



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΠΡΟΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

**Υλοποίηση τεχνικών ασφάλειας στο Φυσικό Στρώμα
στην OFDM με Software Defined Radios**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Πίττα Αντώνιου

Επιβλέπων: Μαλιάτσος Κωσταντίνος

Μέλη εξεταστικής επιτροπής: Βουγιούκας Δημοσθένης, Καλλίγερος Εμμανουήλ

Σάμος, Σεπτέμβριος 2023

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Ευχαριστώ την οικογένεια μου, την Ηρώ καθώς και τους συμφοιτητές μου Νίκο, Αβραάμ και Δέσποινα που με βοήθησαν να φτάσω έως εδώ.

© 2023

του

ΠΙΤΤΑΣ ΑΝΤΩΝΙΟΣ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1	Εισαγωγή	10
1.1	Ασφάλεια στο Φυσικό & SDR	10
1.2	Αντικείμενο διπλωματικής	10
2	Θεωρητικό Υπόβαθρο	12
2.1	Γενικά	12
2.1.1	Ασύρματες Επικοινωνίες	12
2.1.2	Ηλεκτρομαγνητικό Φάσμα	17
2.1.3	Ψηφιακές Επικοινωνίες	19
2.2	OFDM	22
2.2.1	Προκλήσεις, Εφαρμογές & Ζητήματα στην OFDM	28
2.3	Ασφάλεια στο Φυσικό Επίπεδο/Physical Layer Security	31
2.3.1	Γενικά	31
2.3.2	Τεχνικές Ασφάλειας στο Φυσικό	32
3	Software Defined Radio	42
3.1	Γενικά	42
3.2	Εφαρμογές	44
3.2.1	Ζώνες λειτουργίας	45
3.2.2	Πλεονεκτήματα	47

3.2.3	Μειονεκτήματα	48
3.3	Παραδείγματα Χρήσης.....	48
4	Πείραμα	51
4.1	Πλατφόρμες και Υλικό που χρησιμοποιήθηκαν.....	51
4.2	MATLAB.....	52
4.2.1	Matlab Transmitting and Receiving	54
4.3	GNU Radio	56
4.3.1	Δέκτης FM με το GNU Radio	58
5	Physical Layer Security with OFDM	60
5.1	Beamforming με OFDM	60
5.1.1	Πομπός – Beamformer, Alice.....	61
5.1.2	Δέκτης, Bob	70
5.1.3	Υποκλοπέας Eve	71
5.2	Αποτελέσματα.....	77
5.2.1	Σενάρια	77
5.2.2	Ρυθμός Μυστικότητας.....	85
6	Συμπεράσματα	91
7	Βιβλιογραφία	92

Λίστα Εικόνων & Γραφημάτων

Εικόνα 2-1: Δίαυλος Επικοινωνίας.....	13
Εικόνα 2-2: Επίδραση Σκέδασης σε ένα σήμα.....	14
Εικόνα 2-3: Επίδραση Ανάκλασης σε ένα σήμα.....	14
Εικόνα 2-4: Επίδραση Περίθλασης σε ηλεκτρομαγνητικά κύματα.....	15
Εικόνα 2-5: Απορρόφηση ηλεκτρομαγνητικών κυμάτων	15
Εικόνα 2-6: Επίδραση Διάθλασης σε ηλεκτρομαγνητικά κύματα.....	16
Εικόνα 2-7: Επίδραση Fast & Slow Fading σε σήμα ανάλογα την απόσταση	17
Εικόνα 2-8: Ονομασία ζωνών συχνοτήτων κατά IEEE & NATO.....	18
Εικόνα 2-9: Μπλοκ διάγραμμα για τον πομπό (πάνω) και το δέκτη (κάτω) της OFDM.....	23
Εικόνα 2-10: Διάγραμμα πομπού OFDM	23
Εικόνα 2-11: Διάγραμμα δέκτη OFDM (χωρίς μπλοκ συγχρονισμού)	25
Εικόνα 2-12: Κυκλικό πρόθεμα (προστασία από το κανάλι και σφάλματα συγχρονισμού).....	26
Εικόνα 2-13: Σύγκριση αποτελέσματος για Zero-Padded DFT.....	27
Εικόνα 2-14: SISO, SIMO, MIMO, MISO	33
Εικόνα 2-15: Σύστημα πομπού-δέκτη και υποκλοπέα	34
Εικόνα 4-1: QPSK Πομπός χρησιμοποιώντας USRP hardware.....	55
Εικόνα 4-2: QPSK Δέκτης χρησιμοποιώντας USRP hardware.....	55
Εικόνα 4-3: Ανάλυση του μπλοκ QPSK δέκτη για USRP hardware.....	56
Εικόνα 4-4: Διάγραμμα ροής - Flowgraph στο λογισμικό GNU Radio, Δέκτη FM.....	58

Εικόνα 4-5: Διαγράμματα από το Time/Frequency & Relative Gain/Frequency από QT Blocks του GNU Radio, Δέκτη FM.....	58
Εικόνα 4-6: Ολοκληρωμένος Δέκτης FM με USRP B200mini.....	59
Εικόνα 5-1: Πομπός 1ο μέρος.....	61
Εικόνα 5-2: Πομπός 2ο μέρος.....	63
Εικόνα 5-3: Πομπός 3ο μέρος.....	64
Εικόνα 5-4: Πομπός 4ο μέρος.....	65
Εικόνα 5-5: Παράμετροι για RF	68
Εικόνα 5-6: Παράμετροι για γενικά χαρακτηριστικά.....	69
Εικόνα 5-7: Δέκτης Bob, 1ο μέρος	70
Εικόνα 5-8: Δέκτης Bob, 2ο μέρος.....	71
Εικόνα 5-9: Δέκτης Eve, 1ο μέρος	71
Εικόνα 5-10: Δέκτης Eve, 2ο μέρος	72
Εικόνα 5-11: Δέκτης Eve, 2ο μέρος	72
Εικόνα 5-12: Μετρητικό σύστημα - τοποθεσία Alice, Bob και Eve.	78
Εικόνα 5-13: Το σύστημα της Alice, Ettus B210 & Lenovo IdeaPad3	79
Εικόνα 5-14: Με πράσινο, η απόσταση που χωρίζει το κοντινό USRP με τον δέκτη και με κίτρινο το μακρινό.....	80
Εικόνα 5-15: Bob και Eve για τα σενάρια 1 και 3.....	81
Εικόνα 5-16: Αποτελέσματα σηματοθορυβικού λόγου λήψης - Σύγκριση Bob & Eve.....	81
Εικόνα 5-17: Άποψη των Bob & Eve για τα σενάρια 2 & 4	82

Εικόνα 5-18: Αποτελέσματα λήψης σήματος και σύγκριση μεταξύ Bob & Eve.....	83
Εικόνα 5-19: Αποτελέσματα λήψης σήματος και σύγκριση μεταξύ Bob & Eve.....	84
Εικόνα 5-20: Αποτελέσματα λήψης σήματος και σύγκριση μεταξύ Bob & Eve.....	85
Εικόνα 5-21: Αποτελέσματα Ρυθμού Μυστικότητας του Bob, για τα Σενάρια 1 & 3.....	86
Εικόνα 5-22: Αποτελέσματα Ρυθμού Μυστικότητας του Bob, για τα Σενάρια 2 & 4.....	87
Εικόνα 5-23: Συγκριτικά Αποτελέσματα Ρυθμού Μετάδοσης, για όλα τα Σενάρια.....	88
Εικόνα 5-24: Ρυθμός μετάδοσης Bob πριν και μετά την εφαρμογή AN	90
Εικόνα 5-25: Ρυθμός μετάδοσης Eve πριν και μετά την εφαρμογή AN.....	90

Λίστα Πινάκων

Πίνακας 2-1: Συμβατική ονοματολογία Ζωνών Συχνοτήτων.....	18
Πίνακας 5-1: Διακοπή μυστικότητας ανά περίπτωση	88

Ακρωνύμια

SDR	Software Defined Radio
PHY-SEC	Physical Layer Security
AN	Artificial Noise
ZF	Zero Forcing
RF	Radio Frequency
CSI	Channel State Information

Περίληψη

Η ευρεία ανάπτυξη τόσο του Διαδικτύου των Πραγμάτων όσο και η ολοένα αυξανόμενη ανάγκη για εξασφάλιση της ασφάλειας στις τηλεπικοινωνίες έχουν δημιουργήσει ζήτηση για νέα αποδοτικά τηλεπικοινωνιακά συστήματα. Σύγχρονες συσκευές και λογισμικό που μειώνουν το κόστος της επικοινωνίας ενώ ταυτόχρονα αυξάνουν το επίπεδο ασφάλειας αναπτύσσονται αυτή τη στιγμή. Το Software Defined Radio (SDR) αποτελεί ένα τέτοιο σύγχρονο σύστημα που αποδίδει τις λειτουργίες των αναλογικών hardware συστημάτων επεξεργασίας σήματος σε ψηφιακούς επεξεργαστές και FPGA κάτι που επιτρέπει μεγαλύτερη ευελιξία στην χρήση των περιφερειακών του Front-end RF κομματιού.

Το αντικείμενο της εργασίας αυτής είναι η εφαρμογή τεχνικών Ασφάλειας στο Φυσικό επίπεδο με την χρήση Software Defined Radio. Εξετάζεται μέσω πειραμάτων τόσο το θεωρητικό μέρος της εφαρμογής τεχνικών ασφάλειας στο Φυσικό Επίπεδο/Physical Layer Security (PLS) σε ένα τηλεπικοινωνιακό σύστημα όσο και την δυνατότητα εφαρμογής σε πραγματικές συνθήκες υπό κλίμακα.

Για την διεξαγωγή των πειραμάτων γίνονται δοκιμές με διαφορετικού τύπου λογισμικά για την διερεύνηση καλύτερης τηλεπικοινωνιακής εκπομπής και λήψης καθώς και προσομοίωσης θεωρητικών μοντέλων με σκοπό την εξαγωγή συμπερασμάτων.

Λέξεις Κλειδιά: Ασφάλεια Φυσικού Επιπέδου, Συστήματα ορισμένα από λογισμικό, Διαμόρφωση ορθογωνικής πολυπλεξίας συχνότητας, ασύρματες επικοινωνίες, διαμόρφωση διαγράμματος ακτινοβολίας, τεχνητός θόρυβος, USRP

Abstract

The widespread development of both the Internet of Things and the ever-increasing need to ensure security in telecommunications have created a demand for new efficient telecommunications systems. Modern devices and software that reduce the cost of communication while simultaneously increasing the level of security are currently being developed. Software Defined Radio (SDR) is one such modern system that renders the functions of analog hardware signal processing systems to digital FPGAs, which allows greater flexibility in the use of the peripherals of the Front-end RF part.

The subject of this work is the application of Security techniques at the Physical level using Software Defined Radio. Both the theoretical part of the application of Physical Layer Security (PLS) techniques in a telecommunications system and the applicability in real conditions at scale are examined through experiments.

To conduct the experiments, tests are carried out with different types of software to investigate better telecommunication transmission and reception as well as simulation of theoretical models in order to draw conclusions.

Key Words: Physical Layer Security, Software Defined Radios (SDR), Orthogonal Frequency Division Multiplexing (OFDM), wireless communications, beamforming, artificial noise, USRP

1

Εισαγωγή

1.1 Ασφάλεια στο Φυσικό & SDR

Οι τεχνικές Ασφάλειας στο Φυσικό τείνουν να αποκτήσουν ζωτική σημασία για την αξιοπιστία, την απόδοση και την ασφάλεια της επικοινωνίας. Μία από τις πιο επαναστατικές προσεγγίσεις στον τομέα του πειραματισμού και ανάπτυξης των τεχνικών αυτών είναι μέσω των SDR - Software Defined Radios, τα οποία επιτρέπουν την υλοποίηση των λειτουργιών του φυσικού στρώματος μέσω λογισμικού, προσφέροντας μεγάλη ευελιξία και δυνατότητες προσαρμογής.

1.2 Αντικείμενο διπλωματικής

Στόχος είναι η δημιουργία ενός τηλεπικοινωνιακού μοντέλου και ενός πειραματικού πεδίου δοκιμών το οποίο θα διαθέτει στοιχεία Ασφάλειας στο Φυσικό Επίπεδο μέσω των μεθόδων του Τεχνητού Θορύβου (Artificial Noise) και της Διαμόρφωσης Διαγράμματος Ακτινοβολίας (Beamforming). Το ζητούμενο είναι να επιτευχθεί ασφαλής επικοινωνία μεταξύ 2 μερών. Συγκεκριμένα γίνεται μια έρευνα για επίτευξη πλήρους προστασίας μέσω της τεχνικής Beamforming & Artificial Noise. Αρχικά θα γίνουν οι απαραίτητες δοκιμές σε περιβάλλον προσομοίωσης και μετέπειτα μέσω ενός τηλεπικοινωνιακού συστήματος με τη χρήση USRP και Software Defined Radio. Σε αυτή τη εργασία,

γίνεται χρήση Software Defined Radios (SDRs) της σειράς των B200mini, B210 & X310 μέσω GNU Radio σε λογισμικό Ubuntu 20.04 και της Matlab/Simulink Matlab σε λογισμικό Windows 11.

2

Θεωρητικό Υπόβαθρο

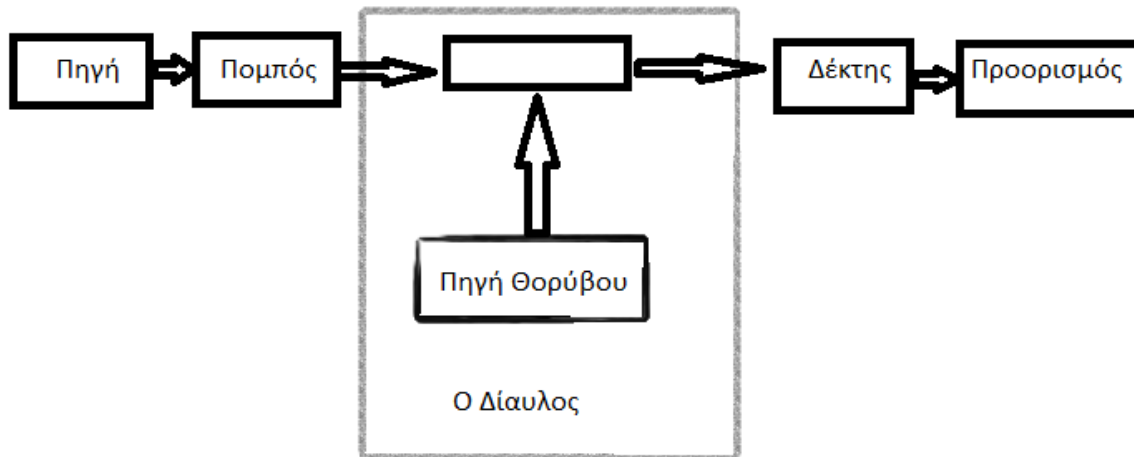
2.1 Γενικά

2.1.1 Ασύρματες Επικοινωνίες

Θέτοντας τη θεωρητική βάση την κατανόηση του αντικειμένου της παρούσας εργασίας είναι οι Ασύρματες Επικοινωνίες. Αρχικά, κρίσιμη θεωρείται η έννοια του Ασύρματου Διαύλου, η οποία αποτελεί το βασικό θεωρητικό κομμάτι των Ασύρματων Επικοινωνιών είτε αυτά αφορά την ραδιοτηλεδοποίηση, κινητές τηλεπικοινωνίες, δορυφορικά συστήματα κλπ. Η βασική αρχιτεκτονική ενός τυπικού συστήματος επικοινωνιών ασύρματου [1], παρουσιάζεται στο σχήμα.

Δίνοντας τον τυπικό ορισμό, μια πηγή πληροφοριών επιχειρεί να αποστείλει πληροφορίες σε έναν προορισμό. Τα δεδομένα μετατρέπονται σε σήμα κατάλληλο για την αποστολή από τον πομπό και στη συνέχεια αποστέλλονται μέσω του διαύλου. Ο διάυλος μπορεί να μεταβάλλει το σήμα με διάφορους τρόπους. Για αυτόν τον λόγο, ο Δέκτης πρέπει να βρίσκεται σε θέση να επεξεργαστεί το σήμα ώστε να το παραδώσει στον προορισμό του χωρίς αλλοιώσεις και χωρίς λάθη.

Στην περίπτωση του ασύρματου Διαύλου, οι πηγές θορύβου ξεχωρίζουν στις πολλαπλασιαστικές και τις προσθετικές επιδράσεις.



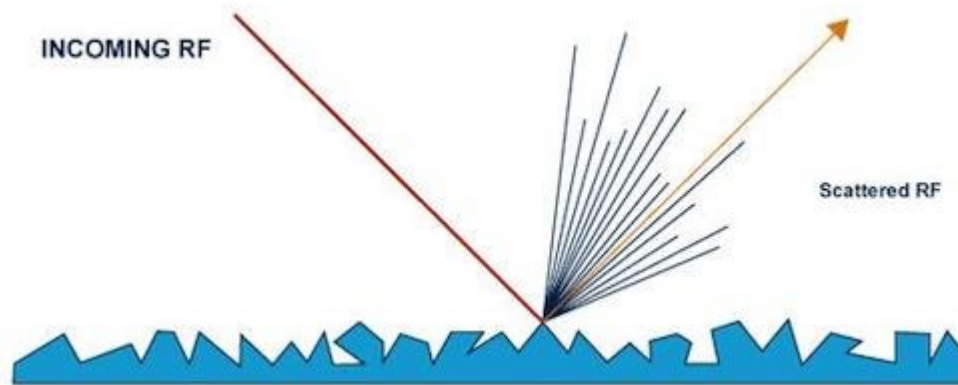
Εικόνα 2-1: Δίαυλος Επικοινωνίας

Ο προσθετικός θόρυβος προκύπτει από τον θόρυβο που ο ίδιος ο πομπός μπορεί να παράξει (π.χ. θόρυβος βολής στοιχείων), θερμικούς, ατμοσφαιρικούς, κοσμικούς παράγοντες κ.α.

Ο πολλαπλασιαστικός θόρυβος αφορά τις διάφορες διεργασίες κατά την ασύρματη διάδοσή των κυμάτων ανάμεσα από την κεραία λήψης και εκπομπής τους.

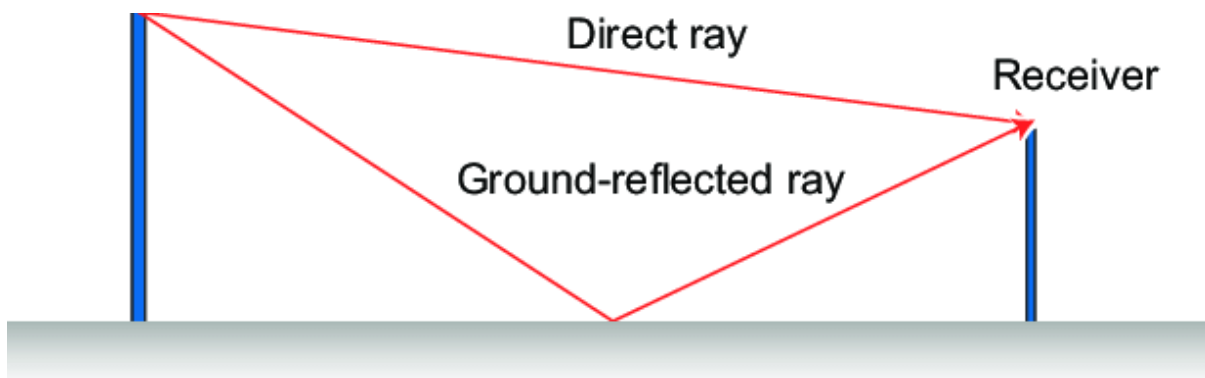
Ειδικότερα, οι διεργασίες αυτές ονομάζονται:

Σκέδαση/Scattering: Όταν ένα ηλεκτρομαγνητικό κύμα έρχεται σε επαφή με τραχιές επιφάνειες όπως η θάλασσα, κτήρια ή σε ανώμαλο έδαφος, τότε αυτό υπόκειται σε σκέδαση και υπάρχει διάδοση των ακτινών του αρχικού σήματος σε πολλές διευθύνσεις. Αυτό μπορεί να προκαλέσει προβλήματα σε συστήματα ασύρματων επικοινωνιών [2].



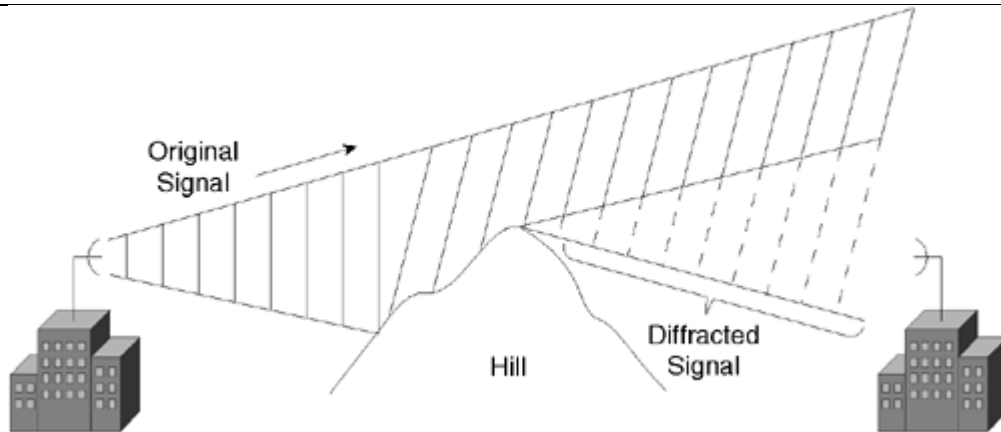
Εικόνα 2-2: Επίδραση Σκέδασης σε ένα σήμα

Ανάκλαση/Reflection: Προκαλείται από λείες επιφάνειες που συναντά το σήμα, και αυτό έχει ως αποτέλεσμα να φτάνουν στον δέκτη τόσο η ακτίνα άμεσα από τον πομπό αλλά -και σε δεύτερο χρόνο- η ανακλώμενη ακτίνα. Το φαινόμενο αυτό μπορεί να προκαλέσει ή να έχει μεγάλη συνεισφορά στο φαινόμενο του multipath fading, με τα διαφορετικά σήματα άμεσα ή ανακλώμενα να δημιουργούν παρεμβολές φτάνοντας στο δέκτη [2].



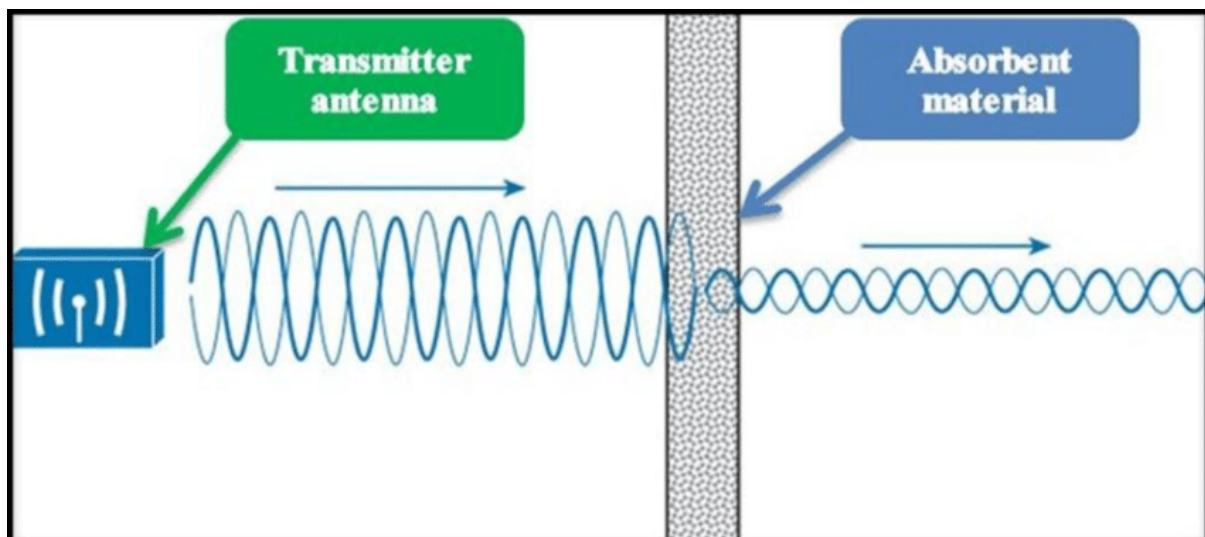
Εικόνα 2-3: Επίδραση Ανάκλασης σε ένα σήμα

Περίθλαση/Diffraction: Μέρος των ηλεκτρομαγνητικών κυμάτων, κάμπτονται από φυσικές ακμές (στέγες κτιρίων/κορυφές λόφων κ.α.) εξαιτίας της περίθλασης και μεταδίδονται στο κενό που υπάρχει πίσω από αυτές [3].



Εικόνα 2-4: Επίδραση Περίθλασης σε ηλεκτρομαγνητικά κύματα

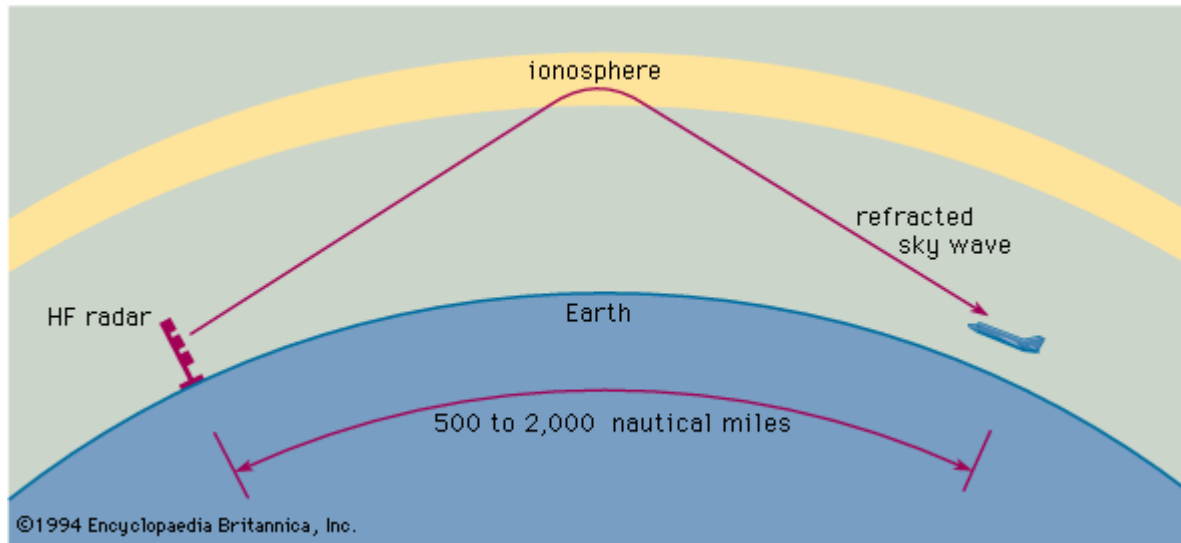
Απορρόφηση/Absorption: Στην μετάδοση κυμάτων μπορεί τα ηλεκτρομαγνητικά κύματα να εκπέσουν πάνω σε διάφορα υλικά (π.χ. τοίχους, έδαφος κ.α.) και αυτά να απορροφήσουν ή να εξασθενίσουν μέρος της ηλεκτρομαγνητικής ακτινοβολίας. Υλικά με μεγάλη απορρόφηση χρησιμοποιούνται για τη κατασκευή ανηχοϊκών θαλάμων που προορίζονται για δοκιμές ηλεκτρομαγνητικών συστημάτων όσο υλικά τεχνολογίας stealth [4].



Εικόνα 2-5: Απορρόφηση ηλεκτρομαγνητικών κυμάτων

Διάθλαση/Refraction: Σε αυτή τη εξειδικευμένη περίπτωση υπάρχει το φαινόμενο όπου για συγκεκριμένες συχνότητες σε κάποια ατμοσφαιρικά στρώματα μπορεί να υπάρξει διάθλαση

του μεταδιδόμενου ηλεκτρομαγνητικού κύματος και αυτό να “ταξιδέψει” σε μακρινές αποστάσεις. Αυτό παρατηρείται ειδικά με την Ιονόσφαιρα και τις επικοινωνίες σε HF [4]



Εικόνα 2-6: Επίδραση Διάθλασης σε ηλεκτρομαγνητικά κύματα

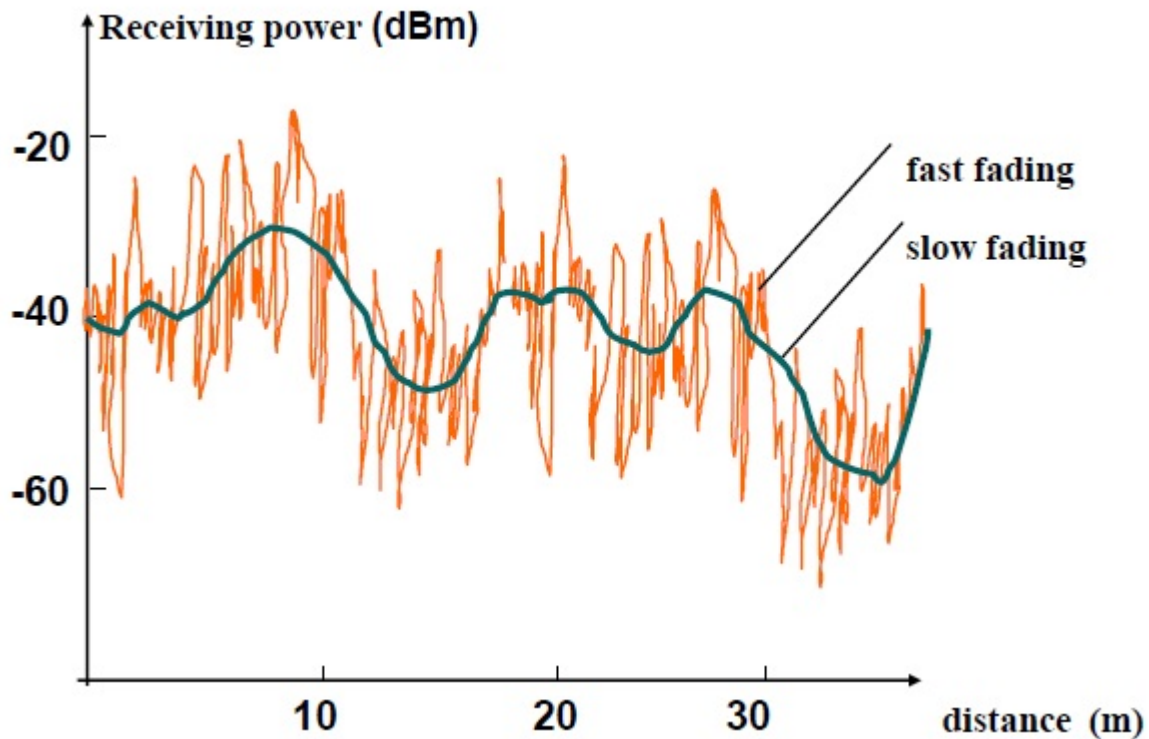
Εξαιτίας των παραπάνω διεργασιών που μπορεί να συμβούν σε ένα ηλεκτρομαγνητικό κύμα, παρατηρούνται συνολικά φαινόμενα όπως η σκίαση/ αργές διαλείψεις (slow fading) του διαύλου και γρήγορες διαλείψεις (fast fading) πάνω στο λαμβανόμενο σήμα ενός κινούμενου τηλεπικοινωνιακού συστήματος[8].

Οι γρήγορες διαλείψεις, προκαλούνται από τη πολυδιαδρομική μετάδοση (multipath) του σήματος που προκαλούν ενισχυτική ή καταστροφική επίδραση στην ισχύ του σήματος. Αυτό έχει ως αποτέλεσμα πολύ σύντομες διακυμάνσεις στη φάση και την ένταση και πλάτος του σήματος σε μικρή απόσταση.

Αντίστοιχα οι αργές διαλείψεις/shadowing, προκαλούνται από μεγάλα ή πολύ μεγάλα αντικείμενα και όγκους που παρεμβάλλεται μεταξύ 2 σημείων που επικοινωνούν ασύρματα. Αυτό έχει ως αποτέλεσμα τη σταδιακή μείωση της ισχύος του σήματος ανάλογα και με την απόσταση που διανύεται.

Είναι σημαντικό να αναφέρουμε ότι τόσο οι αργές όσο και οι γρήγορες διαλείψεις επηρεάζουν την μέση ισχύ του σήματος, με τη διαφορά ότι οι γρήγορες διαλείψεις έχουν πιο πολύ στιγμιαίο αντίκτυπο και οι αργές συμβαίνουν με χαμηλότερο βαθμό και σε πιο μεγάλο χωρικό εύρος [5].

Παρακάτω παρατίθεται ένα τυπικό διάγραμμα διακύμανση της λήψης ισχύος ενός σήματος σε σχέση με την απόσταση εξαιτίας της επίδρασης γρήγορων και αργών διαλείψεων.



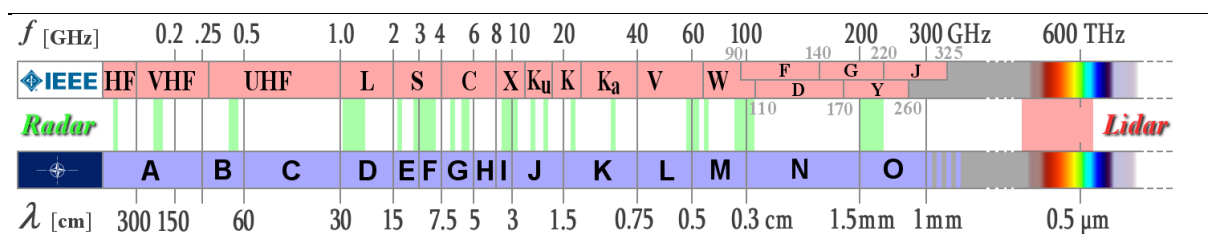
Εικόνα 2-7: Επίδραση Fast & Slow Fading σε σήμα ανάλογα την απόσταση

2.1.2 Ηλεκτρομαγνητικό Φάσμα

Τα τηλεπικοινωνιακά συστήματα λειτουργούν πάνω σε συγκεκριμένες συχνότητες του ηλεκτρομαγνητικού φάσματος. Η διάδοση στις σημερινές συνθήκες γίνεται στις συχνότητες από 3 KHz έως και 200 GHz, ενώ ολοένα και οδεύουμε στις επικοινωνίες THz.

Παρακάτω παρατίθεται εικόνα που δείχνει τους διαφορετικούς τρόπους διαίρεσης του φάσματος σε ζώνες συχνοτήτων καθώς και τις σχετικές ονοματοδοσίες τους από τον [Institute of Electrical and Electronics Engineers](#) (IEEE) και κατά NATO.

Radios



Εικόνα 2-8: Ονομασία ζωνών συχνοτήτων κατά IEEE & NATO

Πίνακας 2-1: Συμβατική ονοματολογία Ζωνών Συχνοτήτων

Ζώνη	Περιοχή συχνοτήτων	Προέλευση ονομασίας
HF band	3 - 30 MHz	High Frequency
VHF band	30-300 MHz	Very High Frequency
UHF band	300-1000 MHz	Ultra High Frequency Η περιοχή από 216 έως 450 MHz μερικές φορές ονομαζόταν P-band: Παλαιότερα, διότι τα βρετανικά ραντάρ χρησιμοποιούσαν τη ζώνη αυτή αλλά αργότερα μεταπήδησαν σε υψηλότερες συχνότητες.
L band	1 - 2 GHz	Long wave
S band	2 - 4 GHz	Short wave
C band	4 - 8 GHz	Compromise (συμβιβασμός) ανάμεσα στο S και το X
X band	8 - 12 GHz	Χρησιμοποιήθηκε κατά το Β' Παγκόσμιο Πόλεμο για συστήματα ελέγχου πυρός, το X θυμίζει το σταυρόνημα σκόπευσης.
<u>K_u band</u>	12-18 GHz	Kurz-under
<u>K band</u>	18 - 27 GHz	Kurz (βραχύς, στα Γερμανικά)

<u>K_a band</u>	27-40 GHz	Kurz-above
<u>V band</u>	40 - 75 GHz	
<u>W band</u>	75 - 110 GHz	Το W ακολουθεί το V στο αγγλικό αλφάβητο
<u>mm band</u>	110 - 300 GHz	(χιλιοστομετρικά κύματα)

2.1.3 Ψηφιακές Επικοινωνίες

Για την εκπόνηση της εργασίας έγινε θεώρηση και χρήση Ψηφιακών Συστημάτων. Συγκεκριμένα έγινε χρήση Ψηφιακών Συστημάτων Διαμόρφωσης και Αποδιαμόρφωσης.

Τα Ψηφιακά Συστήματα Διαμόρφωσης χρησιμοποιούνται σε ενσύρματες και ασύρματες επικοινωνίες. Σκοπός τους είναι η μετάδοση ψηφιακής πληροφορίας μέσω αναλογικής φέρουσας σταθερής συχνότητας και πλάτους.

Τα συστήματα αυτά παρουσιάζουν μεγάλη ανοχή στον θόρυβο και δυνατότητα για εφαρμογή καλύτερων τεχνικών επεξεργασίας σήματος, κρυπτογράφησης και πολυπλεξίας.

Τα ψηφιακά συστήματα με αναλογική φέρουσα συχνότητα μεταβάλλουν κάποια παράμετρο της αναλογικής φέρουσας (πλάτος/συχνότητα/φάση ή συνδυασμός μεταξύ τους) σε διακριτές τιμές ανάλογα το σήμα. Αυτές οι διακριτές τιμές αποτελούν τα σύμβολα της διαμόρφωσης τα οποία αναπαρίστανται από b πλήθος bits. Κάθε μπλοκ b bits αντιστοιχεί σε:

$M = 2^b$ σύμβολα.

Η επιλογή της τεχνικής ψηφιακής διαμόρφωσης εξαρτάται από τις αντίστοιχες απαιτήσεις. Παράμετροι που λαμβάνονται υπόψη για αυτή την επιλογή είναι ο βαθμός απόδοσης ισχύος/power efficiency, ο φασματικός βαθμός απόδοσης/bandwidth efficiency, η αντοχή στις παρεμβολές/θόρυβο και οι παραμορφώσεις που εισάγονται στο κανάλι μετάδοσης, η συμπεριφορά στις διαλείψεις και στις πολυδιαδρομικές μεταδόσεις ενώ επίσης λαμβάνεται

υπόψη η πολυπλοκότητα και το κόστος υλοποίησης του ίδιου του τηλεπικοινωνιακού συστήματος [6].

Οι πιο βασικές διαμορφώσεις ψηφιακών επικοινωνιών είναι οι Binary Phase Shift Keying (BPSK), η Quadrature Phase Shift Keying (QPSK), η Quadrature Amplitude Modulation (QAM), η Frequency Shift Keying (FSK) και Amplitude Shift Keying (ASK). Οι παραπάνω διαμορφώσεις διαφοροποιούνται στα χαρακτηριστικά που αφορούν τον τρόπο που γίνεται η κωδικοποίηση των δεδομένων σε ψηφιακά διακριτά σύμβολα. Εν συντομία παρατίθενται παρακάτω:

BPSK:

- Η BPSK χρησιμοποιεί δύο καταστάσεις φάσης για να αναπαραστήσει δυαδικά δεδομένα (0 και 1).
- Στην BPSK, μια κατάσταση φάσης (π.χ. 0°) αντιπροσωπεύει ένα δυαδικό σύμβολο και μια άλλη κατάσταση φάσης (π.χ. 180°) αντιπροσωπεύει το άλλο σύμβολο.
- Είναι ανθεκτική έναντι του θορύβου και χρησιμοποιείται συχνά ως η απλούστερη μορφή ψηφιακής διαμόρφωσης.

QPSK:

- Η QPSK χρησιμοποιεί τέσσερις καταστάσεις φάσης για να αναπαραστήσει δύο bit δεδομένων.
- Διαιρεί τον κύκλο φάσης σε τέσσερα ίσα τμήματα και κάθε συνδυασμός δύο γειτονικών τμημάτων αντιπροσωπεύει ένα μοναδικό σύμβολο 2 bit.
- Η QPSK είναι πιο αποδοτική ως προς το εύρος ζώνης από η BPSK και χρησιμοποιείται ευρέως σε ψηφιακά συστήματα επικοινωνίας.

QAM:

- Η QAM συνδυάζει διαμόρφωση πλάτους και φάσης.

- Χρησιμοποιεί ένα διάγραμμα αστερισμού με πολλαπλά σημεία, όπου κάθε σημείο αντιπροσωπεύει ένα μοναδικό σύμβολο.
- Η QAM διατίθεται σε διάφορες μορφές, όπως 16-QAM ή 64-QAM, με διαφορετικούς αριθμούς σημείων αστερισμού.
- Χρησιμοποιείται σε πολλά συστήματα ψηφιακών επικοινωνιών υψηλής ταχύτητας όπως 4G, 5G, DSL και καλωδιακά μόντεμ.

FSK:

- Το FSK διαμορφώνει τη φέρουσα συχνότητα για να αντιπροσωπεύει ψηφιακά σύμβολα.
- Στο δυαδικό FSK (BFSK), δύο διακριτές συχνότητες αντιπροσωπεύουν τα δύο δυαδικά σύμβολα (0 και 1).
- Χρησιμοποιείται συνήθως σε πρώιμα μόντεμ και σε ορισμένες εφαρμογές ασύρματης επικοινωνίας.

ASK:

- Η ASK διαμορφώνει το πλάτος του φέροντος σήματος για να αναπαραστήσει ψηφιακά σύμβολα.
- Το πλάτος ποικίλλει για την κωδικοποίηση δυαδικών συμβόλων.
- Η ASK χρησιμοποιείται σε απλά συστήματα οπτικών επικοινωνιών και σε ορισμένες εφαρμογές RFID.

Αυτά τα βασικά σχήματα διαμόρφωσης χρησιμοποιούνται ως δομικά στοιχεία σε ψηφιακά συστήματα επικοινωνίας. Πιο πολύπλοκα σχήματα διαμόρφωσης, όπως τα 8-QPSK, 16-QAM ή 256-QAM, προσφέρουν υψηλότερους ρυθμούς δεδομένων κωδικοποιώντας πολλαπλά bit ανά σύμβολο. Η επιλογή του σχήματος διαμόρφωσης εξαρτάται από παράγοντες όπως οι απαιτήσεις για μετάδοση υψηλού ρυθμού δεδομένων, το διαθέσιμο εύρος ζώνης και η

αναλογία σήματος προς θόρυβο του καναλιού επικοινωνίας. Προηγμένες τεχνικές όπως η Ορθογώνια Πολυπλεξία Διαίρεσης Συχνότητας/Orthogonal Frequency Division Multiplexing (OFDM) χρησιμοποιούν επίσης αυτές τις βασικές διαμορφώσεις σε κάθε subcarrier (φορέας χαμηλότερης ισχύος ή συχνότητας που φέρει μέρος της πληροφορίας) για να επιτύχουν ακόμη υψηλότερους ρυθμούς δεδομένων και στα σύγχρονα συστήματα επικοινωνίας.

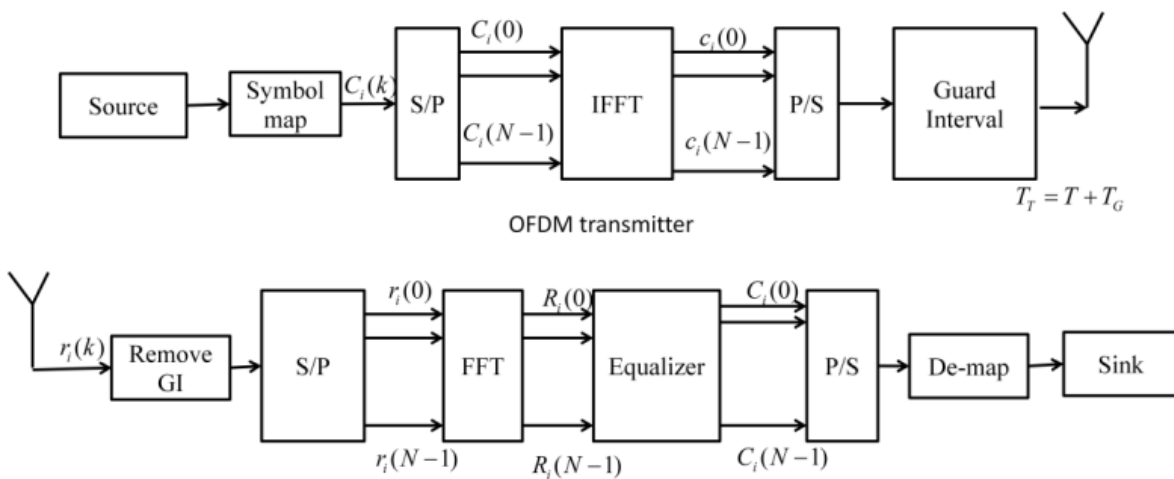
2.2 OFDM

Στο πειραματικό μέρος της εργασίας γίνεται χρήση της Orthogonal Frequency Division Multiplexing μέσω των περιφερειακών Software Defined Radio X310, B210 και B200mini.

Το βασικό θεωρητικό υπόβαθρο για την OFDM παρατίθεται παρακάτω.

Η OFDM αποτελεί μια διαμόρφωση πολλαπλών φερόντων Multi-Carrier Modulation η οποία διαμορφώνει τα προς διαμόρφωση σύμβολα που πρέπει να εκπεμφθούν σε ορθογώνια μεταξύ τους subcarriers (υπο-φορείς). Στην προσπάθεια να εκπεμφθούν παράλληλα ταυτόχρονα N αριθμός sub-streams που μεταφέρουν δεδομένα, πρέπει να υπάρχουν αντίστοιχα N ορθογώνια subcarriers. Αυτό μπορεί να γίνει μέσω της χρήσης του Αντίστροφου Διακριτού Μετασχηματισμού Fourier (Inverse Discrete Fourier Transform (IDFT)) ή του Γρήγορου (αντίστροφου) Μετασχηματισμού Fourier (Inverse Fast Fourier Transform (IFFT)), στο διακριτό πεδίο τιμών και το προκύπτον σήμα εκπέμπεται σειριακά. Η πληροφορία στον δέκτη λαμβάνεται με τη χρήση μιας μονάδας DFT/FFT. Πάμε όμως να αναλύσουμε πιο λεπτομερώς το σύστημα της OFDM.

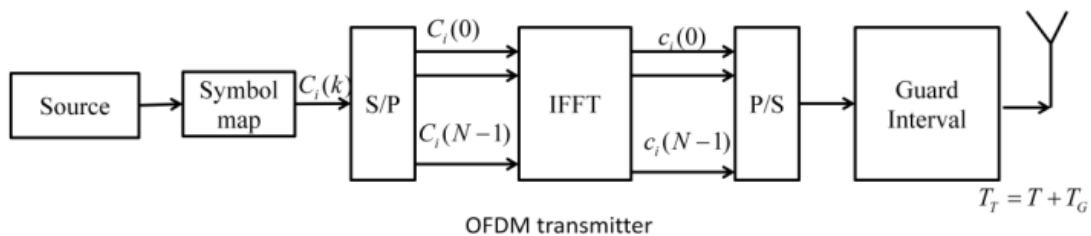
Παρακάτω παρατίθεται το σχεδιάγραμμα ενός πομπο-δέκτη OFDM, με το πάνω σύνολο μπλοκ να επιδεικνύει τις λειτουργίες και τις διαδικασίες δημιουργίας σήματος OFDM στον πομπό και το κάτω, να παρουσιάζει τις αντίστοιχες λειτουργίες του δέκτη [13].



Εικόνα 2-9: Μπλοκ διάγραμμα για τον πομπό (πάνω) και το δέκτη (κάτω) της OFDM

Ας δούμε ξεχωριστά τώρα τις δυο διαδικασίες, ξεκινώντας από τον πομπό .

Λειτουργία Πομπού στην OFDM:



Εικόνα 2-10: Διάγραμμα πομπού OFDM

Ο πομπός της OFDM λειτουργεί συνοπτικά ως εξής:

- **Πηγή - Source**

Πρόκειται για την πηγή των δεδομένων που πρέπει να μεταδοθούν. Τα δεδομένα είναι συνήθως σε ψηφιακή μορφή, όπως bits ή bytes.

- **Ψηφιακή διαμόρφωση συμβόλων - Symbol map**

Το ψηφιακό σήμα από την πηγή υποβάλλεται σε διαμόρφωση, όπου τα bits μετατρέπονται σε σύμβολα. Αυτά τα σύμβολα μπορούν να αντιπροσωπεύουν πολλαπλά bits και συχνά λαμβάνουν μιγαδικές τιμές (με πραγματικό και φανταστικό μέρος) βάσει του σχήματος διαμόρφωσης που ακολουθείται, όπως η QAM (Quadrature Amplitude Modulation) ή η PSK (Phase Shift Keying).

- **S/P (Μετατροπή από Σειριακή σε Παράλληλη - Serial to Parallel)**

Αυτό το στάδιο μετατρέπει τη σειριακή ροή των συμβόλων σε πολλαπλές παράλληλες ροές. Προετοιμάζει τα δεδομένα για να επεξεργαστούν παράλληλα, διασφαλίζοντας ότι κάθε ροή δεδομένων θα διαμορφώσει το δικό της υπο-φορέα στο επόμενο στάδιο.

- **IFFT (Inverse Fast Fourier Transform)**

Οι παράλληλες ροές δεδομένων μετατρέπονται από το συχνοτικό πεδίο στο χρονικό πεδίο χρησιμοποιώντας το IFFT. Συνεπώς, λαμβάνει σύμβολα που έχουν προετοιμαστεί στο πεδίο συχνοτήτων και τα χαρτογραφεί στο χρονικό πεδίο, δημιουργώντας τα σύμβολα OFDM. Κάθε σύμβολο περιέχει τώρα πληροφορίες από πολλαπλές παράλληλες ροές δεδομένων, διαμορφώνοντας τον δικό της υπο-φορέα.

- **P/S (Μετατροπή από Παράλληλη σε Σειριακή - Parallel to Serial)**

Μετά τον IFFT, τα χρονικά σύμβολα OFDM, τα οποία επεξεργάζονται παράλληλα, μετατρέπονται πίσω σε μια σειριακή ροή για μετάδοση.

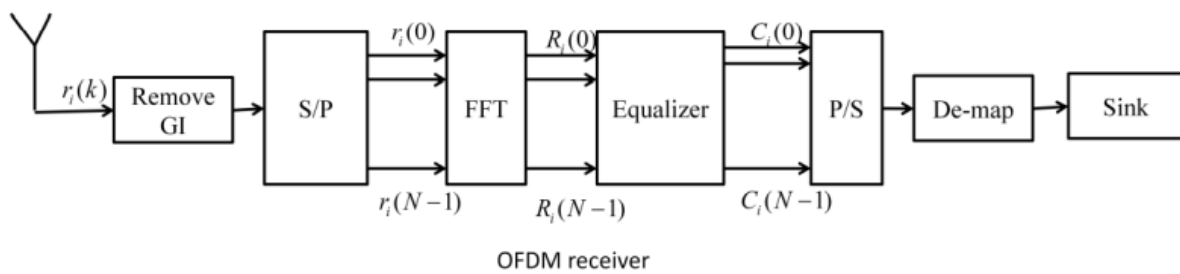
- **Διάστημα φύλαξης - Guard Interval**

Πρόκειται για μια προστατευτική διαδικασία για την πρόληψη παρεμβολών μεταξύ διαδοχικών συμβόλων OFDM. Ένα τμήμα του τέλους κάθε συμβόλου OFDM αντιγράφεται και προστίθεται στην αρχή του ίδιου συμβόλου, δημιουργώντας αυτό που είναι γνωστό ως κυκλικό πρόθεμα - cyclic prefix. Αυτό διασφαλίζει ότι ακόμη και αν υπάρχει καθυστέρηση και η αρχή ενός συμβόλου παρεμβάλλεται με το τέλος του προηγούμενου συμβόλου, τα δεδομένα δεν παραμορφώνονται - χάνονται επειδή επαναλαμβάνονται στο cyclic prefix. Ο συνολικός χρόνος T_t για το σύμβολο OFDM

με το guard interval είναι το άθροισμα του πραγματικού χρόνου του συμβόλου OFDM, T , και του guard interval T_G . Το κυκλικό πρόθεμα μετατρέπει επίσης τη διαδικασία της γραμμικής συνέλιξης του σήματος με το κανάλι, σε κυκλική συνέλιξη δίνοντας τη δυνατότητα χρήσης εύκολων και απλών μεθόδων εξισορρόπησης καναλιού (one-tap frequency equalizer).

Στην ουσία, ο πομπός OFDM διασφαλίζει ότι τα δεδομένα διαμορφώνονται σε πολλές ορθογώνιες συχνότητες, εκμεταλλευόμενος αποτελεσματικά το φάσμα και παρέχοντας αντίσταση σε διάφορα είδη παρεμβολών και στο φαινόμενο multipath.

Λειτουργία Δέκτη στην OFDM:



Εικόνα 2-11: Διάγραμμα δέκτη OFDM (χωρίς μπλοκ συγχρονισμού)

Ο δέκτης της OFDM λειτουργεί συνοπτικά όπως στο σχήμα, με κύρια block τα εξής:

- **Equalizer (Εξισορρόπηση)**

Σε πραγματικές συνθήκες μετάδοσης, το σήμα μπορεί να επηρεαστεί από διάφορες παραμορφώσεις του ραδιοδιαύλου, όπως οι διαλείψεις (fading). Ο equalizer αντισταθμίζει αυτές τις δυσλειτουργίες για να ανακτήσει τα αρχικά δεδομένα. Ουσιαστικά, προσαρμόζει τα πλάτη και τις φάσεις των ληφθέντων υπο-φορέων OFDM για να αντισταθμίσει τις επιδράσεις του καναλιού. Λόγω του κυκλικού προθέματος, στην OFDM η διαδικασία εκτίμησης και εξισορρόπησης καναλιού απλοποιείται σημαντικά (πρακτικά σε έναν πολλαπλασιασμό ανά subcarrier).

- **P/S (Parallel to Serial)**

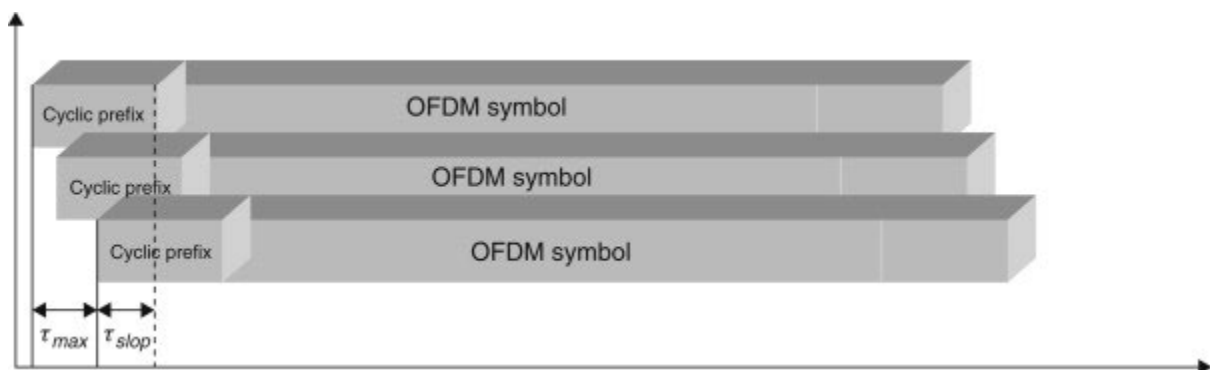
Οι παράλληλες ροές δεδομένων, πλέον στον τομέα συχνότητας, μετατρέπονται πίσω σε μια συνεχή σειριακή ροή. Αυτό προετοιμάζει τα δεδομένα για την αποχαρτογράφηση.

- **Ψηφιακή Αποδιαμόρφωση - Symbol Demap**

Αυτή η διαδικασία περιλαμβάνει την αντίστροφη της αρχικής χαρτογράφησης συμβόλων που έγινε στον πομπό. Τα μιγαδικά σύμβολα μετατρέπονται πίσω στα αρχικά δυαδικά δεδομένα.

- **Τελικό στάδιο (Καταβόθρα) Sink**

Τέλος, τα ανακατασκευασμένα δυαδικά δεδομένα στέλνονται στο sink ή την έξοδο του δέκτη, ολοκληρώνοντας έτσι τη λήψη και την αποκωδικοποίηση των μεταδοθέντων δεδομένων.



Εικόνα 2-12: Κυκλικό πρόθεμα (προστασία από το κανάλι και σφάλματα συγχρονισμού)

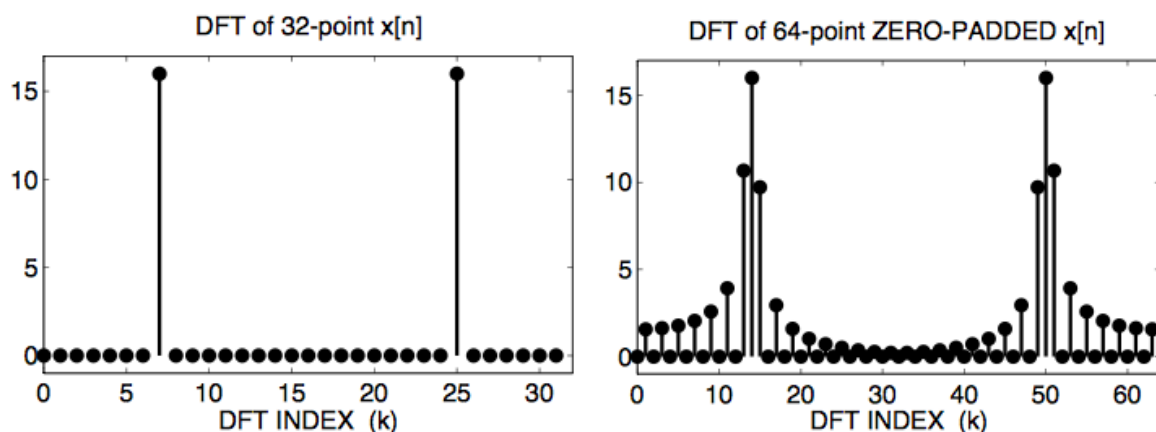
Στον πομπό OFDM, όταν αναφέραμε ότι το διάστημα φύλαξης ('Guard Interval'), αντιστοιχεί στο κυκλικό πρόθεμα ('Cyclic Prefix') που φαίνεται σε αυτό το διάγραμμα. Το διάστημα προστασίας ή το κυκλικό πρόθεμα προστίθεται για να διασφαλιστεί ότι τα σύμβολα OFDM προστατεύονται από παρεμβολές στο περιβάλλον μετάδοσης.

Από την πλευρά του δέκτη, όταν αναφερόμαστε στην «Κατάργηση του GI», γίνεται λόγος για τη διαδικασία αφαίρεσης αυτού του κυκλικού προθέματος (ή του διαστήματος προστασίας) πριν από την επεξεργασία του πραγματικού συμβόλου OFDM. Αφαιρώντας το κυκλικό πρόθεμα, ο δέκτης μπορεί να εστιάσει στο κύριο σύμβολο OFDM, το οποίο περιέχει τα πραγματικά δεδομένα που πρέπει να αποκωδικοποιηθούν [9].

Η παρεμβολή που προκαλείται από το φαινόμενο της Inter-Symbol Interference στην OFDM πρακτικά παύει να υπάρχει. Ένας πομπός OFDM που λειτουργεί μέσω της χρήσης της Inverse Fast Fourier Transform (IFFT) με εισαγωγή του Cyclic Prefix ή μέσω του Zero Padded (ZP), δύναται να χρησιμοποιήσει στο δέκτη σε κάθε subcarrier μετά τον FFT έναν one-tap equalizer, μετατρέποντας την (κυκλική) συνέλιξη του πεδίου του χρόνου σε πολλαπλασιασμό στο πεδίο της συχνότητας.

Το zero-padding συνίσταται ουσιαστικά στην προσθήκη μηδενικών στο τέλος ενός σήματος. Όταν υπολογίζουμε το DFT αυτής της ακολουθίας zero-padded, παίρνουμε μια πυκνότερη αναπαράσταση συχνότητας. Αυτό δεν εισάγει καμία νέα πληροφορία συχνότητας, αλλά παρέχει μια πιο λεπτομερή προβολή ή μια λεπτότερη ανάλυση του ίδιου φασματικού περιεχομένου.

Παρακάτω παρουσιάζονται 2 γραφικές παραστάσεις που επιδεικνύουν την έννοια του zero padding στο πλαίσιο του Discrete Fourier Transform (DFT).



Εικόνα 2-13: Σύγκριση αποτελέσματος για Zero-Padded DFT

Στο παράδειγμα αυτό, με τον βασικό DFT 32-σημείων βλέπουμε μόνο το σήμα στα subcarriers ενδιαφέροντος, ενώ με zero padding γίνεται υπερδειγματοληψία στη συχνότητα με αποτέλεσμα να μπορούμε να μελετήσουμε τους πλευρικούς λοβούς των υπο-φορέων.

1. **DFT 32-σημείων $x[n]$** : Αυτός ο γράφος αναπαριστά το DFT ενός 32-σημείου ακολουθίας. Το DFT μεταφράζει μια πεπερασμένη ακολουθία από τον αρχικό της χρόνο ή τον χώρο στον αντίστοιχο χώρο στον τομέα συχνότητας, δείχνοντας πόσο από κάθε συχνότητα παρουσιάζεται στην αρχική ακολουθία.
2. **DFT 64-σημείων ZERO-PADDED** : Σε αυτόν το γράφο, η αρχική ακολουθία 32 σημείων $x[n]$ έχει γίνει zero-padded για να παραχθεί μια ακολουθία 64 σημείων. Το zero-padding, πρακτικά προσθέτει μηδενικά στο τέλος του σήματος. Όταν γίνεται ο υπολογισμός της DFT σε αυτήν την ακολουθία, παρέχεται μια πιο “πυκνή” κατανομή αναπαράστασης συχνοτήτων.

2.2.1 Προκλήσεις, Εφαρμογές & Ζητήματα στην OFDM

2.2.1.1 Εφαρμογές

Εξαιτίας των πλεονεκτημάτων της η OFDM, βρίσκει εφαρμογή πάνω σε πολλά σύγχρονα τηλεπικοινωνιακά μοντέλα σήμερα. Συγκεκριμένα βρίσκει εφαρμογή σε πρωτόκολλα όπως DAB/DVB-T, WLANs, Broadband Radio Access Networks, LTE, NR, High Performance Local Area Network II. Επιπλέον αποτελεί μέρος των προτύπων IEEE802.11 & IEEE802.16 υψηλής μετάδοσης δεδομένων για ασύρματα LANs & MANs.

Η OFDM όπως και κάθε πολύπλοκο σύστημα ψηφιακής μετάδοσης δεδομένων, αντιμετωπίζει κάποια προβλήματα που χρήζουν μελέτης και επίλυσης. Μερικά από αυτά σχετίζονται με το κομμάτι της μετάδοσης δεδομένων, ενώ άλλα με το κομμάτι της ασφάλειας. Παρακάτω προχωράμε σε μια σύντομη αναφορά τους.

2.2.1.2 Ζητήματα Μετάδοσης

Για το κομμάτι της μετάδοσης, πρωτίστως εγείρεται το ζήτημα του υψηλού Peak-to-Average Power Ratio (PAPR).

Ένα από τα σημαντικά προβλήματα με το OFDM είναι το **υψηλό PAPR** των εκπεμπόμενων σημάτων. Αυτό απαιτεί γραμμική ενίσχυση στο σήμα, κάτι που μπορεί να προκαλέσει σε υψηλές τιμές την παραμόρφωση του. Επίσης αυτό μπορεί να αποδειχθεί προβληματικό από άποψη ενέργειας, μιας και οι ενισχυτές λειτουργούν οικονομικότερα όταν βρίσκονται σε κατάσταση πλήρους ή καθόλου ενίσχυσης [10]. Επιπλέον υπάρχει μεγάλο ενεργειακό κόστος στην μετατροπή Αναλογικού προς Ψηφιακού σήματος (και το αντίστροφο), εξαιτίας της πολυπλοκότητας του σε απαιτήσεις δυναμικού εύρους. Ειδικά σε μεγάλα δίκτυα κινητής αυτό μπορεί να σημαίνει μεγάλη κατανάλωση ενέργειας συνολικά.

Σημαντικό θέμα είναι και τα ζητήματα συγχρονισμού στην OFDM. Μιας και αυτή απαιτεί συνεχή συγχρονισμό ώστε δέκτης και πομπός να μπορούν να επικοινωνούν σωστά λαμβάνοντας όλα τα στοιχεία επικοινωνίας με την ακριβή σειρά. Εάν υπάρχει μια μικρή μετατόπιση, μπορεί να οδηγήσει σε παρεμβολή μεταξύ συμβόλων. Η Ολίσθηση Συχνότητας - **Carrier Frequency Offset (CFO)** μπορεί να προκαλέσει μικρές αναντιστοιχίες στη συχνότητα μεταξύ του πομπού και του δέκτη μπορεί να προκαλέσουν παρεμβολές μεταξύ των φορέων, υποβαθμίζοντας την απόδοση του συστήματος. Ενώ υπάρχει και **ευαισθησία στη μετατόπιση Doppler**, εφόσον η OFDM διαιρεί το φάσμα σε πολλά στενά υποκανάλια, είναι πιο ευαίσθητο στις αλλαγές συχνότητας λόγω του φαινομένου Doppler, ειδικά σε σενάρια υψηλής κινητικότητας.

Επιπρόσθετα ο θόρυβος φάσης μπορεί να προκαλέσει ένα κοινό σφάλμα φάσης και παρεμβολές μεταξύ των φορέων.

Τέλος, είναι η μειωμένη φασματική αποδοτικότητα που προκαλεί η μετάδοση δεδομένων εξαιτίας του πλεονασμού του Guard Interval & Cyclic Prefix. Για να μετριάσει την παρεμβολή πολλαπλών διαδρομών, η OFDM χρησιμοποιεί Guard Interval (CP ή ZP), το οποίο μπορεί να φτάσει έως και 25% των συνολικών μεταδιδόμενων δεδομένων.

2.2.1.3 Ζητήματα Ασφάλειας

Όσον αφορά το κρίσιμο κομμάτι της ασφάλειας στην OFDM, υπάρχει μια πληθώρα ζητημάτων που πρέπει να αναφερθούν και κατόπιν να γίνει μια ανάλυση επίλυσής τους τόσο υπό τη σκεπή της παρούσας διπλωματικής εργασίας όσο και σε μελλοντικές.

Κύριο ζήτημα στην ασφάλεια, αποτελούν οι υποκλοπές. Όπως και κάθε τηλεπικοινωνιακό σύστημα, έτσι και στην OFDM, ένα υποκλοπέας μπορεί να λάβει τα εκπεμπόμενα σήματα, να τα αποδιαμορφώσει και να τα αποκωδικοποιήσει ώστε να μάθει το περιεχόμενο της επικοινωνίας.

Σημαντικό θέμα ασφάλειας αποτελούν επίσης οι Παρεμβολές/Jamming. Αν και η OFDM αποτελεί ένα τηλεπικοινωνιακό σχήμα που έχει ανοχές σε στενού εύρους (narrowband) jamming, εντούτοις κάτι τέτοιο δεν ισχύει αν υπάρχει παρεμβολή από κάποιον broadband jammer, αν αυτός εκπέμπει σε όλο το εύρος συχνοτήτων της εκπεμπόμενης OFDM.

Επιπλέον τόσο το γνωστό “Spoofing” όσο και οι επιθέσεις επανάληψης (Replay Attacks) αποτελούν απειλές για τα σύγχρονα OFDM [7]. Αυτό μπορεί εν τέλει να οδηγήσει σε Άρνηση Υπηρεσίας (Denial of Service (DoS)) στο σύστημα, όπως μπορεί να συμβεί και στη περίπτωση που πολλοί “επιτιθέμενοι”, προσπαθούν να ρίξουν με μεγάλο όγκο κίνησης/traffic στο δίκτυο επικοινωνίας.

Τα παραπάνω αποτελούν σημαντικές προκλήσεις ασφαλείας και με την εισαγωγή της OFDM σε massive MIMO συστήματα, επιτακτική είναι η εύρεση λύσεων και αντιμέτρων. Πρωτίστως το κομμάτι της ασφάλειας δηλαδή της διασφάλισης της αξιοπιστίας, της ακεραιότητας και της μυστικότητας της επικοινωνίας είναι το κύριο ζητούμενο. Αυτά μπορούν να επιτευχθούν με διάφορους τρόπους.

Μέθοδοι κρυπτογράφησης και αυθεντικοποίησης μπορούν να ενσωματωθούν στη επικοινωνία μέσω OFDM για να εξασφαλιστεί η μυστικότητα, η αυθεντικότητα και η ακεραιότητα των μηνυμάτων. Ενώ μέθοδοι όπως η διαμόρφωση δέσμης/beamforming και η αναπήδηση συχνοτήτων/frequency hopping μπορούν να εξασφαλίσουν την ακεραιότητα έναντι παρεμβολών.

Ωστόσο, αυτό μπορεί να ενέχει κάποιο σημαντικό κόστος, τόσο από άποψη χρηματική όσο και από άποψη ενεργειακή και υπολογιστική (ειδικά στα συστήματα κρυπτασφάλειας). Σε αυτό το σημείο λοιπόν, γίνεται η εισαγωγή του Physical Layer Security που καλείται να δώσει μια προσιτή λύση στο κομμάτι της ασφάλειας επικοινωνίας σε ασύρματα δίκτυα και όχι μόνο.

2.3 Ασφάλεια στο Φυσικό Επίπεδο/Physical Layer Security

2.3.1 Γενικά

Η ασφάλεια φυσικού επιπέδου/ Physical Security (PHY-SEC), αναφέρεται στα μέτρα ασφαλείας που εφαρμόζονται στο φυσικό επίπεδο ενός συστήματος επικοινωνίας. Το φυσικό επίπεδο είναι το χαμηλότερο επίπεδο του μοντέλου OSI (Open Systems Interconnection) και είναι υπεύθυνο για τη μετάδοση bits σε ένα φυσικό μέσο, όπως ένα ενσύρματο ή ασύρματο κανάλι.

Τα μέτρα ασφαλείας του φυσικού επιπέδου έχουν σχεδιαστεί για να προστατεύουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων που μεταδίδονται μέσω ενός συστήματος επικοινωνίας, αποτρέποντας μη εξουσιοδοτημένη πρόσβαση ή παρεμβολή στο φυσικό κανάλι. Αυτά τα μέτρα μπορεί να περιλαμβάνουν τεχνικές όπως η αναπήδηση συχνότητας, το φάσμα διασποράς και η διαμόρφωση δέσμης, καθώς και μέτρα φυσικής ασφάλειας, όπως ασφαλή καλώδια και περιβλήματα.

Η ασφάλεια του φυσικού επιπέδου είναι μια σημαντική πτυχή της ασφάλειας της επικοινωνίας, καθώς βοηθά να διασφαλιστεί ότι τα δεδομένα προστατεύονται από φυσικές απειλές, όπως υποκλοπές ή παρεμβολές. Συχνά χρησιμοποιείται σε συνδυασμό με μέτρα ασφαλείας υψηλότερου επιπέδου, όπως η κρυπτογράφηση, για την παροχή μιας ολοκληρωμένης λύσης ασφαλείας για συστήματα επικοινωνίας.

Η ασφάλεια του φυσικού επιπέδου στοχεύει στην προστασία του φυσικού επιπέδου ενός συστήματος επικοινωνίας από διάφορους τύπους επιθέσεων και τρωτών σημείων που θα

μπορούσαν να θέσουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα του συστήματος.

Υπάρχουν διάφορες τεχνικές που μπορούν να χρησιμοποιηθούν για την επίτευξη ασφάλειας φυσικού επιπέδου, μερικές εκ των οποίων παρατίθενται αναλυτικά παρακάτω.

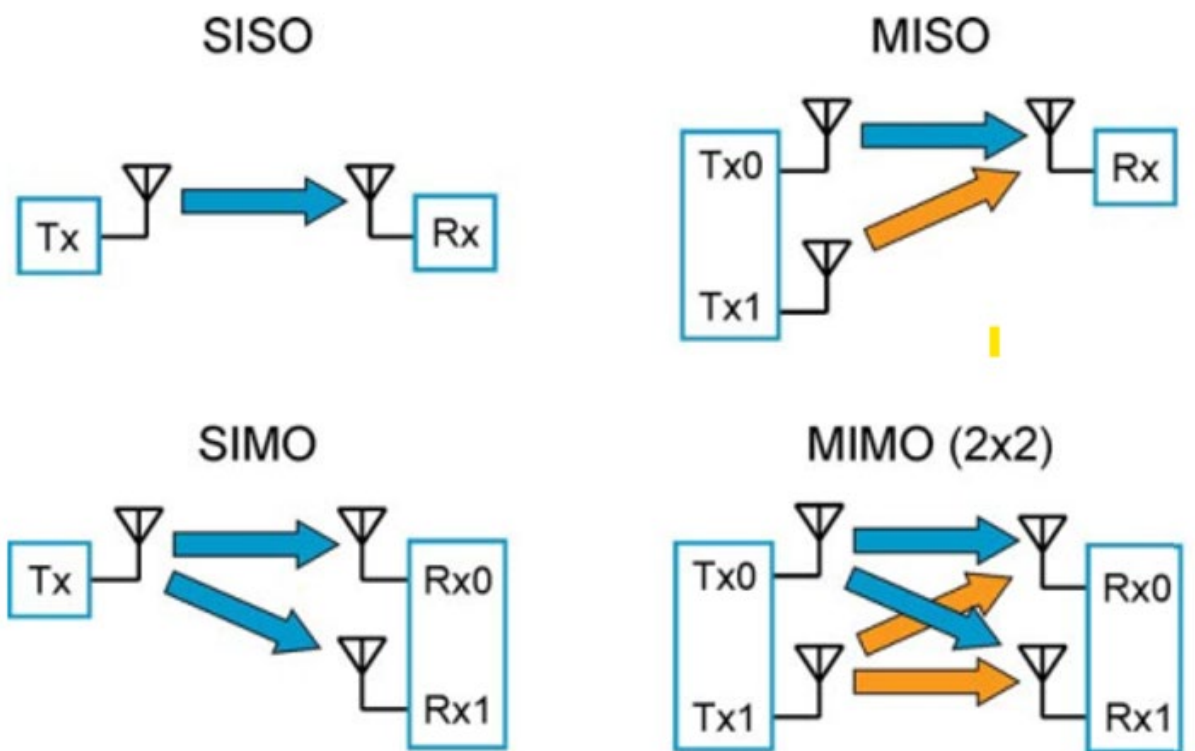
2.3.2 Τεχνικές Ασφάλειας στο Φυσικό

2.3.2.1 Beamforming

Beamforming είναι μια τεχνική που χρησιμοποιείται σε συστήματα ασύρματων επικοινωνιών για να κατευθύνει τη μετάδοση ή τη λήψη ενός σήματος προς μια συγκεκριμένη κατεύθυνση ή ένα σύνολο κατευθύνσεων. Αυτό μπορεί να γίνει ρυθμίζοντας τη φάση ή/και το πλάτος του σήματος σε κάθε στοιχείο κεραίας στη συστοιχία, το οποίο δημιουργεί μια «δέσμη» ενέργειας σήματος που κατευθύνεται προς την επιθυμητή κατεύθυνση. Η διαμόρφωση δέσμης μπορεί να χρησιμοποιηθεί για τη βελτίωση του λόγου σήματος προς θόρυβο (SNR) ή/και την αύξηση της εμβέλειας του συστήματος επικοινωνίας. Απαιτεί κατ' ελάχιστο πολλές κεραίες στον πομπό.

Η τεχνική του **Beamforming** σχετίζεται άμεσα με το τηλεπικοινωνιακό σύστημα που χρησιμοποιείται, ιδιαίτερα με τα MISO και MIMO. Με την τεχνική Beamforming, το σήμα στοχεύεται προς μία συγκεκριμένη κατεύθυνση με την χρήση πολλαπλών κεραιών. Αυτό ενισχύει το σήμα προς τον συγκεκριμένο δέκτη και μειώνει τις παρεμβολές. Επομένως, η χρήση πολλαπλών κεραιών σε συνδυασμό με το Beamforming μπορεί να βελτιώσει σημαντικά την απόδοση του δικτύου και την ποιότητα του σήματος.

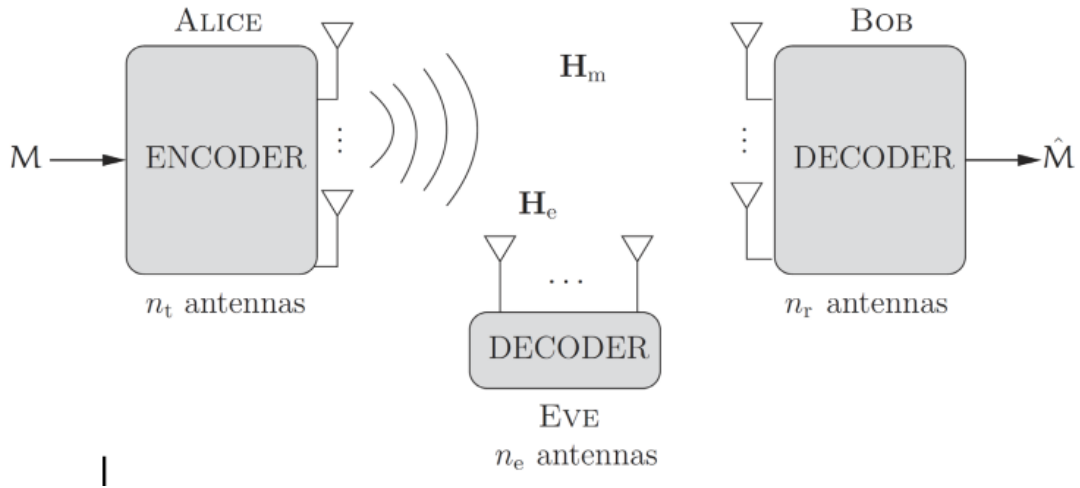
Μερικά από τα συστήματα που χρησιμοποιείται το beamforming είναι το **MIMO (Multiple Input Multiple Output)** όπου έχουμε πολλαπλές κεραίες τόσο στον πομπό όσο και στον δέκτη και η **MISO (Multiple Input Single Output)** με πολλαπλές κεραίες στον πομπό αλλά μόνο μία στον δέκτη.



Εικόνα 2-14: SISO, SIMO, MIMO, MISO

Επιπλέον υπάρχουν τα **SISO (Single Input Single Output)**, με μια κεραία στον πομπό και μία στον δέκτη και τέλος τα **SIMO (Single Input Multiple Output)**, με μια κεραία στον πομπό αλλά πολλαπλές στον δέκτη, που όμως δεν θα μας απασχολήσουν στα πλαίσια του beamforming [2].

Στα συστήματα πολλαπλής εισόδου και πολλαπλής εξόδου (MIMO), τα οποία χρησιμοποιούν έναν πληθυσμό από M πομπούς και N δέκτες, η δημιουργία δέσμης είναι μια τεχνική για να ενισχύσει το σήμα σε συγκεκριμένες κατευθύνσεις. Αυτό επιτυγχάνεται ρυθμίζοντας τη φάση και το πλάτος του σήματος σε κάθε κεραία με τρόπο που να βελτιστοποιεί το λόγο σήμα προς θόρυβο (SNR) στον δέκτη.



Εικόνα 2-15: Σύστημα πομπού-δέκτη και υποκλοπέα

Στο παραπάνω διάγραμμα περιγράφεται ένα μοντέλο επικοινωνίας με επίκεντρο την ασφάλεια. Η **Alice** (πομπός) θέλει να στείλει ένα μήνυμα (M) στον **Bob** (δέκτη) μέσω των n_t κεραιών που διαθέτει. Έπειτα γίνεται η κωδικοποίηση του μηνύματος και ακολουθεί η ασύρματη μετάδοσή του μέσω **MIMO** (Multiple Input Multiple Output) τεχνικές. Ο **Bob** λαμβάνει το σήμα και προσπαθεί να το αποκωδικοποιήσει. Στο μεταξύ, η **Eve** (υποκλοπέας) προσπαθεί να υποκλέψει την επικοινωνία του Bob και της Alice, διαθέτοντας n_e κεραίες. Ο στόχος είναι να εξασφαλιστεί ότι η **Eve** δεν μπορεί να αποκτήσει πληροφορίες για το μήνυμα M παρά την παρέμβασή της.

Το H_m αποτελεί έναν πίνακα ο οποίος αντιπροσωπεύει το κανάλι επικοινωνίας μεταξύ Bob και Alice, που έχει υποστεί αλλαγές εξαιτίας απωλειών και διαλείψεων κατά τη μετάδοση του στον χώρο.

Αντίστοιχα και για τον πίνακα H_e , που αποτελεί το κανάλι μεταξύ Eve και Alice.

Σκοπός της σχεδίασης του παραπάνω τηλεπικοινωνιακού μοντέλου είναι, μέσω της διαμόρφωσης δέσμης/beamforming να επιτευχθεί μυστικότητα καναλιού.

Για να γίνει αυτό θα πρέπει πρωτίστως να υπολογιστεί ο ρυθμός μετάδοσης πληροφορίας R_m , χωρίς λάθη (σε όρους Θεωρίας Πληροφορίας), του Bob και της Alice [12].

$$R_m = \log \left| I_2 + \frac{1}{\sigma_n^2} H_m K_X H_m^H \right|$$

Το σ αποτελεί τη διασπορά του θορύβου του Bob, το H_m^H δηλώνει τον αναστροφосуζηγή του H_m .

Για λόγους κατανόησης παρακάτω παρατίθεται, μαζί με μια σύντομη εξήγηση για τα σήματα στο μοντέλο Eavesdrop [11].

Το σήμα στο μέρος της Alice (θεωρώντας MISO με δυο κεραίες στον πομπό) είναι y :

$$y = [h_1 \quad h_2] \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + n$$

$$y = h_1 x_1 + h_2 x_2 + n$$

$$y = h_1 a_1 s + h_2 a_2 s + n$$

Με a_1 και a_2 , τα βάρη των αντίστοιχων καναλιών στον beamformer, s το σήμα πληροφορίας και h_1 και h_2 , οι μιγαδικοί συντελεστές του καναλιού.

Εφόσον λοιπόν ισχύει:

$$a_1 = \frac{h_1^*}{|h_1|}$$

$$a_2 = \frac{h_2^*}{|h_2|}$$

Τότε για το σήμα της Alice έχουμε:

$$y = \frac{h_1 h_1^* s}{|h_1|} + \frac{h_2 h_2^* s}{|h_2|} + n.$$

Το σήμα, εν τέλει που λαμβάνει ο Bob είναι:

$$y = (|h_1| + |h_2|)s + n.$$

Το οποίο αποδεικνύεται ότι προσφέρει το μέγιστο SNR συνολικά για πεπερασμένη ισχύ εκπομπής (Maximal Ratio Transmission - MRT). Η διαμόρφωση δέσμης συμβάλλει κυρίως στην ασφάλεια από χωρική άποψη:

- Χωρική Εστίαση/Spatial Focus: Το Beamforming συγκεντρώνει το μεταδιδόμενο σήμα σε μια στενή δέσμη που στοχεύει στον επιθυμητό δέκτη. Αυτή η χωρική εστίαση καθιστά δύσκολο για τους κρυφακούς να υποκλέψουν το σήμα, εκτός εάν είναι τοποθετημένοι ακριβώς εντός της διαδρομής της δέσμης.
- Χωρικός Διαχωρισμός/Spatial Separation: Εστιάζοντας στον επιθυμητό δέκτη και απορρίπτοντας σήματα από άλλες κατευθύνσεις, η διαμόρφωση δέσμης ενισχύει τον χωρικό διαχωρισμό. Αυτό σημαίνει ότι ακόμα κι αν οι υποκλοπείς βρίσκονται κοντά, λαμβάνουν ένα πολύ πιο αδύναμο σήμα, καθιστώντας πιο

δύσκολο για αυτούς να αποκωδικοποιήσουν ή να παρεμποδίσουν την επικοινωνία. Μάλιστα με κατάλληλη κωδικοποίηση αυτό καθίσταται αδύνατο.

- Μετριασμός Παρεμβολών/Interference Mitigation: Το beamforming μπορεί επίσης να βοηθήσει στον μετριασμό των παρεμβολών, συμπεριλαμβανομένων των προσπαθειών σκόπιμης εμπλοκής (jamming), συγκεντρώνοντας την ισχύ του σήματος όπου χρειάζεται και ελαχιστοποιώντας τις παρεμβολές από άλλες κατευθύνσεις.

Στα προηγούμενα, παρουσιάστηκε το MRT για MISO κανάλια. Γενικεύοντας σε MIMO, πρακτικά το Beamforming λειτουργεί ως εξής:

Για τη βελτιστοποίηση της δημιουργίας δέσμης, μπορεί να χρησιμοποιηθεί ο αλγόριθμος της αποσύνθεσης ιδιοζουσών τιμών (Singular Value Decomposition - SVD). Αν ο πίνακας του καναλιού είναι ο A , τότε μπορεί να αναπαρασταθεί ως:

$$A=U \Sigma V^H$$

με το U να είναι ο πίνακας των ιδιοδιανυσμάτων του AA^H , το Σ να είναι ένας διαγώνιος πίνακας που περιέχει τις ιδιάζουσες τιμές του A και το V^H να είναι ο συζυγής ανάστροφος του πίνακα των ιδιοδιανυσμάτων του $A^H A$ [11].

Στη δημιουργία δέσμης, το διάνυσμα που μεταδίδεται x προκωδικοποιείται χρησιμοποιώντας τον πίνακα V . Το προκωδικοποιημένο σήμα s είναι:

$$s = V x$$

Για φυσική ασφάλεια, επιλέγονται οι στήλες του V που αντιστοιχούν στις μεγαλύτερες ιδιοτιμές, επικεντρώνοντας την ενέργεια στα ισχυρότερα χωρικά κανάλια. Η ασφάλεια στο φυσικό επίπεδο εκμεταλλεύεται την εγγενή τυχαιότητα των ασύρματων καναλιών, βελτιστοποιώντας τον λόγο σήματος προς θόρυβο (SNR) για τον νόμιμο δέκτη ενώ ελαχιστοποιείται για τυχόν υποκλοπείς.

Η χρήση του SVD για δημιουργία δέσμης εξασφαλίζει ότι το ενισχυμένο σήμα είναι προσανατολισμένο προς την κατεύθυνση του νόμιμου δέκτη. Το SVD προσφέρει μια βάση για τον προσδιορισμό των κύριων κατευθύνσεων του ασύρματου καναλιού. Κατά την εκπομπή, ο πομπός μπορεί να επικεντρωθεί στις κατευθύνσεις αυτές για να βελτιστοποιήσει τον λόγο σήματος προς θόρυβο (SNR) στον δέκτη.

Σε ένα σενάριο φυσικής ασφάλειας, ο πομπός ενδέχεται να επικεντρώσει την ενέργεια σε αυτές τις κύριες κατευθύνσεις, εξασφαλίζοντας ότι μόνο ο νόμιμος δέκτης (με τη σωστή γνώση του καναλιού) μπορεί να αποκτήσει πρόσβαση στο σήμα. Ταυτόχρονα, ένας υποκλοπέας θα αντιμετωπίζει ένα αδύναμο ή ακατανόητο σήμα λόγω της εστιασμένης δημιουργίας δέσμης.

Επομένως, η χρήση του SVD στη δημιουργία δέσμης προσφέρει μια δυναμική τεχνική για τη βελτιστοποίηση της απόδοσης των συστημάτων MIMO. Σε συνδυασμό με τεχνικές φυσικού επιπέδου ασφάλειας, η δημιουργία δέσμης βοηθά στην παροχή ασφαλούς και αποτελεσματικής επικοινωνίας σε ασύρματα δίκτυα.

2.3.2.2 *Artificial Noise*

Το μοντέλο τεχνητού θορύβου (AN) είναι ένα μαθηματικό μοντέλο που χρησιμοποιείται για να περιγράψει τη διαδικασία προσθήκης θορύβου (επίσης γνωστή ως "padding") σε ένα μεταδιδόμενο σήμα προκειμένου να βελτιωθεί η ασφάλεια ενός συστήματος επικοινωνίας. Το μοντέλο AN βασίζεται στην υπόθεση ότι ο αποστολέας και ο παραλήπτης έχουν πρόσβαση σε ένα κοινό μυστικό κλειδί, το οποίο χρησιμοποιείται για τη δημιουργία του σήματος θορύβου και την αφαίρεση του από το λαμβανόμενο σήμα [11].

Το μοντέλο AN τυπικά θεωρεί ότι η Alice εκπέμπει το εξής σήμα:

$$\mathbf{x}_k = \mathbf{a}_k \mathbf{s}_k + \mathbf{w}_k$$

Δοθέντος ότι το x_k αντιπροσωπεύει το μιγαδικό Γκαουσιανό διάνυσμα συμβόλων, a_k είναι το βάρος του καναλιού για το beamforming, το s_k είναι το σήμα πληροφορίας και τέλος το w_k είναι το μιγαδικό Γκαουσιανό διάνυσμα δειγμάτων για το AN, το οποίο παράγει η Alice για δεδομένο πίνακα καναλιού H_k με βάση την σχέση:

$$\mathbf{H}_k^H \mathbf{w}_k = 0$$

Αυτό συμβαίνει ώστε η Alice, επιλέγει το w_k , ώστε αυτό να είναι μέρους του μηδενικού υποχρου (null-space) H_k^H , το οποίο είναι ο αναστροφosuζυγής πίνακα του καναλιού H_k του Alice-Bob .

$$\mathbf{y}_k = \mathbf{H}_k^H \mathbf{x}_k + \mathbf{n}_k$$

$$\mathbf{y}_k = \mathbf{H}_k^H (\mathbf{a}_k \mathbf{s}_k + \mathbf{w}_k) + \mathbf{n}_k$$

$$\mathbf{y}_k = \mathbf{H}_k^H \mathbf{a}_k \mathbf{s}_k + \mathbf{n}_k.$$

$$\mathbf{z}_k = \mathbf{G}_k^H \mathbf{a}_k \mathbf{s}_k + \mathbf{G}_k^H \mathbf{w}_k + \mathbf{e}_k$$

Αντίστοιχα, το σήμα της Eve θα είναι το z_k :

Όπου το AN παρουσιάζεται ως $G_k^H w_k$, το οποίο αποτελεί το σήμα που λαμβάνει η Eve, με κανάλι G_k . Το δεύτερο σκέλος της εξίσωσης, δηλαδή το κομμάτι του AN, δεν επηρεάζει τον Bob γιατί το w_k , βρίσκεται στο null-space του και επηρεάζει πρακτικά όλους τους υπόλοιπους δέκτες του σήματος, πλην του Bob. Συνεπώς οι υποκλοπείς αποτυγχάνουν να αποκωδικοποιήσουν σωστά το σήμα της Alice.

Η ισχύς μετάδοσης του σήματος είναι συγκεντρωμένη στη δημιουργία μετάδοσης του AN έναντι του σήματος πληροφορίας, με το τελικό μεταδιδόμενο σήμα να είναι

$$\mathbf{x}_k = \sqrt{(1 - r)}\mathbf{s}_k + \sqrt{r}\mathbf{w}_k$$

Με το r , να αποτελεί το λόγο ισχύος του AN προς την ισχύ από το μεταδιδόμενο σήμα. Επιστρέφοντας στην ανάλυση του SVD για το beamforming, η ανώτερη ανάλυση ισοδυναμεί με εκτίμηση των ασθενέστερων ιδιζουσών τιμών, που δεν επηρεάζουν το σήμα στον Bob σημαντικά και αποστολή προς αυτές τις κατευθύνσεις του AN.

Το μοντέλο AN είναι μια απλή και αποτελεσματική τεχνική για τη βελτίωση της ασφάλειας ενός συστήματος επικοινωνίας, καθώς απαιτεί μόνο παραγωγή θορύβου ώστε να προστεθεί στο σήμα. Ωστόσο, είναι επίσης μια σχετικά αδύναμη μορφή ασφάλειας, καθώς το padding είναι εύκολο να αφαιρεθεί από έναν εισβολέα εάν είναι σε θέση να υποκλέψει το σήμα και να αποκτήσει το κοινό μυστικό κλειδί. Ως αποτέλεσμα, το μοντέλο AN χρησιμοποιείται συχνά σε συνδυασμό με άλλα μέτρα ασφαλείας (όπως κρυπτογράφηση ή φάσμα εξάπλωσης) για να παρέχει ένα πιο ισχυρό επίπεδο ασφάλειας. Έχει όμως και ένα σημαντικό πλεονέκτημα. Δεν απαιτεί γνώση της θέσης ή του καναλιού του υποκλοπέα.

2.3.2.3 Alamouti Coding

Η κωδικοποίηση Alamouti είναι μια τεχνική χωροχρονικής κωδικοποίησης που μπορεί να χρησιμοποιηθεί για τη βελτίωση της απόδοσης ενός συστήματος ασύρματης επικοινωνίας αξιοποιώντας την ποικιλομορφία του καναλιού. Η χωροχρονική κωδικοποίηση περιλαμβάνει τη μετάδοση πολλαπλών αντιγράφων του ίδιου μηνύματος σε διαφορετικές χρονοθυρίδες ή διαφορετικές κεραίες, προκειμένου να βελτιωθεί η αξιοπιστία και η αποτελεσματικότητα του συστήματος.

Η κωδικοποίηση Alamouti είναι ένας συγκεκριμένος τύπος χωροχρονικής κωδικοποίησης που αναπτύχθηκε από τον S. M. Alamouti το 1998. Έχει σχεδιαστεί για χρήση σε ένα ασύρματο σύστημα επικοινωνίας με δύο κεραίες εκπομπής και μία κεραία λήψης. Σε αυτό το σύστημα,

ο πομπός στέλνει δύο αντίγραφα του ίδιου μηνύματος, το καθένα κωδικοποιημένο με διαφορετικό σύμβολο μιγαδικής τιμής. Ο δέκτης είναι στη συνέχεια σε θέση να ανακτήσει το αρχικό μήνυμα χρησιμοποιώντας την διαφορισιμότητα του καναλιού για να ακυρώσει τα αποτελέσματα της εξασθένησης και των παρεμβολών.

Ασφαλείς επικοινωνίες με Alamouti Coding (Secure Communications with Alamouti Coding):

Η κωδικοποίηση Alamouti συμβάλλει στην ασφάλεια από την άποψη κωδικοποίησης και ανίχνευσης σφαλμάτων:

- Coding Redundancy: Η κωδικοποίηση Alamouti στέλνει δύο εκδόσεις των ίδιων δεδομένων με γνωστή μαθηματική σχέση μεταξύ τους. Αυτός ο πλεονασμός βοηθά τον νόμιμο δέκτη να εντοπίσει τυχόν αποκλίσεις μεταξύ των λαμβανόμενων σημάτων. Οποιοσδήποτε μη εξουσιοδοτημένος υποκλοπέας που προσπαθούσε να υποκλέψει την επικοινωνία θα λάμβανε αυτά τα δύο σήματα, αλλά δεν θα γνώριζε τη σχέση, καθιστώντας σχεδόν αδύνατο για αυτούς να αποκωδικοποιήσουν το αρχικό μήνυμα.
- Error Detection and Correction: Εάν ένας υποκλοπέας επιχειρήσει να παραβιάσει ένα από τα σήματα, ο νόμιμος δέκτης μπορεί να εντοπίσει την ασυνέπεια και να ζητήσει αναμετάδοση ή να εφαρμόσει τεχνικές διόρθωσης σφαλμάτων για να ανακτήσει τα σωστά δεδομένα.
- Secrecy through Mathematical Complexity: Η μαθηματική πολυπλοκότητα που εισάγεται από την κωδικοποίηση Alamouti προσθέτει ένα επιπλέον επίπεδο ασφάλειας. Η αποκρυπτογράφηση των πληροφοριών χωρίς να είναι γνωστό το σχήμα κωδικοποίησης είναι μια πολύ απαιτητική δουλειά.

3

Software Defined Radio

3.1 Γενικά

Το Software Defined Radio (SDR) αποτελεί ένα τηλεπικοινωνιακό σύστημα που αποδίδει τις λειτουργίες των αναλογικών hardware συστημάτων επεξεργασίας σήματος σε ψηφιακούς επεξεργαστές και FPGA κάτι που επιτρέπει μεγαλύτερη ευελιξία στην πραγματοποίηση δοκιμών ασυρμάτων δικτύων και στη χρήση/παραμετροποίηση των περιφερειακών του Front-end RF κομματιού.

Ένα ιδανικό Software Radio (SR) μπορεί να θεωρηθεί ένα σύστημα επικοινωνίας που υλοποιεί όλες τις λειτουργίες επικοινωνίας πέραν του Front-end RF κομματιού με λογισμικό σε μονάδες Ψηφιακής Επεξεργασίας Σήματος (DSP). Σε αυτό το ιδανικό σύστημα, παράμετροι όπως το εύρος ζώνης, η διαμόρφωση και η συχνότητα μπορούν να αναπροσδιοριστούν απλά με μια αλλαγή ή ένα διαφορετικό λογισμικό.

Ωστόσο ορισμένες λειτουργίες του πομποδέκτη δεν μπορούν να εφαρμοστούν πρακτικά άμεσα σε λογισμικό όπως αναλογικά φίλτρα, ενισχυτές ισχύος, μετατροπείς αναλογικού σε ψηφιακό και μετατροπείς ψηφιακού σε αναλογικό. Αυτά τα στοιχεία υλικού επιβάλλουν περιορισμούς στο εύρος ζώνης και στο εύρος συχνοτήτων που επιτυγχάνεται από το σύστημα. Ένα σύστημα

που χρησιμοποιεί λογισμικό για να καθορίσει ένα μεγάλο (κυρίαρχο) κομμάτι της κυματομορφής του σήματος ορίζεται ως SDR.

Τα SDR διαθέτουν πολύ μεγαλύτερη ευελιξία από τα παραδοσιακά ραδιοσυστήματα και μπορούν να χρησιμοποιηθούν για μια ποικιλία εφαρμογών.

Το Universal Software Radio Peripheral (USRP) είναι μια οικογένεια SDR που κατασκευάζεται από Ettus Research. Τα βασικά χαρακτηριστικά του USRP σε σύγκριση με άλλα εμπορικά SDRs είναι ότι οι συσκευές είναι σχετικά φθηνές και αποτελούν Υλικό Ανοικτού Κώδικα. Τα USRP έχουν υιοθετηθεί σε μεγάλο βαθμό από το open-source radio όπως το GNU Radio που το καθιστά χρήσιμο εργαλείο για την δοκιμή και κοινοποίηση διάφορων πειραματικών αποτελεσμάτων.

Σε ένα σύστημα SDR, το front-end RF (ραδιοσυχνότητας) και η επεξεργασία της ζώνης βάσης συνήθως υλοποιούνται χρησιμοποιώντας λογισμικό που εκτελείται σε επεξεργαστή γενικής χρήσης, αντί να χρησιμοποιεί ειδικά εξαρτήματα υλικού. Αυτό επιτρέπει στα συστήματα SDR να αναδιαρθρωθούν ώστε να υποστηρίζουν διαφορετικά πρότυπα επικοινωνίας, συχνότητες και σχήματα διαμόρφωσης χωρίς την ανάγκη αλλαγής υλικού.

Το USRP (Universal Software Radio Peripheral) είναι μια πλατφόρμα υλικού που χρησιμοποιείται για εφαρμογές ραδιοσυστημάτων με τις κυματομορφές να καθορίζονται πλήρως από λογισμικό (SDR). Παράγεται πλέον από την National Instruments (που εξαγόρασε την Ettus) και αποτελείται από μια σειρά συσκευών που υποστηρίζεται πλέον εξολοκλήρου από το λογισμικό LabVIEW της εταιρείας.

Μια συσκευή USRP αποτελείται συνήθως από μια μητρική πλακέτα με επεξεργαστή γενικής χρήσης και μια θυγατρική πλακέτα που χρησιμοποιείται για διασύνδεση με το μπροστινό μέρος RF (ραδιοσυχνότητα). Η θυγατρική πλακέτα μπορεί εύκολα να αντικατασταθεί για να υποστηρίξει διαφορετικά εύρη συχνοτήτων, εύρη ζώνης και υποδοχές RF.

Για τη χρήση μιας συσκευής USRP, θα χρειαστεί το κατάλληλο λογισμικό και οι αντίστοιχοι drivers. Στη συνέχεια, η συσκευή μπορεί να συνδεθεί στον υπολογιστή μέσω σύνδεσης USB ή Ethernet. Αφού συνδεθεί και διαμορφωθεί η συσκευή, μπορεί να χρησιμοποιηθεί για

μετάδοση ή λήψη ασύρματων σημάτων και εκτέλεση άλλων εργασιών SDR, όπως επεξεργασία και ανάλυση σήματος.

Οι συσκευές USRP χρησιμοποιούνται συνήθως στην έρευνα και ανάπτυξη, καθώς και σε εκπαιδευτικά και εμπορικά περιβάλλοντα, για να καταστεί δυνατή η ανάπτυξη και η δοκιμή συστημάτων SDR.

3.2 Εφαρμογές

Οι συσκευές USRP (Universal Software Radio Peripheral) μπορούν να χρησιμοποιηθούν για ένα ευρύ φάσμα εφαρμογών ραδιοσυστημάτων. Μερικές κοινές λειτουργίες για τις οποίες μπορούν να χρησιμοποιηθούν οι συσκευές USRP περιλαμβάνουν:

Συστήματα ασύρματης επικοινωνίας: Οι συσκευές USRP μπορούν να χρησιμοποιηθούν για τη μετάδοση και λήψη σημάτων χρησιμοποιώντας διάφορα πρότυπα ασύρματης επικοινωνίας, όπως WiFi, Bluetooth και κινητής τηλεφωνίας. Μπορούν επίσης να χρησιμοποιηθούν για την εφαρμογή προσαρμοσμένων συστημάτων ασύρματης επικοινωνίας, όπως δίκτυα πλέγματος ή δίκτυα ad-hoc.

Συστήματα ραντάρ: Οι συσκευές USRP μπορούν να χρησιμοποιηθούν για τη μετάδοση και λήψη σημάτων ραντάρ για εφαρμογές όπως η απεικόνιση, η ανίχνευση και ο εντοπισμός θέσης. Μπορούν να χρησιμοποιηθούν για την υλοποίηση συστημάτων ραντάρ που λειτουργούν σε μια ποικιλία ζωνών συχνοτήτων, συμπεριλαμβανομένων των ζωνών μικροκυμάτων, χιλιοστών κυμάτων και τεραχερτζ (με χρήση κατάλληλων κάτω/άνω μετατροπών συχνότητας).

Αναγνώριση ραδιοσυχνοτήτων (RFID): Οι συσκευές USRP μπορούν να χρησιμοποιηθούν για την εφαρμογή συστημάτων RFID για εφαρμογές όπως η παρακολούθηση περιουσιακών στοιχείων, η διαχείριση της αλυσίδας εφοδιασμού και ο έλεγχος πρόσβασης. Μπορούν να χρησιμοποιηθούν για τη μετάδοση σημάτων RFID και για την ανάγνωση και εγγραφή ετικετών RFID.

Παρακολούθηση και ανάλυση φάσματος: Οι συσκευές USRP μπορούν να χρησιμοποιηθούν για την εκτέλεση ανάλυσης φάσματος και την παρακολούθηση του φάσματος

ραδιοσυχνοτήτων για την ανίχνευση και τον χαρακτηρισμό σημάτων. Μπορούν να χρησιμοποιηθούν για τον προσδιορισμό της χρήσης του φάσματος και των παρεμβολών και για τη μέτρηση της απόδοσης των συστημάτων ασύρματης επικοινωνίας.

Μέτρηση και δοκιμή ραδιοσυχνοτήτων: Οι συσκευές USRP μπορούν να χρησιμοποιηθούν για την εκτέλεση μετρήσεων και δοκιμών ραδιοσυχνοτήτων, όπως βαθμονόμηση ισχύος και συχνότητας, δοκιμή κεραίας και ανάλυση διαμόρφωσης. Μπορούν να χρησιμοποιηθούν για την αξιολόγηση της απόδοσης εξαρτημάτων και συστημάτων RF και για την αντιμετώπιση προβλημάτων.

Τα SDR χρησιμοποιούνται ως τηλεπικοινωνιακός εξοπλισμός σε ποικιλία μη επανδρωμένων εναέριων οχημάτων (UAV) και αεροσκαφών, συμπεριλαμβανομένων στρατιωτικών αεροσκαφών. Τα SDR είναι κατάλληλα για χρήση σε αυτούς τους τύπους εφαρμογών λόγω της ευελιξίας και της προσαρμοστικότητας τους, καθώς μπορούν εύκολα να διαμορφωθούν εκ νέου μέσω ενημερώσεων λογισμικού ή αλλαγών στο λογισμικό.

3.2.1 Ζώνες λειτουργίας

Όπως και οι παλαιότερες αρχιτεκτονικές συστημάτων, έτσι και τα SDR μπορούν και χρησιμοποιούν όλο το εύρος συχνοτήτων που χρησιμοποιούσαν και οι προκάτοχοί τους. Μια ενδεικτική χρήση SDRs ανά μπάντα συχνοτήτων είναι η ακόλουθη:

V/UHF SDR: Πρόκειται για SDR που έχουν σχεδιαστεί για χρήση στις ζώνες πολύ υψηλής συχνότητας (VHF) και εξαιρετικά υψηλής συχνότητας (UHF). Χρησιμοποιείται σε μια ποικιλία στρατιωτικών και αεροδιαστημικών εφαρμογών, συμπεριλαμβανομένων συστημάτων επικοινωνίας, δικτύωσης και αισθητήρων.

SDR ζώνης X: Πρόκειται για SDR που έχει σχεδιαστεί για χρήση στην περιοχή συχνοτήτων της ζώνης X (περίπου 8-12 GHz). Χρησιμοποιείται σε μια ποικιλία στρατιωτικών και αεροδιαστημικών εφαρμογών, συμπεριλαμβανομένων των συστημάτων ραντάρ και επικοινωνιών.

SDR ζώνης Ka: Πρόκειται για ένα SDR που έχει σχεδιαστεί για χρήση στην περιοχή συχνοτήτων Ka-band (περίπου 26,5-40 GHz). Χρησιμοποιείται σε μια ποικιλία στρατιωτικών και αεροδιαστημικών εφαρμογών, συμπεριλαμβανομένων των συστημάτων δορυφορικής επικοινωνίας.

SDR ζώνης L: Αυτό είναι ένα SDR που έχει σχεδιαστεί για χρήση στην περιοχή συχνοτήτων της ζώνης L (περίπου 1-2 GHz). Χρησιμοποιείται σε μια ποικιλία στρατιωτικών και αεροδιαστημικών εφαρμογών, συμπεριλαμβανομένων συστημάτων επικοινωνίας και δικτύωσης, καθώς και τα συστήματα πλοήγησης.

Τα ραδιοσυστήματα που καθορίζονται από λογισμικό είναι ανθεκτικά σε παρεμβολές επειδή μπορούν εύκολα να αναπροσαρμοστούν εκ νέου μέσω ενημερώσεων λογισμικού ή αλλαγών στο λογισμικό. Αυτό τους επιτρέπει να προσαρμοστούν γρήγορα στις μεταβαλλόμενες συνθήκες εμπλοκής και να διατηρήσουν την απόδοσή τους.

Σε περίπτωση επίθεσης παρεμβολής, ένα σύστημα SDR μπορεί να αναδιαμορφωθεί γρήγορα ώστε να χρησιμοποιεί διαφορετική ζώνη συχνοτήτων ή πρωτόκολλο επικοινωνίας ή να εφαρμόζει αντίμετρα όπως η αναπήδηση συχνότητας κάτι το οποίο δυσχαιρένει το έργο για έναν εισβολέα να εμποδίσει αποτελεσματικά το σύστημα επικοινωνίας.

Επιπλέον, τα SDR μπορούν να εξοπλιστούν με προηγμένους αλγόριθμους επεξεργασίας σήματος που έχουν σχεδιαστεί για να μετριάζουν τις επιπτώσεις της εμπλοκής (jamming) και των παρεμβολών. Αυτοί οι αλγόριθμοι μπορούν να χρησιμοποιηθούν για την ανίχνευση και τον χαρακτηρισμό σημάτων εμπλοκής και για την ακύρωση ή την καταστολή των επιπτώσεών τους στο σύστημα επικοινωνίας. Συνολικά, η δυνατότητα γρήγορης και εύκολης επαναδιαμόρφωσης ενός συστήματος SDR ως απόκριση στις μεταβαλλόμενες συνθήκες εμπλοκής το καθιστά μια ισχυρή και ανθεκτική πλατφόρμα επικοινωνίας που είναι εύρωστη σε επιθέσεις παρεμβολής.

Παρακάτω παρατίθενται αναλυτικά τα πλεονεκτήματα και τα μειονεκτήματα των SDR καθώς και αναλυτικά οι εφαρμογές σε πραγματικά συστήματα.

3.2.2 Πλεονεκτήματα

Ευελιξία και προσαρμοστικότητα: Ένα από τα κύρια πλεονεκτήματα των SDR είναι η ευελιξία και η προσαρμοστικότητά τους. Τα SDR μπορούν εύκολα να αναδιαμορφωθούν μέσω ενημερώσεων λογισμικού ή αλλαγών στο λογισμικό, γεγονός που τους επιτρέπει να υποστηρίζουν ένα ευρύ φάσμα προτύπων και πρωτοκόλλων επικοινωνίας. Αυτό τα καθιστά κατάλληλα για χρήση σε στρατιωτικές επικοινωνίες, όπου η ανάγκη υποστήριξης πολλαπλών απαιτήσεων επικοινωνίας είναι κοινή. Για παράδειγμα, ένα σύστημα SDR μπορεί να αναδιαμορφωθεί γρήγορα ώστε να υποστηρίζει ένα νέο πρότυπο επικοινωνίας ή πρωτόκολλο που εισάγεται ή να λειτουργεί σε διαφορετική ζώνη συχνοτήτων.

Αντίσταση στις παρεμβολές: Τα SDR μπορεί να είναι ανθεκτικά σε επιθέσεις παρεμβολής, επειδή μπορούν να διαμορφωθούν γρήγορα σε απόκριση στις συνθήκες εμπλοκής. Για παράδειγμα, ένα σύστημα SDR μπορεί να διαμορφωθεί εκ νέου ώστε να χρησιμοποιεί διαφορετική ζώνη συχνοτήτων ή πρωτόκολλο επικοινωνίας ή να εφαρμόζει αντίμετρα όπως η μετάβαση συχνότητας ή το φάσμα εξάπλωσης, προκειμένου να μετριαστούν οι επιπτώσεις της εμπλοκής. Αυτό μπορεί να κάνει τα SDR μια ισχυρή και ανθεκτική πλατφόρμα επικοινωνίας που είναι ανθεκτική σε επιθέσεις παρεμβολής.

Οικονομία & Απόδοση: Τα SDR μπορεί να είναι πιο οικονομικά από τα παραδοσιακά συστήματα ραδιοσυστημάτων, καθώς δεν απαιτούν την αγορά και αντικατάσταση εξειδικευμένων εξαρτημάτων υλικού. Αυτό μπορεί να είναι ιδιαίτερα σημαντικό σε στρατιωτικά περιβάλλοντα, όπου οι προϋπολογισμοί μπορεί να είναι περιορισμένοι. Τα SDR μπορεί επίσης να είναι πιο οικονομικά στη συντήρηση και επισκευή, καθώς δεν απαιτούν εξειδικευμένα εξαρτήματα υλικού.

Ευκολία συντήρησης: Τα SDR δεν απαιτούν εξειδικευμένα εξαρτήματα υλικού, γεγονός που καθιστά ευκολότερη τη συντήρηση και την επισκευή τους. Αυτό μπορεί να είναι ιδιαίτερα σημαντικό σε περιπτώσεις όπου η διαθεσιμότητα ανταλλακτικών μπορεί να είναι περιορισμένη.

3.2.3 Μειονεκτήματα

Περιορισμένες δυνατότητες υλικού: Ένα μειονέκτημα των SDR είναι ότι συνήθως υλοποιούνται χρησιμοποιώντας επεξεργαστές γενικής χρήσης, οι οποίοι μπορεί να έχουν περιορισμένες δυνατότητες υλικού σε σύγκριση με εξειδικευμένα στοιχεία υλικού. Αυτό μπορεί να επηρεάσει την απόδοση και την ακρίβεια ενός συστήματος SDR, ιδιαίτερα για εφαρμογές που απαιτούν επεξεργασία υψηλής απόδοσης ή υψηλής ακρίβειας. Για παράδειγμα, ένα σύστημα SDR ενδέχεται να μην μπορεί να επεξεργαστεί σήματα τόσο γρήγορα ή με ακρίβεια όσο ένα σύστημα που χρησιμοποιεί εξειδικευμένα στοιχεία υλικού.

Πολυπλοκότητα: Τα SDR μπορεί να είναι πολύπλοκα συστήματα που απαιτούν εξειδικευμένες γνώσεις και δεξιότητες για το σχεδιασμό, την ανάπτυξη και τη συντήρηση. Αυτό μπορεί να καταστήσει πιο δύσκολη την εύρεση και πρόσληψη προσωπικού με την απαραίτητη τεχνογνωσία και μπορεί επίσης να αυξήσει τον χρόνο και το κόστος ανάπτυξης και συντήρησης ενός συστήματος SDR.

Εξάρτηση από λογισμικό: Τα SDR βασίζονται σε λογισμικό για την εκτέλεση των λειτουργιών τους, πράγμα που σημαίνει ότι μπορεί να είναι ευάλωτα σε επιθέσεις ή αποτυχίες που βασίζονται σε λογισμικό. Εάν ένα σύστημα SDR παραβιαστεί ή παρουσιάσει βλάβη λογισμικού, ενδέχεται να μην είναι σε θέση να εκτελέσει τις προβλεπόμενες λειτουργίες του. Αυτό μπορεί να είναι ανησυχητικό σε εφαρμογές, όπου η αξιοπιστία των συστημάτων επικοινωνίας είναι κρίσιμη.

3.3 Παραδείγματα Χρήσης

Η τεχνολογία SDR έχει ένα ευρύ φάσμα εφαρμογών, συμπεριλαμβανομένων των στρατιωτικών επικοινωνιών, δορυφορικών επικοινωνιών, της ασύρματης δικτύωσης και των εμπορικών ασύρματων συστημάτων. Συχνά χρησιμοποιείται σε καταστάσεις όπου είναι απαραίτητο να υποστηριχθούν πολλαπλά πρότυπα επικοινωνίας ή να αναπτυχθούν γρήγορα νέα συστήματα επικοινωνίας. Τα συστήματα SDR χρησιμοποιούνται επίσης στην έρευνα και ανάπτυξη για να καταστεί δυνατή η δοκιμή και η αξιολόγηση νέων τεχνολογιών επικοινωνίας.

Μερικοί παράγοντες που πρέπει να ληφθούν υπόψη κατά την αξιολόγηση των συστημάτων SDR περιλαμβάνουν το εύρος συχνοτήτων και το εύρος ζώνης που μπορεί να υποστηρίξει το σύστημα, τον τύπο των συνδέσεων RF (ραδιοσυχνότητας) που διαθέτει, την απόδοση και την ακρίβεια του συστήματος και την ευκολία χρήσης και την ευελιξία του περιβάλλοντος λογισμικού.

Ορισμένα δημοφιλή συστήματα SDR που είναι διαθέσιμα αυτήν τη στιγμή περιλαμβάνουν την πλατφόρμα USRP (Universal Software Radio Peripheral) που παράγεται από την National Instruments, την πλατφόρμα LimeSDR που παράγεται από την Lime Microsystems και την πλατφόρμα HackRF που παράγεται από την Great Scott Gadgets. Όλα αυτά τα συστήματα προσφέρουν μια σειρά από χαρακτηριστικά και δυνατότητες και είναι κατάλληλα για μια ποικιλία εφαρμογών SDR.

Ορισμένα συστήματα SDR υψηλής τεχνολογίας, όπως αυτά που χρησιμοποιούνται για στρατιωτικές ή εμπορικές εφαρμογές, μπορεί να είναι πιο ακριβά από άλλα λόγω των προηγμένων δυνατοτήτων και επιδόσεων τους. Αυτά τα συστήματα μπορεί να περιλαμβάνουν χαρακτηριστικά όπως δέκτες υψηλής δυναμικής περιοχής, κάλυψη συχνότητας ευρείας ζώνης και προηγμένες δυνατότητες επεξεργασίας σήματος.

Ένα παράδειγμα ενός ραδιοσυστήματος που ορίζεται από λογισμικό (SDR) που χρησιμοποιείται σε απαιτητικές στρατιωτικές εφαρμογές είναι το AN/PRC-117G, το οποίο παράγεται από την Harris Corporation. Το AN/PRC-117G είναι ένα φορητό SDR που έχει σχεδιαστεί για χρήση σε στρατιωτικές επικοινωνίες. Μπορεί να λειτουργήσει σε ένα ευρύ φάσμα συχνοτήτων και μπορεί να υποστηρίξει πολλαπλά πρότυπα επικοινωνίας, συμπεριλαμβανομένων των τακτικών δορυφορικών επικοινωνιών, μικροκυματικές ζεύξεις οπτικής επαφής και των επικοινωνιών πέρα του ορίζοντα.

Άλλα παραδείγματα SDR που χρησιμοποιούνται σε απαιτητικές εφαρμογές ακριβείας περιλαμβάνουν το AN/PRC-155, το οποίο είναι ένα manpack SDR που παράγεται από την Harris Corporation, και το AN/USC-61 (C) Digital Modular Radio (DMR), το οποίο παράγεται από την Rockwell Collins και είναι το πρώτο SDR που χρησιμοποιήθηκε από τον αμερικανικό

στρατό. Αυτά τα συστήματα χρησιμοποιούνται συνήθως για τακτικές επικοινωνίες και μπορούν να υποστηρίξουν μια ποικιλία προτύπων και πρωτοκόλλων επικοινωνίας.

Στις **εμπορικές επικοινωνίες**, τα SDR χρησιμοποιούνται συχνά σε ραδιοσυστήματα σταθερής τοποθεσίας. Αυτοί οι τύποι ραδιοσυστημάτων μπορούν να χρησιμοποιηθούν για ποικίλες εφαρμογές, όπως ασύρματη δικτύωση, ευρυζωνική πρόσβαση και ραδιοφωνική μετάδοση.

Το srsLTE αποτελεί μια πρώτη πλατφόρμα με SDR που θα λειτουργεί πάνω στο LTE (4G) και NR(5G) [14]. Το ίδιο ισχύει και για την ανοιχτή πλατφόρμα Open Air Interface.

Τα SDR χρησιμοποιούνται επίσης σε μια ποικιλία άλλου εξοπλισμού, όπως συστήματα ραντάρ, συστήματα RFID (αναγνώριση ραδιοσυχνοτήτων) και συστήματα παρακολούθησης φάσματος. Χρησιμοποιούνται επίσης στην έρευνα και ανάπτυξη για να καταστεί δυνατή η δοκιμή και αξιολόγηση νέων τεχνολογιών επικοινωνίας.

4

Πείραμα

4.1 Πλατφόρμες και Υλικό που χρησιμοποιήθηκαν

Για την εργασία χρησιμοποιήθηκαν τα παρακάτω κομμάτια υλικού:

1. 1 Laptop Lenovo Ideapad3 (Alice)
2. 1 Laptop Asus ZenBook (Bob & Eve)
3. 1 Ettus X310 (Alice)
4. 1 Ettus B210 (Alice και Bob)
5. 2 Ettus B200mini (Bob & Eve)

Τα τεχνικά χαρακτηριστικά των συσκευών είναι τα παρακάτω:

Laptop Lenovo Ideapad GAMING

- CPU: AMD® Ryzen 7 4800h with radeon graphics × 16
- Memory: 15,0 GiB
- Graphics: AMD® Renoir / AMD® Renoir

- OS Type: 64-bit

Ettus B200mini

- FPGA: Xilinx Spartan-6 XC6SLX75
- Frequency range: 70 MHz – 6 GHz
- Instantaneous bandwidth: 56 MHz

Ettus B210

- FPGA: Spartan 6 XC6SLX150
- Frequency range: 70 MHz – 6 GHz
- Instantaneous bandwidth: 56 MHz
- Full duplex, MIMO (2 Tx & 2 Rx)

Ettus X310

- FPGA: Kintex 7 -410T
- Frequency range: 10 MHz – 6 GHz
- Instantaneous bandwidth: 160 MHz
- Full duplex, MIMO (2 Tx & 2 Rx)

4.2 MATLAB

Το MATLAB (συντομογραφία "Matrix Laboratory") είναι μια γλώσσα προγραμματισμού και ένα περιβάλλον λογισμικού που χρησιμοποιείται συνήθως για επιστημονικούς και μαθηματικούς υπολογισμούς κυρίως σε επιστήμες μηχανικών. Αναπτύχθηκε και συντηρείται

από την MathWorks, μια εταιρεία που ειδικεύεται σε εργαλεία λογισμικού για τεχνικούς υπολογισμούς.

Το MATLAB διαθέτει ένα ευρύ φάσμα εργαλείων και λειτουργιών που μπορούν να χρησιμοποιηθούν για την ανάλυση και την οπτικοποίηση δεδομένων, το σχεδιασμό και τη δοκιμή αλγορίθμων και τη δημιουργία εφαρμογών για διάφορους τομείς, συμπεριλαμβανομένων των συστημάτων επικοινωνίας. Μερικά από τα εργαλεία και τις λειτουργίες που σχετίζονται με την επικοινωνία που είναι διαθέσιμα στο MATLAB περιλαμβάνουν:

Toolbox/Εργαλειοθήκη συστήματος επικοινωνίας: Αυτή η εργαλειοθήκη παρέχει ένα σύνολο λειτουργιών και μπλοκ για το σχεδιασμό, την προσομοίωση και την ανάλυση συστημάτων επικοινωνίας. Περιλαμβάνει υποστήριξη για ένα ευρύ φάσμα τεχνικών ψηφιακής και αναλογικής επικοινωνίας, όπως διαμόρφωση, αποδιαμόρφωση, διόρθωση σφαλμάτων και κωδικοποίηση καναλιών.

Toolbox/Εργαλειοθήκη επεξεργασίας σήματος: Για την επεξεργασία και την ανάλυση σημάτων και εικόνων η Matlab προσφέρει το ξεχωριστό αυτό toolbox. Περιλαμβάνει υποστήριξη για ένα ευρύ φάσμα τεχνικών επεξεργασίας σήματος, όπως φιλτράρισμα, ανάλυση Fourier και φασματική εκτίμηση.

Toolbox/Εργαλειοθήκη WLAN: Η εργαλειοθήκη αυτή διαθέτει στην βιβλιοθήκη της ένα σύνολο λειτουργιών και μπλοκ για το σχεδιασμό και την προσομοίωση ασύρματων τοπικών δικτύων (WLAN) με βάση το πρότυπο IEEE 802.11. Περιλαμβάνει υποστήριξη για ένα ευρύ φάσμα λειτουργιών που αφορούν ειδικά το WLAN, όπως μοντελοποίηση καναλιών, διαμόρφωση και διόρθωση σφαλμάτων.

Toolbox/Εργαλειοθήκη LTE και 5G Toolbox: Τέλος, μέσω αυτών των εργαλειοθηκών παρέχονται στο χρήστη λειτουργίες και μπλοκ για το σχεδιασμό και την προσομοίωση δικτύων κινητής τηλεφωνίας 4G Long-Term Evolution (LTE) και 5G New Radio (NR). Περιλαμβάνει δε, υποστήριξη για ένα ευρύ φάσμα χαρακτηριστικών που αφορούν ειδικά το LTE και το NR,

όπως διαμόρφωση, κωδικοποίηση καναλιών και επικοινωνία πολλαπλών εισόδων πολλαπλών εξόδων (MIMO).

Αυτά είναι μερικά μόνο παραδείγματα των εργαλείων και λειτουργιών που σχετίζονται με την επικοινωνία που είναι διαθέσιμα στο Matlab. Υπάρχουν πολλά άλλα εργαλεία και λειτουργίες που είναι διαθέσιμα στο λογισμικό, ανάλογα με τις συγκεκριμένες ανάγκες και απαιτήσεις του χρήστη.

Στην εργασία αυτή εξερευνήθηκαν κυρίως οι δυνατότητες του λογισμικού πάνω στα USRP και μέσω του Communications Toolbox.

Για αυτό τον λόγο, μέσω έτοιμων παραδειγμάτων δοκιμάστηκε η εκπομπή και λήψη σημάτων μέσω έτοιμων blocks κώδικα όπως αυτά είναι διαθέσιμα για όποιον διαθέτει το αντίστοιχο toolbox.

4.2.1 Matlab Transmitting and Receiving

Στο λογισμικό Matlab υπάρχει η δυνατότητα μέσω του Documentation να αποκτήσουμε πρόσβαση στο Communications Toolbox Support Package for USRP Radio.

Μέσω του λογισμικού Matlab, μπορούμε να εκτελέσουμε εκπομπή και λήψη ψηφιακού σήματος μέσω των USRPs.

Συγκεκριμένα μπορούμε να “στήσουμε” ένα τηλεπικοινωνιακό σύστημα ψηφιακής διαμόρφωσης QPSK. Αμφότερα ο πομπός και ο δέκτης, υπάρχουν μοντελοποιημένα στο Simulink της Matlab. Συγκεκριμένα είναι το QPSK Transmitter using USRP hardware & QPSK Receiver using USRP hardware. Με τις παρακάτω ρυθμίσεις μπορεί να γίνει εκπομπή και λήψη με τη χρήση ενός USRP B210 ή B200mini.

QPSK Transmitter using USRP hardware

Σε αυτό το έτοιμο μοντελοποιημένο σύστημα, η Matlab δίνει τη δυνατότητα εκπομπής σημάτων ασύρματα με τη διαμόρφωση QPSK. Το μοντέλο του Simulink είναι το κάτωθι και απαρτίζεται από τα παρακάτω κομμάτια:

QPSK Transmitter with USRP(R) Hardware

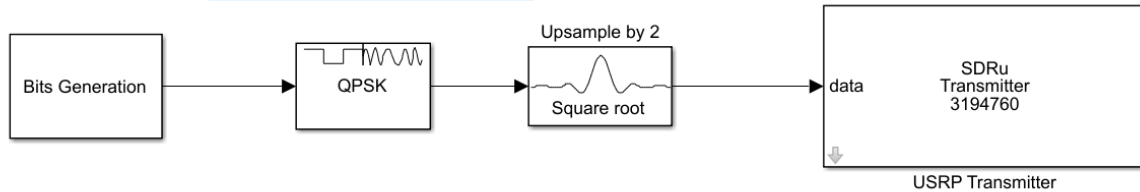
Info

Note: Before running the QPSK models, first run the companion models for frequency offset calibration.

Open the companion sdrufreqcalibtx model

Open the companion sdrufreqcalibrx model

Open the companion sdruqpsktx model



Copyright 2011-2020 The MathWorks, Inc.

Εικόνα 4-1: QPSK Πομπός χρησιμοποιώντας USRP hardware

Σε αυτό το έτοιμο μοντελοποιημένο σύστημα, η Matlab δίνει τη δυνατότητα λήψης σημάτων ασύρματα με τη διαμόρφωση QPSK. Το μοντέλο του Simulink είναι το κάτωθι και απαρτίζεται από τα παρακάτω κομμάτια:

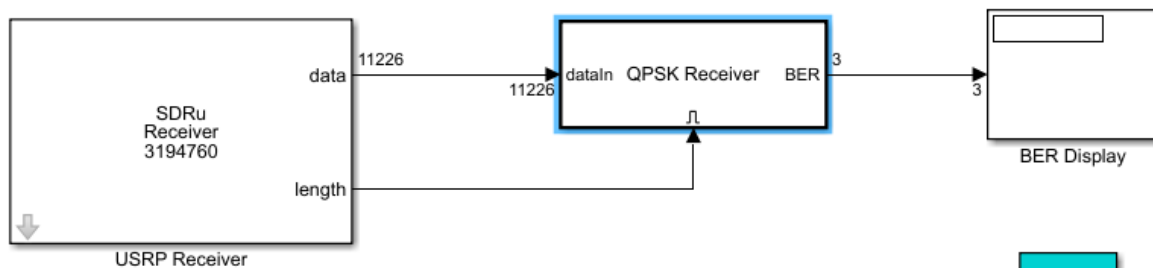
QPSK Receiver with USRP(R) Hardware

Note: Before running the QPSK models, first run the companion models for frequency offset calibration.

Open the companion sdrufreqcalibtx model

Open the companion sdrufreqcalibrx model

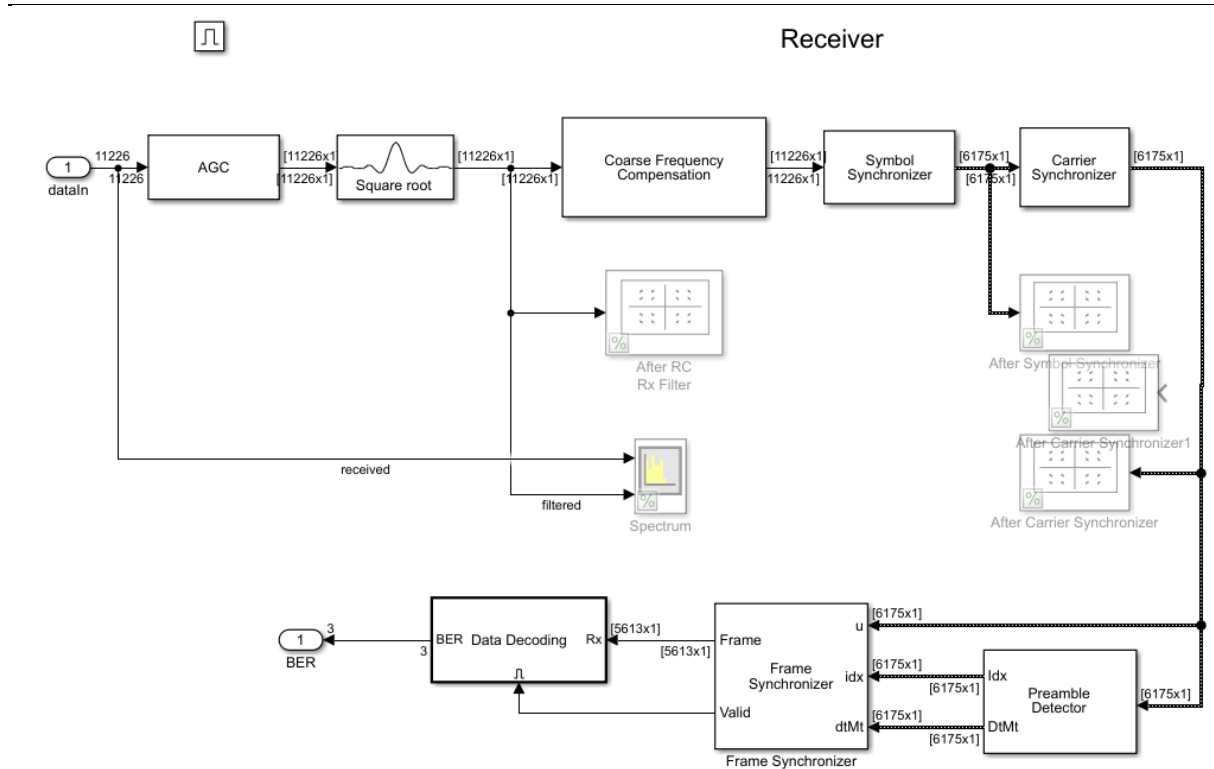
Open the companion sdruqpsktx model



Copyright 2011-2020 The MathWorks, Inc.

Info

Εικόνα 4-2: QPSK Δέκτης χρησιμοποιώντας USRP hardware



Εικόνα 4-3: Ανάλυση του μπλοκ QPSK δέκτη για USRP hardware

4.3 GNU Radio

Μέσω του ελεύθερου λογισμικού GNU Radio μπορούμε να επεξεργαστούμε και να μοντελοποιήσουμε συστήματα επεξεργασίας σημάτων και Software Defined Radio. Μέσω εξωτερικών συσκευών RF, το GNU Radio, μπορεί να δημιουργήσει Software Defined Radio (SDR) ή να μοντελοποιήσει προσομοιώσεις χωρίς επιπλέον Hardware.

Το λογισμικό του GNU Radio παρέχει τα απαραίτητα εργαλεία για να λειτουργήσει ένα Software Radio ή για άλλες εφαρμογές επεξεργασίας σημάτων. Το λογισμικό αυτό παρέχει τα απαραίτητα “δομικά” blocks επεξεργασίας σημάτων, που προσομοιώνουν τις παραπάνω εφαρμογές ως “Flowgraphs”. Τα διαγράμματα αυτά ροής, αποτελούνται από ένα σύνολο συνδεδεμένων μπλοκ. Ο πηγαίος κώδικάς τους είναι γραμμένος είτε σε C++ είτε σε Python.

Η δομή του GNU Radio είναι σε C++, ενώ το γραφικό περιβάλλον της διεπαφής (GNU Radio Companion) είναι σε Python.

Το GNU Radio αποτελείται από μια συλλογή βιβλιοθηκών λογισμικού και εργαλείων που μπορούν να χρησιμοποιηθούν για το σχεδιασμό, την υλοποίηση και τη δοκιμή ενός ευρέος φάσματος συστημάτων και εφαρμογών επικοινωνίας. Περιλαμβάνει υποστήριξη για ένα ευρύ φάσμα τεχνικών ψηφιακής και αναλογικής επικοινωνίας, όπως διαμόρφωση, αποδιαμόρφωση, διόρθωση σφαλμάτων και κωδικοποίηση καναλιού.

Το GNU Radio παρέχει ένα πλαίσιο για τη δημιουργία προσαρμοσμένων “custom” blocks ανάλυσης σημάτων, που δεν υπάρχουν στις αρχικές βιβλιοθήκες του λογισμικού. Περιλαμβάνει υποστήριξη για ένα ευρύ φάσμα πλατφορμών υλικού και διεπαφών λογισμικού, καθιστώντας εύκολη την ενσωμάτωση με άλλα συστήματα και συσκευές.

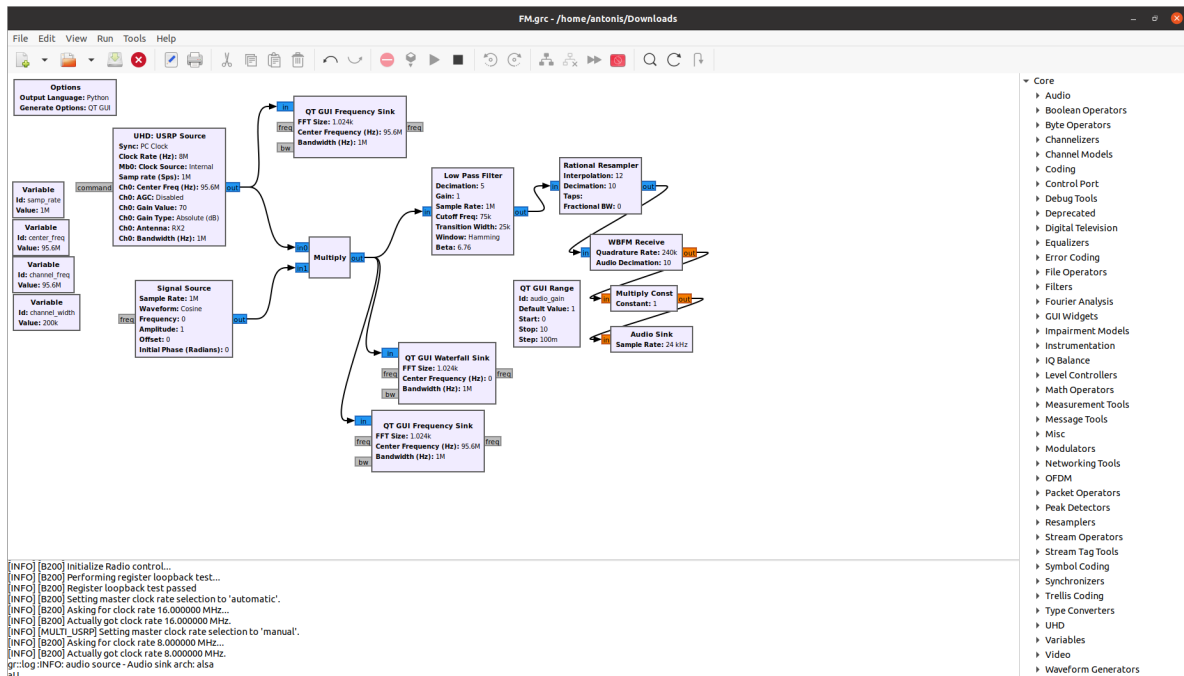
Εκπαιδευτικές και ερευνητικές εφαρμογές: Το GNU Radio χρησιμοποιείται συχνά σε εκπαιδευτικά και ερευνητικά περιβάλλοντα για την εξερεύνηση και κατανόηση των αρχών των συστημάτων επικοινωνίας. Παρέχει μια ευέλικτη και προσαρμόσιμη πλατφόρμα για την κατασκευή και τον πειραματισμό με διαφορετικές τεχνικές και πρωτόκολλα επικοινωνίας.

Το GNU Radio χρησιμοποιείται ευρέως από ερευνητές, μηχανικούς και χομπίστες που ενδιαφέρονται να κατασκευάσουν και να πειραματιστούν με SDR και συστήματα επικοινωνίας. Είναι διαθέσιμο για ένα ευρύ φάσμα λειτουργικών συστημάτων, συμπεριλαμβανομένων των Linux, macOS και Windows.

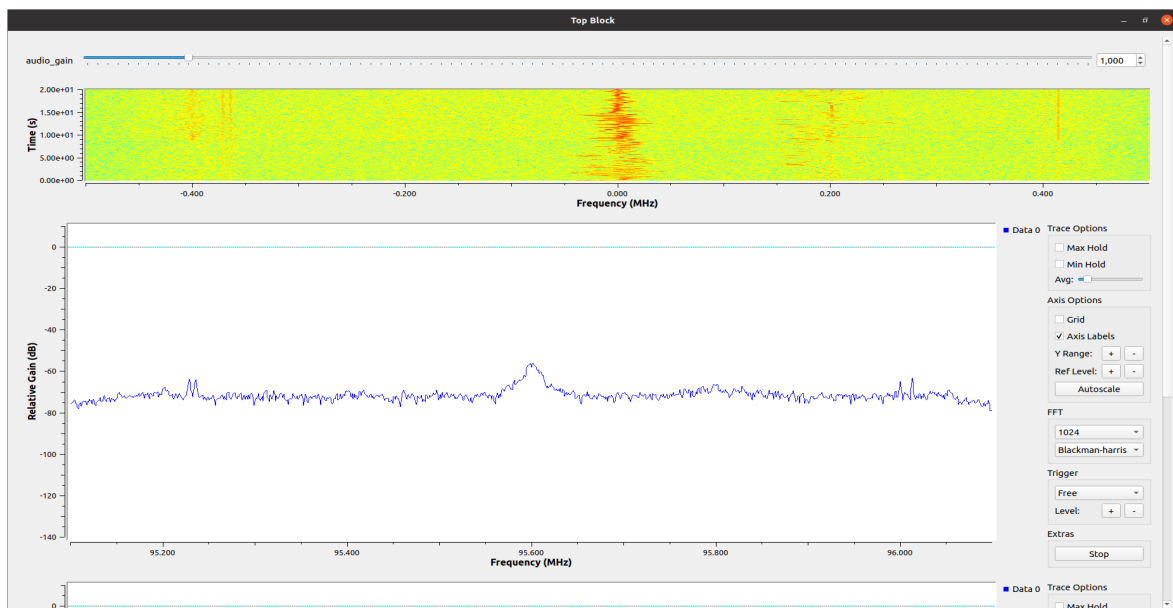
Παρακάτω παρατίθενται μερικές δυνατότητες του λογισμικού ανοιχτού κώδικα καθώς και το πείραμα της εργασίας που αφορά την εφαρμογή τεχνικών ασφάλειας στο Φυσικό Επίπεδο.

4.3.1 Δέκτης FM με το GNU Radio

Για το πρώτο παράδειγμα χρήσης του GNU Radio για τον εντοπισμό και την παρακολούθηση τοπικών ραδιοφωνικών σημάτων έχει δημιουργηθεί το ακόλουθο flowgraph GNU Radio



Εικόνα 4-4: Διάγραμμα ροής - Flowgraph στο λογισμικό GNU Radio, Δέκτη FM



Εικόνα 4-5: Διαγράμματα από το Time/Frequency & Relative Gain/Frequency από QT Blocks του GNU Radio, Δέκτη FM



Εικόνα 4-6: Ολοκληρωμένος Δέκτης FM με USRP B200mini

5

Physical Layer Security with OFDM

5.1 Beamforming με OFDM

Πριν γίνει η εισαγωγή και παρουσίαση των διαφορετικών μερών του συστήματος που δημιουργήσαμε για το μοντέλο Alice, Bob & Eve καθώς και όλων των ξεχωριστών blocks λειτουργιών στο GNU Radio που τους απαρτίζουν ως οντότητες, πρέπει να παρατεθούν τα γενικά χαρακτηριστικά της μετάδοσης σε OFDM που χρησιμοποιήθηκαν.

Αρχικά το μήκος του FFT είναι 64, το sample_rate έχει οριστεί σε 250k, το packet_len είναι 96 και το length_tag_pilots είναι 8. Σε κάθε πλευρά του φάσματος, 8 subcarriers παραμένουν αχρησιμοποίητα, ως διαστήματα φύλαξης.

Οι “**πιλότοι**” που χρησιμοποιήθηκαν είναι στο σύνολο **16** (pilot_carriers_0 και pilot_carriers_1) ενώ το payload μεταφέρεται από τα υπόλοιπα (occupied_carriers). Οι πιλότοι είναι χωρισμένοι σε 2 διαφορετικές ομάδες των 8. Με τις 2 ομάδες να χωρίζονται και να παίρνουν τις τιμές -1 και 1 ως pilot_symbols_1 & pilot_symbols_0. Έπειτα για την δημιουργία του beamforming, στο block του OFDM Carrier Allocator δίνεται το pilot_symbols_ext_1 και pilot_symbols_ext_0 όπου σε συνάρτηση με το ποιο pilot symbol εκπέμπεται το άλλο OFDM

Carrier Allocator εκπέμπει μηδέν. Κοινώς, όταν το ένα RF chain εκπέμπει πιλότους, το άλλο εκπέμπει μηδενικά και αντίστροφα. Ενδεικτικά:

$\text{pilot_symbols_ext_1} = ((0,-1,0,-1,0,1,0,-1,1,0,-1,0,1,0,1,0),)$

$\text{pilot_symbols_ext_0} = ((1,0,1,0,-1,0,1,0,0,-1,0,1,0,-1,0,-1),)$

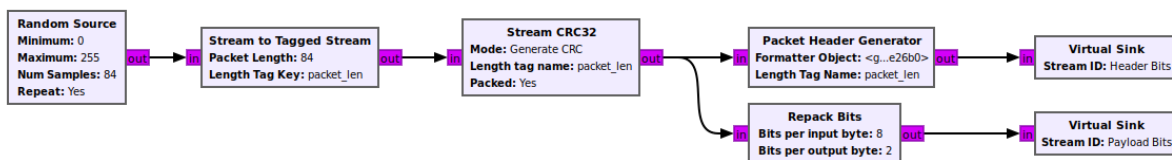
Αναλυτικά παρακάτω παρατίθενται τα ξεχωριστά μέρη του συστήματος και αναλύεται η λειτουργία τους.

5.1.1 Πομπός – Beamformer, Alice

Ξεκινώντας με τον πομπό στο Beamforming, πρέπει να αναφέρουμε τα blocks που χρησιμοποιήθηκαν για αυτόν. Αυτά χωρίζονται σε 4 μεγάλα “εικονικά” block. Με τη σειρά έχουμε την **Δημιουργία Δεδομένων και Πακέτων**, έπειτα το **OFDM Symbol Mapping** και τέλος το **Beamforming & Μετάδοση**.

Δημιουργία Δεδομένων και Πακέτων

Μέσω αυτού του συνόλου των block του GNU Radio, λαμβάνονται οι τυχαίες τιμές που θέλουμε να επικοινωνήσουμε μεταξύ των 2 μερών (Alice & Bob), τα ενθυλακώνει σε δομές “πακέτων” με τους δικούς τους headers, μετά γίνεται η προσθήκη των 32-bit CRC για τον έλεγχο της ακεραιότητας των πακέτων και κατόπιν γίνεται η μεταποίηση των bit (για τα payload bits) και ταυτόχρονα η προσθήκη των Packet Header (για τα header bits – επικεφαλίδα που ενημερώνει τον δέκτη για το μέγεθος του payload). και τέλος την αποστολή τους στα αντίστοιχα Header & Payload bits.



Εικόνα 5-1: Πομπός 1ο μέρος

Random Source

Παράγουμε μέσω αυτού τυχαίες τιμές στο εύρος από 0 έως και 255. Αυτό θα δημιουργεί το συρμό δεδομένων για τις δοκιμές. Επίσης έχει ρυθμιστεί να παράγει 84 τιμές κάθε φορά που ενεργοποιείται, αυτό συμβαίνει συνεχόμενα μιας και έχει προεπιλεγεί το “Repeat”. Η επιλογή έγινε ώστε να δημιουργούνται (μαζί με το CRC, πιλότους, κλπ) 11 σύμβολα OFDM ανά πακέτο.

Stream to Tagged Stream

Μετατρέπει το stream δεδομένων του Random Source σε πακέτα συγκεκριμένου μήκους (στη προκειμένη περίπτωση το μήκος είναι ίδιο με τον αριθμό των τιμών, 84).

Stream CRC32

Μέσω αυτού του block, γίνεται ο απαραίτητος έλεγχος σφαλμάτων. Το 32-bit CRC (Cyclic Redundancy Check) παράγεται για κάθε πακέτο. Η τιμή του CRC συνήθως προστίθεται ώστε ο δέκτης να μπορεί να ελέγξει την ακεραιότητα των δεδομένων. Αν το σήμα έχει υποστεί την όποια αλλαγή εξαιτίας θορύβου ή παρεμβολών τότε το εκπεμπόμενο CRC θα είναι διαφορετικό από το λαμβανόμενο CRC και συνεπώς θα υπάρχει ένδειξη σφάλματος. Το CRC πραγματοποιεί μια διαίρεση πολωνύμου μεταξύ των δεδομένων και γνωστής ακολουθίας. Για να θεωρηθεί η λήψη ενός πακέτου σωστή πρέπει να υπολογίσουν τόσο πομπός όσο και δέκτης το ίδιο υπόλοιπο.

Packet Header Generator

Αυτό το block προσθέτει ένα header σε κάθε πακέτο. Η προσθήκη του header είναι απαραίτητη για το συντονισμό και συγχρονισμό με τον δέκτη.

Repack Bits

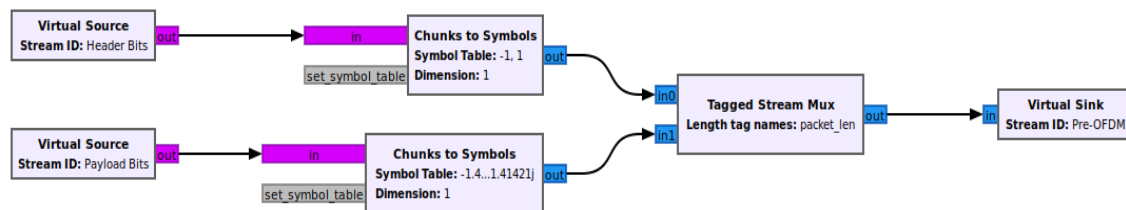
Το μπλοκ αυτό διαμορφώνει πρακτικά τον τρόπο με τον οποίο, δημιουργούνται τα πακέτα του payload. Σε αυτή τη περίπτωση έχουμε για κάθε 8 bits (1 byte) δεδομένων εισόδου σε 2 bits εξόδου. Υποδηλώνεται έτσι ότι θα χρησιμοποιηθεί QPSK διαμόρφωση.

Virtual Sink (Header Bits & Payload Bits)

Τέλος τα 2 Virtual Sinks, υπάρχουν ώστε τα Header Bits & Payload Bits, να καταλήξουν στο επόμενο στάδιο της διαδικασίας ξεχωριστά ώστε να γίνει σωστά η δημιουργία συμβόλων της OFDM (Symbol Mapping)

OFDM Symbol Mapping

Ομάδα μπλοκ που πραγματοποιεί την αντιστοίχιση bit σε σύμβολα με βάση σηματοστερισμό payload και header για τα χρησιμοποιούμενα subcarriers. Στη συγκεκριμένη περίπτωση του δόθηκε ο σηματοστερισμός QPSK για payload και BPSK για header.



Εικόνα 5-2: Πομπός 2ο μέρος

Virtual Sources:

- **Virtual Source (Header Bits)** Το stream των header σε bits που δημιουργήθηκε στο προηγούμενο στάδιο.
- **Virtual Source (Payload Bits)** Το stream των δεδομένων/payload σε bits που δημιουργήθηκε στο προηγούμενο στάδιο.

Chunk to Symbols Mapping:

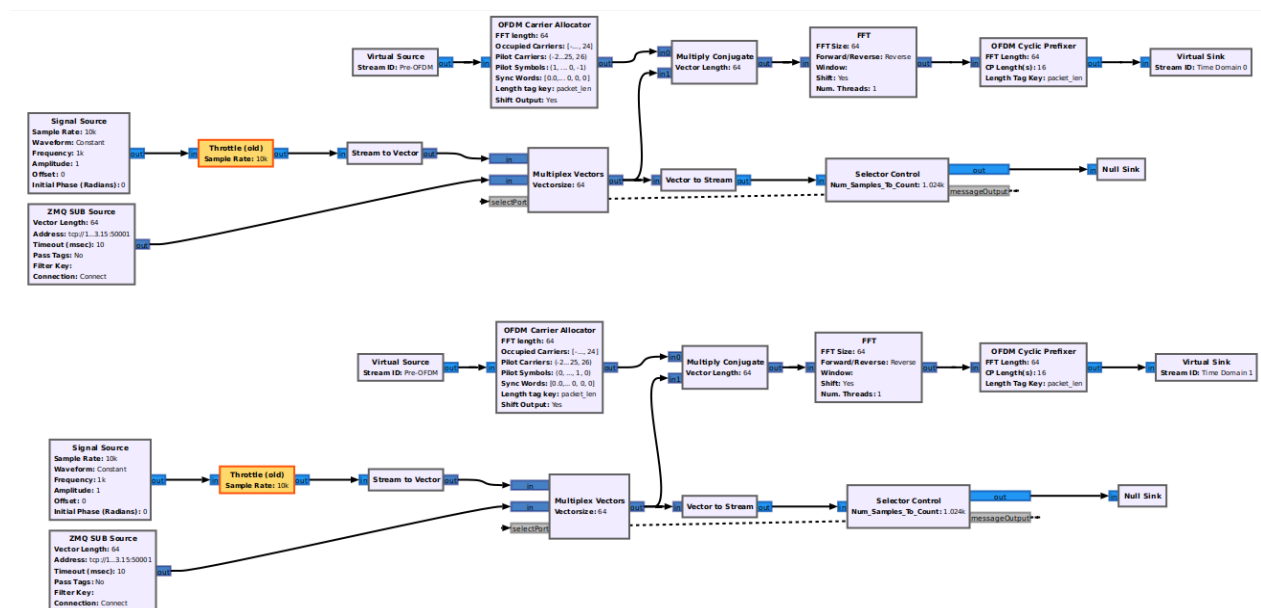
- **Chunks to Symbols (Header)** Σε αυτό το block τα εισερχόμενα bits από τα Header Bits γίνονται σύμβολα της διαμόρφωσης BPSK, με τιμές $[-1, 1]$.

- **Chunks to Symbols (Payload)** Σε αυτό το block τα εισερχόμενα bits από τα Payload Bits γίνονται σύμβολα της διαμόρφωσης QPSK.

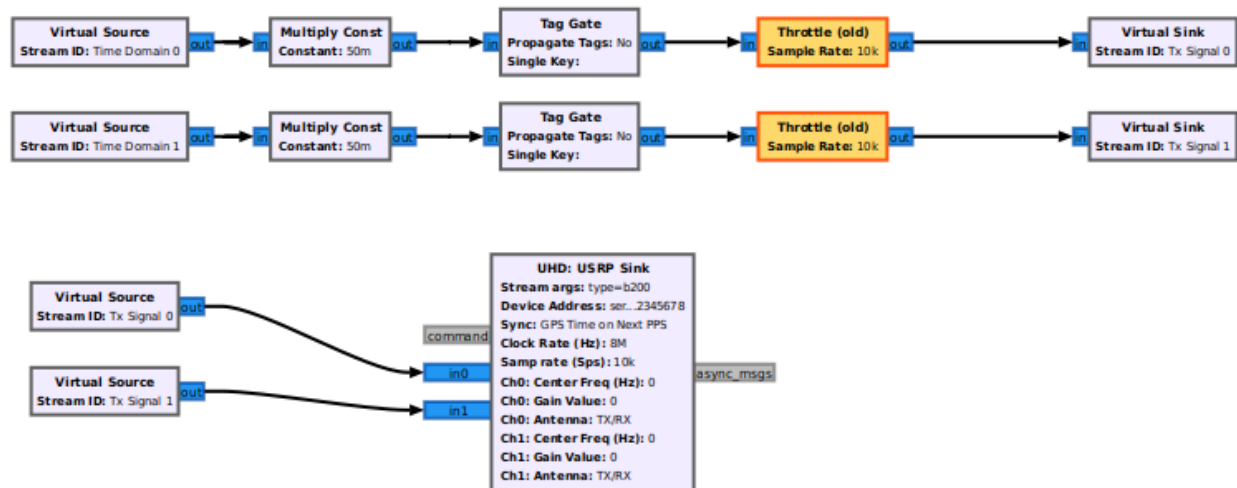
Tagged Stream Mux Σε αυτό το μπλοκ γίνεται ο συνδυασμός των 2 παραπάνω symbol streams, header & payload. Το κάθε ένα διαθέτει συγκεκριμένο μήκος δηλαδή tagged length, ώστε να γίνεται σωστά ο διαχωρισμός των πακέτων στο κομμάτι του δέκτη.

Virtual Sink (Pre-OFDM)

Τέλος το Virtual Sink, έχει πλέον τα έτοιμα σύμβολα τα οποία θα περάσουν επιπρόσθετη διαμόρφωση για να εκπεμφθούν κάτω από το σχήμα της OFDM.



Εικόνα 5-3: Πομπός 3ο μέρος



Εικόνα 5-4: Πομπός 4ο μέρος

Virtual Source (Pre-OFDM)

Αυτό το block παίρνει τα διαμορφωμένα σύμβολα που αναμένεται να περάσουν από περαιτέρω επεξεργασία ώστε να εκπεμφθούν ως OFDM .

ZMQ SUB Source

Το ZeroMQ (ZMQ) αποτελεί το block μέσω του οποίου επικοινωνούνται τα στοιχεία του καναλιού Alice-Bob πίσω στον πομπό. Αυτό γίνεται μέσω μιας άλλης οδού επικοινωνίας και δικτύου στην οποία έχουν πρόσβαση πομπός και δέκτης (για πειραματικούς λόγους χρησιμοποιείται τοπικό δίκτυο ethernet ή wifi). Σε πραγματικό σύστημα, η ανάδραση από το δέκτη θα γινόταν μέσω αμφίδρομης επικοινωνίας στο ασύρματο μέσο.

OFDM Carrier Allocator

Το block, πρακτικά τοποθετεί τα σύμβολα που λαμβάνει στους υποφορείς/subcarriers της OFDM. Σε αυτό το block πρέπει να δοθεί το μήκος του FFT (που θα γίνει σε 2ο χρόνο), τα σύμβολα των πιλότων για την εκτίμηση καναλιού, τα sync words που είναι απαραίτητα για τον

συγχρονισμό καθώς και τα Length Tag Key, όπου πρακτικά ορίζεται το μήκος κάθε πακέτου (όπως έχει αναφερθεί και στη προηγούμενη φάση). Τέλος ορίζεται και το Shift Output που είναι για την ενεργοποίηση/απενεργοποίηση του DC carrier shifting (αν δηλαδή θέλουμε να θεωρούμε FFT από -32 έως 31 subcarriers ή από 0 έως 64).

Cubic Interpolation (interp)

Αύξηση του sample rate με χρήση της κυβικής παρεμβολής. Το μπλοκ φτιάχτηκε στα πλαίσια της διπλωματικής. (<https://www.paulinternet.nl/?page=bicubic>)

Complex Conjugate

Το block παράγει τον μιγαδικό συζυγή της εισόδου στην έξοδο.

Multiply

Το block αυτό, πολλαπλασιάζει τα διαφορετικά σήματα από το "Complex Conjugate" και το "OFDM Carrier Allocator". Σε αυτό το σημείο εισάγεται στο σήμα το ειδικό βάρος για την δημιουργία της “δέσμης” (η πληροφορία έρχεται μέσω του ZMQ source μετά από το complex conjugate). Με αυτόν τον πολλαπλασιασμό εφαρμόζεται ο beamformer ανά subcarrier.

Stream to Vector

Μετατρέπει τα streaming data σε διάνυσμα/vector format.

FFT (Fast Fourier Transform)

Μετατρέπει, το σήμα από το πεδίο του χρόνου στο πεδίο της συχνότητας. Το block αυτό, παίρνει τα δείγματα και τα τοποθετεί σε frequency subcarriers.

OFDM Cyclic Prefixer

Προσθήκη του κυκλικού προθέματος/cyclic prefix σε κάθε σύμβολο της OFDM, ώστε να αντιμετωπιστεί το φαινόμενο της πολυδιαδρομικής διασυμβολικής παρεμβολής.

Throttle

Πρακτικά επιβάλλει την επεξεργασία των δεδομένων που διέρχονται από αυτό με ένα συγκεκριμένο sample rate.

UHD: USRP Sink

Όπως έχουμε αναφερθεί νωρίτερα, για την εκπομπή του σήματος θα χρησιμοποιηθεί ένα SDR. Για την διασύνδεση του με το λογισμικό του GNU Radio υπάρχει το Universal Software Radio Peripheral (USRP) Sink block. Σε αυτό το block ορίζουμε τις επιμέρους τιμές για τον καθορισμό της εκπομπής. Δηλαδή το Sample Rate, και έπειτα παραμετροποιούμε τα επιμέρους στοιχεία της εκπομπής όπως κεντρική συχνότητα, το κέρδος/gain και την αντίστοιχη κεραία για κάθε κανάλι.

Η παραμετροποίηση του USRP έγινε ως εξής για τα χαρακτηριστικά RF και για τα γενικά χαρακτηριστικά εκπομπής και λήψης.

Properties: UHD: USRP Sink

General Advanced RF Options Documentation

Ch0: Center Freq (Hz) 1100000000

Ch0: Gain Value 70

Ch0: Gain Type Absolute (dB)

Ch0: Antenna TX/RX

Ch0: Bandwidth (Hz) 0

Ch1: Center Freq (Hz) 1100000000

Ch1: Gain Value 70

Ch1: Gain Type Absolute (dB)

Ch1: Antenna TX/RX

Ch1: Bandwidth (Hz) 0

OK Cancel Apply

Εικόνα 5-5: Παράμετροι για RF

Properties: UHD: USRP Sink

General

Advanced

RF Options

Documentation

Input Type

Complex float32

Wire Format

Automatic

Stream args

Stream channels

[]

Device Address

"serial=3150302"

Device Arguments

""

Sync

No Sync

Start Time (seconds)

-1.0

Clock Rate (Hz)

4000000

Num Mboards

1

Mb0: Clock Source

Default

Mb0: Time Source

Default

Mb0: Subdev Spec

Num Channels

2

Samp rate (Sps)

samp_rate

TSB tag name

""

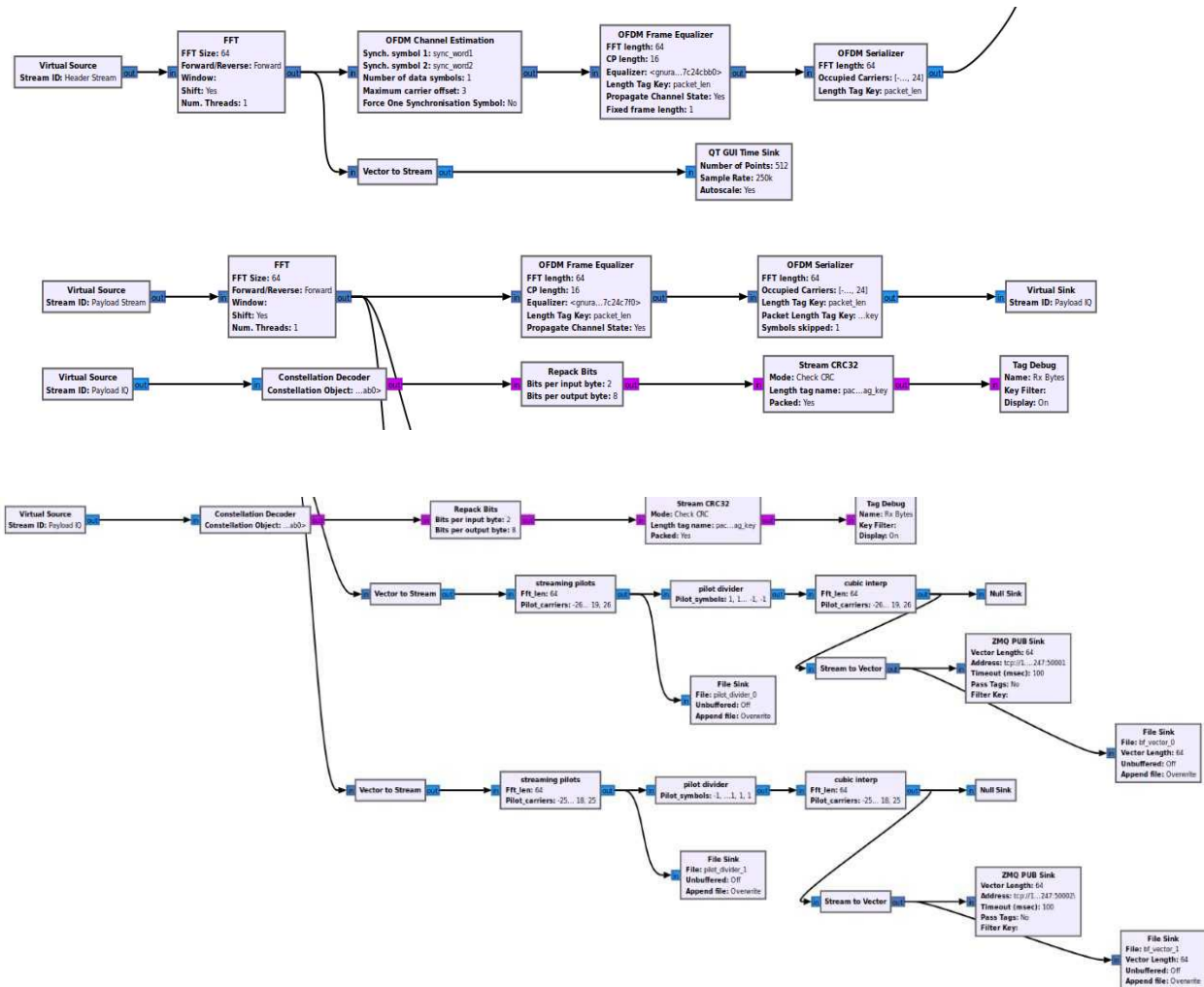
OK

Cancel

Apply

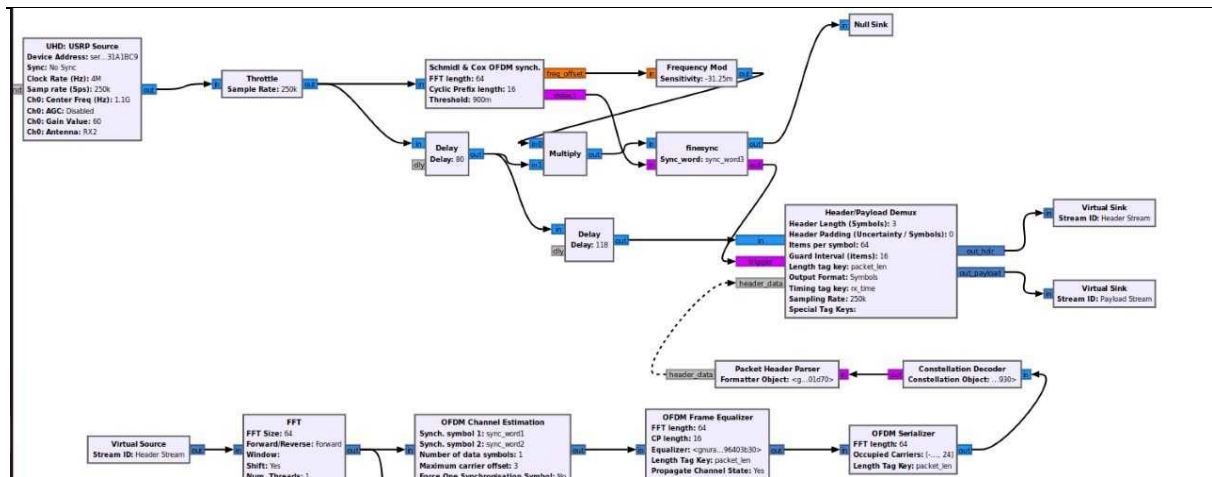
Εικόνα 5-6: Παράμετροι για γενικά χαρακτηριστικά

5.1.2 Δέκτης, Bob



Εικόνα 5-7: Δέκτης Bob, 1ο μέρος

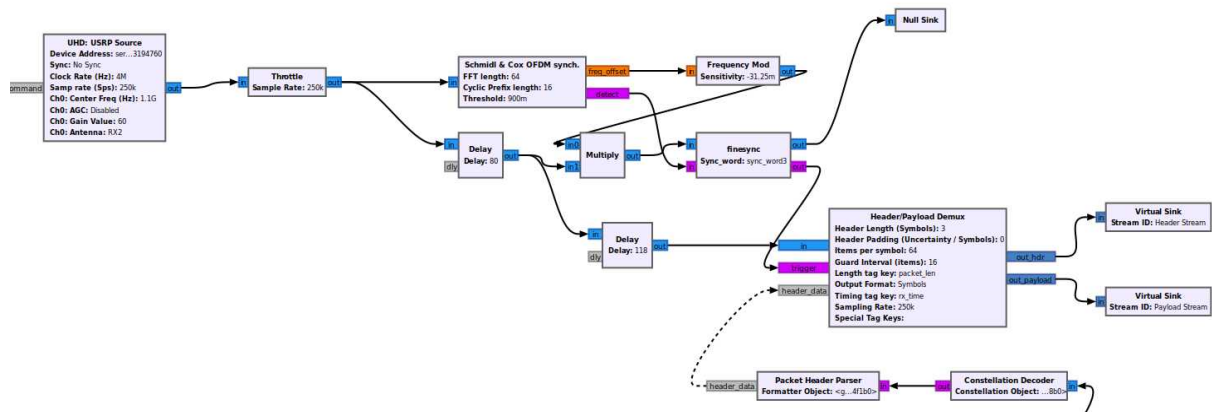
Διπλωματική εργασία: Υλοποίηση τεχνικών ασφάλειας στο Φυσικό Στρώμα στην OFDM με Software Defined Radios



Εικόνα 5-8: Δέκτης Bob, 2^ο μέρος

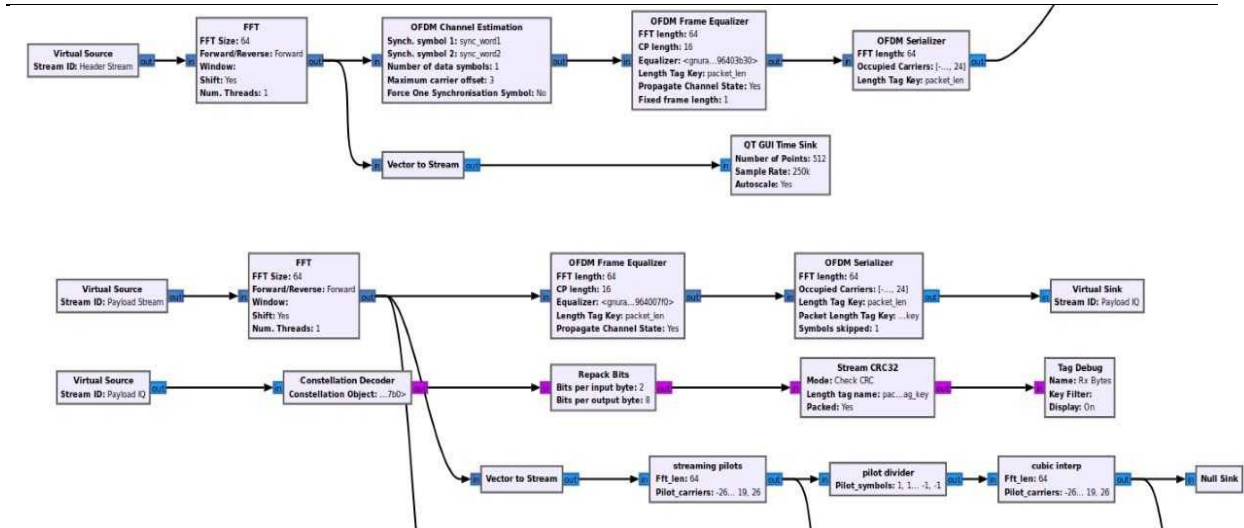
5.1.3 Υποκλοπέας Eve

Για την Eve, έχουμε το παρόμοιο flowgraph με τον Bob, με τη διαφορά ότι δεν επικοινωνεί μέσω ZMQ με την Alice, την πληροφορία για την κατάσταση καναλιού όπως ο Bob.

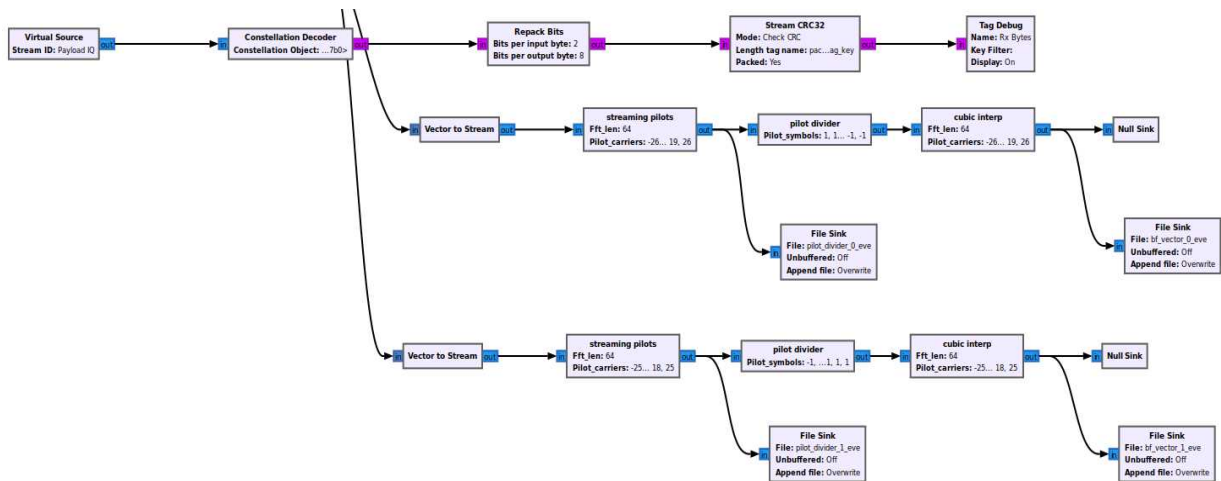


Εικόνα 5-9: Δέκτης Eve, 1^ο μέρος

Διπλωματική εργασία: Υλοποίηση τεχνικών ασφάλειας στο Φυσικό Στρώμα στην OFDM με Software Defined Radios



Εικόνα 5-10: Δέκτης Eve, 2^ο μέρος



Εικόνα 5-11: Δέκτης Eve, 2^ο μέρος

Στη συνέχεια αναλύονται τα επιπλέον μπλοκς που χρησιμοποιήθηκαν ή υλοποιήθηκαν στο δέκτη (Bob ή/και Eve).

UHD: USRP Source

Σε αυτό το block βρίσκεται η απαραίτητη διεπαφή για την παραμετροποίηση του USRP (Universal Software Radio Peripheral) B200 και B210 που αποτελούν τον δέκτη μας. Σε αυτό, γίνεται η συλλογή των σημάτων και έπειτα προωθείται στο υπόλοιπο GNU Radio flowgraph που έχουμε δημιουργήσει.

Ενδεικτικά παρατίθενται οι παράμετροι που χρησιμοποιήθηκαν στο πείραμα:

Sync: Synchronization mode.

Sample Rate (Fs): 250k δείγματα ανά δευτερόλεπτο.

Center Frequency (fc): Κεντρική συχνότητα λαμβανόμενου σήματος (1.1 και 2.2 GHz). Σημειώνεται ότι η επιλογή συχνότητας έγινε ώστε να μην υπάρχουν παρεμβολές από πραγματικά ραδιοσυστήματα.

Gain: Amplification setting.

Antenna: Κεραία που παρέχεται από το USRP.

Throttle (old)

Όπως και η νεότερη έκδοση του, έτσι και αυτό επιβάλλει την επεξεργασία των δεδομένων που διέρχονται από αυτό με ένα συγκεκριμένο sample rate.

Schmidl & Cox OFDM Synch.

Αυτό το block, εκτελεί τις διεργασίες συγχρονισμού για τα OFDM σύμβολα σύμφωνα με τη μέθοδο Schmidl & Cox. Αυτό είναι πολύ βασικό για την ορθή αποκωδικοποίηση των συμβόλων της OFDM. Πραγματοποιεί coarse (χονδρικό) συγχρονισμό και είναι πιθανό να υπάρχουν λάθη. Επίσης χρησιμοποιείται για τον υπολογισμό της συχνότητας ολίσθησης μεταξύ πομπού και δέκτη.

Frequency Mod

Διαμορφώνει τη συχνότητα του ληφθέντος σήματος, ανάλογα με την εκτίμηση φάσης του Schmidl and Cox, που οδηγεί στην διόρθωση της ολίσθησης συχνότητας. Σημαντική σημείωση σε αυτό το σημείο αποτελεί το γεγονός ότι απαιτείται η ύπαρξη blocks που θα βοηθήσουν για την αντιμετώπιση του **Carrier Frequency Offset (CFO)**.

Multiply

Αυτό το block πολλαπλασιάζει 2 σήματα μαζί στο πεδίο του χρόνου.

Delay

Αυτό το block εισάγει καθυστέρηση στο σύστημα ώστε να μπορέσουν να εισαχθούν ορθά τα διαφορετικά σήματα από το beamforming.

QT GUI Time Sink

Το block αυτό μας προσφέρει ένα γραφικό περιβάλλον στο οποίο μπορούμε να δούμε το σήμα στο πεδίο του χρόνου real-time.

Header/Payload Demux

Με αυτό το Demux, γίνεται ο διαχωρισμός header και payload του data stream.

Virtual Sink (Header Stream & Payload Stream)

Όπως και στον πομπό (Alice) έτσι και στον δέκτη, χρησιμοποιούμε Virtual Sink για να διαχειριστούμε καλύτερα στο flowgraph τα headers και το payload.

Σε αυτό το κομμάτι του flowgraph γίνονται τα απαραίτητα αρχικά στάδια για την επεξεργασία του σήματος. Τα blocks που το απαρτίζουν συγκεντρώνονται στη λήψη, συγχρονισμό και αρχική επεξεργασία του σήματος. Έμφαση δίνεται και στον διαχωρισμό headers και payload ώστε σε μετέπειτα beamforming του συστήματος MISO (Multiple Input, Single Output)

Virtual Source (Header Stream and Payload Stream)

Η συνέχεια των Virtual Sinks, headers και payload.

FFT

Σε αυτό το block, γίνεται το Fast Fourier Transform για το ληφθέν σήμα.

OFDM Frame Equalizer

Πρακτικά στο block αυτό γίνεται εκτίμηση του ραδιοδιαύλου και εξισορρόπηση με χρήση one-tap frequency domain equalizer. Στην συγκεκριμένη υλοποίηση χρησιμοποιούνται τα sync words του προοιμίου για την εκτίμηση.

OFDM Serializer

Μετατρέπει το σήμα της OFDM από παράλληλα streams σε σειριακά stream.

Constellation Decoder

Αποκωδικοποιεί το σήμα σε σύμβολα βάση της θέσης τους στα διαγράμματα αστερισμών/constellation diagrams (ανάλογα της διαμόρφωσής τους π.χ. PSK).

Repack Bits

Αλλάζει τη μορφή του format των bits και δίνει στην έξοδο του διαφορετικό αριθμό bit πληροφορίας ανά byte

Stream CRC32

Όπως είχαμε αναφερθεί και στον πομπό, για τη λειτουργία του CRC32, έτσι και εδώ έχουμε το block αυτό έτσι ώστε να γίνει ο απαραίτητος έλεγχος για την ακεραιότητα των δεδομένων. Πρόκειται για έναν υπολογισμό υπολοίπου σε μια πολυωνυμική διαίρεση.,

Tag Debug

Αυτό το block μας βοηθάει στο debugging, ώστε να παρακολουθούμε τα tags εντός του flowgraph.

Vector to Stream

Όπως είδαμε και την αντίστροφη διαδικασία στο κομμάτι του πομπού, έτσι και εδώ αυτό το block μετατρέπει τα vector data σε ένα serialized stream.

Band Pass Filter

Επιτρέπει στα σήματα εντός ορισμένου ορίου να περνάνε και απορρίπτει τα υπόλοιπα σήματα.

ZMQ PUB Sink

Το block αυτό επικοινωνεί μέσω του μέσω ZMQ PUB Source τα στοιχεία του καναλιού Alice-Bob πίσω στον πομπό.

Packet Header Parser

Αυτό το block διαβάζει τον header των δεδομένων κάθε πακέτου και εξάγει πληροφορίες.

Εκτός από τα παραπάνω, υλοποιήθηκαν και καινούρια μπλοκς που επιτελούν συγκεκριμένες λειτουργίες.

Finesync

Όπως αναφέρθηκε ο αλγόριθμος Schmidl and Cox δεν πετυχαίνει ακριβή συγχρονισμό. Το συγκεκριμένο μπλοκ παίρνει τη σκυτάλη από τον Schmidl & Cox και το σήμα αφού έχει διορθωθεί η ολίσθηση συχνότητας και πραγματοποιεί εταιροσυσχέτιση του σήματος γύρω από το σημείο συγχρονισμού που έχει υπολογιστεί, με το γνωστό preamble (το sync_word_3 που είναι το sync_word_1 εκφρασμένο στο πεδίο του χρόνου). Η μεγιστοποίηση της ετεροσυσχέτισης δίνει ένα ξεκάθαρο, ακριβές σημείο συγχρονισμού.

streaming_pilots

Ένα μπλοκ που διαχωρίζει τους πιλότους από κάθε RF αλυσίδα εκπομπής, ώστε να τα χρησιμοποιήσει για την πραγματοποίηση του beamforming στον πομπό.

pilot_divider

Το μπλοκ αυτό καθορίζει πώς ακριβώς γίνεται το beamforming. Παίρνει ως είσοδο τους απομονωμένους πιλότους, διαιρεί με τις αρχικές τιμές των πιλότων και εκτιμά το κανάλι με Zero Forcing (ZF). Στη συνέχεια:

- Πραγματοποιεί SVD και αποφασίζει αν θα προχωρήσει σε MRT beamforming ή αν θα γίνει εκπομπή AN. Αυτό γίνεται με τους εξής κανόνες:
 - Αν ο δέκτης έχει μια αλυσίδα, τότε εφαρμόζεται MRT.
 - Αν ο δέκτης έχει δυο αλυσίδες και η μια ιδιοτιμή είναι τουλάχιστον 20πλάσια από την άλλη 13 dB διαφορά, τότε πραγματοποιείται AN. Θα σταλεί στον πομπό μέσω ZMQ το precoding vector με τις ιδιάζουσες τιμές που θα πραγματοποιούν το AN.
 - Σε διαφορετική περίπτωση στέλνονται πίσω οι συντελεστές του MRT για 2x2 MIMO.

Στο 2ο μέρος του Διαγράμματος γίνονται τα επόμενα στάδια της επεξεργασίας του σήματος, όπου φιλτράρονται τα σημαντικά μέρη του σήματος, γίνεται η αποκωδικοποίηση & αποδιαμόρφωση του σήματος. Έπειτα εξάγονται όλες οι χρήσιμες πληροφορίες για αυτό. Επίσης σε αυτό το σημείο γίνεται και η επικοινωνία με τον πομπό ώστε αυτός να μάθει την εκτίμηση καναλιού και να παραμετροποιήσει ορθά τις τιμές των πινάκων του για το beamforming.

5.2 Αποτελέσματα

5.2.1 Σενάρια

Στην παρούσα εργασία, οι ερευνητικές δοκιμές εστιάζουν στα εξής σενάρια μεταξύ Alice-Eve-Bob:

1. Εκπομπή Alice, χωρίς υλοποίηση Τεχνικής Ασφάλειας στο Φυσικό με τον Bob σε κοντινότερη απόσταση από αυτήν της Eve.
2. Εκπομπή Alice, χωρίς υλοποίηση Τεχνικής Ασφάλειας στο Φυσικό με την Eve σε κοντινότερη απόσταση από αυτήν του Bob.

3. Εκπομπή Alice και υλοποίηση Beamforming με τον Bob να βρίσκεται σε κοντινότερη απόσταση σε σχέση με την Eve.
4. Εκπομπή Alice και υλοποίηση Beamforming με την Eve σε κοντινότερη απόσταση σε σχέση με τον Bob.
5. Εκπομπή Alice και υλοποίηση Artificial Noise για όλες τις περιπτώσεις.



Εικόνα 5-12: Μετρητικό σύστημα - τοποθεσία Alice, Bob και Eve.

Η Alice χρησιμοποιεί το B210, βρίσκεται εντός κλειστού χώρου και εκπέμπει μέσω 2 κεραιών. Στην δοκιμή του AN, η Alice εκπέμπει μέσω του X310, πάλι μέσω 2 κεραιών.



Εικόνα 5-13: Το σύστημα της Alice, Ettus B210 & Lenovo IdeaPad3

Σε αυτό το σημείο, πρέπει να αναφερθεί ότι τα 2 USRPs που ανάλογα το σενάριο, προσομοιώνουν την Eve και τον Bob, έχουν τοποθετηθεί σε απόσταση τέτοια ώστε το ένα να βρίσκεται λίγο πιο κοντά στο πομπό/Alice. Ενώ κανένα από τα δυο σε καμία περίπτωση δεν έχει οπτική επαφή με τον πομπό.



Εικόνα 5-14: Με πράσινο, η απόσταση που χωρίζει το κοντινό USRP με τον δέκτη και με κίτρινο το μακρινό

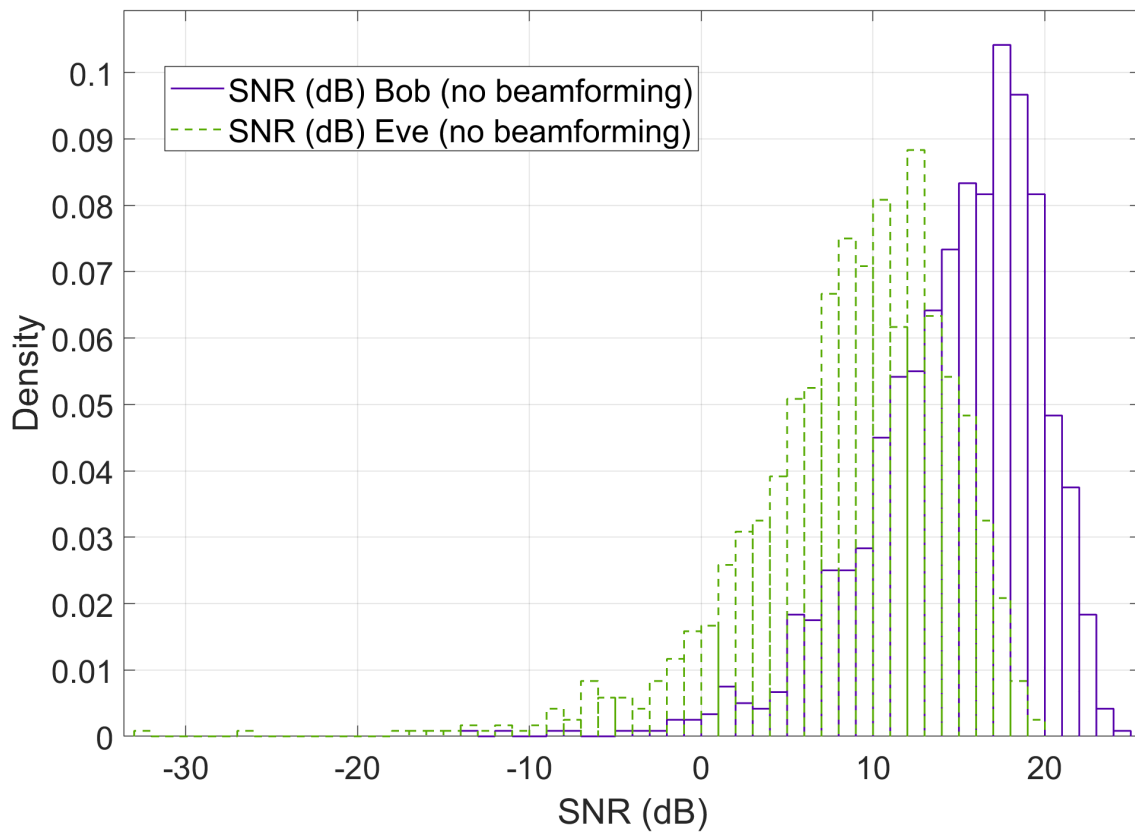
Σενάριο 1: Εκπομπή Alice, χωρίς υλοποίηση Τεχνικής Ασφάλειας στο Φυσικό με τον Bob σε κοντινότερη απόσταση από αυτήν της Eve.

Σε αυτό το σενάριο ο Bob βρίσκεται λίγο πιο κοντά στην Alice από την Eve. Στην **Error! Reference source not found.** με πράσινο χρώμα το B200mini μέσω του οποίου λαμβάνει ο Bob σε αυτή τη περίπτωση, αυτό το USRP βρίσκεται σε κοντινότερη απόσταση σε σύγκριση με το αντίστοιχο USRP της Eve.



Εικόνα 5-15: Bob και Eve για τα σενάρια 1 και 3

Τα αποτελέσματα για το σενάριο φαίνονται στην παρακάτω Εικόνα 5-16.



Εικόνα 5-16: Αποτελέσματα σηματοθορυβικού λόγου λήψης - Σύγκριση Bob & Eve

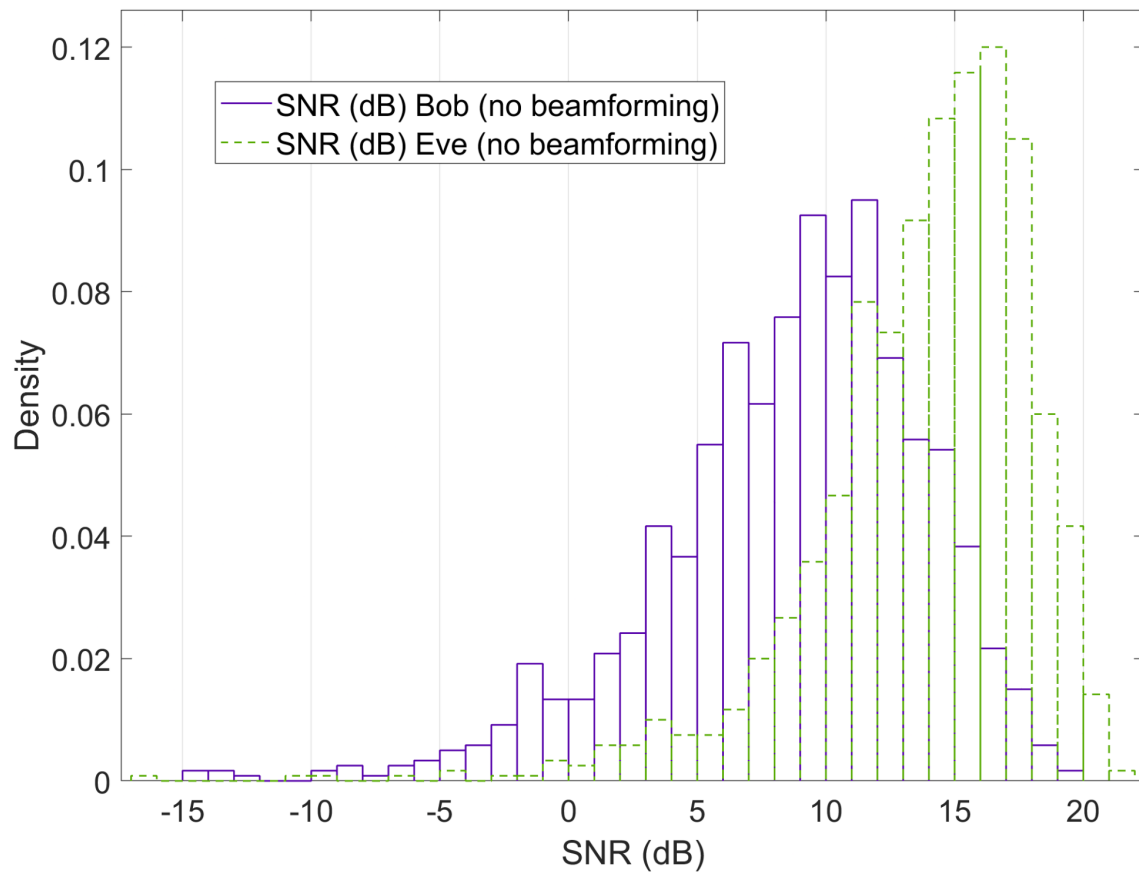
Παρατηρούμε, ότι ο Bob, όντας πιο κοντά στην πηγή εκπομπής Alice, έχει στατιστικά μεγαλύτερο SNR και συνεπώς λαμβάνει ισχυρότερο σήμα από την Eve όπως ήταν και το αναμενόμενο. Κατά συνέπεια κατά μέσο όρο η χωρητικότητα μυστικότητας είναι κατά μέσο όρο θετική.

Σενάριο 2: Εκπομπή Alice, χωρίς υλοποίηση Τεχνικής Ασφάλειας στο Φυσικό με την Eve σε κοντινότερη απόσταση από αυτήν του Bob.



Εικόνα 5-17: Αποψη των Bob & Eve για τα σενάρια 2 & 4

Τα αποτελέσματα για το σενάριο φαίνονται στην παρακάτω Εικόνα 5-18.



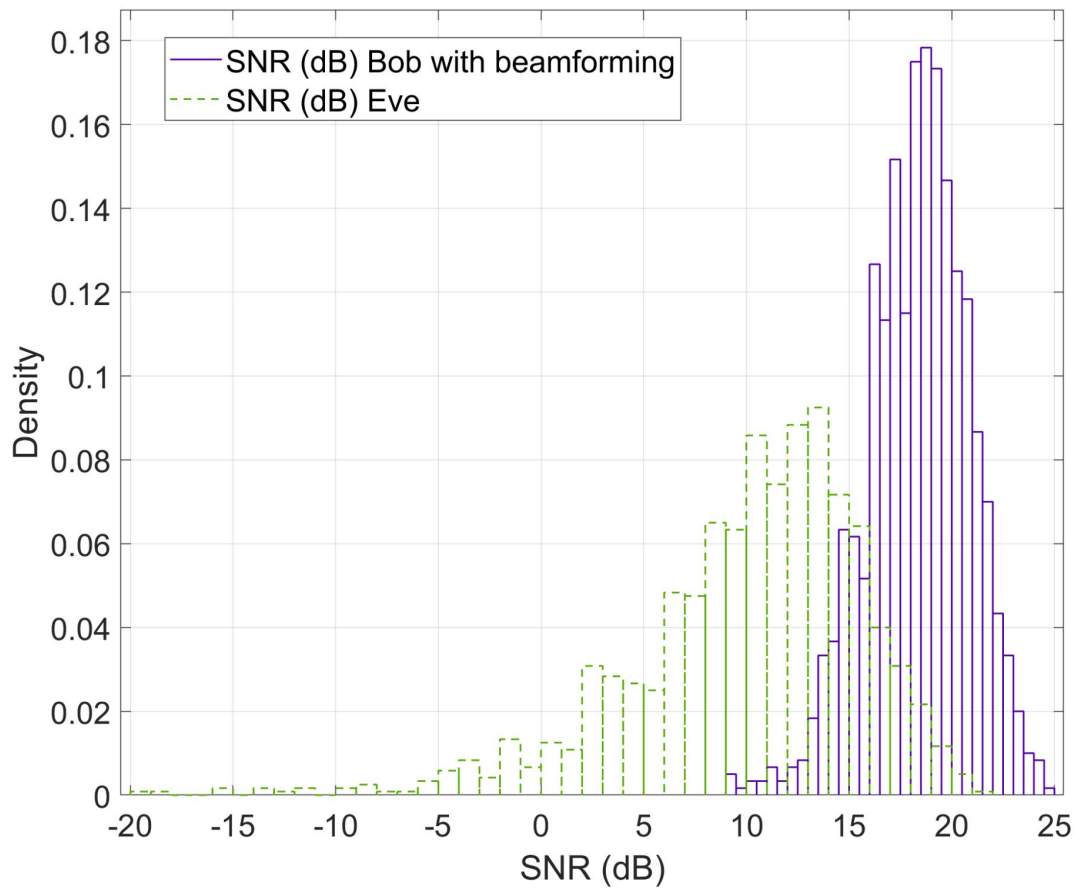
Εικόνα 5-18: Αποτελέσματα λήψης σήματος και σύγκριση μεταξύ Bob & Eve

Παρατηρούμε, ότι αυτή τη φορά η Eve, όντας πιο κοντά στην πηγή εκπομπής, έχει στατιστικά μεγαλύτερο SNR άρα και ισχυρότερο σήμα από τον Bob.

Σενάριο 3: Εκπομπή Alice και υλοποίηση Beamforming με τον Bob να βρίσκεται σε κοντινότερη απόσταση σε σχέση με την Eve.

Σε αυτή τη περίπτωση, η διαφορά στη λήψη σήματος είναι σημαντικά πιο μεγάλη με τον Bob να έχει μέχρι και διπλάσιο σχεδόν SNR εν συγκρίσει με την Eve.

Τα αποτελέσματα για το σενάριο φαίνονται στην παρακάτω Εικόνα 5-19

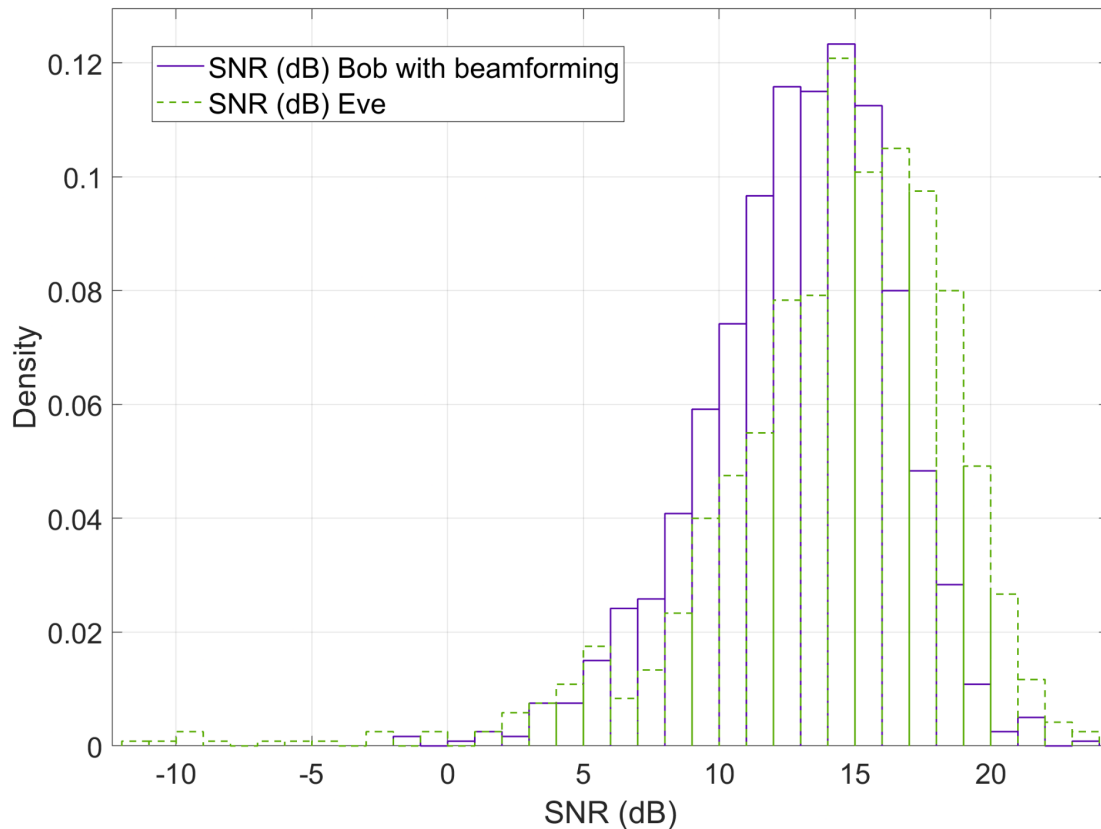


Εικόνα 5-19: Αποτελέσματα λήψης σήματος και σύγκριση μεταξύ Bob & Eve

Το beamforming και η διαφορά της απόστασης με την Eve, δίνουν ξεκάθαρο πλεονέκτημα στον Bob.

Σενάριο 4: Εκπομπή Alice και υλοποίηση Beamforming με την Eve σε κοντινότερη απόσταση σε σχέση με τον Bob.

Τα αποτελέσματα για το σενάριο φαίνονται στην παρακάτω Εικόνα 5-20.



Εικόνα 5-20: Αποτελέσματα λήψης σήματος και σύγκριση μεταξύ Bob & Eve

Στο τελευταίο σενάριο, παρατηρείται επίσης πλεονέκτημα του Bob σε ορισμένο εύρος του SNR, ακόμα και αν η απόσταση του με την Alice είναι μεγαλύτερη συγκριτικά με την Eve. Η τελευταία παρότι πλεονεκτεί σε απόσταση και αρχικό SNR, χάνει το πλεονέκτημα σε μεγάλο αριθμό περιπτώσεων.

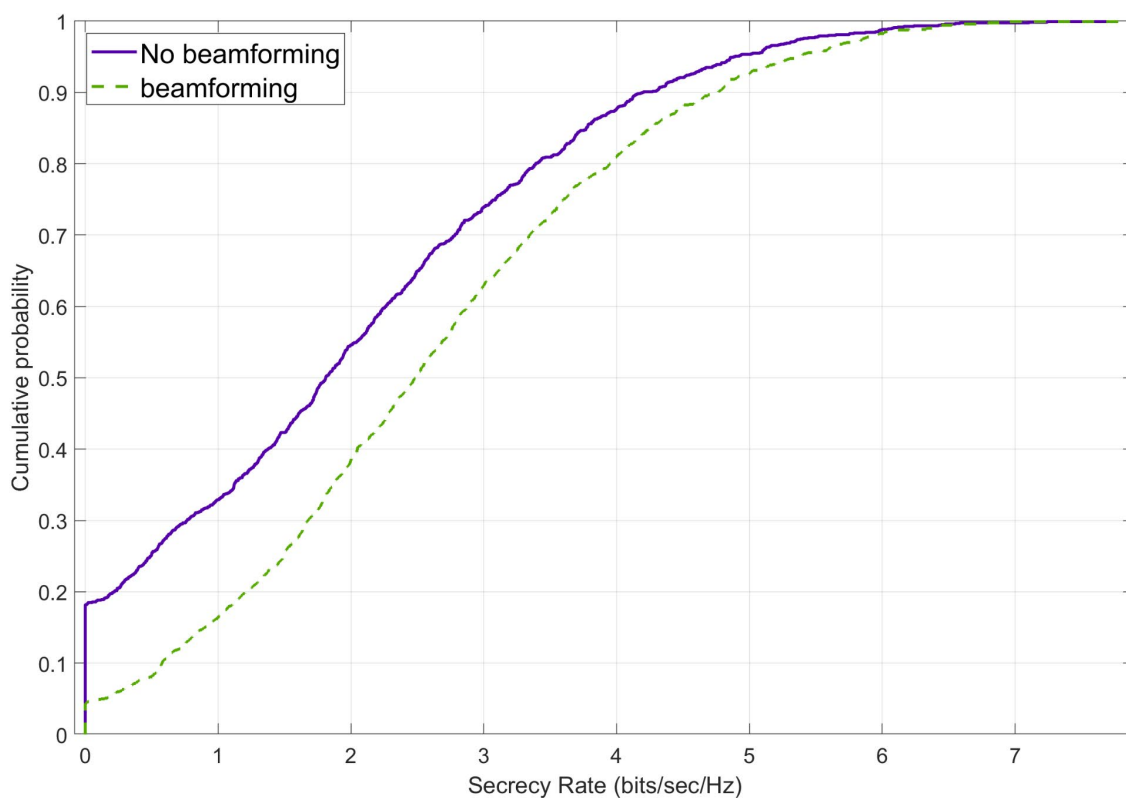
5.2.2 Ρυθμός Μυστικότητας

Σε αυτό το μέρος θα αναλύσουμε τον **Ρυθμό Μυστικότητας** τους συστήματος που δημιουργήσαμε. Αυτός αντιπροσωπεύει τον μέγιστο επιτεύξιμο ρυθμό δεδομένων μεταξύ του πομπού Alice και του Bob, διατηρώντας παράλληλα την εμπιστευτικότητα των μεταδιδόμενων πληροφοριών, από τις υποκλοπές της Eve και υπολογίζεται πρακτικά από τη διαφορά του

Ρυθμού (ή της χωρητικότητας) Alice-Bob με τον Ρυθμό (ή την χωρητικότητα) Alice-Eve. Στο πείραμα μας παρουσιάζεται ο Ρυθμός Μυστικότητας με τον οποίο μπορεί να μεταδοθεί ασφαλής πληροφορία ανά δευτερόλεπτο για κάθε Hertz εύρους ζώνης. Ένας υψηλότερος ρυθμός μυστικότητας είναι επιθυμητός, καθώς υποδηλώνει ότι μπορεί να μεταδοθεί περισσότερη πληροφορία με ασφάλεια σε λιγότερο χρόνο.

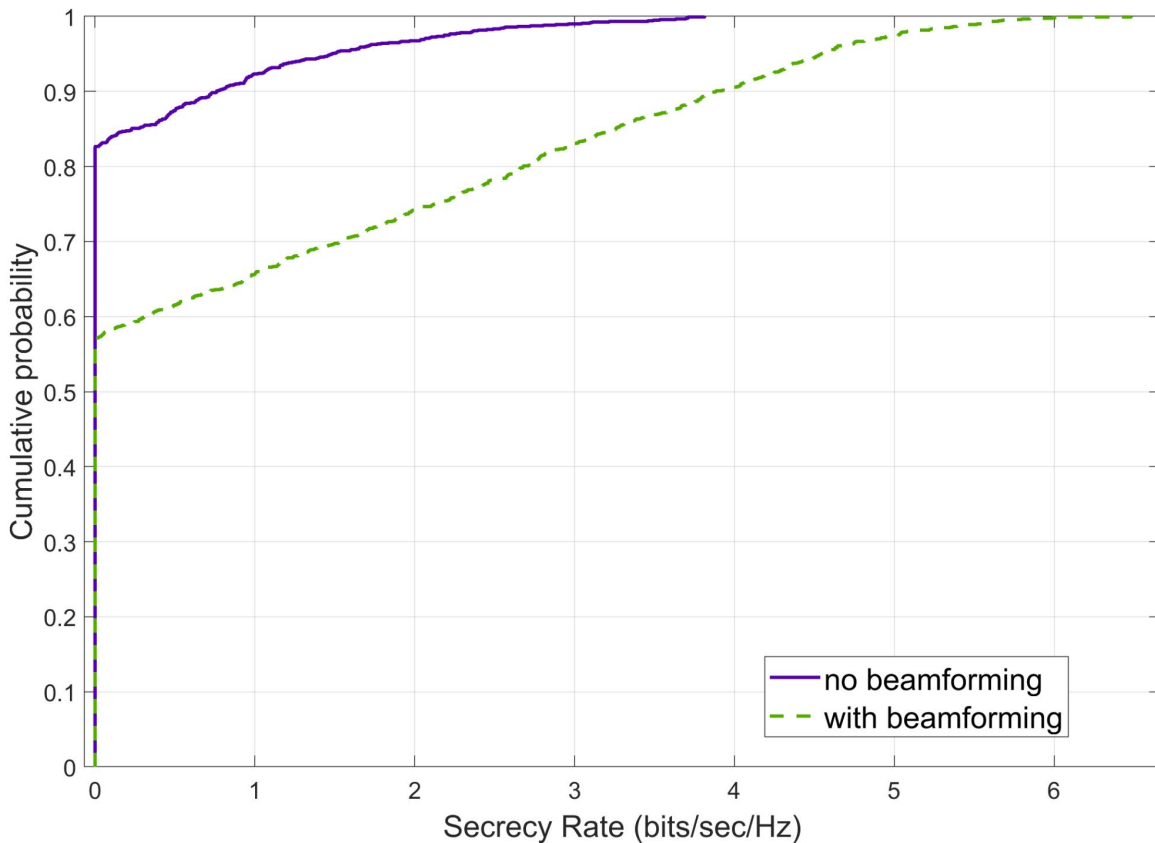
Ο κάθετος άξονας δείχνει τη συσσωρευτική πιθανότητα, που μπορεί να θεωρηθεί ως η πιθανότητα ότι ο ρυθμός μυστικότητας είναι μικρότερος ή ίσος με μια συγκεκριμένη τιμή.

Αρχικά μπορούμε να δούμε τον ρυθμό μυστικότητας που επιτυγχάνεται με τη χρήση Beamforming στο σενάριο 3 και τον ρυθμό διάδοσης του σήματος στο σενάριο 1, δηλαδή τη περίπτωση χωρίς Beamforming με τον Bob να βρίσκεται πιο κοντά στην Alice σε σύγκριση με την Eve. Παρατηρείται όπως είναι αναμενόμενο ότι μεγαλύτερος ρυθμός μετάδοσης δεδομένων με μυστικότητα είναι στην περίπτωση με Beamforming.



Εικόνα 5-21: Αποτελέσματα Ρυθμού Μυστικότητας του Bob, για τα Σενάρια 1 & 3

Στη περίπτωση που η Eve είναι πιο κοντά στην Alice, σχετικά με τον Bob, η διαφορά του ρυθμού μυστικότητας με Beamforming είναι ακόμα πιο μεγάλη.



Εικόνα 5-22: Αποτελέσματα Ρυθμού Μυστικότητας του Bob, για τα Σενάρια 2 & 4

Σε οποιαδήποτε δεδομένη τιμή συσσωρευτικής πιθανότητας, ο ρυθμός απορρήτου με beamforming είναι γενικά υψηλότερος από αυτόν χωρίς beamforming. Ειδικά στην περίπτωση των σεναρίων με τον Bob εγγύτερα στην Alice, υπάρχει αυξημένος Ρυθμός Μυστικότητας.

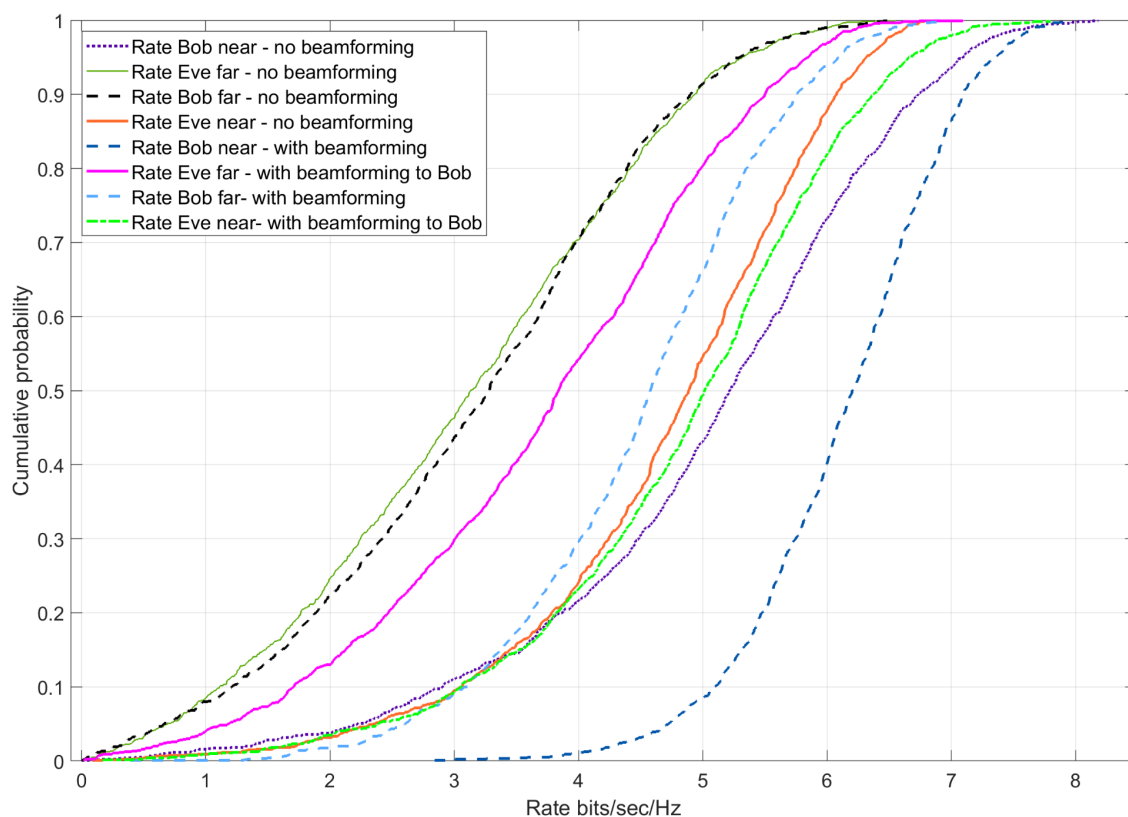
Αμφότερα τα γραφήματα υπογραμμίζουν το πλεονέκτημα της χρήσης beamforming όσον αφορά τη βελτίωση του ρυθμού απορρήτου όπως ήταν το αναμενόμενο.

Στον ακόλουθο πίνακα, εμφανίζεται και το ποσοστό «διακοπής μυστικότητας» (secrecy outage), δηλαδή το ποσοστό των περιπτώσεων που η μυστικότητα είναι μηδενική.

Πίνακας 5-1: Διακοπή μυστικότητας ανά περίπτωση

No beamforming – Bob Near	18%
No beamforming – Eve Near	80.6%
With beamforming – Bob Near	5.3%
With beamforming – Eve Near	61%

Στην Εικόνα 5-23, γίνεται μια συνολική παρουσίαση του Ρυθμού Μυστικότητας, αυτή τη φορά μπορούμε να συγκρίνουμε αναλυτικά τις επιδόσεις του Beamforming ανά δέκτη.



Εικόνα 5-23: Συγκριτικά Αποτελέσματα Ρυθμού Μετάδοσης, για όλα τα Σενάρια

Παρατηρώντας το παραπάνω Γράφημα, μπορούμε να συμπεράνουμε τα εξής:

1. Μέσω του Beamforming βελτιώνεται γενικά ο ρυθμός μετάδοσης για τον Bob.
2. Ο Bob στην κοντινή απόσταση έχει υψηλότερους ρυθμούς μετάδοσης σε σύγκριση με τον Bob στην μακρινή απόσταση.
3. Η Eve δείχνει παρόμοια συμπεριφορά, ωστόσο, υπάρχουν ορισμένες διαφοροποιήσεις, δεν έχει ανάλογη αύξηση όταν υλοποιείται το Beamforming. Αυτό μάλιστα οφείλεται ότι βρίσκεται και αρκετά κοντά με τον Bob. Σε άλλη περίπτωση που βρισκόταν σε πολύ διαφορετική διεύθυνση η απώλεια στο σήμα θα ήταν μεγαλύτερη.
4. Είναι ενδιαφέρον να παρατηρήσουμε ότι ο "Eve", ακόμη και όταν το "beamforming" εφαρμόζεται προς τον "Bob", εξακολουθεί να έχει έναν σχετικά υψηλό ρυθμό μετάδοσης, γεγονός που μπορεί να θεωρηθεί ως ενδείξεις για θέματα ασφάλειας ή παρεμβολές.

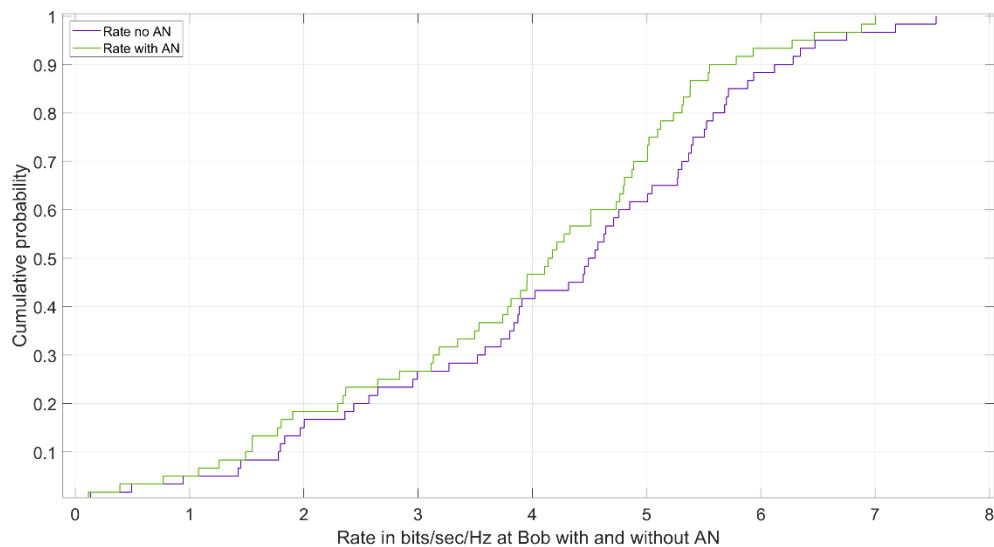
Σε γενικές γραμμές, αυτό το γράφημα μπορεί να χρησιμεύσει ως βάση για τη βελτίωση της τεχνικής του "beamforming", της απόδοσης των δεκτών και την αντιμετώπιση προκλήσεων που σχετίζονται με την ασφάλεια και τις παρεμβολές στο σύστημα επικοινωνίας.

Όσον αφορά τον πειραματισμό με την χρήση Artificial Noise, πραγματοποιήθηκαν δοκιμές όπου η Alice συνδέθηκε με USRP X310 (2 κεραίες), ο Bob με USRP B210 (2 κεραίες) και η Eve με USRP B200mini (1 κεραία).

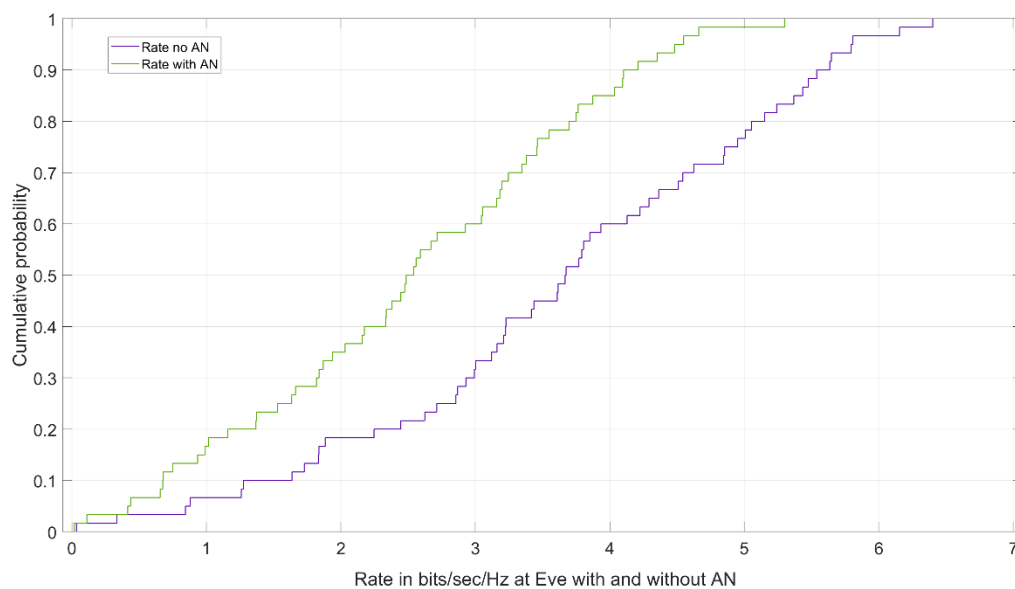
Λόγω των συνθηκών της μέτρησης με τον Bob και την Eve σε κοντινή απόσταση, δεν προέκυψαν πολλά αποτελέσματα για χρήση AN. Όπως ειπώθηκε, σε κάθε βήμα γινόταν έλεγχος του SVD και αν η μεγαλύτερη ιδιάζουσα τιμή ξεπερνούσε κατά 20 φορές την μικρότερη (13 dB), τότε επιλεγόταν η τεχνική του AN. Κατά τα πειράματα, αυτό πραγματοποιήθηκε λίγες φορές και τα αποτελέσματα δεν είναι τόσο αντιπροσωπευτικά.

Παρόλα αυτά παρατηρείται, ότι με την εφαρμογή της τεχνικής AN, ο σηματοθορυβικός λόγος και κατά συνέπεια ο ρυθμός στην Eve λαμβάνει ένα σημαντικό χτύπημα με μια μέση πτώση rate που ξεπερνά το 1 bit/sec/Hz. Ο Bob δεν επηρεάζεται από την άλλη ιδιαίτερα. Υπάρχει

πτώση αλλά σχετικά ανεπαίσθητη. Αυτό θα έχει τον αντίστοιχο αντίκτυπο στην χωρητικότητα μυστικότητας.



Εικόνα 5-24: Ρυθμός μετάδοσης Bob πριν και μετά την εφαρμογή AN



Εικόνα 5-25: Ρυθμός μετάδοσης Eve πριν και μετά την εφαρμογή AN

6

Συμπεράσματα

Από το πειραματικό μέρος της εργασίας μπορούμε με ασφάλεια να συμπεράνουμε ότι είναι εφικτό να υπάρξει ασφαλής επικοινωνία μεταξύ 2 μερών με τη χρήση Beamforming στην OFDM. Αυτό, μάλιστα μπορεί να επιτευχθεί ακόμα και όταν ο υποκλοπέας βρίσκεται σε πλεονεκτική θέση εν συγκρίσει με τον νόμιμο αποδέκτη (όντας κοντινότερα στον πομπό) χωρίς όμως κάποιο πρωτόκολλο κρυπτογράφησης. Επίσης μέσω του συνδυασμού OFDM με το Beamforming, μπορεί να επιτευχθεί ακόμα υψηλότερος ρυθμός μετάδοσης δεδομένων καθώς και η πλήρης ακεραιότητα των δεδομένων.

Το αποτέλεσμα των πειραμάτων που διεξήχθησαν σε αυτή την εργασία, επιβεβαιώνουν τα μαθηματικά μοντέλα πάνω στα οποία στηρίζονται οι θεωρίες της Ασφάλειας στο Φυσικό για μυστικότητα και ασφάλεια επικοινωνίας μέσω Beamforming.

7

Βιβλιογραφία

- [1] Antennas and Propagation for Wireless Communication Systems, Sonders Simon, Aragon-Zabal Alejanthro
- [2] Antenna Theory: Analysis and Design, Constantine A. Balanis
- [3] Electromagnetic Waves and Radiating Systems, Edward C. Jordan & Keith G. Balmain
- [4] Radar Absorbing Materials: From Theory to Design and Characterization, R.M. Jha
- [5] Wireless Communications, Andrea Goldsmith
- [6] Digital Communications, John G. Proakis and Masoud Salehi
- [7] Securing the IEEE 802.16 OFDM WiMAX PHYSICAL AND MAC Layer Using STBC Coding and Encryption
- [8] "Radio Wave Propagation: Concepts and Applications, Michael Marcus
- [9] "OFDM for Wireless Multimedia Communications, Richard Van Nee and Ramjee Prasad.
- [10] Peak-to-Average Power Ratio Reduction of OFDM Signals using Signal Space Diversity, Mark Fimoff.
- [11] Physical Layer Security for MIMO Wireless Systems, Joseph R. Childress
- [12] Physical-Layer Security From Information Theory to Security Engineering, Matthieu Bloch, Joao Barros.
- [13] Implementation of OFDM systems using GNU Radio and USRP, Duc Toan Nguyen
- [14] srsLTE: An Open-Source Platform for LTE Evolution and Experimentation, Ismael, Gomez-Miguel, Andres Garcia-Saavedra, Paul D. Sutton, Pablo Serrano, Cristina Cano, Douglas J. Leit