Communications*, vol. 20, n°. 5, p. 3168–3179, 2021.

[36] W. Liu, M. Li, X. Tian, Z. Wang et Q. Liu, "Transmit filter and artificial noise design for secure MIMO-OFDM systems," *ArXiv*, vol. abs/1704.08007, 2017.

[37] M. Bloch, J. Barros, M. R. D. Rodrigues et S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, n°. 6, p. 2515–2534, 2008.

[38] Y. Liang, H. V. Poor et S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, n°. 6, p. 2470–2492, 2008.

[39] P. K. Gopala, L. Lai et H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, n°. 10, p. 4687–4698, 2008.

[40] E. Güvenkaya et H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," dans *2014 IEEE International Conference on Communications Workshops (ICC)*, 2014, p. 813–818.

[41] J. M. Hamamreh, E. Basar et H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, vol. 5, p. 25 863–25 875, 2017.

[42] S. Liang, Z. Fang, G. Sun et J. Zhang, "A physical layer security approach based on optical beamforming for indoor visible light communication," *IEEE Communications Letters*, vol. 24, n°. 10, p. 2109–2113, 2020.

[43] C. D. T. Thai, "Beamforming and jamming for physical-layer security with different trust degrees," *AEU - International Journal of Electronics and Communications*, vol. 128, p. 153458, 2021.

[44] J. Song, B. Lee, J. Park, M.-S. Lee et J.-H. Lee, "Beamformer design for physical layer security in dual-polarized millimeter wave channels," *IEEE Transactions on Vehicular Technology*, vol. 69, n°. 10, p. 12 306–12 311, 2020.

[45] A. Nooraiepour et T. M. Duman, "Randomized serially concatenated LDGM codes for the gaussian wiretap channel," *IEEE Communications Letters*, vol. 22, n°. 4, p. 680–683, 2018.

[46] Y. Masuda, E. Okamoto et T. Yamamoto, "Low complexity decoding of downlink chaos NOMA scheme with physical layer security," dans *2020 IEEE 17th Annual Consumer Communications Networking Conference (CCNC)*, 2020, p. 1–6.

[47] S. Karachontzitis, S. Timotheou, I. Krikidis et K. Berberidis, "Security-aware max–min resource allocation in multiuser OFDMA downlink," *IEEE Transactions on Information Forensics and Security*, vol. 10, n°. 3, p. 529–542, 2015.

[48] S. A. G. Shirazi, "Impact of a time-varying rician fading channel on the performance of alamouti transmit diversity technique," dans *2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2007, p. 1–4.

[49] S. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 16, n°. 8, p. 1451–1458, 1998.

[50] M. Damen, K. Abed-Meraim et J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Transactions on Information Theory*, vol. 48, n°. 3, p. 628–636, 2002.

[51] T. Allen, J. Cheng et N. Al-Dhahir, "Secure space-time block coding without transmitter CSI," *IEEE Wireless Communications Letters*, vol. 3, n°. 6, p. 573–576, 2014.

[52] P. O. Akuon et H. Xu, "Secure signal and space alamouti scheme," *SAIEE Africa Research Journal*, vol. 107, n°. 4, p. 237–244, 2016.

[53] M. Yusuf et H. Arslan, "Enhancing physical-layer security in wireless communications using signal space diversity," dans *MILCOM 2016 - 2016 IEEE Military Communications Conference*, 2016, p. 1190–1194.

[54] R. S. P. Cruz et M. B. Loiola, "Wireless physical-layer security using precoding and an active eavesdropper," *Brazilian Telecommunication Symposium and Signal Processing*, 2017.

[55] J. M. Hamamreh, E. Guvenkaya, T. Baykas et H. Arslan, "A practical physical-layer security method for precoded OSTBC-based systems," dans *2016 IEEE Wireless Communications and Networking Conference*, 2016, p. 1–6.

[56] S. J. Maeng, Y. Yapici, I. Guvenc, H. Dai et A. Bhuyan, "Precoder design for mmwave UAV communications with physical layer security," dans *2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2020, p. 1–5.

[57] A. Mayouche, D. Spano, C. G. Tsinos, S. Chatzinotas et B. Ottersten, "Learning-assisted eavesdropping and symbol-level precoding countermeasures for downlink MU-MISO systems," *IEEE Open Journal of the Communications Society*, vol. 1, p. 535–549, 2020.

[58] T.-H. Nguyen, J. Louveaux, P. De Doncker et F. Horlin, "Performance analysis of matched-filter precoded MISO-OFDM systems in the presence of imperfect CSI," dans *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, p. 1–5.

[59] A. Al-nahari, "Physical layer security using massive multiple-input and multiple-output: passive and active eavesdroppers," *The Institution of Engineering and Technology Communications*, vol. 10, p. 50–56, 2016.

[60] J. Zhu, R. Schober et V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 13, n°. 9, p. 4766–4781, 2014.

[61] N.-P. Nguyen, H. Q. Ngo, T. Q. Duong, H. D. Tuan et K. Tourki, "Secure massive MIMO with the artificial noise-aided downlink training," *IEEE Journal on Selected Areas in Communications*, vol. 36, n°. 4, p. 802–816, 2018.

[62] C. H. Bennett, G. Brassard et J.-M. Robert, "Privacy amplification by public discussion," *SIAM Journal on Computing*, vol. 17, n°. 2, p. 210–229, 1988.

[63] U. Maurer et S. Wolf, "Secret-key agreement over unauthenticated public channels .i. definitions and a completeness result," *IEEE Transactions on Information Theory*, vol. 49, n°. 4, p. 822–831, 2003.

[64] ——, "Secret-key agreement over unauthenticated public channels-part ii: the simulatability condition," *IEEE Transactions on Information Theory*, vol. 49, n°. 4, p. 832–838, 2003.

[65] ——, "Secret-key agreement over unauthenticated public channels .ii. privacy amplification," *IEEE Transactions on Information Theory*, vol. 49, n°. 4, p. 839–851, 2003.

[66] T. Wang, Y. Liu et A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, vol. 21, n°. 6, p. 1835–1846, 2015.

[67] R. Frenkiel, "A high-capacity mobile radiotelephone system model using a coordinated small-zone approach," *IEEE Transactions on Vehicular Technology*, vol. 19, n°. 2, p. 173–177, 1970.

[68] W. R. Young, "Advanced mobile phone service: Introduction, background, and objectives," *The Bell System Technical Journal*, vol. 58, n°. 1, p. 1–14, 1979.

[69] E. Björnson, J. Hoydis et L. Sanguinetti, "Massive MIMO networks: Spectral, energy, and hardware efficiency," *Foundations and Trends in Signal Processing*, vol. 11, n°. 3-4, p. 154–655, 2017.

[70] H. Q. Ngo, E. G. Larsson et T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Transactions on Communications*, vol. 61, n°. 4, p. 1436–1449, 2013.

[71] E. G. Larsson, O. Edfors, F. Tufvesson et T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Communications Magazine*, vol. 52, n°. 2, p. 186–195, 2014.

[72] X. Rao et V. K. N. Lau, "Distributed compressive CSIT estimation and feedback for FDD multi-user massive MIMO systems," *IEEE Transactions on Signal Processing*, vol. 62, n°. 12, p. 3261–3271, 2014.

[73] J. Choi, D. J. Love et P. Bidigare, "Downlink training techniques for FDD massive MIMO systems: Open-loop and closed-loop training with memory," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, n°. 5, p. 802–814, 2014.

[74] J. Chen et V. K. N. Lau, "Two-tier precoding for FDD multi-cell massive MIMO time-varying interference networks," *IEEE Journal on Selected Areas in Communications*, vol. 32, n°. 6, p. 1230–1238, 2014.

[75] A. Adhikary, J. Nam, J.-Y. Ahn et G. Caire, "Joint spatial division and multiplexing—the large-scale array regime," *IEEE Transactions on Information Theory*, vol. 59, n°. 10, p. 6441–6463, 2013.

[76] F. Hu, Y. Lu, L. Jin, Z. Xia, G. Zhang et J. Xiao, "Hybrid energy efficiency friendly frequency domain TR algorithm based on PSO algorithm evaluated by novel maximizing HPA efficiency evaluation criteria," *Energies*, vol. 15, n°. 917, p. 1–19, 2022.

[77] S. P. Yadav et S. C. Bera, "Nonlinearity effect of power amplifiers in wireless communication systems," dans *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, 2014, p. 12–17.

[78] C. Mollen, E. G. Larsson et T. Eriksson, "Waveforms for the massive MIMO downlink: Amplifier efficiency, distortion, and performance," *IEEE Transactions on Communications*, vol. 64, n°. 12, p. 5050–5063, 2016.

[79] S. Weinstein et P. Ebert, "Data transmission by frequency-division multiplexing using the discrete fourier transform," *IEEE Transactions on Communication Technology*, vol. 19, n°. 5, p. 628–634, 1971.

[80] J. W. Cooley et J. W. Tukey, "An algorithm for the machine calculation of complex fourier series," *Mathematics of Computation*, vol. 19, n°. 90, p. 297–301, 1965.

[81] R. Saravanan et P. Sujatha, "A state of art techniques on machine learning algorithms: A perspective of supervised learning approaches in data classification," dans *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2018, p. 945–949.

[82] M. A. El Mrabet, K. El Makkaoui et A. Faize, "Supervised machine learning: A survey," dans *2021 4th International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2021, p. 1–10.

[83] K. Kontolati, D. Loukrezis, D. G. Giovanis, L. Vandanapu et M. D. Shields, "A survey of unsupervised learning methods for high-dimensional uncertainty quantification in black-box-type problems," *Journal of Computational Physics*, vol. 464, p. 111313, 2022.

[84] X. Wang, S. Wang, X. Liang, D. Zhao, J. Huang, X. Xu, B. Dai et Q. Miao, "Deep reinforcement learning: A survey," *IEEE Transactions on Neural Networks and Learning Systems*, p. 1–15, 2022.

[85] P. Domingos, "A few useful things to know about machine learning," *Communications of the ACM*, vol. 55, n°. 10, p. 78–87, 2012.

[86] Y. LeCun, Y. Bengio et G. Hinton, "Deep learning," *Nature 521*, p. 436–444, 2015.

[87] C. Zhang, P. Zhou, C. Li et L. Liu, "A convolutional neural network for leaves recognition using data augmentation," dans *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, 2015, p. 2143–2150.

[88] R. Socher, Y. Bengio et C. D. Manning, "Deep learning for NLP (without magic)," dans *Proceedings of the 50th Annual Meeting of the Association for Computational Linguistics: Tutorial Abstracts*. Jeju Island, Korea: Association for Computational Linguistics, juill. 2012, p. 5. [En ligne]. Disponible: https://aclanthology.org/P12-4005

[89] S. Rajendran, W. Meert, D. Giustiniano, V. Lenders et S. Pollin, "Deep learning models for wireless signal classification with distributed low-cost spectrum sensors," *IEEE Transactions on Cognitive Communications and Networking*, vol. 4, n°. 3, p. 433–445, 2018.

[90] T. O'Shea et J. Hoydis, "An introduction to deep learning for the physical layer," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, n°. 4, p. 563–575, 2017.

[91] H. Ye, G. Y. Li et B.-H. Juang, "Power of deep learning for channel estimation and signal detection in OFDM systems," *IEEE Wireless Communications Letters*, vol. 7, n°. 1, p. 114–117, 2018.

[92] W. Lyu, Z. Zhang, C. Jiao, K. Qin et H. Zhang, “Performance evaluation of channel decoding with deep neural networks,” dans *2018 IEEE International Conference on Communications (ICC)*, 2018, p. 1–6.

[93] D. Cassioli, R.-F. Liao, H. Wen, J. Wu, H. Song, F. Pan et L. Dong, “Power of deep learning for channel estimation and signal detection in OFDM systems,” *Wireless Communications and Mobile Computing*, vol. 2018, p. 6497340, 2018.

[94] C. Zhang, P. Patras et H. Haddadi, “Deep learning in mobile and wireless networking: A survey,” *IEEE Communications Surveys and Tutorials*, vol. 21, n°. 3, p. 2224–2287, 2019.

[95] M. Chen, U. Challita, W. Saad, C. Yin et M. Debbah, “Artificial neural networks-based machine learning for wireless networks: A tutorial,” *IEEE Communications Surveys and Tutorials*, vol. 21, n°. 4, p. 3039–3071, 2019.

[96] Q. Mao, F. Hu et Q. Hao, “Deep learning for intelligent wireless networks: A comprehensive survey,” *IEEE Communications Surveys and Tutorials*, vol. 20, n°. 4, p. 2595–2621, 2018.

[97] T. Hong et Z.-P. Li, “Peak-to-average power ratio reduction for an artificial noise aided secure communication system,” dans *2016 3rd International Conference on Information Science and Control Engineering (ICISCE)*, 2016, p. 1370–1374.

[98] J. M. Hamamreh et H. Arslan, “Joint PHY/MAC layer security design using ARQ with MRC and null-space independent PAPR-aware artificial noise in SISO systems,” *IEEE Transactions on Wireless Communications*, vol. 17, n°. 9, p. 6190–6204, 2018.

[99] T. Hong et G. Zhang, “Power allocation for reducing PAPR of artificial-noise-aided secure communication system,” dans *Hindawi Mobile Information Systems*, 2020, p. 1–15.

[100] S.-H. Tsai et H. V. Poor, “Power allocation for artificial-noise secure MIMO precoding systems,” *IEEE Transactions on Signal Processing*, vol. 62, n°. 13, p. 3479–3493, 2014.

[101] P. Colantonio, F. Giannini, R. Giofre et L. Piazzon, “The doherty power amplifier”, in advanced microwave circuits and systems,” *Advanced Microwave Circuits and Systems. London, United Kingdom*, 2010.

[102] R. Zayani, H. Shaiek et D. Roviras, "PAPR-aware massive MIMO-OFDM downlink," *IEEE Access*, vol. 7, p. 25 474–25 484, 2019.

[103] H. Q. Ngo, E. G. Larsson et T. L. Marzetta, "Aspects of favorable propagation in massive MIMO," dans *2014 22nd European Signal Processing Conference (EUSIPCO)*, 2014, p. 76–80.

[104] A. A. Alammari et M. Sharique, "Spatial channel correlation for local scattering with linear MMSE-based estimator and detector in multi-cell large scale MU-MIMO networks," *Trans. on Emerging Telecommunications Technologies*, vol. 32, n°. 12, 2021.

[105] H. Yin, D. Gesbert, M. Filippou et Y. Liu, "A coordinated approach to channel estimation in large-scale multiple-antenna systems," *IEEE Journal on Sel. Areas in Comm.*, vol. 31, n°. 2, p. 264–273, 2013.

[106] P. Jolanta et H. Thomas, "Mixtures of traces of Wishart and inverse Wishart matrices," vol. 50, p. 1–17, 2021.

[107] J. M. Robb, *Aspects of Multivariate Statistical Theory, Chapter 3*, 2005.

[108] A. Goldsmith et K. (Firm), *Wireless Communications*, ser. Cambridge Core. Cambridge University Press, 2005. [En ligne]. Disponible: https://books.google.fr/books?id=n-3ZZ9i0s-cC

[109] L. T. Yang, R. Zhang; X. Cheng, "Secure massive MIMO under imperfect CSI: Performance analysis and channel prediction," *IEEE Transactions on Information Forensics and Security*, vol. 14, p. 1610– 1623, 2018.

[110] H. Zhao, Y.-y. Tan, G.-f. Pan et Y.-f. Chen, "Ergodic secrecy capacity of MRC/SC in single-input multiple-output wiretap systems with imperfect channel state information," *Frontiers of Information Technology and Electronic Engineering*, vol. 18, n°. 4, p. 578 – 590, 2017.

[111] T. Yang, R. Zhang, X. Cheng et L. Yang, "Performance analysis of secure communication in massive MIMO with imperfect channel state information," dans *2018 IEEE International Conference on Communications (ICC)*, 2018, p. 1–6.

[112] R. Kumar et S. S. Chauhan, "Physical layer security for multiuser multi-eavesdropper multi-input multi-output (MIMO) system in the presence of imperfect feedback," *International Journal of Communication Systems*, vol. 33, n°. 17, p. e4604, 2020.

[113] C. T. Dung, L. X. Hung, T. M. Hoang, H. Van Toan et L. T. Dung, "Secrecy performance analysis for MIMO relay system with transmit/receive antenna selection under imperfect CSI," dans *2020 International Conference on Advanced Technologies for Communications (ATC)*, 2020, p. 106–110.

[114] M. A. A. Hyadi, Z. Rezki, "An overview of physical layer security in wireless communication systems with CSIT uncertainty," *The Bell System Technical Journal*, vol. 4, p. 6121– 6132, 2016.

[115] P. Sure et C. M. Bhuma, "A survey on OFDM channel estimation techniques based on denoising strategies," *Engineering Science and Technology, an International Journal*, vol. 20, n°. 2, p. 629–636, 2017.

[116] Z. Xiao, Z. Mingtong et W. Chengyou, "Iterative threshold channel estimation in ORGV convolutional code MISO-OFDM system," *IETE Technical Review*, p. 1–16, 2021.

[117] H. Xie, G. Andrieux, Y. Wang, J.-F. Diouris et S. Feng, "Efficient time domain threshold for sparse channel estimation in OFDM system," *International Journal of Electronics and Communications*, vol. 68, n°. 4, avr. 2014.

[118] S. Tuffery, "Deep learning: From big data to artificial intelligence with R: Deep learning for natural language processing," p. 431–478, 2023.

[119] N. Le, V. S. Rathour, K. Yamazaki, K. Luu et M. Savvides, "Deep reinforcement learning in computer vision: a comprehensive survey," *Artificial Intelligence Review*, vol. 55, n°. 4, p. 2733–2819, 2022.

[120] T. Zhou, H. Zhang, B. Ai, C. Xue et L. Liu, "Deep-learning-based spatial–temporal channel prediction for smart high-speed railway communication networks," *IEEE Transactions on Wireless Communications*, vol. 21, n°. 7, p. 5333–5345, 2022.

[121] V. Rizzello et W. Utschick, "Learning the CSI denoising and feedback without supervision," dans *2021 IEEE 22nd International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2021, p. 16–20.

[122] G. Klambauer, T. Unterthiner, A. Mayr et S. Hochreiter, "Self-normalizing neural networks," dans *26th International Conference on Neural Information Processing Systems*, vol. 1, 2017, p. 899–907.

[123] A. K. Gizzini, M. Chafii, A. Nimr et G. Fettweis, "Deep learning based channel estimation schemes for IEEE 802.11p standard," *IEEE Access*, vol. 8, p. 113 751–113 765, 2020.

[124] P. Yadav, S. Kumar et R. Kumar, "A comprehensive survey of physical layer security over fading channels: Classifications, applications, and challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 32, n°. 9, p. e4270, 2021. [En ligne]. Disponible: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4270

[125] T. Pollet, M. Van Bladel et M. Moeneclaey, "BER sensitivity of OFDM systems to carrier frequency offset and wiener phase noise," *IEEE Transactions on Communications*, vol. 43, n°. 2/3/4, p. 191–193, 1995.

[126] M. Yusuf et H. Arslan, "Controlled inter-carrier interference for physical layer security in OFDM systems," dans *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, 2016, p. 1–5.

[127] H. Li, X. Wang et J.-Y. Chouinard, "Eavesdropping-resilient OFDM system using sorted subcarrier interleaving," *IEEE Transactions on Wireless Communications*, vol. 14, n°. 2, p. 1155–1165, 2015.

[128] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, M. Zhao et J. Wang, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Transactions on Wireless Communications*, vol. 12, n°. 6, p. 2717–2729, 2013.

[129] M. Yusuf et H. Arslan, "On signal space diversity: An adaptive interleaver for enhancing physical layer security in frequency selective fading channels," *Physical Communication*, vol. 24, p. 154–160, 2017.

[130] T. Akitaya, S. Asano et T. Saba, "Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems," dans *2014 IEEE International Conference on Communications Workshops (ICC)*, 2014, p. 807–812.

[131] F. Renna, N. Laurenti et H. V. Poor, "Achievable secrecy rates for wiretap OFDM with QAM constellations," dans *Proceedings of the 5th International ICST Conference on Performance Evaluation Methodologies and Tools*, ser. VALUETOOLS '11. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2011, p. 679–686.

[132] Z. Mheich, F. Alberge et P. Duhamel, "Achievable secrecy rates for the broadcast channel with confidential message and finite constellation inputs," *IEEE Transactions on Communications*, vol. 63, n°. 1, p. 195–205, 2015.

[133] T. Allen, A. Tajer et N. Al-Dhahir, "Secure alamouti MAC transmissions," *IEEE Transactions on Wireless Communications*, vol. 16, n°. 6, p. 3674–3687, 2017.

[134] J. Jin, C. Xiao, M. Tao et W. Chen, "Linear precoding for cognitive multiple access wiretap channel with finite-alphabet inputs," dans *2016 IEEE International Conference on Communications (ICC)*, 2016, p. 1–6.

[135] W. Zeng, Y. R. Zheng et C. Xiao, "Multiantenna secure cognitive radio networks with finite-alphabet inputs: A global optimization approach for precoder design," *IEEE Transactions on Wireless Communications*, vol. 15, n°. 4, p. 3044–3057, 2016.

[136] K. Cao, Y. Cai, Y. Wu, W. Yang et X. Guan, "Secure communication for MISO secrecy channel with multiple multiantenna eavesdroppers having finite alphabet inputs," *IEEE Access*, vol. 6, p. 7402–7411, 2018.

[137] K. Cao, Y. Cai, Y. Wu et W. Yang, "Cooperative jamming for secure communication with finite alphabet inputs," *IEEE Communications Letters*, vol. 21, n°. 9, p. 2025–2028, 2017.

[138] K. Cao, Y. Wu, Y. Cai et W. Yang, "Secure transmission with aid of a helper for MIMOME network having finite alphabet inputs," *IEEE Access*, vol. 5, p. 3698–3708, 2017.

[139] Y. E. H. Shehadeh et D. Hogrefe, "An optimal guard-intervals based mechanism for key generation from multipath wireless channels," dans *2011 4th IFIP International Conference on New Technologies, Mobility and Security*. IEEE, 2011, p. 1–5.

[140] Y. Wu, Y. Yu, Y. Hu, Y. Sun, T. Wang et Q. Zhang, "Channel-based dynamic key generation for physical layer security in OFDM-PON systems," *IEEE Photonics Journal*, vol. 13, n°. 2, p. 1–9, 2021.

[141] H. M. Furqan, J. M. Hamamreh et H. Arslan, "New physical layer key generation dimensions: Subcarrier indices/positions-based key generation," *IEEE Communications Letters*, vol. 25, n°. 1, p. 59–63, 2021.

[142] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Transactions on Information Theory*, vol. 28, n°. 1, p. 55–67, 1982.

[143] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R.-A. Stoica, G. Abreu et H. Haas, "Physical-layer security in 6G networks," *IEEE Open Journal of the Communications Society*, vol. 2, p. 1901–1914, 2021.

[144] H. Alakoca, M. Namdar, S. Aldirmaz-Colak, M. Basaran, A. Basgumus, L. Durak-Ata et H. Yanikomeroglu, "Metasurface manipulation attacks: Potential security threats of ris-aided 6G communications," *IEEE Communications Magazine*, vol. 61, n°. 1, p. 24–30, 2023.

[145] L. Zhao, X. Zhang, J. Chen et L. Zhou, "Physical layer security in the age of artificial intelligence and edge computing," *IEEE Wireless Communications*, vol. 27, n°. 5, p. 174–180, 2020.

[146] N. Yang et A. Shafie, "Terahertz communications for massive connectivity and security in 6G and beyond era," *IEEE Communications Magazine*, p. 1–7, 2022.