Universitatea Politehnica din Bucuresti. Facultatea de Electronica, Telecomunicatii si Tehnologia Informatiei

MAC SM Bluetooth

Lacatusu Raluca – Cristina

Serbanescu George
Grupa 441 A

Bucuresti 2013

CUPRINS:

Impartire cuprins pe student:

Lacatusu Raluca – Cristina – 1,2,5,6,7

Serbanescu George – 3, 4

1. Notiuni introductive despre tehnologia Bluetooth

Bluetooth este un standard pentru o retea personala wireless care se bazeaza pe unde radio. Conexiunea Bluetooth este diferita de conexiunile cu fir care conecteaza intre ele o multitudine de dispositive facand uz de o mare varietate de conectori cu diverse forme, marimi si numar de pini. Tehnologia Bluetooth elimina necesitatea de a conecta dispozitivele prin fire, intrucat dispozitivele pot comunica fara a fi conectate prin fire, ci folosind unde radio pentru a transmite si reception date.

Aceasta tehnologie a fost proiectata pentru transmiterea/receptionarea datelor pe distante scurte (~10m). Astfel, consumul de putere este mai redus, fiind ideala pentru dispozitivele mici, portabile, care functioneaza pe baterie.

Prin Bluetooth se pot transporta atat date cat si voce. Bluetooth-ul este un set de specificatii bazate pe unde radio, pentru o retea wireless personala si creeaza o cale prin care se poate realiza schimbul de informatii intre aparate (telefoane mobile, laptop-uri, imprimante etc.) printr-o frecventa radio sigura si de raza mica.

Dispozitivele Bluetooth comunica intre ele atunci cand se afla in aceeasi raza de actiune. Acestea folosesc un sistem de comunicatii radio astfel incat nu este nevoie sa fie aliniate pentru a transmite. Ele pot fi chiar in camera diferite, daca transmisiunea este puternica.

In 2008, la niversarea a 10 ani de existent, numarul de dispositive compativile cu Bluetooth livrate de la crearea ei a ajuns la 2 miliarde la nivel mondial. Aceasta tehnologie este utilizata nu doar de telefoanele mobile si PC-uri, dar si de aproape toate dizpozitivele electronice dedicate utilizatorilor, dispositive medicale, de fitness, masini sau case inteligente.

Bluetooth reprezinta cea mai usoara modalitate de a conecta echipamente intr-o retea comuna, mobila, care a revolutionat modul de utilizare al unui computer, si care a reusit sa mentina securitatea la un nivel ridicat.

(sursa - BLUETOOTH SPECIFICATION Version 2.1 + EDR, Bluetooth Qualification Program Reference Document (PRD,) 26 July 2007, http://www.bluetooth.com)

2. Istoricul Bluetooth

Conceptul de Bluetooth a aparut in cadrul diviziei de telefonie mobila a companiei Ericsson. Dr. Jaap Haartsen este cel care a inventat tehnologia Bluetooth, in timp ce lucra la Ericsson in anii 1990 si a fost nominalizat ca finalist al Premiului European pentru Inventatorul Anului in categoria industrie. Dr. Haartsen a colaborat cu o echipa de ingineri Ericsson pentru a face tehnologia Bluetooth disponibila pe piaţa. Cel mai apropiat colaborator al sau a fost Sven Mattisson

In 1998 a fost fondata organizatia Bluetooth Special Interest Group (SIG) din care faceau parte IBM, Intel, Motorola si Nokia. Aceasta organizatie are rolul de a vinde tehnologia Bluetooth firmelor care

vor sa implementeze aceasta tehnologie. Astazi SIG Numara peste 1800 de membri din intreaga lume. In 1999 SIG a lansat o platform open-source avand 1500 de pagini. Documentatia este disponibila tuturor, fabricantii avand drepturi de autor asupra produselor lor la baza carora sta aceasta specificatie.

Denumirea de “Bluetooth” este inspirata din numele regelui danez Harald, care era supranumit “Dinte Albastru” pentru ca fructele lui preferate erau afinele. Acest rege a unit in secolul 10 triburile din Norvegia, Danemarca si Suedia. Comparativ cu Harald, aceasta tehnologie uneste echipamente prin folosirea undelor radio.

(sursa – http://en.wikipedia.org/wiki/Bluetooth)

3. Principiile Bluetooth

Core-ul Bluetooth-ului este format din emitator – transmitator in frecventa radio, banza de baza si stiva de protocoale. Acest sistem permite interconectarea dispozitivelor si schimbul de informatii intre acestea.

Standardului Bluetooth, ca si WiFi, foloseste tehnica FHSS (Frequency Hopping Spread Spectrum), care presupune divizarea banzii de frecventa de 2.402-2.480 GHz, in 79 de canale, fiecare de cate 1MHz si transmit apoi semnalul folosind o secventa de canale cunoscuta de emitatoare si receptoare. Astfel, prin schimbarea canalelor standardul Bluetooth poate evita interferentele cu alte semnale radio.

Operatiile in frecventa radio folosesc o frecventa modulata binar pentru a diminua complexitatea transceiver-ului. Rata pentru simboluri este de 1 Megasymbol pe secunda (Msps) suportand o rata de trasfer de 1 Megabit pe secunda (Mbps) sau, cu EDR (Enhanced Data Rtae), o rata mult mai mare de transfer de pana la 3,2 Mbps. Cele doua moduri de transfer sunt cunoscute ca Basic Rate (Transfer de Baza) sau Enhanced Data Rate (Transfer de date ridicat).

Pe parcursul unei operaţii obişnuite, un canal de comunicatie radio este partajat de un grup de dispozitive sincronizate dupa un tact de ceas si modulare in frecventa. Un dispozitiv ofera sincronizarea de referinta si este recunoscut ca *master* (principal). Celelalte dispozitive sunt cunoscute ca *slave* (secundare). Un grup de dispozitive sincronizate in acest mod formeaza o retea de tip piconet (reţea de date ad-hoc care interconecteaza dispozitive utilizand protocoale Bluetooth). Aceasta reprezinta forma de baza a comunicatiilor bazate pe tehnologia fara fir Bluetooth.

Ocazional, doua retele de tip piconet pot intra in coliziune pe acelasi canal de comunicatie, dar vor comuta automat catre o noua frecventa si vor fi retransmise datele pierdute. Modelul comutarii de canal poate fi adaptat astfel incat sa excluda intervale de frecventa care pot interfera cu alte dispozitive.

Fizic, canalul de comuncatie este divizat in unitati de timp cunoscute sub denumirea de sloturi. Informatiile sunt transmise intre dispozitivele Bluetooth in pachete pozitionate in aceste sloturi. Aceasta

tehnologie permite transmisiunea de tip duplex prin utilizarea schemei diviziunii in timp. (TTD – time division duplex).

Inca de la lansare au fost elaborate mai multe cerinte pentru Bluetooth care, pe parcurs, au imbunatatit aspectele deficitare ale acestei tehnologii.

3.1. Versiuni

a) Bluetooth 1.0 si 1.0B

Prima versiune Bluetooth (1.0) apare in 1999. Versiunile 1.0 si 1.0B au avut multe probleme. Producatorii au intampinat dificultati in a rezolva aceste probleme pentru a face ca produsele sa fie interoperabile. Au existat cazuri in care dispozitivele cu Bluetooth sa nu se inteleaga intre ele, mai ales daca erau fabricate de firme diferite.

b) Bluetooth 1.1

Aceasta versiune a rezolvat multe din problemele existente la versiunile anterioare (1.0 si 1.0B). A fost introdus support pentru canalele necriptate. De asemenea, a fost adaugat un indicator al puterii semnalului de transminiune.

c) Bluetooth 1.2

Aceasta versiune adduce imbunatatiri seminificative, dar, in acelasi timp, este si compatibila cu versinea 1.1. Viteza practica a transmisiei de date a fost marita la 721 kbps. Cele mai semnificative modificari au fost:

- Dispozitivele devin mai rezistente la interferente cu alte aparate ce emit unde radio in spectrul 2.4GHz
- Viteza transferului de date creste
- Calitatea audio este imbunatatita – sunetul este mai clar daca sunt folosite headset-uri fara fir.

d) Bluetooth 2.0

Versiunea 2.0 este compatibila cu versiunile anterioare, dar aduce si imbunatatiri:

- Viteza de transmisie este de 3 ori mai mare
- Este introdusa Enhanced Data Rate (EDR) prin care viteza de transfer a datelor creste la 3Mbps, chiar sip e o raza de actiune de 100m in cazul unor dispositive

- Consum de energie mai mic – acest lucru este foarte folositor in cazul utilizarii laptopurilor sau a telefoanelor
- Rata erorilor de transmisie (BER – bit ratio error) mai mica
- O mai buna gestionare a conexiunii intre mai multe dispositive
- A fost introdus controlul fluxului de date si a modurilot de retransmisiue pentru L2CAP

e) Bluetooth 3.0

Versiunea 3.0 a fost adoptata de catre Bluetooth pe 21 aprilie 2009. Bluetooth 3.0 + HS ofera viteze de transfer teoretice de pana la 24Mbit/s. Principalele caracteristice sunt AMP (Alternate MAC / PHY), adaugarea de 802.11 ca un transport de mare viteza. Un dispozitiv Bluetooth 3.0, fara sufixul "+ HS" nu va beneficia de viteza foarte mare.

f) Bluetooth 4.0

Bluetooth SIG a lansat caietul de sarcini pentru versiunea 4.0 si aceasta versiune a fost adoptata la 30 iunie 2010.

Aceasta versiune este impartita in 2 grupuri: Bluetooth Smart Ready si Bluetooth Smart. Pentru a intelege de ce aceasta tehnologie a fost impartita in 2 grupuri trebuie sa analizam ce lipsuri avea vechea versiune de Bluetooth. Marile probleme ale vechii versiuni erau: consumul mare de baterie si asocierea/re-asocierea constanta a gadget-urilor conectate.

Bluetooth 4.0 este conceput pentru a rezolva aceste probleme si de a fi mai inteligent (de aici si denumirea de Bluetooth Smart) cu privire la gestionarea acestor conexiuni, mai ales atunci cand se pune accent pe conservarea energiei. Noua tehnologie pune mai putin accent pe mentiunerea unui flux constant de informatii. In schimb, se concentreaza pe trimiterea informatiei sub forma de biti putini atunci cand este nevoie si apoi pune conexiunea in modul “sleep” in perioadele urmatoare de “stand-by”.

Cand 2 dispozitive cu Bluetooth 4.0 sunt conectate se pierde putina baterie deoarece conexiunea este in stare latenta, exceptie facand cazul in care se trimit date critice. La dispozitivele cu Bluetooth 3.0 era recomandat sa se inchida Bluetooth-ul atunci cand nu era folosit. Acum nu mai este nevoie de acest lucru.

3.2. Comunicatii in radio frecventa prin frequency hopping

Specificatiile noi folosesc o tehnologie imbunatatita, care ajuta gadget-uri de zi cu zi sa fie conectate mai mult timp datorita faptului ca nu se consuma multa energie. In plus, Bluetooth 4.0 permite ca o noua clasa de gadget-uri, cum ar fi trackere de fitness, dispozitive medicale, brelocuri cheie pentru masina, chiar si luminile de acasa sa fie controlate mai usor.

Specificaţiile Bluetooth includ un sistem complex de soluţii hardware, software şi interoperabilitatea lor. Setul de specificaţii Bluetooth, dezvoltat de cei de la Ericsson şi celelalte companii, raspunde necesitaţii existenţei reţelelor fara fir cu raza mica de acţiune. Protocolul de baza Bluetooth este o combinaţie de circuite şi comutaţie de pachete ceea ce-l face potrivit atat pentru voce cat şi pentru date.

Tehnologia Bluetooth fara fir este implementata in emiţatoare-receptoare, mici şi ieftine, ce acţioneaza pe distanţe mici, şi care se gasesc deja incorporate in dispozitivele mobile sau care, in cazul notebook-urilor, sunt introduse in adaptoare ca PC card-uri.

Tehnologia Bluetooth foloseşte la nivel global banda radio de 2.4GHz, banda nelicenţiata de ISM(Industrial, Scientific, Medical). Utilizarea unei benzi de frecvenţa comune presupune utilizarea dispozitivului Bluetooth personal, oriunde in lume, existand astfel posibilitatea conectarii cu alte astfel de dispozitive.

Aşadar utilizarea acestei benzi presupune deopotriva aspecte pozitive cat şi negative: pozitive deoarece banda poate fi folosita fara nici un cost, negative pentru ca banda este finita şi mai sunt alte tipuri de dipozitive care utilizeaza aceeaşi banda. In prezent banda de 2.4 GHz mai este folosita de:

- Telefoanele fara fir ce utilizeaza banda de 2.4 GHz
- Reţelele fara fir 802.11
- Unele aparate care supravegheaza nou nascuţii
- Cuptoare cu micounde

Avand mai multe dispozitive ce utilizeaza aceleasi frecvente, banda se poate aglomera, iar acest lucru poate duce la aparitia unor interferente. Se poate intampla ca mesajul provenit de la o sursa oarecare sa fie receptionat de mai multe dispozitive radio, insa, pentru ca acestea sa se acordeze pe frecvenţele exacte, necesare recepţiei in secvenţa şi apoi asamblarii mesajului, trebuie sa cunoasca modelul frequecy hopping.

Avantajul modelului „frequency hopping” este reducerea interferentei radio, datorita faptului ca toate dispozitivele radio efectueaza acest salt de la o frecventa la alta in mod aleator si foarte repede.

Rolul de master si slave sunt temporale si au seminificatie doar atata timp cat dispozitivele cu aceste roluri se afla conectate in retea. Ele pot opera doar ca master sau doar ca slave.

Din acest punct de vedere, putem spune ca Bluetooth-ul isi schimba aleator frecventa de-a lungul unui spectru de frecventa, sarind pe o noua frecventa dupa ce primeste/trimite fiecare pachet de date. In concluzie, nu vor mai exista interferente pentru ca Bluetooth-ul nu se realizeaza pe o singura frecventa.

Al doilea avantaj al acestei metode este securitatea pentru comunicatii datorita faptului ca doar receptorul care cunoaste codul de imprastiere poate receptiona si asambla toate pachetele dintr-un mesaj. Pachetele sunt cantitati mici de date.

3.3. Conceptul de master si slave

Cand doua dispozitive se conecteaza si astfel stabilesc o conexiune Bluetooth, la nivelul de baseband, unul va avea rolul de master(stapan), iar celalalt va avea rolul de slave(sclav). Orice dispozitiv Bluetooth poate lua unul din aceste 2 roluri, sau chiar ambele roluri deodata, intr-o retea ca si master si in alta retea ca si slave.

Rolul de „master" se refera la modul de realizare a sincronizarii comunicatiei de tip FHSS intre dispozitive. „Master-ul" este cel care stabileste modelul frequency hopping, dar si faza secventei de salt. Toate dispozitivele „supuse" aceluiasi „master" isi vor schimba frecventa in acelasi timp cu „master-ul". De cele mai multe ori, „master-ul" este cel care initializeaza conexiunea.

Unele dispozitive Bluetooth pot fi configurate sa activeze intr-un singur rol, insa majoritatea işi pot asuma oricare rol, in funcţie de modul de utilizare in care este implicat. Aşadar, un dispozitiv master poate comunica cu mai multe dispozitiv slave, mai exact cu pana la 7 dispozitive slave active şi chiar pana la 255 de dispozitive slave aflate in stare inactiva, numita parked.

Dispozitivele slave, impreuna cu masterul, cu care comunica formeaza ceea ce specificaţia numeşte o picoreţea (piconet). Deci intr-o picoreţea nu poate exista decat un singur master. Relaţia master – slave este necesara in comunicaţia la nivelurile inferioare Bluetooth dar in general dispozitivele pot fi considerate "egale".

Atunci cand un dispozitiv stabileşte o legatura punct la punct cu un alt dispozitiv, rolul pe care fiecare dintre cele doua şi-l asuma – master sau slave – este adesea lipsit de importanţa, este irelevant pentru protocoalele de la nivelurile superioare, ca şi pentru utilizatorii dispozitivelor.

3.4. Bluetooth vs. Infraroşu vs. Wi-Fi

„Infrarosu" este o tehnologie fara fir care faciliteaza conectarea dispozitivelor(telefoane, PDA, laptopuri etc.) cu alte dispozitive mobile sau sincronizarea cu computerul. Infrarosul are raza de actiune foarte mica si nu transmite decat daca intre cele doua dispozitive nu exista obiecte. Infrarosul functioneaza prin emiterea unor unde optice. In schimb, Bluetooth-ul foloseste unde radio.

Aceasta tehnologie este folosita de telecomenzile TV. Distanta de la care poate functiona variaza in functie de puterea semnalului emitatorului, dar este de obicei mai mica de 10m. Pentru ca semnalul infrarosu sa fie detectat, trebuie sa existe o linie directa intre emitator si receptor. Daca exista un perete sau un obiect mare intre ele doua dispozitive, semnalul nu va putea trece mai departe.

Infrarosu a fost strandardizat de Infrared Data Association (IrDA). Un mare avantaj pe care il are tehnologia Bluetooth in fara tehnologiei IrDa este disparitia limitarii care impunea vizibilitatea directa intre cele doua „ochiuri" IrDA.

Bluetooth, pe de alta parte, foloseste o frecventa radio, care permite transmiterea prin pereti si prin alte obiecte.Gama standard a unui dispozitiv Bluetooth Clasa 3 este de aproximativ 50 m, ceea ce il face ideal pentru sincronizarea PDA-uri cu calculatoare, pentru folosirea castilor fara fir pentru telefonul mobil. Deoarece tehnologia Bluetooth se bazeaza pe un standard de frecventa de 2,4 GHz, diferite

dispozitive Bluetooth pot comunica de obicei unele cu celelalte, indiferent de producator. Cele mai multe dispozitive infrarosu functioneaza doar cu echipament avand acelasi producator.

Diferenta principala este aceea ca Bluetooth utilizeaza unde radio ultrascurte(lungimea de unda de ordinul cm), iar infrarosu utilizeaza trenuri de impulsuri optice, cvasi-luminoase (lungimea de unda 700-1600 nm). Cu infrarosu, senzorii ambelor dispozitive trebuie sa se afle in linie vizuala , fara obstacole intre emitator si receptor.

Infrarosu functioneaza numai intre doua dispozitive in acelasi timp. Undele radio strabat obstacolele, inclusiv peretii(evident, cu atenuare data de absorbţia energiei de mediul solid) si se emit omnidirecţional (sferic).

Bluetooth si Wi-Fi sunt tehnologii complementare. In timp ce Wi-Fi este o extindere a retelelor Ethernet , inlocuind reteaua de cabluri UTP arborescenta, Bluetooth este conceput pentru a inlocui firele intr-un spatiu cu raza de 10 metri, oferind conexiuni de date, voce si audio. Bluetooth este ideal pentru dispozitive cu putere generata de acumulator deoarece consuma putina energie.

In timp ce Bluetooth este pe cale de a inlocui infrarosu in multe domenii diferite, tehnologia nu este menita sa fie utilizata pentru crearea de retele fara fir. In schimb, tehnologia Wi-Fi, care are o gama mai larga si latime de banda mai mare decat Bluetooth, este standardul pe care cele mai multe echipamente de retea wireless il utilizeaza.

3.5. Sincronizarea automata

Dispozitivele portabile cum sunt computerele notebook, PAD-uri, telefoane inteligente (smart phones) ne fac viaţa mai uşoara oferindu-ne posibilitatea sa aflam intr-un mod rapid şi comod informaţii de care avem nevoie in viaţa de zi cu zi. Iar aceste informaţii pentru a fi cu adevarat utile necesita actualizarea continua.informaţii personale ca liste cu “lucruri de facut”, programari,diverse chestiuni organizatorice, etc. ar putea fi distribuite, conţinute in mai multe dispozitive pe care cineva le deţine şi le foloseşte.

Sincronizarea reprezinta procesul prin care date provenite din doua surse diferite fuzioneaza pe baza unui set de reguli, astfel incat cele doua seturi de date rezultate sa fie identice, sau cel puţin sa reflecte informaţii identice. Se doreşte deci ca datele conţinute in memoria unui dispozitiv sa corespunda cu cele dintr-un altul, primul asigurand actualizarea celui de-al doilea. Un exemplu comun este acela al sincronizarii unui personal digital assistant cu un computer desktop sau chiar cu un notebook.

Astazi acest lucru se realizeaza folosind cabluri seriale speciale şi software de asemenea specializat pentru un anumit tip de dispozitiv. Se poate spune ca, in varianta clasica sincronizarea este un proces conştient al utilizatorului datelor respective intru-cat implica conectarea unui cablu serial, apasarea unui buton sau indreptarea unul catre celalalt a doua dispozitive ce lucreaza in infraroşu, şi lansarea unei aplicaţii.

Cu Bluetooth totul este mult mai simplu: in primul rand protocoalele standard şi formatele obiectelor din specificaţia sa permit ca datele dintr-un dispozitiv sa fie sincronizate cu date dintr-un oricare alt dispozitiv, fie ca acestea sunt PDA-uri, computere notebook, telefoane inteligente sau chiar date accesate printr-un punct de acces la date.

Un alt fapt care pledeaza pentru inlocuirea variantei clasice de sincronizare prin fire, cu acest model de utilizare Bluetooth este acela ca prin Bluetooth se asigura, aşa cum spune şi numele modelului, o sincronizare automata, ceea ce inseamna ca sincronizarea se realizeaza imediat ce dispozitivele in discuţie se afla unul in vecinatatea celuilalt fara ca posesorul lor sa intervina in vreun fel (aceasta facilitate poarta numele de proximity networking).

(sursa - Lawrence Harte, Introduction to Bluetooth: Technology, Market, Operation, Profiles, & Services, *ALTHOS*, 2004)

4. Topologia comunicaţiilor Bluetooth

Modelul retelei Bluetooth este unul special datorita comunicarii de tipul "de la egal la egal" (peer-to-peer), adica dispozitivele comunicante sunt considerate egale. Aceasta inseamna ca atunci cand un dispozitiv radio se apropie de un altul si intra in "raza de actiune" a acestuia, ele pot stabili o conexiune. Dispozitivele Bluetooth pot fi configurate la nivelul baseband astfel incat sa accepte doar anumite conexiuni sau chiar sa nu accepte niciuna.

Distanta nominala pe care se poate desfasura o comunicatie intre dispozitive radio Bluetooth standard, adica cu nivel de putere de 0dBm, este 10m.

Datorita faptului ca dispozitivelor Bluetoth le este necesara o singura conditie pentru a putea incepe sa comunice intre ele – aceasta conditie fiind cunoscuta sub numele de *proximity networking* – pot aparea „personal aria networks" din care pot face parte: telefoane mobile, pagere, calculatoare notebook şi PAD-uri. O alta aplicatie a acestei facilitati de comunicatie este interactivitatea dintre dispozitivele mobile şi cele fixe (imprimante, puncte de acces la reţea – network access points – chioşcuri telefonice, automate pentru vanzare de produse diverse, etc.).

4.1. Retele Piconet

O reţea Piconet (picoreţea) este o reţea Bluetooth. Ea este alcatuita dintr-un dispozitiv **master** şi unul sau un dispozitiv care devine **slave.** Dispozitivul **master** este cel care initializeaza o conexiune Bluetooth. O picoretea poate fi compusa dintr-un dispozitiv master si maxim 7 dispozitive slave active.

Dispozitivele slave pot doar sa transmita date cand timpul de propagare este asigurat de dispozitivul master, altfel ele nu pot comunica direct unul cu celalalt, toata comunicatia fiind directionata prin dispozitivul master. Dispozitivele slave işi sincronizeaza saltul in frecventa cu cel al dispozitivului master utilizand ceasul dispozitivului master si adresa Bluetooth.

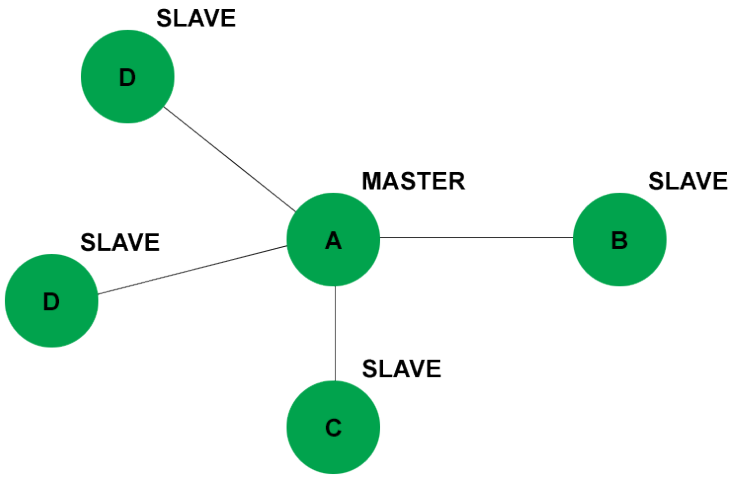

Fig. 1 Reţea Piconet

Reţelele Piconet au forma de stea cu dispozitivul master situat central. Pasul in frecvenţa nu este sincronizat intre reţelele Piconet, din acest motiv diferite reţele se pot ciocni arbitrar pe aceeaşi frecvenţa.

Dupa cum spuneam, o picoretea este alcatuita dintr-un singur master si mai multe dispozitive slave aflate in proximitate, care sunt conectate la acel master. In oricare moment dispozitivele slave se pot afla intr-una din starile active, sniff, hold sau parked. Pot exista, in limitele aceleasi suprafete, dispozitive care nu sunt supuse „masterului”, deci nu fac parte din picoretea, incluzandu-se aici cele aflate in standby.

De asemenea, este posibil ca un dispozitiv sa faca parte din mai multe picoretele in acelasi timp. Atunci cand doua sau mai multe picoretele se suprapun cel putin partial in timp si spatiu, se formeaza o retea *scatternet*. Principiile de organizare si functionare ale unei picoretele individuale se aplica pentru fiecare picoretea in parte din componenţa unei scatternet. Deci fiecare are un singur master si un set de slave-uri care pot fi active si parcate; fiecare are propriul sau model de salt al frecventei stabilit de catre masterul propriu.

Un slave poate face parte din mai multe picoretele pe rand, stabilind conexiuni cu diversi masteri din apropiere cu care se si sincronizeaza. Este posibil ca un acelasi dispozitiv sa fie slave intr-o picoretea si sa-si asume rolul de master intr-alta.

Topologia reţelei scatternet ofera o metoda flexibila prin care dispozitivele pot intretine conexiuni multiple, fapt extrem de util in cazul dispozitivelor mobile, care in mod frecvent se apropie si se departeaza de alte dispozitive.

4.2. Retele Scatternet

Unitatile Bluetooth care se afla in acelasi domeniu de actiune radio pot realiza conexiuni ad-hoc, punct la punct sau punct la multipunct. Mai multe picoretele legate ad-hoc formeaza **scatternet.** Un nod intermediar conecteaza doua picoreţele. Nodul intermediar trebuie sa-şi modifice in permanenţa ceasul astfel incat saltul in frecvenţa sa fie actualizat in fiecare picoreţea.

Acest lucru duce la o reducere a canalelor necesare transferului de date intre nodul intermediar şi cel de tip master, o reducere chiar la jumatate a ratei de transfer. Nu se noteaza in specificaţiile Bluetooth 1.1 sau 1.2 ce fel de pachete trebuie rutate intre picoreţele. Din aceasta cauza, comunicaţiile intre picoreţele nu sunt eficiente. Fiecare pico-retea este stabilita pe un canal diferit, cu salt in frecventa. Toti cei care utilizeaza aceeasi pico-retea sunt sincronizati pe acest canal.

4.3. Retele cu mai multe noduri

Prin schimbarea rolului, doua dispozitive pot avea fie rol de master, fie rol de slave intr-o picoreţea. Fie doua dispozitive A şi B. Dispozitivul A se conecteaza la dispozitivul B, deci A devine master in reţeaua Piconet constituita din dispozitivele A şi B ca in figura **Fig. 7.**

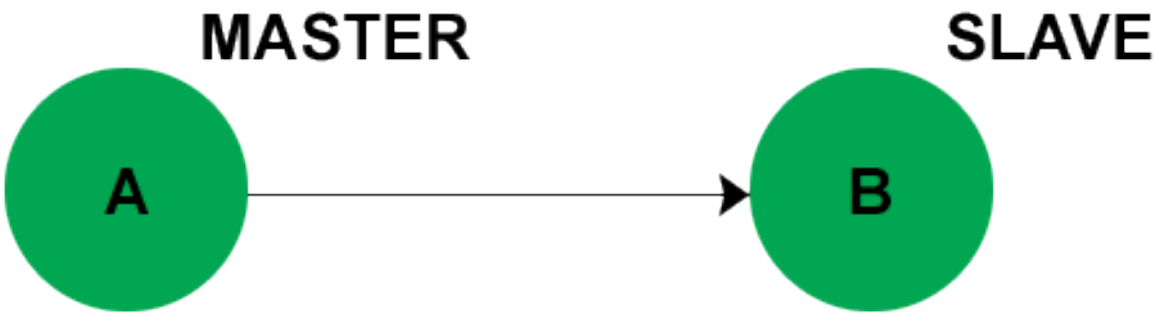

Fig. 2 Picoreţea cu doua noduri

Apoi un dispozitiv vrea sa se alature picoreţelei. Dispozitvul C se conecteaza la dispozitivul master, A. Intrucat dispozitivul C a iniţiat conexiunea, el devine automat dispozitivul cu rol de master al conexiunii dintre A şi C. In momentul de faţa avem doua dispozitive cu rol de master , deci prin urmare avem doua picoreţele. Dispozitivul A este nod intermediar pentru aceste doua picoreţele, avand rol de master pentru dispozitivul B şi rol de slave pentru dispozitivul C, precum in figura **Fig. 3.**

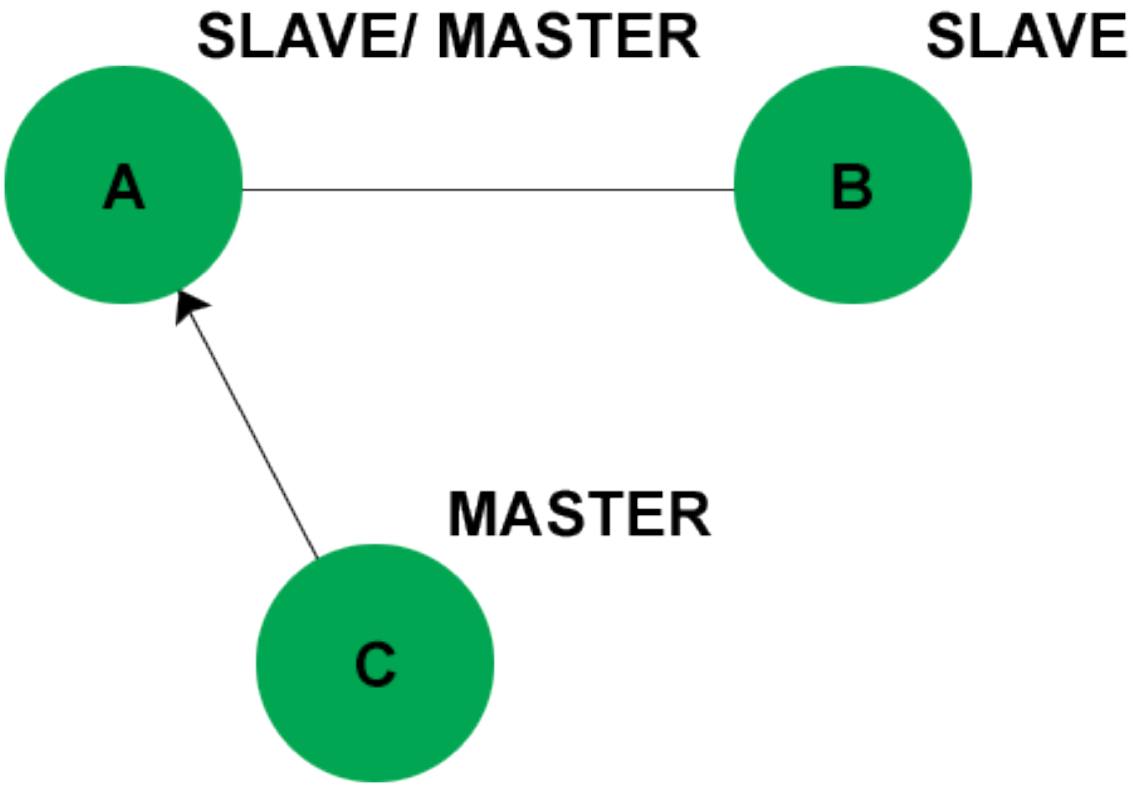

Fig. 3 Reţea Scatternet cu trei noduri

Figura **Fig. 3** ne arata ca schimbarea rolului intre dispozitivele A şi C conduce la formarea unei picoreţele in care dispozitivul A are rol de master şi ambele dispozitive B şi C rol de slave. Aşadar cand un nou dispozitiv vrea sa se integreze intr-o picoreţea este nevoie de un schimb de roluri , altfel se ajunge la o reţea de tip scatternet.

(sursa - http://electronics.howstuffworks.com/bluetooth3.htm

-https://docs.google.com/viewer?a=v&q=cache:JfCWn68hE0IJ:www.ee.ucl.ac.uk/~afernand/Example1.pdf+&hl=ro&gl=ro&pid=bl&srcid=ADGEESg65vh3WKLeWINTrrUkz2g79n3A4BvKIEG4A8w2Hgc0b1hPsq0ei9abIb0dWZtlocr1GUpbLpigIhUa1s-JHZKWzFLHV8VFXTnoGvqv7B2JVcBPrvyy7vAAb9DhnTr2xJaZaupp&sig=AHIEtbRpFNTuFOMATgaSbUl3graqfMyqYg)

5. Specificatii Bluetooth

Cu ajutorul protocoalelor Bluetooth, dispozitivele se pot localiza unele pe altele intr-o anumita suprafata, se pot conecta intre ele si pot schimba date intre ele.

5.1. Componentele stivei de protocoale

Exista 3 grupuri de elemente ale stivei de protocoale:

a) Grupul protocoalelor de transport

Acest grup cuprinde protocoalele ce permit dispozitivelor Bluetooth localizarea altor dispozitive Bluetooth, dar si crearea si configurarea legaturilor fizice prin care se face exchange de fisiere.

Acest protocoale sunt:

- Radio (RFCOMM – Radio frequency communication)
- Protocolul de control al legaturii logice (L2CAP – Logical link control and adaptation protocol)
- Protocolul Baseband

b) Grupul protocoalelor de mijloc (middleware)

Acest grup este format din protocoale de transport suplimentare, dar necesare aplicatiilor externe. Aceste protocoale sunt:

- PPP – Point to Point Protocol
- TCP – Transmission Control Protocol
- OBEX – Object Exchange Protocols
- SDP – Service discovery Protocol
- SMP – Low Energy Security Manager Protocol
- AVDTP – Audio/video control transport protocol
- LCP – Link Control Protocol
- NCPS – Network Control Protocols
- UDP
- IP
- WAP
- BNEP – Bluetooth ntework encapsulation protocol

c) Grupul aplicatiilor

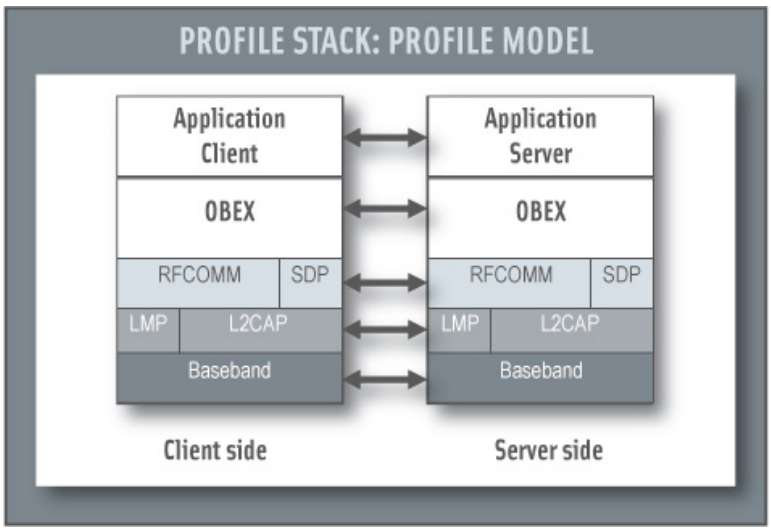

Figura 5.1 Stiva de protocoale Bluetooth

(sursa imagine - https://www.bluetooth.org/Building/HowTechnologyWorks/ProfilesAndProtocols/GOEP.htm)

(sursa - http://en.wikipedia.org/wiki/Bluetooth_protocols

https://docs.google.com/viewer?a=v&q=cache:3ffGYnJh1YoJ:www.bluetooth.org/docman/handlers/DownloadDoc.ashx%3Fdoc_id%3D89%26vId%3D128+&hl=ro&gl=ro&pid=bl&srcid=ADGEEShxZLhedilTdTWJG-CECy20dbL64LvUXfMx4yeZW-6PGaEMiJ47U52UfFrhykbkqr5__sYSz3AK2OjKksaI0041f2TrbW-EYOqrq74I2f7ZqsPlmZIIccQevuNzHp7IXF0giTFG&sig=AHIEtbSh3-zW6JDnAw4_TkC4jiJkqkUYNQ)

6. Securitatea Bluetooth

Caietul de sarcini Bluetooth include caracteristici de securitate la nivel de link. Acesta suporta autentificarea (unidirectionala sau reciproca) si criptarea datelor. Aceste caracteristici se bazeaza pe o cheie secreta care este partajata de o pereche de dispozitive. Pentru a genera aceasta cheie, o procedura de „pairing" este utilizata cand cele doua dispozitive comunica pentru prima data.

Organizatia Bluetooth SIG are in prezent peste 7000 de membrii, dar are si un grup se ocupa in permanenta de dezvoltarea securitatii. Acest grup primeste constant informatii si cerinte legate de securitatea datelor care se transmit prin Bluetooth.

Procedurile "link" sunt definite in Baseband Blueooth si in Link Manager Protocol Specifications. Profilele Bluetooth descriu modul de utilizare a protocoalelor Bluetooth intr-un mod interoperabil. In ceea ce priveste securitatea, aceasta se face in General Access. Acest profil specifica 3 moduri de securitate pentru un dispozitiv:

- Modul de securitate 1 (non-sigura/insecur) – Un dispozitiv nu va initia nicio procedura de securitate
- Modul de securitate 2 (securitate intarita la nivelul serviciului) – Un dispozitiv nu initiaza procedurile de securitate inainte de stabilirea canalului L2CAP. Acest mod permite politici diferite, dar si flexibile de acces pentru aplicatiile care ruleaza, dar care au si cerinte speciale de securitate.

- Modul de securitate 3 (securitate intarita la nivelul legaturii) – Un dispozitiv initiaza procedurile de securitate inainte ca legatura de set-up la nivel de LMP sa fie finalizata.

6.1. Nivele de securitate

Se pot defini diferite niveluri de securitate pentru dispozitive si servicii.

Pentru dispozitive exista 2 niveluri de incredere:

- Dispozitiv de incredere – dispozitiv cu retea fixa (pereche), care este de incredere si are acces nelimitat la toate serviciile;
- Dispozitic neacreditat sau „untrusted" – dispozitiv care nu are nicio relatie permanenta fixa (dar poate sa aiba o relatie temporara) sau un dispozitiv care are o relatie fixa, dar nu este considerata ca fiind de incredere. Accesul la servicii este limitat.

Pentru servicii, cerintele de autorizare, autentificare si criptare sunt stabilite in mod independent, dar unele restrictii inca se pot aplica. Cerintele de acces permit sa se defineasca 3 niveluri de securitate:

- Serviciile care necesita autorizarea si autentificarea – accesul automat se acorda numai la dispozitivele de incredere. Alte dispozitive au nevoie de o autorizatie de utilizare.
- Serviciile care necesita numai autentificarea – autorizare nu este necesara.
- Servicii deschise tutoror dispozitivelor – autentificarea nu este necesara, nu este necesara nici autorizaria de utilizare

Un nivel de securitate implicit este definit pentru a deservi nevoile aplicatiei. Acest nivel implicit va fi folosit doar daca alte setari nu se gasesc in baza de date „security" relationata la un serviciu anume.

6.2. Riscuri si Limitari

Au fost luate in considerare urmatoarele scenarii pentru a identifica limitarile:

- Scenariul 1 – Exista doua dispozitive Bluetooth. Fiecare dispozitiv are un set de aplicatii: calendar, sincronizare de fisiere etc. Cele doua dispozitive vor comunica printr-o legatura Bluetooth pentru a efectua o anumita sarcina, cum ar fi sincronizarea calendarelor.
- Scenariul 2 – Exista mai mult de doua dispozitive ca in scenariul 1. Toate dispozitivele vor comunica prin legatura Bluetooth pentru a efectua diferite sarcini care nu necesita securitate excesiva, cum ar fi schimb de carti de vizita sau de numere de telefon.
- Scenariul 3 – Un mic dispozitiv, cum ar fi un PDA necesita acces printr-o legatura Bluetooth la serviciile de infrastructura: Internet, e-commerce, baze de date corporative etc. Un astfel de device va fi conectat la un „punct de acces LAN" prin legatura Bluetooth. Punctul de acces LAN va fi conectat la serviciile de infrastructura prin intermediul unei retele LAN cu/fara fir. Aceasta este o structura ierarhica pe 3 nivele, unde primul nivel este device-ul, al doilea este reteaua LAN si al treilea este infrastructura.

Arhitectura de securitate Bluetooth are urmatoarele limitari:

- Suport pentru aplicatii dedicate – in toate scenariile, cererea nu va efectua apeluri catre managerul de securitate. In schimb, o aplicatie cu suport Bluetooth este obligata sa faca cereri in legatura cu securitatea la managerul de securitate Bluetooth.
- Numai dispozitivul este autentificat, nu si utilizatorul. Daca este necesara autentificarea utilizatorului, prin alte mijloace, vor fi necesare alte caracteristici de securitate.
- In legatura cu scenariul 1 – nu exista un mecanism definit pentru autorizarea prestabilita per serviciu. Cu toate acestea, o politica mai flexibila poate fi pusa in aplicare cu aceasta arhitectura, fara a fi nevoie de a schimba stiva de protocoale Bluetooth. Desigur, modificarile managerului de securitate, dar si procesele de inregistrare vor fi necesare.
- Arhitectura pe 3 niveluri – arhitectura de securitate prezentata este construita respectand procedurile de securitate Baseband, dar si securitatea legaturii si autentificarea reciproca a dispozitivelor.

Din punct de vedere al securitatii, algoritmii de criptare Bluetooth sunt siguri si eficienti. Au existat si cazuri in care datele au fost compromise, dar nu din cauza tehnologiei, ci din cauza implementarii.

6.3. Vulnerabilitati Bluetooth

6.3.1. Bluejacking

Bluejacking, cel mai vechi atac Bluetooth, este un bun exemplu de a arata modul in care securitatea si confortul utilizatorului se influenteaza reciproc. Metoda cea mai comuna de bluejacking se face prin procesul de trimitere a unei carti de vizite electronice Bluejackerii modifica procedura interschimbarii de carti de vizita. Persoanele cu telefoane in modul nedescoperibile evita atacul bluejack, dar ei trebuie sa efectueze un pas suplimentar de stabilire a accesibilitate, in scopul de a primi o carte de vizita legitima.

Bluejacking este foarte usor de facut. Ea incepe cu crearea unui nou contact in agenda telefonica a unui bluejacker, dar in campul Nume, in loc sa tastati numele unei persoane, bluejacker tipareste un scurt mesaj. Apoi, este pur si simplu o chestiune de a alege un telefon Bluetooth din apropiere, in metrou sau intr-un mall, de exemplu, si sa-l trimiti. Telefoanele care sunt in mod vizibil, si, astfel, disponibile pentru a fi bluejacker, apar pe ecranul telefonului bluejacker-lui. Dupa alegerea unuia, probabil la intamplare, bluejacker trimite cartea de vizita surogate, precum si de contact "nume" (mesajul) apare pe telefonul bluejacked.

Pentru ca este atat de usor bluejacking, acesta a devenit aproape un moft in Europa, in cazul in care primele telefoane cu Bluetooth s-au vandut.

Producatorii de telefoane, desigur, nu gasesc bluejacking amuzant, ei accentuand securitatea peste conectivitatea usoara.

6.3.2. Bluesnarfing

Cu bluesnarfing, puteti sa va conectati fara fir la unele telefoane Bluetooth fara stirea proprietarului telefonului si puteti descarca agenda, calendarul, si, uneori, mai mult. O versiune avansata a bluesnarfing poate modifica chiar si acele fisiere in unele telefoane bluesnarfed.

Bluesnarfing nu este o procedura simpla. Software-ul bluesnarfing scris in Java poate rula pe orice telefon mobil J2ME-a permis, ceea ce este mai putin probabil sa atraga suspiciune.

Un mijloc principal de bluesnarfing este cu un program numit Bloover. (Nume, o combinatie de Bluetooth si Hoover, a fost ales pentru programele care colecteaza informatii). Bloover a fost scris de Martin Herfurt, un cercetator de la Salzburg Cercetare Forschungsgesellschaft mbH si un lector de la Universitatea din Salzburg. Munca timpurie in definirea vulnerabilitatii bluesnarf a fost facut de Adam Laurie, avand sediul in Marea Britanie, iar acum este ofiter de securitate la Secure Bunker Gazduire Ltd., si de Marcel Holtman, un expert in Bluetooth si Linux. Herfurt, Laurie, si Holtman sunt toti membri ai Grupului de experti in securitatea Bluetooth SIG.

6.3.3. Bluebugging

Bluebugging este o forma de atac Bluetooth, adesea cauzata de lipsa de atentie. Este limitata de puterea de transmisie radio. Aceasta forma de atac merge mai departe de *bluejacking* si *bluesnarfing,* permitand preluarea aproape completa a unui telefon. Un bluebugger poate directiona un telefon sa efectueze apeluri fara ca proprietarul sa stie, apoi telefonul actioneaza ca un dispozitiv de bugging, interceptand conversatii din apropierea telefonului. In mod similar, un bluebugger poate seta redirectionarea apelurilor si apoi primirea apelurilor destinate victimei bluebug.

Bluebuggers au, de asemenea, capacitatea de bluesnarf, astfel incat acestea sa poata citi agende telefonice si calendare. Din fericire, exista doar putine modele vulnerabile la acest tip de atac.

Ca si in cazul bluejacking si bluesnarfing, procesul uneori incepe cu impingerea o carte de vizita electronica. La cateva telefoane Motorola timpurii, de exemplu, cineva ar putea trimite o carte de vizita utilizand o procedura care, pentru comoditate, nu au nevoie de autentificare sau de intrare PIN-ul. Cu telefoane noi, precum si cu telefoane mai vechi care au fost stabilite cu upgrade-uri de firmware, bluebugging devine mult mai dificil.

(sursa - http://www.eetimes.com/design/communications-design/4017819/

The-Bluejacking-Bluesnarfing-Bluebugging-Blues-Bluetooth-Faces-Perception-of-Vulnerability

- *http://www.bluejackingtools.com*
- *https://docs.google.com/viewer?a=v&q=cache:3ffGYnJh1YoJ:www.bluetooth.org/docman/handlers/DownloadDoc.ashx%3Fdoc_id%3D89%26vId%3D128+&hl=ro&gl=ro&pid=bl&srcid=ADGEEShxZLhedilTdTWJG-CECy20dbL64LvUXfMx4yeZW-6PGaEMiJ47U52UfFrhykbkqr5__sYSz3AK2OjKksaI0041f2TrbW-EYOqrq74I2f7ZqsPlmZIIccQevuNzHp7IXF0giTFG&sig=AHIEtbSh3-zW6JDnAw4_TkC4jiJkqkUYNQ*
- *https://docs.google.com/viewer?a=v&q=cache:_WDA-jwSJGsJ:www.bluetooth.org/docman/handlers/DownloadDoc.ashx%3Fdoc_id%3D90%26vId%3D129+&hl=ro&gl=ro&pid=bl&srcid=ADGEESg1ejyXLe0qyIX9Q2SQWB5lFyxFJDIgeaB8gIqBjCJyN21Su2z5H3dy5kRhpdghVID73K4CwMyiFYdBqoayTavMWjfpGcEZRe8epmQ4uuZDf0iKI0XtbALWlD3ZdXv0MZWeYcqn&sig=AHIEtbRF2414d_WbVydYULfjPfB6gy0LXg)*

7. Modele de utilizare a dispozitivelor Bluetooth

- *Casca Bluetooth* – este unul dintre cele mai utilizate dispozitive care foloseste Bluetooth-ul. Majoritatea telefoanelor permit conectarea unui astfel de dispozitiv. Utiliztorul castii Bluetooth poate primi apeluri telefonice fara a-si folosi mainile. Casca este obligatorie atunci cand utilizatorul este la volan.

(sursa - http://www.tu.ro/i/cado/b/casti-bluetooth-neon-bt-v2-0-ultra-compact-1306.JPG)

- *Tastatura si mouse prin Bluetooth* – aceste dispozitive periferice pot fi conectate la calculator ori printr-un receiver care se conecteaza la calculator, ori direct, fara a se folosi vreun cablu.

(sursa - http://fl1.shopmania.org/files/p/ro/t/321/kit-tastatura-mouse-dell-0yj097-bluetooth-multimedia~41648321.jpg)

- *Tehnologia NFC* – Near Field Communication este o retea wireless de frecventa inalta pe distante scurte, care permite schimbul de date intre dispozitive. Nokia a folosit tehnologia NFC pentru casti Bluetooth si pentru boxe.

(sursa - http://www.techspot.com/articles-info/385/nfc-uses2.jpg)

- *Printare/scanare prin Bluetooth* – majoritatea echipamentelor periferice de printare vin cu optiunea de listare, scanare fara a conecta un cablu intre laptop/desktop si imprimanta. Acest lucru este foarte benefic pentru ca nu mai exista cabluri intre cele 2 echipamente, dar si daca exista mai multe calculatoare conectate la o singura imprimanta.

(sursa - http://i.clubafaceri.ro/clients/34/79521/0/officejet-100-imprimanta-portabila-inkjet-color-a4-bluetooth-2274217_big.jpg)

- *Muzica si multimedia* – muzica poate fi ascultata facandu-se o legatura Bluetooth intre echipamente.
- *Transfer de date* – dispozitivele pot sa partajeze informatii, date, fisiere fara a se face conexiunea cu un fir.

(sursa - http://en.wikipedia.org/wiki/Near_field_communication)