ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΨΗΦΙΑΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΔΙΚΤΥΑ»

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Software Defined Radios και υλοποίηση τεχνικών ασφαλείας φυσικού στρώματος»

Νικόλαος Γ. Σιαφάκας
Α.Μ.: ΜΨΕ2009

Επιβλέπων Καθηγητής:
Δρ. Κωνσταντίνος Μαλιάτσος

ΠΕΙΡΑΙΑΣ

Φεβρουάριος 2023

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία εκπονήθηκε στα πλαίσια ολοκλήρωσης του ΠΜΣ «Ψηφιακές Επικοινωνίες και Δίκτυα» του Πανεπιστημίου Πειραιώς, με σκοπό τη μελέτη της εφαρμογής της νέας τεχνολογία του Software Defined Radio στην υλοποίηση τεχνικών ασφαλείας φυσικού επιπέδου.

Στο 1^{ο} Κεφάλαιο της εργασίας γίνεται μια γενική εισαγωγή και περιγράφεται σύντομα η εξέλιξη των ασύρματων επικοινωνιών με σκοπό να γίνουν σαφείς στον αναγνώστη οι σύγχρονες ανάγκες που οδήγησαν στην ανάπτυξη της τεχνολογίας αυτής, αλλά και στο να διαφανεί ο σημαντικός ρόλος που θα παίξει στο εγγύς μέλλον.

Στη συνέχεια στο 2^{ο} Κεφάλαιο, παρουσιάζεται αναλυτικά το USRP N210 της Ettus Research, το οποία ήταν διαθέσιμα για την εκπόνηση της εργασίας και περιγράφονται οι δυνατότητες αλλά και οι περιορισμοί αυτού.

Στα Κεφάλαια 3 και 4 αναλύονται οι έννοιες της ασφάλειας επικοινωνιών υπό το γενικότερο πλαίσιο και η ασφάλεια φυσικού επιπέδου, ενώ στο Κεφάλαιο 5 γίνεται ανάλυση μερικών από τις τεχνικές ασφαλείας του φυσικού επιπέδου.

Στο 3^{ο} Κεφάλαιο της εργασίας γίνεται μια περιγραφή του ανοιχτού λογισμικού GNURadio αλλά και του προγράμματος GNURadio Companion, μέσω του οποίου αναπτύσσονται real-time εφαρμογές Software Defined Radio.

Στο κεφάλαιο 6 γίνεται εισαγωγή στο GNURadio και αναλύονται οι βασικές παραμετροποιήσεις αυτού, ενώ στο Κεφάλαιο 7 γίνεται υλοποίηση δύο πομποδεκτών σε GNURadio, QAM και OFDM.

Τέλος, η πτυχιακή εργασία κλείνει στο Κεφάλαιο 8 με διαπιστώσεις-συμπεράσματα που προέκυψαν από την εκπόνησή της αλλά και με προτάσεις για μελλοντικές εργασίες και πιθανές χρήσεις του Software Defined Radio σε τεχνικές υλοποίησης φυσικής ασφάλειας.

Λέξεις Κλειδιά: Software Defined Radio, SDR, GRC, USRP, N210, Ettus Research, πομποδέκτης, Matlab, LabView, Bandwidth, QAM, GFSK, PSK, δέκτης, FM ραδιοφωνία, cognitive radio, constellation, FFT Sink, Ασφάλεια Φυσικού Στρώματος, PLS, Ασφάλεια Επικοινωνιών, Κρυπτογραφία, Συστήματα MIMO

ABSTRACT

This thesis elaborated within the framework of completion of University of Piraeus Postgraduate program «Digital Communications and Networks» in order to study the utilization of the upcoming technology of Software Defined Radio in the implementation of physical layer security techniques.

In the first part of thesis a general introduction and a briefly description of the evolution of wireless communications take place, in order for the reader to understand the reasons and motivations that lead to the development of this technology but also make clear the important role that this technology will play in communications field in the near future.

Subsequently, an analytically introduction to Ettus Research's USRP N210 is given, which recently obtained from the labs of School of Telecommunications and Electronics of Signals Officers and capabilities and restrictions of the device are given.

In next two chapters an analysis of information security and physical layer security is taking place, while in chapter 5 the reader will find an attend of furthermore analysis of some physical layer's techniques.

In Chapter 6 of thesis a description of open source software GNURadio and program GNURadio Companion, which is a program to envelope real time applications, is given, while in chapter 7 is taking place the implementation of two kinds of transmitters, those of QAM and OFDM.

Finally, this thesis ends with conclusions that came through the elaboration but also with suggestions for future work and possible use of Software Defined Radios in the implementation of physical layer' s security techniques.

Keywords: Software Defined Radio, SDR, GRC, USRP, N210, Ettus Research, transmitter, Matlab, LabView, Bandwidth, QAM, GFSK, PSK, δέκτης, FM radio, cognitive radio, constellation, FFT Sink, Physical Layer Security, PLS, Communications Security, Cryptography, MIMO Systems

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω στο σύνολό τους, τους καθηγητές του ΠΜΣ «Ψηφιακές Επικοινωνίες και Δίκτυα», με την καθοδήγηση των οποίων και παρά τις δυσκολίες της φοίτησης λόγω των μέτρων πρόληψης κατά της πανδημίας του ιού COVID-19, οι σπουδαστές εκτιμώ ότι αποκομίσαμε σημαντικά εφόδια και εμπειρίες για τη συνέχιση της ενασχόλησή μας με τον τομέα των τηλεπικοινωνιών. Ιδιαιτέρως θα ήθελα να ευχαριστήσω τον καθηγητή κ. Κωνσταντίνο Μαλιάτσο για την αμέριστη βοήθεια που μου προσέφερε και την προθυμία του να με καθοδηγήσει σε όλα τα προβλήματα που συνάντησα κατά την εκπόνηση της εργασίας. Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου, για τη στήριξή της σε όλες τις δυσκολίες της ζωής μου, τη σύντροφό μου και συνοδοιπόρο της ζωής μου Βικτώρια που πάντα είναι στο πλάι μου και με υπομένει και πάνω από όλα το Θεό, που με αξίωσε να παρακολουθήσω το υπόψη ΠΜΣ και να διευρύνω τους ορίζοντές μου στον σύγχρονο χαοτικό πεδίο των επικοινωνιών.

ΠΕΡΙΕΧΟΜΕΝΑ ΠΙΝΑΚΩΝ	**ΣΕΛ.**
Πίνακας 2.1.2: Προσφερόμενα USRP της ETTUS……	
Πίνακας 2.1.3: Bandwidth θυγατρικών καρτών USRP της ETTUS…….	
Πίνακας 2.1.4: Bandwidth μητρικών καρτών USRP της ETTUS……	
Πίνακας 2.1.5: Τα διάφορα υποστηριζόμενα interfaces των USRP της ETTUS…….	
Πίνακας 2.3.1: Χαρακτηριστικά USRP N210……..	

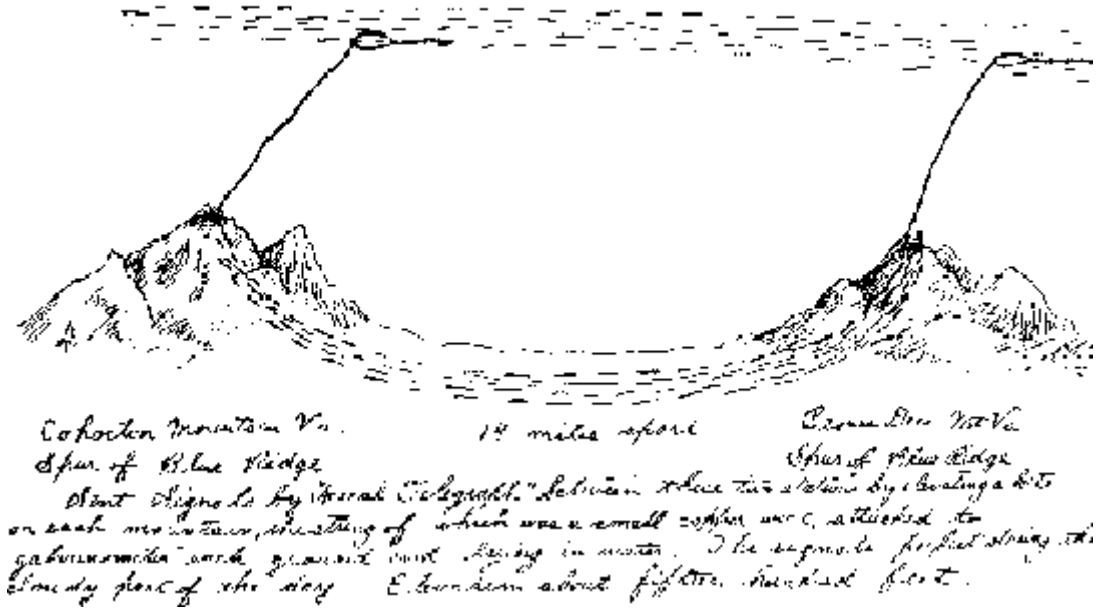
1. ΕΙΣΑΓΩΓΗ

1.1 Η/Μ κύμα - η ανακάλυψη ενός νέου αόρατου κόσμου

Ήταν το πρώτο μισό του 18ου αιώνα όταν εξελίξεις πηγάζουσες από την αλματώδη βιομηχανική επανάσταση διαμόρφωναν ένα νέο πρίσμα υπό το οποίο ο άνθρωπος θα προσπαθούσε να ερμηνεύσει τα φυσικά φαινόμενα και να θέσει την συνεχώς αναπτυσσόμενη τεχνολογία στην υπηρεσία της ανθρωπότητας, ψάχνοντας νέους, πρωτόγνωρους και άγνωστους έως τότε τρόπους. Την εποχή αυτή, μεγάλοι πατέρες όχι μόνο των τηλεπικοινωνιών αλλά και των θετικών επιστημών γενικότερα διατύπωναν θεμελιώδεις νόμους, πειραματικούς ή θεωρητικούς και έθεταν την πρόκληση προς την τεκμηρίωσή τους μέσω των νέων, καινοτόμων για την εποχή τεχνολογιών.

Το 1864, ο πατέρας της ενοποιημένης θεωρίας του ηλεκτρομαγνητισμού, Σκώτος Φυσικός James Clerk Maxwell έδειξε σε θεωρητικό αλλά και μαθηματικό επίπεδο ότι τα ηλεκτρομαγνητικά κύματα μπορούν να διαδοθούν στον ελεύθερο χώρο [1].

Το 1866, ο Majlon Loomis, Αμερικανός οδοντίατρος επέδειξε επιτυχώς την «ασύρματη τηλεγραφία» με τη βοήθεια χαρταετών στη θέση κεραιών, ενώ την κα-



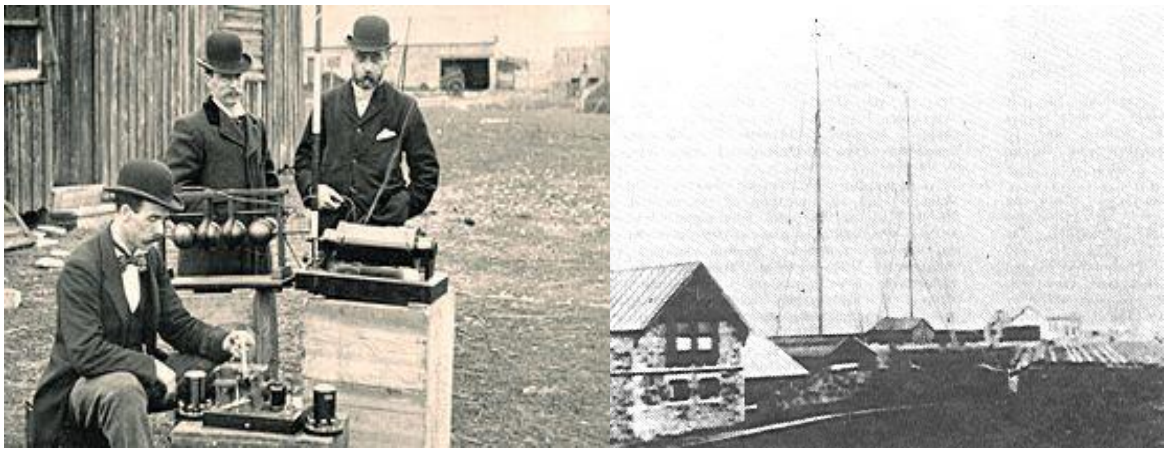
Εικόνα 1.1.1

τοχύρωση της πρώτης ασύρματης εκπομπής πέτυχε 30 χρόνια αργότερα ο Gulielmo Marconi, Ιταλός εφευρέτης [3].

Ο Marconi έστειλε και έλαβε το πρώτο ραδιοσήμα στην Ιταλία το 1895. Το 1902 έστειλε το πρώτο ασύρματο σήμα, το γράμμα «S» από την Αγγλία στο

Newfoundland. Ηταν το πρώτο διατλαντικό μήνυμα ραδιοτηλέγραφου σε συνολική απόσταση περίπου 1700 μιλίων.

Εν τω μεταξύ το 1886 ο Γερμανός φυσικός Heinrich Rudolf Hertz, ήταν ικανός να αποδείξει πειραματικά τη θεωρία του Maxwell επιδεικνύοντας ότι γρήγορες εναλλαγές στο ηλεκτρικό ρεύμα θα μπορούσαν να εκπεμφθούν στον αέρα σαν ραδιοκύματα όμοια με αυτά του φωτός [3].



Εικόνα 1.1.2

Συγχρόνως με τον Marconi ένας άλλος λαμπρός επιστήμονας και μεγάλος εφευρέτης, ο Σέρβος Nikola Tesla, έβγαλε δικές του πατέντες για ραδιοπομπούς εστιασμένες βέβαια προς την κατεύθυνση του διακαούς πόθου του, την ενέργεια και την ασύρματη και δωρεάν διανομή αυτής σε όλη την υφήλιο.

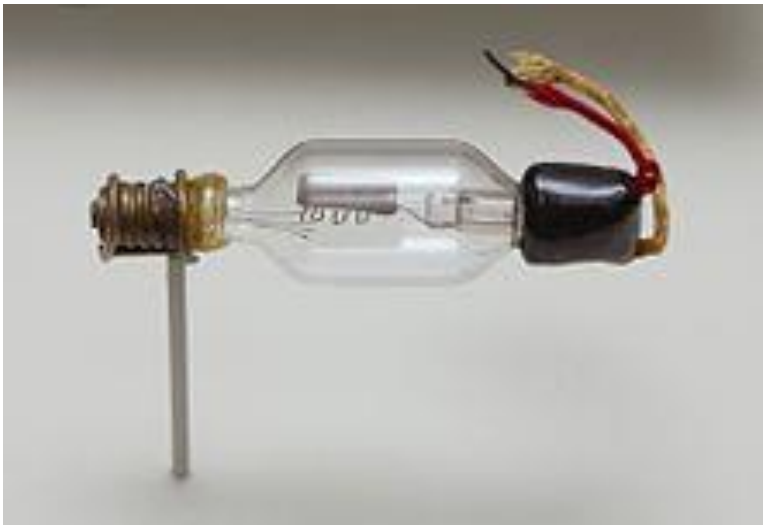
1.2 Η εξέλιξη των ασύρματων επικοινωνιών

Η μετουσίωση των ασύρματων επικοινωνιών από επικοινωνίες ραδιοτηλεγραφίας σε φωνής έγινε αργά. Η ραδιοτηλεγραφία είναι αποστολή μέσω ραδιοκυμάτων των ίδιων ακριβώς μηνυμάτων που αποστέλλονται και με τον κανονικό τηλέγραφο, δηλαδή τελείες και παύλες σε λογική ακολουθία. Η ραδιοτηλεγραφία αρχικά χρησιμοποιήθηκε για επικοινωνίες πλοίων. Το 1905 οι αναφορές της ρωσοϊαπωνικής ναυμαχίας στο Port Arthur μεταδόθηκαν για πρώτη φορά ασύρματα με ραδιοτηλεγραφία. Το 1905, ο Robert E. Peary, εξερευνητής της Ανταρκτικής μετέδωσε μέσω ραδιοτηλεγραφήματος το περίφημο: «Βρήκα τον Πόλο!».

Στη συνέχεια η εξέλιξη της ηλεκτρονικής και η αναδυόμενη ανάγκη για τη θεώρησή της ως ξεχωριστή επιστήμη από αυτή της φυσικής ήταν το γεγονός που άρχισε να δίνει τεράστια ώθηση προς την κατασκευή των πρώτων πομποδεκτών φωνής.

Η ανακάλυψη του τρίοδου ενισχυτή καθώς και του ανιχνευτή ηλεκτρομαγνητικής ακτινοβολίας από τον Lee De Forest έθεσαν σε νέα βάση τον τρόπο αντιμετώπισης του προβλήματος κατασκευής πομποδέκτη. Απαράμιλλη επίσης ήταν η συνεισφορά του στην κατασκευή λυχνιών κενού, αφού αυτός έθεσε τη βάση για τον ευρύτατα μετέπειτα αναπτυσσόμενο τομέα, ο οποίος ανθεί έως τις

μέρες μας, μέσω της κατασκευής της πρώτης τρίοδης ενισχύτριας λυχνίας κενού, του «Audion» [5]. Ο De Forest, μέσω της κατασκευής του ενισχυτή, κατάφερε να ενισχύσει τη συχνότητα που λάμβανε η κεραία προ της εφαρμογής της στον ανιχνευτή του δέκτη και έτσι ακόμα και αδύναμα σήματα μπορούσαν να ακουστούν. Χρησιμοποίησε πρώτος την ένοια «ασύρματος» και το αποτέλεσμα της εργασίας του De Forest ήταν η κατασκευή των πρώτων πομποδεκτών ΑΜ για λειτουργία από πλήθος σταθμών ταυτόχρονα, γεγονός που από τους υπάρχοντες ραδιοτηλεγράφους δεν ήταν εφικτό να υλοποιηθεί.



Εικόνα 1.2.1

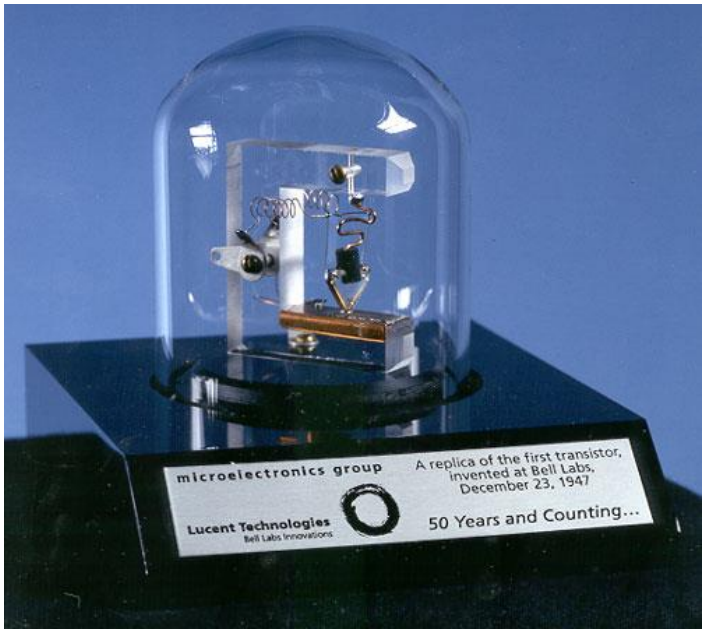
Η ραδιοφωνία ΑΜ ήταν εδώ και ήταν γεγονός. Εγκαινιάστηκε το 1920, όταν ο ραδιοσταθμός KDKA του Pittsburg εξέπεμψε για πρώτη φορά. Από τούδε καιξής η ραδιοφωνία ΑΜ θα γνώριζε τεράστια άνθηση στις ΗΠΑ αλλά και σε όλο τον άλλο κόσμο.

Στη συνέχεια ο Καναδός Reginald A.Fessenden εισήγαγε την έννοια της διαμόρφωσης και την «υπερετερώδυνη αρχή», η οποία επιτρέπει τη λήψη και εκπομπή στο ίδιο μέσο χωρίς αλληλοπαρεμβολή.

Άλλη μια μεγάλη προσωπικότητα που έθεσε την προσφορά του στις ασύρματες τηλεπικοινωνίες ήταν ο Edwin Howard Armstrong, ο οποίος το 1933 κατασκεύασε και επέδειξε το πρώτο σύστημα επικοινωνίας FM, το οποίο παρείχε σαφώς βελτιωμένη απόδοση σε σχέση με τη διαμόρφωση ΑΜ από την πλευρά διαχείρισης του θορύβου.

Το πρώτο σύστημα τηλεόρασης κατασκευάστηκε στις ΗΠΑ από τον V.K.Zworykin και επιδείχθηκε το 1929. Η εμπορική εκπομπή τηλεόρασης άρχισε στο Λονδίνο από το BBC και το ημερολόγιο έδειχνε τότε 2 Νοεμβρίου 1936. Πέντε χρόνια αργότερα η FCC έδωσε έγκριση τηλεοπτικής εκπομπής στις ΗΠΑ.

Το τεράστιο άλμα στην εξέλιξη της μικροηλεκτρονικής και κατά συνέπεια των ασύρματων τηλεπικοινωνιών ήρθε το 1947 με την ανακοίνωση της κατασκευής του πρώτου transistor από τους Walter Brattain, John Bardeen, Robert Noyce των εργαστηρίων Bell [6].



Εικόνα 1.2.2

Από το σημείο αυτό και μετέπειτα η εικόνα των πομποδεκτών έμελλε να αλλάξει κατά ριζικό τρόπο και θα διατηρούσε τις βασικές αυτές αλλαγές για πολύ μεγάλο διάστημα, έως τις μέρες μας, με σαφείς βελτιώσεις στην τεχνολογία των υλικών κατασκευής μέσω εισαγωγής νέων, πιο αξιόπιστων αλλά και ακριβέστερων μεθόδων κατασκευής με ταυτόχρονο υποβιβασμό της κλίμακας κατασκευής.

Το 1954, μια τότε μικρή εταιρία στην Ιαπωνία, η Sony, παρουσίασε τον πρώτο ασύρματο με transistor. Από την πρώτη παρουσίαση αυτή του ασύρματου με transistor έως σήμερα, ελάχιστα έχουν αλλάξει από τη γενική φιλοσοφία δομής του, πλην όμως τεράστιες αλλαγές σημειώθηκαν σε επιμέρους χαρακτηριστικά του ως αποτέλεσμα των παρακάτω συνισταμένων:

α. Η τεχνολογία των υλικών και η έρευνα για νέα πιο εξωτικά υλικά ποτέ δε σταμάτησε, με αποτέλεσμα την διαρκή αύξηση της ποιότητας κατασκευής και τη χρήση υλικών που πλησιάζουν τα όρια του ιδανικού για κάθε επιμέρους λειτουργία που θα επιθυμούσαμε.

β. Η κλίμακα κατασκευής των transistor και κατ’ επέκταση η κλίμακα ολοκλήρωσης αυτών μίκραινε διαρκώς με την πάροδο του χρόνου επιτρέποντας υφιστάμενες λειτουργίες με τεράστια επεξεργαστική ισχύ πλέον σε μέγεθος τσέπης. Στην αυγή της νέας χιλιετίας πλέον η δυνατότητα ολοκλήρωσης σε ακόμα μικρότερο επίπεδο έφτασε το υλικό στα όριά του, με αποτέλεσμα σήμερα να αναζητούνται άλλες μέθοδοι αύξησης της επεξεργαστικής ισχύος.

γ. Ο σχεδιασμός και η δοκιμαστική λειτουργία των επιμέρους δομικών μονάδων των πομποδεκτών με τη βοήθεια υπολογιστών έδωσε τη δυνατότητα στους μηχανικούς να τελειοποιήσουν και να μοντελοποιήσουν τις δομικές αυτές μονάδες με αποτέλεσμα να μπορούν να κατασκευάσουν το τελικό προϊόν διαμορφωμένο σύμφωνα με τις ανάγκες του εκάστοτε χρήστη.

δ. Η ανάγκη για εξοικονόμηση ενέργειας και ελάττωση της εκπεμπόμενης ακτινοβολίας έκανε πιο απαιτητικές τις δομικές αυτές μονάδες από την πλευρά του ισοζυγίου ενέργειας. Νέα υλικά και τεχνολογίες εισήχθησαν, λιγότερο ενεργειακά δαπανηρές και περισσότερο έξυπνες στη διαχείριση της κατανάλωσης.

ε. Η ψηφιακή εποχή που ανέτειλε στο τέλος του πρώτου μισού του εικοστού αιώνα και ακόμα και σήμερα είναι σε διαρκή ζύμωση, έμελλε επίσης να αλλάξει τον τρόπο κατασκευής των πομποδεκτών, όχι ως προς τις αρχικές λειτουργίες τους αλλά προσθέτοντας νέες δομικές μονάδες. Οι εργασίες των Nyquist (1924), Hartley (1928), Wiener (1942), Kotelnikov (1947), Shannon (1948) και Hamming (1950) είναι αυτές που έθεσαν τα θεμέλια των σύγχρονων συστημάτων επικοινωνιών. Πλέον πάνω στις ίδιες βασικές αρχές ασύρματης μετάδοσης του κλασσικού πομποδέκτη η πληροφορία κρυπτογραφείται, πολυπλέκεται, κωδικοποιείται, αντιστοιχίζεται σε σύμβολα και τελικώς με αναλογική μορφή στέλνεται στον έξω κόσμο για να ακολουθήσει η αντίστροφη διαδικασία στο δέκτη. Η νέα εποχή έφερε τη δυνατότητα προσαρμοστικής διαμόρφωσης, της εισαγωγής δηλαδή στοιχειώδους «εξυπνάδας» στους ίδιους τους πομποδέκτες, η οποία τους παρέχει αυτόματα τη δυνατότητα να μεταβάλλουν τη λειτουργία των επιμέρους δομικών μονάδων τους ώστε να προσαρμοστούν σε θορυβώδη περιβάλλοντα παρέχοντας πάντα στο χρήστη μια ελάχιστη εγγυημένη ποιότητα υπηρεσίας [9].

στ. Η ανάγκη για τηλεπικοινωνιακή κάλυψη των πιο απομακρυσμένων περιοχών της υφηλίου καθώς και η κατάκτηση του διαστήματος έφερε στο φως την ανάγκη για κατασκευή κάποιων από τις πιο τεχνολογικά εξελιγμένες κατασκευές που θα επιχειρούσε ποτέ ο άνθρωπος, αυτές των τηλεπικοινωνιακών δορυφόρων.

Και αυτά που αναφέρθηκαν πιο πάνω, είναι μόνο μερικά από τα χαρακτηριστικά που προσέδωσαν στις ασύρματες τηλεπικοινωνίες τη σημερινή τους μορφή, μέσα από μια διαρκή αλληλεπίδραση και ανατροφοδότηση των αποτελεσμάτων του ενός τομέα των Θετικών Επιστημών στον άλλο κ.λπ..

1.3 Η γέννηση των Software Defined Radios

Μέσα σε αυτή τη διαρκή τεχνολογική ζύμωση, η ανάγκη για ανταλλαγή πληροφορίας οποιασδήποτε μορφής και μάλιστα μεγάλου όγκου από οποιοδήποτε σημείο της γης προς οποιοδήποτε άλλο έφερε στο φως μια νέα απαίτηση. **Την απαίτηση για ένα καθολικό, ενοποιημένο σύστημα ασύρματων επικοινωνιών που θα μπορεί να κάνει χρήση σε πραγματικό χρόνο κάθε γνωστού πρωτοκόλλου ασύρματων επικοινωνιών και με δυνατότητα συντονισμού σε σχετικά μεγάλο εύρος ζώνης και κατόπιν απαίτησης του χρήστη ή όχι, ώστε να μπορεί να καλύψει επικοινωνίες από μερικά KHz έως αρκετά GHz**.

Εικόνα 1.3.1

Καθολικό και ενοποιημένο γιατί η γέννηση συνεχώς νέων πρωτοκόλλων επικοινωνίας από τη μία πλευρά εξυπηρετούσε μία συγκεκριμένη ανάγκη δίνοντας λύσεις σε εξεζητημένα προβλήματα, από την άλλη όμως έκανε το σύγχρονο πεδίο των τηλεπικοινωνιών πολύ σύνθετο, ιδιαίτερα στον τομέα των κινητών επικοινωνιών, των οποίων οι απαιτήσεις αλλάζουν κάθε λίγα χρόνια.

Να μπορεί να κάνει χρήση σε πραγματικό χρόνο κάθε γνωστού πρωτοκόλλου διότι αφενός παρουσιάζεται η ανάγκη προσαρμογής λόγω των εκάστοτε αναγκών του χρήστη και αφετέρου λόγω συνθηκών του περιβάλλοντος. Αυτό θα γίνεται με μέριμνα του χρήστη είτε αυτόματα, οπότε το νέο αυτό σύστημα θα πρέπει να διαθέτει ένα στοιχειώδη βαθμό ευφυΐας.

Να έχει δυνατότητα συντονισμού σε όσο το δυνατό μεγαλύτερο εύρος ζώνης ώστε η διαλειτουργικότητα να καλύπτει τα περισσότερα δυνατά ήδη ανεπτυγμένα πρωτόκολλα επικοινωνιών που υπάρχουν σήμερα σε υλικό. Αναδεικνύεται έτσι η ανάγκη για πιο ορθολογιστική διαχείριση και καταμερισμό του πολύτιμου φάσματος αλλά και πλήρη αξιοποίηση αυτού σε όλο το εύρος του.

Ο όρος «Software Radio» χρησιμοποιήθηκε για πρώτη φορά από την E-Systems, σημερινή Rytheon σε ένα εταιρικό newsletter της και αναφέρονταν σε ένα πρωτότυπο ψηφιακό δέκτη βασικής ζώνης, ο οποίος ήταν εφοδιασμένος με ένα array από επεξεργαστές το οποίο θα εκτελούσε προσαρμοστικό φιλτράρισμα προς ελαχιστοποίηση της παρεμβολών και αποδιαμόρφωση σημάτων βασικής ζώνης [8].

Το 1991 μέσω του DARPA του DoD των ΗΠΑ αναπτύχθηκε το πρόγραμμα SPEAKeasy, το οποίο καθόριζε την κατασκευή ασύρματου πομποδέκτη με το physical layer του ανεπτυγμένο σε λογισμικό. Ο πρωταρχικός στόχος, ο οποίος πήγαζε από τις απαιτήσεις της USAF, ήταν η ανάπτυξη ενός πομποδέκτη που θα υποστήριζε τουλάχιστον δέκα από τα υπάρχοντα στρατιωτικά πρωτόκολλα ασύρματης επικοινωνίας και θα μπορούσε να λειτουργήσει σε οποιαδήποτε περιοχή συχνοτήτων ανάμεσα στα 2 MHz και στα 2GHz. Ο δευτερεύων στόχος ήταν να ενσωματώνει τη δυνατότητα να υποστηρίζει και μελλοντικά πρωτόκολλα και διαμορφώσεις με κάποια αναβάθμιση. Μια αναλυτική περιγραφή από την περιγραφή σε ένα έγγραφο της DARPA είναι η εξής: «Το SPEAKeasy είναι μια προσπάθεια να κατασκευασθεί το PC στον ασύρματο κόσμο».

Το 1992 ο Joseph Mitola, δημοσιεύει ένα άρθρο για το Software Radio στο IEEE, το οποίο έχει τίτλο: «Software Radio: επισκόπηση, κριτική ανάλυση και μελλοντικές τάσεις». Για πολλούς θεωρείται ο πατέρας του Software Radio και αυτή η αναγνώριση ήρθε χάρη στη σημασία που έδωσε στον όρο «Software Radio» έναντι σε αυτόν της E-Systems, της οποίας το πρωτότυπο αναφερόταν μόνο σε δέκτες και όχι σε έναν ολοκληρωμένο πομποδέκτη. Αργότερα, το 1998 ο Mitola έδωσε τον ορισμό «Cognitive Radios» για εκείνους τους πομποδέκτες που επιτηρούν το φάσμα λειτουργίας τους και έχουν την απαραίτητη ευφυία ώστε να προσαρμόζονται σε αυτό όταν απαιτηθεί.

Το 1996 δημιουργείται η πρώτη βιομηχανική συνεργασία αφιερωμένη στο SDR υπό τον τίτλο «The Modular Multifunction Information Transfer System Forum – MMITS)». Το 1998 ο τίτλος της έγινε «SDR Forum» και το 2010 μετονομάστηκε σε «Wireless Innovation Forum». Στο forum συμμετείχαν άτομα και κυβερνητικοί οργανισμοί, καθώς επίσης και από τη βιομηχανία και την πανεπιστημιακή κοινότητα, όλοι καθοδηγούμενοι από το τις συναφείς με το SDR τεχνολογίες.

Το επόμενο χρονικά γεγονός στην εξέλιξη του SDR έλαβε χώρα όταν το DoD των ΗΠΑ δημιούργησε το 1997 το «Joint Tactical Radio System – JTRS», το οποίο σχεδιάζονταν να είναι το δίκτυο δεδομένων και φωνής νέας γεννιάς τουλάχιστον για τις δυνάμεις που επιχειρούν σε τακτικό επίπεδο. Δημιουργήθηκε για να αυξήσει την διαλειτουργικότητα και τη φορητότητα συγκεκριμένου αριθμού κυματομορφών (HAVE QUICK II, HF ALE, SINCGARS κτλ.) διαμέσω του αυστηρού καθορισμού και της παραμετρικοποίησης των διαφόρων επιπέδων και διεπαφών, η οποία αρχιτεκτονική έγινε γνωστή ως «Software Communication Architecture – SCA». Το JTRS, αρκετά μεγαλόπνοο ως σχέδιο, το 2011 ακυρώθηκε αφού κρίθηκε ότι απέτυχε στους στόχους του και έχοντας δαπανηθεί το ποσό των 15 δις δολαρίων κατά τις συντηρητικότερες εκτιμήσεις. Παρόλα αυτά, η τεχνογνωσία που αποκτήθηκε έθεσε τη βάση για περαιτέρω έρευνα και ανάπτυξη.

Το 1998 η Nutaq (τότε Lyrtech) σε συνεργασία με την MathWorks έθεσε τη βάση για τη δημιουργία του πρώτου περιβάλλοντος το οποίο θα μπορούσε να δημιουργήσει απευθείας εκτελέσιμα αρχεία από ένα μοντέλο του Simulink για ένα DSP της Texas Instruments και ένα FPGA της Xilinx. Προσπαθώντας να κάνουν πράξη αυτή την καινοτομία, οι ερευνητές ήρθαν αντιμέτωποι με μια μεγάλη δυσκολία: να γράψουν κώδικα για embedded processors. Οι υπομονάδες του DSP και του FPGA ήταν τοποθετημένες μαζί σε μια πλακέτα που λέγονταν SignalMaster. Διασυνδέονταν με ένα A/D και ένα D/A τμήμα και αποτελούσε ολόκληρη η συσκευή μία από τις πρώτες πλατφόρμες ανάπτυξης SDR για εργαστήρια κια πανεπιστήμια.

Τρία χρόνια μετά, το έτος 2001 και έχοντας την βάση του σε μια διεπαφή προερχόμενη από το MIT που ονομάζονταν PSpectra, ιδρύθηκε το GNU Radio από τον Eric Blossom και χρηματοδοτήθηκε από τον John Gilmore της Sun Microsystems. Το GNU Radio είναι μια open-source διεπαφή για την ανάπτυξη SDR εφαρμογών σε περιβάλλον PC. Με πάνω από 5.000 δηλωμένους χρήστες το 2012, είναι μακράν το πιο δημοφιλές εργαλείο ανάπτυξης SDR. Πλέον πλήρη πρότυπα για P25, 802.11, ZigBee, Bluetooth, RFID, DECT, GSM και ακόμα και για

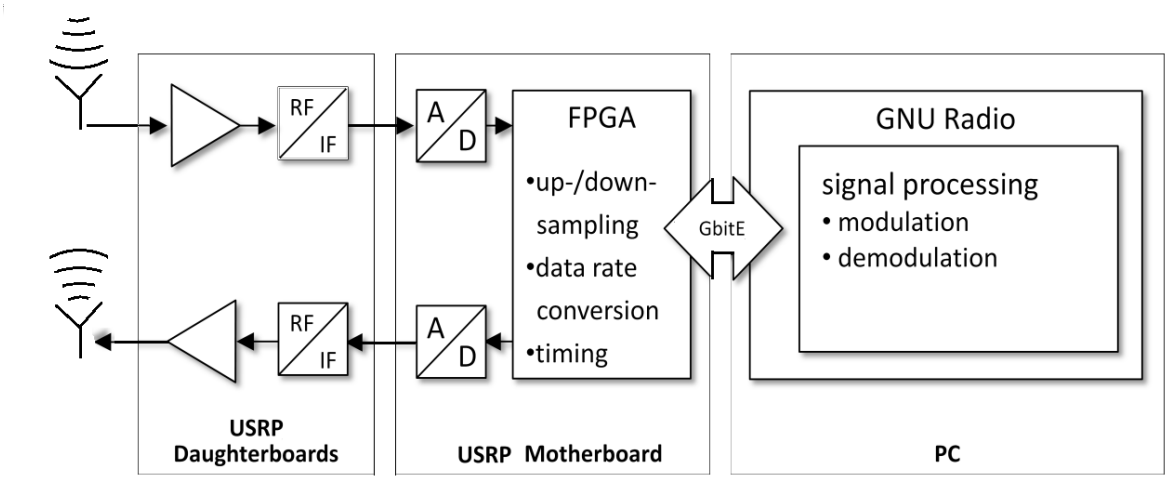
LTE είναι έτοιμα πακέτα μπορεί κάποιος απλά να τα κατεβάσει απευθείας και να τα χρησιμοποιήσει σε ένα σύστημα x86.

Το έτος 2006, δύο θεωρητικά μεγάλοι αντίπαλοι στον τομέα των ηλεκτρονικών, η Xilinx και η Texas Instruments ενώνουν τις δυνάμεις τους και με τη Nutaq για να κατασκευάσουν την πρώτη καθολικά ολοκληρωμένη, stand-alone πλατφόρμα ανάπτυξης SDR. Ήταν εφοδιασμένη με ένα ARM, έναν DSP και ένα FPGA και με ένα συντονιζόμενο front-end τμήμα RF με δυνατότητα συντονισμού από 200 MHz έως 1 GHz (τα επόμενα χρόνια εισήχθησαν τα διαφορετικά εύρη ζώνης). Η πλατφόρμα δεν ήταν μεγαλύτερη από ένα κουτί παπουτσιών και μπορούσε να τροφοδοτηθεί από μια μπαταρία, γεγονός που έθετε σε νέα βάση τις πιθανότητες για εκτός εργαστηρίου εφαρμογές και έρευνα.

1.4 Τι είναι τελικά το Software Defined Radio;

Μετά από την παραπάνω ιστορική αναδρομή και ανάλυση, εύλογα κάποιος θα αναρωτηθεί: «τί είναι λοιπόν το software defined radio και πως ορίζεται». Ένα σύνολο ορισμών μπορεί να δοθεί, ένας εκ των οποίων έρχεται απευθείας από το ίδιο το Wireless Innovation Forum [12]:

«ασύρματος στον οποίο κάποιο μέρος ή ολόκληρο το σύνολο των λειτουργιών του φυσικού επιπέδου εκτελούνται από λογισμικό»



Σχήμα 1.4.1

Ως ασύρματος δε θεωρείται μόνο ο κλασσικός ασύρματος πομποδέκτης στρατιωτικών ή παρόμοιων εμπορικκών εφαρμογών αλλά οποιαδήποτε συσκευή εκπέμπει ή λαμβάνει σήματα στην περιοχή των RF του ηλεκτρομαγνητικού φάσματος με σκοπό την διακίνηση πληροφορίας. Στο σημερινό κόσμο, ασύρματοι πομποδέκτες υπάρχουν σε διάφορες συσκευές όπως κινητά, Η/Υ, κλειδιά αυτόματου ανοίγματος θυρών, αυτοκίνητα, τηλεοράσεις, κ.λπ..

Οι παραδοσιακοί, υλοποιημένοι σε hardware ασύρματοι μπορούν να τροποποιηθούν με παρέμβαση μόνο στο υλικό τους. Αυτό έχει ως αποτέλεσμα υψηλό κόστος και μικρή ελαστικότητα στην υποστήριξη πολλαπλών πρωτοκόλλων

επικοινωνίας. Από την άλλη πλευρά, η τεχνολογία SDR προσφέρει μια αποδοτική και οικονομική λύση σε αυτό το πρόβλημα, επιτρέποντας τη λειτουργία με πολλούς διαφορετικούς τρόπους, σε πολλές διαφορετικές μπάντες και με δυνατότητα υλοποίησης πολλών διαφορετικών ασύρματων συσκευών σε λογισμικό.

Το SDR καθορίζει ένα σύνολο από τεχνολογίες υλικού και λογισμικού όπου κάποιες ή όλες από τις λειτουργίες ενός ασυρμάτου (οι οποίες επίσης απαντώνται υπό τον όρο «physical layer processing») υλοποιούνται με τη βοήθεια λογισμικού που δύναται να τροποποιηθεί ή firmware το οποίο λειτουργεί σε προγραμματιζόμενες διατάξεις επεξεργασίας. Οι συσκευές που κάνουν χρήση αυτής της τεχνολογίας περιλαμβάνουν FPGA's, DSP's, GPP's, programmable SoC's ή άλλες εφαρμογές. Η χρήση αυτών των τεχνολογιών μας επιτρέπει να προσδώσουμε νέες δυνατότητες στα υπάρχοντα συστήματα ασυρμάτων, χωρίς να υπάρξει απαίτηση για νέο υλικό.

1.5 Ένα πολλά υποσχόμενο μέλλον στις ασύρματες επικοινωνίες

Από το σημείο της δημιουργίας της πρώτης ολοκληρωμένης πλατφόρμας SDR και μετέπειτα οι εξελίξεις στον τομέα αναμένονται ραγδαίες καθώς παρόμοιες πλατφόρμες που άρχισαν να αναπτύσσονται από τη Microsoft, τη Datasoft, τη Nutaq αλλά και άλλες μεγάλες εταιρίες άρχισαν λόγω της φορητότητας να εισάγονται στα εκπαιδευτικά ιδρύματα για περαιτέρω έρευνα και ανάπτυξη. Αυτό, σε συνδυασμό με τη ραγδαία ανάπτυξη των FPGA's, την καρδιά κάθε πλατφόρμας SDR, αναμένεται να φέρει τεράστια αλλαγή στην εικόνα των ασύρματων πομποδεκτών όπως τους γνωρίζαμε έως σήμερα.

Η λογική του «ένα για όλα» αποτελεί έναν από τους πρωταρχικούς στόχους ανάπτυξης εφαρμογών σε SDR και σε αυτή τη χρονική συγκυρία είναι πιο απαραίτητη από ποτέ, καθώς η πολυπλοκότητα των πρωτοκόλλων επικοινωνιών έχει σιγά σιγά επιφέρει έναν κορεσμό στην ίδια τη διαχείρισή τους και αποτελεί έναν πραγματικό πονοκέφαλο για τον μηχανικό που πρέπει να σχεδιάσει διαλειτουργικά συστήματα. Το μεγάλο στοίχημα για την ανάπτυξη του SDR είναι κατά πόσο θα καταφέρει να κυριαρχήσει σε ολοένα και μεγαλύτερο τμήμα του φάσματος, καθώς ο υλικός περιορισμός του τμήματος front-end , δηλαδή του σταδίου RF, πάντα δηλώνει παρών ως μοναδική διέξοδος από το ψηφιακό λογισμικό προς τον αναλογικό κόσμο. Ήδη τα υπαρχοντα USRP της Ettus Research καλύπτουν εύρος ζώνης από μερικά KHz έως 6 GHz και αναμένεται περεταίρω αύξηση του εύρους αυτού.

Ιδιαίτερα για τις στρατιωτικές επικοινωνίες διαφαίνεται εδώ το τεράστιο όφελος και ο πρωταγωνιστικός ρόλος που αναμένεται να διαδραματίσει το SDR. Σε τακτικό επίπεδο, όπου ένας σταθμός επικοινωνίας υπάρχει απαίτηση να είναι ταυτόχρονα συνδεδεμένος σε διαφορετικά δίκτυα, διαφορετικών πρωτοκόλλων και σε τελείως διαφορετικές φασματικές περιοχές, έως σήμερα θα απαιτούσε την ύπαρξη ισάριθμων σταθμών ασυρμάτου. Αυτό ήρθε να αλλάξει η λογική του «ένα για όλα» και ο σκοπός φαίνεται σιγά σιγά να επιτυγχάνεται.

Η αποδοτικότητα του φάσματος αναμένεται να αυξηθεί καθώς η ανάπτυξη εφαρμογών σε SDR ακολουθεί το παράδειγμα του ABC – «Always Best Connected»[10] επιτρέποντας την αδιάλειπτη λειτουργία μεταξύ διαφορετικών

standards και πρωτοκόλλων όχι μόνο εντός μιας ξεχωριστής οικογένειας (π.χ. κυψελωτών επικοινωνιών) αλλά και μεταξύ διαφορετικών ιεραρχικών επιπέδων των διαφόρων συστημάτων (π.χ. δορυφόροι, επικοινωνίες κυψέλης, τοπικά δίκτυα και οικιακά δίκτυα). Το παραπάνω απαιτεί ένα τρόπο διαφορετικής θεώρησης του φάσματος και δυναμικής διαχείρισής του, κάτι που μέχρι σήμερα γίνονταν στατικά και κατά βάση με γεωγραφικούς περιορισμού. Η ανάπτυξη εφαρμογών σε SDR προσφέρει αυτόν ακριβώς τον ευέλικτο και δυναμικό τρόπο μετάπτωσης χωρίς κόστος σε υλικό, αφού όλα γίνονται στον ψηφιακό κόσμο με ταυτόχρονο επαναπρογραμματισμό του υλικού.

Πλέον των ανωτέρω χαρακτηριστικών που δείχνουν τη σπουδαιότητα των SDR, η τεχνολογία τους φαίνεται ότι μπορεί να δράσει σαν το κλειδί για μία σειρά από άλλες τεχνολογίες που έχουν τη βάση τους πάνω στον επαναπρογραμματισμό των πομποδεκτών και σήμερα συζητούνται ή έχουν αρχίσει ήδη να υλοποιούνται στον τομέα των ασύρματων επικοινωνιών.

Η τεχνολογία του SDR δεν είναι απαραίτητο να συμπεριλαμβάνει αυτές τις τεχνολογίες, αντίστροφα η ίδια η φιλοσοφία του SDR μπορεί να προσφέρει σε αυτές την κατάλληλη ευκαμψία ώστε να πετύχουν το στόχο τους, μειώνοντας το κόστος και αυξάνοντας παράλληλα την αποδοτικότητα του συστήματος. Οι τεχνολογίες αυτές, σε τρεις γενικές κατηγορίες είναι:

α. <u>Adaptive Radio</u>

Το adaptive radio είναι ασύρματη τεχνολογία στην οποία τα συστήματα επικοινωνιών έχουν τη δυνατότητα να παρακολουθούν διαρκώς την απόδοσή τους και να τροποποιούν ανάλογα τις παραμέτρους τους ώστε να βελτιώσουν την απόδοση αυτή. Η χρήση SDR σε ένα ασύρματο σύστημα adaptive radio θα προσέφερε περισσότερους βαθμούς ελευθερίας στην προσαρμοστικότητα και κατ' επέκταση υψηλότερα επίπεδα απόδοσης και καλύτερη παρεχόμενη ποιότητα υπηρεσίας σε μία ασύρματη ζεύξη.

β. <u>Cognitive Radio</u>

Το cognitive radio είναι ασύρματη τεχνολογία στην οποία, τα συστήματα επικοινωνιών παρακολουθούν τόσο τα εσωτερικά τους χαρακτηριστικά εκτελούν δηλαδή λειτουργία adaptive radio, όσο και το περιβάλλον τους, δηλαδή το κομμάτι του φάσματος που χρησιμοποιείται και αλλά την ίδια τη χρήση που γίνεται σε αυτό το κομμάτι. Μπορούν να πάρουν αποφάσεις για τη συμπεριφορά λειτουργίας τους καταγράφοντας αυτές τις πληροφορίες και ακολουθώντας τα αποτελέσματα από την επεξεργασία τους μεταβάλλοντας την αρχικοποίηση που έχει γίνει με την έναρξη λειτουργίας τους.

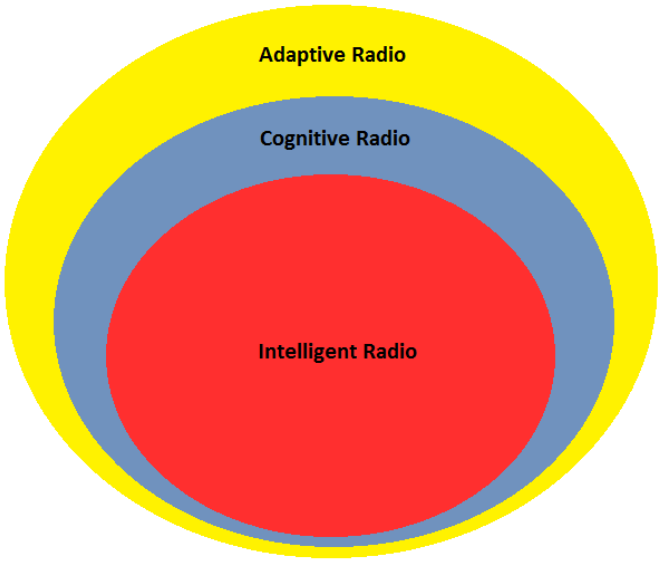
Η τεχνολογία του cognitive radio δηλαδή καταργεί τις σαφείς έως σήμερα διαχωριστικές γραμμές που καθορίζονταν από το τρίπτυχο «υπηρεσία/τεχνολογία ασύρματης πρόσβασης/μπάντα φάσματος», παρέχοντας τη δυνατότητα μετάπτωσης σε τμήματα του φάσματος που είτε δεν χρησιμοποιούνται ή υπο-χρησιμοποιούνται, με σκοπό και πάλι την αξιοποίηση όλου του πολύτιμου φάσματος.

./.

Τεράστια και κεφαλαιώδους σημασίας είναι η χρησιμότητα των παραπάνω, αν αναλογισθεί κανείς την έννοια της παρεμβολής, η οποία δημιουργείται στο σύγχρονο περιβάλλον, ηθελημένης εάν πρόκειται για στρατιωτικές εφαρμογές ή ακούσιας όταν απλά επέλθει κορεσμός ασύρματων εκπομπών γύρω από την ίδια περιοχή συχνοτήτων σε μια γεωγραφική περιοχή. Η λογική των cognitive radio, η οποία ακολουθεί την τεχνολογία των SDR, έρχεται να καταπολεμήσει αυτό ακριβώς το φαινόμενο μέσω της προσαρμοστικότητας με ταυτόχρονη συνεχή παρακολούθηση και εξέταση του φάσματος.

γ. Intelligent Radio

Το intelligent radio είναι τεχνολογία cognitive radio η οποία διαθέτει νοημοσύνη και είναι ικανή να «εκπαιδεύει» τη μηχανή πάνω στην οποία αναπτύσσεται. Αυτό επιτρέπει στο cognitive radio να βελτιώσει τους τρόπους με τους οποίους υιοθετεί τις διάφορες αλλαγές της εσωτερικής απόδοσης αλλά και του περιβάλλοντος με σκοπό την βελτιστοποίηση της παρεχόμενης υπηρεσίας στον τελικό χρήστη.



Σχήμα 1.5.1

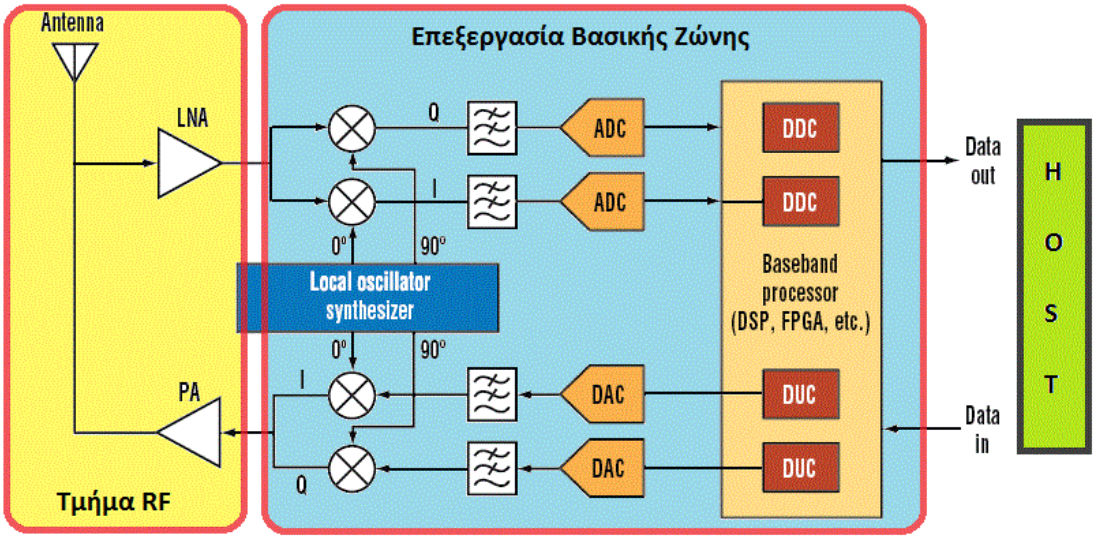
Οι παραπάνω ασύρματες τεχνολογίες, όπως αναφέρθηκαν, δεν αναφέρονται απαραίτητα σε ένα μόνο κομμάτι εξοπλισμού, αλλά μπορεί να είναι κατανεμημένες σε διάφορα μέρη κατά μήκος ενός δικτύου, τα οποία συνεργάζονται μεταξύ τους.

Μπορεί εύκολα λοιπόν κανείς να διακρίνει από τα παραπάνω, τον τεράστιο ρόλος που πρόκειται να διαδραματίσει η τεχνολογία του SDR στις σύγχρονες ασύρματες τηλεπικοινωνίες πάσης φύσεως τα επόμενα χρόνια και οι νέες δυνατότητες που θα προσδώσει σε αυτές, πάντα με ένα και μοναδικό σκοπό: την αύξηση της ποιότητας υπηρεσίας προς τον τελικό αποδέκτη.

2. ΠΕΡΙΓΡΑΦΗ USRP ΤΗΣ ETTUS RESEARCH™

2.1 Γενική επισκόπηση USRP της Ettus Research™ [11]

Για τις ανάγκες της παρούσας πτυχιακής εργασίας επιλέχθηκε από τα προϊόντα της αγοράς που αφορούν την τεχνολογία SDR, να γίνει αναφορά σε αυτά της Ettus Research, καθώς αποτελεί μια εταιρεία με τεράστια πρωτοποριακή έρευνα και ανάπτυξη πάνω στο αντικείμενο. Για να μπορέσει να γίνει μια σύντομη ανάλυση των προϊόντων που παρέχει η Ettus Research αρκούντως κατανοητή, είναι απαραίτητο πρώτα να δοθεί ένα πολύ γενικό δομικό διάγραμμα των τριών βασικών σταδίων που απαρτίζουν κάθε συσκευή USRP, ανεξαρτήτως άλλων χαρακτηριστικών.



Σχήμα 2.1.1

Το τμήμα RF σε γενικές γραμμές, είναι αυτό στο οποίο όλες οι διεργασίες γίνονται στον αναλογικό κόσμο, περιλαμβάνει μία ή δύο smart antennas, συνδετήρες SMA για τη διασύνδεση με αυτές, καθώς επίσης ενισχυτή χαμηλού θορύβου για το τμήμα της λήψης και ενισχυτή ισχύος για αυτό της εκπομπής. Το τμήμα αυτό υλοποιείται στη θυγατρική πλακέτα της συσκευής.

Το τμήμα επεξεργασίας βασικής ζώνης για τη λήψη μεταφέρει το σήμα από την RF περιοχή στην βασική ζώνη αναλύοντάς το κατά την είσοδο στις ορθογώνιες συνιστώσες I,Q και δειγματοληπτεί αυτό με σκοπό να το παραδώσει στο τμήμα DSP, το οποίο υλοποιείται σε ένα FPGA. Το FPGA υλοποιεί λειτουργία up-down conversion και προωθεί το παραγόμενο stream μέσω κατάλληλης διασύνδεσης, η οποία μπορεί να είναι Ethernet ή USB στον συνδεδεμένο host για περαιτέρω επεξεργασία. Η αντίστροφη ακριβώς διαδικασία γίνεται για το τμήμα εκπομπής. Το τμήμα επεξεργασίας βασικής ζώνης υλοποιείται στη μητρική πλακέτα της συσκευής.

Τέλος, ο host αναλαμβάνει την επιθυμητή περαιτέρω επεξεργασία, κωδικοποίηση, κρυπτογράφηση, διαμόρφωση, κτλ., μέσω τριών υποστηριζόμενων διεπαφών. Του λογισμικού LabView της εταιρίας National Instruments, του λογισμικού Simulink της εταιρίας MathWorks και τέλος ενός ελεύθερου

λογισμικού, ανεπτυγμένου από την κοινότητα του Linux, του GNU Radio. Οι δυνατότητες που παρέχουν οι παραπάνω πλατφόρμες, θα αναλυθούν στη συνέχεια, καθώς η επιλογή της κατάλληλης από αυτές είναι η τελική συνισταμένη του σκοπού της ανάπτυξης ενός ασύρματου συστήματος και των δυνατοτήτων-περιορισμών του υλικού.

Έχοντας κάνει αυτή τη βασική διάκριση μεταξύ των δομικών μονάδων των συσκευών USRP της Ettus Research στον παρακάτω πίνακα φαίνεται το σύνολο των διατιθέμενων από την εταιρία μητρικών καρτών, οι ενδεικτικές εργοστασιακές τιμές τους, τα βασικά χαρακτηριστικά αυτών, καθώς επίσης και οι συμβατές θυγατρικές κάρτες (πλην των σειρών B, η οποία αποτελείται μόνο από μία κάρτα).

USRP X SERIES
X310(~4.900€):

• Two wide-bandwidth RF daughterboard slots
  ○ Up to 120MHz bandwidth each (wideband versions of CBX, WBX, SBX)
  ○ Daughterboard selection covers DC to 6 GHz
• Large customizable Xilinx Kintex-7410 FPGA for high performance DSP
• Multiple high-speed interfaces
Dual 10 Gigabit Ethernet - 200 MS/s Full Duplex
PCIe Express (Desktop) - 200 MS/s Full Duplex
PCIe Express (Desktop) - 200 MS/s Full Duplex
ExpressCard (Laptop) - 50 MS/s Full Duplex
Dual 1 Gigabit Ethernet - 25 MS/s Full Duplex

X300 (~3.950€):

• Two wide-bandwidth RF daughterboard slots
  ○ Up to 120MHz bandwidth each (wideband versions of CBX, WBX, SBX)
  ○ Daughterboard selection covers DC to 6 GHz
• Large customizable Xilinx Kintex-7325 FPGA for high performance DSP
• Multiple high-speed interfaces
  ○ Dual 10 Gigabit Ethernet - 200 MS/s Full Duplex
  ○ PCIe Express (Desktop) - 200 MS/s Full Duplex
  ○ ExpressCard (Laptop) - 50 MS/s Full Duplex
  ○ Dual 1 Gigabit Ethernet - 25 MS/s Full Duplex

USRP N (Network) SERIES
N210 (~1.850€):
• Modular Architecture: DC-6 GHz • Dual 100 MS/s, 14-bit ADC • Dual 400 MS/s, 16-bit DAC • DDC/DUC with 25 MHz Resolution • Up to 50 MS/s Gigabit Ethernet Streaming • Fully-Coherent MIMO Capability • Gigabit Ethernet Interface to Host • 2 Gbps Expansion Interface • Spartan 3A-DSP 3400 FPGA

- 1 MB High-Speed SRAM
- Auxiliary Analog and Digital I/O
- 2.5 ppm TCXO Frequency Reference
- 0.01 ppm w/ GPSDO Option
- Recommended daughterboards: UBX, WBX, SBX, CBX

N200 (~1.700€):

- Modular Architecture: DC-6 GHz
- Dual 100 MS/s, 14-bit ADC
- Dual 400 MS/s, 16-bit DAC
- DDC/DUC with 25 mHz Resolution
- Up to 50 MS/s Gigabit Ethernet Streaming
- Fully-Coherent MIMO Capability
- Gigabit Ethernet Interface to Host
- 2 Gbps Expansion Interface
- Spartan 3A-DSP 1800 FPGA
- 1 MB High-Speed SRAM
- Auxiliary Analog and Digital I/O
- 2.5 ppm TCXO Frequency Reference
- 0.01 ppm w/ GPSDO Option
- Recommended daughterboards: UBX, WBX, SBX, CBX

USRP B SERIES

USRP B200mini-i (Board only):

- Wide frequency range: 70 MHz - 6 GHz
- Up to 56 MHz of instantaneous bandwidth
- Full duplex operation
- Programmable, industrial-grade Xilinx Spartan-6 XC6SLX75 I-Grade FPGA
- Fast and convenient bus-powered USB 3.0 connectivity
- Synchronization with 10 MHz clock reference or PPS time reference
- GPIO and JTAG for control and debug capabilities

USRP B200mini (Board only):

- Wide frequency range: 70 MHz - 6 GHz
- Up to 56 MHz of instantaneous bandwidth
- Full duplex operation
- Programmable Xilinx Spartan-6 XC6SLX75 C-Grade FPGA
- Fast and convenient bus-powered USB 3.0 connectivity
- Synchronization with 10 MHz clock reference or PPS time reference
- GPIO and JTAG for control and debug capabilities

USRP B210 (Board Only) (~1.100€):

- First fully integrated, two-channel USRP device with continuous RF coverage from 70 MHz – 6 GHz
- Full duplex, MIMO (2 Tx & 2 Rx) operation with up to 56 MHz of real-time bandwidth (61.44MS/s quadrature)
- Fast and convenient SuperSpeed USB 3.0 connectivity

USRP B200 (Board Only) (~700€)::

- The first fully integrated USRP device with continuous RF coverage from 70 MHz –6 GHz
- Full duplex operation with up to 56 MHz of real time bandwidth (61.44MS/s quadrature)
- Fast and convenient bus-powered connectivity using SuperSpeed USB 3.0

Άλλες εκδόσεις:
USRP1 (~650€):
• Use with GNU Radio • Modular Architecture: DC-6 GHz • Connectivity for Two, Complete Tx/Rx chains • Two Dual 64 MS/s, 12-bit ADC's • Two Dual 128 MS/s, 14-bit DAC's • DDC/DUC with 15 mHz Resolution • Up to 16 MS/s USB Streaming • USB 2.0 Interface to Host • Auxiliary Digital and Analog I/O • 25 ppm TCXO Frequency Reference • Recommended daughterboards: UBX, WBX, SBX, CBX
USRP E310 (~2.750€):
RF Capabilities

• AD9361 RFIC
  ○ 2x2 MIMO transceiver
  ○ Up to 56 MHz of bandwidth
  ○ Frequency coverage from 70 MHz - 6 GHz
  ○ Flexible rate 12-bit ADC/DAC
• TX & RX front-end filter banks
• Synchronization input (PPS)
Processing
• Xilinx Zynq 7020
  ○ Dual ARM Cortex A9 – 667 MHz
  ○ Xilinx 7 Series FPGA
• 1GB DDR3 RAM for ARM CPUs
• 512 MB DDR3 RAM for FPGA Logic
Peripherals
• 10/100/1000 BASE-T Ethernet
• Stereo audio output & mono mic input
• Integrated GPS receiver
• Host USB Support

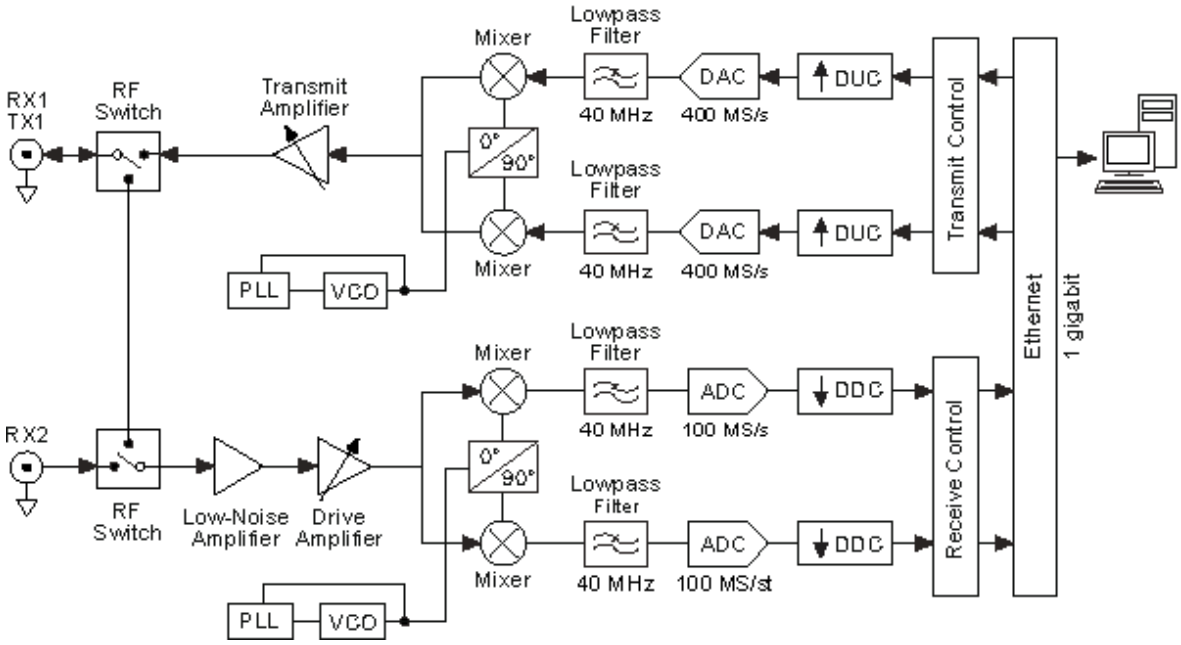
Πίνακας 2.1.2

Πρέπει να τονισθεί ότι το κόστος αφορά μόνο την προμήθεια της μητρικής κάρτας, η δε θυγατρική της επιλογής του εκάστοτε χρήστη υπόκειται σε ξεχωριστή χρέωση, συγκριτικά πολύ μικρότερη πάντως από αυτή της μητρικής. Άλλωστε, το κύριο κόστος στο ολοκληρωμένο πακέτο ενός SDR αποτελείται από το state of the art των σημερινών τηλεπικοινωνιακών μικροηλεκτρονικών, το οποίο δεν είναι άλλο από το FPGA της μητρικής κάρτας. Οι προσφερόμενες θυγατρικές κάρτες της Ettus αναφέρονται συνοπτικά στην επόμενη ενότητα όπου αναλύεται το θέμα του τελικού εύρους ζώνης που καλύπτει ένα SDR.

2.2 Bandwidth συσκευών USRP [11]

Ποιό είναι το bandwidth μιας συσκευής USRP; Αυτή η βασική ερώτηση είναι ταυτόχρονα και ο γενικός και ίσως μοναδικός περιορισμός των δυνατοτήτων

της. Για να γίνει κατανοητό το πως υπολογίζεται το τελικό bandwidth ενός συγκεκριμένου USRP θα πρέπει να γίνει πρώτα μια γενική περιγραφή των μονάδων που το απαρτίζουν, επιχειρώντας να κατέβουμε ακόμα ένα επίπεδο πιο κάτω σε επίπεδο block διαγράμματος από την προηγούμενη συνοπτική περιγραφή που έγινε.



Σχήμα 2.1.1

Ακόμα κι αν κάποια χαρακτηριστικά διαφέρουν από μοντέλο σε μοντέλο, όλες οι συσκευές USRP χρησιμοποιούν την ίδια γενική αρχιτεκτονική, αυτήγ που φαίνεται στο παραπάνω σχήμα. Σε πολλές περιπτώσεις, το τμήμα RF, οι μίκτες, τα φίλτρα, οι ταλαντωτές και οι ενισχυτές απαιτείται να μεταφράσουν το σήμα από το πεδίο RF, από τη βασική ζώνη ή το τμήμα IF. Το RF ή IF σήμα δειγματοληπτείται από ADC's και τα ψηφιακά δείγματα προωθούνται χρονισμένα σε ένα FPGA. Το FPGA εκτελεί μια ψηφιακή μετατροπή κατά την οποία το σήμα υφίσταται έναν υποβιβασμό (digital-down conversion), η οποία περιλαμβάνει λειτουργίες συντονισμού και διάφορα φιλτραρίσματα για το απαραίτητο decimation, την ελάττωση δηλαδή του ρυθμού δειγματοληψίας του σήματος. Μετά το decimation, το stream με τα data εξόδου τροφοδοτείται στον Η/Υ μέσω της ανάλογης διεπαφής (USB ή Ethernet). Η αντίστροφη διαδικασία λαμβάνει χώρα στην αλυσίδα εκπομπής.

Το bandwidth του USRP διαφέρει σε κάθε σημείο της αλυσίδας. Τρεις είναι οι γενικές κατηγορίες bandwidth, το αναλογικό bandwidth, το bandwidth επεξεργασίας του FPGA και το bandwidth του host Η/Υ. Το bandwidth του συστήματος είναι συνεπώς το ελάχιστο από τα bandwidth της daughterboard, του FPGA processing και του host. Ακόμα, πρέπει να τονισθεί, όπως θα γίνει φανερό και από τα παραδείγματα που ακολουθούν, ότι πρέπει να ληφθεί μέριμνα ώστε να αποφευχθεί το αναλογικό bandwidth να είναι μεγαλύτερο από αυτό των ρυθμών δειγματοληψίας των ADC/DAC της κάθε αλυσίδας για να αποφευχθούν φαινόμενα overflow/underflow.

Το **αναλογικό bandwidth** είναι το συνολικό χρήσιμο bandwidth (3 dB) μεταξύ της RF port και του IF ή του baseband interface. Τυπικά αυτό το bandwidth καθορίζεται από τα φίλτρα IF ή baseband στη θυγατρική κάρτα, τα οποία είναι σχεδιασμένα ώστε να αποφεύγεται το φαινόμενο του aliasing όταν η θυγτρική συνδεθεί με μια μητρική κάρτα με ADC/DAC με δεδομένους ρυθμούς δειγματοληψίας. Στον παρακάτω πίνακα παραθέτονται τα προσφερόμενα bandwidth των διαφόρων θυγατρικών που διαθέτει η ETTUS:

Daughterboard	Frequency Coverage	Analog Bandwidth
WBX-120	50 MHz – 2.2 GHz	120 MHz
SBX-120	400 MHz – 4.4 GHz	120 MHz
CBX-120	1.2 GHz – 6 GHz	120 MHz
WBX	50 MHz – 2.2 GHz	40 MHz
SBX	400 MHz – 4.4 GHz	40 MHz
CBX	1.2 GHz – 6 GHz	40 MHz
TVRX2	50 MHz – 860 MHz	Configurable – 1.7 to 10 MHz
DBSRX2	800 MHz – 2.3 GHz	Configurable – 8 to 80 MHz
BasicRX/BasicTX	1 – 250 MHz	Determined by ADC/DAC sample rates. External filter required.
LFRX/LFTX	DC-30 MHz	30 MHz

Πίνακας 2.1.2

Το **bandwidth του FPGA processing** είναι το αντίστροφο του ρυθμού δειγματοληψίας που μπορεί να παρασχεθεί από τον ADC ή DAC στη μητρική κάρτα του USRP. Αυτό θέτει και το υποθετικό μέγιστο bandwidth ενός συστήματος που σχεδιάζεται με το USRP. Για παράδειγμα, το FPGA του USRP X300/X310 στέλνει και λαμβάνει σύμβολα στα 200 MS/s αντίστοιχα από τους DAC και ADC. Στον παρακάτω πίνακα φαίνονται τα bandwidth των διαφόρων μητρικών καρτών των USRP της ETTUS. Ο stock σχεδιασμός FPGA όλων των USRP συσκευών περιλαμβάνει αλυσίδες DSP οι οποίες παρέχουν ολισθήσεις συχνότητας, decimation για τα εισερχόμενα stream και interpolation για τα εξερχόμενα. Αυτές οι DSP λειτουργίες υποστηρίζονται στο καθορισμένο bandwidth του FPGA processing. Μια διαφορετική παραμετροποίηση και επαναπρογραμματισμός του FPGA σαφώς θα επιφέρει αλλαγή και στο υποστηριζόμενο bandwidth.

USRP ™ Model	ADC Processing Bandwidth (MS/s)	DAC Processing Bandwidth (MS/s)
USRP B100	64 MS/s	128 MS/s
USRP 1	64 MS/s	128 MS/s
USRP E100/E110	64 MS/s	128 MS/s
USRP B200/B210	61.44 (simplex)	61.44 (simplex)
USRP N200/N210	100 MS/s	100 MS/s
USRP X300/X310	200 MS/s	200 MS/s

Πίνακας 2.1.3

Το interface του host H/Y είναι αυτό που επιτρέπει στα δεδομένα να ρέουν από το FPGA του USRP και του host H/Y και συνεπώς καθορίζει το **bandwidth του host H/Y**. Οι περισσότερες εφαρμογές κάνουν stream I/Q data από και προς το USRP. Στον παρακάτω πίνακα φαίνονται μερικές από τις επιλογές interface που είναι διαθέσιμες με τα διάφορα μοντέλα USRP που διατίθενται στην αγορά. Επίσης φαίνεται ο ρυθμός δειγματοληψίας του host με δείγματα I/Q των 16-bit**.** Τα περισσότερα μοντέλα USRP παρέχουν την επιλογή για σύμβολα μήκους 8-bit και έτσι συνεπώς διπλασιάζεται το bandwidth του host H/Y. Ακόμα πρέπει να τονισθεί ότι ο όρος «full duplex» σημαίνει ότι το interface μπορεί να κάνει stream και προς τις δύο κατευθύνσεις στον ρυθμό που αναγράφεται.

Μερικά interfaces όπως το USB 3.0, δεν παρέχει ξεχωριστά μονοπάτια για αποστολή και λήψη δεδομένων αλλά επαναχρησιμοποίηση του διαύλου σε λειτουργία «half duplex». Σε αυτή την περίπτωση το ολικό bandwidth που καθορίζεται από το interface θα μοιράζεται μεταξύ των λειτουργιών εκπομπής και λήψης του USRP χωρίς αυστηρό καθορισμό.

Τέλος, πρέπει να σημειωθεί ότι **η πραγματική δυνατότητα streaming δεδομένων θα εξαρτηθεί από την επεξεργαστική ισχύ του host H/Y, την πολυπλοκότητα της εφαρμογής, δηλαδή του DSP και άλλους παράγοντες.** Ο παρακάτω πίνακας απλά αναφέρει το μέγιστο θεωρητικό throughput για καθένα interface.

Interface	USRP ™ Devices	Host Sample Rate (MS/s @ 16-bit I/Q)	Half/Full Duplex
USB 2.0	USRP ™ 1, B100	8	Half Duplex
USB 3.0	B200/B210	61.44	Half Duplex
Gigabit Ethernet	N200/N210	25	Full Duplex
10 Gigabit Ethernet	X300/X310	200	Full Duplex
PCI-Express (4-lane PCIe card)	X300/X310	200	Full Duplex
PCI-Express (1-lane ExpressCard)	X300/X310	50	Full Duplex
OMAP GPMC	E100/E110	4	Half Duplex

Πίνακας 2.1.4

Ακόμα, όπως προαναφέρθηκε, πρέπει να γίνει σαφές ότι **η χρήση θυγατρικών καρτών με μεγάλο bandwidth σε συνδυασμό με USRP χαμηλότερου bandwidth θα οδηγήσει στο φαινόμενο του aliasing**, οπότε αυτό είναι κάτι που πρέπει πάντα να λαμβάνεται υπόψη.

Ετσι λοιπόν γίνεται σαφές ότι ο καθορισμός του bandwidth ενός συστήματος που σχεδιάζεται με USRP είναι συνδυασμός πολλών παραγόντων. Τα παρακάτω παραδείγματα μπορούν να καταστήσουν αυτό πιο σαφές:

Παράδειγμα 1: Ένα σύστημα που χρησιμοποιεί το USRP X300/X310 (200 MS/s) με interface 10 GigE (200 MS/s), με μια εφαρμογή πλήρως

βασισμένη στον host H/Y και μια daughterboard με bandwidth 40 MHz θα δώσει ένα χρήσιμο bandwidth 40 MHz, δηλαδή η daughterboard είναι αυτή που θέτει το όριο, παρόλο που το USRP αλλά και το χρησιμοποιούμενο interface έχει μεγαλύτερες δυνατότητες.

Παράδειγμα 2: Ένα σύστημα που χρησιμοποιεί το USRP N200/N210 (100 MS/s) με interface 1GigE (25 MS/s), με μια εφαρμογή πλήρως βασισμένη στον host H/Y, η οποία απαιτεί 16-bit δείγματα και με μια daughterboard στα 40 MHz θα έχει διαθέσιμο bandwidth περίπου ίσο με 20 MHz. Το όριο τίθεται από το interface του host H/Y, το οποίο μπορεί να κάνει stream έως 25 MS/s, το οποίο μεταφράζεται σε περίπου 20 MHz bandwidth.

Παράδειγμα 3: Ένα σύστημα που χρησιμοποιεί το USRP X300/X310 (200 MS/s) με interface 1 GigE (25 MS/s) για εφαρμογή command/control με την επεξεργασία των RX/TX streams να γίνεται εξ' ολοκλήρου στο FPGA και μια daughterboard στα 120 MHz έχει χρησιμοποιήσιμο bandwidth έως 120 MHz. Βλέπουμε ότι παρόλο που το FPGA μπορεί να επεξεργαστεί δείγματα με ρυθμό έως 200 MS/s, η daughterboard αποτελεί το τελικό όριο στο συνολικό διαθέσιμο bandwidth.

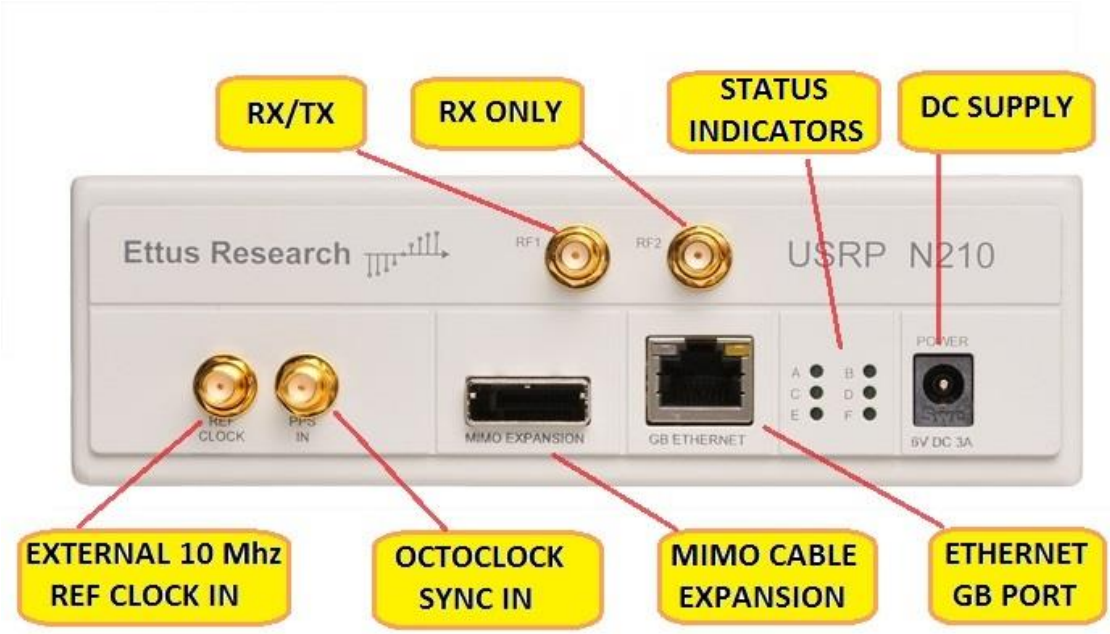
2.3 Το USRP N210 της Ettus Research

Για την υλοποίηση της παρούσας πτυχιακής εργασίας χρησιμοποιήθηκε το USRP N210, με θυγατρική κάρτα την SBX της Ettus Research, κάλυψης εύρους συχνοτήτων από 400 MHz έως 4,4 GHz και με αναλογικό bandwidth 40 MHz.

Το USRP N210 είναι ιδανικό για λειτουργία σε υψηλές συχνότητες και μεγάλο bandwidth, επιτρέποντας ανάπτυξη ακόμα και δικτυακών εφαρμογών. Τα χαρακτηριστικά του συνοψίζονται στον παρακάτω πίνακα.

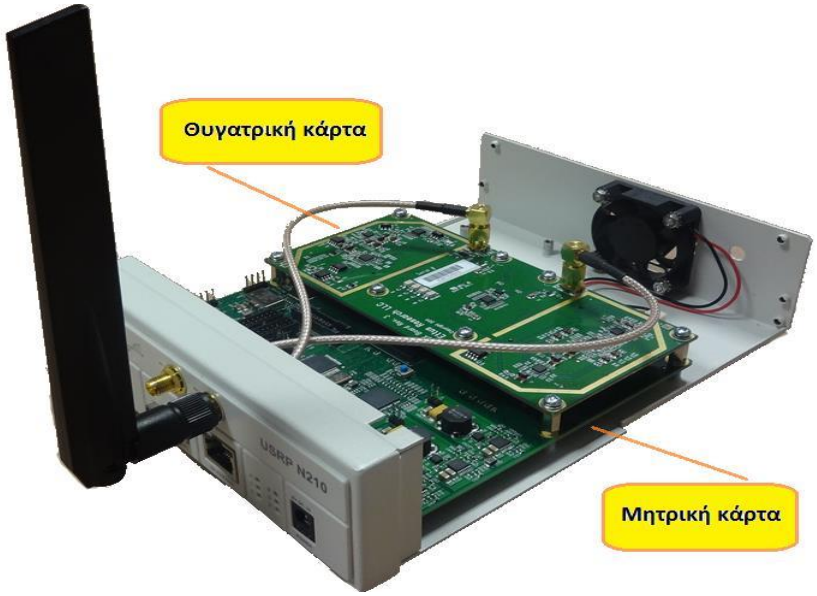
Χρήση	GNU Radio, LabVIEW™ and Simulink™
Κάλυψη εύρους ζώνης	Από 400 MHz έως 4,4 GHz
Ρυθμοί	• Dual 100 MS/s, 14-bit ADC • Dual 400 MS/s, 16-bit DAC
Επικοινωνία με host	Έως 50 MS/s Gigabit Ethernet Streaming
Δυνατότητα επέκτασης	Έως 2x2 MIMO μέσω διασύνδεσης
FPGA	Spartan 3A-DSP 3400 FPGA
Μνήμη	1 MB High-Speed SRAM

Πίνακας 2.3.1



Εικόνα 2.3.2

Το USRP N210 προσφέρει τη δυνατότητα λειτουργίας σε δύο κανάλια, σε ένα για εκπομπή/λήψη και σε ένα μόνο για λήψη. Στην πρόσοψη της συσκευής βρίσκονται οι ανάλογοι SMA συνδετήρες και ακόμα συνδετήρας για τροφοδοσία, ενδεικτικές λυχνίες, ο συνδετήρας Ethernet, ο συνδετήρας για επέκταση MIMO, καθώς και δύο ακόμα συνδετήρες για χρήση εξωτερικών σημάτων χρονισμού.



Εικόνα 2.3.3

Στο εσωτερικό της συσκευής, μπορεί κάποιος να διακρίνει τις δύο πλακέτες, η λειτουργία των οποίων αναλύθηκε στην προηγούμενη παράγραφο, τη μητρική πλακέτα, η οποία αποτελεί και την καρδιά της συσκευής καθώς ενσωματώνει τις λειτουργίες της ADC, DAC και ψηφιακής επεξεργασίας σήματος

στη βάση του USRP και τη θυγατρική, η οποία εκτελεί τις αναλογικές λειτουργίες και που τοποθετείται πάνω στη μητρική με τελικές εξόδους τους συνδετήρες SMA.

3. ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

3.1 Γενικά

Η έννοια της ασφάλειας, ενώ σε πρώτο χρόνο δεν απασχόλησε τους επιστήμονες που διεξήγαγαν έρευνα πάνω στις τηλεπικοινωνίες, καθώς αρχικά ο στόχος ήταν η εκπομπή και λήψη μεγάλου όγκου πληροφορίας με τον πιο αποδοτικό τρόπο, γρήγορα ήρθε στην επιφάνεια για να αναδείξει την αναγκαιότητα προστασίας της πληροφορίας που ταξιδεύει στο φυσικό μέσο από κάθε επίδοξο λαθρακουστή, ο οποίος θέλει την πληροφορία προς ίδιον όφελος.

Προκειμένου να γίνει πιο κατανοητή η έννοια της ασφάλειας κατά την εφαρμογή της στα διάφορα συστήματα επικοινωνιών, είναι απαραίτητη η διακριτή καταγραφή βασικών εννοιών [25][26], με όσο το δυνατό πιο σαφή τρόπο, όπως παρακάτω:

α. Απειλή

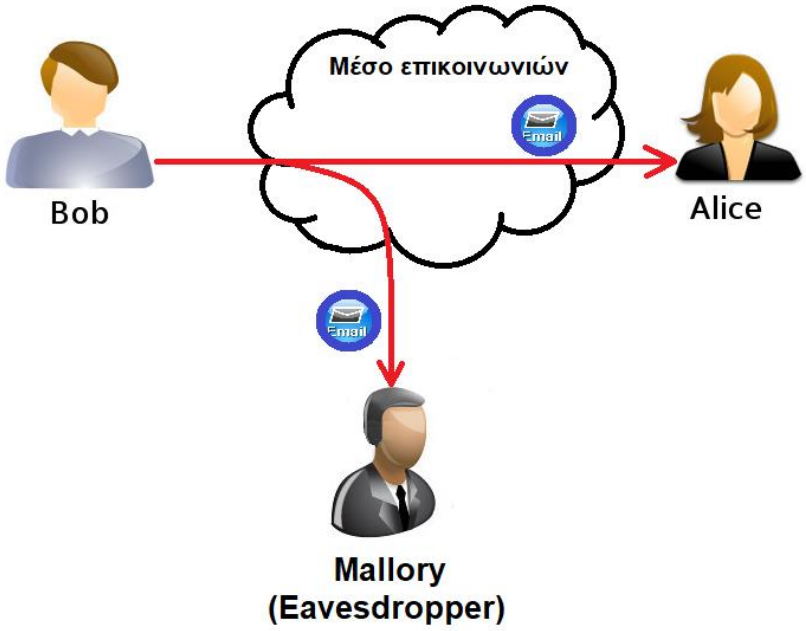
Η δυνατότητα η οποία υπάρχει εγγενώς από κατασκευής ενός συστήματος για παραβίαση ασφαλείας, μετά από ενέργεια ενός επίδοξου επιτιθέμενου προσώπου, είναι δηλαδή η δυνατότητα να εκμεταλλευτεί κάποιος μια εγγενή ευπάθεια του συστήματος.

β. Επίθεση

Η ενέργεια με την οποία ένας λαθρακουστής εκμεταλλεύεται ενδεχόμενες τρωτότητες ενός τηλεπικοινωνιακού συστήματος, με σκοπό την παράκαμψη των υπηρεσιών ασφαλείας και την παραβίαση αυτού. Οι προσπάθειες εισόδου στη δικτυακή δομή ανάλογα με τον στόχο τους μπορούν να διακριθούν σε δύο κατηγορίες εισβολών, τις παθητικές και τις ενεργητικές.

(1) Παθητικές Επιθέσεις

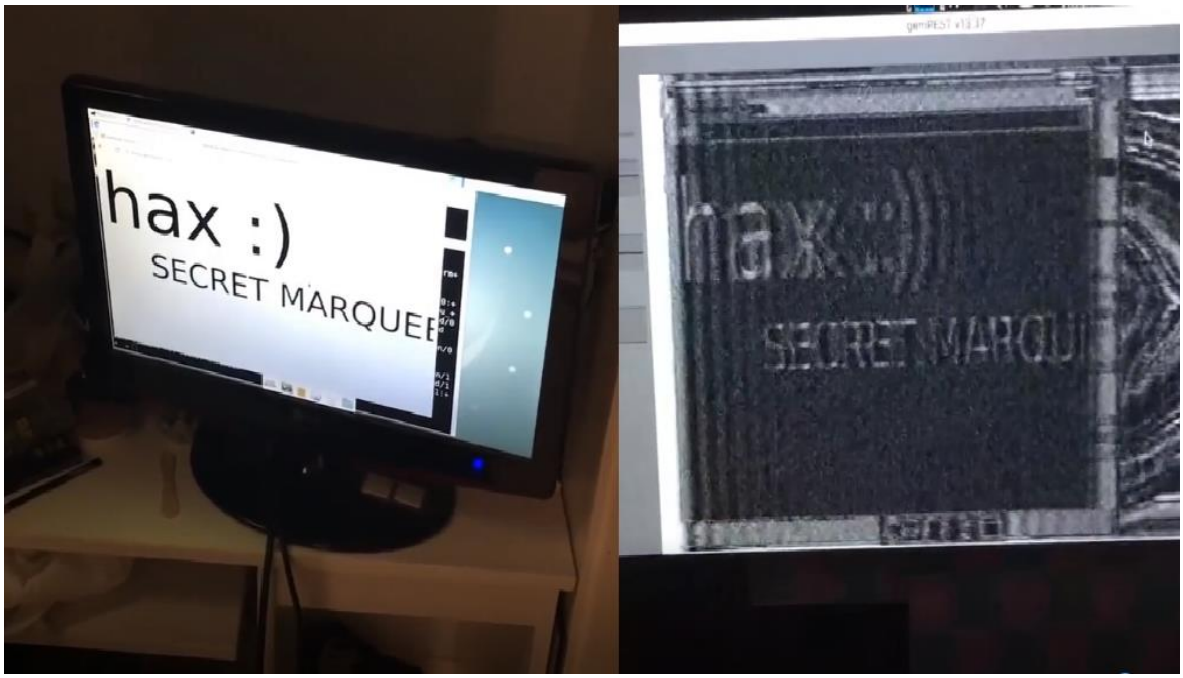
Στις παθητικές επιθέσεις, ο εισβολέας παρατηρεί τα μηνύματα, που διέρχονται στο φυσικό μέσον επικοινωνιών (αέρας, οπτική ίνα, χαλκός, κ.λπ.), χωρίς να παρεμβαίνει στη φύση και τη ροή τους. Αυτού του είδους εισβολές διακρίνονται σε δυο υποκατηγορίες παθητικής εισβολής.



Εικόνα 3.1.1

(α) Παρατήρηση του περιεχομένου των μηνυμάτων, κατά την οποία ο εισβολέας υποκλέπτει μέρος ή τον σύνολο των διακινουμένων πληροφοριών.

Ένα εξαιρετικό παράδειγμα παθητικής επίθεσης και δη στο φυσικό επίπεδο είναι η εκμετάλλευση της ακτινοβολίας TEMPEST για υποκλοπή πληροφορίας (στην περίπτωσή μας χαρακτήρες ASCII και κωδικοποιημένο video) που διακινείται σε μη ηλεκτρομαγνητικά θωρακισμένες καλωδιώσεις (π.χ. καλώδιο σύνδεσης πληκτρολογίου με κεντρική Η/Υ, καλώδιο HDMI σύνδεσης οθόνης σε κεντρική μονάδα Η/Υ, κ.λπ.). Η τεχνική βασίζεται στο νόμο Biot-Savart, ο οποίος προβλέπει τη δημιουργία μαγνητικού πεδίου γύρω από κάθε αγωγό που διαρρέεται από ηλεκτρικό ρεύμα. Τέτοιοι αγωγοί είναι τα καλώδια διασύνδεσης των περιφερειακών του Η/Υ με την κεντρική μονάδα αυτού, έστω π.χ. το καλώδιο σύνδεσης του πληκτρολογίου, πατώντας το γράμμα «Α», τότε ο αντίστοιχος χαρακτήρας ASCII (01000001) μετατρέπεται σε συγκεκριμένη, μοναδική κυματομορφή και διοχετεύεται στο φυσικό μέσο (καλώδιο χαλκού). Γύρω της θα παραχθεί πεδίο συγκεκριμένης συχνότητας. Εντός εμβέλειας του υπόψη πεδίου (έως δεκάδες μέτρα), τοποθετώντας σε ικανή απόσταση ένα δέκτη, αποκωδικοποιώντας κάθε φορά που πατιέται ένα πλήκτρο στον Η/Υ στόχο (άρα κυκλοφορεί ρεύμα στο καλώδιο του πληκτρολογίου) την εκπεμπόμενη συχνότητα στον αντίστοιχο χαρακτήρα ASCII (άρα αντίστοιχο πλήκτρο) που πατήθηκε στον Η/Υ στόχο και ξανακωδικοποιώντας τον σε ένα τερματικό στον Η/Υ μας, μπορούμε κάλλιστα να αναπαράγουμε ότι πληκτρολογεί ο ανυποψίαστος χρήστης του Η/Υ στόχου, στο δικό μας Η/Υ. Αντίστοιχα, με παρόμοια διαδικασία μπορεί να επιτευχθεί η αναπαραγωγή ολόκληρης της οθόνης του Η/Υ στόχου στον Η/Υ μας, όπως αυτό φαίνεται στην παρακάτω εικόνα.



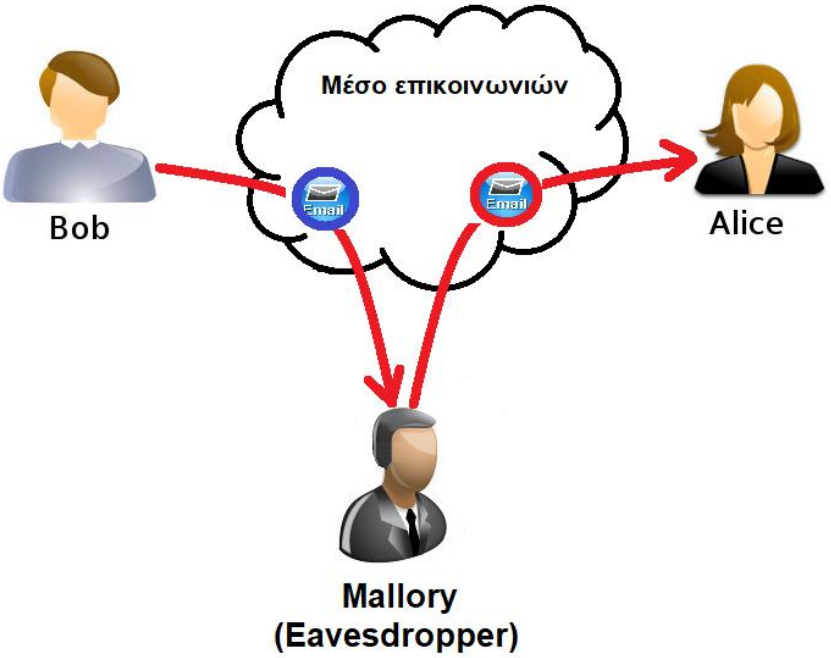
Εικόνα 3.1.2

(β) Ανάλυση της κυκλοφορίας, κατά την οποία ο εισβολέας καταγράφει και αναλύει τα διερχόμενα μηνύματα με σκοπό τη συγκέντρωση άμεσων ή επαγωγικών πληροφοριών. Οι πληροφορίες αυτές αφορούν τη δομή του συστήματος, τα χρησιμοποιούμενα πρωτόκολλα, την ονοματολογία, τους ενεργούς χρήστες, τους ενεργούς κόμβους, τις εκτελούμενες εφαρμογές και τις υπηρεσίες του συστήματος.

(2) Ενεργητικές Επιθέσεις

Στις ενεργητικές εισβολές ο εισβολέας επεξεργάζεται τα διερχόμενα μηνύματα και πιθανά εισάγει νέα. Αυτού του είδους εισβολές διακρίνονται σε τέσσερις υποκατηγορίες:

(α) Τη μεταβολή των μηνυμάτων. Κατά την παραβίαση αυτή μεταβάλλεται το περιεχόμενο των μηνυμάτων (δεδομένα, διευθύνσεις, τμήματα ελέγχου), εισάγονται νέα μηνύματα ή μεταβάλλεται η σειρά των αποστελλόμενων μηνυμάτων, έτσι ώστε να δημιουργηθεί ένα μη εξουσιοδοτημένο αποτέλεσμα. Ως παράδειγμα μπορεί να αναφερθεί τροποποίηση ενός μηνύματος ώστε να δοθεί άδεια χρήσης συγκεκριμένων αρχείων σε μη εξουσιοδοτημένο χρήστη.



Εικόνα 3.1.3

(β) Τη διαγραφή μηνυμάτων, κατά την οποία καταστρέφεται μέρος ή το σύνολο των μηνυμάτων, που ανταλλάσσονται κατά τη διάρκεια των συνόδων.

(γ) Την καθυστέρηση επικοινωνίας ή άρνηση εξυπηρέτησης. Ο εισβολέας άμεσα με την κατακράτηση και επαναποστολή μηνυμάτων ή έμμεσα με την εισαγωγή υψηλού φόρτου στο δίκτυο προκαλεί καθυστέρηση της επικοινωνιακής κυκλοφορίας.

(δ) Μεταμφίεση του εισβολέα. Στην περίπτωση αυτή ο εισβολέας δημιουργεί μία, ή περισσότερες συνόδους με ψευδή ταυτότητα. Αυτό επιτυγχάνεται με την υφαρπαγή των στοιχείων ταυτότητας ενός «νόμιμου» χρήστη, καθώς και με την επανάληψη μηνυμάτων που έχουν αντιγραφεί από μία προηγούμενη «νόμιμη» σύνοδο.

Οι ενεργητικές επιθέσεις έχουν τα αντίθετα χαρακτηριστικά από τις παθητικές. Εξαιτίας του γεγονότος ότι οι παθητικές επιθέσεις είναι δύσκολο να ανιχνευθούν, χρησιμοποιούνται μέτρα αποτροπής τους. **Από την άλλη πλευρά, είναι αρκετά δύσκολο να αποτραπεί εντελώς μια ενεργητική επίθεση, αφού κάτι τέτοιο θα απαιτούσε τη συνεχή φυσική προστασία όλων των επικοινωνιακών υποδομών και καναλιών**, γεγονός το οποίο αυξάνει κατακόρυφα και σε ασύμφορο βαθμό τα λειτουργικά κόστη της τηλεπικοινωνιακής υποδομής.

Κατά συνέπεια, αυτό το οποίο επιδιώκεται και γίνεται προσπάθεια να είναι άμεσο και διαρκές, είναι η ανίχνευση των επιθέσεων αυτών και η ταχεία ανάκαμψη του δικτύου από κάθε είδους διακοπή ή καθυστέρηση προκλήθηκε από αυτές. Μάλιστα, εξαιτίας του χαρακτήρα της ανίχνευσης, το γεγονός δηλαδή ότι ο

επιτιθέμενος μπορεί να γνωρίζει ότι το τηλεπικοινωνιακό δίκτυο εποπτεύεται, αυτό από μόνο του μπορεί να λειτουργήσει αποτρεπτικά στην εκδήλωση επιθέσεων.

3.2 Βασικές αρχές ασφάλειας επικοινωνιών

Κατά τη διαδικασία του σχεδιασμού των συστημάτων επικοινωνιών, η αρχή επιχειρησιακής λειτουργίας τους, είναι απαραίτητο να προβαίνει, με βάση τη διαβάθμιση της διακινούμενης αλλά και της αποθηκευμένης σε αυτά πληροφορίας, το σχεδιασμό του σχεδίου ασφαλείας υπό το τρίπτυχο της προστασίας χώρων και υποδομών, πληροφοριακών συστημάτων και δεδομένων. Οι βασικές αρχές, οι οποίες καλείται ένα ολοκληρωμένο σύστημα ασφαλείας επικοινωνιών να ενσωματώνει πλήρως, είναι οι παρακάτω:

α. Εμπιστευτικότητα (Confidentiality)

Στόχος της είναι η εξασφάλιση του γεγονότος ότι η πληροφορία δε θα γίνει διαθέσιμη, θα παραμείνει μυστική και οποιοδήποτε μη εξουσιοδοτημένο ή αναρμόδιο πρόσωπο δε θα μπορεί να την αποκτήσει στην αρχική της αναγνώσιμη μορφή εκτελώντας επιθέσεις παθητικού ή ενεργητικού τύπου. Η πληροφορία θα πρέπει να κατηγοριοποιείται ανάλογα με την σημαντικότητά της, ανάλογα δηλαδή με το τι επιπτώσεις θα έχει η εμφάνισή της σε λάθος άτομα. Έτσι, θα μπορούν να μπουν διαφορετικοί περιορισμοί σε κάθε κατηγορία που θα δημιουργηθεί.

Όσο σημαντικότερα είναι αυτά που πρέπει να προστατευτούν τόσο ισχυρότερα μέτρα θα πρέπει να λαμβάνονται (π.χ. απομόνωση από το δίκτυο συστημάτων που ανταλλάσσουν κρίσιμα δεδομένα, τοποθέτηση επιπλέον μέτρων προστασίας, κρυπτογράφηση και σε ακραία περίπτωση θα μπορούν να υπάρχουν μόνο τυπωμένα όσα θέλουμε να προστατευτούν (π.χ. σχέδια, οδηγίες κ.λπ.).

β. Ακεραιότητα (Integrity)

Η αρχή της ακεραιότητας εξασφαλίζει πως τα δεδομένα κατά τη μετάδοσή τους από τον ένα χρήστη στον άλλο δε θα υποστούν καμία αλλοίωση από μη εξουσιοδοτημένα ή αναρμόδια πρόσωπα ή με μη ανιχνεύσιμο τρόπο και θα φτάσουν αυτούσια στον αποδέκτη. Σε περιπτώσεις τροποποίησης θα πρέπει να παράγονται σχετικά μηνύματα ειδοποίησης, ώστε να είναι δυνατό να ελεγχθεί η σκοπιμότητα της τροποποίησης και το είδος αυτής.

γ. Διαθεσιμότητα (Availability)

Αυτή εξασφαλίζει πως το σύστημα θα μπορεί να είναι διαθέσιμο για χρήση οποτεδήποτε του ζητηθεί και μέσα σε αποδεκτά χρονικά όρια. Υπολογιστές, πομποδέκτες, συσκευές δικτύου και κατ' επέκταση δίκτυα στο σύνολό τους θα πρέπει να μπορούν να ανακάμπτουν από ενδεχόμενη διακοπή λειτουργίας, η οποία οφείλεται σε βλάβη ή επίθεση από κάποιον λαθρακουστή όσο γίνεται γρηγορότερα. (π.χ. με Σχέδιο Αποκατάστασης από Καταστροφή – Disaster Recovery Plan και Σχέδιο Επιχειρησιακής Συνέχειας – Business Continuity).

δ. Πιστοποίηση ταυτότητας (Authentication)

Η αρχή αυτή εξασφαλίζει ότι ένας χρήστης ενός συστήματος είναι όντως ο χρήστης που δηλώνει και διαθέτει όλα εκείνα τα διαπιστευτήρια ώστε να κάνει χρήση του συστήματος και όχι ένας τρίτος, κακόβουλος χρήστης. Αποτελεί βασική αρχή για την εφαρμογή της ασφάλειας στα τηλεπικοινωνιακά συστήματα, καθώς χωρίς αυτή οι λοιπές αρχές δεν έχουν καμία υπόσταση.

ε. Μη αποποίηση (Non- repudiation)

Η αρχή της μη αποποίησης επίσης παίζει ουσιώδη ρόλο στην ασφάλεια επικοινωνιών, καθώς αναφέρεται στην απαραίτητη εκείνη ιδιότητα που θα πρέπει να παρέχει ο σχεδιασμός της, ώστε να μπορούν να καταγραφεί και να αποδειχθεί το σύνολο της δραστηριότητας των χρηστών κατά τη χρήση του δικτύου. Χρήστης ο οποίος απέστειλε μήνυμα σε άλλο χρήστη ή παρέλειψε να πράξει κάτι δε θα πρέπει σε καμία περίπτωση να μπορεί να αποποιηθεί τα παραπάνω γεγονότα.

Οι παραπάνω αρχές αποτελούν τη «χρυσή πεντάδα» στη μελέτη και εφαρμογή κανόνων ασφαλείας επικοινωνιών σε κάθε επικοινωνιακό σύστημα και απώλεια ή εφαρμογή τους υπό συνθήκες/παραδοχές πάντα δημιουργεί κενά ασφαλείας και αφήνει χώρο για δράση κακόβουλων προσώπων.

Οι αρχές αυτές, καταγράφονται σε κάθε βιβλίο ή ερευνητικό έγγραφο που αφορά σε ασφάλεια Η/Υ, ασφάλεια επικοινωνιών ή κρυπτογραφία, όπως αναλύθηκαν πιο πάνω με τα αρχικά τους (CIANA - Confidentiality, Integrity, Availability, Non-repudiation and Availability) είτε ελαφρώς τροποποιημένες και συγχωνευμένες ως (CIA - Confidentiality, Integrity and Availability).

Οι υπόψη αρχές έρχονται να συμπληρωθούν από δύο άλλες γενικές αρχές, οι οποίες αφενός δεν απαντώνται συχνά στη διεθνή αλληλογραφία ως αυτούσιες έννοιες αλλά απορρέουν από πληθώρα θεσμικών κειμένων, ιδίως στρατιωτικού τύπου (κυρίως ΝΑΤΟϊκών) και είναι οι παρακάτω:

στ. Αρχή Ανάγκης Γνώσης (Need-to-Know Principle)

Η αρχή ανάγκης γνώσης αποτελεί ακρογωνιαίο λίθο στην ασφάλεια επικοινωνιών και δε θα πρέπει να συγχέεται με αυτή της πιστοποίησης ταυτότητας. Αναφέρεται στο γεγονός ότι ένας χρήστης ενός επικοινωνιακού συστήματος, παρότι μπορεί να είναι πιστοποιημένος ως οντότητα ώστε να μπορεί να κάνει χρήση του συστήματος αυτό δε σημαίνει ότι θα πρέπει να έχει πρόσβαση σε κάθε πληροφορία που διακινείται εντός του υπόψη συστήματος ή αφορά στην ίδια την αρχιτεκτονική του συστήματος. Για να μπορέσει να πράξει τούτο, απαιτείται κάθε φορά ειδική άδεια από την υπεύθυνη εκείνη αρχή, η οποία είναι επιφορτισμένη με την ασφάλεια του συστήματος.

Στην κατάρτιση του σχεδίου ασφαλείας επικοινωνιών λοιπών των επικοινωνιακών συστημάτων, θα πρέπει να γίνεται σαφής διαχωρισμός μεταξύ της πιστοποίησης ταυτότητας (authentication) και της εξουσιοδότησης (security clearance), καθώς το πρώτο πηγάζει από τον τύπο της οντότητας (εάν είναι δηλαδή πιστοποιημένος χρήστης ή όχι ενός συστήματος) ενώ το δεύτερο από τα

καθήκοντα που το έχουν ανατεθεί (σε ποιά συγκεκριμένα μέρη/αρχεία/πληροφορίες του συστήματος δικαιούται να έχει πρόσβαση).

ζ. Ταχύτητα Διαβίβασης Πληροφορίας και Ασφάλεια Μέσου Διαβίβασης

Η αξία της πληροφορίας κατά το πέρασμα του χρόνου κατά τη συνηθέστερη περίπτωση μεταβάλλεται, δε διαρκεί για μεγάλο χρονικό διάστημα και ως εκ τούτου κάποια χρονική στιγμή μπορεί και να μηδενιστεί εντελώς. Η απόδοση λοιπόν βαθμού ασφαλείας σε μια πληροφορία, προκύπτει ως αποτέλεσμα της σχέσης αμοιβαιότητας μεταξύ του χρονικού διαστήματος για το οποίο έχει αξία η πληροφορία και κατά συνέπεια της επιλογής του κατάλληλου μέσου για διαβίβαση και της διαβάθμισης του μέσου αυτού. Πληροφορία άμεσης αξιοποίησης που δεν έχει αξία το αμέσως επόμενο χρονικό διάστημα, διαβιβάζεται άμεσα, με το πρώτο διαθέσιμο μέσο, για το οποίο υπερισχύει η ταχύτητα έναντι της διαβάθμισης. Πληροφορία η οποία δεν είναι άμεσης εκμετάλλευσης διαβιβάζεται με το ασφαλέστερο μέσο, ακόμα και αν υστερεί το μέσο αυτό σε ταχύτητα.

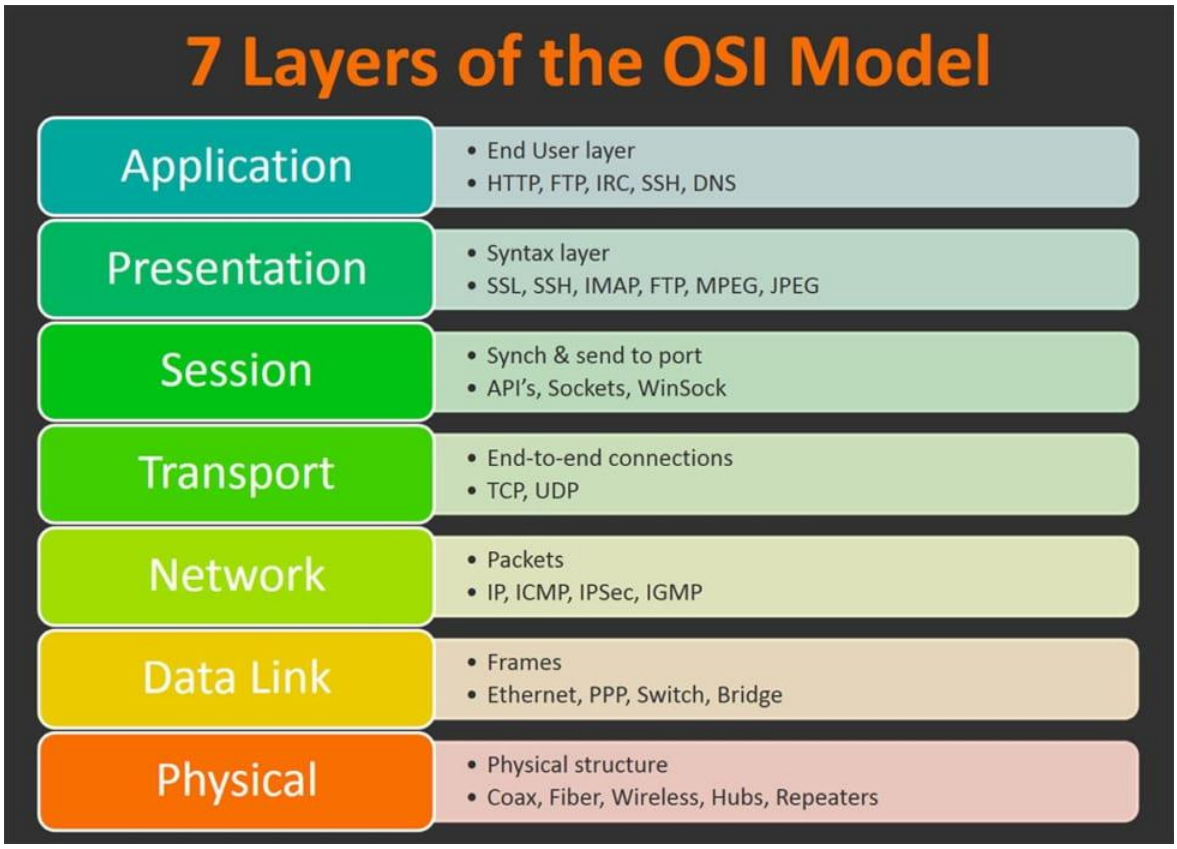
Το παραπάνω είναι εξαιρετικά σημαντικό στο σχεδιασμό επικοινωνιακών συστημάτων, καθώς η χρήση του συστήματος μπορεί να γίνει απείρως πολύπλοκη και το κόστος υλοποίησης τεράστιο άνευ λόγου, επειδή δεν έχει γίνει ορθή εκτίμηση βαθμού ασφαλείας στη διακινούμενη πληροφορία.

Ένα εξαιρετικό παράδειγμα για το παραπάνω θα μπορούσε να αποτελέσει η αναγνώριση δύο παραγόντων (2FA - Two Factor Authentication) που χρησιμοποιείται για την ενίσχυση της ασφάλειας π.χ. λογαριασμών e-mail στον παγκόσμιο ιστό. Η γεννήτρια κωδικών στο τερματικό του χρήστη (κινητό ή tablet) παράγει ένα κωδικό, τον οποίο ο χρήστης πρέπει να τον εισάγει στη φόρμα εισόδου του λογαριασμού του e-mail του, ώστε να πιστοποιηθεί η ταυτότητά του. Εάν παρέλθει χρονικό διάστημα π.χ. 30 δευτερολέπτων ο παραπάνω κωδικός απενεργοποιείται, συνεπώς χάνει την αξία του και κανέναν δεν ενδιαφέρει εκ των υστέρων αν θα τον αποκτήσει ένας επιτιθέμενος. Η ασφαλής μετάδοση δεδομένων λοιπόν εδώ που θα γίνει μεταξύ χρήστη και εξυπηρετητή που κάνει την αυθεντικοποίηση ώστε να επιτραπεί η είσοδος του χρήστη στην υπηρεσία του e-mail αφορά μόνο στο χρονικό παράθυρο των 30 δευτερολέπτων ανταλλαγής κωδικών.

3.3 Τα επίπεδα του μοντέλου δικτύου OSI και οι σημαντικότερες ευπάθειες σε αυτά

Το μοντέλο δικτύου OSI (Open Systems Interconnection) είναι μια διαστρωματωμένη, αφηρημένη περιγραφή για τη σχεδίαση τηλεπικοινωνιακών και δικτυακών πρωτοκόλλων και υποδιαιρεί τις λειτουργίες ενός τηλεπικοινωνιακού δικτύου σε μια κατακόρυφη στοίβα επτά (7) επιπέδων, για το καθένα από τα οποία μπορεί να οριστεί κάποιο πρωτόκολλο σε μία συγκεκριμένη υλοποίηση. Κάθε επίπεδο αξιοποιεί τις λειτουργίες του αμέσως κατωτέρου του στη στοίβα, ενώ ο στόχος του είναι να παρέχει λειτουργικότητα στο αμέσως ανώτερο επίπεδό του. Το

κάθε πρωτόκολλο υλοποιείται σε υλικό ή σε λογισμικό, με τα κατώτερα πρωτόκολλα να υλοποιούνται συνήθως σε υλικό και τα ανώτερα σε λογισμικό.



Εικόνα 3.3.1

Αρχίζοντας από το ανώτερο επίπεδο (Application – Εφαρμογής) προς το κατώτερο (Physical – Φυσικό), παρατίθεται πιο κάτω μια σύντομη περιγραφή των βασικών λειτουργιών των υπόψη επιπέδων, οι ευπάθειές τους καθώς και τρόποι αντιμετώπισης αυτών [27].

α. <u>Επίπεδο 7 – Εφαρμογής</u>:

(1) Το επίπεδο εφαρμογής είναι αυτό το οποίο παρέχει στο χρήστη τη δυνατότητα να προσπελάσει μέσω κάποιας εφαρμογής που εκτελείται στο τερματικό του τις πληροφορίες ενός δικτύου, κάνοντας χρήση των υψηλού επιπέδου λειτουργιών των προγραμμάτων που χρησιμοποιούν το δίκτυο αυτό. Στο επίπεδο αυτό η αλληλεπίδραση με το χρήστη γίνεται μέσω γραφικού περιβάλλοντος (user interface). Επειδή το επίπεδο εφαρμογής βρίσκεται στην κορυφή της λίστας, μπορεί να θεωρηθεί ότι είναι το τελευταίο προπύργιο στο οποίο μπορεί να αντιμετωπισθεί ένας επιτιθέμενος, εάν αυτό δεν καταστεί εφικτό στα πιο κάτω επίπεδα.

(2) <u>Ενδεικτικά Χρησιμοποιούμενα Πρωτόκολλα</u>:

(α) Naming (DNS, WINS)
(β) File-transfer (HTTP, FTP)
(γ) Messaging (SMTP)
(δ) Access (Telnet, RDP)

(3) Ευπάθειες: Επιθέσεις τύπου distributed denial-of-service (DdoS), HTTP floods, SQL injections, cross-site scripting (XSS), parameter tampering και επιθέσεις Slow Loris. Άλλοι τύποι επιθέσεων όπως ιοί, worms, phishing, key loggers, backdoors, program logic flaws, bugs, και Trojan horses.

β. Επίπεδο 6 – Παρουσίασης:

(1) Το επίπεδο παρουσίασης είναι αυτό το οποίο μετασχηματίζει τα δεδομένα σε τυπική μορφή που την αναμένει το επίπεδο εφαρμογών, επιτρέποντας την ανταλλαγή δεδομένων μεταξύ ανόμοιων μεταξύ τους χρηστών. Στο επίπεδο αυτό τα δεδομένα μπορεί να υφίστανται κρυπτογράφηση, συμπίεση, κωδικοποίηση MIME και όποια άλλη διαμόρφωση απαιτεί η μορφή δεδομένων ή ο σχεδιαστής του πρωτοκόλλου. Παραδείγματα αποτελούν η μετατροπή αρχείων από κώδικα EBCDIC σε κώδικα ASCII και η μετατροπή της δομής των δεδομένων σε μορφή XML ή αντίστροφα (π.χ. από XML σε έγγραφο τύπου DOC).

(2) Ενδεικτικά Χρησιμοποιούμενα Πρωτόκολλα:

(α) Encryption (TLS-SSL, SSH)
(β) Messaging (IMAP)
(γ) Data compression (JPEG, MPEG)
(δ) File transfer (FTP)

(3) Ευπάθειες: Επιθέσεις τύπου SSL hijacking, encryption downgrade attacks, decryption attacks, encoding attacks, DDoS attacks.

γ. Επίπεδο 5 – Συνόδου:

(1) Το επίπεδο συνόδου είναι αυτό το οποίο ελέγχει τις συνόδους (δηλαδή τις ανταλλαγές δεδομένων) μεταξύ δύο υπολογιστών, του Α και του Β. Ξεκινά, διαχειρίζεται και τερματίζει τη σύνδεση μεταξύ μιας τοπικής και μιας απομακρυσμένης εφαρμογής. Αντιμετωπίζει λειτουργίες FDX (full-duplex, οι Α και Β μιλούν ταυτόχρονα από δύο κανάλια) ή HDX (half-duplex, μιλάει ο Α και μετά απαντάει ο Β από το ένα διαθέσιμο κανάλι), ενώ υποστηρίζει διαδικασίες αποθήκευσης κατάστασης, αναβολής, τερματισμού και επανεκκίνησης.

(2) Ενδεικτικά Χρησιμοποιούμενα Πρωτόκολλα:

(α) Application communication (NetBIOS – standard και όχι πρωτόκολλο)
(β) Multimedia (H.245)

(3) Ευπάθειες: Επιθέσεις τύπου Session Hijacking, Man-in-the-Middle (MITM), Blind attack, Man-in-the-browser, SSH Sniffing.

δ. Επίπεδο 4 – Μεταφοράς:

(1) Το επίπεδο μεταφοράς διεκπεραιώνει τη μεταφορά των δεδομένων από χρήστη σε χρήστη, απαλλάσσοντας έτσι τα ανώτερα επίπεδα από

κάθε φροντίδα να προσφέρουν αξιόπιστη μεταφορά δεδομένων από το ένα άκρο της επικοινωνίας στο άλλο. Το επίπεδο μεταφοράς ελέγχει την αξιοπιστία ενός χρησιμοποιούμενου καναλιού με έλεγχο ροής, καθώς και έλεγχο σφαλμάτων. Ορισμένα πρωτόκολλα καταγράφουν καταστάσεις και συνδέσεις, οπότε κρατούν λογαριασμό των πακέτων και επανεκπέμπουν αυτά που δεν παρελήφθησαν σωστά.

(2) Ενδεικτικά Χρησιμοποιούμενα Πρωτόκολλα:

Data Streaming (TCP, UDP, SCTP)

(3) Ευπάθειες: Επιθέσεις τύπου SYN flood attack, TCP Sequence prediction, TCP Session hijacking, UDP flood attack, UDP-based amplification attacks, και αναγνωριστικές επιθέσεις τύπου packet sniffing, ping sweeping, port scanning, phishing, social engineering και internet information queries.

ε. Επίπεδο 3 – Δικτύου:

(1) Το επίπεδο δικτύου παρέχει τα λειτουργικά και διαδικαστικά μέσα για τη μεταφορά στοιχειοσειρών πακέτων δεδομένων από μια προέλευση σε έναν προορισμό, μέσα από ένα ή περισσότερα ενδιάμεσα δίκτυα, ενώ διατηρεί την ποιότητα εξυπηρέτησης που απαιτεί το επίπεδο μεταφοράς. Το επίπεδο δικτύου εκτελεί λειτουργίες δρομολόγησης, και αναφέρει σφάλματα σχετικά με την παράδοση των πακέτων. Οι δρομολογητές λειτουργούν στο επίπεδο αυτό (όπως και switches layer 3) διακινώντας δεδομένα ανάμεσα σε διασυνδεδεμένα δίκτυα, τα οποία όλα μαζί απαρτίζουν ένα ευρύτερο δίκτυο. Το πλέον αναγνωρίσιμο παράδειγμα πρωτοκόλλου δικτύου είναι το Πρωτόκολλο Διαδικτύου (αγγλ. Internet Protocol, IP).

(2) Ενδεικτικά Χρησιμοποιούμενα Πρωτόκολλα:

(α) Data packets transmission (Ipv4, Ipv6, MPLS – μεταξύ επιπέδου 2 και 3)
(β) Network issues diagnosis (ICMP)
(γ) Packet encryption (Ipsec)
(δ) Addressing (ARP)
(ε) Routing protocols (RIP, GRP, OSPF, EGP, κ.λπ.)

(3) Ευπάθειες: Επιθέσεις τύπου IP Spoofing and jamming, ICMP attack, Smurf attack, Worm-hole, Black hole attacks, Sybil attack, Packet sniffing και selective forwarding attacks.

στ. Επίπεδο 2 – Ζεύξης Δεδομένων:

(1) Το επίπεδο ζεύξης δεδομένων παρέχει τα λειτουργικά και διαδικαστικά μέσα για τη μεταφορά δεδομένων από μια συσκευή ενός τοπικού δικτύου σε άλλη, αλλά και για την ανίχνευση και διόρθωση σφαλμάτων που συμβαίνουν στο φυσικό επίπεδο. Οι μη ιεραρχημένες διευθύνσεις των συσκευών εδώ είναι οι φυσικές (π.χ. MAC διευθύνσεις), δηλαδή είναι προκαθορισμένες και

αποθηκευμένες στις κάρτες δικτύου των επικοινωνούντων κόμβων από το εργοστάσιο.

(2) Ενδεικτικά Χρησιμοποιούμενα Πρωτόκολλα:

(α) Transfer mode (ATM)
(β) Frame routing (Frame Relay)
(γ) Communication between routers (PPP)
(δ) Wireless LAN (IEEE 802.11)
(ε) Wired LAN's (Ethernet)
(στ) Software Defined Networks (Open Flow)

(3) Ευπάθειες: Επιθέσεις τύπου ARP Spoofing, MAC cloning, DoS, Spanning tree attack, VLAN hopping και τύπου DHCP attacks.

ζ. Επίπεδο 1 – Φυσικό:

Το επίπεδο αυτό θα αναλυθεί εκτενώς στην επόμενη παράγραφο, λόγω του γεγονότος ότι, η μελέτη της ασφάλειας επικοινωνιών που βασίζεται στο φυσικό επίπεδο του μοντέλου OSI αποτελεί την κεντρική ιδέα της παρούσας διπλωματικής εργασίας.

3.4 Το φυσικό επίπεδο του μοντέλου OSI – Πόσο ασφαλές είναι;

Το φυσικό επίπεδο είναι το κατώτατο επίπεδιο του μοντέλου OSI και είναι υπεύθυνο για τη φυσική επικοινωνία μεταξύ των τερματικών σταθμών, είναι δε επιφορτισμένο με την κωδικοποίηση και τη μετάδοση των δεδομένων υπό την έννοια των «ηλεκτρο-μηχανικών» όρων της έννοιας της τάσης και των διαφόρων κυματομορφών. Υπό την εξέταση του φυσικού επιπέδου από πλευράς ασφαλείας επικοινωνιών [27] μπορούμε να διευρύνουμε την έννοια φυσικό επίπεδο σε όλους εκείνους τους φυσικούς παράγοντες που υπάρχουν και μετέχουν στη διαδικασία διακίνησης της πληροφορίας μεταξύ των τερματικών σταθμών, όπως το φυσικό μέσο (αέρας, χαλκός, οπτική ίνα, κ.λπ.), τροφοδοσία δικτυακών συσκευών, φυσική πρόσβαση του προσωπικού στις δικτυακές συσκευές, θέση δικτυακών συσκευών στο χώρο (φυλασσόμενος ή μη χώρος), κ.λπ..

Το φυσικό επίπεδο του μοντέλου OSI αποτελεί ίσως το πιο κρίσιμης σημασίας επίπεδο για τη μετάδοση της πληροφορίας, είναι όμως το πιο ευαίσθητο και εύκολα μεταβλητό. Αυτό συμβαίνει γιατί δεν εξαρτάται από τη λογική και τους αυστηρούς κανόνες που μπορούν να εφαρμοσθούν στα ανώτερα επίπεδα αλλά καθαρά από τη σταθερότητα ή τις μεταβολές του ίδιου του περιβάλλοντος, αλλά και τη δυνατότητα ελεύθερης πρόσβασης υποψήφιων επιβουλέων στη μεταδιδόμενη πληροφορία, θέματα τα οποία στο μεγαλύτερο ποσοστό τους δε μπορούν να ελεγχθούν.

Τα χρησιμοποιούμενα πρωτόκολλα στο φυσικό επίπεδο είναι πολλά στον αριθμό τους με τα πιο βασικά όπως παρακάτω:

α. Ethernet 10 BASET, 10BASE2, 10BASE5, 10BASE-TX, 100BASE-FX, 1000BASE-T, 1000BASE-SX
β. EIA RS-232, EIA-422, EIA-423, RS-449, RS-485
γ. USB physical layer
δ. DSL
ε. ISDN
στ. T1 and other T-carrier links, and E1 and other E-carrier links
ζ. Υπέρυθρες
στ. Varieties of 802.11 Wi-Fi physical layers
ζ. Frame Relay
η. Επικοινωνίες οπτικών ινών
θ. ITU Recommendations

Όπως αναφέρθηκε ήδη το μέσο μετάδοσης της πληροφορίας στο φυσικό επίπεδο μπορεί να είναι ο αέρας ο χαλκός, οπτική ίνα, κ.λπ., διαχωρίζοντας έτσι τους τα κανάλια επικοινωνίας σε δύο τύπους, στα ενσύρματα και στα ασύρματα.

Ιδιαίτερα για τις ασύρματες ζεύξεις, η ασφάλεια των οποίων μελετάται σε αυτή την εργασία, το φυσικό επίπεδο είναι εκείνο που εκπέμπει/λαμβάνει τα διαμορφωμένα σήματα μέσω του ασύρματου interface του πομποδέκτη, τα διαμορφώνει/αποδιαμορφώνει και στη συνέχεια τα οδηγεί στο ασύρματο κανάλι ή τα προωθεί στο ανώτερο επίπεδο αντίστοιχα. Εξαιτίας των εγγενών χαρακτηριστικών της ασύρματης μετάδοσης, στο φυσικό επίπεδο είναι δυνατό να λάβουν χώρα επιθέσεις που περιλαμβάνουν φίμωση, παρεμβολές, υποκλοπή δεδομένων και traffic analysis. Τα παραπάνω είδη επιθέσεων, εμπίπτουν στα δύο γενικότερα είδη, όπως αυτά αναλύθηκαν στην παρ. 3.1, στις ενεργητικές και παθητικές επιθέσεις [28].

α. <u>Ενεργητικές επιθέσεις</u>

Οι ενεργητικές επιθέσεις περιλαμβάνουν τη φίμωση (jamming) και την παρεμβολή (interference). Και τα δύο είδη επιθέσεων υλοποιούνται σε γενικές γραμμές με παρόμοιο τρόπο, με την εκπομπή από τρίτο πομπό, ανεπιθύμητων για το σύστημα πομπού-δέκτη του φίλιου τηλεπικοινωνιακού συστήματος, σημάτων σε συγκεκριμένες περιοχές του φάσματος. Η διαφορά μεταξύ τους έγκειται στο στόχο στον οποίο επιτίθενται. Ο στόχος για τη φίμωση είναι ο πομπός και το επιθυμητό αποτέλεσμα είναι να κρατάει διαρκώς απασχολημένο το ασύρματο κανάλι, εκπέμποντας πάντα σε μεγαλύτερη ισχύ, καθιστώντας έτσι τον πομπό, μη λειτουργικό (όχι πραγματικά αλλά σε όρους εκπομπής του επιθυμητού σήματος). Από την άλλη ο στόχος της παρεμβολής είναι να υποβαθμίσει την ποιότητα του ληφθέντος σήματος στο δέκτη, χειροτερεύοντας το σηματοθορυβικό λόγο.

Οι περισσότερες επιθέσεις φίμωσης είναι κακόβουλες επιθέσεις, από την άλλη πλευρά η παρεμβολή δύναται να συμβεί και κατά ακούσιο τρόπο, από κοντινούς ανταποκριτές του ιδίου τηλεπικοινωνιακού συστήματος, όταν αυτοί εκπέμπουν στις ίδιες περιοχές συχνοτήτων μεταξύ τους.

Σύμφωνα με τις διαφορετικές τεχνικές που υλοποιούνται οι παραπάνω επιθέσεις, για τη φίμωση διακρίνουμε τις παρακάτω περιπτώσεις:

(1) Spot jamming: Αφορά την εκπομπή μέγιστης δυνατής ισχύος σε μία μοναδική συχνότητα ώστε να επικαλυφθεί/εξουδετερωθεί τελείως η φίλια εκπομπή του επιθυμητού σήματος.

(2) Sweep jamming: Είναι η φίμωση ενός συνόλου συχνοτήτων, μεταξύ των οποίων ο παρεμβολέας μεταπηδά διαρκώς, Η υπόψη τεχνική χρησιμοποιείται για τη φίμωση συστημάτων αναπήδησης συχνότητας, η απαραίτητη προϋπόθεση όμως είναι ο επιτιθέμενος να γνωρίζει το μοτίβο εναλλαγής μεταξύ των συχνοτήτων που χρησιμοποιεί το οικείο σύστημα επικοινωνιών (TRANSEC). Επιπλέον, εφαρμόζεται σε μία συχνότητα κάθε φορά και όχι στο σύνολο συχνοτήτων.

(3) Barrage jamming: Αφορά στη φίμωση περιοχής συχνοτήτων, με σκοπό την καθολική απαγόρευσή της από τους φίλιους χρήστες του συστήματος επικοινωνιών. Το μειονέκτημά της είναι ότι δεδομένης ισχύος εξόδου του παρεμβολέα, όσο πιο μεγάλη είναι η προς απαγόρευση περιοχής συχνοτήτων, τόσο πιο μικρή επίδραση έχει η φίμωση, αφού η ισχύς ισοκατανέμεται στο προς απαγόρευση φάσμα.

(4) Deceptive jamming: Στην περίπτωση αυτή εκπέμπουν δεδομένα στο δίκτυο, τα οποία οι χρήστες τα λαμβάνουν ως κανονικά πακέτα δεδομένων, εξαπατώντας έτσι το δέκτη ως προς την πραγματική πηγή των εισερχόμενων δεδομένων.

Επιπλέον, για την περίπτωση της παρεμβολής, διακρίνουμε τις παρακάτω περιπτώσεις:

(5) Sustained Interference:

Ο επιτιθέμενος στέλνει διαρκώς δεδομένα υπό τη μορφή σήματος παρεμβολής, με σκοπό να επηρεάσει την κανονική επικοινωνία. Ο δέκτης λαμβάνει τα δεδομένα υπό τη μορφή θορύβου, ο σηματοθορυβικός λόγος συνεχώς μικραίνει και η επικοινωνία με αυτό τον τρόπο χειροτερεύει.

(6) Random interference: Αυτού του είδους η παρεμβολή δεν γίνεται κατά συνεχόμενο τρόπο όπως στο προηγούμενο παράδειγμα αλλά σε τυχαία διαστήματα και με τυχαία συχνότητα.

(7) On-Demand interference: Στην περίπτωση αυτή γίνεται χρήση της παρεμβολής ώστε να κρατιέται ο δίαυλος ανενεργός, εάν βρίσκεται σε ανενεργή κατάσταση. Με το που επιχειρήσει ο φίλιος πομπός να αποστείλει δεδομένα στο χρήστη, με άλλα λόγια να βγει από την ανενεργή κατάσταση, το σήμα παρεμβολής αποστέλλεται άμεσα, ταυτόχρονα, με αποτέλεσμα τελικά η επιθυμητή πληροφορία να μη φτάνει ποτέ στο δέκτη.

β. Παθητικές επιθέσεις

Οι παθητικές επιθέσεις, όπως προαναφέρθηκε, αφορούν σε δύο υποκατηγορίες, αυτή της υποκλοπής (eavesdropping) και ανάλυση κίνησης (traffic

analysis). Στηρίζουν τη λειτουργία τους στο απλούστερο εκ των χαρακτηριστικών του ασύρματου καναλιού, αυτό της ευρείας εκπομπής. Το ασύρματο κανάλι, εκ των πραγμάτων και εκ της φύσεώς του δεν είναι δυνατό να μπει σε συγκεκριμένο δρόμο/διαδρομή. Η ασύρματη εκπομπή υπόκειται στους νόμους της ανάκλασης, διάθλασης και περίθλασης, όπως κάθε Η/Μ κύμα και κατά συνέπεια το κύμα αυτό είναι πολύ πιθανό έως σίγουρο να φτάσει σε κάθε ανεπιθύμητο δέκτη, ο οποίος δύναται να το αναλύσει και να το χρησιμοποιήσει.

(1) Υποκλοπή: Η υποκλοπή σε ένα ασύρματο σύστημα στην κλασική του μορφή, χωρίς τεχνικές προστασίας που θα αναφερθούν παρακάτω, ακόμα και αν χρησιμοποιεί κατευθυντικές κεραίες, θα πρέπει να θεωρείται δεδομένη. Με άλλα λόγια, το σήμα στην διαμορφωμένη του από το φυσικό επίπεδο μορφή θα πρέπει να θεωρείται σίγουρο ότι θα φτάσει στον επιτιθέμενο. Από εκεί και πέρα, το αν ο επιτιθέμενος θα καταφέρει από το καταγραφέν και υποκλαπέν σήμα να εξάγει την αρχική πληροφορία, είναι ζήτημα που θα πρέπει να συνεξετασθεί με τεχνικές ασφαλείας που υλοποιήθηκαν στα ανώτερα επίπεδα του μοντέλου OSI, όπως κωδικοποίηση και κρυπτογράφηση.

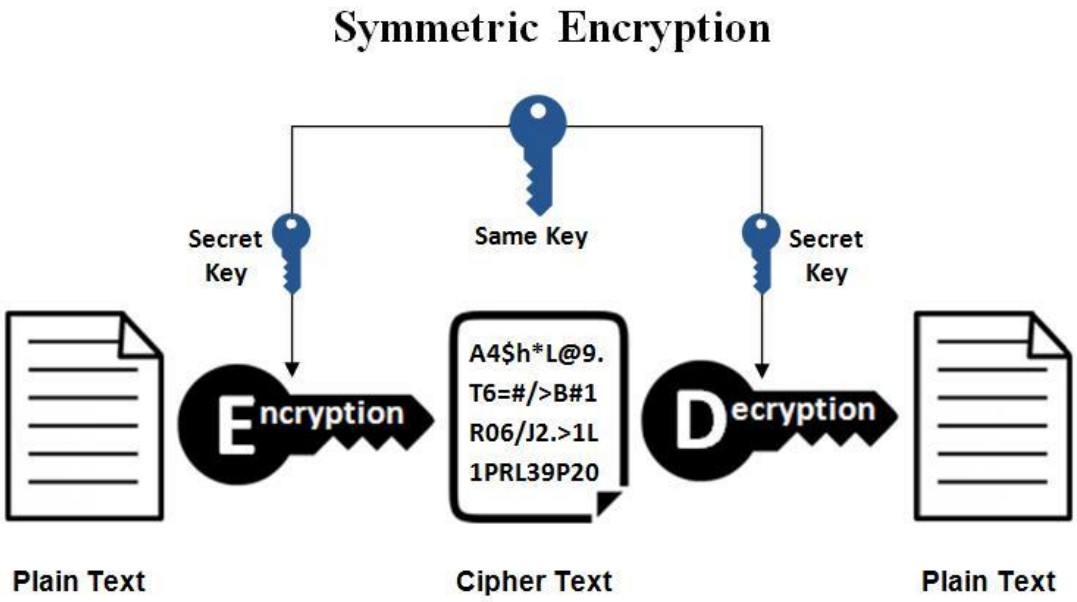
(2) Ανάλυση κίνησης: Η ανάλυση κίνησης αναφέρεται στην εξαγωγή χρήσιμης πληροφορίας από την αλλαγή στη ροή πληροφορίας στο δίκτυο, η οποία μπορεί να μεταφραστεί σε εκτέλεση ή μη συγκεκριμένων ενεργειών. Για παράδειγμα, η αποστολή μηνυμάτων συγκεκριμένη ώρα κάθε μέρα μπορεί σε ένα δίκτυο να υποδηλώνει ότι τα μηνύματα αυτά είναι αναφορές καταστάσεως ή αναφορές λειτουργικότητας ενός δικτύου.

4. ΑΣΦΑΛΕΙΑ ΦΥΣΙΚΟΥ ΕΠΙΠΕΔΟΥ

4.1 Γενικά

Στα σύγχρονα συστήματα επικοινωνιών, οι αρχές ασφαλείας επικοινωνιών, όπως αυτές αναλύθηκαν στην παράγραφο 3.2 της παρούσας μελέτης, πραγματοποιούνται κυρίως στα ανώτερα επίπεδα του μοντέλου OSI. Ιδίως η αρχή της εμπιστευτικότητας, η οποία μας ενδιαφέρει στην παρούσα διπλωματική εργασία, εξασφαλίζεται με τη χρήση τεχνικών κρυπτογράφησης-αποκρυπτογράφησης:

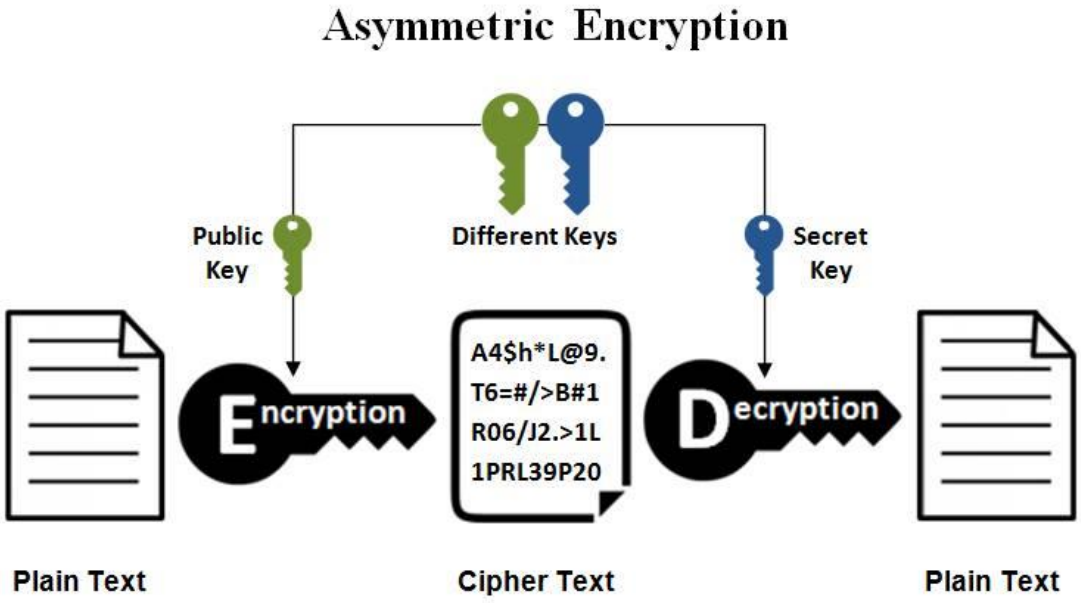
α. Ιδιωτικού κλειδιού (συμμετρική κρυπτογράφηση), οπότε απαιτείται παράλληλα με τη λειτουργία του τηλεπικοινωνιακού συστήματος ένας αξιόπιστος μηχανισμός διανομής των υπόψη κλειδιών από μια έμπιστη πηγή στους τελικούς χρήστες. Όλοι οι χρήστες του δικτύου διαθέτουν τώρα τα ίδια κλειδιά, οπότε από αυτή τη στιγμή και μετά οποιοδήποτε μήνυμα παραληφθεί, μπορεί στα ανώτερα επίπεδα με τη χρήση αυτών να αποκρυπτογραφηθεί και να αναγνωσθεί.



Σχήμα 4.1.1

β. Δημόσιου κλειδιού (ασύμμετρη κρυπτογράφηση), βάση της οποίας αποτέλεσε η εργασία των Diffie-Hellman το 1976, όπου προτάθηκε μία επαναστατική τεχνική που επιλύει το πρόβλημα της ανταλλαγής κλειδιού από απόσταση, χωρίς να απαιτείται άμεση επαφή για τον παραπάνω σκοπό, θέτοντας έτσι τις βάσεις για την κρυπτογραφία δημοσίου κλειδιού. Πράγματι, το 1977 οι Ronald L. Rivest, Adi Shamir και Leonard M. Adleman (τότε στο MIT) πρότειναν ένα ιδιαίτερα επιτυχημένο (έως και σήμερα) κρυπτοσύστημα δημοσίου κλειδιού, γνωστό ως RSA, το οποίο βασίζει τη λειτουργία του σε δύο κλειδιά, το δημόσιο και το ιδιωτικό κλειδί. Το δημόσιο κλειδί του χρήστη Β είναι γνωστό σε όλους τους χρήστες του δικτύου, ενώ το ιδιωτικό μόνο σε αυτόν. Έτσι, όταν ο χρήστης Α θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον Β, το κρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί του Β (το οποίο είναι γνωστό σε όλους), ενώ ο

Β το αποκρυπτογραφεί με το ιδιωτικό του κλειδί (το οποίο δεν γνωρίζει κανένας άλλος στο δίκτυο).



Σχήμα 4.1.2

Οι παραπάνω μέθοδοι, αν και εξασφαλίζουν την εμπιστευτικότητα της διακίνησης πληροφορίας έως ένα βαθμό, παρουσιάζουν μειονεκτήματα και πολλές φορές υστερούν σε υλοποίηση, συνεπώς ενισχύεται με αυτό τον τρόπο η ανάγκη για ενίσχυση της ασφάλειας επικοινωνιών στο φυσικό επίπεδο, καθώς:

α. Στην περίπτωση της συμμετρικής κρυπτογράφησης ο υπόψη μηχανισμός διανομής κλειδιών θα πρέπει να διασφαλίσει ότι τα κλειδιά κρυπτογράφησης θα φτάσουν αποκλειστικά στους εξουσιοδοτημένους τελικούς χρήστες, οι τελικοί χρήστες ότι δε θα χάσουν τα υπόψη κλειδιά, ούτε θα παραδώσουν αυτά σε κάποιον κακόβουλο τρίτο χρήστη. Σε διαφορετική δε περίπτωση όλη η ασφάλεια του συστήματος επικοινωνιών έχει καταρρεύσει, καθώς οποιοσδήποτε έχει στη διάθεσή του το κλειδί κρυπτογράφησης/αποκρυπτογράφησης μπορεί να αποκρυπτογραφήσει οποιοδήποτε μήνυμα.

β. Στην ασύμμετρη κρυπτογράφηση εξακολουθεί να υπάρχει μια οντότητα/αρχή, η οποία εγγυάται ότι η παραγωγή και η διανομή του μοναδικού ζεύγους κλειδιών (δημόσιου και ιδιωτικού) είναι απαραβίαστη και μοναδική για κάθε χρήστη, ξανά υπεισέρχεται δηλαδή το τρίτο πρόσωπο, το οποίο όλοι οι χρήστες απαιτείται να εμπιστευτούν.

γ. Παρότι η πληροφορία κρυπτογραφείται, όπως προαναφέρθηκε και ιδιαίτερα για το ασύρματο κανάλι, μπορεί κάλλιστα να υποκλαπεί από οποιονδήποτε. Από εκεί και πέρα θα πρέπει να καταστεί σαφές ότι οποιαδήποτε σύγχρονη μέθοδος κρυπτογράφησης και να χρησιμοποιηθεί η πληροφορία παραμένει πιθανό να μπορέσει να ανακτηθεί στην αρχική της μορφή καθώς στη σύγχρονη κρυπτογραφία, κεντρικό ρόλο διαδραματίζει η έννοια της αποδείξιμης ασφάλειας και ο κλάδος της υπολογιστικής πολυπλοκότητας. Με άλλα λόγια, όλοι

οι σύγχρονοι αλγόριθμοι κρυπτογράφησης προσπαθούν να επιτύχουν ένα επίπεδο πολυπλοκότητας, το οποίο είναι αρκούντως ικανό να τους καταστήσει σχετικά ασφαλείς έναντι κάποιου επιτιθέμενου που χρησιμοποιεί υπολογιστικές τεχνικές βασισμένες στις τελευταίες, τρέχουσες τεχνολογικές εξελίξεις. Κανείς δεν εγγυάται δηλαδή ότι με τα κατάλληλα υπολογιστικά εργαλεία και σε κατάλληλο χρόνο, ένα μήνυμα κρυπτογραφημένο με κάποιο σύγχρονο αλγόριθμο κρυπτογράφησης είναι αδύνατο να αναλυθεί και να αποκαλυφθεί στην αρχική του μορφή αλλά μάλλον απίθανο. Οι λόγοι που οι αλγόριθμοι κρυπτογράφησης επιλέγεται να παραμένουν «σχετικά» και όχι «απολύτως» ασφαλείς είναι τα γεγονότα ότι:

(2) Η απόλυτη ασφάλεια συνεπάγεται σε επιβάρυνση του συστήματος επικοινωνιών με εξαιρετικά μεγάλο όγκο πληροφορίας, τη δημιουργία δηλαδή στα διακινούμενα μηνύματα υπερβολικού overhead, μεγαλύτερου μάλιστα από την ίδια την καθαρή πληροφορία, αλλά και πολυπλοκότητα στην κατασκευή, κάτι που είναι ασύμφορο. Η πλήρης μυστικότητα και ο αλγόριθμος που μπορεί να την επιτύχει υπάρχει, και αυτό αποδείχτηκε μαθηματικά από τον Claude Shannon, πλην όμως με το παραπάνω τίμημα.

(2) Δε θα πρέπει ποτέ να λησμονιέται ποτέ, όπως αναλύθηκε στην παρ.3.2, η αξία της πληροφορίας σε σχέση με το χρόνο και κατά συνέπεια με το χρόνο που θέλει κάποιος επιτιθέμενος να «σπάσει» ένα κρυπτογραφημένο μήνυμα. Με άλλα λόγια δεν ενδιαφέρει το εάν επιτιθέμενος καταφέρει να εξάγει το αρχικό μήνυμα από το κρυπτογράφημα εάν, λόγω της υπολογιστικής πολυπλοκότητας του αλγόριθμου, στο χρόνο που απαιτείται να το κάνει το μήνυμα έχει χάσει την αξία του και πομπός και δέκτης έχουν αλλάξει κλειδί κρυπτογράφησης.

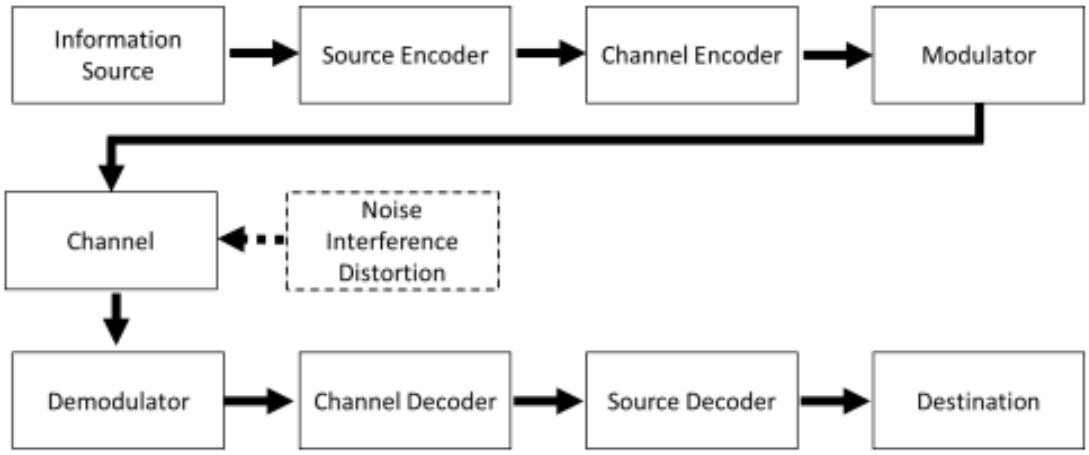
δ. Ενώ οι σύγχρονοι αλγόριθμοι μπορεί να έχουν μεγάλη ανθεκτικότητα σε επιθέσεις, απαιτώντας συστήματα με μεγάλη υπολογιστική ισχύ ώστε να σπάσουν, πολλές φορές είναι δύσκολο οι κλασικές τεχνικές κρυπτογράφησης να εφαρμοστούν σε αναδυόμενες νέες τεχνολογίες. Ένα τέτοιο παράδειγμα αποτελούν τα ασύρματα ad-hoc δίκτυα, τα οποία αποτελούνται από πολλές διαφορετικού τύπου και υπολογιστικής ισχύος συσκευές. Σε τέτοιου είδους δίκτυα είναι εξαιρετικά δύσκολη η ανάπτυξη τεχνικών κρυπτογράφησης, τόσο ιδιωτικού, όσο και δημόσιου κλειδιού, αφενός γιατί σε ότι αφορά στην πρώτη κατηγορία τίθεται το ερώτημα για το ποιος είναι ο τρόπος με τον οποίο δύνανται να διαμοιραστούν με ασφαλή τρόπο κλειδιά κρυπτογράφησης σε ad-hoc συσκευές, ενώ στη δεύτερη υπάρχει πάντα η ποικιλομορφία και οι διαφορετικές δυνατότητες των συσκευών που απαρτίζουν ένα τέτοιο δίκτυο.

Πλέον των παραπάνω, σε αντίθεση με τις κλασικές τεχνικές, πολλά αποτελέσματα που προέκυψαν από την ανάπτυξη της θεωρίας της πληροφορίας, της επεξεργασίας σήματος αλλά και της ίδιας της κρυπτογραφίας, έδειξαν ότι μπορούν να κερδηθούν πολλά στον τομέα της ασφάλειας εάν αξιοποιηθούν χαρακτηριστικά του φυσικού επιπέδου. Για παράδειγμα, ενώ μέχρι πρότινος με την κλασική προσέγγιση ο λευκός θόρυβος και οι διαλείψεις αντιμετωπίζονταν ως πρόβλημα στις ασύρματες επικοινωνίες, η θεωρία της πληροφορίας κάνει λόγο για αποτελέσματα από τη χρήση τους που μπορούν να μας βοηθήσουν να κρύψουμε μηνύματα από κάποιον κακόβουλο χρήστη ή να αυθεντικοποιήσουμε χρήστες και

συσκευές σε ένα δίκτυο, χωρίς να υπάρχει ανάγκη να κάνουμε χρήση ενός κλειδιού. Τα αποτελέσματα αυτά, εάν μπορούν να εφαρμοστούν ευρέως σε συστήματα επικοινωνιών, με έναν αποδοτικό τρόπο από πλευράς κόστους, υπολογιστικής πολυπλοκότητας αλλά και πλεονάζουσας πληροφορίας που ενδεχομένως εισάγουν στο σύστημα επικοινωνιών, συνιστούν όλους εκείνους τους μηχανισμούς ασφαλείας επικοινωνιών που καλείται ασφάλεια φυσικού επιπέδου.

4.2 Κωδικοποίηση

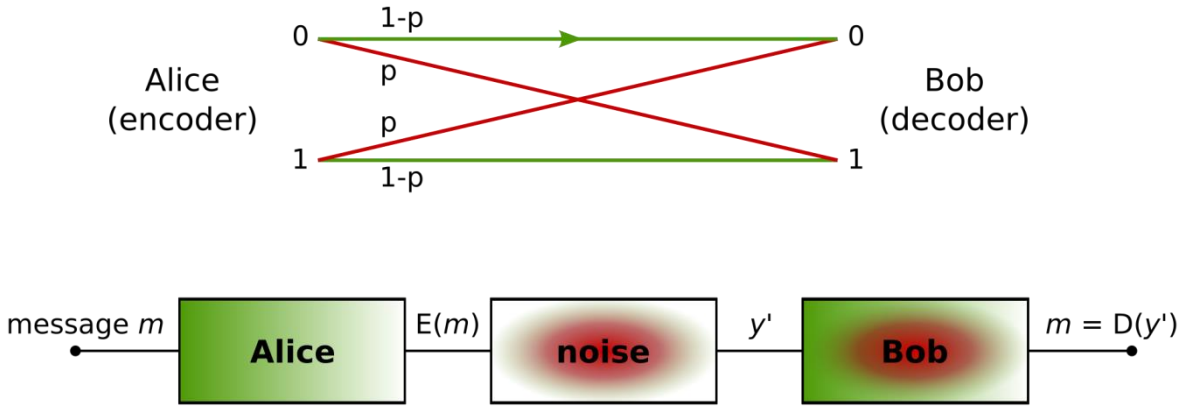
Για να γίνει λίγο πιο σαφές για τον αναγνώστη το περιβάλλον υπό το οποίο μελετούνται οι τεχνικές ασφαλείας φυσικού επιπέδου, είναι απαραίτητο παρακάτω να γίνει μια σύντομη αναφορά στην κωδικοποίηση, ώστε να μπορέσουν να συνδεθούν μεταξύ τους έννοιες όπως κέρδος αυτής και χωρητικότητα καναλιού.



Σχήμα 4.2.1

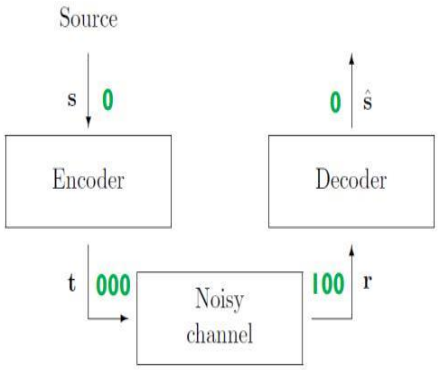
Σκοπός της κωδικοποίησης των δεδομένων είναι η αποτελεσματικότερη διακίνησή τους μέσα σε ένα δίαυλο επικοινωνίας. Ο δίαυλος αυτός μπορεί να είναι από ένα τυπωμένο κύκλωμα σε κάρτα έως συνεστραμμένο ζεύγος χαλκού, οπτική ίνα ή ο ίδιος ο αέρας. Κάθε ένα από αυτά τα μέσα που αναφέρθηκαν υποφέρει από διαφορετικά προβλήματα-μηχανισμούς οι οποίοι επιδρούν στη διάδοση όπως ανακλάσεις του εκπεμπόμενου σήματος, εξασθένηση, παραμόρφωση φάσης και πλάτους, ενδοδιαμόρφωση, ηχώ, crosstalk, ολίσθηση συχνότητας κ.λπ.. Όλοι αυτοί οι μηχανισμοί επιδρούν με δυσμενή τρόπο στη διάδοση και συνεπώς στην αξιόπιστη μετάδοση της πληροφορίας.

Το τηλεπικοινωνιακό κανάλι, όπως έχει ξαναφερθεί χαρακτηρίζεται από ένα σύνολο πιθανοτήτων, βάσει των οποίων ο δέκτης μπορεί να εκτιμήσει σωστά ότι έχει λάβει το σύμβολο που πραγματικά εκπέμφθηκε από τον πομπό. Έτσι λοιπόν, έστω το απλούστερο είδος καναλιού, το οποίο ονομάζεται Δυαδικό Συμμετρικό Κανάλι (Binary Symmetric Channel – BSC). Για μια είσοδο στο κανάλι από την πλευρά του πομπού του bit πληροφορίας «0», η πιθανότητα ο δέκτης να εκτιμήσει ότι έλαβε το bit «1» είναι p, ενώ ότι έλαβε το σωστό bit «0» είναι 1-p. Αντίστοιχα ισχύει και για το εκπεμπόμενο bit «0» στο κανάλι.



Σχήμα 4.2.2

Η πιθανότητα p, λήψης του εσφαλμένου bit πληροφορίας στο δέκτη, αφού αυτό έχει ταξιδέψει μέσα στο τηλεπικοινωνιακό κανάλι, αποτελεί προϊόν φυσικών διεργασιών στο κανάλι, κατά συνέπεια δεν μπορεί να μειωθεί κάτω από κάποιο επίπεδο ώστε το BER του συστήματος να φτάσει στο επιθυμητό επίπεδο. Αν για παράδειγμα μοντελοποιηθεί το παραπάνω σύστημα ως ένας σκληρός δίσκος Η/Υ που αποθηκεύει δεδομένα σε bit πληροφορίας «0» και «1», τότε η πιθανότητα p θα ήταν ένας συνδυασμός παραγόντων της φυσικής συμπεριφοράς των κονεκτόρων, της κεφαλής εγγραφής, κ.λπ., οι οποίοι θα δημιουργήσουν σφάλματα. Απαραίτητο λοιπόν αντίμετρο για το παραπάνω γεγονός, είναι το σύστημα να σχεδιαστεί με τρόπο ώστε να δέχεται τα σφάλματα, αλλά να διαθέτει μηχανισμούς που τα εντοπίζουν και τα διορθώνουν. Αυτό είναι και το νόημα της χρήσης κωδικών εύρεσης και διόρθωσης λαθών.



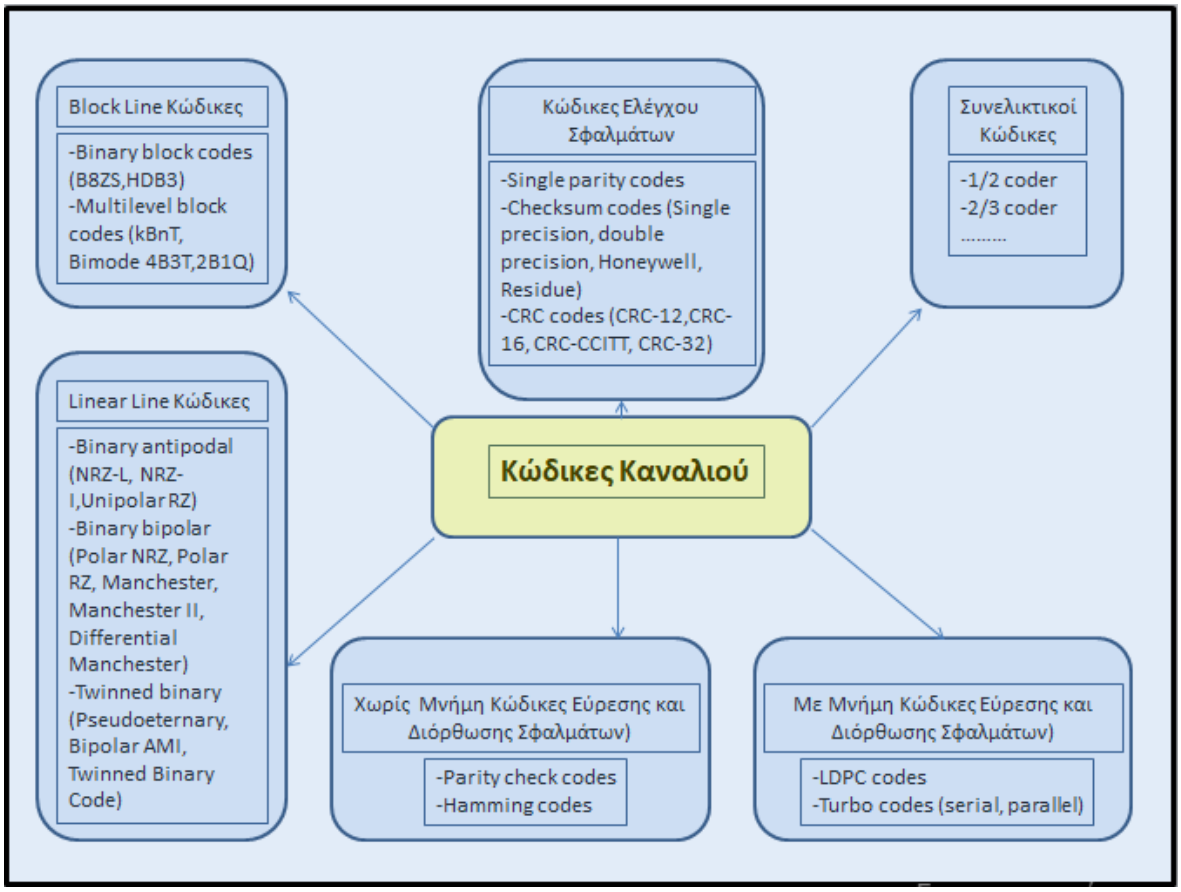
Source (s)	Transmitted (t)
0	000
1	111

Recevied (r)	Decoded (ŝ)
000	0
001	0
010	0
011	1
100	0
101	1
110	1
111	1

Σχήμα 4.2.3

Σε μερικές περιπτώσεις οι φυσικές διεργασίες που λαμβάνουν χώρα στο κανάλι είναι τόσο ισχυρές, ώστε να προκαλούν πολύ μεγάλα ποσοστά λαθών. Έτσι λοιπόν, αρχικά για επικοινωνία σε μικρού μήκους γραμμές μεταφοράς και για χαμηλούς ρυθμούς, χρησιμοποιούνται απλοί γραμμικοί κώδικες ώστε να μειώσουν αυτό το ποσοστό λαθών. Αυτοί οι κώδικες μπορεί να είναι μονοπολικοί ή διπολικοί και ακόμα μπορεί να περιέχουν ή όχι πληροφορία για σήμα ρολογιού στο εσωτερικό τους.

Μια γενική κατηγοριοποίηση των χρησιμοποιούμενων κωδικών καναλιού από διάφορα ενσύρματα ή ασύρματα συστήματα, χωρίς να αναλυθεί η περαιτέρω χρήση τους δίνεται στο παρακάτω σχήμα.



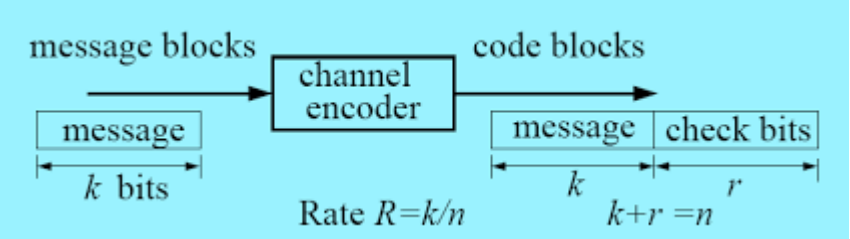
Σχήμα 4.2.4

Όταν το εύρος ζώνης του καναλιού είναι περιορισμένο απαιτούνται πιο αποδοτικοί κώδικες οι οποίοι μπορεί να χρησιμοποιούν σύμβολα διαφόρων επιπέδων και να εναλλάσσουν τα εισερχόμενα bit δεδομένων ώστε να επιτρέπουν στο δέκτη το συγχρονισμό. Οι πιο περίπλοκοι και αποδοτικοί κώδικες χρησιμοποιούν block κωδικοποίηση ή συνελικτική κωδικοποίηση ώστε να βελτιώσουν την απόδοση της μετάδοσης.

Στους linear line κώδικες, όπως οι Polar NRZ και Bipolar AMI, τα μεταδιδόμενα δεδομένα εξαρτώνται γραμμικά από τα δεδομένα-bit πληροφορίας, ενεργούν δηλαδή σε stream δεδομένων.

Από την άλλη πλευρά, ο HDB3 ανήκει στους block line κώδικες, λειτουργεί δηλαδή σε block πληροφορίας. Χρησιμοποιούνται γενικά για να κωδικοποιήσουν k bit πληροφορίας σε n λιγότερα σύμβολα. Οι πιθανοί συνδυασμοί για τα k και n πρέπει να ικανοποιούν τη σχέση: $2^k \leq L^n$, όπου L είναι ο αριθμός των διαθέσιμων σταθμών κβαντισμού του σήματος. Όταν η ανισότητα δεν ικανοποιείται, ο πλεονασμός μπορεί να χρησιμοποιηθεί για αποσφαλμάτωση, πληροφορίες χρονισμού ή για να ελαχιστοποιήσει το μετρικό RDS (Running Digital Sum). Το RDS είναι μια συνάρτηση, η οποία προσθέτει τα ψηφιακά επίπεδα που

εκπέμπονται. Κάθε «1» που εκπέμπεται αυξάνει το RDS κατά ένα, ενώ αντίστροφα, κάθε «0» το ελαττώνει κατά ένα.



Σχήμα 4.2.5

Η άλλη χρήση των block κωδίκων είναι να επιλύσουν το πρόβλημα συγχρονισμού του δέκτη, όταν ο δίαυλος δεν εμφανίζει καμία κίνηση για μεγάλο χρόνο εξαιτίας της μετάδοσης πολλών μηδενικών bit ή πολλών «1». Οι B8ZS και HDB3 κώδικες είναι παραδείγματα τέτοιων κωδίκων που προλαμβάνουν τη μετάδοση πολλών μηδενικών. Οι block κώδικες έχουν το μειονέκτημα ότι απαιτούν το framing του εισερχόμενου block. Το framing αυξάνει το overhead των μεταδιδόμενων δεδομένων καθώς και την κατασκευαστική πολυπλοκότητα πομπού και δέκτη.

4.3 Κώδικες γραμμής

Οι κώδικες γραμμής ουσιαστικά χρησιμοποιούνται για τη μετάδοση ενός σήματος μέσα σε μια γραμμή μεταφοράς, δεδομένων δηλαδή υπό ψηφιακή μορφή. Μερικοί κώδικες γραμμής αποτελούν στην ουσία μια ψηφιακή διαμόρφωση ή μετάδοση βασικής ζώνης και χρησιμοποιούνται όταν μια γραμμή μεταφοράς μπορεί να μεταδώσει DC σήματα.

Η κωδικοποίηση γραμμής γίνεται αναπαριστώντας το προς μετάδοση ψηφιακό σήμα με μια κυματομορφή η οποία είναι συγκεκριμένων χαρακτηριστικών για το εκάστοτε καθορισμένο φυσικό μέσο και κατ' επέκταση και για τον εξοπλισμό στην πλευρά της λήψης. Η μορφή τότε που λαμβάνει η τάση, το ρεύμα ή ο αριθμός εγχεόμενων φωτονίων σε σχέση με το χρόνο, τα οποία στοιχεία χρησιμοποιούνται για να αναπαραστήσουν τα ψηφιακά δεδομένα, ονομάζεται κωδικοποίηση γραμμής. Οι πιο κοινοί τύποι κωδικοποίησης γραμμής είναι οι τύποι unipolar, polar, bipolar και Manchester κωδικοποίησης.

Αφού τα ψηφιακά δεδομένα αναπαρασταθούν με τον παραπάνω τρόπο, υπάρχουν οι παρακάτω επιλογές για το σήμα που δημιουργείται.

α. Το προς μετάδοση σήμα βασικής ζώνης να εγχυθεί απευθείας σε μια γραμμή μεταφοράς με τη μορφή εναλλαγών τάσης, ρεύματος, φωτονίων σε συνάρτηση με το χρόνο.

β. Το προς μετάδοση σήμα βασικής ζώνης να υποστεί περαιτέρω επεξεργασία, μέσω της pulse shaping διαδικασίας (για να περιοριστεί το εύρος ζώνης του) και στη συνέχεια να διαμορφωθεί (για να οδηγηθεί σε επιθυμητή

φέρουσα) έτσι ώστε να δημιουργηθεί τελικά ένα σήμα RF και τελικώς να εκπεμφθεί στον ελεύθερο χώρο.

4.4 Κωδικοποίηση και χωρητικότητα

Για ένα κανάλι περιορισμένου εύρους ζώνης, το μέγιστο άνω όριο για αξιόπιστη ψηφιακή μετάδοση δίνεται από το νόμο των Hartley-Shannon [19]. Αυτός ο νόμος δείχνει τη σχέση μεταξύ του εύρους ζώνης του καναλιού και του λόγου σήματος προς θόρυβο με τη μέγιστη χωρητικότητα του καναλιού και καθορίζει το μέγιστο αριθμό συμβόλων που μπορούν να μεταδοθούν στη μονάδα του χρόνου. Διατυπώνεται ως εξής:

C = B * log2(1 + SNR) (σε symbols/second)

όπου:

C=χωρητικότητα του καναλιού
B=εύρος ζώνης καναλιού
SNR=λόγος σήματος προς θόρυβο

Η εξίσωση αυτή δείχνει ότι ο μέγιστος ρυθμός με τον οποίο μπορούμε να στείλουμε δεδομένα στο δίαυλο χωρίς σφάλματα περιορίζεται από το εύρος ζώνης του καναλιού, το επίπεδο ισχύος του σήματος και το επίπεδο ισχύος του θορύβου. Το άνω αυτό όριο χωρητικότητας του καναλιού καθορίζεται για συγκεκριμένο κανάλι. Είναι η μέγιστη χωρητικότητα μετάδοσης που μπορεί να επιτευχθεί σε ένα κανάλι με δεδομένο το σχήμα κωδικοποίησης και εκπομπής. Πιο αναλυτικά, από το νόμο αυτό εξάγονται τα παρακάτω συμπεράσματα:

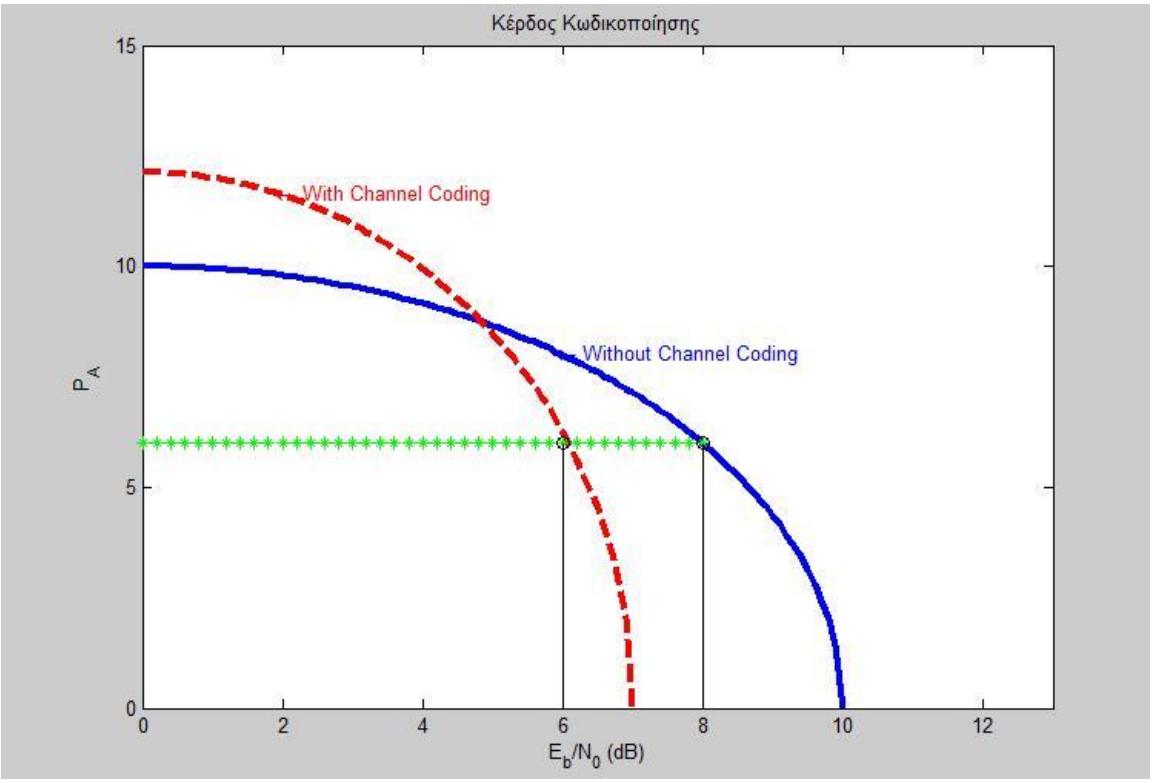
- Το bandwidth περιορίζει πόσο γρήγορα τα σήματα πληροφορίας μπορούν να αποσταλούν στο δεδομένο κανάλι.
- Ο σηματοθορυβικός λόγος περιορίζει τον όγκο της πληροφορίας, ο οποίος μπορεί να συμπιεσθεί σε κάθε αποστελλόμενο σύμβολο. Η αύξηση του σηματοθορυβικού λόγου κάνει τα σύμβολα πιο ανθεκτικά απέναντι στο θόρυβο.

- Για να αυξηθεί ο ρυθμός μετάδοσης της χρήσιμης πληροφορίας τότε θα πρέπει να υπάρξει ένα trade off μεταξύ του SNR και του δεδομένου Bandwidth του καναλιού.

- Θεωρητικά για ένα κανάλι χωρίς καθόλου θόρυβο, ο λόγος SNR θα γινόταν άπειρος και συνεπώς θα ήταν δυνατό να αποστείλουμε άπειρη ποσότητα πληροφορίας σε ένα πολύ μικρό εύρος ζώνης.

Τώρα όταν τα δεδομένα είναι κωδικοποιημένα, το κανάλι μπορεί να μεταδώσει δεδομένα με το ίδιο bit rate και να «ανεχθεί» μικρότερο σηματοθορυβικό λόγο και να έχει ταυτόχρονα την ίδια αξιοπιστία. Αυτό ονομάζεται **κέρδος κωδικοποίησης** και εκφράζεται σε dB. Στο παρακάτω διάγραμμα φαίνεται το κέρδος κωδικοποίησης σε dB για δεδομένη στάθμη θορύβου σε συγκεκριμένο τηλεπικοινωνιακό δίαυλο. Συνεπώς, όπως μπορεί κανείς εύκολα να διακρίνει, είναι φανερό ότι μπορούμε να ανταλλάξουμε αυτή την πολύτιμη διαφορά σηματοθορυβικού λόγου είτε με εύρος ζώνης που καταλαμβάνουμε στο δίαυλο,

είτε να αυξήσουμε την πραγματική πληροφορία, δηλαδή το bit rate, καταλαμβάνοντας το ίδιο εύρος ζώνης.



Σχήμα 4.4.1

Ο σκοπός όλης της θεωρίας, η οποία έχει αναπτυχθεί για την κωδικοποίηση καναλιού είναι να βρεθούν κώδικες που μπορούν να εκτελέσουν γρήγορη μετάδοση της χρήσιμης πληροφορίας, περιέχουν πολλές κωδικές λέξεις (μεγάλη περιεκτικότητα) και τέλος μπορούν να διορθώσουν ή τουλάχιστον να ανιχνεύσουν σφάλματα που έχουν συμβεί. Συνήθως η επιλογή ενός κώδικα καναλιού για μια συγκεκριμένη εφαρμογή αποτελεί ένα trade off στους παραπάνω παράγοντες και οι απαιτήσεις από ένα συγκεκριμένο κώδικα καθορίζονται από τα επίπεδα πιθανότητας σφάλματος για ένα συγκεκριμένο δίαυλο.

Υπάρχει μία οριακή τιμή του σηματοθορυβικού λόγου E_b/N_0, κάτω από την οποία δεν είναι εφικτή η αλάνθαστη μετάδοση σε οποιοδήποτε ρυθμό μετάδοσης πληροφορίας. Η οριακή τιμή του σηματοθορυβικού λόγου E_b/N_0 ονομάζεται **όριο του Shannon**. Η εργασία του Shannon παρείχε μία θεωρητική απόδειξη για την ύπαρξη κωδικών που μπορούν να βελτιώσουν την πιθανότητα σφάλματος P, ή να μειώσουν τον απαιτούμενο σηματοθορυβικό λόγο E_b/N_0, από τα επίπεδα σχημάτων δυαδικής διαμόρφωσης χωρίς κωδικοποίηση στα επίπεδα που προσεγγίζουν το όριο. Για παράδειγμα για πιθανότητα σφάλματος της τάξης του 10^{-5}, το σχήμα διαμόρφωσης BPSK απαιτεί ένα σηματοθορυβικό λόγο E_b/N_0 των 9,6 dB (η βέλτιστη δυαδική διαμόρφωση χωρίς κωδικοποίηση). Ωστόσο, η δουλειά του Shannon υποσχέθηκε την ύπαρξη μίας θεωρητικής βελτίωσης της απόδοσης των 11.2 dB πάνω από την απόδοση της βέλτιστης δυαδικής

διαμόρφωσης χωρίς κωδικοποίηση, με τη χρήση τεχνικών κωδικοποίησης. Σήμερα είναι πραγματοποιήσιμη μία βελτίωση της απόδοσης των 7 dB.

Ο απλούστερος κώδικας καναλιού, αν και καθόλου αποδοτικός, θα ήταν μια απλή επανάληψη των κωδικοποιημένων bit μία ή περισσότερες φορές. Με τον τρόπο αυτό, ένας δέκτης θα μπορούσε να ανιχνεύσει σφάλματα που συνέβησαν από τις δυσμενείς επιδράσεις του διαύλου κατά τη μετάδοση και στο τέλος πετώντας τις πλεοναστικές ρέπλικες του απεσταλμένου σήματος να κρατήσει μόνο τα χρήσιμα bit. Το block δεδομένων που στέλνεται με τον παραπάνω τρόπο σπάει σε μικρότερα κομμάτια (π.χ. σε 4 μικρότερα block) και στέλνεται κυκλικά, δηλαδή πρώτα το $1^{ο}$ ψηφίο του $1^{ου}$ block, μετά το $1^{ο}$ του δεύτερου κ.λπ.. Αυτό συμβαίνει τρεις φορές, ώστε τα data να διασπαρθούν και να αποφευχθούν μαζικές συγκεντρώσεις (burst) σφαλμάτων.

Σε άλλες εφαρμογές, όπως στις δορυφορικές επικοινωνίες, απαιτείται άλλη συμπεριφορά από τους κώδικες καναλιού καθότι εκεί ο δίαυλος περιορίζεται από το θερμικό θόρυβο στο δέκτη, ο οποίος είναι μια οντότητα που έχει συνεχόμενη υπόσταση, όχι όπως αυτή των μεγάλων συγκεντρώσεων σφαλμάτων που αναφέρθηκαν.

Άλλο παράδειγμα αποτελούν οι κινητές επικοινωνίες, στις οποίες πρέπει να αντιμετωπιστούν φαινόμενα ταχέων διαλείψεων, οι οποίες λαμβάνουν χώρα ακόμα και αν ο δέκτης κινηθεί για λίγα εκατοστά, οπότε απαιτείται σχεδίαση εξειδικευμένων κωδίκων για να αντιμετωπιστεί το φαινόμενο.

Η μελέτη των κωδίκων καναλιού γίνεται μέσω της αλγεβρικής θεωρίας κωδικοποίησης, η οποία αποτελεί ένα από τα πεδία της θεωρίας κωδικοποίησης και σ' αυτή οι κώδικες αναπαριστούνται με αλγεβρικούς όρους ώστε να μελετηθούν περαιτέρω. Η θεωρία αυτή βοηθάει στην κατάταξη των κωδίκων καναλιού σε δύο μεγάλες υποκατηγορίες:

α. Block κώδικες
β. Συνελικτικοί κώδικες

και αναλύει τις παρακάτω τρεις ιδιότητες ενός κώδικα:

α. Μήκος λέξης κώδικα
β. Συνολικός αριθμός έγκυρων κωδικών λέξεων
γ. Ελάχιστη απόσταση μεταξύ δύο κωδικών λέξεων, κάνοντας χρήση της «απόστασης Hamming» ή της «απόστασης Lee».

Στη γενική τους μορφή, όπως αναφέρθηκε, οι κώδικες καναλιού πρέπει αν όχι να κάνουν διόρθωση λαθών, στην ελάχιστη περίπτωση να εντοπίζουν αυτά.

4.5 Πληροφορία και εντροπία

Σύμφωνα με τη θεωρία της πληροφορίας, η «κατάπληξη» (surprisal η πρωτότυπη αγγλική έκφραση για αυτή), είναι η αποτύπωση του πόσο πιθανό είναι να συμβεί το αποτέλεσμα Ε μιας παρατήρησης. Όταν η πιθανότητα ***p(E)*** είναι κοντά στο 1, τότε το παραπάνω μέγεθος είναι μικρό, όταν όμως η πιθανότητα

μικραίνει, τόσο πιο αβέβαιο είναι το αποτέλεσμα και κατά συνέπεια τόσο μεγαλύτερη η «κατάπληξη». Έτσι λοιπόν μπορεί να οριστεί η «κατάπληξη» ή αλλιώς η πληροφορία ενός γεγονότος ***E***, όπως ονομάστηκε, ως:

$$I(E) = -log_2\big(p(E)\big) \quad \text{ή αντιστοίχως} \quad I(E) = log_2\left(\frac{1}{p(E)}\right)$$

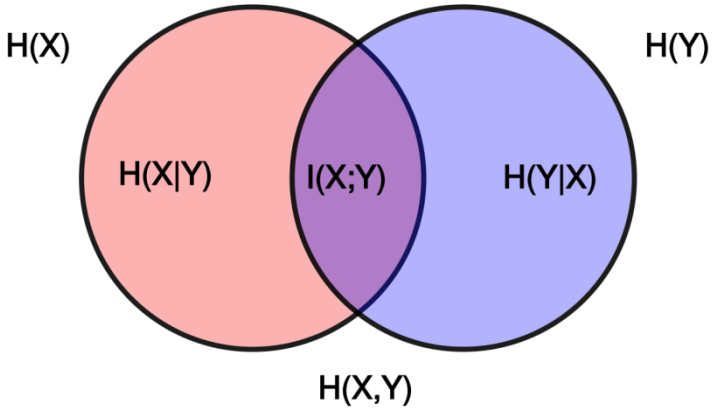
Έστω μια μεταβλητή ***X***, η οποία ορίζεται ως:

$$X \in \{x, A_x, P_x\}$$

όπου ***x*** είναι ένα σύνολο ενδεχομένων, ***Ax*** ένα σύνολο πιθανών τιμών που τα ενδεχόμενα αυτά μπορούν να πάρουν και ***Px*** ένα σύνολο που αποτελείται από τις πιθανότητες που μπορεί να πάρουν οι υπόψη τιμές του συνόλου ***Ax***. Τότε σύμφωνα με το έργο του Shannon, η εντροπία ***H*** της μεταβλητής ***X*** είναι:

$$H_{(X)} = -\sum_{x \in X} P_x * log_2 P_x$$

Σχηματικά, ο κανόνας αλυσίδας των διαφορετικών ειδών εντροπίας (κοινή, υπό συνθήκη και οριακή), σε περίπτωση που έχουμε δύο ανεξάρτητες μεταξύ τους, τυχαίες μεταβλητές ***X*** και ***Y***, δίδεται όπως παρακάτω:



Σχήμα 4.5.1

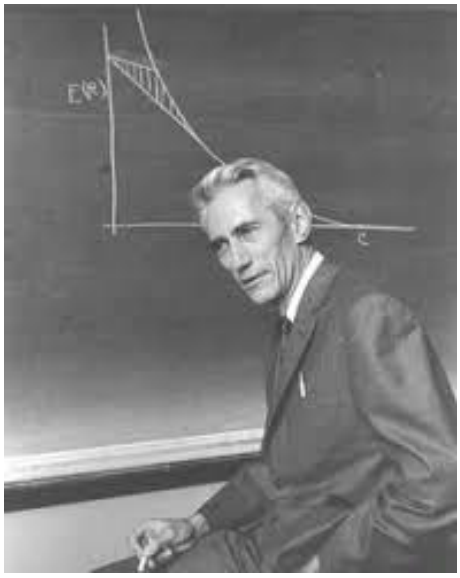
Σε μαθηματική απεικόνιση:

$$I(X;Y) = H(X) - H(X \vee Y)$$

και αντίστοιχα:

$$I(Y;X) = H(Y) - H(Y \vee X)$$

4.6 Shannon, Wyner και η τέλεια μυστικότητα



Το 1949 ο Claude Shannon έθεσε τη βάση για την ανάπτυξη της θεωρίας της ασφαλούς επικοινωνίας σε ένα τηλεπικοινωνιακό κανάλι, περιγράφοντας για πρώτη φορά στην εργασία του το κανάλι αυτό ως «παρακολουθούμενο» κανάλι (wiretap channel) [28]. Ο Shannon θεώρησε το χώρο μεταξύ του Bob, της Alice και του Mallory ως κανάλια που έχουν αρχή και τέλος τις παραπάνω οντότητες και μέσα στα οποία ταξιδεύουν bit πληροφορίας, υποστήριξε δε ότι παρότι το κανάλι παρακολουθείται από τον Mallory που δύναται να υποκλέψει όλο το διακινούμενο όγκο πληροφορίας, μπορεί να επιτευχθεί απόλυτη μυστικότητα μεταξύ του Bob και της Alice, εφόσον αυτοί κρυπτογραφούν/αποκρυπτογραφούν το μήνυμά τους με ένα γνωστό και στους δύο, μυστικό όμως κλειδί, το οποίο δεν επαναχρησιμοποιείται ποτέ (one-time pad - OTP). Έστω λοιπόν, όπως και στο παρακάτω σχήμα ότι ο Bob επιθυμεί να στείλει το μήνυμα ***M*** στην Alice μέσα από το υπόψη κανάλι. Τότε χρησιμοποιώντας το OTP κλειδί ***K*** εκτελεί την πράξη XOR σε κάθε bit πληροφορίας ***M*** και παράγει έτσι το κρυπτογράφημα ***C***:

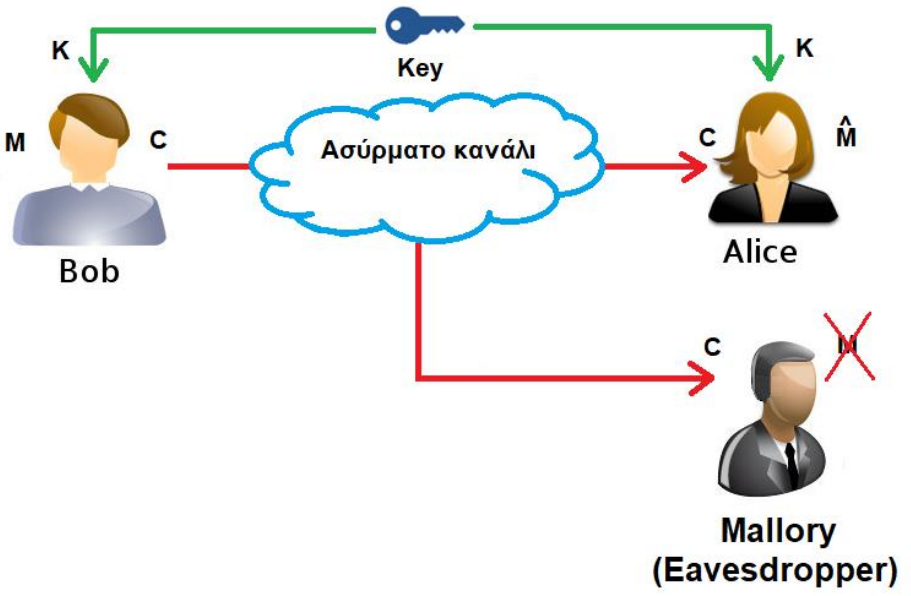
$$C = M \oplus K$$

Το κρυπτογράφημα ***C*** λαμβάνεται τόσο από τη νόμιμη χρήστη Alice, όσο και από τον επιτιθέμενο στο σύστημα Mallory.

Η Alice επαναλαμβάνει την πράξη του XOR με το κλειδί ***K*** που ήδη διαθέτει και ανακτά το αρχικό μήνυμα:

$$M = C \oplus K$$

ενώ ο Mallory μη διαθέτοντας το μοναδικό κλειδί, δεν μπορεί να αποκρυπτογραφήσει το μήνυμα, αλλά όσο και να προσπαθήσει να μαντέψει το κλειδί δεν θα τα καταφέρει, καθώς, όπως μαθηματικά απέδειξε ο Shannon, αυτό είναι αδύνατο από τη στιγμή που το χρησιμοποιούμενο OTP κλειδί είναι στατιστικά ανεξάρτητο από το μήνυμα ***M***.



Σχήμα 4.6.1

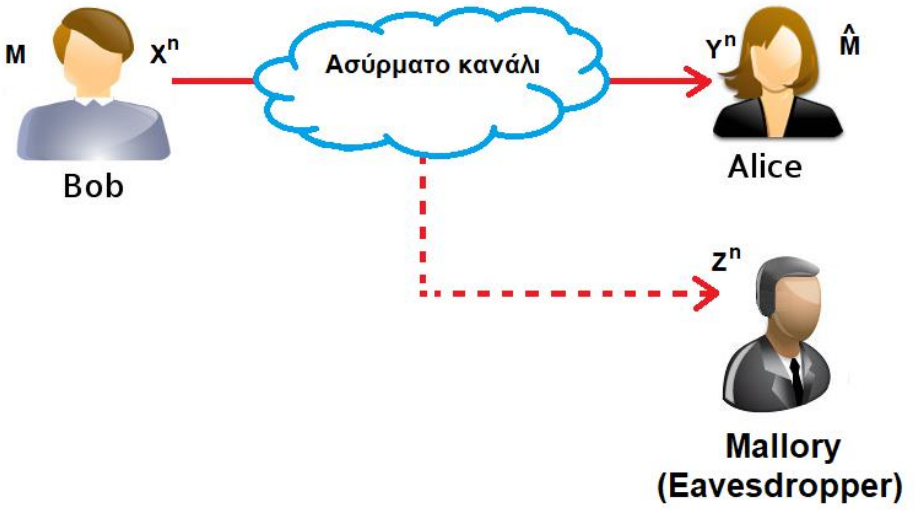
Εκείνο όμως το οποίο έχουμε πληρώσει ως τίμημα, δεν μας επιτρέπει τη χρήση της παραπάνω μορφής κρυπτογράφησης (OTP) στις καθημερινές επικοινωνίες. Το χρησιμοποιούμενο κλειδί για να παρέχει πλήρη ασφάλεια, για να είναι δηλαδή στατιστικά ανεξάρτητο με το εκπεμπόμενο μήνυμα θα πρέπει να έχει την ίδια τουλάχιστο και μεγαλύτερη εντροπία από αυτό ***[***$H(K) \geq H(M)$***]***. Με άλλα λόγια, το μήκος του κλειδιού να είναι όσο το μήκος του μηνύματος ή μεγαλύτερο από αυτό, γεγονός το οποίο καθιστά την υλοποίηση στην πράξη στις συνήθεις επικοινωνίες ως μη αποδοτική και ασύμφορη.

Το 1975, ο Aaron D. Wyner [29] παρουσίασε το δικό του μοντέλο σχετικά με την επίτευξη ασφαλούς επικοινωνίας σε ένα ασύρματο τηλεπικοινωνιακό κανάλι, όπου και οι δύο ασύρματες ζεύξεις μεταξύ Bob- Alice και Bob-Mallory είναι θορυβώδεις.

Ο Wyner θεώρησε την περίπτωση όπου δεδομένα στέλνονται από έναν πομπό (Bob) σε ένα δέκτη (Alice) πάνω από ένα διακριτό, χωρίς μνήμη κανάλι (Digital Memoryless Channel – DMC), το οποίο παρακολουθείται από έναν τρίτο άτομο και από εδώ και στο εξής για τις ανάγκες αυτής της πτυχιακής εργασίας θα ονομάζεται στην ελληνική γλώσσα «λαθρακουστής» λαθρακουστή(Mallory). Μάλιστα, θεώρησε δεύτερο κανάλι, επίσης DMC, μέσω του οποίου διοχετεύονται τα δεδομένα από τον πομπό στον λαθρακουστή, επίσης θορυβώδες.

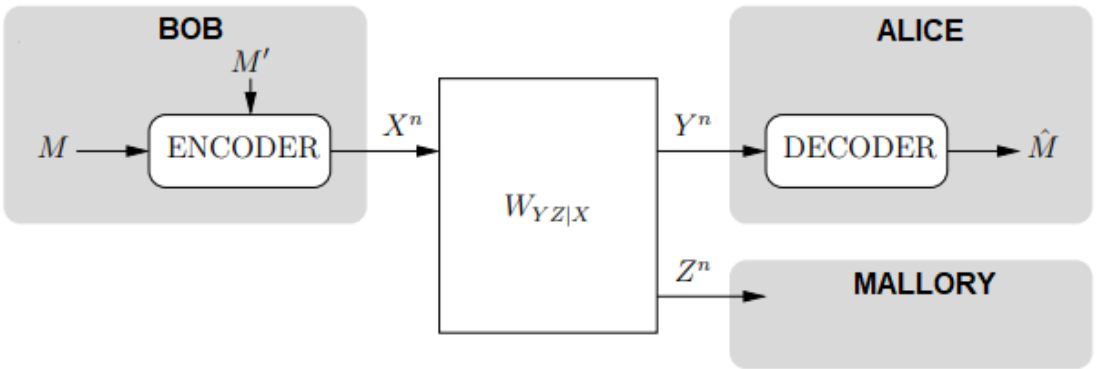
Η κωδικοποίηση και αντίστοιχα αποκωδικοποίηση είναι αποδεκτή, τόσο στον πομπό, όσο και στο δέκτη, με την παραδοχή μάλιστα ότι το είδος αυτής είναι

γνωστά στον λαθρακουστή. Ο σχεδιαστής του συστήματος έχει προσπαθήσει να αυξήσει το ρυθμό μετάδοσης δεδομένων ***R*** μεταξύ του πομπού και του δέκτη, ενώ αντίστοιχα και την ασάφεια ***d*** με την οποία ο λαθρακουστής βλέπει τα να διοχετεύονται στο κανάλι. Ο Wyner απέδειξε ότι εάν $d = Hs$, όπου ***Hs*** η εντροπία της πηγής, τότε μπορεί να θεωρηθεί ότι η μετάδοση δεδομένων είναι απόλυτα ασφαλής. Με άλλα λόγια εάν η παρατήρηση του καναλιού από την πλευρά του λαθρακουστή είναι πάντοτε κατώτερη ποιοτικά από αυτή του δέκτη, τότε μπορεί να υπάρξει ασφαλής επικοινωνία μεταξύ πομπού και δέκτη, κρατώντας την πληροφορία που ανταλλάσσεται κρυφή από τον λαθρακουστή, χωρίς τη χρήση κρυπτογράφησης.



Σχήμα 4.6.2

Έστω ξανά το παρακάτω τηλεπικοινωνιακό σύστημα όπου το ζητούμενο είναι για τον πομπό (Bob) να ανταλλάξει μηνύματα με ρυθμό ***R***, ο οποίος αναπαρίσταται από την τυχαία μεταβλητή $M \in \{1; 2^{nR}\}$, κωδικοποιώντας τα σε κωδικές λέξεις X^n , μήκους **n** και εκπέμποντας τις λέξεις αυτές X^n πάνω σε ένα θορυβώδες, χωρίς μνήμη κανάλι, το οποίο έχει ως χαρακτηριστικό την πιθανότητα αντιστροφής των εκπεμφθέντων bit πληροφορίας ίση με $W_{YZ\vee X}$.



Σχήμα 4.6.3

Ο δέκτης που παρατηρεί το σήμα Y^n είναι ο επιθυμητός χρήστης (Alice), ο οποίος θα πρέπει να είναι σε θέση να κάνει σωστή εκτίμηση του ληφθέντος μηνύματος $\hat{M}$, όσο πιο κοντινή γίνεται στο ***M***, με πολύ μεγάλη πιθανότητα. Ο δέκτης που παρατηρεί το σήμα Z^n είναι ο ανεπιθύμητος χρήστης/λαθρακουστής (Mallory), ο οποίος κανονικά δεν θα πρέπει να είναι σε θέση να δει καμία πληροφορία για το μήνυμα ***M***. Η κωδικοποίηση του μηνύματος έχει γίνει με τη βοήθεια μιας τοπικής γεννήτριας ψευδοτυχαίων αριθμών $M' \in \{1; 2^{nR'}\}$**,** η οποία θεωρούμε ότι είναι γνωστή μόνο στον πομπό (Bob).

Θεωρούμε ότι ένας κώδικας γι αυτό το πρόβλημα επικοινωνιών καλείται «κώδικας παρακολουθούμενου καναλιού» (wiretap code). Τότε είναι δυνατή η επίτευξη μυστικής επικοινωνίας μεταξύ πομπού (Bob) και δέκτη (Alice), εφόσον υπάρχει μια ακολουθία wiretap codes με αυξανόμενο μήκος block, τέτοιοι ώστε:

$$lim_{n\to\infty} P\left(M \neq \hat{M}\right) = 0 \quad \text{(Αρχή της ακεραιότητας)}$$

και:

$$lim_{n\to\infty} I(M; Z^n) = 0 \quad \text{(Αρχή της εμπιστευτικότητας)}$$

Από τις δύο παραπάνω σχέσεις μπορούμε να συμπεράνουμε ότι στην πλευρά του Bob, προκειμένου να ικανοποιηθεί η αρχή της ακεραιότητας, κρίνεται απαραίτητη η εισαγωγή ενός κώδικα καναλιού, ο οποίος θα αντισταθμίσει την επίδραση του θορύβου. Ο υπόψη κώδικας, όπως αναφέρθηκε σε προηγούμενη ενότητα θα εισάγει πληροφορία πλεονασμού στο προς εκπομπή μήνυμα. Από την πλευρά του ο Mallory, δεν επιθυμεί την εισαγωγή αυτής της πλεοναστικής πληροφορίας, διότι έτσι έχει να αντιμετωπίσει μεγαλύτερο όγκο διακινούμενης πληροφορίας, κάτι που δυσκολεύει το έργο του να εξαγάγει την πραγματική πληροφορία από το εκπεμπόμενο μήνυμα.

Επιπλέον, από τις δύο προσεγγίσεις του Shannon και του Wyner, προκύπτουν τα εξής συμπεράσματα:

α. Η προσέγγιση του Wyner διαφέρει ως προς εκείνη του Shannon σε δύο (2) βασικά σημεία:

(1) Το μοντέλο του Wyner περιλαμβάνει την παρουσία θορύβου στο τηλεπικοινωνιακό κανάλι, κάτι που δεν ισχύει στο μοντέλο του Shannon.

(2) Το μοντέλο του Wyner δεν περιλαμβάνει την ανταλλαγή οποιουδήποτε μυστικού κλειδιού μεταξύ πομπού (Bob) και δέκτη (Alice).

β. Η τοπική γεννήτρια ψευδοτυχαίων αριθμών M' που λειτουργεί στον πομπό έχει παρεμφερή ρόλο με αυτόν του OTP του μοντέλου του Shannon, σκοπός της είναι να καταστήσει όσο πιο δυνατό τυχαία την κωδικοποίηση του μηνύματος στον πομπό, πριν αυτό εκπεμφθεί στο κανάλι. Το M' αξίζει να σημειωθεί ότι είναι γνωστό μόνο στον Bob και όχι στην Alice ή τον Mallory.

γ. Τα στατιστικά μεγέθη του καναλιού και του wiretap κώδικα που χρησιμοποιείται για την κωδικοποίηση είναι γνωστά σε όλους, ο δε Mallory λειτουργεί παθητικά ως επιτιθέμενος στο σύστημα.

δ. Το παράδειγμα προσπαθεί να εφαρμόσει μόνο τις αρχές της εμπιστευτικότητας και της ακεραιότητας. Η αρχή της αυθεντικότητας υποτίθεται ότι έχει λυθεί με άλλη μέθοδο, η οποία δεν εξετάζεται εδώ.

Έχοντας υπόψη όλες τις παραπάνω παρατηρήσεις, μπορεί να οριστεί η έννοια του secrecy capacity, παρεμφερής με αυτή της χωρητικότητας καναλιού όταν απαιτείται πλέον μυστικότητα στην επικοινωνία, ως το ανώτατο όριο από όλους εκείνους τους ρυθμούς επικοινωνίας που μπορούν να επιτευχθούν με τη χρήση wiretap κωδίκων.

Το secrecy capacity δίνεται από τη σχέση:

$$C_s = \max_{V \to X \to YZ} \big(I(V;Y) - I(V;Z) \big)$$

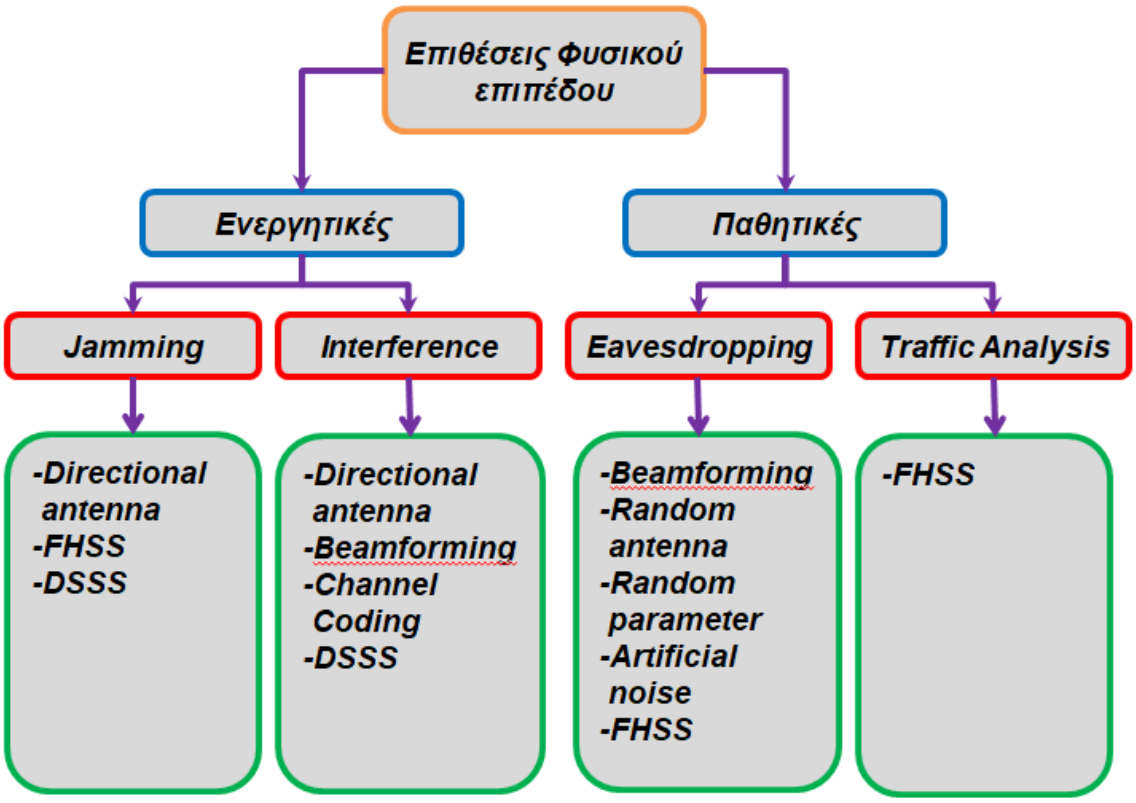
Με απλούς όρους, μπορούμε να εξηγήσουμε την παραπάνω σχέση και να ορίσουμε το secrecy capacity ως τη διαφορά μεταξύ του ρυθμού μιας αξιόπιστης μετάδοσης πληροφορίας $I(V;Y)$από τον Bob στην Alice και του ρυθμού μιας μετάδοσης/διαρροής πληροφορίας $I(V;Z)$ προς τον λαθρακουστή Mallory. Από αυτό μπορούμε να συμπεράνουμε ότι όσο η διαφορά αυτή διατηρείται θετική, τότε υπάρχει μυστικότητα στην επικοινωνία μεταξύ Bob και Alice. Όταν πλέον η παρατήρηση του Mallory εξισωθεί με αυτή της Alice, τότε $Y = Z$ και επομένως το secrecy capacity του καναλιού γίνεται μηδέν, άρα δεν υπάρχει ασφαλής επικοινωνία.

5. ΤΕΧΝΙΚΕΣ ΥΛΟΠΟΙΗΣΗΣ ΑΣΦΑΛΕΙΑΣ ΦΥΣΙΚΟΥ ΕΠΙΠΕΔΟΥ

5.1 Γενικά

Με την πάροδο των ετών και την εξέλιξη των ασύρματων επικοινωνιών, οι παραπάνω θεωρίες για ασφαλή επικοινωνία στο φυσικό επίπεδο άρχισαν να βρίσκουν εφαρμογή και να γίνονται πράξη, μέσα από ένα πρίσμα καινοτόμων συστημάτων επικοινωνιών, όπως τα συστήματα MIMO (Multiple-Input Multiple-Output) και SIMO (Single-Input Multiple-Output). Τα συστήματα αυτά πλέον προσφέρουν αυξημένο secrecy capacity και μεγάλη ασφάλεια στο φυσικό επίπεδο, σε συνδυασμό με άλλες τεχνικές ασφαλείας, μερικές από τις οποίες θα αναλυθούν παρακάτω.

Πριν την αναφορά στις υπόψη τεχνολογίες, εάν επιχειρήσουμε μια κατάταξη, με βάση τα είδη των επιθέσεων που μπορούν να λάβουν χώρα στο φυσικό επίπεδο, όπως αναλύθηκαν στο Κεφ. 3, καθώς και μερικοί από τους τρόπους προστασίας στους οποίους θα αναφερθούμε στη συνέχεια, αυτή θα είχε την παρακάτω δενδροειδή δομή:



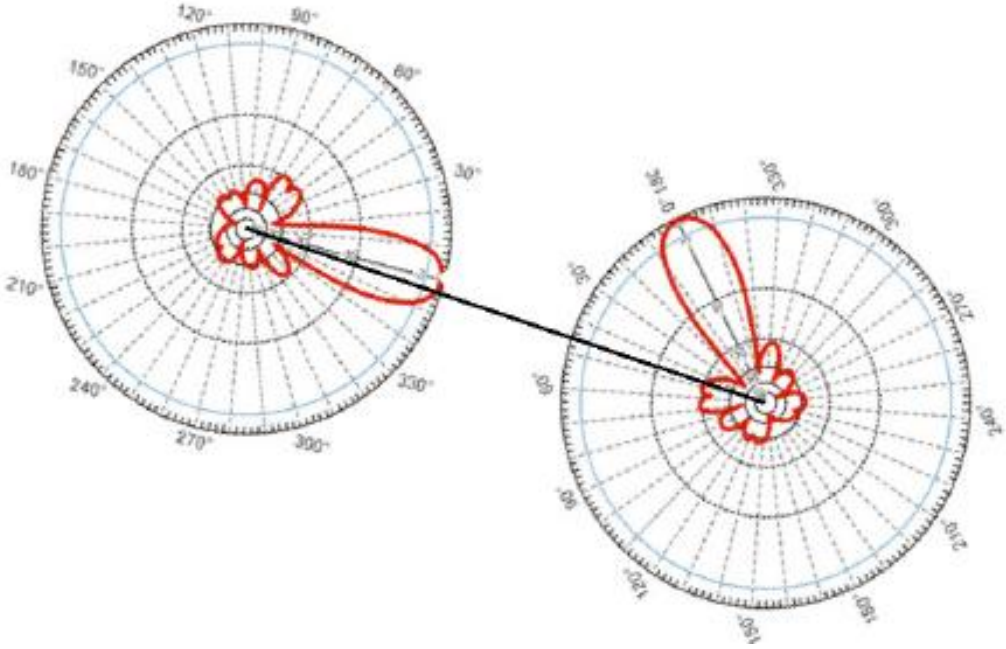
Σχήμα 5.1.1

5.2 Τεχνικές στο πεδίο του χώρου (Spatial Domain)

Η υπόψη κατηγορία περιλαμβάνει τεχνικές όπως κατευθυντικές κεραίες, beamforming και κάποιες άλλες βελτιωμένες τεχνολογίες βασισμένες στο beamforming. Με τις υπόψη τεχνικές, ένα τηλεπικοινωνιακό σύστημα μπορεί με μεγάλη επιτυχία να αντισταθεί σε επιθέσεις παρεμβολών, απαγόρευσης χρήσης του Η/Μ φάσματος αλλά και υποκλοπής.

α. Κατευθυντικές κεραίες και beamforming

Μια κατευθυντική κεραία, αξιοποιεί/συγκεντρώνει την εκπεμπόμενη ισχύ σε μία ή περισσότερες συγκεκριμένες κατευθύνσεις/λοβούς ακτινοβολίας, ενώ σε άλλες περιοχές του χώρου εκπέμπει με μικρότερη ισχύ. Με τον τρόπο, συγκεντρώνοντας δηλαδή την ακτινοβολία σε συγκεκριμένες κατευθύνσεις, η απόσταση ακτινοβολίας της κεραίας μεγαλώνει, αυξάνοντας έτσι και την περιοχή κάλυψης.



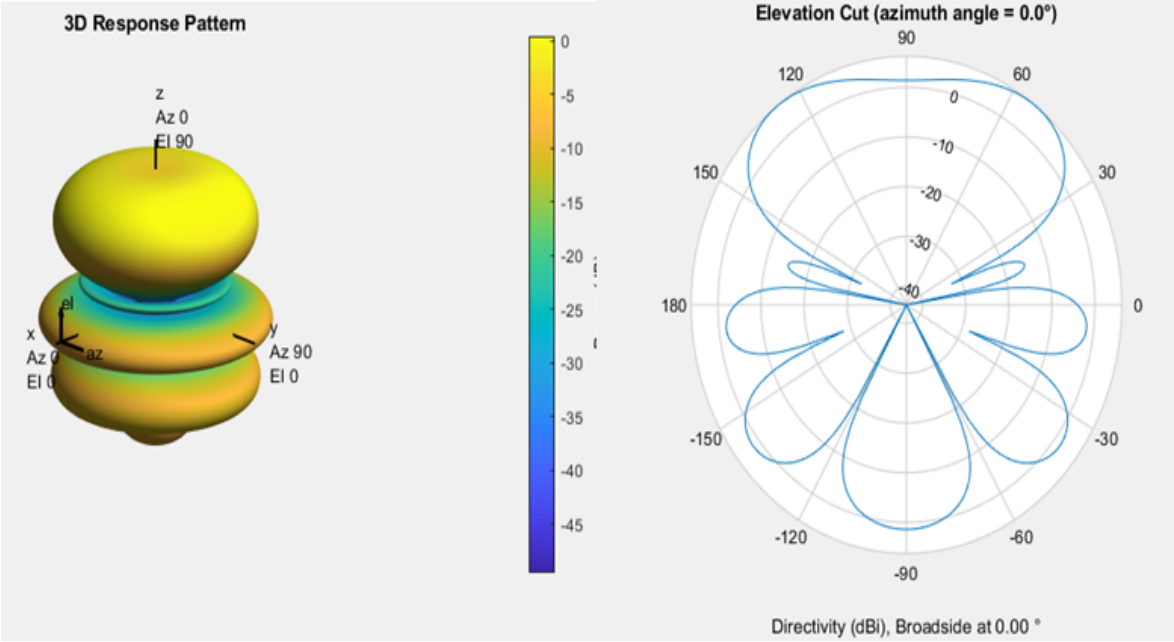
Σχήμα 5.2.1

Ένα άλλο βασικό πλεονέκτημα των κατευθυντικών κεραιών, το οποίο αξιοποιείται στην περίπτωσή μας είναι η δυνατότητα ευθυγράμμισης (alignment) των κύριων λοβών ακτινοβολίας πομπού-δέκτη μεταξύ τους. Με την έναρξη εκπομπής του σήματος πληροφορίας ο δέκτης δύναται να ευθυγραμμίσει τον κύριο λοβό ακτινοβολίας της κεραίας του με το δέκτη, αφήνοντας στην ουσία κάποιον λαθρακουστή ή δεύτερο πομπό που ασκεί ακούσια παρεμβολή, χωρικά στον τομέα των δευτερευόντων λοβών, ελαττώνοντας σε πολύ μεγάλο βαθμό τα σήματα παρεμβολών ή jamming. Επιπλέον, αντίστοιχα ελαττώνει τη δική του επίδραση σε τρίτους φίλιους χρήστες και αντιμετωπίζει με επιτυχία κάποιον λαθρακουστή που γνωρίζει τη θέση του στο χώρο, ο οποίος προσπαθεί να υποκλέψει το εκπεμπόμενο σήμα, στέλνοντας στην κατεύθυνσή του μικρότερο μέρος της ισχύος εξόδου (μικρότερος σηματοθορυβικός λόγος).

Επιπρόσθετα οι κατευθυντικές κεραίες υπερτερούν έναντι των απλών, ισοτροπικών, στο γεγονός ότι πέρα από την αντιμετώπιση σημάτων παρεμβολών και jamming, επιτυγχάνουν το ίδιο αποτέλεσμα με πολύ μικρότερη ισχύ εξόδου (κατανάλωση ενέργειας) και επομένως έχουν πολύ μικρότερες πιθανότητες εντοπισμού και ραδιογωνιομετρήσεως από τις αντίστοιχες ισοτροπικές.

Η τεχνική του beamforming από την άλλη πλευρά, δεν είναι τίποτε άλλο από μία «έξυπνη» εκδοχή της κατευθυντικής κεραίας, η οποία πέρα από την κλασική προσέγγιση αυτής, ενσωματώνει την ιδέα των συστοιχιών κεραιών (antenna arrays). Οι κεραίες αυτές είναι δυνατό με κατάλληλη χρήση της γεωμετρίας τους, την απόσταση μεταξύ των στοιχείων τους αλλά και μεγέθη που χρησιμοποιούνται ως «βάρη» για κάθε στοιχείο ξεχωριστά (weighted beamformer) να τροποποιούν «κατά παραγγελία» του χρήστη κάθε φορά το διάγραμμα

ακτινοβολίας και κατά συνέπεια την κατεύθυνση και τη μορφή των λοβών ακτινοβολίας τους, ώστε να συγκεντρώσουν το κύριο μέρος της ισχύος εξόδου στην επιθυμητή κατεύθυνση.



Εικόνα 5.2.2

Τα παραπάνω, σε συνδυασμό με τις σύγχρονες τεχνικές κατασκευής κεραιών (συστοιχίες κεραιών, patched antennas, intelligent meta-surfaces, κ.λπ.) αλλά και με έξυπνες τεχνικές διαχείρισης του κέρδους και της πόλωσής τους για αντιμετώπιση θορύβου και διαλείψεων, καθιστούν τις κατευθυντικές κεραίες μια πολύ καλή λύση στο θέμα ασφάλειας φυσικού επιπέδου.

β. <u>Τεχνητός θόρυβος (Artificial Noise - AN)</u>

Η τεχνική του τεχνητού θορύβου βασίζεται στην ιδέα ότι στο κανάλι επικοινωνίας μεταξύ του Bob και της Alice έχει μεγαλύτερο secrecy capacity από αυτό μεταξύ του Bob και του Mallory (λαθρακουστή). Αυτό σημαίνει ότι το πρώτο κανάλι έχει καλύτερο CSI (Channel State Information) από το δεύτερο, δηλαδή είτε έχουμε βρει κάποιο μηχανισμό ώστε να καλυτερέψουμε αισθητά την ποιότητα του πρώτου καναλιού σε σχέση με το δεύτερο ή αντίστροφα, να χειροτερέψουμε το δεύτερο σε σχέση με το πρώτο.

Η πιο συνήθης τεχνική είναι ο πομπός να χρησιμοποιεί ένα μέρος της ισχύος του ώστε να παράγει θόρυβο που θα διοχετεύσει στο κανάλι του λαθρακουστή σε συνδυασμό με την τεχνική του beamforming, για το λόγο αυτό δε ονομάζεται τεχνική τεχνητού θορύβου. Το κύριο πλεονέκτημά της είναι ότι η μυστικότητα η οποία υπόσχεται είναι ευθέως ανάλογη με το SNR στο δέκτη του λαθρακουστή, αφού οποιαδήποτε αύξηση στο SNR του Mallory, αυτόματα αυξάνει και το ποσοστό του τεχνητού θορύβου, το οποίο ο Mallory δέχεται στο κανάλι του από τον Bob.

Για να κατασκευάσει τον τεχνητό θόρυβο ο Bob πρέπει να γνωρίζει το CSI της Alice. Για ένα κανάλι επιπέδων διαλείψεων που ακολουθεί την κατανομή Rayleigh, η Alice αρκεί να στείλει τα χαρακτηριστικά του καναλιού στον Bob, σε χρόνο μικρότερο από το χρόνο συνοχής αυτού. Επιπλέον, πρέπει να επισημανθεί ότι η μυστικότητα της τεχνικής δεν βασίζεται στη μυστική μετάδοση του CSI του καναλιού από την Alice στον Bob, δεν έχει δηλαδή καμία σημασία εάν ο Mallory υποκλέψει την παραπάνω πληροφορία. Έστω λοιπόν ότι w_k ο όρος που εκφράζει τον AN, τότε ο Bob εκπέμπει:

$$x_k = s_k + w_k$$

όπου x_k και w_k είναι γκαουσιανά μιγαδικά διανύσματα με το w_k επιλεγμένο από το μηδενοχώρο του h_k ώστε να ικανοποιείται η συνθήκη:

$$H_k w_k = 0$$

Το διάνυσμα w_k (AN), παράγεται από το εσωτερικό γινόμενο:

$$w_k = Z_k v_k$$

όπου ο όρος Z_k είναι ένας αναστρέψιμος πίνακας που αποτελεί ορθοκανονική βάση για το μηδενοχώρο του H_k. Έτσι λοιπόν, αφού ο λαθρακουστής (Mallory) είναι πιθανό να βρίσκεται σε μια θέση ευθυγραμμισμένη με αυτή της Alice, η καλύτερη τεχνική είναι να επιλεγεί κάθε στοιχείο του πίνακα v_k ως μια τυχαία μεταβλητή, η οποία ακολουθεί την κανονική (γκαουσιανή) κατανομή. Με αυτό τον τρόπο, το διάνυσμα w_k παράγεται ψευδοτυχαία, από το διαθέσιμο σετ διανυσμάτων της ορθοκανονικής βάσης του μηδενοχώρου του καναλιού της Alice, επομένως ο αριθμός των πιθανών διανυσμάτων βάσεως για το κανάλι της Alice, δηλαδή το N_{null}, βρίσκεται από τη διαφορά του μήκους των διανυσμάτων μεταξύ του Bob και της Alice:

$$N_{null} = N_{Bob} - N_{Alice} \qquad \text{με} \qquad N_{Bob} \geq N_{Alice}$$

Τότε, το σήμα που θα ληφθεί από την Alice θα είναι:

$$y_k = H_k x_k + n_k$$

$y_k = H_k(s_k + w_k) + n_k$, και συνεπώς:

$$y_k = H_k s_k + n_k$$

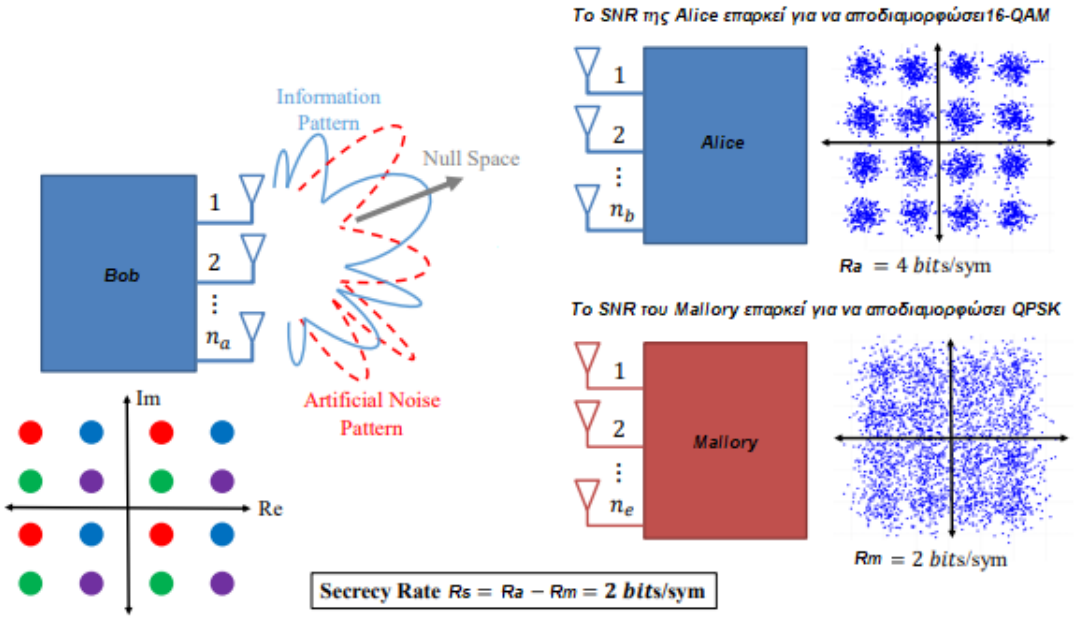
και το σήμα που θα ληφθεί από τον Mallory αντίστοιχα θα είναι:

$$z_k = G_k x_k + e_k$$

$z_k = G_k(s_k + w_k) + e_k$, και συνεπώς:

$$z_k = G_k s_k + G_k w_k + e_k$$

όπου το μη μηδενικό μέγεθος $H_k w_k$, αναπαριστά τον επιπλέον θόρυβο τον οποίο βλέπει στο δέκτη του ο Mallory.



Εικόνα 5.2.3

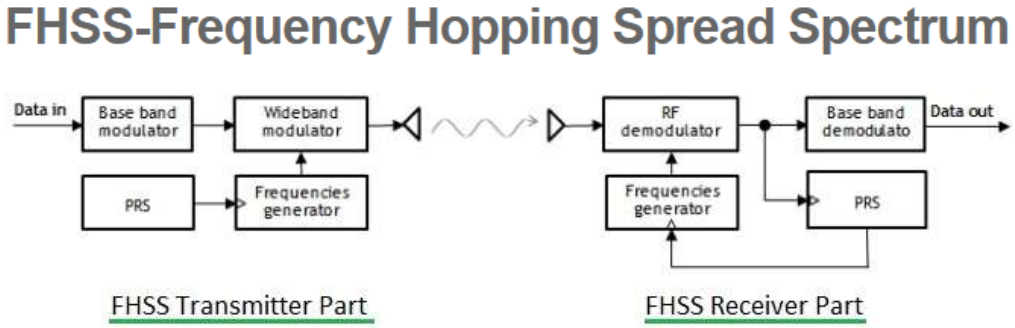
Στο παραπάνω σχήμα οπτικοποιείται το αποτέλεσμα της επίδρασης του τεχνητού θορύβου στο δέκτη του Mallory. Έτσι, η Alice, έχοντας απαλλαγεί από τον τεχνητό θόρυβο λόγω του τρόπου με τον οποίο αυτός παράχθηκε στον πομπό του Bob, την έμμεση δηλαδή ακύρωσή του, ο Mallory, «ζώντας» σε κανάλι που δεν ικανοποιεί τις συνθήκες ορθογωνιότητας με αυτό του πομπού εμφανίζει στο δέκτη του χειρότερο SNR. Το αποτέλεσμα είναι να μην μπορεί να αποκωδικοποιήσει το εκπεμπόμενο σχήμα διαμόρφωσης 16-QAM, αλλά ένα επίπεδο κάτω, δηλαδή QPSK. Το secrecy rate θα είναι η διαφορά μεταξύ των ρυθμών της Alice και του Mallory, άρα 2 bits/symbol.

5.3 Τεχνικές στο πεδίο της συχνότητας (Frequency Domain)

Οι τεχνικές στο πεδίο της συχνότητας, με κυρίαρχη εκείνη του spread spectrum, αποτελούν την πιο διαδεδομένη μορφή αμυντικού μηχανισμού έναντι επιθέσεων στο φυσικό επίπεδο. Η ιδέα της τεχνικής του spread spectrum ξεκίνησε από το μεγάλο εφευρέτη Nikola Tesla και αργότερα αναπτύχθηκε ιδίως σε στρατιωτικές εφαρμογές. Η τεχνική του spread spectrum χρησιμοποιείται ώστε το αρχικό σήμα να διαμορφωθεί και να εκπεμφθεί σύμφωνα με μια ψευδο-τυχαία ακολουθία, με το δέκτη να αποδιαμορφώνει το σήμα χρησιμοποιώντας την ίδια ακολουθία, προκειμένου να εξάγει το αρχικό σήμα. Η τεχνική του spread spectrum χωρίζεται σε πολλές κατηγορίες, με τις δύο πιο σημαντικές όμως που ενδιαφέρουν να είναι η αναπήδηση συχνότητας (Frequency Hopping Spread Spectrum – FHSS) και η Direct Sequence Spread Spectrum (DSSS).

α. Frequency Hopping Spread Spectrum (FHSS)

Στην εφαρμογή της υπόψη τεχνικής, το σήμα μετά τη διαμόρφωση μεταφέρεται σε μια φέρουσα συχνότητα στην περιοχή RF, η οποία όμως δεν παραμένει σταθερή αλλά αλλάζει σύμφωνα με μια ψευδο-τυχαία ακολουθία, την οποία γνωρίζουν και έχουν συμφωνήσει ο πομπός και ο δέκτης, σε συγκεκριμένη χρονική στιγμή (hops/sec).



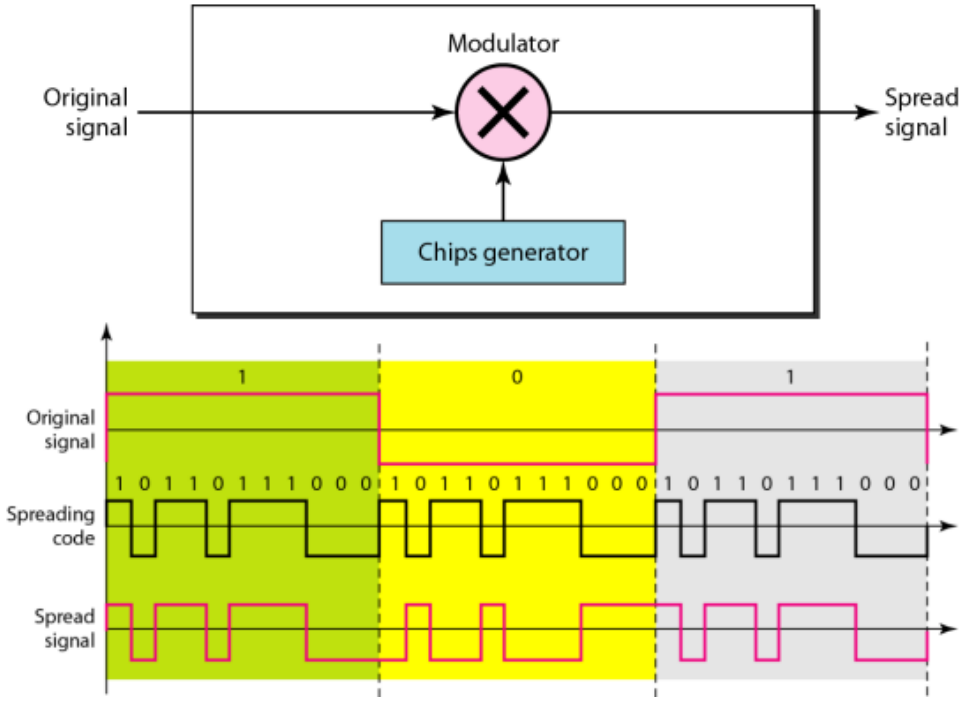
Σχήμα 5.3.1

Με τον παραπάνω τρόπο, το τηλεπικοινωνιακό σύστημα αποκτά αντοχή και επιβιωσιμότητα, τόσο απέναντι σε επιθέσεις τύπου jamming αλλά και υποκλοπών. Ο λαθρακουστής (Mallory) μη γνωρίζοντας την ψευδοτυχαία ακολουθία που χρησιμοποιείται, η οποία όπως αναφέρθηκε είναι γνωστή στην Alice, δεν γνωρίζει την κάθε χρονική στιγμή τη συχνότητα εκπομπής του Bob, άρα δε μπορεί να λάβει και να αποκωδικοποιήσει το εκπεμπόμενο σήμα, αφού η ισχύς του εκπεμπόμενου σήματος έχει διαμοιραστεί σε ένα ευρύ πεδίο συχνοτήτων. Μέσα από το ευρύ πεδίο αυτό, με τη μέθοδο της συσχέτισης (correlation), η Alice είναι σε θέση να αποκωδικοποίησει το ληφθέν σήμα, ακόμα και εάν αυτό έχει επίπεδο ισχύος κοντά σε αυτό του θορύβου.

Επιπλέον, οι επιθέσεις τύπου jamming σε συστήματα που κάνουν χρήση της υπόψη τεχνικής είναι λιγότερο αποτελεσματικές, καθώς για να καταφέρουν να φιμώσουν τον πομπό απαιτείται συγκέντρωση εκπεμπόμενης ισχύος σε περιοχή συχνοτήτων και όχι σε συγκεκριμένη συχνότητα του φάσματος.

β. Direct Sequence Spread Spectrum (DSSS)

Σε μια δεύτερη εκδοχή τεχνικών διασποράς φάσματος, το σήμα πληροφορίας $S_{(t)}$ πολλαπλασιάζεται με ένα κατάλληλο σήμα ευρείας ζώνης $Sc_{(t)}$, το οποίο καλείται κώδικας διασποράς (spreading code) και είναι ανεξάρτητος από το σήμα πληροφορίας.



Σχήμα 5.3.2

Ο κώδικας αποτελείται από διαδοχικούς παλμούς με πλάτος **±1** και πολύ μικρή χρονική διάρκεια T_c. Οι παλμοί αυτοί καλούνται **chips**, η διάρκειά τους **chip interval**, ενώ το μέγεθος $\frac{1}{T_c}$ λέγεται **chip rate**. Ο κώδικας έχει εύρος ζώνης $B_c \cong \frac{1}{T_c}$. Αν το σήμα πληροφορίας έχει παλμούς διάρκειας T_s και εύρος ζώνης $B_s \cong \frac{1}{T_s}$, τότε ο spreading factor θα είναι $\frac{B_c}{B_s} \cong \frac{T_s}{T_c}$.

Ο πολλαπλασιασμός των δύο σημάτων στην εκπομπή έχει ως αποτέλεσμα το φάσμα του τελικού σήματος να προκύπτει από τη συνέλιξη των επιμέρους φασμάτων, δηλαδή:

$$S_{DS}(t) = S(t) \cdot S_c(t) \rightarrow S_{DS}(f) = S(f) * S_c(f)$$

Συνεπώς, το φάσμα του spread spectrum σήματος καθορίζεται από το φάσμα του κώδικα διασποράς και μάλιστα $B_{DS} \cong B_C$.

Στο δέκτη, έχοντας γνώση για τον κώδικα διασποράς, ακολουθείται η ακριβώς αντίστροφη διαδικασία, οπότε εάν ο λευκός προσθετικός θόρυβος (AWGN) είναι $n_{(t)}$, τότε θα έχουμε:

$$y(t) = r(t) \cdot S_c(t) = \left(S(t) \cdot S_c(t) + n_{(t)}\right) \cdot S_c(t) = S(t) \cdot S_c^2(t) + n_{(t)} \cdot S_c(t)$$

όπου $n_{(t)} \cdot S_c(t) = n_c(t)$

Εάν λοιπόν ο κώδικας $Sc_{(t)}$ επιλεγεί τέτοιος ώστε να έχει χαρακτηριστικά λευκού θορύβου, τότε ο όρος $n_c(t)$ στην τελευταία εξίσωση θα είναι επίσης AWGN.

Από τα παραπάνω, μπορεί κανείς εύκολα να αντιληφθεί ότι η τεχνική FHSS, παρότι είναι δύσκολο να εφαρμοστεί λόγω της ανάγκης γνώσης της ψευδο-τυχαίας ακολουθίας αναπήδησης σε πομπό και δέκτη αλλά και της ανάγκης συγχρονισμού μεταξύ αυτών, είναι πολύ αποτελεσματική στην αντιμετώπιση παρεμβολών στο σήμα στενής ζώνης. Σε περίπτωση που η παρεμβολή συνεχίσει να υφίσταται, αυξάνει ο ρυθμός αναπήδησης, εξασθενώντας έτσι τη δυνατότητα του λαθρακουστή για ανίχνευση και επομένως για traffic analysis. Επιπλέον, αξίζει να σημειωθεί ότι λόγω του γεγονότος ότι η τεχνική FHSS έχει υποδεέστερες απαιτήσεις σε hardware από αυτή του DSSS, μπορεί να εφαρμοστεί σε πολλά συστήματα αυτού του είδους, δηλαδή χαμηλής υπολογιστικής ικανότητας και κόστους, διατηρώντας αντίστοιχους ρυθμούς με αυτούς της τεχνικής DSSS.

5.4 Τεχνικές στο πεδίο του χώρου-χρόνου (Space-Time Domain)

α. Τυχαίες Παράμετροι και Τυχαία Επιλογή Κεραίας Εκπομπής

Η λογική της μεθόδου των τυχαίων παραμέτρων ή κεραιών [30] του τηλεπικοινωνιακού καναλιού είναι βασισμένη στην τεχνική του beamforming, που διατυπώθηκε σε προηγούμενη παράγραφο. Υλοποιείται χρησιμοποιώντας τυχαιότητα στην επιλογή της κεραίας εκπομπής ή στη χρήση διαφορετικών βαρών σε κάθε κεραία του συστήματος εκπομπής και έχει ως αποτέλεσμα την ακανόνιστη, μη συνεχή και αναμενόμενη λήψη του σήματος από τους επιβουλείς, χωρίς να επηρεάζονται όμως οι κανονικοί χρήστες.

Στη συγκεκριμένη περίπτωση γίνεται χρήση της τεχνικής του Low Power Probability (LPI) interception, της ιδιότητας εκείνης δηλαδή που μπορούμε να προσδώσουμε στον πομπό ώστε κάνοντας χρήση χαμηλής ισχύος εκπομπής, ευρέως φάσματος εκπομπής, διαφορετικών συχνοτήτων εκπομπής ή άλλων παρόμοιων χαρακτηριστικών να μη μπορεί να εντοπιστεί από έναν λαθρακουστή και να υποκλαπεί το εκπεμφθέν σήμα. Ο πομπός εδώ, τροποποιεί διαρκώς τα χαρακτηριστικά της κεραίας εκπομπής, έτσι ώστε να επιτύχει τυχαιότητα στο ίδιο το κανάλι επικοινωνίας μεταξύ του πομπού και των κανονικών δεκτών ή του λαθρακουστή.

Ο λαθρακουστής, αφήνεται στο να χρησιμοποιήσει τεχνικές και αλγόριθμους όπως το blind de-convolution, προκειμένου να «μαντέψει» το σήμα πληροφορίας και να το εξάγει από τη ληφθείσα, ακανόνιστη και ψευδοτυχαία μορφή, ενώ οι κανονικοί χρήστες, έχοντας γνώση της «τυχαιότητας» των κεραιών ή των βαρών εκπομπής αυτών, δεν επηρεάζονται.

β. Space-Time Coding

Η κωδικοποίηση χώρου-χρόνου είναι μια τεχνική, η οποία λειτουργεί με την εκπομπή πολλαπλών αντιγράφων του σήματος στον πομπό από πολλαπλές διαφορετικές κεραίες και στη συνέχεια με την αξιοποίηση των διαφορετικών, πολλαπλών εκδοχών του εκπεμφθέντος σήματος στο δέκτη, έτσι ώστε να βελτιωθεί η αξιοπιστία των εκπεμπόμενων πληροφοριών.

Το εκπεμπόμενο σήμα, φεύγοντας από τις διαφορετικές κεραίες και ταξιδεύοντας στο φυσικό μέσο από τον πομπό προς το δέκτη, υφίσταται μια σειρά φυσικών διεργασιών που το υποβαθμίζουν όπως η ανάκλαση, η περίθλαση, η διάθλαση, η πρόσθεση θερμικού θορύβου στο δέκτη, διεργασίες οι οποίες δεν λειτουργούν όμοια για κάθε εκδοχή του σήματος αυτού. Κατά συνέπεια, κάποιες από τις εκδοχές του ληφθέντος σήματος θα είναι πιο κοντά στην αρχική εκπεμπόμενη και κάποιες άλλες όχι. Η τεχνική της κωδικοποίησης χώρου-χρόνου λειτουργεί ακριβώς με αυτό τον τρόπο, συνδυάζει όλες τις ληφθείσες εκδοχές του αρχικού σήματος με το βέλτιστο τρόπο, έτσι ώστε να λάβει όσο δυνατό μεγαλύτερη από την αρχική εκπεμπόμενη πληροφορία χωρίς σφάλματα.

Από την πρώτη εμφάνιση της ιδέας δόθηκε ιδιαίτερο ενδιαφέρον, καθώς η παραπάνω τεχνική έμοιαζε να μπορεί να αντισταθμίσει σε μεγάλο βαθμό το φαινόμενο των διαλείψεων αλλά και του θερμικού θορύβου στο δέκτη. Μελετήθηκαν δε διάφορες εκδοχές, με πολλαπλές κεραίες εκπομπής και λήψης (συστήματα MIMO), όπως και με πολλαπλές στον πομπό/δέκτη και μία κεραία στο δέκτη/πομπό αντίστοιχα (συστήματα MISO και SIMO), οι οποίες αρχικά έκαναν χρήση συνελικτικών κωδίκων.

Μέχρι το 1998 οι τεχνικές διαφορισμού εφαρμόζονταν αποκλειστικά στο δέκτη, κάνοντας χρήση αλγορίθμων όπως ο MRC (Maximum Ratio Combining). Το βασικό μειονέκτημα των υπόψη τεχνικών ήταν ότι οι πολλαπλές κεραίες στο δέκτη δημιουργούσαν πρόβλημα, καθώς κάθε μία απαιτούσε τη δικιά της RF αλυσίδα, γεγονός μη πρακτικό, ιδιαίτερα για τις συσκευές κινητής τηλεφωνίας που έπρεπε να κρατιούνται σε μικρή κλίμακα κατασκευής και με μικρή κατανάλωση ενέργειας.

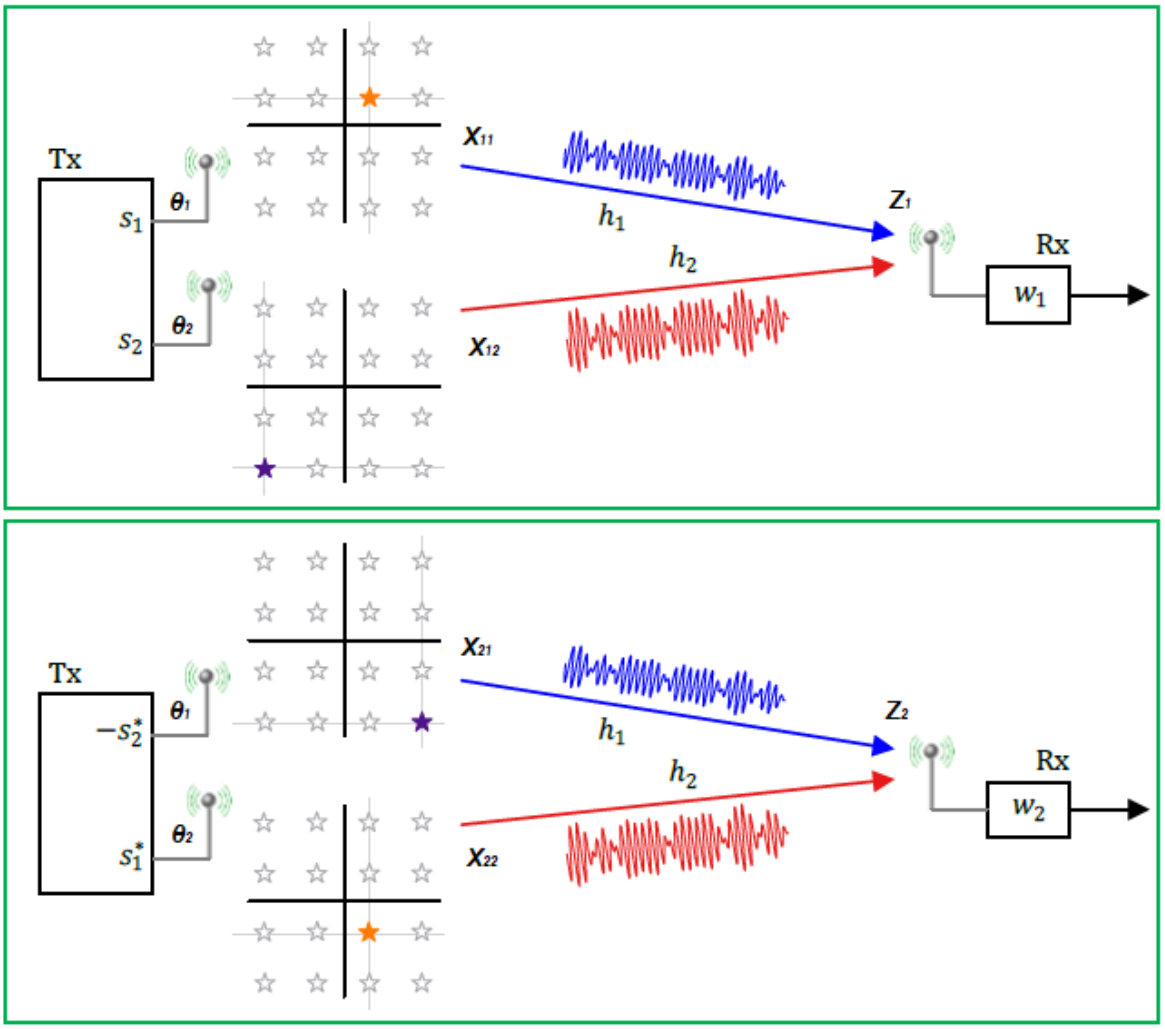
Ο Siavash Alamouti πρότεινε τότε [31], τη χρήση block κωδικών STBC (Space-Time Block Code) για εφαρμογή διαφορισμού στην εκπομπή του τηλεπικοινωνιακού συστήματος και απέδειξε ότι είναι δυνατό να επιτύχουμε τα ίδια αποτελέσματα με πολλαπλές κεραίες στον πομπό και μία κεραία στο δέκτη (σύστημα MISO). Επιπλέον απέδειξε ότι η ανάκτηση των δεδομένων στο δέκτη μπορούσε να γίνει με γραμμική υπολογιστική πολυπλοκότητα, απαιτώντας έτσι επεξεργαστική ισχύ παρόμοια με αυτή του αλγορίθμου MRC. Το απλουστευμένο σχήμα κωδικοποίησης Alamouti για δύο κεραίες εκπομπής και μία λήψης, συνήθως απεικονίζεται με έναν 2x2 πίνακα, όπου οι στήλες παριστάνουν διαφορετικά timeslots, ενώ οι γραμμές τις 2 κεραίες εκπομπής:

$$C = \begin{bmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{bmatrix}, \text{ όπου (*) ο συζυγής μιγαδικός}$$

Για πολλές τεχνικές ασφάλειας στο φυσικό επίπεδο, η εφαρμογή τους απαιτεί ακριβή εκτίμηση πληροφοριών για το τηλεπικοινωνιακό κανάλι (CSI – Channel State Information), διαφορετικά γίνονται λιγότερο αξιόπιστες και δημιουργούν πρόβλημα στο δέκτη. Στο σχήμα όμως STDC Alamouti, έχει προταθεί [32] μια τεχνική, η οποία δίνει τη δυνατότητα ασφαλούς επικοινωνίας μεταξύ πομπού και δέκτη, χωρίς τη γνώση του CSI από τον πομπό. Η υπόψη τεχνική χρησιμοποιεί την αμοιβαία μέτρηση του RSSI (Received Signal Strength Indicator) και από τις δύο πλευρές (πομπός-δέκτης), της οποίας η τιμή χρησιμοποιείται για να τροφοδοτήσει έναν αλγόριθμο ψευδοτυχαίων αριθμών που

με τη σειρά του θα παράξει δύο τιμές για ολίσθηση φάσης, τη ***θ1*** και τη ***θ2***. Οι δυο ολισθήσεις φάσεις εφαρμόζονται σε κάθε μία από τις κεραίες εκπομπής, έτσι ώστε για κάθε αυτούσια κωδική λέξη η πληροφορία ***s1*** και ***s2*** να κωδικοποιηθεί ως:

$$X = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} = \begin{bmatrix} s_1 e^{j\theta_1} & -s_2 e^{j\theta_2} \\ s_2^* e^{j\theta_1} & s_1^* e^{j\theta_2} \end{bmatrix}$$



Εικόνα 5.4.1

Αξίζει να σημειωθεί ότι το σχήμα, ακόμα και μετά τη στροφή φάσης που δέχτηκε, έχει διατηρήσει την ορθογωνιότητά του. Έτσι λοιπόν, για την εκπομπή του σήματος ***X*** από τον Bob, το ληφθέν σήμα για την Alice θα είναι:

$$z = Xh + n$$

$$z = H^{+(\theta_1,\theta_2)s+n}$$

$$\begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \end{bmatrix} = \begin{bmatrix} s_1 e^{j\theta_1} & -s_2 e^{j\theta_2} \\ s_2^* e^{j\theta_1} & s_1^* e^{j\theta_2} \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \end{bmatrix} \rightarrow$$

$$\begin{bmatrix} z_1 \\ -z_2^* \end{bmatrix} = \begin{bmatrix} h_1 e^{j\theta_1} & -h_2 e^{j\theta_2} \\ h_2^* e^{j\theta_1} & h_1^* e^{j\theta_2} \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} + \begin{bmatrix} n_1 \\ -n_2^* \end{bmatrix}$$

και με τη χρήση του αλγορίθμου MRC, μπορεί να γίνει εκτίμηση της εκπεμπόμενης πληροφορίας ως εξής:

$$\tilde{z}_{Alice} = H^{+(\theta_1,\theta_2)z}$$

Αντίστοιχα, ο Mallory εάν λαμβάνει έστω σήμα y:

$$y = Xg + e$$

τότε η εκτίμησή του για το εκπεμπόμενο σήμα θα είναι:

$$\tilde{y} = G(\theta_1, \theta_2)s + \tilde{e}$$

το οποίο μετά το decomposition θα είναι:

$$\tilde{Y}_{Mallory} = G^{+(\theta_1,\theta_2)y}$$

όπου H^{+}_{*} και G^{+}_{*} οι ψευδοαντίστροφοι πίνακες των H^{+}_{*} και G^{+}_{*}

Ο πομπός, εκπέμπει τα σύμβολα αφού παράξει και εφαρμόσει σε αυτά οποιοδήποτε ζευγάρι από τις διαθέσιμες στροφές φάσης και συνεπώς ο Mallory δεν μπορεί να υπολογίσει το ακριβές μήνυμα όπως αυτό αποστάλθηκε, αφού είναι απαραίτητο να γνωρίζει ακριβώς τον όρο $G(\theta_1, \theta_2)$.

Το πλεονέκτημα της υπόψη τεχνικής, όπως προαναφέρθηκε, είναι ότι μπορεί να επιτύχει ασφάλεια, χωρίς να είναι απαραίτητη η πρότερη γνώση του CSI για το τηλεπικοινωνιακό κανάλι. Για να καταφέρει ο Mallory να υποκλέψει την πληροφορία, θα πρέπει να υπολογίσει τα(θ_1, θ_2) μέσα από N^2 δυνατούς συνδυασμούς μεταξύ τους, γεγονός που σε περίπτωση που χρησιμοποιηθεί η μέθοδος του exhaustive search, απαιτεί υπολογιστική πολυπλοκότητα του επιπέδου $O(N^4)$ Παρόλα αυτά, δεν εγγυάται μεγάλο βαθμό ασφαλείας και παρουσιάζει αδυναμίες, καθώς έχει αποδειχθεί ότι με γνώση της μίας εκ των δύο στροφών φάσης και έχοντας εγγύτητα στο δέκτη (Alice), ο Mallory τελικά έχει αρκετά μεγάλη πιθανότητα να μπορεί να υποκλέψει την πληροφορία.

6. ΤΟ GNU RADIO

6.1 Τι είναι το GNU Radio [14]

Το GNU Radio είναι ένα ανοικτού κώδικα πακέτο λογισμικού, το οποίο πρωτοπαρουσιάστηκε το 1998 από τον Eric Blossom και όταν συνδυαστεί με hardware εξοπλισμό όπως ένα USRP, επιτρέπει την πλήρη ανάπτυξη εφαρμογών SDR. Το GNU Radio μπορεί να χρησιμοποιηθεί και χωρίς καμιά άλλη διασύνδεση hardware, για την υλοποίηση block διαγραμμάτων όπως στο παρακάτω σχήμα, στο οποίο έχει υλοποιηθεί ένα απλό διάγραμμα ροής στο GRC (GNU Radio Companion), το γραφικό εργαλείο σχεδίασης του GNU Radio:

Εικόνα 6.1.1

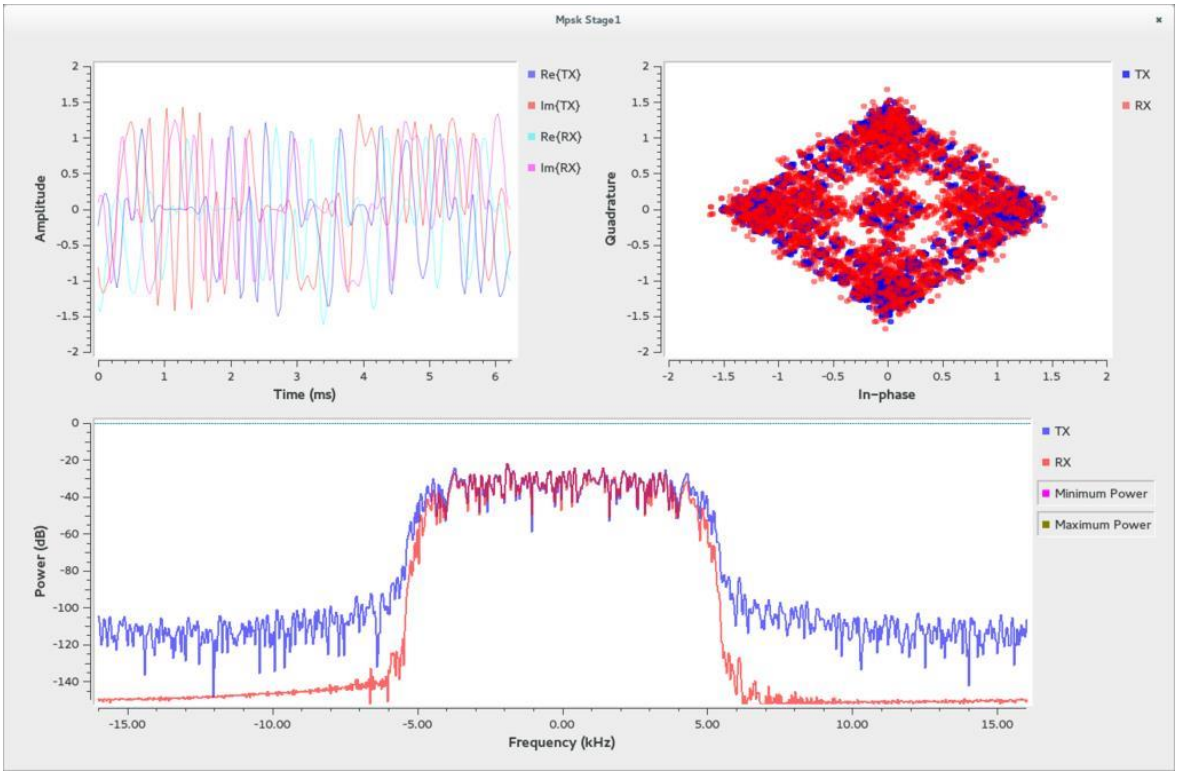
Το προτεινόμενο λειτουργικό σύστημα για την ανάπτυξη εφαρμογών SDR είναι Linux, ωστόσο μπορεί ακόμα να λειτουργήσει σε MS Windows χρησιμοποιώντας περιβάλλοντα που μοιάζουν με Linux, όπως για παράδειγμα το Cygwin ή το MinGW/MSYS αλλά και σε Mac OS και NetBSD.

Οι περισσότερες εφαρμογές του GNU Radio είναι γραμμένες σε Python, ενώ στα block όπου γίνεται η επεξεργασία σήματος χρησιμοποιείται C++. Εντολές Python χρησιμοποιούνται για έλεγχο όλων παραμέτρων του USRP που πρέπει να υλοποιηθούν σε λογισμικό, όπως η ισχύς εκπομπής, το κέρδος, η συχνότητα, η επιλογή κεραίας κ.λπ., κάποιες από τις οποίες μπορούν ακόμα και να τροποποιηθούν ενώ η εφαρμογή εκτελείται.

Η Python είναι μια αντικειμενοστραφής γλώσσα προγραμματισμού, γνωστή για την ευκολία σύνταξης. Είναι ελεύθερη γλώσσα γραμμένη σε πρότυπο ANSI C και εκτελείται σε Windows, Unix/Linux, MAC OS, Java, κ.λπ.. Λόγω της αντικειμενοστραφούς φύσης της, τα προγράμματα σε Python μπορούν να ενσωματώσουν κλάσεις γραμμένες σε άλλες αντικειμενοστραφείς γλώσσες, όπως η C++. Αυτό χρησιμοποιείται στο GNU Radio όπου τα block επεξεργασίας σήματος είναι γραμμένα σε C++ και η Python έρχεται να τα «κολλήσει» μεταξύ τους και να ελέγξει το διάγραμμα ροής. Αυτό γίνεται χρησιμοποιώντας το ανοικτού κώδικα εργαλείο που καλείται Simplified Wrapper and Interface Generator – SWIG, το οποίο κάνει αυτή τη διασύνδεση δυνατή δημιουργώντας κοινές βιβλιοθήκες εξίσου για τη C++ και την Python.

Το GNU Radio είναι χτισμένο πάνω σε δύο θεμελιώδεις δομές, block επεξεργασίας σήματος και διαγράμματα ροής. Τα block είναι φτιαγμένα ώστε να έχουν ένα καθορισμένο αριθμό πορτών εισόδου και εξόδου, αποτελώντας έτσι δομικά στοιχεία όπου γίνεται επεξεργασία σήματος. Όταν τα block αυτά συνδεθούν κατάλληλα τότε δημιουργείται ένα διάγραμμα ροής. Τα block του GNU Radio μπορούν να κατηγοριοποιηθούν γενικά σε δεξαμενές (sinks), πηγές (sources) και φίλτρα (filters). Οι πηγές είναι block που έχουν μόνο έξοδο, καμία είσοδο και χρησιμοποιούνται ως το πρώτο στοιχείο στο προς κατασκευή διάγραμμα ροής. Οι δεξαμενές αντίθετα, στερούνται εξόδων και έχουν μόνο είσοδο και χρησιμοποιούνται ως τελικά στοιχεία. Ως φίλτρα μπορούν να θεωρηθούν όλα τα ενδιάμεσα block και έχουν και εισόδους και εξόδους.

Ένας αριθμός από block όπως για διάφορες τεχνικές διαμόρφωσης/ αποδιαμόρφωσης, διάφορα φίλτρα, ανιχνευτές σήματος κτλ υπάρχουν στη βασική βιβλιοθήκη του GNU Radio, πολλές φορές όμως όπου ένα απαιτούμενο block για τη σχεδίαση δεν υπάρχει, μπορεί να γραφεί εξαρχής. Γραφικά περιβάλλοντα όπως δεξαμενές FFT και παλμογράφοι υποστηρίζονται ακόμα από το GNU Radio (GRC). Τα διαγράμματα ροής δημιουργούνται είτε ως ιεραρχικά block είτε ως top block. Τα top blocks είναι κορυφαίου επιπέδου διαγράμματα ροής και περιέχουν όλα τα άλλα διαγράμματα ροής και δεν έχουν πόρτες εισόδου/εξόδου. Τα ιεραρχικά block, από την άλλη πλευρά, περιέχουν ένα συγκεκριμένο αριθμό πορτών εισόδου/εξόδου για διασύνδεση σε άλλα block και οι οποίες προωθούνται στην αμέσως επόμενη ανώτερη κλάση μέσω κλήσεως συναρτήσεων. Όλα τα βασικά block επεξεργασίας σήματος είναι συνδεδεμένα με αυτό τον τρόπο εντός ιεραρχικών block και επομένως όλο το ανώτερου επιπέδου block μπορεί να χρησιμοποιηθεί ως ενιαίο.



Εικόνα 6.1.2

Η επικοινωνία μεταξύ των block επιτυγχάνεται με τη χρήση data streams, όπου όλα τα στοιχεία του stream αποτελούνται από τον ίδιο τύπο δεδομένων. Για να γίνεται σωστά η αρχικοποίηση του data stream, πρέπει οι τύποι δεδομένων μεταξύ της εξόδου ενός block και της εισόδου σε ένα άλλο να έχουν καθορισθεί ίδιοι. Οι υποστηριζόμενοι από το GNU Radio τύποι δεδομένων είναι οι παρακάτω:

- Byte , 1 byte data
- Short, 2 byte integer
- Int, 4 byte integer
- Float, 4 byte floating point
- Complex, ζεύγος float, ισοδύναμο με 8 bytes

Ο τύπος data που χρησιμοποιείται καθορίζεται στο τέλος του block, για παράδειγμα το gr_multiply_ii θα πάρει δύο integers ως είσοδο και θα βγάλει integer ως έξοδο ενώ το gr_multiply_ff θα κάνει το ίδιο με float και θα παράξει ως αποτέλεσμα έναν float. Block τα οποία μετατρέπουν data types από τη μια μορφή στην άλλη όπως π.χ. το gr_complex_to_float block, επίσης υποστηρίζονται από το GNU Radio.

Ένα από τα πιο απλά παραδείγματα του GNU Radio είναι αυτό του dial_tone, το οποίο χαρακτηρίζεται, σε παραλληλία με άλλες γλώσσες προγραμματισμού ως το «Hello World» του GNU Radio. Στο παράδειγμα αυτό, το οποίο για λόγους πληρότητας παρατίθεται παρακάτω ώστε να δοθεί μια συνοπτική εικόνα της λειτουργίας του GNU Radio για χρήση από τερματικό, παράγονται δύο ημιτονικά σήματα ίδιου πλάτους στις συχνότητες 350 Hz και 440 Hz, τα οποία αναπαριστούν τον dial τόνο στην σταθερή τηλεφωνία των ΗΠΑ και στέλνονται για αναπαραγωγή στην κάρτα ήχου.

```
#!/usr/bin/env python

from gnuradio import gr
from gnuradio import audio, analog

class my_top_block(gr.top_block):
    def __init__(self):
        gr.top_block.__init__(self)

        sample_rate = 32000
        ampl = 0.1

        src0 = analog.sig_source_f(sample_rate, analog.GR_SIN_WAVE, 350, ampl)
        src1 = analog.sig_source_f(sample_rate, analog.GR_SIN_WAVE, 440, ampl)
        dst = audio.sink(sample_rate, "")
        self.connect(src0, (dst, 0))
        self.connect(src1, (dst, 1))

if __name__ == '__main__':
    try:
        my_top_block().run()
```

```
except [[KeyboardInterrupt]]:
    pass
```

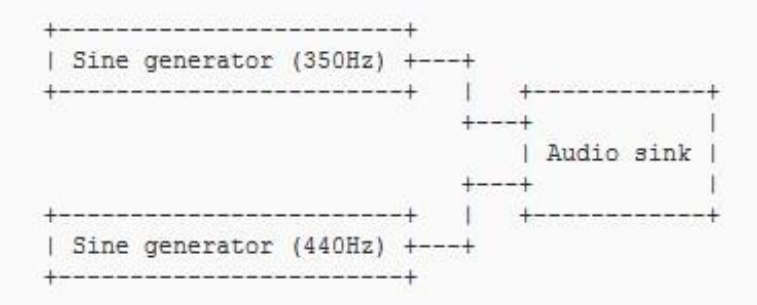
Η πρώτη γραμμή είναι γνωστή σε όποιον έχει το ελάχιστο υπόβαθρο σε συστήματα Linux. Λέει στο shell ότι αυτό το αρχείο είναι ένα αρχείο Python και επομένως θα πρέπει να χρησιμοποιηθεί ο διερμηνέας της Python για να εκτελεσθεί. Η γραμμή αυτή είναι απαραίτητη για να εκτελεσθεί το πρόγραμμα απευθείας από το τερματικό.

Οι γραμμές 3 και 4 κάνουν import τα ανάλογα modules για να εκτελεσθεί το GNU Radio. Το import είναι ανάλογο του #include της C/C++. Εδώ εισάγονται τρία modules από το GNU Radio, τα gr, audio και analog. Το πρώτο, είναι το βασικό module του GNU Radio, το οποίο είναι απαραίτητο για να εκτελεσθεί οποιαδήποτε εφαρμογή GNU Radio. Το δεύτερο και τρίτο εισάγουν τα modules όπου υπάρχουν audio device blocks και blocks με αναλογικές λειτουργίες σημάτων και διαμόρφωσης.

Οι γραμμές 6-17 ορίζουν μια κλάση η οποία καλείται my_to_block προέρχεται από μια άλλη κλάση, την gr.top_block και είναι στην ουσία το container μέσα στο οποίο βρίσκεται το διάγραμμα ροής. Αφού η μητρική κλάση είναι η gr.top_block, αυτό δίνει τη δυνατότητα αυτόματα να κληρονομηθούν στη νέα κλάση όλες οι δυνατότητες και συναρτήσεις που είναι απαραίτητες για πρόσθεση block και σύνδεση μεταξύ τους.

Μόνο μία συνάρτηση ορίζεται για την κλάση αυτή, η __init__(), η οποία είναι ο constructor της συγκεκριμένης κλάσης. Στην πρώτη γραμμή αυτής της συνάρτησης (γραμμή 8) καλείται ο constructor της μητρικής κλάσης (στην Python, αυτό όπως και πολλά άλλα πράγματα πρέπει να γίνονται κατηγορηματικά, να δηλώνονται σαφώς, αυτή είναι μια από τις θεμελιώδεις ιδιότητές της). Στη συνέχεια ορίζονται δύο μεταβλητές, το sample_rate και το ampl. Αυτές θα ελέγχουν το sample rate και το επιθυμητό πλάτος των γεννητριών σήματος.

Πριν εξηγήσουμε τις επόμενες γραμμές, ας ρίξουμε μια ματιά παρακάτω στο διάγραμμα ροής του παραδείγματος:



Σχήμα 6.1.3

Αποτελείται από τρία blocks και δύο συνδέσεις. Τα block καθορίζονται στις γραμμές 13-15 όπου παράγονται δύο σήματα, τα src0 και src1. Αυτές οι πηγές παράγουν διαρκώς ημιτονικά σήματα στις δοθείσες συχνότητες και στον

καθορισμένο ρυθμό δειγματοληψίας. Το πλάτος εξόδου καθορίστηκε μέσω της μεταβλητής ampl σε 0.1. Το γράμμα «f» στο όνομα του Block analog.sig_source_f δείχνει ότι η έξοδος είναι τύπου float, όπως και πρέπει να γίνεται αφού η audio sink δέχεται είσοδο δειγμάτων floating point με πλάτος από -1 έως +1, σημεία στα οποία θα πρέπει να δίνεται προσοχή, όπως αναλύθηκε πιο πάνω.

Η signal sink ορίζεται στη γραμμή 15, audio.sink() και επιστρέφει ένα block το οποίο παίζει το ρόλο μιας κάρτας ήχου και αναπαράγει ότι δείγματα του μεταβιβάζονται. και εδώ πρέπει να τονισθεί ότι η συχνότητα δειγματοληψίας πρέπει να καθορίζεται σαφώς καθώς το GNU Radio δεν είναι σε θέση να εξάγει την αρμόζουσα κατά περίπτωση συχνότητα δειγματοληψίας από το είδος των στοιχείων που τοποθετούνται και μόνο ή από τις ροές δεδομένων.

Οι γραμμές 16 και 17 συνδέουν τα blocks. Η γενική σύνταξη για διασύνδεση των block είναι self.connect (block1, block2, block3,…), η οποία θα συνδέσει την έξοδο του block1 στην είσοδο του block2, την έξοδο του block2 στην είσοδο του block3 κ.ο.κ.. Η εντολή connect () δηλαδή μπορεί να χρησιμοποιηθεί μία φορά μόνο. Εδώ ακολουθείται ειδική σύνταξη αφού θέλουμε να συνδέσουμε τη src0 με την πρώτη είσοδο του dst και τη src1 με τη δεύτερη είσοδο του dst.

Αυτή ήταν όλη η διαδικασία για τη δημιουργία του διαγράμματος ροής. Οι τελευταίες 5 γραμμές δεν κάνουν τίποτε άλλο παρά να ξεκινήσουν το διάγραμμα (γραμμή 22). Οι εντολές try και except απλώς σιγουρεύουν ότι το διάγραμμα (το οποίο κανονικά θα έτρεχε για άπειρο χρόνο) σταματά όταν πατιέται Ctrl+C, το οποίο στην ουσία εγείρει ένα interrupt της Python.

Τέλος, πρέπει να σημειωθεί ότι εδώ η κλάση my_top_block εκτελείται χωρίς να κατασκευασθεί ένα instance αυτής πρώτα. Στη Python αυτό είναι γενικά αποδεκτό, ιδιαίτερα όταν έχουμε μια κλάση από την οποία θα κατασκευασθεί ένα και μόνο instance ούτως ή άλλως. παρόλα αυτά, θα μπορούσε κι εδώ να κατασκευασθεί ένα instance αυτής της κλάσης και στη συνέχεια να κληθεί με τη run().

Το παραπάνω παράδειγμα αναλύθηκε ώστε καταστεί όσο το δυνατό πιο σαφής ο τρόπος με τον οποίο η Python και το GNU Radio συνεργάζονται για να κατασκευασθεί το επιθυμητό διάγραμμα ροής. Αυτή η διαδικασία είναι μονόδρομος για κατασκευή block τα οποία δεν υπάρχουν στις βιβλιοθήκες του γραφικού εργαλείου GRC, το οποίο απλοποιεί σε εξαιρετικό βαθμό τα πράγματα, παρέχοντας δυνατότητα ταχύτατης σχεδίασης και ανάπτυξης εφαρμογών.

6.2 Γιατί GNU Radio και όχι Matlab ή LabView

Το Simulink της Mathworks, όπως επίσης και το LabView της Texas Instruments είναι επιστημονικά εργαλεία τα οποία επίσης υποστηρίζονται από το USRP N210 της Ettus Research μέσω του UHD driver, όπως και το GNU Radio. Η υλοποίηση ωστόσο ενός συστήματος πομποδέκτη σε SDR με τη χρήση Simulink ή LabView ή μέσω του GNU-Radio πρέπει κάθε φορά να εκτιμάται λαμβάνοντας υπόψη τους παρακάτω παράγοντες:

α. Η εφαρμογή που πρόκειται να αναπτυχθεί θα είναι real-time ή off-line;

β. Υπάρχει ανάγκη για ανάπτυξη γραφικού block διαγράμματος των βαθμίδων ή όχι;

γ. Θέλουμε να χρησιμοποιήσουμε τη φυσική γλώσσα του συστήματος ή να γίνει μεταγλώττιση;

Έτσι σε γενικές γραμμές από την υλοποίηση ενός project σε Matlab ή LabView ή με GNU Radio, μπορούν να εξαχθούν τα παρακάτω συμπεράσματα:

α. Το Simulink χρησιμοποιείται ευρέως για off-line ανάλυση (ακόμα και με τη χρήση του USRP), ενώ το GNU Radio χρησιμοποιείται συνήθως για real-time ανάλυση.

β. Στο Simulink απαραίτητο εργαλείο για γραφικό τρόπο λειτουργίας είναι το Simulink, ενώ το GRC είναι το εξ' ορισμού εργαλείο ανάπτυξης για εφαρμογές SDR με το GNU Radio (περιλαμβάνεται στο πακέτο εγκατάστασης του GNU Radio).

γ. Για να επιτευχθεί ανάλυση real-time, στο Simulink ο κώδικας πρέπει πρώτα να μεταφραστεί σε γλώσσα C και να γίνει μεταγλώττιση, χρησιμοποιώντας εργαλεία όπως ο Matlab Coder ή ο Simulink Coder. Αυτοί οι μεταφραστές υποστηρίζουν μόνο ένα τμήμα ττου πυρήνα των δυνατοτήτων της γλώσσας του Matlab. Στο GNU Radio δεν υπάρχει τέτοιος περιορισμός, όλες οι δυνατότητες υποστηρίζονται πλήρως, ο κώδικας είναι εξ' ολοκλήρου ανοιχτός και επιδέχεται οποιαδήποτε μετατροπή.

δ. Το διάγραμμα ροής του GNU Radio είναι γραμμένο σε Python, με αποτέλεσμα να μη χρειάζεται να γίνει compile πριν την εκτέλεση, για ανάλυση σε real-time εφαρμογές.

ε. Το GNU Radio έχει καλύτερη υποστήριξη στους drivers του USRP, το Matlab δεν υποστηρίζει το Legacy USRP.

στ. Το γραφικό περιβάλλον του GRC χρησιμοποιεί διαφορετικά χρώματα για να χαρακτηρίσει τους διαφορετικούς τύπους δεδομένων σε κάθε block, διευκολύνοντας έτσι το χρήστη, το Simulink μόνο το μαύρο χρώμα.

6.3 Αρχικοποίηση PC για χρήση USRP N210 με GRC

Για την υλοποίηση της παρούσας πτυχιακής εργασίας επιλέχθηκε η εγκατάσταση της έκδοσης Ubuntu 20.04.05 LTS 64-bit Linux. Η εγκατάσταση είναι σχετικά απλή και στο διαδίκτυο [15] μπορεί κάποιος ακόμα και άπειρος χρήστης να αναζητήσει και να λάβει σαφείς οδηγίες βήμα προς βήμα για τη συνολική εγκατάσταση του λογισμικού.

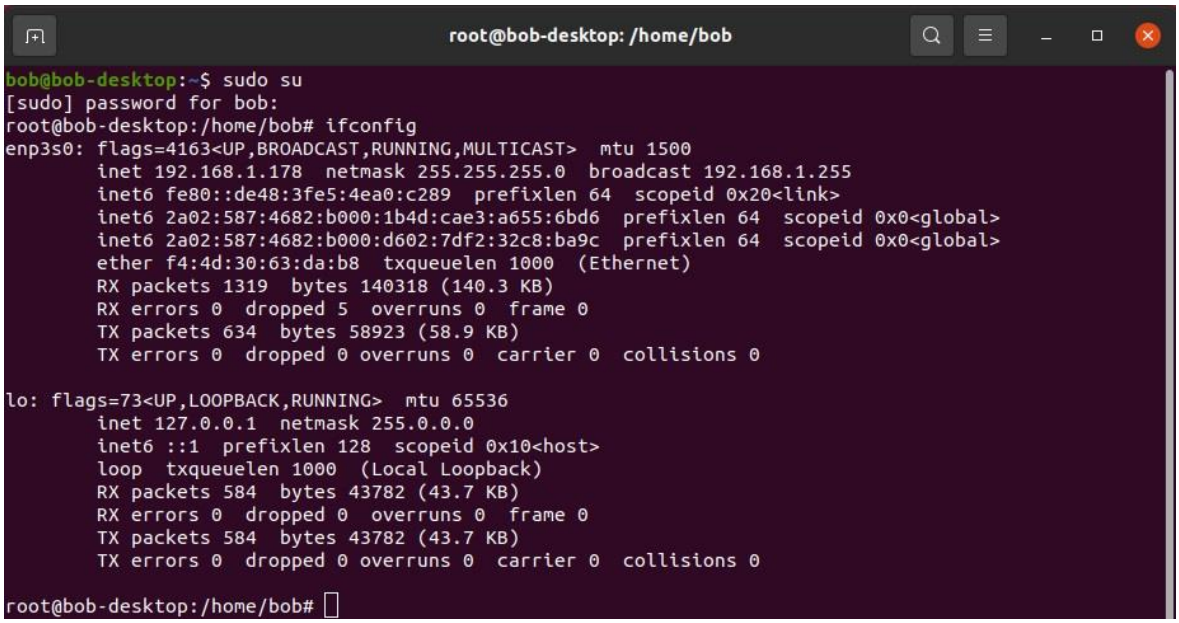
Αφού εγκατασταθεί το πακέτο του Ubuntu, είναι απαραίτητη στο Linux η εγκατάσταση του βασικού πακέτου ανοικτού λογισμικού UHD (όπως και για MS Windows ή Mac OS ανάπτυξη εφαρμογών SDR) ώστε να καταφέρει σε πρώτη φάση να αναγνωρίσει τη συσκευή USRP, η οποία είναι διασυνδεδεμένη στον τερματικό Η/Υ, έστω του Bob:

```
bob@Bob-PC:~$ sudo apt-get install uhd-host
[sudo] password for bob:
Reading package lists... Done
……(εκτέλεση)….
```

Μετά την εγκατάσταση του βασικού πακέτου του UHD, ο χρήστης εκτελέσει διαδοχικά στο τερματικό τις παρακάτω εντολές με δικαιώματα root ώστε να γίνουν τα απαραίτητα updates στο πακέτο UHD και να εγκατασταθεί το GNU Radio:

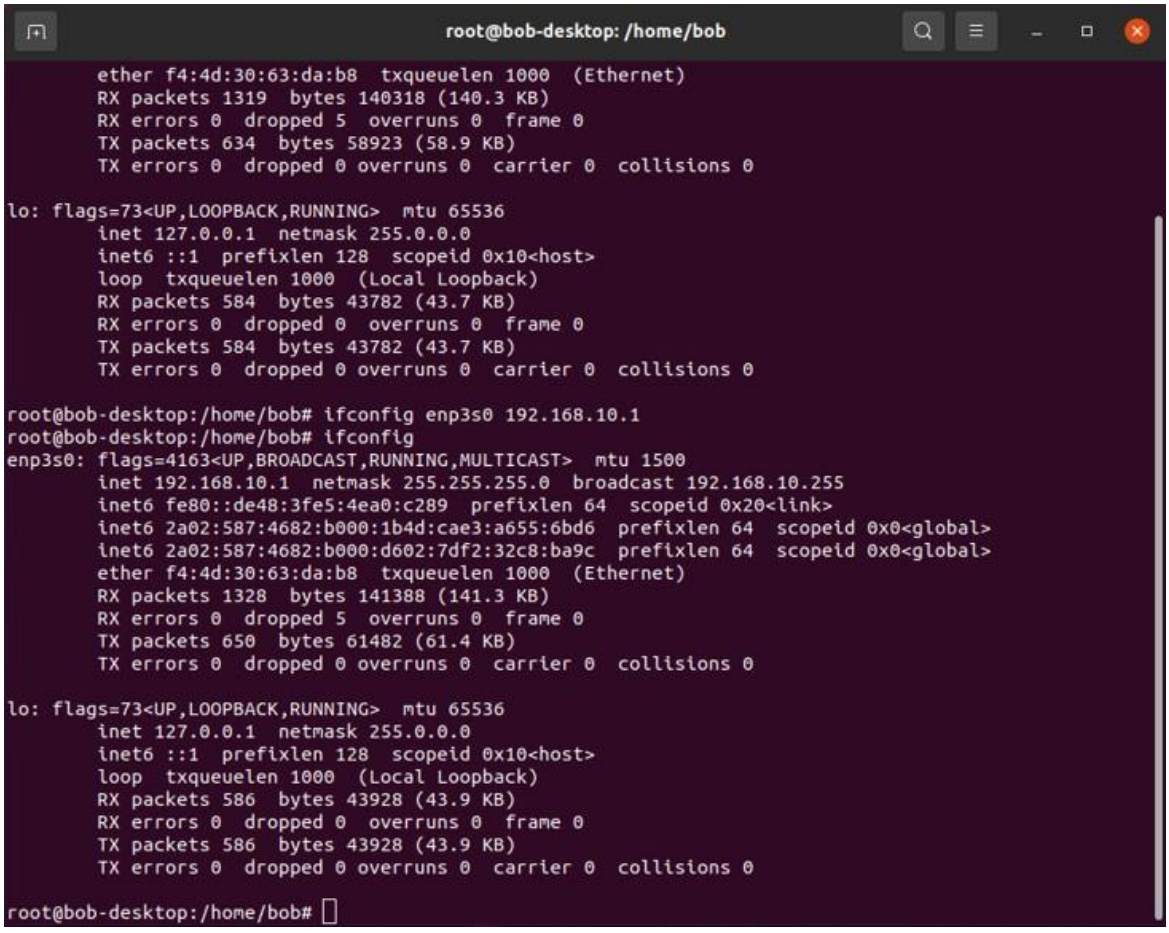
```
sudo add-apt-repository ppa:gnuradio/gnuradio-releases

sudo apt-get update

sudo apt-get install gnuradio python3-packaging
```

Από το σημείο αυτό και μετά, με την ολοκλήρωση δηλαδή του update του UHD, συνδέοντας στο pc τη συσκευή USRP μέσω του καλωδίου Ethernet και την τροφοδοτούμε με ρεύμα, προκειμένου να εκτελέσουμε για αρχή μια υποτυπώδη συνομιλία μέσω τερματικού. **Θα πρέπει επίσης να τονιστεί το γεγονός ότι οι συσκευές USRP N210 της Ettus, επικοινωνούν με το host pc μόνο εφόσον αυτό διαθέτει κάρτα Gbit Ethernet.** Σε διαφορετική περίπτωση, όπως συνέβη κατά την εκπόνηση της παρούσας πτυχιακής εργασίας όπου δαπανήθηκε αρκετός χρόνος μέχρι να διαπιστωθεί το παραπάνω, αφού η εταιρία στο specification της για τη συσκευή δεν αναφέρει τον περιορισμό αυτό, το host pc δεν θα καταφέρει ποτέ να αναγνωρίσει τη συσκευή και κατ' επέκταση ο χρήστης να προχωρήσει στη δημιουργία οποιασδήποτε εφαρμογής. Μόνη εξαίρεση αποτελεί η διασύνδεση της συσκευής με παλιότερου τύπου pc (NIC με 100 Mbit Ethernet), μέσω switch Gbit Ethernet, όπου εκεί κατά κάποιο τρόπο γίνεται ένα bypass στον περιορισμό αυτό, αφού η πρώτη πόρτα που βλέπει το USRP είναι Gbit, πλην όμως το τελικό bandwidth περιορίζεται σημαντικά, όπως αναλύθηκε σε προηγούμενη ενότητα. Κατόπιν της σύνδεσης της συσκευής, ελέγχουμε τα interface δικτύου του pc μας με την εντολή ifconfig:



Εικόνα 6.3.1

Οι συσκευές USRP N210 έρχονται στο χρήστη με προρυθμισμένη στατική IP την 192.168.10.2, συνεπώς για να επικοινωνήσουμε με αυτή θα πρέπει να ρυθμίσουμε επίσης μια στατική IP στη NIC του host pc μας, το οποίο γίνεται με την εντολή ifconfig enp3s0 192.168.10.1, όπου enp3s0 το όνομα της NIC, το οποίο μπορεί να διαφέρει από ένα υπολογιστή σε άλλο:



Εικόνα 6.3.2

Αφού εκτελεστεί και η παραπάνω εντολή, το τερματικό μας επιστρέφει τη νέα κατάσταση της NIC με αλλαγμένη την IP. Από αυτό το σημείο και μετά είμαστε σε θέση να «μιλήσουμε» στη συσκευή. Πληκτρολογώντας uhd_ και με το Tab του πληκτρολογίου, μας ανοίγει ένα suggestion menu, το οποίο αποτελείται από βασικές εντολές της βιβλιοθήκης του UHD, το οποίο εγκαταστήσαμε προηγουμένως. Μέσω της εντολής uhd_find_devices, παίρνουμε το παρακάτω αποτέλεσμα που φαίνεται στην εικόνα 6.3.3, ότι δηλαδή η συσκευή βρέθηκε και είναι τύπου USRP2, έχει IP 192.168.10.2 και serial F51986. Επιβεβαιώνουμε την επικοινωνία με ένα ping στην IP της και μας επιστρέφει επίσης το αποτέλεσμα. Η στατική προρυθμισμένη IP του USRP μπορεί βέβαια να αλλάξει σε οποιαδήποτε επιθυμητή από το χρήστη (προσοχή στο subnet mask, πρέπει να είναι ίδιο και στο host) με την εντολή:

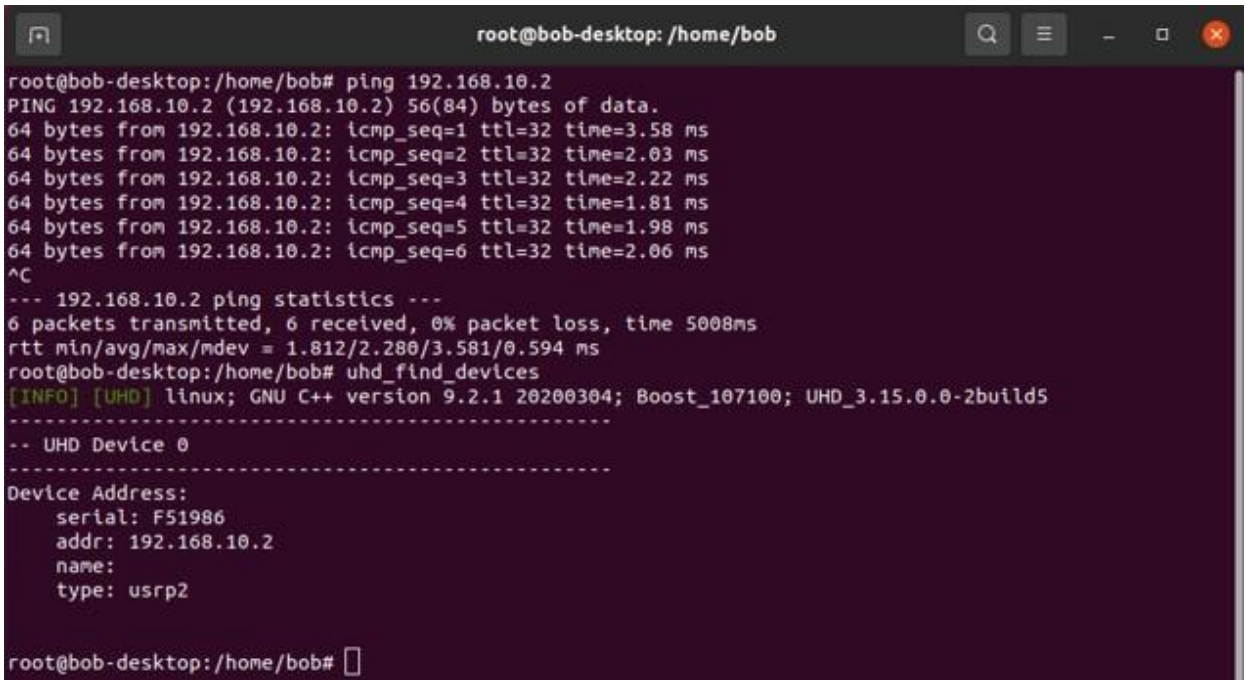
usrp_burn_mb_eeprom--key=ip-addr--val=XXX.XXX.XXX.XXX

,όπου X η επιθυμητή IP.

Στη συνέχεια, προκειμένου για πρώτη χρήση του USRP (χωρίς εγκατεστημένο firmware), θα πρέπει να εγκατασταθεί το ROM image του και το firmware για το FPGA, τα οποία αφού τα κατεβάσουμε από το site της εταιρίας, από το εξής directory (http://files.ettus.com/binaries/master_images/), εκτελούμε διαδοχικά τις παρακάτω δύο εντολές:

1. usrp_n2xx_net_burner.py –addr=XXX.XXX.XXX.XXX –fw=<Path>
2. usrp_n2xx_net_burner.py –addr=XXX.XXX.XXX.XXX –fpga=<Path>

,όπου το «Path» υποδηλώνει τη θέση που βρίσκονται τα δύο αρχεία που μόλις κατεβάσαμε στο host pc μας.



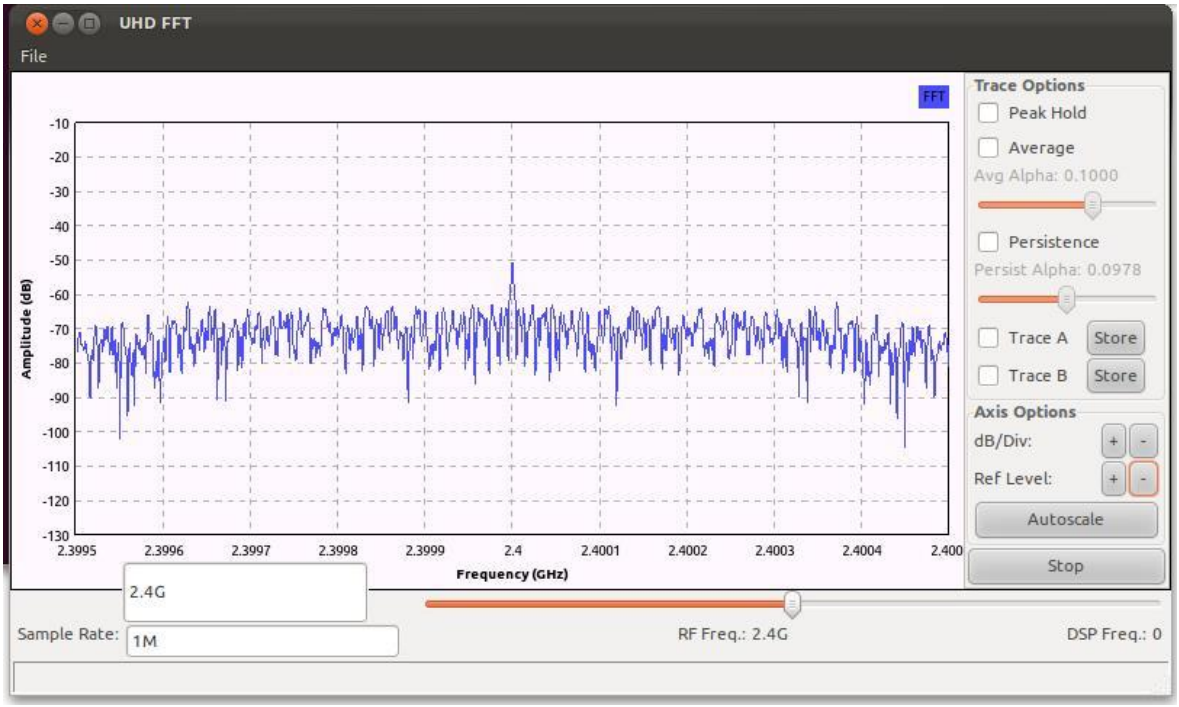
Εικόνα 6.3.3

./.

Επισημαίνεται ότι η διαδικασία αλλαγής IP, εγγραφής του ROM image και εγκατάστασης του firmware για το FPGA μπορεί να απλοποιηθεί μέσω του γραφικού εργαλείου NI-USRP της National Instruments για Windows OS, όπου τα παραπάνω γίνονται με μεγαλύτερη απλότητα. Για να χρησιμοποιηθεί το εργαλείο θα πρέπει προηγουμένως να εγκατασταθεί και το πακέτο UHD.

Ιδιαίτερη προσοχή πρέπει να τηρείται κατά την ολοκλήρωση της παραπάνω διαδικασίας (εγγραφή ROM image και εγκατάσταση firmware) **καθώς μετά τα βήματα που αναφέρθηκαν απαιτείται αποσύνδεση της συσκευής από την τροφοδοσία και επανεκκίνηση, διαφορετικά μπορεί να χάσει όλες τις ρυθμίσεις της, συμπεριλαμβανόμενης και της στατικής IP**. Εάν συμβεί το παραπάνω τότε δεν υπάρχει τρόπος να δούμε τη συσκευή από το τερματικό, οπότε η μόνη λύση είναι να ανοιχτεί η συσκευή και να πατηθεί ο διακόπτης «s2», οποίος βρίσκεται πάνω στη μητρική κάρτα της, ενώ ταυτόχρονα γίνεται επανεκκίνηση, ώστε να επανέλθει στις εργοστασιακές της ρυθμίσεις.

Μετά από την παραπάνω διαδικασία, προαιρετικά εκτελούμε την εντολή uhd_fft –freq 2.4e9 από το προτεινόμενο menu, η οποία θα μας επιστρέψει το παράθυρο της εικόνας 6.3.4, το οποίο αποτελεί ένα στοιχειώδες εργαλείο επισκόπησης του λαμβανόμενου φάσματος της UHD βιβλιοθήκης από τη συσκευή μας και θα επιβεβαιώσει την ορθή λειτουργία της. Το παράθυρο αυτό εκτελεί έναν fft στο φάσμα εισόδου και παρουσιάζει το αποτέλεσμα σε ζωντανό χρόνο. Στο παράδειγμα που παρατίθεται διακρίνεται καθαρά το spike στα 2.4 GHZ, όπου είναι η συχνότητα εκπομπής του οικιακού WiFi, το οποίο εξέπεμπε κατά την λήψη του snapshot.



Εικόνα 6.3.4

Στη συνέχεια, το τελευταίο βήμα που πρέπει να γίνει εάν επιθυμούμε γραφική σχεδίαση εφαρμογών και όχι εκτέλεση των προγραμμάτων της Python από το τερματικό, είναι η εγκατάσταση του προγράμματος GRC. Η εγκατάσταση αυτή μπορεί πλέον για λόγους απλότητας να γίνει μέσα από το software center του πλευρικού μενού του Ubuntu, μιας και πλέον η εφαρμογή υποστηρίζεται επίσημα από την κοινότητα ή απλά ανοίγοντας το τερματικό δίνοντας δικαιώματα super user, σε περίπτωση που το είχαμε κλείσει προηγουμένως και εκτελώντας την εντολή:

```
bob@Bob-PC:~$ sudo apt-get install grc
[sudo] password for bob:
……(εκτέλεση)….
```

Η παραπάνω ρουτίνα θα εγκαταστήσει το GRC, το οποίο μπορούμε πλέον να το βρούμε σαν εφαρμογή στο dash του Ubuntu και να το εκτελέσουμε. Το GRC είναι έτοιμο για χρήση και ο χρήστης είναι έτοιμος να φτιάξει την πρώτη του εφαρμογή-πομποδέκτη μέσω του γραφικού περιβάλλοντος του GRC που μόλις εγκαταστάθηκε.

7. ΥΛΟΠΟΙΗΣΕΙΣ ΣΕ SOFTWARE DEFINED RADIO

7.1 Αποφάσεις επί της τελικής υλοποίησης

Αναλύοντας στο κεφάλαιο 5 πιθανούς τρόπους υλοποίησης ασφάλειας στο φυσικό επίπεδο και με βάση τον διατιθέμενο εξοπλισμό, προέκυψαν τα παρακάτω συμπεράσματα:

α. Η υλοποίηση τεχνικών που βασίζονται στα χαρακτηριστικά των κεραιών εκπομπής και λήψης (τεχνικές χώρου και χώρου-χρόνου) απαιτούν την ύπαρξη συσκευών USRP που έχουν δυνατότητα MIMO, στην προκειμένη δε περίπτωση τα υπάρχοντα USRP N210 της Ettus Research, έχουν την υπόψη δυνατότητα, μετά όμως από αναβάθμιση (επιπλέον υλικά όπως κεραίες, καλώδια συνδεσμολογίας, κ.λπ.), τα οποία δεν διατίθενται στη συγκεκριμένη χρονική στιγμή).

β. Το σύνολο των τεχνικών ασφαλείας φυσικού επιπέδου, απαιτούν την προ της έναρξης ασφαλούς επικοινωνίας «συμφωνία» μεταξύ πομπού και δέκτη, για ένα «μυστικό κλειδί», το οποίο είτε αφορά σε κρυπτογράφηση σε ανώτερο επίπεδο ή σε γνώση μόνο στα νόμιμα μέλη συγκεκριμένων χαρακτηριστικών (αναλόγως τη χρησιμοποιούμενη τεχνική), τα οποία θα τους βοηθήσουν να εξάγουν την αρχική πληροφορία από το κανάλι, αφήνοντας εκτός του επιτιθέμενο.

γ. Η πιο πλήρης θεωρητικά τεχνική, από άποψης εφαρμογής σε συστήματα ad-hoc, τα οποία μπορούν θεωρητικά να εκκινήσουν ασφαλή επικοινωνία μετρώντας χαρακτηριστικά όπως το RSSI, είναι αυτή του space-time coding. Εδώ πρέπει να σημειωθεί ότι σε αυτή την προσέγγιση, εξετάζεται μόνο η αρχή της εμπιστευτικότητας και όχι της αυθεντικότητας, με άλλα λόγια, θα πρέπει να βρεθεί άλλος τρόπος ώστε οι οντότητες να αποδείξουν την ταυτότητά τους στο δίκτυο.

δ. Η λήψη μετρήσεων για το RSSI είναι απαραίτητο να γίνει για ένα ικανό χρονικό διάστημα, να παρθούν πολλές τιμές και ιδανικά η σχετική θέση πομπού και δέκτη να μεταβάλλεται διαρκώς ώστε να αλλάζουν τα χαρακτηριστικά του διαύλου, άρα και η ποικιλία των μετρήσεων. Με τον τρόπο αυτό αυξάνει η εντροπία του συνόλου τιμών των μετρήσεων και κατ' επέκταση η τυχαιότητα στις τελικές τιμές. Δημιουργείται λοιπόν ένα τελικό σύνολο τιμών, το οποίο γνωρίζει μόνο ο πομπός και ο δέκτης και όχι ο επιτιθέμενος, αφού είναι απίθανο να έχει πάρει τις ίδιες μετρήσεις, και ως εκ τούτου είναι ικανό να τροφοδοτήσει ένα μηχανισμό κρυπτογράφησης σε ανώτερο επίπεδο που έχει τη βάση του στα χαρακτηριστικά του καναλιού, δηλαδή του φυσικού επιπέδου.

Σε συνέχεια λοιπόν των παραπάνω σκέψεων και προβληματισμών, δόθηκε έμφαση στον πειραματισμό στο εργαστήριο στη δημιουργία και δοκιμές για αποστολή-λήψη αρχείων με τη βοήθεια ενός MQAM πομπού και δέκτη και ενός OFDM πομπού και δέκτη, δεδομένου ότι όπως προαναφέρθηκε η εμπιστευτικότητα της ζεύξης ανατέθηκε σε ανώτερο επίπεδο, βασισμένη όμως σε μετρήσεις του φυσικού επιπέδου.

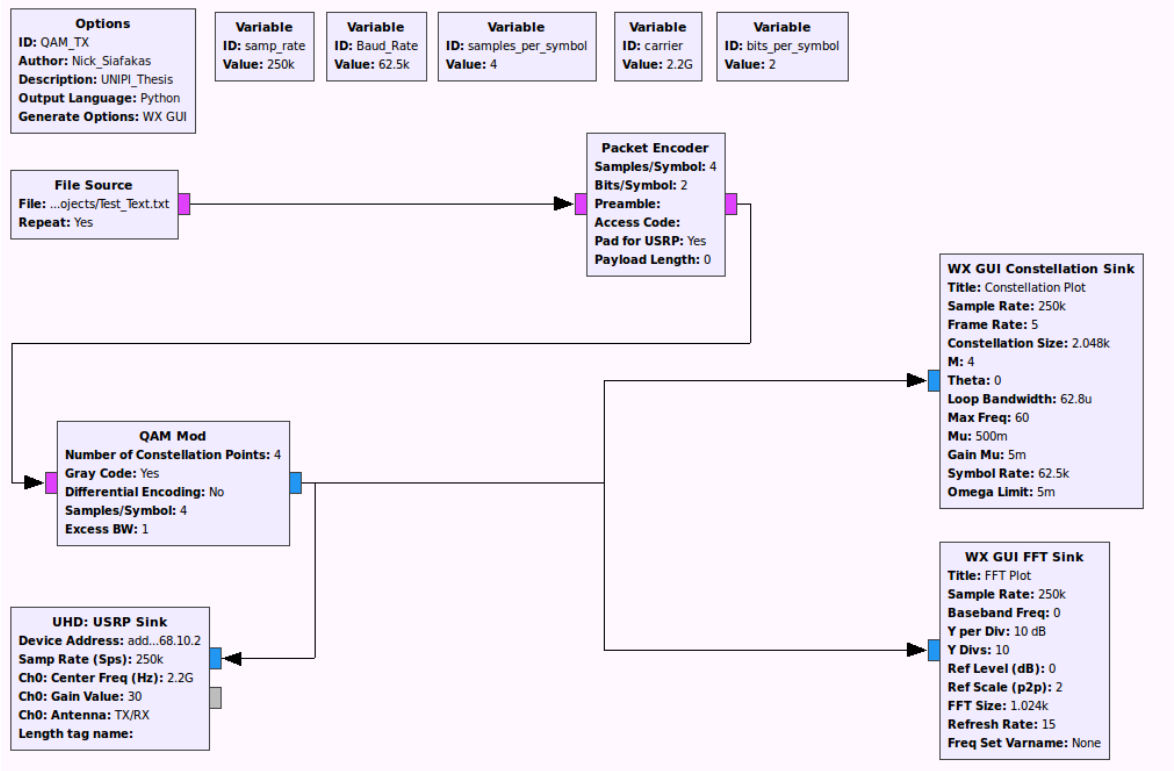
Εικόνα 7.1.1

Οι πληροφορίες για την υλοποίηση των παραπάνω πομπών και δεκτών, αντλήθηκαν τόσο από ελεύθερα project που υπάρχουν από το διαδίκτυο, όσο και από την ίδια την ιστοσελίδα του GNURadio.

7.2 Πομπός QAM

Ο πομπός QAM χρησιμοποιήθηκε με επιτυχία για M ίσο με 4 και 16, πλην όμως το GRC δεν υποστηρίζει μεγαλύτερα σχήματα στην παρούσα κατάσταση και επομένως για ανάπτυξη αυτών πρέπει να προγραμματισθούν εξαρχής από μηδενική βάση τα αντίστοιχα block που απαιτούνται και να εισαχθούν στη βιβλιοθήκη του GRC προς χρήση.

Οι κυριότερες παράμετροι του συστήματος, όπως η συχνότητα δειγματοληψίας, τα bits ανά σύμβολο, κ.λπ. έχουν δηλωθεί ως καθολικές μεταβλητές με σκοπό την εύκολη αλλαγή και προσαρμογή τους, χωρίς να επηρεάζεται η λειτουργικότητα των υπόλοιπων block του διαγράμματος.

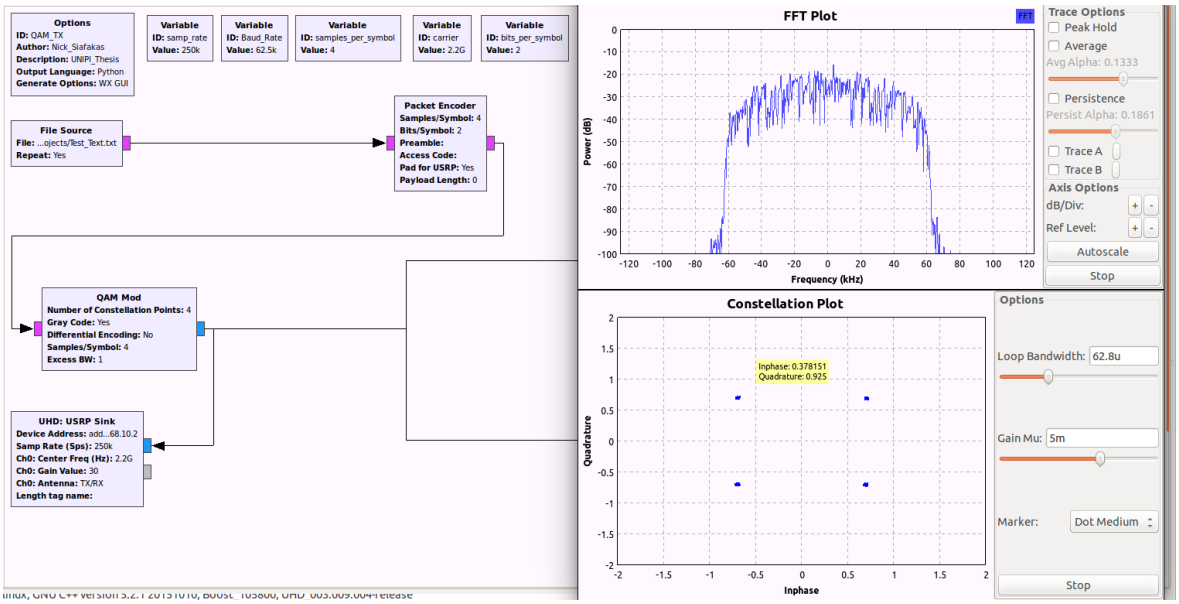


Εικόνα 7.2.1

Το προς αποστολή σήμα αποτελεί ένα αρχείο αποθηκευμένο σε ένα directory του host PC, το οποίο δηλώνουμε στο block File Source, δηλώνοντας ταυτόχρονα αν θέλουμε να επαναλαμβάνεται συνεχώς η αποστολή του αρχείου ή όχι.

Τα εξερχόμενα δεδομένα, ως συρμός από bit, αντιστοιχίζονται από το block «Packet Encoder» σε τιμές -1 και 1 αντί των 0 και 1. Ακολουθεί η διαμόρφωση QAM με το block «QAM Mod». Ο υπάρχων διαμορφωτής QAM της βιβλιοθήκης του GRC παρέχει εκτός από δυνατότητα για κωδικοποίηση Gray της επιπλέον διαφορικής κωδικοποίησης. Στην υλοποίηση της 16QAM, όπως είναι το παραπάνω παράδειγμα, αφού το M είναι ίσο με 16, τότε στον κωδικοποιητή πακέτων η αντιστοίχιση είναι 4 bit/σύμβολο.

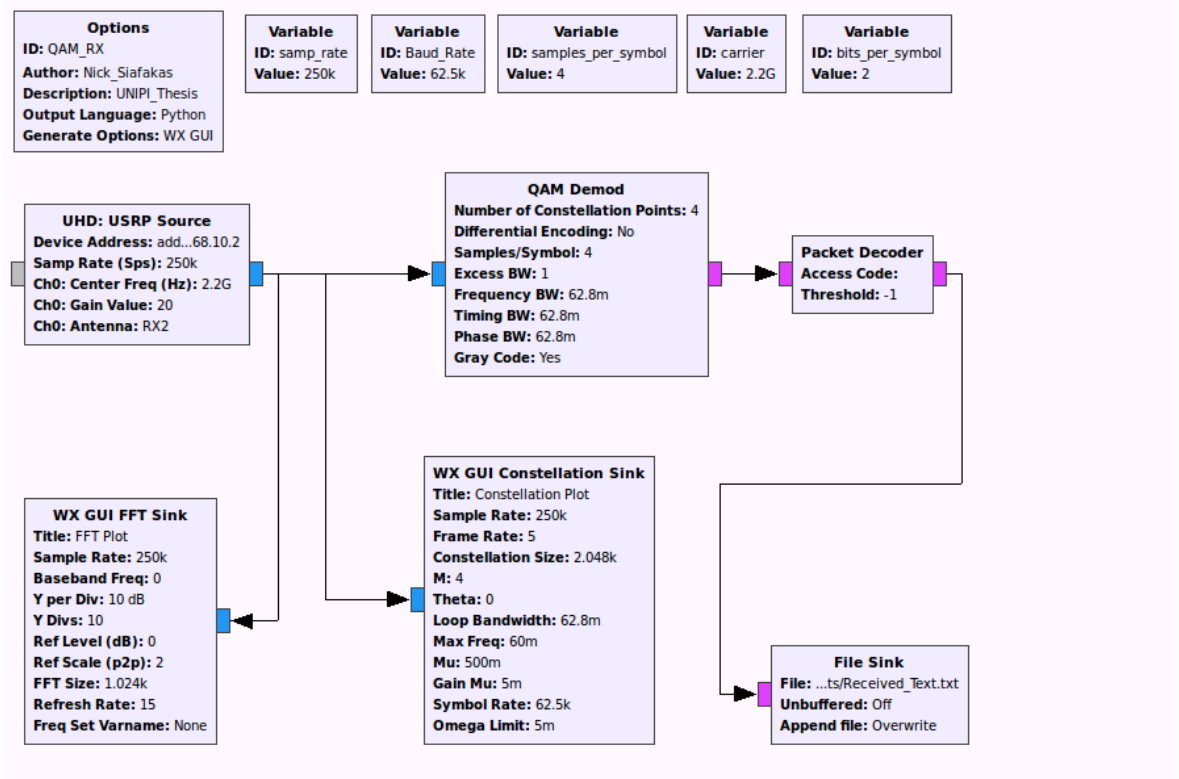
Τέλος, ακολουθεί η εκπομπή των διαμορφωμένων συμβόλων, μέσω του block του USRP του host PC.



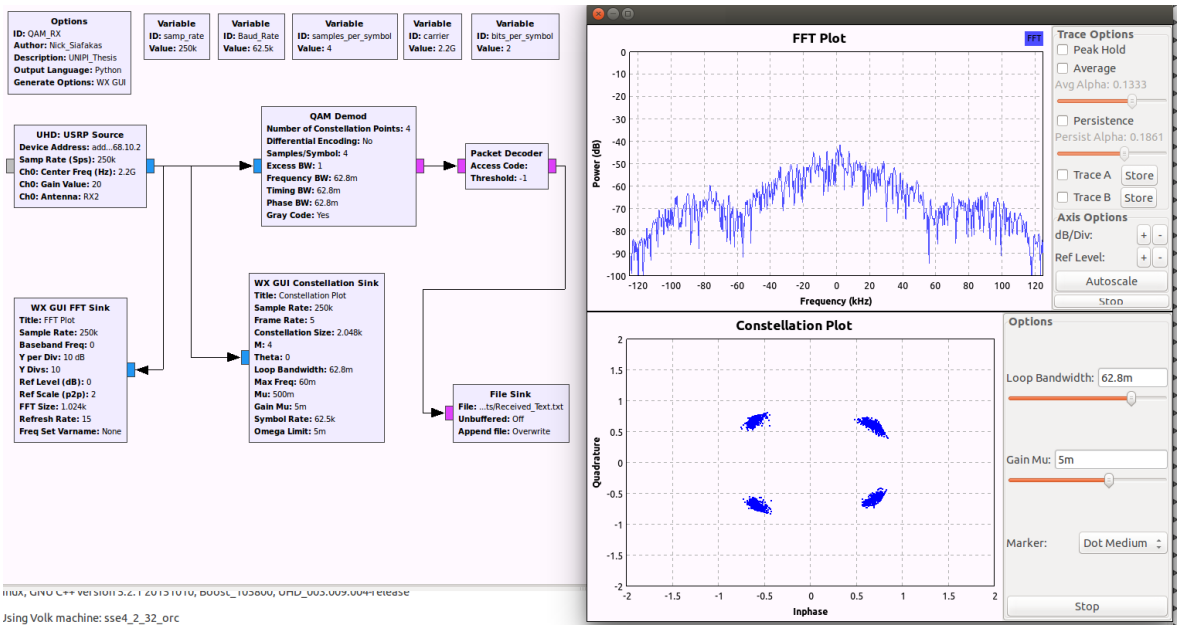
Εικόνα 7.2.2

7.3 Δέκτης QAM

Κατ' αντιστοιχία, με την ανάστροφη διαδικασία, ο δέκτης της 16QAM του παραδείγματος:



Εικόνα 7.3.1



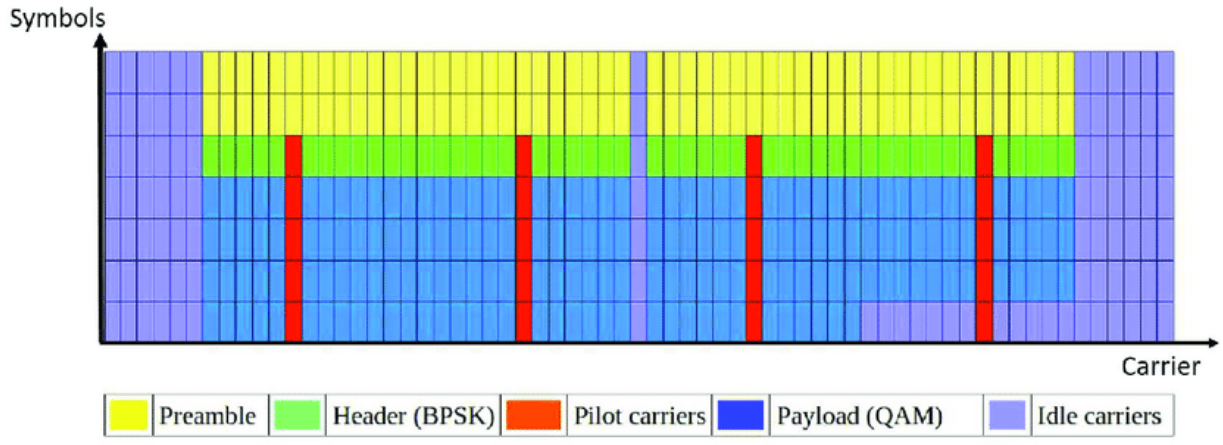
Εικόνα 7.3.2

Στο δέκτη υλοποιείται ακριβώς η αντίστροφη διαδικασία από αυτή του πομπού. Με τη διάταξη της εικόνας 7.1.1 επετεύχθη η αποστολή αρχείου εικόνας από το host PC Bob σε αυτό της Alice και αποθήκευσή του σε αυτό.

Αξίζει να σημειωθεί ότι από τα σχήματα διαμόρφωσης που δοκιμάστηκαν (QPSK, GFSK, QAM), το σχήμα αυτό είναι και το καλύτερο από άποψη φασματικής απόδοσης καθώς έχουμε το μεγαλύτερο βαθμό διαμόρφωσης, συνεπώς αντιστοίχιση περισσότερων ψηφίων ανά σύμβολο και άρα μεγαλύτερο ρυθμό μετάδοσης δεδομένων ανά Hz φάσματος.

7.4 Πομπός OFDM

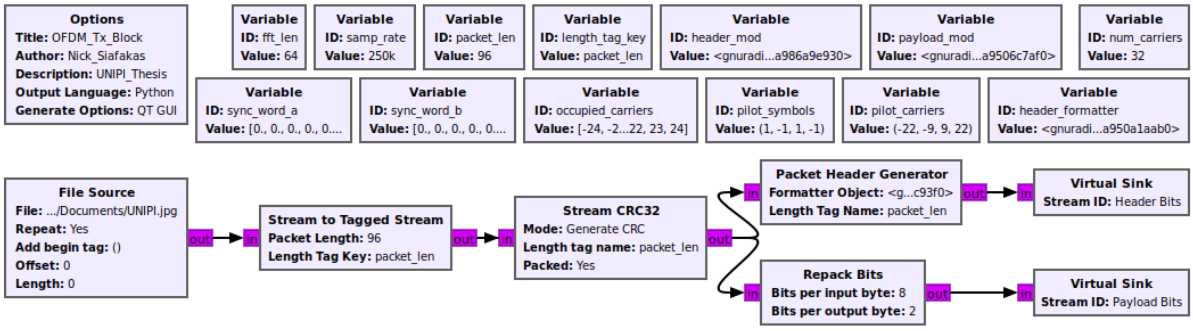
Ο πομπός OFDM υλοποιήθηκε, καθώς κατά βάση αποτέλεσε το κεντρικό αντικείμενο σπουδής στα περισσότερα μαθήματα του μεταπτυχιακού, ως το σχήμα που χρησιμοποιείται σήμερα κατά κόρον στις κινητές επικοινωνίες.



Εικόνα 7.4.1

./.

Το block διάγραμμα του πομπού, κατά τμήματα a, b και c για λόγους διευκόλυνσης του αναγνώστη, όπως αυτό υλοποιήθηκε στο GNURadio, είναι το παρακάτω:



Εικόνα 7.4.2

Οι κυριότερες παράμετροι του συστήματος, όπως το μήκος του FFT, η συχνότητα δειγματοληψίας, το μέγεθος του πακέτου δεδομένων, οι λέξεις συγχρονισμού, τα φέροντα τα οποία θα χρησιμοποιηθούν, κ.λπ. έχουν δηλωθεί ως μεταβλητές με σκοπό την εύκολη αλλαγή και προσαρμογή τους, χωρίς να επηρεάζεται η λειτουργικότητα των υπόλοιπων block του διαγράμματος.

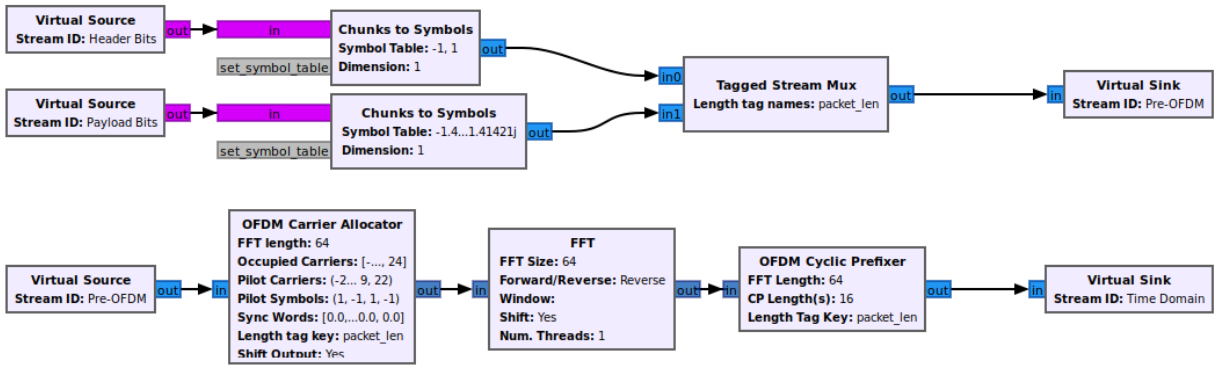
Η πηγή δεδομένων εδώ είναι μια εικόνα, αποθηκευμένη τοπικά στο host pc, η οποία επαναλαμβάνεται. Στη συνέχεια περνιέται στο block «stream to tagged stream», το οποίο προσθέτει tags/πληροφορίες για τα block που ακολουθούν. Το block που ακολουθεί είναι αυτό που αναλαμβάνει τον κυκλικό έλεγχο πλεονασμού (CRC Cyclic Redundancy Check), δηλαδή τον έλεγχο για σφάλματα. Τέλος, στον πρώτο αυτό γύρο επεξεργασίας, το block «Packet Header Generator» θα κατασκευάσει το header για τα πακέτα δεδομένων και τα δύο stream θα αποθηκευτούν προσωρινά σε δύο sinks. Το block «Repack bits» προετοιμάζει τα δεδομένα για διαμόρφωση (8 bit για 1 bit για BPSK και 8 bit για 2 bits για QPSK)

Τα δεδομένα, αφού ξαναδιαβαστούν, κωδικοποιούνται με τα block «Chunks to symbols» η μεν ροή του header σε BPSK κωδικοποίηση, ενώ η ροή bits του payload σε QPSK σύμβολα και οι δύο νέες ροές οδηγούνται στη MUX, από όπου η μία έξοδος που προκύπτει, ξανα-αποθηκεύει τα δεδομένα σε μία sink. Η MUX παράγει την έξοδο σειριακά, επιλέγοντας κάθε φορά διαδοχικά πακέτα από τις ροές εισόδου.

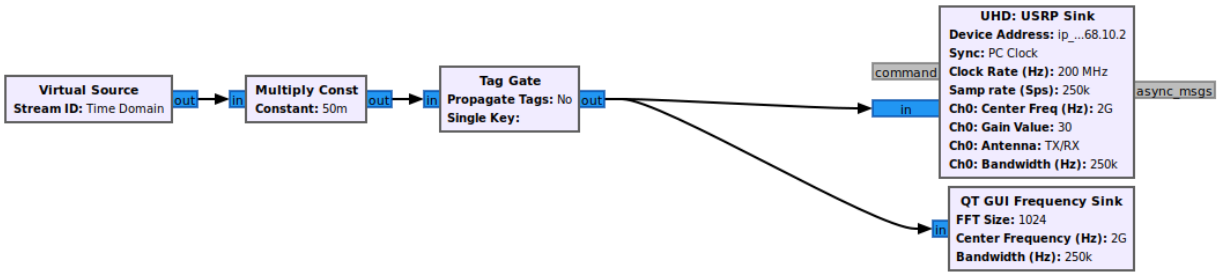
Στη συνέχεια, αφού ξαναδιαβαστούν τα δεδομένα, ο OFDM carrier allocator τοποθετεί τα σήματα-πιλότους και τα χρήσιμα δεδομένα στις καθορισμένες θέσεις των φερόντων του IFFT. Ακολουθεί η μετατροπή στο πεδίο του χρόνου και στη συνέχεια μπροστά από κάθε OFDM σύμβολο προστίθεται το κυκλικό πρόθεμα (CP-Cyclic Prefix).

Τέλος, τα σύμβολα είναι έτοιμα προς εκπομπή, αφού οδηγηθούν στο διασυνδεδεμένο USRP, στο οποίο έχουν ρυθμιστεί παράμετροι όπως sampling rate, bandwidth, carrier frequency και channel gain.

Εδώ έχουν επιλεγεί 48 carriers, τέσσερις πιλότοι στις θέσεις -22, -9, 9 και 22 (εικόνα 7.2.1), πιλότοι σύμβολα (1,-1,1,-1) και λέξη συγχρονισμού με μέγεθος όσο το fft (64 float αριθμοί).



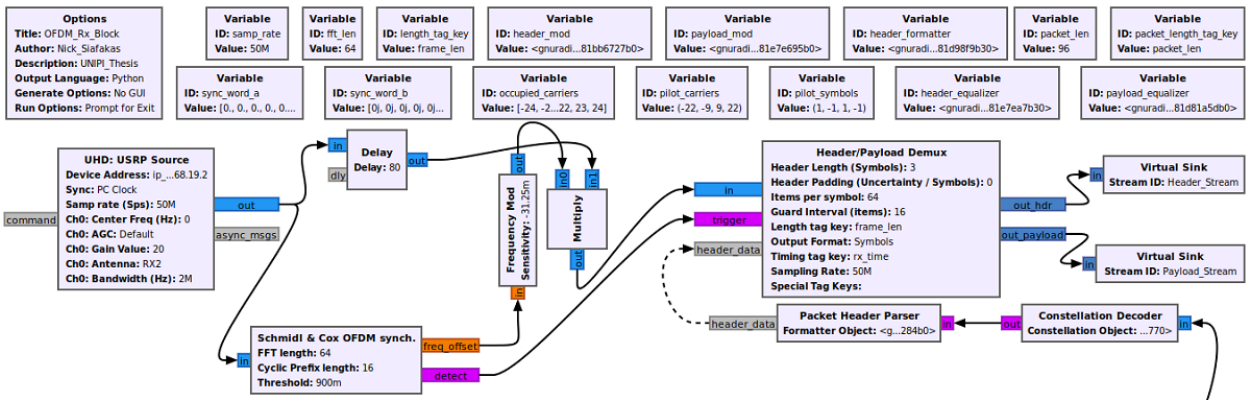
Εικόνα 7.4.3



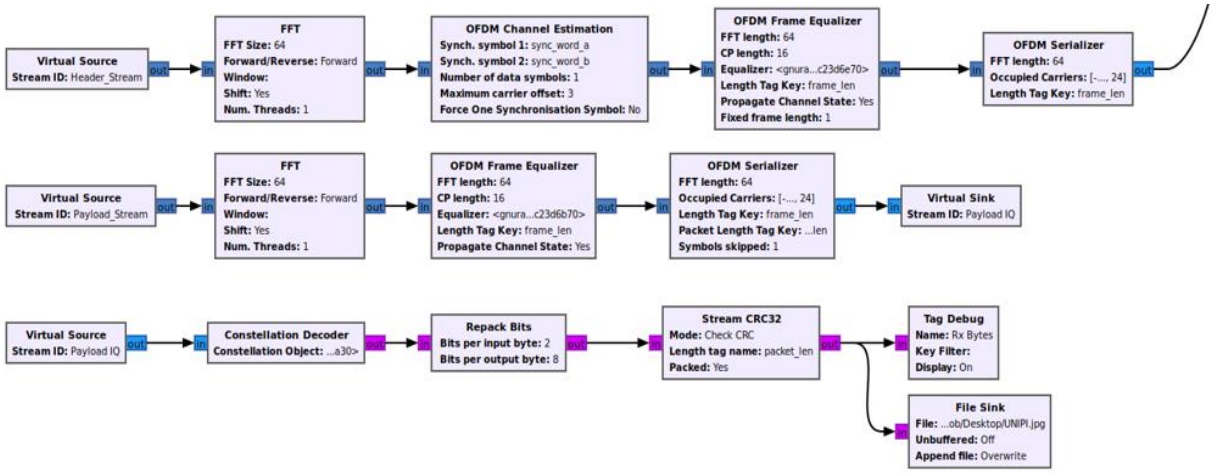
Εικόνα 7.4.4

7.5 Δέκτης OFDM

Το block διάγραμμα του δέκτη, κατά τμήματα a και b, για λόγους διευκόλυνσης του αναγνώστη, όπως αυτό υλοποιήθηκε στο GNURadio, είναι το παρακάτω:



Εικόνα 7.5.1



Εικόνα 7.5.2

Κατά την αντίστροφη διαδικασία το σήμα προερχόμενο από την εκπομπή, οδηγείται στο USRP, όπου μετά τη δειγματοληψία, παράγεται έξοδος σε μιγαδική μορφή. Το block «Schmidl & Cox OFDM synchronization» χρησιμοποιείται για συγχρονισμό, με σκοπό να ανιχνευτεί η αρχή του πακέτου και να γίνει η διόρθωση του frequency offset με τα preambles (sync words).

Το block «Header/Payload Demux» από-πολυπλέκει το header από το payload. Παίρνει το εισερχόμενο σήμα και το κάνει drop μέχρι να λάβει ένα trigger. Το trigger αυτό το δίνει το προηγούμενο block «Schmidl & Cox OFDM synchronization» και είναι ένα σήμα μεγάλης ενέργειας σε σχέση με τον απλό θόρυβο, την αρχή του οποίου (πακέτου) εντοπίζει το υπόψη block. Μόλις γίνει το trigger, το δείγμα περνάει στην εξερχόμενη πόρτα «0».

Αφού το μήκος του header είναι πάντα γνωστό/ρυθμιζόμενο, εισάγεται το απαραίτητο μήκος και οδηγείται προς αποδιαμόρφωση στη μία εκ των δύο ροών. Μόλις αποδιαμορφωθεί το header, ανατροφοδοτεί την αποδιαμορφωμένη πληροφορία πίσω (όπως για παράδειγμα το μήκος του payload, έτσι ώστε να αποδιαμορφωθεί το payload στη δεύτερη ροή δεδομένων.

Παράλληλα, τα block της άλλης ροής (FFT, OFDM Channel Estimation, Frame Equalizer και Serializer) αναλαμβάνουν κατά σειρά τη μετατροπή από το πεδίο χρόνου στο πεδίο συχνότητας, την εκτίμηση του διαύλου, την εξομάλυνση της επίδρασης του καναλιού στα ληφθέντα σύμβολα και τέλος την αφαίρεση των σημάτων-πιλότων με σκοπό να εξαχθούν μόνο τα πραγματικά δεδομένα του συμβόλου.

Τέλος, ακολουθεί ο αποχαρακτηρισμός των συμβόλων σε bits πληροφορίας, ο έλεγχος CRC και η αποθήκευση της πληροφορίας στο host PC.

Με τη διάταξη της εικόνας 7.1.1 επετεύχθη η αποστολή αρχείου εικόνας από το host PC Bob σε αυτό της Alice και αποθήκευσή του σε αυτό.

8. ΔΙΑΠΙΣΤΩΣΕΙΣ – ΣΥΜΠΕΡΑΣΜΑΤΑ

Κάνοντας την παραπάνω ανάλυση και καταγράφοντας τα συμπεράσματα που προέκυψαν από αυτή την τριβή και ενασχόληση αφενός με την νέα τεχνολογία του Software Defined Radio και αφετέρου με την ασφάλεια επικοινωνιών των τηλεπικοινωνιακών συστημάτων, μπορούν να καταγραφούν τα παρακάτω συμπεράσματα:

α. Το θέμα της ασφάλειας είναι τόσο ευρύ και αγκαλιάζει κάθε πτυχή και στάδιο στη διακίνηση της πληροφορίας από τον πομπό μέχρι τον τελικό αποδέκτη. Ως εκ τούτου, η φυσική ασφάλεια δεν δύναται να εξασφαλίσει από μόνη της την ασφαλή μεταφορά της πληροφορίας από τον πομπό στο δέκτη, ακόμα και αν συνδυαστούν τεχνικές που αναφέρθηκαν προηγουμένως (για παράδειγμα beamforming και τροποποιημένο σχήμα Alamouti μαζί). Ιδανικά, σε κάθε επίπεδο λειτουργίας θα πρέπει να εφαρμόζονται ξεχωριστές τεχνικές ασφαλείας, έτσι ώστε συσσωρευτικά να δημιουργείται ένα ολοκληρωμένο σχέδιο ασφαλείας.

β. Η τεχνολογία του software defined radio αποτελεί το πολλά υποσχόμενο μέλλον στις ασύρματες επικοινωνίες, το οποίο διαρκώς κερδίζει έδαφος. Το μεγαλύτερο ίσως πλεονέκτημα του SDR, μιλώντας και σε επίπεδο έρευνας και ανάπτυξης, είναι ότι απαιτείται μόνο ένα αρχικό κόστος προμήθειας των πλατφορμών και τίποτε άλλο και δεν απαιτεί εργαστήρια με κοστοβόρους εξοπλισμούς ή πολύπλοκες κατασκευές σε υλικό. Ιδιαίτερα το GNURadio, το οποίο επιλέχθηκε εδώ να μελετηθεί στα πλαίσια που αυτό ήταν δυνατό, αποτελεί εργαλείο ανοικτού κώδικα, με σχετικά ικανοποιητικές δυνατότητες για την ανάπτυξη real-time εφαρμογών.

γ. Η ανάπτυξη τεχνικών ασφαλείας για το φυσικό επίπεδο με τη βοήθεια του Software Defined Radio είναι κάτι που μπορεί κάλλιστα να αξιοποιηθεί και να διερευνηθεί περαιτέρω, με τους παρακάτω πιθανούς τρόπους:

(1) Ομαδοποίηση των USRP για δημιουργία συστημάτων MIMO, εκπομπής ή/και λήψης, αξιοποιώντας έτσι τις τεχνικές ασφαλείας φυσικού επιπέδου χώρου, όπως το beamforming.

(2) Συγγραφή κώδικα για δημιουργία block στη βιβλιοθήκη του GNURadio, ο οποίος θα αξιοποιεί τεχνικές DHSS και θα έχει χρήση/εφαρμογή σε διάφορους πομποδέκτες που είναι δυνατό να κατασκευαστούν σε αυτό. Η τεχνική FHOP μπορεί κάλλιστα να τροφοδοτηθεί με κλειδί για τη λειτουργία αναπήδησης, όπως περιγράφεται στην επόμενη παράγραφο.

(3) Συγγραφή κώδικα για δημιουργία block στη βιβλιοθήκη του GNURadio, το οποίο θα καταγράφει χαρακτηριστικά του καναλιού και θα δημιουργεί ένα πίνακα N-bit. Στη συνέχεια, χρήση αυτού του πίνακα είτε για την υλοποίηση της τροποποιημένης τεχνικής Alamouti που αναλύθηκε σε προηγούμενο κεφάλαιο ή ως κλειδιού για την κρυπτογράφηση της πληροφορίας σε ανώτερο επίπεδο OSI από το φυσικό.

Κλείνοντας την παρούσα πτυχιακή, θα πρέπει να τονισθεί και να εμπεδωθεί από το σύνολο, όχι μόνο των εμπλεκομένων με την ασφάλεια επικοινωνιών αλλά

και απλών χρηστών που ανταλλάσσουν πληροφορίες που επιθυμούν να παραμείνουν απόρρητες ότι η ασφάλεια πάντα όπως αναφέρθηκε ξανά δρα συσσωρευτικά και χτίζεται σε όλα τα επίπεδα, πρέπει δε διαρκώς να ελέγχεται και να βελτιώνεται. Άλλωστε, ισχύει πάντα το ρητό:

«ΑΣΦΑΛΗΣ ΕΙΝΑΙ ΜΟΝΟ Η ΠΛΗΡΟΦΟΡΙΑ ΠΟΥ ΔΕΝ ΑΠΟΣΤΑΛΘΗΚΕ ΠΟΤΕ»

9. ΠΑΡΑΡΤΗΜΑΤΑ

ΠΙΝΑΚΑΣ ΣΥΝΤΜΗΣΕΩΝ

3GPP	3rd Generation Partnership Project
ACM	Adaptive Coding and Modulation
ADC	Analog-to-digital converter
API	Application Programming Interface
BS	Base Station
BSC	Base Station Controller
BSS	Base Station Subsystem (BTS + BSC)
BTS	Base Transceiver Station
CF	Center frequency
DAC	Digital-to-analog converter
DC	Direct current
DDC	Digital down converter
Downlink	Signal sent from BS to MS
DUC	Digital up converter
DUT	Device under test
FM	Frequency Modulation
FPGA	Field-programmable gate array
GbitE	Gigabit Ethernet
GNU	GNU's Not Unix
GRC	GNU Radio Companion
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
I/Q	Inphase & Quadrature
IF	Intermediate Frequency
IP	Internet Protocol
LO	Local Oscillator
LTE	Long Term Evolution
MS	Mobile station
NCO	Numerically-controlled oscillator
PBX	Private branch exchange
PCB	Printed Circuit Board
PPM	Parts per million
PLL	Phase-locked loop
PSK	Phase shift keying
PSTN	Public switched telepfone network
RF	Radio Frequency

Rx	Receive path
SDR	Software-Defined Radio
SMA	SubMiniature version A (coaxial RF connector)
STDOUT	Standard output (where a application writes ist output data to)
SWIG	Simplified Wrapper and Interface Generator
PSTN	Public switched telephone network
QAM	Quadrature amplitude modulation
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Subsriber Identity
TTL	Transistor-transistor logic
Tx	Transmit path
UDP	User Datagram Protocol
Uplink	Signal sent from MS to BS
USB	Universal Serial Bus
USRP	Universal Software Radio Peripheral
VCC	Common-collector voltage (IC power supply pin)
XML	Extensible Markup Language