ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Τεχνικές Βελτιστοποίησης Ασφάλειας Φυσικού Στρώματος στα Ασύρματα Συστήματα Επικοινωνιών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κόσσυφας Πολύκαρπος

Επιβλέπων : Αθανάσιος Δ. Παναγόπουλος
Επίκουρος Καθηγητής Ε.Μ.Π.

Αθήνα, Ιανουάριος 2016

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Τεχνικές Βελτιστοποίησης Ασφάλειας Φυσικού Στρώματος στα Ασύρματα Συστήματα Επικοινωνιών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κόσσυφας Πολύκαρπος

Επιβλέπων : Αθανάσιος Δ. Παναγόπουλος
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 15η Ιανουαρίου 2016.

.....	.....	.....
Αθανάσιος Δ. Παναγόπουλος	Παναγιώτης Κωττής	Χρήστος Καψάλης
Επικ. Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Ιανουάριος 2016

.....

Κόσσυφας Πολύκαρπος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Οι ασύρματες επικοινωνίες αποτελούν ένα αναπόσπαστο κομμάτι της σύγχρονης κοινωνίας, χρησιμοποιούμενες ευρέως στην καθημερινότητα αλλά και σε στρατιωτικές εφαρμογές. Δεδομένου ότι η πλειοψηφία των ανθρώπων βασίζεται στις ασύρματες επικοινωνίες για τη μετάδοση σημαντικών και ιδιωτικών δεδομένων, η ασφάλεια των ασύρματων επικοινωνιών καθίσταται ως ένας τομέας κριτικής σημασίας με πολλές προκλήσεις για τους μηχανικούς. Παραδοσιακά, η ασφάλεια θεωρείται ως ένα ανεξάρτητο χαρακτηριστικό το οποίο τοποθετείται στα ανώτερα του φυσικού στρώματος επίπεδα, ενώ όλα τα ευρέως χρησιμοποιούμενα κρυπτογραφικά πρωτόκολλα σχεδιάζονται και εφαρμόζονται χωρίς να λαμβάνουν υπόψη τις ιδιαιτερότητες του ασύρματου μέσου μετάδοσης. Στο πλαίσιο αυτό, αναδύεται ο τομέας της ασφάλειας φυσικού στρώματος, όπου έρχεται να ενισχύσει ακόμη περισσότερο την ασφάλεια των επικοινωνιών, λειτουργώντας συμπληρωματικά ή αυτοτελώς από μία κλασική μέθοδο κρυπτογραφίας ανωτέρου επιπέδου. Η παρούσα διπλωματική εργασία, λοιπόν, πραγματεύεται το θέμα της ασφάλειας φυσικού στρώματος στις ασύρματες επικοινωνίες. Αρχικά, παρέχεται στον αναγνώστη το βασικό θεωρητικό υπόβαθρο από τις ασύρματες επικοινωνίες αλλά και την ασφάλεια σε αυτές ώστε να καταστεί ευκολότερη η μελέτη της εργασίας αυτής. Στη συνέχεια, παρουσιάζονται οι βασικές έννοιες της ασφάλειας στο φυσικό στρώμα, με σημαντικότερη εξ αυτών τη χωρητικότητα ασφαλείας, και διερευνάται η επίδραση των χαρακτηριστικών του ασύρματου καναλιού σε αυτήν. Το κύριο μέρος της εργασίας μελετά τη βελτιστοποίηση της χωρητικότητας ασφαλείας μέσω της διαχείρισης της ισχύος μετάδοσης. Επιπρόσθετα, η εργασία ασχολείται με τη διασφάλιση ασφαλούς ασύρματης επικοινωνίας διαμέσου της εφαρμογής τεχνικών που βασίζονται στη συνεργασία μεταξύ διαφορετικών χρηστών του δικτύου και αναλύεται μία συγκεκριμένη συνεργατική τεχνική ασφαλείας φυσικού στρώματος. Τέλος, για την εξαγωγή πειραματικών αποτελεσμάτων πραγματοποιήθηκαν προσομοιώσεις με τη χρήση της γλώσσας προγραμματισμού Matlab.

Λέξεις κλειδιά: ασύρματες επικοινωνίες, ασφάλεια, φυσικό στρώμα, πληροφοριοθεωρητική ασφάλεια, χωρητικότητα ασφαλείας, κανάλι υποκλοπής, διαχείριση πόρων, αναμεταδότες, συνεργατικά δίκτυα

Abstract

Wireless communications have become an integral part of modern-day society, widely used in civilian and military applications. Since the majority of people rely heavily on wireless networks for transmission of important and private data, security in wireless communications is a critical domain with many challenges for engineers. Traditionally, security is viewed as an independent feature addressed above the physical layer, while all widely used cryptographic protocols are designed and implemented without taking into consideration the physical characteristics of the wireless medium. In this regard, physical layer security is emerging as a promising paradigm designed for improving the security of wireless transmissions, as a complementary or independent solution to a conventional cryptographic upper layer technique. Therefore, this thesis addresses the issue of the physical layer security in wireless communications. Firstly, the basic theoretical background of wireless communications and wireless security is provided to the reader in order to facilitate the comprehension of this thesis. Moreover, the principles of physical layer security are being presented -where secrecy capacity is considered to be as the basic notion- and the impact of the broadcast characteristic of the wireless channel is investigated. The main part of the study is devoted to optimizing security capacity through power management at the transmitter. Furthermore, the work deals with ensuring secure wireless communication by applying techniques based on cooperation between different users of the network and a cooperative technique is employed. Finally, as a benchmark, the Matlab programming language was used to perform simulations.

Keywords: wireless communications, security, physical layer, information-theoretic security, secrecy capacity, wiretap channel, resource management, relays, cooperative networks

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου, κ. Αθανάσιο Παναγόπουλο, για την εμπιστοσύνη που μου έδειξε και την ανάθεση του συγκεκριμένου, πολύ ενδιαφέροντος, θέματος διπλωματικής.

Επιπλέον, θα ήθελα να εκφράσω τις ιδιαίτερες ευχαριστίες μου στον διδάκτορα Πουλάκη Μάριο, για τη συνεχή εποπτεία και ουσιαστική καθοδήγηση καθ' όλη τη διάρκεια εκπόνησης της διπλωματικής μου εργασίας. Οι γνώσεις του και η βοήθεια που μου παρείχε υπήρξαν πολύτιμες για την περάτωσή της.

Τέλος, ευχαριστώ την οικογένειά μου που αποτελεί το στήριγμά μου σε κάθε βήμα της ζωής μου.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

1

ΑΣΥΡΜΑΤΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ

Η ανάπτυξη των τηλεπικοινωνιών τις τελευταίες δεκαετίες είναι ραγδαία. Τηλεπικοινωνιακά συστήματα σχεδιάζονται και κατασκευάζονται συνεχώς έχοντας ως στόχο τη μετάδοση πληροφορίας. Η πληροφορία αυτή μεταφέρεται από θέση σε θέση με τη βοήθεια των τηλεπικοινωνιακών καναλιών. Τα συνηθέστερα τηλεπικοινωνιακά κανάλια είναι ο ελεύθερος χώρος, τα καλώδια ή γραμμές μεταφοράς και οι οπτικές ίνες. Η πληροφορία μεταφέρεται, δηλαδή, είτε ενσύρματα είτε ασύρματα. Οι ενσύρματες επικοινωνίες παρέχουν εξαιρετική ποιότητα επικοινωνίας και είναι λιγότερο ευάλωτες σε επιθέσεις ασφαλείας, ωστόσο τα τελευταία χρόνια σημειώνουν μεγαλύτερη ανάπτυξη οι ασύρματες επικοινωνίες. Οι λόγοι είναι η ταχύτατη, χαμηλού κόστους εγκατάσταση σε σχέση με την εγκατάσταση καλωδίων, γραμμών μεταφοράς, η ευκολία επέκτασης του δικτύου και η εξυπηρέτηση κινητών επικοινωνιών καθώς και η δυσκολία εγκατάστασης σταθερών ενσύρματων ζεύξεων σε απομακρυσμένες περιοχές.

Το συγκεκριμένο κεφάλαιο παρέχει το βασικό θεωρητικό υπόβαθρο σχετικά με τις ασύρματες επικοινωνίες, εστιάζοντας στο ασύρματο κανάλι και τους αναμεταδότες, καθώς αποτελούν βάση για τα επόμενα Κεφάλαια της συγκεκριμένης Διπλωματικής Εργασίας. Αρχικά, αναλύεται το ασύρματο κανάλι και τα επιμέρους φαινόμενα που το απαρτίζουν. Στη συνέχεια, γίνεται μία σύντομη αναφορά στην κατηγοριοποίηση των ασύρματων συστημάτων και τέλος, παρουσιάζονται τα συνεργατικά δίκτυα και συγκεκριμένα οι αναμεταδότες και τα συνήθη πρωτόκολλα που χρησιμοποιούνται.

1.1 Το Ασύρματο Κανάλι

Το ασύρματο κανάλι είναι το μέσο μετάδοσης ενός ασύρματου τηλεπικοινωνιακού συστήματος. Πιο συγκεκριμένα, το ασύρματο μέσο διάδοσης είναι ο ελεύθερος χώρος. Ως

γνωστόν, κατά την επικοινωνία μεταξύ ενός πομπού και ενός δέκτη, ηλεκτρική ενέργεια μετατρέπεται μέσω της κεραίας του πομπού σε ηλεκτρομαγνητική ενέργεια και ακτινοβολείται στον ελεύθερο χώρο. Όταν το ηλεκτρομαγνητικό κύμα φτάσει στην κεραία του δέκτη τότε μετατρέπεται μέσω αυτής σε ηλεκτρική ενέργεια. Τα ηλεκτρομαγνητικά κύματα των ασύρματων επικοινωνιών περιλαμβάνουν τις συχνότητες από 3 kHz έως 300 GHz (ραδιοσυχνότητες) και ονομάζονται ραδιοκύματα.

Η διάδοση των ηλεκτρομαγνητικών κυμάτων μέσω του ελεύθερου χώρου γίνεται με διάφορους τρόπους: είτε με ζεύξη οπτικής επαφής (Line of Sight – LoS) είτε όταν δεν υφίσταται οπτική επαφή (Non-Line of Sight – NLoS), λόγω παρεμβολής εμποδίων, μέσω των φαινομένων της ανάκλασης, περίθλασης και σκέδασης.

Ανάκλαση (reflection): Είναι το φαινόμενο το οποίο παρουσιάζεται όταν ένα διαδιδόμενο ηλεκτρομαγνητικό κύμα προσπίπτει σε εμπόδιο με διαστάσεις πολύ μεγαλύτερες σε σχέση με το μήκος κύματός του. Το φαινόμενο αυτό επικρατεί κυρίως σε περιβάλλοντα εσωτερικού χώρου.

Περίθλαση (diffraction): Το φαινόμενο της περίθλασης εμφανίζεται όταν στη ζεύξη παρεμβάλλονται εμπόδια, όπως ανωμαλίες του εδάφους (βουνά, λόφοι), κτίρια, ακόμη και η καμπυλότητα της γης κ.α. Στην περίπτωση αυτή, δημιουργούνται δευτερεύουσες πηγές ακτινοβολίας επί της επιφάνειας των εμποδίων (σύμφωνα με την αρχή του Huygens) και έτσι επιτυγχάνεται διάδοση σε περιοχές όπου δεν υπάρχει οπτική επαφή μεταξύ πομπού και δέκτη.

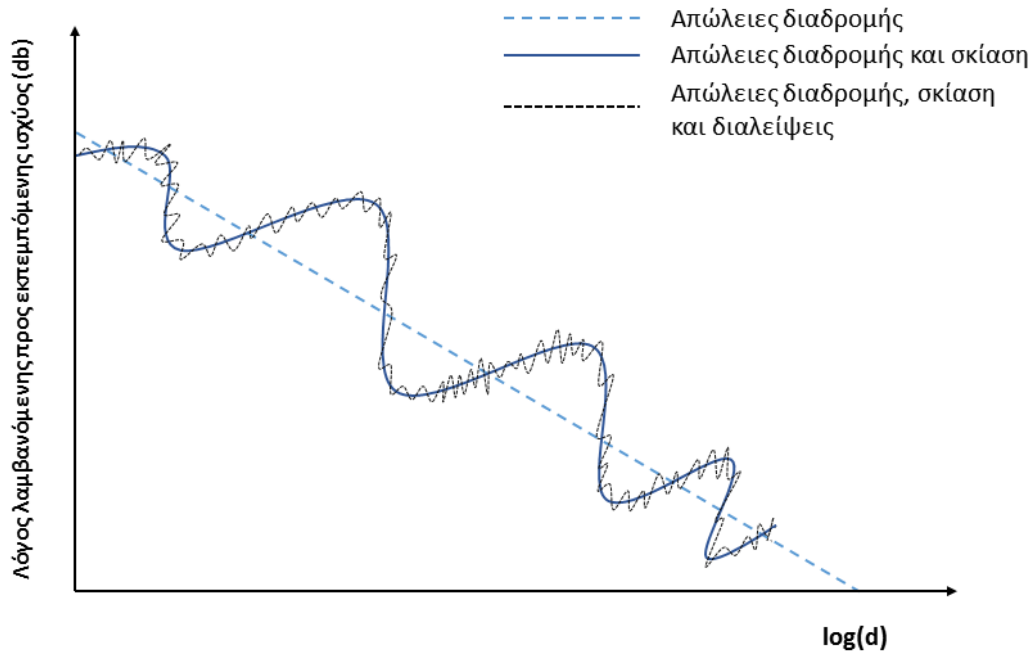
Σκέδαση (scattering): Σκέδαση συμβαίνει όταν κατά τη διεύθυνση διάδοσης υπάρχουν πολλά αντικείμενα μικρών διαστάσεων σε σχέση με το μήκος κύματος της ακτινοβολίας. Τα αντικείμενα αυτά ονομάζονται σκεδαστές και στην πράξη μπορεί να είναι οι ανωμαλίες του εδάφους, τα κτίρια, η βλάστηση, οι στύλοι στους δρόμους κ.α.

Στην περίπτωση της ζεύξης με οπτική επαφή η διάδοση είναι σχετικά απλή, σε αντίθεση με τη διάδοση μη οπτικής επαφής, όπου λόγω των παραπάνω φαινομένων η διάδοση των ραδιοκυμάτων υπόκειται σε επιπρόσθετες απώλειες διάδοσης. Οι απώλειες διάδοσης διακρίνονται στις απώλειες διάδοσης μεγάλης κλίμακας και στις απώλειες διάδοσης μικρής κλίμακας.

Οι απώλειες διάδοσης μεγάλης κλίμακας χαρακτηρίζουν τις μεταβολές της ισχύος του σήματος κατά μήκος σχετικά μεγάλων αποστάσεων (αρκετά μεγαλύτερες από το μήκος κύματος) πομπού-δέκτη και περιλαμβάνουν την απόσβεση της ισχύος, η οποία για δεδομένη απόσταση μεταξύ πομπού και δέκτη θεωρείται σταθερή και αντιστοιχεί στη μέση απώλεια διάδοσης ή διαδρομής (path loss), και τη μεταβολή της ισχύος λήψης λόγω του φαινομένου της σκίασης (shadowing).

Οι απώλειες διάδοσης μικρής κλίμακας χαρακτηρίζουν τις ταχείες μεταβολές της ισχύος λήψης κατά μήκος μικρών αποστάσεων (λίγα μήκη κύματος) ή κατά την διάρκεια συντόμων χρονικών περιόδων. Οφείλονται κυρίως στο φαινόμενο της πολυδιαδρομικής διάδοσης ή πολλαπλής διόδευσης (multipath), του γεγονότος δηλαδή ότι το λαμβανόμενο σήμα αποτελείται από το άθροισμα των συνιστωσών που προέρχονται από διαφορετικές κατευθύνσεις. Είναι γνωστές σαν διαλείψεις πολλαπλής διόδευσης (multipath fading), διαλείψεις μικρής κλίμακας (small scale fading) ή απλά σαν διαλείψεις (fading).

Στο Σχήμα 1.1 απεικονίζεται σε λογαριθμική κλίμακα η μέση απώλεια διάδοσης μιας ζεύξης πομπού-δέκτη (απώλειες διαδρομής), η αργή μεταβολή λόγω σκίασης και η ταχεία μεταβολή λόγω διαλείψεων συναρτήσει της απόστασης από τον πομπό.



Σχήμα 1.1: Εξάρτηση των απωλειών διαδρομής, της σκίασης και των διαλείψεων από την απόσταση πομπού-δέκτη.

Όπως παρατηρείται, κατά τη σχεδίαση των τηλεπικοινωνιακών συστημάτων πρέπει να ληφθούν υπόψη πολλοί παράγοντες, όπως τα χαρακτηριστικά του περιβάλλοντος μεταξύ πομπού και δέκτη, τα εμπόδια που παρεμβάλλονται, ο καιρός και γενικά οτιδήποτε μπορεί να θεωρηθεί ότι επηρεάζει τη μετάδοση. Για τον χαρακτηρισμό, λοιπόν, του ασύρματου καναλιού έχουν αναπτυχθεί διάφορα μοντέλα, τα οποία ερμηνεύουν τη διάδοση του κύματος και αποτελούν θεμελιώδη εργαλεία για τον σχεδιασμό και την υλοποίηση των τηλεπικοινωνιακών συστημάτων.

Από τη μία πλευρά, υπάρχουν τα μοντέλα καναλιού μεγάλης κλίμακας τα οποία προβλέπουν τη συμπεριφορά του καναλιού για αποστάσεις αρκετά μεγαλύτερες από το μήκος κύματος. Διακρίνονται στα φυσικά ή αναλυτικά μοντέλα και στα εμπειρικά μοντέλα. Τα φυσικά/αναλυτικά μοντέλα βασίζονται στη φυσική θεώρηση των μηχανισμών διάδοσης, λαμβάνοντας υπόψιν τα γεωμετρικά χαρακτηριστικά του περιβάλλοντος διάδοσης, όπως τα κτήρια, η μορφολογία του εδάφους κ.α. Τα εμπειρικά μοντέλα προτείνουν απλές σχέσεις που προκύπτουν μετά από στατιστική επεξεργασία πλήθους πειραματικών δεδομένων. Αν και τα εμπειρικά μοντέλα πλεονεκτούν ως προς την ευκολία χρήσης τους, εφαρμόζονται μόνο εφόσον ικανοποιούνται συγκεκριμένες συνθήκες, παρόμοιες με αυτές για τις οποίες αναπτύχθηκαν. Αντίθετα, τα φυσικά μοντέλα χαρακτηρίζονται από πολυπλοκότητα αλλά και υψηλότερη αξιοπιστία σε μεγαλύτερη ποικιλία συνθηκών διάδοσης.

Από την άλλη πλευρά, τα μοντέλα καναλιού μικρής κλίμακας είναι κυρίως μαθηματικά μοντέλα, τα οποία προσεγγίζουν τα ασύρματα κανάλια από στατιστικής πλευράς. Αντιμετωπίζουν, δηλαδή, τον συντελεστή καναλιού ή αλλιώς το πλάτος ή κέρδος τάσης του

καναλιού $(g \geq 0)$ ως τυχαία μεταβλητή που ακολουθεί μία συγκεκριμένη στατιστική κατανομή. Έτσι, αναφέρονται στην $f_G(g)$, δηλαδή τη συνάρτηση πυκνότητας πιθανότητας (probability density function – pdf) της μεταβλητής g. Συχνά, επίσης, χρησιμοποιείται το κέρδος ισχύος του καναλιού $h = |g|^2 \geq 0$ και η αντίστοιχη pdf προκύπτει από τον μετασχηματισμό:

$$f_H(h) = \frac{f_G\left(\sqrt{h}\right)}{2\sqrt{h}} \tag{1.1}$$

1.1.1 Απώλειες διαδρομής (path losses)

Οι απώλειες διαδρομής αντιστοιχούν ουσιαστικά στη μέση απώλεια διαδρομής, η οποία αποτελεί ντετερμινιστικό μέγεθος που, εφόσον δεν μεταβάλλονται τα χαρακτηριστικά της ασύρματης ζεύξης, υπολογίζεται μία φορά. Εξαρτώνται από το περιβάλλον διάδοσης του κύματος και από την απόσταση μεταξύ πομπού και δέκτη και εκφράζουν τη βαθμιαία μείωση της μέσης τιμής της περιβάλλουσας του σήματος καθώς αυξάνεται η απόσταση αυτή [1]. Οφείλονται στην επέκταση του μετώπου, την απορρόφηση, τη διασπορά του κύματος κ.α. Το αντίστροφο των απωλειών του καναλιού καλείται κέρδος καναλιού. Οι τιμές του κέρδους καναλιού εκφράζονται ως ανάλογες με τον λόγο της ισχύος λήψης P_R προς την ισχύ εκπομπής P_T σε dB και προστίθενται στο κέρδος του συστήματος (κέρδος ισχύος του καναλιού), το οποίο θα πρέπει να είναι εκφρασμένο και αυτό σε dB. Όταν δεν υπάρχουν απώλειες διαδρομής είναι $P_R = P_T$ και ο λόγος αυτός ισούται με 1, δηλαδή 0dB. Όταν υπάρχουν απώλειες ο λόγος είναι μικρότερος της μονάδας και συνεπώς το κέρδος έχει αρνητικό πρόσημο σε dB.

1.1.1.1 Αναλυτικά μοντέλα απωλειών διαδρομής

Τα συνηθέστερα αναλυτικά μοντέλα υπολογισμού των απωλειών διαδρομής είναι το μοντέλο απωλειών ελευθέρου χώρου, το γενικό μοντέλο απωλειών διάδοσης και το μοντέλο των δύο ακτίνων.

Το μοντέλο απωλειών ελευθέρου χώρου εφαρμόζεται σε ασύρματες ζεύξεις οπτικής επαφής (LoS) και βασίζεται στην εξίσωση Friis:

$$\frac{P_R}{P_T} = G_T G_R \left(\frac{\lambda}{4\pi d}\right)^2 \tag{1.2}$$

όπου G_T, G_R τα κέρδη κεραιών πομπού και δέκτη αντίστοιχα, λ το μήκος κύματος του ηλεκτρομαγνητικού κύματος και d η απόσταση μεταξύ πομπού και δέκτη. Ο παράγοντας $L_{f_s} = (4\pi d / \lambda)^2$ είναι γνωστός και ως απώλειες ελευθέρου χώρου (free space losses). Σε μορφή dB οι απώλειες ελευθέρου χώρου γράφονται υπό τη μορφή:

$$L_{f_s} = 32.45 + 20\log(f_{\text{MHz}}) + 20\log(d_{\text{km}}) \tag{1.3}$$

όπου η συχνότητα f εκφράζεται σε MHz και η απόσταση d σε km.

Παρατηρείται ότι οι απώλειες ελευθέρου χώρου αυξάνουν ανάλογα με το τετράγωνο της απόστασης που διανύει το ραδιοκύμα. Παρόλα αυτά, στις περισσότερες περιπτώσεις των

ασύρματων συστημάτων η απόσβεση αποτελεί συνάρτηση της απόστασης με εκθέτη απωλειών, ο οποίος καθορίζει την κλίση της καμπύλης απόσβεσης, που υπερβαίνει την τιμή του 2. Για τον λόγο αυτό, έχει αναπτυχθεί το γενικό μοντέλο απωλειών διάδοσης το οποίο εφαρμόζεται και σε συστήματα NLoS. Σε αυτό το μοντέλο ο εκθέτης απωλειών εξαρτάται από το περιβάλλον διάδοσης (βλ. Πίνακα 1.1).

Το μοντέλο των δύο ακτίνων βασίζεται στην τεχνική παρακολούθησης ακτίνας (ray tracing), δηλαδή της καταγραφής των ακτινικών διαδρομών από τον πομπό προς τον δέκτη. Στο συγκεκριμένο μοντέλο η διάδοση του σήματος περιγράφεται με μία απευθείας διαδρομή μεταξύ πομπού και δέκτη και μία ανακλώμενη, συνήθως στο έδαφος. Επιπλέον, ορισμένα εμπειρικά μοντέλα που έχουν αναπτυχθεί για τον υπολογισμό των απωλειών διαδρομής είναι το μοντέλο IEEE 802.16 SUI και το μοντέλο COST 231-Hata, τα οποία βασίζονται σε μετρήσεις των χαρακτηριστικών διάδοσης και χρησιμοποιούνται κυρίως για την καταρχήν διαστασιολόγηση αλλά όχι για την λεπτομερή σχεδίαση ενός συστήματος [1].

Περιβάλλον	Εκθέτης απωλειών c
Ελεύθερος χώρος	2
Αστική περιοχή	2.7 - 3.5
Οικία	3
Εσωτερικοί χώροι LoS	1.6 - 1.8
Εσωτερικοί χώροι NLoS	4 – 6

Πίνακας 1.1: Τυπικές τιμές του εκθέτη απωλειών.

1.1.2 Σκίαση (shadowing)

Εκτός από τη βαθμιαία μείωση, η μέση τιμή της περιβάλλουσας του σήματος παρουσιάζει μικρές διακυμάνσεις λόγω της παρεμπόδισης των ραδιοκυμάτων από εμπόδια κατά μήκος της διαδρομής διάδοσης. Επειδή η θέση, το μέγεθος και οι διηλεκτρικές ιδιότητες των εμποδίων αυτών, καθώς και οι μεταβολές των επιφανειών ανάκλασης και της θέσης των σκεδαστών είναι γενικά άγνωστες, η συνολική απώλεια διάδοσης αποτελεί τυχαία μεταβλητή. Το τυχαίο αυτό φαινόμενο, το οποίο αναπαριστά τις τοπικές διακυμάνσεις του καναλιού, καλείται σκίαση και έχει επιβεβαιωθεί πειραματικά σε ασύρματα δίκτυα εσωτερικού και εξωτερικού χώρου ότι ακολουθεί τη λογαριθμοκανονική (log-normal) κατανομή [1]. Για το λόγο αυτό η σκίαση είναι γνωστή και ως λογαριθμοκανονική σκίαση (log-normal shadowing).

1.1.2.1 Κατανομή Lognormal

Τα κανάλια σκίασης, επομένως, χαρακτηρίζονται από την κατανομή Lognormal, τα οποία σε dB ακολουθούν την κανονική κατανομή. Η pdf για το πλάτος του καναλιού δίνεται από την εξής σχέση:

$$f_G(g) = \frac{2\xi}{g\sqrt{2\pi\sigma}} \exp\left[-\frac{(2\xi \ln g - \mu)^2}{2\sigma^2} \right] \qquad (1.4)$$

όπου $\xi = 10/\ln 10$ και μ, σ η μέση τιμή και η τυπική απόκλιση του καναλιού σε dB αντίστοιχα. Από τη σχέση (1.1) προκύπτει η pdf του κέρδους ισχύος του καναλιού:

$$f_{\mathrm{H}}(h) = \frac{\xi}{h\sqrt{2\pi}\sigma} \exp\left[-\frac{(\xi \ln h - \mu)^2}{2\sigma^2} \right] \tag{1.5}$$

Παρατηρείται ότι η λογαριθμοκανονική κατανομή για την περιγραφή της σκίασης χαρακτηρίζεται πλήρως από τη μέση τιμή και την τυπική απόκλιση του συντελεστή καναλιού, οι οποίες τιμές προκύπτουν από μετρήσεις ή εφαρμογή του κατάλληλου εμπειρικού μοντέλου.

Αξίζει να σημειωθεί ότι ο συνδυασμός της απόσβεσης λόγω διάδοσης (απώλειες διαδρομής) και της απόσβεσης λόγω σκίασης περιορίζει σημαντικά τις επιδόσεις των ασυρμάτων δικτύων. Αυτό συμβαίνει διότι προκειμένου ένα σύστημα να θεωρείται ότι λειτουργεί σωστά, θα πρέπει η ισχύς λήψης P_R να μην γίνει χαμηλότερη από ένα κατώφλι [1]. Η ελάχιστη τιμή αυτή της ισχύος λήψης $P_{R,\min}$ ονομάζεται ευαισθησία του δέκτη. Δεδομένου ότι η σκίαση είναι τυχαία μεταβλητή, η ισχύς λήψης ακολουθεί τη λογαριθμοκανονική κατανομή. Συνεπώς, ορίζεται η πιθανότητα διακοπής ενός συστήματος λόγω απωλειών διάδοσης και σκίασης ως η πιθανότητα η ισχύς λήψης σε κάποια απόσταση να γίνει μικρότερη της ευαισθησίας του δέκτη.

1.1.3 Διαλείψεις (fading)

Με τον όρο διαλείψεις μικρής κλίμακας αναφέρονται οι ταχείες μεταβολές που παρατηρούνται στο πλάτος, τη φάση και τη συχνότητα του σήματος σε αποστάσεις της τάξης του μήκους κύματος ή σε μικρά χρονικά διαστήματα. Οι κυριότεροι φυσικοί παράγοντες που συνδέονται με το φαινόμενο των διαλείψεων είναι η πολυδιαδρομική διάδοση, το φαινόμενο Doppler και το εύρος ζώνης εκπομπής του σήματος:

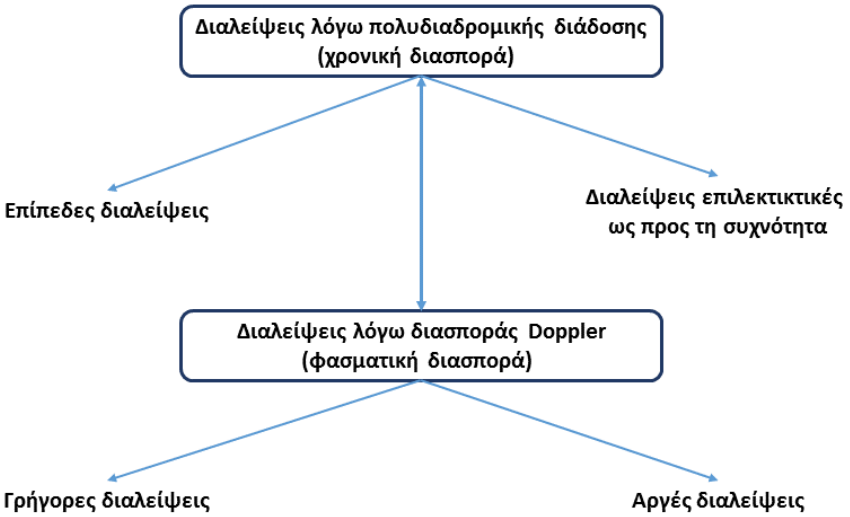
Πολυδιαδρομική διάδοση: Οι μηχανισμοί διάδοσης των κυμάτων (ανάκλαση, περίθλαση, σκέδαση) έχουν σαν αποτέλεσμα τη δημιουργία πολλαπλών εκδοχών του εκπεμπόμενου σήματος, οι οποίες φθάνουν στην κεραία λήψης σε διαφορετικούς χρόνους ακολουθώντας διαφορετικές διαδρομές. Στον δέκτη, επομένως, η υπέρθεση των συνιστωσών αυτών οδηγεί σε αθροιστική ή αφαιρετική συμβολή και έτσι προκύπτουν οι ταχείες μεταβολές στην ισχύ του λαμβανόμενου σήματος για μικρές χωρικές ή χρονικές μετατοπίσεις.

Φαινόμενο Doppler: Εμφανίζεται όταν υπάρχει σχετική κίνηση μεταξύ πομπού και δέκτη ή ακόμη και κινητικότητα των σκεδαστών που υπάρχουν στο περιβάλλον διάδοσης. Προκαλείται, έτσι, μεταβολή της φέρουσας συχνότητας (μετατόπιση ή ολίσθηση Doppler) λόγω του φαινομένου Doppler.

Εύρος ζώνης εκπομπής του σήματος: Εάν το εύρος ζώνης συχνοτήτων του εκπεμπόμενου σήματος υπερβαίνει το εύρος ζώνης του καναλιού, προκαλείται παραμόρφωση στο λαμβανόμενο σήμα, χωρίς ωστόσο η επίδραση των διαλείψεων να είναι τόσο σημαντική.

Οι διαλείψεις μικρής κλίμακας κατηγοριοποιούνται σε τέσσερις διαφορετικούς τύπους διαλείψεων ανάλογα με τους μηχανισμούς που τις προκαλούν (Σχήμα 1.2). Η καθυστέρηση λόγω πολυδιαδρομικής διάδοσης οδηγεί σε χρονική διασπορά, όπου οι διαλείψεις

που προκαλούνται διακρίνονται σε επίπεδες διαλείψεις (flat fading) και διαλείψεις επιλεκτικές ως προς τη συχνότητα (frequency selective fading). Από την άλλη πλευρά, η μετατόπιση Doppler οδηγεί σε φασματική διασπορά, ενώ οι αντίστοιχες διαλείψεις ταξινομούνται σε ταχείες διαλείψεις (fast fading) και αργές διαλείψεις (slow fading). Οι δύο αυτοί μηχανισμοί διαλείψεων είναι ανεξάρτητοι μεταξύ τους και σε αρκετές περιπτώσεις συνυπάρχουν.



Σχήμα 1.2: Τύποι διαλείψεων μικρής κλίμακας

1.1.3.1 Στατιστικά μοντέλα διαλείψεων

Ανάλογα με τη φύση του ασύρματου περιβάλλοντος διάδοσης, υπάρχουν διαφορετικά στατιστικά μοντέλα διαλείψεων μικρής κλίμακας που περιγράφουν τη συμπεριφορά του πλάτους του καναλιού, εκ των οποίων τα πιο συνηθισμένα είναι οι κατανομές Rayleigh, Rice και Nakagami-m [2].

Κατανομή Rayleigh

Η κατανομή Rayleigh χρησιμοποιείται συχνά για να μοντελοποιήσει τα κανάλια πολυδιαδρομικών διαλείψεων σε ζεύξεις NLoS. Οι pdfs για το πλάτος και το κέρδος ισχύος του καναλιού δίνονται αντίστοιχα από τις σχέσεις:

$$f_G(g) = \frac{g}{\sigma^2}\exp\left(-\frac{g^2}{2\sigma^2}\right) \tag{1.6}$$

$$f_H(\mathrm{h}) = \frac{1}{2\sigma^2}\exp\left(-\frac{h}{2\sigma^2}\right) \tag{1.7}$$

όπου το σ προκύπτει από το μέσο κέρδος ισχύος του καναλιού $E[h] = 2\sigma^2$. Παρατηρείται ότι η $f_H(h)$ αντιστοιχεί στην εκθετική κατανομή. Αυτό συμβαίνει διότι η ισχύς είναι ανάλογη του τετραγώνου του πλάτους του καναλιού και αποδεικνύεται ότι όταν μία τυχαία μεταβλητή ακολουθεί την κατανομή Rayleigh, το τετράγωνο της μεταβλητής αυτής ακολουθεί την εκθετική κατανομή.

Κατανομή Rice

Η κατανομή Rice χαρακτηρίζει τα κανάλια πολυδιαδρομικών διαλείψεων σε περιπτώσεις όπου υπάρχει διαδρομή LoS μεταξύ πομπού και δέκτη. Στην κατανομή αυτή οι pdfs για το πλάτος και το κέρδος ισχύος του καναλιού δίνονται αντίστοιχα από τις εξής σχέσεις:

$$f_G(g) = \frac{g}{\sigma^2}\exp\left(-\frac{s^2}{2\sigma^2}-\frac{g^2}{2\sigma^2}\right)I_0\left(\frac{sg}{\sigma^2}\right) \tag{1.8}$$

$$f_H(\mathrm{h}) = \frac{1}{2\sigma^2}\exp\left(-\frac{s^2}{2\sigma^2}-\frac{h}{2\sigma^2}\right)I_0\left(\frac{s\sqrt{h}}{\sigma^2}\right) \tag{1.9}$$

όπου το $I_0(.)$ είναι η τροποποιημένη συνάρτηση Bessel πρώτου είδους μηδενικής τάξης, το s είναι η παράμετρος μη κεντρικότητας και το σ προέρχεται από το μέσο κέρδος ισχύος του καναλιού $E[h]=s^2+2\sigma^2$. Η κατανομή Rice περιγράφεται συχνά με χρήση του παράγοντα Rice $K = s^2/\left(2\sigma^2\right)$. Όταν $K=0$ προκύπτει κανάλι με διαλείψεις Rayleigh (μόνο συνιστώσες NLoS), ενώ όταν $K\to\infty$ προκύπτει κανάλι χωρίς διαλείψεις με μοναδική συνιστώσα τη συνιστώσα LoS. Οι διαλείψεις Rice $\left(K\in(0,\infty)\right)$ εμφανίζουν ηπιότερα χαρακτηριστικά από τις διαλείψεις Rayleigh $\left(K=0\right)$.

Κατανομή Nakagami-m

Η κατανομή Nakagami-m χρησιμοποιείται για τη στατιστική περιγραφή καναλιών πολυδιαδρομικών διαλείψεων όπου οι κατανομές Rayleigh και Rice δεν παρέχουν ικανοποιητική περιγραφή. Η κατανομή Nakagami-m χρησιμοποιεί την παράμετρο m για να μοντελοποιήσει το κανάλι ανάλογα με την ένταση των διαλείψεων. Οι pdfs για το πλάτος και το κέρδος ισχύος του καναλιού δίνονται αντίστοιχα ως εξής:

$$f_G(g) = \frac{2g^{2m-1}}{\beta^m\Gamma(m)}\exp\left(-\frac{g^2}{\beta}\right) \tag{1.10}$$

$$f_H(\mathrm{h}) = \frac{h^{m-1}}{\beta^m\Gamma(m)}\exp\left(-\frac{h}{\beta}\right) \tag{1.11}$$

όπου $\Gamma(\mathrm{x})=\int_0^\infty t^{x-1}e^{-t}dt$ η συνάρτηση Γάμμα, $\beta = E[h]/m$ η παράμετρος κλίμακας και $m\geq 0$ η παράμετρος μορφοποίησης διαλείψεων (fading-shape parameter), η οποία αντιπροσωπεύει την ένταση των διαλείψεων. Πιο συγκεκριμένα, για $m=0.5$ η κατανομή αντιπροσωπεύει κανάλια που εμφανίζουν ισχυρές διαλείψεις, για $m=1$ περιγράφει τα κανάλια Rayleigh, για $m>1$ μπορούν να προσεγγιστούν οι κατανομές Rice και Lognormal, ενώ για $m\to\infty$ η κατανομή περιγράφει τα κανάλια χωρίς πολυδιαδρομικές διαλείψεις, όπως το κανάλι λευκού προσθετικού γκαουσιανού θορύβου (Additive White Gaussian Noise – AWGN). Επομένως, η κατανομή Nakagami-m αποτελεί μία γενικευμένη κατανομή που μπορεί να περιγράψει κανάλια που υποφέρουν από διαλείψεις Rayleigh, διαλείψεις Rice αλλά και από άλλους τύπους διαλείψεων.

1.2 Ασύρματα Συστήματα Επικοινωνιών

Οι ασύρματες τεχνολογίες επικοινωνιών κατηγοριοποιούνται συνήθως ανάλογα με την εμβέλειά τους, την περιοχή δηλαδή που μπορούν να καλύψουν [3]. Με κριτήριο την εμβέλειά τους, λοιπόν, τα ασύρματα δίκτυα διακρίνονται σε:

Ασύρματα προσωπικά δίκτυα (Wireless Personal Area Networks – WPANs): είναι τεχνολογία μικρής εμβέλειας όπου η ακτίνα κάλυψης των δικτύων αυτών είναι της τάξης μεγέθους των μερικών μέτρων (< 10 m). Στην τεχνολογία WPANs ανήκουν οι τεχνολογίες Bluetooth και ZigBee.

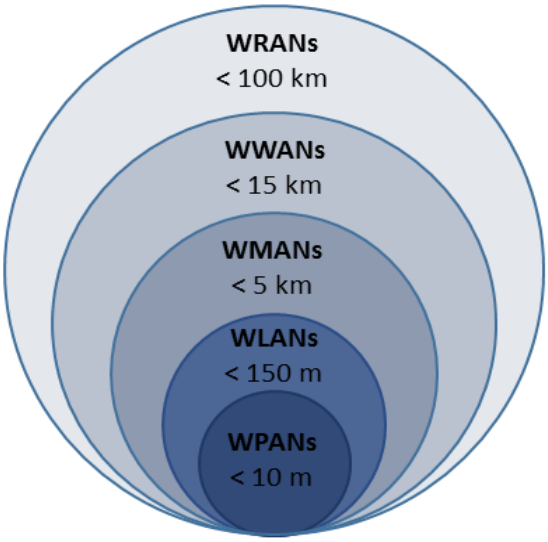
Ασύρματα τοπικά δίκτυα (Wireless Local Area Networks – WLANs): η τεχνολογία αυτή έχει σχεδιαστεί για να παρέχει ασύρματη επικοινωνία υψηλών ρυθμών μετάδοσης με τοπική εμβέλεια (ακτίνα κάλυψης 150 m περίπου), με χαρακτηριστικότερη εμπορική εφαρμογή την τεχνολογία WiFi.

Ασύρματα μητροπολιτικά δίκτυα (Wireless Metropolitan Area Networks – WMANs): παρέχουν ευρυζωνική ασύρματη πρόσβαση σε απόσταση της τάξης μεγέθους μιας αστικής περιοχής ή ενός δήμου (< 5 km). Χαρακτηριστική εμπορική εφαρμογή της τεχνολογίας αυτής είναι η τεχνολογία WiMAX (είναι γνωστή και ως πρότυπο IEEE 802.16).

Ασύρματα δίκτυα ευρείας κάλυψης (Wireless Wide Area Networks – WWANs): έχουν σχεδιαστεί έτσι ώστε να παρέχουν ασύρματες επικοινωνίες σε ευρείες γεωγραφικές περιοχές (σε αποστάσεις μικρότερες των 15 km περίπου). Περιλαμβάνουν τα κυψελωτά και τα δορυφορικά δίκτυα.

Ασύρματα περιφερειακά δίκτυα (Wireless Regional Area Networks – WRANs): η κάλυψη των δικτύων αυτών είναι της τάξης μεγέθους μιας ευρύτερης γεωγραφικής περιοχής (< 100 km), όπως ενός νομού. Χαρακτηριστική εμπορική εφαρμογή της κατηγορίας αυτής είναι η τεχνολογία IEEE 802.22.

Η ανωτέρω διάκριση των ασυρμάτων δικτύων με κριτήριο την εμβέλειά τους απεικονίζεται στο Σχήμα 1.3.



Σχήμα 1.3: Ταξινόμηση ασυρμάτων δικτύων με κριτήριο την εμβέλειά τους.

Ένας άλλος τρόπος κατηγοριοποίησης των ασυρμάτων δικτύων μπορεί να γίνει με κριτήριο την τοπολογία τους οπότε και διακρίνονται σε δίκτυα σημείου-προς-σημείο (point-to-point – PTP), σημείου-προς-πολλαπλά σημεία (point-to-multipoint – PMP) και πολλαπλών σημείων-προς-πολλαπλά σημεία (multipoint-to-multipoint – MPMP). Άλλες κατηγοριοποιήσεις γίνονται με βάση άλλα χαρακτηριστικά όπως τον ρυθμό μετάδοσης δεδομένων, την ισχύ μετάδοσης κ.α. Τέλος, μία σημαντική κατηγορία ασυρμάτων δικτύων, καθώς συνεισφέρουν σημαντικά στη βελτίωση των επικοινωνιών αλλά και της ασφάλειάς τους, είναι τα συνεργατικά δίκτυα (cooperative networks). Στην επόμενη ενότητα παρουσιάζονται τα δίκτυα αυτά και οι βασικές τεχνικές που χρησιμοποιούνται.

1.3 Συνεργατικά Δίκτυα

Οι συνεργατικές επικοινωνίες είναι ένας αναδυόμενος κλάδος, ο οποίος στοχεύει στην ενίσχυση της απόδοσης των συμβατικών δικτύων. Βασίζονται στην τεχνική του συνεργατικού διαφορισμού (cooperative diversity) όπου με την προσθήκη ενός ή περισσοτέρων βοηθητικών κόμβων, οι οποίοι ονομάζονται αναμεταδότες ή επαναλήπτες (relays) πετυχαίνουν κέρδος διαφορισμού, αφού ο δέκτης χρησιμοποιεί τόσο το απευθείας σήμα από τον πομπό αλλά και τα σήματα των βοηθητικών κόμβων προκειμένου να βελτιωθεί η απόδοση του συστήματος.

Στα συνεργατικά δίκτυα υπάρχουν δύο βασικές μεθοδολογίες αναμετάδοσης, η σταθερή αναμετάδοση (fixed relaying) και η επιλεκτική αναμετάδοση (selective relaying) [4]. Στη σταθερή αναμετάδοση, οι πόροι του συστήματος διατίθενται εξ αρχής μεταξύ του πομπού και του αναμεταδότη. Αυτό σημαίνει ότι η αναμετάδοση είναι προκαθορισμένη, δηλαδή ανεξάρτητα από τις συνθήκες ο εκάστοτε αναμεταδότης του συστήματος έχει συγκεκριμένους πόρους και σταθερή αναμετάδοση. Από την άλλη πλευρά, στην επιλεκτική αναμετάδοση, ο αναμεταδότης συμμετέχει στην επικοινωνία εφόσον οι συνθήκες είναι ευνοϊκές. Για παράδειγμα, εάν το κανάλι μεταξύ πομπού και αναμεταδότη υπόκειται σε δριμύτατες διαλείψεις τότε ο αναμεταδότης παραμένει ανενεργός.

Η σταθερή αναμετάδοση έχει το πλεονέκτημα της εύκολης εφαρμογής, αλλά το μειονέκτημα της απώλειας σε εύρος ζώνης [4]. Αυτό συμβαίνει διότι συγκεκριμένοι πόροι του καναλιού κατανέμονται σταθερά στον αναμεταδότη για τη μετάδοση, πράγμα το οποίο μειώνει τον γενικό ρυθμό μετάδοσης. Το πρόβλημα αυτό εμφανίζεται κυρίως σε περιπτώσεις όπου το κανάλι μεταξύ πομπού και δέκτη είναι αρκετά καλό, ενώ αντίθετα το κανάλι του αναμεταδότη-πομπού ή αναμεταδότη-δέκτη δεν είναι καλό. Αυτό το πρόβλημα προσπαθεί να ξεπεράσει η επιλεκτική αναμετάδοση.

Ανάλογα με το είδος της επεξεργασίας που συντελείται στον αναμεταδότη, τα δύο βασικά είδη των τεχνικών που χρησιμοποιούνται στις συνεργατικές επικοινωνίες (συνεργατικά πρωτόκολλα – cooperation protocols) είναι η ενίσχυση και προώθηση (Amplify and Forward – AF) και η αποκωδικοποίηση και προώθηση (Decode and Forward – DF). Στη πρώτη περίπτωση, ο αναμεταδότης απλά ενισχύει και προωθεί το λαμβανόμενο από τον πομπό σήμα προς τον δέκτη, ενώ στην δεύτερη, ο αναμεταδότης αποκωδικοποιεί το λαμβανόμενο σήμα, το επανακωδικοποιεί και στη συνέχεια το προωθεί προς τον δέκτη. Σημειώνεται ότι η σταθερή αναμετάδοση χρησιμοποιεί εξίσου και τις δύο τεχνικές, ενώ η επιλεκτική αναμετάδοση χρησιμοποιεί την τεχνική DF, οπότε και στην περίπτωση αυτή

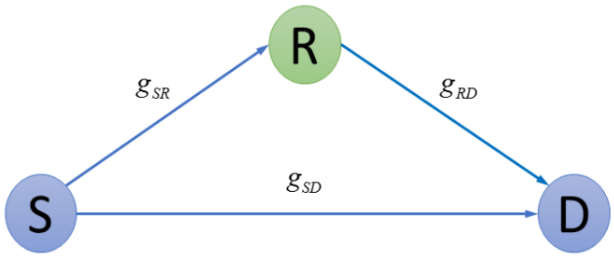
ονομάζεται επιλεκτική DF αναμετάδοση. Στη συνέχεια της ενότητας αυτής, αναλύονται οι τεχνικές AF και DF που αφορούν τη σταθερή αναμετάδοση.

1.3.1 Συνεργατικές τεχνικές

Για τους σκοπούς της ανάλυσης των συνεργατικών τεχνικών AF και DF της σταθερής αναμετάδοσης θεωρείται δίκτυο αποτελούμενο από έναν πομπό-πηγή (source – S), έναν δέκτη-προορισμό (destination – D) και έναν αναμεταδότη (relay – R).

Στο Σχήμα 1.4 απεικονίζεται το απλό αυτό μοντέλο, όπου η πηγή μεταδίδει με ισχύ P_1 και ο αναμεταδότης με ισχύ P_2. Βέβαια, στη συνέχεια θεωρείται η ειδική περίπτωση όπου τόσο η πηγή όσο και ο αναμεταδότης μεταδίδουν με ίση ισχύ P. Στο δίκτυο αυτό η επικοινωνία μεταξύ του πομπού και του δέκτη επιτυγχάνεται σε δύο φάσεις:

- Στη φάση 1, ο πομπός στέλνει το μήνυμα στον προορισμό, ενώ ταυτόχρονα το μήνυμα λαμβάνεται επίσης από τον αναμεταδότη.
- Στη φάση 2, ο αναμεταδότης βοηθάει την πηγή προωθώντας ή αναμεταδίδοντας το μήνυμα στον προορισμό.



Σχήμα 1.4: Απλό μοντέλο συνεργατικού δικτύου.

1.3.1.1 Πρωτόκολλο αναμετάδοσης AF

Στο πρωτόκολλο αναμετάδοσης ενίσχυσης και προώθησης, ο αναμεταδότης λαμβάνει το σήμα από τον πομπό και το μεταδίδει ενισχυμένο προς τον δέκτη. Τα λαμβανόμενα από τον αναμεταδότη και τον δέκτη σήματα δίνονται αντίστοιχα από τις σχέσεις:

$$y_{SR} = \sqrt{P} g_{SR} x + w_{SR} \tag{1.12}$$

$$y_{SD} = \sqrt{P} g_{SD} x + w_{SD} \tag{1.13}$$

όπου x είναι το σήμα πληροφορίας, g_{SD}, g_{SR} είναι οι συντελεστές (κέρδη τάσης) των καναλιών πηγής-προορισμού και πηγής-αναμεταδότη αντίστοιχα και w_{SD}, w_{SR} ο λευκός προσθετικός γκαουσιανός θόρυβος (AWGN) μηδενικής μέσης τιμής και διακύμανσης N_0. Θεωρούνται Rayleigh κανάλια μεταξύ των τριών κόμβων. Σε αυτό το πρωτόκολλο, στόχος του αναμεταδότη είναι να καλύψει τις απώλειες λόγω των διαλείψεων του καναλιού μεταξύ πομπού και δέκτη. Αυτό επιτυγχάνεται εφόσον ο αναμεταδότης ενισχύσει το σήμα πληροφορίας κατά έναν παράγοντα, ο οποίος είναι αντιστρόφως ανάλογος της ληφθείσας ισχύος του σήματος, ο οποίος συμβολίζεται με:

$$\beta_R = \frac{\sqrt{P}}{\sqrt{P\left|g_{SR}\right|^2 + N_0}} \tag{1.14}$$

Συνεπώς, το σήμα που μεταδίδει ο αναμεταδότης δίνεται ως $\beta_R y_{SR}$ και έχει ισχύ P ίση με την ισχύ του σήματος που μετέδωσε η πηγή. Για να υπολογιστεί η συνολική χωρητικότητα του καναλιού μεταξύ πηγής και προορισμού, πρέπει να υπολογιστεί ο σηματοθορυβικός λόγος (signal-to-noise ratio – SNR) στον προορισμό. Ο SNR του προορισμού είναι το άθροισμα των σηματοθορυβικών λόγων των συνδέσεων του με την πηγή και τον αναμεταδότη. Ο SNR της σύνδεσης με την πηγή δίνεται από τη σχέση:

$$SNR_{SD} = \frac{P\left|g_{SR}\right|^2}{N_0} \tag{1.15}$$

Στη συνέχεια υπολογίζεται ο SNR της σύνδεσης αναμεταδότη και προορισμού. Στη Φάση 2, το λαμβανόμενο από τον προορισμό σήμα, σύμφωνα με την (1.14), δίνεται από τη σχέση:

$$y_{RD} = \frac{\sqrt{P}}{\sqrt{P\left|g_{SR}\right|^2 + N_0}} g_{RD} y_{SR} + w_{RD} \tag{1.16}$$

όπου g_{RD} είναι ο συντελεστής του καναλιού αναμεταδότη-προορισμού και w_{RD} ο προσθετικός θόρυβος. Με βάση τη σχέση (1.12) το σήμα y_{RD} γράφεται ως εξής:

$$y_{RD} = \frac{\sqrt{P}}{\sqrt{P\left|g_{SR}\right|^2 + N_0}} \sqrt{P} g_{RD} g_{SR} x + w'_{RD} \tag{1.17}$$

όπου

$$w'_{RD} = \frac{\sqrt{P}}{\sqrt{P\left|g_{SR}\right|^2 + N_0}} g_{RD} w_{SR} + w_{RD} \tag{1.18}$$

υποθέτοντας ότι οι w_{SR} και w_{RD} είναι ανεξάρτητοι, τότε ο ισοδύναμος θόρυβος w'_{RD} είναι και αυτός τυχαία Gaussian μεταβλητή μηδενικής μέσης τιμής και διακύμανσης

$$N'_0 = \left(\frac{P\left|g_{RD}\right|^2}{P\left|g_{SR}\right|^2 + N_0} + 1 \right) N_0 \tag{1.19}$$

Ο προορισμός λαμβάνει δύο εκδοχές του σήματος πληροφορίας x, μία από το κανάλι πηγής-προορισμού και μία από το κανάλι αναμεταδότη-προορισμού. Υπάρχουν διάφορες τεχνικές που μπορούν να συνδυάσουν τα δύο αυτά σήματα. Η βέλτιστη τεχνική που μεγιστοποιεί τον συνολικό SNR είναι η τεχνική συνδυασμού μεγίστου λόγου (maximal ratio combiner –MRC). Με βάση την τεχνική αυτή, χρησιμοποιείται ένας διαφοριστής ο οποίος έχει γνώση των συντελεστών των καναλιών. Η έξοδος του διαφοριστή στον προορισμό γράφεται ως εξής:

$$y = a_1 y_{SD} + a_2 y_{RD} \tag{1.20}$$

δηλαδή τα δύο σήματα που λαμβάνει ο προορισμός πολλαπλασιάζονται με έναν συντελεστή και στη συνέχεια αθροίζονται. Οι συντελεστές a_1 και a_2 σχεδιάζονται ώστε να μεγιστοποιήσουν τον συνολικό SNR. Αποδεικνύεται [4] ότι δίνονται από τις σχέσεις:

$$a_1 = \frac{\sqrt{P} g_{SD}^*}{N_0} \tag{1.21}$$

$$a_2 = \frac{\sqrt{\frac{P}{P|g_{SR}|^2 + N_0}} \sqrt{P} g_{SR}^* g_{RD}^*}{\left(\frac{P|g_{RD}|^2}{P|g_{SR}|^2 + N_0} + 1 \right) N_0} \tag{1.22}$$

Υποθέτοντας ότι το σήμα πληροφορίας x έχει μοναδιαία μέση ενέργεια, ο στιγμιαίος SNR της εξόδου του διαφοριστή MRC είναι:

$$\Gamma = \Gamma_1 + \Gamma_2 \tag{1.23}$$

όπου

$$\begin{aligned} \Gamma_1 &= \frac{\left| a_1 \sqrt{P} g_{SD} \right|^2}{|a_1|^2 N_0} \\ &= \frac{P|g_{SD}|^2}{N_0} \end{aligned} \tag{1.24}$$

$$\begin{aligned} \Gamma_2 &= \frac{\left| a_2 \sqrt{\frac{P}{P|g_{SR}|^2 + N_0}} \sqrt{P} g_{SR} g_{RD} \right|^2}{|a_2|^2 N_0'} \\ &= \frac{1}{N_0} \frac{P^2 |g_{SR}|^2 |g_{RD}|^2}{P|g_{SR}|^2 + P|g_{RD}|^2 + N_0} \end{aligned} \tag{1.25}$$

Τελικά, η στιγμιαία συνολική χωρητικότητα (μέγιστη αμοιβαία πληροφορία) της ζεύξης πηγής-προορισμού του συστήματος του Σχήματος (1.4) όπου ο αναμεταδότης χρησιμοποιεί την τεχνική AF δίνεται από τη σχέση:

$$C_{AF} = \frac{1}{2} \log\left(1 + \Gamma_1 + \Gamma_2\right) \tag{1.26}$$

Αντικαθιστώντας τις τιμές των SNRs από τις σχέσεις (1.24) και (1.25) προκύπτει:

$$C_{AF} = \frac{1}{2} \log\left(1 + \frac{P|g_{SD}|^2}{N_0} + \frac{P^2 |g_{SR}|^2 |g_{RD}|^2}{\left(P|g_{SR}|^2 + P|g_{RD}|^2 + N_0 \right) N_0} \right) \tag{1.27}$$

1.3.1.2 Πρωτόκολλο αναμετάδοσης DF

Στο πρωτόκολλο αναμετάδοσης αποκωδικοποίησης και προώθησης, ο αναμεταδότης αφού λάβει, στη Φάση 1, το σήμα πληροφορίας από τον πομπό, το αποκωδικοποιεί, στη συνέχεια το επανακωδικοποιεί και τέλος το προωθεί, στη Φάση 2, προς τον δέκτη. Ωστόσο, εάν η αποκωδικοποίηση στον αναμεταδότη είναι λανθασμένη και ο αναμεταδότης προωθήσει το λανθασμένο αυτό σήμα στον προορισμό, η αποκωδικοποίηση στον προορισμό είναι ανούσια. Συνεπώς, η απόδοση του συστήματος περιορίζεται από τον

χειρότερο σύνδεσμο μεταξύ πηγής-προορισμού και πηγής-αναμεταδότη. Οπότε η συνολική χωρητικότητα μεταξύ πηγής και προορισμού ισούται κάθε στιγμή με την χωρητικότητα του πιο αδύναμου καναλιού μεταξύ του καναλιού πηγής-προορισμού και του συνδυασμού των καναλιών πηγής-αναμεταδότη και αναμεταδότη-προορισμού. Συγκεκριμένα, η στιγμιαία χωρητικότητα του συστήματος για DF αναμετάδοση δίνεται από την σχέση:

$$C_{DF} = \frac{1}{2}\min\left\{\log\left(1+\frac{P|g_{SR}|^2}{N_0}\right), \log\left(1+\frac{P|g_{SD}|^2}{N_0}+\frac{P|g_{RD}|^2}{N_0}\right)\right\} \qquad (1.28)$$

Η σχέση (1.28) ισχύει εφόσον ο αναμεταδότης αποκωδικοποιήσει σωστά το μήνυμα. Εάν η αποκωδικοποίηση είναι λάθος τότε η χωρητικότητα του συστήματος ισούται με τη χωρητικότητα του καναλιού μεταξύ πηγής και προορισμού.

Βιβλιογραφία - Αναφορές 1ου Κεφαλαίου

[1] Π. Κωττής, Π.-Δ. Αράπογλου, Ασύρματες Επικοινωνίες, Εκδόσεις Τζιόλα, 2014.

[2] M. K. Simon, M. S. Alouini, Digital Communication over Fading Channels, Wiley, New York, 2nd edition, 2005.

[3] E. Hossain, D. Niyato, Z. Han, Dynamic Spectrum Access and Management in Cognitive Radio Networks, Cambridge University Press, 2009.

[4] K. J, Liu, A. Sadek, W. Su, A. Kwasinski, Cooperative Communications and Networking, Cambridge University Press, 2009.

2

Ασφαλεια Ασυρματων Επικοινωνιων

Οι ασύρματες επικοινωνίες αποτελούν ένα αναπόσπαστο κομμάτι της σύγχρονης κοινωνίας, με τη χρήση τους να ποικίλει από την απλή καθημερινή χρήση έως τις στρατιωτικές εφαρμογές. Εξαιτίας της μετάδοσης μέσω της διεπαφής του αέρα, το ασύρματο μέσο μεταφοράς είναι προσβάσιμο τόσο σε εξουσιοδοτημένους όσο και σε μη-νόμιμους χρήστες. Αντίθετα, στις ενσύρματες επικοινωνίες οι συσκευές είναι άμεσα συνδεδεμένες μεταξύ τους με καλώδια, έτσι η πρόσβαση σε κόμβους εκτός δικτύου καθίσταται δυσκολότερη, ώστε να μπορέσουν να βλάψουν την επικοινωνία. Ως εκ τούτου, το ανοικτό περιβάλλον επικοινωνίας καθιστά τις ασύρματες μεταδόσεις περισσότερο ευάλωτες από τις ενσύρματες σε επιθέσεις ασφαλείας. Δεδομένου ότι η πλειοψηφία των ανθρώπων βασίζεται στις ασύρματες επικοινωνίες για τη μετάδοση σημαντικών και ιδιωτικών πληροφοριών, όπως πχ. οι συναλλαγές με πιστωτικές κάρτες, η ασφάλεια των ασύρματων επικοινωνιών είναι ένας τομέας κριτικής σημασίας με πολλές προκλήσεις για τους μηχανικούς. Αντικείμενό της είναι η αντιμετώπιση δυσμενών καταστάσεων, οι οποίες σχετίζονται με την απώλεια ακεραιότητας δεδομένων, τις υποκλοπές και παρεμβολές μεταδιδόμενης πληροφορίας, την είσοδο και μετάδοση στο δίκτυο ψευδών ή τροποποιημένων μηνυμάτων πληροφορίας και την κατασπατάληση πόρων.

Στο κεφάλαιο αυτό γίνεται μία εισαγωγή σε θέματα ασφαλείας στις ασύρματες επικοινωνίες. Αρχικά, παρουσιάζεται το μοντέλο αναφοράς Ανοικτής Διασύνδεσης Συστημάτων (Open System Interconnection – OSI), αρχιτεκτονική την οποία ακολουθούν τα ασύρματα δίκτυα. Στη συνέχεια, αναλύονται οι απαιτήσεις ασφαλείας των ασύρματων δικτύων και τέλος γίνεται μία σύντομη αναφορά και ταξινόμηση των επιθέσεων και των απειλών ασφαλείας.

2.1 Διαστρωμάτωση κατά OSI

Τα σύγχρονα συστήματα επικοινωνιών (ασύρματα και ενσύρματα) αναλύονται ως ένα σύνολο διαδοχικών επιπέδων-στρωμάτων. Με τη διαστρωμάτωση επιτυγχάνεται ο κατακερματισμός του πολύπλοκου προβλήματος της επικοινωνίας μεταξύ των κόμβων του δικτύου σε επιμέρους, απλούστερα στην επίλυσή τους, προβλήματα. Η αρχή αυτή της διαστρωμάτωσης καταδεικνύεται καλύτερα από το μοντέλο Διασύνδεσης Ανοικτών Συστημάτων (OSI).

Το μοντέλο αναφοράς OSI είναι ένα θεωρητικό μοντέλο που περιγράφει τον τρόπο με τον οποίο μπορούν να επικοινωνήσουν μεταξύ τους δύο οποιαδήποτε διαφορετικά συστήματα. Βασίζεται σε επτά επίπεδα-στρώματα [1]. Κάθε στρώμα χρησιμοποιεί συγκεκριμένα πρωτόκολλα και εκτελεί συγκεκριμένες λειτουργίες. Τα επτά στρώματα και οι αντίστοιχες λειτουργίες τους είναι:

1. *Φυσικό Στρώμα (Physical layer – PHY):* Είναι υπεύθυνο για τη μετάδοση ακατέργαστων bits μέσω ενός επικοινωνιακού διαύλου και κατά συνέπεια καλύπτει τη φυσική διεπαφή μεταξύ κόμβων ενός δικτύου καθώς και τους κανόνες με τους οποίους τα bits μεταδίδονται.

2. *Στρώμα Ζεύξης Δεδομένων (Data link layer):* Κύρια λειτουργία του στρώματος αυτού είναι η οργάνωση των bits σε λογικές μονάδες, οι οποίες ονομάζονται πλαίσια (frames) και περιέχουν πληροφορίες από το επίπεδο δικτύου. Επίσης, είναι υπεύθυνο για την αξιοπιστία της μετάδοσης μέσω της αναγνώρισης ή και της διόρθωσης σφαλμάτων. Ο ρόλος του στρώματος ζεύξης δεδομένων γίνεται πιο περίπλοκος όταν υπάρχουν πολλαπλοί κόμβοι οι οποίο μοιράζονται το ίδιο μέσο. Αντίστοιχα, το τμήμα του στρώματος που είναι υπεύθυνο για την πολλαπλή πρόσβαση είναι το υπόστρωμα Ελέγχου Πρόσβασης στο Μέσο (Medium Access Control – MAC).

3. *Στρώμα Δικτύου (Network layer):* Το επίπεδο δικτύου είναι υπεύθυνο για την παράδοση των πακέτων (τα πλαίσια οργανώνονται σε πακέτα ώστε να τα χειριστεί το επίπεδο δικτύου) μεταξύ της αρχικής προέλευσης και του τελικού προορισμού.

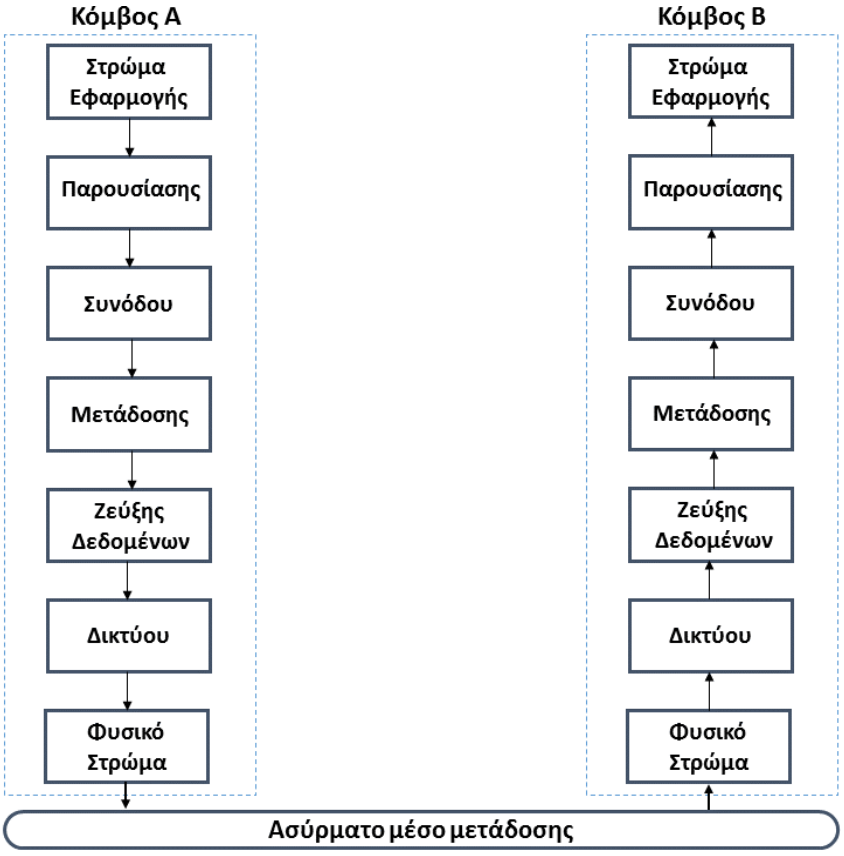
4. *Στρώμα Μετάδοσης (Transport layer):* Βασική λειτουργία του στρώματος μετάδοσης είναι η παροχή υπηρεσίας μεταφοράς με σύνδεση. Είναι, δηλαδή, υπεύθυνο για την από άκρο σε άκρο παράδοση (από την προέλευση ως τον προορισμό) ολόκληρου του μηνύματος.

5. *Στρώμα Συνόδου (Session layer):* Το στρώμα συνόδου ή επίπεδο συνεδρίας έχει σχεδιαστεί για τον έλεγχο του διαλόγου μεταξύ των χρηστών. Εγκαθιδρύει, συντηρεί και συγχρονίζει τον διάλογο των συστημάτων που επικοινωνούν μεταξύ τους.

6. *Στρώμα Παρουσίασης (Presentation layer):* Το επίπεδο αυτό ασχολείται με την σύνταξη και την σημασιολογία των πληροφοριών που ανταλλάσσονται μεταξύ δύο συστημάτων. Αντιμετωπίζει το γεγονός ότι κάθε σύστημα μπορεί να χρησιμοποιεί τη δική του μέθοδο κωδικοποίησης.

7. *Στρώμα Εφαρμογής (Application layer):* Το στρώμα εφαρμογής προσφέρει τον τρόπο πρόσβασης των λογισμικών εφαρμογών στην αρχιτεκτονική του OSI. Είναι η διεπαφή με τους χρήστες.

Όπως παρουσιάζεται στο Σχήμα 2.1, ένας κόμβος δικτύου (κόμβος Α) χρησιμοποιεί την παραπάνω διαστρωμάτωση για τη μετάδοση πακέτων δεδομένων σε έναν άλλο κόμβο του δικτύου (κόμβος Β). Πριν σταλούν τα δεδομένα στο φυσικό μέσο μεταφοράς (ασύρματο μέσο για τις ασύρματες επικοινωνίες) διατρέχουν και τα επτά επίπεδα, τα οποία προσθέτουν στα δεδομένα πληροφορίες ελέγχου, μέχρι να συναντήσουν το φυσικό επίπεδο. Συγκεκριμένα, το πακέτο δεδομένων στον κόμβο Α διευρύνεται με επιπλέον πληροφορίες από τα πρωτόκολλα κάθε επιπέδου ξεκινώντας από το στρώμα εφαρμογής. Ως αποτέλεσμα, δημιουργείται ένα ενθυλακωμένο πακέτο το οποίο μεταδίδεται ασύρματα (για ασύρματες επικοινωνίες) στον κόμβο Β, ο οποίος θα εκτελέσει αποκελυφοποίηση του πακέτου με τη βοήθεια των αντίστοιχων πρωτοκόλλων κάθε επιπέδου, ξεκινώντας από το φυσικό στρώμα και καταλήγοντας στο στρώμα εφαρμογής, προκειμένου να ανακτήσει την αρχική πληροφορία.



Σχήμα 2.1: Μοντέλο αναφοράς OSI για την ασύρματη επικοινωνία μεταξύ δύο κόμβων.

2.2 Απαιτήσεις Ασφαλείας Ασυρμάτων Δικτύων

Στα ασύρματα δίκτυα η πληροφορία ανταλλάσσεται μεταξύ εξουσιοδοτημένων χρηστών, αλλά, όπως προαναφέρθηκε, η διαδικασία αυτή είναι ευάλωτη σε διάφορες κακόβουλες απειλές εξαιτίας της broadcast φύσης του ασύρματου μέσου. Η έννοια της ασφάλειας ενός ασύρματου δικτύου, λοιπόν, έγκειται στην προστασία των δεδομένων που μεταδίδονται μεταξύ των κόμβων του δικτύου από αλλοιώσεις ή διαρροές, στην εξασφάλιση

των πόρων του δικτύου και στην ικανότητα παροχής από τους κόμβους ικανής και αξιόπιστης πληροφορίας. Από τα παραπάνω προκύπτουν και οι απαιτήσεις ασφαλείας, οι οποίες αποτελούν τις προδιαγραφές ασφαλείας του δικτύου και είναι οι παρακάτω [2]:

1. *Αυθεντικότητα ή πιστοποίηση (Authentication) και Μη-αποποίηση (Non-repudiation):* Η αυθεντικότητα αναφέρεται στην πιστοποίηση της ταυτότητας ενός κόμβου του δικτύου έτσι ώστε να διακρίνονται οι εξουσιοδοτημένοι από τους μη-νόμιμους χρήστες. Στα ασύρματα δίκτυα, ένα ζευγάρι κόμβων θα πρέπει πρώτα να εφαρμόσει αμοιβαία πιστοποίηση προτού προβεί σε εγκατάσταση σύνδεσης για μετάδοση δεδομένων [3]. Τυπικά, ένας κόμβος δικτύου είναι εξοπλισμένος με μια ασύρματη κάρτα διασύνδεσης δικτύου (network interface card) και διαθέτει μία μοναδική διεύθυνση ελέγχου πρόσβασης μέσων (MAC address), η οποία χρησιμοποιείται για πιστοποίηση. Εκτός από την πιστοποίηση επιπέδου MAC, υπάρχουν και οι πιστοποιήσεις επιπέδου δικτύου, μετάδοσης και εφαρμογής. Άλλοι δύο τύποι πιστοποιήσεων είναι η πιστοποίηση οντότητας (entity authentication) και η πιστοποίηση προέλευσης δεδομένων (data origin authentication). Η πρώτη χρησιμοποιείται για να επιβεβαιώσει τις οντότητες σε μια συνεδρία επικοινωνίας, ενώ η δεύτερη ασχολείται με την έγκριση της ταυτότητας ενός δημιουργού δεδομένων. Από την άλλη πλευρά, η μη-αποποίηση εγγυάται ότι ο πομπός ενός μηνύματος δεν μπορεί να αρνηθεί την αποστολή του και ο δέκτης ενός μηνύματος δεν μπορεί να αρνηθεί την λήψη του. Ψηφιακές υπογραφές, οι οποίες λειτουργούν ως μοναδικά αναγνωριστικά για ατομικούς χρήστες, χρησιμοποιούνται για σκοπούς μη-αποποίησης. Η συγκεκριμένη απαίτηση είναι σημαντική για τον εντοπισμό κόμβων που έχουν εκτεθεί σε κακόβουλη ενέργεια.

2. *Εμπιστευτικότητα (Confidentiality) και Έλεγχος πρόσβασης (Access control):* Ως εμπιστευτικότητα ορίζεται ως η εξασφάλιση ανάγνωσης και γνωστοποίησης ύπαρξης δεδομένων μόνο από εξουσιοδοτημένους χρήστες και αποφυγή υποκλοπής τους από μη-εξουσιοδοτημένους χρήστες με χρήση παθητικών επιθέσεων (οι παθητικές επιθέσεις θα οριστούν σε επόμενη ενότητα) [4]. Η εμπιστευτικότητα σχετίζεται στενά με το απόρρητο δεδομένων (data privacy), όπως η κρυπτογράφηση δεδομένων (data encryption) και η διαχείριση κλειδιού κρυπτογράφησης (encryption key management). Τα δεδομένα που στέλνονται από έναν πομπό θα πρέπει να είναι προσβάσιμα μόνο από τον δέκτη στον οποίο προορίζονται. Η κρυπτογράφηση δεδομένων είναι μία δημοφιλής τεχνική για διασφάλιση της εμπιστευτικότητας. Με την κρυπτογράφηση, ακόμη και στην περίπτωση που ένας εισβολέας έχει πρόσβαση στα δεδομένα που μεταδίδονται, ίσως δεν έχει την ικανότητα να εξάγει σημαντική πληροφορία από αυτά. Η άλλη πλευρά της εμπιστευτικότητας είναι η προστασία της ροής της κίνησης των δεδομένων από ανάλυση παράνομων εισβολέων. Αναλυτικότερα, εξασφαλίζει ότι ένας κακόβουλος εισβολέας δεν δύναται να καθορίσει οποιαδήποτε πληροφορία από την κίνηση δεδομένων, όπως η θέση πομπού/δέκτη, η συχνότητα μετάδοσης και άλλα χαρακτηριστικά της επικοινωνίας. Επιπλέον, ως ένας εναλλακτικός μηχανισμός εμπιστευτικότητας, ο έλεγχος πρόσβασης περιορίζει και ελέγχει τις συσκευές που έχουν πρόσβαση στους συνδέσμους της επικοινωνίας. Έτσι, κάθε οντότητα θα πρέπει να πιστοποιηθεί εκ των προτέρων ώστε να της δοθεί πρόσβαση στην επικοινωνία και τους αντίστοιχους συνδέσμους. Ωστόσο, εξαιτίας του ασύρματου

τρόπου επικοινωνίας ο έλεγχος πρόσβασης είναι ευάλωτος σε επιθέσεις όπως η ωτακουστία ή λαθρακρόαση (eavesdropping) και υπάρχουν πολλά εμπόδια στην επίτευξη μιας περιεκτικής στρατηγικής ελέγχου πρόσβασης.

3. *Ακεραιότητα (Integrity):* Η ακεραιότητα ορίζεται ως η εξασφάλιση πληρότητας των δεδομένων που διακινούνται στους κόμβους του δικτύου. Σύμφωνα με αυτήν, η πληροφορία που μεταδίδεται σε ένα ασύρματο δίκτυο θα πρέπει να είναι ακριβής και αξιόπιστη κατά τη διάρκεια του κύκλου ζωής της, αντιπροσωπεύοντας την πληροφορία της πηγής χωρίς παραποίηση ή τροποποίηση από μη-εξουσιοδοτημένους χρήστες [2]. Η ακεραιότητα ελέγχει ακόμη εάν κάποια οντότητα εισάγει τη σωστή πληροφορία, εάν η πληροφορία ανταποκρίνεται στις πραγματικές συνθήκες και εάν, υπό τις ίδιες συνθήκες, έχουν αναπαραχθεί απαράλλακτα δεδομένα. Οι επιθέσεις ‘’Άνθρωπος στη μέση’’ (Man in the middle – MITM) μπορεί να στοχεύουν την ακεραιότητα δεδομένων καθώς κρυφακούν την επικοινωνία και ίσως δημιουργήσουν νέες πορείες επικοινωνίας και εισάγουν κατεστραμμένα πακέτα [5].
4. *Διαθεσιμότητα (Availability):* Ως διαθεσιμότητα ορίζεται ως η δυνατότητα προσπέλασης της πληροφορίας από εξουσιοδοτημένους χρήστες και κόμβους του δικτύου. Υποδηλώνει ότι οι εξουσιοδοτημένοι χρήστες είναι πράγματι σε θέση να έχουν πρόσβαση στο ασύρματο δίκτυο οποιαδήποτε στιγμή και σε οποιοδήποτε σημείο κατόπιν αίτησης. Η διαθεσιμότητα της πληροφορίας πρέπει να υφίσταται ακόμη και σε περιπτώσεις διαταραχών όπως επιθέσεις ή εξάντληση πόρων, δηλαδή οι κόμβοι δεν πρέπει να τίθενται σε κατάσταση άρνησης εξυπηρέτησης (Denial of Service – DoS).

Οι προαναφερθείσες απαιτήσεις ασφαλείας (αυθεντικότητα, μη-αποποίηση, εμπιστευτικότητα, έλεγχος πρόσβασης, ακεραιότητα, διαθεσιμότητα) είναι συμπληρωματικές μεταξύ τους. Θα πρέπει, δηλαδή, να παρέχονται ταυτόχρονα έτσι ώστε να επιτευχθεί ασφαλής επικοινωνία.

2.3 Επιθέσεις Ασφαλείας στα Ασύρματα Δίκτυα

Στην ενότητα αυτή παρουσιάζονται οι πιο συνηθισμένες επιθέσεις ασφαλείας που συναντώνται στα ασύρματα συστήματα επικοινωνιών και γίνεται ταξινόμησή τους σε παθητικές και ενεργητικές επιθέσεις.

2.3.1 Παθητικές επιθέσεις

Οι παθητικές επιθέσεις μόνο παρακολουθούν και αναλύουν την κίνηση του δικτύου και δεν διακόπτουν τη λειτουργία του, αλλά έχουν ως σκοπό να υποκλέψουν μεταδιδόμενη πληροφορία από τα ασύρματα κανάλια. Δύο είναι οι κυριότερες παθητικές επιθέσεις, η παθητική λαθρακρόαση (passive eavesdropping) και η ανάλυση κίνησης (traffic analysis):

Eavesdropping: Η ωτακουστία ή λαθρακρόαση είναι ένας τρόπος για έναν ακούσιο δέκτη (ο οποίος καλείται ωτακουστής-eavesdropper) να υποκλέψει ένα μήνυμα. Οι ωτακουστές παρακολουθούν την επικοινωνία χωρίς ωστόσο να μπορούν

να τροποποιήσουν το μεταδιδόμενο μήνυμα. Στοχεύουν την παραβίαση της εμπιστευτικότητας του μηνύματος, όπως αναφέρθηκε παραπάνω.

Ανάλυση κίνησης: Η ανάλυση κίνησης είναι επίσης μία κατηγορία παθητικών επιθέσεων οι οποίες δεν τροποποιούν το μεταδιδόμενο μήνυμα. Οι αναλυτές κίνησης είναι σε θέση να αποκαλύψουν σημαντικές πληροφορίες (όπως η συχνότητα μετάδοσης, η τοποθεσία και η ταυτότητα πομπού/δέκτη), οι οποίες μπορούν να χρησιμοποιηθούν από άλλου είδους επιθέσεις.

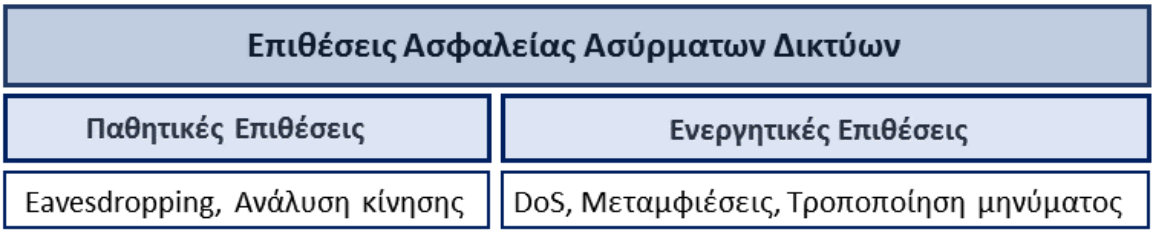
2.3.2 Ενεργητικές επιθέσεις

Οι ενεργητικές επιθέσεις είναι μία κατηγορία επιθέσεων οι οποίες είναι ικανές να επέμβουν στις λειτουργίες του δικτύου, όπως, για παράδειγμα, να τροποποιήσουν ή να διαγράψουν ένα μήνυμα. Οι πιο συνηθισμένες ενεργητικές επιθέσεις είναι οι επιθέσεις άρνησης εξυπηρέτησης (Denial of Service – DoS attacks), οι μεταμφιέσεις (masquerade attacks) και οι τροποποιήσεις μηνυμάτων (message modifications):

Άρνηση εξυπηρέτησης: Οι επιθέσεις άρνησης εξυπηρέτησης στοχεύουν στην εξάντληση των πόρων του δικτύου έτσι ώστε το δίκτυο να μην μπορεί πλέον να εξυπηρετεί τους εξουσιοδοτημένους κόμβους. Η κατανεμημένη άρνηση εξυπηρέτησης (Distributed Dos) είναι μία πιο σοβαρή επίθεση DoS. Ενώ οι επιθέσεις DoS στοχεύουν μία συσκευή και μία σύνδεση επικοινωνίας, στις επιθέσεις DDoS προσβάλλονται πολλαπλές συσκευές και επιθέσεις.

Μεταμφιέσεις: Σε μία επίθεση μεταμφίεσης, ο εισβολέας προσποιείται ότι είναι ένας νόμιμος χρήστης του δικτύου και προσπαθεί να λάβει πιστοποίηση ώστε να σφετεριστεί τους πόρους του συστήματος. Κατά τις επιθέσεις του τύπου αυτού συνήθως εμπεριέχονται και άλλου τύπου ενεργητικές επιθέσεις. Για παράδειγμα, μπορούν να συλληφθούν οι αλληλουχίες ελέγχου ταυτότητας και έτσι ο εισβολέας να αποκτήσει πρόσβαση σε πληροφορίες των μηνυμάτων [4].

Τροποποίηση μηνύματος: Οι επιθέσεις αυτού του τύπου αναφέρονται στις επιθέσεις όπου ο εισβολέας εκτελεί αλλαγές, προσθήκες ή διαγραφές στο περιεχόμενο του αρχικού μηνύματος που μεταδίδεται στο σύστημα επικοινωνίας.



Σχήμα 2.2: Κατηγοριοποίηση επιθέσεων ασφαλείας.

Μία επιπλέον κατηγοριοποίηση των επιθέσεων ασφαλείας είναι η ταξινόμησή τους σε εσωτερικές και εξωτερικές. Οι εσωτερικές επιθέσεις προκαλούνται από συσκευές του δικτύου που έχουν προσβληθεί κακόβουλα, ενώ οι εξωτερικές επιθέσεις γίνονται από συσκευές εκτός του δικτύου. Ταξινόμηση των επιθέσεων μπορεί επίσης να γίνει με βάση την απαίτηση ασφαλείας στην οποία στοχεύουν. Συνεπώς, προκύπτουν επιθέσεις ασφαλείας κατά της αυθεντικότητας, εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας. Οι

επιθέσεις κατά της αυθεντικότητας και της εμπιστευτικότητας στοχεύουν σε υποκλοπή ή τροποποίηση δεδομένων και αντιμετωπίζονται συνήθως με κρυπτογραφικές τεχνικές που προστατεύουν το απόρρητο δεδομένων. Όπως προαναφέρθηκε, οι επιθέσεις κατά τις διαθεσιμότητας αναφέρονται ως DoS επιθέσεις. Τέλος, οι επιθέσεις κατά τις ακεραιότητας αποσκοπούν στη διοχέτευση στο δίκτυο ψευδών ή τροποποιημένων δεδομένων.

2.4 Ασφάλεια Ασυρμάτων Δικτύων από τη Σκοπιά του Μοντέλου Αναφοράς OSI

2.4.1 Απειλές ασφαλείας

Κάθε στρώμα-επίπεδο του μοντέλου αναφοράς OSI αντιμετωπίζει διαφορετικά θέματα και προκλήσεις ασφαλείας, από τη στιγμή που εκτελεί διαφορετικές λειτουργίες και βασίζεται σε διαφορετικά πρωτόκολλα και έτσι παρουσιάζει διαφορετικά ευάλωτα σημεία σε θέματα ασφαλείας [2]. Συνεπώς διαφορετικές επιθέσεις ασφαλείας απειλούν διαφορετικά επίπεδα στα συστήματα επικοινωνιών. Σε αυτό το σημείο, παρουσιάζονται συνοπτικά οι κυριότερες απειλές των διαφορετικών επιπέδων του μοντέλου αναφοράς OSI.

Το *Φυσικό Στρώμα* είναι ευάλωτο ως προς την ασφάλεια δεδομένης της προσβασιμότητας του ασύρματου μέσου σε μη-εξουσιοδοτημένους χρήστες. Για παράδειγμα, το eavesdropping είναι μία εκ των επιθέσεων κατά του φυσικού στρώματος. Σε άλλες περιπτώσεις, ενεργητικές επιθέσεις δημιουργούν θόρυβο και στοχεύουν στην παρεμπόδιση της επικοινωνίας μεταξύ κόμβων ενός δικτύου. Οι επιθέσεις αυτές ονομάζονται επιθέσεις ηθελημένης παρεμβολής (jamming attacks) [4]. Ακόμη, οι επιθέσεις αλλοίωσης και υποκλοπής (tampering attacks) στοχεύουν στη φυσική καταστροφή των κόμβων, εκμεταλλευόμενες την απομακρυσμένη λειτουργία, και στην υποκλοπή ευαίσθητων δεδομένων, όπως κρυπτογραφικών κλειδιών, με σκοπό την ανάθεση στον επιτιθέμενο του ελέγχου του κόμβου που δέχεται τη κακόβουλη ενέργεια.

Όσον αφορά το *Στρώμα Ζεύξης Δεδομένων* και κυρίως το υπόστρωμα MAC αυτού, υπάρχουν επιθέσεις όπως η πλαστογράφηση MAC (MAC spoofing) και η υποκλοπή διεύθυνσης MAC (MAC address theft) οι οποίες στοχεύουν στη λειτουργία της πιστοποίησης. Επιθέσεις DoS και MITM μπορούν, επίσης, να στοχεύουν στο υπόστρωμα MAC [6]. Συγκεκριμένα, στις επιθέσεις MITM ενεργητικοί ωτακουστές στέλνουν παραπλανητικά πακέτα εγκαθιστώντας συνδέσεις με τα θύματά τους διασπώντας την απευθείας σύνδεση του νόμιμου ζευγαριού που επικοινωνεί. Άλλη κατηγορία επιθέσεων στο επίπεδο αυτό αφορούν την παραγωγή πολλαπλών διευθύνσεων MAC ανά τακτά χρονικά διαστήματα προκειμένου να πλημμυρίσει ο πίνακας της συσκευής που περιέχει τις διευθύνσεις MAC του δικτύου [7]. Η σύγκρουση δεδομένων (data collision) είναι επίθεση ασφαλείας που απειλεί, επίσης, το επίπεδο ζεύξης. Η κατάσταση σύγκρουσης δεδομένων λαμβάνει χώρα όταν δύο ή περισσότεροι γειτονικοί κόμβοι αποστέλλουν ταυτόχρονα πακέτα δεδομένων στο ίδιο κανάλι επικοινωνίας. Σκοπός της επίθεσης είναι η απώλεια πακέτων, λόγω προσβολής του πρωτοκόλλου MAC, και η δημιουργία σφαλμάτων στο δίκτυο και ανάγκης επανεκπομπών.

Η πλαστογράφηση IP διευθύνσεων (IP spoofing), η επίθεση δρομολόγησης (routing attack) και η επιλεκτική προώθηση (selective forwarding) στοχεύουν στο *Στρώμα Δικτύου*, το οποίο χρησιμοποιεί το πρωτόκολλο IP. Η πλαστογράφηση IP είναι μέθοδος επίθεσης όπου ο επιτιθέμενος πλαστογραφεί ή παραποιεί τις διευθύνσεις IP των πακέτων προκαλώντας την αποτυχία του νόμιμου δέκτη στην εύρεση της πραγματικής διεύθυνσης IP του αποστολέα του πακέτου. Οι επιθέσεις δρομολόγησης βλάπτουν το πρωτόκολλο δρομολόγησης με διάφορους τρόπους, όπως με την προσθήκη ή διαγραφή διαδρομών στον πίνακα δρομολόγησης. Επίσης, οι επιθέσεις αυτές μπορεί να δημιουργήσουν ανεπιθύμητους βρόχους δρομολόγησης, οι οποίοι προσελκύουν ή απωθούν τη διακίνηση μηνυμάτων και οδηγούν τόσο σε ενεργειακή εξάντληση κόμβων λόγω συνεχών εκπομπών ετεροχρονισμένων μηνυμάτων, όσο και σε καθυστερήσεις στην επικοινωνία. Στην επιλεκτική προώθηση ο κόμβος που έχει προσβληθεί θα προωθήσει επιλεκτικά ορισμένα πακέτα, απορρίπτοντας τα υπόλοιπα, τα οποία χάνονται.

Το *Στρώμα Μετάδοσης* χρησιμοποιεί είτε το πρωτόκολλο ελέγχου μετάδοσης (transmission control protocol – TCP) είτε το πρωτόκολλο δεδομενογραφημάτων χρήστη (user datagram protocol – UDP). Το TCP είναι ένα πρωτόκολλο αξιόπιστο, με σύνδεση στο οποίο ο πομπός μπορεί να εγγυηθεί τη λήψη του μηνύματος από τον δέκτη μέσω ενός αναγνωριστικού μηνύματος. Έτσι, υποστηρίζεται ο έλεγχος ροής. Το UDP είναι ένα πρωτόκολλο μη αξιόπιστο, χωρίς σύνδεση, που χρησιμοποιείται σε γρήγορες εφαρμογές και ερωταποκρίσεις για άμεση παράδοση και όχι απαραίτητα ορθή παράδοση, στο οποίο ο πομπός δεν μπορεί να εγγυηθεί την αξιοπιστία της επικοινωνίας [1]. Μία εκ των επιθέσεων που απειλούν το επίπεδο μετάδοσης και αφορούν το πρωτόκολλο TCP είναι η επίθεση πλημμύρας (flooding attack), στην οποία ο κακόβουλος κόμβος στέλνει επαναλαμβανόμενα πακέτα προς τον κόμβο που πρόκειται να προσβληθεί. Ο κόμβος που δέχεται την επίθεση διαθέτει πόρους ώστε να διατηρήσει τη σύνδεση με τον κόμβο που ελέγχει ο επιτιθέμενος. Με την επίθεση αυτή, προκαλείται μεγάλος αριθμός εκπομπών, οι οποίοι εξαντλούν τους ενεργειακούς πόρους του δικτύου, και ακολούθως το χρόνο ζωής του. Συνεπώς, οι επιθέσεις πλημμύρας καταλήγουν σε άρνηση εξυπηρέτησης. Άλλου είδους επιθέσεις που στοχεύουν το επίπεδο αυτό είναι οι επιθέσεις αποσυγχρονισμού (desynchronization attacks). Στόχος της επίθεσης αποσυγχρονισμού είναι η διαταραχή της σύνδεσης μεταξύ δύο συσκευών του δικτύου. Η επίθεση μπορεί να πραγματοποιηθεί με αποστολή πλαστογραφημένων μηνυμάτων σε μία συσκευή, η οποία ζητάει την επανεκπομπή των μηνυμάτων που έχουν χαθεί.

Στο *Στρώμα Εφαρμογής*, ιοί (viruses), σκώληκες (worms) και δούρειοι ίπποι (trojan horses) είναι οι συνηθέστερες απειλές. Τεχνικά, ο ιός επισυνάπτεται σε ένα πρόγραμμα ή αρχείο και μεταφέρεται από μια συσκευή σε άλλες μέσω της μεταφοράς των μολυσμένων αρχείων ή της εγκατάστασης των μολυσμένων προγραμμάτων. Ο ιός εξαπλώνεται και κάνει ευάλωτο το δίκτυο στις επιθέσεις. Οι σκώληκες λειτουργούν παρόμοια με τους ιούς, χωρίς ωστόσο την εμπλοκή κάποιου χρήστη. Από την άλλη πλευρά, οι δούρειοι ίπποι είναι προγράμματα που προσπαθούν να παραπλανήσουν τον χρήστη και να τον οδηγήσουν στην εγκατάσταση των προγραμμάτων τα οποία θα μολύνουν τη συσκευή του. Συνδυασμός απειλών (blended threats) από ιούς, σκώληκες και δούρειους ίππους προκαλούν

πολλαπλές βλάβες σε ένα δίκτυο. Επίσης, οι επιθέσεις DDoS απειλούν το στρώμα εφαρμογής.

Όσον αφορά, τέλος, τα *Στρώματα Συνόδου* και *Παρουσίασης*, δεν υπάρχουν ουσιαστικές επιθέσεις που να στοχεύουν τα δύο αυτά στρώματα, καθότι οι λειτουργίες των επιπέδων αυτών αφορούν στον τρόπο παρουσίασης και επικοινωνίας μεταξύ των συστημάτων, εξυπηρετούν δηλαδή τυπικούς σκοπούς.

2.4.2 Επισκόπηση βελτιώσεων της ασφάλειας στρωμάτων της αρχιτεκτονικής δικτύου

Στην ενότητα αυτή γίνεται μία ανασκόπηση των μηχανισμών για την ενίσχυση της ασφάλειας από την οπτική γωνία του μοντέλου αναφοράς OSI. Εδώ, το θέμα της ασφάλειας του φυσικού στρώματος περιορίζεται σε μία σύντομη εισαγωγή, ενώ εκτενής παρουσίαση θα γίνει στο Κεφάλαιο 3. Είναι προφανές ότι οι επιθέσεις ασφαλείας απειλούν διαφορετικά στρώματα της αρχιτεκτονικής του δικτύου και για τον λόγο αυτό στις σύγχρονες προσεγγίσεις βελτιώσεων της ασφάλειας συμπεριλαμβάνονται τα περισσότερα στρώματα. Ωστόσο, αυτές οι προσεγγίσεις αφορούν κυρίως τα ανώτερα του φυσικού επιπέδου στρώματα, ενώ, μόλις πρόσφατα, άρχισε να αυξάνεται το ενδιαφέρον για τις τεχνικές βελτίωσης της ασφάλειας μέσω του φυσικού στρώματος [8]. Ας σημειωθεί ότι με τον συνδυασμό διαφορετικών μεθόδων μπορούν να επιτευχθούν σημαντικά αποτελέσματα. Για παράδειγμα, η αυθεντικότητα των χρηστών μπορεί να επιτευχθεί μέσω συνδυασμού διάφορων μεθόδων πιστοποίησης, όπως η πιστοποίηση διεύθυνσης MAC ή ο απλός έλεγχος ταυτότητας με κωδικό. Από την άλλη πλευρά, ένας αριθμός μεθόδων ασφαλείας βελτιώνει την ασφάλεια εμπλέκοντας περισσότερα του ενός επίπεδα του μοντέλου OSI, όπως η παραγωγή μυστικού κλειδιού για κρυπτογραφικούς σκοπούς βασιζόμενο στα φυσικά χαρακτηριστικά της σύνδεσης ή του μέσου της επικοινωνίας.

Οι τεχνικές κρυπτογράφησης χρησιμοποιούν κυρίως μαθηματικά εργαλεία και κρυφά κλειδιά για να πετύχουν την ασφάλεια του συστήματος επικοινωνίας ενάντια σε μη νόμιμες οντότητες. Ο κύριος στόχος της κρυπτογράφησης είναι η διασφάλιση της εμπιστευτικότητας δεδομένων, της ακεραιότητας δεδομένων, της αυθεντικότητας και της μη-αποποίησης διαμέσου των διαφορετικών επιπέδων της αρχιτεκτονικής του δικτύου. Για τον σκοπό αυτό, έχουν αναπτυχθεί η κρυπτογραφία δημόσιου και ιδιωτικού κλειδιού (γνωστές και ως ασύμμετρη και συμμετρική κρυπτογραφία αντίστοιχα). Στην συμμετρική κρυπτογραφία, τα ίδια κλειδιά χρησιμοποιούνται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Ενώ στην ασύμμετρη κρυπτογραφία, χρησιμοποιείται ένα δημόσιο κλειδί για την κρυπτογράφηση του μηνύματος και η αποκρυπτογράφησή του στον δέκτη γίνεται με το αντίστοιχο ιδιωτικό κλειδί, το οποίο αλλάζει από δέκτη σε δέκτη [5]. Χρησιμοποιώντας τις τεχνικές αυτές κρυπτογραφίας, οι οποίες εφαρμόζονται στα ανώτερα στρώματα, ένα λάθος στο λαμβανόμενο μήνυμα οδηγεί σε πολλαπλά λάθη στο αποκρυπτογραφημένο κείμενο. Για τον λόγο αυτό, σε πιο πρόσφατες μελέτες, το προχωρημένο πρότυπο κρυπτογράφησης (advanced encryption standard – AES) συνδυάζεται με την κωδικοποίηση turbo (turbo coding) εξαιτίας της δυνατότητας διόρθωσης λαθών της δεύτερης.

Στο Φυσικό Στρώμα τα σενάρια των επιθέσεων περιλαμβάνουν συνήθως την παρουσία ενός ωτακουστή ο οποίος προσπαθεί να υποκλέψει πληροφορία από την επικοινωνία

μεταξύ κόμβων του δικτύου ή να προκαλέσει ηθελημένη παρεμβολή. Για να αντιμετωπισθούν αυτά τα θέματα έχουν αναπτυχθεί διάφορες τεχνικές όπως η πληροφοριοθεωρητική ασφάλεια (information-theoretic security), η μορφοποίηση δέσμης (beamforming), το συνεργατικό jamming, οι οποίες θα παρουσιαστούν σε επόμενα κεφάλαια (Κεφάλαια 3 και 5). Κρυπτογραφία εφαρμόζεται, επίσης, και στο φυσικό στρώμα με την τεχνική της φασματικής εξάπλωσης (spread spectrum – SS), στην οποία γίνεται εξάπλωση του εύρους συχνοτήτων του βασικού σήματος με σκοπό τη προστασία του από ωτακουστές, παρεμβολές κτλ. Υπάρχουν δύο βασικές μεθοδολογίες της τεχνικής αυτής: η φασματική εξάπλωση με αναπήδηση συχνότητας (frequency hopping spread spectrum – FHSS) και η φασματική εξάπλωση άμεσης ακολουθίας στοιχείων (direct sequence spread spectrum – DSSS). Στη πρώτη μεθοδολογία, η συχνότητα του φέροντος αλλάζει συχνά ώστε οι μη εξουσιοδοτημένες οντότητες να αδυνατούν να προσεγγίσουν το σήμα του φέροντος. Στη δεύτερη, το βασικό σήμα πληροφορίας πολλαπλασιάζεται με σήμα ψευδοθορύβου ανεξάρτητου από το σήμα πληροφορίας και στη συνέχεια το προκύπτον σήμα μεταδίδεται χωρίς ο μη-εξουσιοδοτημένος κόμβος να μπορεί να ανακτήσει το αρχικό σήμα [4]. Οι τεχνικές της φασματικής εξάπλωσης χρησιμοποιούν κλειδιά μικρότερου μήκους σε σχέση με την κρυπτογράφηση στα ανώτερα στρώματα, αλλά από την άλλη πλευρά αυξάνουν το χρησιμοποιούμενο εύρος συχνοτήτων.

Στο υπόστρωμα MAC, για την αντιμετώπιση των επιθέσεων πλημμυρίσματος μπορούν να γίνουν περιορισμοί στον αριθμό των διευθύνσεων MAC τους οποίους θα λαμβάνει κάθε θύρα.

Επιπρόσθετα, η προστατευμένη πρόσβαση Wi-Fi (Wi-Fi protected access –WPA) και η προστατευμένη πρόσβαση Wi-Fi 2 (WPA 2) είναι δύο ευρέως χρησιμοποιούμενα πρωτόκολλα στο Στρώμα Δικτύου. Επιπλέον, για την αντιμετώπιση των επιθέσεων δρομολόγησης έχει αναπτυχθεί η δεύτερη έκδοση του πρωτοκόλλου δρομολόγησης πληροφοριών (routing information protocol – RIP-V2).

Για την ασφάλεια του Στρώματος Μετάδοσης, χρησιμοποιούνται τα πρωτόκολλα ασφάλεια στρώματος μετάδοσης (transport layer security – TLS) και στρώμα ασφαλών υποδοχών (secure sockets layer – SSL), τα οποία στην ουσία εφαρμόζουν κρυπτογραφία.

Τέλος, στο Στρώμα Εφαρμογής η απλή συνήθης τεχνική για την βελτίωση της ασφάλεια είναι η χρήση ονόματος χρήστη και κωδικού.

Βιβλιογραφία - Αναφορές 2ου Κεφαλαίου

[1] Φ. Κωνσταντίνου, Α. Κανάτας, Γ. Πάντος, *Συστήματα Κινητών Επικοινωνιών,* Παπασωτηρίου, 2013.

[2] Y. Zou, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances and future trends", to appear in Proceedings of the IEEE, 2015.

[3] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks", *IEEE Transactions on Wireless Communications*, vol. 5, no. 9, pp. 2569-2577, September 2006.

[4] Y. Shiu, S. Y. Chang, H. Wu, S. C. Huang, and H. Chen, "Physical layer security in wireless networks: a tutorial", in *Wireless Communications, IEEE*, vol.18, no.2, pp.66-74, April 2011.

[5] A. Menezes, P. Oorschot, and S. Vanstone, *Handbook of applied Cryptography*, CRC press, 1996.

[6] G. Vikram, S. Krishnamurthy, and M. Faloutsos, "Denial of service attacks at the MAC layer in wireless ad hoc networks", in *MILCOM Proceedings, IEEE,* vol. 2, pp. 1118-1123, 2002.

[7] C. Sean, "Hacking Layer 2: Fun with Ethernet Switches", *Blackhat* [Online Document], 2002.

[8] B. Matthieu, J. Barros, *Physical-layer security: from information theory to security engineering*, Cambridge University Press, 2011.

3

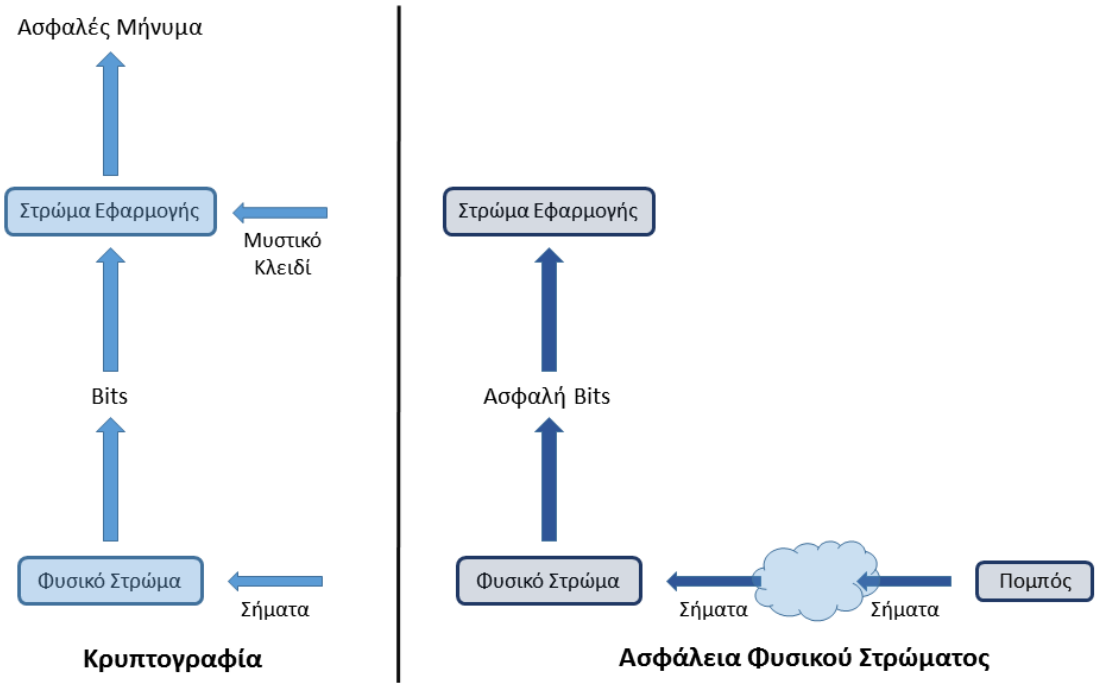
Ασφαλεια Φυσικου Στρωματος

Οι επικοινωνίες στα ασύρματα δίκτυα είναι ιδιαίτερα ευάλωτες σε επιθέσεις ασφαλείας εξαιτίας των εγγενών χαρακτηριστικών του μέσου μετάδοσης. Τα δύο θεμελιώδη χαρακτηριστικά του ασύρματου μέσου μετάδοσης, η ευρυεκπομπή (broadcast) και η υπέρθεση (superposition), παρουσιάζουν διαφορετικές προκλήσεις στην εξασφάλιση αξιόπιστων ή/και ασφαλών επικοινωνιών παρουσία κακόβουλων χρηστών, όπως μη-εξουσιοδοτημένων χρηστών, αναξιόπιστων κόμβων κ.α. Το χαρακτηριστικό της ευρυεκπομπής στις ασύρματες επικοινωνίες, δηλαδή της διάδοσης προς όλες τις κατευθύνσεις στον χώρο του ηλεκτρομαγνητικού κύματος, έχει ως αποτέλεσμα την άφιξη των μεταδιδόμενων σημάτων σε πολλούς ανεπιθύμητους χρήστες. Οι κακόβουλοι χρήστες, οι οποίοι εκμεταλλευόμενοι το χαρακτηριστικό αυτό προσπαθούν να υποκλέψουν πληροφορία από μία εν εξελίξει επικοινωνία χωρίς να γίνουν αντιληπτοί, ονομάζονται, όπως προαναφέρθηκε στο Κεφάλαιο 2, ωτακουστές και οι αντίστοιχες επιθέσεις τους ονομάζονται παθητικές επιθέσεις ασφαλείας. Από την άλλη πλευρά, το χαρακτηριστικό της υπέρθεσης στο ασύρματο μέσο, της δυνατότητας δηλαδή ουδέτερων χρηστών να εμπλακούν/παρεμβάλλουν στην επικοινωνία ενός ζευγαριού στο δίκτυο, επιτρέπει σε έναν κακόβουλο πομπό (jammer) να μεταδώσει σήματα παρεμβολής ώστε να υποβαθμίσει το κανάλι του νόμιμου δέκτη. Η ενέργεια αυτή καλείται jamming και ανήκει στις ενεργητικές επιθέσεις ασφαλείας. Το συγκεκριμένο κεφάλαιο, όπως και τα Κεφάλαια 4 και 5, ασχολείται με την αντιμετώπιση των παθητικών επιθέσεων ασφαλείας και συγκεκριμένα της ωτακουστίας (eavesdropping). Ωστόσο, είναι σημαντικό να αναφερθεί εδώ ότι στο Κεφάλαιο 5, προτείνεται συνεργατική τεχνική όπου χρησιμοποιείται jamming για την αντιμετώπιση των παθητικών ωτακουστών.

Χρησιμοποιώντας το μοντέλο OSI ως μοντέλο αναφοράς, τα μέτρα ασφαλείας για την προστασία των δεδομένων που ανταλλάσσονται μεταξύ των χρηστών ενός ασύρματου δικτύου συνήθως λαμβάνουν χώρα σε ανώτερα του φυσικού στρώματος επίπεδα και

χρησιμοποιούν κυρίως κρυπτογραφικές τεχνικές, όπως η συμμετρική και η ασύμμετρη κρυπτογραφία (βλέπε Κεφάλαιο 2). Ωστόσο, οι τεχνικές κρυπτογράφησης βασίζονται στην παραδοχή ότι οι αντίπαλοι διαθέτουν περιορισμένη υπολογιστική ισχύ ώστε να καθίσταται αδύνατο να αποκρυπτογραφήσουν το μήνυμα χωρίς τη γνώση του μυστικού κλειδιού. Με την ταχεία ανάπτυξη των υπολογιστικών συστημάτων η παραδοχή αυτή καθίσταται πλέον αμφισβητήσιμη, δεδομένου ότι αλγόριθμοι κρυπτογράφησης (ciphers) οι οποίοι θεωρούνταν πρακτικώς «άτρωτοι» στο παρελθόν, σήμερα λόγω της συνεχής ανάπτυξης της υπολογιστικής ισχύος θεωρούνται ευάλωτοι [1]. Έτσι, οι αδυναμίες που εμφανίζουν πολλές εφαρμοσμένες τεχνικές κρυπτογράφησης [2], η έλλειψη θεμελιωδών αποδείξεων της δυσκολίας του προβλήματος αποκρυπτογράφησης που οι αντίπαλοι θα έχουν να αντιμετωπίσουν, αλλά και η αυξανόμενη υπολογιστική ισχύ ωθούν στην αναζήτηση αποδεδειγμένα «άτρωτων» μεθόδων ασφαλείας.

Στο πλαίσιο αυτό, αναδύεται ο τομέας της ασφάλειας στο φυσικό στρώμα (physical layer security), όπου έρχεται να ενισχύσει ακόμη περισσότερο την ασφάλεια των επικοινωνιών, λαμβάνοντας υπόψη τις ιδιαιτερότητες του ασύρματου μέσου μετάδοσης (π.χ. την τυχαιότητα του ασύρματου καναλιού), αλλά και τη γεωγραφική θέση των χρηστών που επιθυμούν να ανταλλάξουν πληροφορίες με ασφάλεια και αξιοπιστία. Σκοπός της είναι να ελαχιστοποιήσει το μέγεθος των δεδομένων που θα διαρρεύσουν σε μη-εξουσιοδοτημένους χρήστες ώστε να είναι αδύνατο να αποκτήσουν έμπιστες πληροφορίες. Οι πρώτες θεωρητικές μελέτες στην ασφάλεια φυσικού στρώματος, οι οποίες βασίστηκαν στην πληροφοριοθεωρητική (information-theoretic) προσέγγιση της ασφάλειας που εισήγαγε ο Shannon στο [3], πραγματοποιήθηκαν αρχικά από τον Wyner το 1975 [4] και στη συνέχεια από τους Cziszár και Körner το 1978 [5].



Σχήμα 3.1: Διαφορά μεταξύ κρυπτογραφίας και τεχνικών ασφαλείας φυσικού στρώματος.

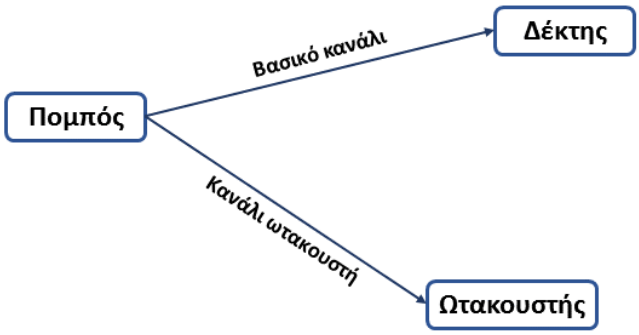
Στο Σχήμα 3.1 απεικονίζεται η θεμελιώδης διαφορά μεταξύ της κρυπτογραφίας και των τεχνικών ασφαλείας του φυσικού στρώματος: η κρυπτογραφία εφαρμόζεται κατά κόρον στα ανώτερα στρώματα του μοντέλου OSI, όπως το στρώμα εφαρμογής, και απαιτεί την

ύπαρξη μυστικού κλειδιού, ενώ η ασφάλεια φυσικού στρώματος περιλαμβάνει τις τεχνικές ασφαλείας που εφαρμόζονται στο φυσικό στρώμα και ουσιαστικά δεν χρησιμοποιούν μυστικά κλειδιά. Αξίζει να σημειωθεί ότι δεδομένης της ανεξαρτησίας των στρωμάτων του μοντέλου OSI, η εφαρμογή τεχνικών ασφαλείας στο φυσικό στρώμα δεν εμποδίζει τις μεθόδους ασφαλείας των ανωτέρων στρωμάτων. Συνεπώς, τεχνικές ασφαλείας διαφορετικών επιπέδων μπορούν να εφαρμοστούν ταυτόχρονα ώστε να επιτευχθούν ακόμη καλύτερα αποτελέσματα. Ο συνδυασμός μεθόδων ασφαλείας διαφορετικών επιπέδων (cross-layer security) έχει διερευνηθεί σε πρόσφατες μελέτες, όπως στην [6].

Σκοπός του κεφαλαίου αυτού είναι η παρουσίαση των βασικών εννοιών της ασφάλειας στο φυσικό στρώμα καθώς και η διερεύνηση της επίδρασης των χαρακτηριστικών του ασύρματου καναλιού στην ασφάλεια του στρώματος αυτού. Αρχικά, εισάγονται οι έννοιες που περιγράφουν το βασικό μοντέλο της ασφάλειας φυσικού στρώματος στα ασύρματα δίκτυα, όπως το κανάλι υποκλοπής (wiretap channel) και η πληροφορία της κατάστασης καναλιού (channel state information – CSI). Στη συνέχεια, παρουσιάζονται οι μετρικές (metrics) που χαρακτηρίζουν την επίδοση των μεθόδων ασφαλείας που εφαρμόζονται στο φυσικό στρώμα. Για την καλύτερη κατανόηση των μετρικών αναλύεται η ασφάλεια φυσικού στρώματος για ασύρματα κανάλια διαλείψεων Rayleigh εξάγοντας και αξιολογώντας τα αποτελέσματα. Τέλος, γίνεται μία σύντομη ανασκόπηση των σημαντικότερων τεχνικών ασφαλείας που αφορούν το φυσικό στρώμα.

3.1 Βασικές Έννοιες Ασφάλειας Φυσικού Στρώματος

Το απλούστερο δίκτυο, για το οποίο προκύπτουν θέματα ασφαλείας, είναι αυτό που αποτελείται από έναν πομπό (transmitter), έναν δέκτη (receiver) και έναν ωτακουστή (eavesdropper) (Σχήμα 3.2). Ο πομπός προτίθεται να στείλει ένα ιδιωτικό μήνυμα στον δέκτη, μέσω ασύρματης επικοινωνίας, χωρίς ο ωτακουστής να μπορέσει να αντλήσει πληροφορία. Ο Wyner, στην πρωτοποριακή του εργασία [4], ονόμασε το βασικό μοντέλο του Σχήματος 3.2 ως μοντέλο καναλιού υποκλοπής (wiretap channel model), αφού το ασύρματο κανάλι μεταξύ πομπού και δέκτη (βασικό κανάλι – main channel) επιτρέπει τη διαρροή πληροφορίας προς ανεπιθύμητους δέκτες, δημιουργείται έτσι το κανάλι του ωτακουστή το οποίο ονομάζεται και κανάλι υποκλοπής. Στη συνέχεια ο όρος wiretap κανάλι επεκτάθηκε με τον όρο κανάλι ευρυεκπομπής (broadcast channel) από τους Cziszár και Körner στο [5].



Σχήμα 3.2: Βασικό μοντέλο ασύρματης επικοινωνίας μεταξύ ενός πομπού και ενός νόμιμου δέκτη, παρουσία ενός παθητικού ωτακουστή.

Με βάση το σύστημα του Σχήματος 3.2 παρουσιάζονται στη συνέχεια οι βασικότερες μετρικές της απόδοσης της ασφάλειας στο φυσικό στρώμα.

3.1.1 Πληροφορία κατάστασης καναλιού

Ένα βασικό χαρακτηριστικό που καθορίζει τις μεθόδους ασφαλείας στο φυσικό στρώμα είναι κατά πόσο ο πομπός γνωρίζει την κατάσταση του καναλιού (CSI) προς τον δέκτη (main channel) και προς τον ωτακουστή (eavesdropper's channel) αντίστοιχα. Οι βασικές πληροφορίες για τα κανάλια αυτά που ο πομπός επιθυμεί να γνωρίζει είναι η χωρητικότητά τους, οι συντελεστές των δύο καναλιών, η θέση του δέκτη και του ωτακουστή.

Στα απλούστερα σενάρια γίνεται η υπόθεση ότι ο πομπός διαθέτει πλήρη CSI, δηλαδή γνωρίζει τη χωρητικότητα και τους συντελεστές των δύο καναλιών. Στην πράξη όμως υπάρχουν πολλοί λόγοι οι οποίοι προκαλούν ατέλειες στην CSI, οδηγώντας είτε σε μερική ή καθόλου γνώση της, είτε σε στατιστική γνώση της. Τέτοιοι λόγοι μπορεί να είναι οι εξής:

- Δεν υπάρχει ανάδραση από την πλευρά του ωτακουστή. Δεδομένου ότι ο ωτακουστής είναι παθητικός δεν μεταδίδει σήματα για να εντοπιστεί η θέση του και να αποκτηθούν πληροφορίες για το κανάλι του.
- Οι δέκτες πολλές φορές παρέχουν μερική γνώση της CSI λόγω του σηματοθορυβικού λόγου (signal-to-noise ratio – SNR).
- Οι συνδέσεις μεταξύ πομπού και δέκτη είναι ατελείς. Πολλές φορές γίνονται λάθη στη μετάδοση του σήματος ή υπάρχει καθυστέρηση.
- Λανθασμένη εκτίμηση της κατάστασης των καναλιών μπορεί να οφείλεται στις απώλειες που παρουσιάζουν τα ασύρματα κανάλια και την χρονομεταβλητότητα λόγω των διαλείψεων.

3.1.2 Χωρητικότητα ασφαλείας

Η θεμελιώδης μετρική ασφάλειας που χρησιμοποιείται στην ασφάλεια φυσικού στώματος καλείται *χωρητικότητα ασφαλείας (secrecy capacity)*. Είναι ο μέγιστος ασφαλής ρυθμός του συστήματος, δηλαδή ο μέγιστος ρυθμός μετάδοσης μεταξύ πομπού και δέκτη για τον οποίο ο ωτακουστής δεν είναι σε θέση να υποκλέψει πληροφορία.

Στην [4] ο Wyner, για το απλό μοντέλο του Σχήματος 3.2 θεώρησε θορυβώδη κανάλια χωρίς μνήμη, όπου το κανάλι του ωτακουστή αποτελεί μία υποβαθμισμένη έκδοση του βασικού καναλιού. Στην περίπτωση αυτή όρισε τη χωρητικότητα ασφαλείας ως τη διαφορά των χωρητικοτήτων Shannon των δύο καναλιών ως εξής:

$$C_S = C_M - C_E \tag{3.1}$$

όπου C_M , C_E οι χωρητικότητες Shannon του βασικού καναλιού και του καναλιού του ωτακουστή αντίστοιχα.

Στην [7] μελετήθηκαν τα κανάλια λευκού προσθετικού γκαουσιανού θορύβου (Additive White Gaussian Noise – AWGN) και αποδείχθηκε ότι εάν και τα δύο κανάλια είναι Gaussian κανάλια, η χωρητικότητα ασφαλείας δίνεται από τη σχέση (3.1) στην περίπτωση που η διαφορά είναι θετική, αλλιώς είναι μηδενική, όπως φαίνεται στην παρακάτω εξίσωση:

$$C_S = \left[C_M - C_E\right]^+ \tag{3.2}$$

όπου $[x]^+ = \max\{x, 0\}$. Συνεπώς, ασφαλής επικοινωνία μπορεί να επιτευχθεί εφόσον ο δέκτης διαθέτει καλύτερο κανάλι από τον ωτακουστή.

3.1.2.1 Εργοδική χωρητικότητα ασφαλείας

Η εργοδική χωρητικότητα ασφαλείας ισούται με τη μέση τιμή της χωρητικότητας ασφαλείας:

$$\bar{C}_S = E[C_S] \tag{3.3}$$

και χρησιμοποιείται σε χρονομεταβλητά συστήματα, όπου προκύπτουν εργοδικά δεδομένα για την κατάσταση του συστήματος. Η χωρητικότητα ασφαλείας υπολογίζεται μέσω της (3.2) για κάθε διαφορετική κατάσταση του συστήματος.

3.1.3 Πιθανότητα μη-μηδενικής χωρητικότητας ασφαλείας

Η πιθανότητα ύπαρξης μη-μηδενικής (αυστηρά θετικής) χωρητικότητας ασφαλείας είναι μία παράμετρος ασφαλείας η οποία χαρακτηρίζει τα κανάλια με διαλείψεις και δίνεται από την εξής σχέση:

$$\Pr[C_S > 0] = \Pr[C_M > C_W] \tag{3.4}$$

3.1.4 Πιθανότητα αποκοπής ασφαλείας

Η πιθανότητα αποκοπής (outage probability) συναρτήσει ενός επιθυμητού ρυθμού ασφαλείας, χρησιμοποιείται επίσης σε κανάλια με διαλείψεις και ισούται με την πιθανότητα η χωρητικότητα ασφαλείας να είναι μικρότερη ενός επιθυμητού ρυθμού ασφαλείας $R_S > 0$ (target secrecy rate):

$$\Pr_{out}\left[R_S\right] = \Pr[C_S < R_S] \tag{3.5}$$

3.2 Χωρητικότητα Ασφαλείας Rayleigh Καναλιών

Στην ενότητα αυτή, μελετάται το πρόβλημα προσδιορισμού της χωρητικότητας ασφαλείας για κανάλια με διαλείψεις Rayleigh. Στη συνέχεια, μέσω προσομοιώσεων αξιολογείται η απόδοση της πληροφοριοθεωρητικής ασφάλειας φυσικού στρώματος (information-theoretic physical layer security) για τα Rayleigh κανάλια.

3.2.1 Μοντέλο συστήματος

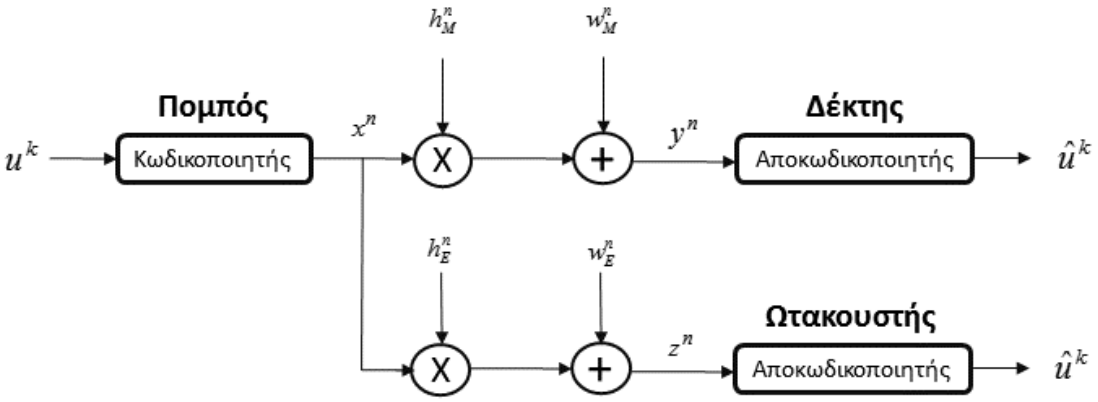
Όμοια με το μοντέλο του Σχήματος 3.2, στο Σχήμα 3.3 θεωρείται το πρόβλημα όπου ένας νόμιμος χρήστης προτίθεται να στείλει το μήνυμα u σε έναν άλλον χρήστη. Κάθε κομμάτι του μηνύματος u^k κωδικοποιείται στην κωδική λέξη (codeword) $x^n = \left[x(1), ..., x(i), ..., x(n)\right]$ και μεταδίδεται προς τον δέκτη μέσω χρονοδιακριτού Rayleigh καναλιού (το βασικό κανάλι). Ένας τρίτος μη-εξουσιοδοτημένος χρήστης (ωτακουστής) παρακολουθεί την επικοινωνία μεταξύ του νόμιμου ζευγαριού μέσω επίσης χρονοδιακριτού Rayleigh καναλιού (το κανάλι του ωτακουστή ή κανάλι υποκλοπής).

Οι έξοδοι των δύο καναλιών δίνονται αντίστοιχα από τις σχέσεις:

$$y(i) = g_M(i)x(i) + w_M(i) \tag{3.6}$$

$$z(i) = g_E(i)x(i) + w_E(i) \tag{3.7}$$

όπου $g_M(i)$, $g_E(i)$ οι συντελεστές των δύο καναλιών και $w_M(i)$, $w_E(i)$ οι προσθετικοί θόρυβοι. Ο θόρυβος θεωρείται AWGN μηδενικής μέσης τιμής και διακύμανσης N_M και N_E για κάθε κανάλι αντίστοιχα. Το βασικό κανάλι και το κανάλι του ωτακουστή θεωρούνται και quasi-static, δηλαδή οι συντελεστές των καναλιών είναι μεν τυχαίες μεταβλητές αλλά παραμένουν σταθερές και ανεξάρτητες για τη μετάδοση κάθε κωδικής λέξης, συνεπώς $g_M(i) = g_M$, $g_E(i) = g_E, \forall i$.



Σχήμα 3.3: Μοντέλο επικοινωνίας μεταξύ πομπού και δέκτη, παρουσία ωτακουστή για κανάλια Rayleigh.

Οι στιγμιαίοι SNRs στην είσοδο του δέκτη και του ωτακουστή δίνονται αντίστοιχα από τις σχέσεις:

$$\gamma_M(i) = \frac{h_M(i)P}{N_M} = \frac{h_M P}{N_M} = \gamma_M \tag{3.8}$$

$$\gamma_E(i) = \frac{h_E(i)P}{N_E} = \frac{h_E P}{N_E} = \gamma_E \tag{3.9}$$

όπου $h_M(i) = |g_M(i)|^2 = |g_M|^2 = h_M$ και $h_E(i) = |g_E(i)|^2 = |g_E|^2 = h_E$ τα κέρδη ισχύος των δύο καναλιών αντίστοιχα και P η ισχύς μετάδοσης του πομπού. Επιπλέον, η στιγμιαία χωρητικότητα (ανηγμένη ως προς το εύρος ζώνης) δίνεται αντίστοιχα για κάθε κανάλι από τις σχέσεις:

$$C_M = \log_2(1 + \gamma_M) \tag{3.10}$$

$$C_E = \log_2(1 + \gamma_E) \tag{3.11}$$

Επομένως, η στιγμιαία χωρητικότητα ασφαλείας του μελετώμενου συστήματος δίνεται, επίσης, από τη σχέση (3.2).

Στην περίπτωση που ο πομπός διαθέτει πλήρη CSI και άρα γνωρίζει τους στιγμιαίους SNRs των δύο καναλιών, μέσω των σχέσεων (3.10) και (3.11) προκύπτει:

$$C_S = \begin{cases} \log_2(1+\gamma_M) - \log_2(1+\gamma_E), & \text{για } \gamma_M > \gamma_E, \\ 0, & \text{για } \gamma_M \le \gamma_E \end{cases} \tag{3.12}$$

3.2.2 Εργοδική χωρητικότητα ασφαλείας Rayleigh καναλιών

Η εργοδική χωρητικότητα ασφαλείας των καναλιών Rayleigh δίνεται με τη βοήθεια της σχέσης (3.3), ολοκληρώνοντας για όλες τις καταστάσεις των δύο καναλιών [8]:

$$\overline{C}_S = \int_0^\infty \int_0^\infty \left[\log_2(1+\gamma_M) - \log_2(1+\gamma_E)\right]^+ f(\gamma_M) f(\gamma_E) d\gamma_M d\gamma_E \tag{3.13}$$

όπου $f(\gamma_M)$, $f(\gamma_E)$ οι συναρτήσεις πυκνότητας πιθανότητας (probability density functions – pdfs) των SNRs των δύο καναλιών. Δεδομένου ότι τα κανάλια υπόκεινται σε διαλείψεις Rayleigh, οι pdfs των κερδών ισχύος των δύο καναλιών ακολουθούν την εκθετική κατανομή (βλ. Κεφάλαιο 1) και δίνονται από τη σχέση:

$$f(h_x) = \frac{1}{\overline{h}_x} \exp\left(-\frac{h_x}{\overline{h}_x}\right) \tag{3.14}$$

όπου *x* = *M* ή *E*. Υπενθυμίζεται ότι $\overline{h}_M = \mathrm{E}\{h_M\}$ και $\overline{h}_\mathrm{E} = \mathrm{E}\{h_\mathrm{E}\}$ είναι οι μέσες τιμές των κερδών ισχύος του βασικού καναλιού και του καναλιού υποκλοπής, αντίστοιχα. Αναλογικά, οι pdfs των SNRs των δύο καναλιών δίνονται από τη σχέση:

$$f(\gamma_x) = \frac{1}{\overline{\gamma}_x} \exp\left(-\frac{\gamma_x}{\overline{\gamma}_x}\right) \tag{3.15}$$

όπου $\overline{\gamma}_x = \dfrac{\overline{h}_x P}{N_x}$. Με βάση τις σχέσεις (3.8) και (3.9), η σχέση (3.13) γράφεται ως εξής:

$$\overline{C}_S = \int_0^\infty \int_0^\infty \left[\log_2\left(1+\frac{h_M P}{N_M}\right) - \log_2\left(1+\frac{h_E P}{N_E}\right)\right]^+ f(h_M) f(h_E) dh_M dh_E \tag{3.16}$$

Στην περίπτωση που ο πομπός διαθέτει πλήρη CSI και για τα δύο κανάλια, τότε μπορεί να μεταδίδει μόνο όταν το βασικό κανάλι είναι καλύτερο από το κανάλι υποκλοπής, δηλαδή όταν $\gamma_M > \gamma_E$ ή, αντίστοιχα, $h_M > h_E$ και η εργοδική χωρητικότητα ασφαλείας προκύπτει ως εξής:

$$\overline{C}_S^{(F)} = \int_0^\infty \int_{\gamma_E}^\infty \left[\log_2(1+\gamma_M) - \log_2(1+\gamma_E)\right] f(\gamma_M) f(\gamma_E) d\gamma_M d\gamma_E \tag{3.17}$$

3.2.3 Ύπαρξη χωρητικότητας ασφαλείας

Η πιθανότητα ύπαρξης της χωρητικότητας ασφαλείας δίνεται από τη σχέση (3.4):

$$\Pr[C_S > 0] = \Pr[C_M > C_W] = \Pr[\gamma_M > \gamma_W] \tag{3.18}$$

και λαμβάνοντας υπόψη ότι οι SNRs των δύο καναλιών είναι τυχαίες, ανεξάρτητες μεταξύ τους, μεταβλητές που ακολουθούν την εκθετική κατανομή (βλ. σχέση (3.15)) η σχέση (3.18) γράφεται ως εξής:

$$\begin{aligned}\Pr[C_S > 0] &= \int_0^{\infty}\int_0^{\gamma_M} f\left(\gamma_M,\gamma_E\right)d\gamma_E d\gamma_M \\ &= \int_0^{\infty}\int_0^{\gamma_M} f\left(\gamma_M\right)f\left(\gamma_E\right)d\gamma_E d\gamma_M \\ &= \frac{\overline{\gamma}_M}{\overline{\gamma}_M+\overline{\gamma}_E}\end{aligned} \tag{3.19}$$

Το ενδιαφέρον αποτέλεσμα της σχέσης (3.19) είναι ότι πιθανότητα μη-μηδενικής χωρητικότητας ασφαλείας υφίσταται ακόμα και στην περίπτωση όπου ο μέσος SNR του βασικού καναλιού είναι μικρότερος από τον SNR του καναλιού υποκλοπής.

Η πιθανότητα αποκοπής συναρτήσει ενός επιθυμητού ρυθμού ασφαλείας $R_S > 0$ δίνεται από τη σχέση (3.5) και με τη βοήθεια του θεωρήματος ολικής πιθανότητας (total probability theorem) γράφεται ως εξής:

$$\Pr_{out}[R_S] = \Pr[C_S < R_S \mid \gamma_M > \gamma_{\mathrm{E}}]\Pr[\gamma_M > \gamma_{\mathrm{E}}] + \Pr[C_S < R_S \mid \gamma_M \le \gamma_{\mathrm{E}}]\Pr[\gamma_M \le \gamma_{\mathrm{E}}] \tag{3.20}$$

Ισχύει ότι

$$\Pr[\gamma_M \le \gamma_{\mathrm{E}}] = 1 - \Pr[\gamma_M > \gamma_{\mathrm{E}}] \overset{(3.19)}{=} \frac{\overline{\gamma}_{\mathrm{E}}}{\overline{\gamma}_M+\overline{\gamma}_E} \tag{3.21}$$

καθώς και

$$\begin{aligned}\Pr[C_S < R_S \mid \gamma_M > \gamma_{\mathrm{E}}] &= \Pr[\log_2\left(1+\gamma_M\right) - \log_2\left(1+\gamma_E\right) < R_S \mid \gamma_M > \gamma_{\mathrm{E}}] \\ &= \Pr[\gamma_M < 2^{R_S}(1+\gamma_E) - 1 \mid \gamma_M > \gamma_{\mathrm{E}}] \\ &= \int_0^{\infty}\int_{\gamma_E}^{2^{R_S}(1+\gamma_E)-1} f\left(\gamma_M,\gamma_E \mid \gamma_M > \gamma_{\mathrm{E}}\right)d\gamma_E d\gamma_M \\ &= \int_0^{\infty}\int_{\gamma_E}^{2^{R_S}(1+\gamma_E)-1} \frac{f\left(\gamma_M\right)f\left(\gamma_E\right)}{f\left(\gamma_M > \gamma_{\mathrm{E}}\right)}d\gamma_E d\gamma_M \\ &= 1 - \frac{\overline{\gamma}_M+\overline{\gamma}_E}{\overline{\gamma}_M+2^{R_S}\overline{\gamma}_E}\exp\left(-\frac{2^{R_S}-1}{\overline{\gamma}_M}\right)\end{aligned} \tag{3.22}$$

Επιπρόσθετα, επειδή $R_S > 0$, ισχύει ότι

$$\Pr[C_S < R_S \mid \gamma_M \le \gamma_{\mathrm{E}}] = 1 \tag{3.23}$$

Αντικαθιστώντας τις εξισώσεις (3.19), (3.21), (3.22) και (3.23) στην (3.20) προκύπτει η ακόλουθη σχέση για την πιθανότητα αποκοπής ασφαλείας:

$$\Pr_{out}[R_S] = 1 - \frac{\overline{\gamma}_M}{\overline{\gamma}_M+2^{R_S}\overline{\gamma}_E}\exp\left(-\frac{2^{R_S}-1}{\overline{\gamma}_M}\right) \tag{3.24}$$

Ενδιαφέρον παρουσιάζει η ασυμπτωτική συμπεριφορά της πιθανότητας αποκοπής για ακραίες τιμές των τιμών R_S, $\overline{\gamma}_M$ και $\overline{\gamma}_E$. Συγκεκριμένα, από την (3.24) προκύπτει ότι όταν

$R_S \to 0$ τότε $\Pr_{out}[R_S] \to \frac{\overline{\gamma}_E}{\overline{\gamma}_M + \overline{\gamma}_E}$, ενώ όταν $R_S \to \infty$ τότε $\Pr_{out}[R_S] \to 1$, δηλαδή καθίσταται αδύνατο για τον πομπό να μεταδώσει ασφαλή πληροφορία (σε τόσο υψηλούς ρυθμούς). Επιπλέον, όταν $\overline{\gamma}_M \gg$ η σχέση (3.24) γίνεται $\Pr_{out}[R_S] \approx 1 - \exp\left(-\frac{2^{R_S}-1}{\overline{\gamma}_M}\right)$ και όταν $\overline{\gamma}_M \ll$ τότε $\Pr_{out}[R_S] \approx 1$, πάλι δηλαδή γίνεται αποκοπή επικοινωνίας μεταξύ του πομπού και νόμιμου δέκτη.

3.2.4 Αποτελέσματα προσομοιώσεων

Στην ενότητα αυτή παρουσιάζονται οι προσομοιώσεις που εκτελέστηκαν για την αξιολόγηση της χωρητικότητας ασφαλείας στην πληροφοριοθεωρητική ασφάλεια φυσικού στρώματος και της συμπεριφοράς της πιθανότητας αποκοπής για κανάλια που υπόκεινται σε διαλείψεις Rayleigh. Μέσω των προσομοιώσεων αυτών εξάγονται σημαντικά αποτελέσματα για την επίδραση των καναλιών με διαλείψεις στην ασφάλεια φυσικού στρώματος. Όλες οι προσομοιώσεις αφορούν το μοντέλο συστήματος του Σχήματος 3.2 με βάση την παραπάνω ανάλυση.

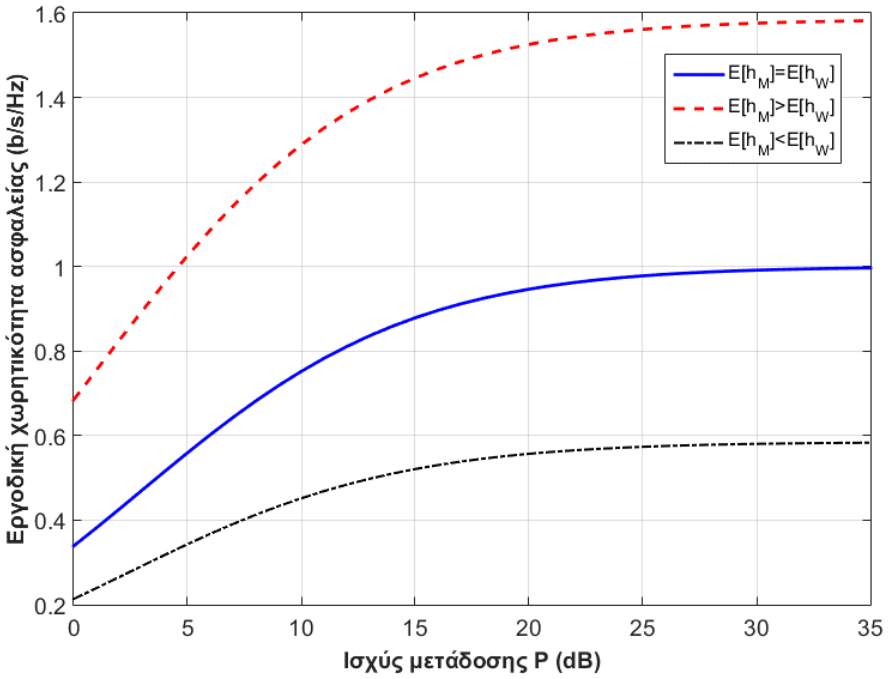
Για τις συγκεκριμένες προσομοιώσεις θεωρείται ότι ο πομπός διαθέτει πλήρη CSI για το βασικό κανάλι, ενώ γνωρίζει τη μέση τιμή του κέρδους ισχύος του καναλιού υποκλοπής (μερικό CSI). Έτσι, για τον υπολογισμό της εργοδικής χωρητικότητας χρησιμοποιείται η σχέση (3.16), ενώ ο πομπός, μη διαθέτοντας πλήρη CSI του καναλιού του ωτακουστή, μεταδίδει με σταθερή ισχύ ίση με την ισχύ που δίνεται κάθε φορά. Εάν διέθετε πλήρη CSI και για τα δύο κανάλια, για καλύτερα αποτελέσματα, θα μπορούσε να εφαρμόσει πολιτική βέλτιστης κατανομής ισχύος, η οποία αναλύεται στο επόμενο κεφάλαιο. Επιπλέον, θεωρείται μοναδιαία διακύμανση του θορύβου για τα δύο κανάλια $\left(N_M = N_W = 1\right)$. Τέλος, για την εκτέλεση των προσομοιώσεων χρησιμοποιήθηκε το πρόγραμμα Matlab και ο υπολογισμός των απαραίτητων ολοκληρωμάτων έγινε με αριθμητική ολοκλήρωση.

Στο Σχήμα 3.4 παρουσιάζεται η εργοδική χωρητικότητα ασφαλείας ως προς την ισχύ μετάδοσης για τις ακόλουθες περιπτώσεις:

- Ο δέκτης και ο ωτακουστής διαθέτουν το ίδιο κανάλι κατά μέσο όρο $\left(\overline{h}_M = \overline{h}_E = 1\right)$
- Ο δέκτης διαθέτει χειρότερο (μέσο) κανάλι από τον ωτακουστή $\left(\overline{h}_M = 1 < \overline{h}_E = 2\right)$
- Ο δέκτης διαθέτει καλύτερο (μέσο) κανάλι από τον ωτακουστή $\left(\overline{h}_M = 1 > \overline{h}_E = 2\right)$

Όπως παρατηρείται, μεγαλύτερη εργοδική χωρητικότητα ασφαλείας, συνεπώς μεγαλύτερος ρυθμός μετάδοσης δεδομένων μεταξύ πομπού και δέκτη, προκύπτει στην περίπτωση που το βασικό κανάλι είναι καλύτερο (κατά μέσο όρο) από το κανάλι του ωτακουστή, ενώ μικρότερη $\overline{C}_S$ όταν ο ωτακουστής διαθέτει πιο ικανό κανάλι από το νόμιμο δέκτη. Ακόμη, για μικρές τιμές της ισχύος μετάδοσης (περιοχή 0 έως 10 dB περίπου), όταν υπάρχει αύξηση στη διαθέσιμη ισχύ, αυξάνεται παράλληλα σημαντικά και η χωρητικότητα ασφαλείας, με τον ρυθμό αύξησης να ελαττώνεται σιγά σιγά και τελικά για πολύ μεγάλες τιμές της μέσης ισχύος η χωρητικότητα σταθεροποιείται ασυμπτωτικά σε μια συγκεκριμένη τιμή. Τέλος, το πιο ενδιαφέρον αποτέλεσμα είναι η ύπαρξη θετικής

χωρητικότητας ασφαλείας στην δυσμενή περίπτωση όπου ο ωτακουστής διαθέτει καλύτερο κανάλι προς τον πομπό από τον δέκτη.



Σχήμα 3.4: Εργοδική χωρητικότητα ασφαλείας ως προς την ισχύ μετάδοσης για διάφορες τιμές των $\bar{h}_M$, $\bar{h}_E$.

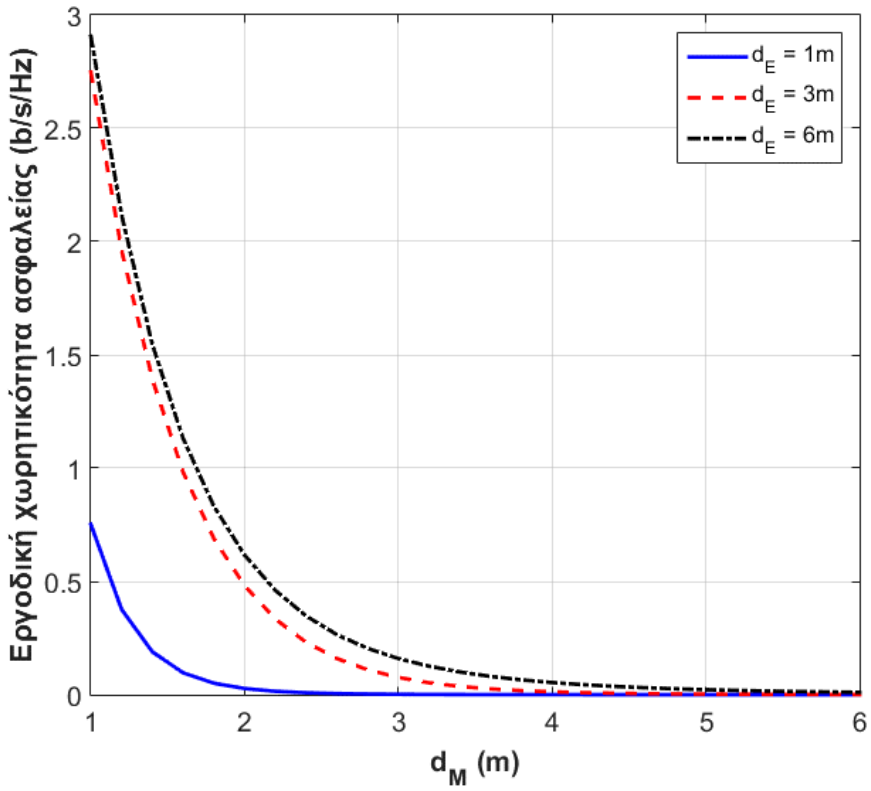
Στο επόμενο σενάριο προσομοίωσης, για μία πιο ρεαλιστική αξιολόγηση της επίδρασης των χαρακτηριστικών του ασύρματου καναλιού, μελετάται η χωρητικότητα ασφαλείας ως προς τις απώλειες διάδοσης. Για το σκοπό αυτό, θεωρείται η περίπτωση του γενικού μοντέλου διάδοσης σε περιβάλλον εσωτερικού χώρου NLoS (ο εκθέτης απωλειών τίθεται ίσος με $c=4$, βλ. Πίνακα 1.1, Κεφάλαιο 1). Επομένως, οι μέσες τιμές των κερδών ισχύος των δύο καναλιών δίνονται, αντίστοιχα, από τις σχέσεις:

$$\bar{h}_M = \frac{1}{d_M^c} \tag{3.25}$$

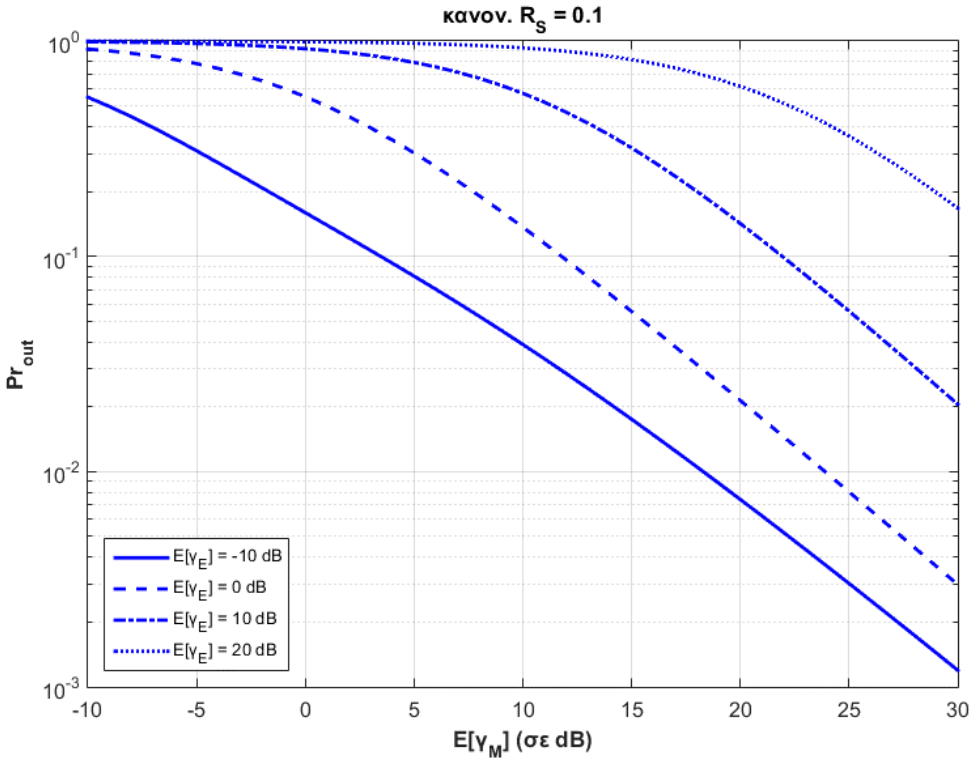
$$\bar{h}_E = \frac{1}{d_E^c} \tag{3.26}$$

όπου d_M, d_E οι αποστάσεις δέκτη και ωτακουστή από τον πομπό, αντίστοιχα.

Στο Σχήμα 3.5 παρουσιάζεται η εργοδική χωρητικότητα ασφαλείας για τρεις θέσεις του ωτακουστή στο σύστημα. Ο πομπός μεταδίδει με σταθερή ισχύ $P=10\,Watt$. Παρατηρείται ότι η χωρητικότητα ασφαλείας έχει υψηλότερες τιμές, δηλαδή η απόδοση της πληροφοριοθεωρητικής ασφάλειας στο φυσικό στρώμα είναι συνεπώς πολύ καλή, όταν ο ωτακουστής βρίσκεται πιο μακριά από τον πομπό σε σχέση με τον δέκτη. Επιπλέον, όπως είναι λογικό καθώς ο δέκτης απομακρύνεται από τον πομπό μειώνεται σημαντικά ο ασφαλής ρυθμός μετάδοσης, καθώς αυξάνονται οι απώλειες διάδοσης δυσχεραίνοντας το βασικό κανάλι. Ωστόσο, θετική χωρητικότητα ασφαλείας επιτυγχάνεται ακόμα και σε περιπτώσεις όπου ο ωτακουστής βρίσκεται πιο κοντά στον πομπό σε σχέση με τον δέκτη (πχ. όταν $d_M=1.5\,m$ και $d_E=1\,m$).



Σχήμα 3.5: Εργοδική χωρητικότητα ασφαλείας σε σχέση με τη θέση του δέκτη για διάφορες θέσεις του ωτακουστή (P=10 Watt).



Σχήμα 3.6: Πιθανότητα αποκοπής για κανονικοποιημένο επιθυμητό ρυθμό ασφαλείας $R_S = 0.1$ σε σχέση με τον μέσο SNR του βασικού καναλιού.

Στην επόμενη προσομοίωση (Σχήμα 3.6), εξετάζεται η πληροφοριοθεωρητική ασφάλεια φυσικού στρώματος από τη σκοπιά της μετρικής της πιθανότητας αποκοπής ασφαλείας. Η προσομοίωση αυτή αφορά το σύστημα του σχήματος 3.2. Η πιθανότητα αποκοπής υπολογίζεται μέσω της σχέσης (3.24) για έναν κανονικοποιημένο επιθυμητό ρυθμό ασφαλείας ίσο με 0.1. Η κανονικοποίηση πραγματοποιείται σε σχέση με την χωρητικότητα του βασικού καναλιού με SNR ίσου με $\overline{\gamma}_M$.

Όπως αναμενόταν, όταν το κανάλι του ωτακουστή είναι σημαντικά καλύτερο του βασικού καναλιού κατά μέση τιμή, η ασφαλής επικοινωνία τείνει να αποκοπεί ($\Pr_{out} \to 1$), ενώ η πιθανότητα αποκοπής είναι σχετικά μικρή ($\Pr_{out} \to 0$) στην αντίθετη περίπτωση. Επίσης, επιβεβαιώνεται και εδώ ότι η επίδραση των διαλείψεων επιτρέπει την επίτευξη θετικού ασφαλή ρυθμού σε περιπτώσεις όπου ο ωτακουστής διαθέτει ικανότερο κανάλι από τον δέκτη.

3.2.5 Συμπεράσματα

Μέσω της πληροφοριοθεωρητικής ασφάλειας φυσικού στρώματος το σύστημα μπορεί να σχεδιαστεί ώστε να πετύχει ένα σημαντικό επίπεδο ασφαλείας, ακόμη και στην περίπτωση που αντίπαλος διαθέτει ικανό κανάλι και ίσως καλύτερο από αυτό του νόμιμου ζευγαριού που επικοινωνεί. Ωστόσο, δεν εγγυάται ασφάλεια με πιθανότητα ένα, καθώς η χωρητικότητα ασφαλείας περιορίζεται σημαντικά από το φαινόμενο των χρονομεταβλητών διαλείψεων που συναντάται στα ασύρματα κανάλια. Επιπλέον, ο υπολογισμός της χωρητικότητας ασφαλείας προϋποθέτει τη γνώση των καναλιών επικοινωνίας πράγμα το οποίο στην πράξη δεν είναι πάντα εφικτό.

3.3 Επισκόπηση Τεχνικών Ασφαλείας Φυσικού Στρώματος

Στο κεφάλαιο αυτό παρουσιάστηκε η πληροφοριοθεωρητική ασφάλεια φυσικού στρώματος, η οποία παρέχει το θεωρητικό υπόβαθρο για τη μελέτη της ασφάλειας του φυσικού στρώματος και ως τεχνική ασφαλείας αποτελεί τη βάση των τεχνικών ασφαλείας που εφαρμόζονται στο φυσικό στρώμα. Τέτοιες τεχνικές είναι οι ασφαλείς on-off μεταδόσεις (secure on-off transmissions), η μορφοποίηση δέσμης (beamforming) οι συνεργατικές τεχνικές(cooperative techniques). Οι παραπάνω τεχνικές ονομάζονται επίσης και τεχνικές επεξεργασίας σήματος (signal processing techniques).

Οι ασφαλείς on-off μεταδόσεις εφαρμόζονται κυρίως σε δίκτυα μονής κεραίας, όπου ο πομπός δεν έχει πλήρη CSI, αλλά μπορεί να το εκτιμήσει κάποιες στιγμές. Εκτιμώντας το στιγμιαίο CSI, ο πομπός αποφασίζει αν θα μεταδώσει προς τον δέκτη ή όχι, μεταδίδοντας πχ. σε στιγμές που ικανοποιούνται κάποιες απαιτήσεις για το CSI με βάσει κάποια δοσμένα κατώφλια τιμών. Στο [9] μελετήθηκε μία απλή on-off μεθοδολογία για Rayleigh κανάλια όπου ο πομπός διαθέτει μερικό CSI του βασικού καναλιού και στατιστικά δεδομένα για το κανάλι του ωτακουστή. Οι He και Zhou στο [10] πρότειναν διάφορες ασφαλείς on-off μεταδόσεις και μελέτησαν την απόδοσή τους ως προς την πιθανότητα αποκοπής ασφαλείας.

Η μορφοποίηση δέσμης εφαρμόζεται σε κανάλια με πολλαπλές κεραίες με μερικό CSI. Ο πομπός προσπαθεί να μεταδώσει με τέτοιο τρόπο ώστε να σχηματιστεί μια ισχυρή δέσμη

προς τον δέκτη (η κορυφή του κέρδους του σήματος να κατευθύνεται στον δέκτη - κατευθυντικότητα). Επιπλέον, μέρος της ισχύς του πομπού χρησιμοποιείται για τη δημιουργία τεχνητού θορύβου, ο οποίος μεταδίδεται μαζί με την πληροφορία ώστε να εξασθενίσει το κανάλι του ωτακουστή. Η τεχνική αυτή βασίζεται στη στιγμιαία γνώση της CSI του βασικού καναλιού, χωρίς να χρειάζεται η CSI του καναλιού υποκλοπής. Στα [28] και [29] οι Negi και Goel μία στρατηγική μορφοποίησης δέσμης με παράλληλη προσθήκη ψευδοθορύβου. Στην τεχνική αυτή ο πομπός μορφοποιεί τη δέσμη προς τον δέκτη και επιπλέον στέλνει θόρυβο προς όλες τις κατευθύνσεις εκτός από τη διεύθυνση του δέκτη και έτσι επηρεάζει το κανάλι του ωτακουστή και όχι του δέκτη.

Μία βασική συνεργατική τεχνική, η οποία θα παρουσιαστεί στο Κεφάλαιο 5, είναι το συνεργατικό jamming. Στην τεχνική αυτή, οι ανεξάρτητοι πομποί του δικτύου μεταδίδουν σήματα τα οποία εμπλέκονται με τον δέκτη αλλά και με τον ωτακουστή, μειώνοντας την ικανότητα αποκωδικοποίησης και των δύο, αφού ελαττώνονται αντίστοιχα οι χωρητικότητές τους. Δεδομένου ότι η χωρητικότητα ασφαλείας ισούται με τη διαφορά των χωρητικοτήτων των δύο καναλιών, αν το jamming γίνει με τέτοιο τρόπο ώστε να μειωθεί περισσότερο η χωρητικότητα του καναλιού υποκλοπής τότε θα προκύψει βελτίωση στη συνολική χωρητικότητα ασφαλείας. Επιπλέον ανασκόπηση των συνεργατικών τεχνικών γίνεται επίσης στο κεφάλαιο 5.

Βιβλιογραφία - Αναφορές 3ου Κεφαλαίου

[1] B. Schneier, “Cryptographic design vulnerabilities”, *IEEE Computer*, vol. 31, no. 9, pp. 26-33, Sep.1998

[2] G. Kapoor, S. Piramithu, “Vulnerabilities in some recently proposed RFID ownership transfer protocols*”, IEEE Commun. Lett.,* vol. 14, no. 3, pp. 260-262, Mar. 2010.

[3] C. Shannon, “Communication theory of secrecy systems”, *Bell system technical journal*, vol. 28, no. 4, pp. 656-715, 1949.

[4] A. Wyner, “The wire-tap channel”, *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[5] I. Cziszár, J. Körner, “Broadcast channels with confidential messages”, *IEEE Trans. on Inform. Theory,* vol. 24, no. 3, pp. 339-348, 1978.

[6] Kaliszan, Michal, J. Mohammadi, S. Stanczak. “Cross-layer security in two-hop wireless Gaussian relay network with untrusted relays*”, IEEE International Conference on Communications (ICC)*, 2013.

[7] S. Leung-Yan-Cheong, M. Hellman, “The gaussian wiretap channel”, *IEEE Trans. on Inform. Theory,* vol. 24, no. 4, pp. 451-456, July 1978.

[8] P. Gopala, L. Lai, H. Gamal, “On the secrecy capacity of fading channels”, *IEEE Trans. on Inform. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[9] Z. Rezki, A. Khisti, M.-S. Alouini, “On the ergodic secrecy capacity of the wiretap channel under imperfect main channel estimation”, in *Proc. Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, pp. 952–957, Nov. 2011.

[10] B. He, X. Zhou, “Secure on-off transmission design with channel estimation errors”, submitted to *IEEE Trans. Inf. Forensics Security*, Apr. 2013.

[11] R. Negi, S. Goel, “Secret communication using artificial noise”, in *Proc. IEEE VTC*, vol. 3, Dallas, TX, pp. 1906–1910, Sept. 2005.

[12] S. Goel, R. Negi, “Guaranteeing secrecy using artificial noise”, *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

4

Διαχειριση Ισχυος στην Ασφαλεια Φυσικου Στρωματος

Οι ασύρματες επικοινωνίες αναπτύσσονται με γρήγορους ρυθμούς και σε συνδυασμό με τις υψηλές απαιτήσεις σε ταχύτητα αλλά και σε αυτονομία, η διαχείριση των ραδιοπόρων του συστήματος (Radio Resource Management – RRM) καθίσταται ως μία από τις σημαντικότερες σύγχρονες προκλήσεις που οι μηχανικοί καλούνται να αντιμετωπίσουν. Στο κεφάλαιο αυτό, αρχικά γίνεται μία σύντομη αναφορά στους πόρους των ασύρματων δικτύων και στην ανάγκη της διαχείρισής τους. Στη συνέχεια, αναλύεται ένας εξ' αυτών, η ισχύς. Πιο συγκεκριμένα, στο απλό μοντέλο της ασύρματης επικοινωνίας μεταξύ πομπού και δέκτη παρουσία ωτακουστή, αναλύεται η ισχύς εκπομπής σε σχέση με τα ασύρματα κανάλια και περιγράφεται το πρόβλημα της βελτιστοποίησης (optimization) της χωρητικότητας ασφαλείας σε σχέση με αυτήν.

4.1 Διαχείριση Πόρων Ασύρματων Δικτύων

Με τη συνεχή εξέλιξη των ασύρματων δικτύων αυξάνονται ολοένα και περισσότερο οι απαιτήσεις για υψηλότερους ρυθμούς μετάδοσης δεδομένων και χαμηλότερες καθυστερήσεις, παράλληλα με την ικανοποίηση δεδομένων στόχων σε ποιότητα υπηρεσιών. Οι απαιτήσεις αυτές καλύπτονται ως ένα βαθμό από την ανάπτυξη των νέων τεχνολογιών. Ωστόσο λόγω της πεπερασμένης φύσης των διαθέσιμων πόρων των ασύρματων δικτύων η ικανοποίηση των απαιτήσεων αυτών, υπό αυτές τις συνθήκες, μπορεί να επιτευχθεί μέσω της διαχείρισης πόρων στις ασύρματες επικοινωνίες. Η διαχείριση πόρων αφορά

αποδοτικές διεργασίες, οι οποίες καθορίζουν τον τρόπο και τις διαδικασίες ελέγχου, διαμοιρασμού και ανάθεσης των διαθέσιμων πόρων ενός ασύρματου δικτύου στον εκάστοτε χρήστη του [1]. Πιο συγκεκριμένα, η διαχείριση πόρων αναφέρεται στη βέλτιστη χρήση των πόρων με βάση την πληροφορία του ασύρματου περιβάλλοντος και τις απαιτήσεις ποιότητας υπηρεσιών.

4.1.1 Πόροι ασύρματων δικτύων

Πόροι ασύρματων δικτύων είναι οι διαχειρίσιμες φυσικές οντότητες μέσα στο ασύρματο δίκτυο, οι οποίες επηρεάζουν την απόδοση του. Υπάρχουν διάφορα είδη πόρων στα ασύρματα συστήματα [2], ανάλογα με το είδος των επικοινωνιών πχ. σταθερές ή κινητές, οι σημαντικότεροι των οποίων είναι οι ακόλουθοι:

1. *Εύρος ζώνης (bandwidth):* Το εύρος ζώνης είναι το πλάτος της ζώνης συχνοτήτων που καταλαμβάνει η μετάδοση ενός σήματος και καθορίζει τον μέγιστο αξιόπιστο ρυθμό μετάδοσης και τη πρόσβαση στο ασύρματο μέσο. Το εύρος ζώνης είναι πρακτικά πεπερασμένο και η ολοένα αυξανόμενη ζήτηση περιορίζει τη χρήση του από τους χρήστες και της υπηρεσίες και αυξάνει το κόστος απόκτησής του.
2. *Ισχύς (power):* Η ισχύς είναι η ενέργεια που απαιτείται για να σταλεί ένα bit ή ένα σύμβολο από τον πομπό στον δέκτη. Με μεγαλύτερη ισχύ, βελτιώνεται η ποιότητα της ασύρματης ζεύξης, αφού ο πομπός μπορεί να εισάγει περισσότερη πληροφορία σε κάθε σύμβολο που μεταδίδεται και άρα να αυξήσει τον ρυθμό μετάδοσης. Περιορίζεται από πολλούς παράγοντες καθώς περισσότερη ισχύς σημαίνει μεγαλύτεροι ενισχυτές και μεγαλύτερη κατανάλωση ενέργειας και συνεπώς μεγαλύτερο κόστος και λιγότερη αυτονομία. Από την άλλη πλευρά, υπάρχει και ένα κατώφλι για την ισχύ εξαιτίας του θορύβου.
3. *Αποθήκευση (storage):* Οι γρήγοροι ρυθμοί μετάδοσης και οι πιθανές εκρήξεις δεδομένων δημιουργούν την ανάγκη ύπαρξης αποθηκευτικών χώρων στις διάφορες οντότητες μέσα στο δίκτυο. Οι πόροι αποθήκευσης αναφέρονται στην πεπερασμένη χωρητικότητα των διαφόρων αποθηκευτικών στοιχείων, τα οποία υπάρχουν σε κάθε οντότητα μέσα στα δίκτυα (π.χ. τερματικά, δρομολογητές).
4. *Επεξεργασία (processing):* Οι πόροι επεξεργασίας αντιπροσωπεύουν την πεπερασμένη υπολογιστική ισχύ των στοιχείων του δικτύου όπως πχ. τερματικά, δρομολογητές. Υψηλή ικανότητα επεξεργασίας οδηγεί σε βελτίωση της ποιότητας της επικοινωνίας και σε αύξηση της ταχύτητας, ωστόσο η κατανάλωση όλων των διαθέσιμων πόρων επεξεργασίας ενός κόμβου μπορεί να υποβαθμίσει το συνολικό σύστημα.
5. *Χρόνος (time):* Ο χρόνος διαδραματίζει πολύ σημαντικό ρόλο στις ασύρματες επικοινωνίες, καθώς τα ασύρματα δίκτυα λειτουργούν κάτω από χρονομεταβαλλόμενες συνθήκες, αυξάνοντας την αναξιοπιστία. Τέτοια προβλήματα είναι οι καθυστερήσεις, οι διακυμάνσεις, οι διαλείψεις, οι οποίες καθιστούν απαραίτητη την ύπαρξη αποδοτικών μηχανισμών διαχείρισης του χρόνου.

4.1.2 Τεχνικές διαχείρισης πόρων

Η διαχείριση των πόρων των ασύρματων δικτύων μπορεί να πραγματοποιηθεί με τους εξής δύο τρόπους: κεντρικοποιημένη ή κατανεμημένη διαχείριση. Στη πρώτη μέθοδο, υπάρχει ένας κεντρικός διαχειριστής για όλο το δίκτυο, ο οποίος συλλέγει πληροφορίες από κάθε ζεύγος πομπού-δέκτη και κατανέμει κατάλληλα τους πόρους. Κατά την προσέγγιση αυτή, το πρόβλημα της διάθεσης των πόρων είναι καθολικό, παρέχοντας ευσταθή και συνεπή διαχείριση. Στη δεύτερη μέθοδο, χρησιμοποιείται τοπική προσέγγιση αφού κάθε ζεύγος πομπού-δέκτη καθορίζει τους πόρους που θα χρησιμοποιήσει με βάση τις πληροφορίες που διαθέτει. Συχνά, για να επιτευχθεί σωστή διαχείριση χρησιμοποιούνται και οι δύο παραπάνω τρόποι σε συνδυασμό (υβριδική διαχείριση).

Οι βασικότερες τεχνικές διαχείρισης πόρων που χρησιμοποιούνται στα ασύρματα δίκτυα, βασιζόμενες στους τρόπους που προαναφέρθηκαν, είναι οι εξής:

- διαχείριση εύρους ζώνης (bandwidth management),
- διαχείριση ισχύος (power management),
- διαχείριση κίνησης (traffic management) και
- διαχείριση χρόνου (time management).

Οι παραπάνω τεχνικές μπορούν να συνδυαστούν μεταξύ τους για να επιτύχουν συνολικά αποδοτικότερη λειτουργία του δικτύου.

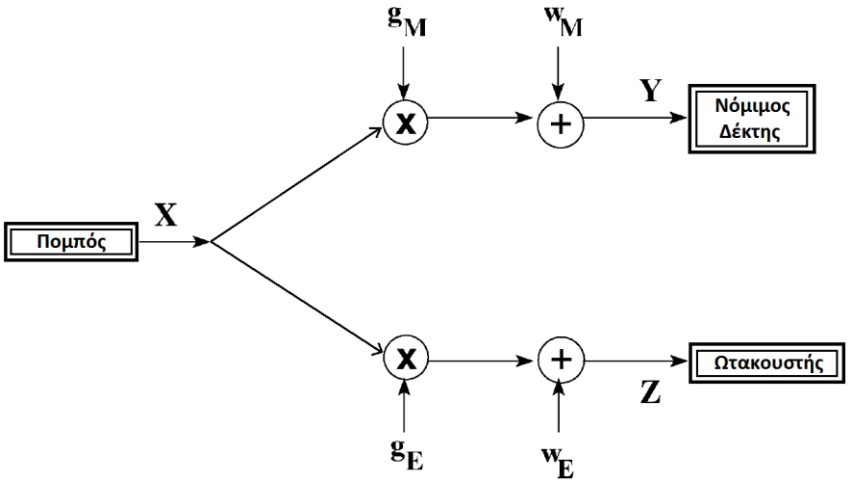
4.2 Έλεγχος Ισχύος για Βελτιστοποίηση Χωρητικότητας Ασφαλείας

Στο προηγούμενο κεφάλαιο (Κεφάλαιο 3) περιγράφηκε η έννοια της χωρητικότητας ασφαλείας χωρίς να ενδιαφέρει η βελτιστοποίησή της και χωρίς τη θεώρηση περιορισμού στους διαθέσιμους πόρους. Προηγουμένως, αναφέρθηκε ότι οι περιορισμοί που εισάγουν οι φυσικοί πόροι στις επικοινωνίες απαιτούν τη σωστή διαχείρισή τους με στόχο τη βέλτιστη χρήση τους. Σε αυτό το κεφάλαιο, λοιπόν, ερευνάται κατά πόσο οι περιορισμοί σε διαθέσιμους πόρους επηρεάζουν τα χαρακτηριστικά της ασφάλειας στο φυσικό στρώμα μέσω ενός προβλήματος βελτιστοποίησης με περιορισμό (constrained optimization problem).

Ως περιοριστικός παράγοντας θεωρείται η ισχύς μετάδοσης στον πομπό (ισχύς εκπομπής). Συγκεκριμένα, η μέση τιμή της ισχύος δεν θα πρέπει να ξεπερνάει μια συγκεκριμένη δοθείσα τιμή. Δεδομένης αυτής της συνθήκης, θα χρησιμοποιηθεί μία πολιτική βέλτιστης κατανομής ισχύος και θα αποδειχθεί ότι μπορεί να επιτευχθεί ικανοποιητική χωρητικότητα ασφαλείας ακόμη και στην περίπτωση που το βασικό κανάλι μεταξύ του πομπού και του νόμιμου παραλήπτη (main channel) είναι χειρότερο, κατά μέσο όρο, από το κανάλι μεταξύ του πομπού και του εισβολέα του δικτύου που κρυφακούει τη μετάδοση (κανάλι υποκλοπής - wiretap channel [3]).

4.2.1 Μοντέλο συστήματος

Όπως και στο προηγούμενο κεφάλαιο, μελετάται το απλό σενάριο της ασύρματης επικοινωνίας μεταξύ ενός πομπού (transmitter) και ενός νόμιμου δέκτη (legitimate receiver) παρουσία ενός ωτακουστή (eavesdropper), το οποίο απεικονίζεται στο Σχήμα 4.1.



Σχήμα 4.1: Μοντέλο συστήματος ασφαλείας στο φυσικό στρώμα για ασύρματα κανάλια με διαλείψεις.

Αναλυτικότερα, γίνεται η υπόθεση ότι τα κανάλια υπόκεινται σε διαλείψεις Rayleigh παρουσία λευκού προσθετικού γκαουσιανού θορύβου (AWGN) μηδενικής μέσης τιμής και μοναδιαίας διακύμανσης $(N_0 = 1)$ και στα δύο κανάλια, w_M και w_E αντίστοιχα. Με $h_M = |g_M|^2$ συμβολίζεται το κέρδος ισχύος του καναλιού μεταξύ πηγής-προορισμού (main channel) και με $h_E = |g_E|^2$ το κέρδος ισχύος του καναλιού μεταξύ πηγής-ωτακουστή (eavesdropper's channel), όπου g_M, g_E οι συντελεστές (κέρδη πλάτους) των δύο καναλιών αντίστοιχα. Σχετικά με τα κέρδη των δύο καναλιών θεωρείται ότι παραμένουν αμετάβλητα κατά τη διάρκεια ενός συνεχούς διαστήματος συνοχής (coherence interval) και αλλάζουν ανεξάρτητα από το ένα διάστημα στο άλλο (block fading). Στην κατάσταση i του συστήματος, τα σήματα που λαμβάνονται από τον προορισμό και τον εισβολέα δίνονται, αντίστοιχα, από τις παρακάτω σχέσεις:

$$y(i) = g_M(i)x(i) + w_M(i)$$

$$z(i) = g_E(i)x(i) + w_E(i)$$

όπου $x(i)$ είναι το σήμα που εκπέμπεται από τον πομπό.

4.2.2 Διατύπωση προβλήματος

Στη συνέχεια, περιγράφεται το πρόβλημα της διαχείρισης ισχύος για το παραπάνω μοντέλο συστήματος. Αναλυτικότερα, το πρόβλημα διατυπώνεται ως εξής: πως ο πομπός θα επιλέξει να κατανείμει την ισχύ μετάδοσης ώστε να επιτύχει τη μέγιστη χωρητικότητα ασφαλείας έχοντας ως περιορισμό τη διατήρηση της μέγιστης τιμής μέσης ισχύος $\overline{P}$. Όπως θα αναλυθεί στη συνέχεια, το συγκεκριμένο πρόβλημα αποτελεί πρόβλημα βελτιστοποίησης με περιορισμό, όπου χρησιμοποιείται η τεχνική της διαχείριση ισχύος μετάδοσης του πομπού.

Θεωρείται η περίπτωση όπου ο πομπός γνωρίζει την κατάσταση των δύο καναλιών σε κάθε στιγμή, διαθέτει δηλαδή πλήρη CSI (channel state information) και για τα δύο κανάλια (full CSI at the transmitter - CSIT). Επομένως, οι τιμές h_M και h_E είναι γνωστές στον πομπό. Είναι εύλογο να αναμένεται ότι η βέλτιστη στρατηγική είναι να επιτρέπει ο πομπός την μετάδοση όταν $h_M > h_E$ και να προσαρμόζει την ισχύ μετάδοσής του ανάλογα με τις στιγμιαίες τιμές h_M και h_E. Σύμφωνα με τα παραπάνω, η χωρητικότητα ασφαλείας δίνεται από το παρακάτω θεώρημα:

Θεώρημα [4]: Όταν τα κέρδη των καναλιών του δέκτη και του ωτακουστή είναι γνωστά στον πομπό, η εργοδική χωρητικότητα ασφαλείας ισούται με:

$$\overline{C}_S^{(F)} = \max_{P(h_M,h_E)} \int_0^\infty \int_{h_E}^\infty \left[\log_2(1+h_M P(h_M,h_E)) - \log_2(1+h_E P(h_M,h_E))\right] f(h_M) f(h_E) dh_M dh_E \qquad (4.1)$$

δεδομένου ότι ισχύει

$$\mathrm{E}\{P(h_M,h_E)\} \le \overline{P} \qquad (4.2)$$

Λεπτομερής απόδειξη του θεωρήματος υπάρχει στο [4]. Ωστόσο, εδώ θα υπογραμμιστούν τα κυριότερα σημεία της. Με βάση το σενάριο, μετάδοση πραγματοποιείται όταν $h_M > h_E$, χρησιμοποιώντας βέλτιστη πολιτική εκχώρησης ισχύος που ικανοποιεί τον περιορισμό (4.2). Όπως προαναφέρθηκε, για πλήρη CSI στον πομπό, η ισχύς μετάδοσης εξαρτάται από τις συνθήκες των δύο καναλιών. Από τη θεωρία της χωρητικότητας ασφαλείας διαύλων (βλ. Κεφάλαιο 3) ο μέγιστος ρυθμός αξιόπιστης μετάδοσης που μπορεί να επιτευχθεί χωρίς διαρροή πληροφορίας σε κάθε στιγμή ισούται με $\left[\log_2(1+h_M P(h_M,h_E)) - \log_2(1+h_E P(h_M,h_E))\right]^+$, όπου $[x]^+ = \max\{x,0\}$. Ολοκληρώνοντας για όλες τις πιθανές τιμές των κερδών ισχύος των δύο καναλιών προκύπτει η μέση τιμή του μέγιστου ρυθμού μετάδοσης (average achievable perfect secrecy rate) ως εξής:

$$\begin{aligned} R_S^{(F)} &= \int_0^\infty \int_0^\infty \left[\log_2(1+h_M P(h_M,h_E)) - \log_2(1+h_E P(h_M,h_E))\right]^+ f(h_M) f(h_E) dh_M dh_E \\ &= \int_0^\infty \int_{h_E}^\infty \left[\log_2(1+h_M P(h_M,h_E)) - \log_2(1+h_E P(h_M,h_E))\right] f(h_M) f(h_E) dh_M dh_E \end{aligned} \qquad (4.3)$$

όπου $f(h_M)$ και $f(h_E)$ είναι οι συναρτήσεις πυκνότητας πιθανότητας των κερδών ισχύος των δύο καναλιών αντίστοιχα.

4.2.3 Βέλτιστη πολιτική εκχώρησης ισχύος

Για να επιτευχθεί η μέγιστη χωρητικότητα ασφαλείας θα πρέπει πρώτα να βρεθεί η βέλτιστη ισχύς (optimal power allocation) που μεγιστοποιεί την (4.1) και ταυτόχρονα ικανοποιεί την (4.2). Παρατηρείται ότι η συνάρτηση $y(P) = \log_2(1+h_M P) - \log_2(1+h_E P)$ είναι κοίλη (concave) ως προς *P* όταν $h_M > h_E$. Συνεπώς και η συνάρτηση (4.3) είναι κοίλη ως προς P, αφού τα μη αρνητικά ολοκληρώματα διατηρούν την κυρτότητα [5]. Για την επίλυση του προβλήματος ορίζεται η συνάρτηση Lagrange (βλ. Παράρτημα) ως εξής:

$$\begin{aligned} L(P,\lambda) = &\int_0^\infty \int_{h_E}^\infty \left[\log_2(1+h_M P(h_M,h_E)) - \log_2(1+h_E P(h_M,h_E))\right] f(h_M) f(h_E) dh_M dh_E \\ &- \lambda\left(\int_0^\infty \int_{h_E}^\infty P(h_M,h_E) f(h_M) f(h_E) dh_M dh_E - \overline{P}\right) \end{aligned} \qquad (4.4)$$

Για την εύρεση της βέλτιστης λύσης, τίθεται η παράγωγος ίση με το μηδέν ως εξής:

$$\frac{\partial L}{\partial P} = \frac{h_M}{1+h_M P} - \frac{h_E}{1+h_E P} - \lambda = 0 \tag{4.5}$$

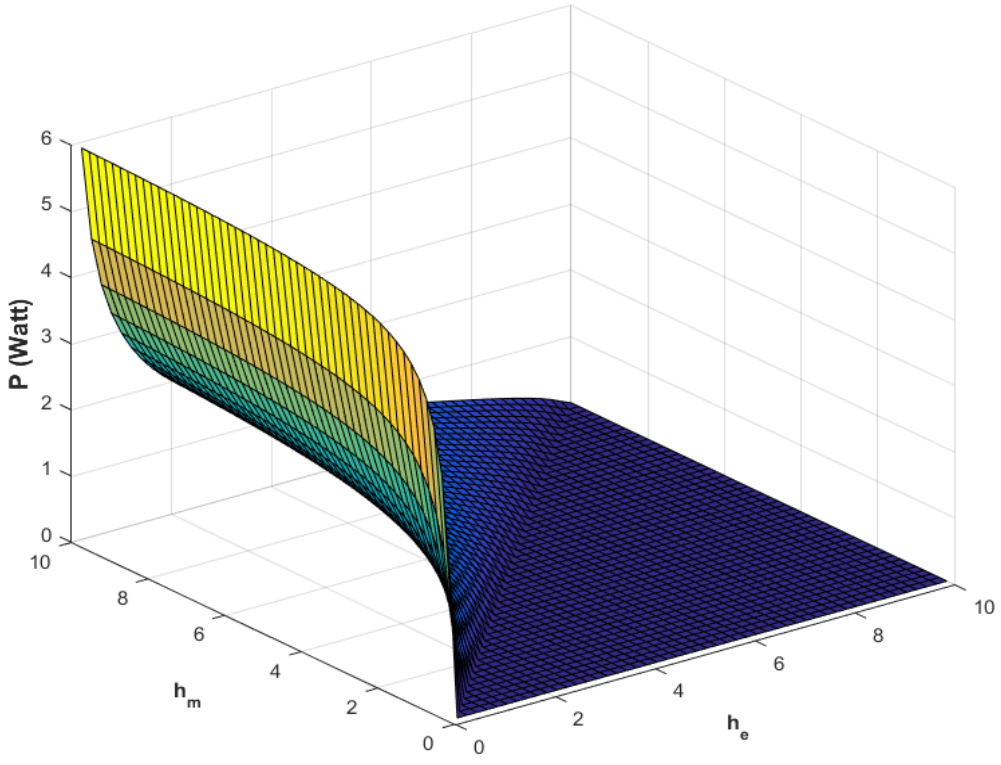
όπου η παράμετρος λ (πολλαπλασιαστής Lagrange) είναι μία σταθερά που ικανοποιεί την ισότητα του περιορισμού (4.2).

Η λύση της (4.5) είναι η εξής:

$$P(h_M, h_E) = \frac{1}{2}\left[\sqrt{\left(\frac{1}{h_E} - \frac{1}{h_M}\right)^2 + \frac{4}{\lambda}\left(\frac{1}{h_E} - \frac{1}{h_M}\right)} - \left(\frac{1}{h_M} + \frac{1}{h_E}\right)\right] \tag{4.6}$$

Εάν για κάποιες τιμές των καναλιών η τιμή της $P(h_M, h_E)$ γίνει αρνητική, τότε εφόσον δεν υπάρχει αρνητική ισχύς και δεδομένης της κυρτότητας της συνάρτησης $y(P)$, η βέλτιστη τιμή της $P(h_M, h_E)$ είναι 0 για αυτές τις τιμές των καναλιών. Συνεπώς, η σχέση που μας δίνει τη βέλτιστη κατανομή ισχύος είναι η ακόλουθη:

$$P(h_M, h_E) = \frac{1}{2}\left[\sqrt{\left(\frac{1}{h_E} - \frac{1}{h_M}\right)^2 + \frac{4}{\lambda}\left(\frac{1}{h_E} - \frac{1}{h_M}\right)} - \left(\frac{1}{h_M} + \frac{1}{h_E}\right)\right]^+ \tag{4.7}$$



Σχήμα 4.2: Στιγμιαία κατανομή ισχύος για λ=0.075.

Στο Σχήμα 4.2 απεικονίζεται ενδεικτικά η κατανομή της στιγμιαίας ισχύος για διάφορες τιμές των κερδών ισχύος των δύο καναλιών για $\overline{P} = 1 Watt$. Για τον συγκεκριμένο περιορισμό ο πολλαπλασιαστής Lagrange ισούται με $\lambda = 0.075$ περίπου. Παρατηρείται ότι μετάδοση πραγματοποιείται όταν $h_M > h_E$ και όσο μεγαλύτερη είναι η διαφορά $h_M - h_E$,

δηλαδή όσο καλύτερο είναι το κανάλι του δέκτη σε σχέση με το κανάλι του ωτακουστή, τόσο μεγαλύτερη είναι και η ισχύς μετάδοσης.

4.2.4 Αποτελέσματα προσομοιώσεων

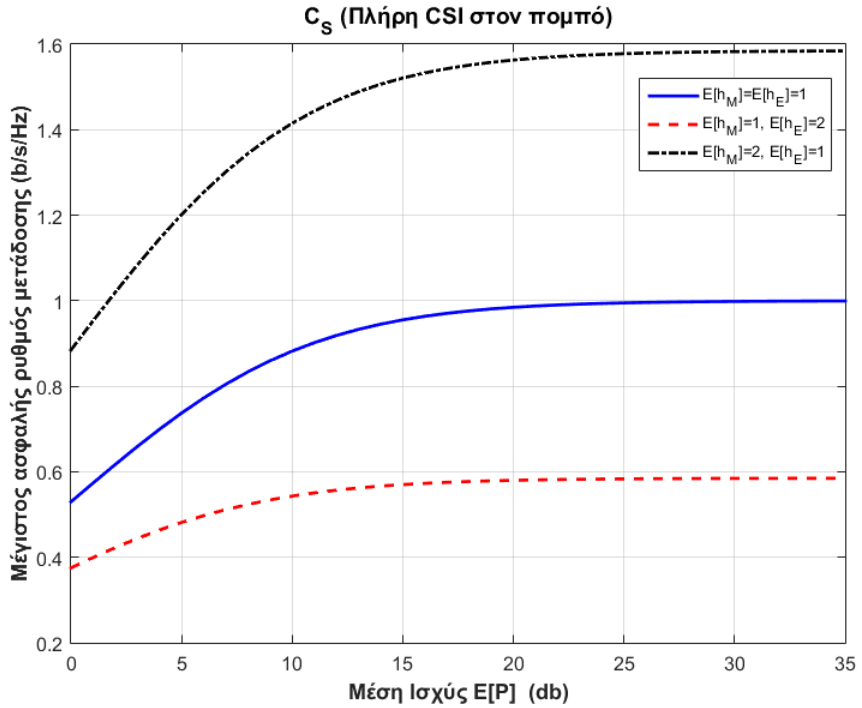
Σε αυτή την ενότητα, παρουσιάζονται οι προσομοιώσεις που εκτελέστηκαν για την αξιολόγηση της απόδοσης της πολιτικής εκχώρησης ισχύος που αναλύθηκε στην προηγούμενη ενότητα. Πιο συγκεκριμένα, μελετήθηκε η κανονικοποιημένη-συμμετρική περίπτωση διαλείψεων Rayleigh όπου $\bar{h}_M = \bar{h}_E = 1$. Υπενθυμίζεται ότι $\bar{h}_M = \mathrm{E}\{h_M\}$ και $\bar{h}_{\mathrm{E}} = \mathrm{E}\{h_{\mathrm{E}}\}$ είναι οι μέσες τιμές των κερδών ισχύος του βασικού καναλιού και του καναλιού υποκλοπής, αντίστοιχα. Επίσης, οι συναρτήσεις πυκνότητας πιθανότητας των καναλιών δίνονται ως $f(h_x) = \frac{1}{\bar{h}_x}\exp\left(-h_x / \bar{h}\right)$ όπου *x* = *M* ή *E*, αφού για τα Rayleigh κανάλια τα κέρδη ισχύος ακολουθούν την εκθετική κατανομή. Επίσης, μελετήθηκε το ασύμμετρο σενάριο όπου ο ωτακουστής διαθέτει καλύτερο κανάλι από τον νόμιμο δέκτη $\left(\bar{h}_M = 1,\ \bar{h}_E = 2\right)$.

Υπενθυμίζεται εδώ η μεθοδολογία εύρεσης της μέγιστης χωρητικότητας ασφαλείας $\bar{C}_S^{(F)}$, όπου ο πομπός διαθέτει πλήρη CSI, για μία δοθείσα μέγιστη τιμή μέσης ισχύος $\bar{P}$: Αρχικά βρίσκεται η τιμή του *λ* που ικανοποιεί την ισότητα του περιορισμού (4.2) αντικαθιστώντας τη στιγμιαία ισχύ που δίνεται από την (4.7) με βάση τη δοθείσα τιμή $\bar{P}$. Έπειτα υπολογίζεται η στιγμιαία ισχύς από τη σχέση (4.7) για το υπολογιζόμενο *λ* και αντικαθίσταται στο ολοκλήρωμα (4.3). Η σχέση (4.3) δίνει τη ζητούμενη χωρητικότητα ασφαλείας (μέγιστος ασφαλής ρυθμός μετάδοσης). Για τις προσομοιώσεις χρησιμοποιήθηκε το πρόγραμμα Matlab και ο υπολογισμός των απαραίτητων ολοκληρωμάτων έγινε με αριθμητική ολοκλήρωση.

Στο Σχήμα 4.3 παρουσιάζεται η (εργοδική) χωρητικότητα ασφαλείας ως προς τη μέγιστη μέση ισχύ μετάδοσης για τις ακόλουθες περιπτώσεις:

- Ο δέκτης και ο ωτακουστής διαθέτουν το ίδιο κανάλι κατά μέσο όρο ($\bar{h}_M = \bar{h}_E = 1$)
- Ο δέκτης διαθέτει χειρότερο μέσο κανάλι από τον ωτακουστή ($\bar{h}_M = 1 < \bar{h}_E = 2$)
- Ο δέκτης διαθέτει καλύτερο μέσο κανάλι από τον ωτακουστή ($\bar{h}_M = 2 > \bar{h}_E = 1$)

Όπως παρατηρείται, μεγαλύτερη χωρητικότητα ασφαλείας προκύπτει στην περίπτωση που το κανάλι μεταξύ πομπού και δέκτη είναι καλύτερο (κατά μέσο όρο) από το κανάλι μεταξύ πομπού και ωτακουστή, ενώ μικρότερη όταν ο ωτακουστής διαθέτει πιο ικανό κανάλι από το νόμιμο δέκτη. Δεδομένου ότι ο πομπός γνωρίζει κάθε στιγμή την κατάσταση των καναλιών, όσο καλύτερο είναι το κανάλι μεταξύ αυτού και του νόμιμου δέκτη τόσο αυξάνει ο ασφαλής ρυθμός μετάδοσης, αφού μπορεί να εκμεταλλευτεί όλη τη διαθέσιμη ισχύ για να μεταδώσει.

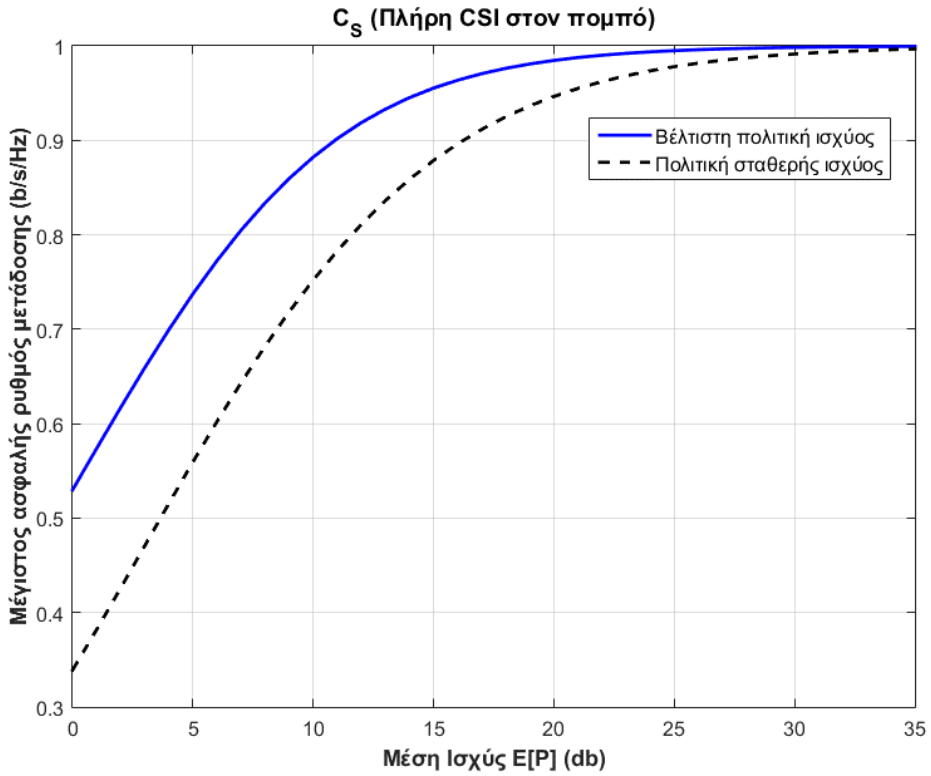


Σχήμα 4.3: Χωρητικότητα ασφαλείας ως προς τη μέγιστη μέση ισχύ μετάδοσης για διάφορες τιμές των $\overline{h}_M$, $\overline{h}_E$.

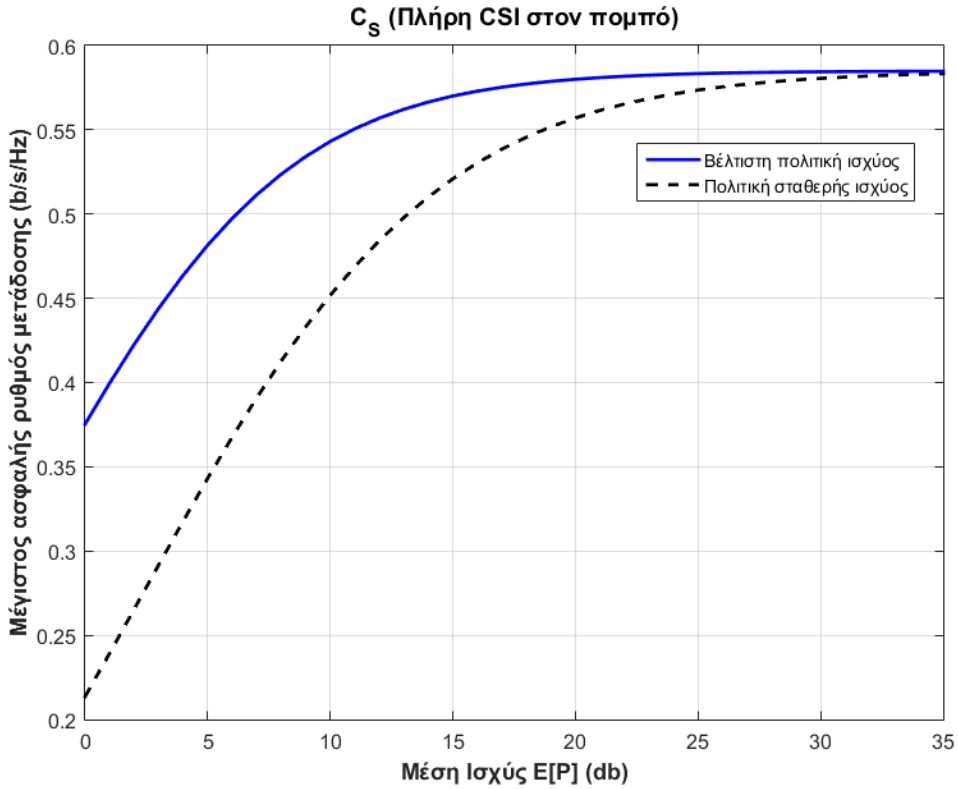
Στη συνέχεια εκτελέστηκαν άλλα δύο σενάρια προσομοιώσεων όπου συγκρίνεται η πολιτική βέλτιστης κατανομής ισχύος, όπως παρουσιάστηκε προηγουμένως, με την εργοδική χωρητικότητά ασφαλείας (Κεφάλαιο 3) όπου ο πομπός μεταδίδει με σταθερή ισχύ (πολιτική σταθερής ισχύος), ίση με τη μέγιστη μέση τιμή που δίνεται κάθε φορά από τον περιορισμό, όταν $h_M > h_E$, δηλαδή $P_{in} = \begin{cases} \overline{P}, & \text{αν } h_M > h_E \\ 0, & \text{αν } h_M \le h_E \end{cases}$. Η περίπτωση αυτή ουσιαστικά συμβαίνει όταν ο πομπός δεν διαθέτει την CSI του καναλιού υποκλοπής, οπότε δεν δύναται να εφαρμόσει την πολιτική βελτιστοποίησης ισχύος που παρουσιάζεται εδώ.

Στο Σχήμα 4.4 θεωρείται η συμμετρική περίπτωση ($\overline{h}_M = 1,\ \overline{h}_E = 1$). Παρατηρείται ότι η πολιτική βέλτιστης κατανομής ισχύος (optimal power allocation policy) βελτιώνει αισθητά τη χωρητικότητα ασφαλείας σε σύγκριση με την πολιτική σταθερής ισχύος. Για μεγάλες τιμές της μέσης ισχύος, άρα για μεγάλες τιμές του μέσου σηματοθορυβικού λόγου SNR, ο μέγιστος ασφαλής ρυθμός μετάδοσης συγκλίνει κοντά στην τιμή 1 b/s/Hz και στις δύο περιπτώσεις. Για χαμηλά SNRs ο έλεγχος της ισχύος μας επιτρέπει να επιτύχουμε αρκετά καλούς ρυθμούς μετάδοσης σε σχέση με τη μετάδοση χωρίς βελτιστοποίηση.

Τέλος, εκτελέστηκε το σενάριο προσομοίωσης όπου $\overline{h}_M = 1,\ \overline{h}_E = 2$. Τα αποτελέσματα παρουσιάζονται στο Σχήμα 4.5, όπου επιβεβαιώνεται το ενδιαφέρον αποτέλεσμα ότι μπορεί να επιτευχθεί μη μηδενικός ασφαλής ρυθμός μετάδοσης δεδομένων από τον πομπό στον δέκτη σε κανάλια με διαλείψεις Rayleigh ακόμα και στην περίπτωση που ο ωτακουστής διαθέτει πιο ικανό κανάλι από τον νόμιμο δέκτη (κατά μέσο όρο). Και σε αυτή την περίπτωση φαίνεται ότι η πολιτική βέλτιστης κατανομής ισχύος βελτιώνει αισθητά τη χωρητικότητα ασφαλείας, ειδικά για μικρές τιμές του SNR. Συνεπώς, φαίνεται η θετική επίδραση των διαλείψεων στη βελτίωση της χωρητικότητας ασφαλείας καθώς και η κρίσιμη επίδραση της διαχείρισης ισχύος στις ασύρματες επικοινωνίες.



Σχήμα 4.4: Σύγκριση βέλτιστης πολιτικής ισχύος και πολιτικής σταθερής ισχύος για $\overline{h}_M = \overline{h}_E = 1$.



Σχήμα 4.5: Σύγκριση βέλτιστης πολιτικής ισχύος και πολιτικής σταθερής ισχύος για $\overline{h}_M = 1, \overline{h}_E = 2.$

Βιβλιογραφία – Αναφορές 4ου Κεφαλαίου

[1] Μ. Πουλάκης, *Μηχανισμοί Βελτιστοποίησης Χρονοπρογραμματισμού και Διαχείρισης Πόρων για Διασφάλιση Ποιότητας Υπηρεσίας σε Ασύρματα Δίκτυα*, *Διδακτορική Διατριβή*, ΕΜΠ, Μάιος 2014.

[2] I. Priggouris, E. Zervas, S. Hadjiefthymiades, “Location Based Network Resource Management”, *Handbook of Research on Mobile Multimedia, Idea Group Reference*, May 2006.

[3] A.D. Wyner, “The wire-tap channel”, *Bell Syst. Tech. J.*, vol.54, pp. 1355-1387, Oct. 1975.

[4] P. Gopala, L. Lai, and H.El Gamal,, "On the Secrecy Capacity of Fading Channels", *IEEE Trans. on Inform. Theory*, vol.54, no.10, pp.4687-4698, Oct. 2008.

[5] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge Univiversity. Press, 2004.

5

Συνεργατικες Τεχνικες για Βελτιωση της Ασφαλειας στο Φυσικο Στρωμα

Σε ένα ασύρματο δίκτυο με πολλαπλά ζεύγη πομπών-δεκτών, όταν μεταδίδεται πληροφορία μεταξύ ενός ζευγαριού οι υπόλοιποι χρήστες του δικτύου παραμένουν σιωπηλοί ή μεταδίδουν σε διαφορετική συχνότητα, ώστε να αυξάνεται η αξιοπιστία (reliability) της μετάδοσης. Ωστόσο, όταν είναι επιθυμητός ο συνδυασμός ασφάλεια με αξιοπιστία, οι ανεξάρτητοι χρήστες του δικτύου μπορούν να συμμετάσχουν με διάφορους τρόπους ώστε να μεγιστοποιηθεί ο αξιόπιστος ρυθμός δεδομένων μεταξύ κάποιου συγκεκριμένου ζευγαριού. Το κεφάλαιο αυτό, λοιπόν, ασχολείται με τη διασφάλιση της ασφαλούς ασύρματης επικοινωνίας χρησιμοποιώντας τεχνικές που βασίζονται στη συνεργασία μεταξύ διαφορετικών χρηστών μέσα στο δίκτυο. Αρχικά, παρέχεται μία περιεκτική σύνοψη πρόσφατων προόδων στον τομέα της ασφάλειας φυσικού στρώματος οι οποίες εγγυούνται την αξιοπιστία και ασφάλεια της μετάδοσης χρησιμοποιώντας συνεργατικές τεχνικές στο ασύρματο μέσο. Στη συνέχεια, το κεφάλαιο εστιάζει σε ένα συγκεκριμένο μηχανισμό ο οποίος συνδυάζει την τεχνική ενίσχυσης και προώθησης (amplify-and-forward) με την τεχνική της ηθελημένης παρεμβολής (jamming). Τέλος, για την αξιολόγηση του μηχανισμού αυτού εξάγονται αποτελέσματα μέσω προσομοιώσεων και συγκρίσεων.

5.1 Σύνοψη Πρόσφατων Τεχνικών

Στην ενότητα αυτή γίνεται μία επισκόπηση των βασικών συνεργατικών τεχνικών ασφαλείας (cooperative techniques) που έχουν αναπτυχθεί για εφαρμογή στο φυσικό στρώμα.

Οι τεχνικές αυτές χωρίζονται, κυρίως, σε δύο κατηγορίες: στην πρώτη κατηγορία οι «συνεργάτες» του ζεύγους πομπού-δέκτη κάνουν jamming (cooperative jamming), ενώ στη δεύτερη οι «συνεργάτες» αναμεταδίδουν μέρους του μηνύματος που θέλει να μεταδώσει ο πομπός στον δέκτη (cooperative relaying). Συχνά χρησιμοποιείται συνδυασμός των δύο αυτών τεχνικών. Έμφαση θα δοθεί στην παρουσίαση των βασικών τους αρχών, παραπέμποντας τον αναγνώστη στις δημοσιεύσεις όπου έχουν αρχικά προταθεί και σε δημοσιεύσεις όπου έχουν λεπτομερώς αναλυθεί και εφαρμοστεί.

Cooperative jamming: Το συνεργατικό jamming βασίζεται στην παραγωγή σημάτων από ανεξάρτητους πομπούς για τη βελτίωση του ασφαλή ρυθμού μετάδοσης μεταξύ ενός δοθέντος ζευγαριού πομπού-δέκτη. Η συγκεκριμένη έννοια αρχικά προτάθηκε στο [1] και αναπτύχθηκε περαιτέρω στα [2] και [3]. Στη συνέχεια παρουσιάζεται μία απλή περίπτωση με σκοπό να δείξει πως εφαρμόζεται η τεχνική αυτή: Έστω ένα δίκτυο όπου ένας πομπός θέλει να επικοινωνήσει με ασφάλεια με έναν χρήστη παρουσία ενός ωτακουστή (eavesdropper). Θεωρείται επιπλέον ένας κόμβος αναμετάδοσης (relay node) ως ανεξάρτητος χρήστης στο ίδιο δίκτυο. Όταν ο κόμβος αναμετάδοσης μεταδίδει σήματα τα οποία είναι ανεξάρτητα από το μήνυμα που προτίθεται ο πομπός να στείλει στον δέκτη, αυτά τα σήματα δημιουργούν παρεμβολή στον ωτακουστή αλλά και στον νόμιμο δέκτη, μειώνοντας έτσι τη χωρητικότητα ασφαλείας των καναλιών τους. Δεδομένου ότι η θεωρητική χωρητικότητα ασφαλείας ισούται με τη διαφορά των χωρητικοτήτων ασφαλείας μεταξύ δέκτη και ωτακουστή, η παρεμβολή αυτή (jamming) μπορεί να γίνει με τέτοιο τρόπο ώστε να αυξήσει τη χωρητικότητα ασφαλείας του νόμιμου ζευγαριού πομπού-δέκτη.

Υπάρχουν διάφοροι τρόποι με τους οποίους μπορεί να εφαρμοστεί το συνεργατικό jamming. Ένας τρόπος είναι ο ανεξάρτητος κόμβος, που θέλει να βοηθήσει τον πομπό-δέκτη, να στέλνει ανεξάρτητο και όμοια κατανεμημένο (independent identically distributed – i.i.d.) Gaussian θόρυβο. Ο τρόπος αυτός έχει αναπτυχθεί για κανάλια πολλαπλής πρόσβασης στα [2] και [3]. Ένας άλλος τρόπος, ο οποίος έχει προταθεί στην εργασία [4] είναι η προώθηση θορύβου (noise forwarding). Σε αυτή την προσέγγιση, ο βοηθητικός κόμβος μεταδίδει επιπρόσθετη τυχαιότητα (θόρυβο) στο δίκτυο με τη μορφή κώδικα αντί για i.i.d. Gaussian θόρυβο. Η διαφορά έγκειται στο ότι σε αυτήν τη περίπτωση ο δέκτης είναι σε θέση να αποκωδικοποιήσει τον κώδικα θορύβου και να καταλάβει ότι δεν περιέχει πληροφορία και έτσι να κρατήσει τη πληροφορία που θέλει, ενώ από την άλλη πλευρά ο ωτακουστής δεν γνωρίζει τον κώδικα θορύβου και έτσι δεν μπορεί να τον διαχωρίσει από το σήμα πληροφορίας.

Cooperative relaying: Σε αυτή την περίπτωση ο πομπός αρχικά μεταδίδει προς τον βοηθητικό κόμβο, αλλά και προς το δέκτη. Στη συνέχεια ο βοηθητικός κόμβος είτε αποκωδικοποιεί το σήμα και το προωθεί προς το νόμιμο δέκτη, η οποία τεχνική ονομάζεται αποκωδικοποίηση και προώθηση (decode and forwarding – DF) [5] είτε συμπιέζει το μήνυμα που έλαβε και στη συνέχεια το προωθεί, η οποία τεχνική ονομάζεται συμπίεση και προώθηση (compress and forwarding – CF) [6] προς το δέκτη με στόχο να βελτιώσει τη χωρητικότητα του καναλιού μεταξύ πομπού και δέκτη, ώστε τελικά να αυξηθεί η χωρητικότητα ασφάλειας. Επίσης, στην ερευνητική εργασία [7] εξετάζεται μία μέθοδος όπου ο αναμεταδότης (βοηθητικός κόμβος) αποκωδικοποιεί και επανακωδικοποιεί τα ληφθέντα από τον πομπό σήματα και στη συνέχεια τα προωθεί στον προορισμό. Η απόδοση της βοηθητικής αναμετάδοσης εξαρτάται κυρίως από τη θέση του αναμεταδότη στο δίκτυο. Γενικά είναι επιθυμητό ο αναμεταδότης να βρίσκεται μακριά από τον ωτακουστή και κοντά στο νόμιμο δέκτη.

Τέλος, στο [8] συγκρίνεται η απόδοση μεταξύ συνεργατικού jamming και συνεργατικού relaying σε ένα ζευγάρι πηγής-προορισμού μονής κεραίας, όπου ο αναμεταδότης διαθέτει πολλαπλές κεραίες και χρησιμοποιεί DF τεχνική για την αναμετάδοση. Επίσης, προτείνεται ένας τρόπος όπου συνδυάζει τις δύο παραπάνω τεχνικές.

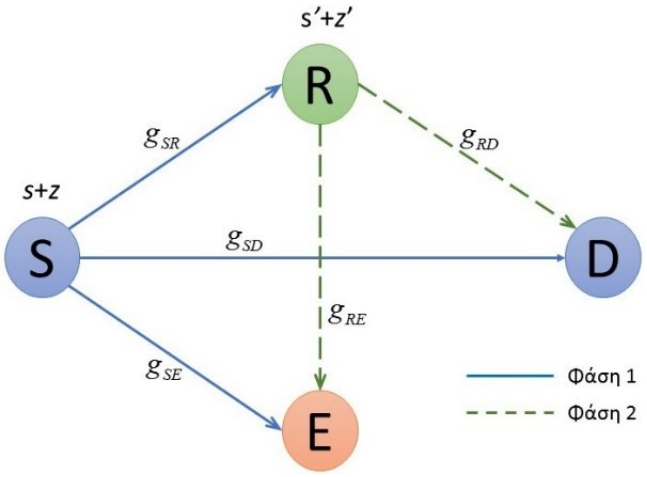
Στη συνέχεια του κεφαλαίου θα παρουσιαστεί μία συνεργατική τεχνική όπου συνδυάζει αναμετάδοση και jamming, αλλά για την αναμετάδοση ο κόμβος μονής κεραίας θα ενισχύει και στη συνέχεια θα προωθεί το μήνυμα (amplify and forward – AF), η οποία βασίζεται στο [9].

5.2 Μηχανισμός Συνεργατικού Jamming με Χρήση Τεχνικής Αναμετάδοσης Ενίσχυσης και Προώθησης

Στην ενότητα αυτή παρουσιάζεται ο μηχανισμός συνεργατικού jamming για ασφαλείς επικοινωνίες σε δίκτυα με αναμεταδότες που χρησιμοποιούν τεχνική AF. Ερευνάται μια μέθοδος όπου ο αναμεταδότης χρησιμοποιεί μέρος της διαθέσιμης ισχύος του για να δημιουργήσει παρεμβολές στον ωτακουστή και το υπόλοιπο για να αναμεταδώσει το μήνυμα. Υποθέτουμε ότι τόσο ο αναμεταδότης όσο και ο δέκτης έχουν εκ των προτέρων γνώση των σημάτων παρεμβολής. Χρησιμοποιείται πολιτική βέλτιστης κατανομής ισχύος η οποία καθορίζει πως θα εκχωρηθεί η ισχύς μεταξύ του σήματος που μεταφέρει το μήνυμα και του σήματος που προκαλεί παρεμβολές ανάλογα με τις συνθήκες των καναλιών. Στη συνέχεια παρουσιάζεται αναλυτικά το μοντέλο συστήματος, η βέλτιστη πολιτική ισχύος καθώς και τα αποτελέσματα των προσομοιώσεων για την αξιολόγηση της μεθόδου.

5.2.1 Μοντέλο συστήματος

Θεωρείται δίκτυο αποτελούμενο από μια πηγή (source - S), έναν προορισμό (destination – D), έναν έμπιστο αναμεταδότη AF (relay – R) και έναν παθητικό ωτακουστή (eavesdropper – E) (Σχήμα 5.1).



Σχήμα 5.1: Δίκτυο τεσσάρων κόμβων με αναμεταδότη AF.

Η μετάδοση γίνεται σε δύο φάσεις: στη πρώτη φάση η πηγή S (πομπός) εκπέμπει το σήμα x_S προς τον προορισμό D (δέκτης) και τον αναμεταδότη R, ενώ στην δεύτερη φάση ο

αναμεταδότης επανεκπέμπει το σήμα που έλαβε στη πρώτη φάση προς τον προορισμό. Τελικά, ο δέκτης συνδυάζει τα δύο αυτά σήματα με αποτέλεσμα να βελτιωθεί συνολικά η χωρητικότητα ασφαλείας του δικτύου. Επιπλέον, θεωρούνται κανάλια με επίπεδες διαλείψεις Rayleigh και ότι η πληροφορία της κατάστασης όλων των καναλιών είναι διαθέσιμη (full CSI). Επίσης, γίνεται η υπόθεση ότι ο θερμικός θόρυβος σε κάθε κόμβο είναι λευκός Gaussian μηδενικής μέσης τιμής και διακύμανσης σ^2.

Η κεντρική ιδέα του μηχανισμού jamming που παρουσιάζεται εδώ είναι να παραχθεί τεχνητός θόρυβος ο οποίος θα υποβαθμίζει το κανάλι του ωτακουστή αλλά δεν θα επηρεάζει το κανάλι του δέκτη. Έτσι, ο πομπός και ο αναμεταδότης ενισχύουν την ασφάλεια μεταδίδοντας τα σήματα που περιέχουν πληροφορία μαζί με τεχνητό θόρυβο που προκαλεί παρεμβολές. Θεωρείται ότι ο αναμεταδότης και ο πομπός έχουν γνώση των σημάτων παρεμβολής που στέλνει ο πομπός και επιπλέον ο δέκτης γνωρίζει το σήμα παρεμβολής που στέλνει ο αναμεταδότης.

Τόσο ο πομπός-πηγή (S) όσο και ο αναμεταδότης (R) χρησιμοποιούν μέρος της διαθέσιμης ισχύος για να μεταδώσουν το σήμα πληροφορίας και το υπόλοιπο για να μεταδώσουν το σήμα παρεμβολής. Έστω a_i ($0 \le a_i \le 1$, όπου $i \in \{S, R\}$) ο συντελεστής που καθορίζει την κατανομή της ισχύος στα σήματα πληροφορίας και παρεμβολής αντίστοιχα. Έτσι, η ισχύς που διατίθεται από τον πομπό για τη μετάδοση του σήματος πληροφορίας και του σήματος παρεμβολής είναι $a_S P_S$ και $(1-a_S)P_S$ αντίστοιχα, όπου P_S η διαθέσιμη στον πομπό ισχύς. Ενώ, η ισχύς που διατίθεται από τον αναμεταδότη για την μετάδοση της ενισχυμένης εκδοχής του ληφθέντος σήματος και του σήματος παρεμβολής είναι $a_R P_R$ και $(1-a_R)P_R$ αντίστοιχα, όπου P_R η διαθέσιμη ισχύς στον αναμεταδότη.

Στη Φάση 1, το σήμα που στέλνει η πηγή δίνεται από την παρακάτω σχέση:

$$x_S = \sqrt{a_S P_S}\, s + \sqrt{(1-a_S)P_S}\, z \tag{5.1}$$

όπου s είναι το σήμα πληροφορίας και z το σήμα παρεμβολής, μοναδιαίας ισχύος αμφότερα. Επομένως, τα σήματα που λαμβάνουν ο αναμεταδότης R, ο νόμιμος δέκτης D και ο ωτακουστής E δίνονται από τις παρακάτω σχέσεις αντίστοιχα:

$$y_R = \sqrt{a_S P_S}\, g_{SR} s + \sqrt{(1-a_S)P_S}\, g_{SR} z + w_R \tag{5.2}$$

$$y_{D1} = \sqrt{a_S P_S}\, g_{SD} s + \sqrt{(1-a_S)P_S}\, g_{SD} z + w_{D1} \tag{5.3}$$

$$y_{E1} = \sqrt{a_S P_S}\, g_{SE} s + \sqrt{(1-a_S)P_S}\, g_{SE} z + w_{E1} \tag{5.4}$$

όπου g_{ij} ο συντελεστής (κέρδος πλάτους) του καναλιού μεταξύ του κόμβου i και του κόμβου j $(i \neq j)$ (όπου $i \in \{S, R\}$, $j \in \{R, D, E\}$) και w_R , w_{D1} και w_{E1} είναι ο προσθετικός θόρυβος των αντίστοιχων καναλιών. Επίσης, ας σημειωθεί εδώ ότι τόσο ο αναμεταδότης όσο και ο δέκτης μπορούν να αφαιρέσουν εντελώς το σήμα παρεμβολής z .

Στη Φάση 2, το σήμα που στέλνει ο αναμεταδότης με AF τεχνική ισούται με:

$$x_R = \sqrt{a_R P_R}\, s' + \sqrt{(1-a_R)P_R}\, z' \tag{5.5}$$

όπου s' είναι το επανεκπεμπόμενο από τον αναμεταδότη σήμα πληροφορίας κανονικοποιημένο σύμφωνα με τον παράγοντα $\beta = \sqrt{E\{|\sqrt{a_S P_S}\, g_{SR} s + w_R|^2\}}$ ως εξής:

$$s' = \sqrt{a_S P_S} g_{SR} s + w_R / \beta \tag{5.6}$$

και z' είναι ένα νέο σήμα παρεμβολής ανεξάρτητο του z. Επομένως, τα σήματα που λαμβάνουν, σε αυτή τη φάση, ο δέκτης και ο ωτακουστής είναι:

$$y_{D2} = \sqrt{a_R P_R} g_{RD} s' + \sqrt{(1-a_R) P_R} g_{RD} z' + w_{D2} \tag{5.7}$$

$$y_{E2} = \sqrt{a_R P_R} g_{RE} s' + \sqrt{(1-a_R) P_R} g_{RE} z' + w_{E2} \tag{5.8}$$

Στη συνέχεια, εφαρμόζοντας την τεχνική συνδυασμού μεγίστου λόγου (Maximal Ratio Combining – MRC), ο συνολικός σηματοθορυβικός λόγος (SNR) Γ_D στον δέκτη και ο συνολικός λόγος σήμα-προς-παρεμβολή-και-θόρυβο (signal-to-interference-and-noise SINR) Γ_E στον ωτακουστή δίνονται αντίστοιχα από τις σχέσεις:

$$\Gamma_D = a_S \gamma_{SD} + \frac{a_S a_R \gamma_{SR} \gamma_{RD}}{1 + a_S \gamma_{SR} + a_R \gamma_{RD}} \tag{5.9}$$

$$\Gamma_E = \frac{a_S \gamma_{SE}}{1 + (1-a_S)\gamma_{SE}} + \frac{a_S a_R \gamma_{SR} \gamma_{RE}}{1 + \gamma_{RE} + a_S \gamma_{SR} + a_S (1-a_R) \gamma_{SR} \gamma_{RE}} \tag{5.10}$$

όπου $\gamma_{ij} = P_i h_{ij} / \sigma^2$ ο SNR της αντίστοιχης ζεύξης και $h_{ij} = \left| g_{ij} \right|^2$ το κέρδος ισχύος του αντίστοιχου καναλιού (με $i \in \{S, R\}$, $j \in \{R, D, E\}$). Όπως έχει αναφερθεί ο προορισμός D γνωρίζει τα σήματα παρεμβολής και συνεπώς χρησιμοποιεί τις παρατηρήσεις και από τις δύο φάσεις για να βελτιώσει τελικά την ικανότητα λήψης του σήματος πληροφορίας εκμεταλλευόμενος την συνεργασία πομπού και αναμεταδότη. Εξαλείφει εντελώς τα σήματα παρεμβολής και των δύο φάσεων, ενώ ο ωτακουστής E δεν έχει αυτή την δυνατότητα με αποτέλεσμα τα σήματα αυτά να μειώνουν τον SINR του ωτακουστή. Έτσι, οι χωρητικότητες (αμοιβαίες πληροφορίες) των καναλιών πηγής-προορισμού και πηγής-ωτακουστή δίνονται αντίστοιχα από τις σχέσεις:

$$C_D = \frac{1}{2} \log_2 (1 + \Gamma_D) \tag{5.11}$$

$$C_E = \frac{1}{2} \log_2 (1 + \Gamma_E) \tag{5.12}$$

Ο πομπός διαθέτει πλήρη CSI και για τα δύο κανάλια, οπότε ο μέγιστος ρυθμός μετάδοσης ο οποίος εξασφαλίζει αξιοπιστία και ασφάλεια ενάντια στον ωτακουστή σε κάθε στιγμή (βλ. Κεφ.3) ισούται με:

$$R_s = \max \{C_D - C_E, 0\} \tag{5.13}$$

Αντικαθιστώντας τις σχέσεις (5.11) και (5.12) στην (5.13) προκύπτει ο στιγμιαίος μέγιστος αξιόπιστος ρυθμός μετάδοσης (ή χωρητικότητα ασφαλείας):

$$\begin{aligned} R_S = \max \Bigg\{ & \frac{1}{2} \log_2 \left(1 + a_S \gamma_{SD} + \frac{a_S a_R \gamma_{SR} \gamma_{RD}}{1 + a_S \gamma_{SR} + a_R \gamma_{RD}} \right) - \\ & \frac{1}{2} \log_2 \left(1 + \frac{a_S \gamma_{SE}}{1 + (1-a_S)\gamma_{SE}} + \frac{a_S a_R \gamma_{SR} \gamma_{RE}}{1 + \gamma_{RE} + a_S \gamma_{SR} + a_S (1-a_R) \gamma_{SR} \gamma_{RE}} \right), 0 \Bigg\} \end{aligned} \tag{5.14}$$

Όπως παρατηρείται, για να βελτιωθεί η R_S μπορεί να μειωθεί η C_E δημιουργώντας παρεμβολές στον ωτακουστή. Βέβαια, παρότι τα σήματα αυτά δεν δημιουργούν παρεμβολές στον αναμεταδότη και στον δέκτη, η C_D μειώνεται επειδή απαιτείται μέρος της διαθέσιμης ισχύος (περιορισμός της ισχύος στους κάθε κόμβους S και R) για να δημιουργηθούν τα σήματα jamming. Προκύπτει επομένως ένα πρόβλημα βελτιστοποίησης εκχώρησης ισχύος ανάμεσα στο σήμα πληροφορίας και το σήμα παρεμβολών. Στη συνέχεια, αναλύεται και επιλύεται αυτό το πρόβλημα, το πώς δηλαδή θα επιλεγεί το ζευγάρι (a_S, a_R) ώστε να μεγιστοποιηθεί η χωρητικότητα ασφαλείας ανάλογα με τις συνθήκες.

5.2.2 Βελτιστοποίηση κατανομής ισχύος

Θεωρώντας ότι $a_S = a_R = a$, δηλαδή η πηγή και ο αναμεταδότης χρησιμοποιούν τον ίδιο παράγοντα κατανομής ισχύος και ότι επιλέγεται η χωρητικότητα ασφαλείας να είναι μη αρνητική, προκύπτει το παρακάτω πρόβλημα βελτιστοποίησης, το οποίο διατυπώνεται ως εξής:

$$\max_{a} \; R_S(a)$$
$$\text{s.t.} \quad 0 \le a \le 1$$

όπου

$$R_S(a) = \frac{1}{2}\log_2\left(\frac{1 + a\gamma_{SD} + \dfrac{a^2\gamma_{SR}\gamma_{RD}}{1 + a\gamma_{SR} + a\gamma_{RD}}}{1 + \dfrac{a\gamma_{SE}}{1 + (1-a)\gamma_{SE}} + \dfrac{a^2\gamma_{SR}\gamma_{RE}}{1 + \gamma_{RE} + a\gamma_{SR} + a(1-a)\gamma_{SR}\gamma_{RE}}}\right)$$

Για την επίλυση του παραπάνω προβλήματος παραγωγίζεται η παράσταση 4^{R_S} και εξισώνεται με το μηδέν. Παρατηρείται ότι η βέλτιστη τιμή του παράγοντα *α* είναι η θετική λύση ενός πολυωνύμου 8ου βαθμού στο διάστημα [0,1] και η αντίστοιχη τιμή R_S είναι ο μέγιστος ασφαλής ρυθμός μετάδοσης.

Στην συνέχεια, για λόγους σύγκρισης παρουσιάζονται δύο απλούστερες στρατηγικές κατανομής ισχύος: η στρατηγική απευθείας μετάδοση με jamming (direct transmission with jamming – DTJ) και η στρατηγική AF αναμετάδοση χωρίς jamming (AFR), με σκοπό να αξιολογηθεί η απόδοση του μηχανισμού συνεργατικού jamming (cooperative jamming – CJ) με AF που παρουσιάστηκε προηγουμένως.

Απευθείας μετάδοση με jamming (DTJ): Σύμφωνα με τη στρατηγική αυτή δεν υπάρχει ο αναμεταδότης. Η πηγή μεταδίδει σήμα πληροφορίας αλλά και σήμα παρεμβολής ταυτόχρονα. Τίθεται και εδώ ως a ο παράγοντας κατανομής της ισχύος μεταξύ του σήματος πληροφορίας και του σήματος παρεμβολής. Οι χωρητικότητες ασφαλείας προορισμού και ωτακουστή δίνονται από τις σχέσεις:

$$C_D = \frac{1}{2}\log_2(1 + a\gamma_{SD}) \tag{5.15}$$

$$C_E = \frac{1}{2}\log_2\left(1 + \frac{a\gamma_{SE}}{1 + (1-a)\gamma_{SE}}\right) \tag{5.16}$$

Χρησιμοποιώντας την (5.13) προκύπτει:

$$R_S = \max_a \left\{ \log_2 \left(\frac{(1+a\gamma_{SD})(1+(1-a)\gamma_{SE})}{1+\gamma_{SE}} \right), 0 \right\} \tag{5.17}$$

Παραγωγίζοντας την R_S και θέτοντας την παράγωγο ίση με 0 προκύπτει ότι η R_S μεγιστοποιείται όταν $a = \frac{\gamma_{SD} - \gamma_{SE} + \gamma_{SD}\gamma_{SE}}{2\gamma_{SD}\gamma_{SE}}$.

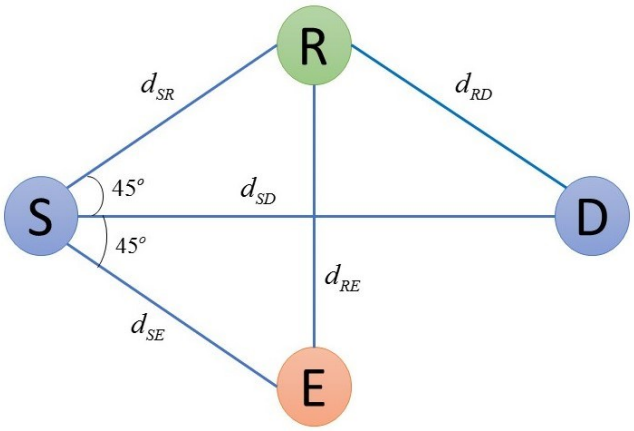
AF αναμετάδοση χωρίς jamming (AFR): Η στρατηγική αυτή είναι υποπερίπτωση της AF αναμετάδοσης με jamming (CJ) όπου τίθεται $a_S = a_R = 1$, δηλαδή όλη η ισχύς και στον πομπό και στον αναμεταδότη χρησιμοποιείται για τη μετάδοση του σήματος πληροφορίας, ενώ δεν στέλνεται καθόλου σήμα παρεμβολής. Συνεπώς, από την (5.14) για $a_S = a_R = 1$ προκύπτει ο μέγιστος ασφαλής ρυθμός:

$$R_S = \max \left\{ \frac{1}{2} \log_2 \left(\frac{1+\gamma_{SD} + \frac{\gamma_{SR}\gamma_{RD}}{1+\gamma_{SR}+\gamma_{RD}}}{1+\gamma_{SE} + \frac{\gamma_{SR}\gamma_{RE}}{1+\gamma_{SR}+\gamma_{RE}}} \right), 0 \right\} \tag{5.18}$$

Όπως παρατηρείται ο ασφαλής ρυθμός μετάδοσης στην (5.18) δεν μπορεί να είναι θετικός όταν $\gamma_{SE} > \gamma_{SD}$ και $\gamma_{RE} > \gamma_{RD}$, το οποίο συναντάται ιδιαίτερα σε συστήματα όπου ο ωτακουστής είναι αρκετά κοντά στην πηγή. Έτσι, η στρατηγική AFR εκμεταλλεύεται την συνεργασία για να βελτιώσει τον ασφαλή ρυθμό μετάδοσης αλλά δεν εγγυάται θετική χωρητικότητα ασφαλείας όταν ο ωτακουστής είναι κοντά στην πηγή.

5.2.3 Αποτελέσματα προσομοιώσεων

Στην ενότητα αυτή, θα αξιολογηθεί η απόδοση των τριών στρατηγικών που παρουσιάστηκαν παραπάνω μέσω προσομοιώσεων. Αρχικά, εκτελούνται κάποιες προσομοιώσεις για το συνεργατικό jamming (CJ) με AF αναμετάδοση, για να εξαχθεί η συμπεριφορά της στρατηγικής αυτής σε διάφορες περιπτώσεις. Έπειτα, συγκρίνονται οι τρεις στρατηγικές μεταξύ τους.



Σχήμα 5.2: Θέσεις κόμβων συστήματος (σε δύο διαστάσεις) προς προσομοίωση.

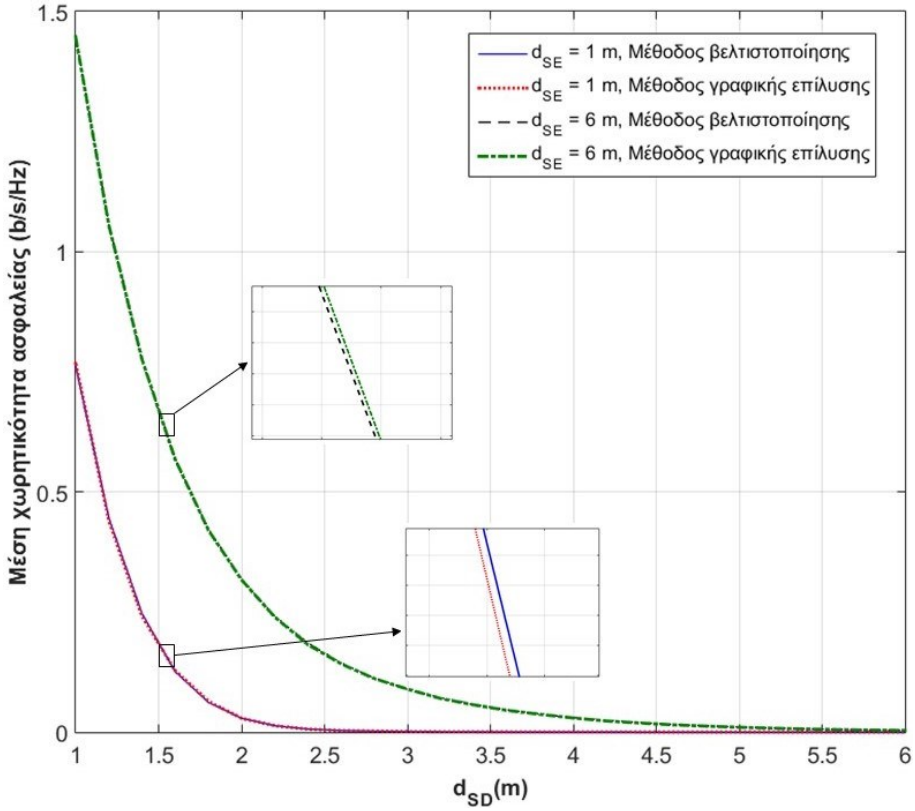
Για τις προσομοιώσεις θεωρήθηκε ότι τα κανάλια αντιμετωπίζουν διαλείψεις Rayleigh, μη επιλεκτικές ως προς τη συχνότητα, με απώλειες διάδοσης (path losses). Έτσι, το μέσο κέρδος ισχύος κάθε καναλιού ισούται με $E[h_{ij}] = d_{ij}^{-c}$, όπου d_{ij} είναι η απόσταση μεταξύ του κόμβου i και του κόμβου j και $c = 4$ ο εκθέτης απωλειών διαδρομής. Επίσης, θεωρείται στους κόμβους S και P διαθέσιμη ισχύς $P = 10\,Watt$ και διακύμανση θορύβου $\sigma^2 = 1$. Στο Σχήμα 5.2 φαίνονται οι αρχικές θέσεις των κόμβων του συστήματος με τις αντίστοιχες αποστάσεις. Οι δύο γωνίες που δίνονται στο σχήμα παραμένουν σταθερές.

Για τις προσομοιώσεις χρησιμοποιήθηκε το πρόγραμμα Matlab, στο οποίο για κάθε περίπτωση εκτελέστηκαν Monte Carlo προσομοιώσεις αποτελούμενες από 10^5 ανεξάρτητα δείγματα για κάθε κανάλι. Για την εύρεση της βέλτιστης τιμής του παράγοντα κατανομής ισχύος a χρησιμοποιήθηκαν δύο μεθοδολογίες: στη πρώτη μεθοδολογία (μέθοδος βελτιστοποίησης, όπως παρουσιάστηκε παραπάνω) έγινε επίλυση της εξίσωσης 2ου βαθμού μέσω του Matlab για να βρεθεί η τιμή του a που μηδενίζει τη πρώτη παράγωγο της R_S, ενώ σύμφωνα με τη δεύτερη μεθοδολογία, για κάθε τιμή του α στο διάστημα [0, 1] υπολογίζεται η αντίστοιχη τιμή της R_S και επιλέγεται η μεγαλύτερη τιμή (μέθοδος γραφικής επίλυσης). Όπως θα παρουσιαστεί στη συνέχεια, οι δυο μέθοδοι παράγουν παρόμοια αποτελέσματα. Ωστόσο, λόγω της πολυπλοκότητας του προβλήματος (εξαιτίας της εξίσωσης 8ου βαθμού και των προσομοιώσεων Monte Carlo για 5 κανάλια) η μεθοδολογία βελτιστοποίησης είναι αρκετά χρονοβόρα και για τον λόγο αυτό χρησιμοποιείται η μέθοδος γραφικής επίλυσης, η οποία είναι αρκετά πιο γρήγορη λόγω της ευκολίας που παρέχει το Matlab στη διαχείριση πινάκων. Συγκεκριμένα, χρησιμοποιείται για τον παράγοντα α διάνυσμα (πίνακας) από 0 μέχρι 1 με βήμα 0,0001. Για κάθε *α* βρίσκεται η αντίστοιχη τιμή του R_S και έτσι προκύπτει διάνυσμα από το οποίο επιλέγεται η μέγιστη τιμή και η αντίστοιχη θέση για το *α*. Συνεπώς, για κάθε ανεξάρτητη περίπτωση υπολογίζεται η βέλτιστη R_S με απόκλιση 10^{-4}. Αρχικά, χρησιμοποιήθηκαν και οι δύο μέθοδοι για να συγκριθούν και να αποδειχθεί η ορθότητα και η σύγκλιση των δύο μεθόδων.

5.2.3.1 Συνεργατικό jamming (CJ)

Οι προσομοιώσεις σε αυτήν την ενότητα αφορούν το συνεργατικό jamming με αναμεταδότη AF (CJ στρατηγική).

Στο Σχήμα 5.3 φαίνεται ο μέσος βέλτιστος ασφαλής ρυθμός σε σχέση με την απόσταση του προορισμού από την πηγή για AF αναμετάδοση με jamming. Για την προσομοίωση αυτή ο αναμεταδότης απέχει 3 μέτρα από την πηγή ενώ λαμβάνονται δύο περιπτώσεις όπου ο ωτακουστής απέχει 1 μέτρο και 6 μέτρα από την πηγή αντίστοιχα. Η απόσταση πηγής προορισμού (d_{SD}) μεταβάλλεται από 1m έως 6m. Οι υπόλοιπες αποστάσεις προκύπτουν εύκολα γεωμετρικά με βάση το Σχήμα 5.2. Όπως είναι λογικό, όσο η απόσταση πηγής-προορισμού μεγαλώνει τόσο μειώνεται και η μέση χωρητικότητα ασφαλείας. Στις προσομοιώσεις αυτές εκτελέστηκαν και οι δύο μέθοδοι για να αποδειχθεί ότι συγκλίνουν. Πράγματι, οι δύο καμπύλες παρουσιάζουν ελάχιστη απόκλιση.

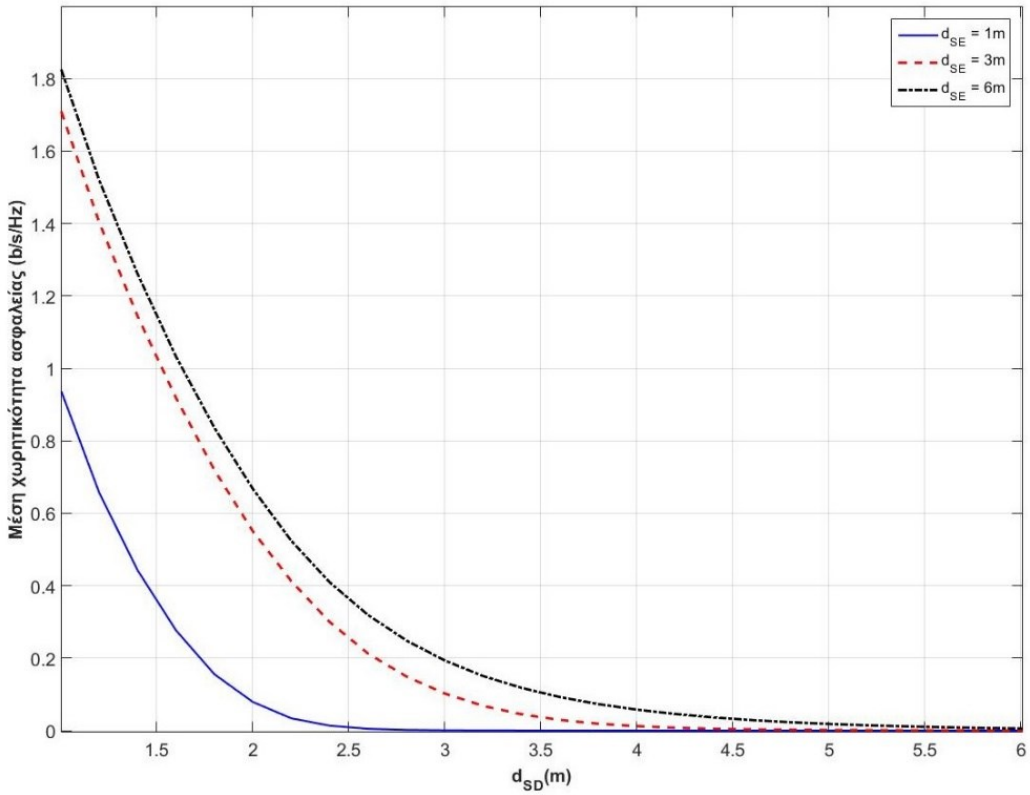


Σχήμα 5.3: Μέση χωρητικότητα ασφαλείας σε σχέση με τη θέση του προορισμού (P_{in} = 10 Watt, d_{SR} = 3m).

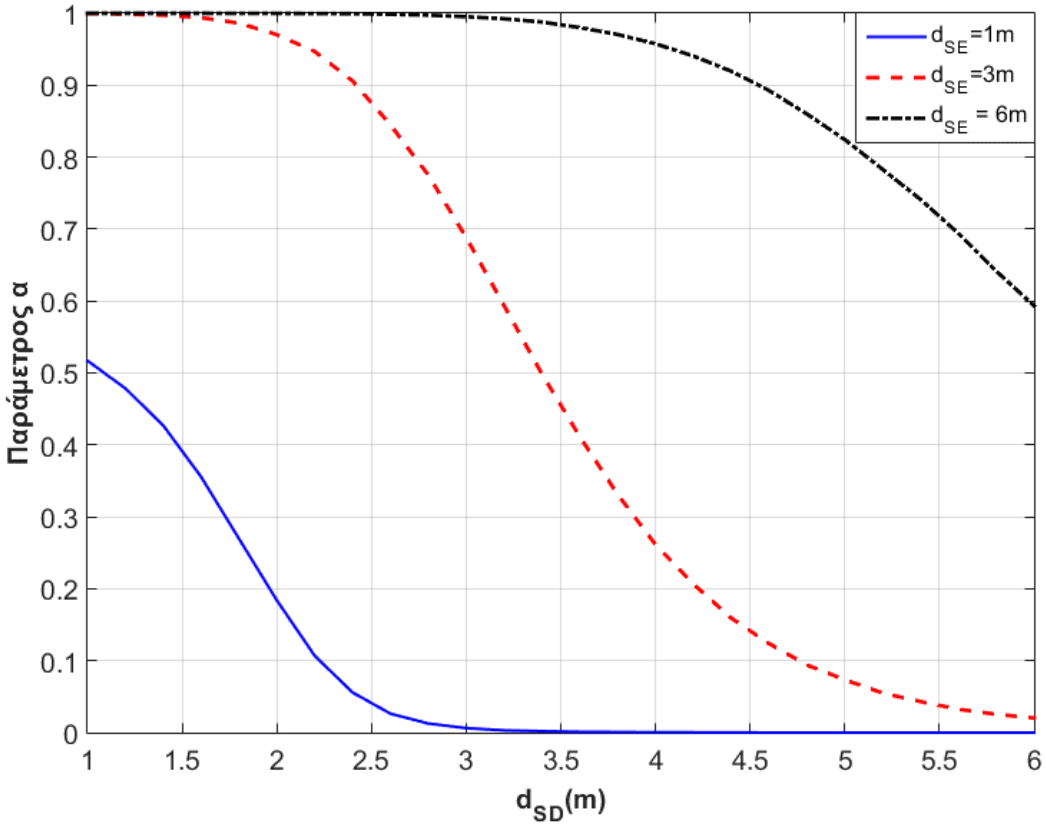
Στη συνέχεια παρουσιάζεται η συμπεριφορά του συνεργατικού jamming με αναμετάδοση AF αλλά και το πως κατανέμεται η ισχύς μεταξύ του σήματος πληροφορίας και του σήματος παρεμβολής (παράμετρος *α*) για διάφορες καταστάσεις του συστήματος.

Στο Σχήμα 5.4 παρουσιάζεται η μέση χωρητικότητα ασφαλείας για τρεις θέσεις του ωτακουστή στο σύστημα. Ο αναμεταδότης απέχει 1 μέτρο από την πηγή. Η χωρητικότητα ασφαλείας έχει υψηλότερες τιμές και η απόδοση της στρατηγικής είναι πολύ καλή όταν ο ωτακουστής βρίσκεται πιο μακριά από την πηγή σε σχέση με τον αναμεταδότη, δηλαδή όταν $d_{SE} = 3m$ και $d_{SE} = 6m$. Επιπλέον, στην περίπτωση που ωτακουστής και αναμεταδότης ισαπέχουν από τον πομπό η στρατηγική αυτή μας παρέχει ικανοποιητική μέση χωρητικότητα ασφαλείας εφόσον ο προορισμός δεν βρίσκεται σε απόσταση μεγαλύτερη των δύο μέτρων περίπου από τον πομπό. Όσο ο δέκτης απομακρύνεται η χωρητικότητα ασφαλείας τείνει στο 0.

Στο Σχήμα 5.5 απεικονίζεται το πως κατανέμεται η ισχύς μεταξύ του σήματος πληροφορίας και του σήματος παρεμβολής. Υπενθυμίζεται εδώ ότι *a* είναι το ποσοστό της ισχύος που ο πομπός και ο αναμεταδότης διαθέτουν για τη μετάδοση του σήματος πληροφορίας, ενώ (1-*α*) είναι το ποσοστό της ισχύος για τη μετάδοση του σήματος παρεμβολής. Το Σχήμα 5.5 επιβεβαιώνει ότι όσο πιο ευνοϊκές είναι οι συνθήκες για την επικοινωνία μεταξύ πηγής και προορισμού τόσο μεγαλώνει το ποσοστό της ισχύος που διατίθεται για τη μετάδοση του σήματος πληροφορίας. Αντίστοιχα, όταν ο ωτακουστής βρίσκεται κοντά στον πομπό και ο προορισμός μακριά (πχ. $d_{SE} = 1m$ και $d_{SD} = 6m$) δεν υπάρχει μετάδοση πληροφορίας αλλά μόνο jamming $(a \to 0)$.

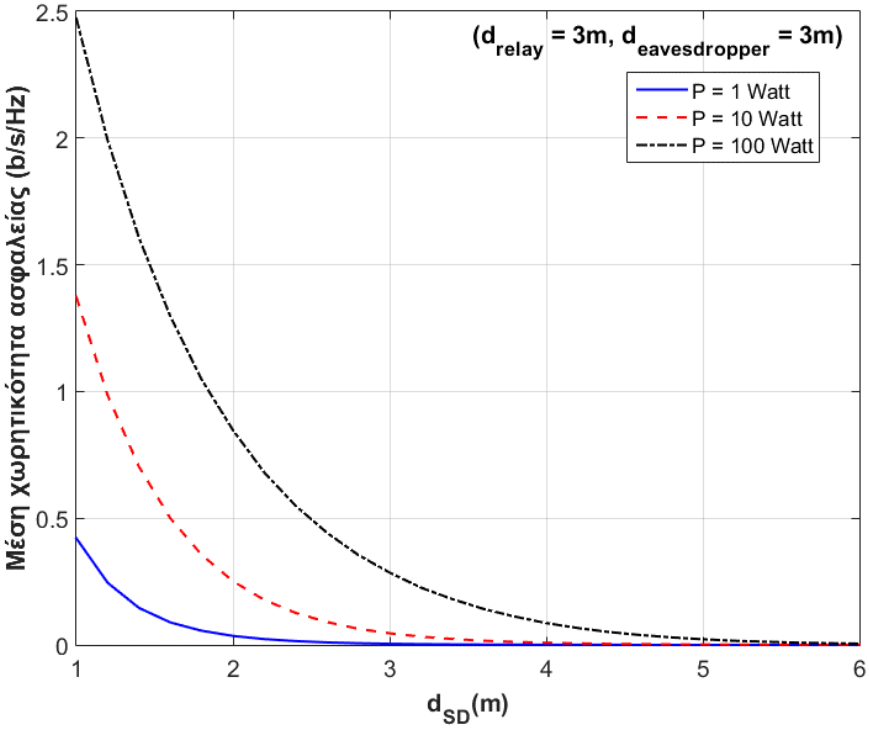


Σχήμα 5.4: Μέση χωρητικότητα ασφαλείας σε σχέση με τη θέση του προορισμού (P_{in} = 10 Watt, d_{SR} = 1m).

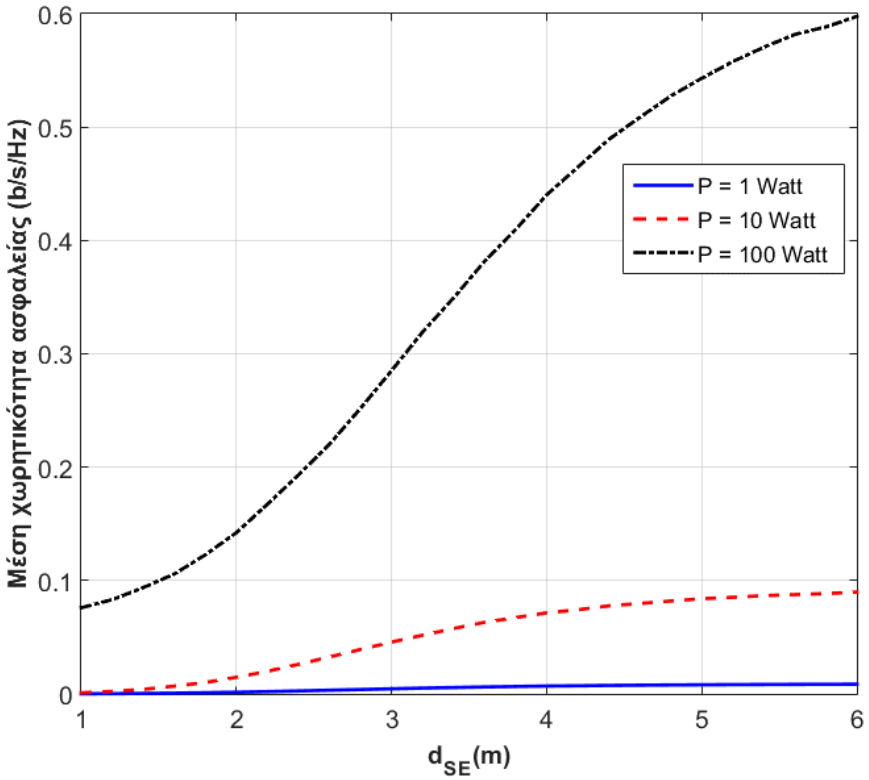


Σχήμα 5.5: Παράγοντας κατανομής ισχύος σε σχέση με τη θέση του δέκτη (P_{in}=10Watt, d_{SR}=1m).

Στις επόμενες δύο προσομοιώσεις (Σχήματα 5.6 και 5.7) παρουσιάζεται η συμπεριφορά του CJ για τρεις τιμές της διαθέσιμης ισχύος(1, 10 και 100 Watt αντίστοιχα). Προφανώς, με περισσότερη διαθέσιμη ισχύ, η πηγή και ο αναμεταδότης μπορούν να αυξήσουν τη χωρητικότητα ασφαλείας μεταξύ πηγής και προορισμού.



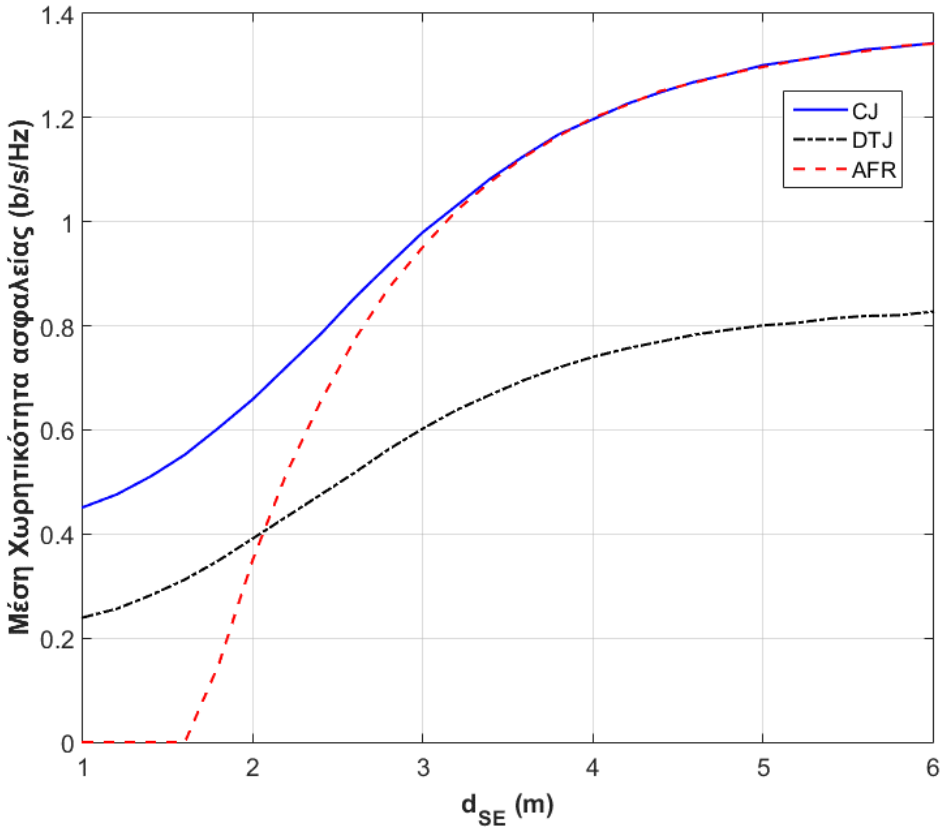
Σχήμα 5.6: Μέση χωρητικότητα ασφαλείας σε σχέση με τη θέση του δέκτη για διάφορες τιμές της διαθέσιμης ισχύος στην πηγή και τον αναμεταδότη (d_{SR} = 3m, d_{SE}=3m).



Σχήμα 5.7: Μέση χωρητικότητα ασφαλείας σε σχέση με την απόσταση του ωτακουστή από την πηγή για διάφορες τιμές της διαθέσιμης ισχύος (d_{SD} = 3m, d_{SR}=3m).

Στο Σχήμα 5.6 παρατηρείται ότι για το συγκεκριμένο σενάριο επιτυγχάνεται πολύ καλή χωρητικότητα ασφαλείας για $P_{in} = 10\,Watt$ ενώ ακόμη και με $P_{in} = 1\,Watt$ επιτυγχάνεται μη μηδενική χωρητικότητα ασφαλείας και η απόδοση του CJ είναι αρκετά καλή όταν ο δέκτης βρίσκεται σχετικά κοντά στον πομπό $(d_{SD} < 2m)$. Ενώ όπως παρατηρείται στο Σχήμα 5.7, όταν ο προορισμός και ο αναμεταδότης δεν βρίσκονται αρκετά κοντά στην πηγή (συγκεκριμένα απέχουν 3 μέτρα από αυτήν) χρειάζεται σημαντική ισχύς (άνω των 10 Watt) για να επιτευχθεί ικανοποιητικός ασφαλής ρυθμός.

Για τη σύγκριση μεταξύ των τριών στρατηγικών που παρουσιάστηκαν (CJ, DTJ και AFR) εκτελούνται προσομοιώσεις, όπου ο αναμεταδότης απέχει $\sqrt{2}$ μέτρα από την πηγή και ο δέκτης 2 μέτρα (βλ. Σχήμα 5.2). Η απόσταση μεταξύ πηγής-ωτακουστή μεταβάλλεται από 1 έως 6 μέτρα. Επίσης, θεωρούνται 50 watt διαθέσιμης ισχύος στην πηγή και τον αναμεταδότη αντίστοιχα, ενώ ο εκθέτης απωλειών διαδρομής είναι και εδώ $c = 4$.

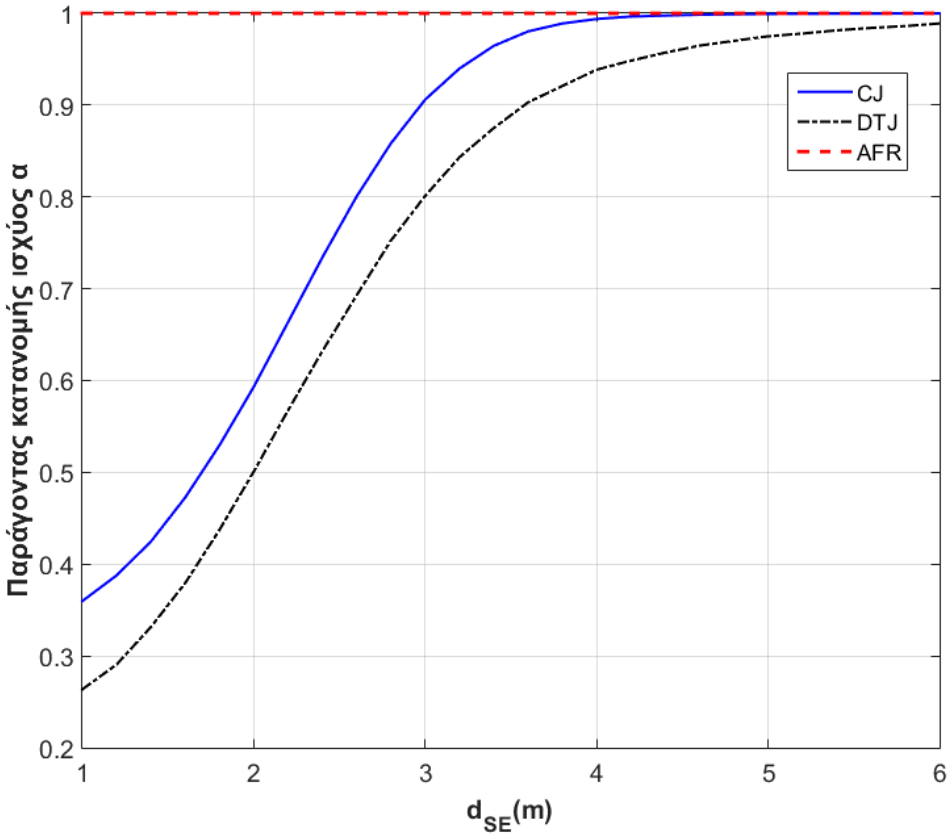


Σχήμα 5.8: Μέση χωρητικότητα ασφαλείας σε σχέση με τη θέση του ωτακουστή (d_{SD} = 2m, d_{SR}= $\sqrt{2}$ m)

Στο Σχήμα 5.8 παρουσιάζονται τα αποτελέσματα των προσομοιώσεων και παρατηρείται ότι το συνεργατικό jamming με αναμετάδοση (CJ) είναι πιο αποδοτικό από τις άλλες δύο στρατηγικές. Η αναμετάδοση AF χωρίς jamming (AFR) είναι αποδοτική όταν ο ωτακουστής είναι μακριά από την πηγή και τον αναμεταδότη. Σε αυτή την περίπτωση όλη η διαθέσιμη ισχύς χρησιμοποιείται για να βελτιώσει τα γ_{SD} και γ_{RD}. Όταν ο ωτακουστής κινείται αρκετά κοντά στην πηγή οι ρυθμοί ασφαλείας μειώνονται και στις τρεις στρατηγικές, αφού για την απευθείας μετάδοση με jamming (DTJ) αλλά και την CJ περισσότερη

ισχύς κατανέμεται για τη μετάδοση του σήματος παρεμβολής και έτσι προκαλείται παρεμβολή όχι μόνο στον ωτακουστή αλλά και στον δέκτη (όπως επιβεβαιώνεται και παρακάτω), ενώ στην AFR ο λόγος είναι ότι αυξάνεται ο γ_{RE}.

Τέλος, στο Σχήμα 5.9 απεικονίζονται οι μέσες τιμές του παράγοντα α για τις τρεις στρατηγικές σε σχέση με την απόσταση του ωτακουστή από την πηγή. Όπως είναι λογικό, όταν ο ωτακουστής βρίσκεται αρκετά κοντά στην πηγή το μεγαλύτερο ποσοστό της ισχύος χρησιμοποιείται για τη μετάδοση του σήματος παρεμβολής στις CJ και DTJ. Στη στρατηγική AFR δεν υπάρχει σήμα παρεμβολής ($\alpha = 1$).



Σχήμα 5.9: Μέση τιμή του παράγοντα *α* σε σχέση με τη θέση του ωτακουστή (d_{SD} = 2m, d_{SR}= $\sqrt{2}$ m).

Συνοπτικά, στο κεφάλαιο αυτό παρουσιάστηκε ένας μηχανισμός για τη βελτίωση της ασφάλειας στο φυσικό στρώμα. Η στρατηγική αυτή αφορά ασύρματα δίκτυα με αναμεταδότες AF δυο φάσεων παρουσία ενός ωτακουστή. Σύμφωνα με τη μέθοδο αυτή, τόσο η πηγή όσο και ο αναμεταδότης χρησιμοποιούν μέρος της διαθέσιμης ισχύος τους για τη μετάδοση του σήματος πληροφορίας και το υπόλοιπο μέρος για τη δημιουργία και μετάδοση του σήματος jamming. Προκύπτει έτσι πρόβλημα βελτιστοποίησης κατανομής ισχύος για τη μεγιστοποίηση του ασφαλή ρυθμού μετάδοσης, το οποίο αναλύθηκε και έγινε σύγκριση με άλλες δύο στρατηγικές κατανομής ισχύος. Οι προσομοιώσεις και τα αριθμητικά αποτελέσματα, επιβεβαίωσαν ότι πράγματι η στρατηγική που παρουσιάστηκε έχει ως αποτέλεσμα υψηλές τιμές χωρητικότητας ασφαλείας σε σχέση με τις άλλες δυο απλούστερες στρατηγικές ακόμη και σε συνθήκες όπου ο ωτακουστής βρίσκεται αρκετά κοντά στην πηγή.

Βιβλιογραφία – Αναφορές 5ου Κεφαλαίου

[1] E. Tekin and A. Yener, “Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy”, in *Proc. 44th Annu. Allerton Conf. Commun., Contr., Comput.*, 2006.

[2] E. Tekin and A. Yener, “The multiple access wire-tap channel: Wireless secrecy and cooperative jamming”, in *Proc. Information Theory and Applications Workshop*, 2007.

[3] E. Tekin and A. Yener, “The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming”, *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[4] J. Xie and S. Ulukus, “Secure degrees of freedom of the Gaussian wiretap channel with helpers”, in *Proc. 50th Annu. Allerton Conf. Commun., Contr., Comput.*, 2012.

[5] X. Rui, J. Hou, L. Zhou, “Decode-and-forwarding with full-duplex relaying”, in *International Journal of Communication Systems*, vol.25, no.2, pp.270-275, 2012.

[6] X. He and A. Yener, “Cooperation with an untrusted relay: A secrecy perspective”, *IEEE Trans. Inform. Theory*, vol. 56, no. 8, pp. 3807–3827, August 2010.

[7] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperative relays”, *IEEE Trans. Signal Processing*, vol. 58, no. 3, 2010.

[8] L. Tang, X. Gong, J. Wu, J. Zhang, “Secure wireless communications via cooperative relaying and jamming”, in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE* , vol., no., pp.849-853, 5-9 December 2011.

[9] A. Li, Y. Xu, Y. Wang, L. Sun, “Amplify-and-forward-based cooperative jamming strategy with power allocation for secure communication”, in *International Journal of Communication Systems*, published online in Wiley Online Library, 2014.

ΠΑΡΑΡΤΗΜΑ

ΘΕΩΡΙΑ ΒΕΛΤΙΣΤΟΠΟΙΗΣΗΣ

Στο παράρτημα αυτό παρουσιάζονται ορισμένες βασικές αρχές από τη θεμελιώδη θεωρία βελτιστοποίησης (optimization theory) [1], [2], δεδομένου ότι κατά τη σχεδίαση των ασύρματων συστημάτων εμφανίζονται συχνά προβλήματα βελτιστοποίησης και ιδιαίτερα κατά τη διαχείριση των πόρων τους. Αρχικά ορίζεται το πρόβλημα βελτιστοποίησης με περιορισμούς (constrained optimization problem) και στη συνέχεια παρουσιάζονται οι πολλαπλασιαστές Lagrange και τέλος οι συνθήκες Karush-Kuhn-Tucker (KKT).

Ορισμός προβλήματος με περιορισμούς

Στα περισσότερα προβλήματα βελτιστοποίησης εμπεριέχονται περιορισμοί στις παραμέτρους τους και εμφανίζονται εξαιτίας μαθηματικών και φυσικών περιορισμών όπως για παράδειγμα είναι η πεπερασμένη φύση των διαθέσιμων πόρων τους.

Ένα πρόβλημα βελτιστοποίησης με περιορισμούς έχει την εξής μορφή:

$$\begin{aligned} &\min_{x\in\mathbb{R}} f(x) \\ &\text{s.t.} \quad x \in S \end{aligned} \tag{Π.1}$$

όπου το διάνυσμα $x=(x_1,.....,x_n)$ αποτελεί τη μεταβλητή βελτιστοποίησης του προβλήματος στο σύνολο $\mathbb{R}$, η συνάρτηση $f:\mathbb{R}\quad\mathbb{R}$ αντιστοιχεί στην προς βελτιστοποίηση αντικειμενική συνάρτηση και $S\subseteq\mathbb{R}$ είναι το κλειστό σύνολο περιορισμών. Ας σημειωθεί ότι ένα πρόβλημα μεγιστοποίησης μπορεί να μετασχηματιστεί σε πρόβλημα ελαχιστοποίησης της μορφής (Π.1), εάν θεωρηθεί η αντίθετη αντικειμενική συνάρτηση $-f$.

Συνηθέστεροι τύποι περιορισμών

Στην πράξη προκύπτουν διάφοροι τύποι περιορισμών. Εδώ παρουσιάζονται οι πιο συνηθισμένοι [1]:

Οριακοί περιορισμοί (bound constraints): Είναι της μορφής $l_i \le x_i \le u_i$ για κάποιες κατώτερες και ανώτερες τιμές l_i και u_i, για $i = 1,...,n$.

Γραμμικές ανισότητες (linear inequalities): Οι περιορισμοί γραμμικών ανισοτήτων έχουν τη μορφή $Ax \le b$, για κάποιον πίνακα A διαστάσεων $m \times n$ και διάνυσμα b μήκους m.

Γραμμικές ισότητες (linear equalities): Οι περιορισμοί γραμμικών ισοτήτων έχουν τη μορφή $Ax = b$, όπου A και b πίνακες-στήλη m σειρών.

Μη γραμμικοί περιορισμοί (nonlinear constraints): Οι μη-γραμμικοί περιορισμοί στη γενική τους μορφή γράφονται ως εξής:

$$\begin{aligned} g_i(x) &= 0 \ για \ i = 1,...,m \\ h_j(x) &\le 0 \ για \ j = 1,...,p \end{aligned} \qquad (Π.2)$$

όπου g_i, h_j είναι συνεχείς συναρτήσεις.

Κυρτοί περιορισμοί (convex constraints): Ένα κυρτό σύνολο S ικανοποιεί την ακόλουθη ιδιότητα: για κάθε δύο σημεία x και y στο S το σημείο $(1-u)x+uy$, για $u \in [0,1]$, βρίσκεται επίσης στο S.

Συνθήκες πρώτης τάξης για τοπική βελτιστότητα

Ένα εφικτό[1] σημείο x είναι τοπικό ελάχιστο του προβλήματος βελτιστοποίησης (Π.1) εάν το $f(x)$ είναι μικρότερο από την τιμή που παίρνει η *f* για οποιοδήποτε άλλο εφικτό σημείο σε κάποια περιοχή του S. Έτσι, το x είναι τοπικό ελάχιστο εάν $x \in S$ και υπάρχει μια περιοχή με ακτίνα ε έτσι ώστε $f(x) \le f(y)$ για κάθε y στο $\{y \in S \mid 0 < d(x,y) < \varepsilon\}$. Ωστόσο, δεν είναι όλα τα τοπικά ελάχιστα κριτικά σημεία της f, επειδή πρέπει να ληφθούν υπόψη πως οι περιορισμοί επηρεάζουν την περιοχή.

Πολλαπλασιαστές Lagrange

Αρχικά, θεωρείται το πρόβλημα βελτιστοποίησης (Π.1) με μη-γραμμικό περιορισμό ισότητας, ως εξής:

$$\begin{aligned} &\min_{x \in \mathbb{R}} \ f(x) \\ &\text{s.t. } g_i(x) = 0 \ για \ i = 1,...,m \end{aligned} \qquad (Π.3)$$

Όπου οι συναρτήσεις f και g είναι διαφορίσιμες.

[1] Ένα σημείο ονομάζεται εφικτό όταν ικανοποιεί τους περιορισμούς του προβλήματος.

Διακρίνονται δύο περιπτώσεις:

Ένα περιορισμός ($m=1$**)**. Σύμφωνα με την αρχή των πολλαπλασιαστών Lagrange, κάθε τοπικό μέγιστο ή ελάχιστο του προβλήματος (Π.3) πρέπει ταυτόχρονα να ικανοποιεί τις ακόλουθες εξισώσεις:

$$\begin{aligned} \nabla f(x) + \lambda \nabla g_1(x) &= 0 \\ g_1(x) &= 0 \end{aligned} \qquad (\Pi.4)$$

για κάποια τιμή του λ. Η μεταβλητή λ είναι γνωστή ως πολλαπλασιαστής Lagrange. Σημειωτέον ότι ίσως υπάρχουν πολλαπλά σημεία x τα οποία ικανοποιούν την (Π.4), κάθε μία από τις οποίες έχει διαφορετικό πολλαπλασιαστεί Lagrange.

Πολλαπλοί περιορισμοί. Οι παρακάτω συνθήκες γενικεύουν τους πολλαπλασιαστές Lagrange για πολλαπλούς περιορισμούς:

$$\begin{aligned} \nabla f(x) + \lambda_1 \nabla g_1(x) + \ldots + \lambda_m \nabla g_m(x) &= 0 \\ g_1(x) &= 0 \\ &\vdots \\ g_m(x) &= 0 \end{aligned} \qquad (\Pi.5)$$

όπου $\lambda_1, \ldots, \lambda_m$ είναι οι πολλαπλασιαστές Lagrange. Όλα τα τοπικά ελάχιστα πρέπει να ικανοποιούν την (Π.5). Έτσι η (Π.5) είναι αναγκαία αλλά όχι ικανή συνθήκη για βελτιστότητα.

Χρήση πολλαπλασιαστών Lagrange για αριθμητική βελτιστοποίηση. Για το πρόβλημα βελτιστοποίησης (Π.3) ορίζεται η ακόλουθη συνάρτηση Lagrange:

$$L(x, \lambda_1, \ldots, \lambda_m) = f(x) + \sum_{i=1}^{m} \lambda_i g_i(x) \qquad (\Pi.6)$$

Τότε το πρόβλημα βελτιστοποίησης με περιορισμούς ισοδυναμεί με το πρόβλημα εύρεσης των κρίσιμων σημείων της συνάρτησης L στο $\mathbb{R}$. Επομένως, εάν ορισθεί $\lambda = (\lambda_1, \ldots, \lambda_m)$ αρκεί να βρεθεί σημείο (x, λ) τέτοιο ώστε:

$$\nabla L(x, \lambda) = \begin{bmatrix} \nabla_x L(x, \lambda) \\ \nabla_\lambda L(x, \lambda) \end{bmatrix} = \begin{bmatrix} \nabla f(x) + \sum_{i=1}^{m} \lambda_i \nabla g_i(x) \\ g_1(x) \\ \vdots \\ g_m(x) \end{bmatrix} = 0 \qquad (\Pi.7)$$

Συνθήκες Karush-Kuhn-Tucker

Οι ΚΚΤ συνθήκες επεκτείνουν τους πολλαπλασιαστές Lagrange σε προβλήματα βελτιστοποίησης με περιορισμούς ανισοτήτων.

Το πρόβλημα βελτιστοποίησης με περιορισμούς ανισοτήτων τίθεται ως εξής:

$$\begin{aligned} &\min_{x\in\mathbb{R}} f(x) \\ &\text{s.t. } g_i(x) = 0 \ \gamma\iota\alpha\ i = 1,...,m \\ &\quad h_j(x) \le 0 \ \gamma\iota\alpha\ j = 1,...,p \end{aligned} \qquad (\Pi.8)$$

όπου όλες οι συναρτήσεις είναι διαφορίσιμες.

Ένα περιορισμός ($m = 0$ και $p = 1$ **)**. Εάν x είναι τοπικό ελάχιστο της $f(x)$ τέτοιο ώστε $h_1(x) < 0$, τότε ο περιορισμός ικανοποιείται για μια περιοχή γύρω από το x και έτσι το x είναι τοπικό ελάχιστο του προβλήματος. Από την άλλη πλευρά, θα μπορούσε να υπάρξει τοπικό ελάχιστο στο σύνορο του συνόλου S, το οποίο αποτελείται από τα σημεία που ικανοποιούν τη σχέση $h_1(x) = 0$. Συνεπώς, για να βρεθούν αυτά τα σημεία, η h_1 αποτελεί περιορισμό ισότητας και μπορεί να χρησιμοποιηθεί η μέθοδος των πολλαπλασιαστών Lagrange.

Επομένως, υπάρχουν οι ακόλουθες δύο περιπτώσεις:

6. $\nabla f(x) = 0$ και $h_1(x) < 0$.
7. $h_1(x) = 0$ και υπάρχει πολλαπλασιαστής Lagrange μ τέτοιος ώστε:

$$\nabla f(x) + \mu \nabla h_1(x) = 0$$

Ένας τρόπος να γραφτούν μαζί οι δύο παραπάνω περιπτώσεις είναι με το ακόλουθο σύνολο:

$$\begin{aligned} \nabla f(x) + \mu \nabla h_1(x) &= 0 \\ \mu &\ge 0 \\ h_1(x) &\le 0 \\ \mu h_1(x) &= 0 \end{aligned} \qquad (\Pi.9)$$

στο οποίο ο όρος $\mu h_1(x) = 0$ αποτελεί τη συμπληρωματική συνθήκη.

Πολλαπλοί περιορισμοί ($m = 0$**).** Στην περίπτωση αυτή οι λύσεις του προβλήματος (Π.8) πρέπει να ικανοποιούν τις εξής συνθήκες:

$$\begin{aligned} \nabla f(x) + \mu_1 \nabla h_1(x) + ... + \mu_p \nabla h_p(x) &= 0 \\ \mu_j &\ge 0 \ \gamma\iota\alpha\ j = 1,...,p \\ h_j(x) &\le 0 \ \gamma\iota\alpha\ j = 1,...,p \\ \mu_j h_j(x) &= 0 \ \gamma\iota\alpha\ j = 1,...,p \end{aligned} \qquad (\Pi.10)$$

όπου $\mu_1,...,\mu_p$ είναι οι πολλαπλασιαστές ΚΚΤ.

Γενική μορφή. Χρησιμοποιώντας τη συνάρτηση Lagrange οι συνθήκες που πρέπει να ικανοποιούν οι λύσεις του προβλήματος (Π.8) γράφονται ως εξής:

$$\begin{aligned} \nabla L(x,\lambda,\mu) = \nabla f(x) + \sum_{i=1}^{m} \lambda_i \nabla g_i(x) + \sum_{j=1}^{p} \mu_j \nabla h_j(x) = 0 \\ \mu_j \geq 0 \ \gamma\iota\alpha \ j = 1,...,p \\ g_i(x) = 0 \ \gamma\iota\alpha \ i = 1,...,m \\ h_j(x) \leq 0 \ \gamma\iota\alpha \ j = 1,...,p \\ \mu_j h_j(x) = 0 \ \gamma\iota\alpha \ j = 1,...,p \end{aligned} \qquad (\Pi.11)$$

όπου $\lambda_1,...,\lambda_m$ και $\mu_1,...,\mu_p$ είναι οι πολλαπλασιαστές ΚΚΤ.

Βιβλιογραφία Παραρτήματος

[1] S. Boyd, L. Vandenberghe, *Convex Optimization,* Cambridge University Press, 2004.

[2] J. M. Borwein, A. S. Lewis, *Convex Analysis and Nonlinear Optimization,* Springer, 2000.