Aplicatii Java



Proiect de curs

Student

Pascu Adrian

Profesor indrumator

Conf. dr. Petac Eugen

Anul I Medii Virtuale Multimodale Distribuite



Facultatea de Matematica si Informatica

http://www.modis.ro/assets/images/siglaUOC.gif

Universitatea Ovidius Constanta

Cuprins

Introducere

Bluetooth este un standard deschis proprietate tehnologia wireless pentru schimbul de date pe distanţe scurte (folosind transmisii de scurtă lungime de undă radio în banda ISM 2400 - 2480 MHz) de dispozitive fixe şi mobile, crearea unei reţele personale zona (PANS), cu un nivel ridicat de securitate. Creat de către furnizorul de telecomunicaţii Ericsson în 1994, [1] a fost iniţial conceput ca o alternativă fără fir la RS-232 cablurilor de date. Se poate conecta mai multe dispozitive, depăşirea problemelor de sincronizare.

Istoria tehnologiei Bluetooth

Free Bluetooth a fost lansat în 1994 de către Ericsson, o companie suedeză, în scopul de a elimina dezordinea în case şi birouri. În 1998, tehnologia Bluetooth a fost incepand de a lua forma şi a condus la dezvoltarea a grupului de interes Bluetooth Special (SIG), membrii fondatori IBM, Intel, Nokia, Toshiba şi Ericsson au aruncat oficial greutatea lor în spatele tehnologiei Bluetooth. În termen de şase luni, succesul şi versatilitatea tehnologiei Bluetooth a fost evidentă, şi alte companii au alăturat iniţiativei. De acolo, adoptarea standardului Bluetooth a explodat, în creştere în prezenţa globală, care este astăzi.

Evolutia standard Bluetooth

Tehnologia Bluetooth a fost proiectat pentru a permite schimbul de date şi voce, la tarife de până la1 Mbps pe secunda. Iniţial, standardul utilizat link-uri scurte gama de radio în 2.GHz Instrumentaţie ştiinţifice şi medicale (ISM) "banda liberă." Ariei de acoperire precoce a se situa în jurul valorii de dispozitive Bluetooth, 5 metri, dar acum - după extinderea în lăţime de bandă 700-800 kb - se atinge, în general, o gamă de aproximativ 10 metri, în cazul în care sa conexiuni fără sudură de radio a crea ceea ce este cunoscut ca o reţea fără fir personale. Gama de frecvenţe de transmisie pentru Bluetooth stă între 2,4 şi 2.4835 GHz, cu o viteză maximă de transfer de, de obicei, 2.0 Mbps pe secundă (unele dispozitive de a gestiona pana la 3 Mbps pe secunda). Gama, eficienţa şi viteza de tehnologia Bluetooth continuă să crească, datorită lucrărilor de Bluetooth SIG.

De ce se numeşte Bluetooth?

Dezvoltatorii acestei tehnologii fără fir folosit pentru prima dată numele de "Bluetooth" ca un nume de cod, dar ca trecut timp, numele blocat.  
Cuvântul "Bluetooth" este luat de la al 10-lea secol danez Regele Harald Bluetooth. Regele Bluetooth au fost influente în unirea scandinave Europa în timpul unei ere atunci când regiunea a fost sfâşiată de războaie şi de clanuri a început totul.  
Fondatorii de Bluetooth SIG simţit numele a fost de montare, deoarece:  
1) Bluetooth tehnologie a fost dezvoltat pentru prima oară în Scandinavia, şi  
2) tehnologia Bluetooth este capabil de a uni diferite industrii, cum ar fi telefonul mobil, de calcul, şi a pieţelor de automobile. Tehnologia fără fir Bluetooth simplifică şi combină forme multiple de comunicare fără fir într-o singură, sigur, consum redus de energie, low-cost, de frecvenţă radio disponibile la nivel global.

Bluetooth SIG

Numele de "Bluetooth" şi logo-ul său sunt mărci înregistrate de către privata comerciale de asociere numit Bluetooth Special Interest Group (SIG).  
Fondata in septembrie 1998, Bluetooth SIG este o unificare de lideri în domeniul telecomunicaţiilor, de calcul, reţea, automatizari industriale, şi de industria de automobile. Astazi, Bluetooth SIG este responsabil pentru încurajarea şi susţinerea de cercetare şi dezvoltare în tehnologia Bluetooth.  
Bluetooth SIG include companiile membre promotor Microsoft, Ericsson, IBM, Intel, Agere, Motorola, Nokia, şi Toshiba, plus mii de companii şi membru asociat aflată (BlueTomorrow.com e societatea-mamă, SP Commerce LLC, este un membru adoptă licenţă şi un certificat de Bluetooth SIG).

Bluetooth versiunile

Specificaţiei Bluetooth versiunea 1.1 şi anterioare  
Mai multe versiuni caietul de sarcini Bluetooth au fost lansate începând cu tehnologia Bluetooth a fost introdus în 1998.  
Versiunile 1.0 si 1.0B au avut prea multe probleme şi constrângeri pentru producători pentru a dezvolta cu succes dispozitive Bluetooth. Principala problemă a fost lipsa de interoperabilitate între dispozitive.  
Versiunea Bluetooth 1.1 Core este prima versiune de operare cu adevarat de succes a tehnologiei Bluetooth. Bluetooth 1.1 corectat multe dintre problemele găsite în versiunile anterioare. Ca rezultat: Dispozitive folosind Bluetooth 1.1 au interoperabilitate mult mai mare.

Bluetooth Versiunea 1.2

Multe dintre noile dispozitive Bluetooth, precum telefoanele celulare mai recente, sunt vândute cu versiunea mai nouă caietului de sarcini Bluetooth 1.2. Deci, ceea ce noi caracteristici / beneficii are Bluetooth 1.2 oferă?  
• înapoi compatibil cu Bluetooth 1.1  
• Frecvenţă adaptivă Hopping - ajută la reducerea interferenţelor radio prin eliminarea de utilizare a frecvenţelor înghesuiţi în secvenţa de salt  
• Viteze de transmisie (1 Mbps)  
• Conexiuni extinderea sincrone orientate pe link-uri - îmbunătăţeşte calitatea vocii de conexiuni audio prin care sa permita retransmisia de date corupte.  
• Puterea semnalului primit Indicator  
• Host Controller Interface (HCI), suport pentru 3-fire UART  
• acces la informaţii HCI calendarul pentru aplicaţii Bluetooth

Bluetooth versiunea 2.0 + EDR (Enhanced Data Rate)

S-ar putea fi mai multe tehnologii de comunicare, dar toate au un singur lucru in comun: repede înseamnă mai bine. Bluetooth SIG realizat acest lucru, şi a lucrat la îmbunătăţirea viteze de versiunea Bluetooth 1.2. Bluetooth versiunea 2.0 + EDR a fost anunţată de către Bluetooth SIG în iunie 2004 şi a început să apară în dispozitive Bluetooth la sfârşitul anului 2005.  
Bluetooth versiunea 2.0 + EDR oferă rate de transfer de date de până la trei ori mai rapid decat caietul de sarcini Bluetooth original. Bluetooth versiunea 2.0 + EDR oferă, de asemenea, îmbunătăţită cu mai multe conectivitate. Cu Bluetooth 2.0 + EDR, utilizatorii vor putea să mai eficient rula mai multe dispozitive Bluetooth în acelaşi timp. Ca rezultat, personală Bluetooth-Area Networks (PAN) sau Piconets vor deveni mai frecvente.  
De exemplu, utilizatorii vor avea posibilitatea de a sincroniza un computer activat pentru Bluetooth cu un PDA Bluetooth, şi în acelaşi timp, ei pot asculta muzică folosind o pereche de căşti fără fir Bluetooth.  
Computere şi dispozitive informatice au fost unele dintre primul dispozitivele să utilizeze Bluetooth 2.0 + EDR, în timp ce dispozitivele audio şi imagini sunt aşteptate să urmeze în scurt timp. Sony a anuntat ca va folosi Bluetooth 2.0 + EDR, în noua sa PlayStation 3. PlayStation 3 va folosi relatărilor-l pentru controlere wireless.  
Aici este o listă a principalelor accesorii / caracteristicile pe care le veţi găsi cu

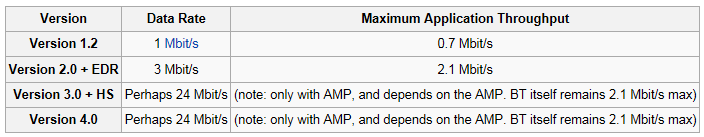
Bluetooth Specification versiunea 2.0 + EDR:

• compatibilitatea cu versiunile anterioare Bluetooth  
• De trei ori viteza de transmisie mai rapid (10 de ori, în unele cazuri)  
• Enhanced Data Rate de pana la 3 Mbps  
• Consum de curent mai mic din cauza cicluri de taxe reduse  
• Broadcast / multicast de sprijin  
• Simplificarea multi-legătură într-scenarii, datorită lăţimii de bandă disponibile mai multe  
• distribuită mass-media de control al accesului protocoale  
• îmbunătăţit în continuare Eroare Bit Rate de performanţă  
Versiune Bluetooth 2.1 + EDR (Enhanced Data Rate)  
Accesorii cu Bluetooth Versiune Core 2.1 + EDR includ:  
• Îmbunătăţirea Împerecherea  
• Enhanced Power Optimizare

Bluetooth versiunea 3.0 + HS (High Speed)

Dispozitivele de consum utilizând Bluetooth versiunea 3.0 + HS va profita de ratele mai mari de date utilizand radio 802.11 menţinând în acelaşi timp în continuare interfaţa Bluetooth clasic. Cu Versiunea 3.0, de mare viteza nu va mai necesita o architechure reţea stabilită.  
Există două caracteristici cheie care consumatorii vor beneficia de Bluetooth 3.0 + HS:  
• Unicast de date fără conexiune - reduce latenţa şi oferă mai rapid experienţe mai sigure  
• Enhanced Power Control - asigură abandonului mai puţin, o comună sumă utilizatori Bluetooth plângere  
Producătorii vor beneficia, de asemenea, de Versiune Bluetooth 3.0 + HS. Calitatea produselor Bluetooth companiilor "creşte, în timp, în acelaşi timp, reducerea costurilor de fabricaţie. Cu testarea acum standardizate şi automatizate, obtinerea de noi produse Bluetooth pe piaţă va fi mult mai simplu şi mai rapid.

Bluetooth Versiunea 4.0

Caietul de sarcini, caracteristici:  
  
• ultra-mici de vârf, mediu şi consumul de energie modul inactiv  
• abilitatea de a alerga de ani standard monedă celule de baterii  
• low cost  
• Multi-furnizor de interoperabilitate  
• gamă îmbunătăţită



Bluetooth stiva de protocoale

Articole principale: Bluetooth protocoale stivă şi Bluetooth  
". Bluetooth este definită ca o arhitectură de protocol de strat format din protocoale de bază, protocoale de înlocuire cablu, telefonie protocoale de control, şi protocoalelor adoptate" protocoale obligatorie pentru toate stive Bluetooth sunt: ​​LMP, L2CAP şi PSD. În plus, aceste protocoale sunt aproape universal acceptate: HCI şi RFCOMM.

LMP (Link Management Protocol)  
Utilizate pentru controlul asupra legăturii radio între două dispozitive. Pus în aplicare de pe controller.

L2CAP (Logical Link Control & protocol de adaptare a)  
Folosit pentru a multiplex mai multe conexiuni logice între două dispozitive folosind diferite protocoale de nivel superior. Oferă segmentarea şi reasamblarea de pe pachetele de aer.  
În modul de bază, L2CAP oferă pachete cu o sarcină utilă de până la 64KB configurabil, cu 672 octeţi ca MTU implicit, şi 48 de bytes ca minime obligatorii sprijinite MTU.  
În modurile de control Retransmission & Flow, L2CAP poate fi configurat pentru date fiabile sau izocrone pe canal prin efectuarea verificărilor şi retransmisia CRC.  
Addendum Bluetooth Core specificaţii 1 adaugă două moduri suplimentare L2CAP la caietul de sarcini de bază. Aceste moduri condamna în mod eficient Retransmission original şi moduri de control Flow:  
• Mod de retransmisie Enhanced (ERTM): Acest mod este o versiune îmbunătăţită a modului de retransmisie original. Acest mod oferă un canal L2CAP de încredere.  
• Mod Streaming (SM): Acesta este un mod foarte simplu, cu nici o retransmisie sau de control al fluxului. Acest mod oferă un canal de L2CAP nesigur.  
Fiabilitatea în oricare dintre aceste moduri este opţional şi / sau suplimentar garantat de cea mai mică stratul de Bluetooth BDR / EDR interfaţa aer prin configurarea numărul de retransmisii şi timeout culoare (de timp după care aparatul de radio va fi aruncat pachete). In-Pentru succesiunea este garantată de stratul inferior.  
Numai canale L2CAP configurate în ERTM sau SM pot fi operate peste link-uri logice AMP.

SDP (Service Discovery Protocol)  
Service Discovery Protocol (SDP), permite unui dispozitiv pentru a descoperi servicii suportate de către alte dispozitive, precum şi parametrii lor asociate. De exemplu, atunci când conectarea unui telefon mobil la un set cu cască Bluetooth, PSD va fi folosit pentru a determina ce profile Bluetooth sunt suportate de către setul cu cască (Headset Profile, Profil Hands Free, Advanced Audio Distribution Profile (A2DP), etc), precum şi setările protocolului multiplexorul necesare pentru conectarea la fiecare dintre ele. Fiecare serviciu este identificat printr-un identificatorul unic universal (UUID), cu serviciile oficiale (Profiluri Bluetooth) atribuie o formă UUID scurt (16 biţi, mai degrabă decât pe deplin 128) / vichitra

HCI (Host / Controller Interface)  
Standardizate de comunicare între stiva gazdă (de exemplu, un PC sau telefon mobil OS) şi controler (IC Bluetooth). Acest standard permite stiva de gazdă sau controller IC care urmează să fie schimbate cu adaptări minime.  
Există mai multe standarde de transport HCI strat, fiecare folosind o interfaţă hardware diferite pentru a transfera aceeaşi comandă, eveniment şi de pachete de date. Cele mai frecvent utilizate sunt USB (în PC-uri) şi UART (în telefoane mobile şi PDA-uri).  
În dispozitivele Bluetooth cu funcţionalitate simplă (de exemplu, căşti), stiva gazdă şi controller poate fi implementată pe microprocesor aceeaşi. În acest caz, HCI este facultativă, deşi de multe ori puse în aplicare ca o interfata software-ul intern.

RFCOMM (Emulare Serial Port)  
De frecvenţă radio de comunicaţii (RFCOMM) este un protocol de înlocuire cablu folosit pentru a crea un flux de date serial virtual. RFCOMM prevede pentru transportul de date binare şi emulează EIA-232 (anterior RS-232) semnale de control asupra stratului de banda Bluetooth.  
RFCOMM oferă o simplă fluxul de date fiabile pentru utilizator, similar cu TCP. Este folosit în mod direct de profile de telefonie multe legate ca un operator de transport pentru comenzi AT, precum şi fiind un strat de transport pentru OBEX prin Bluetooth.  
Multe aplicaţii Bluetooth utilizarea RFCOMM din cauza sprijinului său pe scară largă şi API la dispoziţia publicului pe majoritatea sistemelor de operare. În plus, aplicaţiile care utilizează un port serial de a comunica rapid poate fi portat de a utiliza RFCOMM.

BNEP (Bluetooth încapsulare protocol de reţea)  
BNEP este utilizat pentru transferul de date un alt stiva de protocoale lui printr-un canal L2CAP. Scopul său principal este transmiterea de pachete IP în profilul personal Networking Area. BNEP îndeplineşte o funcţie similară la SNAP în LAN fără fir.

AVCTP (Audio / Video Transport Control Protocol)  
Utilizat de către mai multe date de control de la distanţă pentru a transfera AV / C comenzi de peste un canal L2CAP. Butoanele de control de muzică pe un set de căşti stereo utiliza acest protocol pentru a controla music player-ul.

AVDTP (Audio / Video Distribution Protocolul privind transporturile)  
Utilizate de către Advanced Audio Distribution Profile pentru a transmite muzica la casti stereo de peste un canal L2CAP. Destinate a fi utilizate de către mai multe date de distribuţie video de transmisie Bluetooth.

Telephony control protocol  
De control de telefonie protocol binar (TCS BIN) este protocolul de bit-orientat care defineşte de control al apelurilor de semnalizare pentru stabilirea de apeluri de voce şi de date între dispozitivele Bluetooth. În plus, "TCS BIN defineşte procedurile de gestionare a mobilităţii pentru manipularea grupurilor de dispozitive Bluetooth TCS."  
TCS-BIN este utilizat doar de profilul de telefonie fără fir, care nu a reuşit să atragă implementatori. Ca atare, este doar de interes istoric.

Protocoalelor adoptate  
Protocoalelor adoptate sunt definite de alte standarde de luare a organizaţiilor şi a încorporat în stiva de protocoale Bluetooth, permiţând Bluetooth pentru a crea protocoalelor numai atunci când este necesar. Protocoalelor adoptate se numără:  
Point-to-Point Protocol (PPP)  
Internet protocol standard pentru transportul datagramelor IP printr-o legătură punct-la-punct.  
TCP / IP / UDP  
Fundaţia Protocoalele pentru protocolul TCP / IP suită

Obiect de schimb Protocolul (OBEX)  
Sesiunea-layer protocol pentru schimbul de obiecte, oferind un model de obiect şi reprezentare funcţionarea

Wireless Application Enviroment / Wireless Application Protocol (WAE / WAP)  
WAE specifică un cadru cerere pentru dispozitivele wireless si WAP este un standard deschis pentru a oferi utilizatorilor mobili acces la servicii de telefonie şi de informaţii.

De corectare a erorilor Baseband  
În funcţie de tipul de pachet, pachete individuale pot fi protejate de corecţie a erorilor, fie o treime de corectare a erorilor rata forward (FEC) sau cota de 2 / 3. În plus, pachetele cu CRC vor fi retransmise până la recunoscut de cerere se repetă automat (ARQ).

Configurarea conexiunilor  
Orice dispozitiv Bluetooth în modul de descoperire va transmite următoarele informaţii la cerere:  
• Dispozitiv de nume  
• Dispozitiv de clasă  
• Lista de servicii  
• informaţii tehnice (de exemplu: caracteristici ale dispozitivului, producator, caietul de sarcini Bluetooth utilizate, ceas offset)  
Orice dispozitiv poate efectua o anchetă pentru a găsi alte dispozitive să se conecteze la, şi orice dispozitiv poate fi configurat pentru a răspunde la asemenea întrebări. Cu toate acestea, în cazul în care aparatul încearcă să se conecteze stie adresa a dispozitivului, întotdeauna răspunde la solicitările de conectare directă şi transmite informaţiile afişate în lista de mai sus dacă este solicitat. Utilizarea serviciilor unui dispozitiv ar putea necesita asociere sau de acceptare de către proprietarul acestuia, dar conexiunea în sine poate fi iniţiată de orice dispozitiv şi a ţinut până când iese din raza de acţiune. Unele dispozitive pot fi conectate la un singur dispozitiv la un moment dat, şi conectarea la ele le împiedică să se conecteze la alte dispozitive şi care figurează în anchetele până când nu deconectaţi de la celălalt aparat.  
Fiecare dispozitiv are un număr unic de 48 de biţi adresa. Cu toate acestea, aceste adrese nu sunt, în general, prezentate în anchete. În schimb, numele prietenos Bluetooth sunt utilizate, care poate fi setat de utilizator. Acest nume apare atunci când scanează un alt utilizator pentru dispozitive şi în listele de dispozitive asociate.  
Cele mai multe telefoane au numele Bluetooth setat la producător şi de modelul de telefon în mod implicit. Cele mai multe telefoane mobile si laptop-uri arată doar numele Bluetooth şi programe speciale sunt necesare pentru a obţine informaţii suplimentare despre dispozitivele de la distanţă. Acest lucru poate fi confuz ca, de exemplu, ar putea exista mai multe telefoane în zona numită T610 (a se vedea Bluejacking).

Împerecherea

Motivaţie  
Multe din serviciile oferite prin Bluetooth poate expune date private sau să permită partidului de conectare pentru a controla dispozitivul Bluetooth. Din motive de securitate, este, prin urmare, necesar pentru a controla dispozitivele care li se permite să se conecteze la un dispozitiv Bluetooth dat. În acelaşi timp, este util pentru dispozitivele Bluetooth pentru a stabili automat o conexiune, fără intervenţia utilizatorului de îndată ce acestea sunt în gamă.  
Pentru a rezolva acest conflict, Bluetooth utilizează un proces numit împerechere. Două dispozitive trebuie să fie asociat la comunice unul cu celălalt. Procesul de împerechere este de obicei declanşează automat prima dată când un dispozitiv care primeşte o cerere de conexiune de la un dispozitiv cu care nu este încă asociat (în unele cazuri, ghidul de dispozitiv ar putea avea nevoie pentru a face legătură într dispozitivului Bluetooth vizibil pentru alte dispozitive prima). Odată ce o asociere a fost stabilită, este amintit de dispozitive, care se pot conecta apoi la fiecare, fără intervenţia utilizatorului. Atunci când dorit, relaţia de asociere pot fi ulterior înlăturate de către utilizator.

Punerea în aplicare  
În timpul procesului de împerechere, cele două aparate implicate se stabilească o relaţie, prin crearea unui secret partajat cunoscut ca o cheie de legătură. Dacă o cheie de legătură sunt stocate de către ambele dispozitive se spune să fie asociat sau lipite. Un dispozitiv care vrea să comunice doar cu un dispozitiv de lipit poate autentifica criptografice identitatea celuilalt aparat, şi astfel să fie sigur că este acelaşi dispozitiv este asociat anterior cu. Odată ce o cheie legătură într-a fost generată, o autentificată legătură ACL între dispozitivele pot fi criptate, astfel încât datele pe care le schimbă între ele pe calea undelor este protejat împotriva trage cu urechea.  
Tastele legătură într pot fi şterse în orice moment de către oricare dispozitiv. Dacă este făcută de către oricare dispozitiv aceasta va elimina implicit bonding dintre dispozitive, astfel încât este posibil ca unul dintre dispozitivele de a avea o cheie de legătură într-păstrate, dar nu trebuie să fie conştienţi de faptul că nu mai este legat de dispozitivul asociat cu tasta de link-ul dat.  
Servicii Bluetooth necesită, în general, fie de criptare sau autentificare, şi, ca o astfel de asociere înainte de a permite un dispozitiv la distanţă pentru a utiliza serviciul dat. Unele servicii, cum ar fi profilul Object Push, alege să nu ceară în mod explicit de autentificare sau de criptare, astfel încât asocierea nu interferează cu experienţă de utilizare asociate cu utilizarea serviciului de cazuri.

Mecanisme de împerechere  
Asocierea mecanisme s-au schimbat în mod semnificativ odată cu introducerea Secure Simple Pairing în Bluetooth v2.1. Au rezumă mecanismele de împerechere:

Asociere Legacy: Aceasta este singura metodă disponibilă în Bluetooth v2.0 şi înainte. Fiecare dispozitiv trebuie să introduceţi un cod PIN, asocierea este o reuşită numai dacă ambele dispozitive introduceţi acelaşi cod PIN. Orice 16-byte UTF-8 şir poate fi folosit ca un cod PIN, însă nu toate dispozitivele pot fi aptă de a intra toate codurile posibile PIN.

Limited dispozitivele de intrare: exemplu evident al acestei clase de dispozitiv este un Bluetooth hands-free setul cu cască, care au, în general, puţine intrări. Aceste dispozitive au de obicei un cod PIN fix, de exemplu "0000" sau "1234", care sunt hard-coded în dispozitiv.

Numerice dispozitivele de intrare: Telefoanele mobile sunt exemple clasice ale acestor dispozitive. Acestea permit unui utilizator să introduceţi o valoare numerică până la 16 cifre în lungime.

Alfa-numeric dispozitivele de intrare: PC-uri şi smartphone-uri sunt exemple de aceste dispozitive. Acestea permit unui utilizator să introduceţi complet UTF-8 textul după cum un cod PIN. Dacă asocierea cu un dispozitiv mai puţin capabil să ghidul trebuie să fie conştient de limitările de intrare pe alt dispozitiv, nu există nici un mecanism disponibil pentru un dispozitiv capabil să determine modul în care aceasta ar trebui să limiteze intrare disponibile unui utilizator poate folosi.

Împerecherea Secure simplă (SSP): Acest lucru este necesar prin Bluetooth v2.1. Un dispozitiv Bluetooth v2.1 pot utiliza numai asocierea moştenire pentru a interopera cu un dispozitiv v2.0 sau mai devreme. Asocierea Secure simplă foloseste o forma de criptografia cu chei publice, şi are următoarele moduri de funcţionare:

Doar o fabrică: dupa cum implica numele, această metodă pur şi simplu funcţionează. Nr ghidul de interacţiune este necesară, totuşi, un dispozitiv poate solicita utilizatorului pentru a confirma procesul de împerechere. Această metodă este de obicei folosit de căşti cu capacităţi foarte limitate IO, şi este mai sigură decât mecanismul de PIN-ul fix, care este de obicei folosit pentru a asocia mai vechi de acest set de dispozitive limitat. Această metodă oferă nici un om nu la mijloc (MITM) de protecţie.

Comparaţie numerică: Dacă ambele aparate au un ecran şi cel puţin se poate accepta un binar Da / Nu introduse de utilizator, acestea pot utiliza de comparare numerica. Această metodă se afişează un cod de 6 cifre numeric pe fiecare dispozitiv. Utilizatorul ar trebui să compare numere pentru a se asigura că acestea sunt identice. În cazul în care comparaţia reuşeşte, utilizator (i) ar trebui să confirme asocierea de pe dispozitiv (e), care poate accepta o intrare. Această metodă oferă protecţie MITM, presupunând ghidul confirmă pe ambele dispozitive şi realizează efectiv compararea în mod corespunzător.

Passkey de intrare: Această metodă poate fi utilizată între un dispozitiv cu un afişaj şi un dispozitiv de intrare cu tastatura numerică (cum ar fi o tastatură), sau două dispozitive cu intrare tastatura numerică. În primul caz, display-ul este folosit pentru a afişa un cod de 6 cifre numerice pentru utilizator, care introduce apoi codul de pe tastatură. În al doilea caz, utilizatorul de fiecare dispozitiv introduce acelaşi număr de 6 cifre. Ambele cazuri oferă protecţie MITM.

Out of band (OOB): Această metodă foloseşte un mijloc de comunicare externă, cum ar fi Near Field Communication (NFC) să facă schimb de unele informaţii utilizate în procesul de împerechere. Împerecherea este completat prin radio Bluetooth, dar solicită informaţii de la mecanismul de OOB. Acest lucru oferă doar nivelul de protecţie MITM care este prezent în mecanismul OOB.  
SSP este considerat simplu, din următoarele motive:  
• În majoritatea cazurilor, aceasta nu are nevoie de un utilizator pentru a genera o cheie de acces.  
• Pentru a putea folosi-cazurile care nu necesită o protecţie MITM, ghidul de interacţiune a fost eliminată.  
• Pentru comparaţie numerice, MITM de protecţie poate fi realizat cu o comparaţie simplă egalitate de către utilizator.  
• Utilizarea OOB cu NFC va permite asocierea dispozitive când se închide pur şi simplu, mai degrabă decât necesită un proces de descoperire de lungă durată

.  
Ceea ce priveşte securitatea

Înainte de Bluetooth v2.1, criptarea nu este necesară şi poate fi oprit în orice moment. În plus, cheia de criptare este numai bun pentru aproximativ 23.5 oră, folosind o cheie de criptare singur mai mult timp decât acesta permite atacuri simplu XOR pentru a prelua cheia de criptare.

• Dezactivarea de criptare este necesara pentru mai multe operaţiuni normale, aşa că este problematic pentru a detecta dacă criptarea este dezactivată pentru un motiv valabil sau pentru un atac de securitate.

• Bluetooth v2.1 adrese de acest lucru în următoarele moduri:

o criptare este necesar pentru toate non-SDP (Service Discovery Protocol) conexiunile

o O Pauză de criptare nou şi Reluare funcţie este utilizată pentru toate operaţiunile normale de criptare care necesită să fie dezactivate. Acest lucru permite identificarea cu uşurinţă de funcţionare normală de la atacuri de securitate.  
 o Cheie de criptare este necesar să fie actualizate înainte de a expira.  
Tastele legătură într-pot fi stocate pe sistemul de fişiere dispozitiv, nu pe chip Bluetooth în sine. Mulţi producători de cip Bluetooth permite tastele legătură într-fi stocate pe dispozitiv, cu toate acestea, în cazul în care dispozitivul este amovibil acest lucru înseamnă că tasta de legătură se va muta cu aparatul.

Air interface  
Protocol funcţionează în licenţă-free banda ISM la 2.402-2.480 GHz [44]. Pentru a evita interferenţele cu alte protocoale care folosesc banda de 2,45 GHz, protocolul Bluetooth imparte banda de la 79 de canale (fiecare 1 MHz lăţime) şi schimbă canalele de până la 1600 de ori pe secundă. Implementari cu versiunile 1.1 şi 1.2 viteze ajunge de 723.1 kbit / s. Versiunea 2.0 implementări Bluetooth caracteristica Enhanced Data Rate (EDR) si ajunge la 2.1 Mbit / s. Punct de vedere tehnic, versiunea 2.0 dispozitive au un consum de putere mai mare, dar de trei ori mai rapid reduce timpul de transport, reducând consumul de energie în mod eficient la jumătate din dispozitive 1.x (presupunând că sarcina de trafic egal).

Securitate

Prezentare generală  
Bluetooth pune în aplicare de confidenţialitate, autentificare şi derivare cheie cu algoritmi personalizate bazate pe cifru SIGURE bloc +. Bluetooth generaţie cheie este, în general, bazat pe un cod PIN Bluetooth, care trebuie să fie introdusă în ambele dispozitive. Această procedură ar putea fi modificate în cazul în care unul dintre dispozitivele are un cod PIN fix (de exemplu, pentru căşti sau dispozitive similare, cu o interfaţă de utilizator restricţionat). In timpul asociere, o cheie de initializare sau o cheie master este generată, folosind algoritmul de E22. E0 cifru flux este utilizat pentru criptarea pachetelor, acordarea de confidenţialitate şi se bazează pe un secret criptografic comun, şi anume o cheie legătură într generate anterior sau tasta de master . Aceste chei, folosite pentru criptarea ulterioară a datelor transmise prin intermediul interfetei de aer, se bazează pe codul PIN Bluetooth, care a fost introdusă în una sau ambele dispozitive.

O prezentare generală a Bluetooth exploateaza vulnerabilitati a fost publicat în 2007 de către Andreas Becker.

În septembrie 2008, Institutul Naţional de Standarde şi Tehnologie (NIST) a publicat un Ghid de securitate Bluetooth, care va servi ca referinţă pentru organizaţii cu privire la capacităţile de securitate de Bluetooth şi măsurile pentru asigurarea în mod eficient tehnologiile Bluetooth. În timp ce Bluetooth are beneficiile sale, acesta este susceptibil de a respingerea atacurilor asupra serviciului, interceptarea, man-in-the-middle atacuri, modificarea mesaj, şi deturnarea de resurse. Utilizatorii / organizaţiile trebuie să evalueze nivelul lor de risc acceptabil şi includerea de securitate în ciclul de viaţă al dispozitivelor Bluetooth. Pentru a contribui la atenuarea riscurilor, incluse în document NIST sunt liste de verificare de securitate cu orientări şi recomandări pentru crearea şi menţinerea piconets sigure Bluetooth, casti, iar cititorii smart card.

V2.1 Bluetooth - finalizat în 2007, cu dispozitive de consum apărând pentru prima oară în 2009 - face schimbări semnificative la adresa securităţii Bluetooth, inclusiv de asociere. A se vedea secţiunea # Împerecherea mecanisme pentru mai multe detalii despre aceste modificări Bluejacking

Articol principal: Bluejacking  
Bluejacking este trimiterea fie o imagine sau un mesaj de la un utilizator la un utilizator neavizat prin intermediul tehnologiei fără fir Bluetooth. Aplicaţii comune includ mesaje scurte (de exemplu, "Ai fost doar bluejacked!"). [48] ​​Bluejacking nu implică eliminarea sau modificarea oricăror date de la dispozitiv. Bluejacking poate implica, de asemenea, luarea de control al unui mobil fără fir şi telefonând la o linie cu tarif special, deţinută de bluejacker.  
Istorie de problemele de securitate

Timpuriu

În 2001, Jakobsson şi Wetzel de la Bell Laboratories a descoperit deficienţe în protocolul Bluetooth de asociere şi, de asemenea, a subliniat vulnerabilităţi în sistemul de criptare În anul 2003., Ben şi Adam Laurie de la AL Digital Ltd. a descoperit că deficienţele serioase în unele implementări slabă a Bluetooth de securitate poate duce la divulgarea datelor cu caracter personal Într-un experiment ulterior., Martin Herfurt din trifinite.group a fost în măsură să facă un câmp de judecată la târguri CeBIT, care arată importanţa problemei către lume. Un nou atac numit BlueBug a fost folosit pentru acest experiment. În 2004, primul virus pretinse prin Bluetooth pentru a se răspândi printre telefoanele mobile a apărut pe sistemul de operare Symbian. Virusul a fost descris pentru prima data de Kaspersky Lab şi solicită utilizatorilor să confirme instalarea software-ului înainte de necunoscut se poate propaga. Virusul a fost scris ca o dovada-of-concept de către un grup de scriitori virus cunoscut sub numele de "29A" şi trimis la grupurile anti-virus. Astfel, ar trebui să fie privită ca o potenţială ameninţare de securitate (dar nu real) la tehnologia Bluetooth sau sistemul de operare Symbian, deoarece virusul nu sa raspandit in afara acestui sistem. În august 2004, un experiment record mondial de stabilire (a se vedea, de asemenea, sniping Bluetooth) a arătat că gama de aparate de radio Bluetooth clasa 2 ar putea fi extins la 1.78 km (1.08 mile), cu antene direcţionale şi amplificatoare de semnal [53]. Aceasta reprezintă un potenţial ameninţare la adresa securităţii, pentru că permite atacatorilor să acceseze dispozitive de vulnerabile Bluetooth de la o distanta dincolo de aşteptări. Atacatorul trebuie să fie, de asemenea, posibilitatea de a primi informaţii de la victimă pentru a configura o conexiune. Nr atac poate fi făcută împotriva unui dispozitiv Bluetooth excepţia cazului în care atacatorul stie adresa Bluetooth şi ce canale pentru a transmite mai departe.

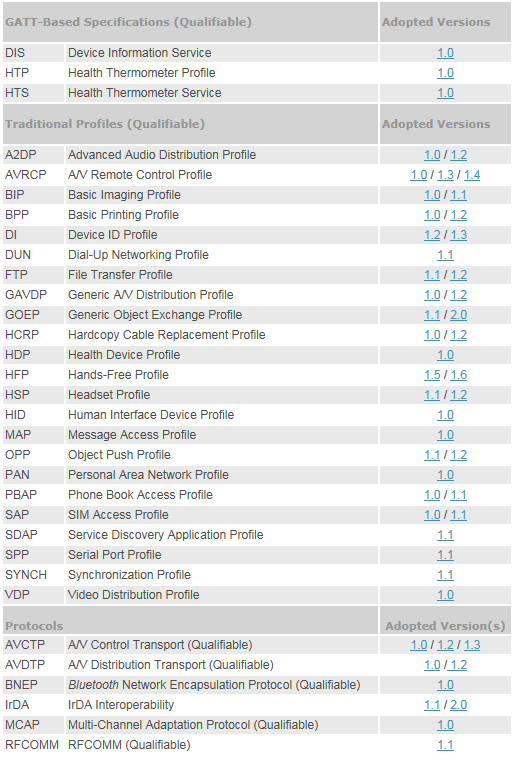
2005  
În ianuarie 2005, un vierme de malware mobil cunoscut sub numele de Lasco.A a început direcţionarea telefoanele mobile folosind sistemul de operare Symbian (platforma Series 60), utilizarea dispozitivelor Bluetooth activat pentru a se multiplica şi răspândi la alte dispozitive. Viermele este auto-instalare şi începe odată ghidul de mobil aprobă transferul de fişiere (velasco.sis) de la un alt dispozitiv. Odată instalat, viermele incepe caută alte dispozitive Bluetooth activat pentru a infecta. În plus, viermele infecteaza alte fişiere SIS pe aparat., Permiţând replicarea la un alt aparat, prin utilizarea de mass-media amovibil (Secure Digital, Compact Flash, etc). Viermele poate face dispozitivul mobil instabilă.

În aprilie 2005, Universitatea din Cambridge cercetatorii in securitate a publicat rezultatele punerii lor în aplicare efectivă a atacurilor pasive împotriva asocierea PIN-ul pe bază de între dispozitivele Bluetooth comerciale, confirmând atacurile care urmează să fie practic rapid si Bluetooth simetrice stabilirea metodă-cheie care urmează să fie vulnerabil. Pentru a remedia această vulnerabilitate, care au realizat-o punere în aplicare care a arătat că mai puternică, unitate asimetrice cheie este fezabil pentru anumite categorii de dispozitive, cum ar fi telefoanele mobile.

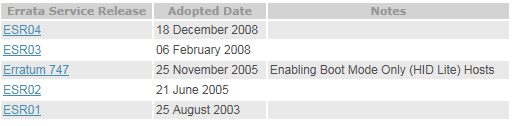
În iunie 2005, Yaniv Shaked şi lână Avishai a publicat un document care descrie ambele metode active şi pasive pentru obţinerea PIN-ul pentru o legătură Bluetooth. Atacul pasiv permite unui atacator echipate corespunzător pentru a trage cu urechea în domeniul comunicaţiilor şi parodie, în cazul în care atacatorul a fost prezent la momentul de asociere iniţial. Metode active face uz de un mesaj special construit, care trebuie să fie introduse într-un anumit punct din protocol, pentru a face master şi slave repetaţi procesul de împerechere. După aceea, prima metodă poate fi folosită pentru a sparge codul PIN. Slăbiciune Acest atac lui majoră este că are nevoie de ghidul de dispozitive sub atac pentru a re-introduceţi codul PIN în timpul atacului în cazul în care dispozitivul îi determină să. De asemenea, acest atac activă necesită, probabil, hardware-ul personalizat, deoarece cele mai multe dispozitive Bluetooth disponibile pe piaţă nu sunt capabile de sincronizare necesare.

În august 2005, poliţia din Cambridgeshire, Anglia, a emis avertismente despre hoţii care folosesc telefoane cu tehnologie Bluetooth pentru a urmări alte dispozitive din stânga în maşini. Poliţia informarea utilizatorilor să se asigure că orice conexiuni mobile de networking sunt de-activat în cazul în care laptop-uri şi alte dispozitive sunt lăsate în acest fel.

2006  
În aprilie 2006, cercetatorii de la reţea şi Secure F-Secure a publicat un raport care avertizează de numărul mare de dispozitive lăsat într-o stare vizibilă, şi a emis statisticile cu privire la răspândirea diferitelor servicii de Bluetooth şi uşurinţa de răspândirea unui vierme Bluetooth eventuală.

2007  
În octombrie 2007, la Conferinţa de Securitate Hack.lu Luxemburgheză, Kevin Finistere şi Thierry Zoller a demonstrat şi a lansat un shell root la distanţă prin Bluetooth pe Mac OS X v10.4 şi v10.3.9. Ei au demonstrat, de asemenea, codul PIN luetooth prima şi cracare Linkkeys, care se bazează pe cercetare de lână şi Shaked.

Adopted Bluetooth Errata Service Releases



Channel Manager

Manager de canal este responsabilă pentru crearea, gestionarea şi închidere  
L2CAP canale pentru transportul de protocoale de service şi datele aplicaţiei  
fluxuri. Manager de canal utilizează protocolul L2CAP a interacţiona cu un  
manager de canal pe o distanţă (peer), dispozitiv pentru a crea aceste canale L2CAP şi conectaţi obiective lor la entităţile corespunzătoare. Manager de canal  
interacţionează cu managerul său legătură într-un local sau PAL AMP de a crea legături noi logice (Dacă este necesar) şi pentru a configura aceste link-uri pentru a oferi calitatea necesară de serviciu pentru tipul de date de a fi transportată.

L2CAP Resource Manager

Blocul L2CAP manager de resurse este responsabil pentru gestionarea comanda  
de depunere de fragmente PDU la baseband şi unele programarea relativă  
între canale pentru a se asigura că canale L2CAP cu angajamentele QoS sunt  
nu refuzat accesul la canalul fizic datorită epuizării resurselor Controller.  
Acest lucru este necesar din cauza modelului arhitectural nu îşi asumă faptul că un  
Controller-a buffering nelimitate, sau că HCI este o conductă de lăţime de bandă infinit.  
L2CAP manageri de resurse pot efectua, de asemenea, în conformitate trafic de poliţie pentru a  
a se asigura că cererile sunt depunerea SDUs L2CAP în limitele lor de  
negociabil setările QoS. Modelul general Bluetooth Detalii de transport îşi asumă  
bine-au comportat aplicaţii, şi nu defineşte modul în care o punere în aplicare este  
de aşteptat să se ocupe de această problemă.

Security Manager protocol  
Security Manager Protocol (SMP) este protocolul peer-to-peer utilizată pentru a genera  
chei de criptare şi cheile de identitate. Protocol opereaza peste un dedicat  
imobilizate L2CAP canal. Blocul SMP gestionează, de asemenea, de depozitare a  
chei de criptare şi cheile de identitate şi este responsabil pentru generarea aleatoare  
adrese şi rezolvarea adrese aleatoare cu identităţile dispozitiv cunoscut.  
SMP bloc interfeţe direct cu operatorul de a oferi cheile stocate utilizate pentru  
criptare şi autentificare în timpul procedurilor de criptare sau de asociere.  
Acest bloc este folosit doar în sistemele de LE. Funcţionalităţi similare în sistemul BR / EDR  
este conţinută în blocul Link Manager în Controller. Funcţionalitate SMP este în gazdă, pe sisteme LE pentru a reduce costurile punerii în aplicare a LE numai  
controlori.

Caracteristica protocol  
Protocolul atribut (ATT), bloc pune în aplicare protocolul peer-to-peer  
între un server şi un client atribut atribut. Clientul ATT comunică  
cu un server de ATT pe un dispozitiv la distanţă printr-o L2CAP fix dedicat  
canal. Clientul ATT trimite comenzi, cereri, si confirmari la  
ATT server. Serverul de ATT trimite răspunsurile, notificările şi indicaţiile pentru  
client. Aceste comenzi ATT client şi solicită oferi un mijloc pentru a citi  
şi a scrie valori de atribute pe un dispozitiv de la egal la egal cu un server de ATT.

AMP Manager protocol  
Managerul AMP este un strat care utilizează L2CAP să comunice cu un egal  
Manager AMP pe un dispozitiv la distanţă. De asemenea, în mod direct interfeţe cu PAL AMP  
AMP pentru scopuri de control. Managerul AMP este responsabil pentru a descoperi  
AMP de la distanţă (e) şi determinarea disponibilitatea acestora. Se colectează de asemenea informaţii  
AMP despre distanţă (e). Această informaţie este utilizată pentru a configura şi gestiona AMP  
link-uri fizice. Managerul AMP foloseste un canal dedicat de semnalizare L2CAP  
de a comunica cu managerul de la distanţă AMP (e).

Generic atribut profil  
Generic Profil atribut (GATT), bloc reprezintă funcţionalitatea  
server atribut şi, opţional, clientul atributul. Profilul descrie  
ierarhie de servicii, caracteristicile şi atributele utilizate în serverul de atribut.  
Bloc oferă interfeţe pentru a descoperi, cititul, scrisul şi indicând de  
caracteristicile serviciilor şi atributele. GATT este utilizat pe dispozitive LE LE pentru mai multe date serviciu de căutare.

Generic Access Profile  
Profil de acces generic (GAP) bloc reprezintă funcţia de bază comune  
pentru toate dispozitivele Bluetooth, cum ar fi modurile de transport şi procedurile de acces utilizate de către transporturi, protocoalele şi profilurile de aplicaţii. Servicii de GAP includ dispozitiv  
descoperire, moduri de conectare, de securitate, autentificare, modele de asociere şi de serviciu de căutare.

BR / EDR / LE Controller Blocuri de arhitectură  
În cazul în care implementari BR / EDR şi sistemele LE sunt combinate,  
blocuri arhitecturale pot fi partajate între sisteme sau fiecare sistem poate  
au propriile lor instanţiere a blocului.

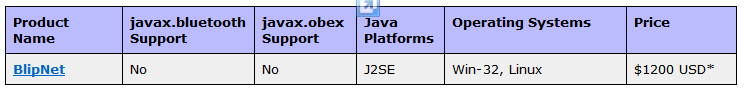
Device Manager  
Device Manager este blocul funcţional în baseband care controlează  
comportamentul general al dispozitivului Bluetooth. Acesta este responsabil pentru toate operaţiunile de  
sistemul Bluetooth, care nu sunt direct legate de transport date, cum ar fi  
întrebător pentru prezenţa de dispozitive Bluetooth din apropiere, conectarea la Bluetooth dispozitive, sau de a face dispozitivul Bluetooth locale descoperit sau conectabile prin alte dispozitive.  
Cereri de Manager dispozitive de acces la mediul de transport de la baseband  
controlor de resurse, în scopul de a îndeplini funcţiile sale.  
Device Manager controlează, de asemenea, comportamentul dispozitivului local implicat de un număr de comenzi HCI, cum ar fi gestionarea Numele dispozitivului local, orice legătură într-stocate chei, şi alte funcţionalităţi.

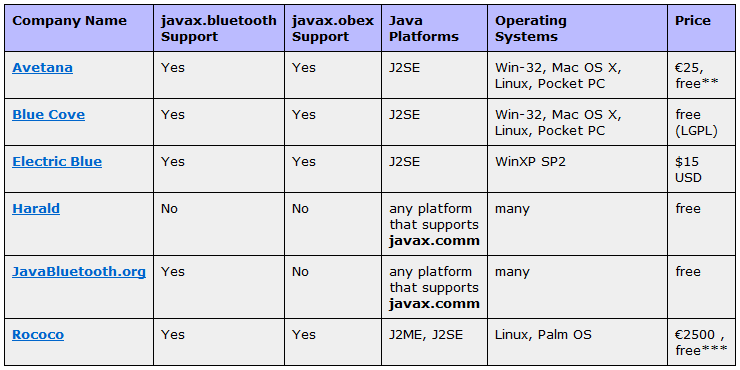
Link Manager  
Managerul legătură într-este responsabil pentru crearea, modificarea şi eliberarea de  
link-uri logice (şi, dacă este necesar, transporturi asociate lor logică), precum şi  
actualizare a parametrilor referitoare la legăturile fizice între dispozitive. Legătură într-manager realizeaza acest lucru prin comunicarea cu managerul link-ul din Bluetooth de la distanţă folosind dispozitive de gestionare Link Protocol (LMP) în BR / EDR şi Legătură într-Layer Protocol (LL), în LE. LM sau protocol LL permite crearea de noi legături logice şi de transporturi de logică între dispozitive atunci când este necesar, precum şi controlul general al legătură într-şi de transport atribute, cum ar fi oferirea posibilităţii de criptare privind transportul logic, de adaptare de puterea de emisie în BR / EDR pe link-ul de fizică, sau de ajustare setări de QoS în BR / EDR pentru o legătură logică.

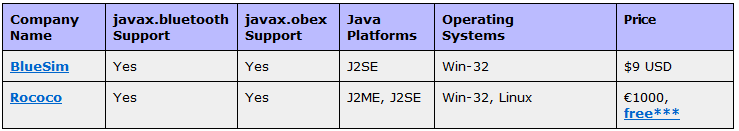
Baseband Resource Manager  
Manager de resurse baseband este responsabil pentru toate căile de acces la radio  
mediu. Acesta are două funcţii principale. În centrul său este un programator care acordă timp pe canalele de fizică la toate entităţile care au negociat un acces  
contract. Alte funcţii principal este de a negocia contractele de acces cu aceste  
entităţi. Un contract de acces este în mod eficient un angajament pentru a furniza o anumită QoS care este necesară pentru a oferi o cerere de utilizator cu o aşteaptă  
performanţă.  
Contractul de acces şi funcţia de planificare trebuie să ţină cont de orice comportament care necesită utilizarea de controllerul primar. Aceasta include (de exemplu)normal de schimb de date între dispozitivele conectate prin link-uri logice, şi  
transporturi logică, precum şi utilizarea de mediu radio pentru a efectua anchete,  
face conexiuni, să fie detectate sau conectabil, sau de a lua citirile de la  
transportatorii neutilizate în timpul utilizării a frecvenţei de adaptare salt de modul.  
În unele cazuri, în BR / EDR sisteme de programarea unei rezultate legătură logică în schimbarea unei legătură într-o logică canal fizic diferit de cel care a fost utilizat anterior. Acest lucru poate fi (de exemplu), ca urmare a implicării în scatternet, o  
funcţia de anchetă periodice, sau scanarea pagina. În cazul în care canalele fizice sunt nu slot de timp aliniat, apoi manager de resurse, de asemenea, conturile pentru realinierea de timp între sloturile de pe canal fizic original şi sloturile de pe noul  
fizice canal. În unele cazuri, sloturile va fi în mod natural aliniat ca urmare a  
ceas acelaşi aparat să fie folosit ca o referinţă pentru ambele canale fizice.

Link Controller  
Regulatorul legătură într-este responsabil pentru codare şi decodare a Bluetooth  
pachetele din sarcina utilă de date şi parametri referitoare la canalul fizic,  
de transport şi de logică legătură într-logică.

Controlerul legătură într-efectuează controlul în protocolul de semnalizare legătură într-BR / EDR şi  
legătură într-protocol de strat in LE (în strânsă legătură cu funcţia de programare a  
manager de resurse), care este folosit pentru a comunica de control al fluxului şi confirmarea şi să solicite retransmitere semnale. Interpretarea acestor semnale  
este o caracteristică de transport logic asociate cu banda  
de pachete. Interpretarea şi controlul de semnalizare de control este în mod normal legătură într-asociat cu scheduler manager de resurse lui.

PHY  
Blocul PHY este responsabil pentru transmiterea şi primirea de pachete de informare  
pe canalul fizic. O cale de control între banda şi  
PHY bloc permite bloc baseband pentru a controla calendarul şi frecvenţa purtătoare  
blocului PHY. Blocul PHY transformă un flux de date către şi de la  
canal fizic şi baseband în formate necesare.  


Software-ul Kituri Numai Dezvoltare - kituri Software Numai sunt pentru dezvoltatorii de intermediar, care deja au achiziţionat hardware Bluetooth, şi au nevoie de un kit Bluetooth Java de dezvoltare, care este compatibil cu hardware-ul lor.

Kituri de dezvoltare Simulare - kituri de dezvoltare de simulare sunt (de obicei), nu este compatibil cu hardware-ul Bluetooth reale, şi doar simula interacţiunea dintre dispozitivele Bluetooth într-un JVM

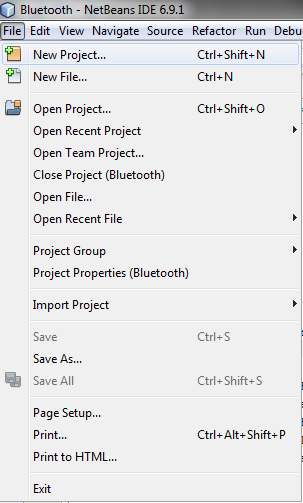
SDK

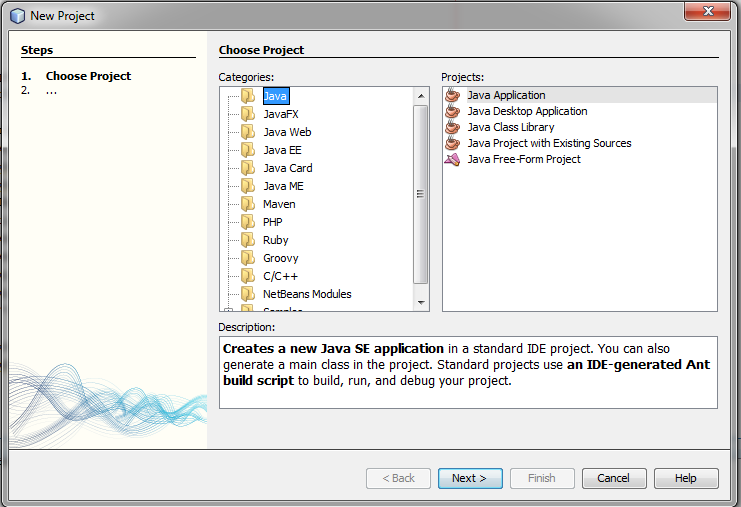
Java 2 Platform, Micro Edition (J2ME).  
Java ME Platform SDK este un set de instrumente de stat-of-the-art pentru dezvoltarea de aplicatii mobile. Acesta prevede emularea de dispozitive, un mediu de dezvoltare de sine stătătoare, şi un set de utilitare pentru dezvoltarea rapidă a aplicaţiilor Java ME.  
  
Pe Windows, Java ME SDK 3.0 este succesorul popularului Java Wireless Toolkit 2.5.2 şi Java 1.0 Toolkit pentru CDC. Se integrează CLDC, CDC şi Blu-ray Disc Java (BD-J), tehnologie într-un singur SDK.  
  
Java ME SDK 3.0 este acum disponibil pentru Windows XP şi Vista 32-bit, precum şi pentru Mac OS. Mac OS presă al aduce sprijinul pentru dezvoltare mobile CLDC pentru utilizatorii de Mac, pentru prima dată.  
  
Android SDK  
  
Android Software Development Kit (SDK), versiunea 1.0 a fost lansat pe 24 septembrie 2008. Aceasta este prima versiune stabilă a platformei Android şi ar trebui să permită dezvoltatorilor să îşi pregătească cererile pentru telefoane disponibile în comerţ. Android SDK este disponibil pentru Windows, Mac OS X, Linux şi şi include instrumente, precum şi un emulator Android pentru a rula aplicaţii.

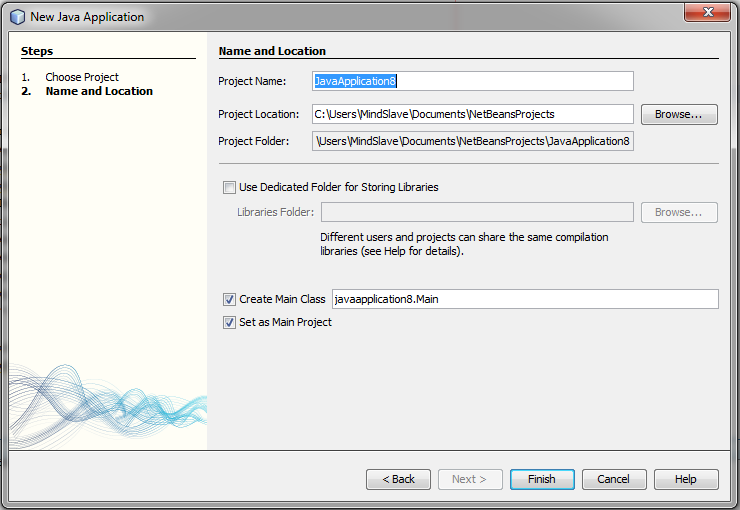
BlueCove  
BlueCove este o bibliotecă de Java pentru Bluetooth (JSR-82 punere în aplicare), care în prezent interfeţe cu Mac OS X, WIDCOMM, BlueSoleil Bluetooth şi stiva Microsoft incluse în Windows XP SP2 sau Windows Vista şi WIDCOMM Bluetooth şi Microsoft stivă pe Windows Mobile.  
BlueCove-GPL este modul suplimentar GPL autorizate pentru a sprijini runtime BlueCove pe Linux BlueZ.  
BlueCove JSR-82 modul Emulator este modul suplimentar pentru BlueCove pentru a simula stivă Bluetooth.  
BlueCove pot fi utilizate în Java Standard Edition (J2SE) 1.1 sau mai nou.

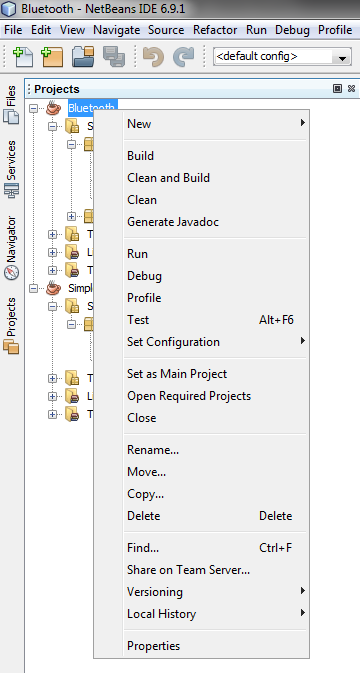
IDE

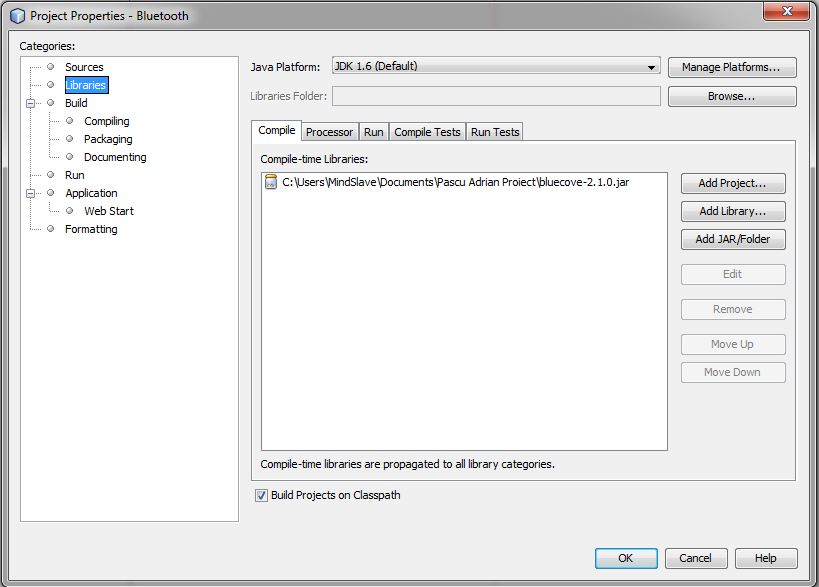
Netbeans







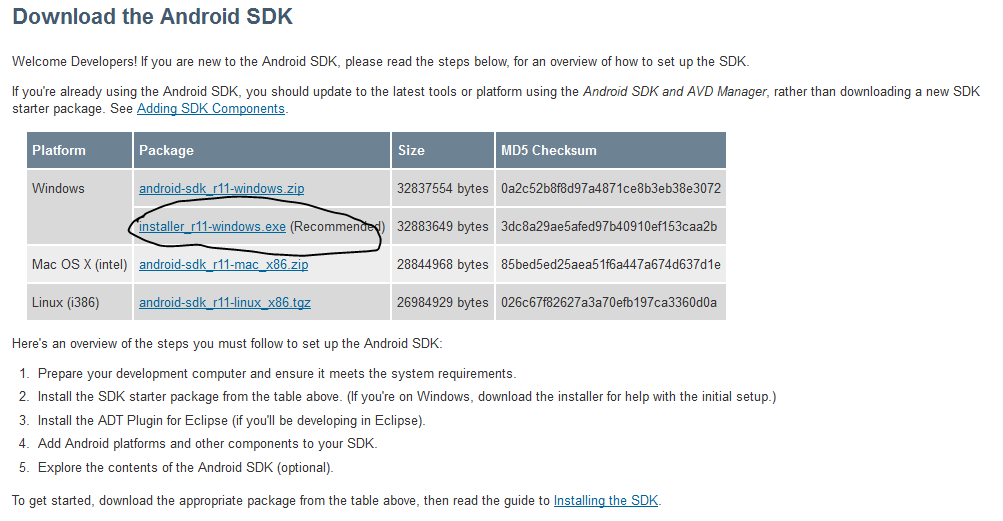




Eclipse

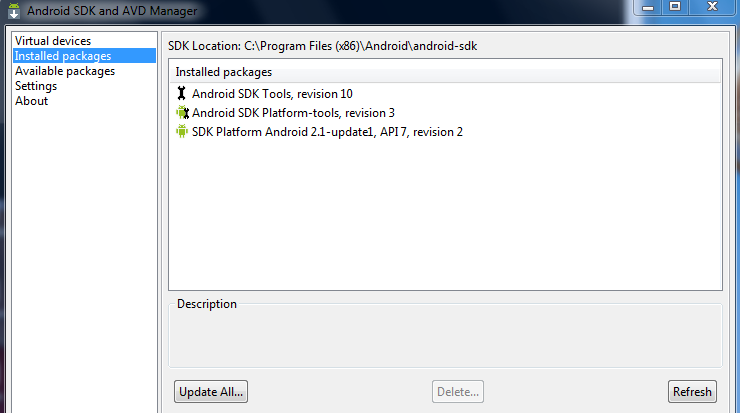
## Instalare SDK Android:

1.Se intra pe pagina: <http://developer.android.com/sdk/index.html>



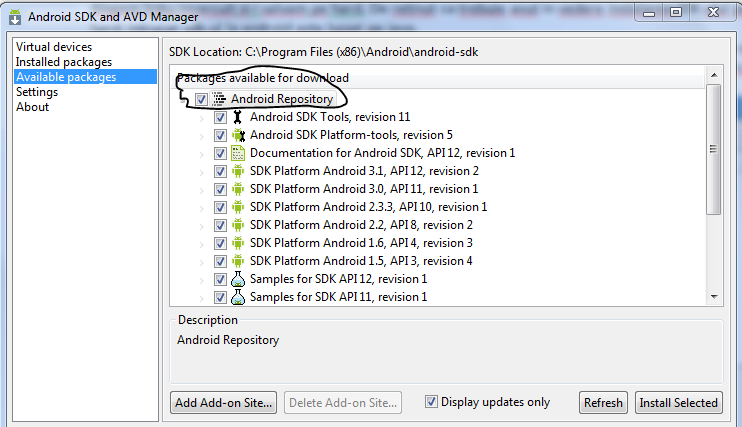
1. Alegem link-ul incercuit si il salvam pe hard. De retinut ca trebuie avut in vedere instalarea JDK-ului pe hard, intrucat sdk-ul la android este bazat pe java.

2. Intram in SDK manager si instalam pachetele corespunzatoare dezvoltarii. Trebuie retinut ca este indicat sa se downloadeze versiunea minima de sdk care va fi ulterior suportata de aplicatie. O aplicatie facuta in android 1.6 va fi rulata de un terminal cu android 2.1, de exemplu.



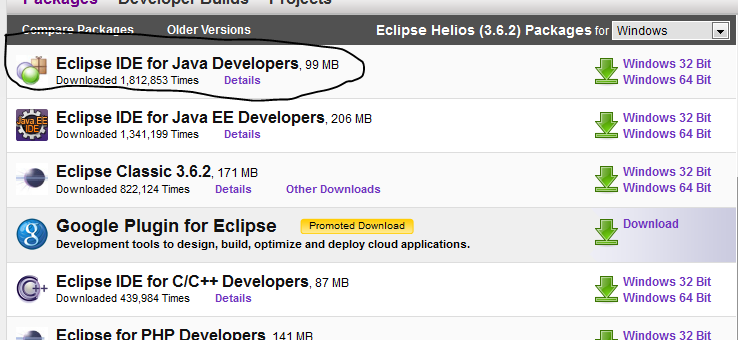
Pachetele instalate

Se alege apoi Available packages, respective Android repository si se selecteaza SDK-ul ce va fi downloadat si cu sampleurile respective.

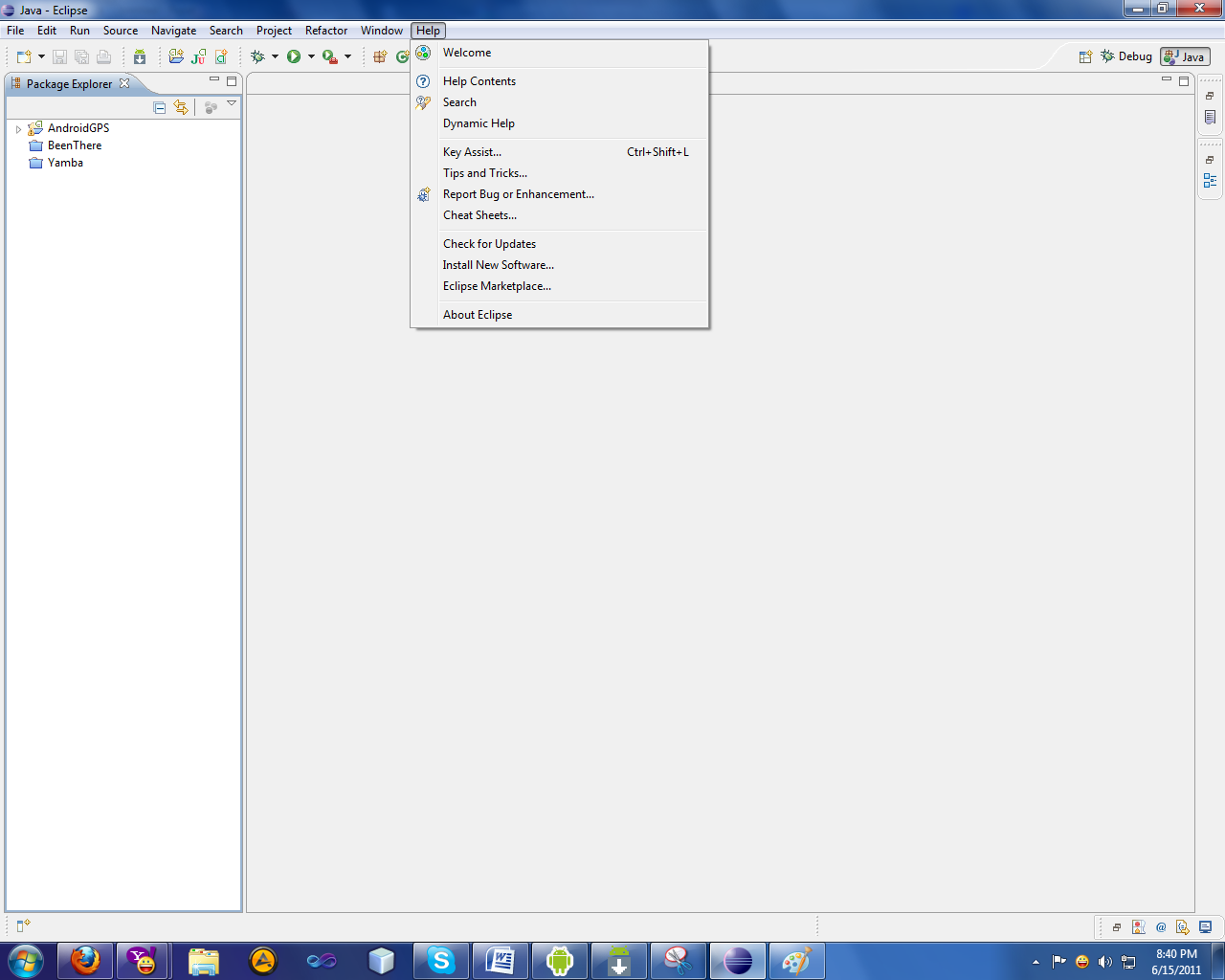


Apoi selectam install selected.

3. Odata instalat sdk-ul Android, putem crea aplicatii ce pot fi rulate de emulatorul din SDK. Totusi deoarece aceasta varianta este mai complicata si mai costisitoare, vom alege folosirea unei IDE (Integrated Development Environment), in cazul de fata IDE-ul recomandat de producatorul Androidu-lui, Google, este recomandat ca fiind Eclipse, pentru el existand un plugin official, care simplifica foarte mult dezvoltarea de aplicatii pe terminale mobile. Astfel vom incepe prin a downloada eclipse de la adresa: <http://www.eclipse.org/downloads/>

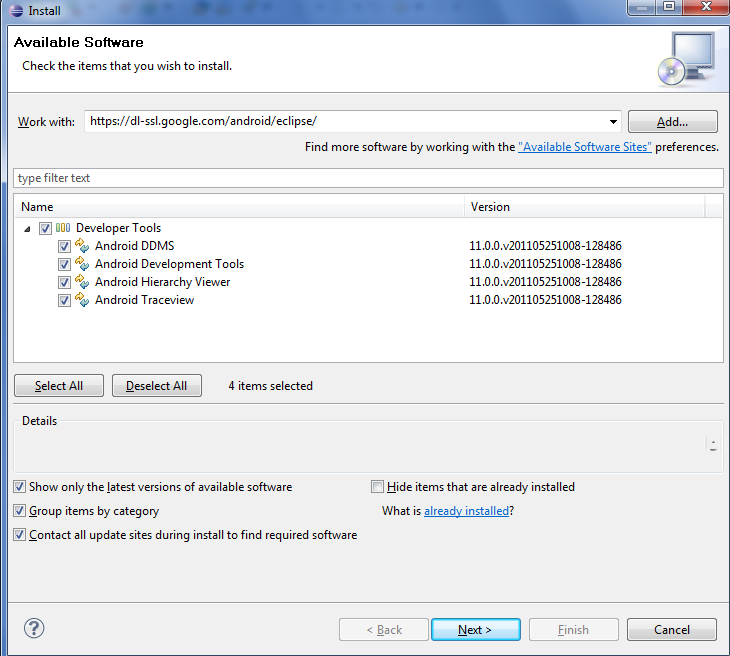
 Si vom downloada eclipse versiunea de 32 biti.

4. Se dezarhiveaza arhiva downloadata ce contine kitul de instalare si apoi se deschide eclipse.exe. De mentionat ca veti fi intrebat de un workspace. Odata setat workspace-ul se va downloada pluginul official pentru dezvoltarea aplicatiilor. Primul pas pe care-l vom face va fi sa mergem in eclipse->Help->Install New Software…

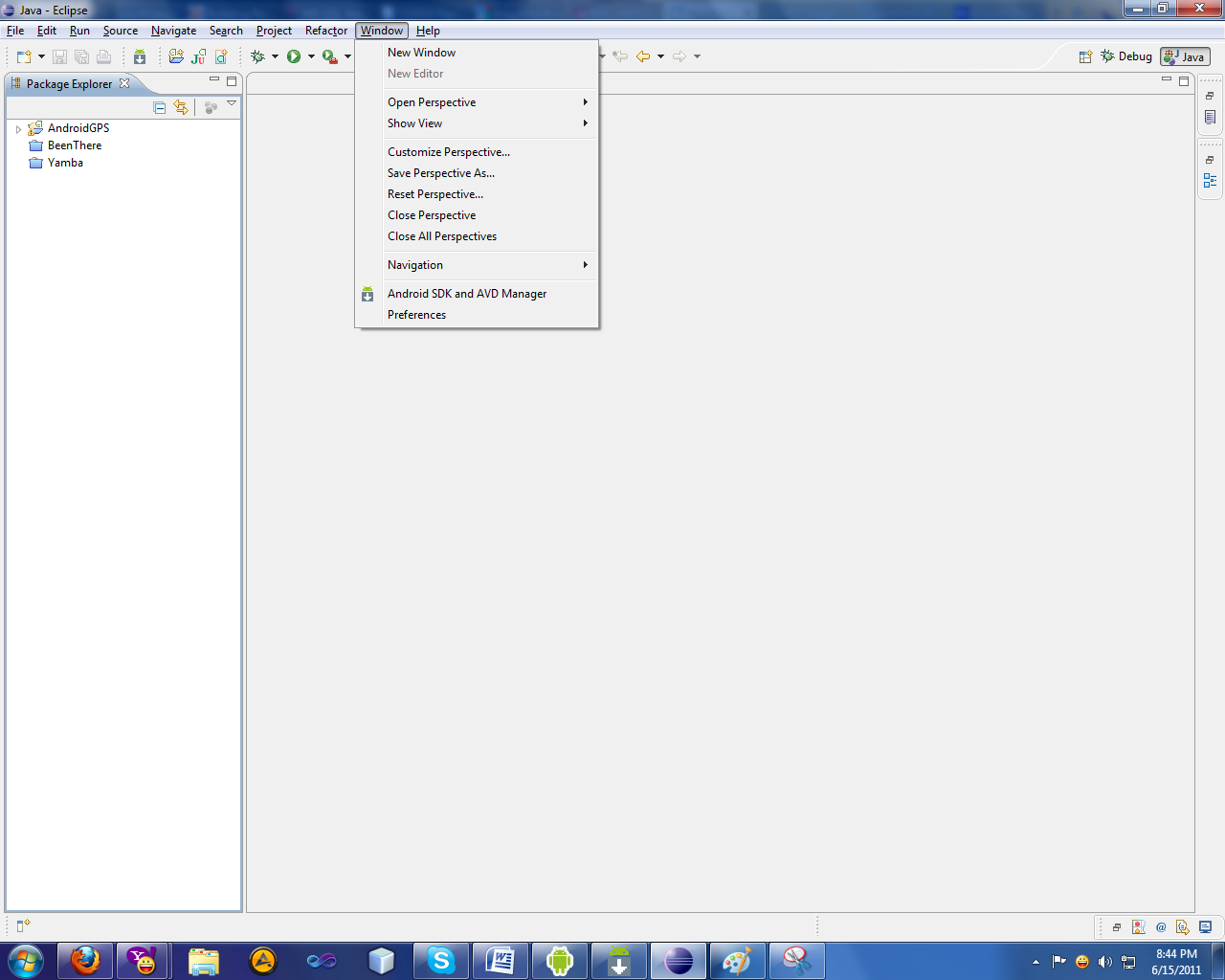


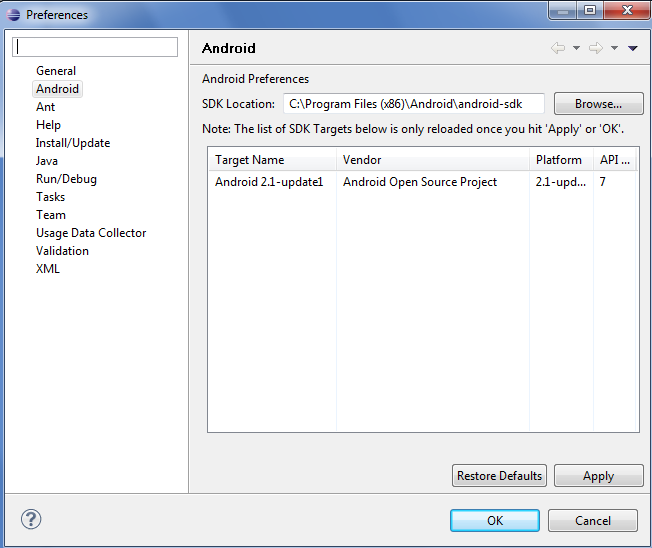
5. In fereastra nou deschisa se introduce in textboxul work with:

https://dl-ssl.google.com/android/eclipse/

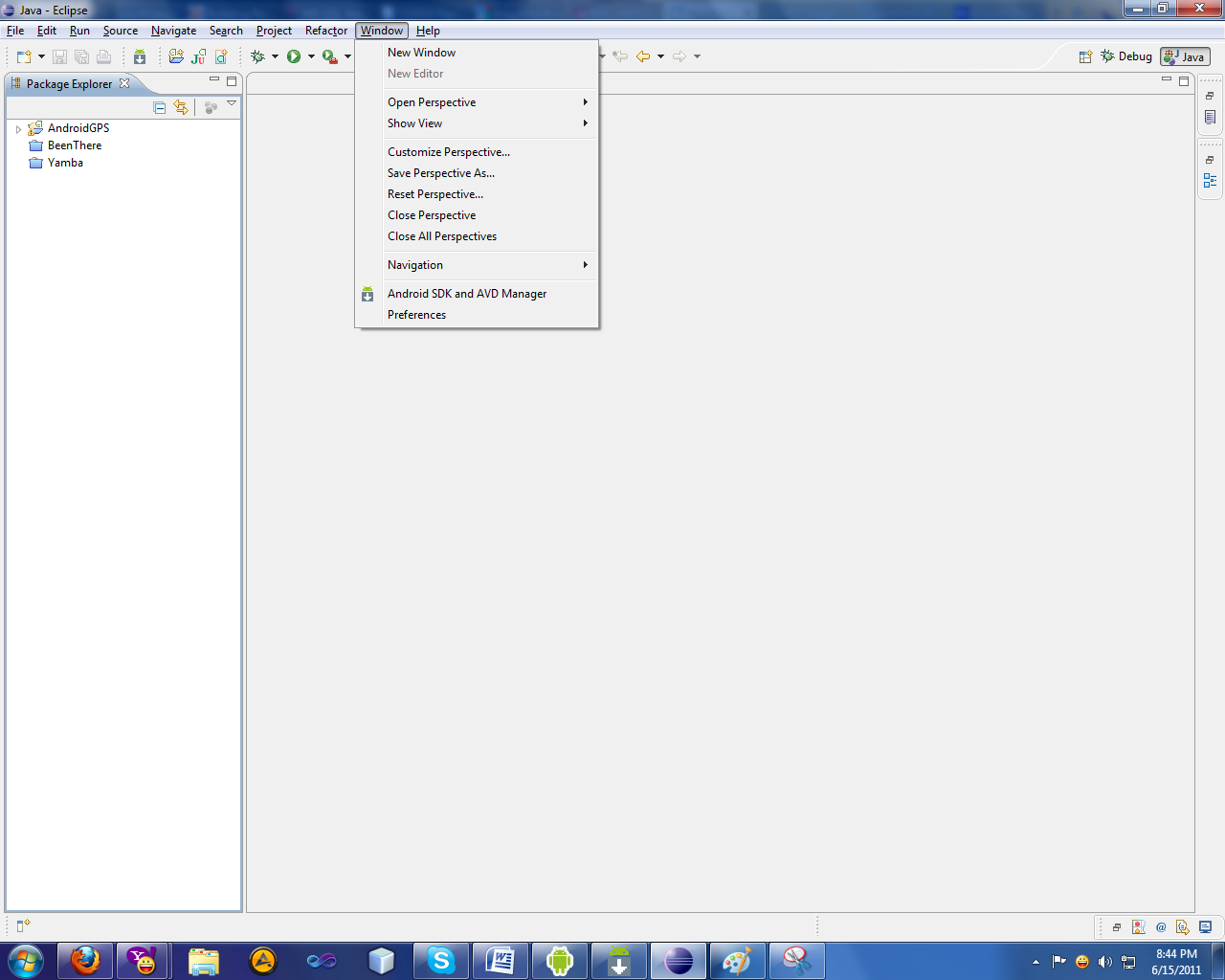


6. Apoi se da next->next->finish, si se restarteaza eclipse.

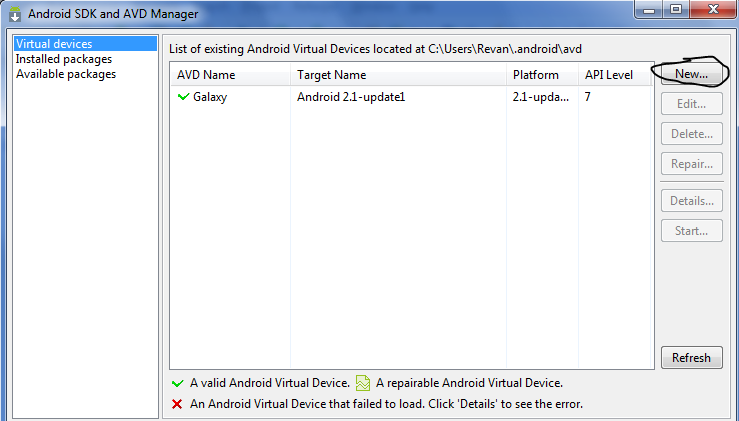
7. Se da calea sdk-ului in eclipse. Pentru asta vom merge la window->Preferences si vom selecta android. 



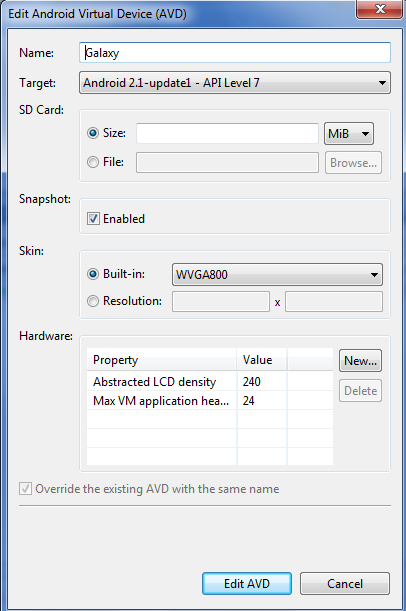
8. Ultimul pas, trebuie sa ne creem un device, pe care va rula emulatorul. Practic toate proiectele pe care le vom crea in eclipse si vor fi rulate, vor trebui a fi rulate pe un emulator care va simula un telefon mobil cu sistemul de operare Android. Aici sunt mai multe setari de care trebuie sa tinem cont, dar cea mai importanta este rezolutia telefonului. In aplicatia nostra am folosit un telefon Samsung Galaxy S, aplicatia fiind gandita pentru rezolutia acestui telefon, bineinteles pe viitor va fi portata si pe alte rezolutii. Prin urmare in eclipse vom selecta window->SDK and AVD Manager:



Apoi vom allege Virtual Devices din fereastra, respective New.

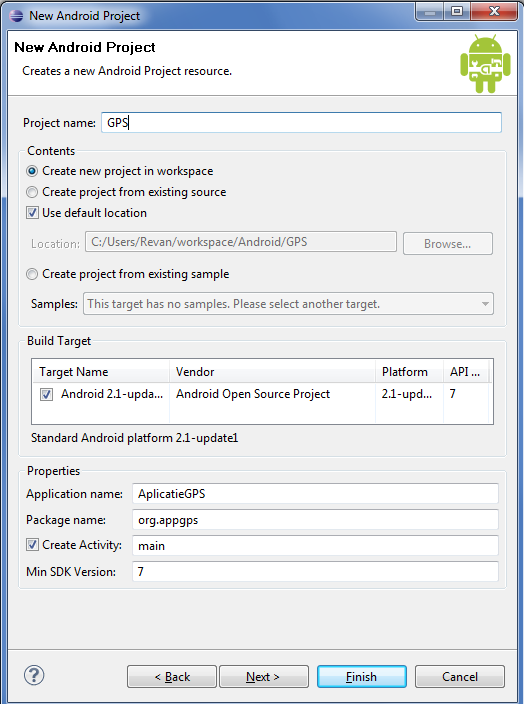


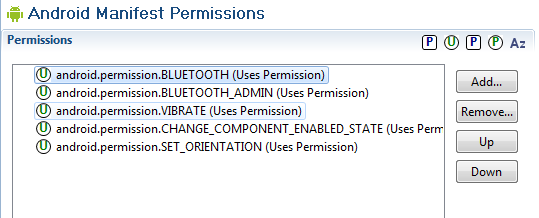
Vom completa apoi informatiile din formularul care apare:



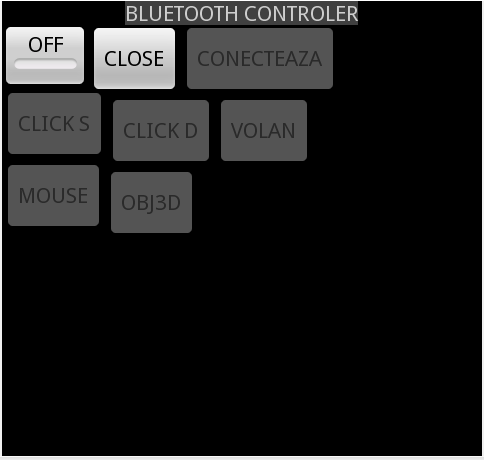
Astfel am pregatit mediul pentru dezvoltarea urmatoarei aplicatii.

# Dezvoltarea aplicatiei

1. Vom deschide un nou proiect Android in Eclipse in care vom da urmatoarele setari
2. Orice aplicatie Android, care se instaleaza pe terminalul mobil are anumite permisiuni care le cere sistemului si care utilizatorul trebuie sa le accepte. Acest lucru se traduce print-un manifest al aplicatiei in care se specifica cerintele functionale si nefunctionale ale aplicatiei si permisiunile. Aici manifest este un fisier xml, in care se scriu setarile/cerintele. Pentru GPS cerintele fiind urmatoarele:



1. Odata setat manifestul nu ne mai ramane decat realizarea aplicatiei. Primul lucru pe care-l vom face va fi sa creem un nou layout ce-l vom lega unei activitati. Trebuie retinut ca in Android UI se poate crea in doua feluri, declarativ (fisier xml) sau imperative (cod java). Interfata grafica fiind una oarecum simpla vom folosi design view care vine odata cu pluginul de la android si vom crea urmatoarea interfata grafica:



4. Aceasta interfata grafica este de fapt in locul celei care este create default de plugin cand se creeaza un nou proiect, aceasta fiind deja legata cu o activitate.

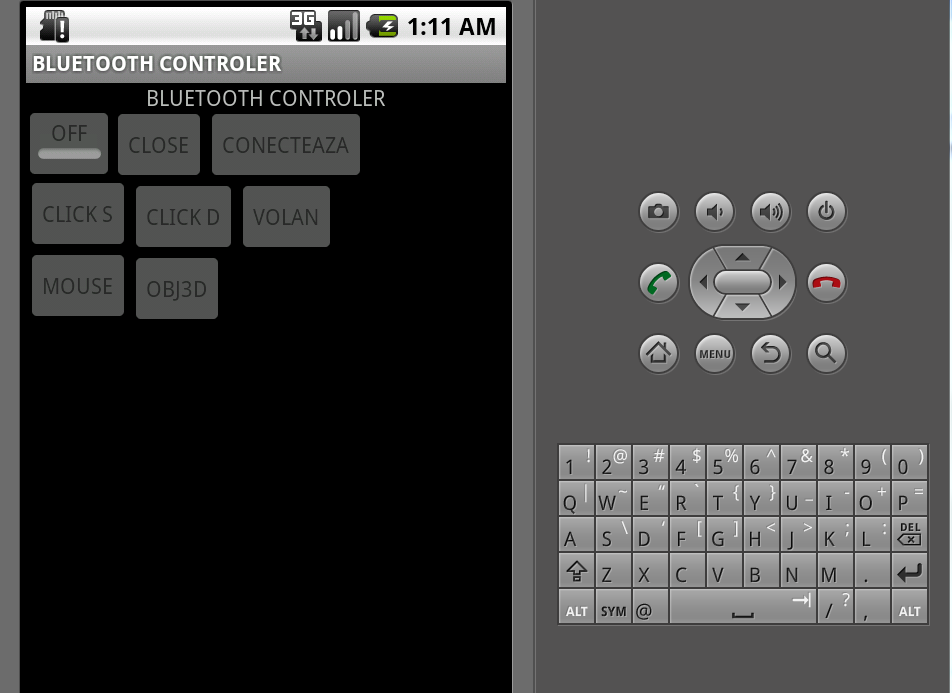
5. Selectam main.java (care este activitatea noastra principala) si ne asiguram in metoda onCreate avem urmatoarele randuri:

public void onCreate(Bundle savedInstanceState) {

super.onCreate(savedInstanceState);

setContentView(R.layout.*main*);

}



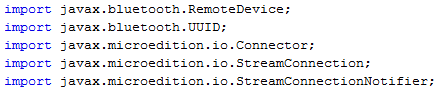
6. Emulatorul nu suporta conexiune tip bluetooth, drept urmare vom rula aplicatia pentru test direct pe telefon. Din setarile USB ale telefonului trebuie selectat Debugging mode on. Astfel in momentul in care vom rula proiectul din eclipse aplicatia se v-a instala automat pe telefon si v-a porni pe acesta.

Prezentarea aplicatiei

Proiectul a fost conceput utilizand libraria bluecove impreuna cu NetbeansIde pentru clientul si serverul de pe computer si utilizand Android SDK impreuna cu Eclipse IDE pentru aplicatia de pe mobil.

Server

Pentru conexiunea bluetooth sunt necesare importurile:



In primul rand trebuie setate toate datele necesare conexiunii bluetooth



Unde setam UUID(universally unique identifiers) ce reprezinta un id unic de identificare a serviciului bluetooth.

Valoarea setata(1101 sau 0X1101 pe 16bit) reprezinta Portul Serial Bluetooth

Dupa setarea datelor necesare cream un StreamConnectionNotifier ce are rolul de a anunta o incercare de conexiune din partea unui device.



In momentul in care primim informatia ca un device doreste o conexiune acceptam si deschidem aceasta conexiune.

Dupa deschiderea conexiuni preluam deviceului conectat de unde putem obtine date gen nume, id etc...



Pentru citirea informatiilor primite de la deviceul conectat deschidem un InputStreamReader pe care il vom citi cu un BufferedReader.



Obtinem informatia primita in format String dupa care procesam informatia

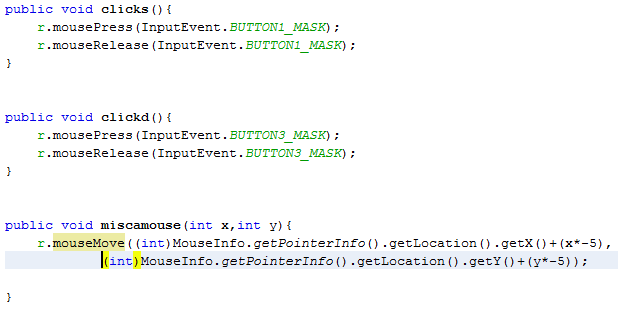


Verificam mesajul primit pentru comenzi cunoscute pe care le executam, sau daca mesajul nu contine o comanda este afisat folosint System.out.print



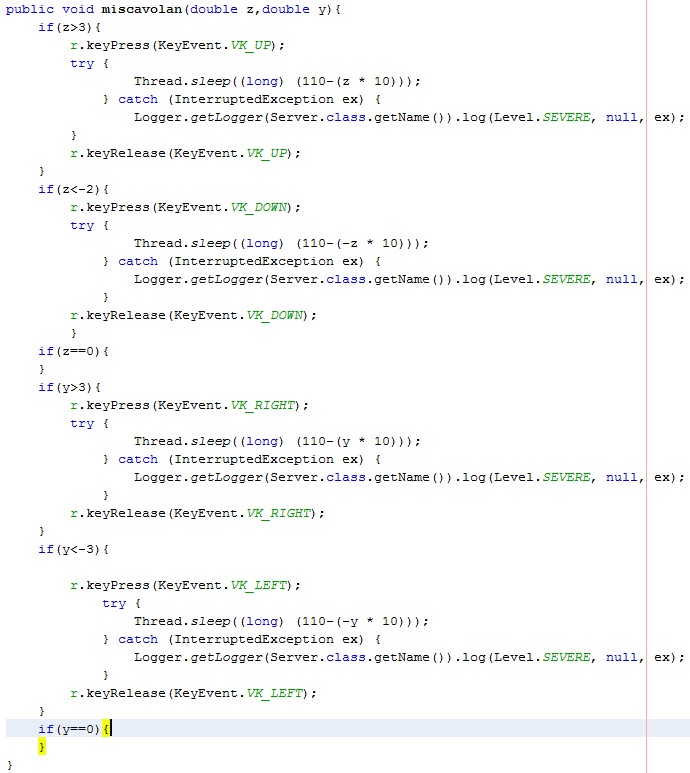
Pentru fiecare comanda exista o metoda ce se executa pentru a realiza actiunea dorita de utilizator.

Metodele pentru executarea actiunilor legate de mouse:



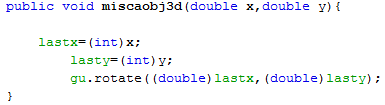
Metodele pentru actiunile legate de mouse utilizeaza o instanta a clase robot ce permite simularea apasarii butoanelor mouseului si miscarea pointerului pe ecranul computerului.

Metodele pentru executarea actiunilor legate de simulatorul “volan”:



Utilizeaza tot clasa robot pentru simularea apasarii butoanelor in functie de semnalul primit de la deviceul conectat.

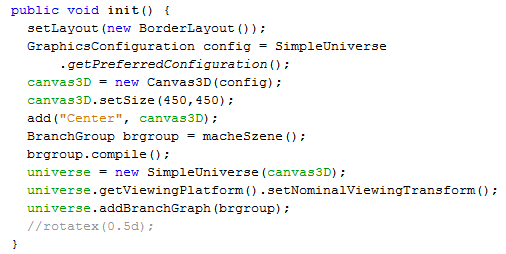
Metoda de miscare a obiectului 3d:



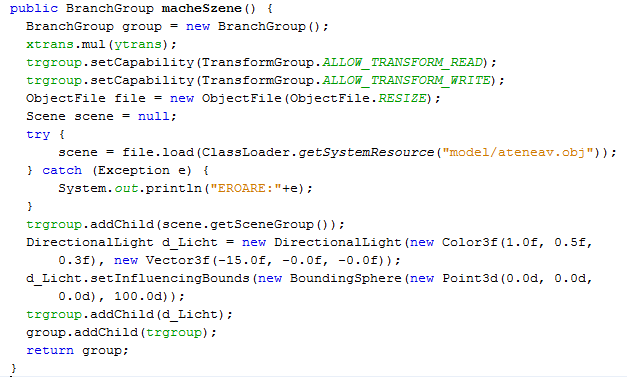
Apeleaza o metoda din clasa Grafica.java

Clasa Grafica:

Metoda de initiere a universului:



Initiaza universul ce contine un Canvas3d pe care vom desena obiectele 3d importate.

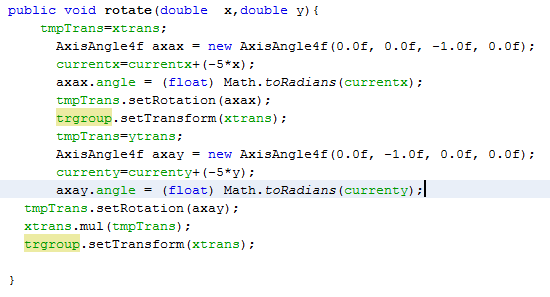


Metoda BranchGroup importa obiectul vrml folosind ClassLoader si il ataseaza unui grup impreuna cu o lumina directionala.

Metoda de distrugere a universului:

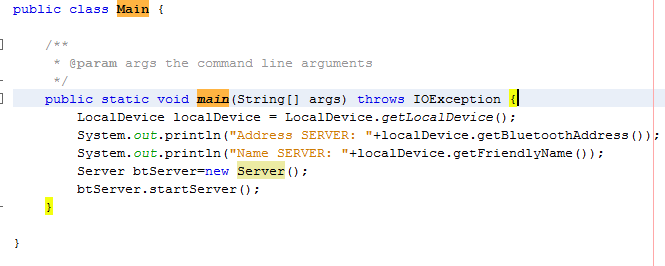


Metoda ce executa rotatia obiectului 3D:



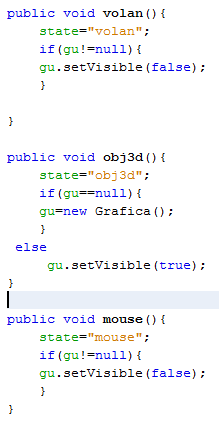
Realizeaza o transformare de rotatie a obiectului 3D cu un anumit unghi in jurul uneia din axe.

Clasa main



Preia informatiile deviceului pe care ruleaza serverul si afiseaza Adresa si Numele acestuia. Apoi porneste serverul Bluetooth.

Metodele de schimbare a starii simulatorului si executie a metodelor necesare de pornire a simulatorului in starea respectiva si de oprire a starilor anterioare:



Server testing

Test server-client mobile 1 – VIDEO

Test server-client mobile 2-VIDEO

Test server-client mobile 3-VIDEO

Test Server-Client Computer

Test Server-Client Mobile

TESTE CLIENT TELEFON - SERVER 1.-VIDEO

Test Server-Client Computer

Test server-client computer 1 –VIDEO

Test Client Computer-Server

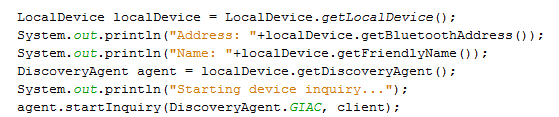
Test CLIENT COMPUTER-SERVER 1-VIDEO

Client Computer

Clientul utilizeaza urmatoarele importuri pentru conexiunea Bluetooth:

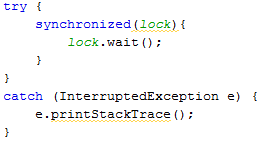


Clientul implementeaza interfata DiscoveryListener ce se ocupa cu ascultarea starii agentului ce cauta deviceurile vizibile din raza de actiune.

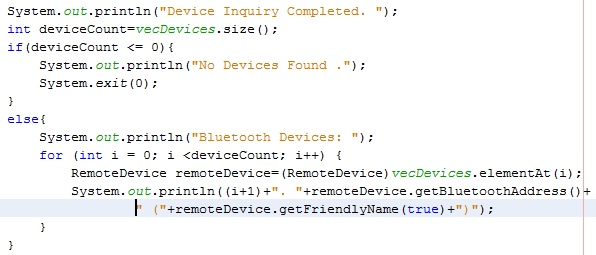


Cream un LocalDevice pentru a prelua datele deviceului pe care ruleaza aplicatia.

Afisam numele si adresa aplicatiei. Pe urma cream un agent ce are responsabilitatea de a cauta deviceurile vizibile din raza de actiune. Pornim agentul si preluam lista de deviceuri.

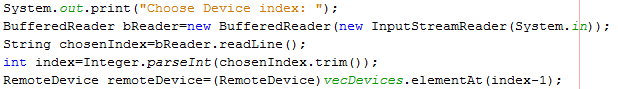


Utilizam lock pentru a astepta pana la finalizarea preluarii deviceurilor.

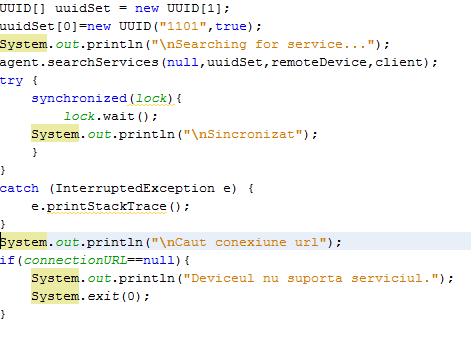


Dupa finalizarea preluarii listei de deviceuri, in cazul in care nu s-a gasit un device vizibil in raza de actiune afisam mesajul prin care informam acest lucru.

In cazul gasirii a cel putin un device afisa o lista cu acestea si atribuim pentru fiecare un id.



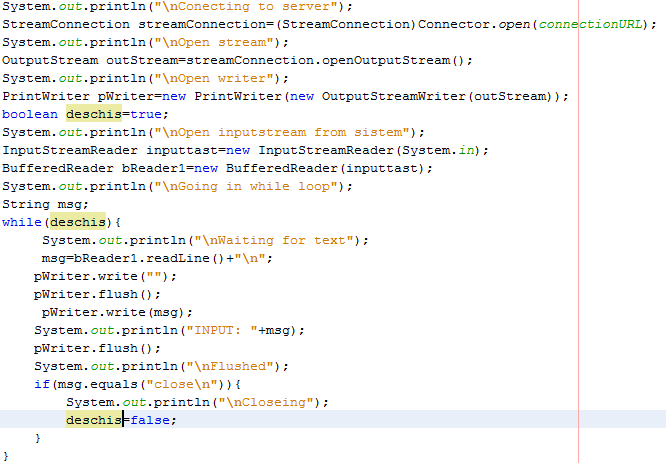
Cerem alegerea unui device din lista si il extragem din vectorul de deviceuri.



Setam idul unic de identificare dupa care cautam serviciul server pe deviceul selectat.

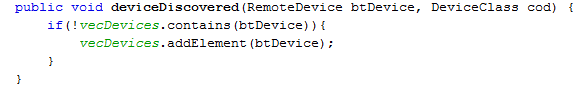
In cazul in care nu exista un serviciul ce are Portul Serial 1101 deschis consideram ca acel device nu suporta serviciul necesar. Drept urmare inchidem conexiunea.

Daca deviceul selectat contine serviciul necesar deschidem streamul conexiunea cu devieceul:



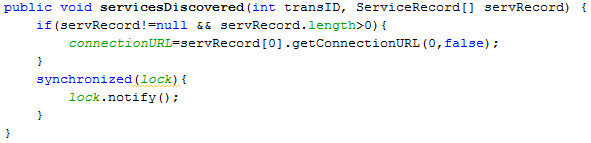
Dupa deschiderea streamului de conexiune deschidem un OutputStream prin intermediul caruia vom trimite informatia introdusa de utilizator. Cu ajutorul unui PrintWriter vom trimite mesajul introdus pe care il preluam in interiorul unei bucle tip while.

Metoda deviceDiscovered ce introduce deviceurile descoperite in vectorul de deviceuri:



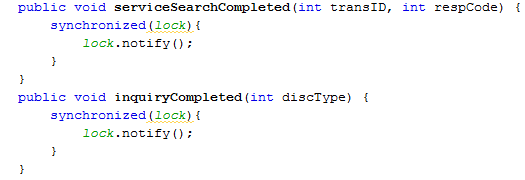
Preia informatiile despre device si clasa acestuia si introduce deviceul in vector.

Metoda servicesDiscovered verifica serviciile existente pe deviceul conectat pentru a stii daca contine serviciul dorit.



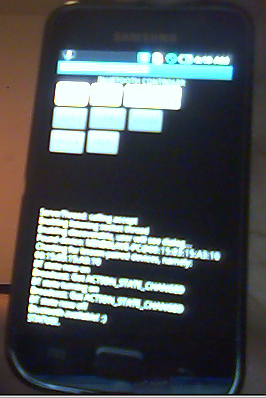
Cand gaseste serviciul dorit preia urlul acestuia si notifica continuarea algoritmului de conectare.

Metodele search completed si inquiry completed

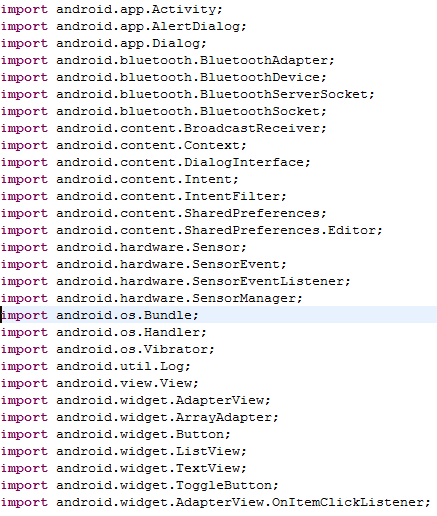


Notifica finalizarea cautarii de deviceul si a preluarii datelor acestora.

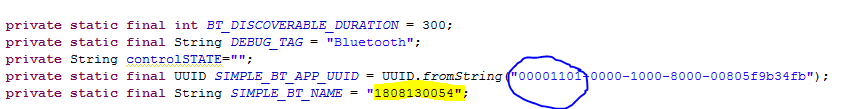
Client Mobile



Aplicatia client mobile foloseste urmatoarele importuri pentru conexiunea si transferul de date prin

 Bluetooth

Initializam datele necesare conexiunii Bluetooth



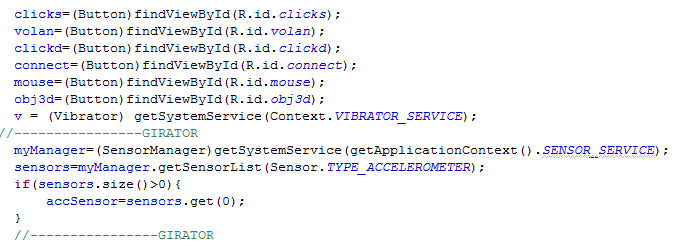
A se observa incercuit idul de identificare contine idul portului serviciului serverului la care vrem sa ne conectam. Portul reprezinta Portul Serial Bluetooth.Restul idului este autogenerat pentru unicitate.

A se observa si seria ce reprezinta numele (idul serie) al telefonului(este afisat de catre server cand se indeplineste o conexiune).

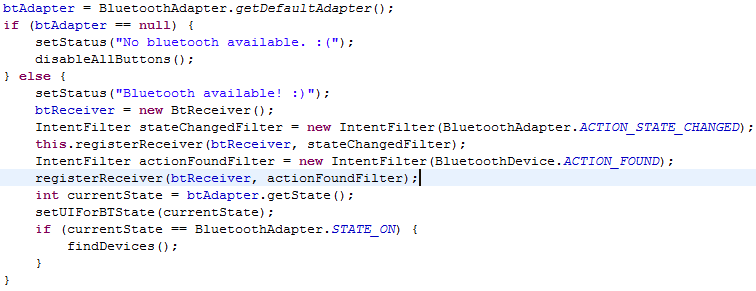
Metoda de initializare a aplicatiei pe mobil:



In interiorul metodei initializam obiectele din interfata grafica si obiectele necesare conexiunii Bluetooth



Observam initializarea butoanelor si a Managerului pentru senzorul Accelerometrului.

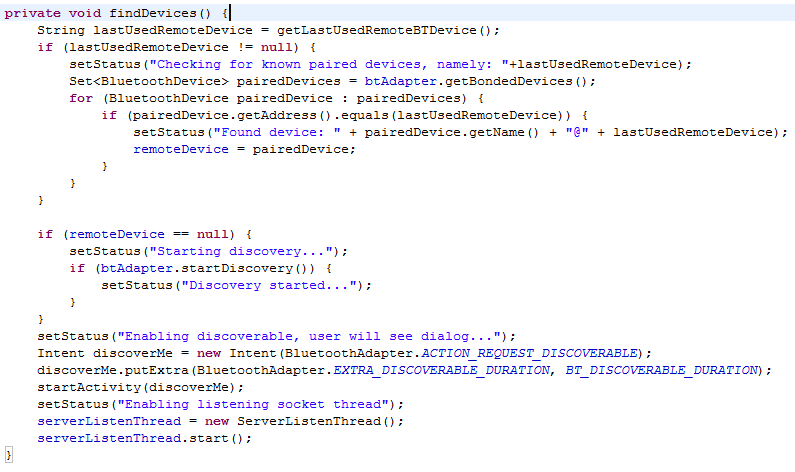


Verificam daca telefonul are suport Bluetooth.

Si cream filtre pentru actiunile ce vor include adaptorul Bluetooth.

Dupa verificarea starii curente a adaptorului Bluetooth.

Daca acesta este pornit apelam metoda de cautare a deviceurilor vizibile in raza de actiune.

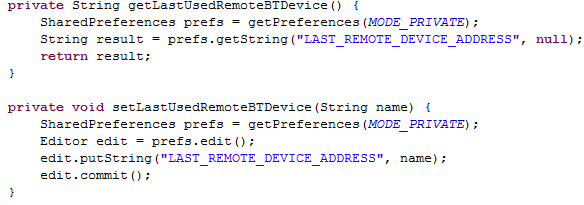


Metoda se imparte in trei cazuri. In primul rand cautam deviceul care a fost utilizat ultima oara. Apoi cautam deviceurile Paired cu telefonul si afisam lista in status. In ultimul caz pornim descoperirea deviceurilor vizibile in raza de actiune.

In final activam starea de a putea fi descoperit a telefonului pentru a realiza o conexiune Paired cu deviceul selectat sau autoales(ultimul utilizat).

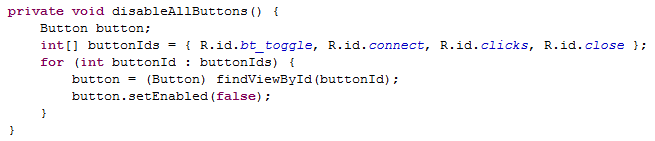
Initializam si pornim Threadul de ascultare a feedbackului.

Metodele de atribuire si preluare a ultimului device paired folosit



Editam fisierul prefs in care introducem adresa ultimului device conectate remote.

Metoda de dezactivare a butoanelor din interfata

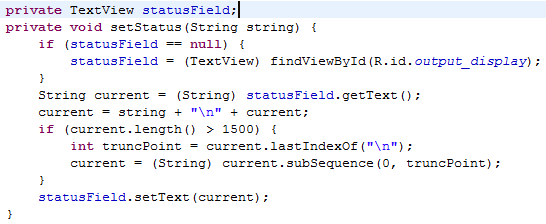


Aceasta metoda este utilizata in momentul in care nu gasim un adaptor Bluetooth pe telefon.



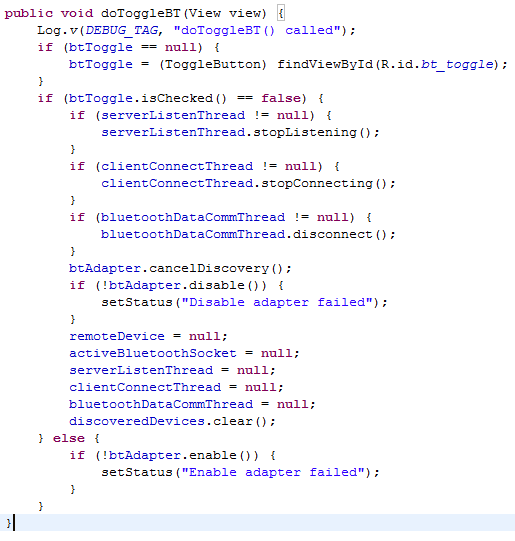
Aceasta metoda modifica starea butoanelor din interfata in functie de starea adaptorului Bluetooth (inchis sau deschis).

Metoda de setare a statusului



Adauga text la status pentru a vizualiza in format text (consola) ce actiuni se petrec in aplicatie.

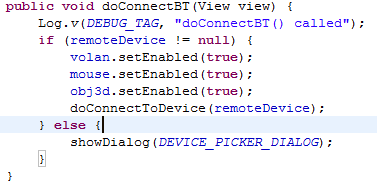
Metoda butonului toggle ON/OFF



In aceasta metoda activam si dezactivam adaptorul Bluetooth.

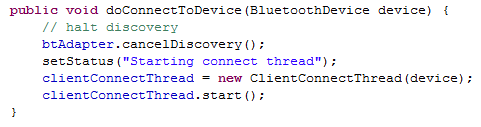
Pentru a nu pierde date in momentul in care dezactivam adaptorul anulam descoperirea de deviceuri si setam toate componentele necesare conexiuni la valoarea null, dupa care stergem lista de deviceuri descoperite, acestea ne mai fiind necesare.

Metoda butonului connect



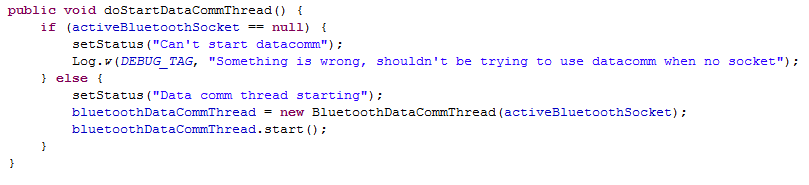
Aceasta metoda activeaza butoanele ce pot fi utilizate dupa conexiune si apoi apeleaza metoda de conexiune la un device selectat.

Metoda de conectare a deviceului selectat



Aceasta metoda opreste descoperirea deoarece am selectat deja la ce device dorim sa ne conectam, dupa care porneste un Thread pentru conexiunea cu deviceul respective.

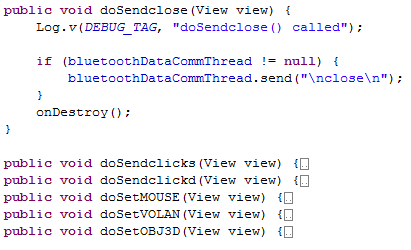
Pornirea threadului de comunicare date



Se initializeaza un thread nou pe care apoi il pornim.

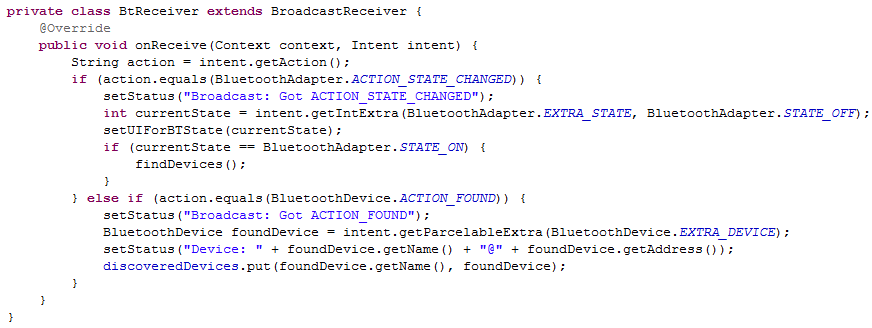
Threadul se initializeaza cu Socketul active conexiunii Bluetooth.

Metodele de transmitere date si comenzi



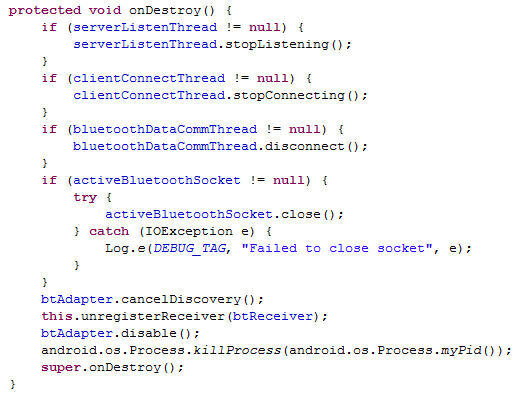
Toate metodele de transmitere date sau comenzi utilizeaza threadul comunicare date pornit inainte.

Clasa Broadcast Receiver (de primire a datelor)

’Aceasta metoda realizeaza o conexiune de tip primire feedback cu deviceul selectat..

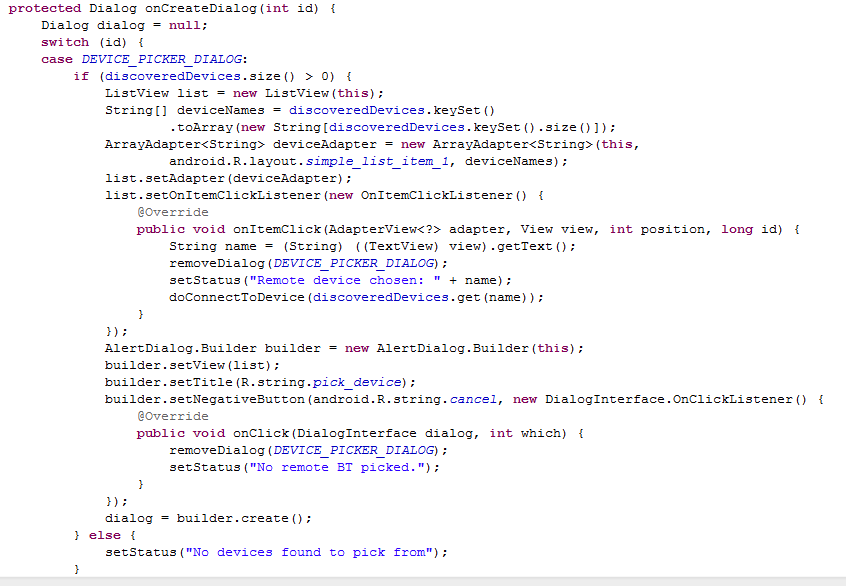
Utilizeaza o clasa abstracta BroadcastReceiver specializata pe primirea de date.

Metoda de distrugere a aplicatiei



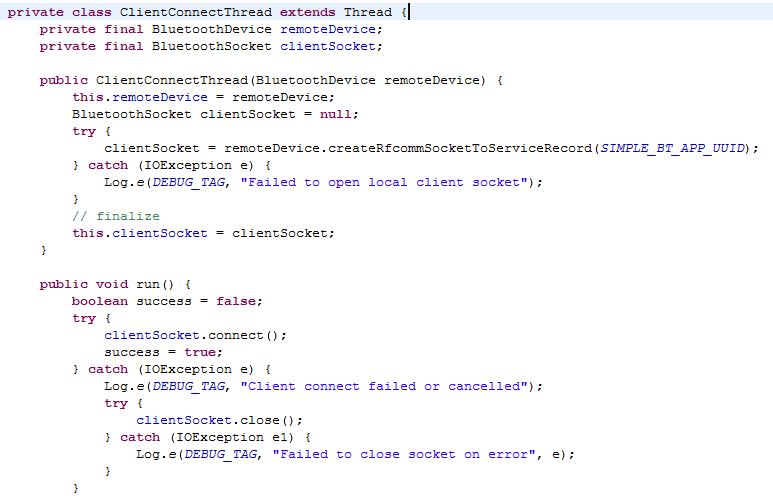
Opreste orice actiune legata de Bluetooth, dezactiveaza adaptorul, dupa care distruce procesele si aplicatia.

Metoda ce creeaza dialogul cu lista de deviceuri

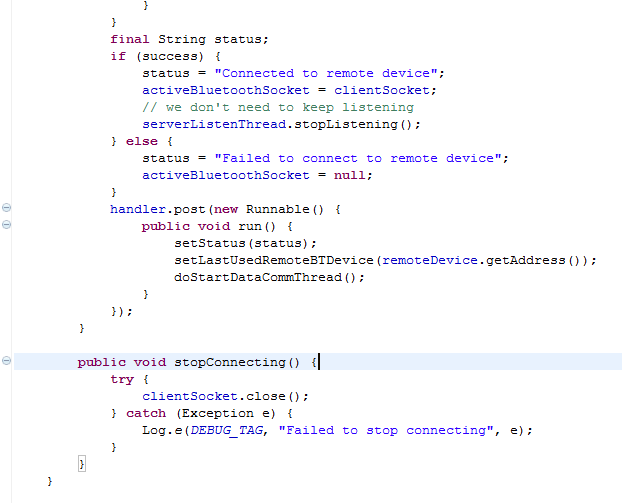


Creeaza un dialog in care este afisata lista cu deviceuri gasite in urma cautarii si trateaza actiunile, de selectare a deviceului dorit, dupa care apeleaza metoda de conectare cu deviceul respectiv.

Clasa ce trateaza conexiunea cu fiecare client (pentru multiclient )

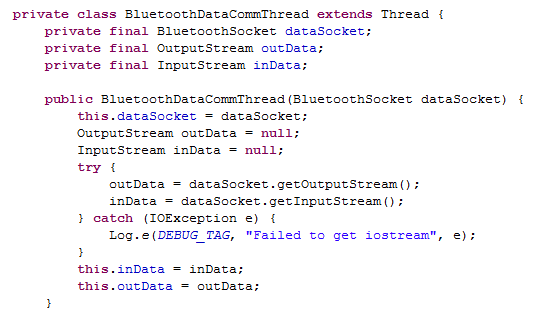


Creeaza socketul de conexiune la serviciul aplicatiei si conecteaza acel socket.

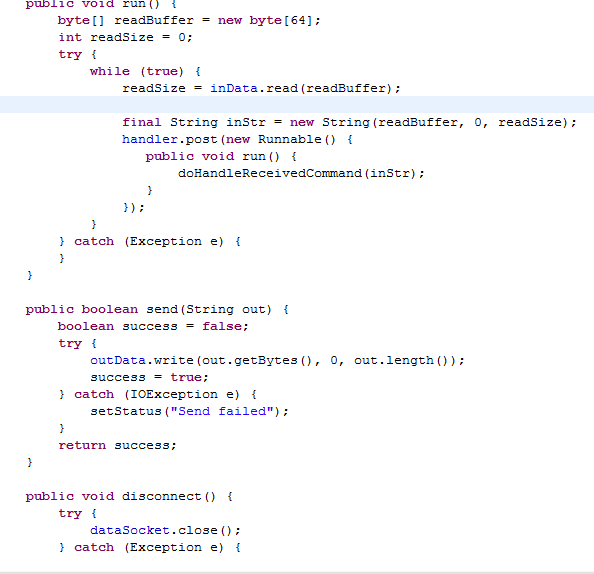


Cand este reusita conexiunea pe socket se deschide un thread de comunicare date si se salveaza adressa clientului ca ultim device folosit ca remote.

Clasa Bluetooth Data communication thread



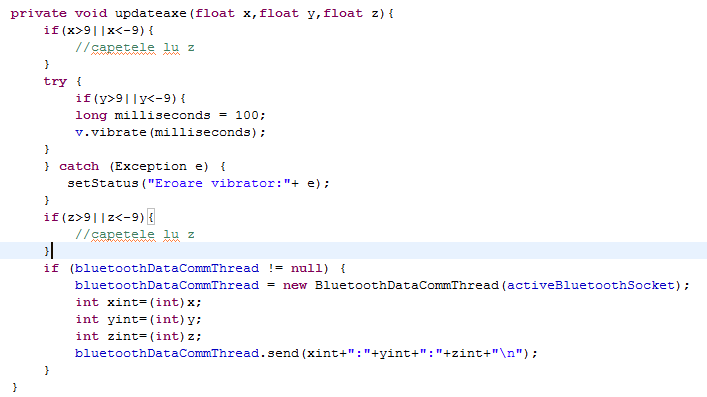
Utilizeaza conexiunea socketelor pentru a deschide streamuri de input-output.



Metoda run porneste threadul de date, metoda send trimite date prin streamul output deschis.

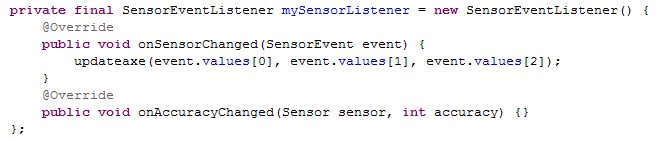
Metoda disconnect inchide socketul si astfel si conexiunea intre deviceuri pe acel socket.

Metoda update axe



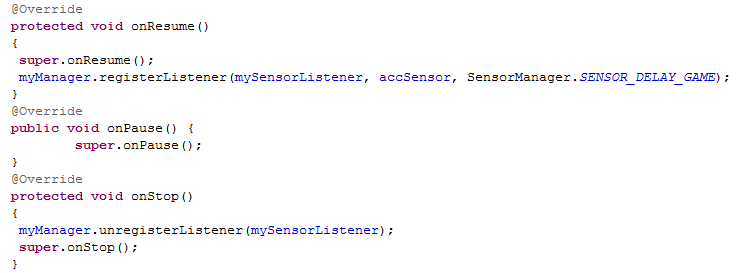
Preia datele si actualizeaza starea curenta a axelor dupa care trimite informatia catre server.

Sensor Event Listener



Suprascrie metodele Eventurilor realizate de sensor, si anume senzorul Accelerometrului.

Suprascrierea metodelor aplicatiei



Aici suprascriem metodele de oprire pauza si reluare a aplicatiei pentru a putea stopa sau reporni Listenerul pentru accelerometru.

Tutorial de utilizare a aplicatiilor

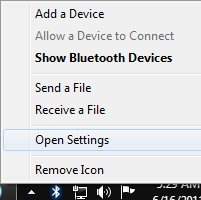
Server

Cerinte minime:

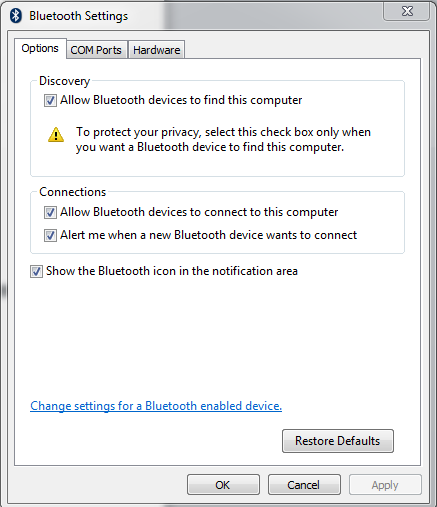
Necesita existenta unui adaptor Bluetooth, activarea acestuia si setarea sa pentru a putea fi gasit de alte deviceuri.

Mode de utilizare:

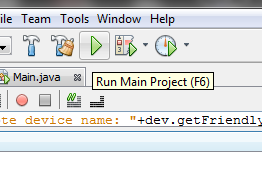
Se activeaza adaptorul Bluetooth,



se seteaza pentru a putea fi descoperit,



dupa care se porneste aplicatia.



Client telefon

Cerinte minime

Sistem de operare android, adaptor Bluetooth, accelerometru

Instructiuni de utilizare

Se instaleaza aplicatia pe telefon utilizand IDE-ul Eclipse cu android sdk instalat in prealabil.

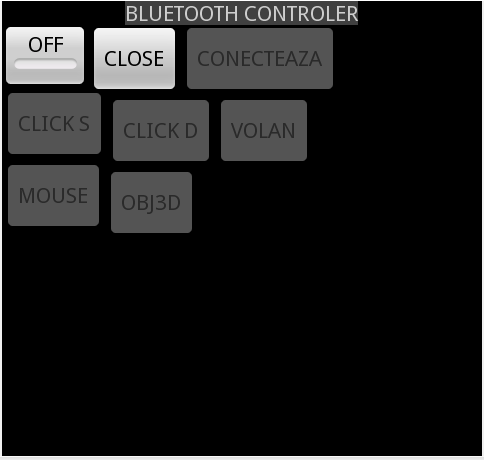
Se seteaza starea usb a telefonului Debugging ON

Se conecteaza telefonul la calculator cu ajutorul cablului de date,

Se deschide aplicatia in Eclipse

Ruleaza proiectul

Aplicatia v-a fi instalata si deschisa automat dupa instalare.



Daca nu este pornit adaptorul bluetooth, se apara butonull on/off.

Se asteapta activarea adaptorului, dupa care se apasa butonul connect.

Daca e prima utilizare a aplicatiei se selecteaza din lista deviceul la care doriti sa va conectati.

In status se v-a semnala realizarea(sau esuarea) conexiunii.

Dupa reusirea conexiuni se pot folosi butoanele MOUSE, VOLAN si OBJ3D pentru selectarea modului.

Pentru modulul Mouse pointerul se controleaza in felul urmator:

Telefonul se tine in pozitie orizontala cu partea de sus a telefonului spre inainte.

Inclinand partea de sus a telefonului spre podea, pointerul se misca in jos.

Inclinand partea de sus a telefonului spre tavan, pointerul se misca in sus.

Inclinand spre partea stanga telefonul, pointerul se v-a misca spre stanga.

Inclinand spre partea dreapta telefonul, pointerul se v-a misca spre dreapta.

Pentru a actiona functiile click stanga si click dreapta folositi butoanele clicks respectiv clickd de pe ecranul telefonului.

Pentru modulul volan masina se controleaza in felul urmator:

Telefonul se v-a tine inclinand partea de sus spre stanga.

Pentru a accelera se v-a inclina telefonul spre inainte, iar pentru a incetinii spre inapoir.

Pentru a fira se v-a inclina telefonul spre stanga respectiv spre dreapta.

Pentru modulul OBJ3D obiectul 3D se controleaza astfel:

Telefonul se tine ca in pozitia modulului mouse.

Inclinajus inainte si inapoi v-a roti obiectul in jurul axei sale perpendiculara pe orizontala.

Inclinajul spre stanga dreapta v-a roti obiectul pe axa sa paralela cu orizontala dar perpendiculara pe suprafata ecranului.

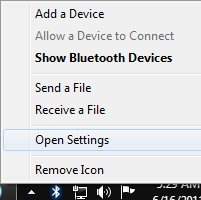
Client computer

Cerinte minime:

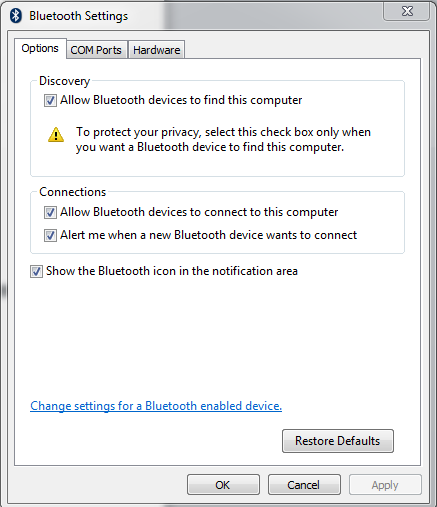
Necesita existenta unui adaptor Bluetooth, activarea acestuia si setarea sa pentru a putea fi gasit de alte deviceuri.

Mode de utilizare:

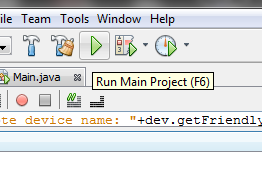
Se activeaza adaptorul Bluetooth,



se seteaza pentru a putea fi descoperit,



dupa care se porneste aplicatia.



Dupa cautarea deviceurilor vizibile se introduce numarul respectiv deviceului dorit dupa care se apasa enter.

Se asteapta realizarea conexiunii.

Dupa realizarea conexiunii veti fi anuntat ca se asteapta introducerea de date text.

Se scrie data si se apasa enter.

BIBLIOGRAFIE

1. www.bluetooth.com
2. www.wikipedia.com
3. Bluetooth 1.1: Connect Without Cables (2nd Edition) Jennifer Bray,Charles F. Sturman
4. Discovering Bluetooth Michael Miller
5. Bluetooth Security (Artech House Computer Security Series) Christian Gehrmann,Joakim Persson,Ben Smeets
6. Bluetooth Application Programming with the Java APIs (The Morgan Kaufmann Series in Networking) C Bala Kumar,Paul Kline,Tim Thompson
7. http://bluecove.org/
8. http://developer.android.com