ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΠΜΣ ΣΤΗΝ ΕΠΙΣΤΗΜΗ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Ασφάλεια ασύρματων δικτύων στο φυσικό επίπεδο»

PHY layer security in wireless networks

ΔΗΜΗΤΡΙΟΣ ΒΟΤΤΑΣ

Α.Μ.: 2022202002004

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: κ. ΚΩΝΣΤΑΝΤΙΝΟΣ ΠΕΠΠΑΣ

Τρίπολη Δεκέμβριος 2022

Περιεχόμενα

Περίληψη

Στην παρούσα εργασία εξετάζεται η ασφάλεια των ασύρματων δικτύων στο φυσικό επίπεδο.. Αρχικά παρουσιάζονται οι απαιτήσεις ασφαλείας στα ασύρματα δίκτυα, καθώς και οι προσεγγίσεις στο φυσικό επίπεδο. Στη συνέχεια, μέσα από την δεύτερη παρουσίαση, γίνεται αναφορά στη συνεργατική αναμετάδοση με αξιόπιστους και αναξιόπιστους αναμεταδότες, καθώς και στη συνεργατική παρεμβολή. Επίσης, εξετάζουμε μία περίπτωση ενός δικτύου μυστικότητας με πολλούς φιλικούς παρεμβολείς και υποκλοπείς, όπου η πηγή θέλει να επικοινωνήσει με ασφάλεια με τον προορισμό. Μέσω μαθηματικών εκφράσεων καταλήγουμε σε ένα αλγόριθμο και σχολιάζονται τα αποτελέσματα. Τέλος παρουσιάζονται εν συντομία τα συστήματα πολλαπλών εισόδων- πολλαπλών εξόδων (MIMO) και τα θέματα ασφάλειας σε αυτά.

Τέλος, η εργασία ερευνά την αναζήτηση ασφάλειας φυσικού επιπέδου σε διάφορες τεχνολογίες 5G, όπως π.χ μαζικό κύμα πολλαπλών εισόδων πολλαπλών εξόδων(massive MIMO), χιλιοστών επικοινωνίας, ετερογενή δίκτυα, μη ορθογώνια πολλαπλής πρόσβασης και full-duplex. Επίσης, συμπεριλαμβάνουμε τις βασικές έννοιες καθεμιάς από τις προαναφερθείσες τεχνολογίες. Προσδιορίζονται επίσης μελλοντικά πεδία έρευνας και τεχνικές προκλήσεις της ασφάλειας φυσικού επιπέδου.

Λέξεις – κλειδιά: ασύρματα δίκτυα, φυσικό επίπεδο, χωρητικότητα μυστικότητας, συνεργατική αναμετάδοση, παρεμβολέας, υποκλοπέας, πιθανότητα διακοπής απορρήτου, 5G, MIMO.

1 Εισαγωγή

Τα ασύρματα δίκτυα έχουν έναν αρκετά σημαντικό ρόλο σε πολλές εφαρμογές. Ωστόσο, η ασφάλεια της μεταφοράς πληροφοριών μέσω ασύρματων δικτύων παραμένει ένα κρίσιμο ζήτημα. Είναι εξαιρετικής σημασίας να διασφαλιστεί ότι οι εμπιστευτικές πληροφορίες είναι προσβάσιμες μόνο στους νόμιμους χρήστες και όχι στους εισβολείς.

Η προστασία από κακόβουλους εισβολείς αποτελεί ένα ζήτημα που διερευνάται στα σύγχρονα τηλεπικοινωνιακά δίκτυα από τους νόμιμους χρήστες τους, τόσο για την προστασία των δεδομένων όσο και για την παροχή ποιοτικών υπηρεσιών. Τα ασύρματα δίκτυα είναι ευάλωτα σε θέματα ασφάλειας λόγω δύο βασικών χαρακτηριστικών τους, την εκπομπή σε όποιον χρήστη έχει πρόσβαση στο μέσο διάδοσης (αέρας) και την εύκολη παρεμβολή από τους άλλους χρήστες.

Η εμπλοκή και η υποκλοπή είναι δύο κύριες επιθέσεις στο φυσικό επίπεδο ενός ασύρματου δικτύου..

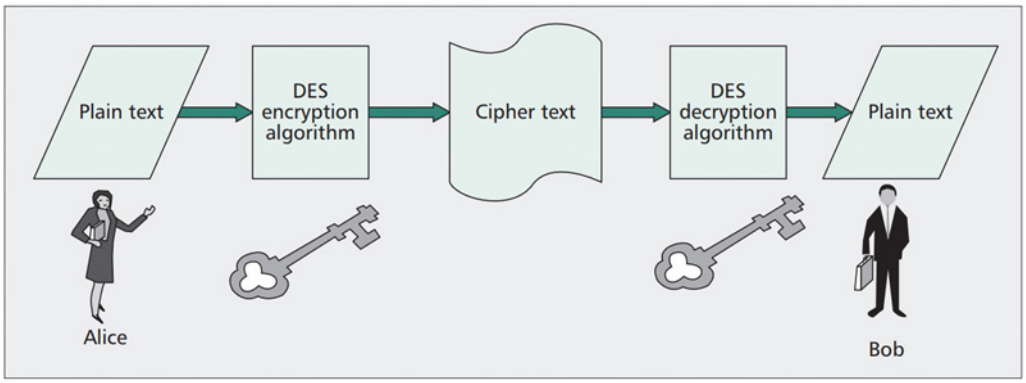
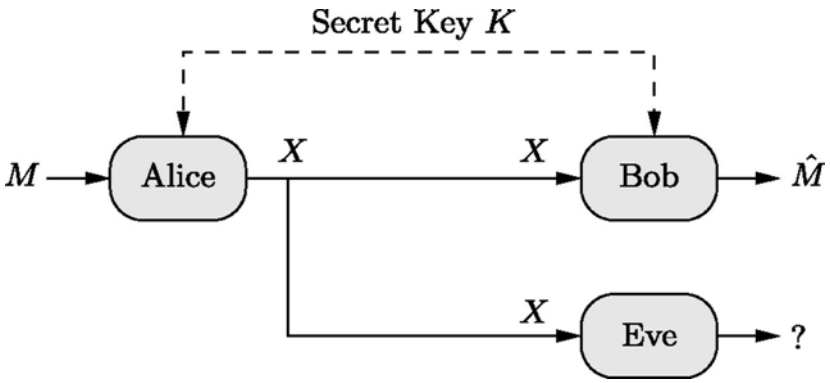


Figure 1. *The symmetric data encryption/decryption algorithm has been widely used in networks. This secret key cryptology operates in both transmission directions. Alice sends an encrypted message to Bob with a secret key. Bob may use the secret key to decipher the message. Because this message has been encrypted, even if the message is intercepted, the eavesdropper between Alice and Bob will not have the secret key to decipher the message.*

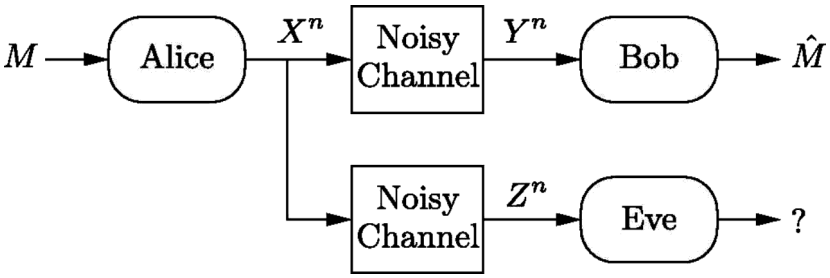
Αντί να χρησιμοποιήσετε ένα πρόσθετο κανάλι, οι μέθοδοι φυσικού επιπέδου μπορούν να χρησιμοποιηθούν εδώ για τη διανομή μυστικών κλειδιών, την παροχή απορρήτου τοποθεσίας και τη συμπλήρωση αλγορίθμων ασφαλείας ανώτερου επιπέδου. Η εφαρμογή συστημάτων ασφαλείας φυσικού επιπέδου καθιστά πιο δύσκολο για τους εισβολείς να αποκρυπτογραφήσουν τις μεταδιδόμενες πληροφορίες.

1.1 Shannon System



Οι βασικές έννοιες της θεωρητικής ασφάλειας πληροφοριών εισήχθησαν για πρώτη φορά από τον Shannon στην εργασία του το 1945. Ο πομπός αποσκοπεί στην ασφαλή αποστολή ενός μηνύματος M σε ένα νόμιμο (legitimate) δέκτη, ο οποίος παράγει μια εκτίμηση του μηνύματος Mˆ . Αυτό πρέπει να γίνεται με τη μικρότερη δυνατή πιθανότητα σφάλματος εκτίμησης, ενώ ο υποκλοπέας αποκτά όσο το δυνατόν λιγότερες πληροφορίες. Για να επιτευχθεί αυτό, πρέπει να υπάρχει ένα πλεονέκτημα του νόμιμου δέκτη σε σχέση με τον υποκλοπέα, το οποίο μοντελοποιήθηκε από τον Shannon ως μυστικό κλειδί K. Αυτό είναι μια πληροφορία που είναι διαθέσιμη στον πομπό και στον νόμιμο δέκτη, αλλά όχι στον υποκλοπέα. Χρησιμοποιώντας το κλειδί K, ο πομπός κωδικοποιεί το M σε μια κωδική λέξη X, η οποία στη συνέχεια μεταδίδεται στον νόμιμο δέκτη και επίσης αποκτάται από τον υποκλοπέα. Στη συνέχεια, ο νόμιμος δέκτης είναι σε θέση να παράγει την εκτίμηση Mˆ χάρη στη γνώση του κλειδιού K.

1.2 Wyner's Wiretap Channel

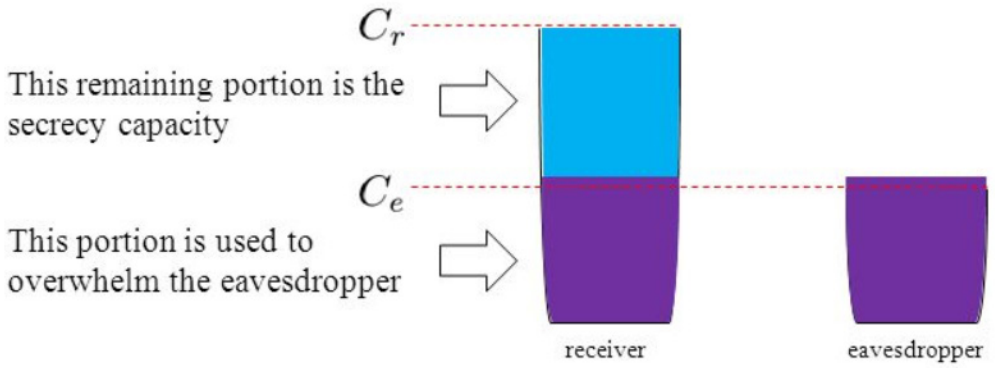


Μια προφανής αδυναμία της έννοιας της ασφάλειας του Shannon είναι ότι δεν λαμβάνει υπόψη τον θόρυβο που επηρεάζει τις παρατηρήσεις της Eve σχετικά με την κωδική λέξη. Προκειμένου να ληφθούν υπόψη τα χαρακτηριστικά PHY του ασύρματου συστήματος, ο Wyner εισήγαγε ένα μοντέλο διαύλου υποκλοπής (wiretap channel model) το οποίο αναφέρουμε ως το υποβαθμισμένο κανάλι διαύλου υποκλοπής DW T C (Degraded Wiretap Channel), Σε αυτό το μοντέλο, η Alice κωδικοποιεί το μήνυμα M σε μια κωδική λέξη X, η οποία στη συνέχεια μεταδίδεται στον Bob μέσω του κύριου καναλιού W και λαμβάνεται από τον Bob ως Y , ο οποίος στη συνέχεια παράγει μια εκτίμηση Mˆ του μηνύματος. Το Y περνάει επίσης μέσω του καναλιού του ωτακουστή W0 και λαμβάνεται από την Eve ως Z.

1.3 Secrecy Capacity - χωρητικότητα μυστικότητας

Η χωρητικότητα μυστικότητας ορίζεται ως η διαφορά μεταξύ της χωρητικότητας του κύριου καναλιού και της χωρητικότητας του καναλιού υποκλοπής.

Για τον υπολογισμό αυτής της μέτρησης απαιτείται πλήρης γνώση των καναλιών επικοινωνίας



Η χωρητικότητα μυστικότητας, C_s, για ένα ασύρματο κανάλι είναι η μέτρηση που χρησιμοποιείται περισσότερο στην αξιολόγηση PLS. Το C_s ορίζεται ως η διαφορά χωρητικότητας μεταξύ του κύριου και του καναλιού υποκλοπής. Αυστηρά μιλώντας, ορίζει το μέγιστο μυστικό ρυθμό με τον οποίο οι μυστικές πληροφορίες καλύπτονται αξιόπιστα στον πομπό ενώ παραμένουν μη ανακτήσιμες από την Eve [51]. Ως εκ τούτου, το C_s σε μια οιονεί στατική περίπτωση καναλιού εξασθένισης διατυπώνεται όπως στο [26] από τον τύπο:

$$C_{\mathrm{S}} = \max\{C_{\mathrm{B}} - C_{\mathrm{E}}, 0\}$$
$$= \max\{\mathrm{W}\log_2(1+\gamma_{\mathrm{B}}) - \mathrm{W}\log_2(1+\gamma_{\mathrm{E}}), 0\} \qquad (1)$$

Χωρίς απώλεια γενικότητας, θεωρείται κανονικοποιημένο εύρος ζώνης W = 1 στην προαναφερθείσα χωρητικότητα για μορφοποιήσεις. Σύμφωνα με αυτό το σενάριο, είναι δυνατό να επιτευχθεί ασφαλής μετάδοση μόνο εάν ο νόμιμος σύνδεσμος έχει καλύτερο SNR από τον σύνδεσμο υποκλοπής, δηλαδή:

$$C_{\mathrm{S}} = \begin{cases} \log_2\left(\frac{1+\gamma_{\mathrm{B}}}{1+\gamma_{\mathrm{E}}}\right), & \text{if } \gamma_{\mathrm{B}} > \gamma_{\mathrm{E}} \\ 0, & \text{if } \gamma_{\mathrm{B}} \leq \gamma_{\mathrm{E}}, \end{cases} \qquad (2)$$

Αξίζει να τονιστεί ότι το C_S χρησιμοποιείται ευρέως από τους ερευνητές για τον υπολογισμό του SOP [32].

1.4 Πιθανότητα διακοπής της μυστικότητας

Το SOP ορίζεται ως η πιθανότητα ότι το απόρρητο της χωρητικότητας πέφτει κάτω από ένα στόχο απορρήτου της R_S. Με άλλα λόγια, όταν το τρέχον C_S δεν είναι περισσότερο από ένα προκαθορισμένο R_S στόχο, συμβαίνει η διακοπή του απορρήτου. Αυτό το γεγονός σημαίνει ότι το τρέχον ποσοστό απορρήτου δεν μπορεί να εγγυηθεί την απαίτηση ασφάλειας. Μπορεί να διατυπωθεί ως στο [53] από την εξίσωση :

$$\mathrm{SOP} = \Pr\{C_{\mathrm{S}}(\gamma_{\mathrm{B}}, \gamma_{\mathrm{E}}) < R_{\mathrm{S}}\}$$
$$\overset{(a)}{=} \Pr\left\{\left(\frac{1+\gamma_{\mathrm{B}}}{1+\gamma_{\mathrm{E}}}\right) < 2^{R_{\mathrm{S}}}\right\}$$
$$\overset{(b)}{\geq} \Pr\left\{\frac{\gamma_{\mathrm{B}}}{\gamma_{\mathrm{E}}} < 2^{R_{\mathrm{S}}}\right\} \qquad (3)$$

όπου το Pr {·} δηλώνει πιθανότητα. Το SOP στο (a) υποδηλώνει ότι κάθε φορά που $R_S < C_S$, το κανάλι υποκλοπής θα είναι χειρότερο από το νόμιμο κανάλι. Έτσι, είναι δυνατή η ασφαλής επικοινωνία [54]. Αξίζει να σημειωθεί ότι η τελευταία λέξη της τεχνολογίας στο ερευνητικό θέμα του PLS που εστιάζει σε διαφορετικούς τύπους καναλιών που εξασθενούν είναι ότι ο υπολογισμός του (b) λόγω της απλούστερης μαθηματικής του ικανότητας μεταφοράς όσον αφορά τη διατύπωση στο (a). Επιπλέον, η

εξίσωση στο (b) είναι πολύ γνωστή ως το κάτω όριο του SOP και αντιπροσωπεύει την αναλογία δύο τετραγωνισμένων τυχαίων μεταβλητών (RVs), συγκεκριμένα: γ_B και γ_E, που μπορεί να ακολουθήσει οποιαδήποτε εξασθένιση κατανομής. Σε αυτό το πλαίσιο, για να αξιολογήσουμε την απόδοση του PLS σε γενικά κανάλια και τις αντίστοιχες ειδικές περιπτώσεις τους, δύο πρόσφατες εργασίες που προτάθηκαν στο [35, 36] αναπτύχθηκαν σε κλειστή μορφή για την αναλογία δύο τετραγώνων RV της μεγάλης πλειοψηφίας των μοντέλων καναλιών που ξεθωριάζουν που χρησιμοποιούνται για να χαρακτηρίσουν το περιβάλλον διάδοσης του 5G. Παρά τις σημαντικές πληροφορίες που παρέχει το SOP στον χαρακτηρισμό της απόδοσης μυστικότητας, έχει τα εξής μειονεκτήματα:

i) δεν μπορεί να ποσοτικοποιήσει τον όγκο των δεδομένων που διαρρέουν στους υποκλοπείς όταν συμβαίνει η διακοπή (δηλαδή, ασφάλεια μετάδοσης).
ii) δεν μπορεί να προσφέρει καμία πληροφορία σχετικά με την ικανότητα του Bob να αποκωδικοποιεί τα μεταδιδόμενα δεδομένα με επιτυχία (δηλαδή, αξιοπιστία μετάδοσης).
iii) δεν μπορεί να προσφέρει οποιαδήποτε πληροφορία σχετικά με την ικανότητα του υποκλοπέα να αποκρυπτογραφήσει εμπιστευτικά δεδομένων με επιτυχία.
iv) δεν μπορεί να είναι συνδέεται άμεσα με τις απαιτήσεις ποιότητας υπηρεσίας (QoS) για υπηρεσίες δικτύου [57].

Με κίνητρο τους περιορισμούς του SOP, οι ερευνητές στο [58, 59] πρότειναν νέες μετρήσεις για να ξεπεραστούν τα τρία προαναφερθέντα μειονεκτήματα του SOP. Έτσι, οι συγγραφείς δίνουν περισσότερες πληροφορίες στο PLS και πώς μετριέται το απόρρητο. Αξίζει τον κόπο να αναφέρουμε ότι ο ορισμός του SOP και του C_S μπορεί επίσης να χρησιμοποιηθεί στο σενάριο με πολλαπλές κεραίες σε διαφορετικούς κόμβους. Οι αναγνώστες αναφέρονται στο [60-62] για περαιτέρω ανάλυση αυτού του τομέα. Στη συνέχεια, σύμφωνα με το κλασική SOP που ορίζεται παραπάνω, η εναλλακτική διακοπή μυστικότητας ορίζεται ακολούθως.

1.5 Εναλλακτική Διατύπωση Διακοπής Απορρήτου

Όπως αναφέρθηκε προηγουμένως, η συμβατική διατύπωση SOP στο (3) δεν κάνει διάκριση μεταξύ αξιοπιστίας και ασφάλειας. Επομένως, ένα συμβάν διακοπής λειτουργίας στο (3) μπορεί να συνεπάγεται είτε σφάλμα για την επίτευξη μυστικότητας είτε ότι το μεταδιδόμενο μήνυμα δεν μπορεί να αποκωδικοποιηθεί με επιτυχία από τον Bob. Από τις παραπάνω σκέψεις, προτάθηκε μια εναλλακτική διατύπωση μυστικότητας εκτός ηλικίας στο [63], η οποία μετράει ότι τα μεταδιδόμενα δεδομένα δεν τηρούν το απόρρητο. Σε μία τέτοια σύνθεση, η διαφορά ρυθμού R_E $\Delta = R_B - R_S$ δηλώνει το κόστος της ασφάλειας κατά τη μετάδοση των δεδομένων. Επίσης, R_B είναι ο ρυθμός των μεταδιδόμενων μηνυμάτων και R_S είναι το ποσοστό των εμπιστευτικών δεδομένων. Αξίζει να αναφέρουμε ότι ο Bob μπορεί να αποκωδικοποιήσει οποιοδήποτε μεταδιδόμενο μήνυμα επιτυχώς εάν και μόνο εάν $C_B > R_B$, ενώ η μυστικότητα αποτυγχάνει αν $C_E > R_E$. Επομένως, το εναλλακτικό SOP μπορεί να προσομοιωθεί ως η υπό όρους πιθανότητα ένα μήνυμα να μεταδίδεται.

$$SOP_A = \Pr\{C_E > R_B - R_S | \text{μετάδοση μηνύματος}\} \quad (4)$$

Σε αντίθεση με τον ορισμό SOP στο (3), η διατύπωση στο (4) λαμβάνει υπόψη σημαντικές παραμέτρους σχεδιασμού του συστήματος, συμπεριλαμβανομένου του ρυθμού των μεταδιδόμενων μηνυμάτων R_B, και το γεγονός αν μεταδόθηκε ένα μήνυμα ή όχι. Επιπλέον, αυτή η μέτρηση είναι χρήσιμη όταν η Alice γνωρίζει το στιγμιαίο CSI του Bob. Δεδομένου ότι σε αυτό το σενάριο, η Alice επιλέγει αν θα μεταδώσει ή όχι και αν η Alice αποφασίζει να μεταδώσει, θα το κάνει ενδεχομένως με κυμαινόμενα ποσοστά ανάλογα με το CSI του Bob. Σε αντίθεση περίπτωση, δηλαδή όταν η μετάδοση πραγματοποιείται με σταθερό ρυθμό, η εναλλακτική διατύπωση SOP στο (4) μειώνει την άνευ όρων πιθανότητα.

Αυτή η μέτρηση αναγνωρίζεται στις πιο πρόσφατες ερευνητικές εργασίες που σχετίζονται με την απόδοση στο PLS. Οι αναγνώστες μπορούν να ανατρέξουν στο [64–68] για πιο λεπτομερείς πληροφορίες σχετικά με αυτό το ερευνητικό θέμα.

1.6 Μετρήσεις βασισμένες σε κλασματική αμφισβήτηση

Με βάση τον περιορισμό του κλασικού SOP στο (3) για τη μέτρηση τόσο της ποσότητας διαρροής δεδομένων όσο και της ικανότητας της Eve να αποκωδικοποιεί εμπιστευτικά δεδομένα, τρεις νέες μετρήσεις προτάθηκαν στο [69]. Αυτές οι μετρήσεις μετρούν την απόδοση μυστικότητας των ασύρματων συστημάτων από την προοπτική μερικής μυστικότητας έναντι οιονεί στατικής εξασθένισης. Η κλασματική αμφιβολία (δηλαδή, Δ) είναι τυχαία ποσότητα λόγω των χαρακτηριστικών εξασθένισης του μέσου πολλαπλασιασμού. Μαθηματικά, η κλασματική ισοδυναμία για μια δεδομένη πραγματοποίηση εξασθένισης του καναλιού εκφράζεται ως [69]

$$\Delta = \begin{cases} 1, & \text{if } C_{\mathrm{E}} \leq C_{\mathrm{B}} - R_{\mathrm{S}} \\ \left(C_{\mathrm{B}} - C_{\mathrm{E}}\right)/R_{\mathrm{S}}, & \text{if } C_{\mathrm{B}} - R_{\mathrm{S}} < C_{\mathrm{E}} < C_{\mathrm{B}} \\ 0, & \text{if } C_{\mathrm{B}} \leq C_{\mathrm{E}}. \end{cases} \qquad (5)$$

Από το (5), οι συγγραφείς στο [49] πρότειναν τις ακόλουθες μετρήσεις:

1. **Γενικευμένη Πιθανότητα Διακοπής Απορρήτου (GSOP):**

Αυτή η μέτρηση σχετίζεται με ασύρματα συστήματα με διακριτά επίπεδα μυστικότητας μετρημένα σε όρους της ικανότητας της Eve να αποκωδικοποιεί τις εμπιστευτικές πληροφορίες και δίνεται από GSOP = Pr {Δ < θ} , (6)

όπου 0 < θ < 1 αντιπροσωπεύει την ελάχιστη λογική τιμή της κλασματικής αμφισβήτησης. Εδώ, η ικανότητα αποκρυπτογράφησης του εμπιστευτικού μηνύματος της Eve ορίζεται επιλέγοντας διαφορετικές τιμές του θ. Για παράδειγμα, το συμβατικό SOP είναι μια ιδιαίτερη περίπτωση του GSOP για θ = 1.

2. **Ασυμπτωτικό κάτω όριο στην αποκωδικοποίηση της Eve με πιθανότητα σφάλματος:**

Αυτή η μέτρηση ορίζεται ως ο μέσος όρος της κλασματικής διχογνωμίας και δίνεται με $\bar{\Delta} = E[\Delta]$, (7) στην οποία το $E[\cdot]$ είναι η πράξη προσδοκίας. Αξίζει να αναφέρουμε ότι, όταν η εντροπία των δεδομένων για τη μετάδοση είναι αρκετά μεγάλη, το σφάλμα αποκωδικοποίησης της Eve για μια δεδομένη πραγματοποίηση εξασθένησης είναι μικρότερη που οριοθετείται από την κλασματική αμφιβολία, δηλαδή , $Pe \geq \bar{\Delta}2$.

3. **Μέσος ρυθμός διαρροής πληροφοριών:**

Αυτή η μέτρηση προσφέρει μια ιδέα για το πόσο γρήγορα διαρρέουν τα δεδομένα προς την Eve , όταν μια μετάδοση αμετάβλητου ρυθμού, R_S, υιοθετείται στο σύστημα. Μπορεί να εκφραστεί ως $R_L = E[(1 - \Delta) R_S] = (1-\Delta)Rs$ (8).

Στο [50,51], οι ερευνητές ερεύνησαν την απόδοση του PLS χρησιμοποιώντας διαφορετικές τοπολογίες μετάδοσης με βάση τις προαναφερθείσες μετρήσεις.

1.7 Πιθανότητα αναχαίτισης

Ένα συμβάν αναχαίτισης συμβαίνει όταν το C_S είναι αρνητικό ή πέφτει κάτω από το 0. Αυτό σημαίνει ότι το κανάλι υποκλοπής έχει καλύτερο SNR από το νόμιμο κανάλι. Η πιθανότητα αναχαίτισης μπορεί να διατυπωθεί όπως στο [52] από $P_{int} = P_r \{C_S (\gamma_B, \gamma_E) < 0\}$ (9). Αν και αυτή η μέτρηση δεν έχει διερευνηθεί ευρέως σύμφωνα με τη βιβλιογραφία, διερευνάται επί του παρόντος για την αξιολόγηση της απόδοσης μυστικότητας των ασύρματων καναλιών. Οι αναγνώστες παραπέμπονται στο [53–55] για περισσότερες πληροφορίες σε αυτό το πεδίο έρευνας.

1.8 Πιθανότητα αυστηρά θετικής ικανότητας μυστικότητας

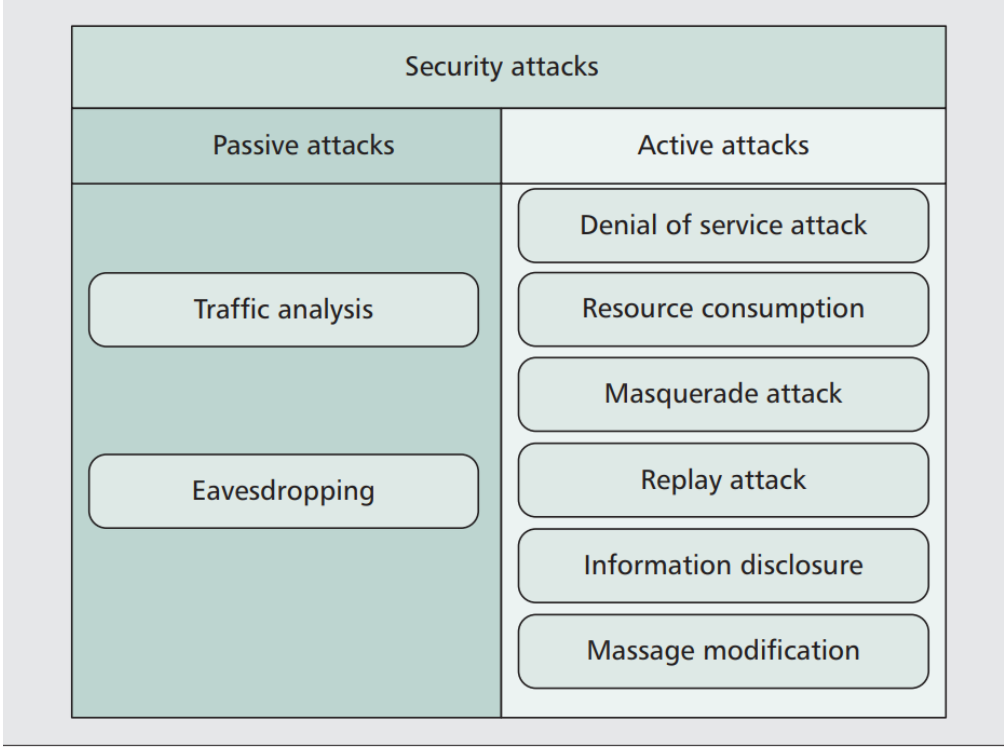
Η πιθανότητα του SPSC είναι η πιθανότητα ότι το C_S παραμένει υψηλότερο από 0. Αυτό σημαίνει ότι το απόρρητο στην επικοινωνία έχει επιτευχθεί. Μαθηματικά, μπορεί να γραφτεί όπως στο [56] από

$P_{SPSC} = Pr \{C_S (\gamma_B, \gamma_E) > 0\}$. (10)

Στο [57-59], οι ερευνητές ερεύνησαν την απόδοση ασφάλειας των ασύρματων συστημάτων με βάση τη μέτρηση SPSC σε διαφορετικά μοντέλα καναλιών που εξασθενούν.

2 Επιθέσεις ασφαλείας στα ασύρματα δίκτυα

2.1 Παθητικές και ενεργές



2.2 Παθητικές επιθέσεις

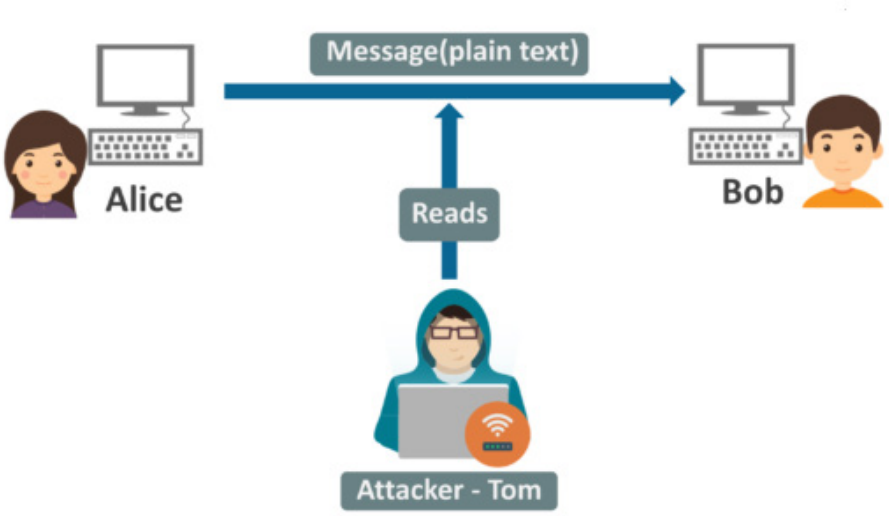
Παραβίαση: Είναι η μη εξουσιοδοτημένη παρακολούθηση ιδιωτικών επικοινωνιών σε πραγματικό χρόνο, όπως μια τηλεφωνική κλήση ή ένα άμεσο μήνυμα.

• Γενικά, η κρυπτογράφηση χρησιμοποιείται για να ξεπεραστεί αυτό το πρόβλημα.

Ανάλυση Κυκλοφορίας: Διαδικασία παρακολούθησης και ανάλυσης μηνυμάτων προκειμένου να εξαχθούν συμπεράσματα στην επικοινωνία.

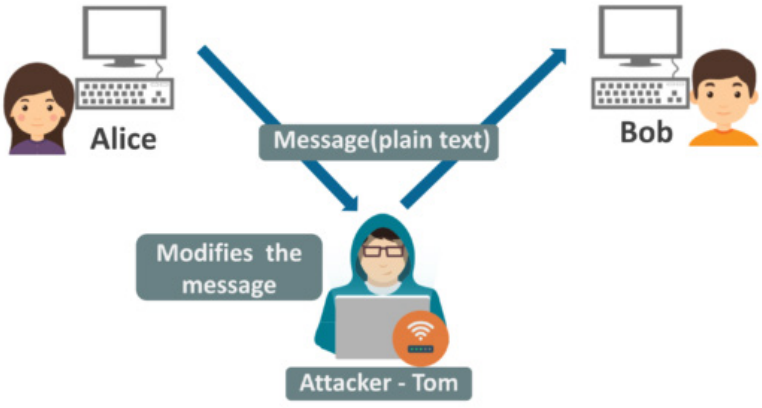
• Όσο μεγαλύτερος είναι ο αριθμός των μηνυμάτων που αποθηκεύονται, τόσο περισσότερο μπορεί να επηρεαστεί από την κίνηση.

• Η ανάλυση κυκλοφορίας μπορεί επίσης να γίνει με κρυπτογραφημένες πληροφορίες.



2.3 Ενεργές επιθέσεις

Οι ενεργές επιθέσεις χωρίζονται βασικά σε τρεις κατηγορίες : στις επιθέσεις (DoS Attacks, Resource Consumption) που επιχειρούν να εξαντλήσουν τους πόρους του δικτύου, όπως π.χ κάνουν οι παρεμβολές στο φυσικό επίπεδο (Jamming), στις επιθέσεις όπου ο κακόβουλος χρήστης υποκρίνεται ότι είναι νόμιμος προκειμένου να υποκλέψει πληροφορία ή πόρους του δικτύου (Masquerade Attack), και τέλος στις επιθέσεις όπου ένας συμβιβασμένος (compromised) κόμβος διοχετεύει πληροφορία του δικτύου σε μη εξουσιοδοτημένους κόμβους, είτε αλλοιώνει αυτή την πληροφορία (Information Disclosure, Message Modication).

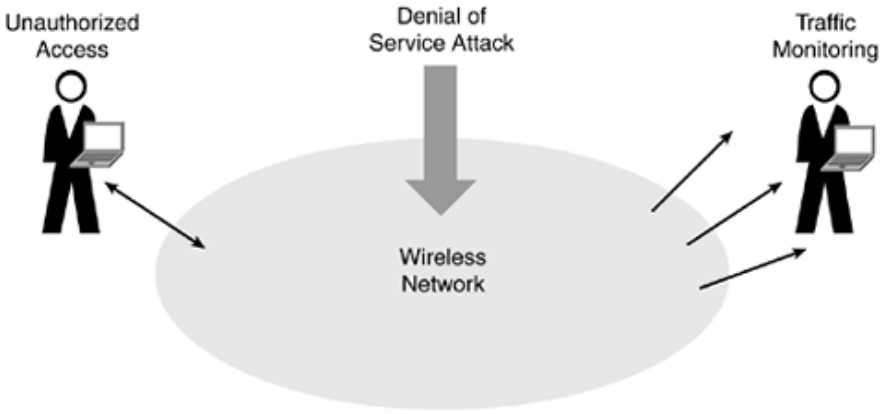


Μια ενεργή επίθεση είναι μια εκμετάλλευση δικτύου στην οποία ο εισβολέας προσπαθεί να πραγματοποιήσει αλλαγές στα δεδομένα του στόχου ή των δεδομένων καθ 'οδόν προς τον στόχο.

Denial of Service (Dos)

Ένας εισβολέας προσπαθεί να εξαντλήσει τον πόρο που διατίθεται στους νόμιμους χρήστες του. Στο φυσικό επίπεδο, η παρεμβολή ραδιοσυχνοτήτων χρησιμοποιείται για να καταλάβει τη μεταδιδόμενη ζώνη σήματος.

• Με αυτόν τον τρόπο η επικοινωνία διακόπτεται και ένας αντίπαλος κάνει τους επιθετικούς κόμβους να υποφέρουν από DoS.



Masquerade attacks

Σε μια επίθεση μεταμφιέσεως ένας εισβολέας εξαπατά τον μηχανισμό ελέγχου ταυτότητας και προσποιείται ότι είναι νόμιμος χρήστης, διακόπτοντας έτσι την επικοινωνία.

Αποκάλυψη πληροφοριών και τροποποίηση μηνυμάτων

Ένας συμβιβασμένος κόμβος λειτουργεί ως διαρροή πληροφοριών.

• Πληροφορίες όπως η περιοδικότητα της κυκλοφορίας μεταξύ δύο κόμβων μπορεί να είναι πολύτιμες για έναν εισβολέα.

Η τροποποίηση μηνύματος αναφέρεται σε προσθήκη ή διαγραφή περιεχομένου επικοινωνίας δικτύου από έναν αντίπαλο.

2.4 Απαιτήσεις ασφαλείας ασύρματων δικτύων

Επαλήθευση και Αδυναμία Αποκήρυξης

Η επαλήθευση αναφέρεται στην επιβεβαίωση ότι μια αίτηση για επικοινωνία προέρχεται από έναν νόμιμο παραλήπτη, είτε ότι τα δεδομένα δημιουργήθηκαν από έναν νόμιμο χρήστη του δικτύου. Η ιδιότητα της αδυναμίας αποκήρυξης αναφέρεται στην αδυναμία του πομπού και του δέκτη να αρνηθούν ότι έστειλαν ή δέχτηκαν δεδομένα αντίστοιχα. Επιτυγχάνεται κυρίως με την χρήση ψηφιακών υπογραφών.

Εχεμύθεια

Εχεμύθεια ονομάζεται η απαίτηση να προστατεύονται τα σταλθέντα δεδομένα είτε τα δεδομένα λειτουργίας του δικτύου από έναν παθητικό κακόβουλο δέκτη, τον ωτακουστή.

Ακεραιότητα

Η ακεραιότητα αναφέρεται στην δυνατότητα του δικτύου να εγγυάται στους χρήστες του ότι τα δεδομένα που αποστέλλονται δεν έχουν αλλοιωθεί από κάποια επίθεση,

Διαθεσιμότητα

Όταν ένα δίκτυο ικανοποιεί την απαίτηση της διαθεσιμότητας, εγγυάται στους χρήστες του ότι όποια επίθεση και αν δεχτεί από κακόβουλους εισβολείς, οι υπηρεσίες του δικτύου θα προσφέρονται κανονικά.

Αντίσταση στην εμπλοκή

Η εμπλοκή είναι μια απλή τεχνική παρέμβασης στα κανάλια επικοινωνίας.

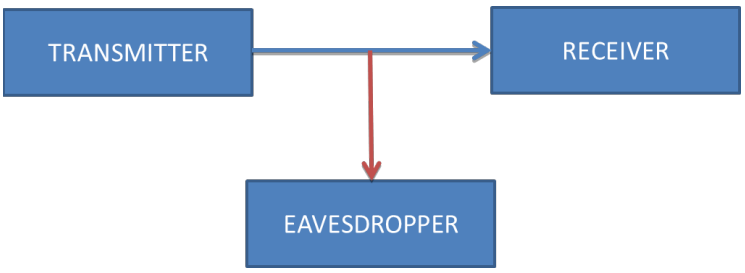
•Ένας παρεμβολέας μπορεί να στείλει σήματα παρεμβολής που διαταράσσουν τη λήψη σήματος.

•Οι ενεργοί παρεμβολείς στέλνουν συνεχώς ραδιοσήματα στο κανάλι και έτσι εμποδίζουν την επικοινωνία των χρηστών.

•Οι αντιδραστικοί παρεμβολείς παραμένουν αδρανείς μέχρι τη στιγμή που αισθάνονται μετάδοση στο κανάλι. Μόλις συμβεί αυτό, στέλνουν σήματα παρεμβολής.

Αντίσταση στην υποκλοπή

Η απόκρυψη πληροφοριών είναι μια μέθοδος για την ενσωμάτωση ιδιωτικών πληροφοριών σε διαδικασία σήματος ή θορύβου.



3 Προσεγγίσεις στην ασφάλεια φυσικού επιπέδου

Οι υπάρχουσες τεχνικές ασφαλείας φυσικού επιπέδου μπορούν να ταξινομηθούν σε τέσσερις μεγάλες κατηγορίες:

3.1 Προσέγγιση καναλιών

Αποτύπωμα ραδιοσυχνότητας : Αυτό το σύστημα αποτελείται από πολλαπλά συστήματα αισθητήρων που συλλαμβάνουν και εξάγουν χαρακτηριστικά της ραδιοσυχνότητας από κάθε ληφθέν σήμα.

Ένα σύστημα ανίχνευσης εισβολής επεξεργάζεται τα σύνολα των χαρακτηριστικών και δημιουργεί ένα δυναμικό δακτυλικό αποτύπωμα για κάθε εσωτερικό αναγνωριστικό πηγής που προέρχεται από λίγα πακέτα.

Αυτό το σύστημα RF παρακολουθεί τη χρονική εξέλιξη κάθε δακτυλικού αποτυπώματος και εκδίδει ειδοποίηση όταν εντοπίζεται ένα περίεργο δακτυλικό αποτύπωμα διακρίνοντας έναν εισβολέα.

Πολυπλεξία αποσύνθεσης αλγεβρικού καναλιού- προκωδικοποίηση : τα μεταδιδόμενα διανύσματα κώδικα δημιουργούνται από μοναδική αποσύνθεση τιμής singular value decomposition (SVD) της μήτρας συσχέτισης που περιγράφει τα χαρακτηριστικά καναλιού μεταξύ πομπού και δέκτη.

Τυχαιοποίηση συντελεστών μετάδοσης MIMO (multiinput multi-output):

• Ο πομπός δημιουργεί μια διαγώνια μήτρα που εξαρτάται από την παλμική απόκριση του καναλιού δέκτη πομπού

.• Η διαγώνια μήτρα έχει τη μοναδική ιδιότητα να μην ανιχνεύεται σε έναν εισβολέα.

• Μειώνει την παρακολούθηση σημάτων.

3.2 Προσέγγιση κώδικα

Κύριος στόχος είναι να βελτιωθεί η ανθεκτικότητα έναντι του παρεμβολής και υποκλοπές.

Κωδικοποίηση διόρθωσης σφάλματος

Ένα μόνο σφάλμα στο ληφθέν κρυπτογράφημα θα προκαλέσει μεγάλο αριθμό σφαλμάτων στο αποκρυπτογραφημένο απλό κείμενο.

Για να ξεπεραστεί αυτό το πρόβλημα χρησιμοποιείται ένα σχήμα με κρυπτογραφημένη τούρμπο κωδικοποίηση (coding and advanced encryption standard) (AES)

Ένα ασφαλές κανάλι επικοινωνίας έχει δημιουργηθεί με βάση την επιλογή N ψευδο τυχαίων bit από M κωδικοποιημένα bit.

Spread spectrum coding είναι μια τεχνική σηματοδότησης στην οποία είναι ένα σήμα εξαπλώνεται με ακολουθία θορύβου σε μια ευρεία ζώνη συχνοτήτων με συχνότητα μεγαλύτερο από αυτό του αρχικού σήματος.

Οι παραδοσιακές κρυπτογραφικές τεχνικές μπορούν να έχουν μεγάλο μέγεθος κλειδιού, ωστόσο, Το σύστημα φάσματος εξάπλωσης περιορίζεται σε εύρος συχνοτήτων φορέα.

Στο **CDMA (Code-division multiple access)** σύστημα όλοι οι χρήστες μοιράζονται το ίδιο κανάλι που χρησιμοποιεί διαφορετικούς κωδικούς εξάπλωσης για να διακρίνει τα σήματά του.

3.3 Προσέγγιση ισχύος

Η προστασία δεδομένων μπορεί επίσης να διευκολυνθεί χρησιμοποιώντας προσεγγίσεις ισχύος. Ο συνηθισμένα σχήματα σε αυτές τις προσεγγίσεις περιλαμβάνουν την απασχόληση κατευθυντικές κεραίες και την έγχυση κατευθυντικής κεραίας:

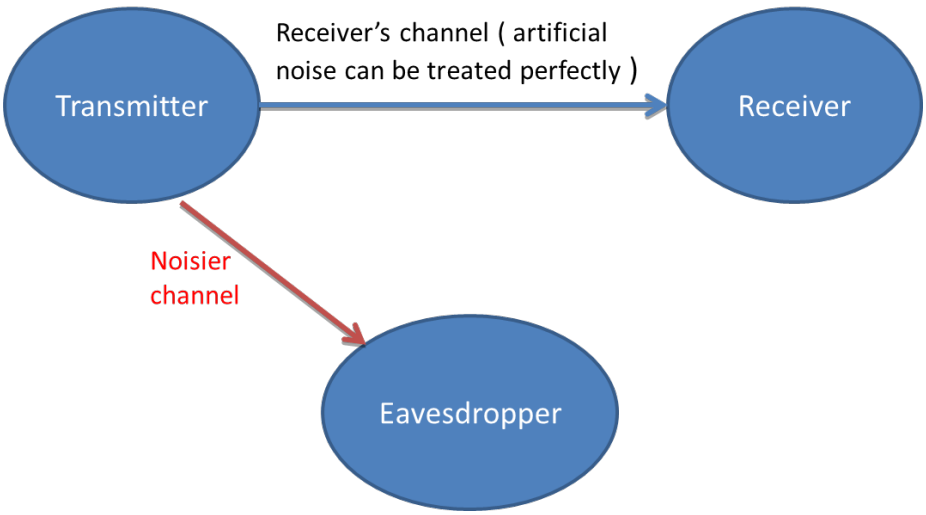
Οι κατευθυντικές κεραίες μπορούν να βελτιώσουν την χωρητικότητα του δικτύου και να αποφύγουν τις προσπάθειες παρεμβολής.

Όταν αναπτύσσονται στον νόμιμο πομπό, μπορούν να κατευθύνουν τις πληροφορίες στον νόμιμο δέκτη, καθιστώντας έτσι δύσκολη την παραβίαση σε διαφορετικές θέσεις λήψης. τεχνητού θορύβου

Σχέδιο τεχνητού θορύβου:

• Το τέλειο απόρρητο μπορεί να επιτευχθεί όταν το κανάλι εισβολέων είναι πιο θορυβώδες από το κανάλι δεκτών.

• Ο τεχνητός θόρυβος χρησιμοποιείται για να βλάψει το κανάλι του εισβολέα, αλλά δεν επηρεάζει το κανάλι του δέκτη, καθώς ο θόρυβος δημιουργείται στον κεντρικό χώρο του καναλιού του δέκτη.



3.4 Προσέγγιση σχεδιασμού σήματος

Εξετάστε ένα δίκτυο που αποτελείται από πολλούς πομπούς κεραίας και αρκετούς δέκτες απλής κεραίας (δέκτης και υποκλοπής).

• Ο πομπός έχει γνώση του καναλιού και καταγράφονται τα σχόλια του παραλήπτη.

• Χρησιμοποιείται το σχέδιο τεχνητού θορύβου και η ποιότητα της υπηρεσίας (Qos) μπορεί να επιτευχθεί χρησιμοποιώντας υψηλότερη διαμόρφωση ή υψηλότερους κωδικούς διόρθωσης σφαλμάτων.

SECURITY SCHEMES	RESISTED ATTACKS	ACHIEVED SECURITY REQUIREMENT
RF fingerprint	Eavesdropping, resource consumption, masquerade	Authentication confidentiality
Rand MIMO	Eavesdropping	Confidentiality
AES CDMA	Eavesdropping	Confidentiality
ACDM (algebraic channel decomposition multiplexing)	Eavesdropping	Confidentiality
FHSS (frequency hopping spread spectrum)	Jamming, eavesdropping, traffic analysis	Availability confidentiality
Pseudo-chaotic DS/SS (spread spectrum direct)	Jamming, eavesdropping, traffic analysis	Confidentiality
Artificial Noise	Eavesdropping	Confidentiality

Approach	Method	Number of secret keys	Time required at 10^6 decryptions/ms
RF fingerprint	24-bit DES	1.7×10^8 keys	8.4 milliseconds
IS-95 CDMA	42-bit LFSR	4.4 × 1012 keys	2.2 seconds
AES CDMA	128-bit AES	3.4×10^{38} keys	5.4×10^{18} years
Rand-MIMO	Random matrix	3.4×10^{38} 4 × 4 matrix	5.4×10^{18} years

Table 2. *Required decryption time comparison.*

3.5 Υπολογιστική πολυπλοκότητα

Όσο μεγαλύτερος είναι ο αριθμός των πλήκτρων, τόσο υψηλότερο είναι το επίπεδο ασφάλειας.

Η υπολογιστική πολυπλοκότητα γίνεται ζήτημα όταν οι δέκτες πρέπει αποκρυπτογράφηση όλων των μηνυμάτων, έτσι χρησιμοποιείται έλεγχος ταυτότητας δεδομένων διάκριση μεταξύ εισβολέων και πομπών.

4 Συνεργατική αναμετάδοση

Fundamentals of Physical Layer Security
Performance Metrics
➢ Secrecy Rate ➢ Equivocation Rate ➢ Secrecy capacity ➢ Secrecy outage probability ➢ Intercept probability ➢ Probability of strictly positive secrecy capacity
General System Model
➢ Cooperative relaying ➢ Cooperative jamming

- Μέτρο μυστικότητας: η τιμή της μεταφερόμενης πληροφορίας για το μυστικό μήνυμα.
- Μέτρηση Αμφιβολίας: είναι η μέτρηση για την αμφιβολία του ωτακουστή για το εμπιστευτικό μήνυμα.
- Χωρητικότητα μυστικότητας: το μέγιστο εύρος μυστικότητας που μπορεί να επιτευχτεί.
- Η πιθανότητα να επιτύχουμε μη αρνητικό στόχο μυστικότητας.
- Η πιθανότητα η χωρητικότητα μυστικότητας να πέσει κάτω από το μηδέν.
- Η πιθανότητα η χωρητικότητα μυστικότητας να παραμείνει πάνω από το μηδέν.

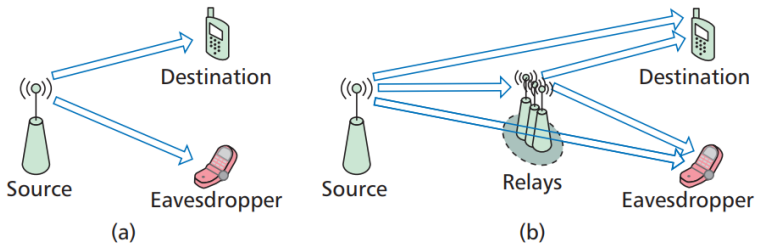


Figure 1. a) Wyner's wire-tap channel; b) wire-tap channel with cooperative relaying for enhanced security.

4.1 Συνεργατική αναμετάδοση

Είναι μια αποτελεσματική μέθοδος αύξησης του εύρους και της αξιοπιστίας των ασύρματων δικτύων.

Η αναμετάδοση γίνεται σε δύο φάσεις:

1. Το μήνυμα μεταδίδεται από την πηγή στον αναμεταδότη και τον προορισμό.
2. Ο αναμεταδότης μεταδίδει το μήνυμα στον προορισμό χρησιμοποιώντας συγκεκριμένο πρωτόκολλο.

Πρωτόκολλα:

- **Amplify-and-forward (AF):** Ο αναμεταδότης εκπέμπει μια διαβαθμισμένη έκδοση του ληφθέντος μηνύματος.
- **Compress-and-forward (CF)** : Ο αναμεταδότης συμπιέζει το μήνυμα πριν το μεταδώσει.
- **Compute-and-forward (CTF)** : Ο αναμεταδότης αποκωδικοποιεί τον γραμμικό συνδυασμό των μεταδιδόμενων μηνυμάτων, που λαμβάνονται από μία θορυβώδη παρατήρηση του καναλιού, το οποίο στη συνέχεια μεταφέρεται στον προορισμό. Ο προορισμός επιλύει τα επιθυμητά μηνύματα, αφού λάβει επαρκή αριθμό γραμμικών συνδυασμών.
- **Decode-and-forward (DF)** : Ο αναμεταδότης αποκωδικοποιεί το ληφθέν μήνυμα και στη συνέχεια το κωδικοποιεί ξανά για να το μεταδώσει στον προορισμό.

Το AF γενικά είναι πιο εύκολο να εφαρμοστεί, με κύριο μειονέκτημα την ενίσχυση του θορύβου. Από την άλλη πλευρά το DF παρέχει καλύτερη απόδοση όταν ο αναμεταδότης βρίσκεται κοντά στη πηγή ή σε περίπτωση καλών συνθηκών καναλιού.

Με βάση την ικανότητα μετάδοσης και λήψης, υπάρχουν δύο τύποι μετάδοσης:

1. **half-duplex (HD) αναμεταδότες:** χρειάζεται δύο ορθογώνιες χρήσεις καναλιών για μετάδοση και λήψη πληροφοριών.

2. **full-duplex (FD) relays** : μπορεί ταυτόχρονα να μεταδίδει και να λαμβάνει πληροφορίες, επιτρέποντας την αποτελεσματικότερη χρήση του φάσματος.

Παρά την χαμηλή απόδοση φάσματος, ο half duplex προτιμάται στα συστήματα εξαιτίας της χαμηλής πολυπλοκότητας και της ευκολίας στην εφαρμογή του.

4.2 Αναξιόπιστοι αναμεταδότες

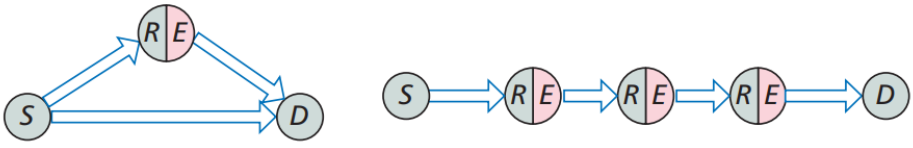


Figure 2. Wireless relay networks with untrusted relays where a relay R acts as both a helper and an eavesdropper E: a) three-node model; b) multihop model.

Η πηγή S και ο προορισμός D ζητούν βοήθεια από έναν ή περισσότερους κόμβους R για τη μετάδοση των πληροφοριών, αλλά ταυτόχρονα το ζεύγος προέλευσης – προορισμός επιθυμεί να διατηρήσει τις πληροφορίες μυστικές από αυτούς τους κόμβους. Παραδείγματα τέτοιου είδους συναντάμε σε κυβερνητικούς ή οικονομικούς οργανισμούς, όπου κάθε κόμβος δεν έχει το ίδιο επίπεδο ασφάλειας.

Μπορούμε να βελτιώσουμε την ασφάλεια εκμεταλλευόμενοι την αναμετάδοση με αναξιόπιστους κόμβους;

- Όταν υπάρχει ένας ορθογώνιος σύνδεσμος στο δεύτερο βήμα από τον αναμεταδότη προς τον προορισμό, κάποιος επιτυγχάνει υψηλότερο ρυθμό μυστικότητας αντιμετωπίζοντας τον αναμεταδότη E όχι μόνο σαν υποκλοπέα αλλά και ως βοηθό. Αυτό το ενδιαφέρον αποτέλεσμα ισχύει για την αναμετάδοση AF και CF, καθώς και για την DF σε χαμηλό επίπεδο.

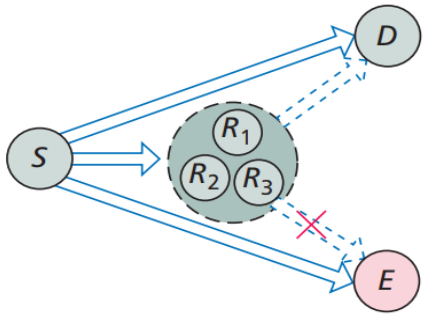
- Μεταφορά εμπιστευτικών μηνυμάτων μέσω πολλαπλής επικοινωνίας με μια αλυσίδα συνδεδεμένων μη αξιόπιστων αναμεταδοτών εξετάστηκε στο δεύτερο σχήμα. Είναι ενδιαφέρον σύμφωνα με αυτό το μοντέλο δικτύου γραμμών, ότι το απόρρητο από άκρο σε άκρο μπορεί να επιτευχθεί και ότι το ποσοστό μυστικότητας έχει αποδειχθεί ανεξάρτητο από τον αριθμό των βημάτων.

4.3 Αξιόπιστοι αναμεταδότες

Σε σενάρια αξιόπιστης αναμετάδοσης, η πηγή υποβοηθείται από έναν ή περισσότερους αξιόπιστους κόμβους για τη μετάδοση εμπιστευτικών πληροφοριών στον προορισμό, παρουσία ενός παθητικού υποκλοπέα. Σε αντίθεση με τη περίπτωση των αναξιόπιστων αναμεταδοτών, οι αξιόπιστοι κόμβοι μπορούν να αξιοποιηθούν πλήρως για να βελτιωθεί σημαντικά η ασφάλεια.

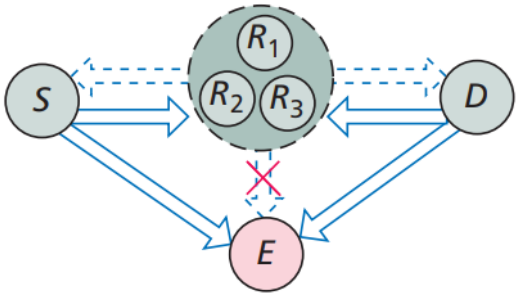
Αυτό το σενάριο έχει λάβει μεγάλη προσοχή στη βιβλιογραφία.

Ανάλογα με το αν η πληροφορία ρέει προς μία πλευρά (OW) ή και στις δύο (TW) έχουμε:



OW relaying

Στην OW, ένας κόμβος θέλει να επικοινωνήσει με ένα κόμβο προορισμού με τη βοήθεια ενός αναμεταδότη, έτσι οι πληροφορίες ρέουν με μονόδρομο τρόπο (δηλαδή από την πηγή προς τον προορισμό). Αυτό συνήθως συμβαίνει σε δύο φάσης μετάδοσης. Η πηγή επικοινωνεί με τους αναμεταδότες στην πρώτη φάση και εκείνοι με τον προορισμό στη δεύτερη.



TW relaying

Στην TW δύο κόμβοι θέλουν να ανταλλάσουν ροές δεδομένων και πληροφοριών με αμφίδρομο τρόπο. Αυτό συμβαίνει σε δύο ή τρεις φάσεις. Οι κόμβοι επικοινωνούν με τους αναμεταδότες ταυτόχρονα ή με τη σειρά σε μία ή δύο φάσεις και ο αναμεταδότης μεταδίδει στην τρίτη φάση. Ο υποκλοπέας μπορεί να ακούσει τις πληροφορίες σε μία ή περισσότερες φάσεις.

Ένας αναμεταδότης: οι τεχνικές DF ή AF συνήθως λαμβάνονται υπόψη στη βιβλιογραφία μαζί με τα πρωτόκολλα αναμετάδοσης OW ή TW.

Πολλοί αναμεταδότες: η πιο κοινή προσέγγιση αναμετάδοσης γίνεται με την ακτινοβολία. Σε αυτή την προσέγγιση, πολλοί αναμεταδότες μεταδίδουν μια σταθμισμένη έκδοση του οπτικοποιημένου σήματος (για DF) ή του θορυβώδους ληφθέντος μηνύματος (για AF).

Μπορεί να επιτευχθεί πλήρης μηδενισμός του σήματος στο υποκλοπέα. Ένα τέτοιο σχήμα διαμόρφωσης δέσμης / μηδενισμού ισχύει τόσο για την αναμετάδοση OW όσο και για την αναμετάδοση TW.

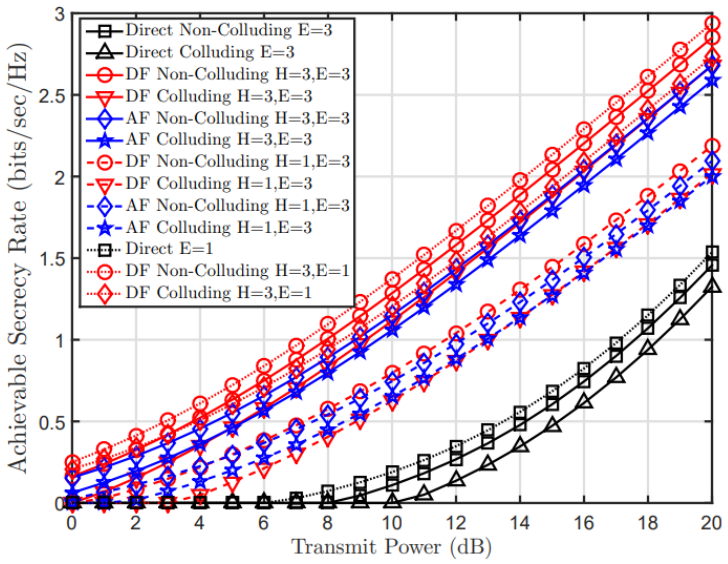


Fig. 4: Achievable secrecy rate for different secure cooperative relaying scenarios.

Από το σχήμα μπορεί να παρατηρηθεί ότι ο επιτεύξιμος ρυθμός μυστικότητας γενικά αυξάνεται με αύξηση της ισχύος μετάδοσης. Αυτή η αύξηση του ποσοστού απορρήτου είναι χαμηλότερη για άμεση μετάδοση και υψηλότερη για DF. Πιο συγκεκριμένα για την περίπτωση άμεσης μετάδοσης, ο ρυθμός μυστικότητας αυξάνεται καθώς ο αριθμός των υποκλοπέων μειώνεται από 3 σε 1. Για την περίπτωση πολλαπλών υποκλοπών, το ποσοστό απορρήτου για τους μη συνεργαζόμενους υποκλοπείς είναι μεγαλύτερο από τους συνεργαζόμενους. Παρόμοιες τάσεις για DF και AF. Για το DF το μεγαλύτερο ποσοστό απορρήτου επιτυγχάνεται υπό συνθήκες μη συμπαιγνίας. Γενικά το ποσοστό μυστικότητας είναι υψηλότερο όταν οι βοηθοί είναι περισσότεροι από τους υποκλοπείς. Ωστόσο σε χαμηλότερες τιμές ισχύος, το AF ξεπερνά το DF.

4.4 Συνεργατική παρεμβολή για ασφάλεια

Ο βοηθητικός κόμβος μπορεί να θυσιάσει ολόκληρο το εύρος προκειμένου να δημιουργήσει παρεμβολές στον υποκλοπέα και να υποβαθμίσει την απόδοσή του.

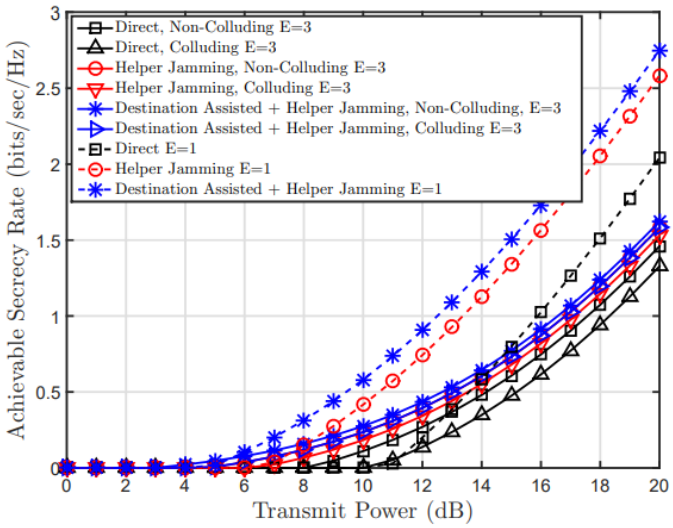
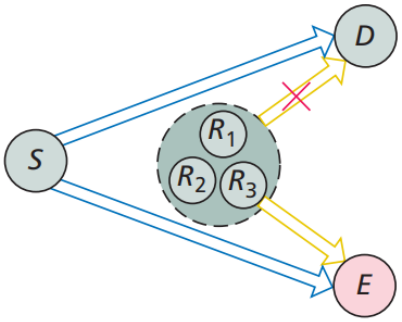


Fig. 5: Achievable secrecy rate for different secure cooperative jamming scenarios.

Στο σχήμα φαίνεται πως το μεγαλύτερο ποσοστό μυστικότητας υπάρχει με την άμεση μετάδοση. Γενικά αυξάνεται η απόδοση της μυστικότητας με το παρεμβολή και όταν ο αριθμός των υποκλοπέων μειώνεται.

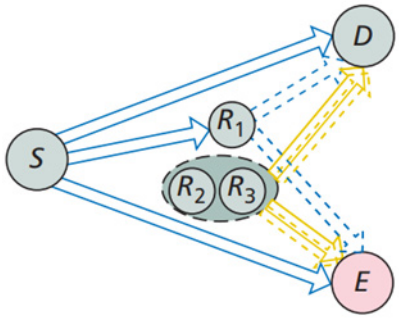
4.4.1 Παρεμβολείς



Jamming

Ο κύριος στόχος είναι να ενισχυθεί η χωρητικότητα των έμπιστων-νόμιμων συνδέσεων μειώνοντας ταυτόχρονα την ικανότητα των συνδέσμων υποκλοπής.

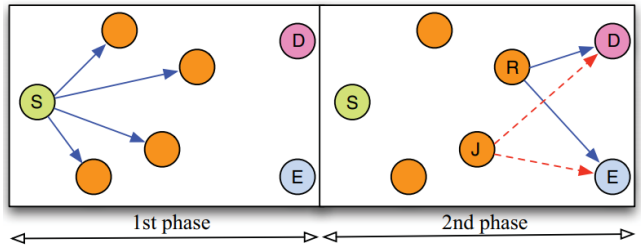
4.4.2 Αναμετάδοση-Παρεμβολή



Relaying/jamming

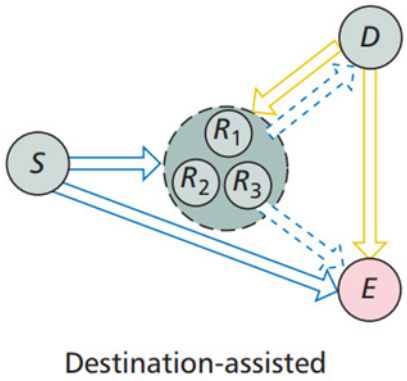
Τεχνικές παρεμβολής που δημιουργούν τεχνητή παρεμβολή στον κόμβο του υποκλοπέα προκειμένου να μειωθεί η χωρητικότητα του σχετικού συνδέσμου.

Σενάριο αναμετάδοσης- παρεμβολής.



- Οι αναμεταδότες δεν μπορούν να μεταδίδουν και να λαμβάνουν ταυτόχρονα και επομένως η επικοινωνία πραγματοποιείται σε δύο ορθογώνια κανάλια.
- Κατά τη διάρκεια της φάσης μετάδοσης, η πηγή μεταδίδει τα δεδομένα της και οι αναμεταδότες μπορούν να αποκωδικοποιήσουν με επιτυχία το σήμα πηγής από ένα σύνολο αποκωδικοποίησης $C_d \subseteq S$.
- Ο πρώτος αναμεταδότης R που λειτουργεί μια συμβατική λειτουργία αναμετάδοσης, ανήκει στο υποσύνολο C_d και προωθεί το μήνυμα προέλευσης προκειμένου να βοηθήσει την πηγή να παραδώσει το μήνυμά της στον προορισμό.
- Από την άλλη πλευρά, ο δεύτερος αναμεταδότης J μπαίνει σε λειτουργία παρεμβολής, οπότε δεν χρειάζεται να αποκωδικοποιήσει το σήμα προέλευσης και χρησιμοποιείται για τη δημιουργία σκόπιμης παρεμβολής στη μετάδοση του αναμεταδότη.
- Υποθέτουμε ότι οι άμεσοι σύνδεσμοι ($S \rightarrow S$, $S \rightarrow E$) δεν είναι διαθέσιμοι και ως εκ τούτου η ασφάλεια αφορά μόνο το συνεργατικό κανάλι.

4.4.3 Υβριδική Αναμετάδοση-Παρεμβολή



Destination-assisted

Η πηγή και ο προορισμός στέλνουν σήματα παρεμβολής στην πρώτη φάση στους αναμεταδότες. Στη δεύτερη φάση, οι αναμεταδότες μεταδίδουν μια σταθμισμένη έκδοση του σήματος που λαμβάνεται στην προηγούμενη φάση. Ταυτόχρονα, η πηγή στέλνει μια υπέρθεση σημάτων εμπλοκής και πληροφοριών. Το σήμα παρεμβολής σε αυτήν την υπέρθεση έχει σχεδιαστεί για να ακυρώνει το στοιχείο παρεμβολής λόγω της πηγής στον προορισμό, ενώ το στοιχείο παρεμβολής που οφείλεται στον προορισμό μπορεί εύκολα να ακυρωθεί αφού είναι γνωστό. Αυτή η ιδέα τεχνητού θορύβου έχει επεκταθεί και οι αναμεταδότες TW.

5 Κατανομή ισχύος και πιθανότητα διακοπής απορρήτου

5.1 SIGNAL FADING

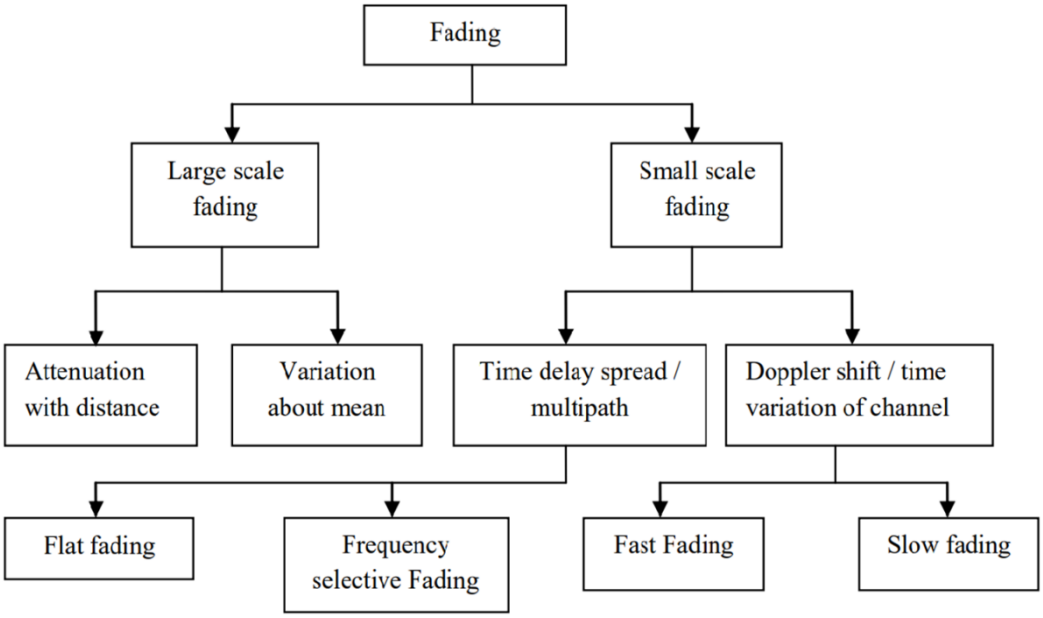
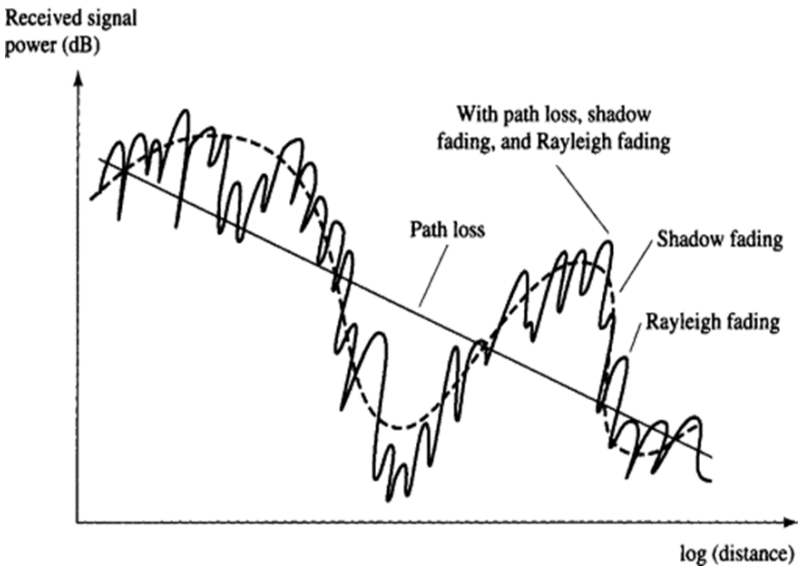


Fig. 1 Fading Manifestations

Η εξασθένιση μεγάλης κλίμακας, αναφέρεται στην αλλαγή που προκαλείται από τις επιδράσεις του σήματος ταξιδεύοντας σε μεγάλες περιοχές. Αυτό το φαινόμενο επηρεάζεται από εμφανή περιγράμματα εδάφους (λόφους, δάση, πινακίδες, συστάδες κτιρίων κ.λπ.) μεταξύ του πομπού και του δέκτη. Η εξασθένιση μικρής κλίμακας αναφέρεται στις δραματικές αλλαγές στο πλάτος και τη φάση του σήματος.



Εμφανίζεται ο συνδυασμός απώλειας διαδρομής, σκίασης και επίπεδου εξασθένισης. Η πτώση ισχύος σε σχέση με απόσταση λόγω απώλειας διαδρομής είναι αρκετά αργή, ενώ η διακύμανση του σήματος λόγω σκίασης αλλάζει πιο γρήγορα και η διακύμανση λόγω επίπεδης εξασθένισης είναι πολύ γρήγορη

5.2 Μοντέλο Συστήματος

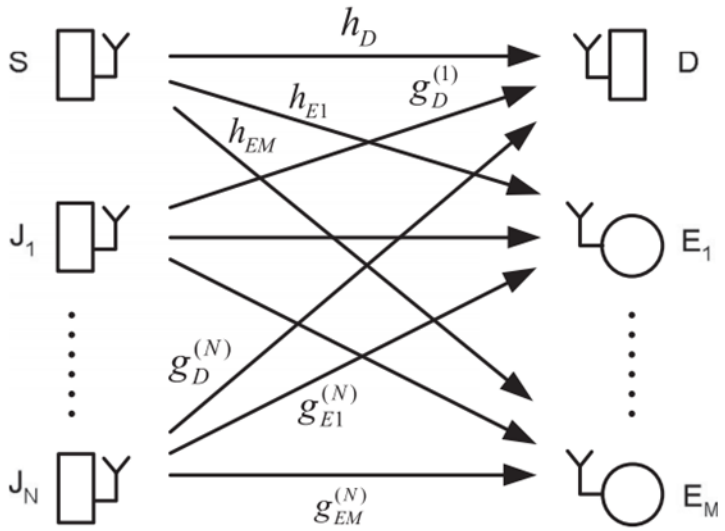


Fig. 1. Considered secrecy network with one source, one destination, and multiple jammers in the presence of multiple eavesdroppers.

Θεωρούμε ένα δίκτυο μυστικότητας, όπως φαίνεται στο Σχ. 1, με μία πηγή **S**, η οποία επικοινωνεί με έναν προορισμό **D** και N παρεμβολείς $J_1,J_2,\ldots, J_N$ παρουσία M υποκλοπέων $E_1,E_2,\ldots E_M$. Η πηγή S επιθυμεί να μεταδώσει ασφαλείς πληροφορίες στον προορισμό D. Υποθέτουμε ότι όλοι οι κόμβοι δικτύου είναι εξοπλισμένοι με μία μόνο κεραία. Συμβολίζουμε με:

- $\mathbf{h_D}$ ο συντελεστής καναλιού μεταξύ της πηγής S και του προορισμού D .
- $\mathbf{h_{Em}}$ ο συντελεστής καναλιού μεταξύ του S και του mth υποκλοπέα Em , με m = 1, 2,...,M.
- $\mathbf{g_D^{(n)}}$ ο συντελεστής καναλιού μεταξύ του nth παρεμβολέα J_n and D .
- $\mathbf{g_{Em}^{(n)}}$ ο συντελεστής καναλιού μεταξύ του nth παρεμβολέα J_n και του υποκλοπέα E_m .

Τα λαμβανόμενα σήματα στα D και E_m μπορούν και μαθηματικά να εκφραστούν :

$$y_D = \sqrt{P_s} h_D x_s + \sum_{i=1}^{N} \sqrt{P_i} g_D^{(i)} x_c^{(i)} + \eta_D \qquad (1)$$

$$y_{Em} = \sqrt{P_s} h_{Em} x_s + \sum_{i=1}^{N} \sqrt{P_i} g_{Em}^{(i)} x_c^{(i)} + \eta_{Em} \qquad (2)$$

όπου x_s είναι το μεταδιδόμενο σήμα από το S στο D, και x_c το σήμα παρεμβολής. Επίσης, η_D και η_{Em} είναι ο θόρυβος στην πηγή και στον υποκλοπέα Em αντίστοιχα. Η κατανομή ισχύος στο J_i και S συμβολίζονται με P_i και P_s, αντίστοιχα.

Με την υπόθεση του Gaussian θορύβου, ο εφικτός ρυθμός μυστικότητας στο D ορίζεται ως:

$$\gamma_D = \frac{P_s |h_D|^2}{\sum_{i=1}^{N} P_i |g_D^{(i)}|^2 + \sigma_D^2} \qquad (4)$$

$$\gamma_{Em} = \frac{P_s |h_{Em}|^2}{\sum_{i=1}^{N} P_i |g_{Em}^{(i)}|^2 + \sigma_{Em}^2}. \qquad (5)$$

Σκοπεύουμε να μεγιστοποιήσουμε το επιτεύξιμο ποσοστό απορρήτου στον κόμβο προορισμού D, με τη διαθέσιμη ισχύ εκπομπής στον κόμβος προέλευσης και όλους τους διαθέσιμους N παρεμβολείς.

Το πρόβλημα μεγιστοποίησης του ποσοστού απορρήτου μπορεί επομένως να διατυπωθεί ως :

$$\text{P1}: \quad \max_{\mathbf{p} \succeq \mathbf{0}} \quad R_s$$

$$\text{s.t.} \quad P_i \leq \bar{P}_i \quad \forall i \qquad (6)$$

όπου Ṗi είναι η μέγιστη διαθέσιμη ισχύς μετάδοσης σε J_i και $p = [P_1 P_2 \cdots P_N]^T$.

5.3 Απαραίτητες συνθήκες για θετικό ρυθμό μυστικότητας

Το πρόβλημα βελτιστοποίησης **P1**, που διατυπώνεται στο (6), είναι έγκυρο ή αξίζει να επιλυθεί μόνο όταν είναι δυνατόν να επιτευχθεί ένας θετικός ρυθμός μυστικότητας για ένα δεδομένο σύνολο καναλιών και μετάδοσης ισχύος σε D και J_is. Μέσω της επαλήθευσης αυτών των συνθηκών σκοπιμότητας, η πηγή μπορεί να αποφασίσει εάν θα μπορέσει να επιτύχει μεγιστοποίηση του ποσοστού απορρήτου, και να αποκτήσει ο προορισμός θετικό ποσοστό απορρήτου.

Από το (3), πρέπει να πληρούνται οι ακόλουθες προϋποθέσεις για m = 1, 2, ..., M:

$$\frac{P_s|h_D|^2}{\sum_{i=1}^{N} P_i|g_D^{(i)}|^2+\sigma_D^2} > \frac{P_s|h_{Em}|^2}{\sum_{i=1}^{N} P_i|g_{Em}^{(i)}|^2+\sigma_{Em}^2}. \quad (7)$$

5.4 Διαδικαστική προσέγγιση για τη λύση του προβλήματος μεγιστοποίησης του ρυθμού

Αναπτύσσουμε έναν επαναληπτικό αλγόριθμο για την κατανομή ισχύος p στους παρεμβολείς, ο οποίος βασίζεται σε προσέγγιση του αρχικού προβλήματος P1. Αναδιατυπώνοντας (6) και εισάγοντας μια νέα χαλαρή μεταβλητή τ, το αρχικό πρόβλημα μεγιστοποίησης απορρήτου P1 μπορεί να γραφτεί ως:

$$\begin{aligned} \text{P2}: \quad & \min_{\mathbf{p}\succeq\mathbf{0},\tau\geq 0} \quad \tau \\ & \text{s.t.} \quad \Gamma_{Em}(\mathbf{p}) \triangleq \frac{\Phi_{Em}(\mathbf{p})}{\Psi_{Em}(\mathbf{p})} \leq \tau, \forall m \\ & \qquad P_i \leq \bar{P}_i, \forall i \end{aligned} \quad (11)$$

where

$$\begin{aligned} \Psi_{Em}(\mathbf{p}) \triangleq & \left(\sum_{i=1}^{N} P_i|g_D^{(i)}|^2 + P_s|h_D|^2 + \sigma_D^2\right) \\ & \times \left(\sum_{i=1}^{N} P_i|g_{Em}^{(i)}|^2 + \sigma_{Em}^2\right) \triangleq \sum_{k} \psi_{Em}^{(k)} \end{aligned} \quad (12)$$

and

$$\begin{aligned} \Phi_{Em}(\mathbf{p}) \triangleq & \left(\sum_{i=1}^{N} P_i|g_{Em}^{(i)}|^2 + \sigma_{Em}^2 + P_s|h_{Em}|^2\right) \\ & \times \left(\sum_{i=1}^{N} P_i|g_D^{(i)}|^2 + \sigma_D^2\right). \end{aligned} \quad (13)$$

5.5 Algorithm A

Algorithm A: Secrecy Rate Maximization.

Step 1: Initialization of power allocation vector $\mathbf{p}$

Step 2: Repeat

1) Calculate $\Psi_{Em}(\mathbf{p})$, $\forall m$ using (12).
2) Calculate $\alpha_k^{(m)}$, $\forall k,\ m$ using (16).
3) Determine $\hat{\Psi}_{Em}(\mathbf{p})$, $\forall m$ by using (15).
4) Solve the standard geometric programming problem in (17).

Step 3: Until required accuracy is achieved or the maximum number of iterations is reached.

5.6 Ανάλυση της πιθανότητας διακοπής απορρήτου (SOP)

Αναλύουμε την πιθανότητα διακοπής απορρήτου του προτεινόμενου συστήματος συνεργατικής παρεμβολής μέσω καναλιών εξασθένισης Rayleigh.

$$P_{\text{out}} = \Pr\left[\log_2 \frac{\gamma_D + 1}{\gamma_{E_{\max}} + 1} < \mathcal{R}\right] \qquad (22)$$

Το R υποδηλώνει το ρυθμό σε bits ανά δευτερόλεπτο (bps) ανά Hertz.

5.7 Προσομοίωση και συμπεράσματα

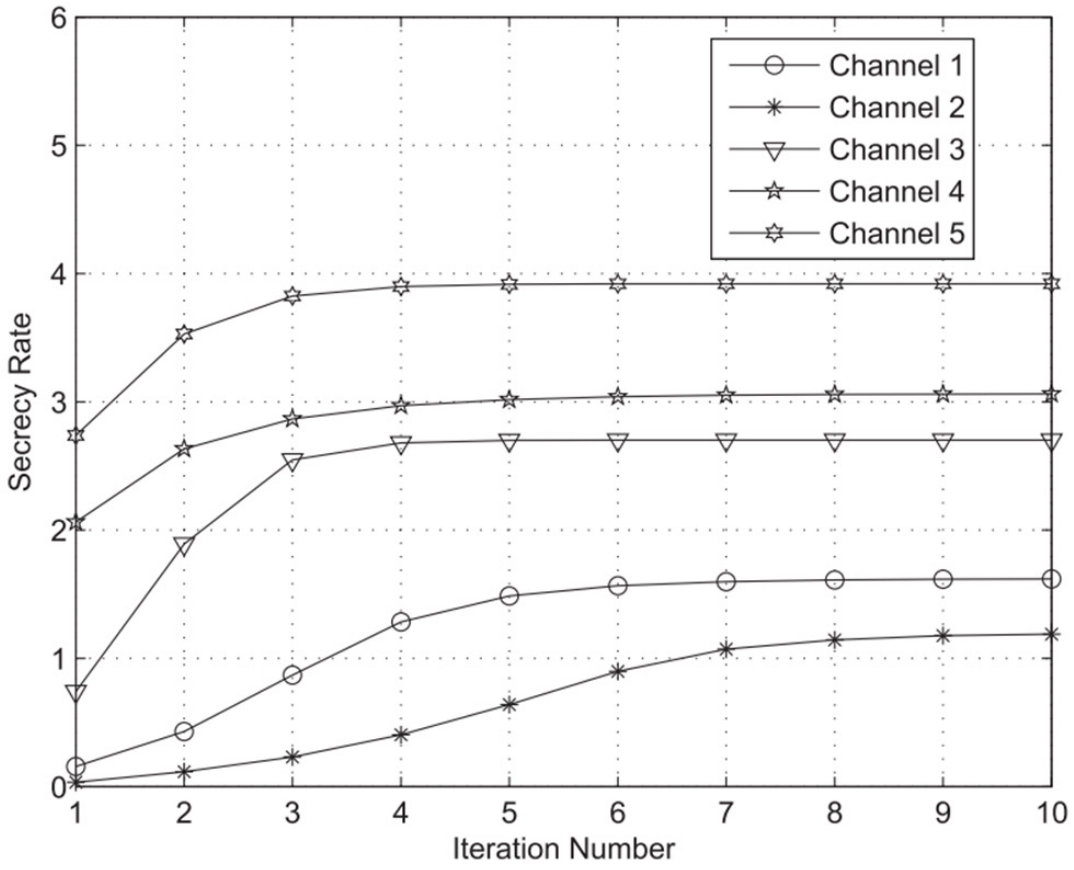


Fig. 2. Convergence of the proposed secrecy rate maximization Algorithm A for different sets of wireless channels.

Αυτό αποκαλύπτει ότι το επιτευχθέν ποσοστό απορρήτου θα αυξάνεται μονοτονικά σε κάθε επανάληψη, κάτι που μπορεί επίσης να παρατηρηθεί από τα αποτελέσματα προσομοίωσης, που παρουσιάζονται στο Σχ. 2.

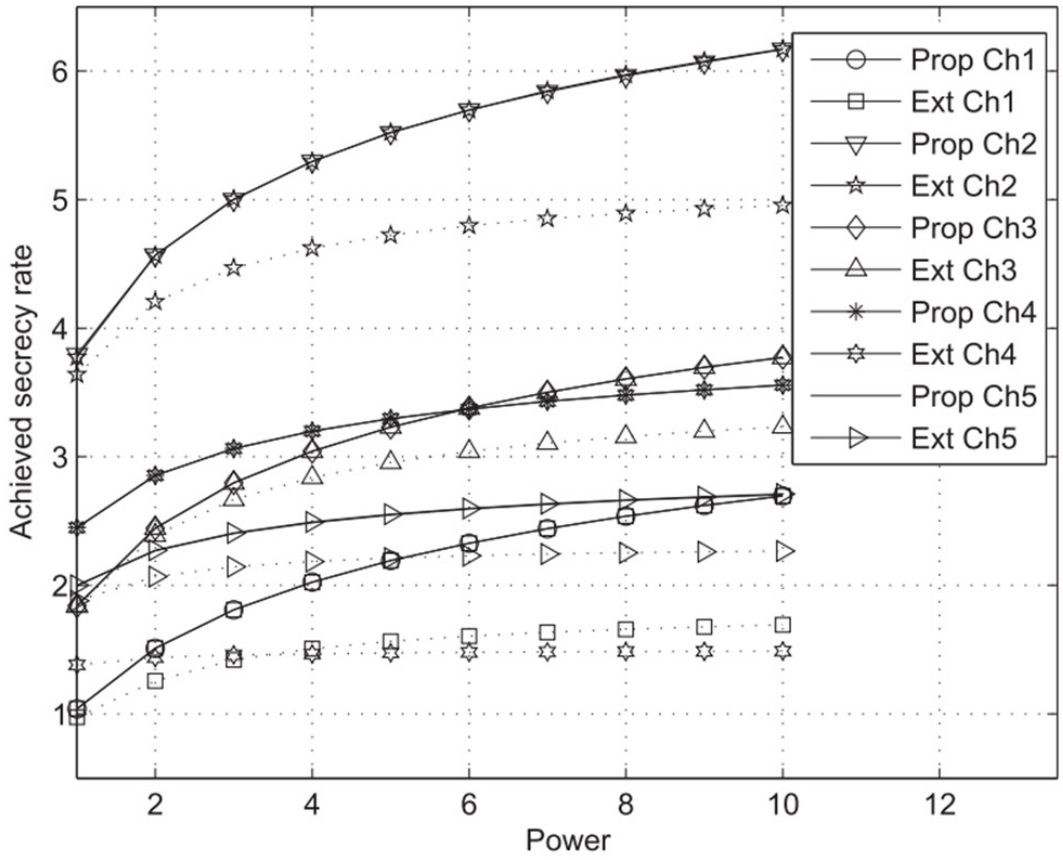


Fig. 3. Achieved secrecy rates of Algorithm A, the scheme in [19], and the best jammer selection scheme for five sets of different wireless channels with different maximum available transmit power. The dotted lines denote the best jammer selection scheme.

Απεικονίζει τα επιτευχθέντα ποσοστά μυστικότητας για διαφορετική διαθέσιμη ισχύ εκπομπής στην πηγή και στους συνεργατικούς παρεμβολείς για διαφορετικά κανάλια, όπου θεωρείται ότι η μέγιστη διαθέσιμη ισχύς μετάδοσης στην πηγή και στους συνεργατικούς παρεμβολείς είναι η ίδια.

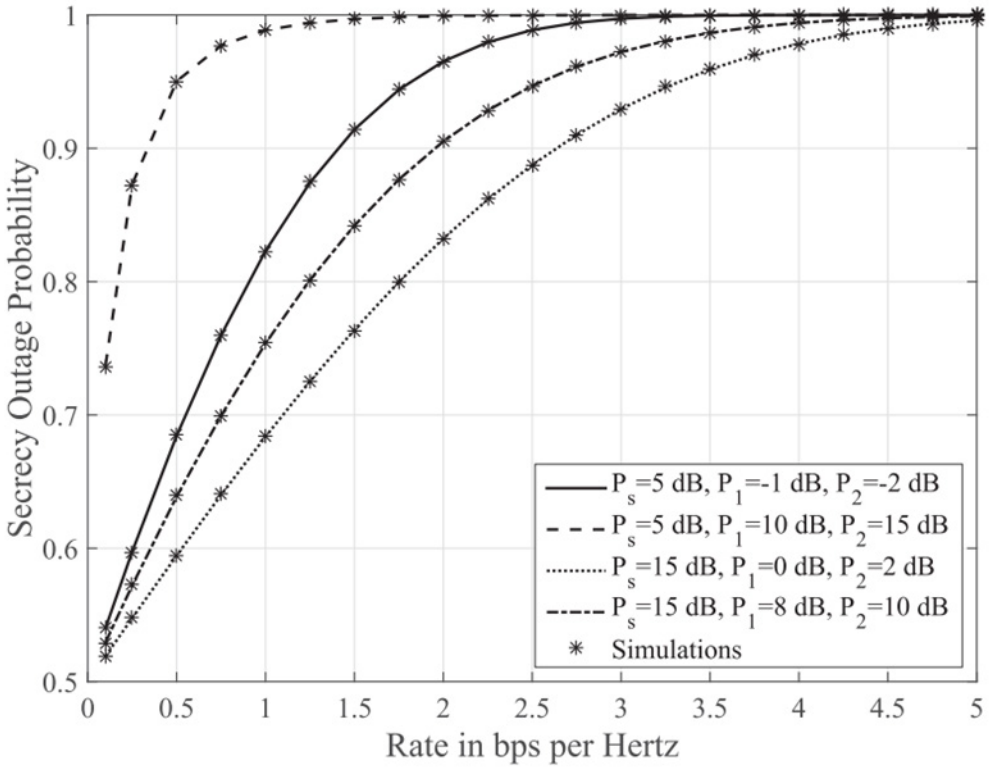


Fig. 4. P_{out}, as a function of the rate $\mathcal{R}$, in bps per Hz, for $N = 2$ cooperative jammers, $M = 1$ eavesdroppers, and various power levels.

Το Σχήμα 4 απεικονίζει την απόδοση πιθανότητας διακοπής απορρήτου (secrecy outage probability SOP) ως συνάρτηση του ρυθμού R σε bps ανά Hertz για N = 2 φιλικούς παρεμβολείς, M = 1 υποκλοπείς και διάφορα επίπεδα ισχύος. Σε αυτό το σχήμα φαίνεται ότι προκύπτει η προσομοίωση στον υπολογιστή για SOP ταιριάζει απόλυτα με τα αντίστοιχα αριθμητικά για όλες τις εξεταζόμενες παραμέτρους. Όπως αναμενόταν, το SOP υποβαθμίζεται με αυξανόμενες τιμές για R. Επιπλέον, όσο η ισχύς μετάδοσης της πηγής S αυξάνεται και οι δυνάμεις μετάδοσης στους δύο παρεμβολείς J1 και J2 μειώνονται, το SOP βελτιώνεται. Η καλύτερη απόδοση SOP σε αυτό το σχήμα για όλες τις θεωρούμενες τιμές R επιτυγχάνεται με Ps = 15 dB, P1= 0 dB και P2 = 2 dB, και η χαμηλότερη τιμή για το SOP είναι 0,5.

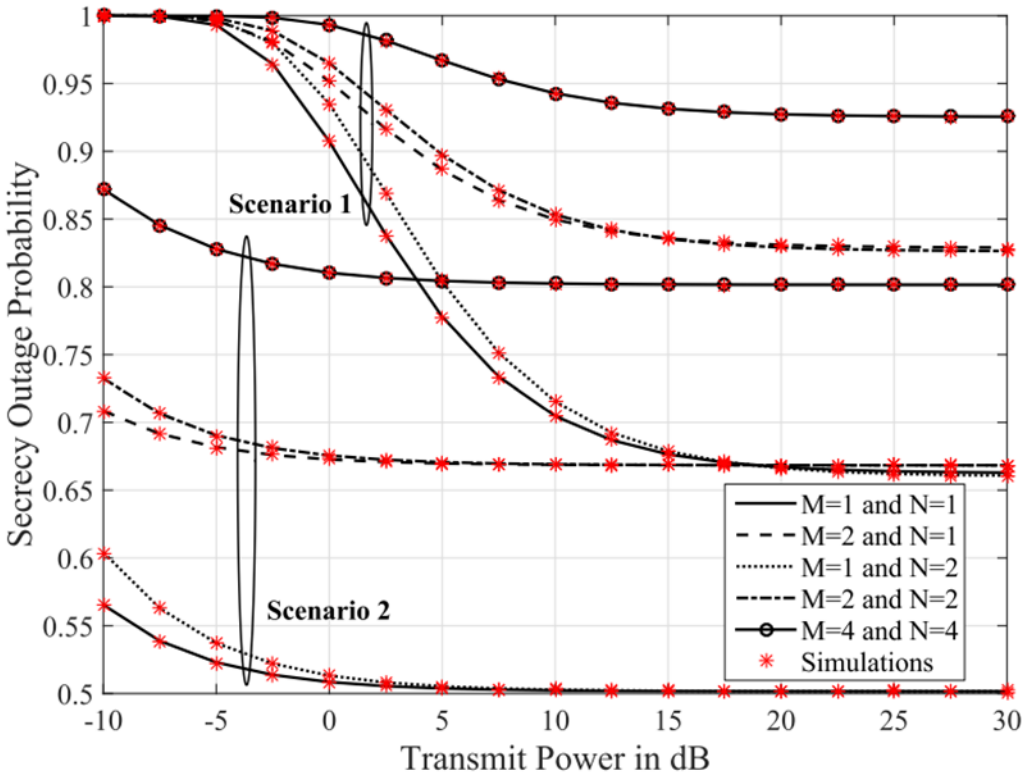


Fig. 5. SOP performance P_{out} as a function of source's transmit power P_s in decibels for both Scenarios 1 and 2, as well as various numbers of cooperative jammers and eavesdroppers.

Η απόδοση της πιθανότητας διακοπής απορρήτου SOP ως συνάρτηση της ισχύος Ps της μετάδοσης της πηγής S απεικονίζεται στο Σχήμα 5. Στην ακόλουθη μετάδοση εξετάστηκαν δύο σενάρια:

1) Σενάριο 1: R = 1, P1 =−4 dB και Pi = P1 + (i - 1) dB με i = 2, 3 και 4 και

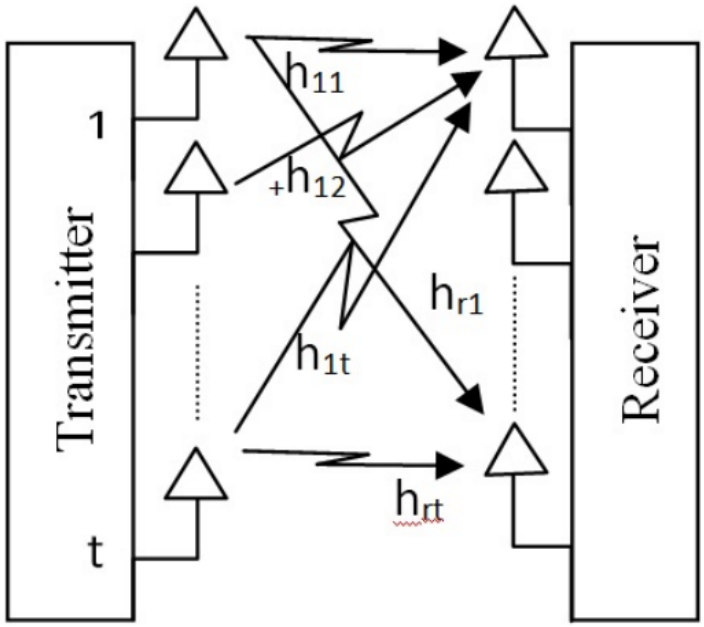
2) Σενάριο 2: R = 0,01, P1 = 1 dB και Pi = P1 + (i - 1) dB με i = 2, 3 και 4.

Τα αποτελέσματα προσομοίωσης υπολογιστή για το SOP συμπίπτουν με τα αριθμητικά για όλες τις παραμέτρους που εξετάστηκαν. Επιπλέον, είναι προφανές ότι, για τις ίδιες τιμές N και M, η απόδοση SOP του σεναρίου 2 είναι πάντα καλύτερη από αυτήν του σεναρίου 1. Και στα δύο σενάρια, επιτυγχάνεται το ελάχιστο SOP N = M = 1 και το μέγιστο με N = M = 4. Επίσης, όπως αναμένεται, το SOP βελτιώνεται με τις αυξανόμενες τιμές του Ps για όλες τις υποθετικές περιπτώσεις. Επιπλέον, φαίνεται σε αυτό το σχήμα ότι, όσο το M αυξάνεται ενώ το N διατηρείται σταθερό, το SOP υποβαθμίζεται σημαντικά. Αυτή η υποβάθμιση της απόδοσης μπορεί να αντιμετωπιστεί για κάποιο εύρος τιμών Ps αυξάνοντας το N. Ωστόσο, η αύξηση N εισάγει μια ποινή απόδοσης στο SOP, η οποία χρειάζεται να ληφθεί υπόψη κατά το σχεδιασμό ενός συνεργατικού σχεδίου παρεμβολής.

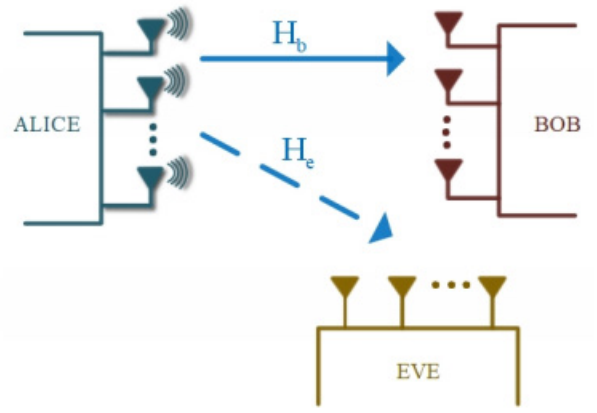
6 Συστήματα πολλαπλών εισόδων - πολλαπλών εξόδων Multiple-Input Multiple-Output (MIMO)

6.1 Βασικά χαρακτηριστικά

Το MIMO είναι μια τεχνολογία για ασύρματες επικοινωνίες που χρησιμοποιούν πολλές κεραίες ταυτόχρονα (και ο πομπός και ο δέκτης) για τη μεταφορά δεδομένων. Σαν αποτέλεσμα έχει την βελτίωση του καναλιού και του εύρους ζώνης του ασύρματου δικτύου, ελαχιστοποιεί τις παρεμβολές και τα σφάλματα και βελτιστοποιεί την ταχύτητα των δεδομένων. Κυρίως, το MIMO εκμεταλλεύεται ένα φυσικό φαινόμενο ραδιοκυμάτων, που ονομάζεται διάδοση πολλαπλών διαδρομών, και συνδυάζει ροές δεδομένων φτάνοντας σε διαφορετικές γωνίες και σε διαφορετικούς χρόνους. Η χωρητικότητα και η απόδοση (απόδοση και ανθεκτικότητα) εξαρτώνται από το αριθμός κεραιών με μια συσκευή. Ως εκ τούτου, όσο ο αριθμός των κεραιών αυξάνεται, το δίκτυο γίνεται πιο ανθεκτικό στις παρεμβολές και στη παρεμβολή. Όταν ο αριθμός των κεραιών είναι σημαντικά μεγάλος, αυτό το σύστημα αναφέρεται ως «Massive MIMO».



6.2 Wiretap channel σε συστήματα MIMO



MIMO wiretap channel model

Και η χωρητικότητα μυστικότητας δίνεται από τον τύπο:

$$C_s = \max_{K_x \succ 0, tr(K_x \preceq P)} \frac{\log_2|\mathbf{I} + \mathbf{H}_b \mathbf{K}_x \mathbf{H}_b^H|}{\log_2|\mathbf{I} + \mathbf{H}_e \mathbf{K}_x \mathbf{H}_e^H|}$$

όπου I ο μοναδιαίος πίνακας, το Kx είναι ο πίνακας συνδιακύμανσης του σήματος μετάδοσης x, το P είναι η μέγιστη ισχύς μετάδοσης., H_b ο συντελεστής καναλιού μεταξύ της πηγής Alice και του δέκτηBob και H_e ο συντελεστής καναλιού μεταξύ της πηγής Alice και του υποκλοπέα Eve.

Δηλαδή ο αριθμητής είναι η χωρητικότητα του νόμιμου δέκτη Bob και ο παρονομαστής του υποκλοπέα Eve. Η χωρητικότητα μυστικότητας ορίζεται ως το μέγεθος που προκύπτει από το προκείμενο πρόβλημα βελτιστοποίησης: εύρεση Kx που μεγιστοποιεί το ρυθμό μετάδοσης μυστικότητας (secrecy rate). Θα πρέπει το Kx να είναι θετικά ημιορισμένος πίνακας και το άθροισμα των διαγώνιων στοιχείων του να φράσετε από Π. Ουσιαστικά σημαίνει ότι το άθροισμα των ισχύων των ανεξάρτητων παράλληλων συμβόλων εκπομπής να μη ξεπερνά το συνολικό power της εκπομπής P.

6.3 Θέματα ασφάλειας στο φυσικό επίπεδο για συστήματα MIMO

- Αυθεντικοποίηση συσκευής
- Δημιουργία και διανομή κλειδιών
- Τεχνικές εμπιστευτικότητας δεδομένων
    - Πίνακας ανακατασκευής
    - Τεχνητός θόρυβος και τεχνητό γρήγορο ξεθώριασμα
    - Σχέδια εμπιστευτικότητας δεδομένων βάσει καναλιού
    - Συνεργατική παρεμβολή και Beamforming
- Συνεργατική εμπλοκή βασισμένη σε συνεχή μετάδοση

6.3.1 Αυθεντικοποίηση συσκευής

Table 1 A summary of the PLS device authentication schemes

Device authentication schemes	Beamforming based on channel characteristics	Generating a symmetric encryption key from channel characteristics	Generating an asymmetric encryption key from channel characteristics	Pilot comparison	Estimating the channel frequently
Advantage	No additional cost and overhead	Achieving authentication and confidentiality at the same time	Achieving authentication and confidentiality at the same time	No additional cost or overhead	No additional cost or overhead
Limitation	Exchanged information are sent in plaintext	Generating encryption keys based on channel characteristics only is a weak assumption since acquiring channel information is not an impossible task	Asymmetric encryption is complex and can not only rely on channel characteristics	Can not rely on pilot comparison for the authentication process only	Additional channel estimations are required
Resource and communication cost	Authentication is verified through multiple rounds	Two steps are done prior to data transmission: (1) Key extraction. (2) Encryption and decryption operations are performed	Two steps are done prior to data transmission: (1) Key extraction. (2) Encryption and decryption operations are performed	Every a specific period pilots are compared with previously acquired ones which are saved	Estimating the channel multiple times
Complexity	Not computationally complex	Not computationally complex: performing XOR operations	Computationally complex: asymmetric encryption	Not computationally complex: performing comparison	Not computationally complex

6.3.2 Παρεμβολή και Beamforming

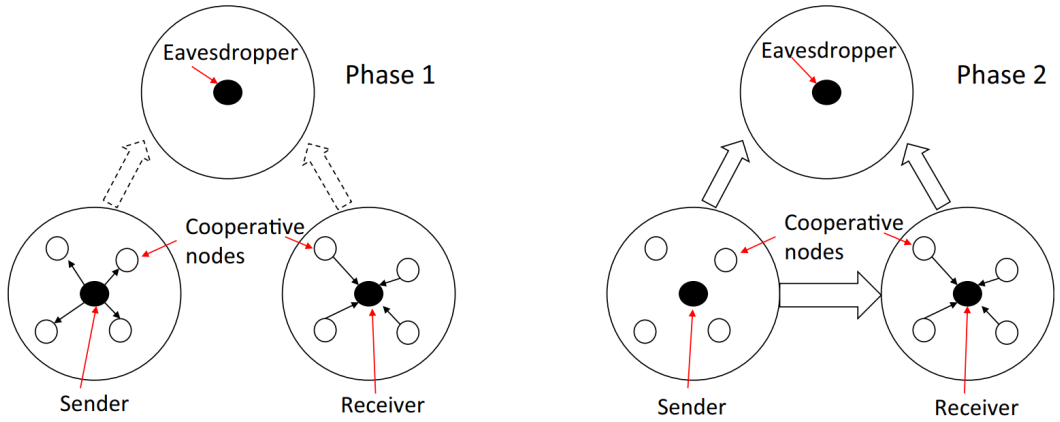
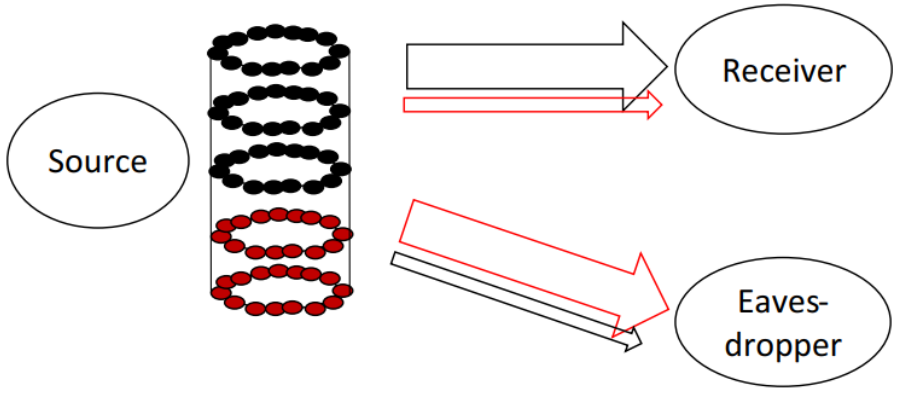


Fig. 9 A MIMO PLS scheme for relay communication systems based on cooperative jamming

Ένα παράδειγμα με συνεργατική παρεμβολή σε σύστημα MIMO φαίνεται στο παραπάνω σχήμα και αποτελείται από δύο φάσεις. Στην πρώτη φάση, ο πομπός στέλνει τα προεπεξεργασμένα δεδομένα σε Ν συνεταιριστικούς κόμβους στο σύμπλεγμα του, και ταυτόχρονα, μερικοί από τους κόμβους στέλνουν σήματα παρεμβολής στον δέκτη. Στη δεύτερη φάση, ο πομπός και οι κόμβοι Ν στέλνουν δεδομένα στον δέκτη, με αποτέλεσμα ένα να δημιουργηθεί ένα εικονικό σύστημα MISO. Επίσης, οι κόμβοι παρεμβολής στέλνουν ξανά τα ίδια σήματα παρεμβολής στον δέκτη . Ο δέκτης μπορεί απλά να ανακτήσει το πραγματικό σήμα αφαιρώντας τα ληφθέντα σήματα στη πρώτη και στη δεύτερη φάση.

6.3.3 Συνεργατική παρεμβολή βασισμένη σε συνεχή μετάδοση



MIMO PLS scheme based on simultaneous data transmission and jamming

Όπως φαίνεται στο σχήμα η κυλινδρική διάταξη, που αποτελείται από πολλές κυκλικές συστοιχίες που στοιβάζονται η μία πάνω στο άλλη, χωρίζεται σε δύο συστοιχίες: η πρώτη χρησιμοποιείται για τη μετάδοση χρήσιμων πληροφοριών στον προοριζόμενο χρήστη με μικρή διαρροή προς τη δεύτερη συστοιχία, η οποία χρησιμοποιείται γα να μεταδίδει σήματα παρεμβολής στον υποκλοπέα. Αυτό μπορεί να επιτευχθεί μέσω διαμόρφωσης δέσμης στην οποία η κύρια δέσμη που χρησιμοποιείται για την αποστολή χρήσιμων πληροφοριών κατευθύνεται προς τον προοριζόμενο χρήστη και η δέσμη που μεταδίδει το σήμα παρεμβολής κατευθύνεται προς τον υποκλοπέα.

7 Τεχνολογίες Φυσικού Επιπέδου Επόμενης Γενιάς

Σχεδιάζεται να επιτευχθούν δίκτυα κινητής τηλεφωνίας επόμενης γενιάς με υψηλά ποσοστά χωρητικότητας για την αντιμετώπιση της ταχείας ανάπτυξης της κίνησης δεδομένων. Ο συνδυασμός βασικών τεχνολογιών 5G θεωρείται ως μια οικονομικά αποδοτική λύση για την κάλυψη του υψηλού QoS απαιτήσεις στο 5G. Ωστόσο, η δραματική αύξηση σε όγκο δεδομένων και τα πολύπλοκα σενάρια επικοινωνίας προβάλλουν υψηλότερες απαιτήσεις για την ασφάλεια του 5G. Εδώ, εξετάζουμε τις έννοιες καθεμιάς από τις πολλά υποσχόμενες τεχνολογίες ενεργοποίησης για το 5G, συμπεριλαμβανομένων των πλεονεκτημάτων και των μειονεκτημάτων τους. Στη συνέχεια, συνοψίζουμε τα πιο πρόσφατα ερευνητικά αποτελέσματα του PLS για τεχνολογίες 5G.

7.1 Massive MIMO

Το Massive MIMO είναι μια τοπολογία πολλών χρηστών στην οποία το ο σταθμός βάσης (BS) διαθέτει μεγάλο αριθμό κεραιών όπως που απεικονίζεται στο Σχήμα 5. Αυτές οι ρυθμίσεις παρέχουν αρκετούς βαθμούς ελευθερίας για δίκτυα, καλύτερη απόδοση σε χωρητικότητες καναλιών και βελτίωση των ποιοτήτων επικοινωνίας στα δίκτυα 5G [92]. Για λόγους ασφαλείας, το τεράστιο MIMO παρέχει έναν πολύ προσανατολισμένο οδηγό δέσμης για την τοποθεσία του νόμιμου χρήστη. Έτσι, η διαρροή πληροφοριών μειώνεται σημαντικά σε ανεπιθύμητες τοποθεσίες (δηλαδή, την Eve) [93].

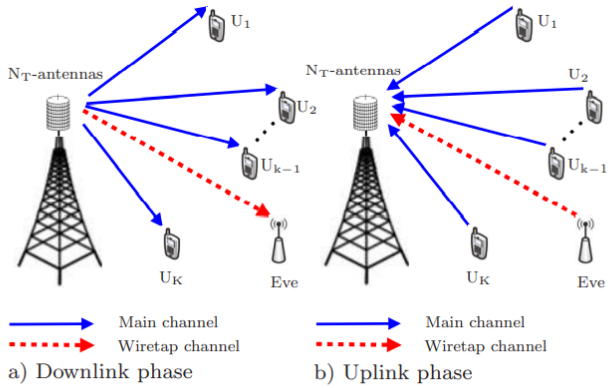


Fig. 5 Massive MIMO downlink with K legitimate user nodes, U_k for $k = 1, \cdots, K$, and an eavesdropper.

Οι συγγραφείς στο [94] ήταν οι πρώτοι που διερεύνησαν τα μειονεκτήματα της απόδοσης του PLS υποθέτοντας ότι το ο αριθμός των κεραιών πηγαίνει στο άπειρο (δηλαδή, το τεράστιο MIMO). Σε αντίθεση με το παραδοσιακό MIMO, το τεράστιο MIMO παρουσιάζει τι ακόλουθες μεγάλες προκλήσεις: 1) Η διαδικασία εκτίμησης CSI είναι ένα δύσκολο έργο. 2) Τα μοντέλα καναλιών δεν είναι ανεξάρτητα καθώς οι αποστάσεις των κεραιών είναι μικρότερες από το μισό του μήκους κύματος. Επομένως, το τεράστιο MIMO είναι ένα ανοιχτό ερευνητικό πεδίο [95]. Στη συνέχεια, ερευνούμε τις

τρέχουσες επιθέσεις ασφαλείας της τεράστιας MIMO που βασίζονται σε περιπτώσεις παθητικής και ενεργητικής υποκλοπής, αντίστοιχα.

7.1.1 Σενάρια Παθητικής Υποκλοπής

Η βασική έννοια εδώ είναι ότι η ύπαρξη ενός παθητικού υποκλοπέα δεν επηρεάζει καθόλου τη δέσμη μετάδοσης στο B_S. Άρα, έχει αμελητέα επίδραση στο C_S. Πρόσφατα, στο [96] αναπτύχθηκε ένας αλγόριθμος για τη βελτιστοποίηση της κατανομής ισχύος της μετάδοσης δέσμης για MIMO μαζικής μάζας μιας κυψέλης που αποτελείται από έναν παθητικό υποκλοπέα με πολλαπλές κεραίες. Τα ευρήματα έδειξαν ότι αυτή τη δέσμη μετάδοσης μπορεί να επιτύχει τη βέλτιστη απόδοση από άποψη του C_S. Οι συγγραφείς στο [97] ερεύνησαν ασφαλείς μεταδόσεις πολλαπλών ζευγών μαζικών συστημάτων αναμετάδοσης MIMO AF θεωρώντας το Ricean fading. Σε αυτό το έργο, το εφικτό ποσοστό μυστικότητας αθροίσματος μεγιστοποιείται χρησιμοποιώντας μια τοπολογία ελέγχου ισχύος. Επίσης, η χρήση των προγραμμάτων AN-aiding για την υποβάθμιση του καναλιού υποκλοπής και για τη βελτίωση της ασφάλειας στο τεράστιο MIMO αναλύθηκε στο [98]. Άλλες προσεγγίσεις στη massive MIMO με παθητικούς υποκλοπείς περιλαμβάνουν την επίδραση των ελλείψεων υλικού στην απόδοση PLS της τεράστιας κατερχόμενης ζεύξης MIMO με πολλαπλές κεραίες [99], ανάλυση απόδοσης ασύρματων επικοινωνιών σε μαζικό MIMO πολλών χρηστών με χρήση ατελούς CSI [100], και ανάλυση SOP για τεράστια σενάρια MIMO [101].

7.1.2 Σενάρια ενεργών υποκλοπών

Ένας μεγάλος αριθμός ερευνητικών εργασιών PLS το θεωρεί αυτό το CSI του Bob είναι γνωστό στην Alice και δεν μπαίνει στη διαδικασία για την απόκτηση αυτού του CSI. Στη διάρκεια της διπλής διαίρεσης (TDD) του μαζικού MIMO, κατά την φάση της ανερχόμενη ζεύξη , οι νόμιμοι κόμβοι μεταδίδουν πιλοτικά σήματα στο BS να εκτιμήσει το CSI για την μεταγενέστερη μετάδοση του κατά την κατερχόμενη ζεύξη. Ταυτόχρονα, μια ενεργή υποκλοπή μπορεί να παρέμβει στο στάδιο της εκπαίδευσης για να προκαλέσει έναν μόλυνση στο BS (βλέπε Εικόνα 6). Αυτές οι δυνάμεις στη φάση μετάδοσης (δηλαδή κατερχόμενη ζεύξη) του BS προς εγγενώς μορφή δέσμης προς τον υποκλοπέα αυξάνοντας την ισχύ του λαμβανόμενου σήματος [102]. Αυτό το γεγονός υποθέτει ότι ένα ποσοστό μυστικότητας μπορεί να μην είναι εφικτό. Το αποτέλεσμα αυτής της επίθεσης είναι ότι τα πλεονεκτήματα του PLS για μαζικό MIMO έχουν χαθεί [103]. Για την παράκαμψη του αναφερόμενου περιορισμού, οι ακόλουθες εργασίες διερεύνησαν τεχνικές για να αποφεύγεται η πιλοτική επίθεση μόλυνσης (PCA). Στο [104], οι συγγραφείς πρότειναν μια αξιόπιστη επικοινωνία που δεν χρειάζονται στατιστικές πληροφορίες σχετικά με τους συνδέσμους για το TDD του μαζικού MIMO με ενεργό υποκλοπέα. Στην προτεινόμενη μετάδοση, ένα ασύγχρονο πρωτόκολλο χρησιμοποιείται αντί του συμβατικού σύγχρονου πρωτοκόλλου.

Μια πολιτική ελέγχου ισχύος μετάδοσης παρουσιάστηκε στο [105], για κατανομή ισχύος εκπομπής στο BS/αναμεταδότη για μεγιστοποίηση του επιτεύξιμου ποσοστού μυστικότητας στο Massive MIMO στον κατερχόμενο σύνδεσμο. Για το PLS στο τεράστιο MIMO, το [86] έχει σχεδιάσει ένα ισχυρό σχήμα μαζί

με τη διαμόρφωση δέσμης AN για να παραδώσει τους νόμιμους κόμβους και τους υποκλοπείς διαφορετικούς λόγους σήματος προς παρεμβολή και θόρυβο (SINR). Άλλες ασφαλείς μαζικές μεταδόσεις έναντι ενεργών υποκλοπέων περιλαμβάνει τη στρατηγική συνεργατικού σχήματος [107], σύστημα μετάδοσης ασφαλούς κατερχόμενης ζεύξης με τη βοήθεια δεδομένων [108], και ο σχεδιασμός ασφαλών επικοινωνιών που βασίζεται στο θεωρία παιγνίων[109].

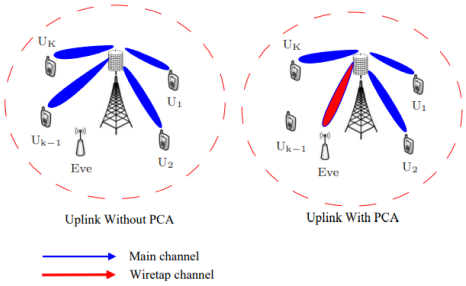


Fig. 6 PCA on massive MIMO systems.

7.2 mm-Wave

Σήμερα, τα περισσότερα ασύρματα συστήματα διατίθενται στο φάσμα ζώνης 300 MHz έως 3 GHz, το οποίο είναι εξαιρετικά γεμάτο. Σε αυτό το πλαίσιο, mm-Wave5 είναι μια πολύ πρωτοποριακή βασική λύση για τα επόμενα ασύρματα δίκτυα (5G και πέρα) για να ξεπεραστεί αυτός ο περιορισμός. Η ιδέα πίσω από τις επικοινωνίες mm-Wave είναι να εκμεταλλευτεί το ανεκμετάλλευτο σύστημα προδιαγραφών κυμάτων mm υψηλής συχνότητας, που κυμαίνεται από 3-300 GHz για να αντιμετωπίσει μελλοντικές εφαρμογές για κινητές συσκευές πολλαπλών Gigabit ανά δευτερόλεπτο. Σε αντίθεση με τα δίκτυα μικροκυμάτων, τα δίκτυα mm-Wave έχουν πολλά νέα χαρακτηριστικά, όπως μεγάλο αριθμό κεραιών , μικρής εμβέλειας, και διαφορετικούς νόμους διάδοσης [112]. Η υιοθέτηση του στα συστήματα δικτύων PLS mm-Wave είναι ένα εξαιρετικά αναδυόμενο θέμα έρευνας. Σε αυτόν τον τομέα έχουν αναπτυχθεί αρκετές προσεγγίσεις . Το γενικό μοντέλο του PLS για mm-Wave, τεράστια MIMO, FD και Small Cells για 5G παρουσιάζεται στο Σχ. 7. Στη συνέχεια, εξετάζουμε ορισμένες από τις τρέχουσες εργασίες για να επισημάνουμε τις δυνατότητες αυτού του αναδυόμενου πεδίου. Οι κύριες ερευνητικές εργασίες επικεντρώνονται στα 28, 38 και 60 GHz [114].

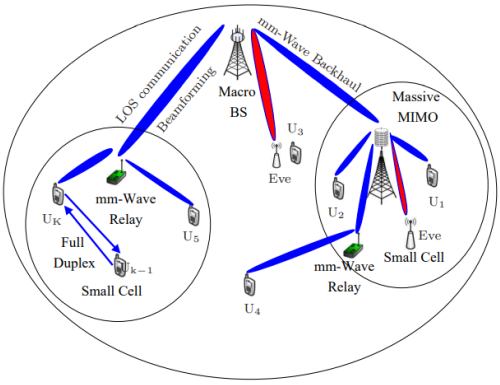


Fig. 7 Illustration of promising technologies such as mm-Wave, massive MIMO, Full Duplex, and Small Cells.

Στο [115], για μεγιστοποίηση του SNR (δηλαδή, για βελτίωση του C_S), οι συγγραφείς πρότειναν AN με δύο στάδια ασφαλή μεθόδους υβριδικής διαμόρφωσης δέσμης στο σενάριο υποκλοπής MIMO mm-Wave relay. Εδώ, ο συνδυασμός των αλγόριθμων υβριδικής διαμόρφωσης δέσμης δύο σταδίων με AN επιτρέπει την εγγύηση υψηλής απόδοσης και ασφάλειας επικοινωνίας. Οι συγγραφείς στο [116] διερεύνησαν ασφαλείς τεχνικές επικοινωνίας, δηλαδή τη μέγιστη αναλογία μετάδοσης (MRT) beamforming, και AN beam forming. Συγκεκριμένα, αναπτύχθηκε η βέλτιστη ισχύς κατανομή μεταξύ AN και το σήμα ενδιαφέροντος που μεγιστοποιεί το C_S για τη διαμόρφωση δέσμης. Σχετικά με τα τροχαία περιβάλλοντα, στο [117], οι ερευνητές πρότειναν μια τεχνική PLS που βασίζεται στη θέση για ασφαλή mm-Wave επικοινωνία οχημάτων. Μια τέτοια προτεινόμενη τεχνική εκμεταλλεύεται μεγάλο αριθμό κεραιών στις mm-Συχνότητες κυμάτων για να μπλοκάρουν τους υποκλοπείς με ευαίσθητους δέκτες. Η τεχνική αποδείχθηκε ότι προσφέρει καλή ανά απόδοση όσον αφορά το SOP. Άλλες προσεγγίσεις περιλαμβάνουν το PLS Analysis of Hybrid mm-Wave Networks [118], και C_S του 5G mm-Wave Small Κύτταρα [119].

7.3 HetNets – Μικρές κυψέλες

Παραδοσιακά, τα μακροκυτταρικά δίκτυα είναι αποτελεσματικά προσφέροντας κάλυψη περιοχής για εφαρμογές και υπηρεσίες φωνής που υποστηρίζουν χαμηλή κίνηση δεδομένων αλλά περιορισμένη στην παροχή υψηλών ρυθμών δεδομένων. Έτσι, μια από τις πολλά υποσχόμενες λύσεις για τους χρήστες πρόκειται να μειώσουν το μέγεθος της κυψέλης σε μελλοντικά έργα ασύρματου δικτύου [120]. Σε αυτό το πλαίσιο, το HetNets θα εκτελέσει ένα κεντρικό ρόλο για την κάλυψη των απαιτήσεων του 5G. Ο στόχος του HetNetsis είναι να κάνει αποτελεσματική χρήση του φάσματος για να ικανοποιήσει τη θεαματική αύξηση των απαιτήσεων δεδομένων στις επερχόμενες υπηρεσίες κινητής τηλεφωνίας. Στις τοπολογίες HetNets, χρήστες με διαφορετικές δυνατότητες (δηλαδή, ισχύς μετάδοσης, περιοχές κάλυψης, κ.λπ.) υλοποιούνται για να είναι μέρος μιας ιεραρχικής δομή πολλαπλών επιπέδων, όπως απεικονίζεται στο Σχήμα 8. Οι κόμβοι υψηλής ισχύος (HPN) με πεδία ηλικίας ευρείας ραδιοκάλυψης βρίσκονται στο κελί μακροεντολής, ενώ χαμηλής ισχύος κόμβοι (LPN) με περιορισμένη κάλυψη βρίσκονται σε μικρά κελιά [24]. Τα μικρά κελιά (συνήθως με κάλυψη λίγων μέτρων) μπορεί να έχουν διαφορετικές διαμορφώσεις. Για παράδειγμα, τα femtocells που χρησιμοποιούνται συνήθως σε σπίτια και εταιρείες ανάπτυξης και τα picocells που χρησιμοποιούνται για άφθονη κάλυψη εξωτερικού χώρου [120]. Επιπλέον, το HetNets περιλαμβάνει ένα επίπεδο συσκευής που ενσωματώνει συσκευή σε συσκευή (D2D) επικοινωνίες. Αυτή η τεχνολογία ευνοεί συσκευές της γύρω περιοχής για απευθείας σύνδεση και συνεργασία χωρίς να χρησιμοποιούμε HPN/LPN, γεγονός που τις καθιστά ισχυρό εργαλείο για υπηρεσίες δεδομένων χαμηλής καθυστέρησης και υψηλής απόδοσης [121]

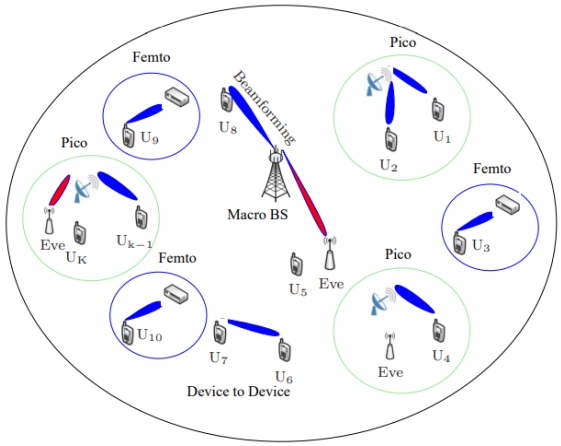


Fig. 8 HetNets with legitimate users and eavesdroppers.

Η τοπολογία πολλαπλών επιπέδων στο HetNets συνεπάγεται τεχνικές προκλήσεις (π.χ. αυτοοργάνωση, backhauling, han dover και παρεμβολές) στη διερεύνηση του PLS σε σύγκριση με την παραδοσιακή μονοβάθμια αρχιτεκτονική [122]. Στη συνέχεια, εξετάζουμε τις πιο πρόσφατες εργασίες που αφορούν τις προαναφερθείσες προκλήσεις των HetNets στο PLS. Σε δύο νέες προσεγγίσεις [123,124], η απόδοση του PLS σε δίκτυα πολλαπλών κυψελών έχει μελετηθεί. Οι ερευνητές έχουν εκμεταλλευτεί τις συνεργατικές εκπομπές πολλαπλών κεραιών για τη βελτίωση του C_S υποθέτοντας: i) ένα μόνο υποκλοπέα [123], και ii) ένας πολλαπλός αναξιόπιστος εκδότης [124]. Στο [125], οι συγγραφείς παρουσίασαν μια τοπολογία ακυρωμένης ευκαιριακής επιλογής κεραίας (IC-OAS) για τη βελτίωση του PLS στο HetNets. Εδώ, ένα παθητικός υποκλοπέας θεωρείται ότι παρεμποδίζει τις επικοινωνίες τόσο των μάκρο όσο και των μικρών κελιών Άλλα έργα ασφαλούς επικοινωνίας σε συστήματα συστημάτων HetNets περιλαμβάνουν: Στρατηγικές Stochastic Geometry [126], η κρυφή ανάλυση διακοπής, υποβάλλεται σε κανάλια εξασθένισης Nakagami-m [127] και σχεδιασμός ασφαλών επικοινωνιών με βάση θεωρία παιγνίων [128].

7.4 Full-Duplex

Μεταξύ των πολλά υποσχόμενων τεχνολογιών για το 5G, η τεχνολογία FD φέρει σημαντικές προκλήσεις για τις επικοινωνίες PLS. Από τη μία πλευρά, το FD επιτρέπει στον κόμβο προορισμού να δημιουργήσει AN να παρέμβει στον υποκλοπέα και να λάβει τα δεδομένα ταυτόχρονα. Από την άλλη πλευρά, εάν το σταγονόμετρο μαρκίζας έχει την τεχνολογία FD, μπορεί να επιτεθεί ενεργά ο δέκτης στη μετάδοση ενώ κρυφακούει. Επίσης, τα συστήματα FD μπορούν να διπλασιάσουν τη φασματική απόδοση όσον αφορά τα κοινά σχήματα ημιαμφίδρομης λειτουργίας. Ωστόσο, το κύριο μειονέκτημα που επηρεάζει τη μετάδοση του FD είναι η διαχείριση του σήματος αυτοπαρεμβολής που επιβλήθηκε από την κεραία μετάδοσης στην κεραία λήψης μέσα στον ίδιο πομποδέκτη [129]. Η έρευνα για το FD η επικοινωνία PLS μπορεί να ταξινομηθεί σε τέσσερις κατηγορίες σχημάτων FD PLS. Συγκεκριμένα, το FD δέκτης, ο πομπός και δέκτης FD, το FD BS, και ο υποκλοπής FD [113]. Στη συνέχεια, εξετάζουμε τα περισσότερα τρέχουσες εργασίες σχετικά με τις διαφορετικές διαμορφώσεις του την προαναφερθείσα τεχνολογία FD. Στο [130], οι συγγραφείς πρότειναν μια νέα μέθοδο εκπαίδευσης καναλιών (CT) για τον Δέκτη FD με

σκοπό τη βελτίωση PLS. Σε αυτή τη ρύθμιση, ο δέκτης (δηλαδή, ο Bob) είναι εξοπλισμένος με κεραίες NB. Έτσι, μπορεί ταυτόχρονα να λαμβάνει τα δεδομένα και να μεταδίδει AN στον υποκλοπέα. Εδώ, για να μειωθεί η μη ακυρώσιμη αυτοπαρέμβαση λόγω του μεταδιδόμενου AN, ο κόμβος προορισμού πρέπει να εκτιμήσει το κανάλι αυτοπαρέμβασης πριν από το στάδιο της επικοινωνίας. Στο [131] θεωρήθηκε πρόβλημα παθητικής και έξυπνης υποκλοπής επίθεσης στο σύστημα υποκλοπής MIMO, όπου ο δέκτης λειτουργεί με λειτουργία FD. Σε ένα τέτοιο μοντέλο συστήματος, ο έξυπνος υποκλοπέας ακυρώνει την παρεμβολή (που προκαλείται από τον δέκτη) κλέβοντας το CSI μεταξύ νόμιμων κόμβων. Για να αντιμετωπιστεί αυτό, οι συγγραφείς παρουσίασαν μια προσέγγιση συνεργατικής παρεμβολής μεταξύ πομποδεκτών για την επίτευξη της βέλτιστης απόδοσης PLS. Σχετικά με το FD ενεργό υποκλοπέα (FDAE), στο [132], αναλύθηκε η απόδοση κατά της υποκλοπής και κατά της εμπλοκής σε σενάρια D2D. Σε αυτήν την περίπτωση, το FDAE μπορεί να υποκλέψει παθητικά μυστικά δεδομένα σε τοπολογίες D2D και να μπλοκάρει ενεργά όλα τα νόμιμα κανάλια. Από αυτή την άποψη, οι συγγραφείς πρότειναν μια ιεραρχική μέθοδο ελέγχου ισχύος με πολλαπλός εξοπλισμός κόμβων D2D και ένας κυψελοειδής κόμβος αντιμετωπίσει την έξυπνη FDAE. Άλλες εργασίες περιλαμβάνουν στρατηγικές FD στο HetNets [133, 134], μεγιστοποίηση του ποσοστού μυστικότητας στο Wireless Multi-Hop Δίκτυα FD [135] και βασισμένη σε ασφαλή επικοινωνία σχετικά με την κοινή σχεδίαση πληροφοριών και τη διαμόρφωση δέσμης AN για τα δίκτυα FD [136].

7.5 Μη ορθογώνια πολλαπλή πρόσβαση

Λόγω της περιορισμένης φασματικής απόδοσης των ορθογώνιων συστημάτων πολλαπλής πρόσβασης (OMA) σε ασύρματα δίκτυα, τα σχέδια OMA δεν είναι κατάλληλα για την αντιμετώπιση της εκρηκτικής αύξησης της κίνησης δεδομένων του 5G. Ως αποτέλεσμα, η NOMA αναδεικνύεται ως ένας πολλά υποσχόμενος υποψήφιος για πολλαπλή πρόσβαση 5G για να παρέχει τεράστια συνδεσιμότητα και μεγάλο σύστημα απόδοσης [137]. Εξάλλου, είναι γνωστό ότι το NOMA θα χρησιμοποιήσει προηγμένες τεχνικές λήψης όπως η διαδοχική ακύρωση παρεμβολών (SIC) για ισχυρή πολλαπλή πρόσβαση. Αυτό το γεγονός μπορεί να είναι ένα μειονέκτημα όσον αφορά τις καθυστερήσεις επεξεργασίας. Ευτυχώς, η μετάδοση/λήψη διαμορφώνουν σχήματα με χαμηλή καθυστέρηση για συστήματα NOMA και έχουν διερευνηθεί στη βιβλιογραφία. Το βασικό μοντέλο NOMA για το PLS φαίνεται στο Σχήμα 9. Υπάρχουν δύο είδη σεναρίων υποκλοπών: i) ο παθητικός υποκλοπέας, του οποίου το κανάλι δεν μπορεί να είναι γνωστό στο Alice. ii) ο ενεργητικός υποκλοπής (δηλαδή κοινός χρήστης), του οποίου το κανάλι μπορεί γίνει γνωστό στην Alice. Ως εκ τούτου, η παροχή επιπέδων ασφάλειας έναντι των δύο τύπων υποκλοπών στη τεχνολογία NOMA είναι ένα προκλητικό ερευνητικό θέμα στο σχεδιασμό των δικτύων 5G [57]. Η κύρια ιδέα πίσω από το PLS για το NOMA είναι να μετριάσει τα προβλήματα ασφάλειας βρίσκοντας τη βέλτιστη πολιτική κατανομής ενέργειας που μεγιστοποιεί το ποσοστό αθροίσματος μυστικότητας (SSR) ενώ ικανοποιεί το QoS απαίτησης των χρηστών. Στη συνέχεια, ερευνούμε τις βασικές συνεισφορές σχετικά με PLS σε συστήματα 5G NOMA. Στο [138], οι συγγραφείς διερεύνησαν την απόδοση του PLS σε ένα σχήμα NOMA μονής εισόδου (SISO) μεγιστοποιώντας το SSR του NOMA που υπόκειται στις απαιτήσεις QoS των χρηστών. Εδώ, η NOMA έχει αποδείξει μια αξιοσημείωτη βελτίωση SSR σχετικά με την κλασική OMA.

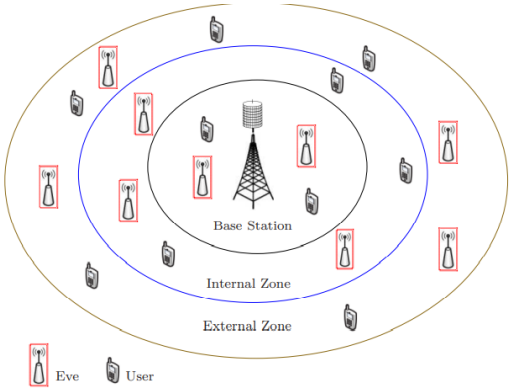


Fig. 9 PLS model for NOMA

Στο [139], οι ερευνητές πρότειναν μια ασφαλή μετάδοση για κατερχόμενη ζεύξη πολλαπλής εισόδου απλής εξόδου (MISO) NOMA με ενεργειακά αποδοτικό σχεδιασμό. Σε αυτή την προσέγγιση, φάνηκε ότι η συνεταιριστική εμπλοκή NOMA είναι ένα σύστημα που επιτυγχάνει πολύ καλύτερες επιδόσεις μυστικότητας από το σύστημα απευθείας μετάδοσης NOMA. Η μυστικότητα σε συνεχόμενη ασύρματη πληροφορία και μεταφορά ισχύος (SWIPT) σε συστήματα κατερχόμενης ζεύξης NOMA διερευνήθηκε στο [140]. Αργότερα, οι προκλήσεις ασφαλείας των χρηστών σε ένα εξαιρετικά πυκνό δίκτυο μελετήθηκαν στο [141]. Εδώ, αποδείχθηκε ότι η πολλαπλή πρόσβαση που βασίζεται στο NOMA είναι επιτυχής για την επίτευξη υψηλής SSR για χρήστες σχεδιάζοντας αποτελεσματικά τους πόρους κατανομής. Άλλα ενδιαφέροντα έργα περιλαμβάνουν την απόδοση του PLS σε ανερχόμενη ζεύξη NOMA χρησιμοποιώντας μια προσέγγιση στοχαστικής γεωμετρίας για την ανάλυση της αποτελεσματικής απόδοσης μυστικότητας [142], η επίδραση της τυχαίας κινητικότητας στη μεγιστοποίηση SSR του σε συστήματα NOMA υπόκεινται σε όρια ισχύος και το QoS των χρηστών [143], το επιτεύξιμο ποσοστό μυστικότητας χρησιμοποιώντας τη βέλτιστη σχεδίαση ασφαλείας στα NOMA VLC δίκτυα [144] και η βελτιστοποίηση του SSR και για τους κύριους χρήστες, αλλά και τυχαία αναπτυγμένους δευτερεύοντες χρήστες στο υποκείμενο γνωστικό ράδιο δίκτυο NOMA [145].

8 Συμπεράσματα

Η ασφάλεια σε φυσικό επίπεδο στα ασύρματα δίκτυα είναι μία τεχνική που έρχεται να συμπληρώσει και να βελτιώσει την ασφάλεια επικοινωνίας στα ασύρματα δίκτυα. Σε σύγκριση με τις κρυπτογραφικές προσεγγίσεις, η ασφάλεια φυσικού επιπέδου είναι ένα διαφορετικό παράδειγμα όπου επιτυγχάνεται η μυστικότητα εκμεταλλευόμενοι τις ιδιότητες του φυσικού στρώματος του συστήματος επικοινωνίας, όπως θερμικός θόρυβος, παρεμβολές και τη χρονικά μεταβαλλόμενη φύση των καναλιών εξασθένισης.

Εξετάζοντας ζητήματα με συνεργατικούς παρεμβολείς και υποκλοπείς, συμπεραίνω ότι όσο το πλήθος των παρεμβολέων αυξάνεται τόσο αυξάνεται η παρεμβολή η οποία επηρεάζει όμως εκτός από τους υποκλοπείς, και το νόμιμο δέκτη. Επίσης αυξάνεται και το κόστος της διαδικασίας διανομής ισχύος, η οποία απαιτεί γνώση των καναλιών. Η ισορροπία λοιπόν μεταξύ κόστους και χρήση συνεργατικής παρεμβολής είναι ένα ζήτημα που χρίζει διερεύνησης. Από την άλλη πλευρά όσο αυξάνονται οι υποκλοπείς τόσο αυξάνεται η πιθανότητα κάποιος από αυτούς να επιτύχει την υποκλοπή, χωρίς να υπάρχει περιορισμός στο πλήθος τους.

Στον τομέα των τεχνολογιών 5G, προκύπτουν τα ακόλουθα ερευνητικά θέματα από το τις τεχνολογίες που αξιολογήθηκαν σε αυτήν την έρευνα:

– Τα μοντέλα καναλιών με ακριβή εξασθένιση παίζουν αξιοσημείωτο ρόλο σε έναν βέλτιστο σχεδιασμό ασφαλούς μετάδοσης 5G. Έτσι, ορισμένες προσπάθειες έχουν προσανατολιστεί στην πρόταση νέων πιο ακριβών μοντέλων καναλιών που παρέχουν καλύτερη προσαρμογή σε μετρήσεις πεδίου σε μια ποικιλία των νέων σεναρίων διάδοσης κυμάτων mm. Σε αυτό το κείμενο, όπως ισχυρίζονται οι συγγραφείς στο [126] τόσο Fluctuating Multiple-Ray όσο και το N-Wave with Diffuse τα μοντέλα εξασθένισης ισχύος αποτελούν πολλά υποσχόμενα εναλλακτικά μοντέλα για να χαρακτηρίσουν το περιβάλλον διάδοσης στις επικοινωνίες mm-Wave. Επομένως, η απόδοση των τεχνικών PLS σε αυτά τα γενικευμένα κανάλια είναι ένα σημαντικό θέμα για περαιτέρω διερευνήσεις.

– Η παροχή PLS συνήθως συνεπάγεται συμβιβασμό άλλων απαιτήσεων του QoS του συστήματος. Για παράδειγμα, υψηλής ασφάλειας επίπεδα συνήθως θυσιάζουν την απόδοση, ενώ τα σχήματα AN θέτουν σε κίνδυνο την απόδοση ισχύος. Με βάση αυτούς τους παράγοντες, ο χαρακτηρισμός των μετρήσεων μυστικότητας στο αντίπαλα μοντέλα ασύρματων μέσω μη παραδοσιακών (π.χ., κλασματική αμφιβολία, μέση διαρροή πληροφοριών, μετρήσεις του ποσοστού και του GSOP) είναι βασικά θέματα σε μελλοντικές έρευνες.

– Στα παραδείγματα ασφάλειας, μια πολλά υποσχόμενη κατεύθυνση έρευνας είναι η ενσωμάτωση του PLS και της κλασικής ασύρματης κρυπτογραφίας. Συγκεκριμένα, σε φυσικό επίπεδο μπορούν να αξιοποιηθούν τα χαρακτηριστικά του μέσου για το σχεδιασμό νέων αλγορίθμων ασφαλείας προς βελτίωση του τρέχοντος ελέγχου ταυτότητας και τη διαχείριση κλειδιών σε υψηλότερα στρώματα. Ωστόσο, η ενοποίηση και των δύο προσεγγίσεων δεν έχει μελετηθεί σωστά επί του παρόντος. Επομένως, αυτό το θέμα χρήζει περαιτέρω διερεύνησης.

– Μια ενδιαφέρουσα μελλοντική ερευνητική κατεύθυνση θα μπορούσε να είναι μια λεπτομερής έρευνα για τα κύρια μειονεκτήματα και τα πλεονεκτήματα του ελέγχου ταυτότητας φυσικού επιπέδου (PLA) και Generation Secret-Key στο 5G. Υπό αυτή την έννοια, σε ερευνητικό πεδίο, το οποίο δεν έχει διερευνηθεί ακόμη εκτενώς στη βιβλιογραφία, είναι η μηχανική μάθηση για έξυπνο PLA σε ασύρματα δίκτυα 5G.

– Λόγω του συνδυασμού καινοτόμων τεχνολογιών για την κάλυψη των αυξανόμενων απαιτήσεων της κυκλοφορίας δεδομένων και αναδυόμενων υπηρεσιών, είναι απαραίτητο να διερευνηθούν τεχνικές για το PLS σχετικά με αυτά τα νέα σενάρια δικτύου. Μέσα σε αυτά τα δίκτυα ξεχωρίζουν τα ακόλουθα: Unmanned Aerial Vehicles (UAV), enhanced Mobile Broadband (eMBB), Ultra-Reliable, and Low-Latency Communications (URLLC), massive Machine-Type Communications (mMTC), and Vehicle-to-Everything (V2X) networks.

Πηγές – Βιβλιογραφία

1. Physical Layer Security In Wireless Networks: A Tutorial
YI-SHENG SHIU AND SHIH YU CHANG, HSIAO-CHUN WU, SCOTT C.-H. HUANG, HSIAO-HWA CHEN.

2. Physical Layer Security in Wireless Cooperative Relay Networks: State of the Art and Beyond
Leonardo Jiménez Rodríguez, Nghi H. Tran, Trung Q. Duong, Tho Le-Ngoc, Maged Elkashlan, and Sachin Shetty

3. Relay Selection for Secure Cooperative Networks with Jamming
Ioannis Krikidis,, John S. Thompson,, and Steve McLaughlin

4. A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security Furqan Jameel, Shurjeel Wyne, Georges Kaddoum, Trung Q. Duong

5. COOPERATIVE COMMUNICATIONS HARDWARE, CHANNEL & PHY
Mischa Dohler, Yonghui Li

6. Cooperative Communications and Networking
K. J. Ray Liu, Ahmed Sadek, Weifeng Su, Andres Kwasinski

7. Improving Wireless Physical Layer Security via Cooperating Relays
Lun Dong,, Zhu Han,, Athina P. Petropulu, and H. Vincent Poor

8. Secure Communication Via an Untrusted Non-Regenerative Relay in Fading Channels
Jing Huang, Amitav Mukherjee, and A. Lee Swindlehurst

9. Securing Relay Networks with Artificial Noise: An Error Performance-Based Approach
Ying Liu ,Li

10. Physical Layer Security in Wireless Cooperative Relay Networks: State of the Art and Beyond
Leonardo Jiménez Rodríguez, Nghi H. Tran, Trung Q. Duong, Tho Le-Ngoc, Maged Elkashlan, and Sachin Shetty

11. Relay Selection for Secure Cooperative Networks with Jamming
Ioannis Krikidis,, John S. Thompson,, and Steve McLaughlin

12. A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security Furqan Jameel, Shurjeel Wyne, Georges Kaddoum, Trung Q. Duong

13. COOPERATIVE COMMUNICATIONS HARDWARE, CHANNEL & PHY
Mischa Dohler, Yonghui Li

14. Cooperative Communications and Networking
K. J. Ray Liu, Ahmed Sadek, Weifeng Su, Andres Kwasinski

15. Secure Communications With Cooperative Jamming: Optimal Power Allocation and Secrecy Outage *Analysis Kanapathippillai Cumanan, George C. Alexandropoulos, Zhiguo Ding, and George K. Karagiannidis.*

16. Modeling and Characterization of Different Types of Fading *Channel*
Md. Golam Sadeque, Shadhon Chandra Mohonta, Ali Firoj.

17. High-Performance Communication Networks
Jean Walrand and Pravin Varaiya

18. Physical layer security schemes for MIMO systems: an overview *Reem Melki, Hassan N. Noura, Mohammad M. Mansour, Ali Chehab*

19. Power Allocation Strategies for MIMO Wireless system under Fading Environment

Rajat Sapra, Neeraj Varshney

20. An Overview of Key Technologies in Physical Layer Security

Abraham Sanenga , Galefang Allycan Mapunda, Tshepiso Merapelo Ludo Jacob, Leatile Marata, Bokamoso Basutli and Joseph Monamati Chuma .

21. *D. Liu, W. Hong, T. S. Rappaport, C. Luxey, and W. Hong*. What will 5g antennas and propagation be? IEEE Transactions on Antennas and Propagation, 65(12):6205–6212, Dec 2017.

22. *Y. Gao, S. Hu, W. Tang, Y. Li, Y. Sun, D. Huang,S. Cheng, and X. Li.* Physical layer security in 5g based large scale social networks: Opportunities and challenges. IEEE Access, 6:26350–26357, 2018.

23. *W. Stallings*. 'Cryptography and Network Security:Principles and Practice. Prentice Hall, New York, NY,USA, 2008.

24. *N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo*. Safeguarding 5g wireless communication networks using physical layer security. IEEE Communications Magazine, 53(4):20–27, April 2015.

25. *C. E. Shannon*. Communication theory of secrecy systems. Bell Syst. Tech. J., 28(4):656–715, October 1949.

26. *A. D. Wyner*. The wire-tap channel. Bell Syst. Tech. J., 54(8):1355–1387, October 1975.

27. *I. Csiszar and J. Korner.* Broadcast channels with confidential messages. IEEE Transactions on Information Theory, 24(3):339–348, May 1978.

28. *S. Leung-Yan-Cheong and M. Hellman*. The Gaussian wire-tap channel. IEEE Transactions on Information Theory, 24(4):451–456, July 1978.

29. *J. F. Paris.* Statistical characterization of κ−μ shadowed fading. IEEE Transactions on Vehicular Technology,63(2):518–526, 2014.

30. F. J. Lopez-Martinez, J. M. Romero-Jerez, and J. F. Paris. On the calculation of the incomplete mgf with applications to wireless communications. IEEE Transactions on Communications, 65(1):458–469, 2017.
31. *M. D. Yacoub*. The α-η-κ-μ fading model. IEEE Transactions on Antennas and Propagation, 64(8):3597–3610, 2016.
32. *A. Mathur, Y. Ai, M. R. Bhatnagar, M. Cheffena, and T. Ohtsuki*. On physical layer security of α-η-κ-μ fading channels. IEEE Communications Letters, 22(10):2168–2171, Oct 2018.
33. *W. Zeng, J. Zhang, S. Chen, K. P. Peppas, and B. Ai.* Physical layer security over fluctuating two-ray fading channels. IEEE Transactions on Vehicular Technology,67(9):8949–8953, Sep. 2018.
34. *J. D. Vega Sanchez, D. P. Moya Osorio, F. Javier LopezMartinez, M. C. Paredes Paredes, and L. UrquizaAguiar*. On the secrecy performance over N-wave with diffuse power fading channel. Mar. 2020, arXiv:2002.05206. [Online].
35. *L. Kong and G. Kaddoum*. On physical layer security over the fisher-snedecor F wiretap fading channels.IEEE Access, 6:39466–39472, 2018.
36. *L. Yang, M. O. Hasna, and I. S. Ansari*. Physical layer security for tas/mrc systems with and without co-channel interference over ημ fading channels. IEEE Transactions on Vehicular Technology, 67(12):12421–12426, Dec 2018.
37. *S. Wang, X. Xu, K. Huang, X. Ji, Y. Chen, and L. Jin*.Artificial noise aided hybrid analog-digital beamforming for secure transmission in mimo millimeter wave relay systems. IEEE Access, 7:28597–28606, 2019.
38. *S. Yan, X. Zhou, N. Yang, T. D. Abhayapala, and A. L.Swindlehurst*. Secret channel training to enhance physical layer security with a full-duplex receiver. IEEE Transactions on Information Forensics and Security,13(11):2788–2800, Nov 2018
39. *H. A. Shah and I. Koo*. A novel physical layer security scheme in ofdm-based cognitive radio networks. IEEE Access, 6:29486–29498, 2018.
40. *P. Yan, Y. Zou, and J. Zhu*. Energy-aware multiuser scheduling for physical-layer security in energyharvesting underlay cognitive radio systems. IEEE Transactions on Vehicular Technology, 67(3):2084–2096, March 2018.
41. *F. Ud Din and F. Labeau*. Multiple antenna physical layer security against passive eavesdroppers: A tutorial. In 2018 IEEE Canadian Conference on Electrical Computer Engineering (CCECE), pages 1–6, May 2018.
42. *L. Qing, H. Guangyao, and F. Xiaomei*. Physical layer security in multi-hop af relay network based on compressed sensing. IEEE Communications Letters,22(9):1882–1885, Sep. 2018.
43. *H. Boche and C. Deppe*. Secure identification under passive eavesdroppers and active jamming attacks. IEEE Transactions on Information Forensics and Security,14(2):472–485, Feb 2019.
44. *B. Bhushan and G. Sahoo*. Recent advances in attacks,technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. Wireless Pers Commun., 98(2):2037–2077, January 2018.

45. *Z. Liu, N. Li, X. Tao, S. Li, J. Xu, and B. Zhang*. Artificial-noise-aided secure communication with fullduplex active eavesdropper. In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pages 1–7, Oct 2017
46. *S. Timilsina, G. A. Aruma Baduge, and R. F. Schaefer*. Secure communication in spectrum-sharing massive mimo systems with active eavesdropping. IEEE Transactions on Cognitive Communications and Networking,4(2):390–405, June 2018.
47. *L. Li, A. P. Petropulu, and Z. Chen*. Mimo secret communications against an active eavesdropper. IEEE Transactions on Information Forensics and Security, 12(10):2387–2401, Oct 2017.
48. *K. N. Le*. Performance analysis of secure communications over dual correlated rician fading channels. IEEE Transactions on Communications, 66(12):6659–6673, Dec 2018.
49. *G. C. Alexandropoulos and K. P. Peppas*. Secrecy outage analysis over correlated composite nakagami- m/gamma fading channels. IEEE Communications Letters, 22(1):77–80, Jan 2018.
50. *K. N. Le and T. A. Tsiftsis*. Wireless security employing opportunistic relays and an adaptive encoder under outdated csi and dual-correlated nakagami- m fading. IEEE Transactions on Communications, 67(3):2405–2419, March 2019.
51. P*. K. Gopala, L. Lai, and H. El Gamal*. On the secrecy capacity of fading channels. IEEE Transactions on Information Theory, 54(10):4687–4698, Oct 2008.
52. *M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin*. Wireless information-theoretic security. IEEE Transactions on Information Theory, 54(6):2515–2534, June 2008.
53. *V. U. Prabhu and M. R. D. Rodrigues*. On wireless channels with M-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity. IEEE Transactions on Information Forensics and Security, 6(3):853–860, Sep. 2011.
54. *L. Wang.* Physical Layer Security in Wireless Cooperative Networks. Springer, Cham, Switzerland, 2018.
55. *C. R. N. Da Silva, N. Simmons, E. J. Leonardo, S. L. Cotton, and M. D. Yacoub*. Ratio of two envelopes taken from α - μ , η - μ , and κ - μ variates and some practical applications. IEEE Access, 7:54449–54463, 2019.
56. *J. D. Vega Sanchez, D. P. Moya Osorio, E. E. Benitez Olivo, H. Alves, M. C. Paredes Paredes, and L. UrquizaAguiar*. On the statistics of the ratio of nonconstrained arbitrary α - μ random variables: A general framework and applications. Transactions on Emerging Telecommunications Technologies, Dec 2019.
57. *J. M. Hamamreh, H. M. Furqan, and H. Arslan.* Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey.IEEE Communications Surveys Tutorials, 21(2):1773–1828, Secondquarter 2019.
58. *B. He, X. Zhou, and A. L. Swindlehurst*. On secrecy metrics for physical layer security over quasi-static fading channels. IEEE Transactions on Wireless Communications, 15(10):6913–6924, Oct 2016.
59. *L. Mucchi, L. Ronga, X. Zhou, K. Huang, Y. Chen, and R. Wang*. A new metric for measuring the security of an environment: The secrecy pressure. IEEE Transactions on Wireless Communications, 16(5):3416–3430,May 2017.

60. *R. Zhao, H. Lin, Y. He, D. Chen, Y. Huang, and L. Yang*. Secrecy performance of transmit antenna selection for mimo relay systems with outdated csi. IEEE Transactions on Communications, 66(2):546–559, Feb 2018.
61. *L. Kong, S. Vuppala, and G. Kaddoum*. Secrecy analysis of random mimo wireless networks over α-μ fading channels. IEEE Transactions on Vehicular Technology, 67(12):11654–11666, Dec 2018.
62. *M. E. P. Monteiro, J. L. Rebelatto, R. D. Souza, and G. Brante.* Maximum secrecy throughput of mimome fso communications with outage constraints. IEEE Transactions on Wireless Communications, 17(5):3487–3497, May 2018.
63. *X. Zhou, M. R. McKay, B. Maham, and A. Hjrungnes*. Rethinking the secrecy outage formulation: A secure transmission design perspective. IEEE Communications Letters, 15(3):302–304, March 2011.
64. *H. Alves, M. De Castro Tom, P. H. J. Nardelli, C. H. M. De Lima, and M. Latva-Aho*. Enhanced transmit antenna selection scheme for secure throughput maximization without csi at the transmitter. IEEE Access, 4:4861–4873, 2016.
65. *H. Zhao, L. Yang, G. Pan, and M. Alouini*. Secrecy outage analysis over fluctuating two-ray fading channels. Electronics Letters, 55(15):866–868, 2019.
66. *S. Yan, B. He, Y. Cong, and X. Zhou*. Covert communication with finite block length in awgn channels. In 2017 IEEE International Conference on Communications (ICC), pages 1–6, May 2017.
67. *Z. Li, P. Mu, Z. Li, H. Wang, W. Zhang, and T. Zheng*. Nonadaptive transmission for slow fading misose wiretap channel with adjustable power allocation. In GLOBECOM 2017 - 2017 IEEE Global Communications Conference, pages 1–6, Dec 2017.
68. *B. He, A. Liu, N. Yang, and V. K. N. Lau*. 1on the design of secure non-orthogonal multiple access systems. IEEE Journal on Selected Areas in Communications, 135(10):2196–2206, Oct 2017.
69. *B. He, X. Zhou, and A. L. Swindlehurst*. On secrecy metrics for physical layer security over quasi-static fading channels. IEEE Transactions on Wireless Communications, 15(10):6913–6924, Oct 2016.
70. *K. T. Phan, Y. Hong, and E. Viterbo*. Adaptive resource allocation for secure two-hop relaying communication. IEEE Transactions on Wireless Communications, 17(12):8457–8472, Dec 2018.
71. *D. P. Moya Osorio, H. Alves, and E. E. Benitez Olivo*. On the secrecy performance and power allocation in relaying networks with untrusted relay in the partial secrecy regime. IEEE Transactions on Information Forensics and Security, 15:2268–2281, 2020.
72. *A. Naeem, M. H. Rehmani, Y. Saleem, I. Rashid, and N. Crespi*. Network coding in cognitive radio networks: A comprehensive survey. IEEE Communications Surveys Tutorials, 19(3):1945–1973, thirdquarter 2017.
73. *J. M. Moualeu, W. Hamouda, and F. Takawira*. Intercept probability analysis of wireless networks in the presence of eavesdropping attack with co-channel interference. IEEE Access, 6:41490–41503, 2018.

74. *Y. Choi and D. Kim*. Optimal power and rate allocation in superposition transmission with successive noise signal sharing toward zero intercept probability. IEEE Wireless Communications Letters, 7(5):824–827, Oct 2018.
75. *F. Jameel, Z. Chang, and T. Ristaniemi*. Intercept probability analysis of wireless powered relay system in kappa-mu fading. In 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), pages 1–6, June 2018.
76. *F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong*. A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. IEEE Communications Surveys Tutorials, 21(3):2734–2771, thirdquarter 2019
77. *H. Lei, C. Gao, Y. Guo, and G. Pan*. On physical layer security over generalized gamma fading channels. IEEE Communications Letters, 19(7):1257–1260, July 2015.
78. *H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe*. Performance analysis of physical layer security over generalized-k fading channels using a mixture gamma distribution. IEEE Communications Letters, 20(2):408–411, Feb 2016.
79. *X. Liu*. Probability of strictly positive secrecy capacity of the rician-rician fading channel. IEEE Wireless Communications Letters, 2(1):50–53, February 2013.
80. *K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nalanathan, Z. Ding, and G. K. Karagiannidis*. Physicallayer security jamming: Theoretical limits and practical designs in wireless networks. IEEE Access, 5:3603–3611, December 2017.
81. *T. V. Pham, T. Hayashi, and A. T. Pham*. Artificialnoise-aided precoding design for multi-user visible light communication channels. In 2018 IEEE International Conference on Communications Workshops (ICC Workshops), pages 1–6, May 2018.
82. *S. Yan, N. Yang, I. Land, R. Malaney, and J. Yuan*. Three artificial-noise-aided secure transmission schemes in wiretap channels. IEEE Transactions on Vehicular Technology, 67(4):3669–3673, April 2018.
83. *Y. Gu, Z. Wu, Z. Yin, and X. Zhang*. The secrecy capacity optimization artificial noise: A new type of artificial noise for secure communication in mimo system. IEEE Access, 7:58353–58360, March 2019.
84. *J. D. Vega D. P. Moya Osorio and H. Alves*. Physical Layer Security for 5G and Beyond in 5G REF: The Essential 5G Reference Online. John Wiley & Sons, 2019.
85. *A. Mukherjee and A. L. Swindlehurst*. Robust beamforming for security in mimo wiretap channels with imperfect csi. IEEE Transactions on Signal Processing, 59(1):351–361, Jan 2011.
86. *T. Lv, H. Gao, and S. Yang*. Secrecy transmit beamforming for heterogeneous networks. IEEE Journal on Selected Areas in Communications, 33(6):1154–1170, June 2015.
87. *W. Zhang, J. Chen, Y. Kuo, and Y. Zhou*. Transmit beamforming for layered physical layer security. IEEE Transactions on Vehicular Technology, 68(10):9747–9760, Oct 2019.
88. *F. He, H. Man, and W. Wang*. Maximal ratio diversity combining enhanced security. IEEE Communications Letters, 15(5):509–511, May 2011.
89. *L. Dong, Z. Han, A. P. Petropulu, and H. V*. Poor. Improving wireless physical layer security via cooperating relays. IEEE Transactions on Signal Processing, 58(3):1875–1888, March 2010.

90. *M. Chraiti, A. Ghrayeb, C. Assi, and M. O. Hasna*. On the achievable secrecy diversity of cooperative networks with untrusted relays. IEEE Transactions on Communications, 66(1):39–53, Jan 2018.
91. *R. Zhao, X. Tan, D. Chen, Y. He, and Z. Ding*. Secrecy performance of untrusted relay systems with a full-duplex jamming destination. IEEE Transactions on Vehicular Technology, 67(12):11511–11524, Dec 2018.
92. *R. F. Schaefer, G. Amarasuriya, and H. V. Poor*. Physical layer security in massive mimo systems. In 2017 51st Asilomar Conference on Signals, Systems, and Computers, pages 3–8, Oct 2017.
93. *X. Wang A. Al-Dulaimi and C. Lin*. 5G Networks: Fundamental Requirements, Enabling Technologies, and Operations Management. John Wiley & Sons Inc, New Jersey, NJ, USA, 2018.
94. *J. Zhu, R. Schober, and V. K. Bhargava.* Secure transmission in multicell massive mimo systems. IEEE Transactions on Wireless Communications, 13(9):4766–4781, Sep. 2014.
95. *Y. Liu, H. Chen, and L. Wang*. Physical layer security for next generation wireless networks: Theories, technologies, and challenges. IEEE Communications Surveys Tutorials, 19(1):347–376, Firstquarter 2017.
96. *W. Wu, X. Gao, Y. Wu, and C. Xiao*. Beam domain secure transmission for massive mimo communications. IEEE Transactions on Vehicular Technology, 67(8):7113–7127, Aug 2018.
97. *X. Zhang, D. Guo, and K. Guo*. Secure performance analysis for multi-pair af relaying massive mimo systems in ricean channels. IEEE Access, 6:57708–57720, 2018.
98. *N. Nguyen, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and K. Tourki*. Secure massive mimo with the artificial noiseaided downlink training. IEEE Journal on Selected Areas in Communications, 36(4):802–816, April 2018.
99. *J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava*. Analysis and design of secure massive mimo systems in the presence of hardware impairments. IEEE Transactions on Wireless Communications, 16(3):2001–2016, March 2017.
100. *T. Yang, R. Zhang, X. Cheng, and L. Yang*. Performance analysis of secure communication in massive mimo with imperfect channel state information. In 2018 IEEE International Conference on Communications (ICC), pages 1–6, May 2018.
101. *H. Wei, D. Wang, X. Hou, Y. Zhu, and J. Zhu*. Secrecy analysis for massive mimo systems with internal eavesdroppers. In 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), pages 1–5, Sep. 2015.
102. *B. Akgun, M. Krunz, and O. Ozan Koyluoglu*. Vulnerabilities of massive mimo systems to pilot contamination attacks. IEEE Transactions on Information Forensics and Security, 14(5):1251–1263, May 2019.
103. *X. Zhou, B. Maham, and A. Hjorungnes*. Pilot contamination for active eavesdropping. IEEE Transactions on Wireless Communications, 11(3):903–907, March 2012.
104. *D. Hu, W. Zhang, L. He, and J. Wu*. Secure transmission in multi-cell multi-user massive mimo systems with an active eavesdropper. IEEE Wireless Communications Letters, 8(1):85–88, Feb 2019.

105. *D. Kudathanthirige, S. Timilsina, and G. A. Aruma Baduge*. Secure communication in relay-assisted massive mimo downlink with active pilot attacks. IEEE Transactions on Information Forensics and Security, 14(11):2819–2833, Nov 2019.
106. *F. Zhu, F. Gao, H. Lin, S. Jin, J. Zhao, and G. Qian*. Robust beamforming for physical layer security in bdma massive mimo. IEEE Journal on Selected Areas in Communications, 36(4):775–787, April 2018.
107. *R. Wu, S. Yuan, and C. Yuan*. Secure transmission against pilot contamination: A cooperative scheme with multiple antennas. In 2018 IEEE Symposium on Computers and Communications (ISCC), pages 00052–00057, June 2018.
108. *Y. Wu, C. Wen, W. Chen, S. Jin, R. Schober, and G. Caire*. Data-aided secure massive mimo transmission with active eavesdropping. In 2018 IEEE International Conference on Communications (ICC), pages 1–6, May 2018.
109. *L. D. H. Sampaio, T. Abrao, and F. R. Durand*. Game theory based resource allocation in multi-cell massive mimo ofdma networks. In 2017 IEEE Wireless Communications and Networking Conference (WCNC), pages 1–6, March 2017.
110. *T. Rappaport, R. Heath, R. Daniels, and J. Murdock*. Mimo for millimeter-wave wireless communications: Beamforming, spatial multiplexing, or both? IEEE Communications Magazine, 52(12):110–121, Dec 2014.
111. *H.-M. Wang and T.-X. Zheng*. Physical Layer Security in Random Cellular Networks. Springer, Singapore,2016.
112. *Z. Lin, X. Du, H. Chen, B. Ai, Z. Chen, and D. Wu.* Millimeter-wave propagation modeling and measurements for 5g mobile networks. IEEE Wireless Communications, 26(1):72–77, February 2019.
113. *Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao*. A survey of physical layer security techniques for 5g wireless networks and challenges ahead. IEEE Journal on Selected Areas in Communications, 36(4):679–695, April 2018.
114. *T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez*. Millimeter wave mobile communications for 5g cellular: It will work! IEEE Access, 1:335–349, 2013.
115. *S. Wang, X. Xu, K. Huang, X. Ji, Y. Chen, and L. Jin.* Artificial noise aided hybrid analog-digital beamforming for secure transmission in mimo millimeter wave relay systems. IEEE Access, 7:28597–28606, 2019.
116. *Y. Ju, H. Wang, T. Zheng, Q. Yin, and M. H. Lee.* Safeguarding millimeter wave communications against randomly located eavesdroppers. IEEE Transactions on Wireless Communications, 17(4):2675–2689, April 2018.
117. *M. E. Eltayeb and R. W. Heath*. Securing mmwave vehicular communication links with multiple transmit antennas. In 2018 IEEE International Conference on Communications Workshops (ICC Workshops), pages 1–6, May 2018.
118. *S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu*. On the physical layer security analysis of hybrid millimeter wave networks. IEEE Transactions on Communications, 66(3):1139–1152, March 2018.

119. *K. Xiao, W. Li, M. Kadoch, and C. Li*. On the secrecy capacity of 5g mmwave small cell networks. IEEE Wireless Communications, 25(4):47–51, AUGUST 2018.
120. *M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder.* 5g: A tutorial overview of standards, trials, challenges, deployment, and practice. IEEE Journal on Selected Areas in Communications, 35(6):1201–1221,June 2017.
121. *R. I. Ansari, C. Chrysostomou, S. A. Hassan,M. Guizani, S. Mumtaz, J. Rodriguez, and J. J.P. C. Rodrigues*. 5g d2d networks: Techniques, challenges, and future prospects. IEEE Systems Journal,12(4):3970–3984, Dec 2018.
122. *D. Lopez-Perez, I. Guvenc, G. de la Roche, M. Kountouris, T. Q. S. Quek, and J. Zhang.* Enhanced intercell interference coordination challenges in heterogeneous networks. IEEE Wireless Communications, 18(3):22–30, June 2011.
123. *L. Xiang, D. W. K. Ng, R. Schober, and V. W. S. Wong*. Cache-enabled physical layer security for video streaming in backhaul-limited cellular networks. IEEE Transactions on Wireless Communications, 17(2):736– 751, Feb 2018.
124. *L. Xiang, D. W. K. Ng, R. Schober, and V. W. S. Wong.* Secure video streaming in heterogeneous small cell networks with untrusted cache helpers. IEEE Transactions on Wireless Communications, 17(4):2645–2661, April 2018.
125. *Y. Zou, M. Sun, J. Zhu, and H. Guo*. Security-reliability tradeoff for distributed antenna systems in heterogeneous cellular networks. IEEE Transactions on Wireless Communications, 17(12):8444–8456, Dec 2018.
126. *W. Wang, K. C. Teh, S. Luo, and K. H. Li*. Physical layer security in heterogeneous networks with pilot attack: A stochastic geometry approach. IEEE Transactions on Communications, 66(12):6437–6449, Dec 2018.
127. *S. Wang, Y. Gao, N. Sha, G. Zhang, H. Luo, and Y. Chen.* Physical layer security in two-tier heterogeneous cellular networks over nakagami channel during uplink phase. In 2018 10th International Conference on Communication Software and Networks (ICCSN),pages 1–5, July 2018.
128. *N. Wu, X. Zhou, and M. Sun*. Secure transmission with guaranteed user satisfaction in heterogeneous networks: A two-level stackelberg game approach. IEEE Transactions on Communications, 66(6):2738–2750, June 2018.
129. *A. Babaei, A. H. Aghvami, A. Shojaeifard, and K. Wong*. Full-duplex small-cell networks: A physicallayer security perspective. IEEE Transactions on Communications, 66(7):3006–3021, July 2018.
130. *S. Yan, X. Zhou, N. Yang, T. D. Abhayapala, and A. L. Swindlehurst*. Secret channel training to enhance physical layer security with a full-duplex receiver. IEEE Transactions on Information Forensics and Security, 13(11):2788–2800, Nov 2018.
131. *J. Kim, J. Kim, J. Lee, and J. P. Choi*. Physical-layer security against smart eavesdroppers: Exploiting fullduplex receivers. IEEE Access, 6:32945–32957, 2018.
132. *Y. Luo, Z. Feng, H. Jiang, Y. Yang, Y. Huang, and J. Yao*. Game-theoretic learning approaches for secure d2d communications against full-duplex active eavesdropper. IEEE Access, 7:41324–41335, 2019.

133. *A. Babaei, A. H. Aghvami, A. Shojaeifard, and K. Wong*. Full-duplex small-cell networks: A physicallayer security perspective. IEEE Transactions on Communications, 66(7):3006–3021, July 2018.
134. *P. Anokye, R. K. Ahiadormey, C. Song, and K. Lee*. Achievable sum-rate analysis of massive mimo fullduplex wireless backhaul links in heterogeneous cellular networks. IEEE Access, 6:23456–23469, 2018.
135. *F. Tian, X. Chen, S. Liu, X. Yuan, D. Li, X. Zhang, and Z. Yang*. Secrecy rate optimization in wireless multi-hop full duplex networks. IEEE Access, 6:5695–5704, 2018.
136. *Y. Dong, A. E. Shafie, M. J. Hossain, J. Cheng, N. AlDhahir, and V. C. M. Leung*. Secure beamforming in full-duplex swipt systems with loopback self-interference cancellation. In 2018 IEEE International Conference on Communications (ICC), pages 1–6, May 2018.
137. *Z. Ding W. Liang and H. V. Poor*. , Non-Orthogonal Multiple Access (NOMA) for 5G Systems. Cambridge University Press, 2017.
138. *Y. Zhang, H. Wang, Q. Yang, and Z. Ding*. Secrecy sum rate maximization in non-orthogonal multiple access. IEEE Communications Letters, 20(5):930–933, May 2016.
139. *B. Su, Q. Ni, and B. He.* Robust transmit designs for secrecy rate constrained miso noma system. In 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), pages 1–5, Sep. 2018