**MAC SM BLUETOOTH**

**Geaba Alin**

**Marinescu Alexandru Valentin**

**Frîncu Robert**

**441A**

**CUPRINS**

1. Notiuni introductive despre tehnologia Bluetooth (Frîncu Robert)
2. Istoricul Bluetooth (Marinescu Alexandru)
3. Principiile Bluetooth (Frîncu Robert)
4. Specificatiile Bluetooth (Geaba Alin)
5. Protocoale de transport (Frîncu Robert)
6. Securitatea Bluetooth (Marinescu Alexandru)
7. Caracteristicile functionarii dispozitivelor radio Bluetooth (Geaba Alin)
8. Modele de utilizare a dispozitivelor Bluetooth (Marinescu Alexandru)
9. Bibliografie

**Cap.1 Noțiuni introductive**

 **despre tehnologia Bluetooth**

Tehnologia Bluetooth fără fir, a fost dezvoltată în 1994 de Ericcson, în Suedia. Principalul scop a fost, eliminarea necesității cablurilor pentru a realiza conexiuni între dispozitive, precum PDA-uri sau PC-ui. Chiar dacă exista conexiunea prin infraroșu la momentul respectiv, această soluție nu era viabilă deoarece era nevoie de o linie imaginara de o distanță foarte mică între dispozitive pentru a reuși conexiunea. Prin urmare, Ericcson a plasat câte un radio de putere joasă în fiecare dispozitiv, permițându-le să comunice fără fir prin ziduri sau orice alt material nemetalic. Dupa ce Erricson a început dezvoltarea Bluetooth-ului, acest concept a înflorit într-o tehnologie radio care conecta simultan multiple dispozitive într-o rețea personală(PAN).

Datorită posibilităților nenumărate ale Bluetooth-ului, în 1998 s-a format SIG(Special Interest Group) pentru continuarea dezvoltării specificării Bluetooth-ului IEE 802.15. Această specificare, standartiza dezvoltarea Bluetooth-ului, pentru ca dispozitivelor de la producători diferiți să le fie permisă comunicarea unuia cu celalalt.



**Cap.2 Istoric bluetooth**

Conceptul de bluetooth a fost inventat de compania Ericsson în 1994 și a fost conceptut ca alternativă pentru RS-232.

Specificațiile au fost formalizate de Bluetooth Special Interest Group (SIG), fondată în 20 May 1998. Companiile inițiale ce făceau parte din această organizație au fost Ericsson, IBM, Intel, Tochiba și Nokia. SIG supraveghează dezvoltarea specificațiilor, protejează trademark-ul și gestionează programele de calificare.

Termenul folosit pentru această tehnologie “Bluetooth” a fost inspirata din numele regelui danez Harald, care era supranumit “Dinte Albastru”. Acest rege a unit în secolul 10 triburile din Norvegia, Danemarca si Suedia. Ideea acestui nume a fost propusă în 1997 de Jim Kardach ce a dezvoltat un sistem de comunicație între telefoane mobile și calculatoare.

**Evenimente importante:**

1998: A fost fondată ogranizația SIG (Bluetooth Special Interest Group)

 Numele BlueTooth a fost adoptat oficial

1999: Specificațiile 1.0 au fost eliberate

2000: Primul telefon cu tehnologia Bluetooth apare pe piață

 Prima pereche de căști pe bazată pe această tehnologie

2002: Primul combo de mouse-tastatură

 Primu receiver GPS

2003: Bluetooth Core Specification, versiunea 1.2 a fost adoptată de SIG

2004: SIG adoptează Core Specification versiunea 2.0

2005: SIG lansează suita de testare (PTS) versiunea 1.0

2007: SIG lansează PTS versiunea 2,1,1

2008: SIG lansează PTS versiunea 3.0

2009: SIG adoptează versiunea 3.0 HS pentru CORE Specification

 SIG anunță Bluetooth v 4.0

2010: SIG adoptă versiunea 4.0 pt Core Specification

 Este lansat PTS v 4.1

2013: SIG lansează versiunea 4.1

2014: SIG lansează versiunea 4.2

**Cap.3 Principiile Bluetooth**

Sistemul nucleului (core) bluetooth constă în emiţătorul-transmiţătorul în frecvenţă radio (RF), banda de bază şi stiva de protocoale. Acest sistem oferă servicii care permit interconectarea dispozitivelor şi schmbul de informaţii între acestea.

Bluetooth operează într-o bandă nelicenţiată ISM, la 2,4 GHz. Sistemul implică un emiţător-receptor de bandă pentru a combate interferenţele si scăderea semnalului, precum şi mai multe canale de comunicaţie. Operaţiile în frecvenţă radio folosesc o frecvenţă modulată binar, perfect conturată pentru a diminua complexitatea tranceiver-ului. Rata pentru simboluri este de 1 Megasymbol pe secundă (Msps) suportând o rată de trasfer de 1 Megabit pe secundă (Mbps) sau, cu EDR (Enhanced Data Rtae), o rată mul mai mare de transfer de până la 3,2 Mbps. Cele două moduri de transfer sunt cunoscute ca Basic Rate (Transfer de Bază) sau Enhanced Data Rate (Transfer de date ridicat).

Pe parcursul unei operaţii obişnuite, un canal de comunicaţie radio este partajat de un grup de dispozitive sincronizate după un tact de ceas şi modulare în frecvenţă. Un dispozitiv oferă sincronizarea de referinţă şi este recunoscut ca *master* (principal). Restul dispozitivelor sunt recunoscute ca *slave* (secundare). Un grup de dispozitive sincronizate în acest mod formează o reţea de tip piconet (reţea de date ad-hoc care interconectează dispozitive utilizând protocoale Bluetooth). Aceasta reprezintă forma de bază a comunicaţiilor bazate pe tehnologia fără fir Bluetooth.

Până în prezent am prezentat pe scurt, la nivel de pricipiu, comunicaţiile Bluetooth. În continuare vom prezenta mai detaliat funcţionarea tehnologiei bluetooth şi a protocoalelor implicate.

**Cum funcționează Bluetooth-ul**

Tehnologia Bluetooth se învârte în jurul unui microcip de circa 9mm x 9mm, care funcționează ca un link pe distanta scurta și este si destul de ieftin in comparative cu alte metode wireless. Acoperirea acestei tehnologii este de 10m care suporta simultan atat transmisii de voce cat si de date pentru dispozitive multiple. Pana la 8 dispozitive pot fi conectate intr-o retea de tip piconet si pana la 10 piconet-uri pot exista pe aria de 10m a dispozitivului. Fiecare retea piconet suporta pana la 3 dispozitive de voce full duplex.

Viteza de transfer este 1Mb/s, dar de fapt rata reala este de 432kbps pentru transmisiunea full duplex , 721/56kbps pt transmisiunea asimetrica si 384kbps pt transmisiunea tms2000. Tehnologia wireless Bluetooth a fost conceputa sa fie la fel de sigura precum un fir avand implementate autentificari pana la 128biti cu chei publice/ private.



**Radio frecvența și salturile spectrale**

Chiar dacă zona va fi plină de zgmot, acesta nu va interfera cu conexiunea Bluetooth. A fost concepută să folosească ACK rapid și salturi în frecvență, ceea ce fac conexiunile robuste. Conexiunea este bazată pe pachete și va sări pe o nouă frecvență după ce pachetul va fi primit. Acest lucru nu ajută doar la eliminarea problemelor legate de interferențe dar de asemenea adaugă și un grad de securitate ridicată asupra pachetelor. Viteza este de 1Mb/s incluzând headerele. Transmisiile full duplex sunt asigurate prin TDM( time division multiplexing).

Cipul radio al Bluetooth-ul functionează într-o bandă nelicentiată ISM de 2.4GHz. Transmisiunea în bandă se face astfel: se separă banda de 2.4 GHz în 79 de subbenzi de câte 1MHz fiecare, pornind cu 2402 și terminându-se la 2480. Spectrul astfel împrăștiat este folosit pt a sari de pe un canal pe altul, într-o ordine la aleatoare ceea ce aduce un plus de securitate. Pot exista 1600 de salturi pe secundă. Raza standard a frecvenței este de 10m dar poate fi extinsă la 100m prin creșterea puterii de transmisie.

**Transmisiunea datelor**

Datele pot fi transmise în 2 feluri, sincron sau asincron. SCO(synchronous connection oriented) este o metodă folosită în primul rand pentru voce , și ACL(asynchronous connectionless) este folosită pt date. Într-o rețea piconet, fiecare pereche master-slave folosește o transmisiune diferită și moduri ce pot fi schimbate oricând. TDD(time division duplex) este folosit atât de SCO cât și de ACL, și ambele suportă 16 tipuri de pachete , dintre care 4 sunt pachete de control care sunt la fel în fiecare tip. Datorită nevoii de fluiditate în transmisiune, pachetele SCO sunt în general livrate la intervale de timp rezervate și sunt trimise în grup fără să permită altor transmisiuni să întrerupă transmisiunea curentă. Link-urile ACL suportă transmisiuni simetrice și asimetrice.

Latimea de bandă este controlată de o unitate master, care determină cât poate folosi din bandă fiecare unitate slave. Unitațile de tip slave nu pot transmite date până când nu au avizul unității master. Master-ul poate trimite mesaje de broadcast tuturor unitatilor de tip slave printr-un link ACL.

**Aranjamentul rețelei**

Topologia unei rețele Bluetooth poate fi punct-la-punct sau punct-la-multipunct. Orice unitate în piconet poate realiza o conexiune către alt piconet pentru a forma un scatternet.



 Fig 1.

**Cap.4 Specificații si trăsături**

Aparatele care dispun de Bluetooth comunică între ele atunci când se află în aceeași rază de acțiune. Ele folosesc un sistem de comunicații radio, așa că nu este nevoie să fie poziționate față în față pentru a transmite; dacă transmisia este suficient de puternică, ele pot fi chiar și în camere diferite.

Gruparea Bluetooth Special Interest Group (SIG) are rolul de a vinde firmelor tehnologia Bluetooth și de a urmări evoluția acestei.

Printr-o rețea Bluetooth se poate face schimb de informații între diverse aparate precum telefoane mobile, *laptop*-uri, calculatoare personale, imprimante, camere foto și video digitale sau console video printr-o unde radio criptate (sigure) și de rază mică, desigur numai dacă aparatele respective sunt înzestrate și cu Bluetooth.

**Bluetooth 1.0 și 1.0B**

Versiunile 1.0 și 1.0B au avut multe probleme tehnice care au facut producătorii să întâmpine mari dificultăţi în a face produsele lor funcţionale.

**Bluetooth 1.1**

* Multe din erorile găsite la versiunea 1.0B au fost reparate
* Suport pentru canale necriptate
* A fost adăugat un indicator al puterii semnalului de transmisie

**Bluetooth 1.2**

* Aceasta versiune este compatibilă cu 1.1.
* Viteza practică a transmisiei de date a fost mărită la 721 kbps, la fel ca la versiunea 1.1
* A fost introdus un flow control si moduri de retransmitere pt L2CAP.

**Bluetooth 2.0**

Această versiune este compatibilă cu versiunile 1.x. Principala îmbunătățire este introducerea unei viteze de transmisie mai mari numite *Enhanced Data Rate*, care permite o viteză de 3,2 mbps. Îmbunătățirea a creat următoarele efecte:

* viteza de transmisie de 3 ori mai mare,
* consum de energie mai mic,
* rata erorilor de transmisie (BER - *bit error rate*) mai scăzută.

**Bluetooth v3.0**

Versiunea 3.0 a fost adoptată de către Bluetooth SIG în data de 21 Aprilie 2009. Bluetooth 3.0 îmbunătățește viteza de transfer teoretică până la 24 Mb/s. Saltul vitezei a fost posibil datorită introducerii unei legături 802.11. Vitezele îmbunătățite nu pot fi prezente și în cadrul unei conexiuni cu un standard mai vechi datorită lipsei legăturii 802.11 în dispozitivele de generație mai veche.

**Bluetooth v4.0**

Versiunea Bluetooth v4.0 este mai bună decât versiunea Bluetooth v3.0. Aduce multe noutăți care fac viața oamenilor mai ușoară prin simpla apăsare a butonului ”Închide/Deschide Bluetooth” pentru a partaja împreună cu cei dragi fotografiile și aplicațiile dorite.

Aceasta versiune a fost denumita Bluetooth Smart si a fost adoptata in 30 iunie 2010, incluzand Bluetooth-ul clasic, Bluetooth high speed dar si Bluetooth low energy. Bluetooth-ul high speed este bazat pe wi-fi si cel clasic pe conectiuni bluetooth normale.

**Bluetooth 4.1**

Data adoptarii acestei versiuni este 4 decembrie 2013. Noutatile acestei versiuni sunt bazate strict pe partea software, partea hardware fiind aceeasi.

**Bluetooth 4.2**

A fost lansat pe 2 decembrie 2014. Introduce specificatii cheie pentru conceptul de Internet of Things.

**Cap.5 Protocoale de transport**

Arhitectura protocoalelor Bluetooth este asemănătoare cu cea a OSI. Scopul final al acestei arhitecturi este acela de a permite interoperabilitatea aplicațiilor. Acest lucru se realizează când aplicațiile din dispozitivele conectate rulează folosind protocoale identice. Stive diferite de protocoale sunt utilizate pt aplicații diferite. Ca structură, Bluetooth-ul foloseste un nivel fizic și legătura de date precum se observă în figură.



Fig.2

O aplicaţie nu utilizează toate protocoalele din stivă; în schimb, urmează una dintre căile verticale (a se vedea figură), conform necesităţilor serviciului corespunzător aplicaţiei. Stiva completă de protocoale conţine atât protocoale ce sunt specifice tehnologiei wireless Bluetooth, precum LMP şi L2CAP, şi acele protocoale, precum OBEX (Object Exchange Protocol), UDP (User Datagram Protocol) şi WAP (Wireless Application Protocol), care pot fi folosite pentru comunicaţii cu alte platforme.

**Protocoale ale Nucleului Bluetooth**

Aceste protocoale sunt specifice tehnologiei wireless Bluetooth, dezvoltate de Bluetooth SIG. RFCOMM şi TCS BIN au fost dezvoltate tot de către Bluetooth SIG, dar acestea se bazează pe standarde deja existente: ETSI TS 07.10 şi Recomandarea ITU-T Q.931. Protocoalele nucleului Bluetooth plus nivelul radio sunt cerute de aproape toate dispozitivele Bluetooth, în timp ce restul protocoalelor sunt utilizate doar la nevoie.

**Baseband (BB)**

Nivelul benzii de bază (baseband - BB) permite legătura fizică RF între unităţi Bluetooth ale unei pico-reţele. De vreme ce sistemele RF Bluetooth utilizează tehnologia cu spectru extins şi salt în frecvenţă, în care pachetele sunt transmise în fante temporale pe anumite frecvenţe, acest nivel utilizează proceduri Inquiry şi Page pentru sincronizarea transmisiei cu salturi în frecvenţă şi a clock-urilor diferitelor dispozitive Bluetooth.

Pachetele conţinând informaţii audio pot fi transferate între dispozitive Bluetooth, conform unor modele de utilizare. Informaţiile audio din pachetele SCO sunt rutate direct la şi din banda de bază, fără a mai trece prin L2CAP. Modelul audio este o componentă relativ simplă a specificaţiilor Bluetooth: orice două dispozitive Bluetooth pot transmite şi primi informaţii audio de la unul la altul doar prin deschiderea unei legături audio.



**Link Manager Protocol (LMP)**

LMP este responsabil de stabilirea (setarea) şi controlul legăturii între dispozitivele Bluetooth, incluzând controlul şi negocierea dimensiunilor pachetelor din banda de bază. Mai este de asemenea utilizat şi în procedurile de securizare: autentificare şi criptare. LMP controlează de asemenea modurile energetice şi ciclurile de lucru ale dispozitivelor radio Bluetooth şi stările conexiunilor unei unităţi Bluetooth într-o picoreţea. Mesajele LMP sunt filtrate şi interpretate de LM la recepţie, astfel că ele nu sunt niciodată transmise nivelelor superioare. Mesajele LMP au prioritate în faţa datelor utilizatorului. Astfel că, dacă LM necesită transmiterea unui mesaj, acesta nu va fi întârziat din cauza traficului L2CAP.



**Logical Link Control and Adaptation Protocol (L2CAP)**

L2CAP suportă pentru protocoalele superioare proceduri de multiplexare, de segmentare şi reasamblare a pachetelor şi de control a calităţii serviciilor (Quality of Service – QoS). L2CAP permite protocoalelor şi aplicaţiilor de nivel superior să transmită şi să primească pachete de date de până la 64 kbytes lungime. Deşi protocolul pentru BB oferă atât legături SCO cât şi ACL, L2CAP este definit doar pentru legături ACL şi nici nu este prevăzut vreun fel de suport pentru legături SCO. Canalele audio de calitate vocală, pentru aplicaţiile de telefonie şi audio, sunt manipulate prin legături SCO în banda de bază. Oricum, informaţiile audio pot fi împachetate şi trimise şi utilizând protocoale de comunicaţie prin legături la nivelul L2CAP.



**Service Discovery Protocol (SDP)**

Descoperirea de servicii este un element important în cadrul de lucru Bluetooth, deoarece SD stă la baza tuturor modelelor de utilizare. Cu ajutorul SDP, informaţiile despre dispozitive, servicii şi caracteristici ale dispozitivelor pot fi tabelate în liste, cu ajutorul cărora utilizatorul, cunoscând astfel serviciile dispozitivelor din vecinătate, poate selecta între aceste servicii. După aceasta, se pot stabili conexiuni cu unul sau mai multe dispozitive Bluetooth.

**Cap.6 Securitatea Bluetooth**

Sistemele pe baza de wireless reprezintă un risc de securitate deoarece unde radio pot să fie interceptate. Acest lucru poate sa ducă la compromiterea dispozitivului și a rețelelor la care este conectat.

 Link-urile bluetooth folosesc algoritmi de criptare și autentificare printr-o cheie pre-shared, considerați o metodă bună de securitate daca sunt implementați și folosiți corect. Securitatea bluetooth se bazează în primul rând lungimea și factorul aleator a cheii folosite pentru asocierea bluetooth, unde dispozitivele se autentifică mutual pentru prima dată, setează o cheie link pentru autentificari viitoare și encriptare.

Un alt factor important pentru securitate sunt setările conectivitatea și ușurința de a fi descoperit, unde aceste setări permit unui dispozitiv bluetooth să găsească și să se conecteze la un alt dispozitiv, iar o setare opțională de a accepta cereri de conectare oferă securitate în plus.

Bluetooth oferă câteva moduri de securitate:

* Modul 1: non-secure
* Modul 2: service level enforced security
* Modul 3: link level enforced security
* Modul 4: link level enforced security with encrypted key exchange

Dezvoltatorii de dispozitive determină ce mod să includă într-un dispozitiv bluetooth. Utilizatorii pot să hotărească dispoztive “trusted devices” ce pot să transfere date fară să ceară permisiune. Când un alt dispozitiv încearcă să se conecteze la un alt dispozitiv, utilizatorul repectiv trebuie să hotarească dacă îi oferă acest drept.

 Nivele de securitate a unui dispozitiv și nivele de securitate a unui serviciu lucrează împreună pentru a proteja dispozitivul de transmiteri de date neautorizate. O metodă de securitate inclusă constă în proceduri de identificare și autorizarea ce permite utilizatorului să facă o alegere în a deschide un fișier sau să accepte un transfer de date. Utilizatorul poate de asemenea să schimbe modul bluetooth în “non-discoverable” pentru a evita conectarea cu alte dispozitive bluetooth.

**Vulnerabilități:**

**Bluejacking**

Bluejacking constă în trimiterea de mesaje nesolicitate prin blutooth catre dispozitive bluetooth de exemplu telefonul mobil sau laptopuri. Acest mesaj conținea un cărți de vizite electronice și era transmis prin protocolul OBEX.

Bluejacking este de obicei inofensiv și usor de realizat. Procesul constă în:

1. crearea unui nou contact ,

2. introducerea mesajului în câmpul de nume,

3. salvarea contactului ,

4. trimiterea prin optiunea „send via Bluetooth”

Daca victima nu realizează ce înseamnă mesajul poate să adauge contactul trimis în contactele telefonului astfel când sunt trimise mesaje din nou există șansa să le deschidă automat deoarece contactul există.

**Bluesnarfing**

Bluesnarfing înseamnă furtul de informație de la un dispozitiv wireless prin conexiune bluetooth. Prin exploatarea unei vulnerabilități a implementării bluetooth atacatorul poate să acceseze informații precum agenda de telefon , calendarul , e-mai și mesajele. Dispozitivele sunt vulnerabile atunci când sunt în modul de descoperire și dacă opreste acest mod oferă un nivel de protecție

**Bluebugging**

Bluebugging este o tehnică ce permite atacatorilor să acceseze comenzi de telefon pe dispozitive bluetooth aflate în modul de descoperire. Astfel atacatorii pot să: inițieze convorbiri telefonice, asculte convorbirile telefonice, conecteze la internet.

De asemenea au capacitatea de bluesnarf, adică să citeasca mesaje , agende telefonice ,etc.

**Cap.7 Caracteristici sau parametri cheie ai**

 **funcţionării dispozitivelor radio Bluetooth**



**Modulatia**

Este de tipul GFSK (Gaussian frequency shift keying). Aceasta este o modulaţie cu deplasare de frecvenţă, pentru care filtrul FTJ folosit pentru limitarea spectrului de frecvenţă, este un filtru Gaussian. Produsul bandă-timp BT este un parametru care descrie calitatea formelor de undă transmise, exprimată ca produs între banda filtrului de modulaţie (FTJ gaussian) şi perioada unui bit.

Transmisia datelor se face la o viteză de semnalizare de 1 Msimbol/s, ceea ce înseamnă în condiţiile utilizării modulaţiei binare GFSK un debit de 1 Mb/s pe un link.



**Puterea la emisie**

Conform acestui parametru echipamentele se împart în 3 clase aşa cum se poate vedea în tabelul următor:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Clasa** | **Puterea maximă de emisie** | **Puterea nominală** | **Puterea minimă acceptată la o putere maximă setată** | **Menţiuni** |
| 1 | 100 mW (20 dBm) | - | 1 mW (00 dBm) | - |
| 2 | 2,5 mW (4 dBm) | 1mW | 0,25 mW (-6 dBm) | - |
| 3 | 1 mW (00 dBm) | - | - | Condiţia pentru un dispozitiv bluetoooth radio tipic |

**Fig.3**

**Sensibilitatea receptorului**

Nivelul de sensibilitate al unui receptor Bluetooth este definit ca nivelul unui semnal de intrare pentru care se atinge o rată a erorilor pe bit (BER) de 0,1%. Cerinţa este ca această rată să fie atinsă pentru un nivel de –70dBm sau chiar mai scăzut. Un receptor trebuie să atingă acest nivel de sensibilitate pentru semnale de intrare generate de orice transmiţător care este în conformitate cu specificaţia.
Puterea transmiţătorului şi sensibilitatea receptorului au valori stabilite special pentru reducerea costului şi a necesarului de putere pentru dispozitivele Bluetooth.



**Toleranţele pentru frecvenţele radio**

Se remarcă aici două probleme:

• acurateţea frecvenţei iniţiale (frecvenţa centrală, stabilită înaintea transmiterii oricărei informaţii)

• abaterea admisă pentru frecvenţele centrale la care se transmit efectiv pachetele de informaţie.

|  |  |
| --- | --- |
| **Lungimea în intervale temporle a pachetului** | **Abaterea admisă** |
| 1 | ±25 KHz |
| 3 | ±40 KHz |
| 5 | ±40 KHz |

Fig.4

**Cap.8 Modele de utilizare a**

 **dispozitivelor Bluetooth**

* **Tastatura si mouse prin Bluetooth**

Acest dispozitive periferice pot să fie conectate direct sau cu ajutorul unui receiver la calculator, tabletă sau alte dispozitive ce accepta input.



* **Scanare/printare prin bluetooth**

Majoritatea echipamentelor de printare vin cu opțiunea de scanare, listare fară a seta un cablu între desktop/laptop și imprimantă.



* **Cască Bluetooth**

Este unul dintre cele mai utilizate dispozitive bluetooth deoarece majoritatea telefoanelor permit conectarea unui astfel dispozitiv. De obicei este folosit pentru primirea de apeluri sau pentru redarea de muzică.



* **Transfer de date**

Dispozitivele pot să transfere informații, date, fișiere fară a se face conexiunea cu un fir.

**Bibliografie**

<http://www.ustudy.in/sites/default/files/images/btprotocoldiagram.gif>

<http://www.hp.com/ctg/Manual/c00186949.pdf>

<https://www.google.ro/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjh5vGbw7XKAhWJ1xQKHfv6Bw0QFgggMAA&url=https%3A%2F%2Fwww.bluetooth.org%2Fdocman%2Fhandlers%2FDownloadDoc.ashx%3Fdoc_id%3D40909&usg=AFQjCNHAduEsU-btfmmVb3cZjzDUTDLQ1g&sig2=MSsxbziM789xGZMWn34Kng>

<https://ro.wikipedia.org/wiki/Bluetooth>

<https://www.nsa.gov/ia/_files/factsheets/i732-016r-07.pdf>

<https://developer.bluetooth.org/TechnologyOverview/Pages/Security.aspx>

<http://electronics.howstuffworks.com/bluetooth4.htm>

<http://searchmobilecomputing.techtarget.com/definition/Bluejacking>

<http://www.wikihow.com/Bluejack>

<https://www.techopedia.com/definition/5046/bluesnarfing>

<http://www.webopedia.com/TERM/B/bluebugging.html>

<https://www.techopedia.com/definition/5044/bluebugging>

Fig.1 http://doi.ieeecomputersociety.org/cms/Computer.org/dl/mags/pc/2008/03/figures/mpc20080300061.gif

Fig.2

 http://images.slideplayer.com/15/4827865/slides/slide\_24.jpg