Le code Raptor pour la gestion d'interférence, la sécurité et l'optimisation des antennes dans m-MiMo

Par

Djedjiga BENZID

THÈSE PAR ARTICLES PRÉSENTÉE À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE COMME EXIGENCE PARTIELLE À L'OBTENTION DU DOCTORAT EN GÉNIE
Ph. D.

MONTRÉAL, LE 03 FÉVRIER 2021

ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

PRÉSENTATION DU JURY

CETTE THÈSE A ÉTÉ ÉVALUÉE

PAR UN JURY COMPOSÉ DE :

M. Michel Kadoch, directeur de la thèse
Département de génie électrique à l'École de technologie supérieure

M. Witold Suryn, président du jury
Département de génie logiciel et de TI à l'École de technologie supérieure

Mme Nadjia Kara, membre du jury
Département de génie logiciel et de TI à l'École de technologie supérieure

Mme Halima Elbiaze, examinateur externe
Département d'informatique, UQAM

ELLE A FAIT L'OBJET D'UNE SOUTENANCE DEVANT JURY ET PUBLIC

LE 16 DÉCEMBRE 2020

À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

REMERCIEMENTS

J'aimerais, en premier lieu, témoigner ma reconnaissance à mon directeur de recherche, Monsieur Michel Kadoch, pour son encadrement tout au long de ce travail. Je le remercie pour son temps, sa patience, ses bonnes orientations et ses précieux conseils.

Mes sincères remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner ce travail.

Mes profonds remerciements vont aussi à toute ma famille pour le soutien continu qu'ils m'ont apporté tout au long de ma démarche.

Les codes Raptor pour la gestion d'interférence, la sécurité et l'optimisation des antennes dans m-MiMo

Djedjiga BENZID

RÉSUMÉ

La prochaine génération des réseaux sans fil, nommée (5G), est une solution prometteuse pour déployer une future infrastructure de la société numérique fiable et robuste. Cette dernière s'appuie sur des solutions clés, telles que la technologie Massive Multi-Input Multi-Output (m-MiMo) dont les propriétés promettent d'augmenter le débit et la capacité du réseau pour faire face au nombre élevé des utilisateurs. Toutefois, cette technologie pose certains défis qui limitent de son déploiement, à savoir la contamination du canal, l'écoute à la couche physique, la consommation excessive d'énergie et la complexité de traitement due à l'usage d'un grand nombre d'éléments de la chaîne radio fréquence.

À cet effet, les trois contraintes citées ci-dessus font l'objet de notre thèse. Notre objectif principal est de proposer des solutions simples fiables et robustes pour faire face à ces contraintes. À cet égard, nous avons proposé trois modèles dans lesquels nous exploitons les caractéristiques de la couche physique afin d'éviter l'ajout supplémentaire dans la consommation des ressources en matière d'énergie et de traitement, qui est déjà problématique dans m-MiMo. À cet effet, nous introduisons les codes correcteurs d'erreurs, plus précisément les codes Raptor, pour fonctionner avec m-MiMo, et ce, pour réduire l'intensité des contraintes que nous avons soulevées dans cette thèse.

La première solution que nous avons mise de l'avant consiste à pallier la contrainte des séquences pilotes contaminées. Pour ce faire, nous avons eu recours à un modèle dont les codes Raptor sont combinés à la technique de détection MMSE (Minimum Mean Square Error). Dans cette approche, les symboles décodés avec le code Raptor sont utilisés par le détecteur MMSE pour estimer le canal par le récepteur, et ce, sans utiliser les séquences pilotes. Cette solution contribue non seulement à éviter la contamination des séquences pilotes, mais aussi à réduire la consommation de ressources, d'énergie et de traitement.

Dans le but d'approfondir cette étude, trois codes FEC (Forward Error Correction) : Raptor, LT (Luby Transform) et LDPC (Low-Density Parity-Check) et trois techniques de filtrage MMSE, ZF (Zero Forcing) et MRC (Maximal Ratio Combining) sont utilisés. L'étude a été effectuée sur un canal d'évanouissement lent (slow fading Channel), un canal qui ne change pas dans le temps ou très peu.

La deuxième solution est consacrée à la résolution du problème d'écoute dans la couche physique dans les m-MiMo. Pour cela, nous avons proposé d'exploiter judicieusement les

caractéristiques des codes Raptor et de m-MiMo à des fins de sécurité. Cette proposition contribue à sécuriser la couche physique et à éviter la consommation excessive d'énergie ainsi que la complexité de traitement du signal AN.

Notre objectif en lien avec la troisième contrainte est de déterminer comment sélectionner le meilleur sous-ensemble d'antennes au niveau du récepteur sous un CSI imparfait. Ainsi pour le choix du nombre performant d'antennes, la méthode de Lagrangien et l'algorithme de water-filling sont utilisés. La sélection est basée sur un critère de maximisation de l'information mutuelle utilisant des symboles décodés par code Raptor.

Les solutions présentées sont évaluées par des simulations numériques. Au bout du compte, les résultats montrent que nos solutions proposées ont permis d'atteindre les performances idéales en matière du taux d'erreurs, capacité et de sécutité.

Mots-clés : 5G, Contamination des séquences pilotes, Massive-MiMo, Raptor code, Sécurité, Sélection d'antennes, Water filling Algorithm.

Using Raptor Code to Mitigate Issues Related to Pilot Channel Contamination, Data Secrecy, and Antenna Selection in m-MiMo

Djedjiga BENZID

ABSTRACT

The next generation of wireless networks, known as the fifth generation (5G), is a promising foundation for creating a reliable and robust infrastructure for a future digital society. 5G networks are based on key new technologies, such as massive multi-input multi-output (m-MiMo), that promise to increase network throughput and capacity and allow the network to cope with a large number of users.

m-MiMo, an extension of conventional MiMo, uses hundreds of antennas to reduce interference and prevent channel errors. The large number of antennas in m-MiMo also improves network security by enabling beamforming, a technique where the energy of the antennas is centralized in the direction of the legitimate receiver and an artificial noise (AN) signal is projected in the direction of malicious users.

Despite these benefits, there are still challenges that limit the applications of m-MiMo, including (1) channel contamination, (2) eavesdropping at the physical layer, and (3) excessive power consumption and complexity due to the use of a large number of elements of the radio frequency chain. Pilot sequence contamination is interference that results from processing the same pilot symbols in adjacent cells, whereas eavesdropping is an attack in which an intruding node intercepts messages exchanged between users, creating confidentiality problems in the network. The third constraint relates to energy mismanagement and to the processing complexity that is generated by elements of the radio frequency (RF) transmission chain.

The three constraints mentioned above are the subject of this thesis. Our main goal is to resolve issues related to channel contamination and physical layer security, as well as to optimize the number of antennas (parts of the radio frequency chain) in m-MiMo. To this end, we propose three models where we introduce Raptor codes, a form of error-correcting codes, into m-MiMo systems. The Raptor codes effectively reduce the magnitude of the problems associated with m-MiMo.

Raptor codes are a class of fountain codes that serve as error correctors in channel coding. These codes allow errors in a message to be detected and corrected without requiring the sender to retransmit the data, which is favorable in wireless networks where retransmission is not desirable due to channel errors.

To overcome the constraint of contaminated pilots, we first propose a model where the Raptor codes are combined with a minimum mean square error (MMSE) filtering technique to work with m-MiMo. In our model, the receiver uses the symbols decoded with the Raptor code to estimate the channel, rather than the pilot sequences sent by the transmitter. This solution helps

estimate the channel while preventing pilot contamination. It also manages system energy more efficiently and reduces congestion in the network.

We tested our model using three forward error correction codes (Raptor, Luby transform, and low-density parity-check) and three filtering techniques (MMSE, zero-forcing, and maximum-ratio combining). The study was performed on a slow fading channel, which either does not change over time or changes very little. Simulation results showed that our model achieves ideal performance using MMSE filtering with symbols decoded by the Raptor code.

We then propose a solution for preventing eavesdropping at the physical layer in m-MiMo. Our goal is to develop features that will allow Raptor codes to be used judiciously with m-MiMo for security purposes. Where appropriate, Raptor codes can be used as a tool by the intruder to reinforce his intrusion. Our proposal helps to secure the physical layer, avoid excessive power consumption, and reduce processing complexity. We tested our second model using a simulated intruder who had the most resources in terms of power, processing, and number of antennas, and who had perfect channel state information (CSI).

Our third chapter addresses the problem of excessive power consumption and processing complexity in m-MiMo by evaluating how to select the best subset of antennas at the receiver under imperfect CSI. We propose a water-filling algorithm based on a mutual information maximization criterion and on symbols decoded by Raptor code. Our method optimizes the number of antennas and, therefore, the number of frequency chain elements. Simulation results showed that our proposed solution achieves the same optimal values as the conventional exhaustive search method**.**

Keywords : 5G, Antennas selection Pilot contamination, Massive-MiMo, Code Raptor, Secrecy , Water filling algorithm**.**

TABLES DES MATIÈRES

Page

LISTE DES FIGURES

Page

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

3C	Collaboration Computing, Communication
2D	Two-dimensional
3D	Three-dimensional
3GPP	3 rd Generation Partnership Project
ACK	Acknowledgement
ALE	Automatic Link Establishment
AN	Artificial Noise
AWGN	Additive white Gaussian noise
ARQ	Automatic Repeat reQuest
BER	Bit ERror
BP	Belief Propagation
BPSK	Binary Phase Shift Keying
BS	Base Station
CA	Carrier Aggregation
CDMA	Code Division Multiple Access
CPS	Cyber Physical System
CoMP	Coordinated Multi-Point
CR	Cognitive Radio
CSI	Channal State Informations
DL	Down Link
DVB	Digital Video Broadcast
eNB	evolved NodeB

FEC	Forward Error Correction
FFR	Fractional Frequency Reuse
FPC	Fractional Power Control
Gb	Giga byte
GSM	Global System for Mobile Communications
GTIN	Global Trade Item Number
H-eNB	Home eNode B
Het-Net	Heterogeneous Network
ICI	Inter-Cell Interfence
ICIC	Inter-Cell Interfence coordination
ID	Identification
IoT	Internet of Things
IPv6	Internet Protocol version 6
LDPC	Low-Density Parity-Check
LLR	The likelihood ratio
LT	Luby Transform
LTE	Long Term Evolution
LTE-A	Long Term Evolution Advanced
MAC	Media Access Control
MBMS	Multimedia Broadcast and Multicast Services
MIMO	Multiple-Input Multiple-Output
MIMO-DAS	MIMO distributed antenna system
MME	Mobility Management Entity
MMSE	Minimum Mean Square Error

MRC	Maximal Ratio Combining
MRT	Maximal Ratio Transmission
PLS	physical layer security
PNC	Physical Network Coding
RAN	Radio Access Network
RF	Radio Frequence
SINR	Signal-to-interference-plus-noise ratio
SISO	Single-input single-output
SNR	Signal-to-Noise Ratio
SVD	Singular Value Decomposition
SON	Self-Organized Networks
UE	User equipment
UL	Up Link
UMTS	Universal Mobile Telecommunications System
WFA	Water Filling Algorithm
Wi-Fi	Wireless Fidelity
WMHN	Wireless Multi Hop Network
WPA	Water Pouring Algorithm
WSN	Wireless Sensor Network
ZF	Zero Forcing
ZFB	Zero Forcing beamforming

INTRODUCTION

La révolution technologique de l'Internet est en pleine effervescence avec l'arrivée des objets connectés. En effet, il est prévu que d'ici 2025, 150 milliards d'objets seront reliés par Internet. Ce nombre croissant d'utilisateurs humains et objets implique l'emploi exponentiel de données sans fil. Afin de gérer cette expansion sans précédent du volume du trafic, une future solution inédite des réseaux sans fil basée sur de nouvelles méthodes est primordiale. Ces réseaux doivent être plus rapides, plus intelligents et plus agiles.

Les réseaux 5G sont cette solution du futur qui s'avère 5 fois plus rapide que la 4G actuellement déployée, plus précisément 100 fois plus importante en matière de débit, ce qui lui permettrait d'atteindre un taux de transmission de 20 Gigas Byte (Gb) par seconde, soit aussi agile que la fibre optique actuelle. En outre, la technologie 5G promet d'augmenter la capacité de 1000 fois par rapport à la technologie 4G existante (Zhou et al., 2014). En plus de cela, la 5G prévoit améliorer la qualité de service des utilisateurs de 99,99 % tout en diminuant la latence de bout en bout, ce qui se traduirait par une baisse de 25 fois par rapport à la latence actuelle de la 4G. L'usage de l'énergie dans les réseaux 5G serait également considéré ; il est attendu que celle-ci soit réduite de 90 % par rapport à la consommation actuelle de puissance par les équipements réseaux 4G (S. Wong, 2017). Pour satisfaire à ces engagements, les réseaux 5G s'appuient sur des éléments primordiaux comme m-MiMo.

La technologie m-MiMo est une amélioration de MiMo, impliquant l'emploi de centaines d'antennes, ce qui permet d'augmenter la capacité du canal de dix fois ou plus. La solution m-MiMo est appropriée aussi pour réduire les interférences et la complexité du traitement du signal pour plusieurs utilisateurs et s'avère souhaitable pour éliminer le bruit thermique et les erreurs du canal (Bogale et Le, 2014) et (Zirwas, Amin et Sternad, 2016). Le nombre élevé d'antennes améliore également la sécurité grâce à l'aptitude de cette technologie à focaliser parfaitement l'énergie dans la direction du récepteur légitime et à faire rayonner un signal de bruit dans la direction de tout intrus.

0.1 Description du problème

La technologie de m-MiMo constitue une technologie attrayante et offre d'énormes avantages aux futurs réseaux. Toutefois, elle souffre de contraintes majeures affectant ses performances en raison de l'utilisation d'un grand nombre d'antennes. Ces contraintes sont énumérées ci-dessous :

- la contamination des séquences pilotes ;
- la sécurité de la couche physique ;
- l'augmentation des coûts et la consommation d'énergie générée par l'utilisation d'un grand nombre d'éléments de la chaîne de fréquences radio (RF).

La contamination des séquences pilotes est une interférence générée par la réutilisation des mêmes symboles pilotes dans les cellules voisines. En effet, dans les réseaux multicellulaires, la station de base (BS) a besoin d'informations sur l'état du canal (CSI) pour estimer le canal des signaux transmis dans la liaison montante. À cet effet, chaque usager envoie une séquence pilote orthogonale qui contient des informations sur l'état du canal à la station de base qui l'utilise pour estimer le canal. Cependant, dans les systèmes multicellulaires, il est impossible d'allouer une séquence pilote orthogonale à chaque utilisateur dans toutes les cellules en raison de l'étroitesse de l'intervalle de cohérence, c'est pour cela que ces séquences pilotes orthogonales sont réutilisées dans plusieurs cellules, ce qui engendre une interférence des symboles pilotes dans les cellules adjacentes.

En outre, l'emploi de plusieurs antennes implique l'utilisation d'un nombre colossal de séquences pilotes, ce qui peut générer une surcharge dans les réseaux de 5G qui se traduit par une augmentation de l'utilisation de la bande passante et de la capacité de traitement. De plus, l'envoi de ces séquences requiert une grande puissance de transmission de l'émetteur.

Une autre contrainte à laquelle fait face la technologie m-MiMo est l'attaque d'écoute clandestine. À vrai dire, la technologie m-MiMo est plus sécuritaire que MiMo conventionnel, grâce à son habileté à orienter l'énergie en direction de l'utilisateur légitime et à focaliser le

signal de bruit artificiel (AN) en direction de l'intrus. Cependant, cette approche ne peut s'appliquer que lorsque l'intrus possède moins de ressources (énergie, code correcteur et une capacité de traitement) et moins d'antennes. Le cas échéant, la sécurité ne peut être assurée dans le réseau. En outre, la conception de AN dans la technologie m-MiMo implique généralement une énorme complexité de calcul, ce qui est inefficace en matière de coût de traitement (Zhu et Xu, 2016). De plus, la mise en œuvre de ce signal nécessite une énergie excessive qui est estimée à n^{β}, n étant la variance du bruit du récepteur légitime, n> 1, β étant une constante> 1.

La troisième contrainte que nous soulevons dans cette thèse est le coût et la complexité du traitement qu'implique le déploiement de la technologie m-MiMo. À vrai dire, l'utilisation d'un grand nombre d'antennes ne requiert beaucoup d'énergie ni une grande ressource de traitement. Cependant, les antennes nécessitent l'utilisation de plusieurs éléments de la chaîne radiofréquence (RF) aux deux extrémités de la liaison qui ont besoin d'une énergie colossale et introduisent une complexité de calcul.

Nous appelons une chaîne radiofréquence (RF), les équipements nécessaires utilisés dans les opérations de traitement que subit le signal sans fil à l'émission et à la réception. À l'émission, ces opérations sont indispensables et consistent à adapter le signal au canal de propagation. À la réception, des opérations inverses sont requises pour récupérer le signal.

Pour faire face au problème de coût et complexité de traitement, la méthode de sélection d'antennes est utilisée. Dans cette approche, un sous-ensemble des antennes disponibles au niveau de l'émetteur et du récepteur est choisi selon un critère prédéfini.

Dans MiMo conventionnel, la méthode la plus optimale pour trouver un sous-ensemble d'antennes est la méthode de recherche exhaustive qui a été largement utilisée. Cependant, cette méthode s'avère inefficace pour le système m-MiMo, et ce, en raison du grand nombre d'antennes qui demande beaucoup de ressources de traitement. Ainsi, les solutions de sélections proposées jusqu'à maintenant supposent que le canal est parfaitement connu au

récepteur, ce qui est impossible dans la pratique. De ce fait, un algorithme de sélection d'antennes optimal, rapide, moins coûteux en ressource et qui prend en compte CSI est souhaitable dans les systèmes de m-MiMo.

0.2 Objectifs

L'objectif principal de ce travail est de résoudre les problèmes discutés dans la section précédente.

Notre premier objectif principal est de résoudre le problème des séquences pilotes contaminées dans les m-MiMo et d'éviter les contraintes secondaires qui découlent de leur usage, à savoir la consommation d'énergie dépensée lors de l'envoi des séquences pilotes, la surcharge dans les réseaux et la complexité qui est due à l'utilisation excessive des ressources de traitement.

Le second objectif principal est de proposer une solution qui permet d'assurer la sécurité de la couche physique dans le cas d'un intrus possédant de grandes ressources telles que les codes Raptor, une grande capacité de traitement et un grand nombre d'antennes.

La solution proposée doit prendre en considération les contraintes secondaires citées ci-dessus qui sont résumées dans les différents points suivants :

- éviter une surconsommation de l'énergie requise pour la mise en œuvre du signal AN.
- réduire la complexité de calcul introduite lors de la conception de AN.

Le troisième principal objectif est de diminuer l'impact des éléments de chaîne radiofréquence sur m-MiMo. Cette opération nécessite un algorithme de sélection d'antennes optimal, rapide, moins coûteux en ressource et qui prend en compte les CSI dans les systèmes de m-MiMo. Par conséquent, nous nous intéressons, dans cette thèse, à la résolution des contraintes suivantes :

- sélectionner le meilleur sous-ensemble d'antennes au niveau du récepteur sous un CSI imparfait ;
- utiliser un algorithme économe en énergie afin de réduire la consommation d'énergie ;
- utiliser un algorithme simple qui ne requiert pas une grande capacité de calcul.

0.3 Méthodologie

Dans cette recherche, nous nous intéressons à la résolution des contraintes liées à l'usage d'un grand nombre d'antennes par m-MiMo, à savoir la contamination des séquences pilotes, la sécurité à la couche physique, l'augmentation des coûts de traitement et la consommation d'énergie générée par l'utilisation d'un grand nombre d'éléments de la chaîne de fréquences radio (RF).

Pour le problème de la contamination des séquences pilotes dans m-MiMo, nous avons proposé une solution basée sur l'utilisation de l'approche des symboles décodés pour estimer le canal m-MiMo.

Le principe de cette solution consiste à envoyer les données d'informations sans utiliser les séquences pilotes. À la réception, les données sont décodées avec le code Raptor et ensuite utilisées par le détecteur linéaire MMSE pour estimer un canal d'évanouissement lent, un canal qui ne change pas rapidement dans le temps. L'estimation du canal est ensuite utilisée dans le calcul de rapports de vraisemblance (LLR : LikeLihood Ratio) pour décoder les nouveaux symboles envoyés par l'émetteur. Dans cette étape, un processus de décodage transparent (soft) est effectué en utilisant l'algorithme de propagation de croyance (BP).

Pour permettre d'estimer le canal en utilisant des données d'informations décodées, nous avons modifié l'expression de détecteur MMSE pour modéliser notre solution. Cette étude a été vulgarisée pour inclure deux autres codes de FEC, à savoir LT et LDPC. Deux techniques de filtrage ZF et MRC ont été aussi introduites dans l'étude où nous avons également modifié leur expression pour modéliser notre solution.

La deuxième solution concerne le problème de la sécurité à la couche physique qui vise à anéantir un intrus utilisant les codes Raptor et plusieurs antennes. En outre, l'intrus possède un SNR élevé lui permettant d'épier le canal principal. En effet, l'intrus est un nœud dissimulé à l'émetteur et son canal est inconnu par le récepteur légitime, ce qui en fait un nœud passif. Ce statut lui permet d'être à proximité de l'émetteur pour augmenter sa force du signal et sa capacité d'écouter le canal principal. Cependant, le fait qu'il soit passif vis-à-vis des autres parties ne lui permet pas de demander une retransmission de données en cas de réception de paquets corrompus. En utilisant les propriétés PLS, nous proposons d'exploiter les caractéristiques des codes Raptor et de la technologie m-MiMo conjointement et d'une façon judicieuse afin de pallier la contrainte citée ci-dessus.

Nous exploitons la caractéristique de code Raptor où l'émetteur produit un flux infini de paquets de données et le récepteur collecte ces paquets de données jusqu'à ce qu'ils récupèrent le message, ensuite il envoie un message-STOP à la source. Pour exploiter cette fonctionnalité dans la sécurisation du canal, le récepteur légitime doit récupérer le message avant que l'intrus ne le fasse. Ceci peut être réalisé lorsque le nœud malveillant est en Outage (non disponible, car le SNR est faible). En fait, lorsque la variance du signal bruit de l'intrus σ_v est supérieure à la variance du signal du récepteur légitime σ_b, les performances en matière de SNR de l'intrus sont réduites par rapport à celles de l'utilisateur légitime ; par conséquent, lorsque ce dernier récupère le message, il envoie un accusé de réception du décodage réussi au codeur (émetteur) pour arrêter la génération des symboles codés. Et comme l'intrus est passif, son canal n'est pas connu par l'émetteur, il ne peut pas demander de retransmettre des données supplémentaires lui permettant de récupérer le message. Par conséquent, il ne sera pas en mesure de récupérer son signal une fois que le récepteur légitime a réussi à décoder son message. Pour satisfaire cette condition, nous avons utilisé un signal de bruit artificiel en direction de l'intrus et dans l'espace nul des utilisateurs légitimes. En utilisant cette technique, le taux d'erreur binaire (BER) de l'intrus augmente beaucoup plus rapidement. Cette méthode vise à réduire l'efficacité du canal de l'intrus, ce qui permet au canal principal de récupérer le signal avant celui-ci. Une analyse théorique a été menée pour déterminer la quantité d'énergie du signal AN nécessaire pour brouiller le canal de l'intrus. Celle-ci a été conclue par une expression de

forme fermée qui permet de déterminer la valeur de la variance du signal bruit de l'intrus σ_v en fonction de la variance du signal du récepteur légitime σ_b qui permet d'assurer la sécurité au canal principal.

Finalement, nous abordons le problème de coût et de complexité de traitement introduit par l'utilisation de chaîne de fréquence dans m-MiMo. Pour ce faire, nous avons proposé une solution permettant l'optimisation de nombre d'antennes au récepteur. À cet effet, nous avons utilisé la méthode de sélection d'antennes, une méthode qui consiste à choisir un sous-ensemble des antennes disponibles au niveau du récepteur, basée sur un critère de sélection prédéfini, pour réduire la complexité et le coût du système dans m-MiMo.

La méthode de lagrangien est utilisée pour optimiser la puissance des antennes de réception sélectionnées. Étant donné que le problème d'optimisation est convexe, nous l'avons résolu avec l'algorithme water-filling basé sur la maximisation du critère de capacité d'un canal.

La maximisation a été effectuée sur le canal dont les informations ne sont pas disponibles à la réception. À cet effet, nous avons utilisé les informations décodées avec les codes Raptor. Plusieurs opérations de calcul de simplification ont été réalisées pour réduire la complexité de traitement. Enfin, nous avons abouti à l'expression d'optimisation simple et économe en énergie et qui ne requiert pas de ressources de traitement.

0.4 Contribution et nouveautés

La nouveauté principale de cette étude réside dans le fait qu'elle est la première à utiliser les codes Raptor et m-MiMo pour pallier les contraintes citées dans cette thèse. D'autres nouvelles contributions y sont également apportées, elles sont citées comme suit :

Notre première solution contribue à résoudre la contrainte de contamination des séquences pilotes dans m-MiMo en utilisant un modèle ne nécessitant pas l'utilisation des séquences pilotes ni l'ajout d'autres éléments supplémentaires.

En évitant l'envoi des séquences pilotes, nous permettons à l'émetteur d'économiser l'énergie et la bande passante nécessaires à l'envoi des séquences pilotes. D'autre part, le récepteur n'aura pas à traiter les symboles pilotes pour estimer le canal ; par conséquent, il va réduire la consommation de ressources de traitement requise pour estimer le canal. De ce fait, notre contribution est aussi écologique.

Dans la deuxième solution, nous contribuons avec un nouveau modèle pour la sécurité de la couche physique. La nouveauté de notre contribution est qu'elle est la première à traiter un problème de sécurité en présence d'un intrus utilisant un code Raptor et un grand nombre d'antennes.

Notre solution consiste à utiliser les codes Raptor et le signal AN de m-MiMo en direction de l'intrus afin de l'anéantir. Pour ce faire, nous avons eu recours à une expression fermée permettant de déterminer la quantité d'énergie requise pour brouiller le canal de l'intrus. De plus, en utilisant les caractéristiques des codes Raptor, nous avons contribué à réduire la consommation d'énergie nécessaire pour déployer le signal AN. De ce fait, notre contribution s'avère aussi écologique et d'ordre sécuritaire.

Dans la troisième solution, nous avons mis de l'avant une méthode pour l'optimisation du nombre d'antennes pouvant être utilisées afin de diminuer la complexité de traitement et la consommation excessive de l'énergie par les éléments de RF.

La solution proposée contribue à la diminution de la consommation d'énergie. En effet, l'utilisation de lagrangienne et de l'algorithme de Watte filing ne requiert pas une recherche exhaustive, ce qui rend le processus de traitement moins complexe. En outre, la méthode des symboles décodés avec Raptor demande moins d'énergie d'envoi à l'émetteur et évite la surcharge dans le réseau de transmission. De ce fait, notre contribution est aussi écologique et économique.

0.5 Structure de la thèse

Cette thèse est une thèse par article et elle est organisée comme suit. Le chapitre 1 présente deux parties importantes. La première partie aborde des généralités sur certaines méthodes des réseaux sans fil qui font l'objet de cette étude, à savoir le codage du canal, l'estimation du canal et m-MiMo. La deuxième partie du chapitre 1 présente la revue de littérature qui fournit un aperçu sur une variété de techniques qui ont été trouvées dans la littérature et sont connexes à notre étude. Le chapitre 2 présente notre solution pour la contamination des séquences pilotes dans m-MiMo. Le chapitre 3, quant à lui, aborde la solution de la contrainte de la sécurité à la couche physique. Enfin, le chapitre 4 est consacré à la troisième solution concernant l'optimisation du nombre d'antennes pour réduire le coût et la complexité de traitement dans m-MiMo. Nous concluons cette thèse au chapitre 5 où nous présentons une conclusion de la recherche et formulons quelques recommandations pour les travaux futurs.

CHAPITRE 1

GÉNÉRALITÉS ET ÉTAT DE L'ART

Dans les réseaux 5G, comme dans tous les réseaux sans fil, la transmission fiable d'un message nécessite une succession d'opérations à l'émission dans le but de préparer le signal et de l'adapter au canal de propagation. Ainsi, il requiert une série d'opérations inverses en réception afin de recouvrer le message d'origine. Dans cette thèse, nous nous intéressons uniquement à deux opérations importantes, à savoir le codage du canal et l'estimation du canal, dont les caractéristiques vont être exploitées pour atteindre la performance attendue par 5G.

1.1 Codage du canal

Le codage du canal, communément connu sous le nom de correcteur d'erreurs, est une technique utilisée pour rendre une transmission résiliente aux erreurs provenant du bruit, des interférences ou des évanouissements du canal. Cette méthode consiste à introduire une quantité appropriée de redondances dans les messages à la source, ce qui permet au récepteur de détecter ou de corriger les erreurs survenues lors de la propagation du message envoyé. Il existe deux catégories de correcteurs d'erreurs, le protocole de demande de répétition automatique (ARQ) et la méthode de correction d'erreur directe (FEC, forward error correction).

Dans la méthode ARQ, le rôle du code est de détecter de manière fiable les erreurs survenues dans le message reçu. Dans le cas où ce dernier serait corrompu, une demande de retransmission du même message est amorcée (Exemple de paquets IP dans Internet).

Dans l'approche FEC, le code n'a pas recours à la retransmission dans le cas où le message reçu est corrompu, étant donné que les erreurs détectées sont corrigées par le récepteur grâce à des algorithmes de décodage conçus à cet effet. Les codes FEC sont utiles dans les systèmes où les retransmissions sont coûteuses, impossibles ou très lentes, comme dans le cas de communications sans fil GSM, satellites et sous-marines.

Il existe deux modèles de codes FEC structurellement différents, à savoir les codes de bloc et les codes de convolution (Osman, 2009). Les deux types de codes ont été largement utilisés pour le contrôle des erreurs dans les systèmes de communication et de stockage.

Les codes de bloc peuvent être divisés à leur tour en deux catégories, les codes de bloc linéaires et non linéaires. Les codes de bloc non linéaires ne sont jamais utilisés dans des applications pratiques et sont peu étudiés (Ryan, 2009). Parmi les codes linéaires répandus de FEC, citons Low-Density Parity-Check (LDPC) développé par Gallager au début des années 1960.

LDPC est basé sur l'algorithme de décodage de propagation de croyance (BP), qui lui permet d'atteindre les limites de Shannon en matière de performance de décodage, ce qui le rend très puissant. Les codes LDPC sont plus performants sur les canaux de bruit gaussien blanc additif (AWGN) et n'atteignent généralement pas leur optimum sur les canaux non gaussiens. Un domaine d'application intéressant pour les codes LDPC est le canal d'effacement à taux fixe. Ce dernier nécessite une estimation de débit basée sur l'état du canal a priori pour contourner l'effacement du canal (Farrell et Honary, 2005). Cependant, la probabilité d'effacement, qui détermine la capacité du canal, peut changer lors de la transmission sur un réseau. Par conséquent, un taux de codage dynamiquement variable serait avantageux.

D'autres enjeux ont également contribué à l'apparition des codes Fontaine, le problème occasionné par l'utilisation de la méthode (ARQ) dans les codes (FEC). En effet, quand le nombre des récepteurs pouvant demander la retransmission simultanée des données est élevé, un long délai de bout en bout est engendré, et ce, en raison de la longue attente que peut observer un récepteur pour envoyer une demande de retransmission. Ce dernier doit patienter pour que tous les autres récepteurs reçoivent correctement les paquets de données afin d'envoyer sa demande.

Les codes Fontaines sont particulièrement utilisés dans la norme de 3GPP dans la diffusion et la multidiffusion ; deux autres applications très importantes des codes Fontaine sont Luby Transform (LT) et les codes Raptor.

Le code LT est conçu par Michael Luby qui a eu recours à un décodage analogue à celui utilisé par LDPC. Cependant, les codes LT introduisent une complexité de traitement en raison de l'augmentation du nombre de variables utilisées pour atteindre la performance de décodage. Une telle complexité génère une longue latence de décodage, ce qui entraîne un problème du plancher d'erreur. Dans le plancher d'erreur, la courbe de performance BER ne diminue pas incontestablement avec l'augmentation du SNR (He, Yang et Song, 2011). Pour résoudre ce problème et améliorer la fiabilité de ce code, les codes Raptor ont été conçus à la fin de l'année 2000 en utilisant un code d'effacement supplémentaire. Ce code supplémentaire peut être le code LDPC. Les codes Raptor, étant une application idéale des codes Fontaine, héritent de tous les avantages de celui-ci tels qu'une meilleure fiabilité du système, tout en permettant un large degré de liberté dans le choix des paramètres de transmission.

Le code Raptor, standardisé par l'organisation 3GPP, peut être adopté pour l'émission de flux multimédia en temps réel, par exemple une diffusion multimédia (Multimedia Broadcast and Multicast Services MBMS), la diffusion multimédia sur une plateforme UMTS (Universal Mobile Telecommunications System) et la diffusion multiple de vidéo numérique (Digital Video Broadcast DVB). Les codes Raptor peuvent être aussi exploités dans la sécurité pour combattre l'écoute à la couche physique en tirant profit de la caractéristique où un nœud légitime doit intercepter suffisamment de paquets pour récupérer le message envoyé avant l'intrus. C'est dans ce contexte que s'inscrit cette thèse qui vise à utiliser les codes Raptor pour fiabiliser les transmissions et les sécuriser dans les réseaux 5G.

1.2 Estimation du canal

Dans les réseaux sans fil, les symboles doivent être efficacement récupérés au niveau du récepteur pour obtenir une transmission fiable. Cependant, une récupération efficace des symboles peut être compliquée par l'interférence inter-symboles. Pour réduire l'impact lié aux résidus de cette interférence, des techniques d'égalisation sont utilisées. L'une des principales techniques de détection utilisées dans la pratique est le détecteur à maximum de vraisemblance (ML). Cette technique optimise les performances du récepteur, lui permettant de détecter tous

les signaux émis par l'émetteur. Cependant, il a été montré que la complexité de la technique ML augmente de façon exponentielle lorsque le nombre d'utilisateurs augmente.

Pour réduire la complexité de décodage des détecteurs ML, le récepteur peut utiliser comme solution alternative un filtrage linéaire sur le signal reçu. Bien que les méthodes de détection linéaire soient moins fiables que la détection ML, les détecteurs linéaires fonctionnent de manière optimale lorsqu'un grand nombre d'antennes est utilisé, comme dans m-MiMo. Trois techniques de détection linéaire sont considérées dans cet article: les récepteurs à combinaison à taux maximum (MRC), les récepteurs à zéro forçage (ZF) et les récepteurs à erreur minimum moyenne carrée (MMSE) (Muaayed, 2017) (Ngo, 2015).

1.2.1 Combinaison à taux maximum (MRC)

Le principe primordial de la technique de détection MRC est de maximiser le rapport signal sur bruit (SNR) reçu de chaque vecteur. Le récepteur multiplie le flux reçu par la transposée conjuguée de la matrice de canal, puis détecte chaque vecteur séparément, réduisant ainsi la complexité de mise en œuvre du détecteur. Malgré cet avantage, le récepteur MRC fonctionne mal dans les scénarios où l'interférence est limitée.

1.2.2 Récepteur Forçage à Zéro (ZF)

L'objectif des récepteurs à forçage zéro (ZF) est d'éviter les effets des pilotes contaminés en utilisant le pseudo-inverse de la matrice de gain de canal. Le principal avantage des récepteurs ZF est que le traitement du signal est simple; cependant, l'utilisation du pseudo-inverse de la matrice de canal peut également amplifier le bruit. Si l'interférence entre les symboles est importante, les performances du récepteur se détériorent. Les récepteurs ZF sont plus complexes à implémenter que les récepteurs MRC, car ils doivent en plus calculer la matrice de gain de canal.

1.2.3 Erreur Minimum Moyenne Carrée (MMSE)

Pour réduire l'altération des symboles, MMSE utilise la technique des moindres carrés entre les événements aléatoires évalués et les événements prévus. Le détecteur MMSE est considéré comme le filtre linéaire le plus efficace, car il maximise le SNR reçu.

1.3 Massive MiMo

m-MiMo est une amélioration de la technologie MIMO, utilisant des centaines d'antennes. La Figure 1.1 montre un exemple de déploiement m-MiMo.

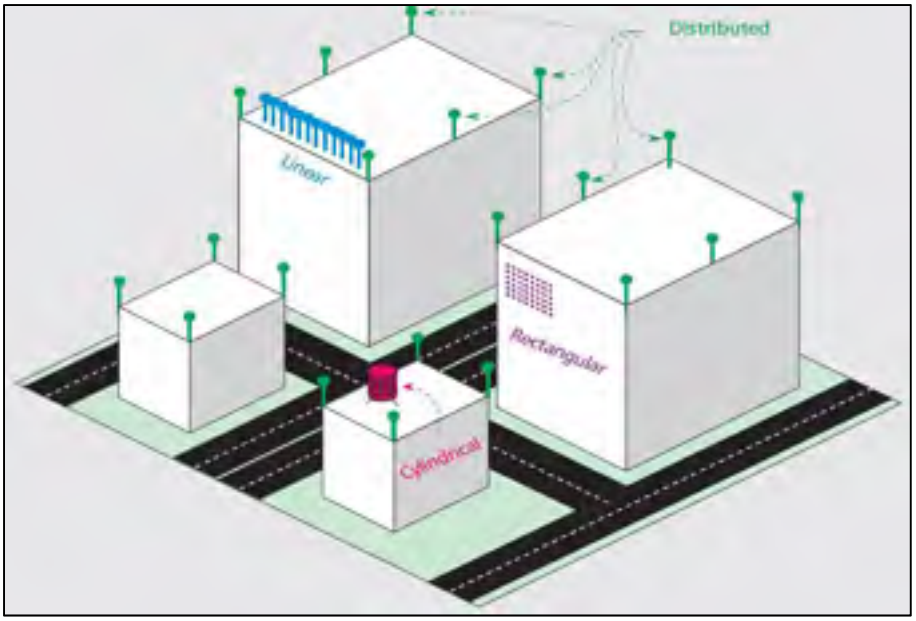

Figure 1.1 Exemple de massive MiMo
Tirée de (Larsson et al., 2014)

La technologie m-MiMo est considérée comme la technologie clé pour faire face à la capacité croissante des utilisateurs des réseaux mobiles 5G. Dans cette partie, nous allons énumérer les principales caractéristiques de cette technologie, à savoir ses avantages, ses limites et son application.

1.3.1 Avantages de la technologie m-MiMo

Les principaux avantages de la technologie M-MIMO sont les suivants (Larsson et al., 2014):

1.3.1.1 Une réduction de la latence.

Dans les réseaux sans fil, la latence est due aux évanouissements en raison de multiples trajets que le signal peut emprunter pour arriver à sa destination. Les ondes résultant de ces trajets interfèrent entre elles de façon destructive. Pour réduire d'une manière significative la latence sur l'interface radio, m-MIMO s'appuie sur la formation de faisceaux (beamforming) afin d'éviter les évanouissements et par conséquent la latence.

1.3.1.2 Simplification de la couche d'accès multiple.

En raison du grand nombre d'antennes dans m-MiMo, Chaque terminal peut recevoir la totalité de la bande passante, ce qui rend la plupart de la signalisation de contrôle de la couche physique redondante.

1.3.1.3 Augmentation de la robustesse contre les interférences

Les réseaux sans fil sont caractérisés par leur technique de transmission de diffusion en raison de la bande passante limitée, ce qui les expose à des attaques comme le brouillage. m-MIMO, grâce à ses implémentations intelligentes utilisant l'estimation et le décodage de canal conjoints, peut réduire considérablement ce problème.

1.3.1.4 Communication backhaul

La technologie m-MIMO peut être utilisée pour remplacer des communications filaires de fibre optique par liaisons hyperfréquences afin d'assurer des communications fiables à haut débit

entre deux stations de base (BS) en dirigeant les faisceaux d'antennes d'une BS en direction de l'autre BS, et ce, grâce à la technique de beam-forming(Wang et al., 2019).

1.3.2 Contraintes de la technologie m- MIMo

Devant tous ces avantages, la technologie m-MiMo fait face à certaines contraintes réduisant ses performances. Ces contraintes sont citées ci-dessous :

1.3.2.1 Réciprocité du canal

L'opération de duplexage temporel repose sur la réciprocité des canaux. Cependant, les chaînes RF de la station de base et des terminaux peuvent ne pas être réciproques entre la liaison montante et la liaison descendante (Larsson et al., 2014).

1.3.2.2 Contamination des séquences pilotes

Pour l'estimation du canal, la station de base reçoit des informations sur l'état du canal que le terminal lui envoie sous forme de séquences pilotes orthogonales en liaison montante. Dans un scénario de fonctionnement typique, le nombre maximum de séquences pilotes orthogonales dans un intervalle de cohérence de 1 ms est estimé à environ 200, ce qui s'avère insuffisant pour les systèmes multicellulaires. Pour remédier à ce manque, les pilotes sont réutilisés d'une cellule à l'autre, ce qui engendre une interférence entre les séquences dans les cellules adjacentes (Larsson et al., 2014).

1.3.2.3 Complexité de traitement du signal

Les antennes m-MIMO génèrent de grandes quantités de données en bande de base qui doivent être traitées en temps réel. Ce traitement doit être linéaire, ce qui nécessite la conception et la mise en œuvre d'algorithmes optimisés (Larsson et al., 2014).

1.3.2.4 Coût des équipements radio fréquence

La conception de centaines de chaînes RF et d'autres équipements numériques tels que les convertisseurs numériques requièrent des coûts de fabrication.

1.3.2.5 Perturbations matérielles:

m-MIMO utilise un grand nombre d'antennes pour compenser le bruit, les évanouissements et les interférences. Pour éviter les coûts élevés dans sa conception, des composants à faible coût peuvent être employés, ce qui peut générer des imperfections matérielles telles que le bruit de phase (Larsson et al., 2014).

1.3.2.6 Consommation d'énergie interne:

À vrai dire, la technologie m-MIMO ne consomme pas beaucoup d'énergie ; au contraire, elle permet de réduire la puissance rayonnée 1000 fois tout augmentant considérablement le débit des données. Cependant, en pratique, la puissance totale consommée comprend le coût du traitement du signal en bande de base dont la consommation peut être excessive en raison de l'utilisation de nombreux équipement (Larsson et al., 2014).

1.3.3 Applications de la technologie massive MiMo

Le champ d'application de m-MiMo est vaste, dans cette section nous abordons certain domaines qui sont décrits comme suit (Muaayed, 2017):

1.3.3.1 Internet des objets :

Avec l'arrivée de l'Internet des objets (IoT) et des communications de machine à machine (M2M), les réseaux 5G doivent servir un grand nombre d'appareils. Pour ce faire, des capteurs nécessitant de faibles débits de données sont utilisés pour interconnecter ces appareils. Toutefois, cela requiert d'énormes quantités de capteurs, ce qui pose des problèmes à la

connectivité réseau. À cet effet, la technique de m-MIMO est introduite pour gérer les ressources radio.

1.3.3.2 Réseaux de véhicules

L'utilisation de m-MIMO permettra un échange plus rapide de grandes quantités de données entre les véhicules, tout en réduisant les interférences entre les véhicules qui sont équipés de m-MIMO pour effectuer des communications efficaces de véhicule à véhicule (V2V) dans un système de transport intelligent (ITS).

1.3.3.3 Réseaux ferroviaires

Les BS couvrant les voies ferrées pourraient bénéficier de techniques m-MIMO pour transmettre des débits de données élevés pour des trains circulant à grande vitesse.
De plus, cette technique permettra d'interconnecter plusieurs wagons en installant un très grand nombre d'antennes sur le toit du train pour former m-MIMO.

1.3.3.4 Réseaux de sécurité publique

La technologie m-MIMO peut être utilisée pour transmettre des informations de manière sécurisée et fiable à un grand nombre de membres du personnel de la sécurité publique sur un site d'incident.

1.3.3.5 Communications multimédias

Les antennes m-MIMO peuvent contribuer à améliorer la qualité de service dans les communications multimédias en utilisant la technique de formation de faisceau (beam-forming) et la gestion efficace des ressources radio au niveau des couches physiques et MAC (Medium Access Control). Les implémentations en temps réel de haute qualité pourraient aussi avoir des implications importantes dans les scénarios de sécurité publique.

1.3.3.6 Applications de sécurité

La technologie m-MIMO peut être utilisée pour sécuriser la couche physique contre l'écoute par des utilisateurs malveillants, et ce, en utilisant la formation de faisceaux. Cette méthode consiste à envoyer un signal bruit en direction d'un intrus afin de diminuer la puissance de son canal et envoyer le signal information dans la direction du nœud légitime, éliminant ainsi, ou réduisant considérablement la capacité de l'intrus à détecter la transmission des messages non chiffrés.

1.4 Revue de littérature

La cinquième génération des réseaux sans fil (5G) est une technologie prometteuse conçue pour répondre à la demande d'un nombre croissant d'utilisateurs. Répondre à cette demande nécessite des technologies de pointe comme m-MiMo qui est considéré comme l'une des technologies les plus prometteuses pour les réseaux 5G pour augmenter les performances et le débit du réseau. En effet, m-MiMo améliore la technologie MiMo conventionnelle en introduisant des centaines d'antennes et s'avère favorable à la construction de l'infrastructure d'une société numérique du futur. La technologie m-MiMo réduit également les interférences et la complexité de traitement associées à plusieurs utilisateurs et est souhaitable pour éliminer le bruit thermique, les évanouissements et les erreurs d'estimation de canal (Bogale et Le, 2014); (Zirwas, Amin et Sternad, 2016).

Cependant, les performances de m-MiMo sont réduites face aux contraintes majeures que rencontre cette technologie, à savoir la contamination des pilotes, la sécurité à la couche physique ainsi que le coût et la complexité de traitement (Appaiah, Ashikhmin et Marzetta, 2010).

Récemment, les méthodes exploitant les caractéristiques de la couche physique ont été grandement déployées dans la recherche pour faire face aux problèmes des réseaux sans fil. À cet effet, nous avons proposé une solution utilisant les codes Raptor conjointement m-MiMo pour résoudre les contraintes citées ci-dessus. Cependant, l'utilisation des codes Raptor avec

les m-MiMo n'est en aucun cas abordée dans la littérature ; c'est pourquoi notre étude va explorer les travaux de recherche soulevant des solutions des m-MiMo et ceux proposant des solutions des codes Fontaines, plus particulièrement les codes Raptor.

Plusieurs travaux de recherche ont mis de l'avant des solutions pour diminuer l'effet des symboles pilotes contaminés. Parmi ces solutions, celle proposée par (Khoueiry et Soleymani, 2014) utilise les données reçues décodées avec le code Raptor pour estimer le canal. Cette méthode permet d'estimer le canal sans recourir aux séquences pilotes, ce qui évite la contamination du canal et permet une gestion efficace de l'énergie. Néanmoins, cette étude est effectuée sur un canal d'évanouissement lent de Rayleigh, négligeant l'effet du bruit gaussien pour estimer le CSI.

Dans le même contexte, un nouveau système est proposé par les auteurs (Majumder et Verma, 2013), où les symboles d'information décodés avec les codes Raptor sont utilisés pour estimer CSI avec filtre de Wiener. Cependant, cette étude ne peut être efficace pour les réseaux 5G où la technologie m-MiMo est utilisée. En effet, les auteurs étudient un canal d'évanouissement de Rayleigh et ne tiennent pas compte du canal m-MiMo où un grand nombre d'antennes est utilisé. En outre, m-MiMo utilise des détecteurs linéaires qui lui sont adéquats et qui fonctionnent différemment du filtre de Wiener.

Afin de résoudre le problème de l'interférence des symboles contaminés dans m-MiMo, nous avons proposé dans des travaux antérieurs un nouveau modèle (Benzid et Kadoch, 2018). Dans ce modèle, des symboles décodés par les codes Raptor sont utilisés pour estimer le canal avec le détecteur linéaire MMSE.

Dans cette approche, nous avons prouvé que nous pouvons réduire la contamination des pilotes dans m-MiMo en utilisant des symboles décodés au lieu des symboles pilotes transmis.

Comme il a été mentionné auparavant dans cette thèse, le détecteur linéaire MMSE est choisi pour sa robustesse parmi d'autres détecteurs. Cependant, il a été montré que dans m-MiMo, où

un grand nombre d'antennes est utilisé, tous les détecteurs linéaires fonctionnent de manière optimale. Pour approfondir notre recherche, nous avons inclus d'autres techniques de filtrage, à savoir la combinaison de rapport maximum (MRC) et la technique de forçage nul (ZF). D'autre part, trois codes FEC : Raptor, LT et LDPC sont également introduits dans cette étude présentée dans le Chapitre 1.

Cependant, les codes Raptor utilisés pour résoudre le problème des séquences contaminées sont considérés comme une arme à double tranchant. En effet, en raison de leurs pouvoirs leur permettant de récupérer le signal, ces derniers peuvent être exploités comme un outil d'intrusion par un nœud malveillant possédant plusieurs antennes. Ceci met le réseau face à une contrainte d'écoute.

De plus, les réseaux sans fil de cinquième génération (5G) basés sur la transmission de diffusion souffrent d'une menace critique : l'écoute clandestine. Ce problème peut être résolu à l'aide de protocoles cryptographiques ; cependant, les protocoles cryptographiques sont complexes et peuvent être difficiles à mettre en œuvre en raison de la topologie active des réseaux sans fil, qui ne permet pas une gestion efficace des clés de sécurité. Récemment, la méthode de sécurité de la couche physique (PLS) a été appliquée comme solution alternative pour atténuer le problème de confidentialité. Les méthodes PLS exploitent les caractéristiques des schémas de couche physique, y compris la modulation, les multi-entrées massives multi-sorties (m-MiMo) et le codage de canal, pour garantir la confidentialité des données transmises. Une de ces méthodes PLS est le code de fontaine, où le destinataire légitime doit récupérer le message avant que l'espionnage ne le fasse. Cependant, cette fonctionnalité ne peut pas être exploitée dans les réseaux 5G en présence d'un intrus utilisant m-MiMo. De plus, la conception des signaux de bruit artificiel (AN) dans m-MiMo est complexe en matière de calcul et nécessite une consommation d'énergie excessive, ce qui limite la capacité du code de fontaine à garantir le secret des données.

Plusieurs solutions ont été proposées dans la littérature pour sécuriser la couche physique contre l'écoute. Parmi ces solutions, on retrouve la méthode de m-MiMo aidé par AN. Un

signal de bruit artificiel est généré en direction de l'intrus malveillant et dans l'espace nul des utilisateurs légitimes, ce qui dégrade le canal de l'intrus sans affecter l'utilisateur autorisé (Wei et al., 2015) (Zhu, Schober et Bhargava, 2014) (Zhou et McKay, 2010). Néanmoins, pour garantir le secret, ces solutions exigent que le nombre d'antennes d'émission soit supérieur au nombre d'antennes de l'intrus (Goel et Negi, 2008). Le cas échéant, lorsque l'intrus utilise un grand nombre d'antennes pour l'écoute, la sécurité ne peut être garantie. En outre, la conception de AN entraîne une grande complexité de calcul lorsque le nombre d'antennes est grand.

Un autre moyen pour assurer la sécurité utilisant des solutions PLS sans AN a été proposé dans la recherche antérieure (Dean et Goldsmith, 2017). Cependant, ces études, bien qu'elles soient fiables, ne prennent pas en compte le cas d'un intrus utilisant les codes Raptor. D'autre part, il existe beaucoup de solutions dans la littérature qui proposent d'utiliser les codes Fontaine pour sécuriser la couche physique. Cette méthode exploite la propriété de ces codes dans laquelle l'émetteur produit un flux infini de paquets de données et le récepteur collecte ces paquets de données jusqu'à ce qu'il récupère le message ; ensuite, il envoie un message-STOP à la source. Pour exploiter cette fonctionnalité dans la sécurisation du canal, le récepteur légitime doit récupérer le message avant que l'intrus ne le fasse. Ceci peut être réalisé lorsque le nœud malveillant possède un faible SNR faible (Niu et al., 2014) (Sun et Xu, 2019).

Néanmoins, ces solutions ne peuvent pas garantir la sécurité dans les réseaux 5G lorsqu'un nœud malintentionné utilise m-MiMo. À cet effet, dans nos travaux précédents, nous avons mis de l'avant une solution pour le problème d'écoute dans le cas d'un intrus possédant le plus grand nombre d'antennes et utilisant des codes Raptor (Benzid, Kadoch et Cheriet, 2019).

La méthode proposée utilise un code Raptor basé sur LDPC perforé et assisté par un bruit artificiel (AN). L'objectif de cette méthode est de cacher certaines informations aux nœuds intrus et de les brouiller avec un signal de bruit artificiel. En utilisant cette technique, le taux d'erreur binaire (BER) de l'intrus augmente beaucoup plus rapidement qu'il ne le fait lorsqu'il

est transmis sans perforation. Cette méthode vise à réduire l'efficacité du canal de l'intrus, ce qui permet au canal principal de récupérer le signal avant celui-ci.

Par conséquent, la récupération du signal d'origine nécessite une énergie élevée pour atteindre les meilleures performances sur le canal légitime.
Pour contourner cette contrainte, une étude plus approfondie a été proposée dans le chapitre 2. La solution proposée est une analyse théorique menée pour élaborer le mode d'emploi de ces codes dans m-MiMo en présence d'un intrus possédant de grandes ressources.

Cependant, les deux solutions proposées, bien qu'elles aient fait preuve de performance et de fiabilité, présentent une certaine faiblesse due à l'utilisation d'un grand nombre d'antennes et de codes Raptor. Il s'agit du problème de complexité de traitement de signal et de la consommation excessive de l'énergie.

Une meilleure façon de contourner ce problème est d'optimiser le nombre d'antennes en y sélectionnant le meilleur sous-ensemble à l'émetteur ou au récepteur. Cependant, la méthode de recherche exhaustive utilisée dans MiMo conventionnel ne peut être utilisée dans m-MiMo. Plusieurs études ont été effectuées pour proposer une méthode simple et performante afin de diminuer la complexité de calcul et la consommation excessive de l'énergie dans m-MiMo. Parmi ces méthodes, on retrouve celles proposées par (Selvam et Vishvaksenan, 2019). (Gao et al., 2013) (Chang et al., 2017) (Liu et Wang, 2016) (Gao, Vinck et Kaiser, 2017).

Cependant, à notre connaissance, la plupart des solutions proposées dans la littérature, bien qu'elles soient rapides et optimales, supposent que le canal est parfaitement connu lors du choix des antennes ; or, ceci est impossible dans la pratique, principalement lorsque m-MiMo souffre d'une contamination pilote.
Motivés par ces observations, nous avons proposé d'étudier la sélection des antennes en prenant en compte la présence de la contamination pilote sous CSI imparfait.

Pour ce faire, nous avons utilisé un algorithme de watter filling basé sur la maximisation du critère de capacité pour trouver le sous-ensemble optimal des antennes (Phan et Tellambura, 2007). De plus, nous avons eu recours aux symboles décodés avec les codes LDPC pour estimer le canal (Benzid et Kadoch, 2018). L'idée derrière cette approche est de récupérer les données d'informations et de les utiliser pour estimer le canal qui rentre dans la maximisation de la capacité.

CHAPITRE 2

FOUNTAIN CODES AND LINEAR FILTERING TO MITIGATE PILOT CONTAMINATION ISSUE IN MASSIVE MIMO

Djedjiga Benzid [a], Michel Kadoch [b]

[a, b] Department of Electrical Engineering, École de technologie supérieure,
1100 Rue Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Paper Published in Network and Communication Technologies, January 2019

2.1 Abstract

The fifth generation of cellular mobile (5G) is a future technology designed to meet the demand of a growing number of users. Meeting this demand requires advanced technologies; very large multi-input multi-output (MiMo), also known as massive MiMo (m-MiMo), is considered to be one of the most promising technologies for 5G networks. However, the performance of m-MiMo is limited by pilot contamination. To mitigate pilot contamination issues in m-MiMo, we previously proposed a new scheme where Raptor-decoded symbols are used to estimate the channel using the minimum mean square error (MMSE) technique. The main benefit of this method is that the receiver does not need a transmitted pilot symbol to evaluate the channel, which saves power at transmission. Our results additionally showed that the MMSE scheme achieved the perfect channel. We originally used the MMSE detector and Raptor code because they have been shown to be robust among other schemes of linear detectors and corrector codes; however, in the case of m-MiMo, all linear detectors have been shown to work optimally. In this article, we enhance our previous method by including an additional linear filter. For this purpose, we consider two additional detectors, zero-forcing (ZF) and maximum-ratio combining (MRC), in addition to an MMSE detector. Our objective was to determine the ideal filtering technique and the robustness of fountain code for addressing the pilot

contamination problem. Simulation results showed that the ZF detector attains the same level of performance as the MMSE detector using Raptor-decoded symbols, while the MRC detector achieved lower performance compared to the other two schemes.

2.2 Introduction

To meet the growing user capacity of mobile cellular networks, a new generation of cellular mobile (5G) is planned for 2020, where advanced systems such as massive multi-input multiple-output (m-MiMo) are used to increase network performance and throughput. M-MiMo schemes enhance conventional MiMo technology by incorporating hundreds of antennas and are favorable for building the infrastructure of a digital future society. They are reliable, resilient, and energy-efficient, and can connect users to the Internet and to other network infrastructure and clouds (Larsson et al., 2014). The advanced technology of m-MiMo also reduces the interference and processing complexity associated with multiple users and is desirable for eliminating thermal noise, fading, and channel estimation errors (Bogale et Le, 2014); (Zirwas, Amin et Sternad, 2016). However, these advantages are counteracted by pilot contamination, a major constraint affecting m-MiMo (Appaiah, Ashikhmin et Marzetta, 2010).

Pilot contamination is interference that results from processing the same pilot symbols in adjacent cells. To recover the received signals in multi-cell systems, knowledge of channel state information (CSI) is generally required at the base station (BS). To evaluate the CSI, the BS receives an orthogonal pilot sequence from each user. However, in multi-cell networks, it is not possible to assign an exclusive orthogonal pilot sequence to a single user because the channel coherence interval is narrow. The network therefore reuses pilot sequences from various cells, generating interference between the received channel estimation in a specific cell and pilots transported by users of other cells. This article addresses the pilot contamination issue in m-MiMo and is organized as follows: Section 2.3 describes previous research on pilot contamination; Sections 2.4 and 2.5 introduce the

channel estimation schemes and fountain codes, respectively, that are used in m-MiMo; Section 2.6 describes the system model that we propose; Section 2.7 discusses our simulation results; and Section 2.8 concludes the paper.

2.3 Literature Review

One way to fix the pilot contamination problem is to avoid it by assuming that CSI is well-known at the receiver (Appaiah, Ashikhmin et Marzetta, 2010). However, in practice, it is impossible for the receivers to achieve a perfect CSI. The channel must therefore be estimated to recover the received signal. Several solutions to diminish the effect of contaminated pilot symbols have been proposed; one of the most well-known of these methods is the Single decomposition (SVD) method. However, it was shown that these channel estimation methods become highly complicated when using multiple antennas (Bogale et Le, 2014). To solve this problem, Bogale and Le (2014) proposed an iterative algorithm for a multi-user m-MiMo system to enhance the pilot symbols and evaluate the channel. Nevertheless, the authors assumed that the receiver has perfect knowledge of the CSI, which is difficult to obtain in practice.

Another method to avoid the pilot interference issue is to estimate the channel using the received data. The main advantage of this technique is that the sender does not need to transmit supplementary bits or pilot symbols to achieve a similar level of performance, thus saving the energy the transmitter would need to transmit the pilots. (Khoueiry et Soleymani, 2014) proposed one such estimation scheme. The main idea behind their proposition was to calculate the CSI when it is unavailable at the receiver. They used Raptor codes in a slow Rayleigh fading channel to evaluate their scheme; however, they neglected the Gaussian noise in their estimation of the CSI. (Majumder et Verma, 2013) proposed a similar system, in which Raptor-decoded information symbols were used to estimate CSI using a Wiener filter estimator; however, this approach is not suitable for the large number of antennas used in m-MiMo, where detection schemes are different from the

Wiener filter. To fix the problem of symbol interference in m-MiMo systems with a large number of antennas, we previously proposed a new scheme in which Raptor-decoded symbols are used to estimate the channel using linear MMSE detectors (Benzid et Kadoch, 2018). Our approach effectively mitigated pilot contamination in m-MiMo using decoded symbols instead of transmitted pilot symbols. We chose the linear MMSE detector because it is more robust than other detectors; however, it has been shown that all linear detectors perform optimally in m-MiMo. In this paper, we complement our previous study by considering alternative linear detection schemes. We specifically compare the MMSE receiver with maximum-ratio combining (MRC) and zero-forcing (ZF) receivers to evaluate whether the choice of detector influences the efficacy of our approach for avoiding pilot contamination.

2.4 Channel Estimation

In wireless networks, symbols must be effectively recovered at the receiver to achieve a reliable transmission. However, effective symbol recovery can be complicated by interference. To reduce the impact of inter-symbol interference, equalization techniques are used to remove the residues. One of the principal detection techniques used in practice is the maximum likelihood (ML) detector. This technique optimizes the performance of the receiver, allowing it to detect all signals transmitted from the transmitter. However, it has been shown that the complexity of the ML technique increases exponentially when the number of users increases.

To reduce the decoding complexity of ML detectors, the receiver can instead use linear filtering on the received signal. Although linear detection schemes are less reliable than ML detection, linear detectors work optimally when a large number of antennas are used, as in m-MiMo. Three schemes of linear detection are considered in this paper: maximum ratio-combining (MRC) receivers, zero-forcing (ZF) receivers, and minimum mean square error (MMSE) receivers (Muaayed, 2017) (Ngo, 2015).

2.4.1 Maximum-Ratio Combining (MRC)

The main principle of the MRC detection technique is to maximize the received signal-to-noise ratio (SNR) of each vector. The receiver multiplies the received stream with the conjugate transpose of the channel matrix $\boldsymbol{H}$ and then detects each vector separately, reducing the implementation complexity of the detector. Despite this advantage, the MRC receiver performs poorly in scenarios where the interference is restricted.

2.4.2 Zero-Forcing Receiver (ZF)

The objective of zero-forcing (ZF) receivers is to avoid the effects of the contaminated pilots by using the pseudo-inverse of the channel gain matrix. The main advantage of ZF receivers is that signal processing is simple; however, using the pseudo-inverse of the channel matrix can also amplify the noise. If the interference between the symbols is important, the performance of the receiver deteriorates. ZF receivers are more complex to implement than MRC receivers because they must additionally compute the channel gain matrix.

2.4.3 Minimum Mean Square Error (MMSE)

To reduce symbol alteration, the MMSE scheme uses the least squares technique between the evaluated random events and the intended events. The MMSE scheme is considered the most efficient linear filter because it maximizes the received SNR.

2.5 Erasure and Rateless Codes

In coding theory, an erasure code is a forward error correction code that adds redundancy to the system to tolerate failures. This method does not require retransmission or feedback. The transmitter sends data packets to the receiver and adds redundancy to the message; no acknowledgement is needed to confirm received packets. The receiver rejects any

corrupted packet (Moreira et Farrell, 2006). Erasure codes are useful in systems where retransmissions are costly or impossible.

Rateless codes are characterized by a non-fixed code rate: the source can generate a limitless number of encoded packets, with the number of packets determined on the fly (Madge et MacKay, 2006). When a rateless code is used, the transmitter floods the receiver with unlimited streams of coded bits. The receivers collect bits until the content has been retrieved, and then they send a “stop” message to the transmitter.

2.5.1 Low-Density Parity-Check (LDPC)

Among the erasure codes, low-density parity-check (LDPC) codes are the most important class. Developed by Robert Gallager in the early 1960s, LDPC codes are decoded using iterative belief propagation (BP) algorithms, which make LDPC decoders very powerful since they attain the Shannon limits in terms of their decoding performance. LDPC codes perform better on additive white Gaussian noise (AWGN) channels and generally do not perform optimally on non-Gaussian channels (Farrell et Honary, 2005). The most important applications of LDPC codes are the Internet and wireless networks (Farrell et Honary, 2005) .

2.5.2 Fountain Code

A fountain code, also known as a rateless erasure code, can be compared to water dropping from a fountain into a container. In a fountain code system, the transmitter (the fountain) generates a continuous flow of transmitted data packets and the receiver (the container) collects data packets to recover the sent message. Fountain codes, such as the Luby Transform (LT) and Raptor codes, are a promising form of sparse graph code.

2.5.3 Luby Transform (LT)

Designed by Michael Luby in 1998, the Luby transform (LT) code is the first application of universal fountain codes. The decoding approach employed by LT codes is analogous to the approach used by LDPC decoding.

2.5.4 Raptor Codes

Raptor codes are an enhancement of LT codes designed in late 2000 and published in late 2001 (Shokrollahi, 2006). The Raptor codes use two concatenated codes: an LT code and an erasure code. The erasure code used in the Raptor code is generally the LDPC code.

2.6 System Model

In this section, we present a novel channel estimation scheme. Figure 2.1 illustrates the block diagram of the system. The transmitter comprises a Raptor encoder and a binary phase-shift keying (BPSK) modulator. The Raptor encoder is a succession of two encoders: an LDPC encoder and an LT encoder. The receiver includes the channel estimator followed by a Raptor decoder, which contains an LT decoder and an LDPC decoder.

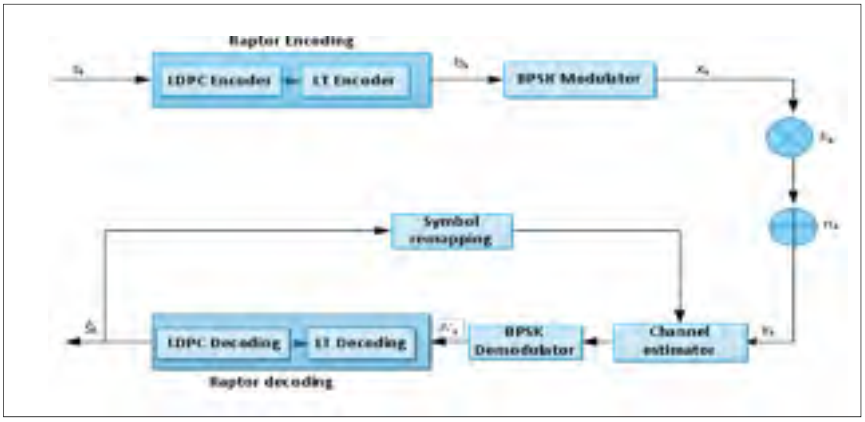

Figure 2.1 Model system

At the transmitter, the source generates a block message $sk \in k$ = {0,1, …...K− 1}, and sk is converted to the code word $bk \in of\ k$= 0,1, … L − 1 bits. The BPSK modulator is used to generate the symbols vector $xk \in \{-1,1\}$, k= 0,1, … L − 1. These symbols xk are transferred over a slow flat fading channel. At the receiver, the signal yk is received at the linear filter node (channel estimator). The equation of the received signal after the channel has been estimated is given as follows:

$$Y = H * X + N \tag{2.1}$$

H is the channel matrix $\in \mathbb{C}^{NxN}$, which defines the fading coefficients of the transmit antennas N_t and the receive antennas N_r. The form of H is presented below:

$$H = \begin{bmatrix} h_{11} & \dots & h_{1N_r} \\ \vdots & \ddots & \vdots \\ h_{N_t1} & \cdots & h_{N_tN_r} \end{bmatrix}$$

The coefficients of H are independent and identically distributed (i.i.d.), with zero mean and variance σ_h^2. H is modelled as a Rayleigh random variable, and its probability density function is specified by:

$$p(h_k) = \frac{h_k}{\sigma_h^2} e^{\frac{h_k}{2\sigma_h^2}}, h > 0 \tag{2.2}$$

Yin Equation (2.1) is the received symbols vector, $X \triangleq [x_1 \dots x_k]^T$ is the vector of transmitted symbols, and N is the additive white Gaussian noise (AWGN) vector with elements that are i.i.d. and have zero mean and variance σ_h^2.

2.6.1 Channel Estimation

In this section, we describe the three most common techniques for estimating the channel using decoded symbols.

2.6.1.1 MMSE Channel Estimation

Let $\widehat{H}$ be an estimated random variable coefficient of H and Y be the observed random variable. X is the transmitted pilot symbols. Assume that R_{HY} is the cross-covariance between H and Y and R_{YY} is the covariance of Y. The estimated channel of H can then be given as follows:

$$\widehat{H} = (R_{HY}R_{YY}^{-1})Y \tag{2.3}$$

$$R_{HY} = E\{HY^T\} = E\{H(HX+N)^T\} = E\{HH^TX^T\} + E\{(HN^T)\} \tag{2.4}$$

$(\cdot)^T$ and E{·} denote the matrix transpose and expected value, respectively.

The term $E\left\{\left(HN^T\right)\right\} = 0$ because H and N are i.i.d. Assume that $E\{HH^T\} = N_t\sigma_h^2 I$ and $E\{NN^T\} = N_t\sigma_n^2 I$, where I is the matrix identity, σ_n is the variance of the noise signal, and σ_h is the variance of the channel H. Because X does not change, we can state:

$$E\left\{HH^TX^T\right\} = X^TE\left\{HH^T\right\} = N_t\sigma_h^2X^T \tag{2.5}$$

By substituting Equation (2.5) in Equation (2.4), we have:

$$R_{HY} = N_t\sigma_h^2X^T \tag{2.6}$$

$$R_{YY} = E\{YY^T\} = XX^TE\{HH^T\} + E\{NN^T\}$$

$$R_{YY} = XX^TN_t\sigma_h^2I + N_t\sigma^2I \tag{2.7}$$

By substituting Equations (2.6) and (2.7) in Equation (2.3), we have:

$$\widehat{H} = (\mathrm{X}\mathrm{X}^T + \frac{\sigma_n^2}{\sigma_h^2}I)^{-1}\mathrm{X}^TY \tag{2.8}$$

As discussed above, to resolve the issue of contaminated pilot symbols, we consider Raptor-decoded information as an alternative to pilot symbols for estimating CSI. Pilot symbols X are therefore replaced by $\hat{S}$ in Equation (2.8) and the estimated channel $\widehat{H}$ is expressed as shown below:

$$\widehat{H} = (\hat{S}\hat{S}^T + \frac{\sigma_n^2}{\sigma_h^2} I)^{-1} \hat{S}^T Y \tag{2.9}$$

2.6.1.2 ZF Channel Estimation

The goal behind using ZF channel estimation is to minimize the error vector. The error vector is the norm of $Y - HX$, where Y is the measurement or observed random variable, X is the transmitted pilot symbols, and H is the unknown random variable coefficients vector. Let $\widehat{H}$ be the estimated random variable coefficients of H and let F be the error vector. In this case, F can be expressed as follows:

$$F = \|Y - HX\|^2 = (Y - HX)^T (Y - HX) \tag{2.10}$$

To minimize the error F we use vector differentiation $\frac{\mathrm{dF}}{\mathrm{dH}}$, and we set the derivative equal to zero so that Equation (2.10) becomes:

$$\frac{dF}{dH} = 0 \Rightarrow -2X^T Y + X^T HX = 0 \tag{2.11}$$

By resolving Equation (2.10), the estimate of H for the ZF scheme is given as

$$\widehat{H} = X^T Y (X^T X) \tag{2.12}$$

Because the information-decoded symbols $\hat{S}$ are used as a substitute to pilot symbols X, as in Section 2.6.1.1, Equation (2.12) becomes:

$$\hat{H} = \left(\hat{S}\hat{S}^T\right)^{-1} \hat{S}^T Y \tag{2.13}$$

We note that at high SNR, when σ_n trends to 0, Equation (2.9) of the MMSE channel estimate becomes similar to Equation (2.13) of the ZF channel estimate.

2.6.1.3 MRC Channel Estimation

The filtering in MRC channel estimation is indicated by multiplying the received signal by the conjugate transpose of the channel estimate. In our case, we use the MMSE channel estimate. From Equations (2.1) and (2.9), this produces:

$$\tilde{Y} = \hat{H} * Y \tag{2.14}$$

Let $\hat{h}_j$ be the j^{th} element of $\hat{H}$, where $\hat{H}$ is the MMSE channel estimate calculated in Equation (2.9). $\hat{h}_j$ is expressed as:

$$\hat{h}_j = (\hat{S}_j \hat{S}_j{}^T + \frac{\sigma_n^2}{\sigma_h^2} I)^{-1} \hat{S}_j Y_j \tag{2.15}$$

By substituting Equation (2.14) in Equation (2.13), we get:

$$\tilde{Y}_{j+1} = (\hat{S}_j \hat{S}_j{}^T + \frac{\sigma_n^2}{\sigma_h^2} I)^{-1} \hat{S}_j Y_j Y_{j+1} \tag{2.16}$$

2.6.2 Decoding

After the channel has been estimated, the soft decoding process is performed using the belief propagation (BP) algorithm. The messages are passed between the variable nodes o and the check nodes i. The likelihood ratios (LLR) of channels for each coded bit are given as follows:

$$Z_0 = \ln\left(\frac{P(\hat{s}_k = 1 | y_k, h_k)}{P(\hat{s}_k = -1 | y_k, h_k)}\right) \tag{2.17}$$

By employing the independence property between $\hat{S}_k$ and $\hat{h}_k$ and using the Bayes rule, we can convert Equation (2.17) to:

$$Z_0 = \ln\left(\frac{P(y_k|\mathrm{h}_k,\hat{s}_k=1)}{P(y_k|\mathrm{h}_k,\hat{s}_k=-1)}\right) + \ln\left(\frac{P(\hat{s}_k=1)}{P(\hat{s}_k=-1)}\right) \quad (2.18)$$

With equal probability for the input S, the term on the right side of Equation (2.17) is equal to zero. In the output of the matched filter, y_k, the probability is given as follows:

$$P\left(y_k|\mathrm{h}_k,\hat{s}_k=\pm 1\right) = \frac{1}{\sigma_n\sqrt{2\pi}} e^{\frac{(y_k \pm h_k)^2}{2\sigma_n^2}} \quad (2.19)$$

By substituting Equation (2.19) in Equation (2.18), we have:

$$Z_0 = \frac{2\hat{h}_k}{\sigma_n^2} y_k \quad (2.20)$$

The estimated channel can be calculated in the first iteration of decoding, so Z_0 is expressed as:

$$Z_0 = \frac{2}{\sigma_n^2} y_k$$

2.6.2.1 Raptor Decoding

Raptor decoding is used to retrieve the transmitted message. Figure 1.2 shows the decoding graph for Raptor code. At iteration 0 of the BP decoding algorithm, if the output node o and the input node i are neighbors, the LLR of the received channel from o to i is expressed as follows:

$$m_{o,i}^{(0)} = Z_0 \quad (2.21)$$

For all subsequent iterations, $l = 1, \cdots, N^{itr}$, the LLR updating process of LT decoding is completed as follows (Etesami et Shokrollahi, 2006):

$$m_{io}^{(l)} = \sum_{o' \neq o} m_{o'i}^{l-1} \quad (2.22)$$

$$i = 1, \ldots, n$$

$$tanh\left(\frac{m_{o,i}^{(l)}}{2}\right) = tanh\left(\frac{z_0}{2}\right) \prod_{i' \neq i} tanh\left(\frac{m_{i',o}^{(l)}}{2}\right) \quad (2.23)$$

o=1,…,L

$m_{o,i}^{(l)}$ and $m_{i,o}^{(l)}$ are the messages sent from o to i and from i to o, respectively, at iteration l. Z_0 is the LLR corresponding to the output symbo l o calculated in Equation (2.17) and received from the channel. After processing the decoder for l iterations, the LLR of each input node i is given as:

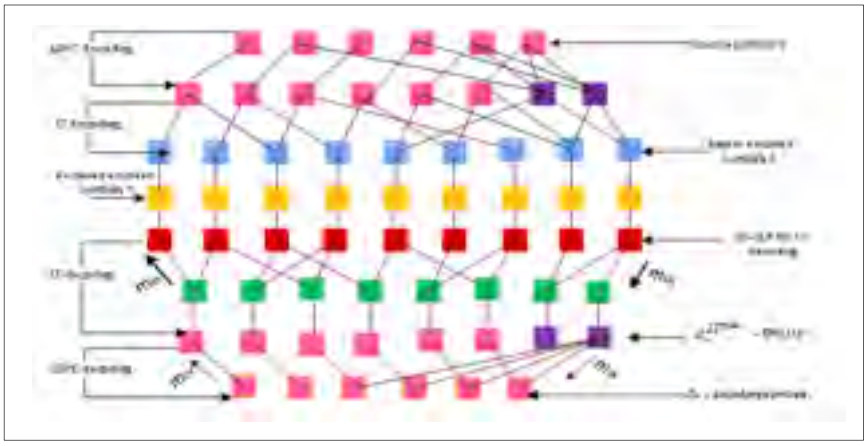

Figure 2.2 Decoding graph of Raptor code

$$d_i^{LT^l} = \sum_{o \in P(i)} m_{oi}^l \quad (2.24)$$

At iteration N^{itr}, the LLR of the input nodes is calculated as:

$$d_i^{LT^{N_{iter}}} = \sum_{o \in P(i)} m_{oi}^l \quad (2.25)$$

where $P(i)$ is the sum of overall output bits o adjacent to i.

The LLR calculated in Equation (2.25), named the output LLR, is the LLR obtained from LT decoding. This LLR is considered the *a priori* LLR and is used as an input for LDPC decoding.

At iteration 0 of the decoding algorithm, the messages sent by each variable node to its adjacent check nodes are the LLRs obtained from the LT decoding. The procedure for updating the LLR for LDPC decoding is given by:

$$m_{v,c}^{(0)} = d_v^{LT^{N_{iter}}} \text{ if o and i are neighbours} \tag{2.26}$$

$$tanh(\frac{m_{c,v}^{(l)}}{2}) = \prod_{\substack{v=1 \\ v\prime \neq v}}^{n} tanh(\frac{m_{v\prime,c}^{(l-1)}}{2}) \tag{2.27}$$

$$m_{vc}^{l} = m_{v,c}^{(0)} + \sum_{c\prime \neq c} m_{c\prime,v}^{l-1} \tag{2.28}$$

$m_{c,v}^{l}$ are the messages of the LDPC decoder. The messages are transferred from the variable nodes v to the check nodes c and from the check nodes c to the variable nodes v, respectively. At iteration l, at the LDPC decoder, we get:

$$Z_v = \sum m_{c',v}^{l} \tag{2.29}$$

For each decoded bit (c, v), a hard decision is made as follows:

$$\hat{S} = \begin{Bmatrix} 0, & if & m_{io}^{APP} \leq 0 \\ 1, & if & m_{io}^{APP} \geq 0 \end{Bmatrix} \tag{2.30}$$

After the hard decision, the estimated channel $\widehat{H}$ is recalculated using Equation (2.9).

2.6.2.2 LT Decoding

The belief propagation (BP) algorithm is used for the soft decoding process. LT decoding consists of LDPC decoding. At iteration 0 of the BP decoding algorithm, if the output node *o* and the input node *i* are neighbors, then the received channel LLR from o to i is expressed as follows:

$$m_{o,i}^{(0)} = Z_0 \text{ if o and i are neighbours} \tag{2.31}$$

$$tanh(\frac{m_{o,i}^{(l)}}{2}) = tanh(\frac{z_0}{2}) \prod_{i' \neq i} tanh(\frac{m_{i',o}^{(l-1)}}{2}) \tag{2.32}$$

The process of updating variable nodes at iterations l = 1, $\cdots$,N^{itr} is given by:

$$m_{io}^{(l+1)} = \sum_{o' \neq o} m_{o'i}^{l} \tag{2.33}$$

At the N^{itr} iteration, the LLR of each variable node is computed as:

$$m_{io}^{N_{iter}} = \sum_{o' \neq o} m_{o'i}^{l} \tag{2.34}$$

For each decoded bit (*o, i*), the hard decision is made as follows:

$$\hat{S} = \begin{cases} 0, & if \quad m_{io}^{N_{iter}} \leq 0 \\ 1, & if \quad m_{io}^{N_{iter}} \geq 0 \end{cases} \tag{2.35}$$

2.6.2.3 LDPC Decoding

At iteration 0 of BP decoding algorithm, if the output node *o* and the input node *i* are neighbors, the received channel LLR from o to i is expressed as follows:

$$m_{o,i}^{(0)} = Z_0 \tag{2.36}$$

$$tanh(\frac{m_{o,i}^{(l)}}{2}) = tanh(\frac{m_{i',o}^{(l)}}{2}) \tag{2.37}$$

To update variable nodes at iteration *l,* where $l = 1, \cdots N^{itr}$, the message from LDPC variable nodes to check nodes is calculated as:

$$m_{io}^{(l+1)} = Z_0 + \sum_{o' \neq o} m_{o'i}^{l} \tag{2.38}$$

At iteration N^{itr}, the *a posteriori* log-likelihood ratio is calculated, and the decision information of each variable node is computed as shown below:

$$m_{io}^{APP} = Z_0 + \sum_{o' \neq o} m_{o'i}^{l} \tag{2.39}$$

For each decoded bit (*o, i*), a hard decision is made as follows:

$$\hat{S} = \begin{cases} 0, & if \quad m_{io}^{APP} \leq 0 \\ 1, & if \quad m_{io}^{APP} \geq 0 \end{cases} \tag{2.40}$$

2.7 Simulation and Results

In this section, we present the numerical results from simulations using our proposed channel estimation and decoding scheme. The model system shown in Fig. 2.1 was evaluated with a simulated m-MIMO system that contained 16 antennas at the receiver and transmitter. We used Raptor code at a rate of 0.98 and LT code and LDPC code with the degree distribution used by (Majumder et Verma, 2013). The results achieved using our system are then compared to other approaches found in the literature and to regular estimator systems. In this paper, we use the

term “regular estimator systems” to indicate detectors that do not use decoded information to estimate the channel.

2.7.1 Channel Estimation Using MMSE and Raptor Code

Three scenarios are studied in this subsection: perfect CSI available at the receiver, our proposed scheme, and no CSI available at the receiver. In all systems, Raptor-decoded symbols were used to estimate the MMSE channel scheme. The length N of the code word was 800,000 bits, and the message length K was 7,840 bits.

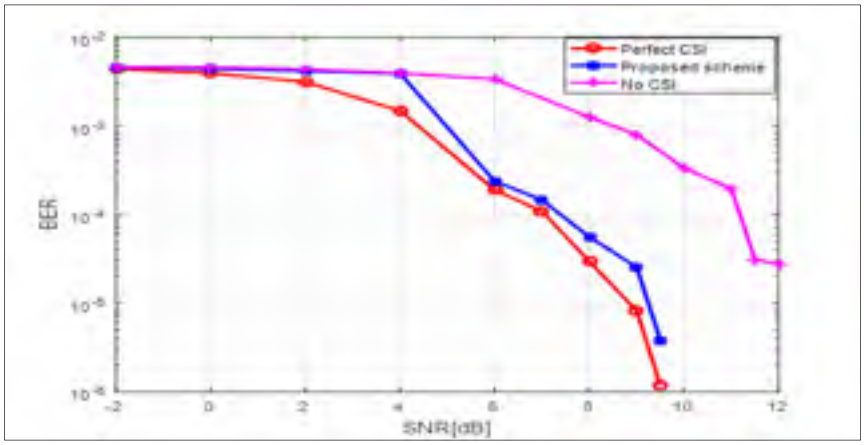

Figure 2.3 Channel estimation using MMSE and Raptor code

As shown in Figure.2.3, our proposed scheme (blue) achieved results that were comparable to the ideal scenario in which the state of the channel is available at the receiver (perfect CSI graph, red). This scheme recorded a bit error ratio (BER) of 10^{-6}. Our scheme performs better than the scenario where the CSI is unknown at the receiver (magenta), attaining a lower SNR threshold and BER.

The threshold SNR values from our proposed scheme are comparable to those obtained by (Khoueiry et Soleymani, 2014); however, we achieved a smaller BER than (Khoueiry et Soleymani, 2014) were able to obtain.

2.7.2 Channel Estimation Approach Using MMSE , LT and LDPC Codes

In this subsection, our proposed Raptor code scheme is compared to schemes that use LT- or LDPC-decoded symbols. All schemes used an MMSE detector. The length *N* of the code word was 15,860 bits, the length *K* of the message was 160,000 bits, and the number of transmit and receive antennas was the same as before.

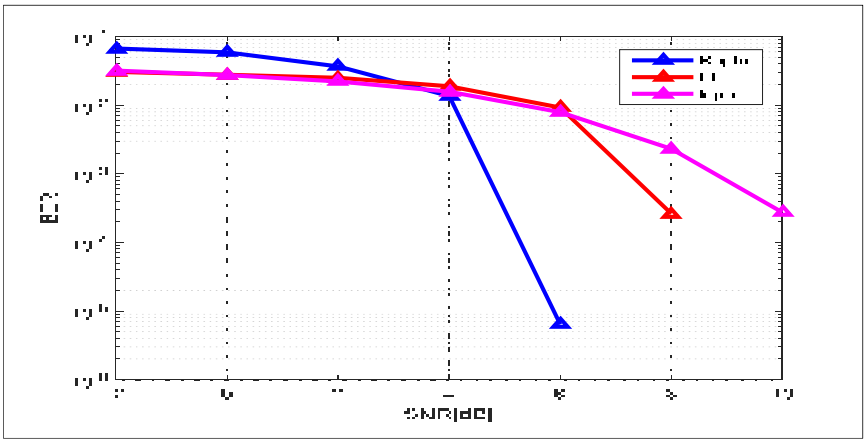

Figure 2.4 MMSE estimation using LDPC, LT and Raptor codes

Figure 2.4 shows that Raptor code performs better than the LT and the LDPC codes when using an MMSE detector. The Raptor code performs about 2 dB from the LT code and 4 dB from the LDPC code. The LDPC codes achieve the worst BER values, presumably because LDPC codes are designed to be used on additive white Gaussian noise (AWGN) channels and do not perform well on non-Gaussian channels (Farrell et Honary, 2005). Raptor codes perform better than LT codes because the structure and characteristics of rateless codes make them better at correcting errors.

2.7.3 Raptor Code with MMSE, ZF, and MRC Detectors

In this subsection we consider two additional filtering systems, ZF and MRC, which are both

simulated using Raptor-decoded symbols. In this simulation, we estimated a message with a length *K* equal to 16,000 bits. The length *N* of the code word was 160,000 bits and the number of transmit and receive antennas was the same as before.

As shown in Figure 2.5, the Raptor code in this MMSE simulation did not have the same SNR threshold or BER as the simulation presented in Section 2.7.1. This is because the simulation in this subsection used a lower number of decoding iterations and a shorter code length than the simulation in Section 2.7.1.

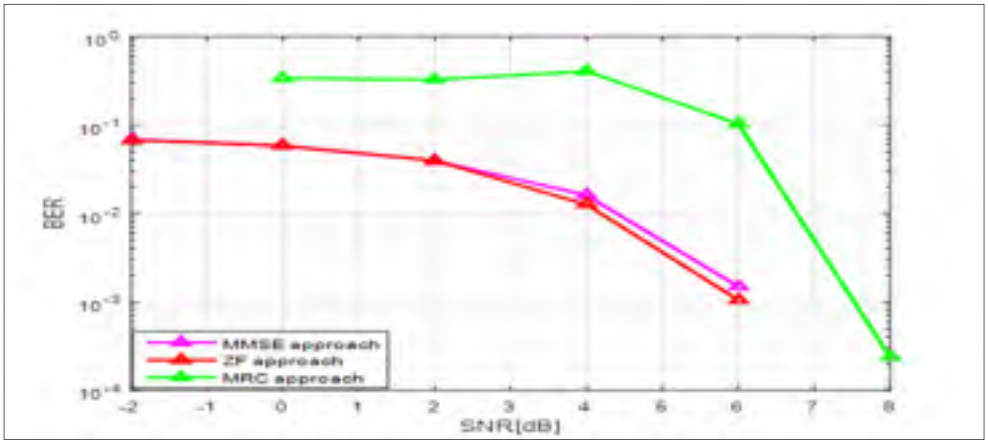

Figure 2.5 MMSE, ZF and MRC estimated using Raptor-decoded symbols

Figure 2.5 shows that both ZF and MMSE receiver schemes perform equally well using Raptor-decoded symbols and outperform the MRC technique. We can obtain the same performance for ZF and MMSE receivers because the number of antennas is high, which allows ZF receivers to obtain a high SNR, as explained in Section 2.6.1.2 When the SNR is high, both MMSE and ZF perform similar calculations for the channel estimate and therefore achieve the same performance. Because ZF and MMSE achieve similar performance outcomes, the remaining simulations presented in this section focus only on ZF and MMSE.

2.7.4 Channel Estimation using MMSE and ZF and Raptor code

In this subsection, we consider the case when the channel is estimated with received symbols using regular MMSE and ZF filters, which means that Raptor code is used to recover the information but not to estimate the channel. We name this scenario "channel estimation with no decoded information" and compare the results to those obtained from our proposed scheme, where decoded symbols are used to obtain the CSI.

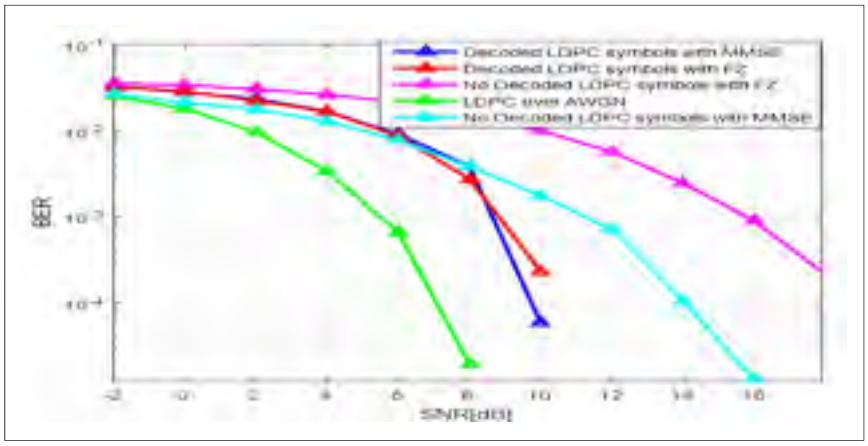

Figure 2.6 Raptor-decoded symbols with MMSE and ZF

In this simulation, we estimated a message with length K equal to 16,000 bits. The length N of the code word was 160,000 bits and the number of transmit and receive antennas was the same as before.

Figure 2.6 shows that ZF and MMSE receivers reached the same SNR threshold of 8 dB using LDPC-decoded symbols to estimate the channel. However, when no decoded symbols were used, the performance of both ZF and MMSE receivers deteriorated, as evidenced by their lower SNR threshold. This result is logical: the decoded information was recovered with few errors, and so using the correctly decoded information to estimate the channel adds robustness to the detector scheme.

2.7.5 Channel Estimation Using MMSE, ZF and LT Code

In this subsection, we compare the use of LT-decoded information over an AWGN channel to schemes that use either LT-decoded or no decoded information over a fading channel. The channel was estimated with MMSE and ZF techniques. In this simulation, we estimated a message with a length K equal to 16,000 bits. The length N of the code word was 160,000 bits, and the number of transmit and receive antennas was the same as before.

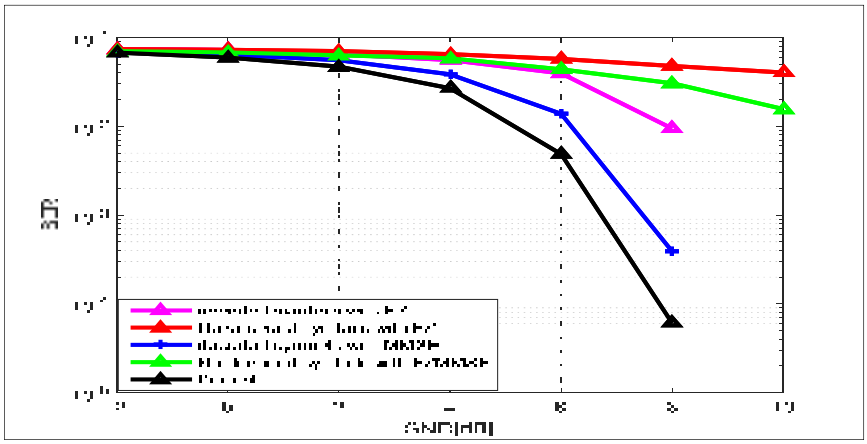

Figure 2.7 LT code with MMSE and ZF

As shown in Figure 2.7, the LT code over an AWGN channel (blue) and the LT code over a fading channel achieved the same SNR threshold and BER when estimated with MMSE-decoded symbols. However, the fading channel estimated with no decoded information, using either MMSE or ZF receivers, achieved a worse SNR threshold than the channel estimated with LT-decoded information by approximately 2 dB. This result was expected, because decoded information contains fewer errors than information that has not been decoded. We additionally noticed that the MMSE and ZF receivers did not achieve the same level of performance using LT code as they did using Raptor codes. This is because the Raptor code is better at correcting errors; using Raptor code to estimate the channel thus enhances the performance of ZF receivers, which should work optimally when the number of antennas is high.

2.7.6 Channel Estimation using MMSE and ZF and LDPC Code

In this section, we simulate a scenario using LDPC-decoded information over an AWGN channel and compare the results to those obtained using LDPC codes over a fading channel with either decoded information or no decoded information. Simulations included either MMSE or ZF estimation. As shown in Fig. 8, LDPC codes over an AWGN channel (green) performed better than LDPC over a fading channel.

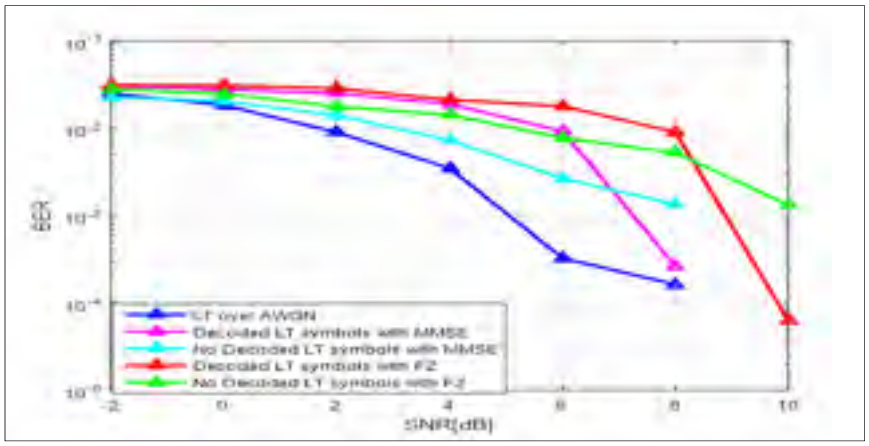

Figure 2.8 LDPC using MMSE and ZF

As discussed in previous sections, the LDPC code performs well on AWGN channels because it was designed to be used on AWGN; it does not perform well on non-Gaussian channels (Farrell et Honary, 2005). We note that the LDPC code over a fading channel with decoded information, using either MMSE or ZF, performed better than with no decoded information. Because the decoded information has been corrected, it is more reliable and therefore more robust for channel estimation.

2.8 Conclusion

In this article, we presented a new scheme for resolving the pilot contamination problem in m-MiMo. The main idea behind our approach is to use decoded symbols as an alternative to transmitted pilot symbols for estimating the channel. In our previous work, we studied MMSE

channel estimation with Raptor-decoded symbols to evaluate the CSI in m-MiMo. To enhance our research, we extended our work to include other linear detectors for estimating the channel and other corrector codes for obtaining decoded symbols. Specifically, we included ZF and MRC receivers to evaluate the channel and the LT and LDPC codes to obtain corrected information. We evaluated our approach by simulating several scenarios. Numerical results show that, when a large number of antennas are used, MMSE and ZF receivers perform similarly. In addition, we show that Raptor-decoded symbols are better than LDPC and LT decoding schemes for estimating the channel, thus proving that using Raptor-decoded symbols with linear filtering can prevent pilot contamination in m-MiMo. The main advantage of our proposed approach is that it saves energy: because pilot symbols are not required at the receiver, power consumption at the transmit antennas decreases. Another benefit of our new system is that it is robust and reliable, achieving a smaller BER compared to other methods of channel estimation. Finally, by using corrector code to estimate the channel, we avoid network overhead. Because the corrector code adds redundancy to the sent packet, retransmission or feedback are not required.

CHAPITRE 3

INVITED PAPER: RAPTOR CODE AND MASSIVE MIMO FOR SECURE WIRELESS DELIVERY IN 5G

Djedjiga Benzid [a], Michel Kadoch [b]

[a, b] Department of Electrical Engineering, École de technologie supérieure,
1100 Rue Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Paper Published in Journal of Electrical and Electronic Engineering, november 2019

3.1 Abstract

Fifth generation (5G) wireless networks based on broadcast transmission suffer from a critical threat: eavesdropping. This issue can be fixed using cryptographic protocols; however, cryptographic protocols are complex and can be challenging to implement due to the active topology of wireless networks, which does not permit effective management of security keys. Recently, the physical layer security (PLS) method has been applied as an alternative solution for mitigating the privacy problem. PLS methods exploit the characteristics of physical layer schemes, including modulation, massive multi-input multi-output (m-MiMo), and channel coding, to ensure the privacy of transmitted data. One such PLS method is the fountain code, where the legitimate receiver must recover the message before the eavesdropper does. However, this feature cannot be exploited in 5G networks in the presence of an intruder using m-MiMo. Furthermore, the design of artificial noise (AN) signals in m-MiMo is computationally complex and requires excessive energy consumption, limiting the ability of fountain code to ensure data secrecy. In this article, we propose a new method to avoid this problem by judiciously exploiting the features of both fountain code and m-MiMo. Our new approach uses the Raptor code, as well as the m-MiMo parameters aided by an AN signal, while reducing the transmission power of the AN. Numerical results indicate that our new approach ensures the protection of legitimate users on the channel and minimizes energy

expenditure, making our approach a greener and more secure method for data transmission.

3.2 Introduction

The technological revolution of the Internet is thriving with the arrival of connected objects. By 2020, mobile cellular network capacity is expected to be 1,000 times larger than that of existing networks (Zhou et al., 2014). To meet the increasing demand for user capacity in these networks, fifth-generation (5G) wireless networks have been introduced. Based on new approaches and technologies, 5G networks are considered to be a promising wireless system for meeting the ever-growing demand for cellular data. Similar to other wireless networks, 5G has a quick and straightforward approach to the channel due to its broadcasting transmission technique. Nevertheless, this characteristic exposes it to eavesdropping attacks. In an eavesdropping attack, also known as a sniffing or snooping attack, an intruder node spies on the messages exchanged between users, leading to confidentiality issues throughout the network. This problem can be fixed by deploying cryptographic protocols in higher layers of communication systems (Zhu et al., 2013). However, due to the dynamic topology of wireless networks, cryptographic protocols suffer from several problems, including symmetric and asymmetric cryptography key distribution and management and the high complexity of cryptographic key processing (Zhu et al., 2013). Physical layer security (PLS) has therefore been proposed as an alternative to cryptography for securing the upper layers of communication systems.

There are several promising technologies for PLS in 5G wireless networks, including channel coding, massive multiple-input multiple-output (m-MiMo), millimeter-wave communications, heterogeneous networks, and other applications such as non-orthogonal multiple access and full-duplex technology. m-MiMo is an enhancement of conventional MiMo technology that was recently proposed for securing the physical layer in 5G networks. An example of m-MiMo is presented in Figure 3.1.

In m-MiMo, the base station is equipped with hundreds of antennas. The large number of

antennas increases the network capacity by ten times or more and concurrently enhances network secrecy compared to traditional MIMO (Larsson et al., 2014). Furthermore, the large number of antennas permits the transmitter (hereafter “Alice”) to focus perfectly narrow and directional energy in the direction of the legitimate receiver (hereafter “Bob”) and to radiate an artificial noise (AN) signal in the direction of any inconsistent intruder that reduces its signal power. The benefit of secrecy unfortunately disappears once an eavesdropper (hereafter “Eve”) is equipped with a number of antennas that is greater than or equal to the number of antennas of the legitimate transmitter. In addition, the design of the AN signal needed in m-MiMo usually involves enormous computational complexity, which is cost-inefficient (Zhu et Xu, 2016). Moreover, the implementation of AN requires excessive energy on the order of $(n)^{\beta}$, where n is the noise variance of Bob, $n > 1$, and β is a constant > 1. The details of these results are provided in Section 3.4, where we provide a theoretical analysis of our proposed approach.

Another approach that can be used to prevent eavesdropping in the physical layer relies on error corrector codes. Raptor codes have recently been employed because they can reliably stop a transmission between authorized parties. To provide some background on this approach, Section 3.3 presents an overview of erasure and rateless codes, the family of codes to which Raptor code belongs.

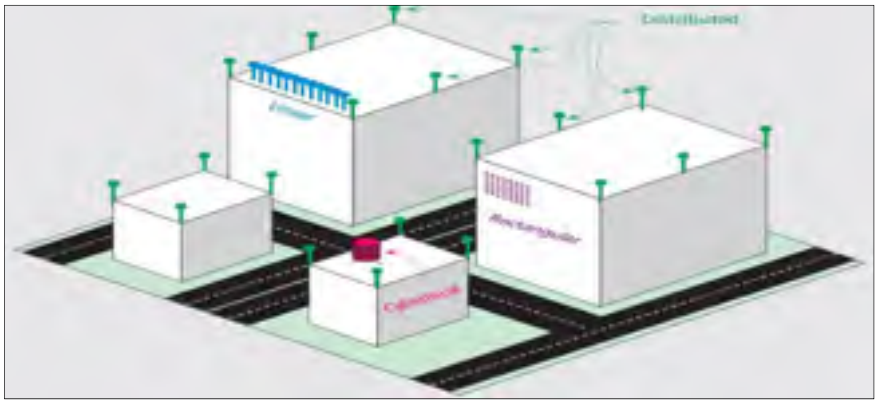

Figure 3.1 An example of massive MiMo
Taken from (Larsson et al., 2014)

In the Raptor code, which is a class of the fountain code, Alice generates an infinite number of encoded packets on the fly. The receivers collect the bits until they recover the message and then send a “stop” message to the source (MacKay, 2004). In wiretapping channels, this feature can be exploited to secure the physical layer. Exploiting this feature implies that the legitimate destination (Bob) must recover the *K* independent coded packets before the eavesdropper (Eve) (Niu et al., 2014);(Sun et Xu, 2019).

To ensure that Bob intercepts a sufficient number of K packets before Eve, the signal-to-interference ratio (SNR) of the legitimate receiver must be higher than that of the intruder. Most PLS methods consider an eavesdropper with a single antenna; however, these methods cannot be effectively applied to 5G wireless networks because an intruder using m-MiMo will have a high SNR and will therefore be able to quickly recover the signal. Furthermore, Raptor codes can be converted into a tool that the eavesdropper can use to spy on the legitimate channel. m-MiMo technology also suffers from several limitations, described above, that further complicate the ability of Raptor code and m-MiMo to effectively ensure secrecy in the presence of an intruder with a large number of antennas.

To ensure security in wireless channels using Raptor code even when the eavesdropper uses a large number of antennas, we developed an approach that fully exploits the feature of Raptor codes in which Bob must intercept a sufficient number of K packets before Eve. In this study, we show that for this to happen, the power needed to design an AN signal must be at least $\varsigma(n)$ instead of $(n)^{\beta}$, where ς is a constant between 1 and β (that is, $1 < \varsigma < \beta$). Motivated by this observation, we propose to exploit the features of Raptor code, while accounting for the natural characteristics of m-MiMo and AN, to data ensure secrecy while reducing power consumption, thus guaranteeing a secure, green transmission.

To our knowledge, our work is the first to address a security problem in the presence of an intruder who is using Raptor code and an m-MiMo system with a large number of antennas; previous studies have largely focused on security issues with conventional MiMo. To affirm our statement of novelty, we offer a theoretical analysis in this article. In this paper, we do not

discuss ergodic secrecy capacity. Such a discussion is not necessary with fountain code because the transmitted packets of confidential data are correlated and only a certain number of packets are required for data recovery (Zhu et Xu, 2016).

This study is an extension of two previous works cited in this paper. We first added new technologies, such as m-MiMo, to the study done by (Niu et al., 2014). Furthermore, we studied the Raptor code, which is an application of the fountain code used by (Niu et al., 2014). We then expanded on our own previous study (Benzid, Kadoch et Cheriet, 2019), adding a theoretical analysis to demonstrate how the characteristics of m-MiMo and Raptor code are judiciously exploited to secure the physical layer on wireless networks without using punctured data.

This paper is outlined as follows: Section 3.3 provides a general review of erasure and rateless codes; Section 3.4 presents previous work on the use of fountain codes and m-MiMo for data security; Section 3.5 introduces our scheme and provides a theoretical analysis of our proposed approach; Section 3.6 presents and discusses the simulation results; and Section 3.7 concludes the paper.

3.3 Erasure and Rate Less Codes

Erasure code is a forward error correction code that adds redundancy to the system to correct errors that occurred while data was being transmitted. The source transmits information symbols while adding redundancy to the message, which allows the receiver to retrieve the message without needing to request that corrupted packets be retransmitted or to acknowledge received packets. Erasure codes are suitable for schemes where the retransmission of packets is expensive or undesirable.

The low-density parity-check (LDPC) codes are an essential class of erasure codes designed by Robert Gallager in 1960. The decoding of LDPC codes is based on iterative belief propagation (BP) algorithms, which permit LDPC decoders to achieve a decoding performance

near the Shannon boundaries. LDPC codes perform better on additive white Gaussian noise (AWGN) channels and generally do not attain their ideal reliability on non-Gaussian channels (Farrell et Honary, 2005).

Rateless codes are error-correcting codes that are distinguished by their variable rate. The transmitter generates an infinite number of encoded packets on the fly, and the receivers collect the received bits until they recover the message. Once the message has been recovered, the receivers send a “stop” message to the source.

Fountain codes, such as the Luby Transform (LT) and Raptor codes, are a promising form of sparse graph code that unify the proprieties of rateless and erasure codes (MacKay, 2004). The most important application of fountain codes is the Internet or wireless networks (Farrell et Honary, 2005).

The LT codes, designed by Michael Luby in 1998, were the first application of universal fountain codes. The LT encoding method is based on a bipartite graph identical to that used in LDPC codes, and LT decoding is correspondingly analogous to LDPC decoding. One of the most practical applications of LT codes is in distributed multi-user information storage systems (Moreira et Farrell, 2006). In LT codes, a short augmentation in overhead can be introduced to improve code performance. The overhead is the variation between the number of the received edges and the number of input edges. A considerable increase in overhead generates an extended decoding latency, leading to an error floor problem because of the associated processing complexity. To solve the problem of this complexity and to enhance the reliability of LT, Raptor codes were designed in late 2000 by adding an additional erasure code (Shokrollahi et Luby, 2011; Stockhammer et al., 2008). The supplementary erasure code can be an LDPC code (Ryan et Lin, 2009).

3.4 Related Work

Several solutions have been proposed in the literature to secure the physical layer from

eavesdropping. In this section, we summarize the solutions that use fountain codes and m-MiMo. The m-MiMo approaches can be classified into two categories: those that use m-MiMo aided by AN and those that use m-MiMo without AN. In the first category, the noise signal is generated in the direction of the malicious intruder and the null space channel of the legitimate user, thereby degrading the intruder's channel without affecting the authorized user. (Wei et al., 2015) proposed an AN method for ensuring secure transmission over correlated fading channels in a multi-user multi-cell system. For this purpose, an m-MiMo system assisted by maximum ratio transmission (MRT) precoding was used to secure the main channel in the presence of an active eavesdropper using multiple antennas.

Another solution for the multi-cell setting, when the AN signal causes inter-cell interference, has been considered in system design in the literature (Zhu, Schober et Bhargava, 2014). The authors of this proposal introduced a closed form that derives bounds. Their results allowed them to predict under what conditions a positive secrecy rate is possible. (Zhou et McKay, 2010) focused on optimizing power allocation between the AN signal and the main channel, with the goal of reducing the complexity of this optimization problem. They recommended using a closed formula to reach the confidentiality rate in fading channels.

To effectively ensure the secrecy of transmitted data, all three AN-based solutions cited above require that the number of transmitting antennas be higher than the number of eavesdropping antennas (Goel et Negi, 2008). Unfortunately, if the intruder uses a large number of antennas for eavesdropping, the secrecy of transmitted data cannot be guaranteed with these approaches. In addition, the design of AN systems usually requires immense computational complexity through a null-space calculation when the number of the antennas is large.

PLS solutions, which use m-MiMo without the aid of AN, have been recommended as an alternative to AN-based m-MiMo. PLS solutions exploit other properties of the physical layer to enhance communication security in the case of an intruder with a higher number of antennas. One such PLS solution secures the m-MIMO system by scaling down the power for both training and information transmission as the number of antennas increases (Zhu et Xu, 2016).

Those authors addressed the power efficiency of a pilot-contaminated multi-cell m-MIMO system in the presence of eavesdroppers employing m-MIMO. Dean and Goldsmith (2017) suggested using physical layer cryptography to secure the channel between Alice and Bob. In their solution, parallel channel decomposition is performed between Alice and Bob. Eve has a different channel and cannot retrieve the signal because of the linear complexity (Dean et Goldsmith, 2017).

A similar approach, referred to as the original symbol phase-rotated (OSPR) scheme, has been proposed in two papers. This method randomly rotates the phase of the original symbols at the base station (BS) before they are transmitted; the papers describing this method consider the security of communication on the downlink and uplink transmission. An additional parameter, termed the radiated power scaling (RPS) factor, is used to optimally correct the overall transmit power with a different number of BS antennas in order to reduce power consumption (Chen et al., 2016a);(Chen et al., 2016b). However, these OSPR studies did not consider the case when Eve uses Raptor codes.

Another way to ensure security at the physical layer is by using error-correcting code. One such solution is the punctured LDPC method. In this scheme, the LDPC-encoded message is punctured before transmission. To achieve reliability and secrecy, the authors of this method assume that the legitimate receiver operates at a high SNR and that the eavesdropper operates at a low SNR. However, it has been shown that punctured messages perform worse than messages that are not punctured; recovering the original word on the legitimate channel therefore requires a large amount of energy to achieve optimal performance. (Niu et al., 2014) first studied the physical characteristics of fountain codes and proposed that a transmit power control (TPC) strategy should be adopted if the quality of the source-destination link was lower than that of the eavesdropper link. Their method is desirable when the illegitimate receiver is in an outage and the legitimate receiver has a high SNR. Another study proposed a solution that uses fountain codes and is based on an outage prediction and limited feedback. This method accounts for the nature of real-world systems and proposes the impact of instantaneous channel state information (CSI) (Sun et Xu, 2019).

The studies mentioned above give a general theoretical analysis of how the characteristics of fountain code are exploited to secure the physical layer on wireless networks; however, they did not consider a new wireless network like 5G, which is different than previous networks because of the use of new technologies such as m-MiMo. These studies also did not address the different categories of fountain codes, even though Raptor code has been shown to perform differently than LT codes.

In our previous work, we proposed using Raptor code based on punctured LDPC to reduce the ability of intruder channels to recover data (Benzid et Kadoch, 2018). However, the punctured data needed a large amount of energy to improve the original message. Furthermore, by using the fountain code, the transmitted packets of confidential data are correlated, and thus only a certain number of packets are required for data recovery (Zhu et Xu, 2016). In this paper, we therefore consider Raptor code without the use of punctured LDPC.

(Kacewicz et Wicker, 2009) recommended another solution that uses fountain code, in which Raptor codes are used to efficiently forward the information symbols through several parallel paths. They showed that Raptor codes can be used to guarantee multiple reliable and robust simultaneous paths. However, their work was dedicated to the protection of the network layer. In addition, they considered the binary erasure channel, which does not consider variation in the channel such as fading, the attenuation of the transmitted signal, and additive noise (AWGN) at the receiver.

In the following section, certain symbols are used to indicate mathematic operations in our proposed transmission security scheme. Uppercase characters in bold indicate matrices. $[\cdot]^H$ signifies the conjugate of a complex matrix, and $[\cdot]$ † denotes the transposed matrix of the conjugate matrix. The notation $E[\cdot]$ indicates the norm of a vector, and $\|\cdot\|$ denotes the determinant of a matrix. I_M denotes the identity matrix of M*M. Tr(A) is the trace of A. * denotes the multiplication operator.

3.5 System Model

As represented in the bloc diagram in Figure 3.2, Alice wants to transmit an *S* bit message to Bob and uses a Raptor code to encode the message. The source block message $S \in \{0,1\}$ of $k \in \{0,1,2\ldots..K\text{-}1\}$ is first encoded with LDPC with a rate $R=k/n$, where k and n are the lengths of the data blocks and the code words, respectively. The LDPC code word is then encoded with LT code to produce the code word $b_k \in \{0,1\}$ of $k \in \{0,1,2\ldots..K\text{-}1\}$.

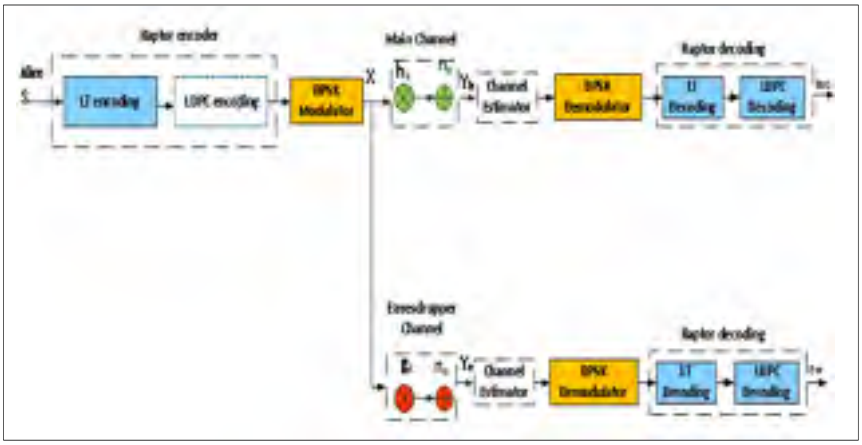

Figure 3.2 Block diagram system

The code word b_k is modulated in BPSK to convert the symbols vector to an *n* bit code word X_n that is then is sent over an AWGN flat fading channel to Bob.

Eve, a passive eavesdropper, can move closer to Alice, which increases the strength of the received signal and allows Eve to spy on the main channel. Suppose that the transmitter, Alice, and the receiver, Bob, are equipped with N_t and N_r antennas, respectively. Eve has N_e antennas to listen to the signal being transmitted between Alice and Bob, and $N_e > N_t > N_r$. All parties know the channel between the transmitter and the legitimate receiver, but the channel state information (CSI) of the intruder channel is not known. An example of a wiretap channel is depicted in Figure 3.3.

To ensure secrecy, Alice divides the transmit signal into two parts: one part carries the secret message for Bob and the second part carries the AN signal to confuse Eve's channel.

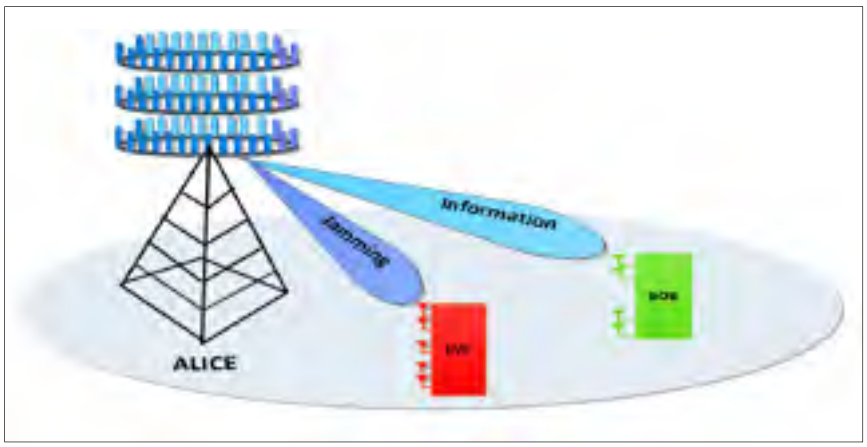

Figure 3.3 Wiretap channel
Taken from (Benzid, Kadoch et Cheriet, 2019)

Alice determines X as the sum of the data transporting the signal information U and the data transporting the AN signal W.

$$X = U + W \tag{3.1}$$

U and W are complex Gaussian vectors, and W is designed to be in the null space of H, such that $H^*W = 0$. If Z is an orthonormal basis for the null space of H, then $W = Z * V$ and $Z * Z^H = I$.

H is the channel between Alice and Bob and is a circularly symmetric complex Gaussian random variable with zero mean and variance $\sigma_h^2 = d_{AB}^{-\alpha}$. The coefficients of H are represented by an $N_t * N_r$ matrix. d_{AB} is the distance between Alice and Bob, and α is the path loss coefficient. The received signals at the legitimate Y_b and the eavesdropper Y_e receivers are determined as follows:

$$Y_b = H(U + W) + n_b \tag{3.2}$$

As $H*W= 0$, Equation (3.2) for the signal Y_b can be simplified to:

$$Y_b = \mathrm{HU} + \mathrm{n}_b \tag{3.3}$$

$$Y_e = GU + GW + n_e \tag{3.4}$$

In these equations, n_b is the Gaussian noise of the receivers and n_e is the Gaussian noise of the intruder. G is the channel between Alice and Eve and is unknown to the transmitter and the receiver. G inputs are modeled as independent symmetric Gaussian random variables of zero mean and variance. The coefficients of G are represented by an $N_t * N_e$ matrix. The AN signal is supposed to be AWGN and is given by:

$$\mathbb{E}\{n_b n_b^H\} = \sigma_b^2$$

$$\mathbb{E}\{n_e n_e^H\} = \sigma_e^2$$

The following equations give the SNR of Bob and Eve:

$$SNR_b = \frac{H * S * S^H * H^H}{\sigma_b^2}$$

$$SNR_e = \frac{G*S*S^H*G^H}{G*Z*Z^H*G*\sigma_v^2+\sigma_e^2}$$

Because Eve is a passive intruder, Eve can move closer to Alice, so that $d_{AB}^{\alpha} > d_{AE}^{\alpha}$. Suppose that Eve and Bob have the same SISO channel capacity C, and C_e and C_b represent the capacity of Eve and Bob, respectively, in m-MiMo.

Let N_{NS} be the number of antennas in the null space of Bob, where $N_{NS} = \dim(\mathrm{Z} = \text{null space (H)})$, The condition to realize the null space is that $N_{NSmin} \leq N_{NS} \leq N_{NSmax}$, where $N_{NSmax} = N_t - 1$ and $N_{NSmin} = N_t - N_r$, and we suppose that $N_t - N_r > N_r$.

The capacity of Eve can be expressed as follows:

$$C_e = \frac{N_t - N_r}{N_r} * log(I + SNR_b) = (I + SNR_b)^{\beta} \tag{3.5}$$

$$\Rightarrow I + SNR_e = (I + SNR_b)^{\beta} \tag{3.6}$$

We suppose that $\beta = \frac{N_t - N_r}{N_r} > 1$. Because $SNR_b > 0$ and β is a positive integer, we can apply the binomial theorem to the term $(I + SNR_b)^{\beta}$ and rewrite Equation (3.6) as:

$$I + SNR_e = (I + SNR_b)^{\beta} = \sum_{i=0}^{\infty} \binom{\beta}{i} (SNR_b)^{\beta} \tag{3.7}$$

$$\Rightarrow SNR_e = \sum_{i=1}^{\infty} \binom{\beta}{i} (SNR_b)^{\beta} \tag{3.8}$$

$\binom{\beta}{i}$ is a binomial coefficient, and can be expressed as follows:

$$\binom{\beta}{i} = \frac{i(i-1)(i-2)(i-\beta+1)}{\beta!}$$

In the worst case, when $\sigma_e \to 0$, SNR_e is given as follows:

$$SNR_e = \frac{G * S * S^H * G^H}{G * Z * Z^H * G * \sigma_v^2}$$

To ensure the secrecy of the data being transmitted, it is necessary that $SNR_e < (SNR_b)^{\beta}$. This can alternatively be written as:

$$\left(\frac{G * S * S^H * G^H}{G * Z * Z^H * G * \sigma_v^2}\right) < \left(\frac{H * S * S^H * H^H}{\sigma_b^2}\right)^{\beta} \tag{3.9}$$

$$\Rightarrow \sigma_v^2 > (\sigma_b^2)^{-\beta} \tag{3.10}$$

If $\sigma_b < 1$, then $(\sigma_v)^\beta \gg 1$. To achieve the requirement shown in Equation (3.9), the transmitter must design an AN signal with an energy equivalent to the $(power\ noise\ of\ Bob)^\beta$. This is an enormous amount of energy, making the AN signal an environmentally unsustainable method for secure data transmission. However, using fountain code to secure the channel leads to the inequality below(Niu et al., 2014) , (Sun et Xu, 2019) :

$$\varepsilon_{AE} > \varepsilon_{AB} \tag{3.11}$$

The inequality above (3.11) allows Bob to intercept the message before Eve. Because the Raptor code is a class and application of fountain codes, the inequality (3.10) should also be sufficient for Raptor codes.

ε_{AB} and ε_{AE} are the outage probabilities at Bob and Eve, respectively, and are expressed by the follow equations:

$$\varepsilon_{AB} = P_r\{(1 + SNR_b) < R\} = 1 - e^{-d_{AB}^{\alpha}/\rho_b} \tag{3.12}$$

$$\varepsilon_{AE} = P_r\{(1 + SNR_e) < R\} = 1 - e^{-d_{AE}^{\alpha}/\rho_e} \tag{3.13}$$

$$\rho_b = \frac{P}{\sigma_b}$$

$$\rho_e = \frac{P}{\sigma_v}$$

P is the transmit power. As mentioned above, to ensure that the data being transmitted remain secure, it is necessary that $\varepsilon_{AE} > \varepsilon_{AB}$ (Niu et al., 2014), which means that $\frac{\sigma_v * d_{AE}^{\alpha}}{P} > \frac{\sigma_b * d_{AB}^{\alpha}}{P}$, or that:

$$d_{AE}^{\alpha} < d_{AB}^{\alpha}$$

which means that $\frac{\sigma_v * d_{AE}^{\alpha}}{P} > \frac{\sigma_b * d_{AB}^{\alpha}}{P}$., as $d_{AE}^{\alpha} < d_{AB}^{\alpha}$, this implies that $\sigma_v > \sigma_b$, hence

$$\sigma_v = \varsigma * \sigma_b \tag{3.14}$$

ς>1 is integer coefficient.

By comparing the result found in equation (3.14) with that found of (3.10), we realize, evidently, that the power that can be dedicated to design AN using the feature of Raptor code is less then that using massive MiMo aided NA without exploiting raptor code feature.
At the receiver, for both Bob and Eve, the Belief Propagation (BP) algorithm is used to achieve the soft decoding process.

The likelihood ratios (LLR) of the channel for both Bob and Eve are given as follows:

$$Z_{0,b} = \ln\left(\frac{P(\hat{s}_k=1|y_k,h_k)}{P(\hat{s}_k=-1|y_k,h_k)}\right) \tag{3.15}$$

If we employ the independence property between $\hat{\mathrm{s}}_{\mathrm{k}}$ and $\hat{h}_k$ and use the Bayes rule, Equation 3.15 becomes:

$$Z_{0,b} = \ln\left(\frac{P(y_k|\mathrm{h}_k,\hat{s}_k=1)}{P(y_k|\mathrm{h}_k,\hat{s}_k=-1)}\right) + \ln\left(\frac{P(\hat{s}_k=1)}{P(\hat{s}_k=-1)}\right) \tag{3.16}$$

With equal probability for the input $\hat{S}$, the term on the right side of Equation (3.16) is equal to zero. In the output of the matched filter, y_k, the probability is given as follows:

$$P(y_k|\mathrm{h}_k,\hat{s}_k = \pm 1) = \frac{1}{\sigma_b\sqrt{2\pi}} e^{\frac{(y_k \pm h_k)^2}{2\sigma_b^2}} \tag{3.17}$$

By substituting Equation (3.17) in Equation (3.16), we get:

$$Z_{0,b} = \frac{2\hat{h}_k}{\sigma_b^2} Y_b \tag{3.18}$$

The LLR for Eve can be found in the same way as for Bob using Equations (3.15), (3.16), and (3.17), and can therefore be expressed as follows:

$$Z_{0,e} = \frac{2\hat{g}_k}{\sigma_v^2} Y_e \tag{3.19}$$

At iteration 0 of the BP decoding algorithm, if *o* and *i* are neighbors, the received channel LLR

from the output node o to the input node i is expressed as follows:

$$m_{o,i}^{(0)} = Z_{0,t} \tag{3.20}$$

t can be replaced with either *b* or *e* to designate Bob or Eve, respectively. For all subsequent iterations, the LLR updating process of LT decoding is completed as follows:

$$m_{io}^{(l)} = \sum_{o\prime \neq o} m_{o\prime i}^{l-1} \tag{3.21}$$

$$tanh(\frac{m_{o,i}^{(l)}}{2}) = tanh(\frac{z_0}{2}) \prod_{i' \neq i} tanh(\frac{m_{i',o}^{(l)}}{2}) \quad o = 1,\ldots, \text{L} \tag{3.22}$$

$m_{o,i}^{(l)}$ and $m_{i,o}^{(l)}$ are the messages sent from the output node $o$to the input node $i$and from $i$to the o, respectively, at iteration l. z_0 is the LLR corresponding to the output symbol o that was calculated in Equations (3.18) and (3.19) for Bob and Eve, respectively, and received from the channel. After the decoder has been processed for $l$iterations, the LLR of each input node $i$is given as:

$$d_i^{LT^l} = \sum_{o \in P(i)} m_{oi}^l \tag{3.23}$$

At iteration N^{itr}, the LLR of the input nodes is calculated as:

$$d_i^{LT^{N_{iter}}} = \sum_{o \in P(i)} m_{oi}^l \tag{3.24}$$

where $P(i)$ is the sum of the overall output bits $o$adjacent to *i.* This LLR, named the output LLR, is the LT-decoding LLR and is considered to be the *a priori* LLR used as the input for LDPC decoding. At iteration 0 of the decoding algorithm, the messages sent by each variable node to its adjacent check nodes are the LLR obtained from the LT decoding process. The procedures for updating the LLR prior to LDPC decoding are given by:

$$m_{v,c}^{(0)} = d_v^{LT^{N^{iter}}} \text{ if o and i are neighbors} \tag{3.25}$$

Alice and Bob use 16 and 8 antennas, respectively, while Eve uses 32 antennas. The variance of AN is $\sigma_v = 2 * \sigma_b$.

$$tanh(\frac{m_{c,v}^{(l)}}{2}) = \prod_{\substack{v=1 \\ v\prime \neq v}}^{n} tanh(\frac{m_{v\prime,c}^{(l-1)}}{2}) \tag{3.26}$$

$$m_{vc}^{l} = m_{v,c}^{(0)} + \sum_{c\prime \neq c} m_{c\prime,v}^{l-1} \tag{3.27}$$

$m_{v,c}^{l}$ and $m_{c,v}^{l}$ are the messages obtained by the LDPC decoder. These messages are transferred from the variable nodes *v* to the check nodes c and from the check nodes c to the variable nodes *v*, respectively. At iteration *l*, at the LDPC decoder, we get:

$$Z_v = \sum m_{c\prime,v}^{l} \tag{3.28}$$

For each decoded bit (c*, v*), a hard decision is made as follows:

$$\hat{S} = \begin{cases} 0 \text{ if } Z_v \geq 0 \\ 1 \text{ if } Z_v < 0 \end{cases} \tag{3.29}$$

3.6 Simulation Results

In this section, we present the results from simulations evaluating the performance of our scheme. The code word length chosen for LDPC encoding was 80,000 bits, the message length was 980 bits, and the code rate was 0.98. The degree of distribution of the LT encoding was the same as that used by (Benzid et Kadoch, 2019) and is given by: $\Omega(x) = 0.008x + 049x^2 + 0.166x^3 + 0.073x^4 + 0.083x^5 + 0.056x^8 + 0.037x^9 + 0.056x^{19} + 0.025x^{65} + 0.003x^{66}$. Alice and Bob used 16 and 8 antennas, respectively, while Eve used 32 antennas. The variance of AN was $\sigma_v = 2 * \sigma_b$.

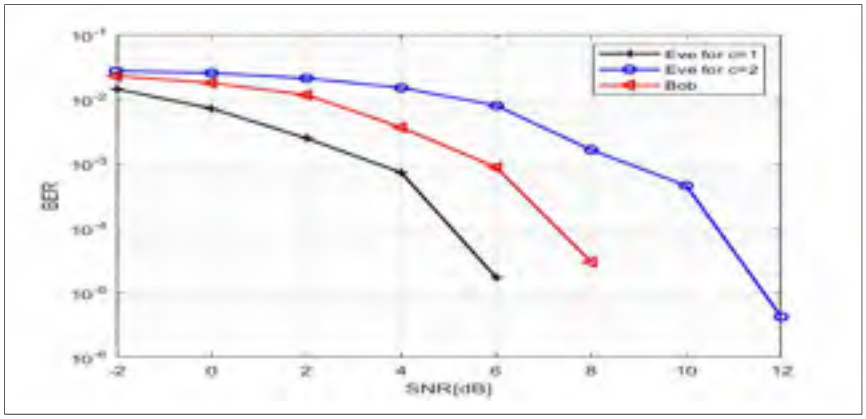

Figure 3.4 BER of Bob and Eve

Figure 3.4 shows that, when our approach was not applied, Eve was able to retrieve the information before Bob at an SNR threshold of 6 dB . However, when our proposed secrecy method was used, Bob was the first to retrieve the message at an SNR threshold of 8dB.

Because $\sigma_v > \sigma_b$, Eve's performance was worse than Bob's. Once Bob has recovered the message, Bob sends an acknowledgement of successful decoding to the encoder (Alice) and tells Alice to stop generating the encoded symbols.

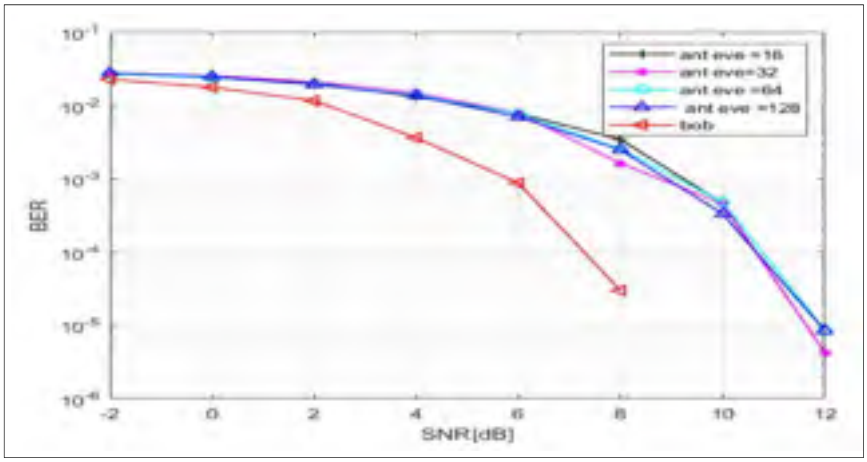

Figure 3.5 BER of Eve with different number of antennas

Because Eve is an eavesdropper, Eve cannot request that Alice retransmit the additional data that would allow Eve to retrieve the message. Eve is therefore not able to recover the signal once Bob has successfully decoded the message.

Figure 3.5 shows that Eve is unable to recover the data sent by Alice despite the number of antennas deployed by Eve, i.e., 16, 32, 64, 128 antennas. The graph also shows the possibility of retrieving the channel at an SNR threshold of 12 dB. That allows Bob to be the first to retrieve the message.

Figure 3.6 gives an overview of the different values that the coefficient c can take to ensure the safety of the transmission. The graph also shows that the channel can be retrieved after Bob at an SNR threshold value of 12 dB. The graph shows that security is guaranteed when $c > 1.2$, which conforms to Equation (3.14) in Section 3.5.

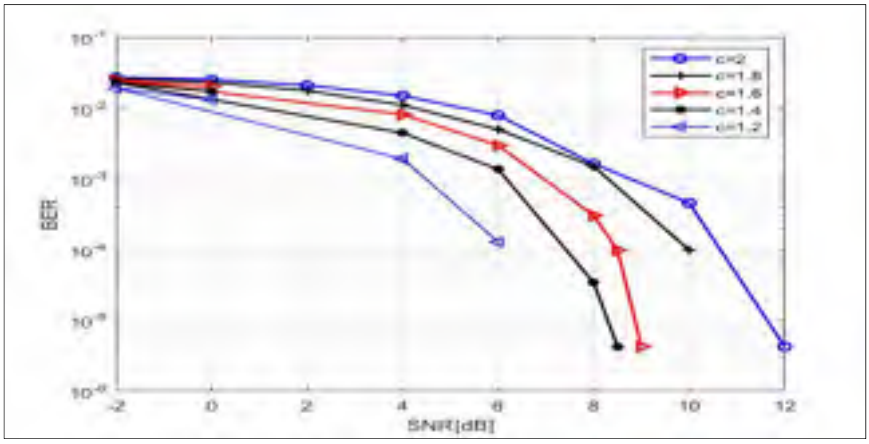

Figure 3.6 BER of Eve with different values of a coefficient c

We also studied the performance of the Raptor code compared to LT and LDPC codes. The results from this comparison are presented in Figure 3.7, which shows that the Raptor code performs better than the LT and LDPC codes.

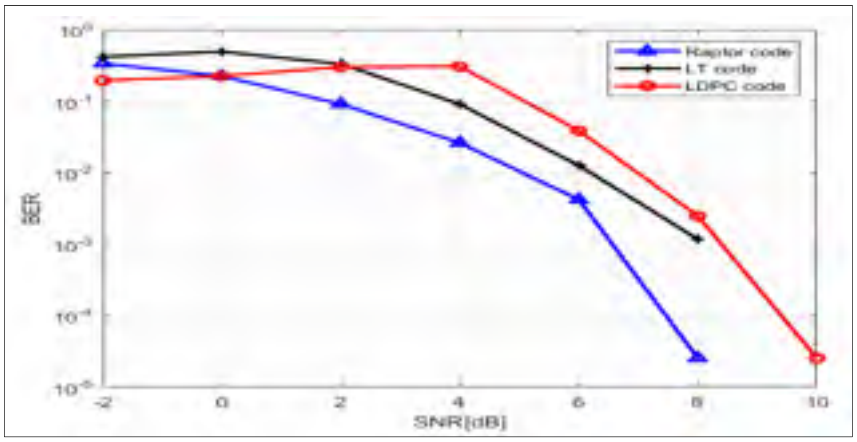

Figure 3.7 BER of Bob with LDPC, LT and Raptor codes

Because the Raptor code is a succession of two erasure codes, and in this case, we used the LDPC and LT codes, the overhead factor included in LT was also studied in this simulation. The overhead coefficient defines the number of variables that are involved in decoding. In LT codes, when the number of edges is large, a longer processing time is needed to decode the message. The large number of edges allowed us to recover the message, but also caused a delay in message recovery and added complexity to the treatment process. To avoid this inconvenience, Bob must optimally choose the coefficient that will enable it to improve the signal while minimizing the delay.

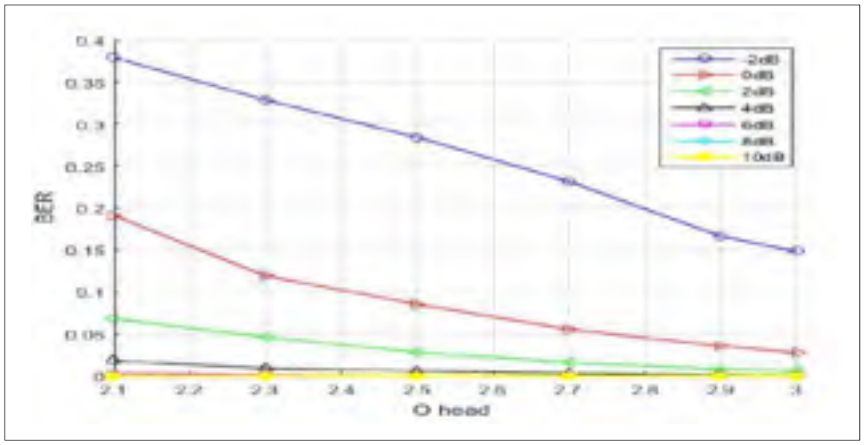

Figure 3.8 BER of Bob with different overhead factor

Figure 3.8 shows that, at a low SNR, a larger number of edges are required to enhance the message. For example, the information can be successfully retrieved at an SNR of 10dB when the overhead coefficient is 2.1. However, at a lower SNR, it is impossible to recover the message since the BER trends to 0.2 and the overhead factor trends to 3.

3.7 Conclusion

In this paper, we proposed a new approach to addressing the security problems associated with using m-MiMo in 5G wireless networks. Our approach ensures data secrecy, even against eavesdroppers equipped with a large number of antennas and decoding resources. Our proposed scheme exploits the features of m-MiMo and Raptor codes to secure the main channel while minimizing power consumption, thus providing a secure, green transmission. We examined our scheme under certain assumptions, including the assumption of a perfect channel between the transmitter and the legitimate receiver. Analytical expressions for the achievable secrecy of our proposed system have been developed to investigate its performance. Numerical results show that our system succeeds in securing the main channel, regardless of the resources or number of antennas available to the eavesdropper. Future work remains to be done to evaluate the effects of CSI on our new method.

CHAPITRE 4

RAPTOR CODE FOR SELECTING A RECEIVER ANTENNA

Djedjiga Benzid [a], Michel Kadoch [b]

[a, b] Department of Electrical Engineering, École de technologie supérieure,
1100 Rue Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Paper submitted for publication in IEEE Wireless Communications Letters, october 2020

4.1 Abstract

Massive multiple-input multiple-output (m-MIMO) is a promising technique for operating fifth-generation wireless networks, but it suffers from the higher cost and processing complexity of the radio frequency chain. One solution to this problem is improving the antenna selection method. However, many antenna selection methods require knowledge of channel state information (CSI) to choose the highest-performing subset of antennas, but this is not possible due to the pilot contamination problem in m-MIMO. Furthermore, the exhaustive search method used in conventional multiple-input multiple-output is inefficient for the m-MIMO system. In this letter, we present an optimal selection algorithm for determining the best subset of antennas at the receiver despite having imperfect CSI. For this purpose, we propose a water-filling algorithm based on the mutual information maximization criterion and Raptor-decoded symbols. Simulation results show that our proposed selection algorithm attains the same optimal values as the exhaustive search method.

4.2 Introduction

Massive multiple-input multiple-output (m-MIMO) is a promising technique that uses hundreds of antennas at the transmitter and receiver to improve channel performance in fifth-generation (5G) wireless networks. m-MIMO demonstrates improved link reliability, data rate,

and radiated energy efficiency relative to conventional systems. However, the large number of antennas requires the addition of radio frequency (RF) chain elements at both link ends, increasing the cost and system complexity of m-MIMO. In this paper, we consider an antenna selection method that resolves this cost and complexity problem. Our method provides a powerful solution in which a subset of the available antennas at the transmitter and receiver are selected, based on a predefined selection criterion, to reduce the cost and system complexity of m-MIMO.

In conventional MIMO, the exhaustive search method is used to find the highest-performing subset of antennas. However, the exhaustive search method is inefficient for m-MIMO because of the large number of antennas that m-MIMO requires. An optimal antenna selection algorithm that is faster than an exhaustive search is therefore required for m-MIMO.

Several solutions have been proposed in the literature to deal with the antenna selection problem in m-MIMO. One study used a maximum sum-rate criterion to find the optimal number of antennas that reduce transit power consumption (Selvam et Vishvaksenan, 2019). Another study used the maximization of capacity/sum-rate as the selection criteria for transmit antenna in the downlink of massive MIMO (Gao et al., 2013). The authors of this second study performed several measurement campaigns in the 2.6 GHz frequency range and used convex optimization to select the antenna subset that maximizes the dirty-paper coding (DPC) capacity in the downlink; they also assumed that perfect channel state information (CSI) was available at the transmitter. A third method for selecting an optimal antenna is based on a binary searching algorithm using the maximizing energy criterion (Chang et al., 2017). The authors of this third method aimed to ensure energy efficiency in the m-MIMO system and assumed there was imperfect channel estimation at the transmitter.

An algorithm that selects antennas with the highest channel gain in m-MIMO has also been proposed (Liu et Wang, 2016). In this approach, the selected antennas are combined with nonorthogonal multiple access (NOMA) to achieve high spectral efficiency in the 5G communication network. Antenna selection at the receiver side has also been studied (Gao,

Vinck et Kaiser, 2017). In that study, upper channel capacity bounds were statistically derived for both the SAS and FAS systems in the largescale limit, and the authors assumed that the CSI was only available at the receiver side.
Several of these solutions are fast and optimal. However, most of the solutions that have been proposed in the literature, including those cited above, assume that the channel is perfectly known when selecting antennas. This is impossible in practice, especially when m-MIMO suffers from pilot contamination.

Motivated by these observations, we previously proposed a method of antenna selection that accounts for the presence of pilot contamination and imperfect CSI (Benzid et al., 2020). For this purpose, we used a water-filling algorithm to find the optimal subset of the antennas that maximized the ergodic capacity (Phan et Tellambura, 2007). Moreover, we used low-density parity-check (LDPC)-decoded symbols to estimate the channel(Benzid et Kadoch, 2018) .

The idea behind our original approach was to use the LDPC decoder to retrieve the received symbols; the recovered message was then used to estimate the gain H. The estimated channel Hˆ was then employed to select the optimal subset of antennas that satisfied the criterion of maximum capacity.

In this study, we enhance the performance of our previously published method for antenna selection by proposing the use of the Raptor code to estimate the channel. At the beginning of the process, when the decoded symbols are not yet available, we assume that the estimated channel is equal to one (that is, $\widehat{H}$ =1); moreover, no subset is selected.
This letter is organized as follows: Section II presents the system models. Section III considers the joint water-filling and Raptor decoding scheme. Section IV presents the simulation results, and Section V concludes the paper.

4.3 System model

We consider an m-MIMO system with a total of N_t transmit antennas and N_r receive antennas, and $N_r \geq N_t$. For each transmission period, a set of $L_r < N_r$ receive antennas is chosen for signal reception. Here, we consider the case where $L_t > N_t$ to ensure spatial multiplexing. If $L_t < N_t$, the system will be rank-deficient (Phan et Tellambura, 2007). The channel gains form the channel matrix $\boldsymbol{H} = [h_{ij}] \in \mathbb{C}^{N_r \times N_t}$, where $h_{ij} \sim \mathcal{CN}(0,1)$ are independent and identically distributed (i.i.d.). Moreover, $\boldsymbol{H}$ is known to the transmitter but not to the receiver. N_t Raptor-encoded symbols are sent through the channel, and the received signal is given by:

$$Y = HX + N \tag{4.1}$$

$\boldsymbol{X}$ contains the elements x_i,which represent the transmitted signals from antenna i. $\boldsymbol{Y}$ contains the entries y_j, which represent the received signals of the jth antenna where $j = 1, \ldots, N_r$.
The Gaussian noise vector $\boldsymbol{N} \in C^{N_r}$ consists of i.i.d. $CN(0, N0)$ variables so that

$$E[\boldsymbol{N}\boldsymbol{N}^{\dagger}] = \sigma_n^2 I_{Nr} .$$

The receiver uses the belief propagation algorithm to retrieve the transmitted message with a soft decoding process. The likelihood ratios of the channel for each coded bit are expressed as follows (Phan et Tellambura, 2007):

$$Z_0 = \frac{2\hat{H}}{\sigma_n^2} Y \tag{4.2}$$

The details for Raptor encoding and decoding are provided in a previous study [7].
$\widehat{H}$ is the estimated random variable coefficients of H. The channel estimation is calculated using the minimum mean squared error (MMSE) as previously described (Phan et Tellambura, 2007). The $\widehat{H}$ channel is given by:

$$\widehat{H} = R_{HH}(R_{HH}XX^T + \sigma_n^2 I)^{-1} X^T Y \tag{4.3}$$

where R_{HH} is the covariance of H.

To avoid symbol pilot contamination, the Raptor-decoded symbols $\hat{S}$ are used instead of the pilot symbols X to estimate the channel, as previously described (Benzid et Kadoch, 2018). Hence, X is substituted with $\hat{S}$ in (4.3) as follows:

$$\widehat{H} = R_{HH}(R_{HH}SS^T + \sigma_n^2 I)^{-1}S^T Y \tag{4.4}$$

However, to perfectly estimate H at the receiver, the average bit error rate (BER) must approach zero, which means that the message must be entirely recovered (i.e., $S = X$); otherwise, the system is in outage and H cannot be estimated.

Corresponding to this outage probability, there is a minimum received signal-to-noise ratio (SNR), SNR_{min}, given by:

$$P_{out} = p(SNR < SNR_{min}) \tag{4.5}$$

$$BER = \frac{1}{2} erfc\sqrt{SNR}$$

$$BER_{max} = \frac{1}{2} erfc\sqrt{SNR_{min}}$$

$$BER_{max} \propto \frac{1}{SNR}$$

$$P_{out} = p(BER > BER_{max})$$

When $SNR \geq SNR_{min}$, the outage probability at the receiver reaches zero: $P_{out} \to 0$ and $BER \to 0$.

Under the fad fading, the channel is varying slowly. The capacity of the channel C can therefore be expressed as the maximum of mutual information using the following equation:

$$C = log_2\, det(I + SNR) \tag{4.6}$$

Because $= \frac{\hat{H}\hat{H}^T}{\sigma_n^2}$, (4.6) can be rewritten as:

$$C = log_2\, det\left(I + \frac{\hat{H}\hat{H}^T}{\sigma_n^2}\right) \tag{4.7}$$

4.3.1 Antenna Selection

As discussed in the previous section, no symbols are recovered when $SNR = SNR_{min}$ in the outage probability. In this case, the estimated channel cannot be processed with our approach, and our antenna selection algorithm will therefore not be applied because it depends on maximizing the capacity, as depicted in (4.7).

However, when the BER at the receiver approaches the zero, $\hat{H}$ can be calculated. Antenna selection can then be performed to find the optimal antenna subset. As in a previous study (Phan et Tellambura, 2007), a diagonal matrix Δ of size $N_r \times N_r$ is defined as follows:

$$\Delta_i = \begin{cases} 1, & \text{if } i^{th} \text{ receive antenna selected} \\ 0, & \text{otherwise} \end{cases} \tag{4.8}$$

$Tr(\Delta) = \sum_i^{N_r} \Delta_i = L_r \leq N_r$ represents the number of receive antennas selected at the reception. The received signal is re-written, including receive antenna selection, as:

$$Y = \Delta HX + N \tag{4.9}$$

The ergodic capacity function of selected antennas can be written through the matrix Δ as follows:

$$C = log_2\, det\left(I + \Delta\widehat{H}\widehat{H}^H\right) \tag{4.10}$$

The optimization problem is to pick the L_r receive antennas such that the capacity in (3.10) is maximized. It is equivalent to finding the matrix Δ such that:

$$C(\Delta) = arg \max_{\substack{\Delta_i \in\{0,1\} \\ \sum_i \Delta_i = L_r}} log_2\, det\left(I + \Delta\widehat{H}\widehat{H}^H\right) \tag{4.11}$$

The antenna selection problem in the massive antenna system can be expressed as:

$$\underset{\{\Delta\}}{\text{maximize}}\, C(\Delta) = \log_2 det\left(I + \Delta\widehat{H}\widehat{H}^H\right) \tag{4.12}$$

subject to:

$$0 \leq \Delta \leq 1 \rightarrow (\text{Condition 1}) \tag{4.13}$$

$$Trace(\Delta) = L_r \rightarrow (Condition\ 2)$$

However, the term $\widehat{H}\widehat{H}^H$ introduces a complexity on the order of $o(n^6)$. This complexity can be reduced using the low-rank approximation method. The key point is to use the single value decomposition (SVD) method to achieve an ideal low-level estimator.

According to the signal processing theory, the channel correlation matrix can be decomposed using SVD of low-rank approximation, as previously described (Guo et Li, 2011):

$$R_{HH} = U \wedge U^H \tag{4.14}$$

U is a unitary matrix and ∧ is a diagonal matrix with the singular values of R_{HH}. The MMSE equation can therefore be represented by:

$$svd(\widehat{H}) = U \wedge U^H (U \wedge U^H SS^T + \sigma_n^2)^{-1} SY \tag{4.15}$$

If taking $\Sigma = \wedge (U \wedge U^{H_P} + \sigma_n^2)^{-1}$, the eigenvalue of ∧ is $\lambda_1 \geq \lambda_2 \geq \cdots \lambda_n \geq 0$ non-zero.

$$\Sigma = \frac{\lambda_k SY}{\lambda_k SS^T + \sigma_n^2} \tag{4.16}$$

Only the diagonal value is considered in the low rank, so Σ could be written by:

$$\Delta_P = \begin{cases} \frac{\lambda_k SY}{\lambda_k SS^T + \sigma_n^2} & if\ k = 0;\ 1; \ldots\ldots\ldots P-1; \\ 0 & if\ k = P; P+1; \ldots\ldots\ldots N-1; \end{cases} \tag{4.17}$$

Then, finally, the SVD algorithm can be represented as previously described [8]:

$$\Sigma = \begin{bmatrix} \Delta_P & 0 \\ 0 & 0 \end{bmatrix} \tag{4.18}$$

$$\Delta_P = \begin{bmatrix} \frac{\lambda_0 S^T Y}{\lambda_0 SS^T + \sigma_n^2} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \frac{\lambda_{P-1} S^T Y}{\lambda_{p-1} SS^T + \sigma_n^2} \end{bmatrix} \tag{4.19}$$

$$svd(\widehat{H}\widehat{H}^H) = U\Delta_p^2 U^H = U \begin{bmatrix} \Delta_P{}^2 & 0 \\ 0 & 0 \end{bmatrix} U^H \tag{4.20}$$

$$\Delta_P{}^2 = \begin{bmatrix} \frac{\lambda_0 SYY^H S^T}{(\lambda_0 SS^T + \sigma_n^2)^2} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \frac{\lambda_{P-1} SYY^H S^T}{(\lambda_{P-1} SS^T + \sigma_n^2)^2} \end{bmatrix} \tag{4.21}$$

The simplification term in the denominator can be written as:

$$(SS^T\lambda_0 + \sigma_n^2)^2 = \lambda_0 S^T SSS^T + (\sigma_n^2)^2 \tag{4.22}$$

hence,

$$\Delta_P{}^2 = \begin{bmatrix} \frac{\lambda_0 SYY^H S^T}{SS^T SS^T + (\sigma_n^2)^2} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \frac{\lambda_{P-1} SYY^H S^T}{SS^T SS^T + (\sigma_n^2)^2} \end{bmatrix} \tag{4.23}$$

In high SNR, $\Delta_P{}^2$ in (4.23) can be rewritten as follows:

$$\Delta_P{}^2 = \begin{bmatrix} \lambda_o \frac{YY^T}{SS^T} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_{p-1} \frac{YY^T}{SS^T} \end{bmatrix} \tag{4.24}$$

$$\Delta_P{}^2 = \sum_{k=1}^{p} \lambda_k \left(\frac{Y_k}{S_k}\right)^2 \tag{4.25}$$

And the equation (4.11) becomes:

$$(\Delta) = arg \max_{\substack{\Delta_i \\ \sum_i \Delta_i}} log_2 \, det\left(I + \Delta(U\Delta_P{}^2 U^H)\right) \tag{4.26}$$

Because $U\Delta U^H = \Pi$,

$$C(\Delta) = log_2\, det(I + \Delta_P \Pi \Delta_P) \tag{4.27}$$

The objective function is concave in Π. However, the Π are binary integer variables, which make the optimization problem non-deterministic polynomial-time (NP)-hard. In order to solve this optimization problem, as in a previous study (Gao et al., 2015), we relax the constraint that each Π must be a binary integer to the weaker constraint that:

$$0 \leq \Pi \ \leq 1 \tag{4.28}$$

The original problem thus becomes a convex optimization problem solvable with water-filling. The Lagrangian method is used to optimize the power of the selected received antennas L_r. Let $f(\Pi) = \log_2 det(I + \Delta_P \Pi \Delta_P)$ and $(\Pi) = tr(\Pi) - L_r$.

The Lagrangian equation is given as follows:

$$\mathcal{L}(\Pi, \psi) = \Delta_P \Pi \Delta_P - \psi(tr(\Pi) - L_r) \tag{4.29}$$

The derived form of equation (4.26) is given above:

$$\frac{\partial \mathcal{L}(\Pi,\psi)}{\partial \Pi} = \frac{\Delta_P \Delta_P}{(I+\Delta_P \Pi \Delta_P)} - \ \psi = 0 \tag{4.30}$$

$$\psi {\Delta_P}^{-2} = (I + \Delta_P \Pi \Delta_P) \Rightarrow$$

$$\psi^{-1} {\Delta_P}^2 - 1 = \Delta_P \Pi {\Delta_P}^H \Rightarrow \Pi = \psi^{-1} - {\Delta_P}^{-2} \tag{4.31}$$

$$\frac{\partial \mathcal{L}(\Pi,\psi)}{\partial \psi} = -tr(\Sigma_s) + L_r = 0$$

From (4.28) at optimality, Π is diagonal. Then the following water filling solution can be obtained

$$\Pi = \left(\psi^{-1} - {\Delta_P}^{-2}\right)^{+} \tag{4.32}$$

4.4 Simulation results

The performance of our scheme is evaluated in this section. The codeword length chosen for LDPC encoding is 80000 bits, the message length is 980 bits, and the code rate is 0.98. The degree of distribution of the LT encoding is the same as that used in (Benzid et Kadoch, 2019)and is as follows:$\Omega(x) = 0.008x + 049x^2 + 0.166x^3 + 0.073x^4 + 0.083x^5 + 0.056x^8 + 0.037x^9 + 0.056x^{19} + 0.025x^{65} + 0.003x^{66}$. Furthermore, we use a massive-MIMO system involving 16 antennas at receiver and eight antennas at the transmitter and a subset of the selected antennas Lr=12.

Figures 4.1 show the relationship between the ergodic capacity and the received SNR. The ergodic capacity is very low when the SNR is between -15dB and -5dB and is far from the optimal values. Because the message is not retrieved at these values of SNR, the channel is not accurately estimated. However, once the SNR is 0dB or higher, the values of the ergodic capacity attain the optimal values since the message is entirely recovered and the channel is correctly estimated.

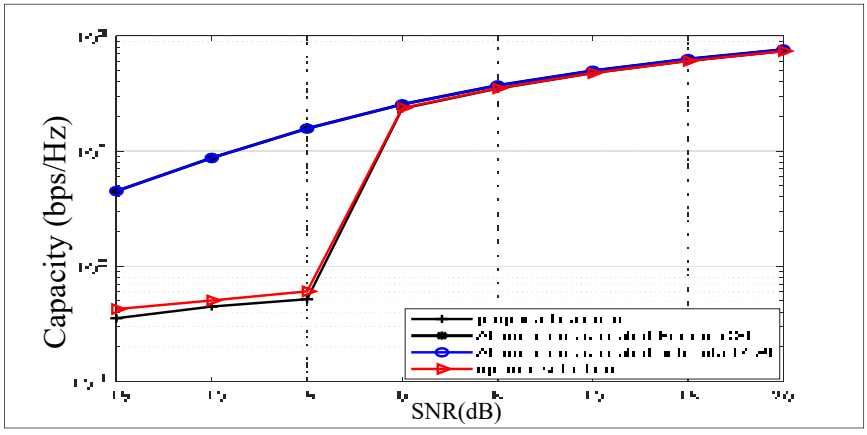

Figure 4.1 Ergodic capacity vs. SNR

Figure.4.2. shows the relationship between the ergodic capacity and the received SNR of successful decoding. The values of the ergodic capacity of the proposed attain the optimal value for different value of Lr=12, 10,8.

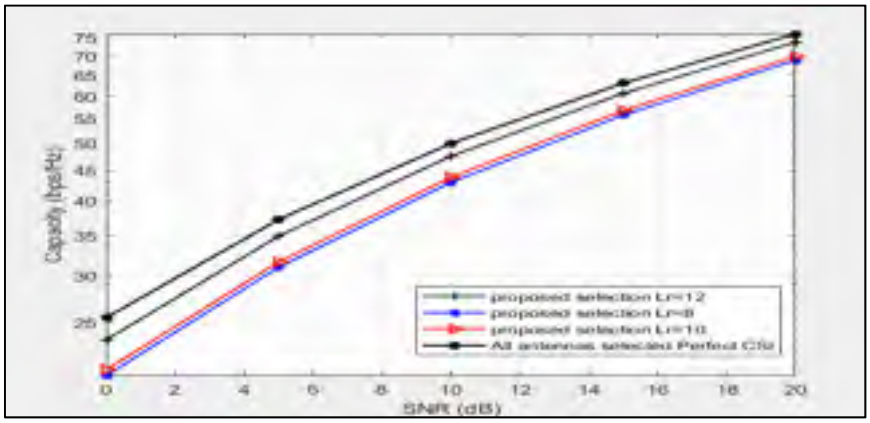

Figure 4.2 Ergodic capacity vs. SNR for successful decoding

Figure 4.3. compares the results of the Raptor-based antenna optimization method proposed in this letter with the results of the LDPC-based method from our previous study. The channel estimated with Raptor code attains higher optimal values of the capacity than the channel estimated with LDPC code.

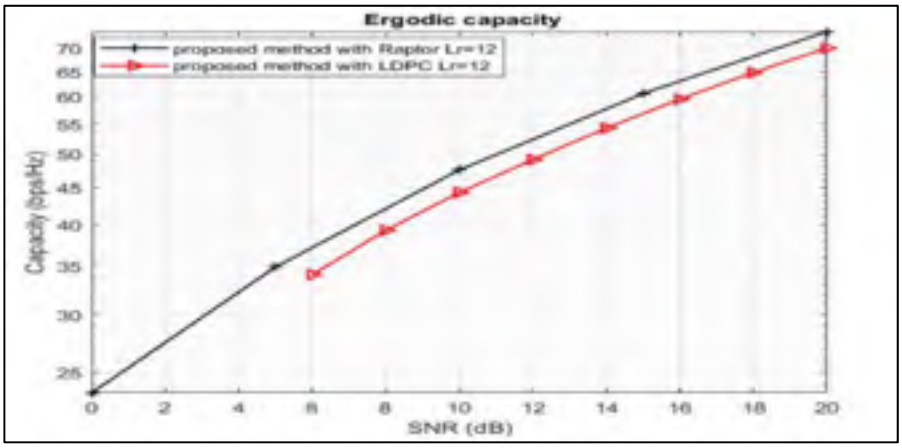

Figure 4.3 Ergodic capacity of Raptor and LDPC codes

4.5 Conclusion

This letter describes an antenna selection method based on mutual information maximization that has the potential to reduce the cost of m-MIMO. In this method, antenna selection is performed under imperfect CSI and Raptor-decoded symbols are used to estimate the channel. The decoded symbols are then used in the water-filling algorithm to select the highest-performing subset of antennas. Simulation results confirm that the ergodic capacity reaches optimal values when the information symbols are successfully decoded with Raptor code

CHAPITRE 5

CONCLUSION, TRAVAUX FUTURS ET LISTE DES PUBLICATIONS

5.1 Conclusion

Pour faire face au nombre de données et d'utilisateurs qui ne cesse de croître, une nouvelle génération de réseaux sans fil plus agile, plus habile et plus robuste que la 4G est déployée.

Celle-ci repose sur des technologies innovantes, puissantes et primordiales, telles que la technologie m-MiMo, pour satisfaire ses utilisateurs en matière de débit et de capacité. La solution m MiMo contribue à la diminution de l'interférence et à la complexité de traitement pour plusieurs utilisateurs. Cependant, cette dernière souffre de contraintes majeures affectant ses performances, à savoir la contamination des séquences pilotes, la sécurité à la couche physique, l'augmentation des coûts et la consommation d'énergie générée par l'utilisation d'un grand nombre de chaînes de fréquences radio (RF). Pour résoudre ces problèmes, nous avons proposé trois solutions présentées dans les trois chapitres de cette thèse.
Dans ces solutions nous exploitons les caractéristiques de la couche physique afin d'éviter l'ajout supplémentaire dans la consommation des ressources en matière d'énergie et de traitement, qui est déjà problématique dans m-MiMo. La nouveauté principale de ces solutions réside dans le fait qu'elles sont les premières à utiliser les codes Raptor et m-MiMo pour pallier les contraintes citées dans cette thèse.

La première solution vise à pallier le problème de contamination des pilotes lorsque les informations sur le canal (CSI) ne sont pas disponibles à la réception. Cette méthode consiste à utiliser les données reçues et décodées avec les codes Raptor pour l'estimation du canal, ce qui lui permet de dispenser des séquences pilotes envoyées par l'émetteur. Avec cette solution, non seulement nous contribuons à éviter la contrainte de contamination des séquences pilotes, mais cela nous permet aussi de diminuer l'énergie requise pour l'émission de pilotes et d'éviter la congestion des réseaux due à l'utilisation excessive des séquences pilotes. L'étude a été

menée sur un canal d'évanouissement lent qui ne change pratiquement pas dans le temps. Trois codes FEC : Raptor, LT et LDPC et trois techniques de détection linéaire, MMSE, ZF et MRC, sont utilisés dans cette étude pour évaluer notre approche. Les résultats de la simulation montrent que le modèle proposé atteint les performances idéales en matière de BER d'un canal en utilisant le MMSE avec des symboles décodés par le code Raptor.

La seconde solution présentée dans le chapitre 3 est consacrée à la sécurité de la couche physique. Dans cette méthode, les codes Raptor sont utilisés pour sécuriser le réseau. Une analyse théorique a été menée à cet effet pour permettre l'emploi adéquat des codes Raptor et m-MiMo à des fins de sécurité. L'étude a été accomplie sur un intrus possédant les plus grandes ressources en matière d'énergie, de traitement et de nombre d'antennes utilisant un canal CSI parfait. Les résultats de cette simulation indiquent qu'avec la méthode proposée, l'intrus est incapable d'intercepter les données, bien qu'il possède les plus grandes ressources.

La troisième solution, présentée au chapitre 4, vise à sélectionner un nombre d'antennes de m-MiMo pour diminuer la grande consommation de ressources en matière d'énergie et de traitement des chaînes RF. À cet effet, la méthode de lagrangien et l'algorithme water-filling sont utilisés en se basant sur la maximisation de capacité du canal. Étant donné que l'étude est effectuée sur un canal dont CSI n'est pas disponible au récepteur, les symboles décodés avec les codes Raptor sont employés pour l'estimation du canal.

Les solutions présentées sont évaluées par des simulations numériques. Au bout du compte, les résultats montrent que nos solutions proposées ont permis d'atteindre nos objectifs en matière du taux d'erreurs, sécurité et capacité.

5.2 Travaux futurs

Récemment le 3GPP a choisi les codes polaires comme des codes correcteurs d'erreur des réseaux 5 G. Pour les travaux futurs, il serait d'ailleurs intéressant d'introduire ces codes dans l'approche proposée dans cette thèse pour résoudre les séquences pilotes contaminées. Ces codes font partie de la classe de codes de blocs linéaires : ils sont basés sur le concept de polarisation de canal. Leur encodage explicite et leur décodage simple les rendent moins complexes et moins exigeants en matière de mémoire. Ces codes peuvent atteindre un débit élevé et des performances de BER, meilleures que celles des codes de pointe (Sharma et Salim, 2017).

Les réseaux 5G peinent encore à être déployés que les chercheurs travaillent déjà sur une nouvelle génération des réseaux sans fil 6G. Comme dans la 5G, la sécurité de la couche physique constitue un problème critique pour les réseaux sans fil 6G. Pour pallier cette contrainte, certaines techniques de sécurité de la couche physique proposées pour la 5G sont maintenues pour les réseaux 6G telles que LDPC basé sur m-MiMo (Yang et al., 2019).

Nous considérons d'ailleurs que les travaux proposés dans cette thèse, concernant la sécurité de la couche physique, peuvent être reconduits pour les réseaux 6G et qu'une étude approfondie pourrait être envisageable.

5.3 Liste des publications

Ci-dessous la liste des publications issues des travaux liés à cette thèse : Journaux (Publiés et soumis) :

5.3.1 Articles de journaux

Benzid, Djedjiga, et Michel Kadoch. 2019. « Fountain Codes and Linear Filtering to Mitigate Pilot Contamination Issue in Massive MiMo ». *Network and Communication Technologies,* vol. 4, p. 1.

Benzid, Djedjiga, et Michel Kadoch. 2019b. « Raptor code and massive MiMo for secure wireless delivery in 5G ». *Journal of Electrical and Electronic Engineering,* vol. 7, nº 6, p. 134-142.

Benzid, Djedjiga, et Michel Kadoch. October 2020 « Raptor code for selecting a receiver antenna» Paper submitted for publication in IEEE Wireless Communications Letters.

5.3.2 Articles de conférences

Benzid, Djedjiga, et Michel Kadoch. 2018. « Raptor code to mitigate Pilot contamination in Massive MiMo ». *Procedia Computer Science,* vol. 130, p. 310-317.

Benzid, Djedjiga, Michel Kadoch et Mohamed Cheriet. 2019. « Raptor Code based on punctured LDPC for Secrecy in Massive MiMo ». In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*. p. 1884-1889. IEEE.

Benzid, Djedjiga, Kadoch Michel, Zhengwei Chang, Jizhao Lu et Rongke Liu. 2020. « LDPC for receive antennas selection in massive MiMo ». In *2020 International Wireless Communications and Mobile Computing (IWCMC)*. p. 322-325. IEEE.

BIBLIOGRAPHIE

Appaiah, Kumar, Alexei Ashikhmin et Thomas L Marzetta. 2010. « Pilot contamination reduction in multi-user TDD systems ». In *2010 IEEE International Conference on Communications*. p. 1-5. IEEE.

Benzid, Djedjiga, et Michel Kadoch. 2018. « Raptor code to mitigate Pilot contamination in Massive MiMo ». *Procedia Computer Science,* vol. 130, p. 310-317.

Benzid, Djedjiga, et Michel Kadoch. 2019. « Fountain Codes and Linear Filtring to Mitigate Pilot Contamination Issue in Massive MiMo ». *Network and Communication Technologies,* vol. 4, p. 1.

Benzid, Djedjiga, Michel Kadoch et Mohamed Cheriet. 2019. « Raptor Code based on punctured LDPC for Secrecy in Massive MiMo ». In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*. p. 1884-1889. IEEE.

Benzid, Djedjiga, Kadoch Michel, Zhengwei Chang, Jizhao Lu et Rongke Liu. 2020. « LDPC for receive antennas selection in massive MiMo ». In *2020 International Wireless Communications and Mobile Computing (IWCMC)*. p. 322-325. IEEE.

Bogale, Tadilo Endeshaw, et Long Bao Le. 2014. « Pilot optimization and channel estimation for multiuser massive MIMO systems ». In *Information Sciences and Systems (CISS), 2014 48th Annual Conference on*. p. 1-6. IEEE.

Chang, Zheng, Zhongyu Wang, Xijuan Guo, Zhu Han et Tapani Ristaniemi. 2017. « Energy-efficient resource allocation for wireless powered massive MIMO system with imperfect CSI ». *IEEE Transactions on Green Communications and Networking,* vol. 1, n^{o} 2, p. 121-130.

Chen, Bin, Chunsheng Zhu, Wei Li, Jibo Wei, Victor CM Leung et Laurence T Yang. 2016a. « Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper ». *IEEE Access,* vol. 4, p. 3016-3025.

Chen, Bin, Chunsheng Zhu, Lei Shu, Man Su, Jibo Wei, Victor CM Leung et Joel JPC Rodrigues. 2016b. « Securing uplink transmission for lightweight single-antenna UEs

in the presence of a massive MIMO eavesdropper ». *IEEE Access,* vol. 4, p. 5374-5384.

Dean, Thomas R, et Andrea J Goldsmith. 2017. « Physical-layer cryptography through massive MIMO ». *IEEE Transactions on Information Theory,* vol. 63, nº 8, p. 5419-5436.

Etesami, Omid, et Amin Shokrollahi. 2006. « Raptor codes on binary memoryless symmetric channels ». *IEEE Transactions on Information Theory,* vol. 52, nº 5, p. 2033-2051.

Farrell, PG, et B Honary. 2005. « Capacity approaching codes design and implementation ». *IEE Proceedings-Communications,* vol. 152, nº 6, p. 1060-1061.

Gao, Xiang, Ove Edfors, Jianan Liu et Fredrik Tufvesson. 2013. « Antenna selection in measured massive MIMO channels using convex optimization ». In *2013 IEEE globecom workshops (GC Wkshps)*. p. 129-134. IEEE.

Gao, Xiang, Ove Edfors, Fredrik Tufvesson et Erik G Larsson. 2015. « Multi-switch for antenna selection in massive MIMO ». In *2015 IEEE Global Communications Conference (GLOBECOM)*. p. 1-6. IEEE.

Gao, Yuan, Han Vinck et Thomas Kaiser. 2017. « Massive MIMO antenna selection: Switching architectures, capacity bounds, and optimal antenna selection algorithms ». *IEEE Transactions on Signal Processing,* vol. 66, nº 5, p. 1346-1360.

Goel, Satashu, et Rohit Negi. 2008. « Guaranteeing secrecy using artificial noise ». *IEEE transactions on wireless communications,* vol. 7, nº 6.

Guo, Wei, et Guojin Li. 2011. « Study on channel estimation of Long Term Evolution ». In *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*. p. 367-369. IEEE.

He, Yejun, Jie Yang et Jiawei Song. 2011. « A survey of error floor of LDPC codes ». In *2011 6th International ICST Conference on Communications and Networking in China (CHINACOM)*. p. 61-64. IEEE.

Kacewicz, A., et S. B. Wicker. 2009. « Secrecy and reliability using Raptor codes in the presence of a wiretapper in a multiple path wireless network ». In *2009 International*

Conference on Wireless Communications & Signal Processing. (13-15 Nov. 2009), p. 1-5.

Khoueiry, B. W., et M. R. Soleymani. 2014. « Joint channel estimation and raptor decoding over fading channel ». In *2014 27th Biennial Symposium on Communications (QBSC)*. (1-4 June 2014), p. 168-172.

Larsson, Erik G, Ove Edfors, Fredrik Tufvesson et Thomas L Marzetta. 2014. « Massive MIMO for next generation wireless systems ». *IEEE communications magazine,* vol. 52, nº 2, p. 186-195.

Liu, Xin, et Xianbin Wang. 2016. « Efficient antenna selection and user scheduling in 5G massive MIMO-NOMA system ». In *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*. p. 1-5. IEEE.

MacKay, David JC. 2004. « Fountain codes ».

Madge, Oliver GH, et David JC MacKay. 2006. « Efficient fountain codes for medium blocklengths ». *IEEE TRANSACTIONS ON COMMUNICATIONS*, p. 1.

Majumder, Saikat, et Shrish Verma. 2013. « Joint channel estimation and decoding of Raptor code on fading channel ». *Indian Journal of Computer Science and Engineering Vol,* vol. 4, nº 2, p. 168-173.

Moreira, Jorge Castiñeira, et Patrick Guy Farrell. 2006. *Essentials of error-control coding*. John Wiley & Sons.

Muaayed, AL-Rawi. 2017. « Massive MIMO system: an overview ». *International journal of open information technologies,* vol. 5, nº 2.

Ngo, Hien Quoc. 2015. *Massive MIMO: Fundamentals and system designs*, 1642. Linköping University Electronic Press.

Niu, Hao, Masayuki Iwai, Kaoru Sezaki, Li Sun et Qinghe Du. 2014. « Exploiting fountain codes for secure wireless delivery ». *IEEE Communications Letters,* vol. 18, nº 5, p. 777-780.

Osman, Onur, and Osman Nuri Uçan. 2009. *Contemporary Coding Techniques and Applications for Mobile Communications*. Auerbach Publications.

Phan, Khoa T, et C Tellambura. 2007. « A water-filling algorithm for receive antenna selection based on mutual information maximization ». In *2007 10th Canadian Workshop on Information Theory (CWIT)*. p. 128-131. IEEE.

Ryan, William E., and Shu Lin. 2009. *Channel Codes: Classical and Modern*. Cambridge University Press.

Ryan, William, et Shu Lin. 2009. *Channel codes: classical and modern*. Cambridge university press.

S. Wong, Vincent W. & Schober, Robert & Wing Kwan Ng, Derrick & Wang, Li-Chun. 2017. « Overview of New Technologies for 5G Systems ». In *Key technologies for 5g wireless systems*, sous la dir. de Press, Cambridge University.

Selvam, Paranche Damodaran, et Kuttathati Srinivasan Vishvaksenan. 2019. « Antenna Selection and Power Allocation in Massive MIMO ». *Radioengineering,* vol. 28, nº 1, p. 340-346.

Sharma, A., et M. Salim. 2017. « Polar Code: The Channel Code contender for 5G scenarios ». In *2017 International Conference on Computer, Communications and Electronics (Comptelix)*. (1-2 July 2017), p. 676-682.

Shokrollahi, Amin. 2006. « Raptor codes ». *IEEE transactions on information theory,* vol. 52, nº 6, p. 2551-2567.

Shokrollahi, Amin, et Michael Luby. 2011. « Raptor codes ». *Foundations and trends® in communications and information theory,* vol. 6, nº 3–4, p. 213-322.

Stockhammer, Thomas, Amin Shokrollahi, Mark Watson, Michael Luby et Tiago Gasiba. 2008. « Application layer forward error correction for mobile multimedia broadcasting ». *Handbook of mobile broadcasting: DVB-H, DMB, ISDB-T and media flo*, p. 239-280.

Sun, Li, et Hongbin Xu. 2019. « Fountain-Coding-Based Secure Communications Exploiting Outage Prediction and Limited Feedback ». *IEEE Transactions on Vehicular Technology,* vol. 68, nº 1, p. 740-753.

Wang, Mingjin, Feifei Gao, Shi Jin et Hai Lin. 2019. « An overview of enhanced massive MIMO with array signal processing techniques ». *IEEE Journal of Selected Topics in Signal Processing,* vol. 13, nº 5, p. 886-901.

Wei, Hao, Dongming Wang, Xiaoyun Hou, Yan Zhu et Jun Zhu. 2015. « Secrecy analysis for massive MIMO systems with internal eavesdroppers ». In *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*. p. 1-5. IEEE.

Yang, P., Y. Xiao, M. Xiao et S. Li. 2019. « 6G Wireless Communications: Vision and Potential Techniques ». *IEEE Network,* vol. 33, nº 4, p. 70-75.

Zhou, Xiangyun, et Matthew R McKay. 2010. « Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation ». *IEEE Transactions on Vehicular Technology,* vol. 59, nº 8, p. 3831-3842.

Zhou, Yiqing, Ling Liu, Hongyan Du, Lin Tian, Xiaodong Wang et Jinglin Shi. 2014. « An overview on intercell interference management in mobile cellular networks: From 2G to 5G ». In *2014 IEEE International Conference on Communication Systems*. p. 217-221. IEEE.

Zhu, Jun, Robert Schober et Vijay K Bhargava. 2014. « Secure transmission in multicell massive MIMO systems ». *IEEE Transactions on Wireless Communications,* vol. 13, nº 9, p. 4766-4781.

Zhu, Jun, et Wei Xu. 2016. « Securing massive MIMO via power scaling ». *IEEE Communications Letters,* vol. 20, nº 5, p. 1014-1017.

Zhu, Yan, Yongkai Zhou, Shivani Patel, Xiao Chen, Liang Pang et Zhi Xue. 2013. « Artificial noise generated in MIMO scenario: Optimal power design ». *IEEE Signal Processing Letters,* vol. 20, nº 10, p. 964-967.

Zirwas, Wolfgang, Muhammad Bilal Amin et Mikael Sternad. 2016. « Coded CSI Reference Signals for 5G-Exploiting Sparsity of FDD Massive MIMO Radio Channels ». In *Smart Antennas (WSA 2016); Proceedings of the 20th International ITG Workshop on*. p. 1-8. VDE.