Full-duplex joint self-interference cancellation, channel estimation and decoding approaches for IoT transmissions physical layer security

Quoc Bao Vuong

DOCTORAT BRETAGNE LOIRE / MATHSTIC

Université de Bretagne Occidentale

Région Bretagne

THÈSE DE DOCTORAT DE

L'UNIVERSITÉ
DE BRETAGNE OCCIDENTALE

ÉCOLE DOCTORALE N° 601
Mathématiques et Sciences et Technologies de l'Information et de la Communication
Spécialité : *Télécommunications*

Par
Quoc Bao VUONG

Approches Conjointes d'Annulation d'Auto-Interférences, d'Estimation de Canal et de Décodage en Full-Duplex pour la Sécurité de la Couche Physique des Transmissions IoT

Full-Duplex Joint Self-Interference Cancellation, Channel Estimation and Decoding Approaches for IoT Transmissions Physical Layer Security

Thèse présentée et soutenue à Brest, le 12 Octobre 2022
Unité de recherche : Lab-STICC, CNRS, UMR 6285, 29238 Brest Cedex 3, France

Rapporteurs avant soutenance :

Didier LE RUYET	Professeur des universités, CNAM / CEDRIC
E. Veronica BELMEGA	Professeure de l'Université Gustave Eiffel, CNRS, LIGM - UMR 8049 CNRS

Composition du Jury :

Président :	Iyad DAYOUB	Professeur des universités, Université Polytechnique Hauts-de-France
Examinateurs :	E. Veronica BELMEGA	Professeure de l'Université Gustave Eiffel, CNRS, LIGM - UMR 8049 CNRS
	Sébastien HOUCKE	Professeur des universités, IMT-Atlantique
	Didier LE RUYET	Professeur des universités, CNAM / CEDRIC
	Lap Luat NGUYEN	Maître de Conférences, International University - VNU HCMC
Dir. de thèse :	Roland GAUTIER	Maître de Conférences Hors Classe, HDR, Université de Bretagne Occidentale
Co-dir. de thèse :	Anthony FICHE	Maître de Conférences, Université de Bretagne Occidentale
	Mélanie MARAZIN	Maître de Conférences, Université de Bretagne Occidentale

Acknowledgements

I would like to thank the Brest Institute of Computer Science and Mathematics (IBNM) CyberIoT Chair of Excellence at the University of Brest, and the Pôle d'Excellence Cyber of the Brittany region for their financial support for my Ph.D. thesis. I am also thankful for the financial support from the Direction Europe and International (DEI), University of Brest (UBO) to help me follow an international mobility in Vietnam for 4 months from January 2021 to April 2021. In particular, this mobility research is jointly supported by the IBNM and the DEI grant "PhD STUDENT INTERNATIONAL MOBILITY" for mobility funding in International University, Ho Chi Minh City, Vietnam.

My deepest thanks should also go to Prof. AZOU Stéphane (ENIB/Lab-STICC) and Prof. BERDER Olivier (Univ. Rennes 1/IRISA) for their comments and recommendations during the CSI committees. It helps me not only revising my works after each year but also having more ideas for the incoming works. I also extend my gratitude to all the jury members who have accepted to take the time to evaluate this thesis. Their insightful comments significantly contributed to improve this thesis.

I would like to give warm thanks to Dr. TA Quang Hien and Dr. NGUYEN Lap Luat, for their considerate and responsive guidance throughout the whole mobility and also the following projects. I sincerely appreciate the valuable time, enthusiasm, and sharing of essential experiences, knowledge, and advice to help me complete this dissertation. I also express my heartfelt thanks to all lecturers and staff of the School of Electrical Engineering (SEE-HCMIU) who helped me to have a warm working environment during the mobility.

I want to express from the bottom of my heart to Assoc. Prof. HDR GAUTIER Roland (Director), Assoc. Prof. FICHE Anthony (Co-supervisor) and Assoc. Prof. MARAZIN Mélanie (Co-supervisor), who are my PhD thesis supervisors, for their conduction and contribution to my works during three years of my PhD thesis. Also, I am grateful to all the professors and members of the UBO Brest and IUT Quimper Lab-STICC/T2I3/SI3 team. Especially, to Prof. RADOI Emanuel, Assoc. Prof. BAGHIOUS El-Houssain, Assoc. Prof. YOUSSEF Roua, Ms. DESPINA-STOIAN Cristina who have donated their priceless comments and advice to my works and played an important role in my thesis project. Working with my team has been an enjoyable and valuable learning experience, which has inspired me to face challenges, question thoughts, and express ideas.

Last but not least, a thankful sentence to my family for everything.

Brest, June 2022 by VUONG Quoc Bao.

Table of Contents

List of Abbreviations

3GPP	The Third Generation Partnership Project
5G	5th Generation wireless systems standard
ADC	Analog-to-Digital Converter
AF	Amplify-and-Forward
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
B-DMC	Binary-input Discrete Memory Channel
BER	Bit Error Rate
BG	Base Graph
BPS	Best Performance Scheme
CFO	Carrier Frequency Offset
CRC	Cyclic Redundancy Check
CRLBs	Cramér–Rao Lower Bounds
DAC	Digital-to-Analog Converter
DCI	Downlink Control Information
DFE	Decision Feedback Equalizer
DM	Decision Metric
DSIC	Digital Self-Interference Cancellation
DSICED3_W/OF	Digital Self-Interference Cancellation, Equalization, Demodulation, De-interleaving and Decoding Without Feedback
ECC	Error Correcting Codes
eMBB	enhanced Mobile Broadband
FD	Full-Duplex
FDD	Frequency Division Duplex

FIR	Finite Impulse Response
HD	Half–Duplex
ICA	Independent Component Analysis
ITU	International Telecommunication Union
JIB_DSICED3	Joint Iterative Blind Digital Self-Interference Cancellation, Equalization, Demodulation, De-interleaving and Decoding
JIB_DSICED3_PF	Joint Iterative Blind Digital Self-Interference Cancellation, Equalization, Demodulation, De-interleaving and Decoding with Partial Feedback
JSIB_DSICED3	Joint Iterative Semi-Blind Digital Self-Interference Cancellation, Equalization, Demodulation, De-interleaving and Decoding
LDPC	Low Density Parity Check
LLR	Log-Likelihood-Ratio
LMS	Least Mean Square
LNA	Low Noise Amplifier
LoRa	Long Range
LoS	Line-of-Sight
LPWAN	Low-Power Wide-Area Networks
LS	Least Square
LTE	Long Term Evolution
ML	Maximum Likelihood
mMTC	massive Machine-Type Communication
MSE	Mean Square Error
MTC	Machine Type Communications
NB-IoT	Narrow Band IoT
nLoS	non Line-of-Sight
OSI	Open Systems Interconnection
PA	Power Amplifier

PBCH	Physical Broadcast Channel
PDCCH	Physical Downlink Control Channel
PDSCH	Physical Downlink Shared Channel
PM	Path Metric
PUCCH	Physical Uplink Control Channel
PUSCH	Physical Uplink Shared Channel
QC-LDPC	Quasi-Cyclic Low Density Parity Check
QPP	Quadratic Polynomial Permutation
RLS	Recursive Least Square
RLS-CMA	Recursive Least Square - Constant Modulus Algorithm
SAR	Successive Approximation Registers
SB_DSICED3_W/OF	Semi-Blind Digital Self-Interference Cancellation, Equalization, Demodulation, De-interleaving and Decoding Without Feedback
SC	Successive Cancellation
SCLD	Successive Cancellation List Decoding
SCLD-CA	Successive Cancellation List Decoding with CRC Aided
SDR	Software Define Radio
SI	Self-Interference
SINR	Signal-to-Interference-plus-Noise ratio
SISO	Single Input Single Output
SMMSE	Semi-blind Minimum Mean Square Error
SNR	Signal to Noise Ratio
SPA	Sum-Product Algorithm
TDD	Time Division Duplex
TDL	Tapped Delay Lines
UCI	Uplink Control Information
uRLLC	ultra-Reliable Low-Latency Communications

List of Notations

$\oplus$	XOR operation
$\otimes$	Kronecker product operation
$*$	Convolution operation
$\lfloor . \rfloor$	Taking the positive integer
$(.)^*$	Conjugate operation
$(.)^T$	Transpose operation
$(.)^{\mathcal{H}}$	Hermitian transpose operation
$(.)^{-1}$	Inverse operation
E	Frame length after modulation
E'	Frame length after modulation and after adding pilot symbols
K	Information length
M	Modulation order
M_{List}	5G Polar codes list size
N	Code word length
R	Code rate
SNR_X	Signal to noise ratio at user X
Z	Lifting size of 5G QC-LDPC codes
$\bar{u_c}$	Average degree of the check nodes
$\bar{u_v}$	Average degree of the variable nodes
$\Pi_{IL}^{\max}$	Interleaving pattern sequence

α	Partial feedback coefficient
β	Pilot symbols ratio coefficient
λ	Forget factor of RLS algorithm
$\mathbf{w}_Y$	Back ground noise at user Y
$\mathcal{B}_{ADC}$	Quantization bit resolution of ADC
$\mathcal{B}_{DAC}$	Quantization bit resolution of DAC
$\mathcal{V}_{ADC}$	Dynamic voltage range of ADC
$\mathcal{V}_{DAC}$	Dynamic voltage range of DAC
σ_Y^2	Noise power at user Y
i_{max}	Maximum number of joint iterative iterations
j_{max}	Maximum number of 5G QC-LDPC decoding iterations
m_{over}	Oversampling factor
m_{up}	Up-sample factor
p_X	Transmitted power of user X
$A \subset B$	A belong to B or A is the subset of B
$A(i,j)$	Element at the position (i,j) of matrix $\mathbf{A}$
$\mathbf{A}$	Matrix $\mathbf{A}$
$\mathbf{A(n)}$	Circulant shifting the binary matrix $\mathbf{A}$ to the right n times
$\mathbf{a}$	Vector $\mathbf{a}$
$\mathbf{a^n}$	Vector $\mathbf{a}$ with length n
$\mathbf{a_{1:n}}$	Vector $\mathbf{a}$ with element from 1 to n
$\mathbf{H}$	Exponent Parity check matrix of 5G QC-LDPC codes
$\mathbf{H}_{LDPC}$	Parity check matrix
$\hat{\mathbf{h}}_{XX}$	Estimation of self-interference channel gain vector at user X
$\hat{\mathbf{h}}_{XY}$	Estimation of channel gain vector between user X and user Y

$\mathbf{h}_{XX}$	Self-interference channel gain vector at user X
$\mathbf{h}_{XY}$	Channel gain vector between user X and user Y
$\mathbf{x}_X$	Transmitted signal vector at user X
$\mathbf{y}_{DSIC}$	Received signal vector after ADC process and to be passed through DSIC process
$\mathbf{y}_{XX}$	Self-interference signal vector at user X
$\mathbf{y}_{XY}$	Receiving signal vector that transmitted from user X to user Y
$\mathbf{y}_X$	Received signal vector at user X
ρ_{XX}	Self-interference to noise ratio at user X
ρ_{XY}	Self-jamming to noise ratio from user X to user Y
$\tilde{y}''[n]$	n-th symbol of equalized value of received signal vector $\mathbf{y}$ in discrete time domain
$\tilde{y}[n]$	n-th symbol of residual value of received signal vector $\mathbf{y}$ in discrete time domain
$\hat{x}[n]$	n-th symbol of estimation value of signal vector $\mathbf{x}$ in discrete time domain
$x'[n]$	n-th symbol of concatenation signal vector $\mathbf{x}$ with pilot symbols in discrete time domain
$x(t)$	Signal x in continuous time domain
$x[k]$	k-th bit of signal vector $\mathbf{x}$ in bit domain
$x[n]$	n-th symbol of signal vector $\mathbf{x}$ in discrete time domain

List of Figures

List of Tables

Résumé

Ces dernières années, le développement et la démocratisation rapide des communications sans fil et mobiles ont conduit à créer le besoin croissant de transmissions de données à haut débit, nécessitant obligatoirement une optimisation des ressources énergétiques et de l'efficacité spectrale. Les systèmes de communication 5G et au-delà (5G & Beyond) doivent atteindre un ensemble d'objectifs dans le cadre des futurs réseaux sans fil et seront omniprésents, centrés sur l'humain, exploitant de manière optimale les bandes de fréquences disponibles, très sécurisés et intelligents. Toutes les évolutions 5G et au-delà sont et seront exploitées aussi bien dans le secteur industriel comme les usines intelligentes, les transports et l'énergie; que dans les domaines grand public comme la santé, l'automatisation, la technologie des transports et l'éducation. Il est indispensable d'assurer l'intégrité des données tout au long de la chaîne de transmission. Dans ce contexte plein de défis, la recherche sur la 5G et au-delà attend avec impatience de révéler de nouveaux problèmes ouverts passionnants. Pour fournir divers services en termes de faible latence, d'accès massif et de sécurité, de nombreuses technologies émergentes ont été proposées pour la 5G et au-delà et en particulier pour les applications de l'Internet des objets (IoT) et les communications dites écologiques (green communications). La technologie la plus prometteuse au niveau de la couche physique, pour la conception de transmissions permettant d'utiliser efficacement le spectre, est la transmission Full-Duplex (FD) qui permet de transmettre et recevoir simultanément dans la même bande de fréquence du canal utilisé.

Afin de doubler "en théorie" l'efficacité spectrale, par rapport à la méthode traditionnelle utilisant la transmission Half-Duplex (HD), la composante du signal liée à l'auto-interférence (SI) produite intrinsèquement par tout système FD doit être supprimée ou réduite jusqu'à un niveau proche du bruit de fond. C'est le plus grand défi dans les systèmes de transmission FD, et de nombreuses solutions ont été proposées à différents niveaux de la chaîne de transmission, telles que l'annulation au niveau radiofréquence (RF), l'annulation au niveau analogique et l'annulation au niveau numérique. Cependant, les transmissions FD, sous condition d'un bon contrôle du phénomène de SI, ont suscité l'intérêt d'un grand nombre de chercheurs pour leurs applications possibles aux problèmes de sécurité de la couche physique (PLS), en utilisant l'auto-brouillage ou le bruit artificiel (AN) à des fins de sécurisation de la transmission. De plus, des schémas de codage canal récents et efficaces proposés pour les nouveaux standards de communications, tels que les codes 5G Quasi-Cyclic Low Density Parity Check (QC-LDPC), les

codes polaires 5G et les turbo codes LTE sont à considérer et semblent des candidats potentiels, non seulement pour améliorer la fiabilité de la transmission des données, mais également pour réduire le phénomène de SI en FD et afin d'améliorer la sécurité en termes de PLS.

Par conséquent, le contenu de cette thèse vise à exploiter l'état de l'art sur les transmissions FD, de l'annulation de la SI dans le domaine numérique et des schémas récents de codage de canal radio afin d'améliorer d'abord la robustesse et les performances attendues des systèmes de transmissions au niveau de la couche physique, puis leur sécurité, en particulier dans les transmissions par paquets courts pour les applications de type IoT et les communications dites écologiques ou vertes.

Tout d'abord, l'impact des phénomènes de la SI et du bruit de quantification générés par les processus de conversion numérique-analogique (DAC) / conversion analogique-numérique (ADC) au niveau de l'émetteur et du récepteur sur les performances des systèmes de transmission FD ayant une antenne à l'émission et une antenne à la réception (SISO : Single Input Single Output) sont pris en compte. Des schémas de codage de canal efficaces et récents sont utilisés afin de surmonter les effets de la SI résiduelle et du bruit de quantification dans le processus d'annulation ou de réduction. L'impact de la résolution en nombre de bits au niveau de la quantification des convertisseurs est également discuté et en particulier les compromis nécessaires en termes de sélections conjointes des résolutions en nombre de bits par rapport aux performances attendues au niveau des processus DAC/ADC, surtout dans le contexte des transmissions IoT et les communications écologiques ou vertes. Ensuite, les performances de différentes architectures de dispositifs de quantification au niveau du récepteur telles que $\Sigma\Delta$, mi-hauteur à pas gaussien (Gaussian with mid-rise), pipeline et registres à approximation successive ADC (SAR) sont évaluées. Les résultats soulignent que l'utilisation de schémas de codage de canal est nécessaire pour les systèmes de transmission FD.

Malgré cela, les recherches de la littérature dans le cadre de transmissions FD par paquets courts sont toujours en cours et elles font apparaître la nécessité d'utiliser plus de symboles de données pour obtenir une bonne statistique de convergence afin d'obtenir des résultats significatifs. Par conséquent, ces approches ne semblent toujours pas être des solutions satisfaisantes pour des systèmes de transmission économes en temps, en bande passante et en puissance pour la transmission de paquets courts en contexte de transmission FD. Afin de pallier ces inconvénients, un algorithme itératif conjoint aveugle d'annulation de la SI, d'estimation du canal de propagation et de décodage pour les transmissions FD via la rétroaction d'estimations du canal et de messages décodés combinés avec le processus d'annulation d'auto-interférence numérique (DSIC) est proposé dans cette thèse. L'algorithme aveugle proposé estime simultanément les canaux de SI et de propagation et décode les messages à chaque itération de décodage des codes 5G QC-LDPC. Une boucle de rétroaction est formée à l'aide de l'estimation de canal de prop-

agation temporaire et du message décodé pour améliorer l'annulation de la SI et également l'estimation du canal ainsi que le décodage dans l'itération suivante. Les résultats soulignent que l'algorithme proposé surpasse l'algorithme conventionnel sans rétroaction, en particulier à un rapport signal sur bruit (SNR) élevé et un petit nombre de symboles, et nécessite beaucoup moins de temps de traitement tout en atteignant les performances de convergence. Les résultats montrent également que l'algorithme proposé est moins sensible au niveau de la puissance de la SI que l'algorithme conventionnel. De plus, cette thèse propose également un schéma de rétroaction partielle, qui n'utilise qu'une faible portion de symboles de rétroaction pour l'estimation de canal, afin de réduire considérablement le temps de traitement et la complexité de calcul tout en maintenant les performances à un niveau acceptable, ce qui est tout à fait adapté à une utilisation de cet algorithme itératif aveugle pour des transmissions FD par paquets courts dans les applications IoT et les communications écologiques.

Cependant, lors de l'utilisation de l'algorithme aveugle, il persiste un nombre d'erreurs de décodage résiduelles qui semble tout de même assez significatif dans la région à bas SNR. Par conséquent, une version semi-aveugle est donc développée prenant en compte quelques symboles pilotes supplémentaires et permettant une coopération lors de l'estimation des canaux pour former la composante de rétroaction et sans nécessiter de ré-encodage. Les résultats montrent que cet algorithme semi-aveugle atteint non seulement des performances presque optimales, mais réduit également considérablement le temps de traitement et la complexité de calcul. Cet algorithme semi-aveugle permet également d'améliorer les performances du système, en particulier à faible SNR. Les résultats de cette étude mettent en évidence le potentiel en termes d'efficacité de cet algorithme itératif semi-aveugle conjoint pour des transmissions FD par paquets courts dans le cadre de scénarios pratiques pour la 5G et au-delà et/ou l'IoT.

Enfin, l'évaluation de la mise en œuvre de la sécurité au niveau de la couche physique (PLS) par transmission de type FD à paquets courts dans un contexte d'écoute indiscrète passive et active est considérée dans cette thèse. En effet, les schémas de rétroaction aveugle et semi-aveugle proposés sont appliqués au niveau du récepteur légitime pour améliorer la PLS dans une transmission SISO FD. En particulier, le récepteur légitime et le récepteur espion peuvent simultanément recevoir le signal voulu de l'émetteur et diffuser un signal d'auto-brouillage ou de brouillage à l'autre. Les résultats montrent que les algorithmes proposés surpassent l'algorithme existant en termes de fiabilité et de sécurité. Ils montrent également que les algorithmes proposés sont moins sensibles que l'algorithme conventionnel, aussi bien au niveau de la SI, que des signaux d'auto-brouillage ou des interférences de brouillage. Les résultats soulignent également que les algorithmes proposés montrent une robustesse non seulement vis-à-vis des facteurs de sécurité et de fiabilité, mais également à la consommation énergétique, ce qui convient parfaitement aux transmissions IoT à paquets courts et aux communications vertes.

Introduction

General Background

Full-Duplex (FD) Transmission

It is certainly that wireless communications will remain one of the pillars of the developed world in the future. Every day, more data is transmitted over the air, requiring greater efficiency from wireless communications systems in all areas. Especially, when human beings are moving deeply toward the 5th Generation wireless systems standard (5G) networks and beyond, the most important target is ensuring the spectrum efficiency and obtaining the extremely high data rate [1–4]. Moreover, the fast development of wireless and mobile communication leads to the requirement of the invention of new and innovate techniques in order to fulfill the demands of modern society [5–10]. Therefore, the research community has proposed various solutions and techniques such as increasing the number of transceiver's antennas [11, 12] or transmitters over a higher center frequency, in which the bandwidth is increased over time [13, 14].

Consequently, an efficient spectrum sharing technique called Full-Duplex (FD) transmission has been proposed [3, 10]. FD radio technology transmissions, which simultaneously transmit and receive information at the same channel used with the same spectrum and at the same time, can boost the spectrum efficiency. Unlike traditional communication systems, which operate in Half–Duplex (HD) mode [15–17] by dividing the transmitter and receiver in the time domain as Time Division Duplex (TDD) or in the frequency domain as Frequency Division Duplex (FDD), FD transmission systems can use the time-frequency resource at the same time for transmission and reception. Fig. 1 shows the usage spectrum and the time resource for the TDD, FDD, and FD transmission systems. It can be seen that FD transmission uses more efficiently the resources than the other traditional methods. In mathematics, spectral efficiency can be illustrated by using the Shannon theorem, which is the relationship between the capacity ($\mathcal{C}$), bandwidth ($\mathcal{W}$), and Signal-to-Interference-plus-Noise ratio (SINR) of a practical communication system,

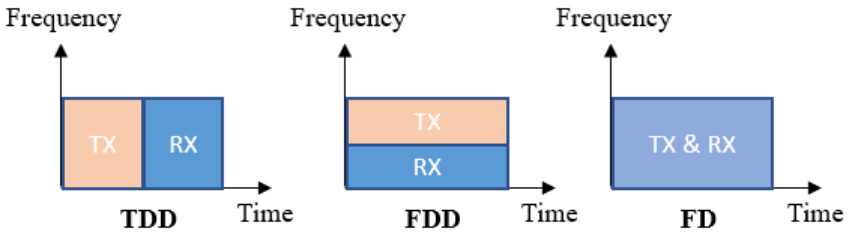


Fig. 1: Graphical presence of time and frequency resources in TDD, FDD and FD transmission systems.

which is given in Equation (1):

$$\begin{aligned} \mathcal{C}_{HD} &= \mathcal{W}\log(1+SINR_{HD}), \\ \mathcal{C}_{FD} &= 2\mathcal{W}\log(1+SINR_{FD}). \end{aligned} \tag{1}$$

Although they have the same overall bandwidth $\mathcal{W}$, the FD transmission capacity is double that of HD transmission. Therefore, FD is a promising technique for 5G wireless networks as it can "in theory" double the spectral efficiency, compared to traditional HD transmission [18, 19]. However, due to the same channel used for transmission and reception, the problem of Self-Interference (SI) should be considered carefully, which is illustrated in details in the following chapters of this thesis.

Due to the efficient use of resource and outstanding compared with traditional methods, FD transmission has many applications to the modern transmission networks, not only for transmitting data but also for maintaining security. As shown in Fig. 2, we first consider a FD base station sending data on the downlink to one HD user and receiving data on the uplink from another HD user. In this case, the base station operates in FD mode and can send and receive simultaneously over the same frequency slot, while it would need two time and frequency resources to transmit and receive if HD mode is used. Secondly, a FD relay station receives and forwards simultaneously the signal between two HD terminals. Thus, the relay can increase the spectral efficiency compared to HD operation. Moreover, FD transmission in a cognitive radio network allows secondary terminals to sense network traffic while transmitting themselves signal [20]. They do not have to stop sending to listen to the channel and can stop transmitting as soon as the principal terminal starts using it. The power of the remaining SI after cancellation must be smaller than the power of the received primary user for this application to be feasible. Last but not least, securing wireless data transfer can also benefit from FD transmission. The receiver simultaneously broadcasts a jamming signal while receiving the useful signal, causing the eavesdropper to receive a superposition of the intended signal and the jamming signal. It is impossible for the eavesdropper to detect the beneficial signal without prior information on the structure of the two signals [9, 21, 22].

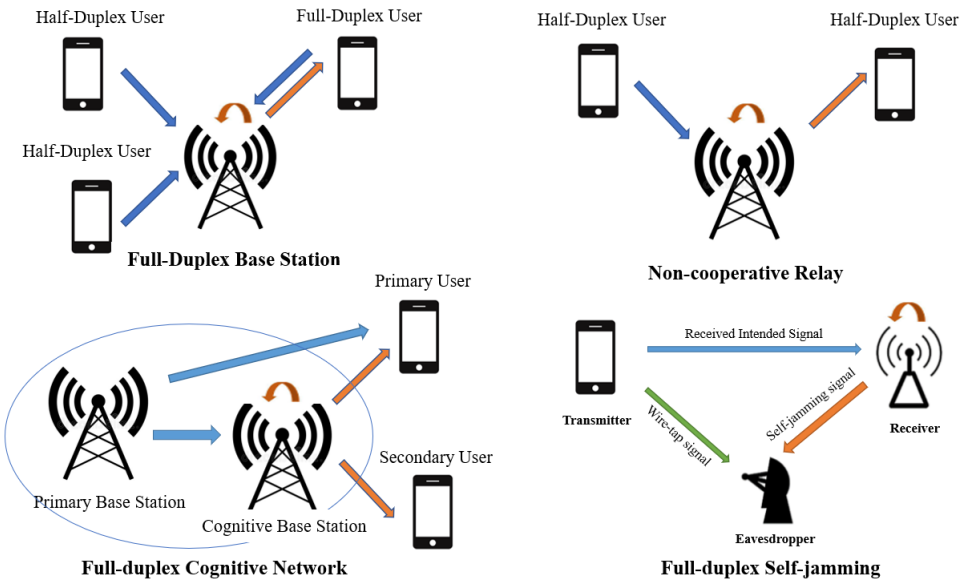


Fig. 2: Example of FD transmission applications.

Internet of Things (IoT)

Next-generation wireless communication systems will connect billions of IoT devices and user elements along with billions of people, enable machine-to-machine communications in a heterogeneous and dynamic environment, and provide low-latency computing and storage resources on demand at the deep edge and in the cloud [23, 24]. In [25], an appropriate definition of IoT is given that might be a good starting point: "a world where physical objects are seamlessly integrated into the information network and where physical objects become active participants in business processes". It is true that the "Internet" has evolved the human lives ultimately, but then again the new adopted technology IoT has promoted dummy machines to smart, autonomous and interactive machines [24]. In recent years, IoT aims to allow ubiquitous connections between things with computing, communication, and sensing ability. IoT can be seen as the next generation interconnection area that will enable connectivity between people's devices and machines, enabling actions to take place without human intervention. Now, it has been become an integral part of human's life in various applications such as in industrial domain (manufacturing, utility management, agriculture, etc) and in public domain (healthcare, e-commerce, etc), which is shown in Fig. 3. With the huge amount of IoT devices, which is up to billions of computing devices, ranging from a well smartphone to embedded low-cost, low-energy and lightweight computing devices, wireless is seen as the best option to avoid installation costs while providing ubiquitous connection [26].

Traditionally, many wireless transmission technologies have been used to provide massive IoT devices connection. Well-known standards are Bluetooth, Zigbee and Z-Wave, which are classified as short-range communication technologies. However, their operation has faced with the problems of power, cost, complexity, and data rate, when the

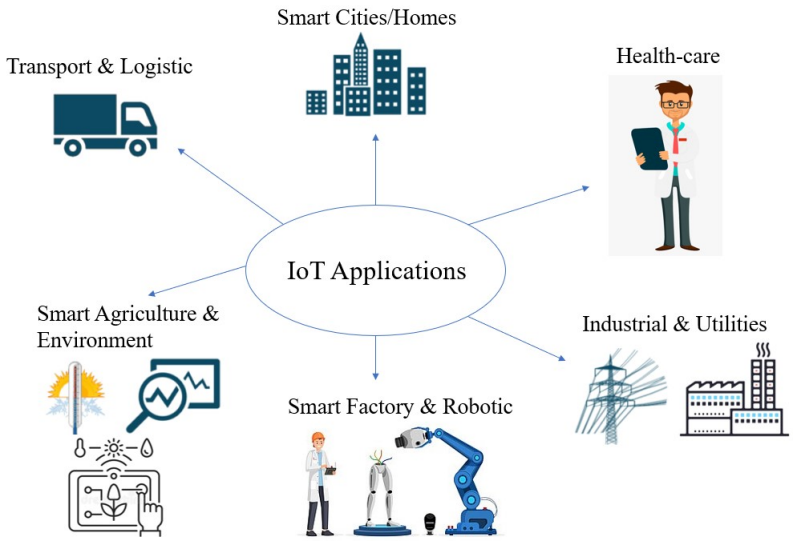


Fig. 3: IoT networks and industrial applications.

IoT system requires larger covering areas with numerous IoT devices. To overcome these problems, a solution based on the second to fourth generation of cellular networks such as 2G, 3G, and 4G has been implemented, but consumes excessive energy from the devices in the network [27]. Therefore, the Low-Power Wide-Area Networks (LPWAN) can be seen as a promised candidate for IoT transmission because it can adapt the requirements of high efficiency energy (more than 10 years battery), large covering area (from 10 to 40 km), and inexpensive wireless modules (less than 2 euros per device per year) [28]. Many features of LPWAN are currently operated in unlicensed frequency band as well as licensed frequency band. Narrow Band IoT (NB-IoT) is a different transmission technology belonging to LPWAN, which uses the narrowband radio frequency of Release 13 of the Long Term Evolution (LTE) standard of The Third Generation Partnership Project (3GPP). A lot of telecom companies have used NB-IoT as transmission standard in IoT networks such as water meter in Spanish Vodafone and smart city applications in China because of the quality of service, coverage and battery life, etc [29]. However, 5G and IoT technologies are more than just a new generation of wireless technology. It represents a fundamental change in the mobile ecosystem, unleashing a powerful combination of extraordinary speed, expanded bandwidth, low latency, and increased power efficiency that drives billions of more connections and changes our world. It's unleashing a massive IoT ecosystem where networks can serve billions of connected devices, with the right trade-offs between speed, latency and cost. It leads to the requirement of different wireless technology such as:

- massive Machine-Type Communication (mMTC), or energy-efficient 5G, adopts existing LTE LPWAN, where NB-IoT and LTE-M technologies are part of the mMTC category of 5G [27, 29, 30];

- ultra-Reliable Low-Latency Communications (uRLLC), or mission-critical 5G, is a new class of performance communication that focuses on the highest possible reliability while enabling latency as low as 1ms [31];
- enhanced Mobile Broadband (eMBB), or high speed 5G, is predominantly high data throughput that leverages new, greater bandwidth 5G spectrum [31].

Physical Layer Security (PLS)

The Open Systems Interconnection (OSI) model was created by the International Organization for Standardization, allowing several communication systems to communicate using standard protocols on seven layers, including application layer, presentation layer, session layer, transport layer, network layer, data link layer, and physical layer [32], as shown in Fig. 4.

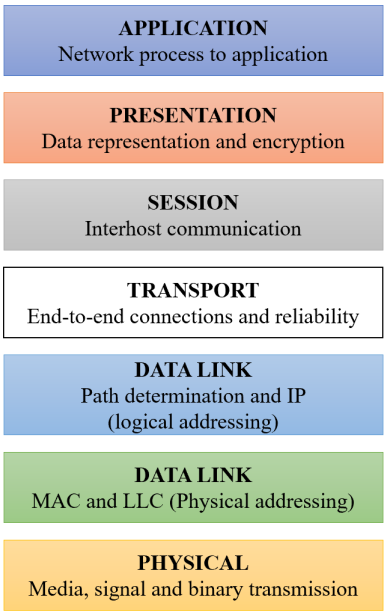


Fig. 4: OSI model.

Normally, most network security algorithms are implemented in the upper layers of the communication system such as application layer, transport layer, and network layer. However, the physical layer that provides an electrical, mechanical, and procedural interface to the transmission medium between devices, is found to be more robust when it comes to security. Although the complexity of the security algorithms may become an issue, PLS can simplify the security algorithms in terms of power efficiency and computational complexity [33]. Therefore, even though eavesdroppers can be equipped with high-power computational devices, the reliability and security of the network can also remain, which means that the eavesdropper does not catch information and the intended information is not affected or corrupted by a jamming signal, respectively [34]. Furthermore, the connection of devices in a 5G network is usually ascertained; they can access or leave the network

randomly at any time, so it is too difficult to implement the cryptographic key distribution technique [34]. Therefore, exploiting an emerging PLS technique for 5G transmission has received a great deal of research interest. In wireless networks, PLS securely transferring confidential data has been considered a challenging task because of the broadcast nature of wireless environments. In addition to approaches of using cryptography methods [35], security based on information theory has been widely acknowledged as an attractive for security enhancement in wireless networks [36–38].

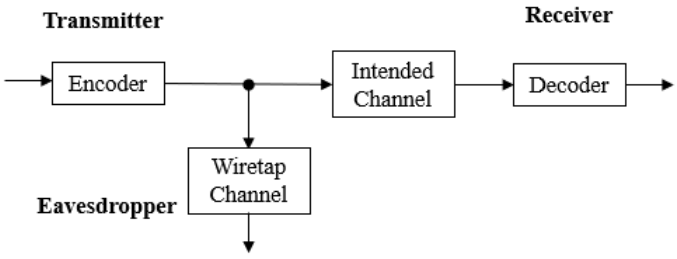


Fig. 5: Wiretap channel model.

In the information and coding community, the wiretap channel model, which is shown in Fig. 5, was first proposed by Wyner in [39] and further polished in 1978 by Csiszar and Korner for broadcast channels with confidential messages [40]. In wireless PLS, the key idea is to exploit the characteristics of wireless channels such as fading gains to transmit a message from a source to an intended destination by the intended channel while keeping this message confidential from the listening of eavesdroppers by wiretap channel. The main objective is to provide information privacy of transmitted data, solely based on the hypothesis that the channel from the transmitter to the eavesdropper is noisier and weaker than the channel from the transmitter to the legitimate receiver. In wiretap channel, there are two types of eavesdropper, such as passive eavesdropper, which only listens to the intended message, and active eavesdropper, which can also broadcast the interference or jamming signal to the legitimate receiver. The active eavesdropper was introduced by Ozarow and Wyner as the second type of wiretap channel named wiretap channel II, where the active eavesdropper not only listens to the intended transmitter, but can also transmit a jamming signal to the legitimate receiver [41]. Therefore, various solutions should be studied to improve the PLS such as the use of self-jamming or Artificial Noise (AN). [9, 21, 42–44].

Motivation

The rapid growth in complexity of IoT networks leads to the requirement of a high-security mechanism within an IoT network to protect private and confidential information. Because once an IoT device is hacked, the hackers can gain control and attack other devices in the network. Therefore, confidentiality in wireless medium, or PLS, becomes more vital to protect the legitimate information as well as improve the system's performance [34].

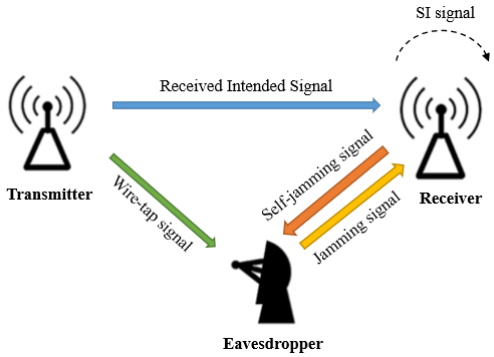


Fig. 6: Example of FD transmission to avoid eavesdropper.

The use of a FD transmission may be a first level of data security at the legitimate receiver by receiving simultaneously the useful signal and broadcasting a self-jamming signal in one transmission media, as shown in Fig. 6. Thus, the received signal will be more difficult to exploit by an eavesdropper who intercepts the communication [18]. Moreover, the eavesdropper can also broadcast its own jamming signal to the legitimate receiver in order to reduce his reception behavior. Therefore, a robustness innovation in the decoding mechanism should be explored to not only overcome the jamming interference but also reduce the SI problem in the FD transmission. In recent years, many signal processing techniques using FD transmission in PLS have been developed to support the security. The authors in [45] explored the PLS of an Ad-hoc wireless network, where the legitimate receiver works in FD transmission. It simultaneously receives the legitimate information and transmits the AN or self-jamming signal to destroy the operation of the eavesdropper node. In the study of the authors in [46], it was proposed that the joint of the information and jamming beamforming for PLS with the FD base station degrades eavesdropper decoding and increases the secret rate in the wireless system. Furthermore, channel secrecy capacity and transmission message reliability can be a problem for communications with finite block length or short-packet [47]. Therefore, PLS in short-packet transmission is recently an open area for focusing on 5G applications & beyond.

Moreover, the use of a FD transmission with good control of SI will also be considered as a first level of data confidentiality and accuracy in wireless medium in 5G and IoT networks; for instance of transmitting simultaneously the information signal and the self-jamming signal to not only protect the legitimate information but also improve the system's performance [48]. However, achieving doubled spectral efficiency in FD transmission is a challenging task due to the difficulty of suppressing the SI component, which could be up to 120 dB in power in real networks [8, 10, 49–51]. It is necessary to cancel the SI component to the noise floor level and otherwise the spectral efficiency cannot be realized because of high level of interference, especially in short-packet transmissions for IoT applications and green communications.

In this context, in order to secure IoT transmissions and green communications, but

also 5G scenarios & beyond, very few studies have been carried out to conceive of how in practice, especially at the physical layer, where robust processing can address emerging security issues. Generally, studies have been limited to improve the correction powers of the transmitted data in order to combat the effects of the propagation channel, but not to ensure, for example, a feedback of useful information to the higher level layers (for the mechanisms of intrusion detection, information routing, etc.), the identification of sensors and connected objects, their geographic location within the network, the detection and location of the presence of potential jammers nearby, etc.

Moreover, the authors in [52] shown that channel coding as 5G Quasi-Cyclic Low Density Parity Check (QC-LDPC) codes and 5G Polar codes are considered as the potential of PLS for 5G and beyond. The development of 5G will lead to expanse the IoT network by providing the platforms to connect a number of mMTC devices to Internet. A network of mMTC devices in IoT requires novel fundamental security for point-to-multipoint systems and multipoint-to-point systems with a very large number of downlink receivers and uplink transmitters, respectively. Therefore, it is necessary to answer the question of how to protect legitimate transmission data over wireless transmissions in PLS.

Consequently, my Ph.D. thesis named "Full-Duplex Joint Self-Interference Cancelation, Channel Estimation and Decoding Approaches for IoT Transmissions Physical Layer Security" has been pointed out and researched. In fact, a FD transmission scheme with digital modulation, channel coding, Digital-to-Analog Converter (DAC)/Analog-to-Digital Converter (ADC), Digital Self-Interference Cancellation (DSIC), equalizer processes needs to be adaptively and efficiently developed in the context of IoT transmission security.

Thesis Works and Contributions

This thesis is a subpart of the IBNM CyberIoT Chair: "Security of the physical layer - an indispensable issue for the democratization of the Internet of Things", which focuses mainly on the field of Cyber-Physical systems, associated signal and information processing. This chair therefore aims to provide practical and innovative solutions to these problems, which are currently very little addressed at the physical layer level. The main challenge of the thesis relates more particularly to the use of efficient and robust error detector/corrector codes in the presence of strong interference in FD transmission, and capable of improving the SI cancellation and overall performance during the decoding procedure, especially in short-packet transmissions. First, we illustrated in the digital domain the channel coding schemes in case of FD transmission to overcome the effects of residual SI and quantization noise in the cancellation process, which produced by the quantization devices in DAC/ADC processes. These codes must have properties which allow good resistance to interference and fault correction. In addition, they will be optimized by integrating as closely as possible with other processes such as modulation,

interleaver, and channel estimation processes to form a transmission system, which is suited to the context of combating interference and eavesdropping. Research for such schemes is not trivial and requires new criteria to evaluate the performance of codes and new metrics to take into account the detection of an interference attempt in the decoding process. Consequently, two joint iterative channel estimation and decoding schemes (blind and semi-blind version) have been proposed. Then, in order to enhance the PLS, we applied these proposed algorithms with self-jamming technique to the FD short-packet wiretap transmission systems in case of passive and active eavesdroppers. The proposed algorithms show its robustness not only in reliability factor, by improving the overall performance during channel estimation and decoding processes, but also in security factor by reducing the security gap smaller than the conventional methods. This thesis works have been published as journal papers or conference proceedings. These papers are:

Journal:

- Bao Quoc Vuong, Roland Gautier, Anthony Fiche, Mélanie Marazin, Ta Quang Hien, Nguyen Lap Luat: *"Joint Iterative Blind Self-Interference Cancellation, Propagation Channel Estimation and Decoding Processes in Full-Duplex Transmissions"*, in IEEE Access 10: 22795 - 22807 (February 2022).

- Bao Quoc Vuong, Roland Gautier, Ta Quang Hien, Nguyen Lap Luat, Anthony Fiche, Mélanie Marazin: *"Joint Semi-Blind Self-Interference Cancellation and Equalization Processes in 5G QC-LDPC-Encoded Short-Packet Full-Duplex Transmissions"*, belongs to the Special Issue Full-Duplex Wireless Communication in MDPI Sensors 22(6): 2204 (March 2022).

- Bao Quoc Vuong, Roland Gautier, Anthony Fiche, Melanie Marazin and Cristina Despina-Stoian: *"Secrecy Coding Analysis of Short Packet Full-Duplex Transmissions with Joint Iterative Channel Estimation and Decoding Processes."*, belongs to the Special Issue Physical-Layer Security for Wireless Communications, in MDPI Sensors 22(14): 5257 (July 2022).

International Conference Proceeding:

- Bao Quoc Vuong, Roland Gautier, Anthony Fiche and Mélanie Marazin, *"Full-Duplex Efficient Channel Codes for Residual Self-Interference/Quantization Noise Cancellation*", in the proceeding of The IEEE 15th International Conference on Signal Processing and Communication Systems (ICSPCS), Sydney, Australia, 2021. (Online)

Thesis Organization

The outline of this thesis is organized as follows:

First of all, a general introduction to the FD transmission systems and its application is shortly introduced. Moreover, the contexts of IoT transmission and PLS area are also pointed out. Then, the motivation and contributions of this thesis are mentioned. Last but not least, the thesis organization is also provided.

In Chapter 1, we start with a brief survey of the most relevant state-of-the-art cancellation techniques. We summarize the existing architectures to reconstruct and cancel the SI component. Then, a brief overview of the existing estimation algorithms used to reconstruct the SI for SI cancellation in the propagation domain, analog domain, and digital domain is presented. Moreover, in this thesis, we focus mainly on the digital domain cancellation technique to suppress the residual SI component. The DSIC process has been introduced with Least Mean Square (LMS) and Recursive Least Square (RLS) algorithms to estimate the SI channel and reconstruct SI component. Simulation results are also provided for the estimation of the channel of these two methods. Furthermore, channel coding schemes are considered as the potential of PLS for 5G and beyond, The construction of encoding and decoding processes of 5G QC-LDPC codes, 5G polar codes and LTE Turbo codes is described in details in this chapter.

In Chapter 2, the impact of SI level and quantization noise, which are produced by DAC/ADC processes, on the performance of Single Input Single Output (SISO) FD transmission systems is considered. First, the channel coding schemes in the digital domain are used to overcome the effects of residual SI and quantization noise in the cancellation process. Then, we illustrate the influence of quantization noise on the DSIC process and compare the effects of SI channel power to the SISO FD transmission system with and without DSIC. Later, the Bit Error Rate (BER) performance obtained with and without the DAC/ADC process will be illustrated by changing the quantization bit resolution in the DAC/ADC process. Next, the performances of different quantizer device architectures at the receiver such as $\Sigma\Delta$ [53], Gaussian with mid-rise [54], pipeline [55] and Successive Approximation Registers ADC (SAR) [56] are evaluated. Finally, a comparison between the system with and without DAC/ADC is considered for both the case of HD and FD transmission. Last but not least, the choice of bit resolution for DAC/ADC process is also noticed. The results of this chapter emphasize that the use of channel coding schemes and DSIC process is necessary for FD transmission systems.

In Chapter 3, we propose first a joint iterative blind SI cancellation, propagation channel estimation and decoding algorithm in FD transmissions via feedback of channel estimates and decoded messages combined with the process of DSIC. Unlike the conventional algorithm, the proposed blind algorithm simultaneously estimates the self-interference and propagation channels and decodes messages in each iteration of 5G QC-LDPC codes

decoding. The temporary estimations of the intended channel and decoded message are fed back to improve self-interference cancellation and also channel estimation and decoding in the next iteration. This chapter further proposes a partial feedback scheme, which only uses a few feedback symbols for channel estimation, to significantly reduce processing time and computational complexity while maintaining performance. These good properties seem quite suitable for a use of this proposed blind iterative algorithm for short-length packet FD transmissions in IoT applications and green communications.

In Chapter 4, to avoid the effect of consequent decoding error in the first proposed scheme in Chapter 3 when using the blind algorithm in the low region of Signal to Noise Ratio (SNR), a semi-blind version is developed taking into account only a few pilot symbols and cooperating with the estimated version of the intended channel to form the feedback component.

In Chapter 5, we implement a combination of two joint iterative channel estimation and decoding techniques and self-jamming technique to enhance PLS in a SISO FD transmission. Indeed, the legitimate receiver and eavesdropper can simultaneously receive the intended signal from the transmitter and broadcast the self-jamming or jamming signal to the other. The proposed blind and semi-blind algorithms in previous chapters are used. In case of passive eavesdropper, the blind channel estimation with feedback scheme is applied, where the temporary channel estimate and decoded message are fed back to improve both channel estimation and decoding processes in the next iteration. In case of active eavesdropper, the semi-blind algorithm is considered by trading four pilot symbols and only requiring the feedback for channel estimation processes.

To sum up the contributions of this thesis, a brief summary is shown in the conclusion and future works.

Chapter 1

Literature Review

This chapter first provides a brief survey of the most relevant state-of-the-art cancellation techniques. Then, the existing architectures to reconstruct and cancel the SI are summarized. A brief overview of the existing estimation algorithms are also presented, which are used to reconstruct the SI for SI cancellation in propagation domain, analog domain as well as digital domain is presented. Moreover, we focus mainly on the digital domain cancellation technique to suppress the residual SI component in this thesis, the DSIC process has been introduced with LMS and RLS algorithms in order to estimate the SI channel and reconstruct SI component. Simulation results are also provided for the estimation of the channel of these two methods. Furthermore, the construction of encoding and decoding processes of 5G QC-LDPC codes, 5G polar codes and LTE Turbo codes is also described in details in this chapter.

1.1 State-of-the-Art of the Self-Interference Cancellation in Full-Duplex Systems

In FD transmission systems, the total signal at the receiver consists of the interference signal caused by its wireless transmissions, the intended signal arriving from another system, and also the environment noise. The main purpose of SI mitigation techniques is to cancel as much as possible the SI signal and to ensure the recovering of the intended signal. So, SI cancellation would play the most critical role in implementing practical FD communication systems both academia [6, 57] and industry [58, 59]. Consequently, many researches have been focused on the potential techniques for channel estimation and SI cancellation in FD communication, especially in short-packet FD transmissions for IoT applications [50, 60–62].

Indeed, the process of cancelling the SI in a FD transmission system is usually separated into three different stages or domains such as RF cancellation, analog cancellation and digital cancellation, which is shown in Fig. 1.1. Firstly, in terms of wireless propa-

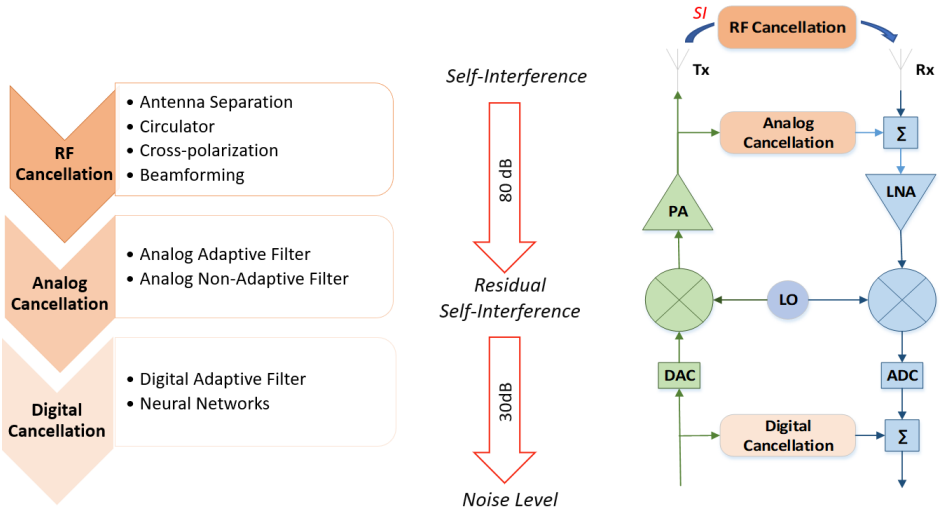


Fig. 1.1: Self-Interference cancellation techniques.

gation, there is the possibility of combining techniques such as antenna direction, cross-polarization or transmit beamforming, which is called antenna SI cancellation technique or RF cancellation. In this case, the desired signal may also be affected by these methods, which motivates the introduction of analog circuit domain techniques. The latter consists of subtracting a copy of the transmitted signal from the received one, adjusted with a proper gain, phase, and delay, usually performed by RF circuits. Although the applications of the mentioned methods can achieve the required power-to-interference-plus-noise level to reliably communicate in test sets, when taking into account real environment effects, it is usually not enough. To deal with channel variations in such scenarios, adaptive filters in the digital domain are employed, allowing heavy signal processing necessary to estimate the SI channel and reconstruct the SI component. Moreover, this domain allows the use of techniques such as optimal power allocation, adaptive filtering, adaptive beamforming, etc., to further improve the mitigation of SI. However, this thesis focuses mainly on the digital domain, with the assumption that the SI level is greater than the noise level of 30 to 50 dB.

1.1.1 RF Cancellation

Also known as passive suppression, antenna cancellation is the annulation achieved in the electromagnetic field and consists of increasing the isolation between the receiving and transmitting antennas to avoid receiver circuit saturation [8, 63–65]. The antenna SI-cancellation techniques aim to reduce the SI that impinges on the receiving antennas by a proper design of the transmitting and receiving antenna structures. Antenna cancellation can be implemented using advanced antenna design to improve isolation between transmitting and receiving antenna ports [66] or using an auxiliary transmitting antenna [67]. Antenna SI-cancellation can be achieved by using antenna separation, polarization, and isolation [64], directional antennas [63] or antennas placement to create null space

at the received antennas [65]. The applicability of each one of these methods depends on the application and the physical constraints of the system. When a FD transceiver is designed, we have the choice between two methods of interfacing antennas. Either we use physically separate antennas for transmission or reception, or we use a shared antenna in which one antenna to simultaneously transmit and receive, where the transmission and reception paths are isolated through a circulator, which are shown in Fig. 1.2, respectively.

(a) Dual Separated Antenna.

(b) Shared antenna via circulor.

Fig. 1.2: Antenna domain suppression configurations.

1.1.2 Analog Cancellation

After suppression in RF cancellation, the SI component will continuously go to the analog cancellation that uses the knowledge of the transmitted SI to suppress the SI before the LNA and ADC by subtracting an estimate of the received SI from the received signal. A copy version of the transmitted signal, which is obtained from the output of Power Amplifier (PA), is used to pass through a cancellation circuit to reconstruct a copy of the received SI. The signal at the PA output also includes the distortions of the transmitter, which are reduced by the analog cancellation stage. The design of the cancelling circuit is highly related to the nature of the SI channel. In FD transmission, the SI channel can be separated into internal reflections with a lower number of pathways, shorter delays, and stronger amplitudes when compared to the external or far-filed reflections. The internal reflections are almost static by depending on the internal components and the structure of the transceiver, while the external reflections vary according to the surrounding environment. Therefore, the analog cancellation stage reduces the static internal reflections due to the difficulty to adapt the analog circuits with the variations of the external reflections. One famous solution is using Tapped Delay Lines (TDL) of variable delays and tunable attenuators to model the SI channel, which is similar to an analog Finite Impulse Response (FIR) filter. The lines are then collected back, summed up and the total signal is then subtracted from the received signal. The TDL structure is described in Fig. 1.3. Control algorithms are used to find the optimal coefficients for the attenuator, the phase shifter, and the delay line of each tap. The parameters of the circuit are adjusted to minimize the

residual energy after cancellation and the error between the response of the circuit and the internal reflections' response [68, 69]. The SI reduction of the TDL varies from 30 to 45 dB [63, 69, 70]. Furthermore, the advantage of digital signal processing techniques can also be used to accurately reconstruct the linear channel response and suppress the SI components coming from the random external reflections by using a digital symbol-synchronous FIR filter. The transmit signal is tapped in digital baseband and properly reconstruct SI by adjusting the attenuation and phase accordingly. The reconstructed SI signal is converted to the analog domain and combined with the SI signal before Low Noise Amplifier (LNA) through a coupler [71, 72].

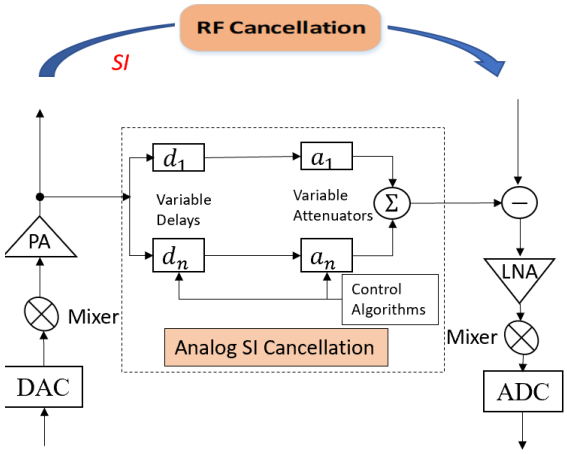


Fig. 1.3: Analog cancellation stage.

1.1.3 Digital Cancellation

After RF cancellation and analog cancellation techniques, a large amount of SI remains to be reduced in the following cancellation stages, which is called residual SI. In particular, external reflections need more adaptive cancellation methods, which can be done using digital signal processing to suppress the SI level from 30 to 50 dB to the noise level. Several methods have been proposed to cancel SI in the digital domain, such as using neural networks [4, 10, 73] or using a digital adaptive filter [74, 75]. In this chapter, we first implement a DSIC algorithm based on the improved variable step using and comparing the Least Mean Square (LMS) and Recursive Least Square (RLS) algorithms. The adaptive filter at the channel estimation step is used to monitor the time variation of wireless channel via updating steps, to get a better estimate of the channel state, and a better reconstruction of the interference signal in real time. Let us consider a simple DSIC process at user A as shown in Fig. 1.4.

At the receiver, the copy version of the input signal (called SI signal) $x_A[n]$ and the received signal at Rx after ADC process $y_A[n]$ are used to calculate the system error signal $\mathcal{E}(n)$, with n the index step. Then, based on the error signal $\mathcal{E}(n)$, we can control and modify the unknown SI channel vector $\hat{\mathbf{h}}_{AA}$ by using the LMS and RLS algorithms [76].

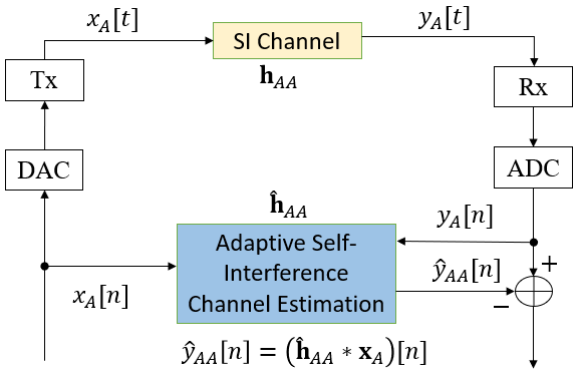


Fig. 1.4: Digital Self-Interference Cancellation Process.

As a result, we can effectively track the estimation of the SI wireless channel $\hat{\mathbf{h}}_{AA}$, which generates an interference signal as $\hat{y}_{AA}[n] = (\hat{\mathbf{h}}_{AA} * \mathbf{x}_A)[n]$.

1.1.3.1 LMS Algorithm

The LMS algorithm [76] belongs to a class of adaptive filters used to mimic a desired filter by finding the filter coefficients that relate to produce the least mean square of the error signal, which is calculated by the difference between the desired and the actual signal. It is a stochastic gradient descent method in that the filter is only adapted based on the error at the current time. The mathematical expression for this algorithm is given as follows:

1. Initial value: $\hat{\mathbf{h}}_{AA}^{[0]} = \overbrace{[0, 0, ..., 0]}^{L}$ with L is the length of the SI channel;
2. Computation: for : $n = L, L+1, ..., length(\mathbf{x_A})$;

$$\mathcal{E}[n] = y_A[n] - \hat{\mathbf{h}}_{AA}^{[n]\mathcal{H}}\mathbf{x}[n]; \tag{1.1}$$

where $\mathbf{x}[n] = [x_A[n], x_A[n-1], ..., x_A[n-L+1]]$

$$\hat{\mathbf{h}}_{AA}^{[n+1]} = \hat{\mathbf{h}}_{AA}^{[n]} + \mu\mathcal{E}^*[n]\mathbf{x}[n] \tag{1.2}$$

where:

- μ is a step size factor that controls the algorithm stability and rate of convergence;
- $\hat{\mathbf{h}}_{AA}^{(n)\mathcal{H}}$ is the Hermitian transposition of $\hat{\mathbf{h}}_{AA}$;
- $\mathcal{E}^*[n]$ is the complex conjugate of $\mathcal{E}[n]$

The convergence and performance of this algorithm depend on the learning rate step. If μ is small, the LMS algorithm converges very slowly, while too large values of μ may lead to a less stable solution around the minimum value.

1.1.3.2 RLS Algorithm

The RLS filter [76] is derived from the Least Square (LS) algorithm and uses an average time error. It is an adaptive filter algorithm that recursively finds the coefficients that minimize a weighted linear least squares cost function related to the input signals. It is different with the LMS algorithm that aim to reduce the mean square error. In the RLS derivation, the input signals are considered deterministic, while for the LMS and similar algorithms, they are considered stochastic. Compared to other adaptive filter algorithms, the RLS exhibits extremely fast convergence. However, this benefit comes at the cost of high computational complexity. The mathematical expression for this algorithm is given as follows:

1. Initial value:

- $\hat{\mathbf{h}}_{AA}^{[0]} = \overbrace{[0, 0, ..., 0]}^{L}$ with L is the length of the SI channel;
- $\mathcal{T}(0) = \delta^{-1}\mathbf{I}$ where $\mathbf{I}$ is the identity matrix of rank L;

2. Computation: for : $n = L, L+1, ..., length(\mathbf{x_A})$;

$$\mathcal{E}[n] = y_A[n] - \hat{\mathbf{h}}_{AA}^{(n-1)\mathcal{H}}\mathbf{x}[n] \tag{1.3}$$

where $\mathbf{x}[n] = [x_A[n], x_A[n-1], ..., x_A[n-L+1]]$

$$\mathbf{q}[n] = \frac{\mathcal{T}[n-1]\mathbf{x}[n]}{\lambda(1 + \mathbf{x}^{\mathcal{H}}[n]\lambda^{-1}\mathcal{T}[n-1]\mathbf{x}[n])} \tag{1.4}$$

$$\mathcal{T}[n] = \frac{1}{\lambda(\mathcal{T}[n-1] - q[n]\mathbf{x}^{\mathcal{H}}[n]\mathcal{T}[n-1])} \tag{1.5}$$

$$\hat{\mathbf{h}}_{AA}^{(n)} = \hat{\mathbf{h}}_{AA}^{(n-1)} + \mathcal{E}^{*}[n]\mathbf{q}[n] \tag{1.6}$$

where:

- λ is the forgetting factor and should be chosen between 0.9 and 1;
- δ is the regularization parameter used to initialize $\mathcal{T}(0)$, and should be assigned a small value for a high signal-to-noise ratio (SNR) (greater than 10 dB) and a large value for a low SNR (less than 10 dB) [76];
- $\mathbf{x}^{\mathcal{H}}[n]$ is the Hermitian transposition of $\mathbf{x}[n]$.

1.1.3.3 Rayleigh Distribution Channel Model

In FD transmission, the SI channel consists of two components: Line-of-Sight (LoS), which is generated by the direct link between the transmitter and receiver, and non Line-of-Sight (nLoS), which is produced by signal scatters. So, its first tap could be modeled as

Rician fading, and the remaining channel taps are modeled as Rayleigh fading [75]. The LoS component is cancelled by RF cancellation and analog cancellation processes, and the remained residual component will be cancelled in digital domain [77]. In this thesis, we focus mainly on the digital domain to cancel the residual SI signal after RF and analog SI cancellation. So, the Rayleigh distribution channel and its impusle response is expressed as:

$$h_{AA}(t) = \sqrt{\frac{p_A}{2}}[p_1\delta(t-\tau_1) + p_2\delta(t-\tau_2) + ... + p_L\delta(t-\tau_L)] \tag{1.7}$$

where p_A is the total channel power, $p_1, p_2, ..., p_L$ are the taps power of the channel in linear scale, $\tau_1, \tau_2, ..., \tau_L$ is the tap relative delay in ns and L is the channel length.

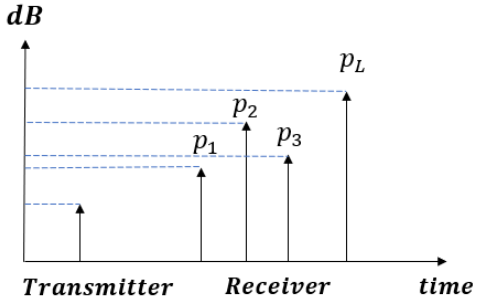


Fig. 1.5: Impulse response of a multi-path channel.

In the context of FD transmission and also FD short-packet transmission for IoT applications, the intended channel is usually modeled as Rayleigh distribution [50, 61, 77, 78]. Therefore, in this thesis, it is reasonably to use the International Telecommunication Union (ITU) – R channel models on the intended channel, that based on Rayleigh distribution with several models such as indoor office, pedestrian and vehicle test environment [79]. The power of each tap (in dB) and delay (in ns) are listed in Table 1.1.

Table 1.1: ITU – R Channel Model Parameters

Tap	**Indoor Office**		**Pedestrian**		**Vehicular**	
	Power (dB)	**Delay (ns)**	**Power (dB)**	**Delay (ns)**	**Power (dB)**	**Delay (ns)**
1	0	0	0	0	0	0
2	-3	50	-9.7	110	-1	310
3	10	110	-19.2	190	-9	710
4	-18	170	-22.8	410	-10	1090
5	-26	290	0	0	-15	1730
6	-32	310	0	0	-20	2510

1.1.3.4 Comparison of DSIC Process Using LMS and RLS Algorithms

In this section, the simulation results will be analyzed to examine the performance of DSIC process on SISO FD transmission at a particular user A. The intended channel is based on the ITU-R pedestrian model. Fig. 1.6 shows the channel estimation error of the

DSIC process using the LMS algorithm and the RLS algorithm. The SI power p_A will be set at 30 dB and the signal-to-noise ratio at user A (SNR_A) is fixed at 20 dB. In this case, the step μ in LMS algorithm and the forgetting factor λ in RLS algorithm will be changed. In general, we can see that the DSIC process is quite good for both algorithms used. In LMS method, the estimate error reduces when the step μ decreases, and when $\mu = 0.01$, the channel estimation error (in dB) slowly goes to the final result and can reach to nearly -19 dB. Vice versa, in the RLS method, the increase of forgetting factor λ will lead to the decrease of the channel estimation error (in dB), especially it can go to about -28 dB when $\lambda = 0.999$ and it can be observed that there is nearly no delay for the system to reach the saturation value. The RLS method quickly approaches the final value of the channel estimation error or the received signal error, while the LMS algorithm needs up to about 1000 transmitted symbols to achieve the final result. It makes sense with the work in [74, 75], where the RLS algorithm gives a better choice in the DSIC process, compared to other methods.

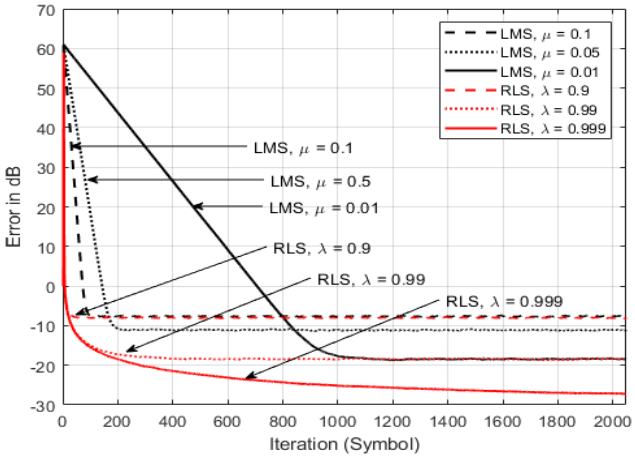


Fig. 1.6: Channel estimation error, $p_A = 30$ dB, $SNR_A = 20$ dB.

In summary, it can be seen that the RLS algorithm outperforms the LMS algorithm in the DSIC process in SISO FD transmission. In particular, it has a faster convergence and is also less sensitive than the LMS algorithm. Therefore, for the remainder of this thesis, the RLS algorithm with $\lambda = 0.999$ is used for implementation.

Although the SI component can be suppressed to noise floor level by using several cancellation methods, channel coding schemes must be used in any FD communication systems in order to improve data correction errors and system performance over noisy communication channels. In the next section, the efficient and up-to-date channel coding schemes such as 5G QC-LDPC codes, 5G Polar codes and LTE Turbo codes will be introduced, which are suitable coding techniques in short-packet transmission, especially for the IoT standard [80–83]. The encoding and decoding processes of these channel coding techniques are also introduced in details.

1.2 Channel Coding Schemes for 5G Transmissions

Information theory and Error Correcting Codes (ECC) are the research areas that study information measurement as well as reliable transmission and compression. Among the ECC, Low Density Parity Check (LDPC) codes and Polar codes are the most efficient codes because they can nearly achieve Shannon capacity performance [84, 85]. LDPC codes were first proposed by Gallager in 1962 [84] and Tanner with graph theory in 1981 and were rediscovered again by MacKay in the late 1990s [86], where Polar codes were introduced by Arikan in [85]. The 3GPP project has introduced the QC-LDPC and Polar codes as standard codes of the 5G New Radio (NR) for the control information in uplink and downlink on the eMBB, uRLLC and mMTC because it supports a number of lifting sizes and different code rates with high throughput and low latency, which are suitable coding techniques in short-packet transmission, especially for the IoT standard [80, 82, 83]. Furthermore, Turbo code, which is the fundamental channel coding technique in the 3G, 4G LTE system, and 4G Machine Type Communications (MTC), NB-IoT [87], can also be considered as a candidate in the 5G channel coding scheme for short-packet information with lower processing throughput for mMTC [88–90]. Turbo codes were original introduced by C. Berrou in 1993 [91], which implemented by using parallel concatenation convolution codes to increase the length of the codes and increase the security. Many investigations have been conducted to compare and validate the performance of LDPC, Polar and Turbo codes for the 5G channel [89, 92, 93], and they also found that Turbo codes were also a potential coding technique with short-packet transmission, especially for the IoT standard. Therefore, the content of construction, encoding and decoding processes of three channel coding schemes will be described in detail in the following parts.

1.2.1 5G Quasi-Cyclic Low Density Parity Check Codes

By definition, the parity check matrix $\mathbf{H}_{LDPC}$ of a LDPC code has a low density of 1's. Each parity check matrix $\mathbf{H}_{LDPC}$ of a LDPC code can be visualized with a Tanner graph. Equation 1.8 is a parity-check matrix of an LDPC code with four 1's in each row and 2 ones in each column, and Fig. 1.7 shows the corresponding Tanner graph of the $(10, 5)$ LDPC codes. The Tanner graph contains two types of nodes: the symbol node (or variable node) f and the check node c. Each check node and symbol node represent one row and one column, respectively, in the parity check matrix $\mathbf{H}_{LDPC}$. $\mathbf{H}_{LDPC}$ has the size of 5×10 for 5 check nodes and 10 symbol nodes. In Fig. 1.7, the check node c_i and the symbol node f_j are connected if $H_{LDPC}(i, j) = 1$.

Furthermore, 3GPP has introduced QC-LDPC as the standard code of 5G to eMBB data channel, because it supports for a number of lifting sizes and different code rates [80]. It can be seen as the coding chain of Physical Uplink Shared Channel (PUSCH) and

Physical Downlink Shared Channel (PDSCH) [80]. In the following parts, we first review and introduce the contents of circulant permutation matrix and the base graph matrix, which are the fundamentals to construct QC- LDPC codes and adapt for 5G LDPC codes. After that, the process of building the exponent parity check matrix, constructing the code word in encoding, and reconstructing the message bits in decoding are presented.

$$\mathbf{H}_{LDPC} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \tag{1.8}$$

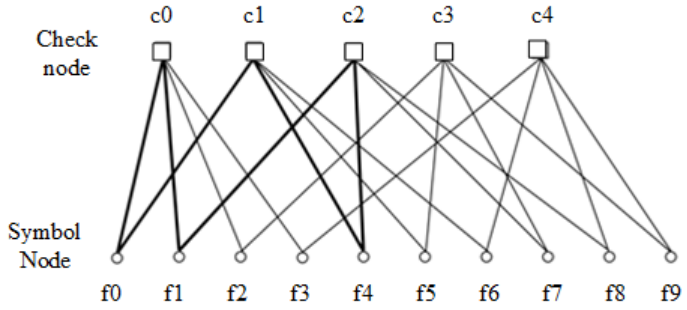


Fig. 1.7: Tanner graph.

1.2.1.1 Circulant Permutation Matrix

Let Z be a positive integer and $\mathbf{Z}_c = [-1, 0, 1, 2, ..., Z-1]$, we present a circular permutation matrix of size $\mathbf{I}(\mathcal{P}_{i,j})$ by circularly shifting the identity matrix $\mathbf{I}$ of size $Z \times Z$ to the right $\mathcal{P}_{i,j}$ times, where $\mathcal{P}_{i,j} \in \mathbf{Z}_c$. We denote this binary circulant matrix by $\mathcal{Q}(\mathcal{P}_{i,j})$ and it becomes more sparse with increasing Z. For convenience, we denote $\mathcal{Q}(0)$ as the identity matrix and $\mathcal{Q}(-1)$ as the null matrix. Let take an example of the lifting size $Z = 3$ and we get:

$$\begin{aligned} \mathcal{Q}(0) &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \mathcal{Q}(-1) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \\ \mathcal{Q}(1) &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \mathcal{Q}(2) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \end{aligned} \tag{1.9}$$

Table 1.2 shows all possible lifting sizes Z where $\gamma \in \{2, 3, 5, 7, 9, 11, 13, 15\}$, $0 \leq \theta \leq 7$, $Z = \gamma 2^{\theta}$ and the set index i_{LS}.

Table 1.2: All possible lifting sizes of Z

Set index i_{LS}	γ	θ	**Set of lifting size** Z
0	2	{0,1,2,3,4,5,6,7}	{2,4,8,16,32,64,128,256}
1	3	{0,1,2,3,4,5,6}	{3,6,12,24,48,96,192,384}
2	5	{0,1,2,3,4,5,6}	{5,10,20,40,80,160,320}
3	7	{0,1,2,3,4,5}	{7,14,28,56,112,224}
4	9	{0,1,2,3,4,5}	{9,18,36,72,144,288}
5	11	{0,1,2,3,4,5}	{11,22,44,88,176,352}
6	13	{0,1,2,3,4}	{13,26,52,104,208}
7	15	{0,1,2,3,4}	{15,30,60,120,240}

The exponent parity check matrix $\mathbf{H}$ of the QC-LDPC code is presented by the following $m_b \times n_b$ array of $Z \times Z$ circulants over the finite Galois field GF(2):

$$\mathbf{H} = \begin{bmatrix} \mathcal{Q}(\mathcal{P}_{1,1}) & \mathcal{Q}(\mathcal{P}_{1,2}) & \dots & \mathcal{Q}(\mathcal{P}_{1,n_b}) \\ \mathcal{Q}(\mathcal{P}_{2,1}) & \mathcal{Q}(\mathcal{P}_{2,2}) & \dots & \mathcal{Q}(\mathcal{P}_{2,n_b}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{Q}(\mathcal{P}_{m_b,1}) & \mathcal{Q}(\mathcal{P}_{m_b,2}) & \dots & \mathcal{Q}(\mathcal{P}_{m_b,n_b}) \end{bmatrix} \tag{1.10}$$

The value of $\mathcal{P}_{i,j}$ is calculated by using the formula $\mathcal{P}_{i,j} = \mathrm{mod}(\mathcal{V}_{i,j}, Z)$ where $\mathcal{V}_{i,j}$ is the shift coefficient of the $(i,j) - th$ element in the corresponding shift design and given in the Table 5.3.2-2 and Table 5.3.2-3 according to [80].

For example, take the base matrix $\mathbf{B}$ with the size of 3×3 and the lifting size $Z = 3$, so $\mathcal{P}_{i,j} \in [-1, 0, 1, 2]$;

$$\mathbf{B} = \begin{bmatrix} 1 & -1 & 0 \\ 2 & 1 & -1 \\ -1 & 0 & 2 \end{bmatrix} \Rightarrow \mathbf{H} = \begin{bmatrix} \mathcal{Q}(1) & \mathcal{Q}(-1) & \mathcal{Q}(0) \\ \mathcal{Q}(2) & \mathcal{Q}(1) & \mathcal{Q}(-1) \\ \mathcal{Q}(-1) & \mathcal{Q}(0) & \mathcal{Q}(2) \end{bmatrix} \tag{1.11}$$

Using the equation (1.9), after doing the circularly shifting, the exponent parity check matrix $\mathbf{H}$ becomes:

$$\mathbf{H} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \tag{1.12}$$

1.2.1.2 Base Graph Characteristics

According to [80, 94], there are two possible Base Graph (BG) with the same structure in 5G LDPC codes: **BG1** and **BG2**. **BG1** is designed for large block lengths up to 8448 and code rates from 1/3 to 8/9 while **BG2** is targeted for the smaller information block lengths less than 3840 and code rates from 1/5 to 2/3. In particular, the base matrix **BG1** has a maximum size of $m_Z \times n_Z = 46 \times 68$, while **BG2** has a maximum size of $m_Z \times n_Z = 42 \times 52$. The Fig. 1.8 shows the scatter diagram of **BG1** for 5G LDPC codes with different code rate.

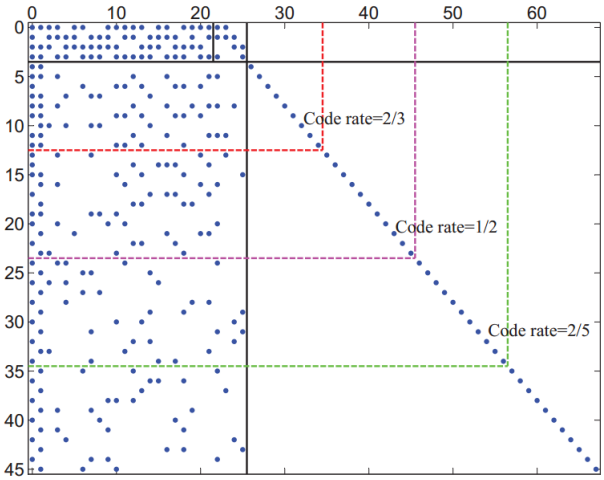


Fig. 1.8: Scatter diagram of **BG1**, Copyright © 2018 IEEE [95].

The base matrix $\mathbf{BG} \in \{\mathbf{BG1}, \mathbf{BG2}\}$ can be separated into six smaller matrices as shown in Fig. 1.9, where k_b denotes the number of columns of the information circulant and is expressed as:

$$\mathbf{BG} = \begin{bmatrix} \mathbf{A} & \mathbf{D} & \mathbf{O} \\ \mathbf{E_1} & \mathbf{E_2} & \mathbf{I} \end{bmatrix} \tag{1.13}$$

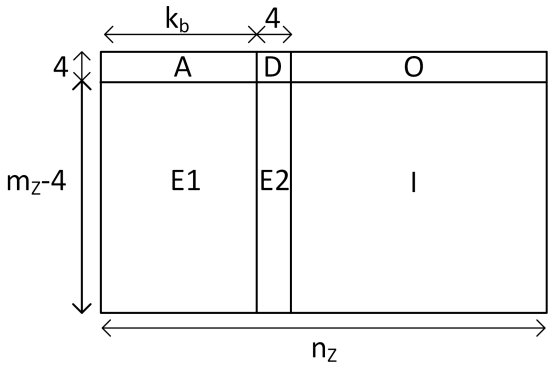


Fig. 1.9: Structure of the base matrix **BG**.

where **A** is the matrix of systematic bits, **D** is a square matrix with bidiagonal structure: the first column is of weight 3 and the other column has an upper bidiagonal

structure, **O** is a null matrix and **I** is an identity matrix. We can present these matrices as follows:

$$\mathbf{A} = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,k_b} \\ a_{2,1} & a_{2,2} & \dots & a_{2,k_b} \\ a_{3,1} & a_{3,2} & \dots & a_{3,k_b} \\ a_{4,1} & a_{4,2} & \dots & a_{4,k_b} \end{bmatrix}, \mathbf{E}_1 = \begin{bmatrix} e_{1,1} & e_{1,2} & \dots & e_{1,k_b} \\ e_{2,1} & e_{2,2} & \dots & e_{2,k_b} \\ \dots & \dots & \ddots & \vdots \\ e_{m_Z-4,1} & e_{m_Z-4,2} & \dots & e_{m_Z-4,k_b} \end{bmatrix}, \\ \mathbf{E_2} = \begin{bmatrix} e_{1,k_b+1} & e_{1,k_b+2} & \dots & e_{1,k_b+4} \\ e_{2,k_b+1} & e_{2,k_b+2} & \dots & e_{2,k_b+4} \\ \dots & \dots & \ddots & \vdots \\ e_{m_Z-4,k_b+1} & e_{m_Z-4,k_b+2} & \dots & e_{m_Z-4,k_b+4} \end{bmatrix}, \tag{1.14}$$

There are two types of **D** for each base graph based on the value of i_{LS} as the following:

$$\mathbf{D}_{BG1\_1} = \begin{bmatrix} 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \\ -1 & -1 & 0 & 0 \\ 1 & -1 & -1 & 0 \end{bmatrix} \text{ and } \mathbf{D}_{BG1\_2} = \begin{bmatrix} 0 & 0 & -1 & -1 \\ 105 & 0 & 0 & -1 \\ -1 & -1 & 0 & 0 \\ 0 & -1 & -1 & 0 \end{bmatrix} \\ \mathbf{D}_{BG2\_1} = \begin{bmatrix} 0 & 0 & -1 & -1 \\ -1 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 \\ 0 & -1 & -1 & 0 \end{bmatrix} \text{ and } \mathbf{D}_{BG2\_2} = \begin{bmatrix} 1 & 0 & -1 & -1 \\ -1 & 0 & 0 & -1 \\ 0 & -1 & 0 & 0 \\ 1 & -1 & -1 & 0 \end{bmatrix} \tag{1.15}$$

In **BG1**, $\mathbf{D}_{BG1\_1}$ is used for $i_{LS} = \{0, 1, 2, 3, 4, 5, 7\}$ and $\mathbf{D}_{BG1\_2}$ is used for $i_{LS} = 6$. Where in **BG2**, $\mathbf{D}_{BG2\_1}$ is used for $i_{LS} = \{0, 1, 2, 4, 5, 6\}$ and $\mathbf{D}_{BG2\_2}$ is used for $i_{LS} = 7$.

1.2.1.3 How to Construct an Exponent Parity Check Matrix H

A set of base graph matrices will be built according to the lifting size, as mentioned in Table 1.2. To implement a specific information length and code rate, puncturing and shortening methods are used for 5G LDPC codes. Shortening is designed to only add zero to the information bits, and puncturing is applied to both the information bits and the parity bits of the code word. Furthermore, the 5G LDPC encoder will ignore the first 2 column bits because both **BG1** and **BG2** and for all code rates, these bits are punctured before transmission. The rest of this section describes how to construct an exponent parity check matrix **H** for an (N, K) LDPC code with information length K and code rate $R = K/N$. According to 3GPP in [80], $k_b = 22$ in **BG1** and $k_b \in \{10, 9, 8, 6\}$ in **BG2**, which based on the size of information bits K. The authors in [94] introduced an algorithm to determine the base graph matrix and k_b based on the value of information length K, and the code rate R, which is presented in Algorithm 1.1.

The construction of **H** with $m_b Z$ rows and $n_b Z$ columns consists of the following steps:

Algorithm 1.1: Determine the Base Graph Matrix and K_b in 5G QC-LDPC Codes

Inputs : K, R;
Outputs : Base matrix, k_b;
if $K > 3840$ **then**
  Base matrix = **BG1** ;
else if $K \leq 308$ **then**
  Base matrix = **BG2** ;
else
  if $R > (2/3)$ **then**
    Base matrix = **BG1**;
  else
    Base matrix = **BG2**;
  end
end
if *Base matrix* = ***BG1*** **then**
  $k_b = 22$;
else
  if $K > 640$ **then**
    $k_b = 10$;
  else if $560 < K \leq 640$ **then**
    $k_b = 9$;
  else if $192 < K \leq 560$ **then**
    $k_b = 8$;
  else
    $k_b = 6$;
  end
end
return Base matrix, k_b;

Step 1: For the given K and R, choose the suitable base graph matrix and k_b according to Algorithm 1.1.

Step 2: Choose Z as the minimum value according to Table 1.2, in which $k_b Z \geq K$

Step 3: Select the nearest integers Θ greater than or equal to k_b/R and calculate $n_b = \Theta + 2$ and $m_b = n_b - k_b$.

Step 4: Based on the value of Z, the suitable matrix from the set of built-in base graph matrices will be chosen.

Step 5: Convert each element of the matrix chosen in the previous into a binary circulant permutation matrix of size $Z \times Z$ or zero matrix of the same size to obtain the exponent parity check matrix **H** with the size of $m_b Z \times n_b Z$.

Step 6: Puncturing and shortening will apply to the encoding process for implementing the compatible property of 5G LPDC, where:

- Number of punctured bits from the first 2 columns: $N_{punct1} = 2Z$,
- Number of shortened information bits: $N_{pad} = k_b z - N$,

- Number of punctured bits from right to left: $N_{punct1} = n_b - 2Z - N - N_{pad}$

Step 7: Finally, we obtain the possible exponent parity check matrix **H**. This matrix **H** will be used for the encoding and decoding of the (N, K) 5G LDPC codes.

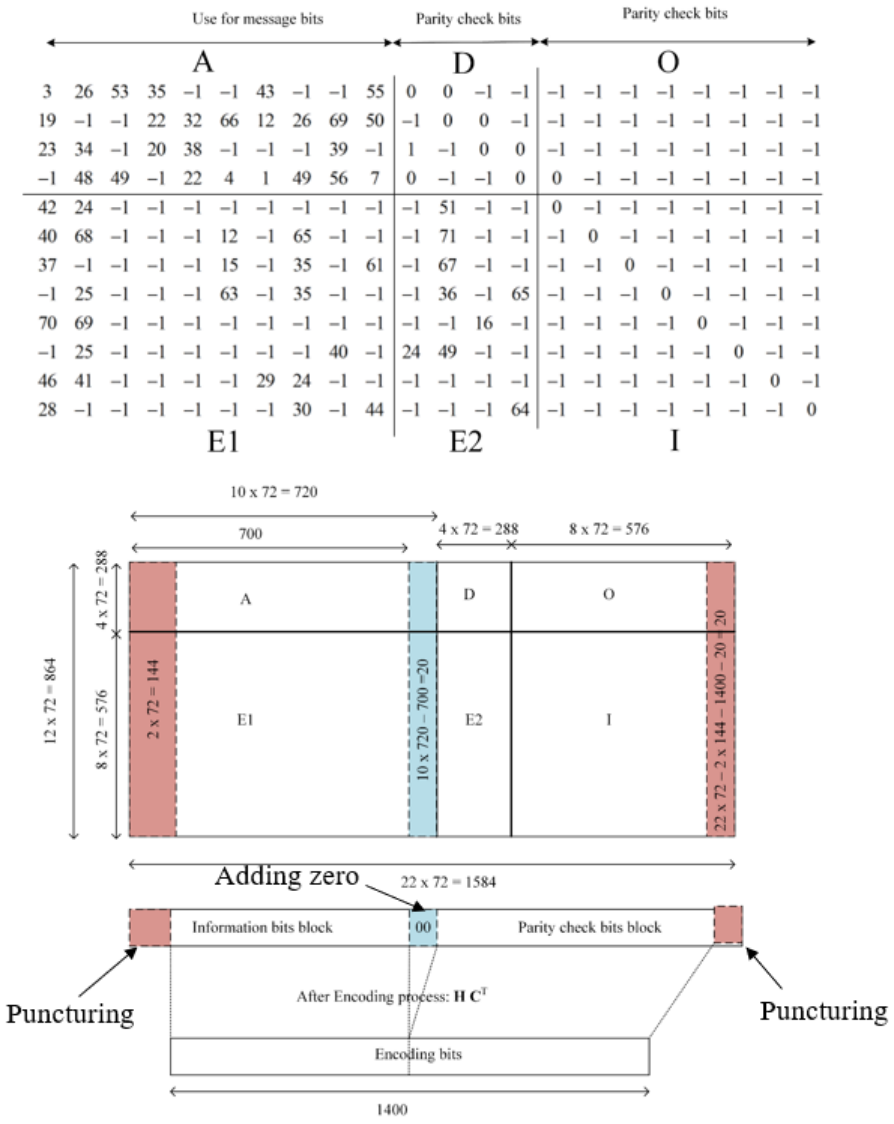


Fig. 1.10: Example of a construction of **H** in (1400,700) 5G QC-LDPC codes, $R = 1/2$.

For example, we construct a parity check matrix **H** that using for the encoding $(1400, 700)$ 5G QC-LDPC codes with code rate $R = 1/2$.

- First, based on Algorithm 1.1, we use **BG2** and $k_b = 10$;

- We choose $Z = 72$ to satisfy condition $k_b Z \geq K$;

- We determine $\Theta = 10/1/2 = 20$ so $n_b = \Theta + 2 = 22$ and $m_b = n_b - k_b = 12$;

- We obtain the matrix $(12, 22)$ as shown in Fig. 1.10, and continue to convert each of its elements into a binary circulant permutation matrix of size 72×72 or a zero matrix of the same size to obtain the exponent parity check matrix **H** with the size of 864×1584;

- We apply the puncturing and shortening processes to the previous exponent parity check matrix H to obtain the $(1400, 700)$ LDPC codes.

- Number of punctured bits of the first 2 columns: $N_{punct1} = 2Z = 2 \times 72 = 144$;
- Number of shortened information bits: $N_{pad} = k_b Z - K = 10 \times 72 - 700 = 20$;
- Number of punctured bits from right to left: $N_{punct2} = 22 \times 72 - 144 - 1400 - 20 = 20$.

1.2.1.4 5G QC-LDPC Encoding Process

Let us consider a code word $\mathbf{c}$, in which each element is a vector of length Z: $\mathbf{c} = [\ \mathbf{x} \quad \mathbf{s_d} \quad \mathbf{s_e}] = [x_1, ..., s_{k_b}, s_{d1}, ..., s_{d4}, s_{e1}, ..., s_{e_{mb}-4}]$ where $\mathbf{x}$ is the message bits and $\mathbf{s_d}, \mathbf{s_e}$ is the extra bits to construct the code word $\mathbf{c}$. It can be found by the following steps:

Step 1: The encoding process is performed as the following equation:

$$\begin{aligned} \mathbf{H}\mathbf{c}^T &= \begin{bmatrix} \mathbf{A} & \mathbf{D} & \mathbf{O} \\ \mathbf{E_1} & \mathbf{E_2} & \mathbf{I} \end{bmatrix} \begin{bmatrix} \mathbf{x}^T \\ \mathbf{s}_d^T \\ \mathbf{s}_e^T \end{bmatrix} = 0, \\ &=> \begin{cases} \mathbf{A}\mathbf{x}^T + \mathbf{D}\mathbf{s}_d^T = 0 & (*) \\ \mathbf{E_1}\mathbf{x}^T + \mathbf{E_2}\mathbf{s}_d^T + \mathbf{I}\mathbf{p}_e^T = 0 & (**) \end{cases} \end{aligned} \tag{1.16}$$

Step 2: From the equation 1.16 (*), and for example $\mathbf{D} = \mathbf{D}_{BG_1}$, we can calculate for $\mathbf{s_d}$:

$$\begin{cases} \sum_{j=1}^{k_b} a_{1,j} x_j + s_{d1}^{(1)} + s_{d2} = 0 \\ \sum_{j=1}^{k_b} a_{2,j} x_j + s_{d1} + s_{d2} + s_{d3} = 0 \\ \sum_{j=1}^{k_b} a_{3,j} x_j + s_{d3} + s_{d4} = 0 \\ \sum_{j=1}^{k_b} a_{4,j} x_j + s_{d1}^{(1)} + s_{d4} = 0 \end{cases} \tag{1.17}$$

where $s_{d1}^{(l)}$ denotes the $l-th$ right circulant shifted of s_{d1} for $0 \leq l \leq Z$. Solving the set of equations above, we obtain:

$$\begin{cases} s_{d1} = \sum_{i=1}^{4} \phi_i \\ s_{d2} = \phi_1 + s_{d1} \\ s_{d3} = \phi_2 + s_{d2} \\ s_{d4} = \phi_3 + s_{d3} \end{cases} \text{, where } \phi_i = \sum_{j=1}^{k_b} a_{i,j} x_j;\ i = 1, 2, 3, 4 \tag{1.18}$$

Step 3: The elements of the vector $\mathbf{s_e}$ can now be calculated based on the equation 1.16 (**) and the value of the elements of the vector $\mathbf{s_d}$ above. They are:

$$s_{ei} = \sum_{j=1}^{k_b} e_{i,j} x_j + \sum_{j=1}^{4} c_{i,k_b} + j s_{dj}, i = 1, 2, ..., m_b - 4 \tag{1.19}$$

1.2.1.5 5G QC-LDPC Decoding Process

In the 5G LDPC decoding process, the Sum-Product Algorithm (SPA) [96, 97] with an efficient message passing schedule will be used, where the check node c_i and the symbol node f_j send message that carry their guesses of code word bits to each other until it reaches the maximum number of interactions. Let Q_{fc} be the message that passes from a symbol node f to a check node c , while R_{cf} is the message that passes from c to f and $p_f(0)$ and $p_f(1)$ is the probability that the transmitted bit f is zero and one, respectively. Let C and F denote the sets of check nodes and symbol nodes, respectively. The Log-Likelihood-Ratio (LLR) can be applied to reduce the complexity because the SPA uses a lot of multiplications and the LLR can replace it by summation in the log-domain. The decoding process can be described in the following main steps:

Initialization step:

The symbol nodes f are initialized with the received bits from the output of the demodulator and then send the first iteration's input message to the check nodes c connected to them. Let denote $P_f = \log \frac{p_f(0)}{p_f(1)}$. The messages from the symbol nodes to the check nodes in the belief propagation are:

$$\mathbf{Q}_{fc} \leftarrow P_f + \sum_{c' \in S(f) \backslash c} R_{c'f} \tag{1.20}$$

where $S(.)$ is the set of neighbor nodes in the graph with all symbol nodes c' connected to the check node f except c.

Horizontal step:

The check node c is calculated to process the messages that came from the symbol nodes. Then it replies the new messages back to the symbol node as the equation:

$$R_{cf} \leftarrow 2\tanh^{-1}\left(\prod_{f' \in U(c) \backslash f} \tanh(\frac{Q_{f'c}}{2})\right) \tag{1.21}$$

In the log-domain, it can be rewritten as:

$$R_{cf} \leftarrow \varphi^{-1}\left(\sum_{f' \in U(c) \backslash f} \varphi(Q_{f'c})\right), \tag{1.22}$$

where $\varphi(x) = (sign(x), -\log\tanh(\frac{|x|}{2}))$, and $\varphi^{-1}(sign, x) = (-1)^{sign} \times -\log\tanh(\frac{|x|}{2})$.

Vertical step:

This step is present at the symbol nodes. It is used to process the messages coming from the check nodes and to calculate the reply messages back. So, each symbol node f can be obtained by the following:

$$Q_f \leftarrow P_f + \sum_{c \in U(f)} R_{cf} \tag{1.23}$$

Decision step:

When the maximum number of iterations is achieved, it will go to the decision step by apply the hard decision to the possible value of the symbol code. It is 1 if its log-likelihood value is less than 0 and 0 otherwise. Based on [96], the computation and memory of the decoding step can be reduced by using Q_f and R_{cf} to compute the Q_{fc} message on the fly. Let us substitute equation 1.20 to equation 1.22, we get the updating formula for the incoming and outgoing messages from a check node c:

$$R_{cf}^{new} = \varphi^{-1}\left(\sum_{f' \in U(c) \setminus f} \varphi(Q_f - R_{cf'})\right) \tag{1.24}$$

$$Q_f^{new} = Q_f^{old} - R_{cf}^{old} + R_{cf}^{new} \tag{1.25}$$

In summary, the 5G QC-LDPC decoding in this thesis is described in Algorithm 1.2.

Algorithm 1.2: 5G QC-LDPC Decoding Process

Inputs : c, f
Outputs : Q_f
Initialization: for all $f \in \mathbf{F}, c \in \mathbf{C}$, $R_{cf} \leftarrow 0$,
for all $f \in \mathbf{F}$, $Q_f \leftarrow P_f$
Iteration :
for all $c \in \mathbf{C}$
$T \leftarrow \sum_{f \in U(c)} \varphi(Q_f - R_{cf})$
for all $f \in U(c)$
$Q_{temp} \leftarrow Q_f - R_{cf}$
$R_{cf} \leftarrow \varphi^{-1}(T - \varphi(Q_{temp}))$
$Q_f \leftarrow Q_{temp} + R_{cf}$
end
end
Returns : Q_f

The next subsection will present the encoding and decoding processes of 5G Polar Codes.

1.2.2 5G Polar Codes

Polar codes are a class of linear block code introduced by Arikan in 2009 [85]. It focuses on a new phenomenon called as "channel polarization" and has attracted the attention of researcher to implement as the channel correcting schemes on the 5G standard in recent years. As the result, the 3GPP chose Polar codes as a possible channel coding scheme for the 5G network because it can achieve the capacity of symmetric channels. According to the 3GPP project document [80], 5G Polar codes are applied as channel coding for the uplink channel and the downlink channel of the 5G NR network. In uplink channel, it is used to encode the Uplink Control Information (UCI) channel over the Physical Uplink Control Channel (PUCCH) and the Physical Uplink Shared Channel (PUSCH). In the downlink channel, the 5G Polar codes are also considered as the coding scheme for the Downlink Control Information (DCI) channel of the Physical Downlink Control Channel (PDCCH) and the payload in the Physical Broadcast Channel (PBCH). In this section, we will introduce the fundamental concepts of the channel polarization, code design, encoding, and decoding process of 5G Polar codes.

1.2.2.1 Channel Polarization

Channel polarization phenomenon was first highlighted by Arikan in [85] as a method of combining numerous N identical copies of a Binary-input Discrete Memory Channel (B-DMC) to obtain a N synthetic bits channel for improving the capacity. Then, the mutual information of this channel tends towards 0 (completely noisy channels) or towards 1 (perfectly noiseless channels) based on the size of N. Let us consider matrix $\mathbf{G}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ is the basic polarization kernel of Polar codes. The code word $\mathbf{c} = [c_0, c_1]$ was encoded by a two bits input vector $\mathbf{u} = [u_0, u_1]$ and the matrix $\mathbf{G}_2$ as $\mathbf{c} = \mathbf{u}\mathbf{G}_2$, where $c_0 = u_0 \oplus u_1$ and $c_1 = u_1$ as presented in Fig 1.11.

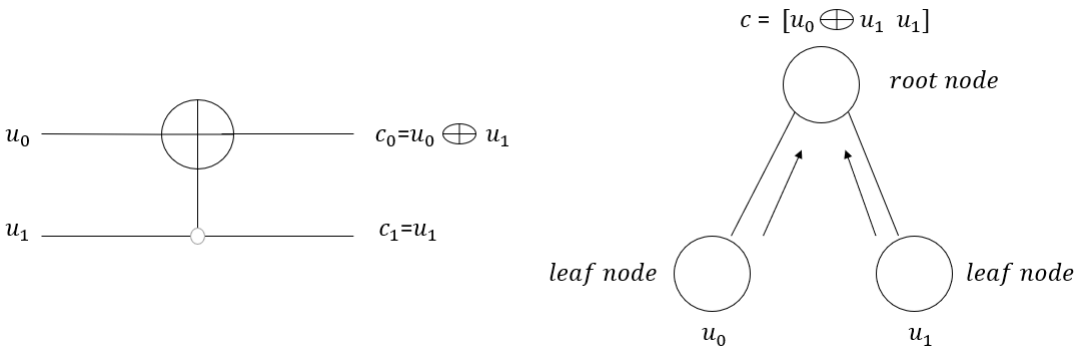


Fig. 1.11: Basic polarization kernel $\mathbf{G_2}$ and binary tree representation.

Polar codes are based on the concatenation of several basic polarization kernels. The general form of the channel transformation matrix is defined as $\mathbf{G}_N = \mathbf{G}_2^{\otimes n_{polar}}$ with

$n_{polar} = log_2(N)$, which is the Kronecker product of $\mathbf{G}_2$, and can be calculated as $\mathbf{G}_N = \begin{bmatrix} \mathbf{G}_{N/2} & 0 \\ \mathbf{G}_{N/2} & \mathbf{G}_{N/2} \end{bmatrix}$. For example,

$$\mathbf{G}_4 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} \mathbf{G}_2 & 0 \\ \mathbf{G}_2 & \mathbf{G}_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix},$$

$$G_8 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{1.26}$$

Let us define the length of the Polar codes in the form $N = 2^{n_{polar}}$ and K is the number of information bits. 5G Polar codes support the maximum code length up to 1024 [98]. The code design of an (N, K) 5G Polar codes is to form the K best synthetic channels with the highest reliability to transmit the information bits. It will sort each channel in reliability order and assign K information bits to the most reliable channels. The remained $N - K$ channels are not carrying any information or called as frozen. A length-N code word $\mathbf{d}$ is generated as $\mathbf{d} = \mathbf{u}\mathbf{G}_N = \mathbf{u}{\mathbf{G}_2}^{\otimes n_{polar}}$. The details of 5G Polar encoder will be given in the next sections.

For example, let us consider the binary tree representation is shown in Fig. 1.12:

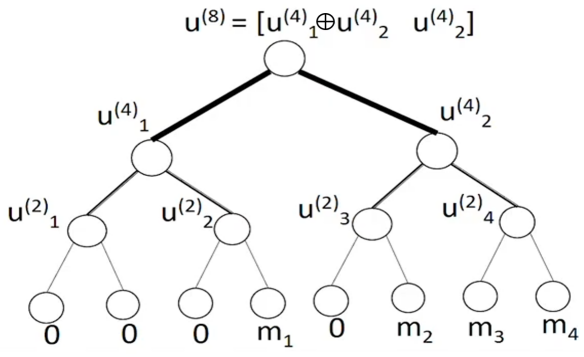


Fig. 1.12: Binary tree representation of (8,4) 5G Polar encoding.

- The (8,4) 5G Polar codes with the reliability bit channel sequence: 0 1 2 4 3 5 6 7;
- The frozen bit channel positions: 0 1 2 4;
- The information bit m_1, m_2, m_3, m_4 will be assigned to the channel position 3,5,6,7;

- By the binary tree representation, the code word after Polar code is

  $\mathbf{d} = [m_1 \oplus m_2 \oplus m_3 \oplus m_4, m_1 \oplus m_2 \oplus m_4, m_1 \oplus m_3 \oplus m_4, m_1 \oplus m_4, m_2 \ldots$

  $\oplus m_3 \oplus m_4, m_2 \oplus m_4, m_3 \oplus m_4, m_4]$.

1.2.2.2 Mother Polar Codes Length

In 5G network and its applications, the initial number of information bits K is given and is attached by V Cyclic Redundancy Check (CRC) bits to form a bit sequence $K' = K + V$. A code word length N' needs to be created in order to adapt the code rate $R = K'/N'$. To satisfy this requirement, a mother Polar code length N is built, which $N_{min} = 32$ and $N_{max} = 1024$ for uplink channel and $N_{max} = 512$ for downlink channel. The minimum value of the code rate is 1/8. The parameters of 2 types of channel in 5G are summarized in Table 1.3.

Table 1.3: Parameters of 2 kinds of channel in 5G

Parameter	**Uplink**		**Downlink**	
	K>20	12<K<19	**PDCCH**	**PBCH**
$N_{max}(n_{max})$	1024 (10)		512 (9)	
$N_{min}(n_{min})$	32 (5)			
Message length K_{max}	1706		140	32
Message length K_{min}	12		1	32
CRC length V	11	6	24	
Parity check bit n_{pc}	0	3	0	

The power n_{polar} of the mother Polar code length is chosen as the equation:

$$n_{polar} = \max(\min(n_1, n_2, n_{\max}), n_{\min}) \tag{1.27}$$

where n_{max} and n_{min} are given in Table 1.3. While n_2 is the upper bound on the code based on the minimum value of the code rate $R_{min} = 1/8$, which is $n_2 = \log_2(K'/R_{\min}) = \log_2(8K')$. Where n_1 is calculated based on:

$$n_1 = \begin{cases} \lceil \log_2(N') \rceil - 1 \text{if } N' \leq (\frac{9}{8}).2^{\lceil \log_2(N') \rceil - 1} \text{ and } \frac{K'}{N'} < \frac{9}{16} \\ \lceil \log_2(N') \rceil \quad \text{otherwise} \end{cases} \tag{1.28}$$

In the case of a length of message $K_{max} > N_{max}$, the message sequence will be divided into 2 small blocks and encoded independently as well as transmitted simultaneously. If K is even, the message is separated into 2 blocks of length $K'' = K/2$. While K is odd, the first message sequence is the combination of the first $\lfloor K/2 \rfloor$ and a zero padding at the beginning [98]. It is active for the uplink channel because the message length in the

uplink channel can be higher than the maximum length of the mother Polar code. It can skip for the downlink channel because the message length in the downlink channel is always less than the length of the mother Polar codes.

1.2.2.3 Construction of 5G Polar Encoding Process

In this subsection, the construction of 5G Polar encoding process for downlink channel and uplink channel in 5G are shown in Fig 1.13. To adapt the code rate R before going to the upper communication layers, the rate matching and interleaving should be applied. We will describe in detail the function of each component in the diagram.

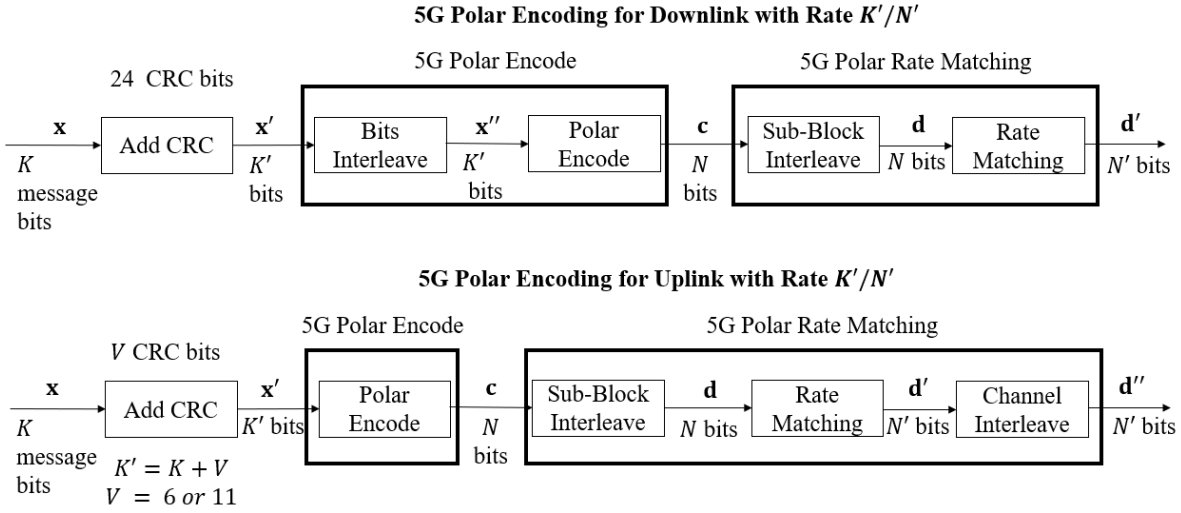


Fig. 1.13: 5G Polar encoding for Downlink/Uplink with rate K'/N'.

A. CRC Adding

In 5G Polar codes, the V CRC bits will be added to the K information bits to form the K' bits on the input of the Polar encoder. Based on [80], there are three possible CRC polynomials as follows:

$$\begin{aligned} CRC6(g) &= g^6 + g^5 + 1 \\ CRC11(g) &= g^{11} + g^{10} + g^9 + g^5 + 1 \\ CRC24(g) &= g^{24} + g^{23} + g^{21} + g^{20} + g^{17} + g^{15} + g^{13} + g^{12} + g^8 + g^4 + g^2 + g + 1 \end{aligned} \tag{1.29}$$

Let present the input information bit sequence as $\mathbf{x} = [x_0, x_1, ..., x_{K-1}]$ and the CRC check bit sequence as $\mathbf{v} = [v_0, v_1, ..., v_{V-1}]$, where K is the length of the input message and V is the number of CRC bits, respectively. The encoding process between $\mathbf{x}$ and $\mathbf{v}$ is carried out in a systematic form, which means that in GF(2), the polynomial:

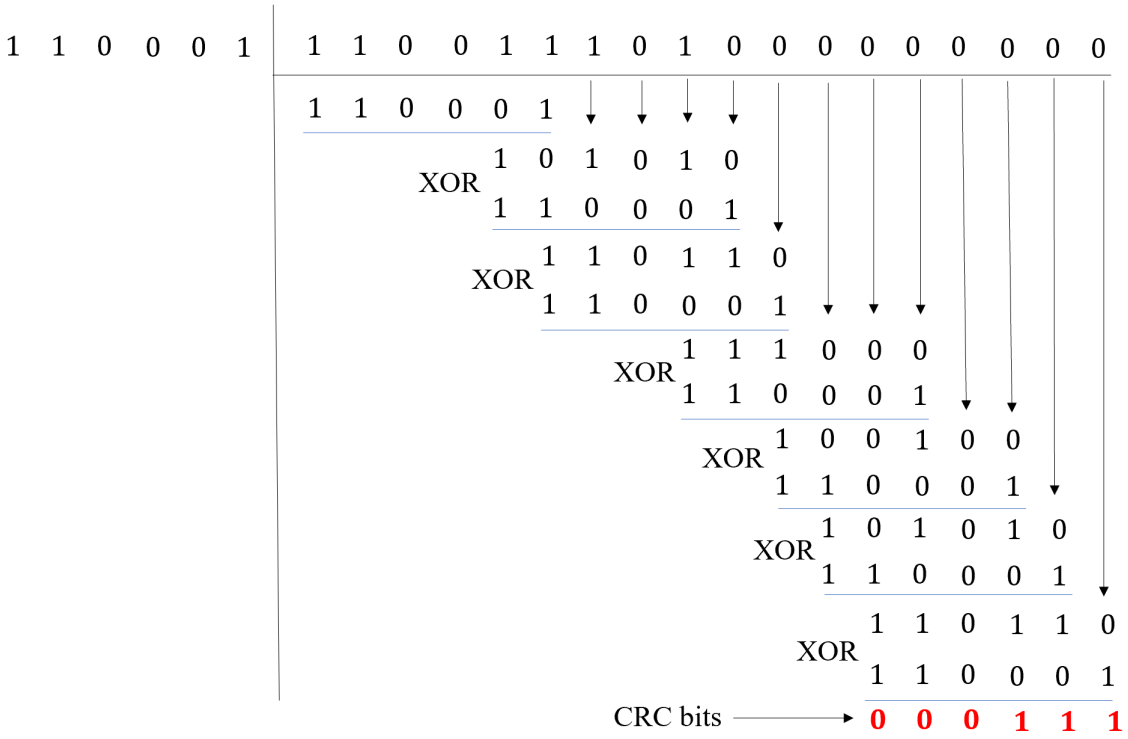
$$x_0 g^{K+V-1} + x_1 g^{K+V-2} + ... + x_{K-1} g^V + v_0 g^{V-1} + v_1 g^{V-2} + ... + v_{V-2} g^1 + v_{V-1} \tag{1.30}$$

yields a remainder equal to 0 when divided by the corresponding CRC generator polynomial. The total number of K' bits added to the input of the Polar encoder is denoted as $\mathbf{x}' = [x'_0, x'_1, ..., x'_{K'-1}]$, in which $K' = K + V$. The elements have the relationship as follows:

$$\begin{aligned} x'_i &= x_i \text{ for } i = 0, 1, 2, ..., K-1 \\ x'_i &= v_{i-K} \text{ for } i = K, K+1, K+2, ..., K+V-1 \end{aligned} \tag{1.31}$$

For example:

Let us consider $\mathbf{x} = [\ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ ]$ as the input information bit sequence and using the CRC polynomial $CRC6 = \left[\ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \right]$. We will find the CRC check bit sequence as $\mathbf{v} = [\ v_0\ \ v_1\ \ v_2\ \ v_3\ \ v_4\ \ v_5\ ]$ by attached 6 zero bits to the message and make a bit division in GF (2) as the following:



So we obtain the CRC check bit $\mathbf{v} = [\ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ ]$ and the input of Polar encoder is denoted as $\mathbf{x}' = [\ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ ]$ with the length of K' bits, which is corresponding to the polynomial presented in the equation (1.30).

B. Bits Interleaver

The bits interleaver is used to reduce the complexity of the decoding and reduce the computation of mobile devices [98]. It only applies to the downlink channel and bypasses for the uplink channel. In particular, the K' bits after the attachment of the CRC are presented as the sequence $\mathbf{x}' = [x'_0, x'_1, ..., x'_{K'-1}]$ and it is interleaved into the sequence

$\mathbf{x}'' = [x'_{\Pi(0)}, x'_{\Pi(1)}, x'_{\Pi(2)}, ..., x'_{\Pi(K'-1)}]$ where $\Pi(k)$ for $k = 0, 1, ..., K' - 1$ is determined by using Algorithm 1.3. According to [80], the maximum number of interleaver is $K_{IL}^{\max} = 164$ and the interleaving pattern sequence $\Pi_{IL}^{\max}$ is also given in Table 1.4. It is also noticed that the last bit is not interleaved to keep the majority of CRC bits at the end of the message [98].

Algorithm 1.3: Determine the Interleaver Pattern $\Pi(k)$

Inputs : $\Pi_{IL}^{max}, K_{IL}^{max}, K'$;
Outputs : $\Pi(k)$;
Initialization: $k = 0$;
for $m = 0$ *to* $K_{IL}^{max} - 1$ **do**
  if $\Pi_{IL}^{max}(m) > K_{IL}^{max} - K'$ **then**
    $\Pi(k) = \Pi_{IL}^{max}(m) - (K_{IL}^{max} - K')$;
    $k = k + 1$;
  else
    Go to Return;
  end
end
return $\Pi(k)$;

Table 1.4: Interleaving pattern sequence $\Pi_{IL}^{\max}(m)$, copy right © 2018 3GPP [80]

m	$\Pi_{IL}^{\max}(m)$	m	$\Pi_{IL}^{\max}(m)$	m	$\Pi_{IL}^{\max}(m)$	m	$\Pi_{IL}^{\max}(m)$	m	$\Pi_{IL}^{\max}(m)$	m	$\Pi_{IL}^{\max}(m)$
0	0	28	67	56	122	84	68	112	33	140	38
1	2	29	69	57	123	85	73	113	36	141	144
2	4	30	70	58	126	86	78	114	44	142	39
3	7	31	71	59	127	87	84	115	47	143	145
4	9	32	72	60	129	88	90	116	64	144	40
5	14	33	76	61	132	89	92	117	74	145	146
6	19	34	77	62	134	90	94	118	79	146	41
7	20	35	81	63	138	91	96	119	85	147	147
8	24	36	82	64	139	92	99	120	97	148	148
9	25	37	83	65	140	93	102	121	100	149	149
10	26	38	87	66	1	94	105	122	103	150	150
11	28	39	88	67	3	95	107	123	117	151	151
12	31	40	89	68	5	96	109	124	125	152	152
13	34	41	91	69	8	97	112	125	131	153	153
14	42	42	93	70	10	98	114	126	136	154	154
15	45	43	95	71	15	99	116	127	142	155	155
16	49	44	98	72	21	100	121	128	12	156	156
17	50	45	101	73	27	101	124	129	17	157	157
18	51	46	104	74	29	102	128	130	23	158	158
19	53	47	106	75	32	103	130	131	37	159	159
20	54	48	108	76	35	104	133	132	48	160	160
21	56	49	110	77	43	105	135	133	75	161	161
22	58	50	111	78	46	106	141	134	80	162	162
23	59	51	113	79	52	107	6	135	86	163	163
24	61	52	115	80	55	108	11	136	137		
25	62	53	118	81	57	109	16	137	143		
26	65	54	119	82	60	110	22	138	13		
27	66	55	120	83	63	111	30	139	18		

C. Polar Encoder

In this step, a vector $\mathbf{x}' = [x'_0, x'_1, x'_2, ..., x'_{K'-1}]$ which is received after CRC attachment of the uplink channel or a vector $\mathbf{x}'' = [x''_0, x''_1, x''_2, ..., x''_{K'-1}]$ which is obtained after the bits interleaver process of the downlink channel will be expanded to the vector $\mathbf{u} = [u_0, u_1, ..., u_{N-1}]$ with the addition of parity check bits n_{PC} and frozen bit. The n_{PC} bits (only used for the uplink channel, as shown in Table 1.3) are concatenated with the K' message and CRC bits to form $K'' = K' + n_{PC}$ bits.

The 3GPP project in [80] introduced the technique to present the reliability of the channel in sequence. In particular, the channel reliability order is calculated according to the Polar channel sequence $\mathbf{Q}_0^{N_{\max}-1} = \{\mathbf{Q}_0^{N_{\max}}, \mathbf{Q}_1^{N_{\max}}, ..., \mathbf{Q}_{N_{\max}-1}^{N_{\max}}\}$, where $0 \leq Q_0^{N_{\max}} \leq N_{\max}$ denotes a bit index before Polar encoding for $i = 0, 1, ..., N_{\max}-1$ and $N_{max} = 1024$ in 5G. Let's denote $W(Q_i^{N_{\max}})$ is the reliability of bit index, the ascending order of reliability in the Polar sequence if present as $W(Q_0^{N_{\max}}) < W(Q_1^{N_{\max}}) < ... < W(Q_{N_{\max}-1}^{N_{\max}})$. For smaller Polar codes length N bits, a sequence $\mathbf{Q}_0^{N-1}$ is derived from the sequence for N_{max}, which is arranged in ascending order of reliability $W(Q_0^N) < W(Q_1^N) < ... < W(Q_{N-1}^N)$. The Polar sequence $\mathbf{Q}_0^{N_{\max}-1}$ and its corresponding reliability $W(Q_i^{N_{\max}})$ are given in Table 5.3.1.2-1 of [80].

Let us denote $\bar{Q}_I^N$ as the set of information bits, $\bar{Q}_F^N$ as the set of frozen bits and Q_{PC}^N as the set of parity check bits, where $Q_{PC}^N \subset \bar{Q}_I^N$. Based on the reliability sequence $\mathbf{Q}_0^{N_{\max}-1}$, the K'' best synthetic channels with the highest reliability to transmit the information bits and parity check bits. The remained $N - K''$ channels are frozen. The mechanism for assigning K'' information bits and parity check bits to $\mathbf{u}$ is presented in Algorithm 1.4. As a result, a length-N code word $\mathbf{c}$ is generated as $\mathbf{c} = \mathbf{u}\mathbf{G}_N = \mathbf{u}\mathbf{G}_2^{\otimes n_{polar}}$, where $n_{polar} = \log_2 N$. The encoding process is performed in GF(2).

D. Sub-block Interleaver

Before going to the rate matching, the N encoded bits of $\mathbf{c} = [c_0, c_1, ..., c_{N-1}]$ pass through the sub-block interleaver S, which separated the N encoded bits into 32 sub-blocks of length $J = \lfloor N/32 \rfloor$. The output $\mathbf{d} = [d_0, d_1, ..., d_{N-1}]$ is generated as the Algorithm 1.5 and the graphical demonstration when assuming $N = 32$ is presented in Fig. 1.14, where the sub-block interleaver pattern $P_{sub}(i)$ is given in Table 1.5.

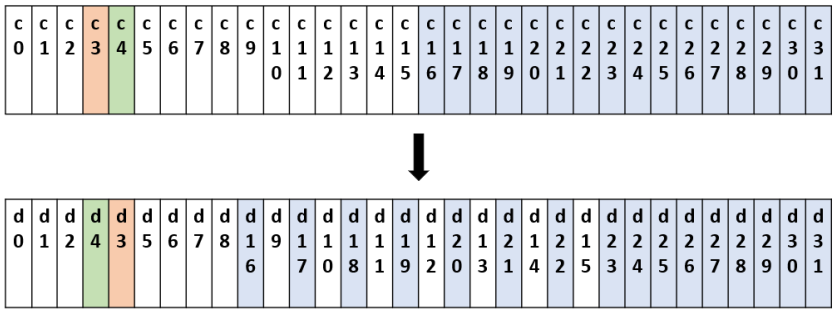


Fig. 1.14: Graphical presentation of sub-block interleaving process.

Algorithm 1.4: Generate $u = [u_0, u_1, \ldots, u_{N-1}]$

Inputs : $n_{PC}, \bar{Q}_I^N, \bar{Q}_F^N, Q_{PC}^N$;
Outputs : $u = [u_0, u_1, \ldots, u_{N-1}]$;
Initialization: $k = 0$;

if $n_{PC} > 0$ **then**
  /* Parity check bits available */
  $m_0 = 0; m_1 = 0; m_2 = 0; m_3 = 0; m_4 = 0$;
  for $n = 0$ *to* $N - 1$ **do**
    $m_z = m_0; m_0 = m_1; m_1 = m_2; m_2 = m_3; m_3 = m_4; m_4 = m_z$;
    if $n \in \bar{Q}_I^N$ **then**
      if $n \in Q_{PC}^N$ **then**
        $u_n = l_0$;
      else
        $u_n = x_k''$ for DL or $u_n = x_k'$ for UL;
        $k = k + 1$;
        $m_0 = m_0 \oplus u_n$;
      end
    else
      $u_n = 0$;
      /* Frozen */
    end
  end
else
  /* No parity check bits */
  for $n = 0$ *to* $N - 1$ **do**
    if $n \in \bar{Q}_I^N$ **then**
      $u_n = x_k''$ for DL or $u_n = x_k'$ for UL;
      $k = k + 1$;
    else
      $u_n = 0$;
      /* Frozen */
    end
  end
end
return $u = [u_0, u_1, \ldots, u_{N-1}]$.

Algorithm 1.5: Generate Interleaver Bits $\mathbf{d} = [d_0, d_1, \ldots, d_{N-1}]$;

Inputs : $\mathbf{c} = [c_0, c_1, \ldots, c_{N-1}]$;
Outputs : $\mathbf{d} = [d_0, d_1, \ldots, d_{N-1}]$;

for $n = 0$ *to* $N - 1$ **do**
  $i = \lfloor n/J \rfloor$;
  /* P_{sub} is based on Table 2.5 */
  $S(n) = P_{sub}(i)J + \mathrm{mod}(n, J)$;
  $d_n = c_{S(n)}$;
end
return $\mathbf{d} = [d_0, d_1, \ldots, d_{N-1}]$

Table 1.5: The sub-block interleaver pattern $P_{sub}(i)$

i	$P_{sub}(i)$	**i**	$P_{sub}(i)$	**i**	$P_{sub}(i)$	**i**	$P_{sub}(i)$
0	0	8	8	16	12	24	24
1	1	9	16	17	20	25	25
2	2	10	9	18	13	26	26
3	4	11	17	19	21	27	28
4	3	12	10	20	14	28	27
5	5	13	18	21	22	29	29
6	6	14	11	22	15	30	30
7	7	15	19	23	23	31	31

E. Rate matching

The rate matching process, including puncturing, shortening and repetition, is performed as a circular buffer with the input is the bit sequence $\mathbf{d} = [d_0, d_1, ..., d_{N-1}]$ from the sub-block interleaver. The bit selection output bit sequence $\mathbf{d}' = [d'_0, d'_1, ..., d'_{N'-1}]$ is generated as follows:

- Puncturing: The mother code with N bits is punctured when $N' \leq N$. In this case, the first $Z = N - N'$ bits are not transmitted, so the element $d'_i = d_{i+Z}$ for $i = 0, 1, ..., N' - 1$;
- Shortening: The mother code with N bits is shortening when $N' \leq N$ and $R > 7/16$. In this case, the last $Z = N - N'$ bits are not transmitted, so the element $d'_i = d_i$ for $i = 0, 1, ..., N' - 1$;
- Repetition: In this case, the length N' is larger than the mother code length N, so the first $Z = N - N'$ bits are transmitted twice, with $d'_i = d_{(i) \bmod (N)}$ for $i = 0, 1, ..., N' - 1$.

F. Channel Interleaver

Before going to the modulation process, the bit sequence $\mathbf{d}' = [d'_0, d'_1, ..., d'_{N'-1}]$ is interleaved using a triangular bit interleaver to improve the performance of the coding scheme for high-order modulation [98]. It only happens in the process of uplink channel, and bypasses in downlink channel. Let us denote Φ as the smallest integer such that $\Phi(\Phi + 1) \geq 2E$, and Φ can be calculated as $\Phi = \left\lceil \frac{\sqrt{8N'+1}-1}{2} \right\rceil$. An auxiliary $\Phi \times \Phi$ matrix $\mathbf{T}$ is created, and the channel vector $\mathbf{d}'' = [d''_1, d''_2, ..., d''_{N'-1}]$ is generated based on the matrix as the Algorithm 1.6.

1.2.2.4 Construction of 5G Polar Decoding Process

The flowchart of the 5G Polar decoding process is shown in the Fig. 1.15. In fact, the LLRs belief information with length N' received from the channel and the demodula-

Algorithm 1.6: Generate Channel Interleaver Bits $\mathbf{d}'' = [d''_0, d''_1, \ldots, d''_{N'-1}]$

Inputs : $\mathbf{d}' = [d'_0, d'_1, \ldots, d'_{N'-1}], \Phi$;
Outputs : $\mathbf{d}'' = [d''_0, d''_1, \ldots, d''_{N'-1}]$;
Initialization: $k = 0$;
for $i = 0$ *to* $\Phi - 1$ **do**
  for $j = 0$ *to* $\Phi - 1 - i$ **do**
    if $k < N'$ **then**
      $t_{i,j} = d'_k$;
    else
      $t_{i,j} = NULL$;
    end
    $k = k + 1$;
  end
end
Initialization: $k = 0$;
for $i = 0$ *to* $\Phi - 1 - j$ **do**
  for $j = 0$ *to* $\Phi - 1$ **do**
    if $t_{i,j} \# NULL$ **then**
      $d''_k = t_{i,j}$;
      $k = k + 1$;
    end
  end
end
return $\mathbf{d}'' = [d''_0, d''_1, \ldots, d''_{N'-1}]$

tion process will be passed through the rate recovery process to reconstruct the message sequence length N. The Successive Cancellation List Decoding with CRC Aided (SCLD-CA) decoder with the list of size M_{List} is implemented in 5G Polar codes [80, 98]. The idea is to produce a size M_{List} list of possible code words by working in parallel on a group of Successive Cancellation (SC) decoders, rather than producing a single code word. After that, based on the CRC attachment to the input, the decoder will estimate the input message signal. The details of 5G Polar decoder will present as follows:

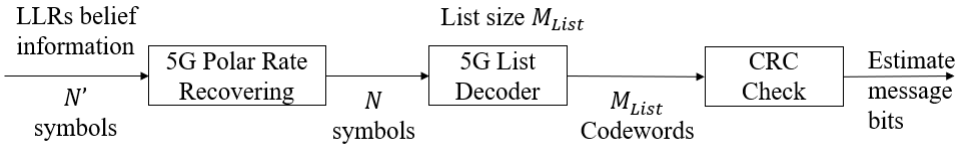


Fig. 1.15: 5G Polar decoding process.

A. 5G Polar rate recovering

The bit sequence $\mathbf{d}'' = [d''_0, d''_1, ..., d''_{N'-1}]$ which is received after the channel interleaver of uplink channel or the bit sequence $\mathbf{d}' = [d'_0, d'_1, ..., d'_{N'-1}]$ which is achieved by the rate matching process of downlink channel, will be modulated, i.e. using QPSK, and propagated over the wireless channel. At the receiver, the noisy signal is soft QPSK

demodulated to output LLR value sequence with length N'. The 5G Polar rate recovering is applied by using puncturing, shortening, or repetition processes as follows:

- For puncturing, the corresponding LLR values for the bits removed in rate matching step are set to zero;
- For shortening, the corresponding LLR values for the bits removed in rate matching step are set to a large value;
- For repetition, the set of LLR values corresponding to first N bits are selected.

Then, the recovery LLR values with the length N are decoded by the SCLD-CA decoder algorithm, which is described in details from the fundamental in the following steps.

B. Successive Cancellation Decoder

Firstly, we consider the basic decoding algorithm of 5G Polar codes, which is based on the Successive Cancellation (SC) process and was originally proposed in [85]. It can be described as a depth-first binary tree search with priority to the left side, where leaf nodes are the N bits to be estimated, and soft information on the received code bits is input at the root node. In this case, the frozen bits are always decoded to be 0 while the value of information bits can be reconstructed by using the hard decision on the soft information bit when a leaf node is reached. In general, the SC decoder for the (N, K) Polar codes can be presented into 3 steps as described in Fig. 1.16.

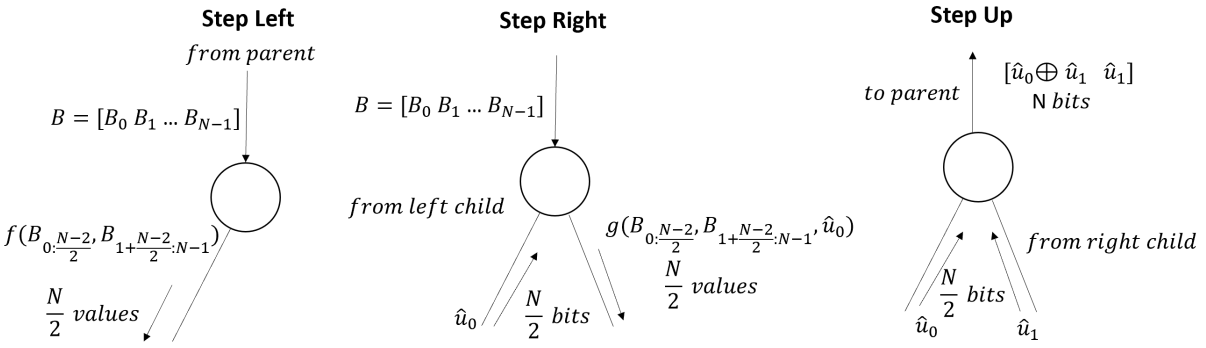


Fig. 1.16: Successive Cancellation decoder flowchart.

Step Left The node will receive the LLR belief information from its parent $\mathbf{B} = \{B_0, B_1, \dots, B_{N-1}\}$ and calculate the min-sum function f for the information to its left child:

$$f(\mathbf{a}_{0:N-1}, \mathbf{b}_{0:N-1}) = [f(a_0, b_0), f(a_2, b_2), ..., f(a_{N-1}, b_{N-1})] \tag{1.32}$$

where $f(a, b) = \text{sgn}(a)\text{sgn}(b)\min(|a|, |b|)$.

Step Right The node receives the hard decision estimated bit $\hat{u}_0$ from its left child

and calculate the g function for the information to its right child:

$$g(\mathbf{a}_{0:N-1}, \mathbf{b}_{0:N-1}, \mathbf{e}) = [g(a_0, b_0, e_0), g(a_1, b_1, e_1), ..., g(a_{N-1}, b_{N-1}, e_{N-1})] \tag{1.33}$$

where $g(a, b, e) = b + (1 - 2e)a$ and $e \in (0, 1)$.

Step Up The node receives the hard decision estimated bit $\hat{u}_1$ from it right child and combines with the estimated bit $\hat{u}_0$ from its left child, it will recalculate the information to it parent by using the kernel product as the encoding step $[\hat{u}_0 \oplus \hat{u}_1 \ \hat{u}_1]$.

The sequence of operations of Polar decoders can be summarized as the following:

i. Start at root;

ii. Check if it is not leaf, do the following in sequence;

- Do step Left and go to the left child;
- When decision is received from left child, do step Right and go to the right child;
- When decision is received from right child, do step Up and go to parent.

iii. If leaf, make a decision and go to parent;

- If i is the frozen position $=>$ $\hat{u}_i = 0$;
- If i is the message position $=>$ $\hat{u}_i = 0$ when $B(u_i) \geq 0$ and $\hat{u}_i = 1$ when $B(u_i) < 0$.

For example: considering the sequence of operation of $(4, 1)$ Polar decoder as described in the flowchart in the Fig. 1.17. The $(4, 1)$ Polar decoder is done by the following step:

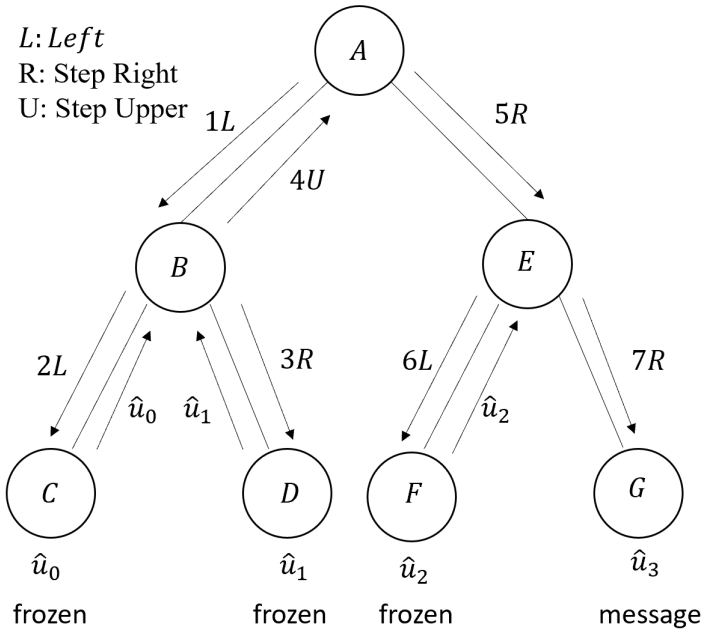


Fig. 1.17: Binary tree representation of $(4, 1)$ 5G Polar decoding

Step 1: The incoming LLR belief information comes from the channel to node A is given by $\mathbf{B}_0 = [\ 0.1 \quad 1.2 \quad -1.6 \quad 0.4]$. It is not leaf, so we do step "1L" by calculating the f function as the equation (1.32) and go to its left child node B.

1L: $\mathbf{B}_1 = [\ f(0.1, -1.6) \quad f(1.2, -0.4)] \ = [\ -0.1 \quad -0.4]$;

Step 2: At node B, it receives the incoming belief information $\mathbf{B}_1$ from node A. It is not a leaf, so we take step "2L" by calculating the function f and go to its left child C.

2L: $\mathbf{B}_2 = [f(-0.1, -0.4)] = 0.1$;

Step 3: At node C, it is a leaf and also is frozen, so $\hat{u}_0 = 0$ and goes to its parent node B.

Step 4: At node B, it receives the decision of its left child, so doing step "3R" by using the function g as the equation (1.33) with input are $\mathbf{B}_1$ and $\hat{u}_0 = 0$, and going to node D of its right child.

3R: $\mathbf{B}_3 = [g(-0.1, -0.4, 0)] = -0.5$;

Step 5: At node D, it is a leaf and also is frozen, so $\hat{u}_1 = 0$ and goes to its parent node B.

Step 6: At node B, it receives the decision from its right child, so does the step "4U".

4U: $\mathbf{B}_4 = [\ \hat{u}_0 \oplus \hat{u}_1 \quad \hat{u}_1\ ] = [\ 0 \quad 0]$;

Step 7: At node A, it receives the incoming belief information $\mathbf{B}_4$ from node B, so it will do step "5R" by using the g function with the input $\mathbf{B}_0$ and $\mathbf{B}_4$ and goes to its right child node E.

5R: $\mathbf{B}_5 = [\ g(0.1, -1.6, 0) \quad g(1.2, -0.4, 0)] = [\ -1.5 \quad 0.8]$;

Step 8: At node E, it is not a leaf, so we do the step Left "6L" by calculating the f function and go to its left child node F.

6L: $\mathbf{B}_6 = [f(-1.5, 0.8)] = -0.8$;

Step 9: At node F, it is a leaf and also is frozen, so $\hat{u}_2 = 0$ and goes to its parent node E.

Step 10: At node E again, it receives the decision from its left child so doing step Right "7R" by using g function with the input are $\mathbf{B}_5$ and $\hat{u}_2$,and go to its right child node G.

7R: $\mathbf{B}_7 = [g(-1.5, 0.8, 0)] = -0.7$;

Step 11: At node G, it is a leaf and not frozen. Therefore, we can determine the by using the belief information $\mathbf{B}_7$. Because $\mathbf{B}_7 < 0 => \hat{u}_3 = 1$.

Step 12: Finally, we obtain all the estimated bits $[\ \hat{u}_0 \quad \hat{u}_1 \quad \hat{u}_2 \quad \hat{u}_3] = [\ 0 \quad 0 \quad 0 \quad 1]$.

The SC can be considered an efficient technique in Polar decoder because it can achieve Shannon channel capability [85], and also has low complexity when implemented in hardware and software [99, 100]. However, its performance is still in lower error correction in comparison with other channel coding techniques [101]. Therefore, to improve performance, the authors in [101] introduced the new decoder method named Successive Cancellation List Decoding (SCLD).

C. Successive Cancellation List Decoder

The idea is to produce a size M_{List} list of possible code words by working in parallel on a group of SC decoders, instead of producing a single code word. When the leaf node is reached, the information bits will be considered in both possible values 0 and 1, which double the number of candidate code words. At the same time, Decision Metric (DM) is also assigned. If the leaf node is frozen, there is only one decision 0 for the estimate bit, but DM also needs to be assigned based on the value of the incoming LLR belief information. The estimation output and the assignation of DM in SCLD is summarized in Algorithm 1.7. Moreover, the Path Metric (PM) is also used to calculate the summation of the decision metrics DM on a path of SC decoder. When the number of paths is equal to the size of the list M_{List}, the SCLD will choose M_{List} paths with the lowest PM and ignore the other paths with a higher PM. Then, the decoder works in the same process until it reaches the final bit which need to estimate. At this state, there are M_{List} possible code words, the SCLD will choose the code word with the lowest PM values. The summary of SCLD process is described in Fig. 1.18.

Algorithm 1.7: Estimation output and assigning DM in SCLD

Inputs : $P_{LLR}(u_i)$ is the LLR belief information leaf node u_i;
Outputs : $\hat{u}_i, DM$;

if u_i *is not frozen* **then**
  if $P(u_i) \geq 0$ **then**
    $\begin{cases} \hat{u}_i = 0, DM = 0 \\ \hat{u}_i = 1, DM = |P_{LLR}(u_i)| \end{cases}$;
  else
    $\begin{cases} \hat{u}_i = 1, DM = 0 \\ \hat{u}_i = 0, DM = |P_{LLR}(u_i)| \end{cases}$;
  end
else
  /* u_i is frozen */
  $\hat{u}_i = 0$;
  if $P_{LLR}(u_i) \geq 0$ **then**
    $DM = 0$;
  else
    $DM = |P_{LLR}(u_i)|$
  end
end
return $\hat{u}_i, DM$

In Fig. 1.18, the SCLD needs to obtain the estimate code word $[\ \hat{u}_0 \quad \hat{u}_1 \quad ... \quad \hat{u}_{N-1}]$. Assuming that the first four bits are not frozen, the path metric PM is 0 at the beginning and the list size $M_{List} = 4$. The SC decoder process will be applied until it reaches the leaf node u_0. By using Algorithm 1.7, the decoder will consider in both values 0 and 1 for $\hat{u}_0$ and assign the DM metric to each path and update the path metric PM. The process is continued by using SC decoder for $\hat{u}_1$ and for $\hat{u}_2$. At the stage 4, there are 8 possible

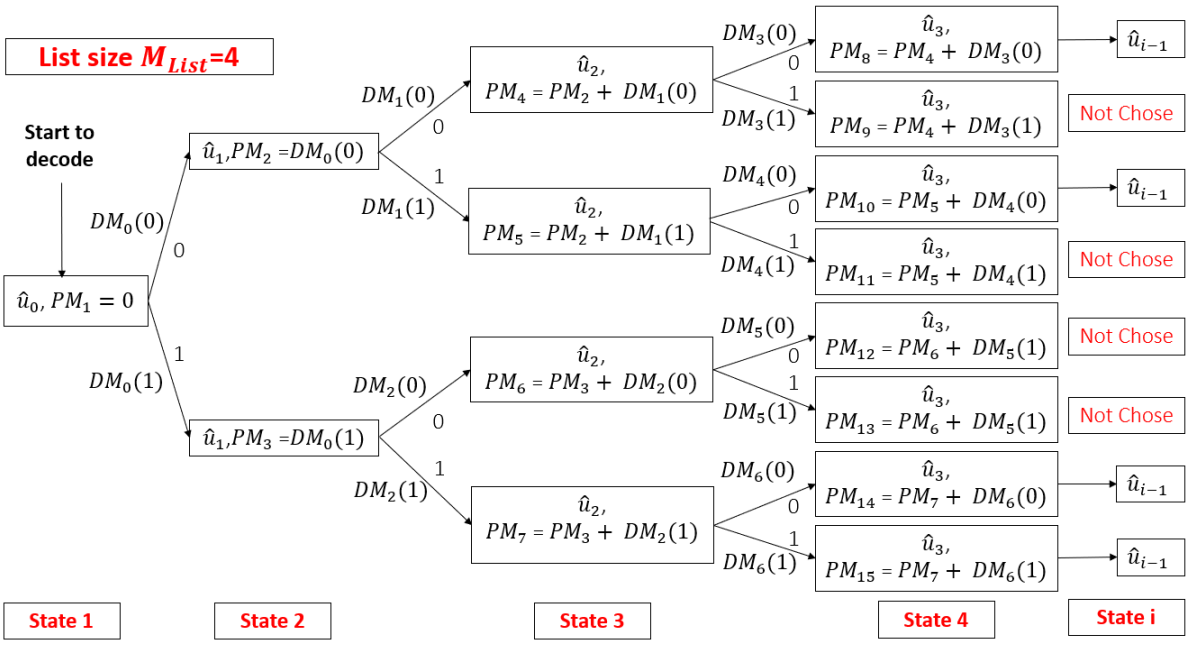


Fig. 1.18: Successive Cancellation List Decoding (SCLD) process.

paths, and they are over the list size M_{List}, so the SCLD will take only 4 paths with the lowest PM value (assuming that PM_8, PM_{10}, PM_{14} and PM_{15} have the lower value than others), and ignore the others' path. The process will continue until the bit u_{N-1} is estimated. At the stage i, there are 4 possible code words and the decoder will choose the path with the lowest PM value to be estimated code words $[\ \hat{u}_0 \quad \hat{u}_1 \quad ... \quad \hat{u}_{N-1}]$.

The SCLD process is discussed with a better performance of error correction in comparison with SC algorithm. However, to further improve performance, the authors in [102–104] introduced the new technique Successive Cancellation List Decoding with CRC Aided (SCLD-CA) by adding the assistant bits or the redundancy bits called CRC bits to the information bits.

D. Successive Cancellation List Decoding with CRC-Aided

In SCLD-CA, the decoding process is almost similar to that of the SCLD algorithm. The difference is only at the end of SCLD process. In fact, instead of relying on only the value of PM to determine the possible code word, the SCLD-CA process also checks the CRC bits. The estimated code word passing the CRC check will be determined as the estimate code word, otherwise, the decoder will choose the code word with the lowest value of PM if no one passes the CRC check. Elsewhere, if there are more than one code word satisfying the CRC check, the decoder also chose the candidate will the smallest PM.

According to [80, 81], the 3GPP project has chosen SCLD-CA as the fundamental decoder for the 5G Polar code, with a list size $M_{List} = 8$ and the CRC length is 6 or 11 for the uplink channel and 24 for the downlink channel.

1.2.3 LTE Turbo Codes

1.2.3.1 Construction of the LTE Turbo Encoding Process

In this section, the construction of the LTE Turbo encoding process for the downlink channel and the uplink channel in the LTE system is shown in Fig. 1.19. Because the LTE Turbo encoder provide the standard code rate 1/3. To adapt for any given code rate R before going to the upper communication layers, the rate matching should be applied. We will describe in detail the function of each component of the diagram.

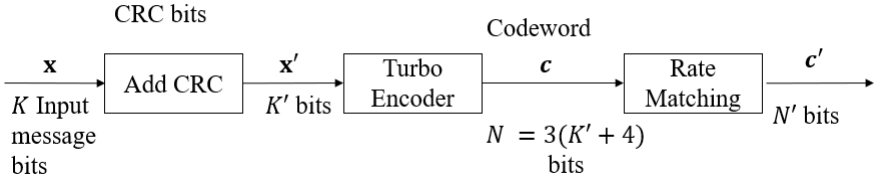


Fig. 1.19: LTE Turbo encoding process with rate K/N_{Turbo}.

A. CRC Adding

In LTE Turbo codes, the V CRC bits will be added to the K information bits to form K' bits to the input of the Turbo encoder. It also is used to detect the availability of any bit error at the end of each iteration in the turbo decoder to reduce computational complexity and boost the performance of the decoder. Based on [87], there are four possible CRC polynomials, such as the following:

$$\begin{aligned}
&CRC_8(g) = g^8 + g^7 + g^4 + g^3 + g + 1;\\
&CRC_{16}(g) = g^{16} + g^{12} + g^5 + 1;\\
&CRC_{24A}(g) = g^{24} + g^{23} + g^{18} + g^{17} + g^{14} + g^{11} + g^{10} + g^7 + g^6 + g^5 + g^4 + g^3 + g + 1;\\
&CRC_{24B}(g) = g^{24} + g^{23} + g^6 + g^5 + g + 1
\end{aligned} \tag{1.34}$$

Let present the input information bit sequence as $\mathbf{x} = [x_0, x_1, ..., x_{K-1}]$ and the CRC check bit sequence as $\mathbf{v} = [v_0, v_1, ..., v_{V-1}]$. The encoding between $\mathbf{x}$ and $\mathbf{v}$ is performed in a systematic form, which means that in GF(2), the polynomial:

$$x_0 g^{K+V-1} + x_1 g^{K+V-2} + ... + x_{K-1} g^V + v_0 g^{V-1} + v_1 g^{V-2} + ... + v_{V-2} g^1 + v_{V-1} \tag{1.35}$$

yields a remainder equal to 0 when divided by the corresponding CRC generator polynomial. The K' bits to the input of Turbo encoder is denoted as $\mathbf{x}' = [x'_0, x'_1, ..., x'_{K'-1}]$, in which $K' = K + V$ the elements x'_i and x_i have the relationship as:

$$\begin{aligned}
&x'_i = x_i \text{ for } i = 0, 1, 2, ..., K-1\\
&x'_i = v_{i-K} \text{ for } i = K, K+1, K+2, ..., K+V-1
\end{aligned} \tag{1.36}$$

B. LTE Turbo Encoder

In this step, a vector $\mathbf{x}' = [x'_0, x'_1, ..., x'_{K'-1}]$ received after CRC attachment process will be expanded to the vector $\mathbf{c}$ with the length of $N' = 3(K' + 4)$. This vector contains three streams $\mathbf{c}^{(i)} = [c_0, c_1, ..., c_{D-1}]$, where $i \in \{0, 1, 2\}$ and $D = K' + 4$. As shown in Fig. 1.20, LTE Turbo codes operate with the base rate of 1/3 as the standard of channel coding scheme. It operates based on the parallel concatenation of two 8-states convolution encoders and is separated by a Turbo interleaver. The first stream is the systematic bits while the second and the third streams are the outputs of the two convolution encoders, called Parity 1 and Parity 2 bit streams, respectively. At each encoder, the tail bits with length equal to 4 will be added to the end of each encoded information stream bit, so the length of each stream is $D = K' + 4$.

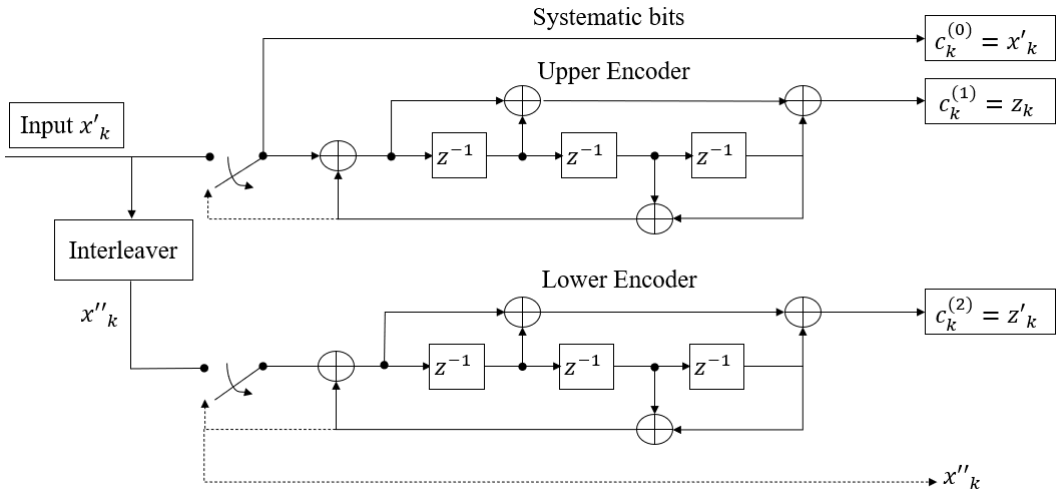


Fig. 1.20: LTE Turbo encoder.

C. Transfer Function

To construct an LTE Turbo encoder, we first need to specify the trellis structure of the constituent encoder based on the polynomial of the transfer function. The transfer function of the 8-state constituent code for the parallel concatenated convolution code is:

$$\Gamma(z) = \left[1, \frac{\Gamma_1(z)}{\Gamma_0(z)}\right] \tag{1.37}$$

where $\Gamma_0(z) = 1 + z^{-2} + z^{-3}$ is the polynomial for the feedback connection and $\Gamma_1(z) = 1 + z^{-1} + z^{-3}$ is the polynomial for the feed-forward connection. First of all, we build for the binary-number representation of the polynomials, for example (1011) for the feedback and (1101) for the feed-forward and convert them to an octal representation, which are 13 and 15, respectively. As a result, the LTE Turbo code diagram in Fig. 1.20 has a constraint length of 4, a generator polynomial matrix of [13 15] and the polynomial for the feedback connection of 13.

D. Interleaver

Another important parameter in LTE Turbo codes is the interleaver, which is based on a simple Quadratic Polynomial Permutation (QPP) scheme. Let take the input $\mathbf{x}' = [x'_0, x'_1, ..., x'_{K'-1}]$ into the interleaver and the output $\mathbf{x}'' = [x''_0, x''_1, ..., x''_{K'-1}]$ is obtained after permuting the indices of the input bits. The relationship between them is described as follows:

$$x''(i) = x'_{\epsilon(i)}, \quad i = 0, 1, ..., K' - 1 \tag{1.38}$$

where the relationship between the input index $\epsilon(i)$ and the output index i is presented in the following quadratic polynomial form:

$$\epsilon(i) = (f_1.i + f_2.i^2) \bmod (K') \tag{1.39}$$

where K' is the length of the information from the input block with 188 different values for the LTE system, f_1, f_2 are the constants that depend on the value of K', and the relationship between K', i, f_1, f_2 is summarized in Table 5.1.3-3 of [87].

E. Trellis Termination

The output from the encoder are $c_k^{(0)} = x'_k, c_k^{(1)} = z_k, c_k^{(2)} = z'_k$, where $k = 0, 1, ..., K'-1$. The trellis termination should be applied to these output streams to know the starting and ending states of the encoder on the decoder side to avoid loss of performance [105]. We take the tail bits from the shift register feedback when all information bits are encoded and multiplex them at the end of each stream encoding of information bits. In Fig. 1.20, when the upper switch in the lower position and the second encoder is disabled, the first three tail bits will be used to terminate the first constituent encoder. Vice versa, when the lower switch is turned off at the lower position and the first encoder is disabled, the last three tail bits will be used to terminate the second encoder [106]. The transmitted bits after trellis termination are then:

$$\begin{array}{l} c_{K'}^{(0)} = x'_K, c_{K'+1}^{(0)} = z_{K'+1}, c_{K'+2}^{(0)} = x''_{K'}, c_{K'+3}^{(0)} = z'_{K'+1} \\ c_{K'}^{(1)} = z'_K, c_{K'+1}^{(1)} = z_{K'+2}, c_{K'+2}^{(1)} = z'_{K'}, c_{K'+3}^{(1)} = x''_{K'+2} \\ c_{K'}^{(2)} = x'_{K'+1}, c_{K'+1}^{(2)} = z_{K'+2}, c_{K'+2}^{(2)} = x''_{K'+1}, u_{K'+3}^{(2)} = z'_{K'+2} \end{array} \tag{1.40}$$

F. Rate Matching

The rate matching process, including the subblock-interleaver, the bit collection, the bit selection, and puncturing, is an important feature in modern communication to adapt for various coding rate. In LTE channel coding with rate matching, let us start with the initial standard code rate 1/3. If the requested rate is less than 1/3, we do the repeating in Turbo code output bits. If the requested rate is greater than 1/3, bit puncturing is applied. The whole process is shown in Fig. 1.21.

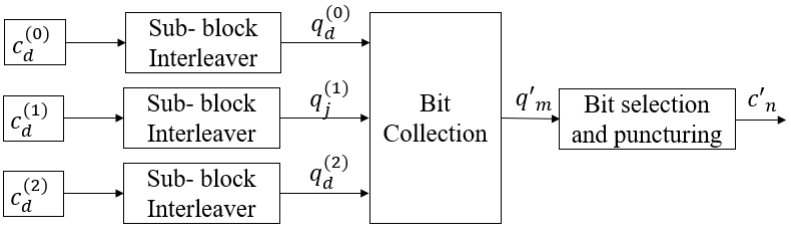


Fig. 1.21: LTE Turbo codes rate matching process.

a. Subblock- interleaver

In this step, we first subdivide each of the three streams into 32 bits sections and interleave each of these sections. Since each stream may be not divisible by 32, we add dummy bits to the beginning of the streams such that the obtaining vector can be divided into 32 bit sections. The bit sequence $\mathbf{c}_d^{(i)} = [c_0^{(i)}, c_1^{(i)}, ..., c_{D-1}^{(i)}]$, where $i \in \{0, 1, 2\}$, $d = 0, 1, 2, ..., D-1$ and $D = K' + 4$ from turbo encoder and trellis termination process will be interleaved by the subblock-interleaver to achieve the bit sequence $q_d^{(i)} = [q_0^{(i)}, q_1^{(i)}, ..., q_{D_\Pi - 1}^{(i)}]$, where D_Π is defined as follows [87]:

Step 1: Assign $C_{sub} = 32$ is the number of columns of the matrix;

Step 2: Determine the number of rows of the matrix R_{sub}, such that $D \leq R_{sub} \times C_{sub}$;

Step 3: If $R_{sub} \times C_{sub} > D$ then $N_D = R_{sub} \times C_{sub} - D$ dummy bits are padded such that: $s_d =< Null >$ for $d = 0, 1, ..., N_D - 1$. Then $s_{N_D + d} = c_d^{(i)}$ for $d = 0, 1, ..., D-1$, and the bit sequence y_d is written to the matrix $R_{sub} \times C_{sub} > D$ row by row, begin with bit s_0 in the position $(0, 0)$ as:

$$\begin{bmatrix} s_0 & s_1 & s_2 & \cdots & s_{C_{sub}-1} \\ s_{C_{sub}} & s_{C_{sub}+1} & s_{C_{sub}+2} & \cdots & s_{2C_{sub}-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{(R_{sub}-1)\times C_{sub}} & s_{(R_{sub}-1)\times C_{sub}+1} & s_{(R_{sub}-1)\times C_{sub}+2} & \cdots & s_{(R_{sub}\times C_{sub}-1)} \end{bmatrix}$$

In the next steps, we construct $c_d^{(0)}$, $c_d^{(1)}$ and $c_d^{(2)}$ as follows:

i. For $c_d^{(0)}$ and $c_d^{(1)}$:

Step 4: Based on the pattern $\Omega(j)$ where $j = 0, 1, ..., C_{sub} - 1$ in Table. 1.6, we perform the inter-column permutation for the matrix in which $\Omega(j)$ is the original column position of the $j - th$ permuted column. The inter-column permuted $R_{sub} \times C_{sub}$ matrix is:

$$\begin{bmatrix} s_{\Omega(0)} & s_{\Omega(1)} & s_{\Omega(2)} & \cdots & s_{\Omega(C_{sub}-1)} \\ s_{\Omega(0)+C_{sub}} & s_{\Omega(1)+C_{sub}} & s_{\Omega(2)+C_{sub}} & \cdots & s_{\Omega(C_{sub}-1)+C_{sub}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{\Omega(0)+(R_{sub}-1)\times C_{sub}} & s_{\Omega(1)+(R_{sub}-1)\times C_{sub}} & s_{\Omega(2)+(R_{sub}-1)\times C_{sub}} & \cdots & s_{\Omega(C_{sub}-1)+(R_{sub}-1)\times C_{sub}} \end{bmatrix}$$

Step 5: The bit sequence of the output of the subblock-interleaver is read out column

by column from the inter-column permuted $R_{sub} \times C_{sub}$ matrix and denote as $q_d^{(i)} = [q_0^{(i)}, q_1^{(i)}, ..., q_{D_\Pi-1}^{(i)}]$, where $q_d^{(i)} = [q_0^{(i)}, q_1^{(i)}, ..., q_{D_\Pi-1}^{(i)}] \ldots$ and $D_\Pi = R_{sub} \times C_{sub}$.

Table 1.6: Inter-column permutation pattern for sub-block interleaver

Number of columns C_{sub}	**Inter-column permutation pattern** $\Omega(0), \Omega(1), ..., \Omega(C_{sub}-1)$
32	0, 16, 8, 24, 4, 20, 12, 28, 2, 18, 10, 26, 6, 22, 14, 30, ... 1, 17, 9, 25, 5, 21, 13, 29, 3, 19, 11, 27, 7, 23, 15, 31

ii. For $c_d^{(2)}$:

Step 6: The bit sequence of the output of the subblock-interleaver, which is denoted as $q_d^{(2)} = [q_0^{(2)}, q_1^{(2)}, ..., q_{D_\Pi-1}^{(2)}]$, where $q_d^{(2)} = s_{\pi(d)}$ and $\pi(d)$, is calculated as:

$$\pi(d) = \left(P_{Turbo} \left(\left\lfloor \frac{d}{R_{sub}} \right\rfloor \right) + C_{sub} \left(d \bmod R_{sub} \right) + 1 \right) \bmod D_\Pi \tag{1.41}$$

The pattern P_{Turbo} is defined as Table. 1.6.

b. Bit collection, selection and puncturing

By using a circular buffer concept, the circular buffer of length $D_q = 3D_\Pi$ for a code block is generated as:

$$q'_d = q_d^{(1)} \quad for \quad d = 0, 1, ..., D_\Pi - 1;$$

$$q'_{D_\Pi+2d} = q_d^{(1)} \quad for \quad d = 0, 1, ..., D_\Pi - 1;$$

$$q'_{D_\Pi+2d+1} = q_d^{(2)} \quad for \quad d = 0, 1, ..., D_\Pi - 1;$$

Before going to the modulation process, by removing the dummy bits that adding in the previous step and the selecting the first few bits in the sequence, the new bit sequence $\mathbf{c}' = [c'_0, c'_1, ..., c'_{N'-1}]$ is produced by puncturing process to adapt for the desired coding rate.

1.2.3.2 Construction of LTE Turbo Decoding Process

The flowchart of the LTE Turbo decoding process is shown in Fig. 1.22.

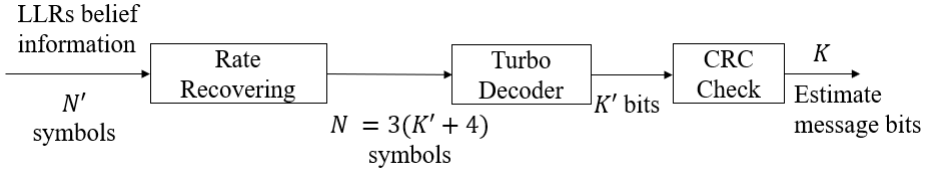


Fig. 1.22: LTE Turbo decoding process.

In this process, the LLR belief information contains N' symbols received from the

channel, and the demodulation process will pass through the rate recovery process to reconstruct the length of the message sequence N. The rate recovering process is performed as the inverse operations to those in the rate-matching process to obtain N' LLR samples to become inputs to the 1/3 turbo decoder. Based on the addition of trellis termination to the encoder, these samples will be decomposed into a systematic block and two parity blocks, where each block contains K' LLR samples. The Turbo decoder consists of two Soft-Input Soft-Output decoders and uses the Max-Log Maximum A Posteriori (Max-Log-MAP) algorithm [107]. After that, based on the CRC attachment to the input, the decoder will estimate the input message signal. At the end of each iteration, the code word that passes the CRC check will be determined as the estimated code word; otherwise, the decoder will continue the operations to achieve the maximum number of iterations and obtain the last estimated code word.

A. LTE Turbo Decoder

Fig. 1.23 shows the LTE Turbo decoder diagram, where we have two constituent decoders and two interleavers, two de-interleavers in the feed-forward and the feedback loop, respectively.

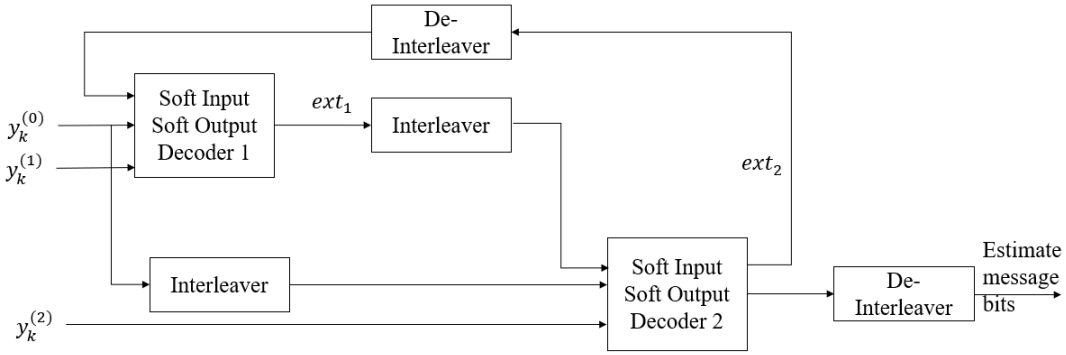


Fig. 1.23: LTE Turbo decoder.

The same trellis structure and interleaver as the encoder are used. First, the systematic symbols stream and the first parity symbols stream are added to the first decoder while the interleaver of the systematic symbols stream and the second-parity symbols stream are added to the second decoder. When starting the decoding process, the extrinsic information is generated by the first decoder, it is just a cleared-up version instead of the final LLR. Then the extrinsic information is interleaved and send to the second decoder. It combines with the interleaver of the systematic symbols stream and the second parity symbols stream to perform the second decoder. Similarly, it also generates extrinsic information and sends to the first decoder. But instead of interleaving, the de-interleaver is applied, and the iteration is done. In the next iteration, the first decoder performs the same process as the previous step, but at this moment, it has the extrinsic information obtained from the second decoder, so it will produce a more reliable output. The decoding

process continues until the CRC check process is passed or the maximum number of iterations is achieved. After any iteration, the total LLR is calculated as follows:

$$L_{y_k(total)} = L_{y_k(channel)} + L^{ext(2\to1)}_{y_{Deint(k)}} + L^{ext(1\to2)}_{y_{(k)}} \tag{1.42}$$

where $L_{y_k(channel)} = \log\left(\frac{P_r\{c_k=0|y_k\}}{P_r\{c_k=1|y_k\}}\right)$ is the LLR information received from the channel and after demodulation process, $ext(1 \to 2)$ is the extrinsic information from the first decoder to the second decoder, $ext(2 \to 1)$ is the extrinsic information from the second decoder to the first decoder, $Deint(k)$ is the de-interleaved position of c_k.

1.3 Conclusion

In conclusion, this chapter summarizes the state-of-the-art in SI cancelation processes, especially in the digital domain with the LMS and RLS algorithms. In fact, the RLS algorithm with $\lambda = 0.999$ gives a sufficient performance in DSIC process, so it will be used to implement in the following chapters. Then, the encoding and decoding processes of new radio channel coding schemes for 5G networks are also studied.

In the next chapter, we will investigate in the digital domain the channel coding schemes in case of SISO FD transmission to overcome the effects of residual SI and quantization noise in the cancelation process. Then, we illustrate the influence of quantization noise on DSIC process and compare the effects of SI channel power on the SISO FD transmission system with and without DSIC process.

Chapter 2

Full-Duplex Efficient Channel Codes for Residual Self-Interference/ Quantization Noise Cancellation

FD transmission systems are becoming very attractive techniques for 5G & beyond transmissions by offering higher spectral efficiency. The implementation of a real FD system can be a challenging task due to the analog and residual SI and some imperfections introduced by analog components such as quantization error of DAC/ADC processes. This chapter investigates in the digital domain different channel coding schemes to compensate the residual SI and quantization noise in the cancellation process in case of SISO FD transmission. The promising 3GPP channel coding schemes such as 5G QC-LDPC, 5G Polar Codes and LTE Turbo codes, which have been described in detail in Section 1.2, have been considered. Moreover, difference quantizer device architectures such as $\Sigma\Delta$, Gaussian with mid-rise, pipeline, and SAR are applied in the ADC process on the receiver side. Low-bit ADC quantizers with oversampling method are also considered for low cost, low power consumption and simple hardware devices, which are the characteristics of green communications and IoT applications [48]. Several numerical simulations are performed to evaluate the BER performance. The content of this chapter has been published in the following paper:

- Bao Quoc Vuong, Roland Gautier, Anthony Fiche and Mélanie Marazin, *"Full-Duplex Efficient Channel Codes for Residual Self-Interference/Quantization Noise Cancellation"*, in the proceeding of The IEEE 15th International Conference on Signal Processing and Communication Systems (ICSPCS), Sydney, Australia, 2021. (Online)

2.1 Introduction

In the future, the rapid growth of wireless and broadband communication requires higher spectral efficiency to account for the higher rate, lower latency transmission, and maintain a high level of security when we move toward the 5G standard. Due to the efficient use of resource and outstanding compared with traditional HD methods, FD transmission systems are widely used for many applications. However, the problem of SI phenomenon is the main challenge of FD transmission, which could be up to 120 dB in power when the system suffers from a strong SI environment [49]. Therefore, it is necessary to cancel the SI component to the noise floor level; otherwise, the spectral efficiency cannot be realized because of the high level of interference, especially in short-packet transmissions for IoT applications and green communications.

Moreover, quantization noise, which is produced by the quantization process performed by the DAC at the transmitter and the ADC at the receiver, is also a major factor affecting the performance of FD transmission systems [108]. The quantization bit resolution and the dynamic voltage range should be chosen carefully on the basis of the requirements of the sampling rate and the applications. Many DAC/ADC transceiver devices have been designed and launched out to the market for 4G, 5G and also IoT applications. For example, the LTC2000 DAC family [109] uses a quantization resolution of 11-16 bits for LTE MIMO and 5G transmissions at the transmitter. While at the receiver, the 12 bits $\Sigma\Delta$ AD9361 [110] is used in ADC process of 4G and 5G transmission. DAC/ADC process is an important part of any communication system, therefore, it is necessary to take into account the problem of residual quantization noise of DAC/ADC process in FD transmission.

So, in this chapter, we investigated in the digital domain the channel coding schemes in case of SISO FD transmission to overcome the effects of residual SI and quantization noise in the cancellation process. The remaining of this chapter is organized as follows. Section 2.2 briefly describes the model of SISO FD transmission system with new radio channel coding schemes, DSIC process, and DAC/ADC process. The simulation specifications and results are presented in Section 2.3. Finally, some highlight conclusions are given in Section 2.4.

2.2 SISO Full-duplex Transmission and Digital Self-Interference Cancellation Process

2.2.1 General System Model

The general SISO FD transmission model between two users A and B in the presence of the channel coding schemes, DSIC, and DAC/ADC processes is described in Fig. 2.1.

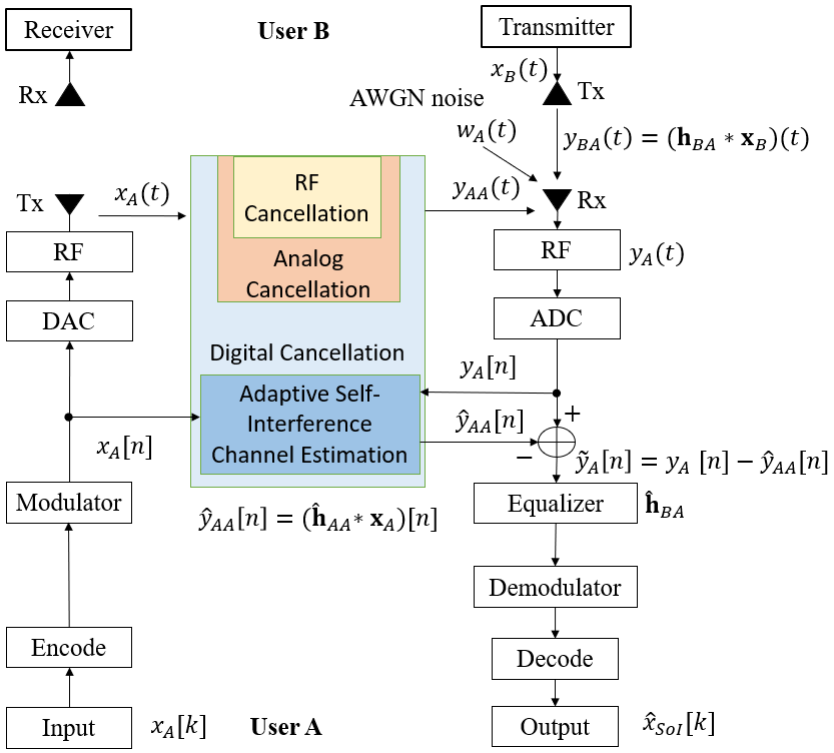


Fig. 2.1: SISO Full-Duplex transmission and SIC cancellation flowchart.

At the transmitter of user A, the digital input signal $x_A[k]$ is encoded by using three channel coding schemes proposed by 3GPP project such as 5G QC-LDPC codes, 5G Polar codes [80] and LTE Turbo codes [87] with CRC attachment and rate matching including bit shortening, bit puncturing or bit repeating should be applied to create a code word with length N [82, 87, 98]. These processes are described in details in Section 1.2. The encoded signal will then be modulated by using the QPSK modulator and transmitted through the DAC converter, which denotes as $x_A(t)$. Then it becomes an RF transmitting signal and is sent by transmitting antenna Tx to user B. We have the same process at the transmitter of user B to obtain the transmitting signal of interest $x_B(t)$ and it will be transmitted through the multipath fading channel environment with Additive White Gaussian Noise (AWGN) from the environment.

At the receiver of user A, the signal $y_A(t)$ consists of several signals, including the signal of interest $y_{BA}(t)$ of user B, the SI signal $y_{AA}(t)$ from the transmitter of user A, and the complex AWGN $w_A(t)$ with $\mathcal{CN}(0, {\sigma_A}^2)$. It can be given as:

$$\begin{aligned} y_A(t) &= y_{AA}(t) + y_{BA}(t) + w_A(t) \\ &= (\mathbf{h}_{AA} * \mathbf{x}_A)(t) + (\mathbf{h}_{BA} * \mathbf{x}_B)(t) + w_A(t) \end{aligned} \tag{2.1}$$

where $\mathbf{h}_{BA}$, $\mathbf{h}_{AA}$ are the channel gain of the intended fading channel and the SI channel with i.i.d. complex Gaussian random variables with $\mathcal{CN}(0, 1)$ [77, 111], respectively, and $(*)$ is the convolution operation. The SI channel is fixed with 3 taps under the assumption

that any LoS component is efficiently reduced by antenna isolation and the major effect comes from scattering. These channel models are independent in each transmission frame. The intended channel $\mathbf{h}_{BA}$ is modeled according to the ITU–R channel model [79].

The received signal will pass through the ADC process to convert to the discrete time domain, denoted by $y_A[n]$. Then, the reference transmitted signal $x_A[n]$ in the digital domain is used to cancel the SI component using the RLS algorithm, which is described in Section 1.1.3.2. As a result, we can effectively obtain the estimation of the SI channel $\hat{\mathbf{h}}_{AA}$. Therefore, the output signal can be expressed as follows:

$$\begin{aligned}\tilde{y}_A[n] &= y_A[n] - \hat{y}_{AA}[n] = y_{BA}[n] + y_{AA}[n] - \hat{y}_{AA}[n] + w_A[n] \\ &= (\mathbf{h}_{BA} * \mathbf{x}_B)[n] + (\mathbf{h}_{AA} * \mathbf{x}_A)[n] - (\hat{\mathbf{h}}_{AA} * \mathbf{x}_A)[n] + w_A[n] \end{aligned} \tag{2.2}$$

Then, the residual signal $\tilde{y}_A[n]$ will go to an equalizer with the RLS algorithm, which is similar to Section 1.1.3.2, to first estimate the intended channel and then reconstruct the intended signal of user B. After that, the equalized signal will pass through the demodulation block to obtain the LLR sequence. At the decoder, the LLR is used to reduce the calculation complexity by replacing a very large number of multiplications by summation in log-domain as in [97]. The LLR belief information received from the demodulation process will pass through the rate recovery process to reconstruct the message sequence of length N [82, 87, 98]. The SPA algorithm with an efficient message passing schedule [96], SCLD-CA [101] and Max-Log-MAP algorithm [107], which are described in detail in the previous chapter, are used in the decoding process for 5G LDPC codes, 5G Polar codes, and LTE Turbo codes, respectively. After that, based on the attachment of the CRC, the estimated signal of interest from user B $\hat{x}_{SoI}[k]$ is achieved.

2.2.2 DAC/ADC process

2.2.2.1 Analog-to-Digital Converter Quantization Noise

Although the majority of the SI component can be eliminated by the antenna isolation and analog cancellation techniques, the residual SI is still strong enough to influence the weak intended signal from the distant radio node. Furthermore, the ADC has a very limited dynamic range or quantization level Ψ which is defined as the ratio of the largest possible output $\mathcal{V}$ (full-scale voltage) to the quantization bit resolution $\mathcal{B}$, as shown in Fig. 2.2. In particular, upon the ADC, the dynamic range of the signal of interest is well below the dynamic range of the ADC, so it just takes a few bits of the ADC for quantization. However, the stronger residual SI occupies the whole dynamic range of the ADC, which is much greater than the signal of interest; therefore, it leads to the noisy in the signal of interest after digital SI cancellation. For example, considering the influence of ADC quantization for the case of without and with SI signal as shown in Fig 2.3. From

Fig. 2.3a, it can be seen that there is a minor effect on the reconstruction signal and the signal of interest quality remains well because there is no SI at the ADC input and the dynamic range of desired signal is belonged to the whole dynamic range of ADC. On the contrary, when SI occurs at the input of ADC as shown in Fig. 2.3b, the output of the signal of interest is very noisy, although the digital cancellation process is used to eliminate SI component. Therefore, in FD transmission, the dynamic range of ADC and the resolution of ADC should be carefully considered.

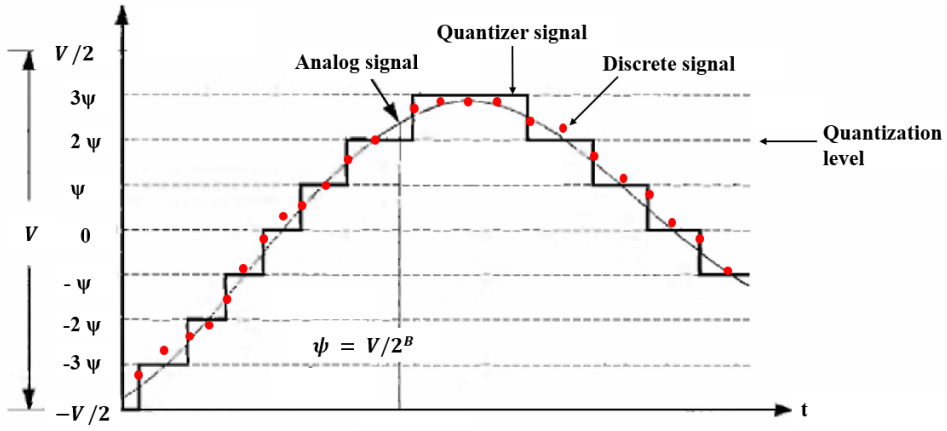
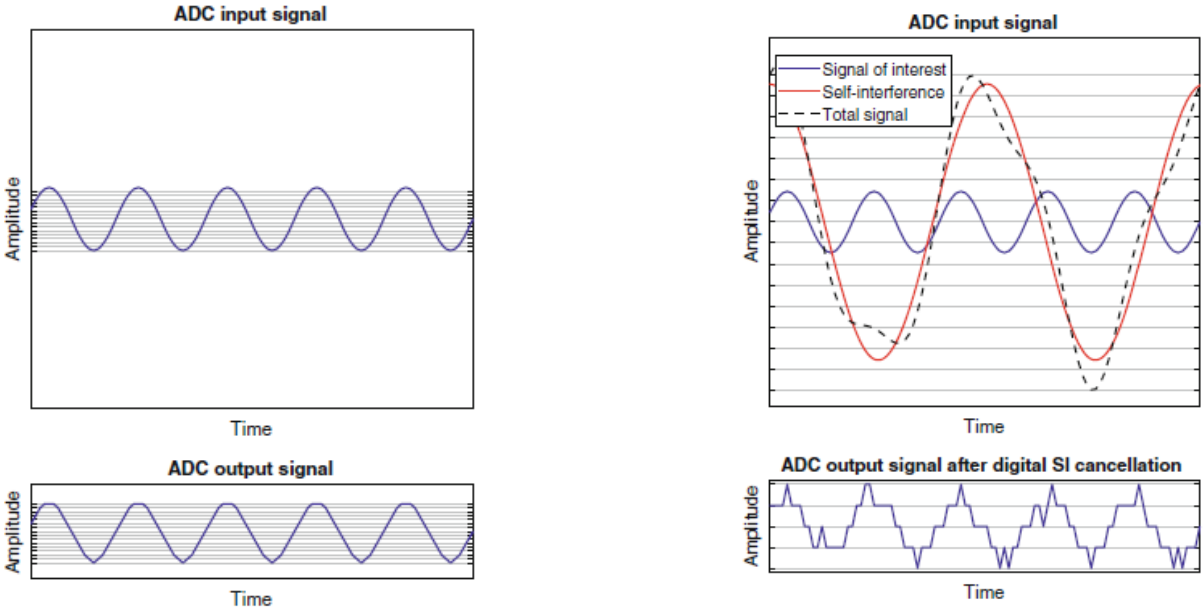


Fig. 2.2: Example of quantization level.



(a) Without SI

(b) With SI

Fig. 2.3: Effect of ADC quantization noise, Copyright © 2020 Springer Nature [112].

2.2.2.2 DAC Process at Transmitter

The DAC process at the transmitter is presented in Fig. 2.4. The QPSK symbols with double complex number will be separated into 2 separated components: In-phase and Quadrature, each component then passes independently through the up sample with

the factor m_{up} and then goes through DAC quantizer with the bit resolution $\mathcal{B}_{DAC}$, the dynamic voltage range $\mathcal{V}_{DAC}$ before going to the analog reconstructor [113] which is acted as a low pass filter with cutoff frequency $F_{cutoff} = F_S/2$, where F_s is the sampling rate, in order to convert these discrete values to the continuous values and send to the wireless fading environment.

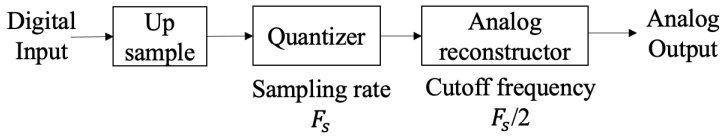


Fig. 2.4: DAC process.

2.2.2.3 ADC Process at Receiver

At the receiver as described in Fig. 2.5, the In-phase and Quadrature components that are received from the channel may pass through different types of ADC such as $\Sigma\Delta$, Gaussian with mid-rise, pipeline as well as SAR with the bit resolution $\mathcal{B}_{ADC}$ and the dynamic voltage range $\mathcal{V}_{ADC}$ in order to obtain the discrete time form. The oversampling method, with oversampling factor m_{over} and sampling rate F_s on the Nyquist interval $[-F_s/2; F_s/2]$, is also applied in order to reduce the effects of quantization noise in low bit quantization ADC [48]. Then, the signals go continuously to the digital/decimator filter. The output of these filters provides a digital representation of the quantized input signal. After that, these components will be mixed again to form the symbols with double complex numbers. Then these symbols will go through the SI channel estimation process to cancel the SI signal.

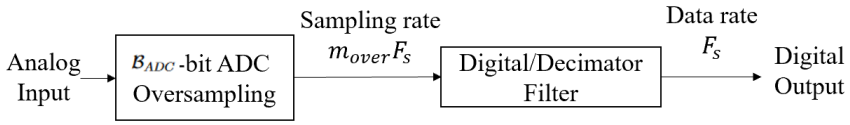


Fig. 2.5: ADC process.

2.3 Results And Discussions

2.3.1 Simulation Specifications

In this section, the BER performance for different testing scenarios is computed by using Monte Carlo simulation on MATLAB. First, we illustrate the influence of quantization noise to DSIC process and SI channel power to SISO FD transmission system. Then, the BER performance obtained with and without the DAC/ADC process will be illustrated by changing the quantization bit resolution at DAC/ADC process. Next, the performances of different quantizer device architectures in the receiver such as $\Sigma\Delta$ [53], Gaussian with midrise [54], pipeline [55] and Successive Approximation Registers ADC (SAR) [56] are evaluated. After that, a comparison between the system with and without

DAC/ADC for both case of HD and FD transmission for all channel coding schemes is considered. Finally, the choice of bit resolution for DAC/ADC process is also noticed. For the rest of this chapter, the system without DAC/ADC process is called the ideal case. For 5G LDPC codes, the base graph matrix **BG2** is implemented for all simulations. For 5G Polar codes, the SCLD-CA decoder technique with the list size $M_{List} = 8$ is used. Low-bit ADC quantizers with oversampling method are also considered for low cost, low power consumption and simple hardware devices, which are the characteristics of green communications and IoT applications [48]. Based on background noise as the reference, let us denote $\rho_{AA} = p_A/\sigma_A^2$ and $SNR_A = p_B/\sigma_A^2$ as the self-interference to noise ratio and signal-to-noise ratio, where p_A, p_B and σ_A^2 are the power of SI signal, intended signal and background noise, respectively. The information size is set at 512 bits, which is equal to 64 bytes and belongs to the maximum length of information in some IoT standards such as Long Range (LoRa) communication, where maximum size of information is 2048 bits, and equals to 256 bytes [28]. The simulation parameters are summarized in Table 2.1.

Table 2.1: Simulation Specifications

Parameter	**Value**
Code word block size (N)	1024 bits
Information size (K)	512 bits
Code rate (R)	1/2
Number of transmission frames	10^6
CRC length	11
5G LDPC codes base graph	**BG2**
5G Polar codes list size (M_{List})	8
Modulation scheme	QPSK
Up-sample factor (m_{up})	4
Oversampling factor (m_{over})	4
Sampling rate (F_s)	1 GHz
Quantization bit resolution of DAC/ADC ($\mathcal{B}_{DAC}, \mathcal{B}_{ADC}$)	1, 2, 3, 4, 6, 8, 12, 14
Dynamic voltage range of DAC ($\mathcal{V}_{DAC}$)	2 V
Dynamic voltage range of ADC ($\mathcal{V}_{ADC}$)	4 V
SI channel taps	3
Forget factor λ in RLS algorithm	0.999

2.3.2 Effect of Quantization Noise and SI Channel Power on SI Channel Estimation and BER Performance

First, we consider the impact of DAC/ADC quantization noise and self-interference to noise ratio ρ_{AA} on the channel SI estimation process for 5G QC-LDPC codes, 5G

Polar codes and LTE Turbo codes, as shown in Fig. 2.6 and Fig. 2.7, respectively. For DAC/ADC processes, the 14 bits DAC LTC2000 family [109] will be added at the transmitter side ($\mathcal{B}_{DAC} = 14$ bits) and the 12 bits $\Sigma\Delta$ AD9361 [110] will be used at the receiver side ($\mathcal{B}_{ADC} = 12$ bits). These parameters are chosen because they usually used in the DAC/ADC process for 4G and 5G transmissions [109, 110]. Throughout this thesis, the MSE of the SI channel and the intended channel are, respectively, given by [114]

$$\text{MSE}_{AA} = \|\mathbf{h}_{AA} - \hat{\mathbf{h}}_{AA}\|^2, \tag{2.3}$$

$$\text{MSE}_{BA} = \|\mathbf{h}_{BA} - \hat{\mathbf{h}}_{BA}\|^2. \tag{2.4}$$

Let us consider the SI channel estimation error of FD transmission with and without DAC/ADC using 5G QC-LDPC codes, as shown in Fig. 2.6. It can be observed that the presence of DAC/ADC quantization noise destroys from about 2 to 7 dB when self-interference to noise ratio (ρ_{AA}) varies from 0 to 30 dB, respectively, in comparison to the FD ideal case, which is the SISO FD transmission without using DAC/ADC processes. Therefore, the DAC/ADC quantization noise has a major effect on SI channel estimation in FD transmission systems.

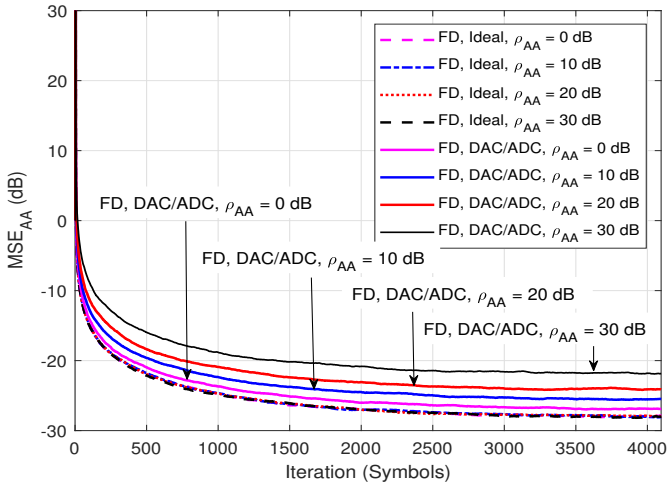
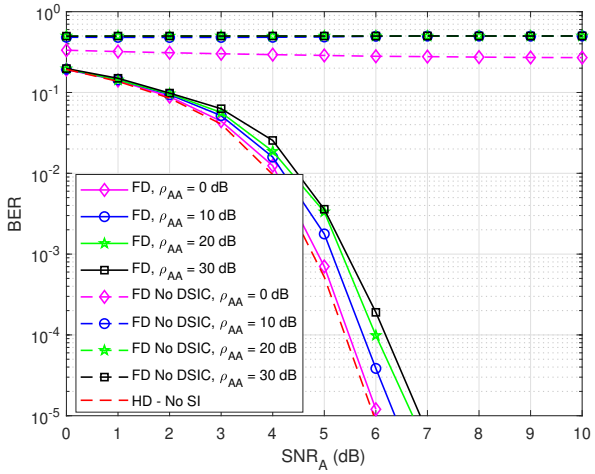


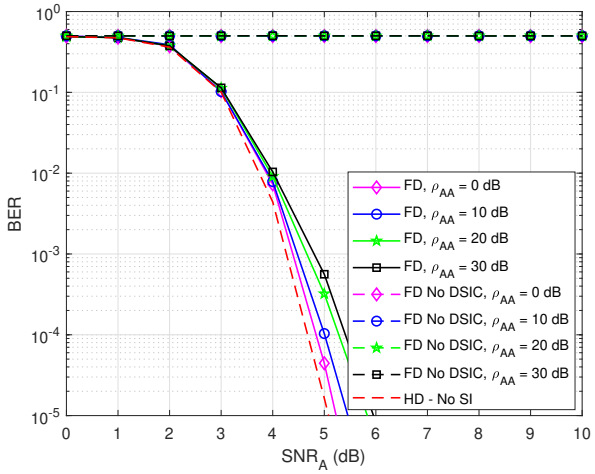
Fig. 2.6: SI channel estimation error of FD transmission with and without DAC/ADC process; $\mathcal{B}_{DAC} = 14$ bits, $\Sigma\Delta$ ADC with $\mathcal{B}_{ADC} = 12$ bits.

As shown in Fig. 2.7, the self-interference to noise ratio (ρ_{AA}) is also an important factor that affects the system performance for all channel coding schemes. Indeed, when ρ_{AA} increases, the BER performance will decrease. In the FD transmission with the DSIC process, when ρ_{AA} equal to 0 dB and 10 dB, the results are closed as the case of HD transmission. However, at a high value of ρ_{AA}, the SI component becomes dominant factor and the curves levels off at higher BER values, so the system needs more power in SNR to obtain the same result, i.e. when ρ_{AA} increases to 20 dB and 30 dB. In FD transmission without the DSIC process, the system cannot estimate and reconstruct again the transmission signal, regardless of channel coding schemes used. Therefore, it

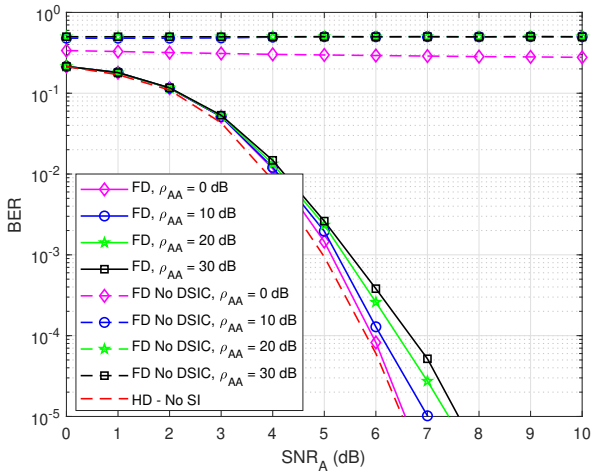
highlights the crucial role of DSIC process in FD transmission systems.



(a) 5G QC-LDPC



(b) 5G Polar



(c) LTE Turbo

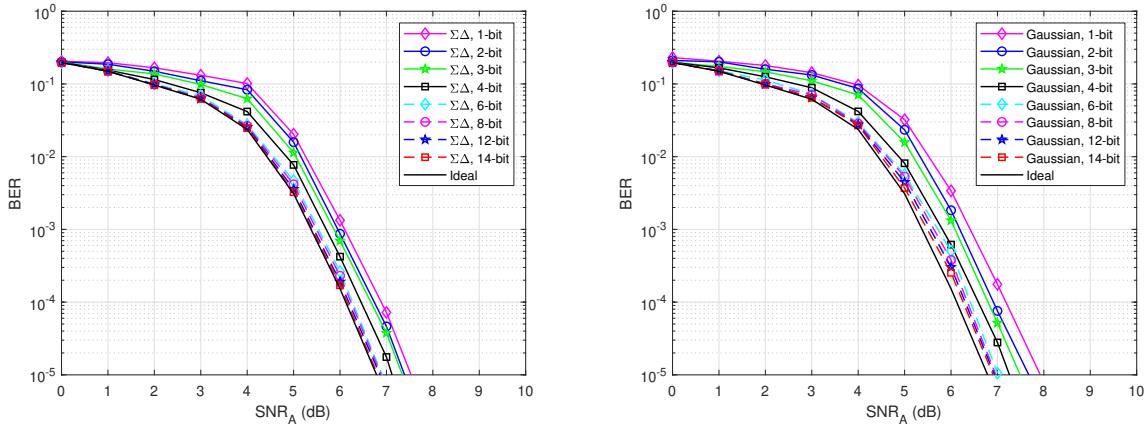
Fig. 2.7: BER of FD system with and without DSIC in different values of ρ_{AA}, $\mathcal{B}_{DAC} = 14$ bits, $\Sigma\Delta$ ADC with $\mathcal{B}_{ADC} = 12$ bits.

2.3.3 Effect of Bit Resolution of ADC on BER Performance

Then, Fig. 2.8 shows the BER performances of the FD system by changing the bit resolution $\mathcal{B}_{ADC}$ of 4 different types of ADC architectures such as $\Sigma\Delta$ [53], Gaussian with mid-rise [54], pipeline [55] and SAR ADC [56]. In this case, the oversampling factor is set at $m_{over} = 4$, which is a possible choice based on [48]. The 5G QC-LDPC channel coding scheme is used and $\mathcal{B}_{DAC} = 14$ bits according to LTC2000 family [109]. The self-interference power to noise ratio ρ_{AA} is fixed at 30 dB, which is the residual SI level that the DSIC process needs to cancel in order to approach the spectral efficiency in FD transmission. In general, we can see that the increase in bit resolution of ADC ($\mathcal{B}_{ADC}$) can improve the BER performance for all ADC architectures. Indeed, for high bit resolution values from 6 to 14 bits, the system can nearly approach the ideal case. However, with low-bit quantization from 1 to 4 bits ADC, the system needs more power (dB) in SNR to obtain the same BER result as in the ideal case. It is also noticed that the low-bit ADC has better performances and converges quickly to free error because oversampling method has been applied in ADC process. In fact, oversampling spreads the quantization noise in high frequency to reduce its effects. The gain between low-bit ADC and the ideal case is about 1 to 1.5 dB depending on ADC quantizer device architectures. Consequently, $\mathcal{B}_{ADC} = 6$ bits is a possible solution in the ADC process to reduce the impact of DAC/ADC quantization noise in FD transmission systems. In the next subsection, a comparison of different ADC architectures will be illustrated based on the BER performance.

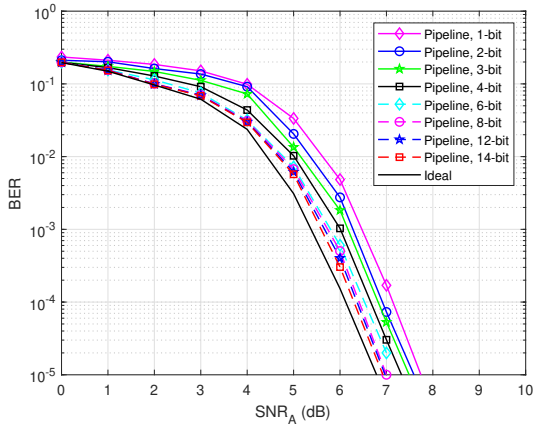
2.3.4 Effect of ADC Quantizer Device Architectures on BER Performance

The quality of system performances also depends on the choice of different types of ADC quantizer such as $\Sigma\Delta$, Gaussian with mid-rise, pipeline as well as SAR. In this case, the bit resolution of the DAC is set at $\mathcal{B}_{DAC} = 14$ bits according to the LTC2000 family [109], while the bit resolution of the ADC is chosen at $\mathcal{B}_{ADC} = 12$ bits for all ADC architectures. The self-interference power to noise ratio is fixed at 30 dB ($\rho_{AA} = 30$ dB). In general, for all channel coding schemes, the system can approximately reach the BER value of the ideal case for all types of ADC quantizer as illustrated in Fig. 2.9. In particular, the $\Sigma\Delta$ seems to give the best result because the larger value of over-sampling factor, i.e, $m_{over} = 4$ will give the better achievement in $\Sigma\Delta$ quantizer when compared with other ADC quantizer devices architectures, which has been proved in [48]. It again confirms the practical application of the 12 bits $\Sigma\Delta$ ADC in 5G transmission systems, according to $\Sigma\Delta$ AD9361 [110]. Therefore, $\Sigma\Delta$ ADC with $\mathcal{B}_{ADC} = 12$ bits is chosen to further implement in this chapter.

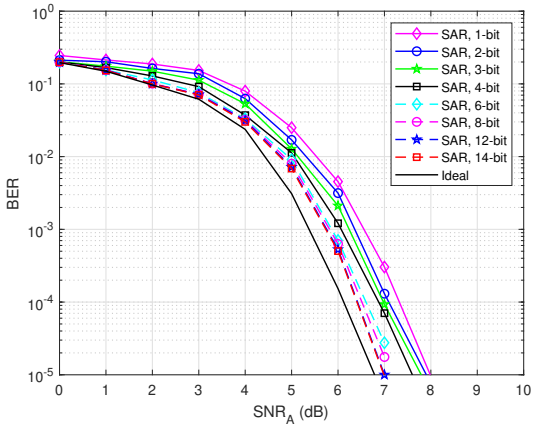


(a) ΣΔ.

(b) Gaussian with mid-rise.



(c) Pipeline

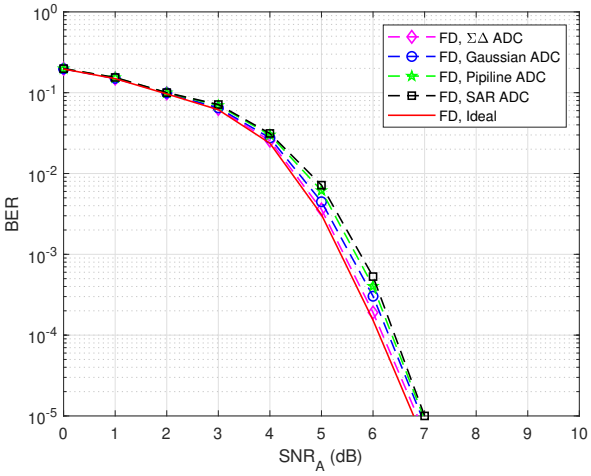


(d) SAR

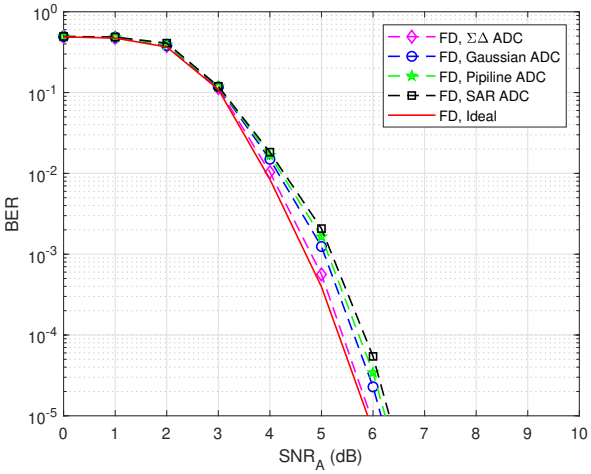
Fig. 2.8: BER of FD transmission by changing $\mathcal{B}_{ADC}$ for different ADC architectures, $\mathcal{B}_{DAC} = 14$ bits and $\rho_{AA} = 30$ dB.

2.3.5 Effect of Bit Resolution of DAC on BER Performance

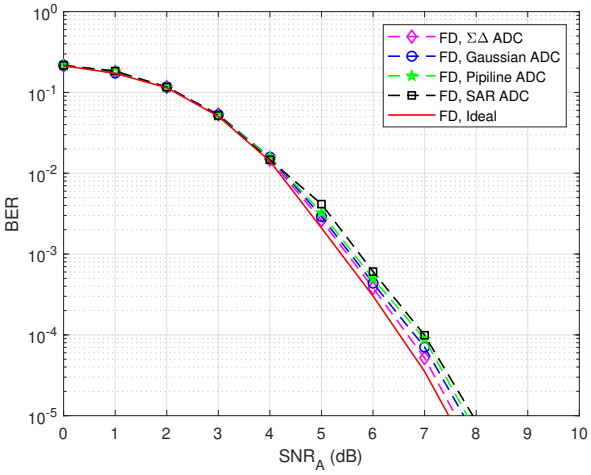
Next, the BER performance of the FD system is calculated by changing the bit resolution $\mathcal{B}_{DAC}$ of the DAC for all channel coding schemes. While the 12 bits ΣΔ ADC according to ΣΔ AD9361 [110] will be set at the receiver side. The oversampling method is also used with an oversampling factor $m_{over} = 4$. The SI power to noise ratio ρ_{AA} is set at 30 dB. Based on the results in Fig. 2.10, we can observe that the quantization bit resolution of the DAC significantly affects the system performance. The decrease in bit resolution $\mathcal{B}_{DAC}$ leads to a decrease in BER performance. For example, the values of $\mathcal{B}_{DAC}$ from 1 to 4 bits show the worst results compared to the others. On the contrary, when the values of B_{DAC} go to 6 bits and further, the system will obtain saturation and reach almost the ideal case. Therefore, $\mathcal{B}_{DAC} = 6$ bits is also a sufficient solution in DAC process to reduce the impact of DAC/ADC quantization noise in FD transmission systems.



(a) 5G QC-LDPC

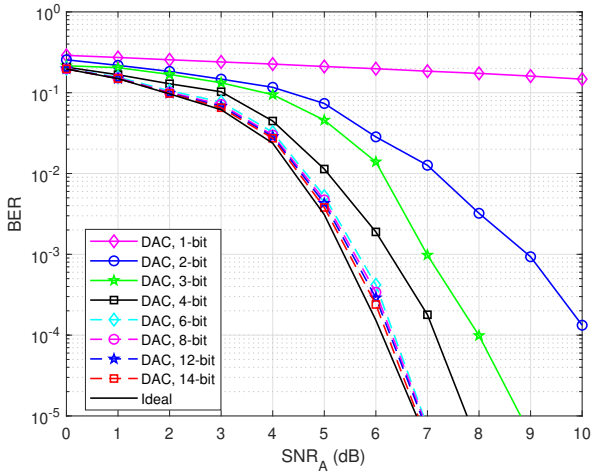


(b) 5G Polar

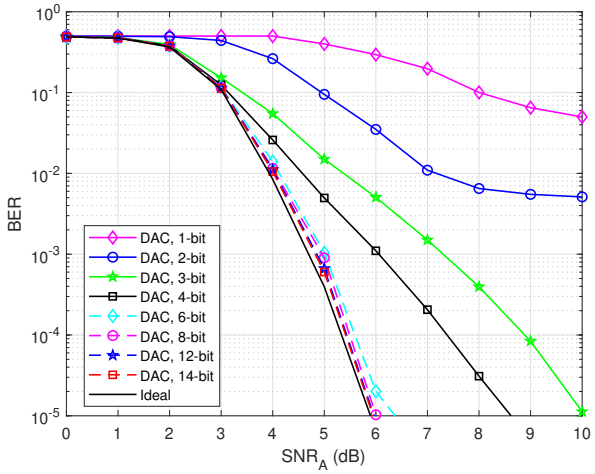


(c) LTE Turbo

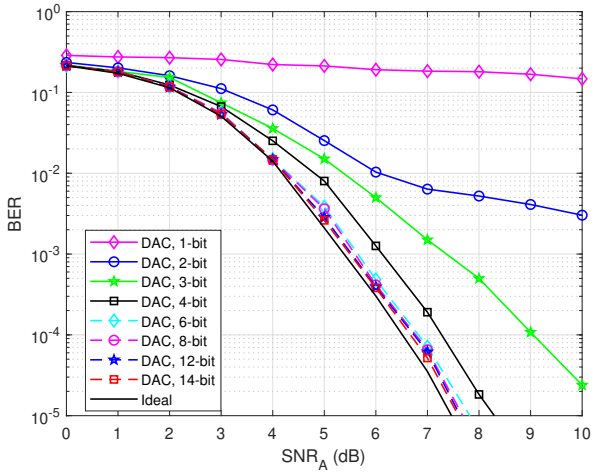
Fig. 2.9: BER of FD transmission with different types of ADC quantizer, $\mathcal{B}_{DAC} = 14$ bits, $\mathcal{B}_{ADC} = 12$ bits, $\rho_{AA} = 30$ dB.



(a) 5G QC-LDPC

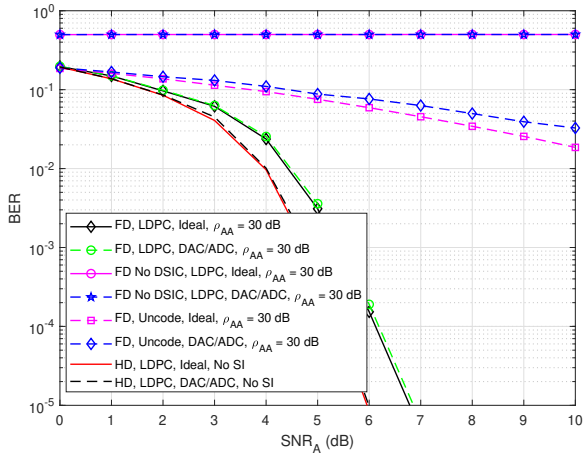


(b) 5G Polar

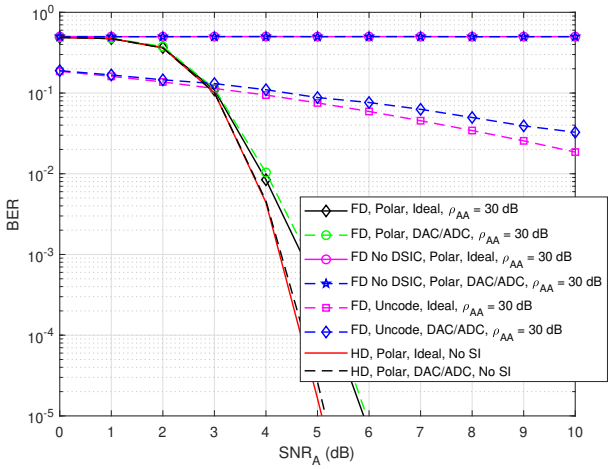


(c) LTE Turbo

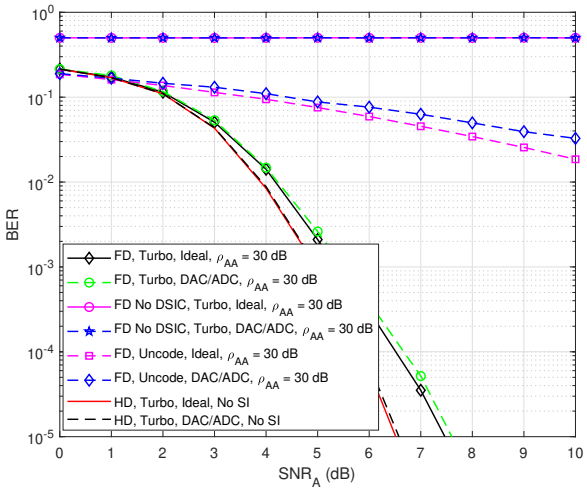
Fig. 2.10: BER of FD transmission by changing $\mathcal{B}_{DAC}$, $\Sigma\Delta$ ADC with $\mathcal{B}_{ADC} = 12$ bits, $\rho_{AA} = 30$ dB.



(a) 5G QC-LDPC

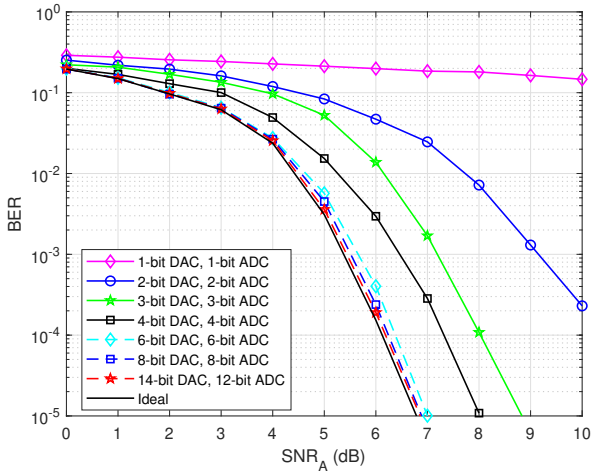


(b) 5G Polar

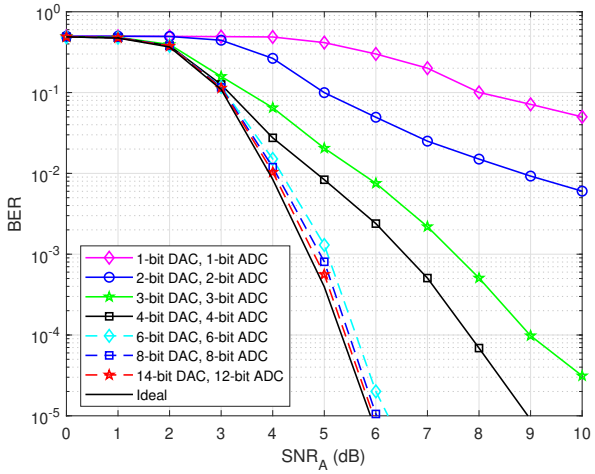


(c) LTE Turbo

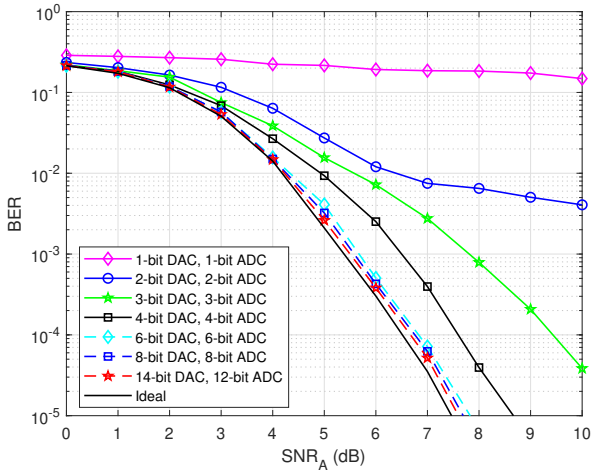
Fig. 2.11: Comparison between the FD system with and without DAC/ADC processes, $\mathcal{B}_{DAC} = 14$ bits, $\Sigma\Delta$ ADC with $\mathcal{B}_{ADC} = 12$ bits.



(a) 5G QC-LDPC



(b) 5G Polar



(c) LTE Turbo

Fig. 2.12: BER of FD system with different bit resolution in DAC/ADC, $\Sigma\Delta$ ADC, $\rho_{AA} = 30$ dB, $m_{over} = 4$.

2.3.6 Effect of Channel Coding Schemes in FD Transmission on BER Performance

The effect of residual SI and quantization noise to the SI channel estimation process has been pointed out in Section 2.3.2. To overcome this problem, channel coding schemes have been considered in FD transmission systems. In this case, the bit resolution of the DAC is set to $\mathcal{B}_{DAC} = 14$ bits, while the bit resolution of the ADC is chosen at $\mathcal{B}_{ADC} = 12$ bits. The SI power to noise ratio ρ_{AA} is set at 30 dB. In particular, Fig. 2.11 shows how channel coding schemes improve BER performance in the FD transmission system. It shows an interesting result where the system with channel coding can reconstruct well the information signal, and it can approximately reach to the curve of ideal case. In contrast, in the case of FD transmission without using channel coding schemes, the gap between the curves of ideal case and the curves of DAC/ADC case are larger and can be clearly observed with the increase of SNR. In HD transmission, the difference between ideal case and DAC/ADC case is less efficient, the system can estimate the information signal well because the SI interference does not happen. In contrast, considering the system performance in FD transmission without DSIC process, it cannot estimate the input information when the SI interference is not cancelled by DSIC process regardless of channel coding schemes used. Consequently, it can be concluded that the channel coding schemes play an important role in the performance of FD transmission, it can compensate the influences of residual SI and quantization noise in the DAC/ADC process. Among these coding techniques, 5G Polar codes go faster to free error floor and provide better performances in the high region of SNR, but they need more than 3 dB in low SNR to go below the curve of the uncoding system. While the LTE Turbo codes give quite the worst result than others by slowly convergence to error floor. Therefore, the 5G QC-LDPC codes seem to give a sufficient result in both low and high regions of the SNR and achieve better performance in general than the uncoding system.

2.3.7 Effect of Choosing Bit Resolution of DAC/ADC on BER Performance

Last but not least, the bit resolution in both the DAC and ADC processes is reduced to propose a trade-off in choosing the appropriate bit resolution for a real communication system, as shown in Fig. 2.12. In this case, the SI power to noise ratio ρ_{AA} is set at 30 dB, the oversampling factor is also fixed at $m_{over} = 4$ and the $\Sigma\Delta$ ADC is used. For all coding schemes, when the bit resolution in DAC/ADC process goes larger than 6 bits, the BER curves can nearly achieve to the ideal case. However, when the bit resolution reduces to 4 bits or smaller, it notices that the bit resolution strongly affects to the system performance. Therefore, combined with Sections 2.3.3 and 2.3.5, the bit

resolution should be carefully chosen depending on the applications. It is necessary to select the bit resolution of the DAC/ADC from 6 bits and higher. Nevertheless, if we want to choose low-bit ADC from 1 to 4 bits at the receiver for green communication systems with simple hardware, low cost, and low power consumption, the bit resolution of DAC must be set up at high values, i.e. larger than 6 bits and oversampling method also need to be applied in ADC process.

2.4 Conclusion

In this chapter, we point out the effects of residual SI and quantization noise due to the DAC/ADC process on the FD transmission system. First, it can be clearly seen that self-interference to noise ratio is a major factor that degrades the system performances, and it can be cancelled by using the DSIC process in FD transmission. Moreover, the quantization noise significantly destroys and degrades the transmission quality. Therefore, the bit resolution should be carefully chosen with high value, i.e. larger than 6 bits for both DAC/ADC processes. If the green communications system and IoT applications are considered with low-bit ADC, i.e. from 1 to 4 bits, the bit resolution of DAC must be chosen at high value and the oversampling should be applied in the ADC process in order to reduce the effects of quantization noise. Besides, the $\Sigma\Delta$ ADC seems to be the best choice in ADC process. Furthermore, the use of channel coding schemes plays a significant role in FD transmission. It can estimate and reconstruct the information signal approximately as in the ideal case. Therefore, channel coding techniques such as 5G QC-LDPC codes, Polar codes, and Turbo codes are the admired candidates for the integrity of information in FD transmission, and 5G QC-LDPC codes seem to give sufficient results. Therefore, for the rest of this thesis, the 5G QC-LDPC codes will be used to further implement and develop. For the ADC/DAC process, it is assumed that the bit resolution is chosen high enough to avoid the impact of the quantization process, that is, using 12 bits $\Sigma\Delta$ ADC.

Chapter 3

Jointly Iterative Blind Self-Interference Cancellation, Propagation Channel Estimation and Decoding Processes in Short-packet Full-Duplex Transmissions

In Chapter 2, channel coding schemes can be used to compensate for residual SI and quantization noise problems. However, global digital signal processing at the receiver must be improved and adjusted for short-packet transmission to achieve a good convergence of the channel estimation and decoding processes. Therefore, this chapter proposes a joint iterative blind SI cancellation, channel estimation, and decoding algorithm in FD transmissions combined with the DSIC process. Unlike the conventional without feedback algorithm, the proposed blind algorithm simultaneously estimates the SI and intended channels and decodes messages with 5G QC-LDPC codes. Then, the temporary estimations of the intended channel and the decoded message are fed back to improve the SI cancellation and also the channel estimation and decoding in the next iteration. This chapter further proposes a partial feedback scheme, which only uses a few feedback symbols for channel estimation, to significantly reduce processing time and computational complexity while maintaining performance. These good properties seem quite suitable for using this proposed blind iterative algorithm on short-packet FD transmissions in IoT applications and green communications. The content of chapter has been published in:

- Bao Quoc Vuong, Roland Gautier, Anthony Fiche, Mélanie Marazin, Ta Quang Hien, Nguyen Lap Luat: *"Joint Iterative Blind Self-Interference Cancellation, Propagation Channel Estimation and Decoding Processes in Full-Duplex Transmissions"*, in IEEE Access 10: 22795 - 22807 (February 2022).

3.1 Introduction

In the era of 5G wireless communications, associated with IoT support, to enable many new devices to communicate and to be able to make autonomous decisions by deploying diverse technologies and connecting massive devices [115–117]: two main services are targeted, namely uRLLC and mMTC [118]. The uRLLC strictly requires reliability and latency, since it concentrates on supporting mission-critical applications such as intelligent transportation and industry automation [116, 119]. The mMTC brings advantages on energy efficiency, since it concentrates on supporting massive machine-type applications which can be up to thousands of devices such as wearable or smart applications and sensors in IoT [11]. In order to be efficient, both uRLLC and mMTC require the use of short-packet information frame, and certainly provide short-packet transmissions in their applications. Moreover, the implementation of physical-layer security for both uRLLC and mMTC leads to promote even more the use of short-packet transmissions [115]. Short-packet transmission is considered as fundamental security issue in 5G and IoT applications compared to the normal packet transmission system to ensure robustness with respect to interception (eavesdropper) or self-jamming [120].

Traditionally, the digital signal processing mechanisms at the receiver such as equalizer (Decision Feedback Equalizer (DFE), linear equalizer, etc.), demodulation, de-interleaving, and decoding processes work independently, and thus, the problem of time consumption and transmission quality have not been adapted in case of short-packet transmission. In FD transmission systems, the DSIC requires more processing steps at the receiver and the assumption on the signal knowledge and SI channels must be made to perform the blind or semi-blind estimations [5, 71, 121, 122]. Particularly, joint algorithms of channel estimation are proposed, for instance, as in [114]. With an iterative Maximum Likelihood (ML) channel estimator for both SI and intended (propagation) channels can be estimated by taking into account the known SI, the pilots and unknown data symbols of the signal. However, performances are significantly degraded in short-packet communication due to consecutive pilot transmission over a long period. In [123], the joint estimate coefficients for both SI, intended channels, and transceiver impairments have been proposed using subspace algorithm. Nevertheless, the results in short-packet communication are still in expectation because it needs more data symbols to obtain a good second-order statistic of received signal. So, it is still not a satisfying solution for time, bandwidth, and power efficient approaches for short-packet transmission in the FD system. This issue is a constraint since it requires numerous pilot symbols to obtain the saturation of channel estimation. Therefore, the short length of pilot symbols for channel estimation in short-packet communications receives a lot of concerns. Furthermore, the use of FD short-packet transmission has also faced some drawbacks such as the high estimation error of the SI channel [50] as well as the high latency of the decoding process, i.e. in the

5G QC-LDPC decoder [90, 93], because the decoder uses many iterations to achieve the convergence or saturation level. These challenges of the FD short-packet transmission still attract a lot of interests of researchers in recent years.

In this chapter, we investigate joint iterative channel estimation and decoding algorithms in FD transmissions in the digital domain via feedback of channel estimates and decoded messages combined with the process of DSIC. The first algorithm is a blind version. The idea is to repeat the simultaneous process of channel estimation and decoding with the DSIC process via feedback to minimize the error of channel estimates and decoded messages. The intended message is temporarily decoded from the received signal and later is re-encoded, re-modulated, re-interleaved, and fed back to the process per each 5G QC-LDPC decoding iteration. After some iterations for a sufficient saturation, the channel estimates and decoded messages can be achieved with the minimum error. The channel estimation process is based on the RLS algorithm, as it has a better performance compared to others [74, 124, 125]. It is used to monitor the change in time of the SI channel per each iteration to get a better estimation and reconstruction of the interference and intended signals. Firstly, we illustrate the influence of the proposed algorithm in both SI and intended channel estimations. Furthermore, a partial feedback scheme is considered to reduce the processing time of the proposed blind algorithm.

Throughout this chapter, the performance evaluation of the proposed algorithms is based on four metrics: Mean Square Error (MSE), Bit-Error-Rate (BER), processing time and computational complexity. The contributions of this chapter can be summarized as follows:

- We propose a joint iterative blind channel estimation and decoding for short-frame transmissions via feedback;
- We characterize the out-performance of the system with feedback using the proposed algorithm compared to that without feedback;
- We point out that the number of joint iterations in the proposed algorithms with the use of 5G QC-LDPC codes is required only four iterations to achieve the convergence performance;
- We further propose a partial feedback scheme which only use a partial number of modulated symbols in feedback loop for channel estimation processes, and it can significantly reduce the processing time and computational complexity while maintaining the convergence performance;

The remaining of this chapter is organized as follows. Section 3.2 briefly describes the system model of FD transmissions with 5G QC-LDPC codes and the conventional DSIC algorithm. Section 3.3 proposes the joint iterative blind channel estimation and decoding algorithm. Numerical results and comparisons with the conventional algorithm

are shown in Section 3.4. Section 3.5 introduces the partial feedback scheme, then a comparison between blind and partial blind feedback schemes is shown in Section 3.6 with the processing time and computational complexity of all schemes. Finally, some highlights and conclusions will be discussed in Section 3.7.

3.2 Conventional DSICED3_W/OF Scheme

The conventional FD transmission between user A and B with the presence of 5G LDPC codes and DSIC process has been described in Section 2.2 of Chapter 2. However, an interleaver process needs to be added in order to achieve better channel bit locations in Gray mapping of modulation with the modulation order M, especially in short-packet transmission. Therefore, in this chapter, we further introduce the Digital Self-Interference Cancellation, Equalization, Demodulation, De-interleaving and Decoding Without Feedback (DSICED3_W/OF) scheme, which is shown in Fig. 3.1.

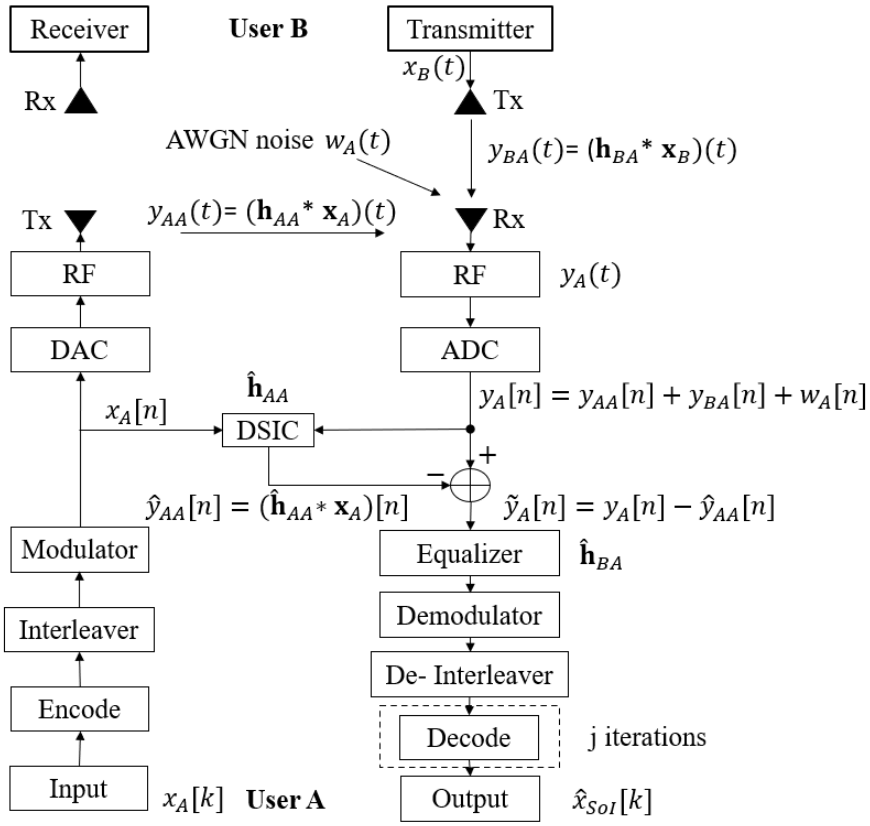


Fig. 3.1: SISO FD transmission with conventional DSICED3_W/OF scheme.

On the transmitting side, the sequence of input information messages $x_A[k]$ in the bit domain, where $k \in [1, K]$, will be encoded by using the (N, K) 5G QC-LDPC codes, to form a code word of length N, as presented in Section 1.2.1.4. Then, this sequence of code words is interleaved, modulated with the QPSK modulator by modulation order $M = 4$ to form a complex symbol sequence $x_A[n]$, where $n \in [1, E]$ and $E = N/log_2(M)$.

The mathematical expression of interleaver process is based on Section 5.4.2.2 in [80] and summarized in Algorithm 3.1. A graphical example of the interleaving process in 5G QC-LDPC codes is also shown in Fig. 3.2. After that, it is converted to the continuous-time domain by the DAC process to form the transmitted signal $x_A(t)$ and to be passed to the RF for transmitting to node B. The same process is applied at node B for $x_B(t)$.

Algorithm 3.1: Interleaver Algorithm in 5G QC-LDPC

Inputs : $a_1, a_2, ..., a_N$;
Outputs : $b_1, b_2, ..., b_N$;
Iteration: :

```
for col = 0 to N/M − 1 do
    for row = 0 to M − 1 do
        b_{row+col×M} = a_{row×N/M+col}
    end
end
```

Fig. 3.2: Example of bit interleaving in 5G QC-LDPC codes.

At the receiving side, node A receives the summation signal $y_A[t]$ and then passes it to the ADC process for being converted to the discrete time domain signal, $y_A[n]$. Here, the bit resolution and voltage dynamic range of the DAC/ADC architecture should be chosen high enough to avoid the residual quantization noise error, which has been studied in Chapter 2. In this chapter, the impacts of DAC/ADC, other hardware impairments on the SI cancellation and the synchronization problem between the signals are not considered (which is outside of this thesis but essential in practice). The DSIC process is then applied to obtain the estimated SI channel $\hat{\mathbf{h}}_{AA}$ by using an adaptive filter with the RLS algorithm with the forgetting factor $\lambda = 0.999$. Since node A knows its transmitted signal $x_A[n]$, a copy version of $x_A[n]$ can be used to eliminate the SI component to obtain:

$$\tilde{y}_A[n] = y_A[n] - \hat{y}_{AA}[n] = y_A[n] - (\hat{\mathbf{h}}_{AA} * \mathbf{x}_A)[n]. \tag{3.1}$$

Then, the residual signal continously goes to an equalizer process in order to obtain the estimated intended channel $\hat{\mathbf{h}}_{BA}$ and the equalized signal $\tilde{y}''_A[n]$. The Recursive Least

Square - Constant Modulus Algorithm (RLS-CMA) blind equalization algorithm [126] has been used and the mathematical expression for this algorithm is given as follows:

1. Initial value:

- $\hat{\mathbf{h}}_{BA}^{[0]} = \overbrace{[0, 0, ..., 0]}^{L}$ with L is the length of the intended channel;
- $\mathcal{T}(0) = \delta^{-1}\mathbf{I}$ where $\mathbf{I}$ is the identity matrix of rank L;
- $\tilde{\mathbf{y}}''_A[n] = 0$;

2. Computation: for : $n = L, L+1, ..., length(\tilde{\mathbf{y}}_A)$;

$$\mathcal{U}[n] = \mathbf{y}[n](\hat{\mathbf{h}}_{BA}^{(n-1)\mathcal{H}}\mathbf{y}[n])^* \tag{3.2}$$

where $\mathbf{y}[n] = [\tilde{y}_A[n], \tilde{y}_A[n-1], ..., \tilde{y}_A[n-L+1]]$;

$$\mathcal{E}[n] = \frac{E[|\tilde{\mathbf{y}}''_A[n]|^4]}{E[|\tilde{\mathbf{y}}''_A[n]|^2]} - \hat{\mathbf{h}}_{BA}^{(n-1)\mathcal{H}}\mathcal{U}[n] \tag{3.3}$$

$$\mathbf{q}[n] = \frac{\mathcal{T}[n-1]\mathcal{U}[n]}{\lambda(1 + \mathcal{U}^{\mathcal{H}}[n]\lambda^{-1}\mathcal{T}[n-1]\mathcal{U}[n])} \tag{3.4}$$

$$\mathcal{T}[n] = \frac{1}{\lambda(\mathcal{T}[n-1] - q[n]\mathcal{U}^{\mathcal{H}}[n]\mathcal{T}[n-1])} \tag{3.5}$$

$$\hat{\mathbf{h}}_{BA}^{(n)} = \hat{\mathbf{h}}_{BA}^{(n-1)} + \mathcal{E}^*[n]\mathbf{q}[n] \tag{3.6}$$

$$\tilde{\mathbf{y}}''_A[n] = \hat{\mathbf{h}}_{BA}^{(n-1)\mathcal{H}}\mathbf{y}[n] \tag{3.7}$$

where:

- λ is the forgetting factor and should be chosen between 0.9 and 1;
- δ is the regularization parameter used to initialize $\mathcal{T}(0)$, and should be assigned a small value for a high signal-to-noise ratio (SNR) (greater than 10 dB) and a large value for a low SNR (less than 10 dB) [76];
- $\mathcal{U}^{\mathcal{H}}[n]$ is the Hermitian transposition of $\mathcal{U}[n]$.

Afterthat, the binary output $\hat{x}_{SoI}[k]$ of the intended signal can be obtained from the equalized signal $\tilde{y}''_A[n]$ via demodulation, de-interleaving and decoding processes. In decoding process, the LLR belief sequence received from the soft remapping QPSK demodulation process will be used for decisions and the SPA decoding algorithm is performed as described in Section 1.2.1.5. To reconstruct the intended binary input signal $\hat{x}_{SoI}[k]$ from node B, we use the SPA at node A, that is, the message passing between the check nodes and the symbol nodes to guess the bits transmitted from each other at each iteration j until it reaches the maximum number of interactions j_{max}.

However, the conventional DSICED3_W/OF scheme requires the LLR sequences and decoding updated per iteration after channels are estimated, and the SI is canceled, which means that the channel estimations and the SI cancellation are separated from the decoding process. This leads to some drawbacks of this conventional scheme, such as the high estimation error of the SI channel [50], as well as the high latency of the 5G QC-LDPC decoder [90, 93] in short-packet transmissions. To overcome these drawbacks, channel estimations and SI cancellations should be embedded in the iterative decoding process to obtain a novel scheme, which we name Joint Iterative Blind Digital Self-Interference Cancellation, Equalization, Demodulation, De-interleaving and Decoding (JIB_DSICED3) scheme.

3.3 Proposed Joint Iterative Blind Scheme

The JIB_DSICED3 scheme is shown in Fig. 3.3, in which the proposed scheme is developed on the principle that the processes of SI cancellation and decoding of the desired signal can benefit from each other via the temporary decoding and feedback loop after each joint iteration decoding i, where $i \in [1, i_{max}]$. We emphasize that, different from the iteration j that performs the iteration decoding in the system without feedback in Section 3.2, the iteration i in the proposed algorithm is for the joint channel estimation and decoding via feedback. We also emphasize that including many j iterations decoding in each of the i iterations in the JIB_DSICED3 scheme will increase latency and complexity because the SPA decoding process between the check node and variable nodes is an optimal iterative decoding algorithm, but with high computational complexity [127]. Therefore, the proposed scheme will only consider one iteration decoding ($j_{max} = 1$) for each joint iteration i, called temporary decoding, and it will be later proven that the proposed scheme requires only a few iterations to achieve saturation performance. The proposed iterative algorithm is presented in the following four main steps:

Step 1: SI channel estimation and DSIC process

First, a copy version of the transmitted signal $x_A[n]$ in the digital domain and the received signal at the receiver of node A after the ADC process $y_A[n]$ are used to calculate the error signal in the DSIC process. Then, based on this error, we can control and modify the unknown SI channel vector $\hat{\mathbf{h}}_{AA}$ using an adaptive filter with the RLS algorithm. As a result, we can effectively obtain the estimation of the SI channel and achieve the interference component $\hat{y}_{AA}[n]$. The output signal after this step can be expressed as:

$$\tilde{y}_A^{(i)}[n] = y_A[n] - \hat{y}_{AA}^{(i)}[n] = y_A[n] - (\hat{\mathbf{h}}_{AA}^{(i)} * \mathbf{x}_A)[n]. \tag{3.8}$$

Step 2: Intended channel estimation

The residual signal $\tilde{y}_A^{(i)}[n]$ received from Step 1 will pass through an equalizer first to

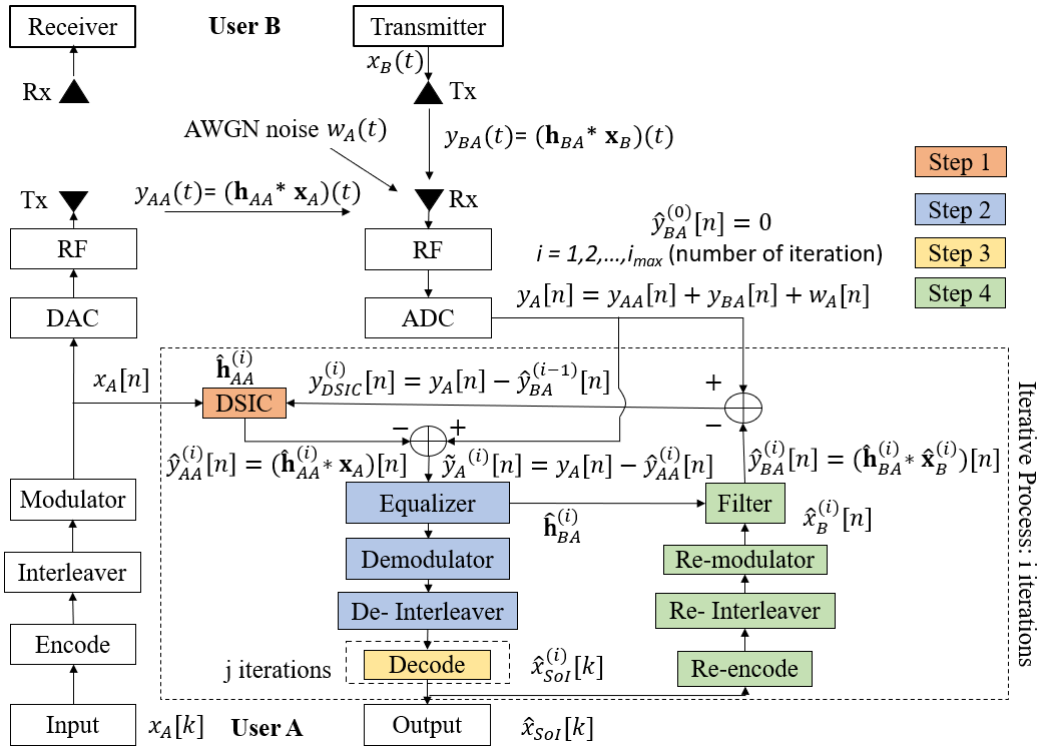


Fig. 3.3: SISO FD transmission with the proposed JIB_DSICED3 scheme.

estimate the intended multipath fading channel $\hat{\mathbf{h}}_{BA}$ and then to obtain the equalized signal with reduction of the effects of the multipath fading channel and AWGN noise. Here, a blind channel estimation method with RLS-CMA algorithm [126] is applied with no knowledge from the transmitting signal from node B, where the initial value of $\mathbf{x}_B = \mathbf{0}$ when starting the iterative process. Then, the equalized signal continues to go to the QPSK demodulator and de-interleaver process to get the LLR belief information sequence for decoding.

Step 3: Decoding of the intended signal

Then, the temporary estimation of binary intended signal of node B $\hat{x}_{SoI}^{(i)}[k]$ is achieved by using 5G QC-LDPC decoding process with the exchange belief information between the variable nodes and check nodes as Section 1.2.1.5 for each iteration. In this step, only one SPA decoding iteration is used ($j_{max} = 1$).

Step 4: Feedback loop

When the temporary binary data of the intended signal is estimated and the maximum number of joint iteration i_{max} is not reached, it goes to the feedback loop with re-encoding, re-interleaving, and re-modulation processes to obtain the feedback signal $\hat{x}_B^{(i)}[n]$. This signal will take a convolution process with the estimation version of the intended channel $\hat{\mathbf{h}}_{BA}^{(i)}$, which is obtained in Step 2, to form the feedback intended signal as $\hat{y}_{BA}^{(i)}[n] = (\hat{\mathbf{h}}_{BA}^{(i)} * \hat{\mathbf{x}}_B^{(i)})[n]$. Consequently, the intended signal feedback $\hat{y}_{BA}^{(i)}[n]$ is used to temporarily remove the intended component to optimize the SI channel estimation process for the

next iteration of decoding. It is given by:

$$y_{DSIC}^{(i+1)}[n] = y_A[n] - \hat{y}_{BA}^{(i)}[n]. \tag{3.9}$$

The proposed algorithm can be summarized in Algorithm 3.2.

Algorithm 3.2: Proposed Joint Iterative Blind Scheme

Inputs : $\mathbf{y}_A, \mathbf{x}_A, i_{max}, K, N, M$;
Outputs : $\hat{\mathbf{h}}_{AA}^{(i_{max})}, \hat{\mathbf{h}}_{BA}^{(i_{max})}, \mathbf{x}_{SoI}^{(i_{max})}$;
Initialization: $\hat{\mathbf{y}}_{BA}^{(0)} = \mathbf{0}$, $\hat{\mathbf{h}}_{AA}^{(0)} = \mathbf{0}$, $\hat{\mathbf{h}}_{BA}^{(0)} = \mathbf{0}$, $\hat{\mathbf{x}}_B^{(0)} = \mathbf{0}$;

for $i = 1$ *to* i_{max} **do**
  /* Perform all steps for all of E symbols, with $E = N/log_2(M)$, N is code word length, M is modulation order */
  for $n = 1$ *to* E **do**
    Step 1: SI channel estimation and DSIC process
    Estimate: $\hat{\mathbf{h}}_{AA}^{(i)}$;
    Calculate: $\tilde{y}_A^{(i)}[n] = y_A[n] - \hat{y}_{AA}^{(i)}[n] = y_A[n] - (\hat{\mathbf{h}}_{AA}^{(i)} * \mathbf{x}_A)[n]$;
    Step 2: Intended channel estimation
    Estimate: $\hat{\mathbf{h}}_{BA}^{(i)}$ and calculate LLR belief sequence of $\mathbf{x}_{SoI}^{(i)}$;
  end
  /* Decoding for all K symbols */
  for $k = 1$ *to* K **do**
    Step 3: Decoding of the intended signal
    Decoding: $x_{SoI}^{(i)}[k]$;
  end
  if $i < i_{max}$ **then**
    /* Perform Step 4 for all E symbols */
    for $n = 1$ *to* E **do**
      Step 4: Feedback loop
      Perform feedback loop to get $\hat{x}_B^{(i)}[n]$;
      Calculate: $\hat{y}_{BA}^{(i)}[n] = (\hat{\mathbf{h}}_{BA}^{(i)} * \hat{\mathbf{x}}_B^{(i)})[n]$;
      Update: $y_{DSIC}^{(i+1)}[n] = y_A[n] - \hat{y}_{BA}^{(i)}[n]$;
    end
  else
    /* It is the end of the process of this algorithm */
    Go to return
  end
end
return $\hat{\mathbf{h}}_{AA}^{(i_{max})}, \hat{\mathbf{h}}_{BA}^{(i_{max})}, \mathbf{x}_{SoI}^{(i_{max})}$.

3.4 Comparison Between Blind Without/With Feedback Schemes: DSICED3_W/OF vs JIB_DSICED3

In this section, the most important metrics in channel estimation performance, MSE and BER in the two cases with and without feedback, will be computed by using Monte Carlo simulations on MATLAB. The input information length is chosen a few tens or a few hundred bits and QPSK is used as modulation scheme, which are suitable in the context of short-packet IoT transmissions, i.e. LoRa has maximum information size of 2048 bits (256 bytes) [28]. In addition, the impact of different code rates is also considered. For 5G QC-LDPC codes, the base graph matrix **BG2** is implemented for all simulations. Initially, the SI channel is fixed with 3 taps, while the intended channel is fixed with 4 taps according to the ITU–R channel model for pedestrian environment [79]. These channels are generated independently in each transmission frame. Based on the background noise as reference and without loss in generality, we further denote $\rho_{AA} = p_A/\sigma_A^2$ is the self-interference to noise ratio and $SNR_A = p_B/\sigma_A^2$ is the SNR at user A, where p_A, p_B and σ_A^2 are the power of SI signal, intended signal and background noise at user A, respectively. The simulation parameters are summarized in Table 3.1.

Table 3.1: Simulation Specifications

Parameter	Value
Code word length (N)	64, 128, 256, 512, 1024
Information length (K)	32, 64, 128, 256, 512
Modulation scheme (M)	QPSK ($M = 4$)
Frame length after modulation ($E = N/log_2(M)$)	32, 64, 128, 256, 512
Code rate (R)	1/3, 1/2, 2/3, 3/4, 5/6
Number of transmission frames	10^6
SI channel taps	3
Intended channel taps	4
Forget factor λ	0.999

Next, we will characterize the performance of the proposed scheme JIB_DSICED3 and compare it to that of the conventional scheme DSICED3_W/OF in terms of the MSE and BER performances.

3.4.1 MSE Performances

In this subsection, we also introduce a particular scheme called Best Performance Scheme (BPS), which corresponds to a lower bound (but not realistic in practice) using the proposed JISB_DSICED3 scheme considering that all intended E symbols from user B are known, as a benchmark to characterize the optimality of the proposed JISB_DSICED3 scheme in terms of MSE and for performance comparison. Indeed, in this limit case,

all the intended E symbols are also known, and the system does not need to perform the temporary decoding in Step 3 and re-encoding, re-interleaving and re-modulation processes in Step 4. Instead, in Step 4, it only considers using all known E symbols to do a filter process with the estimation version of intended channel in Step 2 to obtain the estimation version of intended signal $\mathbf{y}_{BA}$ for subtraction in the next iterations.

First of all, Fig. 3.4 and Fig. 3.5 show the MSE in decibel (dB) scale of the SI and intended channels versus number of modulated symbols E for various values of number of decoding iterations, respectively. Based on the background noise as the reference, the self-interference to noise ratio ρ_{AA} and SNR_A are set at 30 dB and 20 dB, respectively. It can be seen that the MSE significantly decreases as the number of joint iterations increases, and converges to -25 dB as the number of transmitted symbols increases.

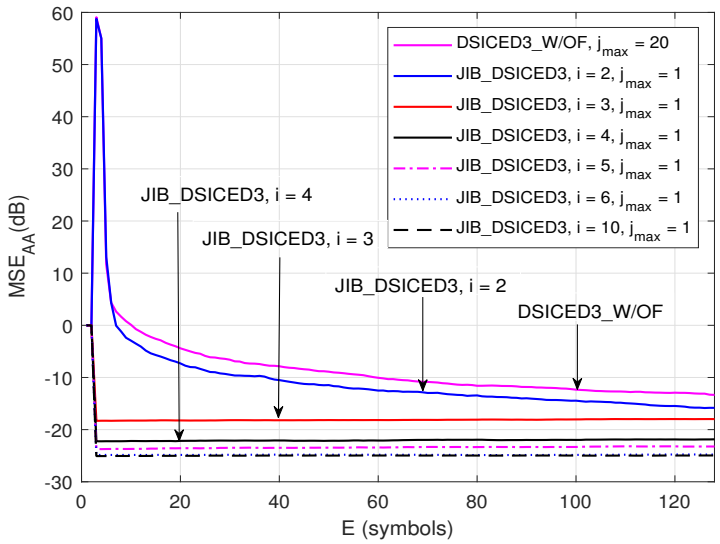


Fig. 3.4: MSE_{AA} (dB) after the i-th decoding iteration versus E symbols; $R = 1/2$, $\rho_{AA} = 30$ dB and $SNR_A = 20$ dB.

It can also be seen that the MSE of the proposed scheme converges to -25 dB (the critical or saturation value) much faster than that of the conventional scheme. More specifically, the JIB_DSICED3 scheme only requires 4 iterations to achieve saturation performance even for a few transmitted symbols while the DSICED3_W/OF scheme remains a high error in channel estimation process, e.g. 0 dB for about 10 transmitted symbols in Figures. 3.4 and 3.5. Therefore, the proposed JIB_DSICED3 scheme significantly reduces latency and shows its robustness and practical applications in 5G & beyond and IoT transmission, in which strict requirements of extremely short-packet transmissions and low latency are considered.

Fig. 3.6 and Fig. 3.7 show the MSE of the SI and intended channels versus SNR_A (dB). It can be clearly seen that the MSE decreases as the SNR_A increases. The results show that the proposed scheme outperforms the conventional DSICED3_W/OF scheme, especially for high SNR_A (≥ 0 dB). The JIB_DSICED3 curves can converge quickly to the saturation error floor, while the DSICED3_W/OF curves only reach around 10^{-2} to

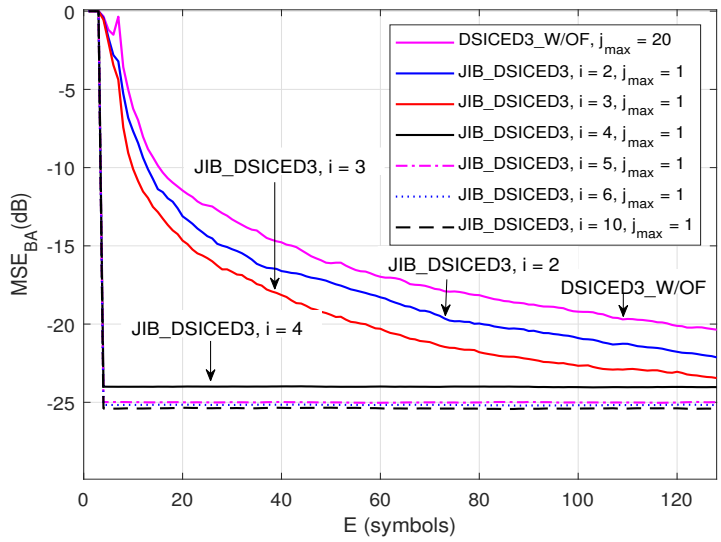


Fig. 3.5: MSE_{BA} (dB) after the i-th decoding iteration versus E symbols; $R = 1/2$, $\rho_{AA} = 30$ dB and $SNR_A = 20$ dB.

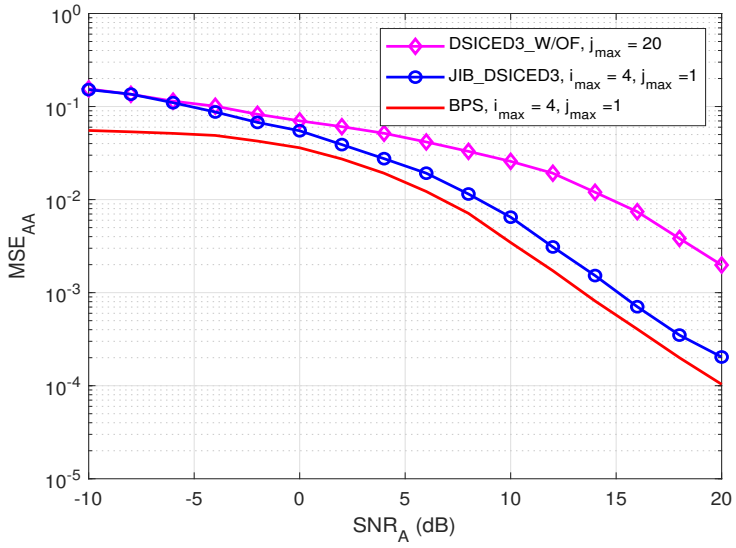


Fig. 3.6: MSE_{AA} versus SNR_A; $R = 1/2$, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

10^{-3}, although the JIB_DSICED3 scheme needs fewer iterations than the conventional one. Furthermore, the JISB_DSICED3 scheme is nearly optimal as its performance is approximately reached to that of the BPS scheme (as a lower bound), especially in the high region of SNR_A (≥ 0 dB), which is considered the range of interest in FD transmissions [128].

3.4.2 BER Performances

First, the BER performances of DSICED3_W/OF and JIB_DSICED3 schemes with different code rates, such as $R \in \{1/3, 1/2, 2/3, 3/4, 5/6\}$, are shown in Figures 3.8 and 3.9, respectively. It can be seen that when the code rate R increased, this leads to a de-

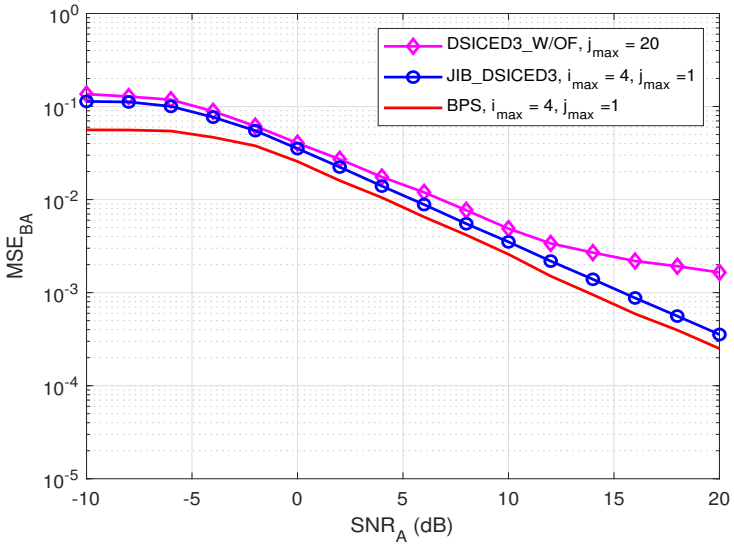


Fig. 3.7: MSE_{BA} versus SNR_A; $R = 1/2$, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

crease in the BER performance, and the relative behavior of the algorithm with feedback JIB_DSICED3 with respect to the code rate behaved in the same way as the conventional algorithm without feedback DSICED3_W/OF. For all code rates, the proposed blind feedback algorithm JIB_DSICED3 is better than the conventional algorithm without feedback DSICED3_W/OF. Therefore, depending on the purposes and applications, the code rate has to be chosen carefully because it can lead to a significant loss in terms of performance (code rate $R \in \{2/3, 3/4, 5/6\}$) or a too large loss of throughput (code rate $R = 1/3, 1/2$). For the rest of this chapter, the code rate was set at $1/2$ as a particular example in order to illustrate the out-performance of the proposed with feedback algorithm JIB_DSICED3 over the conventional without feedback algorithm DSICED3_W/OF.

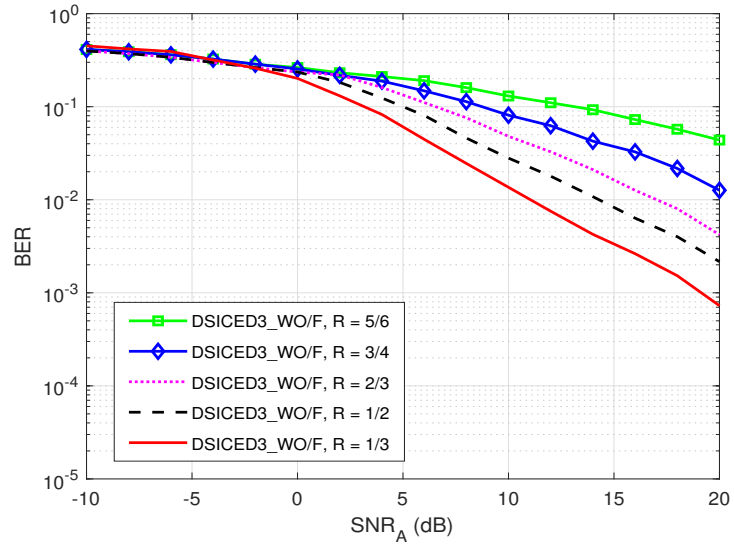


Fig. 3.8: BER of DSICED3_W/OF scheme versus SNR_A for different code rates R; $j_{max} = 20$, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

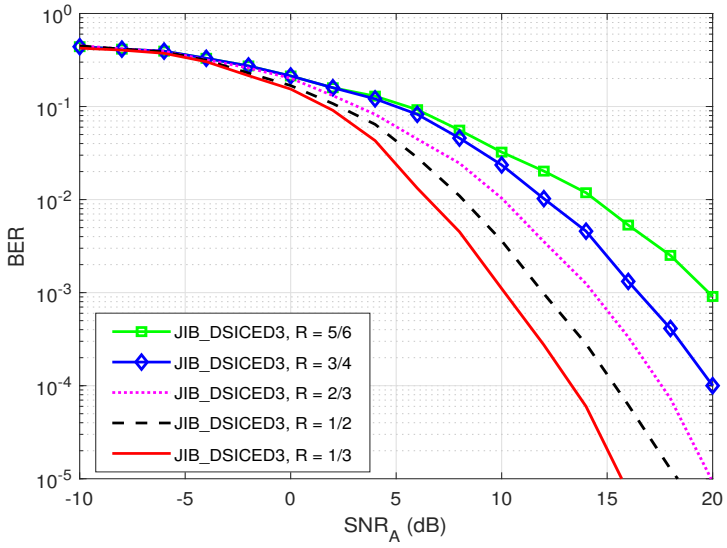


Fig. 3.9: BER of JIB_DSICED3 scheme versus SNR_A for different code rates R; $i_{max} = 4$, $j_{max} = 1$, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

Next, Fig. 3.10 shows BER of the DSICED3_W/OF scheme versus SNR_A after j_{max} iterations. It is noted that the without feedback scheme DSICED3_W/OF needs up to 20 iterations ($j_{max} = 20$) to converge and reach the saturation floor. Therefore, for the rest of this chapter, we chose $j_{max} = 20$ iterations for the DSICED3_W/OF scheme.

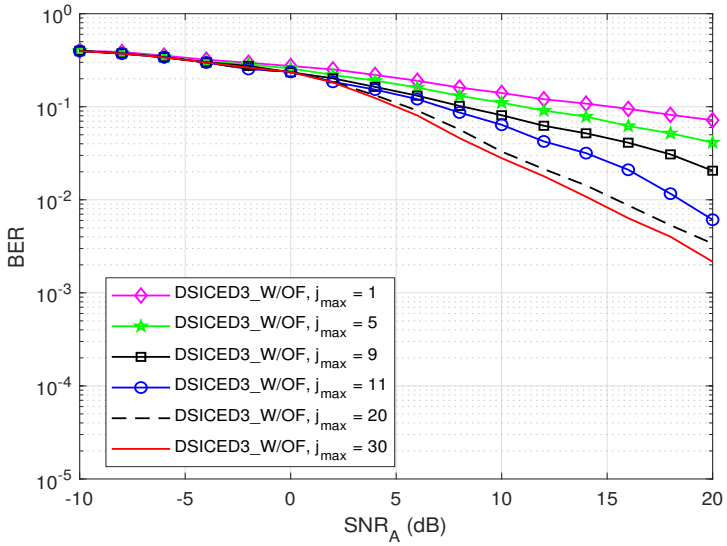


Fig. 3.10: BER of DSICED3_W/OF scheme versus SNR_A for different values of j_{max}; $R = 1/2$, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

Fig. 3.11 shows BER of the JIB_DSICED3 scheme versus SNR_A after i_{max} iterations. It can be seen that BER significantly decreases as SNR_A increases, and that the gain of JIB_DSICED3 over DSICED3_W/OF is bigger for larger SNR_A. At low SNR_A (≤ 0 dB), the conventional DSICED3_W/OF scheme seems to have slightly better in BER

than JIB_DSICED3 scheme. Because the high error of decoding at the first iteration of JIB_DSICED3 scheme in the low region of SNR_A leads to the consequence of a higher error in the next iterations. However, at high SNR_A (≥ 0 dB), which is the range of interest in FD transmissions [128], the proposed JIB_DSICED3 scheme outperforms the conventional DSICED3_W/OF scheme even when only 2 iterations are required. Moreover, BER of the proposed JIB_DSICED3 scheme when $i_{max} = 4$ and $j_{max} = 1$ is quite close to that when $i_{max} = 10$ and $j_{max} = 1$, as shown in Fig. 3.11. When we fix the maximum number of joint iterations $i_{max} = 4$ and try to vary the maximum number of decoding iterations, the results are very close to each other, as shown in Fig. 3.12. Thus, it confirms again the convergence performance when $i_{max} = 4$ and $j_{max} = 1$.

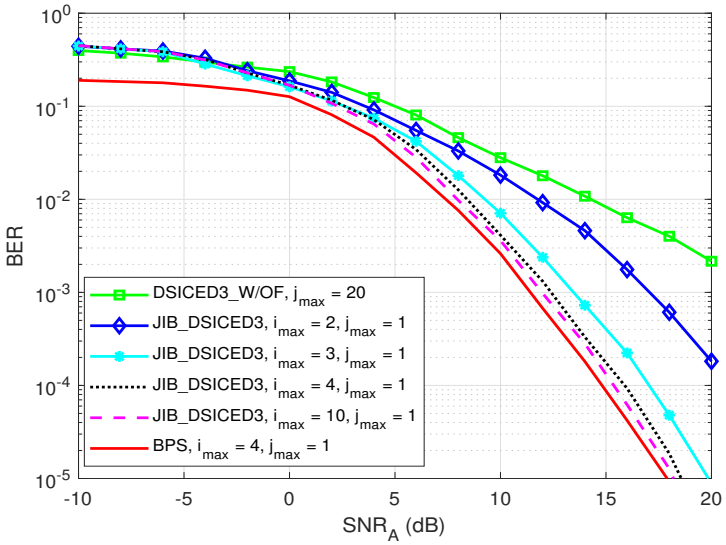


Fig. 3.11: BER of JIB_DSICED3 scheme versus SNR_A for different values of i_{max} iterations; $R = 1/2$, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

Fig. 3.13 shows the BER of the proposed JIB_DSICED3 scheme versus SNR_A after $i_{max} = 4$ iterations, for different values of self-interference to noise ratio ρ_{AA}. It can be seen that BER increases as the SI power increases, and the increase of BER is bigger for larger SNR_A. Moreover, the result indicates that the increase of SI power has fewer effects on the proposed JIB_DSICED3 scheme; for example, to maintaining BER at 10^{-4}, it is needed to increase roughly 0.5 dB in the SNR_A in order to compensate the increasing of 10 dB of self-interference to noise ratio ρ_{AA}, which is usually remained at high level in SISO FD transmission in practice. This result is critical in practical applications, since the proposed JIB_DSICED3 scheme is less sensitive to the SI level, which is useful for 5G FD transmission.

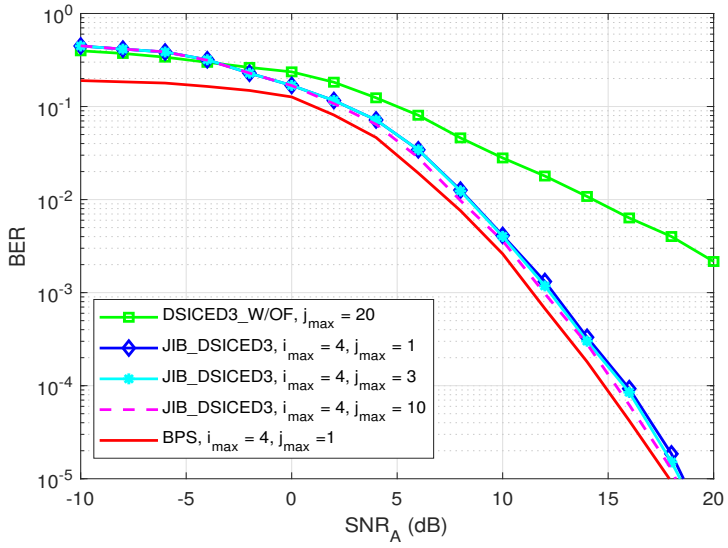


Fig. 3.12: BER of JIB_DSICED3 scheme versus SNR_A for different values of j_{max} iterations; $R = 1/2$, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

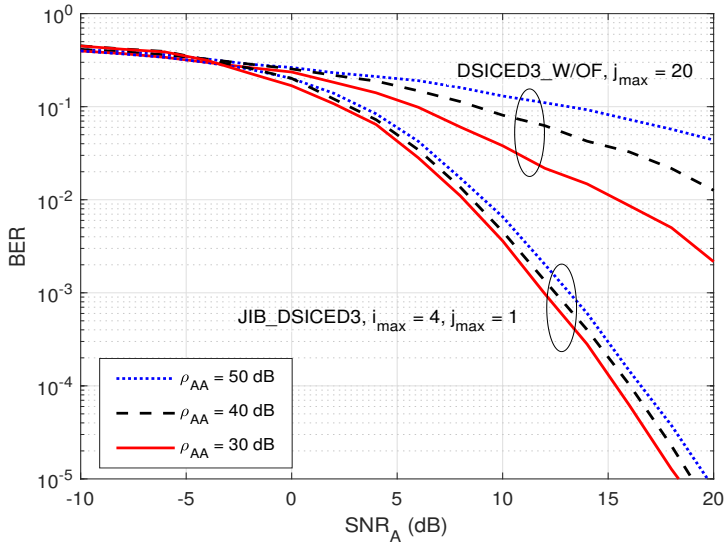


Fig. 3.13: BER of JIB_DSICED3 scheme versus SNR_A for different value of ρ_{AA} dB; $R = 1/2$, $E = 128$ symbols.

3.5 Proposed Blind Partial Feedback Scheme

Although the joint iterative blind scheme JIB_DSICED3 shows its robustness compared to the conventional without feedback scheme DSICED3_W/OF; its processing time can still be improved. In this section, we further introduce a partial feedback scheme version and name it as Joint Iterative Blind Digital Self-Interference Cancellation, Equalization, Demodulation, De-interleaving and Decoding with Partial Feedback (JIB_DSICED3_PF). Instead of using all modulated symbols for SI channel and intended channel estimation processes in feedback loop, a partial number of modulated symbols αE (with $0 < \alpha \leq 1$), where α is called partial feedback coefficient, will be used to construct

the estimation of intended signal and doing subtraction and estimation processes after the first iteration. The partial feedback scheme is illustrated in Fig. 3.14.

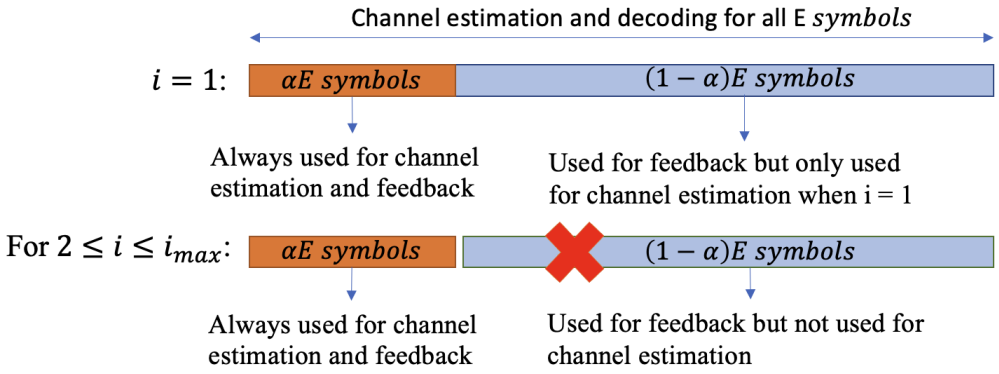


Fig. 3.14: Graphical presentation of the joint iterative blind partial feedback scheme.

Here, the algorithm also performs i_{max} iterations indexed by i for the channel estimation and message decoding. It should be noted that for $i = 1$ (first iteration), a first channel estimation and message decoding is performed to obtain all K bits, which is used to avoid a significant number of errors when starting the process of iterative algorithm. In Step 4 of the first iteration, the system performs re-encoded, re-interleaved and re-modulated processes to form E modulated symbols in feedback loop, and only $\alpha E = \alpha N/(log_2(M)$ symbols are used to form the estimation intended channel and perform updating subtraction and estimation process. From the second iteration $i \geq 2$, the system will perform the channel estimations with partial αE symbols instead of using all symbols, while the decoding process still perform the temporary decoding and feedback loop for all E modulated symbols to get K bits message. When the system reaches the maximum number of iterations i_{max}, the feedback loop is stopped and all symbols are decoded to obtain the estimated binary sequence $\hat{\mathbf{x}}_{SoI}$ of node B. The partial feedback algorithm can be summarized in Algorithm 3.3.

Next, we will characterize the performance of the partial feedback scheme JIB_DSICED3_PF in terms of MSE and BER with the simulation specifications as declared in Section 3.4. Moreover, in the next section, the impacts of different number of taps of SI channel and intended channel are also considered. The processing time and computational complexity of the with and without feedback schemes are also indicated.

Algorithm 3.3: Proposed Joint Iterative Blind Partial Feedback Scheme Version

Inputs : $\mathbf{y}_A, \mathbf{x}_A, i_{max}, \alpha, K, N, M$;
Outputs : $\hat{\mathbf{h}}_{AA}^{(i_{max})}, \hat{\mathbf{h}}_{BA}^{(i_{max})}, \mathbf{x}_{SoI}^{(i_{max})}$;
Initialization: $\hat{\mathbf{y}}_{BA}^{(0)} = \mathbf{0}$, $\hat{\mathbf{h}}_{AA}^{(0)} = \mathbf{0}$, $\hat{\mathbf{h}}_{BA}^{(0)} = \mathbf{0}$, $\hat{\mathbf{x}}_{B}^{(0)} = \mathbf{0}$;

for $i = 1$ *to* i_{max} **do**
  if $i = 1$ **then**
    /* Perform Step 1 and Step 2 for all of $E = N/log_2(M)$ symbols */
    for $n = 1$ *to* E **do**
      Step 1: SI channel estimation and DSIC process
      Estimate: $\hat{\mathbf{h}}_{AA}^{(i)}$;
      Calculate: $\tilde{y}_A^{(i)}[n] = y_A[n] - \hat{y}_{AA}^{(i)}[n] = y_A[n] - (\hat{\mathbf{h}}_{AA}^{(i)} * \mathbf{x}_A)[n]$;
      Step 2: Intended channel estimation
      Estimate: $\hat{\mathbf{h}}_{BA}^{(i)}$ and LLR belief sequence of $\mathbf{x}_{SoI}^{(i)}$;
    end
    /* Decoding for all K bits */
    for $k = 1$ *to* K **do**
      Step 3: Decoding of the intended signal Decoding: $x_{SoI}^{(i)}[k]$;
    end
  else
    /* Perform Step 1 and Step 2 for only $\alpha E = \alpha N/(log_2(M)$ symbols */
    for $n = 1$ *to* αE **do**
      Step 1: SI channel estimation and DSIC process
      Estimate: $\hat{\mathbf{h}}_{AA}^{(i)}$;
      Calculate: $\tilde{y}_A^{(i)}[n] = y_A[n] - (\hat{\mathbf{h}}_{AA}^{(i)} * \mathbf{x}_A)[n]$;
      Step 2: Intended channel estimation
      Estimate: $\hat{\mathbf{h}}_{BA}^{(i)}$;
    end
    /* Decoding for all K bits */
    for $k = 1$ *to* K **do**
      Step 3: Decoding of the intended signal Decoding: $x_{SoI}^{(i)}[k]$;
    end
  end
  if $i < i_{max}$ **then**
    /* Feedback loop with E symbols */
    for $n = 1$ *to* E **do**
      Step 4: Feedback loop
      Perform feedback loop to get $\hat{\mathbf{x}}_B^{(i)}$;
    end
    /* Updating with only αE symbols */
    for $n = 1$ *to* αE **do**
      Calculate: $\hat{y}_{BA}^{(i)}[n] = (\hat{\mathbf{h}}_{BA}^{(i)} * \hat{\mathbf{x}}_B^{(i)})[n]$;
      Update: $y_{DSIC}^{(i+1)}[n] = y_A[n] - \hat{y}_{BA}^{(i)}[n]$;
    end
  end
  Go to return
end
return $\hat{\mathbf{h}}_{AA}^{(i_{max})}, \hat{\mathbf{h}}_{BA}^{(i_{max})}, \mathbf{x}_{SoI}^{(i_{max})}$.

3.6 Comparison Between Blind and Partial Blind Feedback Schemes: JIB_DSICED3 vs JIB_DSICED3_PF

3.6.1 MSE Performances

Fig. 3.15 and Fig. 3.16 show the MSE of the SI channel and the intended channel versus number of iterations i for different values of α, respectively, and $SNR_A = 10$ dB, $\rho_{AA} = 30$ dB, $E = 128$ symbols. It can be seen that the MSE of the partial feedback scheme JIB_DSICED3_PF converges fast and, when $\alpha E = 32$ symbols ($\alpha = 1/4$), it reaches the saturation performance close to that of the JIB_DSICED3 scheme. It can also be observed that, when $\alpha E = 32$ symbols or $\alpha = 1/4$, the JIB_DSICED3_PF scheme requires 4 iterations to achieve the saturation performance, similar to the JIB_DSICED3 scheme. Therefore, these results indicate the efficient use of partial feedback in both the SI and intended channel estimation processes.

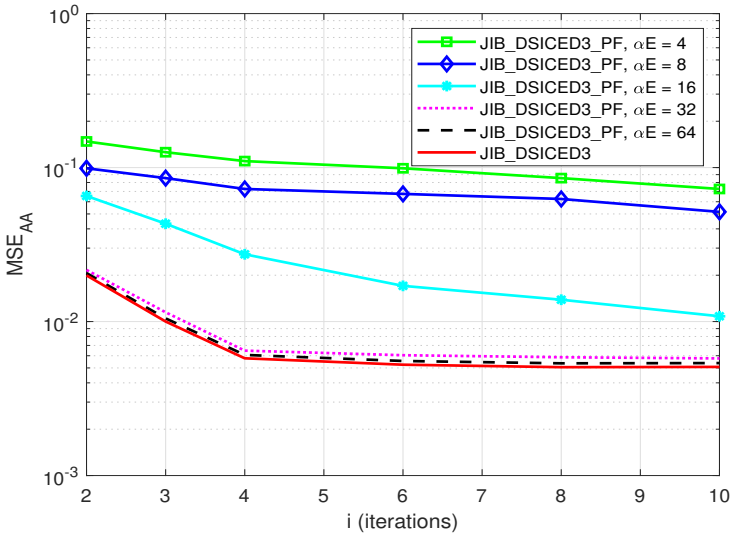


Fig. 3.15: MSE_{AA} versus i; $R = 1/2$, $SNR_A = 10$ dB, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

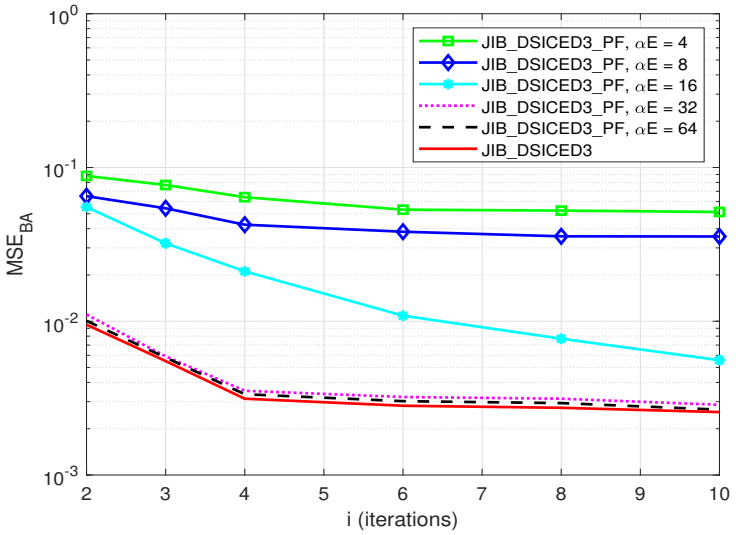


Fig. 3.16: MSE_{BA} versus i; $R = 1/2$, $SNR_A = 10$ dB, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

Furthermore, Fig. 3.17 and Fig. 3.18 illustrate the MSE of the SI channel and the intended channel when changing the number taps of SI channel $(3, 4, 5, 6)$ and the number of taps of intended channel $(4, 6, 7, 8)$, respectively. It can be seen that changing the number of taps on these channels does not significantly affect the performance of MSE. Indeed, the proposed JIB_DSICED3_PF scheme gives a sufficient MSE performances regardless the number of taps of SI channel and intended channel.

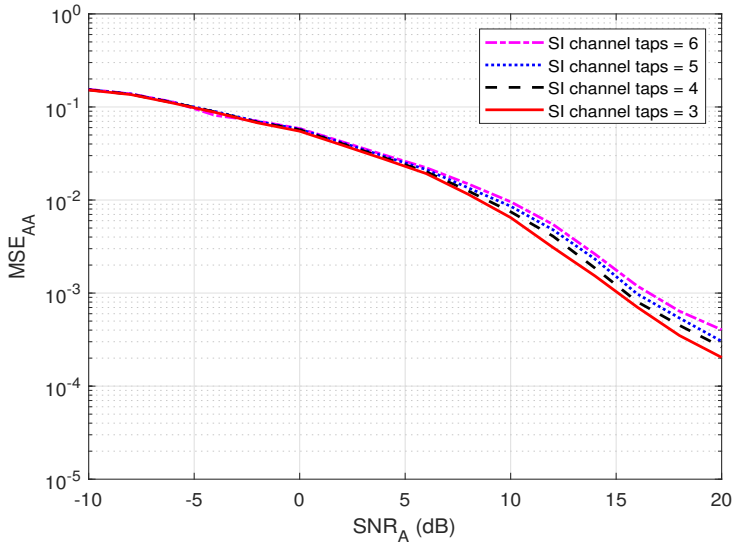


Fig. 3.17: MSE_{AA} of JIB_DSICED3_PF scheme versus SNR_A for different number of SI channel taps; $R = 1/2$, $\rho_{AA} = 30$ dB, $\alpha = 1/4$ and $E = 128$ symbols.

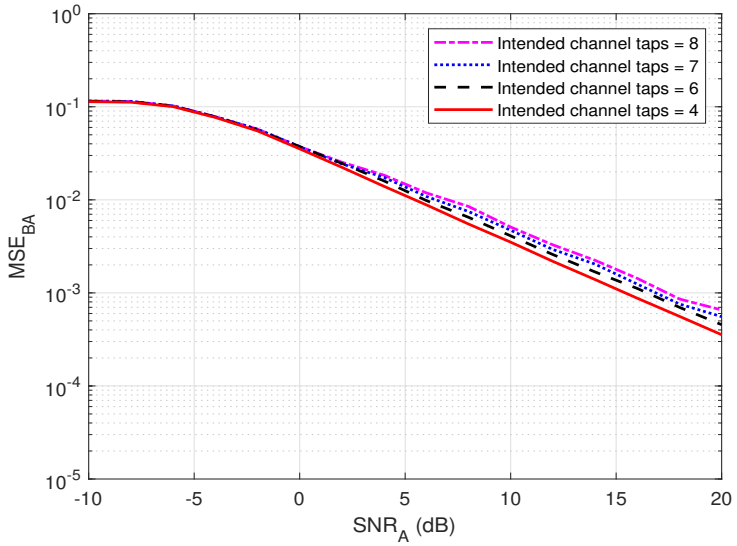


Fig. 3.18: MSE_{BA} of JIB_DSICED3_PF scheme versus SNR_A for different number of intended channel taps; $R = 1/2$, $\rho_{AA} = 30$ dB, $\alpha = 1/4$ and $E = 128$ symbols.

3.6.2 BER Performances

Fig. 3.19 shows BER of the partial feedback scheme JIB_DSICED3_PF versus α for different values of SNR_A. Similar with MSE performances, the BER of JIB_DSICED3_PF scheme also achieves the saturation performance when $\alpha E = 32$ symbols or $\alpha = 1/4$. Furthermore, the comparison of the three schemes such as without feedback DSICED3_W/OF, with feedback JIB_DSICED3 and with partial feedback JIB_DSICED3_PF, versus total number of modulated symbols, E, is illustrated in Fig. 3.20. In this case, the different number of information bits $K \in \{32, 64, 128, 256, 512\}$ are used, which correspond to the length of code word $N \in \{64, 128, 256, 512, 1024\}$ and the length of modulated symbols $E \in \{32, 64, 128, 256, 512\}$, respectively, and the partial feedback coefficient $\alpha = 1/4$. The result shows that the BER performance of JIB_DSICED3 and JIB_DSICED3_PF is nearly the same, regardless of total number of symbols. Moreover, at low values of SNR_A, i.e. $SNR_A = 5$ dB, the two feedback schemes JIB_DSICED3 and JIB_DSICED3_PF also have better performance than the DSICED3_W/OF scheme for small value of E, i.e. $E \leq 128$ symbols and the performance of three schemes converges closed to each other as E is sufficiently large. Furthermore, for larger SNR_A, i.e. $SNR_A = 10$ dB, the gap between the two feedback schemes JIB_DSICED3 and JIB_DSICED3_PF compared to the DSICED3_W/OF scheme is also bigger.

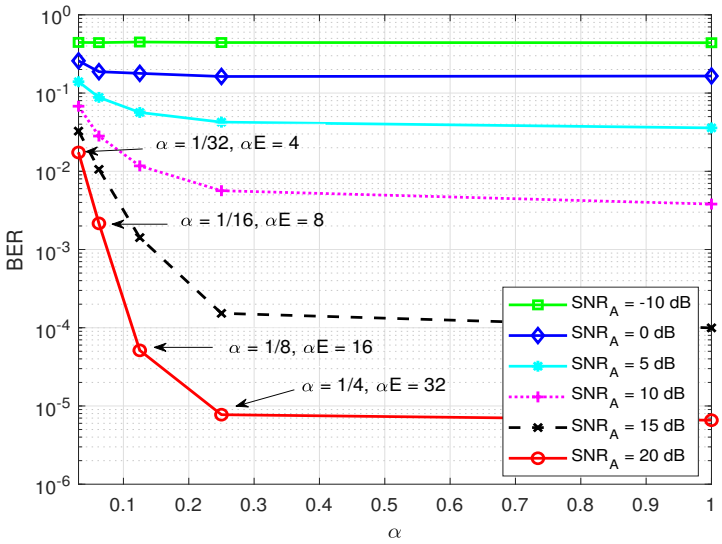


Fig. 3.19: BER of JIB_DSICED3_PF scheme versus α; $R = 1/2$, $i_{max} = 4$, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

Therefore, these results again confirm the efficient use of partial feedback to significantly reduce computation complexity and processing time, which will be illustrated in Section 3.6.3, in feedback loop while guaranteeing the close performance of the original with feedback scheme. It also indicates that the two feedback schemes JIB_DSICED3 and JIB_DSICED3_PF are useful not only for short-packet transmission but also for high region of SNR_A.

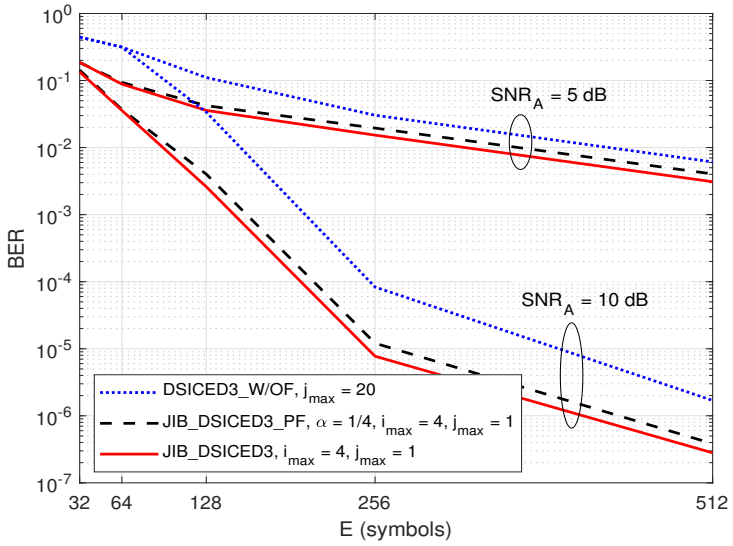


Fig. 3.20: BER of DSICED3_W/OF, JIB_DSICED3, and JIB_DSICED3_PF schemes versus E; $R = 1/2$, $\alpha = 1/4$; $\rho_{AA} = 30$ dB.

Furthermore, the BER performance of proposed JIB_DSICED3_PF versus different number of αE symbols and total E symbols for different number of taps of intended channel $(4, 6, 7, 8)$ are shown in Fig. 3.21 and Fig. 3.22, respectively. The results emphasize that it is also less sensitive to the BER performance of partial feedback version for the number of αE symbols for feedback in channel estimation, regardless of the number of taps of intended channel and total E symbols. Consequently, $\alpha = 1/4$ is a sufficient choice for the proposed JIB_DSICED3_PF scheme.

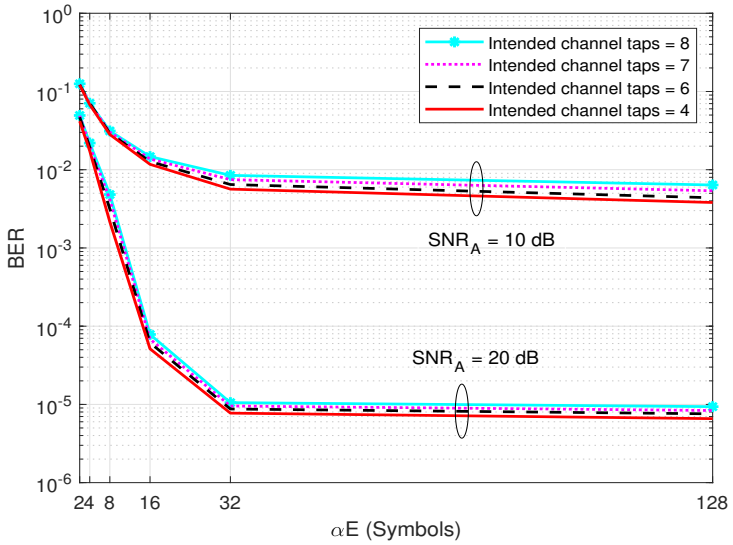


Fig. 3.21: BER of JIB_DSICED3_PF scheme versus αE for different number of intended channel taps; $R = 1/2$, $i_{max} = 4$, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

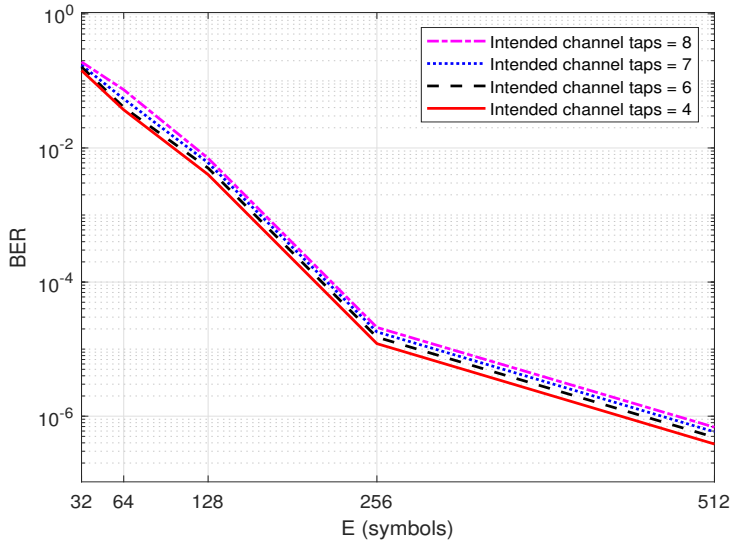


Fig. 3.22: BER of JIB_DSICED3_PF scheme versus E for different number of intended channel taps; $R = 1/2$, $\alpha = 1/4$; $\rho_{AA} = 30$ dB and $SNR_A = 10$ dB.

3.6.3 Processing Time and Computational Complexity

In this section, we compare the processing time and the computational complexity of the with feedback scheme JIB_DSICED3, partial feedback scheme JIB_DSICED3_PF and the conventional without feedback scheme DSICED3_W/OF. The processing time is a crucial metric for performance evaluation since it quantifies the effectiveness of the algorithm, especially in 5G short-packet transmissions and IoT applications.

A computer with the hardware configuration of Intel (R) Core (TM) I5-10500 CPU @ 3.10 GHz (12 CPUs), memory 16 GB of RAM is used with MATLAB version 2020b. Because the maximum number of decoding iterations is fixed at the same value to achieve the optimal (best) results in all cases of SNR_A, the processing time for different levels of SNR_A is nearly the same. Therefore, this configuration is only used to calculate the processing time to obtain the MSE and BER at the particular SNR_A level, $SNR_A = 10$ dB. For the simulation parameters, we set $E = 128$ symbols, $\alpha = 1/4$, $\rho_{AA} = 30$ dB, 10^6 transmission frames, $i_{max} = 4$ and $j_{max} = 1$ for two feedback schemes JIB_DSICED3 and JIB_DSICED3_PF and $j_{max} = 20$ for without feedback scheme DSICED3_W/OF. Based on the results in Table 3.2, it can be seen that the with feedback scheme JIB_DSICED3 takes less roughly three times than the without feedback scheme DSICED3_W/OF. This is mainly due to the decrease in the number of iterations in the SPA decoding, which takes up most of the processing time of the decoder process in 5G QC-LDPC encoded FD short-packet transmissions [90, 93]. Indeed, when $j_{max} = 1$ in two feedback schemes compared with $j_{max} = 20$ in without feedback scheme and these schemes are using the same algorithms for channel estimation (with RLS algorithm) and decoding process (with SPA algorithm).

Furthermore, it is obvious that the processing time is improved in the partial feedback

Table 3.2: Processing Time of DSICED3_W/OF, JIB_DSICED3 and JIB_DSICED3_PF schemes

Algorithm	**Processing time (in minute)**	**Ratio respects to (DSICED3_W/OF)**
DSICED3_W/OF scheme	615.6	1
JIB_DSICED3 scheme	181.2	0.294
JIB_DSICED3_PF scheme	116.8	0.189

scheme JIB_DSICED3_PF compared to the with feedback scheme JIB_DSICED3 due to a significant reduction in the feedback number of symbols for channel estimation processes (see Figs. 3.15 and 3.16 where the partial feedback scheme with $\alpha E = 32$ symbols or $\alpha = 1/4$ requires 4 iterations to achieve the same saturation performance as the with feedback scheme JIB_DSICED3). Thus, a nearly one-third or ~ 0.35 times reduction of the JIB_DSICED3_PF scheme compared to JIB_DSICED3 is shown in Table 3.2.

Moreover, the computational complexity of three schemes is analyzed based on the summation of the asymptotic behavior of the number of operations including additions, subtractions, multiplications, divisions, XOR operation based on [125, 129–133]. Because of the identity and symmetric at the transmitter side, this chapter only considers calculating the total asymptotic behavior of the number of operations at the receiver side. The formulas for calculating the relative number of computations for each operation are summarized in detail in Table. 3.3, where $\bar{u_v}, \bar{u_c}$ are denoted the average degree of the variable nodes, and the average degree of the check nodes of the parity check matrix $\mathbf{H}$, respectively.

Table 3.3: Summary of asymptotic behavior of the number of operations

Operation	**Asymptotic behavior of the number of operations**
Modulation/ Demodulation	$\mathcal{O}(N)$
Interleaver/De-Interleaver	$\mathcal{O}(N)$
Encoding	$\mathcal{O}(N)$
SPA decoding	$j_{max}.((2.N.\bar{u_v} + (N-K)(3.\bar{u_c} - 1))) \approx \mathcal{O}(N.\bar{u_v}.j_{max})$
RLS algorithm	$\mathcal{O}(N^2)$

Fig. 3.23 shows the asymptotic behavior of the number of operations for different values of symbols E, which is used to calculate the total asymptotic behaviors of operations to obtain the MSE and BER at the particular SNR_A level, $p_B/\sigma_A^2 = 10$ dB. For the simulation parameters, we set $\alpha = 1/4$, $\rho_{AA} = 30$ dB, 10^6 transmission frames, $i_{max} = 4$ and $j_{max} = 1$ for two feedback schemes JIB_DSICED3 and JIB_DSICED3_PF and $j_{max} = 20$ for the without feedback scheme DSICED3_W/OF. It can be seen that the proposed two feedback schemes JIB_DSICED3 and JIB_DSICED3_PF have less cost for completing the computation than the conventional without feedback scheme DSICED3_W/OF.

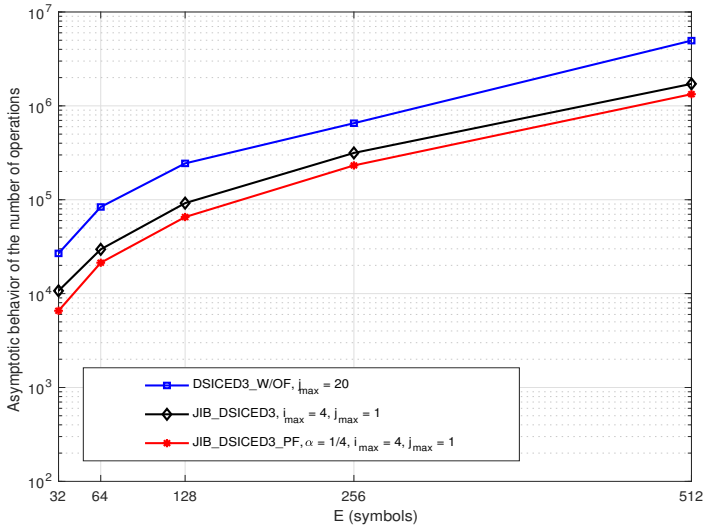


Fig. 3.23: Asymptotic behavior of the number of operations of DSICED3_W/OF, JIB_DSICED3, JIB_DSICED3_PF schemes versus E; $R = 1/2$, $\alpha = 1/4$, $SNR_A = 10$ dB, $\rho_{AA} = 30$ dB.

3.7 Conclusion

This chapter proposed a joint iterative blind channel estimation and decoding algorithm in FD transmissions via feedback of estimated channel and decoded message with DSIC process, named JIB_DSICED3 scheme. The novelty of the proposed algorithm is to take advantage of iterative algorithms of 5G QC-LDPC in the decoding process to design simultaneous channel estimation and decoding in each iteration to efficiently cancel the SI component and improve the simultaneous channel estimation and decoding in the next iteration. To reduce the processing time, this chapter further proposed a partial feedback scheme where only a partial number of modulated symbols in feedback loop (with $\alpha = 1/4$) are used for channel estimations process, named JIB_DSICED3_PF scheme. The numerical results showed that the proposed algorithm outperforms the conventional algorithm DSICED3_W/OF in terms of MSE, BER, processing time, computational complexity, and SI sensitivity. More specifically, the proposed algorithm requires only four iterations to achieve the saturation performance and achieve a significant reduce of BER, e.g. about 10^{-1} decrease in BER of the proposed algorithm over the conventional one for the intended SNR_A of 10 dB. When the self-interference to noise ratio ρ_{AA} increases 10 dB, the proposed algorithm tends to be less sensitive to the level of SI, as it requires an increase of 0.5 dB of the intended SNR_A to maintain the same BER. All these results indicate the practical use of the proposed algorithm in short-packet FD transmissions for IoT applications and green communications with strict requirements of low-latency and energy efficiency. However, at low region of the SNR, higher number of residual errors of decoding consequently degrades the overall performance of the proposed blind scheme. Hence, using a few pilot symbols can avoid this consequent decoding error. Therefore, a semi-blind scheme with the addition of pilot symbols to the transmitter will be considered in the next chapter.

Chapter 4

Joint Semi-Blind Self-Interference Cancellation and Equalization Processes in 5G QC-LDPC Encoded Short-packet Full-Duplex Transmissions

In this chapter, we propose a joint semi-blind SI cancellation and equalization processes in 5G QC-LDPC encoded short-packet FD transmissions. To avoid the effect of channel estimation processes when using short-packet transmissions with blind algorithm in low region of SNR, this semi-blind algorithm is developed by taking into account only a small number of pilot symbols, which is added to the intended information sequence after modulation process and using for the feedback loop of the estimation of the channels. The results show that this semi-blind algorithm not only achieves nearly optimal performance but also significantly improves the performance of MSE, BER, processing time, and computational complexity. The results of this study highlight the potential efficiency of this joint semi-blind iterative algorithm for 5G & Beyond and/or IoT transmissions practical scenarios. The content of this chapter has been published in the paper:

- Bao Quoc Vuong, Roland Gautier, Ta Quang Hien, Nguyen Lap Luat, Anthony Fiche, Mélanie Marazin: *"Joint Semi-Blind Self-Interference Cancellation and Equalization Processes in 5G QC-LDPC-Encoded Short-Packet Full-Duplex Transmissions"*, belongs to the Special Issue Full-Duplex Wireless Communication in MDPI Sensors 22(6): 2204 (March 2022).

4.1 Introduction

As introduced in Chapter 3 and many researches, in comparison to the infinite packet transmission system, short-length packet transmission is considered a foundation of physical layer security in 5G and IoT applications to ensure robustness of artificial noise or self-jamming techniques [120]. Last but not least, when the 5G is going to the final stage, the 6G has received a lot of interest from the researcher community because it is aimed at supporting more diversified applications. Therefore, both uRLLC and mMTC techniques should be explored deeply in order to fully support for short-packet communications not only to provide an efficiency data transmission but also to ensure communication reliability [134, 135]. In recent years, the authors in [114, 123] have proposed joint algorithms for channel estimation, SI cancellation, and signal detection in FD transmission. However, the results are not satisfactory in short-packet transmission because the systems require a lot of data symbols to obtain a good second-order statistic of the received signal. Therefore, the constraint of time, bandwidth and power efficient approaches for short-packet transmission in FD transmission have to be considered carefully. Indeed, a potential technique for channel estimation and data detection in short-packet FD transmission is to consider semi-blind channel estimation, which is the concatenation between the known pilot symbols and the information symbols in order to form a transmitted sequence [50, 60]. For example, the authors in [50] proposed an iterative semi-blind receiver with Carrier Frequency Offset (CFO) for uRLLC in short-packet FD transmission systems. In addtion, a semi-blind FD Amplify-and-Forward (AF) relay system with adaptive SI processing assisted by Independent Component Analysis (ICA) is proposed to improve low latency and high reliability in IoT communications [61]. Furthermore, a new Semi-blind Minimum Mean Square Error (SMMSE) technique is also proposed to further suppress the residual SI power in FD mmWave Massive MIMO Systems [62]. Their proposed algorithm is used to overcome the problem of ergodic capacity and outage capacity as well as the length of pilot symbols, which are the most challenges in short-packet transmission.

In this chapter, to overcome the poor performance of blind algorithm at low region of the SNR as shown in Chapter 3, a semi-blind algorithm is proposed for joint iterative SI cancellation and intended channel estimation in 5G QC-LDPC encoded FD short-packet transmissions in the digital domain. The principle of semi-blind is taking into account only a small number of pilot symbols and the feedback of the estimate of the channel to achieve a nearly optimal performance and efficient uses in practical scenarios. Throughout this chapter, the performance evaluation of the proposed algorithms is also based on four metrics: MSE, BER, processing time, and computational complexity. The contributions of this chapter can be summarized as follows:

- We propose a joint iterative semi-blind SI cancellation and channel estimation in 5G QC-LDPC encoded short-packet FD transmissions by adding pilot symbols,

compared to the blind method in Chapter 3 without adding pilot symbols;

- We characterize the out-performance of the system with proposed algorithm compared to the proposed blind algorithm in Chapter 3 and the conventional blind and semi-blind without feedback algorithms. In particular, this semi-blind technique can significantly improve the performances of MSE and BER, while requiring only the addition of a few pilot symbols for the channel estimation feedback processes.

- We point out that the time consumption and computational complexity of the proposed algorithm is lower than the conventional algorithm, which is suitable for IoT applications and green communications.

The remaining of this chapter is organized as follows. Section 4.2 briefly describes the system model of FD transmissions with the conventional DSIC algorithm, the encoder and decoder processes. Section 4.3 proposes the joint iterative semi-blind channel estimation and decoding algorithm. Then, the numerical results and comparisons with the conventional algorithm in terms of MSE and BER performances are presented in Section 4.4. Last but not least, a comparison between the blind with feedback scheme proposed in Chapter 3 and the semi-blind with feedback scheme in terms of MSE, BER, processing time, and computational complexity is also illustrated in Section 4.5. Finally, some highlights and conclusions will be discussed in Section 4.6.

4.2 Conventional SB_DSICED3_W/OF Scheme

This section presents the conventional semi-blind without feedback algorithm, the encoder and the decoder processes at the transmitter and receiver, respectively.

4.2.1 System Model

Let us consider a short-packet transmission model between two users, A and B, which are equipped with two antennas for simultaneously transmitting and receiving information in FD modes as shown in Fig. 4.1. The transmission mechanism is almost similar to the transmission model in Section 3.2. The unique difference is that an equalizer using the RLS algorithm is applied with the assistance of pilot symbols, which are added into the information message modulated sequence on the transmitting side of user B, to estimate the intended channel and obtain the equalized signal. After channel estimation and equalizer processes, the binary output $\hat{x}_{SoI}[k]$ of the signal of interest can be obtained from the equalized signal $\tilde{y}''_A[n]$ via pilot removing, demodulation, de-interleaving and decoding processes in the decoder process. The flow diagram of the encoder and decoder processes will be presented in detail in Section 4.2.2.

This transmission model is called the conventional algorithm, and we name it as Semi-Blind Digital Self-Interference Cancellation, Equalization, Demodulation, De-interleaving

and Decoding Without Feedback (SB_DSICED3_W/OF) scheme. Next, we will briefly introduce the encoder and decoder processes of the transmitted signal with adding pilot symbols $x'_A(t)$ and $x'_B(t)$ from user A and B, and on the receiver side of user A, respectively.

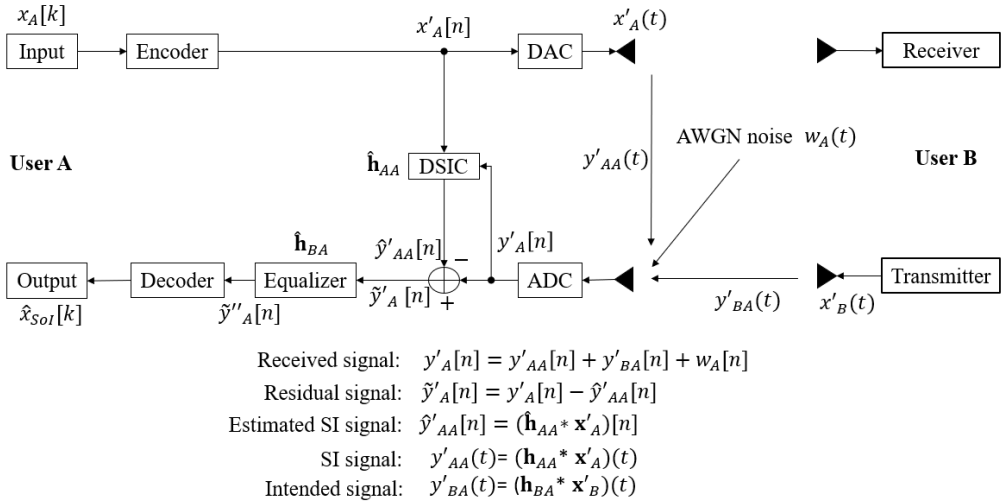


Fig. 4.1: SISO FD transmission with conventional SB_DSICED3_W/OF scheme.

4.2.2 Encoder and Decoder Process

The construction of encoder and decoder processes is described in Fig. 4.2. On the transmitting side, the binary input signal $x_A[k]$, where $k \in [1, K]$, is encoded using the (N, K) 5G LDPC encoding process to form a code word of length N. The encoding technique between the exponent parity check matrix $\mathbf{H}$ and the information bit sequence is based on Section 1.2.1.4, where N and K denote the length of the code word and the length of the information, respectively. Then, the obtained code word will be interleaved and modulated by using QPSK modulator with the modulation order $M = 4$, in order to form the signal $x_A[n]$, where $n \in [1, E]$ and $E = N/log_2(M)$. Then, the βE known pilot symbols will be added to the message sequence after the modulation process to form the transmitted signal $x'_A[n]$ with a length of $E' = (1 + \beta)E$, where β denotes the coefficient of the pilot symbols. Finally, this signal will pass to the DAC process to convert to the continuous time signal $x'_A(t)$. The encoder process for the signal of interest $x_B[k]$ is similar to that of the SI signal $x_A[k]$ to obtain $x'_B(t)$, which is transmitted to user A.

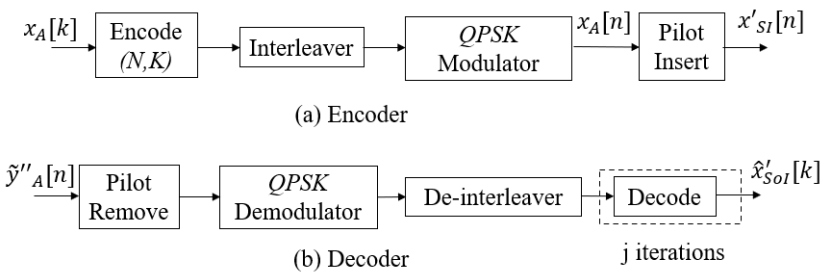


Fig. 4.2: Encoder and decoder process.

At the received side, the residual signal after DSIC process $\tilde{y}'_A[n]$ will pass through the equalization with RLS algorithm to estimate the intended channel and obtain the equalized signal $\tilde{y}''_A[n]$. Then, the pilot symbols are removed from this signal before going to the QPSK demodulator and de-interleaver processes to form the LLR belief sequence. Then, this LLR sequence will be used for decoding and decisions. To obtain the estimated binary input signal $\hat{x}_{SoI}[k]$ from node B, the SPA based on Section 1.2.1.5 is applied at node A, which is the message that passes between the check nodes and the symbol nodes to guess the bits transmitted from each other in each iteration j until it reaches the maximum number of decoding interactions j_{max}.

4.3 Proposed Joint Iterative Semi-Blind Scheme

In this section, we propose a joint iterative semi-blind channel estimation and decoding scheme version, named Joint Iterative Semi-Blind Digital Self-Interference Cancellation, Equalization, Demodulation, De-interleaving and Decoding (JSIB_DSICED3) scheme, and shown in Fig. 4.3.

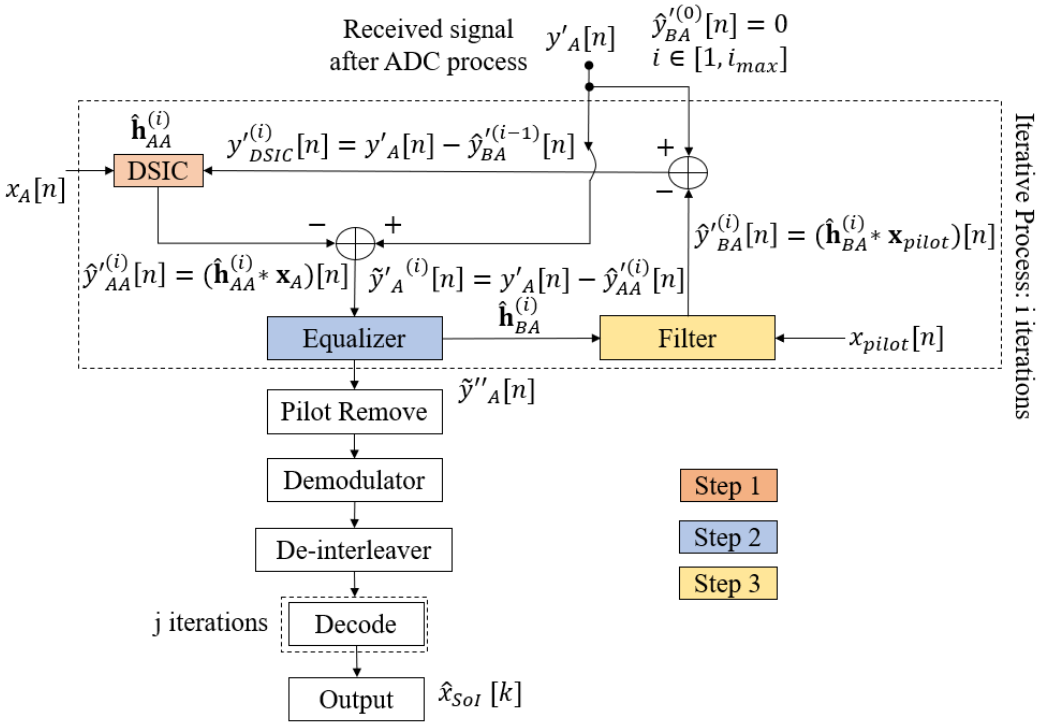


Fig. 4.3: SISO FD transmission with the proposed JISB_DSICED3 scheme.

The process of the semi-blind algorithm is shown in Fig. 4.3, in which the proposed scheme is developed on the principle that the processes of SI cancellation and intended channel estimation can benefit from each other via the feedback loop after each joint iteration decoding i, where $i \in [1, i_{max}]$. We emphasize that, different from iteration j performing iteration decoding in the conventional algorithm in Section 4.2, iteration i

in the proposed algorithm is for joint SI cancelation and the estimation of the intended propagation channel via feedback. Based on the knowledge of pilot symbols transmitted by node B, the system does not need to perform the temporary decoding and encoding for feedback. Indeed, it only performs the feedback loop by these pilot symbols $\mathbf{x}_{pilot}$. Let us denote βE, where $\beta \in [0, 1]$ is the ratio coefficient of the pilot symbols, is the number of pilot symbols that are added to the E modulated symbols of the information signal sequence after the encoding, interleaving, and modulation process to form the $E' = (1 + \beta)E$ symbols for a transmission frame. It should be noted that for $i = 1$ (first iteration), a first SI cancellation and intended channel estimation is performed for all E' symbols, which is used to avoid a significant number of errors and obtain a good level of convergence when starting the process of iterative algorithm. For the remaining iterations, that is, $i \in [2, i_{max}]$, the system only performs the feedback loop using the known pilot symbols $\mathbf{x}_{pilot}$ with a length of βE. After the system completes the joint iterative process, i.e. $i = i_{max}$, the estimations of the SI channel and intended channel are used to fully cancel the SI component and achieve the equalized signal, respectively. Then, these pilot symbols are removed from the equalized signal $\tilde{y}''_A[n]$ and the system continues to perform the decoder process by the demodulation, de-interleaver and decoding processes, in order to achieve the intended message sequence $\mathbf{x}_{SoI}$. It should be noted that performing many j iterations in decoding process will increase latency and complexity because of high computational complexity in the SPA decoding process [136]. Therefore, when we achieve the best channel estimation ($i = i_{max}$), the proposed scheme will only consider one decoding iteration ($j_{max} = 1$) in the SPA decoding algorithm to obtain good results, because if we include more decoding iterations j, it does not significantly improve performance, as shown in Chapter 3. The graphical presentation of proposed joint iterative semi-blind SI cancellation and equalization processes algorithm can be shown in Fig. 4.4 and the proposed algorithm with three main steps is summarized in Algorithm 4.1.

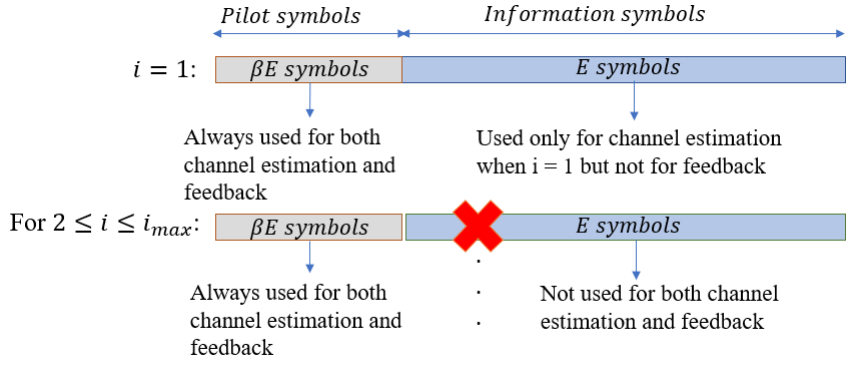


Fig. 4.4: Graphical presentation for joint iterative semi-blind scheme.

In the following sections, the simulation results and discussions of the proposed semi-blind scheme JISB_DSICED3 will be illustrated.

Algorithm 4.1: Iterative part of the proposed Joint Iterative Semi-Blind Scheme

Inputs : $\mathbf{y}'_A, \mathbf{x}'_A, i_{max}, \mathbf{x}_{pilot}, \beta, K, N, M$;
Outputs : $\hat{\mathbf{h}}_{AA}^{(i_{max})}, \hat{\mathbf{h}}_{BA}^{(i_{max})}$;
Initialization: $\hat{\mathbf{y}}'_{BA}{}^{(0)} = \mathbf{0}$, $\hat{\mathbf{h}}_{AA}^{(0)} = \mathbf{0}$, $\hat{\mathbf{h}}_{BA}^{(0)} = \mathbf{0}$;
for $i = 1$ *to* i_{max} **do**
  if $i = 1$ **then**
    /* Perform Step 1 and Step 2 for all of $E' = (1+\beta)E$ symbols and $E = N/log_2(M)$ symbols, where β is the pilot symbol coefficient, N is the code word length, M is the modulation order */
    for $n = 1$ *to* E' **do**
      Step 1: SI channel estimation and DSIC process
      Estimate: $\hat{\mathbf{h}}_{AA}^{(i)}$;
      Calculate: $\tilde{y}'_A{}^{(i)}[n] = y'_A[n] - \hat{y}'_{AA}{}^{(i)}[n] = y'_A[n] - (\hat{\mathbf{h}}_{AA}^{(i)} * \mathbf{x}'_A)[n]$;
      Step 2: Intended channel estimation
      Estimate: $\hat{\mathbf{h}}_{BA}^{(i)}$;
    end
  else
    /* Perform Step 1 and Step 2 for only $\beta E = \beta N/(log_2(M)$ known pilot symbols, where β is the pilot symbols coefficient, N is the code word length, M is the modulation order */
    for $n = 1$ *to* βE **do**
      Step 1: SI channel estimation and DSIC process
      Estimate: $\hat{\mathbf{h}}_{AA}^{(i)}[n]$;
      Calculate: $\tilde{y}'_A{}^{(i)}[n] = y'_A[n] - (\hat{\mathbf{h}}_{AA}^{(i)} * \mathbf{x}'_A)[n]$;
      Step 2: Intended channel estimation
      Estimate: $\hat{\mathbf{h}}_{BA}^{(i)}$;
    end
  end
  if $i < i_{max}$ **then**
    /* Perform Step 3 for only βE known pilot symbols, where β is the pilot symbols coefficient */
    for $n = 1$ *to* βE **do**
      Step 3: Feedback loop
      Using $\mathbf{x}_{pilot}$ to form feedback loop to get $\hat{\mathbf{y}}'^{(i)}_{BA}$;
      Calculate: $\hat{y}'_{BA}{}^{(i)}[n] = (\hat{\mathbf{h}}_{BA}^{(i)} * \mathbf{x}_{pilot}^{(i)})[n]$;
      Update: $y'_{DSIC}{}^{(i+1)}[n] = y'_A[n] - \hat{y}'_{BA}{}^{(i)}[n]$;
    end
  else
    Go to return
  end
end
return $\hat{\mathbf{h}}_{AA}^{(i_{max})}, \hat{\mathbf{h}}_{BA}^{(i_{max})}$.

4.4 Comparison Between Semi-blind Without/With Feedback Schemes: SB_DSICED3_W/OF versus JISB_DSICED3

In this section, the performances of the proposed semi-blind scheme JISB_DSICED3, compared to the conventional scheme SB_DSICED3_W/OF, are illustrated in terms of MSE, BER, processing time, and computational complexity using Monte Carlo simulations on MATLAB. The effects of different code rates of 5G QC-LDPC codes are compared. Moreover, different number of taps of SI channel and intended channel are also considered. These channels are generated independently in each transmission frame. Based on the background noise as reference and without loss in generality, we further denote $\rho_{AA} = p_A/\sigma_A^2$ as the self-interference to noise ratio and $SNR_A = p_B/\sigma_A^2$ as the SNR at user A, where p_{SI}, p_B and σ_A^2 are the power of SI signal, intended signal and background noise at user A, respectively. It is also noticed that the semi-blind without feedback scheme SB_DSICED3_W/OF needs up to 20 iterations ($j_{max} = 20$) to converge and to reach the saturation floor, while the feedback scheme JISB_DSICED3 requires only 4 joint iterations and 1 decoding iterations ($i_{max} = 4, j_{max} = 1$) to reach that floor, similar with the blind feedback scheme JIB_DSICED3 in Chapter 3. The choice of the number of pilot symbols will be arbitrary set at $\beta E = 4$ symbols for both MSE and BER performances, and it will be clearly proven later in Section 4.4.2. The simulation parameters are summarized in Table. 4.1.

Table 4.1: Simulation Specifications

Parameter	**Value**
Code word length (N)	64, 128, 256, 512, 1024
Information length (K)	32, 64, 128, 256, 512
Code rate	1/3, 1/2, 2/3, 3/4, 5/6
Modulation scheme	QPSK ($M = 4$)
Frame length after modulation ($E = N/log_2(M)$)	32, 64, 128, 256, 512
Number of transmission frames	10^6
SI channel taps	3, 4, 5, 6
Intended channel taps	4, 6, 7, 8
Pilot symbols ratio coefficient β	1/4, 1/8, 1/16, 1/32, 1/64
Index of joint iterations in JISB_DSICED3 scheme	$i_{max} = 4, j_{max} = 1$
Index of iteration of SPA decoding in SB_DSICED3_W/OF	$j_{max} = 20$

4.4.1 MSE Performances

First, Fig. 4.5 shows the MSE of JISB_DSICED3 versus SNR_A for different number of taps of SI channel, where $\beta E = 4$ symbols and the number of taps of intended channel is fixed at 4 taps. The result indicates that the variation of the number of taps of SI channel does not affect the SI channel estimation process. Similarly, Fig. 4.6 illustrates

the MSE of the intended channel versus SNR_A for various numbers of taps of the intended channel. The MSE performance is also less sensitive to the change in the number of taps of intended channel. Therefore, it can be seen that the $\beta E = 4$ symbols are suitable choice for the JISB_DSICED3 scheme in MSE performances. For the rest of this chapter, the SI channel is fixed with 3 taps, while the intended channel is fixed with 4 taps for further implementations.

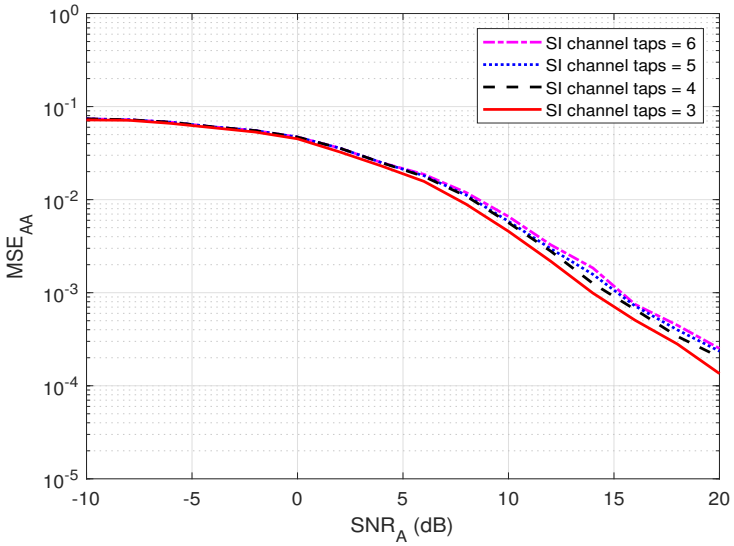


Fig. 4.5: MSE_{AA} of JISB_DSICED3 scheme versus SNR_A for different values of SI channel tap; $R = 1/2$, $i_{max} = 4$, $\rho_{AA} = 30$ dB, $\beta E = 4$ symbols and $E = 128$ symbols.

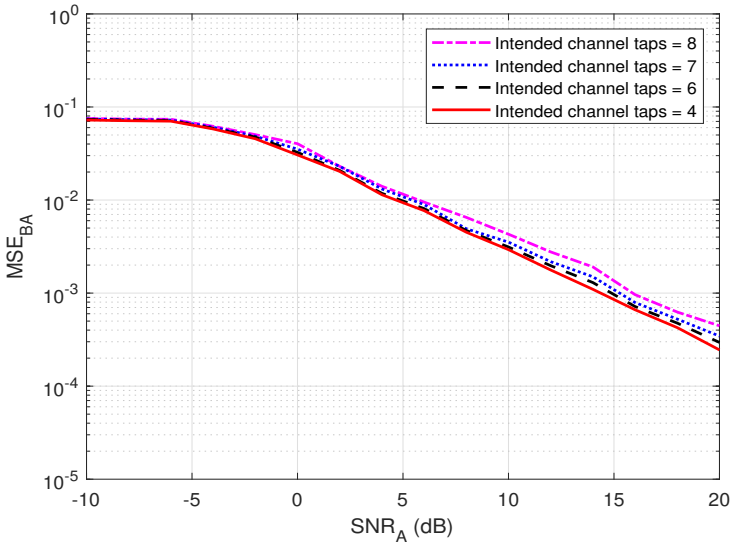


Fig. 4.6: MSE_{BA} of JISB_DSICED3 scheme versus SNR_A for different values of intended channel tap; $R = 1/2$, $i_{max} = 4$, $\rho_{AA} = 30$ dB, $\beta E = 4$ symbols and $E = 128$ symbols.

In this subsection, we also introduce the best performance scheme, as a benchmark to characterize the optimality of the semi-blind scheme JISB_DSICED3 in terms of MSE and for performance comparison, corresponding to a lower bound using the proposed JISB_DSICED3 considering that all $E' = (1 + \beta)E$ are known. So, in this limit case, all intended E symbols are also known, not only the pilot symbols for both channel estimations and feedback.

Fig. 4.7 and Fig. 4.8 compare the MSEs of two schemes such as JISB_DSICED3 and SB_DSICED3_W/OF with the best performance scheme versus SNR_A, for the SI channel and the intended channel, respectively. First, the results show that the feedback scheme JISB_DSICED3 has a better performance compared to the conventional scheme SB_DSICED3_W/OF, especially in high SNR_A ($SNR_A > 5$ dB). Furthermore, the semi-blind feedback scheme JIB_DSICED3 shows a slightly better result in low SNR_A ($SNR_A < 5$ dB), compared to the conventional scheme SB_DSICED3_W/OF due to the improvement after the feedback loops. The results also show that the semi-blind scheme JISB_DSICED3 is nearly optimal, as its performance is pretty close to that of the best performance scheme, i.e. assuming that the intended symbols are known at the receiver.

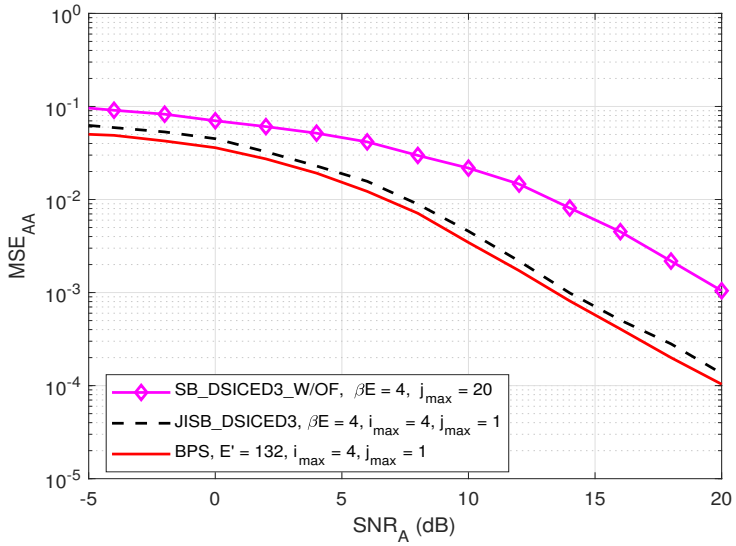


Fig. 4.7: MSE_{AA} versus SNR_A; $R = 1/2$, $i_{max} = 4$, $j_{max} = 20$, $\rho_{AA} = 30$ dB, $\beta E = 4$ symbols and $E = 128$ symbols.

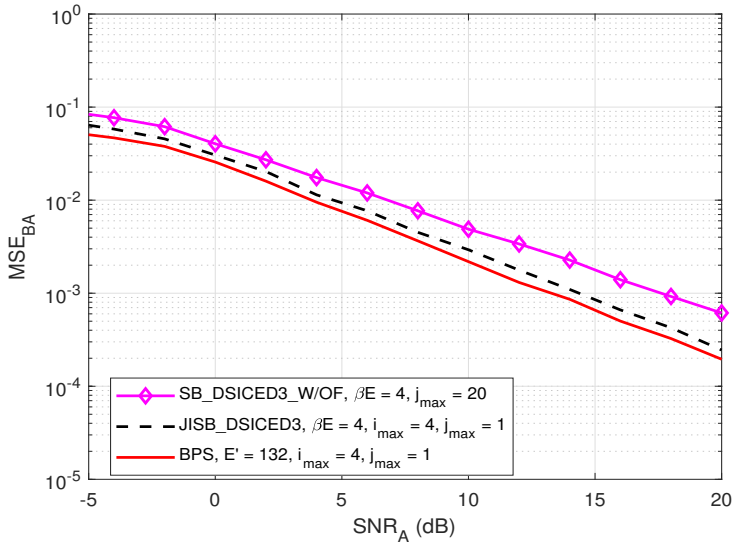


Fig. 4.8: MSE_{BA} versus SNR_A; $R = 1/2$, $i_{max} = 4$, $j_{max} = 20$, $\rho_{AA} = 30$ dB, $\beta E = 4$ symbols, and $E = 128$ symbols.

4.4.2 BER Performances

First, the effects of different code rates such as $R \in \{1/3, 1/2, 2/3, 3/4, 5/6\}$ on the BER performance of SB_DSICED3_W/OF and JISB_DSICED3 schemes have been implemented in Figure 4.9 and Figure 4.10, respectively.

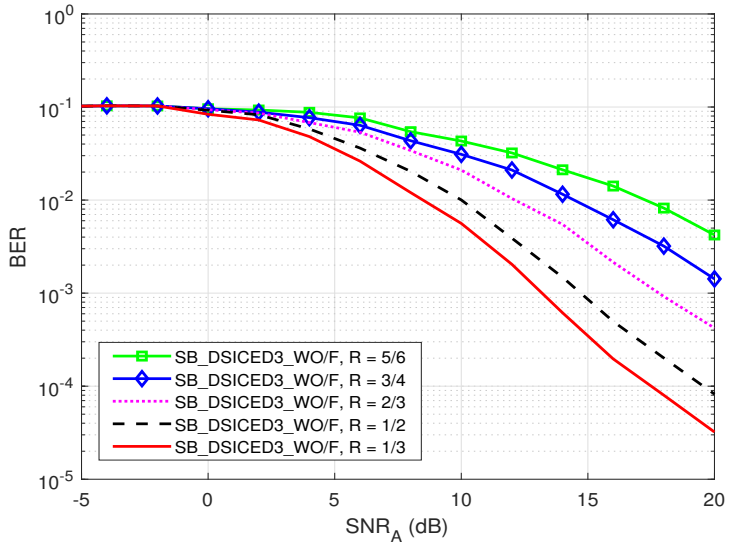


Fig. 4.9: BER of SB_DSICED3_W/OF scheme versus SNR_A for different code rates R ; $j_{max} = 20$, $\rho_{AA} = 30$ dB, $\beta E = 4$ symbols and $E = 128$ symbols.

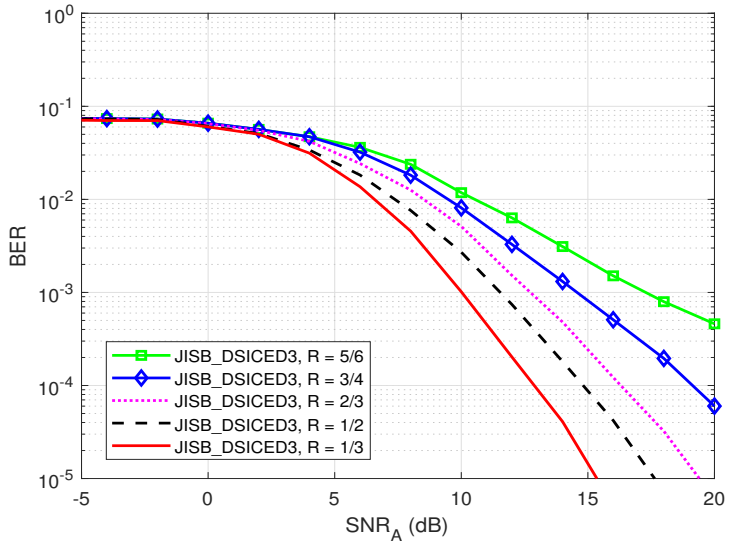


Fig. 4.10: BER of JISB_DSICED3 scheme versus SNR_A for different code rates R; $i_{max} = 4$, $j_{max} = 1$, $\rho_{AA} = 30$ dB, $\beta E = 4$ symbols and $E = 128$ symbols.

Similarly to the blind algorithms in Chapter 3, the relative behavior of the algorithm with feedback JISB_DSICED3 with respect to the code rate behaves in the same way as the conventional algorithm without feedback SB_DSICED3_W/OF, that is, when the code rate R is increased, the BER performance will decrease. For all code rates, the proposed semi-blind feedback scheme JISB_DSICED3 has better performance than the conventional algorithm without feedback SB_DSICED3_W/OF. For the rest of this chapter, the code rate is fixed at 1/2 as a particular example in order to illustrate the out performance of

proposed with feedback algorithm JISB_DSICED3 over the conventional without feedback algorithm SB_DSICED3_W/OF.

Fig. 4.11 and Fig. 4.12 show BER of the semi-blind scheme versus the number of pilot symbols βE for different values of SNR_A and number of taps of intended channel $(4, 6, 7, 8)$, respectively, where $\rho_{AA} = 30$ dB and $E = 128$ symbols. Fig. 4.13 shows the BER of the JISB_DSICED3 scheme versus E for different number of taps of intended channel. It can be seen that only minimum four pilot symbols ($\beta E = 4$ symbols or $\beta = 1/32$) are needed for the semi-blind channel estimation to achieve the saturation level regardless of number of taps of intended channel used. Thus, the minimum required pilot symbols makes the semi-blind scheme favorable in practical implementations for short-packet transmission.

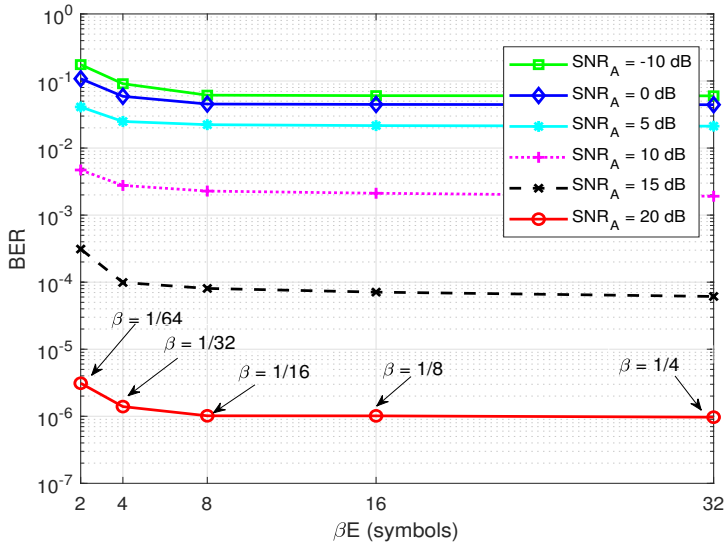


Fig. 4.11: BER of JISB_DSICED3 scheme versus βE for different values of SNR_A; $R = 1/2$, $i_{max} = 4$; $\rho_{AA} = 30$ dB and $E = 128$ symbols.

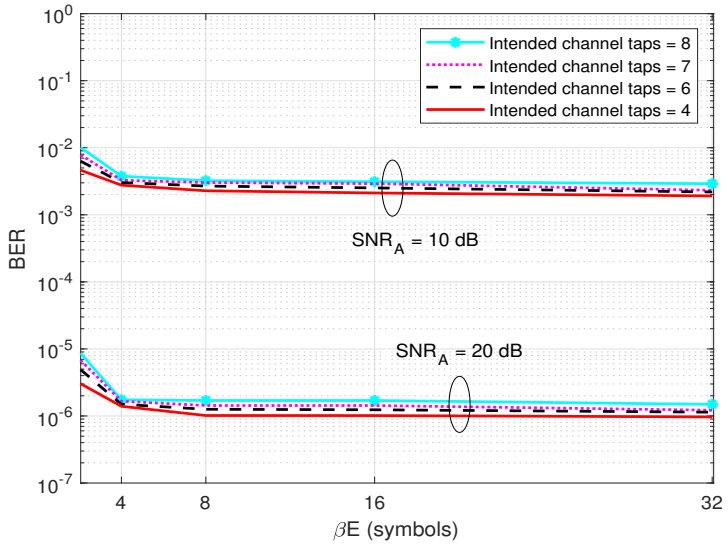


Fig. 4.12: BER of JISB_DSICED3 scheme versus βE for different values of intended channel tap; $i_{max} = 4$; $R = 1/2$, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

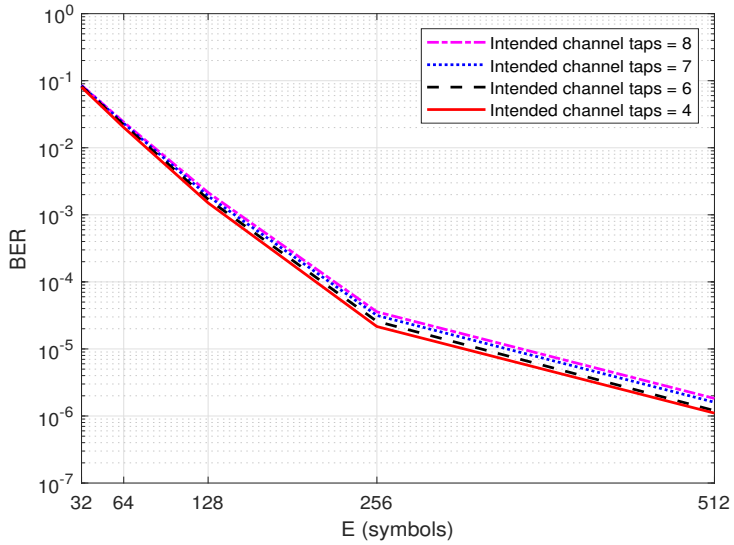


Fig. 4.13: BER of JISB_DSICED3 scheme versus E for different values of intended channel tap; $R = 1/2$, $i_{max} = 4$;$SNR_A = 10$ dB, $\rho_{AA} = 30$ dB and $\beta E = 4$ symbols.

Fig. 4.14 compares the BERs of the semi-blind scheme JISB_DSICED3 and the conventional semi-blind without feedback scheme SB_DSICED3_W/OF versus SNR_A, for different values of $E \in \{32, 64, 128\}$ symbols, $\beta E = 4$ symbols and $\rho_{AA} = 30$ dB. In fact, the increase of E symbols leads to the increase of BER performance on both schemes, due to the good level of convergence in channel estimations with more symbols. We observe that, at low SNR_A (≤ 5 dB), BER of the JISB_DSICED3 scheme is slightly lower than that of the SB_DSICED3_W/OF scheme regardless of total number symbols. However, at high SNR_A (≥ 5 dB), the semi-blind scheme JISB_DSICED3 shows its out-performance with faster convergence. This is due to the use of minimum four pilot symbols, which are added to the information sequence, for better performance in the semi-blind scheme.

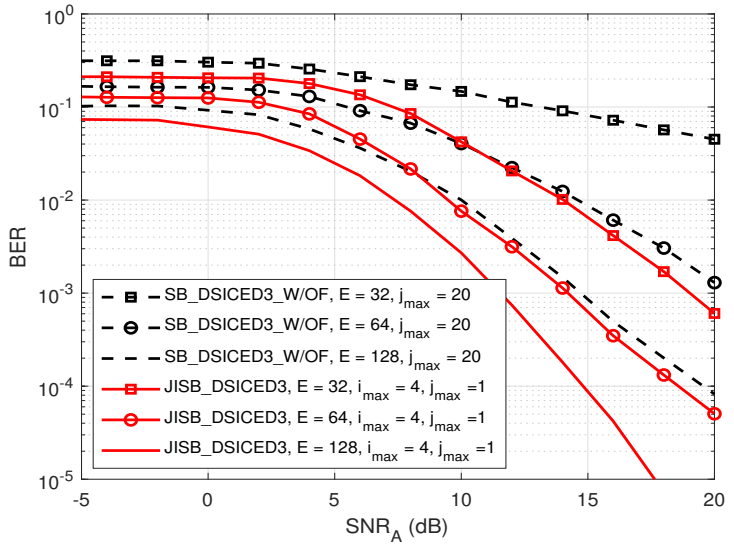


Fig. 4.14: BER of SB_DSICED3_W/OF and JISB_DSICED3 schemes versus SNR_A; $R = 1/2$, $\beta E = 4$ symbols, and $\rho_{AA} = 30$ dB.

Last but not least, Fig. 4.15 shows the BERs performance versus different values of E symbols, where $\beta E = 4$ symbols. The result indicates that the semi-blind scheme JISB_DSICED3 has better performance than the conventional semi-blind without feedback scheme SB_DSICED3_W/OF, regardless of total number of transmitted symbols and SNR_A level. It also shows that when the number of symbols E and the value of SNR_A increase, the gaps between two schemes are larger, which is clearly shown when $SNR_A = 10$ dB. This is due to the advantage of having known pilot symbols and feedback loops. Therefore, it indicates that the semi-blind scheme JISB_DSICED3 is an optimum solution not only for short-packet transmission, but also for a low region of SNR_A, which are the operation characteristics of IoT transmission and green communication.

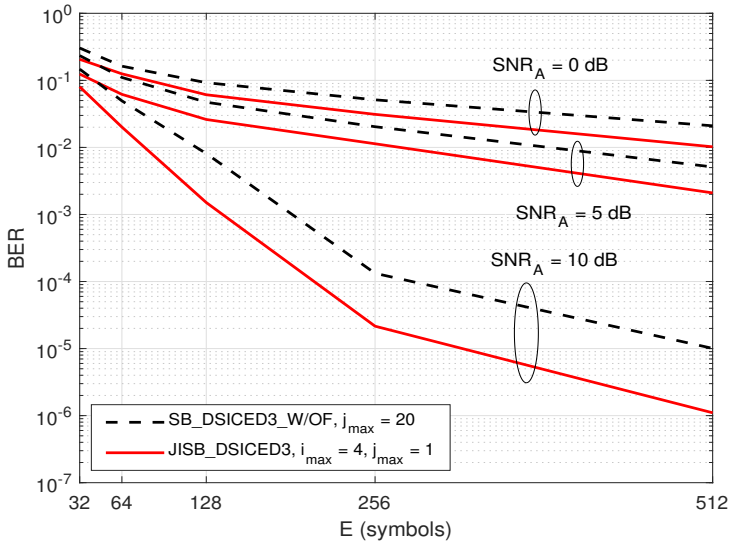


Fig. 4.15: BER of SB_DSICED3_W/OF and JISB_DSICED3 schemes versus E; $R = 1/2$, $\beta E = 4$ symbols and $\rho_{AA} = 30$ dB.

4.5 Comparison Between Blind and Semi-blind Feedback Schemes: JIB_DSICED3 vs JISB_DSICED3

In this section, a comparison between the blind and semi-blind feedback schemes, JIB_DSICED3 (which is shown in Chapter 3) and JISB_DSICED3, is illustrated in terms of MSE, BER performances, processing time and computational complexity, where the simulation specifications are defined similar to Section 3.4 and Section 4.4.

4.5.1 MSE Performances

Fig. 4.16 and Fig. 4.17 compare MSEs between the proposed blind scheme JIB_DSICED3, the proposed semi-blind scheme JISB_DSICED3 and the best performance scheme versus SNR_A, for the SI channel and the intended channel, respectively. It can be seen that

the semi-blind scheme JISB_DSICED3 outperforms the blind scheme JIB_DSICED3, especially at low SNR_A ($SNR_A \leq 0$ dB). However, in high region of SNR_A ($SNR_A \geq 0$ dB), the results show that the semi-blind scheme JISB_DSICED3 and the blind scheme JIB_DSICED3 are nearly optimal as their performances are pretty close to that of the best performance scheme. It is also noticed that they have better performance than two without feedback schemes, as discussed in Section 3.4.1 and Section 4.4.1, respectively.

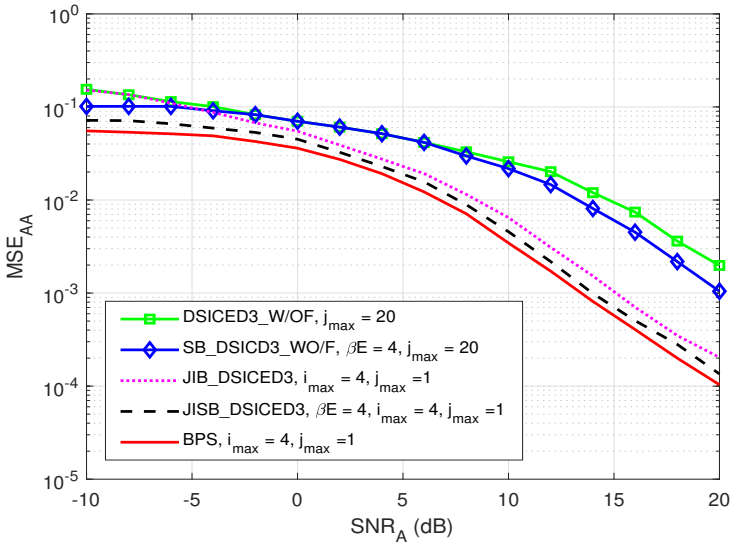


Fig. 4.16: MSE_{AA} of JIB_DSICED3 and JISB_DSICED3 schemes versus SNR_A; $R = 1/2$, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

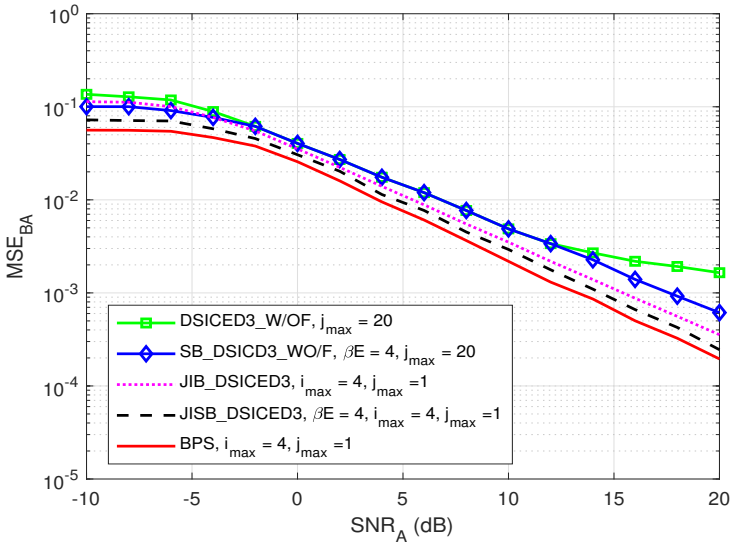


Fig. 4.17: MSE_{BA} of JIB_DSICED3 and JISB_DSICED3 schemes versus SNR_A; $R = 1/2$, $\rho_{AA} = 30$ dB and $E = 128$ symbols.

4.5.2 BER Performances

Fig. 4.18 compares the BERs of the semi-blind scheme JISB_DSICED3 and the blind scheme JIB_DSICED3 versus SNR_A, for different values of E symbols, where $\beta E = 4$ symbols, $E = \{32, 64, 128\}$ symbols, and $\rho_{AA} = 30$ dB. It can be seen that, at high SNR_A (≥ 0) dB, the BER of the JISB_DSICED3 scheme is slightly lower than that of the JIB_DSICED3 scheme regardless of the total number of transmitted symbols, as also shown in Fig. 4.19 for SNR_A at 5 and 10 dB. This is due to the trade-off of four pilot symbols for better performance in the semi-blind scheme. However, at low $SNR_A \leq 0$ dB, the semi-blind scheme JISB_DSICED3 shows its out-performance and interestingly, its BER is much lower compared to the blind scheme JIB_DSICED3 for larger total number of transmitted symbols, E, i.e. when $SNR_A = 0$ dB as also shown in Fig. 4.19. This is due to the advantage of having known pilot symbols to avoid the consequent decoding error in the feedback loop. It is noted that the proposed blind and semi-blind feedback schemes can improve significantly the BER performance compared to the conventional blind/semi-blind without feedback schemes, as shown in Section 3.4.2 and Section 4.4.2. Furthermore, we consider the relationship between signal to noise ratio SNR and energy per bit to noise power spectral density ratio E_b/N_0, where the ratio between number of information symbols (E) and the total symbols after adding pilots (E'), as following:

$$E_b/N_0 = (SNR).(\frac{E}{E'}); \tag{4.1}$$

Therefore, in Fig. 4.18, the BER's curve of semi-blind scheme JISB_DSICED3 need to be shifted to the right hand side by E/E' (dB), i.e, when $E = 32$ symbols, it needs to shifted by $32/36 = 0.8$ (dB), and it also approximately closed to the blind scheme JIB_DSICED3. However, in this thesis, we only use SNR instead of E_b/N_0 to simplify the notation of signal to noise ratio because the characteristic of system performance is not changed too much, that is the out-performance of semi-blind scheme in low region of SNR compared to blind scheme and both of them have better performance in high region of SNR compared to the conventional without feedback schemes.

4.5.3 Processing Time and Computational Complexity

In this section, we compare the processing time and computational complexity of the proposed blind scheme JIB_DSICED3 and the proposed semi-blind scheme JISB_DSICED3. In this case, a computer is used with the same hardware configuration as blind algorithm in Section 3.6.3. So, this configuration is used to calculate the processing time to achieve the MSE and BER at the particular SNR_A level, $SNR_A = 10$ dB. For the simulation parameters, we set the self-interference to noise ratio $\rho_{AA} = 30$ dB, 10^6 transmission frames, $E = 128$ symbols and $\beta = 1/32$ ($\beta E = 4$ symbols), $i_{max} = 4$ and $j_{max} = 1$

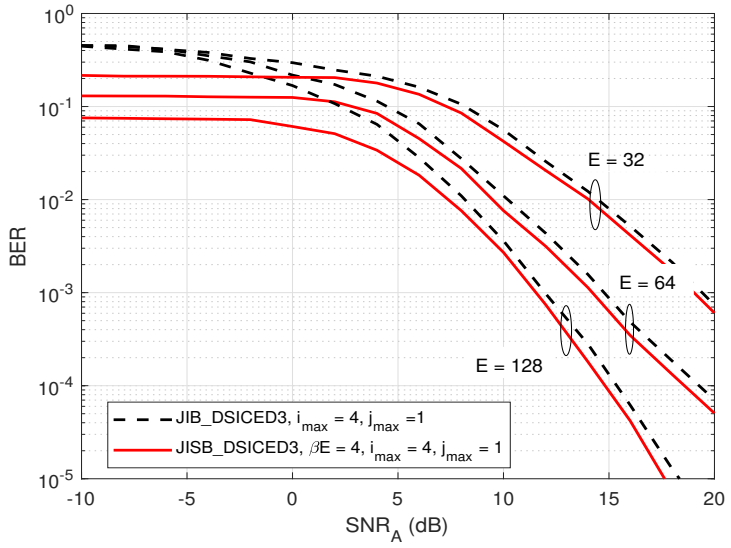


Fig. 4.18: BER of JIB_DSICED3 and JISB_DSICED3 schemes versus SNR_A; $R = 1/2$, $\rho_{AA} = 30$ dB and $\beta E = 4$ symbols.

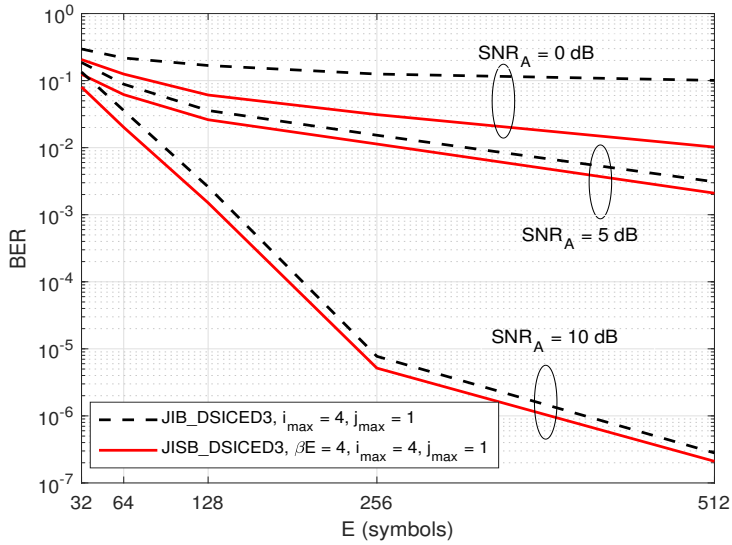


Fig. 4.19: BER of JIB_DSICED3 and JISB_DSICED3 schemes versus E; $R = 1/2$, $\rho_{AA} = 30$ dB.

for the blind/semi-blind schemes (JIB_DSICED3, JISB_DSICED3) and $j_{max} = 20$ for the blind/semi-blind without feedback schemes (DSICED3_W/OF, SB_DSICED3_W/OF).

Based on the results in Table 4.2, we observe that the semi-blind scheme JISB_DSICED3 can significantly reduce the processing time and shows the fastest result because temporary decoding and encoding are not required in the feedback loop and the number of iterations in the SPA decoding process is also reduced, which takes less roughly 10 times compared to the semi-blind without feedback scheme SB_DSICED3_W/OF. This is because the semi-blind scheme only needs one decoding iteration ($j_{max} = 1$) to obtain a good result when achieving the best value of channel estimations, while the semi-blind without feedback scheme SB_DSICED3_W/OF needs up to 20 iterations ($j_{max} = 20$)

Table 4.2: Processing Time of SB_DSICED3_W/OF, DSICED3_W/OF, JIB_DSICED3 and JISB_DSICED3 schemes

Algorithm	**Processing time (in minute)**	**Ratio respects to (SB_DSICED3_W/OF)**
SB_DSICED3_W/OF scheme	617.5	1
DSICED3_W/OF scheme	615.6	0.996
JIB_DSICED3 scheme	181.2	0.293
JISB_DSICED3 scheme	62.3	0.101

to converge and to reach the saturation floor. Furthermore, the processing time of semi-blind scheme JISB_DSICED3 is less than nearly 3 times compared to the blind scheme JIB_DSICED3 because it does not require to perform the temporary decoding, re-encoding, re-interleaving and re-modulation processes for feedback loop.

Moreover, the computational complexity of four schemes is computed based on the summation of total asymptotic behavior of the number of operations as Table. 3.3 in Section 3.6.3. Because of the identity and symmetric at the transmitter side, this chapter also only considers calculating the total asymptotic behavior of the number of operations at the receiver side.

Fig. 4.20 shows the number of computations versus various values of symbols E, which is used to calculate the total asymptotic behavior of the number of operations to obtain the MSE and BER at the particular SNR_A level, $SNR_A = 10$ dB. For the simulation parameters, we set $\beta E = 4$ symbols, $\rho_{AA} = 30$ dB, 10^6 transmission frames, $i_{max} = 4$ and $j_{max} = 1$ for the proposed blind/semi-blind feedback schemes (JIB_DSICED3, JISB_DSICED3) and $j_{max} = 20$ for the conventional blind/semi-blind without feedback scheme (DSICED3_W/OF, SB_DSICED3_W/OF). The result indicates that the proposed semi-blind feedback scheme JISB_DSICED3 requires less cost for completing the computation than the blind feedback scheme JIB_DSICED3 and the conventional blind/semi-blind without feedback schemes (DSICED3_W/OF, SB_DSICED3_W/OF). It is due to the known pilot symbols for feedback loops and the requirement of fewer iterations on the decoding step. Therefore, this result emphasizes the practical implementation of the scheme in 5G short-packet transmissions, especially in IoT transmissions and green communications with low power consumption.

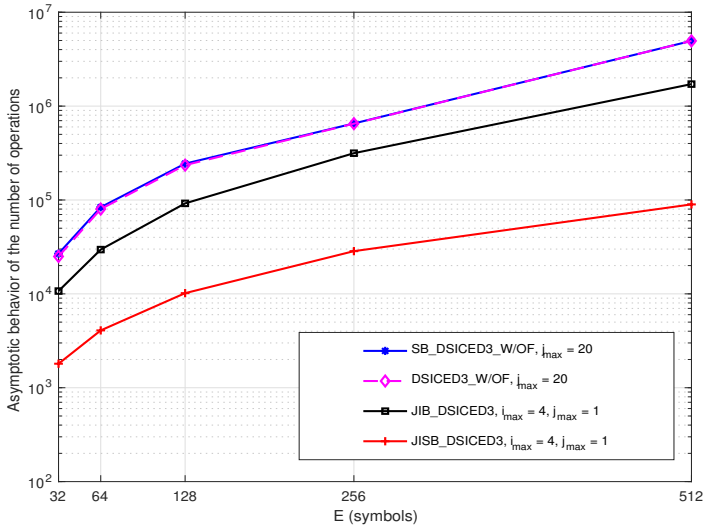


Fig. 4.20: Asymptotic behavior of the number of operations of SB_DSICED3_W/OF, DSICED3_W/OF, JIB_DSICED3 and JISB_DSICED3 schemes versus E; $R = 1/2$, $\beta E = 4$ symbols, $SNR_A = 10$ dB and $\rho_{AA} = 30$ dB.

4.6 Conclusion

This chapter proposed a joint iterative semi-blind SI cancellation and intended channel estimation in 5G QC-LDPC encoded short-packet FD transmissions, via feedback of the known pilot symbols, named JISB_DSICED3 scheme. The innovation of the proposed algorithm is to take advantage of known pilot symbols and iterative algorithms to design simultaneous SI cancelation and the estimated intended channel to efficiently cancel the SI component and improve the estimation of the simultaneous channel in the next iterations. This semi-blind algorithm adds only a minimum of four pilot symbols to the information symbols while not requiring the feedback of temporary decoded messages. The numerical results showed that the proposed semi-blind algorithm JISB_DSICED3 is nearly optimal and efficiently increases the performance of the MSE and BER. The significant reduction in processing time and computational complexity of the semi-blind feedback algorithm JISB_DSICED3 is impressive, as it only requires the feedback of the channel estimate for $i_{max} = 4$ iterations and only one ($j_{max} = 1$) decoding iteration, where the decoding algorithm has prohibitive computational cost. All these results indicate the efficient use of this semi-blind feedback algorithm, especially since the use or the insertion of these pilot symbols does not in practice really lead to a real loss of data rate because they are already generally required for time and frequency synchronization. Last but not least, the choice between semi-blind JISB_DSICED3 and blind JIB_DSICED3 schemes should be based on the applications and purposes. They can significantly reduce the processing time and computational complexity, compared to the conventional without feedback schemes. Both are possible solutions for short-packet FD transmission, which are the operation characteristics of IoT transmissions and green communications. All proposed schemes

and their performance are summarized in the Table. 4.3. Indeed, the conventional blind and semi-blins without feedback algorithms do not satisfy the requirement of short-packet transmissions in terms of MSE, BER, processing time and complexity performances. In contrast, both semi-blind JISB_DSICED3 and blind JIB_DSICED3 schemes are appreciated solutions for short-packet FD transmission. The advantages and disadvantages of each scheme are shown in Table. 4.4, where the blind scheme work well on high region of SNR but it shows a worst result in low region of SNR. Therefore, semi-blind scheme is introduced to overcome the problem of low region of SNR, but it requires adding of pilot symbols. Consequently, the use of these schemes are mostly depended on various applications and purposes.

In the next chapter, the application of the proposed blind and semi-blind algorithms on the PLS of wiretap FD short-packet transmission will be considered.

Table 4.3: All of proposed schemes and their performances.

Scheme	DSIC	MSE		BER		Time	Complexity
		Low SNR	High SNR	Low SNR	High SNR		
Blind w/o feedback (DSICED3_WO/F)	✓ (only for long-packet)	✗	✗	✗	✗	✗	✗
Semi-blind w/o feedback SB_DSICED3_WO/F	✓ (only for long-packet)	✗	✗	✗	✗	✗	✗
Blind scheme JIB_DSICED3	✓	✗	✓	✗	✓	✓	✓
Partial blind scheme JIB_DSICED3_PF	✓	✗	✓	✗	✓	✓	✓
Semi-blind scheme JISB_DSICED3	✓	✓	✓	✓	✓	✓	✓

Table 4.4: Advantages and Disadvantages of Proposed Blind and Semi-blind Schemes.

Scheme	Advantage	Disadvantage
Blind algorithm (JIB_DSICED3)	• Good performance in high SNR • Do not require pilot symbols	• Low performance in of SNR
Semi-blind algorithm (JISB_DSICED3)	• Good performance in both high and low SNR	• Require pilot symbols

Chapter 5

Secrecy Coding Analysis of Short-packet Full-Duplex Transmissions with Joint Iterative Channel Estimation and Decoding Processes

In this chapter, a combination of joint iterative channel estimation and decoding technique and self-jamming technique in the presence of an eavesdropper has been implemented and evaluated, to enhance the PLS area for FD short-packet transmissions. Indeed, the legitimate receiver and eavesdropper can simultaneously receive the intended signal from the transmitter and broadcast a self-jamming or jamming signal to the other. In case of passive eavesdropper, the blind channel estimation with feedback scheme, which is introduced in Chapter 3, is applied, where the temporary estimation of intended channel and decoded message are fed back to improve both channel estimation and decoding processes. Only blind algorithm is implemented in case of passive eavesdropper because it achieves sufficient performance results and does not require adding pilot symbols as the semi-blind algorithm. In case of active eavesdropper, the semi-blind algorithm, which is introduced in Chapter 4, must be taken into account by trading four pilot symbols and only requiring the feedback for channel estimation processes because of its robustness in low region of SNR. The content of this chapter has been published in:

- Bao Quoc Vuong, Roland Gautier, Anthony Fiche, Melanie Marazin and Cristina Despina-Stoian: *Secrecy Coding Analysis of Short Packet Full-Duplex Transmissions with Joint Iterative Channel Estimation and Decoding Processes.*, belongs to the Special Issue Physical-Layer Security for Wireless Communications in MDPI Sensors 22(14): 5257 (July 2022).

5.1 Introduction

In recent years, many researchers have focused on secrecy channel coding techniques in the wiretap channel [22, 137–139]. In particular, the authors in [137] evaluated the reliability and security over the flat and fast fading Gaussian wiretap channel for the various LDPC codes construction with the puncturing and scrambling techniques. Furthermore, the authors in [140] used McEliece coding method based on LDPC codes to guarantee both information reliability between intended users and security metric with respect to eavesdropper in PLS. The authors in [138] also studied the combination of LDPC codes and AN by designing the scrambling matrix to reduce the probability of outage and improve PLS. Then, the authors in [139] proposed combining the LDPC codes at the transmitter and an iterative decoding algorithm at the receiver to reduce the security gap in the Gaussian wiretap channel. The obtained results show that their proposed scheme outperforms the punctured scheme in terms of the equivocation rate and the security gap.

As a metric of PLS, the security gap was first introduced in [141], which is calculated as the ratio of the Bit Error Rate (BER) on the linear scale or the difference of the BERs on the log scale achieved by the legitimate receiver and the eavesdropper, to ensure that the legitimate receiver can reliably receive the intended message and maintain security throughout transmission.

Therefore, in this chapter, we propose and implement a new scheme that combines joint iterative channel estimation and decoding using 5G QC-LDPC codes with FD self-jamming of the legitimate receiver to enhance security and reliability, which means that the eavesdropper does not catch the information and the indented information is less affected or corrupted by the jamming signal, respectively, in two scenarios: passive eavesdropper and active eavesdropper. For the rest of this chapter, the performance evaluations of the proposed algorithms are based on three metrics: MSE, BER, and security gap (S_g). The contributions of this chapter can be summarized as follows:

- We evaluate a combination of self-jamming technique with a joint iterative blind or semi-blind channel estimation and decoding for a FD short-packet transmissions in the cases of passive and active eavesdroppers, respectively;

- We characterize that the system developed based on the new proposed algorithms have better performance compared to the conventional without feedback in terms of security metrics;

- We point out that the legitimate receiver are less sensitive to the self-interference from itself as well as the jamming power from the eavesdropper in our approach.

- We emphasize that the proposed algorithms provide a higher robustness not only to the security and reliability factors but also to the power consumption by reducing

the SNR at legitimate receiver for decoding the message, which suits for the short-packet FD IoT transmissions and green communications.

The remaining of this chapter is organized as follows. Section 5.2 briefly describes the general system model of the FD transceiver in the passive/active eavesdropper scenarios and the security gap. Section 5.3 studies the application of the joint iterative blind channel estimation and decoding algorithm at the legitimate receiver in the case of passive eavesdroppers, with numerical results and comparisons with the conventional blind without feedback algorithm. Section 5.4 introduces the system model using semi-blind feedback algorithm in case of active eavesdropper and simulation results. Finally, some highlights and conclusions will be discussed in section 5.5.

5.2 Full-Duplex Transceiver with Passive/Active Eavesdropper Transmission System

5.2.1 General System Model

Considering a short packet FD transmission wiretap channel between three users, such as user B (transmitter), user A (legitimate receiver), and user E (eavesdropper) as shown in Fig. 5.1, where the transmitter is equipped with only one antenna for transmission, while the receiver and the eavesdropper are attached with one transmitter and one receiver antennas to simultaneously receive the intended information message and transmit self-jamming or jamming signals. 5G QC-LDPC codes, which are considered fundamental codes for short-packet uplink and downlink transmissions [80, 82, 95], are used in all transceivers.

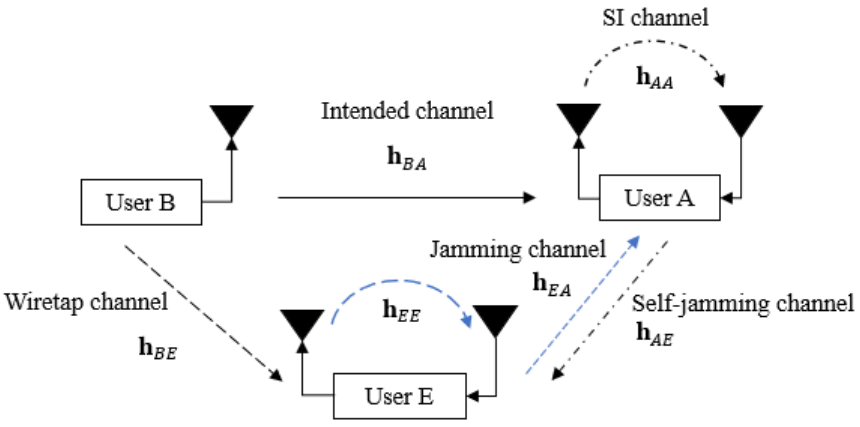


Fig. 5.1: General system model.

At the transmitter, the (N, K) 5G QC-LDPC encoding process is performed as Section 1.2.1.4, where K and N denote the length of information message and code word message, respectively. Let us denote the channel gain between two users and the SI channel gain

of itself as $\mathbf{h}_{XY}$ and $\mathbf{h}_{YY}$, respectively, in which $X \in \{A, B, E\}$ and $Y \in \{A, E\}$, where A, B, E represent user A, user B, and user E, respectively. In this chapter, the SI channel is modeled as quasi-static Rayleigh fading in the digital domain due to the assumption that the LoS component is fully suppressed by antenna and analog cancellation techniques, whereas the residual SI is the nLoS component [63, 75]. Note that $\mathbf{h}_{XY}$ and $\mathbf{h}_{YY}$ are i.i.d complex Gaussian random variables with $\mathcal{CN}(0, 1)$ [77, 111]. Moreover, the transmitted power of each user is denoted as p_X, where $X \in \{A, B, E\}$ and we further denote $\mathbf{w}_Y$ as the complex background noise at user Y with $\mathcal{CN}(0, \sigma_Y^2)$, where $Y \in \{A, E\}$. Based on the background noise as reference and without loss in generality, we further denote $\rho_{XY} = p_X/\sigma_Y^2$ and $\rho_{YY} = p_Y/\sigma_Y^2$, where $X, Y \in \{A, E\}$, as the power to noise ratio provided by the self-jamming or jamming channel from user X to user Y, and the SI channel at user Y, respectively. We also denote $SNR_A = p_B/\sigma_A^2$ and $SNR_E = p_B/\sigma_E^2$ as the SNR at user A and user E, where σ_A^2 and σ_E^2 are the background noise power at user A and user E, respectively.

In this chapter, we assume the following hypotheses:

- In case of passive eavesdropper, only blind channel estimation is used, where there is no knowledge about the channel state information at all communication users;
- In case of active eavesdropper, both blind and semi-blind channel estimation, where all transceivers share a few pilot symbols, are mainly implemented;
- User E knows the parity check matrix $\mathbf{H}$ of user B and performs SPA decoding mechanism; and user E also uses RLS algorithm in DSIC process as user A in case of active eavesdropper;
- Both user A and user E have equal computation capabilities and the location of user E is closed enough to user A to broadcast its jamming signal and is also attacked by the self-jamming signal from user A;
- The channel gains at the receiver and the eavesdropper are constant within a code word and change from one to another in fading channels;
- The impact of hardware impairments on the SI cancellation is not considered (which is outside the scope of this study but essential in practice). Moreover, the problem of synchronization process between the transceivers is also not taken into account. Last but not least, the bit resolution of DAC/ADC is chosen higher enough to bypass the effect of quantization noise, i.e. larger than 6 bits for both DAC/ADC process or the oversampling should be applied in ADC process if the green communications system and IoT applications are considered with low-bit ADC, which was studied in Chapter 2.

- On the one hand, there is an assumption concerning the relative positions of the various transmitters/receivers where we do not take into account the distances between these users and the distance between antennas. In particular, for the case of user A and user E, it seems coherent and acceptable to consider that the powers of the background noises σ_A^2 and σ_E^2 are identical (both users in the same environment). On the other hand, under the assumption of channels without loss (unity mean deviation on all the paths) for $\mathbf{h}_{AA}$ and $\mathbf{h}_{AE}$, it is possible to simplify the notations and to denote in general the self-jamming power to noise ratio as ρ_{SJ} for both self-interference (ρ_{AA}) and self-jamming (ρ_{AE}) channels in case of passive eavesdropper and self-jamming channel from user A to user E ρ_{AE} and jamming channel from user E to user A in case of active eavesdropper. Since in these conditions, we have $\rho_{SJ} = \rho_{AA} = \rho_{AE}$ in case of passive eavesdropper and $\rho_{SJ} = \rho_{AE} = \rho_{EA}$ in case of active eavesdropper, respectively.

5.2.2 Security Gap

In the practical context of the wiretap channel when the short-packet is used for transmission, the typical BER performance criteria is usually used to ensure two aspects of performance such as reliability and secrecy conditions [137]. Let us denote BER_A and BER_E as the average BER of user A and user E, respectively. While $BER_{A,max}$ and $BER_{E,min}$ are the maximum BER that user A can achieve and the minimum BER that user E can obtain, respectively. The reliability condition is hold when $BER_A \leq BER_{A,max}$, which means that the BER of user A should be maintained at low value to enhance the reliability condition. While the security condition is achieved when $BER_E \geq BER_{E,min}$, which means that the BER of user E should be remained at a sufficient high value to guarantee the security.

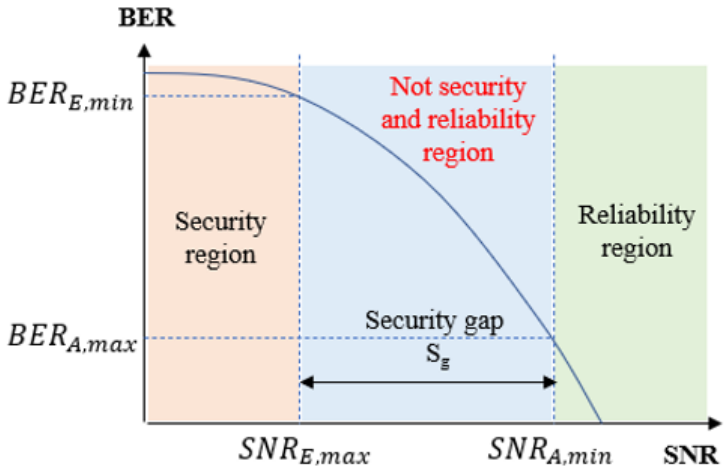


Fig. 5.2: Security gap.

According to [44, 141], the security gap, which is the minimum difference of SNRs (in dB) required to guarantee the legitimate receiver security over the eavesdropper, is calculated as:

$$S_g(dB) = SNR_{A,min} - SNR_{E,max} \tag{5.1}$$

where $SNR_{A,min}$ is the minimum SNR corresponding to $BER_{A,max}$, where user A has to operate to make sure the BER below some reliability thresholds, i.e. $BER_{A,max} = 10^{-5}$, which is sufficient level for practical applications [137]. Similarly, $SNR_{E,max}$ is the maximum SNR corresponding to $BER_{E,min}$ in which the BER of user E can reach approximately a threshold, that is, $BER_{E,min} = 0.5$, which is called the security threshold because user E cannot exactly decode the information message in this region [141].

The graphical presentation of security gap is shown in Fig. 5.2. In fact, the size of the security gap S_g indicates the minimum cost of the difference in SNRs between user A and user E that maintains the possibility of secure communication, the higher values of S_g will lead to a higher transmission cost. Therefore, the objective of this chapter is to reduce the size of the security S_g gap as much as possible and it tends to go to lower than 0 for fully security and reliability factors. In particular, the SNR of user A, $SNR_A = p_B/\sigma_A^2$ (dB) on the main channel must be small enough to ensure that user A can correctly decode the information message from user B assuming the lowest possible power. In contrast, the SNR of user E, $SNR_E = p_B/\sigma_E^2$ (dB) on the wiretap channel must be as large as possible to guarantee that the self-jamming broadcasting from user A still affects the decoding process of user E.

Next, we will consider the first case with passive eavesdropper and the presence of blind feedback algorithm.

5.3 Case I: Passive Eavesdropper

5.3.1 Passive Eavesdropper System Model

The wiretap channel system models with the use of FD self-jamming and passive eavesdropper are shown in Fig. 5.3 and Fig. 5.4 in the case of without feedback and with feedback schemes, respectively. User A is operated in FD transmission mode to simultaneously receive the intended information message from user B and transmit the self-jamming signal to destroy the decoding capacity of user E, while user E just tries to listen and decode the message from user B. The transmission strategy of the proposed scheme is as follows. User B wants to send his encoded message $\mathbf{x}_B$ to the legitimate receiver user A through the main channel $\mathbf{h}_{BA}$, while passive eavesdropper user E tries to listen and decode user B's message through the wiretap channel $\mathbf{h}_{BE}$.

The received signals in the digital domain at user A and user E, respectively, are given

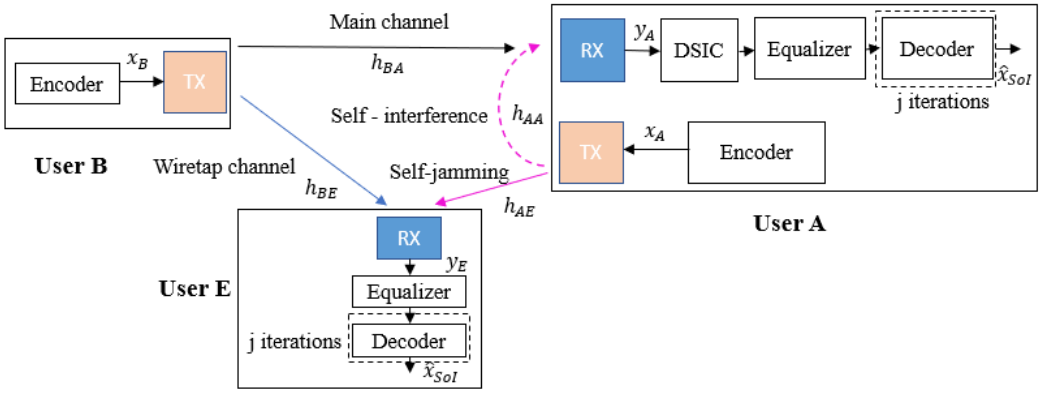


Fig. 5.3: Blind without feedback scheme at user A in case of passive eavesdropper.

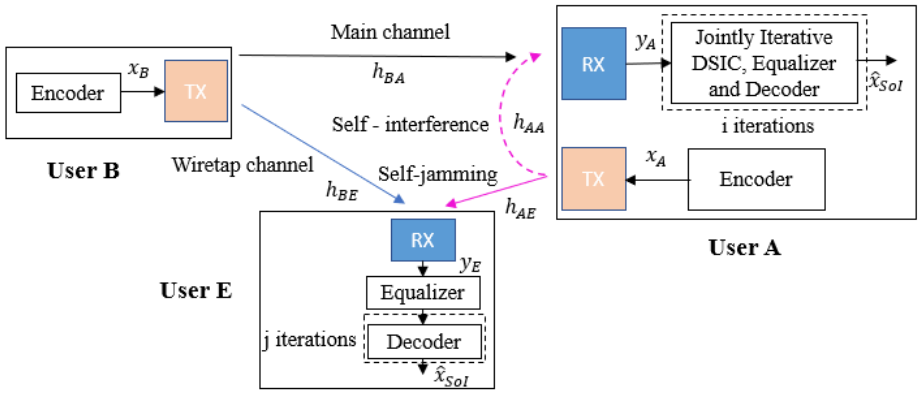


Fig. 5.4: Blind feedback scheme at user A in case of passive eavesdropper.

by the following:

$$\begin{aligned} y_A[n] &= y_{BA}[n] + y_{AA}[n] + w_A[n] \\ &= (\sqrt{p_B}\mathbf{x}_B * \mathbf{h}_{BA})[n] + (\sqrt{p_A}\mathbf{x}_A * \mathbf{h}_{AA})[n] + w_A[n]; \end{aligned} \tag{5.2}$$

$$\begin{aligned} y_E[n] &= y_{BE}[n] + y_{AE}[n] + w_E[n] \\ &= (\sqrt{p_B}\mathbf{x}_B * \mathbf{h}_{BE})[n] + (\sqrt{p_A}\mathbf{x}_A * \mathbf{h}_{AE})[n] + w_E[n]; \end{aligned} \tag{5.3}$$

where $\mathbf{w}_A$ and $\mathbf{w}_E$ are the complex AWGN of the receiver channel of user A and user E, with $\mathcal{CN}(0, \sigma_A^2)$ and $\mathcal{CN}(0, \sigma_E^2)$, respectively, and $(*)$ is the convolution operation.

The legitimate receiver user A obtains the signal $\mathbf{y}_A$ and performs two possible decoding strategies to eliminate the SI component and obtain the estimation of the intended signal $\hat{\mathbf{x}}_{SoI}$. First, it may use a classical blind without feedback scheme (DSICED3_W/OF) where the DSIC and decoding processes are independent, as presented in Fig. 5.3 and studied in Section 3.2 of Chapter 3. Second, it can use a more efficient scheme based on joint iterative blind channel estimation and decoding through feedback, as shown in Fig. 5.4, which we call the blind feedback scheme (JIB_DSICED3), which is studied in Section 3.3 of Chapter 3. Only blind algorithm is implemented in case of passive eavesdropper because it achieves sufficient performance results in high region of SNR, when user A

does not receive jamming signal from user E. At the same time, user E also tries to listen to the transmission over the wiretap channel and only performs the equalization process and the classical SPA decoding process to get the original signal $\mathbf{x}_B$.

5.3.2 Simulation Specifications

To evaluate the secrecy performance of our proposed schemes, MSE, BER, and security gap S_g will be computed by using Monte Carlo simulations on MATLAB. For the rest of this chapter, the MSE of the channel estimation in the intended receiver user A and the eavesdropper user E are given by, respectively, [114]

$$\text{MSE}_{XX} = \mid \mathbf{h}_{XX} - \hat{\mathbf{h}}_{XX} \mid^2, \tag{5.4}$$

$$\text{MSE}_{XY} = \mid \mathbf{h}_{XY} - \hat{\mathbf{h}}_{XY} \mid^2 . \tag{5.5}$$

For 5G QC-LDPC codes, the base graph matrix **BG2** [80] is implemented for all simulations. The SI channel and self-jamming or jamming channel are fixed with 3 channel taps based on Rayleigh distribution with $\mathcal{CN}(0, 1)$. The intended main channel and wiretap are fixed with 4 channel taps and the power of each tap is according to the ITU–R channel model [79]. These channels are generated independently in each transmission frame. The simulation parameters of this paper are summarized in Table. 5.1.

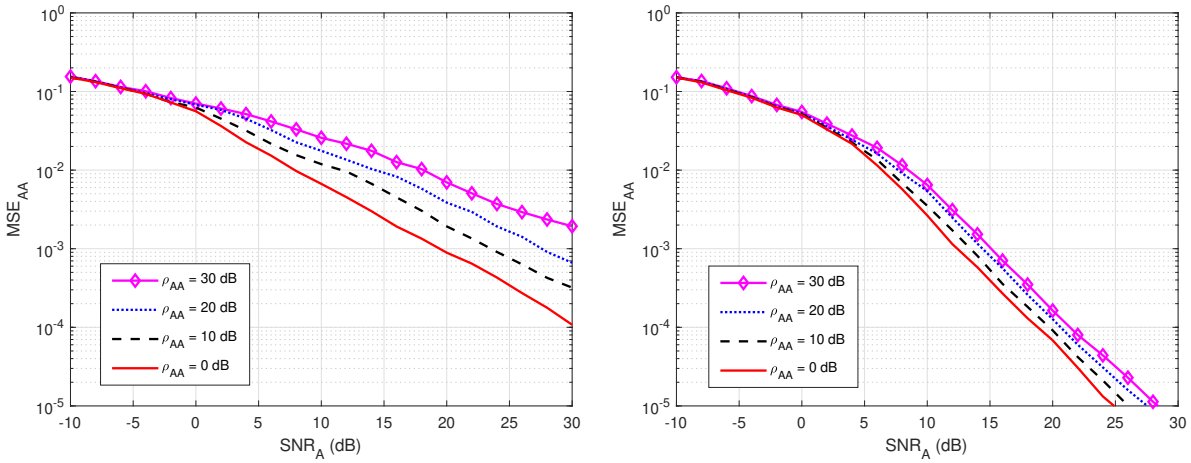
Table 5.1: Simulation Specifications

Parameter	**Value**
Number of transmission frames	10^6
Number of information bits K	128
Number of code word bits N	256
Code rate	1/2
Modulation scheme	QPSK
Number of taps of SI channel h_{AA}, h_{EE}	3
Number of taps of self-jamming channel h_{AE}	3
Number of taps of jamming channel h_{EA}	3
Number of taps of main channel h_{BA}	4
Number of taps of wiretap channel h_{BE}	4
Number of pilot symbols in semi-blind scheme	4
Index of iterations (i_{max}, j_{max}) for feedback schemes	(4,1)
Index of iterations j_{max} for without feedback schemes	20

5.3.3 MSE Performances in Passive Case

5.3.3.1 MSE at the legitimate user A

First, the MSEs of SI channel and intended channel at user A are computed for different values of self-interference to noise ratio ρ_{AA}. For instance, Fig. 5.5a and Fig. 5.5b show the MSEs of the SI channel versus SNR_A in the legitimate receiver user A in case of blind without feedback and blind feedback schemes, respectively. Similarly, Fig. 5.6a and Fig. 5.6b illustrate the MSEs of the intended channel versus the SNR_A at user A in case of blind without feedback and blind feedback schemes, respectively. It can be seen that MSEs significantly increase as the self-interference to noise ratio of user A (ρ_{AA}) increases, and the blind feedback scheme outperforms the without feedback scheme. It can also be observed that the increase of the self-interference to noise ratio of user A has less effect on the blind feedback scheme than the without feedback scheme. For example, maintaining MSE_{AA} at 10^{-3}, when ρ_{AA} increases from 0 to 30 dB, requires an increase of SNR_A only around 2.5 to 3 dB in the blind feedback scheme. However, it requires an increase of roughly 10 dB on the without feedback scheme. Therefore, the use of the blind feedback scheme can significantly improve the channel estimation processes at user A.

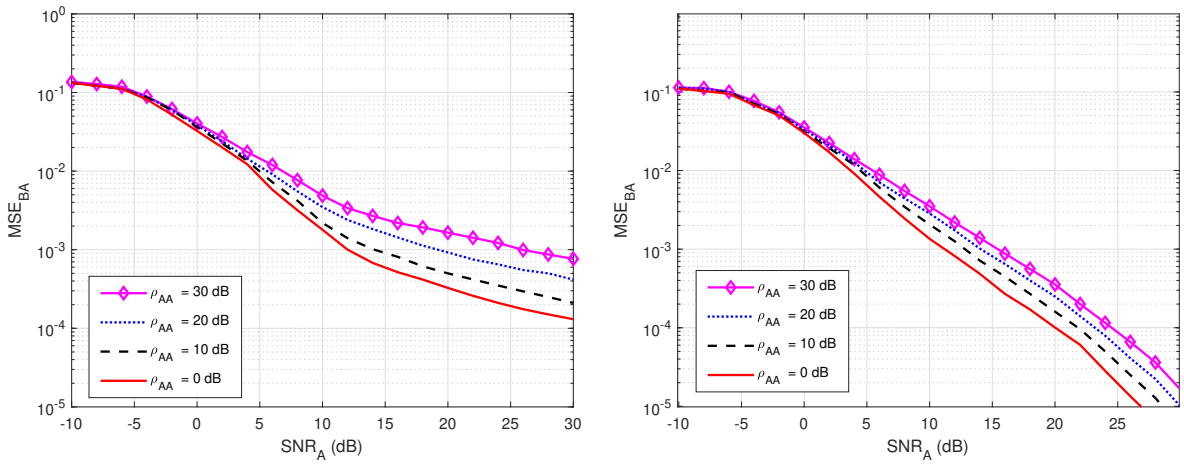


(a) Without feedback. (b) Blind feedback

Fig. 5.5: MSE_{AA} versus SNR_A in case of passive eavesdropper.

5.3.3.2 MSE at the eavesdropper user E

Next, we also evaluate the MSE of the wiretap channel h_{BE} versus the signal-to-noise ratio at the eavesdropper user E (SNR_E) for various values of self-jamming to noise ratio from user A, ρ_{AE}. Based on Fig. 5.7, it can be clearly observed that user E cannot estimate the wiretap channel well, especially in the case of a high value of the self-jamming to noise ratio of user A, ie. ρ_{AE} increases higher than 10 dB. This behavior is due to the lack of knowledge of reference signal of the transmitter as well as the power of self-jamming signal



(a) Without feedback. (b) Blind feedback.

Fig. 5.6: MSE_{BA} versus SNR_A in case of passive eavesdropper.

from user A, which is too greater than the power of intended signal. So, we can conclude that user E cannot accurately estimate the wiretap channel in passive mode.

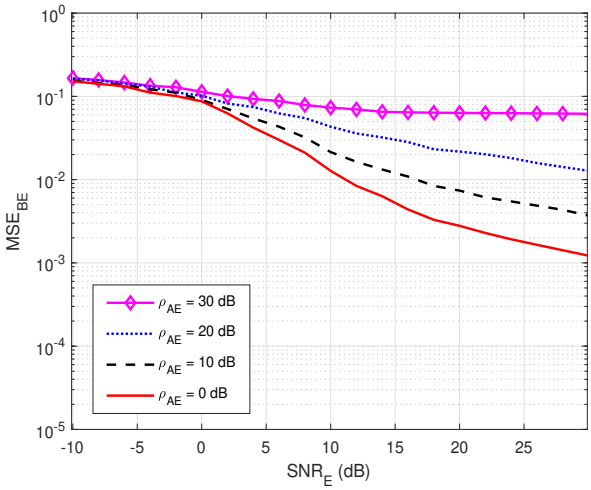


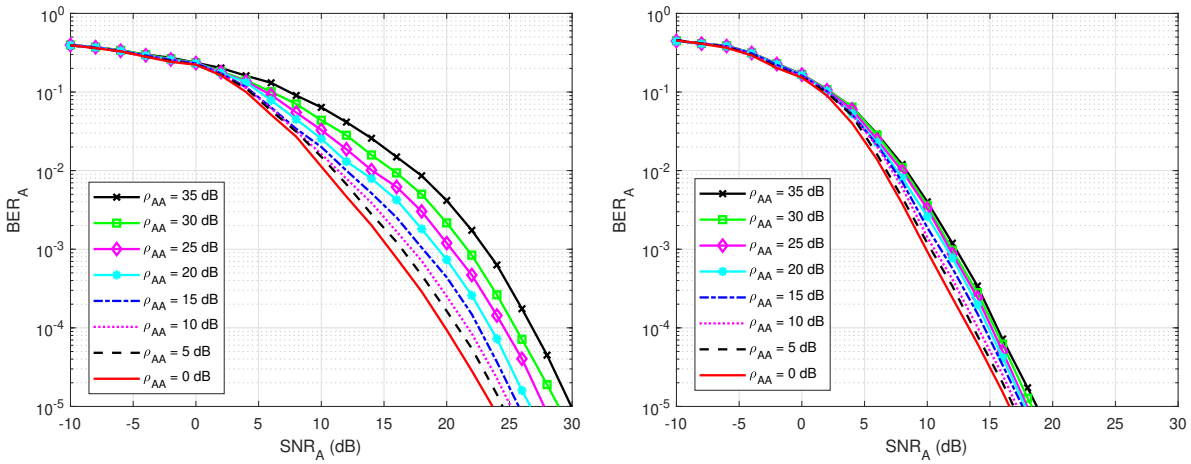
Fig. 5.7: MSE_{BE} versus SNR_E in case of passive eavesdropper.

5.3.4 BER Performances in Passive Case

5.3.4.1 BER at the legitimate receiver user A

BER performances versus SNR_A of user A, for different values of the self-interference to noise ratio of user A (ρ_{AA}) are presented in Fig. 5.8a and Fig. 5.8b for both without feedback and blind feedback scheme, respectively. We can observe that self-interference to noise ratio also significantly impacts on the BER performance, i.e. BER increases as the ρ_{AA} increases and the rise of BER is bigger for larger SNR_A. It also shows an interesting result that when maintaining $BER_A = 10^{-5}$ and increasing the self-interference to noise

ratio ρ_{AA} from 0 to 30 dB, the blind feedback scheme needs about 2 to 3 dB in SNR_A to obtain that BER, while the without feedback scheme requires larger than 5 dB in SNR_A to achieve comparable results. Therefore, in the passive eavesdropper case, the increase of self-interference to noise ratio has less effect on the blind feedback scheme in the BER performance at the legitimate receiver user A.



(a) Blind without feedback. (b) Blind feedback.

Fig. 5.8: BER_A versus SNR_A in case of passive eavesdropper.

5.3.4.2 BER at the eavesdropper user E

At the eavesdropper user E, BER performances versus SNR_E, is also calculated to evaluate how much user E can decode the message sent from user B. For the rest of this chapter, we have decided to keep the same BER ranges (10^0 to 10^{-5}) without focusing on the useful ranges in order to allow a visual comparison of the different schemes and especially the performances difference between legitimate user A and eavesdropper E. As shown in Fig. 5.9, it is shown that the presence of a self-jamming signal from user A has a significant impact on the estimation and decoding process of user E, regardless of the knowledge of the channel coding used for decoding. The best BER that user E can obtain is about $BER_E = 10^{-3}$ at $SNR_E = 30$ dB. Furthermore, when the self-jamming to noise ratio ρ_{AE} is greater than 15 dB, user E almost cannot decode the intended message from user B. It can be explained that user A can estimate well the SI channel and cancel the SI component because user A has its generated self-jamming signal $\mathbf{x}_A$ as reference. Moreover, applying the blind feedback scheme also improves the channel estimation and decoding processes although user A also has no knowledge about reference signal from user B. In contrast, user E has no knowledge about the reference signal of user B and the self-jamming signal of user A and there is no interference cancellation mechanism applying, instead, it uses only the SPA decoding scheme to decode the intended message.

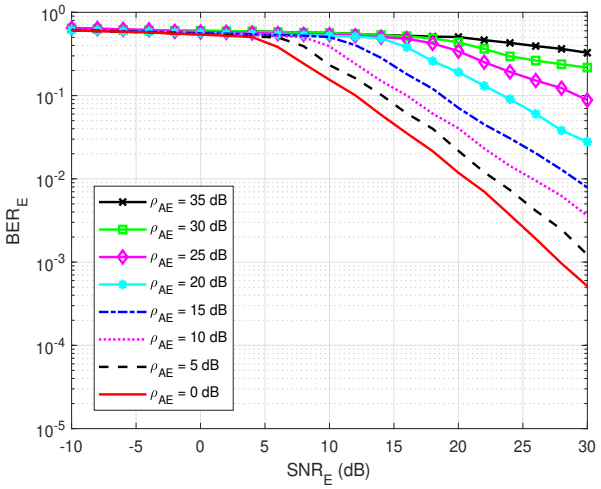


Fig. 5.9: BER_E versus the SNR_E in case of passive eavesdropper.

Therefore, user E can not efficiently operate in the estimation and decoding process. In summary, applying the joint iterative estimation and decoding to the legitimate receiver user A can significantly improve the secrecy reliability factor in FD wiretap transmission, and also maintains well security factor because user E cannot decode the intended message from user B.

5.3.5 Security Gap Performance

The security gap S_g is clearly related to the error rate achieved on the receiver side of user A and user E. In order to adapt for the practical applications, we set up $BER_{A,max} = 10^{-5}$ and $BER_{E,min} = 0.5$ for the maximum and minimum average errors that user A and user E can reach, respectively. Based on the results in Fig. 5.8 and Fig. 5.9, the minimum SNR at the legitimate user A, $SNR_{A,min}$ and the maximum SNR at the eavesdropper user E, $SNR_{E,max}$ to obtain $BER_{A,max} = 10^{-5}$ and $BER_{E,min} = 0.5$ can be pointed out, respectively. Then, these values are recorded corresponding to different levels of the general self-jamming power to noise ratio ρ_{SJ}. Finally, the security gap S_g is calculated based on Equation 5.1 and summarized in Table. 5.2.

Fig. 5.10 shows the security gap versus the various values of the self-jamming power to noise ratio (ρ_{SJ}) in the case of blind without feedback and blind feedback at user A. The result shows that the increase of self-jamming power to noise ratio ρ_{SJ} leads to a decrease in the security gap S_g. For example, the security gap S_g can be dramatically reduced from 7 to 10 dB when the blind feedback scheme is applied. Indeed, S_g can go to -0.2 dB when $\rho_{SJ} = 35$ dB. Therefore, it obtains an important target of the PLS, which is to maintain the security gap as small as possible.

Next, we will consider the second case with active eavesdropper, where user E can also send its jamming message to destroy the reception and decoding processes of user A.

Table 5.2: Security gap S_g in case of passive eavesdropper

ρ_{SJ}	$SNR_{E,max}$	**Without feedback at user A**		**Blind feedback at user A**	
		$SNR_{A,min}$	S_g	$SNR_{A,min}$	S_g
0	4.1	23.8	19.7	16.5	12.4
5	5.8	24.5	18.7	16.8	10.8
10	8.1	25.1	17	17.2	9.1
15	10.3	25.6	15.3	17.6	7.3
20	12.4	26.7	14.3	17.9	5.5
25	14.3	27.5	13.2	18.1	3.8
30	16.6	29	12.4	18.3	1.7
35	18.8	30	11.2	18.6	-0.2

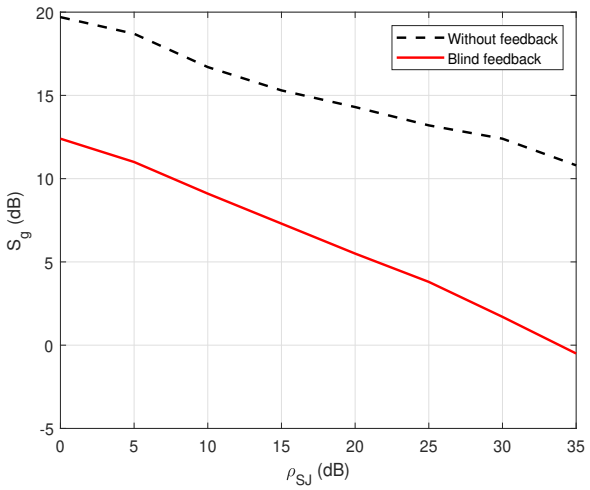


Fig. 5.10: S_g versus ρ_{SJ} in case of passive eavesdropper.

5.4 Case II: Active Eavesdropper

5.4.1 Active Eavesdropper System Model

The wiretap channel system model with the use of FD self-jamming and the presence of an active eavesdropper is shown in Fig. 5.11.

In this case, both user A and user E operate in FD transmission mode to simultaneously receive the intended information message from user B and transmit the self-jamming or jamming signal to other users. In particular, user B wants to send his encoded message $\mathbf{x}_B$ to the legitimate receiver user A by the intended channel, while the eavesdropper user E not only tries to listen to and decode user B's message by the wiretap channel, but also broadcasts simultaneously its jamming signal to user A. Consequently, the received

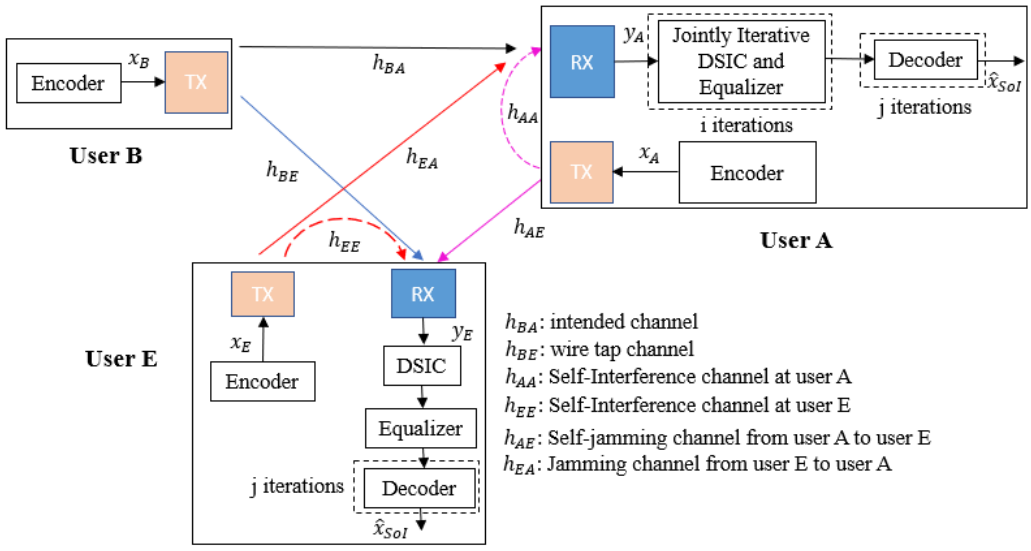


Fig. 5.11: Wiretap FD transmission with self-jamming in case of active eavesdropper.

signals in digital domain at user A and user E, respectively, are given by:

$$\begin{aligned} y_A[n] &= y_{BA}[n] + y_{AA}[n] + y_{EA}[n] + w_A[n] \\ &= (\sqrt{p_B}\mathbf{x}_B * \mathbf{h}_{BA})[n] + (\sqrt{p_A}\mathbf{x}_A * \mathbf{h}_{AA})[n] + (\sqrt{p_E}\mathbf{x}_E * \mathbf{h}_{EA})[n] + w_A[n]; \end{aligned} \tag{5.6}$$

$$\begin{aligned} y_E[n] &= y_{BE}[n] + y_{EE}[n] + y_{AE}[n] + w_E[n] \\ &= (\sqrt{p_B}\mathbf{x}_B * \mathbf{h}_{BE})[n] + (\sqrt{p_E}\mathbf{x}_E * \mathbf{h}_{EE})[n] + (\sqrt{p_A}\mathbf{x}_A * \mathbf{h}_{AE})[n] + w_E[n]; \end{aligned} \tag{5.7}$$

It can be seen that the signal-to-noise ratio at user A is reduced due to the impact of the jamming signal from user E, which leads to an increase in noise at the receiver of user A. Therefore, besides the proposed blind feedback scheme, the joint iterative SI channel estimation and equalization processes with the semi-blind algorithm JSIB_DSICED3, which has been studied in Section 4.3 of Chapter 4, should be used at user A in order to eliminate the SI component and estimate the intended signal $\hat{\mathbf{x}}_{SoI}$. Because the proposed semi-blind algorithm shows its robustness in the low region of SNR, compared to the blind algorithm. Indeed, the principle of this algorithm is to use four pilot symbols between the transceivers (which is a sufficient number of pilot symbols as shown in Section 4.3) to perform the channel estimation processes as well as feedback loop. At user E, in order to distinguish the decoding behavior of the legitimate receiver (user A) and the eavesdropper (user E), and also show the robustness of two proposed feedback schemes over the conventional without feedback schemes, user E will use only blind without feedback scheme DSICED3_WO/F and semi-blind without feedback scheme SB_DSICED3_WO/F. In case of semi-blind without feedback scheme, it is also assumed that four pilot symbols are observed by user E. This scheme is studied in Section 4.2 of Chapter 4.

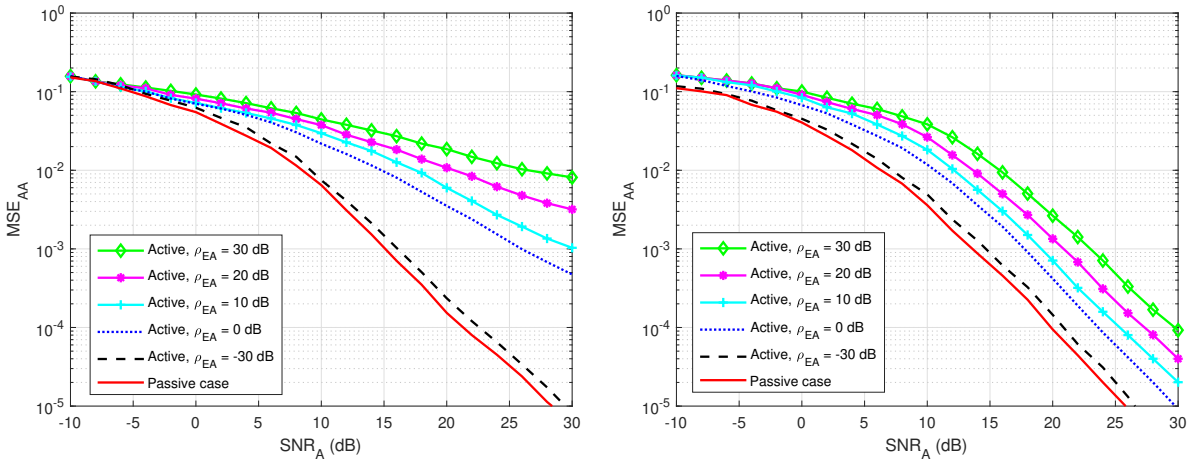
Next, we will introduce the performance in terms of MSE, BER and security gap S_g

in the case of active eavesdropper.

5.4.2 MSE performances in Active Case

5.4.2.1 MSE at the legitimate receiver user A

First of all, Fig. 5.12 and Fig. 5.13 illustrate the MSEs of the SI channel and the intended channel at user A for the blind feedback scheme and the semi-blind feedback scheme, respectively, versus SNR_A, for different power values of the jamming to noise ratio ρ_{EA} broadcast from user E, while the self-interference to noise ratio at user A, ρ_{AA}, is fixed at 30 dB. It can be seen that the presence of jamming signal from user E impacts significantly on the SI channel estimation at user A, where it increases the noise level at receiver side at user A, compared with the passive case. Indeed, the gain between each MSE's curve is bigger than in the passive case, whatever the algorithm used, which means that the system requires higher SNR_A to estimate the channel. Furthermore, the semi-blind feedback scheme outperforms the blind feedback scheme, i.e. it converges faster to the error floor and achieves better results than the blind feedback scheme because the trace off of four pilot symbols is used. Therefore, using the semi-blind algorithm can improve the channel estimation processes and reduce the impact of jamming signal from eavesdropper.

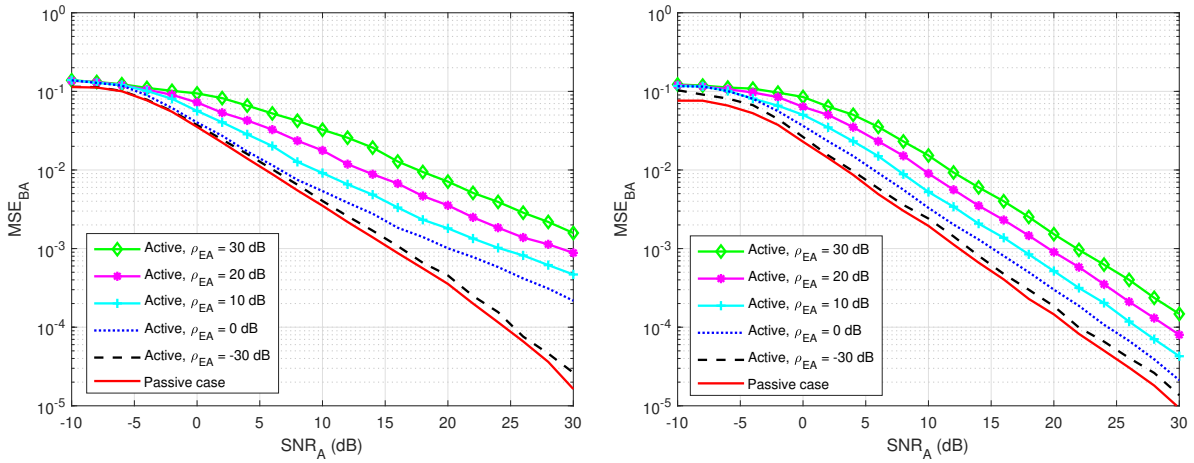


(a) Blind feedback. (b) Semi-blind feedback.

Fig. 5.12: MSE_{AA} versus SNR_A, $\rho_{AA} = 30$ dB in case of active eavesdropper.

5.4.2.2 MSE at the eavesdropper user E

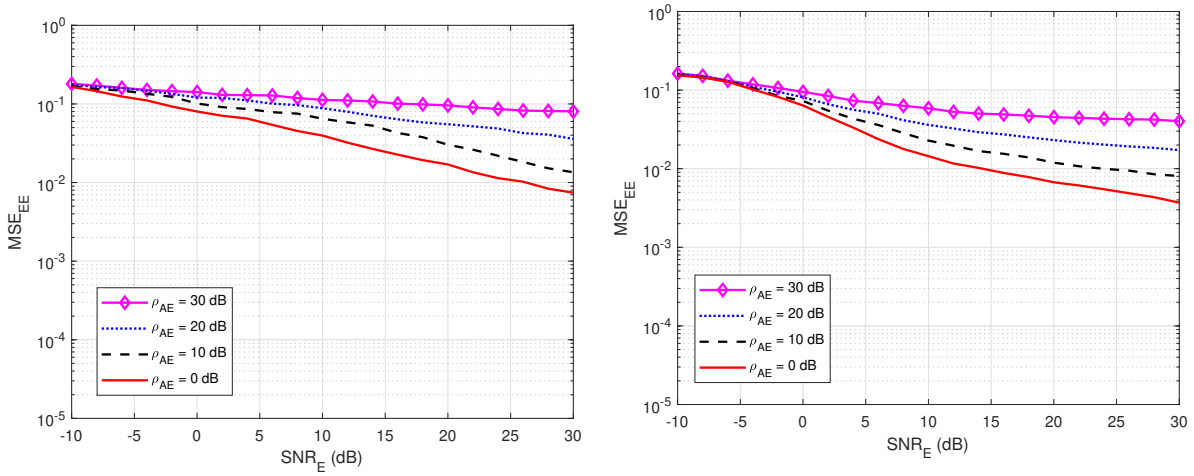
Next, Fig. 5.14 and Fig. 5.15 show the MSEs of the SI channel $\mathbf{h}_{EE}$ and the wiretap channel $\mathbf{h}_{BE}$ versus SNR_E at the eavesdropper user E, for various values of self-jamming to noise ratio from user A, ρ_{AE}. The self-interference to noise ratio at user E, ρ_{EE}, is fixed at 30 dB. It can be clearly observed that user E can not estimate well the wiretap channel



(a) Blind feedback. (b) Semi-blind feedback.

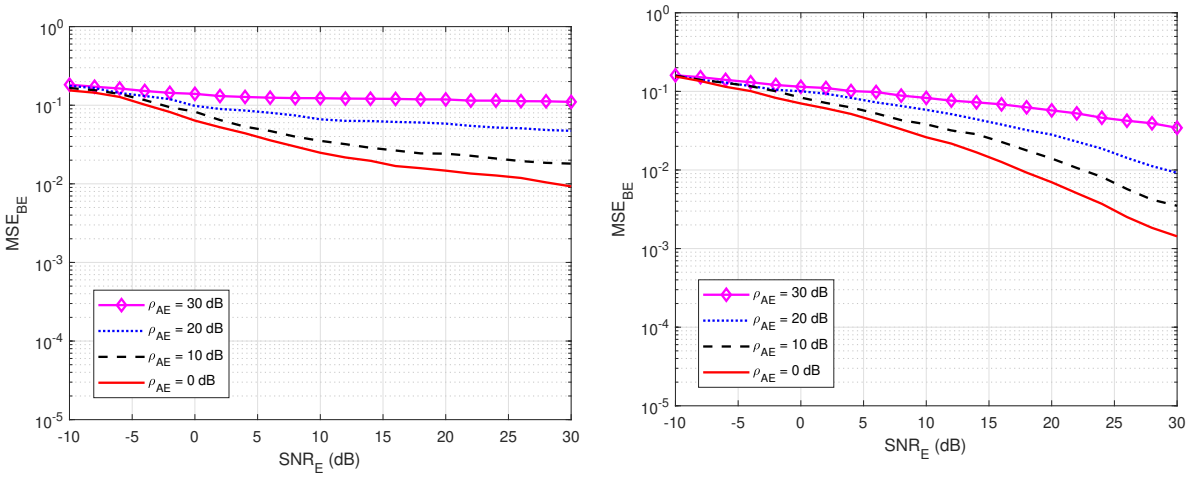
Fig. 5.13: MSE_{BA} versus SNR_A, $\rho_{AA} = 30$ dB in case of active eavesdropper.

as well as the SI channel, especially in case of high value of self-jamming to noise ratio from user A, i.e. ρ_{AE} increases higher than 20 dB. So, self-jamming signal provided by user A influences significantly to the receiver side of user E, where user E can not perform well the wiretap channel estimation in active mode although user E also knows the pilot symbols. Moreover, the power of the combination of the self-jamming of user A and its SI component at user E is also higher than the power level of the intended message from user B. Therefore, the blind without feedback scheme and semi-blind without feedback scheme, which are applied to user E, cannot estimate the channels well.



(a) Blind without feedback (b) Semi-blind without feedback

Fig. 5.14: MSE_{EE} versus SNR_E, $\rho_{EE} = 30$ dB in case of active eavesdropper.



(a) Blind without feedback

(b) Semi-blind without feedback

Fig. 5.15: MSE_{BE} versus SNR_E, $\rho_{EE} = 30$ dB in case of active eavesdropper.

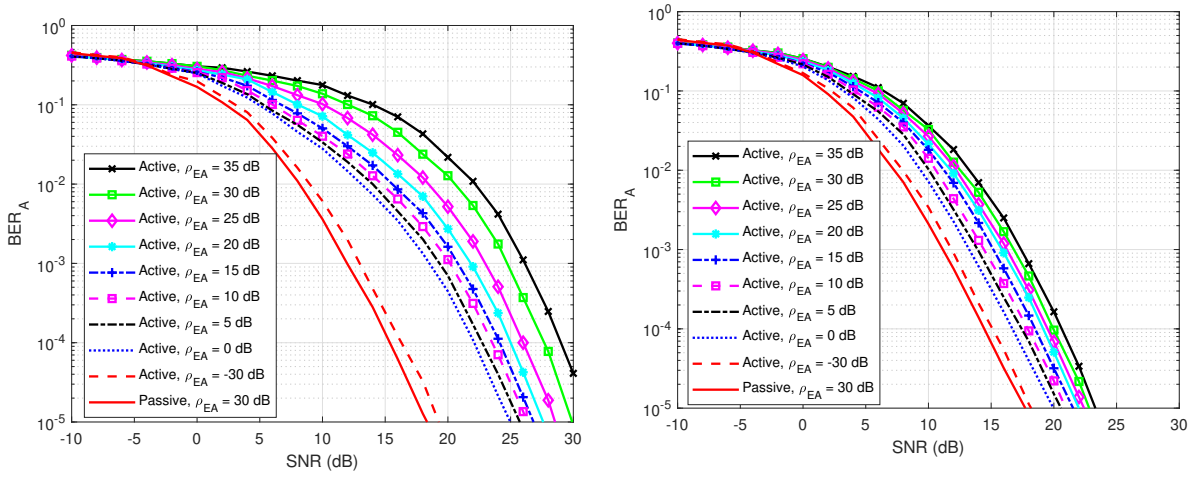
5.4.3 BER Performances in Active Case

5.4.3.1 BER at the legitimate receiver user A

BER performances versus SNR_A at user A for different values of jamming to noise ratio from user E (ρ_{EA}) are illustrated in Fig. 5.16a and Fig. 5.16b for both blind feedback scheme and semi-blind scheme at user A, respectively. The self-interference to noise ratio at user A (ρ_{AA}) is set at 30 dB. We can observe that BER increases as the jamming to noise ratio of user E (ρ_{EA}) increases and the increase of BER is bigger for larger SNR_A, compared with the passive case. We can also remark that the semi-blind scheme is less sensitive to the jamming from user E than the blind feedback scheme, and it also converges faster to the error floor than the other. In particular, when maintaining $BER_A = 10^{-5}$ and increasing the jamming to noise ratio, ρ_{EA} from 0 to 30 dB, the blind feedback scheme needs about 5 dB in SNR_A, while the semi-blind feedback scheme requires only 2.5 to 3 dB to reach that result. Therefore, the semi-blind feedback scheme is suitable in the case of active eavesdropper because the increase of jamming power from the active user E has less influence in BER performance at the legitimate receiver user A. In fact, it can considerably improve the reliability factor of secrecy in FD wiretap transmission in the case of active eavesdropper.

5.4.3.2 BER at the eavesdropper user E

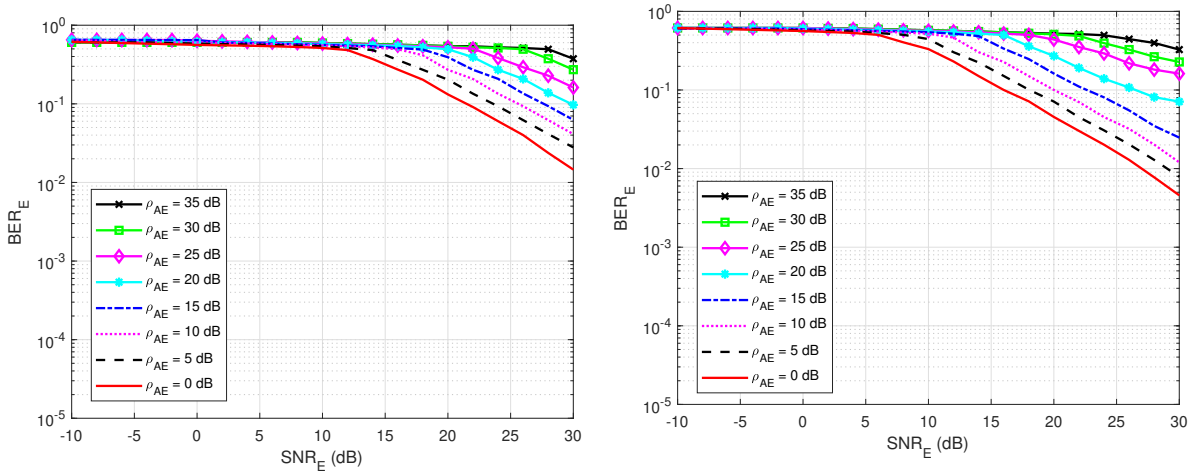
At the active eavesdropper user E, BER performances versus SNR_E, is also calculated to evaluate the amount of message that user E can decode. As shown in Fig. 5.17, it can be seen that the combination of both jamming signal from user A and self-interference component at itself has a major impact on the estimating and decoding process of user E. Because the combination power of these two signals is too large than the power of the



(a) Blind feedback

(b) Semi-blind feedback.

Fig. 5.16: BER_A versus SNR_A, $\rho_{AA} = 30$ dB in case of active eavesdropper.



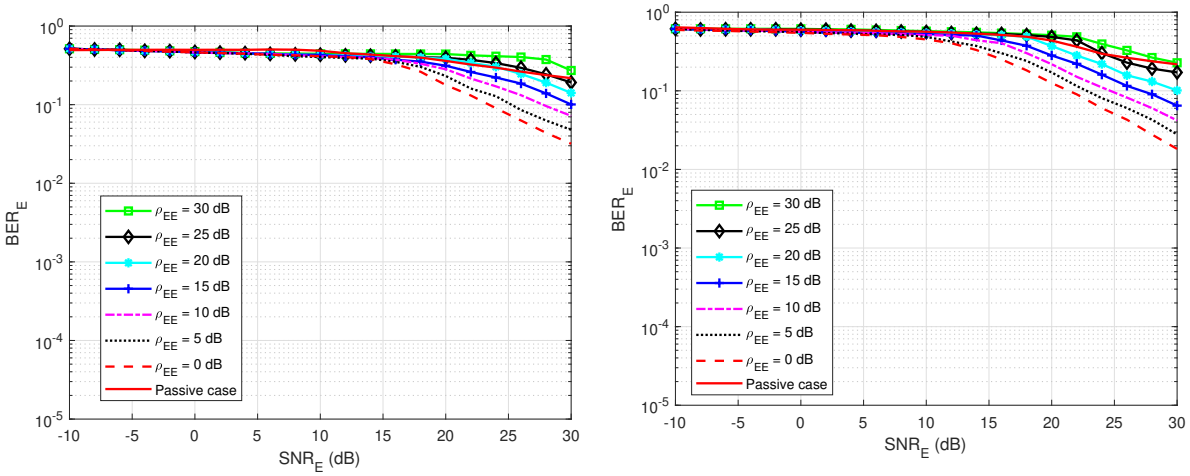
(a) Blind without feedback

(b) Semi-blind without feedback.

Fig. 5.17: BER_E versus SNR_E, $\rho_{EE} = 30$ dB in case of active eavesdropper.

intended signal, and user E only uses the blind or semi-blind without feedback scheme for channel estimation and decoding, regardless of the knowledge of channel coding used for decoding and the four pilot symbols. The best BER that user E can obtain is about $BER_E = 10^{-2}$ at $SNR_E = 30$ dB, corresponding to the lowest level of self-jamming to noise ratio from user A, $\rho_{AE} = 0$ dB. Consequently, when the power of self-jamming signal from user A increases, user E needs very large SNR_E to decode the intended message from user B.

Furthermore, Fig. 5.18 shows the BER of user E versus SNR_E for various values of the self-interference to noise ratio of itself, ρ_{EE}, while the self-jamming to noise ratio of user A, ρ_{AE} is fixed at 30 dB. It shows that if user E tries to increase the power of jamming signal that is sent to user A, it leads to the increase of BER of itself because of the increase of self-interference to noise ratio ρ_{EE}. Although SI can be suppressed by the knowledge of SI signal by classical DSIC process, the interference from self-jamming



(a) Blind without feedback

(b) Semi-blind without feedback.

Fig. 5.18: BER_E versus SNR_E, $\rho_{AE} = 30$ dB in case of active eavesdropper.

signal from user A still significantly impacts on the blind without feedback scheme and semi-blind without feedback scheme. It looks like the case of passive eavesdropper, when user E cannot suppress well the interference from jamming signal of user A. However, the BER of user A is less sensitive to the increase power of user E, especially for the semi-blind feedback scheme, as shown in Fig. 5.16.

Therefore, it can be concluded that user E cannot decode well the message regardless when blind without feedback scheme or semi-blind without feedback scheme are used.

5.4.4 Security Gap Performance

Considering the same assumptions that have been made for background noises and propagation channels in the case of passive eavesdropper in Section 5.3.5, it is also possible to simplify the notations and to denote in general the self-jamming power to noise ratio as ρ_{SJ} for both self-jamming (ρ_{AE}) and jamming (ρ_{EA}) channels. Since in these conditions, we have $\rho_{SJ} = \rho_{AE} = \rho_{EA}$. Adapting for practical applications, we also set $BER_{A,max} = 10^{-5}$ and $BER_{E,min} = 0.5$ for the maximum and minimum average errors that user A and user E can obtain, respectively. According to the results in Fig. 5.16 and 5.17, in order to achieve $BER_{A,max} = 10^{-5}$ and $BER_{E,min} = 0.5$, the minimum SNR at the legitimate user A, $SNR_{A,min}$ and the maximum SNR at the eavesdropper user E, $SNR_{E,max}$ can be pointed out for different values of general self-jamming power to noise ratio (ρ_{SJ}) and for different decoding schemes at user A and user E, respectively. Then, the security gap S_g is calculated based on $SNR_{A,min}$ and $SNR_{E,max}$ and summarized in Table. 5.3 and Table. 5.4 when using blind without feedback and semi-blind without feedback at user E, respectively.

Fig. 5.19 shows the comparison of the security gap S_g with the various values of the general self-jamming power to noise ratio, ρ_{SJ} between the application of the blind

Table 5.3: The security gap when applying blind without feedback scheme at user E.

ρ_{SJ}	**Blind without feedback at user E**	**Blind feedback at user A**		**Semi-blind feedback at user A**	
	$SNR_{E,max}$	$SNR_{A,min}$	S_g	$SNR_{A,min}$	S_g
0	10.7	24.9	14.2	19.9	9.2
5	12.8	25.7	12.9	20.3	7.5
10	15.4	26.3	10.9	21	5.6
15	17.5	26.8	9.3	21.5	4
20	19.9	27.6	7.7	22	2.1
25	22.2	28.5	6.3	22.3	0.1
30	25.6	29.8	4.2	22.8	-2.8
35	28.5	30.7	2.2	23.7	-4.8

Table 5.4: The security gap when using semi-blind without feedback scheme at user E.

ρ_{SJ}	**Semi-blind without feedback at user E**	**Blind feedback at user A**		**Semi-blind feedback at user A**	
	$SNR_{E,max}$	$SNR_{A,min}$	S_g	$SNR_{A,min}$	S_g
0	6.2	24.9	18.7	19.9	13.7
5	8.2	25.7	17.5	20.3	12.1
10	10.8	26.3	15.5	21	10.2
15	13.4	26.8	13.4	21.5	8.1
20	16.1	27.6	11.5	22	5.9
25	18.2	28.5	10.3	22.3	4.1
30	21.5	29.8	8.3	22.8	1.3
35	24.2	30.7	6.5	23.1	-1.1

feedback scheme and the semi-blind feedback scheme on the decoding side of user A. It indicates that the increase in the self-jamming power to noise ratio ρ_{SJ} leads to a decrease in the security gap S_g for all cases. The proposed semi-blind feedback scheme also allows reducing the security gap S_g from about 5 to 7 dB compared to the blind feedback scheme regardless of the use of the blind or semi-blind without feedback scheme in user E. When the semi-blind feedback is applied at user A and the blind without feedback is used at user E It can also seen that the security gap can approach to 0 at $\rho_{PJ} = 25$ dB and also lower than 0 when $\rho_{PJ} > 25$ dB, i.e. $S_g = -2.8$ dB when $\rho_{SJ} = 30dB$, which is the

perfect security and reliability condition. Therefore, it can maintain the security gap as small as possible, which is the most important factor in PLS. Furthermore, the SNR_A of user A is reduced when performing channel estimation or decoding the message using the semi-blind feedback scheme, compared to the blind feedback scheme, which means that the system not only guarantees the security factor, but also improves power consumption.

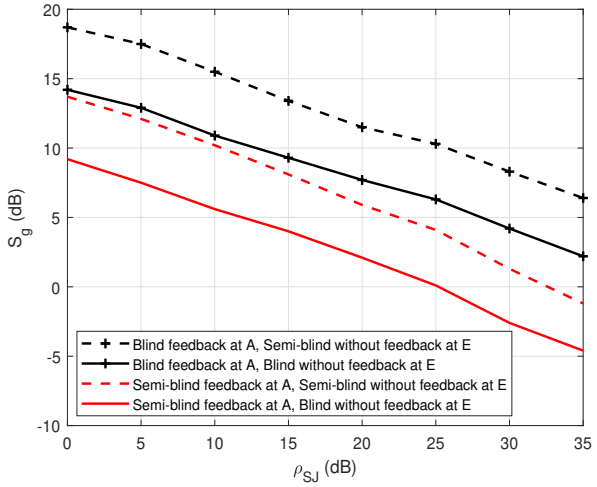


Fig. 5.19: S_g versus ρ_{SJ} in case of active eavesdropper.

5.5 Conclusion

The secrecy analysis of FD short-packet transmission in wiretap channel for both passive and active eavesdroppers has been implemented subject to the constraints of MSE, BER, and security gap S_g. This chapter highlights that the presence of a jamming signal has a major effect on the reliability and security factors in PLS. To deal with it, a joint iterative SI channel estimation, propagation channel estimation, and decoding algorithm in FD transmissions via feedback has been applied at the legitimate receiver including blind feedback or semi-blind feedback schemes in the case of passive and active eavesdropper, respectively. The numerical results show that the proposed algorithms, such as the blind feedback scheme in the passive case and the semi-blind feedback scheme in the active case, outperform the conventional without feedback algorithm, where the security gap S_g is significantly reduced. Moreover, it can be noticed that the blind feedback scheme in the case of passive eavesdropper and semi-blind feedback scheme in the case of active eavesdropper are less sensitive to the increase of self-jamming power. Moreover, the SNR of the legitimate receiver is reduced when applying the proposed schemes to decode the intended message, which means that the system not only ensures the security factor well, but also significantly improves the power consumption by reducing the transmitting power. Therefore, the presence of joint iterative estimation and decoding with blind and semi-blind algorithms at the legitimate receiver is highly recommened to enhance the security of FD wiretap transmission, especially in short-packet transmission specific to IoT applications and green communications.

Conclusion and Future Works

Conclusion

In conclusion, this thesis first summarizes the state-of-the-art in SI cancelation processes, especially in the digital domain with the LMS and RLS algorithms. In fact, the RLS algorithm with $\lambda = 0.999$ gives a sufficient performance in DSIC process. Then, the encoding and decoding processes of recent and efficient radio channel coding schemes for 5G networks are also studied.

Then, this thesis illustrates the effects of residual SI and quantization noise due to the DAC/ADC process on the SISO FD transmission system. It can be clearly seen that SI power is a major factor that degrades the system performances and the quantization noise also significantly degrades the transmission quality. Therefore, the bit resolution should be chosen carefully and oversampling should be applied in ADC process in order to reduce the effects of quantization noise, especially for green communications system and IoT applications. Furthermore, the use of channel coding schemes for new radio network such as 5G QC-LDPC, Polar codes and Turbo codes plays a significant role in FD transmission. They allow a reconstruction of the informative signal close to optimal performances without SI and quantization noise. Therefore, such high performance channel coding techniques are prime candidates to ensure information integrity in FD transmission. Among these coding schemes, 5G LDPC codes seem to give sufficient results, so we choose it as the main coding scheme for further implementation of our proposed algorithms throughout this thesis.

Moreover, this thesis also proposed joint iterative channel estimation and decoding algorithm in SISO FD short packet transmissions with DSIC process for blind and semi-blind algorithms, which are denoted as JIB_DSICED3 and JSIB_DSICED3, respectively. The beauty-of-art of the proposed blind algorithm is taking advantage of iterative algorithms of 5G LDPC at the decoding process to design simultaneous channel estimation and decoding in each iteration in order to efficiently cancel the SI component and improve the simultaneous channel estimation and decoding in the next iteration. However, the blind algorithm has poor performance in the low region of the SNR. Therefore, the semi-blind algorithm should be further developed and proposed. The innovation of the proposed semi-blind algorithm is taking advantage of known pilot symbols and iterative algorithms to improve the system performance in the low region of SNR. Numerical results

showed that the proposed algorithms outperform the conventional algorithm in terms of MSE, BER, processing time, computational complexity and SI sensitivity. As a result, the choice between semi-blind and blind schemes depends on the applications and purposes. Both of them are relevant solutions for short packet FD transmission, which is one of the important functional characteristics of IoT transmissions and green communications.

Last but not least, this thesis illustrates that the power of the self-jamming signal or the jamming signal is the major factor that affects the reliability and security factors in PLS. To deal with it, a joint iterative SI channel estimation, propagation channel estimation, and decoding algorithm in FD transmissions with blind or semi-blind algorithms has been applied at the legitimated receiver in the case of passive and active eavesdroppers, respectively. Numerical results show that the proposed algorithms, such as blind feedback scheme in passive case and semi-blind feedback scheme in active case, outperform the conventional without feedback algorithm, where security gap S_g is decreased significantly. Moreover, it also shows that the proposed schemes are less sensitive to the increasing of self-jamming power. Moreover, the SNR of the legitimate receiver is reduced when the proposed schemes are applied, which means that the system not only guarantees well the security factor but also improves significantly the power consumption regardless of the varying of the position of eavesdropper. Therefore, the presence of joint iterative estimation and decoding with blind and semi-blind algorithms at the legitimate receiver is highly recommended to enhance the security of FD wiretap transmission, especially in short-packet transmission for IoT applications and green communications.

Future Works

Many interesting factors still remain and should be examined further in FD short-packet transmission and channel coding schemes, especially in the physical layer security area. The impacts of a higher order of modulation in FD short-packet transmissions need to be considered. Therefore, it is possible to expand this work to the non-binary LDPC codes, which are used to overcome the weakness of the binary codes in short code lengths and higher orders of modulation such as 16-QAM or 64-QAM. In the near future, a Software Define Radio (SDR) implementation of the proposed algorithm will be developed in realistic transmission scenarios to evaluate its performance on real signals, especially for IoT applications and green communications. For the PLS area, it is interesting to switch the two decoding algorithms and behaviors of the legitimate receiver and the eavesdropper. The decoding strategies of the eavesdropper are also considered in near future, i.e. using 2 antennas or blind source separation to decode the message from the transmitter. Then, different criteria to evaluate the PLS should be studied such as secure key generation. The impact of different locations of eavesdropper and the distances between three users (transmitter, receiver and eavesdropper) is also implemented for different values of ρ_{AA} and ρ_{AE} in case of passive eavesdropper and ρ_{AE} and ρ_{EA} in case of active eavesdropper.

Last but not least, the theoretical and analytical approach for both Cramér–Rao Lower Bounds (CRLBs) for channel estimation and also the lower bound of the BER will be considered in the near future.

List of Publications

Journals:

- Bao Quoc Vuong, Roland Gautier, Anthony Fiche, Mélanie Marazin, Ta Quang Hien, Nguyen Lap Luat: *"Joint Iterative Blind Self-Interference Cancellation, Propagation Channel Estimation and Decoding Processes in Full-Duplex Transmissions"*, in IEEE Access 10: 22795 - 22807 (February 2022).

- Bao Quoc Vuong, Roland Gautier, Ta Quang Hien, Nguyen Lap Luat, Anthony Fiche, Mélanie Marazin: *"Joint Semi-Blind Self-Interference Cancellation and Equalization Processes in 5G QC-LDPC-Encoded Short-Packet Full-Duplex Transmissions"*, belongs to the Special Issue Full-Duplex Wireless Communication in MDPI Sensors 22(6): 2204 (March 2022).

- Bao Quoc Vuong, Roland Gautier, Anthony Fiche, Melanie Marazin and Cristina Despina-Stoian: *"Secrecy Coding Analysis of Short Packet Full-Duplex Transmissions with Joint Iterative Channel Estimation and Decoding Processes."*, belongs to the Special Issue Physical-Layer Security for Wireless Communications, in MDPI Sensors 22(14): 5257 (July 2022).

International Conference Proceeding:

- Bao Quoc Vuong, Roland Gautier, Anthony Fiche and Mélanie Marazin, *"Full-Duplex Efficient Channel Codes for Residual Self-Interference/Quantization Noise Cancellation*", in the proceeding of The IEEE 15th International Conference on Signal Processing and Communication Systems (ICSPCS), Sydney, Australia, 2021. (Online)

References

[1] Ericsson AB, *5G Radio Access*, 2015. [Online]. Available: https://www.ericsson.com/assets/local/publications/white-papers/wp-5g.pdf.

[2] Huawei Technologies Co. Ltd., *5G: A Technology Vision*, 2013. [Online]. Available: http://www.huawei.com/ilink/en/download/HW_314849.

[3] R. Khan, N. Tsiga, and R. Asif, "Interference Management with Reflective In-Band Full-Duplex NOMA for Secure 6G Wireless Communication Systems," *Sensors*, vol. 22, no. 7, 2022. DOI: https://doi.org/10.3390/s22072508.

[4] M. Elsayed, A. A. Aziz El-Banna, O. A. Dobre, W. Shiu, and P. Wang, "Full-Duplex Self-Interference Cancellation Using Dual-Neurons Neural Networks," *IEEE Communications Letters*, vol. 26, no. 3, pp. 557–561, 2022. DOI: 10.1109/LCOMM.2021.3136030.

[5] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band Full-Duplex Wireless: Challenges and Opportunities," *IEEE Journal on selected areas in communications*, vol. 32, no. 9, pp. 1637–1652, 2014.

[6] S. Hong *et al.*, "Applications of Self-interference Cancellation in 5G and Beyond," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 114–121, 2014. DOI: 10.1109/MCOM.2014.6736751.

[7] R.-A. Pitaval, O. Tirkkonen, R. Wichman, K. Pajukoski, E. Lahetkangas, and E. Tiirola, "Full-Duplex Self-backhauling for Small-cell 5G Networks," *IEEE Wireless Communications*, vol. 22, no. 5, pp. 83–89, 2015.

[8] Y. Chen, C. Ding, and Y. Jia Y.and Liu, "Antenna/Propagation Domain Self-Interference Cancellation (SIC) for In-Band Full-Duplex Wireless Communication Systems," *Sensors*, vol. 22, no. 5, 2022. DOI: https://doi.org/10.3390/s22051699.

[9] A. Silva, M. Gomes, J. Vilela, and W. Harrison, "SDR Proof-of-Concept of Full-Duplex Jamming for Enhanced Physical Layer Security," *Sensors*, vol. 21, no. 3, 2021. DOI: https://doi.org/10.3390/s21030856.

[10] M. Elsayed, A. A. A. El-Banna, O. A. Dobre, W. Shiu, and P. Wang, "Low Complexity Neural Network Structures for Self-Interference Cancellation in Full-Duplex Radio," *IEEE Communications Letters*, vol. 25, no. 1, pp. 181–185, 2021. DOI: 10.1109/LCOMM.2020.3024063.

[11] C. Bockelmann *et al.*, "Massive Machine-type Communications in 5G: Physical and MAC-layer Solutions," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 59–65, 2016.

[12] F. Rusek *et al.*, "Scaling Up MIMO: Opportunities and Challenges with Very Large Arrays," *IEEE Signal Processing Magazine*, vol. 30, no. 1, pp. 40–60, 2013.

[13] O. E. Ayach, S. Rajagopal, S. Abu-Surra, Z. Pi, and R. W. Heath, "Spatially Sparse Precoding in Millimeter Wave MIMO Systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1499–1513, 2014.

[14] T. Bai and R. W. Heath, "Coverage and Rate Analysis for Millimeter-Wave Cellular Networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1100–1114, 2015.

[15] M. M. Razlighi, N. Zlatanov, and P. Popovski, "Dynamic Time-Frequency Division Duplex," *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3118–3132, 2020. DOI: 10.1109/TWC.2020.2970701.

[16] W.-C. Wong, C.-E. Sundberg, and N. Seshadri, "Shared Time Division Duplexing: An Approach to Low-delay High-quality Wireless Digital Speech Communications," *IEEE Transactions on Vehicular Technology*, vol. 43, no. 4, pp. 934–945, 1994. DOI: 10.1109/25.330156.

[17] L. Calderin, S. Ramakrishnan, A. Puglielli, E. Alon, B. Nikolić, and A. M. Niknejad, "Analysis and Design of Integrated Active Cancellation Transceiver for Frequency Division Duplex Systems," *IEEE Journal of Solid-State Circuits*, vol. 52, no. 8, pp. 2038–2054, 2017. DOI: 10.1109/JSSC.2017.2700360.

[18] M. Atallah, G. Kaddoum, and L. Kong, "A Survey on Cooperative Jamming Applied to Physical Layer Security," in *Proceedings of the IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)*, 2015.

[19] Z. Zhang, K. Long, A. V. Vasilakos, and L. Hanzo, "Full-Duplex Wireless Communications: Challenges, Solutions, and Future Research Directions," *Proceedings of the IEEE*, vol. 104, no. 7, pp. 1369–1409, 2016.

[20] E. Ahmed, A. Eltawil, and A. Sabharwal, "Simultaneous Transmit and Sense for Cognitive Radios using Full-Duplex: A First Study," in *Proceedings of the 2012 IEEE International Symposium on Antennas and Propagation*, 2012, pp. 1–2.

[21] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving Physical Layer Secrecy Using Full-Duplex Jamming Receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, 2013.

[22] N. Merhav, "Encoding Individual Source Sequences for the Wiretap Channel," *Entropy*, vol. 23, no. 12, 2021. DOI: https://doi.org/10.3390/e23121694.

[23] Y. Qian, "Internet of Things and Next Generation Wireless Communication Systems," *IEEE Wireless Communications*, 2021.

[24] D. C. Nguyen *et al.*, "6G Internet of Things: A Comprehensive Survey," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 359–383, 2022. DOI: 10.1109/JIOT.2021.3103320.

[25] S. Haller, S. Karnouskos, and C. Schroth, "The Internet of Things in an Enterprise Context," in *Future Internet Symposium*, Springer, Berlin, Heidelberg, 2008.

[26] E. Sallum, N. Pereira, M. Alves, and M. Santos, "Improving Quality-Of-Service in LoRa Low-Power Wide-Area Networks through Optimized Radio Resource Management," *Journal of Sensor and Actuator Networks 9*, vol. 9, no. 1, p. 10, Feb. 2020.

[27] K. Mekki, E. BAJIC, F. Chaxel, and F. Meyer, "A Comparative Study of LPWAN Technologies for Large-scale IoT Deployment," *ICT Express*, vol. 5, no. 1, pp. 1–7, Mar. 2019.

[28] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range Communications in Unlicensed Bands: The Rising Stars in the IoT and Smart City Scenarios," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 60–67, 2016.

[29] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1561–1581, 2019.

[30] S. Narayanan, D. Tsolkas, N. Passas, and L. Merakos, "NB-IoT: A Candidate Technology for Massive IoT in the 5G Era," in *2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2018, pp. 1–6.

[31] N. Varsier, L.-A. Dufrène, M. Dumay, Q. Lampin, and J. Schwoerer, "A 5G New Radio for Balanced and Mixed IoT Use Cases: Challenges and Key Enablers in FR1 Band," *IEEE Communications Magazine*, vol. 59, no. 4, pp. 82–87, 2021.

[32] *ISO/IEC 7498-1:1994 Information Technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*, International Organization for Standardization (ISO), 1994.

[33] M. A. M. Albashier, A. Abdaziz, and H. A. Ghani, "Performance Analysis of Physical Layer Security over Different Error Correcting Codes in Wireless Sensor Networks," in *2017 20th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2017, pp. 191–195.

[34] B. V. Nguyen, H. Jung, and K. Kim, "Physical Layer Security Schemes for Full-Duplex Cooperative Systems: State of the Art and Beyond," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 131–137, 2018.

[35] E. da Silva, A. L. dos Santos, L. C. P. Albini, and M. N. Lima, "Identity-based Key Management in Mobile Ad Hoc Networks: Techniques and Applications," *IEEE Wireless Communications*, vol. 15, no. 5, pp. 46–52, 2008.

[36] P. K. Gopala, L. Lai, and H. El Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[37] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical Layer Security in Wireless Networks: A Tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[38] Y. Liang, H. V. Poor, and S. Shamai, "Secure Communication Over Fading Channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[39] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, pp. 1355–1387, 1975.

[40] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[41] L. H. Ozarow and A. D. Wyner, "Wire-Tap Channel II," *Bell System Technical Journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[42] H.-M. Wang, C. Wang, and D. W. K. Ng, "Artificial Noise Assisted Secure Transmission Under Training and Feedback," *IEEE Transactions on Signal Processing*, vol. 63, no. 23, pp. 6285–6298, 2015.

[43] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure Communication via Sending Artificial Noise by the Receiver: Outage Secrecy Capacity/Region Analysis," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628–1631, 2012.

[44] Z. Dryer, A. Nickerl, M. A. C. Gomes, J. P. Vilela, and W. K. Harrison, "Full-Duplex Jamming for Enhanced Hidden-Key Secrecy," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–7.

[45] T. X. Zheng, H. M. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical Layer Security in Wireless Ad Hoc Networks under A Hybrid Full-/Half-Duplex Receiver Deployment Strategy," *IEEE Transactions on Wireless Communications*, vol. 16, no. 6, pp. 3827–3839, 2017.

[46] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Transactions on Signal Processing*, vol. 62, no. 24, pp. 6391–6401, 2014.

[47] N. Arı, N. Thomos, and L. Musavian, "Active Eavesdropping in Short Packet Communication: Average Secrecy Throughput Analysis," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2021, pp. 1–6. DOI: 10.1109/ICCWorkshops50388.2021.9473562.

[48] L. L. Nguyen, D. H. Nguyen, A. Fiche, T. Huynh, and R. Gautier, "Low-bit Quantization Methods for Modulated Wideband Converter Compressed Sensing," in *Proceedings of the IEEE Global Communications Conference, GLOBECOM*, 2019.

[49] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-Layer Security for Full Duplex Communications With Self-Interference Mitigation," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[50] Y. Liu, X. Zhu, E. G. Lim, Y. Jiang, and Y. Huang, "Fast Iterative Semi-Blind Receiver for URLLC in Short-Frame Full-Duplex Systems With CFO," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 4, pp. 839–853, 2019.

[51] J. Zhang *et al.*, "Self-Interference Cancellation: A Comprehensive Review from Circuits and Fields Perspectives," *Electronics*, vol. 11, no. 2, 2022. DOI: https://doi.org/10.3390/electronics11020172.

[52] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. K. Wong, and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[53] W. Kester, *ADC Architectures III: Sigma-Delta ADC Basics Tutorial*, Analog Devices, 2016.

[54] J. Max, "Quantizing for Minimum Distortion," *IRE Trans. Inf. Theory*, vol. 6, no. 1, pp. 7–12, 1960.

[55] W. Kester, *ADC Architectures V: Pipelined Subranging ADCs Tutorial*, Analog Devices, 2016.

[56] W.Kester, *ADC Architectures II: Successive Approximation ADCs Tutorial*, Analog Devices, 2009.

[57] T. Riihonen, S. Werner, and R. Wichman, "Hybrid Full-Duplex/Half-Duplex Relaying with Transmit Power Adaptation," *IEEE Transactions on Wireless Communications*, vol. 10, no. 9, pp. 3074–3085, 2011. DOI: 10.1109/TWC.2011.071411.102266.

[58] 3GPP, *Full-Duplex Configuration of Un and Uu Subframes for Type I Relay, 3GPP TSG RAN WG1 R1-100139, Technical Report*, 2010.

[59] 3GPP, *Text Proposal on In-band Full-Duplex Relay for TR 36.814, 3GPP TSG RAN WG1 R1-101659, Technital Report*, 2010.

[60] S. Chakraborty and D. Sen, "Semi-Blind Data Detection and Non-Linear Equalization in Full-Duplex TWR-OFDM Systems With High Mobility," *IEEE Transactions on Wireless Communications*, vol. 18, no. 12, pp. 6000–6014, 2019.

[61] H. Duan, X. Zhu, Y. Jiang, Z. Wei, and S. Sun, "An Adaptive Self-Interference Cancelation/Utilization and ICA-Assisted Semi-Blind Full-Duplex Relay System for LLHR IoT," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2263–2276, 2020. DOI: 10.1109/JIOT.2019.2958823.

[62] A. Koc and T. Le-Ngoc, "Full-Duplex mmWave Massive MIMO Systems: A Joint Hybrid Precoding/Combining and Self-Interference Cancellation Design," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 754–774, 2021. DOI: 10.1109/OJCOMS.2021.3069672.

[63] E. Everett, A. Sahai, and A. Sabharwal, "Passive Self-Interference Suppression for Full-Duplex Infrastructure Nodes," *IEEE Transactions on Wireless Communications*, vol. 13, no. 2, pp. 680–694, Feb. 2014.

[64] C. Anderson *et al.*, "Antenna Isolation, Wideband Multipath Propagation Measurements, and Interference Mitigation for On-frequency Repeaters," Apr. 2004, pp. 110–114, ISBN: 0-7803-8368-0.

[65] J. I. Choi, S. Hong, M. Jain, S. Katti, P. Levis, and J. Mehlman, "Beyond Full-Duplex Wireless," in *2012 Conference Record of the Forty Sixth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, 2012, pp. 40–44.

[66] D. Korpi, M. Heino, C. Icheln, K. Haneda, and M. Valkama, "Compact Inband Full-Duplex Relays With Beyond 100 dB Self-Interference Suppression: Enabling Techniques and Field Measurements," *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 2, pp. 960–965, 2017.

[67] J. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti, "Achieving Single Channel, Full-Duplex Wireless Communication," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking - MobiCom '10*, Association for Computing Machinery (ACM), 2010, pp. 1–12.

[68] D. Bharadia, E. Mcmilin, and S. Katti, "Full-Duplex Radios," vol. 43, Sep. 2013, pp. 375–386, ISBN: 978-1-4503-2056-6.

[69] K. Kolodziej, J. McMichael, and B. Perry, "Adaptive RF Canceller for Transmit-receive Isolation Improvement," Jan. 2014, pp. 172–174.

[70] M. Duarte *et al.*, "Design and Characterization of a Full-Duplex Multiantenna System for WiFi Networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 3, pp. 1160–1177, Mar. 2014, ISSN: 0018-9545.

[71] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven Characterization of Full-Duplex Wireless Systems," *IEEE Transactions on Wireless Communications*, vol. 11, no. 12, pp. 4296–4307, 2012.

[72] M. Duarte and A. Sabharwal, "Full-Duplex Wireless Communications using Off-the-shelf Radios: Feasibility and First Results," Dec. 2010, pp. 1558–1562.

[73] Y. Kurzo, A. Burg, and A. Balatsoukas-Stimming, "Design and Implementation of a Neural Network Aided Self-Interference Cancellation Scheme for Full-Duplex Radios," in *2018 52nd Asilomar Conference on Signals, Systems, and Computers*, 2018, pp. 589–593. DOI: 10.1109/ACSSC.2018.8645295.

[74] C. Despina-Stoian, A. Digulescu-Popescu, S. Alexandra, R. Youssef, and E. Radoi, "Comparison of Adaptive Filtering Strategies for Self-Interference Cancellation in LTE Communication Systems," in *The 13th International Conference on Communications (COMM)*, 2020.

[75] E. Ahmed and A. M. Eltawil, "All-Digital Self-Interference Cancellation Technique for Full-Duplex Systems," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3519–3532, 2015.

[76] S. Haykin, *Adaptive Filter Theory*. Pearson, 1993, vol. 29.

[77] A. Koohian, H. Mehrpouyan, A. A. Nasir, S. Durrani, and S. D. Blostein, "Residual Self-interference Cancellation and Data Detection in Full-Duplex Communication Systems," in *IEEE International Conference on Communications (ICC)*, 2017.

[78] G. Liu, W. Feng, Z. Han, and W. Jiang, "Performance Analysis and Optimization of Cooperative Full-Duplex D2D Communication Underlaying Cellular Networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 11, pp. 5113–5127, 2019. DOI: 10.1109/TWC.2019.2932982.

[79] *Guidelines for Evaluation of Radio Transmission Technologies for IMT-2000*, International Telecommunication Union, 1997.

[80] 3GPP, *TS 38.212 NR- Multiplexing and Channel Coding*, 2018.

[81] T. Specification, "Final Report of 3GPP RAN1 ad-hoc NR1 Meeting," 2017.

[82] J. H. Bae, A. Abotabl, H. P. Lin, K. B. Song, and J. Lee, "An Overview of Channel Coding for 5G NR Cellular Communications," *Transactions on Signal and Information Processing*, vol. 8, no. 17, 2019.

[83] K. M. Malviya and D., "Polar Code : An Advanced Encoding And Decoding Architecture For Next Generation 5G Applications," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 7, no. 5, pp. 26–29, 2015.

[84] R. G. Gallager, "Low Density Parity Check Codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 21–28, 1962.

[85] E. Arikan, "Channel Polarization: A Method for Constructing Capacity-achieving Codes for Symmetric Binary-input Memoryless Channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, 2009.

[86] D. MacKay, "Good Error-correcting Codes Based on very Sparse Matrices," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 399–431, 1999.

[87] 3GPP, *Multiplexing and Channel Coding*, 2020.

[88] W. Abdulwahab and A. Abdulrahman Kadhim, "Comparative Study of Channel Coding Schemes for 5G," in *Proceedings of the IEEE International Conference on Advanced Science and Engineering*, 2018.

[89] K. D. Rao, "Performance Analysis of Enhanced Turbo and Polar Codes with List Decoding for URLLC in 5G Systems," in *Proceedings of the 5th IEEE International Conference for Convergence in Technology (I2CT)*, IEEE, 2019.

[90] Z. Hajiyat, A. Sali, M. Mokhtar, and F. Hashim, "Channel Coding Scheme for 5G Mobile Communication System for Short Length Message Transmission," *Wireless Personal Communications*, vol. 106, May 2019.

[91] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near SHANNON Limit Error-correcting Coding and Encoding: Turbo-codes," in *Proceedings of the IEEE International Conference on Communications*, 1993.

[92] R. Maunder, "A Vision for 5G Channel Coding," *AccelerComm White Paper*, Oct. 2016.

[93] O. Iscan, D. Lentner, and W. Xu, "A Comparison of Channel Coding Schemes for 5G Short Message Transmission," in *2016 IEEE Globecom Workshops (GC Wkshps)*, 2016, pp. 1–6.

[94] H. Li *et al.*, "Self-interference Cancellation Enabling High-throughput Short-reach Wireless Full-Duplex Communication," *IEEE Transactions on Wireless Communications*, vol. 17, no. 10, 2018.

[95] H. Li, B. Bai, X. Mu, J. Zhang, and H. Xu, "Algebra-Assisted Construction of Quasi-Cyclic LDPC Codes for 5G New Radio," *IEEE Access*, vol. 6, pp. 50 229–50 244, 2018.

[96] E. Sharon, S. Litsyn, and J. Goldberger, "An Efficient Message-passing Schedule for LDPC Decoding," *IEEE Convention of Electrical and Electronics Engineers in Israel, Proceedings*, no. 4, pp. 223–226, 2004.

[97] X. Zhang and P. H. Siegel, "Quantized Iterative Message Passing Decoders with Low Error Floor for LDPC Codes," *IEEE Transactions on Communications*, vol. 62, no. 1, pp. 1–14, 2014.

[98] V. Bioglio, C. Condo, and I. Land, "Design of Polar Codes in 5G New Radio," *IEEE Communications Surveys and Tutorials*, 2020.

[99] C. Leroux, A. J. Raymond, G. Sarkis, and W. J. Gross, "A Semi-parallel Successive-cancellation Decoder for Polar Codes," *IEEE Transactions on Signal Processing*, vol. 61, no. 2, 2013.

[100] B. L. Gal, C. Leroux, and C. Jego, "Software Polar Decoder on An Embedded Processor," in *IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation*, 2014.

[101] I. Tal and A. Vardy, "List Decoding of Polar Codes," *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2213–2226, 2015.

[102] A. Balatsoukas-Stimming, M. B. Parizi, and A. Burg, "LLR-Based Successive Cancellation List Decoding of Polar Codes," *IEEE Transactions on Signal Processing*, vol. 63, no. 19, pp. 5165–5179, 2015.

[103] K. Niu and K. Chen, "CRC-aided Decoding of Polar Codes," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1668–1671, 2012.

[104] C. Pillet, V. Bioglio, and C. Condo, "On List Decoding of 5G-NR Polar Codes," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, 2020, pp. 1–6.

[105] B. Tahir, S. Schwarz, and M. Rupp, "BER Comparison between Convolutional, Turbo, LDPC, and Polar codes," *Proceedings of the 24th International Conference on Telecommunications: Intelligence in Every Form, ICT 2017*, 2017.

[106] C. B. Schlegel and L. C. Pérez, *Trellis and Turbo Coding*. 2004, pp. 1–386, ISBN: 9780471667841.

[107] S. Benedetto, G. Montorsi, F. Pollara, and D. Divsalar, "A Soft-Input Soft-Output Maximum A Posteriori (MAP) Module to Decode Parallel and Serial Concatenated Codes.," *TDA Progress Report*, 1996.

[108] A. Masmoudi and T. Le-Ngoc, "Residual Self-interference After Cancellation in Full-Duplex Systems," in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 4680–4685.

[109] *LTC2000 Family DAC Datasheet*, Analog Devices.

[110] *12-Bit, 6 GSPS/10.25 GSPS, JESD204B, RF Analog-to-Digital Converter Datasheet*, Analog Devices.

[111] T. Kim, M. Kyungsik, and S. Park, "Self-Interference Channel Training for Full-Duplex Massive MIMO Systems," *Sensors*, vol. 21, no. 9, 2021. DOI: `https://doi.org/10.3390/s21093250`.

[112] K. Dani, A. Lauri, R. Taneli, and et al, *Digital Self-Interference Cancellation for Low-Cost Full-Duplex Radio Devices*. Singapore: Springer Nature, 2020.

[113] S. J. Orfanidis, *Introduction to Signal Processing*. Prentice –Hall, 1996.

[114] A. Masmoudi and T. Le-Ngoc, "A Maximum-Likelihood Channel Estimator for Self-Interference Cancelation in Full-Duplex Systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, 2016.

[115] G. Durisi, T. Koch, and P. Popovski, "Toward Massive, Ultrareliable, and Low-latency Wireless Communication with Short Packets," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1711–1726, 2016.

[116] P. Schulz *et al.*, "Latency Critical IoT Applications in 5G: Perspective on the Design of Radio Interface and Network Architecture," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 70–78, 2017.

[117] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[118] P. Popovski, "Ultra-reliable Communication in 5G Wireless Systems," in *1st International Conference on 5G for Ubiquitous Connectivity*, IEEE, 2014, pp. 146–151.

[119] J. Lee, Y. Kwak, F. Luo, and C. Zhang, "5G Standard Development: Technology and Roadmap," in *Signal Processing for 5G: Algorithms and Implementations*, Wiley-IEEE Press, 2016, pp. 561–575.

[120] H.-M. Wang, Q. Yang, Z. Ding, and H. V. Poor, "Secure Short-packet Communications for Mission-critical IoT Applications," *IEEE Transactions on Wireless Communications*, vol. 18, no. 5, pp. 2565–2578, 2019.

[121] D. Kim, H. Ju, S. Park, and D. Hong, "Effects of Channel Estimation Error on Full-Duplex Two-way Networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 9, pp. 4666–4672, 2013.

[122] D. Liu, B. Zhao, F. Wu, S. Shao, X. Pu, and Y. Tang, "Semi-Blind SI Cancellation for In-Band Full-Duplex Wireless Communications," *IEEE Communications Letters*, vol. 22, no. 5, pp. 1078–1081, 2018. DOI: 10.1109/LCOMM.2018.2809622.

[123] A.Masmoudi and T. Le-Ngoc, "Channel Estimation and Self-Interference Cancelation in Full-Duplex Communication Systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, 2017.

[124] A. T. Kristensen, A. Balatsoukas-Stimming, and A. Burg, "On the Implementation Complexity of Digital Full-Duplex Self-Interference Cancellation," in *2020 54th Asilomar Conference on Signals, Systems, and Computers*, 2020, pp. 969–973. DOI: 10.1109/IEEECONF51394.2020.9443274.

[125] S. Yao, H. Qian, K. Kang, and M. Shen, "A Recursive Least Squares Algorithm with Reduced Complexity for Digital Predistortion Linearization," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013, pp. 4736–4739. DOI: 10.1109/ICASSP.2013.6638559.

[126] Y. Xiao and J.-y. Sun, "RLS CMA Blind Equalization with Adaptive Forgetting Factor Controlled by Energy Steady State," in *2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, 2016, pp. 935–939. DOI: 10.1109/CISP-BMEI.2016.7852845.

[127] L. Mostari and A. taleb-ahmed, "High performance short-block binary regular LDPC codes," *AEJ - Alexandria Engineering Journal*, Nov. 2018.

[128] V. Aggarwal, M. Duarte, A. Sabharwal, and N. K. Shankaranarayanan, "Full- or Half-Duplex? A Capacity Analysis with Bounded Radio Resources," in *2012 IEEE Information Theory Workshop*, 2012, pp. 207–211.

[129] I. D. Fîciu, C. L. Stanciu, and C. Anghel C.and Elisei-Iliescu, "Low-Complexity Recursive Least-Squares Adaptive Algorithm Based on Tensorial Forms," *Applied Sciences*, vol. 18, 2021.

[130] M. J. Khokhar and M. S. Younis, "Development of the RLS Algorithm Based on the Iterative Equation Solvers," in *2012 IEEE 11th International Conference on Signal Processing*, vol. 1, 2012, pp. 272–275. DOI: 10.1109/ICoSP.2012.6491653.

[131] J. K. Kim, S. P. Balakannan, M. H. Lee, and C. J. Kim, "Low Complexity Encoding of LDPC Codes for High-rate and High-speed Communication," in *2008 First International Conference on Distributed Framework and Applications*, 2008, pp. 189–193. DOI: 10.1109/ICDFMA.2008.4784435.

[132] M. Sybis, K. Wesolowski, K. Jayasinghe, V. Venkatasubramanian, and V. Vukadinovic, "Channel Coding for Ultra-Reliable Low-Latency Communication in 5G Systems," in *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, 2016, pp. 1–5. DOI: 10.1109/VTCFall.2016.7880930.

[133] J. W. Y. D. S. O. S. J. Park, "Interceptor complexity analysis for mixed BPSK–QPSK modulated frequency hopping spread spectrum systems," *Physical Communication*, vol. 40, 2020.

[134] C. Feng and H.-M. Wang, "Secure Short-Packet Communications at the Physical Layer for 5G and Beyond," *IEEE Communications Standards Magazine*, vol. 5, no. 3, pp. 96–102, 2021. DOI: 10.1109/MCOMSTD.121.2100028.

[135] H. V. Poor, M. Goldenbaum, and W. Yang, "Fundamentals for IoT Networks: Secure and Low-latency Communications," Jan. 2019, pp. 362–364, ISBN: 9781450360944. DOI: 10.1145/3288599.3288643.

[136] L. Mostari and A. taleb-ahmed, "High performance short-block binary regular LDPC codes," *AEJ - Alexandria Engineering Journal*, Nov. 2018.

[137] B. Macro, M. Nicola, R. Giocomo, and C. Franco, "Security Gap Analysis of Some LDPC Coded Transmission Schemes over the Flat and Fast Fading Gaussian Wiretap Channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 15, no. 232, Oct. 2015.

[138] Z. Yang, Y. Fan, and A. Wang, "Artificial Noise and LDPC Code Aided Physical Layer Security Enhancement," in *2014 International Conference on Information and Communications Technologies (ICT 2014)*, 2014, pp. 1–6.

[139] J. Du, "A Partially Coupled LDPC Coded Scheme for the Gaussian Wiretap Channel," *IEEE Communications Letters*, vol. 24, no. 1, pp. 7–10, 2020.

[140] L. Li, Y. Xing, X. Yao, and Y. Luo, "McEliece Coding Method based on LDPC Code with Application to Physical Layer Security," in *2021 7th International Conference on Computer and Communications (ICCC)*, 2021, pp. 2042–2045. DOI: 10.1109/ICCC54389.2021.9674295.

[141] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "Ldpc codes for the gaussian wiretap channel," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 532–540, 2011.

DOCTORAT BRETAGNE LOIRE / MATHSTIC

Université de Bretagne Occidentale

Titre : Approches Conjointes d'Annulation d'Auto-Interférences, d'Estimation de Canal et de Décodage en Full-Duplex pour la Sécurité de la Couche Physique des Transmissions IoT

Mot clés : Full-Duplex, Codage Canal, Annulation d'interférences, l'algorithme aveugle et semi-aveugle, Short-packet, Sécurité Couche Physique pour les Communications

Résumé : Cette thèse a pour but d'améliorer la fiabilité des données et de renfoncer la sécurité au niveau de la couche physique dans le cadre de transmissions IoT. Pour atteindre ces objectifs, l'utilisation d'une transmission SISO Full-Duplex a été retenue. L'un des inconvénients de ce mode de transmission est qu'il est nécessaire d'annuler analogiquement et/ou numériquement l'auto-interférence, afin de conserver des performances admissibles. L'auto-interférence résiduelle après annulation analogique partielle peut être supprimée en partie à l'aide d'algorithmes numériques d'annulation d'auto-interférence. Tout d'abord, plusieurs codes correcteurs d'erreurs, utilisés dans le cadre de la 5G, ont été étudiés afin d'améliorer l'annulation de l'auto interférence résiduelle et du bruit de quantification. Ensuite, deux schémas (aveugle et semi-aveugle) itératifs conjoints ont été développés dans le cadre de transmissions Full-Duplex de paquets courts afin de supprimer l'auto-interférence résiduelle et d'améliorer conjointement l'estimation des canaux de transmission et le décodage de l'information. Les algorithmes proposés offrent de meilleures performances que l'algorithme conventionnel en termes d'erreur quadratique moyenne, de taux d'erreur binaire, de temps de calcul, de complexité de calcul et de sensibilité. Enfin, cette thèse montre également que la combinaison des algorithmes itératifs conjoints et de l'auto brouillage au niveau du récepteur légitime est fortement recommandée afin de garantir la fiabilité et la sécurité des données dans le cas où la transmission serait écoutée et/ou perturbée par un brouilleur.

Title: Full-Duplex Joint Self-Interference Cancellation, Channel Estimation and Decoding Approaches for IoT Transmissions Physical Layer Security

Keywords: Full-Duplex, Channel Coding, Self-Interference Cancellation, Joint Iterative Blind and Semi-Blind Algorithm, Short-packet, Physical Layer Security

Abstract: This thesis aims to improve data reliability and security at the physical layer level in the context of Internet of Things (IoT) transmissions. To achieve these goals, the use of a SISO Full-Duplex (FD) transmission has been considered. One of the disadvantages of this mode of transmission is that it is necessary to cancel the Self-Interference (SI) in RF/analog domains and/or in digital domain to maintain sufficient performance. In fact, residual SI after partial analog cancellation can be partly suppressed using digital SI cancellation algorithms. First of all, several error correcting codes that used in the context of 5G & Beyond, have been studied to improve the cancellation of the residual SI and quantization noise. Afterwards, two joint iterative (blind and semi-blind) schemes have been developed within the framework of short-packet FD transmissions to jointly remove the residual SI and improve the estimation of the transmission channels and the decoding process. The proposed algorithms provide better performance than the conventional algorithm in terms of Mean Square Error (MSE), Bit Error Rate (BER), processing time, computational complexity and SI sensitivity. Finally, this thesis also shows that the combination of joint iterative algorithms and self jamming at the legitimate receiver is strongly recommended to ensure reliability and data security in the case that the transmission is eavesdropped and/or disrupted by a jammer.