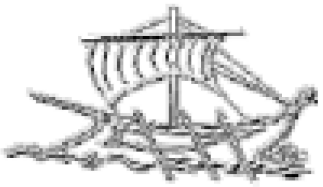


ΑΕΙ ΠΕΙΡΑΙΑ Τ.Τ.
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Χρήση τεχνολογιών προσωπικών δικτύων για ανίχνευση πλήθους

Γιαννούσης Χρήστος
κ
Ζορμπάς Κυριάκος

Εισηγητής: Δρ Χαράλαμπος Πατρικάκης, Αναπληρωτής Καθηγητής

ΑΘΗΝΑ
ΜΑΙΟΣ 2017

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Χρήση τεχνολογιών προσωπικών δικτύων για ανίχνευση πλήθους

Γιαννούσης Χρήστος
Α.Μ. 43211
κ
Ζορμπάς Κυριάκος
Α.Μ. 43088

Εισηγητής:

Δρ Χαράλαμπος Πατρικάκης, Αναπληρωτής Καθηγητής

Εξεταστική Επιτροπή:

……,
……,

Ημερομηνία εξέτασης …./…./2017

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Ζορμπάς Κυριάκος,

Του Αθανάσιου, με αριθμό μητρώου 43088 φοιτητής του Τμήματος Μηχανικών Η/Υ Συστημάτων Τ.Ε. του Α.Ε.Ι. Πειραιά Τ.Τ. πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα

προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

Ο κάτωθι υπογεγραμμένος Γιαννούσης Χρήστος,
Του Βασιλείου, με αριθμό μητρώου 43211 φοιτητής του Τμήματος Μηχανικών Η/Υ Συστημάτων Τ.Ε. του Α.Ε.Ι. Πειραιά Τ.Τ. πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:
«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.
Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.
Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα πτυχιακή εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, σε ένα ενδιαφέρον γνωστικό αντικείμενο. Θέλουμε να ευχαριστήσουμε το επιβλέπων καθηγητή μας Δρ Χαράλαμπο Πατρικάκη για όλη την βοήθεια και καθοδήγηση που μας παρείχε κατά την διάρκεια εκπόνησης της συγκεκριμένης πτυχιακής εργασίας. Επίσης, θέλουμε να ευχαριστήσουμε το ΑΕΙ ΠΕΙΡΑΙΑ Τ.Τ. που μας έδωσε πρόσβαση στον ανηχοϊκό θάλαμο που διαθέτει για εκτέλεση των πειραμάτων.

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία ασχολείται με την χρήση τεχνολογιών προσωπικών δικτύων για ανίχνευση πλήθους. Συγκεκριμένα οι τεχνολογίες που θα αναλύσουμε είναι αρχικά, η περίπτωση των κινητών δικτύων (GSM / 3G / 4G) και έπειτα αυτή του Wi-Fi. Στην περίπτωση του Wi-Fi περιγράφουμε τον εξοπλισμό και τα βήματα που πρέπει να ακολουθήσουμε για να εφαρμόσουμε την τεχνική Passive Wi-Fi tracking ή όποια έμμεσα θα μας βοηθήσει να κάνουμε ανίχνευση πλήθους. Στη συνέχεια θα παρουσιαστούν κάποιες σχετικά νέες τεχνολογίες όπως αυτή του Bluetooth χαμηλής ενέργειας (BLE) καθώς και η λειτουργία του NFC και RFID. Όσο αναφορά την τεχνολογία BLE κατασκευάζουμε και περιγράφουμε την χρήση των ibeacon όπου με την βοήθεια της εφαρμογής android που αναπτύξαμε μπορούμε να βρούμε την τοποθεσία του χρήστη. Κλείνοντας, αναφέρουμε τα μέσα μαζικής δικτύωσης τα οποία μας δίνουν και αυτά με την σειρά τους αρκετά στοιχεία για τον εντοπισμό των ατόμων στον χώρο. Η διαφορά της τελευταίας τεχνικής από τις υπόλοιπες είναι ότι ο χρήστης οικειοθελώς μας δίνει τα απαραίτητα στοιχειά για τον εντοπισμό του ενώ στις υπόλοιπες τεχνικές η ανίχνευση γίνετε πολλές φορές εν αγνοία του. Για αυτό τον λόγο πρέπει να αναφέρουμε ότι η παρούσα πτυχιακή εργασία γίνετε μόνο για ερευνητικούς σκοπούς και όχι για εκμετάλλευση τρίτων. Τέλος όλες οι δοκιμές έγιναν με χρήση αποκλειστικά δικών μας συσκευών και δεν έγινε καμία χρήση προσωπικών δεδομένων τρίτων, και αυτό γιατί όλες οι δοκιμές πραγματοποιήθηκαν σε κατάλληλα διαμορφωμένο εργαστηριακό περιβάλλον (ανηχοϊκος θάλαμος),

τον οποίο μας παρείχε το τμήμα Ηλεκτρονικών Μηχανικών Τ.Ε και θέλουμε να το ευχαριστήσουμε που μας έδωσε την άδεια για την χρήση του.

ABSTRACT

The present thesis concerns the crowdsensing though the use of PAN technologies. Specifically the technologies that we are going to analyze firstly, are the case of Location identification through the use of Cellular networks technologies (GSM/3G/4G) and then the case of Wi-Fi. Concerning the case of Wi-Fi, we are describing the proper equipment and the steps that we have to follow, to apply the Passive Wi-Fi tracking technique that will help us with crowdsensing. Then they presented some relatively new technologies, as this of Bluetooth-BT (and Bluetooth Low Energy - BLE) and this of NFC and RFID. About the BLE technology we are manufacture and describing the use of ibeacon, where with the help of android application that we developed, we can find the user's location. In conclusion, we report the web and online Social Networks which give us enough information to identify the atoms in space.The difference of the last service of the others, is that the user voluntarily provides us with the necessary information to detect him, while the other detection techniques become many times unknowingly. For this reason we must mention that this thesis become only for research purposes and not for exploitation. Finally, all tests were made using exclusively our own devices and there was no use of personal data to third parties, and this is why all the tests performed on appropriately configured lab environment (anechoic chamber).

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Δίκτυα

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: iBeacon , Wi-Fi , Crowd Sensing, Tracking, BLE

Περιεχόμενα

1. Εισαγωγή 15
2. Τεχνολογίες ανίχνευσης πλήθους 19
   2.1 Ταυτοποίηση τοποθεσίας μέσω της χρήσης της κινητής τεχνολογίας δικτύων (GSM / 3G / 4G) 20
   2.2 Η περίπτωση του Wi-Fi 21
   2.3 Passive Wi-Fi Tracking 23
   2.4 Probe Requests 23
   2.5 Monitor Mode 25
   2.6 Προστασία 26
   2.7 MAC Randomization 26
   2.8 Η περίπτωση του Bluetooth-BT (και Bluetooth Low Energy - BLE) 27
   2.9 iBeacon 28
   2.10 Εμβέλεια ibeacon 29
   2.11 Ρυθμίσεις 30
   2.12 Κατανάλωση ενέργειας 30
   2.13 Ιστορική Εξέλιξη 31
   2.14 Συμβατές συσκευές 32
   2.15 Περιπτώσεις και παραδείγματα χρησιμότητας των ibeacon 32
3. Πειραματική προσέγγιση 35
   3.1 Κατασκευή ενός Passive Wi-Fi Tracker 35
   3.2 Αρχιτεκτονική συσκευής Intel Galileo 35
   3.3 PuTTY 36
   3.4 Εγκατάσταση Προγράμματος 39
   3.5 Κατασκευή ibeacon με Raspberry Pi 42
   3.6 Μετατροπή Raspberry Pi1 και Pi2 σε ibeacon 43
   3.7 Μετατροπή Raspberry Pi3 σε ibeacon 45
   3.8 Κατασκευή εφαρμογής Android 46
      Activity_monitoring.xml 46

Activity_ranging.xml 47
MonitoringActivity.java 48
RangingActivity.java 51
AndoidManifest.xml 55
3.9 Η περίπτωση του NFC και RFID 56
3.10 Η περίπτωση του διαδικτύου και των μέσων μαζικής δικτύωσης 57
4. Νομικά και Ηθικά ζητήματα 59
4.1 Ευρωπαϊκοί κανονισμοί-αποφάσεις-πλαίσια 59
5. 5. Επίλογος 64
6. Συντομογραφίες 65
7. Βιβλιογραφία 66
8. Παράρτημα εικόνων εφαρμογής 72

1. Εισαγωγή

Πλήθος είναι ένας μεγάλος αριθμός ατόμων τα οποία έχουν συγκεντρωθεί σε μια περιοχή χωρίς οργάνωση ή πειθαρχεία. Μεγάλη συγκέντρωση πλήθους παρατηρείται συνήθως σε διάφορες ψυχαγωγικές, πολιτιστικές ή πολιτικές εκδηλώσεις καθώς και σε γήπεδα, αεροδρόμια, τουριστικά θέρετρα, μνημεία, εκκλησιές, πορείες και τέλος στα μέσα μαζικής μεταφοράς.

Κατά καιρούς η ιστορία έχει δείξει ότι τόσοι πολλοί άνθρωποι μαζεμένοι σε ένα σημείο μπορεί να προκαλέσει από υλικές καταστροφές και τραυματισμούς ατόμων μέχρι και τον θάνατό τους. Παρακάτω αναφέρονται μερικά από τα ποιο χαρακτηριστικά τέτοια συμβάντα.

1. Ημερομηνία: 9 Μαρτίου 1946
   Τοποθεσία : Burnden Park, Bolton, Manchester, England
   Θάνατοι : 33

   Στο Burnden Park, όταν ένα παιχνίδι μεταξύ των ομάδων Bolton Wanderers και Stoke City λάμβανε χώρα ένας τοίχος κατέρρευσε και σύνθλιψε τους θεατές, ξεκινώντας έτσι μια άτακτη φυγή, που σκότωσε 33 ανθρώπους. Περισσότεροι από 400 τραυματίστηκαν. Το πλήθος ήταν πάνω από 85.000 ανθρώπους. [58]

Εικόνα 1.1 Καταστροφή στο Burnden Park [58]

2. Ημερομηνία: 11 Απριλίου 2001
   Τοποθεσία: Ellis Park Stadium, Johannesburg, South Africa
   Θάνατοι: 43

   Το Ellis Park Stadium είχε χωρητικότητα 60.000 άτομα αλλα υπάρχουν αναφορές που λένε ότι στο γήπεδο εκείνη την μέρα έγιναν δεκτοί 120.000 οπαδοί. Αυτό είχε ως αποτέλεσμα να στριμωχτούν τα άτομα ανάμεσα στα καθίσματα και να προκαλέσει τον θάνατο 43 ανθρώπων. [58]

3. Ημερομηνία: 11 Μαΐου 1985
   Τοποθεσία: Valley Parade Stadium, Bradford, England.
   Θάνατοι: 56

Κατά την διάρκεια του αγώνα μία από τις εξέδρες έπιασε φωτιά το οποίο είχε ως αποτέλεσμα να πεθάνουν 56 άτομα και να τραυματιστούν πάνω από 450.Η καταστροφή ήταν τόσο μεγάλη εξαιτίας της κακής διαχείρισης εκκένωσης του πλήθους. [58]

Εικόνα 1.2 Φωτιά σε εξέδρα [58]

4. Ημερομηνία: 21 Ιουνίου 2016
   Τοποθεσία: NYC Subway Station, New York.
   Θάνατοι: 0

   Εκείνο το πρωί στο σιδηροδρομικό σταθμό Central Park North 2 άτομα άρχισαν να διαπληκτίζονται όταν κάποια στιγμή κάποιος φώναξε «κρατάει όπλο» αυτό είχε ως αποτέλεσμα δεκάδες άτομα να ποδοπατηθούν στην προσπάθεια τους να απομακρυνθούν.[59]

5. Ημερομηνία: 23 Μαΐου 2099
   Τοποθεσία: Rabat, Morocco
   Θάνατοι: 11

   Κατά την διάρκεια ενός μουσικού φεστιβάλ, στο οποίο παρευρισκόντουσαν τουλάχιστον 10.000 άτομα, 11 από αυτά ποδοπατήθηκαν μέχρι θανάτου. Η ευθηνή βαραίνει την αστυνομία η οποία έκλεισε πολλές από τις εξόδους της συναυλίας δημιουργώντας συνωστισμό στην έξοδο του κόσμου .[60]

6. Ημερομηνία: 1 Ιανουριου 2015
   Τοποθεσία: Chenyi Square, Shanghai.
   Θάνατοι: 36

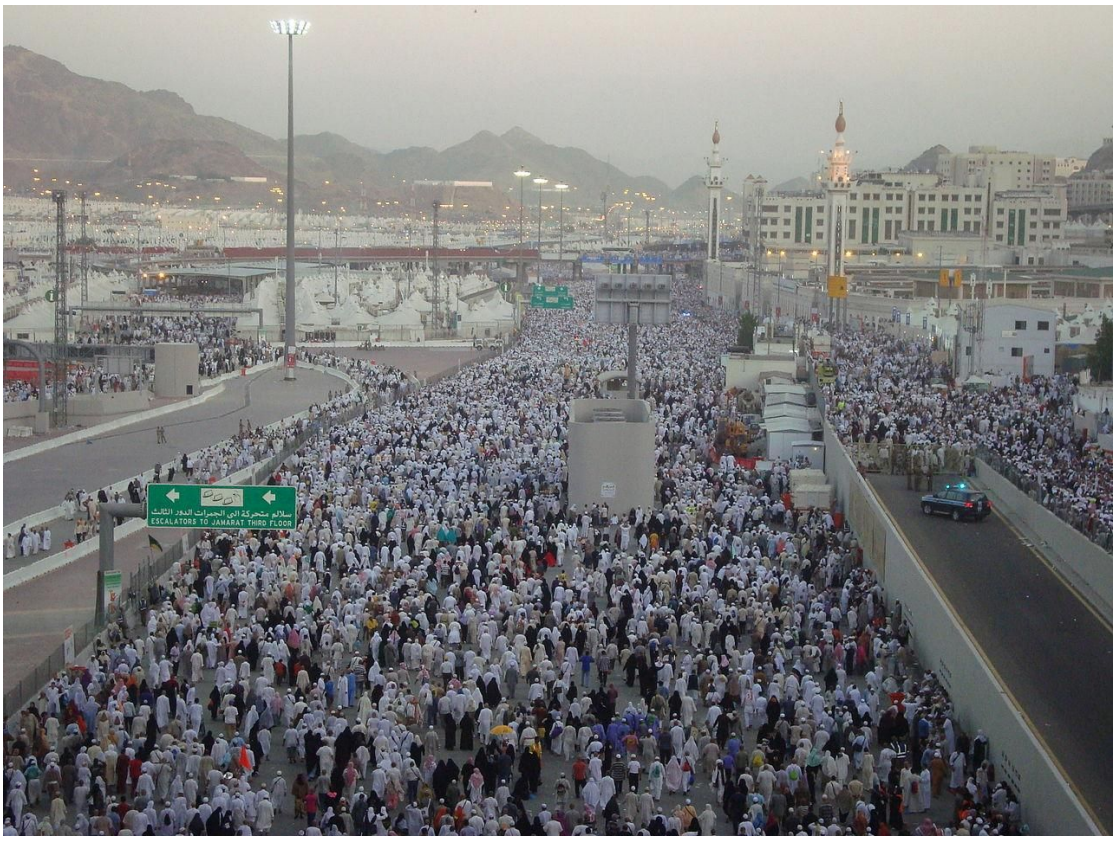
300.000 άτομα είχαν μαζευτεί για να γιορτάσουν την αλλαγή του χρόνου. Εξαιτίας του συνωστισμού 36 άτομα πέθαναν και άλλα 49 τραυματιστήκαν 13 εκ των οποίων πολύ σοβαρά.[61]

Εικόνα 1.3 Παραμονή Πρωτοχρονιάς στην Σαγκάη [61]

7. Ημερομηνία: 24 Σεπτεμβριου 2015
   Τοποθεσία: Mina, Mecca, Saudi Arabia.
   Θάνατοι:769

769 προσκυνητές στη Μέκκα ποδοπατήθηκαν μέχρι θανάτου, ύστερα από κίνηση πανικού του πλήθους, ενώ περισσότεροι από 800 τραυματίσθηκαν, σύμφωνα με τις αρχές της Σαουδικής Αραβίας. Παρόλα αυτά το τοπίο για τον ακριβή αριθμό των νεκρών είναι θολό και αυτό γιατί σύμφωνα με το Αμερικάνικο πρακτορείο Associated Press οι νεκροί ανερχόντουσαν στους 2.411 ακόμα σύμφωνα με το πρακτορείο Reuters οι νεκροί υπολογίστηκαν στους 2.070. Ενώ το Γαλλικό πρακτορείο Agence France-Presse έγραψε πως οι αποθανόντες ήταν 2.236.[63][64]

Το συγκεκριμένο περιστατικό θεωρείται από τα ποιο καταστροφικά της σύγχρονης ιστορίας και συνέβη όταν δύο μεγάλες ομάδες πιστών συναντήθηκαν σε σταυροδρόμι πεζοπορικού άξονα στη Μίνα, την τοποθεσία κατασκήνωσης των περισσότερων από 2 εκατ. μουσουλμάνων που πραγματοποιούν το ετήσιο προσκύνημα στη Μέκκα.[62]



Εικόνα 1.4 Ο δρόμος για την γέφυρα Jamarat [65]

Για αυτό τον λόγο στην παρούσα πτυχιακή εργασία παρουσιάζονται οι τρόποι με τους οποίους μπορούμε να ανιχνεύουμε το πλήθος έτσι ώστε να προλαμβάνονται όσο το δυνατόν παρόμοιες με τις παραπάνω καταστάσεις. Στο κεφάλαιο δύο θα ασχοληθούμε με τη χρήση των iBeacons (BLE) και πώς μπορούμε να τα χρησιμοποιήσουμε για την ανίχνευση πλήθους. Στη συνέχεια θα δούμε πώς μπορούμε να μετατρέψουμε μια Wi-Fi συσκευή ώστε να καταγράφει τον αριθμό των ατόμων μέσα σε ένα χώρο. Τέλος θα ερευνήσουμε το νομικό πλαίσιο που καλύπτει αυτού του είδους τις τεχνολογίες.

2. Τεχνολογίες ανίχνευσης πλήθους

Η συνεχόμενη αύξηση των κινητών συσκευών ικανών για επικοινωνία σε πολύ υψηλό εύρος συχνοτήτων, η υψηλή προγραμματιστική ισχύ καθώς και το μικρό τους μέγεθος καθιστά τα smartphones ως ένα αναπόσπαστο κομμάτι του καθημερινού εξοπλισμού μας. Μαζί με αυτά ήρθε και η ικανότητα να βρισκόμαστε πάντα συνδεδεμένοι σε μία ή περισσότερες μορφές ασύρματης διαδικτυακής τεχνολογίας δίνοντας πρόσβαση σε ένα ευρύ τοπικό ή προσωπικό εύρος επικοινωνίας. (Με τη χρήση του GSM/3G/4G, WLAN ή PAN τεχνολογιών.)

Η ικανότητα της αδιάκοπης συνδεσιμότητας με τη χρήση των παραπάνω τεχνολογιών συνοδεύεται με την ικανότητα εντοπισμού της θέσης της συσκευής. Κάθε συσκευή διαθέτει μία σειρά από μοναδικούς κωδικούς αναγνώρισης όπως ο International Mobile Station Equipment Identity (IMEI) που συνήθως βρίσκεται πίσω από την μπαταρία του κινητού, ο Integrated Circuit CardID (ICCID) ένας 19 – ψήφιος αριθμός τυπωμένος μέσα στην κάρτα SIM του κινητού, ο Mobile Equipment Identifier (MEID) ένας αριθμός που μπορούμε να τον δούμε συνήθως ως έναν IMEI αριθμό σε 16 δική μορφή. Ο Secure Element ID Number (SEID) ο οποίος χρησιμοποιείται από την Appleγια να ασφαλίσει της πληρωμές που γίνονται μέσω κινητού και φυσικά τις MAC διευθύνσεις του κάθε δικτύου οποιασδήποτε μορφής όπως GSM/3G/4G, το Wi-Fiκαι τις συσκευές του Bluetooth. Όλοι αυτοί οι ξεχωριστοί κωδικοί αναγνώρισης κάνουν δυνατή την ταυτοποίηση και τον εντοπισμό ξεχωριστά της κάθε κινητής συσκευής, με το βαθμό επιτυχίας να διαφέρει ανάλογα με την τεχνολογία (ή τον συνδυασμό) που χρησιμοποιείται

Φυσικά με την ενσωμάτωση του GPS στις κινητές συσκευές ακόμα και στις wearable, τις καθιστά ικανές για συνεχόμενη αναφορά της θέσης, επιτρέποντας έτσι για ακόμα καλύτερη ακρίβεια στον εντοπισμό της θέσης, την στιγμή που η τεχνολογία για τον εντοπισμό μέσα σε έναν εσωτερικό χώρο έχει ήδη ξεκινήσει βασισμένη στο σύστημα Bluetooth Low Energy (BLE), στο Radio Frequency Identification (RFIDs) και στο Near Field Communications (NFCs) τα οποία επιτρέπουν τον εντοπισμό του χρήση σε μια εμβέλεια ακόμα και μικρότερη του ενός μέτρου. Όμως αυτό προϋποθέτει πως ο χρήστης έχει συναινέσει στο να δώσει τη πληροφορία για την θέση του που λαμβάνει η κινητή του/της συσκευή, όπως τα δεδομένα του GPS, ή έχει προσελκύσει κάποιο RFIDή NFC σημείο. Από την άλλη πλευρά, οι τεχνολογίες του BLE και RFID χρησιμεύουν και στον ακούσιο εντοπισμό μιας συσκευής, όπως θα δούμε παρακάτω.

Παρόμοια περίπτωση εθελοντικής αναφοράς της τοποθεσίας του χρήστη είναι και τα Social Networks (κοινωνικά δίκτυα).

SNs : Η ευρεία διάδοση των SNs, η ικανότητα και ο «τρόπος ζωής» των χρηστών των κοινωνικών δικτύων, τους οποίους οδηγεί στην δήλωση της θέσης τους μέσα από μια πληθώρα από SN εφαρμογών όπως το Facebook,

το Instagram, το Snapchat και το Foursquare έχουν καταστήσει δυνατό τον εντοπισμό της συσκευής και του χρήστη στο χώρο και το χρόνο.

Από τα παραπάνω, είναι προφανές πως ο εντοπισμός μιας συσκευής μπορεί να γίνει με πολλούς τρόπους, μέσο της χρήσης των διαδικτυακών τεχνολογιών ασύρματων και ενσύρματων, ή με την εθελοντική συνεισφορά του χρήστη για την τοποθεσία του. Αυτό μπορεί να γίνει με ενεργητικό ή και παθητικό τρόπο το οποίο εξαρτάται από το αν ο χρήστης είναι ενημερωμένος για τη λειτουργία των εργαλείων εντοπισμού της θέσης και των διαθέσιμων τεχνολογιών.

Όλα τα παραπάνω έρχονται να συμβάλουν σε ένα σετ από τεχνολογικά εργαλεία, που μπορούν να χρησιμοποιηθούν με σκοπό να εντοπίσουν τη θέση του χρήστη. Ακόμα και στις περιπτώσεις που μόνο η τοποθεσία της συσκευής είναι γνωστή, είναι εφικτό να τη συνδέσουμε με τον χρήστη της συσκευής. Σε πολλές χώρες για την εγγραφή σε ένα δίκτυο θα πρέπει να γίνει με την καταγραφή του χρήστη με ένα ID αριθμό χρήστη. Επίσης ο συνδυασμός φωνής και δεδομένων μπορούν να χρησιμοποιηθούν για την ταυτοποίηση και τον εντοπισμό του χρήστη. Αυτές οι μέθοδοι χρησιμοποιούνται συχνά ιδικά σε νομικές πράξεις [1].

Για παράδειγμα ένας ύποπτος, για τις βομβιστικές επιθέσεις στη Γερμανία το 2010, εντοπίστηκε μέσο των δεδομένων που λήφθηκαν από το κινητό του και του GPS που ήταν ενσωματωμένο στη συσκευή [2]. Επίσης η αστυνομία της Αγγλίας κατάφερε να εντοπίσει και να συλλάβει τους δράστες για το θάνατο ενός δωδεκάχρονου κοριτσιού και 3 άλλων γυναικών σε μια αποφοίτηση, με τον ίδιο πάλι τρόπο.

Να σημειωθεί όμως, πως ο εντοπισμός ενός χρήστη και μιας συσκευής παίρνει νομικές διαστάσεις και επιπλοκές μιας και εντάσσεται στο πλαίσιο των απόρρητων προσωπικών δεδομένων. Σύμφωνα με [4], οι λόγοι για την επεξεργασία προσωπικών δεδομένων είναι η συγκατάθεση του ίδιου του χρήστη ή κάποια νομική διαδικασία πρέπει να επιτευχθεί ή για το δημόσιο συμφέρον. Από την άλλη η ανώνυμη επεξεργασία δεδομένων σχετικών με την τοποθεσία της συσκευής για περιπτώσεις όπως η αριθμητική εκτίμηση του πλήθους είναι χρήσιμη, ίδιος σε περιπτώσεις δημόσιας ασφάλειας.

Εδώ λοιπόν θα αναλύσουμε τις διάφορες μεθόδους που υπολογιστικά δίκτυα και τεχνολογίες του Ιστού μπορούν να χρησιμοποιηθούν για τον υπολογισμό του πλήθους (crowd-sensing) σε πραγματικό χρόνο, αποτελεσματικά και πολύ οικονομικά.

2.1 Ταυτοποίηση τοποθεσίας μέσω της χρήσης της κινητής τεχνολογίας δικτύων (GSM / 3G / 4G)

Η χρήση των κινητών δικτύων με σκοπό την παροχή εκτίμησης όσον αφορά την πυκνότητα και (ενδεχομένως) την ροή του πλήθους θεωρείται ιδανική σε πολλές περιπτώσεις, λόγω του μεγάλου αριθμού των smartphones,

παρόλα αυτά δεν είναι τόσο αποτελεσματική όσο δείχνει αρχικά. Ο λόγος είναι ότι υπάρχουν θέματα που αφορούν κυρίως, την ιδιωτική ζωή του κάθε ανθρώπου που θα πρέπει να αντιμετωπιστεί με ([2, 4]), δεδομένου ότι η νομοθεσία προστατεύει την προσωπική ζωή του κάθε ατόμου. Ως εκ τούτου, ακόμη και αν η τριγωνοποίηση (triangulation) της θέσης ή η πολυπλεύριση (multilateration) του κάθε ατόμου μπορεί να επιτευχθεί από το σταθμό βάσης της κινητής τηλεφωνίας [2, 3], οι κανονισμοί απαιτούν ότι τα αναγκαία νομοθετικά μέτρα πρέπει να ληφθούν πρώτα από τις αρχές πριν επιτραπούν τα εν λόγω μέτρα, [4]. Κατά συνέπεια, η επεξεργασία των δεδομένων που προέρχονται από δίκτυα κινητής τηλεφωνίας μπορούν να θεωρηθούν πιο αποτελεσματικά ως μετά - εργαλείο ανάλυσης, όπου η συμπεριφορά και οι κινήσεις ενός ατόμου μπορούν να μελετηθούν, προκειμένου να εντοπίσει αν υπήρχαν ύποπτες και ενδεχομένως επικίνδυνες κινήσεις του ατόμου ή αν συμμετείχε σε εγκληματικές δραστηριότητες. Δεδομένου ότι ο χρόνος που απαιτείται για την απόκτηση άδειας για τη χρήση των προσωπικών δεδομένων από τις αρχές μπορεί να είναι μεγάλος , ειδικά όταν πρόκειται για κρίσιμες καταστάσεις, όπως μια τρομοκρατική επίθεση, αυτή η τεχνική δεν αφήνει αρκετό χρόνο για να οργανωθεί και να προετοιμαστεί οποιαδήποτε ενέργεια αντιμετώπισης καταστάσεων έκτακτης ανάγκης, επειδή η ροή των γεγονότων προηγείται κάθε αντίδρασης.

2.2 Η περίπτωση του Wi-Fi

Πρόσφατα, η χρήση των τεχνολογιών ασύρματων δικτύων (όπως το 802.11 - Wi-Fi) για την εκτίμηση του πλήθους γίνεται όλο και πιο δημοφιλής. Οι σταθμοί Wi-Fi στέλνουν περιοδικά μηνύματα Εκπομπών (Beacon messages), περίπου κάθε 100 ms από προεπιλογή (by default), αλλά αυτός ο αριθμός μπορεί να αλλάξει χειροκίνητα στην επιθυμητή συχνότητα, προκειμένου να δηλώσει την παρουσία του ασύρματου δικτύου[5].Σε αυτό το μήνυμα Beacon, το Service Set Identifier (SSID), ένας διακριτικός αριθμός που προσδιορίζει ένα δίκτυο, περιλαμβάνεται, μαζί με πληροφορίες που αφορούν τις δυνατότητες του δικτύου. Οι συσκευές με ενεργοποιημένο Wi-Fi σαρώσουν την περιοχή για να λάβουν το μεταδιδόμενο SSID και να σχηματιστή μια Independent Basic Service Set (IBSS) με το σταθμό. Κάθε Wi-Fi συσκευή μπορεί να σαρώσει την περιοχή για τυχόν μηνύματα Beacon είτε σε παθητική κατάσταση, απλά ακούγοντας κάθε πότε φθάνουν τα μηνύματα στα διάφορα κανάλια, χωρίς να στέλνει κανένα probe request(αίτημα σύνδεσης), ή σε ενεργή κατάσταση, όπου η συσκευή εκπέμπει ενεργά probe requests σε όλα τα πιθανά λειτουργικά κανάλια. Τυπικά, τα Wi-Fi σήματα μεταδίδονται σε δύο διαφορετικές συχνότητες, στα 2,4 GHz και στα 5 GHz.

Πρόσφατα, εκμεταλλευόμενοι αυτά τα χαρακτηριστικά του Wi-Fi, πολλές δημοσιεύσεις αναφέρουν τον τρόπο με τον οποίο μπορεί να γίνει η ενεργητική και η παθητική ανίχνευση των συσκευών, καθώς και τις πρακτικές εφαρμογές για την εκτίμηση του αριθμού των πεζών ή των οχημάτων που

έχουν ανιχνευτεί. [6,7].Στο [6], οι συγγραφείς μελέτησαν πώς η λήψη των παθητικών σημάτων Wi-Fi (δηλαδή, Wi-Fi probe requests), από έναν αριθμό Wi-Fi συσκευών και τη χρήση ενός κεντρικού διακομιστή (server)μπορεί να χρησιμοποιηθεί για την εκτίμηση της κατεύθυνσης του ιδιοκτήτη της συσκευής. Οι ληφθέντες Wi-Fi μεταδόσεις φέρουν την μοναδική διεύθυνση MAC της συσκευής, που επιτρέπει την αναγνώριση της συσκευής από διάφορες Wi-Fi συσκευές διάσπαρτα στην περιοχή. Αυτές οι Wi-Fi συσκευές μπορούν να καταγράψουν και να αναφέρουν οποιαδήποτε μετάδοση Wi-Fi που λήφθηκε, ακόμη και σε πραγματικό χρόνο, χωρίς υψηλά έξοδα όσον αφορά την επικοινωνία ή τον υπολογισμό.

Η χρήση ειδικών αλγορίθμων, όπως ο προτεινόμενος Straw-man αλγόριθμος, μπορεί να επιτρέψει την ανίχνευση της κατεύθυνσης της συσκευής, θεωρώντας την τοποθεσία του τηλεφώνου ως την τοποθεσία του ανιχνευτή που κατέλαβε το σήμα του τηλεφώνου και στη συνέχεια να παρεμβάλει τις θέσεις του τηλεφώνου ανάμεσα σε δύο επιτυχημένες ανιχνεύσεις. Επιπλέον, όταν η μέθοδος αυτή χρησιμοποιείται για ένα μεγάλο αριθμό συσκευών, τότε μπορεί να μας δώσει πληροφορίες για τις κυκλοφοριακές συνθήκες ή για την κίνηση ροής του πλήθους.

Τόσο οι κατανεμημένες όσο και κεντρικοποιημένες (distributed and centralized) αρχιτεκτονικές μπορούν να χρησιμοποιηθούν για αυτό το σκοπό , με αλγορίθμους που εκτελούνται την ίδια στιγμή στην συσκευή που κάνει την ανίχνευση (και αυτό είναι πολύ εύκολο και φέρει ένα πολύ χαμηλό κόστος, δεδομένου ότι μπορεί να τρέξει σε χαμηλού κόστους υπολογιστές όπως ένα Raspberry Pi ο οποίος έχει πολύ μικρό μέγεθος), ή ένα κεντρικό διακομιστή για τον οποίο οι συσκευές παρακολούθησης αναφέρουν τα αποτελέσματα της παρακολούθησης τους. Στην τελευταία περίπτωση, ο συνδυασμός των δεδομένων από όλες τις συσκευές μπορεί να οδηγήσει σε εξαιρετικά ακριβή αποτελέσματα. Η ποιότητα της πρόβλεψης έγκειται στον αριθμό των μεταδόσεων της συσκευής που έχουν συλληφθεί.

Δυστυχώς, παθητική παρακολούθηση Wi-Fi πάσχει από ορισμένα τρωτά σημεία που βλάπτουν την αξιοπιστία του. Πρώτον, τα επίπεδα θορύβου επηρεάζουν τη σύλληψη των probe requests. Η απώλεια διαδρομής, η ισχύς της μετάδοσης και το ξεθώριασμα είναι μερικά από τα χαρακτηριστικά που μπορούν να επηρεάσουν τη λήψη των παθητικών μεταδόσεων Wi-Fi. Επιπλέον, το γεγονός ότι τα smartphones δεν είναι τροποποιημένα ώστε να μεταδίδουν σε συγκεκριμένα και συχνά χρονικά διαστήματα, αλλά να μεταδίδουν σχετικά με τη διακριτική τους ευχέρεια(τα χρονικά διαστήματα από 30 έως 120 δευτερόλεπτα έχουν μετρηθεί, ανάλογα με τη συσκευή), μαζί με την αραιή τοποθεσία των Wi-Fi monitor μπορεί να οδηγήσει σε παρατεταμένες περιόδους χωρίς να έχει ληφθεί κάποια μετάδοση, γεγονός που καθιστά δύσκολο να παρακολουθείτε η συσκευή σε μικρά χρονικά διαστήματα και επιδεινώνει την ποιότητα των προβλέψεων σχετικά με την κατεύθυνση του.

Υπάρχουν αρκετά παραδείγματα της πρακτικής χρήσης των τεχνικών που περιγράφονται παραπάνω. Στο [7], η ιδέα της παθητικής σύλληψης Wi-Fi

σημάτων χρησιμοποιείται για την ανάλυση της ροής από ένα πλήθος πεζών που χρησιμοποιούν MAC Address Probe Sensors (AMP Αισθητήρες) για να παρακολουθούνται ανώνυμα οι διευθύνσεις MAC των συσκευών στην περιοχή. Ο συνολικός αριθμός των συλληφθέντων διευθύνσεων MAC γύρω από ένα αισθητήρα AMP μπορεί να χρησιμοποιηθεί ως μια εκτίμηση του πλήθους που βρίσκεται στην περιοχή, ενώ η ανάλυση των συλλεχθέντων διευθύνσεων από διαφορετικούς αισθητήρες μπορεί να δώσει εκτίμηση σχετικά με τη ροή του πλήθους. Αυτό το είδος των πληροφοριών μπορεί να είναι χρήσιμο, όχι μόνο σε περιόδους καταστροφής, αλλά και κατά τη διάρκεια της καθημερινότητας Ο αισθητήρας AMP που περιγράφεται στο έγγραφο είναι μια χαμηλού κόστους και μικρού μεγέθους συσκευή που διαθέτει προσαρμογέα Wi-Fi που τρέχει σε monitor mode (λειτουργία αδρανείας) για να βοηθήσει στη συλλογή, passive Wi-Fi probe requests. Εκτός από τις διευθύνσεις MAC, η αραίωση της ισχύς του ληφθέντος σήματος (RSSI)μπορεί επίσης να μετρηθεί με βάση την απόσταση μεταξύ ενός αισθητήρα AMP και του smartphone. Σε μια άλλη περίπτωση [8], Wi-Fi Media Access Control Scanners (Σαρωτές Ελέγχου Πρόσβασης σε μέσα μαζικής ενημέρωσης)χρησιμοποιήθηκαν στη σάρωση για σήματα Wi-Fi στην περιοχή. Σε αυτήν την περίπτωση, η σάρωση των ασύρματων καναλιών γίνεται τόσο στην παθητική όσο και στην ενεργητική κατάσταση.

Μετά την probing φάση στη λειτουργία ενεργής σάρωσης, μια φάση ελέγχου ταυτότητας εκτελείται πριν η σύνδεση μεταξύ των δύο τμημάτων εγκατασταθεί .Η διάρκεια της φάσης εποπτείας είναι πολύ μικρή (ειδικά όταν συγκρίνεται με την διάρκεια της τεχνολογίας Bluetooth) περίπου 8 ms, επιτρέποντας την περιοδική ανίχνευση των σημάτων με μια περίοδο, τόσο μικρή όσο 1 sec. Ο πολλαπλός αριθμός των φορών που η διεύθυνση MAC μιας συσκευής θα μπορούσε να συλληφθεί από έναν αισθητήρα συνιστάται να χρησιμοποιείται για τον προσδιορισμό του χρόνου διαδρομής του.

2.3 Passive Wi-Fi Tracking

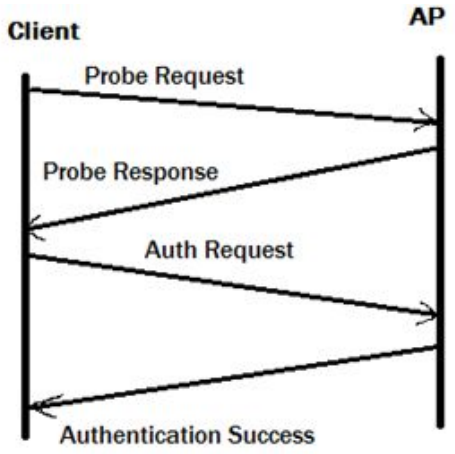
Στη σημερινή εποχή, ο μέσος άνθρωπος είναι συνεχώς συνδεμένος στο διαδίκτυο είτε αυτό έχει τη μορφή μιας διαδικτυακής πλατφόρμας όπως ένας περιηγητής (Microsoft Edge, Chrome, Firefox) ή τη μορφή κάποιας εφαρμογής από μια σύγχρονη κινητή συσκευή (smartphone, tablet). Οι κινητές συσκευές χρησιμοποιούν είτε το Wi-Fi είτε τα δεδομένα του κινητού για να συνδεθούν στο διαδίκτυο. Η χρήση του Wi-Fi καθιστά τις συσκευές και επομένως τον χρήστη, εύκολο να εντοπιστούν από κάποιον μέσω μιας διαδικασίας που ονομάζεται Παθητικός Wi-Fi Εντοπισμός (**PassiveWi-FiTracking**). Τα τελευταία χρόνια η χρήση αυτής της μεθόδου έχει αυξηθεί από διαφημιστές, πωλητές και άλλους για την παραγωγή στατιστικών. Πώς όμως λειτουργεί αυτή η τεχνολογία του **Passive Wi-Fi Tracking**;

2.4 Probe Requests

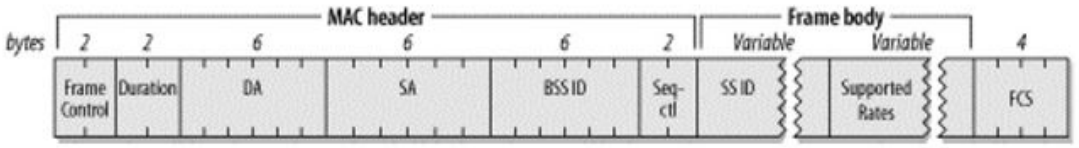
Όταν ένας Wi-Fi client, όπως είναι ένα laptop ή ένα smartphone, ψάχνει να συνδεθεί σε κάποιο δίκτυο υπάρχουν δύο τρόποι με τους οποίους μπορεί να το πετύχει. Η πρώτη μέθοδος που χρησιμοποιείται κυρίως από laptop και γενικά από μη-κινητές συσκευές (non-smartphones), είναι το σκανάρισμα για Beacon Frames. Τα Beacon Frames είναι «πακέτα» τα οποία εκπέμπονται από ένα Wi-Fi για κάνει γνωστή την παρουσία του στο χώρο. Όταν βρεθεί το Beacon Frame από κάποιο δίκτυο με το οποίο είχε συνδεθεί παλαιότερα, ξεκινά η διαδικασία της σύνδεσης της συσκευής με το Wi-Fi.

Η δεύτερη μέθοδος, η οποία χρησιμοποιείται περισσότερο από smartphones, αποστέλλει περιοδικά πακέτα τα οποία ονομάζονται Probe Requests. Τα πακέτα αυτά περιέχουν την μοναδική MAC (**Media Access Control Address**) διεύθυνση του πελάτη (client) και κάποιες φορές το όνομα του δικτύου με το οποίο είχε συνδεθεί προηγουμένως. Αυτή η μέθοδος έχει το πλεονέκτημα να πραγματοποιεί μια ασύρματη σύνδεση πολύ πιο γρήγορα, λόγω της ταχύτερης και συνεχόμενης εκπομπής των Probe Request από το να περιμένει από το Wi-Fi router να εκπέμψει κάποιο Beacon Frame.

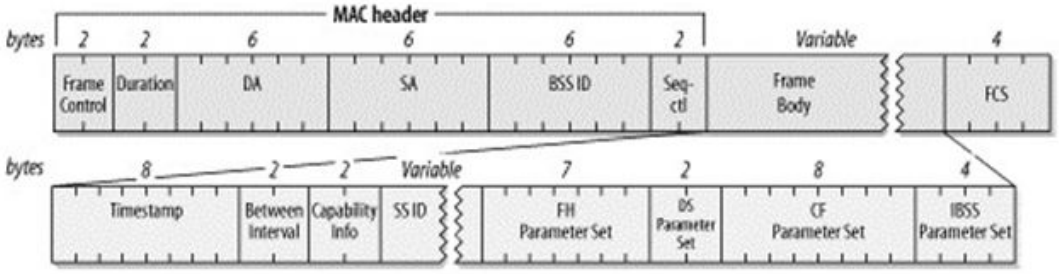
Μπορεί αυτή η μέθοδος να είναι πιο βολική και γρήγορη για να κάνουμε μια σύνδεση σε ένα Wi-Fi όμως το κάνει πιο εύκολο σε κάποιον να συλλέξει τα δεδομένα και να μπορέσει να παρακολουθήσει άλλους ανθρώπους.



Εικόνα 2.1 Probe request [56]



Εικόνα 2.2 WLAN Probe Request Frame [57]



Εικόνα 2.3 WLAN Probe Response Frame [57]

Τα probe responses περιλαμβάνουν πληροφορία που είναι χρήσιμη για τη συσκευή που έστειλε το probe request. Πληροφορία όπως το SSID δηλαδή το όνομα της συσκευής, τον υποστηριζόμενο ρυθμό μετάδοσης (supported data rates), τους τύπους encryption που χρησιμοποιεί αν χρειαστεί, και διάφορες άλλες δυνατότητες του Access Point.

2.5 Monitor Mode

Οι συσκευές Wi-Fi μπορούν να λειτουργήσουν σε 6 καταστάσεις λειτουργίας. Τα routers συνήθως λειτουργούν σε Master mode ενώ οι clients σε Managed mode.

- Master (λειτουργεί ως access point)
- Managed (συσκευές πελάτες π.χ. κινητά, φορητοί υπολογιστές)
- Ad-Hoc (P2P λειτουργία που οι συσκευές επικοινωνούν χωρίς κάποια βάση)
- Mesh (ένα σχεδιασμένο Ad-Hoc, P2P)
- Repeater (επεκτείνει το σήμα ενός access point)
- Monitor (λειτουργεί ως ανιχνευτής)

Όμως αν θέλαμε να ανιχνεύσουμε την παρουσία άλλων ασύρματων δικτύων τότε θα πρέπει να βάλουμε τη συσκευή μας σε λειτουργία Monitor. Ενώ η συσκευή βρίσκεται σε αυτή τη λειτουργία, παύει να εκπέμπει την

παρουσία του στο χώρο, καθιστώντας την πρακτικά αόρατη και δύσκολο να καταλάβει κανείς την παρουσία της.

Η Microsoft σε παλαιότερες εκδόσεις των Windows δεν επέτρεπε την αλλαγή λειτουργίας των Wi-Fi. Με την έκδοση των Windows Vista και των επόμενων αναβαθμίσεων επιτράπηκε η αλλαγή σε λειτουργία Monitor Mode. Πώς όμως μπορούμε να προστατευτούμε από κάτι τέτοιο ;

2.6 Προστασία

Από τα πρώτα θέματα που πρέπει να γνωρίζουμε σε ένα γενικό πλαίσιο είναι πως δεν υπάρχει προστασία στο διαδίκτυο. Η καλύτερη λύση στο παραπάνω πρόβλημα για την προστασία μας από τέτοια συστήματα είναι να κλείσουμε το Wi-Fi του κινητού όπου δε το χρειαζόμαστε. Με αυτό τον τρόπο το κινητό σταματάει να εκπέμπει probe requestsκαι έτσι γίνεται αόρατο από άλλους. Από την άλλη αυτό δεν είναι και τόσο πρακτικό.

Για τις Android συσκευές υπάρχουν κάποιες εφαρμογές οι οποίες περιορίζουν τη λειτουργία του Wi-Fi σε συγκεκριμένα δίκτυα. Αυτό γίνεται με το να εντοπίζουν δίκτυα τα οποία έχουμε ορίσει ως ασφαλή και να ενεργοποιούν το Wi-Fi μόνο όταν βρισκόμαστε σε εμβέλεια συνδεσιμότητας.

Για τις iOS συσκευές οι επιλογές είναι αρκετά περιορισμένες εκτός και ανέχεται «σπασμένη» (jailbreak) συσκευή. Αυτό γιατί η Appleδεν επιτρέπει σε τρίτες εφαρμογές να ενεργοποιούν και να απενεργοποιούν το Wi-Fi της συσκευής. Το iOS 7, εισήγαγε την πτυσσόμενη κάτω μπάρα για την γρήγορη επεξεργασία κάποιον βασικών ρυθμίσεων, μια από αυτές είναι και η ενεργοποίηση ή απενεργοποίηση του Wi-Fi. Έτσι θα πρέπει ο χρήστης πάντα χειροκίνητα να κλείνει το Wi-Fi όταν φεύγει από το σπίτι.

2.7 MAC Randomization

Η Apple με το iOS 8 πρόσθεσε μια καινούργια λειτουργία στις συσκευές της. Η λειτουργία αυτή ονομάζεται MAC Randomization και ουσιαστικά αλλάζει την MAC διεύθυνση του δικτύου της συσκευής κάνοντας τον εντοπισμό της αρκετά δύσκολο. Κάθε φορά που ο χρήστης ανοίγει το Wi-Fi στη συσκευή του αυτό ξεκινά να στέλνει προς τα έξω probe requests, όμως αντί να εκπέμπει την πραγματική της MAC διεύθυνση, χρησιμοποιεί μια ψεύτικη. Όταν κάποιο δίκτυο ανιχνεύσει το probe requestκαι απαντήσει με ένα probe response τότε με το αίτημα σύνδεσης που θα ζητήσει η συσκευή μας θα αποσταλεί και η πραγματική MAC διεύθυνση της [9].

Ακολουθώντας τις προσπάθειες της Apple, τον τελευταίο καιρό παρόμοια χαρακτηριστικά έχουν εμφανιστεί και από τα υπόλοιπα λειτουργικά συστήματα (OS) όπως τα Windows 10, όπου το χαρακτηριστικό τους είναι να παρέχουν την ίδια διεύθυνση MAC, όταν ερωτάται από το ίδιο δίκτυο, χρησιμοποιώντας έναν αποτελεσματικό αλγόριθμο. Το Android επίσης είχε

αναφέρει πως θα εισάγει την τεχνολογία της τυχαιοποίηση της MAC για την έκδοση 6 και πάνω, παρόλα αυτά ακόμα δεν έχει εφαρμοστεί ενώ βρισκόμαστε στην έκδοση 7. Τέλος, τα Linux έχουν επίσης υιοθετήσει αυτό το χαρακτηριστικό από την έκδοση kernel 3,18 και άνω.

- Η ίδια randomized Mac διεύθυνση χρησιμοποιείται για όλα τα probe requests όσο η συσκευή δεν βρίσκεται σε αδράνεια (sleep mode)

- Η randomized Mac διεύθυνση αλλάζει κάθε φορά που η συσκευή επανέρχεται από αδράνεια (sleep mode).[10]

2.8 Η περίπτωση του Bluetooth-BT (και Bluetooth Low Energy - BLE)

Πριν πάμε να περιγράψουμε τον τρόπο με τον οποίο το BT και το BLE μπορούν να χρησιμοποιηθούν για τον προσδιορισμό της θέσης μιας συσκευής και, ενδεχομένως, να παρέχουν εκτίμηση του πλήθους, θα πρέπει να αναφέρουμε ότι η χρήση των BLE έχει καθιερωθεί για ανίχνευση σε εσωτερικούς χώρους. Οι BLE συσκευές λειτουργούν, παρόμοια με τους Wi-Fi πομποδέκτες, στα 2,4 GHz (ή κοντά σε εμάς που θα περιγράφει αργότερα) και στέλνουν περιοδικά ραδιοσήματα (που μπορούν να αλλάξουν χειροκίνητα) στα beacons που μπορούν να χρησιμοποιηθούν για την εύρεση της τοποθεσίας μιας συσκευής. Επομένως, η αποτελεσματικότητα της χρήσης BLE είναι εξαιρετικά καλή σε εσωτερικούς χώρους αφού το σήμα μειώνεται σημαντικά όταν η απόσταση γίνεται μεγαλύτερη από 1m (δηλαδή, η ισχύς του σήματος είναι αντιστρόφως ανάλογη με το τετράγωνο της απόστασης μεταξύ του πομποδέκτη και του ανταποκριτή).Αυτή η τεχνολογία χρησιμοποιείται, κυρίως, από μικρές συσκευές που ονομάζονται ibeacons που εισήχθησαν από την Apple για να επωφεληθούν από τα πλεονεκτήματα του BLE, ειδικά για εσωτερικό εντοπισμό τοποθεσίας.

Μέσω της δυνατότητας χρησιμοποίησης των παραπάνω τεχνικών για την ανίχνευση της θέσης μιας συσκευής μπορούν να προσφερθούν ακριβείς πληροφορίες θέσης, όπως στην περίπτωση ενός αισθητήρα GPS ή για έναν πάροχο να χρησιμοποιεί τις πληροφορίες αυτές για να βρει την τοποθεσία του χρήστη εφόσον έχει δώσει πρώτα την συγκατάθεση του. Αντίθετα με την μετάδοση των δεδομένων θέσης που εκπέμπονται από τη συσκευή του χρήστη τα οποία δεν είναι ανώνυμα (όμως για να γίνει αυτό απαιτείται η χρήση σύνδεσης δικτύου), επιπλέον για να γίνει αυτό χρειάζεται ειδικό λογισμικό ή διάφορες διεργασίες οι οποίες θα πρέπει να εκτελούνται στις συσκευές των χρηστών. Στις επόμενες παραγράφους θα επικεντρωθούμε στον τρόπο με τον οποίο η ανίχνευση θέσης μπορεί να επιτευχθεί χωρίς την ανάγκη ειδικής εφαρμογής ή την ανάμιξη του χρήστη, παρόμοια με την περίπτωση του Wi-Fi, αλλά για μικρότερο εύρος.

Χρησιμοποιώντας BLE για τον προσδιορισμό θέσης αντί για Wi-Fi modules είναι παρόμοιο με τη λύση που παρουσιάστηκε νωρίτερα για το Wi-Fi Media Access Control Scanners. Όπως στην περίπτωση του Wi-Fi, έτσι

και στην χρήση τεχνολογίας Bluetooth υπάρχουν προτάσεις για την πρακτική χρήση της στην αναγνώριση τοποθεσιών. Για παράδειγμα [8], οι Bluetooth Media Access Control Scanners χρησιμοποιούνται για να συλλάβουν το MAC-ID των συσκευών που έχουν ενεργοποιημένο το Bluetooth. Δεδομένου ότι πρόσφατα ο αριθμός αυτών των συσκευών έχει αυξηθεί γρήγορη η παραπάνω λύση μπορεί να παρέχει μια εκτίμηση σχετικά με το πλήθος των ανθρώπων σε μια περιοχή. Επιπλέον, περιγράφεται ότι μια BLE συσκευή μπορεί να είναι σε δύο κύριες καταστάσεις και σε επτά υπό-καταστάσεις.

Οι δύο κύριες καταστάσεις είναι η κατάσταση αναμονής, όπου η συσκευή δεν αλληλεπιδρά με το περιβάλλον, και η κατάσταση σύνδεσης, όπου γίνεται μεταφορά δεδομένων μεταξύ των συνδεδεμένων συσκευών. Για τις επιμέρους καταστάσεις του connection mode(κατάσταση σύνδεσης), οι διαφορετικές καταστάσεις περιλαμβάνουν inquiry, inquiry-scan, inquiry response, page, page scan, slave response and master response modes. Ο απαιτούμενος χρόνος για το inquiry mode είναι πολύ περισσότερος από τον προσδοκώμενο όταν χρησιμοποιείτε το Wi-Fi, και είναι ίσο με 10.24 δευτερόλεπτα για το σάρωμα κάθε μιας από τις 79 διαθέσιμες συχνότητες του BT (είναι μεταξύ 2.402 GHz και 2.48 GHz), χωρισμένα σε 32 κανάλια. Δυστυχώς, δεδομένου ότι ο χρόνος ανίχνευσης είναι αρκετά μεγάλος (λόγω του αυξημένου inquiry time) η απόσταση της κάθε συσκευής με ενεργοποιημένο BT είναι κρίσιμης σημασίας ως προς την επιτυχία της σύλληψης του Id της του που μπορεί να οδηγήσει σε εκτίμηση όσον αφορά την κίνησή της.

Σε μια άλλη περίπτωση [17], η χρήση των ibeacons προτείνεται για την εύρεση της τοποθεσίας του ιδιοκτήτη είτε σε εξωτερικούς χώρους ή, κατά προτίμηση, σε κλειστούς χώρους.Εφόσον οι BLE συσκευές μπορούν να είναι είτε master devices(κύριες συσκευές)για να αναζητούν και να δημιουργούν πολλές συνδέσεις ή slave devices(δευτερεύουσες συσκευές) (συνδεδεμένες σε ένα single master) και η μεταφορά των δεδομένων ολοκληρώνετε στις περιοδικές συνδέσεις μεταξύ των συσκευών, η συνολική κατανάλωση ενέργειας μειώνεται σημαντικά. Ειδικά τα ibeacons μπορούν να διασκορπιστούν σε μια περιοχή και να μεταδίδουν περιοδικά ένα σήμα το οποίο μπορεί να εντοπιστεί από κάθε BLE συσκευή που στη συνέχεια είναι ικανή να υπολογίσει την απόσταση από τη συσκευή μετάδοσης .Επιπλέον [18], σε μια προσέγγιση για την αύξηση της ακρίβειας εντοπισμού η οποία επιτυγχάνεται με την βοήθεια συσκευών με ενεργοποιημένο BLE και ibeacons έχει προταθεί και μελετάται , χρησιμοποιώντας έναν μαθηματικό τύπο που ενισχύει τον αλγόριθμο φιλτραρίσματος σωματιδίων για την επίτευξη υψηλότερων αποτελεσμάτων προσδιορισμού τοποθεσίας.

2.9 iBeacon

Τα ibeacons αναπτύχθηκαν από την Apple και παρουσιαστήκαν στο κοινό το 2013 στο συνέδριο της Apple στην Καλιφόρνια[19]. Έπειτα και άλλες εταιρίες δημιούργησαν τα δικά τους ¨ibeacon¨ τα οποία τυπικά τα λέμε απλώς

beacons. Τα ibeacons λοιπόν είναι χαμηλής ισχύος πομποί , εξοπλισμένοι με Bluetooth χαμηλής ενέργειας ή BLE(Bluetooth Low Energy) ονομάζονται επίσης Bluetooth 4.0 ή Bluetooth Smart, οι οποίοι μεταδίδουν ραδιοσήματα. Τα ibeacons είναι απλές συσκευές οι οποίες αλληλεπιδρούν με smartphones και tablets όταν βρίσκονται εντός της εμβέλειας τους ώστε να εκτελέσουν κάποιες ενέργειες.[20][21]

Τα ραδιοσήματα που εκπέμπουν τα ibeacons είναι ένα μοναδικό αναγνωριστικό (universally unique identifier (UUID)) [22] το οποίο τους δόθηκε από μια συμβατή εφαρμογή ή από ένα λογισμικό και χρησιμοποιείτε για να ξεχωρίζουμε τα ibeacon μεταξύ τους. Επιπλέον με αυτό το αναγνωριστικό σε συνδυασμό με κάποια άλλα byte που στέλνει το ibeacon μπορούμε να βρούμε την φυσική τοποθεσία της συσκευής[23] είτε να ανιχνεύσουμε ανθρώπους είτε να ενεργοποιήσουμε με βάση την τοποθεσία της συσκευής μια ενέργεια όπως να έρθει μια ειδοποίηση στο κινητό μας η οποία να μας ενημερώνει για κάτι σχετικό με τον χώρο τον οποίο βρισκόμαστε. Αυτές οι ειδοποιήσεις ονομάζονται push notifications και λειτουργούν ακόμα και όταν η οθόνη του κινητού είναι απενεργοποιημένη.

Τα ibeacons μαζί με την βοήθεια ενός smartphone μπορούν να βρουν όπως είπαμε την θέση μας στο χώρο, έτσι λοιπόν μπορούμε να φτιάξουμε ένα GPS[24][25] για εσωτερικούς χώρους. Τα ibeacons διαφέρουν από άλλες τεχνολογίες εντοπισμού διότι πρέπει ο χρήστης να έχει μια συγκεκριμένη εφαρμογή στην συσκευή του ώστε να αλληλεπιδράσει με τα ibeacon οπότε δεν γίνετε να τον ανιχνεύσει κάποιος όταν περνά κοντά από ένα ibeacon χωρίς την συγκατάθεση του.

Εικόνα 2.4 Διάφορα είδη iBeacon [26]

2.10 Εμβέλεια ibeacon

Μια συσκευή iOS η οποία λαμβάνει σήμα από ένα ibeacon μπορεί να υπολογίσει την απόσταση του από το ibeacon. Η απόσταση μεταξύ του ibeacon και της συσκευής χωρίζετε σε 3 κατηγορίες[27].

- Άμεση: Λίγα εκατοστά
- Κοντινή: Μερικά μέτρα
- Μακρινή: Μεγαλύτερη από 10 μέτρα

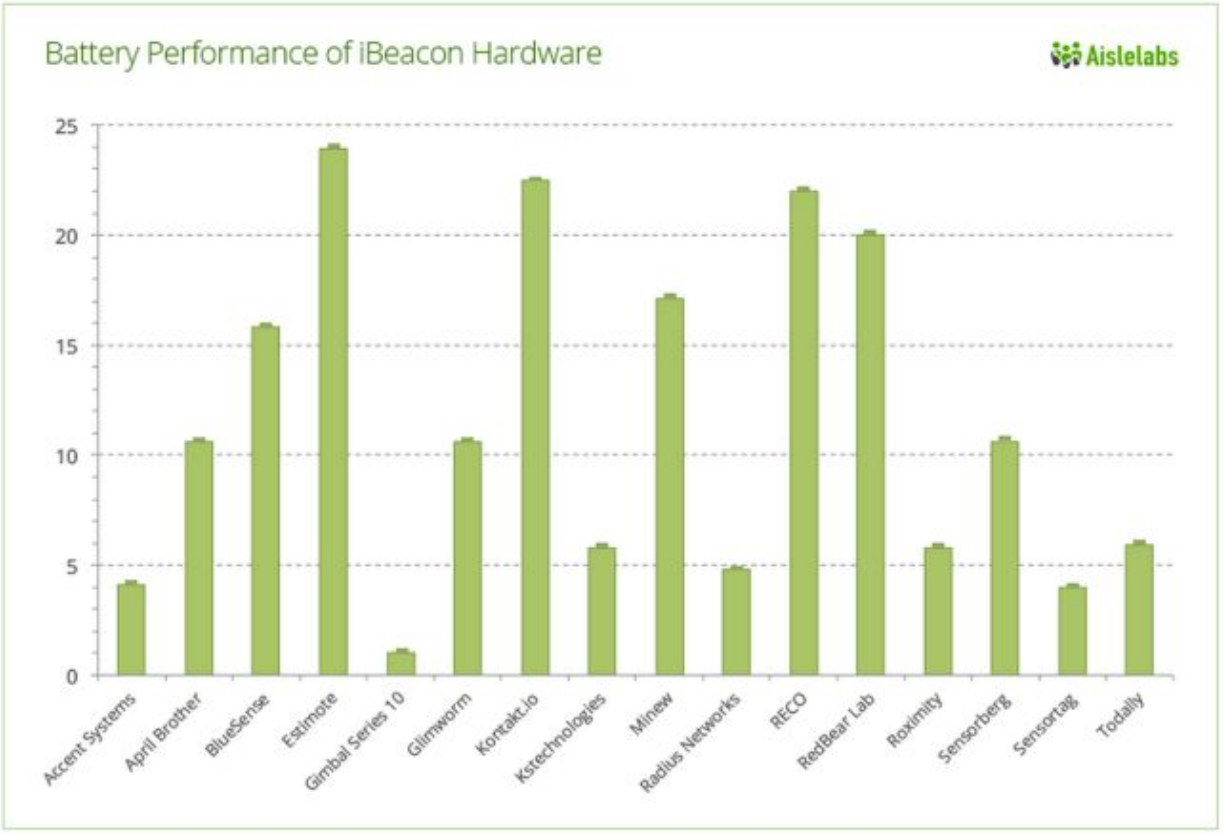
Όπως προαναφέραμε ένα ibeacon μπορεί να μας πει πότε ένας χρήστης εισέρχεται ή εξέρχεται από την εμβέλεια του, ούτος ώστε να είναι ικανό να κάνει διαφορετικές ενέργειες η συσκευή ανάλογα σε ποιά από τις παραπάνω κατηγορίες εμβελείας βρίσκετε[28]. Η μέγιστη απόσταση εκπομπής ενός ibeacon εξαρτάται από πολλούς παράγοντες όπως η τοποθεσία και η θέση του στον χώρο, καθώς και το αν βρίσκετε μέσα σε κάποια θήκη, κουτί ή τσάντα. Γενικά όμως τα συνηθισμένα ibeacon εκπέμπουν μέχρι και 70 μέτρα. Τέλος υπάρχουν και τα ibeacon μεγάλης εμβέλειας τα οποία φτάνουν μέχρι και τα 450 μέτρα.

2.11 Ρυθμίσεις

Κάθε ibeacon έχει της δικές του συγκεκριμένες ρυθμίσεις παρόλα αυτά όμως με το κατάλληλο λογισμικό μπορούμε να τις διαμορφώσουμε όπως θέλουμε. Αυτό που μπορούμε να αλλάξουμε είναι η συχνότητα μετάδοσης των ραδιοσημάτων καθώς και την ισχύ τους, αυτές οι αλλαγές όμως επηρεάζουν και την διάρκεια ζωής της μπαταρίας του ibeacon. Άλλες αλλαγές που μπορούμε να κάνουμε είναι να αλλάξουμε το UUID το οποίο είναι ένα μοναδικό αναγνωριστικό του ibeacon και περιέχει 32 δεκαεξαδικά ψηφία, χωρίζεται σε 5 ομάδες, που χωρίζονται με παύλες και μοιάζει κάτι σαν – f8856da6-4fa1-4e98-8064-bc5b71e0592e.Τέλος είναι εφικτό να αλλάξουμε ελάχιστη (minor) και την μεγίστη (major) τιμή του ibeacon .Αυτές οι 2 τιμές είναι αριθμοί από 0 έως 65.535 και χρησιμοποιούνται για μεγαλύτερη ακρίβεια στο να αναγνωρίσουμε ένα ibeacon από το να χρησιμοποιήσουμε μόνο το UUID του.[29]

2.12 Κατανάλωση ενέργειας

Το πρωτόκολλο BLE είναι σημαντικά πιο αποτελεσματικό από τα κλασικά Bluetooth. Αρκετές εταιρίες όπως η Texas Instruments [30] και η Nordic Semiconductor φτιάχνουν πλέον ειδικά chipset δηλαδή ολοκληρωμένα κυκλώματα αποκλειστικά για ibeacon. Η κατανάλωση ενέργειας του ibeacon εξαρτάται από την συχνότητα μετάδοσης και την ισχύ των σημάτων που στέλνει. Μια μελέτη που έγινε ανάμεσα σε 16 εταιρίες παράγωγης ibeacon έδειξε πως η διάρκεια ζωής του κυμαίνετε από 1 έως 24 μήνες. Οι προκαθορισμένες ρυθμίσεις της Apple μαζί με μια απλή στρογγυλή μπαταριά λιθίου μπορεί να κρατήσει 1-3 μήνες αν αλλάξουμε όμως την συχνότητα μετάδοσης η μπαταριά μπορεί να διαρκέσει από 2 έως 3 χρόνια[31]. Ένας ακόμα σημαντικός παράγοντας που επηρεάζει την διάρκεια ζωής της μπαταρίας είναι χρόνος ο όποιος σαρώνει το κινητό για τα ibeacon καθώς και το πόσες φορές γίνετε το σάρωμα[32]. Τέλος σημαντικό είναι να αναφέρουμε ότι μια έρευνα της Aislelabs [33] έδειξε ότι τα παλαιότερα μοντέλα κινητών καταναλώνουν πιο πολύ μπαταρία από τα ibeacon σε σχέση με νεότερα μοντέλα. Συγκριμένα το iphone4s καταναλώνει 11% της μπαταριάς την ώρα ενώ το iphone5s 5% [34].



Εικόνα 2.5 Απόδοση μπαταρίας του iBeacon ανάλογα την εταιρεία κατασκευής του [35]

2.13 Ιστορική Εξέλιξη

Στα μέσα του 2013 η Apple παρουσίασε τα ibeacon και οι ειδικοί έγραψαν για το πώς σχεδιαστήκαν στο να βοηθήσουν την βιομηχανία λιανικού εμπορίου απλοποιώντας τις πληρωμές και αξιοποιώντας τις προσφορές των διαφόρων ιστοσελίδων. Το Δεκέμβριο του 2013 η Apple ενεργοποίησε τα ibeacons σε 254 καταστήματα λιανικής πώλησης των ΗΠΑ[36]. Τα McDonalds έχουν χρησιμοποιήσει τα ibeacon για να δώσουν ειδικές προσφορές για τους καταναλωτές στα καταστήματα της[37]. Τον Μάιο του 2014 βγήκαν στην αγορά διάφορα ibeacon το καθένα με δικά του προεγκατεστημένα χαρακτηριστικά όσον αφόρα την ισχύ και την συχνότητα μετάδοσης[38]. Κάποια από αυτά μπορούν να εκπέμψουν σε χαμηλές συχνότητες 1Hz και αλλά σε γρήγορες όπως τα 10Hz. Τα ibeacon είναι ακόμα καινούρια τεχνολογία και ακόμα εξελίσσετε. Θεωρητικά όλες οι συσκευές οι οποίες έχουν BLE μπορούν να ανιχνεύσουν τα ibeacon. Όσον αφορά τις συσκευές οι οποίες τρέχουν λογισμικό Android πρέπει η έκδοση τους να είναι από Android 4.3+ και πάνω ώστε να μπορέσουν να ανιχνεύσουν ένα ή περισσότερα ibeacon[39]. Ενώ αν η έκδοση είναι από Android 5.0 ("Lollipop") και πάνω η συσκευή μπορεί να μετατραπεί και η ίδια σε ibeacon.

2.14 Συμβατές συσκευές

- iOSσυσκευέςμεBluetooth 4.0 (iPhone 4S και μετά , iPad (Τρίτη γενιά) καιμετά, iPad Mini (πρώτη γενιά) και μετά, iPod Touch (Πέμπτη γενιά))[40][41]
- Macintosh υπολογιστές με λειτουργικό XMavericks (10.9) καιBluetooth 4.0
- Android 4.3+ (π.χ. Samsung Galaxy S3/S4/S5/S6/S7, Samsung Galaxy Note 2/3/4, G3/G4/G5)
- Windows Phone συσκευές με την Lumia Cyan αναβάθμιση ή παραπάνω.

2.15 Περιπτώσεις και παραδείγματα χρησιμότητας των ibeacon

1. **Λιανικό εμπόριο**
   - Οι καταναλωτές μπορούν να βαθμολογήσουν την εμπειρία τους σε ένα κατάστημα ή εμπορικό κέντρο.
   - Οι καταναλωτές μπορούν να επισημάνουν ένα προϊόν για έναν φίλο τους που να έψαχνε για αυτό.
   - Λεπτομερείς πληροφορίες και βοήθεια για το πάρκινγκ.
   - Εμφάνιση λεπτομερειών για ένα συγκεκριμένο προϊόν όταν βάζουμε δίπλα το κινητό.
   - Εμφάνιση διαφημίσεων και ειδήσεων όταν ο πελάτης είναι σε ούρα για να περνάει ευχάριστα την ώρα του.
   - Προσφορά εκπτωτικών κουπονιών εάν οι πελάτες κάνουν κοινοποίηση το προϊόν που αγόρασαν σε ένα μέσο κοινωνικής δικτύωσης ώστε αυτό να προσελκύσει και άλλους πελάτες.
   - Αναγνώριση των παλιών πελατών ώστε να έχουν διάφορα δώρα.
   - Ενημέρωση των πελατών πότε έχει πολύ ή λίγο κόσμο το κατάστημα.
2. **Ιατροφαρμακευτική περίθαλψη**
   - Τα νοσοκομεία μπορούν να προσφέρουν χάρτη και πληροφορίες σχετικά με το που είναι κάθε τμήμα του ή για το που είναι κάποιος γιατρός ή νοσοκόμος εκείνη την στιγμή.
   - Ανακοίνωση για το πότε γίνονται δωρεάν check-up ή για το πότε κάποιο νοσοκομείο χρειάζεται αίμα.
   - Τα ασθενοφόρα μπορούν να στέλνουν ειδοποιήσεις για το ποια διαδρομή ακολουθούν εκείνη την ώρα ώστε να προειδοποιούνται οι οδηγοί για να κάνουν στην άκρη.
3. **Εκπαίδευση**

- ➢ Οι καθηγητές έξω από τις αίθουσες τους μπορούν να έχουν τοποθετημένο ibeacon που θα ενημερώνει για το τι μάθημα γίνετε μέσα στην αίθουσα καθώς και τι ώρες διεξάγεται.
- ➢ Στα Πανεπιστήμια θα δίνεται χάρτης με πληροφορίες για το που βρίσκονται όλοι οι τομείς του όπως που είναι οι διάφορες αίθουσες διδασκαλίας ή οι καφετερίες η βιβλιοθήκη και τα γήπεδα.
- ➢ Θα γίνετε αυτόματη παρουσία των μαθητών κατά την είσοδο τους στην αίθουσα το οποίο είναι χρήσιμο και για τους γονείς να ξέρουν αν τα παιδία τους έφτασαν στο σχολειό.

4. **Τουρισμό**
   - ➢ Αυτόματο check-in στα ξενοδοχεία
   - ➢ Ξεκλείδωμα της πόρτας του δωματίου καθώς και άλλες ενέργειες μέσα στο δωμάτιο όπως το άνοιγμα της τηλεόρασης.
   - ➢ Να τους στέλνουν νέα σχετικά με την περιοχή του ξενοδοχείου στο όποιο διαμένουν όπως πληροφορίες για τον καιρό ή για διαφορές εκδηλώσεις.
   - ➢ Οι υπάλληλοι ανάλογα τις ρυθμίσεις του κινητού θα γνωρίζουν την γλώσσα του πελάτη.
   - ➢ Δεν θα χρειάζεται ξεναγός διότι τα ibeacon που θα είναι τοποθετημένα στα αξιοθέατα και μέσα στα μουσεία θα ενημερώνουν τον χρήστη σχετικά με το τι είναι αυτό που βλέπει.
   - ➢ Ενημέρωση για το ποια μέρη έχουν εκείνη την στιγμή πολύ κόσμο όπως ποιά εστιατόρια, καφετερίες ή ακόμα και ποιές παράλιες.
5. **Ψυχαγωγία**
   - ➢ Ενημέρωση σχετικά με τα καλυτέρα μαγαζιά βάση βαθμολογίας.
   - ➢ Καθώς περνάμε έξω από έναν κινηματογράφο θα μας ενημερώνει για τις ώρες προβολής των ταινιών.
   - ➢ Γρήγορο check-in σε γήπεδα και συναυλίες.
6. **Ταξίδια**
   - ➢ Σε σιδηροδρομικούς σταθμούς σε λιμάνια και αεροδρόμια θα δίνεται χάρτης με οδηγίες για το που βρίσκονται οι διάφορες είσοδοι και έξοδοι καθώς και σε ποια είσοδο πρέπει να πάμε ανάλογα το εισιτήριο μας καθώς θα υπάρχει και ενημέρωση για τυχόν καθυστερήσεις.
   - ➢ Έξω από τα πρακτορεία οι χρηστές θα ενημερώνονται για προσφορές σε εισιτήρια.
   - ➢ Τοποθέτηση ibeacon στις αποσκευές για να βρεθούν ποιο γρήγορα και να μην χαθούν.
7. **Εταιρία**

- ➢ Οι υπάλληλοι θα γνωρίζουν που βρίσκονται μεταξύ τους, το οποίο θα είναι χρήσιμο και για τον διευθυντή να βλέπει αν οι υπάλληλοι του είναι στα πόστα τους.
- ➢ Αυτόματο check-in και check-out των εργαζομένων κατά την είσοδο και έξοδο τους από τον χώρο εργασίας τους.
- ➢ Ενημέρωση για το πότε λαμβάνει χώρα μια σύσκεψη όπου μετά το τέλος της θα στέλνεται η παρουσίαση(διαφορά slides) σε αυτούς που παρευρεθήκαν.

8. Αυτοκινητοβιομηχανία

- ➢ Ξεκλείδωμα του αυτοκίνητου, άνοιγμα της τάπας για την είσοδο των καυσίμων καθώς και άνοιγμα του πορτ μπαγκάζ.
- ➢ Μαζί με τους χάρτες της Google μπορεί να ειδοποιήσει για τον καιρό και την κίνηση που θα συναντήσει στην διαδρομή που επέλεξε ο χρήστης.

9. Διαφήμιση

- ➢ Οι διαφημιστικές εταιρίες χρησιμοποιούν ibeacon για ποιο δυναμικές και έξυπνες διαφημίσεις οι οποίες θα είναι προσαρμοσμένες στην γλώσσα του χρήστη ανάλογα με ποια γλώσσα έχει στις ρυθμίσεις της συσκευής του.
- ➢ Τα προϊόντα που θα διαφημίζονται θα δείχνουν στον χρήστη αν τα χρησιμοποίει κάποιος από τους φίλους του σε συνεργασία με τα μέσα κοινωνικής δικτύωσης.

10. Προσωπική χρήση

- ➢ Να ανοίγει το φως όταν εισέρχεται ο χρήστης στο σπίτι καθώς και να τον ειδοποιεί όποτε μπαίνει κάποιος άλλος.
- ➢ Να κλειδώνει αυτόματα ο υπολογιστής του όποτε φεύγει από αυτόν.
- ➢ Να τοποθετεί ο χρήστης ibeacon στα πράγματα που χάνει συχνά, ώστε να τα βρίσκει ποιο εύκολα όπως τα κλειδιά του.
- ➢ Θα μπορεί ο χρήστης να αυτοματοποιήσει τις συσκευές του σπιτιού του για να δουλεύουν όποτε θελήσει απλώς χρησιμοποιώντας το κινητό του. Όπως να ανοίξει το κλιματιστικό το πλυντήριο πιάτων και ρούχων την τηλεόραση καθώς και τον φούρνο.

11. Γενική χρήση

- ➢ Θα βοηθάει τους ανθρώπους με προβλήματα όρασης να προχωρούν δίνοντας τους φωνητικές οδηγίες για τα εμπόδια που υπάρχουν στο δρόμο τους.
- ➢ Θα δίνει οδηγίες διαφυγής από έναν χώρο έναν συμβεί σεισμός ή ξεσπάσει πυρκαγιά ώστε να οδηγήσει τον χρήστη έξω με ασφάλεια.

[42][43][44][45]

3. Πειραματική προσέγγιση

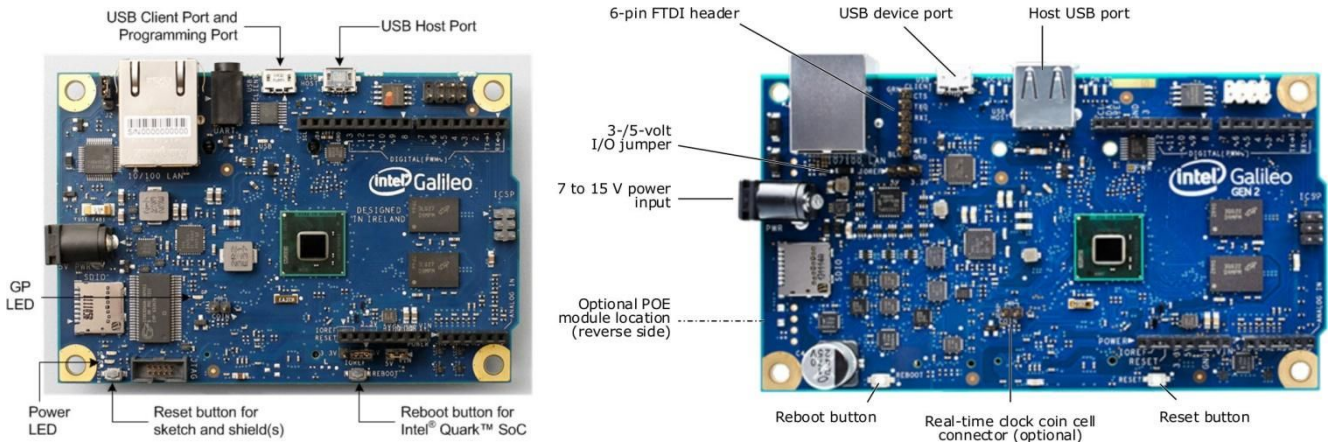
3.1 Κατασκευή ενός Passive Wi-Fi Tracker

Υπάρχουν πολλοί τρόποι για να κατασκευαστεί μια τέτοια συσκευή που θα μπορεί να ανιχνεύει τα probe request και να τα καταγράφει. Η πιο απλή λύση είναι με τη χρήση ενός προγράμματος όπως είναι το Wireshark. Με ένα ειδικό φιλτράρισμα το Wireshark μπορεί να μας καταγράφει τα probe request που ανιχνεύει. Όμως κάτι τέτοιο δεν είναι και πολύ πρακτικό και οικονομικά ασύμφορο, μιας και που για να μπορέσει κανείς να φτιάξει ένα δίκτυο από τέτοιους ανιχνευτές θα χρειαστεί πολλά laptop οπότε το κόστος θα ήταν αρκετά μεγάλο.

Γι' αυτό το λόγο μπορούμε να χρησιμοποιήσουμε πιο οικονομικές συσκευές όπως είναι τα Raspberry-Pi με ενσωματωμένο Wi-Fi αντάπτορα ή ένα μικρό TP-Link router με εγκατεστημένο ελεύθερο λειτουργικό. Τέλος υπάρχει άλλη μια λύση, και με την οποία θα ασχοληθούμε εκτενώς παρακάτω, κάνοντας χρήση μιας Galileo Gen 1 συσκευής με ενσωματωμένο αντάπτορα για Wi-Fi.

3.2 Αρχιτεκτονική συσκευής Intel Galileo

Ο CEO της εταιρείας Intel, Brian Krzanich, ανακοίνωσε στις 3 Οκτωβρίου 2013 μια συμφωνία συνεργασίας με την Arduino LLC, την κορυφαία πλατφόρμα hardware ανοιχτού λογισμικού της κοινότητας δημιουργών και εκπαίδευσης. Ο κ. Krzanich αποκάλυψε την πλακέτα «Galileo» της Intel, το πρώτο προϊόν σε μια νέα οικογένεια πλακετών ανάπτυξης συμβατών με Arduino, που χρησιμοποιούν αρχιτεκτονική Intel[1]. Το Galileo λοιπόν είναι μια πλακέτα μικροελεγκτή βασιζόμενη στον επεξεργαστή Intel®[2]η όποια έχει τις δυνατότητες ενός υπολογιστή και χρησιμοποιείτε συνήθως από άτομα χωρίς μεγάλη τεχνική κατάρτιση για την δημιουργία ενός project όπως ένα passive Wi-Fi tracker. Το μικρό του μέγεθος σε σχέση με τις δυνατότητες του το καθιστά ένα από τα πλεονεκτήματα του[11][12].



Εικόνα 3.1 Intel Galileo [13]

Πιο συγκεκριμένα τα χαρακτηριστικά του Galileo Gen 1είναι [13]:

- Κατασκευαστής: Intel Corporation
- Τιμή Γνωριμίας :63 €
- Ημέρα κυκλοφορίας: 17 Οκτωβρίου 2013
- Λειτουργικό Σύστημα: Linux(Yocto)
- Επεξεργαστής: Intel Quark X1000 400 MHz
- Μνήμη: 256 MB
- Αποθηκευτικός χώρος: Micro SD card,SDHC card
- Ισχύς: 15 W

Αντίστοιχα τα χαρακτηριστικά του GalileoGen 2 είναι [13]:

- Κατασκευαστής : Intel Corporation
- Τιμή Γνωριμίας : 65 €
- Ημέρα κυκλοφορίας : 10 Ιουλίου 2014
- Λειτουργικό Σύστημα : Linux
- Επεξεργαστής : IntelQuarkX1000 32-bit 400 MHz
- Μνήμη : 256 MB
- Αποθηκευτικός χώρος : Flash Memory, Micro SD card,EEPROM 8 kb,
- Ισχύς : 15 W

Αφού συνδέσουμε όλα τα απαραίτητα καλώδια για τη σωστή λειτουργία του Galileo, θα χρειαστούμε να εγκαταστήσουμε στον Windows υπολογιστή μας το πρόγραμμα το οποίο θα μας επιτρέψει την σειριακή επικοινωνία, μέσο του jack -RS232 καλωδίου, με το Galileo.Υπάρχουν αρκετά προγράμματα για αυτή τη δουλειά, εμείς θα χρησιμοποιήσουμε το PuTTY.

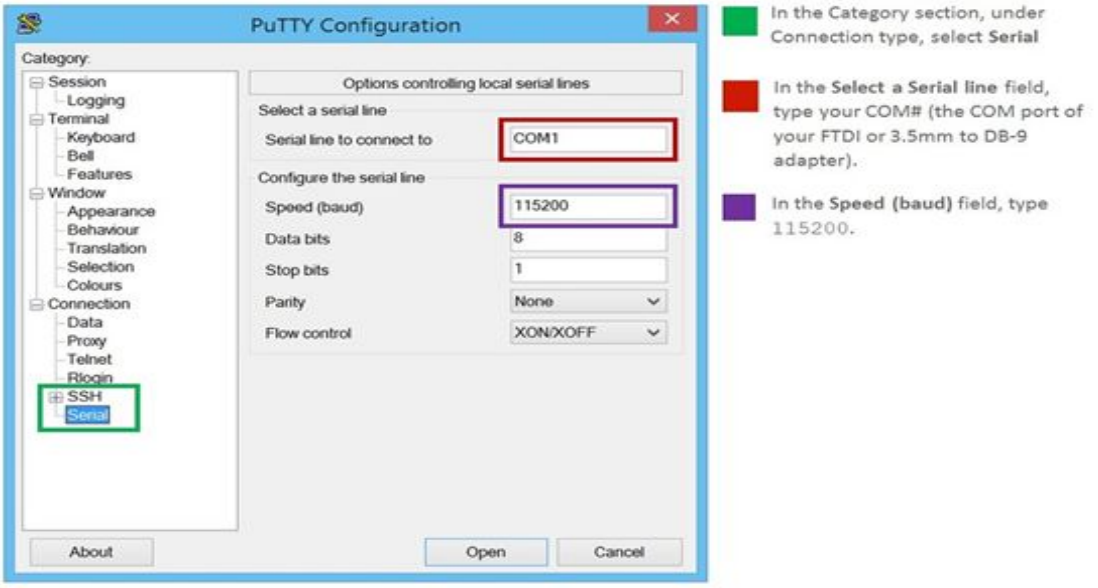
3.3 PuTTY

Το PuTTY είναι μία ελεύθερη κονσόλα τερματικής-προσομοίωσης, σειριακής-προσομοίωσης «ανοιχτού κώδικα» (OpenSource) και δικτυακή πλατφόρμα μεταφοράς αρχείων. Υποστηρίζει αρκετά πρωτόκολλα δικτύωσης

όπως SCP, SSH, Telnet, rlogin καθώς και σύνδεση socket. Επίσης μπορεί να συνδεθεί και με σειριακή πόρτα. Το πρόγραμμα αυτό αρχικά γράφτηκε για Microsoft Windows αλλά στη πορεία εκδόθηκε και για άλλα λειτουργικά.

[14]

Αφού κατεβάσουμε το PuTTY και το εγκαταστήσουμε, το τρέχουμε και το ρυθμίζουμε όπως βλέπουμε στη παρακάτω εικόνα:



Εικόνα 3.2 Ρύθμιση του Serial στο PuTTY [15]

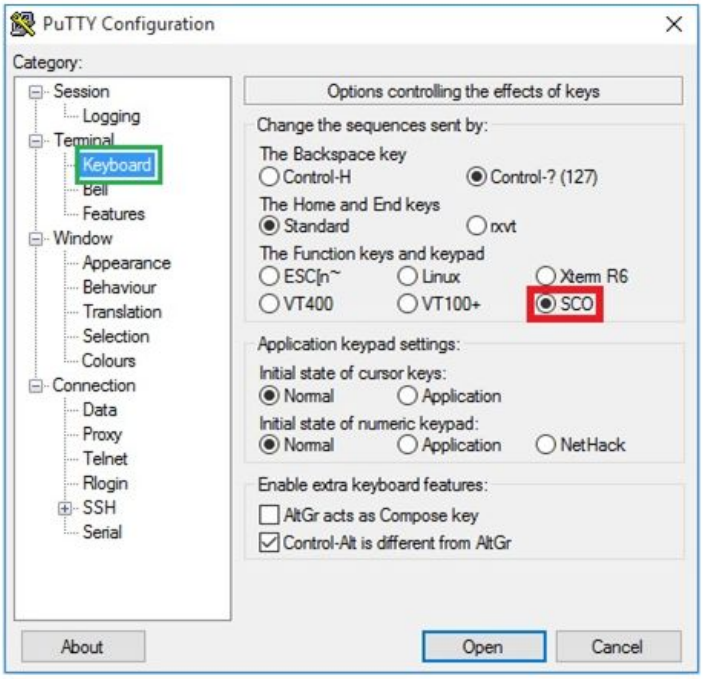
Κατεβάζουμε το PuTTY από τον παρακάτω σύνδεσμο:

[http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html]

Για να δούμε σε ποια πόρτα είναι συνδεδεμένο (π.χ. COM8), πάμε στη διαχείριση συσκευών (Device Manager)και ψάχνουμε να βρούμε τα ports. Εκεί θα δούμε τις πόρτες στις οποίες ακούνε οι συνδεμένες συσκευές.

Εικόνα 3.3 Έλεγχος πόρτας σύνδεσης [15]

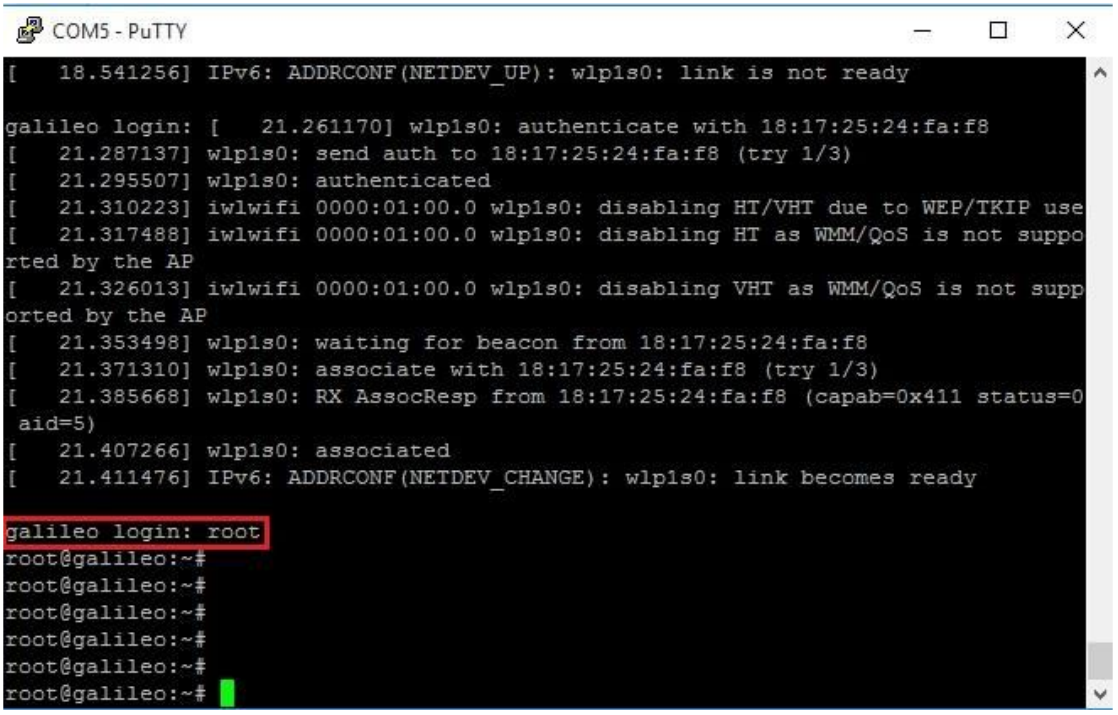
Επομένως στο serial port βάζουμε την πόρτα που βλέπουμε στη διαχείριση συσκευών και στο Speed(baud) βάζουμε την τιμή 115200.Στη συνέχεια επιλέγουμε την καρτέλα Terminal και στο Keyboard, στο Fuction of keys and keypad επιλέγουμε τη ρύθμιση SCO.



Εικόνα 3.4 Ρύθμιση του Keyboard στο PuTTY [16]

Αφού τελικός τρέξουμε το PuTTY με τις συγκεκριμένες ρυθμίσεις πατώντας το κουμπί Open κάτω δεξιά, θα εμφανιστεί ένα serial monitor στο οποίο θα ζητείται κωδικός πρόσβασης (password) όπως φαίνεται και στην εικόνα από κάτω. Ο κωδικός είναι root.

3.4 Εγκατάσταση Προγράμματος



Εικόνα 3.5 Σύνδεση στο σύστημα

Αφου βάλουμε τον κωδικό θα παρατηρήσουμε πως πλέον έχουμε συνδεθεί στο σύστημα ως root.

Πλέον είμαστε έτοιμοι να ξεκινήσουμε την εγκατάσταση των πακέτων που θα χρειαστούμε για τη σωστή λειτουργία του σκάνερ μας. Πρώτα συνδέουμε το Galileo στο διαδίκτυο μέσο της θύρας Ethernet για να μπορέσουμε να ενημερώσουμε τα προγράμματα που περιέχονται στο λειτουργικό καθώς και να εγκαταστήσουμε και νέα. Πληκτρολογούμε τις παρακάτω εντολές στο τερματικό:

root@OpenWrt:~# opkg update

root@OpenWrt:~# opkg upgrade tar wget

root@OpenWrt:~# opkg install python

Για να λειτουργήσει το πρόγραμμά μας θα πρέπει να εγκαταστήσουμε δύο ακόμα βιβλιοθήκες, είναι η tcpdump και η libpcap. Οι βιβλιοθήκες αυτές συνήθως είναι εγκατεστημένες εξαρχής σε ένα σύστημα όμως στα linuxyocto τα οποία και χρησιμοποιούμε δεν είναι. Οπότε κατεβάζουμε τις τελευταίες εκδόσεις τους από τον παρακάτω σύνδεσμο

http://www.tcpdump.org/index.html#latest-release

και περνάμε τα δύο αυτά αρχεία στην SDCard που χρησιμοποιούμε. Στη συνέχεια μέσα από το Galileo αντιγράφουμε τα δύο αρχεία από την κάρτα

μνήμης (SDCard)σε κάποιο φάκελο (directory) του Galileo και ξεκινάμε την εγκατάστασή τους.

Π.χ.

```
# cp tcpdump-3.8.1.tar.gz /usr/local/src/
# cp libpcap-0.8.1.tar.gz /usr/local/src/
# cd /usr/local/src
# tar -zxvf tcpdump-3.8.1.tar.gz
# tar -zxvf libpcap-0.8.1.tar.gz
# cd libpcap-0.8.1
# ./configure ; make ; make install
# cd ../tcpdump-3.8.1
# ./configure ; make ; make install
```

[16]

Ένα επιπλέον πρόγραμμα που θα πρέπει να εγκαταστήσουμε είναι το scapy. Το scapy κάνει διαχείριση των πακέτων του δικτύου, εμείς θα το χρειαστούμε ώστε να συλλέγουμε και να καταγράφουμε τα proberequest. Με τον ίδιο τρόπο που εγκαταστήσαμε τις παραπάνω βιβλιοθήκες θα εγκαταστήσουμε και το scapy. Κατεβάζουμε στον υπολογιστή μας, την τελευταία έκδοση από εδώ (http://www.secdev.org/projects/scapy/files/scapy-latest.tar.gz) και το περνάμε στην μνήμη του Galileo (SDCard).Έπειτα δημιουργούμε ένα φάκελο directory μέσα στο Galileo με το όνομα scapykαι αντιγράφουμε από την SDCard το αρχείο που περάσαμε για την εγκατάσταση του scapy.

```
# cp scapy-latest.tar.gz ~/scapy
# tar -xvf scapy-latest.tar.gz
# cd scapy*
# python setup.py install
# cd ..; rm -rf scapy*
```

```
root@OpenWrt:~# mkdir /overlay; cd /overlay
```

```
root@OpenWrt:/overlay/scripts# wget http://bitbucket.org/edkeeble/wifi-scan/get/e2a08627f05d.zip --no-check-certificate -O wifiscan.zip

root@OpenWrt:/overlay/scripts# unzip wifiscan.zip

root@OpenWrt:/overlay/scripts# mv edkeeble-wifi-scan-e2a08627f05d wifi-scan

root@OpenWrt:/overlay/scripts# cd ~
```

Στη συνέχεια θα χτυπήσουμε την εντολή **ifconfig** η οποία θα μας δείξει τα στοιχεία για το ενσύρματο και ασύρματο δίκτυο. Αυτό όμως που μας ενδιαφέρει από τη συγκεκριμένη εντολή είναι να δούμε το όνομα του ασύρματου δικτύου το οποίο θα χρησιμοποιήσουμε παρακάτω. Στην παρακάτω εικόνα βλέπουμε το αποτέλεσμα που μας επιστρέφει η παραπάνω εντολή

```
root@galileo:~# ifconfig
enp0s20f6 Link encap:Ethernet  HWaddr 98:4F:EE:00:33:02
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:1042 (1.0 KiB)
          Interrupt:45 Base address:0x4000

enp0s20f6:avahi Link encap:Ethernet  HWaddr 98:4F:EE:00:33:02
          inet addr:169.254.4.2  Bcast:169.254.255.255  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          Interrupt:45 Base address:0x4000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:164 errors:0 dropped:0 overruns:0 frame:0
          TX packets:164 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14852 (14.5 KiB)  TX bytes:14852 (14.5 KiB)

wlp1s0    Link encap:Ethernet  HWaddr C8:F7:33:C4:5C:D9
          inet addr:192.168.1.70  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2a02:2149:811c:300:caf7:33ff:fec4:5cd9/64 Scope:Global
          inet6 addr: fe80::caf7:33ff:fec4:5cd9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:482 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:31846 (31.0 KiB)  TX bytes:16229 (15.8 KiB)

root@galileo:~#
```

Εικόνα 3.6 Εκτέλεση εντολής ifconfig

Βλέπουμε πως το όνομα του ασύρματου δικτύου είναι το **wlp1s0** καθώς και τα στοιχεία του. Στη συνέχεια θα θέσουμε τη λειτουργία του ασύρματου δικτύου σε λειτουργία επιτήρησης (monitor mode) για να μπορούμε να ξεκινήσουμε την καταγραφή των ασύρματων δικτύων.

Ξεκινάμε με την εντολή **ifconfig wlp1s0 down** η οποία απενεργοποιεί το ασύρματο δίκτυο (Wi-Fimodule) της συσκευής ώστε να μας επιτραπεί η τροποποίηση της λειτουργίας του. Ακολουθεί η εντολή **iwconfig wlp1s0 mode monitor** η οποία θέτει τη λειτουργία του Wi-Fi σε monitor mode. Τέλος πληκτρολογούμε την **ifconfig wlp1s0 up** ώστε να θέσουμε πάλι σε λειτουργία το Wi-Fi, αυτή τη φορά όμως δε θα διαφημίζει τη παρουσία του στο χώρο αλλά απλώς θα ακούει για άλλα δίκτυα. Η παρακάτω εικόνα δείχνει στη πράξη όλες τις παραπάνω εντολές.

```
root@galileo:~# ifconfig wlp1s0 down
[  526.738231] wlp1s0: deauthenticating from 18:17:25:24:fa:f8 by local choice (reason=3)
[  526.781458] cfg80211: Calling CRDA to update world regulatory domain
root@galileo:~# iwconfig wlp1s0 mode monitor
root@galileo:~# ifconfig wlp1s0 up
[  544.258162] iwlwifi 0000:01:00.0: L1 Disabled; Enabling L0S
[  544.271869] iwlwifi 0000:01:00.0: Radio type=0x2-0x1-0x0
root@galileo:~# ifconfig wlp1s0
wlp1s0    Link encap:UNSPEC  HWaddr C8-F7-33-C4-5C-D9-E5-DE-00-00-00-00-00-00-00-00
          inet addr:192.168.1.70  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:1027 errors:0 dropped:0 overruns:0 frame:0
          TX packets:124 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:64973 (63.4 KiB)  TX bytes:23118 (22.5 KiB)

root@galileo:~# iwconfig wlp1s0
wlp1s0    IEEE 802.11abgn  Mode:Monitor  Tx-Power=15 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

root@galileo:~#
```

Εικόνα 3.7 Εκτέλεση εντολών

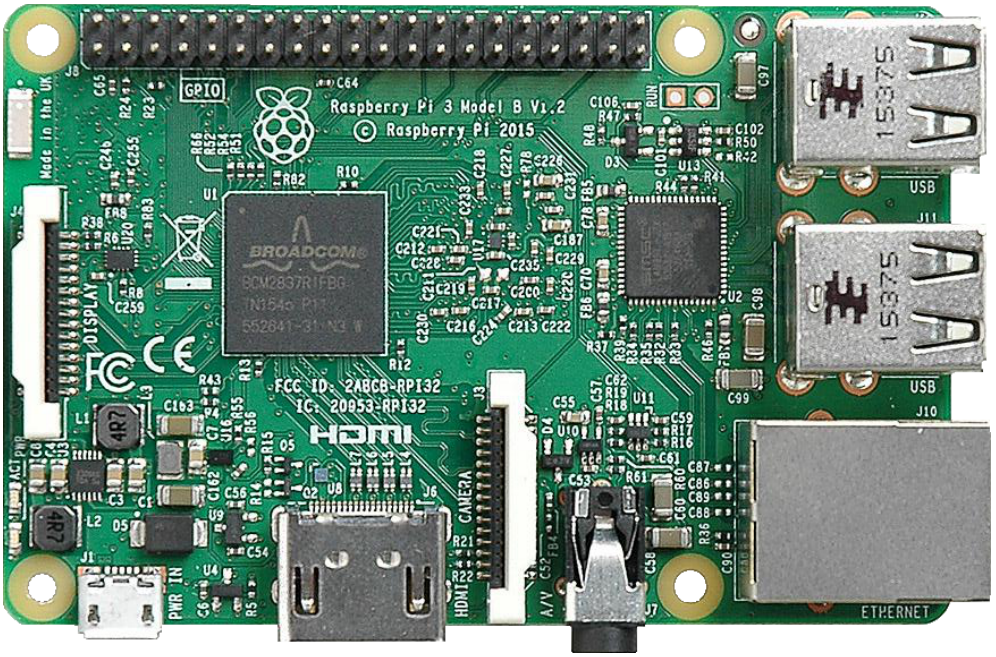
Χτυπώντας ξανά την εντολή **iwconfig wlp1s0** θα δούμε πως το Wi-Fiέχει τεθεί σε λειτουργία monitor. Τέλος πάμε και τρέχουμε το αρχείο crowdsensing.py όπως βλέπουμε στην παρακάτω εικόνα, το οποίο θα αρχίσει και την καταγραφή των Wi-Fi συσκευών που υπάρχουν στην περιοχή.

```
root@galileo:~# cd overlay
root@galileo:~/overlay# ls -l
total 16
-rwxr-xr-x 1 root root 1466 Jul 17 17:41 crowdsensing.py
-rw-r--r-- 1 root root 5035 Sep 18 11:03 file
drwxr-xr-x 3 root root 4096 Jul 17 16:59 scripts
root@galileo:~/overlay# python crowdsensing.py wlp1s0
WARNING: No route found for IPv6 destination :: (no default route?)
[2016-09-20 20:58:01.825719] Starting scan
Scan[  822.578031] device wlp1s0 entered promiscuous mode
ning for:
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source: ec:9b:f3:6e:f5:40 SSID:  RSSi: -50
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source: ec:9b:f3:6e:f5:40 SSID:  RSSi: -50
```

Εικόνα 3.8 Καταγραφή Wi-Fi συσκευών

3.5 Κατασκευή ibeacon με Raspberry Pi

Το Raspberry Pi είναι ένας πλήρης υπολογιστής σε πολύ μικρό μέγεθος. Παρά το μικρό μέγεθος , το Raspberry Pi στην τελευταία του έκδοση διαθέτει τετραπύρηνο επεξεργαστή 1200MHz, διπύρηνη κάρτα γραφικών, 1GB RAM, τέσσερις θύρες USB, έξοδο HDMI, τροφοδοτείται μέσω Micro USB, και έχει 40 pins γενικής χρήσης για σύνδεση με άλλα ηλεκτρονικά και περιφερειακά.[46]



Εικόνα 3.9 Raspberry Pi [46]

3.6 Μετατροπή Raspberry Pi1 και Pi2 σε ibeacon

Για να μετατρέψουμε ένα RaspberryPi 1/2 σε ibeacon πρέπει να ακολουθήσουμε τα παρακάτω βήματα.

Βήμα 1: Κατάλληλος εξοπλισμός

Αυτά που θα χρειαστούμε είναι τα παρακάτω:

- Raspberry Pi1 ή Pi2
- Κάρτα μνήμης τύπου SD/MicroSD χωρητικότητας από 4GB και πάνω
- Bluetooth 4.0 (BLE) USB module
- Ένα καλώδιο USBA/MicroB ,ένα καλώδιο HDMI και ένα Ethernet
- Πληκτρολόγιο, ποντίκι και οθόνη

Βήμα 2: Κατέβασμα του σωστού λειτουργικού

Το λειτουργικό σύστημα που θα χρησιμοποιήσουμε ονομάζετε RASPBIAN JESSIE και μπορούμε να το κατεβάσουμε δωρεάν από την σελίδα της Raspberry στον ακόλουθο σύνδεσμο [47].

Βήμα 3: Εγγραφή του λειτουργικού στην κάρτα SD

Υπάρχουν πολλά λογισμικά που μπορούν να μας βοηθήσουν σε αυτό το βήμα, ένα από αυτά είναι το Win32 Disk Imager.

Βήμα 4: Σύνδεση του Raspberry

- Τοποθετούμε την κάρτα SD στην ειδική εσοχή που έχει το Raspberry.
- Συνδέουμε στις θύρες USB του Raspberry το ποντίκι το πληκτρολόγιο και το Bluetooth 4.0 USB module.
- Συνδέουμε το καλώδιο Ethernetστο Raspberry.
- Με την βοήθεια του καλωδίου HDMI συνδέουμε το Raspberry σε μια οθόνη.
- Συνδέουμε το καλώδιο USBA/MicroB στο Raspberry και είτε σε έναν υπολογιστή είτε σε έναν μετασχηματιστή 5V

Βήμα 5: Εκκίνηση του Raspberry και εγκατάσταση βιβλιοθηκών

Όταν συνδέσουμε το Raspberry στην τροφοδοσία με το καλώδιο USBA/MicroB κάνει εκκίνηση αυτόματα .Μόλις λοιπόν ανοίξει και βρεθούμε στην αρχική οθόνη ανοίγουμε το τερματικό (terminal) και πληκτρολογούμε τις παρακάτω εντολές που θα εγκαταστήσουν τις απαραίτητες βιβλιοθήκες ώστε

να εκπέμψει το Raspberry σαν ibeacon. Για να κατεβάσουμε αυτές τις βιβλιοθήκες χρειαζόμαστε ίντερνετ αλλά εφόσον στο προηγούμενο βήμα συνδέσαμε το καλώδιο Ethernet δεν θα έχουμε πρόβλημα διότι συνδέετε αυτόματα στο διαδίκτυο χωρίς να κάνουμε εμείς κάποια ενέργεια.

```
sudo apt-get install libusb-dev
sudo apt-get install libdbus-1-dev
sudo apt-get install libglib2.0-dev --fix-missing
sudo apt-get install libudev-dev
sudo apt-get install libical-dev
sudo apt-get install libreadline-dev
```

Μόλις εκτελεστούν αυτές οι εντολές πρέπει να κατεβάσουμε και μια βιβλιοθήκη που άφορα το Bluetooth 4.0 USB module και λέγεται BlueZ. Η έκδοση BlueZ που θα κατεβάσουμε είναι η BlueZ 5.41 η οποία είναι και η πιο πρόσφατη μέχρι στιγμής. Οι εντολές που πρέπει να πληκτρολογήσουμε είναι οι παρακάτω:

```
Sudomkdirbluezcdbluezsudowgetwww.kernel.org/pub/linux/bluetooth/bluez-5.41.tar.gzsudogunzipbluez-5.41.tar.gzsudotarxvfbluez-5.41.tarcdbluez-5.41
sudo ./configure --disable-systemd sudo make sudo make install sudo shutdown -r now
```

[48]

Βήμα 6: Ενεργοποίηση εκπομπής του Raspberry σαν ibeacon

Όπως έχουμε εξηγήσει το ibeacon έχει κάποιες τιμές οι οποίες είναι το UUID το Major και το Minor. Τα ibeacon που υπάρχουν στην αγορά έχουν προεγκατεστημένες αυτές τις τιμές στο Raspberry όμως πρέπει να τις ορίσουμε εμείς. Οι τιμές που θα εκχωρήσουμε είναι τυχαίες και θα είναι οι παρακάτω.

UUID:C6 41 8F 30 F5 F8 46 6D AF F8 32 54 6B 27 FE 6D

Major:00 B2

Minor:00 04

Η εντολή που θα εκτελέσουμε στο τερματικό για να οριστούν αυτές οι τιμές είναι η ακόλουθη:

```
sudo hcitool cmd 0x08 0x0008 1E 02 01 1A 1A FF 4C 00 02 15 C6 41 8F 30 F5 F8 46 6D AF F8 32 54 6B 27 FE 6D 00 B2 00 04 C8
```

Σημείωση1: Τα ψηφία 4C 00 είναι αυτά που ορίζουν την συσκευή ως ibeacon, υπάρχουν αντίστοιχα άλλα ψηφία ως αναγνωριστικά για άλλα είδη beacon. **Σημείωση2**: Το ψηφίο C8 είναι αυτό που ορίζει ισχύ της εκπομπής στο 1 μέτρο.

Αφού εκτελέσουμε την παραπάνω εντολή πληκτρολογούμε την επόμενη εντολή:

```
sudo hcitool cmd 0x08 0x000A 01
```

για να αρχίσει το Raspberry να εκπέμπει σαν ibeacon
Αν θέλουμε να σταματήσουμε την εκπομπή πληκτρολογούμε την παρακάτω εντολή:

```
sudo hcitool cmd 0x08 0x000A 00
```

[49]

Βήμα 7: Έλεγχος ibeacon

Για να ελέγξουμε αν το Raspberry εκπέμπει ως ibeacon μπορούμε να κατεβάσουμε δωρεάν μια εφαρμογή από το appstore για συσκευές iOS ή από το Google playstore για συσκευές Android. Μια τέτοια εφαρμογή είναι η Locate Beacon ή η iBeacon Detector

3.7 Μετατροπή Raspberry Pi3 σε ibeacon

Η μετατροπή ενός Raspberry Pi3 σε ibeacon είναι ποιο γρήγορη διαδικασία σε σχέση με τα προηγούμενα μοντέλα και αυτό διότι στο συγκεκριμένο μοντέλο υπάρχει ενσωματωμένο Bluetooth 4.0.Οπότε δεν χρειάζεται να εγκαταστήσουμε καμία επιπλέον βιβλιοθήκη. Άρα το μόνο που έχουμε να κάνουμε είναι να ακολουθήσουμε τα παραπάνω βήματα παραλείποντας το κομμάτι στο βήμα 5 που λέει για την εγκατάσταση βιβλιοθηκών.

3.8 Κατασκευή εφαρμογής Android

Αρχικά να αναφέρουμε ότι το Android είναι ένα λειτουργικό σύστημα για smartphones και tablets το οποίο αναπτύσσεται από την Google και είναι βασισμένο σε Linux.Οι εφαρμογές του γράφονται κυρίως με την αντικειμενοστραφή γλώσσα Java και αναπτύσσονται σε προγραμματιστικά περιβάλλοντα όπως το Eclipse και το Android Studio. [50]

Η συγκεκριμένη εφαρμογή είναι ανεπτυγμένη σε Android Studio το οποίο μπορούμε να το κατεβάσουμε δωρεάν από το παρακάτω link :

https://developer.android.com/studio/index.html

Τέλος να αναφέρουμε ότι για την ανάπτυξη της συγκεκριμένης εφαρμογής χρησιμοποιήσαμε την βιβλιοθήκη Android Beacon Library (AltBeacon) η οποία είναι διαθέσιμη στον παρακάτω σύνδεσμο :

https://altbeacon.github.io/android-beacon-library/

Activity_monitoring.xml

```
<RelativeLayout
xmlns:android="http://schemas.android.com/apk/res/android"
xmlns:tools="http://schemas.android.com/tools"

android:layout_width="match_parent"
android:layout_height="match_parent"
tools:context=".MonitoringActivity"
android:background="#426ad7">
<TextView
android:id="@+id/textView1"
android:layout_width="wrap_content"
android:layout_height="wrap_content"
android:layout_alignParentLeft="true"
android:layout_alignParentTop="true"
android:layout_marginTop="17dp"
android:text="Monitoring Events:"
android:textColor="#000000" />

<Button
android:id="@+id/Button01"
android:layout_width="wrap_content"
android:layout_height="wrap_content"
android:padding="10dp"
android:textColor="#000000"
android:background="@drawable/mybutton"
android:onClick="onRangingClicked"
android:text="Start Tracking"
android:clickable="true"
android:layout_centerVertical="true"
android:layout_centerHorizontal="true" />

<TextView
android:layout_width="wrap_content"
android:layout_height="wrap_content"
android:textAppearance="?android:attr/textAppearanceLarge"
android:id="@+id/textNotif"
android:layout_alignParentEnd="true"
android:layout_alignParentStart="true"
android:layout_below="@+id/textView1" />

</RelativeLayout>t
```

ΤοαρχείοActivity_monitoring.xml ορίζει το γραφικό περιβάλλον (interface) του προγράμματος. Δηλαδή την στοίχιση των textbox και των κουμπιών στην οθόνη της συσκευής, που όλα αυτά συνθέτουν το βασικό menu.

Activity_ranging.xml

```
<RelativeLayout
xmlns:android="http://schemas.android.com/apk/res/android"
xmlns:tools="http://schemas.android.com/tools"
android:layout_width="match_parent"
```

```
android:layout_height="match_parent"
tools:context=".RangingActivity"
android:background="#ffffff">

<TextView
android:layout_width="wrap_content"
android:layout_height="wrap_content"
android:textAppearance="?android:attr/textAppearanceLarge"
android:id="@+id/textResult"
android:layout_below="@+id/textView"
android:layout_alignParentStart="true"
android:background="#ffffff"
android:layout_alignParentEnd="true"
android:textSize="18sp"/>


<TextView
android:layout_width="wrap_content"
android:layout_height="wrap_content"
android:textAppearance="?android:attr/textAppearanceLarge"
android:text="                          Beacons"
android:background="#426ad7"
android:id="@+id/textView"
android:layout_alignParentTop="true"
android:layout_alignParentStart="true"
android:textAlignment="center"
android:textIsSelectable="false"
android:layout_alignParentEnd="true" />

<TextView
android:layout_width="wrap_content"
android:layout_height="wrap_content"
android:textAppearance="?android:attr/textAppearanceLarge"
android:id="@+id/textResult2"
android:background="#ffffff"
android:layout_below="@+id/textView2"
android:layout_alignParentStart="true"
android:layout_alignParentEnd="true"
android:textSize="18sp"/>

<TextView
android:layout_width="wrap_content"
android:layout_height="wrap_content"
android:textAppearance="?android:attr/textAppearanceLarge"
android:id="@+id/textView2"
android:layout_below="@+id/textResult"
android:layout_alignParentStart="true" />

</RelativeLayout>
```

Το αρχείο Activity_ranging.xml ορίζει το interface του προγράμματος κατά την διαδικασία ανίχνευσης των ibeacon. Ορίζει δηλαδή την στοίχιση των textbox για την παρουσίαση των αποτελεσμάτων του σαρώματος. Το συγκεκριμένο περιβάλλον εμφανίζεται όταν πατήσουμε το κουμπί start tracking.

MonitoringActivity.java

```
package org.altbeacon.beaconreference;

import android.Manifest;
import android.annotation.TargetApi;
import android.bluetooth.BluetoothAdapter;
import android.bluetooth.BluetoothDevice;
import android.content.Context;
import android.content.pm.PackageManager;
import android.os.Build;
import android.os.Bundle;
import android.os.RemoteException;
import android.app.Activity;
import android.app.AlertDialog;
import android.content.DialogInterface;
import android.content.Intent;
import android.util.Log;
import android.view.View;
import android.widget.EditText;
import android.widget.TextView;

import org.altbeacon.beacon.BeaconConsumer;
import org.altbeacon.beacon.BeaconManager;
import org.altbeacon.beacon.BeaconParser;
import org.altbeacon.beacon.MonitorNotifier;
import org.altbeacon.beacon.Region;

import java.util.Set;

/**
 *
 * @author dyoung
 * @author Matt Tyler
 */
public class MonitoringActivity extends Activity  {
protected static final String TAG = "MonitoringActivity";
   private static final int PERMISSION_REQUEST_COARSE_LOCATION = 1;
   private BluetoothAdapter mBluetoothAdapter =
BluetoothAdapter.getDefaultAdapter();;
   private static final int REQUEST_ENABLE_BT = 1;

@Override
protected void onCreate(Bundle savedInstanceState) {
      Log.d(TAG, "onCreate");
      super.onCreate(savedInstanceState);
setContentView(R.layout.activity_monitoring);

verifyBluetooth();
logToDisplay("Application just launched");

        if (Build.VERSION.SDK_INT >= Build.VERSION_CODES.M) {
// Android M Permission check
if
(this.checkSelfPermission(Manifest.permission.ACCESS_COARSE_LOCATION)
!= PackageManager.PERMISSION_GRANTED) {
```

```
final AlertDialog.Builder builder = new AlertDialog.Builder(this);
builder.setTitle("This app needs location access");
builder.setMessage("Please grant location access so this app can
detect beacons in the background.");
builder.setPositiveButton(android.R.string.ok, null);
builder.setOnDismissListener(new DialogInterface.OnDismissListener() {

@TargetApi(23)
@Override
public void onDismiss(DialogInterface dialog) {
                        requestPermissions(new
String[]{Manifest.permission.ACCESS_COARSE_LOCATION},
PERMISSION_REQUEST_COARSE_LOCATION);
}

                });
builder.show();
}
        }



    }

@Override
public void onRequestPermissionsResult(int requestCode,
String permissions[], int[] grantResults) {
switch (requestCode) {
case PERMISSION_REQUEST_COARSE_LOCATION: {
if (grantResults[0] == PackageManager.PERMISSION_GRANTED) {
               Log.d(TAG, "coarse location permission granted");
} else {
final AlertDialog.Builder builder = new AlertDialog.Builder(this);
builder.setTitle("Functionality limited");
builder.setMessage("Since location access has not been granted, this
app will not be able to discover beacons when in the background.");
builder.setPositiveButton(android.R.string.ok, null);
builder.setOnDismissListener(new DialogInterface.OnDismissListener() {

@Override
public void onDismiss(DialogInterface dialog) {
                    }

               });
builder.show();
}
return;
}
      }
   }

public void onRangingClicked(View view) {
      Intent myIntent = new Intent(this, RangingActivity.class);
      this.startActivity(myIntent);
}

@Override
```

```
public void onResume() {
super.onResume();
((BeaconReferenceApplication)
this.getApplicationContext()).setMonitoringActivity(this);
}

@Override
public void onPause() {
super.onPause();
((BeaconReferenceApplication)
this.getApplicationContext()).setMonitoringActivity(null);
}

private void verifyBluetooth() {

try {
if
(!BeaconManager.getInstanceForApplication(this).checkAvailability()) {

if (!mBluetoothAdapter.isEnabled()) {

                Intent enableBtIntent = new
Intent(BluetoothAdapter.ACTION_REQUEST_ENABLE);
startActivityForResult(enableBtIntent, REQUEST_ENABLE_BT);
}
else {

                discoverBT();
}
//builder.show();
}
      }
catch (RuntimeException e) {
final AlertDialog.Builder builder = new AlertDialog.Builder(this);
builder.setTitle("Bluetooth LE not available");
builder.setMessage("Sorry, this device does not support Bluetooth
LE.");
builder.setPositiveButton(android.R.string.ok, null);
builder.setOnDismissListener(new DialogInterface.OnDismissListener() {

@Override
public void onDismiss(DialogInterface dialog) {
                finish();
System.exit(0);
}

         });
builder.show();

}

   }

public void discoverBT() {
// Get a set of currently paired devices
Set<BluetoothDevice> pairedDevices =
mBluetoothAdapter.getBondedDevices();
```

```
// If there are paired devices, add each one to the ArrayAdapter
       /* if (pairedDevices.size() > 0) {
            for (BluetoothDevice device : pairedDevices) {
                mPairedDevicesArrayAdapter.add(device.getName() + "\n"
+ device.getAddress());
            }
        } else {
            String noDevices =
getResources().getText(R.string.none_paired).toString();
            mPairedDevicesArrayAdapter.add(noDevices);
        }*/
}

public void logToDisplay(final String line) {
       runOnUiThread(new Runnable() {
public void run() {

            TextView NotText =
(TextView)MonitoringActivity.this.findViewById(R.id.textNotif);
NotText.append(line+"\n");
//editText.setText(line + "\n");
}
       });
}

}
```

Το αρχείο MonitoringActivity.java ορίζει τις βασικές λειτουργίες που θα επιτελέσουν όλα τα κουμπιά και textbox του αρχείου Activity_monitoring.xml. Κατά την εκκίνηση του προγράμματος ζητείται η παροχή άδειας του χρήστη για την ενεργοποίηση του Bluetooth της συσκευής. Στην συνέχεια ο χρήστης θα ενημερώνεται από ειδοποιήσεις που θα εμφανίζονται στην στήλη με τίτλο monitoring events για το αν υπάρχουν ibeacon στην περιοχή. Πατώντας το κουμπί start tracking που εμφανίζεται στην οθόνη της συσκευής του θα εκκινεί την διαδικασία για τον εντοπισμό των ibeacon στην περιοχή. Με το πάτημα του start tracking μεταφερόμαστε στο interface που δημιουργεί το αρχείο Activity_ranging.xml.

RangingActivity.java

```
package org.altbeacon.beaconreference;

import java.util.ArrayList;
import java.util.Collection;

import android.app.Activity;

import android.os.Bundle;
import android.os.RemoteException;
import android.util.Log;
import android.widget.EditText;
import android.widget.ListView;
import android.widget.TextView;
```

```
import org.altbeacon.beacon.AltBeacon;
import org.altbeacon.beacon.Beacon;
import org.altbeacon.beacon.BeaconConsumer;
import org.altbeacon.beacon.BeaconManager;
import org.altbeacon.beacon.BeaconParser;
import org.altbeacon.beacon.RangeNotifier;
import org.altbeacon.beacon.Region;

public class RangingActivity extends Activity implements
BeaconConsumer {
protected static final String TAG = "RangingActivity";
    private BeaconManager beaconManager =
BeaconManager.getInstanceForApplication(this);

@Override
protected void onCreate(Bundle savedInstanceState) {
super.onCreate(savedInstanceState);
setContentView(R.layout.activity_ranging);

beaconManager.bind(this);
}

@Override
protected void onDestroy() {
super.onDestroy();
beaconManager.unbind(this);
}

@Override
protected void onPause() {
super.onPause();
        if (beaconManager.isBound(this))
beaconManager.setBackgroundMode(true);
}

@Override
protected void onResume() {
super.onResume();
        if (beaconManager.isBound(this))
beaconManager.setBackgroundMode(false);
}
/*
    @Override
    public void onBeaconServiceConnect() {
        beaconManager.setRangeNotifier(new RangeNotifier() {
            @Override
            public void didRangeBeaconsInRegion(Collection<Beacon>
beacons, Region region) {
                Log.i(TAG, "didRangeBeaconsInRegion, number of beacons
detected = " + beacons.size());
                // HERE IT IS : the size is Always 1, but the beacon
(UUID etc. can be different)
            }
        });
```

```
        try {
            beaconManager.startRangingBeaconsInRegion(new
Region("apr", null, null, null));
        } catch (RemoteException e) {
            Log.i(TAG, "RemoteException = " + e.toString());
        }
    }*/

@Override
public void onBeaconServiceConnect() {
beaconManager.setRangeNotifier(new RangeNotifier() {
@Override
public void didRangeBeaconsInRegion(Collection<Beacon> beacons, Region
region) {
if (beacons.size() >0) {
int size = beacons.size();
                    int t=0;
Beacon.setHardwareEqualityEnforced(true);


//EditText editText =
(EditText)RangingActivity.this.findViewById(R.id.rangingText);
                        /* if(i==0) {
                            Beacon firstBeacon =
beacons.iterator().next();
                            logToDisplay("UUID: " +
firstBeacon.toString() + "\nDistance: " + firstBeacon.getDistance() +
" meters away.");
                        }else if(i==1){
                            Beacon firstBeacon =
beacons.iterator().next();
                            logToDisplay2("UUID: " +
firstBeacon.toString() + "\nDistance: " + firstBeacon.getDistance() +
" meters away.");
                        }else{
                            Beacon firstBeacon =
beacons.iterator().next();
                            logToDisplay2("UUID: " +
firstBeacon.toString() + "\nDistance: " + firstBeacon.getDistance() +
" meters away.");
                        }*/
Beacon firstBeacon = beacons.iterator().next();
Beacon secondBeacon =beacons.iterator().next();
//String[] Address = new String[size];

                    //TextView numT =
(TextView)findViewById(R.id.textView2);
                   // numT.setText(firstBeacon.getBluetoothAddress());

                   // for (Beacon beacon : beacons) {



                    //}
```

```
for (Beacon beacon : beacons) {
                            t = firstBeacon.getId3().toInt();
                            if(t == 1 || t==2) {
                                logToDisplay("The beacon " +
firstBeacon.toString() + "\nis about " + firstBeacon.getDistance() +
"meters away. ");
/* TextView txt1 =(TextView)findViewById(R.id.textView3);
                                double Dist=firstBeacon.getDistance();
                                txt1.setText(Double.toString(Dist));*/
}else if(t==3 || t==4){
                                logToDisplay2("The beacon " +
secondBeacon.toString() + "\nis about " + secondBeacon.getDistance() +
" meters away.");
/*TextView txt2 =(TextView)findViewById(R.id.textView4);
                                double
Dist2=firstBeacon.getDistance();

txt2.setText(Double.toString(Dist2));*/
}

                        }

                }
            }

        });

        try {
beaconManager.startRangingBeaconsInRegion(new
Region("myRangingUniqueId", null, null, null));
} catch (RemoteException e) {    }
    }

private void logToDisplay2(final String line2) {
        runOnUiThread(new Runnable() {
public void run() {
                TextView editText2 =
(TextView)RangingActivity.this.findViewById(R.id.textResult2);
//editText.append(line+"\n");
editText2.setText(line2+"\n");
}
        });
}

private void logToDisplay(final String line) {
        runOnUiThread(new Runnable() {
public void run() {

                TextView editText =
(TextView)RangingActivity.this.findViewById(R.id.textResult);
//editText.append(line+"\n");
editText.setText(line+"\n");
```

```
}
        });

}

}
```

Το αρχείο RangingActivity.java ορίζει την λειτουργία των textbox του αρχείου Activity_ranging.xmlγια τη σωστή εμφάνιση των ibeacon που ανιχνεύονται. Όταν η συσκευή ανιχνευθεί ένα ibeacon, το πρόγραμμα μας ελέγχει αν το id3 του ibeacon που ανιχνεύθηκε έχει τιμή 1 ή 2 τότε το αποτέλεσμα θα εμφανιστεί στο πρώτο textbox αλλιώς αν το id3 έχει τιμή 3 ή 4 τότε το αποτέλεσμα μας θα εμφανιστεί στο δεύτερο textbox. Η διαδικασία αυτή γίνεται με σκοπό να μπορέσουμε να εμφανίσουμε δύο αποτελέσματα στην οθόνη της συσκευής ταυτόχρονα. Ο κώδικας είναι φτιαγμένος έτσι ώστε να μπορεί να εμφανίσει δύο ibeacon με τις τιμές του id3 να κυμαίνονται μεταξύ του 1 και του 4. Αυτό γίνεται για ευκολία στην διαδικασία ελέγχου της λειτουργίας της εφαρμογής.

AndoidManifest.xml

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
package="org.altbeacon.beaconreference"
android:versionCode="1"
android:versionName="1.0" >

<uses-permission android:name="android.permission.BLUETOOTH"/>
<uses-permission android:name="android.permission.BLUETOOTH_ADMIN"/>

<uses-permission android:name="android.permission.INTERNET"/>
<application
android:allowBackup="true"
android:icon="@drawable/ic_launcher"
android:label="Beacon"
android:theme="@style/AppTheme"
android:name="BeaconReferenceApplication">
<activity
android:name="org.altbeacon.beaconreference.MonitoringActivity"
android:label="Beacon" >
<intent-filter>
<action android:name="android.intent.action.MAIN" />
<category android:name="android.intent.category.LAUNCHER" />
</intent-filter>
</activity>
<activity
android:name="org.altbeacon.beaconreference.RangingActivity"
android:label="Beacon" >
</activity>
</application>

</manifest>
```

Στο αρχείο AndoidManifest.xml ορίζονται όλες οι άδειες και κατ' επέκταση οι λειτουργίες του προγράμματος, που επιτρέπει ο χρήστης κατά την εγκατάσταση του προγράμματος στην συσκευή.

Η συγκεκριμένη εφαρμογή μπορεί να τροποποιηθεί έτσι ώστε να καταγράφει και τις MAC διευθύνσεις των Bluetooth της περιοχής έτσι ώστε να έχουμε μια εκτίμηση για το πλήθος των ατόμων στον χώρο.

3.9 Η περίπτωση του NFC και RFID

Έχοντας περιγράψει τον τρόπο ταυτοποίησης των συσκευών και του πλήθους ο οποίος μπορεί να πραγματοποιηθεί μόνο με την βοήθεια από τους ιδιοκτήτες των συσκευών, θα πρέπει επίσης να αναφέρουμε πως μπορούν να χρησιμοποιηθούν οι τεχνολογίες δικτύωσης, με ελάχιστη συμμετοχή του χρήστη. Σε αυτή την κατηγορία, έχουμε τη χρήση του NFC (Near Field Communication (κοντινό πεδίο επικοινωνίας)) και του RFID(Radio Frequency Identification (Αναγνώρισης ραδιοσυχνοτήτων)). Το NFC είναι μια ασύρματη τεχνολογία μικρής εμβέλειας που έχει εμβέλεια επικοινωνίας περίπου 20 εκατοστά. Με μια συσκευή η οποία έχει ενεργοποιημένο το NFC, ο χρήστης μπορεί να διαβάσει NFC tags(ετικέτες) ή να γράψει σε αυτά , σε αντίθεση με το RFID που τα tags μπορούν μόνο να γραφτούν. Η σύγχρονη χρήση των NFC-tags είναι να ενσωματώνετε ένα σε κάθε μετακίνηση πακέτων που πρόκειται να ταξιδέψουν σε έναν παραλήπτη, προκειμένου να παρέχει δυνατότητες παρακολούθησης. Όταν το πακέτο φτάσει στους αισθητήρες του NFC tracker(ανιχνευτής) και είναι σε σημαντική θέση στην τροχιά του, η τοποθεσία επισημαίνετε και αποστέλλεται σε μια βάση δεδομένων, όπου ο πελάτης μπορεί να το αναζητήσει όποτε θέλει.

Επιπλέον [51], μια άλλη χρήση των NFC-tags και NFC-trackers παρουσιάζεται σε συστήματα παρακολούθησης περιπόλων. Οι φρουροί ενεργοποιούν το NFC στις συσκευές τους και κάθε φορά που φτάνουν σε ένα ορισμένο σημείο στη διαδρομή περιπολίας τους, ένα σήμα στέλνεται σε μια ηλεκτρονική πλατφόρμα που έχει ενημερωθεί σχετικά με τη θέση τους. Το σύστημα έχει ακόμη προγραμματιστεί να ειδοποιεί κάθε φορά που ένας φρουρός έχει αργήσει να ελέγξει συγκεκριμένα σημεία ελέγχου στη διαδρομή του. Τα RFID-tags μπορούν να χρησιμοποιηθούν με τον ίδιο τρόπο όπως και τα NFC-tags, σε ένα εσωτερικό σύστημα αναγνώρισης ραδιοσυχνοτήτων ή να συνδέεται με αντικείμενα των οποίων οι θέσεις πρέπει να παρακολουθούνται. Το RFID-tag, εκτός από την αποθήκευση οποιασδήποτε πληροφορίας γραμμένο σε αυτό, μπορεί να συλλέξει το συνεχόμενο ρεύμα(DC) από έναν αναγνώστη RFID (active tag) ή να σχηματίσει μια μπαταρία (battery-assisted)και μπορεί να στείλει τις πληροφορίες χρησιμοποιώντας μια κεραία σε κάθε αναγνώστη που επικοινωνεί μαζί του. Επίσης, τα RFID-tags μπορούν να

γραφτούν μόνο μία φορά, αλλά μπορούν να διαβαστούν πολλές φορές. Εμπορικές λύσεις που κάνουν χρήση των RFID-tags είναι μεταξύ άλλων η χρήση τους σε χρήστες που πάνε για σκι έτσι ώστε να τους βοηθήσει να έχουν γρήγορη πρόσβαση σε πίστες σκι αρκεί να έχουν το εισιτήριο RFID στο σακάκι τους, ώστε να περνάνε μέσα από τα τουρνικέ [52, 53] και να απολαμβάνουν τη βόλτα τους χωρίς περισπασμούς.

Οι τεχνολογίες αυτές συχνά χρειάζονται τη συγκατάθεση του ατόμου, προκειμένου να χρησιμοποιηθούν για την εκτίμηση του πλήθους και την πρόβλεψη της ροής του. Και οι δύο αυτές τεχνολογίες έχουν ένα πλεονέκτημα το ότι καταφέρνουν να λειτουργούν εξίσου καλά σε εσωτερικούς και εξωτερικούς χώρους, έτσι ώστε η χρήση τους από τα άτομα σε μια εκδήλωση, μαζί με τους αντίστοιχους αναγνώστες / αισθητήρες, (readers / sensors) να μπορούν να ανιχνεύσουν σε πραγματικό χρόνο το πλήθος καθώς και την κίνησή του. Η επιλογή χρήσης αυτής της τεχνολογίας για την μετάδοση μηνυμάτων ή πληροφοριών στους ανθρώπους στο πλήθος που στέκονται σε ορισμένους τομείς πρέπει να αξιοποιηθεί, δεδομένου ότι οι ρόλοι του παραλήπτη- πομπού μπορούν να αλλάξουν.

3.10 Η περίπτωση του διαδικτύου και των μέσων μαζικής δικτύωσης

Η τελική περίπτωση που θα παρουσιάσουμε, αν και απαιτεί την εθελοντική αναφορά της θέσης του χρήστη, μπορεί να θεωρηθεί και ως διαφανής για τον ιδιοκτήτη μιας συσκευής. Ο λόγος είναι ότι με τον πολλαπλασιασμό των μέσων μαζικής δικτύωσης και τις πολυάριθμες εφαρμογές και εργαλεία που ενσωματώνουν την αναφορά της θέσης του χρήστη καθώς και των πληροφοριών GPS που υπάρχουν στις φωτογραφίες που ανεβάζουν συχνά οι χρήστες στα κοινωνικά δίκτυα (Social Networks - SNs), η ανίχνευση της θέσης μιας συσκευής σε μια συγκεκριμένη χρονική στιγμή είναι πολύ εύκολη, απλά με την ανάλυση πληροφοριών από τα μέσα μαζικής δικτύωσης. Ως αποτέλεσμα, το διαδίκτυο και τα SNs παρέχουν ένα μεγάλο όγκο πληροφοριών που, αν χρησιμοποιηθεί σωστά, μπορεί να γίνει ένα σημαντικό εργαλείο για την πρόβλεψη της συμπεριφοράς της μάζας και των συγκεντρώσεων διαμαρτυρίας.

Ειδικές περιπτώσεις χρήσης των SNs και του διαδικτύου οι οποίες μπορούν να χρησιμοποιηθούν για τις εκτίμηση του πλήθους έχουν ήδη αναφερθεί. Στο [54] η μελέτη των δεδομένων από μια δημοφιλής εφαρμογή, όπως οι χάρτες Baidu στην Κίνα, χρησιμοποιείται ως εργαλείο πρόγνωσης για την εκτίμηση του πλήθους σε μια συγκεκριμένη περιοχή μαζί με τη ροή του πλήθους. Η παρακολούθηση της συμπεριφοράς της μάζας μπορεί να χρησιμοποιηθεί για να δημιουργήσει μια αποτελεσματική μέθοδο έγκαιρης προειδοποίησης που μπορεί να χρησιμοποιηθεί για την πρόληψη ατυχημάτων. Στην περίπτωση αυτή, οι συγγραφείς έχουν μελετήσει τα δεδομένα των χαρτών Baidu από το συμβάν στην Σαγκάη το 2014 (Shangai

Stampede), και έχουν δώσει την δίκια τους άποψη όσον άφορα την πρόβλεψη ανώμαλης συμπεριφοράς του πλήθους. Επιπλέον, τα δεδομένα των παραπάνω χαρτών όταν συνδυάζονται με δεδομένα θέσης από την ίδια εφαρμογή, έδειξε ότι σε συνδυασμό μπορούν να επιτύχουν τα πρώτα προειδοποιητικά σημάδια για την ανωμαλία του πλήθους που παρέχει ένα περιθώριο 1-3 ώρες για γρήγορη προετοιμασία για να αποφευχθεί οποιαδήποτε ανάλογη καταστροφή .Ως αποτέλεσμα, ένα μοντέλο μηχανικής μάθησης που καταφέρνει να προβλέπει αποτελεσματικά την πυκνότητα του πλήθους σε ορισμένες περιοχές μία ώρα πριν το πλήθος πραγματικά συναθροιστεί.

Σε μια άλλη περίπτωση, [55], μια μελέτη των διάφορων σε απευθείας σύνδεση (online) πηγών σε 7 διαφορετικές γλώσσες, συμπεριλαμβανομένων των δημοφιλών SNs όπως το Tweeter, έχει δείξει ότι οι σημαντικές συγκεντρώσεις διαμαρτυρίας μπορεί να προβλεφτούν. Σημαντικές διαμαρτυρίες θεωρούνται εκείνες που κερδίζουν, την ίδια ημέρα, πιο ασυνήθιστη κάλυψη της εκδήλωσης από ό, τι είναι σύνηθες σε αυτή τη χώρα.

Για παράδειγμα, για τις χώρες της Μέσης Ανατολής, όπου οι καθημερινές συνθήκες περιλαμβάνουν διάφορους κινδύνους λόγω των συγκρούσεων που λαμβάνουν χώρα, η μελέτη καταφέρνει να επικεντρώνετε σε γεγονότα που δεν περιλαμβάνονται στην "ρουτίνα" της χώρας. Ο προτεινόμενος μηχανισμός πρόβλεψης δεν περιλαμβάνει μόνο την παρακολούθηση των online πηγών, αλλά, ταυτόχρονα, χρησιμοποιεί μηχανική μάθηση ώστε να εφαρμόσουν τις γνώσεις από άλλες χώρες με την υπό εξέταση χώρα, για να πετύχει καλύτερα αποτελέσματα προβλέψεων. Η εφαρμογή αυτού του μηχανισμού κατά τη διάρκεια του πραξικοπήματος της Αιγύπτου έχει δείξει ότι οι μαζικές διαμαρτυρίες θα μπορούσαν να έχουν αποτελεσματικά προβλεφθεί.

Ως αποτέλεσμα, η έγκαιρη ανάλυση των συγκεντρωμένων στοιχείων από τα SNs, τις Κοινωνικές εφαρμογές ή των online πηγών μπορούν να οδηγήσουν σε καλύτερη προετοιμασία και συνεπώς αμεσότερη αντίδραση από τις αρχές για την πρόληψη καταστροφών ή μαζικών διαδηλώσεων.

4. Νομικά και Ηθικά ζητήματα

Όσον αφορά τα νομικά θέματα που προκύπτουν από την ανίχνευση πλήθους, χρησιμοποιώντας τεχνικές όπως αυτή του passive Wi-Fi tracking πρέπει να είμαστε ιδιαίτερα προσεκτικοί. Για παράδειγμα η καταγραφή της MAC διεύθυνσης οποιασδήποτε συσκευής η όποια στέλνει probe requests είναι παράνομη. Αυτό συμβαίνει διότι ο σκοπός που εκπέμπει μια συσκευή probe requests είναι για να συνδεθεί σε ένα δίκτυο. Για αυτό το λόγο στην παρούσα εργασία χρησιμοποιούμε δικές μας συσκευές για την καταγραφή και την επίδειξη των αποτελεσμάτων στο κοινό.

Ως εκ τούτου για να χρησιμοποιηθούν τέτοιες τεχνικές θα πρέπει να υπάρχει η έγκριση του ιδιοκτήτη της εκάστοτε συσκευής. Παρ όλα αυτά η τεχνική της παθητικής καταγραφής Wi-Fi θα βοηθούσε τους φορείς επιβολής του νόμου να ανιχνεύσουν παράνομη δραστηριότητα. Για παράδειγμα θα μπορούσε η αστυνομία να εντοπίσει άτομα τα οποία έχουν συγκεκριμένη MAC διεύθυνση και αλλάζουν συνεχώς SSID(χρησιμοποιώντας ονομασίες γνωστών καταστημάτων τις περιοχής) με σκοπό να παρακινήσουν ανυποψίαστους χρήστες να συνδεθούν στο δίκτυο τους.

4.1 Ευρωπαϊκοί κανονισμοί-αποφάσεις-πλαίσια

Ο Ευρωπαϊκός Κανονισμός 2016/679 (General Data Protection Regulation, GDPR) ψηφίστηκε στις 27.04.2016 και τίθεται σε υποχρεωτική εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης στις 25.05.2018, διαμορφώνοντας ένα ενιαίο νομικό πλαίσιο, χωρίς την ανάγκη ψήφισης εθνικής νομοθεσίας και καταργώντας την υφιστάμενη νομοθεσία. Ο νέος κανονισμός αυξάνει σημαντικά τις υποχρεώσεις των επιχειρήσεων, ενώ το μέγεθος των προβλεπόμενων προστίμων τον τοποθετεί πολύ υψηλά στην ατζέντα της ανώτατης διοίκησης.

Ο Ευρωπαϊκός Κανονισμός 2016/679 (General Data Protection Regulation, GDPR) ψηφίστηκε στις 27.04.2016 και τίθεται σε υποχρεωτική εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης στις 25.05.2018, διαμορφώνοντας ένα ενιαίο νομικό πλαίσιο, χωρίς την ανάγκη ψήφισης εθνικής νομοθεσίας και καταργώντας την υφιστάμενη νομοθεσία. Ο νέος κανονισμός αυξάνει σημαντικά τις υποχρεώσεις των επιχειρήσεων, ενώ το μέγεθος των προβλεπόμενων προστίμων τον τοποθετεί πολύ υψηλά στην ατζέντα της ανώτατης διοίκησης. Το αντικείμενο του Γενικού Κανονισμού 2016/679 είναι η διαμόρφωση ενός ενιαίου νομικού πλαισίου για την επεξεργασία προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης, που θέτει μία σειρά περιορισμών και νέων υποχρεώσεων στις επιχειρήσεις σχετικά με:

- την επεξεργασία των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους, από τη συλλογή έως και την καταστροφή τους,
- τη δυνατότητα μεταφοράς τους σε άλλες χώρες,
- την προστασία των δικαιωμάτων των φυσικών προσώπων,
- την ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) των προσωπικών δεδομένων και
- τις ενέργειες γνωστοποίησης που οφείλει να κάνει η επιχείρηση σε περίπτωση παραβίασης.
- Σε περίπτωση παράβασης προβλέπονται σημαντικά αυξημένα πρόστιμα, που ανάλογα με το είδος και το μέγεθός της, φθάνουν έως τα 20 εκατομμύρια ευρώ ή το 4% του παγκόσμιου ετήσιου κύκλου εργασιών.

Αυτό αφορά όλες τις ιδιωτικές και δημόσιες επιχειρήσεις, καθώς και τις κρατικές αρχές που με οποιοδήποτε τρόπο διαχειρίζονται δεδομένα προσωπικού χαρακτήρα πελατών, πελατών των πελατών τους, εργαζομένων, συνεργατών ή άλλων φυσικών προσώπων. Ως εκ τούτου, ο GDPR αφορά πρακτικά όλες τις επιχειρήσεις, εντός και εκτός Ευρωπαϊκής Ένωσης, εφόσον τα δεδομένα αφορούν Ευρωπαίους πολίτες. [66]

Η απόφαση-πλαίσιο 2008/977 / ΔΕΥ τέθηκε σε ισχύ στις 5 Μαΐου 2016 και τα κράτη μέλη της ΕΕ πρέπει να την μεταφέρουν στην εθνική τους νομοθεσία έως τις 6 Μαΐου 2018.Η οποία αναφέρει ότι γίνετε αρση της προστασία των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις[67]

Οδηγία της Ευρωπαϊκής Ένωσης 2016/680 του Ευρωπαϊκού κοινοβουλίου και συμβούλιου της 27ης Απριλίου 2016 αναφέρει για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου. Μερικες από τις αποφάσεις που της παραπάνω οδηγίας είναι οι ακόλουθες:

- Για την πρόληψη, διερεύνηση και τη δίωξη ποινικών αδικημάτων, οι αρμόδιες αρχές πρέπει να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα που συλλέγονται στο πλαίσιο της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης συγκεκριμένων ποινικών αδικημάτων και πέραν του πλαισίου αυτού, ώστε να κατανοούν καλύτερα τις εγκληματικές δραστηριότητες και να προβαίνουν σε συσχετισμούς μεταξύ διαφορετικών διαπιστωθέντων ποινικών αδικημάτων.

- Για να τηρείται η ασφάλεια σε σχέση με την επεξεργασία και να αποτρέπεται η επεξεργασία κατά παράβαση της παρούσας οδηγίας, τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο ώστε να εξασφαλίζεται το ενδεδειγμένο επίπεδο ασφάλειας και εμπιστευτικότητας, μεταξύ άλλων με την αποτροπή της μη εξουσιοδοτημένης πρόσβασης σε δεδομένα προσωπικού χαρακτήρα ή τη χρήση τους και στον εξοπλισμό που χρησιμοποιείται για την επεξεργασία, λαμβανομένων υπόψη του επιπέδου της διαθέσιμης τεχνολογίας, του κόστους εφαρμογής σε σχέση με τους κινδύνους και τη φύση των δεδομένων προσωπικού χαρακτήρα που πρέπει να προστατευτούν.[68]

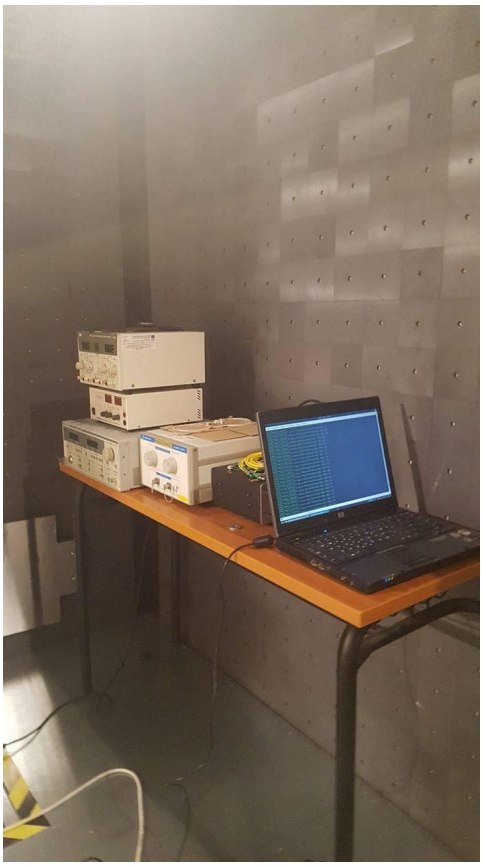
```
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: KLIMECO.GR RSSi: -74
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: Forthnet-A43C21 RSSi: -74
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: Vodafone-16879 RSSi: -75
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: SpeedTouchE3C92B RSSi: -73
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: FunPlay RSSi: -76
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: CARWASH RSSi: -72
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: OTEf37738 RSSi: -77
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      d9:69:6a:bf SSID: 50-50 CAFE RSSi: -72
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: holspot_Goody's RSSi: -77
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: OTE299889 RSSi: -77
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: OLA AND MORE... RSSi: -82
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      d9:69:6a:bf SSID: Iason RSSi: -79
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      d9:69:6a:bf SSID: Forthnet-C28EE8 RSSi: -81
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: Wind WiFi B6A3E0 RSSi: -81
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: KLIMECO.GR RSSi: -80
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      d9:69:6a:bf SSID: Forthnet-A43C21 RSSi: -81
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source       :d9:69:6a:bf SSID: Vodafone-16879 RSSi: -82
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: CYTA 12 RSSi: -77
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: SpeedTouchE3C92B RSSi: -82
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: FunPlay RSSi: -80
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: CARWASH RSSi: -81
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: 50-50 CAFE RSSi: -81
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: holspot_Goody's RSSi: -79
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: OTE299889 RSSi: -86
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: OLA AND MORE... RSSi: -89
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: Forthnet-C28EE8 RSSi: -86
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: KLIMECO.GR RSSi: -86
Probe Request Captured:
Target: ff:ff:ff:ff:ff:ff Source:      :d9:69:6a:bf SSID: 50-50 CAFE RSSi: -84
```

Εικόνα 4.1 Γρήγορη εναλλαγή SSID με ίδια MAC

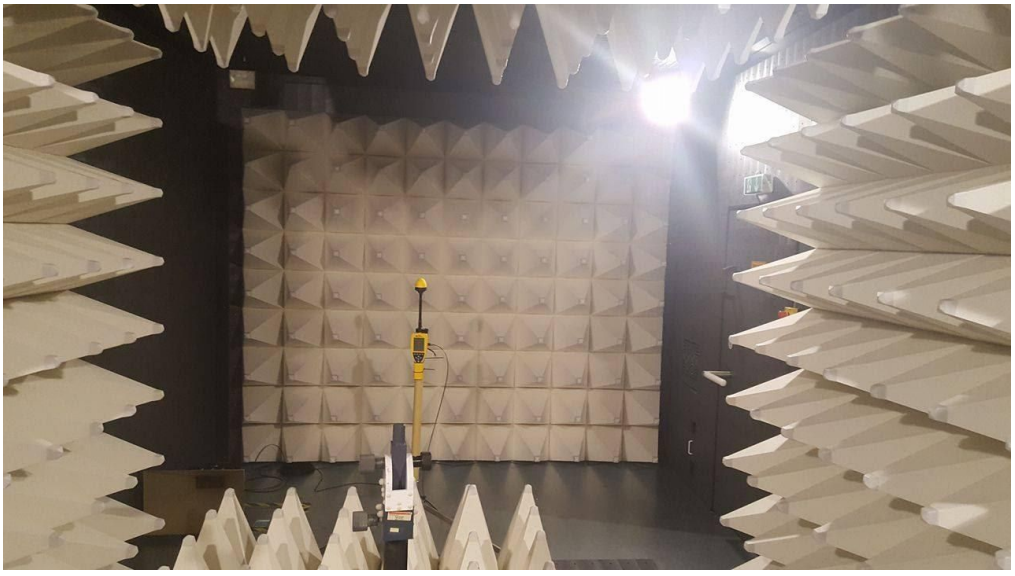
Οι καταγραφές και τα αποτελέσματα των παραπάνω τεχνικών ανίχνευσης πλήθους που παρουσιαστήκαν παραπάνω έγιναν αποκλειστικά με την χρήση των προσωπικών μας συσκευών και έλαβαν χώρα σε ειδικό ανηχοϊκό θάλαμο και θέλουμε να ευχαριστήσουμε το ΑΕΙ ΠΕΙΡΑΙΑ Τ.Τ. που μας έδωσε πρόσβαση σε αυτόν. Οι ανηχοϊκοί θάλαμοι αποτελούν σύγχρονα εργαλεία της ακουστικής, τα οποία έχουν δημιουργηθεί ειδικά για επιστημονικές μετρήσεις,

αυτό που κάνει έναν τέτοιο θάλαμο ιδιαίτερο είναι ότι δεν αφήνει να περάσουν ή να εισέλθουν σήματα μέσα σε αυτόν.

Εικόνα 4.2 Πόρτα ανηχοϊκού θαλάμου



Εικόνα 4.3 Δοκίμη της τεχνικής Passive Wi-fi tracking με laptop



Εικόνα 4.4 Εσωτερικός χώρος ανηχοϊκού θαλάμου

Πρέπει να αναφέρουμε ότι παρούσα εργασία γίνετε για ερευνητικούς σκοπούς και σε καμία περίπτωση δεν γίνετε για εκμετάλλευση τρίτων, έτσι λοιπόν είναι προσωπική ευθύνη του καθενός για το πώς και με τι σκοπό θα χρησιμοποιήσει μια τέτοια τεχνική.

Πέρα όμως από το νομικό κομμάτι υπάρχει και το ηθικό που πρέπει να αναλογιστούμε στην χρήση τέτοιων τεχνολογιών. Γιατί και μόνο η λέξη «ανίχνευση» που χρησιμοποιούμε για να περιγράψουμε τις παραπάνω τεχνολογίες, υποδηλώνει την παραβίαση στην προσωπικό χώρο του κάθε ατόμου.

Η χρήση των τεχνολογιών ανίχνευσης πλήθους εφαρμόζονται για να καλυτερεύσουν την ποιότητα ζωής του ανθρώπου αλλά και για να τον κάνουν να νιώσει ασφάλεια. Εκτός όμως από ασφάλεια ένας άνθρωπος θέλει να νιώθει και ελευθερία η οποία κινδυνεύει να χαθεί. Διότι εάν κάποιος, όπου αυτός ο κάποιος είναι είτε η αστυνομία είτε κάποια κυβέρνηση είτε κάποιος ιδιώτης, ξέρει ανά πάσα στιγμή που βρισκόμαστε αυτομάτως δεν είμαστε ελεύθεροι. Άτομα τα οποία δουλεύουν σε χώρους που παρακολουθούνται συνέχεια όπως τράπεζες ή ακόμα και χώρες όπως η Αγγλία που οι δρόμοι της είναι γεμάτοι κάμερες αναφέρουν πως αισθάνονται σαν φυλακισμένοι. Επιπλέον υπάρχει πάντα ο κίνδυνος αυτές τις πληροφορίες για το που βρισκόμαστε να τις εκμεταλλευτεί κάποιος με σκοπό να μας βλάψει. Συνοψίζοντας λοιπόν όσον αφορά την ηθική της τεχνολογίας έγκειται ως επί των πλείστον στην προσωπική ηθική του κάθε ατόμου που τις χρησιμοποιεί.

5. Επίλογος

Όπως αναφέρθηκε και στα προηγούμενα κεφάλαια, η χρήση της κεντρικής προσέγγισης για την ανίχνευση / εκτίμηση του πλήθους είναι διαθέσιμη, όπως και η χρήση της ανάλυσης βίντεο. Η χρήση του βίντεο προκειμένου να παρέχετε εκτίμηση σε πραγματικό χρόνο σχετικά με την πυκνότητα και τη ροή του πλήθους μπορεί να είναι πολύ αποτελεσματική, αλλά έχει αρκετά μειονεκτήματα που θα πρέπει να αναφερθούν.

Αρχικά, υπάρχουν ζητήματα που σχετίζονται με την προστασία της ιδιωτικής ζωής που πρέπει να αντιμετωπιστούν προτού επιτραπεί οποιαδήποτε καταγραφή βίντεο σε δημόσιους χώρους. Επιπλέον, η μελέτη του ζωντανού βίντεο μπορεί να είναι πολύ χρήσιμο ως μετά - εργαλείο ανάλυσης (δηλαδή, μαζί με τα δεδομένα από ένα κυψελοειδές δίκτυο για την κάλυψη περιοχών όπου το βίντεο δεν είναι διαθέσιμο), όπου η συμπεριφορά του πλήθους μπορεί να μελετηθεί με σκοπό να αποφευχθούν μελλοντικά οι επαναλήψεις των επικίνδυνων συμβάντων. Η εξέταση των γεγονότων σε βίντεο πραγματικού χρόνου δεν αφήνει χρόνο για οργάνωση και προετοιμασία οποιασδήποτε ενέργειας αντιμετώπισης καταστάσεων έκτακτης ανάγκης, δεδομένου ότι η ροή των γεγονότων προηγείται από κάθε αντίδραση. Τέλος, δεδομένου ότι οι θέσεις όπου οι κάμερες που βρίσκονται σε μια πόλη μπορούν να περιοριστούν, ανάλογα επηρεάζεται και η αποδοτικότητα της χρήσης αυτής της μεθόδου.

Ως εκ τούτου, ο ρόλος της εξέτασης των βίντεο είναι πολύ σημαντικός, κυρίως όμως ως εργαλείο μετ-ανάλυσης και όχι για πραγματικό χρόνο. Ταυτόχρονα, η χρήση της παθητικής ανίχνευσης Wi-Fi ή η χρήση BLE συσκευών μπορεί να αντιμετωπίσει το ζήτημα της προστασίας της ιδιωτικής ζωής, αλλά σε βάρος της ακρίβειας στα αποτελέσματα, δεδομένου ότι η εκτίμηση / μέτρηση βασίζεται στην είσοδο, την έξοδο των ατόμων, και όχι την ατομική αναγνώριση. Ωστόσο, όταν πρόκειται για την εκτίμηση του πλήθους, η ανάγκη για υψηλή ακρίβεια του αριθμού των συσκευών δεν είναι κρίσιμη, καθώς δεν υπάρχει ανάγκη για την ταυτοποίηση των κατόχων. Από την άλλη πλευρά οι γρήγορες σε πραγματικό χρόνο εκτιμήσεις, διατηρώντας την ιδιωτική ζωή και την ικανότητα για τη ροή του πλήθους ή τροχιά ανίχνευσης είναι κρίσιμη, για την έγκαιρη προειδοποίηση και σχεδιασμού για το μέλλον. Παρόλα αυτά , η χρήση των τεχνολογιών δικτύωσης για την εκτίμηση του πλήθους είναι ο ποιο αξιόπιστος τρόπος προκειμένου να υπολογιστεί με ακρίβεια ο εντοπισμός όγκων πλήθους.

Τα Πεδία εφαρμογής τους αφορούν κυρίως την ασφάλεια , την προστασία και την ποιότητα στην παροχή υπηρεσιών για τις μεγάλες πολυπληθής εκδηλώσεις καθώς και για την πολεοδομία. Η επιλογή της συγκεκριμένης τεχνολογίας ή ο συνδυασμός των εργαλείων, εξαρτάται ανάλογα με την περίπτωση και τις σχετικές προϋποθέσεις και απαιτήσεις (όπως η ανάγκη για πραγματικό χρόνο ή σχεδόν πραγματικό χρόνο ανίχνευσης), από τον σκοπό της χρήσης των συλλεχθέντων δεδομένων (άμεση ανταπόκριση και προειδοποίηση ή μελλοντικό σχεδιασμό), και τέλος από το επίπεδο συμμετοχής των χρηστών. Τέλος, η χρήση των τυχαίας επιλογής των διευθύνσεων MAC, είναι μια τεχνική που αποδίδει (τοπικά) διαφορετικές διευθύνσεις MAC σε μια συσκευή όταν ερωτάται για πρόσβαση στο Wi-Fi, παρόλα αυτά, εξακολουθεί να είναι πολύ νέα τεχνολογία ώστε να δώσει τα απαιτούμενα αποτελέσματα.

Συντομογραφίες

- **GPS :** Global Positioning System
- **BLE :** Bluetooth Low Energy
- **RFID :** Radio Frequency Identification
- **NFC :** Near Field Communications
- **GSM :** Global System for Mobile Communications
- **WLAN :** Wireless Local Area Network
- **PAN :** Personal Area Network
- **IMEI :** International Mobile Equipment Identity
- **ICCID :** Integrated Circuit Card ID
- **MEID :** Mobile Equipment Identifier
- **SEID :** Secure Element ID
- **SN :** Social Network
- **SSID:** Service Set Identifier

- **IBSS:** Independent Basic Service Set
- **MAC :** Media Access Control
- **AMP:** Address Probe Sensors
- **OS:** Operation System
- **BT :** Bluetooth
- **UUID:** Universally Unique Identifier
- **SD Card** : Secure Digital Card
- **USB :** Universal Serial Bus
- **HDMI :** High-Definition Multimedia Interface

Βιβλιογραφία

1. Gorra,“http://www.leedsbeckett.ac.uk/inn/alic/agorra/2_Chapter2_LiteratureReview.pdf”, [09-05-2016].

2. European Court of Human Rights, “http://www.echr.coe.int/Documents/FS_Data_ENG.pdf”, [09-05-2016].

3. Tidwell, http://www.officer.com/article/12154412/mobile-device-data-unlocks-the-critical-connections-that-solve-crimes, [09-05-2016].

4. European Commission, “http://ec.europa.eu/justice/data-protection/data-collection/legal/index_en.htm”, [09-05-2016].

5. Han, B. & Srinivasan, A., 2012. eDiscovery: Energy efficient device discovery for mobile opportunistic communications, Maryland: University of Maryland.

6. B. M. Musa and Jakob Eriksson. 2012. Tracking unmodified smartphones using Wi-Fi monitors. In Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems (SenSys '12). ACM, New York, NY, USA, 281-294. DOI=http://dx.doi.org/10.1145/2426656.2426685.

7. Uki Fukuzaki, Masahiro Mochizuki, Kazuya Murao, and Nobuhiko Nishio. 2014. A pedestrian flow analysis system using Wi-Fi packet sensors to a real environment. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp '14 Adjunct). ACM, New York, NY, USA, 721-730. DOI=http://dx.doi.org/10.1145/2638728.2641312.

8. M Abbott-Jard, H Shah, and A Bhaskar. Empiricalevaluation of bluetooth and wifi scanning for road transport. Australasian Transport Research Forum (ATRF), 36th, 2013, Brisbane, Queensland, Australia, p. 14, 2013.

9. AirTightTeam,http://blog.mojonetworks.com/ios8-mac-randomization-analyzed/, [23-09-14].

10. http://books.gigatux.nl/mirror/snortids/0596006616/snortids-CHP-2-SECT-4.html

11. Λευτέρης Ξυκομηνός, http://www.zougla.gr/technology/article/intel-ke-arduino-i-plaketa-galileo-me-stoxo-tin-empnefsi-dimiourgikotitas-ma8isis-ke-anakalipsis[09-10-2013].

12. https://www.arduino.cc/en/ArduinoCertified/IntelGalileo

13. http://www.intel.com

14. Wikipedia, https://en.wikipedia.org/wiki/PuTTY [15-09-2016]

15. Intel,https://software.intel.com/en-us/articles/getting-started-with-the-intel-galileo-board-on-windows [09-01-2015]

16. Gigatux,http://books.gigatux.nl/mirror/snortids/0596006616/snortids-CHP-2-SECT-4.html[06-02-2015]

17. Faheem Zafari, Ioannis Papapanagiotou and Konstantinos Christidis, “Micro-location for Internet of Things equipped Smart Buildings”, CoRR, volume 1501.01539, 2015, http://arxiv.org/abs/1501.01539.

18. Faheem Zafari, Ioannis Papapanagiotou, “Enhancing iBeacon Based Micro-Location with Particle Filtering”, GLOBECOM 2015: pp. 1-7.

19. "iOS: Understanding iBeacon". Apple Inc., [12-02-2015].

20. "Bfonics Inc.". Bfonics.com. Retrieved [10-11-14].

21. "Beacons: Everything you need to know.". Pointrlabs.com.[18-01-2015].

22. "iBeacons". Dave Addey. 2013-09-22. [11-12-2013].

23. "Inside iOS 7: iBeacons enhance apps' location awareness via Bluetooth LE". Forums.appleinsider.com. 2013-06-18. [11-12-2013].

24. "Apple iBeacons Explained – Smart Home Occupancy Sensing Solved?". Automated Home. [11-12-2013].

25. "iBeacon Bible" (PDF). Andy Cavallini. [01-01-2014].

26. Aislelabs ,http://www.aislelabs.com/reports/beacon-guide/[04-05-2015]

27. YouTube,"What is a Beacons Range Video Tutorial". [10-11-14].

28. Stackoverflow.com ,"What are the nominal distances for iBeacon "Far", "Near", and "Immediate"[19-05-2014].

29. Simon Toulson, https://support.kontakt.io/hc/en-gb/articles/201620741-iBeacon-Parameters-UUID-Major-and-Minor,[05-09-2015]

30. LarryDignan,http://www.zdnet.com/article/tis-support-of-apples-ibeacon-adds-enterprise-iot-heft/,[17-04-2014]

31. 9to5 mac,"Best iBeacon hardware crowned following extensive stress tests". [03-11-2014].

32. GIGAOM,"Retailers are excited about beacons, but how fast will they drain your smartphone battery?". [09-07-2014].

33. Aislelabs ,"iBeacon and Battery Drain on Phones: A Technical Report".[09-07-2014].

34. Aislelabs,"iBeacon Battery Drain on Apple vs Android: A Technical Report - Aislelabs", [14-08-2014].

35. Aislelabs ,"The Hitchhikers Guide to iBeacon Hardware: A Comprehensive Report by Aislelabs",[03-11-2014].

36. ZDNet, "Apple launches iBeacon in 254 stores to streamline shopping experience". [18-12-2013].

37. Forbes ,"Apple iBeacons Find Their Way Into McDonald's", [18-12-2014].

38. "Building Cross-Platform iBeacon Apps for iOS, Android and Windows with C# and Xamarin".[14-05-2014].

39. Developer.radiusnetworks.com , "A Solution for Android Bluetooth Crashes"[12-06-2014].

40. Apple Inc,"iOS: Understanding iBeacon",[13-03-2014].

41. Bluetoothbeacons.com ,"How to Configure your iPhone as an iBeacon Transmitter",[17-02-2014].

42. Alexandru Bleau ,http://blog.mowowstudios.com/2015/02/100-use-cases-examples-ibeacon-technology/,[04-02-2016].

43. http://blog.twocanoes.com/post/68861362715/10-awesome-things-you-can-do-today-with-ibeacons[12-03-2013].

44. Mellongroup, http://mellongroup.com/products/beacons [09-08-2016].

45. VladimirPetrov,https://www.quora.com/What-are-the-best-uses-for-iBeacon,[22-11-2013].

46. Wikipedia, https://en.wikipedia.org/wiki/Raspberry_Pi, [12-09-2016].

47. https://www.raspberrypi.org/downloads/raspbian/

48. Wade Wegner , http://www.wadewegner.com/2014/05/create-an-ibeacon-transmitter-with-the-raspberry-pi/ , [20-05-2014].

49. Andrew ,https://andrewmemory.wordpress.com/2016/03/29/turning-a-raspberry-pi-3-into-an-ibeacon/ , [29-03-2016].

50. Panos Georgiadis, Chris K ,http://www.doctorandroid.gr/p/iphone.html,[13-09-2016]

51. Ginstr, “http://www.nfc-tracker.com/en/guard-tour-monitoring-system/”, [09-05-2016].

52. SKIDATA,“http://www.skidata.com/fileadmin/user_upload/corporate/press/basis-press-kit_en.pdf”, [09-05-2016].

53. RFIDEAS,“https://www.rfideas.com/sites/www.rfideas.com/files/rfideas/files/case-studies/Aspen_Snowmass.pdf”, [09-05-2016].

54. Jingbo Zhou, Hongbin Pei, Haishan Wu, “Early Warning of Human Crowds Based on Query Data from Baidu Map: Analysis Based on Shanghai Stampede, (Submitted on 22 Mar 2016), arXiv:1603.06780.

55. Kallus, N., “Predicting Crowd Behavior with Big Public Data”, in the Proceedings of the 23rd International Conference on World Wide Web, WWW '14 Companion, 2014, Seoul, Korea, pp.625—630.

56. Rahul Sachin Amey, http://www.techkranti.com/2011_05_01_archive.html, [15-01-2011].

57. RF Wireless World , http://www.rfwireless-world.com/Terminology/WLAN-probe-request-and-response-frame.html, [13-05-2016].

58. CHRIS VALENTINE ,http://oddculture.com/historys-top-15-worst-soccer-disasters [4-08-2015].

59. Lori Bordonaro, http://www.nbcnewyork.com/news/local/Central-Park-North-Subway-Stampede-NYC-Police-NYPD-383785491.html [21-06-2016].

60. Kate Sedgwick, http://matadornetwork.com/nights/10-deadliest-concert-disasters-of-the-last-50-years/ [16-08-2010].

61. BBC, http://www.bbc.com/news/world-asia-china-30646918 [01-01-2015].

62. ΚΟΣΜΟΣ, http://www.kathimerini.gr/832121/article/epikairothta/kosmos/ekatontades-pistoi-podopath8hkan-mexri-8anatoy-sth-mekka [25-09-2015].

63. Yahoo! News, https://www.yahoo.com/news/ap-exclusive-saudi-hajj-disaster-deadliest-ever-strike-111906027.html?ref=gs [10-10-2015].

64. Yahoo! News, https://www.yahoo.com/news/foreign-toll-figures-show-hajj-tragedy-deadliest-history-091459114.html?ref=gs [14-10-2015].

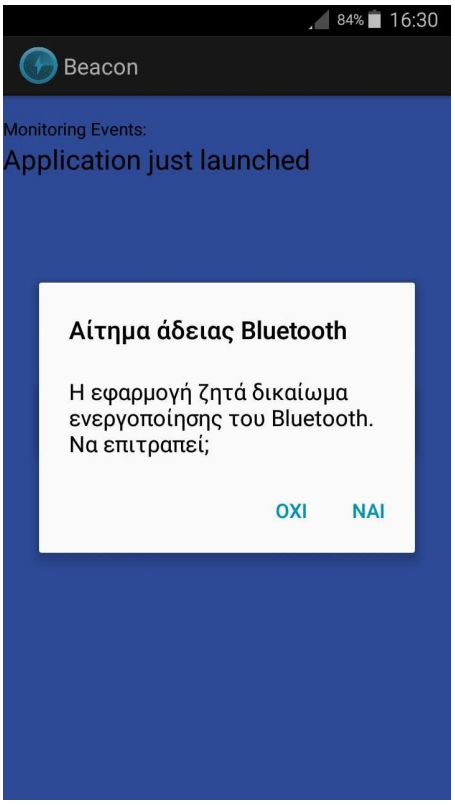
65. Wikipedia, https://en.wikipedia.org/wiki/2015_Mina_stampede#/media/File:The_way_to_Jamarat_Bridge_3.JPG [7-11-2015].

66. Priority, https://www.priority.com.gr/page/gdpr_2016_679/?gclid=CjwKEAjwlpbIBRCx4eT8l9W26igSJAAuQ_HG272pNa21JwvsyPl88RgUPhxg4ggdzCGJC934IUSU3RoCYPvw_wcB [30-4-2016]

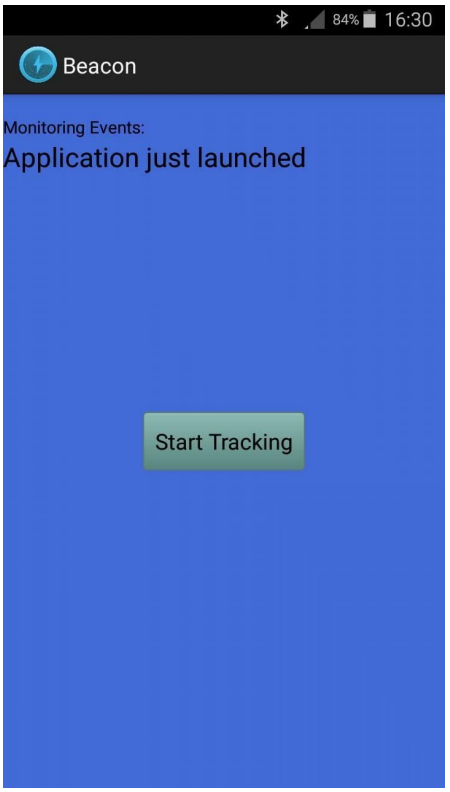
67. Eur-lex,http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977 [30-12-2008]

68. Eur-lex,http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG[04-05-2016]

Παράρτημα εικόνων εφαρμογής

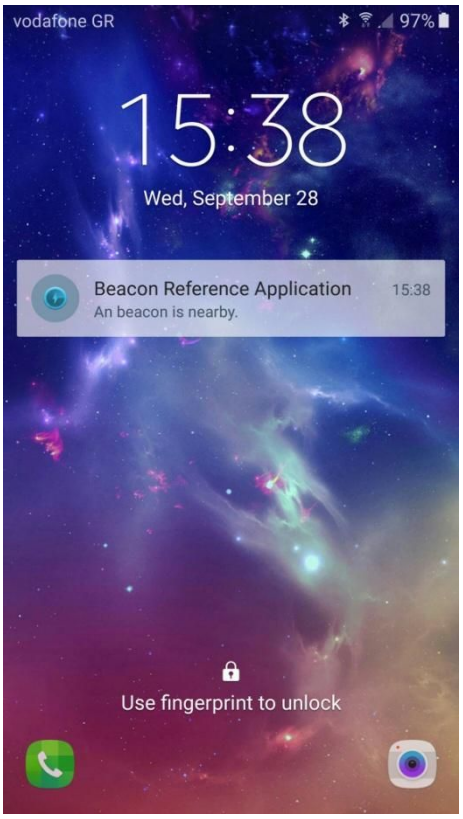


Εικόνα Ενεργοποίηση Bluetooth

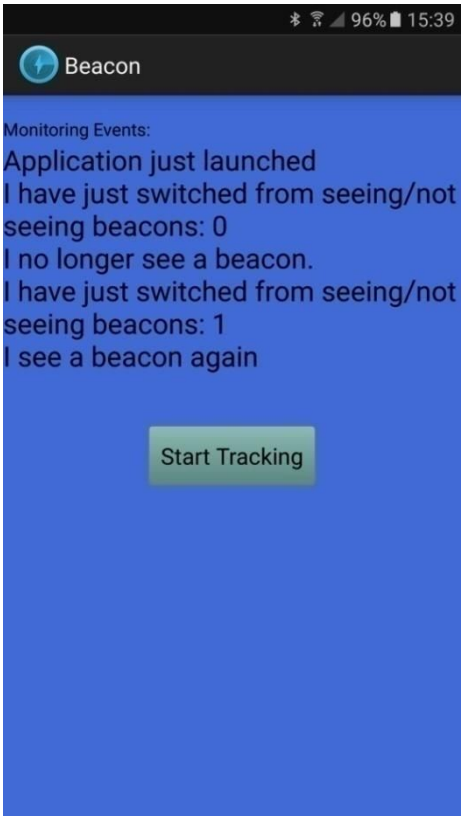


Εικόνα Αναμονή για πάτημα του κουμπιού εκκίνησης της διαδικασίας εύρεσης ibeacon

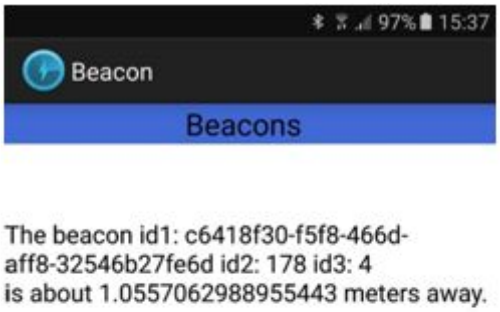
Εικόνα Αναμονή εύρεσης ibeacon



Εικόνα Ειδοποίηση ότι υπάρχει ibeacon στην περιοχή



Εικόνα Ενημέρωση για το πλήθος των ibeacon στην περιοχή



Εικόνα Καταγραφή και εμφάνιση των στοιχείων του ibeacon