Bluetoothin tietoturva

Eero Kaipiainen

Helsinki 20. huhtikuuta 2003

Tietoturvallisuus nykyaikaisessa liiketoimintaympäristössä -seminaari

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Sisältö

1 Johdanto

Bluetooth on teknologia langattomaan kommunikointiin. Bluetoothin kehitys aloitettiin Bluetooth Special Interest Group (SIG) nimisessä ryhmässä vuonna 1998. Perustajajäsenet olivat Ericsson, Nokia, IBM, Intel ja Toshiba. Tämän jälkeen ryhmään on liittynyt useita yrityksiä lisää mukaan lukien Microsoft. Bluetoothin versio 1.0 julkaistiin vuonna 1999 ja versio 1.0B vuonna 2000. Viimeisin versio on 1.1 [5] [6].

Bluetoothin päämääränä on yhdistää erilaisia laitteita langattomasti. Yleisimpiä tapoja yhdistää laitteita Bluetoothilla on esimerkiksi matkapuhelimen ja kannettavan tietokoneen tai taskutietokoneen (PDA) kytkeminen. Bluetoothilla voidaan muodostaa myös niin sanottuja "ad hoc" -verkkoja, joissa korkeintaan kahdeksan laitetta voi kommunikoida keskenään. Verkossa yksi laite toimii *master*-laitteena ja loput toimivat *slave*-laitteina. Bluetoothin käyttöä rajoittaa sen kantama, joka tällä hetkellä on noin kymmenen metriä. Bluetoothia voidaan käyttää esimerkiksi työpaikoilla tai kotona. Työpaikalla voidaan Bluetooth-laitteiden avulla lähettää luottamuksellista tai salaista tietoa, jolloin tarvitaan tietoturvaa [5].

Seuraavassa kappaleessa 2 kerrotaan Bluetooth-laitteiden fyysisestä tominnasta. Kappaleessa 3 käsitellään Bluetoothin tietoturva-arkkitehtuuria ja kappaleissa 4 ja 5 kerrotaan Bluetoothin heikkouksista ja parannusehdostuksista. Kappaleessa 6 kerrotaan eroista Bluetoothin ja WLAN:in tietoturvassa ja lopuksi on yhteenveto kappaleessa 7.

2 Fyysinen toiminta

Bluetooth-laitteet jaetaan kolmeen luokkaan sen perusteella, millä teholla niiden lähetys toimii. Ensimmäiseen luokkaan kuuluvat sellaiset laitteet, joiden kantama on sata metriä ja lähetysteho on 100 mW. Toisessa luokkaan määritellään laitteet, joilla kantama on kymmenen metriä ja lähetysteho on 1 - 2,5 mW. Kolmanteen luokkaan kuuluvat laitteet, joiden lähetysteho on 1 mW ja kantama on 0,1 - 1 metriä [5].

Bluetoothin käyttämä lähetystapa tarjoaa jonkin asteista tietosuojaa, koska lähetystaajuus voi vaihdella 2.4 GHz kaista-alueella, jolloin vain sen kanssa synkronoiduilla vastaanottajilla on mahdollisuus vastaanottaa tietoa. Tätä tekniikkaa kutsutaan FHSS-tekniikaksi (engl. fast frequency spread spectrum) [5] [4].

3 Tietoturva-arkkitehtuuri

Tässä käsitellään Bluetoothin tietoturva-arkkitehtuurista. Aluksi kerrotaan oleellisia asioita, jotka vaikuttavat laitteen turvallisuuteen. Laite voi olla havaittavassa tai havaitsemattomassa tilassa. Lisäksi laiteella on kaksi muuta tilaa. Laitteeseen voidaan ottaa yhteys tai siihen ei voi ottaa yhteyttä. Jokaisella Bluetooth-laitteella on yksikäsitteinen tunniste (engl. Bluetooth device address) BD_ADDR, jota käytetään yhteyden muodostamiseen laitteiden välillä. Jos laite on tilassa että siihen saadaan yhteys, niin todentamisessa käytetään DAC-kooodia (engl. device access code). DAC muodostetaan *slave*-osoitteesta. Jokaista piste-piste- tai piste-monipiste -yhteyttä (engl. point-to-point ja point-multipoint) kohden on olemassa oma kanava ja sillä on tunnisteensa CAC (engl. channel access code). Se muodostetaan *master*-laitteen yksikäsitteisestä osoitteesta. Laite on luotettava tai epäluotettava. Uusi laite on aina epäluotettava. Luottamus laitteiden välillä saavutetaan pariutumisen aikana. Pariutumistapahtumasta kerrotaan myöhemmin lisää [1].

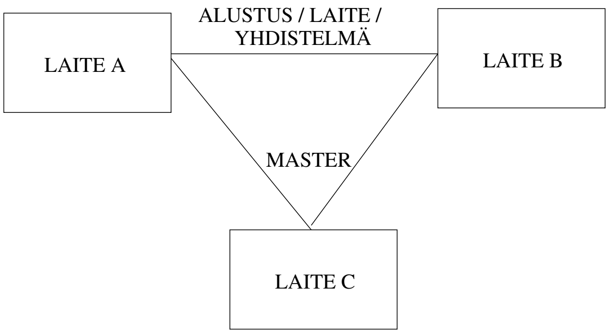
Bluetoothin sovellukset käyttävät useita turvatiloja [1].

- Kun Bluetooth-laite toimii tilassa yksi, se ei ikinä vaadi yhteyden salaamista tai muiden Bluetooth-laitteiden todentamista.

- Kun laite toimii tilassa kaksi, tällöin laite ei aloita Bluetooth-linkin todentamista tai salausta. Tietoturvatoimenpiteitä aloitetaan käyttämään vasta kanavan tai yhteyden muodostamisessa.

- Kun laite on tilassa kolme, se aloittaa tietoturvaproseduurit ennen kuin linkki toisen laitteen välillä on toiminnassa. Tässä tilassa voidaan käyttää kahdenlaista turvapolitiikkaa: vaaditaan todentamista toiselta laitteelta tai vaaditaan sekä todentamista että tiedon salausta.

Bluetooth käyttää seuraavia avaimia PIN-koodi, alustusavain K_{init}, linkkiavain, salausavain K_C ja *master*-avain K_{master} (kuva 1).



Kuva 1: Erilaisia avaimia [5]

PIN-koodi (engl. Personal Identification Key) on joko ennalta määrätty tai se syötetään käsin laitteeseen. PIN-koodin pituus voi olla 8-128 bittiä. PIN-koodin pitää olla sama niissä laitteissa, jotta todentaminen olisi mahdollista laitteiden välillä. Alustusavainta tarvitaan linkkiavaimen muodostamisessa.

Linkkiavaimia on olemassa kahdenlaisia: yhdistelmäavaimet (K_{AB} tai K_{BA}) ja laiteavaimet (K_A tai K_B). Bluetooth-laitteet, joissa on vähän muistia käyttävät laiteavainta (engl. unit key), koska yhdistelmäavaimet voivat viedä liikaa muistia. Tässä tapauksessa laite käyttää laiteavainta kaikissa pariutumisissa muiden laitteiden kanssa. Laiteavain muodostetaan, kun laitetta käytetään ensimmäisen kerran. Yhdistelmäavain on yksikäsitteinen laitepareille.

Salausavainta käytetään yhteyden salaamiseen ja se muodostetaan todentamisvaiheen yhteydessä. *Master*-avainta käytetään, kun halutaan tehdä monilähetys usealle laitteelle.

Alustusavaimen luomisesta alkaa laitteiden pariutumisvaihe. Alustusavain johdetaan laitteen osoitteesta, PIN-koodista ja satunnaisluvusta käyttämällä algoritmia, joka perustuu SAFER+-lohkosalaajaan. Laite luo satunnaisluvun ja lähettää sen toiselle laitteelle. Jos PIN-koodi on lyhyempi kuin 128 bittiä, niin sitä täydennetään laitteen osoitteella BD_ADDR. Tämän jälkeen voidaan muodostaa linkkiavain.

Linkkiavaimen muodostamisessa käytetään kahta tapaa riippuen siitä, että tullaanko käyttämään laiteavainta vai yhdistelmäavainta [6].

Linkkiavain laiteavaimesta.

1. Alustusavain muodostetaan edellä mainitulla tavalla.

2. Laiteavain ja alustusavain yhdistetään käyttämällä SAFER+-lohkosalaajaa ja tulos lähetetään toiselle laitteelle B.

3. Vastaanottava laite B purkaa saamansa viestin omalla alustusavaimella, jolloin se saa saman laiteavaimen, joka on laitteella A. Tästä tulee laitteen B linkkiavain.

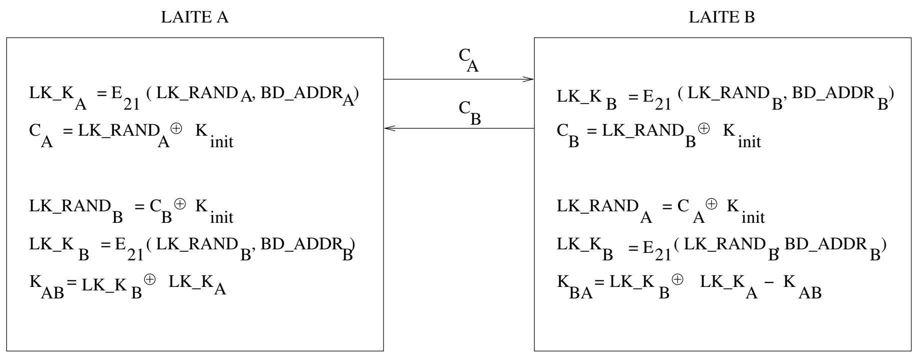
Linkkiavain yhdistelmäavaimesta (kuva 2).

1. Alustusavain muodostetaan edellä mainitulla tavalla.

2. Kumpikin laite A ja B muodostavat satunnaisluvut LK_RAND_A ja LK_RAND_B. Tämän jälkeen ne muodostavat linkkiavaimet edellä olevista satunnaisluvuista ja omasta osoitteestaan. Tämä tapahtuu käyttämällä algoritmia, joka perustuu

SAFER+ -lohkosalaajaan. Kumpikin laite yhdistävät saamansa linkkiavaimen satunnaislukuun XOR-operaatiolla.

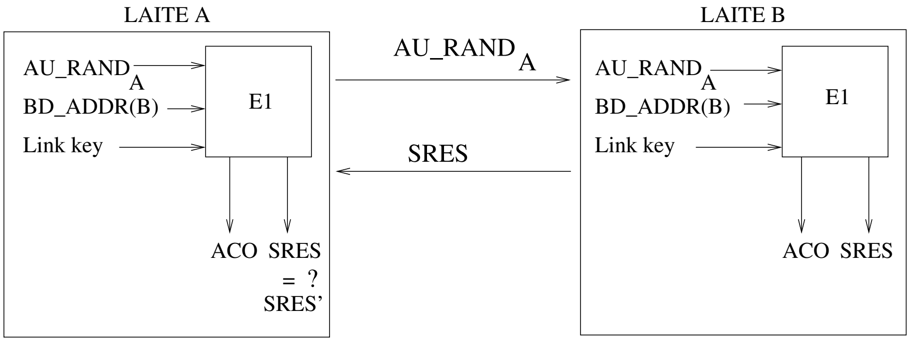
3. Laitteet vaihtavat salatut avaimet.
4. Laitteet purkavat saamansa avaimet kuvassa 2 olevalla tavalla.



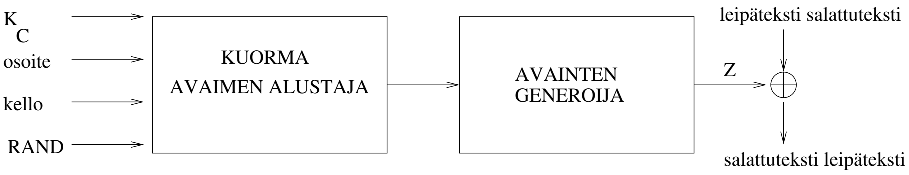
Kuva 2: Yhdistelmäavaimen muodostaminen [6]

Linkkiavaimen muodostamisen jälkeen alkaa todentaminen laitteiden välillä. Laite A (kuva 3) lähettää satunnaisluvun AU_RAND$_A$ laitteelle B. B laskee linkkiavaimesta ja satunnaisluvusta vastausarvon SRES. Laite B lähettää vastauksen takaisin laitteelle A. Laite A tarkistaa, onko vastaus SRES sama kuin ennalta laskettu arvo SRES'. Todentaminen perustuu SAFER+ -lohkosalaajaan. Todentamisen yhteydessä kummatkin laitteet luovat bittijonon ACO (engl. Authentication Ciphering Offset), jota käytetään salauksessa [6].

Salausavain muodostetaann ACO:sta tai *master*-laitteen osoitteesta ja käytössä olevasta linkkiavaimesta. Salaaja koostuu kolmesta osasta (kuva 4). Ensimmäisessä osassa (engl. payload key generator) *master*-laitteen osoite, salausavain, kello ja satunnaisluku järjestetään sopivaan järjestykseen ja ne siirretään neljään LFSR-rekisteriin (engl. linear feedback stream register), jossa niistä luodaan avaimia, joilla leipäteksti salataan tai salattu teksti puretaan. Salausalgoritmi perustuu SAFER+-lohkosalaajaan [6].



Kuva 3: Kuvaus kahden laitteen todentamistapahtumasta [6]



Kuva 4: Salaajan toimintaperiaate [6]

4 Heikkouksia

Tässä kappaleessa esitellään muutamia Bluetoothin heikkouksia. Vakavimmat uhkat kohdistuvat lyhyihin PIN-koodeihin ja sijaintihyökkäykseen, jolla voidaan selvittää laitteen sijainti.

4.1 Laiteavaimet

Todentaminen ja salaus perustuu joko laiteavaimiin tai yhdistelmäavaimiin. Laite, jossa on vähän muistia käyttää laiteavainta linkkiavaimena. Tällöin laite joutuu antamaan sen kaikille niille laitteille joihin se haluaa olla luotettavassa yhteydessä. Ne (luotettavat) laitteet, jotka ovat suorittaneet todentamisen voivat salakuunnella laiteavainta käyttävän laitteen liikennettä [1].

4.2 Lyhyet PIN-koodit

Hyökkääjä voi selvittää laitteiden PIN-koodit salakuuntelemalla niiden käymän avainten vaihdon ja todennusvaiheen. Tämän jälkeen hyökkääjä voi laskea jokaista PIN-koodia kohti alustustusavaimen arvon. Lopuksi hän laskee linkkiavaimen ja tarkistaa sen oikeellisuuden suorittamalla todentamisvaiheen uhrin kanssa [2].

Toisessa tavassa hyökkääjä yrittää arvata järjestelmällisesti PIN-koodeja tiettyyn pituuteen asti. Hyökkääjä tarkistaa jokaisen arvauksen oikeellisuuden todentamistapahtumalla (kappale 3 ja kuva 3). Jos todentaminen onnistuu, tällöin laite tietää saaneensa oikean PIN-koodin. Tätä tapaa käytetään sellaisia laitteita vastaan, joissa on vähän muistia eli ne käyttävät laiteavainta linkkiavaimena [2].

Jos hyökkääjä saa haltuunsa oikean linkkiavaimen, niin se voi tämän jälkeen muodostaa myös salausavaimen. Lisäksi hyökkääjän on mahdollista saada haltuunsa vastapuolen laiteavaimen salakuuntelemalla, jos sellainen on käytössä.

Jos hyökkääjällä on jo hallussa linkkiavain, jota kaksi laitetta käyttää, tällöin hyökkääjä voi ottaa yhteyden kumpaakin laitteeseen ja uskotella niille esittävänsä toista osapuolta (engl middle-person attack). Esimerkiksi hyökkääjä voi tehdä niistä *slave*-laitteita itselleen tai ruveta *slave*- laitteeksi ja tätä kautta saada itselleen osapuolten lähettämät viestit [2].

4.3 Sijaintihyökkäys

Kaksi tai useampi laite voi jakaa saman lähetyskanavan, jolloin ne muodostavat niin sanotun pikonetin (engl. piconet). Jokaisessa pikonetissa on yksi *master*-laite ja muut ovat *slave*-laitteita. Hyökkääjän täytyy siis seurata *master*-laitteen ja *slave*-laitteiden taajuuksia, joilla ne kommunikoivat. Bluetooth käytää muiden Bluetooth-laitteiden havaitsemiseen erityistä *inquiry*-proseduuria. Havaittavassa tilassa olevat laitteet vastaavat *inquiry*-tiedusteluun FHS-paketilla (engl. Frequency Hop Synchronisation), joka sisältää laitteen osoitteen BD_ADDR. FHS-paketti liittyy Bluetoothin käyttämään lähetystaajuuden vaihtamistekniikkaan. Yhteys toiseen laitteeseen suoritetaan käyttämällä *page scan*-proseduuria ja *slave*-laitteet vastaavat *master*-laitteelle, jos ne havaitsevat oman DAC-koodinsa. Kun yhteys on muodostettu laitteiden välillä, niin jokaiseen pakettiin liitetään CAC-arvo. Hyökkkääjän tarvitsee saada haltuunsa yksi FHS-paketti ja jos hän pystyy selvittämään sen sisällön, hän voi alkaa seurata laitteiden taajuden vaihtelua ja liikennettä. Koska tunnisteet pysyvät samoina, hyökkääjän on helppo päätellä *master*- ja *laitteiden* sijainnit ja hän voi myös pitää kirjaa laitteiden liikkeistä [2] [1].

4.4 Salauksen murtaminen

Salauksen murtaminen on mahdollista, mutta hyvin epätodennäköistä. Se voidaan tehdä arvaamalla kolmen pienimmän LFSR-rekisterin ja yhteenlasku rekisterin sisällöt. Tämän jälkeen hyökkääjä yrittää matemaattisesti päätellä neljännen rekisterin sisällön. Lopulta tutkitaan oliko arvaus oikein vertaamalla sitä alkuperäiseen arvoon, joka on saatu salakuuntelemalla. Hyökkääjä tarvitsee noin 128 bittiä alkuperäistä leipätekstiä ja salattua tekstiä. Yhteensä kolmannen rekisterin sisällön päättely ja arvontarkistusvaihe vie 2^{100} bittioperaatiota. Raa'an voiman käyttö vaatisi 2^{128} bittioperaatiota [2].

5 Parannusehtotuksia

Tässä kappaleessa esitellään parannuksia Bluetoothin tietoturvan puutteisiin. Suurimpana ongelma lienee liian lyhyt PIN-koodi, koska se on tietoturvan perusta Bluetoothissa. Lisäksi esitellään keino estää sijaintihyökkäys.

5.1 PIN-koodin pituus ja laiteavaimet

PIN-koodin pitää olla tarpeeksi pitkä ja satunnainen, jotta kappaleessa 4 esitetty tilanne olisi vaikeampi toteuttaa. Esimerkiksi 64 bittiä pitkä PIN-koodi tai pitempi on riittävän turvallinen, jos se on valittu satunnaisesti. Todentamista ei suositella, että se suoritetaan julkisissa paikoissa. Nämä parannukset ovat tosin täysin riippuvaisia laitteiden käyttäjistä tai käyttäjästä [2].

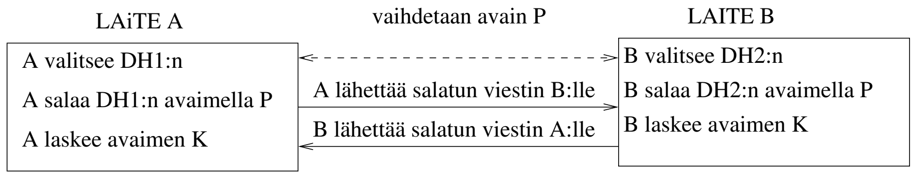
Laitteet voisivat suojata laiteavaimensa paremmin, jos ne eivät käyttäisi laiteavainta linkkiavaimen muodostamiseen vaan laiteavaimesta johdettua avainta. Avain voitaisiin luoda joka kerta uudelleen. [2].

5.2 Diffie-Hellman

Koska Bluetooth-laite on yleensä pienikokoinen mobiililaite, jossa on mahdoton suorittaa monimutkaista laskentaa. Tällöin monimutkaista laskentaa tulee välttää ja tarvitaan kevyempiä lähestymistapoja kuten EKE, joka perustuu Diffie-Hellman-protokollaan. EKE-protokollan tarkoituksena on pienentää hyökkääjän mahdollisuutta saada laitteen PIN-koodi [1].

Aluksi laitteiden käyttäjät tai käyttäjä vaihtavat julkisen avaimen P (kuva 5). Tämän jälkeen kumpikin laitteista A ja B luovat Diffie-Hellmannissa tarvittavan satunnaisluvun. Laite A salaa DH1:n ja laite B salaa DH:2n julkisella avaimella P. Laite A lähettää salatun DH1:n laitteelle B ja vastaavasti laite B lähettää salaamansa DH2:n laitteelle A. Tämän jälkeen kumpikin laite purkaa saamansa viestin avaimella P [1].

Edellä esitetty tilanne ei kuitenkaan vielä estä vastustajaa hyökkäämästä keskeltä eli protokollan tarvitaan tarkistusarvoja. Hän voisi esimerkiksi käyttää syntymäpäivähyökkäystä. Oletetaan, että kolmas osapuoli C saa haltuunsa sekä laitteen A



Kuva 5: EKE -protokolla [1]

lähettämän arvon g^{DH1} että laitteen B lähettämän arvon g^{DH2}. C alkaa luomaan eksponentteja niin kauan kunnes se löytää oikeat arvot c ja d siten, että ehto $f(g^{DH1*c}) = f(g^{DH2*d})$ pätee.

Tämän estämiseksi tarvitaan toimenpiteitä esimerkiksi lisäämällä tarkistusvaiheen edellä olleeseen protokollaan. Kun protokolla on suoritettu, käytetään tarkistusarvoja. Menetelmä on esitelty alla [1]:

1. Laite muodostaa lyhyen ja satunnaisen merkkijonon ja lähettää toiselle laitteelle
2. Toinen laitteista salaa merkkijonon ja aikaisemmin luodun avaimen, jollain salausmenetelmällä. Salattu arvo CV lähetetään toiselle laitteelle. Tällainen menetelmä voisi olla esimerkiksi jokin tiivistefunktio (engl. hash function).
3. Jos kummankin laitteen muodostamat CV-arvot ovat samoja tällöin Diffie-Hellman -avain hyväksytään muussa tapauksessa se hylätään.

5.3 Sijaintihyökkäyksen esto

Suojautumiseen sijainti hyökkäykseltä ehdotetaan kahden uuden tilan lisäämistä Bluetoothin spesifikaatioon, jolloin uudet tilat olisivat seuraavat: tuntematon ja tunnettu [1]. Jokainen tuntemattomassa tilassa toimiva laite käyttää kahta osoitetta:

1. Osoite BD_ADDR, joka on jo määritelty spesifikaatiossa.

2. Laite muodostaa toisen satunnaisen osoitteen BD_ADDR_active, joka on samanpituinen kuin alkuperäinen. Osoite päivitettäisiin tietyn ajanjakson jälkeen uudelleen.

Seuraavaksi käsitellään muutoksia proseduureihin *inquiry* ja *page scan*. *inquiry*-proseduuri palauttaa uuden osoitteen (2) alkuperäisen osoitteen sijasta.

Page scan -proseduuria muutetaan seuraavalla tavalla. Jos laite on jo ennestään pariutunut joidenkin laitteiden kanssa, niin laite kuuntelee näiden osalta DAC-koodeja, jotka perustuvat sekä alkuperäiseen (1) ja uuteen osoitteeseen (2). Tässä tilanteessa oletetaan, että laite tietää osoitteen BD_ADDR, johon yhteyttä ollaan ottamassa.

Laite käyttää muuten samaa *page scan*-mekanismia ja osoitteena *slave*-laitteen BD_ADDR. DAC, CAC ja FHS-paketti muodostetaan osoitteesta BD_ADDR_active.

Kun yhteys on muodostettu ja todentamista ei ole vielä suoritettu, niin *master*-laite lähettää *slave*-laitteelle paketin, joka sisältää osoitteen BD_ADDR_alias (tämän muodostamisesta myöhemmin lisää tietoa). Osoite on sovittu edellisellä kerralla, kun ne ovat olleet yhteydessä. *Slave*-laite pystyy selvittämään osoitteesta BD_ADDR_alias *master*-laiteen oikean osoitteen BD_ADDR. Todentamisessa ja salauksessa käytetään kuitenkin *master*-laitteen alkuperäistä osoitetta BD_ADDR. Jos laitteet eivät ole ennestään pariutuneet, niin CAC, DAC ja FHS-paketti muodostetaan osoitteesta BD_ADDR_active [1].

Kun pariutumisvaihe on suoritettu ja salattu yhteys on toiminnassa, laitteet vaihtavat osoitteensa BD_ADDR ja sopivat satunnaisesti valittavasta osoitteesta BD_ADDR_alias. Kun tätä osoitetta tarvitaan, se joka kerta muutetaan ja vaihdetaan osapuolten välillä. Jokaisen laitteen tulee tosin pitää kirjaa näistä BD_ADDR_alias-osoitteista. Tämä ei välttämättä ole mahdollista laitteissa, joissa on vähän muistia [1].

6 WLAN ja Bluetooth

Bluetooth vaihtaa lähetystaajuuttaan lähetyksissään, jolloin lähetyksien salakuuntelu on vaikeampaa, mutta ei mahdotonta. WLAN-keskitin kaiuttaa kaikki sille tulevat paketit eteenpäin, joten WLAN:in salakuuntelu on helpompaa. WLAN:iin on lisätty tietoturvaa lisääviä piirteitä kuten WEP. Sen tarkoituksena on salata liikenne laitteiden välillä ja kaikki laitteet käyttävät samaa salasanaa. Salaus ei anna juurikaan suojaa, jos verkko on julkinen.

Ei ole helppoa sanoa, että kumman tietoturvallisuus on parempi. WLAN sopii ehkä paremmin lähiverkkoihin ja Bluetooth antaa paremman käytettävyyden monille uusille sovelluksille [3].

7 Yhteenveto

Vaikka Bluetoothista löytyy puutteita, niin se ei tarkoita sitä, etteikö Bluetoothin käyttö ole turvallista. Suurin uhka liittyy lyhyihin PIN-arvoihin, koska jos vastapuoli saa haltuunsa laitteen PIN-koodin, niin tietoturva murentuu täysin. PIN-arvon valinta on lopulta käyttäjän vastuulla. Toisaalta avaimen vaihtoprotokollan lisäämisen tarkoituksena on tuoda enemmän turvaa lyhyitä PIN-koodeja vastaan tehtäviin hyökkäyksiin, jos protokollaan yhdistetään tarkistuarvot, tämän pitäisi ehkäistä kesken hyökkäyksen onnistumista. Toinen ongelma on sijaintihyökkäys ja siihen on ehdotettu uusien tilojen lisäämistä ja *page scan*- ja *inquiry*-proseduurien muuttamista. Tällaisen hyökkäyksen toteuttaminen vaatisi huomattavia taloudellisia resursseja.

Lähteet

1 Gehrmann, Nyberg, “Enhancements to Bluetooth baseband security”, Nordsec ’01

2 Markus Jakobsson and Susanne Wetzel, “Security Weaknesses in Bluetooth”, Lucent Technologies - Bell Labs, Information Sciences Research Center

3 Jyrki Oraskari, “Bluetooth versus WLAN IEEE 802.11x”, Department of Computer Science And Engineering, Helsinki University of Technology

4 Marjaana Träsbäck, “Security of Bluetooth: An overview of Bluetooth Security”, Department of Electrical and Communications Engineering, Helsinki University of Technology

5 J.T Vainio, “Bluetooth security”, Proceedings of Helsinki University of Technology, Telecommunications Software And Multimedia Laboratory, Seminar on Internetworking: Ad Hoc Networking

6 Bluetooth Specification V1.1, www.bluetooth.com/dev/specifications.asp