ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΡΓΑΣΙΑ ΕΞΑΜΗΝΟΥ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ

Bluetooth

ΚΩΝΣΤΑΝΤΙΝΟΣ ΔΙΟΝΥΣΙΟΣ ΤΣΑΜΗΣ

Α.Μ 5908

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

Πατρα 2018

Περιεχομενα

3.11 Λίστα Εφαρμογών

ΑΚΡΩΝΥΜΙΑ

FHSS = Frequncy Hopping Spread Spectrum

AFH = Adaptive Frequency Hopping

GFSK = Gaussian Frequency Shift Keying

PSK = Phase Shift Keying

EDR = Enhansed Data Rate

LE = Low Energy

ΚΕΦΆΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

ΚΕΦΑΛΑΙΟ 1: Η Δημιουργία

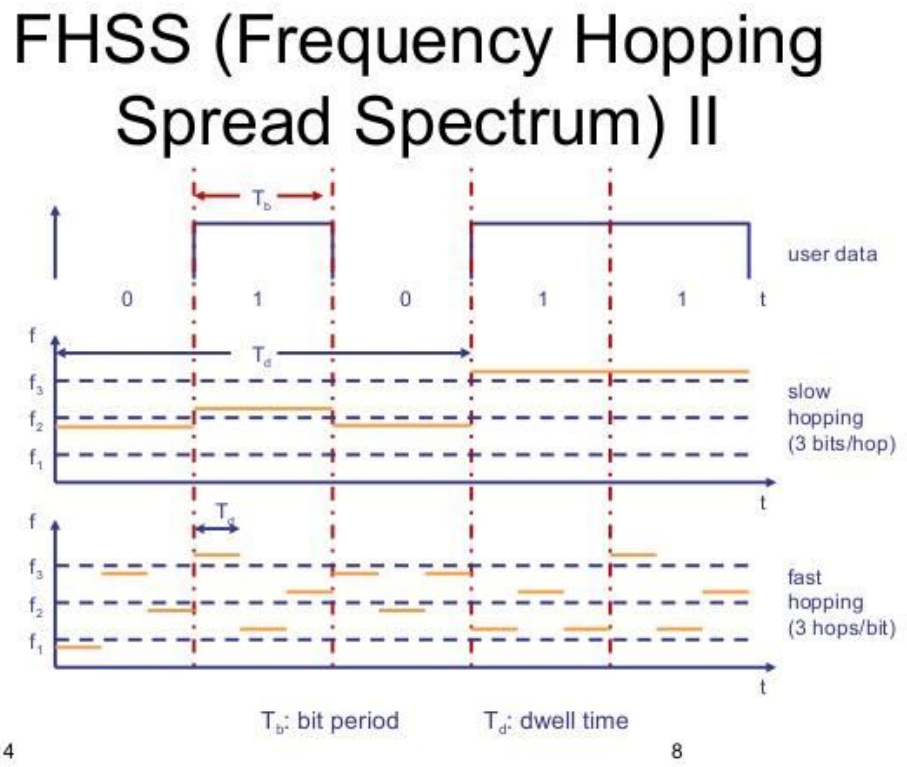
Η ανάπτυξη του bluetooth ξεκίνησε το 1989 από τον CTO της Ericsson, Nils Rydbeck και τον Johan Ullman. Σκοπός ήταν η δημιουργία ασύρματων ακουστικών. Ο Rydbeck ανέθεσε στον Tord Wingren την συγκεκριμενοποίηση των τεχνικών προδιαγραφών (Βασισμένες στην τεχνολογία FHSS) και στους Jaap Haartsen και Sven Mattisson (μηχανικοί στην Ericsson και Lund) την ανάπτυξη.

Η ονομασία του εμπνεύστηκε από το όνομα ενός Δανού Βασιλιά ο οποίος ένωσε όλες τις φυλές της Δανίας.

*1.1 **FHSS***

Πρόκειται για μια μέθοδο μετάδοσης ραδιοκυμάτων εναλλάσσοντας γρήγορα πάροχο μεταξύ πολλών καναλιών συχνοτήτων, χρησιμοποιώντας μια τυχαία συχνότητα την οποία όμως γνωρίζει και ο δέκτης και ο πομπός.

https://www.slideshare.net/ajal4u/fhss-37558708



ΚΕΦΑΛΑΙΟ 2: ΛΕΙΤΟΥΡΓΙΑ

ΚΕΦΑΛΑΙΟ 2: Λειτουργία

2.1 Κύρια Σημεία

Το bluetoth λειτουργεί είτε μεταξύ 2402 και 2480 MHz είτε μεταξύ 2400 και 2483,5 MHz, συμπεριλαμβανομένων των προστατευτικών ζωνών εύρους 2MHz στο κάτω άκρο και 3,5 MHz στο επάνω. Το bluetooth χρησιμοποιεί την ραδιοτεχνολογία FHSS. Χωρίζει τη μεταδιδόμενη πληροφορια σε πακέτα και μεταδίδει το κάθε πακέτο σε ένα από τα 79 κανάλια. Κάθε κανάλι έχει εύρος ζώνης 1MHz ενώ το bluetooth χαμηλής ενέργειας έχει εύρος ζώνης 2 MHz. Συνήθως πραγματοποιεί 800 hops ανα δευτερόλεπτο με το AFH ενεργοποιημένο.

Πρόκειται για packet-based πρωτόκολλο με αρχιτεκτονική master/slave. Ο master μπορεί να επικοινωνήσει μεχρι και με 7 slaves. Όλοι έχουν το ρολόι του master, βάση του οποίου γίνεται η ανταλλαγή πακέτων, και χρονίζεται στα 3200 Hz. Κάθε 2 χτύποι δημιουργούν ένα slot και κάθε 2 slot δημιουργούν ένα ζευγάρι. Στην απλή περίπτωση ο master μεταδίδει στα ζυγά slot και δέχεται στα περιττά. Το αντίστροφο ισχύει για τον slave.

2.2 Bluetooth χαμηλής ενέργειας (LE – Low Energy)

Πρόκειται για την τεχνολογία που μειώνει την κατανάλωση ενέργειας διατηρώντας παράλληλα το ίδιο εύρος επικοινωνίας. Η πρώτη εμφάνιση του low energy bluetooth ήταν στο bluetooth 4.0. Χρησιμοποιεί τις ίδιες ραδιοσυχνότητες 2,4GHz αλλά ένα πιο απλό σύστημα διαμόρφωσης. Σε αντίθεση με το κλασσικό bluetooth και τα 79 κανάλια του 1MHz, χρησιμοποιεί 40 κανάλια των 2 MHz. Μέσα στο κανάλι τα δεδομένα που μεταδίδονται χρησιμοποιούν GFSK διαμόρφωση. Η συγκεκριμένη διαμόρφωση περνά την κυματομορφή μέσα από το φίλτρο Gaussian

κάτι που κάνει τις εναλλαγές ομαλότερες. Για παράδειγμα μια εναλλαγή από το +1 στο -1 θα γινόταν ταχύτατα χωρις το φίλτρο. Με το πέρασμα από το φίλτρο από το +1 παει στο +0,99 στο +0,98... μέχρι το -1 κατι που μας δίνει έναν πολυ ομαλότερο παλμό.

Διαφορές κλασσικού και low energy bluetooth

Τεχνικές προυποθέσεις	Κλασσικό	Low energy
Μέγιστη απόσταση	100m	>100m
Ρυθμός μετάδοσης μεσω αέρα	1-3 Mbit/s	125 kbit/s – 1 Mbit/s – 2 Mbit/s
Ενεργά slaves	7	Εξαρτάται την υλοποίση
Χρονός Ανταπόκρισης	100ms	6ms
Ελάχιστος χρόνος μεταδοσης πληροφορίας	100ms	3ms
Δυνατότητα φωνής	Ναι	Οχι
Κατανάλωση ενέργειας	1W	0,01-0,5 W αναλόγως την περιπτωση χησης
Μέγιστη στιγμιαία κατανάλωση	<30mA	<15mA

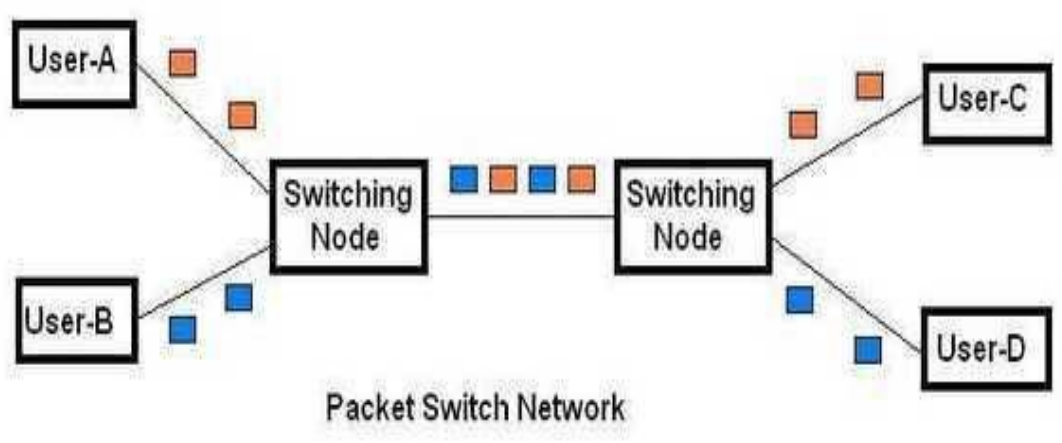
Συμβατά λειτουργικά συστήματα είναι :

- iOS 5 και μετά
- Windows phone 8.1 και μετά
- Windows 8 και μετά

- Android 4.3 και μετά
- Blackberry 10
- Linux 3.4 και μετά
- Unison OS 5.2

*2.3 **Packet switching***

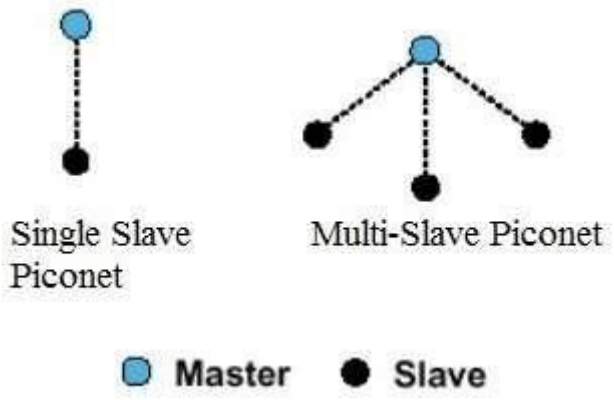
Είναι μια μέθοδος ομαδοποίησης μεταδιδόμενης πληροφορίας μέσω ψηφιακού δυκτίου, σε πακέτα τα οποία αποτελούνται από header και payload. Τα δεδομένα στο header χρησιμοποιούνται από το υλικό του δικτύου για να κατευθύνουν το πακέτο στον προορισμό του, οπού το payload του πακέτου αποσιμπιέζεται. Η μέθοδος αυτη είναι η αρχικη βάση για την επικοινωνια των δεδομένων στα υπολογιστικά δίκτυα παγκοσμίως.



https://www.diagramschematics.us/circuit-switching-and-packet-switching-diagram/

2.4 Master/ Slave

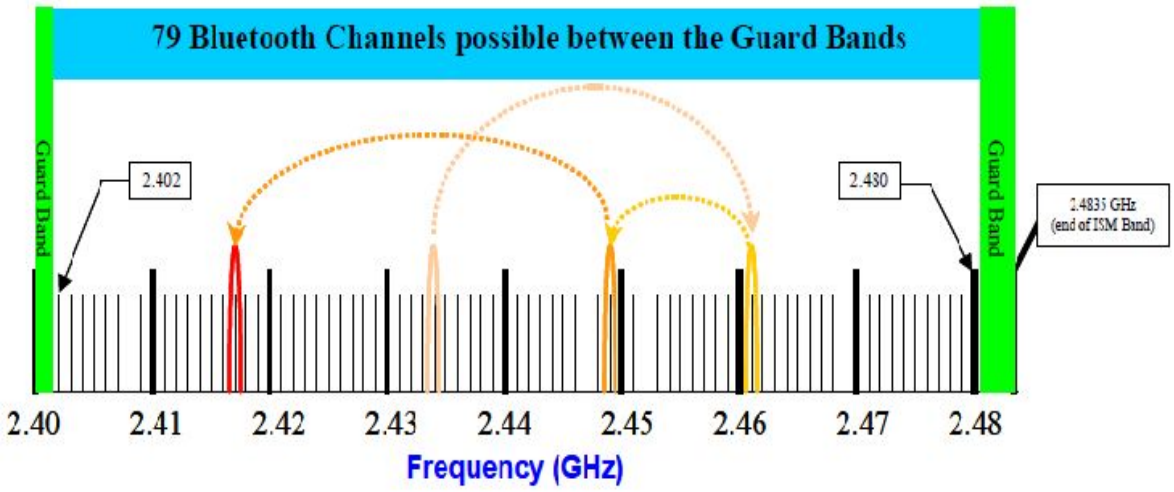
Είναι ένα μοντέλο επικοινωνιών όπου μια συσκευή ή μια διεργασία έχει τον έλεγχο



http://slideplayer.com/slide/4971167/

2.5 Adaptive Frequency Hopping (AFH)

Η κύρια ιδέα πίσω από το AFH είναι να χρησημοποιούνται μόνο οι "καλές" συχνότητες, αποφεύγοντας τις "κακές" οι οποίες είτε χρησιμοποιούνται απο κάποιον τρίτο είτε έχουν μπλοκαριστεί.



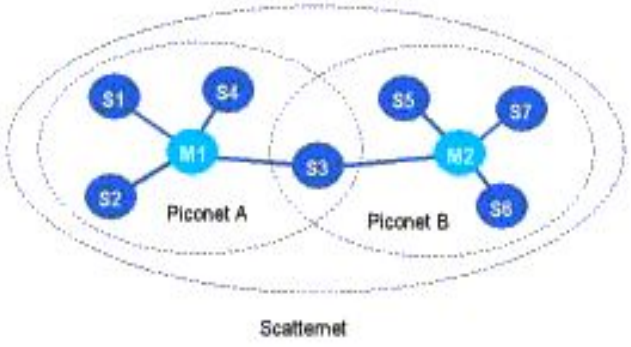
https://sites.google.com/site/nearcommunications/adaptative-frequency-hopping

2.6 Επικοινωνία και Σύνδεση

Μια master bluetooth συσκευή μπορεί να επικοινωνήσει με μέχρι και 7 συσκευές σε ένα piconet αν και δεν φτάνουν όλες οι συσκευές αυτό το μέγιστο όριο. Οι συσκευές μπορούν να αλλάξουν ρόλους και ο slave να γίνει master και το αντίστροφο. Για παράδειγμα τα ασύρματα ακουστικά όταν συνδέονται με ένα κινητό αναγκαστικά ξεκινούν ως master, αλλά υπάρχουν περιπτώσεις που μπορεί να λειτουργήσουν σαν slave. Οπιαδήποτε στιγμή τα δεδομένα μπορούν να μεταφερθούν μεταξύ του master και κάποιας αλλής συσκευής. Ο master επιλέγει σε ποια διεύθυνση θα κατευθύνει την επικοινωνία, συνήθως αλλάζει ταχύτατα σύνφωνα με τον αλγόριθμο round-robin. Μεγαλύτερο φόρτο έχει ο slave καθώς ο master απλά επιλέγει τον slave πρέπει να ακούσει σε κάθε slot που λαμβάνει.

2.6.1 **Piconet**

Ένα piconet είναι ένα δίκτυο το οποίο συνδέει ασύρματες ομάδες χρηστών-συσκευών χρησιμοποιώντας πρωτόκολλα bluetooth. Αποτελείται απο 2 ή περισσότερες συσκευές που χρησιμοποιούν το ίδιο κανάλι(συγχρονισμένα στο ίδιο ρολόι και). Πολλά piconet που επικοινωνούν μέσω ενός κόμβου δημιουργούν ένα scatternet.



http://www.tutorial-reports.com/wireless/bluetooth/architecture.php

2.7 Σύζευξη και Δέσμευση Συσκευών

Πολλές συσκευές που χρησημοποιούν το bluetooth μπορούν να εκθέσει προσωπικά δεδομένα ή να επιτρέψει σε μια συσκευή να ελέγχει την άλλη. Λόγοι ασφαλίας έκαναν αναγκαία την αναγνώριση συγκεκριμένων συσκευών, επιτρέπωντας έτσι τον έλεγχο στο ποιες συσκευές μπορούν να συνδεθούν σε κάποια άλλη συσκευή bluetooth. Την ίδια στιγμή είναι χρήσιμο για τις συσκευές bluetooth να να μπορούν να συνδεθούν χωρίς καμία παρεμβολή από τον χρήστη.

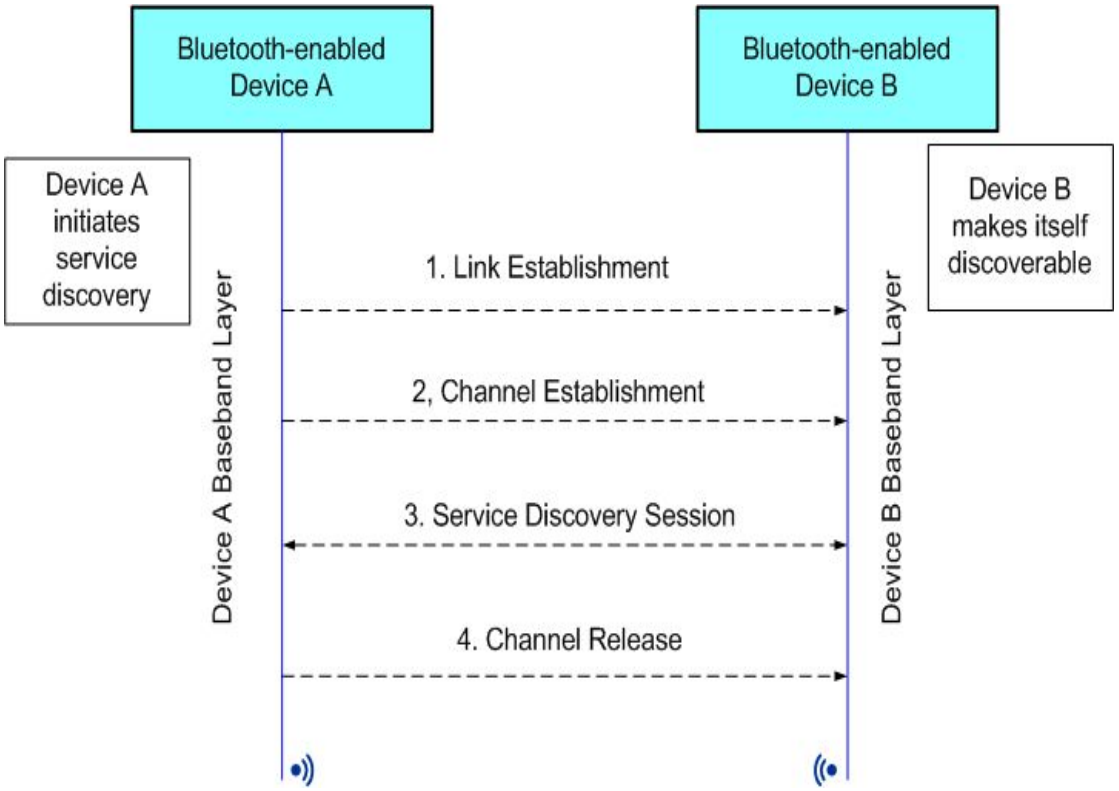
Για τους παραπάνω λόγους το bluetooth χρησημοποιεί μια διαδικασια που ονομάζεται δέσμευση και ο δεσμός δημιουργείται από μια διαδικασια που ονομάζεται σύζευξη. Η διαδικασία σύζευξης ενεργοποιείται είτε από κάποιο συγκεκριμένο αίτημα του χρήστη για να δημιουργήσει ένα δεσμο, είτε ενεργοποιείται αυτόματα όταν συνδέεται σε μια υπηρεσία όπου η ταυτότητα της συσκευής είναι απαραίτητη για λόγους ασφαλείας. Αυτές οι δύο περιπτώσεις αναφέρονται ως αφιερωμένη δέσμευση και γενική δέσμευση αντίστοιχα.

Η σύζευξη συχνά περιλαμβάνει κάποια αληλεπίδραση με τον χρήστη. Η συγκεκριμένη αληλεπίδραση επιβεβαιώνει την ταυτότητα των συσκευών. Όταν η σύζευξη ολοκληρώνεται επιτυχημένα δημιουργείται ο δεσμός μεταξύ των δύο συσκευών, επιτρέποντας σε αυτές τις συσκευές να συνδέονται η μια με την άλλη στο μέλλον χωρίς να επαναλαμβάνουν την διαδικασία σύζευξης για να επιβεβαιωθούν τις ταυτότητες των συσκευών. Όταν επιθυμεί, ο χρήστης μπορεί να αφαιρέσει τον δεσμό.

Κατά την σύζευξη οι δύο συσκευές εγκαθιδρύουν μια σχέση δημιουργώντας ένα κοινό μυστικό γνωστο ως κλειδί συνδέσμου. Εαν και οι δύο συσκευές έχουν το ίδιο κλειδί τότε λέμε ότι είναι συνδεδεμένες. Μια συσκευή που θέλει να επικοινωνεί μόνο με μια συνδεδεμένη συσκευή μπορεί πιστοποιήσει κρυπτογραφικά την ταυτότητα της άλλης συσκευής, επιβεβαιώνοντας ότι είναι η ίδια συσκευή που έκανε σύζευξη πριν. Όταν το κλειδί παράγεται, ένας πιστοποιημένος ασύγχρονος σύνδεσμος μεταξύ των συσκευών μπορεί να κρυπτογραφηθεί ώστε να προστατέψει τα δεδομένα που ανταλάσονται απο υποκλοπές. Ο χρήστης μπορεί να διαγράψει το κλειδί από οποιαδήποτε συσκευή, κάτι το οποίο αφαιρεί τον δεσμό μεταξύ των συσκευών, έτσι

είναι δυνατό για μια συσκευή να έχει αποθυκευμένο ένα κλειδί για μια άλλη συσκευή με την οποία πλέον δεν είναι συζευγμένη.

Οι υπηρεσίες bluetooth γενικά απαιτούν είτε κρυπτογράφηση είτε πιστωποίηση και ως τέτοιες απαιυούν σύζευξη πριν αφήσουν κάποια ασύρματη συσκευή να συνδεθεί.



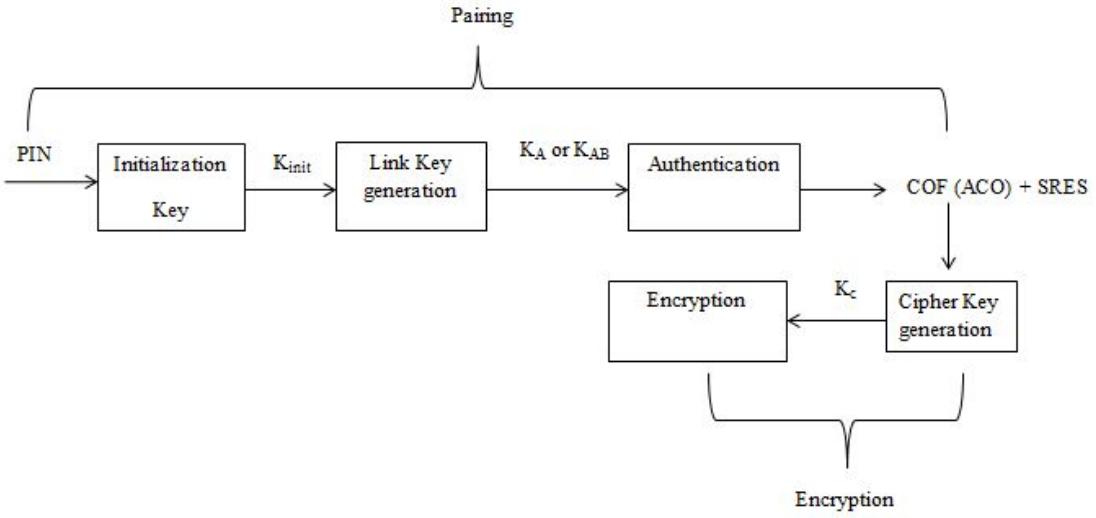
https://msdn.microsoft.com/en-us/library/cc510479.aspx

2.7.1 **Μηχανισμοί Σύζευξης**

Οι μηχανισμοί σύζευξης άλλαξαν σημαντικά με την σύστηση του bluetooth 2.1. Τα παρακάτω συνοψίζουν τους μηχανισμούς.

- Κληρονομική Σύζευξη : Η μόνη μέθοδος διαθέσημη για bluetooth 2.0 και πριν. Κάθε συσκευή πρέπει βάλει έναν κωδικό. Η σύζευξη είναι επιτυχημένη μόνο εαν και οι δύο συσκευές έχουν τον ίδιο κωδικό. Οποιαδήποτε σειρά 16-byte σε UTF-8 μπορεί να χρησιμοποιηθεί ως κωδικός, παρ'όλα αυτά δεν είναι όλες οι συσκευές ικανές να εισάγουν όλους τους πιθανούς κωδικούς. Σε

αυτή την κατηγορία έχουμε υποκατηγορίες. Αρχικα τις συσκευές περιορισμένης εισόδου, με το πιο απλό παράδειγμα να είναι τα ασύρματα ακουστικά που συνήθως έχουν κάποιον προυπάρχον κωδικό προγραματισμένο μέσα στη συσκευή. Συσκευές αριθμητικής εισόδου, οι κινητές συσκευές είναι το πιο κλασσικό παράδειγμα αυτών των συσκευών, επιτρέπουν στον χρήστη να εισάγει μια αριθμητική τιμή μέχρι 16 στοιχεία. Ακόμα υπάρχουν οι συσκευές Αλφαριθμητικής εισόδου, οπως οι υπολογιστές και τα smartphone που επιτρέπουν στον χρήστη να εισάγει ένα ολόκληρο κείμενο σε UTF-8 ως κωδικό.



https://www.researchgate.net/figure/Legacy-pairing-and-encryption-in-Bluetooth-connection-extracted-from-Morrow-2002_296443620

- Απλή Ασφαλής Σύνδεση: Αυτή απαιτείται από το bluetooth 2.1, παρ'όλο που το bluetooth 2.1 μπορεί να χρησημοποιήσει την Κληρονομικη σύζευξη για να συνδεθεί με μια συσκευή bluetooth 2.0 και πριν. Η συγκεκριμένη μορφή σύζευξης χρησημοποιεί μια μορφή κρυπτογράφησης δημόσιου κλειδιού. Η Απλή Ασφαλής σύνδεση ή αλλιώς SSP (Secure Simple Pairing) έχει τους ακόλουθους μηχανισμους πιστωποίησης:
    - Just works: Όπως και το όνομα λέει αυτή η μέθοδος απλά λειτουργεί χωρίς την αλληλεπίδραση του χρήστη. Όμως μπορει να ζητήση την επιβεβαίωση του χρήστη στην διαδικασία της συζευξης. Αυτή η μέθοδος συνήθως χρησημοποιείται από ασύρματα ακουστικά με

μικρές IO δυνατότητες και είναι πιο ασφαλές απ'ότι ο μηχανισμός με τον προυπάρχον κωδικό. Αυτή η μέθοδος δεν παρέχει καμια προστασία σε επιθέσεις.

- Αριθμητική Σύγκριση: Εάν και οι δύο συσκευές έχουν οθόνη, και τουλάχιστον μια απο τις δύο μπορεί να δεχτεί μια δυαδική είσοδο χρήστη ναι/όχι, τότε μπορει να χρησημοποιηθεί η συγκεκριμένη μέθοδος, η οποία εμφανίζει στην οθόνη της κάθε συσκευής έναν κωδικό έξι αριθμητικών ψηφίων. Ο χρήστης πρέπει να ελέξει και να συγκρίνει τους αριθμούς και να βεβαιωθεί ότι είναι ίδιοι. Εαν είναι όντως ίδιοι τότε ο χρήστης πρέπει να επιβεβαιώσει την σύζευξη στην συσκευή που μπορεί να δεχτεί είσοδο. Αυτή η μέθοδος παρέχει προστασία από επιθέσεις, δεδομένου ότι ο χρήστης έχει κάνει σωστα την διαδικασία και τον έλεγχο.
- Καταχώριση αντικλειδιού: Η μέθοδος αυτή μπορει να χρησημοποιηθεί μεταξύ μια συσκευής που έχει οθόνη και μιας τουλαχιστον που έχει οθόνη και πληκτρολόγιο. Στην περίπτωση που έχουμε μόνο την μια με πληκτρολόγιο τότε εμφανίζεται στην οθόνη ένας εξαψήφιος κωδικός τον οποίο ο χρήστης πρέπει να εισάγει στην άλλη μέσω του πληκτρολογίου. Στην περίπτωση που έχουν και οι δύο συσκευές πληκτρολόγιο τότε ο χρήστης κάθε συσκευής πρέπει να εισάγει τον ίδιο εξαψήφιο κωδικό. Η μέθοδος αυτή προστατεύει από επιθέσεις.
- Εκτός Εμβέλειας (OOB – Out Of Band) : Αυτή η μέθοδος χρησημοποιεί εξωτερικά μέσα επικοινωνίας όπως το NFC για να ανταλάξει πληροφορίες που χρησημοποιούνται στην διαδικασία σύζευξης. Η σύζευξη ολοκληρώνεται χρησημοποιόντας bluetooth ράδιο αλλά απαιτεί πληροφορίες από τον μηχανισμο OOB

Η SSP θεωρείται απλή για τους παρακάτω λόγους :

- Στις περισσοτερες περιπτώσεις δεν απαιτεί απο τον χρήστη να παράγει κάποιο κλειδί

- Για την Αριθμητική σύγκριση η προστασία από επιθέσεις μπορεί να επιτευχθει με μια απλή σύγκριση ισότητας από τον χρήστη
- Χρησημοποιόντας την μέθοδο OOB με NFC επιτρέπει την σύζευξη όταν οι συσκευές έρχονται απλά κοντά.

2.7.2 **Ασφάλεια**

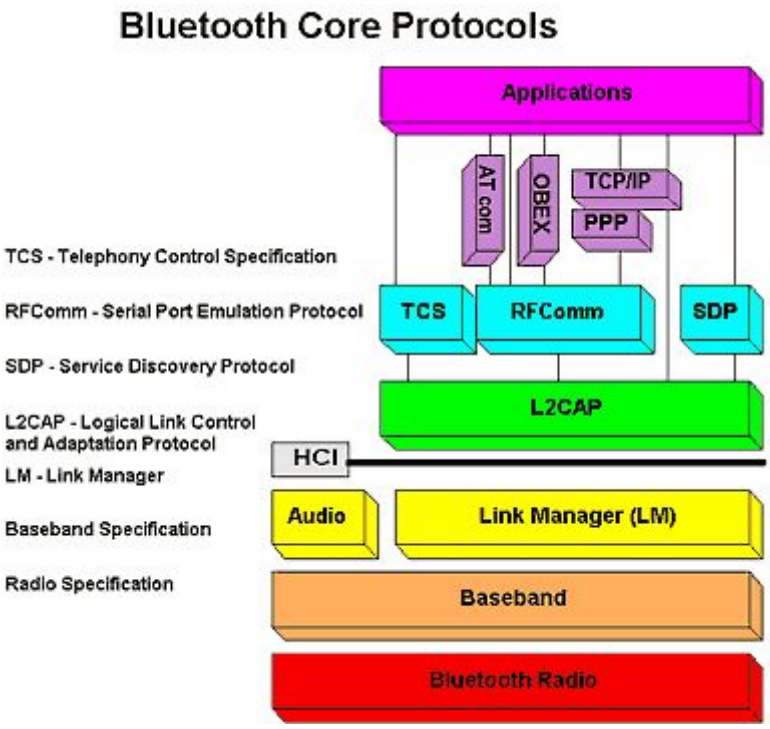
Το bluetooth ενστερνίζεται την παραγωγή εμπιστευτικότητας, πιστοποίησης και κλειδιού βασιζόμενο στην οικογένια ντετερμινιστηκών αλγορίθμων SAFER+ οι οποίοι αποτελούνται από μπλόκ αλγορίθμων τα οποία τα ονομάζουμε E(x) (Π.Χ. E20). Η παραγωγή του κλειδιού γενικα είναι βασισμένη περισσότερο στην πρίπτωση που ονομάσαμε παραπάνω ως καταχώρηση αντικλειδιού, οπού πρέπει να εισάγουμε και στις δύο συσκευές έναν κωδικό. Βεβαια η διαδικασία αλλάζει ανάλογα όταν η μια συσκευή έχει μέσα προγραμματισμένο κωδικό. Κατά την διάρκεια της σύζευξης ένα κλειδί αρχικοποίησης ή master κλειδί παράγεται χρησημοποιόντας τον αλγόριθμο E22. Το μπλόκ αλγορίθμου E0 χρησημοποιείται για την κρυπτογράφηση πακέτων και την παροχή εμπιστευτικότητας, και βασίζεται σε ένα κοινό κρυπτογραφικό μυστικό, το προηγουμένως παραγμένο κλειδί master. Το κλειδί αυτό χρησημοποιείται για την μεταγενέστερη κρυπτογράφηση των δεδομένων που στέλνονται μέσω της διεπαφής.

Ενώ το bluetooth έχει τα προτερίματα του, είναι ευάλοτο σε διάφορες επιθέσεις. Γιαυτό οι χρήστες και οι επιχειρήσεις θα πρέπει να αξιολογήσουν το μέγιστο αποδεκτό επίπεδο ρίσκου που μπορούν να έχουν.

Πριν το bluetooth 2.1 η κρυπτογράφηση δεν ήταν απαραίτητη και μπορούσες να την απενεργοποιήσεις όποτε ήθελες. Επιπλέον το κρυπτογραφημένο κλειδί είναι καλό για

περίπου 23.5 ώρες κάτι το οποίο επιτρέπει ,μετά το πέρας της χρονικής αυτή περιόδου, σε απλέ επιθέσεις να ανακτήσουν το κλειδί.

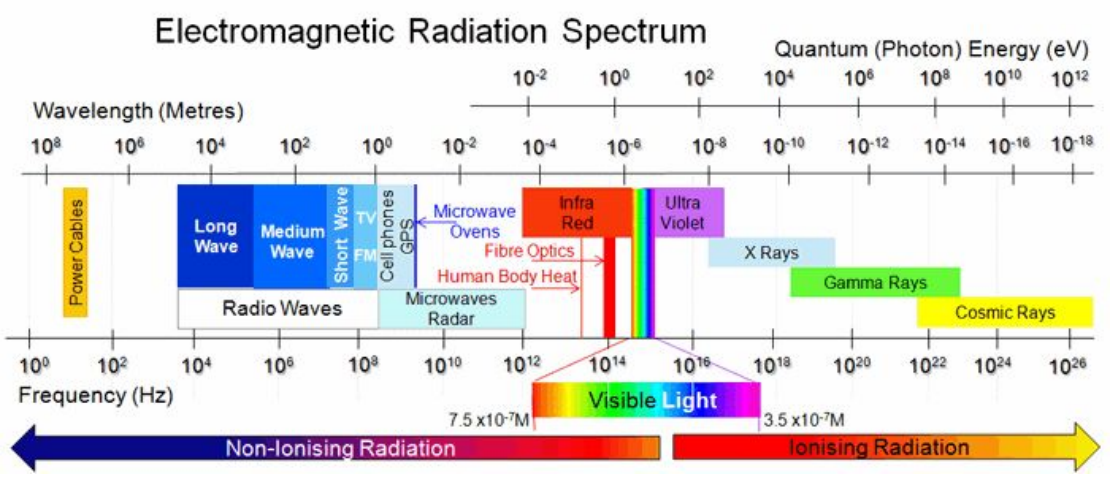
Ακόμα το απενεργοποιήσεις την κρυπτογράφηση είναι απαραίτητο για αρκετές λειτουργίες οπότε είναι δύσκολο να διαπιστώσεις εάν η κρυπτογράφηση έχει απενεργοποιήθεί για κάποια φυσιολογική λειτουργία ή απο κάποια επίθεση



https://securelist.com/bluetooth-bluetooth-security-and-new-year-war-nibbling/36074/

2.7.3 **Υγεία**

Το bluetooth χρησημοποιεί το φάσμα μικροκυμματων των ραδιοσυχνοτύτων στην περιοχή 2.402 GHz με 2.480GHz, η οποία είναι μη-ιονίζουσα ακτινοβολία, με παρόμιο εύρος ζώνης με αυτό που χρησημοποιείτε στα ασύρματα και κινητά τηλέφωνα.



http://www.mpoweruk.com/radio.htm

Μέχρι τώρα δεν έχει προκύψει κάποια συγκεκριμένη βλάβη που προκαλείται ακόμα και αν η ασύρματη εκπομπή έχει περιληφθεί στην λίστα πιθανών καρκινογόνων. Η μέγιστη εκπομπή ενέργειας από το bluetooth είναι 100mW για class 1, 2.5 mW για class 2 και 1 mW για class 3 συσκευές. Ακόμα και με την μέγιστη εκπομπή ενέργειας, το bluetooth εκπέμπει λιγότρη ενέργεια από ότι τα κινητά τηλέφωνα με την χαμηλότερη εκπομπή ενέργειας (η οποία κυμένεται απο 250 mW -2000 mW)

ΚΕΦΑΛΑΙΟ 3: ΕΞΕΛΗΞΗ

ΚΕΦΑΛΑΙΟ 3: Εξέληξη

3.1 Bluetooth 1.0 και 1.0B

Η πρώτη έκδοση του bluetooth (1998) είχε αρκετά προβλήματα και οι κατασκευαστές είχαν πολλές δυσκολίες στο να κάνουν τα προιόντα τους λειτουργικά. Επίσης είχαν υποχρεωτική μετάδοση της διεύθυνσης της συσκευής του bluetooth κατα την διαδικασία σύνδεσης , κάτι που έκανε τη ανωνυμία σε επίπεδο πρωτοκόλλων αδύνατο. Αυτό είχε αρνητική επίδραση σε υπηρεσίες που είχαν σκοπό την χρησιμοποίηση του bluetooth. Η μέγιστη απόσταση που υποστήριζε ήταν 10 μέτρα και το bandwidth 700kbps.

Όπως είδαμε το bluetooth χρησιμοποιεί την 2,4 Ghz συχνότητα την οποία και χωρίζει σε 79 κανάλια χρησιμοποιώντας το FHSS που είδαμε πιο πρίν για να μεταδώσει τα δεδομένα. Δυστυχώς στην Γαλλία, Ιαπωνία, Ισπανία και κάποιες άλλες χώρες η συγκεκριμένη συχνότητα χρησιμοποιείται και για άλλους σκοπούς (π.χ. στρατιωτικές επικοινωνίες). Έτσι το bluetooth 1.0B για να διευκολίνει τις χώρες αυτές, όρισε μια περιοχή σε αυτό το εύρος συχνοτήτων όπου απέφευγε συγκεκριμένες περιοχές. Την συγκεκριμένη περιοχή την χώρισε σε 23 κανάλια. Συσκευές που δημιουργήθηκαν να δουλεύουν σε 79 δεν μπορούσαν να επικοινωνήσουν με συσκευές για 23 κανάλια .

Ακόμα στην έκδοση 1.0B οι slaves δεν μπορούσαν να πουν στον master πόσα slots ανά πακέτο μπορούσαν να χρησιμοποιηθούν κατά την διάρκεια της επικοινωνίας.

Έτσι εάν ο master προσπαθούσε να στείλει περισσότερα slots ανά πακέτο από όσα μπορούσε να υποστηρίξει ο slave τότε η επικοινωνία αποτύγχανε.

3.2 ***Bluetooth 1.1***

Με την δεύτερη έκδοση του bluetooth διορθώθηκαν αρκετά λάθη της προηγούμενης, το σημαντικότερο ήταν η επικύρωση της ταυτότητάς τους. Όταν δυο συσκευές προσπαθούν να δημιουργήσουν μια σύνδεση το πρώτο πράγμα που θα κάνουν είναι να ανταλλάξουν κλειδιά επιβεβαιόνωντας την ταυτότητά τους. Εαν τα κλειδιά δεν ταιριάζουν τότε οι συσκευές δεν θα επικοινωνήσουν μεταξύ τους.

Υπό την έκδοση 1.0Β οι δύο συσκευές έμπαιναν σε έναν ατέλειωτο κύκλο κατα την αρχική επικοινωνία. Οι δύο συσκευές έτρεχαν τον αλγόριθμο για την δημιουργία του κλειδιού αλλά κάθε συσκευή δημιουργούσε ένα διαφορετικό κλειδί, πρόβλημα που περιστρέφεται γύρω από τον συγχρονισμό. Το ποιος δημιουργεί το σωστό κλειδί εξαρτάται απο το ποιος ξεκινά την επικοινωνία (ο master) και πόσο γρήγορα ανταποκρίνεται η άλλη συσκευή (ο slave). Εάν ο slave επεξεργάζεται πιο γρήγορα την πληροφορία απο τον master τότε δημιουργούνται συνθήκες τέτοιες ώστε κάθε συσκευή υπολογίζει ότι είναι ο master. Έτσι οι συσκευές αποτυγχάνουν να παράξουν ταιριαστά κλειδιά.

Το πρόβλημα αυτό το bluetooth 1.1 το λύνει ορίζοντας αναλυτικότερα τα βήματα που χρειάζονται για την επικύρωση των δύο συσκευών. Πιο συγκεκριμένα η έκδοση 1.1 απαιτεί κάθε συσκευή να επιβεβαιώσει τον ρόλο της στην σχέση master/slave, αναγνωρίζοντας το ποια συσκευή ξεκίνησε την διαδικασία της επικοινωνίας.

Ακόμα για να λυθεί το πρόβλημα με τις χώρες που χρησιμοποιούσαν τα 23 κανάλια η εταιρία του Bluetooth διαπραγματεύθηκαν με τις συγκεκριμένες χώρες ώστε να τους επιτραπεί να χρησιμοποιούν και τα 79 κανάλια κάτι το οποίο οδήγησε στη εξάληψη της λειτουργίας 23 καναλιών. Όλες οι συσκευές με Bluetooth 1.1 χρησιμοποιούν 79 κανάλια.

Επιπλέον στην έκδοση 1.1 λύθηκε το πρόβλημα με τα slots ανα πακέτο. Αυτό επιτεύχθηκε επιτρέποντας στον slave να επικοινωνήσει με τον master και δίνοντας του πληροφορίες σχετικά με το μέγεθος των πακέτων. Ο slave σε αυτή την έκδοση μπορεί να πεί στον master να στείλει λιγότερα ή περισσότερα slots ανά πακέτο αναλόγως την περίπτωση.

3.3 Bluetooth 1.2

Σε αυτήν την έκδοση για πρώτη φορά εισήχθηκε το Adaptive Frequency Hopping το οποίο όπως εξηγήθηκε και στην ενότητα 2.1.4 έχει σχεδιαστεί ώστε να μειώσει τις παρεμβολές μεταξύ ασύρματων επικοινωνιών στο φάσμα των 2.4 GHz που λειτουργεί το bluetooth.

Ακόμα βελτιώθηκε η επεξεργασία φωνής και η φωνιτηκή επικοινωνία ειδικά σε θορυβώδη περιβάλοντα. Αυτό το πέτυχε χρησημοποιόντας μεθόδους ανίχνευσης λαθών

Επιπλέον επιταχύνθηκε η διαδικασία σύζευξης μεταδύ δύο συσκευών κατι το οποίο βοήθησε πολύ στην βελτίωση της εμπειρίας χρήσης. Το πιο σημαντικό όμως ήταν ότι διατηρισε την συμβατότητα με τις παλαιότερες εκδόσεις κάτι που επέτρεπε σχεδόν σε όλους τους χρήστες, ακόμα και παλαιότερων εκδόσεων συσκευών, να επικοινωνίσουν.

3.4 Bluetooth 2 +EDR

Στην έκδοση αυτή η οποία κυκλοφόρησε το 2004 συστήθηκε για πρώτη φορά το Enhanced Data Rate (EDR) τεχνολογία που είχε σκοπό την ταχύτερη μεταφορά δεδομένων. Πράγμα που και έγινε αφού η ταχύτητα μεταφοράς αυξήθηκε από 721 kbit/s σε 2.1 Mbit/s.

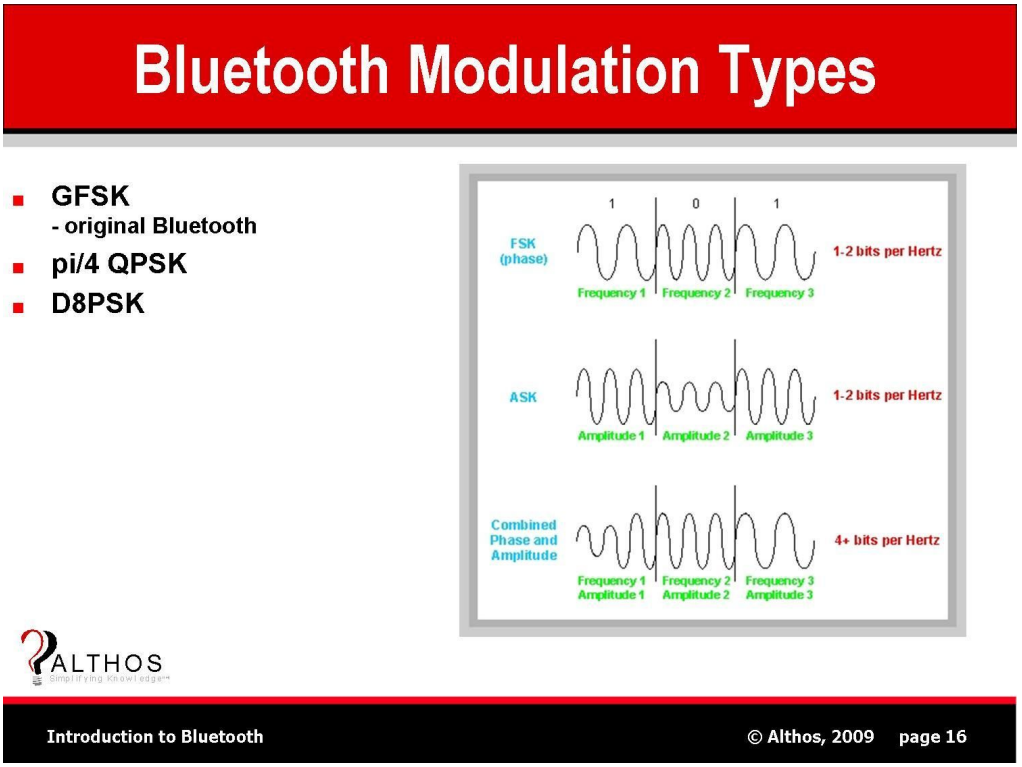
Το EDR χρησημοποιεί ένα συνδιασμό GFSK και Phase Shift Keying με δύο μεταβλητές π/4-DQPSK και 8DPSK. Το EDR μπορεί να προσφέρει χαμηλότερη κατανάλωση μέσω ενός κύκλου μειωμένης περιόδου.

Παρ'όλα αυτά το EDR είναι προαιρετικό χαρακτηριστηκό στην έκδοση αυτή. Πολλά προιόντα μπορούν να επικαλεστούν ότι είναι συμορφωμένα με τις τεχνικές προδιαγραφές του bluetooth 2.0 χωρίς να υποστηρίζουν τις μεγαλύτερες ταχύτητες μεταφοράς.

3.4.1 Gaussian frequency shift keying (GFSK)

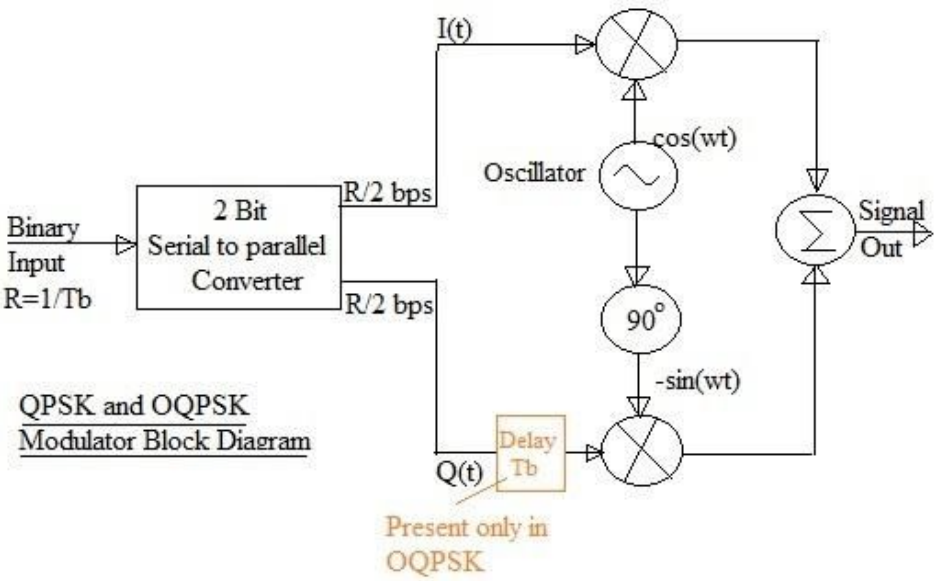
Αντί να διαμορφώνεται η συχνότητα κατευθείαν από τα σύμβολα των ψηφιακών δεδομένων και οι αλλαγές να γίνονται στιγμιαία, η μέθοδος που χρησιμοποιούμε περνάει τον παλμό δεδομένων μέσα απο ένα φίλτρο το οποίο ονομάζεται Gaussian filter. Το συγκεκριμένο φίλτρο έχει την δυνατότητα να μειώνει την ισχύ των γειτονικών συχνοτήτων. Έτσι αντί για το μη-φιλτραρισμένο FSK όπου η εναλλαγή θα γινόταν απο +1 σε -1, όταν η κυματομορφή φιλτράρεται η εναλλαγη περνάει απο ενδιάμεσες καταστάσεις, δηλαδη +1 +0.99 +0.98 …. -0.98 -0.99 -1.

http://www.althos.com/tutorial/Bluetooth-tutorial-modulation-types.html



3.4.2 Phase shift keying (PSK)

Είναι μια μέθοδος ψηφιακής διαμόρφοσης η οποία μεταφέρει δεδομένα αλλάζωντας (διαμορφόνωντας) την φάση ενώς σήματος αναφοράς. Η διαμόρφοση γίνεται αλλάζωντας τις εισόδους του ημιτόνου και το συνημιτόνου σε μια συγκεκριμένη χρονική στιγμή.



http://www.rfwireless-world.com/Terminology/QPSK-vs-DQPSK.html

3.5 Bluetooth 2.1 + EDR

Στην έκδοση αυτή που κυκλοφόρησε το ιούλιο του 2007 το κύριο νέο χαρακτηριστηκό του bluetooth 2.1 ήταν το secure simple pairing (SSP) κάτι το οποίο βελτιώνει την διαδικασία σύζευξης και ταυτόχρονα αυξάνει την δύναμη της ασφάλειας.

Ακόμα ένα χαρακτηριστηκό είναι το EIR το οποίο παρέχει περισσότερες πληροφορίες κατά την διάρκεια αναζήτησης των συσκευών κάτι που βοηθάει στο καλύτερο φιλτράρισμα των συσκευών.

3.6 Bluetooth 3.0 + HS

Η συγκεκριμένη έκδοση, η οποία εκδόθηκε το 2009, θεωρητικά υπόσχεται ταχύτητες που φτάνουν τα 24Mbit/s όχι όμως μέσω του συνδέσμου που δημιουργεί το ίδιο το bluetooth. Αντ'αυτού ο σύνδεσμος που δημιουργεί το bluetooth χρησημοποιείται μόνο για την διαδικασία που ορίζει ποιά συσκευή είναι ο master και ποιά είναι ο slave, ενώ τα μεγάλα πακέτα δεδομένων μεταφέρωνται μέσω ενός συνδέσμου 802.11.

Αυτή είναι και η κύρια προσθήκη σε αυτήν την έκδοση. Παρ'όλα αυτά το χαρακτηριστηκό της μεταφοράς των δεδομένων μέσω του συνδέσμου 802.11 δεν είναι υποχρεωτηκό και ως εκ τουτου μόνο οι συσκευές με το σύμβολο +HS υποστηρίζουν αυτή τη λειτουργεία.

3.7 Bluetooth 4.0 +LE

Η τέταρτη έκδοση η οποία ολοκληρώθηκε τον Ιούνιο του 2010 περιλαμβάνει τα προτόκολα του κλασσικού, υψηλής ταχυτητας, και χαμηλής κατανάλωσης bluetooth. Το υψηλής ταχύτητας βασίζεται στο wifi (802.11 όπως είδαμε και πριν), ενώ το κλασσικό bluetooth αποτελείται από κληρονομιμένα προτόκολα.

Το bluetooth χαμηλής ενέργειας (LE, έχει αναλυθεί στο δεύτερο κεφάλαιο) είναι ένα υποτμήμα του bluetooth 4.0 το οποίο έχει μια εξολοκλήρου νέα στήβα προτοκόλων για την γρήγορη δημιουργία απλών συνδέσμων. Ως εναλλακτηκή των των συνηθησμένων bluetooth προτοκόλων τα οποία συστήθηκαν στι εκδόσεις απο 1.0 μέχρι και 3.0, η συγκεκριμένη τεχνολογλια προτοκόλων έχει στοχεύσει τις εφαρμογές χαμηλής κατανάλωσης.

Σε σύγκριση με το κλασσικό bluetooth το LE προορίζεται να παρέχει σημαντικά μειωμένη κατανάλωση ενέργειας και κόστος διατειρώντας παράλληλα παρόμοιο εύρος επικοινωνίας .

3.8 ***Bluetooth 4.1***

Τον Δεκέμβριο του 2013 ανακοινώθηκε η επίσιμη υιοθέτηση της έκδοσης 4.1. Η έκδοση αυτή είναι μια σταδιακή ενημέρωση του λογισμικού της έκδοσης 4.0 και όχι κάποια αναβάθμηση στο υλικό. Η ενημέρωση αυτή προσθέτει νέα χαρακτηριστηκά τα οποία βελτειώνουν την εμπειρία χρήσης.

Σε αυτά τα χαράκτηριστηκά συμπεριλαμβάνονται η αυξανόμενη υποστήριξη για την συνύπαρξη με δίκτυα LTE, ο ρυθμός ανταλλαγής μεγάλης ποσότητας όγκου δεδομένων καιν η βοήθεια στους developers στο να καινοτομήσουν επιτρέποντας στις συσκευές να λειτουργούν και να υποστηρίζουν πολλαπλούς ρόλους ταυτόχρονα.

3.9 ***Bluetooth 4.2***

Η πρώτη έκδοση η οποία εισάγει χαρακτηριστηκά του λεγόμενου Internet of things. Κύριες βελτειώσεις έχουμε :

- Χαμηλής ενέργειας ασφαλή συνδεση με πακέτα δεδομένων
- Ιδιοτηκότητα επιπέδου συνδέσμου με εκτεταμένες πολιτικές φίλτων σκαναρίσματος
- IPSP έκδοσης 6

Παλαιότερες συσκευές θα μπορούσαν να λάβουν την 4.2 έκδοση με ενημέρωση του frimware τους.

3.10 ***Bluetooth 5***

Η 5η έκδοση του bluetooth η οποία παρουσιάστηκε επίσημα τον Ιούνιο του 2016 εστιάζεται στη επέλαση του Internet of Things. Παρέχει δυνατότητες που μπορούν να διπλασιάσουν την ταχύτητα των 2 Mbit/s με κόστος την μείωση της απόστασης ή μέχρι και τον τετραπλασιασμό της μέγιστης απόστασης με κόστος την μείωση του ρυθμού ανταλαγής δεδομένων και τον οκταπλασιασμό της χωριτηκότητας των μεταδιδόμενων δεδομένων αυξάνοντας το μήκος των πακέτων.

Κύριες περιοχές βελτείωσης είναι:

- Slot availability mask
- 2Mbit/s για LE
- LE μεγάλης απόστασης
- LE αλγόριθμος επιλογής καναλιού

3.11 Λίστα εφαρμογών

Οι εφαρμογές που έχει το bluetooth στην καθημερινή μας ζωή είναι παρα πολλές, κάποιες από αυτές είναι οι εξής:

- Ασύρματος έλεγχος και επικοινωνία μεταξύ κινητού τηλεφώνου και και ασύρματων ακουστηκών. Είναι μια από τις πρώτες εφαρμογές
- Ασύρματος έλεγχος και επικοινωνία μεταξύ κινητού τηλεφώνου και ηχοσυστήματος αυτοκινήτου
- Ασύρματα ακουστηκά και ενδοεπικοινωνία
- Ασύρματη μετάδοση ήχου σε ακουστικά με ή χωρίς δυνατότητες επικοινωνίας
- Ασύρματη μετάδοση δεδομένων απο μια συσκευή fitness σε κινητό
- Ασύρματη Δικτύωση μεταξύ υπολογιστών σε μικρό χώρο και όταν χρειάζεται μικρό εύρος ζώνης
- Μεταφορά αρχείων, επαφών κτλ
- Για εφαρμογές που χρειάζονται χαμηλό εύρος ζώνης
- Ασύρματη γεφύρωση μεταξύ δύο εργοστασιακών ethernet δικτύων
- Για την επικοινωνία των controllers με τις αντίστοιχες παιχνιδοκονσόλες
- Μετάδοση δεδομένων υγείας απο ένα μηχάνημα σε έναν υπολογιστή ή ένα κινητό σε μικρή απόσταση
- Σε συστήματα εντοπισμού πραγματικού χρόνου χρησημοποιούνται για να εντοπίσουν την τοποθεσία αντικοιμένων σε πραγματικό χρόνο

Βιβλιογραφία

Βιβλία:

Δημοσιεύσεις:

URLs:

https://en.wikipedia.org/wiki/Bluetooth_Low_Energy#Radio_interface

https://en.wikipedia.org/wiki/Packet_switching

https://en.wikipedia.org/wiki/Bluetooth#Origin

https://en.wikipedia.org/wiki/Master/slave_(technology)

http://blue-tooth.50webs.com/bluetooth1.1.html

http://grouper.ieee.org/groups/802/15/Bluetooth/profile_10_b.pdf

Αναφορές:

Πρότυπα: