Μέσος ρυθμός διακοπής απορρήτου και μέση διάρκεια διακοπής απορρήτου σε συστήματα ασύρματων επικοινωνιών με ποικιλομορφία πάνω από Nakagami-m Κανάλια εξασθένισης

Aymen Omri , *μέλος, IEEE*, και Mazen O. Hasna , *ανώτερο μέλος, IEEE*

Περίληψη - Η παρούσα εργασία παρουσιάζει μια αναλυτική μεθοδολογία για την αξιολόγηση δύο σημαντικών μετρικών ασφαλείας φυσικού επιπέδου σε κανάλια υποκλοπής. Συγκεκριμένα, εισάγουμε πρώτα την έννοια και την έκφραση του μέσου ρυθμού εξάντλησης μυστικότητας (ASOR) για να ποσοτικοποιήσουμε το μέσο ρυθμό διέλευσης του επιπέδου μυστικότητας σε ένα προκαθορισμένο επίπεδο κατωφλίου μυστικότητας. Στη συνέχεια, εξάγουμε την έκφραση μιας νέας μετρικής, δηλαδή της μέσης διάρκειας διακοπής απορρήτου (ASOD), η οποία είναι ένα μέτρο (σε δευτερόλεπτα) που περιγράφει πόσο καιρό κατά μέσο όρο το σύστημα παραμένει σε κατάσταση διακοπής απορρήτου. Τα αποτελέσματα είναι αρκετά γενικά και αφορούν συστήματα βασισμένα στην ποικιλομορφία που λειτουργούν σε ανεξάρτητα και πανομοιότυπα κατανεμημένα (i.i.d.) κανάλια εξασθένισης Nakagami- m. Πραγματοποιούνται προσομοιώσεις Monte Carlo για την επιβεβαίωση και τη συζήτηση των αναλυτικών αποτελεσμάτων. Τα αποτελέσματα αυτά δείχνουν ότι το ASOR και το ASOD επηρεάζονται ουσιαστικά από την τάξη ποικιλομορφίας και τη μέγιστη μετατόπιση συχνότητας Doppler. Ειδικότερα, και σε αντίθεση με το ASOD, το ASOR έχει μια μέγιστη τιμή που θα πρέπει να λαμβάνεται υπόψη κατά το σχεδιασμό συστημάτων που είναι ευαίσθητα σε πτώση του επιπέδου μυστικότητας, ακόμη και για μικρές χρονικές περιόδους. Επιπλέον, η προτεινόμενη νέα μετρική ASOD μπορεί να έχει μεγάλες τιμές ακόμη και αν η χρησιμοποιούμενη σήμερα μετρική της μέσης διάρκειας εξασθένισης παρουσιάζει χαμηλές τιμές στην υπό εξέταση ζεύξη επικοινωνίας.

Όροι *ευρετηρίου*- Μέση διάρκεια διακοπής απορρήτου, μέσος ρυθμός διακοπής απορρήτου, συνδυασμός μέγιστου λόγου, κανάλια εξασθένισης nakagami-m, κανάλια καλωδιώσεων.

I. Εισαγωγή

Οι ασύρματες επικοινωνίες έχουν καταστεί απαραίτητες για την παροχή κινητής και ευρυζωνικής μεταφοράς δεδομένων. Ωστόσο, η φύση της εκπομπής των ραδιοκυμάτων επιτρέπει στους υποκλοπέους να κρυφακούσουν τα μεταδιδόμενα σήματα που μπορεί να περιλαμβάνουν εξαιρετικά ευαίσθητες και προσωπικές πληροφορίες [1]-[4]. Για το λόγο αυτό, τα θέματα ασφάλειας και ιδιωτικότητας στα ασύρματα δίκτυα επικοινωνίας έχουν λάβει ιδιαίτερη προσοχή [3]-[8]. Παραδοσιακά, η ασφάλεια των ασύρματων επικοινωνιών χρησιμοποιεί κρυπτογραφικές μεθόδους που εκτελούνται στα ανώτερα στρώματα

Το χειρόγραφο παραλήφθηκε στις 15 Μαΐου 2017, αναθεωρημένο στις 3 Οκτωβρίου 2017,
24 Δεκεμβρίου 2017 και 19 Φεβρουαρίου 2018, αποδεκτή 6 Μαρτίου 2018. Ημερομηνία δημοσίευσης 16 Απριλίου 2018, ημερομηνία τρέχουσας έκδοσης 8 Ιουνίου 2018. Η παρούσα δημοσίευση κατέστη δυνατή χάρη στη συμφωνία χορηγίας για την υποστήριξη της έρευνας και της συνεργασίας από την Ooredoo, Ντόχα, Κατάρ. Οι δηλώσεις που διατυπώνονται στο παρόν αποτελούν αποκλειστική ευθύνη των συγγραφέων. Ο συνεργάτης συντάκτης που συντόνισε την αξιολόγηση της παρούσας εργασίας και ενέκρινε τη δημοσίευσή της ήταν ο
J. Park. *(Συγγραφέας: Aymen Omri.)*

Οι συγγραφείς εργάζονται στο Τμήμα Ηλεκτρολόγων Μηχανικών του Πανεπιστημίου του Κατάρ, Ντόχα, Κατάρ (e-mail: eaymenomri@gmail.com).

Έγχρωμες εκδόσεις ενός ή περισσοτέρων από τα σχήματα της παρούσας δημοσίευσης είναι διαθέσιμες στο διαδίκτυο στη διεύθυνση http://ieeexplore.ieee.org.
Αναγνωριστικό ψηφιακού αντικειμένου 10.1109/TWC.2018.2816648

των συστημάτων επικοινωνίας [5]-[7]. Αυτές οι μέθοδοι βασίζονται κυρίως στη δημιουργία, ανταλλαγή και χρήση κρυπτογραφικών κλειδιών. Ωστόσο, ο διαμοιρασμός των μυστικών κλειδιών μεταξύ των εξουσιοδοτημένων χρηστών αποτελεί μεγάλη πρόκληση όσον αφορά τη διανομή και τη διαχείριση των κλειδιών [4], [8]. Επιπλέον, η ραγδαία πρόοδος στην υπολογιστική ισχύ και τους πόρους καθιστά εφικτή την αποκωδικοποίηση των κρυπτογραφημένων ασύρματων σημάτων από τους υποκλοπείς [2]. Ως αποτέλεσμα, απαιτούνται νέοι αποδοτικοί ασύρματοι μηχανισμοί ασφάλειας που δεν βασίζονται στα βαρύτατα και απαιτητικά σε συντονισμό κρυπτογραφικά πρωτόκολλα.

Πρόσφατα, η ασφάλεια σε φυσικό επίπεδο έχει προταθεί ως μια πολλά υποσχόμενη εναλλακτική λύση (ή τουλάχιστον ως συμπλήρωμα) για την προστασία από κακόβουλους υποκλοπέα χωρίς ενδεχομένως την ανάγκη κρυπτογραφικών μεθόδων [3], [4], [8]. Κατ' αρχήν, είναι σε θέση να διασφαλίσει τις επικοινωνίες ακόμη και παρουσία υποκλοπέων με απεριόριστη υπολογιστική ικανότητα [9], [10]. Η ενδιαφέρουσα ιδέα είναι η αξιοποίηση των χαρακτηριστικών του φυσικού επιπέδου για τη βελτίωση της ασφάλειας και της αξιοπιστίας του καναλιού επικοινωνίας. Μια προσέγγιση για την ικανοποίηση τέτοιων απαιτήσεων προτάθηκε για πρώτη φορά από τον Wyner [9], ο οποίος έθεσε τα θεμέλια της θεωρητικής ασφάλειας της πληροφορίας, όπου εισήγαγε την έννοια ενός διακριτού καναλιού χωρίς μνήμη και ανέλυσε την εγγενή ικανότητα του επιτεύξιμου ρυθμού απορρήτου. Υπό το πρίσμα αυτό, έχει διεξαχθεί σημαντικός αριθμός ερευνών σχετικά με το θέμα της βελτίωσης της ασφάλειας του φυσικού στρώματος στις ασύρματες επικοινωνίες. Στο [11], τα αποτελέσματα του Wyner για διακριτά κανάλια καλωδιακής αναπαραγωγής χωρίς μνήμη επεκτάθηκαν στο Gaussian κανάλι καλωδιακής αναπαραγωγής, όπου οι συγγραφείς έδειξαν ότι η χωρητικότητα απορρήτου είναι η διαφορά μεταξύ των χωρητικοτήτων του κύριου καναλιού και του καναλιού καλωδιακής αναπαραγωγής. Για να ενισχυθεί περαιτέρω η ασφάλεια των επικοινωνιών, έχουν προταθεί κοινές συνεργατικές τεχνικές διαμόρφωσης δέσμης και παρεμβολής στα [1], [12] και [13]. Στα [14]-[16], παρουσιάστηκε και αξιολογήθηκε η ασφάλεια φυσικού επιπέδου με τεχνητό θόρυβο. Η ασφάλεια φυσικού στρώματος για διαφορετικά συνεργατικά σχήματα έχει μελετηθεί και διερευνηθεί στα [17]-[22], όπου οι συγγραφείς επιβεβαίωσαν ότι η συνεργασία μπορεί να βελτιώσει σημαντικά την ασφάλεια. Στο [23], οι συγγραφείς πρότειναν ελαχιστοποίηση της ισχύος και μεγιστοποίηση του ρυθμού μυστικότητας για ένα κανάλι μυστικότητας MIMO παρουσία ενός υποκλοπέα πολλαπλών κεραιών.

Η ανάλυση των επιδόσεων αυτών των προτεινόμενων συστημάτων και τεχνικών που έχουν εμφανιστεί μέχρι στιγμής στη βιβλιογραφία έχει επικεντρωθεί κυρίως σε στατιστικά στοιχεία πρώτης τάξης, ιδίως στη μυστικότητα

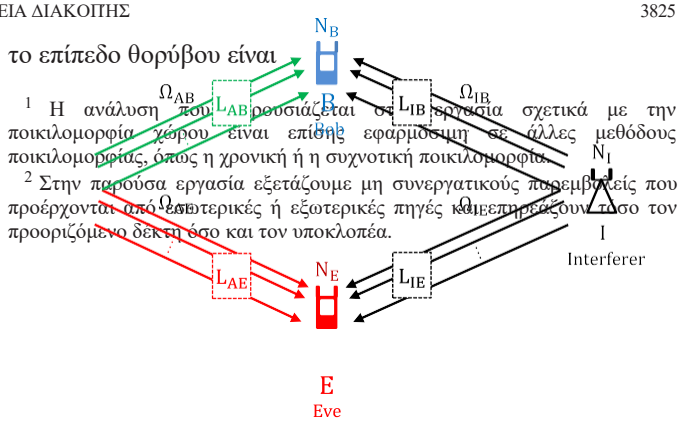
χωρητικότητα και/ή την πιθανότητα διακοπής της μυστικότητας, τα οποία είναι παραδοσιακά τα πιο συχνά χρησιμοποιούμενα μέτρα ασφαλείας για κανάλια υποκλοπής [1], [9], [23], [24]. Για να κατανοήσουμε πλήρως την απόδοση τέτοιων συστημάτων, χρειαζόμαστε μέτρα δεύτερης τάξης για να έχουμε εικόνα της δυναμικής της απόδοσης αυτής. Για παράδειγμα, η πιθανότητα απώλειας μυστικότητας παρέχει μια ιδέα για το κλάσμα των υλοποιήσεων εξασθένισης για τις οποίες το κανάλι μπορεί να υποστηρίξει έναν συγκεκριμένο ρυθμό. Ωστόσο, αποτυγχάνει να δώσει μια ιδέα για το μέσο μήκος (ως προς τις υλοποιήσεις) για το οποίο το κανάλι δεν μπορεί να υποστηρίξει ασφαλή επικοινωνία. Η κινητικότητα είναι μια άλλη διάσταση στην οποία υπεισέρχεται η στατιστική δεύτερης τάξης. Σε ένα σενάριο όπου οι πομποί, οι δέκτες και οι υποκλοπείς κινούνται, μπορεί να χρειαστεί να ελέγξουμε ποια ταχύτητα οδηγεί σε ποια μέση διάρκεια διακοπής απορρήτου, και ως εκ τούτου το σύστημα μπορεί να σχεδιάσει συγκεκριμένα μέτρα για τη μετεγκατάσταση ή την αλλαγή της ταχύτητας των συστατικών του, όποτε αυτό είναι εφικτό. Επιπλέον, και πρόσφατα στο [25], υπάρχει ενδιαφέρον για τη σύζευξη της ασφάλειας φυσικού επιπέδου και της παραγωγής μυστικών κλειδιών, όπου χρησιμοποιούνται διαστήματα καλής απόδοσης μυστικότητας για την ανταλλαγή τέτοιων κλειδιών, ώστε να μπορούν να χρησιμοποιηθούν στην υπόλοιπη μετάδοση. Η μέση διάρκεια διακοπής της μυστικότητας θα διαδραματίσει σημαντικό ρόλο σε τέτοια σενάρια. Γενικά, όποτε έχουμε προσαρμοστικά συστήματα μετάδοσης και δυναμική ανάπτυξη συστημάτων, τα μέτρα του μέσου ρυθμού διακοπής μυστικότητας (ASOR) [ή του μέσου ρυθμού διέλευσης επιπέδου μυστικότητας (ASLCR)] και της μέσης διάρκειας διακοπής μυστικότητας (ASOD) μπορούν να βοηθήσουν ουσιαστικά τόσο στο σχεδιασμό όσο και στην ανάπτυξη του συστήματος, όταν η ασφάλεια αποτελεί πρόβλημα.

Εξ όσων γνωρίζουμε, λίγες δημοσιευμένες αναλυτικές εργασίες έχουν δώσει προσοχή στην επίδραση των στατιστικών στοιχείων εξασθένισης των επιθυμητών και των παρεμβαλλόμενων χρηστών στο μέσο ρυθμό διακοπής και στη διάρκεια διακοπής του συστήματος [26]-[30]. Επιπλέον, οι προηγούμενες εργασίες σχετικά με τα στατιστικά στοιχεία δεύτερης τάξης επικεντρώθηκαν κυρίως στην επίδραση της εξασθένισης και της παρεμβολής, χωρίς να ασχοληθούν με την πλευρά του προβλήματος της ασφάλειας του φυσικού στρώματος. Για παράδειγμα, οι εργασίες αυτές βοήθησαν στην καλύτερη κατανόηση των εκρήξεων σφαλμάτων [31], [32] και στο σχεδιασμό του μεγέθους του interleaver και της κωδικοποιημένης διαμόρφωσης [33]. Ωστόσο, όταν ενδιαφέρει το μέτρο της χωρητικότητας απορρήτου και όχι μόνο τα κύρια μέτρα εξασθένισης του καναλιού, μπαίνουν στο παιχνίδι οι προτεινόμενες μετρικές μας. Πράγματι, δεν υπάρχει ακόμη στη βιβλιογραφία δημοσιευμένη αναλυτική εργασία για το ASOR, και το ASOD των γενικών ασύρματων συστημάτων επικοινωνίας που βασίζονται σε συνδυασμό μέγιστου λόγου (MRC) πάνω σε κανάλια εξασθένισης Nakagami-m.

Υπό το πρίσμα των προαναφερθέντων σχετικών εργασιών, οι κύριες συνεισφορές μας μπορούν να συνοψιστούν ως εξής:

- Εισάγουμε την έννοια του ASOR για να ποσοτικοποιήσουμε το μέσο ποσοστό διέλευσης του επιπέδου μυστικότητας σε ένα προκαθορισμένο επίπεδο κατωφλίου μυστικότητας και εξάγουμε τις αναλυτικές εκφράσεις του για συστήματα περιορισμένου θορύβου και περιορισμένης παρεμβολής.
- Για τη μέτρηση της μέσης χρονικής περιόδου, κατά την οποία το σύστημα παραμένει σε κατάσταση διακοπής της μυστικότητας, εισάγουμε την έννοια της ASOD. Στη συνέχεια, με βάση τις παραγόμενες εκφράσεις της πιθανότητας διακοπής της μυστικότητας (SOP) και της ASOR, παρουσιάζουμε τις εκφράσεις της ASOD για τα δύο γενικά συστήματα που εξετάζουμε.

Το υπόλοιπο της παρούσας εργασίας οργανώνεται ως εξής: Στην Ενότητα II, περιγράφονται τα μοντέλα του συστήματος και του καναλιού. Οι εκφράσεις των SOP, ASOR και ASOD περιγράφονται λεπτομερώς και εξάγονται στην ενότητα



Σχήμα 1. Το μοντέλο του συστήματος.

Τμήμα III. Στην Ενότητα IV, παρουσιάζονται αποτελέσματα προσομοίωσης Monte Carlo για την αξιολόγηση της ακρίβειας των παραγόμενων εκφράσεων και για τη διερεύνηση των μεταβολών των προτεινόμενων μετρικών ασφαλείας. Τέλος, στην ενότητα V διατυπώνονται συμπεράσματα.

II. Μοντελα Συστηματος και Καναλιού

Θεωρούμε ένα ασύρματο σύστημα επικοινωνίας, στο οποίο μια πηγή (Alice) σκοπεύει να στείλει πληροφορίες σε έναν νόμιμο προορισμό (Bob), παρουσία ενός παθητικού υποκλοπέα (Eve) και μιας πηγής παρεμβολής, όπως παρουσιάζεται στο Σχήμα 1. Υποθέτουμε ότι όλοι οι κόμβοι είναι εξοπλισμένοι με πολλαπλές κεραίες, όπου $_{NA}$, $_{NB}$, $_{NE}$ και $_{NI}$ υποδηλώνουν τον αριθμό των κεραιών της Alice, του Bob, της Eve και του παρεμποδιστή, αντίστοιχα. Υποθέτουμε ότι τα κανάλια μεταξύ των διαφόρων κεραιών δεν συσχετίζονται. Κατά συνέπεια, το επιθυμητό σήμα λαμβάνεται στον Bob (Eve) μέσω $_{LAB}$ ($_{LAE}$) ανεξάρτητων και πανομοιότυπα κατανεμημένων (i.i.d.) μονοπατιών ποικιλομορφίας,[1] με την ίδια μέση ισχύ εξασθένισης $_{ΩAB}$ ($_{ΩAE}$), όπου $_{LAB}$ = $_{NA}$ $_{NB}$, και $_{LAE}$ = $_{NA}$ $_{NE}$. Επιπλέον, το σήμα παρεμβολής λαμβάνεται στον Bob (Eve) πάνω σε $_{LIB}$ ($_{LIE}$) ανεξάρτητες και πανομοιότυπα κατανεμημένες (i.i.d.) διαδρομές ποικιλομορφίας, με την ίδια μέση ισχύ εξασθένισης $_{ΩIB}$ ($_{ΩIE}$), όπου $_{LIB}$ = $_{NINB}$, και $_{LIE}$ = $_{NINE}$. Για τους διαφορετικούς κόμβους, υποθέτουμε επίσης ότι όλα τα μονοπάτια ποικιλομορφίας υπόκεινται σε επίπεδη εξασθένιση Nakagami με παράμετρο m. Για την εκμετάλλευση των μονοπατιών ποικιλομορφίας και την παροχή βελτίωσης της ασύρματης σύνδεσης, χρησιμοποιείται ένας δέκτης MRC στον Bob και στην Eve για να συνδυάσει τα λαμβανόμενα σήματα.

Στην παρούσα εργασία, εξετάζουμε δύο είδη συστημάτων, δηλαδή: συστήματα περιορισμένου θορύβου και συστήματα περιορισμένης παρεμβολής. Στα συστήματα περιορισμένου θορύβου, η απόδοση επηρεάζεται κυρίως από το επίπεδο θορύβου που προέρχεται από διάφορα μέρη του συστήματος καθώς και από το υπόβαθρο και η κύρια παράμετρος που πρέπει να εξεταστεί είναι ο λόγος σήματος προς θόρυβο (SNR), όπου η επίδραση των σημάτων παρεμβολής αγνοείται είτε επειδή το σύστημα δεν επηρεάζεται από παρεμβολές, π.χ. με τη χρήση ορθογώνιων συχνοτήτων, είτε επειδή χρησιμοποιούνται τέλεια σχήματα ακύρωσης παρεμβολών. Για συστήματα περιορισμένης παρεμβολής, η απόδοση υποφέρει κυρίως από τις πηγές παρεμβολής,[2] και το επίπεδο θορύβου είναι

[1] Η ανάλυση που παρουσιάζεται σε αυτή την εργασία σχετικά με την ποικιλομορφία χώρου είναι επίσης εφαρμόσιμη σε άλλες μεθόδους ποικιλομορφίας, όπως η χρονική ή η συχνοτική ποικιλομορφία.

[2] Στην παρούσα εργασία εξετάζουμε μη συνεργατικούς παρεμβολείς που προέρχονται από εσωτερικές ή εξωτερικές πηγές και επηρεάζουν τόσο τον προοριζόμενο δέκτη όσο και τον υποκλοπέα.

θεωρείται αμελητέα σε σύγκριση με εκείνη της παρεμβολής. η κύρια παράμετρος που πρέπει να ληφθεί υπόψη εδώ είναι ο λόγος σήματος προς παρεμβολή (SIR).

Για ένα σύστημα περιορισμένου θορύβου, τα SNR στον Η Eve ($_{\gamma E}$) με λήψη MRC μπορεί να γραφεί ως εξής

$$\gamma_B = \frac{\alpha_{AB}^2}{N_0} = \frac{\sum_{l=1}^{L_{AB}} \alpha_{AB,l}^2}{N_0}, \quad (1)$$

και,

$$\gamma_E = \frac{\alpha_{AE}^2}{N_0} = \frac{\sum_{l'=1}^{L_{AE}} \alpha_{AE,l'}^2}{N_0}, \quad (2)$$

αντίστοιχα, όπου, α^2 (α_{AB}^2) είναι το συνολικό λαμβανόμενο επιθυμητό ισχύς σήματος στον Bob (Eve), α^2 ($\alpha_{AE,l'}^2$) είναι το λαμβανόμενο επιθυμητό l^{th} l'^{th} η ισχύς του σήματος στον Bob (Eve) στο μονοπάτι (l') ποικιλομορφίας και N_0 η ισχύς του προσθετικού λευκού γκαουσιανού θορύβου (AWGN).

Για ένα σύστημα περιορισμένης παρεμβολής, το SIR στον Bob ($_{\lambda B}$) και στην Εύα ($_{\lambda E}$) μπορεί να γραφεί ως εξής

$$\lambda_B = \frac{\alpha_{AB}^2}{\alpha_{IB}^2} = \frac{\sum_{l=1}^{L_{AB}} \alpha_{AB,l}^2}{\sum_{n=1}^{L_{IB}} \alpha_{IB,n}^2}, \quad (3)$$

και,

$$\lambda_E = \frac{\alpha_{AE}^2}{\alpha_{IE}^2} = \frac{\sum_{l'=1}^{L_{AE}} \alpha_{AE,l'}^2}{\sum_{n'=1}^{L_{IE}} \alpha_{IE,n'}^2}, \quad (4)$$

αντίστοιχα, όπου α^2 (α_{IB}^2) είναι η συνολική λαμβανόμενη παρεμβολή η ισχύς του σήματος στον Bob (Eve), και $\alpha_{IB,n}^2$ ($\alpha_{IE,n'}^2$) είναι η n^{th} (n'^{th}) λαμβανόμενη ισχύς του σήματος παρεμβολής στον Bob (Eve) από την κεραία

Επιπλέον, το τετράγωνο μιας τυχαίας μεταβλητής είναι μια τυχαία μεταβλητή Γάμμα και το άθροισμα ανεξάρτητων τυχαίων μεταβλητών Γάμμα, με την ίδια παράμετρο κλιμάκωσης, είναι μια τυχαία μεταβλητή Γάμμα [26], επομένως α^2, $\forall \chi \in \{AB, AE, IB, IE\}$ είναι μια τυχαία μεταβλητή Γάμμα με τη γενική έκφραση της συνάρτησης πυκνότητας πιθανότητας (PDF) να δίνεται από [26]

$$p_{\alpha_\chi^2}(v) = \left(\frac{m}{\Omega_\chi}\right)^{mL_\chi} \frac{v^{mL_\chi - 1}}{\Gamma(mL_\chi)} \exp\left(-\frac{m}{\Omega_\chi} v\right). \quad (5)$$

Ηανεξάρτητη από το πλάτος του σήματος, και η έκφραση PDF του $_{\chi}$ δίνεται από [26]

$$p_{\alpha_\chi}(\alpha_\chi) = \frac{1}{\sqrt{2\pi\sigma_\chi}} \exp\left(-\frac{\alpha_\chi^2}{2\sigma_\chi^2}\right), \quad (7)$$

όπου, $\sigma_\chi^2 = \pi^2 f^2 (\Omega_\chi / m)$, και f_{max} είναι το μέγιστο Doppler μετατοπίσεις συχνότητας.

III. Ανάλυση Επιδόσεων

Σε αυτή την ενότητα, εξάγουμε τις εκφράσεις των SOP, ASOR και ASOD τόσο για περιορισμένο θόρυβο όσο και για περιορισμένη παρεμβολή. συστήματα.

A. Ικανότητα απορρήτου (SC)

Για τα γενικά συστήματα ασύρματης επικοινωνίας, η μυστικότητα χωρητικότητα ορίζεται ως το μέγιστο μεταξύ του μηδενός και του

τιμή της διαφοράς μεταξύ των ικανοτήτων των κύριων και των καναλιών υποκλοπής [34]-[36], η οποία μπορεί να εκφραστεί ως εξής

$$SC = \begin{cases} {}_{fCB} - {}_{CE}, & \text{εάν } ({}_{CB} > {}_{CE}) \\ 0, & \text{αλλιώς,} \end{cases} \quad (8)$$

όπου, $_{CB}$ και $_{CE}$ είναι οι στιγμιαίες χωρητικότητες στον στην Εύα, αντίστοιχα.

B. Πιθανότητα διακοπής της μυστικότητας (SOP)

Ως διακοπή απορρήτου μπορεί να οριστεί το γεγονός κατά το οποίο η η στιγμιαία ικανότητα απορρήτου (SC) είναι ίση με ένα προκαθορισμένο όριο (ξ)$_{th}$ ή πέφτει κάτω από αυτό, δηλαδή ($SC \le \xi$) [34], όπου ξ_{th} ορίζεται ως το όριο χωρητικότητας στο οποίο ή κάτω από το οποίο δεν μπορεί να επιτευχθεί ασφαλής επικοινωνία. Κατά συνέπεια, η πιθανότητα διακοπής της μυστικότητας για τα δύο εξεταζόμενα συστήματα προκύπτει ως εξής:

1) Συστήματα περιορισμένου θορύβου: Για ένα σύστημα περιορισμένου θορύβου, η πιθανότητα διακοπής της μυστικότητας ορίζεται ως εξής [34]

$$P_{out}^{(N)}(\xi_{th}) = \mathrm{P}\, SC \le \xi_{th}. \quad (9)$$

Με βάση τα (8) και (9), η έκφραση του $_{Pout}^{(N)}(\xi_{th})$ μπορεί να επαναδιατυπωθεί ως εξής

$$P_{out}^{(N)}(\xi_{th}) = P\{C \le (C + \xi_{th})\}$$

$$= P\left\{\log_2(1+\gamma_B) - \log_2(1+\gamma_E) \le \xi_{th}\right\}$$

$$= P\{\gamma \le 2^{\xi_{th}}(1+\gamma) - 1\}$$

Με βάση την έκφραση PDF του p_{α} 2 , η γενική έκφραση PDF του στιγμιαίου πλάτους εξασθένισης α_{χ} εκφράζεται ως εξής [26].

$$p_{\alpha_{\chi}}(\alpha_{\chi}) = \left(\frac{m}{\Omega_{\chi}}\right)^{mL_{\chi}} 2\,\frac{\alpha_{2mL_{\chi}-1}}{\Gamma(mL_{\chi})} \exp\left\{-\frac{m}{\Omega_{\chi}}\alpha^{2}\right\}. \quad (6)$$

Για το μοντέλο καναλιού Nakagami-m, η χρονική της διαδικασίας πλάτους του σήματος, που , είναι

$$= \int_{0}^{\infty}\int_{0}^{2^{\xi}\text{th}\,(1+y)-1} p_{\gamma_B}(x)\,p_{\gamma_E}(y)\,dx\,\mathrm{d}y, \quad (10)$$

όπου, $p_{\gamma B}$ και $p_{\gamma E}$ είναι οι PDF του $_{\gamma B}$ και $_{\gamma E}$, αντίστοιχα. Με βάση τις (1), (2) και (5), οι αντίστοιχες εκφράσεις PDF δίνονται από

$$p_{\gamma B}(\gamma_{B}) = \left(\frac{m}{\omega_{B}}\right)_{\text{mLAB}\,\gamma\text{mLAB}-1} \exp\left\{\frac{m}{\omega_{B}}\right\}$$

$$\frac{B}{\qquad} - \gamma_{B}, \quad (11)$$

και,

$$p_{\gamma_E}(\gamma) = \frac{\left(\frac{m}{\omega_E}\right)^{m_{LAE}\gamma m_{LAE}-1}}{\Gamma(m_{LAE})} \exp\left(-\frac{m}{\omega_E}\gamma_E\right), \quad (12)$$

όπου, $\omega_B = \Omega_{AB}/N_0$, και $\omega_E = \Omega_{AE}/N_0$. Με βάση την (10-12), η τελική ακριβής έκφραση κλειστής μορφής του $P_{out}^{(N)}(\xi_{th})$ στο Παράρτημα Α και δίνεται από την (13), η οποία φαίνεται στο πάνω μέρος του
επόμενη σελίδα.

Για την ειδική περίπτωση ($\xi_{th} = 0$), που είναι η περίπτωση της
έχοντας διακοπή με την έννοια της αυστηρά θετικής ικανότητας απορρήτου, η έκφραση του $P_{out}^{(N)}(0)$ μπορεί να

$$P_{out}^{(N)}(0) = 1 - \sum_{k=0}^{m_{LAB}-1} \frac{\left(\frac{\omega_B}{\omega_E}\right)^{k+1-m_{LAB}} \binom{m_{LAB}+m_{LAE}-2-k}{m_{LAB}-k-1}}{\left[1+\frac{\omega_E}{\omega_B}\right]^{m_{LAE}-1-k}} \cdot L \quad (14)$$

Συνεχίζοντας με αυτή την ειδική περίπτωση και υποθέτοντας περαιτέρω ότι
($m = m_{LAB} = m_{LAE} = 1$), το οποίο αναφέρεται στην περίπτωση όπου όλα τα κανάλια υποφέρουν από εξασθένιση Rayleigh και όλοι οι κόμβοι είναι εξοπλισμένοι με μία μόνο κεραία, το $P_{out}^{(N)}(0)$ μειώνεται σε

$$P_{out}^{(N)}(0) = \frac{\omega_E}{\omega_B + \omega_E}, \quad (15)$$

η οποία συμφωνεί με την παράγωγη έκφραση στο [34]. Από αυτή την εξίσωση, μπορούμε να παρατηρήσουμε ότι η πιθανότητα διακοπής της μυστικότητας αυξάνεται με το ω_E και είναι αντιστρόφως ανάλογη του ω_B. Επιπλέον, για μεγάλες τιμές του ω_E ($>> \omega_B$), η πιθανότητα αυτή συγκλίνει στη μονάδα, πράγμα αναμενόμενο.

2) Συστήματα περιορισμένης παρεμβολής: Για ένα σύστημα περιορισμένης παρεμβολής και με βάση τις (3), (4) και (9), η έκφραση της πιθανότητας διακοπής της μυστικότητας γράφεται ως εξής

$$P_{out}^{(I)}(\xi_{th}) = P\left[\log_2(1+\lambda_B) - \log_2(1+\lambda_E) \le \xi_{th}\right]$$

$$= P\left[\alpha_{AB}^2 \le \alpha_{IB}^2 (2^{\xi_{th}}(1+\gamma_E) - 1)\right]$$

$$= \int_0^{\infty}\int_0^{\infty}\int_0^{y[2^{\xi_{th}}(1+v)-1]} p_{\alpha_{AB}}(x)\, p_{\alpha_{IB}^2}(y)\, p_{\lambda_E}(v)\, dx\, dy\, dv, \quad (16)$$

όπου, $p_{\alpha_{AB}^2}$ και $p_{\alpha_{IB}^2}$ είναι οι PDF του α_{AB}^2 και α_{IB}^2 τικά, και p_{λ_E} είναι η PDF του λ_E. Καθώς ο λόγος δύο ανεξάρτητων τυχαίων μεταβλητών Γάμμα είναι μια τυχαία μεταβλητή Βήτα [37], και με βάση την (5), η PDF του λ_E εκφράζεται ως εξής

$$p_{\lambda_E}(\lambda) = \frac{\left(\frac{\lambda_E}{\Omega_E}\right)^{m_{LAE}-1}\left(1+\frac{\lambda_E}{\Omega_E}\right)^{-m_{LAE}-m_{LIE}}}{B(m_{LAE}, m_{LIE})}, \quad (17)$$

Για την ειδική περίπτωση ($\xi_{th} = 0$), η έκφραση του $P_{out}^{(I)}(0)$ δίνεται από τη σχέση

$$P_{out}^{(I)}(0) = 1 - \frac{\Omega_B^{m_{LAB}}\Omega_E^{-m_{LAE}}}{B(m_{LAE}, m_{LIE})} \sum_{k=0}^{m_{LLAB}-1} \binom{\rho_B-2-k}{m_{LIB}-1} \times B\left(m_{LAB}+m_{LAE}-1-k, m_{LIB}+m_{LIE}\right) \times {}_2F_1\left(\rho_E, mL_{AE}+mL_{IE}-1; \rho+\rho-1-k; \frac{1-\frac{\Omega_B}{\Omega_E}}{}\right), \quad (19)$$

η οποία απλοποιείται περαιτέρω στην περίπτωση μίας κεραίας Rayleigh
(δηλ. $m = m_{AB} = m_{AE} = m_{IB} = m_{IE} = 1$) σε

$$P_{out}^{(I)}(0) = 1 - \frac{\Omega_B}{\Omega_E} {}_2F_1\left(2, 1, 3, 1-\frac{\Omega_B}{\Omega_E}\right). \quad (20)$$

Παρόμοια με την (15), είναι σαφές ότι η πιθανότητα διακοπής της μυστικότητας, στην περίπτωση συστημάτων περιορισμένης παρεμβολής με αυτές τις συγκεκριμένες παραμέτρους, είναι ανάλογη του Ω_E και αντιστρόφως ανάλογη του Ω_B.

C. Μέσο ποσοστό διακοπής απορρήτου (ASOR)

Ο μέσος ρυθμός διακοπής απορρήτου ορίζεται ως ο μέσος ρυθμός διέλευσης του επιπέδου απορρήτου της στιγμιαίας χωρητικότητας απορρήτου SC στο επίπεδο ξ_{th}, δηλαδή, ποσοτικοποιεί τον αναμενόμενο αριθμό διελεύσεων προς τα κάτω ανά δευτερόλεπτο της χωρητικότητας απορρήτου, η οποία είναι μεταβλητή στο χρόνο. σε ένα επίπεδο κατωφλίου ξ_{th}. Η ASOR για τα δύο εξεταζόμενα συστήματα προκύπτει ως εξής:

1) Συστήματα περιορισμένου θορύβου: Για ένα σύστημα περιορισμένου θορύβου, και με βάση τον ορισμό του SC, η περίπτωση ($SC \le \xi_{th}$) είναι ισοδύναμο με το γεγονός της υπαρξης $r = \sqrt{N_0}\left[2^{\xi_{th}}(1+\gamma_E) - 1\right]$. Κατά συνέπεια, η ASOR, που συμβολίζεται ως $R^{(N)}(\xi_{th})$, είναι ισοδύναμη με το ρυθμό με τον οποίο η προς τα κάτω το επίπεδο r ($= \sqrt{2^{\xi_{th}}(1+\gamma_E) - 1}$). Με βάση το τον γενικό τύπο που παρατίθεται στο [39], η ASOR μπορεί να ως

$$R^{(N)}(\xi_{th}) = \int_0^{\infty}\int_0^{\infty} \dot{r}\, p_r(r)\, p_{\dot{r}}(\dot{r})\, p_{\gamma_E}(y)\, d\dot{r}\, dy, \quad (21)$$

όπου, p_r και $p_{\dot{r}}$ είναι οι PDF των r και $\dot{r}$, αντίστοιχα. Με βάση τις (6) και (7), οι εκφράσεις αυτών των PDF δίνονται ως εξής από

$$p_{\lambda_E}(r) = \frac{\Omega_E^{m}\, B(mL_{AE}, mL_{IE})}{\Gamma(m)}\, r^{m}\exp\left(-\omega^{m} r^2\right), \quad (22)$$

$$\left(\quad\right)^{m}\ 2\ ^{2m-1}\qquad\{\qquad\}$$

όπου, $_{\Omega E}$ = $\frac{\Omega_{AE}}{\Omega_{IE}}$, και B είναι η συνάρτηση Beta [38, εξίσωση 8.380-

1]. Η τελική έκφραση ακριβούς μορφής του $^{(I)}_{P_{out}}(\xi_{th})$ προκύπτει στο Παράρτημα Β και δίνεται από την (18), η οποία παρουσιάζεται στην κορυφή του επόμενη σελίδα, όπου $\Omega_B = \frac{\Omega_{AB}}{\Omega_{IB}}$, $\rho_B = mL_{AB} + mL_{AB}$, $\rho_E =$ $_{mLAE} + _{mLAE}$, και F_{21} είναι η υπεργεωμετρική συνάρτηση Gauss [38, εξίσωση 9.14-

$$\omega_B \qquad\qquad B$$

και,

$$p_r(r) = \frac{\sqrt{N_0}}{\sqrt{2\pi}\ \sigma_{AB}}\ \exp\ -2\frac{N0\ r2}{\sigma_{AB}^2}\ , \qquad (23)$$

όπου, $\sigma^2_{AB} = \pi^2 f^2 (\Omega/m)$. Με βάση την (21-23), το τελικό έκφραση του $R_{(\xi_{th})}$ προκύπτει στο Παράρτημα Γ και δίνεται από την (24), που παρουσιάζεται στο πάνω μέρος της επόμενης σελίδας, όπου x_n και

$$P_{\text{out}}(\xi_{\text{th}}) = 1 - \exp\left(-m\left[2^{\xi_{\text{th}}} - 1\right]\left(\frac{m}{\omega_B}\right)^{mL_{AB}-1}\right) \sum_{k=0}^{mL_{AB}-1} \sum_{n=0}^{mL_{AE}-1-k} \frac{\binom{mL_{AB}-1}{k}\binom{mL_{AE}-1-k}{n}\left(\frac{\omega_B}{\omega_E}\right)^{k+1}\left(\frac{m}{\omega_E}\right)^{n}\left(2^{\xi_{\text{th}}}-1\right)^{n+mL_{AB}}\left[1-2^{-\xi_{\text{th}}}\right]^{mL_{AB}-k-n-1}}{(mL_{AB}-k-n-1)!\left[1+\frac{\omega_E}{\omega_B}2^{\xi_{\text{th}}}\right]^{n+mL_{AE}}}. \tag{13}$$

$$P_{\text{out}}^{(I)}(\xi_{\text{th}}^{\text{oo}}) = 1 - \frac{\Omega_B^{mL_{IB}}\Omega_E^{mL_{AE}}}{B(mL_{AE}, mL_{IE})} \sum_{k=0}^{mL_{AB}-1} \sum_{n=0}^{mL_{IB}-1+k} \frac{\binom{mL_{AB}-1}{k}\binom{mL_{IB}-1+k}{n}\left[1-2^{-\xi_{\text{th}}^{\text{oo}}}\right]^{mL_{AB}-1-k-n}}{\left[\Omega_B-\left(1-2^{-\xi_{\text{th}}^{\text{oo}}}\right)\right]^{\rho_B-mL_{AE}-k-n-1}} \times B\left(n+mL_{AE}, \rho_B+mL_{IE}-n-1-k\right) {}_2F_1\left(\rho_E, n+mL_{AE}; \rho_B+\rho_E-1-k; 1-\frac{1-2^{-\xi_{\text{th}}^{\text{oo}}}(1-\Omega_B)}{\Omega_E}\right). \tag{18}$$

$$R_{\text{th}}^{(N)}(\xi_{\text{th}}) \approx \frac{\sqrt{2\pi} f_{\max} \exp\left(-\frac{m}{\omega_B}\left[2^{\xi_{\text{th}}}-1\right]\right)\left(\frac{m}{\omega_B}\right)^{mL_{AB}}}{\Gamma(mL_{AB})\Gamma(mL_{AE})2^{-\xi_{\text{th}}^{\text{oo}}(2mL_{AB}-1)}m^{-mL_{AE}}\left(\frac{\omega_E}{\omega_B}\right)^{mL_{AE}}} \sum_{n=1}^{N} \frac{w_n x_n^{mL_{AE}-1}}{\left[x_n+1-2^{-\xi_{\text{th}}}\right]^{mL_{AB}+\frac{1}{2}}} \exp\left(-x_n\left[\frac{m2^{\xi_{\text{th}}}}{\omega_B}+\frac{m}{\omega_E}-1\right]\right). \tag{24}$$

---

w_n είναι η n^{th} ακμή (ρίζα) και το βάρος του πολυωνύμου Laguerre N^{th} τάξης, αντίστοιχα.

Για την ειδική περίπτωση ($\xi_{\text{th}} = 0$), η έκφραση μπορεί να παραχθεί σε ακριβή μορφή, όπως φαίνεται στο Παράρτημα Γ, και είναι δίνεται από

$$R^{(N)}(0) = \frac{\sqrt{2\pi} f_{\max} \Gamma\left(mL_{AB}+mL_{AE}-\frac{1}{2}\right)\left(\frac{\omega_B}{\omega_E}\right)^{mL_{AE}-\frac{1}{2}}}{\Gamma(mL_{AB})\Gamma(mL_{AE})\left(1+\frac{\omega_B}{\omega_E}\right)^{mL_{AB}+mL_{AE}-\frac{1}{2}}}. \tag{25}$$

Τώρα, απλοποιώντας περαιτέρω με ($m = L_{AB} = L_{AE} = 1$), η έκφραση του $R^{(N)}(0)$ ανάγεται σε

$$R^{(N)}(0) = \frac{\pi f_{\max}\sqrt{\frac{\omega_B}{\omega_E}}}{\sqrt{2}\left(1+\frac{\omega_B}{\omega_E}\right)}. \tag{26}$$

2) Συστήματα περιορισμένης παρεμβολής: Για συστήματα περιορισμένης παρεμβολής, το γεγονός ($SC \le \xi_{\text{th}}$) είναι ισοδύναμο με το γεγονός $\left[\frac{\alpha_{IB}}{\alpha_{AB}} \le 2^{\xi_{\text{th}}}(1+\lambda_E)-1\right]$. Κατά συνέπεια, $R_{\xi_{\text{th}}}^{(I)}$ είναι ισοδύναμη με το ρυθμό με τον οποίο η διαδικασία β περνάει προς τα κάτω το επίπεδο β ($= \sqrt{2^{\xi_{\text{th}}}(1+\lambda_E)-1}$). Αυτό το ASOR μπορεί να προκύψει από τον γενικό τύπο που παρατίθεται στο [39] ως εξής

$$R_{\text{th}}^{(I)}(\xi_{\text{th}}) = \int_0^\infty \int_0^\infty \beta \dot{\beta} p_{\beta\dot{\beta}}(\beta, \beta\dot{\beta}) p_{\lambda_E}(v) d\beta\dot{\beta}\, dv, \tag{27}$$

όπου, $p_{\beta\dot{\beta}}$ είναι η κοινή PDF των β και $\dot{\beta}$.

ακριβής μορφή

$$R^{(I)}(0) = \frac{\sqrt{2\pi} f_{\max}^{AB} \Omega_E^{mL_{AE}} \Gamma\left(\rho_E-\frac{1}{2}\right)}{\Omega_B^{mL_{AE}} \Gamma(mL_{AB}) \Gamma(mL_{IB}) B(mL_{AE}^2, mL_{IE})} \times B\left(mL_{AB}+mL_{AE}-\frac{1}{2}, mL_{IB}+mL_{IE}-\frac{1}{2}\right) \times F_{21}\left(\rho_E, mL_{AB}+mL_{AE}-\frac{1}{2}; \rho_B+\rho_E-1; 1-\frac{\Omega_B}{\Omega_E}\right). \tag{29}$$

Για την περίπτωση μίας κεραίας Rayleigh ($m = L_{AB} = L_{AE} = L_{IB} = L_{IE} = 1$), η έκφραση του $R^{(I)}(0)$ δίνεται από το την ακόλουθη απλούστερη έκφραση

$$R^{(I)}(0) = \frac{87\sqrt{2\pi} f_{\max}^{AB} \Omega_B}{250\,\Omega_E} {}_2F_1\left(2, \frac{3}{2}; 3; 1-\frac{\Omega_B}{\Omega_E}\right). \tag{30}$$

D. Μέση διάρκεια διακοπής απορρήτου (ASOD)

Το ASOD είναι ένα μέτρο [σε δευτερόλεπτα] που περιγράφει για πόσο χρονικό διάστημα κατά μέσο όρο το σύστημα παραμένει σε κατάσταση διακοπής της μυστικότητας. Ως μέση διάρκειας διακοπής λειτουργίας στα [26] και [39], η ASOD είναι

που εκφράζεται ως

$$T(\xi_{\text{th}}) = \frac{P_{\text{out}}(\xi_{\text{th}})}{R(\xi_{\text{th}})}. \tag{31}$$

Με βάση την (31) και τις παραγόμενες εκφράσεις των SOP και ASOD, η μέση διάρκεια διακοπής της μυστικότητας μπορεί

$^{(I)}$

για π ορισμένου θορύβου και
συσ ε περιορισμένης
τήμ ρ παρεμβολής που
ατα ι παρουσιάζουν

Η τελική έκφραση του $R_{\Delta}(\xi_{th})$ προκύπτει στο Παράρτημα Δ και δίνεται από την (28), η οποία φαίνεται στο κάτω μέρος του επόμενου σελίδα.

Για την ειδική περίπτωση ($\xi_{th} = 0$), η έκφραση του $R^{(I)}(0)$ είναι προκύπτει επίσης στο Παράρτημα Δ και δίνεται από την ακόλουθη σχέση ενδιαφέρον. Για την ειδική περίπτωση ($\xi_{th} = 0$, $m = {}_{LAB} = {}_{LAE} = 1$),

την έκφραση του ASOD για περιορισμένο θόρυβο και παρεμβολές περιορισμένα συστήματα δίνονται από

$$T^{(N)}(0) = \frac{1}{\pi_{fmax}} \frac{\overline{2\,\omega_E}}{\omega_B}, \tag{32}$$

ΠΙΝΑΚΑΣ Ι
ΠΑΡΆΜΕΤΡΟΙ ΠΡΟΣΟΜΟΊΩΣΗΣ

Parameter	Value
Simulation Time [s]	100
Sampling Time (T_s) [s]	$1e-4$
Number of Channel Samples (N_s)	1e6
ξ_{th} [bps/Hz]	0, and 1
f_{max} [Hz]	10, 50, and 100
ω_B | Ω_B [dB]	0 : 20
ω_E | Ω_E [dB]	0, 10, and 20
Order of Laguerre Polynomial (N)	50

και,

$$T^{(n)}(0) = \frac{250\,\Omega_E - 125\Omega_{B2}\,F_1\left(2, 1, 3, 1-\frac{\Omega_B}{\Omega_E}\right)}{87\sqrt{2\pi}f_{max}\,\Omega_{B2}\,F_1\left(2, \frac{3}{2}; 3; 1-\frac{\Omega_B}{\Omega_E}\right)}, \quad (33)$$

αντίστοιχα. Με βάση τις (32) και (33), και για ίσες τιμές των $_{\omega B}(\Omega_B)$ και $_{\omega E}(\Omega_E)$, η υπεργεωμετρική συνάρτηση, στην (33), ανάγεται σε 1. Συνεπώς, η ASOD εξαρτάται σε αυτή την περίπτωση μόνο από τη μέγιστη μετατόπιση Doppler (η οποία σχετίζεται με την
κινητικότητα και τη χρονική μεταβολή του καναλιού) τόσο για συστήματα περιορισμένου θορύβου όσο και για συστήματα περιορισμένης παρεμβολής. Αυτό είναι αναμενόμενο καθώς οι παράμετροι του Bob και της Eve είναι οι ίδιες (όσον αφορά τη μέση ισχύ και τη σειρά ποικιλομορφίας).

Στην επόμενη ενότητα, θα προσπαθήσουμε να αντλήσουμε περισσότερες πληροφορίες για τις παραγόμενες εκφράσεις και για τα δύο εξεταζόμενα συστήματα.

IV. ΑΡΙΘΜΗΤΙΚΆ ΑΠΟΤΕΛΈΣΜΑΤΑ

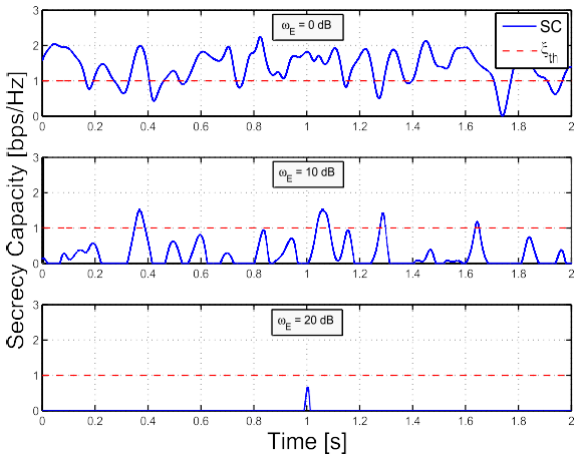
Σε αυτή την ενότητα, και χρησιμοποιώντας προσομοίωση Monte Carlo στο MatLab, παρουσιάζονται αριθμητικά αποτελέσματα για να επιβεβαιωθούν και να συζητηθούν οι αναλυτικές εκφράσεις που προέκυψαν για συστήματα περιορισμένου θορύβου και περιορισμένης διασποράς. Χωρίς απώλεια της γενικότητας, οι κύριες παράμετροι που χρησιμοποιήθηκαν στις προσομοιώσεις μας παρουσιάζονται στον Πίνακα Ι.

Η ακρίβεια των παραγόμενων αναλυτικών εκφράσεων επιβεβαιώνεται από τα αποτελέσματα της προσομοίωσης που παρουσιάζονται στα ακόλουθα σχήματα.

Α. Συστήματα περιορισμένου θορύβου:

Σε αυτό το υποκεφάλαιο, παρουσιάζουμε και συζητάμε τα αριθμητικά αποτελέσματα για συστήματα περιορισμένου θορύβου.

Στο Σχήμα 2, παρουσιάζεται η μεταβολή των υλοποιήσεων της χωρητικότητας απορρήτου, η οποία είναι ουσιαστικά η διαφορά των υλοποιήσεων των κύριων καναλιών και των καναλιών υποκλοπής, συναρτήσει του χρόνου για ένα σύστημα περιορισμένου θορύβου, με $m = 2$, $_{\omega B} = 10$ dB, $_{fmax} = 10$ Hz, $_{\xi th} = 1$ και διαφορετικές τιμές του $_{\omega E}$. Όπως φαίνεται σε αυτό το σχήμα, η χωρητικότητα μυστικότητας μειώνεται με την αύξηση των τιμών του $_{\omega E}$ (κάτι που είναι εμφανές από την περιοχή της καμπύλης κάτω από το $_{\xi th}$. Αυτό οφείλεται στο γεγονός ότι, με την αύξηση του $_{\omega E}$, αυξάνεται το επίπεδο της στιγμιαίας χωρητικότητας στο κανάλι υποκλοπής,

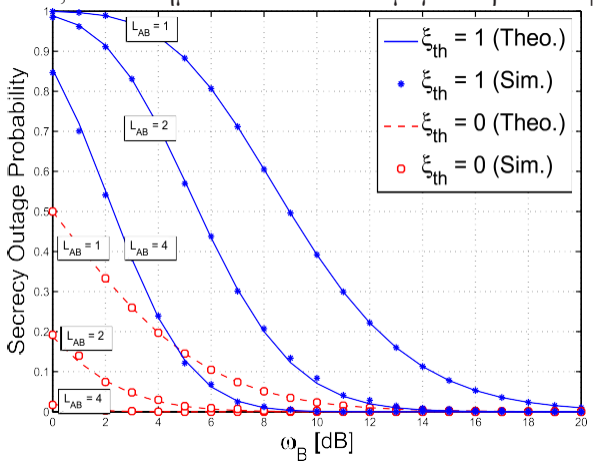


Σχήμα 2. Πραγματοποιήσεις χωρητικότητας απορρήτου σε σχέση με το χρόνο με $m = 2$, $_{LAB} = 2$, $_{LAE} = 2$, $_{\omega B} = 10$ dB, $_{fmax} = 10$ Hz, $_{\xi th} = 1$ και διαφορετικές τιμές του

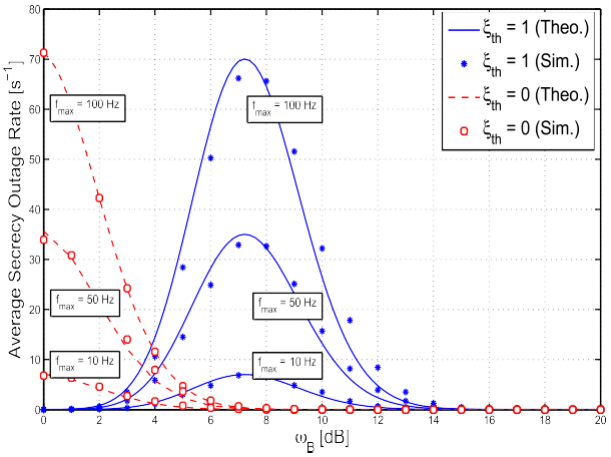
Σχήμα 3. Πιθανότητα απώλειας μυστικότητας συναρτήσει του ω_B για ένα σύστημα περιορισμένου θορύβου, με $m = 2$, $\Omega_{AE} = 1$, $\omega_E = 0$ dB, $f_{max} = 10$ Hz και διαφορετικές τιμές των Ω_{AB} και ξth.

γεγονός που έχει ως αποτέλεσμα τη μείωση της χωρητικότητας απορρήτου των νόμιμων διαύλων επικοινωνίας.

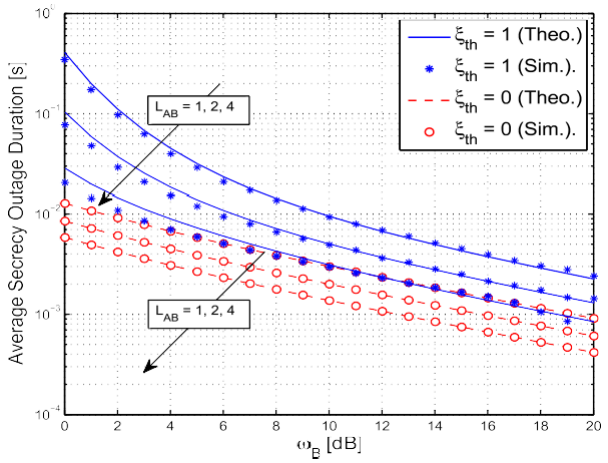
Στο Σχήμα 3 παρουσιάζεται η μεταβολή της πιθανότητας απώλειας μυστικότητας σε σχέση με το ω_B για ένα σύστημα περιορισμένου θορύβου, με $m = 2$, $\Omega_{AE} = 1$, $\omega_E = 0$ dB, $f_{max} = 10$ Hz και διαφορετικές τιμές των Ω_{AB} και ξth. Είναι σαφές ότι η πιθανότητα απόρρητης απόκρυψης μειώνεται με την αύξηση των τιμών των Ω_{AB} και ω_B. Αυτό οφείλεται στο γεγονός ότι οι αυξημένες τιμές των Ω_{AB} και ω_B ενισχύουν το SNR στον Bob, το οποίο μειώνει την πιθανότητα διαφυγής μυστικότητας. Επίσης, και όπως αναμενόταν, φαίνεται σε αυτό το σχήμα ότι η πιθανότητα διακοπής της μυστικότητας μειώνεται με τις μειωμένες τιμές του ξth για όλες τις τιμές του Ω_{AB}. Κατά συνέπεια, τα συστήματα που απαιτούν μεγαλύτερα κατώφλια μυστικότητας πρέπει να χρησιμοποιούν υψηλότερη ποικιλομορφία προκειμένου να διατηρήσουν την ίδια απόδοση απόκρυψης.



$$R^{(I)}(\xi_{th}) \approx \frac{\sqrt{2\pi}\,\Gamma(\rho_B^{-1})\,f_{max}\,\Omega_B^{\,z}\,\Omega_E^{\,IE}}{2\xi_{th}^{(2mLIB^{-1})}\,\Gamma(mL_{AB})\,\Gamma(mL_{IB})\,B(mL_{AE}, mL_{IE})} \sum_{n=1}^{N} \frac{\omega_n x_n}{\left(x_n + \Omega_E^{-1}\right)^{mLAE^{-1}}} \frac{\left(x_n + 1 - 2^{-\xi_{th}^{mLAB^{-2}}}\right)^{\frac{1}{\rho_E}}}{\left(x_n + 1 - 2^{-\xi_{th}}(1 - \Omega_B^{-1})\right)^{\rho_B^{-1}}} \exp(x_n). \quad (28)$$



Σχήμα 4. Μέσος ρυθμός απώλειας μυστικότητας συναρτήσει του $_{\omega B}$ για ένα σύστημα περιορισμένου θορύβου, με m = 4, $_{LAB}$ = 2, $_{LAE}$ = 2, $_{\omega E}$ = 0 dB, και διαφορετικές τιμές των $_{fmax}$ και $_{\xi th}$. (Για N = 50, η αξιολόγηση Laguerre οδηγεί σε μέσο σφάλμα μικρότερο από $1e$ - 2 σε σύγκριση με την αριθμητική αξιολόγηση των ολοκληρώσεων, χρησιμοποιώντας Λογισμικό MatLab.).

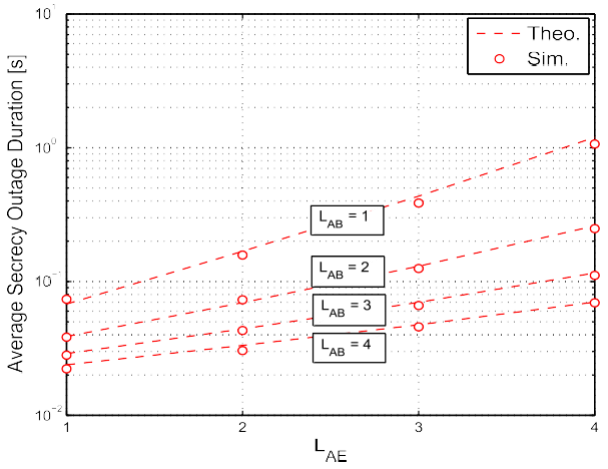


Σχήμα 5. Μέση διάρκεια διακοπής μυστικότητας συναρτήσει του $_{\omega B}$ για ένα σύστημα περιορισμένου θορύβου, με m = 1, $_{LAE}$ = 1, $_{\omega E}$ = 0 dB, $_{fmax}$ = 50 Hz και διαφορετικές τιμές των $_{LAB}$ και ξth.

Στο Σχήμα 4 παρουσιάζεται η μεταβολή του μέσου ρυθμού διακοπής μυστικότητας [ή του μέσου ρυθμού διέλευσης του επιπέδου μυστικότητας] συναρτήσει του $_{\omega B}$ για ένα σύστημα περιορισμένου θορύβου, με m = 4, $_{LAB}$ = 2, $_{LAE}$ = 2, $_{\omega E}$ = 0 dB και διαφορετικές τιμές των $_{fmax}$ και $_{\xi th}$. Όπως φαίνεται σε αυτό το σχήμα, για $_{\xi th}$ = 0 και $_{\xi th}$ = 1, οι αυξημένες τιμές της μέγιστης μετατόπισης της συχνότητας Doppler $_{fmax}$ (η οποία αντικατοπτρίζει τους κόμβους που κινούνται με μεγαλύτερη ταχύτητα) αυξάνουν το μέσο ποσοστό υπέρβασης απορρήτου. Αυτό οφείλεται στο γεγονός ότι ο χρόνος συνοχής του καναλιού είναι αντιστρόφως ανάλογος του $_{fmax}$, γεγονός που οδηγεί σε γρήγορα κανάλια εξασθένισης μεταξύ των διαφόρων κόμβων του δικτύου. Κατά συνέπεια, παρατηρείται μια γρήγορη μεταβολή της χωρητικότητας μυστικότητας, η οποία αυξάνει το μέσο ποσοστό διέλευσης του επιπέδου μυστικότητας. Είναι επίσης σαφές ότι για $_{\xi th}$ = 1, το οποίο αναφέρεται στην περίπτωση όπου το σύστημα έχει υψηλότερες απαιτήσεις όσον αφορά την διακοπή απορρήτου, και για μια $_{max}$, οι καμπύλες δεδομένη τιμή του f ASOR έχουν μέγιστες τιμές. Αυτό οφείλεται στο γεγονός ότι, για μικρές τιμές του $_{\omega B}$, η στιγμιαία ικανότητα απορρήτου είναι ως επί το πλείστον κάτω από το κατώφλι με περιστασιακή διέλευση προς τα πάνω, ενώ σε μεγάλες τιμές του $_{\omega B}$, η στιγμιαία ικανότητα απορρήτου είναι ως επί το πλείστον πάνω από το κατώφλι με περιστασιακή διέλευση προς τα κάτω.

Στο Σχήμα 5, παρουσιάζεται η μεταβολή της μέσης διάρκειας διακοπής της μυστικότητας συναρτήσει του $_{\omega B}$ για ένα σύστημα περιορισμένου θορύβου, με m = 1, $_{LAE}$ = 1, $_{\omega E}$ = 0 dB, $_{fmax}$ = 50 Hz και διαφορετικές τιμές των $_{LAB}$ και $_{\xi th}$. Παρόμοια με τη συμπεριφορά της πιθανότητας διακοπής μυστικότητας, η μέση διάρκεια διακοπής μυστικότητας μειώνεται με την αύξηση των τιμών $_{\Omega B}$ και $_{LAB}$. Αυτό συμβαίνει επειδή, η μέση διάρκεια διακοπής μυστικότητας είναι ευθέως ανάλογη της πιθανότητας διακοπής μυστικότητας, όπως ορίζεται στην Εξ. (31).

Στο Σχήμα 6 παρουσιάζεται η μέση διάρκεια διακοπής της μυστικότητας για ένα σύστημα περιορισμένου θορύβου, με m = 2, $_{\omega B}$ = $_{\omega E}$ = 10 dB, $_{fmax}$ = 10 Hz, $_{\xi th}$ = 0, και διαφορετικές τάξεις ποικιλομορφίας στα κύρια κανάλια και στα κανάλια



Σχήμα 6. Μέση διάρκεια διακοπής απορρήτου σε σχέση με το L για περιορισμένο θόρυβο

σύστημα, με m = 2, $_{\omega B}$ = $_{\omega E}$ = 10 dB, f $_{max}$ = 10 ^{AE} Hz, $_{\xi th}$ = 0, και

συρματοποίησης ($_{LAB}$ και $_{LAE}$). Όπως φαίνεται σε αυτό το σχήμα, η μέση διάρκεια διακοπής μυστικότητας αυξάνεται με τις αυξημένες τιμές του $_{LAE}$ και μειώνεται με τις αυξημένες τιμές του $_{LAB}$. Αυτό οφείλεται στο γεγονός ότι η αύξηση της τάξης ποικιλομορφίας στην Eve ενισχύει την αντίστοιχη χωρητικότητα,

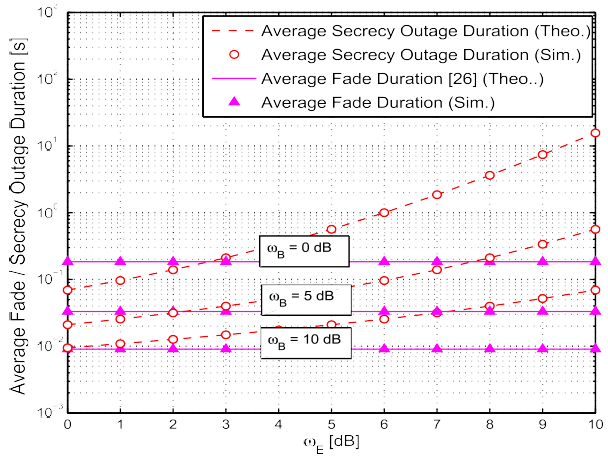
διαφορετικές τιμές του $_{LAB}$.

γεγονός που έχει ως αποτέλεσμα την αύξηση της πιθανότητας διακοπής της μυστικότητας και, ως εκ τούτου, μπορεί να παρατηρηθεί αύξηση της μέσης διάρκειας διακοπής της μυστικότητας. Αντίθετα, οι αυξημένες τιμές του $_{LAB}$ ενισχύουν το SNR στον Bob, γεγονός που μειώνει την πιθανότητα διακοπής μυστικότητας καθώς και τη μέση διάρκεια διακοπής μυστικότητας.

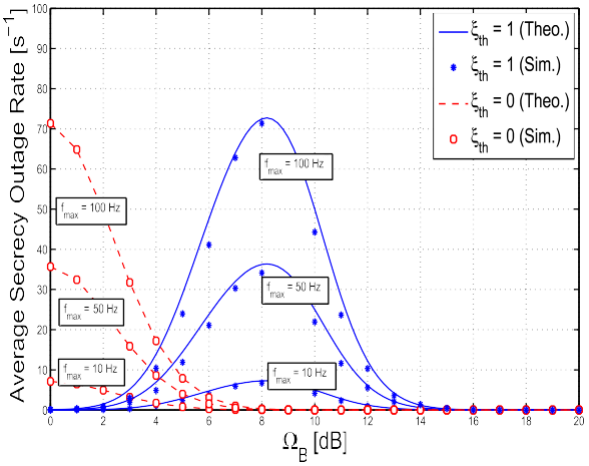
Σημειώνουμε επίσης τη φθίνουσα επίδραση στη μείωση του ASOD καθώς αυξάνουμε *το* $_{LAB}$ για σταθερό $_{LAE}$, το οποίο είναι μια φυσική συμπεριφορά ποικιλομορφίας.

Το Σχήμα 7 παρουσιάζει μια σύγκριση μεταξύ της μέσης διάρκειας διακοπής της μυστικότητας και της γνωστής μέσης διάρκειας εξασθένισης [26]-[28], για ένα σύστημα περιορισμένου θορύβου, με $m = 2$, $_{NA} = 1$, $_{NB} = _{NE} = 2$, $_{fmax} = 10$ Hz, $_{\xi th} = 0$, κατώφλι εξασθένισης ίσο με 5 dB και διαφορετικές τιμές των ω και ω.

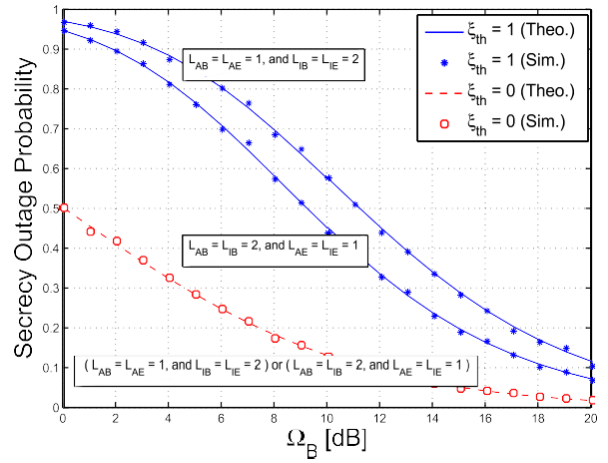
Το σχήμα δείχνει σαφώς το πλεονέκτημα της προτεινόμενης μετρικής σε σχέση με τις τρέχουσες διαθέσιμες μετρικές στη βιβλιογραφία. Ενώ η μέση διάρκεια εξασθένισης δίνει μια σημαντική εικόνα για το κύριο κανάλι, δεν αντικατοπτρίζει το επίπεδο μυστικότητας του συστήματος και παρουσιάζει γενικά αισιόδοξες τιμές (χαμηλότερες από τις αναμενόμενες) για τη διάρκεια των "κακών" διαστημάτων του καναλιού.



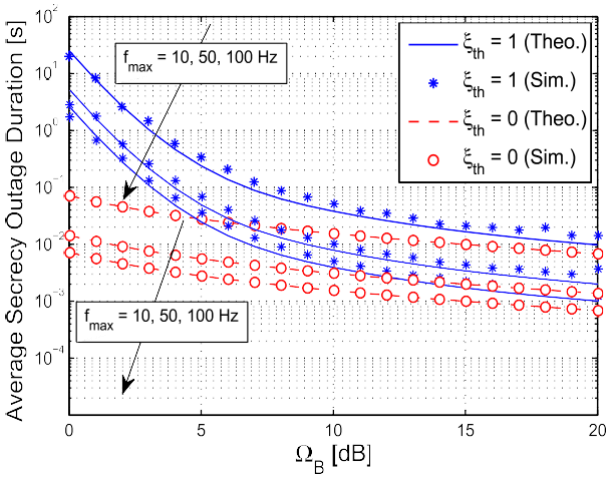
Εικ. 7. Σύγκριση μεταξύ της μέσης διάρκειας απώλειας μυστικότητας και της μέσης διάρκειας εξασθένισης, για ένα σύστημα περιορισμένου θορύβου, με $m = 2$, $_{NA} = 1$, $_{NB} = _{NE} = 2$, $_{fmax} = 10$ Hz, $_{\xi th} = 0$, κατώφλι εξασθένισης ίσο με 5 dB και διαφορετικές τιμές των $_{\omega B}$ και ωE .



Εικ. 9. Μέσος ρυθμός απώλειας μυστικότητας συναρτήσει του $_{\Omega B}$ για ένα σύστημα περιορισμένης παρεμβολής, με $m = 4$, $_{LAB} = 4$, $_{LAE} = 4$, $_{LIB} = 3$, $_{LIE} = 3$, $_{\Omega E} = 0$ dB, και διαφορετικές τιμές των $_{fmax}$ και $_{\xi th}$.



Σχήμα 8.Πιθανότητα διακοπής της μυστικότητας σε σχέση με το Ω για περιορισμένη παρεμβολή σύστημα, με $m = 1$, $\Omega = 0$ dB, f $_{B}$ Hz και διαφορετικές τιμές $_{max} = 10$ $_{E}$ $_{LAB}$, $_{LIB}$, $_{LAE}$, $_{LIE}$, και $_{\xi th}$.



Σχήμα 10. Μέση διάρκεια διακοπής απορρήτου συναρτήσει του $_{\Omega B}$ για μια παρεμβολή περιορισμένο σύστημα, με $m = 2$, $_{LAB} = 2$, $_{LAE} = 2$, $_{LIB} = 2$, $_{LIE} = 2$, $_{\Omega E} = 0$ dB, και διαφορετικές τιμές του f $_{max}$ και $_{\xi th}$.

B. Συστήματα περιορισμένης παρεμβολής:

Για συστήματα περιορισμένης παρεμβολής, και χωρίς απώλεια της γνησιότητας, τα αριθμητικά αποτελέσματα βασίζονται επίσης στις παραμέτρους προσομοίωσης του Πίνακα Ι.

Η μεταβολή της πιθανότητας απώλειας μυστικότητας σε σχέση με το $_{\Omega B}$ για ένα σύστημα περιορισμένης παρεμβολής παρουσιάζεται στο Σχήμα 8, με $m = 1$, $_{\Omega E} = 0$ dB, $_{fmax} = 10$ Hz και διαφορετικές τιμές των $_{LAB}$, $_{LIB}$, $_{LAE}$, $_{LIE}$ και $_{\xi th}$. Όπως φαίνεται σε αυτό το σχήμα, για $_{\xi th} = 1$, η ύπαρξη υψηλότερης τάξης ποικιλομορφίας στη ζεύξη Alice-Bob έχει θετικότερο αντίκτυπο στην απόδοση του συστήματος από τη λήψη σημάτων παρεμβολής της ίδιας τάξης στην Eve. Αυτό συμβαίνει απλώς επειδή η πηγή παρεμβολής επηρεάζει τόσο την Eve όσο και τον Bob. Ωστόσο, για $_{\xi th} = 0$, η αύξηση της τάξης ποικιλομορφίας στη σύνδεση Alice-Bob έχει τον ίδιο αντίκτυπο στην απόδοση του συστήματος με την αύξηση της ποικιλομορφίας των σημάτων παρεμβολής με την ίδια τάξη. Αυτό συμβαίνει επειδή, για $_{\xi th} = 0$, και με βάση τις (3), (4) και (16), η πιθανότητα απώλειας μυστικότητας είναι ευθέως ανάλογη του $(_{LAB\ LIE})$. Επομένως, για σταθερές τιμές των $_{LAE}$, $_{LIB}$,

$_{\Omega B}$, και $_{\Omega E}$, το σενάριο προσομοίωσης ($_{LAB}$ = $_{LAE}$ = 1 και $_{LIB}$ = $_{LIE}$ = 2) παρουσιάζει την ίδια απόδοση όσον αφορά την πιθανότητα διακοπής της μυστικότητας με το σενάριο προσομοίωσης ($_{LAB}$ = $_{LIB}$ = 2 και $_{LAE}$ = $_{LIE}$ = 1). Με βάση αυτό, τα συστήματα που απαιτούν υψηλότερα κατώτατα όρια μυστικότητας για την ανοχή τους σε διακοπές πρέπει να επενδύσουν πόρους στην αύξηση της τάξης ποικιλομορφίας στην κύρια ζεύξη, αντί να βασίζονται στην ύπαρξη μεγάλων επιπέδων παρεμβολής που μπορεί να επηρεάσουν τον υποκλοπέα.

Στο Σχήμα 9 παρουσιάζεται η μεταβολή του μέσου ρυθμού απώλειας μυστικότητας συναρτήσει του $_{\Omega B}$ για ένα σύστημα περιορισμένης παρεμβολής, με m = $_{LAB}$ = $_{LAE}$ = 4, $_{LIB}$ = $_{LIE}$ = 3, $_{\Omega E}$ = 0 dB και διαφορετικές τιμές των $_{fmax}$ και $_{\xi th}$. Παρόμοια με τη συμπεριφορά του μέσου ρυθμού αποτυχίας απορρήτου για συστήματα περιορισμένου θορύβου, οι αυξημένες τιμές του $_{fmax}$, σε αυτό το σενάριο, αυξάνουν το μέσο ρυθμό αποτυχίας απορρήτου. Αυτό οφείλεται στο γεγονός ότι, όπως αναλύθηκε προηγουμένως, η αύξηση της $_{fmax}$ έχει ως αποτέλεσμα τη γρήγορη μεταβολή της χωρητικότητας απορρήτου και, ως εκ τούτου, μπορεί να παρατηρηθεί αύξηση του μέσου ρυθμού διέλευσης του επιπέδου απορρήτου.

Η μεταβολή της μέσης διάρκειας διακοπής της μυστικότητας σε σχέση με $_{\Omega B}$ παρουσιάζεται στο Σχήμα 10, με m = $_{LAB}$ = $_{LAE}$ =

$_{LIB}$ = $_{LIE}$ = 2, $_{\Omega E}$ = 0 dB και διαφορετικές τιμές των $_{fmax}$ και $_{\xi th}$. Όπως φαίνεται σε αυτό το σχήμα, για τις διαφορετικές τιμές του $_{\xi th}$, η μέση διάρκεια διακοπής της μυστικότητας μειώνεται με
τις αυξημένες τιμές της $_{fmax}$. Αυτό οφείλεται στο γεγονός ότι, όπως περιγράφεται λεπτομερώς
για το Σχήμα 9, αυξάνοντας $_{max}$, η μέση διακοπή της
αυξάνεται, γεγονός που μειώνει τη μέση διάρκεια διακοπής της μυστικότητας. Κατά συνέπεια, τα συστήματα που περιβάλλοντα θα πρέπει να εξετάσουν το ενδεχόμενο βελτιστοποίησης του σχεδιασμού τους με βάση
την αναμενόμενη ισχύ του καναλιού υποκλοπής για να αποφευχθεί η εργασία
σε περιοχές διακοπής απορρήτου για μεγάλα χρονικά διαστήματα ή να υποφέρουν από συχνές πτώσεις της χωρητικότητας απορρήτου, ακόμη και με μικρότερες

V. Συμπέρασμα

Στην παρούσα εργασία, προτάθηκε και αξιολογήθηκε μια αναλυτική μεθοδολογία για την αξιολόγηση της ασφάλειας ασύρματων συστημάτων επικοινωνίας με α π ό κ λ ι σ η σε κανάλια υποκλοπής, όπου εισήχθησαν δύο σημαντικές μετρικές ασφάλειας φυσικού στρώματος και οι αντίστοιχες αναλυτικές εκφράσεις.
για κανάλια εξασθένισης Nakagami-m. Με βάση αυτό, έχουν διεξαχθεί αριθμητικές προσομοιώσεις για την αξιολόγηση των
αναλυτικά αποτελέσματα και να διερευνήσει τις διακυμάνσεις του νέου
μετρικές σε διάφορα σενάρια. Τα αποτελέσματα αυτά έδειξαν τη σημασία των προτεινόμενων στατιστικών μετρικών δεύτερης τάξης για
την αξιολόγηση της δυναμικής της ασφάλειας του φυσικού επιπέδου. Συγκεκριμένα, τα ποσοστά πτώσης της ασφάλειας επικοινωνίας και ο μέσος όρος
οι περιοχές διακοπής επηρεάζονται ουσιαστικά από την τάξη ποικιλομορφίας στους δέκτες και τη μέγιστη μετατόπιση συχνότητας Doppler. Επιπλέον, βρήκαμε ότι τα συστήματα με υψηλές απαιτήσεις αποτελεσματικότητας
θα πρέπει να επενδύσει στην αύξηση της τάξης ποικιλομορφίας του κυρίου συνδέσμου.

Παράρτημα
Παραγωγή του $P^{(N)}_{OUT}$ για συστήματα περιορισμένου θορύβου

Σε αυτό το προσάρτημα, παρουσιάζουμε την εξαγωγή της μυστικότητας
έκφραση της πιθανότητας διακοπής στην περίπτωση ενός συστήματος περιορισμένου θορύβου.

Με βάση το (10), $P^{(N)}_{out}$ μπορεί να γραφεί ως

$$P^{(N)}_{out}(\xi_{th}) = \int_0^{\infty}\int_0^{2^{\xi_{th}}(1+y)-1} p_{\gamma_B}(x)\, p_{\gamma_E}(y)\, dx\, dy, \quad (34)$$

Χρησιμοποιώντας την έκφραση $_{B}$ στην (11), και η κατά τμήματα [38, . - .], η (34) μπορεί να ξαναγραφεί ως εξής

$$P^{(N)}_{out}(\xi_{th}) = \frac{m_{mLAB}}{\omega_{mLAB}\Gamma(mL_{AB})} \int_0^{\infty}$$

γίνεται

$$P^{(N)}_{out}(\xi_{th}) = 1 - \frac{m_{mLAB}\, m_{mLAE} \exp\left(-\frac{m[2^{\xi_{th}}-1]}{\omega_B}\right)}{\omega_{mLAB}\,\omega_{mLAE}\,\Gamma(ml)\,\Gamma(mL)} \times \sum_{k=0}^{mL_{AB}-1} \frac{(mL_{AB}-1)(\omega_B)^{k+1}}{k!\,(m2^{\xi_{th}})^{k+1}} \times \left\{\sum_{n=0}^{mL-1} \binom{mL-1}{n} \frac{(-1)^n}{(m2^{\xi_{th}})^n}\right\} \times \int_0^{\infty} \frac{y^{mL_{AE}-1} \exp\left(-\left(\omega_E + \frac{m2^{\xi_{th}}}{\omega_B}\right) y\right)}{(y+1-2^{\xi_{th}})^{mL_{AB}+1+k}}\, dy. \quad (36)$$

Χρησιμοποιώντας το ακόλουθο πεπερασμένο άθροισμα στο [38, εξ. 1.111]

$$(a+y)^N = \sum_{n=0}^{N} \binom{N}{n} a^{N-n} y^n \quad (37)$$

(36) μπορεί να ξαναγραφεί ως εξής

$$P^{(N)}_{out}(\xi_{th}) = 1 - \frac{m_{mLAB}\, m_{mLAE} \exp\left(-\frac{m[2^{\xi_{th}}-1]}{\omega_B}\right)}{\omega_{mLAB}\,\omega_{mLAE}\,\Gamma(ml)\,\Gamma(ml)} \times \sum_{k=0}^{mL_{AB}-1} \frac{(mL_{AB}-1)(\omega_B)^{k+1}}{k!\,(m2^{\xi_{th}})^{k+1}} \times \sum_{k=0}^{mL_{AB}-1-k} \binom{mL_{AB}-1-k}{k} \left(\frac{m}{m2^{\xi_{th}}}\right)^k \times \sum_{n=0}^{mL_{AB}-1-k-n} \binom{mL_{AB}-1-k}{n} (1-2^{-\xi_{th}})^{mL_{AB}-1-k-n} \times \left\{\int_0^{\infty} y^{mL_{AE}-1+n} \exp\left(-\left(\omega_E + \frac{m2^{\xi_{th}}}{\omega_B}\right) y\right) dy\right\}. \quad (38)$$

Με βάση το [38, εξ. 3.351 -], η ολοκλήρωση στην (38) αξιολογείται και το $P^{(N)}_{out}(\xi_{th})$ εκφράζεται ως εξής

$$P^{(N)}_{out}(\xi_{th}) = 1 - \frac{m^{mL_{AB}}\, m^{mL_{AE}} \exp\left(-\frac{m[2^{\xi_{th}}-1]}{\omega_B}\right)}{\omega_B^{mL_{AB}}\, \omega_E^{mL_{AE}}\,\Gamma(ml)\,\Gamma(ml)} \times \sum_{k=0}^{mL_{AB}-1} \frac{(mL_{AB}-1)(\omega_B)^{k+1}}{k!\,(m2^{\xi_{th}})^{k+1}} \times \sum_{k=0}^{mL-1-k} \binom{mL-1-k}{k} \left(\frac{m}{m2^{\xi_{th}}}\right)^k \times \sum_{n=0}^{mL_{AB}-1} \binom{n+mL_{AE}-1}{n} \frac{1}{(1-2^{-\xi_{th}})^{k+n+1-mL_{AB}}} \frac{1}{\left(m_E + m2^{\xi_{th}}_B\right)^{n+mL_{AE}}}.$$

$$\times \int_{0}^{\infty} \exp\left(-\frac{m[2^{\xi_{th}}(1+y)-1]}{\bar{\omega}_B}\right) \frac{y^{mL_{AB}-1}}{(mL_{AB}-1)!\left(\frac{\bar{\omega}_B}{m}\right)^{mL_{AB}}} \times \sum_{k=0}^{mL_{AB}-1} \binom{mL_{AB}-1}{k} \frac{(-1)^k}{k!\left(\frac{\bar{\omega}_B}{m}\right)^{k+1}} \exp\left(-\frac{k[2^{\xi_{th}}(1+y)-1]}{\bar{\omega}_B}\right) p_{\gamma_E}(y)\,dy. \quad (35)$$

Τώρα, αντικαθιστώντας την έκφραση PDF του γ_E στην (35) και χρησιμοποιώντας την ισότητα ($\Gamma(N) = (n-1)!$), η έκφραση του $P_{out}^{(N)}$

$$= \int_{0}^{\infty} \exp\left(-\frac{m[2^{\xi_{th}}(1+y)-1]}{\bar{\omega}_B}\right) \frac{y^{mL_{AB}-1}}{(mL_{AB}-1)!\left(\frac{\bar{\omega}_B}{m}\right)^{mL_{AB}}} \times \sum_{k=0}^{mL_{AB}-1} \binom{mL_{AB}-1}{k} \frac{(-1)^k}{k!\left(\frac{\bar{\omega}_B}{m}\right)^{k+1}} \exp\left(-\frac{k[2^{\xi_{th}}(1+y)-1]}{\bar{\omega}_B}\right) p_{\gamma_E}(y)\,dy. \quad (39)$$

After some simplifications, the final exact closed form expression of $P_{out}^{(N)}(\xi_{th})$ is given by (13) on the top of page 5.

ΠΑΡΆΡΤΗΜΑ Β
ΔΕΡΓΑΣΙΑ ΤΗΣ $\Pi_{OUT}^{(I)}$ ΓΙΑ ΠΑΡΕΜΒΟΛΈΣ ΛΙΌΤΙΜΑ

Σε αυτό το προσάρτημα, εξάγουμε την έκφραση της πιθανότητας διακοπής της μυστικότητας για συστήματα περιορισμένης παρεμβολής.

Με βάση το (16), $P_{\text{out}}^{(I)}$ γράφεται ως

$$P_{\text{out}}^{(I)}(\xi_{\text{th}}) = \int_0^\infty \int_0^\infty \int_0^\infty f_{\gamma_{\text{AB}}}[2^{\xi_{\text{th}}}(1+v)-1]\, f_{\alpha_{\text{AB}}^2}(x)\, f_{\alpha_{\text{IB}}^2}(y) \times f_{\gamma_{\text{AE}}}(v)\, dx\, dy\, dv, \quad (40)$$

Χρησιμοποιώντας την έκφραση PDF της α_{AB}^2, το οποίο δίνεται από την (5), και [38, εξ. 3.351 - 1.8], η (40) μπορεί να επαναδιατυπωθεί ως εξής

$$P_{\text{out}}^{(I)}(\xi_{\text{th}}) = \frac{m^{mL_{\text{AB}}}}{\Omega_{\text{AB}}^{mL_{\text{AB}}}\,\Gamma(mL_{\text{AB}})} \int_0^\infty \int_0^\infty \exp\left(-\frac{my[2^{\xi_{\text{th}}}(1+v)-1]}{\Omega_{\text{AB}}}\right) \times \sum_{k=0}^{mL_{\text{AB}}-1} \frac{(-1)^k k!}{(k)(y[2^{\xi_{\text{th}}}(1+v)-1])^{mL_{\text{AB}}-1-k}} \left(\frac{m}{\Omega_{\text{AB}}}\right)^{k+1} + \left(\frac{\Omega_{\text{AB}}}{m}\right)^{mL_{\text{AB}}} (mL_{\text{AB}}-1)!\, p_{\alpha_{\text{IB}}^2}(y)\, p_{\gamma_{\text{AE}}}(v)\, dy\, dv. \quad (41)$$

Αντικαθιστώντας την έκφραση PDF του α_{IB}^2 στην (41) και χρησιμοποιώντας την ισότητα (Γ(N) = (n - 1)!), η έκφραση του $P_{\text{out}}^{(I)}$ γίνεται

$$P_{\text{out}}^{(I)}(\xi_{\text{th}}) = 1 - \frac{\Omega_{\text{AB}}^{mL_{\text{AB}}}\,\Omega_{\text{IB}}^{mL_{\text{IB}}}\,\Gamma(mL_{\text{AB}})\,\Gamma(mL_{\text{IB}})}{m^{mL_{\text{AB}}}\,m^{mL_{\text{IB}}}} \times \int_0^\infty \int_0^\infty \exp\left(-y\left[\frac{m[2^{\xi_{\text{th}}}(1+v)-1]}{\Omega_{\text{AB}}} + \frac{m}{\Omega_{\text{IB}}}\right]\right) \times \sum_{k=0}^{mL_{\text{AB}}-1} \frac{y^{mL_{\text{IB}}+mL_{\text{AB}}-2-k}}{\left(\frac{\Omega_{\text{AB}}}{m}\right)^{k+1} k!\,(mL_{\text{AB}}-1-k)!} \times 2^{\xi_{\text{th}}(1+v)-1)^{mL_{\text{AB}}-1-k}} f_{\gamma_{\text{AE}}}(v)\, dy\, dv. \quad (42)$$

Με βάση την [38, εξίσωση 3.351], η δεύτερη ολοκλήρωση στην (42), ως προς το y, αξιολογείται, οπότε προκύπτει

$$P_{\text{out}}^{(I)}(\xi_{\text{th}}) = 1 - \frac{m^{mL_{\text{AB}}}\,m^{mL_{\text{IB}}}}{\Omega_{\text{AB}}^{mL_{\text{AB}}}\,\Omega_{\text{IB}}^{mL_{\text{IB}}}\,\Gamma(mL_{\text{AB}})\,\Gamma(mL_{\text{IB}})} \times \left(\frac{\Omega_{\text{AB}}}{m}\right)^{mL_{\text{AB}}} (mL_{\text{AB}}-1)! - \frac{m^{mL_{\text{IB}}}}{\Omega_{\text{IB}}^{mL_{\text{IB}}}\,\Gamma(mL_{\text{IB}})} \left(\frac{\Omega_{\text{AB}}}{m}\right)^{k+1} (mL_{\text{AB}}-1) \times \int_0^\infty \frac{v^{mL_{\text{AB}}-1}}{k!} \sum_{k=0}^{mL_{\text{AB}}-1} \frac{(mL_{\text{IB}}+mL_{\text{AB}}-2-k)!\, m^k}{\left[\frac{m[2^{\xi_{\text{th}}}(1+v)-1]}{\Omega_{\text{AB}}} + \frac{1}{\Omega_{\text{IB}}}\right]^{mL_{\text{IB}}+mL_{\text{AB}}-1-k}} \times 12^{\xi_{\text{th}}}(1+v) - 1^{mL_{\text{AB}}-1-k} f_{\gamma_{\text{AE}}}(v)\, dv. \quad (43)$$

Αντικαθιστώντας την (17) στην (43), η έκφραση του $P^{(I)}(\xi_{\text{th}})$ μπορεί να ειναι ξαναγράφεται ως

$$P_{\text{out}}^{(I)}(\xi_{\text{th}}) = 1 - \frac{m^{mL_{\text{AB}}}\,m^{mL_{\text{IB}}}}{\Omega_{\text{AB}}^{mL_{\text{AB}}}\,\Omega_{\text{IB}}^{mL_{\text{IB}}}\,\Gamma(mL_{\text{AB}})\,\Gamma(mL_{\text{IB}})} \int_0^\infty \int_0^\infty \exp\left(-y\left[\frac{m[2^{\xi_{\text{th}}}(1+v)-1]}{\Omega_{\text{AB}}} + \frac{m}{\Omega_{\text{IB}}}\right]\right) \times \sum_{k=0}^{mL_{\text{AB}}-1} \frac{y^{mL_{\text{IB}}+mL_{\text{AB}}-2-k}}{\left(\frac{\Omega_{\text{AB}}}{m}\right)^{k+1} k!\,(mL_{\text{AB}}-1-k)!} \times 12^{\xi_{\text{th}}}(1+v) - 1^{mL_{\text{AB}}-1-k} f_{\gamma_{\text{AE}}}(v)\, dy\, dv. \quad (42)$$

Με βάση την [38, εξίσωση 3.351], η δεύτερη ολοκλήρωση στην (42), ως προς το y, αξιολογείται, οπότε προκύπτει

$$P_{\text{out}}^{(I)}(\xi_{\text{th}}) = 1 - \frac{m^{mL_{\text{AB}}}\,m^{mL_{\text{IB}}}}{\Omega_{\text{AB}}^{mL_{\text{AB}}}\,\Omega_{\text{IB}}^{mL_{\text{IB}}}\,\Gamma(mL_{\text{AB}})\,\Gamma(mL_{\text{IB}})} \times \left(\frac{\Omega_{\text{AB}}}{m}\right)^{mL_{\text{AB}}} (mL_{\text{AB}}-1)! - \frac{m^{mL_{\text{IB}}}}{\Omega_{\text{IB}}^{mL_{\text{IB}}}\,\Gamma(mL_{\text{IB}})} \left(\frac{\Omega_{\text{AB}}}{m}\right)^{k+1} (mL_{\text{AB}}-1) \times \int_0^\infty \frac{v^{mL_{\text{AB}}-1}}{k!} \sum_{k=0}^{mL_{\text{AB}}-1} \frac{(mL_{\text{IB}}+mL_{\text{AB}}-2-k)!\, m^k}{\left[\frac{m[2^{\xi_{\text{th}}}(1+v)-1]}{\Omega_{\text{AB}}} + \frac{1}{\Omega_{\text{IB}}}\right]^{mL_{\text{IB}}+mL_{\text{AB}}-1-k}} \times 12^{\xi_{\text{th}}}(1+v) - 1^{mL_{\text{AB}}-1-k} f_{\gamma_{\text{AE}}}(v)\, dv. \quad (43)$$

Αντικαθιστώντας την (17) στην (43), η έκφραση του $P^{(I)}(\xi)$ μπορεί να ειναι από το ξαναγράφεται ως

$$P_{\text{out}}^{(I)}(\xi_{\text{th}}) = 1 - \frac{m^{mL_{\text{AB}}}\,m^{mL_{\text{IB}}}}{\Omega_{\text{AB}}^{mL_{\text{AB}}}\,\Omega_{\text{IB}}^{mL_{\text{IB}}}\,\Gamma(mL_{\text{AB}})\,\Gamma(mL_{\text{IB}})} \int_0^\infty \int_0^\infty \exp\left(-y\left[\frac{m[2^{\xi_{\text{th}}}(1+v)-1]}{\Omega_{\text{AB}}} + \frac{m}{\Omega_{\text{IB}}}\right]\right) \times \sum_{k=0}^{mL_{\text{AB}}-1} \frac{y^{mL_{\text{IB}}+mL_{\text{AB}}-2-k}}{\left(\frac{\Omega_{\text{AB}}}{m}\right)^{k+1} k!\,(mL_{\text{AB}}-1-k)!} \times 12^{\xi_{\text{th}}}(1+v) - 1^{mL_{\text{AB}}-1-k} f_{\gamma_{\text{AE}}}(v)\, dy\, dv. \quad (42)$$

Με βάση την [38, εξίσωση 3.351], η δεύτερη ολοκλήρωση στην (42), ως προς το y, αξιολογείται, οπότε προκύπτει

$$P_{\text{out}}^{(I)}(\xi_{\text{th}}) = 1 - \frac{m^{mL_{\text{AB}}}\,m^{mL_{\text{IB}}}}{\Omega_{\text{AB}}^{mL_{\text{AB}}}\,\Omega_{\text{IB}}^{mL_{\text{IB}}}\,\Gamma(mL_{\text{AB}})\,\Gamma(mL_{\text{IB}})} \times \left(\frac{\Omega_{\text{AB}}}{m}\right)^{mL_{\text{AB}}} (mL_{\text{AB}}-1)! - \frac{m^{mL_{\text{IB}}}}{\Omega_{\text{IB}}^{mL_{\text{IB}}}\,\Gamma(mL_{\text{IB}})} \left(\frac{\Omega_{\text{AB}}}{m}\right)^{k+1} (mL_{\text{AB}}-1) \times \int_0^\infty \frac{v^{mL_{\text{AB}}-1}}{k!} \sum_{k=0}^{mL_{\text{AB}}-1} \frac{(mL_{\text{IB}}+mL_{\text{AB}}-2-k)!\, m^k}{\left[\frac{m[2^{\xi_{\text{th}}}(1+v)-1]}{\Omega_{\text{AB}}} + \frac{1}{\Omega_{\text{IB}}}\right]^{mL_{\text{IB}}+mL_{\text{AB}}-1-k}} \times 12^{\xi_{\text{th}}}(1+v) - 1^{mL_{\text{AB}}-1-k} f_{\gamma_{\text{AE}}}(v)\, dv. \quad (43)$$

Αντικαθιστώντας την (17) στην (43), η έκφραση του $P^{(I)}(\xi)$ μπορεί να ειναι από το ξαναγράφεται ως

$$P_{\text{out}}^{(I)}(\xi_{\text{th}}) = 1 - \frac{\Omega_{\text{AB}}^{mL_{\text{IB}}}\,\Omega_{\text{IE}}^{mL_{\text{IE}}}}{B(mL_{\text{AE}}, mL_{\text{IE}})} \sum_{k=0}^{mL_{\text{IB}}+mL_{\text{AB}}-2-k} \binom{mL_{\text{IB}}+mL_{\text{AB}}-2-k}{mL_{\text{IB}}-1} \times \int_0^\infty \frac{2^{-\xi_{\text{th}} mL_{\text{IB}}}\, v^{mL_{\text{IB}}+mL_{\text{AB}}-1-k}}{\left(v+1-\frac{1}{2^{\xi_{\text{th}}}}\right)^{mL_{\text{IB}}+mL_{\text{AB}}-1-k} \left(v+\Omega_{\text{E}}\right)^{mL_{\text{AE}}+mL_{\text{IE}}}} dv. \quad (45)$$

Χρησιμοποιώντας το πεπερασμένο άθροισμα [38, εξ. 1.111] και εκτελώντας κάποια βήματα απλοποίησης, η (45) μπορεί να γραφτεί ως εξής

$$P_{\text{out}}^{(I)}(\xi_{\text{th}}) = 1 - \frac{\Omega_{\text{AB}}^{mL_{\text{IB}}}\,\Omega_{\text{IE}}^{mL_{\text{IE}}}}{B(mL_{\text{AE}}, mL_{\text{IE}})} \sum_{k=0}^{mL_{\text{IB}}+mL_{\text{AB}}-2-k} \binom{mL_{\text{IB}}+mL_{\text{AB}}-2-k}{mL_{\text{IB}}-1} \times \sum_{n=0}^{mL_{\text{AB}}-1-k} \binom{mL_{\text{AB}}-1-k}{n} [1-2^{-\xi_{\text{th}}}]^{mL_{\text{AB}}-1-k-n} \times \int_0^\infty \frac{2^{-\xi_{\text{th}} mL_{\text{IB}}}\, v^{n+mL_{\text{AE}}-1}}{\left(v+1-\frac{1}{2^{\xi_{\text{th}}}}\right)^{mL_{\text{IB}}+mL_{\text{AB}}-1-k} \left(v+\Omega_{\text{E}}\right)^{mL_{\text{AE}}+mL_{\text{IE}}}} dv. \quad (46)$$

Με βάση την [38, εξίσωση 3.197], η ολοκλήρωση στην (46) αξιολογείται και η τελική ακριβής έκφραση της $P_{\text{out}}^{(I)}(\xi_{\text{th}})$ δίνεται από την (18) στο πάνω μέρος της σελίδας 5.

ΠΑΡΑΡΤΗΜΑ Γ
ΠΑΡΑΓΩΓΗ ΤΟΥ $R^{(N)}$ ΓΙΑ ΣΥΣΤΗΜΑΤΑ ΠΕΡΙΟΡΙΣΜΕΝΟΥ ΘΟΡΥΒΟΥ

Για ένα σύστημα περιορισμένου θορύβου, η έκφραση του $R_{\text{th}}^{(N)}$ ASOR, Με βάση το (21), το $R^{(N)}(\xi_{\text{th}})$ δίνεται από τη σχέση

$$R^{(N)}(\xi_{\text{th}}) = \int_0^\infty \int_0^\infty r'\, p_r(r_{\text{th}})\, p_{r'}(r')\, p_{\gamma_{\text{E}}}(y)\, dr'\, dy, \quad (47)$$

Αντικαθιστώντας την έκφραση της $p_{r'}$ της (23) στην (47), $R^{(N)}(\xi_{\text{th}})$ μπορεί να γραφτεί ως

$$R^{(N)}(\xi_{\text{th}}) = \int_0^\infty p_r(r_{\text{th}})\, p_{\gamma_{\text{E}}}(y) \frac{P_{\text{out}}^{(I)}(\xi_{\text{th}})}{2\sqrt{r}\,\sigma_{\text{AB}}} \quad (\ )$$

$$= 1 - \frac{E}{\Omega_{AB}^{mL_{AB}}\Gamma(mL_{AB})\Omega_{IB}^{mL_{IB}}\Gamma(mL_{IB})B(m_{LAE}, m_{LIE})} \times \sum_{k=0}^{m_{LIB}+m_{LAB}-2} \frac{(m_{LIB}+m_{LAB}-2-k)!}{k!}\left(\frac{\Omega_{AB}}{m}\right)^{k+1}\binom{m_{LAB}-1}{k}$$

$$\times \int_0^{\infty} \sqrt{2\pi N r'} \exp\left\{-\frac{N(r'-r_0)^2}{2\sigma_{AB}^2}\right\} dr'dy, \quad (48)$$

Μετά την αξιολόγηση της ολοκλήρωσης ως προς r′, η (48) δίνει στο

$$R^{(N)}(\xi_{th}) = \sqrt{\frac{\sigma_{AB}}{2\pi}} \int_0^{\infty} p_{r_{th}}(r) p_{\gamma_E}(y)\, dy, \quad (49)$$

Τώρα, χρησιμοποιώντας την στην (22), η έκφραση έκφραση του p του p_{γ_E} στο (N) (12), και η έκφραση του σ^{2}_{x} που δίνεται μετά την Εξίσωση (7), $R_{(\xi_{th})}$ αναδιατυπώνεται ως εξής

$$R^{(N)}_{(\xi_{th})} = \frac{\sqrt{2\pi} f_{max}^{m} \left(\frac{m}{\omega_B}\right)^{m_{LAB}}}{\Gamma(mL_{AB})\,\Gamma(mL_{AE})\,2^{-\xi_{th}(2mLAB-1)}\left(\frac{m}{\omega_E}\right)^{-mL_{AE}}} \times \int_0^{\infty} \frac{y^{mL_{AE}-1}}{\left[y+1-2^{-\xi_{th}}\right]^{-mL_{AB}+\frac{1}{2}}} \times \exp\left(-x_n \left(\frac{m2^{\xi_{th}}}{\omega_B}+\frac{m}{\omega_E}\right)\right) dy. \quad (50)$$

Εφαρμόζοντας το θεώρημα Laguerre [40], η μέση έκφραση ASOR δίνεται από την (24) στο πάνω μέρος της σελίδας 5.

Για την ειδική περίπτωση ($\xi_{th} = 0$), και με βάση την (50), η έκφραση του $R(0)$ μπορεί να απλοποιηθεί περαιτέρω ως εξής

$$R^{(N)}(0) = \frac{\sqrt{2\pi} f_{max}^{m} \left(\frac{m}{\omega_B}\right)^{m_{LAB}}}{\Gamma(mL_{AB})\,\Gamma(mL_{AE})\left(\frac{m}{\omega_E}\right)^{-mL_{AE}}} \times \int_0^{\infty} y^{m_{LAE}+m_{LAB}-\frac{3}{2}} \exp\left(-x_n\left(\frac{m}{\omega_B}+\frac{m}{\omega_E}\right)\right) dy. \quad (51)$$

Με βάση την [38, εξίσωση 3.351 3], η ολοκλήρωση στην (51) είναι και η τελική έκφραση του $R^{(N)}(0)$ δίνεται από το ακριβής μορφή (25).

Παράρτημα Δ
Παραγωγή του $R^{(I)}$ για Interference Limited Συστηματα

Με βάση την (27), η έκφραση του ASOR για ένα σύστημα περιορισμένης παρεμβολής προκύπτει ως εξής

$$R^{(I)}_{(\xi_{th})} = \int_0^{\infty}\int_0^{\infty} \beta\, p_{\beta,\beta'}(\beta_{th},\beta)\, p_{\gamma_E}(v)\, d\beta\, dv, \quad (52)$$

Η έκφραση του $p_{\beta,\beta'}$ δίνεται από [26]

$$p_{\beta,\beta'}(\beta_{th},\beta) = \int_0^{\infty}\int_{-\infty}^{\infty} \alpha_{IB}\, p_{\alpha_{AB}}(\beta\,\alpha_{IB})\, p_{\alpha'_{AB}}(\beta\,\alpha_{IB}+\beta'\alpha'_{IB}) \times p_{\alpha_{IB}}(\alpha_{IB})\, p_{\alpha'_{IB}}(\alpha'_{IB})\, d\alpha'_{IB}\, d\alpha_{IB}. \quad (53)$$

Αντικαθιστώντας την (53) στην (52) και με βάση τις λεπτομέρειες εξαγωγής του LCR στην περίπτωση της γνωστής πιθανότητας διακοπής που παρουσιάζεται στο [26], το $R_{(\xi_{th})}$ μπορεί να εκφραστεί ως εξής

$$R'_{(\xi_{th})} = \frac{\sqrt{2\pi}\Gamma(mL_{AB}+mL_{IB}-1) f_{max}}{\Gamma(m_{LAB})\,\Gamma(m_{LIB})\,2^{\frac{1}{2}}}$$

Αντικαθιστώντας την έκφραση PDF του v, που δίνεται από την (17), στην (54), $R'(\xi_{th})$ εκφράζεται ως

$$R^{(I)}(\xi_{th}) = \frac{\sqrt{2\pi}\,\Gamma(m_{LAB}+m_{LIB}-2)\,f_{max}^{\frac{1}{2}}\,\Omega_{mLIB}^{\frac{1}{2}}\,\Omega_E^{mLIE}}{2^{\xi_{th}(2mLIB-1)}\,\Gamma(m_{LAB})\,\Gamma(m_{LIB})\,B(m_{LAE},m_{LIE})} \times \int_0^{\infty} \frac{v^{vmLAE-1}\left[v+1-2^{-\xi_{th}}\right]^{m_{LAB}-2}}{(v+\Omega_E)^{mL_{AE}+mL_{IE}}\,(1-\Omega_B)^{mL_{AB}+mL_{IB}-1}} dv. \quad (55)$$

Εφαρμόζοντας το θεώρημα Laguerre, η έκφραση ASOR είναι δίνεται από την (28).

Για την ειδική περίπτωση ($\xi_{th} = 0$), και με βάση την (55), η έκφραση του $R^{(I)}(0)$ αναδιατυπώνεται ως εξής

$$R^{(I)}(0) = \frac{\sqrt{2\pi}\,\Gamma(m_{LAB}+m_{LIB}-2)\,f_{max}^{\frac{1}{2}}\,\Omega_{mLIB}^{\frac{1}{2}}\,\Omega_E^{mLIE}}{\Gamma(m_{LAB})\,\Gamma(m_{LIB})\,B(m_{LAE},m_{LIE})} \times \int_0^{\infty} \frac{v^{m_{LAB}+m_{LAE}-\frac{3}{2}}}{(v+\Omega_E)^{m_{LAE}+m_{LIE}}\,(v+\Omega_B)^{m_{LAB}+m_{LIB}}} dv. \quad (56)$$

Με βάση την [38, εξίσωση 3.197], η ολοκλήρωση στην (56) αξιολογείται και η τελική έκφραση του $R^{(I)}(0)$ δίνεται από την ακριβή μορφή (29) στη σελίδα 5.

Αναφορες

[1] T. M. Hoang, T. Q. Duong, N.-S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly jammer," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 174-177, Apr. 2017.

[2] S. Iwata, T. Ohtsuki και P.-Y. Kam, "A lower bound on secrecy capacity for MIMO wiretap channel aided by a cooperative jammer with channel estimation error," *IEEE Access*, vol. 5, pp. 4636-4645, Mar. 2017.

[3] Y. J. Tolossa, S. Vuppala, and G. Abreu, "Secrecy-rate analysis in multitier heterogeneous networks under generalized fading model," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 101-110, Feb. 2017.

[4] H.-M. Wang και X.-G. Xia, "Enhancing wireless secrecy via cooperation: *IEEE Commun. Mag,*
(vol. 12, Ιαν. 47-53.

[5] W. K. Harrison και S. W. McLaughlin, "Tandem coding and cryptography on wiretap channels: EXIT chart analysis," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun./Jul. 2009, σσ. 1939-1943.

[6] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin και J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, τόμος 53, αριθ. 8, σ. 2933-2945, Αύγουστος 2007.
και συμφωνία κλειδιών", *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, σελ. 1472-1483, Οκτ. 2012.

[8] M. Bloch, M. Debbah, Y. Liang, Y. Oohama, and A. Thangaraj, "Special issue on physical-layer security," *J. Commun. Netw.*, vol. 14, no. 4,
σελ. 349-351, Αύγουστος 2012.

[9] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, τ. 54, αριθ. 8, σελ. 1355-1387, 1975.

[10] A. Salem and K. A. Hamdi, "Improving physical layer security of AF relay networks via beam-forming and jamming," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC)-Fall*, Σεπ. 2016, σσ. 1-5.

[11] S. Leung-Yan-Cheong και M. E. Hellman, "The Gaussian wire-tap καναλι," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, σ. 451-456, Ιουλ. 1978.

$$\times \int_{0}^{\infty} \{ p_{\lambda_E}(v) \frac{\Omega_B m_{LIB} - 2 \left[\Sigma_{\xi th} \left(1 + v \right) - 1 \right]_{mLAB} - 2}{\left(1 + v \right) - 1 + \Omega_B} \frac{imL_{AB} + mL_{IB}}{2\eta} - 1 \, dv.$$

[12] R. Negi and S. Goel, "Secret communication using artificial noise," στο *Proc. IEEE 62nd Veh. Technol. Conf. (VTC-Fall)*, Σεπ. 2005, σελ. 1906-1910.

[13] S. Goel and R. Negi, "Guaranteing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, τόμος 7, αριθ. 6, σ. 2180-2189, Ιούν. 2008.

[14] X. Zhou και M. McKay, "Ασφάλεια φυσικού επιπέδου με τεχνητό θόρυβο: *Proc. Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Σεπ. 2009, σ. 1-5.
[15] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470-1482, Jun. 2017.
[16] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, σελ. 4347-4362, Νοέμβριος 2015.
[17] K. Tourki and M. O. Hasna, "A collaboration incentive exploiting the primary-secondary systems' cross interference for PHY security enhancement," *IEEE J. Sel. Topics Signal Process.*, τόμος 10, αριθ. 8, σελ. 1346-1358, Δεκέμβριος 2016.
[18] K. Tourki and M. O. Hasna, "Proactive spectrum sharing incentive for physical layer security enhancement using outdated CSI," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 6273-6283, Sep. 2016.
[19] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive secure transmission for physical layer security in cooperative wireless networks," *IEEE Commun. Lett.*, vol. 21, no. 3, σελ. 524-527, Μαρ. 2017.
[20] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, σ. 1875-1888, Μάρτιος 2010.
[21] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985-4997, Oct. 2011.
[22] W. Wang, K. C. Teh, and K. H. Li, "Relay selection for secure successive AF relaying networks with untrusted nodes," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2466-2476, Nov. 2016.
[23] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, σελ. 1678-1690, Μάιος 2014.
[24] N. Bhargav, S. L. Cotton και D. E. Simmons, "Ανάλυση χωρητικότητας μυστικότητας σε κανάλια κ-μ εξασθένισης: *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3011-3024, Jul. 2016.
[25] O. Gungor, C. E. Koksal, and H. El Gamal, "On secrecy outage capacity of fading channels under relaxed delay constraints," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2013, pp. 2024-2028.
[26] L. Yang και M. S. Alouini, "On the average outage rate and aver- age outage duration of wireless communication systems with multiple cochannel interferers," *IEEE Trans. Wireless Commun.*, vol. 3, no. 4, σελ. 1142-1153, Ιουλ. 2004.
[27] A. Olutayo, H. Ma, J. Cheng, and J. F. Holzman, "Level crossing rate and average fade duration for the Beaulieu-Xie fading model," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, σελ. 326-329, Ιούν. 2017.
[28] X. Dong and N. C. Beaulieu, "Average level crossing rate and average fade duration of selection diversity," *IEEE Commun. Lett.*, τόμος 5, αριθ. 10, σελ. 396-398, Οκτ. 2001.
[29] L. Yang, M. O. Hasna, and M. S. Alouini, "Average outage duration of multihop communication systems with regenerative relays," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, σ. 1366-1371, Ιουλ. 2005.
[30] L. Yang και M.-S. Alouini, "Level crossing rate over multiple independent random processes: *IEEE Trans. Wireless Commun.*, τόμος 6, αριθ. 12, σ. 4280-4284, Δεκέμβριος 2007.
[31] K. Otani, K. Daikoku, and H. Omori, "Burst error performance encountered in digital land mobile radio channel," *IEEE Trans. Veh. Technol.*, vol. VT-30, no. 4, σελ. 156-160, Νοεμβρίου 1981.
[32] Z. Cao και Y.-D. Yao, "Definition and drivation of level crossing rate and average fade duration in an interference-limited environment," in *Proc. IEEE 54th Veh. Technol. Conf. (VTC-Fall)*, Οκτ. 2001, σσ. 1608-1611.
[33] M. Patzold and F. Laue, "Level-crossing rate and average duration of fades of deterministic simulation models for Rice fading channels," *IEEE Trans. Veh. Technol.*, vol. 48, no. 4, σ. 1121-1129, Ιουλ. 1999.
[34] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.
[35] X. Chen, X. Chen, and T. Liu, "A unified performance optimization for secrecy wireless information and power transfer over interference channels," *IEEE Access*, vol. 5, pp. 12726-12736, Jul. 2017.
[36] D. B. Rawat, T. White, S. Parwez, C. Bajracharya, and M. Song, "Evaluating secrecy outage of physical layer security in large-scale MIMO wireless communications for cyber-physical systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1987-1993, Dec. 2017.
[37] N. Balakrishnan N. L. Johnson, and S. Kotz, *Continuous Univariate Distributions*, vol. 2, 2nd ed. Hoboken, NJ, USA: Wiley, 1995.
[38] D. Zwillinger, *Table of Integrals, Series, and Products*, 8η έκδοση. San Diego, CA, USA: Academic, 2014.
[39] G. L. Stuber, *Principles of Mobile Communication*, 4η έκδοση. New York, NY, USA: Springer, 2017.
[40] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*. Νέα Υόρκη, Νέα Υόρκη, ΗΠΑ: Dover, 1965.

Ο Aymen Omri (M'13) έλαβε το πτυχίο μηχανικού τηλεπικοινωνιών από την Ακαδημία Αεροπορίας της Τυνησίας το 2007 και τα πτυχία M.Res. και Ph.D. στις τηλεπικοινωνίες από την Εθνική Σχολή Μηχανικών της Τύνιδας, Πανεπιστήμιο Tunis El Manar της Τυνησίας, το 2009 και το 2012.

Από το 2010 έως το 2012, ήταν βοηθός έρευνας στο Τμήμα Ηλεκτρολόγων Μηχανικών του Πανεπιστημίου του Κατάρ, στο Κατάρ, όπου σήμερα είναι μεταδιδακτορικός ερευνητής. Τα ερευνητικά του ενδιαφέροντα περιλαμβάνουν τη μοντελοποίηση, το σχεδιασμό και την ανάλυση επιδόσεων συρμάτινων λιγότερα συστήματα επικοινωνίας. Τα τρέχοντα ερευνητικά του ενδιαφέροντα περιλαμβάνουν τις επικοινωνίες μεταξύ συσκευών, τα δίκτυα που βασίζονται σε UAV και τα ασύρματα δίκτυα επικοινωνίας πέμπτης γενιάς.

Ο Mazen O. Hasna (S'94-M'03-SM'07) έλαβε το βραβείο Πτυχίο B.S. από το Πανεπιστήμιο του Κατάρ, Ντόχα, Κατάρ, το 1994, πτυχίο M.S. από το Πανεπιστήμιο της Νότιας Καλιφόρνιας στο Λος Άντζελες, Λος Άντζελες, Καλιφόρνια, ΗΠΑ, το 1998, και διδακτορικό δίπλωμα από το Πανεπιστήμιο της Μινεσότα Twin Cities, Μινεάπολη, MN, ΗΠΑ, το 2003, όλα στον τομέα της ηλεκτρολογίας. Το 2003 εντάχθηκε στο Τμήμα Ηλεκτρολόγων Μηχανικών του Πανεπιστημίου του Κατάρ, όπου σήμερα είναι αναπληρωτής καθηγητής.

Τα ερευνητικά του ενδιαφέροντα περιλαμβάνουν τη γενική περιοχή της θεωρίας ψηφιακών επικοινωνιών και την εφαρμογή της στην αξιολόγηση της απόδοσης ασύρματων συστημάτων επικοινωνίας σε κανάλια εξασθένισης. Τα τρέχοντα ειδικά ερευνητικά του ενδιαφέροντα περιλαμβάνουν τις συνεργατικές επικοινωνίες, τα δίκτυα που βασίζονται σε UAV, την ασφάλεια φυσικού στρώματος και τα υβριδικά δίκτυα FSO/RF.