Ατομική Διπλωματική Εργασία

Indoors Localization

Χριστόφορος Πανταζής

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Indoors Localization

Χριστόφορος Πανταζής

Επιβλέπων Καθηγητής

Βάσσος Βασιλείου

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

Μάιος 2020

Ευχαριστίες

Θα ήθελα να εκφράσω την ευγνωμοσύνη μου στο Πανεπιστήμιο Κύπρου και συγκεκριμένα στο τμήμα της πληροφορικής που με καθοδήγησε και με προετοίμασε αυτά τα 4 χρόνια των σπουδών μου. Ακόμα θα ήθελα να πω ένα πολύ μεγάλο ευχαριστώ στον κύριο Βάσο Βασιλείου που ήταν πάντα κοντά μας και σαν διδάσκων διάφορων μαθημάτων αλλά και σαν μέντορας και καθοδηγητής της διπλωματική μου εργασίας.

Περίληψη

Το θέμα μου είναι η μελέτη της διαδικτυακής κίνησης πακέτων (network packet traffic) σε ασύρματο δίκτυο με αρχικό σκοπό την υλοποίηση ενός συστήματος συλλογής πακέτων διαφόρων κινητών συσκευών εκ των οποίων θα διαχωρίζονται (ξεχωρίζονται) με το MAC Address τους και κατ' επέκταση την ανίχνευση κίνησης τους στον χώρο. Από το κάθε πακέτο θα συλλέγονται 4 βασικές πληροφορίες: MAC Address, το RSSI (Received Signal Strength indicator) όπου θα είναι ουσιαστικά η δύναμη του σήματος που καταφθάνει στο AP (Access Point) τον οποίο χρησιμοποιούμε για την συλλογή πακέτων και το timestamp όπου θα χρησιμοποιηθεί για την ταυτοποίηση ίδιον πακέτων μεταξύ διαφορετικών Access Points και τέλος το κανάλι στο οποίο μεταφέρθηκε το πακέτο. Με αυτές τις πληροφορίες και με την γνώση που έχουμε για τις φυσικές ιδιότητες των ηλεκτρομαγνητικών κυμάτων μπορούμε να υπολογίσουμε την σχετική απόσταση της συσκευής που έστειλε το πακέτο και του Access Point που το έχει παραλάβει. Πρακτικά για να ξέρουμε που ακριβώς είναι η θέση μιας συσκευή και κατ' επέκταση την κατεύθυνση της κίνησης της πρέπει να υλοποιηθεί ένα σύστημα με τουλάχιστον 3 Access Points. Μετά την συλλογή πακέτων από τους X Access Points, ένα κεντρικοποιημένο σύστημα θα κάνει την επεξεργασία για την εξαγωγή των τοπολογικών πληροφοριών των συσκευών που έχουν συλλεχθεί. Αυτές θα είναι σε γραπτή μορφή τύπου σημείων για να υπάρχει η δυνατότητα επεξεργασίας και ανάλυσης από οποιοδήποτε άλλο εξωτερικό σύστημα αλλά και η εικονική αναπαράσταση της κίνησης των συσκευών για καλύτερη κατανόηση και εξαγωγή συμπερασμάτων.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

1.1 Στόχος

Είναι γεγονός ότι τα τελευταία χρόνια, η ευρεία χρήση των φορητών συσκευών έχει αυξηθεί κατά πολύ καθώς πλέων οι συσκευές όχι μόνο μπορούν να κάνουν αλλά και έχουν τις ίδιες βασικές υπολογιστικές δυνατότητες με αυτές τον συνηθισμένων ηλεκτρονικών υπολογιστών. Λόγο αυτών τον συνθηκών έγιναν πολλές ερευνητικές προσπάθειες για την παρακολούθηση της κινητικότητας των ασύρματων συσκευών. Ένας από τους πιο κοινούς στόχους της ιχνηλάτησης της κίνησης των κινητών συσκευών είναι η εξαγωγή πληροφορίας σχετικά με την πυκνότητα των ανθρώπων και τις κινούμενες τροχιές που βρίσκονται σε ένα συγκεκριμένο περιβάλλον.

Πρακτικά θα μπορούσαμε να απαντήσουμε διάφορες ερωτήσεις που εγείρουν από διάφορα προβλήματα συγκεκριμένων τομέων. Για παράδειγμα, πόσοι πελάτες επισκέπτονται ένα εμπορικό κέντρο καθημερινά και ποια καταστήματα λαμβάνουν περισσότερους πελάτες συγκριτικά με τους άλλους στο εμπορικό κέντρο; Ποια είναι η διαδρομή που διασχίζουν οι περισσότεροι άνθρωποι κάθε μέρα; Αυτή η πληροφορία μπορεί να χρησιμοποιηθεί με σκοπό την προβολή κάποιων διαφημίσεων στο μέγιστο βαθμό απόδοσης που μπορεί να επιφέρει. Σε αυτή την περίπτωση το επιθυμητό είναι να την δουν όσοι περισσότερη άνθρωποι είναι δυνατόν. [9]

Πόσα άτομα περιμένουν σε σταθμό του μετρό και πώς κινούνται οι ροές ανθρώπων μέσα σε σταθμούς ανταλλαγής; Πόσος χρόνος χρειάζεται στους ανθρώπους να διανύσουν από μια είσοδο σε μια έξοδο; Αυτό μπορεί να φανεί χρήσιμο στην κυβέρνηση για να γίνει κάποια διαρρύθμιση

του προγράμματος με σκοπό την αποδοτικότερη χρήση του μετρό από τα άτομα (λιγότερος χρόνος αναμονής κ.τ.λ.).

Γενικά αυτές οι πληροφορίες παρακολούθησης μπορούν να βοηθήσουν τον πάροχο υπηρεσιών να κατανοήσει τα διάφορα μοτίβα και πρότυπα χρήσης δημόσιου χώρου, ώστε να βελτιώσει την κατανομή των πόρων τους.

Επιπλέον, η ανίχνευση κίνησης μεγάλων ανθρώπινων μαζών μπορεί να επιτρέψει νέα εργαλεία για έρευνες έκτακτης ανάγκης που ασχολούνται με το μέγεθος των μαζών και τον τρόπο με τον οποίο σχηματίζονται, διαλύονται ή επιβραδύνονται από περιορισμούς, π.χ. διόδους πόρτας κ.α. [9]

Το σύστημα εντοπισμού με βάση το GPS χρησιμοποιείται ευρέως για τον προσδιορισμό θέσης εξωτερικού χώρου και αυτή η τεχνολογία εφαρμόζεται επί του παρόντος σε πολλές κινητές συσκευές. Δυστυχώς, η κύρια πρόκληση σε εσωτερικούς χώρους είναι η μη διαθεσιμότητα των σημάτων GPS, καθώς αυτή η τεχνολογία απαιτεί Line-of-Sight από την συσκευή στον δορυφόρο. Επιπλέον, ένα τέτοιο σύστημα απαιτεί από τον χρήστη να εγκαταστήσει μια εφαρμογή στην κινητή συσκευή προκειμένου να ενεργοποιήσει τον εντοπισμό GPS, η οποία δεν παρακολουθεί τους ανθρώπους με παθητικό τρόπο.

1.2 **Μεθοδολογία**

Αρχικά αφού κατανόησα το πρόβλημα, τα χώρισα σε βασικά θεωρητικά στάδια και βήματα που θα ακολουθούσα. Ακολούθως έχω μελετήσει κάποια άρθρα που σχετίζονται με το θέμα μου για να πάρω κάποιες πρακτικές ιδέες και μεθόδους για να μπορέσω να αρχίσω την υλοποίηση.

Ακολούθως αφού έγινε η παραπάνω μελέτη, κατέληξα στο συμπέρασμα ότι ο κύριος πρωταγωνιστής θα είναι το RSSI (Received Signal Strength Indicator) όπου η πληροφορία βρίσκεται στο Data Layer ενός ασύρματου πακέτου.

Για αυτό τον λόγο η πρώτη φάση του έργου είναι η συλλογή δεδομένων από φυσικά σημεία μέσα στον χώρο (Σημεία Πρόσβασης AP) και η αποθήκευση τους σε μορφή pcap αρχείων για να γίνει μετέπειτα η εξαγωγή των επιθυμητών πληροφοριών.

Η πρώτη δοκιμή έγινε με το Wi-Fi adapter του προσωπικού μου φορητού υπολογιστή. (βλέπε Κεφάλαιο 3.1) Λόγω μεγάλου ποσοστού σφάλματος η δεύτερη δοκιμή έγινε με την βοήθεια ενός Tp-Link δρομολογητή το οποίο περιείχε OpenWRT firmware.

Μετέπειτα στην $2^{η}$ φάση του έργου έχω συγκέντρωση όλα τα pcap αρχεία που έχουν μαζευτεί από τους διάφορους δρομολογητές σε ένα κεντρικοποιημένο υπολογιστικό σύστημα. Αφού έχουν μαζευτεί όλα τα pcap αρχεία, τότε αρχίζουμε να τα φιλτράρουμε όλα τα διαφορετικές MAC διευθύνσεις και τις αποθηκεύουμε σε ένα αρχείο. Μόλις γίνει αυτό σημαίνει ότι είναι το σήμα κατατεθέν για να αρχίσει η φάση 3.

Η $3^{η}$ φάση είναι το φιλτράρισμα των pcap αρχείων με βάση μια MAC διεύθυνση την φορά. Αυτή την διαδικασία αρχικά υλοποιήθηκε και δοκιμάστηκε με την χρήση βιβλιοθηκών της γλώσσας προγραμματισμού python. Αυτό είχε ως αποτέλεσμα για να αργή η επεξεργασία του αρχείου της τάξεως χρόνου πέντε λεπτών. Λόγο της μεγάλης καθυστέρησης έπρεπε να βρεθεί μια άλλη λύση. Σαν δεύτερη δοκιμή χρησιμοποιήθηκε το πρόγραμμα T-shark που είναι η εκδοχή της wire shark αλλά για την γραμμή εντολών. Λόγο του ότι το T-shark είναι γραμμένο σε C μπόρεσα να κάνω την ίδια δουλεία μέσα σε δευτερόλεπτα. Αφού επιλεγεί μια διεύθυνση και φιλτραριστεί βάση αυτής τότε ξεκινά η επεξεργασία των βασικών στοιχείων που έχει η κάθε εγγραφή του pcap αρχείου. Το πρόγραμμα θα διακρίνει το Signal Strength, το MAC timestamp και Signal Frequency που αργότερα θα μας χρειαστούν για να βρούμε την πληροφορία της απόστασης. Αυτές οι πληροφορίες θα αποθηκευτούν σε ένα άλλο αρχείο για να χρησιμοποιηθούν στην επόμενη φάση.

Στην 4η φάση θα μεταφραστεί με άλλο Python πρόγραμμα η πληροφορία Signal Strength (dB Decibel) που έχει δημιουργηθεί από την 3η φάση σε πραγματική απόσταση (m μέτρα) της φορητής συσκευής (την συγκεκριμένη χρονική στιγμή που δημιουργήθηκε το συγκεκριμένο πακέτο) και του Access Point που έχει συλλάβει το συγκεκριμένο πακέτο. Αυτό γίνεται με την βοήθεια μια φόρμουλας μετατροπής (βλέπε Κεφάλαιο 5).

Στην 5η φάση, αφού έχουμε στην κατοχή μας της φυσικές απόστασης σε μέτρα κάθε πακέτου τότε με ένα άλλο πρόγραμμα Python θα μετατρέπουμε την πληροφορία της απόστασης σε ακριβές σημείο συντεταγμένων ενός νοητού πλέγματος. (όπου στη πραγματικότητα το πλέγμα θα αντιπροσωπά το χώρο που είναι τοποθετημένα τα Access Points) Αυτό θα αποθηκεύετε σε ένα αρχείο για να μπορέσει να γίνει οποιαδήποτε επεξεργασία από οποιαδήποτε εξωτερικά προγράμματα για επίλυση προβλημάτων που προαναφέραμε στην Εισαγωγή. (βλέπε Κεφάλαιο 1.1) Ακόμα θα δημιουργούνται και εικονικά γραφήματα που αντιπροσωπεύουν τις συντεταγμένες των συσκευών στον χώρο και κατ’ επέκταση την κατεύθυνση της κίνησης τους στον χώρο για λόγους καλύτερης κατανόησης και ευκολότερης αποσφαλμάτωσης.

1.3 Δομή

Στο κεφάλαιο 1 είναι η Εισαγωγή όπου εκεί αναπτύσσω τον στόχο μου, τις μεθόδους που χρησιμοποίησα καθόλη την διάρκεια μελέτης και υλοποίησης της εργασίας καθώς και την δομή της διπλωματικής. Ακολούθως έχω συνάψει και το Γλωσσάρι, δηλαδή τις πιο συχνές ορολογίες που θα συναντήσετε για την εξήγηση του έργου.

Στο κεφάλαιο 2 θα δούμε παρόμοια συστήματα εύρεσης της θέσης φορητών συσκευών, αναλύοντας τις διαφορές τους με την δική μου προσέγγιση και θα εξηγήσουμε με λεπτομέρεια την υλοποίηση μου. Τέλος θα αναλύσουμε και θα εξηγήσουμε πολύ καλά το Data Layer όπου εκεί βρίσκονται όλες οι πληροφορίες που χρειάζονται για να μπορέσει να έχει υπόσταση τον έργο.

Στα κεφάλαια 3 - 6 θα αναλύσουμε τις φάσεις του έργου και τι εργαλεία χρησιμοποιήθηκαν για την επίτευξή του αναμενόμενου αποτελέσματος αντίστοιχα.

Στο κεφάλαιο 3 είναι η φάση της συλλογής των δεδομένων από τους διάφορους Access Points και Wi-Fi adapters. Εκτός από την hardware ανάλυση θα μελετήσουμε και το firmware που χρησιμοποιεί ο δρομολογητής καθώς και τα διάφορα προγραμματιστικά εργαλεία που χρειάζονται για να μπορέσει να συλλάβει τα απαραίτητα πακέτα που θέλουμε.

Στο κεφάλαιο 4 είναι η φάση της συλλογής των πακέτων από όλα τα Access Points και Wi-Fi adapters σε ένα κεντρικοποιημένο υπολογιστικό σύστημα για τη μετέπειτα τους επεξεργασία. Μόλις μαζευτούν όλα τα pcap αρχεία θα δείξουμε με ποιο τρόπο συλλέγουμε τις μοναδικές MAC διεύθυνσης.

Στο κεφάλαιο 5 είναι η φάση της εξαγωγής των βασικών πληροφοριών από τα pcap αρχεία για τον υπολογισμό της πραγματικής απόστασης μεταξύ φορητής συσκευής και Access Point. Αυτό γίνεται με την βοήθεια της φόρμουλας μετατροπής dB (Decibel) σε m (μέτρα) όπου και θα επεξηγηθεί σε βάθος.

Στο κεφάλαιο 6 είναι η φάση της συναρμολόγησης της πληροφορίας της απόστασης ίδιον εγγραφών πολλαπλών pcap αρχείων με σκοπό τον υπολογισμό της ακριβής θέσης τους στον χώρο. Επιπρόσθετα θα αναλυθεί και η εικονική αναπαράσταση των σημείων των φορητών συσκευών που μελετούνται στο χώρο για μελέτη της κινήσεις τους και για ευκολότερη αποσφαλμάτοση και μέτρηση σφάλματος.

Τελειώνοντας την υλοποίηση στο κεφάλαιο 6, σειρά έχουν τα συμπεράσματα που θα αναλυθούν στο κεφάλαιο 7. Εκεί θα παρουσιαστούν διάφορα σενάρια σύλληψης πακέτων από μια φορητή συσκευή με μεταβλητό παράγοντα την κινητική τους κατάσταση για να δούμε πως το πρόγραμμα αντιδρά στις ανάλογες περιστάσεις.

1.4 Γλωσσάρι

Πιο κάτω αναφέρονται έννοιες που εμφανίζονται συχνά στο κείμενο, και οι αντίστοιχες αγγλικές ορολογίες τους.

- Router: η συσκευή που είναι υπεύθυνη για την δρομολόγηση των πακέτων στο Δίκτυο.
- Script: Αρχείο που περιέχει σειρά από εντολές προς εκτέλεση π.χ. Bash Script, Python Script.
- Access Point: είναι μια συσκευή ασύρματου δικτύου που λειτουργεί ως πύλη για τη σύνδεση συσκευών σε τοπικό δίκτυο.
- Firmware - Λειτουργικό λογισμικό μιας συσκευής
- OpenWRT - Λειτουργικό λογισμικό με βάση του το Linux λειτουργικό σύστημα για ενσωματωμένες συσκευές.
- Centralized system - Κεντρικοποιημένο σύστημα
- Pcap files – είδος αρχείου που συγκρατεί πληροφορίες για πακέτα διαδικτύου
- Points-Of-Interest (POI)
- Portable Sensing Unit (PSU)
- Frame
- MAC Address
- Received Signal Strength Indicator (RSSI)

Κεφάλαιο 2

Υπόβαθρο

2.1 Παρόμοια Συστήματα Εύρεσης Τοπικοτητας

Ένα παρόμοιο σύστημα (το αποτέλεσμα είναι το ίδιο με το στόχο του έργου) που μελέτησα στην αρχή για να πάρω τα βασικά συστατικά και την γενική ιδέα για το πως δουλεύουν τα πράγματα είναι το Anyplace: A Crowdsourced Indoor Information Service.

Το Anyplace χρησιμοποιεί δύο βασικά εργαλεία για να πετύχει τον σκοπό του. Την φορητή συσκευή και τα Wi-Fi Access Point του περιβάλλοντος που τρέχει το πρόγραμμα Anyplace. Τα κινητά τηλέφωνα μπορούν να μετρήσουν την ισχύ του σήματος που λαμβάνεται από τα γύρω AP και να λάβουν πληροφορίες σχετικά με τη θέση τους με βάση τις βάσεις δεδομένων γεωγραφικής θέσης, οι οποίες διατηρούν πληροφορίες σχετικά με αυτά τα AP (δηλαδή, την ένταση του σήματος αυτών των πομπών σε γνωστές θέσεις στο χώρο). [5]

Για να δημιουργηθεί η βάση δεδομένων χρειάστηκε λεπτομερής χαρτογράφηση εσωτερικών χώρων με λεπτομερή εγγραφή Points-Of-Interest (POI) που μπορεί να επιτευχθεί μέσω crowdsourcing, εσωτερικών κινητών μοντέλων όσο και με την μελέτη εσωτερικών σημάτων για καλύτερη ακρίβεια.[5]

Όπως καταλαβαίνετε το σύστημα για να λειτουργήσει εκτός από τον back-end κομμάτι του (Access point) επιβάλλεται και η χρήση ειδικού προγράμματος στην ίδια την φορητή συσκευή για να στέλνει τα απαραίτητα σήματα προς τους Access Points για να μπορέσουν και αυτή με την σειρά τους να υπολογίσουν την γεωγραφική θέση του κινητού.

Το δικό μας έργο θέλει να βρει την γεωγραφική θέση φορητών συσκευών στην εμβέλεια του δικτύου που χρησιμοποιείται αλλά χωρίς την χρήση κάποιου προγράμματος από την μεριά της συσκευής που θέλουμε να ανιχνεύσουμε. Γι' αυτό τον λόγο έπρεπε να χρησιμοποιήσουμε την πληροφορία της δύναμης του σήματος των πακέτων χωρίς να έχουμε εξωτερική βοήθεια (όπου στην περίπτωση του Anyplace παρέχετε από την ίδια την φορητή συσκευή)

Έχοντας κράτηση σημαντικές πληροφορίες από το Anyplace συνέχισα την μελέτη μου σε ένα άλλο άρθρο που έχει προσέγγιση μια λύση που είναι πιο κοντά στο δικό μας ζητούμενο.

Στο SmartITS: Smartphone-based identification and tracking using seamless indoor-outdoor localization μπορούμε να διακρίνουμε ξεκάθαρα τις εξής φάσεις: ταυτοποίηση, παρακολούθηση και η ιχνηλάτηση πολλαπλών ατόμων που βρίσκονται σε ένα κοινό χώρο χρησιμοποιώντας probe request που εκπέμπονται από τις ασύρματες συσκευές του χρήστη και μια υβριδική τεχνική εντοπισμού. Αυτή η τεχνική εντοπισμού βασίζετε στο GPS Wi-Fi-Cellular το οποίο ιχνηλατεί φορητές συσκευές τόσο σε εξωτερικούς όσο και σε εσωτερικούς χώρους. [8]

Στο σύστημα με την ονομασία SmartITS, χρησιμοποιούν μια έξυπνη συσκευή ως μονάδα ανίχνευσης (ονομάζεται Portable Sensing Unit (PSU)) που σαρώνει παθητικά τα frames που μεταδίδονται από κοντινές ασύρματες φοιτητές συσκευές (Wi-Fi / Bluetooth (BT) / Bluetooth Low Energy (BLE)) και εξάγει τα μοναδικά αναγνωριστικά MAC για να εντοπίσουν τους ιδιοκτήτες των συσκευών χρησιμοποιώντας τις συντεταγμένες θέσης του PSU. Ωστόσο, προτείνουν ένα νέο σύστημα ταυτοποίησης, παρακολούθησης και εντοπισμού τοποθεσίας φορητών συσκευών, το οποίο δεν απαιτεί επιπλέον υποδομή υλικού για ανάπτυξη καθώς και δεν χρειάζεται καθόλου τροποποίηση στη σχεδίαση υλικού. Επιπλέον το PSU, μια μονάδα ανίχνευσης αρκεί για τη λήψη αιτημάτων διερεύνησης και της τοποθεσίας του χρήστη χωρίς την ενεργή συνεργασία του χρήστη.[8]

Από όλες τα παρόμοια έργα που έχω μελετήσει συμπέρανα ότι ο μόνος τρόπος για να μπορέσουμε να υπολογίσουμε την σχετική τοπικότητα μια φορητής συσκευής στο χώρο που χρησιμοποιώ ασύρματο δίκτυο είναι το RSSI (Received Signal Strength Indicator), δηλαδή η δύναμη του σήματος η οποία βρίσκεται μέσα στο πακέτο. Μπορεί να είναι ασταθής και μη αξιόπιστη το RSSI αλλά είναι η μόνη πληροφορία που έχουμε. [1]

2.2 Σύστημα Εύρεσης Τοπικοτητας

Το σύστημα μας χρησιμοποιεί ένα αριθμό από συγχρονισμένους κόμβους (δρομολογητές με αντένες Wi-Fi) για την συλλογή των πακέτων που μεταδίδονται από τους χρήστες των φορητών συσκευών. Τα πακέτα που συλλέγονται είναι όλων των τύπων, δηλαδή από probe request σε οτιδήποτε request κάνει οποιαδήποτε εφαρμογή στην συσκευή καθώς η πληροφορίες που θέλουμε βρίσκονται στο Data-Link Layer το οποίο δεν είναι κρυπτογραφημένο γιατί δεν περιέχει τις πληροφορίες της εφαρμογής. Αυτό κάνει την συλλογή των πακέτων να γίνετε παθητικά, χωρίς κάποια ενέργεια του χρήστη, δηλαδή δεν υπάρχει κανένα πρόγραμμα να τρέχει στην φορητή συσκευή αλλά ούτε χρειάζεται η συσκευή να ενωθεί στο δίκτυο που τρέχει το σύστημα μας. Οι δρομολογητές θα αρχίσουν συγχρονισμένα να συλλέγουν πακέτα σε απόσταση βελησνεκές και θα είναι σε κατάσταση “monitor” για 30 λεπτά. Αφού περάσει η μισή ώρα ότι έχει μαζευτεί θα γραφτεί σε ένα pcap αρχείο από κάθε κόμβο και θα στέλνονται στο κεντρικό υπολογιστικό σύστημα για να γίνει η επεξεργασία και οι κόμβοι με την σειρά τους να ξαναρχίζουν αυτήν την διαδικασία από την αρχή.

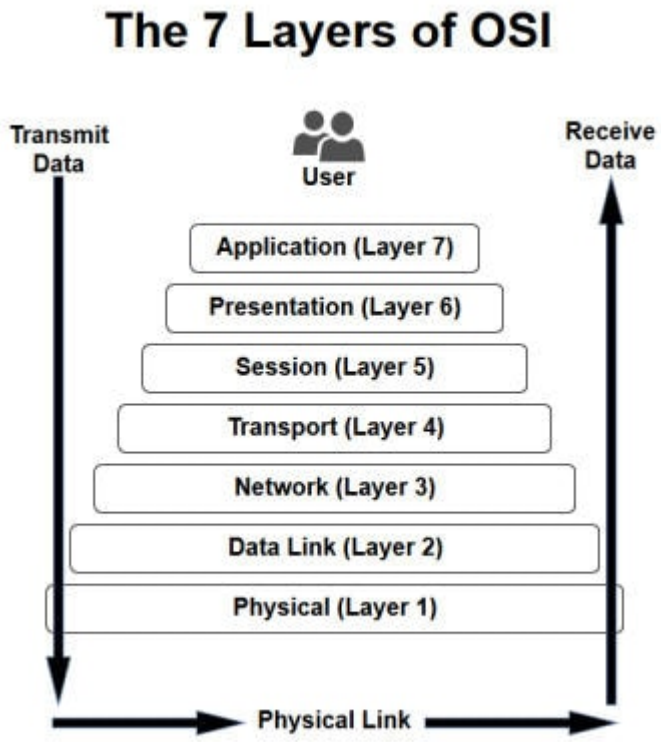
Η λειτουργία “monitor” επιτρέπει στον κόμβο να συλλάβει όλα τα frames του ασύρματου πακέτου (τα μέρη που δεν είναι κρυπτογραφημένα), ακόμα και τα πακέτα που δεν προορίζονται για αυτόν. Η λειτουργία “monitor” με λίγα λόγια δεν απαιτεί στην φορητή συσκευή να είναι συνδεδεμένη στο ίδιο δίκτυο με τον κόμβο που τρέχει αυτή την λειτουργία. Από την άλλη μεριά έχουμε την λειτουργία “promiscuous” που επιτρέπει σε ένα κόμβο να συλλέγει frames από φορητές συσκευές που είναι ενωμένες στο ίδιο δίκτυο με αυτό. Στην λειτουργία “promiscuous” τα Wi-Fi frames υποβάλλονται σε επεξεργασία και η κεφαλίδα του αφαιρείται από πάνω του, ενώ στην λειτουργία “monitor” τα frames περνούν χωρίς καμία επεξεργασία. Επομένως είναι προτιμότερο η λειτουργία “monitor” αφού μας αυξάνει το μέγεθος pcap αχρείου για καλύτερη ανάλυση (δηλαδή μπορεί να συλλέγουν παραπάνω πακέτα αφού συλλέγει όσα πακέτα είναι στην εμβέλεια της συσκευής χωρίς να μας ενδιαφέρει ποιος είναι ο παραλήπτης του πακέτου).

Μια φορητή συσκευή που μπορεί να ενωθεί σε ασύρματο δίκτυο, μπορεί να το κάνει χρησιμοποιώντας μόνο ένα κανάλι την φορά. Τα AP είναι αυτά που καθορίζουν σε ποιο κανάλι θα επικοινωνούν με τις συσκευές που είναι συνδεδεμένη. Γι’ αυτό τον λόγο και επειδή μια συσκευή που θέλει να ενωθεί σε ένα ασύρματο δίκτυο δεν ξέρει ποια AP είναι στο χώρο και κατ’ επέκταση ποια συχνότητα (κανάλι) χρησιμοποιούν οι APς που θέλει να ενωθεί, στείλει τα λεγόμενα probe request. Η ιδιαιτερότητα αυτού του request είναι ότι γίνονται broadcast σε όλα τα

κανάλια για σκοπούς ανακάλυψης γειτονικών Aps. Το ίδιο ισχύει κατά τη λήψη Wi-Fi πακέτων. Στο σενάριο λήψης απλώς μετατρέπουμε την ασύρματη διεπαφή από τη access mode σε monitor mode και ως εκ τούτου μπορεί να παρακολουθεί μόνο ένα κανάλι κάθε φορά.

2.3 Data-Link Layer

Ο International Standards Organization (ISO) ανέπτυξε το μοντέλο Open Systems Interconnection (OSI). Χωρίζει την επικοινωνία δικτύου σε επτά επίπεδα. Σε αυτό το μοντέλο, τα επίπεδο 1-4 θεωρούνται τα κατώτερα στρώματα και αφορούν κυρίως τα κινούμενα δεδομένα. Τα επίπεδα 5-7, που ονομάζονται τα ανώτερα στρώματα, περιέχουν δεδομένα σε επίπεδο εφαρμογής. Τα δίκτυα λειτουργούν βάσει μιας βασικής αρχής, μετάδοση από επίπεδο σε επίπεδο. Κάθε επίπεδο φροντίζει για μια πολύ συγκεκριμένη εργασία και, στη συνέχεια, διαβιβάζει τα δεδομένα στο επόμενο επίπεδο. Κάθε επίπεδο βάζει γύρω από τα δεδομένα την δική του κεφαλίδα με τις δικές του πληροφορίες και το περνά στο επόμενο επίπεδο. [2]



Εικόνα 2.3.1 [2]

Στο μοντέλο OSI, ο έλεγχος περνά από το ένα στρώμα στο άλλο, ξεκινώντας από το επίπεδο εφαρμογής (επίπεδο 7) σε έναν σταθμό, και προχωρώντας στο κάτω επίπεδο, πάνω από το κανάλι επικοινωνίας (που στην δική μας περίπτωση δεν είναι το Ethernet καλώδιο αλλά ο αέρας πού μεταδίδει τα ασύρματα πακέτα μέσω κάποιας συγκεκριμένης κοινής συχνότητας που ακούει το AP) στον επόμενο όπου και εκείνος με την σειρά του αρχίζει να ξεδιπλώνει τα επίπεδα από κάτω προς τα πάνω μέχρι που να φτάσει στο επίπεδο 7. Το μοντέλο OSI αναλαμβάνει το έργο της διασύνδεσης δικτύων και το χωρίζει σε αυτό που αναφέρεται ως κάθετη στοίβα που αποτελείται από τα ακόλουθα 7 επίπεδα. (βλέπε σχήματα 2.3.1) [2]

Application (Επίπεδο 7)

Το μοντέλο OSI, Layer 7, υποστηρίζει εφαρμογές και διαδικασίες τελικών χρηστών. Αναγνωρίζονται Συνέταιροι επικοινωνίας, αναφέρεται η ποιότητα της υπηρεσίας, λαμβάνονται υπόψη ο έλεγχος ταυτότητας χρήστη και το απόρρητο και προσδιορίζονται τυχόν περιορισμοί στη σύνταξη δεδομένων. Όλα σε αυτό το επίπεδο είναι ειδικά για την εφαρμογή. Αυτό το επίπεδο παρέχει υπηρεσίες εφαρμογής για μεταφορά αρχείων, e-mail και άλλες υπηρεσίες λογισμικού δικτύου. [2]

Presentation (Επίπεδο 6)

Αυτό το επίπεδο παρέχει ανεξαρτησία από τις διαφορές στην αναπαράσταση δεδομένων (π.χ. κρυπτογράφηση) μεταφράζοντας από μορφή εφαρμογή σε μορφή δικτύου και αντίστροφα. Το επίπεδο παρουσίασης ουσιαστικά μετατρέπει τα δεδομένων σε μορφή που μπορεί να αποδεχθεί το επίπεδο εφαρμογής αν παραλαμβάνει το πακέτο και το αντίστροφο αν στέλνει το πακέτο προς τα έξω. Αυτό το επίπεδο μορφοποιεί και κρυπτογραφεί δεδομένα για αποστολή σε ένα δίκτυο, παρέχοντας λύση στα τυχόν προβλήματα συμβατότητας. Ονομάζεται μερικές φορές το επίπεδο σύνταξης. [2]

Session (Επίπεδο 5)

Αυτό το επίπεδο δημιουργεί, διαχειρίζεται και τερματίζει συνδέσεις μεταξύ εφαρμογών. Το επίπεδο Session ρυθμίζει, συντονίζει και τερματίζει συνομιλίες, ανταλλαγές και διαλόγους μεταξύ των εφαρμογών σε κάθε άκρο. [2]

Transport (Επίπεδο 4)

Το μοντέλο OSI, επίπεδο 4, παρέχει διαφανή μεταφορά δεδομένων μεταξύ τελικών συστημάτων ή κεντρικών υπολογιστών και είναι υπεύθυνο για την ανάκτηση σφαλμάτων από άκρο σε άκρο και τον έλεγχο ροής. Εξασφαλίζει πλήρη μεταφορά δεδομένων. [2]

Network (Επίπεδο 3)

Το επίπεδο 3 παρέχει τεχνολογίες εναλλαγής και δρομολόγησης, δημιουργώντας λογικές διαδρομές, γνωστές ως εικονικά κυκλώματα, για τη μετάδοση δεδομένων από κόμβο σε κόμβο. Η δρομολόγηση και η προώθηση είναι λειτουργίες αυτού του επιπέδου, καθώς και η παροχή διευθύνσεων (IP), χειρισμός σφαλμάτων, έλεγχος συμφόρησης και αλληλουχία πακέτων. [2]

Data Link (Επίπεδο 2)

Το μοντέλο OSI, επίπεδο 2, τα πακέτα δεδομένων κωδικοποιούνται και αποκωδικοποιούνται σε bits. Παρέχει πρωτόκολλα διαχείριση και μετάδοσης και χειρίζεται σφάλματα στο φυσικό επίπεδο (επίπεδο 1), έλεγχο ροής και συγχρονισμό frame. Το επίπεδο Data Link χωρίζεται σε δύο επιμέρους επίπεδα: το επίπεδο ελέγχου πρόσβασης μέσων (MAC) και το επίπεδο ελέγχου λογικής σύνδεσης (LLC). Το υπο-επίπεδο MAC ελέγχει τον τρόπο με τον οποίο ένας υπολογιστής στο δίκτυο αποκτά πρόσβαση στα δεδομένα και άδεια για τη μετάδοσή τους, ενώ το υπο-επίπεδο LLC ελέγχει το συγχρονισμό των frames, τον έλεγχο ροής και τον έλεγχο σφαλμάτων. [2]

Physical (Επίπεδο 1)

Το μοντέλο OSI, επίπεδο 1 μεταφέρει τη bit-ροή (ηλεκτρική ώθηση, φως ή ραδιοφωνικό σήμα) μέσω του δικτύου σε ηλεκτρικό και μηχανικό επίπεδο. Παρέχει τα μέσα υλικού για την αποστολή και τη λήψη δεδομένων σε έναν φορέα, συμπεριλαμβανομένου του καθορισμού καλωδίων, καρτών και φυσικών πτυχών και αντένες ασύρματου δικτύου. [2]

Για την δική μας περίπτωση ο κόμβος μας κάνει παθητική συλλογή πακέτων με την monitor επιλογή. Αυτό σημαίνει ότι μπορεί να συλλέξει τα γύρο πακέτα εντός εμβέλειας τα οποία δεν προορίζονται γι’ αυτό τον κόμβο. (το πιο πιθανόν θα προορίζονται σε κάποιο AP). Για να αρχίσει μια συσκευή να στέλνει ασύρματα πακέτα με σκοπό να καταλήξουν σε ένα προορισμό μέσω του δικτύου πρέπει πρώτα να γίνει μια συμφωνία μεταξύ της συσκευής και του AP εφόσον η συσκευή έχει το δικαίωμα να ενωθεί σε αυτόν . Σε αυτή την συμφωνία ανταλλάσσονται διάφορες πληροφορίες περί ασφάλειας. Συγκεκριμένα το AP και η συσκευή συμφωνούν ποιο αλγόριθμο κρυπτογράφησης θα χρησιμοποιήσουν και αφού γίνει αυτό ανταλλάσσουν κλειδιά μεταξύ τους. Αυτό γίνεται για σκοπούς κρυπτογράφησης δεδομένων στο επίπεδο εφαρμογής μέχρι και στο επίπεδο μεταφοράς (επίπεδο 7 – 4).

Το σημείο της συλλογής δεδομένων με την monitor επιλογή λειτουργεί γιατί οι πληροφορίες που χρειαζόμαστε για να δουλέψει το έργο μας βρίσκονται στο Data Link επίπεδο. Λόγο αυτής της αρχιτεκτονικής που υποστηρίζει το διαδίκτυο (μοντέλο OSI) το Data Link επίπεδο δεν κρυπτογραφείται (κρυπτογραφείται μόνο σε εσωτερικά δίκτυα όπως ο στρατός) γιατί δεν είναι εφικτό μέσω του Διαδικτύου, επειδή οι ενδιάμεσοι κόμβοι μπορεί να μην είναι ούτε προσβάσιμοι αλλά ούτε ασφαλείς.

Εν κατακλείδα στον κόμβο μας καταφθάνει το πακέτο με προσβάσιμες πληροφορίες από το επίπεδο 1 μέχρι και το επίπεδο 3. Στο Data Link (επίπεδο 2) βρίσκουμε την MAC διεύθυνση της συσκευής που έστειλε το πακέτο, την δύναμη του σήματος και το timestamp που δείχνει την ώρα δημιουργίας του πακέτου από την συσκευή. Όσον αφορά το περιεχόμενο του πακέτου δεν μπορεί να διακριθεί (ούτως ή αλλιώς δεν περιέχει πληροφορίες που χρειαζόμαστε) γιατί είναι κρυπτογραφημένο.

Κεφάλαιο 3

Τρόπος συλλογής πακέτων

3.1 Monitor Mode

Πριν ξεκινήσουμε την ασύρματη συλλογή πακέτων χρησιμοποιώντας τον κόμβο μας, είναι χρήσιμο να κατανοήσουμε τους διαφορετικούς τρόπους λειτουργίας που υποστηρίζονται από ασύρματες Wi-Fi κάρτες. Οι περισσότεροι ασύρματοι χρήστες χρησιμοποιούν μόνο τις ασύρματες κάρτες τους ως σταθμό σε ένα AP. Στη managed λειτουργία, η ασύρματη κάρτα σε συνεργασία με το λειτουργικό σύστημα βασίζονται σε ένα τοπικό AP σε managed λειτουργία για να παρέχουν συνδεσιμότητα στο ασύρματο δίκτυο. (δημιουργώντας μια γέφυρα μεταξύ συσκευής και AP)

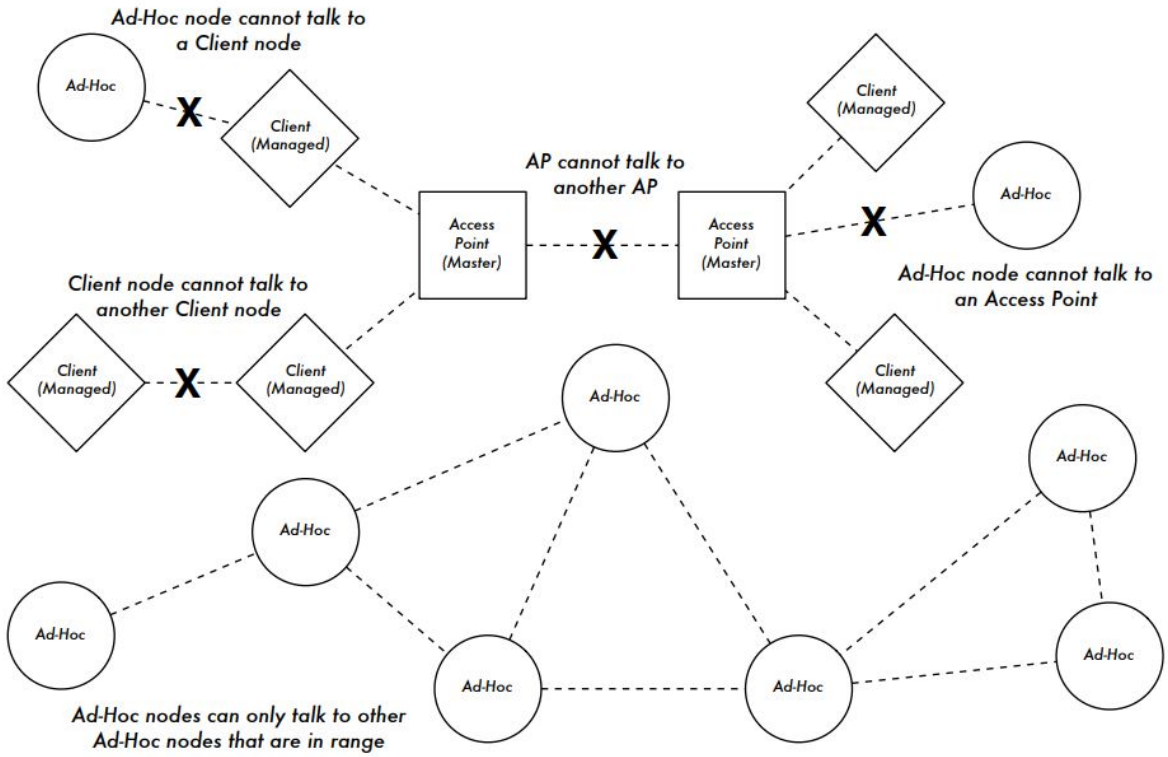
Η managed λειτουργία αναφέρεται επίσης μερικές φορές και ως λειτουργία πελάτη (client). Οι ασύρματες κάρτες σε managed λειτουργία θα ενταχθούν σε ένα δίκτυο που δημιουργήθηκε από έναν master και θα αλλάξουν αυτόματα το κανάλι τους ώστε να συμβιβαστούν με αυτόν του master. Θα δημιουργηθεί μια συσχέτιση (association) μεταξύ κόμβου και πελατών και οι πελάτες θα χρησιμοποιούν των κόμβο με αυτή την λειτουργία σαν AP. Οι Wi-Fi κάρτες σε managed λειτουργία δεν μπορούν να επικοινωνούν απευθείας μεταξύ με άλλες κάρτες σε managed λειτουργία αλλά επικοινωνούν μόνο με έναν συσχετιζόμενο κόμβο με master λειτουργία. [11]

Πολλές ασύρματες κάρτες υποστηρίζουν επίσης την master λειτουργία, όπου η ασύρματη κάρτα παρέχει τις υπηρεσίες ενός AP όταν συνδυάζεται με το κατάλληλο λογισμικό. Η λειτουργία master τους επιτρέπει να διαμορφώσουν το κόμβο ως AP για την παροχή σύνδεσης σε άλλους ασύρματους σταθμούς. [11]

Η master λειτουργία (ονομάζεται επίσης AP λειτουργία ή infrastructure λειτουργία) χρησιμοποιείται για τη δημιουργία μιας υπηρεσίας που μοιάζει με ένα παραδοσιακό AP. Η ασύρματη κάρτα δημιουργεί ένα δίκτυο με ένα συγκεκριμένο όνομα (ονομάζεται SSID) και προσφέρει υπηρεσίες δικτύου (ανταλλαγή πακέτων) σε ένα συγκεκριμένο κανάλι (κανάλι σημαίνει επιλογή συχνότητας). Οι ασύρματες κάρτες σε master λειτουργία μπορούν να επικοινωνούν μόνο με κάρτες που σχετίζονται με αυτή σε Managed λειτουργία. [11]

Μια άλλη κοινή λειτουργία για ασύρματες κάρτες είναι η λειτουργία ad-hoc (ή αλλιώς η λειτουργία Independent Basic Service Set [IBSS]. Δύο ασύρματοι σταθμοί που θέλουν να επικοινωνήσουν ο ένας με τον άλλο μπορούν να το πράξουν μοιραζόμενοι τις ευθύνες ενός AP για ένα περιορισμένο υποσύνολο LAN λειτουργιών. Η λειτουργία Ad-hoc χρησιμοποιείται για βραχυπρόθεσμη συνδεσιμότητα μεταξύ σταθμών, όταν ένα AP δεν είναι διαθέσιμο για την παροχή συνδεσιμότητας στο ασύρματο δίκτυο. [11]

Η Ad-hoc λειτουργία δημιουργεί ένα multipoint-to-multipoint δίκτυο όταν δεν υπάρχει διαθέσιμο master ή AP. Σε λειτουργία ad-hoc, κάθε ασύρματη κάρτα επικοινωνεί απευθείας με τους γείτονές της. Οι κόμβοι πρέπει να βρίσκονται μεταξύ τους για να επικοινωνούν και πρέπει να συμφωνούν για ένα όνομα δικτύου και ένα κανάλι. [11]



Τέλος, οι ασύρματες κάρτες υποστηρίζουν τη monitor λειτουργία. Όταν διαμορφωθεί σε monitor λειτουργία, η ασύρματη κάρτα σταματά να μεταδίδει δεδομένα και εισπράττει το τρέχον επιλεγόμενο κανάλι, αναφέροντας το περιεχόμενο οποιωνδήποτε πακέτων που συλλέγει μέσω του συγκεκριμένου καναλιού στο λειτουργικό σύστημα του κόμβου (στο firmware του δρομολογητή). Αυτός είναι ο πιο χρήσιμος τρόπος λειτουργίας για ανάλυση πακέτων, επειδή μια ασύρματη κάρτα διαμορφωμένη σε monitor λειτουργία αναφέρει ολόκληρο το περιεχόμενο των ασύρματων πακέτων, συμπεριλαμβανομένων των πληροφοριών κεφαλίδας και των κρυπτογραφημένων. [11]

Η monitor λειτουργία χρησιμοποιείται από ορισμένα εργαλεία (όπως το Wireshark, tcpdump, airodumb-ng) για την παθητική συλλογή όλων των πακέτων σε ένα δεδομένο κανάλι. Αυτό είναι χρήσιμο για την ανάλυση προβλημάτων σε ασύρματη σύνδεση ή για την παρατήρηση της χρήσης φάσματος στην τοπική περιοχή. Η monitor λειτουργία δεν χρησιμοποιείται για κανονικές επικοινωνίες.

Άρα όπως συμπεραίνουμε η καταλληλότερη λειτουργία για το δικό μας έργο είναι η monitor λειτουργία όπου παθητικά μπορεί να συλλέγει πακέτα από κοντινές κινητές συσκευές χωρίς να έχει κάποια ιδιαίτερη σχέσει με αυτές ο κόμβος (δηλαδή δεν υπάρχει κάποιος συσχετισμός όπως υπάρχει και μεταξύ των master και managed λειτουργιών).

3.2 Wi-fi Adapter

Οι ιδιοκτήτες σπιτιών και επιχειρήσεων που θέλουν να αγοράσουν εργαλεία δικτύωσης αντιμετωπίζουν μια σειρά πολλές επιλογές. Πολλά προϊόντα υιοθετούν τα ασύρματα πρότυπα 802.11a, 802.11b / g / n ή / και 802.11ac, γνωστά ως τεχνολογίες Wi-Fi. Το Bluetooth και διάφορες άλλες ασύρματες (αλλά όχι Wi-Fi) τεχνολογίες υπάρχουν στην αγορά, καθεμία σχεδιασμένη για συγκεκριμένες εφαρμογές δικτύωσης.

Για γρήγορη αναφορά, το 801.11ax (Wi-Fi 6) είναι το πιο πρόσφατα εγκεκριμένο πρότυπο. Το πρωτόκολλο εγκρίθηκε το 2019. Ακριβώς επειδή ένα πρότυπο έχει εγκριθεί, ωστόσο, δεν σημαίνει ότι είναι το πρότυπο που χρειάζεστε για τη συγκεκριμένη περίπτωσή μας. Τα πρότυπα ενημερώνονται πάντα, όπως και ο τρόπος ενημέρωσης του λογισμικού σε smartphone ή στον υπολογιστή μας. [10]

Το 1997, το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών δημιούργησε το πρώτο πρότυπο WLAN. Δυστυχώς, το 802.11 υποστήριξε μόνο ένα μέγιστο εύρος ζώνης δικτύου 2 Mbps - πολύ αργό για τις περισσότερες εφαρμογές. Για αυτόν τον λόγο, τα ασύρματα προϊόντα με πρότυπο 802.11 δεν κατασκευάζονται πλέον. Ωστόσο, μια ολόκληρη γενιά δημιουργήθηκε κληρονομώντας από το αρχικό πρότυπο. [10]

	802.11 (Legacy)	802.11b (Legacy)	802.11a (Legacy)	802.11g (Legacy)	802.11n (HT)	802.11ac (VHT)	802.11ax (HE)
Year Ratified	1997	1999	1999	2003	2009	2014	2019 (Expected)
Operating Band	2.4 GHz/IR	2.4 GHz	5 GHz	2.4 GHz	2.4/5 GHz	5 GHz	2.4/5 GHz
Channel BW	20 MHz	20 MHz	20 MHz	20 MHz	20/40 MHz	20/40/80/160 MHz	20/40/80/160 MHz
Peak PHY Rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	6.8 Gbps	10 Gbps
Link Spectral Efficiency	0.1 bps/Hz	0.55 bps/Hz	2.7 bps/Hz	2.7 bps/Hz	15 bps/Hz	42.5 bps/Hz	62.5 bps/Hz
Max # SU Streams	1	1	1	1	4	8	8
Max # MU Streams	NA	NA	NA	NA	NA	4 (DL only)	8 (UL & DL)
Modulation	DSSS, FHSS	DSSS, CCK	OFDM	OFDM	OFDM	OFDM	OFDM, OFDMA
Max Constellation / Code Rate	DQPSK	CCK	64-QAM, 3/4	64-QAM, 3/4	64-QAM, 5/6	256-QAM, 5/6	1024-QAM, 5/6
Max # OFDM tones	NA	NA	64	64	128	512	2048
Subcarrier Spacing	NA	NA	312.5 kHz	312.5 kHz	312.5 kHz	312.5 kHz	78.125 kHz

Εικόνα 3.2.1

Ο καλύτερος τρόπος για να καταλάβουμε αυτά τα πρότυπα είναι να θεωρήσουμε το πρότυπο 802.11 ως θεμέλιο και όλες τα άλλα πρότυπα ως δομικά στοιχεία πάνω σε αυτό το αρχικό πρότυπο (802.11) που εστιάζουν στη βελτίωση τόσο μικρών όσο και μεγάλων πτυχών της τεχνολογίας. Ορισμένα δομικά στοιχεία έχουν μικρές βελτιώσεις ενώ άλλα έχουν αρκετά μεγάλες αναβαθμίσεις.

Ο IEEE επεκτάθηκε στο αρχικό πρότυπο 802.11 τον Ιούλιο του 1999, δημιουργώντας τις προδιαγραφές 802.11b. Το 802.11b υποστηρίζει θεωρητική ταχύτητα έως και 11 Mbps. Αναμένεται ένα πιο ρεαλιστικό εύρος ζώνης 5,9 Mbps σε TCP σύνδεση και 7,1 Mbps σε UDP σύνδεση. [10]

Το 802.11b χρησιμοποιεί την ίδια συχνότητα ραδιοκυμανσης (2,4 GHz) με το αρχικό πρότυπο 802.11. Χωρίς την απαραίτητο έλεγχο, οι συσκευές με πρότυπο 802.11b μπορούν να έχουν παρεμβολές από φούρνους μικροκυμάτων, ασύρματα τηλέφωνα και άλλες συσκευές που χρησιμοποιούν την ίδια περιοχή (φάσμα συχνοτήτων) 2,4 GHz. Ωστόσο, με την εγκατάσταση συσκευών με πρότυπο 802.11b σε λογική απόσταση από άλλες συσκευές, οι παρεμβολές μπορούν εύκολα να αποφευχθούν. Το 802.11b αναφέρεται επίσης ως Wi-Fi 1. [10]

Ενώ το 802.11b ήταν σε εξέλιξη, το IEEE δημιούργησε μια δεύτερη επέκταση στο αρχικό πρότυπο 802.11 που ονομάζεται 802.11a. Λόγω του υψηλότερου κόστους του, το 802.11a βρίσκεται συνήθως σε επιχειρηματικά δίκτυα, ενώ το 802.11b εξυπηρετεί καλύτερα την εγχώρια αγορά. [10]

Το 802.11a υποστηρίζει εύρος ζώνης έως 54 Mbps και σήματα σε ρυθμιζόμενο φάσμα συχνοτήτων 5 GHz. Η υψηλότερη συχνότητα του 802.11a δίνει την δυνατότητα στο σήμα να είναι καλύτερο, δηλαδή αντανακλά πιο εύκολα από τοίχους και άλλα εμπόδια σε σχέση με το 802.11b. Η υψηλότερη συχνότητα σημαίνει επίσης ότι το 802.11a έχει μικρότερη απόσταση (μέγιστη απόσταση από την οποία ένας κόμβος με πρότυπο 802,11a μπορεί να παραλάβει πλακέτα από μια άλλη συσκευή η οποία τα στέλνει). [10]

Επειδή τα 802.11a και 802.11b χρησιμοποιούν διαφορετικές συχνότητες, οι δύο τεχνολογίες δεν είναι συμβατές μεταξύ τους. Το 802.11a αναφέρεται επίσης ως Wi-Fi 2. [10]

Το 2002 και το 2003, τα προϊόντα WLAN που υποστηρίζουν ένα νεότερο πρότυπο που ονομάζεται 802.11g. Το 802.11g προσπαθεί να συνδυάσει τα καλύτερα τόσο των 802.11a όσο και των 802.11b. Το 802.11g υποστηρίζει εύρος ζώνης έως 54 Mbps και χρησιμοποιεί τη συχνότητα 2,4 GHz για μεγαλύτερη εμβέλεια. Το 802.11g είναι συμβατό με το 802.11b, πράγμα που σημαίνει

ότι τα AP με πρότυπο 802.11g θα λειτουργούν με wireless network adapters με πρότυπο 802.11b. Το 802.11g αναφέρεται επίσης ως Wi-Fi 3. [10]

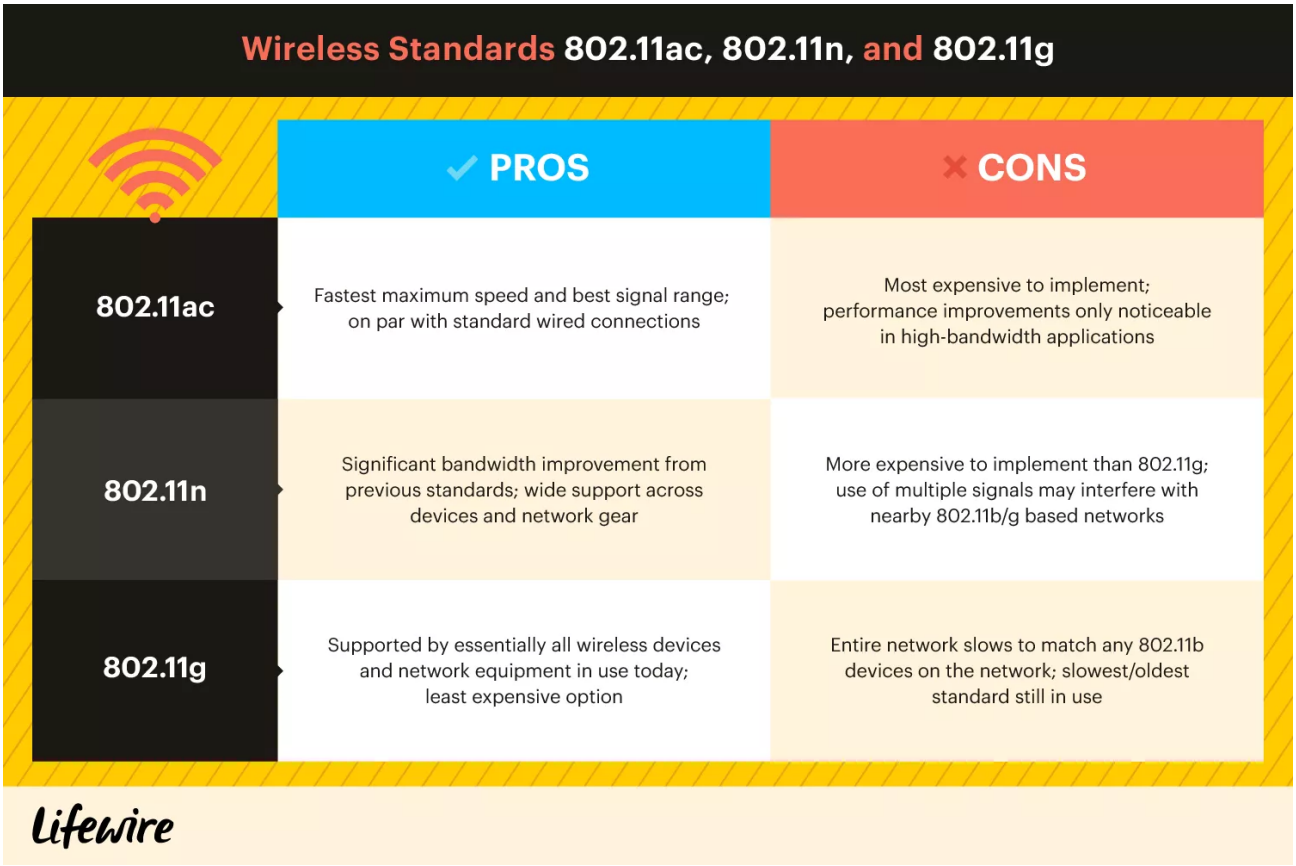
Το 802.11n (επίσης γνωστό και ως Wireless N) σχεδιάστηκε για να βελτιώσει το 802.11g στο εύρος ζώνης που υποστηρίζει, χρησιμοποιώντας πολλά ασύρματα σήματα και κεραίες (που ονομάζονται τεχνολογία MIMO) αντί για ένα. Οι όμιλοι βιομηχανικών προτύπων επικύρωσαν τα 802.11n το 2009 με προδιαγραφές που προβλέπουν έως και 300 Mbps εύρος πλάτους ζώνης δικτύου. Το 802.11n προσφέρει επίσης καλύτερη μέγιστη απόσταση σήματος σε σχέση με τα προηγούμενα πρότυπα Wi-Fi λόγω της αυξημένης έντασης του σήματος και είναι ακόμα συμβατό και με την ταχύτητα 802.11b / g. [10]

Για το 802.11n παρατηρείται σημαντική βελτίωση εύρους ζώνης από προηγούμενα πρότυπα αλλά είναι πιο ακριβό το κόστος εφαρμογής από 802.11g και η χρήση πολλαπλών σημάτων ενδέχεται να επηρεάσει τα κοντινά δίκτυα 802.11b / g. Το 802.11n αναφέρεται επίσης και ως Wi-Fi 4.

Η γενιά του Wi-Fi που σηματοδότησε για πρώτη φορά για τη πιο δημοφιλή χρήση είναι το 802.11ac το οποίο χρησιμοποιεί ασύρματη τεχνολογία διπλής ζώνης, υποστηρίζοντας ταυτόχρονες συνδέσεις και στις ζώνες Wi-Fi 2,4 GHz και 5 GHz. Το 802.11ac προσφέρει συμβατότητα με το πρότυπο 802.11b / g / n και εύρος ζώνης έως 1300 Mbps στη ζώνη 5 GHz συν έως 450 Mbps στα 2,4 GHz. Οι περισσότεροι οικιακοί ασύρματοι δρομολογητές χρησιμοποιούν αυτό το πρότυπο. Το 802.11ac αναφέρεται επίσης ως Wi-Fi 5. [10]

Το 802.ad έχει εγκρίθηκε τον Δεκέμβριο του 2012, αυτό το πρότυπο είναι εξαιρετικά γρήγορο. Ωστόσο, η συσκευή πελάτη πρέπει να βρίσκεται σε απόσταση 11 μέτρων από το σημείο πρόσβασης. [10]

Με την επωνυμία Wi-Fi 6, το πρότυπο 802.11ax κυκλοφόρησε το 2019 και θα αντικαταστήσει το 802.11ac ως το de facto ασύρματο πρότυπο. Το Wi-Fi 6 μέγιστο bandwidth 10 Gbps, χρησιμοποιεί λιγότερη ισχύ, είναι πιο αξιόπιστο σε περιβάλλον με συμφόρηση και υποστηρίζει καλύτερη ασφάλεια. [10]



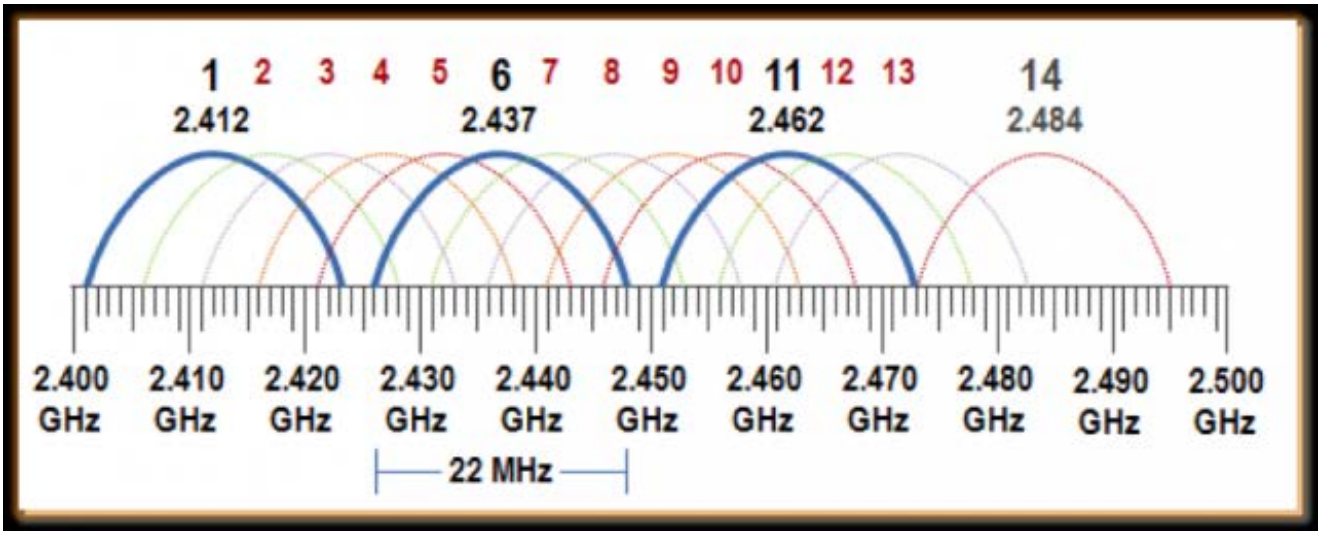
Εικόνα 3.2.2[10]

Αρχικά πρώτα έχω κάνει τις απαραίτητες ρυθμίσεις για πρώτη προσπάθεια συλλογής κοντινών ασύρματων πακέτων μέσω της Wi-Fi adapter κάρτας του προσωπικού μου φορητού υπολογιστή.

Η Wi-Fi κάρτα του Lenovo ideapad 320 είναι η Intel Dual Band Wireless -AC 3165. Η Intel Dual Band Wireless -AC 3165 είναι Intel 2ης γενιάς με πρότυπο 802.11ac, διπλής ζώνης (2.4 GHz και 5 GHz), 1x1 Wi-Fi + Bluetooth. Τα 1x1 αναφέρονται στον αριθμό εκπομπών και λήψης κυμάτων από και προς στην κάρτα Wi-Fi. Για παράδειγμα το 2x2 σημαίνει ότι έχει δύο σημεία μετάδοσης και δύο σημεία λήψεις κυμάτων διαφορετικής συχνότητας την ίδια χρονική στιγμή. Γι' αυτό το λόγο το πρότυπο 802.11n είναι ταχύτερο από την προηγούμενη γενιά τεχνολογιών Wi-Fi επειδή βασίζεται στην παραπάνω λογική.

Λόγο του ότι η κάρτα μας υποστηρίζει 1x1 σημαίνει ότι όταν ενεργοποιήσουμε την monitor λειτουργία θα δεσμεύσει την αντένα στο να συλλέγει πακέτα μιας συγκεκριμένης συχνότητας. Αυτό είναι πρόβλημα γιατί δεν θα μπορέσουμε να συλλέξουμε άλλα πακέτα τα οποία βρίσκονται σε άλλα κανάλια. Και αφού το σύστημα μας θεωρητικά είναι φτιαγμένο για συλλογή πακέτων από πολλές φορητές συσκευές είναι αναγκαίο να μπορέσουμε να συλλέξουμε πακέτα από όσο περισσότερες συσκευές μπορούμε. Η λύση σε αυτό το πρόβλημα είναι αφού ξέρουμε τα κανάλια

στα οποία επικοινωνούν οι γειτονική AP του χώρου (θεωρητικά θα έχουμε admin πρόσβαση στα AP του χώρου που θα βάλουμε σε εφαρμογή τους κόμβους μας για συλλογή δεδομένων) μπορούμε να ρυθμίσουμε τους κόμβους μας να συλλέγουν πακέτα στα συγκεκριμένα κανάλια (συγκεκριμένη συχνότητα). Επειδή τα κανάλια θα είναι περισσότερο από ένα, (για να μην υπάρχει συμφόρηση πακέτων) σε κάθε σημείο πρέπει να μπουν N κόμβοι όπου N ο αριθμός των επιλεγμένων καναλιών από τους AP του χώρου. Κάθε κόμβος θα ακούει σε ένα από τα N κανάλια.



Εικόνα 3.2.3 [3]

3.3 Τεχνική υλοποίηση Wi-Fi Adapter για συλλογή πακέτων σε σύστημα Linux

Η προεπιλεγμένη λειτουργία της Wi-Fi κάρτας είναι η managed λειτουργία η οποία όπως προείπαμε η χρηση της είναι να δημιουργήσει σύνδεση με ένα AP για την παροχή σύνδεσης της συσκευής στο διαδίκτυο. Για για μπορέσει αλλάξει σε monitor λειτουργία πρέπει να γίνει η χρήση ενος προγράμματος το οποίο έχει υλοποιημένα τα απαραίτητα system calls.

Το πως λειτουργεί είναι ότι ο wifi adapter είναι ή γενικά οτιδήποτε hardware κομμάτι είναι συσχετισμένος με μια αντίστοιχη διαπροσωπία. Αυτό γίνεται για να μπορέσει το λειτουργικό σύστημα (όπου σε αυτήν την περίπτωση είναι το Ubuntu Linux) να αποστέλλει και να λαμβάνει εντολές και πληροφοριες αντίστοιχα από το hardware.

Στην δική μας περίπτωση χρησιμοποιείται το airmon-ng το οποίο δέχεται παραμέτρους start/stop για μετατροπή managed σε monitor λειτουργία και monitor σε managed λειτουργία αντοίστοιχα. (βλέπε εικόνα 3.3.1)

MonitorMode.sh

Script > actual_router > wifi_adapter_config > MonitorMode.sh

```
#!/bin/bash

if [[ $1 = on ]]; then
    echo "Enable monitor mode";

    interface_wireless_name=`ifconfig | egrep  "^w" | tr ':' ' ' | awk -F" " '{print $1}'`;

    sudo airmon-ng start $interface_wireless_name
    ifconfig | grep "^w"

    exit 1
fi


if [[ $1 = off ]]; then
    echo "Enable manage mode";

    interface_wireless_name=`ifconfig | egrep  "^w" | tr ':' ' ' | awk -F" " '{print $1}'`;

    sudo airmon-ng stop $interface_wireless_name
    ifconfig | grep "^w"

    exit 1
fi
```

Εικόνα 3.3.1

3.4 Δρομολογητής με OpenWRT

Το OpenWrt Project είναι ένα λειτουργικό σύστημα Linux που λειτουργεί σε embedded συσκευές. Σε σχέση με άλλα στατικό firmware, το OpenWrt παρέχει ένα πλήρως εγγράψιμο σύστημα αρχείων με διαχείριση πακέτων. Αυτό μας απαλλάσσει από την επιλογή και τη διαρρύθμιση της εφαρμογής που παρέχεται από τον προμηθευτή και μας επιτρέπει να προσαρμόσουμε τη συσκευή μέσω της χρήσης πακέτων για οποιαδήποτε εφαρμογή και χρήση. Για προγραμματιστές, το OpenWrt είναι το πλαίσιο για τη δημιουργία μιας εφαρμογής χωρίς να χρειάζεται να δημιουργήσει ένα πλήρες firmware γύρω από αυτό.

Το OpenWrt έχει σχεδιαστεί από επαγγελματίες του δικτύου και άλλους που ενδιαφέρονται για την απόδοση του δικτύου τους. Το OpenWrt ενσωματώνει πολλούς αλγόριθμους από πρόσφατες έρευνες που αποδίδουν πολύ καλύτερες από τα firmware που παρέχεται από προμηθευτή. [15]

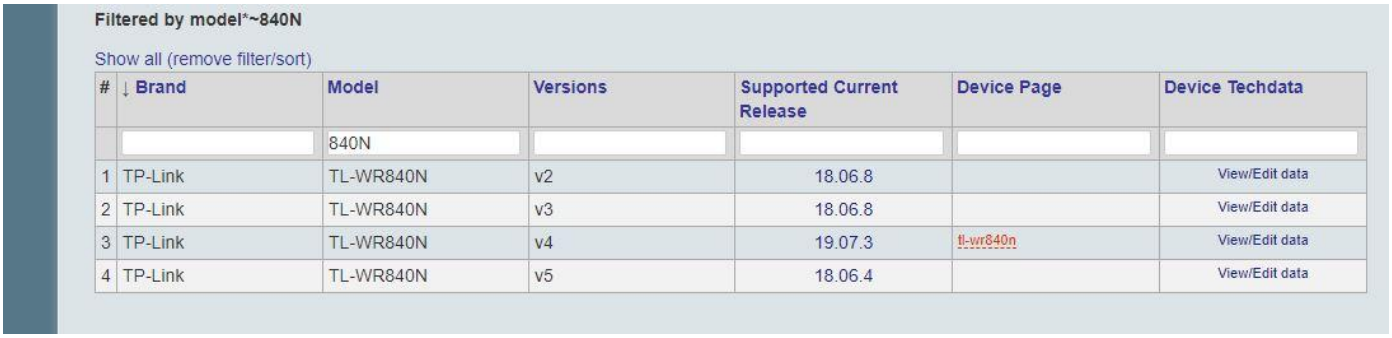
Το OpenWrt είναι σταθερό και λειτουργεί αξιόπιστα για μεγάλα χρονικά διαστήματα με χαμηλή καθυστέρηση ανταπόκρισης και την αυξημένη απόδοση δικτύου μέσω αλγορίθμων ελέγχου bufferbloat. Το Bufferbloat είναι μια αιτία υψηλής καθυστέρησης στα δίκτυα ανταλλαγής πακέτων που προκαλούνται από την υπερβολική προσωρινή αποθήκευση πακέτων. [6]

Οι παλαιότερες συσκευές εξακολουθούν να υποστηρίζονται από νεότερες εκδόσεις του OpenWrt (εφόσον η μνήμη RAM / Flash της συσκευής σας μπορεί να φιλοξενήσει τις νέες εκδόσεις).

Επιπρόσθετα το OpenWrt είναι ένα λογισμικό ανοιχτού κώδικα όπου πολλοί προγραμματιστές από όλο τον κόσμο επανεξετάζουν τον κώδικα πριν κυκλοφορήσει. Αυτό σημένη ότι σε θέματα ασφάλειας θα έχουμε πολλές δοκιμές από πολλούς προγραμματιστές και κατ επέκταση ελέγχους για σκοπούς ανακάλυψη κρυμμένων backdoors ή αδυναμιών που μπορεί να υπάρχει στο σύστημα. [7]

3.5 Ρυθμίσεις OpenWRT στον κόμβο

Στο https://openwrt.org/toh/start μπορούμε να βρούμε αν η συγκεκριμένη μάρκα και μοντέλο υποστηρίζεται από κάποια διάθεση έκδοση του openWRT. (βλέπε εικόνα 3.5.1). Στην δική μας περίπτωση είναι το TP-Link TL-WR840N v5 κι όπως παρατηρούμε είναι η έκδοση OpenWRT 18.06.4.



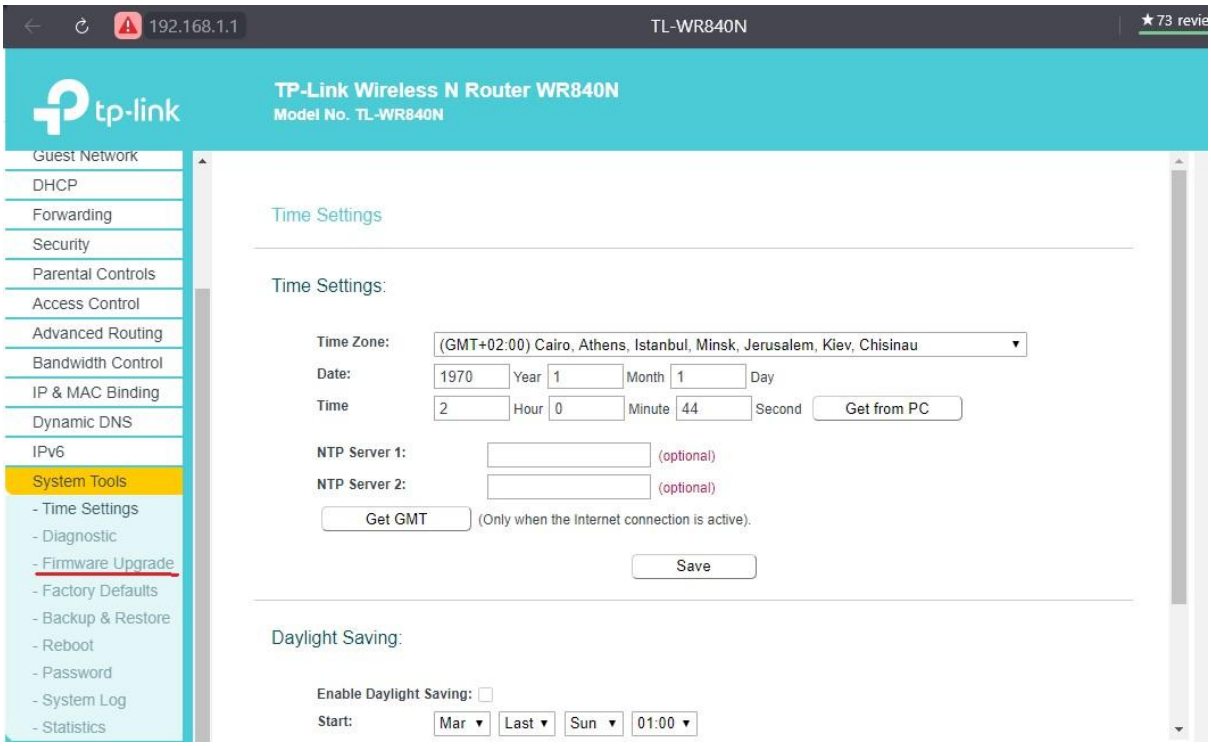
Filtered by model*~840N

Show all (remove filter/sort)

#	↓ Brand	Model	Versions	Supported Current Release	Device Page	Device Techdata
		840N				
1	TP-Link	TL-WR840N	v2	18.06.8		View/Edit data
2	TP-Link	TL-WR840N	v3	18.06.8		View/Edit data
3	TP-Link	TL-WR840N	v4	19.07.3	tl-wr840n	View/Edit data
4	TP-Link	TL-WR840N	v5	18.06.4		View/Edit data

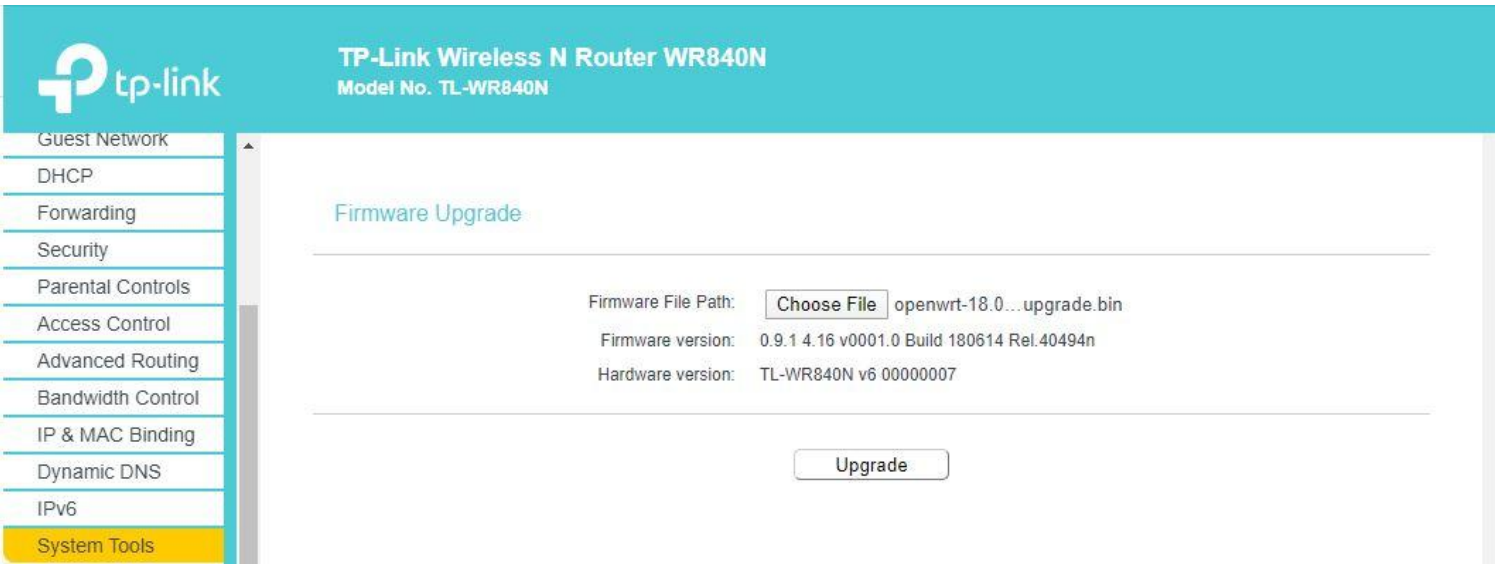
Εικόνα 3.5.1

Αφού γίνει λήψη του binary αρχείου του OpenWRT firmware πρέπει να γίνει η αναβάθμιση του παλιού firmware που τρέχει σαν προεπιλεγμένο firmware από τον προμηθευτή σε OpenWRT. Αυτό γίνεται με μέσα από την γραφική διπροσωπία που παρέχει το firmware του δρομολογητή στην ενότητα Firmware Update. (βλέπε εικόνα 3.5.2)



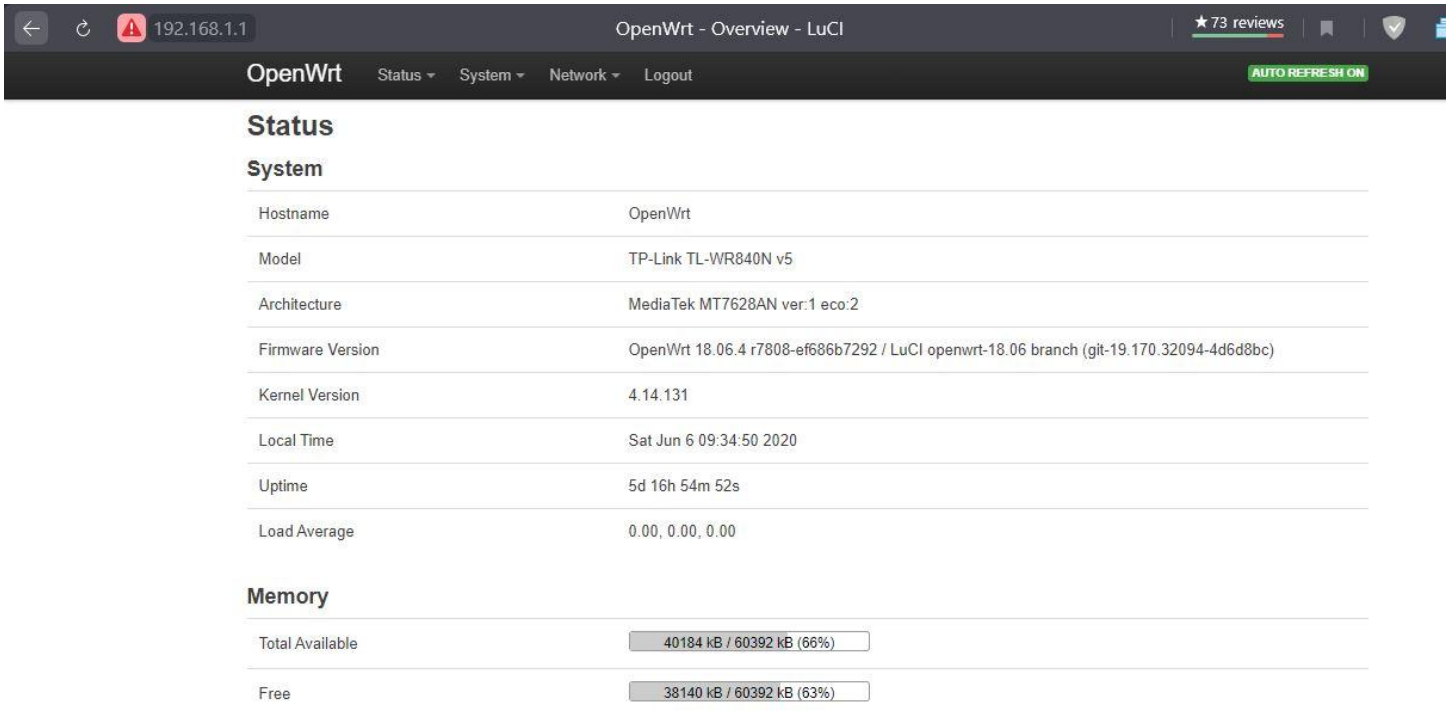
Εικόνα 3.5.2

Το τελευταίο βήμα είναι να φορέσουμε το firmware αρχείο που κατεβάσαμε και πράγματι είναι συμβατό θα αναβαθμιστεί σε OpenWRT. (βλέπε εικόνα 3.5.3)



Εικόνα 3.5.3

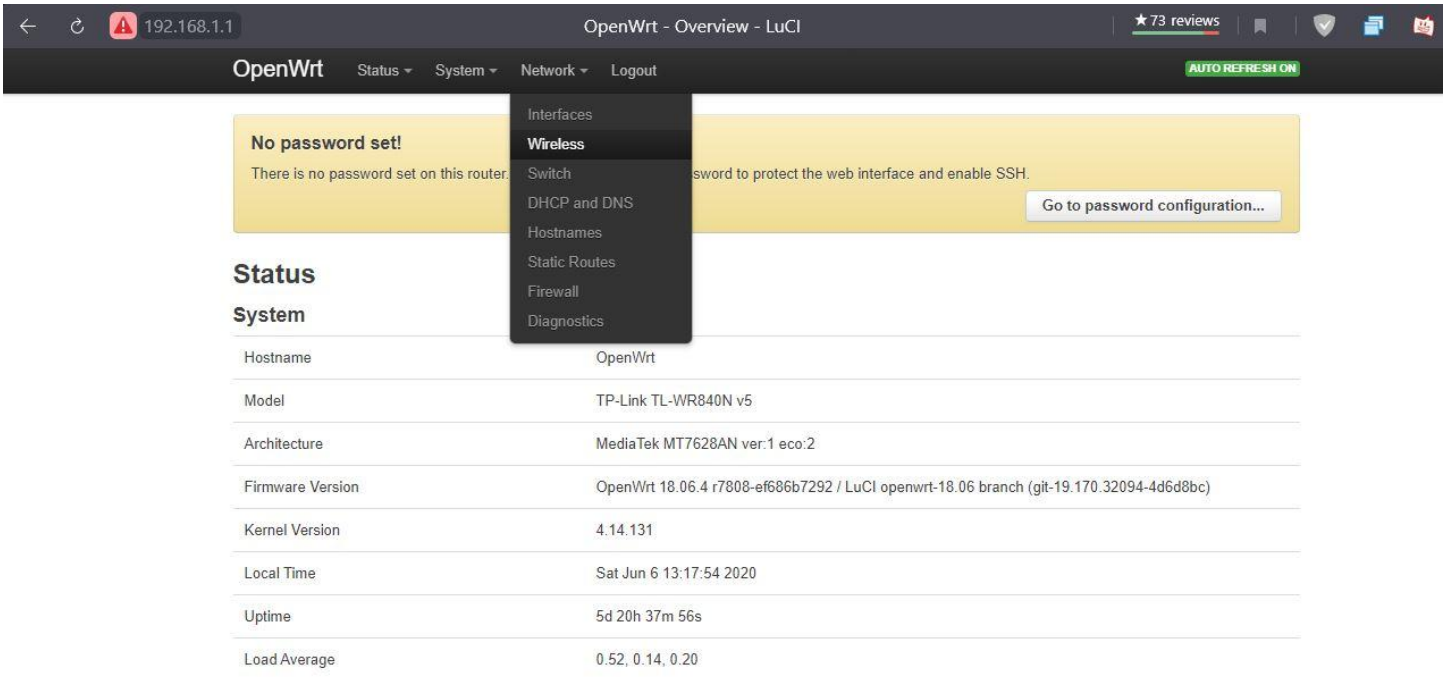
Όταν τελείωση η αναβάθμιση, το προεπιλεγμένο όνομα και κωδικός είναι root και κενό αντίστοιχα. Μόλις ενωθούμε στην γραφική διπροσωπία του OpenWRT θα δούμε στην αρχική σελίδα διάφορες πληροφορίες όπως την kernel έκδοση και την διαθέσιμη μνήμη. Η μνήμη είναι σημαντική γιατί εκεί θα αποθηκεύονται τα διάφορα προγράμματα που θα χρειαστούμε για να μπορέσουμε να μετατρέψουμε των κόμβο σε λειτουργισμό sniffer. (βλέπε εικόνα 3.5.4).



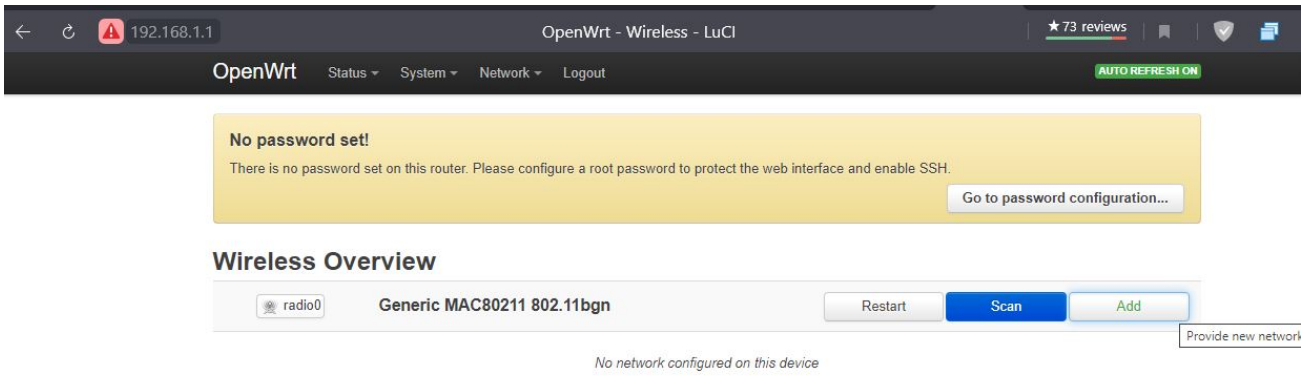
Εικόνα 3.5.4

Όπως αναφέραμε και στο υπό-κεφάλαιο 3.3 για οποιοδήποτε λειτουργικό σύστημα κάθε wifi κάρτα που έχει αντένες για λήψη και αποστολή ασύρματων πακέτων και υποστηρίζει κάποια λειτουργία (όπου στην δική μας περίπτωση είναι η monitor λειτουργία) πρέπει να συσχετίζετε και με μια διπροσωπία για σκοπούς παροχής εντολών διαμέσου του πυρήνα.

Αρχικά στην ενότητα Network, στην υπό-ενότητα Wireless πατούμε το κουμπί Add για να ενεργοποιήσουμε μια νέα λειτουργία στον δρομολογητή (βλέπε εικόνα 3.5.5 και 3.5.6).

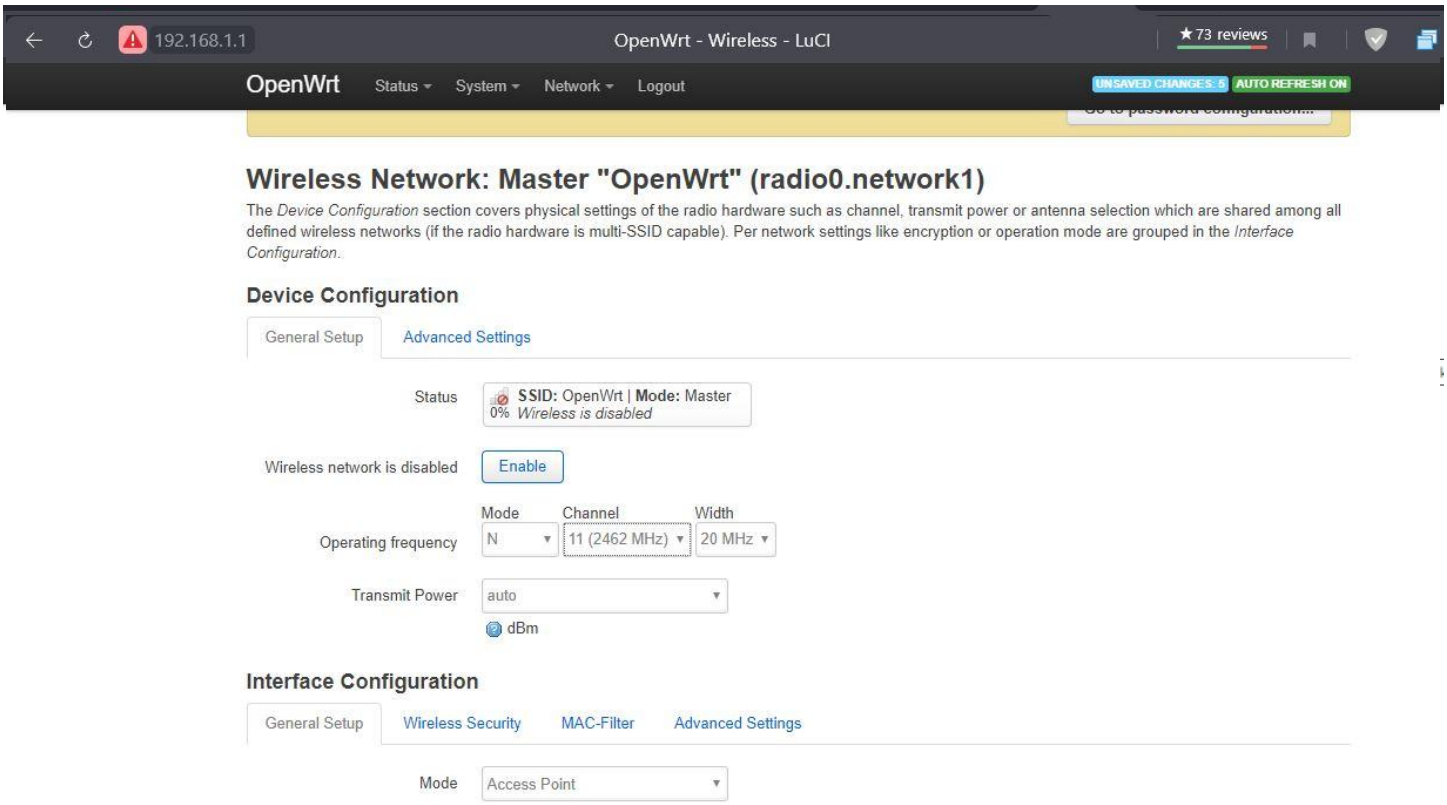


Εικόνα 3.5.5



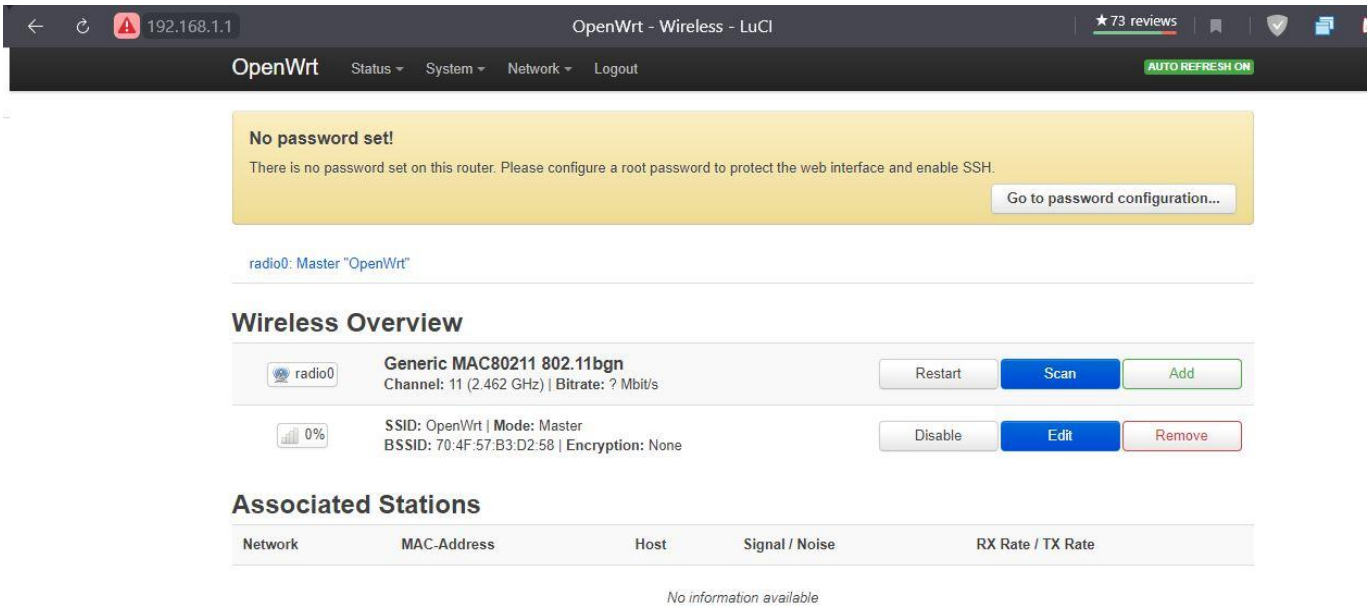
Εικόνα 3.5.6

Το επόμενο βήμα είναι να ρυθμίσουμε την λειτουργεία να είναι σε Access λειτουργία (προεπιλεγμένη λειτουργία) και να δεσμεύεται σε ποιο κανάλι (συχνότητα) να λειτουργεί. (Το αφήνουμε στην προεπιλεγμένη λειτουργία γιατί το script που ετοιμάσαμε θα το μετατρέπει αυτόματα στην monitor λειτουργία). Όταν όλα ρυθμιστούν το save κουμπί θα δημιουργήσει την λειτουργία αλλά θα είναι απενεργοποιημένη. (βλέπε εικόνα 3.5.7)



Εικόνα 3.5.7

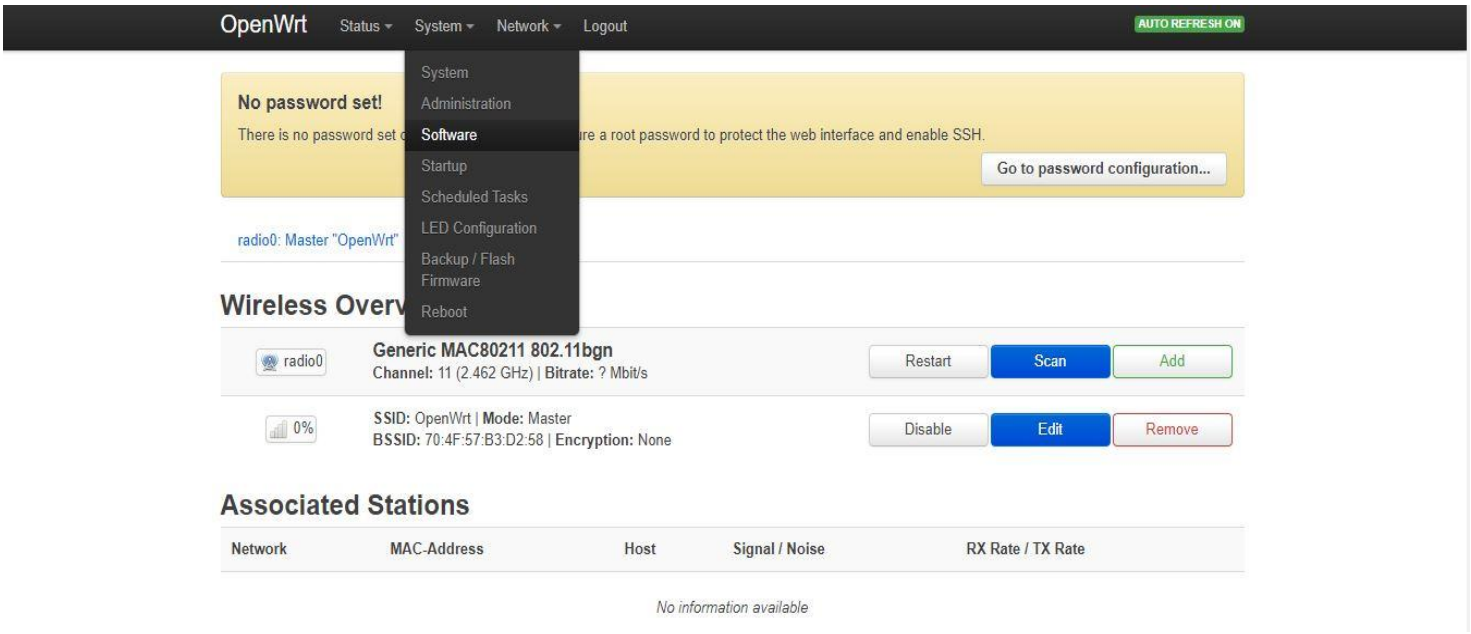
Για επιβεβαίωση της δημιουργίας του Wifi δικτύου με την λειτουργία Access Point (αλλιώς master λειτουργία) μπορούμε να ξανά επιλέξουμε την ενότητα Network, στην υπό-ενότητα Wireless. Κάτω από τον Wireless Overview βρίσκεται ο WiFi adapter (hardware) στον οποίο δημιουργήσαμε την Access Point λειτουργία και κάτω από αυτό πρέπει να εμφανίστηκε η λειτουργία μας η οποία είναι απενεργοποιημένη. Για να την ενεργοποιήσουμε πατάμε το enable κουμπί.(βλέπε εικόνα 3.5.8). Σε αυτή την φάση μπορεί να ενεργοποιήθηκε η λειτουργία (του έχει καταχωρηθεί SSID και BSSID) αλλά είναι ανενεργή (δηλαδή δεν άρχισε η συλλογή πακέτων)



Εικόνα 3.5.8

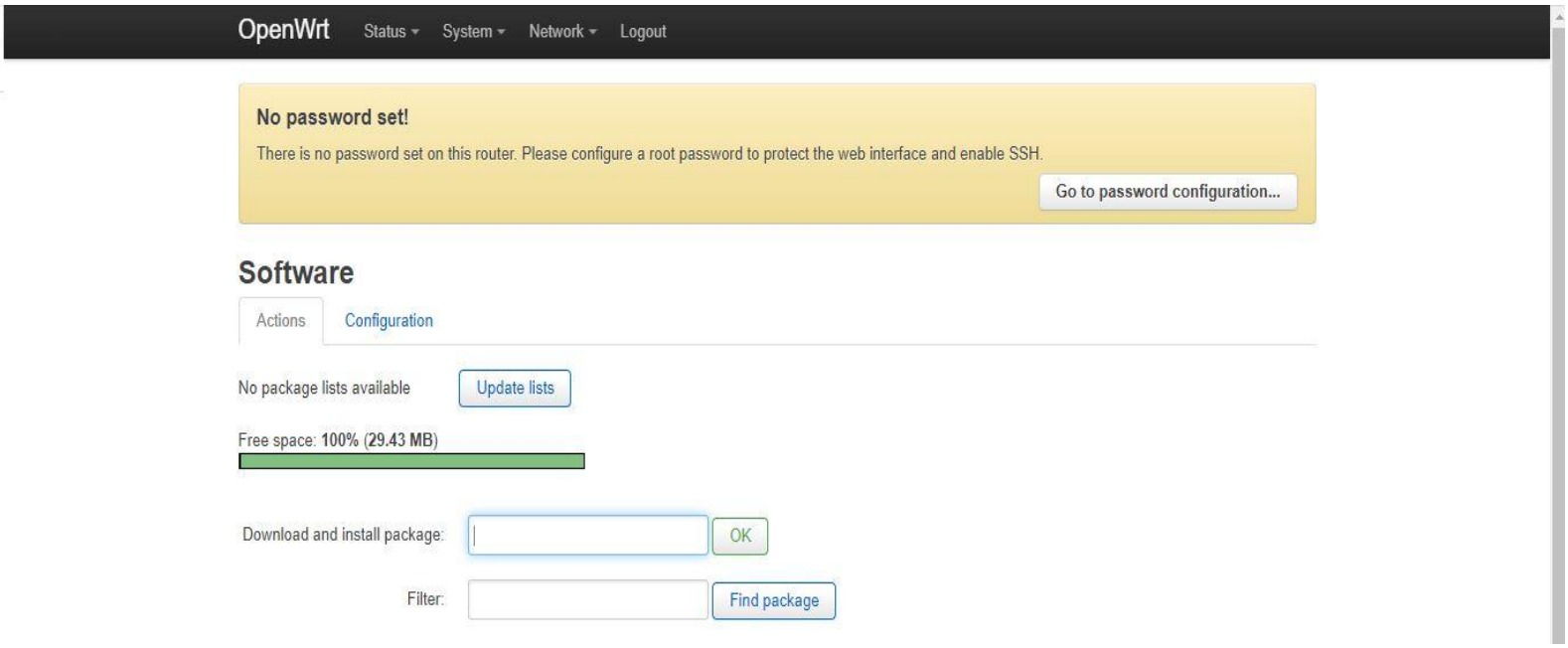
Για να μπορέσουμε να αλλάξουμε την λειτουργία του κόμβου μας και για να αρχίσουμε να δίνουμε εντολές για συλλογή και αποθήκευση πακέτων σε pcap αρχεία πρέπει να εγκαταστήσουμε κάποια προγράμματα τα οποία θα εκτελούνται μέσω της γραμμής εντολών.

Τα διαθέσιμα λογισμικά βρίσκονται στην κατηγορία System, υποκατηγορία Software. (βλέπε εικόνα 3.5.9)



Εικόνα 3.5.9

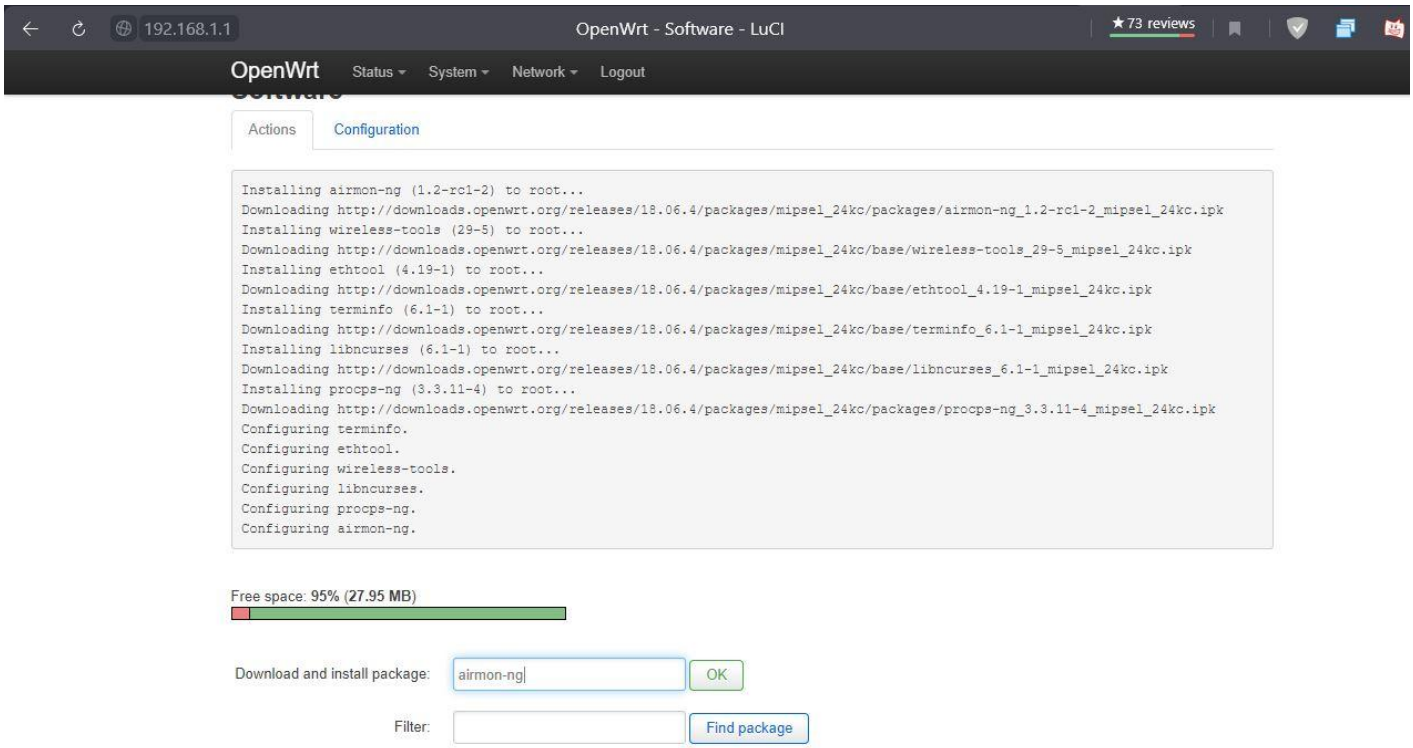
Το OpenWRT έχει είδη αποθετήρια πακέτων (το σύστημα του είναι όπως τα Linux) γι' αυτό πριν να την λήψη των προγραμμάτων χρειάζεται η αναβάθμιση των πακέτων (πατήματος Update lists κουμπιού) για μπορέσουμε να κατεβάσουμε τις τελευταίες εκδόσεις των προγραμμάτων που χρειαζόμαστε. (βλέπε εικόνα 3.5.10)



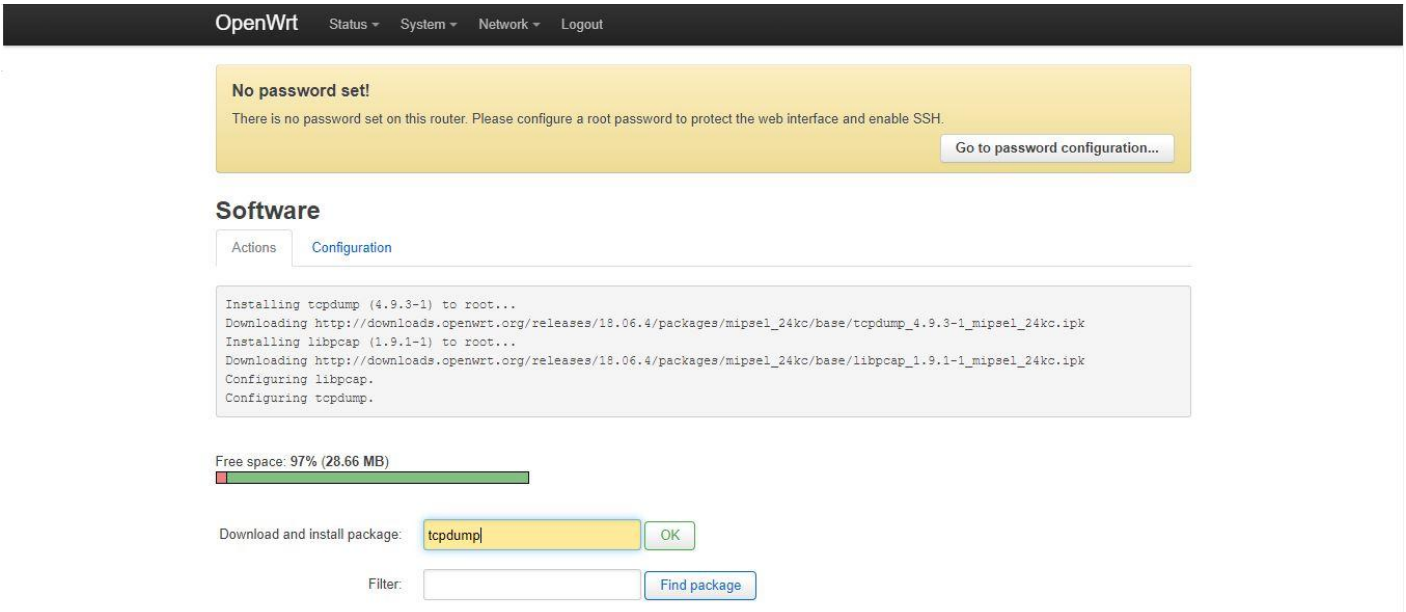
Εικόνα 3.5.10

Αφού αναβαθμιστούν τα αποθετήρια μπορούμε να κατεβάσουμε τα προγράμματα που θέλουμε. Το πρώτο είναι το airmon-ng (βλέπε εικόνα 3.5.11) το οποίο θα μετατρέψει την παρόν λειτουργία σε monitor λειτουργία και το δεύτερο πρόγραμμα είναι το tcpdump (βλέπε εικόνα 3.5.12) το

οποίο μέσω τις διπροσωπίας που σχετίζεται με την wifi λειτουργία μας θα ελέγχει την συλλογή των πακέτων. (ουσιαστικά το πρόγραμμα είναι ο διακόπτης της λειτουργίας από ενεργεί σε ανενεργή και το αντίθετο)



Εικόνα 3.5.11



Εικόνα 3.5.12

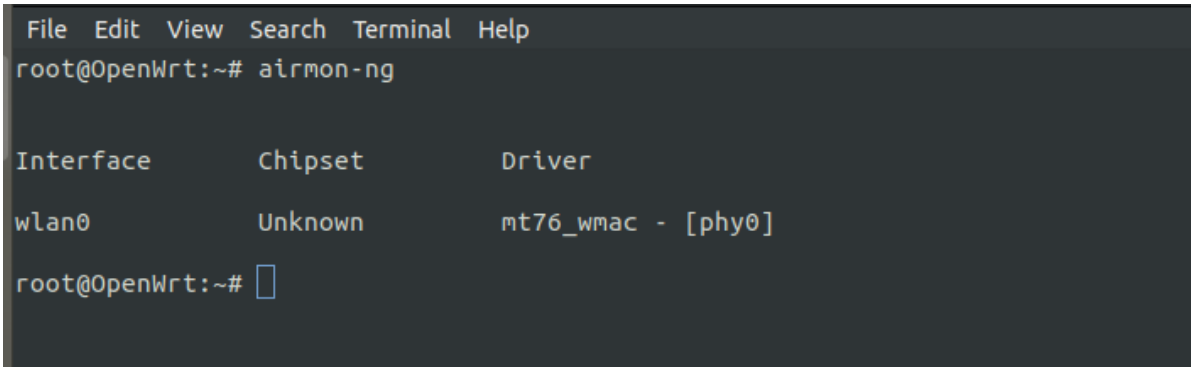
Σε αυτό το σημείο όλες οι διαρρυθμίσεις έχουν τελείωση. Μένη μόνο να δημιουργήσουμε ssh σύνδεση από τον κεντρικό υπολογιστικό σύστημα και να τρέξουμε το τα δύο προγράμματα. Αν

δεν γίνει καμία αλλαγή στις ρυθμίσεις του adapter τότε το airmon-ng θα χρειαστεί να το τρέξουμε μόνο στην αρχή ενώ το tcpdump θα το τρέχουμε κάθε φορά που θα θέλουμε να συλλέγουμε ασύρματα πακέτα.

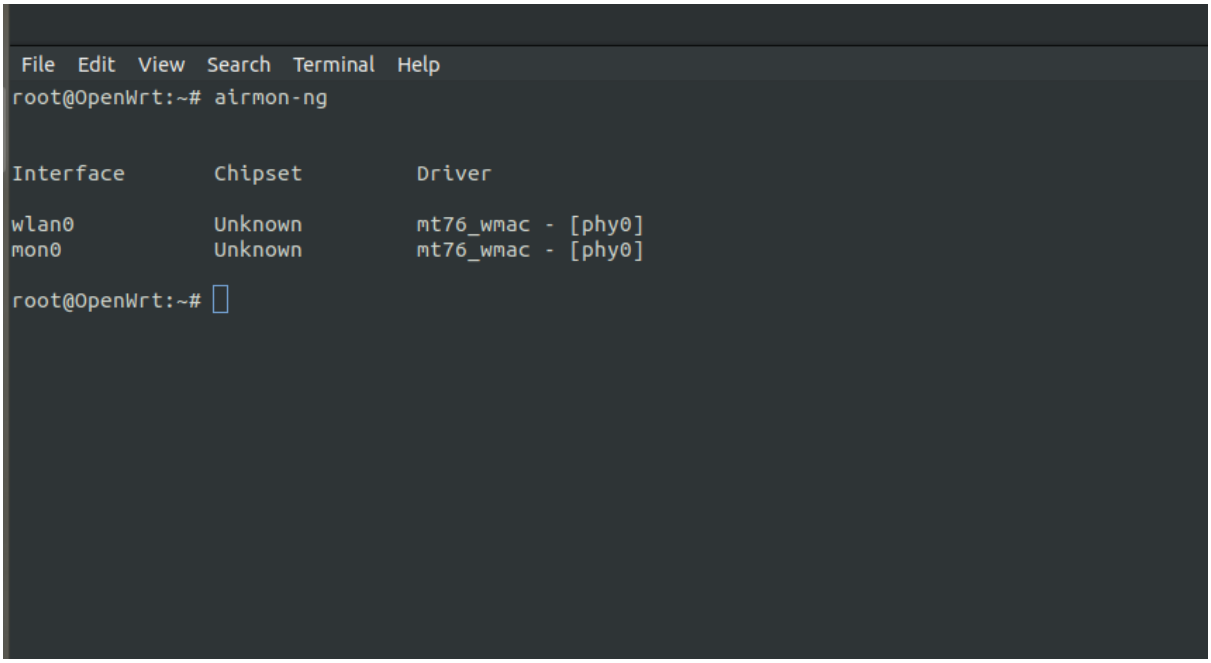
Το airmon-ng αν τρέξει χωρίς παραμέτρους θα μας εκτυπώσει τις διαθέσιμες Ασύρματες διπροσωπίες. (βλέπε εικόνα 3.5.13) Η δική μας είναι η wlan0 επομένως για να την ρυθμίσουμε στην monitor λειτουργία τρέχουμε airmon-ng start wlan0. (βλέπε εικόνα 3.5.14) Αν το πρόγραμμα τερματίσει με επιτυχία τότε μια νέα διπροσωπία θα δημιουργήσει (που στην δική μας περίπτωση έχει το όνομα) που θα συσχετίζετε με την Monitor λειτουργία. Αυτό μπορεί να επαληθευτή τρέχοντας την εντολή airmon-ng χωρίς παραμέτρους (βλέπε εικόνα 3.5.15)

```
File  Edit  View  Search  Terminal  Help
root@OpenWrt:~# airmon-ng start wlan0
ps: unrecognized option: A
BusyBox v1.28.4 () multi-call binary.

Usage: ps

Show list of processes

        w       Wide output
ps: unrecognized option: a
BusyBox v1.28.4 () multi-call binary.

Usage: ps

Show list of processes

        w       Wide output


Interface       Chipset         Driver

wlan0           Unknown         mt76_wmac - [phy0]
                                (monitor mode enabled on mon0)

root@OpenWrt:~#
```

Εικόνα 3.5.14

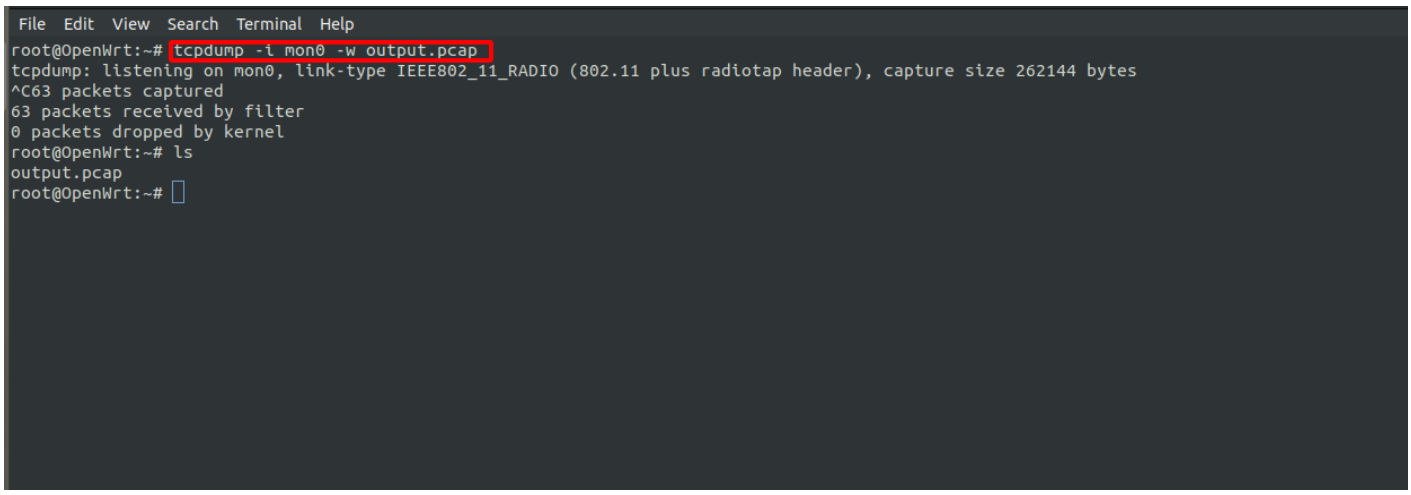


Εικόνα 3.5.13



Εικόνα 3.5.15

Στο tcpdump μετά το -i ακολουθεί το όνομα της διπροσωπίας που θέλουμε να συλλέγονται τα πακέτα και μετά το -w το όνομα του pcap αρχείου που δημιουργείται στο τέλος του προγράμματος (βλέπε εικόνα 3.5.16)


File Edit View Search Terminal Help
root@OpenWrt:~# tcpdump -i mon0 -w output.pcap
tcpdump: listening on mon0, link-type IEEE802_11_RADIO (802.11 plus radiotap header), capture size 262144 bytes
^C63 packets captured
63 packets received by filter
0 packets dropped by kernel
root@OpenWrt:~# ls
output.pcap
root@OpenWrt:~#

Εικόνα 3.5.16

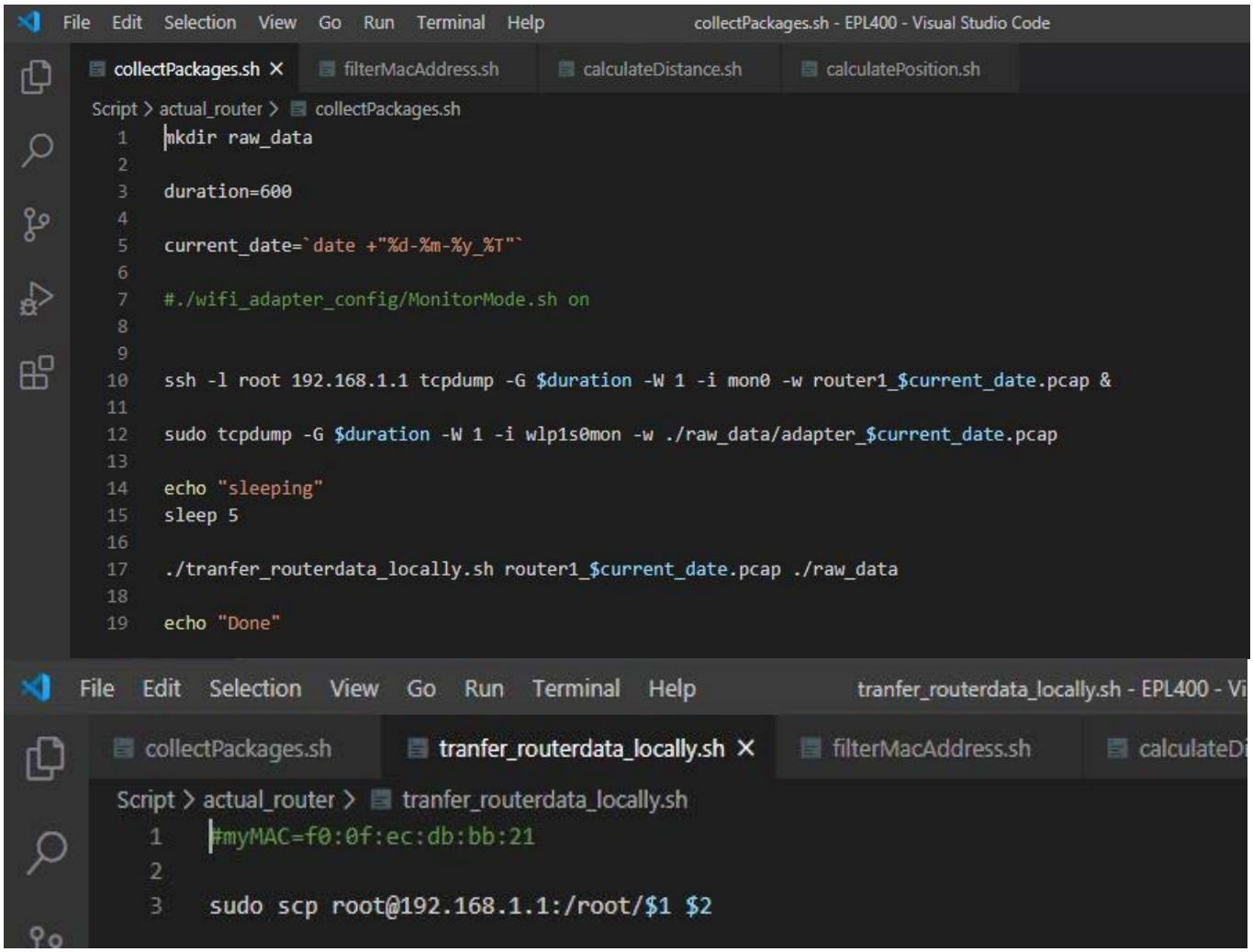
Κεφάλαιο 4

Κεντρικοποιημένο Σύστημα

4.1 Linux Αρχεία εντολών

4.1 Linux Αρχεία εντολών

Το υπολογιστικό μέρος χρησιμοποιεί python προγράμματα και το tshark για γρήγορο και ποιο αποδοτικό φιλτράρισμα του αρχείου. Γι' αυτό το σύστημα χρησιμοποιεί Bash Αρχεία εντολών για των συντονισμό των διάφορων φάσεων. (συλλογή, φιλτράρισμα, υπολογισμός, εξαγωγή αποτελεσμάτων)



Εικόνα 4.1.1

Στο πείραμα μου έχω χρησιμοποίηση τα δεδομένα από την Wi-Fi κάρτα του Laptop μου και από το Tp-link δρομολογητή μου.

Μετά την πρώτη φάση της συλλογής δηλαδή αφότου τελειώσουν τα πρώτα X λεπτά (όπου το X είναι ο χρόνος της φάσης μεταξύ της συλλογής των πακέτων και την δημιουργία pcap αρχείου) τότε το script μας ενεργοποιείται και αρχίζει να συλλέγει τα pcap αρχεία από όλους τους κόμβους και θα τα συγκεντρώνει σε ένα κεντρικό υπολογιστικό σύστημα.

Στις γραμμές 10 και 12 στέλνουμε το σήμα στους δυο μας κόμβους να αρχίσουν την συλλογή των πακέτων για 600 δευτερόλεπτα (η τιμή βρίσκεται στην μεταβλητή duration). (βλέπε εικόνα 4.1.1)

Εκτελούμε την γραμμή 10 στο παρασκήνιο και την γραμμή 12 κανονικά έτσι ώστε να εκτελούνται παράλληλα. Ήταν μια τεχνική για σκοπούς συγχρονισμού συλλογής για όλους τους κόμβους. Μόλις τελείωση ο τελευταίος κόμβος το script θα ξεκολλήσει από την γραμμή 12 αλλά επειδή δεν ξέρουμε αν ο πρώτος κόμβος έχει τελείωση, βασικά του έχουμε βάλει και εκείνου το ίδιο duration αλλά για κάποιο λόγο (π.χ. I/O καθυστερήσεις του firmware) μπορεί να του πάρει λίγο περισσότερο χρόνο. Γι' αυτό στην γραμμή 15 κάνω παύση το script για 5 δευτερόλεπτα για να είμαι σίγουρος ότι ο κάθε κόμβος έχει δημιουργήσει το pcap αρχείο του. Τέλος κάνω secure copy όλα τα pcap αρχεία του κάθε κόμβου στο κεντρικό υπολογιστή.

Επειδή κάθε pcap file θα έχει πάρα πολλά πακέτα από διαφορετικά MAC addresses (ουσιαστικά διαφορετικές συσκευες) θα πρέπει με κάποιο τρόπο να τα φιλτράρουμε όλα. Η διαδικασία είναι να βρούμε όλα τα διαφορετικά μοναδικά MAC σε ένα αρχείο και να τα αποθηκευσουμε σε μορφή λίστας. Από εκεί θα πάρουμε ένα ένα την φορά και θα κάνουμε τις επέμενες διαδικασίες (φιλτραρισμα βάση του επιλεγόμενου MAC, μετατροπή dB σε μέτρα και υπολογισμό της θέσης της συσκευής μέσα στο χώρο).

Το στάδιο του φιλτραρίσματος αρχικά το έκανα με python script και μόνο για ένα MAC address ενός pcap αρχείου το οποίο δημιουργήθηκε από τον κόμβο συλλέγοντας πακέτα για 10 λεπτά του πήρε 4 ολόκληρα λεπτά. Αυτό σημαίνει ότι όταν μεγαλώσει η πυκνότητα τον ατόμων στο χώρο ,δηλαδή να έχουμε να διαχειριστούμε δεκάδες από MAC το προγραμμα μας θα καθυστερεί πάρα πολύ να τελειώσει με αποτέλεσμα να έρχεται η επόμενη σειρα από pcap αρχεία αλλά εμείς να μην έχουμε τελειώσει ακόμα την προηγούμενη.

Η δεύτερη προσπάθεια έχει γίνει με το tshark πρόγραμμα. Εδώ το φιλτράρισμα γίνεται μέσα σε λίγα δευτερόλεπτα. Παρατηρούμε τεράστια διαφορά μεταξύ της προηγούμενη προσπάθειας.

Κεφάλαιο 5

Υπολογιστικό Μέρος Συστήματος

5.1 Φόρμουλα μετατροπή dBm σε m
5.2 Python Πρόγραμμα υπολογισμού απόστασης
5.3 Python Πρόγραμμα υπολογισμού συντεταγμένων σημείων

5.1 Φόρμουλα μετατροπή dBm σε m

Η δύναμη του σήματος εκφράζεται συνήθως και μετριέται σε ντεσιμπέλ (dB) με αναφορά milliwatt ή dBm. Ένα ντεσιμπέλ είναι μια λογαριθμική μονάδα που είναι ένας λόγος της ισχύος του συστήματος προς κάποια αναφορά. Τα dBm είναι η ισχύς εξόδου σε ντεσιμπέλ που αναφέρεται σε 1 mW. [4]

Δεδομένου ότι το dBm βασίζεται σε λογαριθμική κλίμακα σημαίνει ότι για κάθε αύξηση 3 dBm υπάρχει περίπου διπλάσια ισχύ εξόδου και κάθε αύξηση 10 dBm αντιπροσωπεύει δεκαπλάσια αύξηση ισχύος. 10 dBm (10 mW) είναι 10 φορές ισχυρότερο από 0 dBm (1 mW) και 20 dBm (100 mW) είναι 10 φορές πιο ισχυρό από 10 dBm. [4]

Μπορούμε να μετατρέψετε μεταξύ mW και dBm χρησιμοποιώντας τους ακόλουθο τύπο:

$P(dBm) = 10 \cdot \log10(P(mW))$
$P(mW) = 10(P(dBm)/10)$

Το επόμενο βήμα είναι να υπολογίσουμε το Path Loss. Το Path Loss είναι η μείωση της ισχύος ενός ραδιοκύματος που διανύει μια απόσταση. Κάθε φορά που διπλασιάζουμε την απόσταση, λαμβάνουμε μόνο το ένα τέταρτο της ισχύος. Αυτό σημαίνει ότι κάθε αύξηση 6 dBm στην ισχύ εξόδου διπλασιάζει την πιθανή απόσταση που μπορεί να επιτευχθεί. [4]

Εκτός από την ισχύ του πομπού, ένας άλλος παράγοντας που επηρεάζει το εύρος είναι η ευαισθησία του δέκτη. Συνήθως εκφράζεται σε -dBm. Δεδομένου ότι τόσο η ισχύς εξόδου όσο και η ευαισθησία του δέκτη αναφέρονται σε dBm, μπορούμε να χρησιμοποιήσουμε απλή

προσθήκη και αφαίρεση για να υπολογίσετε τη μέγιστη απώλεια διαδρομής που μπορεί να υποστεί ένα σύστημα:

Maximum path loss = transmit power – receiver sensitivity + gains – losses

Όπου transmit power είναι η ισχύς του πακέτου όταν φεύγει από την συσκευή, receiver sensitivity είναι η ισχύς του πακέτου όταν φτάσει στον κόμβο, gains τα τυχών gains από την ίδια την αντένα και losses είναι η εξασθένηση του σήματος.

Λόγο του ότι στον δεν έχουμε ιδανικό περιβάλλον, το σήμα μας μπορεί να αλλοιωθεί από αυτό. (π.χ. εμπόδια, τοίχοι) Γι' αυτό το λόγο μπαίνει άλλη μια παράμετρος, το fade margin όπου προσομοιώνει την ισχύ που χάθηκε από του προαναφερθέντες λόγους. [4]

Οπότε ο τύπος μας γίνετε:
Maximum path loss = transmit power – receiver sensitivity + gains – losses – fade margin

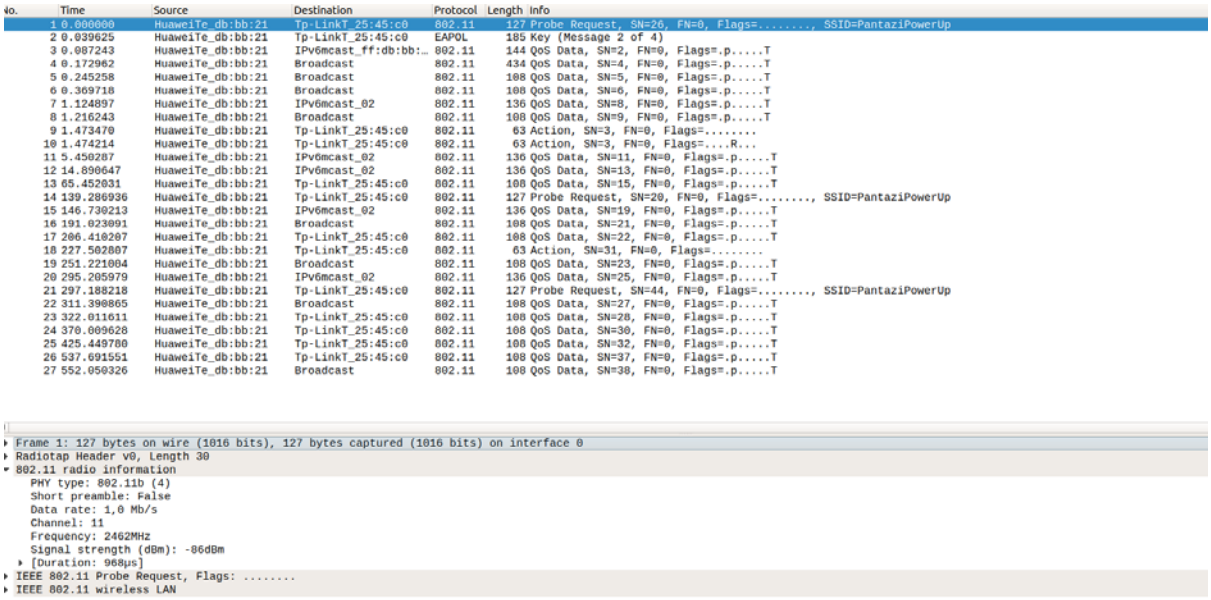
Ο τελικός τύπος τις απόστασης είναι:

$$\text{Distance (km)} = 10^{(\text{maximum path loss} - \text{FSPL} - 20\log(f))/20}$$

Όπου f είναι η συχνότητα που μεταφέρθηκε το πακέτο (κανάλι) και FSPL (Free-Space Path Loss) προσαρμοσμένη σταθερά μέσου όρου ανάλογα με το περιβάλλον. Ουσιαστικά είναι η εξασθένιση της ενέργειας του πακέτου μεταξύ των σημείων τροφοδοσίας και σημείων λήψης χωρίς εμπόδια μέσω του ελεύθερου χώρου (συνήθως αέρα). [4]

5.2 Python Πρόγραμμα υπολογισμού απόστασης

Σε αυτό το στάδιο μετατρέπουμε το pcap αρχείο (βλέπε εικόνα 5.2.1) που περιέχει πακέτα μιας συσκευή σε ένα αρχείο με υπολογισμένες τις φυσικές αποστάσεις. Συγκεκριμένα από κάθε πακέτο θα παίρνουμε 4 πληροφορίες. Οι πρώτες δύο είναι τα dBm ντεσιμπέλ (δύναμη του σήματος μόλις συλλεκτικέ το πακέτο από τον κόμβο) και το κανάλι στο οποίο μεταφέρθηκε το πακέτο.



Εικόνα 5.2.1

Όπως βλέπουμε τον τύπο για την μετατροπή της δύναμης του σήματος σε μέτρα (εικόνα 5.2.2) (γραμμή 16) αρχικά ξέρουμε την δύναμη του πακέτου που φεύγει από την συσκευή (trasmits =10 ντεσιμπέλ όπου 10 είναι ο μέσος όρος των περισσότερων smartphones) πλην την δύναμη του σήματος που έλαβε ο κόμβος. Με αυτή την πράξει βρίσκουμε πόση ενέργεια χάθηκε στο ενδιάμεσο.

```
7
8   def dbm_to_meters(receiver_sesnsitivity, frequency):
9
10      # dBm
11      trasmits = 10
12      gains = 0
13      losses = 15
14      fade_margin = 12
15
16      path_lost = trasmits - receiver_sesnsitivity + gains - losses - fade_margin
17
18      ekthetis = (path_lost -  20*math.log(frequency, 10)) / 20
19
20      return math.pow(10, ekthetis)
21
```

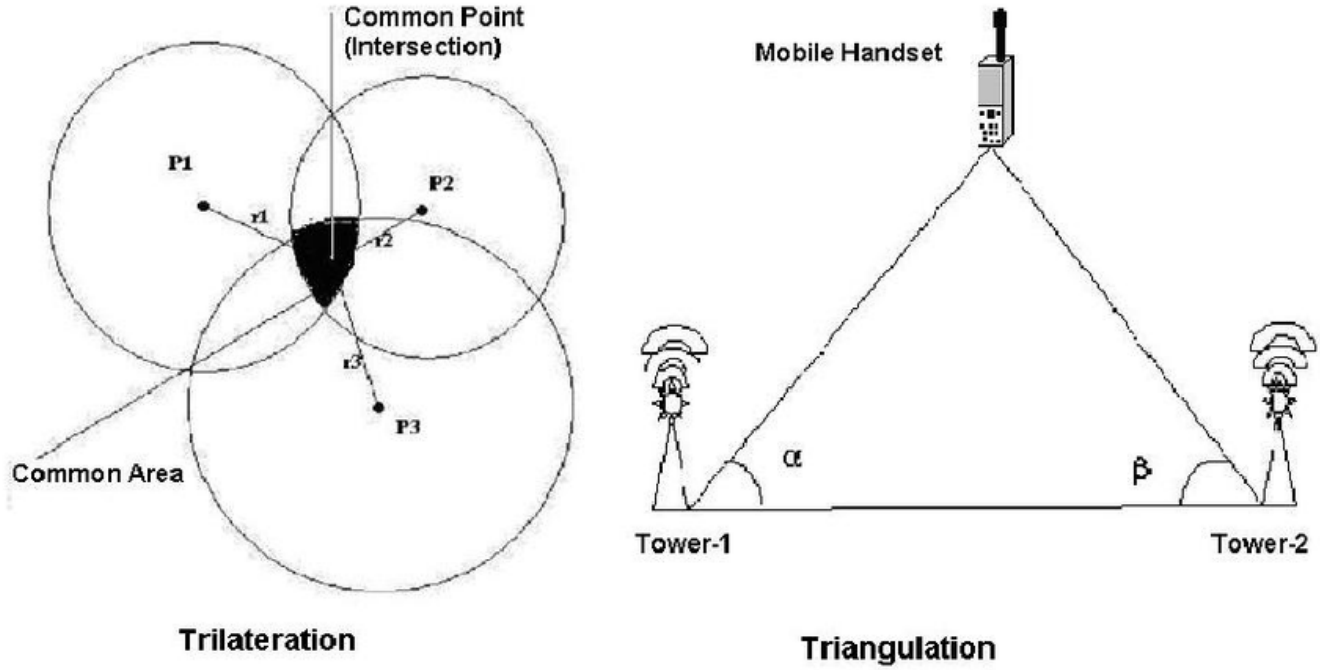
Εικόνα 5.2.2

Οι άλλες μεταβλητές (gain, losses και Fade Margin) πρέπει να μπουν ανάλογα με τον φυσικό χώρο και τα τριγύρω εμπόδια στα οποία βρίσκονται οι κόμβοι. Αν για παράδειγμα υπάρχουν τοίχοι ή εμπόδια μεταξύ των κόμβων τότε θα υπάρχει πολύ Loss σε ενέργεια από εξωτερικούς παράγοντες. Αυτό το βρίσκουμε με την μέθοδο trial and error ώσπου να βρούμε τις ανάλογες τιμές.

Τέλος στην φόρμουλα μπαίνει και η συχνότητα που έχει ταξιδέψει το πακέτο, δηλαδή από πιο κανάλι στάλθηκε. Η φόρμουλα εξάγει την απόσταση σε μέτρα μεταξύ συσκευής και κόμβου.

5.3 Python Πρόγραμμα υπολογισμού συντεταγμένων σημείων

Στο τελευταίο στάδιο αφού έχουμε την φυσική απόσταση της συσκευής από τον κόμβο, θα πάρουμε το ίδιο πακέτο από τουλάχιστον 3 κόμβους. (αυτό θα μας το δείξει το timestamp, ίδιο timestamp σημαίνει ότι είναι το ίδιο πακέτο). Αυτό μας δίνει την δυνατότητα να δημιουργήσουμε 3 νοητούς κύκλους. Όπου κέντρο είναι η γεωγραφικές συντεταγμένες του κύβου στο χώρο και ακτίνα η απόσταση της συσκευής από το κόμβο. Με αυτές τις πληροφορίες μπορούμε προγραμματιστικά να υπολογίσουμε το σημείο τομής των τριών κύκλων (βλέπε εικόνα 5.3.1). Αυτό θα μας δώσει το αποτέλεσμα που θέλουμε, δηλαδή το σημείο της συσκευής που έστειλε το συγκεκριμένο πακέτο την συγκεκριμένη χρονική στιγμή. Αυτή η διαδικασία θα επαναληφθεί για όλα τα διαθέσιμα πακέτα που διαλέξαμε.[13]



Βλέπε εικόνα 5.3.1 [12]

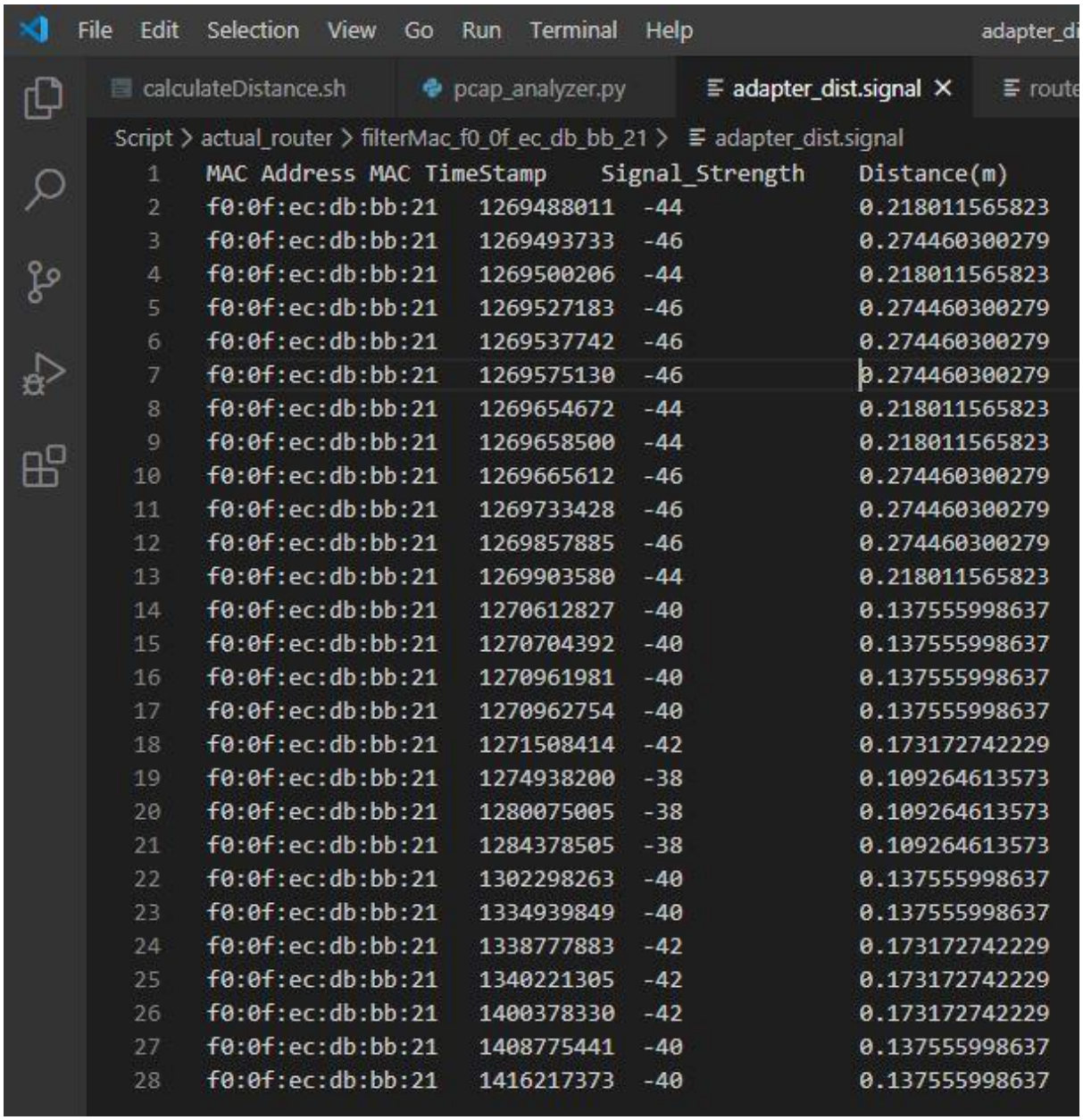
Κεφάλαιο 6

Παρουσίαση αποτελεσμάτων

---

6 Παρουσίαση αποτελεσμάτων

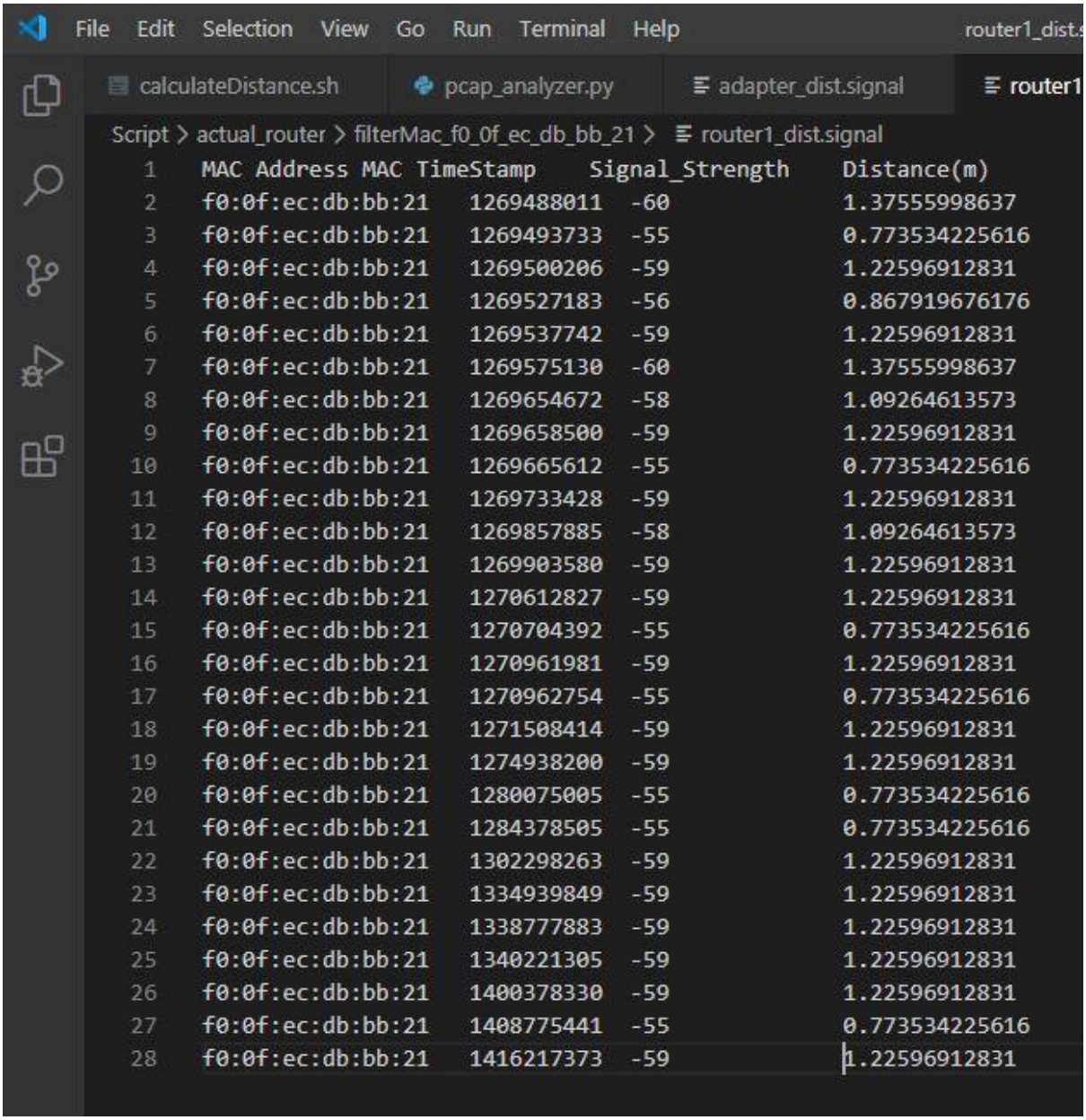
Στάδιο υπολογισμού απόστασης από πακέτα που συλλέχτηκαν από την Wi-Fi κάρτα του Laptop μου (βλέπε εικόνα 6.1)



	MAC Address	MAC TimeStamp	Signal_Strength	Distance(m)
2	f0:0f:ec:db:bb:21	1269488011	-44	0.218011565823
3	f0:0f:ec:db:bb:21	1269493733	-46	0.274460300279
4	f0:0f:ec:db:bb:21	1269500206	-44	0.218011565823
5	f0:0f:ec:db:bb:21	1269527183	-46	0.274460300279
6	f0:0f:ec:db:bb:21	1269537742	-46	0.274460300279
7	f0:0f:ec:db:bb:21	1269575130	-46	0.274460300279
8	f0:0f:ec:db:bb:21	1269654672	-44	0.218011565823
9	f0:0f:ec:db:bb:21	1269658500	-44	0.218011565823
10	f0:0f:ec:db:bb:21	1269665612	-46	0.274460300279
11	f0:0f:ec:db:bb:21	1269733428	-46	0.274460300279
12	f0:0f:ec:db:bb:21	1269857885	-46	0.274460300279
13	f0:0f:ec:db:bb:21	1269903580	-44	0.218011565823
14	f0:0f:ec:db:bb:21	1270612827	-40	0.137555998637
15	f0:0f:ec:db:bb:21	1270704392	-40	0.137555998637
16	f0:0f:ec:db:bb:21	1270961981	-40	0.137555998637
17	f0:0f:ec:db:bb:21	1270962754	-40	0.137555998637
18	f0:0f:ec:db:bb:21	1271508414	-42	0.173172742229
19	f0:0f:ec:db:bb:21	1274938200	-38	0.109264613573
20	f0:0f:ec:db:bb:21	1280075005	-38	0.109264613573
21	f0:0f:ec:db:bb:21	1284378505	-38	0.109264613573
22	f0:0f:ec:db:bb:21	1302298263	-40	0.137555998637
23	f0:0f:ec:db:bb:21	1334939849	-40	0.137555998637
24	f0:0f:ec:db:bb:21	1338777883	-42	0.173172742229
25	f0:0f:ec:db:bb:21	1340221305	-42	0.173172742229
26	f0:0f:ec:db:bb:21	1400378330	-42	0.173172742229
27	f0:0f:ec:db:bb:21	1408775441	-40	0.137555998637
28	f0:0f:ec:db:bb:21	1416217373	-40	0.137555998637

Εικόνα 6.1

Στάδιο υπολογισμού απόστασης από πακέτα που συλλέχτηκαν από την Tp-Link δρομολογητή με OpenWRT firmware (βλέπε εικόνα 6.2)



Εικόνα 6.2

Στο αρχείο που παράχθηκε έχουμε το MAC Address που μας δηλώνει το ID της ταυτότητας της συσκευής , το timestamp θα μας βοηθήσει στο επόμενο στάδιο να κάνουμε matchup τα ίδια πακέτα από διαφορετικούς κόμβους και τέλος έχουμε την απόσταση σε μέτρα μεταξύ κόμβου και συσκευής.

Στο πείραμα η συσκευή έχει τοποθετηθεί έτσι ώστε να είναι μεταξύ των κόμβων σε απόσταση 1 μέτρου. (βλέπε εικόνα 6.3)

Εικόνα 6.3

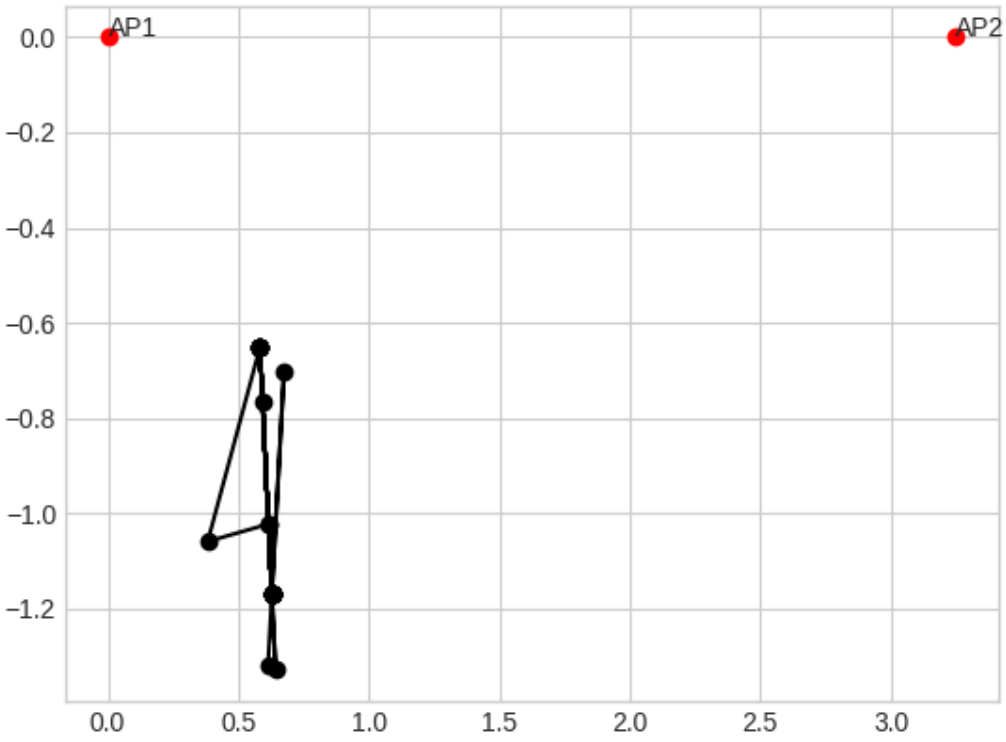
Αφού ξέρουμε την πραγματική απόσταση μεταξύ των κόμβων υπολογίστηκε το ποιο καλό αποτέλεσμα με τον τύπο: $\frac{|\,\pi\rho\alpha\gamma\mu\alpha\tau\iota\kappa\acute{\iota} - \pi\epsilon\iota\rho\alpha\mu\alpha\tau\iota\kappa\acute{\eta}\,|}{\pi\rho\alpha\gamma\mu\alpha\tau\iota\kappa\acute{\iota}}$ X 100.

Τον καλύτερο υπολογισμό τον έχει ο router με διαφορά με ποσοστό συσχέτισης 77% σε σχέση με την Wi-Fi κάρτα που έχει μόνο 19%. (βλέπε εικόνα 6.4) Αυτό ήταν αναμενόμενο καθώς ο router έχει καλύτερο hardware και μεγαλύτερες αντένες για καλύτερη διαχείριση ασύρματων πακέτων. Εξάλλου αυτή είναι η κύρια δουλειά του.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1			Router						Router				
2	ΘεωρητικήΤιμή		Πραγματική Τιμη		Ποσοστο Συσχέτησης		Μέσος Όρος Ποσοστου Συσχέτησης %		Πραγματική Τιμη		Ποσοστο Συσχέτησης		Μέσος Όρος Ποσοστου Συσχέτησης %
3	1		1.375559986		62.44400136		77.61744477		0.218011566		21.80115658		19.0081953
4			0.773534226		77.35342256				0.2744603		27.44603003		
5			1.225969128		77.40308717				0.218011566		21.80115658		
6			0.867919676		86.79196762				0.2744603		27.44603003		
7			1.225969128		77.40308717				0.2744603		27.44603003		
8			1.375559986		62.44400136				0.2744603		27.44603003		
9			1.092646136		90.73538643				0.218011566		21.80115658		
10			1.225969128		77.40308717				0.218011566		21.80115658		
11			0.773534226		77.35342256				0.2744603		27.44603003		
12			1.225969128		77.40308717				0.2744603		27.44603003		
13			1.092646136		90.73538643				0.2744603		27.44603003		
14			1.225969128		77.40308717				0.218011566		21.80115658		
15			1.225969128		77.40308717				0.137555999		13.75559986		
16			0.773534226		77.35342256				0.137555999		13.75559986		
17			1.225969128		77.40308717				0.137555999		13.75559986		
18			0.773534226		77.35342256				0.137555999		13.75559986		
19			1.225969128		77.40308717				0.173172742		17.31727422		

Εικόνα 6.4

Από τις συντεταγμένες και με την βοήθεια βιβλιοθηκών python εξήγαγα την γραφική για την κίνηση της συσκευής που μελετήσαμε. (βλέπε εικόνα 6.5) Παρατηρούμε ότι παρόλο που η πραγματική κινητική κατάσταση της συσκευή ήταν 0 δηλαδή ήταν ακίνητη καθόλη την διάρκεια του πειράματος, η γραφική παράσταση δείχνει ότι η συσκευή έχει μικρές κινητικές δραστηριότητες της τάξεως του μισού μέτρου. Αυτό η αλήθεια ήταν αναμενόμενο γιατί το RSSI δεν είναι και η πιο αξιόπιστη πηγή πληροφορίας. Παρόλα Αυτά δεν μας επηρεάζει αυτή η αστάθεια καθώς ο σκοπός μας είναι να βρούμε την κίνηση της διαδρομής μιας συσκευής και γενικά την κατεύθυνση που κινείται στο χώρο μεγάλων διαστάσεων. Άρα πολύ απλά μπορούμε να θέσουμε κάποια μικρή μεταβολή της κίνησης σαν κάποιου είδους παρεμβολή ή σφάλματος για να πούμε ότι η συσκευή είναι ακίνητη. Αν η μεταβολή της κίνησης είναι πιο μεγάλη από αυτή που ορίσαμε τότε θεωρούμε ότι η συσκευή κινείται σε μια κατεύθυνση



Εικόνα 6.5

Κεφάλαιο 7 Συμπεράσματα

Εν κατακλείδα το σύστημα μας μπορεί να φέρει εις πέρας τις απαιτήσεις του προβλήματος κάτω από συγκεκριμένες προϋποθέσεις. Στην δική μου περίπτωση που πείρα τις μετρήσεις είχα τον δρομολογητή μου να συλλέγει παθητικά δεδομένα και είχα ένα άλλο δρομολογητή να έχει το ρόλο του AP όπου παρείχε ασύρματο δίκτυο για να ενωθεί η συσκευή μου στο διαδίκτυο. Σε μεγάλους χώρους όπως εμπορικά δεν θα έχουν μόνο AP στον χώρο αλλά είναι πιο λογικό να έχουν και Wifi Repeaters. Η λειτουργία ενός Repeater είναι να παίρνει ασύρματα πακέτα και να τα κάνει ξαναστείλει. Ουσιαστικά να τους δίνει ενέργεια για να μπορέσουν να καλύψουν περισσότερη απόσταση. Δυστυχώς στην δική μας περίπτωση το σύστημα μας θα πράξει λάθος δεδομένα σχετικά με την απόσταση της Συσκευής. Για παράδειγμα το κινητό μου στέλνει ένα πακέτο με αρχική δύναμη σήματος 10 και καταλήγει στον κόμβο μου με ενέργεια 4. Επομένως ξέρω ότι έχουν χαθεί 6 μονάδες ενέργειας και βάση της φόρμουλας μετατροπής η συσκευή βρίσκεται χ μέτρα από τον κόμβο. Αν τώρα η συσκευή και ο κόμβος βρίσκονται σε μεγαλύτερη απόσταση και μεταξύ τους έχουμε δύο repeaters και το σενάριο έχει ως εξής. Το κινητό μου στέλνει ένα πακέτο με αρχική δύναμη σήματος 10 και καταλήγει στον πρώτο repeater με δύναμη 4. Ο repeater δίνει ενέργεια στο πακέτο και την παίρνει πάλι σε 10. Στην συνέχεια το πακέτο διανύει και άλλη απόσταση και καταλήγει στον δεύτερο repeater με δύναμη 4. Ο repeater δίνει και αυτός με την σειρά του ενέργεια στο πακέτο και την παίρνει και πάλι σε 10.Τέλως το πακέτο διανύει και άλλη απόσταση και καταλήγει στον κόμβο μου με ενέργεια 4. Ασχέτως όλης αυτής της διαδικασίας ο κόμβος βλέπει μόνο ότι το έχουν χαθεί 6 μονάδες ενέργειας και βάση της φόρμουλας μετατροπής η συσκευή βρίσκεται χ μέτρα από τον κόμβο ενώ στην πραγματικότητα απέχει 3 φορές χ μέτρα.

Μια πιθανή λύση είναι οι κόμβοι να τοποθετηθούν στο ίδιο σημείο που υπάρχουν οι repeaters αλλά δεν ξέρουμε αυτό αν θα δουλέψει. Πρέπει να το δούμε στην πράξη.

Άλλη μια παρατήρηση για την φόρμουλα μετατροπής. Υπάρχει και η δυνατότητα ενσωμάτωσης και του παράγοντα της υγρασίας (από τι φαίνεται επηρεάζει την δύναμη του σήματος). Επομένως μια μελλοντική αναβάθμιση θα μπορούσε να είναι η εφαρμογή αισθητήρων υγρασίας για πιθανών μεγαλύτερη ακρίβεια στην μετατροπή ενέργειας σήματος σε απόσταση.

Τέλος θα ήταν καλό αφού υπάρχει η βασική αρχιτεκτονική και το σύστημα να στηθούν 3 συμβατοί δρομολογητές με OpenWRT σε φυσικές απόστασης μεγάλων δωματίων και να αρχίσουν να συλλέγουν πειραματικά δεδομένα. Αυτό θα μας δώσει καλύτερα στατιστικά για να δούμε αν πράγματι οι πληροφορίες που παράγει είναι ακριβείς σε ρεαλιστικά σενάρια.

Βιβλιογραφία

[1] H. M. Ali, A. Busson, and V. Vèque, “Network layer link management using signal strength for ad-hoc networks,” presented at the Proceedings - IEEE Symposium on Computers and Communications, Jul. 2009, pp. 141–146, doi: 10.1109/ISCC.2009.5202353.

[2] V. Beal, “The 7 Layers of the OSI Model - Webopedia Study Guide.” https://www.webopedia.com/quick_ref/OSI_Layers.asp (accessed Jun. 10, 2020).

[3] D. Coleman, “2.4 GHz Channel Planning,” *Extreme Networks*, Jul. 01, 2012. https://www.extremenetworks.com/extreme-networks-blog/2-4-ghz-channel-planning/ (accessed Jun. 10, 2020).

[4] C. Downey, “Understanding Wireless Range Calculations,” *Electronic Design*, Apr. 03, 2013. https://www.electronicdesign.com/technologies/communications/article/21796484/understanding-wireless-range-calculations (accessed Jun. 09, 2020).

[5] K. Georgiou, T. Constambeys, C. Laoudias, L. Petrou, G. Chatzimilioudis, and D. Zeinalipour-Yazti, “Anyplace: A Crowdsourced Indoor Information Service,” in *2015 16th IEEE International Conference on Mobile Data Management*, Pittsburgh, PA, USA, Jun. 2015, pp. 291–294, doi: 10.1109/MDM.2015.80.

[6] J. Gettys, B. Labs, and K. Nichols, “Bufferbloat: Dark Buffers in the Internet,” p. 15.

[7] C. Hoffman and B. King, “What Is OpenWrt And Why Should I Use It For My Router?,” *MakeUseOf*. https://www.makeuseof.com/tag/what-is-openwrt-and-why-should-i-use-it-for-my-router/ (accessed Jun. 10, 2020).

[8] T. Kulshrestha, D. Saxena, R. Niyogi, V. Raychoudhury, and M. Misra, “SmartITS: Smartphone-based identification and tracking using seamless indoor-outdoor localization,” *Journal of Network and Computer Applications*, vol. 98, pp. 97–113, Nov. 2017, doi: 10.1016/j.jnca.2017.09.003.

[9] K. Li, C. Yuen, and S. Kanhere, “SenseFlow: An Experimental Study of People Tracking,” in *Proceedings of the 6th ACM Workshop on Real World Wireless Sensor Networks - RealWSN ’15*, Seoul, South Korea, 2015, pp. 31–34, doi: 10.1145/2820990.2820994.

[10] B. Mitchell, “802.11 WiFi Standards Explained,” *Lifewire*. https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553 (accessed Jun. 10, 2020).

[11] A. Orebaugh, “Understanding Wireless Card Modes | Engineering360.” https://www.globalspec.com/reference/47547/203279/understanding-wireless-card-modes (accessed Jun. 10, 2020).

[12] M. Sikander Hayat Khiyal, “Trilateration and Triangulation Triangulation In...,” *ResearchGate*. https://www.researchgate.net/figure/Trilateration-and-Triangulation-Triangulation-In-Triangulation-the-directions-of-signal_fig1_264128575 (accessed Jun. 10, 2020).

[13] “Cell Phone Trilateration Algorithm,” *101 Computing*, Mar. 29, 2019. https://www.101computing.net/cell-phone-trilateration-algorithm/ (accessed Jun. 10, 2020).

[14]“Indoor localization: which technology for each use?” https://elainnovation.com/indoor-localization-which-technology-for-each-use.html (accessed Jun. 10, 2020).

[15] “OpenWrt Project: Welcome to the OpenWrt Project,” *OpenWRT Project*. https://openwrt.org/ (accessed Jun. 10, 2020).