



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

**Παραγωγή Κλειδιών και Αυθεντικοποίηση μέσω των
Ιδιοτήτων Εκπομπής και Ασύρματου Καναλιού και
Υλοποίηση με Software Defined Radios**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Κυριαζή Ιωάννη

Επιβλέπων : Μαλιάτσος Κωνσταντίνος, Επίκουρος Καθηγητής

Μέλη εξεταστικής επιτροπής: Μαλιάτσος Κωνσταντίνος, Επίκουρος Καθηγητής
Καλλίγερος Εμμανουήλ, Μόνιμος Επίκουρος Καθηγητής
Βουγιούκας Δημοσθένης, Καθηγητής

Σάμος, Οκτώβριος 2023

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και Ευχαριστίες

Η παρούσα Διπλωματική Εργασία εκπονήθηκε κατά το Εαρινό Εξάμηνο του ακαδημαϊκού έτους 2022-2023 στα πλαίσια του Προπτυχιακού Προγράμματος Σπουδών του τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων που αποτελεί μέρος της Πολυτεχνικής Σχολής του Πανεπιστημίου Αιγαίου.

Ασχολείται με ένα αρκετά κρίσιμο θέμα την εποχή που βρισκόμαστε, την παραγωγή κλειδιών και την αυθεντικοποίηση της εκπομπής και κατ' επέκταση του πομπού μέσω των ιδιοτήτων του λαμβανόμενου σήματος αλλά και του καναλιού με χρήση ραδιοσυχνοτήτων που καθορίζονται από λογισμικό. Με λίγα λόγια, όπως ο κάθε άνθρωπος διαθέτει ένα μοναδικό δακτυλικό αποτύπωμα, έτσι και το κάθε σήμα/ραδιοσυχνότητα και το κανάλι διαθέτουν μοναδικά χαρακτηριστικά. Με αυτό τον τρόπο, μέσα από ένα πρόγραμμα στον υπολογιστή και με την χρήση εξειδικευμένου εξοπλισμού USRP, θα δημιουργήσουμε τις κατάλληλες αλληλουχίες εικονικών εξαρτημάτων (πηγές, ενισχυτές, μαθηματικούς τύπους) προκειμένου ο δέκτης να είναι σε θέση να αξιοποιεί τα μοναδικά χαρακτηριστικά μίας εκπομπής και του καναλιού για την αυθεντικοποίησή της.

Η εργασία εκπονήθηκε με την επίβλεψη του Επίκουρου Καθηγητή του τμήματος κυρίου Μαλιάτσου Κωνσταντίνου, τον οποίο θα ήθελα να ευχαριστήσω θερμά για όλη την καθοδήγηση. Χωρίς την κατανόηση και την ανιδιοτελή υποστήριξή του δεν θα ήταν εφικτή η υλοποίησή της. Η εξεταστική επιτροπή αποτελείται από τον Μόνιμο Επίκουρο Καθηγητή κύριο Καλλίγερο Εμμανουήλ, τον Αναπληρωτή Καθηγητή κύριο Μαλιάτσο Κωνσταντίνο και τον Καθηγητή κύριο Βουγιούκα Δημοσθένη.

Έτσι κλείνει ένα κεφάλαιο το οποίο άρχισε κατά την εισαγωγή μου στο τμήμα τον Σεπτέμβριο του 2018. Η συγκεκριμένη εργασία σηματοδοτεί την λήξη των σπουδών μου καθώς η εκπόνησή της πραγματοποιήθηκε κατά το 10^ο Εξάμηνο που διανύω ακολουθώντας πλήρως τον ορισμένο αριθμό μαθημάτων κάθε εξαμήνου.

Μέσα σε όλα αυτά τα χρόνια, η υποστήριξη που έλαβα από τους γονείς μου ήταν πολύτιμη και καθοριστική. Τόσο η ψυχολογική υποστήριξη σε δύσκολες εργασίες όσο και η τόνωση του ηθικού σε αποτυχίες μου ήταν καταλυτικές για την πορεία μου ως προπτυχιακός φοιτητής. Τους ευχαριστώ θερμά για όλα.

Επιπλέον θα ήθελα να ευχαριστήσω όλους τους φίλους μου που στάθηκαν στο πλευρό μου στις δύσκολες και εύκολες ώρες που πέρασα. Οι συμβουλές τους, η υπομονή τους και η βοήθειά τους τόσο σε ακαδημαϊκά όσο και προσωπικά θέματα ήταν καίριες.

Τέλος, θα ήθελα να αφιερώσω την εργασία στον συνονόματο παππού μου ο οποίος αν και «έφυγε» σε μεγάλη ηλικία ήταν η μεγαλύτερή μου αδυναμία.

© 2023

του

Κυριαζή Ιωάννη

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1	Εισαγωγή	1
1.1	Η Ασφάλεια στις Ασύρματες Επικοινωνίες.....	1
1.2	Αντικείμενο διπλωματικής.....	2
1.3	Δομή της διπλωματικής	3
2	Το Ασύρματο Κανάλι.....	4
2.1	Διαλείψεις Μεγάλης Κλίμακας.....	4
2.1.1	Μοντέλο διάδοσης στον ελεύθερο χώρο	5
2.1.2	Οι Μηχανισμοί Διάδοσης - Ανάκλαση.....	6
2.1.3	Μοντέλο Ανάκλασης (Δύο Ακτινών) στο Έδαφος.....	8
2.1.4	Οι Μηχανισμοί Διάδοσης - Περίθλαση.....	9
2.1.5	Οι Μηχανισμοί Διάδοσης - Σκέδαση	10
2.1.6	Μοντέλα διάδοσης σε εξωτερικούς χώρους.....	11
2.1.7	Μοντέλα διάδοσης σε εσωτερικούς χώρους.....	12
2.2	Διαλείψεις Μικρής Κλίμακας και Πολυδιαδρομές (Multipath).....	13
2.2.1	Ολίσθηση Doppler	13
2.2.2	Μοντελοποίηση καναλιού ως φίλτρο και σχέση εύρους ζώνης και λαμβανόμενης ισχύος	14
2.2.3	Μέτρηση της πολυδιαδρομής μικρής κλίμακας	15
2.2.4	Παράμετροι καναλιών πολυδιαδρομών	17
2.2.5	Τύποι διαλείψεων μικρής κλίμακας	17
2.2.6	Κατανομές διαλείψεων.....	18
2.2.7	Στατιστικά μοντέλα για κανάλια εξασθένησης πολυδιαδρομών	19
2.2.8	Θεωρία των συντελεστών σχήματος πολυδιαδρομών για ασύρματα κανάλια διαλείψεων μικρής κλίμακας.....	20
2.3	Διαμόρφωση Ορθογώνιας Πολυπλεξίας Διαίρεσης Συχνότητας (OFDM).....	22
2.3.1	Η ιδέα της OFDM	22
2.3.2	Συγχρονισμός (Synchronization) και Εκτίμηση του Καναλιού (Channel Estimation).....	25
2.3.3	OFDM Πολλαπλών Εισόδων και Πολλαπλών Εξόδων (MIMO OFDM).....	25
3	Αλλοιώσεις Ραδιοσυχνότητων.....	27
3.1	Εισαγωγή στις Αλλοιώσεις Ραδιοσυχνότητων.....	27
3.1.1	Εισαγωγή στον Θόρυβο Φάσης (Phase Noise).....	28
3.1.2	Μετατόπιση Συχνότητας Φέροντος (CFO – Carrier Frequency Offset)	29

3.1.3	Ανισορροπία μεταξύ Συμφασικής και Ορθογώνιας συνιστώσας (<i>IQ Imbalance – In-phase Quadrature Imbalance</i>).....	30
3.2	Θόρυβος Φάσης (<i>Phase Noise</i>).....	31
3.2.1	Ανάλυση της Απόδοσης.....	34
3.2.2	Εκτίμηση και Αντιστάθμιση.....	35
4	Radio Frequency Fingerprinting	42
4.1	Επισκόπηση του RF Fingerprinting	42
4.2	RF Fingerprinting και παραγωγή κλειδιών	44
4.2.1	Παραγωγή κλειδιών με την χρήση <i>CSI</i>	44
4.2.2	Παραγωγή κλειδιών με την χρήση <i>AoA</i> και <i>AoD</i> του <i>mmWave</i> σε <i>massive MIMO</i> κανάλι	45
4.2.3	Εξαγωγή των ιδιοτήτων του σήματος με χρήση ραντάρ.....	47
5	Ασύρματα Συστήματα Καθορισμένα από Λογισμικό	48
5.1	Επισκόπηση Ασύρματων Συστημάτων Καθορισμένων από Λογισμικό.....	48
5.2	Αρχιτεκτονική ενός SDR συστήματος.....	49
5.3	Εργαλεία Υλοποίησης.....	53
5.3.1	Η συσκευή <i>USRP</i>	54
5.3.2	Το λογισμικό <i>GNU Radio</i>	55
6	Υλοποίηση	57
6.1	Μελέτη υλοποίησης	58
6.2	Μοντέλο Συστήματος	59
6.3	Παραγωγή Κλειδιών	60
6.3.1	Παραγωγή μακροπρόθεσμων κλειδιών.....	61
6.3.2	Παραγωγή βραχυπρόθεσμων κλειδιών.....	62
6.4	Υλοποίηση στο <i>GNU Radio</i>	63
6.4.1	Προπαρασκευαστικά βήματα.....	63
6.4.2	Κυρίως Πείραμα.....	64
6.4.3	Επεξήγηση των μπλοκς του διαγράμματος.....	66
6.4.4	Ανάλυση Αποτελεσμάτων.....	69
7	Συμπεράσματα	73
	Επιστημονική Βιβλιογραφία	75
	Διαδικτυακές Πηγές	79
	Παράρτημα I [Επιλογή Πυλών]	80
	Παράρτημα II [Παραγωγή long-term κλειδιού]	82
	Παράρτημα III [Παραγωγή short-term κλειδιού]	84
	Παράρτημα IV [Καταγραφή χρονικής στιγμής άφιξης πακέτου]	86

Παράρτημα V [Υπολογισμός καθυστέρησης διάδοσης].....	87
Παράρτημα VI [Συγχρονισμός μετά από Schmidl & Cox].....	88
Παράρτημα VII [Υπολογισμός Διαφοράς Φάσης] [17]	90
Παράρτημα VIII [Υπολογισμός Ακριβούς Κινούμενου Μέσου Όρου] [17]	91
Παράρτημα IX [Υπολογισμός Μετατόπισης Φάσης] [17].....	92
Παράρτημα X [Υπολογισμός Συσχέτισης] [17]	93
Παράρτημα XI [Υπολογισμός Γωνίας Αφίξης] [17]	95

Λίστα Εικόνων

Εικόνα 2-1: Διάγραμμα ακτινοβολίας για μία ιστροπική κεραία με (α) οριζόντια πόλωση και (β) κάθετη πόλωση. [13]	6
Εικόνα 2-2: Τρισδιάστατη απεικόνιση της ακτινοβολίας μίας ιστροπικής κεραίας. [13]	6
Εικόνα 2-3: Διάγραμμα ακτινοβολίας για δίπολο $\lambda/2$. [14]	6
Εικόνα 2-4: Τρισδιάστατη απεικόνιση της ακτινοβολίας ενός διπόλου $\lambda/2$. [15]	6
Εικόνα 2-5: Αναπαράσταση της ανάκλασης ενός ηλεκτρομαγνητικού κύματος μαζί με όλη την γεωμετρία της διαδικασίας. (α) Η πόλωση του πεδίου E είναι παράλληλη με το πεδίο που επάνω σε αυτό προσπίπτει το κύμα. (β) Η πόλωση του πεδίου E είναι κάθετη στο πεδίο που επάνω σε αυτό προσπίπτει το κύμα. Οι δείκτες i , r , t αφορούν τα πεδία κατά την πρόσπτωση, μετά την ανάκλαση και μετά την ανάκλαση εντός του μέσου αντίστοιχα. Τα ϵ , μ και σ υποδηλώνουν την επιτρεπτότητα, την διαπερατότητα και την αγωγιμότητα του μέσου αντίστοιχα. Το E είναι το ηλεκτρικό πεδίο. [1]	7
Εικόνα 2-6: Αναπαράσταση διάδοσης κατά το μοντέλο ανάκλασης στο έδαφος. Διάδοση τόσο από οπτική επαφή όσο και από ανάκλαση από το έδαφος. [1]	8
Εικόνα 2-7: Αναπαράσταση περίθλασης ενός κύματος όταν ο πομπός έχει ίδιο ύψος με τον δέκτη (αριστερά) και όταν ο δέκτης έχει μικρότερο ύψος από τον πομπό (δεξιά). [1]	9
Εικόνα 2-8: Οι ομόκεντροι κύκλου αποτελούν τις ζώνες Fresnel. [1]	10
Εικόνα 2-9: Αναπαράσταση της περίθλασης καθώς το κύμα προσπίπτει σε εμπόδιο που παρουσιάζει ευθεία ακμή. [1]	10
Εικόνα 2-10: Αντικατάσταση πολλαπλών εμποδίων με ένα ισοδύναμο για τον υπολογισμό της απώλειας λόγω περίθλασης. [1]	10
Εικόνα 2-11: Αναπαράσταση της σκέδασης σε τραχιά επιφάνεια. [16]	11
Εικόνα 2-12: Απεικόνιση της Ολίσθησης Doppler. [1]	14
Εικόνα 2-13: Συγκεντρωμένοι όλοι οι τύποι διαλείψεων μικρής κλίμακας. [1]	18
Εικόνα 2-14: Απεικόνιση ενός βασικού OFDM πομπού. [2]	23
Εικόνα 2-15: Απεικόνιση ενός βασικού OFDM δέκτη. [2]	23
Εικόνα 3-1: Ο PN εισάγει σήματα παρεμβολής στο εύρος ζώνης του σήματος. [2]	29
Εικόνα 3-2: Διασπορά φάσματος λόγω θορύβου φάσης για ένα σύστημα OFDM. [3]	33
Εικόνα 3-3: Διάγραμμα BER σε σχέση με την αύξηση του θορύβου φάσης για ένα σύστημα OFDM. [3]	33
Εικόνα 3-4: Ένα σύστημα OFDM με αντιστάθμιση PN και ισοσταθμιστή στο πεδίο της συχνότητας. Το $e^{j\varphi(t)}$ αποτελεί το σχήμα του φάσματος του PN. [3]	38
Εικόνα 4-1: Διαδικασία κατηγοριοποίησης δακτυλικών αποτυπωμάτων RF. [4]	43
Εικόνα 4-2: Παραγωγή κλειδιών στο φυσικό επίπεδο για συστήματα massive MIMO χιλιοστομετρικών κυμάτων. [7]	47
Εικόνα 5-1: Αρχιτεκτονική SDR συστήματος για έναν (α) πομπό και για έναν (β) δέκτη. [9]	50
Εικόνα 5-2: Εσωτερική αρχιτεκτονική του USRP. [10]	53
Εικόνα 5-3: Κύρια πλακέτα που αποτελεί το USRP. [10]	54
Εικόνα 5-4: Αρχιτεκτονική του περιβάλλοντος του GNU Radio. [10]	56
Εικόνα 6-1: Το μοντέλο συστήματος του πειράματος. Στην διπλωματική ο δέκτης έχει 2 κεραίες και ο πομπός 1 κεραία. Υφίστανται εξασθενήσεις στο σήμα λόγω παρεμβολής κτιρίων και αντικειμένων. [11]	59
Εικόνα 6-2: Δέκτης για την εύρεση της γωνίας άφιξης. Τα blocks “Signal Source” αφορούν τις κεραίες του δέκτη.	63
Εικόνα 6-3: Αποτελέσματα εκτέλεσης του διαγράμματος της Εικόνας 6-2 που παρουσιάζει την εύρεση της Γωνίας Άφιξης (AoA)	64
Εικόνα 6-4: Μεταβλητές για την εκτέλεση του πειράματος.	69

Εικόνα 6-5: Βραχυπρόθεσμο κλειδί.	70
Εικόνα 6-6: Μακροπρόθεσμο κλειδί.	70
Εικόνα 6-7: Πομπός, OFDM διαμόρφωση και ανίχνευση χρονικής στιγμής άφιξης πακέτου.	71
Εικόνα 6-8: Δέκτης, OFDM αποδιαμόρφωση κεφαλίδας, υπολογισμός χρονικής στιγμής άφιξης πακέτου και υπολογισμός καθυστέρησης διάδοσης πακέτου.	71
Εικόνα 6-9: OFDM αποδιαμόρφωση του Payload, απομόνωση πιλότων, υπολογισμός γωνίας άφιξης, πλάτους και φάσης.	72
Εικόνα 6-10: Παραγωγή κλειδιών.	72

Λίστα Πινάκων

Πίνακας 2-1: Τιμές διαφόρων παραμέτρων διαφόρων υλικών σε διαφορετικές συχνότητες. [1] _____ 7

Ακρωνύμια

3GPP	Third Generation Partnership Project
ACI	Adjacent Channel Interference
ACLR	Adjacent Channel Leakage Power Ratio
ADC	Analog-to-Digital Converter
AoA	Angle of Arrival
AoD	Angle of Departure
ASIC	Application Specific Integrated Circuit
AWGN	Additive White Gaussian Noise
BEP	Bit Error Probability
BER	Bit Error Rate
BLAST	Bell Labs Layered Space-Time
BLE	Bluetooth Low Energy
BPSK	Binary Phase-Shift-Keyed
BS	Base Station
CAD	Computer-Aided Design
CDMA	Code-Division Multiple Access
CFO	Carrier Frequency Offset
CMOS	Complementary Metal-Oxide-Semiconductor
CP	Cyclic Prefix
CPU	Central Process Unit
CRLB	Cramér-Rao Lower Bound
CS	Cyclic Suffix
CSI	Channel State Information
CW	Continuous Wave
DAC	Digital-to-Analog Converter
DDC	Digital Down Converter
DFE	Decision-Feedback Equalizer
DFT	Discrete Fourier Transform
D-H	Diffie-Hellman
dHSIC	d-variable Hilbert-Schmidt Independence Criterion
DSP	Digital Signal Processors
DSSS	Direct-Sequence Spread Spectrum
DUC	Digital Up Converter
DUT	Device Under Test

EIRP	Effective Isotropic Radiated Power
EM	Expectation Maximization
eMBB	enhanced Mobile BroadBand
ERP	Effective Radiated Power
EVD	Eigen-Value Decomposition
EVM	Error Vector Magnitude
FDE	Frequency Domain Equalizer
FDMA	Frequency-Division Multiple Access
FFT	Fast Fourier Transform
FIR	Finite Impulse Response
FPGA	Field Programmable Gate Arrays
FSK	Frequency-Shift-Keyed
GPP	General Purpose Processors
GPU	Graphics Processing Units
HF	High Frequency
I	In-phase
ICI	Inter-Carrier Interference
IDFT	Inverse Discrete Fourier Transform
IDFT	Inverse Discrete Fourier Transform
IF	Intermediate Frequency
IFFT	Inverse Fast Fourier Transform
IoT	Internet of Things
IRE	Intended Radiated Emmissions
ISI	Inter-Symbol Interference
LCR	Level Crossing Rate
LDPC	Low Density Parity Check
LMMSE	Linear Minimum Mean Square Error
LNA	Low Noise Amplifier
LO	Local Oscillator
LOS	Line-Of-Sight
LS	Least-Squares
LTE	Long-Term Evolution
M2M	Machine-To-Machine
MAC	Media Access Control
MAP	Maximum A Posteriori

MDDM	Multi-carrier Delay Diversity Modulation
MIMO	Multiple-Input Multiple-Output
MLearning	Machine Learning
MLikelihood	Maximum Likelihood
MLSE	Maximum Likelihood Sequence Estimation
mMTC	massive Machine-Type Communications
MRC	Maximal-Ratio Combining
MSE	Mean Squared Error
MUI	Multi-User Interference
MUSIC	MUltiple Signal Correlation
OFDM	Orthogonal Frequency Division Modulation
PCA	Principal Component Analysis
PDF	Probability Density Function
PGA	Programmable Gain Amplifier
PKG	Physical-layer Key Generation
PLL	Phase-Locked Loop
PMT	PolyMorphic Types
PN	Phase Noise
PSD	Power Spectral Density
Q	Quadrature
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RCS	Radar Cross Section
RF	Radio Frequency
RF-DNA	Radio-Frequency Distinct Native Attribute
RFF	Radio-Frequency Fingerprinting
RFID	Radio-Frequency IDentification
RNR	Random Noise Radar
SC	Single Carrier
SDR	Software-Defined Radio
SFDR	Spurious-Free Dynamic Range
SINR	Signal-to-Interference and Noise Ratio
SIR	Signal-to-Interference Ratio
SIRCIM	Simulation of Indoor Radio Channel Impulse-response Models
SMRCIM	Simulation of Mobile Radio Channel Impulse-response Models

SNR	Signal-to-Noise Ratio
SRC	Sample Rate Conversion
STBC	Space-Time Block-Coding
STTC	Space-Time Trellis-Coding
SURE	Stimulated Unintended Radiated Emmissions
TDD	Time-Division Multiplexing
T-R	Transmitter-Receiver
UHF	Ultra High Frequency
ULA	Uniform Linear Array
UMTS	Universal Mobile Telecommunications System
URE	Unintended Radiated Emmissions
URLLC	Ultra-Reliable Low-Latency Communications
USRP	Universal Software Radio Peripheral
UWB	Ultra WideBand
V2X	Vehicle-to-Everything
VCO	Voltage Control Oscillator
VHF	Very High Frequency
Wi-Fi	Wireless-Fidelity
WLAN	Wireless Local-Area Network
WMAN	Wireless Metropolitan-Area Network

Περίληψη

Η ασύρματη δικτύωση κατέχει ζωτική θέση τόσο σε πολιτικά όσο και σε στρατιωτικά πλαίσια, εξυπηρετώντας βασικές λειτουργίες. Χρησιμοποιείται παντού είτε στην περιήγηση στο Διαδίκτυο (Wi-Fi), είτε στην ακρόαση μουσικής (Bluetooth), είτε στις καθημερινές συναλλαγές (NFC). Ωστόσο, η διασφάλιση της ασφαλούς μετάδοσης πληροφοριών μέσω ασύρματων δικτύων εξακολουθεί να αποτελεί μια τεράστια πρόκληση. Πρωταρχικής σημασίας είναι η διασφάλιση ότι τα ευαίσθητα δεδομένα παραμένουν αποκλειστικά προσβάσιμα σε εξουσιοδοτημένους χρήστες, ματαιώνοντας κάθε απόπειρα μη εξουσιοδοτημένης εισβολής. Στο θεμελιώδες επίπεδο των ασύρματων δικτύων εμφανίζονται δύο βασικοί τύποι επιθέσεων: jamming (παρεμβολή, παρεμπόδιση) και eavesdropping (υποκλοπή). Αυτές οι επιθέσεις στοχεύουν κυρίως το φυσικό επίπεδο, δημιουργώντας σημαντικές ανησυχίες για την ασφάλεια.

Κατά κύριο λόγο, τα επικρατούντα μέτρα ασφαλείας βασίζονται σε κρυπτογραφικές μεθοδολογίες που εφαρμόζονται στα ανώτερα στρώματα των ασύρματων δικτύων. Κατά την εξέταση συμμετρικών κρυπτογραφικών προσεγγίσεων, όπως το Data Encryption Standard (DES), ένα κοινό ιδιωτικό κλειδί βρίσκεται συνήθως μεταξύ δύο χρηστών. Σε σενάρια όπου οι καθορισμένοι χρήστες δεν έχουν πρόσβαση στο κοινό ιδιωτικό κλειδί, η δημιουργία ενός ασφαλούς καναλιού καθίσταται επιτακτική ανάγκη για την ανταλλαγή κλειδιών. Αντί να δημιουργηθεί σε ένα επιπλέον κανάλι επικοινωνίας, η δυνατότητα έγκειται στην αξιοποίηση τεχνικών φυσικού επιπέδου για τη διανομή εμπιστευτικών κλειδιών. Αυτή η προσέγγιση όχι μόνο ενισχύει το απόρρητο της θέσης αλλά χρησιμεύει επίσης ως συμπλήρωμα των αλγορίθμων ασφαλείας στα ανώτερα στρώματα. Η ενσωμάτωση μηχανισμών ασφαλείας φυσικού επιπέδου προσθέτει ένα επίπεδο πολυπλοκότητας για τους κακόβουλους φορείς που στοχεύουν στην αποκρυπτογράφηση των μεταδιδόμενων δεδομένων. Ένας από αυτούς του τρόπους είναι η επίτευξη αυθεντικοποίησης με την ανάλυση μοναδικών χαρακτηριστικών του σήματος αλλά και του καναλιού και ονομάζεται RF Fingerprinting. Στην συνέχεια αυτές τις πληροφορίες αξιοποιούνται προκειμένου να δημιουργήσει μοναδικά κλειδιά τα οποία μπορούν να χρησιμοποιηθούν σε διάφορες εφαρμογές.

Η παρούσα διπλωματική εργασία θα ασχοληθεί με την παραγωγή κλειδιών μέσω των μοναδικών χαρακτηριστικών του ραδιοσήματος και του καναλιού (φάση, καθυστέρηση διάδοσης, πλάτος και εικονική γωνία άφιξης). Ως αποτέλεσμα παρουσιάζεται μία ακριβής μέθοδος παραγωγής κλειδιών και τα αποτελέσματα επαληθεύονται και λαμβάνονται με την βοήθεια εξοπλισμού USRP που προγραμματίζεται από το GNU Radio. Τέλος λαμβάνονται όλα τα αποτελέσματα και αναλύονται για την επαλήθευση της θεωρίας.

Λέξεις Κλειδιά: Μετρήσεις κεραίας, αλγόριθμοι κατηγοριοποίησης, RF Fingerprinting, επεξεργασία σήματος, ασφάλεια στο φυσικό επίπεδο, ασύρματο κανάλι, ασύρματη διάδοση, σήμα καθορισμένο από λογισμικό, USRP.

Abstract

Wireless networking is vital in both civil and military contexts, serving essential functions. It is used everywhere, whether for browsing the Internet (Wi-Fi), listening to music (Bluetooth), or everyday transactions (NFC). However, ensuring the secure transmission of information over wireless networks remains a huge challenge. Of primary importance is ensuring that sensitive data remains exclusively accessible to authorized users, thwarting any attempt at unauthorized intrusion. At the fundamental level of wireless networks, two main types of attacks occur: jamming and eavesdropping. These attacks mainly target the physical layer, raising significant security concerns.

For the most part, the prevailing security measures are based on cryptographic methodologies applied at the upper layers of wireless networks. When considering symmetric cryptographic approaches, such as the Data Encryption Standard (DES), a shared private key is usually found between two users. In scenarios where the designated users do not have access to the shared private key, establishing a secure channel becomes imperative for key exchange. Instead of creating an additional communication channel, the opportunity lies in leveraging physical layer techniques to distribute confidential keys. This approach not only enhances location privacy but also serves as a complement to the security algorithms in the upper layers. The incorporation of physical layer security mechanisms adds a layer of complexity for malicious actors aiming to decrypt transmitted data. One of these ways is the ability to achieve authentication by analyzing unique signal and channel characteristics, which is called RF fingerprinting. Then, this information is exploited in order to generate unique keys which can be used in various applications.

This thesis will deal with key generation through the unique characteristics of the radio signal and channel (phase, propagation delay, amplitude and virtual angle of arrival). As a result, an accurate key generation method is presented and the results are verified and obtained using USRP equipment programmed by GNU Radio. Finally all the results are obtained and analyzed to verify the theory.

Keywords: *Antenna measurements, classification algorithms, RF Fingerprinting, signal processing, physical layer security, wireless channel, wireless propagation, software defined radio, USRP.*

1

Εισαγωγή

1.1 Η Ασφάλεια στις Ασύρματες Επικοινωνίες

Στα ασύρματα δίκτυα, η επικοινωνία μεταξύ εξουσιοδοτημένων χρηστών είναι ευάλωτη σε υποκλοπή από κάποιον επιτιθέμενο λόγω της εγγενούς φύσης εκπομπής του ασύρματου μέσου. Αυτή η ευπάθεια καθιστά τις ασύρματες μεταδόσεις ιδιαίτερα επιρρεπείς σε επιθέσεις υποκλοπής. Για να εξασφαλιστεί η ασφαλής και εμπιστευτική μετάδοση, τα συμβατικά συστήματα επικοινωνίας βασίζονται συνήθως σε κρυπτογραφικές μεθόδους για να εμποδίσουν τους επιτιθέμενους να υποκλέψουν τα δεδομένα που ανταλλάσσονται μεταξύ εξουσιοδοτημένων χρηστών. Λαμβάνοντας ως ενδεικτικό παράδειγμα την κρυπτογράφηση συμμετρικού κλειδιού, η διαδικασία περιλαμβάνει την εξασφάλιση της μετάδοσης δεδομένων. Αρχικά, ο κόμβος προέλευσης κρυπτογραφεί τα αρχικά δεδομένα (που αναφέρονται ως απλό κείμενο) χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης και ένα μυστικό κλειδί που μοιράζεται αποκλειστικά με τον κόμβο προορισμού. Μετά, το κρυπτογραφημένο απλό κείμενο (που ονομάζεται και κρυπτογράφημα) αποστέλλεται στον προορισμό, όπου αποκρυπτογραφείται με τη χρήση του μυστικού κλειδιού που είναι κοινόχρηστο από πριν. Τονίζεται ότι η ασφάλεια της μετάδοσης κρυπτογραφήματος δεν είναι απολύτως εγγυημένη, καθώς ένας υποκλοπέας θα μπορούσε να αποκρυπτογραφήσει το κρυπτογράφημα χρησιμοποιώντας εξαντλητική αναζήτηση κλειδιών, που συνήθως αναφέρεται ως brute-force επίθεση. Ως αντίμετρο, η έννοια της ασφάλειας φυσικού επιπέδου κερδίζει έδαφος ως εναλλακτική προσέγγιση για τη διασφάλιση των ασύρματων επικοινωνιών από διάφορες προσπάθειες υποκλοπής, συμπεριλαμβανομένων των επιθέσεων brute-force.

Τα θεμέλια για την ασφάλεια φυσικού επιπέδου τέθηκαν με την εμβάθυνση στη σφαίρα των ασφαλών επικοινωνιών εν μέσω της ύπαρξης ενός υποκλοπέα, εστιάζοντας σε ένα διακριτό κανάλι υποκλοπής χωρίς μνήμη. Η επίτευξη απόλυτα ασφαλούς μετάδοσης δεδομένων αποδείχθηκε και

είναι δυνατή όταν η χωρητικότητα του καναλιού της κύριας ζεύξης (που εκτείνεται από την πηγή στον προορισμό) υπερβαίνει εκείνη της ζεύξης υποκλοπής (που εκτείνεται από την πηγή στον υποκλοπέα). Στη συνέχεια, το πεδίο εφαρμογής επεκτάθηκε από το διακριτό κανάλι υποκλοπής χωρίς μνήμη για να συμπεριλάβει το γκαουσιανό κανάλι υποκλοπής. Αυτή η εξέλιξη οδήγησε στην έννοια της «χωρητικότητας μυστικότητας», η οποία καθορίζεται με την ποσοτικοποίηση της διαφοράς μεταξύ της χωρητικότητας καναλιού της κύριας ζεύξης και της ζεύξης υποκλοπής. Όταν η χωρητικότητα μυστικότητας πέφτει σε αρνητική περιοχή, η μετάδοση από την πηγή στον προορισμό χάνει την ασφάλειά της, καθιστώντας τον υποκλοπέα ικανό να υποκλέψει επιτυχώς τη μετάδοση της πηγής. Στην ουσία, αυτό σηματοδοτεί την εμφάνιση ενός συμβάντος υποκλοπής. Η ενίσχυση της ασφάλειας μετάδοσης έναντι επιθέσεων υποκλοπής εξαρτάται από τη μείωση της πιθανότητας ενός συμβάντος υποκλοπής, που συνήθως αναφέρεται ως πιθανότητα υποκλοπής. Ο στόχος αυτός επιτυγχάνεται με την αύξηση της χωρητικότητας μυστικότητας. Όμως, στις ασύρματες επικοινωνίες, το φαινόμενο της εξασθένησης αποτελεί σημαντική πρόκληση, οδηγώντας σε σημαντική επιδείνωση της χωρητικότητας μυστικότητας.

Έτσι, προκειμένου να αυξηθεί η χωρητικότητα μυστικότητας και να εξασφαλισθεί η ασφαλής επικοινωνία μεταξύ πομπού και δέκτη, αναπτύχθηκαν αρκετές έρευνες και εργασίες. Μία από αυτές αφορά το κανάλι πολλαπλών εισόδων και πολλαπλών εξόδων (MIMO). Στόχος ήταν η ενίσχυση της χωρητικότητας της ασύρματης μυστικότητας σε σενάρια εξασθένησης. Επιπλέον, διεξήχθη διεξοδική ανάλυση σε συνεργατικούς αναμεταδότες, με σκοπό την ενίσχυση της ασφάλειας στο φυσικό επίπεδο σε σχέση με την απόδοση του ρυθμού μυστικότητας. Επίσης, διερευνήθηκε μια καινοτόμος στρατηγική που περιλαμβάνει υβριδικές τεχνικές συνεργατικής διαμόρφωσης δέσμης (Beamforming) και παρεμβολών. Ο στόχος ήταν να αυξηθεί η ικανότητα ασύρματης μυστικότητας. Αυτό επιτεύχθηκε με την παροχή δυνατότητας σε συγκεκριμένους κόμβους αναμετάδοσης να υποστηρίξουν τη μετάδοση από την πηγή στον εξουσιοδοτημένο προορισμό με τη χρήση κατανεμημένης διαμόρφωσης δέσμης. Εν τω μεταξύ, οι υπόλοιποι κόμβοι αναμετάδοσης χρησιμοποιήθηκαν για τη μετάδοση τεχνητού θορύβου, με σκοπό να «μπερδέψουν» τυχόν πιθανούς υποκλοπέες. Σε μια πιο σύγχρονη μέθοδο, έχει αναδυθεί ένα νέο πλαίσιο ασφάλειας. Αυτό το πλαίσιο λειτουργεί στη διασταύρωση τόσο του φυσικού επιπέδου όσο και του επιπέδου εφαρμογής, με στόχο την ενίσχυση της ασφάλειας της ασύρματης διανομής πληροφορίας. Αυτό επιτυγχάνεται με την αξιοποίηση όχι μόνο προηγμένων τεχνικών επεξεργασίας σήματος στο φυσικό επίπεδο, αλλά και με την ενσωμάτωση μέτρων ανώτερου επιπέδου, όπως η πιστοποίηση γνησιότητας και οι μέθοδοι υδατογράφησης. Το συνδυασμένο αποτέλεσμα αυτών των στρατηγικών συμβάλλει σε ένα αυξημένο επίπεδο ασφάλειας κατά τη διανομή περιεχομένου μέσω του ασύρματου καναλιού.

1.2 Αντικείμενο διπλωματικής

Η παρούσα διπλωματική, αξιοποιώντας όλες τις απαραίτητες γνώσεις σχετικά με το κανάλι, τις αλλοιώσεις και τις ιδιότητες του ραδιοσήματος και του καναλιού, θα ασχοληθεί με ένα κομμάτι το οποίο είναι αποδεδειγμένα λειτουργικό και αξιόπιστο. Αυτό είναι το RF Fingerprinting και η δυνατότητα παραγωγής κλειδιών για οποιαδήποτε χρήση μέσω αυτού. Στην ουσία το RF Fingerprinting αποτελεί το δακτυλικό αποτύπωμα μίας εκπομπής. Αυτό μπορεί να αποτελείται από την γωνία άφιξης του σήματος στον δέκτη, την φάση, την καθυστέρηση διάδοσης και το πλάτος. Αυτά τα χαρακτηριστικά εξασφαλίζουν την μοναδικότητα του σήματος δημιουργώντας κατάλληλο

έδαφος για την χρήση τους σε εφαρμογές προστασίας της ιδιωτικότητας και εμπιστευτικότητας των δεδομένων που μεταδίδονται μεταξύ ενός πομπού και ενός δέκτη. Συνοπτικά, ο δέκτης, διαθέτοντας περισσότερες από μία κεραίες περιορίζοντας τις διαλείψεις, λαμβάνοντας το σήμα, υπολογίζει την εικονική γωνία άφιξης (AoA – Angle of Arrival), εκτιμά την καθυστέρηση διάδοσης, την φάση και καταγράφοντας το πλάτος εκείνη την χρονική στιγμή, προκειμένου, μέσα από έναν αποδοτικό αλγόριθμο να παραχθούν δυαδικά κλειδιά. Με αυτό τον τρόπο δίνεται η δυνατότητα σε επόμενες εργασίες να αξιοποιήσουν αυτά τα κλειδιά για να επιτύχουν αναγνώριση και αυθεντικοποίηση της εκπομπής από την μεριά του δέκτη έτσι ώστε κανένας επιτιθέμενος να μην μπορεί να παρεμβληθεί και να παραβιάσει την επικοινωνία είτε εξαπατώντας τον δέκτη στέλνοντάς του μη εξουσιοδοτημένη πληροφορία, είτε υποκλέποντας δεδομένα.

1.3 Δομή της διπλωματικής

Στο Κεφάλαιο 1 γίνεται μία γενική επισκόπηση σχετικά με το αντικείμενο που θα ασχοληθεί η παρούσα διπλωματική. Στο Κεφάλαιο 2, αναλύονται οι διαλείψεις μικρής και μεγάλης κλίμακας καθώς και η διαμόρφωση OFDM. Στο Κεφάλαιο 3, γίνεται η περιγραφή των αλλοιώσεων που υφίστανται οι ραδιοσυχνότητες. Από το Κεφάλαιο 4 και έπειτα γίνεται συγκεκριμενοποίηση στο κύριο θέμα της διπλωματικής εργασίας. Αναλυτικότερα, στο Κεφάλαιο 4 περιγράφεται το Radio Frequency Fingerprinting και εξειδικεύεται στην χρήση του για παραγωγή κλειδιών. Στο Κεφάλαιο 5, συζητούνται τα συστήματα ραδιοσυχνοτήτων καθορισμένες από λογισμικό και ειδικεύονται στην χρήση USRP με την βοήθεια του λογισμικού GNU Radio. Τέλος, το Κεφάλαιο 6 αναλύει το πείραμα που θα πραγματοποιηθεί, το μοντέλο συστήματος και παρουσιάζει τα αποτελέσματα από τις πραγματικές πειραματικές δοκιμές.

2

Το Ασύρματο Κανάλι

Στις Ασύρματες Επικοινωνίες με τον όρο «Ασύρματο Κανάλι» θεωρητικά είναι ένα νοητό καλώδιο που συνδέει ασύρματα πομπό και δέκτη με σκοπό την ανταλλαγή δεδομένων μεταξύ τους. Μέσα από αυτό το υποτιθέμενο καλώδιο, διέρχονται όλες οι πληροφορίες που θέλει να στείλει ένας πομπός σε έναν ή πολλούς δέκτες. Στην πραγματικότητα πρόκειται για το κενό ή αέρας μέσω του οποίου θα ταξιδέψουν οι πληροφορίες από το ένα άκρο στο άλλο. Προκειμένου να επικοινωνήσει πομπός και δέκτης, συντονίζονται στην ίδια συχνότητα. Ο αέρας, ωστόσο, δεν είναι σαν το καλώδιο το οποίο περιέχει διαχώριση του εσωτερικού και εξωτερικού περιβάλλοντος (περίβλημα). Στον αέρα το σήμα υπόκειται διάφορες αλλοιώσεις λόγω των αντικειμένων που παρεμβάλλονται (κτίρια, δέντρα, βουνά) και της κινητικότητας του δέκτη, του πομπού ή των σκεδαστών μέσα στον χώρο (αυτό πρακτικά σημαίνει το πόσο μεγάλη είναι η ισοδύναμη ταχύτητα κίνησης του δέκτη). Το πιο δύσκολο διαχρονικά είναι η μοντελοποίηση του ασύρματου καναλιού. Για να λυθεί αυτό το πρόβλημα χρησιμοποιούνται στατιστικές μέθοδοι. Υπάρχουν δύο γενικές κατηγορίες διαλείψεων, οι Διαλείψεις Μεγάλης Κλίμακας οι οποίες περιέχουν τις απώλειες διάδοσης και την σκίαση μέσω βασικών μηχανισμών όπως η ανάκλαση, η περίθλαση και η σκέδαση και οι Διαλείψεις Μικρής Κλίμακας οι οποίες περιέχουν και την διαχώριση του σήματος σε Πολλαπλές Διαδρομές (Multipath) που επηρεάζεται από την χρονική διασπορά, την ολίσθηση Doppler και την αλλαγή στην ισχύ του σήματος λόγω της πολυδιαδρομικότητας. Μέσα σε αυτές περιέχονται και συγκεκριμένοι τρόποι μοντελοποίησης προκειμένου να προβλεφθούν οι αλλαγές στο σήμα.

2.1 Διαλείψεις Μεγάλης Κλίμακας

Η διάδοση των ηλεκτρομαγνητικών κυμάτων οφείλεται στην ανάκλαση, την περίθλαση και την σκέδαση. Όπως είναι φυσικό, είναι αδύνατο όλοι οι δέκτες να έχουν άμεση οπτική επαφή με τον πομπό λόγω των αντικειμένων και κτιρίων που προκαλούν περίθλαση. Επίσης, η ισχύς των ηλεκτρομαγνητικών κυμάτων σε μία συγκεκριμένη θέση και κατά την απομάκρυνση του πομπού από τον δέκτη μειώνεται λόγω ανακλάσεων από διάφορα αντικείμενα με αποτέλεσμα να διασπείρονται στον χώρο ακολουθώντας διαφορετικές διαδρομές. Έχουν αναπτυχθεί αρκετά μοντέλα για την διάδοση ηλεκτρομαγνητικών κυμάτων και προβλέπουν την μεταβλητότητα της ισχύος του σήματος όταν πομπός και δέκτης βρίσκονται σε κοντινή απόσταση καθώς και τον

υπολογισμό της μέσης λαμβανόμενης ισχύος σε συγκεκριμένη απόσταση πομπού και δέκτη. Υπάρχουν δύο κατηγορίες μοντέλων, τα μοντέλα διάδοσης μικρής κλίμακας ή μοντέλα εξασθένησης που χρησιμοποιούνται για την κατανόηση του τρόπου με τον οποίο η ισχύς του σήματος αλλάζει πολύ γρήγορα σε μικρές αποστάσεις ή μικρά χρονικά διαστήματα, και τα μοντέλα διάδοσης μεγάλης κλίμακας που ασχολούνται με την εκτίμηση κάλυψης ραδιοσυχνοτήτων σε μία περιοχή από τον πομπό αλλά και με την μέτρηση της ισχύος σήματος για μεγάλη απόσταση μεταξύ πομπού και δέκτη (T-R). Αυτό το κεφάλαιο θα ασχοληθεί με τα μοντέλα μεγάλης κλίμακας και θα αναλυθούν οι τρόποι με τους οποίους μπορεί να προβλεφθεί η λαμβανόμενη ισχύς σε συστήματα κινητών επικοινωνιών.

2.1.1 Μοντέλο διάδοσης στον ελεύθερο χώρο

Ένα μοντέλο που υφίσταται στις ασύρματες επικοινωνίες είναι το μοντέλο διάδοσης στον ελεύθερο χώρο το οποίο είναι χρήσιμο για να υπολογιστεί το πόσο ισχυρό θα είναι ένα σήμα όταν δεν υπάρχει τίποτα που να το εμποδίζει μεταξύ του πομπού και του δέκτη. Αυτό χρησιμοποιείται συχνά για διάφορες επικοινωνίες όπως οι δορυφορικές και οι ραδιοεξέυξεις που χρειάζονται καθαρή οπτική επαφή (LOS). Το μοντέλο αυτό δείχνει ότι όσο πιο μακριά βρίσκονται ο αποστολέας και ο δέκτης, τόσο πιο αδύναμο θα είναι το λαμβανόμενο σήμα. Ο τύπος που δείχνει αυτή την σχέση είναι:

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \quad (2.1.1.1)$$

με P_t να αποτελεί την ισχύ που λαμβάνει ο δέκτης για μία συγκεκριμένη απόσταση πομπού και δέκτη που δηλώνεται ως d , P_t την ισχύ που εκπέμπεται από τον πομπό, G_r το κέρδος της κεραίας που διαθέτει ο δέκτης, G_t το κέρδος της κεραίας που διαθέτει ο πομπός, λ το μήκος κύματος υπολογισμένο σε μέτρα και L έναν συντελεστή για τις απώλειες του ασύρματου συστήματος που δεν προκαλείται από την διάδοση. Το L πρέπει να είναι μεγαλύτερο ή ίσο του 1 ($L \geq 1$). Εφόσον $L=1$ τότε το σύστημα δεν έχει απώλειες. Συμπληρωματικά της ισότητας 2.1.1.1 υπάρχουν οι παρακάτω ισότητες που αφορούν:

- $\lambda = \frac{c}{f}$ (μήκος κύματος σε μέτρα, όπου c η ταχύτητα του φωτός και f η συχνότητα).
- $G = \frac{4\pi A_e}{\lambda^2}$ (κέρδος της κεραίας, όπου A_e η ενεργός επιφάνειά της).

Η ιδανική κεραία αναφοράς κατανέμει την ακτινοβολία (το σήμα) προς όλες τις κατευθύνσεις με αποτέλεσμα σε κάθε γωνία σε σχέση με αυτή να υπάρχει μοναδιαίο κέρδος. Αυτή η κεραία ονομάζεται ισοτροπική και αποτελεί σημείο σύγκρισης κέρδους διάφορων κεραίων. Μία κεραία εκπέμπει ισχύ ίση με:

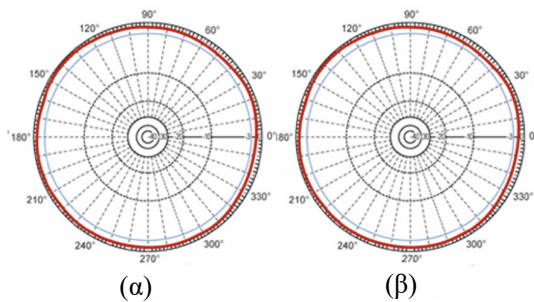
$$EIRP = P_t G_t \quad (2.1.1.2)$$

προς την κατεύθυνση του μεγίστου κέρδους σε σύγκριση με μία ισοτροπική κεραία. Πρακτικά όμως τέτοια κεραία δεν υπάρχει λόγω διάφορων απωλειών σε όλες τις γωνίες της. Γι' αυτό τον λόγο η σύγκριση γίνεται με μία απλή κεραία (δίπολο $\lambda/2$) με αποτέλεσμα η εκπεμπόμενη ισχύς να ονομάζεται ως Effective Radiated Power (ERP). Ένα δίπολο $\lambda/2$ έχει κέρδος κατά 2,15dB

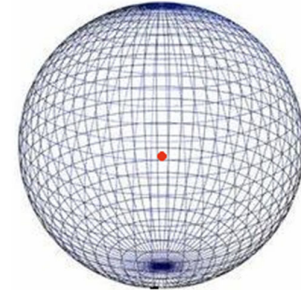
μεγαλύτερο σε σχέση με μία ιστροπική κεραία με αποτέλεσμα το EIRP να είναι μεγαλύτερο κατά 2,15dB από το ERP. [1]

Επομένως είτε έχοντας είτε όχι τα κέρδη κεραιών, μπορεί να υπολογισθεί η απώλεια διαδρομής στο μοντέλο ελεύθερου χώρου:

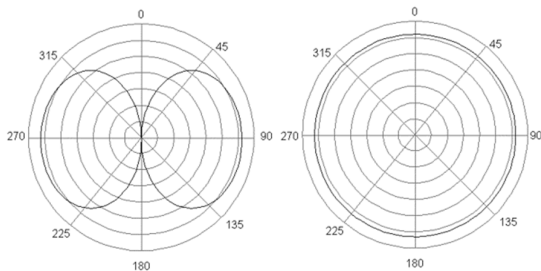
$$PL(dB) = 10 \log \frac{P_t}{P_r} = -10 \log \left(\frac{G_t G_r \lambda^2}{(4\pi)^2 d^2} \right) \text{ ή } -10 \log \left(\frac{\lambda^2}{(4\pi)^2 d^2} \right) \quad (2.1.1.3)$$



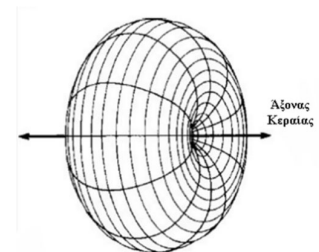
Εικόνα 2-1: Διάγραμμα ακτινοβολίας για μία ιστροπική κεραία με (α) οριζόντια πόλωση και (β) κάθετη πόλωση. [13]



Εικόνα 2-2: Τρισδιάστατη απεικόνιση της ακτινοβολίας μίας ιστροπικής κεραίας. [13]



Εικόνα 2-3: Διάγραμμα ακτινοβολίας για δίπολο $\lambda/2$. [14]

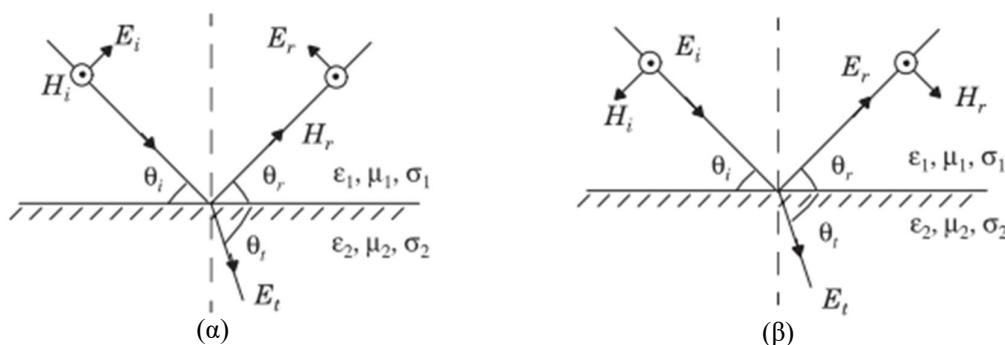


Εικόνα 2-4: Τρισδιάστατη απεικόνιση της ακτινοβολίας ενός διπόλου $\lambda/2$. [15]

2.1.2 Οι Μηχανισμοί Διάδοσης - Ανάκλαση

Η Ανάκλαση επιτυγχάνεται όταν ένα ηλεκτρομαγνητικό κύμα προσπίπτει σε ένα μέσο που έχει διαφορετικά ηλεκτρικά χαρακτηριστικά από το μέσο μέσω του οποίου διαδίδεται. Λόγω αυτού του φαινομένου το κύμα επανεκπέμπεται εν μέρει σε περίπτωση που το μέσο πάνω στο οποίο πέφτει πάνω του είναι τέλειο διηλεκτρικό ή πλήρως σε περίπτωση που είναι τέλειος αγωγός. Το αρχικό κύμα που προσπίπτει στο μέσο, μπορεί να συσχετιστεί με την ένταση του ηλεκτρικού πεδίου των ανακλώμενων κυμάτων που επανεκπέμπονται από την ανάκλαση με την βοήθεια ενός συντελεστή. Ο συντελεστής αυτός προσδιορίζεται από τις ιδιότητες του υλικού, από την πόλωση του κύματος, την γωνία πρόσπτωσης καθώς και την συχνότητα του αρχικού κύματος και ονομάζεται συντελεστής ανάκλασης Fresnel.

Το αρχικό κύμα προσπίπτει επάνω σε διηλεκτρικό μέσο και αφού γίνει η πρόσπτωση χωρίζεται σε δύο συνιστώσες θεωρητικά. Η μία συνιστώσα υποδηλώνει την ανάκλαση του κύματος στο αρχικό μέσο με γωνία r και η άλλη την ανάκλαση του κύματος εντός του διηλεκτρικού μέσου. Εξετάζονται δύο διαφορετικές πολώσεις. Στην πρώτη περίπτωση, η πόλωση του πεδίου E είναι παράλληλη με το πεδίο που επάνω σε αυτό προσπίπτει το κύμα ενώ στην δεύτερη η πόλωση του πεδίου E είναι κάθετη προς αυτό. Για την εύρεση του της διηλεκτρικής σταθεράς είναι απαραίτητο να είναι γνωστά η διαπερατότητα, η αγωγιμότητα και η επιτρεπτότητα (ικανότητα ενός υλικού να αποθηκεύει ενέργεια μέσα του) του μέσου. Όταν το διηλεκτρικό μέσο δεν έχει απώλειες τότε η σταθερά του σχετίζεται με την διαπερατότητά του. Σε περίπτωση που το διηλεκτρικό μέσο έχει απώλειες, τότε η ισχύς απορροφάται από αυτό.



Εικόνα 2-5: Αναπαράσταση της ανάκλασης ενός ηλεκτρομαγνητικού κύματος μαζί με όλη την γεωμετρία της διαδικασίας. (α) Η πόλωση του πεδίου E είναι παράλληλη με το πεδίο που επάνω σε αυτό προσπίπτει το κύμα. (β) Η πόλωση του πεδίου E είναι κάθετη στο πεδίο που επάνω σε αυτό προσπίπτει το κύμα. Οι δείκτες i , r , t αφορούν τα πεδία κατά την πρόσπτωση, μετά την ανάκλαση και μετά την ανάκλαση εντός του μέσου αντίστοιχα. Τα ϵ , μ και σ υποδηλώνουν την επιτρεπτότητα, την διαπερατότητα και την αγωγιμότητα του μέσου αντίστοιχα. Το E είναι το ηλεκτρικό πεδίο. [1]

Για διάφορα αντικείμενα που προσπίπτει πάνω το κύμα έχουν υπολογιστεί διαφορετικοί παράμετροι για κάθε ένα από αυτά σε διαφορετικές συχνότητες. Στον παρακάτω πίνακα φαίνονται αυτοί οι υπολογισμοί:

Πίνακας 2-1: Τιμές διαφόρων παραμέτρων διαφόρων υλικών σε διαφορετικές συχνότητες. [1]

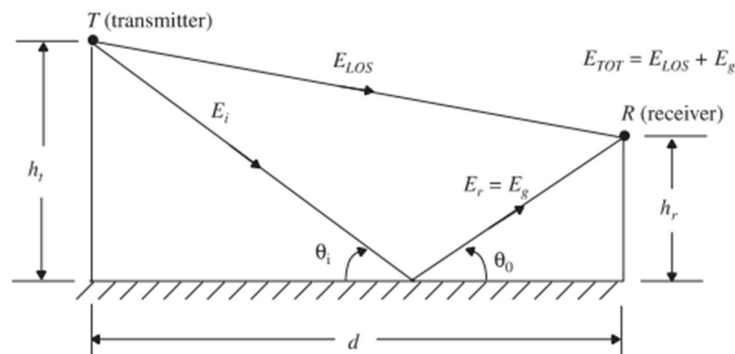
Υλικό	Διηλεκτρική Σταθερά	Αγωγιμότητα	Συχνότητα
Ελλειπές Έδαφος	4	0.001	100
Τυπικό Έδαφος	15	0.005	100
Ιδανικό Έδαφος	25	0.02	100
Θαλασσινό Νερό	81	5	100
Πόσιμο Νερό	81	0.001	100
Τούβλο	4.44	0.001	4000
Ασβεστόλιθος	7.51	0.028	4000
Γυαλί τύπου 707	4	0.00000018	1
Γυαλί τύπου 707	4	0.000027	100
Γυαλί τύπου 707	4	0.005	10000

Στο αρχικό μέσο υπάρχει μία γωνία στην οποία δεν υφίσταται ανάκλαση. Ονομάζεται γωνία Brewster, εμφανίζεται όταν η γωνία πρόσπτωσης επηρεάζει τον συντελεστή ανάκλασης ώστε να είναι μηδενικός και λαμβάνει χώρα μόνο σε κάθετη πόλωση.

Παραπάνω εξετάστηκε η περίπτωση που το προσπίπτον κύμα «πέσει» επάνω σε διηλεκτρικό μέσο. Όταν όμως «πέσει» επάνω σε έναν τέλει αγωγό, επειδή δεν μπορεί να απορροφήσει ηλεκτρομαγνητική ενέργεια, το κύμα θα ανακλαστεί πλήρως χωρίς απώλειες. Έτσι για την περίπτωση που η πόλωση του πεδίου E είναι παράλληλη με το πεδίο που επάνω σε αυτό προσπίπτει το κύμα, ισχύει ότι η γωνία πρόσπτωσης είναι ίση με την γωνία ανάκλασης, το πεδίο E της πρόσπτωσης είναι ίδιο με το πεδίο E στην ανάκλαση και ο συντελεστής ανάκλασης είναι μοναδιαίος. Στην περίπτωση που η πόλωση του πεδίου E είναι κάθετη προς αυτό ισχύει ότι το ηλεκτρικό πεδίο πριν την ανάκλαση είναι ουσιαστικά το αρνητικό ηλεκτρικό πεδίο μετά την ανάκλαση και ο συντελεστής ανάκλασης είναι -1. [1]

2.1.3 Μοντέλο Ανάκλασης (Δύο Ακτινών) στο Έδαφος

Στα ασύρματα κανάλια, το μοντέλο διάδοσης στον ελεύθερο χώρο είναι ανακριβές καθώς στις περισσότερες περιπτώσεις υπάρχουν πολλαπλά φυσικά μέσα διάδοσης. Στην παρακάτω εικόνα (Εικόνα 2-6) απεικονίζεται το μοντέλο ανάκλασης (δύο ακτινών) στο έδαφος το οποίο λαμβάνει υπόψη τόσο τις άμεσες όσο και τις ανακλώμενες από το έδαφος διαδρομές και είναι χρήσιμο για την πρόβλεψη της ισχύος του σήματος σε συστήματα κινητής ραδιοεπικοινωνίας με ψηλούς πύργους και κανάλια μικροκυψελών άμεσης οπτικής επαφής σε αστικά περιβάλλοντα. Το μοντέλο είναι αρκετά ακριβές για αποστάσεις αρκετών χιλιομέτρων. Το συνολικό λαμβανόμενο ηλεκτρικό πεδίο είναι το λαμβανόμενο ηλεκτρικό πεδίο οπτικής επαφής συν το λαμβανόμενο ηλεκτρικό πεδίο που ανακλάται από το έδαφος.



Εικόνα 2-6: Αναπαράσταση διάδοσης κατά το μοντέλο ανάκλασης στο έδαφος. Διάδοση τόσο από οπτική επαφή όσο και από ανάκλαση από το έδαφος. [1]

Στο συγκεκριμένο μοντέλο, προκειμένου να υπολογιστεί η λαμβανόμενη ισχύς για μία απόσταση d μεταξύ πομπού και δέκτη, χρησιμοποιείται ο παρακάτω τύπος:

$$P_r(d) = P_t G_t G_r \frac{(h_t)^2 (h_r)^2}{d^4} \quad (2.1.3.1)$$

Από τον παραπάνω τύπο (2.1.3.1) παρατηρείται ότι όσο πιο μεγάλη είναι η απόσταση d ανάμεσα σε T-R, τόσο μειώνεται η λαμβανόμενη ισχύς. Η διαφορά αυτού του μοντέλου με το μοντέλο

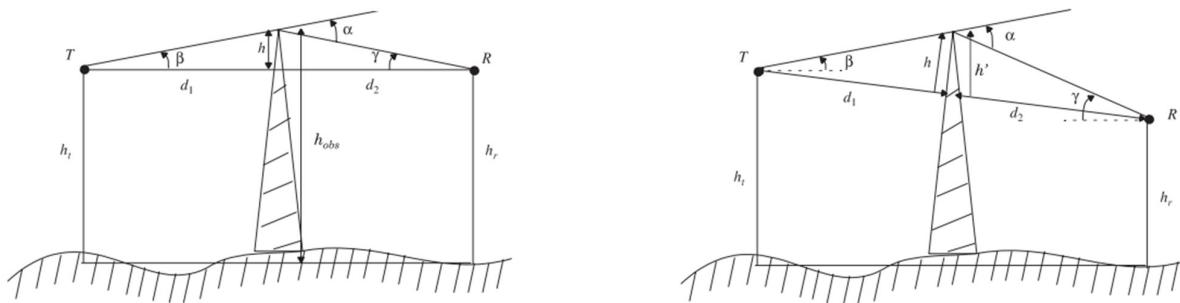
ελεύθερου χώρου είναι ότι στην προκειμένη περίπτωση, η απώλεια διαδρομής είναι πιο γρήγορη. Έτσι η απώλεια αυτή μπορεί να υπολογισθεί με αυτό τον τύπο:

$$PL(dB) = 10 \log P_r = 40 \log d - (10 \log G_t + 10 \log G_r + 20 \log h_t + 20 \log h_r) \quad (2.1.3.2)$$

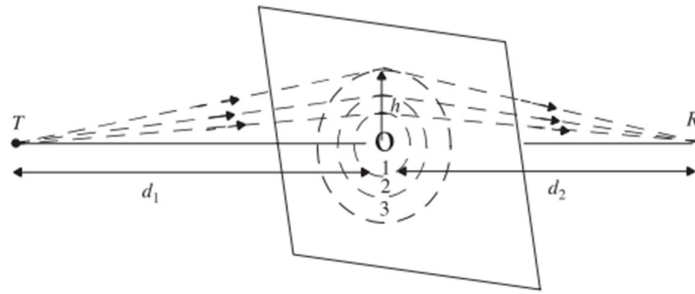
2.1.4 Οι Μηχανισμοί Διάδοσης - Περίθλαση

Η Περίθλαση επιτρέπει στα ραδιοσήματα να ταξιδεύουν γύρω από την καμπυλωτή επιφάνεια της γης και πίσω από εμπόδια, παρόλο που η ισχύς του σήματος μειώνεται όσο προχωράει βαθύτερα σε μία σκιασμένη περιοχή. Για την εξήγηση αυτού του φαινομένου χρησιμοποιείται η αρχή του Huygen, η οποία υποδηλώνει ότι όλα τα σημεία ενός κύματος μπορούν να θεωρηθούν ως σημειακές πηγές για την παραγωγή δευτερογενών κυμάτων που συνδυάζονται για να δημιουργήσουν ένα νέο κύμα στην κατεύθυνση διάδοσης. Η περίθλαση εμφανίζεται όταν τα δευτερεύοντα κύματα διαδίδονται στη σκιασμένη περιοχή. Οι συνιστώσες του ηλεκτρικού πεδίου όλων των δευτερογενών κυμάτων στο χώρο γύρω από το εμπόδιο προστίθενται για να προσδιορίσουν την ένταση του πεδίου ενός περιθλώμενου κύματος στη σκιασμένη περιοχή.

Στην παρακάτω εικόνα (Εικόνα 2-7) απεικονίζεται ένα ζεύγος T-R οι οποίοι διαχωρίζονται από ένα αντικείμενο (εμπόδιο) σε ελεύθερο χώρο. Είναι εύκολα αντιληπτό ότι σε σύγκριση με την άμεση οπτική επαφή το κύμα που ταξιδεύει περνώντας από την κορυφή του εμποδίου, καλύπτει μεγαλύτερη απόσταση. Η θέση του πομπού και του δέκτη, καθώς και το ύψος και η θέση του εμποδίου, επηρεάζουν τη διαφορά φάσης μεταξύ μιας LOS και μιας περιθλώμενης διαδρομής. Σε πραγματικές καταστάσεις, είναι προτιμότερο να μειώνονται όλα τα ύψη με βάση μία σταθερά, έτσι ώστε οι υπολογισμοί να είναι πιο εύκολοι χωρίς να επηρεάζονται οι γωνίες. Μέσω των ζωνών Fresnel (ομόκεντροι κύκλοι στην Εικόνα 2-8) που αποτελούν διαδοχικές περιοχές όπου η απόσταση της LOS διαδρομής είναι μικρότερη από αυτή της περιθλώμενης διαδρομής, μπορεί να υπολογιστεί η απώλεια της περίθλασης. Ο αντίκτυπος αυτών των ζωνών είναι ότι παρέχουν εναλλάξ ευεργετικές και επιβλαβείς παρεμβολές στο συνολικό λαμβανόμενο σήμα. Όσο πιο μεγάλη η ακτίνα του κύκλου (όταν το εμπόδιο είναι στο κέντρο της απόστασης μεταξύ πομπού και δέκτη, η ακτίνα είναι μεγαλύτερη ενώ μικραίνουν όταν αυτό πηγαίνει πιο κοντά είτε στον πομπό είτε στον δέκτη), τόσο μεγαλύτερη απόσταση διανύει το κύμα για να φτάσει στον πομπό. Το φαινόμενο αυτό δείχνει πώς η συχνότητα και η τοποθέτηση των εμποδίων σε σχέση με τον πομπό ή τον δέκτη επηρεάζουν τη σκίαση.



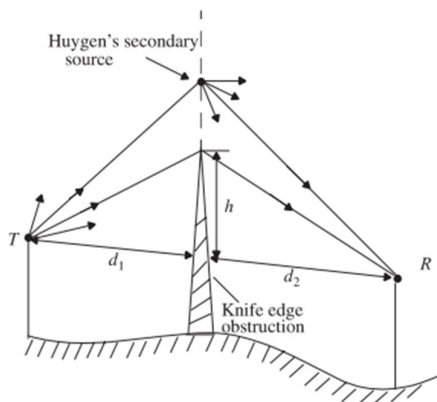
Εικόνα 2-7: Αναπαράσταση περίθλασης ενός κύματος όταν ο πομπός έχει ίδιο ύψος με τον δέκτη (αριστερά) και όταν ο δέκτης έχει μικρότερο ύψος από τον πομπό (δεξιά). [1]



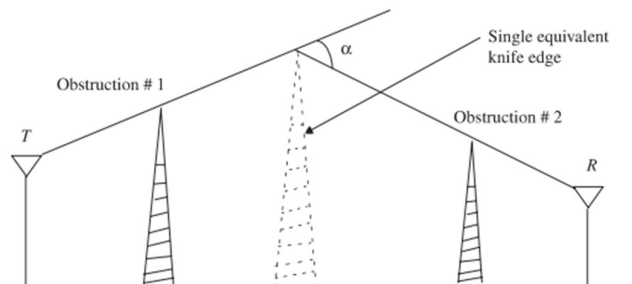
Εικόνα 2-8: Οι ομόκεντροι κύκλοι αποτελούν τις ζώνες Fresnel. [1]

Σε μία πόλη, το σήμα υπόκειται εξασθένηση εξαιτίας της περίθλασης αφού διάφορα εμπόδια όπως λόφοι και κτίρια παρεμβάλλονται μεταξύ πομπού και δέκτη. Γι' αυτό τον λόγο είναι επιβεβλημένη η εκτίμηση της εξασθένησης για να μπορέσει να προβλεφθεί η ισχύς του πεδίου σε μία συγκεκριμένη περιοχή. Παρότι είναι ανακριβείς οι εκτιμήσεις εξασθένησης λόγω της πολυπλοκότητας του εδάφους, έχουν αναπτυχθεί ορισμένες εκφράσεις για τις απώλειες λόγω περίθλασης. Το απλούστερο μοντέλο περίθλασης για αυτές τις εκτιμήσεις είναι η θεωρία ενός αντικειμένου που παρουσιάζει ευθεία ακμή (Knife-Edge). Με την χρήση ζωνών Fresnel μπορεί να λυθεί αυτό το ζήτημα. Στην παρακάτω εικόνα (Εικόνα 2-9) απεικονίζεται η περίθλαση του κύματος σε εμπόδιο με ευθεία ακμή και ενώ ο δέκτης είναι υπό την σκιά του.

Μία άλλη προέκταση της περίθλασης σε ένα μόνο εμπόδιο είναι η περίθλαση σε πολλαπλά εμπόδια που παρουσιάζουν ευθεία ακμή. Έχουν αναπτυχθεί αρκετά μοντέλα. Το πιο ακριβές και απλό είναι η αντικατάσταση των πολλών εμποδίων με ένα ισοδύναμο το οποίο παρουσιάζεται στην παρακάτω Εικόνα 2-10. [1]



Εικόνα 2-9: Αναπαράσταση της περίθλασης καθώς το κύμα προσπίπτει σε εμπόδιο που παρουσιάζει ευθεία ακμή. [1]



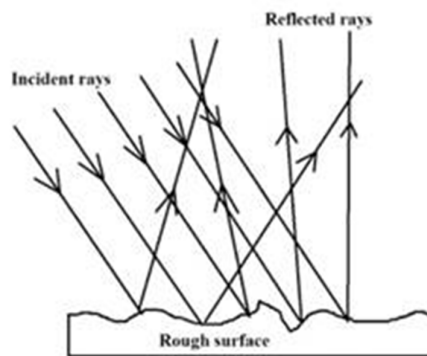
Εικόνα 2-10: Αντικατάσταση πολλαπλών εμποδίων με ένα ισοδύναμο για τον υπολογισμό της απώλειας λόγω περίθλασης. [1]

2.1.5 Οι Μηχανισμοί Διάδοσης - Σκέδαση

Τα μοντέλα ανάκλασης και περίθλασης, τις περισσότερες φορές προβλέπουν ασθενέστερης ισχύος λαμβανόμενο σήμα. Αυτό συμβαίνει λόγω ενός φαινομένου που ονομάζεται Σκέδαση. Κατά την σκέδαση, όταν ένα ηλεκτρομαγνητικό κύμα προσκρούει σε μία τραχιά επιφάνεια, προκαλείται διασπορά (διάχυση) της ενέργειας που υπέστη ανάκλαση προς όλες τις κατευθύνσεις αποδίδοντας

έτσι στον δέκτη πρόσθετη ενέργεια ενισχύοντας την ισχύ του συνολικού λαμβανόμενου σήματος. Στον πραγματικό κόσμο, μερικά παραδείγματα που προκαλούν αυτό το φαινόμενο είναι τα δέντρα και οι στύλοι των φωτιστικών δρόμου. Οι επίπεδες επιφάνειες που είναι μεγαλύτερες από ένα μήκος κύματος μπορούν να μοντελοποιηθούν ως επιφάνειες που επιτρέπουν την ανάκλαση, όμως η τραχύτητά τους μπορεί να προκαλέσει διαφορετικά αποτελέσματα διάδοσης από την κατοπτρική ανάκλαση.

Σε ασύρματα κανάλια, είναι αρκετά χρήσιμο να είναι προσδιορισμένη η θέση μεγάλων και απομακρυσμένων αντικειμένων που επιφέρουν σκέδαση προκειμένου να εκτιμηθεί η ακριβής ισχύς του σκεδαζόμενου σήματος. Η ισχύς αυτή αν διαιρεθεί με την προσπίπτουσα στον στόχο πυκνότητα ισχύος του, ονομάζεται ενεργός διατομή ραντάρ ή επιφάνεια σκέδασης του στόχου (Radar Cross Section - RCS). [1]



Εικόνα 2-11: Αναπαράσταση της σκέδασης σε τραχιά επιφάνεια. [16]

2.1.6 Μοντέλα διάδοσης σε εξωτερικούς χώρους

Στους εξωτερικούς χώρους, το έδαφος και η κατανομή των εμποδίων (σπίτια, δέντρα, βουνά) είναι ακανόνιστη με αποτέλεσμα η διάδοση των ραδιοκυμάτων να υπόκειται σε διάφορες αλλοιώσεις που στον γενικό τους όρο ονομάζονται απώλεια διαδρομής. Γι' αυτό τον λόγο έχουν αναπτυχθεί διάφορα μοντέλα τα οποία προβλέπουν αυτή την κατάσταση ερμηνεύοντας συστηματικά τα λαμβανόμενα δεδομένα μέτρησης. Παρακάτω παρουσιάζονται ορισμένα από αυτά: [1]

Μοντέλο Longley-Rice: Προκειμένου να προβλεφθεί η ισχύς του λαμβανόμενου σήματος μέσα στην περιοχή κάλυψης, γίνεται χρήση κυρίως του μοντέλου ανάκλασης δύο ακτινών στο έδαφος το οποίο ανήκει στην γενικότερη κατηγορία των τεχνικών γεωμετρικής οπτικής. Λειτουργεί για επικοινωνία από σημείο σε σημείο (point-to-point) (διάφορα χαρακτηριστικά της διαδρομής μπορούν εύκολα να εκτιμηθούν) καθώς και για την περίπτωση που οι ιδιότητες της διαδρομής δεν είναι γνωστές (προβλέπονται οι παράμετροι αυτοί). Μοναδικό μειονέκτημα είναι ότι δεν είναι εφικτή η βελτιστοποίηση του μοντέλου σε περίπτωση περιβαλλοντικών εξασθενήσεων (κτίρια, φύλλα δέντρων).

Μοντέλο Durkin (Περίπτωση Χρήσης): Επαναπροσδιορίζει τις ιδιότητες για την διαμόρφωση του εδάφους που παρεμβάλλεται μεταξύ πομπού και δέκτη (LOS διάδοση). Στην συνέχεια εκτιμάται η απώλεια διαδρομής στην ίδια περιοχή. Τέλος, ο δέκτης μετακινείται συνεχώς εντός της

περιοχής κάλυψης προκειμένου να καταγραφεί το περίγραμμα της ισχύος του σήματος. Η ακρίβεια αυτού του μοντέλου είναι πολύ υψηλή, δηλαδή υπάρχει απόκλιση μόνο μερικά dB. Το μειονέκτημα είναι ότι δεν λειτουργεί ακριβώς για διάδοση που οφείλεται σε φύλλα δέντρων, κτίρια κ.α. και δεν υποστηρίζεται η πολυδιαδρομή (multipath) του σήματος εκτός από την ανάκλαση στο έδαφος.

Μοντέλο Okumura: Το μοντέλο που χρησιμοποιείται πιο πολύ. Πρώτα υπολογίζονται οι απώλειες ελεύθερου χώρου (Free Space Path Loss) ενώ στην συνέχεια προστίθεται η μέση απώλεια σε σχέση με τον ελεύθερο χώρο. Στην συνέχεια μειώνονται τα κέρδη ύψους των κεραιών (σταθμού βάσης και κινητής συσκευής) και το κέρδος του τύπου του περιβάλλοντος. Μοναδικό μειονέκτημα είναι ότι σε περίπτωση γρήγορης αλλαγής του εδάφους, το μοντέλο δεν αποδίδει γρήγορα αποτελέσματα.

Μοντέλο Hata: Βασισμένο σε δεδομένα από το μοντέλο Okumura όμως δεν διαθέτει διορθωτικούς συντελεστές για τον τύπο του εδάφους, για την κλίση του και άλλους για βελτιστοποίηση συγκεκριμένης διαδρομής.

Μοντέλο Walfisch και Bertoni: Μέσω της περίθλασης λόγω του ύψους των κτιρίων μπορεί να εκτιμηθεί η μέση ισχύς του σήματος.

2.1.7 Μοντέλα διάδοσης σε εσωτερικούς χώρους

Στο εξωτερικό και στο εσωτερικό περιβάλλον υπάρχουν εμπόδια. Η διαφορά του εσωτερικού από το εξωτερικό είναι ότι στο πρώτο η απόσταση μεταξύ πομπού και δέκτη αλλά και η απόσταση αυτών από τα εμπόδια όπως τοίχοι, πόρτες και άλλα έπιπλα είναι μικρή και κατ' επέκταση μικρότερη σε σχέση με το δεύτερο. Αυτό έχει ως αποτέλεσμα την ταχεία συνεχόμενη αλλαγή του ασύρματου καναλιού ανάλογα με την μορφολογία του εσωτερικού περιβάλλοντος. Οι μηχανισμοί διάδοσης είναι ίδιοι παντού. Γι' αυτόν τον λόγο ήταν επιτακτική η δημιουργία διαφορετικών μοντέλων διάδοσης στους εσωτερικούς χώρους από τους εξωτερικούς. Παρακάτω παρουσιάζονται ορισμένα από αυτά:

Απώλειες λόγω διάταξης του ορόφου (ίδιος όροφος): Κάθε κτίριο έχει διαφορετική διάταξη χώρου στο εσωτερικό του. Χωρίσματα θεωρούνται οι τοίχοι από οποιαδήποτε δομική σύσταση αλλά και κινητές κατασκευές που επιτυγχάνουν διαχωρισμό χώρων. Η χρήση γενικών μοντέλων είναι ανέφικτη λόγω της ποικιλομορφίας των δομικών συστατικών των διάφορων χωρισμάτων. Γι' αυτό τον λόγο έχουν αναπτυχθεί διάφοροι πίνακες που περιέχουν ιδιότητες για κάθε κατασκευή και με τους νόμους της φυσικής προκύπτουν οι μέσες απώλειες σε λαμβανόμενο σήμα στον δέκτη.

Απώλειες λόγω διάταξης μεταξύ πολλών ορόφων: Σημαντικό ρόλο στην εξασθένηση του λαμβανόμενου σήματος παίζει η δομική σύσταση του κτιρίου και κατ' επέκταση των ορόφων, οι εξωτερικές διαστάσεις του καθώς και ο αριθμός και ο τύπος των παραθύρων (φιμέ). Η εξασθένηση στον πρώτο διαχωρισμό με όροφο είναι μεγαλύτερη σε σχέση με κάθε επιπρόσθετο όροφο που υπάρχει στο κτίριο.

Μοντέλο Απώλειας Λογαριθμικής (log-distance) Απόστασης: Αυτό το μοντέλο βασίζεται κυρίως στην απώλεια της ισχύος λόγω της απόστασης λαμβάνοντας υπόψιν τον τύπο και το περιβάλλον του κτιρίου.

Μοντέλο Πολλαπλών Σημείων Διακοπής (Breakpoint) Ericsson: Το μοντέλο αυτό λαμβάνει υπόψιν 4 σημεία διακοπής δηλαδή 4 διαχωρισμούς (όροφοι). Παρέχει ένα μέγιστο και ένα ελάχιστο όριο για την τιμή της απώλειας διαδρομής.

Μοντέλο Συντελεστή Εξασθένησης: Ένα αποδεδειγμένα ευέλικτο, ακριβές και υπολογιστικά αποδοτικό μοντέλο το οποίο λαμβάνει υπόψιν τον τύπο του κτιρίου καθώς και τις απώλειες που προκαλούνται από διάφορα εμπόδια. Αυτό επιτυγχάνεται με την άθροιση των απωλειών λόγω απόστασης συν την κανονικοποίηση της απόστασης μεταξύ πομπού και δέκτη συν την εξασθένηση λόγω διαχωρισμού λαμβάνοντας υπόψιν τις φυσικές ιδιότητες του διαχωριστικού.

Γενικά, ασύρματα συστήματα που υπάρχουν μέσα σε κτίρια σε μία κοντινή περιοχή το ένα από το άλλο και μοιράζονται ίδιες συχνότητες, απαιτούν το λαμβανόμενο σήμα να έχει συγκεκριμένο όριο κατώτατης ισχύς. Σε όσο πιο μεγάλο όροφο βρίσκεται ο δέκτης, τόσο μεγαλύτερη πρέπει να είναι η ισχύς του σήματος προκειμένου να διεισδύσει μέσα από τοίχους και παράθυρα. Έχει παρατηρηθεί ότι ένα κτίριο με περισσότερα παράθυρα, επιτρέπει στον δέκτη εσωτερικά του να λάβει ισχυρότερο σήμα. Με λίγα λόγια, η επιτυχής διείσδυση καθορίζεται από την συχνότητα, από το ύψος του κτιρίου, από το διάγραμμα ανύψωσης της κεραίας αλλά και από την φυσική σύσταση των οικοδομικών υλικών που χρησιμοποιείται σε ένα κτίριο. Η ραγδαία ανάπτυξη της τεχνολογίας οδήγησε στην υλοποίηση λογισμικών για μοντελοποίηση μίας ασύρματης επικοινωνίας (χρήση βάσεων δεδομένων για τα χαρακτηριστικά κτιρίου και εδάφους, χρήση γραφικών απεικονίσεων με τρισδιάστατες δορυφορικές φωτογραφίες για την εκτέλεση μοντέλων ανάκλασης, περίθλασης και σκέδασης). Με αυτό τον τρόπο μπορεί να εκτιμηθεί ακριβώς η ισχύς του λαμβανόμενου σήματος και το επίπεδο των απωλειών είτε σε εσωτερικό είτε στο εξωτερικό περιβάλλον. [1]

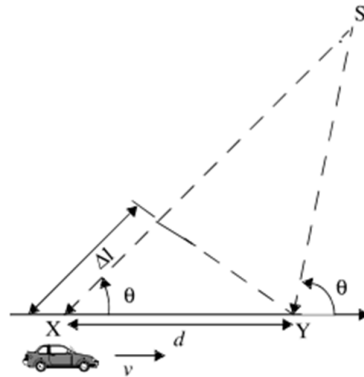
2.2 Διαλείψεις Μικρής Κλίμακας και Πολυδιαδρομές (Multipath)

Οι διαλείψεις μικρής κλίμακας αναφέρονται σε απώλειες λόγω απότομων και γρήγορων (σε μικρό χρονικό διάστημα τάξεως μικρότερης των δευτερολέπτων ή σε μικρή απόσταση) μεταβολών του πλάτους, της φάσης και των καθυστερήσεων που προκαλούνται από τις πολλαπλές διαδρομές που μπορεί να έχει ακολουθήσει ένα ραδιοσήμα. Πολλαπλές διαδρομές ή πολυδιαδρομές ενός σήματος αποτελούν σύνηθες φαινόμενο στις ασύρματες επικοινωνίες και αποτελούν συνιστώσες του αρχικού εκπεμπόμενου το οποίο υπόκειται σε παρεμβολές από τα «είδωλα» του. Στον δέκτη φτάνουν πλήθος συνιστωσών αυτού σε διαφορετικούς χρόνους που ο συνδυασμός τους δίνει ένα λαμβανόμενο σήμα με παραμορφωμένο πλάτος και φάση. Υπάρχουν πολλοί φυσικοί παράγοντες που επηρεάζουν αυτές τις διαλείψεις όπως η διάδοση πολυδιαδρομών που αναφέρθηκε παραπάνω, η ταχύτητα που κινείται ο δέκτης σε σχέση με τον σταθμό βάσης (άμεση επίδραση λόγω ολίσθησης Doppler), η ταχύτητα των αντικειμένων εντός του ασύρματου καναλιού και το εύρος ζώνης του μεταδιδόμενου σήματος. Αυτό το κεφάλαιο θα ασχοληθεί με την αποσαφήνιση των διαλείψεων καθώς και την παρουσίαση μοντέλων μικρής κλίμακας.

2.2.1 Ολίσθηση Doppler

Η Ολίσθηση Doppler είναι ένα φαινόμενο κατά το οποίο επηρεάζει την συχνότητα του εκπεμπόμενου σήματος όπως αυτό φτάνει στο δέκτη. Συνδέει την γωνία μεταξύ του πομπού και του

δέκτη καθώς και την ταχύτητα του δέκτη σε σχέση με τον πομπό. Στο παρακάτω σχήμα (Εικόνα 2-12), απεικονίζεται αυτό το φαινόμενο.



Εικόνα 2-12: Απεικόνιση της Ολίσθησης Doppler. [1]

Από το παραπάνω σχήμα (Εικόνα 2-12), παρατηρείται ότι η πηγή S εκπέμπει ένα σήμα προς τον δέκτη (αυτοκίνητο) το οποίο κινείται κατά μήκος της γραμμής X-Y με συνολικό χρόνο Δt που έχει μία απόσταση d . Λόγω της γωνίας που εμφανίζει ο δέκτης σε σχέση με την πηγή, η διαφορά στα μήκη διαδρομής του κύματος μεταξύ της πηγής και αυτού στις θέσεις X και Y είναι Δl και η διαφορά φάσης σε αυτά είναι $\Delta \phi$. Βλέποντας το σχήμα, με τριγωνομετρία προκύπτουν οι ακόλουθες εξισώσεις:

$$\Delta \phi = \frac{2\pi \Delta l}{\lambda} = \frac{2\pi v \Delta t}{\lambda} \cos \theta \quad (2.2.1.1)$$

$$f_d = \frac{1}{2\pi} \frac{\Delta \phi}{\Delta t} = \frac{v}{\lambda} \cos \theta \quad (2.2.1.2)$$

όπου f_d είναι η συχνότητα Doppler, v είναι η ταχύτητα του δέκτη και λ είναι το μήκος κύματος.

2.2.2 Μοντελοποίηση καναλιού ως φίλτρο και σχέση εύρους ζώνης και λαμβανόμενης ισχύος

Ως κρουστική απόκριση ορίζεται κάθε αντίδραση ενός δυναμικού συστήματος σε εξωτερικές διεγέρσεις. Οι διαλείψεις μικρής κλίμακας μπορούν να συνδεθούν με την κρουστική απόκριση η οποία περιλαμβάνει όλα τα δεδομένα που απαιτούνται για τη μοντελοποίηση ή την εξέταση οποιουδήποτε είδους ασύρματης επικοινωνίας μέσω του καναλιού. Αυτό οφείλεται στη δυνατότητα μοντελοποίησης ενός κινητού ραδιοδιαύλου ως γραμμικού φίλτρου με κρουστική απόκριση που μεταβάλλεται κάθε χρονική στιγμή, όπου η χρονική μεταβολή προκαλείται από την κινητικότητα του δέκτη στο χώρο. Το κανάλι μπορεί να μοντελοποιηθεί ως φίλτρο καθώς αυτή η ιδιότητά του προκύπτει από το άθροισμα των πλατών και των καθυστερήσεων των πολλαπλών κυμάτων που φτάνουν στον δέκτη σε κάθε χρονική στιγμή. Με την βοήθεια της κρουστικής απόκρισης, είναι εφικτή η εκτίμηση και η σύγκριση της αποδοτικότητας διαφορετικών συστημάτων κινητής επικοινωνίας και των μεταδιδόμενων ευρών ζώνης για μία δεδομένη κατάσταση κινητού καναλιού.

Στην πραγματικότητα, η κρουστική απόκριση ενός καναλιού υπολογίζεται με την βοήθεια τεχνικών εκτίμησης καναλιού. Στην περίπτωση που θεωρηθεί η εφαρμογή ενός σήματος συνεχούς

κύματος (CW) τότε στην έξοδο του καναλιού αθροίζονται όλες οι πολυδιαδρομικές συνιστώσες. Στην περίπτωση που οι φάσεις πολυδιαδρομών είναι ομοιόμορφα κατανεμημένες ή όταν τα πλάτη των διαδρομών δεν σχετίζονται, η έξοδος μέσης ισχύος με διέγερση CW για μια περιοχή (μικρής έκτασης) είναι σχετικά όμοια με την μέση ισχύ ενός ευρυζωνικού σήματος. Εάν οι φάσεις των διαδρομών δεν είναι ομοιόμορφα κατανεμημένες, η μέση ισχύς ευρείας ζώνης και η μέση ισχύς του CW συνεχίζουν να είναι ίσες όταν οι διαδρομές έχουν ασύμμετρα πλάτη. Αντιθέτως, αφού ο ίδιος παράγοντας που επηρεάζει τις φάσεις των διαδρομών είναι πιθανό να έχει επίδραση και στα πλάτη, τότε τα πλάτη είναι πιθανό να είναι αλληλεξαρτώμενα. Στις συχνότητες μετάδοσης που χρησιμοποιούνται στα ασύρματα κινητά συστήματα, αυτό το σενάριο είναι εξαιρετικά σπάνιο. Έτσι, μπορεί να παρατηρηθεί ότι τα σήματα ευρείας ζώνης και τα σήματα στενής ζώνης έχουν κατά βάση την ίδια λαμβανόμενη μέση ισχύ.

Η δομή των πολυδιαδρομών μπορεί να αναλυθεί εξολοκλήρου από τον δέκτη από το λαμβανόμενο σήμα όταν το εύρος ζώνης του μεταδιδόμενου σήματος είναι σημαντικά μεγαλύτερο από το εύρος ζώνης συνοχής του καναλιού. Σε αυτή την περίπτωση, οι πολυδιαδρομές απλώνονται σε διαφορετικές καθυστερήσεις και η λαμβανόμενη ισχύς τους μεταβάλλεται λίγο επειδή τα επιμέρους πλάτη πολλαπλών διαδρομών δεν αλλάζουν γρήγορα σε μια τοπική περιοχή. Πολυδιαδρομές που φτάνουν κατά τη διάρκεια μιας περιόδου δειγματοληψίας δεν μπορούν να ξεχωριστούν από τον δέκτη. Οι μετατοπίσεις φάσης των πολυάριθμων μη επιλυμένων (που δεν μπορούν να ξεχωριστούν) συνιστωσών πολυδιαδρομών προκαλούν σημαντικές μεταβολές στην ισχύ του σήματος (διαλείψεις) στο δέκτη, πράγμα που είναι πιο έντονο όταν το εκπεμπόμενο σήμα έχει σχετικά στενό εύρος ζώνης (μεγάλη περίοδος), εμποδίζοντας την ανάλυση των πολυδιαδρομικών συνιστωσών από τον δέκτη. [1]

2.2.3 Μέτρηση της πολυδιαδρομής μικρής κλίμακας

Εξαιτίας της διάρθρωσης της πολυδιαδρομής προκειμένου να προβλεφθούν οι επιδράσεις των διαλείψεων μικρής κλίμακας, έχουν δημιουργηθεί αρκετές τεχνικές σάρωσης ενός καναλιού ευρείας ζώνης. Υπάρχουν τρία διαφορετικά είδη συστημάτων που υλοποιούν αυτές τις τεχνικές. Αυτά είναι τα συστήματα άμεσων παλμών, τα συστήματα εκτίμησης καναλιού διεσπαρμένου φάσματος με χρήση ολισθαίνοντος συσχετιστή (πρακτικά αποτελεί ένα φίλτρο που εφαρμόζει την συνάρτηση συσχέτισης σε κάθε θέση καθώς μετακινείται κατά μήκος του λαμβανόμενου σήματος) και τα συστήματα εκτίμησης καναλιού στο πεδίο της συχνότητας.

Το σύστημα άμεσων παλμών είναι μία τεχνική πρόβλεψης διαλείψεων μικρής κλίμακας το οποίο επιτρέπει στους μηχανικούς να διαπιστώνουν γρήγορα την ένταση του σήματος που λαμβάνεται μέσω ενός καναλιού πολυδιαδρομών σε σχέση με την καθυστέρηση. Πρακτικά, χρησιμοποιείται ένα bi-static (όταν ο πομπός και ο δέκτης βρίσκονται σε διαφορετική τοποθεσία) ραντάρ ευρείας ζώνης το οποίο εκπέμπει έναν συνεχόμενο παλμό. Ένας παλμογράφος υψηλής ταχύτητας χρησιμοποιείται για την αποθήκευση του σήματος αφού ενισχυθεί και αναγνωριστεί η περιβάλλουσά του. Με αυτό τον τρόπο επιτυγχάνεται μία γρήγορη εκτίμηση της κρουστικής απόκρισης του καναλιού που έχει συνδυαστεί με τον παλμό ανίχνευσης. Αυτό το σύστημα παρέχει την ένταση του σήματος που λαμβάνεται μέσω ενός καναλιού πολυδιαδρομών σε σχέση με την καθυστέρηση εφόσον ο παλμογράφος βρίσκεται σε λειτουργία μέσου όρου. Το σύστημα αυτό χαρακτηρίζεται από απλότητα καθώς επιτρέπει την χρήση έτοιμου και ευρείας χρήσης εξοπλισμού. Το πλάτος του παλμού ανίχνευσης είναι ίδιο με την μικρότερη δυνατή καθυστέρηση μεταξύ των

συνιστωσών πολλαπλών διαδρομών που μπορεί να αναλυθεί στο εύρος ζώνης μέτρησης. Το θεμελιώδες ζήτημα με αυτό το σύστημα είναι ότι, επειδή απαιτείται ένα ζωνοπερατό φίλτρο για τη ανάλυση πολλαπλών διαδρομών στον χρόνο, είναι ευάλωτο σε παρεμβολές και θόρυβο. Επιπλέον, η μέθοδος των παλμών εξαρτάται από τη δυνατότητα εκκίνησης του παλμογράφου με το πρώτο σήμα που φτάνει. Εάν το αρχικό σήμα που φθάνει μπλοκαριστεί ή εξασθενεί σοβαρά, το σύστημα δεν μπορεί να ενεργοποιηθεί όπως προβλέπεται. Λόγω της χρήσης ενός ανιχνευτή περιβάλλοντος, δεν είναι δυνατόν να ληφθούν οι φάσεις των επιμέρους συνιστωσών πολλαπλών διαδρομών. Ωστόσο, η μέθοδος αυτή επιτρέπει τον προσδιορισμό της φάσης πολλαπλών διαδρομών όταν χρησιμοποιείται συνεκτικός ανιχνευτής.

Τα συστήματα ευρέως φάσματος έχουν το πλεονέκτημα ότι, ακόμη και αν το σήμα ανίχνευσης είναι ευρείας ζώνης, εξακολουθεί να είναι εφικτή η ανίχνευση του εκπεμπόμενου σήματος με τη χρήση ενός δέκτη στενής ζώνης ακολουθούμενου από έναν μίκτη ευρείας ζώνης, αυξάνοντας το δυναμικό εύρος του συστήματος σε σχέση με τα συστήματα άμεσων παλμών. Ένα φέρον σήμα "εξαπλώνεται" σε ένα μεγάλο εύρος ζώνης από έναν εκτιμητή καναλιού (channel sounder) ευρέως φάσματος συνδυαζόμενο με μια δυαδική ακολουθία ψευδο-θορύβου. Ακολουθεί, η λήψη, το φιλτράρισμα και η από-διασπορά του σήματος με ευρύ φάσμα, με την χρήση μίας πηγής ψευδο-θορύβου η οποία είναι παρόμοια ευθυγραμμισμένη με αυτή που χρησιμοποιείται στον πομπό. Συνδυάζοντας τις ακολουθίες των τσιπ με αυτό τον τρόπο, κατασκευάζεται ένας ολισθαίνων συσχετιστής. Η μέγιστη συσχέτιση επιτυγχάνεται όταν ο κώδικας ψευδο-θορύβου του πιο γρήγορου ρολογιού του τσιπ προλάβει εκείνο του πιο αργού. Όταν δεν υπάρχει μέγιστη συσχέτιση μεταξύ δύο ακολουθιών, προκύπτει ανάμειξη του εισερχόμενου σήματος με ευρύ φάσμα με την ακολουθία του παλμού ενός κώδικα διασποράς άμεσης ακολουθίας (DSSS – Direct-Sequence Spread Spectrum) που δεν είναι συγχρονισμένη. Από αυτό, στην συνέχεια προκύπτει διασπορά σε εύρος ζώνης τουλάχιστον ίσο με την ακολουθία ψευδο-θορύβου. Έτσι, η περισσότερη ισχύς του λαμβανόμενου σήματος μπορεί να απορριφθεί από το φίλτρο στενής ζώνης που ακολουθεί τον συσχετιστή. Με αυτόν τον τρόπο ένας δέκτης ευρέως φάσματος, σε αντίθεση με τον εκτιμητή άμεσων παλμών, επιτυγχάνει κέρδος επεξεργασίας και είναι σε θέση να απορρίπτει παρεμβολές στη ζώνη διέλευσης. Μερικά από τα πλεονεκτήματα αυτού του συστήματος είναι η ικανότητα να απορρίπτει τον θόρυβο της ζώνης διέλευσης, η εξάλειψη της ανάγκης του συγχρονισμού της ακολουθίας ψευδο-θορύβου του πομπού και του δέκτη από τον ολισθαίνοντα συσχετιστή και οι μικρότερες ισχύεις πομπού σε σχέση με τα συστήματα άμεσων παλμών. Τα μοναδικά μειονεκτήματα είναι ότι οι μετρήσεις δεν λαμβάνονται σε πραγματικό χρόνο αλλά συντάσσονται καθώς οι κώδικες ψευδο-θορύβου ευθυγραμμίζονται ο ένας από τον άλλο με χρήση μη συνεκτικού ανιχνευτή, που έχει ως αποτέλεσμα να μην είναι εφικτή η μέτρηση των φάσεων των διάφορων συνιστωσών πολλαπλών διαδρομών.

Ο λόγος για τον οποίο συνδέονται οι τεχνικές του πεδίου του χρόνου και της συχνότητας είναι ότι η κρουστική απόκριση μπορεί να εκτιμηθεί και στο πεδίο της συχνότητας. Η παρακολούθηση της απόκρισης συχνότητας του καναλιού επιτυγχάνεται με έναν «σαρωτή» ο οποίος βρίσκεται υπό τον έλεγχο ενός διανυσματικού αναλυτή δικτύου (vector network analyser) και ένα σύνολο συγκεκριμένων παραμέτρων. Μετακινούμενος σε διακριτές συχνότητες, ο «σαρωτής» σαρώνει ένα συγκεκριμένο εύρος συχνοτήτων (εστιασμένος στο φέρον). Η ποσότητα και τα διαστήματα αυτών των διαδοχικών τιμών συχνότητας επηρεάζουν την χρονική ανάλυση της κρουστικής απόκρισης. Το σύνολο δοκιμαστικών παραμέτρων εκπέμπει μία γνωστή στάθμη σήματος και παρακολουθεί την στάθμη του λαμβανόμενου για κάθε βήμα συχνότητας. Με την βοήθεια αυτών των σταθμών ο

αναλυτής μπορεί να εκτιμήσει την απόκριση διαπερατότητας (transmissivity response) ή αλλιώς τη συνάρτηση μεταφοράς του καναλιού (αναπαράσταση της κρουστικής απόκρισης στο πεδίο της συχνότητας) στο υπό μέτρηση εύρος συχνοτήτων. Στην συνέχεια, παράγεται μία έκδοση κρουστικής απόκρισης με την βοήθεια του αντίστροφου διακριτού μετασχηματισμού Fourier (IDFT – Inverse Discrete Fourier Transform). Μερικά από τα μειονεκτήματα αυτού του συστήματος είναι η προϋπόθεση για ακριβή βαθμονόμηση και συγχρονισμό με χρήση καλωδίων μεταξύ πομπού και δέκτη και η αδυναμία εκτιμήσεων σε πραγματικό χρόνο. [1]

2.2.4 Παράμετροι καναλιών πολυδιαδρομών

Υπάρχουν αρκετές παράμετροι ενός καναλιού πολυδιαδρομών. Πολλές από αυτές προέρχονται από το προφίλ καθυστέρησης ισχύος. Αυτά εκτιμώνται με τις μεθόδους που αναφέρθηκαν παραπάνω και συχνά παρουσιάζονται ως διαγράμματα λαμβανόμενης ισχύος σε συνάρτηση με την μέση καθυστέρηση όλων των διαδρομών σε σχέση με μια σταθερή χρονική καθυστέρηση αναφοράς. Προκειμένου να βρεθεί ένα μέσο προφίλ καθυστέρησης ισχύος μικρής κλίμακας, γίνεται προσδιορισμός των προφίλ καθυστέρησης ισχύος τα οποία υπολογίζονται από τον μέσο όρο των στιγμιαίων εκτιμήσεων καθυστέρησης ισχύος σε μία τοπική περιοχή. Μερικές από αυτές τις παραμέτρους είναι:

Παράμετροι διασποράς στον χρόνο: (α) η μέση πλεονάζουσα καθυστέρηση (η μέση καθυστέρηση όλων των διαδρομών), (β) η τυπική απόκλιση της καθυστέρησης λόγω διασποράς (αθροίζονται οι ισχυρότερες πολυδιαδρομές και στην συνέχεια, το αποτέλεσμα διαιρείται με τα συνολικά βάρη) και (γ) η πλεονάζουσα καθυστέρηση λόγω διασποράς (η διαφορά χρόνου λήψης μεταξύ της αρχικής και της τελικής συνιστώσας πολυδιαδρομής στον δέκτη).

Εύρος ζώνης συνοχής: Είναι μία προσδιορισμένη σχέση που προκύπτει από την τυπική απόκλιση της καθυστέρησης λόγω διασποράς (delay spread). Είναι, ουσιαστικά, ένα εύρος συχνοτήτων όπου υπάρχει σημαντική πιθανή συσχέτιση μεταξύ δύο συνιστωσών συχνότητας και αποτελεί ένα στατιστικό μέτρο του εύρους συχνοτήτων στο οποίο το κανάλι.

Διασπορά Doppler και χρόνος συνοχής: Παράμετροι οι οποίοι περιγράφουν το πόσο το κανάλι μεταβάλλεται με τον χρόνο σε μία περιοχή μικρής κλίμακας. Η διασπορά Doppler είναι η επέκταση/αύξηση του φάσματος ενός σήματος στενής ζώνης που εκπέμπεται μέσω ενός καναλιού διάδοσης πολυδιαδρομών. Προκαλείται με την μεταβολή του ασύρματου καναλιού στον χρόνο και μπορεί να οριστεί ως το εύρος των συχνοτήτων όπου το λαμβανόμενο φάσμα Doppler είναι κατά βάση μη μηδενικό. Το αντιστρόφως ανάλογο μέτρο της διασποράς Doppler είναι ο χρόνος συνοχής ο οποίος αποτελεί το δυικό του Doppler στο πεδίο του χρόνου και προσδιορίζει την χρονική μεταβολή του καναλιού. Με άλλα λόγια, ορίζει ένα χρονικό διάστημα όπου η κρουστική απόκριση του καναλιού είναι ουσιαστικά αμετάβλητη. [1]

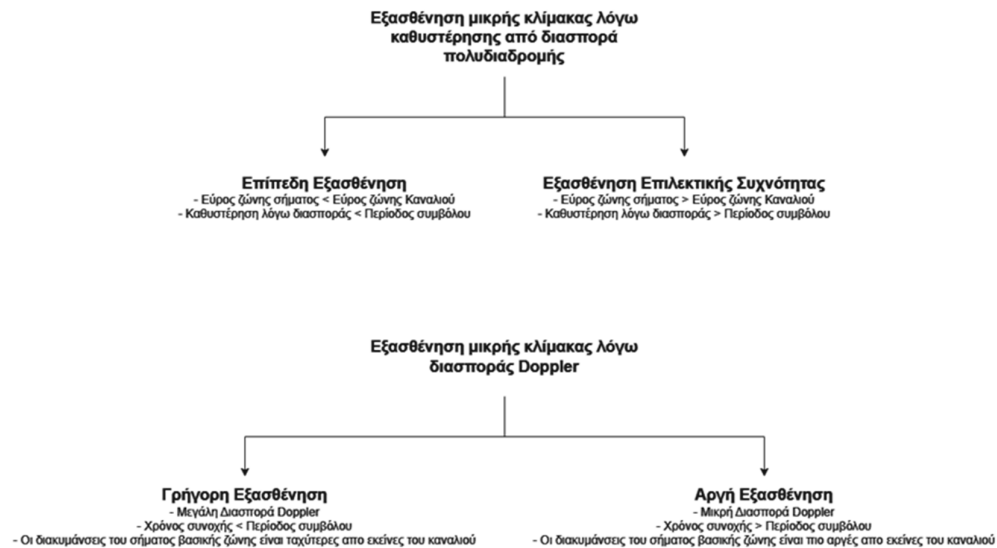
2.2.5 Τύποι διαλείψεων μικρής κλίμακας

Όπως αποδείχθηκε σε παραπάνω κεφάλαιο, το είδος εξασθένησης που υφίσταται ένα σήμα εξαρτάται από την φύση του σε συνάρτηση με τις ιδιότητες του καναλιού στο οποίο διαδίδεται. Διαφορετικά μεταδιδόμενα σήματα θα παρουσιάσουν διάφορες μορφές εξασθένησης ανάλογα με την σχέση μεταξύ των παραμέτρων του σήματος όπως το εύρος ζώνης και των παραμέτρων του

ασύρματου καναλιού όπως η διασπορά Doppler. Υπάρχουν δύο τύποι διαλείψεων μικρής κλίμακας και είναι οι εξής:

Διαλείψεις λόγω καθυστέρησης από διασπορά πολυδιαδρομής: (α) επίπεδες διαλείψεις (υφίστανται όταν το ασύρματο κανάλι έχει σταθερό κέρδος και γραμμική απόκριση φάσης σε εύρος ζώνης μεγαλύτερο από αυτό του εκπεμπόμενου σήματος και η καθυστέρηση λόγω διασποράς είναι μικρότερη από την περίοδο συμβόλου) και (β) εξασθένηση επιλεκτικής συχνότητας (υφίσταται όταν το ασύρματο κανάλι παρουσιάζει σταθερού κέρδους και γραμμική απόκριση φάσης σε εύρος ζώνης που είναι μικρότερο από εκείνο του εκπεμπόμενου σήματος και η καθυστέρηση λόγω διασποράς είναι μεγαλύτερη από την περίοδο του συμβόλου).

Διαλείψεις λόγω διασποράς Doppler: (α) γρήγορες διαλείψεις (υφίσταται όταν υπάρχει μεγάλη διασπορά Doppler, ο χρόνος συνοχής είναι μικρότερος από την περίοδο του συμβόλου και οι διακυμάνσεις του σήματος βασικής ζώνης είναι ταχύτερες από εκείνες του καναλιού) και (β) αργή διάλειψη (υφίσταται όταν υπάρχει μικρή διασπορά Doppler, ο χρόνος συνοχής είναι μεγαλύτερος από την περίοδο του συμβόλου και οι διακυμάνσεις του σήματος βασικής ζώνης είναι πιο αργές από εκείνες του καναλιού). [1]



Εικόνα 2-13: Συγκεντρωμένοι όλοι οι τύποι διαλείψεων μικρής κλίμακας. [1]

2.2.6 Κατανομές διαλείψεων

Υπάρχουν δύο βασικές ευρέως χρησιμοποιούμενες κατανομές διαλείψεων. Αυτές είναι οι εξής:

Κατανομή Διαλείψεων Rayleigh: Η κατανομή Rayleigh εφαρμόζεται κυρίως στα ασύρματα κανάλια για να προσδιορίσει την στατιστικά χρονικά μεταβαλλόμενη φύση της περιβάλλουσας ενός σήματος επίπεδων διαλείψεων ή της περιβάλλουσας μιας επιμέρους συνιστώσας πολυδιαδρομών.

Κατανομή διαλείψεων Rice: Η μικρής κλίμακας κατανομή διαλείψεων της περιβάλλουσας είναι Rice όταν υφίσταται μία κυρίαρχη σταθερή (που δεν έχει υποστεί διάλειψη) συνιστώσα σήματος όπως μία LOS διαδρομή. Σε αυτή την περίπτωση, σε ένα κυρίαρχο σήμα προστίθενται τυχαίες συνιστώσες πολυδιαδρομών που καταφθάνουν σε διάφορες γωνίες. Αυτό έχει ως αποτέλεσμα την εισαγωγή μίας συνιστώσας DC (μέσο πλάτος κατά την διάρκεια της χρονικής

περιόδου ολοκλήρωσης ενός κύκλου του σήματος) στην έξοδο ενός ανιχνευτή περιβάλλουσας. Αυτή η κατανομή προκαλείται από την επίδραση ενός κυρίαρχου σήματος που φθάνει ταυτόχρονα με πολλά ασθενέστερα σήματα πολυδιαδρομών όπως συμβαίνει με τον εντοπισμό ενός ημιτονοειδούς κύματος που υπόκειται σε θερμικό θόρυβο. Το συνδυασμένο σήμα πολυδιαδρομών είναι παρόμοιο με σήμα θορύβου με περιβάλλουσα Rayleigh καθώς το. Κατά συνέπεια, όταν η κύρια συνιστώσα εξασθενεί, η κατανομή Rice μετατρέπεται σε Rayleigh. [1]

2.2.7 Στατιστικά μοντέλα για κανάλια εξασθένησης πολυδιαδρομών

Υπάρχουν διάφορα μοντέλα πολυδιαδρομών για τον προσδιορισμό της στατιστικής φύσης ενός ασύρματου καναλιού.

Μοντέλο Clarke για επίπεδες διαλείψεις: Σε αυτό το μοντέλο τα στατιστικά χαρακτηριστικά των ηλεκτρομαγνητικών πεδίων του λαμβανόμενου σήματος στη τερματική συσκευή (κινητό), προκύπτουν από την επίδραση της σκέδασης. Χρησιμοποιείται ένας σταθερός πομπός με μία κάθετα πολωμένη κεραία. Θεωρείται ότι N κύματα στο αζιμουθιακό επίπεδο με τυχαίες φάσεις φέροντος, τυχαίες αζιμουθιακές γωνίες άφιξης και ίσο μέσο πλάτος κάθε κύματος συνθέτουν το πεδίο το οποίο προσπίπτει στην κεραία του τερματικού. Η λαμβανόμενη κυματομορφή στο πεδίο του χρόνου, η χρονική συσχέτιση μεταξύ των δειγμάτων και η συμπεριφορά της κλίσης των διαλείψεων (πόσο απότομες είναι) εξαρτώνται από την φασματική μορφή της διασποράς Doppler. Προκειμένου να δημιουργηθούν ρεαλιστικές κυματομορφές με διαλείψεις με ορθή χρονική συσχέτιση, οι προσομοιωτές διαλείψεων Rayleigh πρέπει να χρησιμοποιούν ένα φάσμα διασποράς.

Προσομοίωση του Μοντέλου Εξασθένησης Clarke και Gans: Είναι μία διαδεδομένη μέθοδος προσομοίωσης η οποία δημιουργεί ένα προσομοιωμένο σήμα με φασματικές και χρονικές ιδιότητες που είναι αρκετά παρόμοιες με τα εκτιμώμενα δεδομένα χρησιμοποιώντας την διάσπαση του σήματος σε συμφασική και ορθογώνια συνιστώσα κατά τη διαμόρφωση και τη χρήση μιγαδικής ανάλυσης.

Στατιστικά Level Crossing και διαλείψεις: Ο Rice δημιούργησε απλές διατυπώσεις για την εκτίμηση του μέσου αριθμού από Level Crossing και της διάρκειας των διαλείψεων εκτιμώντας τις από κοινού στατιστικές για ένα μαθηματικό πρόβλημα που σχετίζεται με το μοντέλο διαλείψεων Clarke. Προκειμένου να δημιουργηθούν κώδικες ελέγχου σφαλμάτων και διαφορικές λήψεις σε συστήματα κινητών επικοινωνιών απαιτούνται ο ρυθμός Level Crossing και η μέση διάρκεια διάλειψης ενός σήματος με διαλείψεις Rayleigh που είναι κρίσιμα στατιστικά αφού επιτυγχάνεται συσχέτιση του ρυθμού χρονικής μεταβολής του λαμβανόμενου σήματος με την στάθμη του σήματος και την ταχύτητα του κινητού τερματικού. Ο προβλεπόμενος ρυθμός με τον οποίο η περιβάλλουσα Rayleigh διέρχεται από ένα προκαθορισμένο επίπεδο προς την θετική κατεύθυνση, κανονικοποιημένος ως προς την τοπική ενεργό στάθμη του σήματος, είναι γνωστός ως Level Crossing Rate (LCR). Ο πιο πιθανός αριθμός bit σηματοδότησης που είναι πιθανόν να χαθεί κατά τη διάλειψη καθορίζεται από την μέση διάρκεια της εξασθένησης ενός σήματος η οποία επηρεάζεται κυρίως από την ταχύτητα της τερματικής συσκευής (κινητό) και μειώνεται με την αύξηση της μέγιστης συχνότητας Doppler. Σε περίπτωση που το σύστημα κινητής επικοινωνίας διαθέτει ορισμένο περιθώριο διαλείψεων είναι σημαντικό να προσδιοριστεί ο ρυθμός πτώσης του σήματος εισόδου κάτω από ένα προκαθορισμένο επίπεδο και η μέση διάρκεια που παραμένει κάτω από αυτό το επίπεδο (outage). Αυτό είναι απαραίτητο για την συσχέτιση του ρυθμού σφάλματος

ενός Bit (BER – Bit Error Rate) με την αναλογία σήματος προς θόρυβο (SNR – Signal-to-Noise Ratio) κατά την διάρκεια μιας εξασθένησης.

Μοντέλο διαλείψεων Rayleigh δύο ακτινών: Τα στατιστικά δεδομένα για τις διαλείψεις Rayleigh και το μοντέλο του Clarke ισχύουν για καταστάσεις επίπεδων διαλείψεων και αγνοούν την καθυστέρηση πολυδιαδρομών. Η μοντελοποίηση των επιδράσεων της καθυστέρησης λόγω διασποράς πολυδιαδρομών και των διαλείψεων, είναι απαραίτητη στα συστήματα κινητών επικοινωνιών υψηλών ρυθμών δεδομένων. Το μοντέλο διάλειψης Rayleigh δύο ακτινών αποτελεί ένα διαδεδομένο μοντέλο πολυδιαδρομών.

Στατιστικό μοντέλο εσωτερικού χώρου των Saleh και Valenzuela: Οι Saleh και Valenzuela ανέπτυξαν ένα μοντέλο πολυδιαδρομών για ασύρματα κανάλια εσωτερικού χώρου λαμβάνοντας υπόψιν ότι το κανάλι αυτό είναι εξαιρετικά αργά χρονικά μεταβαλλόμενο ή είναι quasistatic (δηλαδή το κέρδος του παραμένει σταθερό κατά την διάρκεια μιας περιόδου χρόνου και στην συνέχεια μεταβάλλεται περίοδο ανά περίοδο χρόνου με ανεξάρτητο τρόπο) και (β) στην περίπτωση έλλειψης LOS διαδρομής, τα στατιστικά δεδομένα της κρουστικής απόκρισης του καναλιού δεν επηρεάζονται από την πόλωση. Οι συνιστώσες πολυδιαδρομών θεωρείται ότι φθάνουν σε ομάδες σύμφωνα με το μοντέλο. Τα πλάτη των λαμβανόμενων συνιστωσών είναι ανεξάρτητες τυχαίες μεταβλητές Rayleigh και τόσο η καθυστέρηση της ομάδας όσο και η πλεονάζουσα καθυστέρηση εντός μίας ομάδας μειώνονται εκθετικά όσον αφορά τη διακύμανσή τους. Οι αντίστοιχες γωνίες φάσης είναι ανεξάρτητες ομοιόμορφες τυχαίες μεταβλητές και κυμαίνονται από 0 έως 2π . Μέσα σε μία ομάδα, οι συνιστώσες πολυδιαδρομών και οι ομάδες δημιουργούν διαδικασίες άφιξης Poisson με διαφορετικούς ρυθμούς. Οι χρόνοι μεταξύ των αφίξεων για τις ομάδες και τις συνιστώσες πολυδιαδρομών εντός μίας ομάδας είναι εκθετικά διανεμημένοι. Ενώ οι συνιστώσες μέσα στην ομάδα δημιουργούνται από πολλαπλές ανακλάσεις από αντικείμενα σε μικρή απόσταση από τον πομπό και τον δέκτη, οι ίδιες ομάδες συνδέονται με την δομή του κτιρίου.

Στατιστικά μοντέλα εσωτερικών και εξωτερικών χώρων SIRCIM και SMRCIM: Αναπτύχθηκε προσομοιωτής μοντέλων κρουστικής απόκρισης του ασύρματου καναλιού εσωτερικού χώρου (SIRCIM – Simulation of Indoor Radio Channel Impulse-response Models) ο οποίος είναι ένα λογισμικό και ένα σύνθετο και πειραματικά παραγόμενο στατιστικό μοντέλο για την παραγωγή μετρήσιμων καναλιών μέσω της διακριτής κρουστικής απόκρισης του καναλιού. Οι προσομοιώσεις κρουστικής απόκρισης εσωτερικών καναλιών μικρής κλίμακας που παράγονται από αυτό το λογισμικό είναι ρεαλιστικές σε σύγκριση με πραγματικές μετρήσεις. Στην συνέχεια υλοποιήθηκε ένα παρόμοιο λογισμικό που αφορά την προσομοίωση μοντέλων κρουστικής απόκρισης του ασύρματου κινητού καναλιού (SMRCIM – Simulation of Mobile Radio Channel Impulse-response Models). Αυτό το λογισμικό προσομοιώνει τις κρουστικές αποκρίσεις των κυψελωτών και μικρο-κυψελωτών καναλιών μικρής κλίμακας εντός πόλεως και αποτελεί αποτέλεσμα μεταγενέστερης εργασίας. [1]

2.2.8 Θεωρία των συντελεστών σχήματος πολυδιαδρομών για ασύρματα κανάλια διαλείψεων μικρής κλίμακας

Δημιουργήθηκε μία νέα τεχνική ανάλυσης για την περιγραφή των επίπεδων μικρής κλίμακας διαλείψεων που συναντά ένας δέκτης σε κάθε τυχαίο κανάλι όσον αφορά τον χρόνο και την θέση (χώρο-χρόνου). Με την χρήση αυτής της μεθόδου, ένα κανάλι πολυδιαδρομών με οποιονδήποτε

βαθμό χωρικής πολυπλοκότητας μπορεί να περιγραφεί με βάση τρεις συντελεστές σχήματος, καθένας από τους οποίους έχουν εύκολα κατανοητή γεωμετρική ερμηνεία. Αυτοί οι συντελεστές χαρακτηρίζουν τα στατιστικά στοιχεία των μεταβολών του λαμβανόμενου σήματος σε ένα κανάλι πολυδιαδρομών.

Όπως αναφέρθηκε και στην αρχή αυτού του κεφαλαίου, με την έννοια της εξασθένησης/διάλειψης μικρής κλίμακας εννοούνται οι απότομες μεταβολές της λαμβανόμενης ισχύος ενός σήματος που προκαλούνται από μικρότερων του μήκους κύματος αλλαγές στον δέκτη. Το αποτέλεσμα αυτού του φαινομένου είναι είτε θετική είτε αρνητική συμβολή διάφορων κυμάτων πολυδιαδρομών που εισέρχονται σε έναν ασύρματο δέκτη. Οι μεταβολές στην ισχύ του λαμβανόμενου σήματος που προκύπτουν από αυτό το φαινόμενο, έχουν επίδραση σε κάθε πλευρά του σχεδιασμού του δέκτη συμπεριλαμβανομένου του δυναμικού εύρους, της ισοστάθμισης, της διαφορικής λήψης, του σχήματος διαμόρφωσης και της κωδικοποίησης καναλιού και διόρθωσης σφαλμάτων. Αυτές οι μεταβολές εξαρτώνται από την γωνία άφιξης (AoA – Angle of Arrival) των καθυστερημένων πολυδιαδρομών σε σχέση με την κατεύθυνση κίνησης. Η φασματική πυκνότητα ισχύος (PSD – Power Spectral Density), ο ρυθμός level-crossing και η μέση διάρκεια της διάλειψης είναι παραδείγματα μετρήσεων μίας διαδικασίας που περιλαμβάνονται στα στατιστικά στοιχεία αυτοσυσχέτισης των διαδικασιών διαλείψεων (ή στατιστικά στοιχεία δεύτερης τάξης/ροής). Παρόλο που τα στατιστικά δεύτερης τάξης συχνά εξετάζονται με την βοήθεια ενός ομοιοκατευθυντικού στο αζιμουθιακό επίπεδο μοντέλου διάδοσης, προκύπτει ότι εξαρτώνται ουσιαστικά από τις γωνίες άφιξης της λαμβανόμενης πολυδιαδρομής. Με άλλα λόγια, συχνά θεωρείται ότι τα κύματα πολυδιαδρομών εισέρχονται στον δέκτη με ίση ισχύ από κάθε πιθανή κατεύθυνση. Ωστόσο, είναι ένα εύλογο και εξιδανικευμένο μοντέλο διάδοσης πολυδιαδρομών για δέκτες που λειτουργούν σε βαριά σκιασμένες περιοχές με μεγάλο αριθμό σκεδαστών και παράγει αναλυτικά αποτελέσματα που αντικατοπτρίζουν σε μεγάλο βαθμό τις αρχικές εκτιμήσεις. Ασχέτως την κατεύθυνση προς την οποία είναι στραμμένος ο κινητός δέκτης, το μοντέλο Clarke δίνει αναλυτικά, ισότροπα αλλά συνήθως μη ρεαλιστικά παρόμοια στατιστικά στοιχεία. Δεδομένου ότι η κατεύθυνση της εισερχόμενης πολυδιαδρομής είναι ένα σημαντικό στοιχείο στην πρόκληση της παρατηρούμενης διάλειψης, μεταγενέστερες εκτιμήσεις και μοντέλα αποκάλυψαν ότι η συμπεριφορά των εισερχόμενων πολυδιαδρομών σε μία τοπική περιοχή παρουσιάζει μικρή ομοιότητα με την υπόθεση της ομοιοκατευθυντικής διάδοσης. Εάν σε έναν δέκτη χρησιμοποιούνται συστήματα κατευθυντικών ή έξυπνων κεραιών, ένα σχεδόν ομοιοκατευθυντικό μοντέλο δεν μπορεί να συλλάβει επαρκώς τα στατιστικά στοιχεία των διαλείψεων. Οποιαδήποτε κατανομή μη ομοιοκατευθυντικών κυμάτων πολυδιαδρομών σε μία τοπική περιοχή όπου η τοπική μέση ισχύς του σήματος θεωρείται ότι είναι wide-sense stationary (ο μέσος όρος μιας στοχαστικής διαδικασίας και η συνάρτηση αυτοσυσχέτισης είναι σταθερά με την πάροδο του χρόνου, αλλά όχι απαραίτητα σταθερές σε κάθε χρονική στιγμή) μπορεί να αναλυθεί ποσοτικά χρησιμοποιώντας την νέα ιδέα των συντελεστών σχήματος πολυδιαδρομών (multipath shape factors). Η αζιμουθιακή κατεύθυνση της μέγιστης διάλειψης, η γωνιακή διασπορά και η γωνιακή στένωση είναι τρεις θεμελιώδεις συντελεστές σχήματος που συνδέονται με ακρίβεια με τον μέσο ρυθμό διάλειψης του λαμβανόμενου σήματος. Αυτή η θεωρία μπορεί να χρησιμοποιηθεί για να εξηγήσει τέσσερα από τα θεμελιώδη στατιστικά στοιχεία διαλείψεων μικρής κλίμακας δεύτερης τάξης, όπως είναι ο ρυθμός level crossing, η μέση διάρκεια διάλειψης, η αυτοσυνδιακύμανση (autocovariance – η συνάρτηση αυτοσυνδιακύμανσης είναι χρήσιμη για έρευνες σε χωρική διαφορική λήψη και καθορίζει την

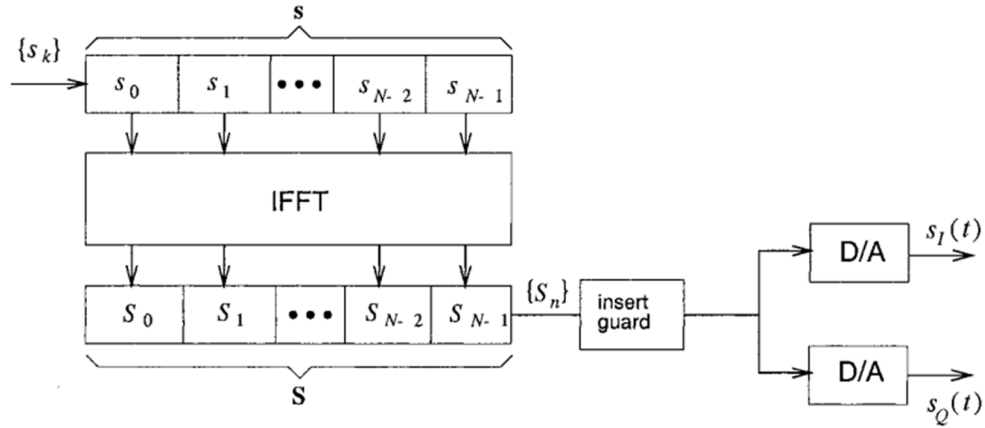
συσχέτιση της περιβάλλουσας της λαμβανόμενης τάσης ως συνάρτηση της μεταβολής της θέσης του δέκτη) και η απόσταση συνοχής (ο χωρικός διαχωρισμός πάνω στον οποίο ένα κανάλι διαλείψεων φαίνεται να παραμένει αμετάβλητο). [1]

2.3 Διαμόρφωση Ορθογώνιας Πολυπλεξίας Διαίρεσης Συχνότητας (OFDM)

Στην παρούσα διπλωματική εργασία, η συγκεκριμένη ενότητα είναι αρκετά σημαντική διότι το μοντέλο συστήματος που θα υλοποιηθεί χρησιμοποιεί την Διαμόρφωση Ορθογώνιας Πολυπλεξίας Διαίρεσης Συχνότητας (OFDM – Orthogonal Frequency Division Multiplexing). Η OFDM είναι μία τεχνική διαμόρφωσης πολλαπλών φερόντων κατά την οποία ένα παράλληλο σύνολο από ομοιόμορφα διατεταγμένους υπο-φορείς (subcarriers) διαμορφώνονται από τα σύμβολα δεδομένων. Παρόλο που τα φάσματα του σήματος για τους διάφορους υποφορείς επικαλύπτονται σε συχνότητα, οι υποφορείς έχουν την απαραίτητη ελάχιστη απόσταση συχνοτήτων που απαιτείται για την διατήρηση της ορθογωνιότητας των αντίστοιχων κυματομορφών τους στο πεδίο του χρόνου. Λόγω της φασματικής επικάλυψης, η κυματομορφή κάνει εξαιρετική χρήση του διαθέσιμου εύρους ζώνης. Η διαμόρφωση αυτή είναι εύκολο να χρησιμοποιηθεί σε κανάλια με καθυστέρηση λόγω διασποράς ή αλλιώς επιλεκτικότητα συχνότητας. Αυτά τα κανάλια περιγράφονται είτε από την διασπορά καθυστέρησης (delay spread) είτε από το εύρος ζώνης συνοχής του καναλιού το οποίο εκτιμά την αποσυσχέτιση του καναλιού στην συχνότητα. Η ενεργός διασπορά καθυστέρησης και το εύρος ζώνης συνοχής είναι αντιστρόφως ανάλογα. Με την χρήση της OFDM, ένα κανάλι επιλεκτικής συχνότητας μπορεί να μετατραπεί σε ένα παράλληλο σύνολο υποκαναλιών επίπεδων διαλείψεων στη συχνότητα με κατάλληλη επιλογή της απόστασης των υποφορέων σε αναλογία με το εύρος ζώνης συνοχής του καναλιού. Στην συνέχεια, θα είναι απλό να χρησιμοποιηθούν μέθοδοι που είναι κατάλληλες για κανάλια επίπεδων διαλείψεων. [2]

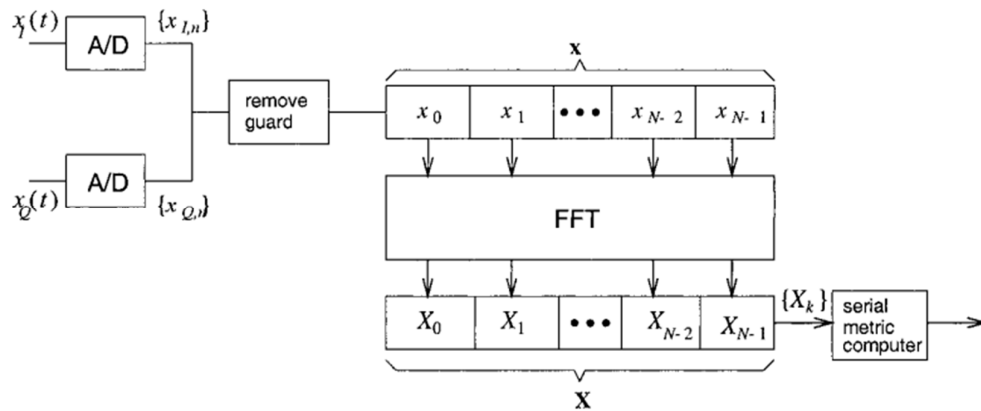
2.3.1 Η ιδέα της OFDM

Για την δημιουργία ενός διαμορφωτή OFDM χρησιμοποιείται ένα αντίστροφος διακριτός μετασχηματισμός Fourier (IDFT – Inverse Discrete Fourier Transform) N σημείων σε ένα μπλόκ με N σύμβολα δεδομένων, σειριοποίηση της εξόδου, εισαγωγή φύλαξης, ακολουθούμενα από έναν μετατροπέα ψηφιακού σε αναλογικό (DAC – Digital to Analog Converter) στα δείγματα IDFT. Στην πράξη, ο υπολογιστικά αποδοτικός αντίστροφος γρήγορος μετασχηματισμός Fourier (IFFT – Inverse Fast Fourier Transform) μπορεί να χρησιμοποιηθεί για την υλοποίηση του IDFT.



Εικόνα 2-14: Απεικόνιση ενός βασικού OFDM πομπού. [2]

Όπως γίνεται αντιληπτό στο παραπάνω σχήμα (Εικόνα 2-14), τα s_k σύμβολα δεδομένων τα οποία υπόκεινται σε IFFT παράγοντας τα σύμβολα δεδομένων στο πεδίο του χρόνου. Η διασπορά καθυστέρησης προκαλεί την διασυμβολική παρεμβολή (ISI – InterSymbol Interference). Προκειμένου να αντιμετωπισθεί αυτό το φαινόμενο, ένα κυκλικό πρόθεμα (CP – Cyclic Prefix) ή guard interval που απαρτίζεται από N_g δείγματα, ακολουθεί κάθε μπλοκ από N συντελεστές IFFT έτσι ώστε το μήκος του καναλιού N_h σε δείγματα να είναι τουλάχιστον ισοδύναμο με το μήκος του κυκλικού προθέματος. Οι τελικοί συντελεστές N_g απλώς επαναλαμβάνονται στο κυκλικό πρόθεμα. Ένα κυκλικό επίθημα (CS – Cyclic Suffix), το οποίο είναι μία επανάληψη των πρώτων συντελεστών N_g IFFT μπορεί αντ’ αυτού να προστεθεί στο τέλος ενός μπλοκ N συντελεστών IFFT. Δεδομένου ότι περιέχει πλεονάζοντα σύμβολα, το guard interval μήκους N_g είναι μία επιβάρυνση που μειώνει την απόδοση ισχύος και το εύρος ζώνης. Ωστόσο, επειδή το guard interval περιλαμβάνει επαναλαμβανόμενα σύμβολα με καθορισμένο μήκος δειγμάτων, μπορεί να χρησιμοποιηθεί για την εκτέλεση λειτουργιών συγχρονισμού χρόνου και συχνότητας στο δέκτη.



Εικόνα 2-15: Απεικόνιση ενός βασικού OFDM δέκτη. [2]

Στον δέκτη (Εικόνα 2-15), ένας μετατροπέας αναλογικού σε ψηφιακό (ADC – Analog to Digital Converter) δειγματοληπτεί το σύνθετο σήμα βασικής ζώνης που ελήφθη, συχνά με μια συχνότητα δειγματοληψίας. Περιστασιακά χρησιμοποιείται κλασματική δειγματοληψία. Το συνολικό κανάλι διακριτού χρόνου παράγεται στην συνέχεια από τη συνέλιξη του DAC στον πομπό με το κανάλι διάδοσης και τον ADC στον δέκτη. Μετά την διαδικασία που εκτελεί ο ADC, σε

περίπτωση CS τα δείγματα μ που λαμβάνονται στο τέλος του συμβόλου OFDM αντικαθιστούν τα δείγματα N_g που λαμβάνονται στην αρχή ενός συμβόλου. Σε περίπτωση CP, γίνεται απομάκρυνση των δειγμάτων N_g που λαμβάνονται κατά την διάρκεια του guard interval κάθε OFDM συμβόλου. Η γραμμική συνέλιξη της σειράς της μεταδιδόμενης ακολουθίας των συντελεστών IFFT με το κανάλι διακριτού χρόνου αλλάζει σε κυκλική συνέλιξη εάν το N_g είναι μεγαλύτερο ή ίσο από το N_h . Αυτό έχει ως αποτέλεσμα, οι επιδράσεις των ISI να εξαλείφονται πλήρως και με ευκολία. Κάθε μπλοκ N εισερχομένων δειγμάτων μετασχηματίζεται πίσω στο πεδίο της συχνότητας χρησιμοποιώντας έναν γρήγορο μετασχηματισμό Fourier (FFT – Fast Fourier Transform) αφού αφαιρεθεί το guard interval. Η αποδιαμόρφωση βασικής ζώνης πραγματοποιείται μέσω αυτής της διαδικασίας FFT. Ένας απλός one-tap ισοσταθμιστής (one-tap equalizer – μία γραμμή καθυστέρησης και κέρδους που χρησιμοποιείται για την ισοστάθμιση των καναλιών επίπεδων διαλείψεων στο πεδίο της συχνότητας) του πεδίου της συχνότητας (FDE – Frequency Domain Equalizer), επεξεργάζεται καθένα από τα N δείγματα του πεδίου συχνότητων τα οποία στην συνέχεια εφαρμόζονται σε μία συσκευή λήψης απόφασης για την ανάκτηση των συμβόλων δεδομένων διαφορετικά, εάν χρησιμοποιείται κώδικας διόρθωσης σφαλμάτων σε έναν αποκωδικοποιητή. Κάθε συντελεστής FFT πολλαπλασιάζεται στο μιγαδικό πεδίο τιμών χρησιμοποιώντας τον one-tap FDE.

Το κύριο πλεονέκτημα της OFDM αναφέρεται συχνά ότι είναι η απλότητα της ισοστάθμισης. Ωστόσο, όπως έχει ήδη αναφερθεί, τα συστήματα μιας φέρουσας μπορούν επίσης να χρησιμοποιούν τις ίδιες μεθόδους ισοστάθμισης. Η ισοστάθμιση στο πεδίο συχνότητας ενός φέροντος (SC-FDE – Single Carrier Frequency Domain Equalization) είναι μια τέτοια μέθοδος. Τα συστήματα SC-FDE στέλνουν δεδομένα σε μπλοκ των N συμβόλων κάθε φορά, όπως ακριβώς και η OFDM. Ένα κυκλικό πρόθεμα μήκους N_g που είναι απλώς μια επανάληψη των τελικών δειγμάτων N_g σε κάθε μπλοκ μήκους N έρχεται πριν από κάθε μπλοκ N συμβόλων δεδομένων. Εναλλακτικά, μπορεί να προστεθεί ένα κυκλικό επίθημα μήκους N_g που είναι επανάληψη των πρώτων δειγμάτων G σε κάθε μπλοκ μήκους N . Μετά την εφαρμογή του μπλοκ μήκους $N+N_g$ σε έναν DAC, μεταφέρεται στη ζώνη των ραδιοσυχνοτήτων (RF – Radio Frequency) και αποστέλλεται μέσω του καναλιού. Η λαμβανόμενη κυματομορφή εφαρμόζεται σε έναν ADC αφού υποστεί κάτω-μετατροπή στη συχνότητα και μετατραπεί σε κυματομορφή μιγαδικής βασικής ζώνης. Μετά από αυτό, με τον ίδιο ακριβώς τρόπο όπως ένας δέκτης OFDM, ο δέκτης εξαλείφει το guard interval. Στη συνέχεια, χρησιμοποιείται ένας FFT N σημείων για τον μετασχηματισμό της ακολουθίας δειγμάτων μήκους N από το πεδίο του χρόνου στο πεδίο της συχνότητας. Ακολούθως, οι N συντελεστές του FFT υποβάλλονται σε ισοστάθμιση στο πεδίο της συχνότητας (FDE). Για να γίνει ισοστάθμιση zero-forcing ή ισοστάθμιση ελάχιστου μέσου τετραγωνικού σφάλματος, ο FDE απλώς πολλαπλασιάζει κάθε συντελεστή FFT με ένα μιγαδικό βάρος, παρόμοια με τον τρόπο που γίνεται στην OFDM. Τα ισοσταθμισμένα δείγματα εφαρμόζονται εν συνεχεία σε μια συσκευή λήψης αποφάσεων ή σε έναν soft-decoder, αφού μεταφραστούν πίσω στο πεδίο του χρόνου με τη χρήση ενός IFFT N σημείων. Ο SC-FDE και η OFDM έχουν παρόμοιο επίπεδο πολυπλοκότητας του συστήματος. Η κύρια διάκριση μεταξύ των δύο είναι ότι το SC-FDE χρησιμοποιεί ένα ζεύγος FFT/IFFT στο δέκτη, ενώ το OFDM χρησιμοποιεί ένα IFFT στον πομπό και ένα FFT στο δέκτη. [2]

2.3.2 Συγχρονισμός (Synchronization) και Εκτίμηση του Καναλιού (Channel Estimation)

Ο συγχρονισμός του χρόνου, η εκτίμηση και διόρθωση της μετατόπισης της συχνότητας (frequency offset) του σήματος, καθώς και η αρχική εκτίμηση του καναλιού, απαιτούνται από ένα σύστημα OFDM που λειτουργεί στη κατάσταση λήψης. Αυτές οι λειτουργίες συγχρονισμού διευκολύνονται συνήθως από ένα προοίμιο συγχρονισμού που αποτελείται από μια ακολουθία εκμάθησης ή τη σύνδεση πολλών ακολουθιών εκμάθησης για συστήματα που μεταδίδουν πληροφορίες με πακετοποιημένο τρόπο ή τρόπο καταιγισμού (burst mode). Κάθε περίοδος εκμάθησης πρέπει να έχει ένα κατάλληλο cyclic guard interval. Στην ροή των OFDM συμβόλων που περιέχουν τα εκπεμπόμενα δεδομένα, εισάγεται κατά περιόδους το προοίμιο συγχρονισμού. Δεδομένου ότι το cyclic guard interval του συμβόλου OFDM αποτελείται από επαναλαμβανόμενα δείγματα που απέχουν μεταξύ τους χρονικά, οι αλγόριθμοι συγχρονισμού μπορούν να επωφεληθούν από αυτό το χαρακτηριστικό. Μπορεί να χρησιμοποιηθεί το διάστημα προστασίας για να εκτιμηθεί η μεταβολή της φάσης που προκαλείται από τις μετατοπίσεις συχνότητας του ταλαντωτή και του καναλιού.

Μόλις ολοκληρωθεί η λήψη του preamble, ο δέκτης μεταβαίνει σε λειτουργία ανάκτησης δεδομένων όπου παρακολουθεί παράλληλα τις αλλαγές στο κανάλι καθώς και την παρέκκλιση στους ταλαντωτές ραδιοσυχνότητας και στο ρολόι δειγματοληψίας. Οι συντελεστές του καναλιού παρακολουθούνται συχνά με την προσθήκη επιπλέον OFDM pilot symbols ή με τη χρήση pilot subcarriers που ακολουθούνται από παρεμβολή (interpolation) στα πεδία χρόνου και συχνότητας για εφαρμογές με σημαντικές διασπορές Doppler, όπως τα επίγεια κινητά συστήματα ασύρματης επικοινωνίας. Δεδομένου ότι τα τερματικά των χρηστών είναι συχνά ακίνητα ή κινούνται αργά, το κανάλι είναι μάλλον στατικό στις εφαρμογές WLAN και WMAN. Λόγω της παρουσίας μετατοπίσεων συχνότητας μεταξύ του πομπού και των τοπικών ταλαντωτών ραδιοσυχνότητας και του ρολογιού δειγματοληψίας στον δέκτη, οι χρονικές διακυμάνσεις του καναλιού εξακολουθούν να προβλέπονται σε αυτό το σενάριο. Τα εξαρτήματα που χρησιμοποιούνται στον εξοπλισμό των εγκαταστάσεων του τερματικού τελικού χρήστη είναι συχνά φθηνά και έχουν μικρές ανοχές. [2]

2.3.3 OFDM Πολλαπλών Εισόδων και Πολλαπλών Εξόδων (MIMO OFDM)

Ένα περιβάλλον διάδοσης με πυκνή διασπορά μπορεί να αξιοποιηθεί από συστήματα ασύρματων επικοινωνιών με πολλές κεραίες εκπομπής και λήψης για την ενίσχυση της χωρητικότητας του καναλιού (η μέγιστη ποσότητα πληροφορίας που μπορεί να μεταδοθεί μέσω ενός καναλιού με δεδομένο εύρος ζώνης, σηματοθορυβικό λόγο και ρυθμό σφαλμάτων). Οι προσεγγίσεις πολλαπλών εισόδων και πολλαπλών εξόδων (MIMO – Multiple Input Multiple Output) κατατάσσονται σε δύο κατηγορίες. Η μία κατηγορία μεγιστοποιεί τη χωρική διαφορισιμότητα, η οποία αυξάνει την αποδοτικότητα ισχύος. Η διαφορισιμότητα καθυστέρησης, η κωδικοποίηση μπλοκ χώρου-χρόνου και η κωδικοποίηση trellis χώρου-χρόνου (STBC – Space-Time Block and Coding και STTC – Space-Time Trellis Coding) είναι παραδείγματα τέτοιων μεθόδων. Η άλλη κατηγορία, η οποία χρησιμοποιείται συχνά σε περιπτώσεις όπου δεν μπορεί να επιτευχθεί πλήρης χωρική διαφοροποίηση, χρησιμοποιεί γραμμική επεξεργασία για την αύξηση της ροής δεδομένων. Η Bell Labs Layered Space-Time (BLAST) είναι μια τέτοια μέθοδος.

Η ποικιλομορφία καθυστέρησης ήταν η πρώτη μέθοδος διαφορικής εκπομπής για συστήματα MIMO. Για τον προσδιορισμό της ακολουθίας εκπομπής στο δέκτη, χρησιμοποιείται η εκτίμηση ακολουθίας μέγιστης πιθανοφάνειας (MLSE – Maximum Likelihood Sequence Estimation) όταν πολλές κεραίες εκπομπής παρέχουν καθυστερημένα αντίγραφα του ίδιου σήματος. Σε αυτά τα

συστήματα μπορούν επίσης να εφαρμοστούν ισοσταθμιστές ανατροφοδότησης αποφάσεων (DFE – Decision Feedback Equalizer). Η μέθοδος της διαφορισιμότητας καθυστέρησης είναι απλή και μπορεί να θεωρηθεί ως ένας συγκεκριμένος κώδικας χώρου-χρόνου.

Για συστήματα MIMO, τα STBC και STTC μπορούν να προσφέρουν πλήρη χωρική διαφορισιμότητα. Προκειμένου να επιτευχθεί πλήρης διαφορισιμότητα, το STBC χρησιμοποιεί το χαρακτηριστικό ορθογωνιότητας του κώδικα, ωστόσο, όταν υπάρχουν περισσότερες από δύο κεραίες εκπομπής, η μετάδοση πλήρους ρυθμού δεν είναι δυνατή. Η πλήρης διαφορισιμότητα εξασφαλίζεται από τη χρήση επαρκούς κωδικοποίησης trellis στο STTC, αν και η δυσκολία της αποκωδικοποίησης αυξάνεται εκθετικά με τον αριθμό των κεραιών εκπομπής. Τόσο το STTC όσο και το STBC δεν μπορούν να κλιμακωθούν όσον αφορά την ποσότητα των κεραιών εκπομπής. Αλλαγές στον αριθμό των κεραιών εκπομπής καθιστούν αναγκαία τη χρήση εναλλακτικών κωδίκων χώρου-χρόνου. Αυτές οι μέθοδοι δημιουργήθηκαν για τον χειρισμό σχεδόν στατικών καναλιών επίπεδων διαλείψεων. Τα STBC και STTC πρέπει να συνδυαστούν με άλλες μεθόδους, όπως η ισοστάθμιση ή η OFDM, που δημιουργούν αποτελεσματικά ένα ή περισσότερα κανάλια κωδικοποίησης επίπεδων διαλείψεων, προκειμένου να χρησιμοποιηθούν σε κανάλια διαλείψεων επιλεκτικών στην συχνότητα.

Για κανάλια συχνοεπιλεκτικών διαλείψεων, έχουν προταθεί διατάξεις MIMO-OFDM που συνδυάζουν STTC ή STBC στις διάφορες κεραίες με OFDM. Αυτές οι στρατηγικές μπορούν να αποδώσουν αρκετά καλά σε κανάλια συχνοεπιλεκτικών διαλείψεων. Ωστόσο, ειδικά όταν υπάρχουν πολλές κεραίες εκπομπής, η πολυπλοκότητα μπορεί να είναι αρκετά υψηλή. Μια άλλη μέθοδος χρησιμοποιεί σε κανάλια επίπεδων διαλείψεων διαφορισιμότητας καθυστέρησης με OFDM. Η διαμόρφωση διαφορισιμότητας καθυστέρησης πολλαπλών φερουσών (MDDM – Multi-carrier Delay Diversity Modulation) είναι μια τεχνική κυκλικής διαφορισιμότητας καθυστέρησης που μπορεί να χρησιμοποιηθεί με OFDM για κανάλια συχνοεπιλεκτικών διαλείψεων. Έρευνα έδειξε ότι η πλήρης χωρική διαφορισιμότητα για MDDM σε κανάλια επίπεδων διαλείψεων είναι δυνατή, υπό την προϋπόθεση ότι η ελάχιστη απόσταση Hamming του εξωτερικού (προ-IFFT) κώδικα διόρθωσης σφαλμάτων είναι ίση ή μεγαλύτερη από τον αριθμό των κεραιών εκπομπής και ότι η απλή διεμπλοκή μπλοκ (block interleaving) αρκεί για να επιτευχθεί καλή κωδικοποίηση κέρδους. Η μέθοδος είναι κλιμακούμενη σε αντίθεση με το STBC και το STTC δηλαδή ο αριθμός των κεραιών εκπομπής μπορεί να μεταβληθεί χωρίς να μεταβληθεί ο κώδικας διόρθωσης σφαλμάτων. Ανάλογα με τις συνθήκες, η MDDM μπορεί να διαχειριστεί τις συχνοεπιλεκτικές διαλείψεις χρησιμοποιώντας συνδυασμό μέγιστου κέρδους (MRC – Maximum-Ratio Combining) ή άλλο είδος συνδυασμού. [2]

3

Αλλοιώσεις Ραδιοσυχνοτήτων

Προκειμένου οι ασύρματοι πομποδέκτες να μπορούν να κυκλοφορούν στην αγορά για διάφορες εφαρμογές, θα πρέπει να είναι οικονομικά προσιτοί. Η χρήση φθηνών μη ιδανικών αναλογικών εξαρτημάτων RF βοηθά στην παραπάνω ανάγκη. Όμως, διάφορα κατασκευαστικά ελαττώματα μπορούν να προκαλέσουν αλλοιώσεις στο RF όπως θόρυβο φάσης (PN), μετατόπιση συχνότητας φέροντος (CFO) και ανισορροπία συμφασικής (I) και ορθογώνιας (Q) συνιστώσας. Αυτές οι αλλοιώσεις μειώνουν την απόδοση των ασύρματων συστημάτων και εισάγουν παρεμβολές εντός και εκτός ζώνης. Το παρόν κεφάλαιο αναλύει και περιγράφει τις διαφορετικές αλλοιώσεις που παρατηρούνται στους ασύρματους πομποδέκτες με έμφαση στα συστήματα που υλοποιούν διαμόρφωση OFDM. Τέλος αναλύονται οι επιπτώσεις αυτών των αλλοιώσεων σε ασύρματες τεχνολογίες που είναι ήδη καθιερωμένες, όπως οι επικοινωνίες πολλαπλών εισόδων και πολλαπλών εξόδων (MIMO), οι μαζικές επικοινωνίες MIMO (massive MIMO), οι επικοινωνίες full-duplex και οι επικοινωνίες χιλιοστομετρικών κυμάτων (mmWave). [3]

3.1 Εισαγωγή στις Αλλοιώσεις Ραδιοσυχνοτήτων

Η ανάπτυξη υπηρεσιών υψηλού ρυθμού δεδομένων σε συστήματα ασύρματων επικοινωνιών πέμπτης γενιάς (5G) και μεταγενέστερα είναι απαραίτητη λόγω της δραματικής αύξησης της κυκλοφορίας των δεδομένων κινητής τηλεφωνίας. Η εμπλουτισμένη κινητή ευρυζωνικότητα (eMBB – enhanced Mobile BroadBand), οι μαζικές επικοινωνίες μεταξύ μηχανών (mMTC – massive Machine Type Communications), οι εξαιρετικά αξιόπιστες επικοινωνίες μικρής καθυστέρησης (URLLC – Ultra Reliable and Low Latency Communications) και οι επικοινωνίες αμφίδρομης επικοινωνίας οχήματος προς τα πάντα (V2X – Vehicle-To-Everything) είναι μερικές ακόμη εφαρμογές που πρέπει να διαχειριστούν τα δίκτυα 5G. Το 5G θέτει σημαντικούς στόχους, όπως ο 1000πλάσιος ρυθμός μετάδοσης δεδομένων, η καθυστέρηση κάτω από 100ms, η μείωση του κόστους δικτύου κατά 50% και η διαθεσιμότητα 95% σε περιοχές με κακή κάλυψη, για να καλύψει αυτές τις τεράστιες ανάγκες συνδεσιμότητας. Ως εκ τούτου, έχουν αναπτυχθεί ασύρματες

τεχνολογίες για την αύξηση της απόδοσης του συστήματος και την ενίσχυση της φασματικής απόδοσης. Μεταξύ αυτών είναι τα συστήματα MIMO και massive MIMO (τα massive MIMO αναφέρονται στα συστήματα μεγάλου αριθμού κεραιών πολλαπλών εισόδων και πολλαπλών εξόδων), οι συνεργατικές επικοινωνίες αναμετάδοσης, τα γνωστικά ασύρματα δίκτυα, τα ασύρματα συστήματα full-duplex και τα συστήματα χιλιοστομετρικών κυμάτων. Αυτά τα συστήματα απαιτούν ένα σύστημα βασικής ζώνης, πολλά front-ends ραδιοσυχνοτήτων, πολυάριθμες κεραιές και άλλα εξαρτήματα στους πομποδέκτες τους. Η μεγιστοποίηση της διαφορισιμότητας και του κέρδους πολυπλεξίας, η διασφάλιση της ποιότητας υπηρεσιών του χρήστη, η ελαχιστοποίηση της εκπομπής εκτός εύρους ζώνης, η επίτευξη ενός προκαθορισμένου μέγιστου ρυθμού, η μείωση των πιθανοτήτων διακοπής και η βελτιστοποίηση της απόδοσης ανίχνευσης δεδομένων αποτελούν απαιτήσεις σχεδιασμού.

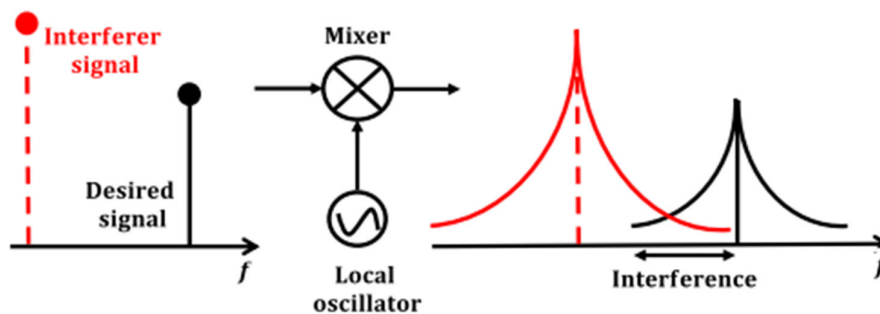
Ο λόγος διαρροής ισχύος σε παρακείμενο δίαυλο (ACLR – Adjacent Channel Leakage Ratio), το μέγεθος διανυσματικού σφάλματος (EVM – Error Vector Magnitude), τα επίπεδα ισχύος ευαισθησίας, ο αποκλεισμός εντός και εκτός ζώνης και άλλα χαρακτηριστικά επηρεάζονται από τις αλλοιώσεις RF στους πομποδέκτες. Απαιτείται η μείωση των επιδράσεων των αλλοιώσεων RF προκειμένου να πληρούνται οι απαιτήσεις του παρόντος και άλλων προτύπων.

Ο ταλαντωτής, ο οποίος παράγει ένα σήμα αναφοράς για τον συγχρονισμό συχνότητας και χρόνου, είναι ένα από τα πιο σημαντικά αναλογικά εξαρτήματα όσον αφορά την πρόκληση αλλοιώσεων RF. Ωστόσο, οι ουσιαστικές αλλοιώσεις, όπως ο θόρυβος φάσης (PN – Phase Noise), η μετατόπιση συχνότητας φέροντος (CFO – Carrier Frequency Offset) και η ανισορροπία μεταξύ συμφασικής (I – In-phase) και ορθογώνιας (Q – Quadrature) συνιστώσας, προκαλούνται από μη ιδανικές ατέλειες και αστάθεια του ταλαντωτή στο πεδίο του χρόνου. Αυτές οι αλλοιώσεις προκαλούν παραμορφώσεις τόσο εντός όσο και εκτός ζώνης. Η απόδοση του συστήματος καταστρέφεται από τις παραμορφώσεις εντός ζώνης, οι οποίες εμφανίζονται εντός του εύρους ζώνης λειτουργίας. Για παράδειγμα, προκαλούν παρεμβολές μεταξύ των φορέων (ICI – Inter-Carrier Interference) και εξαλείφουν την ορθογωνιότητα των υποφορέων στα συστήματα OFDM. Από την άλλη πλευρά, οι παραμορφώσεις εκτός ζώνης εμφανίζονται εκτός του εύρους ζώνης λειτουργίας. Για παράδειγμα, η διασπορά φάσματος παρεμποδίζει τα γειτονικά κανάλια. Αυτές οι παραμορφώσεις προκαλούν σοβαρή μείωση της απόδοσης του συστήματος. Αυτή η επιδείνωση μπορεί να εμφανιστεί με διάφορους τρόπους είτε με μείωση των επιτεύξιμων ρυθμών και αύξηση των διαλείψεων είτε με μείωση του SNR και αύξηση BER είτε με αύξηση του EVM λόγω παραμορφώσεων φάσης και πλάτους στον αστερισμό του σήματος είτε με μείωση της ακρίβειας των εκτιμήσεων του καναλιού. Ως εκ τούτου, οι αλλοιώσεις RF έχουν σημαντικές επιπτώσεις στους ασύρματους πομποδέκτες. [3]

3.1.1 Εισαγωγή στον Θόρυβο Φάσης (Phase Noise)

Όταν ο ταλαντωτής δεν είναι σε θέση να παράγει καθαρά ημιτονοειδή κύματα με το φάσμα Dirac, αναπτύσσεται PN. Οι γρήγορες, σύντομες, τυχαίες αλλαγές στη φάση του φέροντος κύματος που προκαλούνται από τους ταλαντωτές κατά τη διάρκεια των λειτουργιών άνω ή κάτω μετατροπής συχνότητας του σήματος βασικής ζώνης και της αλυσίδας ραδιοσυχνοτήτων είναι η πηγή αυτής της διεύρυνσης του φάσματος. Το φάσμα συχνοτήτων και τα χρονικά χαρακτηριστικά της εξόδου του ταλαντωτή μεταβάλλονται σημαντικά από τον PN. Η παρεμβολή γειτονικού καναλιού (ACI – Adjacent Channel Interference) μπορεί να προκύψει από τη διεύρυνση της φασματικής πυκνότητας

ισχύος (PSD) του PN σε κάθε πλευρά ενός σήματος. Για παράδειγμα, το φάσμα του δέκτη είναι το αποτέλεσμα της συνέλιξης μεταξύ του φάσματος του λαμβανόμενου σήματος ζώνης διέλευσης και του φάσματος του τοπικού ταλαντωτή. Ωστόσο, το φάσμα του ταλαντωτή διασπείρεται ως αποτέλεσμα του PN, προκαλώντας φασματική διασπορά. Η διασπορά που προκύπτει στην Εικόνα 3-1 μπορεί να εισάγει σήματα παρεμβολής στο εύρος ζώνης του σήματος, υποβαθμίζοντας την απόδοση του συστήματος. Επιπλέον, ο PN θέτει ουσιαστικά σε αμφισβήτηση σήματα πολλαπλών φορέων όπως το OFDM, καθώς εξαφανίζει την ορθογωνιότητα των υποφορέων. Η διακαναλική παρεμβολή, τα σφάλματα φάσης σε όλους τους υποφορείς και το ICI μεταξύ των υποφορέων είναι τα αποτελέσματα αυτού.



Εικόνα 3-1: Ο PN εισάγει σήματα παρεμβολής στο εύρος ζώνης του σήματος. [2]

Η παραγόμενη χρονική διακύμανση του καναλιού είναι μια άλλη σημαντική επίπτωση του PN. Με άλλα λόγια, ο αστερισμός του σήματος εκπομπής περιστρέφεται από σύμβολο σε σύμβολο και το ισοδύναμο κανάλι που βλέπει ο δέκτης αλλάζει με το χρόνο. Κατά τη διάρκεια της επεξεργασίας ενός πλαισίου δεδομένων, ο PN σπάει επίσης τη συνοχή μεταξύ της εκτίμησης του καναλιού και του πραγματικού κέρδους του καναλιού. Συνολικά, αυτές οι επιπτώσεις θα μειώσουν το πραγματικό SNR, θα περιορίσουν το BER και θα μειώσουν τους ρυθμούς δεδομένων, τα οποία με την σειρά τους θα μειώσουν την απόδοση των ασύρματων συστημάτων. Ο χαρακτηρισμός του PN σε πραγματικές εφαρμογές είναι ζωτικής σημασίας για όλους αυτούς τους λόγους. Για την ακριβή ανίχνευση δεδομένων, η εκτίμηση και η αντιστάθμιση του PN είναι απαραίτητες.

3.1.2 Μετατόπιση Συχνότητας Φέροντος (CFO – Carrier Frequency Offset)

Η CFO προκύπτει όταν ο τοπικός ταλαντωτής κάτω μετατροπής του δέκτη δεν είναι ακριβώς συγχρονισμένος με το φέρον του λαμβανόμενου σήματος. Αυτή η αναντιστοιχία συχνότητας είναι αποτέλεσμα των ολισθήσεων Doppler και των σφαλμάτων του τοπικού ταλαντωτή. Η ολίσθηση Doppler, η οποία προκύπτει από τη σχετική ταχύτητα του πομπού και του δέκτη, κάνει τον δέκτη να αντιλαμβάνεται μια διαφορετική συχνότητα φέροντος. Στα συστήματα ενός φέροντος (SC) και στα συστήματα πολλαπλών φερόντων, η CFO έχει ως αποτέλεσμα την περιστροφή και την εξασθένηση των σημάτων εκπομπής, εισάγοντας ISI και ICI. Η αμοιβαία ορθογωνιότητα των υποφορέων OFDM διακόπτεται επειδή η CFO μετακινεί το σήμα στο πεδίο της συχνότητας και, ως αποτέλεσμα, κάθε υποφορέας παρεμβαίνει στα σήματα των άλλων υποφορέων. Κατά συνέπεια, τα συστήματα OFDM είναι ιδιαίτερα ευάλωτα στην CFO. Το BER των συστημάτων OFDM θα αυξηθεί εάν ο δέκτης δεν εκτιμήσει με ακρίβεια και δεν διορθώσει τη CFO πριν από τον εντοπισμό

δεδομένων. Επιπλέον, καταδεικνύει ότι η παρουσία CFO καθιστά αδύνατη τη βελτίωση της απόδοσης του μέσου τετραγωνικού σφάλματος (MSE – Mean Squared Error) της εκτίμησης καναλιού με την αύξηση της ποσότητας των συμβόλων εκμάθησης και ότι η CFO καθιστά τον εκτιμητή καναλιού άχρηστο. Είναι ζωτικής σημασίας η ποσοτικοποίηση των επιπτώσεων της CFO στα συστήματα, η εκτίμηση της CFO και η αντιστάθμισή της. [3]

3.1.3 *Ανισορροπία μεταξύ Συμφασικής και Ορθογώνιας συνιστώσας (IQ Imbalance – In-phase Quadrature Imbalance)*

Για τη μετατροπή σύνθετων σημάτων βασικής ζώνης σε ζωνοπερατά σήματα με κέντρο τη συχνότητα του φέροντος και αντίστροφα, ο διαμορφωτής και ο αποδιαμορφωτής συμφασικής και ορθογώνιας συνιστώσας (IQ Modulator – IQ Demodulator) αποτελούν συστατικό του εμπρόσθιου τμήματος RF των ασύρματων πομποδεκτών. Συχνά χρησιμοποιούνται επίσης αρχιτεκτονικές υπερετερόδυνου δέκτη και δέκτη άμεσης μετατροπής (επίσης γνωστός ως δέκτης μηδενικής ενδιάμεσης συχνότητας (IF – Intermediate Frequency) ή ως Ομόδυνος δέκτης). Ο υπερετερόδυνος δέκτης χρησιμοποιεί τη μίξη συχνοτήτων για τη μετατροπή του λαμβανόμενου σήματος σε μια σταθερή ενδιάμεση συχνότητα (IF), η οποία μπορεί να επεξεργαστεί ευκολότερα από την αρχική φέρουσα συχνότητα. Για τη μετατροπή ενός λαμβανόμενου σήματος RF σε σήμα βασικής ζώνης, ο υπερετερόδυνος δέκτης περνάει από δύο φάσεις. Το πρώτο στάδιο χρησιμοποιεί έναν ενισχυτή χαμηλού θορύβου, έναν μίκτη και ζωνοπερατά φίλτρα για να μετατρέψει το λαμβανόμενο σήμα σε σήμα χαμηλής συχνότητας IF. Μέσω της χρήσης ενός αποδιαμορφωτή IQ, ενός συμφασικού τοπικού ταλαντωτή, ενός τοπικού ταλαντωτή ορθογώνιας φάσης, δύο μίκτες και χαμηλοπερατά φίλτρα, το προκύπτον σήμα IF μετατρέπεται σε σήμα βασικής ζώνης.

Αντίθετα, ο δέκτης άμεσης μετατροπής χρησιμοποιεί τον αποδιαμορφωτή IQ για να μετατρέψει το σήμα RF απευθείας στο σήμα βασικής ζώνης σε ένα στάδιο. Για τον σχεδιασμό RF, η προσέγγιση άμεσης μετατροπής είναι πιο επιθυμητή από τη υπερετερόδυνη δομή. Για παράδειγμα, τα συστήματα IEEE 802.11a OFDM χρησιμοποιούν δέκτες άμεσης μετατροπής επειδή καταργούν το στάδιο IF και το φίλτρο απόρριψης εικόνας και επειδή έχουν συνολικά λιγότερα εξαρτήματα εκτός chip. Αυτά τα στοιχεία καθιστούν την ενσωμάτωση απλούστερη χωρίς μεγάλο κόστος και χρησιμοποιούν λιγότερο χώρο και ισχύ. Η άμεση μετατροπή, όμως, παρεμποδίζεται από ασυνέπειες μεταξύ των κλάδων I και Q.

Το πραγματικό και το φανταστικό μέρος του μιγαδικού σήματος παρέχονται με δύο ορθογώνια κανάλια από ιδανικούς διαμορφωτές και αποδιαμορφωτές IQ. Η ανισορροπία IQ που προκύπτει από τις αναντιστοιχίες μεταξύ των κλάδων I και Q, ωστόσο, καταστρέφει αυτή την ορθογωνιότητα και μειώνει την ποιότητα του σήματος. Για τις αναντιστοιχίες ευθύνονται οι αποκλίσεις της διαδικασίας κατασκευής, συμπεριλαμβανομένης της συγκέντρωσης των προσμίξεων, του πάχους οξειδίου, της κινητικότητας και των γεωμετρικών μεγεθών σε όλο το τσιπ. Όσον αφορά τις επιδράσεις τους, μπορεί κανείς να κατηγοριοποιήσει τις αναντιστοιχίες που οδηγούν στην IQ ανισορροπία σε δύο ομάδες. Η πρώτη ομάδα αφορά την ανισορροπία IQ επίπεδης συχνότητας, η οποία οδηγεί σε ατελή διαφορά φάσης 90 μοιρών και άνισα πλάτη των τοπικών ταλαντωτών I και Q και είναι σταθερή σε όλο το εύρος ζώνης του σήματος. Η δεύτερη ομάδα αφορά την ανισορροπία IQ επιλεκτικής συχνότητας, η οποία οδηγεί σε αναντιστοιχία στοιχείων στους κλάδους I και Q, όπως ακατάλληλα προσαρμοσμένα χαμηλοπερατά φίλτρα, και έχει διαφορετικές αποκρίσεις

συχνότητας σε όλο το εύρος ζώνης του σήματος. Πρέπει να ληφθεί υπόψη ότι στα συστήματα ευρείας ζώνης, οι επιλεκτικές ως προς την συχνότητα συνιστώσες I και Q είναι σημαντικές.

Η απόδοση του συστήματος, συμπεριλαμβανομένων του BER, του λόγου σήματος προς παρεμβολή συν θόρυβο (SINR – Signal-to-Interference plus Noise Ratio), της χωρητικότητας και του EVM, επηρεάζεται αρνητικά από αυτές τις ανισορροπίες IQ, οι οποίες προκαλούν επίσης επιζήμιες παρεμβολές λόγω κατοπτρισμού. Η ανισορροπία πλάτους και φάσης IQ δημιουργεί ένα κατοπτρικό είδωλο εντός ζώνης που παρουσιάζεται ως παρεμβολή. Για παράδειγμα, στα συστήματα SC, η ανισορροπία IQ μεταξύ πομπού και δέκτη οδηγεί σε ISI σε κοντινά σήματα. Ο κατοπτρικός υποφορέας του k-οστού υποφορέα OFDM αναφέρεται ως "k" σε συστήματα πολλαπλών φορέων όπως τα OFDM, όπου η ανισορροπία IQ προκαλεί όρους ICI. Επιπλέον, η ανισορροπία IQ μειώνει την αποτελεσματικότητα των μεθόδων εκτίμησης καναλιού προσθέτοντας όρους κατοπτρικής παρεμβολής. Για να συμμορφωθούν τα συστήματα με τα πρότυπα, πρέπει επομένως να αντισταθμιστεί η ανισορροπία IQ. Για παράδειγμα, η ελάχιστη εξασθένηση για τη συνιστώσα του ειδώλου εντός της ζώνης στον πομπό επιτρέπεται να είναι μόνο 25 dB ή 28 dB σύμφωνα με τις απαιτήσεις των ασύρματων συστημάτων LTE/LTE-Advanced του οργανισμού 3GPP (Third Generation Partnership Project). Ως αποτέλεσμα, είναι εφικτό να ρυθμιστεί η ανισορροπία IQ στο αναλογικό πεδίο, κάνοντας, για παράδειγμα, τις συσκευές μεγαλύτερες από φυσική άποψη για να μειώσουμε τις ανισορροπίες IQ. Ωστόσο, αυτές οι μέθοδοι έχουν περιορισμούς, όπως μια παρατεταμένη διαδικασία βαθμονόμησης και μια αύξηση της ισχύος αντιστάθμισης, και συνεπώς δεν μπορούν να ικανοποιήσουν τις απαιτήσεις για τα συστήματα από μόνες τους. Ως αποτέλεσμα, οι εκτιμήσεις ανισορροπίας IQ με βάση την επεξεργασία σήματος και οι μέθοδοι αντιστάθμισης στο ψηφιακό πεδίο θα μπορούσαν να είναι χρήσιμες. [3]

3.2 Θόρυβος Φάσης (Phase Noise)

Το σήμα εξόδου ενός μιγαδικού ταλαντωτή με θόρυβο μπορεί να περιγραφεί ως εξής:

$$C_{osc} = e^{j(2\pi f_c t + \varphi(t))} \quad (3.2.0.1)$$

με f_c να αποτελεί την συχνότητα φέροντος και $\varphi(t)$ τον θόρυβο φάσης (PN). Η PSD σε dBc/Hz του PN χρησιμεύει ως ευρεία περιγραφή του PN στο πεδίο της συχνότητας. Στην πραγματική εφαρμογή, χρησιμοποιούνται δύο τύποι ταλαντωτών: ο συνθέτης με βρόχο κλειδώματος φάσης (PLL – Phase Locked Loop) και ο ταλαντωτής ελεύθερης λειτουργίας (free-running oscillator). Οι ταλαντωτές ελεύθερης λειτουργίας λειτουργούν χωρίς PLL. Η παραγόμενη φάση σε αυτούς τους ταλαντωτές αναπαρίσταται ως συσσώρευση τυχαίων διαιρέσεων συχνότητας. Ωστόσο, ένας στενός βρόχος καταγράφει τις διακυμάνσεις φάσης του φέροντος σήματος στους συνθέτες PLL. Διάφορες έρευνες θεωρούν πηγές λευκού θορύβου για το PN στους ταλαντωτές. Ωστόσο, δεν λαμβάνονται υπόψη άλλοι τύποι θορύβου πυκνότητας έγχρωμου φάσματος, οι οποίες έχουν σημαντικό αντίκτυπο στην απόδοση PN των πρακτικών ταλαντωτών.

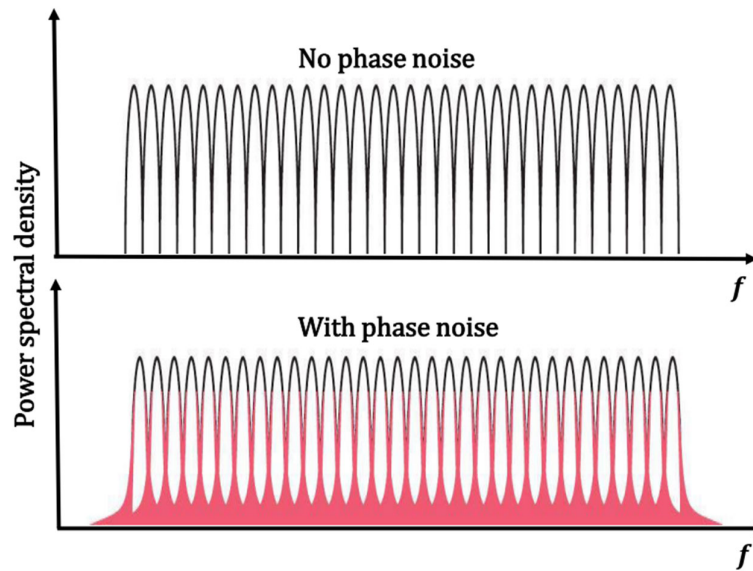
Ταλαντωτές ελεύθερης λειτουργίας ονομάζονται επειδή δεν διαθέτουν είσοδο συγχρονισμού, όπως ένα ρολόι αναφοράς. Λειτουργούν χωρίς αναφορά, επομένως ο PN τους εξαρτάται από τις συνθήκες ενεργοποίησής τους. Το μοντέλο αυτού του είδους ταλαντωτή είναι απλό και χρησιμοποιείται συνήθως σε προσομοιώσεις και μαθηματικές μελέτες. Ο PN που δημιουργείται από έναν ελεύθερο ταλαντωτή, θεωρείται συνήθως διαδικασία Wiener με πηγές λευκού θορύβου και ακολουθεί την κίνηση Brown.

Ο PN μπορεί να αναπαραστεί ως:

$$\varphi(t) = \sqrt{\nu}W(t) \quad (3.2.0.1)$$

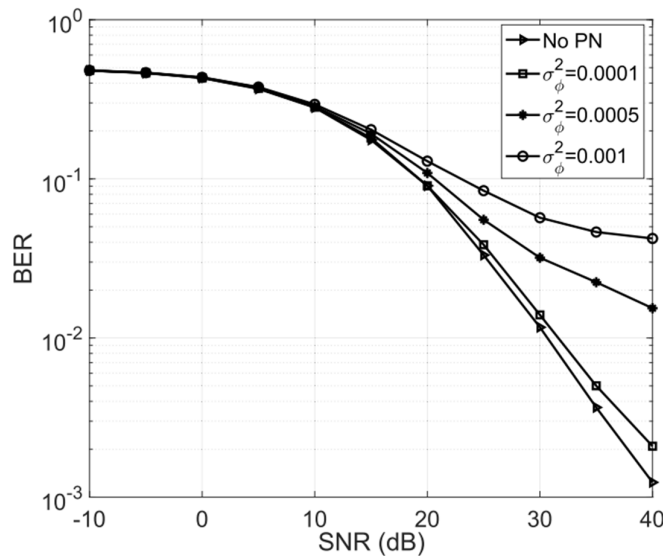
με ν να είναι μία σταθερά που περιγράφει την φασματική διασπορά σε έναν ταλαντωτή που παράγει θόρυβο χρησιμοποιώντας πηγές λευκού θορύβου και $W(t)$ αποτελεί την διαδικασία Wiener η οποία είναι μία στοχαστική διαδικασία συνεχούς χρόνου πραγματικών τιμών.

Ο PLL χρησιμοποιείται συχνά ως συνθέτης συχνότητας σε συστήματα επικοινωνίας. Το βασικό μπλοκ διάγραμμα (block diagram) PLL αποτελείται από διάφορα συζευγμένα στοιχεία αρνητικής ανάδρασης. Η φάση του ταλαντωτή ελέγχου τάσης (VCO – Voltage Control Oscillator) συγκρίνεται με τη φάση του ταλαντωτή αναφοράς από τον ανιχνευτή φάσης. Η συχνότητα του VCO ρυθμίζεται από τη φιλτραρισμένη διαφορά φάσης. Ο VCO και ο ταλαντωτής αναφοράς μπορούν να μοντελοποιηθούν ως ταλαντωτές ελεύθερης λειτουργίας. Για τα PLLs με πηγές λευκού θορύβου και μεταβολή φάσης του σήματος αναφοράς με κίνηση Brown, προτείνεται μια στοχαστική διαφορική εξίσωση. Μια συνιστώσα μιας πολυδιάστατης διαδικασίας Ornstein-Uhlenbeck και η φάση του σήματος αναφοράς μπορούν να συνδυαστούν για να αναπαραστήσουν τη φάση του PLL σε κατάσταση κλειδώματος. Δεν λαμβάνονται υπόψη οι συνέπειες του θορύβου τρεμοπαίσματος (flicker noise) που είναι έγχρωμος θόρυβος (φασματική πυκνότητας $1/f$), για παράδειγμα, τα υψηλά επίπεδα flicker noise που παρουσιάζουν οι PLLs χαμηλής ποιότητας συμπληρωματικού ημιαγωγού μετάλλου-οξειδίου (CMOS – Complementary Metal-Oxide-Semiconductor). Σε όλο το εύρος ζώνης PLL, ο flicker noise έχει αντίκτυπο στην απόδοση PN. Λαμβάνεται υπόψη ένα γραμμικό χρονικά αμετάβλητο μοντέλο PLL στο πεδίο της φάσης, το οποίο υποθέτει λευκό θόρυβο και flicker noise για τον ταλαντωτή αναφοράς ελεύθερης λειτουργίας και λευκό θόρυβο για τον VCO ελεύθερης λειτουργίας. Οι τοπικοί ταλαντωτές τόσο του πομπού όσο και του δέκτη είναι ικανοί να παράγουν PN. Η απόδοση του συστήματος μειώνεται με την εισαγωγή των παραμέτρων περιστροφής φάσης, ISI και ICI, όπως το BER, ο επιτεύξιμος ρυθμός και το EVM. Επιπλέον προκαλείται εκπομπή εκτός ζώνης και διακαναλική παρεμβολή λόγω της επιμήκυνσης του φάσματος από τον PN. Στην παρακάτω εικόνα (Εικόνα 3-2) απεικονίζεται η διασπορά φάσματος για ένα σύστημα OFDM. Θεωρείται ένα σύστημα OFDM με τέλει συγχρονισμό συχνότητας και χρόνου προκειμένου να αποκτηθεί πλήρης εικόνα των επιδράσεων του PN.



Εικόνα 3-2: Διασπορά φάσματος λόγω θορύβου φάσης για ένα σύστημα OFDM. [3]

Μέσα από διάφορες έρευνες, παρατηρείται ότι όσο αυξάνεται ο PN, τόσο αυξάνεται και το BER για ένα σύστημα OFDM. Αυτό μπορεί εύκολα να γίνει κατανοητό από την παρακάτω εικόνα (Εικόνα 3-3).



Εικόνα 3-3: Διάγραμμα BER σε σχέση με την αύξηση του θορύβου φάσης για ένα σύστημα OFDM. [3]

Σύμφωνα με την παραπάνω εικόνα (Εικόνα 3-3), θόρυβος φάσης προκαλεί δύο τύπους παραμορφώσεων. Πρώτον, όλοι οι υποφορείς έχουν την ίδια σταθερή περιστροφή φάσης ή κοινό σφάλμα φάσης. Δεύτερον, προκαλείται παρεμβολή μεταξύ των γειτονικών υποφορέων.

3.2.1 Ανάλυση της Απόδοσης

Αυτή η ενότητα αναφέρεται στην ανάλυση των επιδόσεων των SC συστημάτων με βάση τον PN και των συστημάτων πολλαπλών φορέων (όπως τα συστήματα OFDM). Θεωρείται ένα SC σύστημα με δέκτη PLL με παρεμβολή συνεχούς κύματος (continuous wave interference) σε κανάλι προσθετικού λευκού γκαουσιανού θορύβου (AWGN – Additive White Gaussian Noise). Λαμβάνοντας υπόψη τον λόγο της παρεμβολής προς την απαιτούμενη ισχύ σήματος και το SNR βρόχου, υπολογίζεται η συνάρτηση πυκνότητας πιθανότητας (PDF – Probability Density Function) του σφάλματος φάσης. Αποδεικνύεται ότι η διακύμανση του σφάλματος φάσης του βρόχου θα αυξηθεί παρουσία ενός σήματος παρεμβολής. Έχουν εξεταστεί επίσης οι επιπτώσεις των φασματικών ιδιοτήτων του PN στις επιδόσεις αποκωδικοποίησης, ιδίως στο BER, σε συνεκτικά ψηφιακά συστήματα, σε δυαδικά συστήματα με μεταλλαγή μετατόπισης φάσης (BPSK – Binary Phase-Shift-Key), σε μη συνεκτικά ψηφιακά συστήματα και σε συστήματα με διαμόρφωση μετατόπισης συχνότητας (FSK – Frequency-Shift Keying). Με βάση τα παραπάνω αποδεικνύεται ότι οι φέρουσες στην υψηλή ζώνη λειτουργίας θα παρουσιάσουν μεγαλύτερο βαθμό απώλειας επιδόσεων του συστήματος PN. Επιπλέον, μελετάται η πιθανότητα σφάλματος bit (BEP – Bit Error Probability) του M-QAM (M-Quadrature Amplitude Modulation) με PN σε κανάλια AWGN και κανάλια επίπεδων διαλείψεων. Το κατώτατο όριο σφάλματος bit (BEF – Bit Error Floor) προκύπτει χρησιμοποιώντας έναν ταλαντωτή PLL. Καταδεικνύεται πως η επίδραση του PN στην πιθανότητα σφάλματος γίνεται κυρίαρχη για υψηλό SNR εισόδου.

Επιπλέον εξετάζονται [14] – [16] οι επιπτώσεις του PN στην πολλαπλή πρόσβαση με διαίρεση κώδικα πολλαπλών φερουσών (CDMA – Code-Division Multiple Access). Το CDMA πολλαπλών φερουσών συνδυάζει το CDMA και πολλαπλούς φορείς όπως η OFDM, το οποίο επιτρέπει την ταυτόχρονη χρήση πολλών χρηστών στην ίδια περιοχή συχνοτήτων. Χρησιμοποιώντας κώδικα διασποράς στο πεδίο της συχνότητας, κατανέμει τη ροή δεδομένων σε πολλούς υποφορείς. Υπολογίζεται η πιθανότητα σφάλματος θεωρώντας κατερχόμενη ζεύξη σε κυψελωτό σύστημα και ένας ταλαντωτής ελεύθερης λειτουργίας. Κατά την αύξηση των αριθμών των τόνων/φερόντων, ο αντίκτυπος του PN γίνεται όλο και πιο ισχυρός αναλογικά. Επιπλέον, εξετάζεται ο αντίκτυπος του PN με έναν ταλαντωτή PLL, ο οποίος οδηγεί σε μείωση της απόδοσης SNR. Επίσης, διερευνώνται οι επιπτώσεις του PN σε CDMA πολλαπλών φερουσών. Λαμβάνεται υπόψη ένας πραγματικός ταλαντωτής PLL και η συνεκτική ανίχνευση με διαμόρφωση BPSK. Προκύπτουν ICI και το ανώτερο όριο της διακύμανσης PN σε έναν υποφορέα. Επίσης, εξαιτίας του PN, μειώνεται αρκετά η απόδοση του συστήματος και ειδικά αυξάνεται το BER.

Μια κυματομορφή πολλαπλών φορέων όπως το OFDM παρουσιάζει μεγάλη ευαισθησία στον PN ταλαντωτή. Σε αρκετές έρευνες εκτιμάται το BER ενός συστήματος OFDM με PN και προκύπτουν ακριβείς τύποι πιθανότητας σφάλματος. Θεωρείται ένας ταλαντωτής ελεύθερης λειτουργίας που προσομοιώνει τον PN ως διαδικασία Wiener. Η απόδοση του BER μειώνεται σημαντικά από τον PN και η υποβάθμιση επιδεινώνεται όσο αυξάνεται ο αριθμός των υποφορέων. Επιπλέον, ο PN επιδεινώνει το SNR στα συστήματα OFDM σε σχέση με τα συστήματα SC. Η κοινή περιστροφή φάσης και η ICI ή η απώλεια ορθογωνιότητας είναι οι όροι σφάλματος που επιφέρει η PN στα συστήματα OFDM. Σε πολλές έρευνες έχει επίσης εκτιμηθεί η διακύμανση κάθε όρου σφάλματος για έναν ταλαντωτή ελεύθερης λειτουργίας και έχει εξεταστεί η στατιστική συμπεριφορά των όρων σφάλματος.

Επίσης, γίνεται αριθμητική ανάλυση για να προσδιοριστεί το πόσο επηρεάζονται το BER και η χωρητικότητα ενός συστήματος OFDM από μη γραμμικότητες του πομπού, ο PN, το σφάλμα εκτίμησης καναλιού και τα κανάλια επιλεκτικής συχνότητας. Η χωρητικότητα, ωστόσο, δεν υπολογίζεται σε κλειστή μορφή και απαιτεί αριθμητική εκτίμηση. Ως εκ τούτου, υπάρχουν άλλες έρευνες που διερευνούν την επίδραση του PN στη χωρητικότητα και το SINR των συστημάτων OFDM. Για την κατανομή της ICI, αναπτύσσουν μια στατιστική διατύπωση κλειστής μορφής. Πρέπει να σημειωθεί τα αποτελέσματα των διάφορων ερευνών αφορούν μόνο τον Wiener PN κατά την μελέτη του ταλαντωτή ελεύθερης λειτουργίας.

Άλλες έρευνες [17] – [19] εξετάζουν τον ρυθμό του συστήματος OFDM με την ύπαρξη πρακτικών ταλαντωτών PLL. Επιπλέον, χρησιμοποιούνται συσχετισμένες τυχαίες μεταβλητές γάμμα για τη δημιουργία της κατανομής ισχύος ICI. η μεγιστοποίηση του ρυθμού για δεδομένο μήκος κυκλικού προθέματος, SNR και εύρος ζώνης προσδιορίζεται χρησιμοποιώντας τον ιδανικό αριθμό υποφορέων. Επιπρόσθετα, ενώ υφίσταται PN, IQ ανισορροπία και κανάλι Rayleigh με εξασθένηση μπλοκ, εξετάζεται αναλυτικά η αμοιβαία πληροφορία μεταξύ του πομπού και του δέκτη σε έναν τυχαίο OFDM υποφορέα. Το ποσό της αβεβαιότητας σχετικά με μια τυχαία μεταβλητή που μειώνεται όταν παρατηρείται η τιμή μιας άλλης τυχαίας μεταβλητής, και αντίστροφα, αναφέρεται ως αμοιβαία πληροφορία. Η μέση αμοιβαία πληροφορία εκφράζεται ως αναπαράσταση σειράς υπό πλήρως συσχετισμένους και ασυσχέτιστους κατοπτρικούς υποφορείς. Ακόμη και αν το SNR πλησιάζει στο άπειρο, η αμοιβαία πληροφορία φτάνει σε κορεσμό λόγω των αλλοιώσεων. Επιπλέον, υπολογίζεται ο ακριβής λόγος σήματος προς παρεμβολή (SIR – Signal-to-Interference Ratio) του συστήματος OFDM υπό τις συνδυασμένες επιδράσεις των PN, CFO και χρονο-επιλεκτικών καναλιών, όπου ο χρόνος συνοχής του καναλιού είναι μικρότερος από την περίοδο συμβόλου. Όταν γίνεται συνδυασμός επιδράσεων των PN, CFO και καναλιών επιλεκτικών ως προς τον χρόνο όπου ο χρόνος συνοχής του καναλιού είναι μικρότερος από την περίοδο συμβόλου, γίνεται προσδιορισμός του ακριβή SIR του συστήματος OFDM. Καθώς οι αλλοιώσεις επιδεινώνονται, το SIR γίνεται μικρότερο.

Επίσης εξετάζονται [20] οι επιδράσεις του PN στη διανυσματική OFDM (V-OFDM – Vector-OFDM) για συστήματα με μία μόνο κεραία εκπομπής. Σε δύο ειδικές περιπτώσεις V-OFDM, οι οποίες είναι η OFDM και η SC ισοστάθμιση στο πεδίο της συχνότητας (SC-FDE), γίνεται τροποποίηση του αριθμού και του μήκους των διανυσματικών μπλοκ. Θα πρέπει να σημειωθεί ότι τα συστήματα LTE χρησιμοποιούν SC-FDE/SC-FDMA (FDMA – Frequency Division Multiple Access) στην άνω ζεύξη για να μειώσουν το κόστος και OFDM/OFDMA (OFDMA – Orthogonal Frequency Division Multiple Access) στην κάτω ζεύξη για να επιτύχουν υψηλούς ρυθμούς δεδομένων. Το συνηθισμένο σφάλμα φάσης διανυσματικών μπλοκ και η παρεμβολή μεταξύ διανυσματικών μπλοκ φέροντος επηρεάζουν το V-OFDM. Μια εξίσωση κλειστής μορφής για το SINR της V-OFDM αναπτύσσεται και αποδεικνύεται περαιτέρω ότι το SINR προσεγγίζει τελικά ένα κατώτατο όριο για σημαντικές διακυμάνσεις PN. Αποδεικνύεται επίσης ότι, για ένα συγκεκριμένο επίπεδο PN, η V-OFDM με PN υπερέχει της OFDM χωρίς PN. [3]

3.2.2 Εκτίμηση και Αντιστάθμιση

Οι τεχνικές εκτίμησης και αντιστάθμισης για τη μείωση των φαινομένων PN έχουν ως ισχυρό κίνητρο τις αρνητικές επιδράσεις του PN στις ασύρματες επιδόσεις. Οι τρέχοντες εκτιμητές μπορούν να κατηγοριοποιηθούν ως τυφλές ή υποβοηθούμενες από πιλότους pilot μέθοδοι. Οι

εκτιμητές PN με τη βοήθεια pilot θυσιάζουν την αποδοτικότητα του εύρους ζώνης υπέρ καλά σχεδιασμένων συμβόλων εκπαίδευσης ή pilot συμβόλων στα δεδομένα. Στην πραγματικότητα, η μέθοδος αυτή χρησιμοποιεί τις παρελθοντικές πληροφορίες του δέκτη για να προσεγγίσει τον PN. Στις τυφλές προσεγγίσεις, όμως, ο δέκτης δεν έχει πρόσβαση σε παρελθοντικές γνώσεις. Αυτές οι μέθοδοι αυξάνουν την αποδοτικότητα του φάσματος εξαλείφοντας την ανάγκη για πολλές μεταδόσεις pilot, οι οποίες διαφορετικά θα χρειαζόνταν μεγάλο αριθμό συμβόλων για να λειτουργήσουν ικανοποιητικά.

Για να αντιμετωπιστούν οι αρνητικές επιπτώσεις του PN, έχουν ερευνηθεί θέματα εκτίμησης και ακύρωσης του PN σε συστήματα με ένα φέρον. Εξετάζεται [21], [22] η ανάκτηση φέροντος με τη βοήθεια pilot για συστήματα SC σε κανάλια AWGN παρουσία PN. Θεωρείται ότι το εισερχόμενο φέρον επηρεάζεται από τον PN, ο οποίος παράγεται από έναν ταλαντωτή ελεύθερης λειτουργίας. Επιπλέον, προκειμένου να εκτιμηθεί ο PN με βάση μια σειρά ομοιόμορφα διατεταγμένων pilot συμβόλων, προτείνεται ένα βέλτιστο φίλτρο Wiener. Μειώνοντας το MSE μεταξύ της φάσης του φέροντος και της ανακτημένης φάσης, προσδιορίζεται το βέλτιστο αυτό φίλτρο. Προτείνεται επίσης μια στρατηγική εκτίμησης και αντιστάθμισης PN για κωδικοποιημένα συστήματα μετάδοσης M-QAM με χαμηλής πυκνότητας έλεγχο ισοτιμίας (LDPC – low density parity check) κωδικοποίηση σε κανάλια AWGN και χρησιμοποιούνται ισαπέχοντα γνωστά pilot σύμβολα. Αυτή η μέθοδος υπολογίζει με παρεμβολή τα σφάλματα φάσης στις άλλες θέσεις χρησιμοποιώντας ένα φίλτρο Wiener, αφού τα εκτιμήσει στα σημεία που υπάρχουν pilots.

Καλύπτεται [23], [24] επίσης μια προσέγγιση εκτίμησης PN με τη βοήθεια pilot για ταλαντωτές ελεύθερης λειτουργίας με έγχρωμες πηγές θορύβου όπου χρησιμοποιούνται pilot σύμβολα θωρώντας ένα σύστημα SC και κανάλια AWGN. Προτείνεται ένας εκτιμητής PN που βασίζεται στην εκτίμηση μέγιστης εκ των υστέρων πιθανότητας (MAP – Maximum A Posteriori). Για την απλούστευση των πραγμάτων, προτείνεται ένας τροποποιημένος εξομαλυντής Kalman με soft-input (το soft-input αναφέρεται στο γεγονός ότι τα εισερχόμενα δεδομένα μπορούν να πάρουν τιμές διαφορετικές από 0 ή 1, προκειμένου να δηλωθεί η αξιοπιστία της κάθε εκτίμησης), ο οποίος αποδίδει σχεδόν εξίσου καλά με τον προηγούμενο εκτιμητή και έχει μια αυτοπαλινδρόμη (AutoRegressive – AR) προσέγγιση χαμηλής τάξης του έγχρωμου PN. Παρουσιάζεται [24] ένας τυφλός επαναληπτικός αλγόριθμος που χρησιμοποιεί τη χαμηλοπερατή φύση του φαινομένου PN χωρίς να έχει προηγούμενη γνώση του ακριβούς μοντέλου PN για κοινή αποκωδικοποίηση, εκτίμηση PN και αντιστάθμιση σε συστήματα SC-FDMA. Υπάρχουν ταλαντωτές ελεύθερης λειτουργίας τόσο στην πλευρά του πομπού όσο και στην πλευρά του δέκτη. Επιπλέον, μελετώνται το συνδυασμένο PN εκπομπής-λήψης και το κανονικοποιημένο MSE υπό CFO. Το προτεινόμενο σύστημα είναι ανθεκτικό στην ανακριβή εκτίμηση του καναλιού.

Από την άλλη, υπάρχουν και τα συστήματα Single-User OFDM. Προκειμένου να μελετηθούν, χωρίζονται σε 3 κατηγορίες όπως (α) εκτίμηση και αντιστάθμιση με την βοήθεια pilot, (β) τυφλή εκτίμηση και αντιστάθμιση και (γ) από κοινού εκτίμηση και αντιστάθμιση καναλιού και PN.

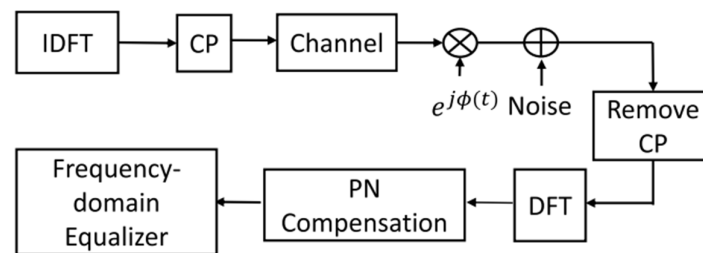
Για την πρώτη κατηγορία, διερευνάται πώς μπορεί να μειωθεί μόνο το κοινό σφάλμα φάσης για συστήματα OFDM σε κανάλια επιλεκτικά ως προς την συχνότητα. Ο όρος του σφάλματος κοινής φάσης εκτιμάται με μια τεχνική ελαχίστων τετραγώνων (LS – Least-Squares) χρησιμοποιώντας pilot subcarriers και μηδενικά δείγματα, τα οποία στη συνέχεια διορθώνονται με την απο-περιστροφή του αστερισμού. Ένας ισοσταθμιστής πεπερασμένης κρουστικής απόκρισης

διορθώνει επίσης τον PN. Χρησιμοποιώντας διάσπαρτους pilots και την μέθοδο LS, υπολογίζονται οι συντελεστές του φίλτρου. Ωστόσο, επειδή το μήκος του φίλτρου περιορίζεται από τον αριθμό των τόνων του πιλότου, δεν μπορεί να διορθωθεί πλήρως το ICI από γειτονικούς υποφορείς. Χρησιμοποιείται μια ημιτονοειδής κυματομορφή για να παραμετροποιηθεί η διαδικασία του PN και η τεχνική LS χρησιμοποιείται για την εκτίμηση των παραμέτρων. Ωστόσο, ένα ημιτονοειδές μπορεί να μην πλησιάζει με ακρίβεια τον PN. Η αναπαράσταση Karhunen-Loève της διαδικασίας του PN χρησιμοποιείται για την ενίσχυση των αποτελεσμάτων και ο προκύπτων πίνακας συνδιακύμανσης χρησιμοποιείται ως στοιχείο βάσης. Η καθοδηγούμενη από τα δεδομένα επιλογή των στοιχείων βάσης για την εκτίμηση LS PN βελτιώνεται ώστε να είναι πιο ακριβής. Τέλος, αποδεικνύεται ότι κάθε σήμα υποφορέων στο πεδίο της συχνότητας μπορεί να εκφραστεί ως το άθροισμα όλων των σημάτων υποφορέων που έχουν σταθμιστεί με ένα διάνυσμα παραμέτρων. Επίσης, για τον προσδιορισμό του διανύσματος στάθμισης διερευνήθηκαν οι τεχνικές της μέγιστης πιθανοφάνειας (MLikelihood – Maximum Likelihood) και του γραμμικού ελάχιστου μέσου τετραγωνικού σφάλματος (LMMSE – Linear Minimum Mean Square Error). Όμως οι διαδικασίες αντιστροφής πινάκων που απαιτούνται για αυτές τις προσεγγίσεις είναι υπολογιστικά δαπανηρές. Κοντά στη συχνότητα ταλάντωσης, το φάσμα του PN έχει μια χαμηλοπερατή περιοχή με εύρος ζώνης που είναι μικρότερο από την απόσταση των υποφορέων. Επομένως, οι χαμηλοπερατές φασματικές συνιστώσες είναι επαρκείς για την προσομοίωση του PN στην πλειονότητα των πραγματικών σεναρίων.

Προτείνεται [25] – [30] ένας αλγόριθμος μείωσης της ICI. Τα βήματα του προτεινόμενου αλγορίθμου έχουν ως εξής: (1) πραγματοποίηση από-περιστροφής του αστερισμού μετά την εκτίμηση του κοινού σφάλματος φάσης με την βοήθεια ενός εκτιμητή LS, (2) λήψη απόφασης για τα μεταδιδόμενα σύμβολα και χρήση των hard-decisions για να εκτιμηθούν οι χαμηλοπερατές φασματικές συνιστώσες χρησιμοποιώντας MMSE και (3) με τη συνέλιξη των υπολογισμένων συντελεστών του διακριτού μετασχηματισμού Fourier (DFT – Discrete Fourier Transform) με τα εισερχόμενα διακριτά σύμβολα, ο PN μειώνεται. Η διάδοση των σφαλμάτων αποτελεί πρόβλημα, δεδομένου ότι η προσέγγιση αυτή απαιτεί ανατροφοδότηση αποφάσεων. Ως αποτέλεσμα, η εκτίμηση και η ποιότητα καταστολής βελτιώνονται με την αύξηση του αριθμού των αξιόπιστων συμβόλων για την εκτίμηση του PN. Ο παραπάνω αλγόριθμος εφαρμόζεται σε επανάληψη για να επιτευχθεί το επιθυμητό αποτέλεσμα. Μετά τη διόρθωση PN, αναδημιουργούν τα μεταδιδόμενα σύμβολα και τα χρησιμοποιούν ξανά για μια επόμενη εκτίμηση και διόρθωση PN. Εξετάζονται τόσο οι ταλαντωτές ελεύθερης λειτουργίας όσο και οι ταλαντωτές PLL.

Η προσέγγιση εκτίμησης του PN [25], [31], [32] δεν είναι κατάλληλη στα όρια των συμβόλων. Προκειμένου να βελτιωθεί η εκτίμηση των ορίων, παρέχονται δύο στρατηγικές βασισμένες στη γραμμική παρεμβολή. Για να καλυτερεύσει η εκτίμηση σφάλματος κοινής φάσης με τη βοήθεια πιλότου, η πρώτη παρεμβάλλει την εκτίμηση του PN στα γειτονικά σύμβολα OFDM. Η δεύτερη χρησιμοποιείται για τη μείωση της ανακρίβειας στα όρια κάθε συμβόλου OFDM, ενισχύοντας έτσι την επαναληπτική προσέγγιση εκτίμησης της ICI. Όμως, λόγω των διαδικασιών αντιστροφής πινάκων και των συσχετίσεων μεταξύ των τιμών DFT του PN, οι προσεγγίσεις αυτές είναι αρκετά περίπλοκες. Λόγω της μεγάλης διάρκειας του κυκλικού προθέματος και του τεράστιου μεγέθους του αστερισμού, μέσα από έρευνες βελτιώνεται η διαδικασία για τη μείωση του ποσοστού σφάλματος ανίχνευσης.

Αντιθέτως, άλλες έρευνες αναπτύσσουν έναν επαναληπτικό αλγόριθμο [33], [34]. Διαιρείται το λαμβανόμενο σύμβολο OFDM σε υπο-μπλοκ στο πεδίο του χρόνου και υπολογίζεται ο μέσος όρος του PN σε κάθε υπο-μπλοκ. Στην Εικόνα 3-4 απεικονίζεται το μοντέλο του συστήματος. Η πολυπλοκότητα μειώνεται μέσω της χρήσης θεμελιωδών δομικών στοιχείων στον αλγόριθμο. Υπολογίζεται επίσης το SINR μετά την αντιστάθμιση του PN. Επιπλέον, για την εκτίμηση του PN, αναπτύσσεται ένας κατάλογος (codebook) που αντιπροσωπεύει ένα σύνολο προβολών. Η επιλογή της προβολή επιτυγχάνεται όταν γίνεται μείωση της ευκλείδειας απόστασης μεταξύ των γνωστών pilot συμβόλων και του αστερισμού των λαμβανόμενων συμβόλων στους pilot υποφορείς. Ο αριθμός των codebooks και η διάσπαση της περιοχής κβαντισμού επηρεάζουν την ακρίβεια αυτής της μεθόδου, η οποία ωστόσο μείωσε την πολυπλοκότητα της εκτίμησης του PN.



Εικόνα 3-4: Ένα σύστημα OFDM με αντιστάθμιση PN και ισοσταθμιστή στο πεδίο της συχνότητας. Το $e^{j\phi(t)}$ αποτελεί το σχήμα του φάσματος του PN. [3]

Μία άλλη μέθοδος εκτίμησης PN χρησιμοποιεί ανατροφοδότηση απόφασης η οποία χρησιμοποιεί τη γεωμετρική δομή που συνδέεται με τις φασματικές συνιστώσες του μιγαδικού εκθετικού όρου (μιγαδικό ημίτονο) της διαδικασίας του PN. Αυτή η γεωμετρία διατυπώνεται ως ένα σύστημα τετραγωνικών μη κυρτών εξισώσεων που περιλαμβάνουν πίνακες μετάθεσης. Συνεπώς, περιγράφεται μια προσέγγιση εκτίμησης PN με βάση πιλότους με διασπορά χωρίς βρόχο ανατροφοδότησης απόφασης. Χρησιμοποιείται η φασματική γεωμετρία του PN και ένα μοντέλο μείωσης της διαστατικότητας. Είναι δυνατή η εκτίμηση του απαραίτητου φασματικού διανύσματος PN με τη χρήση της τεχνικής LS και των διασκορπισμένων pilot υποφορέων. Αποδεικνύεται ότι υπάρχουν λάθη εκτίμησης πλάτους και φάσης αν θεωρηθεί πρόβλημα βελτιστοποίησης χωρίς περιορισμούς (constraints) κατά την εκτίμηση του PN. Ένας περιορισμός της γεωμετρίας PN εφαρμόζεται στον εκτιμητή LS για την μείωση του σφάλματος πλάτους. Αυτή η προσέγγιση βελτιώνει το BER και την απόδοση εκτίμησης.

Για την δεύτερη κατηγορία (τυφλή εκτίμηση και αντιστάθμιση), αυτές οι τεχνικές έχουν σχεδιαστεί για να μειώνουν την πιθανότητα μείωσης της αποδοτικότητας του εύρους ζώνης όταν χρησιμοποιούνται pilot σύμβολα για την εκτίμηση του PN. Προτείνεται μια τυφλή εκτίμηση σφάλματος κοινής φάσης για συστήματα OFDM με τη χρήση ενός εκτιμητή $ML_{likelihood}$. Ωστόσο, το υπολειπόμενο σφάλμα που σχετίζεται με την ICI θα πρέπει να μειωθεί επειδή δεν είναι ασήμαντο. Έτσι, παρουσιάζεται ένας επαναληπτικός υπο συνθήκη αλγόριθμος για από κοινού ανίχνευση δεδομένων και ακύρωση του PN που βασίζεται στην πιθανολογική τεχνική της μεταβλητής συμπερασματολογίας (βήματα στον συλλογισμό που κινούνται από τις προϋποθέσεις στις λογικές συνέπειες). Με βάση τη συνάρτηση κόστους MMSE και περιορισμούς που εισάγονται από τη διαμόρφωση των συμβόλων, προσδιορίζεται το σύμβολο και ακυρώνεται ο PN. Η προτεινόμενη

προσέγγιση, ωστόσο, έχει σημαντικές απαιτήσεις υπολογιστικής πολυπλοκότητας και έχει υψηλό ποσοστό σφάλματος απόφασης. Έτσι προτείνεται μια προσέγγιση τυφλής εκτίμησης. Ένα ενιαίο λαμβανόμενο σύμβολο OFDM χωρίζεται σε υπο-μπλοκ και ο PN κάθε υπο-μπλοκ εκτιμάται ως ο μέσος όρος του χρόνου του. Η ICI που προκύπτει από τον PN μειώνεται ελαχιστοποιώντας τη διακύμανση του PN. Στη συνέχεια, χρησιμοποιείται μια τεχνική που κατευθύνεται από την απόφαση για την εκτίμηση και τη διόρθωση του σφάλματος κοινής φάσης. Αυτή όμως η προσέγγιση είναι αποτελεσματική μόνο για αλφάβητα σηματοδότησης με σταθερό συντελεστή. Οι τυφλοί εκτιμητές βελτιώνουν την αποδοτικότητα του εύρους ζώνης και είναι στατιστικά ιδανικοί, αλλά απαιτούν αρκετή υπολογιστική ισχύ και μπορεί να μην είναι κατάλληλοι για εφαρμογές ευαίσθητες στην καθυστέρηση.

Για την τρίτη κατηγορία (από κοινού εκτίμηση και αντιστάθμιση καναλιού και PN), προτείνεται μία μέθοδος εκτίμησης καναλιού για την από κοινού εκτίμηση καναλιού που αναπτύσσει αποκωδικοποίηση soft-decision. Χρησιμοποιείται ο αλγόριθμος μεγιστοποίησης προσδοκιών (EM – Expectation Maximization), ο οποίος χρησιμοποιεί pilot υποφορείς, για να χειριστεί τη συνδυασμένη εκτίμηση καναλιού και την μείωση του PN. Ωστόσο, η ICI μοντελοποιείται ως AWGN. Ως αποτέλεσμα, προτείνεται ένας ιδανικός συνδυασμένος εκτιμητής καναλιού, CFO και PN μέσω της μεγιστοποίησης της συνάρτησης πιθανοφάνειας. Χρησιμοποιώντας την προηγούμενη γνώση των στατιστικών PN και της ακολουθίας εκπαίδευσης, αναπτύσσεται ένας εκτιμητής MAP. Ωστόσο, πριν από την εκτίμηση του καναλιού στο δέκτη, ο εκτιμητής χρειάζεται πληροφορίες σχετικά με το μήκος του καναλιού, οι οποίες δεν είναι διαθέσιμες. Για την επίλυση αυτού του ζητήματος και την εκτίμηση της συνάρτησης μεταφοράς καναλιού στο πεδίο της συχνότητας, αυτή η τεχνική δεν χρειάζεται να γνωρίζει εκ των προτέρων το μήκος του καναλιού, σε αντίθεση με τον υπολογισμό της κρουστικής απόκρισης του καναλιού στο πεδίο του χρόνου. Αν και υπολογιστικά απαιτητικές, παρουσιάζουν και οι δύο μείωση της απόδοσης με διαμορφώσεις υψηλότερης τάξης.

Από την άλλη πλευρά, μοντελοποιώντας τη διαδικασία PN στο σύμβολο OFDM μέσω δυναμοσειρών, προτείνεται μια τεχνική για την ταυτόχρονη εκτίμηση του καναλιού και του κοινού σφάλματος φάσης. Επιπλέον, προτείνονται offline και online εκτιμητές Monte-Carlo χωρίς προηγούμενη γνώση του PN ή της ισχύος του γκαουσιανού θορύβου. Παρουσιάζεται μια στοχαστική τεχνική EM για την offline εκτίμηση που εκτιμά την ισχύ των άγνωστων PN, CFO, καναλιού και γκαουσιανού θορύβου ταυτόχρονα. Με βάση τους διαδοχικούς αλγορίθμους Monte-Carlo και μηχανικής μάθησης (MLearning – Machine Learning), παρέχεται μια συνδυασμένη τεχνική εκτίμησης του καναλιού, του CFO, του εύρους ζώνης του PN και της διακύμανσης του θορύβου του καναλιού. Η προσέγγιση Monte-Carlo, ωστόσο, προκαλεί στις προτεινόμενες προσεγγίσεις μεγαλύτερη πολυπλοκότητα εκτίμησης και εγγενή ανακρίβεια. Επιπλέον, προτείνεται μια μέθοδος δύο σταδίων για συνδυασμένη εκτίμηση καναλιού και PN. Χρησιμοποιώντας μεθόδους παρεμβολής (interpolation), το πρώτο στάδιο χρησιμοποιεί pilot σύμβολα τύπου μπλοκ για την ταυτόχρονη εκτίμηση των συντελεστών PN και καναλιού στο πεδίο του χρόνου. Στο δεύτερο, οι συνιστώσες PN και τα σύμβολα δεδομένων εκτιμώνται χρησιμοποιώντας ένα μείγμα συμβόλων δεδομένων και pilot συμβόλων.

Παρέχεται [35] – [37] μια συνδυασμένη στρατηγική ισοστάθμισης καναλιού και αντιστάθμισης PN με βάση την ανατροφοδότηση αποφάσεων. Δημιουργείται ένας ανάλογος πίνακας καναλιού συνδυάζοντας τον PN και το κανάλι διαλείψεων. Ωστόσο, η μέθοδος αυτή απαιτεί αρκετές

πολύπλοκες πράξεις αντιστροφής πινάκων. Στην πραγματικότητα, παρατηρώντας τυχαίες διακυμάνσεις φάσης, η μη επαναληπτική παρεμβολή μπορεί να εκτιμήσει τον PN σε συστήματα OFDM βασισμένα σε πακέτα. Αποδεικνύεται πώς μπορεί να μεγιστοποιηθεί μια τετραγωνική μορφή (υπό περιορισμούς) για την εκτίμηση του PN χωρίς την ανάγκη πληροφοριών καναλιού. Ο υπολογιζόμενος PN χρησιμοποιείται από τον εκτιμητή LS για τον εντοπισμό του καναλιού. Οι πιλότοι (pilots) πρέπει να χρησιμοποιούνται σε ολόκληρο το σύμβολο OFDM για την παρακολούθηση του PN, γεγονός που μειώνει τη φασματική απόδοση. Επιπλέον, οι συνδυασμένες εκτιμήσεις καναλιού, CFO και PN μπορούν να εκτιμηθούν χρησιμοποιώντας την προσέγγιση EM. Η προσέγγιση αυτή αποτελείται από δύο βήματα: (1) παρακολούθηση PN με χρήση ενός εκτεταμένου εκτιμητή με βάση το φίλτρο Kalman στο σύμβολο εκπαίδευσης OFDM και (2) εκτίμηση του καναλιού και της CFO με μείωση της συνάρτησης πιθανοφάνειας. Επιπλέον, αναπτύσσεται ένα υβριδικό κατώτερο όριο Cramér-Rao (CRLB - Cramér-Rao Lower Bound) για το ζήτημα της από κοινού εκτίμησης. Ο προτεινόμενος αλγόριθμος βελτιώνει τόσο την απόδοση του μη κωδικοποιημένου όσο και του κωδικοποιημένου BER, ενώ παράλληλα είναι υπολογιστικά αποδοτικός.

Τέλος, μελετώνται τα συστήματα Multi-User OFDMA στα οποία οι υποφορείς χωρίζονται σε ομάδες, γνωστές ως υποκανάλια, και ανατίθενται σε πολλούς χρήστες για ταυτόχρονη μετάδοση. Η παρεμβολή πολλαπλών χρηστών (MUI – Multi-User Interference) δεν υφίσταται λόγω της ορθογωνιότητας των υποφορέων, ακόμη και αν τα σήματα πολλών χρηστών μπορεί να επικαλύπτονται στο πεδίο της συχνότητας. Τα συστήματα OFDMA είναι ευάλωτα στον PN, το οποίο εξαιλεί την ορθογωνιότητα των υποφορέων και οδηγεί σε ICI μεταξύ των υποφορέων και MUI μεταξύ των χρηστών, όπως ακριβώς συμβαίνει και στα συστήματα OFDM. Επομένως, τόσο στην άνω όσο και στην κάτω ζεύξη, απαιτείται εκτίμηση και αντιστάθμιση PN. Οι υπάρχοντες αλγόριθμοι OFDM ενός χρήστη μπορούν να εκτιμήσουν και να διορθώσουν μόνο τον PN κάθε χρήστη, τον οποίο αντιμετωπίζουν στην κάτω ζεύξη. Η κατάσταση είναι διαφορετική για την άνω ζεύξη OFDMA, όπου κάθε χρήστης έχει μοναδικό PN και ο σταθμός βάσης λαμβάνει σήμα με πολλές τιμές PN. Ως εκ τούτου, η εκτίμηση και η ακύρωση του PN στην άνω ζεύξη OFDMA είναι ένα δύσκολο έργο.

Τα συστήματα OFDMA χρησιμοποιούν τρία μοντέλα ανάθεσης υποφορέων: (1) γενικευμένο μοντέλο όπου ανάλογα με την ποιότητα υπηρεσίας (QoS – Quality of Service) του χρήστη και τις συνθήκες του καναλιού, κάθε χρήστης μπορεί να επιλέξει τους υποφορείς, (2) μοντέλο με βάση την υπο-ζώνη όπου κάθε χρήστης έχει πρόσβαση σε μία ή περισσότερες από τις μικρές και συνεχείς υποζώνες που συνθέτουν το εύρος ζώνης, και (3) μοντέλο με περίπλεξη (interleaving) όπου σε όλο το εύρος ζώνης, οι υποφορείς που αντιστοιχούν σε κάθε χρήστη περιπλέκονται. Το μοντέλο με περιπλεκόμενες ζώνες, σε αντίθεση με το παράδειγμα των υποζωνών, προσφέρει πλήρη διαφορισμότητα καναλιού και ενισχύει τη χωρητικότητα σε κανάλια διαλείψεων επιλεκτικά ως προς την συχνότητα. Σε σύγκριση με τα άλλα μοντέλα, το γενικευμένο μοντέλο προσφέρει μεγαλύτερη ευελιξία και επιτρέπει τη δυναμική κατανομή πόρων. Λόγω της επιρροής τους στη MUI, τα μοντέλα ανάθεσης υποφορέων έχουν αντίκτυπο στη διαδικασία μετριάσμου PN.

Προτείνονται [38], [39] δύο τεχνικές εκτίμησης PN με τη βοήθεια πιλότου για την άνω ζεύξη OFDM υπό μοντέλα ανάθεσης υποζώνης και περιπλεκόμενων υποφορέων. Χρησιμοποιούνται τα στατιστικά στοιχεία δεύτερης τάξης των όρων ICI για να αναπτυχθεί μια τεχνική εκτίμησης $ML_{likelihood}$. Επιπλέον, παρά την επιδείνωση της απόδοσης, δημιουργείται επίσης ένας εκτιμητής LS

με μικρότερη υπολογιστική πολυπλοκότητα. Χρησιμοποιώντας ένα μικρό αριθμό πιλότων ανά χρήστη και το μοντέλο ταλαντωτή ελεύθερης λειτουργίας, και οι δύο εκτιμητές διορθώνουν το κοινό σφάλμα φάσης. Επίσης, εξετάζεται η εκτίμηση και η μείωση της φασματικής διασποράς με την βοήθεια πιλότου που προκαλείται από τον PN στις άνω ζεύξεις OFDMA με τη βοήθεια του μοντέλου ταλαντωτή ελεύθερης λειτουργίας. Το φαινόμενο PN του πομπού και οι παρεμβολές είναι προβλήματα που αντιμετωπίζει κάθε χρήστης OFDMA. Αυτή η παρεμβολή προκαλείται από την φασματική διασπορά των υποφορέων κάθε χρήστη σε εκείνους των άλλων χρηστών. Ο προτεινόμενος αλγόριθμος υπολογίζει την επίδραση του καναλιού και το κοινό σφάλμα φάσης πριν από την ανίχνευση των συμβόλων δεδομένων. Τα αναγνωρισμένα σύμβολα χρησιμοποιούνται για τον προσδιορισμό της φασματικής διασποράς.

Συνοψίζοντας, οι αντισταθμιστές PN με τη βοήθεια πιλότου σε όλα τα εξεταζόμενα συστήματα βασίζονται τόσο σε μεροληπτικές όσο και σε αμερόληπτες μεθόδους, όπως η LS και η MMSE. Για τις πρώτες, όπως ο θόρυβος του καναλιού και ο θόρυβος φάσης, δεν απαιτείται προηγούμενη γνώση των στατιστικών των άγνωστων παραμέτρων. Οι δεύτερες, ωστόσο, απαιτούν τη διακύμανση του θορύβου και στατιστικά στοιχεία δεύτερης τάξης. Επιπλέον, το υπολογιστικό κόστος των εκτιμητών με τη βοήθεια πιλότου αυξάνεται από το γεγονός ότι συχνά χρειάζονται αρκετές επαναλήψεις για να συγκλίνουν. Επίσης, αρκετοί αλγόριθμοι $ML_{likelihood}$ και MMSE απαιτούν πολύπλοκες διαδικασίες αντιστροφής πινάκων. Οι τυφλοί εκτιμητές, από την άλλη πλευρά, βελτιώνουν την αποδοτικότητα του εύρους ζώνης, καθώς πραγματοποιούν την εκτίμηση χωρίς την ανάγκη pilot συμβόλων. Ωστόσο, για βέλτιστη απόδοση, χρειάζονται συχνά μέσο όρο σε πολλαπλά σύμβολα δεδομένων. Επιπρόσθετα, σε σύγκριση με τους εκτιμητές με τη βοήθεια πιλότου, έχουν κακή σύγκλιση, υψηλή πολυπλοκότητα και συγκριτικά χαμηλή απόδοση. [3]

4

Radio Frequency Fingerprinting

Για να αυξηθεί η ασφάλεια και η ιδιωτικότητα της ασύρματης επικοινωνίας, το δακτυλικό αποτύπωμα ραδιοσυχνοτήτων αποσκοπεί στη δημιουργία ενός μοναδικού δακτυλικού αποτυπώματος (RF Fingerprinting – Radio Frequency Fingerprinting) για μια ασύρματη συσκευή, το οποίο μπορεί να χρησιμοποιηθεί ως αναγνώριση, παρόμοια με τον τρόπο λειτουργίας ενός βιολογικού δακτυλικού αποτυπώματος. Αυτό έρχεται σε αντίθεση με τις καθιερωμένες αλγοριθμικές μεθόδους ασφάλειας μετάδοσης σε επίπεδο bit. Το RF Fingerprinting, ένα νέο παράδειγμα για τη διασφάλιση της αυθεντικότητας της εκπομπής, εξάγει τα μοναδικά χαρακτηριστικά που κρύβονται στα μεταδιδόμενα ηλεκτρομαγνητικά κύματα αλλά και στο κανάλι. Η συμπερίληψη αναλογικών εξαρτημάτων (όπως μετατροπείς ψηφιακού σε αναλογικό, ζωνοπερατά φίλτρα, μίκτες συχνότητας και ενισχυτές ισχύος) στην αλυσίδα ασύρματης μετάδοσης, καθώς και η εγγενής τυχαιότητα στη διαδικασία κατασκευής, συμβάλλουν σημαντικά σε αυτές τις χαρακτηριστικές ιδιότητες. Ένας αριθμός ασύρματων συσκευών που χρησιμοποιούν διάφορα πρότυπα, όπως CRN, το UMTS (Universal Mobile Telecommunications System), Wi-Fi (Wireless-Fidelity), πομποί push-to-talk, Bluetooth και ταυτοποίηση μέσω ραδιοσυχνοτήτων (RFID – Radio-Frequency IDentification), έχουν υποβληθεί σε δοκιμές RF Fingerprinting. Διαπιστώθηκε ότι κάθε εκπομπή έχει ένα ξεχωριστό RF Fingerprint, και αποδείχθηκε επίσης ότι η πιθανότητα δύο εκπομπές να έχουν τις ίδιες ιδιότητες RF είναι σχεδόν μηδενική. Έτσι, προκειμένου να επικυρωθεί η αυθεντικοποίηση μίας συγκεκριμένης εκπομπής και να διασφαλιστεί η μυστικότητα των μεταδιδόμενων δεδομένων, μπορεί να χρησιμοποιηθεί ένα ξεχωριστό RF Fingerprint. Αυτό το κεφάλαιο θα μελετήσει όλες τις πτυχές αυτής της σημαντικής τεχνικής επίτευξης ασφάλειας στις ασύρματες επικοινωνίες. [4]

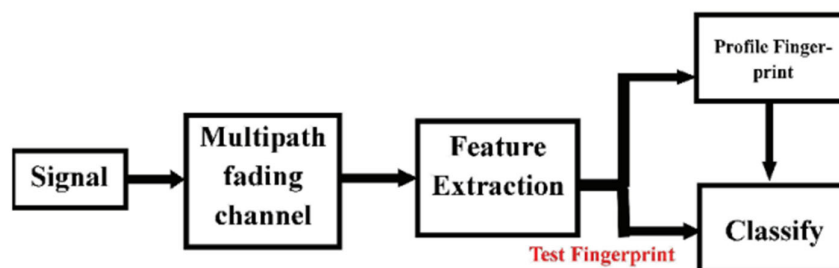
4.1 Επισκόπηση του RF Fingerprinting

Ο ασύρματος εξοπλισμός αναγνωρίζεται συνήθως από συγκεκριμένα RF Fingerprints που παράγονται από τα ασύρματα κυκλώματα. Η επίθεση πλαστοπροσωπίας είναι ένας από τους

σημαντικότερους και πιο επικίνδυνους τύπους επιθέσεων στο ασύρματο δίκτυο. Σε αυτόν τον τύπο επίθεσης, ένας επιτιθέμενος μπορεί να υποδυθεί συσκευές αντιγράφοντας την πλειονότητα των δεδομένων αυθεντικοποίησης, συμπεριλαμβανομένου του κωδικού πρόσβασης και της διεύθυνσης ελέγχου προσπέλασης στο μέσο ή αλλιώς φυσική διεύθυνση (MAC – Media Access Control). Τα ηλεκτρομαγνητικά κύματα που εκπέμπει ο πομπός έχουν ξεχωριστές ιδιότητες που μπορούν να χρησιμοποιηθούν για τη δημιουργία ενός δακτυλικού αποτυπώματος ραδιοσυχνότητας (RFF – Radio-Frequency Fingerprinting).

Η παρούσα διπλωματική εργασία επικεντρώνεται σε συγκεκριμένες μεθόδους επίτευξης αυθεντικοποίησης της εκπομπής χρησιμοποιώντας μοναδικά δακτυλικά αποτυπώματα αξιοποιώντας το φυσικό επίπεδο. Η αυθεντικοποίηση στο φυσικό επίπεδο, συχνά γνωστή ως δακτυλικό αποτύπωμα, αποτελεί μία μέθοδο ελέγχου της γνησιότητας μίας ασύρματης εκπομπής με τον εντοπισμό ιδιαιτεροτήτων που προκύπτουν από ελαττώματα υλικού στο αναλογικό κύκλωμα. Αυτές οι ατέλειες προκαλούνται όταν κατασκευάζεται το κύκλωμα ή το υλικό. Η αυθεντικοποίηση της εκπομπής με την αξιοποίηση του φυσικού επιπέδου έχει χρησιμοποιηθεί για διάφορους λόγους, όπως ο ασφαλής εντοπισμός, ο έλεγχος πρόσβασης, η ανίχνευση κλώνων και η ανίχνευση εισβολών. Το σημαντικότερο πλεονέκτημα της χρήσης ενός φυσικού ελαττώματος του υλικού ως υπογραφή για αυθεντικοποίηση είναι ότι είναι δύσκολο να πλαστογραφηθεί η υπογραφή με τη χρήση άλλων ασύρματων συσκευών. Οι αναμεταδότες HF (High Frequency) RFID, οι αναμεταδότες UHF (Ultra High Frequency) RFID, οι πομποί VHF (Very High Frequency) και οι πομποδέκτες IEEE 802.11 αποτελούν παραδείγματα ασύρματων πλατφορμών για την αναγνώριση εκπομπής με την βοήθεια του φυσικού επιπέδου.

Η λήψη σήματος, η εξαγωγή χαρακτηριστικών και η ταξινόμηση είναι τα τρία βασικά βήματα ενός συστήματος αναγνώρισης ασύρματης συσκευής που βασίζεται στο δακτυλικό αποτύπωμα RF. Απαιτείται η εξαγωγή μοναδικών χαρακτηριστικών από διάφορα τμήματα του σήματος μετά τη σύλληψη του σήματος. Σε σχετικές έρευνες, η εξαγωγή χαρακτηριστικών RF αποτελεί σημαντικό πρόβλημα. Το διαμορφωμένο τμήμα του σήματος χρησιμοποιείται για την εξαγωγή χαρακτηριστικών για την λήψη αποτυπωμάτων RF με βάση το τμήμα του σήματος που βρίσκεται σε σταθερή κατάσταση, το οποίο μπορεί επίσης να εκμεταλλευτεί προηγούμενες πληροφορίες σχετικά με γνωστά σήματα. Αντίθετα, το μεταβατικό (transient) τμήμα των σημάτων (κατά την αφετηρία της εκπομπής, λήψης ή την μετάβαση από μια κατάσταση του συστήματος σε άλλη) εξάγει δακτυλικά αποτυπώματα RF με βάση την μετάβαση. Η σωστή ανίχνευση του μεταβατικού τμήματος σήματος είναι ζωτικής σημασίας για τις τεχνικές που βασίζονται σε μεταβατικό σήμα. [5]



Εικόνα 4-1: Διαδικασία κατηγοριοποίησης δακτυλικών αποτυπωμάτων RF. [4]

4.2 RF Fingerprinting και παραγωγή κλειδιών

Υπάρχουν αρκετές τεχνικές για την αυθεντικοποίηση του εκπεμπόμενου σήματος και τη δημιουργία μυστικών κλειδιών για την ασφάλεια στο φυσικό επίπεδο (PLS – Physical Layer Security). Διάφορες έρευνες επικεντρώνονται στην MLearning, άλλες στην γωνία άφιξης και στην γωνία αναχώρησης, άλλες μόνο στα χαρακτηριστικά του σήματος (συχνότητα, πλάτος, καθυστέρηση κ.α.) και άλλες συνδυάζουν όλους τους παραπάνω τρόπους. Αυτή η ενότητα θα μελετήσει όλους τους πιθανούς τρόπους παραγωγής κλειδιών μέσω του RF Fingerprinting.

4.2.1 Παραγωγή κλειδιών με την χρήση CSI

Η εμφάνιση μεγάλης κλίμακας δικτύων διαδικτύου των πραγμάτων (IoT – Internet of Things), τα οποία έχουν ένα ευρύ φάσμα μη λειτουργικών περιορισμών (ασφάλειας) καθώς και περιορισμούς υπολογιστικής ισχύς, ενεργειακής ισχύος, καθυστερήσεων κ.λπ., έχει προκαλέσει την αναζωπύρωση του ενδιαφέροντος για τις τεχνολογίες PLS για συστήματα έκτης γενιάς (6G). Μία από τις πιο συχνά χρησιμοποιούμενες τεχνικές PLS περιλαμβάνει τον πομπό (Alice) και τον δέκτη (Bob) που χρησιμοποιούν τις υλοποιήσεις του ασύρματου καναλιού για να εξάγουν ένα κλειδί, ενώ παράλληλα χρησιμοποιούν την κοινή τυχαιότητα των ασύρματων καναλιών κατά την περίοδο συνοχής του καναλιού. Όπως αναλύθηκε και στο Κεφάλαιο 2, τα ασύρματα κανάλια χωρίζονται σε δύο κατηγορίες: διαλείψεις πολλαπλών διαδρομών μικρής κλίμακας και διαλείψεις μεγάλης κλίμακας, η οποία περιλαμβάνει την απώλεια διαδρομής και τη σκίαση. Δεδομένου ότι η απώλεια διαδρομής είναι προβλέψιμη, η δημιουργία κλειδιών δεν μπορεί να θεωρηθεί ασφαλής. Από την άλλη πλευρά, η εξασθένηση μικρής κλίμακας είναι συχνά απρόβλεπτη και αποτελεί χρήσιμη πηγή δημιουργίας κλειδιών. Τα υπολογιστικά ελαφριά συστήματα PLS λαμβάνονται επί του παρόντος υπόψη στην εποχή 6G του μαζικού IoT και του IoT για κρίσιμες εφαρμογές.

Αυτή η ενότητα αποδεικνύει πώς το ασύρματο μέσο επικοινωνίας παρέχει τα θεμέλια για δύο κρίσιμες λειτουργίες ασφαλείας, δείχνοντας πώς αυτές οι λειτουργίες μπορούν να αξιοποιηθούν. Η πρώτη κρίσιμη λειτουργία ασφαλείας είναι το δακτυλικό αποτύπωμα ενός σήματος RF για αυθεντικοποίηση του εκπεμπόμενου σήματος. Ειδικότερα, μια πηγή μοναδικότητας (δακτυλικό αποτύπωμα), μπορεί να θεωρηθούν οι διαλείψεις μεγάλης κλίμακας που όμως είναι ουσιαστικά προβλέψιμες. Δεδομένου ότι οι απώλειες διαδρομής και η σκίαση είναι φαινόμενα διαλείψεων μεγάλης κλίμακας που συνδέονται στενά με τον εντοπισμό θέσης, ο εντοπισμός μπορεί να χρησιμοποιηθεί ως δεύτερος παράγοντας της αυθεντικοποίησης σε πρωτόκολλα ελέγχου γνησιότητας πολλαπλών παραγόντων. Η δεύτερη κρίσιμη λειτουργία ασφαλείας είναι η δημιουργία συμμετρικών μυστικών κλειδιών (SKG – Secret Key Generation). Ως αποτέλεσμα των διαλείψεων μικρής κλίμακας στο ασύρματο κανάλι, η SKG ή οι απρόβλεπτες αλλαγές στις πληροφορίες σχετικά με την κατάσταση του καναλιού (CSI – Channel State Information) μπορούν να χρησιμοποιηθούν ως πηγή εντροπίας για τον διαχωρισμό των κλειδιών από μια κοινή παρατήρηση (το κανάλι). Στην ουσία, ένας ισχυρός αντίπαλος με πρόσβαση σε όλους τους αποδοτικούς αλγορίθμους (δηλαδή αλγορίθμους που μπορούν να εκτελεστούν σε πολυωνυμικό χρόνο) αξιολογεί την ποιότητα μιας ψευδοτυχαίας πηγής σε σχέση με την ικανότητά τους να δημιουργούν προβλέψεις επόμενων bit.

Τρεις αρχές - η αμοιβαιότητα του καναλιού μεταξύ της Alice και του Bob, η χωρική αποσυσχέτιση και οι χρονικές μεταβολές - είναι απαραίτητες για την ασφαλή παραγωγή κλειδιών. Για τον λόγο ότι ένας παθητικός δέκτης (Eve) που βρίσκεται κοντά στους νόμιμους χρήστες θα

μπορούσε να παράγει διπλά κλειδιά αφού βρίσκεται σε κοινή τοποθεσία με τους άλλους δύο, η χωρική αποσυσχέτιση είναι ιδιαίτερα κρίσιμη. Το μοντέλο του Jakes προβλέπει ότι όταν ένα τρίτο άτομο βρίσκεται σε απόσταση μισού μήκους κύματος, το κανάλι θα είναι ασυσχέτιστο. Στα διανύσματα του καναλιού, κρατώντας τις πρώτες λίγες κυρίαρχες συνιστώσες του, διεξάγεται μια θεωρητική μελέτη σχετικά με αλγορίθμους προ-επεξεργασίας, όπως η ανάλυση κύριων συνιστωσών (PCA – Principal Component Analysis), για να δημιουργήσουν ένα υψηλής συμφωνίας ασυσχέτιστο μυστικό κλειδί και να διευκολύνουν τη συνδιαλλαγή. Κεντρική υπόθεση αυτής της ενότητας είναι ότι λόγω της εξάλειψης της «θορυβώδους» παρατήρησης κρατώντας μόνο τις βασικές συνιστώσες, η εταιροσυσχέτιση μεταξύ των μετρήσεων του καναλιού του Bob και της Alice, μπορεί να καλυτερεύσει λόγω της PCA.

Ωστόσο, σύμφωνα με πειραματικά ευρήματα, η χωρική αποσυσχέτιση σε απόσταση μισού μήκους κύματος είναι ακριβής μόνο σε περιβάλλοντα με άφθονη σκέδαση. Ενδεικτικά, η διατήρηση των πρώτων λίγων κυρίαρχων βασικών συνιστωσών υπό συνθήκες οπτικής επαφής είναι παρόμοια με τη διατήρηση των ιδιοδιανυσμάτων που συνδέονται με τις προβλέψιμες ιδιότητες μεγάλης κλίμακας. Επομένως, υπό αυτές τις συνθήκες, μια τέτοια μέθοδος θα ήταν αναποτελεσματική. Η ανάπτυξη στατιστικών ελέγχων γύρω από τις μετρήσεις συσχέτισης είναι το δεύτερο κρίσιμο στοιχείο. Η χωρική ή χρονική αποσυσχέτιση δεν συνεπάγεται πάντοτε ανεξαρτησία. Η προβλέψιμη χωρικά ή χρονικά συσχετισμένη συνιστώσα των συντελεστών του ασύρματου καναλιού δεν αφαιρείται συστηματικά κατά την εκτέλεση της SKG.

Για τη μυστικότητα και την ακεραιότητα, μία διαδικασία δημιουργίας κλειδιών που είναι ασφαλής είναι απαραίτητη, για παράδειγμα όταν χρησιμοποιείται με τεχνικές κρυπτογράφησης συμμετρικού κλειδιού. Ωστόσο, η δημιουργία μυστικών κλειδιών δεν μπορεί να χρησιμοποιηθεί για την αυθεντικοποίηση αυτή καθαυτή. Η θέση του κόμβου και το δακτυλικό αποτύπωμα RF είναι δύο παραδείγματα προβλέψιμων και επαληθεύσιμων πηγών μοναδικότητας που απαιτούνται για τον έλεγχο γνησιότητας της εκπομπής. Παρά τον τεράστιο όγκο ερευνών σχετικά με το δακτυλικό αποτύπωμα RF και το SKG, το CSI δεν έχει αντιμετωπιστεί σωστά ως πηγή μοναδικότητας και εντροπίας. Επομένως για την SKG χρησιμοποιούνται λύσεις βασισμένες στη MLearning και την επεξεργασία σήματος για τον διαχωρισμό των διαλείψεων μεγάλης κλίμακας (πηγή μοναδικότητας) από τις διαλείψεις μικρής κλίμακας (πηγή κοινής εντροπίας). Χρησιμοποιούνται τα κριτήρια ανεξαρτησίας Hilbert-Schmidt d-μεταβλητών (dHSIC – d-variable Hilbert-Schmidt Independence Criterion) για να διασφαλισθεί η μυστικότητα, όχι μόνο για να επιβληθεί χωρική αποσυσχέτιση μεταξύ των τοποθεσιών, αλλά και για να επιτευχθεί μια σημαντικά ισχυρότερη χωρική ανεξαρτησία. [6]

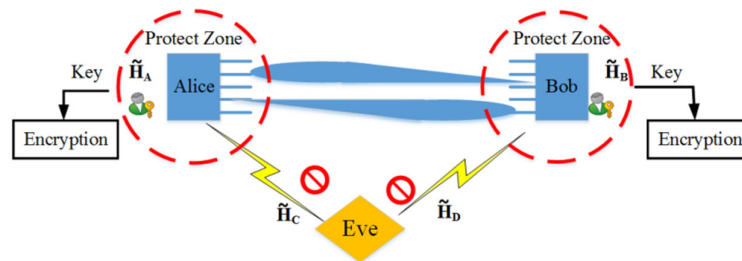
4.2.2 Παραγωγή κλειδιών με την χρήση AoA και AoD του mmWave σε massive MIMO κανάλι

Τα τελευταία χρόνια έχει αυξηθεί σημαντικά το ακαδημαϊκό ενδιαφέρον για την παραγωγή κλειδιών στο φυσικό επίπεδο που χρησιμοποιεί την αμοιβαιότητα και την απρόβλεπτη συμπεριφορά των ασύρματων καναλιών διαλείψεων. Η παραγωγή ενός κοινόχρηστου κλειδιού που χρησιμοποιεί χαρακτηριστικά του φυσικού επιπέδου έχει μικρό υπολογιστικό κόστος και μπορεί να επιτύχει θεωρητική, μαθηματική ασφάλεια πληροφοριών, σε αντίθεση με τη συμβατική διαδικασία ανταλλαγής κλειδιών Diffie-Hellman (D-H). Με άλλα λόγια, η μυστικότητα του παραγόμενου κλειδιού δεν βασίζεται στο πόσο δύσκολο είναι ένα υπολογιστικό ζήτημα, αλλά στις φυσικές αρχές που διέπουν τα ασύρματα κανάλια εξασθένησης. Το massive MIMO, μια από τις πιο εξελιγμένες

τεχνολογίες ασύρματης επικοινωνίας, θεωρείται ως κρίσιμος παράγοντας για τα επόμενα συστήματα επικοινωνίας 5G. Το mmWave χρησιμοποιεί εύρος ζώνης μεταξύ 30 και 300 GHz, διαφοροποιούμενο από τις ήδη χρησιμοποιούμενες τεχνολογίες WiFi και κυψελοειδείς που λειτουργούν σε συχνότητες φέρουσας κάτω από 6 GHz. Η επικοινωνία mmWave μπορεί να επιτύχει εξαιρετικά υψηλό εύρος ζώνης και ταχύτητες δεδομένων λόγω της υψηλής συχνότητας. Με ένα σύστημα massive MIMO, εκατοντάδες στοιχεία κεραίας μπορούν να τοποθετηθούν σε μια συστοιχία σε μια σχετικά μικρή φυσική πλατφόρμα χάρη στα εξαιρετικά μικρά μήκη κύματος της τάξεως των 5,35 mm.

Έχουν προταθεί αρκετές διαδικασίες δημιουργίας κλειδιών στο φυσικό επίπεδο για δίκτυα 3G και 4G, αλλά καμία δεν έχει γίνει για προσεγγίσεις 5G, όπως το mmWave massive MIMO. Λόγω των ξεχωριστών χαρακτηριστικών του καναλιού και του μεγάλου αριθμού κεραίων, η επικοινωνία mmWave massive MIMO παρουσιάζει νέα ζητήματα για τη δημιουργία κλειδιών στο φυσικό επίπεδο σε αντίθεση με τις προηγούμενες διαδικασίες δημιουργίας κλειδιών. Κατ' αρχάς, ένα κανάλι κυμάτων χιλιοστού δεν συμπεριφέρεται όπως ένα γκαουσιανό κανάλι, καθώς έχει περιορισμένο το χαρακτηριστικό της σκέδασης. Κατά συνέπεια, η θεωρητική ανάλυση της χωρητικότητας κλειδιού που είναι σήμερα διαθέσιμη και βασίζεται στην υπόθεση του μοντέλου του καναλιού Gauss δεν μπορεί να χρησιμοποιηθεί. Δεύτερον, για το massive MIMO, η ανάγκη εκτίμησης μεγάλου αριθμού καταχωρήσεων του πίνακα καθιστά την εκτίμηση του καναλιού όλο και πιο δύσκολη καθώς αυξάνονται οι διαστάσεις του πίνακα καναλιού. Τρίτον, σύμφωνα με έρευνες, ένα σημαντικό ποσοστό των bits που δημιουργούνται σε δύο συσκευές μπορεί να μην είναι ίδιο σε καθεστώτα χαμηλού SNR, γεγονός που απαιτεί ένα σημαντικό ποσό επιβάρυνσης προκειμένου να επιτευχθεί συνδιαλλαγή και προκαλείται χαμηλή αποδοτικότητα παραγωγής κλειδιών.

Με αυτόν τον τρόπο χρησιμοποιούνται η εικονική γωνία άφιξης (AoA – Angle of Arrival) και η γωνία αναχώρησης (AoD – Angle of Departure), ως πηγές τυχειότητας για τη δημιουργία εμπιστευτικού κλειδιού στην επικοινωνία mmWave massive MIMO, με στόχο τη γρήγορη και ασφαλή δημιουργία κλειδιών στο φυσικό επίπεδο. Τα οφέλη από τη χρήση εικονικών AoAs και AoDs είναι ποικίλα. Αρχικά, η χρήση αυτών των τεχνικών επιφέρει εκτίμηση με μικρή επιβάρυνση και ευκολία. Σε σύγκριση με την εκτίμηση των CSI, η επιβάρυνση εκτίμησης μειώνεται σημαντικά. Δεύτερον, ο κβαντισμός μπορεί να παραλειφθεί κατά τη διάρκεια της δημιουργίας κλειδιών λόγω του ότι οι εκτιμήσεις εικονικών AoAs και AoDs είναι διακριτές και ακριβείς, γεγονός που κάνει τη διαδικασία να γίνεται ευκολότερη, μειώνεται η ποσότητα των χαμένων bits και αυξάνεται η αποδοτικότητα της δημιουργίας κλειδιών. Οι εκτιμήσεις των εικονικών AoAs και AoDs παρουσιάζουν εξαιρετικά ισχυρή αμοιβαιότητα ακόμη και σε συνθήκες χαμηλού SNR και είναι ανθεκτικές στο θόρυβο. Με αυτόν τον τρόπο, επιτυγχάνονται πολύ υψηλοί δείκτες συμφωνίας bit σε χαμηλό SNR, κάτι που συνήθως δεν είναι εφικτό μέσω της άμεσης αξιοποίησης των εκτιμώμενων πληροφοριών για την κατάσταση του καναλιού. Η επιβάρυνση για «συμφιλίωση» (εξασφάλιση ότι τα bit των κλειδιών είναι ίδια και στα δυο μέρη) μειώνεται σημαντικά με τον υψηλό λόγο συμφωνίας bit, απαραίτητος για τη διασφάλιση της πρακτικότητας και της αποτελεσματικότητας της δημιουργίας κλειδιών στο φυσικό επίπεδο. Επιπλέον, στο πλαίσιο των συστημάτων μας massive MIMO, καθώς αυξάνεται ο αριθμός των κεραίων, παρατηρείται αύξηση του λόγου συμφωνίας bit, που έχει ως αποτέλεσμα αυξημένα ποσοστά παραγωγής κλειδιών. [7]



Εικόνα 4-2: Παραγωγή κλειδιών στο φυσικό επίπεδο για συστήματα massive MIMO χιλιοστομετρικών κυμάτων. [7]

4.2.3 Εξαγωγή των ιδιοτήτων του σήματος με χρήση ραντάρ

Η εξαγωγή διακριτών εγγενών χαρακτηριστικών από ένα σήμα RF (RF-DNA – Radio-Frequency Distinct Native Attribute) επιτυγχάνεται με την επεξεργασία δακτυλικών αποτυπωμάτων του σήματος. Κάθε συσκευή παράγει σήματα που περιέχουν διακριτές ιδιότητες ή χαρακτηριστικά, τα οποία χρησιμεύουν για τη διαφοροποίησή της από άλλες συσκευές παρόμοιας φύσης. Η ιδέα είναι συγκρίσιμη με την αποτύπωση ανθρώπινων δακτυλικών αποτυπωμάτων, κατά την οποία ένα άτομο μπορεί να αναγνωριστεί από ένα άλλο με βάση τα δακτυλικά του αποτυπώματα. Οι παθητικές τεχνικές αποτέλεσαν αντικείμενο αρκετών ερευνών που έδωσαν βάση τόσο στις εκούσιες εκπομπές ακτινοβολίας (IRE – Intended Radiated Emissions) όσο και στις ακούσιες εκπομπές ακτινοβολίας (URE – Unintended Radiated Emissions). Μια μεγάλη κατηγορία ηλεκτρονικών κυκλωμάτων, συμπεριλαμβανομένων των μονωμένων ενισχυτών RF, των μικτών, των ταλαντωτών και των φίλτρων που συνθέτουν ένα τυπικό front-end δέκτη, δεν παράγουν συνήθως ακτινοβολία RF.

Οι διεγερμένες ακούσιες εκπομπές ακτινοβολίας (SURE – Stimulated Unintended Radiated Emissions), αποτελεί μία νέα τεχνική και προκειμένου να αναλύσει τα αποτυπώματα RF-DNA χρησιμοποιεί την ανακλώμενη ενέργεια RF ενός σήματος που προέρχεται από ραντάρ. Χρησιμοποιείται σήμα θορύβου εξαιρετικά ευρείας ζώνης (UWB – Ultra WideBand) το οποίο εκπέμπεται από ένα ραντάρ τυχαίου θορύβου (RNR – Random Noise Radar) και θα χρησιμεύσει ως η κυματομορφή εξακρίβωσης. Λόγω του τεράστιου στιγμιαίου εύρους ζώνης του, το οποίο μπορεί να προκαλέσει μοναδικούς τρόπους συντονισμού στην υπό δοκιμή συσκευή (DUT – Device Under Test), το σήμα αυτό μπορεί να έχει μεγαλύτερη ακρίβεια ταξινόμησης. Η κυματομορφή του θορύβου καθίσταται ιδανική και επιτρέπει ουσιαστική παράλληλη επεξεργασία της διαδικασίας κατηγοριοποίησης καθώς εκπέμπει ταυτόχρονα με άλλες πηγές ραντάρ απουσία παρεμβολών, είναι μη καταστροφική και φασματικά συμβατή σε ανεκτά επίπεδα ισχύος. Έτσι με την βοήθεια των χαρακτηριστικών αυτών, στην συνέχεια αυτά μπορούν να χρησιμοποιηθούν για να δημιουργηθούν κλειδιά που θα επιτρέψουν την αυθεντικοποίηση μίας εκπομπής. [8]

5

Ασύρματα Συστήματα Καθορισμένα από Λογισμικό

Ως ασύρματο σύστημα που καθορίζεται από λογισμικό (SDR – Software-Defined Radio) ορίζεται ένας πομποδέκτης που μπορεί να προγραμματιστεί μέσα από κατάλληλο λογισμικό σε οποιονδήποτε υπολογιστή και έχει τη δυνατότητα να εκτελεί έναν αριθμό πρωτοκόλλων ασύρματης επικοινωνίας χωρίς να απαιτείται η τροποποίηση ή η αναβάθμιση του υλικού. Οι εξελίξεις στο πεδίο του SDR έχουν συμβάλει καταλυτικά στην επέκταση της εξέλιξης των πρωτοκόλλων και σε ένα ευρύ φάσμα εφαρμογών. Αυτή η τάση δίνει μεγαλύτερη έμφαση σε χαρακτηριστικά όπως η δυνατότητα προγραμματισμού, η προσαρμοστικότητα, η ικανότητα για εύκολη μεταφορά και η αποδοτικότητα της ενέργειας. Ο τομέας αυτός εκτείνεται στις επικοινωνίες κυψελοειδούς δικτύου, Wi-Fi και επικοινωνίας μεταξύ μηχανών (M2M – Machine-To-Machine). Ως εκ τούτου, το SDR έχει συγκεντρώσει σημαντικό ενδιαφέρον και έχει μεγάλη σημασία τόσο για τον ακαδημαϊκό όσο και για τον βιομηχανικό τομέα. Ο στόχος των σχεδιαστών SDR είναι να απλοποιήσουν την εφαρμογή των πρωτοκόλλων επικοινωνίας, δίνοντας παράλληλα τη δυνατότητα στους ερευνητές να διεξάγουν πειράματα χρησιμοποιώντας πρωτότυπα μέσα σε έτοιμα δίκτυα. Αυτό το κεφάλαιο, θα ασχοληθεί με την γενική επισκόπηση των SDR καθώς και την μελέτη της αρχιτεκτονικής και τις προκλήσεις αυτής της τεχνολογίας. [9]

5.1 Επισκόπηση Ασύρματων Συστημάτων Καθορισμένων από Λογισμικό

Η πρόοδος των ασύρματων τεχνολογιών έχει μεταμορφώσει την επικοινωνιακή συμπεριφορά των καταναλωτών. Οι ασύρματες τεχνολογίες αποτελούν θεμελιώδη πτυχή της καθημερινής ρουτίνας των χρηστών και ο ρόλος τους αναμένεται να γίνει ακόμη πιο έντονος στο μέλλον. Κατά τη σύνδεση πολυπληθών συσκευών στο διαδίκτυο, προκειμένου να δημιουργήσουν ένα δίκτυο IoT, το αρχικό εμπόδιο έγκειται στην προσαρμογή των θεμελιωδών επιπέδων συνδεσιμότητας και δικτύωσης για την αποτελεσματική διαχείριση του σημαντικού όγκου τελικών σημείων. Έχει εμφανιστεί μια

κλιμακούμενη σειρά ασύρματων πρωτοκόλλων, που περιλαμβάνει τα ZigBee, τα Bluetooth χαμηλής ενέργειας (BLE – Bluetooth Low Energy), LTE, NR καθώς και νέα πρωτόκολλα Wi-Fi, προσαρμοσμένα για εφαρμογές επικοινωνίας IoT και M2M. Αυτά τα πρωτόκολλα προκύπτουν από διάφορες ανάγκες, συμπεριλαμβανομένης της επιτακτικής ανάγκης για αυξημένη ενεργειακή απόδοση. Σε γενικές γραμμές, τα ασύρματα πρότυπα εξελίσσονται ταχύτατα ώστε να ανταποκρίνονται στις μεταβαλλόμενες απαιτήσεις υλικού και στις ανάγκες των χρηστών. Αυτό κατέστησε αναγκαία την δημιουργία ενός πομποδέκτη που μπορεί να υποστηρίξει μια ποικιλία πρωτοκόλλων, τόσο καθιερωμένων όσο και αναδυόμενων. Για την επίτευξη αυτού του στόχου, καθίσταται επιτακτική η αναγνώριση της εγγενούς απαίτησης των πρωτοκόλλων για ένα πλαίσιο ευέλικτο, προγραμματιζόμενο και ικανό για αναδιαμόρφωση.

Η ανάπτυξη πλατφορμών που μπορούν να προγραμματιστούν είναι επιτακτική ανάγκη τόσο από την μεριά (αρχικά) του στρατού όσο και από την μεριά των καταναλωτικών επιχειρήσεων. Δεδομένης της διαρκώς εξελισσόμενης φύσης των ασύρματων πρωτοκόλλων, τα οποία απαιτούν ευελιξία υλικού, η δυνατότητα προγραμματισμού παραμένει πρωταρχικό μέλημα για τους σχεδιαστές σε αυτόν τον τομέα. Το SDR είναι μια τεχνολογία που έχει σχεδιαστεί για τη διευκόλυνση της ασύρματης επικοινωνίας και της ανάπτυξης ασύρματων συστημάτων. Αντί να εξαρτάται από λύσεις βασισμένες σε υλικό, αυτή η τεχνολογία στηρίζεται σε πρωτόκολλα ασύρματης επικοινωνίας που καθορίζονται από λογισμικό. Κατά συνέπεια, αυτό συνεπάγεται τη διευκόλυνση μιας σειράς χαρακτηριστικών και ικανοτήτων. Αυτές περιλαμβάνουν τη δυνατότητα πραγματοποίησης ενημερώσεων και βελτιώσεων μέσω επαναπρογραμματισμού, εξαλείφοντας την ανάγκη αντικατάστασης του υλικού στο οποίο ενσωματώνονται αυτά τα χαρακτηριστικά. Έτσι ανοίγει το δρόμο για τη υλοποίηση ασύρματων συσκευών που είναι τόσο πολυ-ζωνικές όσο και πολυ-λειτουργικές.

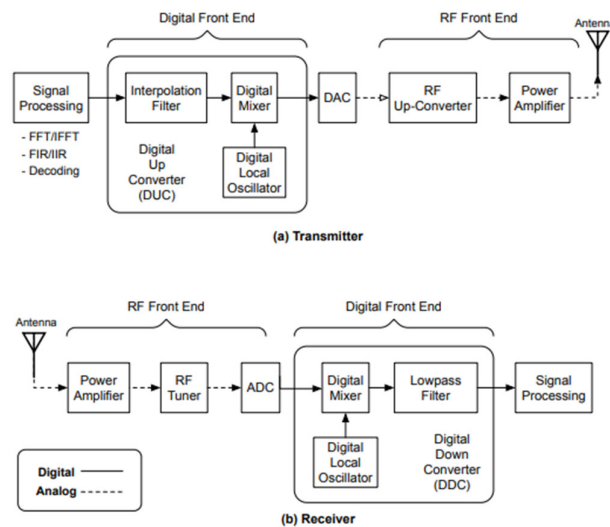
Τα SDR υλοποιούνται με τη χρήση μιας σειράς πλατφορμών υλικού, συμπεριλαμβανομένων επεξεργαστών γενικού σκοπού (GPP – General Purpose Processors), μονάδων επεξεργασίας γραφικών (GPU – Graphics Processing Units), επεξεργαστών ψηφιακών σημάτων (DSP – Digital Signal Processors) και συστοιχιών προγραμματιζόμενων πυλών (FPGA – Field Programmable Gate Arrays). Κάθε πλατφόρμα έχει τα δικά της προβλήματα να αντιμετωπίσει. Μεταξύ αυτών των εμποδίων είναι: η αξιοποίηση της υπολογιστικής ισχύος της επιλεγμένης πλατφόρμας υλικού, η διατήρηση χαμηλής κατανάλωσης ενέργειας, η διευκόλυνση μιας βελτιωμένης διαδικασίας σχεδιασμού και η διαχείριση των δαπανών που σχετίζονται με τα εργαλεία και τον εξοπλισμό. Αυτές οι πλατφόρμες αποτελούν υπόβαθρο για την ανάπτυξη συστημάτων SDR τόσο για την ερευνητική κοινότητα όσο και για την βιομηχανία. Αξιοσημείωτες περιπτώσεις περιλαμβάνουν τα USRPs, Sora, Atomix, Airblue και WARP. Κάθε SDR διαθέτει τη δική του ξεχωριστή προσέγγιση σχεδιασμού, εργαλεία ανάπτυξης, απόδοσης και προβλεπόμενες εφαρμογές. [9]

5.2 Αρχιτεκτονική ενός SDR συστήματος

Αυτή η ενότητα θα ασχοληθεί με την γενική αρχιτεκτονική των συστημάτων SDR. Όπως αναλύθηκε στην προηγούμενη ενότητα, η σημασία των SDR στην εξέλιξη των ασύρματων

προτύπων πηγάζει από την προσαρμοστική τους φύση και την εύκολη δυνατότητα προγραμματισμού τους. Αυτό προκύπτει από το γεγονός ότι η πλειονότητα της ψηφιακής επεξεργασίας σήματος, μαζί με το ψηφιακό front-end που περιλαμβάνει εργασίες όπως η επιλογή καναλιού και η διαμόρφωση/αποδιαμόρφωση, οποίες πραγματοποιούνται ψηφιακά. Συνήθως, η εργασία αυτή εκτελείται μέσω λογισμικού που λειτουργεί σε επεξεργαστές όπως οι GPP και οι DSP. Εναλλακτικά, μπορεί να πραγματοποιηθεί με τη χρήση προγραμματιζόμενου υλικού, όπως οι FPGA. Με την ευρεία έννοια, εστιάζοντας στην πτυχή του πομπού, η διαδικασία περιλαμβάνει τη δημιουργία μιας κυματομορφής βασικής ζώνης, τη μετατροπή της σε κυματομορφή IF, την περαιτέρω μετατροπή της σε κυματομορφή RF και τελικά τη μετάδοση μέσω της κεραίας. Το σήμα RF υποβάλλεται σε δειγματοληψία και αποδιαμόρφωση πριν προχωρήσει στην αποκωδικοποίηση στον δέκτη. Για την εμβάθυνση στις ιδιαιτερότητες αυτής της διαδικασίας, εξετάζεται η πτυχή της λήψης από το σύστημα.

Ξεκινώντας από την κεραία, το σήμα RF υφίσταται ενίσχυση μέσω μιας βαθμίδας RF που εστιάζει σε ένα συγκεκριμένο εύρος ζώνης συχνοτήτων. Μετά, γίνεται μετατροπή αυτού του ενισχυμένου σήματος σε αναλογικό σήμα IF. Ο ADC εκτελεί την ψηφιοποίηση αυτού του σήματος IF, μετατρέποντάς το σε ψηφιακά δείγματα. Αυτά τα δείγματα εισάγονται στη συνέχεια σε ένα στάδιο μίξης, όπου μια άλλη είσοδος προέρχεται από έναν τοπικό ταλαντωτή, η συχνότητα του οποίου ρυθμίζεται από τον έλεγχο συντονισμού. Μετά από αυτό, ο μίκτης εκτελεί τη μετάφραση του σήματος εισόδου σε σήμα βασικής ζώνης. Στη συνέχεια, απομονώνεται ένα μοναδικό σήμα από ένα φίλτρο πεπερασμένης κρουστικής απόκρισης (FIR – Finite Impulse Response) το οποίο περιορίζει αποτελεσματικά το εύρος ζώνης του σήματος και ταυτόχρονα λειτουργεί ως χαμηλοπερατό φίλτρο αποκοπής. Εντός του ψηφιακού κάτω μετατροπέα συχνότητας, μια σειρά πολλαπλασιαστών, αθροιστών και καταχωρητών ολίσθησης αξιοποιούνται στο πεδίο του υλικού, εκπληρώνοντας τις καθορισμένες λειτουργίες όπως περιγράφονται παραπάνω. Έστερα, λαμβάνουν χώρα διαδικασίες όπως η αποδιαμόρφωση και η αποκωδικοποίηση που πραγματοποιούνται στο στάδιο επεξεργασίας του σήματος. Για τον χειρισμό αυτού του σταδίου χρησιμοποιείται συχνά εξειδικευμένο υλικό, όπως ένα ολοκληρωμένο κύκλωμα συγκεκριμένης εφαρμογής (ASIC – Application Specific Integrated Circuit), ή εναλλακτικά συστήματα με δυνατότητα προγραμματισμού, όπως FPGA ή DSP.



Εικόνα 5-1: Αρχιτεκτονική SDR συστήματος για έναν (α) πομπό και για έναν (β) δέκτη. [9]

Με σημείο αναφοράς την Εικόνα 5-1, ένας πομπός και ένας δέκτης SDR αποτελείται από τα ακόλουθα στοιχεία:

- **Κεραία:** Στις διατάξεις SDR, ενσωματώνονται συνήθως πολλαπλές κεραίες για να καλύψουν ένα ευρύ φάσμα ζωνών συχνοτήτων. Συχνά αποκαλούνται ως «έξυπνες», οι κεραίες διαθέτουν την ικανότητα να επιλέγουν αυτόνομα ζώνες συχνοτήτων, να προσαρμόζονται δυναμικά μέσω παρακολούθησης και ακόμη και να αντιμετωπίζουν τις παρεμβολές μέσω ακύρωσής τους. Για τα SDR, οι κεραίες πρέπει να ικανοποιούν ένα συγκεκριμένο σύνολο κριτηρίων που περιλαμβάνουν αυτοπροσαρμογή (που επιτρέπει τον συντονισμό σε πολλές ζώνες), αυτοευθυγράμμιση (που παρουσιάζει ικανότητα διαμόρφωσης δέσμης) και αυτό-ίαση (που απορρίπτει αποτελεσματικά τις παρεμβολές) μεταξύ άλλων.
- **RF Front-End:** Αποτελεί ένα κύκλωμα RF σχεδιασμένο κυρίως για τη μετάδοση και τη λήψη σημάτων σε διάφορες συχνότητες λειτουργίας. Επιπλέον, χρησιμεύει για τη μετατροπή σημάτων από και προς την IF. Η λειτουργικότητα διακρίνεται σε δύο διαδρομές με βάση την κατεύθυνση του σήματος (αν βρίσκεται σε λειτουργία μετάδοσης ή λήψης). Κατά την διαδρομή μετάδοσης, γίνεται μετατροπή των ψηφιακών δειγμάτων σε αναλογικό σήμα μέσω του DAC και στην συνέχεια αυτό το αναλογικό σήμα αποστέλλεται στο RF Front-End όπου συνδυάζεται (αναμιγνύεται) με μια προκαθορισμένη συχνότητα RF, υποβάλλεται σε διαμόρφωση και στη συνέχεια εκπέμπεται. Κατά την διαδρομή λήψης, το σήμα προσπίπτει επάνω στην κεραία και λαμβάνεται από αυτήν. Με την βοήθεια ενός κυκλώματος αντιστοίχισης και προκειμένου να επιτευχθεί η ιδανική μεταφορά ισχύος του σήματος, η είσοδος της κεραίας ενώνεται με το RF Front-End. Μετά, το σήμα διέρχεται από έναν ενισχυτή χαμηλού θορύβου (LNA – Low Noise Amplifier), ο οποίος είναι κοντά στην κεραία, προκειμένου να ενισχύσει τα ασθενή σήματα και να περιορίσει τις παραμορφώσεις λόγω θορύβου. Το ενισχυμένο σήμα, σε συνδυασμό με μια είσοδο από τον τοπικό ταλαντωτή (LO – Local Oscillator), κατευθύνεται στη συνέχεια στον μίκτη με σκοπό την μετατροπή του προς τα κάτω στην IF.
- **Μετατροπή ψηφιακού σε αναλογικό και το αντίστροφο:** Ο DAC είναι επιφορτισμένος με τη δημιουργία του αναλογικού σήματος που προορίζεται για μετάδοση από τα ψηφιακά δείγματα. Στην λήψη, συναντάται ένα κρίσιμο στοιχείο για τους ασύρματους δέκτες, ο ADC. Ο ρόλος του ADC περιλαμβάνει τη μετατροπή σημάτων συνεχούς χρόνου σε σήματα δυαδικής αναπαράστασης και διακριτού χρόνου. Υπάρχουν διάφοροι παράμετροι οι οποίοι μπορούν να αξιολογήσουν την απόδοση του ADC όπως το SNR, το πλήθος των bits ανά δείγμα, το ελεύθερο δυναμικό εύρος (SFDR – Spurious-Free Dynamic Range) και η απώλεια ισχύος. Οι βελτιώσεις στις επιδόσεις των ADC έχουν αποκτήσει δυναμική χάρη στις εξελίξεις στην τεχνολογία SDR. Για παράδειγμα, έχουν δημιουργηθεί πιο ενεργειακά αποδοτικοί ADC, καθώς η κατανάλωση ενέργειας των ADC έχει επιπτώσεις στη διάρκεια ζωής των SDR που τροφοδοτούνται από μπαταρίες.
- **Digital Front-End:** Οι πρωταρχικοί ρόλοι του Digital Front-End περιλαμβάνουν δύο βασικές λειτουργίες. Πρώτον, εκτελεί μετατροπή ρυθμού δειγματοληψίας (SRC – Sample Rate Conversion) δηλαδή την συχνότητα δειγματοληψίας από έναν ρυθμό σε έναν άλλο. Η προσαρμογή αυτή είναι επιβεβλημένη λόγω του απαιτούμενου συγχρονισμού μεταξύ των δύο επικοινωνούντων οντοτήτων. Δεύτερον, εκτελεί καναλοποίηση (Channelization) κατά την οποία πομπός και ο δέκτης ασχολούνται με την πάνω και κάτω μετατροπή στη συχνότητα, αντίστοιχα. Επίσης, αυτή η διαδικασία εμπεριέχει και την πρακτική του φιλτραρίσματος

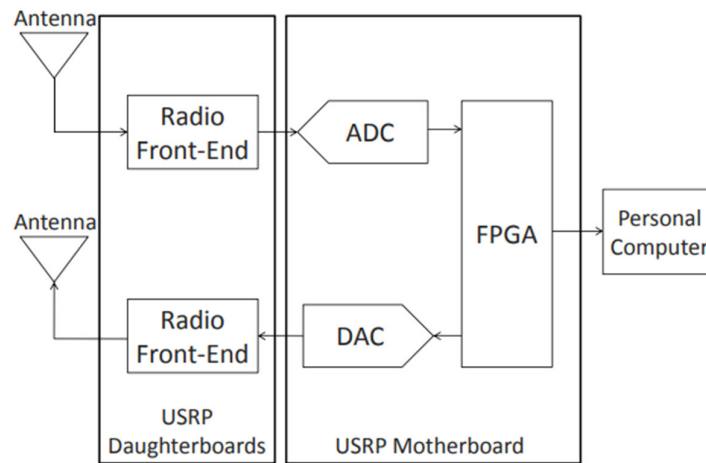
καναλιών, η οποία συνεπάγεται στην απομόνωση καναλιών που διαχωρίζονται με βάση τη συχνότητα. Το interpolation (αύξηση ρυθμού) σε συνδυασμό με χαμηλοπερατά φίλτρα αποτελούν μερικά παραδείγματα της καναλοποίησης. Στην πλευρά του πομπού, σήμα βασικής ζώνης που αναφέρθηκε παραπάνω μετατρέπεται σε IF μέσω του ψηφιακού άνω μετατροπέα (DUC – Digital Up Converter). Τα ψηφιακά δείγματα IF μετατρέπονται στη συνέχεια σε αναλογικό σήμα IF από τον DAC που συνδέεται με το DUC. το αναλογικό σήμα IF υφίσταται μετατροπή σε συχνότητες RF μέσω της χρήσης του άνω μετατροπέα RF. Στην πλευρά του δέκτη, το σήμα IF μετατρέπεται σε ψηφιακά δείγματα από τον ADC. Αυτά τα δείγματα κατευθύνονται στη συνέχεια στην επόμενη μονάδα, γνωστή ως ψηφιακός μετατροπέας προς τα κάτω (DDC – Digital Down Converter). Μέρη του DDC αποτελούν ένας ψηφιακός μίκτης μαζί με έναν αριθμητικά ελεγχόμενο ταλαντωτή. Ο ρόλος του DDC περιλαμβάνει την εξαγωγή του ψηφιακού σήματος βασικής ζώνης από τον ADC. Μετά από αυτό, το σήμα υφίσταται ψηφιακή επεξεργασία από το Digital Front-End, προτού κατευθυνθεί σε μια μονάδα ψηφιακής επεξεργασίας σήματος υψηλής ταχύτητας.

- Επεξεργασία Σήματος: Αυτό το μπλοκ αναλαμβάνει μια σειρά εργασιών επεξεργασίας σήματος, συμπεριλαμβανομένης της κωδικοποίησης και της αποκωδικοποίησης, της αναδιάταξης (interleaving) και της από-αναδιάταξης (deinterleaving), της διαμόρφωσης και της αποδιαμόρφωσης, καθώς και των λειτουργιών ανακατώματος (scrambling) και από-ανακατώματος (descrambling). Η κωδικοποίηση που εφαρμόζεται στο κανάλι λειτουργεί ως κώδικας διόρθωσης σφαλμάτων όπου το κωδικοποιημένο σήμα ενσωματώνει πλεονασμό τον οποίο χρησιμοποιεί ο αποκωδικοποιητής του δέκτη για να ανακατασκευάσει με ακρίβεια το αρχικό σήμα μέσω του αλλοιωμένου λαμβανόμενου σήματος. Οι κώδικες διόρθωσης σφαλμάτων περιλαμβάνουν, μεταξύ άλλων, τους κώδικες συνέλιξης, τους κώδικες Turbo και τους κώδικες ελέγχου ισοτιμίας χαμηλής πυκνότητας (LDPC – Low Density Parity Check). Εντός του μπλοκ επεξεργασίας σήματος, ο αποκωδικοποιητής ξεχωρίζει ως το στοιχείο που απαιτεί τους υψηλότερους υπολογιστικούς πόρους, κυρίως λόγω της πολυπλοκότητας των συστημάτων μεταφοράς δεδομένων και διαχείρισης μνήμης. Η φάση της διαμόρφωσης περιλαμβάνει τον FFT και τον IFFT, οι οποίοι αποτελούν το δεύτερο τμήμα του μπλοκ που αναγνωρίζεται για τη σημαντική πολυπλοκότητά του και τις απαιτήσεις σε πόρους, τόσο σε έκταση όσο και σε ισχύ.

Το τμήμα επεξεργασίας βασικής ζώνης είναι ένας κοινός όρος που χρησιμοποιείται για να υποδηλώσει το τμήμα επεξεργασίας σήματος. Το μπλοκ βασικής ζώνης είναι το μεγαλύτερο μέρος του ψηφιακού τμήματος της υλοποίησης η οποία λειτουργεί πάνω σε ειδικό κύκλωμα υλικού που έχει σχεδιαστεί για αποτελεσματική επεξεργασία σήματος. Ενδεικτικές περιπτώσεις είναι τα SoCs, οι FPGAs, οι DSPs, οι GPPs και οι GPUs. Η άλλη πτυχή της υλοποίησης περιλαμβάνει το λογισμικό, το οποίο παρέχει τόσο τις επιχειρησιακές δυνατότητες όσο και τις αφαιρέσεις υψηλού επιπέδου που είναι απαραίτητες για τη διεξαγωγή εργασιών επεξεργασίας σήματος. [9]

5.3 Εργαλεία Υλοποίησης

Όπως αναφέρθηκε παραπάνω, υπάρχει πλήθος υλοποιήσεων SDR συστημάτων. Πέρα από αυτό όμως υπάρχουν και αρκετά λογισμικά για το χτίσιμο ενός τέτοιου συστήματος. Αυτή η διπλωματική θα ασχοληθεί συγκεκριμένα με το δωρεάν ανοικτό λογισμικό GNU Radio το οποίο στο επόμενο κεφάλαιο (Κεφάλαιο 6) θα χρησιμοποιηθεί για την υλοποίηση του πειράματος. Το Universal Software Radio Peripheral (USRP) είναι ένα δημιούργημα της Ettus Research LLC, σχεδιασμένο για να μετατρέπει τυπικούς προσωπικούς υπολογιστές σε ευέλικτες πλατφόρμες SDR. Στην παρούσα εργασία θα γίνει μία προσομοίωση με σύστημα SDR το οποίο θα επιτελεί την παραγωγή κλειδιών με χρήση των ιδιοτήτων του σήματος και του καναλιού. Η FPGA Altera Cyclone EP1C12 και τέσσερις ADC και DAC υψηλής ταχύτητας στη μητρική πλακέτα αποτελούν την κεντρική μονάδα επεξεργασίας (CPU – Central Process Unit) του USRP. Τα ασύρματα FE, γνωστά ως θυγατρικές κάρτες, χρησιμεύουν ως σημεία σύνδεσης για τους ADCs/DACs, ενώ η FPGA συνδέεται με ένα τσιπ διεπαφής USB3 που διευκολύνει την επικοινωνία με έναν υπολογιστή γενικής χρήσης. Η Εικόνα 5-2 απεικονίζει την εσωτερική αρχιτεκτονική του USRP. Η θεμελιώδης ιδέα που διέπει το USRP είναι ο καταμερισμός των ψηφιακών ασύρματων λειτουργιών μεταξύ της εσωτερικής FPGA και της εξωτερικής CPU. Σε αυτό το πλαίσιο, οι γρήγορες και ευέλικτες εργασίες επεξεργασίας γενικής χρήσης, όπως η μετατροπή προς τα κάτω και προς τα πάνω, η αποκοπή και η παρεμβολή, εκτελούνται εντός της FPGA. Από την άλλη πλευρά, οι διεργασίες που αφορούν συγκεκριμένες κυματομορφές, όπως η διαμόρφωση και η αποδιαμόρφωση, αναλαμβάνονται από την CPU.



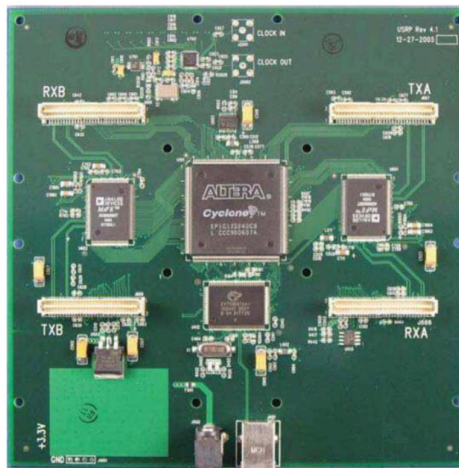
Εικόνα 5-2: Εσωτερική αρχιτεκτονική του USRP. [10]

Μόλις το σήμα υποβληθεί σε επεξεργασία εντός της USRP FPGA, η προκύπτουσα ροή bits μεταδίδεται τελικά μέσω της σύνδεσης USB στην CPU. Σε αυτό το σημείο το περιβάλλον GNU Radio αναλαμβάνει το κεντρικό ρόλο. Το GNU Radio, μια εργαλειοθήκη ελεύθερα διαθέσιμου λογισμικού που διέπεται από την άδεια GPL, έρχεται στο παιχνίδι για να διευκολύνει την υλοποίηση των SDR προγραμμάτων. Μέσα στο GNU Radio, ένας πομποδέκτης απεικονίζεται οπτικά ως γράφημα. Σε αυτό το γράφημα, τα μπλοκ επεξεργασίας σήματος χρησιμεύουν ως κορυφές, ενώ η ροή δεδομένων μεταξύ αυτών των μπλοκ συμβολίζεται με ακμές. Έτσι, η δημιουργία ενός SDR

είναι ανάλογη με τη δημιουργία φυσικών κομματιών ενός ασύρματου συστήματος, τα οποία αποτελούνται από πραγματικά κατασκευαστικά μέρη RF που είναι συνδεδεμένα μεταξύ τους. [10]

5.3.1 Η συσκευή USRP

Η διαμόρφωση της κεντρικής πλακέτας USRP φαίνεται στην Εικόνα 5-3. Το USRP δημιουργήθηκε εξ ολοκλήρου μέσω ενός έργου ανοικτών προδιαγραφών, χρησιμοποιώντας ελεύθερα προσβάσιμο λογισμικό σχεδιασμού με την βοήθεια υπολογιστή (CAD – Computer-Aided Design) ανοικτού κώδικα. Εάν παρατηρηθεί η παρακάτω Εικόνα 5-3, οι τέσσερις μακρόστενες λευκές θύρες διατίθεται για τη σύνδεση των θυγατρικών πλακετών. Μέσα σε αυτές τις υποδοχές, δύο είναι αφιερωμένες στη μετάδοση (TXA και TXB), ενώ οι υπόλοιπες δύο στη λήψη (RXA και RXB). Τα σήματα μετάδοσης και λήψης μεταφέρονται μέσω των ADC/DAC, που συμβολίζονται με τα μαύρα τσιπ που βρίσκονται μεταξύ των λευκών υποδοχών. Στην καρδιά της μητρικής πλακέτας βρίσκεται η Altera Cyclone FPGA, η οποία αναλαμβάνει καθοριστικό ρόλο στην εκτέλεση μέρους των διαδικασιών DSP. Σε κοντινή απόσταση και πιο κάτω από την FPGA, το τσιπ διασύνδεσης USB είναι εμφανές και χρησιμεύει ως αγωγός επικοινωνίας μεταξύ της κεντρικής CPU και της συσκευής.



Εικόνα 5-3: Κύρια πλακέτα που αποτελεί το USRP. [10]

Ενσωματωμένοι στο USRP είναι τέσσερις ADC των 12 ή 14-bit. Με ρυθμό δειγματοληψίας 64 Msamples ανά δευτερόλεπτο, αυτή η διαμόρφωση επιτρέπει την ψηφιοποίηση σημάτων που καλύπτουν εύρος ζώνης έως και 32 MHz. Αναλυτικότερα, όταν ψηφιοποιούνται σήματα που υπερβαίνουν το όριο των 32 MHz για την αποφυγή της αλλοίωσης του φάσματός τους, το Radio Front-End είναι επιφορτισμένο με την ευθύνη της μετατροπής προς τα κάτω αυτών των σημάτων πριν από την είσοδό τους στον ADC. Επιπλέον, η πλακέτα ενσωματώνει έναν ενισχυτή προγραμματιζόμενου κέρδους (PGA – Programmable Gain Amplifier) που προηγείται των ADC. Αυτό εξυπηρετεί τον σκοπό της αξιοποίησης ολόκληρου του φάσματος του διαθέσιμου εύρους εισόδου, ένα ιδιαίτερα πολύτιμο χαρακτηριστικό κατά τον χειρισμό ασθενών σημάτων. Από την μεριά της εκπομπής, η διάταξη περιλαμβάνει τέσσερις DAC 14 ή 16-bit που λειτουργούν με ρυθμό δειγματοληψίας 128 Msamples ανά δευτερόλεπτο (για B200 USRP). Στο πλαίσιο αυτό, η συχνότητα είναι 64 MHz. Για να εξασφαλιστεί η βέλτιστη αποτελεσματικότητα του φίλτρου,

συνιστάται η εφαρμογή υπερ-δειγματοληψίας. Μετά τους DAC, βρίσκεται ένας PGA, ο οποίος παρέχει τη δυνατότητα κέρδους έως και 20 dB.

Η FPGA αποτελεί βασικό ακρογωνιαίό λίθο στην αρχιτεκτονική του USRP. Χρησιμοποιώντας τη γλώσσα περιγραφής υλικού Verilog, η FPGA του USRP υποβάλλεται σε μεταγλώττιση μέσω της έκδοσης Quartus II web της Altera για απρόσκοπτη ενσωμάτωση. Η προεπιλεγμένη διαμόρφωση, ως έχει, προσφέρει ευελιξία για ένα ευρύ φάσμα εφαρμογών. Η FPGA δημιουργεί συνδέσεις με τους ADC, τους DAC και τον ελεγκτή USB. Από την πλευρά της λήψης, ο ADC μετατρέπει το αναλογικό σήμα σε δείγματα 12 ή 14 bit, τα οποία στη συνέχεια αποστέλλονται στην FPGA για επιπλέον επεξεργασία. Στο πλαίσιο αυτό, ένας πολυπλέκτης λειτουργεί για να κατευθύνει το σήμα στον αντίστοιχο μετατροπέα άμεσης μετατροπής προς τα κάτω. Αυτός ο μετατροπέας, με τη σειρά του, είναι υπεύθυνος για τη μετατροπή του σήματος στη βασική ζώνη, ενώ ταυτόχρονα εκτελεί την αποκοπή, μια διαδικασία που διέπεται από έναν καθορισμένο από τον χρήστη παράγοντα. Μετά, εάν υπάρχουν πολλαπλά κανάλια, τα δεδομένα παρεμβάλλονται και προωθούνται σε δείγματα των 16 bit στον ελεγκτή USB. Αυτός ο ελεγκτής ενορχηστρώνει τη μετάδοση των δεδομένων στην CPU. Η σύνδεση USB λειτουργεί σε καθορισμένο ονομαστικό εύρος ζώνης ημι-διπλής (half-duplex) ροής. Αυτό σημαίνει ότι υπάρχει απαίτηση κατανομής αυτού του εύρους ζώνης μεταξύ των κατευθύνσεων άνω και κάτω ζεύξης. Κατά την ανάπτυξη ενός ασυρμάτου συστήματος που χρησιμοποιεί το USRP, το εύρος ζώνης USB αναδεικνύεται ως ένας ιδιαίτερα σημαντικός περιορισμός. Κατά συνέπεια, συγκεκριμένες διαδικασίες του DSP πρέπει να διεξάγονται εντός της FPGA πριν από τη διαβίβαση των δεδομένων στην CPU.

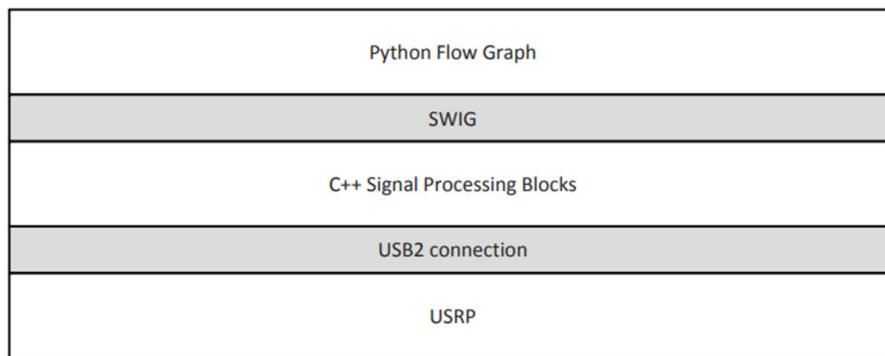
Η κεντρική πλακέτα USRP μπορεί να συνδεθεί με τέσσερις πλακέτες Radio Front-End, που συνήθως αναφέρονται ως θυγατρικές πλακέτες. Κάθε μία από αυτές περιλαμβάνει δύο συνδέσεις SMA (είσοδος-έξοδος) και δύο ADC/DAC υψηλής ταχύτητας. Υπάρχουν θυγατρικές πλακέτες που δεν διαθέτουν κανένα μίκτη, φίλτρο ή ενισχυτή και άλλες έχουν ανεξάρτητους LO, μεταγωγής εκπομπής/λήψης και ενσωματώνουν δυνατότητες MIMO. [10]

5.3.2 Το λογισμικό GNU Radio

Μια εφαρμογή GNU Radio περιλαμβάνει ένα γράφημα ροής, όπου οι ακμές του γραφήματος μπορεί να έχουν τη μορφή πηγών σήματος (source), καταβोधρών (sink) ή μπλοκ επεξεργασίας. Κάθε μπλοκ διαθέτει χαρακτηριστικά που δηλώνουν τον αριθμό των θυρών εισόδου και εξόδου του, καθώς και το συγκεκριμένο είδος δεδομένων που μπορεί να διαχειριστεί. Όπως είναι σαφές, ένα μπλοκ πηγής έχει μόνο θύρες εξόδου, ένα μπλοκ καταβोधρας έχει μόνο θύρες εισόδου και ένα μπλοκ επεξεργασίας διαθέτει πολλαπλές θύρες είτε εισόδου είτε εξόδου. Υπάρχουν δύο ειδών μπλοκ επεξεργασίας σήματος, τα σύγχρονα και τα ασύγχρονα. Επίσης, τα μπλοκ επεξεργασίας μπορούν να διαχειριστούν δεδομένα τύπου float, short, char καθώς και μιγαδικούς αριθμούς. Για να γίνει αντιληπτό τι ακριβώς blocks διαθέτει το λογισμικό αυτό, παρατίθενται ορισμένα παραδείγματα: μπλοκ μαθηματικών υπολογισμών (πρόσθεση αφαίρεση κ.α.), φίλτρα, FFT, γεννήτριες σημάτων, πηγές από USRP και άλλα.

Μέσα στο GNU Radio, η δημιουργία των μπλοκ γίνεται σε C++, ενώ η κατασκευή και η εκτέλεση των γραφημάτων γίνεται σε Python και μαζί αυτές οι δύο γλώσσες προγραμματισμού συνδέονται μέσω της διεπαφής SWIG2. Η παραγωγή ενός γραφήματος ροής με την χρήση της Python είναι μία απλή διαδικασία. Χρησιμοποιώντας το SWIG, όλα τα μπλοκ μπορούν να

προσεγγιστούν απευθείας από τον κώδικα της Python. Αξίζει να τονιστεί ότι το GNU Radio προσφέρει κλάσεις για την αλληλεπίδραση με το USRP (συνίσταται η χρήση αυτής της συσκευής). Όμως το GNU Radio αποτελεί ένα λογισμικό το οποίο είναι γενικής χρήσης με αποτέλεσμα να μην υπάρχουν τροχοπέδη σε περίπτωση χρήσης άλλου υλικού. Για παράδειγμα, η δημιουργία ενός απλού δέκτη AM είναι εφικτή χωρίς να βασίζεται σε ένα USRP. Αυτό είναι ιδιαίτερα εφικτό λόγω της όχι μεγάλης συχνότητας, η οποία επιτρέπει την απευθείας σύνδεση της κεραίας με τον ADC. Η ανάπτυξη μιας υλοποίησης σε GNU Radio χρησιμοποιώντας την Python δεν απαιτεί εξαντλητική κατανόηση του κώδικα C++ μέσα σε κάθε μπλοκ. Τα μπλοκ επεξεργασίας σήματος, εκμεταλλεύονται το υλικό ώστε να παρέχουν υπηρεσίες στον κώδικα Python με την χρήση της διεπαφής SWIG.



Εικόνα 5-4: Αρχιτεκτονική του περιβάλλοντος του GNU Radio. [10]

Το GNU Radio δίνει τη δυνατότητα στους χρήστες να μεταφράσουν διάφορες τεχνολογίες στη σφαίρα του λογισμικού. Αυτή η διαδικασία αποτελείται από την γνώση του φυσικού επιπέδου της τεχνολογίας που μελετάται, χρήση των ήδη υπάρχοντων μπλοκ του GNU Radio ή την κατασκευή νέων μπλοκ επεξεργασίας σήματος, την δημιουργία του διαγράμματος ροής και έπειτα την ενορχήστρωση των μπλοκ.

Το εγχείρημα αυτό μπορεί να φανεί ως μια επίπονη διαδικασία και πολλοί περιορισμοί μπορεί να προκύψουν κατά τη διάρκεια της εκτέλεσης λόγω της εγγενούς αδυναμίας του λογισμικού να αναπαράγει με συνέπεια την αλυσίδα εκπομπής και λήψης του υλικού με απόλυτη ακρίβεια. Το πακέτο GNU Radio παρέχει μια σειρά από εφαρμογές Python. Παρόλα αυτά, ευρέως διαδεδομένες τεχνολογίες υλοποιούνται στο GNU Radio από διάφορες ομάδες. Δυστυχώς όμως, δεν φαίνεται να υπάρχει ένας ολοκληρωμένος διαδικτυακός κατάλογος που να συγκεντρώνει όλες τις υπάρχουσες υλοποιήσεις. Ένας σημαντικός όγκος έρευνας είναι επιβεβλημένος για τον εντοπισμό των υφιστάμενων υλοποιήσεων μαζί με τους σχετικούς περιορισμούς τους. [10]

6

Υλοποίηση

Λόγω των εξαιρετικών δυνατοτήτων για την παραγωγή κλειδιών στο φυσικό επίπεδο (PKG – Physical-layer Key Generation) που παρέχει η αμοιβαιότητα του καναλιού αμφιδρόμησης με διαίρεση χρόνου (TDD – Time Division Duplexing), η ασφάλεια φυσικού επιπέδου γίνεται όλο και πιο σημαντική στα ασύρματα συστήματα επικοινωνιών. Η τεχνική PKG, ωστόσο, παλεύει με το πρόβλημα της εκρηκτικά αυξανόμενης επιβάρυνσης πιλότων καθώς αυξάνεται ο αριθμός των κεραιών. Στην παρούσα διπλωματική εργασία, για συστήματα ευρείας ζώνης με συστοιχία μεγάλων κεραιών, παρέχεται μια συνδυασμένη τεχνική PKG χαμηλού κόστους σε μακροπρόθεσμη και βραχυπρόθεσμη βάση. Πιο συγκεκριμένα, διερευνώνται οι αργά εξελισσόμενες ιδιότητες των γωνιών και των καθυστερήσεων της διαδρομής διάδοσης και δημιουργούνται τα μακροπρόθεσμα κλειδιά με βάση αυτούς τους παράγοντες, λαμβάνοντας παράλληλα υπόψη τη τυχαιότητα του καναλιού σε συστήματα με μεγάλες συστοιχίες κεραιών (σημειώνεται ότι παρότι η εργασία κυρίως αναφέρεται σε μεγάλο αριθμό κεραιών, η υλοποίηση έγινε με δυο κεραιοστοιχεία στο δέκτη λόγω περιορισμών υλικού). Στη συνέχεια, μέσω της εφαρμογής της διαμόρφωσης δέσμης (Beamforming), παρακολουθείται το δυναμικά μεταβαλλόμενο κανάλι. Στη συνέχεια αυτής της παρακολούθησης του καναλιού, δημιουργούνται βραχυπρόθεσμα κλειδιά χρησιμοποιώντας τα αποτελέσματα της παρακολούθησης του καναλιού σε ολόκληρο το φάσμα συχνοτήτων. Με μικρή επιβάρυνση, αυτή η προσέγγιση μπορεί να δημιουργήσει αποτελεσματικά τα κλειδιά τα οποία είναι αποδεδειγμένα τυχαία και μεγάλα. [11]

6.1 Μελέτη υλοποίησης

Στα συστήματα ασύρματης επικοινωνίας, τα μυστικά κλειδιά είναι ζωτικής σημασίας για την εξασφάλιση της ασφάλειας της εκπομπής του σήματος. Στα συμβατικά συστήματα, η διανομή και η ενημέρωση των κλειδιών επιβραδύνονται σημαντικά από τις τεχνολογίες παραγωγής κλειδιών, δεδομένου ότι βασίζονται σε περίπλοκους υπολογισμούς και μαθηματικές αναλύσεις. Τα κλειδιά που παράγονται με συμβατικές μεθόδους κινδυνεύουν να σπάσουν λόγω της ραγδαίας ανάπτυξης της κβαντικής υπολογιστικής. Η PKG, η οποία διαφέρει από τις υπάρχουσες προσεγγίσεις στο ότι χρησιμοποιεί την αμοιβαιότητα και την τυχαιότητα του ασύρματου καναλιού για την παραγωγή κλειδιών, επιτρέπει τη γρήγορη ενημέρωση και διανομή κλειδιών χωρίς την ανάγκη υποδομής δημόσιου κλειδιού.

Η PKG έχει αποδείξει την ικανότητα να υλοποιεί επικοινωνία "one-time-pad" με μικρή επιβάρυνση. Η πλειονότητα των συστημάτων TDD χρησιμοποιεί κλειδιά στο φυσικό επίπεδο. Γίνεται εναλλάξ αποστολή πιλότων μεταξύ των δύο πλευρών επικοινωνίας κατά την διάρκεια της περιόδου συνοχής του καναλιού αξιοποιώντας την αμοιβαιότητα του καναλιού. Αυτή η αμοιβαία προσέγγιση εξασφαλίζει τη συλλογή στενά ανάλογων CSI στο φυσικό επίπεδο, οι οποίες στη συνέχεια χρησιμοποιούνται για τη δημιουργία κλειδιών στο φυσικό επίπεδο. Αρκετές έρευνες που έχουν αναπτυχθεί αφορούν συστήματα με μία κεραία ή μικρής κλίμακας συστήματα MIMO, επειδή διαθέτουν επαρκείς πόρους χρόνου-συχνότητας για να εξετάσουν το κανάλι και να αποκτήσουν μεγάλης συσχέτισης CSI. Όταν όμως υπάρχουν περισσότερες κεραίες, αυξάνεται και η επιβάρυνση των πιλότων. Σε συστήματα που περιέχουν πολλές κεραίες, η PKG αντιμετωπίζει τρομερά εμπόδια. Έχουν γίνει λίγες έρευνες για την παραγωγή κλειδιών σε συστήματα massive MIMO. Σε άλλες έρευνες δημιουργήθηκε ένα κοινό κλειδί μεταξύ δύο συσκευών χρησιμοποιώντας τις εικονικές AoAs και AoDs στο χώρο δέσμης. Για να αυξηθεί ο ρυθμός παραγωγής κλειδιών λαμβάνοντας υπόψη την μικρής κλίμακας διακύμανση του καναλιού, προστέθηκε περαιτέρω μια μικρή γωνία διαταραχής στην AoA του πομπού ως κοινή πηγή τυχαιότητας. Όμως αυτές οι έρευνες δεν έλαβαν υπόψη τους τις ταχέως μεταβαλλόμενες CSI και, αντίθετα, χρησιμοποίησαν μόνο τις αργά μεταβαλλόμενες CSI, όπως η AoA και η AoD. Προκειμένου να ελαχιστοποιηθεί η διάσταση του καναλιού και να αντιμετωπιστεί το πρόβλημα της επιβάρυνσης του πιλότου, χρησιμοποιήθηκε ένας προ-κωδικοποιητής και ένας δέκτης. Το σύστημα στενής ζώνης ήταν το μόνο που λήφθηκε υπόψη στις προαναφερθείσες έρευνες με αποτέλεσμα οι κοινώς χρησιμοποιούμενες προσεγγίσεις OFDM να μην ληφθούν υπόψη.

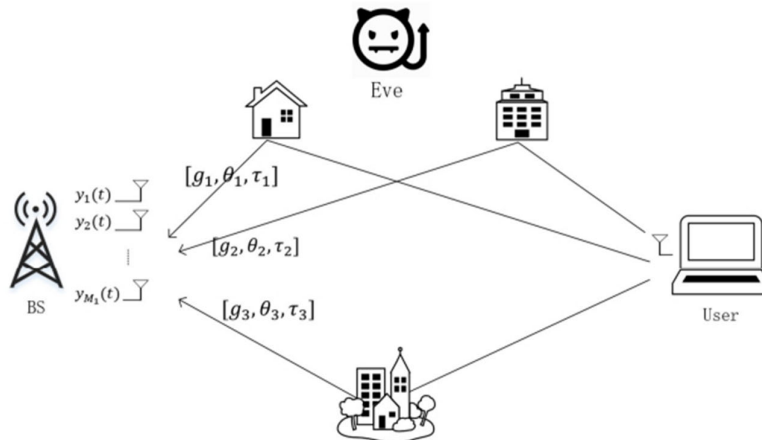
Αυτή η διπλωματική εργασία, ασχολείται με το σύστημα ευρείας ζώνης πολλαπλών κεραιών που διαμορφώνεται με τη χρήση τεχνικών OFDM και παρέχεται μια μοναδική μέθοδος PKG που προκαλεί μικρή επιβάρυνση λόγω πιλότων. Θα γίνει συνδυασμός των τρόπων που αναφέρθηκαν στο Κεφάλαιο 4 δηλαδή χωρίς την χρήση ραντάρ θα γίνει εξαγωγή των CSI και με την χρήση AoA και αυτών, θα παραχθούν τα κλειδιά. Αυτή η προσέγγιση παράγει μακροπρόθεσμα και βραχυπρόθεσμα κλειδιά χρησιμοποιώντας τόσο τις αργά μεταβαλλόμενες όσο και τις γρήγορα μεταβαλλόμενες πληροφορίες κατάστασης καναλιού (CSI), αντίστοιχα. Οι καθυστερήσεις και οι γωνίες των χωρικών χαρακτηριστικών των μονοπατιών στο κανάλι αλλάζουν σταδιακά και αργά με την πάροδο του χρόνου. Τα βραχυπρόθεσμα κλειδιά δημιουργούνται από το αποτέλεσμα εκτίμησης του καναλιού μικρής κλίμακας με πολύ μικρή επιβάρυνση στον πιλότο, ακόμη και όταν το κανάλι μικρής κλίμακας αλλάζει γρήγορα. Για την εκτίμηση της AoA, θα χρησιμοποιηθεί ο

ευρέως διαδεδομένος αλγόριθμος ταξινόμησης πολλαπλών σημάτων (root-MUSIC – Multiple Signal Classification). Τα ιδιοδιανύσματα του πίνακα συσχέτισης της συστοιχίας κεραιών χρησιμεύουν ως βάση για τον αλγόριθμο root-MUSIC [12]. Εξετάζοντας τις ρίζες του πολυωνύμου φάσματος, είναι σε θέση να καθορίσει την εκτίμηση του σήματος. Οι ρίζες του πολυωνύμου που βρίσκονται κοντά στον μοναδιαίο κύκλο αντιστοιχούν στις κορυφές στο χώρο του φάσματος.

Για την δημιουργία των μακροπρόθεσμων κλειδιών, απαιτείται η AoA των πιλότων και η καθυστέρηση διάδοσης. Για την δημιουργία των βραχυπρόθεσμων κλειδιών απαιτείται το πλάτος των πιλότων και η μετατόπιση φάσης (Phase Offset). [11]

6.2 Μοντέλο Συστήματος

Το μοντέλο του συστήματος θα αποτελείται από ένα σύστημα ασύρματης επικοινωνίας TDD OFDM όπως φαίνεται στην παρακάτω Εικόνα 6-1. Η ζώνη άνω/κάτω ζεύξης του καναλιού επικοινωνίας περιλαμβάνει N υποφορείς με απόσταση Δf . Ο σταθμός βάσης (BS – Base Station) που χρησιμοποιείται ως δέκτης διαθέτει μία ομοιόμορφη γραμμική στοιχειοκεραία (ULA – Uniform Linear Array) που αποτελείται από 2 κεραιές. Ο πομπός ή αλλιώς χρήστης διαθέτει μία κεραία. Επίσης θεωρείται και ένας παθητικός υποκλοπέας ο οποίος βρίσκεται σε απόσταση από τον πομπό και τον δέκτη και προσπαθεί να λάβει τα κλειδιά που θα παραχθούν μέσω του καναλιού.



Εικόνα 6-1: Το μοντέλο συστήματος του πειράματος. Στην διπλωματική ο δέκτης έχει 2 κεραιές και ο πομπός 1 κεραία. Υφίστανται εξασθενήσεις στο σήμα λόγω παρεμβολής κτιρίων και αντικειμένων. [11]

Στον τρόπο λειτουργίας ενός TDD συστήματος, μια σημαντική ιδιότητα γνωστή ως αμοιβαιότητα μεταξύ των καναλιών άνω και κάτω ζεύξης που συνδέουν τον BS και τον χρήστη χρησιμοποιείται. Αυτή η αμοιβαιότητα υποδηλώνει ότι τα χαρακτηριστικά που παρατηρούνται στο κανάλι άνω ζεύξης αντικατοπτρίζονται στο κανάλι κάτω ζεύξης. Το κανάλι κατασκευάζεται από πολυάριθμα μονοπάτια διάδοσης, γεγονός που οδηγεί σε αραιή αναπαράσταση. Κάθε μονοπάτι ορίζεται από ένα σύνθετο κέρδος, μια γωνία άφιξης (AoA) ή γωνία αναχώρησης (AoD) και μια χρονική καθυστέρηση. Η προσοχή στρέφεται σε ένα εκτεταμένο χρονικό διάστημα κατά το οποίο τα χωρικά χαρακτηριστικά αυτών των μονοπατιών, συγκεκριμένα οι AoAs/AoDs και οι χρονικές καθυστερήσεις, παραμένουν σχεδόν αμετάβλητα, αλλά τα σύνθετα κέρδη παρουσιάζουν ταχείες

μεταβολές. Αυτό το χρονικό παράθυρο περιλαμβάνει T διακριτές χρονικές στιγμές. Το κανάλι μαθηματικά μπορεί να γραφεί ως:

$$h_m(t) = \sum_{l=1}^L g_l(t) e^{j2\pi m \frac{d}{\lambda} \sin \theta_l} p(\tau_l)$$

με $m=1 \dots M$ όπου M είναι ο συνολικός αριθμός των κεραιών στον BS, L να είναι ο αριθμός των διαδρομών του σήματος, $g_l(t)$ να είναι το κέρδος της l -οστής διαδρομής στην χρονική στιγμή t , $0 < \theta_l < 2\pi$ να είναι η γωνία άφιξης στην άνω ζεύξη και γωνία αναχώρησης στην κάτω ζεύξη, $0 < \tau_l < 1/\Delta_f$ να είναι η καθυστέρηση της l -οστής διαδρομής και $p(\tau_l)$ δηλώνεται ως εξής:

$$p(\tau) = [e^{j2\pi\Delta_f\tau}, e^{j2\pi2\Delta_f\tau}, \dots, e^{j2\pi N\Delta_f\tau}]^T \quad (6.2.2)$$

και δηλώνει την φάση του διανύσματος της OFDM μονάδας. Αφού υφίσταται σήμα πολυδιαδρομής, τότε στον δέκτη φτάνει ένα λαμβανόμενο που ακολουθεί τον παρακάτω τύπο:

$$H(t) = [h_1(t), h_2(t), \dots, h_M(t)]$$

και στην συνέχεια μπορεί να εκφραστεί ως: (6.2.3)

$$H(t) = \sum_{l=1}^L g_l(t) p(\tau_l) a^T(\theta_l) \quad (6.2.4)$$

όπου το a δηλώνεται ως:

$$a(\theta) = \left[e^{j2\pi \frac{d}{\lambda} \sin \theta}, e^{j2\pi 2 \frac{d}{\lambda} \sin \theta}, \dots, e^{j2\pi M \frac{d}{\lambda} \sin \theta} \right]^T \quad (6.2.5)$$

και αποτελεί το διάνυσμα που διαχειρίζονται οι κεραιές του δέκτη.

Στόχος είναι η δημιουργία κλειδιών στο φυσικό επίπεδο σε κάθε διακριτή χρονική στιγμή. Εάν ακολουθηθεί μια προσέγγιση όπου ο BS και ο χρήστης εναλλάσσονται στην εκτίμηση του $H(t)$, ο BS θα έπρεπε να μεταδώσει πιλοτικά σήματα σε M σύμβολα OFDM κατά τη διάρκεια αυτού του συγκεκριμένου χρονικού διαστήματος. Ωστόσο, αυτό θα οδηγούσε σε μια σημαντική επιβάρυνση της κάτω ζεύξης λόγω πιλότων. Για την παράκαμψη αυτού του ζητήματος, η παρούσα διπλωματική υιοθετεί μια εναλλακτική στρατηγική. Αντί να γίνει απευθείας εκτίμηση του εκτεταμένου πίνακα υψηλής διάστασης $H(t)$, αυτή η πρόκληση αντιμετωπίζεται με τη χρήση μιας τεχνικής μείωσης των διαστάσεων. Επιπλέον, αξιοποιούνται τα συμπληρωματικά χαρακτηριστικά της βραδέως μεταβαλλόμενης και της ταχέως μεταβαλλόμενης CSI. Αυτή η από κοινού αξιοποίηση και των δύο τύπων CSI επιτρέπει την επινόηση μιας λύσης που αντιμετωπίζει αποτελεσματικά την ανησυχία της μεγάλης επιβάρυνσης του πιλότου κάτω ζεύξης, ενώ εξακολουθεί να επιτυγχάνει τον στόχο. [11]

6.3 Παραγωγή Κλειδιών

Σε αυτή την ενότητα παρουσιάζονται οι μέθοδοι με τους οποίους θα παραχθούν τα κλειδιά. Υπάρχουν δύο ειδών κλειδιά: τα βραχυπρόθεσμα τα οποία παράγονται από την γρήγορα μεταβαλλόμενη CSI και τα μακροπρόθεσμα τα οποία παράγονται από την αργώς μεταβαλλόμενη CSI.

6.3.1 Παραγωγή μακροπρόθεσμων κλειδιών

Για την παραγωγή μακροπρόθεσμων κλειδιών θα ληφθεί υπόψη οι αργώς μεταβαλλόμενες CSI. Αυτές είναι η γωνία άφιξης και η καθυστέρηση διάδοσης της 1-οστής διαδρομής και οι οποίες παραμένουν σχεδόν σταθερές καθ' όλη την περίοδο επικοινωνίας.

Αρχικά πρέπει να εκτιμηθούν οι AoAs/AoDs τόσο στον πομπό όσο και στον δέκτη. Για αυτή την περίπτωση θα χρησιμοποιηθεί ο αλγόριθμος root-MUSIC ο οποίος θα υπολογίσει σε μοίρες τις AoAs/AoDs κάθε διαδρομής. Συγκεκριμένα, ακολουθούνται ορισμένα βήματα για την επίτευξη αυτού:

1. Καθορισμός του προβλήματος: Υπάρχουν 2 κεραίες στον δέκτη και 1 κεραία στον πομπό και απέχουν μεταξύ τους μία απόσταση. Στις κεραίες προσπίπτουν πολλαπλά σήματα από διαφορετικές κατευθύνσεις. Στόχος η εύρεση των γωνιών από τις οποίες φτάνουν τα σήματα αυτά
2. Συλλογή δεδομένων: Καθεμία από τις 2 κεραίες που διαθέτει ο δέκτης εκτιμά το λαμβανόμενο σήμα για ένα συγκεκριμένο χρονικό διάστημα. Για την επίτευξη αυτού δημιουργείται ένας πίνακας δεδομένων X με διαστάσεις M (αριθμός κεραιών) επί N (αριθμός χρονικών δειγμάτων).
3. Υπολογισμός του πίνακα συνδιακύμανσης (συμμεταβλητότητας): Υπολογίζεται ο πίνακας συνδιακύμανσης του δείγματος $R=XX^H$ (όπου X^H είναι ο συζυγής ανάστροφος του X). Το R είναι μία εκτίμηση της συνδιακύμανσης των λαμβανόμενων σημάτων στις κεραίες.
4. Αποσύνθεση ιδιοτιμών: Εκτέλεση της ανάλυσης ιδιοτιμών (EVD – Eigen-Value Decomposition) του πίνακα συνδιακύμανσης $R=V\Lambda V^H$ όπου V είναι ο πίνακας των ιδιοδιανυσμάτων και Λ είναι ένας διαγώνιος πίνακας ιδιοτιμών. Γίνεται ταξινόμηση των ιδιοτιμών κατά φθίνουσα σειρά και αναδιάταξη ανάλογα τα αντίστοιχα ιδιοδιανύσματα.
5. Εκτίμηση του υποχώρου σήματος: Τα ιδιοδιανύσματα θορύβου καλύπτουν τον υποχώρο θορύβου. Γίνεται επιλογή των πρώτων $M-L$ ιδιοδιανυσμάτων, όπου L είναι ο αριθμός των πηγών (σημάτων). Αυτά τα ιδιοδιανύσματα αντιπροσωπεύουν τον υποχώρο σήματος και καλύπτουν τις AoAs/AoDs.
6. Κατασκευή του φάσματος MUSIC: Για κάθε πιθανή κατεύθυνση θ , υπολογίζει το διάνυσμα $a(\theta)$ που αντιπροσωπεύει τις διαφορές φάσης που εισάγονται από τα σήματα που φτάνουν από αυτή την κατεύθυνση στις κεραίες. Υπολογίζει το φάσμα MUSIC για την κατεύθυνση θ ως:

$$S(\theta) = \frac{1}{\|a(\theta)^H V_N\|^2} \quad (6.3.1.1)$$

όπου V_N είναι ο πίνακας υποχώρου θορύβου.

7. Εντοπισμός των κορυφών στο φάσμα: Ο αριθμός των κορυφών αντιστοιχεί στον αριθμό των πηγών που υπάρχουν. Οι AoAs/AoDs καθορίζονται από τις γωνίες που αντιστοιχούν σε αυτές τις κορυφές.
8. Εκτίμηση AoAs/AoDs: Μετατροπή των γωνιών που αντιστοιχούν στις κορυφές του φάσματος MUSIC σε εκτιμώμενες AoAs/AoDs.
9. Βελτίωση ανάλυσης: Ο τυπικός αλγόριθμος MUSIC μπορεί να έχει ανεπαρκή ανάλυση όταν οι πηγές βρίσκονται σε μικρή απόσταση μεταξύ τους. Στην περίπτωση που παρουσιάζεται στην διπλωματική, ο αλγόριθμος root-MUSIC βελτιώνει την ανάλυση με την εύρεση των ριζών του πολυωνύμου MUSIC. Κάθε ρίζα αντιστοιχεί σε μια AoA/AoD.

10. Υπολογισμός ρίζας (root): Κατασκευή του πολωνύμου MUSIC χρησιμοποιώντας τα ιδιοδιανύσματα του υποχώρου θορύβου και το διάνυσμα $a(\theta)$. Εύρεση των ριζών του πολωνύμου. Ο αριθμός των διακριτών ριζών ισούται με τον αριθμό των πηγών.
11. Υπολογισμός AoA/AoD με χρήση των ριζών: Μετατροπή των ριζών του πολωνύμου MUSIC στις εκτιμώμενες AoAs/AoDs. Οι ρίζες παρέχουν πιο ακριβείς εκτιμήσεις, ειδικά για πηγές που βρίσκονται σε κοντινή απόσταση μεταξύ τους.

Μετά από αυτό πρέπει να εκτιμηθεί η καθυστέρηση της l -οστής διαδρομής η οποία θα υπολογιστεί μέσα από την διαφορά του χρόνου έναρξης εκπομπής του σήματος στον πομπό και της άφιξης του σήματος στον δέκτη.

Έτσι όλα τα στοιχεία που χρειάζονται για την παραγωγή του κλειδιού είναι διαθέσιμα. Δημιουργείται ένας πίνακας Ω ο οποίος ορίζεται ως $\Omega = \{\text{AoA/AoD}, \tau\}$. Μετά, και με χρήση του κώδικα Gray τα δεκαδικά νούμερα AoA/AoD και τ , μετατρέπονται σε δυαδικούς αριθμούς. Τέλος δημιουργείται ένας πίνακας K οποίος ορίζεται ως $K = \{\text{AoA/AoD}, \tau\}$ και περιέχει τα δυαδικά νούμερα που προκύπτουν από τον κώδικα Gray. Ο πίνακας αυτός αποτελεί το μακροπρόθεσμο κλειδί. [11]

6.3.2 Παραγωγή βραχυπρόθεσμων κλειδιών

Εκτός από τα μακροπρόθεσμα κλειδιά, για περισσότερη ασφάλεια παράγεται και ένας δεύτερος τύπος κλειδιών που είναι τα βραχυπρόθεσμα κλειδιά. Για την παραγωγή βραχυπρόθεσμων κλειδιών θα ληφθεί υπόψη οι γρήγορα μεταβαλλόμενες CSI. Αυτές είναι το πλάτος και φάση για κάθε υποφορέα. Αρχικά γίνεται απομόνωση των πιλότων μετά την OFDM με την βοήθεια της συνάρτησης:

$$y(t) = \sqrt{P}h(t) + z(t) \quad (6.3.2.1)$$

όπου $z(t)$ είναι ο πρόσθετος λευκός γκαουσιανός θόρυβος. Από αυτούς τους πιλότους, χρησιμοποιούνται οι πληροφορίες πλάτους και φάσης για να δημιουργηθούν τα βραχυπρόθεσμα κλειδιά. Γίνεται συγκέντρωση όλων των πλάτων των υποφορέων N σε έναν πίνακα (για λόγους απλούστευσης δεν λαμβάνεται υπόψη):

$$M = [M(1), M(2), \dots, M(N)] \quad (6.3.2.2)$$

Στην συνέχεια γίνεται ποσοτικοποίηση του πλάτους ακολουθώντας τον παρακάτω μαθηματικό τύπο:

$$K = \begin{cases} 1, & M(n) > q_+ \\ 0, & M(n) < q_- \\ x, & \text{αλλού} \end{cases} \quad (6.3.2.3)$$

όπου το K είναι το κλειδί, $q_+ = \text{mean} + a \cdot \sigma$, $q_- = \text{mean} - a \cdot \sigma$, με mean να αποτελεί το μέσο πλάτος, a ένα κατώτατο όριο και το σ η τυπική απόκλιση. Μετά, με την χρήση ενός αλγορίθμου level-crossing που παρουσιάζεται στην βιβλιογραφία [13], ανακτάται ένα διάνυσμα p το οποίο περιέχει τις θέσεις που υπάρχει x εντός του K . Με λίγα λόγια, το p γράφεται ως $p = [x_1, x_2, \dots, x_{L_m}]$ με L_m να είναι το μήκος του κλειδιού. Αυτός ο αλγόριθμος βρίσκει μέσα στο K τις θέσεις που υπάρχει x . Αν για παράδειγμα $K = [0, 0, x, 1, x, 1]$, τότε το $p = [2, 4]$. Στην συνέχεια αντικαθιστά τα x σε αυτές τις θέσεις με 0. Δηλαδή το τελικό K θα γίνει $K = [0, 0, 0, 1, 0, 1]$.

Επιπλέον, η ίδια ακριβώς διαδικασία ακολουθείται και για την φάση κάθε πιλότου. Το τελικό βραχυπρόθεσμο κλειδί θα είναι $K = [\text{κλειδί με βάση το πλάτος}, \text{κλειδί με βάση την φάση}]$. [11]

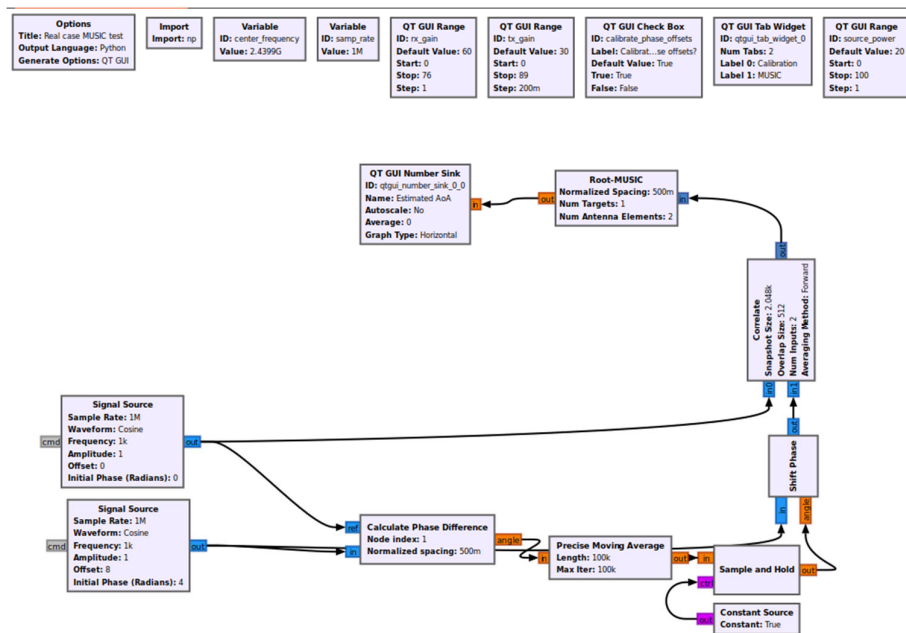
6.4 Υλοποίηση στο GNU Radio

Σε αυτή την ενότητα παρουσιάζονται όλα τα βήματα που ακολουθήθηκαν για να επιτευχθεί το πείραμα με την χρήση του απαραίτητου εργαλείου GNU Radio. Στην πρώτη υποενότητα αυτής της ενότητας παρουσιάζονται τα παρασκευαστικά βήματα που χρειάζονται για να αρχίσει το πείραμα και στην δεύτερη υποενότητα παρουσιάζονται τα βήματα του ολοκληρωμένου πειράματος.

6.4.1 Προπαρασκευαστικά βήματα

Για την εύρεση της εικονική γωνίας άφιξης αλλά και της διαφοράς φάσης ανάμεσα στις 2 κεραίες του δέκτη, χρειάζεται ο αλγόριθμος root-MUSIC και ο αλγόριθμος για την διαφορά φάσης οι οποίοι είναι υλοποιημένοι από την Ettus Research και ανταποκρίνονται πλήρως στα προϊόντα της (USRP). Έτσι η διπλωματική έλαβε υπόψη τους έτοιμους κώδικες σε γλώσσα C++ για το GNU Radio.

Για τον λόγο ότι οι παραπάνω κώδικες είναι έτοιμοι, θα πρέπει να δοκιμαστούν σύμφωνα με τα παραδείγματα που συνοδεύονται. Έτσι σύμφωνα με τα αρχεία της Ettus Research δημιουργείται το παρακάτω διάγραμμα το οποίο απεικονίζει την εύρεση της γωνίας άφιξης για ένα σύστημα δέκτη με 2 κεραίες.

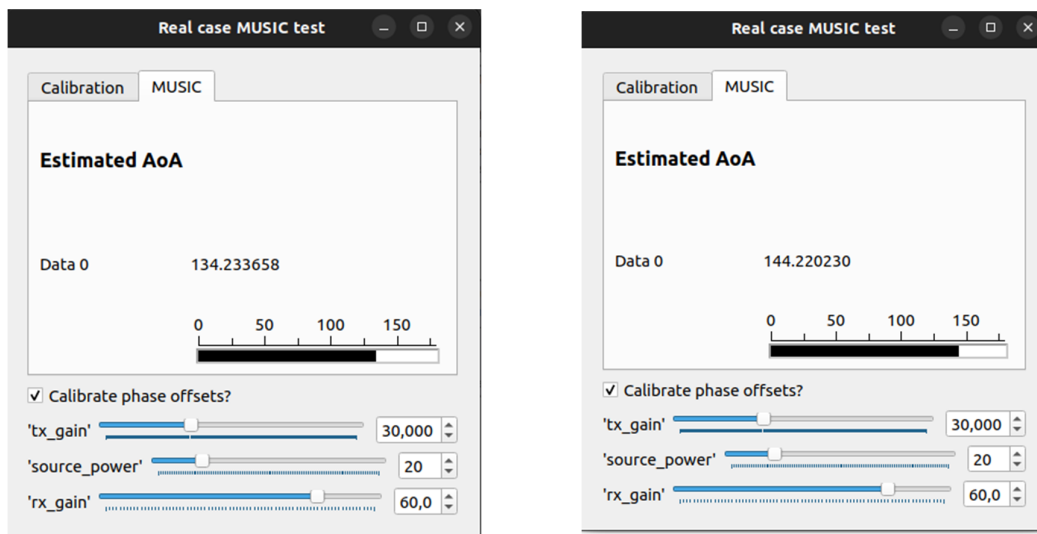


Εικόνα 6-2: Δέκτης για την εύρεση της γωνίας άφιξης. Τα blocks “Signal Source” αφορούν τις κεραίες του δέκτη.

Στην παραπάνω εικόνα (Εικόνα 6-2) απεικονίζεται ένας δέκτης ο οποίος με την βοήθεια κατάλληλων αλγορίθμων θα υπολογίσει την γωνία άφιξης. Αρχικά υπάρχουν δύο κεραίες στον δέκτη. Αυτές είναι τα δύο blocks “Signal Source”. Το σήμα για το οποίο θα βρεθεί η γωνία άφιξης είναι ένα συνημίτονο με συχνότητα 1000 Hz, πλάτος 1, διαφορά φάσης 4 radians και μετατόπιση κατά 8 μονάδες. Στην συνέχεια, πρέπει να βρεθεί η διαφορά φάσης ανάμεσα στις 2 κεραίες (block “Calculate Phase Difference”). Χρήσιμη παράμετρος είναι η απόσταση μεταξύ των δύο κεραιών του δέκτη η οποία χρησιμοποιείται για την εύρεση της σταθεράς διαφοράς φάσης. Ακολουθεί ο υπολογισμός του συζυγή ανάστροφου πίνακα του σήματος των δύο κεραιών και στην συνέχεια ο

πολλαπλασιασμός αυτού με την σταθερά διαφοράς φάσης. Στο τελικό στάδιο, για το αποτέλεσμα θα βρεθεί η εφαπτομένη τόξου (atan2) που αντιστοιχεί στην διαφορά φάσης που απαιτείται. Έπειτα, η έξοδος αυτού του block, περνάει σε ένα άλλο block “Precise Moving Average” για την εκτίμηση του κινούμενου (ολισθαίνοντος) μέσου όρου των φάσεων. Ύστερα, ο κινούμενος μέσος όρος μπαίνει σε ένα block “Sample and Hold” το οποίο προωθεί μόνο την ροή δεδομένων όταν στο σήμα ελέγχου υπάρχει 1 αντί για 0. Η έξοδος αυτού που είναι ο κινούμενος μέσος όρος της διαφοράς φάσης που χρησιμοποιείται ώστε να βρεθεί η ολίσθηση/μετατόπιση φάσης (block “Shift Phase”). Αυτό το μπλοκ, πρακτικά, λαμβάνει το σήμα από την δεύτερη κεραία και το πολλαπλασιάζει με τον μέσο όρο της διαφοράς φάσης ώστε να εξαχθεί το σήμα της δεύτερης κεραίας ολισθημένο κατά την διαφορά φάσης. Ουσιαστικά, το σήμα που λαμβάνει η πρώτη κεραία θα πρέπει να συσχετιστεί με το ολισθημένο της δεύτερης κεραίας (block “Correlate”). Για αυτό τον λόγο, με είσοδο τα δύο σήματα και καθορισμένο τον αριθμό των δειγμάτων που χρησιμοποιούνται για τον υπολογισμό του πίνακα συσχέτισης δειγμάτων, εφαρμόζεται η συνάρτηση αυτοσυσχέτισης. Αφού γίνει η συσχέτιση, η έξοδος εισέρχεται στο block “Root-MUSIC” προκειμένου να υπολογιστεί η γωνία άφιξης (ανάλυση στην Ενότητα 6.3.1). Η έξοδος του block “Root-MUSIC” είναι ένας καθαρός αριθμός float που αντιστοιχεί στις μοίρες της γωνίας.

Από την εκτέλεση του διαγράμματος της Εικόνας 6-2, εμφανίζεται ένα παράθυρο στο περιβάλλον του GNU Radio το οποίο αναγράφει την ακριβή γωνία άφιξης εκείνη την χρονική στιγμή. Αυτό το νούμερο κυμαίνεται από 134 έως 144 μοίρες.



Εικόνα 6-3: Αποτελέσματα εκτέλεσης του διαγράμματος της Εικόνας 6-2 που παρουσιάζει την εύρεση της Γωνίας Άφιξης (AoA)

Από την παραπάνω Εικόνα 6-3 παρατηρείται ότι το πραγματικό σενάριο χρήσης για την εύρεση της γωνίας άφιξης λειτουργεί. Έτσι μπορεί να γίνει η έναρξη της υλοποίησης του πραγματικού πειράματος.

6.4.2 Κυρίως Πείραμα

Αφού έγινε ο έλεγχος για τα blocks που χρησιμοποιήθηκαν από προηγούμενα GNUradio έργα, κατασκευάστηκαν ορισμένα blocks που θα βοηθήσουν για την απομόνωση των πιλότων, την

μέτρηση του χρόνου την στιγμή που ανιχνευτεί πακέτο, την παραγωγή του short-term κλειδιού και την παραγωγή του long-term κλειδιού.

Για να μεταδοθεί ένα σήμα, θα πρέπει να υπάρχει ένας πομπός (Εικόνα 6-7). Πομπός για το σύστημα που θα υλοποιηθεί για την διπλωματική, είναι μία ψηφιακή πηγή (random source) η οποία θα δημιουργεί ένα τυχαίο σήμα σε bytes. Χρησιμοποιείται ένα Stream to Tagged Stream block το οποίο πακετοποιεί την ροή με μήκος 35 το κάθε πακέτο. Μετά ακολουθεί ο OFDM διαμορφωτής με 4 πιλότους και με μετασχηματισμό Fourier μήκους 64. Αφού γίνει η διαμόρφωση τότε πρέπει να συλληφθεί ο χρόνος κατά τον οποίο βρέθηκε ένα πακέτο. Για να βρεθεί ένα πακέτο, χρησιμοποιείται το μπλοκ Schmidl & Cox Synch. το οποίο στην έξοδό του βγάζει 1 όταν βρει πακέτο. Ακολουθεί ένα μπλοκ για την μετατροπή των bytes σε float και στην συνέχεια ένα Python μπλοκ το οποίο θα λαμβάνει το 1 του μπλοκ Schmidl & Cox Synch. και θα καταγράφει την συγκεκριμένη χρονική στιγμή σε milliseconds. Αυτός ο χρόνος θα χρησιμοποιηθεί για την εύρεση της καθυστέρησης διάδοσης του σήματος. Ο χρόνος αυτός είναι μικρότερος από τον χρόνο που θα καταγραφεί στον δέκτη. Προκειμένου να μπορέσει να φτάσει στον δέκτη και να γίνει η αφαίρεση της χρονικής στιγμής εύρεσης πακέτου στον δέκτη πλην την χρονική στιγμή εύρεσης πακέτου στον πομπό, θα χρησιμοποιηθεί το κοινό δίκτυο WiFi. Έτσι με το μπλοκ ZMQ PUB Message Sink, η χρονική στιγμή εύρεσης πακέτου στον πομπό θα μεταδοθεί ως μήνυμα μέσω του κοινού δικτύου WiFi προς τον δέκτη χρησιμοποιώντας την IP διεύθυνσή του. Από την έξοδο του OFDM διαμορφωτή, εξάγεται το διαμορφωμένο σήμα σε ένα Sink που αντιστοιχεί στο USRP Sink.

Ο δέκτης (Εικόνα 6-8) έχει δύο εισόδους αφού είναι σχεδιασμένος με δύο κεραίες για την προσομοίωση ενός MIMO συστήματος. Για αυτό χρησιμοποιείται ένα USRP με δύο κεραίες με αποτέλεσμα το σήμα να λαμβάνεται και από τις δύο κεραίες. Πρακτικά, για τον δέκτη θα δημιουργηθούν δύο flowgraphs δηλαδή 2 OFDM αποδιαμορφώσεις. Για τις ανάγκες του συγχρονισμού, το USRP Source οδηγείται σε ένα μπλοκ Schmidl & Cox Synch. όπου ανιχνεύεται η μετατόπιση φάσης, πολλαπλασιάζεται με το σήμα που έχει καθυστέρηση 80 δείγματα (64 από τον μετασχηματισμό Fourier και άλλα 16 από το μήκος του κυκλικού προθέματος που χρησιμοποιείται από την αποδιαμόρφωση του OFDM σήματος) και με ακόμη μία καθυστέρηση 118 δειγμάτων (καθυστέρηση επεξεργασίας του finesync block) οδηγείται σε ένα μπλοκ Payload/Header Demux προκειμένου να διαχωριστεί το Payload από το Header Stream. Επίσης, το μπλοκ Schmidl & Cox Synch., όταν ανιχνεύσει πακέτο, καταγράφει την συγκεκριμένη χρονική στιγμή με την βοήθεια του get Time μπλοκ και υπολογίζεται η συνολική καθυστέρηση διάδοσης αφαιρώντας την χρονική στιγμή ανίχνευσης πακέτου στον δέκτη από εκείνη του πομπού αφού ληφθεί πρώτα ως μήνυμα με την βοήθεια του μπλοκ ZMQ SUB Message Source. Αυτή η καθυστέρηση αποθηκεύεται σε ένα virtual sink για την εύκολη χρήση του στο μπλοκ που παράγει τα κλειδιά. Το μπλοκ Payload/Header Demux διαχωρίζει την επικεφαλίδα η οποία περιέχει πληροφορίες σχετικά με το μέγεθος και την δρομολόγηση του εκάστοτε πακέτου, από το ωφέλιμο φορτίο το οποίο περιέχει το μήνυμα που μεταδίδεται δηλαδή το περιεχόμενο της μετάδοσης. Για να γίνει αυτό, πρέπει πρώτα να γίνει πιο ακριβής συγχρονισμός σήματος με το μπλοκ finesync το οποίο ελαττώνει το σφάλμα του μπλοκ Schmidl & Cox Synch. (που πραγματοποιεί coarse synchronization) όταν ανιχνεύει 1. Κατά το block Schmidl & Cox Synch κτιμάται και η μετατόπιση της συχνότητας από μία ακολουθία παναλαμβανόμενων δειγμάτων που αποστέλλονται σε κάθε frame (preambles). Καταγράφεται λοιπόν η χρονική στιγμή μέγιστης συσχέτισης με το preamble που υποδηλωθεί την έναρξη του πακέτου, ενώ γίνεται και διόρθωση σφάλματος συχνότητας. Στην συνέχεια η κεφαλίδα του πακέτου

μετά από τον μετασχηματισμό Fourier, υπόκεινται σε εκτίμηση καναλιού (OFDM Channel Estimation). Επακολούθως εκτελείται εξισορρόπηση σε μία ή δύο διαστάσεις σε ένα tagged OFDM frame (OFDM Frame Equalizer). Ακολουθεί η σειριοποίηση των μιγαδικών συμβόλων διαμόρφωσης από τους υποφορείς της OFDM (OFDM Serializer). Μόλις τελειώσει αυτή η διαδικασία, γίνεται αποκωδικοποίηση των σημείων του αστερισμού από έναν σύνθετο χώρο σε (μη πακετοποιημένα) bits με βάση την είσοδο (Constellation Decoder) και στην συνέχεια ακολουθεί ανάλυση των κεφαλίδων των πακέτων (Packet Header Parser). Η πληροφορία οδηγείται στο Header/Payload Demux ως μήνυμα feedback, έτσι ώστε να γίνει γνωστό το μέγεθος και ο τύπος του payload. Η ίδια διαδικασία ακολουθείται και για το payload χωρίς όμως να γίνει ανάλυση των κεφαλίδων (Εικόνα 6-9). Από το FFT του Payload θα γίνει διαίρεση του πλάτους με το μήκος του μετασχηματισμού FFT και μετά θα γίνει η απομόνωση των πιλότων με την βοήθεια του μπλοκ `keep_pilots`. Για να επιτευχθεί η απομόνωση των πιλότων, θα ληφθούν οι θέσεις των πιλότων (π.χ. $\{-21, -7, 7, 21\}$) και οι αρνητικές θέσεις θα προστεθούν με το μήκος του FFT λόγω της φασματικής αναδίπλωσης των αρνητικών συχνοτήτων (π.χ. οι πιλότοι είναι στις θέσεις $-21+64=43$, $-7+64=57$, 21 και 7). Στην συνέχεια θα πρέπει να γίνει η εύρεση της διαφοράς φάσης ανάμεσα στα σήματα των δύο κεραίων (ανάλυση στην Ενότητα 6.4.1). Ακολουθεί η συσχέτιση μεταξύ των σημάτων που καταφθάνουν στις δύο κεραίες και σύμφωνα με την διαφορά φάσης τους, η εύρεση της φάσης και του πλάτους των πιλότων και στην συνέχεια η εύρεση της γωνίας άφιξης με την χρήση του αλγορίθμου root-MUSIC.

Για τη παραγωγή των κλειδιών (Εικόνα 6-10) χρειάζονται δύο μπλοκ. Το πρώτο αφορά την παραγωγή του μακροπρόθεσμου κλειδιού και το δεύτερο την παραγωγή του βραχυπρόθεσμου κλειδιού. Στο πρώτο μπλοκ, για την παραγωγή του κλειδιού χρειάζονται η γωνία άφιξης η οποία εισάγεται στο μπλοκ ως virtual source και η καθυστέρηση διάδοσης μεταξύ πομπού και δέκτη η οποία εισάγεται κι εκείνη στο μπλοκ ως virtual source. Το κλειδί που παράγεται μέσω του αλγορίθμου που τρέχει το μπλοκ (ανάλυση στην Ενότητα 6.4.4 και στην Ενότητα 6.3.1), αποθηκεύεται σε ένα δυαδικό αρχείο για την εύκολη και γρήγορη ανάγνωσή του και χρήση του. Στο δεύτερο μπλοκ, για την παραγωγή του κλειδιού χρειάζονται το πλάτος και η φάση. Χρησιμοποιείται το μπλοκ Complex to Mag Phase για τον διαχωρισμό του πλάτους από την φάση (Εικόνα 6-9) και αποθηκεύονται σε δύο διαφορετικά sinks που αφορά το πλάτος και την φάση. Στην συνέχεια εισάγονται και τα δύο στο μπλοκ ως virtual sources και το κλειδί που παράγεται μέσω του αλγορίθμου που τρέχει το μπλοκ (ανάλυση στην Ενότητα 6.4.4 και στην Ενότητα 6.3.2), αποθηκεύεται σε ένα δυαδικό αρχείο για την εύκολη και γρήγορη ανάγνωσή του και χρήση του. Έτσι, το flowgraph με την χρήση των USRPs ως πειραματικό εξοπλισμό παράγει τα κλειδιά που απαιτούνται και αποθηκεύονται σε αρχεία για κάθε χρήση.

6.4.3 Επεξήγηση των μπλοκς του διαγράμματος

- Virtual Source: Εικονική πηγή για την «αναπαραγωγή» του εξαγόμενου σήματος από την διαμόρφωση OFDM.
- UHD: USRP Sink: Η εκπομπή του διαμορφωμένου σήματος μέσω του εξοπλισμού USRP.
- UHD: USRP Source: Η λήψη του διαμορφωμένου σήματος μέσω του εξοπλισμού USRP για την αποδιαμόρφωσή του και την παραγωγή των απαιτούμενων κλειδιών.
- Stream to Tagged Stream: Μετατρέπει μια κανονική ροή σε ροή με ετικέτες (GNUradio specific).

- Random Source: Πηγή που δημιουργεί έναν αριθμό δειγμάτων τυχαίων αριθμών [min, max) που σημαίνει ότι η μέγιστη τιμή δεν θα συμπεριληφθεί.
- IChar To Complex: Μετατροπή ροής αλληλοδιαδοχικών χαρακτήρων σε ροή μιγαδικών αριθμών (με χρήση ASCII).
- OFDM Transmitter: Ιεραρχικό μπλοκ για διαμόρφωση OFDM.
- Schmidl & Cox OFDM synch.: Εξάγει την μετατόπιση συχνότητας, ως κλάσμα τις απόστασης μεταξύ δυο διαδοχικών υποφορέων OFDM και την (κατά προσέγγιση) αρχή του πρώτου συμβόλου OFDM μετά το πρώτο (διπλασιασμένο/επαναλαμβανόμενο) σύμβολο OFDM. Η αρχή επισημαίνεται με ένα 1 (παντού αλλού είναι 0). Πρωταρχικός σκοπός του είναι η επίτευξη συγχρονισμού μεταξύ πομπού και δέκτη παρουσία μετατόπισης της φέρουσας συχνότητας. Παρόλα αυτά, λόγω κυκλικού προθέματος και δομής έχει σφάλμα.
- Complex to Imag: Βγάζει το φανταστικό μέρος μιας ροής μιγαδικών αριθμών.
- Virtual Sink: Κατάληξη του τελικού σήματος μετά την επεξεργασία (καταβόθρα). Το sink μπορεί να χρησιμοποιηθεί από ένα virtual source σε άλλο σημείο του flowchart.
- Frequency Mod: Αυτό το μπλοκ είναι ένα μιγαδικό ημίτονο ελεγχόμενου πλάτους εισόδου. Βγάζει ένα σήμα, το οποίο έχει μια διαδοχική αύξηση της φάσης που είναι ανάλογη της ευαισθησίας και του πλάτους εισόδου.
- Delay: Καθυστέρηση της εισόδου κατά έναν ορισμένο αριθμό δειγμάτων.
- Header/Payload Demux: Αυτό το μπλοκ έχει σχεδιαστεί για την αποπολυπλεξία πακέτων από μια διαδοχική μετάδοση. Η τυπική εφαρμογή για αυτό το μπλοκ είναι η περίπτωση που λαμβάνονται πακέτα με μήκος που δεν έχει ακόμη καθοριστεί. Αυτό το μπλοκ θα περάσει το τμήμα επικεφαλίδας σε άλλα μπλοκ για αποδιαμόρφωση. Χρησιμοποιώντας τις πληροφορίες από την αποδιαμορφωμένη επικεφαλίδα, στη συνέχεια θα εξάγει το ωφέλιμο φορτίο. Η αρχή της επικεφαλίδας πρέπει να αναγνωρίζεται από ένα σήμα ενεργοποίησης.
- Finesync: Αυτό το μπλοκ δημιουργήθηκε στα πλαίσια της διπλωματικής για να ελαττώσει το σφάλμα του μπλοκ Schmidl & Cox Synch. όταν αυτό ανιχνεύει 1 προκειμένου να είναι πιο ξεκάθαρη η αρχή του σήματος. Αυτό θα βοηθήσει στην βελτίωση του συγχρονισμού και έτσι στην λήψη καλύτερων αποτελεσμάτων.
- Get time (πομπού): Όταν βλέπει 1 στην είσοδό του, καταγράφει την χρονική στιγμή. Αν βλέπει οτιδήποτε άλλο δεν καταγράφει τίποτα. Βοηθά στην εύρεση της καθυστέρησης διάδοσης. Στην συνέχεια μετατρέπει αυτό τον χρόνο σε μήνυμα για την μετάδοσή του μέσω του μπλοκ ZMQ PUB Message Sink στον δέκτη με την χρήση της IP του στο κοινό δίκτυο.
- Get time (δέκτη): Όταν βλέπει 1 στην είσοδό του, καταγράφει την χρονική στιγμή. Αν βλέπει οτιδήποτε άλλο δεν καταγράφει τίποτα. Βοηθά στην εύρεση της καθυστέρησης διάδοσης. Στην συνέχεια μετατρέπει αυτό τον χρόνο σε μήνυμα για εισαγωγή του στο μπλοκ που θα υπολογίσει την καθυστέρηση διάδοσης δηλαδή την αφαίρεση από την χρονική στιγμή του δέκτη πλην εκείνη του πομπού.
- Time diff source: Λαμβάνει το μήνυμα της χρονικής στιγμής άφιξης πακέτου στον δέκτη και το μήνυμα της χρονικής στιγμής άφιξης πακέτου στον πομπό (μέσω λήψης του μηνύματος από το κοινό δίκτυο με χρήση της IP του πομπού στο μπλοκ ZMQ SUB Message Source) και αφαιρεί το πρώτο από το δεύτερο για να βρει την συνολική καθυστέρηση διάδοσης.

- FFT: Αυτό το μπλοκ δέχεται ένα διάνυσμα πραγματικών ή μιγαδικών τιμών και υπολογίζει τον μετασχηματισμό Fourier.
- OFDM Channel Estimation: Εκτίμηση του καναλιού και της μετατόπισης συχνότητας για OFDM από τα preambles (μία ακολουθία γνωστών bits που αποστέλλονται σε κάθε frame).
- OFDM Frame Equalizer: Εκτελεί εξισορρόπηση σε μία ή δύο διαστάσεις σε ένα πλαίσιο OFDM με ετικέτα. Αυτό κάνει δύο πράγματα: Πρώτον, αφαιρεί τη μετατόπιση φέροντος. Εάν βρεθεί μια ετικέτα στο πρώτο στοιχείο με το κλειδί 'ofdm_sync_carr_offset', αυτό ερμηνεύεται ως η μετατόπιση συχνότητας σε αριθμό φερόντων. Στη συνέχεια, εκτελεί εξισορρόπηση σε μία ή δύο διαστάσεις σε ένα πλαίσιο OFDM με ετικέτα. Η πραγματική ισοστάθμιση γίνεται από ένα αντικείμενο ofdm_frame_equalizer, εκτός του μπλοκ.
- OFDM Serializer: Σειριοποιεί μιγαδικά σύμβολα διαμόρφωσης από υποφορείς OFDM. Εξάγει τα μιγαδικά σύμβολα δεδομένων ως ροή με ετικέτες, απορρίπτοντας τα σύμβολα πιλότου. Εάν δοθεί, αναλύονται δύο διαφορετικές ετικέτες: Το πρώτο κλειδί (Length Tag Key) καθορίζει τον αριθμό των συμβόλων OFDM στο πλαίσιο στην είσοδο. Το δεύτερο κλειδί (Packet Length Tag Key) καθορίζει τον αριθμό των μιγαδικών συμβόλων που κωδικοποιούνται σε αυτό το πλαίσιο. Εάν δίνεται, αυτό το δεύτερο κλειδί χρησιμοποιείται στην έξοδο, διαφορετικά χρησιμοποιείται το Length Tag Key (κλειδί μήκους ετικέτας). Εάν δίνονται και τα δύο, το μήκος πακέτου καθορίζει τον μέγιστο αριθμό στοιχείων εξόδου και το μήκος πλαισίου καθορίζει τον ακριβή αριθμό των στοιχείων εισόδου που καταναλώνονται.
- Constellation Decoder: Αποκωδικοποίηση των σημείων ενός μιγαδικού σηματοστερισμού σε (μη πακετοποιημένα) bits με βάση τον κανόνα αντιστοίχισης του αντικειμένου διαμόρφωσης.
- Packet Header Parser: Δημοσιεύει μεταδεδομένα κεφαλίδας ως πολυμορφικούς τύπους (PMT – PolyMorphic Types). Οι πολυμορφικοί τύποι απλοποιούν τη μεταβίβαση μηνυμάτων μεταξύ μπλοκ, καθώς όλα τα δεδομένα είναι του ίδιου τύπου, συμπεριλαμβανομένου του μηνύματος.
- Vector to Stream: Μετατροπή μιας ροής διανυσμάτων σε ροή στοιχείων
- Multiply Const: Πολλαπλασιάζει τη ροή εισόδου με μια βαθμωτή ή διανυσματική σταθερά (στοιχείο προς στοιχείο αν πρόκειται για διάνυσμα).
- keep pilots: Απομονώνει τους πιλότους από όλη την ροή σύμφωνα με τις θέσεις των πιλότων. Το block κατασκευάστηκε σε C++ στα πλαίσια της διπλωματικής.
- Calculate Phase Difference: Υπολογίζει την διαφορά φάσης ανάμεσα στα σήματα που λαμβάνουν οι δύο κεραίες.
- Complex to Mag Phase: Μετατρέπει μια μιγαδική ροή σε πλάτος και φάση (και τα δύο float). Η πρώτη έξοδος είναι το πλάτος και η δεύτερη είναι η φάση (σε ακτίνια).
- Shift Phase: Η μετατόπιση φάσης ανάμεσα στα σήματα δύο κεραιών κατά μία τιμή ακτινίων που καθορίζεται από την είσοδο.
- Precise Moving Average: Ακριβής έκδοση του κινούμενου μέσου όρου που χρησιμοποιεί συσσωρευτή τύπου double για να επιτρέπει μεγαλύτερα μήκη διαστήματος και μεγαλύτερο απαιτούμενο αριθμό μέγιστων επαναλήψεων που επιτρέπουν ακριβέστερα αποτελέσματα.
- Root MUSIC: Αυτό το μπλοκ χρησιμοποιεί τον αλγόριθμο Root-MUSIC για τον προσδιορισμό των AoAs καθενός από τους τόνους num_targets. Η έξοδος είναι ένα

διάνυσμα AoA μήκους num_targets. Το διάνυσμα AoA περιέχει AoAs σε ταξινομημένη διάταξη.

- short term key: Αυτό το μπλοκ παράγει το βραχυπρόθεσμο κλειδί, λαμβάνοντας πληροφορίες από το πλάτος και την φάση.
- long term key: Αυτό το μπλοκ παράγει το μακροπρόθεσμο κλειδί, λαμβάνοντας πληροφορίες από την εικονική γωνία άφιξης και την καθυστέρηση διάδοσης.
- Subtract: Αφαίρεση σε όλες τις ροές εισόδου.
- File Sink: Χρησιμοποιείται για την εγγραφή μιας ροής σε ένα δυαδικό αρχείο.
- Sample and Hold: Κύκλωμα δειγματοληψίας και κράτησης. Δειγματοληπτεί τη ροή δεδομένων (ροή εισόδου 0) και κρατά την τιμή εάν το σήμα ελέγχου είναι 1 (ροή εισόδου 1). Εφόσον το σήμα ελέγχου είναι διαφορετικό από 0, η ροή δεδομένων προωθείται. Όταν το σήμα ελέγχου είναι 0, τα δείγματα εξόδου έχουν την τιμή του τελευταίου προωθημένου δείγματος δεδομένων. Ο έλεγχος του σήματος ελέγχου γίνεται σε κάθε δείγμα, ώστε οι δύο εισοδοί να καταναλώνονται με το ρυθμό δειγματοληψίας.
- Constant Source: Παράγει μια σταθερή πηγή τύπου complex, float, int ή short.
- Correlate: Αυτό το μπλοκ παράγει έναν δειγματικό πίνακα συσχέτισης για το διάνυσμα εισόδου που αποτελείται από τιμές που προέρχονται από τα κανάλια λήψης.

6.4.4 Ανάλυση Αποτελεσμάτων

Για την εκτέλεση του πειράματος, χρησιμοποιήθηκαν οι παρακάτω μεταβλητές (Εικόνα 6-4).

Options Title: Not titled yet Author: gnanis Output Language: Python Generate Options: QT GUI	Variable ID: samp_rate Value: 50k	Variable ID: fft_len Value: 64	Import Import: tagged_streams	Variable ID: header_mod Value: <gnuradio_fft2fft430>	Variable ID: pilot_symbols Value: (1, 1, -1, -1)	Variable ID: payload_mod Value: <gnuradio_fft2fft430>	Variable ID: packet_length_tag_key Value: packet_len	Variable ID: payload_equalizer Value: <gnuradio_fft2fft430>	Variable ID: pilot_carriers_2 Value: -21, -7, 7, 21
	Variable ID: packet_len Value: 96	Variable ID: length_tag_key Value: packet_len	Variable ID: sync_word1 Value: [0, 0, 0, 0, 0, 0]	Variable ID: sync_word2 Value: [0, 0, 0, 0, 0, 0]	Variable ID: pilot_carriers Value: (-21, -7, 7, 21)	Variable ID: header_equalizer Value: <gnuradio_fft2fft430>	Variable ID: occupied_carriers Value: [-26, -24, 24, 26]	Variable ID: header_formatter Value: <gnuradio_fft2fft430>	Variable ID: sync_word3 Value: [0, 0, 760198, 0, 21813, ...]

Εικόνα 6-4: Μεταβλητές για την εκτέλεση του πειράματος.

Εκτελώντας το flowgraph των Εικόνων 6-7, 6-8, 6-9 και 6-10, εξάγονται τα παρακάτω αποτελέσματα. Τα USRPs είναι ρυθμισμένα σε συχνότητα 1.1 GHz και το καθένα είναι συνδεδεμένο σε διαφορετικό υπολογιστή. Ο πομπός έχει κέρδος 65 dB ενώ ο δέκτης έχει κέρδος 40 dB και στις δύο κεραίες.

Από την Εικόνα 6-5, για πλάτος ίσο με 2 το δυαδικό ψηφίο που αντιστοιχεί σύμφωνα με τον αλγόριθμο είναι το 0. Μετά, πάλι για πλάτος ίσο με 2, ο μέσος όρος των δύο τρεχόντων πλατών είναι $(2+2)/2=2$. Το threshold που έχει τεθεί είναι 0,2 και η τυπική απόκλιση αυτού υπολογίζεται σε 0. Επομένως, ισχύει ότι πλάτος = μέσος όρος πλατών - threshold * τυπική απόκλιση. Όλο αυτό σημαίνει $2 = 2 - 0,2 * 0$. Αφού ισχύει αυτό, τότε το δυαδικό ψηφίο που αντιστοιχεί εδώ είναι το x. Από τον αλγόριθμο είναι γνωστό ότι το x αντικαθίσταται με 0. Άρα, το μέχρι στιγμής κλειδί είναι [0, 0]. Το ίδιο γίνεται και για την φάση. Έτσι για αυτό το δείγμα που φαίνεται στην Εικόνα 6-5, το κλειδί πλάτους είναι [0, 0, 0, 0, 0, 0] και το κλειδί της φάσης είναι [0, 0, 1, 0, 0, 0].

Από την Εικόνα 6-6, για γωνία άφιξης ίση με 102, στον κώδικα Gray (αυτός ο κώδικας πραγματοποιεί XOR bit με bit και δεξιά μετατόπιση στο δεκαδικό νούμερο που του έχει δοθεί) αυτός ο αριθμός αντιστοιχεί δυαδικό αριθμό 01010101 και για καθυστέρηση ίση με 0, τότε το κλειδί είναι 0. Άρα για αυτά τα νούμερα, το κλειδί της γωνία άφιξης είναι [0, 1, 0, 1, 0, 1, 0, 1] και το κλειδί της καθυστέρησης είναι [0]. Παρατηρείται ότι η καθυστέρηση διάδοσης είναι μηδαμινή.

Αυτό συμβαίνει λόγω της πολύ μικρής απόστασης μεταξύ τους επειδή βρίσκονταν σε εσωτερικό, κλειστό και ελεγχόμενο χώρο και όχι σε εξωτερικό χώρο.

```
keep_pilots :warning: TTT7
keep_pilots :warning: TTT21
keep_pilots :warning: TTT43
keep_pilots :warning: TTT57
Platos: [0] ==> 2
kleidi platos: [0] ==> 0

Fash: [0] ==> 2.25802
kleidi fash: [0] ==> 0

Platos: [1] ==> 2
kleidi platos: [1] ==> 0

Fash: [1] ==> -1.07992
kleidi fash: [1] ==> 0

Platos: [2] ==> 2
kleidi platos: [2] ==> 0

Fash: [2] ==> 2.65072
kleidi fash: [2] ==> 1

Platos: [3] ==> 2
kleidi platos: [3] ==> 0

Fash: [3] ==> -0.687222
kleidi fash: [3] ==> 0

Platos: [4] ==> 0
kleidi platos: [4] ==> 0

Fash: [4] ==> 0
kleidi fash: [4] ==> 0
```

Εικόνα 6-5: Βραχυπρόθεσμο κλειδί.

```
AOA: [7226] ==> 102
kleidi AOA: [7226] ==> 1010101

T: [7226] ==> 0
kleidi T: [7226] ==> 0

AOA: [7227] ==> 168
kleidi AOA: [7227] ==> 11111100

T: [7227] ==> 0
kleidi T: [7227] ==> 0

AOA: [7228] ==> 143
kleidi AOA: [7228] ==> 11001000

T: [7228] ==> 1.69644e+12
kleidi T: [7228] ==> 0

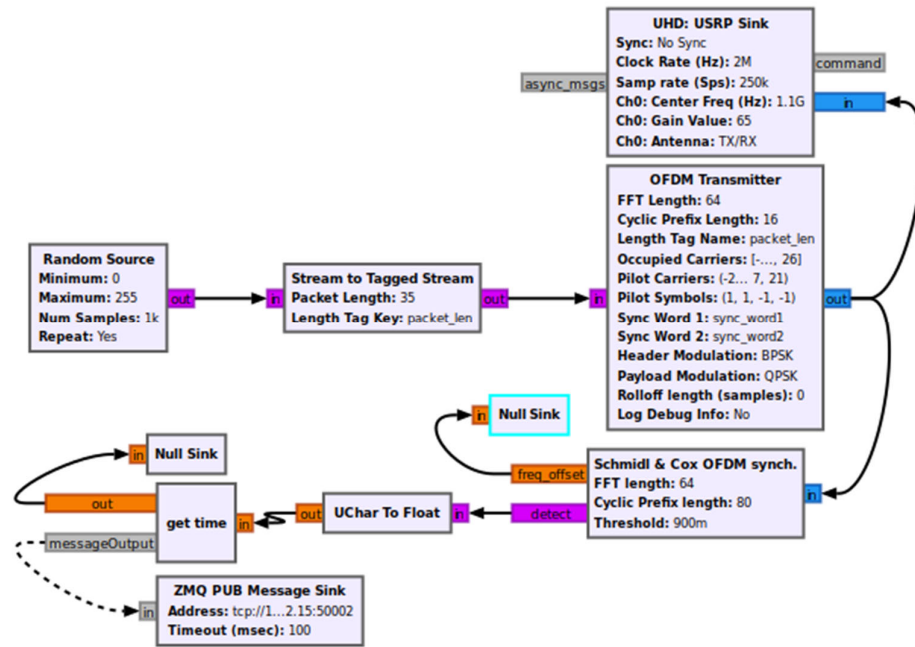
AOA: [7229] ==> 155
kleidi AOA: [7229] ==> 11010110

T: [7229] ==> 0
kleidi T: [7229] ==> 0

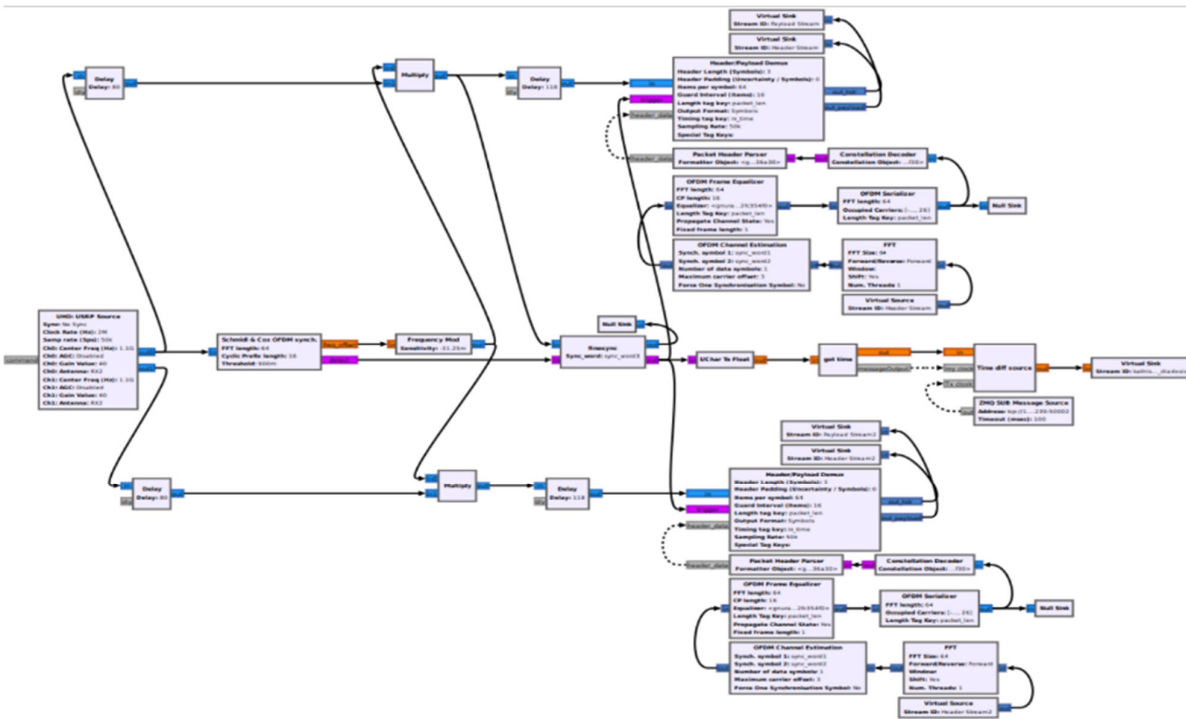
AOA: [7230] ==> 154
kleidi AOA: [7230] ==> 11010111
```

Εικόνα 6-6: Μακροπρόθεσμο κλειδί.

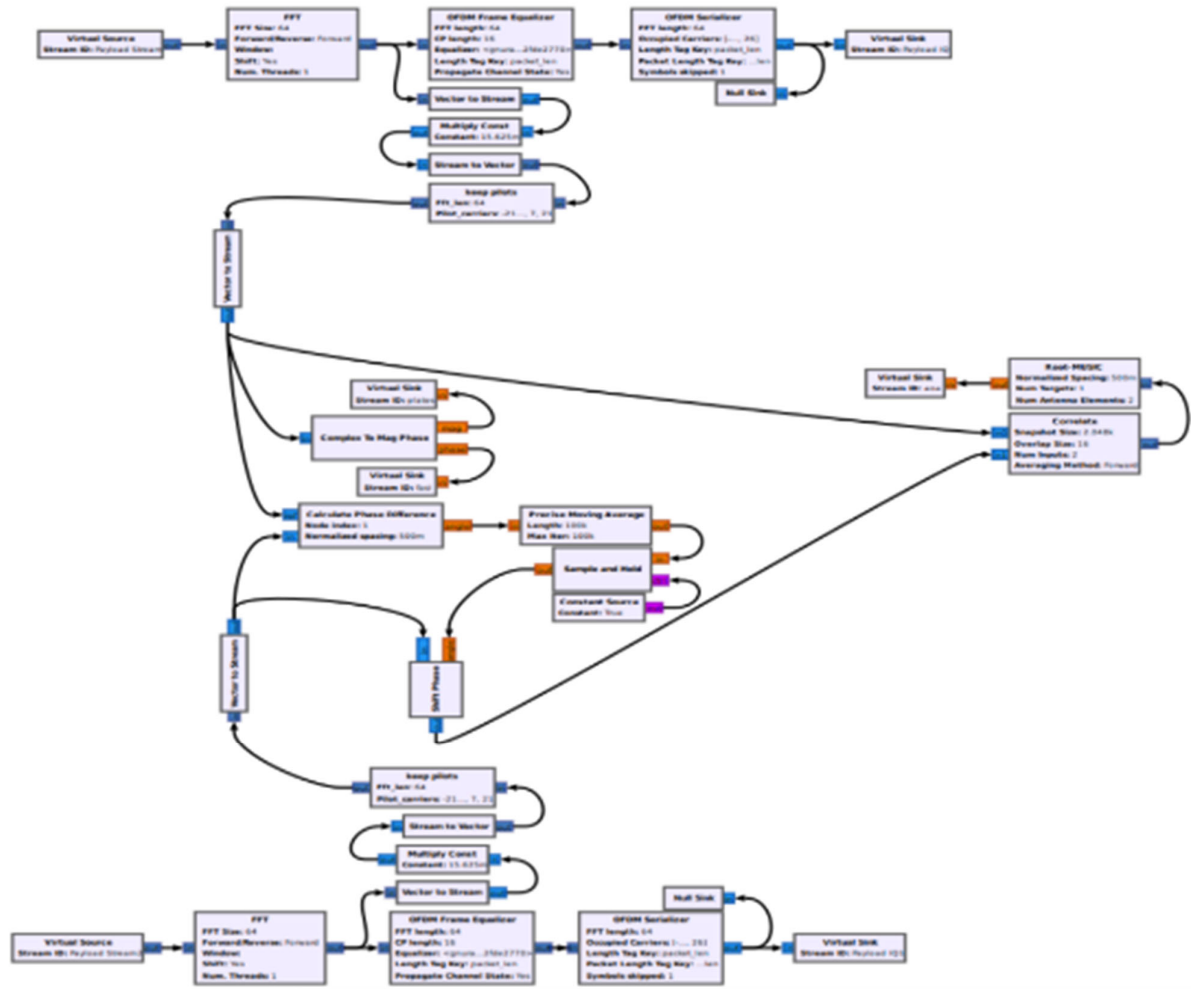
Στην συνέχεια αυτά τα κλειδιά αποθηκεύονται σε 4 διαφορετικά αρχεία, ένα για το κλειδί της γωνίας άφιξης, ένα για το κλειδί της φάσης, ένα για το κλειδί της καθυστέρησης διάδοσης και ένα για το κλειδί του πλάτους.



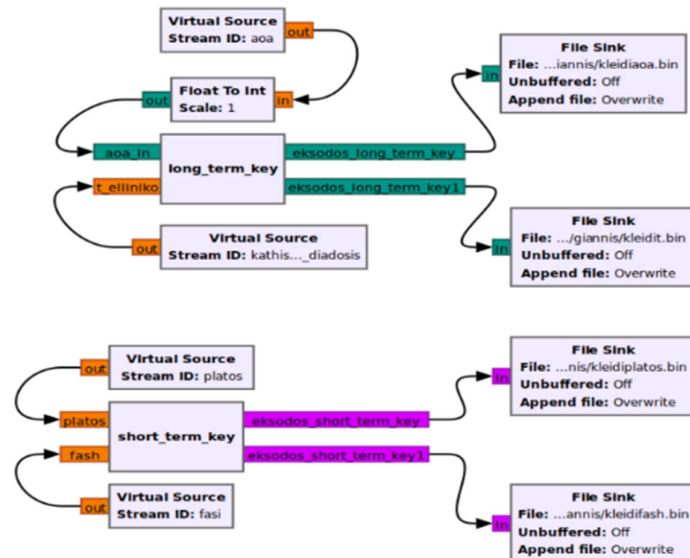
Εικόνα 6-7: Πομπός, OFDM διαμόρφωση και ανίχνευση χρονικής στιγμής άφιξης πακέτου.



Εικόνα 6-8: Δέκτης, OFDM αποδιαμόρφωση κεφαλίδας, υπολογισμός χρονικής στιγμής άφιξης πακέτου και υπολογισμός καθυστέρησης διάδοσης πακέτου.



Εικόνα 6-9: OFDM αποδιαμόρφωση του Payload, απομόνωση πιλότων, υπολογισμός γωνίας άφιξης, πλάτους και φάσης.



Εικόνα 6-10: Παραγωγή κλειδιών.

7

Συμπεράσματα

Η παρούσα διπλωματική εργασία ασχολήθηκε με την παραγωγή κλειδιών χρήσιμων στην αυθεντικοποίηση μίας εκπομπής μέσω των μοναδικών ιδιοτήτων της. Παράχθηκαν δύο είδη κλειδιών, το βραχυπρόθεσμο και το μακροπρόθεσμο κλειδί. Το βραχυπρόθεσμο κλειδί παράγεται με την βοήθεια γρήγορα μεταβαλλόμενων ιδιοτήτων του σήματος όπως είναι το πλάτος και η φάση. Στην συνέχεια, με την εφαρμογή κατάλληλης μαθηματικής συνάρτησης παράγεται το κλειδί. Από την άλλη πλευρά, το μακροπρόθεσμο κλειδί παράγεται με την βοήθεια αργά μεταβαλλόμενων ιδιοτήτων του καναλιού όπως είναι η γωνία άφιξης και η καθυστέρηση διάδοσης. Στην συνέχεια, με χρήση του αλγόριθμου Gray παράγεται το κλειδί. Για να μην υπάρξει αρκετή επιβάρυνση κατά την διαδικασία παραγωγής των κλειδιών, έγινε απομόνωση των πιλότων της OFDM διαμόρφωσης και τα κλειδιά δημιουργήθηκαν με βάση αυτούς. Τέλος, όλα τα κλειδιά αποθηκεύονται σε αρχεία προκειμένου να χρησιμοποιηθούν για οποιαδήποτε άλλη εφαρμογή. Η παραγωγή και χρήση αυτών των κλειδιών, βοηθούν τον δέκτη να αυθεντικοποιεί κάθε φορά το λαμβανόμενο σήμα που δέχεται. Έτσι επιτυγχάνεται ασφάλεια στο φυσικό επίπεδο.

Σε αυτή την εργασία έγινε χρήση του λογισμικού προσομοίωσης ασύρματων συστημάτων GNU Radio και του εξειδικευμένου εξοπλισμού USRP. Η πραγματοποίηση του πειράματος σε τόσο ακριβό εξοπλισμό αναδεικνύει την δυνατότητα επέκτασης αυτού του συστήματος σε πιο μεγάλης εμβέλειας συστήματα όπως τα συστήματα κινητών επικοινωνιών και άλλα.

Υπάρχουν αρκετοί λόγοι που το RF Fingerprinting είναι αρκετά ασφαλές. Αρχικά, δεν παρεμβαίνει στις επικοινωνίες μεταξύ πομπών και δεκτών όπως κάνουν παραδοσιακοί τρόποι κρυπτογράφησης (ανταλλαγή κλειδιών). Σε αντίθεση με ορισμένες μεθόδους κρυπτογράφησης που απαιτούν ενεργή επικοινωνία μεταξύ των συσκευών, το RF Fingerprinting μπορεί να λειτουργήσει παθητικά, χωρίς την ανάγκη άμεσης αλληλεπίδρασης. Επίσης, είναι δύσκολο να πλαστογραφηθεί. Εάν η μέθοδος RF Fingerprinting είναι ακριβής και δεν μπορεί να αντιγραφεί εύκολα, μπορεί να είναι πιο ασφαλής από τις μεθόδους που βασίζονται αποκλειστικά σε κωδικούς πρόσβασης ή ψηφιακά κλειδιά, τα οποία μπορούν ενδεχομένως να κλαπούν ή να εκτιμηθούν. Επιπρόσθετα, χαρακτηρίζεται από επεκτασιμότητα. Θα μπορούσε δυνητικά να επεκταθεί σε μεγάλο αριθμό συσκευών χωρίς την ανάγκη για πρόσθετα διακριτικά ή κλειδιά υλικού. Ωστόσο, υπάρχουν και προκλήσεις σε αυτό τον τρόπο επίτευξης μυστικότητας. Τα σήματα μπορούν να επηρεαστούν από

διάφορους περιβαλλοντικούς παράγοντες. Η εξασφάλιση ακριβούς και αξιόπιστου RF Fingerprinting υπό διαφορετικές συνθήκες αποτελεί σημαντική πρόκληση. Επιπλέον η συλλογή και αποθήκευση δεδομένων ραδιοσυχνοτήτων θα μπορούσε να εγείρει ανησυχίες για την προστασία της ιδιωτικής ζωής. Η διασφάλιση της ηθικής χρήσης της τεχνολογίας και η προστασία της ιδιωτικής ζωής των χρηστών είναι ουσιώδους σημασίας. Τέλος, τα σήματα ραδιοσυχνοτήτων μπορούν να παρεμβληθούν ή να παρεμποδιστούν (παρεμβολές, jamming), διαταράσσοντας ενδεχομένως τη διαδικασία λήψης κλειδιών.

Επιστημονική Βιβλιογραφία

- [1] Rappaport, T. S. (2002). *Wireless Communications: Principles and Practice*. Prentice Hall.
- [2] Li, Y. G., & Stuber, G. L. (2006, May 31). *Orthogonal Frequency Division Multiplexing for Wireless Communications*. Springer Science & Business Media.
- [3] Mohammadian, A., & Tellambura, C. (2021). RF impairments in wireless transceivers: Phase noise, CFO, and IQ imbalance—A survey. *IEEE Access*, 9, 111718-111791.
- [4] Rehman, S. U., Sowerby, K. W., Alam, S., & Ardekani, I. (2014, October). Radio frequency fingerprinting and its challenges. In *2014 IEEE conference on communications and network security* (pp. 496-497). IEEE.
- [5] Soltanieh, N., Norouzi, Y., Yang, Y., & Karmakar, N. C. (2020). A review of radio frequency fingerprinting techniques. *IEEE Journal of Radio Frequency Identification*, 4(3), 222-233.
- [6] Srinivasan, M., Skaperas, S., & Chorti, A. (2021, November). On the Use of CSI for the Generation of RF Fingerprints and Secret Keys. In *WSA 2021; 25th International ITG Workshop on Smart Antennas* (pp. 1-5). VDE.
- [7] Jiao, L., Tang, J., & Zeng, K. (2018, May). Physical layer key generation using virtual AoA and AoD of mmWave massive MIMO channel. In *2018 IEEE Conference on Communications and Network Security (CNS)* (pp. 1-9). IEEE.
- [8] Lukacs, M. W., Zeqolari, A. J., Collins, P. J., & Temple, M. A. (2015). “RF-DNA” fingerprinting for antenna classification. *IEEE Antennas and Wireless Propagation Letters*, 14, 1455-1458.
- [9] Akeela, R., & Dezfouli, B. (2018). Software-defined Radios: Architecture, state-of-the-art, and challenges. *Computer Communications*, 128, 106-125.
- [10] Valerio, D. (2008). Open source software-defined radio: A survey on gnuradio and its applications. Forschungszentrum Telekommunikation Wien, Vienna, Technical Report FTW-TR-2008-002.
- [11] Li, N., Han, Y., Gao, N., & Jin, S. (2022, June). Physical Layer Key Generation Scheme for Wideband Large Antenna Array Systems. In *2022 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)* (pp. 01-05). IEEE.

- [12] Hwang, H. K., Aliyazicioglu, Z., Grice, M., & Yakovlev, A. (2008, March). Direction of arrival estimation using a root-MUSIC algorithm. In Proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 2, pp. 19-21). Citeseer.
- [13] Mathur, S., Trappe, W., Mandayam, N., Ye, C., & Reznik, A. (2008, September). Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In Proceedings of the 14th ACM international conference on Mobile computing and networking (pp. 128-139).
- [14] L. Tomba and W. A. Krzymien, “Effect of carrier phase noise and frequency offset on the performance of multicarrier CDMA systems,” in Proc. Int. Conf. Commun. (ICC), vol. 3, Jun. 1996, pp. 1513–1517.
- [15] L. Tomba and W. A. Krzymien, “Sensitivity of the MC-CDMA access scheme to carrier phase noise and frequency offset,” IEEE Trans. Veh. Technol., vol. 48, no. 5, pp. 1657–1665, Sep. 1999.
- [16] H. Steendam and M. Moeneclaey, “The effect of carrier phase jitter on MCCDMA performance,” IEEE Trans. Commun., vol. 47, no. 2, pp. 195–198, Feb. 1999.
- [17] P. Mathecken, T. Riihonen, N. N. Tchamov, S. Werner, M. Valkama, and R. Wichman, “Characterization of OFDM radio link under PLLbased oscillator phase noise and multipath fading channel,” IEEE Trans. Commun., vol. 60, no. 6, pp. 1479–1485, Jun. 2012.
- [18] A. Gokceoglu, Y. Zou, M. Valkama, P. C. Sofotasios, P. Mathecken, and D. Cabric, “Mutual information analysis of OFDM radio link under phase noise, IQ imbalance and frequency-selective fading channel,” IEEE Trans. Wireless Commun., vol. 12, no. 6, pp. 3048–3059, Jun. 2013.
- [19] V. Nguyen-Duy-Nhat, H. Nguyen-Le, C. Tang-Tan, and T. Le-Ngoc, “SIR analysis for OFDM transmission in the presence of CFO, phase noise and doubly selective fading,” IEEE Commun. Lett., vol. 17, no. 9, pp. 1810–1813, Sep. 2013.
- [20] I. Ngehani, Y. Li, X.-G. Xia, S. A. Haider, A. Huang, and M. Zhao, “Analysis and compensation of phase noise in vector OFDM systems,” IEEE Trans. Signal Process., vol. 62, no. 23, pp. 6143–6157, Dec. 2014.
- [21] A. Spalvieri and L. Barletta, “Pilot-aided carrier recovery in the presence of phase noise,” IEEE Trans. Commun., vol. 59, no. 7, pp. 1966–1974, Jul. 2011.

- [22] N. Kamiya and E. Sasaki, “Pilot-symbol assisted and code-aided phase error estimation for high-order QAM transmission,” *IEEE Trans. Commun.*, vol. 61, no. 10, pp. 4369–4380, Oct. 2013.
- [23] M. R. Khanzadi, R. Krishnan, and T. Eriksson, “Estimation of phase noise in oscillators with colored noise sources,” *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2160–2163, Nov. 2013.
- [24] A. Gomaa and N. Al-Dhahir, “Phase noise in asynchronous SC-FDMA systems: Performance analysis and data-aided compensation,” *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2642–2652, Jul. 2014.
- [25] D. Petrovic, W. Rave, and G. Fettweis, “Effects of phase noise on OFDM systems with and without PLL: Characterization and compensation,” *IEEE Trans. Commun.*, vol. 55, no. 8, pp. 1607–1616, Aug. 2007.
- [26] P. Robertson and S. Kaiser, “Analysis of the effects of phase-noise in orthogonal frequency division multiplex (OFDM) systems,” in *Proc. IEEE Int. Conf. Commun. (ICC)*, vol. 3, Jun. 1995, pp. 1652–1657.
- [27] S. Wu and Y. Bar-Ness, “A phase noise suppression algorithm for OFDMbased WLANs,” *IEEE Commun. Lett.*, vol. 6, no. 12, pp. 535–537, Dec. 2002.
- [28] D. Petrovic, W. Rave, and G. Fettweis, “Phase noise suppression in OFDM including intercarrier interference,” in *Proc. Int. OFDM Workshop (InOWo)*, vol. 3, 2003, pp. 219–224.
- [29] D. Petrovic, W. Rave, and G. Fettweis, “Intercarrier interference due to phase noise in OFDM—estimation and suppression,” in *Proc. IEEE 60th Veh. Technol. Conf. (VTC-Fall)*, vol. 3, Sep. 2004, pp. 2191–2195.
- [30] G. Fettweis, M. Löhning, D. Petrovic, M. Windisch, P. Zillmann, W. Rave, “Dirty RF: A new paradigm,” *Int. J. Wireless Inf. Netw.*, vol. 14, no. 2, pp. 133–148, Jun. 2007.
- [31] V. Syrjala, M. Valkama, N. N. Tchamov, and J. Rinne, “Phase noise modelling and mitigation techniques in OFDM communications systems,” in *Proc. Wireless Telecommun. Symp.*, Apr. 2009, pp. 1–7.
- [32] N. N. Tchamov, J. Rinne, A. Hazmi, M. Valkama, V. Syrjala, and M. Renfors, “Enhanced algorithm for digital mitigation of ICI due to phase noise in OFDM receivers,” *IEEE Wireless Commun. Lett.*, vol. 2, no. 1, pp. 6–9, Feb. 2013.
- [33] M.-K. Lee, K. Yang, and K. Cheun, “Iterative receivers based on subblock processing for phase noise compensation in OFDM systems,” *IEEE Trans. Commun.*, vol. 59, no. 3, pp. 792–802, Mar. 2011.

- [34] S. Negusse, P. Zetterberg, and P. Handel, “Phase-noise mitigation in OFDM by best match trajectories,” *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1712–1725, May 2015.
- [35] R. Corvaja and A. G. Armada, “Joint channel and phase noise compensation for OFDM in fast-fading multipath applications,” *IEEE Trans. Veh. Technol.*, vol. 58, no. 2, pp. 636–643, Feb. 2009.
- [36] P. Rabiei, W. Namgoong, and N. Al-Dhahir, “A non-iterative technique for phase noise ICI mitigation in packet-based OFDM systems,” *IEEE Trans. Signal Process.*, vol. 58, no. 11, pp. 5945–5950, Nov. 2010.
- [37] O. H. Salim, A. A. Nasir, H. Mehrpouyan, W. Xiang, S. Durrani, and R. A. Kennedy, “Channel, phase noise, and frequency offset in OFDM systems: Joint estimation, data detection, and hybrid Cramér-Rao lower bound,” *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3311–3325, Sep. 2014.
- [38] Y.-C. Liao and K.-C. Chen, “Multiuser common phase error estimation for uplink OFDMA communications,” in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2007, pp. 1976–1981.
- [39] L. Samara, V. Syrjala, R. Hamila, and M. Valkama, “Phase noise mitigation in OFDMA uplink,” in *Proc. 6th Int. Symp. Commun., Control Signal Process. (ISCCSP)*, May 2014, pp. 344–347.

Διαδικτυακές Πηγές

- [13] <https://www.everythingrf.com/community/what-is-an-isotropic-antenna>
- [14] https://commons.wikimedia.org/wiki/File:Radiation_Pattern_Dipole_PD.png
- [15] <https://www.sciencedirect.com/topics/engineering/isotropic-antenna>
- [16] <https://blogs.synopsys.com/optical-solutions/2021/10/13/how-light-scattering-measurements-can-improve-your-optical-product-development/>
- [17] <https://github.com/MarcinWachowiak/gr-aoa>

Παράρτημα I [Επιλογή Πιλότων]

```
#include "keep_pilots_impl.h"
#include <gnuradio/io_signature.h>

namespace gr
{
    namespace thesiskyriazisioannis
    {
        keep_pilots::sptr keep_pilots::make(int fft_len, std::vector<int> pilot_carriers)
        {
            return gnuradio::make_block_sptr<keep_pilots_impl>(fft_len, pilot_carriers);
        }

        /*
         * The private constructor
         */
        keep_pilots_impl::keep_pilots_impl(int fft_len, std::vector<int> pilot_carriers)
            : gr::block("keep_pilots",
                gr::io_signature::make(
                    1, 1, sizeof(gr_complex) * fft_len),
                gr::io_signature::make(
                    1, 1, sizeof(gr_complex) * pilot_carriers.size()),
                d_fft_len(fft_len),
                d_pilot_carriers(pilot_carriers)
            )
        {
            for (int i = 0; i < d_pilot_carriers.size(); i++)
            {
                if (d_pilot_carriers[i] < 0)
                {
                    d_pilot_carriers[i] = fft_len + d_pilot_carriers[i];
                }
                // d_logger->warn("TTT{}", d_pilot_carriers[i]);
            }
            sort(d_pilot_carriers.begin(), d_pilot_carriers.end());

            for (int i = 0; i < d_pilot_carriers.size(); i++)
            {
                d_logger->warn("TTT{}", d_pilot_carriers[i]);
            }
        }

        /*
         * Our virtual destructor.
         */
        keep_pilots_impl::~keep_pilots_impl() {}

        void keep_pilots_impl::forecast(int noutput_items, gr_vector_int &ninput_items_required)
        {
            unsigned ninputs = ninput_items_required.size();
            for (unsigned i = 0; i < ninputs; i++)
            {
                ninput_items_required[i] = d_fft_len;
            }

            noutput_items = d_pilot_carriers.size();
        }

        int keep_pilots_impl::general_work(int noutput_items,
                                           gr_vector_int &ninput_items,
                                           gr_vector_const_void_star &input_items,
                                           gr_vector_void_star &output_items)
        {
            gr_complex *in = (gr_complex *)input_items[0];
            gr_complex *out = (gr_complex *)output_items[0];

            sort(d_pilot_carriers.begin(), d_pilot_carriers.end());

            // for (int i = 0; i < noutput_items; i++)
            int jj = 0;
            int j = 0;
            for (j = 0; j < d_fft_len; j++)
            {
                if (j == d_pilot_carriers[jj])
                {
                    *out++ = *in++;
                    jj++;
                }
                else
                {
                    // *out++ = gr_complex(0,0); in++;
                    in++;
                }
            }

            // Tell runtime system how many input items we consumed on
            // each input stream.
        }
    }
}
```

```
consume_each(ninput_items[0]);  
  
// Tell runtime system how many output items we produced.  
return noutput_items;  
}  
} /* namespace thesiskyriazisioannis */  
} /* namespace gr */
```

Παράρτημα II [Παραγωγή long-term κλειδιού]

```
#include "long_term_key_impl.h"
#include <gnuradio/io_signature.h>

using namespace std;

namespace gr
{
    namespace thesiskyriazisioannis
    {
        long_term_key::sptr long_term_key::make()
        {
            return gnuradio::get_initial_sptr(new long_term_key_impl());
        }

        /*
         * The private constructor
         */
        long_term_key_impl::long_term_key_impl()
            : gr::block("long_term_key",
                gr::io_signature::make2(2, 2, sizeof(int), sizeof(float)),
                gr::io_signature::make2(2, 2, sizeof(int), sizeof(int)))
        {
        }

        /*
         * Our virtual destructor.
         */
        long_term_key_impl::~long_term_key_impl() {}

        int
        long_term_key_impl::grayCode(int n)
        {
            return n ^ (n >> 1);
        }

        void
        long_term_key_impl::forecast(int noutput_items, gr_vector_int &ninput_items_required)
        {
            unsigned ninputs = ninput_items_required.size();
            for (unsigned i = 0; i < ninputs; i++)
            {
                ninput_items_required[i] = noutput_items;
            }
        }

        int long_term_key_impl::general_work(int noutput_items,
            gr_vector_int &ninput_items,
            gr_vector_const_void_star &input_items,
            gr_vector_void_star &output_items)
        {
            int *aoa_in = (int *)input_items[0];
            float *t_elliniko = (float *)input_items[1];
            int *eksodos_long_term_key = (int *)output_items[0];
            int *eksodos_long_term_key1 = (int *)output_items[1];

            double d_threshold = 0.2;

            // long-term key generation

            for (int i = 0; i < noutput_items; i++)
            {
                int dyadiko_aoa = grayCode(aoa_in[i]);
                int binaryNum[10];

                int i_1 = 0;
                while (dyadiko_aoa > 0)
                {
                    binaryNum[i_1] = dyadiko_aoa % 2;
                    dyadiko_aoa = dyadiko_aoa / 2;
                    i_1++;
                }

                int k = 0;
```

```
int dyadiko_aoa_pinakas[10];
for (int j = i_1 - 1; j >= 0; j--)
{
    dyadiko_aoa_pinakas[k] = binaryNum[j];
    k++;
}

int aoa_out[10];
for (int u = 0; u < (sizeof(aoa_out) / sizeof(aoa_out[0])); u++)
{
    aoa_out[u] = 0;
}

int k2 = 0;
for (int u = (sizeof(aoa_out) / sizeof(aoa_out[0])) - k; u < (sizeof(aoa_out) / sizeof(aoa_out[0])); u++)
{
    aoa_out[u] = dyadiko_aoa_pinakas[k2];
    k2++;
}

int eksodos_aoa = 0;
for (int u = 0; u < (sizeof(aoa_out) / sizeof(aoa_out[0])); u++)
{
    eksodos_aoa *= 10;
    eksodos_aoa += aoa_out[u];
}

eksodos_long_term_key[i] = eksodos_aoa;

int dyadiko_t_elliniko = grayCode(t_elliniko[i]);
int binaryNum1[10];

int i_2 = 0;
while (dyadiko_t_elliniko > 0)
{
    binaryNum1[i_2] = dyadiko_t_elliniko % 2;
    dyadiko_t_elliniko = dyadiko_t_elliniko / 2;
    i_2++;
}

int k1 = 0;
int dyadiko_t_elliniko_pinakas[10];
for (int j = i_2 - 1; j >= 0; j--)
{
    dyadiko_t_elliniko_pinakas[k1] = binaryNum1[j];
    k1++;
}

int t_out[10];
for (int u = 0; u < (sizeof(t_out) / sizeof(t_out[0])); u++)
{
    t_out[u] = 0;
}
```

Παράρτημα ΙΙΙ [Παραγωγή *short-term* κλειδιού]

```
#include "short_term_key_impl.h"
#include <gnuradio/io_signature.h>

using namespace std;

namespace gr
{
    namespace thesiskyriazisioannis
    {
        short_term_key::sptr short_term_key::make()
        {
            return gnuradio::get_initial_sptr(new short_term_key_impl());
        }

        /*
         * The private constructor
         */
        short_term_key_impl::short_term_key_impl()
            : gr::block("short_term_key",
                gr::io_signature::make2(2, 2, sizeof(float), sizeof(float)),
                gr::io_signature::make2(2, 2, sizeof(unsigned char), sizeof(unsigned char)))
        {
        }

        /*
         * Our virtual destructor.
         */
        short_term_key_impl::~short_term_key_impl() {}

        void
        short_term_key_impl::forecast(int noutput_items, gr_vector_int &ninput_items_required)
        {
            unsigned ninputs = ninput_items_required.size();
            for (unsigned i = 0; i < ninputs; i++)
            {
                ninput_items_required[i] = noutput_items;
            }
        }

        int short_term_key_impl::general_work(int noutput_items,
            gr_vector_int &ninput_items,
            gr_vector_const_void_star &input_items,
            gr_vector_void_star &output_items)
        {
            float *platos = (float *)input_items[0];
            float *fash = (float *)input_items[1];
            unsigned char *eksodos_short_term_key = (unsigned char *)output_items[0];
            unsigned char *eksodos_short_term_key1 = (unsigned char *)output_items[1];

            // for(int i=0; i<noutput_items; i++){
            // short-term key generation
            float d_threshold = 0.2;
            unsigned char kleidi_platos[noutput_items];
            unsigned char kleidi_fash[noutput_items];
            float mo_platos;
            float sum = 0.0;
            float squaredDifferencesSum = 0.0;

            float mo_fash;
            float sum1 = 0.0;
            float squaredDifferencesSum1 = 0.0;

            for (int e = 0; e < noutput_items; e++)
            {
                sum += platos[e];
                mo_platos = sum / e;

                // Calculate the sum of squared differences from the mean

                float diff = platos[e] - mo_platos;
                squaredDifferencesSum += diff * diff;

                // Calculate the variance (squared standard deviation)
            }
        }
    }
}
```

```
float variance = squaredDifferencesSum / (e - 1);

// Calculate the sample standard deviation (square root of variance)
float sigma_platos = sqrt(variance);

if (platos[e] > mo_platos + d_threshold * sigma_platos)
{
    kleidi_platos[e] = '1';
}
else if (platos[e] < mo_platos - d_threshold * sigma_platos)
{
    kleidi_platos[e] = '0';
}
else
{
    kleidi_platos[e] = 'x';
}

if (kleidi_platos[e] == 'x')
{
    kleidi_platos[e] = '0';
}

eksodos_short_term_key[e] = kleidi_platos[e];

sum1 += fash[e];
mo_platos = sum1 / e;

// Calculate the sum of squared differences from the mean
float diff1 = fash[e] - mo_fash;
squaredDifferencesSum1 += diff1 * diff1;

// Calculate the variance (squared standard deviation)
float variance1 = squaredDifferencesSum1 / (e - 1);

// Calculate the sample standard deviation (square root of variance)
float sigma_fash = sqrt(variance1);

if (fash[e] > mo_fash + d_threshold * sigma_fash)
{
    kleidi_fash[e] = '1';
}
else if (fash[e] < mo_fash - d_threshold * sigma_fash)
{
    kleidi_fash[e] = '0';
}
else
{
    kleidi_fash[e] = 'x';
}

if (kleidi_fash[e] == 'x')
{
    kleidi_fash[e] = '0';
}

eksodos_short_term_key1[e] = kleidi_fash[e];
cout << "Platos: [" << e << "] ==> " << platos[e] << "\nkleidi platos: [" << e << "] ==> " <<
eksodos_short_term_key[e] << "\n\n";
cout << "Fash: [" << e << "] ==> " << fash[e] << "\nkleidi fash: [" << e << "] ==> " <<
eksodos_short_term_key1[e] << "\n\n";
}

//}

// each input stream.
consume_each(noutput_items);

// Tell runtime system how many output items we produced.
return noutput_items;
}

} /* namespace thesiskyriazisioannis */
} /* namespace gr */
```

Παράρτημα IV [Καταγραφή χρονικής στιγμής άφιξης πακέτου]

```
import numpy as np
from gnuradio import gr
import pmt
import calendar
import time

class blk(gr.sync_block): # other base classes are basic_block, decim_block, interp_block

    """Embedded Python Block example - a simple multiply const"""
    def __init__(self): # only default arguments here
        """arguments to this function show up as parameters in GRC"""
        gr.sync_block.__init__(
            self,
            name='get time', # will show up in GRC
            in_sig=[np.float32],
            out_sig=[np.float32]
        )

        self.timer = 0
        self.portName = 'messageOutput'
        self.message_port_register_out(pmt.intern(self.portName))

    def work(self, input_items, output_items):
        """example: multiply with constant"""
        length = len(input_items[0])
        for i in range(length):
            if input_items[0][i]>0:
                gmt = time.gmtime(0)
                epoch = time.asctime(gmt)
                ts = round(time.time()*1000) - 1698490083000
                PMT_msg = pmt.from_float(ts)
                self.message_port_pub(pmt.intern(self.portName), PMT_msg)
            output_items[0][i] = input_items[0][i]
        return len(output_items[0])
```

Παράρτημα V [Υπολογισμός καθυστέρησης διάδοσης]

```
import numpy as np
from gnuradio import gr
import pmt

class blk(gr.sync_block): # other base classes are basic_block, decim_block, interp_block
    """Embedded Python Block example - a simple multiply const"""

    def __init__(self): # only default arguments here
        """arguments to this function show up as parameters in GRC"""
        gr.sync_block.__init__(
            self,
            name='Time diff source', # will show up in GRC
            in_sig=[np.float32],
            out_sig=[np.float32]
        )
        # if an attribute with the same name as a parameter is found,
        # a callback is registered (properties work, too).
        self.portName1 = 'my clock'
        self.portName2 = 'Tx clock'
        self.message_port_register_in(pmt.intern(self.portName1))
        self.message_port_register_in(pmt.intern(self.portName2))
        self.set_msg_handler(pmt.intern(self.portName1), self.handle_msg1)
        self.set_msg_handler(pmt.intern(self.portName2), self.handle_msg2)
        self.value1 = 1698490083000
        self.value2 = 1698490083000

    def handle_msg1(self, msg):
        self.value1 = pmt.to_float(msg)

    def handle_msg2(self, msg):
        self.value2 = pmt.to_float(msg)

    def work(self, input_items, output_items):
        """example: multiply with constant"""
        output_items[0][:] = self.value1 - self.value2
        return len(output_items[0])
```

Παράρτημα VI [Συγχρονισμός μετά από Schmidl & Cox]

```
#include "finesync_impl.h"
#include <gnuradio/io_signature.h>
#include <algorithm>
#include <vector>
#include <volk/volk.h>
#include <cmath>

namespace gr {
namespace thesiskyriazisioannis {

finesync::sptr finesync::make(std::vector<gr_complex> sync_word)
{
    return gnuradio::make_block_sptr<finesync_impl>(sync_word);
}
/*
 * The private constructor
 */
finesync_impl::finesync_impl(std::vector<gr_complex> sync_word)
: gr::block("finesync",
    gr::io_signature::make2(
        2, 2, sizeof(gr_complex), sizeof(char)),
    gr::io_signature::make2(
        2, 2, sizeof(gr_complex), sizeof(char))),
    d_sync_word(sync_word),
    d_max_ind(0),
    d_max_val(0),
    d_check(0),
    d_check2(0),
    d_counter(0),
    d_counter2(0),
    d1_counter(0),
    d_first_ind(0)
{
    d_size = d_sync_word.size();

    for (int ii=0; ii<d_size; ii++) {
        d_memory.push_back(gr_complex(ii,0));
        d_sync_word[ii]=gr_complex(d_sync_word[ii].real(), -d_sync_word[ii].imag());
    }
}

/*
 * Our virtual destructor.
 */
finesync_impl::~finesync_impl() {}

void finesync_impl::forecast(int noutput_items, gr_vector_int& ninput_items_required)
{
    //ninput_items_required[1]=ninput_items_required[0];
    ninput_items_required[0]=noutput_items;
    ninput_items_required[1]=noutput_items;
}

int finesync_impl::general_work(int noutput_items,
    gr_vector_int& ninput_items,
    gr_vector_const_void_star& input_items,
    gr_vector_void_star& output_items)
{
    const gr_complex* in0 = reinterpret_cast<const gr_complex*>(input_items[0]);
    const char* in1 = reinterpret_cast<const char*>(input_items[1]);
    gr_complex* out0 = reinterpret_cast<gr_complex*>(output_items[0]);
    char* out1 = reinterpret_cast<char*>(output_items[1]);

    gr_complex tmp = gr_complex(0,0);
    float tmp_abs = 0;
    ninput_items[0] = noutput_items;
    ninput_items[1] = noutput_items;

    for (int ii=0; ii<ninput_items[0]; ii++) {
        // Get the detection result and cast it to integer.
        int tmp0 = static_cast<int>(in1[ii]);
        d_memory.push_back(in0[ii]);
    }
}
```

```
d_memory.erase(d_memory.begin());

if (tmp0==1) {
    // If detected by coarse, we move to mode 1 from mode 0.
    d_check = 1;
    d_counter = 0;
    d1_counter = 0;
}

if (d_check==0) {
    // if in mode 0:
    out0[ii] = gr_complex(0,0);
    out1[ii] = char(0);
} else if (d_check == 1) {
    // if in mode 1:
    if (d1_counter<d_size) {
        out0[ii] = gr_complex(0,0);
        out1[ii] = char(0);
        d1_counter++;
    } else {
        tmp = gr_complex(0,0);
        for (int kk=0; kk<d_size; kk++) {
            tmp = tmp + d_memory[kk]*d_sync_word[kk];
        }
        out0[ii] = tmp;
        out1[ii] = char(0);

        tmp_abs = abs(tmp.real());
        if (tmp_abs>d_max_val) {
            d_max_val= tmp_abs;
            d_max_ind = d_counter;
        }
        d_counter++;
        if (d_counter == 40) {
            d_check = 2;
            d_counter = 0;
            d_counter2 = 0;
            // d_logger->info("RR:{",d_max_ind);
        }
    }
}

if (d_check == 2) {
    if (d_counter==d_max_ind) {
        out1[ii] = char(1);
        d_check = 0;
        d_counter = 0;
        d_max_ind = 0;
        d_max_val = 0;
    } else {
        out1[ii] = char(0);
    }
    out0[ii] = gr_complex(0,0);
    d_counter++;
}

}

// Tell runtime system how many input items we consumed on
// each input stream.
consume_each(ninput_items[0]);

// Tell runtime system how many output items we produced.
return noutput_items;
}
} /* namespace thesiskyriazisioannis */
} /* namespace gr */
```

Παράρτημα VII [Υπολογισμός Διαφοράς Φάσης] [17]

```
#include <gnuradio/io_signature.h>
#include "calc_phase_diff_impl.h"

namespace gr
{
    namespace aoa
    {
        {
            calc_phase_diff::sptr
            calc_phase_diff::make(int node_idx, float norm_spacing)
            {
                return gnuradio::get_initial_sptr(new calc_phase_diff_impl(node_idx, norm_spacing));
            }

            calc_phase_diff_impl::calc_phase_diff_impl(int node_idx, float norm_spacing)
            : gr::sync_block("calc_phase_diff",
                            gr::io_signature::make(2, 2, sizeof(gr_complex)),
                            gr::io_signature::make(1, 1, sizeof(float))),
              d_node_idx(node_idx),
              d_norm_spacing(norm_spacing)
            {
                const int alignment_multiple = volk_get_alignment() / sizeof(gr_complex);
                set_alignment(std::max(1, alignment_multiple));

                // calc constant position diff coeff
                d_loc_shift_coeff = exp(gr_complex(0.0, 1.0) * (float)(-2 * M_PI * d_norm_spacing * d_node_idx));
            }

            calc_phase_diff_impl::~calc_phase_diff_impl()
            {
            }

            int
            calc_phase_diff_impl::work(int noutput_items,
                                       gr_vector_const_void_star &input_items,
                                       gr_vector_void_star &output_items)
            {
                const gr_complex *ref = (const gr_complex *)input_items[0];
                const gr_complex *in = (const gr_complex *)input_items[1];
                float *out = (float *)output_items[0];

                // buffer pointer
                gr_complex *buffer = (gr_complex *)volk_malloc(noutput_items * sizeof(gr_complex), volk_get_alignment());
                // location based phase diff coefficient
                // multiply conjugate of second signal with ref signal
                volk_32fc_x2_multiply_conjugate_32fc(buffer, ref, in, noutput_items);

                // correct by constant location phase diff coefficient
                volk_32fc_s32fc_multiply_32fc(buffer, buffer, d_loc_shift_coeff, noutput_items);

                for (size_t j = 0; j < noutput_items; j++)
                {
                    // calc arg
                    out[j] = fast_atan2f(buffer[j]);
                }

                volk_free(buffer);
                return noutput_items;
            }
        } /* namespace aoa */
    } /* namespace gr */
}
```

Κώδικας από <https://github.com/MarcinWachowiak/gr-aoa>.

Παράρτημα VIII [Υπολογισμός Ακριβούς Κινούμενου

Μέσου Όρου] [17]

```
#include <gnuradio/io_signature.h>
#include "precise_moving_average_impl.h"

namespace gr
{
    namespace aoa
    {
        precise_moving_average::sptr
        precise_moving_average::make(int length, int max_iter)
        {
            return gnuradio::get_initial_sptr(new precise_moving_average_impl(length, max_iter));
        }

        precise_moving_average_impl::precise_moving_average_impl(int length,
                                                                    int max_iter)
            : gr::sync_block("precise_moving_average",
                             gr::io_signature::make(1, 1, sizeof(float)),
                             gr::io_signature::make(1, 1, sizeof(float))),
              d_length(length),
              d_max_iter(max_iter)
        {
            d_scale = static_cast<double>(1.0 / length);
            this->set_history(length);
        }

        precise_moving_average_impl::~precise_moving_average_impl()
        {
        }

        int
        precise_moving_average_impl::work(int noutput_items,
                                           gr_vector_const_void_star &input_items,
                                           gr_vector_void_star &output_items)
        {
            const float *in = (const float *)input_items[0];
            float *out = (float *)output_items[0];

            unsigned int num_iter = (unsigned int)((noutput_items > d_max_iter) ? d_max_iter : noutput_items);
            double sum = in[0];
            for (int i = 1; i < d_length - 1; i++)
            {
                sum += in[i];
            }

            for (unsigned int i = 0; i < num_iter; i++)
            {
                sum += in[i + d_length - 1];
                out[i] = sum * d_scale;
                sum -= in[i];
            }

            return noutput_items;
        }
    } /* namespace aoa */
} /* namespace gr */
```

Κώδικας από <https://github.com/MarcinWachowiak/gr-aoa>.

Παράρτημα IX [Υπολογισμός Μετατόπισης Φάσης] [17]

```
#include <gnuradio/io_signature.h>
#include "shift_phase_impl.h"

namespace gr
{
    namespace aoa
    {
        {
            shift_phase::sptr
            shift_phase::make()
            {
                return gnuradio::get_initial_sptr(new shift_phase_impl());
            }

            shift_phase_impl::shift_phase_impl()
            : gr::sync_block("shift_phase",
                            gr::io_signature::make2(2, 2, sizeof(gr_complex), sizeof(float)),
                            gr::io_signature::make(1, 1, sizeof(gr_complex)))
            {
                const int alignment_multiple = volk_get_alignment() / sizeof(gr_complex);
                set_alignment(std::max(1, alignment_multiple));
            }

            shift_phase_impl::~shift_phase_impl()
            {
            }

            int
            shift_phase_impl::work(int noutput_items,
                                   gr_vector_const_void_star &input_items,
                                   gr_vector_void_star &output_items)
            {
                const gr_complex *in = (const gr_complex *)input_items[0];
                const float *coeff = (const float *)input_items[1];

                gr_complex *out = (gr_complex *)output_items[0];

                // normalize angles to complex coefficients (e^j*coeff)
                for (size_t j = 0; j < noutput_items; j++)
                {
                    out[j] = gr_complex(cos(coeff[j]), sin(coeff[j]));
                }

                // multiply input by shift coeffs calculated from input angles
                volk_32fc_x2_multiply_32fc(out, in, out, noutput_items);

                return noutput_items;
            }
        } /* namespace aoa */
    } /* namespace gr */
}
```

Κώδικας από <https://github.com/MarcinWachowiak/gr-aoa>.

Παράρτημα X [Υπολογισμός Συσχέτισης] [17]

```
#include <gnuradio/io_signature.h>
#include "correlate_impl.h"

namespace gr
{
    namespace aoa
    {
        {
            correlate::sptr
            correlate::make(int inputs, int snapshot_size, int overlap_size, int avg_method)
            {
                return gnuradio::get_initial_sptr(new correlate_impl(inputs, snapshot_size, overlap_size, avg_method));
            }

            correlate_impl::correlate_impl(int inputs, int snapshot_size, int overlap_size, int avg_method)
                : gr::sync_decimator("correlate",
                    gr::io_signature::make(inputs, inputs, sizeof(gr_complex)),
                    gr::io_signature::make(1, 1, sizeof(gr_complex) * inputs * inputs), (snapshot_size -
overlap_size)),
                    d_num_inputs(inputs),
                    d_snapshot_size(snapshot_size),
                    d_overlap_size(overlap_size),
                    d_avg_method(avg_method),
                    d_nonoverlap_size(snapshot_size - overlap_size)
            {
                set_history(d_overlap_size + 1);

                // Create container for temporary matrix
                d_input_matrix = Eigen::MatrixXcf(d_snapshot_size, d_num_inputs);

                // initialize the reflection matrix
                d_J = Eigen::MatrixXf::Identity(d_num_inputs, d_num_inputs);
                d_J = d_J.reverse();
            }

            correlate_impl::~correlate_impl()
            {
            }

            int
            correlate_impl::work(int output_matrices,
                gr_vector_const_void_star &input_items,
                gr_vector_void_star &output_items)
            {
                // Cast pointer
                gr_complex *out = (gr_complex *)output_items[0];

                // Create each output matrix
                for (int i = 0; i < output_matrices; i++)
                {
                    // Form input matrix
                    for (int k = 0; k < d_num_inputs; k++)
                    {
                        memcpy((void *)d_input_matrix.col(k).data(),
                            ((gr_complex *)input_items[k] + i * d_nonoverlap_size),
                            sizeof(gr_complex) * d_snapshot_size);
                    }
                    // Make output pointer into matrix pointer
                    Eigen::Map<Eigen::MatrixXcf> out_matrix(out + d_num_inputs * d_num_inputs * i, d_num_inputs, d_num_inputs);

                    // Do autocorrelation
                    out_matrix = (1.0 / d_snapshot_size) * d_input_matrix.transpose() * d_input_matrix.conjugate();

                    if (d_avg_method == 1)
                    {
                        out_matrix = 0.5 * out_matrix + (0.5 / d_snapshot_size) * d_J * out_matrix.conjugate() * d_J;
                    }
                }

                // Tell runtime system how many output items we produced.
                return (output_matrices);
            }
        } /* namespace aoa */
    } /* namespace gr */
}
```

Κώδικας από <https://github.com/MarcinWachowiak/gr-aoa>.

Παράρτημα XI [Υπολογισμός Γωνίας Άφιξης] [17]

```
#include <gnuradio/io_signature.h>
#include "rootMUSIC_linear_array_impl.h"

namespace Eigen
{
    namespace Vector1
    {
        template <class T>
        inline void push_back(Eigen::Matrix<T, Eigen::Dynamic, 1> &v, const T d)
        {
            Eigen::Matrix<T, Eigen::Dynamic, 1> tmp = v;
            v.conservativeResize(tmp.size() + 1);
            v.head(tmp.size()) = tmp;
            v[v.size() - 1] = d;
        }
    } // namespace Vector1
} // namespace Eigen

namespace gr
{
    namespace aoa
    {
        rootMUSIC_linear_array::sptr
        rootMUSIC_linear_array::make(float norm_spacing, int num_targets, int num_ant_ele)
        {
            return gnuradio::get_initial_sptr(new rootMUSIC_linear_array_impl(norm_spacing, num_targets, num_ant_ele));
        }

        rootMUSIC_linear_array_impl::rootMUSIC_linear_array_impl(float norm_spacing, int num_targets, int num_ant_ele)
            : gr::sync_block("rootMUSIC_linear_array",
                gr::io_signature::make(1, 1, sizeof(gr_complex) * num_ant_ele * num_ant_ele),
                gr::io_signature::make(1, num_targets, num_targets * sizeof(float))),
            d_norm_spacing(norm_spacing),
            d_num_targets(num_targets),
            d_num_ant_ele(num_ant_ele)
        {
            // initialization of the Frobenius companion matrix
            d_comp_mat = Eigen::MatrixXcf(2 * d_num_ant_ele - 2, 2 * d_num_ant_ele - 2).setZero();
            // set the first sub-diagonal to all-ones
            d_comp_mat.diagonal(-1).setOnes();
        }

        rootMUSIC_linear_array_impl::~rootMUSIC_linear_array_impl()
        {
        }

        void
        rootMUSIC_linear_array_impl::get_roots_polynomial(Eigen::MatrixXcf &A, Eigen::VectorXcf &roots)
        {
            Eigen::VectorXcf u(2 * d_num_ant_ele - 1);

            // determine the polynomial vector and normalize it
            for (int ii = -d_num_ant_ele + 1; ii < 0; ii++)
            {
                u(ii + d_num_ant_ele - 1) = A.diagonal(ii).sum();
                u(d_num_ant_ele - 1 - ii) = conj(u(ii + d_num_ant_ele - 1));
            }
            u(d_num_ant_ele - 1) = A.diagonal().sum();
            u = (gr_complex(-1.0, 0.0) / u(2 * d_num_ant_ele - 2)) * u;

            // assign u to the last-column of the Frobenius companion matrix
            d_comp_mat.col(2 * d_num_ant_ele - 3) = u.topRows(2 * d_num_ant_ele - 3);

            // determine its EVD to get roots of the polynomial vector

            Eigen::ComplexEigenSolver<Eigen::MatrixXcf> complex_eigensolver(d_comp_mat);
            roots = complex_eigensolver.eigenvalues();
        }

        int
        rootMUSIC_linear_array_impl::work(int noutput_items,
            gr_vector_const_void_star &input_items,
            gr_vector_void_star &output_items)
        {
        }
    }
}
```

```
const gr_complex *in = (const gr_complex *)input_items[0];
float *out = (float *)output_items[0];
// process each input vector (Rxx matrix)
Eigen::MatrixXcf eig_vec;
Eigen::VectorXcf eigval_roots;
Eigen::VectorXf dist;

Eigen::VectorXcf eigval_roots_inside;
Eigen::VectorXf dist_inside;

for (int item = 0; item < noutput_items; item++)
{
    // make input pointer into matrix pointer;
    Eigen::Map<Eigen::MatrixXcf> in_matrix((gr_complex *)in + item * d_num_ant_ele * d_num_ant_ele,
d_num_ant_ele, d_num_ant_ele);

    Eigen::Map<Eigen::VectorXf> out_vec(out + item * d_num_targets, d_num_targets);

    // determine EVD of the auto-correlation matrix
    Eigen::SelfAdjointEigenSolver<Eigen::MatrixXcf> hermitian_eigensolver(in_matrix);
    eig_vec = hermitian_eigensolver.eigenvalues();

    // noise subspace and its square matrix
    Eigen::MatrixXcf U_N = eig_vec.leftCols(d_num_ant_ele - d_num_targets);
    Eigen::MatrixXcf U_N_sq = U_N * U_N.adjoint();

    // determine the roots of the polynomial generated using U_N_sq
    get_roots_polynomial(U_N_sq, eigval_roots);

    // distance of the roots w.r.t from unit circle
    dist = 1.0 - eigval_roots.array().abs();

    dist_inside.resize(0);
    eigval_roots_inside.resize(0);

    for (Eigen::Index i = 0; i < dist.size(); ++i)
    {
        if (dist(i) > 0.0)
        {
            Eigen::Vector1::push_back<float>(dist_inside, dist(i));
            Eigen::Vector1::push_back<gr_complex>(eigval_roots_inside, eigval_roots(i));
        }
        else
        {
            // do nothing - skip
        }
    }

    // corner case when solutions are outside of unit circle (when sources have the same angle or there are
less visible sources than required)
    // some of the results are correct and it prevents runtime crashes
    if (dist_inside.size() == 0 || dist_inside.size() < d_num_targets)
    {
        dist = dist.array().abs();
        Eigen::Index min_dist_idx;
        while ((d_num_targets - dist_inside.size()) != 0)
        {
            // pick root closes to unity circle, even outside to prevent crashes
            dist.minCoeff(&min_dist_idx);
            Eigen::Vector1::push_back<float>(dist_inside, dist(min_dist_idx));
            Eigen::Vector1::push_back<gr_complex>(eigval_roots_inside, eigval_roots(min_dist_idx));
        }
    }

    Eigen::VectorXf aoa_vec(d_num_targets);
    Eigen::Index min_dist_idx;
    for (int ii = 0; ii < d_num_targets; ii++)
    {
        // find the roots that are closest to the unit circle
        dist_inside.minCoeff(&min_dist_idx);
        // locate the root and convert it to correct form
        aoa_vec(ii) = 180.0 * acos(arg(eigval_roots_inside(min_dist_idx)) / (2 * EIGEN_PI * d_norm_spacing)) /
EIGEN_PI;

        // discard this minimum to find the next minimum
        dist_inside(min_dist_idx) = float(INFINITY);
        eigval_roots_inside(min_dist_idx) = gr_complex(float(INFINITY), 0.0);
    }
    // sort the AoA vector
    // useful for display purposes
    std::sort(aoa_vec.data(), aoa_vec.data() + aoa_vec.size());

    memcpy((char *)&out[item * d_num_targets], (const char *)aoa_vec.col(0).data(), d_num_targets *
sizeof(float));
}
// Tell runtime system how many output items we produced.
```

```
        return noutput_items;  
    }  
    } /* namespace aoa */  
} /* namespace gr */
```

Κώδικας από <https://github.com/MarcinWachowiak/gr-aoa>.