Ατομική Διπλωματική Εργασία

ΔΙΑΧΕΙΡΙΣΗ ΤΟΥ ΦΑΣΜΑΤΟΣ ΣΥΧΝΟΤΗΤΩΝ ΣΤΑ ΕΞΥΠΝΑ ΣΠΙΤΙΑ

Φιλόκυπρος Π. Ιουλιανού

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2016

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Διαχείριση του φάσματος συχνοτήτων στα έξυπνα σπίτια

Φιλόκυπρος Π. Ιουλιανού

Επιβλέπων Καθηγητής
κ. Ανδρέας Πιτσιλλίδης

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Μάιος 2016

Ευχαριστίες

Η ολοκλήρωση αυτής της πτυχιακής υλοποιήθηκε με την υποστήριξη του καθηγητή μου κ. Ανδρέα Πιτσιλλίδη και γι’ αυτό θα ήθελα να εκφράσω τις ιδιαίτερες μου ευχαριστίες κυρίως για την εμπιστοσύνη που μου έδειξε, δίνοντας μου το συγκεκριμένο θέμα που κλήθηκα να μελετήσω, όπως επίσης και για την πολύτιμη βοήθεια και καθοδήγηση του για την επίλυση διαφόρων θεμάτων. Επίσης, θα ήθελα να ευχαριστήσω και τον κ. Γιάννο Μυλωνά για την πολύτιμη βοήθεια που μου έδωσε σχετικά με το εργαλείο προσομοιώσεων που χρησιμοποίησα αλλά και σχετικά με την διπλωματική μου.

Επιπλέον, αισθάνομαι την ανάγκη να επισημάνω την απέραντη ευγνωμοσύνη μου στην οικογένεια μου για όλα όσα μου έχουν προσφέρει κατά την διάρκεια των μαθητικών και φοιτητικών μου χρόνων και την αμέριστη υποστήριξη της σε κάθε μου επιλογή.

Περίληψη

Η ανάγκη για συνύπαρξη ή αλλιώς η ανάγκη για κοινή χρήση του φάσματος από τις ασύρματες τεχνολογίες στην σημερινή εποχή αυξάνεται σημαντικά καθώς οι επιπτώσεις στα συστήματα από την ασυντόνιστη λειτουργία σε μια κοινή συχνότητα είναι τεράστιες. Η αύξηση των data rates, η ραγδαία αύξηση των ατόμων που χρησιμοποιούν αυτές τις τεχνολογίες καθώς και το περιορισμένο εύρος συχνοτήτων είναι μερικοί από τους λόγους που χρειαζόμαστε κάποιους μηχανισμούς για την ομαλή συνύπαρξη και λειτουργία των ασύρματων δικτύων.

Η παρούσα διπλωματική εργασία έχει ως στόχο την αξιολόγηση των μηχανισμών συνύπαρξης των τεχνολογιών Zigbee και WiFi όταν τα δύο δίκτυα λειτουργούν μαζί σε ένα έξυπνο σπίτι. Συγκεκριμένα, αφού μελετήσαμε τον τρόπο λειτουργίας των τεχνολογιών αυτών καθώς και τους μηχανισμούς που διαθέτουν για να αποφεύγουν τις παρεμβολές από τα γειτονικά δίκτυα, προχωρήσαμε στην δημιουργία αντιπροσωπευτικών σεναρίων στον προσομοιωτή OPNET όπου υλοποιούμε δύο ή περισσότερα δίκτυα με κόμβους Zigbee και WiFi.

Έχοντας ρυθμίσει κατάλληλα την κάθε συσκευή στον προσομοιωτή για να αντιπροσωπεύει όσο γίνεται καλύτερα την πραγματικότητα, τρέξαμε τις προσομοιώσεις εξάγοντας αποτελέσματα από διάφορες μετρικές. Στη συνέχεια, αναλύσαμε αυτά τα αποτελέσματα τα οποία μας βοήθησαν να καταλήξουμε σε κάποια συμπεράσματα για την απόδοση των μεθόδων που χρησιμοποιεί η τεχνολογία Zigbee για αποφυγή της παρεμβολής και, τέλος, προτείνουμε τις δικές μας λύσεις και τροποποιήσεις στους υφιστάμενους μηχανισμούς με σκοπό να βελτιωθεί περισσότερο η απόδοση ολόκληρου του δικτύου.

Δηλώνω υπεύθυνα ότι το περιεχόμενο αυτής της εργασίας δεν περιέχει καμία αντιγραφή από άλλη πηγή χωρίς να γίνεται η νενομισμένη αναφορά στην πηγή. Έχω ελέγξει την εργασία μου με πρόγραμμα λογοκλοπής.

Περιεχόμενα

Κατάλογος Σχημάτων

Ακρώνυμα

WLAN - Wireless LAN

WiFi - Wireless Fidelity

IoT - Internet of Things

ISM - Industry Scientific and Medical

LR-WPAN - Low Rate- Wireless Personal Area Network

PHY - Physical Layer

MAC - Media Access Control

TDMA - Time Division Multiple Access

FDMA - Frequency Division Multiple Access

DSSS - Direct Sequence Spread Spectrum

OFDM - Orthogonal Frequency Division Multiplexing

AFHSSSS - Adaptive Frequency Hopping Spread Spectrum

FHSS - Frequency Hopping Spread Spectrum

ACK - Acknowledge

RF - Radio Frequency

PIR - Passive Infrared sensor

GHz - Gigahertz

MHz - Megahertz

Kbps - Kilobits per second

Mbps - Megabits per second

CCA - Clear Channel Assessment

BSS - Basic Service Set

TGk - Target Group k

DCA -Dynamic Channel Assignment

TPC - Transmit Power Control

CHDM - Coverage Hole Detection and Mitigation

SNR - Signal-to-Noise Ratio

SNIR – Signal-to-Noise and Interference Ratio

QoS - Quality of Service

XML - Extensible Markup Language

W - Watt

dBm - Decibel millwatt

IPv6 - Internet Protocol version 6

TCP - Transport Control Protocol

NAV - Network Allocation Vector

RSSI - Received Signal Strength Indicator

Κεφάλαιο 1

Εισαγωγή

1.1 Επισκόπηση και Κίνητρο

Τα τελευταία χρόνια έχει ανθίσει η έρευνα γύρω από τα ασύρματα δίκτυα και η εμφάνιση νέων τεχνολογιών όπως του Zigbee ανοίγει μια νέα κατηγορία έρευνας για τα LR-WPAN. Η τεχνολογία αυτή, όπως και κάθε άλλη ασύρματη τεχνολογία, εισχωρεί στην καθημερινότητά μας λόγω και της νέας τάσης του Internet of Things όπου οι τεχνολογικοί κολοσσοί ευελπιστούν πως σύντομα τα ασύρματα δίκτυα, κυρίως με αισθητήρες, θα αποτελούν αναπόσπαστο κομμάτι του έξυπνου σπιτιού μας προσφέροντάς μας νέες δυνατότητες όπου θα κάνουν την ζωή μας ακόμα πιο εύκολη. Έτσι, το ερευνητικό ενδιαφέρον για το πεδίο αυτό γίνεται όλο και πιο έντονο. Μέχρι στιγμής, έχουν μελετηθεί αρκετές πτυχές των ερωτημάτων και των αναγκών που περικλείονται στα ασύρματα δίκτυα χαμηλής ισχύος, αλλά ένα εξίσου σημαντικό ερευνητικό πεδίο αποτελεί και η ανάγκη της συνύπαρξης με άλλες τεχνολογίες.

Σε ένα έξυπνο σπίτι συνήθως υπάρχει ένας μεγάλος αριθμός από διαφορετικές συσκευές της ίδιας ή διαφορετικής τεχνολογίας, οι οποίες συνδέονται ασύρματα μεταξύ τους και οι περισσότερες χρησιμοποιούν το φάσμα του 2.4 GHz. Επίσης, η κάθε τεχνολογία πιθανόν να χρησιμοποιεί διαφορετικές μεθόδους για να ανιχνεύει τις ελεύθερες συχνότητες, αλλά και για να στέλνει τα δεδομένα στο μέσο. Ως εκ τούτου, η κοινή χρήση του φάσματος από διαφορετικές τεχνολογίες χωρίς να γίνεται κάποιος συντονισμός μεταξύ τους και χωρίς να υπάρχει κάποιος μηχανισμός για αποφυγή των συχνοτήτων που είναι κρατημένες, και άρα αποφυγή της παρεμβολής, οδηγεί συνήθως σε προβλήματα που μειώνουν σημαντικά την απόδοση των δικτύων. Για τον λόγο αυτό, χρειάζεται περαιτέρω έρευνα για την επίλυση των προβλημάτων της συνύπαρξης ανάμεσα σε ασύρματες τεχνολογίες.

Η ενασχόληση μεγάλου αριθμού ερευνών σχετικά με την συνύπαρξη σε ομογενή δίκτυα, δηλαδή την ύπαρξη δικτύων της ίδιας τεχνολογίας, αλλά και το γεγονός ότι υπάρχει μια αμφισβήτηση στο θέμα του κατά πόσον υπάρχει πράγματι κάποια σοβαρή επίπτωση στα δίκτυα διαφορετικών τεχνολογιών που συνυπάρχουν, αποτελούν τα κίνητρα μας για την παρούσα έρευνα στο πεδίο της συνύπαρξης των ασύρματων τεχνολογιών μέσα σε ένα σύγχρονο έξυπνο σπίτι.

1.2 Στόχος και Δομή της εργασίας

Στην παρούσα εργασία θα ασχοληθούμε κυρίως με το πρόβλημα συνύπαρξης του WiFi με το Zigbee. Όπως είπαμε και προηγουμένως, σε ένα σύγχρονο έξυπνο σπίτι μπορεί να συνυπάρχουν πολλές τεχνολογίες. Μερικές από αυτές είναι το WiFi, το Zigbee και το Bluetooth. Εμείς επιλέξαμε να επικεντρωθούμε στις δύο πρώτες τεχνολογίες, αφού το Zigbee είναι και μια σχεδόν πρόσφατη τεχνολογία που θέλει να κυριαρχήσει στο IoT αλλά και επειδή έχουν ήδη γίνει αρκετές μελέτες σχετικά με την συνύπαρξη του Bluetooth και του WiFi.

Έτσι, σε αυτή την εργασία θα μελετήσουμε εκτενώς τον τρόπο λειτουργίας των τριών τεχνολογιών που αναφέραμε, αλλά θα προχωρήσουμε σε πειραματική μελέτη με τον προσομοιωτή OPNET μόνο για τις τεχνολογίες Zigbee και WiFi. Μέσα από τις προσομοιώσεις θα δούμε την λειτουργία των μηχανισμών που χρησιμοποιούν η κάθε τεχνολογία για την μείωση της παρεμβολής που υπάρχει λόγω συνύπαρξης και θα προσπαθήσουμε να εξάγουμε κάποια συμπεράσματα που θα μας βοηθήσουν να προτείνουμε κάποιες περαιτέρω βελτιώσεις σε αυτές τις μεθόδους.

Η παρούσα εργασία έχει δομηθεί με τέτοιο τρόπο ώστε είναι η ακόλουθη:
Αρχικά, στο πρώτο κεφάλαιο εξετάζουμε το πρότυπο IEEE 802.15.4 στο οποίο βασίζεται το Zigbee, καθώς και τις τεχνολογίες του Bluetooth και του WiFi έτσι ώστε να μας βοηθήσουν στην κατανόηση του προβλήματος συνύπαρξης των τριών αυτών τεχνολογιών στο φάσμα του 2.4 GHz, αλλά και ειδικότερα του Zigbee με το WiFi.

Στο δεύτερο και τρίτο κεφάλαιο αναλύουμε εκτενώς τους μηχανισμούς που ήδη παρέχουν οι τεχνολογίες για την αντιμετώπιση των παρεμβολών, συμπεριλαμβανομένου και του Bluetooth, αλλά επικεντρωνόμαστε κυρίως στον μηχανισμό του Frequency Agility που παρέχει το Zigbee για την αποφυγή της παρεμβολής από το WiFi. Ακολούθως στο τέταρτο κεφάλαιο κάνουμε μια εκτενή αναφορά για τον μηχανισμό του Radio Resource Management στο WLAN ο οποίος παρέχει τρεις αλγόριθμους που βελτιώνουν την απόδοση του δικτύου WiFi λαμβάνοντας υπόψη κάποιες μετρικές σχετικά με το περιβάλλον λειτουργίας.

Τέλος, στο πέμπτο κεφάλαιο αναφέρουμε τους πιθανούς προσομοιωτές που μπορούν να χρησιμοποιηθούν για τα σενάρια που δημιουργούμε και συγκρίνοντας με τον OPNET καταλήγουμε στο να επιλέξουμε τον συγκεκριμένο προσομοιωτή. Αφού περιγράψουμε κάποιες αλλαγές που κάναμε στο μοντέλο του Wireless LAN στο OPNET, προχωρούμε στην δημιουργία και περιγραφή σεναρίων που περιέχουν τις τεχνολογίες Zigbee και WiFi και καταλήγουμε στο τελευταίο κεφάλαιο σε κάποια σημαντικά συμπεράσματα που μας βοηθούν να προτείνουμε κάποιες βελτιώσεις και να εισηγηθούμε κάποιες επιλογές για μελλοντική έρευνα.

Κεφάλαιο 2

Οι τεχνολογίες Zigbee, WiFi και Bluetooth

2.1 Εισαγωγή στο πρότυπο IEEE 802.15.4 και το Zigbee

Τα τελευταία χρόνια βλέπουμε μια ραγδαία ανάπτυξη στο πεδίο της ασύρματης τηλεπικοινωνίας. Η υιοθέτηση του προτύπου IEEE 802.11 για τα ασύρματα τοπικά δίκτυα (WLAN) καθώς και τα κυψελοειδή κινητά δίκτυα έχουν αποδείξει πως οι ασύρματες τεχνολογίες χαμηλού κόστους είναι αποδεκτές. Όπως είναι γνωστό, σήμερα υπάρχουν πολλές εφαρμογές που απαιτούν χαμηλό ρυθμό μετάδοσης, χαμηλή κατανάλωση ενέργειας και αποτελούν φτηνές λύσεις σε δίκτυα μικρής εμβέλειας και γι’ αυτό τον λόγο χρειαζόμαστε ένα ασύρματο προσωπικό δίκτυο χαμηλού εύρους ζώνης (LR-WPAN). Για την κάλυψη των αναγκών αυτών έχουν υλοποιηθεί αρκετές λύσεις, αλλά δυστυχώς είναι ακριβές και μη συμβατές με τα προϊόντα διαφορετικών κατασκευαστών. Μέσα σε αυτό το πλαίσιο, δημιουργήθηκε το νέο πρότυπο IEEE 802.15.4 που αφορά τα δίκτυα LR-WPAN προσφέροντας χαμηλό κόστος και μια πιο απλή λύση από τις υπόλοιπες.

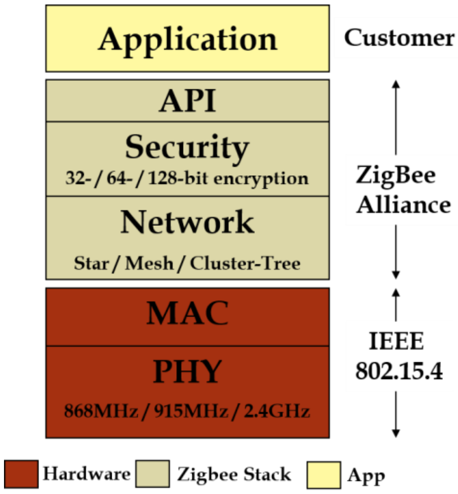
Το πρότυπο IEEE 802.15.4 δημιουργήθηκε από τον οργανισμό Institute of Electrical and Electronics Engineers (IEEE), όπου ο αριθμός 802 είναι το τμήμα που ασχολείται με τις λειτουργίες και τις τεχνολογίες των δικτύων, ο αριθμός 15 είναι η ομάδα που εργάζεται πιο συγκεκριμένα στα ασύρματα δίκτυα και ο αριθμός 4 είναι η ομάδα εργασίας που έχει γράψει το πρότυπο 802.15.4 για τα ασύρματα προσωπικά δίκτυα χαμηλού εύρους ζώνης (LR-WPAN). Στο πρότυπο αυτό περιγράφονται τα χαμηλότερα επίπεδα της στοίβας πρωτοκόλλων, δηλαδή το Φυσικό επίπεδο (PHY) και το επίπεδο Ελέγχου Προσπέλασης Μέσων (MAC).

Πάνω σε αυτό το πρωτόκολλο στηρίζεται η νέα τεχνολογία Zigbee [15] που ιδρύθηκε από την Zigbee Alliance και το οποίον προσθέτει τα ψηλότερα επίπεδα, δηλαδή τα επίπεδα Δικτύου, Μεταφοράς και Εφαρμογών. Η Zigbee Alliance είναι μια συνεργασία από μεγάλες εταιρείες που εργάζονται μαζί για την ανάπτυξη των συσκευών που βασίζονται στη τεχνολογία Zigbee και αυτό έχει οδηγήσει στη ραγδαία αύξηση της χρήσης του προτύπου IEEE 802.15.4. Συγκεκριμένα, η Zigbee Alliance έχει σκοπό να αντικαταστήσει τους ηλεκτρικούς διακόπτες και τους διάφορους απλούς αισθητήρες με δίκτυα από ασύρματους αισθητήρες-κόμβους που επικοινωνούν μεταξύ τους ακόμη και αν αυτοί είναι κατασκευασμένοι από διαφορετικούς κατασκευαστές. Σύμφωνα με την πρόβλεψη της παγκόσμιας εταιρείας ερευνών ON World [4] που έγινε το 2015 αναφέρει πως οι συσκευές Zigbee θα φτάσουν τις 2,5 δις πωλήσεις στα επόμενα 5 χρόνια.

Τα πλεονεκτήματα της τεχνολογίας Zigbee/IEEE 802.15.4 σε σχέση με άλλες παρόμοιες τεχνολογίες είναι:

- Η χαμηλή κατανάλωση ενέργειας αφού η ισχύς των απλών συσκευών είναι 0,001 mW.
- Το χαμηλό κόστος εγκατάστασης που έχει ως αποτέλεσμα να μπορεί να επεκταθεί ευρέως στις ασύρματες εφαρμογές ελέγχου και παρακολούθησης.
- Η υποστήριξη δικτύων με αριθμό κόμβων μέχρι 65,000.
- Αξιοπιστία: υλοποιεί τον αλγόριθμο CSMA/CA από το πρότυπο IEEE 802.15.4 όπου αποφεύγει τις συγκρούσεις πακέτων στο δίκτυο. Επίσης, στο φυσικό επίπεδο MAC υπάρχει η επιβεβαιωμένη μετάδοση των δεδομένων, όπου ο πομπός αναμένει επιβεβαίωση (Acknowledgement) από τον δέκτη για το ότι έλαβε τα δεδομένα που του στάλθηκαν.
- Το ευέλικτο και επεκτάσιμο δίκτυο. Δηλαδή, αν μια συσκευή σταματήσει να λειτουργεί ή προσθέσουμε μια νέα συσκευή στο δίκτυο, δεν θα επηρεάσουμε την λειτουργία του υπόλοιπου δικτύου αφού αυτό θα προσαρμοστεί ανάλογα.
- Η υποστήριξη των τοπολογιών δέντρου, αστέρι και πλέγμα.
- Απλούστερη τεχνολογία από άλλα WPAN (όπως το Bluetooth).
- Ο χαμηλός ρυθμός μετάδοσης που κυμαίνεται μεταξύ 20 kbps και 250 kbps.
- Η δυνατότητα εγκατάστασης των συσκευών σε δύσβατες περιοχές.

- Η λειτουργία σε συχνότητες που δεν χρειάζεται άδεια χρήσης. Πιο συγκεκριμένα λειτουργεί στις 2.400-2.484 GHZ (Παγκόσμια) , 902-928 MHZ (Αμερική) και 868.0-868.6 MHZ (Ευρώπη). Στο φάσμα ISM 2.4 GHz υπάρχουν 16 κανάλια, στο φάσμα 915MHz υπάρχουν 10 κανάλια και στο 868 MHz μόνο 1 κανάλι.
- Η ακτίνα κάλυψης του σήματος είναι στα 30 m περίπου σε εσωτερικό περιβάλλον και 100 m στο εξωτερικό περιβάλλον.



Σχήμα 2.1: Στοίβα πρωτοκόλλου Zigbee

2.1.1 Συσκευές

Οι συσκευές Zigbee χωρίζονται στις ακόλουθες 3 κατηγορίες:

<u>Διαχειριστής του δικτύου (Coordinator):</u> Η σημαντικότερη συσκευή σε ένα Zigbee δίκτυο γιατί χωρίς την ύπαρξη του δεν είναι εφικτή η δημιουργία του δικτύου. Επίσης, υπάρχει μόνο ένας Coordinator σε κάθε δίκτυο γιατί αυτός ξεκινά το δίκτυο. Εφόσον εκτελέσει σάρωση καναλιών, καθορίζει την συχνότητα του δικτύου και θέτει σε λειτουργία το δίκτυο, έτσι ώστε να επιτραπεί η σύνδεση άλλων συσκευών.

<u>Δρομολογητής (Router):</u> Λειτουργεί ως μεσάζον με την μεταφορά των μηνυμάτων από την μια συσκευή στην άλλη και μπορεί να κάνει εφικτή την επέκταση του δικτύου ανάλογα με το αν υπάρχει διαθέσιμη IP διεύθυνση, αν η συσκευή είναι συμβατή με τις προϋποθέσεις του δικτύου και αν επιτρέπεται επιπλέον σύνδεση στο router.

<u>Έξυπνες συσκευές Zigbee (End devices):</u> Είναι αισθητήρες που έχουν την δυνατότητα να παρέχουν πληροφορίες προς τον πατρικό τους κόμβο είτε είναι coordinator είτε router. Όμως, δεν μπορούν να μεταφέρουν δεδομένα από άλλες συσκευές ή να επικοινωνήσουν απευθείας

με άλλα end devices. Αυτό δίνει το πλεονέκτημα να εξοικονομούν ενέργεια με την απενεργοποίηση τους (sleep) σε περιόδους που δεν στέλνουν ή λαμβάνουν δεδομένα.

2.1.2 Καταστάσεις λειτουργίας και τοπολογίες

Τα δίκτυα με συσκευές Zigbee υποστηρίζουν 2 ειδών καταστάσεων λειτουργίας: την beacon και non-beacon λειτουργία. Στα beacon-enabled δίκτυα, ο Zigbee Coordinator στέλνει ανά τακτά χρονικά διαστήματα ένα σήμα, το λεγόμενο beacon, με σκοπό τον συγχρονισμό των συσκευών που βρίσκονται στο δίκτυο και την αφύπνιση τους, αν κοιμούνται, για να παραλάβουν τα μηνύματα που έχουν από τον διαχειριστή. Το πλεονέκτημα με αυτά τα δίκτυα είναι ότι έχουμε εξοικονόμηση ενέργειας από τις συσκευές, αφού μπορεί να «κοιμούνται» μέχρι την επόμενη χρονική στιγμή (time slot) που είναι καθορισμένη ότι θα στείλει ο Coordinator και θα μπορούν να στείλουν δεδομένα οι κόμβοι. Για την πρόσβαση στο κανάλι και για να αποφεύγονται οι συγκρούσεις των πακέτων χρησιμοποιείται ο μηχανισμός slotted CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Από την άλλη μεριά, στα δίκτυα non-beacon enabled δεν υπάρχει συγχρονισμός μεταξύ των συσκευών αφού απουσιάζει η μετάδοση του beacon από τον διαχειριστή-Coordinator. Εδώ όμως, ο Coordinator και ο Router παραμένουν άγρυπνοι και έχουμε μεγαλύτερη κατανάλωση ενέργειας, γιατί δεν ξέρουμε πότε θα στείλει κάποια συσκευή μήνυμα σε κάποιον κόμβο και γι' αυτό παρακολουθούν συνεχώς το δίκτυο. Επίσης, χρησιμοποιείται ο μηχανισμός unslotted CSMA/CA για την πρόσβαση στο κανάλι αφού δεν έχουμε beacon που πρέπει να σταλούν σε συγκεκριμένα time slots.

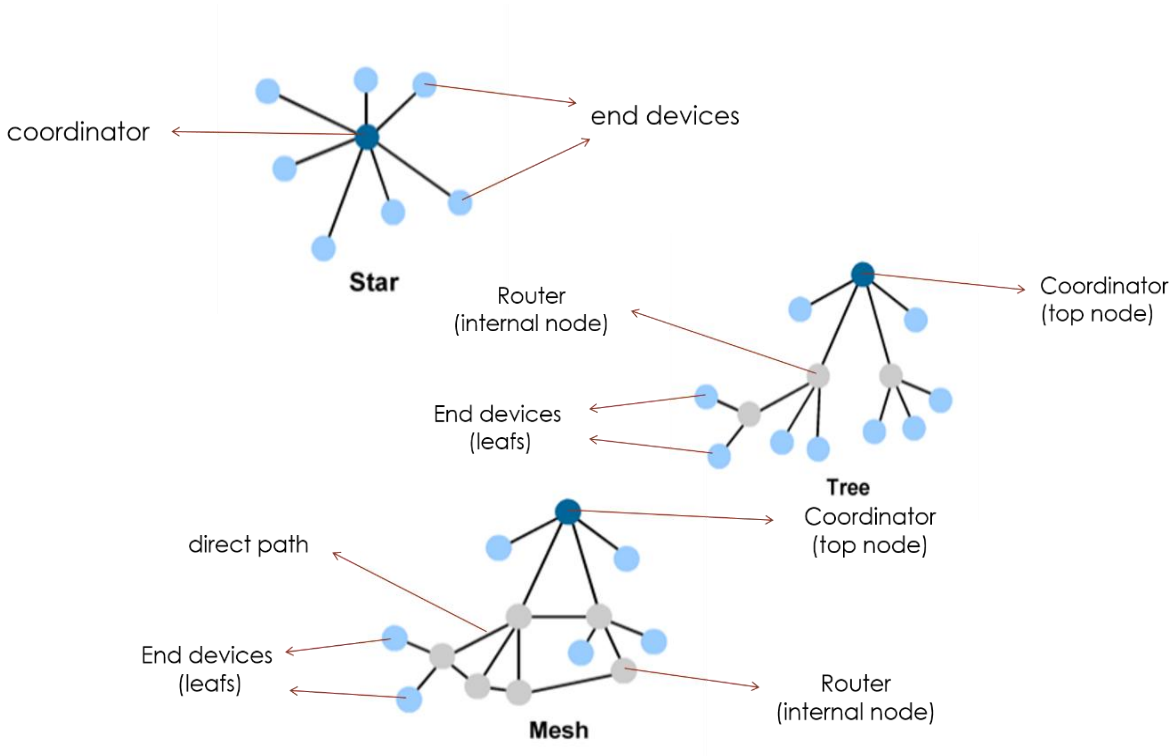
Όσον αφορά τις τοπολογίες στα δίκτυα Zigbee, υπάρχουν 3 ειδών τοπολογίες:

1. <u>Τοπολογία αστερισμού:</u> Υπάρχει ένας κεντρικός κόμβος που είναι ο διαχειριστής (Coordinator), ο οποίος συνδέεται με όλες τις άλλες έξυπνες συσκευές (end devices) στο δίκτυο και όλα τα μηνύματα στο δίκτυο ταξιδεύουν μέσω αυτού. Το πλεονέκτημά της είναι ότι τα πακέτα πηγαίνουν το μέγιστο μέχρι 2 κόμβους για να φτάσει το μήνυμα στον παραλήπτη και έτσι είναι μια απλή τοπολογία. Από την άλλη, ολόκληρη η λειτουργία του δικτύου εξαρτάται από τον διαχειριστή και αν υποστεί κάποιο πρόβλημα τότε το δίκτυο καταρρέει.

   <u>Τοπολογία δέντρου:</u> Έχει ένα κορυφαίο κόμβο που είναι η ρίζα και τα παιδιά της ρίζας είναι οι routers και τα end devices. Οι κόμβοι (end devices) που ενώνονται στον coordinator ή στους routers ονομάζονται παιδιά και οι μόνοι κόμβοι που μπορούν να έχουν παιδιά είναι ο coordinator ή ο router. Για να φτάσει στον προορισμό του ένα μήνυμα, τα end devices επικοινωνούν με τον πατέρα τους μόνο (router ή coordinator),

δηλαδή από κάποιο φύλλο προς την ρίζα, και στη συνέχεια προς τα κάτω μέχρι τον τελικό κόμβο που πρέπει να επικοινωνήσει. Το πλεονέκτημα αυτής είναι ότι υποστηρίζει την κινητικότητα των end devices και έτσι αν μια συσκευή μετακινηθεί θα συνδεθεί ξανά στο δίκτυο με τον πιο κοντινό της πατέρα. Το αρνητικό της τοπολογίας αυτής είναι ότι αν ένας γονέας (router) έχει πρόβλημα, τότε τα παιδιά του δεν θα μπορούν να επικοινωνήσουν με τις υπόλοιπες συσκευές στο δίκτυο. Ακόμη, στην περίπτωση που δύο κόμβοι βρίσκονται σε πολύ κοντινή απόσταση, δεν μπορούν να επικοινωνήσουν απευθείας, αλλά θα πρέπει να ακολουθήσουν την μέθοδο που περιγράψαμε.

2. <u>Τοπολογία πλέγματος:</u> Η δομή αυτή της τοπολογίας μοιάζει με εκείνη του δέντρου, μόνον που εδώ έχουμε μερικά από τα φύλλα να συνδέονται μεταξύ τους. Δηλαδή, επιτρέπει στις συσκευές να συνδέονται απευθείας, αν υπάρχει απευθείας διαδρομή, και να ανταλλάσσουν πληροφορίες χωρίς να χρειάζεται να πηγαίνουν σε κάποιο ενδιάμεσο κόμβο, όπως τον δρομολογητή (router). Εδώ έχουμε πολλά πλεονεκτήματα που μερικά είναι η εύκολη επέκταση του δικτύου με την προσθήκη κόμβων, η ύπαρξη εναλλακτικών διαδρομών αν υπάρχει πρόβλημα με κάποια συσκευή και με την άμεση επικοινωνία έχουμε μειωμένη ισχύ και άρα περισσότερη αυτονομία.



Σχήμα 2.2: Τοπολογίες Zigbee

Τοπολογία	**Πλεονεκτήματα**	**Μειονεκτήματα**
Αστέρι-Star	1. Απλή τοπολογία 2. Μικρός χρόνος αναμονής 3. Μέγιστος αριθμός hops: 2	1. Μικρής κλίμακας 2. Εξάρτηση δικτύου από τον coordinator
Δέντρο-Tree	1. Υποστηρίζει την κινητικότητα των συσκευών.	1. Αδυναμία επικοινωνίας κόμβων όταν ο γονέας απενεργοποιηθεί 2. Απουσία άμεσης επικοινωνίας
Πλέγμα-Mesh	1. Χαμηλό κόστος δρομολόγησης 2. Άμεση επικοινωνία 3. Χρήση χαμηλότερης ισχύς 4. Ευέλικτη 5. Υποστηρίζει την κινητικότητα των συσκευών.	1. Ανάγκες αποθήκευσης πινάκων δρομολόγησης

Σχήμα 2.3: Πίνακας με τις διαφορές των τοπολογιών Zigbee

2.1.3 Εφαρμογές

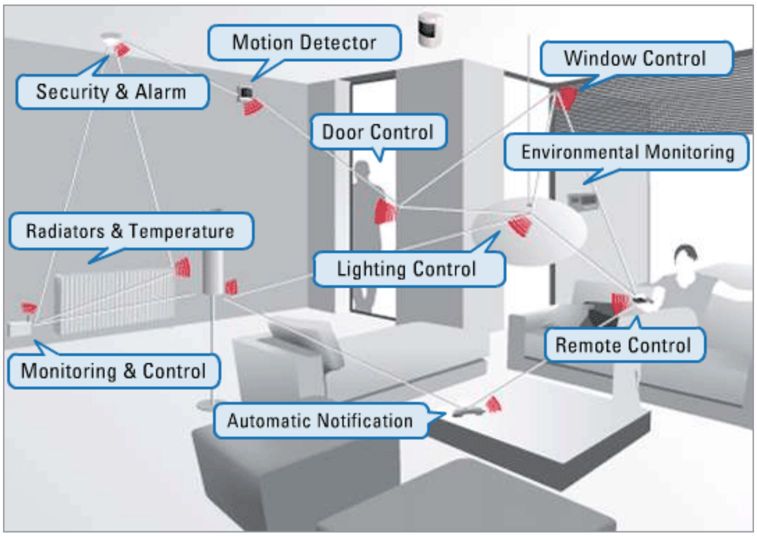
Οι συσκευές Zigbee μπορούν να χρησιμοποιηθούν σε ποικίλες εφαρμογές ανάλογα με το περιβάλλον που βρίσκονται. Πιο κάτω καταγράφουμε μερικές από τις εφαρμογές:

1. Αυτοματοποίηση σπιτιού (Internet of Things): Το Zigbee βοηθά στον έλεγχο των οικιακών συσκευών από απόσταση. Για παράδειγμα, μπορούμε να ελέγξουμε τον φωτισμό του σπιτιού, την θέρμανση, τις συσκευές κλιματισμού, το σύστημα ασφαλείας και πολλές άλλες συσκευές που χρησιμοποιούμε καθημερινά στο σπίτι.

2. Βιομηχανική αυτοματοποίηση: Στα εργοστάσια παραγωγής και κατασκευής προϊόντων, υπάρχει ανάγκη για μια συνεχή επικοινωνία και παρακολούθηση μεταξύ διάφορων παραμέτρων και σημαντικών μηχανημάτων. Με την βοήθεια του Zigbee, το κόστος της επικοινωνίας μειώνεται καθώς και η διαδικασία ελέγχου βελτιώνεται με αποτέλεσμα να έχουμε μεγαλύτερη αξιοπιστία.

3. Smart metering: Το Zigbee παρέχει την δυνατότητα να έχουμε έξυπνους μετρητές ρεύματος στα σπίτια μας και ως αποτέλεσμα να μπορούμε να βλέπουμε τις καταναλώσεις του ρεύματος που κάνουμε με σκοπό να διαχειριστούμε καλύτερα το πώς χρησιμοποιούμε το ρεύμα και να μειώσουμε το κόστος που πληρώνουμε.

4. Παρακολούθηση περιβάλλοντος: Με το Zigbee μπορούμε να παρακολουθήσουμε σε ένα δάσος ή μια περιοχή που μας ενδιαφέρει την θερμοκρασία που υπάρχει, την υγρασία ή άλλους παράγοντες και με βάση αυτά να συμπεραίνουμε αν χρειάζεται να λάβουμε κάποια δράση είτε για βελτίωση των συνθηκών (σε φάρμες) είτε για αποτροπή κάποιας καταστροφής (φωτιά σε δάσος).



Σχήμα 2.4: Παράδειγμα Smart home

2.2 Τεχνολογίες που λειτουργούν στο φάσμα ISM 2.4 GHz

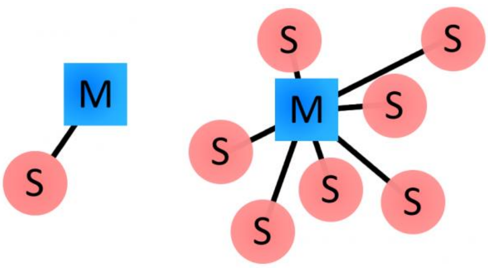
Ένα τυπικό έξυπνο σπίτι περιέχει μια ποικιλία από διάφορες συσκευές που επικοινωνούν ασύρματα με σκοπό να κάνουν το σπίτι πιο έξυπνο. Αυτές οι συσκευές στο έξυπνο σπίτι λειτουργούν συνήθως στο φάσμα συχνοτήτων 2.4 GHz Industry Scientific and Medical (ISM) για τον λόγο ότι η συχνότητα αυτή είναι διαθέσιμη παγκόσμια, χωρίς να χρειάζεται άδεια χρήσης και είναι η κατάλληλη για τις χαμηλού κόστους τεχνολογίες WPAN και WLAN. Συγκεκριμένα, η τεχνολογία Zigbee εκπέμπει συνήθως στο εύρος συχνοτήτων 2.400–2.4835 GHz γιατί είναι παγκόσμια διαθέσιμο και υπάρχουν 16 κανάλια για να επιλέξει. Ταυτόχρονα, στο εύρος 2.400–2.482 GHz βρίσκουμε να χρησιμοποιείται η τεχνολογία IEEE 802.11 b/g/n που βασικά είναι πιο γνωστή ως WiFi και η τεχνολογία IEEE 802.15.1 που είναι το Bluetooth. Σε αυτό το υποκεφάλαιο θα πούμε λίγα λόγια για τις δύο γνωστές τεχνολογίες που λειτουργούν μαζί με το Zigbee.

2.2.1 Bluetooth - IEEE 802.15.1

Με το πρότυπο IEEE 802.15.1 εννοούμε την τεχνολογία Bluetooth [11] που υπάρχει σχεδόν σε όλες τις ηλεκτρονικές συσκευές σήμερα και έχει σκοπό την ασύρματη ανταλλαγή των δεδομένων μεταξύ των συσκευών σε κοντινή απόσταση. Το πρότυπο IEEE 802.15.1 καθορίζει τα πρώτα δύο επίπεδα της στοίβας, φυσικό επίπεδο (PHY) και επίπεδο ελέγχου προσπέλασης μέσων (MAC). Η τεχνολογία Bluetooth λειτουργεί στην συχνότητα 2.4 GHz μαζί με τις τεχνολογίες Zigbee και WiFi, και μοιράζει το φάσμα σε 79 κανάλια με το εύρος ζώνης (bandwidth) στα 1 MHz.

Το πιο σημαντικό χαρακτηριστικό αυτή της τεχνολογίας είναι η τεχνική διαμόρφωσης του σήματος που ονομάζεται Frequency Hopping Spread Spectrum (FHSS) όπου η συχνότητα που μεταδίδει το σήμα ο αποστολέας (transmitter) αλλάζει 1600 φορές το δευτερόλεπτο σε συγχρονισμό με τον παραλήπτη, έτσι ώστε να αλλάζει μαζί του κανάλι για να λαμβάνει τις πληροφορίες. Ακόμη ένα σημαντικό χαρακτηριστικό του Bluetooth είναι ότι οι συσκευές χωρίζονται σε 3 κατηγορίες ανάλογα με την ισχύ που μπορεί να στείλει το σήμα. Συγκεκριμένα, η κατηγορία 1 έχει ως μέγιστη ισχύ τα 100 mW με απόσταση κάλυψης τα 100 m, η κατηγορία 2 στέλνουν με 2,5 mW και φτάνει μέχρι τα 10 m και η κατηγορία 3 έχει μέγιστη ισχύ το 1 mW με την απόσταση να φτάνει στο 1 m.

Σχετικά με τα δίκτυα των συσκευών της τεχνολογίας Bluetooth, αυτά αναφέρονται συχνά ως piconets και χρησιμοποιούν το μοντέλο master/slave για να υπάρχει έλεγχος στο πότε και πού μια συσκευή μπορεί να στείλει δεδομένα. Στο συγκεκριμένο μοντέλο δικτύου, μια συσκευή master μπορεί να συνδεθεί μέχρι και σε 7 διαφορετικές συσκευές slave ταυτόχρονα και κάθε συσκευή slave μπορεί να συνδεθεί με μόνο ένα master. Η συσκευή master συντονίζει την επικοινωνία σε ολόκληρο το δίκτυο piconet και μπορεί να στείλει ή να λάβει δεδομένα από οποιαδήποτε συσκευή slave. Από την άλλη, οι συσκευές slave μπορούν να στείλουν ή να λάβουν δεδομένα μόνο από τον master και όχι μεταξύ τους. Όσον αφορά το πρόβλημα της συνύπαρξης της τεχνολογίας Bluetooth με το WiFi, αυτό αν και σπάνια συμβαίνει δεν θα ασχοληθώ σε αυτή την εργασία. Παράλληλα, πρόβλημα συνύπαρξης υπάρχει μεταξύ του Bluetooth και του Zigbee το οποίον πάλι λειτουργεί στο φάσμα 2.4 GHz. Έχοντας όμως υπόψη



Σχήμα 2.5: Παράδειγμα τεχνολογίας Bluetooth piconet

πως το Bluetooth χρησιμοποιεί την τεχνική FHSS και ότι οι συσκευές Zigbee βασίζονται στην τεχνική DSSS, καταλήγουμε πως δεν υπάρχει σοβαρό πρόβλημα παρεμβολής μεταξύ του Bluetooth και του Zigbee, αφού εκτός του ότι χρησιμοποιούν διαφορετικές τεχνικές αποστολής των δεδομένων, το εύρος ζώνης (bandwidth) κάθε καναλιού στο Zigbee είναι μόνο 2 MHz και του Bluetooth 1 MHz, και άρα η πιθανή παρεμβολή μπορεί να συμβεί μόνο όταν συμπίπτει το κανάλι που επιλέγει το Bluetooth για μια συγκεκριμένη χρονική στιγμή.

2.2.2 WiFi - IEEE 802.11b/g/n/ac

Το πρότυπο IEEE 802.11b/g είναι γνωστό ως WiFi και είναι μια ασύρματη τεχνολογία που υποστηρίζει την επικοινωνία ανάμεσα σε υπολογιστές, δρομολογητές και άλλες συσκευές στα ασύρματα τοπικά δίκτυα (WLAN). Γενικά, το IEEE 802.11 είναι ένα σύνολο από προδιαγραφές για την υλοποίηση του φυσικού επιπέδου (PHY) και του επιπέδου ελέγχου προσπέλασης μέσων (MAC) που χρειάζονται για την επικοινωνία των υπολογιστών σε WLAN δίκτυα. Το πρότυπο δημιουργήθηκε από την ομάδα IEEE 802 και τα γράμματα στο τέλος αναφέρονται σε συγκεκριμένες εκδόσεις του προτύπου. Για παράδειγμα, το γράμμα “g” είναι η έκδοση που μπήκε σε εφαρμογή το 2003 και αντικατέστησε την έκδοση “b” που χρησιμοποιείτο από το 1999. Οι πιο πρόσφατες εκδόσεις είναι οι “n” και “ac”.

Σχετικά με τις συχνότητες λειτουργίας, το IEEE 802.11b/g λειτουργεί στα 2.4 GHz, η έκδοση IEEE 802.11n λειτουργεί ταυτόχρονα στα 2.4 GHz και 5 GHz, και τέλος η τελευταία έκδοση IEEE 802.11ac λειτουργεί μόνο στα 5 GHz. Ανάλογα με την κάθε έκδοση του προτύπου, έχουμε και μια αύξηση στην ταχύτητα μετάδοσης των δεδομένων στο δίκτυο. Με το IEEE 802.11g το εύρος ζώνης φτάνει τα 54 Mbps που είναι μεγαλύτερο από αυτό των 11 Mbps που είχε το IEEE 802.11b αλλά είναι μικρότερο από τα 150 Mbps που πετυχαίνει το IEEE 802.11n. Οι ταχύτητες αυτές των εκδόσεων θεωρούνται μικρότερες από την ταχύτητα των 6,77 Gbps που μπορούμε να φτάσουμε με το πρότυπο IEEE 802.11ac το οποίο είναι και το πιο πρόσφατο.

Όσον αφορά τις τεχνολογίες διαμόρφωσης του σήματος, η τεχνολογία IEEE 802.11b χρησιμοποιεί το DSSS όπου οι πληροφορίες διασκορπίζονται σε μεγαλύτερο εύρος συχνοτήτων από όσον πραγματικά χρειάζεται, με το μέγεθος του bandwidth να είναι 22 MHz ενώ οι τεχνολογίες IEEE 802.11g/n χρησιμοποιούν το OFDM με το μέγεθος του bandwidth να είναι 22 MHz στη συχνότητα 2.4 GHz, και για την συχνότητα 5 GHz που λειτουργεί παράλληλα η έκδοση “n”, το bandwidth είναι 40 MHz. Με την ανάπτυξη της τεχνολογίας IEEE 802.11ac το εύρος των συχνοτήτων που δεσμεύεται για μετάδοση ξεκινά από τα 80 MHz στην πρώτη έκδοση του προτύπου, αλλά λειτουργεί όπως είπαμε μόνο στα 5 GHz. Τέλος, να προσθέσουμε πως τα πρότυπα IEEE 802.11b/g/n καθορίζουν 11 κανάλια για την Αμερική και

13 κανάλια για την Ευρώπη , από τα οποία μόνο 3 κανάλια δεν έχουν επικάλυψη μεταξύ τους. Πιο κάτω βλέπουμε συνοπτικά στον πίνακα τις 3 τεχνολογίες που μόλις περιγράψαμε.

Όνομα	**Bluetooth 4.0 Low Energy (BLE)**	**ZigBee**	**WiFi**
IEEE Standard	802.15.1	802.15.4	802.11 (b, g, n)
Συχνότητα (GHz)	2.4	0.868, 0.915, 2.4	2.4 και 5
Μέγιστο bit rate (Mbps)	1	0.250	11 (b), 54 (g), 600 (n)
Throughput (Mbps)	0.27	0.2	7 (b), 25 (g), 150 (n)
Μέγιστη (εξωτερική) εμβέλεια (Μέτρα)	50	10-100	100-250
Κατανάλωση ρεύματος	Πολύ χαμηλή	Πολύ χαμηλή	Μεγάλη
Αντοχή μπαταρίας	Μήνες μέχρι χρόνια	Μήνες μέχρι χρόνια	Ώρες
Μέγεθος δικτύου	Απροσδιόριστο	64,000+ κόμβοι	255 κόμβοι

Σχήμα 2.6: Πίνακας σύγκρισης Bluetooth, Zigbee και WiFi

2.3 Το πρόβλημα συνύπαρξης του Zigbee στο φάσμα ISM 2.4 GHz

Η λειτουργία διάφορων συσκευών στο φάσμα 2.4 GHz που να είναι της ίδιας τεχνολογίας ή διαφορετικής και η κοινή χρήση του από τις πλείστες τεχνολογίες, μπορεί να οδηγήσει στο πρόβλημα της παρεμβολής μεταξύ των συσκευών και αυτό να επηρεάσει την απόδοση των συστημάτων στο δίκτυο. Πιο κάτω θα περιγράψουμε το πρόβλημα της παρεμβολής που εμφανίζεται στο φάσμα αυτό.

2.3.1 Φάσμα ISM 2.4 GHz

Το φάσμα ISM 2.4 GHz είναι πολύ διάσημο για τις ασύρματες τεχνολογίες εξαιτίας της ελεύθερης χρήσης του που δεν απαιτεί κάποια άδεια και γιατί είναι ένα πολύ μεγάλο φάσμα με 83.5 MHz εύρος ζώνης. Ως αποτέλεσμα, τα συστήματα τηλεπικοινωνιών που λειτουργούν στη ζώνη αυτή πρέπει να επιδεικνύουν προσαρμοστική χρήση του φάσματος, προκειμένου να βελτιώσουν τις επιδόσεις τους και να αντιμετωπίσουν τα επίπεδα παρεμβολής που προκαλούνται από τις υπόλοιπες συσκευές που συνυπάρχουν στις συχνότητες αυτές. Η μελέτη της παρεμβολής που προκαλείται στο φάσμα ISM 2.4 GHz είναι επιτακτική, λόγω της ραγδαίας αύξησης του αριθμού των συσκευών που λειτουργούν σε αυτή τη ζώνη τα τελευταία χρόνια. Αυτή η αύξηση οφείλεται στο ότι τα συστήματα που βασίζονται στο Bluetooth χαμηλής ενεργειακής τεχνολογίας, το Zigbee και το 6LowPAN, κερδίζουν τεράστια δυναμική λόγω του μικρού μεγέθους τους, του χαμηλού κόστους τους και την ελάχιστη κατανάλωση ρεύματος τα οποία προβλέπεται να υπάρχουν 20,8 δισεκατομμύρια συσκευές μέχρι το 2020 με τον ερχομό του Internet Of Things (IoT) [3]. Έτσι, η ζώνη ISM 2.4 GHz γίνεται πολύ «εχθρική».

2.3.2 Πηγές παρεμβολής

Πριν να αναφερθούμε στις πιθανές πηγές της παρεμβολής, θα περιγράψουμε τα είδη της παρεμβολής που υπάρχουν και πιθανόν να συμβούν. Αρχικά, έχουμε την co-channel παρεμβολή η οποία συμβαίνει όταν πολλοί χρήστες είναι σε κοντινή απόσταση και χρησιμοποιούν το ίδιο κανάλι, με αποτέλεσμα να αυξάνεται ο θόρυβος στο κανάλι και να μειώνεται η απόδοση τους. Στη συνέχεια έχουμε την adjacent channel παρεμβολή η οποία συμβαίνει όταν οι συσκευές χρησιμοποιούν γειτονικά κανάλια ενώ βρίσκονται σε πολύ κοντινή απόσταση. Ακόμα ένα είδος παρεμβολής, που είναι και το χειρότερο, είναι όταν υπάρχουν πολλές συσκευές με διαφορετικές τεχνολογίες και βασίζονται σε διαφορετική χρήση του φάσματος, όπως συμβαίνει με τις DSSS και OFDM συσκευές.

Προχωρώντας στις πηγές της παρεμβολής, με την μεγάλη εξάπλωση των ασύρματων συσκευών στην ελεύθερη ζώνη ISM 2.4 GHz οι συσκευές που δημιουργούν παρεμβολές μπορεί να είναι οποιεσδήποτε, αφού οι ασύρματες τεχνολογίες τώρα ενσωματώνονται σε ρολόγια, παπούτσια, MP3 players, και πολλές άλλες συσκευές των καταναλωτών. Επιπλέον, υπάρχουν συσκευές που ενώ προηγουμένως δεν υποστήριζαν ασύρματες τεχνολογίες, τώρα έχουν ενημερωθεί με την τεχνολογία RF και αποτελούν μια πηγή παρεμβολής. Για παράδειγμα, ένας ανιχνευτής κίνησης χρησιμοποιεί ένα συνδυασμό του παθητικού υπέρυθρου αισθητήρα (PIR) και ενός ραντάρ 2.4 GHz για την ανίχνευση κίνησης. Η συσκευή αυτή μοιάζει πανομοιότυπα με τον προκάτοχό της, αλλά η νέα αυτή γενιά δημιουργεί σημαντικές παρεμβολές που μπορούν να διαταράξουν το Wi-Fi δίκτυο μας. Επιπρόσθετα, μεγάλος αριθμός διαφορετικών τύπων συσκευών που λειτουργούν σε αυτό το φάσμα ξεπερνούν τον αριθμό των WiFi συσκευών και σε αυτές περιλαμβάνονται οι φούρνοι μικροκυμάτων, τα ασύρματα τηλέφωνα, οι ασύρματες βίντεο κάμερες, οι συσκευές Zigbee και άλλες πολλές. Όλες αυτές οι μη IEEE 802.11b/g συσκευές λειτουργούν χωρίς κάποια συνεργασία με τις IEEE 802.11b/g συσκευές και προκαλούν σημαντική μείωση στο throughput του δικτύου. Έτσι, υπάρχει ανάγκη για συνύπαρξη και συνεργασία μεταξύ των διάφορων τεχνολογιών που μοιράζονται τις ίδιες συχνότητες.

2.3.3 Κύριοι παράγοντες παρεμβολής

Οι κύριες ασύρματες τεχνολογίες που λειτουργούν σε αυτό το φάσμα και περιγράψαμε προηγουμένως είναι το Bluetooth, το WiFi και το Zigbee, αλλά στην εργασία αυτή θα ασχοληθούμε εκτενώς με το πρόβλημα συνύπαρξης του Zigbee (IEEE 802.15.4) και του WiFi (IEEE 802.11g) χρησιμοποιώντας το πρότυπο IEEE 802.11g επειδή αυτό χρησιμοποιείται ευρέως σήμερα. Φυσικά, το επίπεδο της παρεμβολής εξαρτάται από πολλούς παράγοντες. Οι πιο σημαντικοί παράγοντες είναι: 1) το μέγεθος της ισχύος (power) των συσκευών. Δηλαδή, όσο πιο μεγάλη είναι η ισχύς που λειτουργεί η συσκευή, τόσο πιο μεγάλη είναι η φυσική ζώνη παρεμβολής που δημιουργείται, 2) η συμπεριφορά του σήματος σε σχέση με τον χρόνο. Ορισμένες συσκευές, όπως τα παλιά ασύρματα τηλέφωνα, έχουν συνεχώς ενεργοποιημένο το σήμα τους για ανταλλαγή δεδομένων, ενώ άλλες συσκευές έχουν κάποιες περιόδους που είναι ή όχι ενεργοποιημένες. Άρα, γενικά όσο πιο μεγάλο είναι το χρονικό διάστημα που μια συσκευή έχει ενεργοποιημένο το σήμα της, τόσο πιο μεγάλη θα είναι η επίδραση στο throughput. Τέλος, έχουμε την 3) συμπεριφορά του σήματος σε σχέση με την συχνότητα. Εδώ εννοούμε ότι κάποιες συσκευές λειτουργούν σε συγκεκριμένες συχνότητες και επηρεάζουν συγκεκριμένα κανάλια του WiFi, ενώ άλλες συσκευές, όπως το Bluetooth, αναπηδούν συχνότητες και επηρεάζουν λιγότερο τις υπόλοιπες τεχνολογίες. Έχοντας υπόψη αυτές τις παραμέτρους που καθορίζουν το επίπεδο της παρεμβολής, μπορούμε να μελετήσουμε την περίπτωση του Zigbee με το WiFi (θα αναφερόμαστε με το WiFi ως το πρότυπο IEEE 802.11g).

2.4 Το πρόβλημα συνύπαρξης του Zigbee με το WiFi

Η συνύπαρξη του Zigbee με το WiFi είναι μια περίπτωση που άρχισε να απασχολεί πολύ τελευταίως την ερευνητική κοινότητα, όπως βλέπουμε στα [12,16,17], εξαιτίας και της προσεχούς έλευσης του IoT. Τα χαρακτηριστικά των δικτύων και των δύο τεχνολογιών διαφέρουν κατά πολύ, με αποτέλεσμα να έχουμε ένα ασύμμετρο πρόβλημα συνύπαρξης. Όπως γνωρίζουμε, η ισχύς που λειτουργεί το Zigbee είναι πολύ λιγότερη από αυτή του WiFi και αυτό το καθιστά πιο ευάλωτο σε πιθανή παρεμβολή από το WiFi παρότι το αντίστροφο. Συγκεκριμένα, σύμφωνα με το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI) η μέγιστη ισχύς (transmission power) που ορίζει για το πρότυπο IEEE 802.11g που χρησιμοποιεί την κωδικοποίηση OFDM είναι τα 20 dBm (100 mW) [1] ενώ το Zigbee που είναι μια τεχνολογία χαμηλής ισχύος ορίζεται στα 0 dBm (1 mW) [2]. Συνεπώς, όταν δύο συσκευές, η μία με τεχνολογία ZigBee και η άλλη με WiFi, χρησιμοποιούν το ίδιο κανάλι την ίδια χρονική στιγμή για να επικοινωνήσουν στο δίκτυο τους, εμφανίζεται το πρόβλημα της παρεμβολής το οποίον έχει ως αποτέλεσμα το χάσιμο των πακέτων δεδομένων που μεταδίδουν. Έτσι, οι δύο συσκευές θα προσπαθήσουν να ξαναστείλουν τα πακέτα δεδομένων που χάθηκαν, μέχρι να καταφέρουν να τα αποστείλουν επιτυχώς.

Εκτός από την διαφορά ισχύος στις δύο τεχνολογίες, η μέθοδος μετάδοσης των δεδομένων του WiFi και του Zigbee είναι διαφορετική, όπως και τα διαθέσιμα κανάλια που μπορούν να χρησιμοποιήσουν στο φάσμα των 2.4 GHz. Το WiFi χρησιμοποιεί το OFDM για την μετάδοση των δεδομένων το οποίο χρησιμοποιεί πολλούς carriers για να μεταφέρονται τα δεδομένα, εξοικονομώντας εύρος ζώνης, αλλά το κύριο πλεονέκτημα του είναι η ικανότητά του να αντιμετωπίζει τις κακές συνθήκες του καναλιού χωρίς σύνθετα φίλτρα εξίσωση. Αν και με αυτές τις ιδιότητες του OFDM, η προσεκτική διαχείριση του φάσματος εξακολουθεί να είναι απαραίτητη αν λάβουμε υπόψη και τα διαθέσιμα κανάλια που είναι περιορισμένα για την μετάδοση του σήματος. Παρατηρώντας τα κανάλια που λειτουργεί το WiFi στο φάσμα 2.4 GHz, συνολικά έχουμε 11 κανάλια στην Αμερική, για την Ευρώπη έχουμε διαθέσιμα 13, και στην Ιαπωνία 14. Το εύρος ζώνης για κάθε κανάλι καθορίζεται στα 22 MHz και η απόσταση μεταξύ δύο γειτονικών καναλιών είναι στα 5 MHz. Έτσι, τα διαθέσιμα κανάλια που δεν έχουν επικάλυψη μεταξύ τους και αποφεύγονται οι παρεμβολές στην Ευρώπη είναι τα 1,7,13 και στην Αμερική τα 1,6,11.

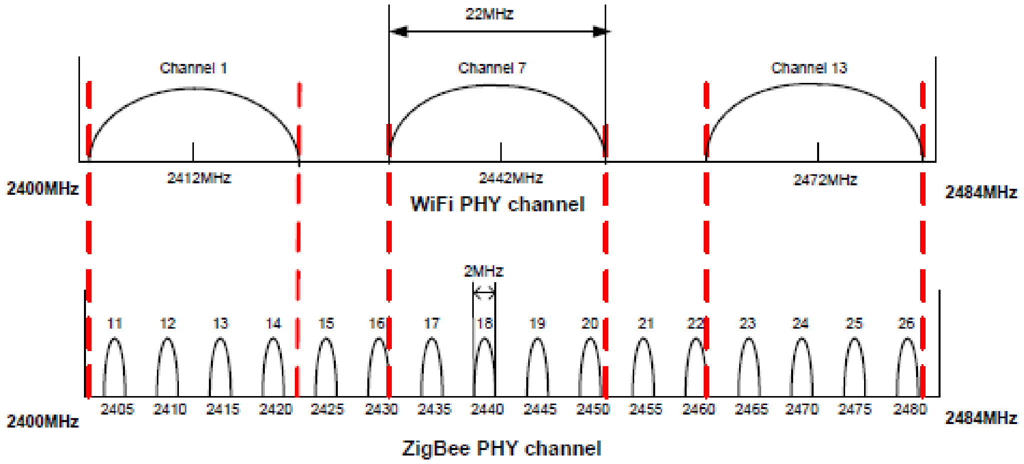
Από την άλλη, το Zigbee βασίζεται στο DSSS με το εύρος ζώνης του spread σήματος να είναι μόνο 2 MHz και όλες οι συσκευές Zigbee λειτουργούν σε σταθερό κανάλι. Τα διαθέσιμα κανάλια σε αυτό το φάσμα είναι 16 κανάλια ξεκινώντας από το κανάλι 11 (2.405 GHz) μέχρι το 26 (2.480 GHz). Ως αποτέλεσμα, τα κανάλια 1, 7 και 13 που χρησιμοποιεί το WiFi στην Ευρώπη έχουν επικάλυψη με τα πλείστα κανάλια του Zigbee, όπως φαίνεται και στο σχήμα παρακάτω, εκτός από τα κανάλια 15,16,21 και 22 τα οποία θα έχουν μικρή επιρροή από την παρεμβολή του WiFi. Επιπρόσθετα, αν και οι δύο τεχνολογίες χρησιμοποιούν την τεχνική CSMA/CA που απαιτεί να «ακούσει το μέσο» μια συσκευή πριν να στείλει, ο χρόνος που «ακούει» το WiFi είναι 20μs ενώ το Zigbee είναι κατά πολύ μεγαλύτερος στα 320μs [7]. Έτσι, έχουμε μεγαλύτερες πιθανότητες για συγκρούσεις πακέτων στις δύο τεχνολογίες.

Το πρόβλημα της παρεμβολής που προκαλείται μεταξύ του WiFi και του Zigbee έχει απασχολήσει αρκετά την ερευνητική κοινότητα. Για παράδειγμα, ο Kim *et al*. έδειξε στο [5] ότι η παρεμβολή από το 802.11 μπορεί να προκαλέσει μείωση της απόδοσης του δικτύου με κόμβους Zigbee. Το να μην μπορεί να θέτει υπό έλεγχο την παρεμβολή ή να μην μπορεί την αποφύγει το IEEE 802.15.4/ZigBee, μπορεί να οδηγήσει στα χειρότερα αποτελέσματα. Αν ένας χρήστης, για παράδειγμα, ενεργοποιήσει ένα λαμπτήρα ο οποίος χρησιμοποιεί την τεχνολογία Zigbee, ο λαμπτήρας μπορεί να ανταποκριθεί με μικρή καθυστέρηση ή μπορεί να μην ανταποκριθεί καθόλου αν τα πακέτα με τις εντολές του Zigbee χάνονται εξαιτίας της παρεμβολής με το WiFi. Αυτό μπορεί να συμβεί και με μεγαλύτερα δίκτυα Zigbee όπου θα υπάρχει μεγαλύτερο πρόβλημα.

Οι ερευνητές Sikora και Groza στο [8] και η Pollin et al. στο [9] επισημαίνουν πως υπάρχουν τέσσερεις παράμετροι για να δημιουργήσουμε την χειρότερη περίπτωση. Μια πρώτη παράμετρος είναι η υπόθεση πως το θύμα και αυτός που παρεμβάλλει χρησιμοποιούν κανάλια που επικαλύπτονται. Η δεύτερη παράμετρος είναι η χρήση του δικτύου (utilization) από το WiFi ή το Zigbee ή και από τα δύο είναι πολύ μεγάλη, τρίτη παράμετρος είναι ότι υπάρχει πολύ κοντινή απόσταση μεταξύ αυτού που παρεμβάλλει και του θύματος και τέλος, αυτός που παρεμβάλλει έχει πολύ υψηλή ισχύ. Το Zigbee είναι το θύμα στο [8] και αυτός που παρεμβάλλει στο [9]. Τα αποτελέσματα δείχνουν πως η παρεμβολή είναι πολύ σοβαρή σε αυτό το σενάριο και συγκεκριμένα το packet error rate είναι πάνω από 90% καθώς και η μείωση του throughput του WiFi στο [9] φτάνει μέχρι το 30%. Το συμπέρασμα στο [8] αναφέρει ότι, ακόμη και αν αναθέσουμε τα μη επικαλυπτόμενα κανάλια στο Zigbee, η ισχύς του WiFi είναι ψηλή και εκτός των καναλιών που μεταδίδει τα δεδομένα και άρα τα κανάλια χωρίς επικάλυψη παρουσιάζουν προβλήματα παρεμβολής.

Σε μια άλλη μελέτη, ο Shuaib et al. στο [10] συμβουλεύει τους ερευνητές να ξεχωρίζουν το Uplink από το Downlink όταν υπάρχει παρεμβολή, γιατί στο WiFi υπάρχουν δύο συσκευές: ο χρήστης και το Access Point. Το Uplink αναφέρεται στη μεταφορά δεδομένων από το χρήστη στο Access Point και το αντίστροφο αναφέρεται ως Downlink. Σε αυτή την αναφορά, τα αποτελέσματα δείχνουν ότι όταν οι δύο τεχνολογίες βρίσκονται κοντά η μία στην άλλη, έχουμε μεγάλη επιρροή στο Uplink παρότι στο Downlink ο λόγος μπορεί να είναι λόγω της διαφορετικής ισχύος μεταξύ του Access Point και του χρήστη, αφού η ισχύς που χρησιμοποιεί ο χρήστης είναι χαμηλότερη από αυτή του Access Point.

Καταλήγοντας, το πρόβλημα συνύπαρξης του Zigbee ή αλλιώς η κοινή χρήση του φάσματος από μη συντονισμένα συστήματα είναι ένα μεγάλο πρόβλημα που πρέπει να μελετηθεί σε ικανοποιητικό βαθμό για να εξάγουμε κάποια αποτελέσματα που θα μας βοηθήσει να προτείνουμε τις κατάλληλες λύσεις, που θα επιλύσουν ή έστω να ελαχιστοποιήσουν το πρόβλημα αυτό.



Σχήμα 2.7: Τα κανάλια του Zigbee και WiFi που επικαλύπτονται στην Ευρώπη

Κεφάλαιο 3

Μηχανισμοί αντιμετώπισης παρεμβολών

3.1 Προτεινόμενοι μηχανισμοί για μείωση των παρεμβολών

Η επίλυση του προβλήματος της συνύπαρξης στο φάσμα 2.4GHz αποτελεί μια πρόκληση που χρειάζεται προσεκτική μελέτη και για αυτό το λόγο πολλοί ερευνητές έχουν προσεγγίσει διάφορους τρόπους για μείωση της παρεμβολής που δημιουργείται. Πιο κάτω περιγράφουμε τις λύσεις που αφορούν το πρότυπο IEEE 802.15.4, το Zigbee και το WiFi.

3.1.1 Μηχανισμοί συνύπαρξης στο πρότυπο IEEE 802.15.4

Στις προδιαγραφές του προτύπου IEEE 802.15.4 υλοποιείται το DSSS ως μια τεχνική που επιτρέπει την συνύπαρξη με άλλες τεχνολογίες. Αυτή η τεχνική μεταδίδει το σήμα σε περισσότερες συχνότητες από αυτές που χρειάζεται, αλλά χρησιμοποιώντας λιγότερη ισχύ για κάθε συχνότητα. Ακόμα ένας μηχανισμός αυτού του προτύπου που αυξάνει τις πιθανότητες για συνύπαρξη χωρίς προβλήματα είναι το γνωστό Frequency Division Multiple Access (FDMA) το οποίο μοιράζει το φάσμα του 2.4 GHz σε 16 κανάλια που διαχωρίζονται με διάστημα 5 MHz μεταξύ τους και από αυτά τα μόνο τα 15,16,21 και 22 δεν επικαλύπτονται από τα κανάλια του WiFi στην Ευρώπη. Παρόλον ότι υπάρχουν αυτές οι μέθοδοι για καλύτερη συνύπαρξη, μια συσκευή Zigbee μπορεί να έχει πρόβλημα παρεμβολής και ως εκ τούτου μια νέα προσέγγιση από το IEEE 802.15.4 είναι το CSMA/CA. Η προσέγγιση αυτή δουλεύει παρόμοια με το CSMA/CD με τη διαφορά ότι η συσκευή «ακούει το μέσο» πριν να ξεκινήσει την μετάδοση των δεδομένων. Ακόμη, υποστηρίζεται το Time Division Multiple Access (TDMA) που ελέγχει την πρόσβαση στο δίκτυο και μοιράζει τον χρόνο σε slots. Με αυτό τον τρόπο, αποφεύγονται οι συγκρούσεις, κυρίως σε δίκτυα μόνο με συσκευές Zigbee, και με την μετάδοση των δεδομένων με ψηλό ρυθμό μετάδοσης (250 Kbps στα 2.4 GHz) μειώνουμε την πιθανότητα για συγκρούσεις, αφού όσο πιο ψηλό ρυθμό μετάδοσης έχουμε σε ένα κανάλι, τόσο πιο μικρό χρόνο χρησιμοποιούμε το κανάλι και άρα έχουμε μικρότερη πιθανότητα να γίνει μια σύγκρουση. Αυτό όμως δεν ισχύει όταν σε ένα ετερογενές δίκτυο συνυπάρχουν συσκευές Zigbee και WiFi, αφού το πρότυπο IEEE 802.11g χρησιμοποιεί την ίδια τεχνική CSMA/CA για να στείλουν δεδομένα και άρα το WiFi δεν θα ακούσει το Zigbee, αφού η ισχύς του όπως είπαμε είναι πολύ μεγαλύτερη.

3.1.2 Μηχανισμοί συνύπαρξης στο Zigbee

Υπάρχουν δύο προσεγγίσεις που σχετίζονται με τη βελτίωση της απόδοσης στα δίκτυα Zigbee όταν συνυπάρχουν με άλλα δίκτυα: οι συνεργατικές μέθοδοι (βασίζονται κυρίως στο πεδίο του χρόνου) και οι μη συνεργατικές (βασίζονται κυρίως στο πεδίο του φάσματος). Στις συνεργατικές μεθόδους, ορισμένες λειτουργίες του δικτύου Zigbee και των άλλων δικτύων, όπως του WiFi, συνεργάζονται με σκοπό να βελτιωθεί η απόδοσή τους όταν συνυπάρχουν. Όταν, για παράδειγμα, ένα δίκτυο με συσκευές Zigbee και WiFi είναι συγχρονισμένο, τότε όταν το ένα δίκτυο είναι ενεργό, το άλλο παραμένει ανενεργό έτσι ώστε να αποφεύγονται οι συγκρούσεις μεταξύ τους. Σε αυτή τη μέθοδο της συνεργασίας πρέπει να υπάρχει επικοινωνία μεταξύ των δικτύων των διαφορετικών τεχνολογιών, έτσι ώστε να μπορούμε να χειριζόμαστε αυτό τον συγχρονισμό. Από την άλλη, οι μη συνεργατικές μέθοδοι είναι απλά κάποιες διαδικασίες, όπου οι συσκευές Zigbee μπορούν να ακολουθήσουν με σκοπό να βελτιωθεί η απόδοσή του δικτύου χωρίς όμως να γνωρίζει τι υπάρχει σε κοντινή απόσταση και ποιες άλλες συσκευές κάνουν παρεμβολές. Γενικά, αυτές οι διαδικασίες βασίζονται στον έλεγχο και στον εντοπισμό των παρεμβολών, στη συχνότητα που λειτουργούν, έτσι ώστε να τις αποφεύγει όσο γίνεται περισσότερο. Πιο κάτω θα επικεντρωθούμε στις μη συνεργατικές μεθόδους, αφού οι συνεργατικές απαιτούν πιο πολύπλοκες υλοποιήσεις.

- <u>Συνεργατικές τεχνικές συνύπαρξης:</u>
  Οι προτάσεις που έχουμε σε αυτή την κατηγορία των τεχνικών συνήθως απαιτεί την ύπαρξη συντονισμού και συνεργασίας μεταξύ του θύματος και αυτού που προκαλεί την παρεμβολή. Μερικοί ερευνητές που έχουν ασχοληθεί με τις τεχνικές αυτές προτείνουν την υλοποίηση χρονικών διαστημάτων, όπως στο TDMA, όπου η κάθε τεχνολογία θα μπορεί να χρησιμοποιεί αυτό τον χρόνο για την ανταλλαγή δεδομένων [6,7,8,16]. Επίσης, μια παρόμοια υλοποίηση είναι να γίνεται έλεγχος της κίνησης των πακέτων,

δηλαδή αν αφήνουμε ένα μεγάλο χρονικό διάστημα μεταξύ διαδοχικών πακέτων, μειώνουμε την πιθανότητα σύγκρουσης στη διάσταση του χρόνου. Μια άλλη προσέγγιση που έχει προταθεί είναι να εντοπίζουμε το κανάλι του Zigbee που υπάρχει ελάχιστη παρεμβολή από το WiFi και να μην επιτρέπεται στο WiFi να χρησιμοποιήσει αυτό το κανάλι κατά την διάρκεια της χρήσης του από το Zigbee. Αυτές οι προσεγγίσεις που περιγράψαμε είναι μερικές που έχουν προταθεί από την ερευνητική κοινότητα, αλλά θεωρούμε πως δεν είναι πρακτικές, λόγω της ανάγκης για αλλαγές στις προδιαγραφές των τεχνολογιών που εξετάζουμε.

- Μη συνεργατικές τεχνικές συνύπαρξης:
  Σε αυτή την κατηγορία των τεχνικών συνύπαρξης περιλαμβάνονται τεχνικές που εστιάζονται στο πεδίο των συχνοτήτων, όπως το CSMA/CA που ενσωματώνεται όπως είπαμε στο πρότυπο IEEE 802.15.4, καθώς και άλλες μέθοδοι, όπως ο δυναμικός έλεγχος της ισχύος, οι οποίες μπορούν να προστεθούν στο σύστημα από τον χρήστη. Μερικές από τις πιο γνωστές τεχνικές, εκτός από το CSMA/CA που ήδη έχουμε εξηγήσει, είναι:

  1) *Εξαιρετικά χαμηλή συχνότητα χρήσης:* Αυτός είναι και ο πιο σημαντικός λόγος που οι συσκευές ZigBee έχουν μεγάλη διάρκεια μπαταρίας. Για παράδειγμα, μια συσκευή μπορεί να ενεργοποιείται κάθε ένα λεπτό, να εκτελεί το CCA και να μεταδίδει τα δεδομένα με αποτέλεσμα αυτή η συχνότητα χρήσης να είναι γύρω στο 0.01%. Αυτός ο κύκλος εργασιών ουσιαστικά επιτρέπει στους κόμβους ZigBee να δημιουργούν πολύ μικρή παρεμβολή στους υπόλοιπους κόμβους, και αν λάβουμε υπόψη μας ότι χρειάζεται μόνο μερικά χιλιοστά του δευτερολέπτου για να εκτελέσει το CCA και να στείλει τα πακέτα, τότε αν το άλλο δίκτυο έχει συχνές περιόδους αδράνειας, θα επιτρέψει στο Zigbee να εκμεταλλευτεί αυτό το διάστημα για να ανταλλάξει δεδομένα.

  2) *Εξάπλωση του σήματος:* Όπως ήδη έχουμε αναφέρει, η μέθοδος εξάπλωσης του σήματος DSSS επιτρέπει στο σήμα μας να έχει το πλεονέκτημα του processing gain[1] σε σχέση με τον παρεμβολέα που βρίσκεται στην ίδια συχνότητα. Έτσι, η εξάπλωση του σήματος βελτιώνει την ευρωστία του δικτύου απέναντι στις παρεμβολές, ενώ από την άλλη μεριά, μπορεί να μειώσει την παρεμβολή που προκαλείται από το Zigbee δίκτυο σε άλλα δίκτυα. Η συνολική ενέργεια του

[1] Είναι η ιδιότητα της αύξησης της τάσης του σήματος μετά την εξάπλωση του.

σήματος με την εξάπλωση δεν αλλάζει, αλλά όταν η ίδια ενέργεια κατανέμεται σε ένα μεγάλο εύρος ζώνης, η ενέργεια του σήματος ανά μονάδα Hertz μειώνεται.

3) *Δυναμική προσαρμογή της ισχύος:* Μια άλλη μέθοδος που μπορεί να βελτιώσει την συνύπαρξη του Zigbee είναι να προσαρμόζεται η ισχύς του πομπού ανάλογα με τις συνθήκες στο κανάλι και της σχετικής απόστασης που βρίσκονται οι υπόλοιποι κόμβοι. Γενικά, η ισχύς που λειτουργεί το Zigbee είναι σε χαμηλά επίπεδα, αλλά παράλληλα ικανοποιητική για να υπάρχει μια αξιόπιστη επικοινωνία με τους κόμβους. Με το να μειώσουμε την ισχύ μετάδοσης του σήματος, μειώνουμε την παρεμβολή που προκαλούμε στις γειτονικές συσκευές, ενώ από την άλλη, ο παραλήπτης γίνεται πιο ευάλωτος σε παρεμβολές. Αν όμως παρατηρούμε ότι γίνονται πολλές προσπάθειες αποστολής των πακέτων χωρίς επιτυχία, τότε αυξάνουμε την ισχύ για να βελτιώσουμε το SIR με αποτέλεσμα την αύξηση της πιθανότητας επιτυχούς επικοινωνίας με τους κόμβους, παράλληλα με την αύξηση της παρεμβολής στα γειτονικά δίκτυα.

4) *Αλλαγή συχνότητας λειτουργίας:* Αλλάζοντας την συχνότητα του καναλιού που λειτουργεί το Zigbee όταν παρατηρείται μεγάλη ενέργεια από ανεπιθύμητα σήματα, είναι μια απλή μέθοδος για να αποφύγουμε τις παρεμβολές. Συγκεκριμένα, σύμφωνα με τις προδιαγραφές του ZigBee Pro, παρέχεται ο αλγόριθμος “Frequency Agility” που επιτρέπει την αλλαγή του καναλιού όταν υπάρχει παρεμβολή στο δίκτυο. Τον αλγόριθμο τον περιγράφουμε στο επόμενο υποκεφάλαιο. Ακόμα και αν δεν περιλαμβάνεται σε ένα Zigbee δίκτυο η τεχνική αυτή, υπάρχει δυνατότητα της δυναμικής αλλαγής του καναλιού λειτουργίας σε κανάλια που δεν χρησιμοποιούνται από άλλα δίκτυα. Αυτή η περίπτωση είναι με την συνύπαρξη του WiFi και Zigbee όπου γνωρίζουμε πως τα κανάλια 15,16,21 και 22 δεν επηρεάζονται από το WiFi και άρα μπορούμε να τα επιλέξουμε για να ελαχιστοποιήσουμε τις παρεμβολές. Αυτή η τεχνική είναι γνωστή ως ευθυγράμμιση των καναλιών.

5) *Προσαρμογή του μεγέθους του πακέτου:* Μια τελευταία μέθοδος που μπορεί να χρησιμοποιηθεί στα δίκτυα Zigbee είναι η προσαρμογή του μεγέθους του πακέτου αναλόγως των συνθηκών που επικρατούν στο κανάλι. Μειώνοντας το μέγεθος του πακέτου έχει ως αποτέλεσμα την βελτίωση του Packet Error Rate

(PER) όταν υπάρχουν παρεμβολές. Παρ' όλα αυτά, αν και υπάρχει αντίληψη πως όταν έχουμε μικρότερα πακέτα σημαίνει υπάρχει μεγαλύτερη πιθανότητα να φτάσει το πακέτο στον προορισμό του πριν εμφανιστεί κάποια παρεμβολή, σε συγκεκριμένα πειράματα που διεξήχθησαν, έχουν δείξει πως αυτή η τεχνική δεν βελτιώνει το PER πάντα.

3.1.3 Μηχανισμοί συνύπαρξης στο WiFi

Οι μηχανισμοί του IEEE 802.11g για συνύπαρξη με άλλες τεχνολογίες αφορούν το πεδίο των συχνοτήτων και το πεδίον του χώρου. Όπως έχουμε περιγράψει σε προηγούμενο κεφάλαιο, τα κανάλια που χρησιμοποιούνται κυρίως από το WiFi γιατί δεν έχουν επικάλυψη μεταξύ τους είναι τα 1,6,11 στην Αμερική και τα 1,7,13 στην Ευρώπη. Συνήθως, αναθέτουμε ένα κανάλι από αυτά στο Access Point (AP) και αυτό δεν αλλάζει, εκτός αν εμείς το αλλάξουμε χειροκίνητα. Μια λύση σχετικά με την ανάθεση των καναλιών (πεδίο συχνοτήτων) θα ήταν αν το AP από μόνο του αποφάσιζε δυναμικά ποιο κανάλι να επιλέξει σε οποιαδήποτε χρονική στιγμή. Η απόφαση για αλλαγή του καναλιού θα βασίζεται στο επίπεδο της παρεμβολής και του θορύβου στο κανάλι, έτσι ώστε όταν εντοπίζει ψηλά επίπεδα παρεμβολής να επιλέγει ένα κανάλι χωρίς θόρυβο. Επίσης, η πολυδιαδρομική διάδοση και το Inter-Symbol interference μπορούν να χρησιμοποιηθούν ως μετρικές για την απόφαση αλλαγής του καναλιού.

Σχετικά με το πεδίο του χώρου, μια προσέγγιση αφορά την προσαρμογή της ισχύος που μεταδίδει το σήμα το AP, έτσι ώστε να είναι πάντα στα χαμηλότερα επίπεδα με σκοπό την ελαχιστοποίηση της παρεμβολής που προκαλείται στα άλλα δίκτυα. Τέλος, μια παρόμοια μέθοδος είναι η δυναμική διάσπαση του πακέτου σε μικρότερα κομμάτια, τα οποία θα βοηθήσουν στην μείωση της παρεμβολής. Ο λόγος είναι ότι το μέγεθος των πακέτων του WiFi δεν χρειάζεται να είναι πάντα το μέγιστο σε κάθε μετάδοση και έτσι όταν έχουμε μικρότερα πακέτα, τα δεδομένα που χρειάζονται να ξαναστείλουμε, όταν αποτύχει η αρχική προσπάθεια αποστολής, θα είναι λιγότερα. Αυτοί οι δυναμικοί αλγόριθμοι μαζί με επιπλέον τρόπους μείωσης των παρεμβολών θα μελετηθούν στο επόμενο κεφάλαιο του Radio Resource Management (RRM).

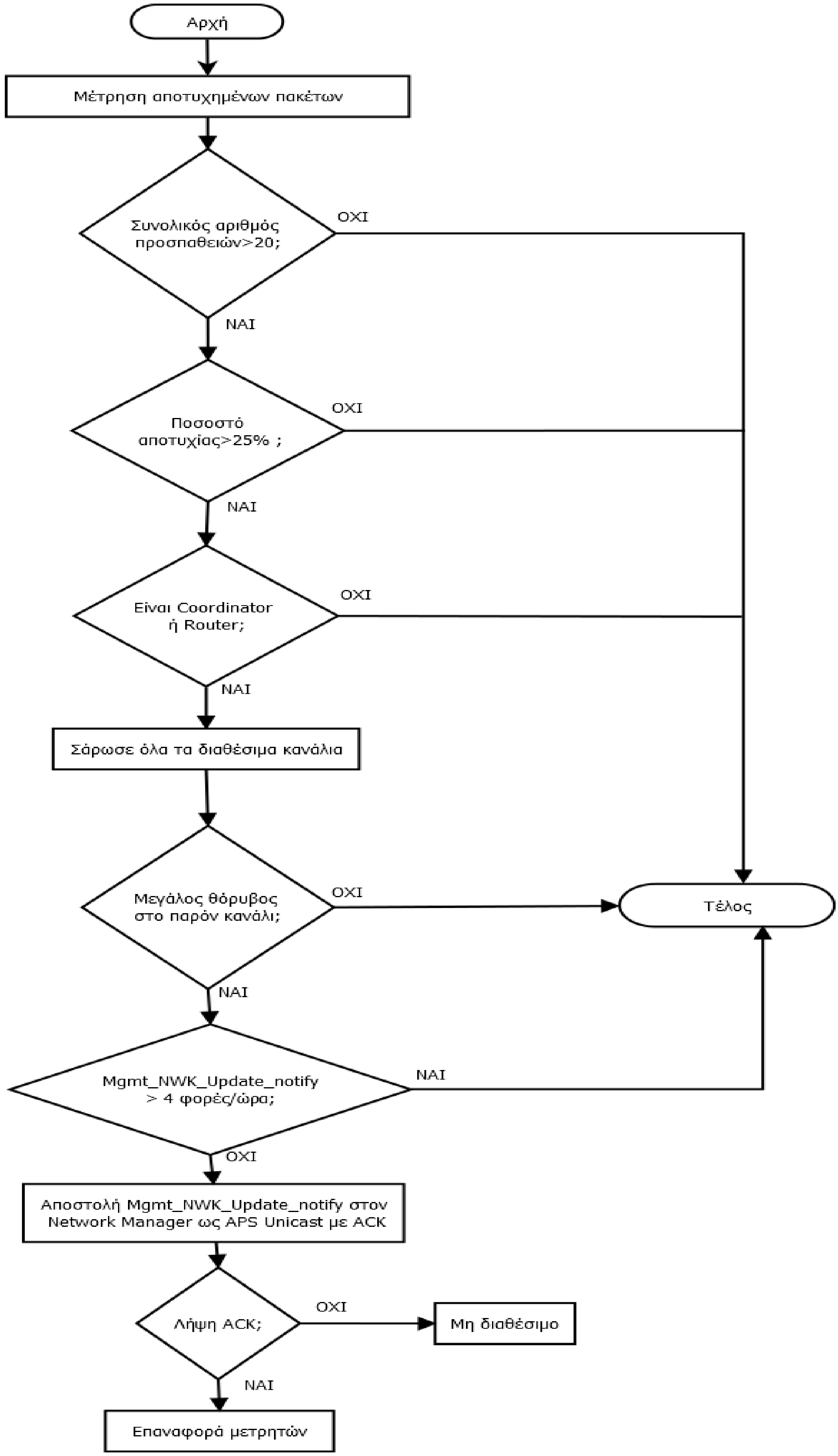
3.2 Zigbee: Αλγόριθμος Frequency agility

Μέχρι τώρα έχουμε μελετήσει τους τρόπους με τους οποίους οι τεχνολογίες του Zigbee και WiFi προσπαθούν να βελτιώσουν την ευρωστία των δικτύων τους. Εξαιτίας, όμως, των μειονεκτημάτων των μεθόδων που είδαμε μέχρι τώρα και ότι η ισχύς του WiFi είναι μεγαλύτερη από του Zigbee, με αποτέλεσμα όταν στέλνει δεδομένα το Zigbee τότε το WiFi δεν το «ακούει», χρειαζόμαστε μια καλύτερη λύση στο πρόβλημα. Για τον λόγο αυτό, μια νέα τεχνική που ονομάζεται Frequency Agility ορίζεται στις προδιαγραφές του Zigbee 2007. Ο συγκεκριμένος αλγόριθμος αποτελεί την πιο πρόσφατη πρόταση από την Zigbee Alliance και έχει σκοπό να επιλύσει το πρόβλημα των παρεμβολών, με το να αλλάξει το κανάλι που λειτουργεί το δίκτυο Zigbee σε ένα νέο κανάλι, όταν υπάρχει σοβαρό πρόβλημα παρεμβολής.

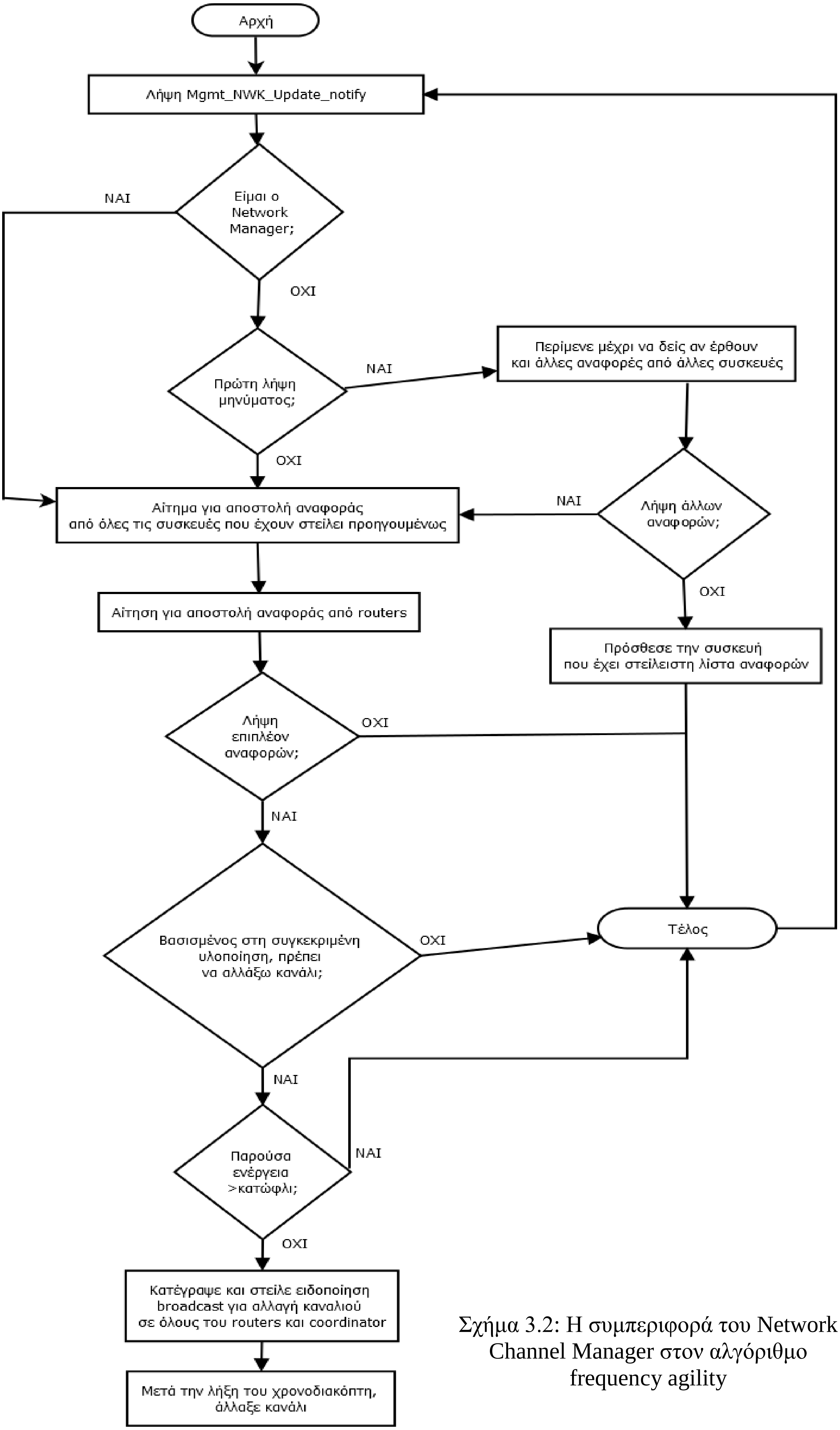
3.2.1 Περιγραφή αλγορίθμου

Το Zigbee όταν λειτουργεί στο φάσμα 2.4 GHz, όπως είπαμε, έχει στη διαθεσιμότητα του 16 κανάλια για να επιλέξει ώστε να λειτουργήσει το δίκτυο. Ως εκ τούτου, μια βέλτιστη πιθανή λύση είναι να μετακινήσουμε ολόκληρο το δίκτυο σε ένα κανάλι που δεν έχει υπάρχει παρεμβολή, ώστε να αποφύγουμε τελείως την παρεμβολή. Για να αλλάξει όμως κανάλι λειτουργίας, είτε θα είναι λόγω κάποιων κανονισμών όπως σε ένα νοσοκομείο που απαγορεύονται ορισμένα κανάλια για προστασία των WLAN, είτε λόγω παρεμβολής που παρατηρείται στο υφιστάμενο κανάλι. Ο αλγόριθμος Frequency Agility και ο οποίος περιγράφεται στις προδιαγραφές του Zigbee 2007 αφορά κυρίως την αλλαγή καναλιού λόγω μεγάλου θορύβου στο κανάλι. Σε αυτό το σημείο πρέπει να τονίσουμε πώς ο αλγόριθμος αυτός είναι εντελώς διαφορετικός από το Frequency Hopping που χρησιμοποιεί το Bluetooth. Συγκεκριμένα, ο αλγόριθμος αναφέρει ότι σε περίπτωση που εντοπιστεί κάποιο είδος παρεμβολής στο δίκτυο, οι συσκευές μπορούν να σαρώσουν τα διαθέσιμα κανάλια έτσι ώστε να βρουν ένα κατάλληλο κανάλι για να μετακινηθεί ολόκληρο το δίκτυο. Η διαδικασία αυτή γίνεται με τον συντονισμό του Network Manager.

Σύμφωνα με τις προδιαγραφές του Zigbee, στον αλγόριθμο πρέπει να υπάρχει ένας συντονιστής που ονομάζεται Network Channel Manager, ο οποίος σε περίπτωση που υπάρχει παρεμβολή, θα έχει ως ρόλο να λάβει τις αναφορές από όλους τους κόμβους του δικτύου και να αλλάξει το κανάλι λειτουργίας όταν το κρίνει απαραίτητο. Συνήθως, αυτός ο συντονιστής είναι Zigbee Coordinator του δικτύου, όμως μπορεί να γίνει κάποιος άλλος κόμβος με το να στείλει μία ενημέρωση Mgmt_NWK_Update_req στους κόμβους. Κατά την διάρκεια της εκτέλεσης του Frequency Agility, ο Zigbee Coordinator και κάθε router έχουν την ευθύνη για να μετρούν τον αριθμό των αποτυχιών μετάδοσης των πακέτων και τον αριθμό των συνολικών μεταδόσεων. Πιο κάτω φαίνεται το λογικό διάγραμμα του αλγόριθμου καθώς και τα κριτήρια που χρησιμοποιεί ο Network Manager για να αποφασίσει αν θα γίνει μια αλλαγή καναλιού.



Σχήμα 3.1: Λογικό διάγραμμα αλγόριθμου frequency agility



Σχήμα 3.2: Η συμπεριφορά του Network Channel Manager στον αλγόριθμο frequency agility

Όπως βλέπουμε στο Σχήμα 3.1, οι routers καταμετρούν όλα τα αποτυχημένα πακέτα και αν αυτός ο αριθμός ξεπεράσει ένα συγκεκριμένο κατώφλι τότε ο Coordinator και οι routers θα σαρώσουν όλα τα διαθέσιμα κανάλια και θα αποστείλουν μια αναφορά με τις ενέργειες που υπάρχουν σε κάθε κανάλι στον Network Manager, μέσω ενός πακέτου Mgmt_NWK_Update_notify. Αυτό θα γίνει μόνο 4 φορές την ώρα, δηλαδή κάθε 15 λεπτά, έτσι ώστε να μην πλημμυρίσει το δίκτυο από αναφορές. Όταν ο Network Manager παραλάβει αυτή την ειδοποίηση (Σχήμα 3.2), θα ζητήσει να παραλάβει και άλλες αναφορές και θα αποφασίσει με κάποιους μηχανισμούς αν πρέπει να αλλάξει κανάλι σε ολόκληρο το δίκτυο ή όχι. Εάν αποφασίσει να γίνει αλλαγή καναλιού, θα στείλει μια ειδοποίηση Mgmt_NWK_Update_req σε όλους τους κόμβους για να γνωρίζουν για την αλλαγή του καναλιού και θα επιλέξει το νέο κανάλι που θα λειτουργεί το δίκτυο. Όσες συσκευές «κοιμούνται» θα ψάξουν ξανά για το δίκτυο όταν ξυπνήσουν έτσι ώστε να κάνουν join. Η αλλαγή του καναλιού μπορεί να γίνει αρκετά γρήγορα, αφού μόλις πάρουν όλοι οι κόμβοι το μήνυμα της αλλαγής, θα αλλάξουν κανάλι και αυτό διαρκεί συνήθως 500 με 800 ms, άρα σε ένα μεγάλο δίκτυο με 2000 κόμβους αυτό μπορεί να γίνει σε 10 δευτερόλεπτα περίπου.

Μέσα από την περιγραφή του αλγόριθμου βλέπουμε πως με μια απλή υλοποίηση μπορούμε να βελτιώσουμε την απόδοση του δικτύου Zigbee όταν βρίσκεται σε ένα κανάλι με παρεμβολές, απλά με την αλλαγή του καναλιού λειτουργίας του δικτύου. Μια μελέτη που έχει γίνει σχετικά με τον συγκεκριμένο αλγόριθμο του ZigBee [13] σε ένα σπίτι έχει δείξει πως, ο μηχανισμός αυτός μπορεί να αποφύγει την παρεμβολή που προκαλείται από τις συσκευές WiFi και να βελτιωθεί απόδοση του δικτύου του ZigBee. Παρόλα αυτά, στο σενάριο που όλα τα κανάλια είναι κρατημένα από το WiFi, ο μηχανισμός δεν είναι τόσο αποδοτικός όσο πρέπει. Επίσης, τονίζει πως ο χρόνος απόκρισης του αλγόριθμου για να αλλάξει το κανάλι εξαρτάται από το Packet-Error-Rate (PER) και τον αριθμό των πακέτων που στέλνουμε. Έτσι, βάζοντας αυτά τα κατώφλια σε χαμηλές τιμές, θα μειώσουμε τον χρόνο που χρειάζεται για να αλλάξουμε κανάλι, αλλά θα αυξήσουμε το signaling overhead.

3.2.2 Ανοικτά ζητήματα

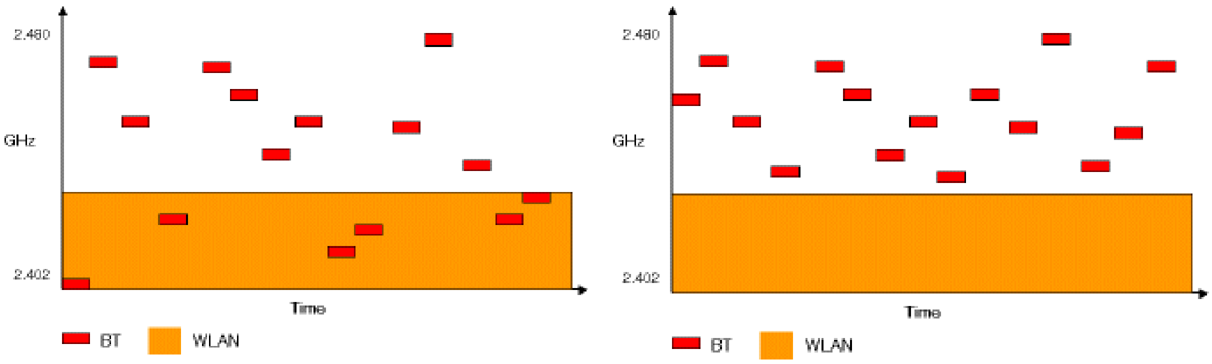
Καταληκτικά, παρατηρούμε πως ο αλγόριθμος έχει κάποια σημεία που χρειάζεται να προσέξουμε καθώς τον μελετούμε. Το πρώτο σημείο σχετίζεται με τις αναφορές που πρέπει να στέλνουν οι κόμβοι και συγκεκριμένα δεν γίνεται ξεκάθαρο τι ακριβώς πρέπει περιλαμβάνει η αναφορά αυτή, και πόσο συχνά πρέπει να στέλνεται. Με άλλα λόγια, η μόνη πληροφορία που στέλνεται είναι η ενέργεια των καναλιών και αυτό γίνεται κάθε 15 λεπτά. Μέσα σε αυτό τον χρόνο, όμως, μπορεί η κατάσταση στο κανάλι να βελτιωθεί και έτσι να μην χρειάζεται να γίνει κάποια αλλαγή. Το δεύτερο σημείο αφορά την επιλογή του καναλιού και με βάση ποια κριτήρια γίνεται και πόση είναι η καθυστέρηση για να γίνει η αλλαγή. Με άλλα λόγια, αν το κανάλι που επιλέγεται είναι πάντα αυτό που έχει την λιγότερη ενέργεια τότε μπορεί να υπάρχει περίπτωση να επιλεγεί ένα κανάλι που έχει επικάλυψη με το WiFi την στιγμή που δεν είναι μεταφέρονται δεδομένα και να θεωρείται πως αυτό το κανάλι είναι το καλύτερο. Ακόμη, αν και είδαμε μέσω μιας μελέτης κάποια πειράματα σχετικά με τον χρόνο που χρειάζεται για να γίνει η αλλαγή , αυτό δεν αποτελεί κανόνα και γι' αυτό χρειάζεται περισσότερη μελέτη για να προσδιορίσουμε τους χρόνους καθυστέρησης καθώς και τα κριτήρια για την επιλογή του κατάλληλου καναλιού.

3.3 Bluetooth: Adaptive Frequency Hopping Spread Spectrum

Παρόλο που στην εργασία αυτή ασχολούμαστε κυρίως με τα προβλήματα και τις πιθανές λύσεις στην συνύπαρξη του Zigbee και WiFi, αξίζει να αναφέρουμε λίγα λόγια για το πρόβλημα που αντιμετωπίζει η τεχνολογία Bluetooth όταν λειτουργεί μαζί με το WiFi και με ποιο τρόπο μπορούμε να μειώσουμε τις παρεμβολές [18]. Εξαιτίας της κοινής χρήσης του φάσματος 2.4 GHz και λόγω της μεθόδου FHSS που χρησιμοποιεί το Bluetooth για αποστολή των δεδομένων και του DSSS ή OFDM από το IEEE 802.111b/g, παρουσιάζεται μείωση στην απόδοση των συστημάτων όταν στέλνουν στην ίδια συχνότητα την ίδια χρονική στιγμή, αλλά το μέγεθος του προβλήματος εξαρτάται από τον όγκο των δεδομένων που μεταφέρονται, από την ισχύ των συσκευών και από τον ρυθμό μετάδοσης του WiFi. Το πρόβλημα της συνύπαρξης έχει απασχολήσει την βιομηχανία για μεγάλο χρονικό διάστημα και γι' αυτό δημιουργήθηκαν το IEEE 802.15.2 Coexistence Task Group από την IEEE και το Bluetooth Special Interest Group (SIG) με σκοπό να μελετήσουν το πρόβλημα και να προτείνουν ένα μοντέλο όπου θα συνυπήρχαν χωρίς προβλήματα οι δύο τεχνολογίες στο φάσμα ISM 2.4 GHz.

3.3.1 Περιγραφή αλγορίθμου

Οι προτεινόμενες τεχνικές που παρουσιάστηκαν χωρίζονται σε συνεργατικές και μη-συνεργατικές τεχνικές. Οι συνεργατικές τεχνικές, όπως και στο Zigbee, απαιτούν επικοινωνία μεταξύ των τεχνολογιών ενώ οι μη-συνεργατικές τεχνικές δεν απαιτούν κάποιο συγχρονισμό. Η πιο σημαντική τεχνική που θα μιλήσουμε είναι το Adaptive Frequency Hopping Spread Spectrum (AFHSS) και ήδη έχει υιοθετηθεί από την έκδοση 1.2 του Bluetooth από το 2003 [14]. Το AFHSS είναι μη-συνεργατική μέθοδος και χρησιμοποιεί τις μετρικές των packet ή frame error rate, την ισχύ του σήματος ή το Signal to Interference Ratio (υλοποιείται συνήθως ως Received Signal Strength Indication) για να ανιχνεύσει την παρουσία άλλων συσκευών στο φάσμα. Για παράδειγμα, αν έχουμε μια συσκευή Bluetooth, θα μπορεί να διατηρεί μια μέτρηση του frame error rate για κάθε συχνότητα που χρησιμοποιεί. Στη συνέχεια, αυτή η συσκευή θα μπορεί να βρει ποιες συχνότητες είναι κρατημένες από άλλους χρήστες και έτσι να προσαρμόσει το μοτίβο των συχνοτήτων που επιλέγει, ώστε να επιλέξει μόνο τις συχνότητες που είναι ελεύθερες και δεν προκαλούν προβλήματα παρεμβολής. Αυτή είναι και η μεγάλη διαφορά του AFHSS έναντι του FHSS, δηλαδή στο AFHSS η συσκευή μπορεί δυναμικά να αλλάξει το μοτίβο που επιλέγει τις συχνότητες με σκοπό να αποφύγει τα κανάλια που είναι κρατημένα (ή «κακά» κανάλια) και να επιλέξει μόνο τα κανάλια που είναι ελεύθερα (ή «καλά» κανάλια) και δεν έχουν παρεμβολές, ενώ στο FHSS υπάρχει μια σταθερή λίστα με συχνότητες που με ένα ψευδο-τυχαίο τρόπο επέλεγε η συσκευή τα κανάλια που θα αναπηδούσε το δίκτυο κάθε φορά. Ανάμεσα στις μη συνεργατικές μεθόδους, το AFHSS είναι αυτό που μεγιστοποιεί την χρήση του φάσματος οδηγώντας σε αύξηση του throughput του Bluetooth. Το μέγεθος της λίστας των καναλιών στο AFHSS, σύμφωνα με τις προδιαγραφές του Bluetooth, πρέπει να είναι τουλάχιστον 20 για να μπορεί να λειτουργεί σωστά η συσκευή, ενώ στο FHSS είχαμε μια σταθερή λίστα από 79 κανάλια που έπρεπε να επισκεφθεί τουλάχιστον μια φορά η συσκευή. Πιο κάτω βλέπουμε την συμπεριφορά του Bluetooth με την τεχνική FHSS όπου τυχαία χρησιμοποιεί τα κανάλια και δίπλα την διαφορά με την νέα τεχνική AFHSSS που αποφεύγει τις παρεμβολές του WLAN.



Σχήμα 3.3: 1) Αριστερά: Συγκρούσεις με το WLAN από την τυχαία συμπεριφορά του FHSS, 2) Δεξιά: Αποφυγή συγκρούσεων με το WLAN χάρη στο AFHSS

3.3.2 Αποδοτικότητα αλγορίθμου

Όπως είναι ξεκάθαρο, ο μηχανισμός AFHSS αποφεύγει τα κατειλημμένα κανάλια από το WLAN και έτσι δεν επηρεάζεται η απόδοση του δικτύου. Γενικά, η μέθοδος αυτή φαίνεται να είναι αποδοτική όταν οι συσκευές που συνυπάρχουν στο ίδιο φάσμα χρησιμοποιούν διαρκώς το ίδιο κομμάτι συχνοτήτων. Αυτό όμως μπορεί να μην ισχύει όταν ο αριθμός των συσκευών που παρεμβάλλουν αυξάνεται σε μια συγκεκριμένη γεωγραφική περιοχή γιατί αυτό θα οδηγήσει σε αφαίρεση ακόμη περισσότερων καναλιών από τη λίστα του frequency hopping μοτίβου και έτσι οι συσκευές θα χρησιμοποιούν για περισσότερο χρόνο τα κανάλια αυξάνοντας, παράλληλα, την πιθανότητα να έχουμε συγκρούσεις με άλλες συσκευές και άρα την μείωση της απόδοσης. Επίσης, αν η πηγή της παρεμβολής αλλάζει δυναμικά κανάλι, όπως το frequency hopping, η τεχνική AFHSS δεν βελτιώνει την κατάσταση, γι' αυτό το λόγο χρειάζεται μια άλλη προσέγγιση όπου όλα τα κανάλια, «καλά» και «κακά», αξιολογούνται με μια πιθανότητα ώστε να χρησιμοποιηθούν ανάλογα με την κατάσταση τους. Έτσι, ο αλγόριθμος θα επιλέγει τα κανάλια που έχουν μεγαλύτερη πιθανότητα για να τα χρησιμοποιήσει.

Επιπρόσθετα, για περαιτέρω βελτίωση της αντοχής του δικτύου έναντι των παρεμβολών που προκαλούν οι τεχνολογίες, όπως το WiFi, που χρησιμοποιούν στατικά κανάλια, το AFHSS απαιτεί από τις συσκευές Bluetooth να χρησιμοποιούν την μέθοδο του ίδιου καναλιού (same channel communication). Υπό κανονικές συνθήκες, σε ένα δίκτυο Bluetooth οι συσκευές slaves επικοινωνούν χρησιμοποιώντας διαφορετική συχνότητα από αυτή του master. Αυτό όμως στην τεχνική AFHSS αλλάζει, αφού απαιτεί από τον master και τις συσκευές slaves να επικοινωνούν χρησιμοποιώντας το ίδιο κανάλι. Ο λόγος είναι για να αποφευχθούν περιπτώσεις όπου ο master μεταδίδει δεδομένα σε ένα «καλό» κανάλι ενώ ο slave ανταποκρίνεται σε ένα «κακό» κανάλι και έτσι θα είχαμε πολλές αποτυχημένες προσπάθειες για να σταλούν τα δεδομένα. Από την στιγμή που μεταδίδουν και οι δύο συσκευές στο ίδιο κανάλι, ο ρυθμός με τον οποίον αναπηδά κανάλια το Bluetooth μειώνεται κατά 50%, δηλαδή μόλις στις 800 φορές το δευτερόλεπτο από τις 1600 που είναι ο κανονικός ρυθμός. Αν και η μείωση αυτή θα οδηγούσε τις συσκευές Bluetooth να είναι πιο ευαίσθητες στις παρεμβολές από άλλες Bluetooth συσκευές, το πλεονέκτημα που παρατηρούμε στη συνολική απόδοση του δικτύου υπερτερεί κατά πολύ έναντι του μειονεκτήματος.

Καταλήγοντας, διαπιστώνουμε πώς ο αλγόριθμος του AFHSS μπορεί να βελτιώσει την απόδοση του συστήματος όταν βρίσκεται σε μια περιοχή που επικρατούν παρεμβολές από γειτονικές συσκευές διαφορετικής τεχνολογίας. Μέσα από τις προδιαγραφές του Bluetooth παρατηρούμε ότι προτείνεται η χρήση του PER και του RSSI για να ανιχνεύουν οι συσκευές τα «κακά» κανάλια και να τα αποφεύγουν. Εδώ αξίζει να επισημάνουμε πως αυτές οι μετρικές διαφέρουν στο πώς κρίνουν την κατάσταση του καναλιού καθώς από την μια μεριά το PER δεν είναι τόσο ακριβές όσο το RSSI στο συνεχή έλεγχο και επαναξιολόγηση ενός καναλιού, ενώ από την άλλη το RSSI καταναλώνει περισσότερη ενέργεια από το PER. Γι' αυτό τον λόγο πρέπει να υλοποιούμε την κατάλληλη τεχνική ανάλογα με τις συσκευές που έχουμε και τον σκοπό που προορίζονται.

Κεφάλαιο 4

Radio Resource Management στο Wireless LAN

4.1 Εισαγωγή στο Radio Resource Management (RRM)

Τα τελευταία χρόνια παρατηρείται μια ραγδαία εξάπλωση των ασύρματων τεχνολογιών IEEE802.11 WLAN ,αφού πλέον μπορούμε να τις βρούμε σε πολλούς χώρους όπως σε σπίτια, πανεπιστημιακούς χώρους και αεροδρόμια. Ο κύριος σκοπός της δημιουργίας του πρωτοκόλλου IEEE 802.11 ήταν η εγκατάσταση των ασύρματων δικτύων κυρίως σε σπίτια ή σε χώρους που υπάρχει μόνο ένα ασύρματο δίκτυο. Σε αυτά τα πλαίσια, η ρύθμιση ενός Accesss Point (AP) στο κατάλληλο κανάλι και με την κατάλληλη ισχύ ήταν μια τετριμμένη διαδικασία. Καθώς ,όμως, το κόστος αγοράς ενός Access Point (AP) συνεχώς μειώνεται, και όσο η ανάγκη για μεγαλύτερη κάλυψη των χρηστών αυξάνεται, όλο και περισσότερα APs εγκαθίστανται σε σχετικά μικρές αποστάσεις το ένα από το άλλο. Χάρις στην ιδιότητα του προτύπου IEEE 802.11 να επιτρέπει την κοινή χρήση του εύρους ζώνης (bandwidth), πολλές εφαρμογές τρέχουν πλέον από τις ασύρματες συσκευές και άρα οι πελάτες των εταιρειών χρειάζονται δίκτυα που να έχουν όλο και πιο πολλή χωρητικότητα για να υποστηρίζουν περισσότερους χρήστες.

Η αύξηση της χωρητικότητας σε ένα ασύρματο δίκτυο WLAN αποτελεί πρόβλημα σε αντίθεση με το ενσύρματο δίκτυο, όπου εκεί έχουμε την ευχέρεια να προσθέσουμε όσο bandwidth χρειαζόμαστε. Στα WLAN, για να προσθέσουμε χωρητικότητα χρειαζόμαστε επιπλέον AP, αλλά αν δεν τα ρυθμίσουμε προσεκτικά και με μεθοδικό τρόπο θα προκαλέσουμε μείωση της χωρητικότητας αντί αύξηση, λόγω παρεμβολών και άλλων παραγόντων. Δεδομένου τα πιο πάνω, στις μέρες μας η διαδικασία εγκατάστασης ενός ασύρματου δικτύου περιπλέκεται και απαιτεί προσεκτική μελέτη του χώρου και των ρυθμίσεων του κάθε AP γιατί, όπως έχουμε αναφέρει σε προηγούμενα κεφάλαια, έχουμε μόνο 3 μη επικαλυπτόμενα κανάλια για να αναθέσουμε στα APs και επειδή το σήμα μπορεί να ταξιδέψει μέσα από τοίχους και άλλα εμπόδια, το να σχεδιάσει κάποιος ένα ασύρματο δίκτυο WLAN οποιουδήποτε μεγέθους αποτελεί ένα δύσκολο εγχείρημα. Ακόμη και αν έχουμε μελετήσει τον χώρο προσεκτικά, το σήμα RF είναι συνεχώς μεταβαλλόμενο και έτσι αν θεωρούμε πως ένα κανάλι με μια συγκεκριμένη ισχύ είναι βέλτιστο την μια στιγμή, μπορεί να αποδειχθεί ότι δεν είναι καθόλου βέλτιστο στην επόμενη χρονική στιγμή. Πλέον, η εγκατάσταση δικτύων μεγάλης εμβέλειας που περιλαμβάνουν πολλά APs αποτελεί μια συνηθισμένη τακτική για τους διαχειριστές δικτύων και η σωστή RF ρύθμιση των APs αποτελεί μια πρόκληση για τους ίδιους, γιατί σε περιπτώσεις σφαλμάτων μπορεί να αυξήσουν το λειτουργικό κόστος του δικτύου. Επίσης, ο λάθος χειρισμός των ρυθμίσεων του δικτύου μπορεί να προκαλέσει προβλήματα στο WLAN όπως αστάθεια στο δίκτυο.

Λαμβάνοντας υπόψη τα πιο πάνω προβλήματα και το ότι οι παράγοντες που καθορίζουν το ασύρματο περιβάλλον, όπως η κίνηση των χρηστών και η διάδοση του σήματος, μεταβάλλονται, χρειαζόμαστε κάποιους μηχανισμούς που θα επιτρέπουν δυναμική και έξυπνη διαχείριση και βελτίωση των πόρων του δικτύου ανάμεσα στα APs. Η καλύτερη λύση στο πρόβλημα θα ήταν να παρέχουμε στους κόμβους που απαρτίζουν το δίκτυο την δυνατότητα να εντοπίζουν τις αλλαγές στο περιβάλλον και να προσαρμόζουν τις ρυθμίσεις τους αυτόματα. Αυτό μπορούμε να το πετύχουμε με την χρήση μιας πολιτικής Radio Resource Management (RRM) σε ένα WLAN η οποία θα παρακολουθεί διαρκώς την κατάσταση του δικτύου και θα βοηθά στην επίλυση των προβλημάτων που εμφανίζονται.

Με την συνεχιζόμενη εξάπλωση των ασύρματων συσκευών και των APs στην ίδια γεωγραφική περιοχή, συχνά διαφορετικά ασύρματα δίκτυα συνυπάρχουν στην ίδια περιοχή. Αυτά τα δίκτυα μπορεί να ανήκουν σε διαφορετικούς διαχειριστές και ως αποτέλεσμα, η εγκατάσταση ενός κεντρικού RRM μηχανισμού θα ήταν πολύ δύσκολη. Ο λόγος είναι διότι μια κεντρική προσέγγιση θα βασίζεται σε ένα κεντρικό κόμβο που θα ελέγχει και θα ρυθμίζει όλες τις συσκευές και των δύο δικτύων και άρα, χρειάζεται ένας κεντρικός διαχειριστής, πράγμα δύσκολο αν ο ένας δεν συμφωνεί να ελέγχεται το δίκτυο του από τον άλλο διαχειριστή. Παρόλα αυτά, σε αυτή την περίπτωση μπορούμε να χρησιμοποιήσουμε μια διαφορετική προσέγγιση όπου οι συσκευές στο κάθε δίκτυο έχουν αρκετή εξυπνάδα, έτσι ώστε να πάρουν τις κατάλληλες αποφάσεις. Αυτή είναι η κατανεμημένη προσέγγιση του RRM μηχανισμού και συνήθως αυτό εφαρμόζεται στις μέρες μας εξαιτίας της δυναμικής φύσης του περιβάλλοντος, όπου χρειάζεται γρήγορη προσαρμογή ανεξάρτητα από τον αριθμό των συσκευών που μοιράζονται το φάσμα και δεν μπορούμε να ελέγξουμε. Επίσης, η κατανεμημένη προσέγγιση βελτιώνει την ευρωστία του δικτύου γιατί μειώνεται η εξάρτηση από μια μοναδική συσκευή (single point of failure) και υπάρχει η δυνατότητα για γρήγορη ανταπόκριση, αφού οι συσκευές πλέον είναι αυτόνομες και αποφασίζουν από μόνες τους.

Σε πολλά δίκτυα, μια ειδική συσκευή που λέγεται controller ελέγχει τα APs και συνεργάζεται μαζί με αυτά καθώς και με άλλους controllers, που μπορεί να ανήκουν σε άλλο BSS, για να πάρει τις αποφάσεις που πρέπει για τις κατάλληλες ρυθμίσεις στο δίκτυο μας. Έτσι, ενεργοποιώντας τον μηχανισμό RRM στο δίκτυο μας, μπορούμε να έχουμε τα πιο κάτω πλεονεκτήματα με την χρήση του:

- Παρακολούθηση του δικτύου σε πραγματικό χρόνο: Ο controller παρέχει μετρήσεις όπως channel utilization, πιθανές παρεμβολές και πόσα κανάλια είναι διαθέσιμα έτσι ώστε να ενημερώνει τον διαχειριστή του δικτύου για τις συνθήκες του δικτύου.
- Κατανομή του φόρτου του δικτύου σε πραγματικό χρόνο (Load balancing): Υπάρχει δυνατότητα από τον controller να διατηρεί μια ισορροπία στον φόρτο εργασίας που έχουν τα APs, έτσι ώστε να διατηρείται η ομαλή λειτουργία του δικτύου.
- Δυναμική επιλογή συχνότητας λειτουργίας (Dynamic frequency selection): Ο controller επιλέγει αυτόματα τα κανάλια για τα APs ανάλογα με τις αλλαγές στο περιβάλλον.
- Έλεγχος ισχύος μετάδοσης (Transmit power control): Ο controller προσαρμόζει αυτόματα την ισχύ που εκπέμπει το κάθε AP με σκοπό να διατηρήσει την ακτίνα κάλυψης και την χωρητικότητα του δικτύου στα πλαίσια για τα οποία έχει σχεδιαστεί.
- Εντοπισμός και κάλυψη μαύρης τρύπας (blackhole): Όταν ένα AP παρουσιάσει κάποιο πρόβλημα και σταματήσει την λειτουργία του, αυτόματα ο controller αυξάνει την ισχύ των γειτονικών APs για να καλύψει την μαύρη τρύπα που εμφανίστηκε.
- Επεκτασιμότητα δικτύου: Όταν προσθέσουμε νέα APs στο δίκτυο, ο controller αυτόματα αναθέτει τα κατάλληλα κανάλια σε αυτά τα APs χωρίς να επηρεάζεται το υπόλοιπο δίκτυο.

- Αυτόματος εντοπισμός και αποφυγή παρεμβολών: Ο controller εντοπίζει αυτόματα και επιλύει το πρόβλημα της παρεμβολής από γειτονικά WLANs ή από συσκευές άλλων τεχνολογιών όπως το Bluetooth ή Zigbee.

4.1.1 Η ανάγκη για RRM στις επιχειρήσεις

Στη σημερινή εποχή που όλο και περισσότερες επιχειρήσεις προσπαθούν να κρατήσουν το QoS των χρηστών τους σε υψηλά επίπεδα, να προστατέψουν όσο περισσότερο γίνεται τα ασύρματα δίκτυα τους καθώς και να ικανοποιήσουν την ανάγκη των χρηστών για κινητικότητα, οδηγούνται στην υιοθέτηση του RRM στο δίκτυο τους για να μειώσουν το κόστος συντήρησης και την πολυπλοκότητα του δικτύου. Με το RRM η κάθε επιχείρηση αναζητά την διατήρηση της αξιοπιστίας στο δίκτυο της με τον όλο και αυξανόμενο αριθμό των κινητών συσκευών που τρέχουν κρίσιμες εφαρμογές καθώς και την αύξηση της παρεμβολής που προκαλείται από τις διάφορες συσκευές. Χωρίς την χρήση κάποια τεχνικής RRM, το δίκτυο μπορεί να έχει απρόβλεπτες συμπεριφορές όταν οι συσκευές και οι χρήστες είναι πολύ περισσότεροι από τον συνηθισμένο αριθμό με αποτέλεσμα να μειώνεται η απόδοση του, η αξιοπιστία του, να αυξάνονται τα λειτουργικά έξοδα καθώς επίσης και να αυξάνεται η πιθανότητα γενικού προβλήματος του δικτύου όταν δεν προσαρμόζεται στις ανάγκες των χρηστών. Για αυτούς τους λόγους, οι εταιρίες δαπανούν μεγάλα ποσά για την αγορά και εγκατάσταση ενός δικτύου που υποστηρίζει το RRM έτσι ώστε οι υπάλληλοι καθώς και οι πελάτες να μπορούν να δουλεύουν με ασφάλεια από οπουδήποτε ακόμα και σε πολυσύχναστα ή σε θορυβώδη περιβάλλοντα χωρίς να μειώνεται η απόδοση του συστήματος τους ακόμη και αν προκύψουν προβλήματα όπου κάποια APs σταματήσουν την κανονική λειτουργία τους.

Κάποια παραδείγματα επιχειρήσεων που χρησιμοποιούν την μέθοδο του RRM είναι: 1) Σε εκπαιδευτικά ιδρύματα η χρήση του RRM βοηθά στην υποστήριξη πολυσύχναστων περιβαλλόντων με την μείωση των παρεμβολών και άλλων προβλημάτων που προκαλούνται στο δίκτυο, 2) στα δίκτυα των νοσοκομείων μειώνεται η παρεμβολή των APs έτσι ώστε να υπάρχει αξιόπιστη πρόσβαση των συσκευών που πρέπει σε αρχεία ασθενών, κλινικές εικόνες και άλλα εργαλεία που χρειάζονται οι γιατροί, και 3) σε ξενοδοχειακές μονάδες χρησιμοποιείται για να υπάρχει μείωση της παρεμβολής καθώς και αξιόπιστη σύνδεση μεταξύ των πελατών σε περιοχές όπου μπορεί να γίνονται συνέδρια.

4.2 Το πρότυπο IEEE 802.11k

Η ομάδα TGk (Radio Resource Measurement) έχει δημιουργήσει το πρότυπο IEEE 802.11k [25] τον Δεκέμβριο 2008 και σύμφωνα με αυτό, το Radio Resource Measurement (RRM) προσπαθεί να επιλύσει κάποια προβλήματα στο φάσμα που λειτουργεί το WiFi με το να παρέχει κάποια γνώση στις συσκευές σχετικά με το περιβάλλον στο οποίο βρίσκονται, ώστε να βελτιωθεί η απόδοση και η αξιοπιστία του δικτύου. Αυτή η γνώση παρέχεται με κάποιες μετρήσεις που γίνονται στο περιβάλλον και για τον λόγο αυτό η ομάδα TGk καθόρισε αυτές τις μετρήσεις που θα μπορούν να διεκπεραιώνουν. Με αυτό τον τρόπο, τα ασύρματα δίκτυα γίνονται πιο αξιόπιστα, επεκτάσιμα και συντηρήσιμα μέσω των μετρήσεων που παρέχονται από τις συσκευές (clients) και οι οποίες έχουν την δυνατότητα να ανταλλάξουν αυτές τις μετρήσεις με τα Access Points (APs) στα οποία συνδέονται. Μεγάλες εταιρίες όπως η Cisco, Aruba, η Ruckus και άλλες βασίζονται σε αυτό το πρότυπο για να δημιουργήσουν δικούς τους μηχανισμούς, είτε σε λογισμικό, είτε με ειδικά μηχανήματα που λέγονται controllers, για να αναθέτουν τα κατάλληλα κανάλια και την ισχύ στα APs ώστε να γίνεται καλύτερη λειτουργία των δικτύων τους. Γενικά μιλώντας, οι νέες δυνατότητες που παρέχει το πρότυπο IEEE 802.11k είναι οι ακόλουθες:

• Η διεκπεραίωση μετρήσεων σε όλα τα κανάλια του φάσματος.

• Η αίτηση καθώς και η αναφορά για λήψη διάφορων μετρήσεων..

• Παροχή πληροφοριών για τα γειτονικά APs.

Οι διάφορες μετρήσεις που αναφέραμε μπορεί να γίνονται είτε στο κανάλι που λειτουργεί η συσκευή (ονομάζονται ταυτόχρονες μετρήσεις), είτε σε διαφορετικά κανάλια (ονομάζονται ειδικές μετρήσεις.). Στην τελευταία περίπτωση, επειδή η συσκευή (client) πρέπει να αποθηκεύσει την τωρινή σύνδεση με το BSS πριν να αλλάξει κανάλι, οι ειδικές μετρήσεις δεν πρέπει να γίνονται συχνά και μόνο για μικρές χρονικές περιόδους. Όσον αφορά τους χρήστες (clients), οι συσκευές τους μπορούν τα ζητήσουν αναφορές από το AP που είναι συνδεδεμένοι, ενώ τα APs μπορούν να ζητήσουν από κάποιο γειτονικό AP για μετρήσεις ή σε μια ομάδα από APs που ανήκουν στο ίδιο BSS. Συνήθως όμως, τα APs ζητούν αναφορές με τις μετρήσεις από τις συσκευές των clients που είναι συνδεδεμένοι σε αυτό. Πιο κάτω περιγράφουμε τα πιο βασικά είδη των αναφορών που μπορούν να ανταλλάξουν οι clients με τα APs. Όταν αναφερόμαστε σε client πιο κάτω, αυτό μπορεί να είναι είτε ένα AP είτε μια συσκευή που υποστηρίζει το πρότυπο IEEE 802.11:

The Beacon Report: Όταν το AP ζητήσει από τον client(s) να πάρει μετρήσεις για το RF περιβάλλον, οι συσκευές στέλνουν ένα beacon report, όπως ονομάζεται η αναφορά αυτή, που περιλαμβάνει πληροφορίες σχετικά με τα beacons που ανίχνευσαν από τα γειτονικά BSS(s), ποια κανάλια χρησιμοποιούν, τις υπηρεσίες που προσφέρουν τα APs που ανακάλυψαν και την ποιότητα της σύνδεσης τους σε αυτά.

Frame Report: Το Frame report περιλαμβάνει πληροφορίες για όλα τα frames που έλαβε ο client από το AP, το received power, το SNR και άλλες μετρήσεις που αφορούν το AP που είναι συνδεδεμένο. Αυτές τις πληροφορίες τις ομαδοποιεί για κάθε διεύθυνση, δηλαδή AP, που ανιχνεύει κατά την διάρκεια των μετρήσεων.

Channel Load Report: Αυτή η αναφορά δημιουργείται από τους clients και στέλνονται στα APs. Βασικά, μας δείχνει την διάρκεια που ένα κανάλι θεωρείτο κατειλημμένο κατά την διάρκεια των μετρήσεων. Ο χρόνος που ένα κανάλι είναι κατειλημμένο ορίζεται ως η χρονική περίοδος όπου το carrier sense (CSMA), το NAV ή και τα δύο δείχνουν ότι το κανάλι είναι busy.

Noise Histogram Report: Η αναφορά του noise histogram περιλαμβάνει όλη την ενέργεια (ισχύ) που δεν ανήκει στο WiFi και η οποία λήφθηκε από την συσκευή που κάνει την αναφορά στο κανάλι που λειτουργεί το δίκτυο. Αυτή η αναφορά δημιουργείται όταν ο μηχανισμός CCA θεωρεί ότι κανάλι είναι ελεύθερο. Συνήθως ζητείται από το AP προς τους clients.

Hidden Station Report: Σε αυτό το είδος αναφοράς περιλαμβάνεται ο αριθμός των fames που έχει στείλει το AP στην κρυφή συσκευή και η διεύθυνση της συσκευής αυτής. Μια κρυφή συσκευή παρακολουθείται από το AP που κάνει την μέτρηση και θεωρείται κρυφή, όταν λάβει τις αρχικές μεταδόσεις από το AP αλλά παρόλο που απαιτούν αποστολή ACK, δεν στέλνει πίσω κάποιο μήνυμα ACK.

Medium Sensing Time Histogram Report: Η αναφορά αυτή στέλνεται από τον client συνήθως στο AP με κάποιες στατιστικές για τις χρονικές περιόδους που το μέσον είναι αδρανές και απασχολημένο όπως το έχει ανιχνεύσει ο client.

STA Statistics report: Εδώ ο client αναφέρει στο AP την ποιότητα της σύνδεσης και της απόδοσης του δικτύου κατά την διάρκεια που εκτελεί τις μετρήσεις.

- **Neighbor report:** Αυτή η αναφορά ζητείται συνήθως από τις απλές συσκευές (όπως smartphones) προς το AP που είναι συνδεδεμένες και έχει σκοπό να βελτιώσει την περιαγωγή ανάμεσα στα WLAN cells ή αλλιώς το handover. Όταν ζητηθεί η αναφορά, το AP στέλνει μια λίστα από τα γειτονικά APs (στο ίδιο ESS) τα οποία η συσκευή μπορεί να χρησιμοποιήσει ως υποψήφια όταν κάνει περιαγωγή από το ένα BSS στο άλλο. Για κάθε AP στη λίστα παρέχονται τα ακόλουθα:
  - BSSID
  - Οι δυνατότητες του AP (όπως το αν υποστηρίζει το 802.11e QoS)

- Σε περίπτωση που η συσκευή θέλει να αλλάξει BSS, αναφέρεται αν μπορεί να γίνει επικοινωνία με κάποιο AP από τη λίστα για να γίνει προ-εξουσιοδότηση
- Το κανάλι του AP

4.3 Μελέτη των αλγορίθμων RRM

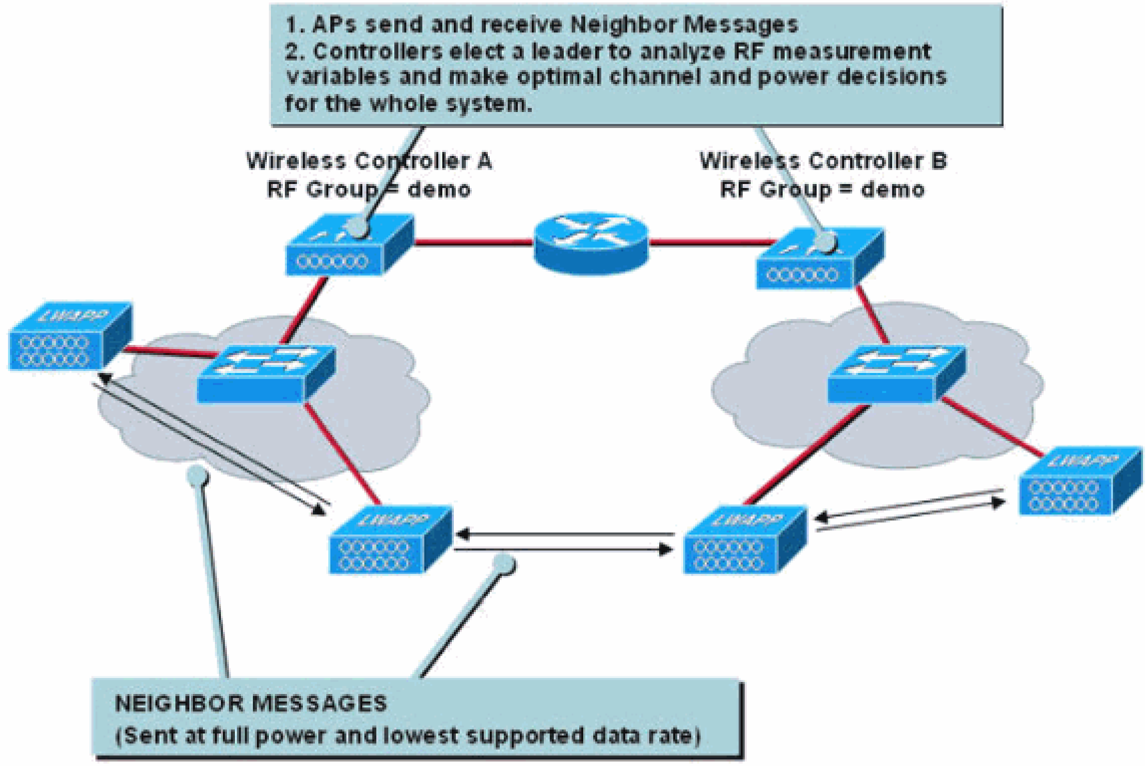
Πριν να προχωρήσουμε στην περιγραφή των αλγορίθμων που χρησιμοποιεί το RRM, θα πρέπει πρώτα να μελετήσουμε τον τρόπο με τον οποίον το δίκτυο ξεκινά τη λειτουργία του και δημιουργεί ένα RF Grouping [20,21,22], όπως λέγεται, και τι υπολογισμούς χρειάζεται να κάνει πριν την εκτέλεση των αλγορίθμων. Πιο κάτω περιγράφουμε κάποια βήματα κατά τα οποία το σύστημα μαθαίνει, δημιουργεί ομάδες και μετά υπολογίζει όσες πληροφορίες χρειάζονται για τους RRM αλγορίθμους:

1. Οι συσκευές που λειτουργούν ως Controllers ανατίθενται αρχικά ένα RF Group name. Αυτό είναι μια λέξη με χαρακτήρες ASCII το οποίον χρησιμοποιούν τα APs για να αποφασίσουν αν το γειτονικό AP που «ακούν» ανήκει στην ίδια ομάδα με αυτά και είναι το ίδιο στους controllers των οποίων τα APs έχουν τις ίδιες ρυθμίσεις και θέλουμε να είναι μια ομάδα.

2. Τα APs στέλνουν κάθε 60 δευτερόλεπτα τα λεγόμενα Neighbor Messages μοιράζοντας πληροφορίες σχετικά με τον εαυτό τους, τους controllers τους και το RF Group name τους. Αυτά τα μηνύματα στέλνονται με την μέγιστη ισχύ και το χαμηλότερο ρυθμό αποστολής για να φτάσει το μήνυμα σε όλα τα APs που βρίσκονται στην κοντινή περιοχή. Τα APs που λαμβάνουν αυτά τα μηνύματα, δέχονται μόνον εκείνα που ανήκουν στο δικό τους RF Group name αλλιώς τα απορρίπτουν. Επίσης, η αποστολή των Neighbor Messages είναι αναγκαία όχι μόνο για την δημιουργία των ομάδων με τα APs, αλλά και από τον αλγόριθμο του Transmit Power Control (TPC) όπου χρειάζεται να ξέρουμε τον τρίτο πιο ηχηρό γείτονα του κάθε AP.

3. Όσα APs λαμβάνουν τα Neighbor Messages και τα επικυρώνουν με βάση το RF Group name, τα προωθούν με την σειρά τους μαζί με τις πληροφορίες του AP που το έχει στείλει καθώς και την διεύθυνση IP του controller, προς τους δικούς τους controllers που είναι συνδεδεμένοι. Οι controllers μετά τη λήψη των πιο πάνω μηνυμάτων μπορούν τώρα να γνωρίζουν ποιοι άλλοι controllers βρίσκονται στο ίδιο RF Group και έτσι δημιουργούν ένα RF domain, όπου

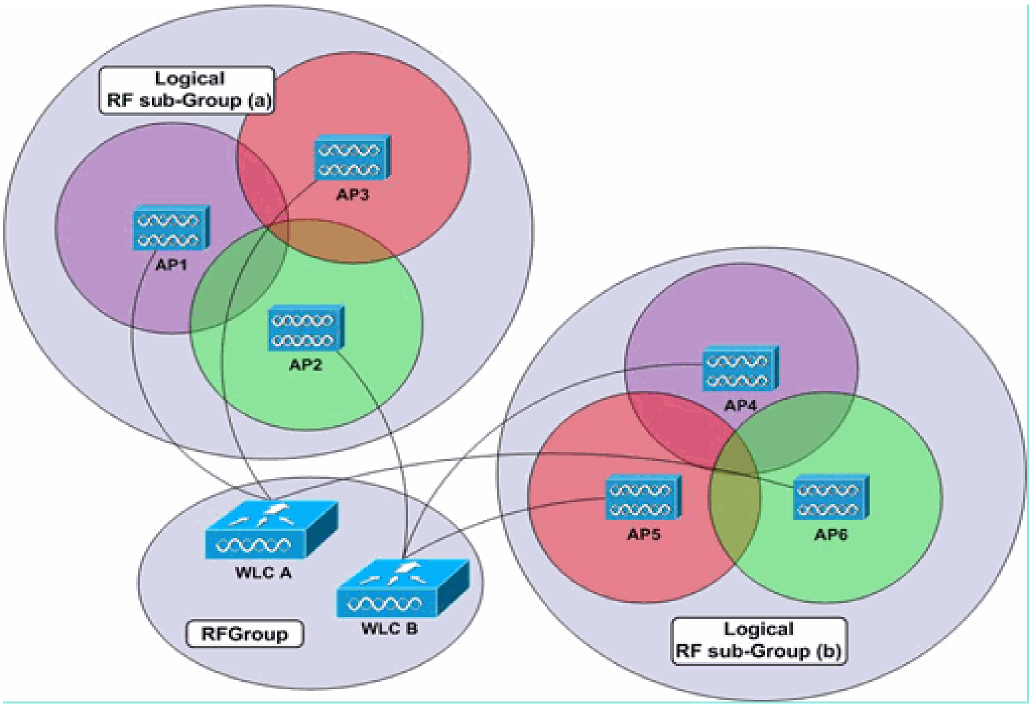
μοιράζονται τις RF πληροφορίες μεταξύ τους. Σε κάθε RF Group οι controllers θα ψηφίσουν έναν RF Group leader, ο οποίος βασικά αναλαμβάνει ηγετικά καθήκοντα παίρνοντας αποφάσεις για τις ρυθμίσεις του δικτύου.



Σχήμα 4.1: Τα Neighbor Messages στέλνονται από τα APs στους Wireless Controllers δίνοντας τους την γενική εικόνα του δικτύου ώστε να προσαρμόζουν ανάλογα την ισχύ και τα κανάλια.

Μετά από τα πιο πάνω βήματα, μαζεύονται οι απαραίτητες πληροφορίες από το RF περιβάλλον για κάθε AP στο RF Group και έτσι ο RF Group leader που ψηφίστηκε είναι έτοιμος να εφαρμόσει τους αλγόριθμους του RRM. Συνολικά υπάρχουν τρείς κύριοι αλγόριθμοι στο RRM, αλλά μόνον οι δύο εκτελούνται από τον RF Group leader, ενώ ο τρίτος εκτελείται σε κάθε controller. Οι δύο κύριοι αλγόριθμοι είναι για την δυναμική προσαρμογή της ισχύος μετάδοσης του AP (Transmit Power Control) και την δυναμική ανάθεση καναλιών (Dynamic Channel Assignment). Ο τρίτος αλγόριθμος είναι για τον εντοπισμό και επιδιόρθωση τρυπών στο δίκτυο (Coverage Hole Detection and Correction) και τρέχει από τον κάθε controller τοπικά και όχι από τον RF Group leader, γιατί βασίζεται στο SNR του κάθε AP. Επίσης, για κάθε RF Group μπορεί να υπάρχουν δύο ή περισσότεροι RF Group leaders γιατί χρειαζόμαστε ένα controller για το φάσμα του 2.4 GHz και ένα άλλο για το φάσμα του 5 GHz. Γενικά έχουμε την ακόλουθη ιεραρχία σε ένα δίκτυο με τον μηχανισμό RRM: 1) το RF Group Name το οποίον είναι κοινό σε όλους τους controllers που ανήκουν σε ένα RF Group, 2) ο RF Group leader που ψηφίζεται από τους controllers που ανήκουν σε ένα RF Group και είναι υπεύθυνος για την εκτέλεση των δύο αλγορίθμων που αναφέραμε και τελευταίο είναι 3) το RF Neighborhood (ή

Sub-Group) το οποίον αποτελείται από πολλά APs που ακούν το ένα το άλλο. Πιο κάτω στο σχήμα 4.2, είναι ένα παράδειγμα που δείχνει ένα RF Group που αποτελείται από 2 controllers και δύο RF Sub-Group που αποτελούνται από 3 APs το καθένα. Ο λόγος που σχηματίζονται 2 RF Sub-Group είναι διότι δεν υπάρχει κάποιο AP από το RF Sub-Group (a) που να ακούει κάποιο AP από το RF Sub-Group (b). Εντούτοις όμως, οι controllers ανήκουν στο ίδιο RF Group γιατί έχουν το ίδιο RF Group Name.



Σχήμα 4.2: Οι controllers (WLCs A και B) ανήκουν στο ίδιο RF Group και τα APs ανήκουν σε δύο διαφορετικά RF sub-Groups.

4.3.1 Αλγόριθμος Dynamic Channel Assignment (DCA)

Ο αλγόριθμος δυναμικής ανάθεσης των καναλιών (DCA) σε κάθε AP αποτελεί το πιο σημαντικό στοιχείο του μηχανισμού RRM [23]. Οι κύριες λειτουργίες του αλγόριθμου είναι: 1) να διαχειρίζεται δυναμικά την ανάθεση των καναλιών για κάθε AP σε ένα RF group με το να παρακολουθεί τα ελεύθερα κανάλια στο RF περιβάλλον, 2) να αξιολογεί την ανάθεση που γίνεται ανά AP και στα δύο φάσματα των 2.4 GHz και 5 GHz, 3) να λάβει αποφάσεις για τα κανάλια που θα αναθέσει με βάσει την μετρική κόστους (Cost Metric) η οποία αξιολογεί την απόδοση του καναλιού με την ποσότητα της παρεμβολής που υπάρχει σε αυτό, και τέλος 4) να μπορεί να διαχειρίζεται το εύρος ζώνης των 20,40,80 ή 160 MHz και να προτείνει δυναμικά το κατάλληλο εύρος στο κάθε AP.

Πριν την εκτέλεση του αλγόριθμου από τον RF Group Leader, θα πρέπει να συγκεντρώσει πληροφορίες για τα κανάλια που είναι διαθέσιμα να χρησιμοποιήσει και τις συνθήκες που επικρατούν στο περιβάλλον. Έτσι, χρειάζεται τις μετρικές του Same Channel Contention, δηλαδή τον αριθμό των APs που λειτουργούν στο ίδιο κανάλι (αλλιώς co-channel interference), το Foreign channel που είναι μια μέτρηση των APs που βρίσκονται σε άλλο RF Group και παρεμβάλλουν στο κανάλι του AP που θα τρέξει ο αλγόριθμος, τον θόρυβο του καναλιού που δημιουργείται από συσκευές άλλων τεχνολογιών όπως Bluetooth, τον φόρτο του καναλιού από το εξεταζόμενο AP και τέλος μια σταθερά που ονομάζεται DCA Sensitivity και την καθορίζει ο χρήστης. Όλες αυτές οι μετρήσεις συνδυάζονται σε μια μετρική που ονομάζεται μετρική κόστους (Cost Metric) η οποία είναι μια RSSI τιμή που δείχνει το SNIR (Signal to Noise Ratio) ενός καναλιού και χρησιμοποιείται για να αξιολογήσει το κάθε κανάλι, για το κάθε AP για να επιλέξει αυτό που θα δώσει την μέγιστη απόδοση.

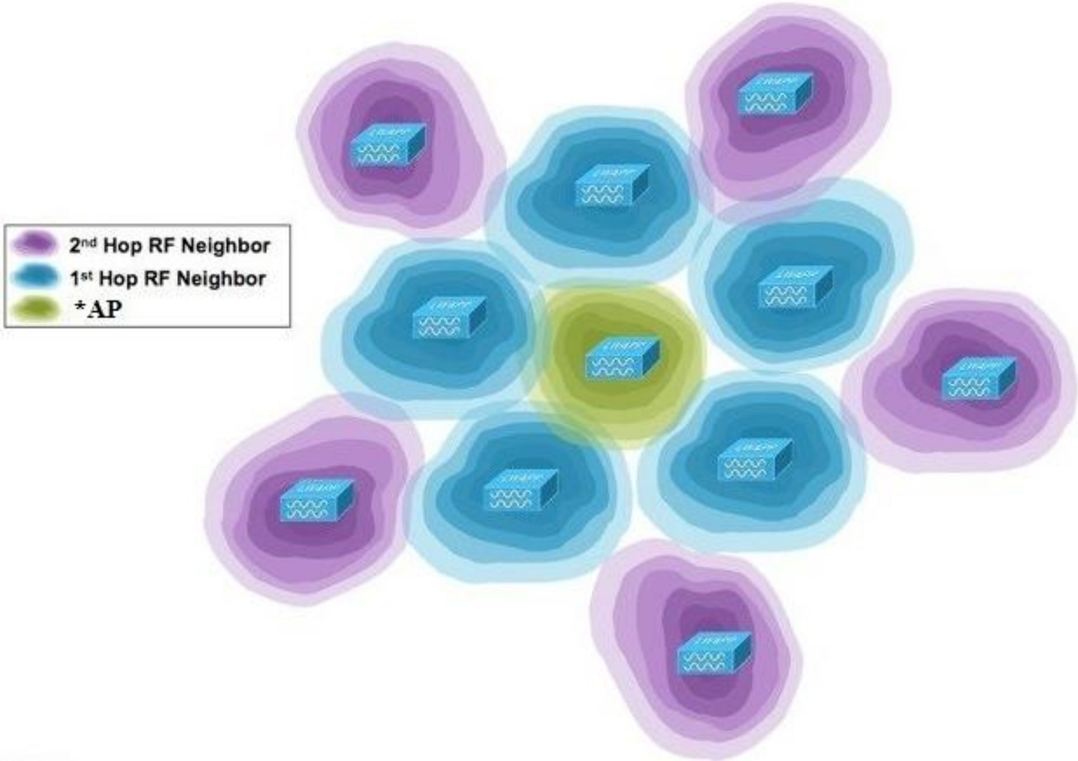
Στη συνέχεια θα περιγράψουμε τον αλγόριθμο ο οποίος εκτελείται από τον RF Group Leader κάθε 10 λεπτά, αλλά δεν σημαίνει πως χρειάζεται να γίνει κάποια αλλαγή καναλιού σε κάθε εκτέλεση:

1. Αρχικά, ο αλγόριθμος ξενικά με τον RF Group Leader να δημιουργεί μια λίστα που ονομάζεται CPCI (Channel Plan Change Initiator) και περιέχει τα AP ταξινομημένα με βάση την τιμή MK από το χειρότερο προς το καλύτερο. Ο RF Group Leader επιλέγει το πρώτο AP της λίστας που έχει την χειρότερη τιμή CM (συμβολίζουμε ως *AP), καθώς και τους γείτονες του που βρίσκονται σε απόσταση ενός hop και δύο hop μακριά από εκείνον μαζί ως μια ομάδα, με σκοπό να αποφασίσει αν ένα πλάνο ανάθεσης καναλιών θα μπορεί να δώσει καλύτερη απόδοση στο δίκτυο. Ένας γείτονας σε απόσταση ενός hop είναι οποιοδήποτε AP που γνωρίζει το *AP μέσω απευθείας επικοινωνίας αφού είναι γείτονες, ενώ ένας γείτονας σε απόσταση δύο hop είναι ένα AP που γνωρίζουμε ότι υπάρχει μέσω ενός AP που είναι σε απόσταση ενός hop.

2. Στη συνέχεια, καθώς γίνεται η αξιολόγηση των καναλιών, ο RF Group Leader μπορεί να αλλάξει τα κανάλια του *AP και των γειτόνων του σε απόσταση ενός hop για να επιτευχθεί μια λύση. Όσον αφορά τους γείτονες σε απόσταση δύο hop, τα κανάλια τους δεν αλλάζουν, γιατί έτσι αποφεύγουμε την πιθανότητα να γίνει μια αλλαγή και να επηρεαστούν όλα τα APs του RF Group. Μετά τους διάφορους υπολογισμούς, θα προκύψουν πολλά πιθανά πλάνα ανάθεσης καναλιών που θα βελτιώνουν την απόδοση του *AP. Γι’ αυτό τον λόγο, κάθε πλάνο ανάθεσης θα περάσει από μια νέα συνάρτηση που ονομάζεται NCCF (Normalized Cumulative Cost Function) και θα προτείνει τα πλάνα τα οποία πρώτα βελτιώνει ή αφήνει την ίδια απόδοση στους γείτονες του *AP μαζί ως μια ομάδα, και ,επίσης, τα πλάνα πρέπει να βελτιώνουν την μετρική κόστους (CM) του *AP.

3. Στο τέλος της διαδικασίας και αφού παρθεί η απόφαση για εφαρμογή του πλάνου ανάθεσης, το *AP μαζί με τους γείτονες του σε απόσταση ενός hop αφαιρούνται από την λίστα CPCI και στην επόμενη επανάληψη του αλγόριθμου ο RF Group Leader θα επιλέξει τυχαία ένα AP από την λίστα CPCI μέχρι να αδειάσει. Για την επιλογή του επόμενου AP, γίνεται μια εναλλαγή μεταξύ της επιλογής ενός τυχαίου ή του χειρότερου AP με βάση την τιμή CM από την λίστα.

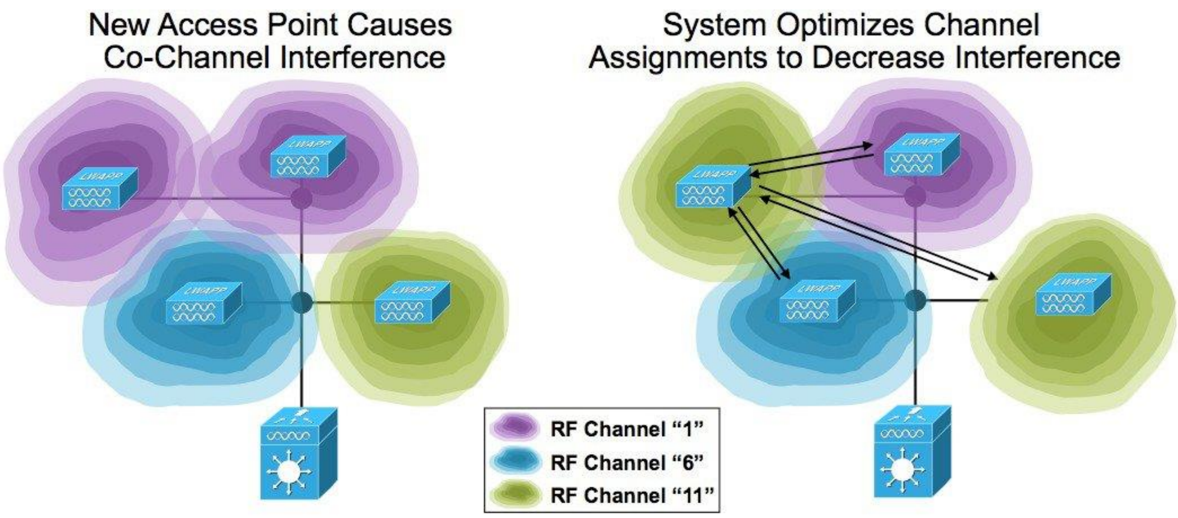
4. Ο αλγόριθμος τερματίζει όταν η λίστα CPCI αδειάσει, ολοκληρωθεί η συνάρτηση NCCF και το προτεινόμενο πλάνο ανάθεσης καναλιών εφαρμοστεί.



Σχήμα 4.3: Παράδειγμα επιλογής του *AP μαζί με τους γείτονες του σε απόσταση ενός και δύο hop

Ο πιο πάνω αλγόριθμος θα τρέχει, όπως είπαμε, κάθε 10 λεπτά, αλλά αυτό δεν σημαίνει πως σε κάθε επανάληψη του θα χρειάζεται να γίνει κάποια αλλαγή καναλιών. Συγκεκριμένα, για να γίνει μια αλλαγή στα κανάλια των APs θα πρέπει η βελτίωση στις συνθήκες του νέου καναλιού να είναι τουλάχιστον ίση με την τιμή της σταθεράς DCA Sensitivity η οποία καθορίζεται από τον χρήστη, αλλιώς δεν θα γίνει αλλαγή του καναλιού.

Το φάσμα 2.4 GHz όπως ξέρουμε μοιράζεται σε πολλές συσκευές οι οποίες είτε είναι συνεχώς ενεργοποιημένες, όπως μια αναλογική βιντεοκάμερα, είτε ενεργοποιούνται σε συχνά διαστήματα, όπως ένας φούρνος μικροκυμάτων. Στην περίπτωση των συσκευών που χρησιμοποιούνται μόνο για μικρές χρονικές περιόδους, υπάρχει πιθανότητα να επηρεάσει την λειτουργία του WiFi, γιατί μοιράζεται το ίδιο φάσμα συχνοτήτων και η ενέργεια που εκπέμπει είναι ικανή να διακόψει τις επικοινωνίες του ασύρματου δικτύου. Ως αποτέλεσμα, χρειαζόμαστε ένα τρόπον που να μπορεί ο πιο πάνω αλγόριθμος να αναγνωρίζει τα κανάλια που επηρεάζονται από αυτές τις συσκευές και να τα αποφεύγει. Μια λύση σε αυτό το πρόβλημα που προτάθηκε από διάφορες εταιρείες είναι να μαρκάρονται τα κανάλια από το AP που εντοπίζει την συγκεκριμένη δραστηριότητα, έτσι ώστε να θυμάται κατά τη διάρκεια των ημερών ποια κανάλια επηρεάζονται από αυτές τις συσκευές και έτσι να μειώνεται η πιθανότητα να επιλέγονται αυτά τα κανάλια από τον RF Group Leader. Μετά από ένα διάστημα κάποιων ημερών, αν σταματήσει η παρουσία της συσκευής στα συγκεκριμένα κανάλια, τότε δεν θα μαρκάρονται πλέον και η πιθανότητα επιλογής τους στον αλγόριθμο θα είναι η ίδια με τα υπόλοιπα κανάλια.



Σχήμα 4.4: Παράδειγμα λειτουργίας του αλγορίθμου DCA

4.3.2 Αλγόριθμος Transmit Power Control (TPC)

Ένας άλλο αλγόριθμος του RRM που τρέχει σε ολόκληρο το δίκτυο από τον RF Group Leader είναι το Transmit Power Control (TPC). Οι αλγόριθμοι TPC και DCA λειτουργούν μαζί με σκοπό να ελέγξουν το σήμα RF στο περιβάλλον και να βελτιώσουν την αποδοτικότητα του δικτύου μας. Ο έλεγχος της ισχύος καθορίζει τα όρια των κελιών του κάθε AP και έτσι μπορούμε με αυτό τον τρόπο να μεγιστοποιήσουμε την κάλυψη του σήματος του δικτύου στο περιβάλλον, χωρίς όμως να προκαλούμε παρεμβολές όπως το co-channel interference. Πιο συγκεκριμένα, ο αλγόριθμος TPC χρησιμοποιεί τις λίστες TX Neighbor και RX Neighbor που δημιουργούνται από την ανταλλαγή των Neighbor messages μεταξύ των APs και οι οποίες περιλαμβάνουν το πώς το AP που ελέγχουμε ακούει τα υπόλοιπα APs (RX Neighbor) και το πώς τα υπόλοιπα APs ακούν το δικό μας AP (TX Neighbor). Με τις λίστες αυτές δημιουργείται μια εικόνα στον RF Group Leader για το πώς ακούει το ένα AP το άλλο μέσα σε ένα RF Neighborhood και σε ολόκληρο το RF Group. Στη συνέχεια, βασιζόμενος σε αυτές τις πληροφορίες, ο αλγόριθμος ρυθμίζει ανάλογα την ισχύ μετάδοσης του κάθε AP έτσι ώστε να μεγιστοποιηθεί η περιοχή κάλυψης και να ελαχιστοποιηθεί η παρεμβολή στο δίκτυο μας.

Ο αλγόριθμος αυτός τρέχει από τον RF Group Leader κάθε 10 λεπτά, όπως και με τον DCA αλγόριθμο, και υπολογίζει την Tx ισχύ μετάδοσης για κάθε AP και για κάθε μέλος του RF Group στις συχνότητες 2,4 GHz και 5 GHz. Για να γίνει όμως η αλλαγή στην ισχύ μετάδοσης του AP χρησιμοποιείται μια σταθερά που καθορίζεται από τον χρήστη και ονομάζεται RRM Power Threshold. Η τιμή της σταθεράς είναι προεπιλεγμένη στα -70 dBm, αλλά μπορεί να πάρει τιμές μεταξύ -50 και -80 dBm και πρέπει να έχει την ίδια τιμή σε όλους τους controllers του RF Group. Με άλλα λόγια, η τιμή αυτή καθορίζει το πόσο δυνατά πρέπει να ακούν τα γειτονικά APs ένα προκαθορισμένο AP. Εκτός από την σταθερά αυτή, το AP που ελέγχεται την δεδομένη στιγμή πρέπει να έχει τουλάχιστον 3 γείτονες, γιατί ο RF Group Leader θα μαζέψει πληροφορίες για τον $3^{ο}$ πιο ηχηρό γείτονα του AP που ελέγχει, από την λίστα των γειτονικών AP. Η πληροφορία για τον $3^{ο}$ κατά ισχύ TX δυνατότερο γείτονα χρειάζεται γιατί υπάρχουν 3 μη επικαλυπτόμενα κανάλια στο φάσμα 2.4 GHz και γιατί ο σκοπός του αλγόριθμου είναι να μειώσει την ισχύ των APs, ώστε αυτός ο γείτονας να ακούγεται με ισχύ ίση με το RRM Power Threshold, δηλαδή στα -70 dBm ή μικρότερο. Η σταθερά RRM Power Threshold μαζί με την πληροφορία της ισχύος του $3^{ου}$ δυνατότερου γείτονα χρησιμοποιούνται για να αποφασίσει ο RF Group Leader κατά πόσον θα προσαρμόσει την ισχύ του κάθε AP.

Ο αλγόριθμος αποτελείται από δύο φάσεις:

1. Στην πρώτη φάση του αλγόριθμου υπολογίζεται η ιδανική ισχύς που πρέπει να στέλνει το AP. Αυτό υπολογίζεται σύμφωνα με την εξίσωση:Tx_Ideal = Tx_Max + (TPC_Threshold - RSSI_3rd)

   όπου

   Tx_Max: η μέγιστη δυνατή ισχύς μετάδοσης για μια συσκευή

   TPC_Threshold: Η σταθερά RRM power threshold που καθορίζεται από τον χρήστη (προεπιλεγμένο στα -70 dBm)

   RSSI_3rd: Ο τρίτος κατά σειρά πιο ηχηρός AP στη λίστα του AP TX Neighbor

   Με βάση την πιο πάνω εξίσωση αποφασίζεται αν χρειάζεται μια αύξηση ή μείωση στην ισχύ ως ακολούθως:

- Εάν η τιμή του Tx_Ideal είναι μεγαλύτερη από την τιμή Tx_Current (υφιστάμενη ισχύς) τότε χρειάζεται αύξηση στην ισχύ του AP.
- Εάν η τιμή του Tx_Ideal είναι μικρότερη από την τιμή Tx_Current (υφιστάμενη ισχύς) τότε χρειάζεται μείωση στην ισχύ του AP.

2. Η δεύτερη φάση περιλαμβάνει την αξιολόγηση των αποτελεσμάτων από την πρώτη φάση και την λήψη της απόφασης αν θα πρέπει να γίνει αλλαγή στην ισχύ ή όχι. Επίσης, επειδή η αλλαγή στην ισχύ Tx ενός AP μπορεί να αλλάξει τα όρια του κελιού που καλύπτει, προστίθεται ένα κατώφλι για να είμαστε εντελώς σίγουροι πως η αλλαγή είναι αναγκαία.

   Πιο συγκεκριμένα λέμε ότι:

   Για μια αύξηση της Tx ισχύος το κατώφλι είναι 3 dB

   Για μια μείωση της Tx ισχύος το κατώφλι είναι 6 dB

   Με αυτό το κατώφλι, η αλλαγή στην Tx ισχύ θα γίνεται όταν υπολογίσουμε το

   Tx_Current - Tx_Ideal = N

   και θα αποφασίσουμε ως ακολούθως:

   - Εάν η τιμή N<= Κατώφλι τότε δεν γίνεται κάποια αλλαγή.
   - Εάν η τιμή N> Κατώφλι τότε θα γίνει η αλλαγή.

Με αυτό τον αλγόριθμο ο RF Group Leader αποφασίζει αν θα υλοποιήσει την αλλαγή στην ισχύ των APs ή όχι. Σε περίπτωση που εφαρμόσει μια μείωση στην ισχύ των APs, θα μειώνεται σταδιακά κατά 3 dB η ισχύς σε κάθε επανάληψή του αλγόριθμου, μέχρι να μην ισχύει η συνθήκη που είδαμε πιο πάνω. Από την άλλη, σε περίπτωση που εφαρμόσει μια αύξηση στην ισχύ των APs, θα αυξάνεται σταδιακά κατά 3 dB η ισχύς σε κάθε επανάληψή του αλγόριθμου μέχρι να φτάσει την τιμή του Tx_Ideal ή του κατωφλίου.

4.3.3 Αλγόριθμος Coverage Hole Detection and Mitigation (CHDM)

Ο τρίτος και τελευταίος αλγόριθμος που ανήκει στον μηχανισμό του RRM είναι ο αλγόριθμος του Coverage Hole Detection and Mitigation (CHDM). Ο αλγόριθμος αυτός είναι ο μόνος που τρέχει τοπικά σε κάθε controller και όχι από τον RF Group Leader, γιατί πρέπει να παρακολουθεί όλα τα APs που συνδέονται σε αυτόν καθώς και κάθε χρήστη που συνδέεται στα APs μαζί με τα επίπεδα SNR του σήματος του. Με αυτό τον τρόπο θα εντοπίσει αν υπάρχει κάποια περιοχή όπου το σήμα των χρηστών δεν είναι ικανοποιητικό, άρα υπάρχει τρύπα, και θα προσπαθήσει να διορθώσει αυτό το πρόβλημα με το να αυξήσει την ισχύ ενός AP ή μιας ομάδας από APs για να βελτιώσει τα επίπεδα του σήματος των χρηστών. Με άλλα λόγια, αν το επίπεδο του SNR του σήματος των χρηστών μειωθεί κάτω από ένα κατώφλι που επιλέγουμε εμείς, τότε ο controller αναλαμβάνει να καλύψει αυτό το πρόβλημα που δημιουργείται με τον τρόπο που περιγράψαμε.

Ο αλγόριθμος χωρίζεται στην φάση του εντοπισμού την τρύπας, Coverage Hole Detection (CHD), και στην φάση επούλωσης της τρύπας, Coverage Hole Mitigation (CHM):

- Στην πρώτη φάση του CHD, το AP διατηρεί για κάθε χρήστη ένα ιστόγραμμα του RSSI του σήματος του διάρκειας 5 δευτερολέπτων. Αν σε αυτές τις μετρήσεις του RSSI οι τιμές του χρήστη για τα 5 δευτερόλεπτα είναι μικρότερες από συγκεκριμένα κατώφλια που ορίζουμε εμείς, τότε μαρκάρεται ως ένα pre-coverage hole γεγονός. Το γεγονός αυτό αποστέλλεται αμέσως από τον AP στον controller, ο οποίος παρακολουθεί τις τιμές RSSI του σήματος για 90 δευτερόλεπτα και αν συνεχίσει το σήμα να είναι κάτω από τις κανονικές τιμές τότε θεωρείται ως ένα πρόβλημα coverage hole. Στο επόμενο στάδιο, ο controller θα αποφασίσει αν αυτό το πρόβλημα coverage hole μπορεί να διορθωθεί με το να ελέγξει πρώτα αν ο χρήστης μπορεί να μεταφερθεί σε ένα γειτονικό AP, αλλά απλά δεν το έχει κάνει. Αυτό μπορεί να ελεγχτεί με το να δει την τοποθεσία του χρήστη και να αξιολογήσει την ποιότητα των σημάτων των γειτονικών APs που μπορεί να ακούσει, βλέποντας τα RSSI τους. Αν υπάρχει κάποιο AP που το σήμα του ξεπερνά το κατώφλι που θέσαμε, τότε διαγράφεται το πρόβλημα αυτό και συνεχίζεται η κανονική λειτουργία του δικτύου. Στην αντίθετη περίπτωση εφαρμόζεται το CHM.

- Στην επόμενη φάση του CHM, γίνεται μια διαδικασία για να διορθωθεί το πρόβλημα που παρουσιάστηκε στην προηγούμενη φάση. Πιο συγκεκριμένα, αν υπάρχει πρόβλημα coverage hole και ικανοποιούνται ορισμένα κριτήρια τότε ο controller θα αυξήσει την ισχύ του AP. Τα κριτήρια που πρέπει να ικανοποιούνται είναι να υπάρχει ένας ελάχιστος αριθμός από χρήστες που να έχουν πρόβλημα coverage hole στο συγκεκριμένο AP και το συνολικό ποσοστό των χρηστών που έχουν πρόβλημα στο συγκεκριμένο AP να είναι μεγαλύτερο από το ποσοστό που καθορίζεται από τον διαχειριστή του δικτύου. Με την ικανοποίηση των κριτηρίων αυτών, η αύξηση της ισχύος στο AP θα γίνεται σταδιακά με κάθε επανάληψη του αλγόριθμου, για να μην δημιουργηθούν προβλήματα στα υπόλοιπα APs.

Όπως βλέπουμε, ο αλγόριθμος CHDM εκτελείται με προσοχή και λαμβάνοντας υπόψη διάφορα κριτήρια, γιατί λειτουργεί ανεξάρτητα από τους DCA και TPC αλγόριθμους, και είναι φανερός ο κίνδυνος με την αύξηση της ισχύος του ενός AP να έχουμε επιπτώσεις στο γειτονικά APs και να προκαλέσουμε παρεμβολές. Λαμβάνοντας όμως υπόψη τις παραμέτρους που αναφέραμε μαζί με την σταδιακή αύξηση της ισχύος, μειώνεται η πιθανότητα επηρεασμού των γειτονικών APs.

4.4 Συμπεράσματα

Συνοψίζοντας, υπάρχουν διάφορες προσεγγίσεις όσον αφορά την υλοποίηση ενός μηχανισμού διαχείρισης πόρων του δικτύου, αλλά συνήθως ακολουθείται είτε η κεντρικοποιημένη προσέγγιση είτε η κατανεμημένη. Όπως είδαμε, η κεντρικοποιημένη προσέγγιση παρόλον ότι είναι πολύ πιο προσιτή και είναι πιο εύκολη στην υλοποίηση, τα προβλήματα και οι δυσκολίες στο να συντονίσουμε τους κόμβους έτσι ώστε να βελτιστοποιήσουμε την χρήση των πόρων του δικτύου, μας οδηγούν στην πιο εξελιγμένη μέθοδο που είναι η κατανεμημένη. Όπως έχουμε αναφέρει, αυτή η λύση απαιτεί από τις συσκευές να έχουν ενσωματωμένη μια «εξυπνάδα» ώστε να μπορούν να λαμβάνουν μόνες τους αποφάσεις και να προσαρμόζονται ανάλογα στο περιβάλλον.

Μέσα σ’ αυτό το πλαίσιο, έχουμε αναπτύξει στο παρόν κεφάλαιο τους αλγόριθμους με τους οποίους ένα δίκτυο που έχει ενεργοποιημένο το RRM μπορεί να προσαρμόζεται δυναμικά στο περιβάλλον με το να αυξάνεται ή να μειώνεται η ισχύς των APs καθώς και να επιλέγεται το κατάλληλο κανάλι για το κάθε ένα AP με σκοπό να μειώνεται η παρεμβολή στο περιβάλλον και να μεγιστοποιείται η περιοχή κάλυψης. Ακόμη, οι αλγόριθμοι προσφέρουν λύσεις σε προβλήματα όπου οι χρήστες έχουν χαμηλό σήμα από κάποιο AP, γιατί μπορεί σε αυτό το AP να έχει μεγάλο φόρτο από τους χρήστες και με την βοήθεια των αλγορίθμων η ισχύς των APs θα αυξηθεί για να διατηρηθεί σε ικανοποιητικά επίπεδα το σήμα στον κάθε χρήστη. Επιπλέον, το RRM προσφέρει την δυνατότητα αυτό-επούλωσης, δηλαδή αν παρουσιαστεί πρόβλημα σε ένα AP και σταματήσει την λειτουργία του, τότε γίνεται μια διαδικασία ώστε τα γειτονικά APs να καλύψουν την περιοχή που λειτουργούσε το προβληματικό AP.

Με τους μηχανισμούς του RRM βλέπουμε πως σε ένα δίκτυο μπορεί να πετύχουμε αποδοτική χρήση του φάσματος και να μειώσουμε τα προβλήματα με τους προσφερόμενους αλγόριθμους. Οι δυνατότητες του RRM, όμως, επεκτείνονται και στον εντοπισμό των παρεμβολών που γίνονται από άλλες τεχνολογίες όπως το Zigbee και το Bluetooth, αλλά και από τον φούρνο μικροκυμάτων ο οποίος μπορεί να επηρεάσει αρκετά ένα δίκτυο WiFi. Με άλλα λόγια, ο μηχανισμός RRM βοηθά τα APs να εντοπίσουν παρεμβολές που δεν ανήκουν στη τεχνολογία WiFi, αλλά μοιράζονται το ίδιο φάσμα 2.4 GHz. Ως αποτέλεσμα, τα APs μπορούν να αποφύγουν τις παρεμβολές που επικρατούν σε ορισμένα κανάλια με το να αποκλείσουν την χρήση των καναλιών τα οποία επηρεάζονται από άλλες τεχνολογίες. Με αυτό τον τρόπο, λειτουργούν πιο έξυπνα οι συσκευές σε ένα δίκτυο WiFi και περιορίζουν την εμφάνιση προβλημάτων στο δίκτυο μας, αλλά και στις συσκευές που μοιράζονται το υπόλοιπο φάσμα. Φυσικά, η υλοποίηση του μηχανισμού αυτού εναπόκειται στην κάθε εταιρεία που αναπτύσσει συσκευές για το πρότυπο IEEE 802.11b/g, αλλά γενικά ο μηχανισμός RRM με αυτή την διαδικασία ελαχιστοποιεί το πρόβλημα των παρεμβολών με τις τεχνολογίες που λειτουργούν στο ίδιο φάσμα με το WiFi.

Κεφάλαιο 5

Αξιολόγηση του αλγόριθμου Frequency agility του Zigbee

5.1 Σύγκριση OPNET Modeler με άλλα εργαλεία προσομοίωσης

Οι προσομοιωτές δικτύου αποτελούν ένα βασικό εργαλείο για τους ερευνητές καθώς τους επιτρέπει να αναλύουν τις συνθήκες που επικρατούν σε ένα δίκτυο και την απόδοσή του. Επίσης, επιτρέπουν την υλοποίηση ή την επαλήθευση κάποιων ιδεών που μπορεί να έχει ένας ερευνητής με σκοπό να μελετήσει τα αποτελέσματα αυτών των υλοποιήσεων. Γενικά, οι προσομοιωτές είναι λογισμικά που μοντελοποιούν διάφορα σενάρια χρησιμοποιώντας μια συγκεκριμένη προγραμματιστική γλώσσα και αυτό σου επιτρέπει να προσθέσεις ή να υλοποιήσεις τις δικές σου ιδέες σε ένα δίκτυο. Σχετικά με τους προσομοιωτές για την τεχνολογία Zigbee, υπάρχει ένας μεγάλος αριθμός από προσομοιωτές που να υποστηρίζουν την συγκεκριμένη τεχνολογία, από τους οποίους κάποιοι είναι πιο γνωστοί από άλλους, ενώ μερικοί έχουν ορισμένους περιορισμούς στα ασύρματα δίκτυα. Πιο κάτω θα περιγράψουμε τους υποψήφιους προσομοιωτές μαζί με τα πλεονεκτήματα του καθενός, αλλά κυρίως θα επικεντρωθούμε στα ζητήματα του γραφικού περιβάλλοντος του χρήστη, στην άδεια χρήσης του πηγαίου κώδικα και στην αποδοτικότητα του κάθε εργαλείου [19].

Έχοντας υπόψη τα πιο πάνω ζητήματα, ακολουθούν οι πιθανοί προσομοιωτές για την προσομοίωση του Zigbee και η σύγκριση τους με τον προσομοιωτή OPNET Modeler:

QualNet

Ο QualNet είναι ένας εμπορικός προσομοιωτής δικτύων που αναπτύχθηκε από την εταιρία SCALABLE Network Technologies. Παρέχει την δυνατότητα για προσομοιώσεις σε πραγματικό χρόνο καθώς και ζωντανά αποτελέσματα κατά την διάρκεια της προσομοίωσης. Επίσης, μπορεί να υποστηρίξει μέχρι 1000 κόμβους Zigbee, και το γραφικό του περιβάλλον επιτρέπει την εύκολη τοποθέτηση των κόμβων, καθώς και την απεικόνιση της υφιστάμενης κατάστασης του δικτύου. Τέλος, τα αποτελέσματα της προσομοίωσης μπορούν να εξαχθούν στη μορφή Extensible Markup Language (XML) που είναι μια εύκολη μορφή για την ανάλυση των αποτελεσμάτων. Όμως, επειδή ο προσομοιωτής είναι εμπορικός και έτσι απαιτείται η αγορά του, δεν τον επιλέξαμε για τα πειράματα μας.

NS-2 και NS-3

Ο Network Simulator 2 (NS-2) είναι ένας προσομοιωτής διακριτών γεγονότων ο οποίος διανέμεται δωρεάν, αφού είναι ανοικτού κώδικα και χρησιμοποιεί γραφικό περιβάλλον GUI το οποίον όμως δεν είναι εύκολο στη χρήση για τους αρχάριους. Αυτός ο προσομοιωτής περιλαμβάνει υλοποιημένα πρωτόκολλα, όπως το IEEE 802.15.4 και γι’ αυτό χρησιμοποιείται από πολλούς ερευνητές. Η νέα έκδοση του είναι ο NS-3 που δημιουργήθηκε το 2011, αλλά δεν παρέχει υλοποιημένα τα πρωτόκολλα που παρείχε ο προκάτοχός του και αυτό αποτελεί ένα από τα μειονεκτήματα του, αφού πρέπει να υλοποιηθούν ξανά τα πρωτόκολλα για τον νέο προσομοιωτή. Ακόμη, αν κάποιος υλοποιήσει ένα σενάριο στους NS-2 και 3 απαιτείται η μεταγλώττιση όλων των αρχείων του προσομοιωτή για να εκτελεστεί το σενάριο και έτσι αποφύγαμε αυτή την επιλογή λόγω έλλειψης αποδοτικότητας.

OMNeT++

Ο OMNeT++ είναι ένας ανοικτού κώδικα προσομοιωτής που αναπτύχθηκε από τον András Varga και την OpenSim Ltd και βασίζεται κυρίως σε ενότητες οι οποίες υλοποιούν ξεχωριστά διάφορα πρωτόκολλα και μπορούν τα κατεβούν από την ιστοσελίδα του δημιουργού. Το γραφικό περιβάλλον του είναι παρόμοιο με το γνωστό εργαλείο Eclipse και έτσι είναι πιο εύκολος ο προγραμματισμός στον προσομοιωτή. Η προγραμματιστική γλώσσα που χρησιμοποιεί είναι η C++ και μαζί με τις δομές που ήδη παρέχει το εργαλείο, κάποιος μπορεί να προγραμματίσει μια ενότητα σχετικά εύκολα. Όσον αφορά τα αποτελέσματα, το OMNeT++ παρέχει μηχανισμούς που επιτρέπουν την αποδοτική εξαγωγή στατιστικών για κάθε προσομοίωση που τρέχουμε και έτσι η δημιουργία των διαγραμμάτων και των γραφικών παραστάσεων είναι πιο εύκολη.

OPNET Modeler

Ο OPNET Modeler είναι ένας εμπορικός προσομοιωτής δικτύων που έχει αναπτυχθεί από την OPNET Technologies Inc. αλλά το 2012 έχει εξαγοραστεί από την Riverbed. Είναι ένας πολύ εξελιγμένος προσομοιωτής που σου δίνει την δυνατότητα για να σχεδιάσεις γρήγορα ένα σενάριο, να εξερευνήσεις μια τεράστια βιβλιοθήκη από παραδείγματα που έχουν ήδη υλοποιηθεί μαζί με τον πηγαίο κώδικα δημοφιλών πρωτοκόλλων, καθώς επίσης να εκτελείς παράλληλα πολλές προσομοιώσεις σε μηχανές με 2 ή περισσότερους επεξεργαστές. Τα πρωτόκολλα επικοινωνίας όπως το IPv6, TCP και το πρότυπο IEEE 802.15.4 που μας ενδιαφέρει, είναι ήδη υλοποιημένα. Επιπλέον, το OPNET παρέχει ένα εύκολο προς τον χρήστη γραφικό περιβάλλον το οποίον περιέχει αναλυτική περιγραφή του κάθε κόμβου και υποστηρίζει ρεαλιστικές ρυθμίσεις σύμφωνα με τα πρωτόκολλα και αυτός μαζί με τους προηγούμενους λόγους δίνει στο εργαλείο τη δημοσιότητα ανάμεσα στους ερευνητές έτσι ώστε να το χρησιμοποιούν τόσο για τα ενσύρματα δίκτυα όσο και στα ασύρματα. Από την άλλη, το κύριο μειονέκτημα του όσον αφορά την δική μας εργασία, είναι ότι ο πηγαίος κώδικας για το επίπεδο δικτύου (Network layer) και των εφαρμογών (Application layer) για το Zigbee δεν είναι διαθέσιμος και έτσι δεν μπορεί κάποιος να τροποποιήσει τις λειτουργίες σε αυτά τα επίπεδα της στοίβας.

Ο πιο κάτω πίνακας συγκεντρώνει τα πιο σημαντικά στοιχεία για τον κάθε προσομοιωτή και στη συνέχεια επιλέγουμε τον πιο κατάλληλο από αυτούς.

Κριτήρια	**OPNET**	**NS-2/3**	**OMNeT++**	**QualNet**
Άδεια χρήσης	Εμπορικό	Ανοικτού κώδικα	Ανοικτού κώδικα	Εμπορικό
Γραφικό περιβάλλον	Καλό- 2D	Πολύπλοκο- Tcl/tk	Περιβάλλον Eclipse	Καλό- 3D
Αποδοτικότητα	Ψηλή	Χαμηλή λόγω πλήρης μεταγλώττισης	Μόνο οι αλλαγές μεταγλωττίζονται	Ψηλή
Γλώσσα προγραμματισμού	Ρυθμίσεις στο GUI και εσωτερικά με C++	C++	C++	-

Σχήμα 5.1: Πίνακας σύγκρισης προσομοιωτών

Σύμφωνα με τον πιο πάνω πίνακα, οι προσομοιωτές που είναι εμπορικά διαθέσιμοι είναι πιο εξελιγμένοι από αυτούς που είναι ανοικτού κώδικα. Ο προσομοιωτής OPNET παρέχει δυνατότητα για λεπτομερή ανάλυση ενός πρωτοκόλλου και πλήρη υποστήριξη στον πηγαίο κώδικα μέσω σχολίων αλλά και εγγράφου προδιαγραφών και επεξηγήσεων, όπου αναλύει την κάθε παράμετρο και την λογική που είναι γραμμένος ο κώδικας. Παρόλα τα μειονεκτήματα που αναφέραμε προηγουμένως, αυτός ο προσομοιωτής υπερτερεί στα ζητήματα που είχαμε δει και αποτελεί ένα από τους πιο αξιόπιστους προσομοιωτές που υπάρχουν σε θέματα δικτύων. Ο πιο σημαντικός λόγος, όμως, που μας οδήγησε στο να επιλέξουμε να χρησιμοποιήσουμε το OPNET για να εκτελέσουμε τις προσομοιώσεις μας, είναι διότι έχει ήδη υλοποιημένη την τεχνολογία Zigbee μαζί με τον αλγόριθμο frequency agility και έτσι εξοικονομούμε χρόνο για περαιτέρω μελέτη των ζητημάτων των διάφορων τεχνολογιών.

5.2 Τροποποιήσεις στο μοντέλο Wireless Lan του OPNET Modeler

Πριν να προχωρήσουμε στην ανάλυση των σεναρίων που μελετήσαμε, θα περιγράψουμε την τροποποίηση που κάναμε στο μοντέλο του Wireless Lan στο OPNET Modeler. Το μοντέλο που υλοποιείται στον προσομοιωτή έχει την δυνατότητα επιλογής του επιθυμητού καναλιού που θα τρέχει το Access Point μαζί με τους χρήστες του. Σε αυτή την επιλογή υπάρχουν τα κανάλια 1 μέχρι 14 καθώς και η επιλογή Auto-assign. Η επιλογή Auto-assign μας δίνει την δυνατότητα να αφήσουμε τον simulator να αποφασίσει ο ίδιος ποιο κανάλι να αναθέσει σε κάθε AP. Δηλαδή, αν έχουμε δύο AP με διαφορετικά BSS σε ένα σενάριο και επιλέξουμε το Auto-assign, τότε ο προσομοιωτής θα αναθέσει αυτόματα ένα κανάλι στο κάθε AP. Ο αλγόριθμος που αναθέτει τα κανάλια είναι ο εξής: Ξεκινώντας από τα μη επικαλυπτόμενα κανάλια, ανάθεσε εκείνα που έχουν διάστημα 6 κανάλια μεταξύ τους, δηλαδή η σειρά για τα κανάλια της Ευρώπης είναι 1,7,13,6,12 και συνεχίζει μέχρι να χρησιμοποιηθούν όλα. Έχοντας υπόψη τον αλγόριθμο αυτό, εμείς δοκιμάσαμε να έχουμε δύο APs με διαφορετικά BSS όπου στο ένα επιλέξαμε χειροκίνητα το κανάλι 1 και στο άλλο επιλέξαμε το Auto-assign για να επιλεγεί αυτόματα το κανάλι. Όταν τρέξαμε την προσομοίωση, όμως, είδαμε πως το κανάλι στο 2ο AP ήταν το κανάλι 1 όπως και στο πρώτο AP. Αυτό το διορθώσαμε με την τροποποίηση του κώδικα που γίνεται ο αλγόριθμος του Auto-assign έτσι ώστε να λαμβάνει υπόψη του τα κανάλια που χρησιμοποιούν τα γειτονικά APs και να επιλέγει ένα διαφορετικό κανάλι που είναι διαθέσιμο για να μην προκαλέσουμε co-channel interference. Επίσης, εκτός από αυτή την τροποποίηση προσθέσαμε την δυνατότητα να εμφανίζεται μια γραφική παράσταση με τα κανάλια που χρησιμοποιούν τα APs στα σενάρια που τρέχουμε για να γνωρίζουμε καλύτερα ποια κανάλια ανατίθενται σε κάθε AP. Ο κώδικας των τροποποιήσεων βρίσκεται στο Παράρτημα Α.

5.3 Προσομοιώσεις στο εργαλείο OPNET Modeler

Το πρόβλημα της συνύπαρξης μεταξύ του Zigbee και του WiFi αποτελεί ένα αμφιλεγόμενο ζήτημα, διότι πολλοί ερευνητές υποστηρίζουν από την μια μεριά πως υπάρχει πράγματι πρόβλημα και χρειάζεται να πάρουμε κάποια μέτρα για να μειώσουμε το θέμα των παρεμβολών ανάμεσα στα συστήματα, ενώ από την άλλη μερικοί υποστηρίζουν πως το πρόβλημα που υπάρχει δεν είναι τόσο σοβαρό. Λαμβάνοντας υπόψη όλες αυτές τις έρευνες που υπάρχουν για το ζήτημα αυτό, στα πλαίσια της εργασίας μας θα ασχοληθούμε με την δημιουργία σεναρίων και την προσομοίωση δικτύων με συσκευές από τις δύο τεχνολογίες που αναφέραμε, ούτως ώστε να μελετήσουμε το πρόβλημα της παρεμβολής και να καταλήξουμε στα δικά μας συμπεράσματα. Κυρίως, θα μελετήσουμε το αν ο αλγόριθμος του frequency agility που υλοποιείται στο Zigbee έχει τα επιθυμητά αποτελέσματα που είναι η αποφυγή της παρεμβολής του WiFi και την βελτίωση της απόδοσης του δικτύου με την αλλαγή του καναλιού λειτουργίας του Zigbee. Για ευκολία, τον αλγόριθμο frequency agility θα τον αναφέρουμε ως FRQAG.

Τα σενάρια που δημιουργήσαμε για να μελετήσουμε τα διάφορα προβλήματα είναι τα ακόλουθα:

1. Συσκευές με τεχνολογία Zigbee μόνο (Zigbee_only)
2. Συσκευές με τεχνολογία Wifi μόνο (WiFi_only)
3. Συσκευές Zigbee να λειτουργούν στο κανάλι 26 με ενεργοποιημένο τον αλγόριθμο FRQAG, μαζί με συσκευές WiFi στο κανάλι 1 (zigbee vs wifi_agile and auto)
4. Συσκευές Zigbee να λειτουργούν στο κανάλι 26 με ενεργοποιημένο τον αλγόριθμο FRQAG, μαζί με συσκευές WiFi στο κανάλι 13 (zigbee vs wifi_agile and ch13)
5. Συσκευές Zigbee να λειτουργούν στο κανάλι 26 με απενεργοποιημένο τον αλγόριθμο FRQAG, μαζί με συσκευές WiFi στο κανάλι 13 (zigbee vs wifi_NOagile and ch13)
6. Συσκευές Zigbee να λειτουργούν στο κανάλι 26 με απενεργοποιημένο τον αλγόριθμο FRQAG, μαζί με συσκευές WiFi στο κανάλι 1 (zigbee vs wifi_NOagile and auto)
7. Δύο δίκτυα Zigbee να λειτουργούν στο κανάλι 26 και 25 με ενεργοποιημένο τον αλγόριθμο FRQAG (2 Zigbee agile)

8. Δύο δίκτυα Zigbee να λειτουργούν στο κανάλι 26 και 25 με ενεργοποιημένο τον αλγόριθμο FRQAG μαζί με 2 δίκτυα WLAN
9. Δύο δίκτυα Zigbee να λειτουργούν στο κανάλι 26 και 25 με ενεργοποιημένο τον αλγόριθμο FRQAG μαζί με 4 δίκτυα WLAN

Στα σενάρια 3 μέχρι 6 χρησιμοποιούμε αρχικά ένα δίκτυο Zigbee μαζί με ένα δίκτυο WLAN, ενώ στη συνέχεια προσομοιώνουμε το κτίριο της Πληροφορικής του Πανεπιστημίου Κύπρου το οποίον έχει 5 πτέρυγες και κάθε πτέρυγα έχει από 2 APs καθώς και από ένα δίκτυο Zigbee για να δούμε πώς είναι οι απόδοση σε ένα κτίριο με περισσότερα από ένα AP.

Τις προσομοιώσεις των σεναρίων με αριθμό 1 μέχρι 6 τις τρέξαμε για περίοδο 12 λεπτών. Οι ρυθμίσεις που χρησιμοποιήθηκαν στις συσκευές Zigbee φαίνονται παρακάτω:

Τοπολογία	Δέντρο
Αριθμός συσκευών	8 End devices, 3 Routers, 1 Coordinator
Data rate (Kbps)	250
Transmission power (W)	0.05W (Coordinator), 0.015W (Router), 0.001W (End device)
Channel sensing duration (seconds)	0.1 (Router), Auto-compute (End devices and Coordinator)
Packet reception threshold (dBm)	-85
Packet interarrival time (seconds)	exponential(0,125)
Packet size (bits)	constant(512)

Σχήμα 5.2: Πίνακας ρυθμίσεων Zigbee

Οι ρυθμίσεις που χρησιμοποιήθηκαν στις συσκευές WiFi φαίνονται παρακάτω:

Τοπολογία	Αστέρι
Αριθμός συσκευών	9 clients, 1 Access Point
WiFi technology	802.11g
Data rate (Mbps)	54
Transmission power (W)	AP:0,2 Client:0,002
Packet reception threshold (dBm)	AP: -71 Client: -79
Packet interarrival time (seconds)	AP:0,05 Client:0,0035

Σχήμα 5.3: Πίνακας ρυθμίσεων WiFi

Στα σενάρια που θα μελετήσουμε, θα συγκρίνουμε τις ακόλουθες μετρικές για ολόκληρο το δίκτυο:

Throughput: Το σύνολο των δεδομένων σε bits που φτάνουν επιτυχώς στο MAC layer όλων των κόμβων και μεταφέρονται στα ψηλότερη επίπεδα της στοίβας.

Load: Ο συνολικός όγκος δεδομένων σε bits που φτάνουν στα ψηλότερα επίπεδα της στοίβας πρωτοκόλλων σε ολόκληρο το δίκτυο.

Delay: Η καθυστέρηση από άκρο σε άκρο όλων των πακέτων που φτάνουν στο MAC layer σε όλους τους κόμβους.

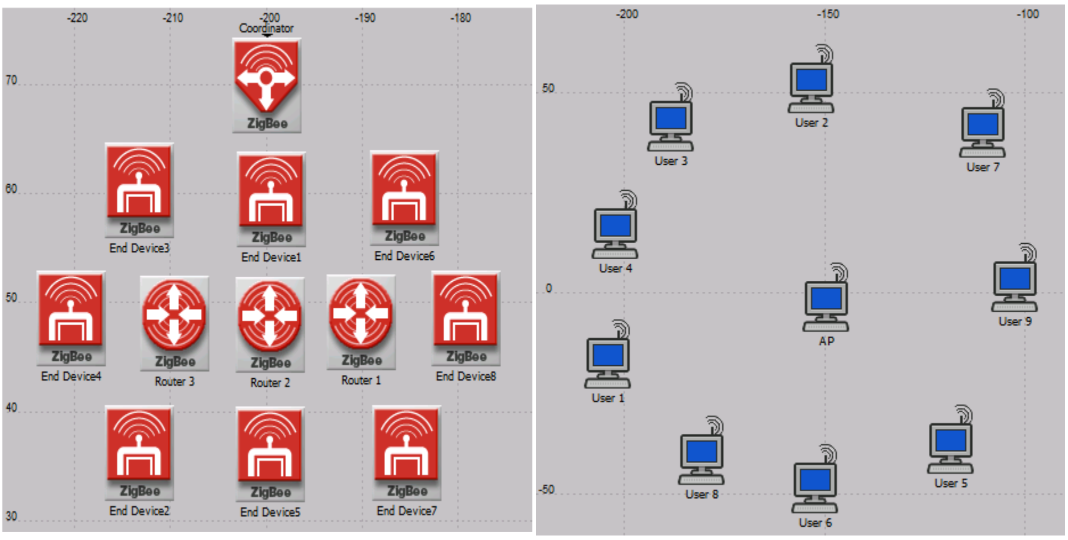
Data Dropped (Retry Threshold Exceeded): Τα δεδομένα των ψηλότερων επιπέδων που γίνονται drop από το MAC layer γιατί το MAC layer δεν έλαβε ACK από τους κόμβους και το όριο επανάληψης της αποστολής των δεδομένων έχει ξεπεραστεί.

Zigbee Transmission Failure Rate: Το ποσοστόν αποτυχίας των δεδομένων που διαδίδονται για τον Coordinator και τον κάθε router του Zigbee δικτύου. Αν αυτό το ποσοστό ξεπεράσει το 25%, τότε ο κόμβος θα στείλει ένα Interference Report το οποίον θα εκκινήσει τον αλγόριθμο FRQAG.

Operating Channel: Είναι το κανάλι που επιλέγει το AP στο WLAN και ο Coordinator στο Zigbee για να λειτουργήσει το δίκτυο και για να επικοινωνούν οι κόμβοι. Στην αρχή, στα πρώτα δύο σενάρια εκτελέσαμε τις συσκευές με τεχνολογία Zigbee και WiFi σε ξεχωριστά περιβάλλοντα και στα υπόλοιπα 4 σενάρια, αυτά τα δίκτυα τα τοποθετήσαμε μαζί στον ίδιο χώρο.

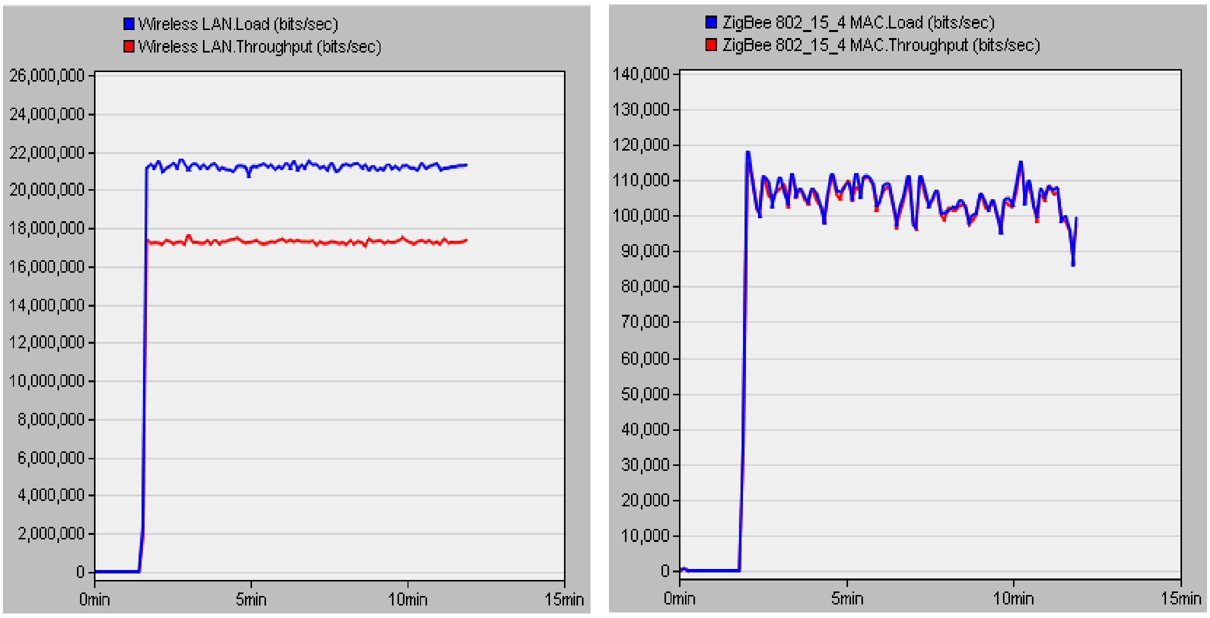
5.3.1 Σενάριο με απομονωμένες τις συσκευές WiFi και Zigbee (αρ. 1 και 2)

Σε αυτά τα σενάρια τα δίκτυα βρίσκονται μόνα τους σε ξεχωριστά σενάρια και δεν υπάρχουν οτιδήποτε παρεμβολές. Οι προσομοιώσεις έτρεξαν για 12 λεπτά συνολικά. Η διάταξη των συσκευών στον χώρο για τα δύο πρώτα σενάρια, όπως και οι αποστάσεις μεταξύ τους φαίνονται στα παρακάτω σχήματα.



Σχήμα 5.4: Διάταξη συσκευών Zigbee για το σενάριο αρ.1 (αριστερά) και WiFi για το σενάριο αρ.2 (δεξιά)

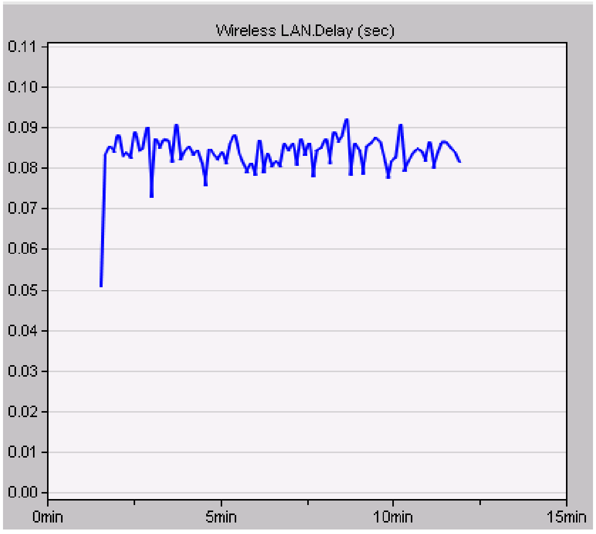
<u>Throughput και Load (bits/sec)</u>

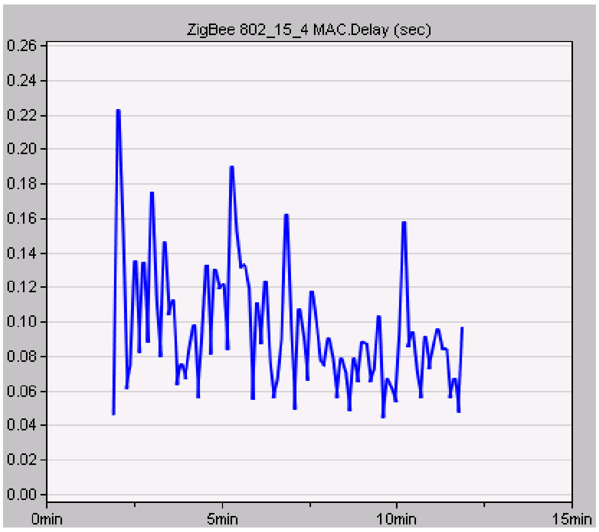


Πιο πάνω βλέπουμε τα αποτελέσματα του Throughput και του Load όταν τρέχουμε τα σενάρια με τις συσκευές WiFi και τις συσκευές Zigbee απομονωμένες χωρίς κάποια παρεμβολή. Αρχίζοντας από τα αριστερά, παρατηρούμε ότι το Load του WLAN αυξάνεται απότομα φτάνοντας γύρω στα 21 Mbits/sec και αυτό οφείλεται στο ότι ξεκινούν οι κόμβοι του δικτύου να στέλνουν δεδομένα στο 2^{o} λεπτό όπως τους ρυθμίσαμε. Παράλληλα, το throughput αυξάνεται μέχρι τα 17 Mbits/sec και άρα είναι μικρότερο από το Load, γιατί το traffic που στέλνεται δεν είναι μόνο δεδομένα αλλά και control traffic και άλλων ειδών πακέτα που απαιτούνται από το πρωτόκολλο. Παρόλα αυτά, κατά την διάρκεια της προσομοίωσης ο ρυθμός αυτός παραμένει στα ίδια επίπεδα και άρα δείχνει ότι το δίκτυο τρέχει συνεχώς χωρίς κάποιο πρόβλημα. Υπολογίζοντας πως το data rate στους κόμβους το ρυθμίσαμε στα 54 Mbps και το packet interarrival time έτσι ώστε να διακινούνται 20 packets/sec από τον AP και 286 packets/sec από κάθε client, κάνοντας τους υπολογισμούς το Load είναι το αναμενόμενο στα 21 Mbits/sec, ενώ αναμέναμε να είχαμε throughput περίπου 20-25 Mbps/sec αλλά όπως φαίνεται έχουμε μόνο 17 Mbits/sec λόγω πιθανών συγκρούσεων των πακέτων στο δίκτυο, αλλά και των διάφορων πακέτων ελέγχου που αναφέραμε με αποτέλεσμα να μειώνεται το throughput.

Στην δεξιά γραφική παράσταση παρατηρούμε το throughput του Zigbee να φτάνει στο $2^{ο}$ λεπτό στα 110 Kbits/sec, αλλά μετά να πέφτει περίπου στα 105 Kbits/sec. Η συμπεριφορά αυτή οφείλεται στο ότι στο $2^{ο}$ λεπτό ξεκινά το δίκτυο ο Coordinator και σταδιακά συνδέονται όλες οι συσκευές στο δίκτυο και αρχίζει να γίνεται η δρομολόγηση των πακέτων σύμφωνα με την τοπολογία του δέντρου. Στον υπόλοιπο χρόνο της προσομοίωσης, το throughput έχει κάποια σκαμπανεβάσματα, αλλά κυρίως παραμένει στα ίδια επίπεδα με τα αρχικά. Αυτές οι μικρές διαφορές στο throughput μπορεί να οφείλονται στο ότι οι routers είναι υπεύθυνοι για την επικοινωνία μεταξύ των End devices και Coordinator και σε μερικές στιγμές να μην μπορούν κάποιες χρονικές στιγμές έχουμε περισσότερα πακέτα από το κανονικό και έτσι οι κόμβοι δεν μπορούν να διαχειριστούν όλα τα πακέτα, με αποτέλεσμα να χάνονται κάποια από αυτά. Επίσης, βλέποντας το Load του δικτύου διακρίνουμε ότι ισούται με το throughput και άρα τα πλείστα δεδομένα που μεταφέρονται στο δίκτυο είναι χρήσιμα και δεν χάνονται. Τέλος, αν υπολογίσουμε πως τα Zigbee δημιουργούν 8 packets/sec, είναι φανερό πως το σύνολο των δεδομένων που μεταφέρονται στα δίκτυα WLAN είναι πολύ περισσότερα από αυτά του Zigbee.

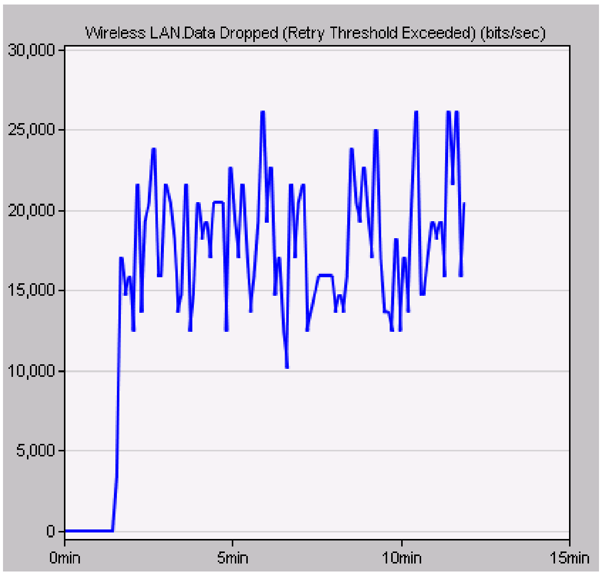
Delay (sec)

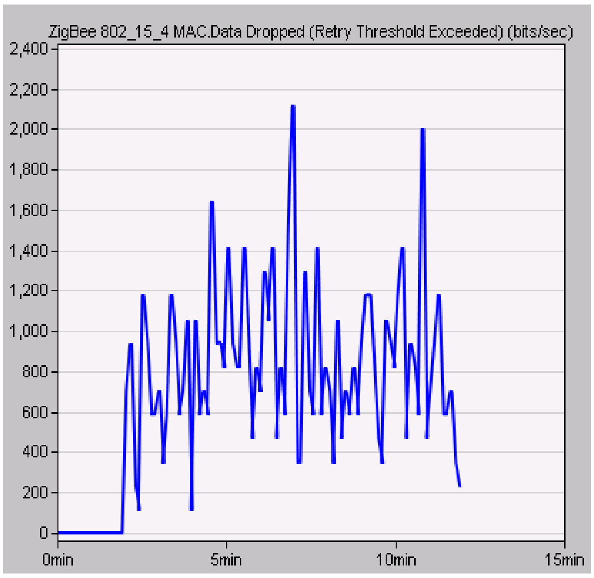




Στις πιο πάνω γραφικές βλέπουμε την καθυστέρηση που υπάρχει στα 2 δίκτυα κατά την διάρκεια των 12 λεπτών. Η γραφική του WLAN στα αριστερά μας λέει πως η καθυστέρηση περίπου στο δίκτυο είναι 85-90 ms και γενικά διατηρείται σε αυτά τα επίπεδα, χωρίς κάποια σημαντική διαφοροποίηση καθώς τρέχει η προσομοίωση. Από την άλλη, η γραφική δεξιά του Zigbee δείχνει ότι η καθυστέρηση έχει μια καθοδική τάση ξεκινώντας από τα 220 ms και φτάνει προς το τέλος της προσομοίωσης γύρω στα 80 ms. Η μεγάλη διαφορά καθυστέρησης στο δίκτυο με τις συσκευές Zigbee οφείλεται στο ότι το δίκτυο λειτουργεί με την τοπολογία δέντρου και έτσι τα πακέτα όλα πρέπει να περάσουν από τους routers όπου έχουν μεγάλο φόρτο για να διαχειριστούν και γι’ αυτό να παρουσιάζονται κάποιες καθυστερήσεις.

Data Dropped (Retry Theshold Exceeded) (bits/sec)

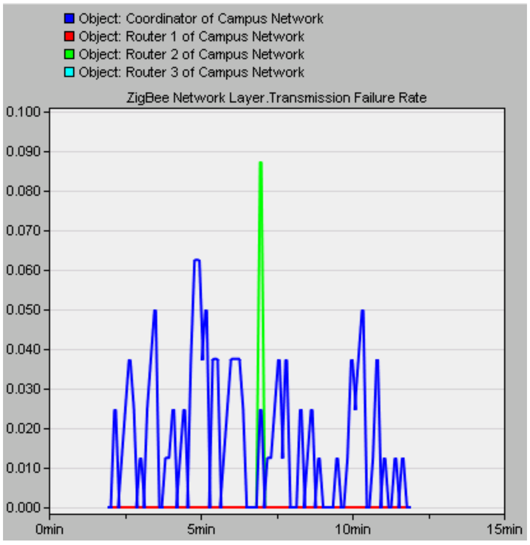




Σε αυτές τις γραφικές παραστάσεις βλέπουμε τα δεδομένα που χάνονται από τις δύο τεχνολογίες όταν ξεπεραστεί ο μέγιστος αριθμός αποτυχημένων προσπαθειών αποστολής των δεδομένων. Στην αριστερή γραφική βλέπουμε το WLAN να ξεκινά να χάνει δεδομένα 15 Kbits/sec και να συνεχίζει με αργό αλλά αυξητικό ρυθμό φτάνοντας το μέγιστο γύρω στα 25 Kbits/sec. Στη μεγαλύτερη διάρκεια της εκτέλεσης, όμως, έχει απώλειες 20 Kbits/sec που είναι πολύ χαμηλό σε σχέση με τον συνολικό αριθμό πακέτων που στέλνονται στο δίκτυο. Αν υπολογίσουμε πως έχουμε throughput όπως είδαμε στα 17 Mbits/sec και τα δεδομένα που χάνουμε 20 Kbits/sec, τότε έχουμε σχεδόν 0,11% απώλεια δεδομένων που είναι πολύ μικρή.

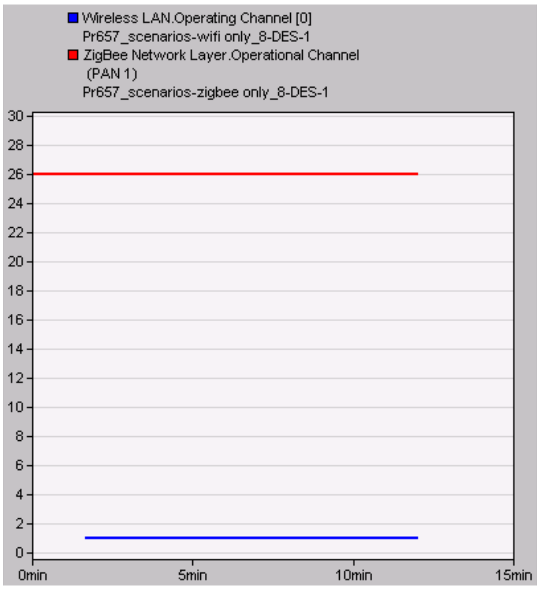
Από την γραφική του Zigbee στα δεξιά, βλέπουμε πως τα δεδομένα που χάνονται είναι αρχικά γύρω στα 800 bits/sec και φτάνουν μέχρι τα 2 Kbits/sec που σχετικά είναι πολύ λίγα σε σχέση με του WLAN. Αυτό το συμπεράναμε έχοντας υπόψη πως το throughput, όπως είδαμε είναι 105 Kbits/sec περίπου, τότε υπολογίζοντας βγάζουμε πως η απώλεια των δεδομένων είναι περίπου 1 με 2%. Άρα παρατηρούμε ότι τα δεδομένα που χάνονται στο Zigbee δίκτυο είναι περισσότερα σε σχέση με το WLAN αλλά γενικά είναι μικρά τα ποσοστά αφού είναι της τάξεως του 1% περίπου.

Zigbee Transmission Failure Rate (%)



Όσον αφορά το Zigbee , βλέπουμε την γραφική του ποσοστού αποτυχίας μετάδοσης των δεδομένων από τον Coordinator και τους 3 Routers του δικτύου. Συγκεκριμένα, παρατηρούμε ότι ο Coordinator είναι η μόνη συσκευή που έχει συνεχώς ένα ποσοστόν αποτυχίας που κυμαίνεται από 0,2% μέχρι 0,6% ενώ για τις υπόλοιπες συσκευές αυτό δεν ισχύει, αφού είναι στο μηδέν το ποσοστό με εξαίρεση τον Router 2 που έχει φτάνει μόνο μια στιγμή λίγο πάνω από το 0,8%. Δηλαδή, το ποσοστόν αποτυχίας είναι πολύ μικρό και γι’ αυτό δεν γίνεται κάποια αλλαγή καναλιού από τον αλγόριθμο του FRQAG, αφού για ενεργοποιηθεί ο αλγόριθμος το ποσοστόν πρέπει να φτάσει το 25% και τα πακέτα που έχουν σταλεί πρέπει είναι περισσότερα από 20.

Operating Channel των 2 τεχνολογιών

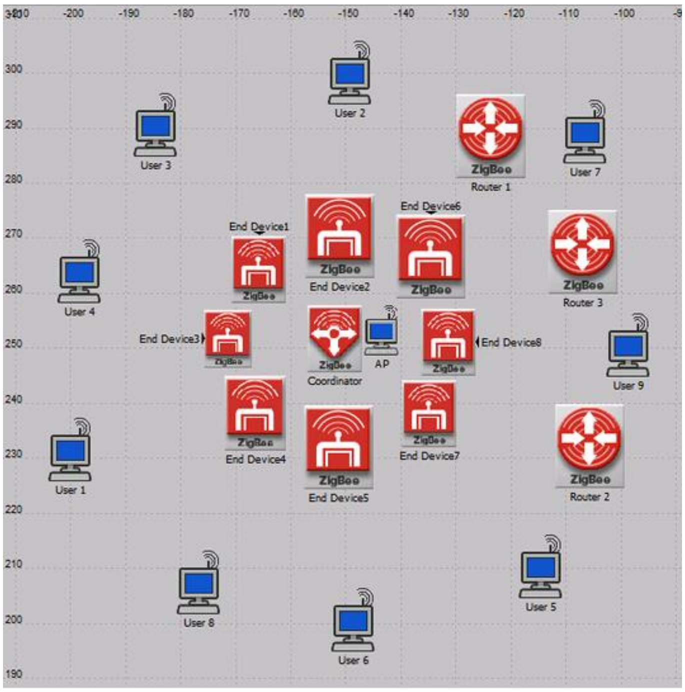


Τέλος, έχοντας περιγράψει τις μετρικές απόδοσης των δικτύων, αξίζει να αναφέρουμε πως το Zigbee λειτουργεί στο κανάλι 26 για το παρόν σενάριο, ενώ το WiFi λειτουργεί στο κανάλι 1. Από την στιγμή που δεν είναι μαζί οι δύο τεχνολογίες αυτό δεν παίζει ρόλο στο παρόν στάδιο, αλλά θα δούμε τα προβλήματα που δημιουργούνται στα σενάρια όπου συνυπάρχουν οι δύο τεχνολογίες στις επόμενες προσομοιώσεις.

Συμπεράσματα σεναρίου: Μέσα από την μελέτη των σεναρίων όπου τα δίκτυα Zigbee και WiFi υπάρχουν χωρίς άλλα δίκτυα μπορούμε να πούμε πως το Throughput στα δίκτυα WLAN είναι πάντα μικρότερο από τον φόρτο που υπάρχει στο δίκτυο, ενώ σχετικά με την καθυστέρηση, στο Zigbee είναι μεγαλύτερη και πιο ασταθής από αυτή του WiFi η οποία διατηρείται στα ίδια επίπεδα περίπου σε όλη την διάρκεια της προσομοίωσης. Τέλος, τα δεδομένα που χάνονται στο Zigbee είναι περισσότερα σε σχέση με το WiFi, αλλά και πάλι είναι μικρά ποσοστά της τάξεως του 1% περίπου.

5.3.2 Σενάρια συνύπαρξης Zigbee και WiFi (αρ. 3 μέχρι 6)

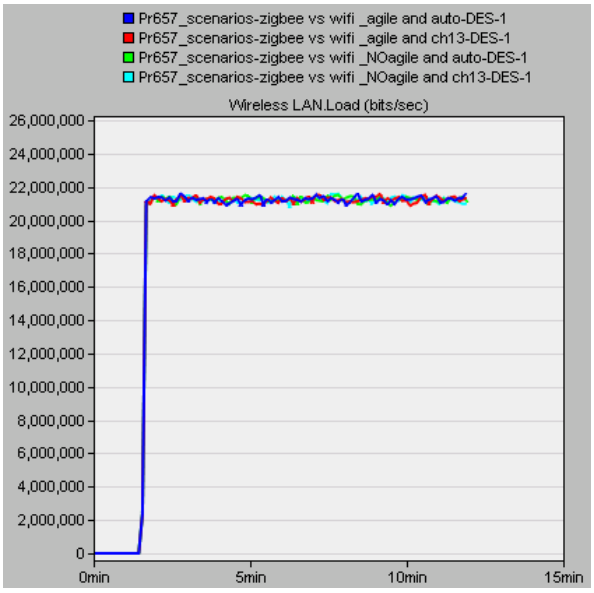
Στα σενάρια με αριθμό 3 με 6 έχουμε τοποθετήσει τα δύο πιο πάνω δίκτυα, Zigbee και WiFi, στον ίδιο χώρο μαζί για να δούμε κατά πόσο επηρεάζεται η απόδοσή τους όταν συνυπάρχουν. Δημιουργήσαμε διαφορετικά σενάρια όπου σε κάθε σενάριο ενεργοποιούμε ή απενεργοποιούμε τον αλγόριθμο FRQAG και προκαλούμε προβλήματα παρεμβολής με το να επιλέξουμε επικαλυπτόμενα κανάλια για τις δύο τεχνολογίες. Έτσι, συνολικά συγκρίνουμε 4 σενάρια όπου στα 2 έχουν ενεργοποιημένο τον FRQAG στο Zigbee και στα υπόλοιπα 2 είναι απενεργοποιημένος. Επίσης, αντίστοιχα πάλι στα 2 σενάρια το WLAN λειτουργεί στο κανάλι 13 και ενώ στα υπόλοιπα στο κανάλι 1. Πιο κάτω φαίνεται η διάταξη των συσκευών στο χώρο:

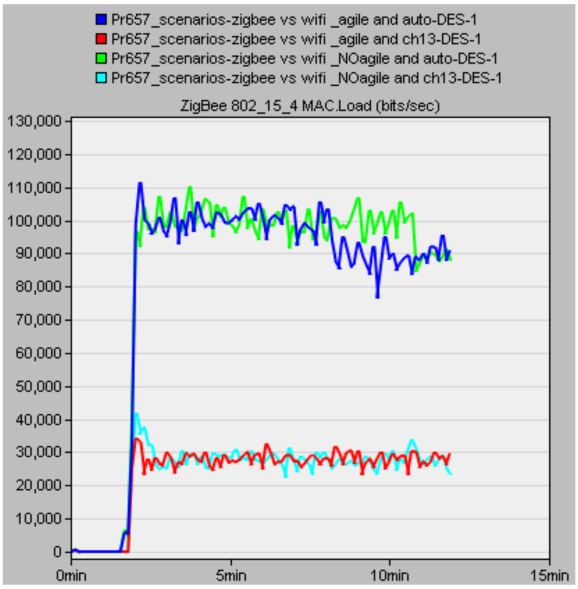


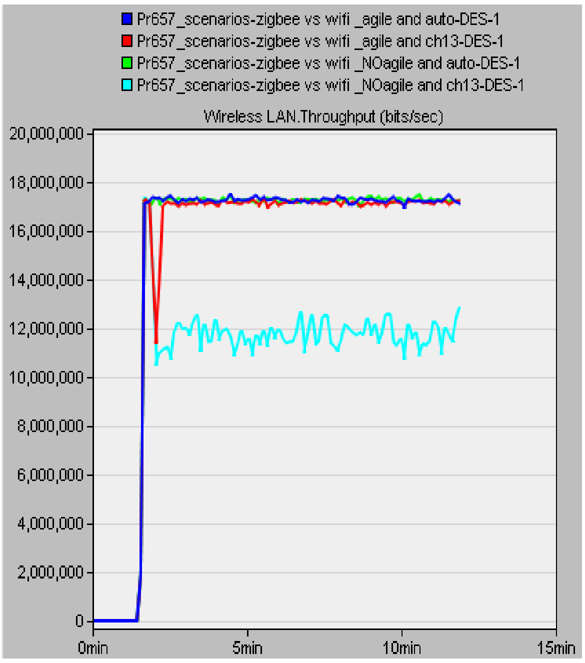
Σχήμα 5.5: Διάταξη συσκευών Zigbee και WiFi για το σενάριο με αρ.3 μέχρι 6.

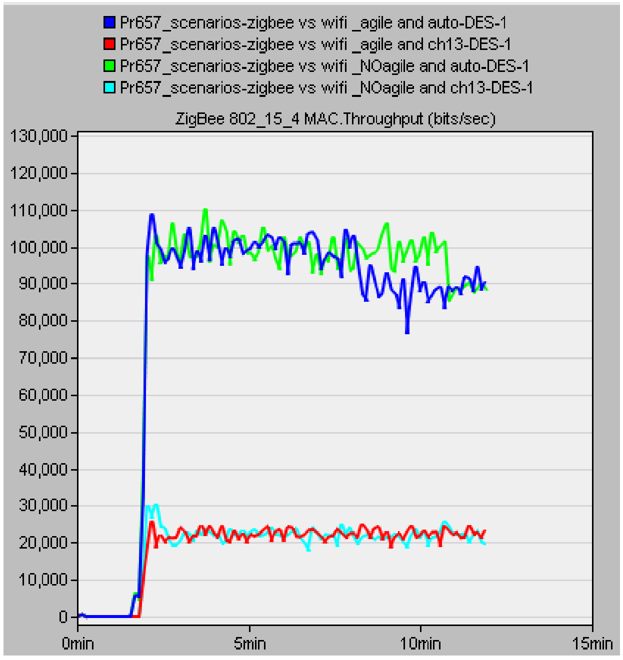
Αξίζει να αναφέρουμε πως οι αποστάσεις μεταξύ του AP και των clients είναι περίπου 50 m ενώ στο Zigbee τα End devices από τον Coordinator απέχουν 20 m ενώ από τους Router κυμαίνεται μεταξύ 20 m (κοντινές συσκευές) και 60 m (μακρινές συσκευές). Αυτές οι αποστάσεις όμως δεν αντιστοιχούν στην πραγματικότητα, όπου η απόσταση του Zigbee πρέπει να είναι περίπου 10 m, γιατί το transmission power των συσκευών στον προσομοιωτή δεν ανταποκρίνεται στις αποστάσεις που έχουμε στην πραγματικότητα. Αυτό προς το παρόν όμως δεν μας επηρεάζει γιατί έχουμε μόνο δύο δίκτυα που συνυπάρχουν χωρίς κάποια άλλα εμπόδια. Στα επόμενα σενάρια όπου θα έχουμε το κτίριο της Πληροφορικής του Πανεπιστημίου Κύπρου ρυθμίζουμε το transmission power για να περιορίζεται στην απόσταση που επιθυμούμε.

Throughput και Load (bits/sec)





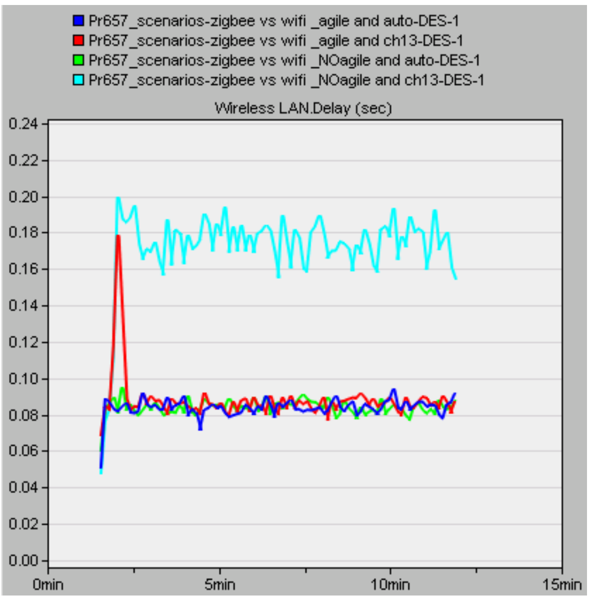


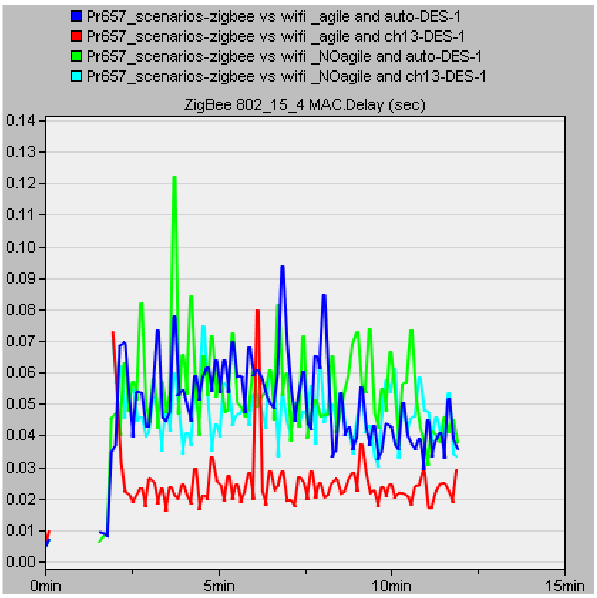


Στις πιο πάνω γραφικές βλέπουμε το Throughput και το Load των 4 σεναρίων μαζί για τις τεχνολογίες WiFi και Zigbee όταν συνυπάρχουν. Παρατηρώντας την αριστερή γραφική παράσταση που είναι το WiFi, φαίνεται πως το Load είναι για όλα τα σενάρια όπως αναμέναμε 21 Mbits/sec και παραμένει το ίδιο μέχρι το τέλος. Από την άλλη, το throughput στα 3 σενάρια είναι περίπου το ίδιο ενώ στο σενάριο όπου ο αλγόριθμος FRQAG είναι απενεργοποιημένος και το AP είναι στο κανάλι 13 τότε μειώνεται κατά πολύ. Συγκεκριμένα, στα σενάρια όπου δεν υπάρχει πρόβλημα παρεμβολής, δηλαδή σε εκείνα που το AP είναι στο κανάλι 1 και το Zigbee στο κανάλι 26, το throughput είναι στα 17 Mbits/sec και άρα δεν επηρεάζεται σχεδόν καθόλου από την παρουσία του Zigbee. Επίσης, στο σενάριο όπου ο αλγόριθμος FRQAG είναι ενεργοποιημένος και το AP είναι στο κανάλι 13 (κόκκινη γραμμή) έχουμε ελάχιστο επηρεασμό στο WiFi, γιατί ο αλγόριθμος του Zigbee ανιχνεύει έγκαιρα την ύπαρξη του WiFi και αλλάζει κανάλι, γι’ αυτό παρατηρείται μια απότομη γραμμή προς τα κάτω και μετά επανέρχεται στα κανονικά επίπεδα. Στην τελευταία περίπτωση, όπου έχουμε επικάλυψη του καναλιού 13 του WiFi με το κανάλι 26 του Zigbee (γαλάζια γραμμή), σημειώνεται μια μείωση του throughput στα 12 Mbits/sec, δηλαδή μειώνεται κατά 29% περίπου το throughput του WLAN. Να τονίσουμε ακόμη ότι το Throughput είναι κατά 4 Mbits/sec μικρότερο από το Load του δικτύου που σημαίνει πως τα δεδομένα που διακινούνται στο δίκτυο δεν είναι όλα χρήσιμα, όπως αναφέραμε και πριν, και υπάρχουν συγκρούσεις στο δίκτυο με αποτέλεσμα την διαφοροποίηση των 2 μετρικών αυτών.

Στην δεύτερη γραφική (στα δεξιά), βλέπουμε το throughput του Zigbee και παρατηρούμε πως στις περιπτώσεις που το AP είναι στο κανάλι 1 και το Zigbee στο κανάλι 26, άρα δεν έχουμε επικάλυψη καναλιών, το throughput είναι στα 100 Kbits/sec το μεγαλύτερο χρονικό διάστημα. Από την άλλη, στις περιπτώσεις που το AP είναι στο κανάλι 13 και το Zigbee στο κανάλι 26, ανεξάρτητα αν είναι ενεργοποιημένος ή όχι ο αλγόριθμος του FRQAG (γαλάζια και κόκκινη γραμμή), φαίνεται ότι το throughput παραμένει μειωμένο στα 22 Kbits/sec. Με άλλα λόγια, όταν υπάρχει πρόβλημα παρεμβολής και άρα το Zigbee και το WiFi χρησιμοποιούν επικαλυπτόμενα κανάλια, το throughput του Zigbee μειώνεται κατά 78%. Τέλος, να αναφέρουμε ότι το Load του δικτύου Zigbee είναι το ίδιο με το throughput και έτσι τα δεδομένα που διακινούνται στο δίκτυο είναι χρήσιμα και υπάρχουν ελάχιστες συγκρούσεις σε αυτό. Άρα, γενικά παρατηρούμε ότι το σενάριο που επηρεάζει και τις 2 τεχνολογίες είναι αυτό που είναι απενεργοποιημένος ο αλγόριθμος FRQAG και τα κανάλια των συσκευών είναι επικαλυπτόμενα και ως αποτέλεσμα έχουμε μείωση του throughput και στα δύο δίκτυα.

<u>Delay (sec)</u>



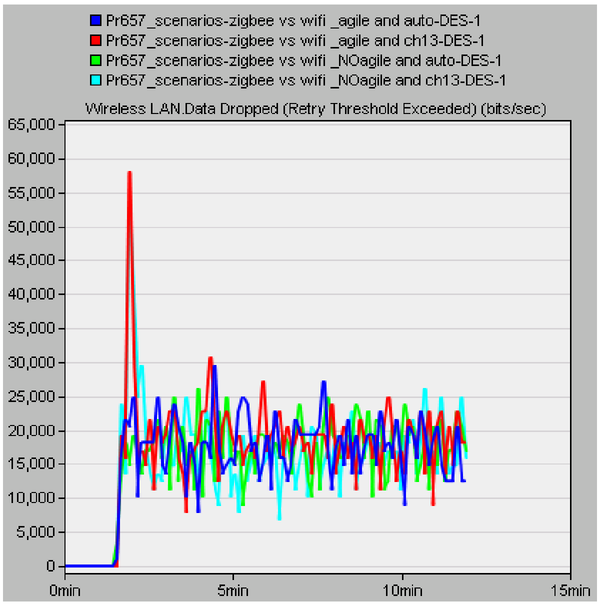


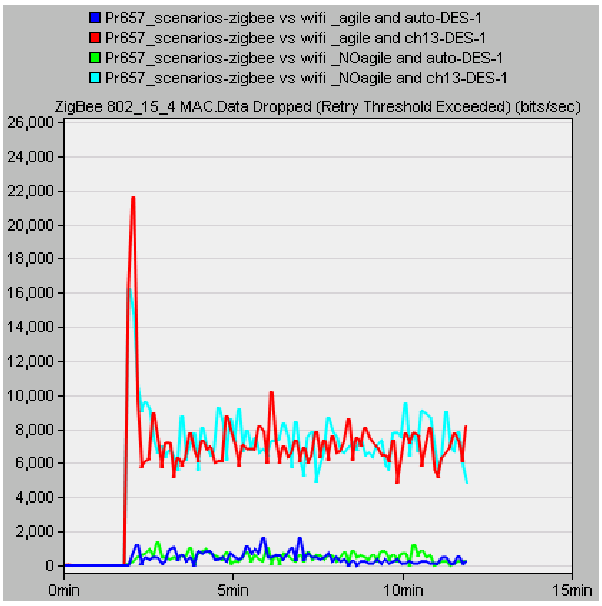
Εδώ θα δούμε πόση καθυστέρηση υπάρχει στο δίκτυο μας στα 4 σενάρια. Όπως φαίνεται στην αριστερή γραφική που είναι το WLAN, η μεγαλύτερη καθυστέρηση υπάρχει στο σενάριο όπου το AP είναι στο κανάλι 13 και το Zigbee στο κανάλι 26 με τον αλγόριθμο FRQAG να είναι απενεργοποιημένος (γαλάζια γραμμή) και έτσι προκαλείται παρεμβολή στα δύο συστήματα με αποτέλεσμα το WiFi να έχει περίπου 160 με 180 ms καθυστέρηση, δηλαδή αυξάνεται κατά 55% η καθυστέρηση. Στα υπόλοιπα 3 σενάρια, η καθυστέρηση που υπάρχει είναι σχεδόν σταθερή στα 90 ms εκτός από το σενάριο όπου το AP είναι στο κανάλι 13 και το Zigbee στο κανάλι 26 αλλά ο αλγόριθμος FRQAG είναι ενεργοποιημένος (κόκκινη γραμμή) και όταν ξεκινά η προσομοίωση έχουμε μια απότομη αύξηση στα 180 ms, αλλά όταν ο αλγόριθμος του Zigbee αλλάξει κανάλι και αποφύγει το WiFi στο $2^{ο}$ λεπτό, η καθυστέρηση επανέρχεται στα 90 ms όπως στα υπόλοιπα δύο σενάρια.

Βλέποντας την γραφική του Zigbee, παρατηρούμε ότι στα περισσότερα σενάρια η καθυστέρηση μεταβάλλεται μεταξύ των τιμών 40 ms με 60 ms. Στο σενάριο, όμως, όπου το AP είναι στο κανάλι 1 και το Zigbee στο κανάλι 26 με τον αλγόριθμο FRQAG είναι ενεργοποιημένος (πράσινη γραμμή) έχουμε μια κάποιες αυξομειώσεις που φτάνουν μέχρι τα 120 ms αλλά αυτό συμβαίνει μόνο μια φόρα σε όλη την διάρκεια. Από την άλλη, το σενάριο που φαίνεται να έχει την χαμηλότερη καθυστέρηση είναι όταν το AP είναι στο κανάλι 13 και το Zigbee στο κανάλι 26 με τον αλγόριθμο FRQAG να εκτελείται, όπως είπαμε και προηγουμένως, και να αλλάζει το κανάλι σε κάποιο που είναι ελεύθερο και γι’ αυτό έχουμε χαμηλή καθυστέρηση στα 20 ms σε όλη την διάρκεια της προσομοίωσης.

Αν τώρα συγκρίνουμε τις καθυστερήσεις σε αυτά τα σενάρια με τα πρώτα σενάρια του WiFi_only και του Zigbee_only, θα λέγαμε ότι στο WiFi δεν επηρεάζονται στα περισσότερα σενάρια εκτός από εκείνο όπου υπάρχει επικάλυψη στα κανάλια με το Zigbee και λόγω της παρεμβολής αυτής μεταξύ τους, αυξάνεται η καθυστέρηση στο δίκτυο. Όσον αφορά το Zigbee, η καθυστέρηση που υπάρχει όταν είναι μόνο του είναι πολύ περισσότερη σε σχέση με αυτά τα σενάρια.

Data Dropped (Retry Theshold Exceeded) (bits/sec)

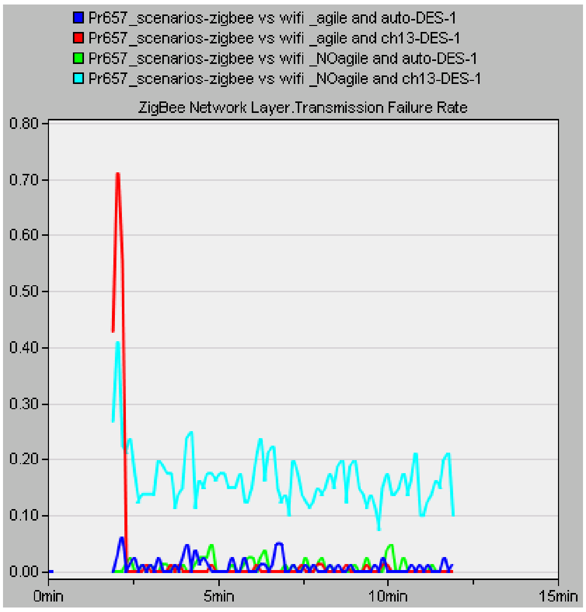




Στις γραφικές παραστάσεις αυτές βλέπουμε τα δεδομένα που χάνονται λόγω υπέρβασης του αριθμού προσπαθειών για αποστολή τους. Στα αριστερά φαίνεται το WLAN, όπου τα δεδομένα που χάνονται στα πλείστα σενάρια είναι περίπου στα 18 με 25 Kbits/sec εκτός από μια απότομη αύξηση στο σενάριο που έχουν επικάλυψη τα κανάλια (κόκκινη γραμμή) και χάνονται μέχρι 58 Kbits/sec αλλά επειδή λειτουργεί ο αλγόριθμος FRQAG αυτός ο ρυθμός μειώνεται δραματικά και πέφτει στα ίδια επίπεδα με τα άλλα σενάρια. Στη μεγαλύτερη διάρκεια της εκτέλεσης, όμως, όλα τα σενάρια έχουν απώλειες 20 Kbits/sec που είναι πολύ χαμηλό σε σχέση με τον συνολικό αριθμό πακέτων που στέλνονται στο δίκτυο. Αν υπολογίσουμε πως έχουμε throughput όπως είδαμε στα 17 Mbits/sec και τα δεδομένα που χάνουμε είναι 20 Kbits/sec, τότε έχουμε σχεδόν 0,12% απώλεια δεδομένων που είναι πολύ μικρή. Επίσης, για το σενάριο που έχουμε παρεμβολή στα κανάλια χωρίς τον αλγόριθμο FRQAG (γαλάζια γραμμή) όπου είχαμε throughput όπως είδαμε στα 12 Mbits/sec, χάνουμε 0,17% των δεδομένων που πάλι είναι μικρό ποσοστό αν υπολογίσουμε ότι χάνονται 20 Kbits/sec μόνο.

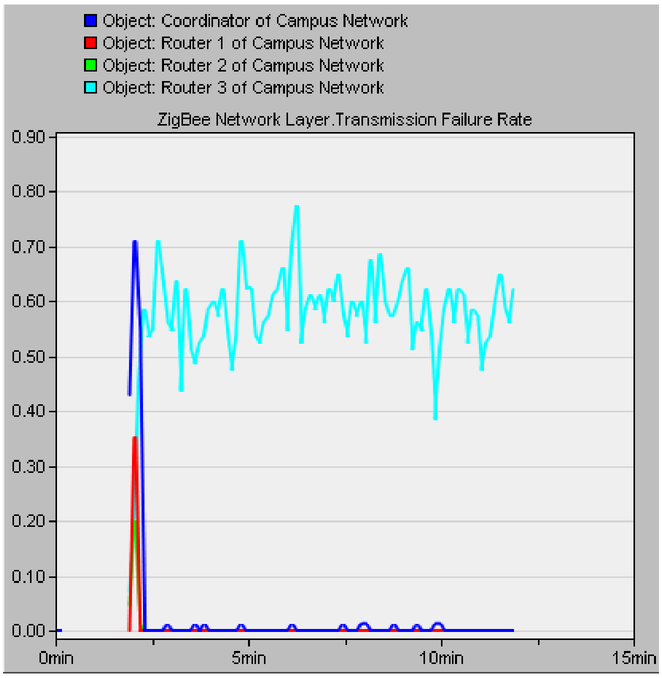
Από την γραφική του Zigbee στα δεξιά, βλέπουμε πως τα δεδομένα που χάνονται αρχικά φτάνουν γύρω στα 22 Kbits/sec για το σενάριο με τον FRQAG και το κανάλι 13 στο WLAN (κόκκινη γραμμή) ενώ παράλληλα φτάνει στα 16 Kbits/sec το σενάριο με τον FRQAG και το κανάλι 13 (γαλάζια γραμμή). Αυτά τα δύο σενάρια στη συνέχεια μειώνεται ο ρυθμός που χάνονται τα δεδομένα και σταθεροποιούνται στα 7 Kbits/sec. Ο λόγος που μειώνεται αυτός ο ρυθμός για το σενάριο με την κόκκινη γραμμή είναι γιατί αλλάζει κανάλι και αποφεύγει την παρεμβολή, ενώ στο 2^{ο} σενάριο με την γαλάζια γραμμή ο ρυθμός μειώνεται γιατί μειώνεται ο φόρτος των δεδομένων στο δίκτυο και έτσι οι κόμβοι στέλνουν λιγότερα δεδομένα. Τα υπόλοιπα 2 σενάρια, με πράσινη και μπλε γραμμή, έχουν κάτω από 2 Kbits/sec ρυθμό απώλειας δεδομένων γιατί τα κανάλια που λειτουργούν τα δύο δίκτυα δεν επικαλύπτονται και άρα δεν έχουμε παρεμβολές.

<u>Zigbee Network Layer: Transmission Failure Rate (%)</u>

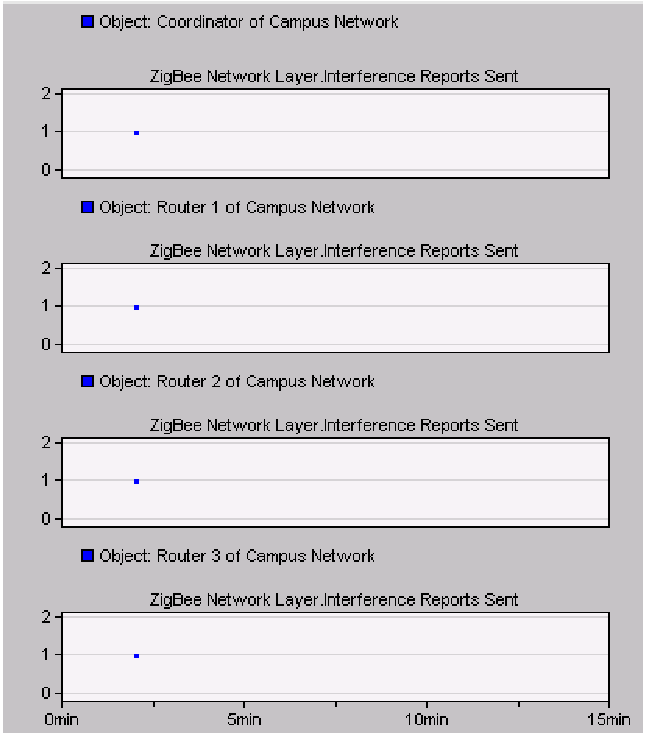


Η γραφική του ποσοστού αποτυχίας μετάδοσης των δεδομένων από τον Coordinator του δικτύου Zigbee μας δείχνει ότι στο σενάριο που το WLAN είναι στο κανάλι 13 και το Zigbee στο κανάλι 26 (κόκκινη γραμμή) το ποσοστό αποτυχίας ανεβαίνει μέχρι το 70% και μετά ξαφνικά μειώνεται στο μηδέν σχεδόν. Αυτό οφείλεται στο ότι το WiFi προκαλεί παρεμβολή στο Zigbee λόγω επικάλυψης των καναλιών λειτουργίας τους και το ποσοστό αποτυχίας του Coordinator ή των routers είναι πάνω από 25%, με αποτέλεσμα να στείλει ο κόμβος που αντιμετωπίζει πρόβλημα παρεμβολής ένα Interference Report και να μπει σε λειτουργία ο αλγόριθμος FRQAG. Στη δική μας περίπτωση και στο σενάριο που υπάρχει παρεμβολή μεταξύ των δύο τεχνολογιών (κόκκινη γραμμή), αρχικά ξεκινά ο Coordinator με ποσοστό μεγαλύτερο του 25% και μετά ακολουθεί ο Router 3, όπως βλέπουμε και στην πιο κάτω γραφική. Στη συνέχεια, ο Coordinator μαζί με τους Routers στέλνουν ένα Interference Report ανεξάρτητα από το ποσοστό αποτυχίας που έχουν, γιατί ρυθμίσαμε τον αλγόριθμο να είναι Active, δηλαδή ο Coordinator ζητά από τους υπόλοιπους Routers του δικτύου να στείλουν το Interference Report πριν να γίνει κάποια αλλαγή καναλιού όταν υπάρχει υπέρβαση του ποσοστού αποτυχίας όπως συμβαίνει εδώ. Έτσι, ο Coordinator όταν λάβει αυτές τις αναφορές, ο αλγόριθμος θα τρέξει και θα επιλέξει ένα κανάλι που έχει μικρότερη ενέργεια και άρα μικρότερη παρεμβολή από το WiFi. Στη γραφική που δείχνει το κανάλι λειτουργίας θα δούμε πως αλλάζει το κανάλι από το 26 στο 17.

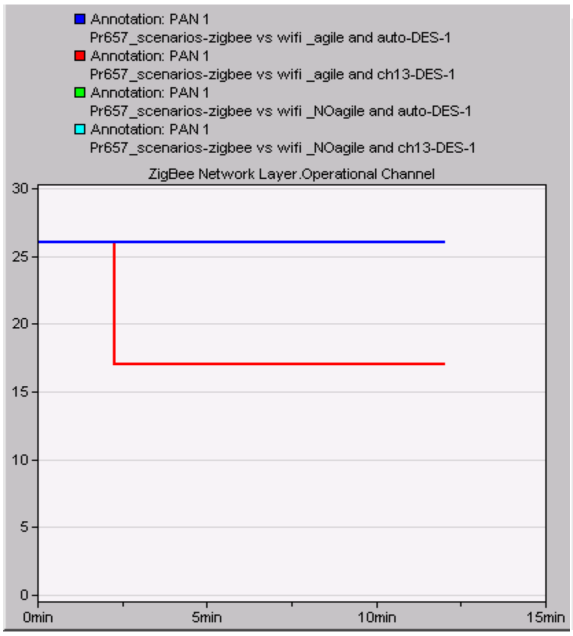
Στην ακόλουθη γραφική παράσταση βλέπουμε τα ποσοστά αποτυχίας μετάδοσης του Coordinator και των 3 Routers του δικτύου Zigbee κατά την διάρκεια της προσομοίωσης στο σενάριο που φαίνεται με την κόκκινη γραμμή. Αξίζει να τονίσουμε πως αν και ο Router 3 εξακολουθεί να έχει ποσοστό αποτυχίας πάνω από 60%, ο αλγόριθμος FRQAG δεν θα εκτελεστεί εκτός αν περάσουν 15 λεπτά σύμφωνα με τις προδιαγραφές του Zigbee. Επίσης, όπως φαίνεται μετά την αλλαγή του καναλιού τα ποσοστά των υπόλοιπων κόμβων έχουν μειωθεί στο μηδέν.

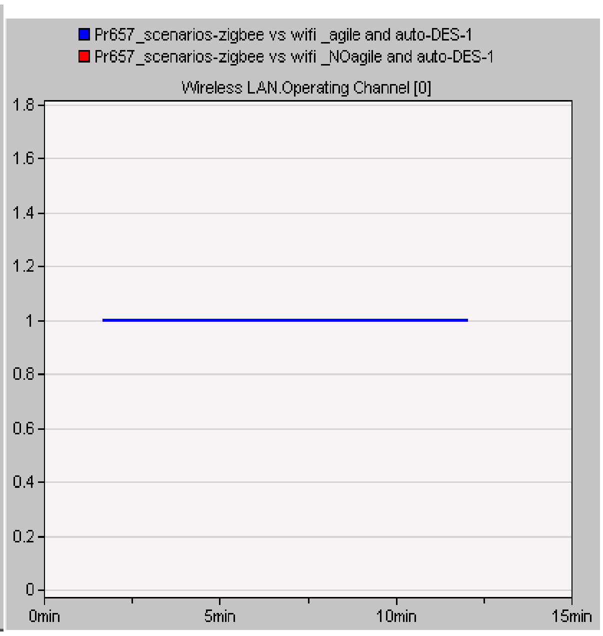


Πιο κάτω φαίνεται η αποστολή των Interference Reports από τους Routers και τον Coordinator του δικτύου μετά από την απαίτηση του Coordinator στο 2^{o} λεπτό περίπου της προσομοίωσης. Όπως είπαμε, η αποστολή των αναφορών γίνεται με βάση τον αλγόριθμο ανεξάρτητα από το ποσοστό αποτυχίας των μεταδόσεων της κάθε συσκευής.



<u>Operating Channel των 2 τεχνολογιών</u>





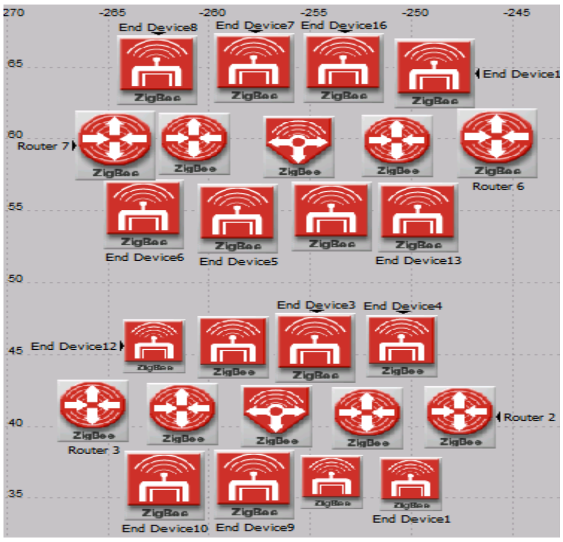
Στις πιο πάνω γραφικές βλέπουμε το κανάλι που λειτουργεί το κάθε δίκτυο της κάθε τεχνολογίας. Στα αριστερά φαίνεται το Zigbee στα 4 σενάρια όπου όλα λειτουργούν στο κανάλι 26 εκτός από το σενάριο με την κόκκινη γραμμή όπου λόγω της εκτέλεσης του αλγόριθμου FRQAG, αλλάζει το κανάλι λειτουργίας και μεταπηδά στο κανάλι 17. Αυτή η αλλαγή όπως είπαμε και προηγουμένως γίνεται γιατί υπάρχει παρεμβολή από το WiFi που εκπέμπει στο κανάλι 13 το οποίο επικαλύπτει το κανάλι 26 του Zigbee και έτσι το ποσοστό αποτυχίας των μεταδόσεων ξεπερνά το 25% στους κόμβους του δικτύου. Στην υπόλοιπη διάρκεια της προσομοίωσης το κανάλι παραμένει σταθερό στο 17 για το σενάριο αυτό και στο 26 για τα υπόλοιπα.

Όσον αφορά το WLAN, στα σενάρια που είναι αυτόματη η επιλογή του καναλιού, το κανάλι λειτουργίας που επιλέγεται είναι το 1 και στα 2 σενάρια αυτά ενώ στα άλλα 2 είναι το κανάλι 13 που το καθορίσαμε εμείς.

<u>Συμπεράσματα σεναρίων:</u> Σε αυτά τα σενάρια όπου τα δίκτυα Zigbee και WiFi συνυπάρχουν καταλήγουμε πως το Throughput στο WLAN μειώνεται κατά 29% ενώ του Zigbee κατά 78% στο σενάριο που έχουμε επικάλυψη των καναλιών λειτουργίας. Επίσης, σε αυτό το σενάριο αυξάνεται κατά 55% η καθυστέρηση του WLAN, ενώ στο Zigbee δεν έχουμε κάποια μεγάλη μεταβολή στην καθυστέρηση. Γενικά, παρατηρούμε ότι το σενάριο που επηρεάζει και τις 2 τεχνολογίες είναι αυτό που τα κανάλια των συσκευών είναι επικαλυπτόμενα και ως αποτέλεσμα έχουμε μείωση του throughput, την αύξηση της καθυστέρησης και την απώλεια δεδομένων και στα δύο δίκτυα.

5.3.3 Σενάριο με 2 Zigbee δίκτυα (αρ. 7)

Σε αυτό το σενάριο προσομοιάζουμε 2 δίκτυα Zigbee όταν βρίσκονται κοντά το ένα στο άλλο έτσι ώστε να δούμε κατά πόσο επηρεάζονται όταν λειτουργούν μαζί. Η διάταξη των συσκευών φαίνεται πιο κάτω:



Σχήμα 5.6: Διάταξη συσκευών Zigbee με αρ.7.

Αναθέσαμε σε κάθε Coordinator από ένα αριθμό στο πεδίο PAN το οποίο είναι μοναδικό και χρησιμοποιείται για την ένδειξη του δικτύου στις συσκευές που θα συνδεθούν. Κάθε δίκτυο αποτελείται από 4 Routers και 8 End devices. Οι ρυθμίσεις των συσκευών παραμένουν οι ίδιες όπως στα προηγούμενα σενάρια, με τον αλγόριθμο FRQAG να είναι ενεργοποιημένος αλλά η διαφορά είναι ότι η μεταβλητή Packet interarrival time (seconds) η οποία είναι exponential

(0,05) αντί 0,125 όπως είχαμε προηγουμένως. Πιο κάτω βλέπουμε το πώς σχηματίζονται τα δίκτυα με τις συσκευές τους:

<u>PAN 1:</u>

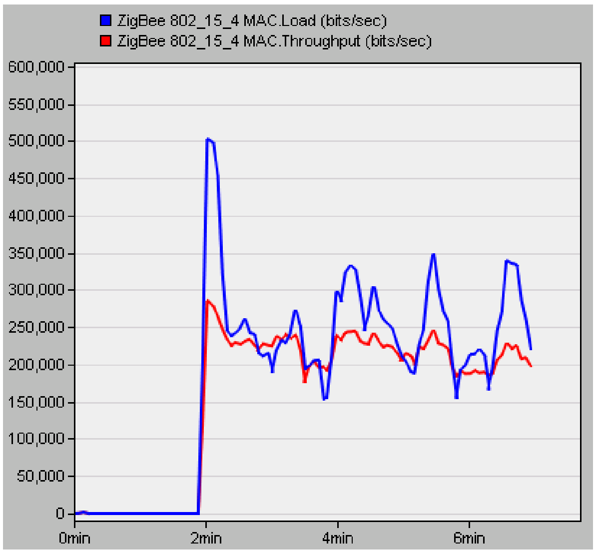
Coordinator	Depth 1	Depth 2
Campus Network.Coordinator (0)		
	Campus Network.Router 2 (1)	
		Campus Network.End Device3 (1092)
		Campus Network.End Device4 (1093)
	Campus Network.Router 3 (1094)	
		Campus Network.End Device11 (2185)
		Campus Network.End Device1 (2186)
	Campus Network.Router 1 (2187)	
		Campus Network.End Device2 (3278)
		Campus Network.End Device10 (3279)
	Campus Network.Router 4 (3280)	
	Campus Network.End Device12 (5466)	
	Campus Network.End Device9 (5467)	

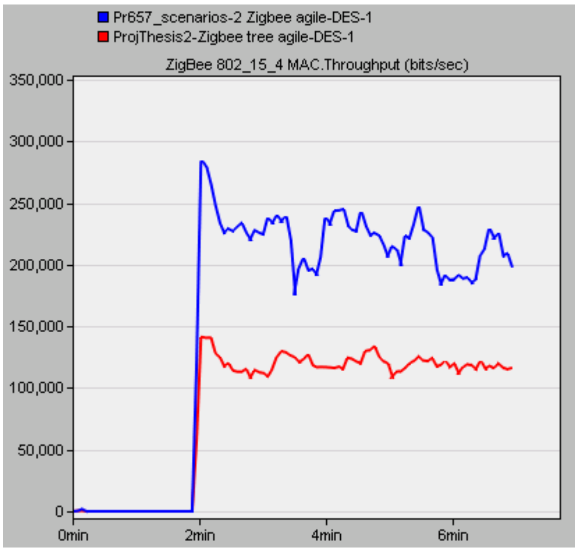
<u>PAN 2:</u>

Coordinator	Depth 1	Depth 2
Campus Network.Coordinator_PAN2 (0)		
	Campus Network.Router 7 (1)	
		Campus Network.End Device15 (1092)
		Campus Network.End Device5 (1093)
	Campus Network.Router 6 (1094)	
		Campus Network.End Device14 (2185)
		Campus Network.End Device7 (2186)
	Campus Network.Router 8 (2187)	
	Campus Network.Router 5 (3280)	
		Campus Network.End Device16 (4371)
		Campus Network.End Device13 (4372)
	Campus Network.End Device6 (5466)	
	Campus Network.End Device8 (5467)	

Θα μελετήσουμε τις μετρικές του Throughput, Load, Delay, Transmission Failure Rate και του Operational Channel όπως είχαμε και πριν, και θα τις συγκρίνουμε με ένα σενάριο όπου υπάρχει μόνο το ένα από τα δύο Zigbee δίκτυα. Τις προσομοιώσεις τις τρέξαμε για περίοδο 7 λεπτών.

<u>Throughput και Load (bits/sec)</u>



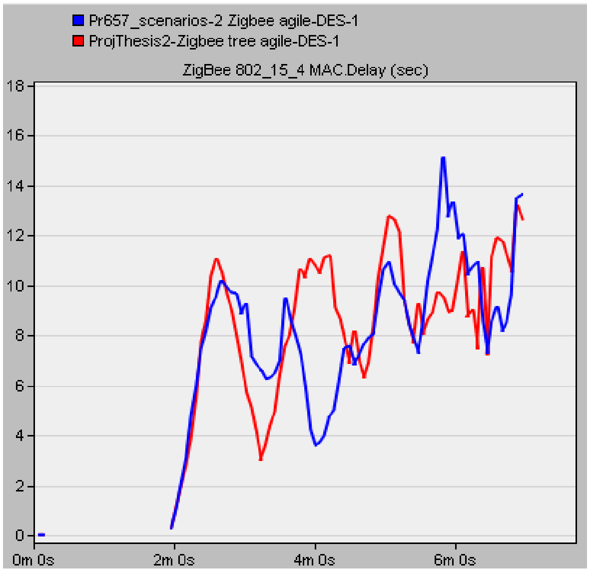


Στην αριστερή γραφική παράσταση, βλέπουμε το Throughput και το Load του Zigbee και παρατηρούμε πως το throughput είναι περίπου στα 200 Kbits/sec το μεγαλύτερο χρονικό διάστημα ενώ το Load είναι λίγο μεγαλύτερο, στα 250 Kbits/sec περίπου, με πολλά σκαμπανεβάσματα. Επίσης, στην αρχή έχουμε μια ραγδαία αύξηση στο Load που φτάνει στα 500 Kbits/sec και μετά πέφτει δραματικά στα 200 Kbits/sec. Ο λόγος είναι ότι στην αρχή έχουμε το αρχικό traffic που στέλνεται από όλες τις συσκευές για να βρουν τα μονοπάτια από τα End devices προς τους Routers και στον Coordinator αφού η τοπολογία είναι αστέρι και έτσι τα πακέτα πρέπει να περνούν πάντα από τους Routers ή τον Coordinator. Ακόμη, να πούμε ότι το Throughput είναι μικρότερο από το Load γιατί δημιουργούνται 20 packets/sec σε κάθε κόμβο και έτσι κάποια δεδομένα συγκρούονται με αποτέλεσμα τα χρήσιμα δεδομένα και αυτά που φτάνουν χωρίς πρόβλημα να είναι λιγότερα από τον συνολικό φόρτο του δικτύου.

Στην δεξιά γραφική παρατηρούμε την σύγκριση του Throughput στο σενάριο με 2 δίκτυα Zigbee (2 Zigbee agile- μπλε γραμμή) σε σχέση με το σενάριο με ένα δίκτυο Zigbee (Zigbee tree agile- κόκκινη γραμμή). Όπως είναι φανερό, το Throughput στο σενάριο όπου έχουμε ένα δίκτυο είναι περίπου στα 130 Kbits/sec και παραμένει σταθερό με ελάχιστες προσαυξήσεις κατά τη διάρκεια της προσομοίωσης, ενώ στο σενάριο με τα δύο δίκτυα το Throughput είναι σχεδόν διπλάσιο στα 200 Kbits/sec όπως είπαμε. Αυτό είναι αναμενόμενο, αφού οι συσκευές στο σενάριο Zigbee tree agile με 1 δίκτυο είναι οι μισές από ότι στο σενάριο που μελετάμε και στο οποίο έχουμε δύο δίκτυα και γι’ αυτό έχουμε διπλάσιο throughput.

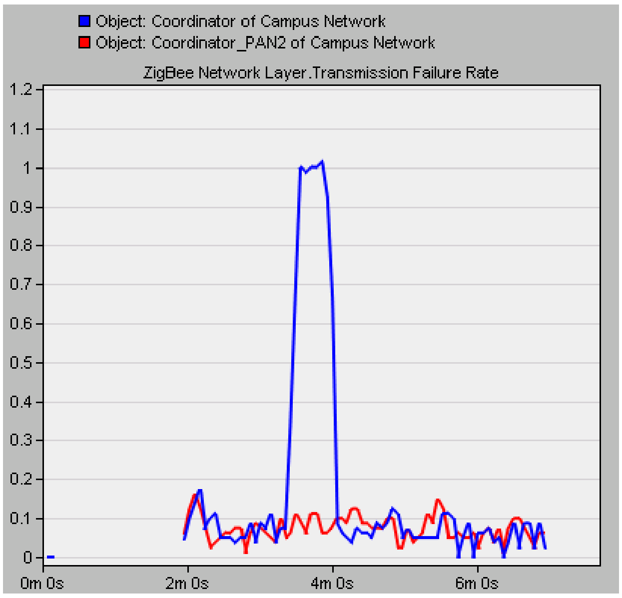
Τέλος, να προσθέσουμε ότι στο 6^{o} λεπτό βλέπουμε μια ξαφνική μείωση στο Throughput και Load στο σενάριο μας γιατί σε εκείνη την στιγμή, όπως θα δούμε και παρακάτω, θα γίνει μια αλλαγή καναλιού από τον αλγόριθμο FRQAG και έτσι θα έχουμε μείωση των χάσιμο κάποιων δεδομένων προσωρινά μέχρι να συντονιστούν όλες οι συσκευές στο νέο κανάλι.

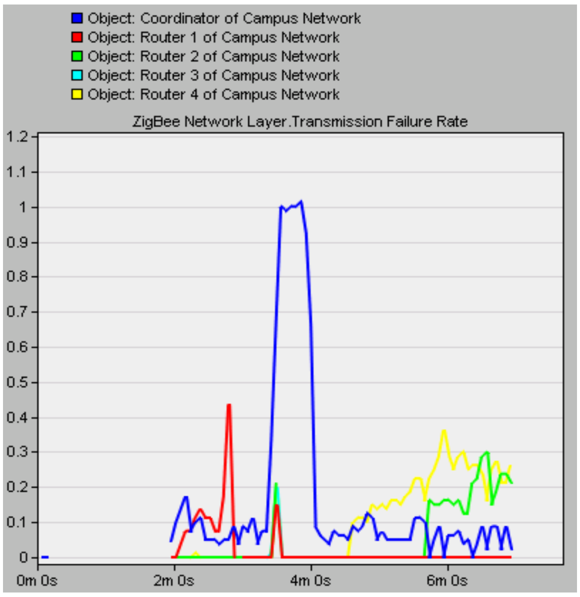
<u>Delay (bits/sec)</u>



Στην γραφική αυτή εικονίζεται η καθυστέρηση που υπάρχει στο σενάριο που μελετάμε (μπλε γραμμή) σε σύγκριση με το σενάριο που υπάρχει ένα δίκτυο Zigbee (κόκκινη γραμμή). Γενικά, μπορούμε να πούμε πως στο σενάριο με την μπλε γραμμή η καθυστέρηση έχει αυξητική τάση και κυμαίνεται μεταξύ 8 και 12 δευτερολέπτων με κάποιες εξαιρέσεις που μπορεί να πέσει μέχρι 7 δευτερόλεπτα αλλά και να αυξηθεί μέχρι τα 14 δευτερόλεπτα. Από την άλλη, στο σενάριο με 1 δίκτυο (κόκκινη γραμμή) η καθυστέρηση πάλι είναι αυξητική και κυμαίνεται μεταξύ 7 και 12 δευτερολέπτων αλλά πάλι υπάρχουν κάποια σκαμπανεβάσματα που πέφτει η καθυστέρηση μέχρι τα 3 δευτερόλεπτα και η μέγιστη τιμή είναι 13 δευτερόλεπτα. Επίσης, να επισημάνουμε ότι στο $6^{ο}$ λεπτό βλέπουμε μια ξαφνική μείωση στη καθυστέρηση στο σενάριο με την μπλε γραμμή και αυτό γίνεται διότι σε εκείνη την στιγμή όπως θα δούμε και παρακάτω, θα γίνει μια αλλαγή καναλιού από τον αλγόριθμο FRQAG και έτσι θα έχουμε μείωση της καθυστέρησης αφού θα πρέπει να αλλάξουν όλες οι συσκευές κανάλι και άρα θα χαθούν τα δεδομένα προσωρινά. Παρόλα αυτά, η τιμή της καθυστέρησης και στα 2 σενάρια είναι πολύ μεγάλη και αυτό οφείλεται στο ότι έχουμε ρυθμίσει να δημιουργούνται 20 packets/sec από κάθε κόμβο και έτσι δημιουργείται μεγάλος φόρτος στο δίκτυο με αποτέλεσμα κάποια δεδομένα να συγκρούονται ή να προσπαθούν να τα ξαναστείλουν οι κόμβοι και έτσι αυξάνεται η καθυστέρηση του δικτύου.

Zigbee Network Layer: Transmission Failure Rate (%)

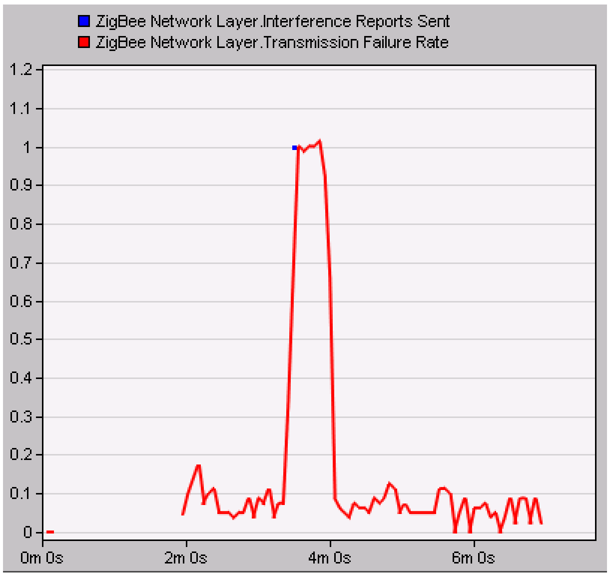


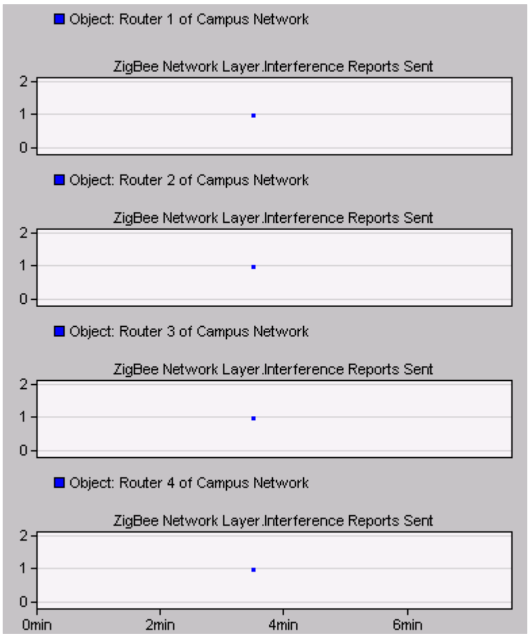


Εδώ βλέπουμε την γραφική του ποσοστού αποτυχίας μετάδοσης των δεδομένων από τους Coordinators και Routers του PAN 1 και PAN 2 των δικτύων Zigbee. Όπως φαίνεται ξεκάθαρα, σε ολόκληρη την χρονική διάρκεια της προσομοίωσης, οι δύο Coordinators έχουν κάτω από 25% αποτυχία μετάδοσης εκτός από μια περίοδο στο $3^{ο}$ με $4^{ο}$ λεπτό όπου ο

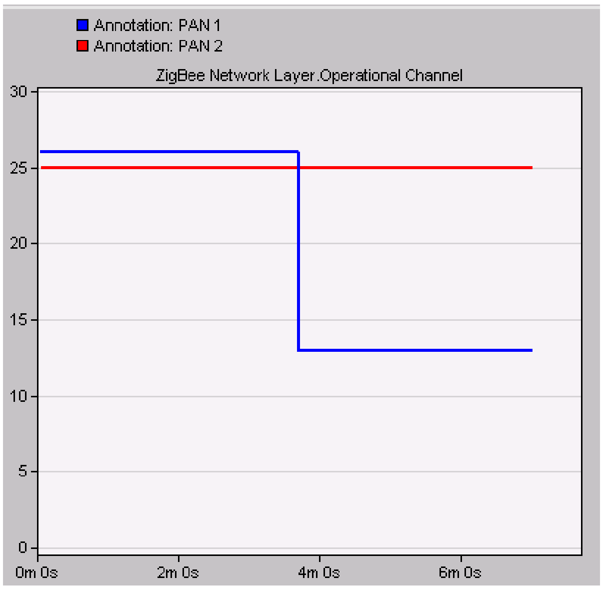
Coordinator του PAN 1 ξαφνικά έχει μια ραγδαία αύξηση φτάνοντας το 100% αποτυχίας μετάδοσης. Αυτό οφείλεται στο ότι τα δύο δίκτυα Zigbee παρεμβάλλονται μεταξύ τους επειδή λειτουργούν στα γειτονικά κανάλια 25 και 26 με αποτέλεσμα να προκαλείται πρόβλημα στο δίκτυο του PAN 1 κυρίως. Έτσι, αν παρατηρήσουμε τους Routers και τον Coordinator του PAN 1, το μεγαλύτερο ποσοστό αποτυχίας το έχει ο Coordinator στο 100% και ακολουθούν ο Router 1 στο 42%, ο Router 4 στο 35%, ο Router 2 στο 30%, και ο Router 3 στο 20%. Το ποσοστό αποτυχίας του Coordinator ή των routers σε μερικές στιγμές είναι πάνω από 25%, με αποτέλεσμα να στείλει ο κόμβος που αντιμετωπίζει πρόβλημα παρεμβολής ένα Interference Report και να μπει σε λειτουργία ο αλγόριθμος FRQAG. Στη δική μας περίπτωση, ο Router 1 είναι ο πρώτος που αντιμετωπίζει πρόβλημα παρεμβολής αλλά όπως θα δούμε δεν στέλνεται κάποιο Interference Report από τον κόμβο στον Coordinator. Η αιτία είναι διότι μόλις λίγα δευτερόλεπτα μετά την αύξηση του ποσοστού, ο κόμβος αποσυνδέεται από το δίκτυο και έτσι δεν προλαβαίνει να στέλνει κάποια αναφορά. Στη συνέχεια, ο Coordinator είναι αυτός που αντιμετωπίζει σοβαρό πρόβλημα και φτάνει το 100% του ποσοστού αποτυχίας και έτσι στέλνει Interference Report μόλις ξεπεράσει το 25% αλλά παράλληλα ζητά αναφορά από όλους τους Routers ανεξάρτητα από το ποσοστό αποτυχίας που έχουν, γιατί ρυθμίσαμε τον αλγόριθμο να είναι Active, δηλαδή ο Coordinator ζητά από τους υπόλοιπους Routers του δικτύου να στείλουν το Interference Report πριν να γίνει κάποια αλλαγή καναλιού όταν υπάρχει υπέρβαση του ποσοστού αποτυχίας όπως συμβαίνει εδώ. Έτσι, ο Coordinator όταν λάβει αυτές τις αναφορές, ο αλγόριθμος θα τρέξει και θα επιλέξει ένα κανάλι που έχει μικρότερη ενέργεια και άρα μικρότερη παρεμβολή από το γειτονικό δίκτυο Zigbee. Στη γραφική που δείχνει το κανάλι λειτουργίας θα δούμε πως αλλάζει το κανάλι από το 26 στο 13.

Στην ακόλουθη γραφική παράσταση βλέπουμε τα ποσοστά αποτυχίας μετάδοσης του Coordinator και την στιγμή που στέλνει την αναφορά του μόλις ξεπεραστεί το 25% ενώ στη δεξιά γραφική βλέπουμε τον χρόνο που στέλνουν τα Interference Report οι 4 Routers, που πως είπαμε ζητείται από τον Coordinator για να πάρει την απόφαση για αλλαγή καναλιού.





<u>Zigbee Operational Channel</u>



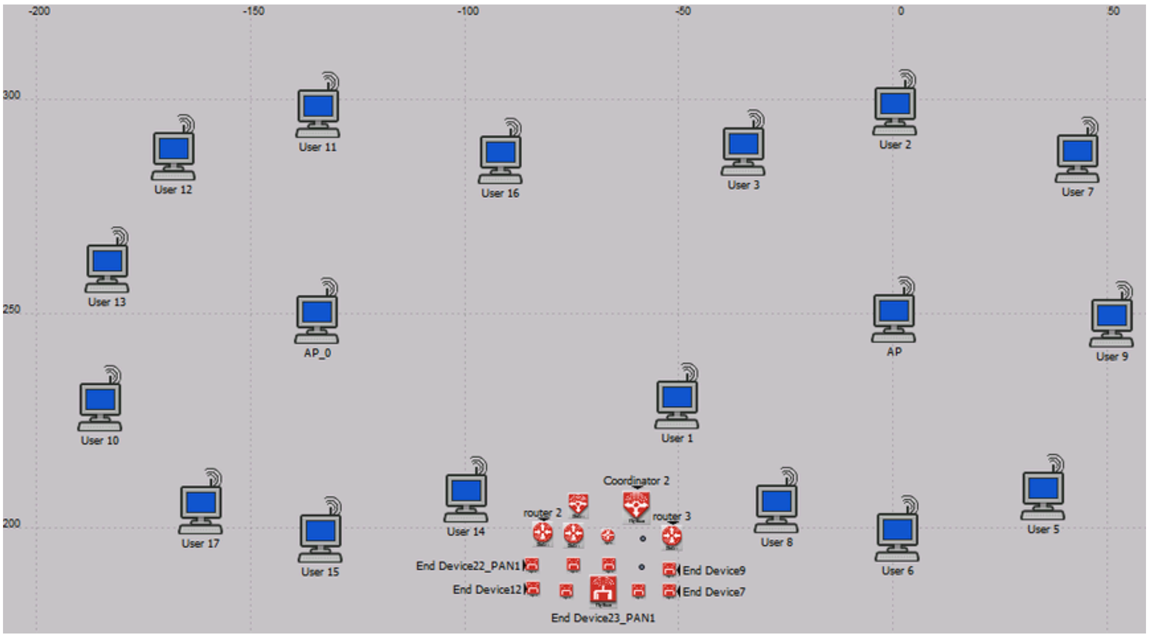
Στην γραφική αυτή βλέπουμε το κανάλι που λειτουργεί το κάθε δίκτυο Zigbee ανάλογα με τον αριθμό PAN. Με την μπλε γραμμή φαίνεται το δίκτυο PAN 1 το οποίο μέχρι το 3^{ο} λεπτό σχεδόν λειτουργεί στο κανάλι 26 ενώ μετά από το λεπτό αυτό αλλάζει στο κανάλι 13. Ο λόγος που αλλάζει κανάλι όπως είπαμε, είναι διότι ο Coordinator αντιμετώπιζε πρόβλημα παρεμβολής από το γειτονικό δίκτυο και έτσι με βάσει και τις αναφορές που πήρε από τους υπόλοιπους κόμβους άλλαξε κανάλι σε ολόκληρο το δίκτυο. Με την κόκκινη γραμμή φαίνεται το PAN 2 το οποίο λειτουργεί στο κανάλι 25 μέχρι το τέλος της προσομοίωσης.

<u>Συμπεράσματα σεναρίων:</u> Στα σενάρια που μελετήσαμε όπου τα 2 δίκτυα Zigbee συνυπάρχουν, βλέπουμε πως το δημιουργείται μεγάλος φόρτος στο δίκτυο με αποτέλεσμα

κάποια δεδομένα να συγκρούονται ή να προσπαθούν να τα ξαναστείλουν οι κόμβοι και έτσι αυξάνεται η καθυστέρηση του δικτύου καθώς επίσης και να έχουμε 100% αποτυχία μετάδοσης από τον Coordinator του ενός δικτύου και άρα να αλλάζει κανάλι λειτουργίας. Άρα, ο αλγόριθμος FRQAG χρησιμεύει και σε αυτές τις περιπτώσεις αφού τα 2 δίκτυα Zigbee μαζί μπορεί να έχουν παρεμβολές μεταξύ τους και έτσι να λειτουργούν σε απομακρυσμένα κανάλια.

5.3.4 Σενάριο με 2 δίκτυα Zigbee μαζί με 2 δίκτυα WLAN (αρ. 8)

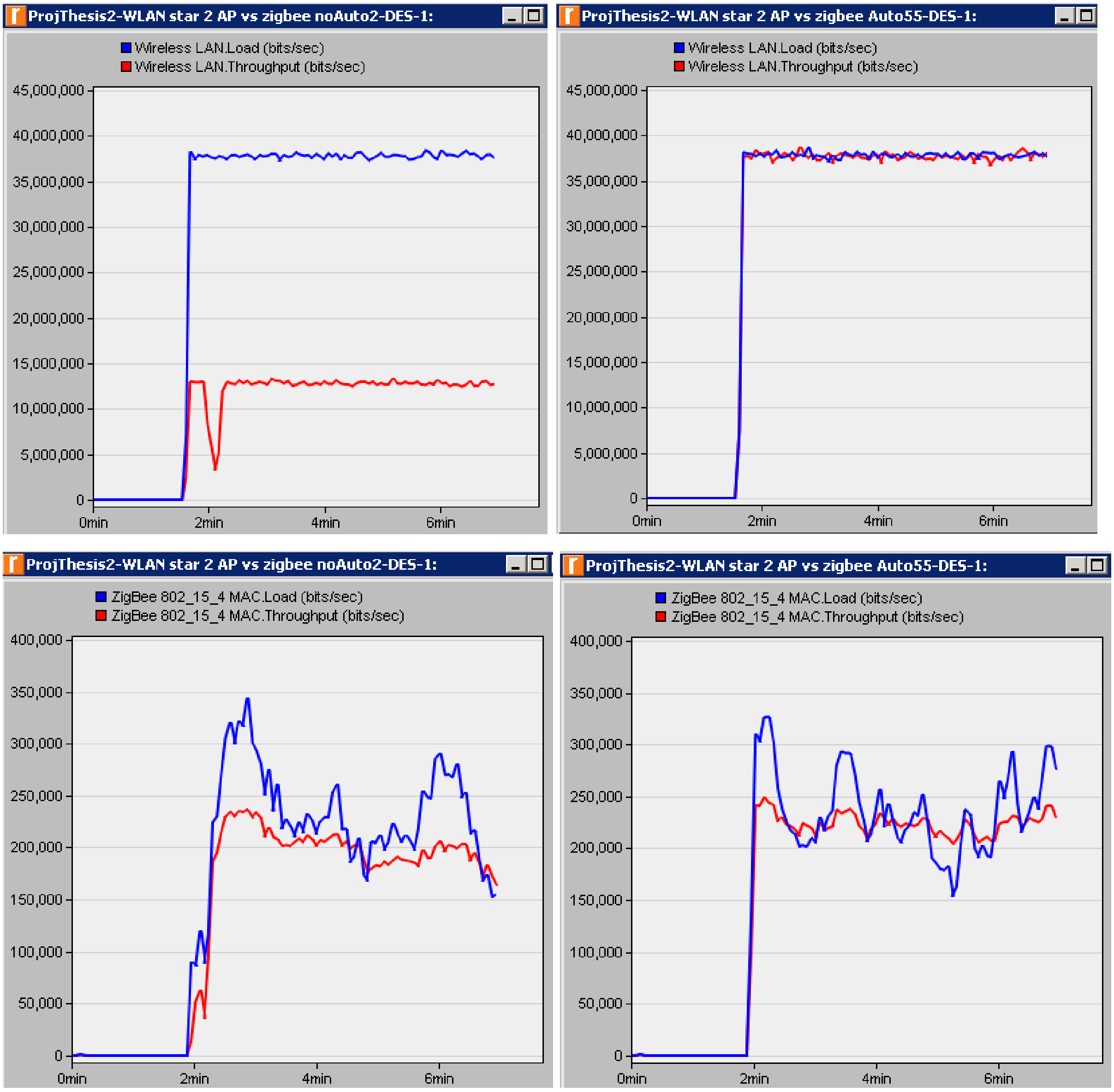
Σε αυτό το σενάριο μελετούμε την επίδραση του WLAN στο Zigbee όταν υπάρχουν δύο AP μαζί με ένα δίκτυο Zigbee. Επίσης, στα δύο AP στη μια προσομοίωση βάλαμε τα κανάλια 1,7 αντίστοιχα ενώ στην άλλη προσομοίωση βάλαμε το κανάλι 13 και στα δύο AP για να δούμε την διαφορά στην απόδοση του Zigbee όπως και στο WLAN λόγω του co-channel interference που δημιουργείται. Το κανάλι του Zigbee είναι το 26.



Σχήμα 5.7: Διάταξη συσκευών Zigbee και WiFi για το σενάριο με αρ.8.

Στη συνέχεια θα περιγράψουμε τα αποτελέσματα των μετρικών που αναφέραμε και σε προηγούμενα σενάρια, καθώς και συγκρίσεις των προσομοιώσεων που έχουν ίδιο κανάλι στα AP και όταν έχουν διαφορετικό.

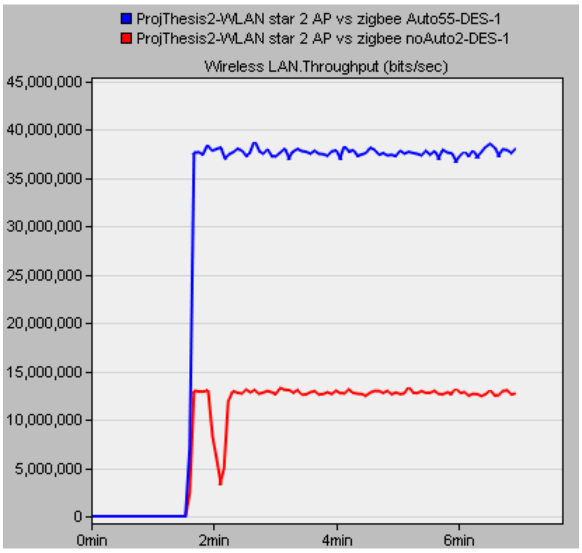
Throughput και Load (bits/sec)

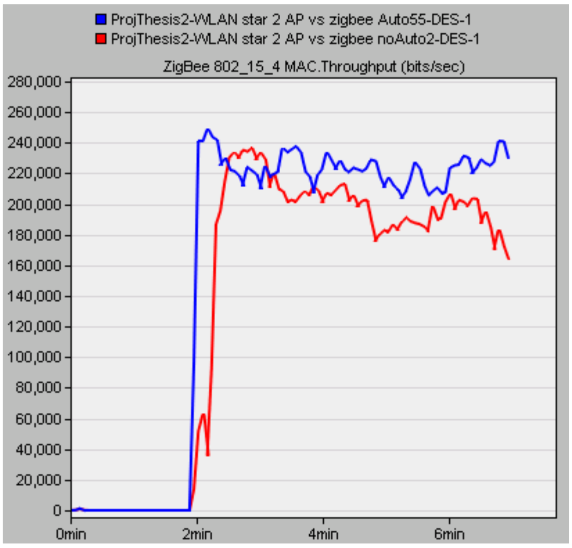


Στις γραφικές της πρώτης γραμμής φαίνονται το Throughput και το Load για το WLAN στο σενάριο που μελετούμε ενώ στην κάτω γραμμή φαίνονται οι ίδιες μετρικές για το Zigbee. Ξεκινώντας από τις γραφικές του WLAN βλέπουμε ότι στο σενάριο *"WLAN star 2 AP vs zigbee noAuto2"* (αριστερή γραφική) όπου το κανάλι στα δύο AP είναι το 13, το Throughput είναι στα 13 Mbits/sec και διατηρείται εκεί κατά την διάρκεια της προσομοίωσης. Από την άλλη, το Load είναι στα 38 Mbits/sec και βλέπουμε πως η διαφορά είναι μεγάλη και ο λόγος είναι διότι τα δύο AP έχουν το ίδιο κανάλι με αποτέλεσμα να προκαλείται co-channel interference και έτσι να μειώνονται τα δεδομένα που είναι χρήσιμα στο δίκτυο αφού προκύπτουν συγκρούσεις των πακέτων και τα περισσότερα χάνονται. Στο ίδιο σενάριο, παρακολουθώντας τη γραφική του Zigbee (κάτω αριστερά), βλέπουμε το Load να έχει μια μεγάλη αύξηση μέχρι το 3^{ο} λεπτό όπου φτάνει τα 350 Kbits/sec και στην συνέχεια ακολουθεί για πτωτική τάση φτάνοντας στα 180 Kbits/sec αλλά και πάλι έχει μια αυξομείωση που στο τέλος καταλήγει στα 150 Kbits/sec χαμηλότερο σημείο. Το Throughput όμως δεν ακολουθεί αυτή την πορεία αλλά παραμένει σχεδόν σταθερό μεταξύ του 180 και 220 Kbits/sec. Η συμπεριφορά του Load οφείλεται στην παρεμβολή που προκαλούν τα δύο APs που λειτουργούν στο ίδιο κανάλι με αποτέλεσμα εκείνες τις στιγμές που σημειώνεται μείωση να αποσυνδέονται κάποιοι κόμβοι από το δίκτυο του Zigbee και να στέλνονται λιγότερα δεδομένα.

Στην δεξιά γραφική του WLAN τώρα, στο σενάριο *"WLAN star 2 AP vs zigbee Auto55"* (δεξιά γραφική) βλέπουμε ότι τα δύο AP μεταξύ τους δεν επηρεάζονται αφού τα κανάλια τους είναι το 1 και 7 και έτσι δεν έχουμε κάποια διαφοροποίηση μεταξύ του Throughput και του Load αφού είναι και τα δύο στα 38 Mbits/sec. Σχετικά με το Zigbee, σε αυτό το σενάριο (κάτω δεξιά) φαίνεται ότι το Load έχει κάποιες προσαυξήσεις μεγαλύτερες σε σχέση με το Throughput το οποίο κυμαίνεται στα 220 με 240 Kbits/sec. Το Load, όπως είπαμε, αυξάνεται μέχρι τα 330 Kbits/sec κάποιες στιγμές ενώ άλλες πέφτει μέχρι τα 155 Kbits/sec και έτσι υπάρχει μια διαφορά με το Throughput που σημαίνει πως κάποια δεδομένα χάνονται στο δίκτυο μας.

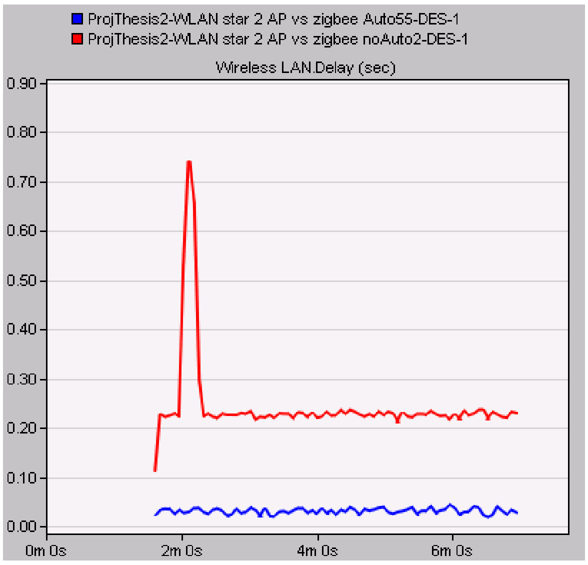
- Σύγκριση Throughput WLAN και Zigbee:

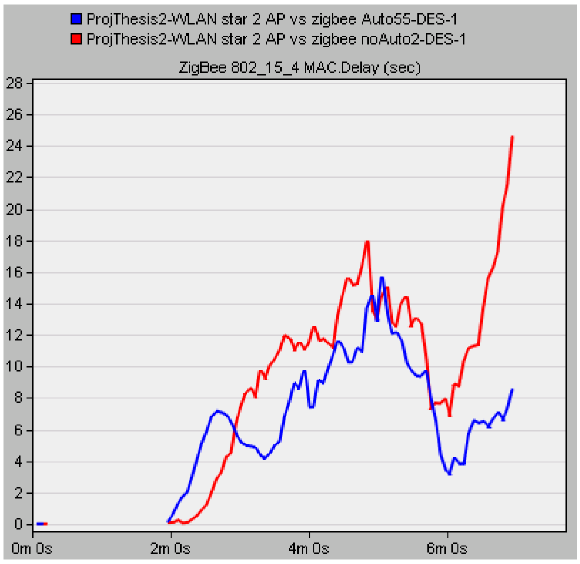




Έχοντας υπόψη τα πιο πάνω που αναφέραμε, εδώ βλέπουμε μια σύγκριση του Throughput των δύο σεναρίων για τις δύο τεχνολογίες. Είναι φανερό πως στο WLAN στο σενάριο με την μπλε γραμμή, όπου δεν υπάρχει παρεμβολή μεταξύ των δύο APs το Throughput είναι κατά πολύ περισσότερο από το σενάριο με την κόκκινη γραμμή ενώ στο Zigbee υπάρχει πάλι μια διαφορά μεταξύ των δύο σεναρίων. Άρα, καταλήγουμε πάλι πως όταν τα APs λειτουργούν στο κανάλι 13 και το Zigbee στο κανάλι 26, τότε μειώνεται κατά 25% το Throughput του Zigbee και κατά 65% του WiFi.

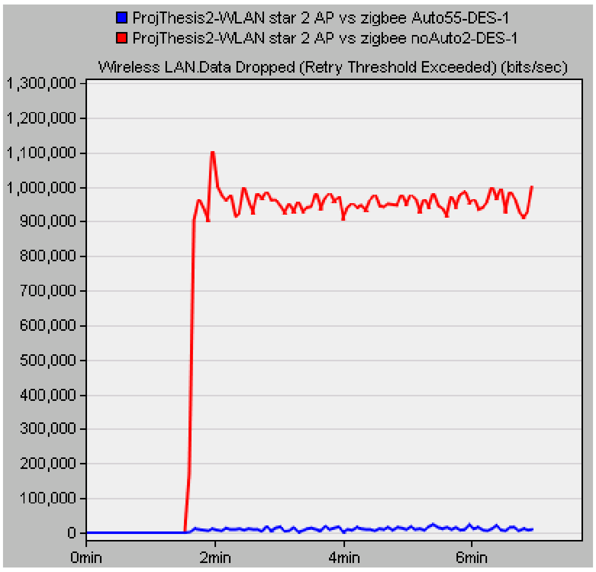
Delay (sec)

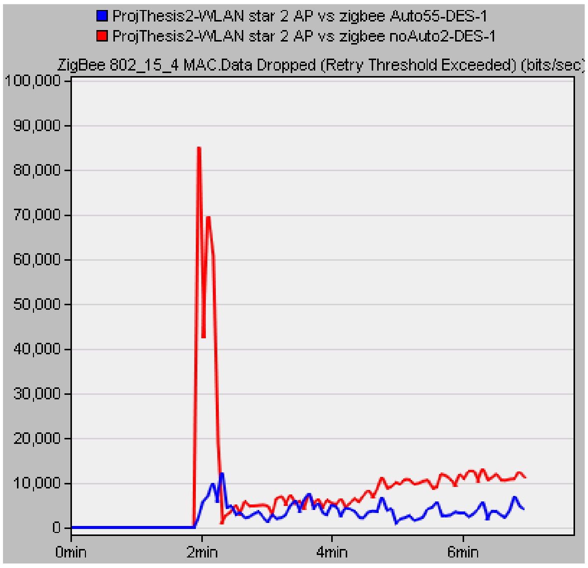




Παρατηρώντας την καθυστέρηση στα δίκτυα που συνυπάρχουν, βλέπουμε μια αισθητή διαφορά στην αριστερή γραφική του WLAN όταν τα APs λειτουργούν στο ίδιο κανάλι. Συγκεκριμένα, η καθυστέρηση ξεκινά στα 220 ms αλλά ξαφνικά φτάνει μέχρι τα 850 ms στο 2^{ο} λεπτό περίπου και ξαναπέφτει στην συνέχει στα 220 ms όπου παραμένει σταθερό μέχρι το τέλος. Συγκρίνοντας με το σενάριο όπου τα APs λειτουργούν σε διαφορετικά κανάλια (μπλε γραμμή), βλέπουμε πως οι καθυστερήσεις είναι κάτω από τα 100 ms για όλη την διάρκεια του σεναρίου αυτού, που είναι πολύ μικρή καθυστέρηση για ένα δίκτυο, και έτσι είναι ξεκάθαρο ότι οι παρεμβολές μεταξύ των APs προκαλούν αύξηση στη καθυστέρηση. Από την άλλη, το Zigbee έχει μεγαλύτερη καθυστέρηση στο σενάριο όπου τα APs λειτουργούν στο ίδιο κανάλι (κόκκινη γραμμή) αν και στα δύο σενάρια ακολουθείται αρχικά αυξητική τάση μέχρι το 5^{ο} λεπτό και μετά πέφτει μέχρι το 6^{ο} λεπτό και ξανανεβαίνει πάλι. Επίσης, η μέγιστη τιμή που φτάνει με την κόκκινη γραμμή είναι τα 24 sec στο τέλος της προσομοίωσης ενώ για την μπλε γραμμή είναι τα 16 sec. Οι τιμές της καθυστέρησης είναι μεγάλες σχετικά αλλά είναι μικρότερες από αυτές που είδαμε στο Zigbee_only σενάριο. Τέλος, φαίνεται ξεκάθαρα πως το Zigbee επηρεάζεται από το co-channel interference αφού αυξάνεται η καθυστέρηση και μειώνεται το Throughput όπως είδαμε.

Data Dropped (Retry Threshold Exceeded) (bits/sec)



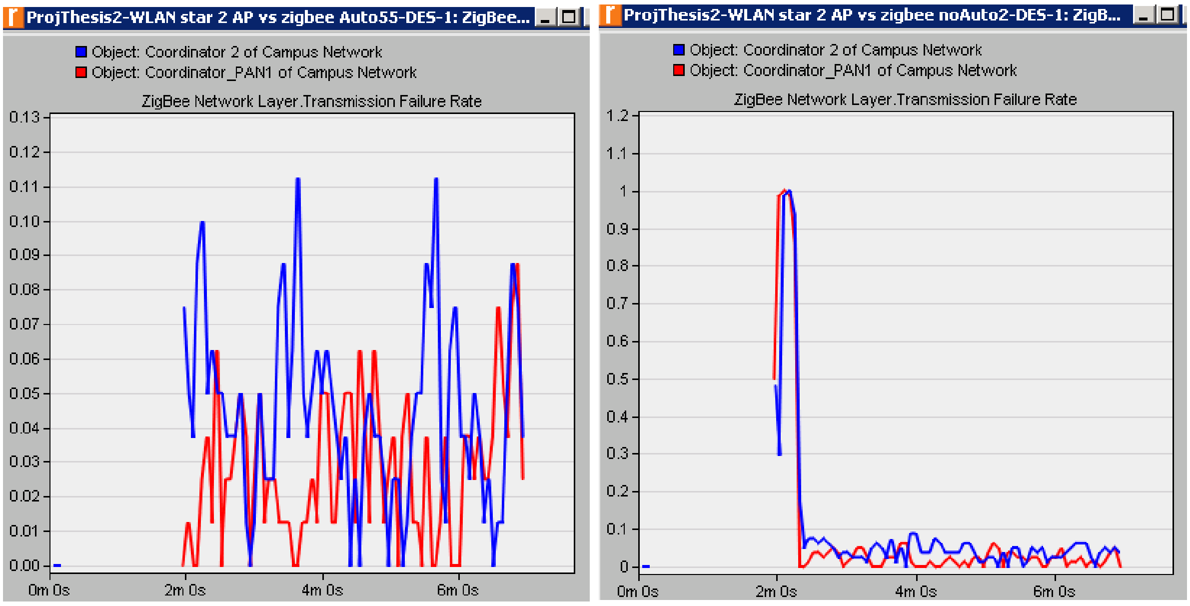


Σε αυτές τις γραφικές παραστάσεις βλέπουμε τα δεδομένα που χάνονται μετά από υπέρβαση του μέγιστου ορίου προσπαθειών για αποστολή τους. Στα αριστερά φαίνεται το WLAN, όπου τα δεδομένα που χάνονται στο σενάριο με τα δύο APs όταν είναι στο ίδιο κανάλι (κόκκινη γραμμή) είναι περίπου 980 Kbits/sec στην μεγαλύτερη διάρκεια αλλά φτάνει το μέγιστο στα 1,1 Mbits/sec και το ελάχιστο στα 900 Kbits/sec. Ο λόγος που σημειώνεται μια αύξηση κοντά στο $2^{ο}$ λεπτό είναι εκεί ξεκινά την λειτουργία του το δίκτυο και ανταλλάσσονται πακέτα ελέγχου μαζί με δεδομένα και έτσι κάποια από αυτά χάνονται, φτάνοντας στο peak της γραφική αλλά μετά επανέρχεται σε πιο σταθερό ρυθμό η απώλεια των δεδομένων. Αντίθετα, στο σενάριο που δεν έχουμε παρεμβολή των καναλιών μεταξύ των APs, τα δεδομένα που χάνονται είναι πολύ λιγότερα, κάτω από 25 Kbits/sec, και έτσι είναι φανερό το πρόβλημα της παρεμβολής που προκαλείται στο WLAN. Αν υπολογίσουμε πως έχουμε throughput όπως είδαμε στα 13 Mbits/sec και τα δεδομένα που χάνουμε είναι 980 Kbits/sec, τότε έχουμε σχεδόν 7,5% απώλεια δεδομένων που είναι μικρή σχετικά.

Από την γραφική του Zigbee στα δεξιά, βλέπουμε πως τα δεδομένα που χάνουμε είναι περισσότερα στο σενάριο με τα επικαλυπτόμενα κανάλια (κόκκινη γραμμή) παρά στο άλλο σενάριο. Τα δεδομένα χάνονται κυρίως στην αρχή της προσομοίωσης όπου φτάνουν στα 85 85 Kbits/sec μέχρι λίγο πριν το $3^{ο}$ λεπτό όπου ο ρυθμός πέφτει κάτω από 10 Kbits/sec. Η αιτία της ξαφνικής αύξησης και μείωσης οφείλεται στην αλλαγή του καναλιού που γίνεται από τον Coordinator σχεδόν μόλις που ξεκινά το δίκτυο γιατί θα δούμε παρακάτω πως αντιμετωπίζει παρεμβολές από το WiFi. Έτσι, χάνονται προσωρινά πολλά δεδομένα αφού οι κόμβοι δεν πιάνουν τα δεδομένα το παλιό κανάλι αλλά αυτό σύντομα λύνεται γιατί ο ρυθμός επανέρχεται σε χαμηλά επίπεδα μόλις συντονιστούν όλοι οι κόμβοι στο νέο κανάλι. Στη συνέχεια, η απώλεια αυξάνεται με τον χρόνο αλλά δεν ξεπερνά τα 15 Kbits/sec που είναι σχετικά λίγα.

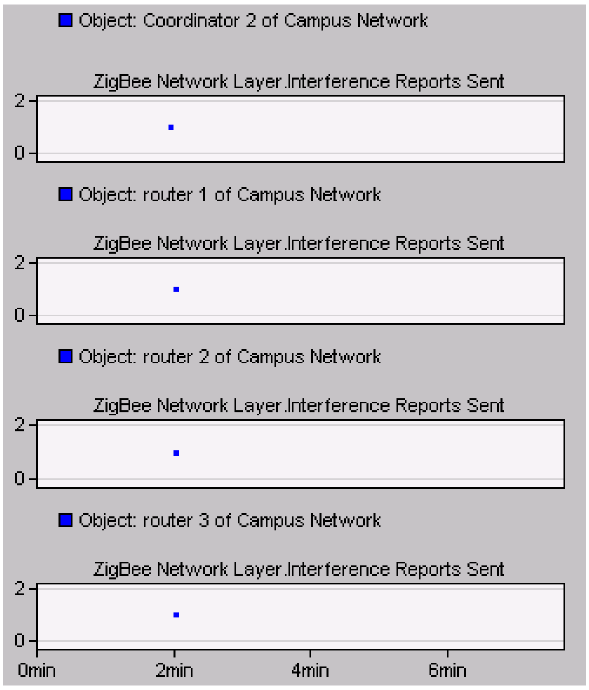
Τέλος, στο σενάριο χωρίς παρεμβολές στο κανάλι, με την μπλε γραμμή, βλέπουμε πως τα δεδομένα είναι αρχικά 10 Kbits/sec αλλά το μεγαλύτερο διάστημα είναι σχεδόν 7 Kbits/sec που δείχνει πως τα δίκτυα δεν έχουν σοβαρό πρόβλημα παρεμβολής.

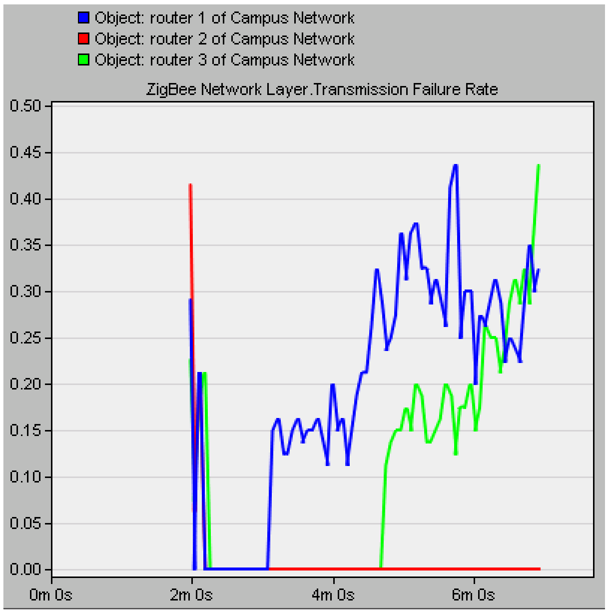
Zigbee Network Layer: Transmission Failure Rate (%)



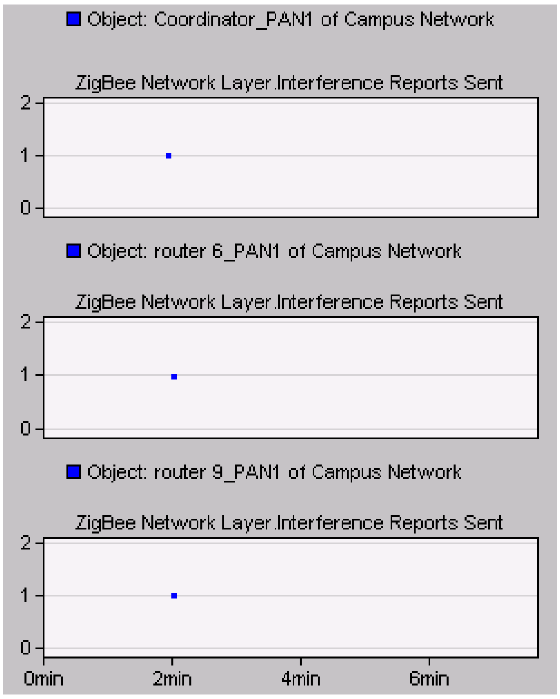
Οι γραφικές που φαίνονται πιο πάνω απεικονίζουν το ποσοστό αποτυχίας μετάδοσης στο δίκτυο Zigbee για τους 2 Coordinatos στο PAN 1 και στο PAN 2 για τα σενάρια όπου τα APs λειτουργούν σε διαφορετικά κανάλια (αριστερή γραφική) και στο ίδιο κανάλι (δεξιά γραφική). Όπως φαίνεται, στο σενάριο χωρίς επικάλυψη καναλιών (αριστερή γραφική) οι Coordinators και των δύο δικτύων δεν αντιμετωπίζουν οποιοδήποτε πρόβλημα αφού τα ποσοστά τους είναι πολύ μικρά και συγκεκριμένα κάτω από 12% και άρα δεν θα τρέξει ο αλγόριθμος του FRQAG. Αντίθετα, στο σενάριο που βλέπουμε στη δεξιά γραφική, και οι δύο Coordinators αντιμετωπίζουν πρόβλημα αρχικά στο $2^{ο}$ λεπτό που ξεκινά το δίκτυο τους γιατί το ποσοστό αποτυχίας μετάδοσης φτάνει και για τους δύο στο 100%. Αυτό σημαίνει πως θα ενεργοποιηθεί ο αλγόριθμος FRQAG αφού είναι πάνω από 25% το ποσοστό και θα γίνει αλλαγή καναλιού στο δίκτυο.

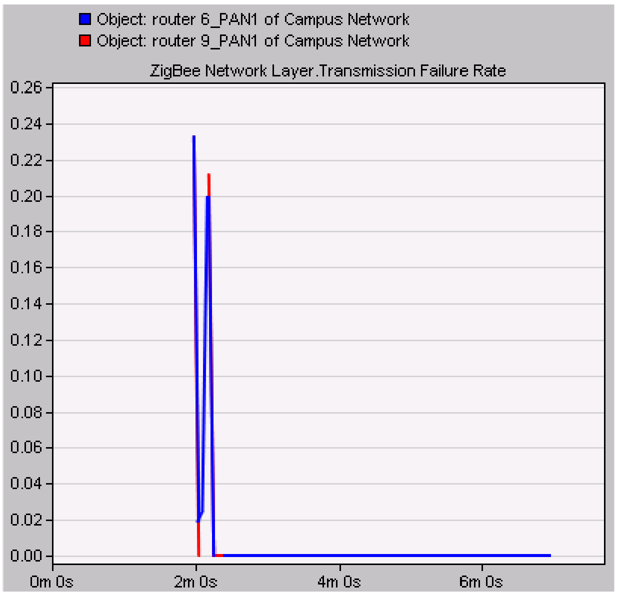
Πιο κάτω φαίνεται τα Interference Reports που στέλνονται από τους Routers του δικτύου PAN 1 και PAN 2 στο σενάριο με τα APs που λειτουργούν στο ίδιο κανάλι. Όταν το ποσοστό αποτυχίας μετάδοσης των δεδομένων ξεπερνά το 25%, ο Coordinator ζητά από όλους τους Routers μια αναφορά για την ενέργεια που επικρατεί σε όλα τα κανάλια. Παρατηρούμε στην αριστερή γραφική για το PAN 2 πως ο Coordinator δημιουργεί μια αναφορά ο ίδιος στο 2ο λεπτό αλλά παράλληλα στέλνονται και από τους Router 1,2 και 3 παρόλο που όπως φαίνεται στην δεξιά γραφική τα ποσοστά αποτυχίας των Routers δεν είναι όλων πάνω από 25%. Αυτό συμβαίνει γιατί ο Coordinator ακολουθεί την Active τακτική και ζητά από όλους αναφορές εκείνη την στιγμή.



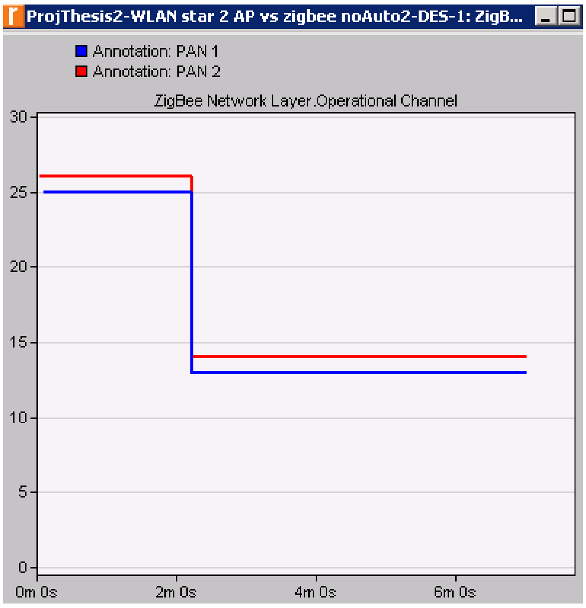


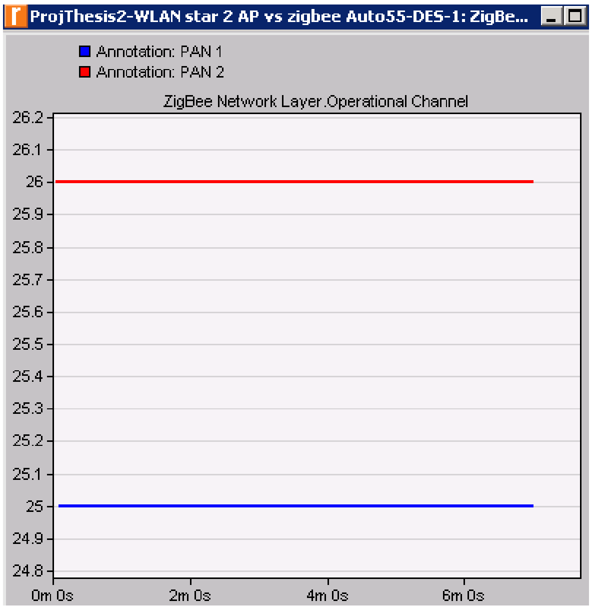
Η ίδια τακτική ακολουθείται και στο PAN 1 όπου έχουμε την ίδια συμπεριφορά στους κόμβους και όπως φαίνεται τα Interference Reports ζητούνται από τους Routers και στέλνονται από αυτούς με λίγα δευτερόλεπτα διαφορά. Στην δεξιά γραφική φαίνεται πως παρόλο που τα ποσοστά αποτυχίας δεν ξεπερνούν το 25%, στέλνουν τις αναφορές όπως αναφέραμε.



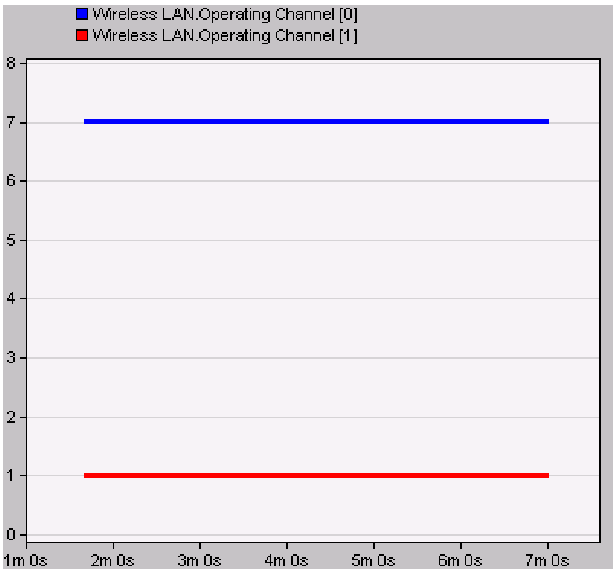


Operational Channel





Στις παραπάνω γραφικές παρουσιάζονται τα κανάλια που λειτουργεί το κάθε δίκτυο Zigbee ανάλογα με τον αριθμό PAN στο σενάριο όπου τα APs είναι στο κανάλι 13 (αριστερά) και σε διαφορετικά κανάλια (δεξιά). Με την μπλε γραμμή φαίνεται το δίκτυο PAN 1 το οποίο στην αριστερή γραφική ξεκινά το 2^{o} λεπτό στο κανάλι 25 αλλά λίγα δευτερόλεπτα μετά μεταπηδά στο κανάλι 13. Ο λόγος που αλλάζει κανάλι όπως είπαμε, είναι διότι ο Coordinator αντιμετώπιζε πρόβλημα παρεμβολής από το WLAN και επειδή το ποσοστό αποτυχίας φτάνει το 100% αλλάζει κανάλι σε ολόκληρο το δίκτυο. Με την κόκκινη γραμμή φαίνεται το PAN 2 το οποίο λειτουργεί στο κανάλι 26 μόλις εκκινεί το δίκτυο αλλά και αυτό αλλάζει κανάλι την ίδια χρονική στιγμή μαζί με το PAN 1 επιλέγοντας το κανάλι 14. Από την άλλη, στην δεξιά γραφική παράσταση βλέπουμε τα κανάλια λειτουργίας του Zigbee όταν τα APs είναι σε διαφορετικά κανάλια. Όπως ήταν αναμενόμενο, το PAN 1 (μπλε γραμμή) και το PAN 2 (κόκκινη γραμμή) μένουν από την αρχή στα κανάλια 25 και 26 αντίστοιχα αφού το ποσοστό αποτυχίας αποστολής δεδομένων δεν ξεπερνά το 25%. Όμως, μια καλύτερη στρατηγική θα ήταν να επιλέξουν τα κανάλια που δεν έχουν επικάλυψη με το WiFi για βέλτιστη απόδοση.

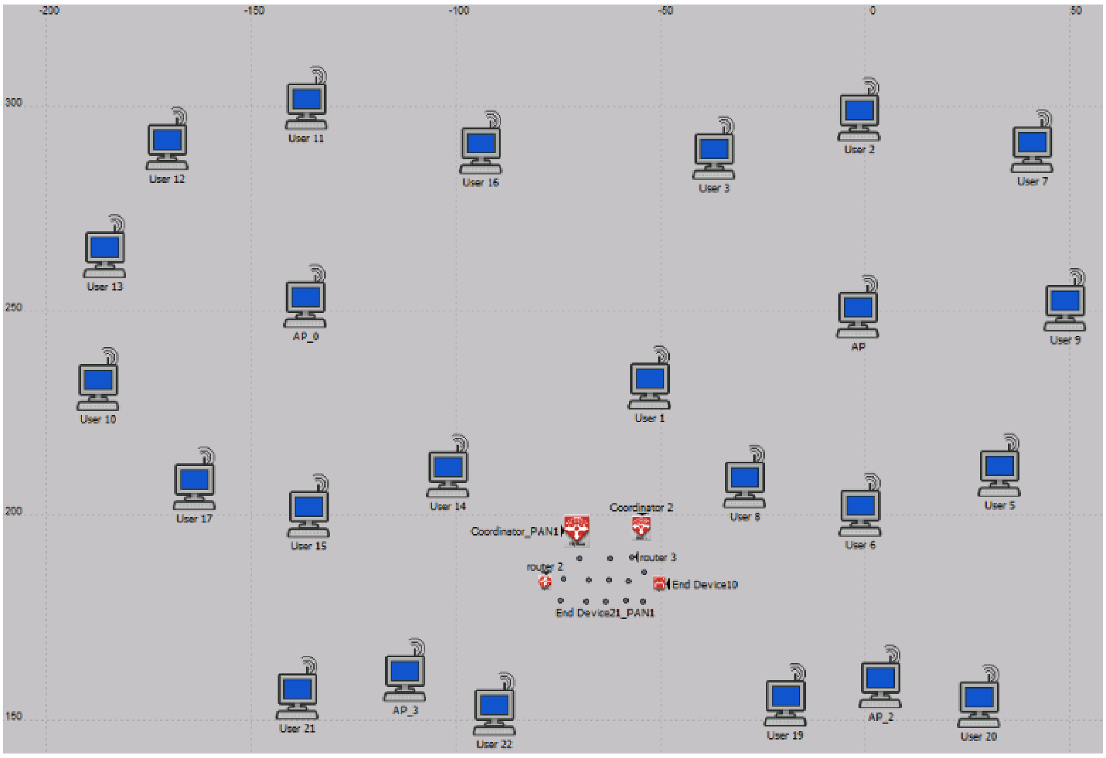


Τέλος, σε αυτή την γραφική απεικονίζονται τα κανάλια που λειτουργούν τα 2 APs στο σενάριο "*WLAN star 2 AP vs zigbee Auto55*" και βλέπουμε πως επιλέγουν τα κανάλια 1 και 7 αντίστοιχα που είναι μη επικαλυπτόμενα. Για το δεύτερο σενάριο εμείς καθορίσαμε τα APs να λειτουργούν στα κανάλια 13 και γι' αυτό δεν απεικονίζονται.

Συμπεράσματα σεναρίων: Σε αυτά τα σενάρια όπου είχαμε 2 δίκτυα WLAN να συνυπάρχουν με 2 δίκτυα Zigbee με την διαφορά ότι τα APs λειτουργούν στα ίδια κανάλια (πρώτο σενάριο) και σε διαφορετικά κανάλια (δεύτερο σενάρια), καταλήγουμε πως οι παρεμβολές που δημιουργούνται από το WiFi επηρεάζουν το Zigbee με αποτέλεσμα πολλά δεδομένα να συγκρούονται ή να προσπαθούν οι κόμβοι να τα ξαναστείλουν και έτσι αυξάνεται η καθυστέρηση του δικτύου καθώς επίσης και μείωση του Throughput. Η παρεμβολή όμως δεν αφορά όπως φαίνεται μόνο το Zigbee αλλά παράλληλα και το WiFi το οποίο έχει δραματική μείωση του Throughput εξαιτίας του co-channel interference. Τέλος, ο FRQAG εδώ φαίνεται να δουλεύει και να έχουμε μια ελάχιστη βελτίωση στην απόδοση του συστήματος.

5.3.5 Σενάριο με δύο δίκτυα Zigbee μαζί με 4 δίκτυα WLAN (αρ.9)

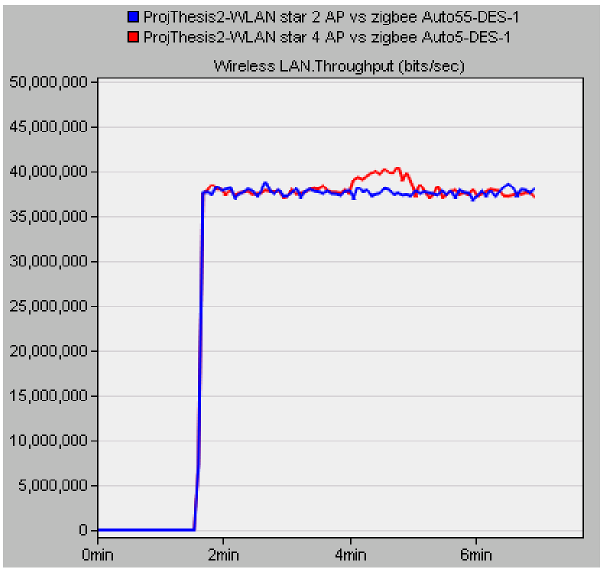
Στο σενάριο αυτό μελετούμε την επίδραση του WLAN στο Zigbee όταν υπάρχουν 4 APs μαζί με δύο δίκτυα Zigbee που λειτουργούν στα κανάλια 26 και 25 με ενεργοποιημένο τον αλγόριθμο FRQAG. Στα 4 APs τα κανάλια που αναθέτουμε είναι Auto-assign, δηλαδή θα μπουν τα κανάλια 1,7,13 και 6. Στα αποτελέσματα που θα δούμε θα συγκρίνουμε το σενάριο αυτό με το προηγούμενο που είχαμε δύο AP και τα κανάλια πάλι ήταν στην επιλογή Auto-assign, με σκοπό να δούμε την διαφορά στην απόδοση του Zigbee όπως και στο WLAN λόγω του αυξημένου αριθμού των APs. Ο χρόνος προσομοίωσης είναι 7 λεπτά. Τέλος, να αναφέρουμε ότι όλα τα APs λειτουργούν με βάση τις αρχικές ρυθμίσεις και, επίσης, τα δύο από τα 4 APs ενεργοποιούνται προσωρινά μεταξύ των χρόνων 240 και 300 sec ενώ τα υπόλοιπα δύο APs είναι συνεχώς ενεργοποιημένα. Πιο κάτω φαίνεται η τοποθέτηση των συσκευών στον χώρο και οι αποστάσεις μεταξύ τους.

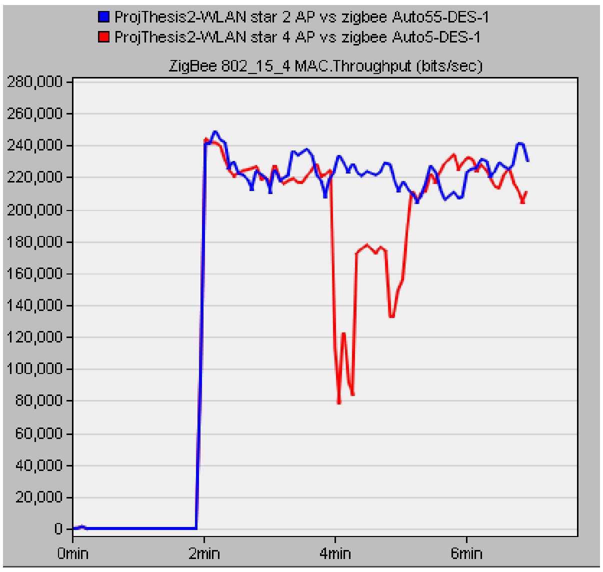


Σχήμα 5.8: Διάταξη συσκευών Zigbee και WiFi για το σενάριο με αρ.9.

Τα αποτελέσματα που εξήγαμε από αυτό το σενάριο τα αναλύουμε πιο κάτω.

<u>Throughput (bits/sec)</u>

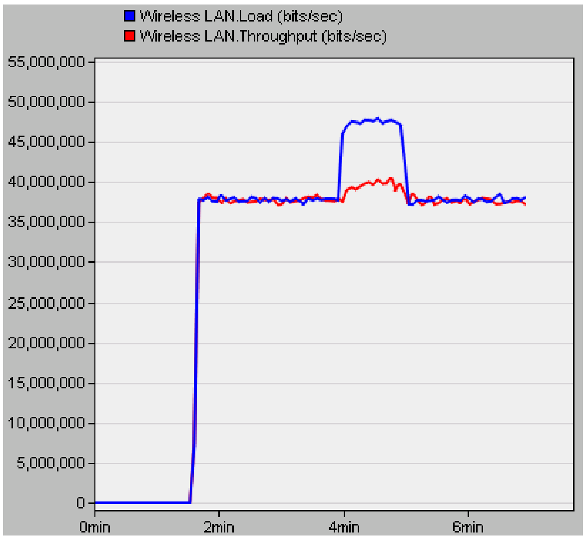


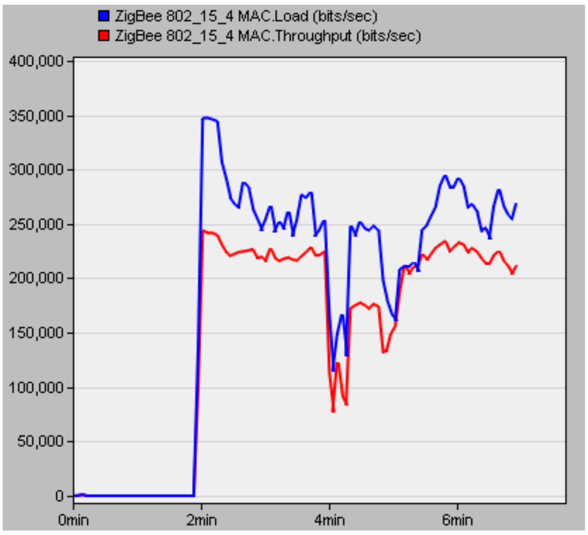


Στις πιο πάνω γραφικές φαίνονται το Throughput για το WLAN και το Zigbee στο σενάριο που μελετούμε σε σύγκριση με το σενάριο που έχουμε μόνο 2 APs τα οποία λειτουργούν σε διαφορετικά κανάλια. Ξεκινώντας από την γραφική του WLAN, βλέπουμε ότι και στα δύο σενάρια το Throughput είναι σχεδόν σταθερό στα 38 Mbits/sec περίπου σε όλη την διάρκεια της προσομοίωσης εκτός από το διάστημα μεταξύ 4ου και 5ου λεπτού στο σενάριο με τα 4 APs (κόκκινη γραμμή) όπου ενεργοποιούνται τα επιπλέον 2 APs και το Throughput είναι αυξημένο κατά 2 Mbits/sec σχεδόν. Έτσι, συνολικά φτάνει μέχρι τα 40 Mbits/sec σε αυτό το διάστημα.

Στη γραφική του Zigbee (δεξιά), βλέπουμε πως το Throughput του δικτύου στα δύο σενάρια έχει κάποια μικρά σκαμπανεβάσματα αλλά είναι πιο εμφανές η επίδραση των 2 APs που ενεργοποιούνται στο διάστημα του 4ου και 5ου λεπτού στο σενάριο με την κόκκινη γραμμή όπου και μειώνεται το Throughput ξαφνικά από τα 220 Kbits/sec στα 80 Kbits/sec όπου μένει εκεί για λίγα δευτερόλεπτα και ξαναπέφτει στα 140 Kbits/sec το 5ο λεπτό και μετά επανέρχεται πίσω στα 220 Kbits/sec. Η πρώτη πτώση που γίνεται στο 4ο λεπτό οφείλεται στην αλλαγή καναλιού που γίνεται στο PAN 2 όπως θα δούμε και παρακάτω αλλά παράλληλα εξαιτίας της ενεργοποίησης των 2 APs. Στη συνέχεια που ανεβαίνει στα 180 Kbits/sec είναι γιατί το δίκτυο επηρεάζεται από τα APs και έτσι μειώνεται το Throughput. Μετά από 1 λεπτό, δηλαδή στο 5ο λεπτό γίνεται η αλλαγή για το PAN 1 και πέφτει το Throughput στα 140 Kbits/sec και στο τέλος ανεβαίνει πίσω στα κανονικά επίπεδα αφού πλέον τα 2 APs έχουν απενεργοποιηθεί. Συγκρίνοντας με το δεύτερο σενάριο με την μπλε γραμμή, το Throughput κυμαίνεται στα 210 με 240 Kbits/sec και το ίδιο γίνεται με την κόκκινη γραμμή εκτός από το σημείο που ενεργοποιούνται τα επιπλέον APs. Έτσι, φαίνεται ξεκάθαρα η παρεμβολή του WLAN στο Zigbee και την μείωση της απόδοσης του συστήματος.

<u>Load (bits/sec)</u>

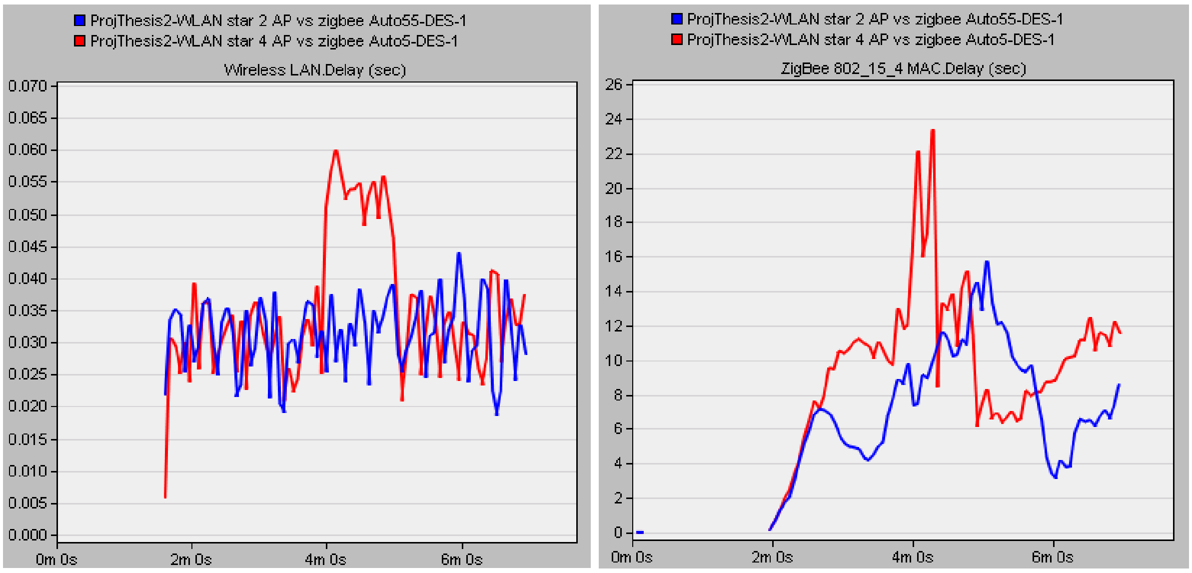




Παρατηρώντας το Load στο WLAN, φαίνεται πως δεν υπάρχει μεγάλη διαφορά με το Throughput αφού παραμένουν και τα δύο το μεγαλύτερο χρονικό διάστημα στα 38 Mbits/sec. Η μεγάλη διαφοροποίηση είναι όταν ενεργοποιούνται τα 2 APs για ένα λεπτό και εκεί το Load φτάνει τα 48 Mbits/sec ενώ το Throughput ανεβαίνει μόνο στα 40 Mbits/sec. Με άλλα λόγια, τα περισσότερα δεδομένα που δημιουργούνται από τα επιπλέον 2 APs δεν είναι χρήσιμα και χάνονται είτε λόγω συγκρούσεων είτε επειδή ο ρυθμός δημιουργίας των πακέτων από τους κόμβους είναι πολύ περισσότερος από αυτό που μπορεί να διαχειριστεί το AP και έτσι γεμίζουν τα buffer με αποτέλεσμα τα πακέτα να χάνονται.

Βλέποντας το Load του Zigbee (δεξιά γραφική) φτάνει τα 350 Kbits/sec αρχικά που γίνεται η εκκίνηση του δικτύου και ανταλλάσσονται δεδομένα και πακέτα ελέγχου ενώ στην συνέχεια μειώνεται μέχρι τα 250 Kbits/sec αν εξαιρέσουμε κάποιες απότομες προσαυξήσεις. Αν συγκρίνουμε το Load με το Throughput μπορούμε να πούμε πως από την αρχή μέχρι το τέλος υπάρχει μια διαφορά στο πόσα δεδομένα είναι χρήσιμα εκτός από μερικές στιγμές όπου οι γραμμές τους τέμνονται όταν υπάρχουν απότομες αυξήσεις ή μειώσεις. Αξίζει να τονίσουμε πως η πτώση και των δύο μετρικών κοντά στο $4^{ο}$ λεπτό οφείλεται στο ότι θα αλλάξουν κανάλια λειτουργίας τα δίκτυα Zigbee και έτσι θα χαθούν κάποια δεδομένα που στέλνουν οι κόμβοι. Από εκεί και πέρα, αυξάνονται πάλι οι μετρικές αλλά το Load είναι μεγαλύτερο από το Throughput.

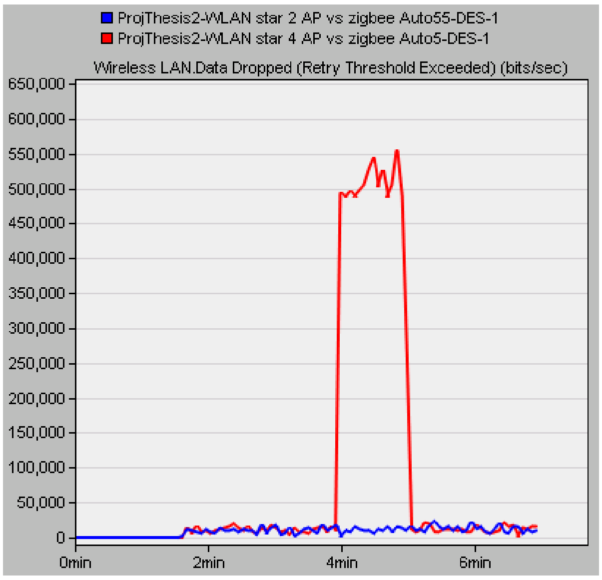
<u>Delay (sec)</u>

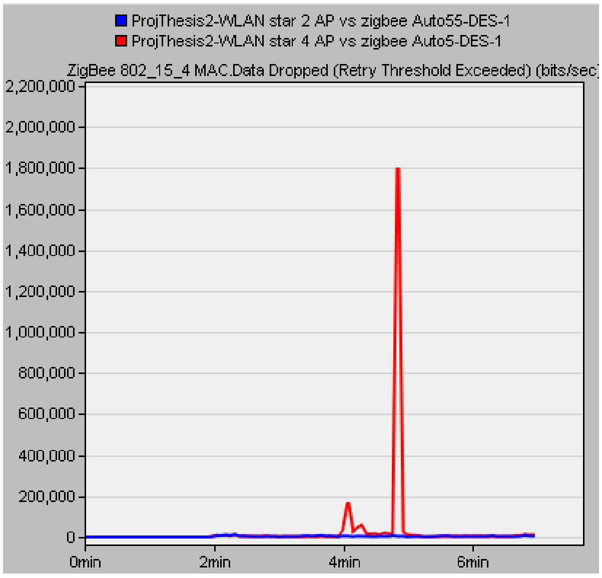


Εξετάζοντας την καθυστέρηση που παρατηρείται στο δίκτυο μας με τα 4 APs σε σχέση με το σενάριο με τα 2 APs, βλέπουμε μια αισθητή διαφορά στην αριστερή γραφική του WLAN όταν τα επιπλέον 2 APs λειτουργούν για περίοδο ενός λεπτού. Συγκεκριμένα, η καθυστέρηση ξεκινά στα 30 ms περίπου και για τα δύο σενάρια αλλά στο $4^{ο}$ λεπτό στο σενάριο με την κόκκινη γραμμή, ξαφνικά εκτοξεύεται η καθυστέρηση στα 60 ms και πέφτει σε λίγα δευτερόλεπτα στα 55 ms μέχρι το $5^{ο}$ λεπτό όπου απενεργοποιούνται τα 2 από τα 4 APs και επιστρέφει στα κανονικά επίπεδα. Αυτό δείχνει ότι η ενεργοποίηση των 2 APs προκαλεί μια αύξηση στην καθυστέρηση διπλάσια από την αρχική. Γενικά μιλώντας, όμως, η καθυστέρηση στο WLAN σε σύγκριση με το σενάριο με ένα απλό δίκτυο WLAN είναι μικρότερη αφού σε εκείνο το σενάριο είχαμε 90 ms καθυστέρηση ενώ εδώ η μέγιστη είναι 60 ms. Ακόμη, αν το συγκρίνουμε με το σενάριο που τα 2 APs έχουν πρόβλημα παρεμβολής, η καθυστέρηση που είχαμε στα 220 ms ήταν πολύ περισσότερη την καθυστέρηση που έχουμε εδώ. Έτσι, φαίνεται πως τα APs δεν επηρεάζονται σχεδόν καθόλου όταν λειτουργούν σε διαφορετικά κανάλια.

Από την άλλη, στην δεξιά γραφική βλέπουμε το Zigbee έχει μια αυξητική τάση η καθυστέρηση και είναι μεγαλύτερη στο σενάριο όπου έχουμε 4 APs (κόκκινη γραμμή) σε σχέση με το σενάριο με τα 2 APs. Και πάλι όμως αν συγκρίνουμε την καθυστέρηση με το αρχικό σενάριο που είναι οι συσκευές Zigbee μόνες τους τότε η μέγιστη καθυστέρηση εδώ των 23 sec είναι κατά 1 δευτερόλεπτο μεγαλύτερη από τα 22 sec που είχαμε στο αρχικό σενάριο. Παρατηρώντας πιο προσεκτικά, η καθυστέρηση στο σενάριο μας (κόκκινη γραμμή) ξεκινά από τα 10 sec με αυξητική τάση ανεβαίνοντας μέχρι το 4^{ο} λεπτό στα 12 sec και μετά με μια απότομη αύξηση φτάνει στα 22 sec γιατί εκεί ενεργοποιούνται τα 2 APs. Παράλληλα, γίνεται η αλλαγή του καναλιού του ενός δικτύου Zigbee και τα πακέτα χάνονται μέχρι να συντονιστούν όλοι οι κόμβοι στο νέο κανάλι γι’ αυτό και η καθυστέρηση ξαφνικά πέφτει στα 16 sec και αυξάνεται τα 23 sec. γιατί τώρα. Μετά από αυτές τις ξαφνικές αυξήσεις, η καθυστέρηση μειώνεται στα 6 sec και αλλά λίγο μετά το 5^{ο} λεπτό αλλάζει κανάλι το δεύτερο δίκτυο Zigbee και βλέπουμε μια μικρή αυξομείωση πάλι της καθυστέρησης. Καταλήγοντας, μπορούμε να πούμε πως η αυξητική τάση οφείλεται στο ότι τα πακέτα που στέλνονται αποτυγχάνουν να φτάσουν επιτυχώς, όπως θα δούμε παρακάτω, λόγω της παρεμβολής των γειτονικών κόμβων Zigbee που αν και λειτουργούν σε γειτονικό κανάλι από το 4^{ο} λεπτό, η ενέργεια τους επηρεάζει την μετάδοση των πακέτων.

Data Dropped (Retry Threshold Exceeded) (bits/sec)

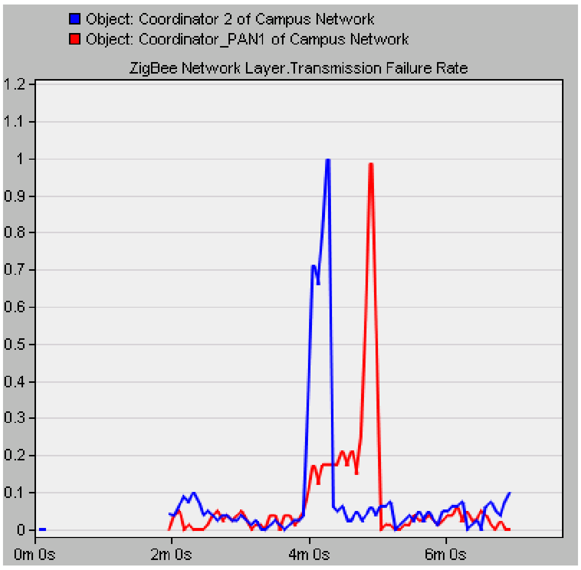




Σε αυτές τις γραφικές παραστάσεις βλέπουμε το Data Dropped στα δίκτυα WLAN και Zigbee. Στα αριστερά φαίνεται το WLAN, όπου τα δεδομένα που χάνονται στο σενάριο με τα 4 APs (κόκκινη γραμμή) είναι το μέγιστο 550 Kbits/sec όταν ενεργοποιούνται τα 2 APs στην περίοδο του 4^{ου} και 5^{ου} λεπτού ενώ στην υπόλοιπη διάρκεια της προσομοίωσης τα δεδομένα που χάνονται είναι κάτω από 50 Kbits/sec. Η απότομη αυτή αλλαγή δείχνει ότι η ενεργοποίηση των 2 APs προκαλεί μείωση των δεδομένων στο δίκτυο αντί αύξηση αν και δεν έχουμε παρεμβολή των καναλιών μεταξύ των APs. Αν υπολογίσουμε πως έχουμε throughput όπως είδαμε στα 38 Mbits/sec και τα δεδομένα που χάνουμε είναι 550 Kbits/sec, τότε έχουμε σχεδόν 1,48% απώλεια δεδομένων που είναι πάρα πολύ μικρή και δεν επηρεάζεται η λειτουργία του δικτύου.

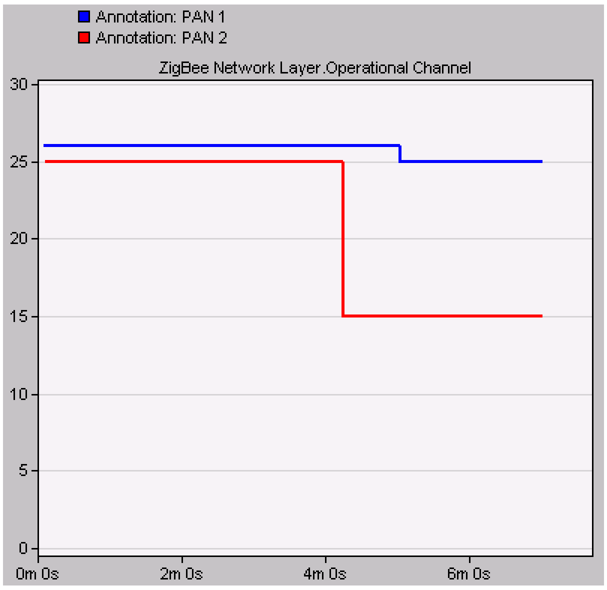
Από την γραφική του Zigbee στα δεξιά, βλέπουμε πως τα δεδομένα που χάνονται είναι κυρίως στο σενάριο με τα 4 APs που μελετάμε και χάνονται στις 2 στιγμές που αλλάζουν κανάλι τα δίκτυα Zigbee. Συγκεκριμένα, στο 4^{ο} λεπτό βλέπουμε ένα spike να φτάνει τα 200 Kbits/sec ενώ στο 5^{ο} λεπτό η απώλεια είναι στα 1,8 Mbits/sec που είναι πολύ περισσότερα από πριν. Η μεγάλη διαφορά των δεδομένων που χάνονται οφείλεται στο ότι το 5^{ο} λεπτό είναι ενεργοποιημένα και τα 4 APs και έτσι επηρεάζεται περισσότερο το δίκτυο του Zigbee με αποτέλεσμα πολλά πακέτα να μην φτάνουν στον προορισμό τους και άρα οι κόμβοι προσπαθούν να τα ξαναστείλουν.

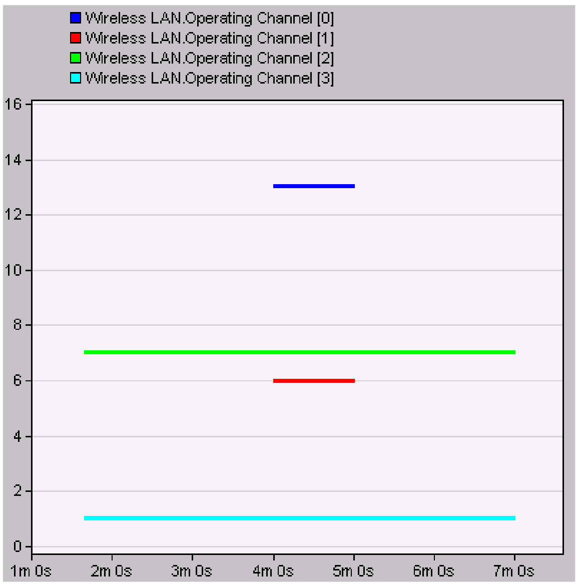
Zigbee Network Layer: Transmission Failure Rate (%)



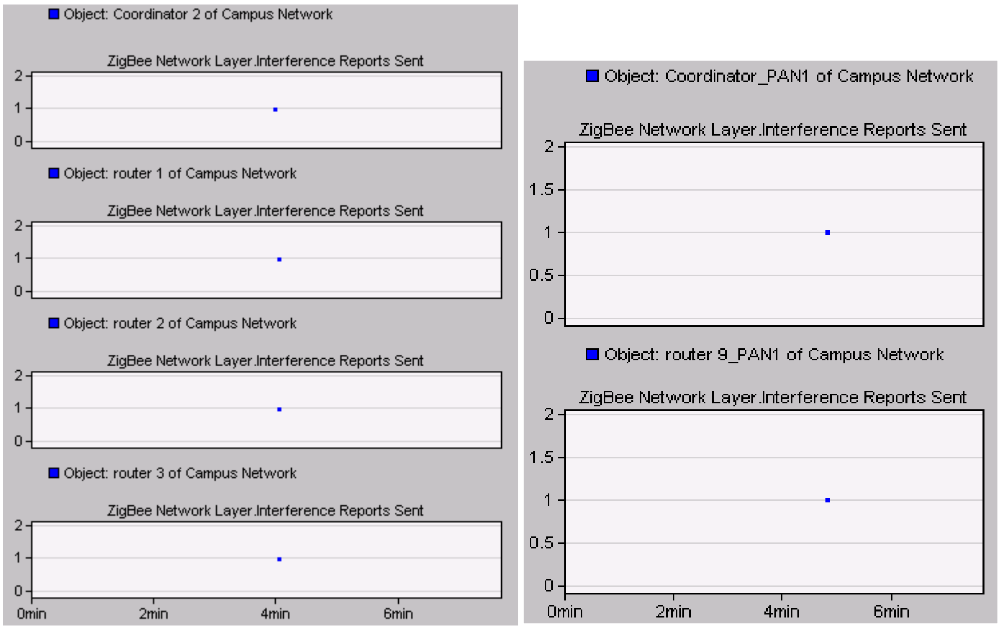
Η γραφική που φαίνεται πιο πάνω απεικονίζει το ποσοστό αποτυχίας μετάδοσης στο δίκτυο Zigbee για τους 2 Coordinators του PAN 1 και του PAN 2 για το σενάριο που μελετάμε. Με την κόκκινη γραμμή φαίνεται ο Coordinator του PAN 1 ο οποίος φτάνει στο 5^{ο} λεπτό το 100% που είναι πολύ μεγάλο ποσοστό και σημαίνει πως θα ενεργοποιηθεί ο αλγόριθμος FRQAG αφού είναι πάνω από 25%. Μετά την αλλαγή του καναλιού το ποσοστό πέφτει στο 5%. Όπως είναι φανερό, η πρώτη στιγμή που υπάρχει αύξηση στα 100% για το PAN 2 είναι στο 4^{ο} λεπτό στο οποίο γίνεται και η ενεργοποίηση των 2 επιπλέον APs του δικτύου WLAN στα κανάλια 6 και 13 και γι’ αυτό επηρεάζονται τα δίκτυα του Zigbee. Το αποτέλεσμα της αύξησης του ποσοστού στο 100% θα είναι να τρέξει ο αλγόριθμος FRQAG και να γίνει αλλαγή καναλιού στα 2 δίκτυα.

Operational Channel

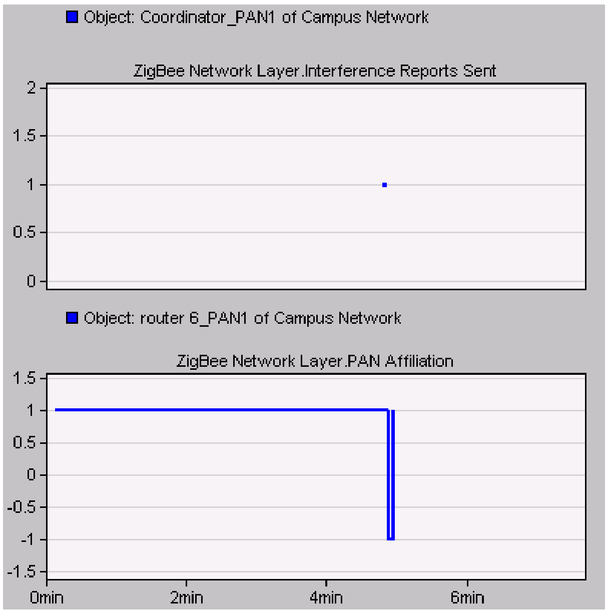




Στην παραπάνω γραφική παρουσιάζονται τα κανάλια που λειτουργεί το κάθε δίκτυο Zigbee ανάλογα με τον αριθμό PAN ID στο σενάριο που έχουμε τα 4 APs σε διαφορετικά κανάλια. Με την κόκκινη γραμμή φαίνεται το δίκτυο PAN 2 το οποίο ξεκινά στο κανάλι 25 αλλά λίγο μετά το 4^{ο} λεπτό μετακινείται στο κανάλι 15. Ο λόγος που αλλάζει κανάλι όπως είπαμε, είναι διότι ο Coordinator αντιμετώπιζε πρόβλημα παρεμβολής από το WLAN και επειδή το ποσοστό αποτυχίας ξεπερνά το 25%, άλλαξε κανάλι σε ολόκληρο το δίκτυο. Με την μπλε γραμμή φαίνεται το PAN 1 το οποίο λειτουργεί στο κανάλι 26 μόλις εκκινεί το δίκτυο και αυτό παραμένει μέχρι το 5^{ο} λεπτό όπου θα μετακινηθεί στο κανάλι 25 το δίκτυο.
Στην δεξιά γραφική παράσταση, βλέπουμε τα κανάλια λειτουργίας των 4 APs στο σενάριο μας. Όπως παρατηρούμε, τα 2 APs που είναι ενεργοποιημένα συνεχώς είναι στα κανάλια 1 και 7 αντίστοιχα ενώ τα 2 προσωρινά APs λειτουργούν στα κανάλια 6 και 13 αντίστοιχα με αποτέλεσμα να προκαλούν παρεμβολές στο δίκτυο Zigbee. Όπως έχουμε αναφέρει πριν την περιγραφή των σεναρίων, τα κανάλια που επιλέγονται από τα APs στο WLAN ακολουθούν τον αλγόριθμο που έχουμε περιγράψει στο προηγούμενο υποκεφάλαιο (5.2) και στον οποίο επιλέγουν πρώτα τα κανάλια που δεν έχουν επικάλυψη μεταξύ τους στην Ευρώπη.
Πιο κάτω εικονίζονται οι κόμβοι που στέλνουν τα Interference Reports σε κάθε PAN. Στο PAN 2 που φαίνεται στην αριστερή γραφική, στέλνονται αναφορές από τα Routers 1,2 και 3 την ίδια χρονική στιγμή που στέλνει και ο Coordinator, δηλαδή στο 4^{ο} λεπτό. Το ίδιο συμβαίνει και στο 5^{ο} λεπτό για το PAN 1 που απεικονίζεται στην δεξιά γραφική, όπου ο Coordinator λαμβάνει την αναφορά από τον Router 9 μόνο.



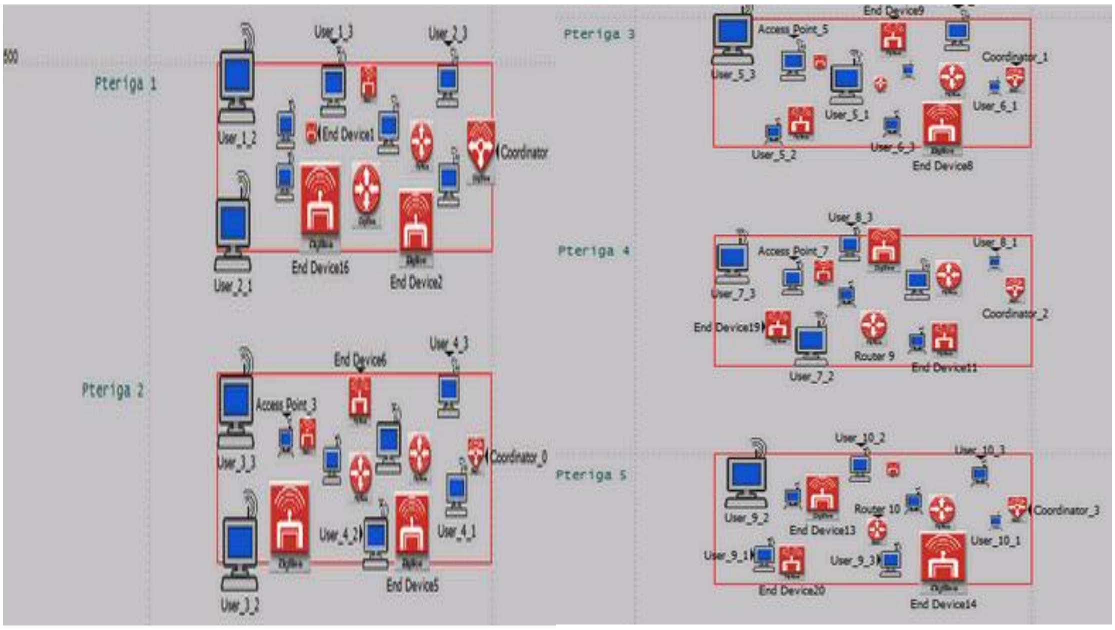
Ο Router 6 του PAN 1 υπό κανονικές συνθήκες θα έπρεπε να στείλει αναφορά στον Coordinator αλλά φαίνεται πως δεν στέλνει γιατί την στιγμή που ζητείται η αναφορά ο κόμβος αποσυνδέεται ξαφνικά από το δίκτυο για λίγο δευτερόλεπτα και επανασυνδέεται όπως βλέπουμε στην γραφική του PAN Affiliation πιο κάτω που συγκρίνεται η στιγμή αποστολής της αναφοράς από τον Coordinator μαζί με την στιγμή που αποσυνδέεται ο κόμβος από το δίκτυο.



<u>Συμπεράσματα σεναρίων:</u> Στο σενάριο που μελετήσαμε και είχαμε 4 δίκτυα WLAN με τα APs να λειτουργούν σε διαφορετικά κανάλια μαζί με 2 δίκτυα Zigbee μπορούμε να συμπεράνουμε πως η ξαφνική ενεργοποίηση των 2 APs βάζει σε λειτουργία τον αλγόριθμο FRQAG. Μελετώντας τα κανάλια που επιλέγονται από το Zigbee, το PAN 2 επιλέγει το κανάλι 15 που είναι μη επικαλυπτόμενο με το WiFi ενώ το PAN 1 επιλέγει το 25 την στιγμή που υπάρχει ακόμα το AP στο κανάλι 13. Επίσης, στην πρώτη περίπτωση η ταχύτητα της απόφασης για αλλαγή του καναλιού γίνεται μόλις που ξεκινούν τα 2 APs ενώ για το PAN 1 η εκτέλεση της αλλαγής γίνεται όταν σχεδόν απενεργοποιούνται τα APs και άρα μειώνονται οι παρεμβολές που δημιουργούνται από το WiFi. Άρα, το Zigbee θα μπορούσε εξ αρχής να επιλέξει τα κατάλληλα κανάλια αποφεύγοντας τις συνέπειες που είχαμε σε αυτό το σενάριο. Τέλος, φαίνεται πως σε ακόμα μια περίπτωση το WiFi επηρεάζει το Zigbee με αποτέλεσμα πολλά δεδομένα να χάνονται και έτσι αυξάνεται η καθυστέρηση του δικτύου και να μειώνεται το Throughput ιδιαίτερα με την ενεργοποίηση των 2 επιπλέον APs.

5.3.6 Ανάλυση σεναρίων κτιρίου Πληροφορικής του Πανεπιστημίου Κύπρου

Τα σενάρια με αριθμό 3 με 6 τα προσομοιώσαμε ξανά αλλά με διαφορετική διαρρύθμιση των συσκευών. Τοποθετήσαμε δηλαδή τις συσκευές Zigbee και WiFi σε ένα σενάριο όλα μαζί προσομοιώνοντας το κτίριο της Πληροφορικής του Πανεπιστημίου Κύπρου. Πιο κάτω φαίνεται η διάταξη των συσκευών στο χώρο:



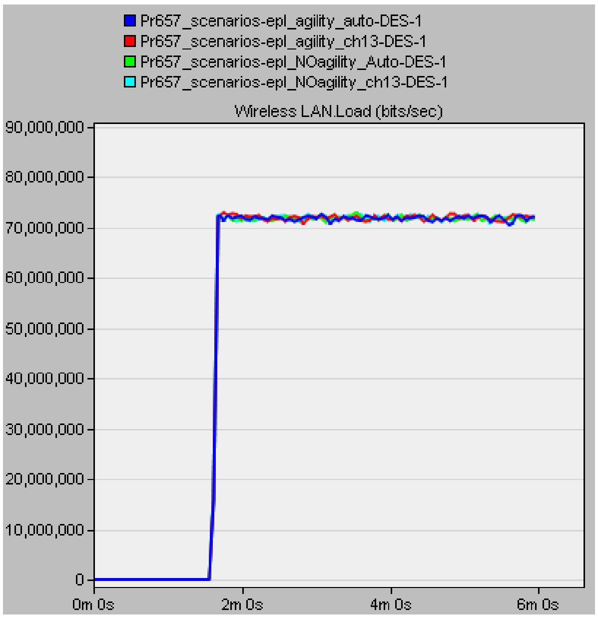
Σχήμα 5.9: Διάταξη συσκευών Zigbee και WiFi για το σενάριο στο κτίριο Πληροφορικής.

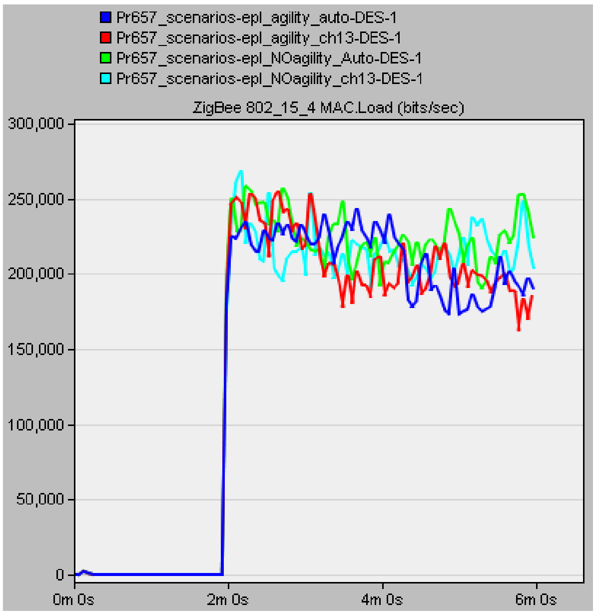
Το κτίριο της Πληροφορικής του Πανεπιστημίου Κύπρου αποτελείται από 5 πτέρυγες και η κάθε πτέρυγα έχει από 2 APs. Εμείς, προσαρμόσαμε το σενάριο έτσι ώστε κάθε πτέρυγα να έχει από ένα δίκτυο Zigbee που να αποτελείται από 4 End devices και 2 Routers. Τα APs έχουν από 3 clients για σκοπούς προσομοίωσης και άρα συνολικά μια πτέρυγα έχει 6 clients που ενώνονται στα 2 APs. Στα δύο σενάρια τα κανάλια στα APs ανατίθενται αυτόματα (Auto-assign) ενώ στα υπόλοιπα δύο είναι στο κανάλι 13. Οι αποστάσεις μεταξύ μιας πτέρυγας με μια άλλη είναι 10 m και το συνολικό μήκος του κτιρίου είναι 115 m. Ακόμη, οι αποστάσεις μεταξύ του AP και των clients είναι περίπου 10 m ενώ στο Zigbee τα End devices από τον Coordinator απέχουν 25 m ενώ από τους Router μεταξύ 10 m (κοντινές συσκευές) και 20 m (μακρινές συσκευές).

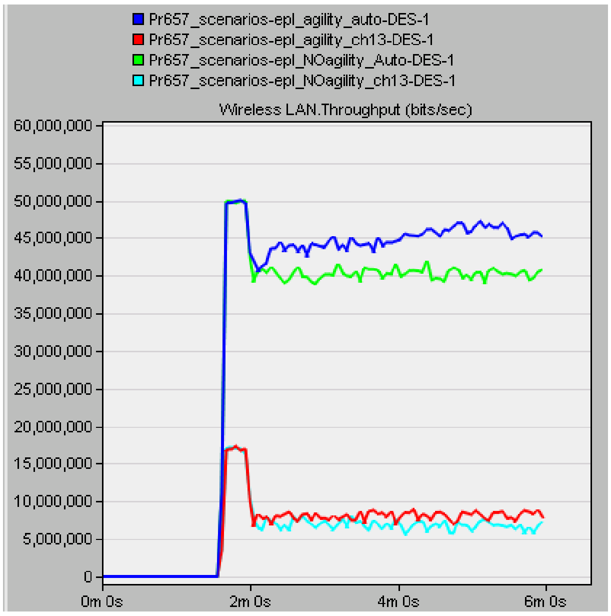
Τρέχοντας αυτό το σενάριο επιθυμούμε να μελετήσουμε την απόδοση του Zigbee και του WLAN σε ένα πραγματικό σενάριο με περισσότερες συσκευές που είναι πιο κοντά στην πραγματικότητα. Για να το πετύχουμε αυτό, ρυθμίσαμε την ισχύ μετάδοσης κάθε συσκευής έτσι ώστε να περιορίσουμε την περιοχή κάλυψης τους στην πτέρυγα που τοποθετούνται όπως φαίνεται στο σχήμα με κόκκινο χρώμα. Οι ρυθμίσεις που αλλάξαμε φαίνονται παρακάτω με τις υπόλοιπες παραμέτρους να παραμένουν οι ίδιες με τα προηγούμενα σενάρια:

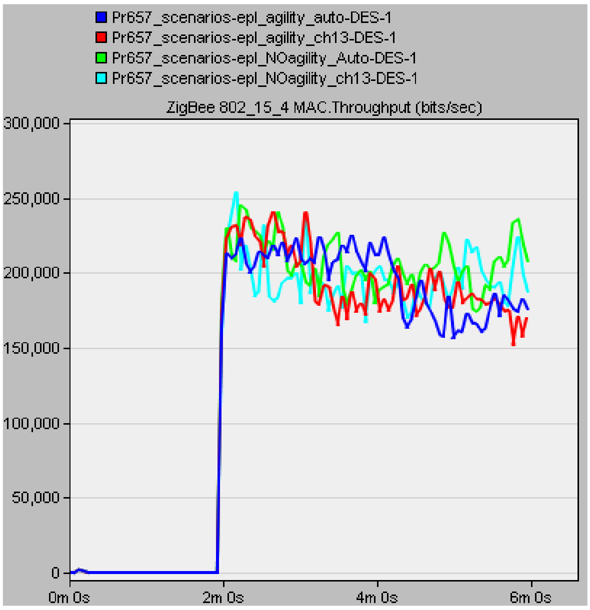
	Transmit Power (W)	Packet reception threshold (dBm)
Coordinator	0,0005	-85
End Device	0,00001	-85
Router	0,00015	-85
WLAN AP και Client	0,0018	-95

<u>Throughput και Load (bits/sec)</u>







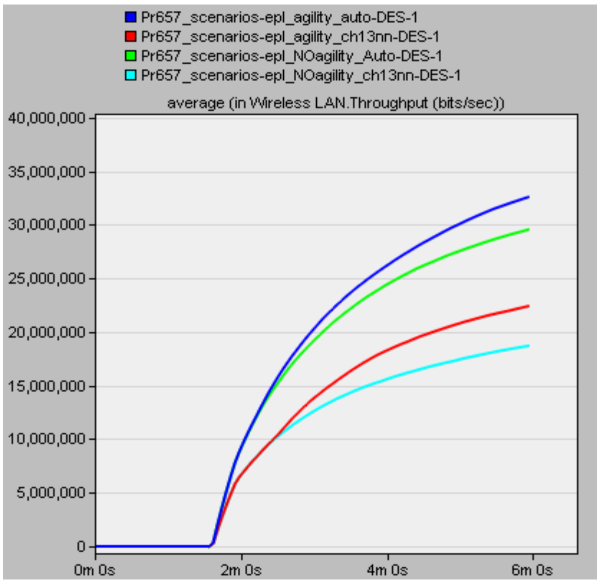


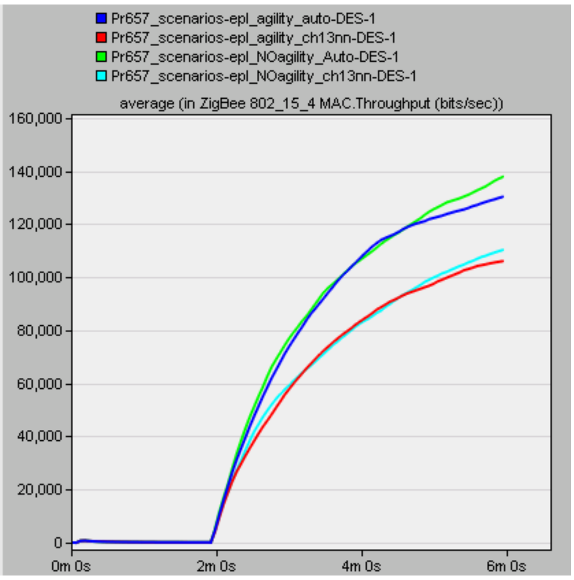
Στις πιο πάνω γραφικές βλέπουμε το Throughput και το Load των 4 σεναρίων όπου οι τεχνολογίες WiFi και Zigbee συνυπάρχουν σε κάθε πτέρυγα. Παρατηρώντας την αριστερή γραφική παράσταση που είναι το WiFi, φαίνεται πως το Load για όλα τα σενάρια είναι στα 71 Mbits/sec, όπως αναμέναμε και παραμένει το ίδιο μέχρι το τέλος. Σχετικά με το Throughput, στα 2 σενάρια όπου τα APs και τα δίκτυα Zigbee λειτουργούν σε διαφορετικά κανάλια είναι πολύ μεγαλύτερο από τα υπόλοιπα 2 σενάρια στα οποία υπάρχει επικάλυψη μεταξύ των καναλιών των δύο τεχνολογιών ανεξάρτητα από τον αν λειτουργεί ή όχι ο FRQAG.

Συγκεκριμένα, στα σενάρια όπου δεν υπάρχει πρόβλημα παρεμβολής, δηλαδή σε εκείνα που τα κανάλια λειτουργίας του AP και του Zigbee δεν επικαλύπτονται, το throughput είναι στα 40 Mbits/sec (πράσινη γραμμή) ενώ το μεγαλύτερο φτάνει στα 45 με 46 Mbits/sec στο σενάριο με ενεργοποιημένο τον FRQAG (μπλε γραμμή). Η μικρή διαφορά του throughput υπάρχει λόγω των επικαλυπτόμενων καναλιών που μπορεί να επιλέξει ο αλγόριθμος ανάθεσης καναλιών. Επίσης, στο σενάριο όπου τα APs είναι στο κανάλι 13 και επικαλύπτεται με το κανάλι του Zigbee με τον FRQAG ενεργοποιημένο (κόκκινη γραμμή) έχουμε μειωμένο throughput γύρω στα 9 Mbits/sec ενώ το χειρότερο είναι στο σενάριο που δεν λειτουργεί ο FRQAG και υπάρχει επικάλυψη με το Zigbee και έτσι το throughput πέφτει στα 6 Mbits/sec. Ο λόγος για τα δύο σενάρια που έχουν πολύ μειωμένο throughput είναι ότι όλα τα APs λειτουργούν στο κανάλι 13 και άρα προκαλείται co-channel interference αλλά παράλληλα το Zigbee βλέπουμε πως προκαλεί ελάχιστη παρεμβολή έστω με τα επικαλυπτόμενα κανάλια και αυτό εξηγεί το ότι το ένα σενάριο είναι στα 6 Mbits/sec ενώ το άλλο έχει κατά 3 Mbits/sec περισσότερο throughput. Σε αυτές τις τελευταίες περιπτώσεις, όπου έχουμε επικάλυψη των καναλιών, υπολογίζοντας το μέγιστο throughput στα 46 Mbits/sec και το χειρότερο στα 6 Mbits/sec, έχουμε δηλαδή κατά 13% μείωση περίπου του throughput στο WLAN στις χειρότερες περιπτώσεις που είναι σχετικά μικρό ποσοστό. Αλλά αν συγκρίνουμε το 71 Mbits/sec του Load με το 6 Mbits/sec του χειρότερου Throughput, τότε το 8,5% του συνολικού φόρτου (κόκκινη και γαλάζια γραμμή) είναι χρήσιμα δεδομένα σε σχέση με τα υπόλοιπα σενάρια που το ποσοστό είναι 64% των χρήσιμων δεδομένων.

Στην δεύτερη γραφική (στα δεξιά), βλέπουμε το Load και το Throughput του Zigbee και είναι φανερό πως οι δύο μετρικές ισούνται και άρα τα δεδομένα που παράγονται από το δίκτυο είναι όλα χρήσιμα. Επίσης, παρατηρούμε πως ακόμη και αν στην αρχή το καλύτερο throughput έχουν τα σενάρια με τον FRQAG ενεργοποιημένο (μπλε και κόκκινη γραμμή), λίγο μετά το 4^{ο} λεπτό αυτό αλλάζει και τα δύο άλλα σενάρια με πράσινη και γαλάζια γραμμή έχουν μεγαλύτερο throughput. Τα ωφέλιμα δεδομένα για τα πρώτα δύο σενάρια είναι στα 215 Kbits/sec (μπλε γραμμή) και στα 240 Kbits/sec (κόκκινη γραμμή) ενώ τα υπόλοιπα δύο έχουν throughput γύρω στα 200 με 215 Kbits/sec. Αυτό αντιστρέφεται μετά το 4^{ο} λεπτό και τα δύο σενάρια που προηγούνταν προηγουμένως, τώρα έχουν χαμηλότερο throughput ενώ τα υπόλοιπα δύο με γαλάζια και πράσινη γραμμή έχουν μεγαλύτερο. Να τονίσουμε ότι ακόμα και αν τα κανάλια ανατίθενται αυτόματα στο σενάριο με την πράσινη γραμμή, συμβαίνει κάποια παρεμβολή γιατί ο αλγόριθμος της ανάθεσης καναλιών βάζει και επικαλυπτόμενα κανάλια και έτσι μπορεί να επηρεαστεί το Zigbee από το WiFi. Ο λόγος της αντιστροφής των throughput των δύο σεναρίων είναι ότι στο σενάριο με την μπλε γραμμή το PAN 3 αλλάζει κανάλι και επιλέγει το κανάλι που λειτουργεί το PAN 2 και επειδή είναι γειτονικά δίκτυα υπάρχει μια παρεμβολή αφού το σήμα μπορεί να φτάσει τα 20 m περίπου στον προσομοιωτή και έτσι η μπλε γραμμή έχει μια μείωση του throughput. Το ίδιο γίνεται και με το σενάριο με την κόκκινη γραμμή όπου το PAN1 επιλέγει το κανάλι που λειτουργεί το PAN 2.

Σε αυτό το σημείο να πούμε πως στις περιπτώσεις που είχαμε αναθέσει το κανάλι 13 σε όλα τα APs (κόκκινη και γαλάζια γραμμή) φαίνεται πως επηρεάζεται περισσότερο το WLAN λόγω του co-channel interference. Για αυτό τον λόγο δοκιμάσαμε να αλλάξουμε στα 2 αυτά σενάρια τα κανάλια στα APs έτσι ώστε να αναθέσουμε το κανάλι 1 στα APs της αριστερής μεριάς ενώ σε αυτά της δεξιάς μεριάς αναθέσαμε το κανάλι 13. Τα αποτελέσματα φαίνονται στις πιο κάτω γραφικές που απεικονίζουν τον μέσο όρο του Throughput για το WLAN (αριστερά) και του Zigbee (δεξιά):

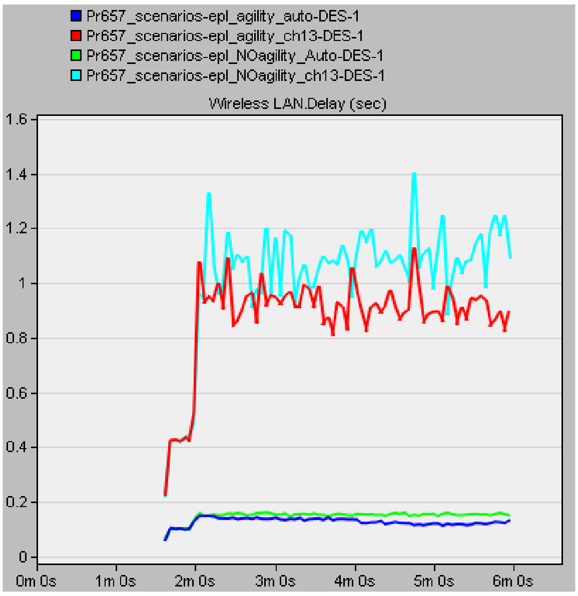


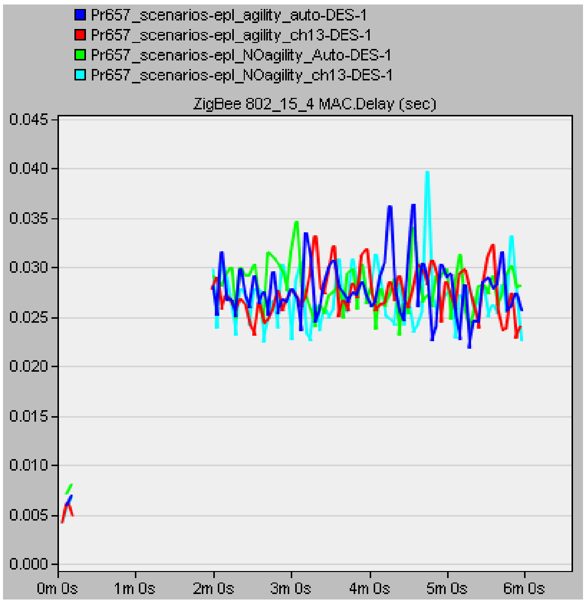


Εδώ βλέπουμε ξεκάθαρα το πόσο επηρεάζεται το Zigbee από το WLAN όπως και το αντίστροφο, αφού φαίνεται να ξεχωρίζουν οι δύο γραμμές και να έχουμε μια μείωση σχεδόν 43% στο WLAN ενώ στο Zigbee η μείωση είναι περίπου στο 15%. Έτσι, είναι φανερό που αν αποφύγουμε το co-channel interference στο WiFi τα αποτελέσματα δείχνουν ξεκάθαρα πως επηρεάζονται και οι δύο τεχνολογίες ακόμα και όταν υπάρχει μια απόσταση 10 m μεταξύ τους.

Άρα, γενικά παρατηρούμε ότι το σενάριο που επηρεάζει και τις 2 τεχνολογίες είναι αυτό που τα κανάλια των συσκευών είναι επικαλυπτόμενα και ως αποτέλεσμα έχουμε μείωση του throughput στο WiFi και στο Zigbee λόγω των παρεμβολών που δημιουργούνται μεταξύ τους.

Delay (sec)

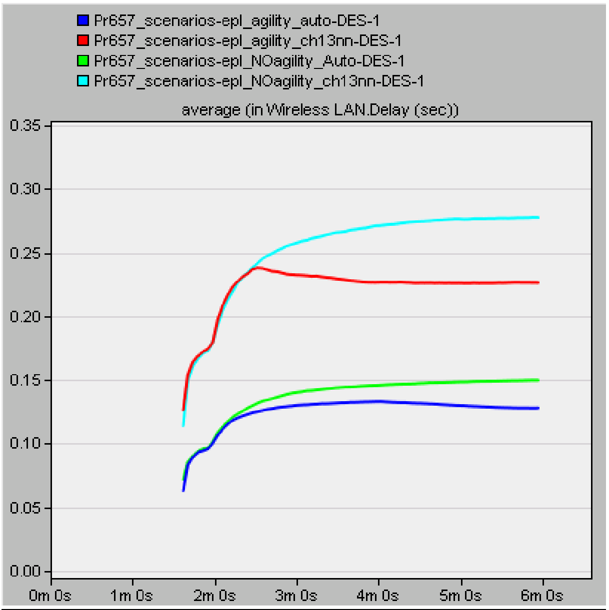


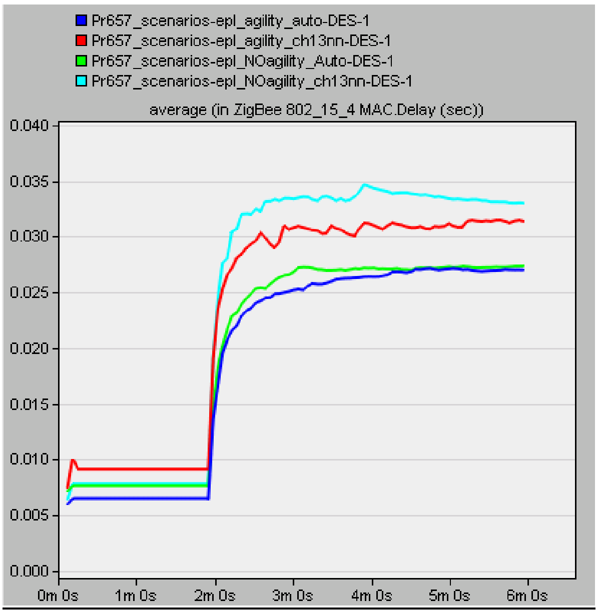


Εδώ απεικονίζεται η καθυστέρηση υπάρχει στο δίκτυο μας στα 4 σενάρια. Όπως είναι ολοφάνερο στην αριστερή γραφική που είναι το WLAN, η μεγαλύτερη καθυστέρηση υπάρχει στο σενάριο όπου το AP είναι στο κανάλι 13 και το Zigbee στο κανάλι 26 με τον αλγόριθμο FRQAG να είναι απενεργοποιημένος (γαλάζια γραμμή) και έτσι προκαλείται παρεμβολή στα δύο συστήματα με αποτέλεσμα το WiFi να έχει πάνω από 1,2 sec καθυστέρηση. Επίσης, αυξημένη καθυστέρηση βλέπουμε στο σενάριο όπου το AP είναι στο κανάλι 13 και το Zigbee στο κανάλι 26 με τον FRQAG ενεργοποιημένο (κόκκινη γραμμή) όπου φτάνει το 1 sec περίπου την καθυστέρηση. Στα υπόλοιπα 2 σενάρια η καθυστέρηση που υπάρχει είναι σχεδόν σταθερή κάτω από 200 ms με μια ελάχιστη διαφορά στο σενάριο με την μπλε γραμμή που δείχνει να έχει την χαμηλότερη καθυστέρηση.

Βλέποντας την γραφική του Zigbee, παρατηρούμε ότι στα περισσότερα σενάρια η καθυστέρηση μεταβάλλεται μεταξύ των τιμών 28 ms με 35 ms αλλά η μεγαλύτερη τιμή είναι στα 40 ms στο σενάριο με την γαλάζια γραμμή. Αξίζει να σημειώσουμε πως η χαμηλότερη καθυστέρηση σε όλη την διάρκεια της προσομοίωσης παρατηρείται στο σενάριο όπου το AP είναι στο κανάλι 13 και το Zigbee στο κανάλι 26 με τον FRQAG ενεργοποιημένο (κόκκινη γραμμή) που πολλές φορές έχει παρόμοιες τιμές και με το σενάριο που φαίνεται με μπλε γραμμή.

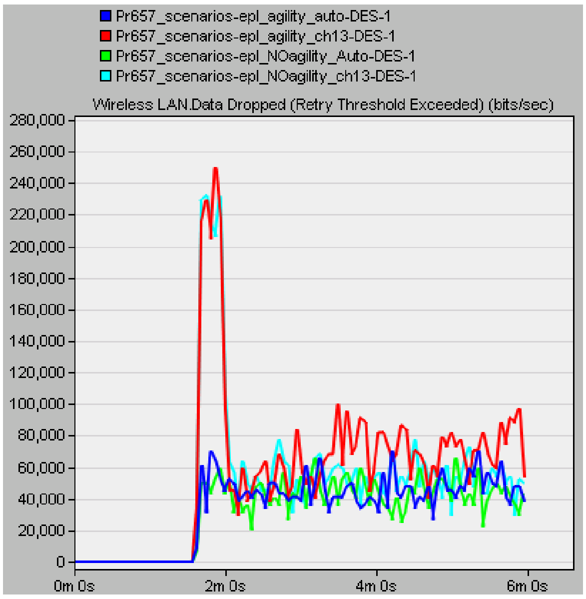
Όπως αναφέραμε και στη μετρική του Throughput, για να αποφύγουμε το co-channel interference αλλάξαμε τα κανάλια λειτουργίας των APs και πήραμε τις πιο κάτω γραφικές του μέσου όρου του Delay για τις δύο τεχνολογίες:

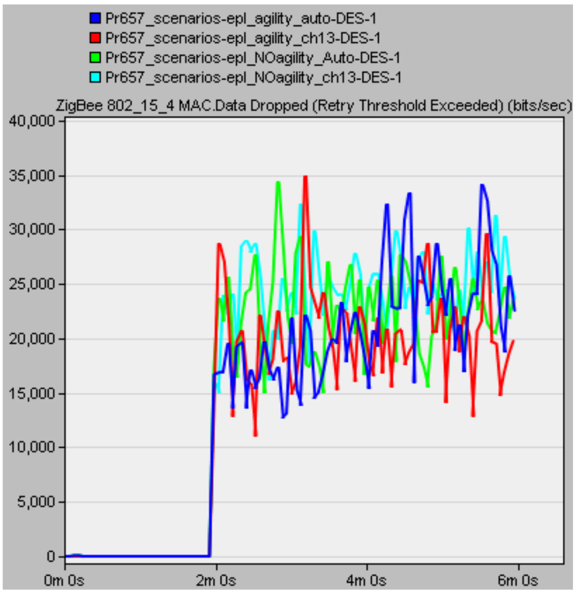




Με την αποφυγή της παρεμβολής μεταξύ των συσκευών του WiFi παρατηρούμε πως η καθυστέρηση φτάνει το μέγιστο τα 280 ms αντί στο 1 δευτερόλεπτο που είχαμε προηγουμένως. Επίσης, η κόκκινη γραμμή φτάνει τα 230 ms ενώ τα υπόλοιπα 2 σενάρια είναι στα 150 ms που σχετικά είναι χαμηλές τιμές σε σχέση με αυτές που είχαμε στο προηγούμενο σενάριο. Το Zigbee φαίνεται πως επηρεάζεται πράγματι από το WiFi αφού ξεχωρίζουν τα δύο σενάρια (γαλάζια και κόκκινη γραμμή) που φτάνουν τα 34 ms ενώ τα άλλα 2 σενάρια ακολουθούν την ίδια περίπου πορεία μέχρι τα 26 ms. Έτσι, έχουμε μια αύξηση κατά 57% στην καθυστέρηση του WLAN ενώ στο Zigbee έχουμε 25% μεταβολή προς τα πάνω.

<u>Data Dropped (Retry Threshold Exceeded) (bits/sec)</u>

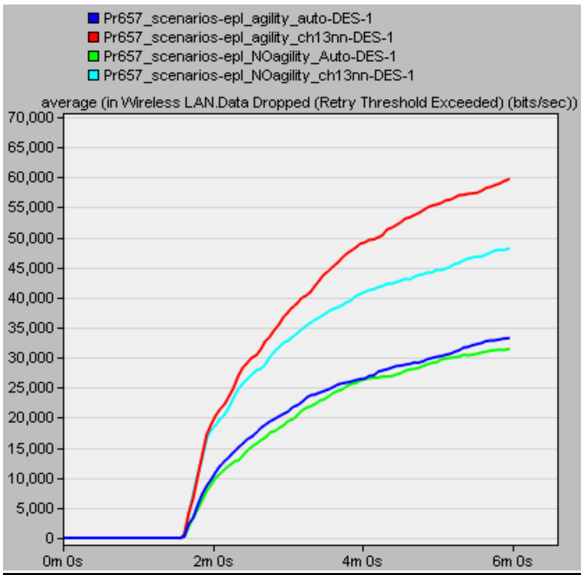


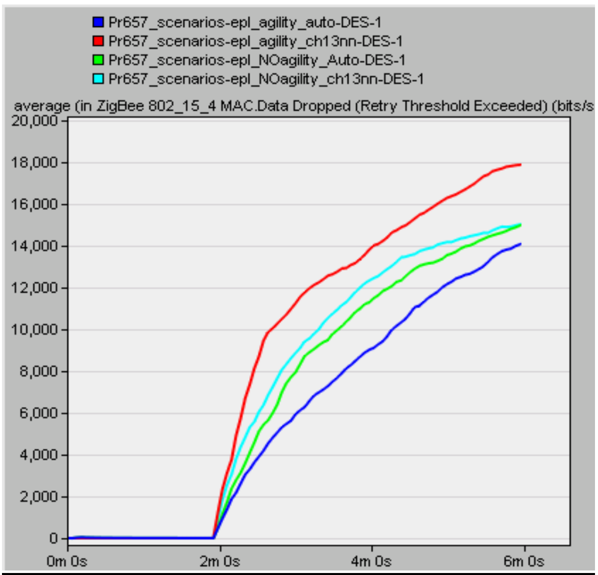


Σε αυτές τις γραφικές παραστάσεις βλέπουμε το Data Dropped στα δίκτυα WLAN και Zigbee. Στα αριστερά φαίνεται το WLAN, όπου τα δεδομένα που χάνονται στα σενάριο που υπάρχει επικάλυψη καναλιών (κόκκινη και γαλάζια γραμμή) φτάνουν αρχικά το μέγιστο 240 Kbits/sec ενώ μετά κατεβαίνουν στα 60 Kbits/sec. Η απότομη αύξηση των δύο σεναρίων συμβαίνει γιατί αρχικοποιούνται τα δίκτυα στα πρώτα λεπτά και στέλνονται πολλά πακέτα ελέγχου και δεδομένων αλλά λόγω συγκρούσεων χάνονται πολλά δεδομένα. Στη συνέχεια, φαίνεται ότι το σενάριο που ξεχωρίζει πάλι είναι αυτό με την κόκκινη γραμμή γιατί έχει ανοδική πορεία μέχρι το $3^{ο}$ λεπτό που χάνονται 90-100 Kbits/sec δεδομένα και σε αυτό τον ρυθμό παραμένει μέχρι το τέλος, αν δεν λάβουμε υπόψη μας κάποια σκαμπανεβάσματα. Τα υπόλοιπα σενάρια κυμαίνονται στα 40-60 Kbits/sec με πολλές αυξομειώσεις.

Από την γραφική του Zigbee στα δεξιά, βλέπουμε πως τα δεδομένα που χάνονται στα 2 σενάρια που είναι απενεργοποιημένος ο FRQAG (γαλάζια και πράσινη γραμμή) ο ρυθμός που έχουμε απώλεια δεδομένων κυμαίνεται στα 25 με 30 Kbits/sec και είναι από τους μεγαλύτερους σε σχέση με τα άλλα σενάρια. Στα υπόλοιπα 2 σενάρια, βλέπουμε ένα απότομο spike στο $3^{ο}$ λεπτό να φτάνει τα 35 Kbits/sec για την κόκκινη γραμμή καθώς και μια απότομη αύξηση του ρυθμού στα 33 Kbits/sec για την μπλε γραμμή στο $4^{ο}$ λεπτό. Συγκεκριμένα, στο $3^{ο}$ λεπτό όπως θα δούμε και την γραφική του καναλιού λειτουργίας, ένα από τα δίκτυα Zigbee αποφασίζει να αλλάξει κανάλι και γι’ αυτό έχουμε ξαφνική απώλεια των δεδομένων σε εκείνη την στιγμή. Το ίδιο συμβαίνει και στο $4^{ο}$ λεπτό με το σενάριο της μπλε γραμμής αλλά η διαφορά είναι ότι η μπλε γραμμή έχει λιγότερη απώλεια δεδομένων στο μεγαλύτερο μέρος της προσομοίωσης εκτός από το τέλος ενώ η κόκκινη γραμμή έχει μεγαλύτερο ρυθμό απώλειας γενικά. Αυτό συμβαίνει γιατί τα APs στο σενάριο με την κόκκινη γραμμή είναι στο κανάλι 13 και άρα τα δίκτυα Zigbee πρέπει να αποφύγουν το κανάλι 26 με τον αλγόριθμο FRQAG αλλά λόγω λανθασμένων αποφάσεων επιλέγουν επικαλυπτόμενα κανάλια και έτσι έχουμε αυξημένη απώλεια δεδομένων.

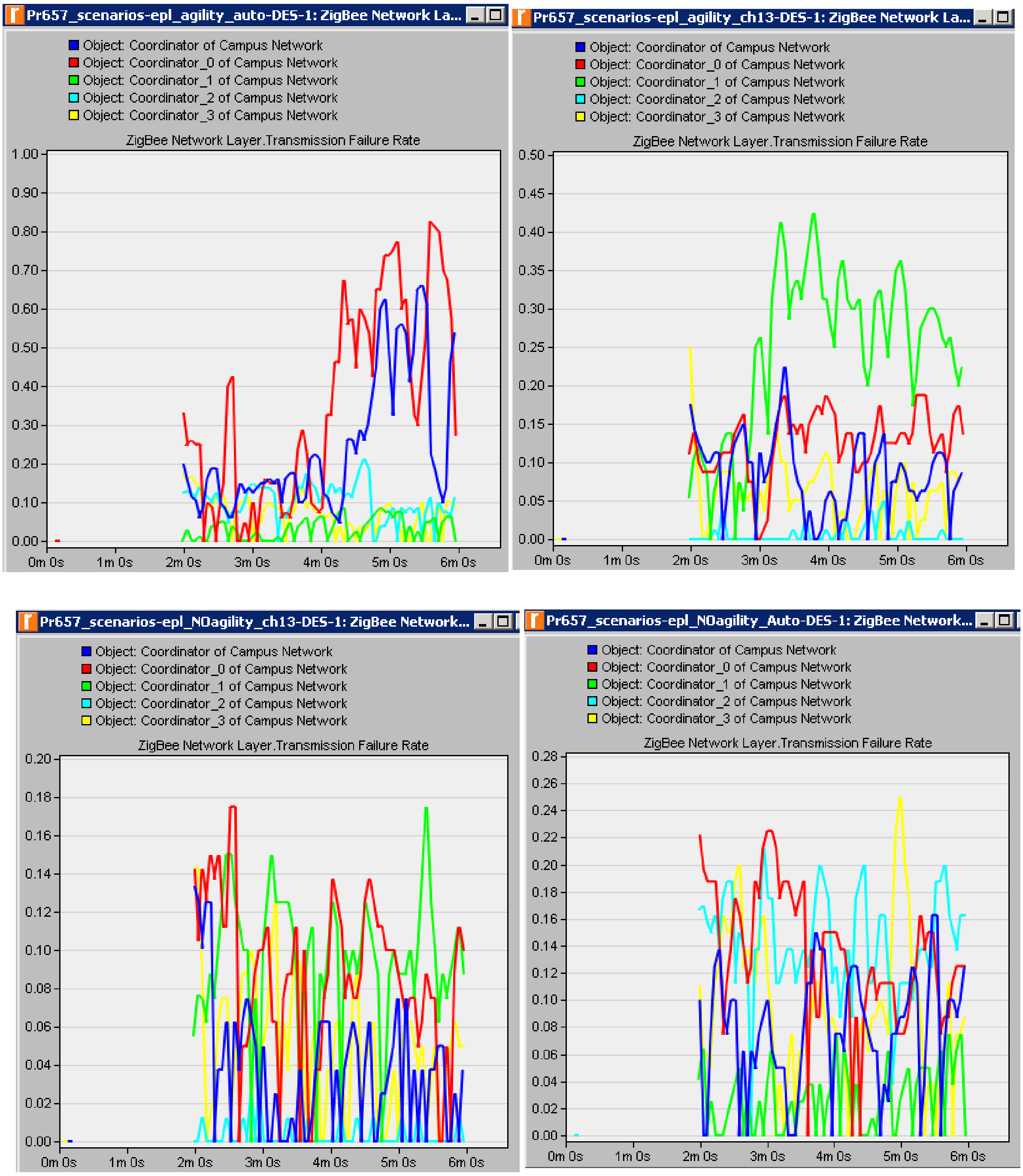
Έχοντας υπόψη αυτά, αναθέσαμε στα APs το κανάλι 1 και 13 στα δύο σενάρια που υπάρχει παρεμβολή και εξήγαμε τις πιο κάτω γραφικές για το μέσο όρο των Data Dropped:





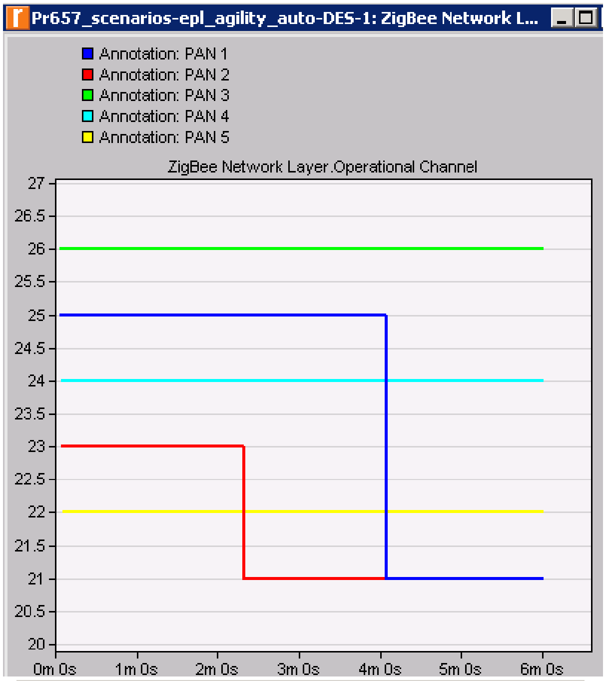
Όπως παρατηρούμε, τα δύο σενάρια που ξεχωρίζουν είναι αυτά με τα επικαλυπτόμενα κανάλια μεταξύ του Zigbee και του WLAN όπου το τελευταίο κατά μέσο όρο χάνει δεδομέναν κατά μέσο όρο 60 Kbits/sec που είναι σχετικά λίγα σε σχέση με το Throughput ενώ στο Zigbee ο μέγιστος ρυθμός απώλειας (κόκκινη γραμμή) είναι στα 18 Kbits/sec που αν υπολογίσουμε το Throughput που είχαμε σε αυτές τις περιπτώσεις τα 110 Kbits/sec, η απώλεια είναι περίπου 17%. Καταλήγοντας, μπορούμε να πούμε πως το Zigbee έχει μεγαλύτερη απώλεια δεδομένων σε σχέση με το WLAN και γενικά επηρεάζεται περισσότερο από τις παρεμβολές λόγω και της χαμηλής ισχύος των συσκευών του.

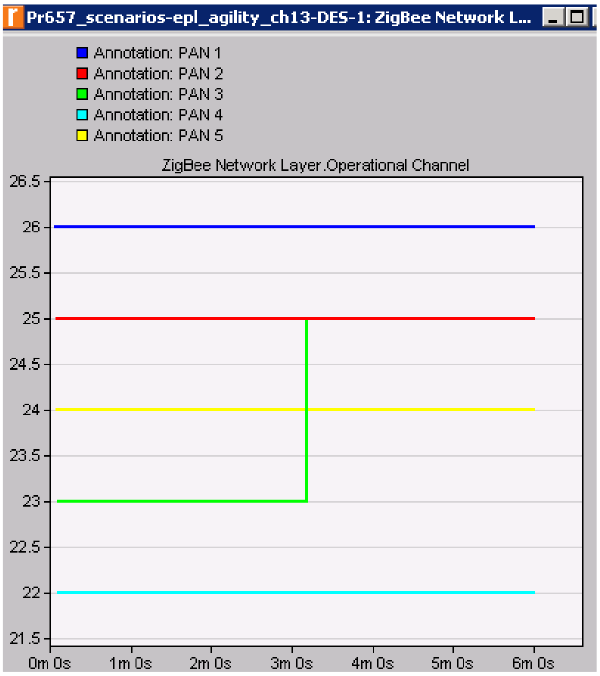
Zigbee Coordinators Transmission Failure Rate (%)

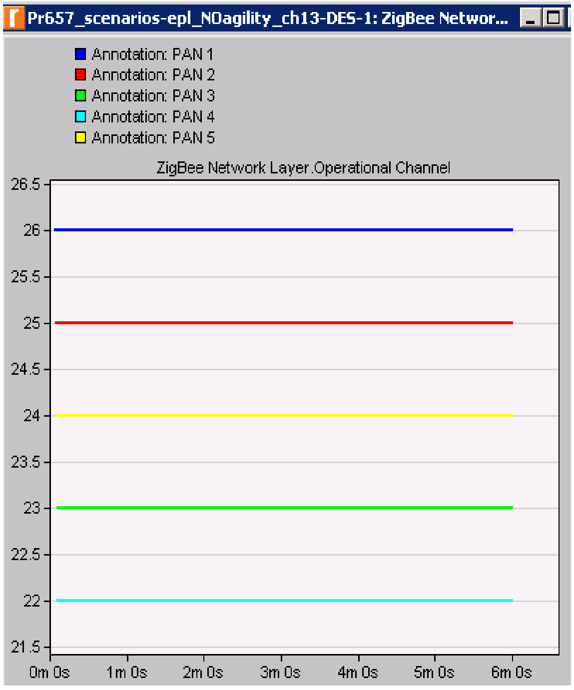


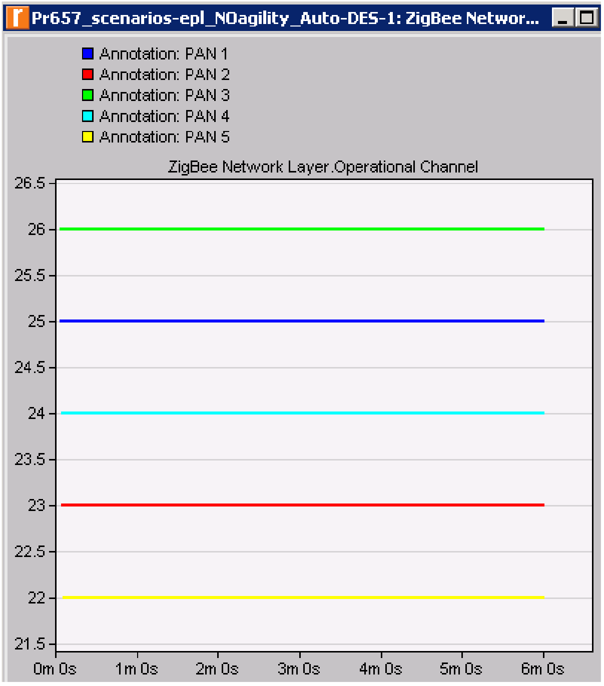
Οι πιο πάνω γραφικές απεικονίζουν το ποσοστό αποτυχίας μετάδοσης των Coordinators στα 5 δίκτυα Zigbee που έχουμε στα σενάρια μας. Ξεκινώντας από την πρώτη γραμμή, βλέπουμε τα σενάρια που είναι ενεργοποιημένος ο FRQAG και παρατηρούμε πως τα ποσοστά αποτυχίας μετάδοσης σε αυτά τα σενάρια είναι μεγαλύτερα από τα υπόλοιπα 2 σενάρια. Συγκεκριμένα, στη πρώτη γραφική (πάνω αριστερά) ο Coordinator_0 είναι ο πρώτος που φτάνει το 40% και άρα αλλάζει κανάλι και γι' αυτό πέφτει το ποσοστό κάτω από 20%. Στη συνέχεια, ειδικότερα κοντά στο 4^{ο} λεπτό βλέπουμε τους Coordinator του PAN 1 (μπλε γραμμή) και PAN 2 (κόκκινη γραμμή) να έχουν αυξητική τάση στο ποσοστό αποτυχίας διάδοσης και φτάνουν το 70% και 80% αντίστοιχα. Η απότομη αύξηση οφείλεται στο ότι το PAN 1 αποφασίζει να αλλάξει κανάλι λόγω αναφορών που παίρνει από τα Routers και επιλέγει το κανάλι 21 που λειτουργεί το PAN 2. Έτσι, αν και τα 2 δίκτυα έχουν 20 m απόσταση που τους χωρίζει, το σήμα φτάνει στη γειτονική πτέρυγα και δημιουργείται παρεμβολή με αποτέλεσμα να έχουμε σκαμπανεβάσματα με ποσοστό αποτυχία μεγαλύτερο του 25%. Οι υπόλοιποι Coordinators παραμένουν με ποσοστό κάτω από 20% όπως βλέπουμε. Στην πάνω δεξιά γραφική παρατηρούμε τον Coordinator PAN 3 (πράσινη γραμμή) από το 3^{ο} λεπτό να έχει ποσοστά αποτυχίας πάνω από 25% και ως εκ τούτου θα αλλάξει κανάλι αλλά θα επιλέξει το κανάλι του PAN 2. Το κανάλι όμως που επιλέγει είναι το 25 το οποίο έχει επικάλυψη με το κανάλι 12 του AP που βρίσκεται το PAN 3 και έτσι έχουμε παραμονή του ποσοστού αποτυχίας σε αυτούς τους ρυθμούς. Όσον αφορά τα υπόλοιπα δίκτυα Zigbee, δεν έχουμε κάποια αύξηση πάνω από 25%. Στις 2 γραφικές της κάτω σειράς όπου απεικονίζουν τα σενάρια που ο αλγόριθμος FRQAG είναι απενεργοποιημένος, τα ποσοστά αποτυχίας είναι κάτω από 18% αλλά αυτό δεν σημαίνει πως είναι μικρό ποσοστό αφού τα πακέτα που στέλνονται στο Zigbee είναι λίγα και το ποσοστό αυτό είναι σημαντικό αφού υποφέρουν από απώλειες δεδομένων.

Operational Channel



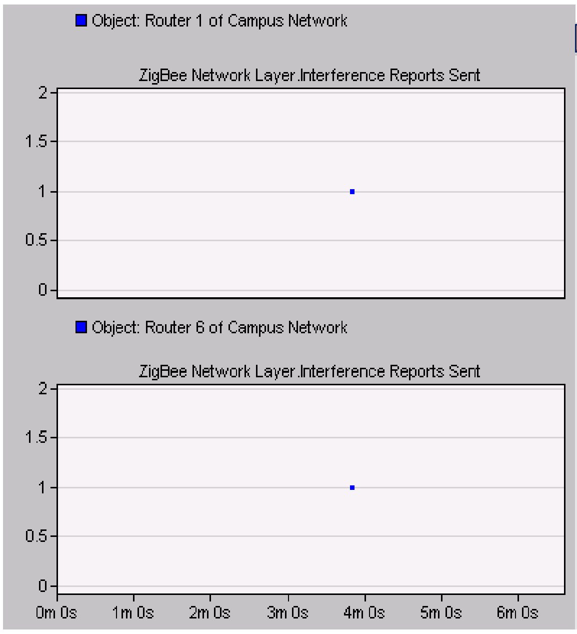


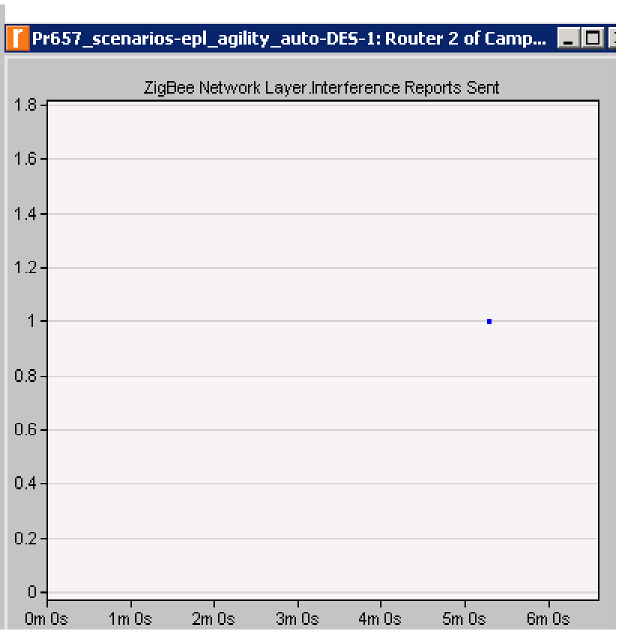




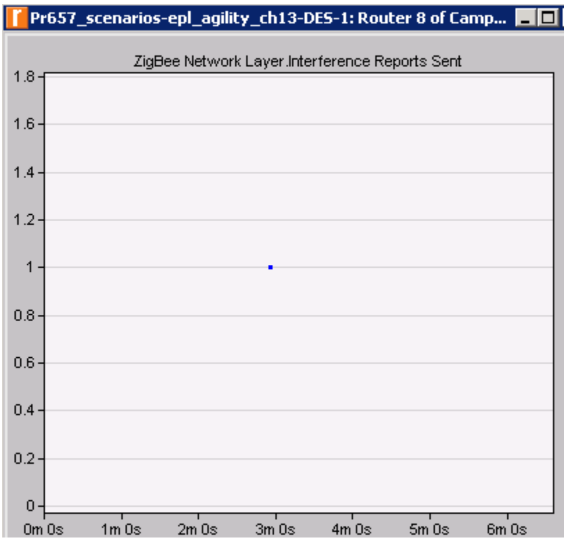
Στις παραπάνω γραφικές παρουσιάζονται τα κανάλια που λειτουργεί το κάθε δίκτυο Zigbee ανάλογα με τον αριθμό PAN ID στα 4 σενάρια που μελετάμε. Στην πρώτη γραμμή είναι τα σενάρια που έχουν ενεργοποιημένο τον FRQAG και η κάτω γραμμή τα σενάρια που δεν τον έχουν ενεργοποιημένο. Όπως βλέπουμε, στα πρώτα 2 σενάρια έχουμε αλλαγή καναλιού από 2 δίκτυα, το PAN 1 και 2, διότι τα ποσοστά αποτυχίας ξεπερνούν το 25%. Το κανάλι που επιλέγουν είναι το 21 και τα δύο δίκτυα με αποτέλεσμα να έχουμε κάποιες παρεμβολές. Το ίδιο φαινόμενο γίνεται και στην πάνω δεξιά γραφική που εδώ μόνο το PAN 3 αλλάζει από το κανάλι 23 στο κανάλι 25 που είναι του PAN 2. Στην κάτω γραμμή είπαμε πως είναι οι γραφικές των σεναρίων που δεν έχουν ενεργοποιημένο τον FRQAG και γι’ αυτό δεν βλέπουμε κάποια αλλαγή στα κανάλια λειτουργίας.

Πιο κάτω φαίνονται οι κόμβοι που στέλνουν τα Interference Reports σε κάθε PAN στα σενάρια με ενεργοποιημένο τον FRQAG. Στο PAN 1 που φαίνεται στην αριστερή γραφική, στέλνονται αναφορές από τα Routers 1 και 6 λίγο πριν το $4^{ο}$ λεπτό όταν τους ζητείται από τον Coordinator. Από την άλλη, στην δεξιά γραφική φαίνεται ο Router 2 του PAN 2 να στέλνει μόνος του λίγο μετά το $5^{ο}$ λεπτό ενώ ο Router 7 δεν στέλνει καθόλου γιατί δεν έχει σύνδεση με το δίκτυο εκείνη την στιγμή.

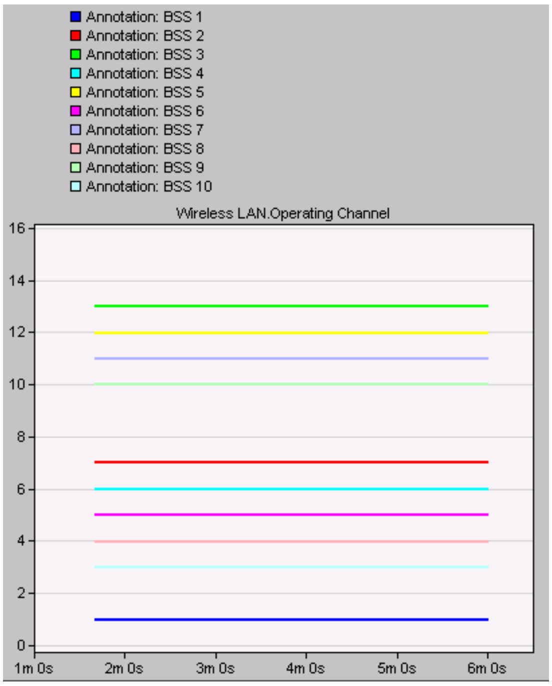




Στην από κάτω γραφική φαίνεται η αναφορά που στέλνει ο Router 8 του PAN 3 στο σενάριο που τα APs είναι το κανάλι 13. Η αναφορά στέλνεται μόνο από αυτόν τον Router στο $3^{ο}$ λεπτό ενώ θα έπρεπε να το κάνει και ο Router 3. Εντούτοις, επειδή ο αλγόριθμος FRQAG θέλει μόνο μια αναφορά από ένα Router , θα εκτελεστεί και θα αλλάξει το κανάλι λειτουργίας.



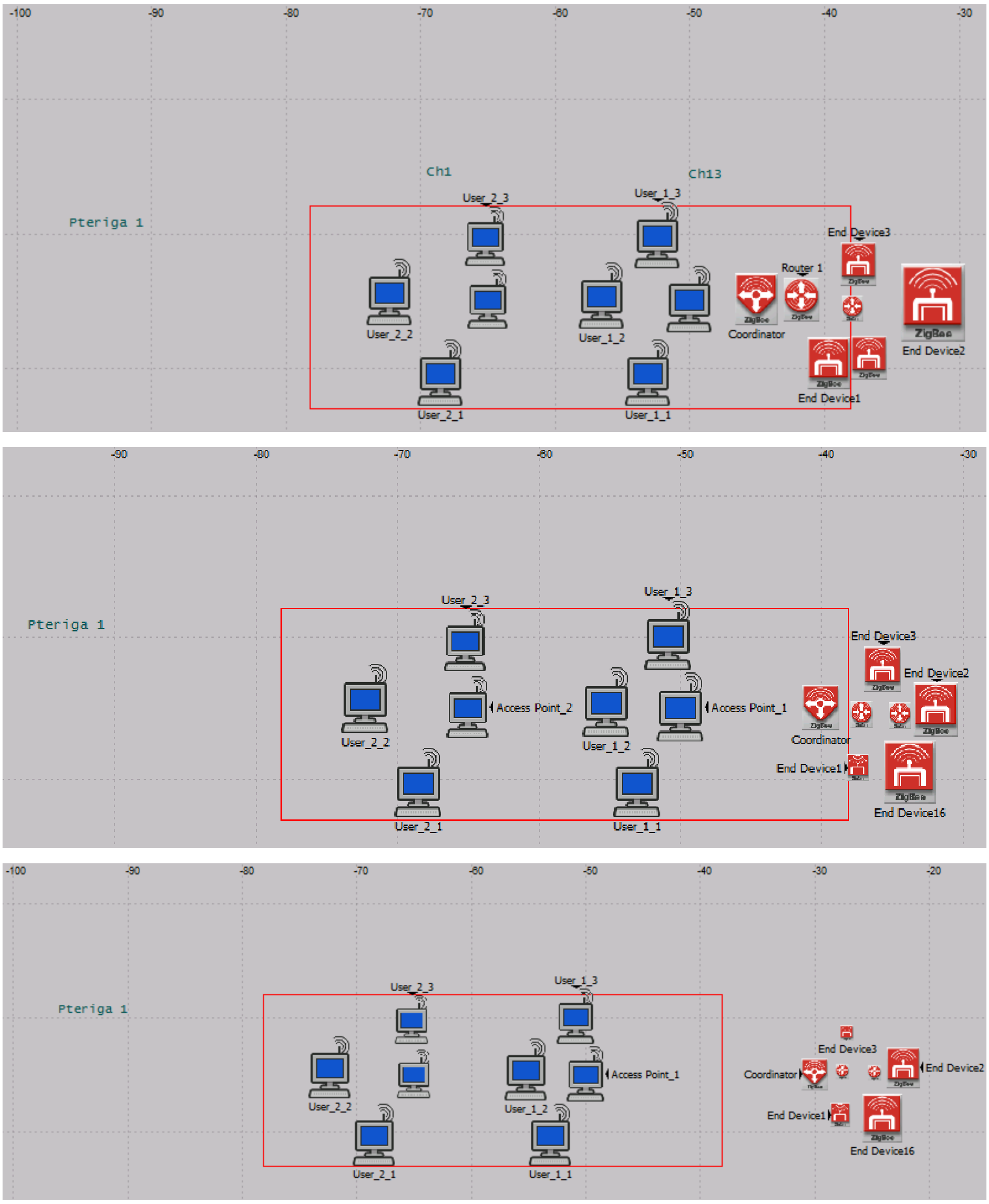
Τέλος, πιο κάτω φαίνονται τα κανάλια λειτουργίας του κάθε BSS των WLAN δικτύων. Η ανάθεση των καναλιών ακολουθεί τον αλγόριθμο που επιλέγει πρώτα τα μη επικαλυπτόμενα κανάλια και αναθέτει στο τέλος όλα τα κανάλια αν χρειαστεί.



<u>Συμπεράσματα σεναρίων:</u> Στα σενάρια που μελετήσαμε είχαμε 5 δίκτυα Zigbee για όλο το κτίριο και 2 δίκτυα WLAN σε κάθε πτέρυγα. Μελετώντας τα σενάρια, το χειρότερο καταλήγουμε να είναι εκείνο που δεν λειτουργεί ο FRQAG και υπάρχει επικάλυψη με το Zigbee. Σε αυτό το σενάριο έχουμε δραματική μείωση του throughput, αυξημένη καθυστέρηση και απώλεια δεδομένων στο δίκτυο. Αξίζει να τονίσουμε πως παρόμοια κατάσταση βρίσκεται και το ίδιο σενάριο αλλά με ενεργοποιημένο τον FRQAG. Ο μηχανισμός του FRQAG που βοηθά για να μειώσει την παρεμβολή στο δίκτυο παίρνει λάθος αποφάσεις όταν έχουμε μεγάλο ποσοστό αποτυχίας μετάδοσης. Συγκεκριμένα, στην μια περίπτωση επιλέγει κανάλια που είναι κατειλημμένα από κάποιο άλλο PAN δίκτυο και έτσι δημιουργούνται προβλήματα συνύπαρξης 2 δικτύων Zigbee έστω και αν χωρίζονται από μια απόσταση 20 m γιατί στον προσομοιωτή οι αποστάσεις που καλύπτει το σήμα δεν είναι πάντα υπολογίσιμες. Ακόμη, στην άλλη περίπτωση το κανάλι που επιλέγει για να αποφύγει την παρεμβολή είναι επικαλυπτόμενο με το κανάλι 13 που λειτουργούν τα APs και έτσι το πρόβλημα γίνεται ακόμη χειρότερο.

5.3.7 Σενάρια με διαφορετικές αποστάσεις μεταξύ Zigbee και WiFi

Στο σενάριο αυτό προσπαθούμε να διαπιστώσουμε αν η αλλαγή στην απόσταση μεταξύ των δύο δικτύων βελτιώνει την απόδοση τους έτσι ώστε να μειωθούν οι παρεμβολές. Έτσι, δημιουργήσαμε 3 σενάρια βασισμένα στο τελευταίο σενάριο με το κτίριο της Πληροφορικής, όπου οι αποστάσεις μεταξύ των 2 δικτύων και συγκεκριμένα μεταξύ των Coordinators με τα APs είναι 5 m, 10 m, και 20 m. Με αυτές τις αποστάσεις θα συγκρίνουμε την απόδοση των δικτύων για να δούμε αν διακρίνεται κάποια βελτίωση καθώς μεγαλώνει η απόσταση μεταξύ τους. Η διάταξη των συσκευών φαίνεται στις παρακάτω εικόνες:



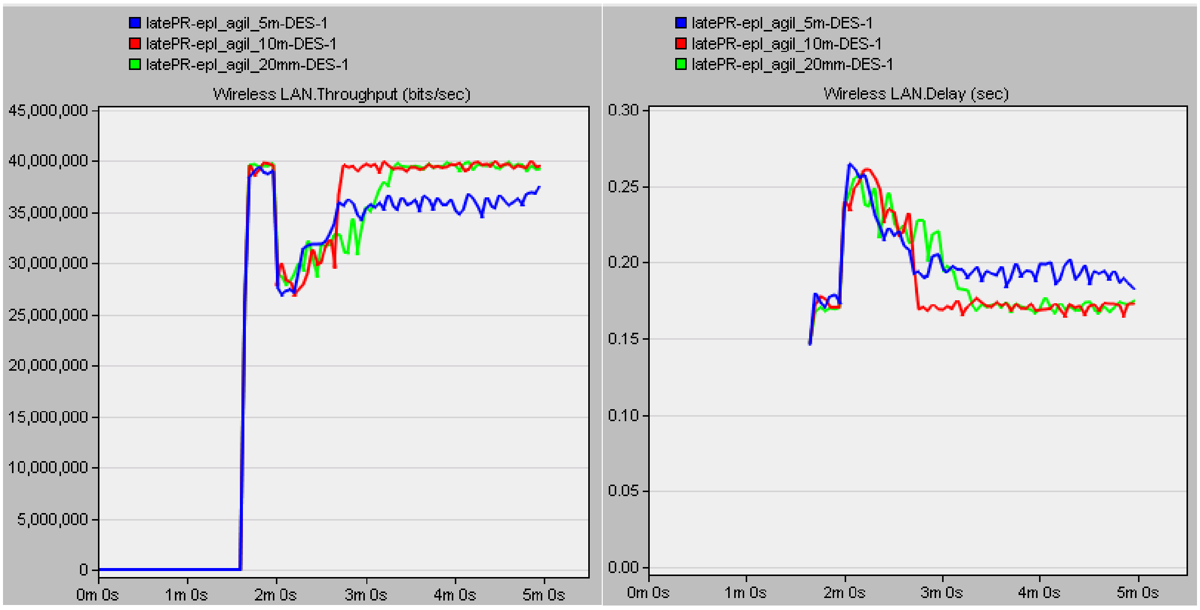
Σχήμα 6.1: Διάταξη συσκευών Zigbee και WiFi για το σενάριο με διαφορετικές αποστάσεις. Εικόνα 1: 5 m, εικόνα 2: 10 m, εικόνα 3: 20m.

Όπως φαίνεται, η πρώτη εικόνα δείχνει το σενάριο που η απόσταση μεταξύ του Coordinator και του AP είναι 5 m, η δεύτερη είναι στα 10 m και η 3η στα 20 m. Οι εικόνες δείχνουν μόνο την πτέρυγα 1 αλλά υπάρχουν όλες οι 5 πτέρυγες που είχαμε στο σενάριο του κτιρίου της Πληροφορικής του Πανεπιστημίου Κύπρου. Να πούμε πως τα APs που βρίσκονται στην αριστερή μεριά λειτουργούν στο κανάλι 1 ενώ στην δεξιά μεριά στο κανάλι 13 για να μην έχουμε co-channel interference. Οι υπόλοιπες ρυθμίσεις για τις συσκευές είναι οι ίδιες με τα σενάρια στο προηγούμενο κεφάλαιο όπως και η ισχύς που προσαρμόσαμε στις συσκευές για να είναι στα όρια της κάθε πτέρυγας και που φαίνονται στον πιο κάτω πίνακα:

	Transmit Power (W)	Packet reception threshold (dBm)
Coordinator	0,0005	-85
End Device	0,00001	-85
Router	0,00015	-85
WLAN AP και Client	0,0018	-95

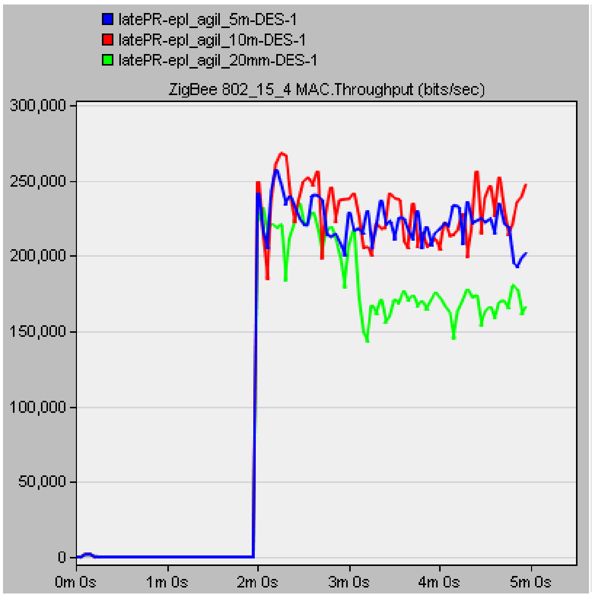
Μετά από την εκτέλεση των 5 λεπτών πήραμε τα αποτελέσματα του Throughput και Delay που αναλύουμε πιο κάτω για τα 3 σενάρια.

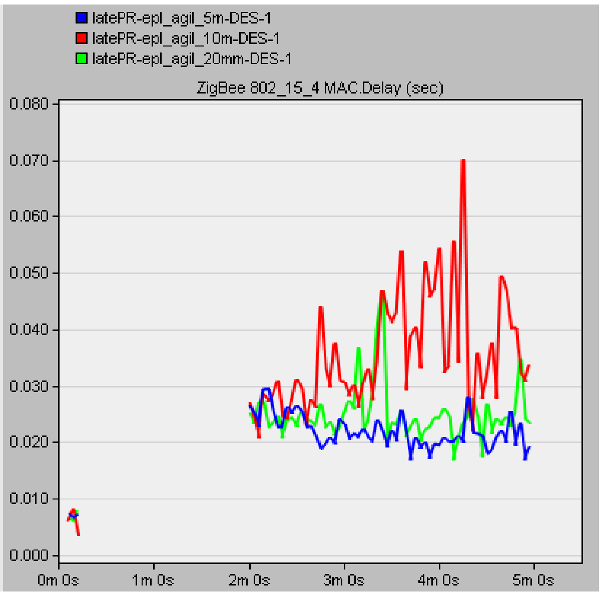
<u>Wireless LAN Throughput (bits/sec) και Delay (sec)</u>



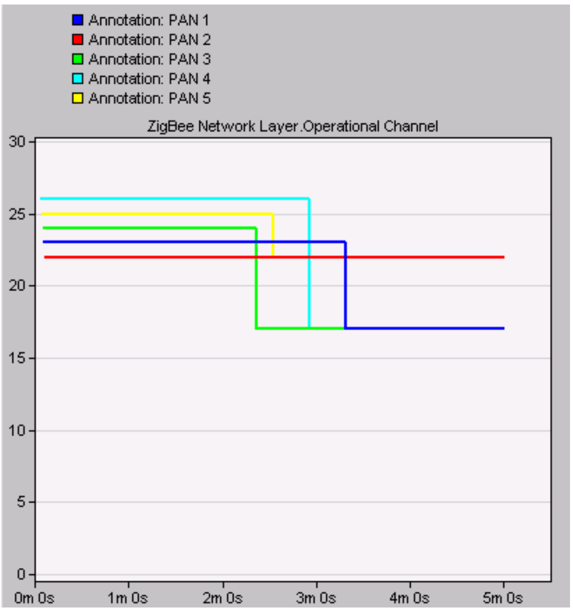
Οι γραφικές δείχνουν το Throughput (αριστερά) και το Delay (δεξιά) για το WLAN. Όπως φαίνεται και είναι αναμενόμενο, το Throughput στα 5 m είναι στα 35 Mbps ενώ στις άλλες 2 περιπτώσεις είναι στα 40 Mbps ,δηλαδή έχουμε μια αύξηση 12,5% όταν έχουμε το Zigbee στα 5 μέτρα μακριά από το AP. Σχετικά με την καθυστέρηση, η διαφορά των 2 σεναρίων στα 10 και 20 m με το σενάριο στα 5 m είναι 4 ms που είναι μικρή διαφορά αλλά φαίνεται πως πάλι επηρεάζεται το WLAN.

<u>Zigbee Throughput (bits/sec) και Delay (sec)</u>



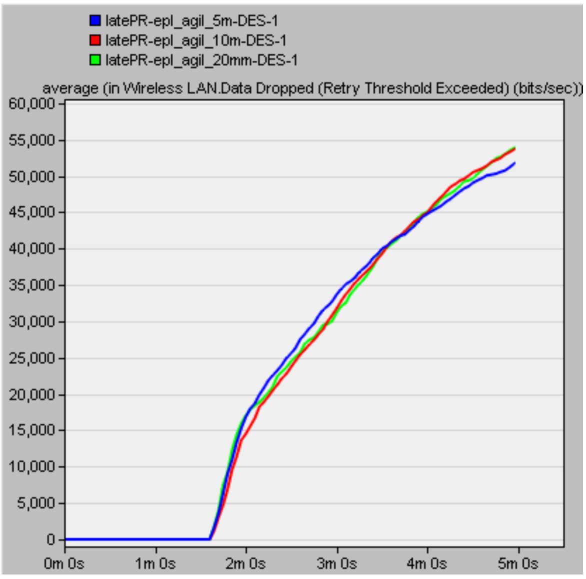


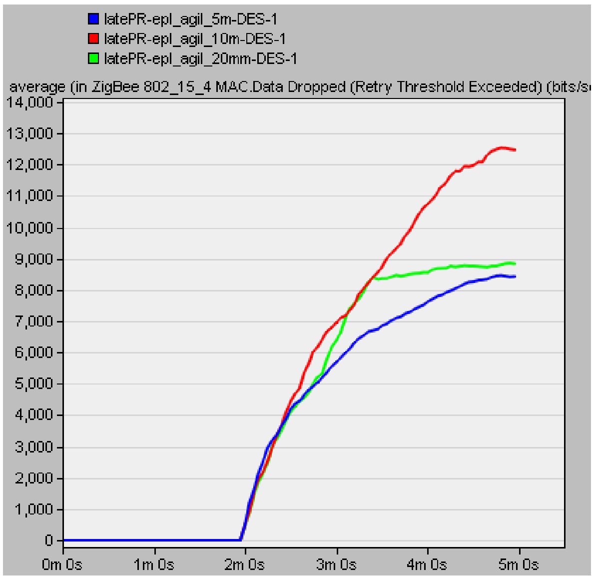
Στην αριστερή γραφική βλέπουμε την διαφορά του Throughput στα 3 σενάρια το οποίο μπορούμε να πούμε πως το χειρότερο είναι στο σενάριο στα 20 m και το καλύτερο στα 10 m. Συγκεκριμένα, στα 5 m έχουμε 220 Kbps, στα 10 m έχουμε 240 Kbps περίπου, και στα 20 m από 230 Kbps πέφτει στα 170 Kbps. Ο λόγος που στα 20 m πέφτει στο 3^{ο} λεπτό στα 170 Kbps είναι γιατί τα 3 από τα Zigbee δίκτυα επιλέγουν το ίδιο κανάλι 17 και έτσι επηρεάζονται το ένα με το άλλο γιατί επίσης η απόσταση μεταξύ των Zigbee είναι 20 m περίπου. Όσον αφορά την καθυστέρηση, η μεγαλύτερη τιμή παρατηρείται στα 70 ms από το σενάριο με την κόκκινη γραμμή ενώ τα υπόλοιπα δύο σενάρια η καθυστέρηση είναι μικρότερη από 40 ms. Πιο κάτω βλέπουμε τα κανάλια λειτουργίας των PAN του Zigbee.



Εδώ βλέπουμε τα κανάλια που λειτουργούν τα δίκτυα Zigbee στο σενάριο που η απόσταση είναι 20 m των 2 τεχνολογιών. Αυτό που απεικονίζεται είναι ότι τα δίκτυα των PAN 3, PAN 4 και PAN 1 επιλέγουν το ίδιο κανάλι 17 όταν εκτελεστεί ο αλγόριθμος του FRQAG στο κάθε ένα. Το PAN 3 από το κανάλι 24, το PAN 4 από το κανάλι 26 και το PAN 1 από το κανάλι 23 επιλέγουν όλοι το κανάλι 17 που θεωρούν πως είναι καλύτερο από τα υπόλοιπα. Ως αποτέλεσμα, αντί να βελτιώνουν την απόδοση του συστήματος, όπως είδαμε μειώνεται και έτσι έχουμε χειρότερη απόδοση από αυτή που έχουμε στα 5 m.

<u>Data Dropped (Retry Threshold Exceeded) - Average (bits/sec)</u>





Σε αυτές τις γραφικές βλέπουμε τα δεδομένα που χάνονται στο WLAN και στο Zigbee όταν αλλάζουμε την απόσταση μεταξύ των δύο δικτύων. Στην αριστερή γραφική του WLAN φαίνεται πως το σενάριο με τα 5 m απόσταση έχει μεγαλύτερη απώλεια στη μεγαλύτερη διάρκεια της προσομοίωσης αλλά η διαφορά με τα υπόλοιπα σενάρια είναι πολύ μικρή.

Συγκεκριμένα, φτάνει στα 54 Kbps η μέγιστη τιμή που έχουν τα 2 σενάρια που φαίνονται με την κόκκινη και πράσινη γραμμή.

Από την άλλη, στην δεξιά γραφική παράσταση φαίνεται ότι το Zigbee έχει μεγαλύτερη απώλεια δεδομένων στα 10 m απόσταση παρότι στα άλλα 2 σενάρια αφού στο πρώτο σενάριο φτάνει τα 12,5 Kbps περίπου ενώ τα άλλα 2 σενάρια έχουν απώλεια κάτω από τα 9 Kbps.

5.4 Εισηγήσεις για βελτίωση απόδοσης δικτύων Zigbee

Έχοντας μελετήσει εκτενώς τα σενάρια όπου συνυπάρχουν οι δύο τεχνολογίες, μπορούμε να προτείνουμε κάποιους τρόπους με τους οποίους θα βοηθήσουμε στην βελτίωση των συνθηκών συνύπαρξης και στην μείωση των παρεμβολών που προκαλούνται στα δίκτυα.

5.4.1 Αλλαγή της απόστασης μεταξύ Zigbee και WiFi

Μια πρώτη και εύκολη προσέγγιση είναι να κρατήσουμε απλά την απόσταση μεταξύ του δικτύου Zigbee και WiFi σε τουλάχιστον 8 μέτρα όπως προτείνεται και στην έρευνα [24]. Συγκεκριμένα, στο [24] καταλήγουν μετά από κάποια πειράματα πως η ασφαλής απόσταση για τις 2 τεχνολογίες είναι τα 8 m καθώς επίσης και η απόσταση των καναλιών που χρησιμοποιούν οι συσκευές πρέπει να είναι έχουν 8 MHz offset για να μην υπάρχει παρεμβολή μεταξύ τους. Ο λόγος είναι ότι η φυσική απόσταση μεταξύ των δικτύων θα μειώσει τις παρεμβολές που προκαλούνται στα δύο δίκτυα και ιδιαίτερα στο Zigbee, με αποτέλεσμα να δούμε μια βελτίωση στο Throughput ολόκληρου του δικτύου. Επίσης, με αυτό τον τρόπο δεν χρειάζεται να κάνουμε κάποια άλλη ρύθμιση ή να αλλάξουμε τις προεπιλεγμένες ρυθμίσεις αφού το δίκτυο θα δουλεύει όπως πρέπει χωρίς να επηρεάζεται από το WiFi.

Όπως φαίνεται στο προηγούμενο σενάριο που δημιουργήσαμε, η αύξηση της απόστασης μεταξύ των 2 δικτύων βελτιώνει σχετικά την απόδοση τους αφού έχουμε αύξηση του Throughput και στις 2 τεχνολογίες καθώς και μείωση της καθυστέρησης στο WLAN αλλά αύξηση της στο Zigbee λόγω της τοπολογίας δέντρου που χρησιμοποιεί. Άρα, όσο μεγαλύτερη είναι η απόσταση μεταξύ των δικτύων τόσο μειώνεται η παρεμβολή της μιας τεχνολογίας πάνω στην άλλη. Ωστόσο, η ελάχιστη απόσταση των 8 μέτρων όπως αναφέρει και η έρευνα [24] είναι η κατάλληλη και ασφαλής πρακτική.

5.4.2 Τροποποίηση του αλγόριθμου Frequency agility

Ένας εναλλακτικός τρόπος που προτείνουμε μέσα από αυτή την εργασία είναι μια τροποποιημένη υλοποίηση του αλγόριθμου Frequency agility ο οποίος τρέχει στον Coordinator του δικτύου Zigbee. Όπως είχαμε αναφέρει στο κεφάλαιο που μελετήσαμε τον συγκεκριμένο αλγόριθμο, η επιλογή του καναλιού από τον Coordinator συνήθως γίνεται με βάση την ενέργεια που έχει το κάθε κανάλι και επιλέγεται το κανάλι με την χαμηλότερη ενέργεια. Όμως, η επιλογή ενός τέτοιου καναλιού δεν είναι η βέλτιστη γιατί μπορεί την επόμενη χρονική στιγμή να ενεργοποιηθεί ένα δίκτυο WiFi και έτσι να χρειαστεί να παραμείνει το δίκτυο του Zigbee για 15 λεπτά στο παρόν κανάλι υποφέροντας από το πρόβλημα της παρεμβολής. Για αυτό τον λόγο, η τροποποίηση που προτείνουμε να γίνει είναι η ακόλουθη:

1) Μέτρησε την ενέργεια σε όλα τα διαθέσιμα κανάλια
2) Έλεγξε την ενέργεια των διαθέσιμων καναλιών ξεκινώντας από τα μη επικαλυπτόμενα, όπου στην Ευρώπη είναι τα 15,16,21,22 και στην Αμερική τα 15,20,25,26.
3) Αν κάποιο από αυτά τα κανάλια είναι στα επιτρεπτά όρια της ενέργειας και δεν υπάρχει άλλο δίκτυο Zigbee, επέλεξε αυτό το κανάλι.
4) Αν υπάρχει κάποιο άλλο δίκτυο Zigbee (πχ. PAN 2) σε αυτά τα κανάλια και υπάρχει κανάλι διαθέσιμο που δεν γειτονεύει με το κανάλι του PAN 2 τότε επέλεξε αυτό το κανάλι. Δηλαδή, αν το PAN 2 είναι στο κανάλι 22 και το κανάλι 15 είναι ελεύθερο, τότε επέλεξε για το PAN 1 το κανάλι 15.
5) Σε περίπτωση που είναι κρατημένα τα πιο πάνω κανάλια προχώρησε στην επιλογή ενός διαθέσιμου καναλιού με την χαμηλότερη ενέργεια και τον χαμηλότερο θόρυβο (noise).

Όπως περιγράψαμε, η υλοποίηση μας προτείνει την επιλογή των καναλιών που είναι μη επικαλυπτόμενα με το WiFi έτσι ώστε να αποφύγουμε την παρεμβολή αν είναι δυνατόν. Με αυτό τον τρόπο εξοικονομούμε χρόνο και πόρους που θα χρειάζονταν σε περίπτωση που αλλάζαμε κανάλι αν επιλέγαμε κάποιο άλλο κανάλι που θα υπήρχε παρεμβολή μετά από σύντομο χρονικό διάστημα. Φυσικά, αυτό δεν μπορεί να γίνει πάντα εφικτό αφού τα κανάλια που δεν επικαλύπτονται με το WiFi είναι μόνο 4 και αν έχουμε περισσότερα δίκτυα Zigbee θα αναγκαστούμε να επιλέξουμε τα κανάλια σύμφωνα με την ενέργεια που κατέγραψαν η κόμβοι και κατέγραψαν στην αναφορά που στέλνουν στον Coordinator. Επίσης, να σημειώσουμε πως προσπαθήσαμε να υλοποιήσουμε στον OPNET την παρούσα λύση αλλά επειδή ο πηγαίος κώδικας του Network layer του Zigbee δεν ήταν διαθέσιμος από τον προσομοιωτή, δεν μπορέσαμε να προχωρήσουμε σε οποιαδήποτε αλλαγή για να τρέξουμε δικά μας σενάρια.

Κεφάλαιο 6

Συμπεράσματα

6.1 Γενικά συμπεράσματα

Έχοντας μελετήσει εκτενώς τις προσομοιώσεις των τεχνολογιών του Zigbee και WiFi στο προηγούμενο κεφάλαιο, μπορούμε να καταλήξουμε σε κάποια γενικά συμπεράσματα. Έχοντας υπόψη πρώτα την περίπτωση ενός ομογενούς δικτύου με συσκευές Zigbee μόνο, βλέπουμε πως η συνύπαρξη των δικτύων δεν είναι ομαλή αφού παρατηρείται απώλεια δεδομένων και ακόμη γίνεται αλλαγή καναλιού με τον αλγόριθμο FRQAG. Αξίζει να σημειώσουμε πως ο προσομοιωτής OPNET αναθέτει σε κάθε δίκτυο Zigbee ένα κανάλι αρχίζοντας από το 26 και προχωρώντας προς το 11. Έτσι, τα 2 δίκτυα Zigbee υπόκεινται σε παρεμβολές ακόμη και σε γειτονικές συχνότητες και γι' αυτό το ένα από τα 2 δίκτυα επιλέγει άλλο κανάλι.

Προχωρώντας τώρα στην περίπτωση ενός ετερογενούς δικτύου όπου συνυπάρχουν οι συσκευές Zigbee με το WLAN, μπορούμε να πούμε πως πράγματι υπάρχει πρόβλημα όταν λειτουργούν σε κοντινές αποστάσεις οι δύο τεχνολογίες. Συγκεκριμένα, μέσα από τις γραφικές είδαμε να υπάρχει μείωση στο Throughput του WLAN από 29% μέχρι 65% ενώ το Zigbee έχει από 25% μέχρι 78% μείωση όταν τα κανάλια λειτουργίας των δύο τεχνολογιών έχουν επικάλυψη. Επίσης, έχουμε αύξηση μεταξύ 55% και 83% της καθυστέρησης του WLAN ενώ για το Zigbee δεν υπάρχει τόσο μεγάλη αλλαγή στην καθυστέρηση σε αυτή την περίπτωση. Ακόμη, η απώλεια των δεδομένων είναι μεγαλύτερη από το WiFi γιατί τα δεδομένα που διακινούνται είναι περισσότερα από αυτά στο δίκτυο του Zigbee.

Γενικά, παρατηρούμε ότι το σενάριο που επηρεάζει και τις 2 τεχνολογίες είναι αυτό που τα κανάλια των συσκευών είναι επικαλυπτόμενα και ως αποτέλεσμα έχουμε μείωση του throughput, την αύξηση της καθυστέρησης και την απώλεια δεδομένων και στα δύο δίκτυα. Ως αποτέλεσμα, αν έχουμε ενεργοποιημένο τον αλγόριθμο FRQAG αναμένουμε να βελτιωθεί η γενική εικόνα του δικτύου μας. Στην περίπτωση που υπάρχει μικρός αριθμός δικτύων Zigbee όπως ένα ή δύο αυτό δουλεύει και το είδαμε στο σενάριο με τα 4 APs όπου αλλάζει κανάλι μόλις ενεργοποιούνται τα 2 APs. Όμως, στο τελευταίο σενάριο με το κτίριο της Πληροφορικής όπου είχαμε 5 δίκτυα Zigbee, ο αλγόριθμος επιλέγει σε 2 διαφορετικές περιπτώσεις το ίδιο κανάλι για 2 διαφορετικά δίκτυα με αποτέλεσμα να μειώνεται το Throughput.

Καταλήγοντας, η μείωση της παρεμβολής από το Zigbee πετυχαίνετε ως ένα βαθμό αλλά πιστεύω πως χρειάζεται να βελτιώσουμε περαιτέρω τον τρόπο με τον οποίο γίνεται η αλλαγή καναλιού από τον αλγόριθμο Frequency Agility έτσι ώστε να γίνεται πιο έξυπνα και να μην επηρεάζει τα υπόλοιπα δίκτυα.

6.2 Μελλοντική εργασία

Η συγκεκριμένη ατομική διπλωματική εργασία αποτελεί την αρχική βάση για έρευνα στον τομέα των ασύρματων δικτύων όταν συνυπάρχουν σε ένα έξυπνο σπίτι. Από τα αποτελέσματα της μελέτης αυτής προτείναμε ήδη κάποιες ενδιαφέρουσες λύσεις που μπορεί κάποιος εκτός από το να τις προσομοιώσει, να τις υλοποιήσει σε πραγματικό περιβάλλον για να δούμε την πραγματική απόδοση της κάθε τεχνολογίες.

Ειδικότερα, ο αλγόριθμος του Frequency Agility μπορεί να τροποποιηθεί όπως αναφέραμε κατάλληλα και υλοποιηθεί σε κάποιον προσομοιωτή έτσι ώστε να συγκρίνουμε την απόδοση του τροποποιημένου αλγόριθμου σε σχέση με τον αρχικό αλλά ακόμη και να χρησιμοποιήσουμε κάποια στοιχεία από αυτή την τεχνική για να υλοποιήσουμε ένα νέο, πιο έξυπνο αλγόριθμο που να βελτιώνει ακόμη περισσότερο το πρόβλημα της παρεμβολής.

Το σημαντικότερο όμως στην παρούσα φάση πιστεύω πως είναι η εκτέλεση εργαστηριακών πειραμάτων με συσκευές WiFi και Zigbee για να επιβεβαιώσουμε τα αποτελέσματα που έχουμε εξάγει πειραματικά μέσω προσομοιώσεων και στην συνέχεια να προχωρήσουμε προς την υλοποίηση των λύσεων που μόλις έχουμε αναφέρει. Επιπλέον, μετά την πειραματική μελέτη των δύο τεχνολογιών θα μπορούσε η έρευνα να προχωρήσει στην συνύπαρξη του Zigbee με το Bluetooth καθώς και όλες οι τεχνολογίες μαζί για να έχουμε μια πλήρη επίγνωση της κατάστασης των δικτύων σε αυτές τις περιπτώσεις.

Βιβλιογραφία

[1] E. T. S. I. 2015, *EN 300 328 V1.8.1*, 2012.

[2] *IEEE Standard 802.15.4*, IEEE, 2003.

[3] R. v. d. Meulen, «Gartner» 10 Νοέμβριος 2015. [Ηλεκτρονικό]. Available: http://www.gartner.com/newsroom/id/3165317.

[4] M. E. Purvis, 17 Ιούνιος 2015. [Ηλεκτρονικό]. Available: http://www.prweb.com/releases/2015/06/prweb12791048.htm.

[5] S. M. Kim, J. W. Chong, C. Y. Jung, T. H. Jeon, J. H. Park, Y. J. Kang, S. H. Jeong, M. J. Kim και D. K. Sung, «Experiments on Interference and Coexistence between Zigbee and WLAN Devices Operating in the 2.4 GHz ISM Band» σε *International Conference on Next Generation PC (NGPC) 2005*, 2005.

[6] B. H. Jung, J. W. Chong, C. Y. Jung, S. M. Kim και D. K. Sung, «Interference mediation for coexistence of WLAN and ZigBee networks» σε *IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2008.

[7] M. Bertocco, G. Gamba και A. Sona, «Is CSMA/CA really efficient against interference in a Wireless Control System? An experimental answer» σε *IEEE International Conference on Emerging Technologies and Factory Automation*, 2008.

[8] A. Sikora και V. F. Groza, «Coexistence of IEEE 802.15.4 with other Systems in the 2.4 GHz-ISM-Band» σε *IEEE Instrumentationand Measurement Technology Conference Proceedings* , 2005.

[9] S. Pollin, I. Tan, B. Hodge, C. Chun και A. Bahai, «Harmful Coexistence Between 802.15.4 and 802.11: A Measurement-based Study» σε *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, 2008.

[10] K. Shuaib, M. Boulmalf, F. Sallabi και A. Lakas, «Co-existence of Zigbee and WLAN, A Performance Study,» σε *Wireless Telecommunications Symposium*, 2006.

[11] «Bluetooth Basics,» Bluetooth SIG, [Ηλεκτρονικό]. Available: https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth.

[12] W. Yuan, X. Wang και J.-P. M. G. Linnartz, «A coexistence model of IEEE 802.15.4 and IEEE 802.11b/g» σε *14th IEEE Symposium on Communications and Vehicular Technology in the Benelux*, 2007.

[13] M. A. Sarijari, M. S. Abdullah, A. Lo και R. A. Rashid, «Experimental studies of the ZigBee frequency agility mechanism in home area networks,» σε *IEEE 39th Conference on Local Computer Networks Workshops (LCN Workshops)*, 2014.

[14] C. Hodgdon, «Adaptive Frequency Hopping for Reduced Interference between Bluetooth and Wireless LAN» Ericsson Technology Licensing, Μάϊος 2003. [Ηλεκτρονικό]. Available: http://www.design-reuse.com/articles/5715/adaptive-frequency-hopping-for-reduced-interference-between-bluetooth-and-wireless-lan.html.

[15] Zigbee Alliance, «Zigbee Specification: Document 053474r17,» ZigBee Standards Organization, 2008.

[16] D. Yang, Y. Xu και M. Gidlund, «Wireless Coexistence between IEEE 802.11- and IEEE 802.15.4-Based Networks: A Survey» *International Journal of Distributed Sensor Networks*, τόμ. 2011, p. 17, 2011.

[17] I. P802.15, «Coexistence analysis of IEEE Std 802.15.4 with other IEEE standards and proposed standards» 802.15 Working Group, 2010.

[18] S. White, «Wi-Fi and Bluetooth coexistence» 2 Μάρτιος 2012. [Ηλεκτρονικό]. Available: http://www.ecnmag.com/article/2012/03/wi-fi-and-bluetooth-coexistence.

[19] M. Małowidzki, «Network Simulators: A developer's perspective» 2011.

[20] I. Cisco Systems, «Cisco Wireless Controller Configuration Guide, Release 8.2,» 2016. [Ηλεκτρονικό]. Available: http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/config-guide/b_cg82/b_cg82_chapter_010001001.html#ID40.

[21] A. Networks, «Adaptive Radio Management and Client match» 2014.

[22] I. Aerohive Networks, «Cooperative Control Wireless LAN Architecture (Version 3.5)» 2011.

[23] R. Nayanajith, «Configuring DCA,» https://mrncciew.com/2013/03/16/configuring-dca/, 2013.

[24] P. Yi, A. Iwayemi και C. Zhou, «Developing ZigBee Deployment Guideline Under WiFi Interference for Smart Grid Applications» σε *IEEE Transactions on Smart Grid,* 2011.

[25] «IEEE Standard 802.11k» IEEE, 2008.

Παράρτημα Α

Σε αυτό το παράρτημα βρίσκεται ο κώδικας για την τροποποίηση του αλγόριθμου auto-assign του WLAN έτσι ώστε να λαμβάνει υπόψη του τα κανάλια που αναθέτουμε εμείς χειροκίνητα στα APs και να μην αναθέτει αυτά τα κανάλια στα υπόλοιπα APs που έχουν την επιλογή auto-assign. Η τροποποίηση γίνεται στο αρχείο wlan_mac_hcf.pr.c. Επίσης, τροποποίησα το αρχείο wlan_support.ex.c για να εισάγω την γραφική παράσταση του Operating Channel στο Wireless LAN για να γνωρίζουμε ποιο κανάλι επιλέγεται από κάθε BSS καθώς και το wlan_support.h για να στηρίζει τα κανάλια της Ευρώπης. Πιο κάτω φαίνονται τα αρχεία που τροποποιήθηκαν:

Αρχείο \models\std\wireless_lan\wlan_mac_hcf.pr.c:

Γραμμή 1300:

```
/* State variable definitions */
typedef struct
    {
    /* Internal state tracking for FSM */
    FSM_SYS_STATE
    /* State Variables */
    OmsT_Dim_Stat_Handle chan_num_handle;
    ...
    } wlan_mac_hcf_state;
```

Γραμμή 1600:

```
#define chan_num_handle                op_sv_ptr->chan_num_handle

/**Global table*/
extern int assigned_ch[14],counter;
```

Γραμμή 1629:

```
static void
wlan_hcf_sv_init (void)
    {
    char stat2[16];
    ...

    /*Registering global statistics*/
    sprintf (stat2, "BSS %d", bss_id);
    chan_num_handle = Oms_Dim_Stat_Reg (my_objid, "Wireless LAN",
"Operating Channel", stat2, OPC_STAT_GLOBAL);
    Oms_Dim_Stat_Annotate (chan_num_handle, stat2);
    ...
    }
```

Γραμμή 2735:

```
static void
wlan_hcf_transceiver_channel_init (int counter)
    {
    WlanT_Bss_Channel_Info*     bss_channel_info_ptr;
    int                         found_channel_num;
    double                      bandwidth_mhz;
    double                      frequency
```

```
    Boolean                         channel_num_supports_40m = OPC_FALSE;
    char                            err_msg1 [512];
```

```
      int j=0;
    /** This function determines the WLAN channel that the surrounding  **/
    /** node will use and configures the transceiver with the           **/
    /** corresponding minimum frequency and bandwidth values.           **/
    FIN (wlan_hcf_transceiver_channel_init ());

    /*Initialize channels*/
    if (counter==0){
        int i=0;
        for (i=0;i<14;i++){
            assigned_ch[i]=0;
        }
    }

    /* Initially set the bandwidth and frequency to the state variable  */
    /* values.                                                          */
    bandwidth_mhz = config_bw_mhz;
    frequency     = config_freq;

    /* Check whether the bandwidth is specified using a special value.  */
    if (bandwidth_mhz == WLANC_PHY_BASED_BW_USED)
        {
        /* Set the bandwidth to the standard value of used physical     */
        /* layer technology.                                            */
        bandwidth_mhz = (is_phy_char_5g(phy_char_flag)) ?
WLANC_11a_CHNL_BANDWIDTH : WLANC_11b_CHNL_BANDWIDTH;

        /* Store the actual value, which we will need if we switch to   */
        /* and then from 11p to our regular PHY technology.             */
        config_bw_mhz = bandwidth_mhz;
        }

    /* Determine the channel number we are going to use.                */
    if (frequency == WLANC_BSS_BASED_FREQ_USED)
        {
        /* Get the BSS channel information.                             */
        bss_channel_info_ptr = wlan_bss_operation_channel_info_get (bss_id,
phy_type);

        channel_num = bss_channel_info_ptr->channel_number;

        /* Get the minimum frequency that corresponds to the selected   */
        /* channel.                                                     */
        frequency = wlan_min_freq_for_chan (channel_num, phy_type);

        /* When the frequency is auto assigned then, they should        */
        /* support 40 MHz capability.                                   */
        channel_num_supports_40m = OPC_TRUE;

        /*Mark the assigned channel that is selected by auto-assign
algorithm*/
        assigned_ch[channel_num-1]=1;

            for (j=0;j<14;j++){
                printf(" %d\t",assigned_ch[j]);
            }
        }
    else
        {
        /* The frequency band that will be used by this node is         */
        /* explicitly specified. Validate it and determine its channel  */
        /* number.                                                      */
```

```
        /* In 802.11/11b/11g networks, for a standard, acceptable       */
        /* channel, the bandwidth has to be 22 MHz, and the minimum     */
        /* frequency between 2401 and 2451 MHz, inclusive, with         */
        /* intervals of 5 MHz (i.e. the roaming feature is currently    */
        /* supported only within first 11 channels. These numbers refer */
        /* to the values of the constants used below as specified in    */
        /* the standard).                                               */
        if ((is_phy_char_5g(phy_char_flag) == OPC_FALSE) && phy_char_flag
!= WlanC_OFDM_11p &&
            bandwidth_mhz == channel_bandwidth && frequency >=
first_chan_min_freq && frequency == ceil (frequency) &&
            (frequency - first_chan_min_freq) / channel_spacing <
channel_count && (int) (frequency - first_chan_min_freq) % (int)
channel_spacing == 0)
            {
            /* The radio band has a valid configuration. Compute its    */
            /* channel number.                                          */
            channel_num = (int) ((frequency - first_chan_min_freq) /
channel_spacing + 1);
            channel_num_supports_40m = OPC_TRUE;

            assigned_ch[channel_num-1]=1;

            for (j=0;j<14;j++){
                printf(" Ch: %d\t",assigned_ch[j]);
                }
            printf("\n");
            }
            ....
        }
    }
```

Γραμμή 7796:

```
static WlanT_Data_Header_Fields*
wlan_hcf_data_header_prepare (WlanT_HCF_Hld_Info* hld_ptr)
    {
    ...
    /* If this is a data frame forwarded by QAP to one of the STAs in   */
    /* its BSS, then fromds bit is set, and address3 field of the       */
    /* header is set to the address of the MAC that is the original     */
    /* source of the packet.                                            */
    if (ap_flag == OPC_BOOLINT_ENABLED)
        {
        Oms_Dim_Stat_Write (chan_num_handle, (int)channel_num);
        pk_dhstruct_ptr->fromds = 1;

        /* If this is an A-MSDU the originating address can be          */
        /* different for each MSDU within A-MSDU.                       */
        pk_dhstruct_ptr->address3 = (IS_AMSDU(hld_ptr) == OPC_TRUE)?
my_address : hld_ptr->orig_addr;
        }
    else
        pk_dhstruct_ptr->fromds = 0;
    ...
    }
```

Γραμμή 10892:

```
static WlanT_HCF_Access_Category
wlan_hcf_interrupts_process (void)    {
    ...
    if (ap_flag == OPC_TRUE || bss_id == WLANC_BSSID_WILDCARD)
```

```
            {
            Oms_Dim_Stat_Write (chan_num_handle, (int)channel_num);

            /* This is an interrupt scheduled by a roaming STA to report
its     */
            /* association or disassociation. Find out the address of the
STA.   */
            sta_mac_addr = roaming_sta_info_ptr->mac_address;

            /* Get the roaming STA info bitmap.
*/
            sta_info_bitmap = roaming_sta_info_ptr-
>roaming_sta_info_bitmap;
    ...}
    }
```

Γραμμή 15976:

```
static Ici*
wlan_hcf_llc_ici_get ()
    {
    /** This function gets the ICI used which will be used to send the  **/
    /** next higher layer packet.                                        **/
    FIN(wlan_hcf_llc_ici_get ());

    /* Multiple ICIs are required only for access points. Non-access    */
    /* points nodes do not require this ICI. If this function is        */
    /* called by a non access point node, we shall simply return        */
    /* an OPC_NIL.                                                      */
    if (ap_flag == OPC_BOOLINT_ENABLED)
        {
        Oms_Dim_Stat_Write (chan_num_handle, (int)channel_num);
        ...
        }
    }
```

Γραμμή 17987:

```
static void
wlan_hcf_sta_addr_register (int bssid, OpT_Int64 sta_addr, int sta_is_ap,
Objid sta_mac_objid, WlanT_Phy_Char_Code phy_char)
    {
    ...
    /** Add the station information to the BSS-based station map.
**/
    FIN (wlan_hcf_sta_addr_register (bssid, sta_addr, sta_is_ap,
sta_mac_objid, phy_char));

    /* Get the BSS mapping handle (owned by called function as a static
*/
    /* variable).
*/
    wlan_bss_mapping_hndl = wlan_bss_mapping_get ();

    /* Check if this is the first station being mapping into this BSS.
*/
    bss_info_ptr = (WlanT_Bss_Mapping_Info *) prg_mapping_value_get
(wlan_bss_mapping_hndl, &bssid);
    if (bss_info_ptr == PRGC_NIL)
        ...
    else
        {
            sprintf (stat_info, "BSS %d", bssid);
            Oms_Dim_Stat_Annotate (global_network_load_handle, stat_info);
```

```
            Oms_Dim_Stat_Annotate (chan_num_handle, stat_info);
        }
    }
```

Αρχείο External Source wlan_support.ex.c:

Γραμμή 17:

```
/*Global variable*/
extern int assigned_ch[14];

...
#define WLANC_2G4_20M_NO_OVERLAP_STEP       6
```

Γραμμή 901:

```
WlanT_Bss_Channel_Info*
wlan_bss_operation_channel_info_get (int bssid, WlanT_Phy_Type
bss_phy_type)
    {
    ...
    /* Check to see if the channel auto assignment algorithim has been  */
    /* executed for 5GHz or not.                                        */
    if (is_phy_type_5g(bss_phy_type) && bss_channels_assigned_5G ==
OPC_FALSE)
        {
        /* Perform channel auto assignment for 5GHz.                    */
        bss_chn_info_ptr = wlan_bss_perform_5g_channel_assignment (bssid,
bss_chn_profiles_info_ptr);

        /* Set the flag to acknowledge that the channels are auto       */
        /* assigned for 5GHz.                                           */
        bss_channels_assigned_5G = OPC_TRUE;
        }
    /* Check to see if the channel auto assignment algorithim has been  */
    /* executed for 2.4GHz or not.                                      */
    else if (is_phy_type_2g4(bss_phy_type) && bss_channels_assigned_2G4 ==
OPC_FALSE)
        {

        /* Perform channel auto assignment for 2.4GHz.                  */
        bss_chn_info_ptr = wlan_bss_perform_2g4_channel_assignment (bssid,
bss_chn_profiles_info_ptr);

        printf("\n First assign the BSSID %d channel num is %d",bssid,
bss_chn_info_ptr->channel_number);

        /* Set the flag to acknowledge that the channels are auto       */
        /* assigned for 5GHz.                                           */
        bss_channels_assigned_2G4 = OPC_TRUE;
        }
    else
        {
        /* The channel auto assignment has been performend.             */
        bss_chn_info_ptr = wlan_bss_channel_profile_from_list_get (bssid,
bss_chn_info_lptr, OPC_NIL);
```

```
/* Mark the assigned channel*/
        assigned_ch[bss_chn_info_ptr->channel_number-1]=1;
        }
```

```
    ...
    }
```

Γραμμή 1116:

```
WlanT_Bss_Channel_Info*
wlan_bss_perform_2g4_channel_assignment (int bssid,
WlanT_BSS_Channel_Profiles_Info* bss_chn_profiles_info_ptr)
    {
    WlanT_Bss_Channel_Info* bss_chn_info_ptr;
    WlanT_Bss_Channel_Info* matching_chn_info_ptr = OPC_NIL;
    List*                   bss_chn_info_lptr;
    int                     num_stas_2040_chn = 0;
    int                     num_stas_20_only_chn = 0;
    int                     chn_2040, chn_20;
    int                     i, list_size,j;
    int                     num_2040_bss;

    /** This function performs the channel assignment for all BSS       **/
    /** operating at 2.4GHz and returns the bss channel information     **/
    /** corresponding to the BSS ID passed in the function.             **/
    FIN (wlan_bss_perform_2g4_channel_assignment ());

    /* Store the list of BSS and number of 20/40 BSS for in local       */
    /* variables for the ease of handling.                              */
    bss_chn_info_lptr            = bss_chn_profiles_info_ptr-
>bss_chn_info_lptr;
    list_size                    = op_prg_list_size (bss_chn_info_lptr);

    /* Get the number of 2.4GHz BSSs from the size of the list.         */
    num_2040_bss                 = bss_chn_profiles_info_ptr->num_2040_bss;

    printf("Number of bss %d",list_size);
    /* Case i: When there are no 20/40 Mhz BSS.                         */
    if (num_2040_bss == 0)
        {
        /* Trace.                                                       */
        if (op_prg_odb_ltrace_active ("wlan_freq_assign"))
            op_prg_odb_print_major ("2G4 Channel assign: No 2040 BSS",
OPC_NIL);

        /* Assign channels from 1 through 11 (North America) with a gap */
        /* of 5 channels in between. The sequence will look like 1, 6,  */
        /* 11, 5, 10, 4, 9,... The channel will be picked as a function */
        /* BSS ID, that is mapped to a BSS index. Note that only        */
        /* channels that are 5 channels apart are non-overlapping.      */
        /* Assume that BSS indices run serially: 0, 1, 2, ...           */
        /* WLANC_2G4_OPER_CHNL_COUNT = 11, and                          */
        /* WLANC_2G4_20M_NO_OVERLAP_STEP = ceil (22.0/5.0) = 5          */
        //WLANC_2G4_20M_NO_OVERLAP_STEP changed to 6
        for (i=0;i<list_size;i++)
            {
                    /* Access the BSS channel info.
*/
            bss_chn_info_ptr = (WlanT_Bss_Channel_Info *)
op_prg_list_access (bss_chn_info_lptr, i)
      j=i-1;
            do{
            j++;
            /* Assign a channel number as per the method described in   */
            /* the comments.                                            */
            bss_chn_info_ptr->channel_number = (j *
WLANC_2G4_20M_NO_OVERLAP_STEP ) % WLANC_2G4_OPER_CHNL_COUNT + 1;
```

```
            }while(assigned_ch[bss_chn_info_ptr->channel_number-1]==1);
//Find a channel that is not assigned

            assigned_ch[bss_chn_info_ptr->channel_number-1]=1;


/* If a BSS Channel info is found with matching BSS id cache it */
            /* to return to the caller*/
            if (bssid == bss_chn_info_ptr->bss_id)
      matching_chn_info_ptr = bss_chn_info_ptr;
            ...
            }
        }
        ...
    }
```

Αρχείο wlan_support.h:

Γραμμή 90:

```
#define WLANC_2G4_OPER_CHNL_COUNT           13
#define WLANC_2G4_20M_NO_OVERLAP_STEP       6
```