ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΙΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΔΙΚΤΥΑ Η/Υ ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ, ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια Φυσικού Επιπέδου Για Ασύρματα Δίκτυα 5G

Physical Layer Security for 5G Wireless Networks

ΟΔΟΝΤΟΠΟΥΛΟΣ ΧΡΗΣΤΟΣ (Α.Μ. 25)

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

ΔΡ. ΕΥΣΤΑΘΙΟΥ ΔΗΜΗΤΡΙΟΣ

ΣΕΡΡΕΣ

ΦΕΒΡΟΥΑΡΙΟΣ 2023

Υπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της Διπλωματικής Εργασίας και πως κάθε βοήθεια που είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στη Διπλωματική Εργασία, με κατάλληλη αναφορά. Επίσης, έχω αναφέρει τις πηγές από τις οποίες έκανα χρήση δεδομένων, εικόνων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες και αναλαμβάνω πλήρως την ευθύνη για τη χρήση των πηγών. Τέλος, βεβαιώνω ότι αυτή η διπλωματική εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά για τις απαιτήσεις του Μεταπτυχιακού Προγράμματος στις Τηλεπικοινωνίες και Δίκτυα Η/Υ.

Οδοντόπουλος Χρήστος

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Περίληψη

Στις μέρες μας η μετάβαση από τη βιομηχανική κοινωνία στην κοινωνία της πληροφορίας πραγματοποιείται μέσα από τη ραγδαία εξέλιξη των νέων τεχνολογιών πληροφορίας και τηλεπικοινωνίας. Η προστασία των δεδομένων και η παροχή ποιοτικών υπηρεσιών αποτελούν βασικά χαρακτηριστικά που αναζητούνται από τους νόμιμους χρήστες στα σύγχρονα τηλεπικοινωνιακά δίκτυα, ώστε να προστατεύονται από τους κακόβουλους χρήστες (υποκλοπείς). Η εύκολη παρεμβολή και η εκπομπή σε όποιον χρήστη έχει πρόσβαση σε μέσο διάδοσης αποδεικνύουν το γεγονός ότι τα ασύρματα δίκτυα είναι ιδιαίτερα επιρρεπή σε θέματα ασφάλειας.

Η ασφάλεια της μετάδοσης της πληροφορίας βασίζεται στην κρυπτογράφηση, η οποία τροποποιεί το μεταδιδόμενο σήμα με ένα τρόπο όπου αν ο υποκλοπέας δεν γνωρίζει πως να το αποκωδικοποιήσει δεν θα τα καταφέρει, διότι η μέθοδος της κρυπτογράφησης βασίζεται στην χρήση ενός μυστικού κλειδιού που γνωρίζουν μόνο οι νόμιμοι χρήστες. Τα προβλήματα που προκύπτουν σε αυτή τη μέθοδο είναι για το πώς θα γίνει η ανταλλαγή του μυστικού κλειδιού με ασφαλή τρόπο. Επίσης, ένα ακόμα σημαντικό πρόβλημα είναι στην μεγάλη υπολογιστική πολυπλοκότητα για τους νόμιμους χρήστες που είναι κοστοβόρα και στο γεγονός ότι τα συστήματα είναι ευάλωτα στα είδη επιθέσεων ασύρματων καναλιών.

Στην εργασία αυτή αναπτύχθηκε μία μέθοδος ενίσχυσης της ασφαλούς μετάδοσης της πληροφορίας αξιοποιώντας τα χαρακτηριστικά της τεχνικής Ορθογώνιας Πολυπλεξίας Διαίρεσης Συχνότητας (Orthogonal Frequency Division Multiplexing, OFDM). Ένα σύμβολο OFDM περιλαμβάνει τους πιλοτικούς υποφορείς, που είναι απαραίτητοι για τη διαδικασία εκτίμησης του ασύρματου καναλιού με βάση την πληροφορία που μεταφέρουν οι πιλοτικοί υποφορείς, η οποία εκτελείται στο νόμιμο δέκτη. Προτείνεται οι θέσεις των πιλοτικών υποφορέων να αλλάζουν σε κάθε OFDM σύμβολο ακολουθώντας μία συγκεκριμένη κατανομή πιθανότητας που είναι γνωστή μόνο στο νόμιμο πομπό και δέκτη. Οπότε, ο υποκλοπέας εκτελεί «τυφλή» εκτίμηση του ασύρματου καναλιού που είναι λιγότερη αποτελεσματική σε σύγκριση με την εκτίμηση του ασύρματου καναλιού με την χρήση πιλοτικών υποφορέων.

Οι προσομοιώσεις εκτελέστηκαν με τη βοήθεια του προγραμματιστικού περιβάλλοντος MATLAB, με σκοπό την εξαγωγή αποτελεσμάτων για το νόμιμο δέκτη σε σχέση με τον τον

δέκτη του ωτακουστή. Στις προσομοιώσεις έγινε χρήση των διαμορφώσεων QPSK και 16-QAM για την άντληση των αποτελεσμάτων σε διάφορες ταχύτητες των κινητών συσκευών, ώστε να έχουμε καλύτερα συμπεράσματα για το πως επηρεάζεται ο ρυθμός εσφαλμένων bit (Bit Error Rate, BER) και το μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού (channel mean square error) στο νόμιμο δέκτη και τον δέκτη του ωτακουστή (υποκλοπέας) σε σχέση με την μεταβολή του σηματοθορυβικού λόγου. Οι δύο κινητές συσκευές κινούνται προς την ίδια κατεύθυνση με ταχύτητα 20 km/h ή 40 km/h ή 80 km/h.

Abstract

Nowadays, the transition from the industrial society to the information society takes place through the rapid development of new information and telecommunication technologies. Data security and the provision of quality services are key features sought by legitimate users in modern telecommunication networks, in order to protect them from malicious users (interceptors). Potential interception and broadcast to any user with access to a wireless medium indicates that wireless networks are particularly susceptible to security issues.

The security of the transmission of information is usually based on encryption, which modifies the transmitted signal in a way that if the eavesdropper does not know how to decrypt/decode it, he will not succeed, because the method of encryption is based on the use of a secret key that only the legitimate users know. A problem that arises in this method is how to exchange the secret key in a secure way. A second issue is the high computational complexity for encryption and decryption for legitimate users which is costly. A third issue is the fact that the legitimate users are vulnerable to various types of wireless channel attacks.

In this M.Sc. thesis, a method of secure information transmission is developed utilizing the characteristics of the OFDM technique (Orthogonal Frequency Division Multiplexing). An OFDM symbol includes the pilot subcarriers, which are necessary for the pilot channel estimation process performed at the legitimate receiver. For the presented work it is assumed that the subcarrier positions change in each OFDM symbol according to the probability distribution function (PDF) known only to the legitimate transmitter and receiver and thus the eavesdropper performs “blind” channel estimation which is less efficient compared to the pilot channel estimation.

The simulations for the legitimate receiver in relation to the eavesdropper are performed using the MATLAB. For the simulations QPSK (Quadrature Phase Shift Keying) and 16-QAM (Quadrature Amplitude Modulation) modulations schemes are used to extract the results at various speeds of the mobile devices (legitimate receiver and eavesdropper). The simulation results show how the Bit Error Rate (BER) and the root mean square error (rms) of the wireless channel estimation at the legitimate receiver and the eavesdropper change versus the signal-to-noise ratio (SNR). In the simulations it is considered that the two wireless devices travel to the same direction with velocities 20, 40 and 80 km/h.

Α. ΘΕΩΡΗΤΙΚΟ ΜΕΡΟΣ

1. Εισαγωγή

1.1 Το δικαίωμα της ελεύθερης επικοινωνίας

Στις μέρες μας η μετάβαση από τη βιομηχανική κοινωνία στην κοινωνία της πληροφορίας πραγματοποιείται μέσα από τη ραγδαία εξέλιξη των νέων τεχνολογιών πληροφορίας και τηλεπικοινωνίας [1]. Η ζωή του ανθρώπου είναι στενά συνδεδεμένη με την επικοινωνία, καθώς η ένταξη και η ύπαρξη του εντός της κοινωνίας προϋποθέτει την επικοινωνία με τους άλλους ανθρώπους. Η ανάπτυξη της προσωπικότητας, η συμμετοχή στην κοινωνική, οικονομική, πολιτική ζωή, προϋποθέτουν την ανεμπόδιστη ανταλλαγή ιδεών, πληροφοριών και μηνυμάτων [2].

Αυτός είναι ο λόγος που τα τελευταία χρόνια αυξάνονται οι νομοθεσίες που αφορούν την διασφάλιση της προστασίας των θεμελιώδων δικαιωμάτων και ιδίως της ιδιωτικής ζωής, καθώς οι κίνδυνοι που μπορούν να προκύψουν για τον πολίτη από την εξέλιξη της επικοινωνίας, επέβαλαν τα τελευταία χρόνια τη ρυθμιστική επέμβαση του νομοθέτη προς την κατεύθυνση της προστασίας των προσωπικών δεδομένων από την αθέμιτη επεξεργασία τους. Για την προστασία του ατόμου από παραβιάσεις της ιδιωτικότητας του δεν αρκεί μόνο η νομοθεσία, αλλά χρειάζεται τόσο η συνδρομή της ίδιας της τεχνολογίας μέσα από εφαρμογές που είναι φιλικές στην προστασία προσωπικών δεδομένων όσο και η ενημέρωση και ευαισθητοποίηση των πολιτών.

Η καταγραφή προσωπικών πληροφοριών και η καταγραφή ή παρακολούθηση των επικοινωνιών προσβάλλει την αξία του ανθρώπου και την ελευθερία του αλλά και δυσχεραίνει ουσιαστικά την απόλαυση και άλλων δικαιωμάτων καθώς και την άσκηση και άλλων συνταγματικά προστατευόμενων ελευθεριών [2]. Η σημαντικότητα του γεγονότος αυτού φαίνεται από συγκεκριμένα άρθρα του συντάγματος που προσδιορίζουν την ελεύθερη επικοινωνία ως απόλυτα απαραβίαστο και η προστασία της αποτελεί υποχρέωση της πολιτείας και μάλιστα με υψηλό βαθμό προτεραιότητας για τις κρατικές υπηρεσίες και τα όργανα της.

1.2 Ιστορία της ασφάλειας στις Τηλεπικοινωνίες

Οι πρώτες κρυπτογραφικές τεχνικές είναι βασισμένες σε μεθόδους, όπως αντιμετάθεση και υποκατάσταση [3]. Στην αντιμετάθεση, τα γράμματα του γραπτού μηνύματος αναδιατάσσονται με τρόπο που είναι γνωστός στον δέκτη, αλλά είναι δύσκολο για τον αποκρυπτογραφητή να το αποκρυπτογραφήσει. Αντίθετα, στην υποκατάσταση, κάθε γράμμα του μηνύματος αντικαθίσταται με ένα διαφορετικό, χρησιμοποιώντας έναν κανόνα που είναι γνωστός μόνο στον προοριζόμενο δέκτη [4].

Απαρχής της γέννησης της ανθρωπότητας γίνονται προσπάθειες για τη διατήρηση της μυστικότητας με διάφορες τεχνικές που βασίζονται στην αντιμετάθεση και στην υποκατάσταση. Η ετυμολογική ανάλυση της λέξης προέρχεται από κρυπτό+γραφή, που αποδίδει την έννοια της λέξης [5]. Η ιστορία της κρυπτογράφησης μπορεί να διαιρεθεί σε τρία στάδια, στο πρώτο στάδιο οι διαδικασίες κρυπτογράφησης αφορούσαν τον τρόπο της έντυπης απεικόνισης (μελάνι και χαρτί), στις οποίες γινόταν αντικατάσταση και αναδιάταξη των γραμμάτων της αλφαβήτου [6]. Ενδεικτικό παράδειγμα αποτελεί ο κρυπτογραφικός αλγόριθμος του Καίσαρα (Caesar shift cipler), όπου κάθε γράμμα του μηνύματος αντικαθίσταται με το γράμμα τρεις θέσεις πιο κάτω στο αλφάβητο και με αυτόν τρόπο αν ο εχθρός έκλεβε το μήνυμα δεν θα είχε την δυνατότητα να το διαβάσει εκτός αν κατάφερνε να καταλάβει το μετασχηματισμό που είχε γίνει στο μήνυμα [7]. Στο δεύτερο στάδιο αναφέρεται οι κρυπτογραφικές μηχανές που αναπτύχθηκαν κυρίως στον Β’ Παγκόσμιο Πόλεμο με χαρακτηριστικό παράδειγμα τη γερμανική μηχανή Enigma, η οποία είχε ένα πληκτρολόγιο ως συσκευή εισόδου και ένα εξώφυλλο ως συσκευή εξόδου. Η μηχανή αποτελείται από τρία μέρη: 1) Ένα πάνελ ελέγχου (plugboard, όπου γινόταν μια απλή υποκατάσταση στο μήνυμα εισόδου, με βάση τη διαμόρφωση της καλωδίωσης. 2) Τρεις περιπλέκτες (scramblers), οι οποίοι ήταν περιστρεφόμενοι δίσκοι, ο καθένας από τους οποίους έκανε διαφορετική υποκατάσταση στις εισόδους του, με βάση την καλωδίωση τους. 3) Έναν ανακλαστήρα, που έστελνε στην έξοδο τους περιπλέκτες μέσω μιας διαφορετικής διαδρομής. Η μηχανή Enigma κάθε φορά που πιεζόταν ένα κλειδί, οι περιπλέκτες θα περιστρέφονταν, πράγμα που σημαίνει ότι το αλφάβητο υποκατάστασης θα άλλαζε με κάθε επανάληψη της διαδικασίας κρυπτογράφησης και έτσι ήταν πολύ δύσκολο να σπάσει η κρυπτογράφηση, μέχρι που το 1932 ο Πολωνός μαθηματικός Marian Rejewski κατάφερε να αναστρέψει την μηχανή Enigma. Ωστόσο, κατά τη διάρκεια του Β’ Παγκόσμιο Πόλεμο βελτιώθηκε ακόμα περισσότερο ο σχεδιασμός της και έγινε πολύ πιο δύσκολο να σπάσει. Τρίτο και τελευταίο στάδιο θεωρείται το σύγχρονο κρυπτογραφικό σύστημα με

αλληλεπίδραση των μαθηματικών που προσέφεραν στον σχεδιασμό και των υπολογιστών που επέτρεψαν τη χρήση πιο περίπλοκων αλγορίθμων κρυπτογράφησης.

Κατά τη διάρκεια των χρόνων η κρυπτογράφηση από τέχνη εξελίχθηκε σε επιστήμη με κύριο στόχο την ασφάλεια των πληροφοριακών και επικοινωνιακών συστημάτων, για αυτό και η μελέτη της σύγχρονης κρυπτογραφίας άπτεται των μαθηματικών και της υπολογιστικής θεωρίας-πολυπλοκότητας [8].

Για να ενισχυθεί η ασφάλεια στις τηλεπικοινωνίες, πέρα από τη χρήση κρυπτογραφικών τεχνικών, στο φυσικό επίπεδο χρησιμοποιούνται και άλλες τεχνικές, οι οποίες μπορούν να εκμεταλλευτούν τα χαρακτηριστικά του καναλιού, όπως η διάδοση πολλαπλών διαδρομών, χωρίς να αυξάνεται πολύ η πολυπλοκότητα, σε σύγκριση με την ασφάλεια ανώτερου επιπέδου. Επίσης, μπορεί να χρησιμοποιηθεί σε συνδυασμό με συστήματα ασφαλείας ανώτερου επιπέδου, όπως έλεγχος ταυτότητας, κρυπτογράφηση, έλεγχος αποδοχής κ.λπ., παρέχοντας ισχυρότερη ασφάλεια. Στα πλαίσια της διπλωματικής εργασίας θα ασχοληθούμε με μια τεχνική ασφάλειας που βασίζεται στην ιδιομορφία ενός OFDM σήματος. Η μέθοδος αυτή, χρησιμοποιεί την τυχαιοποίηση των θέσεων των πιλοτικών υποφορέων καθώς και την πληροφορία που μεταφέρουν ώστε να ενισχύσουν την ασφάλεια των μεταδιδόμενων δεδομένων.

Το κύριο πλεονέκτημα της ασφάλειας φυσικού επιπέδου, σε σύγκριση με τις κρυπτογραφικές τεχνικές, είναι ότι μπορεί να εκμεταλλευτεί τις ικανότητες του συστήματος, κυρίως τα χαρακτηριστικά του καναλιού, όπως η διάδοση πολλαπλών διαδρομών, χωρίς να αυξάνει πολύ την πολυπλοκότητα, σε σύγκριση με την ασφάλεια ανώτερου επιπέδου. Επίσης, μπορεί να χρησιμοποιηθεί σε συνδυασμό με συστήματα ασφαλείας ανώτερου επιπέδου, όπως έλεγχος ταυτότητας, κρυπτογράφηση, έλεγχος αποδοχής, παρέχοντας ακόμη και ισχυρότερη ασφάλεια [9]. Γίνονται πολλές ερευνητικές προσπάθειες ασφάλειας φυσικού επιπέδου που βασίζονται σε τεχνολογίες κωδικοποίησης, προκωδικοποίησης, επεξεργασίας σήματος και εκτίμησης καναλιών για την αντιμετώπιση προκλήσεων που σχετίζονται με την ασφάλεια, όπως φαινόμενα εξασθενισμού, πληροφορίες κατάστασης μερικής/ατελούς καναλιού (CSI), σύνθετα κανάλια δημιουργία κλειδιού PHY , και επιθέσεις πλαστοπροσωπίας ελέγχου ταυτότητας [10], καθώς επίσης προσεγγίσεις για τη μυστικότητα που βασίζονται στο σχεδιασμό κωδικοποίησης καναλιών [11]. Η μέθοδος πολλαπλής πρόσβασης για την εξασφάλιση της ορθογώνιας πολυπλεξίας διαίρεσης συχνότητας (OFDM) σε ασύρματα χρονικά μεταβαλλόμενα κανάλια, χρησιμοποιεί

αντίστροφη πιλοτική εφαρμογή για την εφαρμογή διαμόρφωσης υπέρθεσης με κοινή αποκωδικοποίηση στον δέκτη [12]. Η ασφάλεια φυσικού επιπέδου σε επικοινωνίες πολλαπλών εισόδων-πολλαπλών εξόδων (MISO), η διαμόρφωση δέσμης και η μετάδοση τεχνητού θορύβου επιλέγονται για την αύξηση της ασφάλειας των επικοινωνιών. Ο στόχος είναι μια στρατηγική βελτιστοποίησης που ορίζει έξυπνα την ισχύ μετάδοσης και το μέγεθος της «προστατευόμενης ζώνης» για να επιτύχει πιθανώς τη μυστικότητα σε ένα καθορισμένο ποσοστό απορρήτου στόχου [13]. Η τεχνική που χρησιμοποιείται για την εξασφάλιση της μετάδοσης κατερχόμενης ζεύξης σε ένα σύστημα πολλαπλών εισόδων και πολλαπλών εξόδων (MIMO), είναι η γραμμική προκωδικοποίηση δεδομένων και τεχνητό θόρυβο για να ενισχύσουν το απόρρητο, καθώς θεωρούν ότι οι πληροφορίες κατάστασης καναλιού δεν είναι διαθέσιμες στον νόμιμο πομπό [14].

1.3 Ζητήματα απορρήτου και ιδιωτικότητας στο τομέα των ηλεκτρονικών επικοινωνιών στη σύγχρονη εποχή

Η συνεχής πρόοδος της τεχνολογίας, κυρίως στο τομέα των ηλεκτρονικών επικοινωνιών και η δυνατότητα αντλήσης πληροφοριών από την επεξεργασία των δεδομένων που προκύπτουν από τη χρήση ηλεκτρονικών δικτύων και επικοινωνιών, θέτει σε κίνδυνο τον ιδιωτικό βίο του ατόμου. Αυτοί οι κίνδυνοι υφίστανται και είναι υπαρκτοί τόσο για την ιδιωτικότητα των χρηστών τηλεπικοινωνιακών δικτύων, όσο και χρηστών του διαδικτύου (κυβερνοχώρου).

Η προστασία του απορρήτου αποσκοπεί στη διασφάλιση της ελεύθερης προσωπικής επικοινωνίας, αλλά εγγυάται και το δικαίωμα των ατόμων στην ελεύθερη επικοινωνία με τους άλλους, ως προϋπόθεση αυτόνομων εκδηλώσεων, αποφάσεων και δράσεων και προϋποθέτει δύο τουλάχιστον πρόσωπα, τον αποστολέα και τον παραλήπτη του μηνύματος. Για την προστασία του απορρήτου των επικοινωνιών, η Πολιτεία έχει αναλάβει και υλοποιήσει μια σειρά από σχετικές πρωτοβουλίες για την ενίσχυση του επιπέδου προστασίας του εν λόγω δικαιώματος και τη θεσμική του θωράκιση στο ίδιο το Σύνταγμα. Επιπροσθέτως, ιδρύθηκε στην Ελληνική Αστυνομία, ειδική Υπηρεσία για την πρόληψη και καταστολή των εγκλημάτων παραβίασης του απορρήτου των ηλεκτρονικών επικοινωνιών, η οποία συνεργάζεται με την Α.Δ.Α.Ε. και τελεί υπό την εποπτεία του αρμόδιου Εισαγγελέα [15].

Τα προσωπικά δεδομένα κατηγοριοποιούνται σύμφωνα με τη χρήση τους. Είναι κοινή τακτική η διάκριση ανάμεσα στα δεδομένα που συλλέγονται από έναν συγκεκριμένο φορέα προκειμένου να χρησιμοποιηθούν για μια τρέχουσα - προσωρινή διαδικτυακή εργασία και σε αυτά που τα οποία αποθηκεύονται για χρήση και ανάλυση και/ή πωλούνται σε τρίτα μέρη. Στη δεύτερη κατηγορία, τα είδη των εμπλεκόμενων προσωπικών δεδομένων δύναται να ταξινομηθούν βάση της φύσης τους σε δύο μεγάλες κατηγορίες: Από τη μία πλευρά, στις πληροφορίες που δεν αναμένεται να αλλάξουν δραματικά κατά την πάροδο του χρόνου, οι οποίες αναφέρονται ως στατικές προσωπικές πληροφορίες (static private information). Τέτοιες πληροφορίες αφορούν το οικονομικό ιστορικό, το ιατρικό ιστορικό, τα προσωπικά πιστεύω και η διασύνδεση με ομάδες ανθρώπων, καθώς και τα προσωπικά αρχεία. Από την άλλη πλευρά περιλαμβάνονται οι πληροφορίες οι οποίες αλλάζουν δραματικά με την πάροδο του χρόνου, παρόλα αυτά όμως δύναται να συλλεχθούν και να αναλυθούν κατά τρόπο που να μπορεί να δημιουργηθεί ένα καλά ενημερωμένο προφίλ του ατόμου. Οι πληροφορίες αυτές αναφέρονται ως δυναμικές προσωπικές πληροφορίες, όπως το ιστορικό δραστηριότητας (στο διαδίκτυο) και το ιστορικό περιεχομένου [2].

2. Ασφάλεια Φυσικού Επιπέδου στις Ασύρματες Επικοινωνίες

2.1 Εισαγωγή

Η αλματώδης ανάπτυξη της ενσύρματης δικτύωσης προσέφερε ποικίλες πρωτοποριακές λύσεις, όμως πολλές αδυναμίες και ανεπάρκειες σε αρκετές περιπτώσεις εφαρμογών εξακολουθούν να υφίστανται. Για το λόγο αυτό, φάνηκε από πολύ νωρίς ότι η ευελιξία που έδιναν οι ασύρματες τεχνολογίες για πειραματισμούς θα έδινε τροφή για καινοτόμες αναζητήσεις και εφαρμογές. Ταυτόχρονα, οι ραγδαίες τεχνολογικές εξελίξεις δημιούργησαν όλο και περισσότερες προοπτικές για αύξηση της παραγωγής διαφόρων συσκευών ευρείας χρήσης ενώ το κόστος τους μειώθηκε αισθητά, με αποτέλεσμα την τελευταία δεκαετία τα ασύρματα δίκτυα να κατακτούν όλο και περισσότερο την καθημερινότητα μας. Οι τεχνολογίες υπολογιστών και ασυρμάτων επικοινωνιών έχουν καταστεί ένα πολύ σημαντικό κομμάτι της ζωής των ανθρώπων τις τελευταίες δεκαετίες, καθώς τα ασύρματα δίκτυα έχουν πολλά πλεονεκτήματα σε σχέση με τα ενσύρματα δίκτυα.

2.2 Τα πλεονεκτήματα των ασύρματων επικοινωνιών

Οι λόγοι για τους οποίους προτιμάμε τη χρήση ασύρματων μέσων μετάδοσης είναι οι εξής:

1. Ευκολία, ευελιξία και απλότητα εγκατάστασης: Είναι πολύ εύκολη η εγκατάσταση των ασύρματων δικτύων, η οποία γίνεται χωρίς καλωδίωση.
2. Κόστος: Το κόστος συντήρησης για όλη τη διάρκεια ζωής του είναι πολύ μικρό.
3. Ταχύτητες μετάδοσης: Χάριν στις τεχνολογικές εξελίξεις οι ρυθμοί μετάδοσης των δεδομένων έχουν αυξηθεί. Οι ταχύτητες των ρυθμών μετάδοσης έχουν ξεπεράσει τα 100Mbps ενώ αναμένονται ακόμη μεγαλύτερες ταχύτητες στο μέλλον.
4. Εμβέλεια: Ένα ασύρματο δίκτυο μπορεί να εκπέμπει σε εμβέλεια περίπου μερικών δεκάδων μέτρων σε περιβάλλον γραφείου (δηλαδή σε εσωτερικούς χώρους), και αυτό γιατί τα ραδιοκύματα συναντούν αντιστάσεις καθώς διαπερνούν τους τοίχους και τις οροφές, με αποτέλεσμα να υφίστανται σημαντική μείωση. Επίσης, όταν τα

ασύρματα δίκτυα εκπέμπουν σε ανοικτό χώρο, η εμέλεια τους μπορεί να φθάσει τα 30 χιλιόμετρα.

Παρά τα πολλά πλεονεκτήματα, η ασύρματη επικοινωνία έχει και σημαντικά προβλήματα ασφαλείας [16]. Η προστασία από κακόβουλους εισβολείς αποτελεί ένα χαρακτηριστικό που αναζητείται στα σύγχρονα τηλεπικοινωνιακά δίκτυα από τους νόμιμους χρήστες τους, τόσο για την προστασία των δεδομένων όσο και για την παροχή ποιοτικών υπηρεσιών. Τα ασύρματα δίκτυα είναι ιδιαίτερα επιρρεπή σε θέματα ασφάλειας λόγω δύο βασικών χαρακτηριστικών τους, την εκπομπή σε όποιον χρήστη έχει πρόσβαση στο μέσο διάδοσης (αέρας) και την εύκολη παρεμβολή από τους άλλους χρήστες [17].

2.3 Είδη Επιθέσεων σε Ασύρματα Δίκτυα

Η ασύρματη δικτύωση παίζει εξαιρετικά σημαντικό ρόλο σε πολιτικές και στρατιωτικές εφαρμογές. Ωστόσο, η ασφάλεια της μεταφοράς πληροφοριών μέσω ασύρματων δικτύων παραμένει ένα δύσκολο ζήτημα. Είναι σημαντικό να διασφαλιστεί ότι τα εμπιστευτικά δεδομένα είναι προσβάσιμα μόνο στους προβλεπόμενους χρήστες. Για την καλύτερη κατανόηση του προβλήματος της ασφάλειας στα ασύρματα δίκτυα, παρουσιάζεται μία σύντομη περιγραφή των κυριότερων επιθέσεων που πραγματοποιούνται. Αρχικά, οι κακόβουλες επιθέσεις χωρίζονται σε δύο βασικές κατηγορίες, τις παθητικές και τις ενεργές [18][19].

Ως παθητικές ορίζονται οι επιθέσεις που δε συμπεριλαμβάνουν συμμετοχή του επιτιθέμενου στο δίκτυο. Επίθεση τέτοιου τύπου αποτελεί η Λήψη Πληροφοριών (Snooping/Footprinting), η οποία σχετίζεται με την ανάκτηση απόρρητων προσωπικών δεδομένων από μη εξουσιοδοτημένους χρήστες και χρειάζεται μια ασφαλής μέθοδος κρυπτογράφησης ώστε να αντιμετωπιστεί μία τέτοιου είδους επίθεσης. Άρα ο στόχος μιας παθητικής επίθεσης είναι η υποκλοπή πληροφορίας από τα ασύρματα κανάλια.

Καταρχήν, στην παθητική επίθεση ο επιτιθέμενος μπορεί να διαβάσει όλες τις πληροφορίες που προέρχονται από τα σημεία πρόσβασης, άρα είναι σε θέση να γνωρίζει το όνομα δικτύου (ή SSID). Επίσης είναι πολύ πιθανό να έχει την δυνατότητα να προσδιορίσει τον κατασκευαστή κάθε σημείου πρόσβασης με την βοήθεια της διεύθυνσης MAC του. Μια άλλη μέθοδος που χρησιμοποιείται είναι η τεχνική της ανάλυσης κυκλοφορίας. Η ανάλυση κυκλοφορίας είναι η μελέτη των εξωτερικών στοιχείων των μηνυμάτων, παραδείγματος

χάριν, της συχνότητας επικοινωνίας και του μεγέθους. Ένα πολύ χρήσιμο εργαλείο που χρησιμοποιείται στην ανάλυση, παρακολούθηση και στον εντοπισμό και αντιμετώπιση προβλημάτων στα δίκτυα αλλά και στην εκπαίδευση είναι το Wireshark [20].

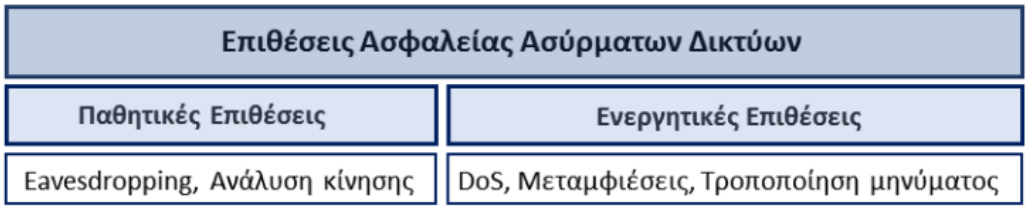
Αντίθετα, οι ενεργητικές επιθέσεις παρενοχλούν την εύρυθμη λειτουργία του ασύρματου δικτύου, στοχεύοντας συνήθως στην αλλοίωση των δεδομένων του και προϋποθέτουν ότι ο επιτιθέμενος αναλαμβάνει ενεργή συμμετοχή στο δίκτυο. Οι ενεργητικές επιθέσεις χωρίζονται, σύμφωνα με το σκοπό που έχουν οι επιτιθέμενοι, σε τρεις βασικές κατηγορίες [21]:

1. Επιθέσεις άρνησης υπηρεσίας (Denial of Service)
2. Μη εξουσιοδοτημένης πρόσβασης επιθέσεις (Unauthorized Access)
3. Επιθέσεις τροποποίησης μηνυμάτων (Man in the Middle Attack)

Οι επιθέσεις άρνησης υπηρεσίας είναι οι πιο διαδομένες επιθέσεις, οι οποίες έχουν την ικανότητα να αχρηστεύουν το δίκτυο. Η επίθεση πλημμύρας (Flood Attack) αποτελεί ένα είδος επίθεσης άρνησης υπηρεσίας, όπου ο επιτιθέμενος για να καταναλώσει όλη την επεξεργαστική ισχύ του δικτύου στέλνει μεγάλο αριθμό πακέτων στο δίκτυο.

Οι μη εξουσιοδοτημένης πρόσβασης επιθέσεις δεν στοχεύουν κάποιο συγκεκριμένο χρήστη, αλλά ολόκληρο το δίκτυο. Ο επιτιθέμενος μπορεί να αποκτήσει λίγα ή όλα τα δικαιώματα του δικτύου, ανάλογα την αρχιτεκτονική του δικτύου, καθώς επίσης ο επιτιθέμενος έχει την δυνατότητα να αντιγράψει το όνομα του δικτύου και να δημιουργήσει ένα άλλο με πιο δυνατό σήμα με την βοήθεια αυτής της τεχνικής. έτσι γίνεται η σύνδεση στο ψεύτικο δίκτυο από τους χρήστες και μεταδίδουν τα μηνύματά τους από αυτό.

Ο επιτιθέμενος στις επιθέσεις τροποποίησης μηνυμάτων κάνει την εμφάνιση του στον χρήστη ως το access point και στο access point ως ο χρήστης και βρίσκεται στην μέση της συνομιλίας. Ο επιτιθέμενος με τον τρόπο αυτό διαβάζει πρώτος τα μηνύματα και έχει την δυνατότητα μετατροπής τους. Δύο μηχανισμοί ασφαλείας που έχουν αναπτυχθεί για τέτοιου είδους επιθέσεις είναι το IPSec και το VPN. Στις επιθέσεις τροποποίησης μηνυμάτων ο επιτιθέμενος με έμμεσο τρόπο αποκτά τα δεδομένα.



Εικόνα 2.1: Είδη επιθέσεων σε ασύρματα δίκτυα

2.4 Απαιτήσεις Ασφαλείας σε Ασύρματα Δίκτυα

Οι απαιτήσεις που έχουν οι χρήστες για την ασφάλεια των ασύρματων δικτύων σχετικά με την ασφάλεια των δεδομένων τους σχετίζονται άμεσα με τα είδη επιθέσεων, και είναι οι παρακάτω:

1. Εμπιστευτικότητα (Confidentiality): Με τον όρο εμπιστευτικότητα αναφερόμαστε στον τρόπο με τον οποίο ευαίσθητα δεδομένα μπορούν να κινηθούν μέσα στο δίκτυο χωρίς να υπάρχει ο κίνδυνος αυτά να γνωστοποιούνται σε μη εξουσιοδοτημένους χρήστες [22]. Η ασφάλεια των δεδομένων είναι από τα κυριότερα κομμάτια της ασφάλειας των δικτύων, για αυτό το λόγο η διαφύλαξη των δεδομένων, δηλαδή η εμπιστευτικότητα επιδιώκετε πρώτιστα από τον μηχανισμό ασφαλείας σε κάθε δίκτυο [23].

2. Ακεραιότητα (Integrity): Με τον όρο ακεραιότητα αναφερόμαστε στην δυνατότητα του δικτύου να εγγυάται στους χρήστες του ότι τα δεδομένα που αποστέλλονται δεν έχουν αλλοιωθεί από κάποια επίθεση. Με αυτόν τον τρόπο κανένας μη εξουσιοδοτημένος χρήστης δεν θα μπορεί να έχει πρόσβαση στα δεδομένα έτσι ώστε να μπορέσει στην συνέχεια να προχωρήσει στην αλλοίωση τους, κατά την μετακίνηση τους μέσα στο δίκτυο [24][25]. Η ακεραιότητα ενός μηνύματος επηρεάζεται από την αλλοίωση του εσωτερικού των μηνυμάτων, την αποστολή του στον τελικό χρήστη και από την προσθήκη επιπλέον πληροφοριών στα δεδομένα, με αποτέλεσμα να προκληθεί ζημιά σε ολόκληρο το δίκτυο.

3. Αυθεντικοποίηση (Authentication): Με τον όρο αυθεντικοποίηση αναφερόμαστε στην επιβεβαίωση του δέκτη για την προέλευση των δεδομένων, δηλαδή από ποιον

αποστολέα έχουν σταλεί, καθώς υπάρχει μεγάλος φόβος ότι ένας μη εξουσιοδοτημένος χρήστης μπορεί με ευκολία να τροποποιήσει τα μηνύματα [26][27]. Για να επαληθευτεί κατά πόσο η ταυτότητα του αποστολέα είναι όντως αυτή που παρουσιάζεται στην περίπτωση της ασφάλειας των δικτύων γίνεται ένας έλεγχος, ώστε να εξακριβωθεί η ταυτότητα του και να εγγυάται στον παραλήπτη πως ο αποστολέας δεν είναι κάποιος εισβολέας.

4. Διαθεσιμότητα (Availability): Με τον όρο διαθεσιμότητα αναφερόμαστε στην εγγύηση στους χρήστες του δικτύου, ότι οι υπηρεσίες του θα προσφέρονται κανονικά ανά πάσα στιγμή, χωρίς αλλοίωση, όποια επίθεση και αν δεχτεί από κακόβουλους εισβολείς. Μια από τις κυριότερες επιθέσεις είναι η παρεμβολή (jamming), κατά την οποία ο κακόβουλος χρήστης εκπέμπει ένα ισχυρό σήμα που υπερκαλύπτει τα νόμιμα εκπεμπόμενα σήματα.

2.5 Εργαλεία Ασφάλειας Δικτύων

Οι επιθέσεις με την συνεχή ανάπτυξη του Διαδικτύου είναι όλο και περισσότερες, γεγονός που οδήγησε στην μελέτη διάφορων τεχνικών και μηχανισμών, με απώτερο σκοπό να αντιμετωπιστούν και να ελαττωθούν. Τα ευαίσθητα δεδομένα και πληροφορίες πρέπει να είναι προστατευμένα από οποιαδήποτε απειλή και να παραμένουν μυστικά προς τον έξω κόσμο, για αυτό το λόγο σε περίπτωση όπου μία από τις μεθόδους αποτύχει σε ένα σημείο στην προστασία του δικτύου, μία άλλη από τις υπόλοιπες μεθόδους θα μπορέσει να αντιμετωπίσει τους κινδύνους. Μερικά εργαλεία για την ασφάλεια και την προστασία του δικτύου είναι τα ακόλουθα:

1. Τείχος Προστασίας (Firewall): Είναι από τους πρώτους μηχανισμούς ο οποίος θα αντιμετωπίσει κάποια απειλή την οποία θα δεχτεί το δίκτυο και θα απαγορέψει να εισέλθουν σε αυτό όποια πακέτα θα θεωρηθούν κακόβουλα. Το τείχος προστασίας μπορεί να είναι υλοποιημένο μέσα στην υποδομή του δικτύου, είτε στο υλικό (hardware) είτε στο λογισμικό (software), περιορίζοντας την πρόσβαση σε μη εξουσιοδοτημένους χρήστες και επιβλέπει την ροή κίνησης των πακέτων απαγορεύοντας τους να εισέλθουν ή να εξέλθουν από το δίκτυο με βάση κάποιων περιορισμών τους οποίους καθορίζει το κάθε δίκτυο ξεχωριστά. Το βασικό μειονέκτημα του τείχους Προστασίας είναι ότι δεν μπορεί να σταθεί ασπίδα

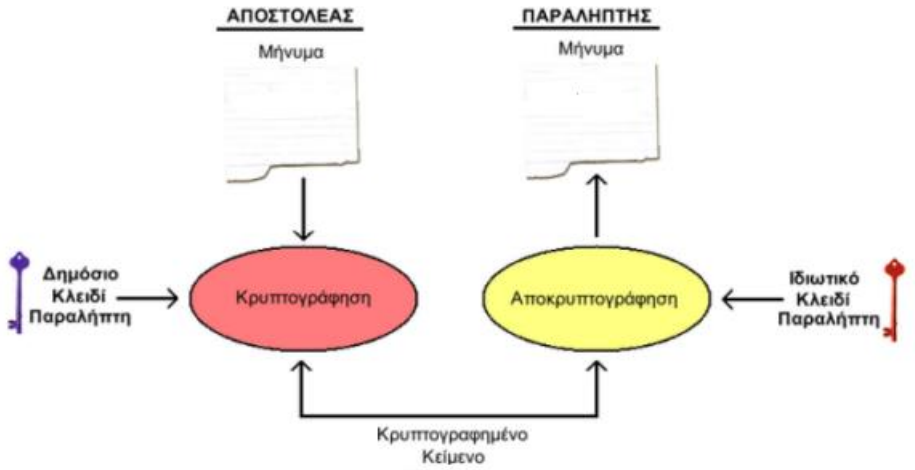
προστασίας σε κάποιον μη εξουσιοδοτημένου χρήστη που βρίσκεται ήδη μέσα στο δίκτυο [28][29].

2. Συστήματα Ανίχνευσης Εισβολής (Intrusion Detection Systems): Είναι συστήματα εντοπισμού και παρακολούθησης μη εξουσιοδοτημένων ατόμων σε ένα δίκτυο και προσπαθούν να αντιμετωπίσουν τυχών κινδύνους που θα δημιουργηθούν. Παρακολουθούν την ροή των πακέτων που ανταλλάσσονται μεταξύ των κόμβων του δικτύου και ελέγχουν αν υπάρχει κάποια κακόβουλη ενέργεια. Οι λόγοι εγκατάστασης ενός τέτοιου συστήματος είναι η ανίχνευση παραβιάσεων, η τεκμηρίωση υπαρκτών απειλών, πρόληψη προβλημάτων, ο έλεγχος ποιότητας για το σχεδιασμό ασφαλείας, καθώς και η θωράκιση παλαιών συστημάτων σε περίπτωση που κρίνεται αναγκαία η διατήρησή τους [30].

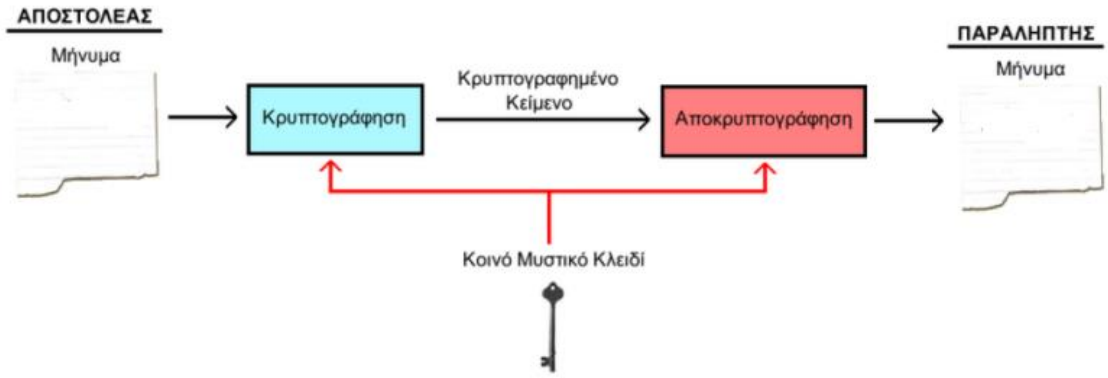
3. Κρυπτογραφικά Συστήματα (Cryptographic Systems): Η κρυπτογράφηση είναι μια μέθοδος που χρησιμοποιείται ευρέως για σκοπούς προστασίας των δεδομένων. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς ώστε 2 ή περισσότερα άκρα επικοινωνίας (π.χ. άνθρωποι, προγράμματα υπολογιστών κλπ.) να ανταλλάξουν μηνύματα, χωρίς κανένας τρίτος να είναι ικανός να διαβάζει την περιεχόμενη πληροφορία εκτός από τα δύο κύρια άκρα. Όταν το μήνυμα φτάσει στο δεύτερο άκρο τότε αυτό είναι υπεύθυνο να αποκρυπτογραφήσει το μήνυμα με την ύπαρξη του κατάλληλου κλειδιού. Το βασικότερο μειονέκτημα των Συστημάτων Κρυπτογραφίας είναι ότι αν έχουν το ίδιο κλειδί στην κατοχή τους δεν μπορεί να διαχωρίσει τον εξουσιοδοτημένο χρήστη από τον μη εξουσιοδοτημένο [31]. Η κρυπτογραφία έχει μακρά ιστορία, που ξεκινάει από την αρχαία Αίγυπτο πριν από 4000 χρόνια, ενώ η αναγωγή της σε επιστήμη γίνεται με την εξάπλωση των υπολογιστών και των δικτύων τους, πριν από περίπου τέσσερις δεκαετίες

Στη συνέχεια παρουσιάζονται οι εικόνες 2.2 και 2.3, όπου διακρίνονται δύο διαφορετικές προσεγγίσεις κρυπτογραφίας, η κρυπτογράφηση συμμετρικού κλειδιού και η κρυπτογράφηση δημόσιου κλειδιού. Η συνεχής αύξηση των δυνατοτήτων των συμβατικών ηλεκτρονικών υπολογιστών, η πρακτική υλοποίηση κβαντικών υπολογιστών και η έλλειψη

μαθηματικής απόδειξης για την κλάση πολυπλοκότητας που ανήκουν τα υπολογιστικά προβλήματα που χρησιμοποιούνται στην κρυπτογραφία αποτελούν παράγοντες που οδηγούν στην αναζήτηση εναλλακτικών τεχνικών για την επίλυση του προβλήματος της εχεμύθειας.



Εικόνα 2.2: Κρυπτογράφηση δημόσιου κλειδιού



Εικόνα 2.3: Κρυπτογράφηση συμμετρικού κλειδιού

Συμπερασματικά, πρέπει λοιπόν ένα δίκτυο, είτε μικρό είτε μεγάλο να προστατεύεται και να επιτρέπει την ασφαλή χρήση του από τους νόμιμους χρήστες. Με την αύξηση και την εξέλιξη των διάφορων τύπων απειλών, πρέπει σκληρότερα μέτρα να λαμβάνονται για την αντιμετώπιση τους. Κανένας εισβολέας δεν επιτρέπεται να έχει πρόσβαση σε πληροφορίες και δεδομένα που διακινούνται μέσα στο δίκτυο, και γενικότερα πρέπει να εξασφαλίζεται πως το δίκτυο δεν έχει καμιά αδυναμία την οποία να μπορεί κάποιος να εκμεταλλευτεί.

2.6 Αρχές ανάπτυξης αποτελεσματικού συστήματος ασφαλείας στο δίκτυο

Ο στόχος για την ασφάλεια των δικτύων, είναι η παροχή προστασίας στα δεδομένα που υπάρχουν σε αυτό, προκαλώντας όσο το δυνατόν λιγότερα προβλήματα στην προσβασιμότητα και παραγωγικότητα των χρηστών. Το δίκτυο διαμορφώνεται με τέτοιο τρόπο έτσι ώστε να ανταποκρίνεται σε συγκεκριμένους κανόνες και απαιτήσεις. Για να αναπτυχθεί ένα αποτελεσματικό σύστημα που θα προσφέρει προστασία στο δίκτυο, θα πρέπει πρώτα να μελετηθούν κάποιες από τις παρακάτω αρχές [32]:

- Ταυτοποίηση των στοιχείων που αποτελούν ένα δίκτυο: Η αποτελεσματική προστασία ενός δικτύου απαιτεί την κατανόηση των βασικών συστατικών που το αποτελούν, ώστε να δίνεται περισσότερη προσοχή σε θέματα ασφάλειας που έχουν άμεση ανάγκη.

- Καθορισμός του κόστους των μέτρων ασφαλείας: Τα μέτρα ασφαλείας τα οποία επιβάλλονται, απαιτούν υπολογιστικούς πόρους για κατανάλωση, γιατί έχουν την δυνατότητα να προκαλέσουν σημαντικά προβλήματα στους χρήστες και καθυστέρηση της εργασίας. Αν το κόστος που απαιτείται για την εφαρμογή αυτών των μέτρων για την ασφάλεια του δικτύου, ξεπερνά τα οφέλη του δικτύου, τότε αποφεύγονται αφού προσφέρουν κακές υπηρεσίες στο δίκτυο.

- Περιορισμός της εμβέλειας της πρόσβασης: Συγκεκριμένα μέρη μέσα σε ένα δίκτυο προστατεύονται περισσότερο, γιατί είναι πιο ευαίσθητα από κάποια άλλα.

- Περιορισμός της εμπιστευτικότητας: Πρέπει να μελετηθεί και να γνωστοποιηθεί ποιες συσκευές μπορεί ένα δίκτυο να εμπιστευθεί και σε ποιο λογισμικό μπορεί να στηριχθεί. Σε καμία περίπτωση δεν πρέπει να θεωρείται ως σωστή η υπόθεση πως δεν υπάρχουν καθόλου λάθη στο λογισμικό.

- Καθορισμός σημείων που αντιμετωπίζουν ρίσκο: Η έρευνα των σημείων τα οποία αντιμετωπίζουν υψηλό ρίσκο επίθεσης από τους εισβολείς αποτελεί μια πολύ σημαντική ενέργεια, για να γνωρίζουν πώς και πού θα ενεργήσουν πολύ από τους επιτιθέμενους και να αποτραπούν μεγάλα προβλήματα στο δίκτυο.

- Κατανόηση βασικών λειτουργιών του δικτύου: Γνωρίζοντας πώς εκτελεί τις βασικές του λειτουργίες το δίκτυο και πώς χρησιμοποιούνται οι συσκευές του δικτύου, είναι πιο εύκολο να εντοπιστούν και να λυθούν προβλήματα ασφάλειας.

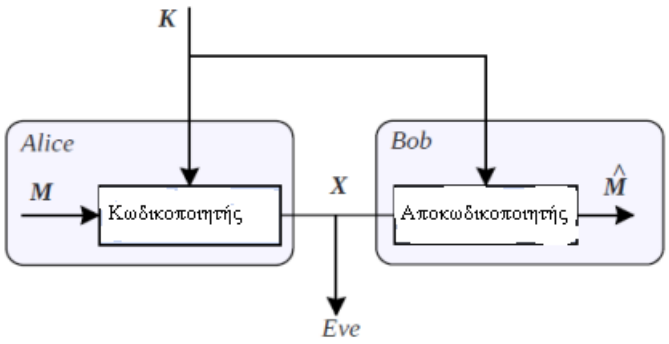
Συμπεραίνουμε πόσο σημαντική είναι η δημιουργία και η ολοκλήρωση ενός αποτελεσματικού συστήματος ασφάλειας στο δίκτυο, που θα προσφέρει στους χρήστες

ασφάλεια και εμπιστοσύνη απέναντι στους κακόβουλους χρήστες. Για να μπορέσει να πραγματοποιηθεί αυτό είναι πολύ σημαντική η γνώση των βασικών αρχών της ασφάλειας στο φυσικό επίπεδο, όπου θα αναλυθούν στο παρακάτω κεφάλαιο.

3. Βασικές Αρχές της Ασφάλειας Φυσικού Επιπέδου

3.1 Η Θεωρία του Shannon

Στην πρωτοποριακή εργασία του Shannon αναφέρθηκαν για πρώτη φορά οι βασικές έννοιες της θεωρητικής ασφάλειας πληροφοριών. Σύμφωνα με τον Shannon, η ασφαλή αποστολή ενός μηνύματος M στο νόμιμο δέκτη είναι ο βασικός σκοπός του πομπού και ο δέκτης στη συνέχεια παράγει μια εκτίμηση του μηνύματος $M^{\wedge}$. Ο ωτακουστής αποκτά όσο γίνεται λιγότερες πληροφορίες, όταν ο δέκτης καταφέρνει να παράγει την εκτίμηση του μηνύματος με τη μικρότερη δυνατή πιθανότητα σφάλματος εκτίμησης. Για να επιτευχθεί αυτό, πρέπει να υπάρχει ένα πλεονέκτημα του νόμιμου δέκτη σε σχέση με τον υποκλοπέα, το οποίο μοντελοποιήθηκε από τον Shannon ως μυστικό κλειδί K. Το κλειδί αυτό πρέπει να είναι διαθέσιμο στον πομπό και το νόμιμο δέκτη, αλλά όχι στον υποκλοπέα. Χρησιμοποιώντας το κλειδί K, ο πομπός κωδικοποιεί το M σε μια κωδική λέξη X, η οποία στη συνέχεια μεταδίδεται στον νόμιμο δέκτη και επίσης αποκτάται από τον υποκλοπέα. Στη συνέχεια, ο νόμιμος δέκτης είναι σε θέση να παράγει την εκτίμηση $M^{\wedge}$ χάρη στη γνώση του κλειδιού K [33]. Στην ασφάλεια της πληροφορίας ο πομπός αναφέρεται ως Alice, ο νόμιμος δέκτης ως Bob και ο ωτακουστής ως Eve.



Εικόνα 3.1: Το μοντέλο του καναλιού Shannon

Ο Shannon διατύπωσε την έννοια secrecy σύμφωνα με την άποψη της αβεβαιότητας του ωτακουστή. Αυτό δίνεται από την υπό συνθήκη εντροπία (conditional entropy) του μηνύματος γνωρίζοντας την κωδική λέξη (codeword) H(M|X), η οποία αναφέρεται ως αβεβαιότητα του ωτακουστή . Για να πετύχουμε τη τέλεια μυστικότητα πρέπει να ισχύει:

$$H(M|X) = H(M) \quad (3.1)$$

ή

$$I(M,X) = 0 \quad (3.2)$$

όπου I (M,X) είναι η αμοιβαία πληροφορία των M και X.

Η Eve δεν έχει τον τρόπο να διαβάσει το μήνυμα χωρίς να γνωρίζει το κλειδί γιατί το μήνυμα είναι ανεξάρτητο από την κωδική λέξη και η εντροπία δεν επηρεάζεται από την γνώση της κωδικής λέξης. Αυτό μπορεί να επιτευχθεί με τη λειτουργία XOR μεταξύ κάθε δυαδικού ψηφίου του μηνύματος M και ενός αντίστοιχου δυαδικού ψηφίου του κλειδιού K, το οποίο υποδηλώνεται ως:

$$X = M \oplus K \quad (3.3)$$

Έτσι καταλήγουμε στην κωδική λέξη X, όπου ακόμα και αν μπορέσει η Eve να διαβάσει και να αποκτήσει την κωδική λέξη, χωρίς την γνώση του K, κάθε bit του μηνύματος να είναι 0 ή 1 με την ίδια πιθανότητα. Ο Bob έχει τη δυνατότητα να διαβάσει το μήνυμα με τον υπολογισμό του

$$M = X \oplus K = M \oplus K \oplus K \quad (3.4)$$

Με την προϋπόθεση ότι το μήκος του K είναι ίσο με το μήκος του M, δηλαδή

$$H(K) > H(M) \quad (3.5)$$

Η προϋπόθεση αυτή μας εξασφαλίζει ότι για κάθε bit του M, θα υπάρχει ένα bit του K, το οποίο δεν έχει χρησιμοποιηθεί ήδη, ώστε να κωδικοποιηθεί ένα άλλο bit M. Η έννοια secrecy αναφέρεται ως κρυπτογραφικό σύστημα του Shannon και αποδεικνύεται το παρακάτω θεώρημα:

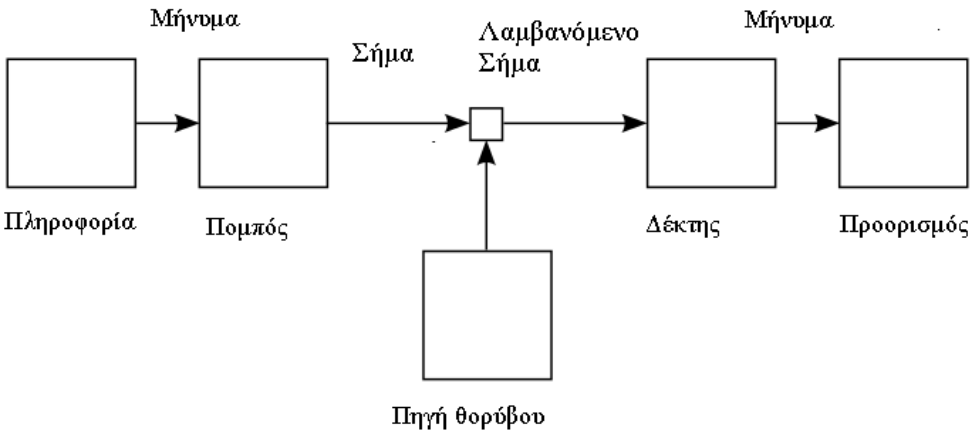
Αν |M| = |X | = |K|, ένα σχήμα κωδικοποίησης για το κρυπτογραφικό σύστημα Shannon, επιτυγχάνει τέλεια μυστικότητα αν και μόνο αν:

- Για κάθε ζεύγος (m, x) ∈ M× X , υπάρχει ένα μοναδικό κλειδί k ∈ K, έτσι ώστε X = e (m, x).
- Το κλειδί K είναι ομοιόμορφα κατανεμημένο στο K.

Σημειώνεται ότι τα M, X και K υποδηλώνουν τα σύνολα όλων των πιθανών τιμών των M, X και K, αντίστοιχα. Επίσης, e : M × K → X δηλώνει τη λειτουργία κωδικοποίησης και d : X × K → M δηλώνει τη λειτουργία αποκωδικοποίησης [34].

Επίσης, ο Bob είναι σε θέση να παράγει μια ακριβή, χωρίς σφάλματα εκτίμηση του μηνύματος. Άρα,

$$X = e(M, K) \text{ και } M = d(X, K) \quad (3.6)$$



Εικόνα 3.2: Μπλοκ διάγραμμα της θεωρίας της πληροφορία του Shannon

3.2 Wyner's Wiretap κανάλι

Οι βασικές έννοιες της θεωρητικής ασφάλειας πληροφοριών του Shannon έχει το μειονέκτημα να μην υπολογίζει το θόρυβο που επηρεάζει τις παρατηρήσεις της Eve σχετικά με την κωδική λέξη. Ο Wyner δημιούργησε το μοντέλο διαύλου υποκλοπής (wiretap channel model), προκειμένου να συμπεριλάβει και τα χαρακτηριστικά του Φυσικού Επιπέδου (PHY) του ασύρματου συστήματος. Σύμφωνα με το μοντέλο του Wyner, η Alice κωδικοποιεί το μήνυμα M σε μια κωδική λέξη X, η οποία στη συνέχεια μεταδίδεται στον Bob μέσω του κύριου καναλιού W και λαμβάνεται από τον Bob ως Y, ο οποίος στη συνέχεια παράγει μια εκτίμηση Mˆ του μηνύματος. Το Y περνάει επίσης μέσω του καναλιού του ωτακουστή W_0 και λαμβάνεται από την Eve ως Z [35].

Το μοντέλο υποκλοπής του ασύρματου διαύλου αναφέρεται ως το υποβαθμισμένο κανάλι διαύλου υποκλοπής DWTC (Degraded Wiretap Channel). Το διακριτό DWTC χωρίς μνήμη αποτελείται από ένα αλφάβητο εισόδου X , δύο αλφάβητα εξόδου Y και Z και τα κανάλια W και W_0 και υποδηλώνεται από τα (X , W, W_0 , Y, Z). Η πιθανότητα μετάβασης (transition probability) του DWTC δίνεται από τον εξής τύπο, όπου το n αποτελεί το μήκος της κωδικής λέξης [4]:

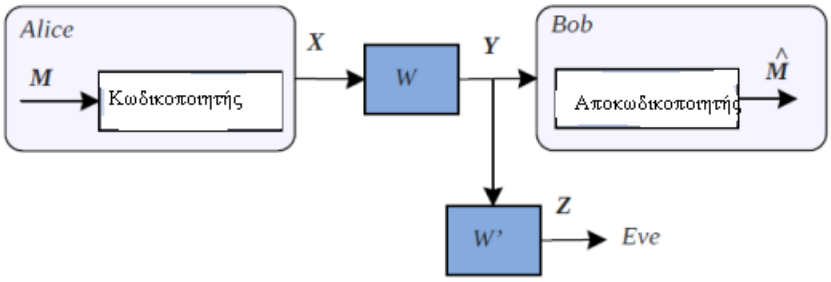
$$P_{YZ|X}(yz \mid x) = \prod_{i=1}^{n} W(y_i \mid x_i)W'(z_i \mid y_i), \forall n \geq 1, \forall (x, y, z) \in \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n \qquad (3.7)$$

Ο Wyner στη θεωρία του εισήγαγε έναν νέο ορισμό για την προϋπόθεση μυστικότητας (secrecy condition). Σύμφωνα με τη θεωρία ~~του~~ αυτή, δεν απαιτείται η αβεβαιότητα του ωτακουστή να είναι ίση με την εντροπία του μηνύματος, απαιτείται ο ρυθμός αβεβαιότητας (equivocation rate), να είναι κοντά στο ρυθμό εντροπίας του μηνύματος.

Ο ρυθμός αβεβαιότητας ορίζεται ως:

$$R_e = \frac{1}{n} H(M \mid Z) \qquad (3.8)$$

Οι κώδικες wiretap έχει αποδειχθεί ότι έχουν αυθαίρετα μικρή πιθανότητα σφάλματος και μυστικότητα στον προοριζόμενο δέκτη. Σε ένα DWTC, το μέγιστο επιτεύξιμο ποσοστό ασφαλούς μετάδοσης ονομάζεται ικανότητα μυστικότητας (secrecy capacity), η οποία είναι θετική όταν η παρατήρηση της Eve Z είναι πιο θορυβώδης από την παρατήρηση του Bob Y, διαφορετικά είναι 0 και θα εξεταστεί λεπτομερώς σε επόμενη ενότητα.



Εικόνα 3.3: Μπλοκ διάγραμμα ενός γενικού συστήματος καναλιών υποκλοπής

Πίνακας 3.1: Πλεονεκτήματα και μειονεκτήματα σε Wiretap Channel

Wiretap Channel	
ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Παρέχει αποδεδειγμένα ανθεκτική προστασία ενάντια στον ωτακουστή, ανεξάρτητα της ισχύος που κατέχει.	Στηρίζεται στην υπόθεση ότι το κανάλι μεταξύ πομπού και δέκτη είναι λιγότερο θορυβώδες από το κανάλι μεταξύ πομπού και ωτακουστή.
Είναι λιγότερη πολύπλοκη και δεσμεύει σημαντικά λιγότερους πόρους από άλλα μοντέλα μετάδοσης.	Καλύπτει μόνο το πρόβλημα της εμπιστευτικότητας, καθώς η αυθεντικοποίηση θεωρείται ότι έχει ήδη γίνει.
Έχει τη δυνατότητα να συνδυαστεί και να ενισχύσει τα άλλα μοντέλα μετάδοσης.	Ο ωτακουστής είναι παθητικός επιτιθέμενος.
Γίνονται έρευνες για βελτιωμένες εκδόσεις του αρχικού μοντέλου καναλιού υποκλοπής.	

3.3 Ορισμός της Μυστικότητας

Ένα από τα βασικά προβλήματα στην κρυπτογραφία είναι η δημιουργία ενός κοινού μυστικού κλειδιού μεταξύ δύο πλευρών. Ο Wyner και στη συνέχεια οι Csiszár και Körner περιέγραψαν και ανέλυσαν ρυθμίσεις για συμφωνία μυστικού κλειδιού με βάση θορυβώδη κανάλια επικοινωνίας. Ο Maurer καθώς και οι Ahlswede και Csiszár γενίκευσαν αυτά τα μοντέλα σε ένα σενάριο που βασίζεται στη συσχετισμένη τυχαιότητα και τη δημόσια συζήτηση. Σε όλες αυτές τις ρυθμίσεις, η ικανότητα μυστικότητας και ο ρυθμός μυστικού κλειδιού, αντίστοιχα, έχουν οριστεί ως οι μέγιστοι επιτεύξιμοι ρυθμοί με τους οποίους μπορεί να δημιουργηθεί ένα άκρως απόρρητο κλειδί από τους νόμιμο πομπό και δέκτη.

Ωστόσο, οι απαιτήσεις απορρήτου ήταν πολύ αδύναμες σε όλους αυτούς τους ορισμούς. Ήταν άγνωστο προηγουμένως πώς να δημιουργηθούν κλειδιά για τα οποία ο ωτοακουστής δεν έχει ουσιαστικά πληροφορίες [36].

Η απαίτηση για τέλεια μυστικότητα προϋποθέτει αξιοπιστία (reliability), αδύναμη ασφάλεια (weak security) και ισχυρές συνθήκες ασφαλείας (strong security conditions).

1. Αξιοπιστία: Η πιθανότητα μετράται σε όλες τις πιθανές τιμές του M. Καθώς το μήκος του μπλοκ τείνει στο άπειρο, η πιθανότητα ότι ο Bob θα κάνει λάθος στην εκτίμηση του διανύσματος πληροφοριών θα πρέπει να τείνει στο μηδέν.

$$\lim_{k\to\infty} \mathcal{P}_r(\hat{M} \neq M) = 0 \quad (3.9)$$

2. Αδύναμη Ασφάλεια: Το I(M, Z) δηλώνει την αμοιβαία πληροφορία μεταξύ M και Z και είναι ίσο με H(M) − H(M | Z) όπου το H(M) δηλώνει την υπό όρους εντροπία του M. Το H(M | Z) δηλώνει την υπό όρους εντροπία του Z δεδομένου του M. Αυτό σημαίνει ότι, καθώς το μήκος του μπλοκ τείνει στο άπειρο, οι πληροφορίες που διαθέτει η Eve θα τείνουν στο μηδέν [4].

$$\lim_{k\to\infty} \frac{I(M;Z)}{k} = 0 \quad (3.10)$$

3. Ισχυρές συνθήκες ασφάλειας: Ο Maurer ισχυρίστηκε ότι η προηγούμενη συνθήκη είναι πολύ αδύναμη, για αυτό ορίστηκε μία ισχυρή συνθήκη μυστικότητας που έλυνε της αδυναμίες της προηγούμενης.

$$\lim_{k\to\infty} I(M;Z) = 0 \quad (3.11)$$

3.4 Χωρητικότητα μυστικότητας (Secrecy Capacity)

Με τον όρο χωρητικότητα μυστικότητας (secrecy capacity) αναφερόμαστε στο μέγιστο επιτεύξιμο ποσοστό ασφαλούς μετάδοσης για ένα συγκεκριμένο κανάλι wiretap και αποτελεί ένα ιδιαίτερα σημαντικό μέτρο της απόδοσης ενός ασφαλούς ασύρματου

συστήματος επικοινωνιών [4]. Σε αυτή την υποενότητα δίνεται το θεωρητικό υπόβαθρο και εξετάζεται η πραγματοποίησή του για διάφορα κανάλια που απαντώνται συχνά στην πράξη.

Η σχέση secrety capacity C_s^{DWTC} ενός DWTC (X , W, W΄ , Y, Z) δίνεται από:

$$C_s^{DWTC} = \max_{px} (I(X; Y) – I(X;Z)) \quad (3.12)$$

όπου το px δηλώνει την κατανομή του αλφαβήτου εισόδου στο σύνολο X.

Παρατηρούμε ότι αν οι παρατηρήσεις του Bob και της Eve είναι ίσες, δηλαδή Y = Z, τότε I(X; Y | Z) = 0 και από τη προηγούμενη σχέση προκύπτει ότι το $C_s^{DWTC} = 0$. Αυτή η παρατήρηση επιβεβαιώνει ότι, για να έχουμε μη μηδενική χωρητικότητα μυστικότητας ,το κανάλι του ωτακουστή πρέπει να υποβαθμιστεί σε σχέση με το κύριο κανάλι. Δείχνει επίσης ότι η ασφάλεια δεν μπορεί να επιτευχθεί μέσω αθόρυβων καναλιών.

Η χωρητικότητα για το κανάλι ανάμεσα στην Alice και Bob είναι [37]:

$$C_B = \log_2\left(1 + g_b \cdot \frac{P_s}{N_B}\right) = \log_2(1 + \gamma_B) \quad (3.13)$$

Και αντίστοιχα για την Alice και Eve:

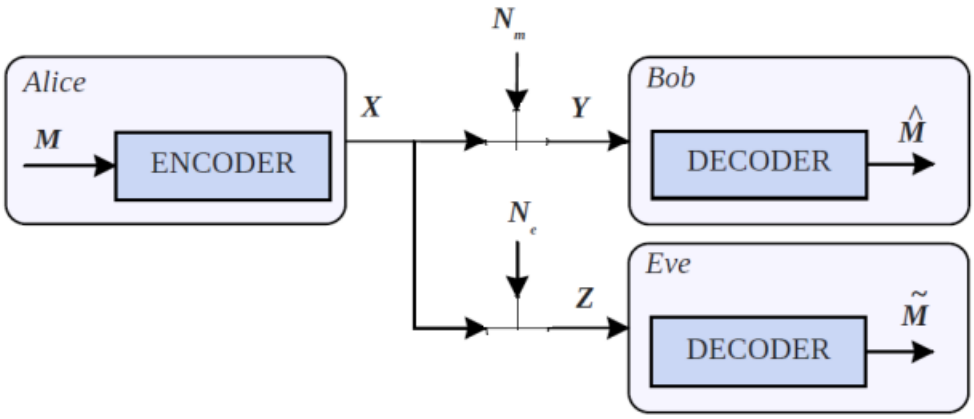
$$C_E = \log_2\left(1 + g_e \cdot \frac{P_s}{N_E}\right) = \log_2(1 + \gamma_E) \quad (3.14)$$

Η χωρητικότητα μυστικότητας (secrecy capacity) είναι τόσο μεγάλη όσο η διαφορά μεταξύ των χωρητικοτήτων του κύριου καναλιού και του καναλιού του ωτακουστή. Άρα, είναι θετικός όταν $\gamma_B > \gamma_E$ και μηδέν όταν $\gamma_B \leq \gamma_E$ και ισχύει:

$$C_s = \begin{cases} \log_2(1+\gamma_B) - \log_2(1+\gamma_E) & if \quad \gamma_B > \gamma_E \\ 0 & if \quad \gamma_B \leq \gamma_E \end{cases} \quad (3.15)$$

3.5 Γκαουσιανό κανάλι

Τα γκαουσιανά κανάλια χρησιμοποιούνται ευρέως, επειδή όχι μόνο παρέχουν μια καλή προσέγγιση πολλών πρακτικών ασύρματων συστημάτων, αλλά είναι επίσης σχετικά εύκολο να μοντελοποιηθούν και να αναλυθούν. Αυτά τα κανάλια χαρακτηρίζονται από ένα πρόσθετο όρο γκαουσιανού θορύβου (AWGN), ο οποίος προστίθεται στο μεταδιδόμενο σήμα [30].



Εικόνα 3.4: Γκαουσιανό wiretap κανάλι

Το secrecy capacity για ένα γκαουσιανό κανάλι δίνεται από την σχέση:

$$C_s = \left(\frac{1}{2}\log\left(1+\frac{E_s}{\sigma_B^2}\right) - \frac{1}{2}\log\left(1+\frac{E_s}{\sigma_E^2}\right)\right)^+ = (C_B - C_E)^+ \quad (3.16)$$

όπου E_s είναι η ενέργεια του μεταδιδόμενου σήματος και ο τελεστής $^+$ επιστρέφει το όρισμα εάν είναι θετικό αλλιώς επιστρέφει 0.

Λαμβάνοντας υπόψη τις σχέσεις της προηγούμενης υποενότητας καταλήγουμε ότι:

$$C_B = \frac{1}{2}\log(1+\frac{E_s}{\sigma_B^2}) \quad (3.17)$$

Καθώς επίσης και

$$C_E = \frac{1}{2}\log(1+\frac{E_s}{\sigma_E^2}) \quad (3.18)$$

Από τις παραπάνω σχέσεις προκύπτει ότι η χωρητικότητα μυστικότητας (secrecy capacity) του γκαουσιανού καναλιού είναι μεγαλύτερο από το μηδέν, αν και μόνο εάν η χωρητικότητα του κύριου καναλιού είναι μεγαλύτερη από την χωρητικότητα του καναλιού του ωτακουστή. Συγκεκριμένα, αν και μόνο εάν ο Bob έχει καλύτερη σχέση σήματος προς θόρυβο SNR από την Eve. Στην πράξη, αυτό επιτυγχάνεται συνήθως εάν η απόσταση μεταξύ Alice και Eve είναι μεγαλύτερη από την απόσταση μεταξύ Alice και Bob.

Λαμβάνοντας το όριο Es → ∞ και σε συνθήκες υψηλής ισχύος, ο όρος ο όρος secrecy capacity γίνεται:

$$\lim_{E_s \to \infty} C_s(E_s) = \left(\frac{1}{2} \log(\frac{\sigma_E^2}{\sigma_B^2}) \right)^+ \quad (3.19)$$

όπου συμπεραίνουμε ότι δεν αυξάνεται απεριόριστα καθώς αυξάνεται η ισχύς σήματος, αλλά τείνει σε ένα ανώτερο όριο.

3.6 Κανάλι με παρεμβολές

Θέλοντας να βελτιώσουμε την χωρητικότητα μυστικότητας της επικοινωνίας προσθέτουμε στο σύστημα γκαουσιανό θόρυβο με ισχύ που ποικίλλει ανάλογα με τις απαιτήσεις. Επίσης, τοποθετούνται N παρεμβολείς στο σύστημα. Η ισχύς του κάθε παρεμβολέα είναι η P_j . Μπορούμε να εκφράσουμε έτσι τα μοντέλα σήματος για αυτό το κανάλι ως εξής [4]:

$$\begin{aligned} y_i &= x_i + n_{B,i} + I_i \\ z_i &= x_i + n_{E,i} + I_i \end{aligned} \quad (3.20)$$

όπου I_i είναι το άθροισμα των παρεμβολών των διανυσμάτων Y,Z από τους N παρεμβολές. Έτσι το secrecy capacity για αυτό το κανάλι είναι:

$$C_s = \frac{1}{2}\log 2(1 + \frac{E_s}{\sigma_B^2 + \sum_{j=1}^{N} I_{Bj}}) - \frac{1}{2}\log 2(1 + \frac{E_s}{\sigma_E^2 + \sum_{j=1}^{N} I_{Ej}}) \quad (3.21)$$

Στην εργασία χρησιμοποιήθηκε η τεχνική πολυπλεξίας/μετάδοσης OFDM για τον υπολογισμό της χωρητικότητας μυστικότητας, οπότε στο επόμενο κεφάλαιο θα γίνει η μελέτη και η επεξήγηση της χρήσης της τεχνικής OFDM.

4. Εκτίμηση Ασύρματου Καναλιού σε Συστήματα OFDM

Η μέθοδος OFDM (Orthogonal Frequency Division Multiplexing) αποτελεί μία ευέλικτη μέθοδος πολυπλεξίας καναλιών με αυξημένη χωρητικότητα που εφαρμόστηκε στις τηλεπικοινωνίες στα τέλη του προηγούμενου αιώνα. Είναι η πιο διάσημη τεχνολογία στον χώρο των τηλεπικοινωνιών την τελευταία δεκαετία σε συστήματα τηλεπικοινωνιών υψηλού ρυθμού [38].

4.1 Ιστορική αναδρομή

Η ανάπτυξη της τεχνικής OFDM ήταν γνωστή από το 1960, μετά από αρκετές έρευνες γύρω από το αντικείμενο έφτασε σε στάδιο ωριμότητας και ανάπτυξης για εμπορική εφαρμογή στις αρχές της δεκαετίας του 1990. Την δεκαετία του 1960 η OFDM χρησιμοποιήθηκε σε στρατιωτικά προγράμματα τα οποία λειτουργούσαν σε ζώνες υψηλής συχνότητας. Ο πρώτος που ανέπτυξε το OFDM ήταν ο Chang το 1966, ο οποίος χρησιμοποίησε επικαλυπτόμενα ορθογωνικά σήματα για μετάδοση δεδομένων. Το 1971 ο Weinstein χρησιμοποίησε το Διακριτό Μετασχηματισμό Fourier (Discrete Fourier Transform) και στην συνέχεια ,το 1980 μελετήθηκε η OFDM για την αποδοτικότητά της σε modems ~~για~~ υψηλών συχνοτήτων ψηφιακές κινητές επικοινωνίες, καθώς και σε εγγραφές υψηλής πυκνότητας. Το 1985 ο Cimini έκανε την πρόταση ορισμού της OFDM ως την καταλληλότερη τεχνική για τις ασύρματες επικοινωνίες. Το 1990 χρησιμοποιήθηκε για ευρεία ζώνης επικοινωνίας πάνω από κινητά ραδιοφωνικά κανάλια FM, καθώς και σε τεχνολογίες όπως το ADSL,VDSL και HDTV.

4.2 Εισαγωγή στην OFDM

Οι απαιτήσεις των σύγχρονων συστημάτων επικοινωνιών απαιτούν μεγαλύτερες ταχύτητες στις επικοινωνίες και παροχή περισσότερων υπηρεσιών. Αυτό επιτυγχάνεται:

- Μεταβαλλόμενη ποιότητα υπηρεσίας

- Ελάχιστη ισχύς εκπομπής
- Αυξημένη Χωρητικότητα

- Ολοκληρωμένα προγραμματιζόμενα στοιχεία
- Ευελιξία

Η Ορθογωνική Πολυπλεξία με Διαίρεση Συχνότητας (OFDM) είναι μία τεχνική μετάδοσης η οποία μεταδίδει ψηφιακά δεδομένα με χρήση πολλαπλών διαδρομών και εξάπλωση καθυστέρησης. Δημιουργείται ένας μεγάλος αριθμός παράλληλων υποφερόντων (subcarriers) και τα δεδομένα χωρίζονται και μοιράζονται σε πολλά υποκανάλια μικρότερου εύρους ζώνης, στη συνέχεια, τα κανάλια σχηματίζουν το φάσμα του μεταδιδόμενου σήματος με τον διαχωρισμό τους σε διαστήματα συχνότητας. Οι αποστάσεις που έχουν οι συχνότητες που δέχονται τα κανάλια είναι τέτοιες ώστε τα σήματα που στέλνονται να είναι ορθογώνια μεταξύ τους [39]. Η αντιμετώπιση των δυο βασικών προβλημάτων που χαρακτηρίζουν τα ασύρματα κανάλια της παρεμβολής και του εξασθένισης (fading) είναι βασικός λόγος χρήσης της OFDM.

Η μετάδοση με διαμόρφωση OFDM έχει τα εξής πλεονεκτήματα:

- Αντιμετωπίζει αποτελεσματικά την πολυόδευση του σήματος.
- Η προσαρμογή του ρυθμού μετάδοσης σε κάθε φορέα στο λόγο σήματος προς θόρυβο (SNR) της υποφέρουσας είναι πιο απλή με αποτέλεσμα την αύξηση του ρυθμού μετάδοσης σε κανάλια που μεταβάλλονται σταδιακά στον χρόνο.
- Αντιμετωπίζει την παρεμβολή, επειδή επηρεάζει σταδιακά ένα μικρό ποσοστό των υποφερουσών.
- Επιτρέπει την υλοποίηση των δικτύων με απλές συχνότητες τα οποία είναι πρόσφορα για τις εφαρμογές ευρεκπομπής.

Ένα από τα μεγαλύτερα πλεονεκτήματα της OFDM είναι η ορθογωνιότητα των παράλληλα μεταδιδόμενων παλμών. Η ορθογωνιότητα επιτρέπει σε πολλαπλά σήματα πληροφορίας να μεταδίδονται σε ένα κοινό κανάλι επικοινωνίας και να ανιχνεύονται χωρίς μεταξύ τους παρεμβολή.

Βέβαια υπάρχουν και κάποια μειονεκτήματα:

- Η OFDM είναι ευαίσθητη ως τεχνική στο θόρυβο φάσης αλλά και στις αποκλίσεις συχνότητας φορέα.

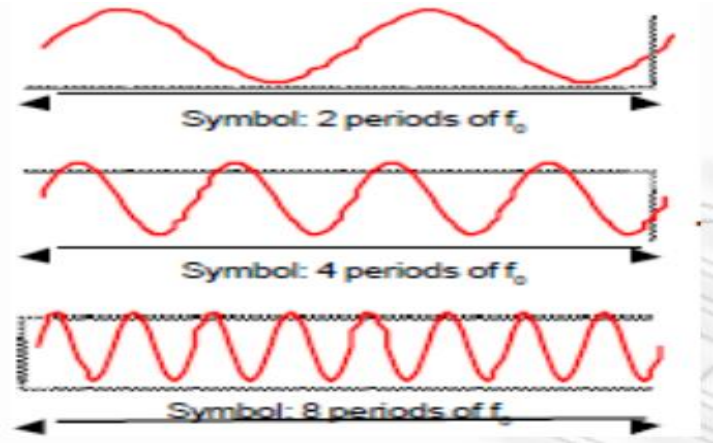
- Απαιτεί υψηλό λόγο μέγιστης προς μέση ισχύ στον πομπό, γεγονός που τείνει να ελαττώσει, την αποδοτικότητα του ενισχυτή στον πομπό.

4.3 Περιγραφή Πολυπλεξίας Ορθογώνιας Διαίρεσης Συχνοτήτων

Στην τεχνική OFDM τα σήματα που στέλνονται πρέπει να είναι ορθογώνια και ανεξάρτητα μεταξύ τους, ώστε ο δέκτης να τα δέχεται χωρίς παρεμβολές. Με την χρήση των subcarriers, καταφέρνουμε την διατήρηση της ορθογωνιότητας και παράλληλα την μεγαλύτερη δυνατή εκμετάλλευση του φάσματος. Για να επιτευχθεί αυτό είναι απαραίτητες δύο προϋποθέσεις [38]:

1. Πεδίο χρόνου: Στη διάρκεια του OFDM συμβόλου T_s (ένα OFDM σύμβολο αποτελείται από ένα σύνολο ημιτόνων καθένα από τα οποία αντιστοιχεί σε κάθε subcarrier και η συχνότητα του είναι ακέραια του αντιστρόφου της διάρκειας του, για να επιτευχθεί η πρώτη προϋπόθεση, $f_n=n/T_s$) πρέπει κάθε subcarrier να έχει ακέραιο αριθμό περιόδων και ο αριθμός των γειτονικών subcarriers να διαφέρει κατά ένα.

2. Πεδίο συχνοτήτων: Το μέγιστο στο φάσμα του κάθε subcarrier να συμπίπτει με τα φασματικά μηδενικά των υπολοίπων. Αυτό έχει σαν επακόλουθο να μη δημιουργούνται παρεμβολές μεταξύ των φερόντων. Έτσι όταν ο δέκτης προσπαθεί να διαχωρίσει τα μεταδιδόμενα σήματα και απομονώσει με τα απαραίτητα φίλτρα την κεντρική συχνότητα κάθε ενός φέροντος η μόνη ενέργεια που θα λάβει θα είναι από το επιθυμητό σήμα μαζί με κάποιο θόρυβο που προστίθεται στο κανάλι.



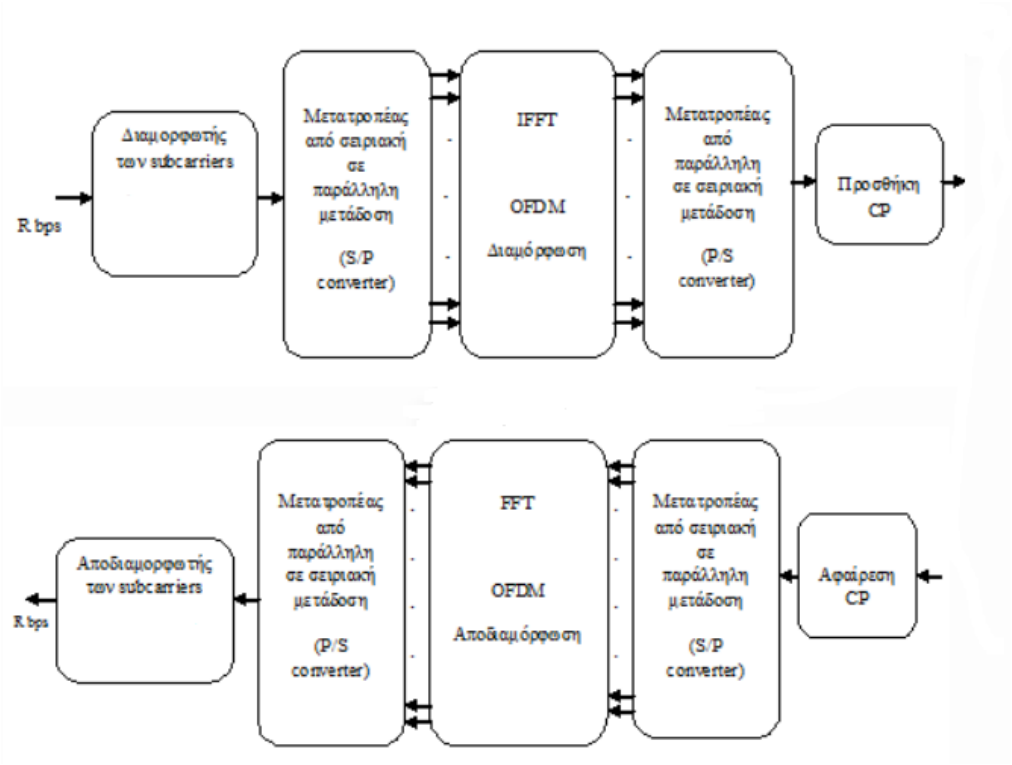
Εικόνα 4.1: Ακέραιος αριθμός περιόδων στη διάρκεια συμβόλου

4.4 Εκπομπή και λήψη σημάτων OFDM

Η OFDM ακολουθία μοιράζεται σε subcarriers και στο καθένα δίνονται τα δεδομένα που είναι προς μετάδοση. Σε αυτό το σημείο έχει επιλεγεί ήδη το φάσμα των συχνοτήτων και ο τύπος διαμόρφωσης, από τον οποίο εξαρτάται το πλάτος και η φάση που θα δοθεί σε κάθε subcarrier. Αρχικά τα δεδομένα εισέρχονται σε σειριακή μορφή και μετατρέπονται σε παράλληλη με τη μορφή subcarriers. Μετατρέπεται το σήμα από το πεδίο συχνοτήτων στο πεδίο του χρόνου μέσω ενός αντίστροφου μετασχηματισμού Fourier (IFFT). Ο IFFT δέχεται έναν αριθμό μιγαδικών σημείων που λέγονται bin και το κάθε ένα από αυτά αντιστοιχεί σε ένα subcarrier και ο αριθμός N εισόδων του IFFT είναι δύναμη του 2, ώστε να μπορεί να εξυπηρετήσει όλα τα subcarriers. Τα δεδομένα των εξόδων του IFFT μετατρέπονται και πάλι σε σειριακή μορφή.

Στη συνέχεια, με τη χρήση OFDM παραμένει η διασυμβολική παρεμβολή γιατί ένα subcarrier μπορεί να ληφθεί από το δέκτη την ίδια στιγμή που λαμβάνεται η καθυστερημένη εκδοχή ενός προηγούμενου subcarrier. Η απαλοιφή από την διασυμβολική παρεμβολή γίνεται με την προσθήκη ενός χρονικού διαστήματος προστασίας στην αρχή του συμβόλου σε κάθε subcarrier, το οποίο θα πρέπει να είναι μεγαλύτερο της μέγιστης τιμής της εξάπλωσης καθυστέρησης του καναλιού, για να μην παρεμβάλλεται από το πεδίο του χρόνου το ένα σύμβολο στο άλλο. Η αντιγραφή του τελευταίου μέρους του συμβόλου γίνεται για την σωστή αντιμετώπιση των παρεμβολών και τοποθετείται στην αρχή σαν διάστημα φύλαξης (cyclic prefix). Η τοποθέτηση στην αρχή του συμβόλου εξυπηρετεί στην διατήρηση του συγχρονισμού του subcarrier στο δέκτη καθώς επίσης και στο γεγονός ότι το κυκλικό πρόθεμα εφαρμόζεται εύκολα μεταξύ του σήματος OFDM και της απόκρισης καναλιού για τη μοντελοποίηση του συστήματος μετάδοσης.

Τέλος, στο δέκτη πραγματοποιείται ακριβώς η αντίθετη διαδικασία, με σκοπό τη παραγωγή του αρχικού ψηφιακού σήματος.



Εικόνα 4.2: Μπλοκ διάγραμμα ενός OFDM συστήματος

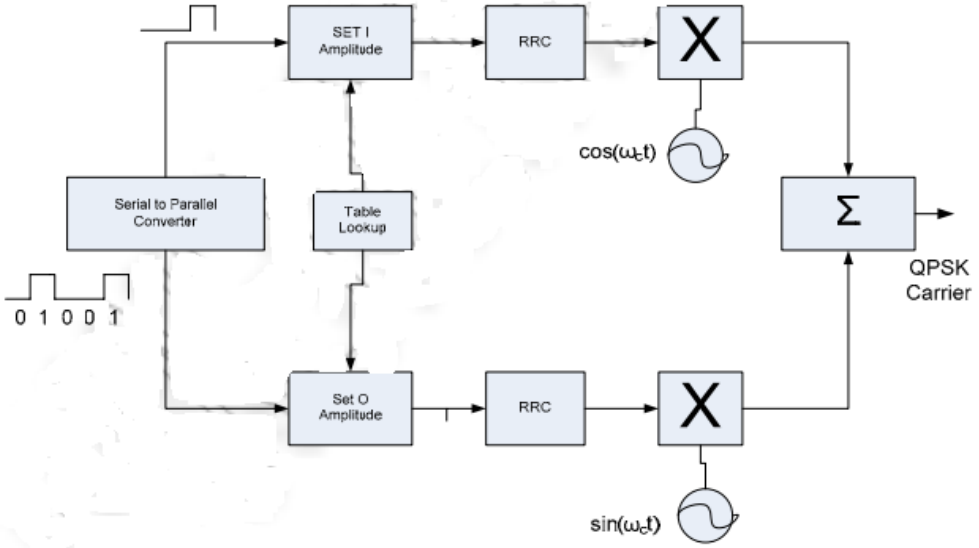
4.5 Διαμόρφωση και Αποδιαμόρφωση Σήματος

Διαμόρφωση σήματος ονομάζεται η διαδικασία μετατροπής των δεδομένων, προκειμένου να διευκολύνεται η μεταφορά τους και να μεταδίδονται με επιτυχία στο μέσο. Οι σημαντικότεροι παράμετροι είναι το πλάτος, η συχνότητα και η φάση. Αντίθετα, αποδιαμόρφωση σήματος είναι η ανάστροφη διαδικασία, ώστε να ανακτηθεί το αρχικό σήμα.

4.6 Διαμόρφωση QPSK

Με τον όρο QPSK (Quadrature Phase Sift Keying) αναφερόμαστε στη διαμόρφωση μετατόπισης φάσης με ορθογωνισμό. Η διαμόρφωση φάσης είναι μία παραλλαγή της διαμόρφωσης της συχνότητας, όπου τα bits ψηφιακής πληροφορίας διαμορφώνουν τη φάση της φέρουσας και δημιουργούν διαφορά φάσης. Η διαμόρφωση QPSK χρησιμοποιείται στις δορυφορικές τηλεοπτικές μεταδόσεις. Η QPSK χρησιμοποιεί τέσσερις φάσεις (0^o ,90^o ,180^o

και 270º) και μπορεί να κωδικοποιήσει 2 bits ανά σύμβολο, δηλαδή για κάθε σύμβολο χρησιμοποιούνται 2 bits [39].

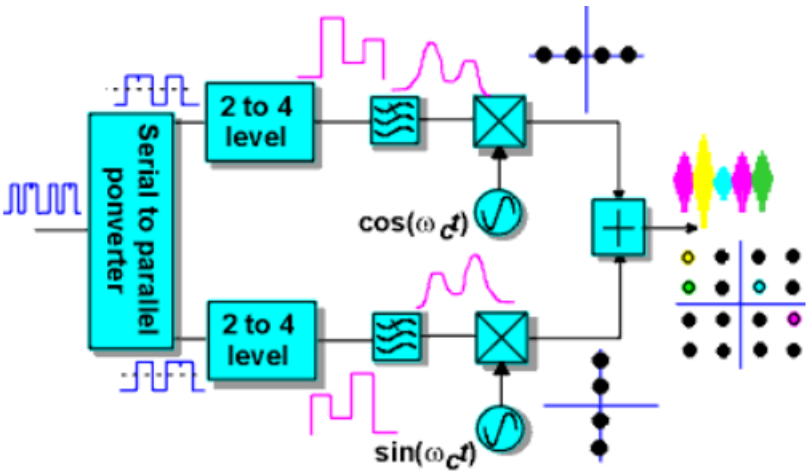


Εικόνα 4.3: Διαμόρφωση QPSK

4.7 Διαμόρφωση QAM

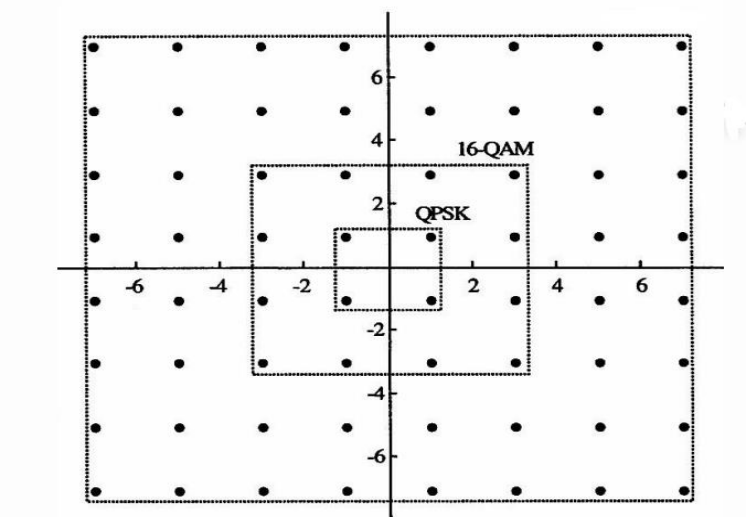
Ένας ακόμη τύπος ψηφιακής διαμόρφωσης είναι αυτός της QAM (Quadrature Amplitude Modulation). Η QAM συνδυάζει τη διαμόρφωση του πλάτους και τη διαμόρφωση της φάσης ταυτόχρονα, δηλαδή διαμορφώνεται μία ημιτονοειδής φέρουσα σε πλάτος και φάση. Κάθε σύμβολο είναι ένας συγκεκριμένος συνδυασμός τιμής πλάτους και φάσης. Το αποτέλεσμα της διαμόρφωσης δεν είναι ένα σήμα μίας συχνότητας, αλλά ένας συνδυασμός συχνοτήτων. Το εύρος συχνοτήτων ενός QAM σήματος εξαρτάται από την ροή των δεδομένων (symbolrate).

Η απλούστερη μορφή διαμόρφωσης QAM είναι στην πραγματικότητα το σύνολο συμβόλων της QPSK, το οποίο μπορεί να θεωρηθεί ως δύο ορθογώνιοι (με διαφορά φάσης 90°) φορείς διαμορφωμένοι κατά πλάτος, με στάθμες πλάτους +α και –α. Αυξάνοντας τον αριθμό των σταθμών πλάτους κάθε φορέα σε τέσσερις, για παράδειγμα ±α και ±3α, προκύπτουν 16 δυνατοί συνδυασμοί συμβόλων στην έξοδο του πομπού, οι οποίοι απέχουν εξίσου στο διάγραμμα αστερισμού και αντιπροσωπεύονται από συγκεκριμένο πλάτος και φάση ο καθένας [40].



Εικόνα 4.4: Διαμόρφωση 16-QAM

Κάθε σημείο του αστερισμού αντιστοιχεί σε μία σειρά από bits ανάλογα τη διαμόρφωση που έχουμε. Ο αριθμός των bits που μεταδίδονται από ένα σύμβολο προκύπτει από το τύπο $\log_2 M$, όπου M ο αριθμός των σημείων στον αστερισμό.



Εικόνα 4.5: Αστερισμοί διαμορφώσεων QPSK και 16-QAM

Β. ΠΡΟΣΟΜΟΙΩΣΗ ΚΑΙ ΑΠΟΤΕΛΕΣΜΑΤΑ

5. Ανάλυση και Αποτελέσματα Προσομοίωσης

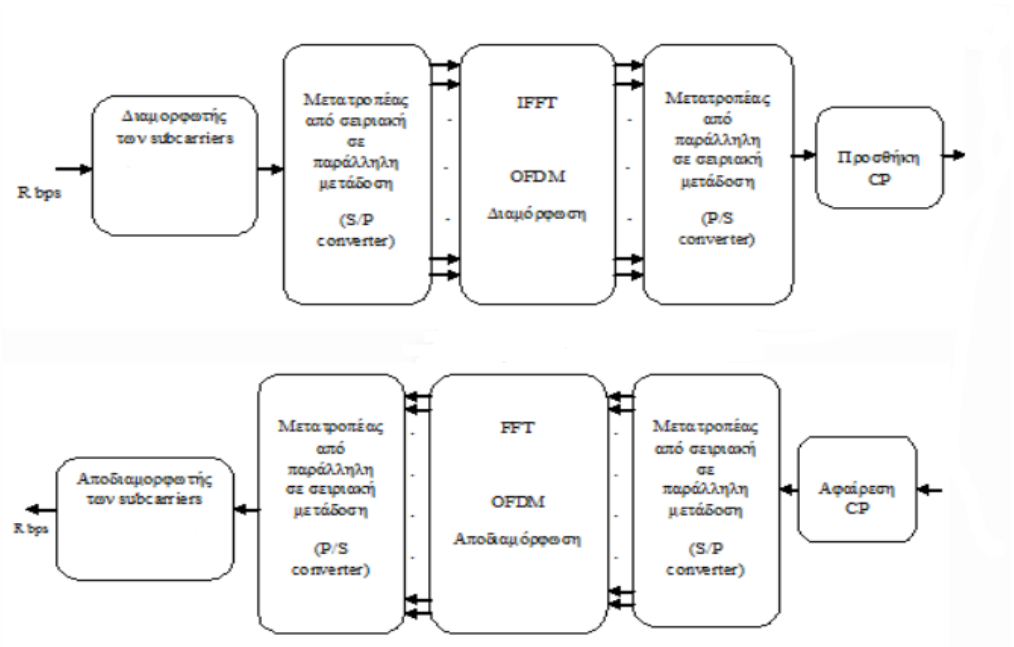
Το 5G ασύρματο δίκτυο που μελετά η συγκεκριμένη διπλωματική εργασία χρησιμοποιεί την τεχνική πολυπλεξίας/διαμόρφωσης OFDM (Orthogonal Frequency Division Multiplexing) για την εκπομπή και λήψη του σήματος πληροφορίας. Ο πομπός αναφέρεται ως Alice, ο νόμιμος δέκτης ως Bob και ο ωτακουστής ως Eve, όπως και στην ασφάλεια της πληροφορίας. Σε ένα σύστημα OFDM θέτουμε τα πιλοτικά κανάλια που έχουν συγκεκριμένο πλήθος και συγκεκριμένες θέσεις όπως αναγράφονται στις τεχνικές προδιαγραφές του συστήματος 5G. Στην εργασία μας μεταβάλουμε τις θέσεις των πιλοτικών καναλιών σε κάθε OFDM σύμβολο. Δηλαδή προτείνεται μία παραλλαγή των τεχνικών προδιαγραφών του δικτύου 5G. Η κατανομή πιθανότητας των θέσεων των πιλοτικών υπομεταφορέων στο φάσμα του σήματος OFDM γνωστοποιείται στο νόμιμο πομπό (Alice) και στο νόμιμο δέκτη (Bob) κατά τη φάση της αυθεντικοποίησης. Ο νόμιμος δέκτης έχει το πλεονέκτημα, επειδή γνωρίζει την πληροφορία που θα έπρεπε να λάβει από τον πομπό στα πιλοτικά κανάλια και μπορεί να την συγκρίνει με αυτή που έλαβε πραγματικά, ώστε να πραγματοποιήσει την εκτίμηση του ασύρματου καναλιού. Ο ωτακουστής δεν γνωρίζει τις θέσεις των πιλοτικών καναλιών και έτσι πρέπει να κάνει «τυφλή» εκτίμηση του ασύρματου καναλιού που είναι λιγότερη αποτελεσματική σε σύγκριση με την εκτίμηση βασισμένη στη πληροφορία που μεταφέρουν τα πιλοτικά κανάλια.

Για την προσομοίωση του OFDM συστήματος χρησιμοποιήθηκε το MATLAB, το οποίο είναι ένα περιβάλλον αριθμητικής υπολογιστικής. Το πλήθος των bits που στάλθηκαν από τον πομπό στον δέκτη ορίστηκε ως NoBits= 2^{22}, καθώς χρειάζονται αρκετά bits προκειμένου να επιτευχθεί υψηλό E_b/N_o. Στην προσομοίωση χρησιμοποιήθηκαν οι ψηφιακές διαμορφώσεις QPSK και 16-QAM.

Στο πομπό με την χρήση του αντιστρόφου γρήγορου μετασχηματισμού Fourier (IFFT) πραγματοποιείται η μετατροπή του σήματος από το πεδίο της συχνότητας στο πεδίο του χρόνου. Ο γρήγορος μετασχηματισμός Fourier απαιτεί το πλήθος των σημείων να είναι δύναμη του 2, για αυτό το λόγο επιλέχθηκε στην εργασία το πλήθος των υποφορέων σε κάθε OFDM σύμβολο να είναι 256 (2^8). Στο πλήθος των 256 υποφορέων (subcarriers), τα 32 από αυτά μεταφέρουν την πληροφορία των πιλοτικών καναλιών, τα οποία μπαίνουν σε

συγκεκριμένες θέσεις (ακολουθώντας συγκεκριμένη κατανομή) και χρησιμοποιούνται από το δέκτη για την αποδιαμόρφωση του σήματος, όπου η τυχαιοποίηση των θέσεων των πιλοτικών καναλιών ακολουθεί κατανομή Poisson.

Για την εκτέλεση της προσομοίωσης ακολουθήθηκε το διάγραμμα ροής των διαδικασιών του OFDM, όπως αναλύθηκε και στο προηγούμενο κεφάλαιο. Αρχικά δημιουργούνται τα δεδομένα σε σειριακή μορφή και μετατρέπονται σε παράλληλη με τη μορφή subcarriers και με την λειτουργία αντίστροφου γρήγορου μετασχηματισμού Fourier (IFFT) πραγματοποιείται η μετατροπή του σήματος από το πεδίο της συχνότητας στο πεδίο του χρόνου. Στην έξοδο των δεδομένων του IFFT μετατρέπονται ξανά σε σειριακή μορφή. Στο σημείο αυτό πραγματοποιείται η προσθήκη ενός χρονικού διαστήματος προστασίας στην αρχή του OFDM συμβόλου σε κάθε subcarrier, που ονομάζεται κυκλικό πρόθεμα (cyclic prefix) και προστίθεται στο σήμα που θα αποστείλει ο πομπός. Στο δέκτη πραγματοποιείται ακριβώς η αντίστροφη διαδικασία, με σκοπό τη παραγωγή του αρχικού ψηφιακού σήματος, δηλαδή αφαιρείται το κυκλικό πρόθεμα και μετατρέπονται τα δεδομένα από σειριακά σε παράλληλα. Στον δέκτη με την λειτουργία ευθέως γρήγορου μετασχηματισμού Fourier (FFT) μετατρέπεται το σήμα από το πεδίο του χρόνου στο πεδίο της συχνότητας και γίνεται μετατροπή των δεδομένων από παράλληλα σε σειριακά, ώστε τελικά ο δέκτης να αποδιαμορφώσει τους υποφορείς και να λάβει τα δεδομένα που του έχει αποστείλει ο πομπός.



Εικόνα 5.1: Μπλοκ διάγραμμα ενός OFDM συστήματος

Παρακάτω παρουσιάζονται τα δεδομένα των προσομοίωσεων που πραγματοποιήθηκαν. Στις προσομοιώσεις θεωρήθηκε ότι οι δύο δέκτες (Bob και Eve) κινούνται με την ίδια ταχύτητα και προς την ίδια κατεύθυνση (ταχύτητες 20, 40 και 80 km/h). Επίσης, χρησιμοποιήθηκαν διαμορφώσεις QPSK και 16-QAM και ανάλογα την διαμόρφωση και την ταχύτητα της εκάστοτε προσομοίωσης υπολογιζόταν η συχνότητα Doppler (F_D), ο παράγοντας r_0 της συνάρτησης Bessel, το οποίο ορίζει αν θα είναι αργή ή γρήγορη η εξασθένιση και το f_T.

$$r_0 = 2*\pi*f_T \qquad (5.1)$$

Σκοπός ήταν ο υπολογισμός των ρυθμού σφαλμάτων bit BER (Bit Error Rate) στον νόμιμο δέκτη (Bob) και στον ωτακουστή (Eve). Ο σηματοθορυβικός λόγος (SNR) μεταβαλλόταν από 0dB μέχρι 60dB με βήμα 5dB. Ταυτόχρονα μελετήθηκε το διάγραμμα αστερισμού για την κάθε διαμόρφωση και η σχέση μεταξύ του σηματοθορυβικού λόγου και του μέσου τετραγωνικού σφάλματος του καναλιού (channel mean square error), χρησιμοποιώντας τον τύπο:

$$\text{CMSE} = \sqrt{\sum_{i=1}^{n} \frac{(\hat{y_i} - y_i)^2}{n}} \qquad (5.2)$$

Ο ρυθμός σφαλμάτων bit (BER), αφορά τη μέτρηση του ρυθμού λαθών, σε μια σειρά ψηφιακών δεδομένων, που μεταφέρονται μέσω ενός καναλιού από μια θέση σε μία άλλη και υπολογίζεται με τον εξής τύπο:

$$BER = \frac{Αριθμός\ σφαλμάτων}{Αριθμός\ απεσταλμένων\ bits} \qquad (5.3)$$

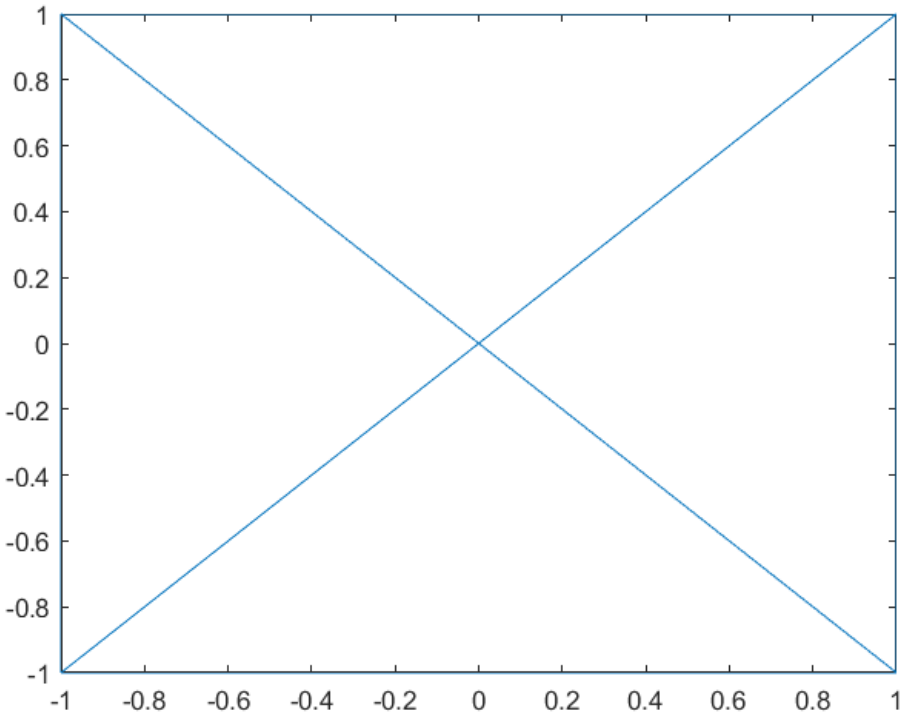
Στον πίνακα 5.1 αναφέρονται οι παράμετροι της προσομοίωσης για ταχύτητα κινητών (Bob και Eve) ίση με 20 km/h, για διαμόρφωση QPSK και τα αποτελέσματα της προσομοίωσης παρουσιάζονται παρακάτω.

Πίνακας 5.1: Παράμετροι προσομοίωσης για QPSK και 20 km/h

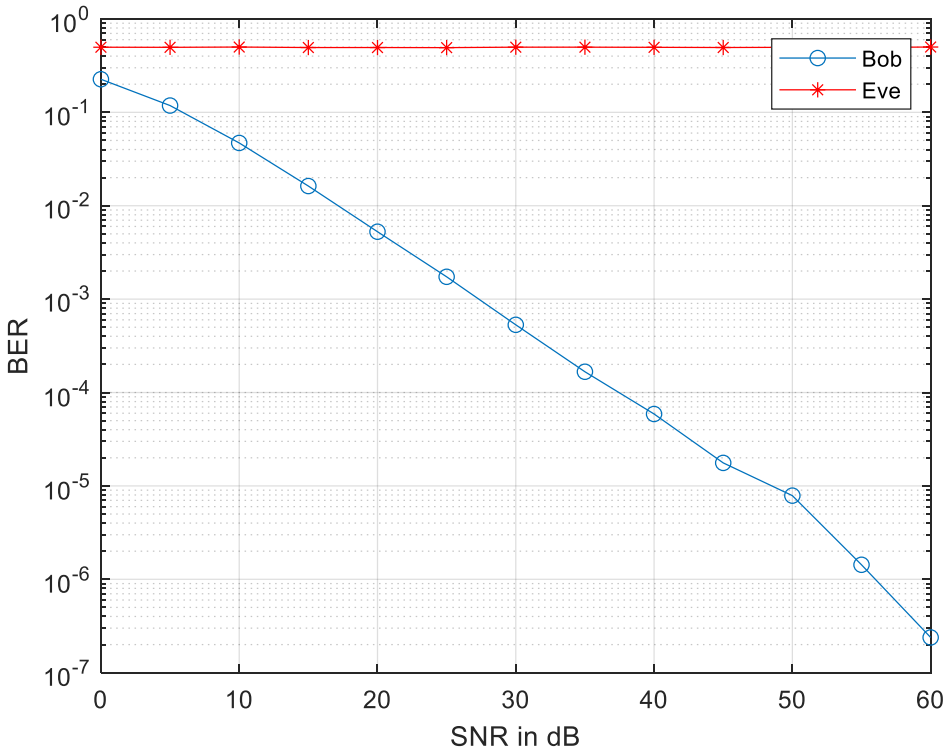
256 subcarriers		
Εύρος ζώνης (Bandwidth) = 3,5 MHz		
Η συχνότητα του carrier f = 3450 MHz ή 3450 * 10^6 Hz		
Η απόσταση μεταξύ των καναλιών Δf	0,015625	MHz ή 15,625 kHz
Η διάρκεια του συμβόλου OFDM είναι: T_OFDM = 1/Δf	0,064	ή 64 μsec
Η διάρκεια του κυκλικού προθέματος T_CP = 1/8 *T_OFDM	8	μsec
Υποθέτουμε ότι έχουμε εξάπλωση καθυστέρησης Δt = 7,5 μsec		
E_b/N_o = 0 dB μέχρι 60 dB με βήμα 5 dB		
c = λc * f (όπου c= 3*10^8 m/sec και f = 3450 *10^6 Hz)	0,086956522	δηλαδή λc= 0,09 m
v= F_D*λc (για v=20 km/h ή 5,55 m/sec και λc= 0,09 m βρίσκουμε το F_D)	61,66666667	δηλαδή F_D= 61,7 Hz
F_T = 2*π*F_D *Δt	0,00290607	
Συμπληρωματική του F_T είναι 1-0,0029 = 0,9971		

Πίνακας 5.2: Αποτελέσματα προσομοίωσης QPSK (ταχύτητα 20 km/h)

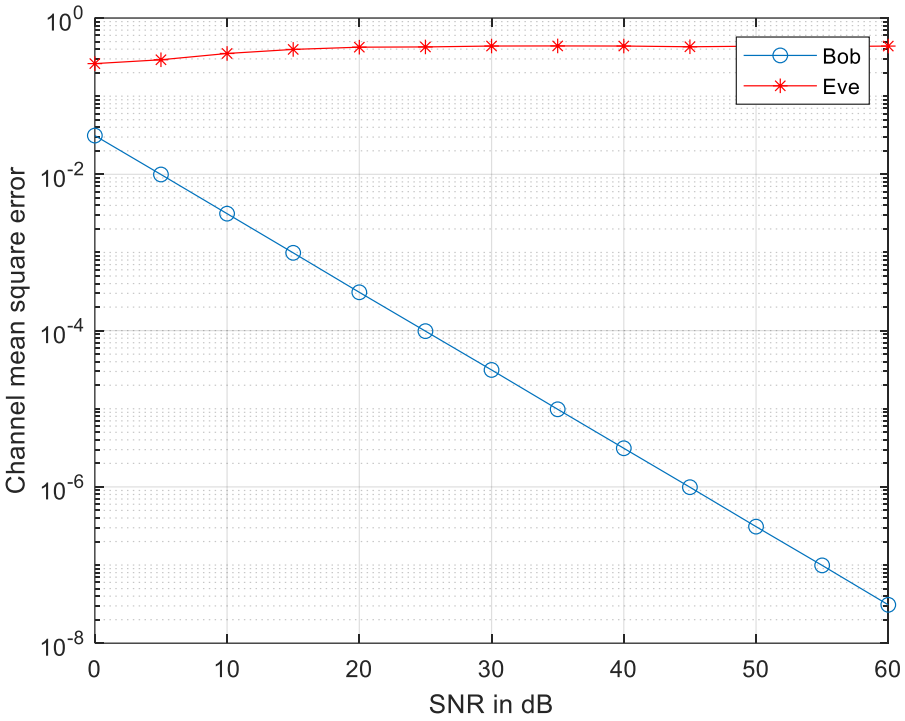
SNR	BER_Bob	BER_Eve	ch_mse (Bob)	che_mse (Eve)
0	0,226114273	0,498007774	0,125320343	1,044680035
5	0,118266821	0,496880054	0,039809692	1,1697719
10	0,047021389	0,500254154	0,012548424	1,408124227
15	0,016249895	0,49434495	0,003958539	1,586838212
20	0,005268812	0,494142771	0,001237432	1,695060441
25	0,001734018	0,492940426	0,000393841	1,707809767
30	0,000530958	0,498539209	0,00012549	1,753897521
35	0,000166893	0,498727798	0,000039388	1,758463519
40	0,000058889	0,496805668	0,000012486	1,753585099
45	0,000017643	0,494473219	3,9655E-06	1,716586443
50	7,8678E-06	0,49684	1,2407E-06	1,746365509
55	1,4305E-06	0,494959354	3,9598E-07	1,723238671
60	2,3842E-07	0,50055337	1,239E-07	1,750885801



Εικόνα 5.2: Διάγραμμα Αστερισμού για QPSK



Εικόνα 5.3: BER του Bob και Eve σε συνάρτηση με το SNR (20km/h).



Εικόνα 5.4: Μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού σε συνάρτηση με το SNR (20km/h)

Στην εικόνα 5.2 φαίνεται το διάγραμμα αστερισμού της διαμόρφωσης QPSK, όπου ο αριθμός των bits 2 που μεταδίδονται από ένα σύμβολο προκύπτει από το τύπο $\log_2 M$, όπου M=4. Επίσης, πρέπει να αναφερθεί ότι το r_0 της συνάρτησης Bessel είναι $r_0 = 2*\pi*f_T = 0.216$.

Από τις εικόνες 5.3 και 5.4 παρατηρούμε ότι το BER του Bob ελαττώνεται όσο αυξάνεται το SNR, ενώ το BER της Eve μένει σταθερό για οποιαδήποτε τιμή του σηματοθορυβικού λόγου προσεγγίζοντας το 0.5 ή (50%). Στην πραγματικότητα η Eve δεν μπορεί να αποδιαμορφώσει το σήμα που λαμβάνει. Ταυτόχρονα, το μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου του καναλιού του Bob μειώνεται και έτσι μπορεί να στείλει περισσότερη πληροφορία με ασφάλεια, ενώ για την Eve παραμένει σταθερή.

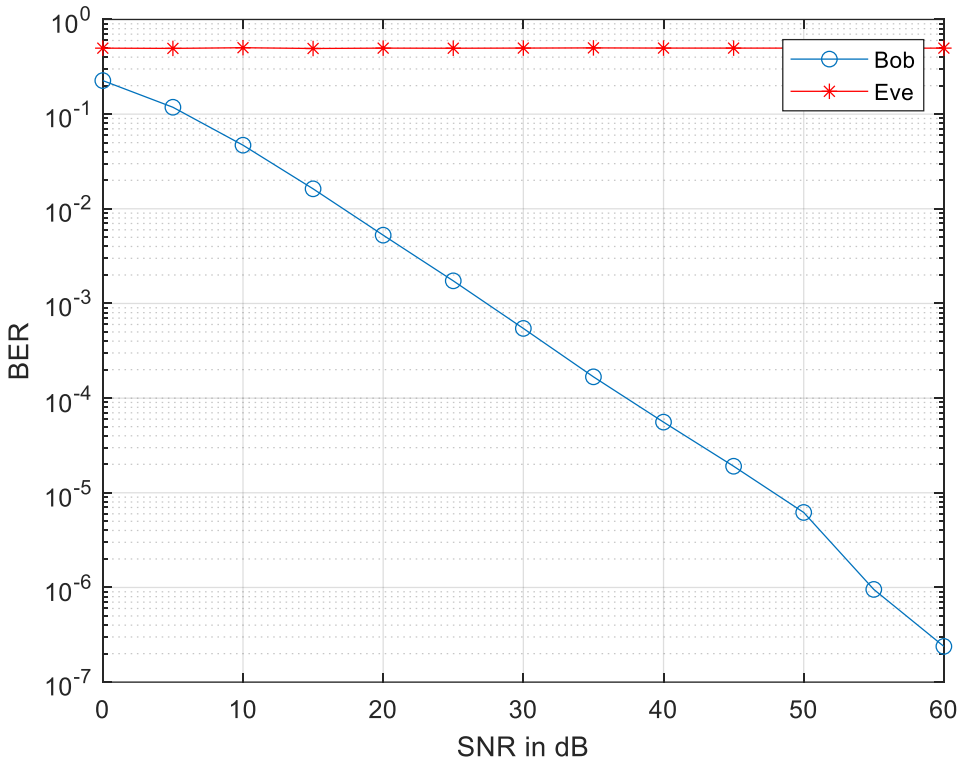
Στη συνέχεια εκτελέστηκε η προσομοίωση για διαμόρφωση QPSK, αλλά με ταχύτητα 40 km/h.

Πίνακας 5.3: Παράμετροι προσομοίωσης για QPSK και 40 km/h

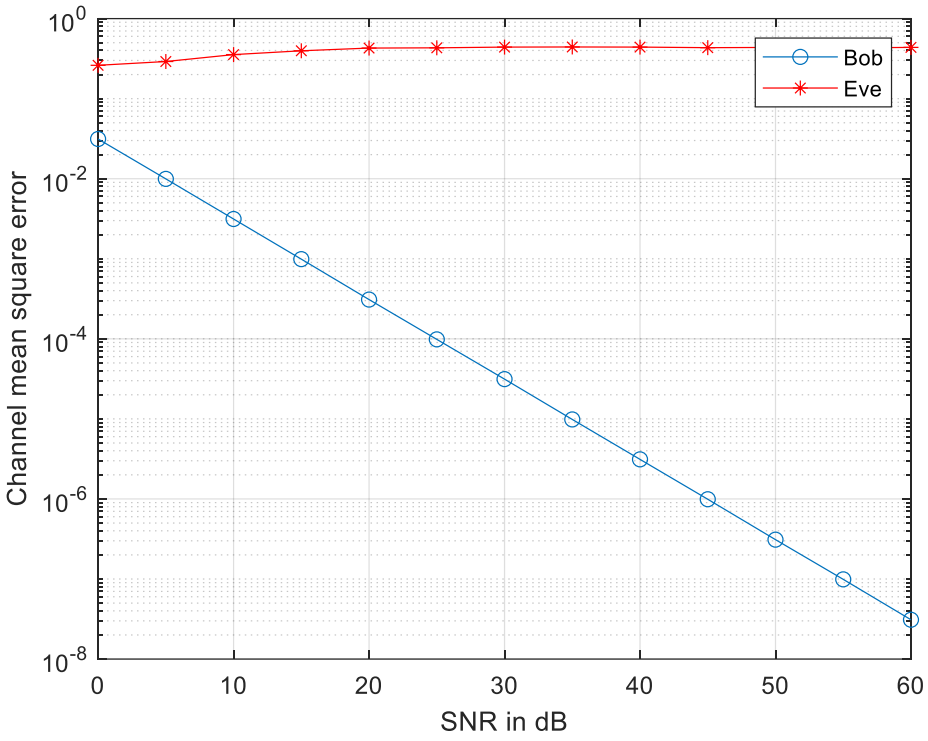
256 subcarriers		
Εύρος ζώνης (Bandwidth) = 3,5 MHz		
Η συχνότητα του carrier f = 3450 MHz ή 3450 * 10^6 Hz		
Η απόσταση μεταξύ των καναλιών Δf	0,015625	MHz ή 15,625 kHz
Η διάρκεια του συμβόλου OFDM είναι: T_OFDM = 1/Δf	0,064	ή 64 μsec
Η διάρκεια του κυκλικού προθέματος T_CP = 1/8 *T_OFDM	8	μsec
Υποθέτουμε ότι έχουμε εξάπλωση καθυστέρησης Δt = 7,5 μsec		
E_b/N_o = 0 dB μέχρι 60 dB με βήμα 5 dB		
c = λc * f (όπου c= 3*10^8 m/sec και f = 3450 *10^6 Hz)	0,086956522	δηλαδή λc= 0,09 m
v= F_D*λc (για v=40 km/h ή 11,11 m/sec και λc= 0,09 m βρίσκουμε το F_D)	123,4444444	δηλαδή F_D= 123,44 Hz
$F_T = 2*\pi*F_D *\Delta t$	0,005814024	
Συμπληρωματική του F_T είναι 1-0,0058 = 0,9942		

Πίνακας 5.4: Αποτελέσματα προσομοίωσης QPSK (ταχύτητα 40 km/h)

SNR	BER_Bob	BER_Eve	ch_mse (Bob)	che_mse (Eve)
0	0,22689867	0,496292114	0,124363025	1,051525433
5	0,117588758	0,50027442	0,039424569	1,194172509
10	0,04715395	0,491928339	0,01236909	1,389669453
15	0,016056061	0,501769543	0,003950361	1,624194242
20	0,0053339	0,501576424	0,001257211	1,713667114
25	0,001746416	0,494216442	0,000392465	1,723131666
30	0,000537872	0,495548248	0,000125027	1,739018661
35	0,000172377	0,495346546	0,000039466	1,73151728
40	0,000045538	0,496205807	0,000012475	1,726824664
45	0,000021696	0,495380163	3,9561E-06	1,722905397
50	5,4836E-06	0,497154474	1,2456E-06	1,729127442
55	1,6689E-06	0,495332956	3,9861E-07	1,734432559
60	4,7684E-07	0,500968933	1,2483E-07	1,74462459



Εικόνα 5.5: BER του Bob και Eve σε συνάρτηση με το SNR (40 km/h)



Εικόνα 5.6: Μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού του Bob και της Eve σε συνάρτηση με το SNR (40 km/h)

Τα αποτελέσματα από τα figure είναι παρόμοια με αυτά της προηγούμενης προσομοίωσης και το r_0 της συνάρτησης Bessel είναι $r_0 = 2*\pi*f_T = 0.212$.

Από τις εικόνες 5.5 και 5.6 παρατηρούμε ότι το BER του Bob ελαττώνεται όσο αυξάνεται το SNR, ενώ το BER της Eve μένει σταθερό για οποιαδήποτε τιμή του σηματοθορυβικού λόγου προσεγγίζοντας το 0.5 ή (50%). Στην πραγματικότητα η Eve δεν μπορεί να αποδιαμορφώσει το σήμα που λαμβάνει. Ταυτόχρονα, το μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου του καναλιού του Bob μειώνεται και έτσι μπορεί να στείλει περισσότερη πληροφορία με ασφάλεια, ενώ για την Eve παραμένει σταθερή.

Στη συνέχεια εκτελέστηκε η προσομοίωση με διαμόρφωση QPSK και για ταχύτητα 80 km/h και τα αποτελέσματα για το BER του Bob και της Eve σε σχέση με το SNR βρέθηκαν παρόμοια με τα προηγούμενα όπως και για το μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου του καναλιού. Το r_0 του Bessel βρέθηκε $r_0 = 0.204$.

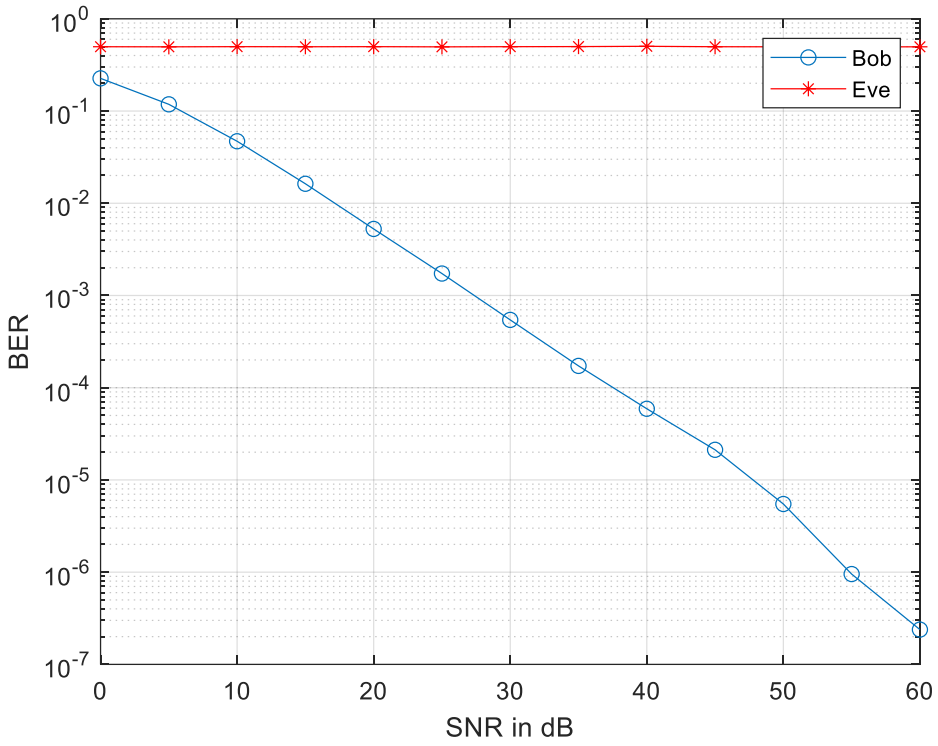
Πίνακας 5.5: Παράμετροι προσομοίωσης για QPSK και 80 km/h

256 subcarriers		
Εύρος ζώνης (Bandwidth) = 3,5 MHz		
Η συχνότητα του carrier f = 3450 MHz ή 3450 * 10^6 Hz		
Η απόσταση μεταξύ των καναλιών Δf	0,015625	MHz ή 15,625 kHz
Η διάρκεια του συμβόλου OFDM είναι: T_OFDM = 1/Δf	0,064	ή 64 μsec
Η διάρκεια του κυκλικού προθέματος T_CP = 1/8 *T_OFDM	8	μsec
Υποθέτουμε ότι έχουμε εξάπλωση καθυστέρησης Δt = 7,5 μsec		
E_b/N_o = 0 dB μέχρι 60 dB με βήμα 5 dB		
c = λc * f (όπου c= 3*10^8 m/sec και f = 3450 *10^6 Hz)	0,086956522	δηλαδή λc= 0,09 m
v= F_D*λc (για v=80 km/h ή 22,22 m/sec και λc= 0,09 m βρίσκουμε το F_D)	246,8888889	δηλαδή F_D= 246,89 Hz
$F_T = 2*\pi*F_D$ *Δt	0,011628519	
Συμπληρωματική του F_T είναι 1-0,0116 = 0,9884		

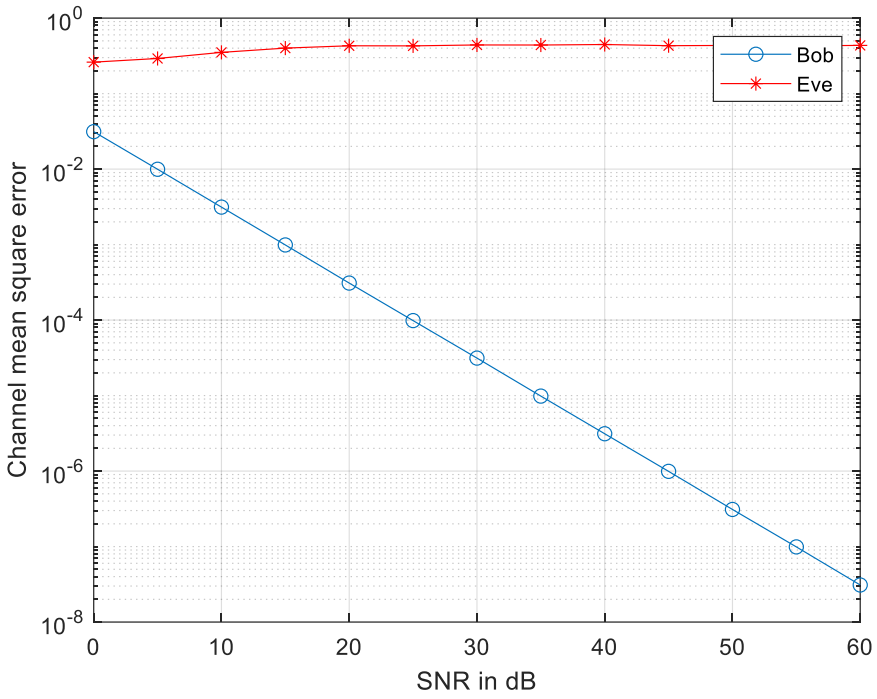
Πίνακας 5.6: Αποτελέσματα προσομοίωσης QPSK (ταχύτητα 80 km/h)

SNR	BER_Bob	BER_Eve	ch_mse (Bob)	che_mse (Eve)
0	0,22845459	0,498481035	0,125769895	1,050556594
5	0,116710663	0,499865532	0,039875562	1,185016155
10	0,047257423	0,501078606	0,012504467	1,419162028
15	0,016137838	0,498038292	0,003942528	1,612034007
20	0,005377531	0,496241331	0,001244454	1,682002643
25	0,001697302	0,495715141	0,000398035	1,732866617
30	0,000566483	0,497291803	0,000124872	1,752965952
35	0,000183821	0,497367382	0,000039613	1,724437633
40	0,000052691	0,499447584	0,00001251	1,754608066

45	0,000017643	0,49386692	3,9641E-06	1,74573067
50	6,1989E-06	0,49413991	1,2515E-06	1,734050729
55	1,1921E-06	0,500855207	3,9404E-07	1,759156178
60	0	0,495416403	1,2437E-07	1,744142524



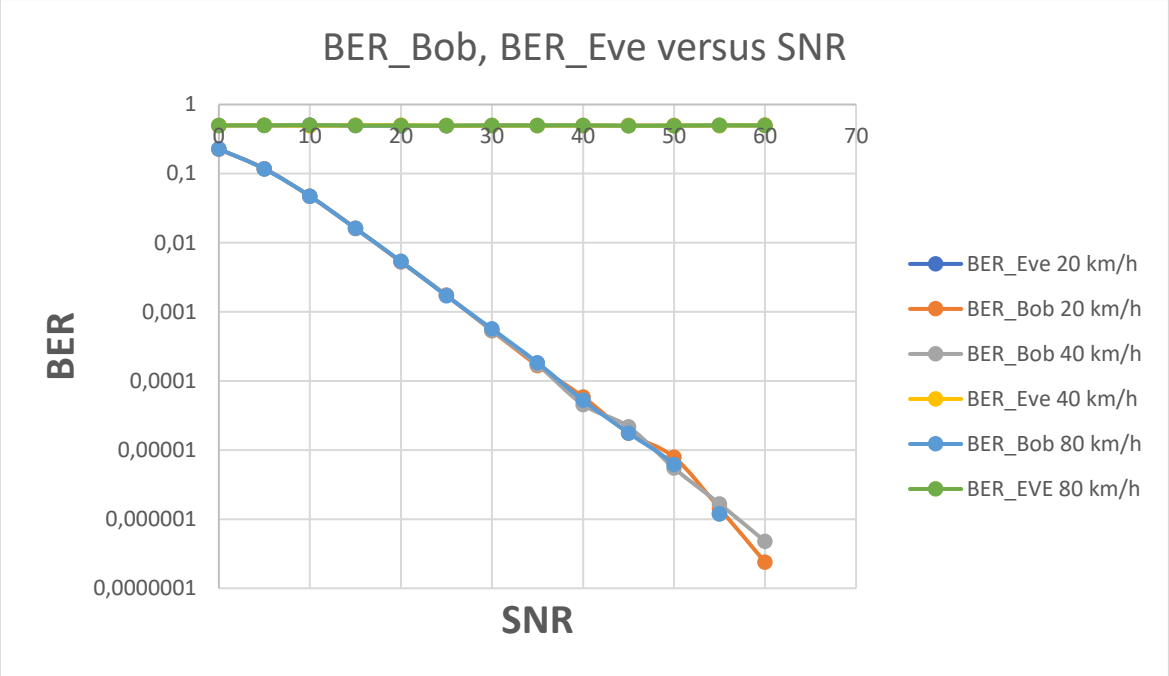
Εικόνα 5.7: BER του Bob και Eve σε συνάρτηση με το SNR (80 km/h)



Εικόνα 5.8: Μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού σε συνάρτηση με το SNR (80 km/h)

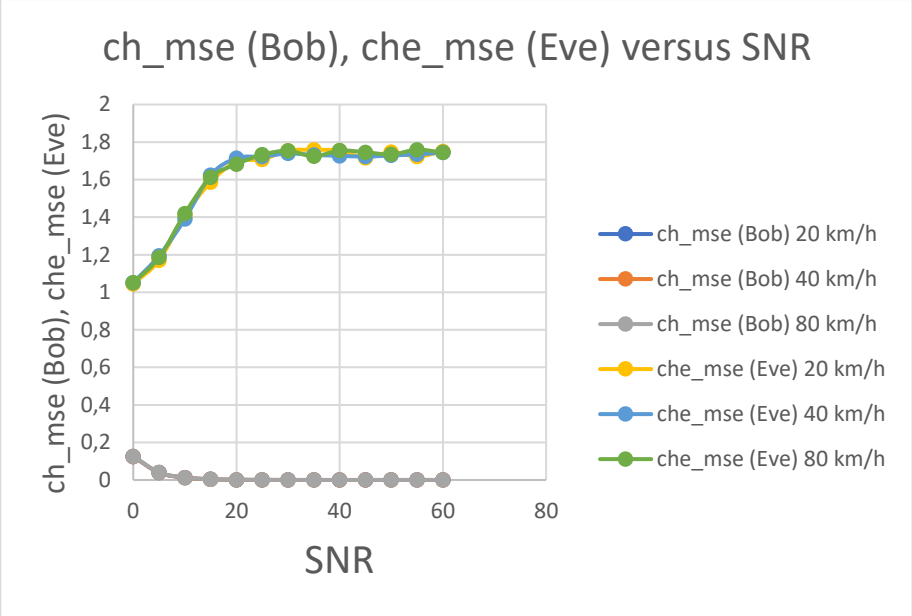
Από τις εικόνες 5.7 και 5.8 παρατηρούμε ότι το BER του Bob ελαττώνεται όσο αυξάνεται το SNR, ενώ το BER της Eve μένει σταθερό για οποιαδήποτε τιμή του σηματοθορυβικού λόγου προσεγγίζοντας το 0.5 ή (50%). Στην πραγματικότητα η Eve δεν μπορεί να αποδιαμορφώσει το σήμα που λαμβάνει. Ταυτόχρονα, το μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου του καναλιού του Bob μειώνεται και έτσι μπορεί να στείλει περισσότερη πληροφορία με ασφάλεια, ενώ για την Eve παραμένει σταθερή.

Με την ολοκλήρωση της προσομοίωσης για διαμόρφωση QPSK, με ταχύτητες 20, 40 και 80 km/h αντίστοιχα δημιουργήθηκαν δύο διαγράμματα με το σύνολο των αποτελεσμάτων. Στην εικόνα 5.9 παρουσιάζεται τα BER του Bob και της Eve σε συνάρτηση με το SNR σε ένα plot, όπου τα αποτελέσματα Bit Error Rate είναι σχεδόν παρόμοια για κάθε προσομοίωση.



Εικόνα 5.9: BER_Bob, BER_Eve versus SNR για QPSK.

Στην εικόνα 5.10 παρουσιάζεται το μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού για τον Bob και την Eve σε συνάρτηση με το σηματοθορυβικό λόγο SNR σε ένα διάγραμμα. Παρατηρούμε ότι για τον Bob σε όλες τις περιπτώσεις αρχίζει με τιμή περίπου στο 0,1 για SNR 0 dB και στη συνέχεια έχει τιμές που πλησιάζουν στο μηδέν, ενώ για την Eve αυξάνεται συνέχεια η τιμής της καθώς ξεκινάει από το 1 και φτάνει μέχρι περίπου το 2. Αυτό το συμπέρασμα επιβεβαιώνει το γεγονός ότι ο δέκτης του ωτακουστή παρουσιάζει μεγαλύτερο ποσοστό σφάλματος bit (BER), σε σύγκριση με τον νόμιμο δέκτη, οπότε ο νόμιμος πομπός μπορεί να στείλει μεγαλύτερο ρυθμό πληροφορίας με ασφάλεια προς τον νόμιμο δέκτη.

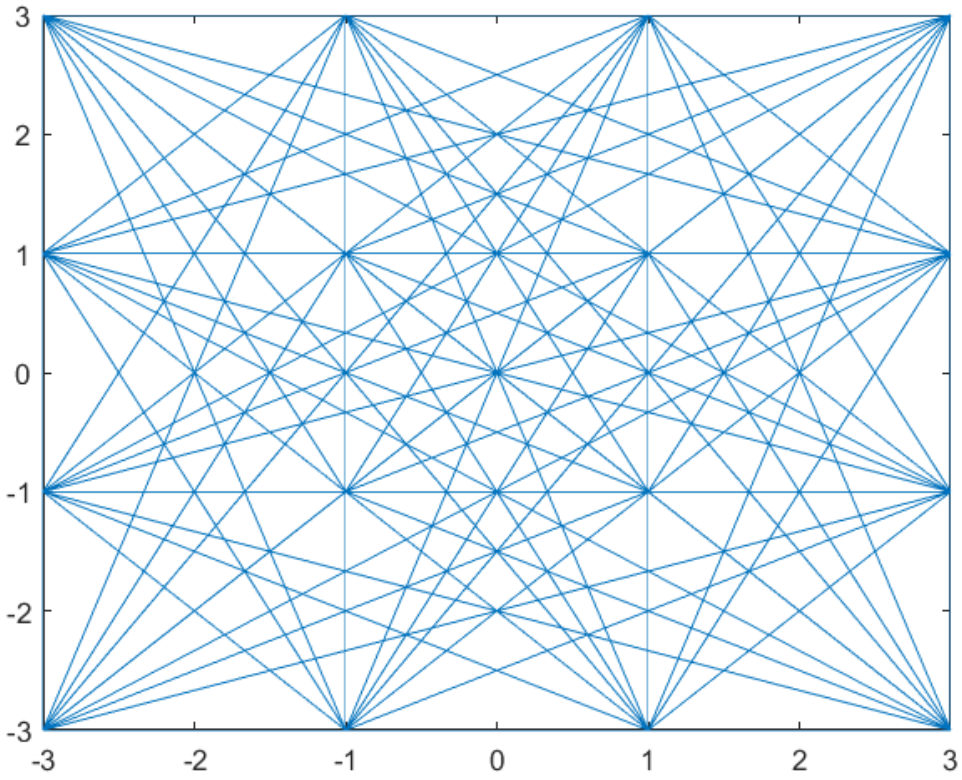


Εικόνα 5.10: Μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού σε συνάρτηση με το SNR για διαμόρφωση QPSK.

Στη συνέχεια εκτελέστηκε προσομοίωση για διαμόρφωση 16-QAM για τις ίδιες ταχύτητες με τη διαμόρφωση QPSK και τα αποτελέσματα ήταν παρόμοια όπως αποδεικνύεται από τις παρακάτω εικόνες. Αρχικά η προσομοίωση υλοποιήθηκε για ταχύτητα 20 km/h.

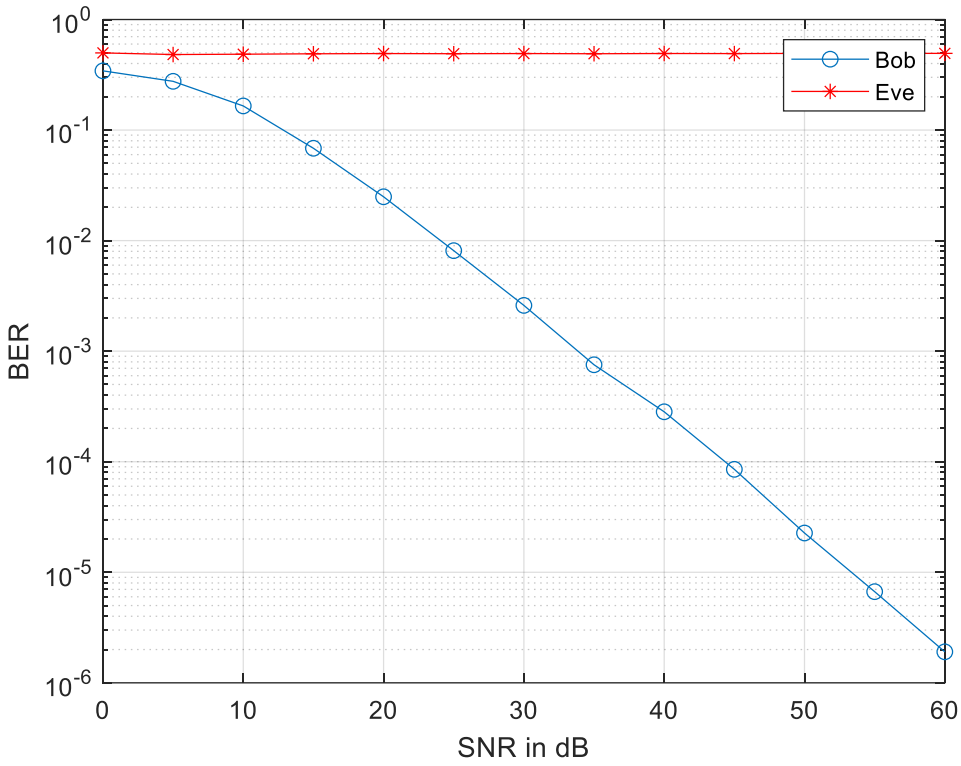
Πίνακας 5.7: Αποτελέσματα προσομοίωσης 16-QAM (ταχύτητα 20 km/h)

SNR	BER_Bob	BER_Eve	ch_mse (Bob)	che_mse (Eve)
0	0,343390226	0,499082327	0,051985961	1,414582382
5	0,275503874	0,483213186	0,016276867	2,633628858
10	0,16361618	0,484309912	0,005202096	4,709786196
15	0,068287611	0,490303755	0,001641319	6,523928127
20	0,024672985	0,490597725	0,000526123	7,14947961
25	0,008253813	0,490921259	0,000165536	7,454080483
30	0,002671957	0,490466356	0,000052262	7,67181589
35	0,000773907	0,492887259	0,000016778	7,78868197
40	0,000259161	0,494203806	0,000005218	7,781697259
45	0,000075817	0,492783546	1,6297E-06	7,741461838
50	0,000026941	0,492006779	5,2569E-07	7,903825204
55	9,7752E-06	0,494276524	1,6767E-07	7,808252378
60	2,6226E-06	0,492219687	5,1796E-08	7,753523563

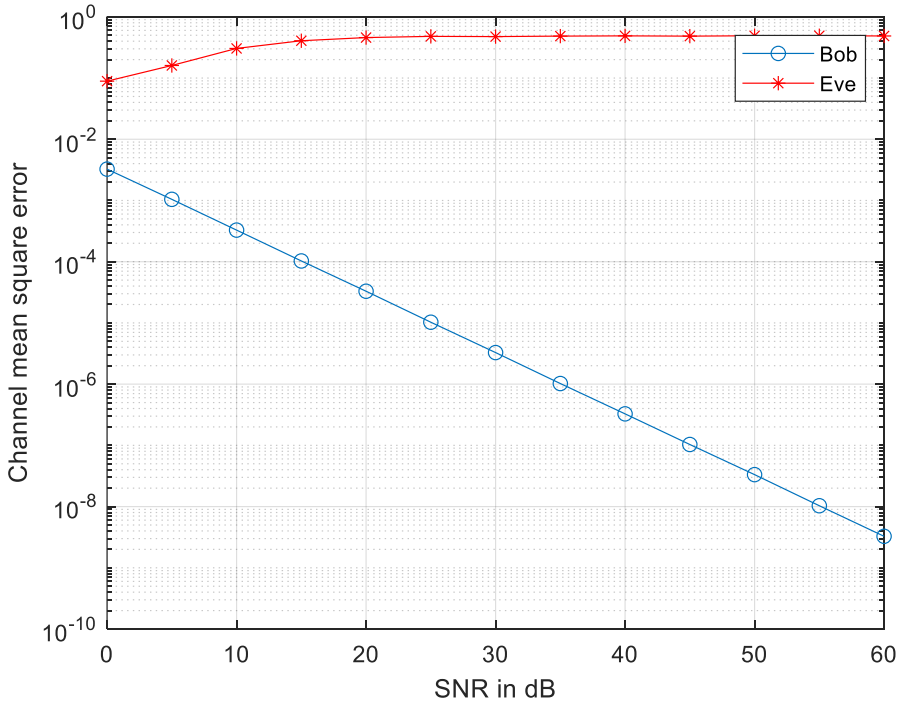


Εικόνα 5.11: Διάγραμμα Αστερισμού για 16-QAM.

Το διάγραμμα αστερισμού σε αυτή τη διαμόρφωση είναι διαφορετικό καθώς με την χρησιμοποίηση του τύπου που έχει αναφερθεί παραπάνω και με το δεδομένο ότι σε διαμόρφωση 16-QAM το M ισούται με 16, προκύπτει από το τύπο $\log_2 M$ ότι ο αριθμός των bits που μεταδίδονται ανά σύμβολο είναι 4.

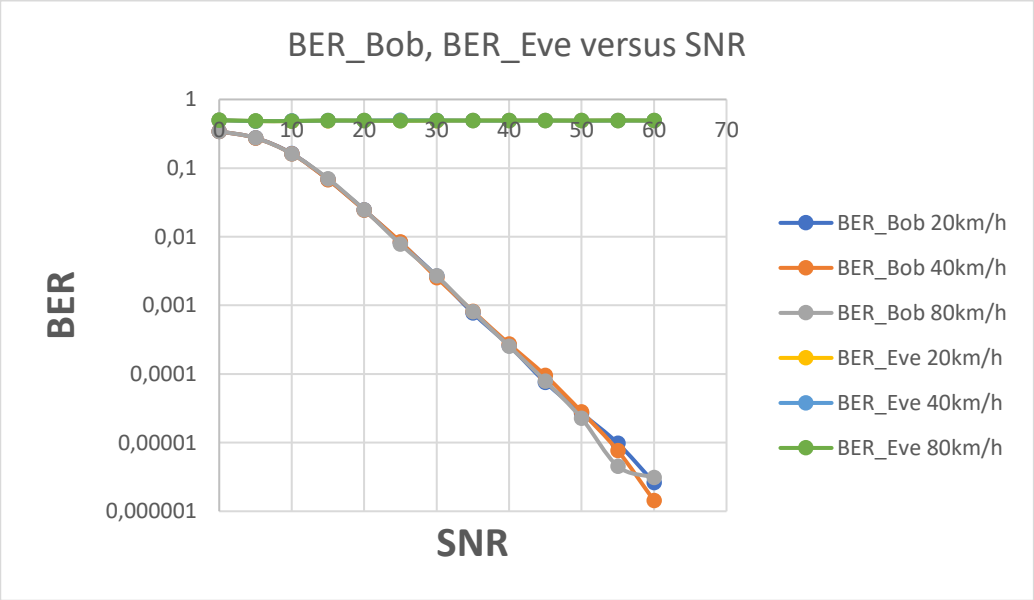


Εικόνα 5.12: BER του Bob και Eve σε συνάρτηση με το SNR (20 km/h)

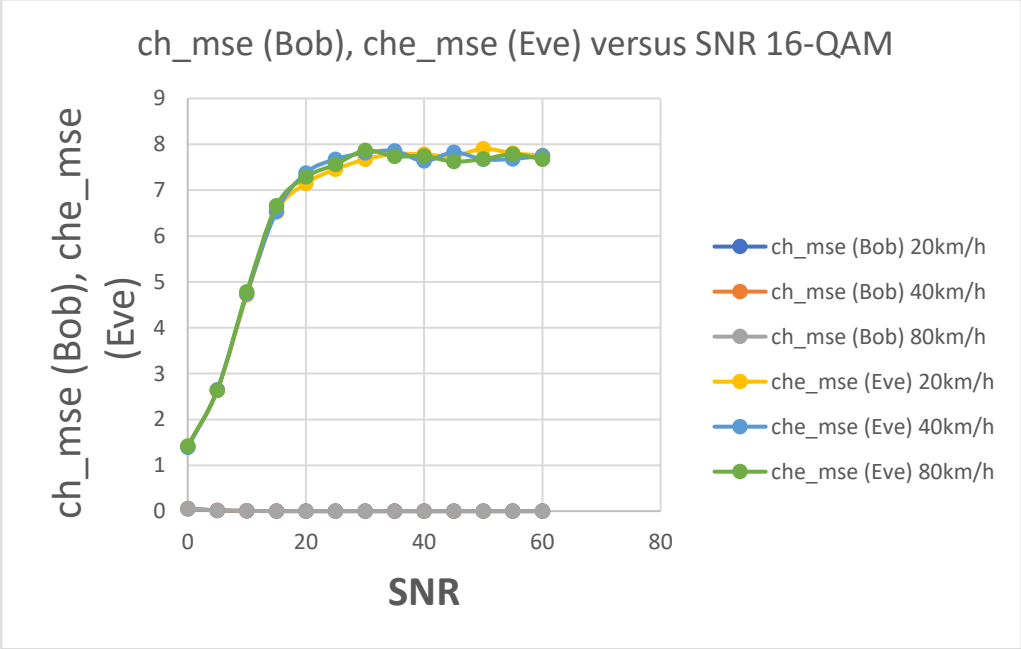


Εικόνα 5.13: Μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού σε συνάρτηση με το SNR για διαμόρφωση 16-QAM (20 km/h)

Η διαδικασία αυτή πραγματοποιήθηκε για τις ταχύτητες των 40 km/h και 80 km/h και τα αποτελέσματα παρουσιάζονται στο παρακάτω κοινό διάγραμμα διαμόρφωσης 16-QAM για το BER του Bob και της Eve σε συνάρτηση με το σηματοθορυβικό λόγο καθώς επίσης το μέσο τετραγωνικό σφάλμα της εκτίμησης του καναλιού για τον Bob και την Eve σε συνάρτηση με το SNR.



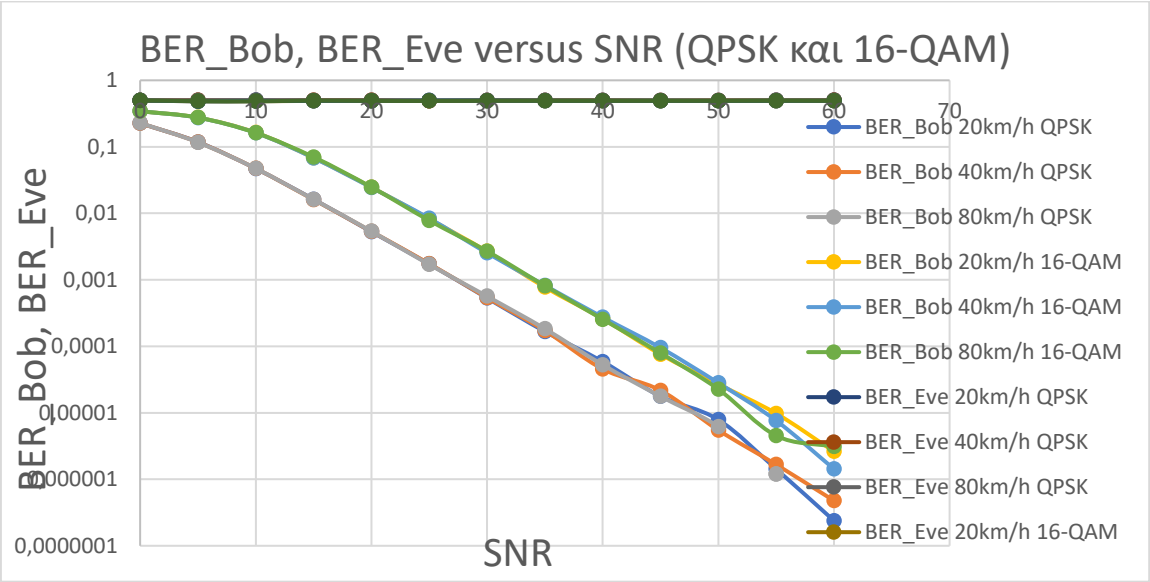
Εικόνα 5.14: BER_Bob, BER_Eve versus SNR για 16-QAM



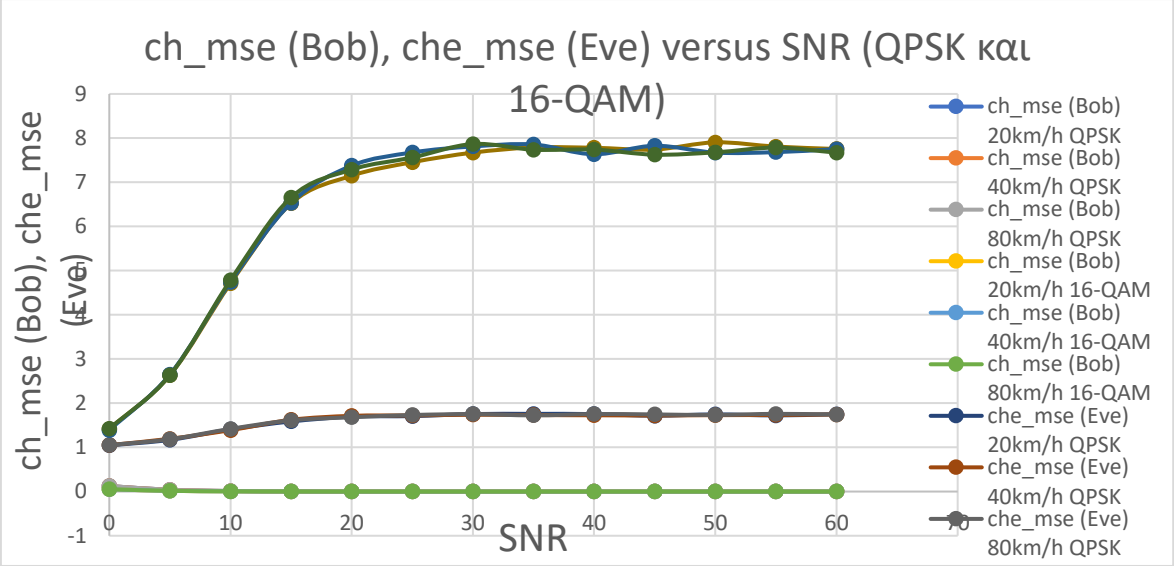
Εικόνα 5.15: Μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού σε συνάρτηση με το SNR για διαμόρφωση 16-QAM.

Παρατηρούμε ότι όπως και στη διαμόρφωση QPSK έτσι και στην 16-QAM το BER του Bob αρχίζει από την τιμή περίπου 0,3 και όσο αυξάνεται το SNR πλησιάζει πολύ κοντά στο μηδέν, σε αντίθεση με την Eve όπου οι τιμές της είναι σταθερά στο 0,5 για όλες τις ταχύτητες όσο μεγάλωνε το SNR προσεγγίζοντας το 0.5 ή (50%). Στην πραγματικότητα η Eve δεν μπορεί να αποδιαμορφώσει το σήμα που λαμβάνει. Παρομοίως και το μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού για τον Bob είναι μόνιμα σε χαμηλές τιμές κοντά στο μηδέν, ενώ ο ωτακουστής, με την αύξηση του σηματοθορυβικού λόγου, αυξάνεται πολύ η τιμή του καθώς αρχίζει από τιμές περίπου στο 1,5 και φτάνει σε πολύ μεγάλες τιμές προσεγγίζοντας το 8.

Τέλος, για την ολοκλήρωση της προσομοίωσης έγιναν δύο διαγράμματα, το πρώτο αφορούσε το Bit Error Rate του Bob και της Eve σε συνάρτηση με το SNR για τη διαμόρφωση QPSK και 16-QAM για ταχύτητες 20, 40 και 80 km/h σε ένα κοινό διάγραμμα, ώστε να επιβεβαιωθεί ότι οι τιμές τους είναι παρόμοιες για οποιαδήποτε από τις δύο διαμορφώσεις, καθώς επίσης και ένα δεύτερο διάγραμμα σύγκρισης ττου μέσου τετραγωνικού σφάλματος της εκτίμησης του ασύρματου καναλιού για τον Bob και την Eve σε σχέση με το SNR. Κάθε διάγραμμα αποτελείται από δώδεκα καμπύλες και περιέχει όλα τα αποτελέσματα που παρουσιάστηκαν παραπάνω σε ένα κοινό διάγραμμα.



Εικόνα 5.16: BER_Bob, BER_Eve versus SNR για QPSK και 16-QAM



Εικόνα 5.17: Μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού σε συνάρτηση με το SNR για διαμόρφωση QPSK και 16-QAM.

6. Συμπεράσματα και Προτάσεις για Επέκταση της Εργασίας

Μέσω της προσομοίωσης μπορούμε να εξάγουμε και να επιβεβαιώσουμε πολύ σημαντικά συμπεράσματα για τον τρόπο συμπεριφοράς του νόμιμου πομπού και δέκτη σε σχέση με τον ωτακουστή. Η προσομοίωση πραγματοποιήθηκε αρκετές φορές, ώστε να επαληθευτούν με ακρίβεια τα αποτελέσματα. Ένα από τα σημαντικά συμπεράσματα είναι το γεγονός ότι ο δέκτης του ωτακουστή παρουσιάζει μεγαλύτερο ποσοστό σφάλματος bit (BER), σε σύγκριση με τον νόμιμο δέκτη, οπότε ο νόμιμος πομπός μπορεί να στείλει μεγαλύτερο ρυθμό πληροφορίας με ασφάλεια προς τον νόμιμο δέκτη. Επίσης, το BER του Bob ελαττώνεται όσο αυξάνεται το SNR, ενώ το BER της Eve μένει σταθερό για οποιαδήποτε τιμή του σηματοθορυβικού λόγου προσεγγίζοντας το 0.5 ή (50%). Στην πραγματικότητα η Eve δεν μπορεί να αποδιαμορφώσει το σήμα που λαμβάνει. Επίσης, το μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου του καναλιού του Bob μειώνεται και έτσι μπορεί να στείλει περισσότερη πληροφορία με ασφάλεια, ενώ για την Eve παραμένει σταθερό σε υψηλότερη τιμή.

Όπως σε κάθε αντικείμενο ενασχόλησης έτσι και εδώ υπάρχουν πολλά περιθώρια για μελλοντικές βελτιώσεις και εξελίξεις. Σε μελλοντική επέκταση της διπλωματικής εργασίας μπορούν να χρησιμοποιηθούν πιο σύνθετες ψηφιακές διαμορφώσεις (32-QAM, 64-QAM), ώστε να εξεταστεί τα αποτελέσματα για τον νόμιμο πομπό σε σχέση με τον ωτακουστή. Επιπλέον, μπορεί να επαληφθεί η προσομοίωση με τη χρήση γρήγορης εξασθένισης/διάλειψης (fast fading) για να παρατηρηθούν οι διαφορές που πιθανώς θα προκύψουν. Επίσης, η εκτίμηση της επίδοσης σε κανάλια γρήγορων Nakagami-m διαλείψεων μέσω προσομοιώσεων, θα έριχνε περισσότερο φως στο θέμα της συμπεριφοράς σε αστικά περιβάλλοντα. Τέλος, θα μπορούσε να πραγματοποιηθεί μία προσομοίωση ενός συστήματος έξυπνης κεραίας σε κανάλι τύπου Rayleigh fading, όπου ο νόμιμος πομπός και ο ωτακουστής θα τοποθετηθούν ομοιοκατευθυντικές κεραίες, ενώ στον νόμιμο δέκτη μια έξυπνη κεραία μεταγωγής λοβών (switched beam).

7. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Ζαχαριουδάκη Δ., Εργασία με τίτλο: «Προστασία Προσωπικών Δεδομένων», Εθνική Σχολή Δημόσιας Διοίκησης, Αθήνα, Ελλάδα, Μάρτιος 2001

[2] Αντώνιος Ι. Καλτσάς, Διπλωματική εργασία με τίτλο: «Ασφάλεια Δικτύων Κινητών Επικοινωνιών : Πρωτόκολλα και Επιθέσεις Ασφάλειας», Αθήνα, Ελλάδα, Ιούνιος 2017

[3] Christof Paar and Jan Pelzl, Understanding cryptography. A textbook for students and practitioners, Foreword by Bart Preneel, 2010

[4] Φίλιππος Χλωρόπουλος, Διπλωματική εργασία με τίτλο: «Βελτιστοποίηση Ασφάλειας Φυσικού Επιπέδου με φιλικούς Παρεμβολείς», Θεσσαλονίκη, Ελλάδα, Μάρτιος 2020

[5] Καραμολέγκου Άννα-Νεφέλη, Διπλωματική εργασία με τίτλο: «Κρυπτογραφία και κρυπτανάλυση από την αρχαιότητα μέχρι σήμερα», Νοέμβριος 2011

[6] Mihir Bellare and Phillip Rogaway, Introduction to Modern Cryptography, University of California, USA, Μάιος 2005

https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf

[7] Dennis Luciano and Gordon D. Prichett. Cryptology: From caesar ciphers to public-key cryptosystems, The College Mathematics Journal, vol. 18, pp. 2-17, Jan. 1987

[8] Simon Blake-Wilson, Information Security, Mathematics, and Public-Key Cryptography, Designs, Codes and Cryptography, vol. 19, pp. 77-99, March 2000

[9] W. Fang, F. Li, Y. Sun, L. Shan, S. Chen, C. Chen and M. Li, "Information Security of PHY Layer in Wireless Networks", Hindawi Journal of Sensors, vol. 2016, Article ID 1230387, 10 pages, 2016. doi:10.1155/2016/1230387

[10] Y. Liu, H.H. Chen, L. Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges", IEEE Communications Surveys & Tutorials, Volume: 19, Issue: 1, First Quarter 2017, pp. 347 – 376

[11] A. Mukherjee, S. Ali, A. Fakoorian, J.Huang, A.L. Swindlehurst "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey", IEEE Communications Surveys & Tutorials, Volume: 16, Issue: 3, Third Quarter 2014, pp. 1550 - 1573

[12] G. R. Tsouri and D. Wulich, “Securing OFDM over Wireless Time-Varying Channels Using Subcarrier Overloading with Joint Signal Constellations,” EURASIP Journal on Wireless Communications and Networking - Special issue on wireless physical layer security, vol. 2009, no. 1, p. 18, Mar. 2009, doi: 10.1155/2009/437824, Article ID: 437824

[13] N. Romero-Zurita, M. Ghogho, and D. McLernon, A. Swami “PHY Layer Security Based on Protected Zone and Artificial Noise” IEEE Signal Processing Letters, Volume: 20, Issue: 5, May 2013, pp. 487 – 490

[14] J. Zhu, R. Schober, V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems", IEEE Trans. Wireless Commun., vol. 15, no. 3, pp. 2245-2261, Mar. 2016

[15] Δαγτόγλου Π., “Ατομικά Δικαιώματα”, Συνταγματικό Δίκαιο, τεύχος. Β’, Αθήνα, Ελλάδα, 1991

[16] Rysavy Research, Mobile Broadband Transformation LTE to 5G, USA, August 2016

[17] Rysavy Research, Security Requirements for Wireless Networking, (2007)

[18] Y. Shiu, S. Y. Chang, H. Wu, S. C. Huang, and H. Chen, Physical layer security in wireless networks: a tutorial, IEEE Wireless Communications, vol. 18, pp. 66–74, April 2011

[19] Hemanta Kumar Kalita and Avijit Kar, Wireless Sensor Network Security Analysis, Next-Generation Networks, vol. 1, pp. 1-10, December 2009

[20] Γιαννακοπούλου Αναστασία, Πτυχιακή Εργασία «Διαχείριση ασφάλειας σε δίκτυα τοπικών ασύρματων επικοινωνιών για το πρότυπο IEEE 802.11», 2012

[21] Παντελή Χαράλαμπος, Διπλωματική Εργασία «ΕΠΙΘΕΣΕΙΣ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΑΙΣΘΗΤΗΡΩΝ ΣΤΟ ΠΡΩΤΟΚΟΛΛΟ RPL», Κύπρος, Μάιος 2015

[22] Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu, Security in Wireless Local Area Networks, Computer and Network SecuritySecurity in Distributed and Networking Systems, pp. 393-419, Florida 2007

[23] Vishal Rathod and Mrudang Mehta, Security in Wireless Sensor Network: A survey, Ganpat Univerity Journal of Engineering and Technology, vol. 1, pp. 35-44, January-June 2011

[24] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, Spins: security protocols for sensor networks, Wireless Networking, vol. 8, pp. 521–534, September 2002

[25] D. W. Carman, P. S. Krus, and B. J. Matt, Constraints and approaches for distributed sensor network security, September 2000

[26] Llanos Tobarra, Diego Cazorlaand and Fernando Cuartero, Formal Analysis of Sensor Network Encryption Protocol, Wireless Networks, Pisa, Italy, October 2007

[27] John A. Stankovic, Wireless Sensor Networks, University of Virginia, June 2006

[28] Bhavya Daya, Network Security: History, Importance, and Future, University of Florida

[29] A Beginner's Guide to Network Security, Cisco Systems, 2001

[30] William Stallings, Cryptography and Network Security Principles and Practise, 5th Edition, 2011

[31] Dr. James H. Yu & Mr. Tom K. Le, Internet and Network Security, 2001

[32] C. E. Shannon, A mathematical theory of communication, The Bell System Technical Journal, vol. 27, pp. 379–423, July 1948

[33] A. D. Wyner, The wire-tap channel, The Bell System Technical Journal, vol. 54, pp. 1355–1387, Oct. 1975

[34] Ueli Maurer and Stefan Wolf, Information-theoretic key agreement: From weak to strong secrecy for free, In Bart Preneel, editor, Advances in Cryptology — EUROCRYPT 2000, pp. 351–368, Berlin, Heidelberg, 2000

[35] Dimitrios Efstathiou, A COLLABORATIVE SECURITY SCHEME FOR OFDM BASED SYSTEMS, Technological Educational Institute (TEI) of Central Macedonia, Σέρρες

[36] S. Leung-Yan-Cheong and M. Hellman, The gaussian wire-tap channel. IEEE Transactions on Information Theory, vol. 24, pp. 451–456, July 1978

[37] Yushi Shen and Ed Martinez, Channel Estimation in OFDM Systems, January 2006

[38] Καφεντζής Βασίλειος, Διπλωματική εργασία με τίτλο «Μελέτη της επίδοσης του OFDM σε ασύρματα κανάλια», 2011

[39] Παπαγεωργίου Μιχαήλ Διπλωματική εργασία με τίτλο «ΤΕΧΝΟΛΟΓΙΚΗ ΕΞΕΛΙΞΗ ΤΗΣ ΑΝΑΛΟΓΙΚΗΣ ΤΗΛΕΟΡΑΣΗΣ ΣΕ ΨΗΦΙΑΚΗ ΚΑΙ ΠΡΟΟΠΤΙΚΕΣ ΜΕΤΑΒΑΣΗΣ ΜΕ ΚΑΙΝΟΤΟΜΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΓΙΑ ΤΟ ΜΕΛΛΟΝ», 2016

[40] Δημήτρης Παπατσώρης, Τηλεπικοινωνιακά Συστήματα ΙΙ, Technological Educational Institute (TEI) of Central Macedonia, Σέρρες, Ελλάδα, Μάιος 2022