ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Έλεγχος Έξυπνων Παρεμβολών στο Διαδίκτυο των Αντικειμένων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΙΩΑΝΝΗ ΓΕΩΡΓΟΥΛΙΑ

Επιβλέπων Καθηγητής:

Συμεών Παπαβασιλείου

Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2017

Έλεγχος Έξυπνων Παρεμβολών στο Διαδίκτυο των Αντικειμένων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΙΩΑΝΝΗ ΓΕΩΡΓΟΥΛΙΑ

Επιβλέπων Καθηγητής:

Συμεών Παπαβασιλείου

Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 25 Οκτωβρίου 2017

…… …… ……

Σ. Παπαβασιλείου Θ. Βαρβαρίγου Ι. Ρουσσάκη

Καθηγητής Ε.Μ.Π. Καθηγήτρια Ε.Μ.Π. Επίκ. Καθηγήτρια Ε.Μ.Π.

Αθήνα, Οκτώβριος 2017

……

ΙΩΑΝΝΗΣ ΓΕΩΡΓΟΥΛΙΑΣ

Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

ΠΕΡΙΛΗΨΗ

Σε αυτήν την διπλωματική εργασία εξετάζεται το πρόβλημα ελέγχου έξυπνης παρεμβολής στο Διαδίκτυο των Αντικειμένων με έμφαση στα παθητικά δίκτυα αναγνώρισης μέσω ραδιοσυχνοτήτων(RFID). Ένας έξυπνος παρεμβολέας/ενεργή RFID ετικέτα επιτίθεται στην μετάδοση δεδομένων κανονικών παθητικών RFID ετικετών μέσω γρήγορου ελέγχου και προσαρμογής της ισχύος μετάδοσής του προκειμένου να μεγιστοποιήσει την ζημιά, δηλαδή μη-ανάγνωση των δεδομένων των κανονικών RFID ετικετών από τον RFID αναγνώστη. Αρχικά, ο συνολικός αριθμός των υποκαναλιών κατανέμεται στις κανονικές ετικέτες με βάση την τεχνική μέγιστου κέρδους καναλιού. Στη συνέχεια το πρόβλημα ελέγχου έξυπνης παρεμβολής διαμορφώνεται ως ένα Stackelberg παίγνιο σε κάθε υποκανάλι, όπου η κανονική ετικέτα είναι ο ηγέτης και ο έξυπνος παρεμβολέας είναι ο ακόλουθος. Ο στόχος κάθε παίκτη, δηλαδή κανονικής ετικέτας και έξυπνου παρεμβολέα, είναι η μεγιστοποίηση της χρησιμότητάς του. Η ύπαρξη και η μοναδικότητα της Stackelberg ισορροπίας αποδεικνύεται ενώ εξάγονται και κλειστοί τύποι της βέλτιστης στρατηγικής ισχύος αντανάκλασης των κανονικών ετικετών και της καλύτερης στρατηγικής ισχύος μετάδοσης του παρεμβολέα. Η απόδοση της προτεινόμενης προσέγγισης αξιολογείται μέσω μοντελοποίησης και προσομοίωσης και η ανωτερότητά της συγκριτικά με άλλες σύγχρονες προσεγγίσεις απεικονίζεται μέσω λεπτομερών αριθμητικών αποτελεσμάτων.

Λέξεις Κλειδιά<<Έξυπνη παρεμβολή, Διαδίκτυο των Αντικειμένων, RFID, Stackelberg ισορροπία, Άρνηση παροχής Υπηρεσιών>>

ABSTRACT

In this diploma thesis the problem of intelligent jamming defense control in the Internet of Things focusing on passive Radio Frequency Identification (RFID) networks is addressed. An intelligent jammer/active RFID tag attacks the normal passive RFID tag's data transmission per each subchannel via quickly controlling and adapting its transmission power to maximize the damage, i.e., non-read normal tags by the RFID reader. Initially, the total number of subchannels is allocated to the normal tags based on the maximum channel gain technique. Then, the intelligent jamming control problem is formulated as a Stackelberg game per each subchannel, where the normal tag is the leader and the intelligent jammer is the follower. The goal of each player, i.e., normal tag and intelligent jammer is to maximize its utility. The existence and uniqueness of the Stackelberg Equilibrium is proved and closed formulas of the normal tags' optimal reflection power and jammer's best response transmission power strategy are derived. The performance of the proposed approach is evaluated via modeling and simulation and its superiority compared to other state of the art approaches is illustrated by detailed numerical results.

Keywords<<Intelligent jamming, Internet of Things, RFID, Stackelberg Equilibrium, Denial of Service>>

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω ιδιαιτέρως τον επιβλέποντα καθηγητή της παρούσας διπλωματικής εργασίας, κ. Συμεών Παπαβασιλείου, τόσο για το ότι μου ανέθεσε ένα τόσο επιστημονικά ενδιαφέρον θέμα, όσο και για την πολύτιμη βοήθεια που μου προσέφερε. Επίσης θα ήθελα να ευχαριστήσω θερμά τη επίκουρη καθηγήτρια κ. Ειρήνη-Ελένη Τσιροπούλου για την συνεχή καθοδήγηση και υποστήριξη που μου παρείχε αλλά και για την άριστη συνεργασία που είχαμε καθ' όλη τη διάρκεια εκπόνησης της εργασίας. Τέλος, θα ήταν παράλειψη αν δεν ευχαριστούσα τους γονείς μου για την στήριξη που μου προσέφεραν στα χρόνια των σπουδών μου στο Πολυτεχνείο.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

1.1 Πρόλογος

2.2 Αντικείμενο της Διπλωματικής Εργασίας

2.3 Δομή της Διπλωματικής Εργασίας

1.1 Πρόλογος

Ο όρος "Διαδίκτυο των Αντικειμένων(Internet of Things)" χρησιμοποιήθηκε πρώτη φορά από τον Kevin Ashton το 1999 για να περιγράψει ένα σύστημα όπου αντικείμενα του φυσικού κόσμου θα μπορούσαν να συνδεθούν στο Διαδίκτυο μέσω αισθητήρων[1]. Συγκεκριμένα, δημιούργησε τον όρο για να απεικονίσει την δυνατότητα αξιοποίησης της τεχνολογίας αναγνώρισης μέσω ραδιοσυχνοτήτων στις εφοδιαστικές αλυσίδες προκειμένου να μετρούνται και να εντοπίζονται προϊόντα χωρίς την ανάγκη ανθρώπινης παρέμβασης. Σήμερα, ο προαναφερθέν όρος έχει γίνει ιδιαίτερα δημοφιλής περιγράφοντας σενάρια όπου η δυνατότητα σύνδεσης στο Διαδίκτυο και η υπολογιστική ικανότητα έχουν επεκταθεί σε διάφορες συσκευές, αισθητήρες και αντικείμενα καθημερινής χρήσης.

Το Διαδίκτυο των Αντικειμένων αποτελεί λοιπόν μείζονος σημασίας για την τεχνολογική βιομηχανία, την πολιτική, την οικονομία, την υγεία και διάφορους άλλους τομείς, όντας ενσωματωμένο σε ένα ευρύ φάσμα δικτυωμένων προϊόντων, συστημάτων και αισθητήρων, τα οποία εκμεταλλεύονται τις εξελίξεις γύρω από την υπολογιστική ισχύ, την σμίκρυνση ηλεκτρονικών συστημάτων και τις διασυνδέσεις των δικτύων, προκειμένου να προσφέρουν νέες δυνατότητες που δεν υπήρχαν προηγουμένως.

Πιο αναλυτικά, η μεγάλης κλίμακας εφαρμογή των IoT συσκευών υπόσχεται την μεταμόρφωση πολλών πτυχών του τρόπου ζωής των ανθρώπων. Για τους καταναλωτές, τα νέα IoT προϊόντα, όπως οι συσκευές με πρόσβαση στο Διαδίκτυο, τα εξαρτήματα αυτοματισμού για το σπίτι, οι συσκευές διαχείρισης ενέργειας κλπ οδηγούν προς την κατεύθυνση της δημιουργίας του "έξυπνου σπιτιού", προσφέροντας περισσότερη ασφάλεια και καλύτερη ενεργειακά απόδοση. Άλλες προσωπικές IoT συσκευές, όπως οι φορητές συσκευές παρακολούθησης της υγείας και της φυσικής κατάστασης και οι ιατρικές συσκευές με δυνατότητα πρόσβασης σε δίκτυο, αλλάζουν τον τρόπο με τον οποίο παρέχονται οι υπηρεσίες υγειονομικής περίθαλψης. Τα προαναφερθέντα εμφανίζονται ως ιδιαίτερα επωφελή για τους ηλικιωμένους και τα άτομα με αναπηρία, οδηγώντας σε βελτιωμένη ποιότητα ζωής μέσα σε λογικά πλαίσια κόστους. Επιπλέον, IoT συστήματα όπως δικτυωμένα οχήματα, έξυπνα συστήματα κυκλοφορίας, και αισθητήρες ενσωματωμένοι σε δρόμους και γέφυρες, φέρνουν όλο και πιο κοντά μας την ιδέα της "έξυπνης πόλης", η οποία συμβάλει στην ελαχιστοποίηση της κυκλοφοριακής συμφόρησης και της κατανάλωσης ενέργειας. Παράλληλα, η IoT τεχνολογία προσφέρει νέες δυνατότητες στον μετασχηματισμό της γεωργίας, της βιομηχανίας και της παραγωγής και διανομής ενέργειας αυξάνοντας την διαθεσιμότητα των πληροφοριών κατά μήκος της αλυσίδας παραγωγής με χρήση διασυνδεδεμένων αισθητήρων. Ωστόσο, παράλληλα με όλα αυτά, θα πρέπει να ληφθούν υπόψη και να αντιμετωπιστούν πολλά ζητήματα και νέες προκλήσεις που γεννιούνται, προκειμένου να οδηγηθούμε στα πιθανά οφέλη που προαναφέρθηκαν και που προκύπτουν γενικότερα από την εκμετάλλευση του IoT.

Ορισμένες εταιρίες και ερευνητικοί οργανισμοί έχουν προσφέρει μεγάλο εύρος προβλέψεων σχετικά με τις πιθανές επιπτώσεις του IoT στο Διαδίκτυο και την οικονομία κατά την διάρκεια των επόμενων χρόνων. Η Cisco, για παράδειγμα, προβλέπει περισσότερα από 24 δισεκατομμύρια αντικείμενα συνδεδεμένα στο Διαδίκτυο μέχρι το

2019[2]. Η Morgan Stanley προβλέπει 75 δισεκατομμύρια δικτυακές συσκευές μέχρι το 2020[3]. Η Huawei ανεβάζει τον πήχη ακόμα ψηλότερα προβλέποντας 100 δισεκατομμύρια IoT συνδέσεις μέχρι το 2025[4] ενώ η McKinsey Global Institute αναφέρει ότι οι επιπτώσεις του IoT στην παγκόσμια οικονομία μπορεί να είναι από 3.9 έως 11.1 τρισεκατομμύρια δολάρια μέχρι το 2025[5]. Ενώ η μεταβλητότητα των προβλέψεων καθιστά οποιοδήποτε συγκεκριμένο αριθμό υπό αμφισβήτηση, όλες μαζί οδηγούν στο συμπέρασμα σημαντικής ανάπτυξης και επιρροής του Διαδικτύου των Αντικειμένων.

Από μία οπτική γωνία λοιπόν παρουσιάζεται το IoT ως ένας επαναστατικός, πλήρως διασυνδεδεμένος "έξυπνος κόσμος" προόδου, αποτελεσματικότητας, και ευκαιριών, με την δυνατότητα προσθήκης δισεκατομμυρίων στην βιομηχανία και την παγκόσμια οικονομία[6]. Από την άλλη, αντιμετωπίζεται από πολλούς ως ένας πιο σκοτεινός κόσμος εποπτείας, παραβίασης της ιδιωτικότητας και της ασφάλειας, και "κλειδώματος" των καταναλωτών οδηγώντας λοιπόν σε πολλούς κινδύνους όπως πειρατεία των αυτοκινήτων που συνδέονται στο Διαδίκτυο[7], ενδεχόμενο εποπτείας λόγω των χαρακτηριστικών αναγνώρισης φωνής των έξυπνων τηλεοράσεων[8], παραβίαση της ιδιωτικότητας εξαιτίας κακής και αφελούς χρήσης των IoT δεδομένων[9] και άλλους πολλούς.

Καθώς λοιπόν το IoT προσφέρει συνεχώς νέες δυνατότητες με πολλαπλά οφέλη για τους ανθρώπους, δημιουργούνται παράλληλα νέα προβλήματα και προκλήσεις που παρεμποδίζουν την ομαλή λειτουργία του πρώτου, με τις τελευταίες να αφορούν κυρίως τους τομείς της ασφάλειας, της ιδιωτικότητας, της διαλειτουργικότητας και των προτύπων, των νομικών και ρυθμιστικών θεμάτων, και των θεμάτων περί δικαιωμάτων.

1.2 Αντικείμενο της Διπλωματικής Εργασίας

Αντικείμενο της παρούσας διπλωματικής εργασίας αποτελεί ο έλεγχος επιθέσεων έξυπνης παρεμβολής στο Διαδίκτυο των Αντικειμένων, με έμφαση στα παθητικά δίκτυα αναγνώρισης μέσω ραδιοσυχνοτήτων. Στόχος των παρεμβολέων είναι η διακοπή της ομαλής λειτουργίας του δικτύου, επεμβαίνοντας στην μετάδοση των πληροφοριών των κανονικών χρηστών και επιδιώκοντας να παρεμποδίσουν την επίτευξή της, η οποία αποτελεί προφανώς τον στόχο των τελευταίων και η αξιολόγηση της βασίζεται στον σηματοθορυβικό λόγο που επιδιώκεται να επιτευχθεί από αυτούς.

Στα πλαίσια λοιπόν των παραπάνω, θεωρείται ένα παθητικό δίκτυο αναγνώρισης μέσω ραδιοσυχνοτήτων που αποτελείται από έναν αναγνώστη, διάφορους αναμεταδότες που εκπέμπουν μέσω αντανάκλασης τις πληροφορίες τους στον πρώτο, και έναν παρεμβολέα, ο οποίος έχει την δυνατότητα να ελέγχει και να προσαρμόζει έξυπνα την ισχύ μετάδοσής του επιδιώκοντας να παρεμποδίσει τους αναμεταδότες να αντανακλάσουν τις πληροφορίες τους στον αναγνώστη. Η συνύπαρξη των προαναφερθέντων διατυπώνεται ως ένα Stackelberg παίγνιο με τον αναμεταδότη να είναι ο ηγέτης και τον παρεμβολέα ο ακόλουθος.

Επιπλέον, προκειμένου να προσομοιώσουμε την συμπεριφορά τους κάτω από ένα κοινό πλαίσιο βελτιστοποίησης, υιοθετείται η έννοια της συνάρτησης χρησιμότητας, η οποία εκφράζει την ικανοποίησή τους σε σχέση με την επίτευξη του στόχου τους,

προσαρμοσμένη φυσικά στον καθένα. Αναμεταδότης και παρεμβολέας, επιδιώκουν να μεγιστοποιήσουν την προαναφερθείσα, ελέγχοντας την ισχύ ανάκλασης και μετάδοσης αντίστοιχα, με το παιχνίδι να καταλήγει σε ισορροπία έχοντας ο καθένας ακολουθήσει την βέλτιστη στρατηγική.

Η απόδοση του προτεινόμενου πλαισίου για την αντιμετώπιση της παρεμβολής αξιολογείται μέσω μοντελοποίησης και προσομοίωσης ενώ η ανωτερότητά της συγκριτικά με άλλες σύγχρονες προσεγγίσεις απεικονίζεται μέσω λεπτομερών αριθμητικών αποτελεσμάτων.

1.3 Δομή της Διπλωματικής Εργασίας

Στην υποενότητα αυτή γίνεται μια σύντομη αναφορά στα κεφάλαια της παρούσας διπλωματικής εργασίας. Συγκεκριμένα, στο κεφάλαιο 2 γίνεται μια αναφορά σε μελέτες που αφορούν το πρόβλημα της βέλτιστης κατανομής πόρων σε ένα ασύρματο δίκτυο, εστιάζοντας στην άνω ζεύξη της γραμμής μεταφοράς, και τονίζεται αφενός πως διαμορφώνεται η συνύπαρξη εγωιστών χρηστών σε ένα δίκτυο και αφετέρου πως προσομοιώνεται η συμπεριφορά τους με την υιοθέτηση της συνάρτησης χρησιμότητας. Στο κεφάλαιο 3, μελετάται πως επηρεάζεται ένα δίκτυο από την προσθήκη κακόβουλου παρεμβολέα, ο οποίος επιθυμεί την υποβάθμιση της απόδοσης των εγωιστών χρηστών, και παραθέτονται μελέτες που δείχνουν πως έχει διαμορφωθεί η θεωρία γύρω από το πρόβλημα των παρεμβολών σήμερα. Τα κεφάλαια 2 και 3 θεμελιώνουν ουσιαστικά πως οδηγηθήκαμε σταδιακά στο πρόβλημα που καλούμαστε να μελετήσουμε και στην θεωρία και τα εργαλεία που θα χρησιμοποιήσουμε. Στο κεφάλαιο 4 διατυπώνεται το πρόβλημα που θα μελετήσουμε, το μοντέλο συστήματος και οι παράμετροί του, καθώς και τα εργαλεία επίλυσης, ενώ στη συνέχεια παρουσιάζεται η λύση του διεξοδικά. Στο κεφάλαιο 5, παρουσιάζονται οι διάφορες προσομοιώσεις που πραγματοποιήθηκαν καθώς και τα αριθμητικά αποτελέσματα που προέκυψαν. Μάλιστα, γίνεται σύγκριση τόσο μεταξύ τους όσο και με αποτελέσματα άλλων σύγχρονων μελετών ώστε αξιολογηθεί η απόδοση του προτεινόμενου πλαισίου και να απεικονιστεί η ανωτερότητά του συγκριτικά με τις προαναφερθείσες. Τέλος στο κεφάλαιο 6 συνοψίζονται τα βασικά συμπεράσματα που προκύπτουν και γίνεται μια εκτίμηση των μελλοντικών επεκτάσεων της παρούσας ερευνητικής μελέτης.

ΚΕΦΑΛΑΙΟ 2

ΔΙΑΧΕΙΡΙΣΗ ΠΟΡΩΝ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

2.1 Εισαγωγικά

2.2 Κατανομή πόρων σε ασύρματα CDMA κυψελωτά δίκτυα

2.3Κατανομή πόρων σε ασύρματα SC-FDMA κυψελωτά δίκτυα

2.4 Κατανομή πόρων σε ασύρματα NOMA κυψελωτά δίκτυα

2.5 Κατανομή πόρων σε φεμτοκυψέλες

2.6 Κατανομή πόρων σε περιβάλλοντα επικοινωνίας συσκευής προς συσκευή

2.7 Κατανομή πόρων στο Διαδίκτυο των Αντικειμένων

2.1 Εισαγωγικά

Όπως έχει καταστεί σαφές, τα δίκτυα ασύρματης επικοινωνίας έχουν πρωτοφανή επίδραση στην παγκόσμια κοινότητα εισβάλοντας στην καθημερινότητα των ανθρώπων. Η εμφάνιση των υπηρεσιών σύννεφου, η επικοινωνία συσκευής με συσκευή, η παροχή υπηρεσιών video στα έξυπνα κινητά και γενικότερα οι απαιτητικές συσκευές και υπηρεσίες σε χωρητικότητα δεδομένων και εύρος ζώνης συχνοτήτων, οδηγούν σε αύξηση των δεδομένων που ζητούν οι χρήστες και διακινούνται σε ένα δίκτυο. Καθώς λοιπόν αυξάνεται συνεχώς ο αριθμός των χρηστών που εκμεταλλεύονται τα ασύρματα δίκτυα και τις δυνατότητές τους, αυξάνονται παράλληλα και οι καταναλισκόμενοι πόροι καθώς και οι προσδοκίες για την ποιότητα των υπηρεσιών που παρέχονται από αυτά. Έτσι, σημαντικές ερευνητικές προσπάθειες έχουν αφιερωθεί στο πρόβλημα της αποδοτικής διαχείρισης και κατανομής των περιορισμένων πόρων ενός συστήματος όπως το εύρος ζώνης, η ισχύς εκπομπής και ο ρυθμός μετάδοσης δεδομένων στα ασύρματα κυψελωτά δίκτυα με στόχο την επίτευξη μέγιστης απόδοσης και ικανοποίησης των απαιτήσεων των χρηστών(Quality of Service-QoS) [10], [11], [40], [35], [38], [56].

Κυρίαρχο ρόλο στην μελέτη του προαναφερθέν προβλήματος κατέχει η θεωρία παιγνίων και η συνάρτηση χρησιμότητας, η οποία αποτελεί ένα μαθηματικό εργαλείο από τον κλάδο της οικονομικής επιστήμης η οποία διευκολύνει τη μελέτη ενός δικτύου δίνοντας νέα διάσταση στην έννοια της βέλτιστης κατανομής πόρων και κατ' επέκταση της βέλτιστης απόδοσης ενός δικτύου. Πιο συγκεκριμένα, εισάγει την έννοια της ικανοποίησης και ευημερίας ενός χρήστη εκφράζοντας ουσιαστικά πόσο ευχαριστημένος είναι με τους πόρους που του έχουν ανατεθεί για την υπηρεσία που έχει ζητήσει. Το παραπάνω αποτελεί σπουδαία καινοτομία καθώς αξιοποιείται για την ανάλυση της συμπεριφοράς του χρήστη ποσοτικοποιώντας την. Οι συναρτήσεις χρησιμότητας έχουν ήδη υιοθετηθεί σε πολλαπλά ερευνητικά πεδία με σκοπό την ποσοτικοποίηση της λαμβανόμενης ευχαρίστησης του χρήστη, π.χ., κατά την περιήγησή του σε ένα μουσείο [66] – [68].

Στη συνέχεια γίνεται μια ανασκόπηση σε προηγούμενες μελέτες της ερευνητικής μας ομάδας που αφορούν το πρόβλημα της βέλτιστης κατανομής πόρων και εστιάζουν στην άνω ζεύξη της γραμμής μεταφοράς του ασύρματου δικτύου αποτελώντας μια σφαιρική εικόνα της προσέγγισης που έχει γίνει γενικότερα με πλήθος αναφορών και συγκρίσεις με άλλες μελέτες. Πιο αναλυτικά, έχει ληφθεί υπόψη η ποικιλία των τεχνικών κωδικοποίησης που υπάρχουν (CDMA, SC-FDMA, NOMA), η ετερογένεια των δικτύων (απλά κυψελωτά, πολυεπίπεδες φεμτοκυψέλες), η διαφορετικότητα των υπηρεσιών (πραγματικού και μη πραγματικού χρόνου), η ποικιλία των πόρων του δικτύου που χρήζουν ιδιαίτερης προσοχής (ισχύς εκπομπής, ρυθμός μετάδοσης δεδομένων, εύρος ζώνης συχνοτήτων) καθώς και η μορφή της συνάρτησης χρησιμότητας (κυρτή, γραμμική, κοίλη). Επίσης έχουν μελετηθεί περιβάλλοντα όπου έγινε χρήση του ορατού φωτός αλλά και της απευθείας επικοινωνίας συσκευής με συσκευή, χωρίς δηλαδή την παρεμβολή του σταθμού βάσης, οδηγούμενοι από τα δίκτυα τρίτης και τέταρτης γενιάς σε αυτό που αποκαλούμε σήμερα Διαδίκτυο των Αντικειμένων.

2.2 Κατανομή πόρων σε ασύρματα CDMA κυψελωτά δίκτυα

Τα εσωτερικά χαρακτηριστικά των ασύρματων επικοινωνιών στα σύγχρονα κυψελωτά συστήματα πολλαπλής πρόσβασης με διαίρεση κώδικα (Code Division Multiple Access-CDMA), όσον αφορά τους σπάνιους ραδιοφωνικούς πόρους του δικτύου, τους φυσικούς περιορισμούς των κινητών κόμβων και τις συνθήκες καναλιού που ποικίλουν ανάλογα με το χρόνο, ανάγκασαν και ενθάρρυναν την υιοθέτηση του ελέγχου της ισχύος εκπομπής των χρηστών, τόσο για την άνω όσο και την κάτω ζεύξη, με στόχο την αποδοτική κατανομή των πόρων και την διαχείριση της παρεμβολής.

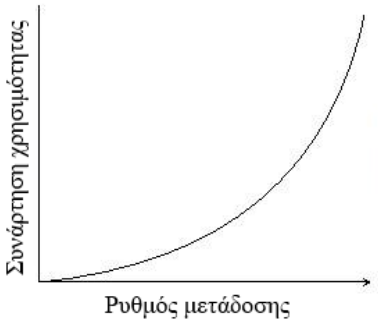
Αρχικά εξετάστηκε το πρόβλημα της αποδοτικής κατανομής της ισχύος στην άνω ζεύξη ενός μονοκυψελωτού ασύρματου CDMA δικτύου με χρονοθυρίδες, δίνοντας έμφαση στην εκπλήρωση των προϋποθέσεων των υπηρεσιών πραγματικού χρόνου [12]. Το αντίστοιχο πρόβλημα διατυπώθηκε ως ένα μη συνεργατικό παιχνίδι όπου οι χρήστες στοχεύουν εγωιστικά στη μεγιστοποίηση της απόδοσής τους βάσει της συνάρτησης χρησιμότητάς τους, κάτω από τους επιβαλλόμενους φυσικούς περιορισμούς, οδηγώντας συνολικά στην μέγιστη αποτελεσματικότητα του συστήματος. Η χρησιμότητα ενός χρήστη αντανακλά το βαθμό ικανοποίησής του σε σχέση με την πραγματική του απόδοση, την εκπλήρωση των προϋποθέσεων ποιότητας της υπηρεσίας και την αντίστοιχη ελάχιστη απαιτούμενη κατανάλωση ενέργειας.

Η ύπαρξη και η μοναδικότητα του σημείου ισορροπίας κατά Nash του προτεινόμενου παιγνίου αποδείχτηκε, όπου όλοι οι χρήστες έχουν επιτύχει την επιθυμητή τιμή σηματοθορυβικού λόγου ή μεταδίδουν με τη μέγιστη ισχύ εκπομπής τους, οδηγώντας ουσιαστικά σε ισορροπία το δίκτυο. Οι ιδιότητες της παραπάνω ισορροπίας μελετήθηκαν αναλυτικά ενώ ποσοτικοποιήθηκε η αμοιβαία αντιστάθμιση μεταξύ της συνολικής απόδοσης των χρηστών και των αυστηρών απαιτήσεων των υπηρεσιών πραγματικού χρόνου, ως προς την ποιότητα της υπηρεσίας.

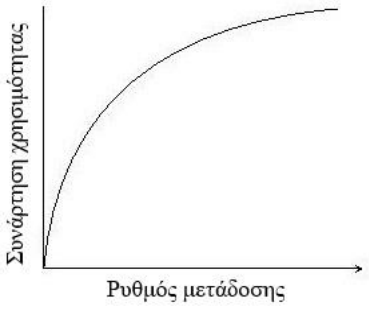
Στη συνέχεια μελετήθηκε το πρόβλημα της κατανομής ισχύος με έμφαση στην υποστήριξη πολλαπλών υπηρεσιών (πραγματικού και μη πραγματικού χρόνου) με ποικίλες και συχνά διαφορετικές QoS προϋποθέσεις μέσω της θεωρίας παιγνίων [13]. Μια από τις θεμελιώδεις διαφορές στην συγκεκριμένη μελέτη, συγκριτικά με αυτές της υπόλοιπης βιβλιογραφίας, έγκειται στον ορισμό και τη μεταχείριση της συνάρτησης χρησιμότητας των χρηστών προκειμένου να εκπληρωθούν ταυτόχρονα οι απαιτήσεις απόδοσης των πολλαπλών υπηρεσιών σε ένα περιβάλλον χρονικής διακύμανσης, όπου οι επιδόσεις των προαναφερθέντων είναι συγγενικές. Συγκεκριμένα, αντί να εκφράζουν απλά την αμοιβαία αντιστάθμιση μεταξύ του αριθμού των αξιόπιστα μεταδιδόμενων bits του κάθε χρήστη και της αντίστοιχης καταναλισκόμενης ισχύος, αντικατοπτρίζουν την αποτελεσματικότητά του ως συνάρτηση της πραγματικής του απόδοσης (goodput) ανά joule καταναλισκόμενης ενέργειας. Προς το σκοπό αυτό, υιοθετήθηκαν σύνθετες συναρτήσεις χρησιμότητας, προσαρμοσμένες για κάθε τύπο υπηρεσίας, όχι απαραίτητα κοίλες, οδηγώντας στη διαμόρφωση ενός μη κυρτού και μη συνεργατικού παιγνίου.

Στο σημείο αυτό αξίζει να τονιστεί ότι η επιλογή της μορφής της συνάρτησης χρησιμότητας έχει τεράστια επιρροή στη φύση του παιχνιδιού και στον τρόπο με τον οποίο οι παίκτες επιλέγουν να ενεργήσουν. Πιο συγκεκριμένα, οι χρήστες υπηρεσιών μη

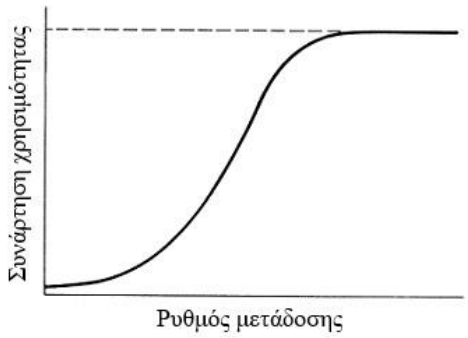
πραγματικού χρόνου(ελαστικές υπηρεσίες) έχουν περισσότερη ανοχή σε μεταβολές του ρυθμού μετάδοσης αλλά εμφανίζουν απαιτήσεις για όσο το δυνατόν υψηλότερο ρυθμό μετάδοσης, κάτι που περιγράφεται με τη χρήση μίας αυστηρά κοίλης ή κυρτής συνάρτησης χρησιμότητας ως προς το ρυθμό μετάδοσης. Αντίθετα, οι χρήστες υπηρεσιών πραγματικού χρόνου (μη ελαστικές υπηρεσίες) απαιτούν σταθερή ρυθμαπόδοση κατά τη διάρκεια παροχής της υπηρεσίας καθώς και ένα κατώτατο όριο ρυθμαπόδοσης ώστε να λειτουργεί η υπηρεσία. Για αυτό τον λόγο προτιμάται μία σιγμοειδής συνάρτηση χρησιμότητας ως προς το ρυθμό μετάδοσης καθότι αυτή περιγράφει εύστοχα την ικανοποίηση των απαιτήσεων των χρηστών σε ρυθμό μετάδοσης καθώς και την άμεση δυσαρέστησή τους, μόλις ο ρυθμός μετάδοσης δεδομένων πάρει τιμές μικρότερες από ένα συγκεκριμένο όριο.



Σχήμα 1: Κυρτή συνάρτηση (convex function)



Σχήμα 2: Κοίλη συνάρτηση (concave function)



Σχήμα 3: Σιγμοειδής συνάρτηση (sigmoidal function)

Στην ίδια κατεύθυνση κινούνται και οι ερευνητικές εργασία [14],[15]. Πιο συγκεκριμένα, στην [14] προκύπτει το συμπέρασμα ότι οι χρήστες μη πραγματικού χρόνου πετυχαίνουν μέγιστη ικανοποίηση για υψηλούς ρυθμούς μετάδοσης δεδομένων, ακόμα και για τους πιο απομακρυσμένους από τον σταθμό βάσης, λόγω του τύπου της συνάρτησης χρησιμότητάς τους που τους οδηγεί σε εκπομπές υψηλής ισχύος, ενώ οι χρήστες πραγματικού χρόνου οδηγούνται σε χαμηλότερη κατανάλωση ενέργειας επιδιώκοντας να ικανοποιήσουν καθορισμένα και αναμενόμενα ποσοστά μετάδοσης δεδομένων.

Στην [15], όπου χρησιμοποιήθηκε αυτόνομη αρχιτεκτονική δικτύου, με λειτουργίες αυτοπροσαρμογής και αυτοβελτίωσης τόσο για τους χρήστες όσο και για το σταθμό

βάσης, στοχεύοντας στην συνολική βελτίωση του δικτύου, παρατηρήθηκε ότι η μέση απόδοση των χρηστών πραγματικού χρόνου είναι σχεδόν σταθερή, ανεξάρτητα από τον αριθμό τους στο σύστημα, λόγω της αυτοπροσαρμογής τους που τους οδηγεί σε απαίτηση πόρων μέχρι να αποκτήσουν ικανοποιητική ροή δεδομένων, ενώ στους χρήστες μη πραγματικού χρόνου η μέση απόδοση αυξάνεται καθώς μειώνεται ο αριθμός τους, εξαιτίας της μείωσης του ανταγωνισμού τους.

Το αποτέλεσμα του μη συνεργατικού παιχνιδιού ως σημείο ισορροπίας κατά Nash, όπως έχει παρουσιαστεί μέχρι τώρα, μπορεί να είναι αναποτελεσματικό από μια πιο κοινωνική σκοπιά εξαιτίας της εγωιστικής συμπεριφοράς των χρηστών. Έτσι, η τιμολόγηση των πόρων του συστήματος αναδείχθηκε ως ένα ισχυρό εργαλείο για την επίτευξη μιας πιο επιθυμητής κοινωνικά προσέγγισης. Η υιοθέτηση κατάλληλων πολιτικών τιμολόγησης δημιουργεί μεγαλύτερο κέρδος για το σύστημα ενθαρρύνοντας τους χρήστες να ανακτούν τους πόρους του τελευταίου πιο αποτελεσματικά.

Βάσει των όσων αναφέρθηκαν, στην ερευνητική εργασία [16] παρουσιάστηκε ένα σενάριο κυρτής τιμολόγησης της ισχύος εκπομπής των χρηστών, ως μέσο αντιμετώπισης της αναποτελεσματικότητας που προαναφέρθηκε σε ένα σύστημα με υπηρεσίες πραγματικού χρόνου και λήφθηκε ένα Pareto βέλτιστο κατά Nash σημείο ισορροπίας. Μια Pareto αποδοτική λύση έχει την ιδιότητα ότι μπορεί να αυξήσει την χρησιμότητα κάποιων χρηστών χωρίς να θίξει άλλους χρήστες του δικτύου. Αριθμητικά αποτελέσματα αποδεικνύουν επίσης την υπεροχή της υιοθέτησης κυρτής τιμολόγησης τόσο απέναντι σε σενάρια χωρίς τιμολόγηση όσο και με γραμμική, με την τελευταία να χαρακτηρίζεται ως μη ρεαλιστική καθώς η ζημιά που προκαλεί ένας χρήστης στους γείτονές του δεν είναι αναλογική της ισχύος μετάδοσής του.

Η προηγούμενη μελέτη επεκτάθηκε σε δίκτυο ποικίλων υπηρεσιών [17] όπου οι πληροφορίες ελέγχου και η λήψη αποφάσεων επαφίενται στους κινητούς κόμβους, οι οποίοι είναι εμπλουτισμένοι με λειτουργίες αυτοβελτιστοποίησης, επιβεβαιώνοντας πως η κυρτή και γενικότερα η μη γραμμική τιμολόγηση οδηγεί σε χαμηλότερη μέση ισχύ εκπομπής των χρηστών και καλύτερη απόδοση βάσει της συνάρτησης χρησιμότητά τους, επιτυγχάνοντας παράλληλα καλύτερη αξιοποίηση των περιορισμένων πόρων ενός δικτύου, με τους πιο απαιτητικούς σε ζήτηση πόρων χρήστες να χρεώνονται με μεγαλύτερη τιμή.

Η μελέτη των CDMA δικτύων με πολιτική κοστολόγησης κλιμακώθηκε στην [18] με τον κοινό έλεγχο της ενέργειας και του ρυθμού εκπομπής των χρηστών. Το πρόβλημα της από κοινού αντιμετώπισης των προαναφερθέντων έχει μελετηθεί αρκετά στην βιβλιογραφία με μερικές μελέτες να ασχολούνται με την διαδοχική επίλυση του καθενός ξεχωριστά, χωρίζοντάς το ουσιαστικά σε δύο προβλήματα, και άλλες με αντικατάσταση του λόγου του ρυθμού εκπομπής προς την αντίστοιχη ισχύ εκπομπής με μια νέα μεταβλητή. Το σταθερό αποτέλεσμα των παραπάνω εξάγεται ανεξάρτητα ή ημι-από κοινού, οδηγώντας σε υψηλούς ρυθμούς εκπομπής και χαμηλή κατανάλωση ισχύος τους χρήστες που βρίσκονται κοντά στον σταθμό βάσης και στην αντίθετη συμπεριφορά αυτούς που βρίσκονται απομακρυσμένοι από την προαναφερθείσα. Λαμβάνοντας υπόψη και την αναποτελεσματικότητα των προηγούμενων από κοινωνική σκοπιά, δημιουργήθηκε η ανάγκη για χρησιμοποίηση πολιτικών τιμολόγησης.

Πιο αναλυτικά στην [18], οι τιμές υπολογίστηκαν ως σήματα που αντανακλούν τις σχέσεις μεταξύ της ζήτησης πόρων και διαθεσιμότητάς τους και χρησιμοποιήθηκαν για τον καλύτερο συντονισμό της κατανομής των πόρων, με την επιβολή κοινωνικής συμπεριφοράς στους χρήστες, και τη βελτίωση της κοινωνικής ευημερίας. Μια συνάρτηση χρησιμότητας συνδέθηκε με τις απαιτήσεις πόρων κάθε χρήστη ενώ οι συντελεστές τιμολόγησης υπολογίστηκαν με βάση την προτεινόμενη τιμολογιακή πολιτική και ανακοινώθηκαν από το ασύρματο σύστημα στους χρήστες. Οι ρυθμοί και η ισχύς εκπομπής επιλέχθηκαν ώστε να ανταποκρίνονται στα σήματα των τιμών με σκοπό να μεγιστοποιηθεί το καθαρό όφελος (δηλαδή η διαφορά μεταξύ χρησιμότητας και κόστους). Επίσης θα πρέπει να διευκρινιστεί ότι η τιμολογιακή πολιτική δεν συνεπάγεται την έννοια της πληρωμής / χρέωσης σε απόλυτες τιμές (δηλαδή μονάδες χρημάτων) από τον χρήστη.

Συμπερασματικά, με δεδομένη την κατάλληλη διατύπωση και ενσωμάτωση των απαιτήσεων της ποιότητας υπηρεσίας των χρηστών στην συνάρτηση χρησιμότητας, η χρήση πολιτικής τιμολόγησης και η επίλυση του προβλήματος κατανομής της ισχύος και του ρυθμού μετάδοσης στο ίδιο βήμα τίθενται καίριας σημασίας στην εν λόγω μελέτη. Μάλιστα αξίζει να αναφερθεί, ότι το προαναφερθέν συμπέρασμα τέθηκε και στα πλαίσια της μελέτης και ανάλυσης ετερογενών ασύρματων δικτύων, η συνέργεια των οποίων απαιτείται ως έναν βαθμό, με την ερευνητική μελέτη [10] να προτείνει ένα ενοποιημένο πλαίσιο αντιμετωπίζοντας το προκύπτον πρόβλημα βελτιστοποίησης ως πρόβλημα δύο μεταβλητών και οδηγώντας πάλι σε ισορροπία που προέκυψε από τον ταυτόχρονο συνυπολογισμό του ρυθμού και της ισχύος εκπομπής.

2.3 Κατανομή πόρων σε ασύρματα SC-FDMA κυψελωτά δίκτυα

Η τεχνική πολλαπλής πρόσβασης μονού φέροντος με διαίρεση συχνότητας(Single Carrier Frequency Division Multiple Access-SCFDMA) αναδείχθηκε ως μια πολλά υποσχόμενη τεχνολογία ραδιοπρόσβασης για τα συστήματα κινητής επικοινωνίας 4ης γενιάς με πλήθος ερευνητικών προσπαθειών να αφιερώνονται στο πρόβλημα της αποδοτικής κατανομής των πόρων στα εν λόγω δίκτυα. Πιο συγκεκριμένα, στα SC-FDMA το συνολικό εύρος ζώνης διαιρείται σε ορθογώνια υποφέροντα, προκειμένου να διατεθεί στους διάφορους χρήστες, προσθέτοντας συνεπώς στο παιχνίδι της κατανομής των πόρων και την συχνότητα.

Μια πρώτη προσέγγιση του εν λόγω προβλήματος αποτέλεσε η ερευνητική εργασία [19] η οποία ασχολήθηκε με την από κοινού βέλτιστη κατανομή ισχύος εκπομπής και υποφερόντων στην άνω ζεύξη ενός SC-FDMA ασύρματου δικτύου, με έμφαση στην υποστήριξη υπηρεσιών πραγματικού χρόνου. Η προτεινόμενη προσέγγιση κινήθηκε με στόχο την εξοικονόμηση ενέργειας και την ικανοποίηση των χρηστών επιβεβαιώνοντας με αριθμητικά αποτελέσματα τα οφέλη από την υιοθέτηση της συνάρτησης χρησιμότητας.

Στην συνέχεια επεκτάθηκε η μελέτη [20] με την ενσωμάτωση ενός μοντέλου διαπραγμάτευσης αντιμετωπίζοντας το πρόβλημα σε τρεις διαδοχικές φάσεις. Πρώτα

υιοθετήθηκε ένα πολυμερές μοντέλο διαπραγμάτευσης, το μοντέλο διαπραγμάτευσης του Rubinstein, το οποίο πηγάζει από την θεωρία παιγνίων και αναφέρεται σε μια κλάση παιχνιδιών διαπραγμάτευσης που χαρακτηρίζονται από εναλλασσόμενες προσφορές μέσα σε άπειρο χρονικά ορίζοντα, για την απόκτηση μιας εφικτής και σταθερής κατανομής υποφερόντων, από την άποψη του αριθμού των υποφερόντων που κατανέμονται ανά χρήστη. Στη συνέχεια, διαφορετικές πολιτικές κατανομής υποφερόντων μπορούν να ακολουθηθούν για τον προσδιορισμό της προαναφερθείσας εκχώρησης ενώ τέλος, στοχεύοντας σε ενεργειακή αποδοτικότητα, ένα πρόβλημα βελτιστοποίησης σε σχέση με την ισχύ μετάδοσης άνω ζεύξης του χρήστη διαμορφώθηκε και επιλύθηκε, προκειμένου να προσδιοριστεί η βέλτιστη κατανομή ισχύος ανά υποφέρον που εκχωρείται σε κάθε χρήστη στις προηγούμενες δύο φάσεις.

Η προαναφερθείσα ερευνητική προσπάθεια συμπληρώθηκε από την [21] η οποία πρότεινε μια κατανεμημένη και με επίκεντρο τον χρήστη κατανομή πόρων, επιτρέποντας παράλληλα την διαφοροποίηση των υπηρεσιών. Η βασική καινοτομία της εν λόγω μελέτης έγκειται στο ότι επιτρέπεται στους χρήστες να επιλέξουν συντελεστή έκπτωσης με τιμή της δικής τους προτίμησης προκειμένου να ανταγωνιστούν τους υπόλοιπους χρήστες στη διαδικασία διαπραγμάτευσης, ενώ στην [20] όλοι οι χρήστες χρησιμοποιούσαν τον ίδιο παράγοντα, γεγονός που δεν επιτρέπει την παροχή διαφοροποιημένων υπηρεσιών. Η τιμή του συντελεστή έκπτωσης αντανακλά την ανάγκη των χρηστών για κατάληψη υποφερόντων αναλογικά με την υπηρεσία που ζητούν, λαμβάνοντας υπόψη τις διαφορές των τελευταίων σε απαιτήσεις ποιότητας της υπηρεσίας. Οι χρήστες που εισέρχονται πρώτοι στην διαδικασία διαπραγμάτευσης, είναι ευνοημένοι εκ των προτέρων συγκριτικά με τους υπόλοιπους. Επιπλέον, ένας χρήστης που υιοθετεί υψηλό συντελεστή έκπτωσης, έχει προνομιούχα θέση. Ως εκ τούτου, με βάση την υπηρεσία που ζητάει ο καθένας, μπορεί να επιλεγεί η κατάλληλη τιμή του συντελεστή έκπτωσης, έτσι ώστε να ζητήσει ανταγωνιστικά πόρους του συστήματος.

Στην ίδια κατεύθυνση κινήθηκε και η ερευνητική εργασία [22] όπου η αντιστοίχηση των υποφερόντων μελετήθηκε τόσο με την τοπική (Local-FDMA) όσο και με την κατανεμημένη (Distributed-FDMA) μέθοδο, όπου στην πρώτη η κατανομή πραγματοποιείται διαδοχικά στους χρήστες αναθέτοντάς τους γειτονικά κανάλια, ενώ στη δεύτερη λαμβάνοντας υπόψη την πολιτική μέγιστου κέρδους, με ανάθεση δηλαδή του κάθε υποφέροντος στον χρήστη με το μεγαλύτερο κέρδος καναλιού. Όπως είναι προφανές, στη δεύτερη μέθοδο ο χρήστης καταλαμβάνει διάσπαρτες συχνότητες σε όλο το εύρος ζώνης. Στο σημείο αυτό αξίζει να σημειωθεί ότι η επέκταση της μελέτης σε εξυπηρέτηση διαφοροποιημένων υπηρεσιών ήταν ιδιαίτερα καθοριστική αν αναλογιστούμε έννοιες όπως τρισδιάστατα πολυμέσα, τηλεόραση υψηλής ευκρίνειας, VoIP(Voice over Internet Protocol), ηλεκτρονική υγεία, ηλεκτρονικά παιχνίδια κλπ που έχουν αρχίσει να αναδύονται στα νέα ασύρματα δίκτυα.

Ανακεφαλαίωση των τελευταίας τεχνολογίας αλγορίθμων κατανομής πόρων στην συγκεκριμένη κατηγορία δικτύων πραγματοποιείται στην [23] η οποία τους κατηγοριοποιεί σε τέσσερις μεγάλες κλάσεις βάσει του απώτερου στόχου της διαδικασίας κατανομής ως εξής: (α) βελτιστοποίηση της απόδοσης, (β) δικαιοσύνη, (γ) ικανοποίηση των απαιτήσεων ποιότητας των χρηστών και (δ) από κοινού κατανομή ισχύος και υποφερουσών.

Συγκεκριμένα, η πρώτη ομάδα αλγορίθμων στοχεύει κατ 'εξοχήν στην κατανομή των υποφερουσών στους χρήστες με σκοπό τη μεγιστοποίηση του συνολικού ρυθμού μετάδοσης του συστήματος. Η δεύτερη κατηγορία λαμβάνει υπόψη κριτήρια δικαιοσύνης, όπως ο προγραμματισμός μέγιστης αντιστοίχισης και η αναλογική δικαιοσύνη, για την ανάθεση των ομάδων πόρων, ενώ ο στόχος της τρίτης ομάδας είναι να ικανοποιήσει τις απαιτήσεις ποιότητας των χρηστών μέσω της αποτελεσματικής κατανομής των προαναφερθέντων. Τέλος, η τέταρτη ομάδα αλγορίθμων, όπου έχει επενδυθεί η μικρότερη ερευνητικά προσπάθεια, λόγω της εγγενής δυσκολίας και της πολυπλοκότητάς του, στοχεύει στην από κοινού κατανομή των υποφερουσών και της ισχύος μετάδοσης άνω ζεύξης στους χρήστες, προκειμένου να επιτευχθεί μεγιστοποίηση της αντιλαμβανόμενης ικανοποίησής τους που αντανακλάται συνήθως από μια κατάλληλα διατυπωμένη συνάρτηση χρησιμότητας.

Επιπρόσθετα τίθεται το πρόβλημα στα πλαίσια πολυκυψελωτού περιβάλλοντος έχοντας κατά νου τον περιορισμό της παρεμβολής και του ρυθμού οπισθόζευξης, με βασικές αρχές της κατανομής πόρων στο προαναφερθέν (α) την καλύτερη κάλυψη, ιδιαίτερα λαμβάνοντας υπόψη τους χρήστες στην άκρη των κυψελών, (β) την βελτιωμένη φασματική απόδοση και (γ) την καλύτερη χρήση των διαθέσιμων πόρων. Εκτενέστερη αναφορά σε πολυκυψελωτά δίκτυα πραγματοποιείται στην συνέχεια.

2.4 Κατανομή πόρων σε ασύρματα NOMA κυψελωτά δίκτυα

Η επιτάχυνση της εξέλιξης προς το Διαδίκτυο κινητού τηλεφώνου και το Διαδίκτυο των Αντικειμένων οδηγεί σε δραματική αύξηση της κυκλοφορίας δεδομένων θέτοντας νέες απαιτήσεις στις ασύρματες επικοινωνίες 5ης γενιάς. Οι τρέχουσες υιοθετημένες τεχνικές ορθογώνιας πολλαπλής πρόσβασης (Orthogonal Multiple Access-OMA) στα συστήματα επικοινωνίας 4ης γενιάς επιτρέπουν σε κάθε μπλοκ πόρων να καταλαμβάνεται από το πολύ έναν χρήστη σε κάθε χρονοθυρίδα, οπότε η ενδοκυψελική παρεμβολή μεταξύ χρηστών εξαλείφεται. Ωστόσο, οι τεχνικές OMA δεν είναι βέλτιστες όσον αφορά τη φασματική απόδοση, λόγω των περιορισμών που απορρέουν από την ορθογώνια φύση της πρόσβασης στο κανάλι.

Πρόσφατα, έχει προταθεί η τεχνική μη ορθογώνιας πολλαπλής προσπέλασης (Non Orthogonal Multiple Access-NOMA) προκειμένου να επιτευχθεί βελτιωμένη φασματική απόδοση, μαζική συνδεσιμότητα, χαμηλό κόστος σηματοδότησης και μικρή καθυστέρηση μετάδοσης [11]. Η τεχνική NOMA επιτρέπει την πολυπλεξία πολλών χρηστών στο ίδιο μπλοκ πόρων (π.χ. συχνότητα), βελτιώνοντας έτσι τη φασματική απόδοση, ενώ αυξάνει ταυτόχρονα την παρεμβολή μεταξύ χρηστών. Η αυξημένη παρεμβολή στον δέκτη εξαλείφεται με εφαρμογή της τεχνικής διαδοχικής ακύρωσης παρεμβολών (Successive Interference Cancellation-SIC), η οποία συνεπάγεται προηγμένο σχεδιασμό του δέκτη. Όπως γίνεται λοιπόν αντιληπτό, η μελέτη της αποτελεσματικής διαχείρισης πόρων στα πλαίσια της προαναφερθείσας τεχνικής μετάδοσης κρίνεται αναπόφευκτη.

Στην ερευνητική εργασία [24], η μελέτη του προαναφερθέντος προβλήματος τίθεται στα πλαίσια της επικοινωνίας με ορατό φως (Visible Light Communication-VLC) σε πολυκυψελωτό δίκτυο, η οποία αναγνωρίζεται ως μια πολλά υποσχόμενη ασύρματη

τεχνολογία που λύνει το πρόβλημα έλλειψης εύρου ζώνης και επιτρέπει μειωμένη ισχύ μετάδοσης των χρηστών, κινούμενη προς την κατεύθυνση ενεργειακά αποδοτικών λύσεων για επέκταση της διάρκειας ζωής της μπαταρίας των χρηστών και γενικότερα του οράματος πράσινης ασύρματης δικτύωσης [41].

Πιο αναλυτικά, εξετάζει το πρόβλημα της επιλογής οπτικού σημείου πρόσβασης (Optical Access Point-OAP) και της κατανομής των πόρων(ισχύος μετάδοσης, εύρος ζώνης) στην άνω ζεύξη των VPAN(Visible Light Communication Personal Area Networks) με δύο διαφορετικές τεχνικές μετάδοσης, την ορθογώνια πολλαπλή πρόσβαση διαίρεσης συχνότητας(Orthogonal Frequency-Division Multiple Access–OFDMA) και τη μη ορθογώνια πολλαπλή πρόσβαση (NOMA). Κάθε χρήστης συνδέεται με μια γενική συνάρτηση χρησιμότητας, η οποία αντιπροσωπεύει την ικανοποίησή του σε σχέση με το συνολικό πρόβλημα κατανομής των πόρων. Όσον αφορά την επιλογή OAP, υιοθετείται η πολιτική επιλογής μέγιστου κέρδους (Max Gain System-MGS), δηλαδή οι χρήστες επιλέγουν ένα OAP για σύνδεση με βάση το υψηλότερο κέρδος διαδρομής. Παράλληλα, υπογραμμίζει και αξιολογεί τα πλεονεκτήματα και τα μειονεκτήματα της κάθε τεχνικής ενώ ανεξάρτητα από αυτές, η διαδικασία λήψης αποφάσεων επαφίεται στους κινητούς χρήστες, εμπλουτίζοντάς τους με διαδικασίες αυτοβελτίωσης. Ωστόσο πρέπει να διευκρινιστεί ότι έγινε η παραδοχή ότι όλοι οι χρήστες ζητούν τον ίδιο τύπο υπηρεσίας.

Η παραπάνω επεκτάθηκε στην [25] όπου μελετήθηκε το πρόβλημα της από κοινού κατανομής της ισχύος και του ρυθμού μετάδοσης δεδομένων στην άνω ζεύξη των ασύρματων δικτύων NOMA ως ένα πρόβλημα βελτιστοποίησης δύο συνεχών μεταβλητών. Μεταξύ των καινοτομιών του παρόντος εγγράφου είναι η εισαγωγή εξελιγμένης συνάρτησης χρησιμότητας που υιοθετείται από κάθε χρήστη, η οποία εκφράζει την ικανοποίηση του χρήστη ως προς την εξυπηρέτησή του, εξετάζοντας ταυτόχρονα τις αιτούμενες υπηρεσίες πραγματικού και μη πραγματικού χρόνου με τρόπο παρόμοιο με την έννοια της ομαδοποίησης υπηρεσιών(service bundling).

Αρχικά, ο όρος "ομαδοποίηση υπηρεσιών" σχεδιάστηκε για να αναφερθεί στην ενσωμάτωση και προσφορά δύο ή περισσότερων προϊόντων, για τις οποίες υπάρχουν διαφορετικές αγορές, σε ένα ενοποιημένο πακέτο. Αυτή η ενσωμάτωση προσφέρει προστιθέμενη αξία στους χρήστες μέσω βελτιωμένης απόδοσης, συμπαγότητας και διασυνδεσιμότητας, ενώ ικανοποιεί ευρύτερο φάσμα απαιτήσεων των χρηστών. Επιπλέον, η ομαδοποίηση μπορεί συλλάβει υψηλότερο πλεόνασμα πελατών και μεταβιβάζει αξία μεταξύ των πακέτων υπηρεσιών.

Στην συγκεκριμένη λοιπόν έρευνα υιοθετείται η χρήση της παραπάνω ορολογίας, αναφερόμενη στη δέσμευση υπηρεσιών πραγματικού και μη πραγματικού χρόνου. Μια τέτοια ομαδοποίηση επιτρέπει στους χρήστες κινητής τηλεφωνίας να διευρύνουν την αντιληπτή ικανοποίησή τους, καταναλώνοντας δύο διακριτές υπηρεσίες, καθώς και τη δυνατότητα εκμετάλλευσης ενός μεγαλύτερου μέρους της συνολικής απόδοσης του δικτύου. Από την άλλη, ο πάροχος δικτύου επωφελείται από το κλείδωμα των πελατών του και την αύξηση των προοπτικών κέρδους του με την πώληση περισσότερων υπηρεσιών σε μια ευρύτερη αγορά, αποκτώντας πλεονέκτημα έναντι των ανταγωνιστών και βελτιώνοντας ταυτόχρονα την αξιοποίηση των πόρων του.

Για την επίλυση του προβλήματος όπως διατυπώθηκε παραπάνω, ακολουθήθηκε μια προσέγγιση με βάση την θεωρία S-modular προκειμένου να βρεθούν κατανεμημένες λύσεις που μειώνουν την απαιτούμενη πολυπλοκότητα τοποθετώντας στο επίκεντρο ενδιαφέροντος τον χρήστη. Πιο αναλυτικά, η θεμελιώδης έννοια του Supermodular παιγνίου είναι ότι η αύξηση της ενέργειας του παίκτη / χρήστη του κινητού (π.χ. αύξηση της ισχύος και του ρυθμού μετάδοσης δεδομένων άνω ζεύξης) για συγκεκριμένες ενέργειες των υπόλοιπων χρηστών, ενισχύει την επιθυμία όλων των παικτών / χρηστών κινητής τηλεφωνίας να αυξήσουν τις ενέργειές τους λόγω στρατηγικής συμπληρωματικότητας.

Τα Supermodular παίγνια εμφανίζονται ως πλέον ελκυστικά προκειμένου να εφαρμοστούν σε προβλήματα κατανομής πόρων, επειδή έχουν ένα εκ των προτέρων μη κενό σύνολο ισορροπίας κατά Nash, με αποτέλεσμα το σύστημα να μπορεί να συγκλίνει σε σταθερές κατανομές πόρων. Πιο συγκεκριμένα, στα Supermodular παίγνια αν ο κάθε παίκτης αρχικά υιοθετήσει τη χαμηλότερη ή τη μεγαλύτερη στρατηγική του, τότε συγκλίνει μονότονα σε ένα σημείο ισορροπίας κατά Nash που εξαρτάται από την αρχική κατάσταση του παίκτη. Επιπλέον, στην περίπτωση που το εξεταζόμενο Supermodular παίγνιο έχει ένα μοναδικό σημείο ισορροπίας κατά Nash, τότε μπορεί να επιλυθεί ενώ οι κανόνες μάθησης και ρύθμισης, δηλαδή οι καλύτερες δυναμικές απόκρισης, Θα συγκλίνουν σε αυτό.

2.5 Κατανομή πόρων σε φεμτοκυψέλες

Σημαντικές ερευνητικές προσπάθειες έχουν αφιερωθεί στο συνδυαστικό πρόβλημα της αύξησης της χωρητικότητας των ασύρματων δικτύων, την επέκταση της κάλυψης των κυψελών και την εισαγωγή νέων υπηρεσιών με παράλληλη μείωση τόσο των κεφαλαιουχικών δαπανών όσο και των λειτουργικών εξόδων. Λαμβάνοντας υπόψη αυτούς τους στόχους, οι φεμτοκυψέλες προκύπτουν ως μια πολλά υποσχόμενη λύση, προσφέροντας σημαντικά οικονομικά οφέλη λόγω του χαμηλού κόστους εγκατάστασής τους σε ένα υπάρχον ασύρματο δίκτυο μακροκυψέλης. Το σύνολο του επικαλυπτόμενου δικτύου αναφέρεται ως φεμτοκυψέλη δύο βαθμίδων και αποτελείται από τις φεμτοκυψέλες και το συμβατικό δίκτυο μακροκυψέλης. Οι χρήστες των πρώτων(Femto Users-FUs) απολαμβάνουν το προνόμιο των εσωτερικών χώρων και της λήψης υψηλότερων ρυθμών δεδομένων με μετάδοση χαμηλότερης ισχύος λόγω της στενής εγγύτητας μεταξύ τους και των δικών τους σημείων πρόσβασης(Access Point-AP). Επιπλέον, οι FUs μοιράζονται το ίδιο φάσμα με τους χρήστες της μακροκυψέλης (Macro Users-MUs), οι οποίοι έχουν αυστηρά υψηλότερη προτεραιότητα σε σχέση με τους πρώτους κατά την πρόσβαση στο υποκείμενο ραδιοφάσμα. Επομένως, η μείωση της παρεμβολής μεταξύ των δυο βαθμίδων είναι μεγάλης σημασίας για την ανάπτυξη φεμτοκυψελών σε ασύρματα δίκτυα δύο επιπέδων και ενσωματώνεται στα πλαίσια της γενικότερης μελέτης της βέλτιστης διαχείρισης πόρων ενός ασύρματου δικτύου.

Στην ερευνητική εργασία [26] αντιμετωπίζεται το κατανεμημένο πρόβλημα της αποδοτικής κατανομής ισχύος στην άνω ζεύξη δικτύου φεμτοκυψέλης δύο βαθμίδων. Η προσέγγιση που ακολουθήθηκε εξετάζει δύο διαφορετικές διαστάσεις, συνυπολογίζοντας τους αντίστοιχους περιορισμούς και τις ιδιότητες που προκύπτουν από κάθε μία από αυτές: (α) την αρχιτεκτονική δύο βαθμίδων, και (β) την ταυτόχρονη υποστήριξη

υπηρεσιών τόσο σε πραγματικό όσο και σε μη πραγματικό χρόνο, με ποικίλες προϋποθέσεις ποιότητας των υπηρεσιών (QoS).

Για την αντιμετώπιση του προαναφερθέντος κάτω από ένα κοινό πλαίσιο, χρησιμοποιήθηκε πάλι η θεωρία μεγιστοποίησης χρησιμότητας δικτύου, όπου κάθε χρήστης, είτε FU είτε MU, σχετίζεται με μια σωστά καθορισμένη συνάρτηση χρησιμότητας, προσαρμοσμένη στις QoS απαιτήσεις, την αιτούμενη υπηρεσία και την βαθμίδα που ανήκει ο χρήστης. Για την περαιτέρω αντιμετώπιση της παρεμβολής εντός των κυψελών και μεταξύ των δύο επιπέδων, και προκειμένου να δοθεί μεγαλύτερη προτεραιότητα στους χρήστες μακροκυψελών (MUs), οι femto χρήστες (FUs) "τιμωρούνται" μέσω μιας κυρτής συνάρτησης κόστους σε σχέση με την ισχύ μετάδοσης άνω ζεύξης, διατηρώντας την τελευταία σε χαμηλά επίπεδα και επιτρέποντας στους MUs να διατηρούν την ποιότητα των υπηρεσιών τους ανεξάρτητα από την παράταξη των σημείων πρόσβασης των δεύτερων. Λόγω της φύσης του, το συνολικό προκύπτον πρόβλημα διαμορφώνεται ως ένα μη συνεργατικό παιχνίδι και επιλύεται χρησιμοποιώντας τη S-Modular θεωρία για τον προσδιορισμό του σημείου ισορροπίας κατά Nash.

Η προηγούμενη έρευνα επεκτάθηκε στην [27] με την ταυτόχρονη κατανομή της ισχύος και του ρυθμού μετάδοσης δεδομένων στους χρήστες(FU και MU), υιοθετώντας συναρτήσεις χρησιμότητας σχεδόν κοίλες και προσαρμοσμένες στην παραπάνω κατανομή, καθώς και την βαθμίδα που ανήκουν και την αιτούμενη υπηρεσία. Όπως είναι λοιπόν προφανές, προέκυψε πρόβλημα δύο μεταβλητών. Για την αντιμετώπισή του ωστόσο, μετατράπηκε σε πρόβλημα μίας μεταβλητής θέτοντας τον λόγο του ρυθμού μετάδοσης προς την αντίστοιχη ισχύ ως μία μεταβλητή και λύνοντας το προκύπτον πρόβλημα. Επίσης αξίζει να τονιστεί ότι το προτεινόμενο πλαίσιο στην εν λόγω μελέτη επέτρεψε την αυτόνομη διαχείριση με γνώμονα τον χρήστη και του επέτρεψε να καταλήξει στην καλύτερη δυνατή στρατηγική του έχοντας ιδιότητες αυτοβελτίωσης και αυτοπροσαρμογής.

Το σενάριο της ισορροπίας κατά Nash υιοθετήθηκε και εδώ όντας η πιο συνηθισμένη μέθοδος για την επίλυση ενός μη συνεργατικού παιγνίου. Το βασικό χαρακτηριστικό του είναι ότι προσφέρει μια προβλέψιμη, σταθερή και καθορισμένη λύση του παιχνιδιού, όπου διάφορες κατηγορίες χρηστών με δυνητικά αντιφατικά συμφέροντα ανταγωνίζονται μέσω αυτόνομης αυτοβελτιστοποίησης και φτάνουν σε ένα σημείο όπου κανένας χρήστης δεν επιδιώκει να παρεκκλίνει. Πιο συγκεκριμένα, στο σημείο ισορροπίας κανένας χρήστης δεν έχει το κίνητρο να αλλάξει τον συνδυασμό της ισχύος και του ρυθμού μετάδοσής του, δεδομένου ότι η χρησιμότητά του δεν μπορεί να βελτιωθεί περαιτέρω κάνοντας οποιεσδήποτε αλλαγές στη στρατηγική του, με δεδομένη την ισχύ, τον ρυθμό μετάδοσής δεδομένων και τον λόγο του δεύτερου προς το πρώτο όλων των άλλων χρηστών.

Η προηγούμενη προσέγγιση είναι εφαρμόσιμη σε συγκεκριμένους τύπους συνάρτησης χρησιμότητας, όπου επιτρέπεται η αντικατάσταση που προαναφέρθηκε, προκειμένου να προκύψει πρόβλημα μίας μεταβλητής. Το προαναφερθέν λοιπόν πρόβλημα λύθηκε πλήρως στην [29] με την χρήση της S-modular θεωρίας λύνοντάς το αυτήν την φορά ως πρόβλημα δύο μεταβλητών, με την υιοθέτηση συναρτήσεων χρησιμότητας που

επιτρέπουν στους χρήστες να εκφράσουν τις QoS απαιτήσεις τους μέσω των ανεξάρτητων μεταβλητών της ισχύος και του ρυθμού μετάδοσης. Στο σημείο αυτό πρέπει να τονιστεί ότι η ικανότητα επίλυσης προβλημάτων δύο μεταβλητών μέσω της S-modular θεωρίας προσφέρει γενικότερα νέες δυνατότητες στο πρόβλημα της κατανομής πόρων, δοκιμάζοντας εναλλακτικές και πιο πολύπλοκες προσεγγίσεις στο εκάστοτε πρόβλημα.

Χαρακτηριστικά, στην ερευνητική εργασία [11] αντιμετωπίζεται το πρόβλημα του από κοινού ελέγχου της ισχύος μετάδοσης και της τιμής κοστολόγησης αναγνωρίζοντας την δεύτερη ως ένα πραγματικό πόρο προς κατανομή ή αλλιώς, ως μια διακριτή συνιστώσα της συνάρτησης χρησιμότητας που πρέπει να καθοριστεί προς την κατεύθυνση της μεγιστοποίηση της ευχαρίστησης κάθε χρήστη, σε αντίθεση με τις συνηθισμένες προσεγγίσεις όπου επιδιώκεται απλά η ενσωμάτωσή του στο εκάστοτε πρόβλημα βέλτιστη κατανομής.

Η μελέτη βέλτιστης διαχείρισης πόρων στην συγκεκριμένη κατηγορία δικτύων κλείνει με την [28] όπου αντιμετωπίζεται το πρόβλημα βέλτιστης επιλογής κυψέλης και κατανομής ισχύος σε ένα δίκτυο φεμτοκυψέλης πολλαπλών υπηρεσιών και ανοιχτής πρόσβασης, επιτρέποντας δηλαδή σε όλους τους χρήστες να έχουν πρόσβαση σε αυτήν. Αφού επιλεγεί η κατάλληλη συνάρτηση χρησιμότητας για κάθε χρήστη, διατυπώνεται το πρόβλημα βέλτιστης επιλογής κυψέλης, με την λύση του να αποτελεί ένα σημείο ισορροπίας κατά Nash που εγγυάται ότι οι χρήστες θα επιλέξουν την πιο κατάλληλη κυψέλη προκειμένου να μεγιστοποιήσουν την ευχαρίστηση και την απόδοσή τους σύμφωνα με τις QoS απαιτήσεις τους. Στην συνέχεια, δεδομένης της ανάθεσης των χρηστών στα κελιά, λύνεται το πρόβλημα της βέλτιστης κατανομής πόρων προς την κατεύθυνση της ενεργειακά αποδοτικότερης λύσης.

2.6 Κατανομή πόρων σε περιβάλλοντα επικοινωνίας συσκευής προς συσκευή

Σημαντικές ερευνητικές προσπάθειες έχουν αφιερωθεί στο πρόβλημα της διαχείρισης παρεμβολών στα ασύρματα δίκτυα, πρόβλημα το οποίο μπορεί να τεθεί στα πλαίσια της κατανομής πόρων, με τις παρεμβολές να αποτελούν μια σημαντική απειλή από την οποία υποφέρουν κυρίως οι χρήστες στα άκρα της κυψέλης [33]. Οι τελευταίοι βρίσκονται στη διασταύρωση δύο ή περισσότερων γειτονικών κυψελών και η απόσταση τους από τους σταθμούς βάσης που εξυπηρετούνται και τους γειτονικούς είναι η υψηλότερο δυνατή. Ως εκ τούτου, απαιτείται μετριασμός παρεμβολών, προκειμένου να επεκταθεί η διάρκεια ζωής της μπαταρίας τους, καθώς και να ικανοποιηθούν οι προϋποθέσεις ποιότητας της υπηρεσίας τους(QoS). Μεταξύ των διαφόρων μεθόδων που έχουν προταθεί στην βιβλιογραφία για την αντιμετώπιση του προβλήματος του μετριασμού των παρεμβολών είναι η επικοινωνία συσκευής με συσκευή(Device to Device-D2D) μεταξύ των χρηστών του κυψελοειδούς δικτύου, η οποία αποτελεί έναν τρόπο άμεσης επικοινωνίας μεταξύ δύο κινητών τερματικών. Η επικοινωνία D2D μπορεί να πραγματοποιηθεί είτε με επικάλυψη(overlay) είτε με την επίστρωση(underlay) ενός κυψελοειδούς δικτύου, με την μελέτη του δεύτερου να είναι πιο δύσκολη συγκριτικά με του πρώτου, σε σχέση με τον μετριασμό των παρεμβολών. Λαμβάνοντας υπόψη το σενάριο επικάλυψης, η επικοινωνία D2D χρησιμοποιεί ειδικούς πόρους(συχνοτικά κανάλια, χρονικά παράθυρα), ενώ στην

περίπτωση υποστρώματος η επικοινωνία D2D μοιράζεται κοινούς πόρους με το υπόλοιπο κυψελοειδές δίκτυο.

Στην ερευνητική μελέτη [30], [71] αντιμετωπίζεται το πρόβλημα του ελέγχου ισχύος άνω ζεύξης στις επικοινωνίες συσκευής προς συσκευή που υποβάλλονται(underlaying) σε ένα κυψελοειδές δίκτυο. Οι πόροι χρόνου και συχνοτήτων του δικτύου είναι οργανωμένοι σε μπλοκ πόρων και οι χρήστες μπορούν να επικοινωνούν μέσω του σταθμού βάσης ή απευθείας μεταξύ τους. Ανεξάρτητα από τον τρόπο επικοινωνίας τους, μπορούν να μοιράζονται και να ανταγωνίζονται για τα ίδια μπλοκ πόρων. Αυτό το είδος αλληλεπίδρασης μεταξύ των χρηστών μοντελοποιείται μέσω ενός μη συνεργατικού παιγνίου ελέγχου ισχύος, όπου η ποιότητα των διαφόρων και διαφορετικών υπηρεσιών των χρηστών λαμβάνεται υπόψη. Η συνάρτηση χρησιμότητας κάθε χρήστη αποτελείται από δύο όρους. Ο πρώτος εκφράζει την προθυμία του χρήστη να επιτύχει καλύτερο λόγο σήματος προς θόρυβο και παρεμβολή(SINR), προκειμένου να πραγματοποιήσει καλύτερο ρυθμό μετάδοσης, ενώ ο δεύτερος όρος αντανακλά τη ζημιά που βιώνει ο χρήστης από τη μετάδοση σε υψηλά επίπεδα ισχύος. Έτσι, η προτεινόμενη συνάρτηση χρησιμότητας εκφράζει αποτελεσματικά την αμοιβαία αντιστάθμιση(tradeoff) μεταξύ των QoS προϋποθέσεων του χρήστη και της αντίστοιχης κατανάλωσης ισχύος.

Η [31] ασχολείται με το πρόβλημα της από κοινού κατανομής των μπλοκ πόρων (Resource Block-RB) και της ισχύος μετάδοσης άνω ζεύξης σε μια επικοινωνία συσκευής προς συσκευή, στα πλαίσια ενός underlay σεναρίου, με επίκεντρο τον περιορισμό των παρεμβολών και την ενεργειακή απόδοση. Για την επίλυση του εν λόγω πολύπλοκου προβλήματος ακολουθείται μια προσέγγιση δύο βημάτων.

Αρχικά, η διαδικασία κατανομής των RB μοντελοποιείται ως ένα ακριβές δυναμικό(potential) παίγνιο το οποίο εμφανίζεται για να ελαχιστοποιήσει τη συνολική παρεμβολή στο δίκτυο. Στη θεωρία παιγνίων, ένα παιχνίδι λέγεται ότι είναι δυναμικό αν το κίνητρο όλων των παικτών να αλλάξουν τη στρατηγική τους μπορεί να εκφραστεί χρησιμοποιώντας μια ενιαία παγκόσμια συνάρτηση που ονομάζεται δυναμική συνάρτηση. Επίσης δεν περιορίζεται εκ των προτέρων ο αριθμός των ζευγών D2D που μπορούν να επαναχρησιμοποιήσουν ένα RB που έχει διανεμηθεί σε μια κυψελωτή σύνδεση(μεταξύ εκπομπού και σταθμού βάσης). Αυτό καθορίζεται δυναμικά από τον στόχο της ελαχιστοποίησης παρεμβολών. Επομένως, ένα RB που δεσμεύεται από μια κυψελωτή σύνδεση, μπορεί ενδεχομένως επαναχρησιμοποιηθεί πολλές φορές από διαφορετικές συνδέσεις D2D(ζεύξη πομπών και δεκτών που επικοινωνούν απευθείας μεταξύ τους) με στόχο την αποδοτική χρήση του ραδιοφάσματος.

Στη συνέχεια ένα μοντέλο μη συνεργατικού παιγνίου προτείνεται για το πρόβλημα κατανομής ισχύος άνω ζεύξης λαμβάνοντας υπόψη το σηματοθορυβικό λόγο(Signal to Interference plus Noise Ratio-SINR).Σε αυτή την περίπτωση, κάθε σύνδεση μεταδίδει στο επιθυμητό επίπεδο ισχύος για να ικανοποιήσει τις SINR απαιτήσεις του, αν αυτό είναι εφικτό. Διαφορετικά, θα μεταδίδει με τη μέγιστη δυνατή ισχύ προκειμένου να επιτευχθεί ένα επίπεδο SINR όσο πιο κοντά στο επιθυμητό. Επίσης έχει μια συνάρτηση χρησιμότητας που μπορεί να υπολογιστεί λαμβάνοντας υπόψη μόνο τοπικές πληροφορίες ενώ εξαρτάται μόνο από την ισχύ μετάδοσης της σύνδεσης και την παρεμβολή που

αισθάνεται σε κάθε RB που χρησιμοποιεί. Τέλος, το πρόβλημα επεκτείνεται σε ένα πολυκυψελωτό περιβάλλον στην ερευνητική εργασία [36].

2.7 Κατανομή πόρων στο Διαδίκτυο των Αντικειμένων

Η μελέτη του προβλήματος αποδοτικής κατανομής κλείνει με την τοποθέτησή του στα πλαίσια του Διαδικτύου των Αντικειμένων(Internet of Things-IoT) το οποίο αποτελεί και το επίκεντρο της συγκεκριμένης διπλωματικής εργασίας. Πιο αναλυτικά, το προαναφερθέν δημιουργεί αρκετές σημαντικές τεχνολογικές προκλήσεις που θα μπορούσαν να εμποδίσουν την αξιοποίηση των δυνητικών οφελών του. Μεταξύ αυτών των σημαντικών προκλήσεων, η σύνδεση των συσκευών σε ένα ευρύ φάσμα εφαρμογών, π.χ. έξυπνο δίκτυο/μέτρηση, έξυπνη γεωργία, παρακολούθηση της υγείας, έξυπνα σπίτια κ.λπ., αποτελεί έναν από τους πιο ενδιαφέροντες τομείς έρευνας και καινοτομίας. Η επικοινωνία μηχανής με μηχανή (Machine to Machine-M2M) διευκολύνει το IoT με την συνδεσιμότητα, βασιζόμενη στην επικοινωνία σημείου με σημείο και χρησιμοποιώντας ενσωματωμένες μονάδες υλικού στις συσκευές και τα ασύρματα δίκτυα που συμμετέχουν στην M2M επικοινωνία. Συγκεκριμένα, η επικοινωνία M2M επιδιώκει αποδοτικούς φασματικά και ενεργειακά τρόπους για να παρέχει μόνιμη συνδεσιμότητα μεταξύ ενός τεράστιου αριθμού συσκευών χαμηλού κόστους χωρίς ή με ελάχιστη ανθρώπινη αλληλεπίδραση [34], [37], [39].

Στην [32] αντιμετωπίζεται το πρόβλημα του σχηματισμού συνασπισμού μεταξύ των συσκευών (M2M) και της διαχείρισης των πόρων. Κάθε συσκευή M2M χαρακτηρίζεται από τη διαθεσιμότητα ενέργειάς της, καθώς και από διαφοροποιημένα για την κάθε μία ενδιαφέροντα να επικοινωνεί με άλλες συσκευές, βάσει της IoT εφαρμογής που εξυπηρετούν από κοινού. Φυσικοί δεσμοί μεταξύ συσκευών υπάρχουν επίσης με βάση τη φυσική απόστασή τους και την ποιότητα του καναλιού επικοινωνίας τους. Αυτοί οι τρεις παράγοντες: η διαθεσιμότητα ενέργειας, τα ενδιαφέροντα και οι φυσικοί δεσμοί, λαμβάνονται υπόψη στη διαδικασία σχηματισμού συνασπισμού και την επιλογή της κεφαλής του.

Το προτεινόμενο πλαίσιο αποτελείται από δύο θεμελιώδη στάδια. Στο πρώτο στάδιο, η αλληλεπίδραση των συμφερόντων των ασύρματων IoT συσκευών και τα ενεργειακά τους επίπεδα, χρησιμοποιούνται προς την κατεύθυνση της δημιουργίας συμμαχιών μεταξύ των συσκευών, λαμβάνοντας υπόψη και τους φυσικούς περιορισμούς που προαναφέρθηκαν. Στο δεύτερο στάδιο, κάθε συσκευή M2M συσχετίζεται με μια ολιστική συνάρτηση χρησιμότητας, η οποία αντιπροσωπεύει το βαθμό ικανοποίησης της συσκευής, όσον αφορά την εκπλήρωση των προϋποθέσεων για την ποιότητα της υπηρεσίας της(QoS), και μπορεί εύκολα να προσαρμόζεται στις διάφορες IoT εφαρμογές λόγω της γενικής φύσης της. Λαμβάνοντας υπόψη τις δημιουργούμενες συμμαχίες μεταξύ των συσκευών M2M, προτείνεται ένα πλαίσιο κατανεμημένης ισχύος για τον προσδιορισμό της βέλτιστης ισχύος μετάδοσης κάθε συσκευής M2M, προκειμένου να εκπληρώσει τις QoS απαιτήσεις της και επιδιώκοντας την μεγιστοποίηση της ικανοποίησής της με εγωιστικό και κατανεμημένο τρόπο.

ΚΕΦΑΛΑΙΟ 3

ΠΑΡΕΜΒΟΛΕΣ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

3.1 Εισαγωγικά

3.2 Παρεμβολές στα παραδοσιακά ασύρματα δίκτυα

3.3 Παρεμβολές στα γνωστικά δίκτυα ραδιοσυχνοτήτων

3.4 Παρεμβολές στο Διαδίκτυο των Αντικειμένων

3.1 Εισαγωγικά

Στο προηγούμενο κεφάλαιο μελετήθηκε το πρόβλημα της βέλτιστης διαχείρισης και κατανομής πόρων σε ένα ασύρματο δίκτυο, με παρουσία χρηστών οι οποίοι στοχεύουν εγωιστικά ο καθένας στην μεγιστοποίηση της ικανοποίησης και της ευημερίας τους, η οποία εκφράζεται μέσω των πόρων που τους ανατίθενται και γενικότερα της ποιότητας της υπηρεσίας που απολαμβάνουν. Ωστόσο, λόγο της φύσης των εκπομπών μετάδοσής τους, τα ασύρματα δίκτυα είναι ιδιαίτερα ευαίσθητα σε επιθέσεις άρνησης υπηρεσιών(Denial of service-DoS) μέσω παρεμβολών στο στρώμα ελέγχου πρόσβασης στο μέσο(Medium Access Control-MAC). Οι προαναφερθείσες πραγματοποιούνται από κακεντρεχείς χρήστες οι οποίοι έχουν ως μοναδικό στόχο την υποβάθμιση της απόδοσης των απλών πομπών και του συστήματος. Η ικανοποίησή τους δηλαδή, καθιστά αναγκαία την μη ικανοποίηση των "εγωιστών" χρηστών, των οποίων ναι μεν η σχέση είναι ανταγωνιστική, αλλά όχι εχθρική, δίνοντας νέα διάσταση στις μέχρι τώρα προσεγγίσεις. Όπως γίνεται λοιπόν σαφές, οι κακόβουλοι αυτοί χρήστες, οι οποίοι στη συνέχεια θα αναφέρονται ως παρεμβολείς, δεν γίνεται να μην ληφθούν σοβαρά υπόψη κατά την προσπάθεια επίτευξης ομαλής και αποδοτικής λειτουργίας ενός δικτύου.

Στην συνέχεια γίνεται αναφορά σε προηγούμενες έρευνες που έχουν ασχοληθεί με το πρόβλημα παρεμβολών στα ασύρματα δίκτυα, εξετάζοντας την συνύπαρξη των κακόβουλων με τους απλούς χρήστες και μελετώντας πως η ευημερία των δεύτερων επηρεάζεται από την δράση των πρώτων. Σημαντική θέση στις προαναφερθείσες προσεγγίσεις κατέχει ξανά η θεωρία παιγνίων καθώς παρέχει ισχυρά εργαλεία για την μοντελοποίηση και την ανάλυση των επιθέσεων παρεμβολής. Η αναδρομή ξεκινά από τα ασύρματα παραδοσιακά δίκτυα(κυψελωτά ασύρματα δίκτυα, ασύρματα δίκτυα αισθητήρων) ώστε να οδηγηθούμε σταδιακά στους παράγοντες που καθορίζουν την ασφάλεια στο Διαδίκτυο των Αντικειμένων, η οποία αποτελεί και το θέμα της παρούσας διπλωματικής εργασίας.

3.2 Παρεμβολές στα παραδοσιακά ασύρματα δίκτυα

Στην ερευνητική μελέτη [42] συζητιέται μια κατηγορία παιχνιδιών παρεμβολής στο στρώμα MAC, μεταξύ ενός συνόλου πομπών και παρεμβολέων, με επίκεντρο το επίπεδο πληροφοριών που έχουν οι χρήστες του δικτύου για τα χαρακτηριστικά των υπολοίπων. Το προαναφερθέν είναι χαρακτηριστικό των κατανεμημένων δικτύων ασύρματης πρόσβασης όπου οι χρήστες δεν έχουν πλήρη και σαφή εικόνα για το δίκτυο και τους άλλους χρήστες. Η ασάφεια αυτή που αντιμετωπίζουν ποικίλει και αφορά διάφορους παράγοντες όπως τους παρακάτω:

• Τύπο χρηστών: αν ο χρήστης είναι πομπός η παρεμβολέας.[43]

• Φυσική παρουσία: αν ο αντίπαλος είναι φυσικά παρών για να μεταδώσει ή όχι[44].

• Διακίνηση πακέτων: την δυναμική του αντιπάλου ως προς τα πακέτα που μπορεί να μεταδώσει, αν δηλαδή μπορεί να τα αποθηκεύσει για μετέπειτα μετάδοση σε περίπτωση συμφόρησης δικτύου(backlogged) ή όχι[45]

• Παράμετροι συστήματος: τα επίπεδα χρησιμότητας των άλλων(συνάρτηση χρησιμότητας και ανταμοιβής)[43],[46]

• Φυσικό κανάλι: τα χαρακτηριστικά του φυσικού καναλιού, όπως το κέρδος, τον θόρυβο του καναλιού[47] ή την πιθανότητα σύλληψης του εκπεμπόμενου πακέτου[43].

Για τη μοντελοποίηση των προαναφερθέντων ελλιπών πληροφοριών χρησιμοποιείται η θεωρία των μπευζιανών παιγνίων, όπου οι παίχτες έχουν πεποιθήσεις με γνωστή κατανομή πιθανότητας για τους υπόλοιπους παρά τις ελλιπείς πληροφορίες(πχ για τις διαθέσιμες στρατηγικές τους). Έτσι, και στο πλαίσιο που εξετάζεται εδώ, η αβεβαιότητα ενός παίκτη διαμορφώνεται μέσω μιας κατανομής πάνω από την εκάστοτε παράμετρο ενδιαφέροντος που θέλουμε να εξετάσουμε κάθε φορά. Οι παίκτες μεγιστοποιούν στη συνέχεια τις αναμενόμενες απολαβές τους, με την προσδοκία τους να είναι πάντοτε σε σχέση με την δοσμένη κατανομή, ενώ οι στρατηγικές ισορροπίας που προκύπτουν από τα παιχνίδια παρεμβολών χαρακτηρίζουν την αναμενόμενη απόδοση στα πλαίσια των DoS επιθέσεων, αποτελώντας οδηγό για τον σχεδιασμό ασφαλών ασύρματων επικοινωνιών.

Στο σημείο αυτό αξίζει να τονιστεί ότι οι διαθέσιμες στρατηγικές κάθε παίχτη είναι πολύ συγκεκριμένες, ανάλογα με το σύνολο των ενεργειών και τον τύπο που του έχει ανατεθεί(παρεμβολέας ή απλός πομπός), στις οποίες και έχει αντιστοιχιστεί κατάλληλη συνάρτηση χρησιμότητας και την οποία επιδιώκει να μεγιστοποιήσει ως απάντηση στις στρατηγικές των υπολοίπων.

Στην ίδια κατεύθυνση κινούνται και οι μελέτες [45] και [48] εξετάζοντας παίγνια από δύο διαφορετικές οπτικές πρόσβασης στο στρώμα MAC, ελεγχόμενης ισχύος και τυχαίας προσπέλασης. Όπως είναι λογικό, η σκοπιά προσέγγισης του στρώματος επηρεάζει τις ενέργειες και τις χρησιμότητες των χρηστών.

Πιο συγκεκριμένα, στην [48] μελετάται ένα μη συνεργατικό παίγνιο, στο οποίο οι πομποί και οι παρεμβολείς επιλέγουν τη δική τους ισχύ μετάδοσης για την εξισορρόπηση του κόστους μετάδοσης που υπόκειται σε περιορισμούς ενέργειας και καθυστέρησης. Πιο αναλυτικά, κάθε πομπός επιδιώκει να ελαχιστοποιήσει το μέσο κόστος ενέργειάς του σύμφωνα με ένα προκαθορισμένο στόχο που έχει θέσει, ο οποίος μπορεί να διατυπωθεί ως ένα άνω όριο στη μέση καθυστέρηση πακέτων. Από την άλλη , κάθε παρεμβολέας επιδιώκει να μεγιστοποιήσει το μέσο κόστος ενέργειας των πομπών σύμφωνα με τον δικό τους περιοριστικό παράγοντα σε μέση κατανάλωση ενέργειας.

Η προαναφερθείσα προσέγγιση τίθεται στα πλαίσια της δυναμικής μεταβολής της κυκλοφορίας πακέτων στο δίκτυο, σενάριο ιδιαίτερα ρεαλιστικό, καθώς ένας εκπομπός μπορεί να λαμβάνει είτε με εκρηκτικό τρόπο και σε συνεχή χρόνο πακέτα από μια εφαρμογή, είτε με τυχαίο τρόπο και ανά τακτά χρονικά διαστήματα. Συνεπώς, με δυναμική κίνηση, ένας παρεμβολέας θα έχει επιτυχές έργο μόνο όταν οι ουρές του πομπού δεν είναι κενές. Εντούτοις, σε ένα κατανεμημένο ασύρματο δίκτυο, οι παρεμβολείς μπορεί να μην έχουν πρόσβαση στην κατάσταση ουράς των πομπών, με τους τελευταίους να μπορούν ενδεχομένως να επωφεληθούν από την απόκρυψη αυτών των πληροφοριών.

Πράγματι, εξετάζοντας διάφορα μοντέλα, αρχικά με ένα ζευγάρι πομπού και παρεμβολέα, παρουσία ενός αλλά και πολλών δεκτών, και στη συνέχεια με αυθαίρετο αριθμό κόμβων, η [48] οδηγείται στο συμπέρασμα ότι οι παρεμβολείς αντιμετωπίζουν απώλεια απόδοσης(οι πομποί έχουν μεγαλύτερη εφικτή απόδοση και μικρότερο μέσο κόστος ενέργειας) όταν δεν γνωρίζουν αν οι ουρές των πομπών είναι κενές ή όχι, καθώς ενδέχεται να ξεκινήσουν επίθεση ενώ δεν υπάρχει μετάδοση πακέτων. Συνεπώς, η αβεβαιότητα κυκλοφορίας είναι ευεργετική για τους τελευταίους.

Ίδιο παράγοντα αβεβαιότητας ελέγχει και η [45] αλλά στα πλαίσια καναλιών τυχαίας πρόσβασης με πιθανότητα σύγκρουσης, δηλαδή οι κόμβοι ελέγχουν πλέον την πιθανότητα μετάδοσης και όχι το επίπεδο ισχύος. Ταυτόχρονη λοιπόν μετάδοση στο ίδιο χρονικό παράθυρο σε ένα κανάλι οδηγεί σε σύγκρουση. Όπως είναι φυσικό, ανάλογα συμπεράσματα με πριν προέκυψαν και στην εν λόγω περίπτωση, όπου μελετήθηκε το σενάριο ο παρεμβολέας να αποκτήσει λάθος πληροφορίες για την κατάσταση της ουράς του πομπού, γεγονός το οποίο θα συμβεί με δεδομένη πιθανότητα αυξάνοντας το επίπεδο ασάφειας που επικρατεί, αλλά και σενάριο με δυνατότητα ανίχνευσης φέροντος από την πλευρά του παρεμβολέα, επιτρέποντάς του δηλαδή να γνωρίζει πότε θα εκπέμψει ο πομπός. Επιπλέον έγινε επέκταση της μελέτης σε πολυκαναλική επικοινωνία επιτρέποντας την σύνδεση ενός κόμβου στο σημείο πρόσβασης από διάφορα πιθανά υποκανάλια, επιλέγοντας βέβαια ένα κάθε φορά για να μεταδώσει. Όπως είναι προφανές, η αύξηση του αριθμού των υποκαναλιών και η δυνατότητα μεταπήδησης από το ένα στο άλλο μειώνει την πιθανότητα παρεμβολής.

Από την σκοπιά και των δύο οπτικών πρόσβασης στο MAC στρώμα εξετάζει την συνύπαρξη των 2 αντιπάλων η ερευνητική μελέτη [43] αλλά με επίκεντρο τον βαθμό αβεβαιότητας ως προς τον τύπο των υπόλοιπων κόμβων. Κάθε τύπος χαρακτηρίζεται από μια συνάρτηση χρησιμότητας που εξαρτάται από το ενεργειακό κόστος και την ανταμοιβή από την απόδοσή του. Αύξηση του επιπέδου ασάφειας ως προς τους εκπομπούς, λειτουργεί και πάλι ευεργετικά γι' αυτούς, καθώς οι παρεμβολείς δεν έχουν κανένα κίνητρο να μπλοκάρουν τις μεταξύ τους μεταδόσεις, με αποτέλεσμα να γίνουν λιγότερο επιθετικοί στις αποφάσεις τους για παρεμβολή, όσο δεν είναι σίγουροι για τον αν οι αντίπαλοι κόμβοι είναι εγωιστές εκπομποί. Στο σημείο αυτό αξίζει να τονιστεί, ότι στην εν λόγω προσέγγιση, η αβεβαιότητα του τύπου των κόμβων διατυπώθηκε και από κοινού με την αβεβαιότητα του ενεργειακού κόστους ως πιθανολογικές πεποιθήσεις(κατανομές πιθανότητας) με τον καθορισμό κατωφλίων αποκοπής για μονοτονικές αποφάσεις μετάδοσης(μεταδίδει ή περιμένει ανάλογα με το κατώφλι).

Ιδιαίτερο ενδιαφέρον παρουσιάζει η [49], όπου γίνεται μελέτη σε ένα υποθαλάσσιο δίκτυο αισθητήρων, το οποίο είναι πιο ευάλωτο σε επιθέσεις παρεμβολής από ένα εσωτερικό ασύρματο δίκτυο. Συγκεκριμένα, λόγω των στενών σε εύρος ζώνης ακουστικών σημάτων και του περιβάλλοντος διάδοσης χρονικής μεταβλητότητας, δεν μπορούν να αντιμετωπιστούν πλήρως οι προαναφερθείσες με τεχνικές κατανεμημένου φάσματος, όπως η αναπήδηση συχνότητας, τεχνικές ιδιαίτερα διαδεδομένες σε ευρυζωνικά δίκτυα ραδιοσυχνοτήτων. Επιπλέον, λόγω της κινητικότητας των αισθητήρων και των παρεμβολέων σε δυναμικά υποθαλάσσια περιβάλλοντα, είναι πρόκληση για τους αισθητήρες να ανιχνεύουν και να εντοπίσουν τους δεύτερους.

Πιο αναλυτικά στην [49], κάθε αισθητήρας επιλέγει την ισχύ μετάδοσής του , παρουσία σημάτων παρεμβολής, ώστε να μεγιστοποιήσει την χρησιμότητά του βάσει του SINR των νόμιμων σημάτων, που φτάνουν στην δεξαμενή που βρίσκεται στην επιφάνεια, και του κόστους μετάδοσης. Από εκεί και πέρα, το στατικό σενάριο παρεμβολής, όπου κάθε παίκτης ξέρει το κέρδος του καναλιού για τα ακουστικά σήματα, μελετάται ικανοποιητικά από την θεωρία παιγνίων, οδηγούμενο σε ένα κατά Nash σημείο ισορροπίας το οποίο αναλύεται μέσω διάφορων προσομοιώσεων σε όρους απόστασης του παρεμβολέα από την δεξαμενή της επιφάνειας.

Από την άλλη, για το σενάριο δυναμικού και άγνωστου υποθαλάσσιου περιβάλλοντος, στο οποίο αισθητήρες και παρεμβολείς κινούνται με τυχαίες ταχύτητες και κατευθύνσεις στον χρόνο, ακολουθείται μια μέθοδος για την αντιμετώπιση της παρεμβολής που στηρίζεται στην ενισχυμένη μάθηση, περιοχή της μηχανικής μάθησης, με τον κάθε αισθητήρα να διαλέγει την ισχύ μετάδοσής του χωρίς γνώση του κέρδους και γενικότερα των παραμέτρων του καναλιού των παρεμβολέων. Συγκεκριμένα, επιστρατεύεται η Q-μάθηση, η οποία μπορεί να χρησιμοποιηθεί για να βρει μια βέλτιστη πολιτική επιλογής δράσης για οποιαδήποτε δεδομένη (πεπερασμένη) διαδικασία απόφασης Markov, μια στοχαστική διαδικασία διακριτού χρόνου, χρήσιμη για την μελέτη προβλημάτων βελτιστοποίησης μέσω δυναμικού προγραμματισμού και ενισχυτικής μάθησης (Markov Decision Process -MDP). Πιο αναλυτικά, λειτουργεί με την εκμάθηση μιας συνάρτησης αξίας ενεργειών που τελικά δίνει την αναμενόμενη χρησιμότητα της λήψης μιας δεδομένης ενέργειας σε μια δεδομένη κατάσταση και ακολουθώντας τη βέλτιστη πολιτική στη συνέχεια. Στην προκειμένη περίπτωση, η Q συνάρτηση έχει ως ορίσματα την παρούσα κατάσταση και την ισχύ μετάδοσης του αισθητήρα.

Παράλληλα με τους παράγοντες αβεβαιότητας που διαμορφώνουν ένα παιχνίδι παρεμβολής, η πορεία του τελευταίου σχετίζεται πλήρως με το αν το παιχνίδι είναι ενός σταδίου η δυναμικό. Στο πρώτο, σε κάθε χρονοθυρίδα, εκπομποί και παρεμβολείς, επιλέγουν στρατηγικές για να μεγιστοποιήσουν την αναμενόμενη χρησιμότητά τους σε κάθε γύρο με βάση την δεδομένου τύπου κατανομή που ισχύει γι' αυτήν. Αποφάσεις και αποτελέσματα προηγούμενων γύρων δεν έχουν καμία απολύτως επίδραση. Αντίθετα, στα δυναμικά παιχνίδια, τα οποία συναντιούνται και στην πράξη, αν οι ίδιοι κόμβοι αλληλεπιδρούν επανειλημμένα σε πολλαπλά χρονικά διαστήματα, ωθούνται στο να μάθουν και να προσαρμοστούν στις στρατηγικές των αντιπάλων τους, γεγονός που δεν επιβάλει εκ των προτέρων γνώση των κατανομών του τύπου και γενικότερα των παραμέτρων των υπόλοιπων παικτών. Με άλλα λόγια λοιπόν, σε ένα πλαίσιο παρεμβολής, ο παίκτης μπορεί να μην παρακολουθεί την δράση των υπολοίπων, αλλά από ανατροφοδότηση μέσω πρωτοκόλλων να συμπεραίνει γι αυτήν προσαρμόζοντας κάθε φορά τις αποφάσεις εκπομπής του μέσω συνεχής ενημέρωσης της στρατηγικής του. Για παράδειγμα, σε ένα MAC τυχαίας πρόσβασης, τριμερής ανατροφοδότηση είναι συνήθως διαθέσιμη (αναμονή, επιτυχία, σύγκρουση) ενώ και η στιγμιαία SINR τιμή ανατροφοδοτείται συχνά για έλεγχο ισχύος.

Δύο σημαντικοί αλγόριθμοι εκμάθησης που συμβάλουν στην προαναφερθείσα ανανέωση των στρατηγικών των παικτών είναι το παιχνίδι κλίσης(gradient play) και το πλασματικό παιχνίδι(fictitious play)[50],[42]. Στο πρώτο, ενσωματωμένο στα πλαίσια του ελέγχου ισχύος, στο τέλος κάθε χρονοθυρίδας, οι χρήστες αξιολογούν την κλίση της

χρησιμότητάς τους σε σχέση με την δικιά τους δράση στο παρόν σημείο λειτουργίας και στη συνέχεια προσαρμόζουν τις ενέργειές τους στο επόμενο χρονικό παράθυρο κάνοντας ένα βήμα προς αυτή την κατεύθυνση. Σε μια MAC ελέγχου ισχύος, η SINR ανατροφοδότηση, μαζί με τις εκτιμήσεις του καναλιού, παρέχει επαρκείς πληροφορίες για τον υπολογισμό αυτής της κλίσης. Μάλιστα, σύμφωνα με αριθμητικά αποτελέσματα της [42], τέτοιες ενημερώσεις μπορούν να οδηγήσουν σε σύγκλιση με ίδιο SINR όπως στο παιχνίδι ενός σταδίου ενώ οι μεταδότες μπορεί να λάβουν μεγαλύτερο SINR από την περίπτωση όπου πλήρεις πληροφορίες για τον τύπο των κόμβων, είναι διαθέσιμες στον παρεμβολέα.

Από την άλλη, το πλασματικό παιχνίδι είναι ένας αλγόριθμος εκμάθησης όπου κάθε χρήστης ενημερώνει τις ενέργειές του υποθέτοντας ότι ο αντίπαλός του παίζει μια τυχαία στρατηγική που δίνεται εμπειρικά από την συχνότητα των προηγούμενων ενεργειών του. Αυτό ταιριάζει σε μια MAC με τυχαία πρόσβαση, όπου η εμπειρική συχνότητα των αποφάσεων μετάδοσης μπορεί να χρησιμοποιηθεί για την εκτίμηση της πιθανότητας μετάδοσης του αντιπάλου. Αν λοιπόν οι εμπειρικές εκτιμήσεις συγκλίνουν, αυτός ο αλγόριθμος φτάνει σε ισορροπία.

3.3 Παρεμβολές στα γνωστικά δίκτυα ραδιοσυχνοτήτων

Πριν την μελέτη της ασφάλειας στα πλαίσια του Διαδικτύου των Αντικειμένων, είναι απαραίτητη η αναφορά στα γνωστικά δίκτυα ραδιοσυχνοτήτων(Cognitive Radio Network-CRN), ένας επαναστατικός τύπος δικτύου δεδομένων που επιτρέπει αποδοτικότερη και ευφυέστερη χρήση του ραδιοφάσματος, αντιμετωπίζοντας προβλήματα στα οποία τα παραδοσιακά δίκτυα αδυνατούν να ενεργήσουν. Συγκεκριμένα, σε ένα γνωστικό δίκτυο ραδιοσυχνοτήτων, επιτρέπεται σε χρήστες χωρίς άδεια(δευτερεύοντες χρήστες) να έχουν πρόσβαση στις αδειοδοτούμενες ζώνες, χωρίς να παρεμβάλλονται από τους κατόχους νόμιμης χρήσης (κύριοι χρήστες). Το προαναφερθέν, τα καθιστά εξαιρετικά ευάλωτα σε κακόβουλες επιθέσεις, καθώς οι δευτερεύοντες χρήστες δεν κατέχουν το φάσμα και επομένως η ευκαιριακή τους πρόσβαση δεν προστατεύεται από τους αντιπάλους. Ο δυναμικός λοιπόν τρόπος διάθεσης του φάσματός τους, καθιστά δύσκολη την εφαρμογή αποτελεσματικών μέτρων ασφαλείας, καθιστώντας την τελευταία σημαντικό θέμα μελέτης[55].

Στην ερευνητική μελέτη [51] συζητιέται το πρόβλημα της παρεμβολής σε ένα γνωστικό δίκτυο ραδιοσυχνοτήτων, όπου παρεμβολείς προσπαθούν να διακόψουν την επικοινωνία των δευτερευόντων χρηστών. Πιο αναλυτικά, οι δεύτεροι είναι σε θέση να μεταδίδουν πληροφορίες σε πολλαπλά κανάλια, εκμεταλλευόμενοι την ευέλικτη πρόσβαση σε αυτά, γεγονός που καθίσταται ευεργετικό για την απόκρυψη της δράσης τους από τους παρεμβολείς, οι οποίοι φυσικά εμφανίζονται με έξυπνες στρατηγικές προσπαθώντας να επιτεθούν αποτελεσματικά. Συνεπώς, διαμορφώνεται ένα σενάριο το οποίο μοντελοποιείται ως ένα παιχνίδι μηδενικού αθροίσματος(zero-sum), μια κατάσταση δηλαδή όπου το κέρδος ή η απώλεια του ενός συμμετέχοντα εξισορροπείται από την απώλεια ή το κέρδος αντίστοιχα του αντιπάλου.

Αρχικά, εξετάζεται η κατάσταση όπου ο δευτερεύων χρήστης μπορεί να έχει μόνο σε ένα κανάλι πρόσβαση την φορά. Προκειμένου να μειωθεί η πιθανότητα να μπλοκαριστεί, πραγματοποιεί αναπήδηση σε πολλαπλά κανάλια, με την προκύπτουσα στρατηγική,

έχοντας γίνει παραδοχή πλήρους γνώσης, να διαμορφώνεται έπειτα από κάποιους γύρους ανταγωνισμού μεταξύ των δύο αντίπαλων στρατοπέδων, βασισμένη στη διαδικασία απόφασης Markov. Μάλιστα αποδεικνύεται ότι η εν λόγω προσέγγιση οδηγεί σε ικανοποιητική εκτίμηση της ισορροπίας του παιγνίου.

Ωστόσο, όπως διευκρινίστηκε πριν, προκειμένου να προσδιοριστεί η στρατηγική άμυνας που βασίζεται στη διαδικασία απόφασης Markov, ο δευτερεύων χρήστης χρειάζεται να γνωρίζει κάποιες πληροφορίες για τον εισβολέα που ενδέχεται να μην είναι άμεσα διαθέσιμες. Ως εκ τούτου, πρέπει να παρακολουθεί και να μαθαίνει από το περιβάλλον. Στη συνέχεια λοιπόν, προτείνεται αρχικά μια διαδικασία μάθησης όπου ο δευτερεύων χρήστης υπολογίζει τις χρήσιμες παραμέτρους που βασίζονται σε προηγούμενες παρατηρήσεις χρησιμοποιώντας εκτίμηση μέγιστης πιθανοφάνειας(Maximum Likelihood Estimation-MLE). Έπειτα, ως εναλλακτικός τρόπος, εφαρμόζεται Q-μάθηση ώστε ο δευτερεύων χρήστης να μαθαίνει και να ανανεώνει την αμυντική στρατηγική του χωρίς γνώση του υποκείμενου μοντέλου Markov.

Τέλος, επεκτείνεται το μοντέλο σε κατάσταση όπου ο δευτερεύων χρήστης μπορεί να έχει πρόσβαση σε όλα τα διαθέσιμα κανάλια ταυτόχρονα, για παράδειγμα, όταν είναι εξοπλισμένος με πολλαπλά ραδιόφωνα. Κάτω από μια τέτοια περίσταση, η αμυντική στρατηγική δεν βασίζεται στην αναπήδηση μεταξύ των καναλιών, αλλά στην κατανομή της ισχύος στα τελευταία με τυχαίο τρόπο. Το προκύπτον παιχνίδι διαμορφώνεται ως ένα παίγνιο Συνταγματάρχης Blotto(Colonel Blotto game), με την στρατηγική ισορροπίας να εξάγεται σε όρους κατανομής πιθανότητας ως προς την κατανεμημένη ισχύ. Μάλιστα, όπως αποδεικνύεται, η στρατηγική άμυνας που προκύπτει μπορεί να ελαχιστοποιήσει τις ζημιές που προκαλούνται από τους επιτιθέμενους στη χειρότερη περίπτωση.

Το προαναφερθέν παίγνιο είναι ένα είδος παιγνίου μηδενικού αθροίσματος δύο ατόμων, στο οποίο οι παίκτες έχουν την εντολή να διανέμουν ταυτόχρονα περιορισμένους πόρους σε διάφορα "πεδία μάχης". Στην κλασσική έκδοση του παιχνιδιού, ο παίκτης που αφιερώνει τους περισσότερους πόρους σε ένα πεδίο μάχης το κερδίζει, με το συνολικό κέρδος(payoff) να είναι ίσο με τον συνολικό αριθμό των πεδίων που θα κερδίσει.

Στην [52] ερευνούνται βέλτιστες στρατηγικές ελέγχου ισχύος για κατανεμημένο φάσμα, το οποίο μοιράζεται στα πλαίσια ενός ανταγωνιστικού ad-hoc(αυτοοργανωμένο δίκτυο) γνωστικού δικτύου ραδιοσυχνοτήτων, με ρεαλιστικούς φυσικούς περιορισμούς, παρουσία ενός παρεμβολέα του οποίου η θέση είναι άγνωστη για τους δευτερεύοντες χρήστες. Συγκεκριμένα, θεωρείται ένα μπευζιανό σενάριο όπου οι δευτερεύοντες χρήστες επιλέγουν την κατανομή της ισχύος μετάδοσής τους σε ένα σύνολο καναλιών(σύμφωνα πάντα με την συνολική διαθέσιμη ισχύ του) ώστε να ικανοποιηθεί ο SINR περιορισμός ανά ζώνη συχνοτήτων στον παραλήπτη, έχοντας παράλληλα ελλιπείς πληροφορίες σχετικά με την θέση του παρεμβολέα. Ο τελευταίος από την άλλη, κατανέμει την ισχύ του ώστε να αποκλείσει όλες τις μεταδόσεις των δευτερευόντων χρηστών, έχοντας όμως πλήρη γνώση για την θέση τόσο των εκπομπών όσο και του παραλήπτη. Ως εκ τούτου, βρίσκεται σε πλεονεκτική θέση.

Γίνεται λοιπόν σαφές ότι η επιτυχία μιας μετάδοσης μέσω ενός συγκεκριμένου καναλιού εξαρτάται όχι μόνο από την ισχύ που επιλέγει ο δευτερεύων χρήστης, αλλά και από την επιλογή της ισχύος του παρεμβολέα και την κατανομή πιθανότητας που διαμορφώνει την θέση του δεύτερου κοντά στον δέκτη του πρώτου. Ελέγχοντας λοιπόν αν το SINR στον δέκτη υπερβαίνει το ελάχιστο όριο, κρίνεται αναλόγως και αν η μετάδοση είναι επιτυχημένη ή όχι. Λόγω λοιπόν της ύπαρξης του προαναφερθέντος σκληρού περιορισμού, το παιχνίδι που περιγράφηκε δεν επιδέχεται απαραίτητα καθαρές στρατηγικές(pure strategies) λύσεις, με την παροχή δηλαδή πλήρως ορισμού του πως θα κινηθεί ένας παίκτης. Γι' αυτό λοιπόν διευρύνθηκε ο χώρος με μικτές στρατηγικές λύσεις(mixed strategies), στρατηγικές δηλαδή όπου κάθε παίκτης αποδίδει συγκεκριμένη θετική πιθανότητα σε κάθε καθαρή στρατηγική, με την παροχή αθροιστικών συναρτήσεων κατανομής(Cumulative Distribution Functions-CDFs) της ισχύος μετάδοσης που θα πρέπει να υιοθετήσουν ο δευτερεύων χρήστης και ο παρεμβολέας στην προκύπτουσα ισορροπία κατά Nash. Τελικά, κάθε χρήστης υιοθετεί την δική του στρατηγική χωρίς να απαιτείται πλήρης γνώση της επιλογής ισχύος μετάδοσης ή της θέσης των χρηστών.

Τέλος στις [53],[54] αντιμετωπίζεται το πρόβλημα της καταπολέμησης της επίθεσης προσομοίωσης κύριου χρήστη(Primary User Like-PUE), στα πλαίσια της οποίας ο επιτιθέμενος στέλνει σήματα κατά την περίοδο ανίχνευσης του φάσματος έτσι ώστε οι δευτερεύοντες χρήστες να εγκαταλείψουν τα αντίστοιχα κανάλια, δημιουργώντας καταστάσεις παρεμβολής κάτω από την παραδοχή γνωστών και άγνωστων στατιστικών των καναλιών αντίστοιχα. Στην πρώτη, εξάγεται η ισορροπία κατά Nash ενός παιχνιδιού μιας βολής(one shot game) όπου η κατανομή πιθανότητας της αναπήδησης εξαρτάται από την ποιότητα των διαφόρων καναλιών, με την προαναφερθείσα ισορροπία να εφαρμόζεται περαιτέρω σε παιχνίδι πολλών σταδίων. Στη δεύτερη, έγινε προσαρμογή του αλγόριθμου του προβλήματος αντίπαλων ληστών(adversarial bandit problem), με σκοπό την εξεύρεση των βέλτιστων αμυντικών στρατηγικών, χρησιμοποιώντας την εμπειρία πρόσβασης στο φάσμα.

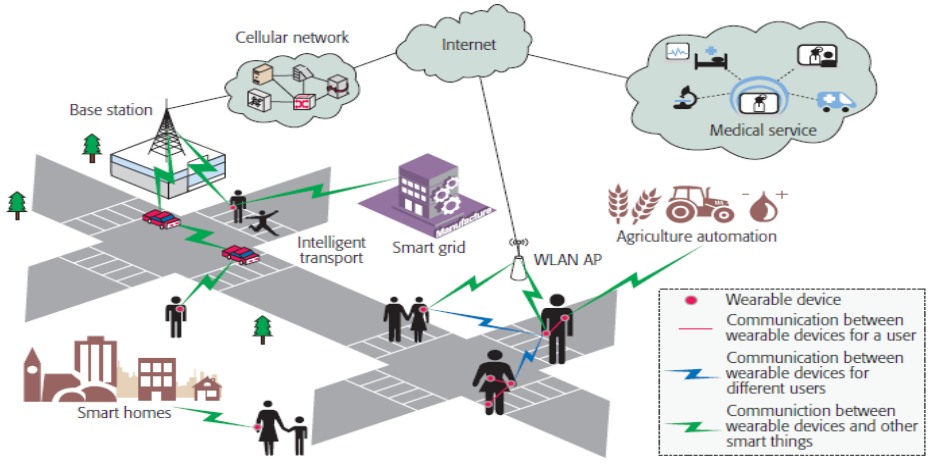
3.4 Παρεμβολές στο Διαδίκτυο των Αντικειμένων

Το Διαδίκτυο των Αντικειμένων [59] αναφέρεται σε διάφορες συσκευές και τεχνολογίες ανίχνευσης πληροφοριών όπως αισθητήρες(sensor), συσκευές αναγνώρισης μέσω ραδιοσυχνοτήτων(Radio Frequency Identification Devices-RFID), το Παγκόσμιο Σύστημα Στιγματοθέτησης(Global Position System-GPS), αισθητήρες υπερύθρων, σαρωτή λέιζερ, πηνίο αέρος κλπ . Η προαναφερθείσα ανίχνευση αναφέρεται σε συλλογή αντικειμένων ή διαδικασιών πραγματικού χρόνου στα πλαίσια της οποίας απαιτείται συνεχής παρακολούθηση, σύνδεση και αλληλεπίδραση. Το πλήθος μάλιστα των πληροφοριών που μπορούν να συλλεχθούν ποικίλει, περιλαμβάνοντας ήχους, φως, θερμότητα, ηλεκτρισμό, τοποθεσίες αλλά και πληροφορίες μηχανικής, χημείας, βιολογίας κλπ. Στα πλαίσια των προαναφερθέντων, έχοντας την δυνατότητα παροχής επικοινωνίας όχι μόνο μεταξύ ανθρώπων, αλλά και μηχανών, το Διαδίκτυο των Αντικειμένων παρέχει δυνατότητες αναγνώρισης(identification), διαχείρισης(management) και ελέγχου(control).

Καθώς λοιπόν αναπτύσσονται ραγδαία οι τεχνολογίας δικτύων και μικροκυκλωμάτων(chip), παράλληλα με την συνεχή αύξηση των απαιτήσεων των εφαρμογών, το Διαδίκτυο των Αντικειμένων εισχωρεί με ραγδαίο τρόπο σε πολλές πτυχές της ανθρώπινης ζωής, όπως για παράδειγμα στην περιβαλλοντική παρακολούθηση, την ιατρική περίθαλψη και τη δημόσια υγεία, την έξυπνη μετακίνηση και το έξυπνο δίκτυο(smart grid), οδηγώντας στην διαμόρφωση μιας έξυπνης κοινότητας όπου οι παραδοσιακές λειτουργίες διαχείρισης και παρακολούθησης προσαρμόζονται στον ευφυή έλεγχο, έτσι ώστε να ικανοποιούνται περισσότερες απαιτήσεις ελέγχου. Γίνεται λοιπόν εμφανές, ότι αρχίζει να αποτελεί αναπόσπαστο κομμάτι του σύγχρονου τρόπου ζωής.

Ωστόσο, ως σύντηξη ετερογενών δικτύων, όχι μόνο περιλαμβάνει τα ίδια προβλήματα ασφαλείας με τα δίκτυο αισθητήρων, τα δίκτυα κινητής τηλεφωνίας και το Διαδίκτυο, αλλά και αρκετά περισσότερα, όπως της προστασίας ιδιωτικής ζωής, του ελέγχου ταυτότητας και πρόσβασης ετερογενών δικτύων, της αποθήκευσης και διαχείρισης πληροφοριών κλπ [60]. Το ετερογενές λοιπόν και μεγάλης κλίμακας περιβάλλον στο οποίο διαρθρώνεται, σε συνδυασμό με τους φυσικούς και υλικούς περιορισμούς των συσκευών του[58], όπως η μνήμη, η ισχύς μετάδοσης και οι δυνατότητες επεξεργασίας τους, καθιστά τις απαιτήσεις ασφαλείας του αυστηρότερες, συγκριτικά με αυτές των συμβατικών ασύρματων δικτύων, και την μελέτη ενεργειακά αποδοτικών αμυντικών στρατηγικών ενάντια στην παρεμβολή, πολύπλοκη αλλά και απαραίτητη.

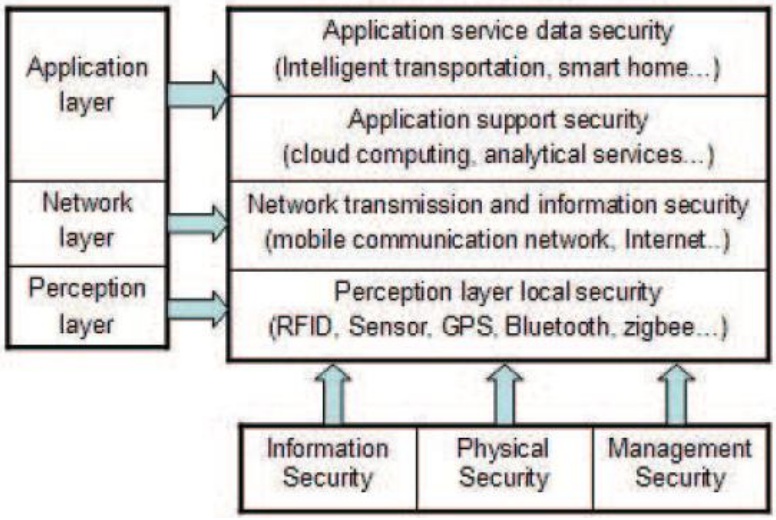
Στην ερευνητική εργασία [61] συζητιέται η σημασία της προστασίας των ευφυών φορητών συσκευών που ‘φοριούνται’ (wearables) από έξυπνες επιθέσεις, σε ένα IoT δίκτυο με επίκεντρο τον άνθρωπο, καθώς παίζουν ρόλο κλειδί στην καθημερινότητά του. Παράλληλα, αναλύονται λεπτομερώς τα διάφορα είδη των τελευταίων που μπορούν να εμφανιστούν, καθώς και αντίμετρα για την αποφυγή τους, από την σκοπιά της αυθεντικότητας, ιδιωτικότητας και ακεραιότητας των δεδομένων.



Σχήμα 4: Εικονογράφηση της αρχιτεκτονικής του ανθρωποκεντικού IoT, με έμφαση στην σύνδεση των διαφόρων wearables με τα περιβάλλοντα IoT συστατικά και εφαρμογές.

Στην ερευνητική μελέτη [57] προσεγγίζεται πιο γενικά το γεμάτο προκλήσεις θέμα της ασφάλειας του Διαδικτύου των Αντικειμένων, εστιάζοντας στην αρχιτεκτονική του και τα χαρακτηριστικά ασφαλείας που πρέπει να διαθέτει, τις επιθέσεις από τις οποίες

κινδυνεύει το κάθε στρώμα στο οποίο χωρίζεται η δομή του προαναφερθέντος(στρώμα αντίληψης, στρώμα δικτύου, στρώμα εφαρμογής) καθώς και στα μέτρα για την αντιμετώπιση των τελευταίων. Αντικείμενο της παρούσας διπλωματικής εργασίας είναι κυρίως η DoS επίθεση στο στρώμα αντίληψης, συνεπώς εκτενής ανάλυση των προηγούμενων ξεφεύγει από τους σκοπούς της.



Σχήμα 5: Αρχιτεκτονική ασφαλείας Διαδικτύου των Αντικειμένων

Στην [62] εισάγεται ένα αναλυτικό πλαίσιο για την μοντελοποίηση των επιθέσεων ασφαλείας στις IoT δομές. Το επινοημένο μοντέλο είναι αρκετά γενικό και θα μπορούσε ευέλικτα να προσαρμοστεί στις διάφορες IoT αρχιτεκτονικές, ευελιξία που οφείλεται στην υποκείμενη θεωρία. Πιο συγκεκριμένα, βασίζεται σε ένα δυναμικό G-δίκτυο(G-network), ένα ανοιχτό δίκτυο G-ουρών που εισήχθη ως μοντέλο για τα συστήματα αναμονής με συγκεκριμένες λειτουργίες ελέγχου, όπως η επαναδρομολόγηση ή η καταστροφή κυκλοφορίας, καθώς και για τα νευρωνικά δίκτυα).

Στα πλαίσια λοιπόν του προαναφερθέντος, παρατηρούνται θετικές αφίξεις που υποδηλώνουν ρεύματα δεδομένων από τα διάφορα δίκτυα συλλογής δεδομένων(π.χ. δίκτυα αισθητήρων) και αρνητικές αφίξεις που αποτελούν επιθέσεις ασφαλείας οι οποίες έχουν ως αποτέλεσμα απώλειες δεδομένων(π.χ. επιθέσεις παρεμβολής). Επίσης, λαμβάνεται υπόψη η ένταση της κάθε επίθεσης αξιολογώντας την ως ελαφριά ή βαριά. Η πρώτη συνεπάγεται απλή απώλεια δεδομένων κίνησης, ενώ η δεύτερη τεράστια. Μάλιστα, το εισαγόμενο μοντέλο επιλύεται σε σχέση με τους ρυθμούς άφιξης και αναχώρησης, σε όρους μέσου αριθμού πακέτων σε κάθε εφαρμογή, και επίπτωσης επίθεσης(ποσοστό απωλειών) ενώ αριθμητικά αποτελέσματα επιβεβαιώνουν την αξιοπιστία του.

Στην [63] μελετάται το πρόβλημα ενός δικτύου όσον αφορά την επίθεση που μπορεί να δεχτεί και την άμυνά του από την οπτική της θεωρίας των πληροφοριών(information theory), τμήμα των εφαρμοσμένων μαθηματικών που ασχολείται με την ποσοτικοποίηση της πληροφορίας. Μέσα λοιπόν από την μαθηματική μοντελοποίηση, βάσει του περίφημου θεωρήματος κωδικοποίησης του Shannon, η έρευνα ως προς τις ικανότητες επίθεσης και άμυνας μετασχηματίζεται σε έρευνα στα κανάλια του επιτιθέμενου και του

αμυνόμενου. Μάλιστα, σε πλαίσια χωρίς διαιτησία, εξετάζεται τόσο το τυφλό σενάριο επίθεσης και άμυνας, όπου κάθε συμμετέχοντας γνωρίζει τα κέρδη και τις απώλειες για τον ίδιο αλλά τίποτα για τον αντίπαλο, όσο και το μη τυφλό, όπου όλοι γνωρίζουν για τα αποτελέσματα και έχουν μάλιστα συναινέσει γι' αυτά. Για να γίνουν περισσότερο κατανοητά τα προαναφερθέντα, στην πρώτη κατηγορία ανήκει η σύγκρουση σε ένα πραγματικό πεδίο μάχης και στη δεύτερη ένας αγώνας σκάκι. Από την οπτική γωνία λοιπόν της χωρητικότητας του καναλιού, στα πλαίσια της θεωρητικής πληροφορικής, η εν λόγω μελέτη δίνει τα θεωρητικά προσπελάσιμα όρια των ικανοτήτων επίθεσης και άμυνας.

Στην [64] προτείνεται ένας μηχανισμός αντιμετώπισης της παρεμβολής, στα πλαίσια μιας θεωρητικής προσέγγισης, όπου στο διαμορφωθέν παιχνίδι ένα συγχωνευμένο κέντρο(κεντρικός έλεγχος) πρέπει να υπερασπιστεί ένα IoT δίκτυο από κόμβους, από μια κακόβουλη επίθεση μέσω ραδιοσυχνοτήτων. Συγκεκριμένα, το πρόβλημα μοντελοποιείται ως ένα Colonel Bloto παίγνιο μεταξύ παρεμβολέα και κέντρου. Στο παιχνίδι αυτό, από τη μια πλευρά ο παρεμβολέας στοχεύει στο να κατανείμει την ισχύ του ανάμεσα στους κόμβους με έξυπνο τρόπο ώστε να θέσει σε κίνδυνο το δίκτυο και χωρίς μάλιστα να τον εντοπίσουν. Από την άλλη, το κέντρο, ενεργώντας ως αμυνόμενος, στοχεύει στο να εντοπίσει ανάλογες επιθέσεις μέσω μιας πιο αποκεντρωμένης ανίχνευσης σε ένα συγκεκριμένο σύνολο κόμβων. Αν η επίθεση εντοπιστεί επιτυχώς, το κέντρο μπορεί δώσει εντολές στους στοχευμένους κόμβους να αυξήσουν την ισχύ μετάδοσής τους σε ένα κατάλληλο επίπεδο ώστε να βελτιώσουν τον σηματοθορυβικό λόγο τους και κατ' επέκταση να διατηρηθεί η απόδοση του δικτύου. Ο αλγόριθμος μάλιστα επίλυσης του παιχνιδιού βασίστηκε στο πλασματικό παιχνίδι(fictitious play) και εφαρμόστηκε σε ιεραρχική αλλά και επίπεδη αρχιτεκτονική δικτύου.

Τα αποτελέσματα έδειξαν ότι η απόδοση του δικτύου βελτιώνεται σημαντικά όσο το κέντρο έχει περισσότερα bits για να διανείμει μεταξύ των κόμβων. Επίσης αποδείχτηκε ότι ο προτεινόμενος μηχανισμός υπερισχύει του μηχανισμού κατανομής των bits με τυχαίο τρόπο. Παράλληλα προέκυψε το συμπέρασμα ότι η απόδοση του δικτύου είναι καλύτερη στην περίπτωση της ιεραρχικής αρχιτεκτονικής συγκριτικά με την επίπεδη, γεγονός που οφείλεται στο ότι το κέντρο τείνει να διαθέσει περισσότερα bits στους κόμβους υψηλότερης συνδεσιμότητας, μιας και η προαναφερθείσα αντιπροσωπεύει ως έναν βαθμό την σημαντικότητα του κόμβου για το δίκτυο.

Στο σημείο αυτό αξίζει να τονιστεί ότι γενικά επικρατεί μια αμοιβαία αντιστάθμιση μεταξύ της ικανότητας ανίχνευσης και της αποδοτικής αξιοποίησης του εύρους ζώνης. Συγκεκριμένα, υλοποιώντας ένα πλήρως κεντρικοποιημένο σύστημα ανίχνευσης, οδηγούμαστε σε βελτίωση της ικανότητας ανίχνευσης αλλά και σε χαμηλότερη παράλληλα απόδοση ως προς το εύρος ζώνης. Αντίθετα, ένα κατανεμημένο σχήμα ανίχνευσης θα αυξήσει το διαθέσιμο εύρος ζώνης του δικτύου, αλλά το αφήνει περισσότερο ευάλωτο σε ενδεχόμενη επίθεση παρεμβολής.

Στην ερευνητική εργασία [68] ερευνάται η ευπάθεια της υποδομής του Διαδικτύου των Αντικειμένων υπό επιθέσεις εκ προθέσεως, συσχετίζοντας την ανθεκτικότητα του δικτύου με την συνδεσιμότητα βάση της θεωρίας διήθησης. Η συγκεκριμένη θεωρία περιγράφει την συμπεριφορά συνδεδεμένων συστοιχιών σε ένα τυχαίο γράφο. Στα

πλαίσια λοιπόν των παραπάνω, προτείνεται και πάλι ένας κεντρικός αμυντικός σχηματισμός, στηριγμένος στο κέντρο σύντηξης, ώστε να αμβλυνθούν οι ζημιές που προκαλούνται, με τον κάθε κόμβο να ανατροφοδοτεί την ελάχιστη τοπική απόφαση (ένα bit) στο κέντρο σε περίπτωση παρεμβολής και στη συνέχεια να οδηγείται σε απομόνωση από τον IoT ελεγκτή(controller), προκειμένου να προστατευθεί το υπόλοιπο δίκτυο, ανάλογα πάντα με το επίπεδο παρεμβολής του. Με την διατύπωση της αμυντικής και επιθετικής στρατηγικής ως ένα παιχνίδι μηδενικού αθροίσματος, το αποτέλεσμα από την ισορροπία που προκύπτει χρησιμοποιείται για την αξιολόγηση της αποτελεσματικότητας του προτεινόμενου μηχανισμού ενώ αναλύεται ειδικά και η ευρωστία των δικτύων, προσανατολισμένα προς το Διαδίκτυο(internet) και τα κυβερνο-φυσικά συστήματα (Cyber-Physical System-CPS) τα οποία απεικονίζουν τα θεμέλια της μελλοντικής υποδομής του IoT.

Τα κυβερνο-φυσικά συστήματα είναι μηχανισμοί που ελέγχονται ή παρακολουθούνται από αλγορίθμους βασισμένους σε υπολογιστή, στενά συνδεδεμένους με το Διαδίκτυο και τους χρήστες. Φυσικά και λογισμικά συστατικά, που είναι βαθιά αλληλένδετα, λειτουργούν σε διαφορετικές χωρικές και χρονικές κλίμακες, παρουσιάζοντας πολλαπλές και ξεχωριστές συμπεριφορικές διαδικασίες και αλληλεπιδρώντας μεταξύ τους με πληθώρα τρόπων που αλλάζουν ανάλογα με το πλαίσιο. Παραδείγματα CPS περιλαμβάνουν το έξυπνο δίκτυο(smart grid),την ιατρική παρακολούθηση, τα ρομποτικά συστήματα, τα συστήματα ελέγχου διαδικασίας κλπ.

Αποτελέσματα έδειξαν ότι ο προτεινόμενος αμυντικός μηχανισμός λειτουργεί αποτελεσματικά, ακόμα και με την αδύναμη τοπική ικανότητα ανίχνευσης και την εγγενής εύθραυστη φύση της διάρθρωσης του δικτύου, ενώ τα δίκτυα με προσανατολισμό προς το Διαδίκτυο παρουσιάστηκαν ως πιο ευάλωτα σε σχέση με τα προαναφερθέντα, εξαιτίας της ύπαρξης κόμβων με σχετικά υψηλό βαθμό συνδεσιμότητας.

Ιδιαίτερης σημασίας είναι η μελέτη [69] που διερευνά μια σοβαρή επίθεση στα Zigbee δίκτυα που ονομάζεται φάντασμα, κινούμενη στα πλαίσια της δυνατότητας εντοπισμού του, με παράθεση ενός αλγορίθμου τριών φάσεων(προσδιορισμός υποψήφιων κόμβων, ομαδοποίηση υποψήφιων κόμβων, υπολογισμός θέσης φαντάσματος), αλλά και της αντοχής γενικότερα σε τέτοιου είδους επιθέσεις. Τα προαναφερθέντα έχουν αναγνωριστεί ως μια ιδιαίτερα σημαντική τεχνική ενεργοποίησης του IoT έχοντας όμως ως μειονέκτημα και αυτά κόμβους περιορισμένων πόρων. Στα πλαίσια λοιπόν της εν λόγω επίθεσης, ένας εισβολέας κατασκευάζει ψευδή μηνύματα για προσελκύσει ένα κόμβο ώστε να κάνει περιττούς υπολογισμούς σχετικά με την ασφάλειά του, εξαντλώντας έτσι σκόπιμα την ενέργεια του κόμβου. Οι συνέπειες της επίθεσης είναι επικίνδυνες καθώς μειώνουν σημαντικά την διάρκεια ζωής του θύματος και διευκολύνουν περεταίρω έναν αντίπαλο να πραγματοποιήσει ποικιλία επιθέσεων και ζημιών, όπως άρνηση υπηρεσίας, επίθεση επανάληψης και απώλεια εμπιστευτικότητας.

Σημαντική ερευνητική προσπάθεια αποτελεί και η [34], όπου ερευνάται το πρόβλημα της προστασίας ενός παθητικού RFID δικτύου από απειλές ασφαλείας που επιβάλλονται από εισβολείς, οι οποίοι εισάγουν υψηλές παρεμβολές στο σύστημα που οδηγούν σε διακοπή της σωστής λειτουργίας. Τα δίκτυα RFID αποτελούν αναπόσπαστο τμήμα των

αναδυόμενου Διαδικτύου των Αντικειμένων, με τα παθητικά να αναδύονται ως ενεργειακές αποδοτικά και χαμηλού κόστους λύσεις, βρίσκοντας εφαρμογή σε ευρείας κλίμακας φάσμα εφαρμογών. Ωστόσο και αυτά, λόγω των περιορισμένων δυνατοτήτων των δικτύων και των συσκευών, είναι ευάλωτα σε πολλές παρεμβατικές ενέργειες. Λεπτομερής περιγραφή της διάρθρωσης ενός τέτοιου δικτύου θα παρουσιαστεί σε επόμενο κεφάλαιο.

Στα πλαίσια λοιπόν της εν λόγω μελέτης, οι παθητικές ετικέτες(tags-αισθητήρες της συγκεκριμένης τεχνολογίας) RFID συνδέονται με μια καλά σχεδιασμένη συνάρτηση χρησιμότητας που αντανακλά από τη μία, τον στόχο τους να έχουν το σήμα τους σωστά αποδιαμορφωμένο από τον αναγνώστη(reader), και από την άλλη το επίπεδο κινδύνου από την συμμετοχή τους στο δίκτυο, κάτι που μεταξύ άλλων απορρέει από τα χαρακτηριστικά του υλικού τους χαρακτηρίζοντάς τα ως κανονικές ετικέτες ή ετικέτες εισβολέα.

Πιο αναλυτικά, κάθε συνάρτηση χρησιμότητας αποτελείται από δύο μέρη: την καθαρή συνάρτηση χρησιμότητας(pure utility function) και την συνάρτηση κινδύνου(risc function). Η πρώτη αντιπροσωπεύει τον βαθμό ικανοποίησης σε σχέση με την επίτευξη του SINR στόχου και την καταναλισκόμενη ισχύ ενώ η δεύτερη το επίπεδο κινδύνου(σε σχέση με την επίδραση και την δυνητική βλάβη στο σύστημα) λαμβάνοντας υπόψη την ισχύ αντανάκλασης και τα χαρακτηριστικά υλικού, όπως το κέρδος της κεραίας και το κέρδος οπισθοσκέδασης, έχοντας τον ρόλο συνάρτησης κόστους(cost function). Εισάγεται λοιπόν ένα πρόβλημα με κίνδυνο μετριασμού λόγω παρεμβολής, όπου στόχος αποτελεί η μεγιστοποίηση της συνάρτησης χρησιμότητας κάθε ετικέτας, με την τελευταία να επιβάλλει σιωπηρά στις ετικέτες να συμμορφώνονται σε μια πιο κοινωνική συμπεριφορά, τιμωρώντας τις ανεπιθύμητες συμπεριφορές μέσω της συνάρτησης κινδύνου.

Τέλος, λόγο της φύσης του, το προτεινόμενο πρόβλημα διατυπώνεται ως ένα μη συνεργατικό παίγνιο μεταξύ όλων των ετικετών(κανονικές και εισβολέων) και το σημείο ισορροπίας κατά Nash καθορίζεται μέσω της υιοθέτησης της θεωρίας των Supermodular παιγνίων με την σύγκλιση στο προαναφερθέν να παρουσιάζεται.

Η επισκόπηση των παρεμβολών κλείνει ικανοποιητικά με την ερευνητική μελέτη [70], όπου προτείνεται μια κεντρικοποιημένη στρατηγική αντι-μπλοκαρίσματος για IoT συστήματα, βασισμένα στην OFDM τεχνική κωδικοποίησης, και στα πλαίσια της οποίας επιτρέπεται σε έναν IoT ελεγκτή να προστατεύει τις συσκευές από κακόβουλους παρεμβολείς ραδιοσυχνοτήτων, δρώντας μάλιστα μόνος του, χωρίς δηλαδή να απαιτεί συνεργασία με τις συσκευές. Πιο αναλυτικά, οι αλληλεπιδράσεις μεταξύ του κόμβου του ελεγκτή και του παρεμβολέα μοντελοποιούνται ως ένα Colonel Bloto παίγνιο με συνεχείς και ασύμμετρους πόρους. Σε αυτό το παιχνίδι ο ελεγκτής, ενεργώντας ως αμυνόμενος, επιδιώκει να αναχαιτίσει την επίθεση παρεμβολής, διανέμοντας την ισχύ του ανάμεσα στα υποκανάλια με έξυπνο τρόπο, έτσι ώστε να μειωθεί ο συνολικός ρυθμός σφάλματος δυαδικών ψηφίων(Bit Error Rate- BER) που προκαλείται από τον παρεμβολέα. Ο τελευταίος από την άλλη, στοχεύει στη διακοπή της απόδοσης του συστήματος, κατανέμοντας την ισχύ παρεμβολής σε διαφορετικές ζώνες συχνοτήτων με στόχο να

μεγιστοποιήσει τον αριθμό των συσκευών που θα επηρεάσει. Με λίγα λόγια, και οι δύο αναζητούν την βέλτιστη εκπομπή ισχύος σε κάθε μία από τις προαναφερθείσες.

Για την επίλυση του προβλήματος, προτάθηκε ένας εξελικτικός αλγόριθμος ο οποίος μπορεί να βρει την μικτή στρατηγική ισορροπίας κατά Nash του Blotto παιγνίου, με κάθε παίκτη να επιδιώκει την μεγιστοποίηση της αποπληρωμής του υιοθετώντας τυχαία στρατηγική. Τα αποτελέσματα μάλιστα προσομοίωσης δείχνουν ότι ο προτεινόμενος αλγόριθμος επιτρέπει στον ελεγκτή να διατηρήσει πάνω από ένα αποδεκτό όριο τον BER, διατηρώντας έτσι την απόδοση του δικτύου και με παρουσία κακόβουλης εμπλοκής, με τους παίκτες να προσαρμόζονται σύμφωνα με δυναμικούς κανόνες και με δεδομένη την στρατηγική του αντιπάλου.

Ωστόσο πρέπει να διευκρινιστεί, ότι η συγκεκριμένη προσέγγιση δεν ασχολείται με την επικοινωνία ανερχόμενης ζεύξης, την μετάδοση δηλαδή σημάτων από τις IoT συσκευές προς το σημείο πρόσβασης(Access Point), όπου οι περιορισμοί ισχύος κάνουν το παιχνίδι παρεμβολής πιο πολύπλοκο. Η συγκεκριμένη λοιπόν διπλωματική εργασία, στοχεύει στην ενασχόληση με το προαναφερθέν κενό, επιδιώκοντας να το συμπληρώσει. Πλέον, έχοντας παρουσιάσει όλα τα μαθηματικά εργαλεία και τις ερευνητικές προσπάθειες που θεμελίωσαν την θεωρία γύρω από την οποία θα κινηθούμε, είμαστε έτοιμοι να προχωρήσουμε στο σενάριο που μελετήθηκε.

ΚΕΦΑΛΑΙΟ 4

ΕΛΕΓΧΟΣ ΕΞΥΠΝΗΣ ΠΑΡΕΜΒΟΛΗΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΑΝΤΙΚΕΙΜΕΝΩΝ

4.1Περιγραφή της RFID τεχνολογίας

4.2 Περιγραφή του μοντέλου συστήματος

4.3 Διατύπωση του προβλήματος ως Stackelberg παίγνιο

4.4 Αντιμετώπιση του προβλήματος έξυπνης παρεμβολής

4.1 Περιγραφή της RFID τεχνολογίας

Το δίκτυο που μελετάμε τίθεται στα πλαίσια της τεχνολογίας αναγνώρισης μέσω ραδιοσυχνοτήτων(RFID). Η προαναφερθείσα στηρίζεται στην επικοινωνία ενός αναγνώστη(reader) ραδιοσυχνοτήτων και ενός αναμεταδότη(tag/transceiver) μέσω ραδιοσημάτων χαμηλής συχνότητας. Ο αναγνώστης εκπέμπει ένα σήμα προς τον αναμεταδότη(στην βιβλιογραφία αναφέρεται ως ετικέτα), στην μνήμη του οποίου έχουν αποθηκευτεί κάποια δεδομένα, και ο αναμεταδότης, δεχόμενος αυτό το σήμα, ενεργοποιείται και αποστέλλει πίσω τα δεδομένα. Τα δεδομένα αυτά μεταδίδονται μέσω ενός ενδιάμεσου λογισμικού(middleware) στο πληροφοριακό σύστημα το οποίο αποθηκεύει και επεξεργάζεται τα συγκεκριμένα δεδομένα που συλλέγονται από τις ετικέτες.

Πιο αναλυτικά, οι αναγνώστες είναι οι συσκευές οι οποίες αναλαμβάνουν να επικοινωνήσουν με τις ετικέτες μεταδίδοντας ραδιοκύματα. Αποτελούνται από την κεραία, η οποία μεταδίδει και λαμβάνει τα σήματα από και προς τις ετικέτες, και την μονάδα ελέγχου, η οποία καθορίζει τις ενέργειες που αναλαμβάνει να εκτελέσει ο αναγνώστης, όπως αποστολή και λήψη σημάτων, ανάγνωση και εγγραφή ετικετών και άλλες λειτουργίες που καθορίζονται από το ενδιάμεσο λογισμικό.

Από την άλλη οι ετικέτες χωρίζονται σε δύο κατηγορίες, τις παθητικές και τις ενεργητικές, ανάλογα με την κατασκευή τους. Επίσης, λόγω κατασκευής, κατηγοριοποιείται ξεχωριστά και μια ακόμα μορφή ετικέτας, η οποία είναι ενδιάμεση των δύο παραπάνω κατηγοριών, οι ημι-παθητικές ετικέτες.

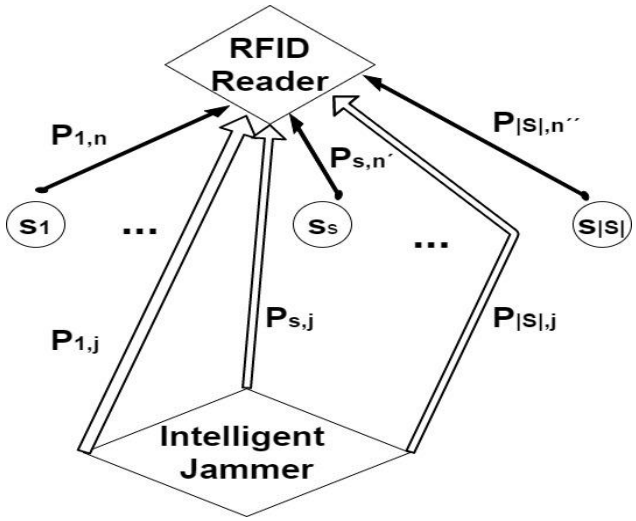
Οι παθητικές ετικέτες(passive tags) αποτελούνται από ένα μικροτσιπ και μια κεραία. Ο αναγνώστης στέλνει ραδιοκύματα τα οποία στη συνέχεια, μέσω της κεραίας, μεταδίδουν ηλεκτρικό ρεύμα στο μικροκύκλωμα που περιλαμβάνει η ετικέτα. Αυτή στέλνει με τον τρόπο αυτό τα δεδομένα, τα οποία έχουν αποθηκευτεί στο μικροτσιπ, ως απάντηση. Όπως γίνεται αντιληπτό λοιπόν, έχουν την ικανότητα να λειτουργούν δίχως να τροφοδοτούνται με ηλεκτρικό ρεύμα από δική τους πηγή, γεγονός που τις καθιστά φθηνές επιλογές αλλά περιορίζει παράλληλα την εμβέλεια λειτουργίας τους και το εύρος των δεδομένων που μπορούν να αποθηκεύσουν και να αναμεταδώσουν.

Οι ενεργές ετικέτες(active tags) λειτουργούν με τον ίδιο ακριβώς τρόπο που λειτουργούν και οι παθητικές. Η διαφορά τους έγκειται στην τροφοδοσία του κυκλώματος που προκαλεί την αναμετάδοση των δεδομένων καθώς διαθέτουν μπαταρίες και μπορούν συνεπώς από μόνες τους να τροφοδοτήσουν το προαναφερθέν. Το παραπάνω επιτρέπει μεγαλύτερη εμβέλεια αναμετάδοσης και μεγαλύτερο μέγεθος αποθηκευμένων δεδομένων αλλά οδηγεί και σε υψηλότερο κόστος.

4.2 Περιγραφή του μοντέλου συστήματος

Θεωρούμε ένα IoT δίκτυο, βασισμένο στην RFID τεχνολογία, το οποίο αποτελείται από $|N|$ παθητικές RFID ετικέτες, όπου N δηλώνει το αντίστοιχο σύνολο τους. Όπως

προειπώθηκε, οι παθητικές ετικέτες δεν έχουν μπαταρία, και ενεργοποιούνται από την σταθερή εκπεμπόμενη ισχύ του αναγνώστη P_R αντανακλώντας πίσω σε αυτόν τις πληροφορίες τους. Επίσης θεωρούμε ότι οι παθητικές ετικέτες έχουν κανονική συμπεριφορά και δεν έχουν κακόβουλη συμπεριφορά μεταξύ τους. Στην υπόλοιπη λοιπόν ανάλυση, θα τις αναφέρουμε ως κανονικές ετικέτες(normal tags). Παράλληλα, θεωρούμε ένα OFDMA περιβάλλον επικοινωνίας, όπου κάθε κανονική ετικέτα $n, n \in N$ καταλαμβάνει ένα υποκανάλι $s, s \in S$ για την μετάδοση των πληροφοριών της. Το σύνολο των υποκαναλιών ορίζεται ως S, όπου $S = \{1, ..., s, ..., |S|\}$.



Σχήμα 6: Έξυπνη παρεμβολή σε ένα RFID δίκτυο

Μέσα στο δίκτυο, υποθέτουμε την ύπαρξη μιας ενεργής RFID ετικέτας παρεμβολής, ετικέτας δηλαδή με μπαταρία. Ο παρεμβολέας πραγματοποιεί επιθέσεις παρεμβολής ελέγχοντας έξυπνα και κατανέμοντας την ισχύ του σε όλα τα υποκανάλια με τέτοιο τρόπο ώστε να μεγιστοποιείται η προκληθείσα βλάβη στο IoT σύστημα, δηλαδή, ο αριθμός των επηρεαζόμενων κανονικών ετικετών. Εδώ θα πρέπει να διευκρινιστεί ότι ενώ κάθε παθητική ετικέτα θεωρείται ότι καταλαμβάνει ένα υποκανάλι, ο παρεμβολέας μπορεί να καταλάβει ταυτόχρονα όλα τα διαθέσιμα κανάλια εάν το επιθυμεί.

Με $g_{s,n}$ και $g_{s,j}$ δηλώνουμε τα κέρδη ισχύος καναλιού σε κάθε υποκανάλι $s, s \in S$ για την κανονική ετικέτα $n, n \in N$ και τον έξυπνο παρεμβολέα j αντίστοιχα. Δεδομένου ότι το εύρος ζώνης του κάθε υποκαναλιού είναι σχετικά μικρό σε σύγκριση με το συνολικό εύρος ζώνης του συστήματος, μοντελοποιούμε τα υποκανάλια μεταξύ ετικετών και αναγνώστη ως κανάλια επίπεδων διαλείψεων Rayleigh(flat-fading). Επίσης, θεωρούμε οπισθοσκέδαση μακρινού πεδίου σε ζώνες πολύ υψηλής συχνότητας(Ultra High Frequency-UHF), όπου η εξασθένιση του ηλεκτρομαγνητικού(Eletromagnetic-EM) πεδίου είναι ανάλογη με $1/d^2$, όπου το d υποδηλώνει την απόσταση μεταξύ ετικέτας και αναγνώστη. Το σήμα παρεμβολής παρεμβαίνει στην μετάδοση του σήματος πληροφορίας της κανονικής ετικέτας σε κάθε υποκανάλι $s, s \in S$, όπως παρουσιάζεται στην εικόνα 6. Ως εκ τούτου, ο σηματοθορυβικός λόγος(SINR) της n κανονικής ετικέτας πάνω από το υποκανάλι s στον αναγνώστη δίνεται από τον εξής τύπο:

$$\gamma_{s,n} = \frac{g_{s,n} P_{s,n}}{g_{s,j} P_{s,j} + I_0}, \forall s \in S, \forall n \in N \quad (1)$$

όπου I_0 ορίζει την ισχύ θορύβου και $P_{s,n}$, $P_{s,j}$ την ισχύ αντανάκλασης της κανονικής ετικέτας n και την ισχύ μετάδοσης του έξυπνου παρεμβολέα στο υποκανάλι s, αντίστοιχα. Η ισχύς αντανάκλασης $P_{s,n}$ της κανονικής ετικέτας έχει άνω όριο, δηλαδή $P_{s,n} \in \left(0, P_n^{Max}\right]$, όπου P_n^{Max} είναι η μέγιστη εφικτή ισχύς αντανάκλασης. Η τελευταία εξαρτάται: (α) από τα χαρακτηριστικά της τοπολογίας(π.χ. την απόσταση d_n μεταξύ RFID αναγνώστη και ετικέτας) και (β) τα χαρακτηριστικά υλικού της ετικέτας. Υποθέτοντας επικοινωνία ενός βήματος(single hop) το άνω όριο αντανάκλασης της παθητικής ετικέτας είναι:

$$P_n^{Max} = P_R G_R G_n K_n \left(\frac{\lambda}{4\pi d_n}\right)^2 \quad (2)$$

όπου P_R είναι η ισχύς μετάδοσης του αναγνώστη R, από την απευθείας επικοινωνία με την n παθητική ετικέτα, G_R και G_n τα κέρδη κεραίας αναγνώστη και κανονικής ετικέτας αντίστοιχα, K_n το κέρδος οπισθοσκέδασης της n ετικέτας. Ο παράγοντας $\left(\frac{\lambda}{4\pi d_n}\right)^2$ περιγράφει τις απώλειες διαδρομής στον ελεύθερο χώρο.

Στην συνέχεια, θεωρούμε ότι κάθε κανονική ετικέτα έχει μια στοχευμένη SINR τιμή γ_n^{target} η οποία αντανακλά τις QoS προϋποθέσεις. Συνεπώς, υποθέτουμε ότι κάθε κανονική ετικέτα, προκειμένου να μεταδώσει επιτυχώς το σήμα πληροφορίας του πάνω από το s υποκανάλι, η λαμβανόμενη SINR τιμή $\gamma_{s,n}$ πρέπει να είναι μεγαλύτερη ή ίση με την στοχευμένη τιμή γ_n^{target}. Άρα, η συνθήκη επιτυχούς μετάδοσης στο υποκανάλι s ορίζεται ως εξής :

$$\frac{g_{s,n} P_{s,n}}{g_{s,j} P_{s,j} + I_0} \geq \gamma_n^{target} \quad (3)$$

4.3Διατύπωση του προβλήματος ως Stackelberg παίγνιο

Προκειμένου να προσομοιώσουμε την συμπεριφορά της ετικέτας και του παρεμβολέα κάτω από ένα κοινό πλαίσιο βελτιστοποίησης, υιοθετείται η έννοια της συνάρτησης χρησιμότητας. Πιο αναλυτικά, τόσο οι κανονικές ετικέτες όσο και ο έξυπνος παρεμβολέας συνδέονται με μια διαφοροποιημένη συνάρτηση χρησιμότητας, η οποία αποτελείται από δύο μέρη: (α) την καθαρή(pure function) συνάρτηση χρησιμότητας και (β) τη βασισμένη στη χρησιμότητα συνάρτηση κόστους(cost function), σε σχέση με την ισχύ. Όσον αφορά τις κανονικές ετικέτες, η καθαρή συνάρτηση χρησιμότητά τους αντιπροσωπεύει τον βαθμό ικανοποίησής τους σε σχέση με την επίτευξη του

στοχευμένου SINR γ_n^{target} , ενώ η συνάρτηση κόστους τους αντιπροσωπεύει το κόστος χρήσης(usage cost) της ισχύος αντανάκλασης. Η δεύτερη επιβάλει μια συντηρητική συμπεριφορά στις κανονικές παθητικές ετικέτες, προκειμένου να εκφράσουν αποτελεσματικά τις ανάγκες τους, όσον αφορά την ισχύ που αντανακλούν, εξοικονομώντας έτσι τις δαπάνες ενέργειας του αναγνώστη προκειμένου να ενεργοποιήσει τις παθητικές ετικέτες. Συνεπώς, η συνάρτηση χρησιμότητας των προαναφερθέντων διαμορφώνεται ως εξής:

$$U_{s,n}\left(P_{s,n},P_{s,j}\right)=\frac{g_{s,n}P_{s,n}}{g_{s,j}P_{s,j}+I_0}-cP_{s,n} \qquad (4)$$

όπου το c δηλώνει το κόστος χρήσης της ισχύος αντανάκλασης για κάθε μονάδα ισχύος. Επιπλέον, συνυπολογίζοντας ότι οι IoT εφαρμογές που βασίζονται στην εν λόγω τεχνολογία είναι χαμηλής μετάδοσης σε bit πληροφορίας, υποθέτουμε ότι ένα υποκανάλι για κάθε κανονική ετικέτα είναι αρκετό ώστε να αντανακλάσει την πληροφορία της στον αναγνώστη.

Όσον αφορά τον παρεμβολέα j , η καθαρή συνάρτηση χρησιμότητας αντιπροσωπεύει την ικανότητά του να παρεμποδίσει την επιτυχή μετάδοση πληροφοριών από κάθε κανονική ετικέτα $n, n \in N$ σε κάθε υποκανάλι $s, s \in S$ μέσα στο δίκτυο. Επίσης, η συνάρτηση κόστους αντιπροσωπεύει το κόστος της ισχύος μετάδοσής του εξαιτίας του γεγονότος ότι ο παρεμβολέας είναι μια ενεργή RFID ετικέτα με περιορισμένη μπαταρία. Η μέγιστη ισχύς μετάδοσης του παρεμβολέα σε κάθε υποκανάλι ορίζεται ως $P_{s,j}^{Max}$, όπου $\sum_{s=1}^{|S|} P_{s,j}^{Max} = P_j^{Max}$. Ως εκ τούτου, η συνάρτηση χρησιμότητας του έξυπνου παρεμβολέα σε κάθε υποκανάλι $s, s \in S$ είναι η εξής:

$$U_{s,j}\left(P_{s,n},P_{s,j}\right)=-\frac{g_{s,n}P_{s,n}}{g_{s,j}P_{s,j}+I_0}-c_jP_{s,j} \quad (5)$$

Στο προτεινόμενο πλαίσιο, η ενεργή ετικέτα παρεμβολής θεωρείται ότι διαθέτει τόσο ευφυΐα όσο και γνώση, συνεπώς είναι ικανή να ελέγχει και να προσαρμόζει την ισχύ εκπομπής της $P_{s,j}$, $\forall s \in S$ βασισμένη στην ισχύ αντανάκλασης της κανονικής ετικέτας $P_{s,n}, \forall s \in S, \forall n \in N$, έτσι ώστε να προκαλέσει την μέγιστη δυνατή ζημιά στην αποδιαμόρφωση του σήματος πληροφορίας που μεταδίδεται από την κανονική ετικέτα στον αναγνώστη. Επομένως, αντιμετωπίζουμε το πρόβλημα ελέγχου έξυπνης παρεμβολής(intelligent jamming control-IJC) ως πρόβλημα ελέγχου της ισχύος αντανάκλασης της κανονικής ετικέτας και της ισχύος μετάδοσης του παρεμβολέα σε κάθε υποκανάλι $s, s \in S$. Το προαναφερθέν λοιπόν πρόβλημα διατυπώνεται ως ένα Stackelberg παίγνιο, ένα στρατηγικό παιχνίδι στα οικονομικά όπου η ηγετική επιχείρηση κινείται πρώτη και στη συνέχεια οι επιχειρήσεις ακόλουθοι κινούνται διαδοχικά. Στην θεωρία παιγνίων, οι παίκτες του προαναφερθέντος είναι ο ηγέτης(leader) και ο

ακόλουθος(follower) και ανταγωνίζονται μεταξύ τους σε ποσότητα. Εν προκειμένω, κανονική ετικέτα και έξυπνος παρεμβολέας είναι οι παίκτες με την πρώτη να είναι ο ηγέτης και τον δεύτερο ο ακόλουθος.

Όπως παρουσιάζεται και στην εικόνα 6, κάθε υποκανάλι λογίζεται ως ένα ανεξάρτητο πεδίο μάχης, όπου οι δύο προαναφερθέντες ανταγωνίζονται μεταξύ τους διανέμοντας τις δυνάμεις τους, δηλαδή την ισχύ τους, με τον παίκτη που κατανέμει το υψηλότερο επίπεδο δύναμης να κερδίζει. Στο σημείο αυτό τονίζεται ότι η βέλτιστη στρατηγική για κάθε κανονική ετικέτα δεν είναι απαραίτητα ταυτόσημη με την μέγιστη ισχύ αντανάκλασης. Στην περίπτωση αυτή, ο ευφυής παρεμβολέας θα γνώριζε εκ των προτέρων την στρατηγική όλων των κανονικών ετικετών και θα μπορούσε έτσι να επιτεθεί ευκολότερα ελέγχοντας στρατηγικά την ισχύ μετάδοσής του σε κάθε υποκανάλι. Επιπλέον, στην περίπτωση που η κανονική ετικέτα διαλέξει διαφορετικό επίπεδο ισχύος αντανάκλασης από το μέγιστο δυνατό, μπορεί να προκαλέσει ταχύτερη εξάντληση της μπαταρίας του παρεμβολέα, ο οποίος θα πρέπει να διανείμει τις περιορισμένες δυνάμεις του σε ένα σύνολο από υποκανάλια, όπου σε μερικά από αυτά μπορεί να είναι ισχυρότερες οι ετικέτες.

Προκειμένου να διαμορφώσουμε το Stackelberg παίγνιο ελέγχου έξυπνης παρεμβολής σε κάθε υποκανάλι, υποθέτουμε ότι η στρατηγική της κανονικής ετικέτας $P_{s,n}, \forall s \in S, \forall n \in N$ δίνεται. Στη συνέχεια, η καλύτερη στρατηγική απάντησης του παρεμβολέα μπορεί να εξαχθεί από την λύση του προβλήματος βελτιστοποίησης της συνάρτησης χρησιμότητάς του, και δίνεται από τον εξής τύπο:

$$\max_{P_{s,j} \in \left(0, P_{s,j}^{Max}\right]} U_{s,j}\left(P_{s,n}, P_{s,j}\right) = -\frac{g_{s,n} P_{s,n}}{g_{s,j} P_{s,j} + I_0} - c_j P_{s,j} \quad (6)$$

Λαμβάνοντας υπόψη το αποτέλεσμα $P_{s,j}^{*}, \forall s \in S$ του προβλήματος βελτιστοποίησης (6), θεωρούμε ότι η κανονική ετικέτα ξέρει ότι υπάρχει ένας έξυπνος παρεμβολέας και αισθάνεται το λαμβανόμενο σήμα παρεμβολής μέσω της εκμετάλλευσης της καθυστέρησης στη λήψη απόφασης από τον παρεμβολέα, όπως θα εξηγηθεί λεπτομερώς στην επόμενη υποενότητα. Επομένως, η κανονική ετικέτα ξέρει την καλύτερη στρατηγική απάντησης του παρεμβολέα $P_{s,j}^{*}, \forall s \in S$, πριν διαλέξει την βέλτιστη αμυντική στρατηγική του. Ο στόχος λοιπόν της κανονικής ετικέτας είναι να μεγιστοποιήσει την χρησιμότητά του, συνεπώς το αντίστοιχο πρόβλημα βελτιστοποίησης διατυπώνεται ως εξής:

$$\max_{P_{s,n} \in \left(0, P_n^{Max}\right]} U_{s,n}\left(P_{s,n}, P_{s,j}\right) = \frac{g_{s,n} P_{s,n}}{g_{s,j} P_{s,j} + I_0} - c P_{s,n} \quad (7)$$

όπου $P_{s,j}^{*}$ είναι η βέλτιστη στρατηγική απάντησης του έξυπνου παρεμβολέα, όπως θα προκύψει από την λύση του προβλήματος βελτιστοποίησης (6) στην επόμενη υποενότητα.

4.4 Αντιμετώπιση του προβλήματος έξυπνης παρεμβολής

Στην υποενότητα αυτή, μελετάμε το πρόβλημα ελέγχου έξυπνης παρεμβολής ως Stackelberg παίγνιο όπως ορίζεται στις σχέσεις (6) και (7). Ο στόχος μας είναι να εξάγουμε κλειστούς τύπους που καθορίζουν την Stackelberg ισορροπία(Stackelberg Equilibrium-SE). Αρχικά, η καλύτερη στρατηγική απάντησης του παρεμβολέα σε κάθε υποκανάλι(στρατόπεδο) καθορίζεται για δοσμένη στρατηγική της κανονικής ετικέτας. Ακολούθως, με δεδομένη την βέλτιστη στρατηγική απάντησης του παρεμβολέα, εξάγουμε την βέλτιστη στρατηγική των κανονικών ετικετών σε κάθε κατειλημμένο υποκανάλι. Στη συνέχεια, εξετάζουμε το Stackelberg παίγνιο για ένα υποκανάλι $s, s \in S$. Το ίδιο πρόβλημα λύνεται ακολουθώντας το ίδιο μοτίβο για κάθε υποκανάλι $s, s \in S$.

Προκειμένου να καθορίσουμε την βέλτιστη στρατηγική απάντησης του έξυπνου παρεμβολέα j, λύνουμε το πρόβλημα βελτιστοποίησης (6) θεωρώντας δοσμένη την στρατηγική $P_{s,n}$ της κανονικής ετικέτας $n, n \in N$.

Θεώρημα 1: Δεδομένης της στρατηγικής της κανονικής ετικέτας $P_{s,n}$, η καλύτερη στρατηγική απάντησης του παρεμβολέα j στο υποκανάλι $s, s \in S$ δίνεται ως εξής:

$$P_{s,j}^{*} = \begin{cases} 0, P_{s,n} \le \dfrac{I_0^2 c_j}{g_{s,n} g_{s,j}} \\ \min\left\{ \sqrt{\dfrac{g_{s,n} P_{s,n}}{g_{s,j} c_j}} - \dfrac{I_0}{g_{s,j}}, P_{s,j}^{Max} \right\}, P_{s,n} > \dfrac{I_0^2 c_j}{g_{s,n} g_{s,j}} \end{cases} \quad (8)$$

Απόδειξη: Για την επίλυση του προβλήματος βελτιστοποίησης (6), ορίζουμε την πρώτη παράγωγο ως προς $P_{s,j}$ της συνάρτησης $U_{s,j}\left(P_{s,n}, P_{s,j}\right)$, με δεδομένη την στρατηγική της κανονικής ετικέτας $P_{s,n}$:

$$\frac{\partial U_{s,j}\left(P_{s,n}, P_{s,j}\right)}{\partial P_{s,j}} = \frac{g_{s,j} g_{s,n} P_{s,n}}{\left(g_{s,j} P_{s,j} + I_0\right)^2} - c_j$$

Έτσι, έχουμε το εξής :

$$\frac{\partial U_{s,j}\left(P_{s,n}, P_{s,j}\right)}{\partial P_{s,j}} = 0 \Leftrightarrow P_{s,j} = \sqrt{\frac{g_{s,n} P_{s,n}}{g_{s,j} c_j}} - \frac{I_0}{g_{s,j}}$$

Ωστόσο, η ισχύς μετάδοσης του παρεμβολέα $P_{s,j}$ πρέπει να είναι μεγαλύτερη από μηδέν, δηλαδή $P_{s,j} > 0$, συνεπώς θα έχουμε $P_{s,j} = \sqrt{\frac{g_{s,n} P_{s,n}}{g_{s,j} c_j}} - \frac{I_0}{g_{s,j}}$ αν $P_{s,n} > \frac{I_0^2 c_j}{g_{s,n} g_{s,j}}$. Σε κάθε

άλλη περίπτωση, αν $P_{s,n} \le \frac{I_0^2 c_j}{g_{s,n} g_{s,j}}$, η ισχύς μετάδοσης του παρεμβολέα είναι ίση με μηδέν, δηλαδή, $P_{s,j} = 0$. Επιπρόσθετα, η ισχύς μετάδοσης του παρεμβολέα είναι άνω φραγμένη, δηλαδή, $P_{s,j} \le P_{s,j}^{Max}$, ως εκ τούτου, συμπεραίνουμε ότι η καλύτερη στρατηγική απάντησης $P_{s,j}^*$ του έξυπνου παρεμβολέα είναι η εξής :

$$P_{s,j}^* = \begin{cases} 0, P_{s,n} \le \dfrac{I_0^2 c_j}{g_{s,n} g_{s,j}} \\ \min\left\{ \sqrt{\dfrac{g_{s,n} P_{s,n}}{g_{s,j} c_j}} - \dfrac{I_0}{g_{s,j}}, P_{s,j}^{Max} \right\}, P_{s,n} > \dfrac{I_0^2 c_j}{g_{s,n} g_{s,j}} \end{cases}$$

Λαμβάνοντας υπόψη την καλύτερη στρατηγική του παρεμβολέα, όπως δίνεται από την εξίσωση (8), η κανονική ετικέτα διαλέγει την βέλτιστη στρατηγική του έχοντας επίγνωση της ενδεχόμενης επίθεσης παρεμβολής. Προκειμένου να καθοριστεί η βέλτιστη στρατηγική της κανονικής ετικέτας, το πρόβλημα βελτιστοποίησης (7) θα πρέπει να επιλυθεί, με δεδομένη την καλύτερη απάντηση από πλευράς έξυπνου παρεμβολέα, δηλαδή, $P_{s,j}^*$. Ως εκ τούτου, καταλήγουμε στο εξής θεώρημα.

Θεώρημα 2: Με δεδομένη την καλύτερη στρατηγική απάντησης του παρεμβολέα, $P_{s,j}^*$, η βέλτιστη στρατηγική απάντησης $P_{s,n}^*$ της κανονικής ετικέτας $n, n \in N$ σε κάθε υποκανάλι $s, s \in S$ προκύπτει ως εξής:

$$P_{s,n}^* = \begin{cases} \min\left\{ \dfrac{g_{s,n} c_j}{4 g_{s,j} c^2}, P_n^{Max} \right\}, \dfrac{g_{s,n}}{g_{s,j} P_{s,j}^{Max} + I_0} < c \le \dfrac{g_{s,n}}{2 I_0} \\ \min\left\{ \dfrac{I_0^2 c_j}{g_{s,n} g_{s,j}}, P_n^{Max} \right\}, \dfrac{g_{s,n}}{2 I_0} < c \le \dfrac{g_{s,n}}{I_0} \\ 0, c > \dfrac{g_{s,n}}{I_0} \\ P_n^{Max}, c < \dfrac{g_{s,n}}{g_{s,j} P_{s,j}^{Max} + I_0} \end{cases} \quad (9)$$

Απόδειξη: Η κανονική ετικέτα $n, n \in N$ είναι ενήμερη για την βέλτιστη στρατηγική απάντησης $P_{s,j}^*$ του έξυπνου παρεμβολέα. Ως εκ τούτου, η συνάρτηση χρησιμότητας της πρώτης, όπως διατυπώθηκε στην εξίσωση (4), μπορεί να αναδιατυπωθεί ως εξής:

$$U_{s,n}\left(P_{s,n},P_{s,j}^{*}\right)=\begin{cases}\left(\dfrac{g_{s,n}}{I_0}-c\right)P_{s,n},P_{s,n}\le\dfrac{I_0^2c_j}{g_{s,n}g_{s,j}}\\ \sqrt{\dfrac{g_{s,n}P_{s,n}c_j}{g_{s,j}}}-cP_{s,n},P_{s,n}>\dfrac{I_0^2c_j}{g_{s,n}g_{s,j}}\\ and\ \ P_{s,n}<\left(P_{s,j}^{Max}+\dfrac{I_0}{g_{s,j}}\right)^2\dfrac{g_{s,j}c_j}{g_{s,n}}\\ \left(\dfrac{g_{s,n}}{g_{s,j}P_{s,j}^{Max}+I_0}-c\right)P_{s,n},P_{s,n}>\dfrac{I_0^2c_j}{g_{s,n}g_{s,j}}\\ and\ \ P_{s,n}\ge\left(P_{s,j}^{Max}+\dfrac{I_0}{g_{s,j}}\right)^2\dfrac{g_{s,j}c_j}{g_{s,n}}\end{cases}$$

Σημειώνεται ότι η ανίσωση $\frac{I_0^2c_j}{g_{s,n}g_{s,j}}<\left(P_{s,j}^{Max}+\frac{I_0}{g_{s,j}}\right)^2\frac{g_{s,j}c_j}{g_{s,n}}$ είναι πάντα θετική, επομένως η συνάρτηση χρησιμότητας ξαναγράφεται ως εξής :

$$U_{s,n}\left(P_{s,n},P_{s,j}^{*}\right)=\begin{cases}\left(\dfrac{g_{s,n}}{I_0}-c\right)P_{s,n},P_{s,n}\le\dfrac{I_0^2c_j}{g_{s,n}g_{s,j}}\\ \sqrt{\dfrac{g_{s,n}P_{s,n}c_j}{g_{s,j}}}-cP_{s,n},\dfrac{I_0^2c_j}{g_{s,n}g_{s,j}}<P_{s,n}<\left(P_{s,j}^{Max}+\dfrac{I_0}{g_{s,j}}\right)^2\dfrac{g_{s,j}c_j}{g_{s,n}}\\ \left(\dfrac{g_{s,n}}{g_{s,j}P_{s,j}^{Max}+I_0}-c\right)P_{s,n},P_{s,n}\ge\left(P_{s,j}^{Max}+\dfrac{I_0}{g_{s,j}}\right)^2\dfrac{g_{s,j}c_j}{g_{s,n}}\end{cases}\qquad(10)$$

Επίσης η συνάρτηση χρησιμότητας $U_{s,n}\left(P_{s,n},P_{s,j}^{*}\right)$ είναι γραμμική σε σχέση με την $P_{s,n}$ αν $P_{s,n}\le\frac{I_0^2c_j}{g_{s,n}g_{s,j}}$ ή αν $P_{s,n}\ge\left(P_{s,j}^{Max}+\frac{I_0}{g_{s,j}}\right)^2\frac{g_{s,j}c_j}{g_{s,n}}$,ενώ είναι αυστηρά κοίλη σε σχέση με την $P_{s,n}$ αν $\frac{I_0^2c_j}{g_{s,n}g_{s,j}}<P_{s,n}<\left(P_{s,j}^{Max}+\frac{I_0}{g_{s,j}}\right)^2\frac{g_{s,j}c_j}{g_{s,n}}$. Στην τελευταία περίπτωση, η πρώτη παράγωγος της $U_{s,n}\left(P_{s,n},P_{s,j}^{*}\right)$ ως προς $P_{s,n}$ δίνεται ως εξής :

$$\frac{\partial U_{s,j}\left(P_{s,n},P_{s,j}^{*}\right)}{\partial P_{s,j}}=\frac{1}{2}\sqrt{\frac{g_{s,n}c_j}{g_{s,j}P_{s,n}}}-c$$

Συνεπώς, έχουμε $\frac{\partial U_{s,j}\left(P_{s,n},P_{s,j}^{*}\right)}{\partial P_{s,j}}=0\Leftrightarrow P_{s,n}=\frac{g_{s,n}c_j}{4g_{s,j}c^2}$ το οποίο είναι ένα κρίσιμο σημείο της $U_{s,n}\left(P_{s,n},P_{s,j}^{*}\right)$. Προκειμένου να εξάγουμε τις μέγιστες τιμές της (10) μελετάμε τις ακόλουθες περιπτώσεις.

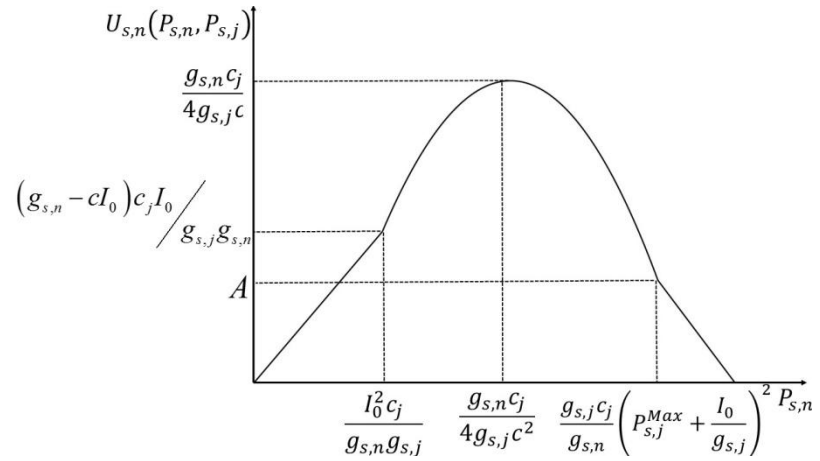
1. $\frac{g_{s,n}}{g_{s,j}P_{s,j}^{Max}+I_0} < c \le \frac{g_{s,n}}{2I_0}$. Τότε επαληθεύεται ότι $\frac{g_{s,n}c_j}{4g_{s,j}c^2} \ge \frac{I_0^2 c_j}{g_{s,n}g_{s,j}}$, επομένως η βέλτιστη στρατηγική της κανονικής ετικέτας είναι $P_{s,n}^* = \min\left\{\frac{g_{s,n}c_j}{4g_{s,j}c^2}, P_n^{Max}\right\}$, όπως παρουσιάζεται στην εικόνα 7(α), όπου $A = \frac{c_j}{g_{s,j}}\left[g_{s,j}P_{s,j}^{Max} + I_0 - \frac{c}{g_{s,n}}\left(g_{s,j}P_{s,j}^{Max} + I_0\right)^2\right]$. Σημειώνεται ότι η σχετική "απόσταση" των A και $\left(g_{s,n} - cI_0\right)c_j I_0 \Big/ g_{s,j}g_{s,n}$, εξαρτάται από τις σχετικές παραμέτρους, αλλά δεν επηρεάζει την τιμή της βέλτιστης στρατηγικής $P_{s,n}^*$..

2. $\frac{g_{s,n}}{2I_0} < c \le \frac{g_{s,n}}{I_0}$ *and* $c > \frac{g_{s,n}}{g_{s,j}P_{s,j}^{Max}+I_0}$. Τότε, επαληθεύεται ότι $\frac{g_{s,n}c_j}{4g_{s,j}c^2} < \frac{I_0^2 c_j}{g_{s,n}g_{s,j}}$, ως εκ τούτου η βέλτιστη στρατηγική της κανονικής ετικέτας είναι $P_{s,n}^* = \min\left\{\frac{I_0^2 c_j}{g_{s,n}g_{s,j}}, P_n^{Max}\right\}$,όπως παρουσιάζεται στην εικόνα 7(β).

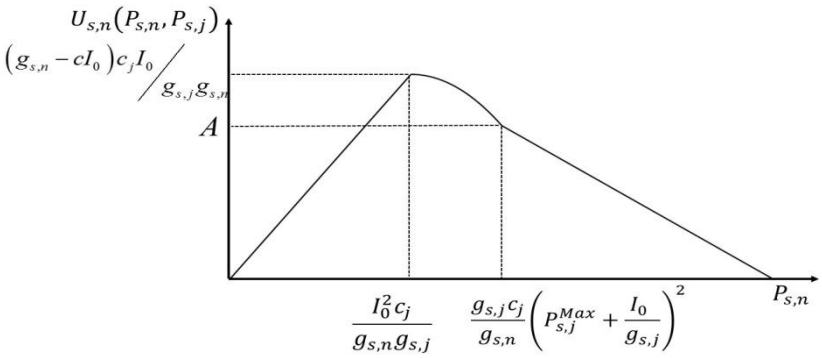
3. $c > \frac{g_{s,n}}{I_0}$. Τότε, η συνάρτηση χρησιμότητας της κανονικής ετικέτας είναι αρνητική, όπως παρουσιάζεται στην εικόνα 7(γ), επομένως η μέγιστη τιμή είναι 0 όταν $P_{s,n}^* = 0$.

4. $c < \frac{g_{s,n}}{g_{s,j}P_{s,j}^{Max}+I_0}$. Στην περίπτωση αυτή, η συνάρτηση χρησιμότητας της κανονικής ετικέτας(10) είναι γνησίως αύξουσα σε σχέση με την $P_{s,n}$, όταν $P_{s,n} > \left(P_{s,j}^{Max} + \frac{I_0}{g_{s,j}}\right)^2 \frac{g_{s,j}c_j}{g_{s,n}}$. Έτσι, η βέλτιστη στρατηγική της κανονικής ετικέτας είναι $P_{s,n}^* = P_n^{Max}$, όπως φαίνεται στην εικόνα 7(δ).

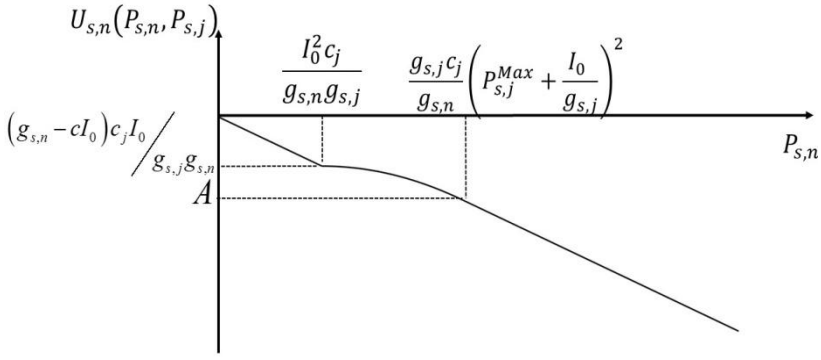
Συνδυάζοντας τις παραπάνω περιπτώσεις που παρουσιάστηκαν, καταλήγουμε στο ότι η βέλτιστη στρατηγική της κανονικής ετικέτας δίνεται από την εξίσωση (9).


$U_{s,n}(P_{s,n},P_{s,j})$
$\frac{g_{s,n}c_j}{4g_{s,j}c}$
$(g_{s,n}-cI_0)c_jI_0 / g_{s,j}g_{s,n}$
A
$\frac{I_0^2c_j}{g_{s,n}g_{s,j}}$
$\frac{g_{s,n}c_j}{4g_{s,j}c^2}$
$\frac{g_{s,j}c_j}{g_{s,n}}\left(P_{s,j}^{Max}+\frac{I_0}{g_{s,j}}\right)^2$
$P_{s,n}$

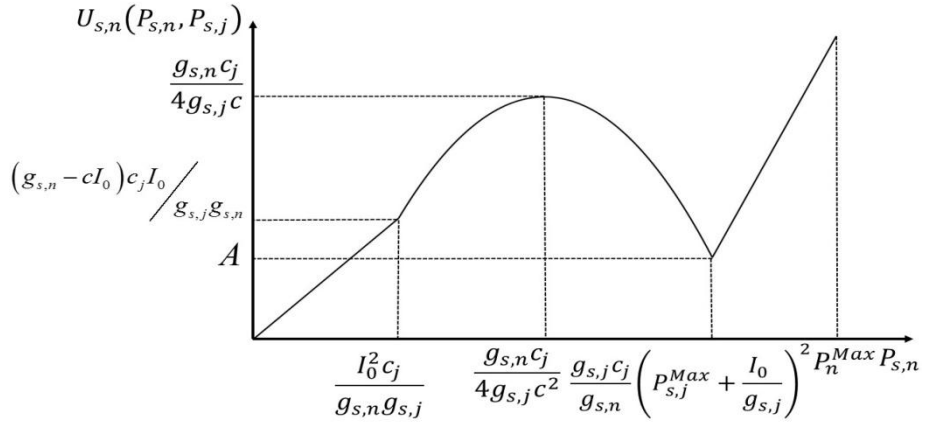
(α)


$U_{s,n}(P_{s,n},P_{s,j})$
$(g_{s,n}-cI_0)c_jI_0 / g_{s,j}g_{s,n}$
A
$\frac{I_0^2c_j}{g_{s,n}g_{s,j}}$
$\frac{g_{s,j}c_j}{g_{s,n}}\left(P_{s,j}^{Max}+\frac{I_0}{g_{s,j}}\right)^2$
$P_{s,n}$

(β)


$U_{s,n}(P_{s,n},P_{s,j})$
$\frac{I_0^2c_j}{g_{s,n}g_{s,j}}$
$\frac{g_{s,j}c_j}{g_{s,n}}\left(P_{s,j}^{Max}+\frac{I_0}{g_{s,j}}\right)^2$
$(g_{s,n}-cI_0)c_jI_0 / g_{s,j}g_{s,n}$
$P_{s,n}$
A

(γ)



(δ)

Σχήμα 7: Μορφές της συνάρτησης χρησιμότητας της κανονικής ετικέτας

Συνδυάζοντας τα Θεωρήματα 1 και 2, καταλήγουμε στην Stackelberg ισορροπία του προβλήματος έξυπνης παρεμβολής.

Θεώρημα 3 : Η Stackelberg ισορροπία του προβλήματος έξυπνης παρεμβολής είναι το ζευγάρι στρατηγικής $\left(P_{s,n}^{SE}, P_{s,j}^{SE}\right)$ σε κάθε υποκανάλι $s, s \in S$, όπου

$$P_{s,n}^{SE} = \begin{cases} \min\left\{\frac{g_{s,n}c_j}{4g_{s,j}c^2}, P_n^{Max}\right\}, \frac{g_{s,n}}{g_{s,j}P_{s,j}^{Max}+I_0} < c \le \frac{g_{s,n}}{2I_0} \\ \min\left\{\frac{I_0^2c_j}{g_{s,n}g_{s,j}}, P_n^{Max}\right\}, \frac{g_{s,n}}{2I_0} < c \le \frac{g_{s,n}}{I_0} \\ 0, c > \frac{g_{s,n}}{I_0} \\ P_n^{Max}, c < \frac{g_{s,n}}{g_{s,j}P_{s,j}^{Max}+I_0} \end{cases} \quad (11)$$

και

$$P_{s,j}^{SE} = \begin{cases} 0, P_{s,n} \le \frac{I_0^2c_j}{g_{s,n}g_{s,j}} \\ \min\left\{\sqrt{\frac{g_{s,n}P_{s,n}}{g_{s,j}c_j}} - \frac{I_0}{g_{s,j}}, P_{s,j}^{Max}\right\}, P_{s,n} > \frac{I_0^2c_j}{g_{s,n}g_{s,j}} \end{cases} \quad (12)$$

Κλείνοντας αυτό το κεφάλαιο, διευκρινίζεται ότι στην ανάλυση αξιολόγησης της επίδοσης που παρέχεται στο επόμενο κεφάλαιο, εξετάζονται δύο διαφορετικά σενάρια σχετικά με την διαθέσιμη μέγιστη ισχύ μετάδοσης του έξυπνου παρεμβολέα σε κάθε

υποκανάλι. Αρχικά, η συνολική διαθέσιμη μέγιστη ισχύς μετάδοσης του παρεμβολέα κατανέμεται ισόποσα σε όλα τα υποκανάλια. Στη συνέχεια, εξετάζεται ένα προχωρημένο σενάριο έξυπνης παρεμβολής(Advanced Intelligent Jammer Control-AIJC), όπου ο παρεμβολέας είναι σε θέση να ελέγχει την μέγιστη ισχύ μετάδοσης που διοχετεύει σε κάθε υποκανάλι προκειμένου να επιτεθεί, ενώ ανιχνεύει την ποιότητα του κέρδους καναλιού των κανονικών ετικετών σε κάθε συγκεκριμένο υποκανάλι.

ΚΕΦΑΛΑΙΟ 5

ΑΡΙΘΜΗΤΙΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

5.1 Εισαγωγικά

5.2 Σενάριο προσομοίωσης

5.3 Παρουσίαση αποτελεσμάτων και συγκριτική μελέτη

5.1 Εισαγωγικά

Στην ενότητα αυτή παρέχουμε μερικά αριθμητικά αποτελέσματα που αξιολογούν τα λειτουργικά χαρακτηριστικά και την απόδοση του προτεινόμενου πλαισίου ελέγχου έξυπνης παρεμβολής. Τα αποτελέσματα προέκυψαν από την εκτέλεση σεναρίων προσομοίωσης με την βοήθεια του υπολογιστικού περιβάλλοντος "Matlab", χρησιμοποιώντας την θεωρία και το μαθηματικό υπόβαθρο που παρατέθηκε στο προηγούμενο κεφάλαιο, μέσω κατάλληλης προσαρμογής και κωδικοποίησης.

Αρχικά, εστιάζουμε στα επιτεύγματα της απόδοσης λειτουργίας του προτεινόμενου πλαισίου όσον αφορά τις σχέσεις μεταξύ της αντανακλώμενης και της εκπεμπόμενης ισχύος των κανονικών ετικετών και του παρεμβολέα αντίστοιχα, σε κάθε κατειλημμένο υποκανάλι. Επιπλέον, διερευνάμε τις σχέσεις των τιμών χρησιμότητας υπό διαφορετικές συνθήκες καναλιού επικοινωνίας. Το προτεινόμενο πλαίσιο συγκρίνεται με το σενάριο χωρίς μηχανισμό τιμολόγησης βάσει χρήσης τόσο για τις κανονικές ετικέτες, όσο και για τον παρεμβολέα [70]. Η σύγκριση αποκαλύπτει την αμοιβαία αντιστάθμιση μεταξύ της πιο επιθετικής συμπεριφοράς του έξυπνου παρεμβολέα, η οποία προκαλεί αυξημένη ζημιά στο IoT δίκτυο, και της αντίστοιχης δαπανημένης ισχύος. Η παρεχόμενη ανάλυση πραγματοποιείται για μια γραμμική και μια τετραγωνική τοπολογία με την πρώτη να συνοδεύεται από μια Monte Carlo ανάλυση πάνω από διαφοροποιημένα κέρδη καναλιού για τις κανονικές ετικέτες και τον παρεμβολέα(υλοποιήθηκαν 10000 περιπτώσεις). Σημειώνεται ότι αρχικά θεωρήσαμε ισόποση κατανομή της συνολικής διαθέσιμης ισχύος μετάδοσης του παρεμβολέα στα διάφορα υποκανάλια.

Στη συνέχεια λοιπόν, παρουσιάζουμε ένα προχωρημένο πλαίσιο ελέγχου έξυπνου παρεμβολέα, όπου ο ευφυής παρεμβολέας όχι μόνο κατανέμει την ισχύ μετάδοσής του στα υποκανάλια με τέτοιο τρόπο ώστε να μεγιστοποιήσει την προκληθείσα ζημιά, αλλά και προσαρμόζει με σύνεση την μέγιστη δυνητικά επενδυμένη ισχύ ανά κανάλι, έτσι ώστε να αυξήσει ακόμα περισσότερο την επιβαλλόμενη ζημιά στην αντίστοιχη παθητική κανονική ετικέτα. Τα αποτελέσματα αποκαλύπτουν τα πλεονεκτήματα όσον αφορά την εξοικονόμηση ενέργειας της ισχύος του παρεμβολέα και την αυξημένη επιβαλλόμενη ζημιά στις κανονικές ετικέτες. Παράλληλα, απεικονίζονται τα οφέλη της υιοθέτησης πολιτικής τιμολόγησης βάσει χρήσης προκειμένου να προστατευθούν οι κανονικές παθητικές ετικέτες.

5.2 Σενάριο προσομοίωσης

Θεωρούμε λοιπόν ένα IoT σύστημα το οποίο αποτελείται από $|N|=256$ κανονικές παθητικές RFID ετικέτες, οι οποίες αντανακλούν τις πληροφορίες τους στον RFID αναγνώστη πάνω από |S|=256 ορθογώνια υποκανάλια, και μια ενεργή RFID ετικέτα/έξυπνο παρεμβολέα. Τα υποκανάλια κατανέμονται στις παθητικές ετικέτες με βάση την τεχνική μέγιστου κέρδους, αναθέτοντας δηλαδή το υποκανάλι στην ετικέτα η οποία χαρακτηρίζεται από το μέγιστο κέρδος καναλιού για το συγκεκριμένο υποκανάλι.

Η συνολική μέγιστη διαθέσιμη ισχύς μετάδοσης του παρεμβολέα σε όλα τα δυνατά υποκανάλια είναι $P_j^{Max} = 2W$ και η ισχύς θορύβου $I_0 = 5 \cdot 10^{-16}$. Επίσης μοντελοποιούμε τα κέρδη ισχύος καναλιού χρησιμοποιώντας το απλό μοντέλο απωλειών μονοπατιού

$g_{s,n/j} = \frac{K_{n/j}}{d_{n/j}^{a}}$, όπου $d_{n/j}$ είναι η απόσταση μεταξύ κανονικής ετικέτας/παρεμβολέα και αναγνώστη, a ο εκθέτης απωλειών απόστασης (στις προσομοιώσεις μας a=2) και $K_{n/j}$ μια λογαριθμοκανονικά κατανεμημένη(lognormal distributed) τυχαία μεταβλητή με μέση τιμή 2.7732 και διακύμανση 0.3139, η οποία αντιπροσωπεύει τις επιλεκτικής συχνότητας συνθήκες καναλιού. Τα κέρδη κεραίας του αναγνώστη και των παθητικών ετικετών είναι G_R =15.8489dbi και G_n =15.8489dbi αντίστοιχα. Επίσης το κέρδος οπισθοσκέδασης των κανονικών ετικετών έχει οριστεί ως K_n = 90%. Ο SINR στόχος των κανονικών ετικετών είναι γ_n^{target} =6db, λαμβάνοντας υπόψη απλή αναφορά ταυτότητας(ID) στον RFID αναγνώστη, π.χ. εφαρμογή εφοδιαστικής αλυσίδας. Το κόστος αντανάκλασης/μετάδοσης που έχει επιβληθεί στις κανονικές ετικέτες (c) και τον παρεμβολέα (c_j) αντίστοιχα, είναι $c = c_j$ =4000000 για την γραμμική τοπολογία, $c = c_j$ =1000000 για την τετραγωνική τοπολογία. Οι παραπάνω τιμές έχουν επιλεχθεί κατάλληλα, έτσι ώστε να είναι ρεαλιστικές, ενώ οι δύο όροι της συνάρτησης χρησιμότητας των κανονικών ετικετών και του παρεμβολέα είναι ίδιας τάξης μεγέθους.

Επιπλέον, όπως έχει προαναφερθεί, εξετάζουμε δύο τοπολογίες, την γραμμική και την ορθογωνική. Συγκεκριμένα, στην πρώτη υποθέτουμε ότι ο αναγνώστης βρίσκεται στην θέση (0,0) και οι κανονικές ετικέτες τοποθετούνται σε μία ευθεία που περνάει από το (0,0), διαδοχικά ο ένας μετά τον άλλον, με βήμα 0.1m, με την πρώτη κανονική ετικέτα να τοποθετείται σε απόσταση 1m από τον αναγνώστη. Όπως προκύπτει λοιπόν, η τελευταία ετικέτα τοποθετείται σε απόσταση 26,5 m από τον αναγνώστη. Ο παρεμβολέας από την άλλη, τοποθετείται στην μέση της διαμορφωμένης τοπολογίας, δηλαδή στα 13.75 m από τον αναγνώστη.

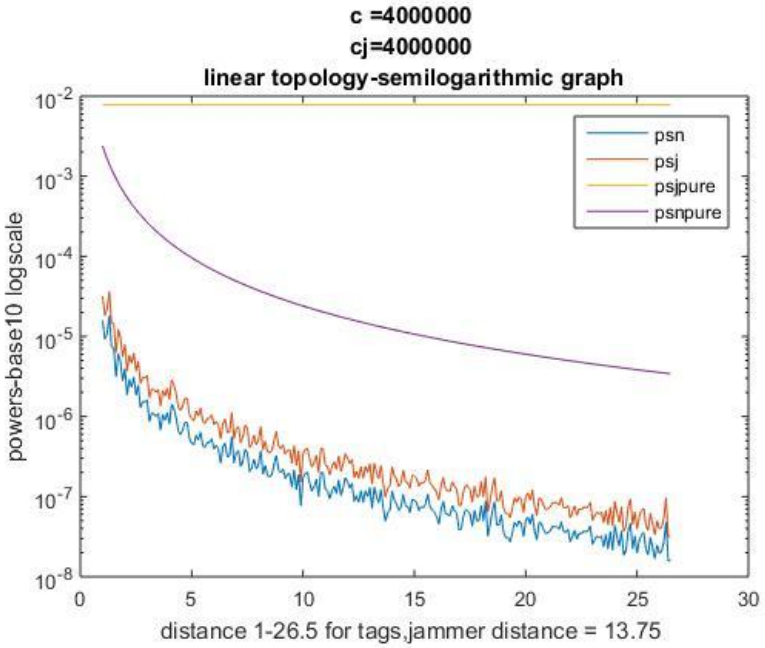
Στην τετραγωνική τοπολογία υποθέτουμε πάλι ότι ο αναγνώστης βρίσκεται στην θέση (0,0) αλλά οι κανονικές ετικέτες και ο παρεμβολέας τοποθετούνται τυχαία σε ένα τετράγωνο διαστάσεων 20x20m με κέντρο το (0,0). Οι θέσεις των προαναφερθέντων προκύπτουν από μια γεννήτρια τυχαίων αριθμών, η οποία παράγει τυχαίες συντεταγμένες στο εύρος από -10 έως 10 και για τους δύο άξονες. Κρατώντας στη συνέχεια την απόστασή τους βάσει συντεταγμένων από τον αναγνώστη, τους τοποθετούμε ξανά σε μια ευθεία ταξινομώντας τους κατά αύξουσα σειρά απόστασης από τον αναγνώστη, και μελετάμε σενάριο παρεμφερές με το πρώτο. Όπως θα φανεί και στη συνέχεια, τα συμπεράσματα που προκύπτουν από τα δύο σενάρια κινούνται προς την ίδια κατεύθυνση, συνεπώς η ανάλυση θα επικεντρωθεί στη μία από τις δύο τοπολογίες, την γραμμική.

5.3 Παρουσίαση αποτελεσμάτων και συγκριτική μελέτη

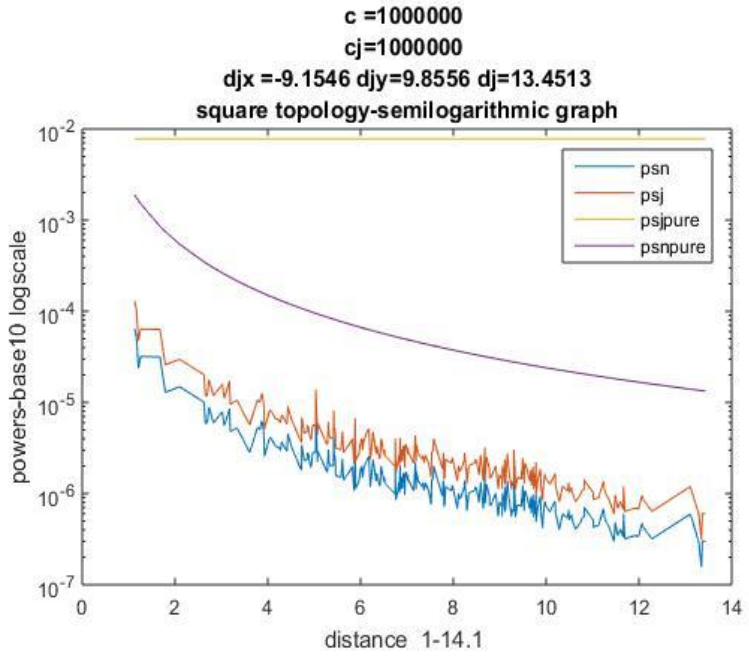
Αρχικά, όπως εξηγήθηκε πριν, ο πρώτος στόχος είναι να συζητήσουμε και να ποσοτικοποιήσουμε τα οφέλη από το προτεινόμενο πλαίσιο έξυπνης παρεμβολής, σε όρους αμοιβαίας αντιστάθμισης μεταξύ ισχύος αντανάκλασης και μετάδοσης σε κάθε κατειλημμένο κανάλι των κανονικών ετικετών και παρεμβολέα αντίστοιχα, καθώς και των αντίστοιχων τιμών χρησιμότητάς τους υπό διαφορετικές συνθήκες καναλιού επικοινωνίας. Υποθέτουμε ότι ο παρεμβολέας κατανέμει ισόποσα τη συνολική μέγιστη

διαθέσιμη ισχύ σε όλα τα υποκανάλια, δηλαδή $P_{s,j}^{Max} = P_j^{Max} / |S|$,επενδύοντας έτσι την ίδια προσπάθεια να επιτεθεί σε κάθε κανονική ετικέτα που επικοινωνεί με τον αναγνώστη μέσω του αντίστοιχου υποκαναλιού. Επιπλέον, μια λεπτομερής σύγκριση παρουσιάζεται ενάντια στο σενάριο όπου η τιμολόγηση βάσει χρήσης δεν λαμβάνεται υπόψη(No Usage based Pricing-NUP) για τις κανονικές ετικέτες και τον παρεμβολέα αντίστοιχα, όπως παρουσιάζεται στην ερευνητική μελέτη [70].

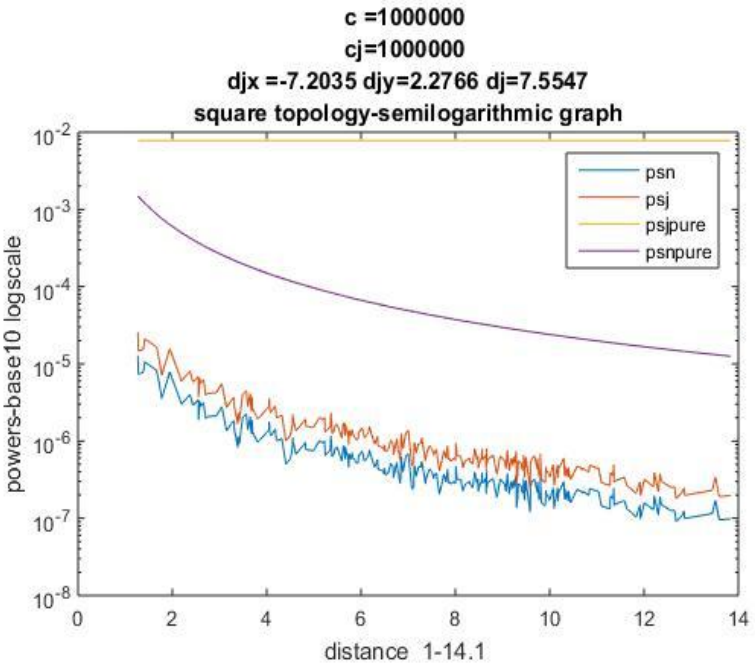
Η εικόνα 8 παρουσιάζει την ισχύ αντανάκλασης των κανονικών ετικετών και την ισχύ μετάδοσης του παρεμβολέα σε κάθε υποκανάλι συναρτήσει της απόστασης της παθητικής ετικέτας από τον αναγνώστη για τα ακόλουθα δύο σενάρια (α) IJC πλαίσιο και (β) NUP πλαίσιο [70], όπου ακολουθείται η ίδια ανάλυση που περιγράφηκε στην ενότητα 4.4, ωστόσο με τις συναρτήσεις χρησιμότητας κανονικών ετικετών/παρεμβολέα(δηλαδή, εξίσωση(4)/(5)) να μην περιλαμβάνουν την συνάρτηση κόστους. Psn/Psj και Psnpure/Psjpure είναι η ισχύς αντανάκλασης/μετάδοσης των παθητικών ετικετών/παρεμβολέα στα πλαίσια (α) και (β) αντίστοιχα.



(α)



(β)



(γ)

Σχήμα 8: Ισχύς αντανάκλασης και διάδοσης κανονικών ετικετών και παρεμβολέα συναρτήσει της απόστασης της κανονικής ετικέτας από τον RFID αναγνώστη για τα IJC και NUP πλαίσια α)γραμμική τοπολογία. β),γ)ορθογωνικές τοπολογίες

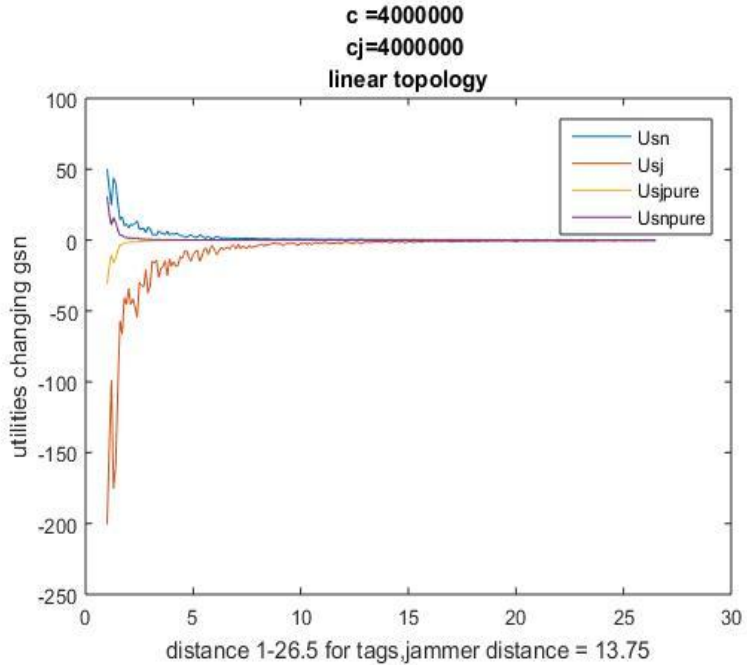
Τα αποτελέσματα λοιπόν αποκαλύπτουν ότι καθώς οι συνθήκες καναλιού των κανονικών παθητικών ετικετών επιδεινώνονται(δηλαδή, πιο απομακρυσμένες ετικέτες από τον αναγνώστη) η ισχύς αντανάκλασής τους μειώνεται. Η παραπάνω παρατήρηση βασίζεται στη σχέση (2), όπου φαίνεται ότι καθώς η απόσταση της κανονικής ετικέτας από τον αναγνώστη αυξάνεται, η μέγιστη διαθέσιμη ισχύς αντανάκλασής του μειώνεται,

και έτσι η βέλτιστη ισχύς αντανάκλασης της κανονικής ετικέτας όπως δίνεται από την εξίσωση(11) μειώνεται επίσης. Όσον αφορά το IJC πλαίσιο, λόγω της μείωσης της ισχύος αντανάκλασης καθώς οι συνθήκες του καναλιού χειροτερεύουν, η αντίστοιχη ισχύς μετάδοσης του παρεμβολέα επίσης μειώνεται, καθώς απαιτείται μικρότερη προσπάθεια προκειμένου ο τελευταίος να προκαλέσει την ίδια βλάβη στις κανονικές ετικέτες. Από την άλλη πλευρά, στο NUP πλαίσιο η βέλτιστη στρατηγική του έξυπνου παρεμβολέα είναι να μεταδώσει με τη μέγιστη ισχύ μετάδοσης ανά υποκανάλι(δηλαδή, $P_{s,j}^{Max} = {}^{P_j^{Max}}\!/_{|S|}$).

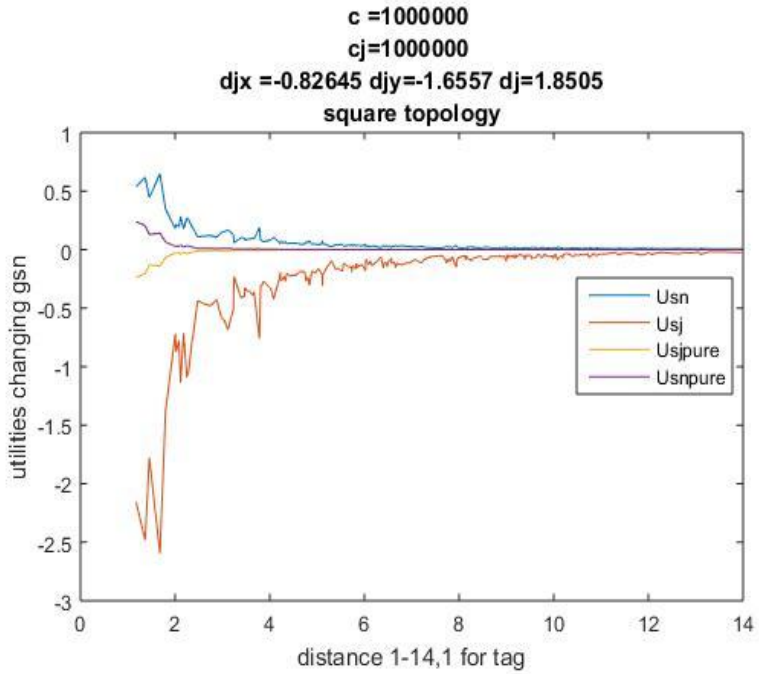
Επομένως η επιθετική συμπεριφορά του παρεμβολέα αναγκάζει τις κανονικές ετικέτες να αυξήσουν την ισχύ αντανάκλασης(συγκριτικά με το IJC πλαίσιο) προκειμένου να επιτύχουν το στοχευμένο SINR και να εκπληρώσουν μια επιτυχημένη επικοινωνία με τον αναγνώστη.

Στο σημείο αυτό τονίζεται ότι σύγκριση των σχημάτων 8(α) με 8(β),8(γ) αποκαλύπτει την ανεξαρτησία των συμπερασμάτων που προκύπτουν από την μορφή της τοπολογίας ενώ σύγκριση της 8(β) με 8(γ) την ανεξαρτησία των προαναφερθέντων από την θέση του παρεμβολέα στην τοπολογία(d_{jx},d_{jy} συντεταγμένες του παρεμβολέα, d_j απόσταση παρεμβολέα από αναγνώστη).

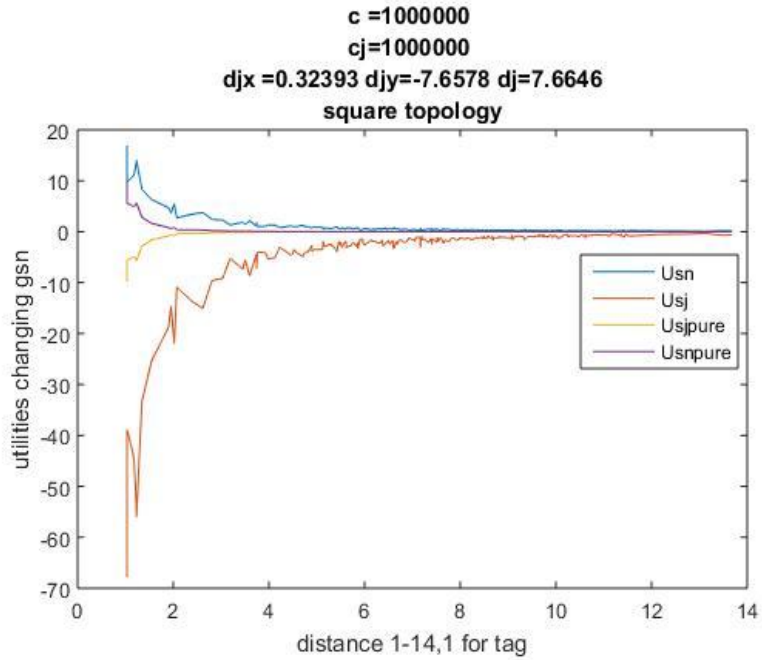
Το σχήμα 9 δείχνει τις τιμές της χρησιμότητας των παθητικών ετικετών και του παρεμβολέα συναρτήσει της απόστασης(έμμεσα του κέρδους καναλιού $g_{s,n}$ το οποίο εξαρτάται κυρίως από την απόσταση) της παθητικής ετικέτας από τον αναγνώστη, για τα IJC και NUP πλαίσια. Usn/Usj και Usnpure/Usjpure είναι η τιμή χρησιμότητας των παθητικών ετικετών/παρεμβολέα στα πλαίσια (α) και (β) αντίστοιχα.



(α)



(β)



(γ)

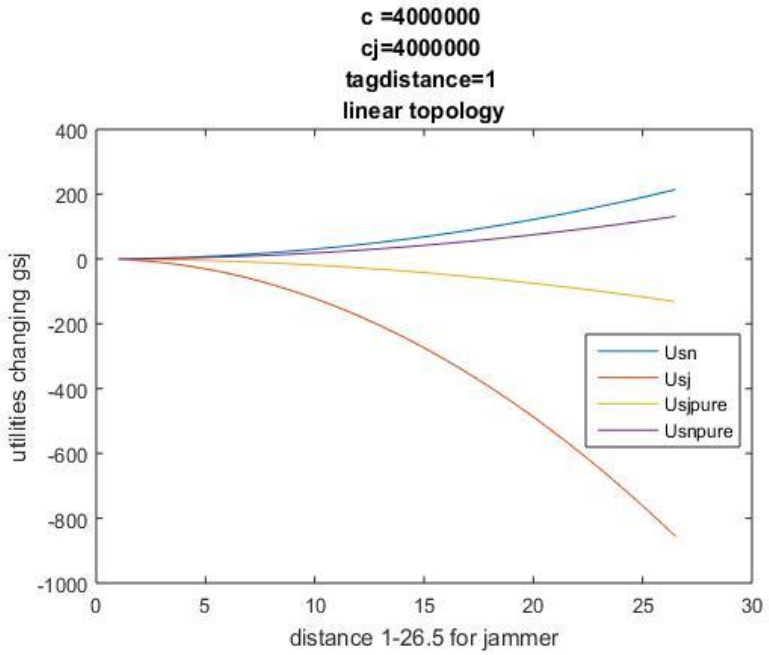
Σχήμα 9: Χρησιμότητες κανονικών ετικετών και παρεμβολέα συναρτήσει της απόστασης της κανονικής ετικέτας από τον RFID αναγνώστη για τα IJC και NUP πλαίσια α)γραμμική τοπολογία β),γ)ορθογωνικές τοπολογίες

Τα αποτελέσματα καταδεικνύουν σαφώς ότι, καθώς οι συνθήκες καναλιού των κανονικών ετικετών χειροτερεύουν(δηλαδή αυξάνεται η απόσταση της κανονικής ετικέτας από τον αναγνώστη), η αντιλαμβανόμενη χρησιμότητά τους μειώνεται, λόγω του γεγονότος ότι η διαθέσιμη ισχύς ανάκλασής τους μειώνεται(όπως παρατηρείται στη σχέση 2), επομένως αγωνίζονται να επιτύχουν το στοχευμένο SINR και γίνονται πιο

ευάλωτοι στην επίθεση του παρεμβολέα. Από την άλλη πλευρά, η χρησιμότητα του ευφυούς παρεμβολέα αυξάνεται καθώς οι συνθήκες των κανονικών ετικετών επιδεινώνονται, λόγω του ότι απαιτείται λιγότερη απαιτούμενη ισχύς μετάδοσης από την πλευρά του παρεμβολέα, προκειμένου να προκληθεί η ίδια ζημιά στις απομακρυσμένες κανονικές ετικέτες από τον αναγνώστη στο IJC πλαίσιο. Όσον αφορά το NUP πλαίσιο, ο παρεμβολέας προκαλεί μεγαλύτερη ζημιά στις κανονικές ετικέτες, συγκριτικά με το IJC σενάριο, ως εκ τούτου η επιτευχθείσα χρησιμότητά του είναι σχετικά μεγαλύτερη. Συνδυάζοντας τα παρατηρούμενα αποτελέσματα των σχημάτων 8(α) και 9(α), όσον αφορά τη σύγκριση των IJC και NUP πλαισίων, καταλήγουμε στο συμπέρασμα ότι η εξοικονόμηση ισχύος του έξυπνου παρεμβολέα στο IJC πλαίσιο είναι 99.98% κατά μέσο όρο συγκριτικά με το NUP πλαίσιο. Επιπλέον, το NUP πλαίσιο επιτυγχάνει 99.39% περισσότερη ζημιά στην κανονική ετικέτα σε σύγκριση με το IJC πλαίσιο.

Σύγκριση επίσης των σχημάτων 9(α) με 9(β),9(γ) αποκαλύπτει ξανά την ανεξαρτησία των συμπερασμάτων που προκύπτουν από την μορφή της τοπολογίας ενώ σύγκριση της 9(β) με 9(γ) την ανεξαρτησία των προαναφερθέντων από την θέση του παρεμβολέα στην τοπολογία(d_{jx},d_{jy} οι συντεταγμένες του παρεμβολέα, d_j η απόσταση παρεμβολέα από αναγνώστη).

Στη συνέχεια μελετάμε την συμπεριφορά μιας συγκεκριμένης κανονικής παθητικής RFID ετικέτας η οποία έχει τοποθετηθεί σε απόσταση d=1m από τον αναγνώστη. Το σχήμα 10 απεικονίζει τις τιμές χρησιμότητας της κανονικής ετικέτας και του παρεμβολέα ως συνάρτηση της απόστασης(έμμεσα του κέρδους καναλιού $g_{s,j}$ το οποίο εξαρτάται κυρίως από την απόσταση) του δεύτερου από τον αναγνώστη, για τα IJC και NUP πλαίσια στη γραμμική τοπολογία(δεν παραθέτουμε τετραγωνική τοπολογία αφού δουλεύουμε αποκλειστικά με σταθερό βήμα 0.1m για τις διάφορες θέσεις του παρεμβολέα στην συγκεκριμένη περίπτωση).



Σχήμα 10: Χρησιμότητες κανονικής ετικέτας και παρεμβολέα ως συνάρτηση της απόστασης του παρεμβολέα από τον RFID αναγνώστη για τα IJC και NUP πλαίσια

Το σχήμα 10 απεικονίζει τις τιμές χρησιμότητας της κανονικής ετικέτας και του παρεμβολέα συναρτήσει της απόστασης του παρεμβολέα από τον αναγνώστη, τόσο για το IJC όσο και για το NUP πλαίσιο. Παρατηρείται λοιπόν ότι η χρησιμότητα της κανονικής ετικέτας βελτιώνεται καθώς η απόσταση του παρεμβολέα αυξάνεται, λόγω του γεγονότος ότι ο τελευταίος δεν είναι σε θέση να επιβάλει την ίδια βλάβη στην κανονική ετικέτα εξαιτίας των επιδεινούμενων συνθηκών του καναλιού και στα δύο πλαίσια. Επίσης στο IJC πλαίσιο, η χρησιμότητα του παρεμβολέα μειώνεται καθώς οι συνθήκες του καναλιού χειροτερεύουν εξαιτίας του γεγονότος ότι ο παρεμβολέας θα πρέπει να δαπανήσει αυξημένη ισχύ μετάδοσης προκειμένου να επιτεθεί στην κανονική ετικέτα. Επιπλέον, παρατηρείται ότι ο παρεμβολέας επιτυγχάνει σχετικά μεγαλύτερη χρησιμότητα στο NUP πλαίσιο συγκριτικά με το IJC(ακόμα και για τις συνθήκες καναλιού του παρεμβολέα που έχουν επιδεινωθεί) κατά 84,63% κατά μέσο όρο. Από την άλλη, οι κανονικές ετικέτες υποφέρουν κατά 38.53% κατά μέσο όρο από την επιδείνωση της χρησιμότητας στο πλαίσιο NUP σε σύγκριση με το IJC, λόγω της πιο επιθετικής συμπεριφοράς του παρεμβολέα μέσω της αυξημένης ισχύος μετάδοσης.

Στη συνέχεια, αντί απλώς ο παρεμβολέας να διανέμει ισόποσα την μέγιστη διαθέσιμη ισχύ σε όλα τα υποκανάλια που μπορεί να καταλάβει, ένα προχωρημένο σενάριο ελέγχου έξυπνης παρεμβολής μελετάται, στα πλαίσια της οποίας επιτρέπεται στον παρεμβολέα να επενδύει με σύνεση την μέγιστη διαθέσιμη ισχύ του σε όλα τα υποκανάλια μέσω της ανίχνευσης της ποιότητας του κέρδους καναλιού της κανονικής ετικέτας. Συγκεκριμένα, ο παρεμβολέας είναι πρόθυμος να επενδύσει αυξημένη μέγιστη διαθέσιμη ισχύ σε εκείνα τα υποκανάλια όπου οι κανονικές ετικέτες έχουν καλές συνθήκες καναλιού, καθώς σε αυτήν την περίπτωση η πρόκληση ζημιάς στις κανονικές ετικέτες θα είναι πιο δύσκολη

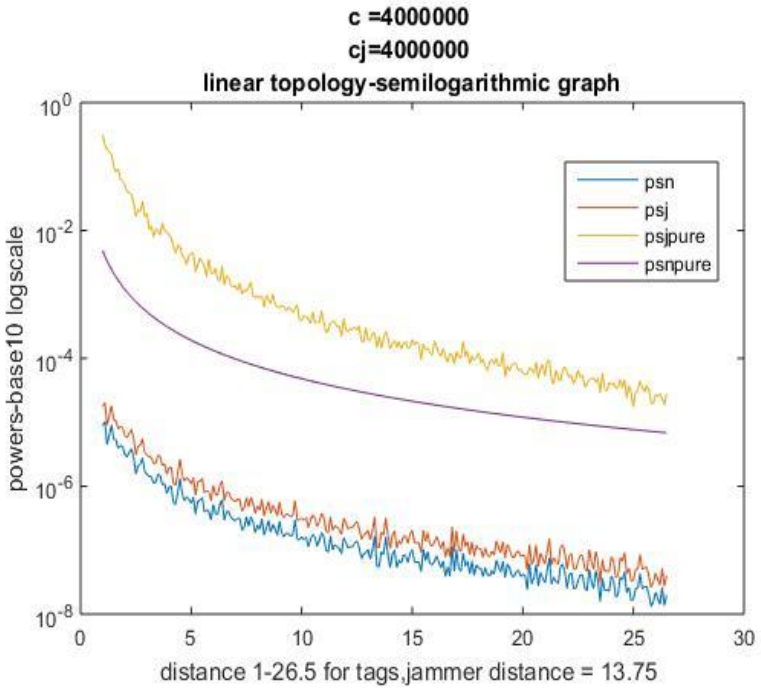
από την άποψη της αυξημένης δαπανημένης ισχύος μετάδοσης. Από την άλλη πλευρά, στα υποκανάλια όπου οι συνθήκες καναλιού των κανονικών ετικετών επιδεινώνονται, ο έξυπνος παρεμβολέας χρειάζεται μικρότερη προσπάθεια για να προκαλέσει ζημιά, μειώνοντας έτσι τη μέγιστη διαθέσιμη ισχύ μετάδοσης που χρειάζεται ανά υποκανάλι.

Με βάση την παραπάνω συζήτηση, στο AIJC σενάριο, η μέγιστη διαθέσιμη ισχύς μετάδοσης του παρεμβολέα σε κάθε υποκανάλι προκύπτει εξής :

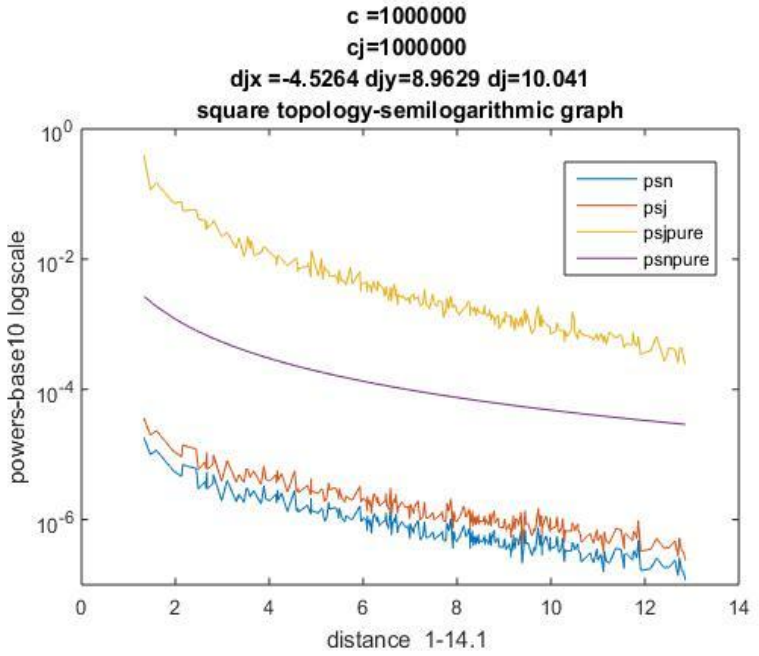
$$P_{s,j}^{Max} = \frac{g_{s,n}}{\sum_{n=1}^{|N|} g_{s,n}^{x}} P_j^{Max} \qquad (13)$$

όπου $x \in \square^{+}$ και αντιπροσωπεύει πόση επίδραση έχει η ποιότητα του κέρδους καναλιού των κανονικών ετικετών στην απόφαση του ευφυούς παρεμβολέα να επενδύσει ένα ποσό της μέγιστης διαθέσιμης ισχύος μετάδοσης σε κάθε υποκανάλι. Στα παρακάτω αποτελέσματα, θεωρήσαμε την περίπτωση x=1.5. Επίσης παρέχουμε μια συγκριτική ανάλυση μεταξύ AIJC και NUP πλαισίου, ενώ το δεύτερο υιοθετεί την εξίσωση (13), προκειμένου να προσδιορίσουμε τη μέγιστη διαθέσιμη ισχύ μετάδοσης του παρεμβολέα σε κάθε υποκανάλι.

Τα σχήματα 11 και 12 παρουσιάζουν την ισχύ ανάκλασης/μετάδοσης και τις τιμές χρησιμότητας των κανονικών ετικετών και του παρεμβολέα σε κάθε υποκανάλι, αντίστοιχα, ως συνάρτηση της απόστασης της κανονικής ετικέτας από τον αναγνώστη τόσο για AIJC όσο και για το NUP πλαίσιο στη γραμμική και την ορθογωνική τοπολογία.

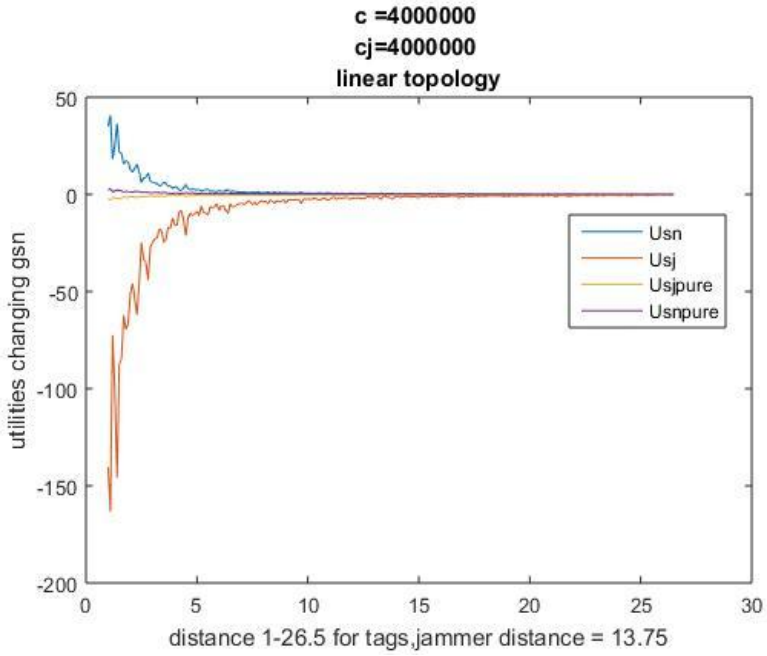


(α)

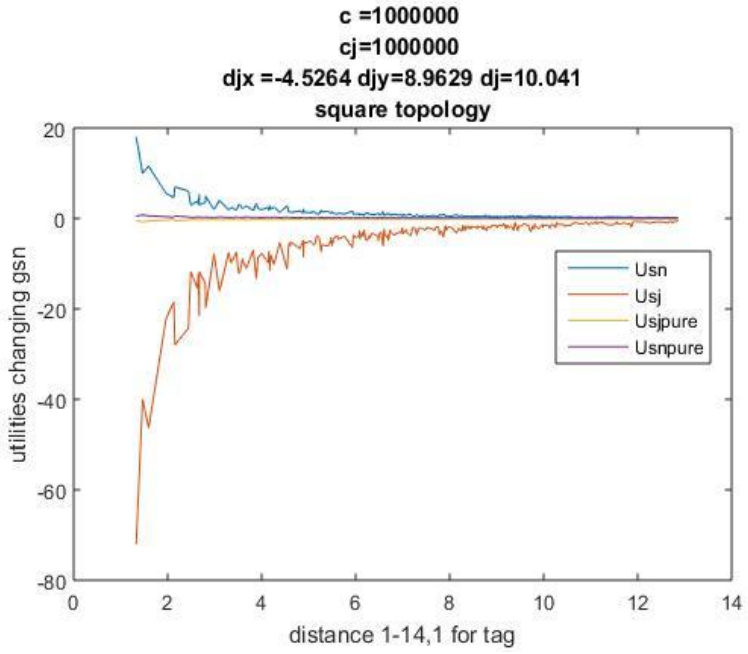


(β)

Σχήμα 11: Ισχύς ανάκλασης και μετάδοσης των κανονικών ετικετών και του παρεμβολέα συναρτήσει της απόστασης της κανονικής ετικέτας από τον αναγνώστη για τα AIJC και NUP(προχωρημένο) πλαίσια α)γραμμική τοπολογία β)τετραγωνική τοπολογία



(α)



(β)

Σχήμα 12:Χρησιμότητες των κανονικών ετικετών και του παρεμβολέα συναρτήσει της απόστασης της κανονικής ετικέτας από τον αναγνώστη για τα AIJC και NUP(προχωρημένο) πλαίσια α)γραμμική τοπολογία. β)τετραγωνική τοπολογία

Τα αποτελέσματα αποκαλύπτουν ότι ο έξυπνος παρεμβολέας, στο NUP πλαίσιο με εφαρμογή της εξίσωσης (13), είναι σε θέση να προσαρμόζει με σοφό τρόπο την μέγιστη επενδυμένη ισχύ μετάδοσης ανά υποκανάλι(σχήμα 11(α)), δηλαδή επενδύοντας αυξημένη μέγιστη διαθέσιμη ισχύ στα υποκανάλια όπου οι συνθήκες καναλιού των κανονικών ετικετών είναι καλές δηλαδή, σε κοντινή απόσταση από τον RFID αναγνώστη). Με βάση την προχωρημένη έξυπνη επένδυση ενέργειας από πλευράς παρεμβολέα, η επιβαλλόμενη ζημιά στις κανονικές ετικέτες αυξάνεται στο NUP πλαίσιο, δηλαδή οι τιμές χρησιμότητας του παρεμβολέα σε κάθε υποκανάλι αυξάνονται κατά μέσο όρο κατά 8000.4249% ενώ των κανονικών ετικετών μειώνονται(σχήμα 12(α)) κατά μέσο όρο κατά 8000.4249% σε σύγκριση με τα αντίστοιχα αποτελέσματα που παρουσιάζονται στο σχήμα 9(α) για το αρχικό NUP πλαίσιο.

Από την άλλη πλευρά, το AIJC πλαίσιο παρουσιάζει μικρές αλλαγές όσον αφορά τη βέλτιστη ισχύ μετάδοσης του παρεμβολέα και των κανονικών ετικετών σε κάθε υποκανάλι(σχήμα 11(α)) συγκριτικά με το IJC πλαίσιο(σχήμα 8(α)). Η παρατήρηση αυτή οφείλεται στο γεγονός ότι οι τιμές ισχύος μετάδοσης ήταν ήδη χαμηλά, συνεπώς ο $\min\{\cdot\}$ τελεστής στις εξισώσεις (11) και (12) δεν επηρεάζεται σημαντικά από την αλλαγή της μέγιστης διαθέσιμης επενδυμένης ισχύος μετάδοσης του παρεμβολέα ακολουθώντας την εξίσωση (13). Κατά συνέπεια, οι επιτευχθείσες τιμές χρησιμότητας του έξυπνου παρεμβολέα και της κανονικής ετικέτας ανά υποκανάλι δεν επηρεάζονται σημαντικά στο AIJC πλαίσιο(σχήμα 12(α)) σε σύγκριση με το πλαίσιο IJC. Η παρατήρηση αυτή έχει μεγάλη σημασία. Επισημαίνεται ότι ακόμα και αν ο παρεμβολέας γίνει ακόμα πιο έξυπνος επενδύοντας με σύνεση την μέγιστη διαθέσιμη ισχύ μετάδοσης ανά κανάλι, το AIJC πλαίσιο είναι αρκετό ισχυρό ενάντια στην επίθεση παρεμβολής, προστατεύοντας

έτσι τις κανονικές ετικέτες και μετριάζοντας την επιθετική συμπεριφορά του παρεμβολέα μέσω υιοθέτησης μηχανισμού τιμολόγησης βάσει χρήσης. Συνεπώς, παρατηρείται ότι στο πλαίσιο AIJC οι τιμές χρησιμότητας(σχήμα 12(α)) παραμένουν σχεδόν οι ίδιες σε σύγκριση με τις αντίστοιχες του IJC πλαισίου(σχήμα 9(α)). Αντίθετα, το προχωρημένο έξυπνο NUP πλαίσιο(σχήμα 12(α)) επιδεινώνει δραματικά τις τιμές χρησιμότητας των κανονικών ετικετών συγκριτικά με τις αντίστοιχες τιμές στο αρχικό NUP πλαίσιο(σχήμα 9(α)) κατά 8000.4249% κατά μέσο όρο.

ΚΕΦΑΛΑΙΟ 6

ΕΠΙΛΟΓΟΣ

6.1Συμπεράσματα

6.2 Μελλοντική εργασία

6.1 Συμπεράσματα

Σε αυτή την διπλωματική εργασία μελετήθηκε το πρόβλημα ελέγχου της έξυπνης παρεμβολής(IJC) στο Διαδίκτυο των Αντικειμένων, με έμφαση στα παθητικά RFID δίκτυα. Ο έξυπνος παρεμβολέας έλεγχε και προσάρμοζε την ισχύ μετάδοσής του προκειμένου να διακόψει την ομαλή επικοινωνία των κανονικών παθητικών RFID ετικετών με τον RFID αναγνώστη. Πριν την διαμόρφωση του προβλήματος ελέγχου έξυπνων παρεμβολών, δύο γενικές συναρτήσεις χρησιμότητας ανατέθηκαν στον έξυπνο παρεμβολέα και την κανονική ετικέτα, οι οποίες διαφοροποιήθηκαν με βάση τον στόχο της κάθε οντότητας, δηλαδή, την πρόκληση ζημιάς στην επικοινωνία των κανονικών ετικετών και την επίτευξη της στοχευμένης SINR τιμής προκειμένου να πραγματοποιηθεί ομαλή επικοινωνία με τον RFID αναγνώστη, αντίστοιχα.

Το IJC πρόβλημα διατυπώθηκε ως ένα Stackelberg παίγνιο για κάθε υποκανάλι, όπου η κανονική ετικέτα ενεργούσε ως ο ηγέτης και ο ευφυής παρεμβολέας σαν ακόλουθος. Κάθε οντότητα, δηλαδή τόσο η κανονική ετικέτα όσο και ο εισβολέας, στόχευε στη μεγιστοποίηση της χρησιμότητά του μέσω ελέγχου της ισχύος αντανάκλασης ή μετάδοσης, αντίστοιχα. Το IJC παίγνιο λύθηκε και η μοναδική Stackelberg ισορροπία προσδιορίστηκε μέσω κλειστής μορφής λύσης. Η βέλτιστη ισχύς αντανάκλασης των κανονικών ετικετών και μετάδοσης του έξυπνου παρεμβολέα ανά υποκανάλι προσδιορίστηκαν στο σημείο Stackelberg ισορροπίας. Η επίδοση του IJC πλαισίου εξετάστηκε σε βάθος μέσω μιας σειράς Monte Carlo προσομοιώσεων ανάλυσης και συγκρίθηκε με αυτή του πλαισίου χωρίς μηχανισμό τιμολόγησης βάσει χρήσης(NUP), όπου το κόστος ανάκλασης/μετάδοσης δεν λήφθηκε υπόψη.

Τα αποτελέσματα έδειξαν ότι με την παροχή προηγμένης νοημοσύνης στον παρεμβολέα, ο τελευταίος γίνεται πιο επιθετικός, όσον αφορά την παρέμβαση που πραγματοποιεί στην επικοινωνία της κανονικής ετικέτας με τον RFID αναγνώστη, προκαλώντας αυξημένη ζημιά. Μια εξαιρετικά ενδιαφέρουσα παρατήρηση είναι ότι ο μηχανισμός τιμολόγησης βάσει χρήσης, σχετικά με την ισχύ ανάκλασης των κανονικών παθητικών RFID ετικετών και την ισχύ μετάδοσης του έξυπνου παρεμβολέα, μπορεί σιωπηρά να λειτουργήσει ως προστατευτικό όχημα των κανονικών ετικετών, περιορίζοντας την επίδραση της επιθετικής συμπεριφοράς του έξυπνου παρεμβολέα και κατά συνέπεια καθιστώντας το IoT σύστημα, που βασίζεται στην RFID τεχνολογία, πιο ισχυρό σε πιθανή προκληθείσα ζημιά από τους ευφυείς παρεμβολείς.

6.2 Μελλοντική εργασία

Μέρος της τρέχουσας και μελλοντικής εργασίας μας είναι η επέκταση του προτεινόμενου IJC πλαισίου προκειμένου να ληφθεί υπόψη ένα πολύ-βηματικό(multi-hop) παθητικό RFID δίκτυο, επικοινωνίας ετικέτας με ετικέτα, όπου οι περιορισμοί της μέγιστης ισχύος αντανάκλασης των κανονικών ετικετών, τις καθιστούν πιο ευάλωτες στις έξυπνες επιθέσεις των παρεμβολέων. Επιπλέον, το πρόβλημα μιας ομάδας εισβολέων, που τοποθετούνται στρατηγικά και ενεργούν έτσι ώστε να προκληθεί η μέγιστη δυνατή ζημιά στο δίκτυο, θα μπορούσε να μελετηθεί μέσω επέκτασης και προσαρμογής του προτεινόμενου πλαισίου. Τέλος, το πρόβλημα της διάκρισης της επίθεσης ενός έξυπνου

παρεμβολέα από ένα λάθος επικοινωνίας σε ένα παθητικό RFID δίκτυο χρήζει μεγάλης σημασίας, προκειμένου να σχεδιαστούν οι αντίστοιχοι μηχανισμοί ελέγχου που θα ανιχνεύουν και θα μετριάζουν την προκαλούμενη βλάβη, όποτε αυτή συμβαίνει.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] K. Rose, S. Eldridge and L. Chapin, "The Internet of Things: An Overview; Understanding the Issues and Challenges of a More Connected World," White Paper, The Internet Society (ISOC), Virginia, USA, October 2015.

[2] Cloud and Mobile Network Traffic Forecast - Visual Networking Index (VNI)." *Cisco*, 2015. http://cisco.com/c/en/us/solutions/serviceprovider/ visual-networking-index-vni/index.html

[3] Danova, Tony. "Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020." *Business Insider*, October 2, 2013. http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10

[4] Global Connectivity Index." Huawei Technologies Co., Ltd., 2015. Web. 6 Sept. 2015. http://www.huawei.com/minisite/gci/en/index.html

[5] Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute, June 2015.

[6] Thierer, Adam, and Andrea Castillo. "Projecting the Growth and Economic Impact of The Internet of Things." George Mason University, Mercatus Center, June 15, 2015. http://mercatus.org/sites/default/files/IoT-EP-v3.pdf

[7] Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway—With Me in It." *WIRED*, July 21, 2015.http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[8] Samsung Smart TV's Voice Recognition Creates Privacy Concerns." *CBS This Morning*. CBS News, February 10, 2015. http://www.cbsnews.com/videos/samsung-smart-tvs-voice-recognition-creates-privacy-concerns/

[9] Bradbury, Danny. "How Can Privacy Survive in the Era of the Internet of Things?" *The Guardian*, April 7, 2015, sec. Technology.http://www.theguardian.com/technology/2015/apr/07/how-can-privacy-survive-the-internet-of-things

[10] E.E. Tsiropoulou, P. Vamvakas, and S. Papavassiliou, "Joint Utility-based Uplink Power and Rate Allocation in Wireless Networks: A Non-cooperative Game Theoretic Framework," Elsevier Physical Communications Journal, vol. 9, pp. 299-307, 2012.

[11] E. E. Tsiropoulou, P. Vamvakas, S. Papavassiliou,"Joint Customized Price and Power Control for Energy-Efficient Multi-Service Wireless Networks via S-Modular Theory," in IEEE Transactions on Green Communications and Networking, vol. 1, no. 1, pp. 17-28, 2017.

[12] T. Kastrinogiannis, E. E. Tsiropoulou, and S. Papavassiliou, "Utility-Based Uplink Power Control in CDMA Wireless Networks with Real-Time Services," in Ad-hoc, Mobile and Wireless Networks (LNCS) Sprigner, vol. 5198, p.p. 307-320, September, 2008.

[13] E. E. Tsiropoulou, T. Kastrinogiannis, and S. Papavassiliou, "QoS-Driven Uplink Power Control in Multi- Service CDMA Wireless Networks - A Game Theoretic Framework," Journal of Communications, Academy Publisher, vol. 4, No 9, pp. 654-668, Oct. 2009.

[14] E.E. Tsiropoulou, T. Kastrinogiannis, and S. Papavassiliou, "A Utility-based Power Allocation Non-cooperative Game for the Uplink in Multi-Service CDMA Wireless Networks," Proc. of IEEE International Wireless Communications and Mobile Computing Conference, pp. 365-370, Leipzig, Germany, June, 2009.

[15] E. E. Tsiropoulou, T. Kastrinogiannis, and S. Papavassiliou, "Realization of QoS Provisioning in Autonomic CDMA Networks under Common Utility-Based Framework," in Proc. of IEEE WoWMoM workshop on Autonomic and Opportunistic Communications (AOC), June, 2009.

[16] E.E. Tsiropoulou, G. Katsinis, and S. Papavassiliou, "Utility-based Power Control via Convex Pricing for the Uplink in CDMA Wireless Networks," European Wireless 2010, pp. 200-206, April, 2010.

[17] E. E. Tsiropoulou, G. Katsinis and S. Papavassiliou, "Distributed Uplink Power Control in Multi-ServiceWireless Networks via a Game Theoretic Approach with Convex Pricing ," in IEEE Transactions on Parallel and Distributed Systems, Vol. 23, Issue 1, pp. 61-68, 2012.

[18] E.E. Tsiropoulou, P. Vamvakas, and S. Papavassiliou, "Energy Efficient Uplink Joint Resource Allocation Noncooperative Game with Pricing," in Proc. of IEEE Wireless Communications and Networking Conference (WCNC 2012), pp. 2352-2356,April, 2012.

[19] E. E. Tsiropoulou and S. Papavassiliou, "Utility-based Uplink Joint Power & Subcarrier Allocation in SCFDMA Wireless Networks," in International Journal of Electronics, Taylor & Francis, Vol. 98, Issue 11, pp. 1581-1587, 2011.

[20] E. E. Tsiropoulou, A. Kapoukakis and S. Papavassiliou, "Energy-efficient Subcarrier Allocation in SC-FDMA Wireless Networks based on Multilateral Model of Bargaining," IFIP Networking 2013,pp. 1-9, Brooklyn, 2013.

[21] E.E. Tsiropoulou, I. Ziras and S. Papavassiliou, "Service Differentiation and Resource Allocation in SC-FDMA Wireless Networks through User-Centric Distributed Non-Cooperative Multilateral Bargaining," in 7th International Conference on Ad Hoc Networks (LNCS) Sprigner, pp. 42-54, September, 2015.

[22] E. E. Tsiropoulou, I. Ziras, S. Papavassiliou, "A Non-Cooperative Approach to the Joint Subcarrierand Power Allocation Problem in Multi-Service SCFDMA Networks," EAI Endorsed Transactions on Mobile Communications and Applications, 2015.

[23] E. E. Tsiropoulou, A. Kapoukakis, S. Papavassiliou, "Uplink Resource Allocation in SC-FDMA Wireless Networks: A Survey and Taxonomy," Computer Networks, Elsevier, vol. 96, pp. 1-28, 2016.

[24] E.E. Tsiropoulou, I. Gialagkolidis, P. Vamvakas, and S. Papavassiliou, "Resource Allocation in Visible Light Communication Networks: NOMA vs OFDMA Transmission Techniques," in International Conference on Ad Hoc Networks (LNCS) Sprigner, pp. 32-46, July, 2016.

[25] P. Vamvakas, E.E. Tsiropoulou, S. Papavassiliou, J. Baras, "Optimization and Resource Management in NOMA Wireless Networks Supporting Real and Non-real Time Service Bundling," 22nd IEEE Symposium on Computers and Communications (ISCC),pp. 697-703, July, 2017.

[26] E.E. Tsiropoulou, G. Katsinis, P. Vamvakas, and S. Papavassiliou, "Efficient Uplink Power Control in Multi- Service Two-Tier Femtocell Networks via a Game Theoretic Approach," IEEE International Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks (CAMAD), pp. 104-108, Berlin, 2013.

[27] E. E. Tsiropoulou, P. Vamvakas, G. Katsinis, S. Papavassiliou, "Combined Power and Rate Allocation in Self- Optimized Multi-Service Two-Tier Femtocell Networks," Computer Communications, Elsevier, vol. 72, pp. 38-48, 2015.

[28] E.E. Tsiropoulou, G. Katsinis, A. Filios, and S. Papavassiliou, "On the Problem of Optimal Cell Selection & Uplink Power Control in Open Access Multi-Service Two-Tier Femtocell Networks," in Ad-hoc, Mobile and Wireless Networks (LNCS) Sprigner, pp. 114-127, June, 2014.

[29] E. E. Tsiropoulou, P. Vamvakas, S. Papavassiliou,"Supermodular Game-based Distributed Joint Uplink Power & Rate Allocation in Two-Tier SC-FDMA Femtocell Networks," in IEEE Transactions on Mobile Computing, 2016. doi: 10.1109/TMC.2016.2622263

[30] G. Katsinis, E.E. Tsiropoulou and S. Papavassiliou, "A Game Theoretic Approach to the Power Control in D2D Communications Underlay Cellular Networks," IEEE International Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks (CAMAD),pp. 208-212, Athens, Greece, 2014.

[31] G. Katsinis, E. E. Tsiropoulou, S. Papavassiliou, " Joint Resource Block and Power Allocation for Interference Management in Device to Device Underlay Cellular Networks: A Game Theoretic Approach," in Mobile Networks and Applications, Springer, pp. 1-13, 2016.

[32] E.E. Tsiropoulou, S.T. Paruchuri, J. Baras, "Interest, Energy and Physical-Aware Coalition Formation and Resource Allocation in Smart IoT Applications," 51st Annual Conference on Information Sciences and Systems (CISS), pp. 1-6, March, 2017.

[33] G. Katsinis, E.E. Tsiropoulou, and S. Papavassiliou, "On the Problem of Resource Allocation and System Capacity Evaluation via a Blocking Queuing Model in D2D enabled Overlay Cellular Networks," in Ad-hoc, Mobile and Wireless Networks (LNCS) Sprigner, pp. 76-89, June, 2015.

[34] E.E. Tsiropoulou, J. Baras, S. Papavassiliou, G. Qu, " On the Mitigation of Interference Imposed by Intruders in Passive RFID Networks," Conference on Decision and Game Theory for Security (GameSec), pp. 62-80, Nov., 2016.

[35] P. Vamvakas, E.E. Tsiropoulou, M. Vomvas, S. Papavassiliou "Adaptive Power Management in Wireless Powered Communication Networks: A User-Centric Approach," IEEE 38th Sarnoff Symposium, Sept., 2017. (to appear)

[36] G. Katsinis, E. E. Tsiropoulou, S. Papavassiliou, "Multicell Interference Management in Device to Device Underlay Cellular Networks," Future Internet, MDPI, vol. 9, no. 3, pp. 1-20, 2017.

[37] E.E. Tsiropoulou, J. Baras, S. Papavassiliou, S. Sinha, "RFID-based Smart Parking Management System," Cyber-Physical Systems, Taylor & Francis, pp. 1-20, 2017 (doi: 10.1080/23335777.2017.1358765).

[38] P. Vamvakas, E. E. Tsiropoulou, S. Papavassiliou, "Dynamic Provider Selection & Power Resource Management in Competitive Wireless Communication Markets," in Mobile Networks and Applications, Springer, pp.1-14, 2017. DOI: 10.1007/s11036-017-0885-y.

[39] E. E. Tsiropoulou, G. Mitsis, S. Papavassiliou, "Interest-aware Energy Collection & Resource Management in Machine to Machine Communications," in Elsevier, Ad Hoc Networks, 2017. ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2017.09.003

[40] E.E. Tsiropoulou, T. Kastrinogiannis and S. Papavassiliou, "Non-cooperative Power Control in CDMAWireless Networks," in "Game Theory for Wireless Communications and Networking" book, Auerbach Publications, CRC Press, Taylor & Francis Group, 2010.

[41] E. E. Tsiropoulou, P. Vamvakas, S. Papavassiliou, "Resource Allocation in Multi-tier Femtocell and Visible- Light Heterogeneous Wireless Networks, " Book Chapter in "Resource Allocation in Next-Generation Broadband Wireless Access Networks" Book, Editors: Chetna Singhal and Swades De, 2016.

[42] Y. E. Sagduyu, R. A. Berry and A. Ephremides, “Jamming games in wireles networks with incomplete information,” in IEEE Communications Magazine, vol. 49, no. 8, pp. 112-118, August 2011.

[43] Y. E. Sagduyu, R. Berry, and A. Ephremides, “MAC Games forDistributed Wireless Network Security with Incomplete Information of Selfish and Malicious User Types,” Proc. Int’l. Conf. Game Theory for Networks,Istanbul, Turkey, May 2009.

[44] E. Altman, K. Avratchenkov, and A. Garnaev, “Jamming Game with Incomplete Information about the Jammer,” Proc. 4th Int’l. ICST Conf. Performance EvaluationMethodologies and Tools (VALUETOOLS), Pisa, Italy, Oct. 2009.

[45] Y. E. Sagduyu, R. Berry and A. Ephremides, “Wireless Jamming Attacks under Dynamic Traffic Uncertainty,” Proc.Int’l. Symp. Modeling and Optimization in Mobile, Ad Hoc,and Wireless Networks, Avignon, France, June 2010.

[46] H. Inaltekin and S. B. Wicker, “Random Access Games:Selfish Nodes with Incomplete Information,” Proc. IEEE MILCOM, Orlando, FL, Oct. 2007.

[47] H. Inaltekin and S. B. Wicker, “Random Access Gameover Noisy Channels with Capture Effect,” Proc. ACM Int’l. Symp. Modeling, Analysis and Simulation of Wirelessand Mobile Sys., Chania, Crete, Greece, Oct. 2007.

[48] Jamming games for power controlled medium access with dynamic traffic," IEEE International Symposium on Information Theory, pp. 1818-1822, Austin, TX, 2010.

[49] L. Xiao, Q. Li, T. Chen, E. Cheng and H. Dai, "Jamming Games in Underwater Sensor Networks with Reinforcement Learning," IEEE Global Communications Conference (GLOBECOM), pp. 1-6, San Diego, CA, 2015

[50] J. S. Shamma and G. Arslan, "Dynamic Fictitious Play,Dynamic Gradient Play, and Distributed Convergence toNash Equilibria," IEEE Trans. Automatic Control, vol. 50,no. 3, Mar. 2005, pp. 312–27.

[51] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," IEEE Journal on Selected Areas in Communications, vol. 30, no. 1, pp. 4–15, January 2012.

[52] R. El-Bardan, S. Brahma, and P. K. Varshney, "Power control with jammer location uncertainty: A game theoretic perspective," in in Proc. of 48th Annual Conference on Information Sciences and Systems (CISS), pp. 1–6, 2014

[53] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, Part I: Known channel statistics," IEEE Trans. Wireless Commun., vol. 9, no. 11, pp. 3566– 3577, Nov. 2010.

[54] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, Part II: Unknown channel statistics," IEEE Trans. Wireless Commun., vol. 10, no. 1, pp. 274–283, Jan. 2011.

[55] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: threats and mitigation," in Proc. International Conference on CognitiveRadio Oriented Wireless Networks and Communications (CrownCom), Singapore, May 2008.

[56] Singhal, C. and De, S. (2017). Resource allocation in next-generation broadband wireless access networks. Hershey, PA: Information Science Reference

[57] K. Zhao and L. Ge, "A survey on the internet of things security," in Proc. of 9th International Conference on Computational Intelligence and Security (CIS). IEEE, pp. 663–667, 2013.

[58] A. Sehgal, V. Perelman, S. Kuryla, and J. Schonwalder, "Management of resource constrained devices in the internet of things," IEEE Communications Magazine, vol. 50, no. 12, pp. 144–149, December 2012.

[59] Hongbo Zhou. Web 4.0: Chinese definition of the Internet of things. Z/OL. China Information World. (37) (2010) (in Chinese)

[60] Geng Yang, Jian Xu, etc.: Security Characteristic and Technology in the Internet of Things. J. Journal of Nanjing University of Posts and Telecommunications (Natural Science). 30(4) (2010) (in Chinese

[61] J. Liu and W. Sun, "Smart Attacks against Intelligent Wearables in People-Centric Internet of Things," in IEEE Communications Magazine, vol. 54, no. 12, Dec. 2016, pp. 44-49.

[62] P. Sarigiannidis; E. Karapistoli; A. Economides, “Modelling the Internet of Things Under Attack: A G-network Approach,” in IEEE Internet of Things Journal , vol.PP, no.99, pp.1-1, 2017. doi: 10.1109/JIOT.2017.2719623

[63] Y. Yang, H. Peng, L. Li and X. Niu, “General Theory of Security and a Study Case in Internet of Things,” in IEEE Internet of Things Journal, vol. 4, no. 2, April 2017, pp. 592-600

[64]M. Labib, S. Ha, W. Saad, and J. H. Reed, “A Colonel Blotto game for anti-jamming in the internet of things,” in 2015 IEEE Global Communications Conference (GLOBECOM). IEEE, pp. 1–6, 2015.

[65] E.E. Tsiropoulou, A. Thanou, S. Papavassiliou,"Quality of Experience-based museum touring: a human in the loop approach," in Social Network Analysis and Mining, Springer, vol. 7, no 1, pp. 1-33, 2017.

[66] E.E. Tsiropoulou, A. Thanou, S. Papavassiliou, "Modelling Museum Visitors Quality of Experience," 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP), pp. 77-82, October, 2016.

[67] E.E. Tsiropoulou, A. Thanou, S.T. Paruchuri, S. Papavassiliou, "Self-organizing Museum Visitor Communities: A Participatory Action Research based Approach," 12th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP),pp. 101-105, July, 2017

[68] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, “Information fusion to defend intentional attack in internet of things,” Internet of Things Journal, IEEE, vol. 1, no. 4, pp. 337–348, 2014

[69] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou and J. Chen, “Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks,” in IEEE Internet of Things Journal, vol. 3, no. 5, Oct. 2016, pp. 816-829

[70] N. Namvar, W. Saad, N. Bahadori, B. Kelley, “Jamming in the Internet of Things: A Game-Theoretic Perspective,” GLOBECOM, pp. 1-6, 2016.

[71] G. Katsinis, E.E. Tsiropoulou, and S. Papavassiliou, "On the Performance Evaluation of Distributed Resource Block and Power Allocation in D2D-enabled Multi-Cell Networks," in Proceedings of ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, November, 2017. (to appear)