Nom	Idowu I. AJAYI
Affiliation	Laboratoire Image Signal Télécommunications Électronique (LISITE) de l'ISEP
Titre de la thèse	Enhanced PHY Layer Security through Frequency and Spatial Diversity
Financement	ISEP & Agence Nationale de Radio Fréquences (ANFR)
Date de thèse	Janvier 2020 – Janvier 2023
Encadrants	L. MROUEH (ISEP, directrice), Y. Medjahdi (IMT Nord Europe, encadrant académique), F. Kaddour (ANFR, encadrante industrielle)

1. CONTEXTE DE LA THÈSE

Ces dernières décennies ont été marquées par un virage inédit de la société et de l'économie vers une grande dépendance des réseaux de communication sans fil et de l'accès illimité à internet. Le web traditionnel des années 1990 à contenu statique a connu plusieurs évolutions allant du web social (web 2.0), au web sémantique (web 3.0) et dernièrement au web des objets (web 4.0). Cette évolution du web n'a pu se faire que grâce aux grandes avancées technologiques qui se sont effectuées en parallèle dans tous les domaines du numérique : l'électronique, les télécommunications, l'informatique et le traitement massif de données. Cette aptitude multiple d'internet de connecter à la fois les appareils, les personnes et les objets a une double facette. D'une part, le web offre un environnement inédit de collaboration, de coordination et de coproduction. D'autre part, tous les utilisateurs du web sont vulnérables en raison des cyberattaques**,** de l'espionnage et du piratage des information et par conséquent l'atteinte à la vie privée et aux données personnelles. La sécurité de la couche physique ou Physical Layer Security (PLS) est un nouveau paradigme utilisé pour renforcer la sécurité des systèmes de communication sans fil avec une complexité de calcul inférieure aux algorithmes de cryptographie classique [1]. Les techniques PLS utilisent les caractéristiques des canaux sans fil telles que l'évanouissement, l'effet de masque et la dispersion des canaux sans fil pour assurer une communication sécurisée entre un émetteur (Alice) et un récepteur légitime (Bob) en présence d'un pirate (Eve). L'objectif de ma thèse est de proposer des stratégies et des **techniques de transmission PLS** permettant de sécuriser les échanges dans les réseaux de communications sans fils tout en considérant les **contraintes pratiques d'implémentation**, à savoir, les contraintes sur l'acquisition de l'état de canal, soit le Channel State Information (CSI)) sur l'émetteur, la connaissance de la stratégie de sécurité sur le récepteur (pirate) et la minimisation de la consommation énergétique.

2. ETAT DE L'ART

2.1 TRAVAUX DE RECHERCHE DANS LA LITERATURE

Plusieurs travaux de recherche ont été proposés dans la littérature pour améliorer la sécurité sur le lien légitime entre Alice et Bob en présence d'un pirate, Eve. La majorité de ces techniques se basent sur une **connaissance complète** du lien radio entre Alice et Bob à l'émetteur comme au récepteur. Nous avons regroupé ces stratégies en cinq catégories principales :

1. L'optimisation de l'allocation de puissance entre Alice et Bob ([2], [3]) ;
2. Les méthodes de diversité avec un entrelacement adaptatif ([11-13]) ;
3. Les méthodes de codage basées sur le « coset coding » ([14-16]) ;
4. Les méthodes de précodage permettant de focaliser l'énergie dans la direction de Bob ([4]-[7]) ;
5. L'injection du bruit artificiel non nuisible à la communication entre Alice et Bob ([8]-[10]) ;

La première catégorie de techniques PLS s'adresse principalement aux systèmes Orthogonal Frequency Division Multiplexing (OFDM). Les techniques d'allocation de puissance comme le waterfilling adaptent l'allocation de puissance entre les différentes sous-porteuses suivant le lien entre Alice et Bob. En se basant sur l'hypothèse que le lien de Eve est complètement décorrélé de celui de Bob, cette répartition de puissance maximisera la capacité entre Alice et Bob mais elle ne sera pas optimisée du côté de Eve. La deuxième catégorie se base sur des techniques de diversité temporelle induite via des délais générés connus par Bob et non par Eve, ou bien sur des séquences d'entrelacement générées à partir du lien radio. La troisième catégorie de technique PLS, dite « coset coding », introduit des bits aléatoires et les combine avec les bits d'information. Le récepteur légitime

est configuré pour connaître que les bits aléatoires ne contiennent pas d'information utiles, et le décodage du signal bruité s'effectue uniquement sur l'espace d'information de Bob. Cette stratégie de décodage est supposée être transparente du côté du pirate Eve. Cette dernière doit décoder à la fois les bits aléatoires et les bits d'information, ce qui rajoute de la confusion côté récepteur. La quatrième et la cinquième catégorie de techniques PLS considèrent des configurations multi-antennes (Multiple Input Multiple Output (MIMO)). L'utilisation d'un précodeur adapté au lien entre Alice et Bob comme le Zero-Forcing (ZF) ou le filtre adapté (Matched Filtering (MF)) permet d'éliminer les interférences entre les antennes sur le récepteur légitime. A contrario, dans le cas de Eve, le précodeur utilisé est non adapté au lien radio entre Alice et Eve. Des interférences multi-antennes résiduelles altèrent ainsi la qualité de la transmission sur ce lien. La stratégie de transmission basée sur l'injection du bruit est convenable au système massive-MIMO dans lequel l'émetteur possède un nombre d'antenne largement supérieur au récepteur. Le bruit artificiel est constitué en multipliant la matrice génératrice de l'espace du canal principal par un bruit Gaussien. A l'émetteur, le bruit artificiel est ajouté à l'information précodée envoyée à l'ensemble des récepteurs Bob. Comme ce bruit artificiel est orthogonal au lien radio entre Alice et Bob, sa contribution sera nulle du côté du récepteur légitime, mais non-nulle du côté de Eve.

2.2 LIMITES TECHNIQUES ET TECHNOLOGIQUES

Les techniques PLS proposées dans la littérature dépendent critiquement de l'hypothèse de la **connaissance parfaite** du lien radio entre Alice et Bob et de sa **réciprocité** dans un système avec duplexage temporel, **Time Division Duplex (TDD)**. Cette hypothèse garantit que Eve n'a aucun moyen d'estimer la valeur du lien radio entre Alice et Bob. Or, dans un système pratique, cette hypothèse n'est pas tout à fait faisable. D'une part, le **CSI parfait** n'est généralement pas disponible en raison des erreurs de l'estimation du canal au niveau du récepteur, un canal de retour bruité entre le récepteur et l'émetteur, un canal variable dans le temps engendrant un CSI expiré, etc. D'une autre part, l'hypothèse de la réciprocité du lien radio n'est pas valide dans un système à duplexage fréquentiel, **Frequency Division Duplex** (FDD). Dans ce système, Bob estime le lien radio et renvoie à Alice les données relatives à ce lien estimé. La probabilité que Eve intercepte ces données sera donc non nulle, et la stratégie de sécurité devient défaillante. Outre les contraintes pratiques liées à l'acquisition de CSI, les hypothèses considérées dans la littérature pour étudier les techniques PLS de codage ne reflètent toujours pas la réalité dans les systèmes de communications sans fil. Certaines hypothèses supposent que la **stratégie de codage adoptée** sur le lien légitime **n'est pas connue** du côté d'Eve ; d'autres hypothèses défavorisent le canal pirate au dépend du canal légitime. Ces deux hypothèses ne sont pas toujours valides dans le cas d'un **récepteur pirate avancé** ayant l'aptitude d'accéder à la stratégie PLS utilisée du côté d'Alice. La dernière contrainte pratique que nous avons identifiée concerne la **minimisation de la consommation énergétique** sur l'émetteur (Alice). Dans les systèmes MIMO massifs, les techniques d'injection de bruit artificiel engendrent un **facteur de crête** ou **Peak to Average Power Ratio** (PAPR) **élevé**. Pour garantir une linéarité de l'amplificateur sur toutes les valeurs du signal, le point de fonctionnement des amplificateurs doit être réduit pour s'adapter aux pics de signaux élevés. L'inconvénient de cette méthode est que les amplificateurs auront une efficacité énergétique faible, et la majorité de l'énergie fournie à l'amplificateur sera gaspillée sous forme de chaleur.

3. RESULTATS SCIENTIFIQUES OBTENUS

En se basant sur les limites techniques et technologiques de l'état de l'art, nos travaux de recherche se sont focalisés sur les questions suivantes :

1. Comment concevoir une stratégie de transmission sécurisée dans un système FDD ?
2. Quel est l'impact du CSI imparfait au récepteur sur la capacité de sécurité ?
3. Comment estimer d'une façon efficace le lien radio pour maximiser la capacité de sécurité ?
4. Comment coder pour sécuriser et fiabiliser le lien légitime tout en dégradant le lien pirate ?
5. Comment sécuriser l'information sans pénaliser le PAPR dans les systèmes MIMO massifs ?

Les performances des techniques PLS proposées sont évaluées en termes de : (a) **Capacité de sécurité** définie comme étant la différence entre la capacité de Shannon du récepteur légitime et celle du récepteur pirate ; (b) **Taux d'erreur** binaire calculé sur récepteur légitime et le récepteur pirate ; (c) **Facteur de crête,** Peak to Average and Power Ratio (PAPR) ; (d) Complexité de l'algorithme.

3.1 PLS POUR LES SYSTEMES FDD AVEC CSI IMPARFAIT : **[C1]**

Notre **première** contribution publiée dans [C1] propose une nouvelle technique **PLS-FDD** dans un système OFDM avec un duplexage en fréquence. Le lien entre Alice et Bob est supposé être connu par le récepteur légitime (Bob) comme par le récepteur pirate (Eve). L'information envoyée sur les différentes sous-porteuses est codée en utilisant un code de répétition, un code Alamouti ou un code algébrique Diagonal Algebraic Space Time (DAST) code. Notre solution de technique de PLS à l'émetteur (Alice) consiste à : (a) Ordonner les sous-porteuses suivant leurs gains ; (b) Identifier les sous-porteuses exploitables (celles qui possèdent un gain supérieur à un seuil) pour le transport d'information ; (c) Définir des couples de sous-porteuses associant une sous-porteuse avec un gain élevé à une sous-porteuse avec un gain faible ; (d) Coder un ou deux symboles sur les porteuses suivant le taux en symbole des schémas de diversité fréquentielle (répétition, Alamouti, ou DAST). Connaissant l'ordre des sous-porteuses, les récepteurs (Bob ou Eve) décodent les informations sur les différentes sous-porteuses en utilisant un décodeur de maximum de vraisemblance. En utilisant cette stratégie, Bob peut exploiter la diversité fréquentielle et la compensation des gains sur les différentes porteuses. Cependant, l'ordre des sous-porteuses sera aléatoire pour Eve et tous les gains de sous-porteuses seront identiquement distribués. En présence d'un CSI imparfait, nous avons évalué **analytiquement** et **numériquement** les taux d'erreur binaire consécutifs à l'utilisation de cette stratégie au niveau des récepteurs légitime et pirate. Nous avons aussi calculé les capacités de Shannon correspondantes et nous avons déduit la capacité de sécurité. Nous avons constaté que la capacité de sécurité est inversement proportionnelle à l'efficacité spectrale : elle est la plus faible en utilisant toutes les sous-porteuses et la plus élevée en n'utilisant que la moitié des sous-porteuses. La sélection de sous-porteuses avec un gain élevé permet de maximiser la capacité de sécurité, du code DAST par rapport au code de répétition et le code Alamouti. Cependant, l'utilisation de toutes les sous-porteuses pour le code DAST n'est pas bénéfique car la capacité de Bob sera en moyenne égale à celle de Eve.

3.2 PLS AVEC CONNAISSANCE IMPARFAITE DU CSI : **[C2], [J2]**

Notre **deuxième** contribution publiée en [C2] étudie la robustesse de notre stratégie PLS-FDD appliqué à un système OFDM contre les erreurs d'estimation du lien radio. Nous considérons un couplage aléatoire des sous-porteuses et un précodage des sous-porteuses avec un filtre adapté à l'émetteur. Comme précédemment, nous avons calculé analytiquement et numériquement les taux d'erreurs binaires et les capacités de sécurité en tenant compte de la variance d'erreur induite par l'estimation du canal. En présence d'un CSI imparfait, nous avons modélisé le **compromis** qui existe entre **l'efficacité spectrale**, la **capacité de sécurité** et la **variance d'erreur** induite par l'estimation du canal radio. Ce compromis permet d'ajuster l'efficacité spectrale en fonction de la variance d'erreur et de la capacité de sécurité cible. Notre **troisième** contribution a été motivée par la dégradation de la capacité de sécurité du schéma PLS-FDD avec l'erreur d'estimation du lien radio sur l'émetteur. Afin de réduire cette variance d'erreur et de maximiser le gain en capacité de sécurité, nous avons proposé dans [J2] deux algorithmes basés sur les réseaux de neurones qui débruitent le canal radio. Le premier algorithme, DenoiseSecNet, utilise le modèle d'auto-encodeur avec du deep learning. Ainsi, cet algorithme prend en entrée la valeur bruitée envoyée sur le canal de retour, et génère une valeur débruitée qui est presque égale au CSI original. Le deuxième algorithme, Hyb-DenoiseSecNet, est un algorithme hybride qui combine classic truncation scheme avec un auto-encodeur peu-profond. Nous avons démontré que l'algorithme Hyb-DenoiseSecNet permet d'obtenir les mêmes performances en capacité de sécurité que DenoiseSecNet mais avec une complexité bien moindre. De plus, en présence de CSI imparfait, nous obtenons, avec nos algorithmes des gains significatifs en termes capacité de sécurité comparé aux méthodes de dé-bruitage classiques.

3.3 PLS AVEC MODULATION INDEXÉE **: [C4], [J3]**

Notre **quatrième** contribution, Indexed Partitioned Modulation propose un schéma de codage pour fiabiliser et sécuriser l'échange de l'information dans un système OFDM. Contrairement à la littérature nous supposons que Eve possède la même connaissance que Bob sur le schéma de codage utilisé par Alice. Notre stratégie consiste à partitionner la constellation QAM en plusieurs sous-ensembles disjoints, indexés par un nombre fini de bits connus uniquement à l'émetteur (Alice) et au récepteur

légitime (Bob), mais pas de l'espion. Cette modulation mappe chaque séquence de bits d'information en plusieurs séquences codées, chacune se trouvant dans une partition différente de l'espace de constellation QAM. L'étiquetage des bits doit garantir que la distance euclidienne entre les symboles voisins de chaque partition est maximisée, ainsi que celle entre les images de la même séquence d'information. Il doit également garantir que la distance de Hamming entre la séquence d'information des symboles voisins dans l'ensemble de la constellation est au moins égale à un. Ce partitionnement associé à l'étiquetage des bits améliore l'information mutuelle entre Alice et Bob et dégrade celle entre Alice et Eve. L'évaluation de la performance de la capacité de securité montre que notre schéma dépasse tous les autres schémas connus dans la littérature.

3.4 PLS AVEC REDUCTION DU FACTEUR DE CRÊTE : **[C3], [J1]**

Notre **cinquième** contribution, mMIMO-PAPR-aware-secure, adresse le problème de réduction du PAPR des techniques PLS avec injection de bruit dans les systèmes TDD-MIMO massifs. Nous considérons un **système multi-utilisateur** dans lequel un émetteur (Alice) transmet simultanément des **messages différents** à plusieurs utilisateurs (Bob) ayant une seule antenne chacun. Nous supposons une connaissance parfaite à l'émetteur comme aux récepteurs du lien radio entre Alice et tous les récepteurs Bob. Un récepteur pirate multi-antennes (Eve) tente de récupérer toutes les informations envoyées à tous les récepteurs. Eve n'a pas accès au CSI entre Alice et tous les Bobs. Le nombre d'antenne à l'émetteur est largement supérieur au nombre d'utilisateurs servis. Dans ce cas, il existe un espace nul, généré par une matrice orthonormale, qui est orthogonale à la matrice du lien MIMO entre Alice et tous les Bobs. Le bruit artificiel est constitué en multipliant cette matrice orthonormale par un bruit Gaussien. A l'émetteur, le bruit artificiel est ajouté à l'information précodée envoyée à l'ensemble des récepteurs Bob. Comme ce bruit artificiel est orthogonal au lien radio entre Alice et Bob, sa contribution sera nulle du côté des récepteurs légitimes, mais elle sera non-nulle du côté de Eve. Les étapes majeures de notre algorithme, consistent à : (1) Précoder les données en utilisant un filtre adapté ou Zero Forcing; (2) évaluer le seuil d'écrêtage optimal pour le signal d'émission en fonction du PAPR visé ; (3) Découper itérativement le signal d'émission en fonction de ce seuil d'écrêtage ; (4) A chaque étape d'itération, nous utilisons un algorithme d'optimisation avec descente de gradient pour transformer le signal excédentaire en un bruit artificiel projeté dans l'espace nul du canal entre Alice et Bob. (5) Répartir la puissance totale entre le signal utile et le bruit artificiel. Nous avons démontré que notre stratégie conserve les mêmes capacités de sécurité et taux d'erreur binaires que la littérature. Cependant, pour une répartition de puissance donnée entre signal utile et bruit artificiel, les valeurs statistiques du PAPR obtenues avec notre stratégie sont nettement inférieures à celle de la littérature. Nous avons ensuite déterminé la répartition optimale de puissance entre le signal utile et le bruit artificiel qui permet de minimiser le PAPR ainsi que la valeur de l'efficacité énergétique de l'amplificateur.

4. PRODUCTION SCIENTIFIQUE

PAPIERS JOURNAUX

[J1]. **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

[J2]. **I. Ajayi,** Y. Medjahdi, O.Okubadejo, L. Mroueh, and F. Z. Kaddour, "Neural Networks for Denoising Imperfect Channel State Information in Physical Layer Security", in final revision to be submitted to IEEE communication letters

[J3]. **I. Ajayi**, L. Mroueh, Y. Medjahdi, and F. Z. Kaddour, "Generalized Indexed Partitioned Modulation for Physical Layer Security in OFDM Communication", in final revision to be submitted to IEEE transaction on communication.

CONFERENCES

[C1]. **I. Ajayi,** Y. Medjahdi, L. Mroueh and F. Kaddour, "Physical Layer Security by Interleaving and Diversity: Impact of Imperfect Channel State Information", 8th IEEE International Conference on Electrical Engineering, Computer Science and Informatics EECSI, Oct 2021, **Best conference paper award**

[C2]. **I. Ajayi,** Y. Medjahdi, L. Mroueh and F. Kaddour, "Impact of Imperfect Channel State Information on Physical Layer Security by Precoding and Diversity", 8th IEEE International Conference on Electrical Engineering, Computer Science and Informatics, Oct 2021

[C3]. **I. Ajayi,** L. Mroueh, Y. Medjahdi, and F. Z. Kaddour, "Secrecy Energy Efficiency in PAPR-Aware Artificial Noise Scheme for Secure Massive MIMO", submitted to IEEE Wireless Communications and Networking Conference (WCNC 2023)

[C4]. **I. Ajayi**, L. Mroueh, Y. Medjahdi, and F. Z. Kaddour, "Indexed Partitioned Modulation for Physical Layer Security in SISO-OFDM Communication", in final revision to be submitted to IEEE Information Theory Workshop 2023.

[C1].J. M. Hamamreh, H. M. Furqan, H. Arslan, “Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey,” IEEE Communications Surveys Tutorials, vol. 21, pp. 1773–1828, 2019.

[C2].X. Chen, H. Qin, L. Xiao, M. Zhao, and J. Wang, “Power- efficient joint resource allocation for multiuser wiretap OFDM channels,” IEEE International Conference, p. 2862aˆ2867, 2015.

[C3].S. Karachontzitis and S. Timotheou, “Security-aware max-min resource allocation in multiuser OFDMA downlink,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, p. 529--542, 2015.

[C4].E. Yaacoub, M. Al-Husseini, “Achieving physical layer security with massive MIMO beamforming,” 11th European Conference Antennas Propagation, p. 1753aˆ1757, 2017.

[C5].S. Liang, Z. Fang, G. Sun, J. Zhang, “A Physical Layer Security Approach Based on Optical Beamforming for Indoor Visible Light Communication,” IEEE Communications Letters, vol. 24, no. 10, pp. 2109–2113, 2020.

[C6].Chan Dai Truyen Thai, “Beamforming and jamming for physical-layer security with different trust degrees,” AEU - International Journal of Electronics and Communications, vol. 128, 2021.

[C7].J. Song, B. Lee, J. Park, M. Lee, J. Lee, “Beamformer De- sign for Physical Layer Security in Dual-Polarized Millimeter Wave Channels,” IEEE Transactions on Vehicular Technology, vol. 69, no. 10, pp. 12 306–12 311, 2020.

[C8].W. Liu, M. Li, X. Tian, Z. Wang, Q. Liu, “Transmit Filter and Artificial Noise Design for Secure MIMO-OFDM Systems,” *arXiv*, 2017.

[C9].S. Hong, C. Pan, H. Ren, K. Wang, A. Nallanathan, “Artificial- Noise-Aided Secure MIMO Wireless Communications via Intelligent Reflecting Surface,” *IEEE Transactions on Communications*, vol. 68, no. 12, pp. 7851–7866, 2020.

[C10]. S. Goel, R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun*, vol. 7, no. 6, pp. 2180–2189, 2008.

[C11]. T. Allen, N. Al-Dhahir, “Secure Space-Time Block Coding without Transmitter CSI,” IEEE Wireless Communications Letters, vol. 3, no. 6, pp. 573–576, 2014.

[C12]. P. O. Akuon, H. Xu, “Secure Signal and Space Alamouti Scheme,” SAIEE, vol. 107, no. 4, pp. 237–244, 2016.

[C13]. M. Yusuf, H. Arslan, “Enhancing Physical-Layer Security in Wireless Communications Using Signal Space Diversity,” Military Communications Conference, 2016.

[C14]. H. Ozarow and A. D. Wyner, “Wire-tap channel II,” *Bell Lab. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, Dec. 1984.

[C15]. A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, “Applications of LDPC codes to the wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[C16]. F. Oggier, P. Solé, and J.-C. Belfiore, “Lattice codes for the wiretap Gaussian channel: Construction and analysis,” *IEEE Trans. Inf. Theory*, vol. 62, no. 10, pp. 5690–5708, Oct. 2016.