SALAUS JA AUTENTIKOINTI LANGATTOMISSA JÄRJESTELMISSÄ

Ville Koskinen

Opinnäytetyö
Maaliskuu 2013
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

VILLE KOSKINEN:
Salaus ja autentikointi langattomissa järjestelmissä

Opinnäytetyö 54 sivua
Maaliskuu 2013

Tämän työn tarkoituksena on esitellä erilaisia autentikointi- ja salaustekniikoita joita käytetään langattomissa järjestelmissä. Koska langattomia järjestelmiä on olemassa todella paljon, aina IrDA infrapunatiedonsiirrosta erilaisiin sensoriverkkoihin ja laajoihin mobiiliverkkoihin, ei tässä työssä voida käsitellä kaikkia järjestelmiä. Työhön valittiin sellaisia langattomia järjestelmiä, joita suurin osa ihmisistä käyttää tietoisesti tai tiedostamattomasti lähes päivittäin.

Työssä käsitellään kahden eri tyypin tietoliikennejärjestelmiä. Ensimmäisissä kappaleissa käsitellään pieniä, paikalliselle alueelle rajoittuneita RFID-, Bluetooth- ja WLAN-järjestelmiä. Toinen osa-alue työssä on laajat mobiiliverkot, joista työhön on otettu GSM, UMTS sekä LTE.

Jokainen järjestelmä esitetään ensin perustasolla, jotta lukija saa kuvan järjestelmän toiminnasta. Tämän jälkeen esitetään järjestelmässä käytettävät salaus- ja autentikointimetodit. Työn tavoitteena on antaa lukijalle selkeä kuva kunkin langattoman järjestelmän rakenteesta ja niissä toteutetuista salaus- ja autentikointikäytänteistä.

Autentikointi ja salaus ovat tärkeitä osia jokaisen verkon tietoturvaa, mutta erityisesti langattomissa verkoissa niitä tarvitaan, koska tietoliikenteen siirtotienä toimii helposti hallinnoitavan kaapelin sijasta ympäröivä ilmakehä. Ilmakehässä lähetettävä data leviää joka suuntaan, lähettävän laitteen lähetystehon rajoissa.

Asiasanat: langaton järjestelmä, tietoturva, autentikointi, salaus

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
ICT Engineering
Telecommunications Engineering and Networks

VILLE KOSKINEN:
Encryption and Authentication in Wireless Systems

Bachelor's thesis 54 pages
March 2013

The purpose of this thesis was to present information about encryption- and authentication techniques in different wireless systems. Due the fact that there are a wide range of different kind of wireless systems, from the IrDA-communications to sensor networks and wide area mobile networks, this thesis cannot cover all of them. The systems that were chosen to this thesis are decided by how common they are in the everyday life for consumers.

Thesis covers two types of telecommunications systems. In the first sections are presented small local area networks: RFID-, Bluetooth- and WLAN-systems. Second type of systems in this thesis is wide area mobile networks. Mobile networks that were chosen to this thesis are GSM-, UMTS- and LTE-networks.

This thesis presents each system first in the basic level to let the reader have a good understanding about systems architecture and how it works. After that is presented the systems authentication- and encryption methods. The purpose of this thesis was to give reader a good understanding how different kind of wireless systems work and how the encryption and authentication is handled in them.

Authentication and encryption are a vital component in any secure network, but especially in wireless systems because the transmission medium used in the system is surrounding atmosphere, not easily manageable cable. Where in cable the data packets are transmitted through cable, in atmosphere the data packets are spread all around as wide as the transmission power allows.

Key words: wireless system, data security, authentication, encryption

SISÄLLYS

LYHENTEET JA TERMIT

2G	2nd Generation, toinen sukupolvi
3G	3rd Generation, kolmas sukupolvi
4G	4th Generation, neljäs sukupolvi
A3	GSM-verkossa autentikaatioon käytettävä salausalgoritmi
A5	GSM-verkossa radiotien salaukseen käytettävä salausalgoritmi
A8	GSM-verkon salausalgoritmi, jolla luodaan salausavain K_c
AES	Advanced Encryption Standard, lohkosalausmenetelmä
A_k	Anonymity Key, salausavain
AMF	Authentication Management Field, autentikaatioon käytetty kenttä
AN	Access Network, liityntäverkko
AuC	Authentication Center, tunnistuskeskus
AUTN	Authentication Token, autentikointimerkki
AV	Authentication Vector, autentikaatiovektori
BSC	Base Station Conroller, tukiasemaohjain
BSS	Base Station Sybsystem, tukiasemaosa ja radioliityntäverkko GSM-järjestelmässä
BTS	Base station, tukiasema
CCMP	Counter Mode with CBC-MAC Protocol, salausprotokolla
C_k	Cipher key, salausavain
CN	Core network, ydinverkko
CRC	Cyclic Redundancy Check, tarkisteavaimen luomiseen tarkoitettu algoritmi
DES	Data Encryption Standard, salausmenetelmä
DIAMETER	autentikointiprotokolla
E_0	Bluetooth-järjestelmässä salaukseen käytettävä jonosalain
E_1	Bluetooth-järjestelmässä autentikointiin käytettävä algoritmi
E_2	Bluetooth-järjestelmässä linkkiavaimen luomiseen käytettävä algoritmi
E_3	Bluetooth-järjestelmässä salausavaimen luomiseen käytettävä algoritmi

E_{21}	Bluetooth-järjestelmässä yksikkö- ja yhdistelmäavaimen luomiseen käytettävä algoritmi
E_{22}	Bluetooth-järjestelmässä alustus- ja isäntäavaimen luomiseen käytettävä algoritmi
EAP	Extensible Authentication Protocol, autentikaatioprotokolla
EIR	Equipment Identity Register, laitetunnusrekisteri
eNB	eNodeB, Evolved Node B, tukiasema LTE-järjestelmässä
E-UTRAN	Evolved UTRAN, radioverkko-osa LTE-järjestelmässä
EPC	Evolved Packet Core, ydinverkko-osa LTE-järjestelmässä
EPS AKA	Evolved Packet System Authentication and Key Agreement, salausalgoritmi
GAP	Generinc Access Profice, yleisin Bluetooth-profiili
GGSN	Gateway GPRS Support Node, reititin joka huolehtii reitityksestä ulkoverkon ja GPRS-verkon välillä
GHz	Gigahertsi, taajuuden yksikkö
GMSC	Gateway MSC, puhelinverkon ja muiden MSCiden välillä sijaitseva MSC
GPRS	General Packet Radio Service, GSM-verkossa toimiva tiedonsiirtopalvelu
GRAIN	Jonosalain
GSM	Groupe Spécial Mobile, myöhemmin Global System for Mobile Communications, toisen sukupolven matkapuhelinjärjestelmä
HC	Host Controller, isäntäkontrolleri
HCI	Host Controller Interface, isäntäkontrollerin liityntärajapinta
HF	High Frequency, suurtaajuus, taajuusalue 3-30 MHz
HLR	Home Location Register, kotirekisteri
HN	Home Network, kotiverkko
HSS	Home Subscriber Server, tilaajatietokanta
IEEE	Institute of Electrical and Electronics Engineers
ICV	Integrity Check Value, tarkistusvektori WEP-salauksessa
I_k	Integrity key, salausavain
IMEI	International Mobile Equipment Identity, mobiililaitteen laitetunnus

IMSI	International Mobile Subscribers Identity, verkon käyttäjän/liittymän tunnus, käytetään verkkoon kirjautuessa
IP	Internet Procol, Internet-protokolla
IrDA	Infrared Data Associationin määrittelemä infrapunasäteilyä käyttävä langaton tiedonsiirtostandardi
ISM-taajuusalue	Industrial, Scientific and Medical, vapaa radiotaajuuskaista. Alunperin tarkoitettu teolliseen, tieteelliseen ja lääketieteelliseen käyttöön
IV	Initialization Vector, alustusvektori WEP-salauksessa
IV	Initialization Values, Alustusmuuttujat UEA2/UIA2-algoritmeissa
ICV	Integrity Check Value, tarkistusvektori WEB-salauksessa
K_{ASME}	salausavain
K_c	Chiphering Key, salausavain
K_{eNB}	salausavain
KDF	Key Derivation Function, funktio
kHz	Kilohertsi, taajuuden yksikkö
K_i	Authentication Key, salausavain
K_{NASenc}	salausavain
K_{NASint}	salausavain
K_{RRCenc}	salausavain
K_{RRCint}	salausavain
K_s	Key Stream, avainjono
K_{UPenc}	salausavain
LTE	Long Term Evolution, neljännen sukupolven matkapuhelinjärjestelmä
LF	Low Frequency, pientaajuus, taajuusalue 30-300 kHz
LFSR	Linear Feedback Shift Register, lineaarinen siirtorekisteri
MAC	Message Authentication Code, tarkistuskoodi
MCC	Mobile Country Code, maatunnus IMSI-koodissa
MHz	Megahertsi, taajuuden yksikkö
MME	Mobility Management Entity, hallintayksikkö LTE-järjestelmässä
MNC	Mobile Network Code, operaattorikohtainen verkkotunnus IMSI-koodissa

MS	Mobile Station, päätelaite GSM-järjestelmässä
MSC	Mobile Switching Center, mobiilikeskus
MSIN	Mobile Subscribers Identification Numer, liittymän/asiakkaan tunniste IMSI-koodissa
MT	Mobile Termination
NAS	Non-Access Stratum, protokollapino joka hallitsee ydinverkon ja päätelaitteen välistä liikennettä
Node B	Tukiasema UMTS-järjestelmässä
NSS	Network Switching Subsystem, GSM-järjestelmän ydinverkko, verkko-osa
OMC	Operations and Maintenance Center, hallinta- ja ylläpitokeskus
OMSS	Operation and Maintenance Subsystem, hallinta- ja ylläpitojärjestelmä
P-GW	Packet Gateway, reititin, huolehtii LTE-verkon yhdistämisestä ulkoverkkoon
PIN	Personal Identification Number, salasanana käytettävä tunnusluku
PKI	Public Key Infrastucture, julkisen avaimen perusrakenne
PSK	Pre-Shared key, ennalta määritelty avain langattomissa verkoissa
PSTN	Public Switched Telephone Network, piirikytkentäinen, perinteinen puhelinverkko
QoS	Quality of Service, palvelun laatu
RADIUS	Remote Authentication Dial In User Service, autentikointiprotokolla
RAND	Random, satunaisluku
RC4	Rivest Cipher 4, salausalgoritmi
RFID	Radio Frequency Identification, radiotaajuinen etätunnistus
RNC	Radio Network Conroller, radioverkko-ohjain
RNS	Radio Network Subsystem, radioverkon alijärjestelmä
RRC	Radio Resource Control, protokolla joka hallitsee päätelaitteen ja tukiaseman välistä liikennettä
S-GW	Serving Gateway, reititin, huolehtii LTE-verkon sisäisen reitityksen

SGSN	Serving GPRS Support Node, reititin joka reitittää GPRS-verkon sisällä
SIM	Subscribers Identity Module, SIM-kortti
SN	Serving Network, palveleva verkko
SNOW 3G	Jonosalain
SRES	Signed Response, kirjattu vastaus
SQN	Sequence, lukujono, järjestysnumero
TMSI	Temporary Mobile Subscriber Identity, verkon käyttäjän/liittymän tunnus, käytetään muuten pl. verkkoon kirjautuminen. Ks. IMSI
TLS	Transport Layer Security, salausprotokolla
Trivium	Jonosalain
UE	User Equipment, käyttäjän laite, päätelaite
UHF	Ultra High Frequency, mikroaaltojen taajuusalue, 0,3-3 GHz
UMTS	Universal Mobile Telecommunications System, kolmannen sukupolven matkapuhelinjärjestelmä
USIM	User Service Identity Module, käyttäjän tunnistuskortti, SIM-kortti UMTS-järjestelmässä
UTRAN	UMTS Terrestrial Radio Access Network, UMTS-järjestelmän radioverkko-osa
VLR	Visitor Location Register, vierailijarekisteri
WEP	Wired Equivalent Privacy, langattoman lähiverkon suojaustekniikka
WLAN	Wireless Local Area Network, langaton lähiverkko
WPA/WPA2	Wi-Fi Protected Access/2, langattoman lähiverkon suojaustekniikka
XMAC	Expected MAC, odotettu MAC
XOR	Exclusive or, ehdoton tai, looginen operaatio
XRES	Expected Response, odotettu vastaus

1 JOHDANTO

Tämän opinnäytetyö esittelee erilaisia langattomia järjestelmiä sekä niissä käytettyjä salaus- ja autentikointimetodeja. Koska langattomia järjestelmiä on olemassa hyvin paljon, ei niitä kaikkia voida tässä opinnäytetyössä esitellä, vaan työssä esitellään vain joitakin yleisiä järjestelmiä.

Tässä työssä käsitellään RFID-, Bluetooth-, WLAN-, GSM-, UMTS- sekä LTE-järjestelmiä. Työssä perehdytään jokaiseen järjestelmään ensin yleisellä tasolla, jotta saadaan kuva kyseisen verkon rakenteesta. Tämän jälkeen esitellään jokaisessa järjestelmässä olevat autentikointi- sekä salausmenetelmät. Työn tarkoitus on antaa lukijalle selkeä yleiskäsitys jokaisesta langattomasta järjestelmästä sekä niiden käyttämistä salaus- ja autentikointimetodeista.

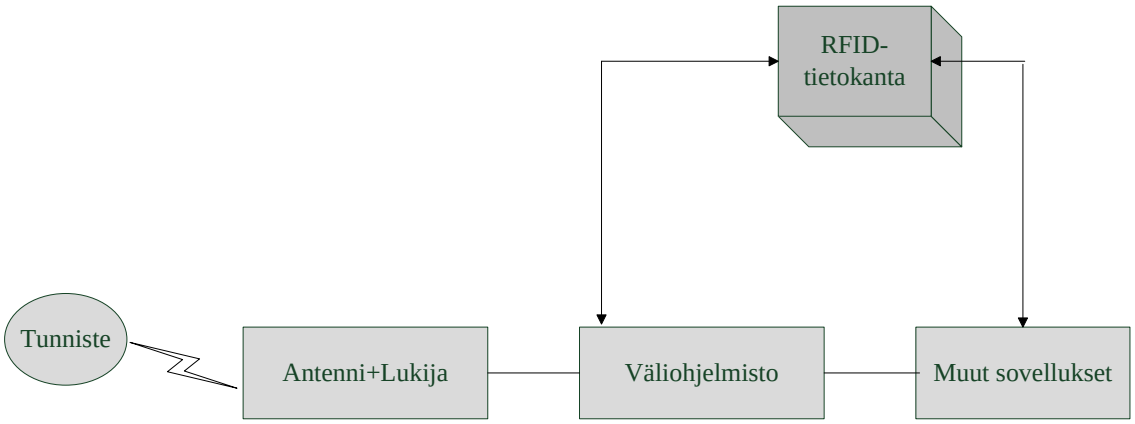
Langattomien verkkojen käyttö on lähes jokaiselle ihmiselle arkipäivää RFID-ovitunnisteiden avulla ja WLAN-verkkoihin, Bluetooth-laitteisiin, ja matkapuhelinverkkoihin kytkettyjen tietokoneiden, matkapuhelimien ja muiden päätelaitteiden kautta. Harva tulee kuitenkaan ajatelleeksi sitä, kuinka paljon erilaisia teknologioita ja protokollia verkko vaatii toimiakseen tai sitä, kuinka haavoittuvainen tietoliikenneyhteys langaton tietoverkko radioteineen on.

Tietoverkkojen turvallinen käyttö vaatii kattavan tietoturvan, alkaen verkon käyttäjien opastuksesta erilaisiin virustorjunta- ja palomuurisovelluksiin. Perinteisen, kaapeleilla rakennetun tietoverkon tiedonsiirron hallinta on suhteellisen yksinkertaista havainnollistaa, koska tietoliikenne kulkee rajoitetun alueen, kaapelin sisällä. Langattomissa verkoissa kaapelin tilalla on radiotie, eli ympäröivä ilmakehä, jonka hallinta vaatii erityisratkaisuja tietoturvan kannalta. Näihin ratkaisuihin kuuluvat myös tässä työssä esitetyt salaus- ja autentikointimetodit, joilla pyritään takaamaan luotettava tiedonsiirto.

2 RFID-TEKNIIKKA

RFID (Radio Frequency Identification) on langatonta tiedonsiirtotekniikkaa hyödyntävä tekniikka, jota käytetään esimerkiksi ihmisten ja esineiden tunnistamisessa. RFID-järjestelmä koostuu kahdesta pääosasta, tunnisteesta ja lukijasta johon on kytketty antenni. Lisäksi lukija on yleensä kytkettynä väliohjelmistoihin, tietokantoihin ja muihin sovelluksiin. Nämä komponentit mahdollistavat RFID-järjestelmän sulauttamisen esimerkiksi koko yrityksen alueelle. (Banks, Hanny, Pachano, & Thompson 2007, 6–7;Kallonen 2006, 8)

Kuvio 1 esittää RFID-järjestelmän infrastruktuurin.



Kuvio 1: RFID-järjestelmän infrastuktuuri. (Banks, ym. 2007, 8)

RFID käyttää useita eri taajuusalueita. LF-taajuusalueella järjestelmä yleensä käyttää 125 kHz taajuutta. HF-taajuusalueella käytetään 13,56 MHz taajuutta, joka on kansainvälisesti vapaa taajuus. LF- ja HF-taajuusalueella toimivien RFID-järjestelmien lukuetäisyys on pieni, joten niiden käyttö rajoittuu pienille etäisyyksille, esimerkiksi kulunvalvontaan. UHF-taajuusalueen RFID-järjestelmät toimivat Yhdysvalloissa 902-928 MHz taajuudella ja Euroopassa 869 MHz alueella. Esimerkiksi Yhdysvaltalainen kauppaketju Wal-Mart käyttää UHF-taajuusalueella toimivaa RFID-järjestelmää tuotteiden tunnistamiseen. Mikroaaltoalueella toimivat RFID-järjestelmä yleensä käyttävät 2,4 GHz taajuutta. Mikroaaltoja käyttävä RFID-järjestelmä on esimerkiksi automaattinen tunnistus tietullissa. (RFID Lab Finland ry)

Käytettävät tunnisteet jaetaan kolmeen eri luokkaan. Passiivisessa tunnisteessa ei ole omaa virtalähdettä vaan tunnisteen ja lukijan väliseen viestintään tarvittavan virran synnyttää lukija. Lukija lähettää radioaallon tunnisteelle ja radioaalto indusoi tarvittavan jännitteen ja virran tunnisteelle.

Aktiivisessa tunnisteessa on oma virtalähde (akku). Koska tunniste käyttää omaa virtalähdettä viestintään, voidaan tunnisteen ja lukijan välinen radiosignaali lähettää suuremmalla teholla ja suuremmalla kantamalla. Toisaalta taas heikkoutena on tunnisteen suuri koko sekä hinta.

Puoliaktiiviset tunnisteet ovat aktiivisen ja passiivisen tunnisteen sekoitus. Passiivinen komponentti aktivoituu kun se osuu lukijan magneettikenttään ja tämä laukaisee aktiivisen osan tunnistetta lähettämään signaalia. Etuna on huomattavasti parempi akun kesto kuin aktiivisessa tunnisteessa. (Banks, ym. 2007, 8–11)

Lukija on antennista ja mikropiiristä koostuva laite, joka lähettää ja vastaanottaa signaalit tunnisteelta. Mikropiiri sisältää vähintään mikroprosessorin, muistia sekä radiolähettimen. (Banks, ym. 2007, 11)

Väliohjelmiston tehtävä on tulkita lukijalta tulleita signaaleja ja verrata niitä tietokantaan syötettyihin tietoihin. Esimerkiksi kulunvalvonnassa voidaan tarkastaa onko kyseisellä tunnisteella pääsyä tilaan. Muut sovellukset eivät oikeastaan kuulu RFID-infrastruktuuriin vaan ovat järjestelmää laajentavia elementtejä. Muu sovellus voi olla esimerkiksi varastonhallintasovellus tai tilaustenhallintasovellus. (Banks, ym. 2007, 15–18)

2.1 Salaus ja autentikointi RFID-järjestelmässä

Monissa RFID-järjestelmissä ei ole mitään tietoturvaratkaisuja, vaan tunnisteet ja lukijat kommunikoivat keskenään ilman mitään salausta. Tähän on päädytty siksi, että vahvat salausmenetelmät vaativat korkeampaa suoritustehoa, joka johtaisi siihen, että RFID-järjestelmän hinta kasvaisi. Kun ajatellaan esimerkiksi tuotetta, jonka kate on kymmenen sentin luokkaa, ei ole loogista kiinnittää siihen 25 senttiä maksavaa RFID-tunnistetta. (Banks, ym. 2007, 273,277–278)

RFID-järjestelmien suurin yksityisyydelle aiheuttama ongelma on se, että tunnisteet voidaan lukea siten, ettei tunnisteen haltija huomaa tapahtumaa. Näin vieras henkilö voi suorittaa esimerkiksi profilointia henkilöille. Tämänkaltainen profilointi voi olla esimerkiksi sitä, että kerätään tietoa henkilön hallussa olevista tuotteista ja ostoksista jotka ovat varustettuna RFID-tunnisteella. Tätä tietoa voidaan jälkikäteen käyttää jossakin toisessa yhteydessä kohdennettujen mainosten esittämisessä. Lisäksi ihmisen sijaintia voidaan valvoa tunnisteiden avulla. (Kallonen 2006, 35–36)

Jotta profilointi ja valvonta toimisivat, täytyy olla olemassa linkki tunnisteiden sekä omistajien välillä. Toisin sanoen, profilointia ei voida suorittaa jos ei tiedetä kenen ostoksia luetaan tai yksittäisen tunnisteen seuraaminen on turhaa, jos ei tiedetä kenen hallussa tunniste on. Kohdennettuja mainoksia voidaan kuitenkin esittää ilman profilointia, henkilön mukanaan kantamien tunnisteita sisältävien tuotteiden perusteella. (Kallonen 2006, 36)

Eräs tapa suojata RFID-tunniste asiattomilta lukijoilta on laittaa se Faradayn häkkiin. Faradayn häkki on metallista valmistettu esine, joka estää sähkömagneettista säteilyä kulkemasta sen sisään tai ulkopuolelle. Tämä tekniikka vaatii kuitenkin käyttäjältä jatkuvasti toimia, koska käyttäjän täytyy poistaa ja laittaa tunniste suojaan jokaisella kerralla, kun tunnistetta luetaan. On kuitenkin joitain erityisratkaisuja, joissa Faradayn häkki on toimiva ratkaisu. Yksi esimerkki on passit, jotka sisältävät RFID-tunnisteen. Passin kansi muodostaa Faradayn häkin ja koska passi luetaan yleensä kansi auki, on näin ollen passin ja tunnisteen sisältämät tiedot muutoin suojattuna kansien sisällä. Mikäli tunniste on kiinnitettynä suureen esineeseen tai esimerkiksi ihmiseen, on todella vaikeaa sulkea tunnistetta häkkiin. Näissä tapauksissa Faradayn häkki ei sovellu suojaamaan tunnistetta. (Banks, ym. 2007, 275; Kallonen 2006, 37)

Toinen tehokas keino välttää tunnisteen asiattomat luvut on ns. tappokäsky. Lukija lähettää tunnisteelle tappokäskyn, joka myös vaatii salasanan, jolla estetään asiattomat tappokäskyt. Asianmukaisen tappokäskyn saatuaan tunniste tuhoutuu, eikä sitä enää voida havaita lukulaitteella. Tappokäsky voidaan antaa esimerkiksi kaupan kassalla tunnisteille, jotka on asennettu ostettaviin tuotteisiin. (Banks, ym. 2007, 276;Kallonen 2006, 36)

Joissakin järjestelmissä on perusteltua käyttää kalliimpia RFID-tunnisteita, jotka pystyvät suorittamaan autentikointia sekä salausta. Nämä järjestelmät ovat kalliita, esimerkiksi satoja tuhansia euroja maksavat sairaalalaitteet voivat olla yksi järjestelmä, johon on syytä asentaa kalliimpi tunniste. (Banks, ym. 2007, 278)

Tämänkaltaisessa järjestelmässä voidaan käyttää symmetristä salausta, jossa sekä lukija että tunniste käyttävät samaa salausavainta. Kun tunniste tuodaan lukijan lukuetäisyydelle, suoritetaan molemminpuolinen autentikointi. Tämä toteutetaan siten, että tunniste luo satunaisluvun R_A jonka se lähettää lukijalle. Lukija luo satunaisluvun R_B ja salaa sen, sekä tunnisteelta saamansa satunaisluvun R_A salausavaimella ja lähettää ne tunnisteelle. Tunniste purkaa salauksen ja vertaa omaa R_A lukuaan lukijan lähettämään R_A lukuun. Mikäli luvut täsmäävät, lukija on onnistuneesti autentikoitunut tunnisteelle. Kun tunniste lähettää vielä puretun R_B luvun lukijalle, joka vertaa sitä alkuperäiseen R_B lukuun ja mikäli ne täsmäävät on tunniste autentikoitunut lukijalle. (Kallonen 2006, 39)

Ongelmana symmetrisessä salauksessa on se, että tunnisteen ja lukijan on tiedettävä sama salausavain. Kun järjestelmä sisältää suuren määrän tunnisteita, on olemassa riski, että avain pystytään selvittämään. Tämä johtaisi tilanteeseen, jossa avainta voitaisiin käyttää järjestelmää vastaan. Yksi ratkaisu tähän on käyttää tunnistekohtaista avainta. Avain luodaan tunnisteen sarjanumeron perusteella käyttäen lukulaitteen salausavainta. Kun tunniste asetetaan lukulaitteen lukuetäisyydelle, ensimmäiseksi lukulaite pyytää tunnistetta lähettämään sarjanumeronsa. Sarjanumeron ja salausavaimen avulla lukija laskee tunnisteen avaimen, jota käytetään liikennöintiin tunnisteen ja lukijan välillä. Tämän jälkeen autentikointi jatkuu kuten symmetrisessäkin järjestelmässä. (Kallonen 2006, 39)

Tiedonsiirron salaukseen voidaan käyttää symmetristä tai asymmetristä salausta. Salausjärjestelmä voi olla jonosalain, jolloin jokainen merkki salataan erikseen tai lohkosalain, jolloin tieto salataan lohkoissa. RFID-järjestelmissä käytetään enimmäkseen symmetrisiä jonosalaimia. (Kallonen 2006, 40)

Esimerkiksi AES-, DES-, GRAIN- ja Trivium-salaimet ovat RFID-järjestelmässä käytettäviä symmetrisiä jonosalaimia. (Estevez-Tapiador, Hernandez-Castro, Peris-Lopez & Ribagorda 2009, 124–128)

3 BLUETOOTH-TEKNOLOGIA

Bluetooth on langaton teknologia lyhyen matkan yhteyksiin. Se suunniteltiin tarjoamaan langatonta rajapintaa erilaisten kuluttajapäätelaitteiden välille. Bluetooth-teknologian kehitys aloitettiin 1990-luvun puolessa välissä Ericsson Mobile Communicationsin toimesta, mutta myöhemmin teknologian ympärille on rakennettu Bluetooth Special Interest Group (SIG) yhteisö, jonka tehtävänä on kehittää sekä valvoa teknologian käyttöä. (Gehrmann, Persson & Smeets 2004, 3)

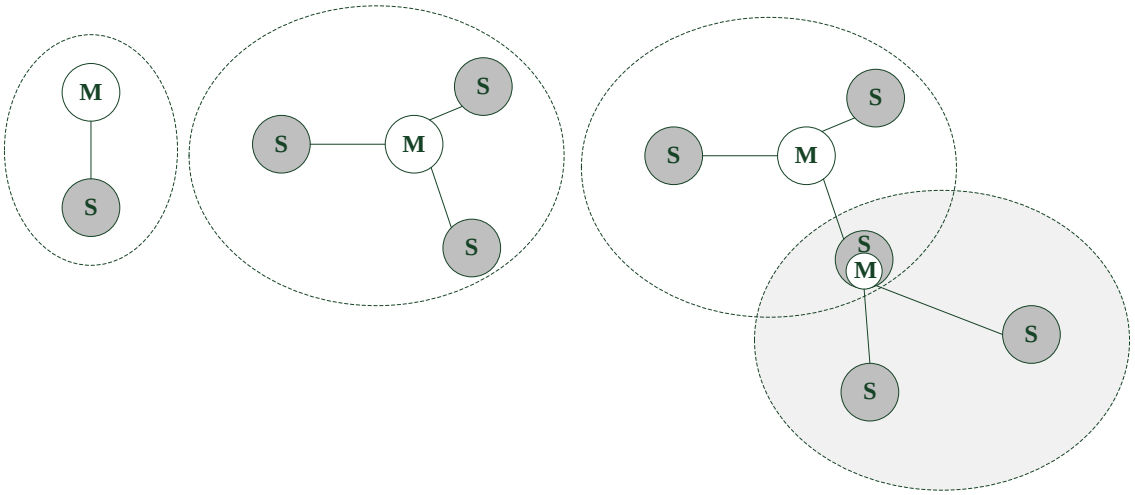
Bluetooth toimii ISM-taajuuskaistalla, 2400–2483,5 MHz:n taajuudella. Joidenkin maiden kohdalla on poikkeuksia, kuten Ranska (2446,5–2483,5 MHz) tai Espanja (2445–2475 MHz). Käytetty taajuuskaista on jaoteltu 1 MHz:n levyisiin kanaviin, jolloin kanavia muodostuu 79 kappaletta (Espanjassa ja Ranskassa 23). Bluetooth käyttää taajuushyppelyä, jossa kanavaa vaihdetaan 1600 kertaa sekunnissa. Hyppelyllä pyritään vähentämään mm. ympäristöstä aiheutuvia häiriöitä signaalissa.

Bluetooth-verkko noudattaa tähtiverkko-topologiaa, jossa voi olla enintään kahdeksan laitetta kerrallaan, muodostaen näin yhden pikoverkon. Jokaisessa verkossa on yksi keskuksena toimiva isäntälaite (master) ja enintään seitsemän renkilaitetta (slave). Jokainen laite voi toimia joko isäntä- tai renkilaitteena. Tiedonvaihto laitteiden välillä toteutetaan kaksisuuntaisena full duplex -liikenteenä, eli tieto voi kulkea samanaikaisesti molempiin suuntiin. Tämä toteutetaan aikajakoisella dupleksilla, jolloin jokaiselle päätelaitteelle on osoitettu tietty aikaikkuna, jolloin se voi lähettää dataa siirtotielle. Aikaikkunat laitteille myöntää verkon isäntälaite.

Liikennöinti on mahdollista vain isäntälaitteelta renkilaitteelle tai toisinpäin. Renkilaitteelta toiselle renkilaitteelle kulkeva liikennöinti kulkee näin ollen aina isäntälaitteen reitittämänä. Jos vain yksi laite (isäntälaite) vastaa tiedon kulusta, siitä voi muodostua verkkoon pullonkaula, joka hidastaa koko verkkoa. Siksi sama laite voi toimia yhdelle verkolle renkilaitteena ja samanaikaisesti olla toiselle verkolle isäntälaitteena. Näin yhden verkon renkilaite voikin vaihtaa itsensä myös isäntälaitteeksi uuteen pikoverkkoon, jolloin kaikkien laitteiden viestintä ei ole yhden isäntälaitteen varassa. (Gehrmann, Persson & Smeets 2004, 8–9)

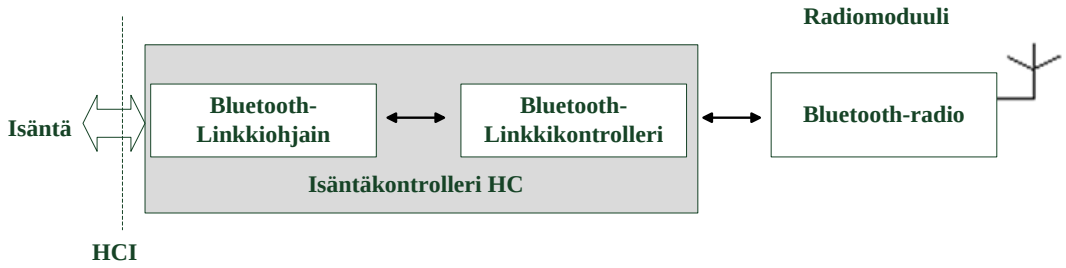
Kahden tai useamman pikoverkon muodostamaa verkkoa kutsutaan hajaverkoksi. Pikoverkot yhdistyvät toisiinsa yhdellä laitteella joka toimii verkkojen välisenä yhdyskäytävänä. Tämä laite voi toimia molemmissa verkoissa joko renkilaitteena, tai isäntälaitteena toisessa verkossa ja renkilaitteena toisessa verkossa. (Toro 2006, 7)

Kuvio 2 esittää joitakin Bluetooth-verkon topologiakuvia: kaksi pikoverkkoa sekä yhden hajaverkon joka muodostuu kahdesta pikoverkosta. Kuviossa M merkitsee isäntälaitetta ja S renkilaitetta.



Kuvio 2: Bluetooth-verkon topologiat. (Gehrmann, Persson & Smeets 2004, 9, muokattu)

SIG ei ole tarkkaan määrittänyt, mitkä Bluetooth-laitteiden osat pitää toteuttaa ohjelmatasolla ja mitkä osat laitteistotasolla. Järjestelmä voidaan mallintaa kahtena toiminnallisena osana: radiomoduulina sekä linkkimoduulina eli linkkikontrollerina. Radiomoduuli vastaa radiosignaalien lähetyksestä. Linkkikontrolleri on yhteydessä ohjelmistopohjaisen linkkiohjaimen LM:n kanssa. Näiden muodostamaa kokonaisuutta kutsutaan nimellä isäntäkontrolleri HC. Linkkikontrollerin tehtävänä on prosessoida kantataajuussignaalia sekä suorittaa fyysisen tason protokollien koodaus. Linkkiohjain vastaa erilaisista protokollista sekä joistakin alhaisen linkkitason toiminnoista kuten datan lähetys ja vastaanotto, yhteyksien muodostaminen, virheiden havaitseminen sekä niiden korjaus sekä autentikointi. Isäntäkontrolleri vastaa taajuushyppelyssä käytettävästä hyppyjärjestyksestä. Kuvio 3 esittää Bluetooth-järjestelmän linkki- sekä radiomoduulin.



Kuvio 3: Bluetooth-järjestelmän linkki- sekä radiomoduuli. (Helsinki University of Technology 2002, 46)

3.1 Salaus ja autentikointi Bluetooth-järjestelmässä

Bluetooth-järjestelmässä käytettävä lähetystekniikan luo jo itsessään hyvän perustan tietoturvalle. Käytettävä taajuushyppely vaikeuttaa lähetysten salakuuntelua sekä niiden häiritsemistä. Lisäksi Bluetooth-verkkojen lyhyet kantamat pitävät verkon liikennöinnin hyvin pienen alueen sisäpuolella. (Helsinki University of Technology 2002, 54)

Bluetooth-järjestelmälle on luotu useita eri profiileja, joista tässä työssä käsitellään GAP-profiilia, koska se on kaikkein yleisin ja monet muut profiilit pohjautuvat siihen. (Opel, Otto-von-Guericke University of Magdeburg, 2003)

Bluetooth-laite sisältää neljä erilaista merkkijonoa, joita käytetään luotaessa luotettavaa linkkitason tietoturvaa Bluetooth-verkossa. Niitä ovat 48-bittinen Bluetooth-laiteosoite BD_ADDR, joka on jokaiselle Bluetooth-laitteelle uniikki osoite, jonka IEEE määrittelee. Lisäksi autentikoinnin yhteydessä käytetään 128-bittistä linkkiavainta. Linkkiavaimesta johdetaan 8-128 -bittinen salausavain, jota käytetään salauksen luomisessa. Lisäksi käytetään 128-bittistä satunaislukua RAND. Lisäksi käyttäjä voi asettaa PIN-koodin, jonka avulla laitteet voivat tunnistaa toisensa. (Helsinki University of Technology 2002, 54;Opel, Otto-von-Guericke University of Magdeburg, 2003)

GAP-profiilissa on määritelty kolme erilaista tietoturvan tasoa. 1. taso on ei suojausta, eli tällä tasolla yhteyttä muodostettaessa eivät laitteet suorita mitään tietoturvaoperaatioita ja verkko on suojaamaton.

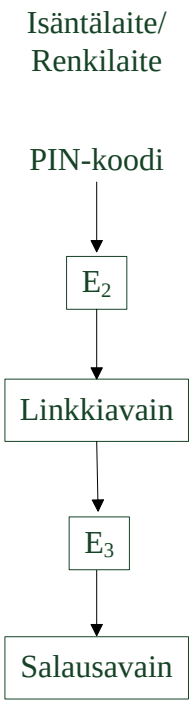
2. tasolla suojaus on palvelutason suojaus, jossa yhteyden suojaus suoritetaan vasta yhteyden muodostamisen jälkeen. Tällä tasolla on kolme erilaista toimenpidettä suojata yhteyttä. Näiden käyttöönotto riippuu vaaditusta tietoturvan tasosta. Taulukossa 1 esitetään nämä toimenpiteet. (Opel, Otto-von-Guericke University of Magdeburg, 2003)

Taulukko 1: Tietoturvatason 2 toimenpiteet. (Opel, Otto-von-Guericke University of Magdeburg, 2003)

Toimenpiteen nimi	**Toiminta**
Lupa/valtuutus	Yhdistäminen sallitaan automaattisesti luotetuille laitteille, joiden tiedot ovat tallennettuna tietokantaan. Muille laitteille pääsy sallitaan tunnistautumisen jälkeen.
Autentikointi	Ennen kuin yhteys sovellukseen voidaan muodostaa, pitää yhteyttä ottavan laitteen autentikoida itsensä.
Salaus	Ennen kuin palvelun käyttö on mahdollista, yhteys täytyy salata.

3. tasolla suoritetaan linkkitason tietoturva. Tässä Bluetooth-laitteet suorittavat tietoturvatoimenpiteet jo ennen, kuin yhteyskanavaa on muodostettu. Tämä ominaisuus on laitteisiin sisäänrakennettu, jolloin se ei ole riippuvainen mahdollisista sovellustason tietoturvatoimenpiteistä. Taso tukee sekä autentikointia, että salausta ja nämä perustuvat jaettuun linkkiavaimeen. (Imai 2005, 80)

Ennen kuin Bluetooth-laitteet voivat kommunikoida keskenään, täytyy niiden välinen yhteys alustaa. Tämän alustusvaiheen aikana luodaan linkkiavaimet. Linkkiavaimet johdetaan käyttäjän syöttämistä PIN-koodista, joka syötetään molempiin laitteisiin. Kun yhteys on alustettu, laitteet suorittavat automaattisesti autentikoinnin sekä yhteyden salauksen. Autentikointiin käytettävä linkkiavain johdetaan PIN-koodista E_2-algoritmilla ja salausavain johdetaan linkkiavaimesta E_3-algoritmilla. Kuviossa 4 esitetään PIN-koodin syötön jälkeen toteutettavat toimenpiteet. (Imai 2005, 80–81)



Kuvio 4: Linkkiavaimen ja salausavaimen luominen isäntä- ja renkilaitteessa. (Imai 2005, 81, muokattu)

Linkkiavaimena voidaan käyttää myös muita avaimia, riippuen käytettävästä sovelluksesta. Näitä ovat yksikköavain, yhdistelmäavain, isäntäavain ja alustusavain.

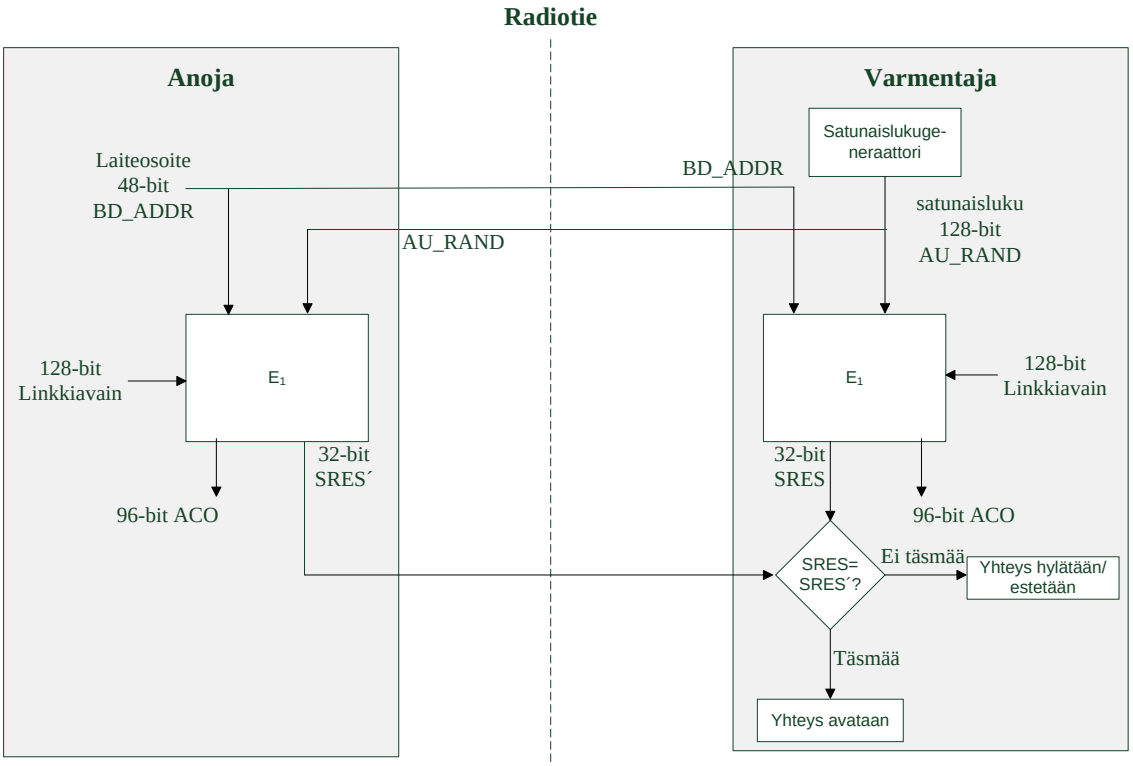
Alustusavainta käytetään kun kaksi toisilleen ennalta tuntematonta laitetta muodostavat yhteyttä. Avain johdetaan yhteyden alustusvaiheessa syötettävästä PIN-koodista, yhteyttä pyytävän laitteen Bluetooth-laiteosoitteesta BD_ADDR sekä satunaisluvusta RAND, E_{22}-algoritmilla. Tuloksena saadaan 128-bittinen alustusavain, jota käytetään avaintenvaihdossa, linkkiavainta luotaessa. Kun vaihto on suoritettu, alustusavain tuhotaan.

Yksikköavain luodaan E_{21}-algoritmin avulla, kun Bluetooth-laitetta käytetään ensimmäistä kertaa. Kun avain on luotu, se tallennetaan laitteen pysyvään muistiin ja sitä harvoin muutetaan. Toinen laite voi käyttää toisen laitteen yksikköavainta linkkiavaimena näiden laitteiden välisessä liikennöinnissä. Yhteyden alustusvaiheessa suoritetaan päätös siitä, kumman osapuolen yksikköavainta käytetään linkkiavaimena.

Yhdistelmäavain luodaan molemmissa laitteissa yhteyden alustusvaiheessa, mikäli laitteisiin on määritelty tämä vaadittavaksi. Avain luodaan E_{21}-algoritmilla, jolle syötteenä annetaan Bluetooth-laiteosoite sekä satunaisluku. Tämän jälkeen laitteet lähettävät toisilleen luodut satunaisluvut ja laskevat yhteydessä käytettävän yhdistelmäavaimen.

Isäntäavain on tilapäinen avain, jonka avulla isäntälaite suorittaa koko verkon salaustoimenpiteet. Isäntäavainta käytetään tilanteissa, joissa isäntälaite lähettää samaa viestiä usealle renkilaitteelle. Avain luodaan käyttäen kahta 128-bittistä satunaislukua sekä E_{22}-algoritmia. Kolmas satunaisluku lähetetään renkilaitteelle, joka käyttää satunaislukua ja linkkiavainta syötteenä E_{22}-algoritmiin. Tämän jälkeen isäntälaite lähettää XOR-operaatiolla lasketun luvun sekä uuden linkkiavaimen renkilaitteelle. Tämä toimenpide suoritetaan jokaisen renkilaitteen kanssa, joissa isäntäavainta halutaan käyttää. (Imai 2005, 82–83; Pitkämäki, Tampereen Teknillinen Yliopisto, 7–8)

Autentikointi Bluetooth-järjestelmissä perustuu haaste-vastaus-menettelyyn. Autentikoinnin osapuolia kutsutaan anojaksi ja varmentajaksi. Anojan tehtävänä on tunnistautua varmentajalle. Kuvio 5 esittää haaste-vastaus-menettelyn.

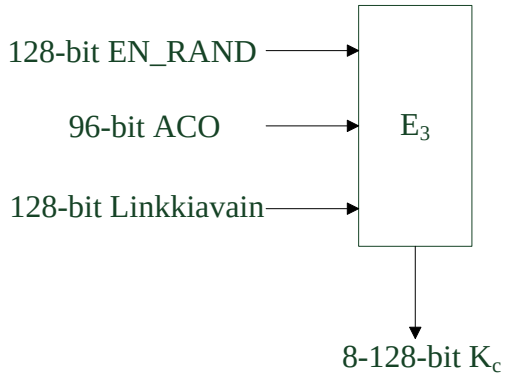


Kuvio 5: Haaste-vaste-menettely Bluetooth-järjestelmän autentikoinnissa. (Imai 2005, 84)

Autentikointitapahtuma alkaa sillä, että anojalaite lähettää Bluetooth-laiteosoitteensa varmentajalle ja varmentaja lähettää anojalle haasteen, satunaisluvun AU_RAND. Varmentaja laskee anojan laiteosoitteesta, satunaisluvusta sekä linkkiavaimesta E_1-algoritmilla vastauksen. Saman toimenpiteen suorittaa myös anoja, joka lähettää varmentajalle oman vastauksensa. Varmentaja vertailee omaa vastaustaan anojan vastauk-

seen ja mikäli ne täsmäävät, voidaan yhteys avata. Samassa yhteydessä 96-bittinen merkkijono ACO tallennetaan. Tätä merkkijonoa käytetään myöhemmin salauksen luomisessa. Jos autentikointi epäonnistuu, laitteet odottavat tietyn aikavälin ajan, ennen kuin autentikointia voidaan yrittää uudelleen. Tämä aikaväli kasvaa eksponentiaalisesti epäonnistuneiden autentikointikertojen mukaisesti.(Imai 2005, 84–85)

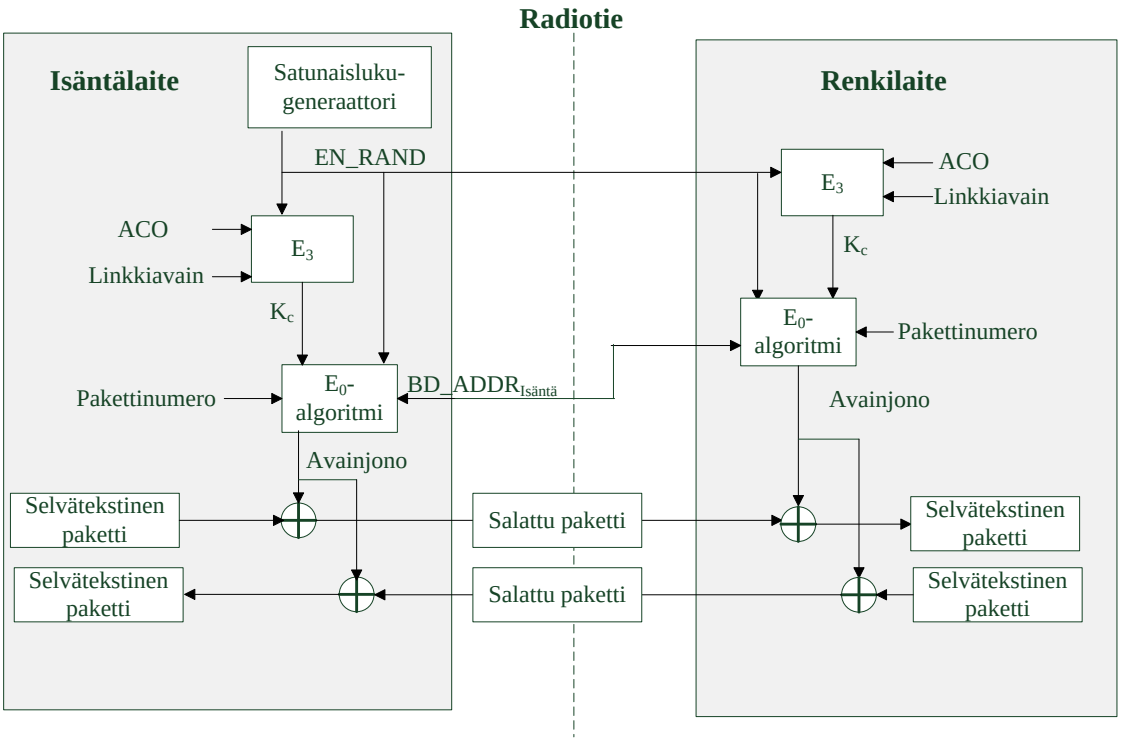
Bluetoothin salaus pohjautuu jonosalaimeen E_0. Salaimen tuottama avainjono yhdistetään selkokieliseen viestiin XOR-operaation avulla ja lähetetään radiotietä pitkin vastaanottajalle. Avainjono muodostetaan lineaarisiin siirtorekistereihin (LFSR) pohjautuvalla algoritmilla. Syötteinä salaimelle toimii isäntälaitteen Bluetooth-laiteosoite BD_ADDR, satunaisluku EN_RAND, pakettinumero (slot number) ja salausavainta K_c. Koska pakettinumero muuttuu jokaisen paketin kohdalla, salausjono muuttuu jokaisen paketin kohdalla. Salausavain K_c muodostuu satunaisluvusta EN_RAND, autentikaation yhteydessä muodostetusta ACO-merkkijonosta sekä linkkiavaimesta E_3-algoritmilla, kuvion 6 mukaisesti.(Imai 2005, 85–86)



Kuvio 6: Salausavaimen luominen Bluetooth-järjestelmässä. (Opel, Otto-von-Guericke University of Magdeburg, 2003)

Kuten kuviossa 6 esitetään, salausavaimen K_c pituus voi olla väliltä 8-128 -bittiä, riippuen vaaditusta tietoturvan tasosta. Avaimen pituus neuvotellaan isäntälaitteen ja renkilaitteen välillä. Samalla määritellään salauksen taso. Tasoja on kolme, joista ensimmäisellä ei salausta suoriteta. Toisella tasolla sallitaan yleislähetysten kulkeminen salaamattomana, mutta yksittäiset lähetykset salataan. Kolmannella tasolla kaikki lähetykset salataan.

Kuvio 7 esittää salauksen toiminnallisen kuvauksen isäntälaitteen ja renkilaitteen välillä.



Kuvio 7: Salaus Bluetooth-verkossa isäntä- ja renkilaitteen välillä. (Imai 2005, 87, muokattu)

4 WLAN-VERKOT

WLAN (Wireless Local Area Network), on langaton lähiverkkotekniikka joka perustuu IEEE:n määrittelemään standardiin IEEE 802.11 jota jälkeenpäin on kehitetty eteenpäin useilla eri versiolla (IEEE 802.11 a, b, d, e, g, h, i, j, n). Alun perin WLAN-tekniikka toimi 2,4 GHz taajuudella, mutta tekniikan kehittyessä käytettäväksi on tullut myös 5 GHz taajuus. (Korowajczuk 2011, 312–313)

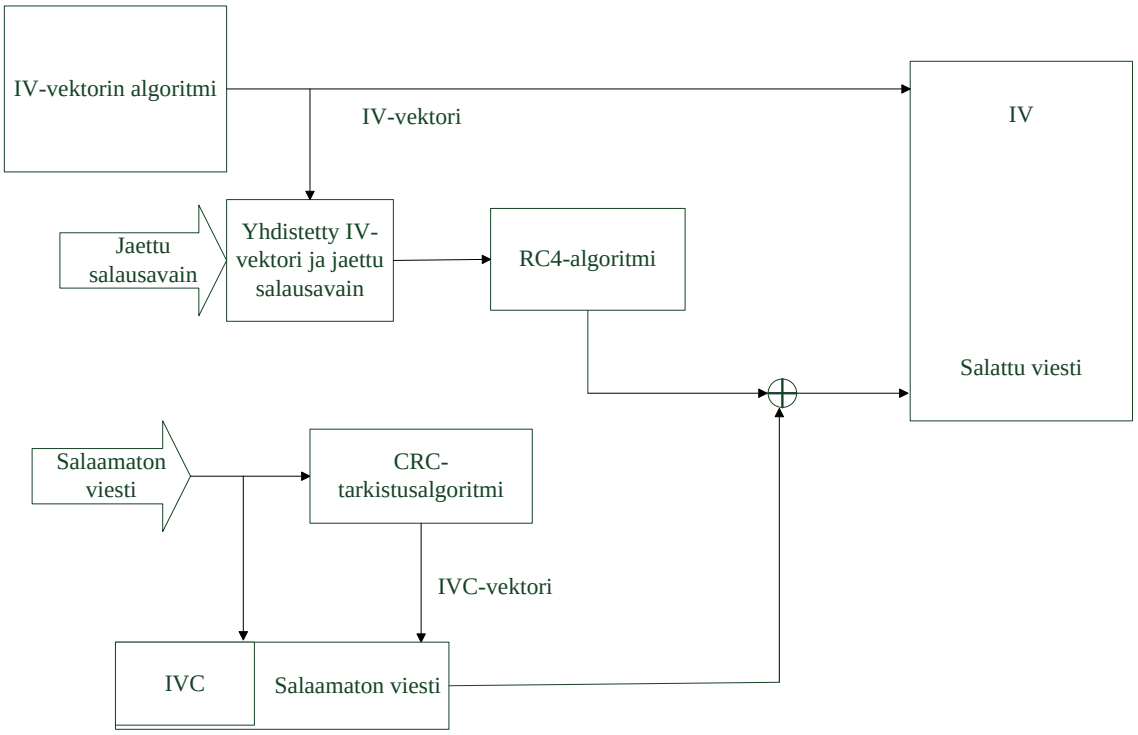
Langattomien lähiverkkojen määrä on kasvanut suureksi, koska langattomuus tuo etuja mukanaan, esimerkiksi edullisuus, joustavuus ja kaapeloinnin määrän vähentäminen. Langattomuus tuo kuitenkin mukanaan myös kasvavan tietoturvauhan ja tarpeen luotettaville tietoturvaratkaisuille. (Prasad & Prasad 2005, 2–5, 95)

4.1 WEP-suojaus

Langattomien lähiverkkojen salaukseen ja autentikointiin kehitettiin ensimmäisenä WEP (Wired Equivalent Privacy)-suojaus, jonka tarkoituksena oli luoda langattomista lähiverkoista yhtä turvallisia käyttää, kuin langallisistakin lähiverkoista. (Subramanian, Gonsalves & Rani 2010, 591)

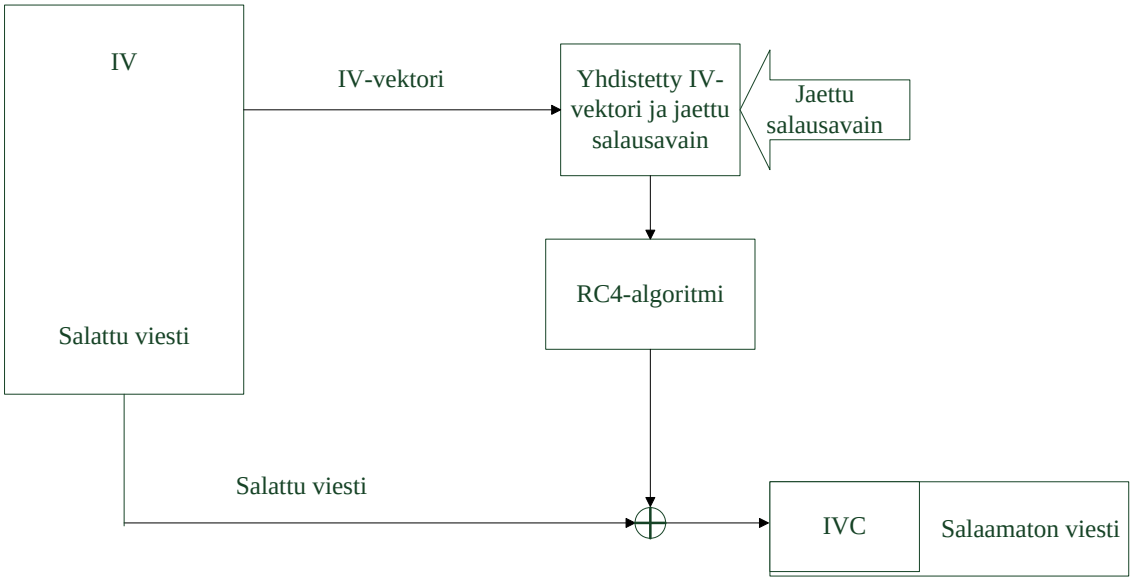
WEP on symmetrinen salausalgoritmi, jossa samaa salausavainta käytetään sekä viestin salaamisessa, että salatun viestin purkamisessa jälleen selkotekstiseen muotoon. WEP käyttää salaukseen RC4-algoritmia, jonka käyttämän salausavaimen pituus voi olla joko 40- tai 104-bittiä. Lisäksi salauksessa käytetään 24-bittistä alustusvektoria IV (Initialization Vector) ja salaamattomasta viestistä CRC-algoritmilla luotua, 32-bittistä tarkistusvektoria ICV (Integrity Check Value). (Imai 2005, 67–68; Wireless Computing)

Kuten kuviosta 8 voidaan nähdä, lähetettävä paketti koostuu salaamattomassa muodossa olevasta aloitusvektorista IV, sekä salatusta viestistä, joka on muodostettu XOR-operaation avulla, käyttäen salausavainta, IV- sekä ICV-vektoreita sekä salaamatonta, alkuperäistä viestiä.



Kuvio 8: WEP-salausprosessi. (Imai 2010, 67)

Salatun viestin purkaminen vastaanottajalla tapahtuu kuvion 9 mukaisesti, käyttäen samaa jaettua salausavainta, sekä salaamattomana lähetettyä IV-vektoria.



Kuvio 9: WEP-salauksen purkamisprosessi. (Wireless Computing)

WEP-salauksessa käytetään ICV-vektoria varmistamaan datan eheys, eli se, ettei data ole muuttunut tiedonsiirron aikana. IV-vektoria käytetään vahventamaan jaettua avainta sekä tuottamaan erilaisen RC4-jonon jokaiselle paketille, joka lähetetään. Molemmissa

näissä vektoreissa on kriittisiä ongelmia, jotka johtavat siihen, että WEP-salaus sisältää vakavia tietoturvauhkia. (Imai 2005, 70)

WEP-salausavaimet ovat staattisia, joten verkon ylläpitäjän on määritettävä kuinka avaimia hallinnoidaan ja vaihdetaan. Avainten vaihtaminen on tehtävä manuaalisesti, joka voi olla erittäin vaikeaa suurissa verkoissa. (Wireless Computing)

Alustusvektori IV, lähetetään salaamattomana, kuten kuvioista 8 sekä 9 voidaan päätellä. Lisäksi koska vektorin pituus on vain 24-bittiä, samaa vektoria käytetään liikennöinnissä, ellei jaettua avainta vaihdeta erittäin usein. Hyökkääjä voi kaapata kaksi pakettia, jotka ovat salattu samalla avaimella, jolloin hyökkääjällä on mahdollisuus purkaa salaus ja saada selville käytettävät salausavaimet. (Imai 2005, 70–71).

Imain (2005, 71) mukaan, jos saadaan kaapattua kaksi pakettia, jotka on salattu samalla avaimella, voidaan salattu viesti purkaa ja saada selville alkuperäinen sisältö yhtälöllä 1. Yhtälössä C_1 ja C_2 ovat salattuja viestejä, joilla on sama salausavain K, mutta eri sisällöt M_1 ja M_2.

$$C_1 = M_1 \oplus K \quad (1)$$
$$C_2 = M_2 \oplus K$$
$$C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K)$$
$$= (M_1 \oplus M_2) \oplus (K \oplus K)$$
$$= (M_1 \oplus M_2)\ [\, Koska\ (K \oplus K) = 0]$$

Yhtälön 1 avulla hyökkääjä saa selville kahden viestin XOR-operaation ja yksinkertaisen satunaisalgoritmin avulla voi päästä käsiksi alkuperäiseen, salaamattomaan viestiin sekä salausavaimiin. (Imai 2005, 71)

Autentikointiin on WEP:iin käytössä kaksi tapaa, avoin- ja jaetun avaimen -autentikointi. Oletuksena järjestelmässä on avoin-autentikointi, joka on tietoturvan kannalta heikko, koska se ei sisällä salausmetodeita. Kuka tahansa voi liittyä verkkoon, jossa avointa autentikointia käytetään. Jaetun avaimen autentikoinnissa sekä WLAN-tukiasemalle, että päätelaitteelle (esim. PC), täytyy asettaa sama, jaettu WEP-salausavain. Kun päätelaiteella yritetään saada yhteyttä WLAN-verkkoon, tukiasema

lähettää päätelaitteelle haasteen, johon se vastaa. Mikäli vastaus on oikein, pääsee päätelaite liittymään verkkoon. (Wireless Computing)

4.2 WPA-salaus

WPA-salaus kehitettiin korjaamaan WEP-salauksessa olevia tietoturva-aukkoja, puutteita sekä autentikaation parantamiseksi. WPA-salaus perustuu vahvaan TKIP-salaukseen (Temporal Key Integrity Protocol) ja tarkistusalgoritmiin MIC (Message Integrity Check). WPA tarjoaa myös vastavuoroisen autentikaation mahdollisuuden, joko EAP-protokollalla tai PSK-teknologialla. Oikein konfiguroituna WPA tarjoaa korkean tason tietoturvaa käyttäjilleen sekä verkolle. (Wi-Fi Alliance 2005, 5)

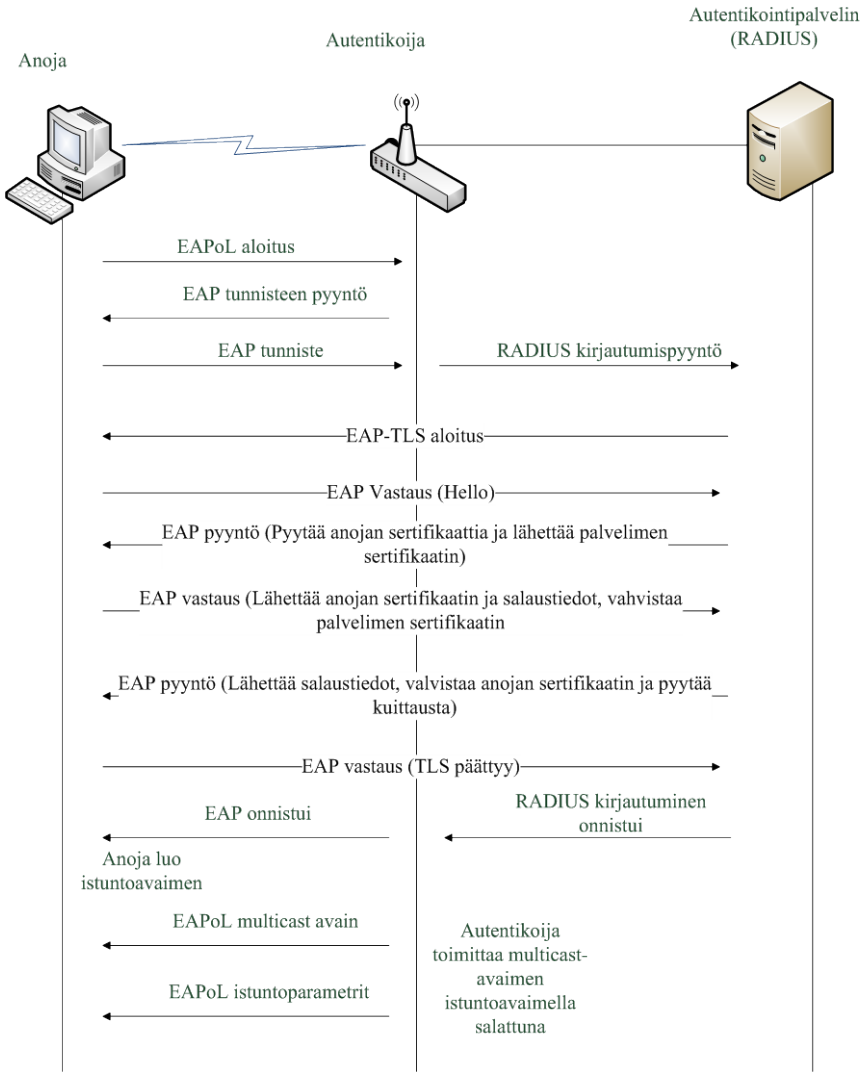
Kuten WEP-salaus, myös WPA käyttää RC4-algoritmia sekä IV-alustusvektoria, tosin WPA:ssa sen pituus on 48-bittiä. TKIP-avain kasvatti salausavaimen pituuden 128-bittiseksi, sekä mahdollisti salausavaimen dynaamisen vaihdon. Salausavaimen vaihtotiheydeksi voidaan määrittää pakettimäärä väliltä 1-10000, riippuen halutun tietoturvan tasosta. Dynaaminen salausavain kasvatti tietoturvaa, koska erilaisia avainvariaatioita voidaan muodostaa 280 biljoonaa. (Rackley 2007, 213)

TKIP-salauksessa käytettävä MIC-tarkistusalgoritmi tarkistaa onko hyökkääjä kaapannut, muokannut tai välittänyt paketteja. Tarkastus suoritetaan siten, että sekä lähettäjä että vastaanottaja suorittavat jokaisen paketin kohdalla matemaattisen laskutoimituksen. Jos vastaanottajan laskema MIC ei vastaa vastaanotetun paketin sisällä olevaa MIC:n arvoa, paketti tuhotaan ja vastatoimiin ryhdytään. Vastatoimet voivat olla salausavaimen uudelleenasetus, avaimen vaihtotiheyden kasvattaminen ja verkon ylläpitäjälle hälyttäminen. (Rackley 2007, 213–214)

EAP-autentikatiossa käytetään kolmea eri osaa. 1. Anoja, yleensä PC tai jokin muu päätelaite, 2. Autentikoija, tässä tapauksessa WLAN-tukiasema sekä 3. Autentikaatiopalvelin. Autentikaatiopalvelimella toimii esimerkiksi RADIUS- tai KERBEROS-palvelu. EAP-autentikaatiosta WLAN- sekä LAN-ympäristössä käytetään nimitystä EAPoL (EAP over LAN)(Chandra 2005, 183–184; Rackley 2007, 215)

Yksi EAP-autentikaatiomuoto on EAP-TLS, joka käyttää sertifiointipohjaista autentikaatiota asiakkaan (päätelaite) ja autentikaatiopalvelimen välillä. Sekä palvelin ja päätelaite vaihtavat keskenään digitaalisia allekirjoituksia. Tätä autentikointimallia kutsutaan nimellä PKI (Public Key Infrastucture). (Rackley 2007, 217)

Kuvio 10 havainnollistaa EAP-TLS-autentikaatiotapahtuman kulkua.



Kuvio 10: EAP-TLS-autentikaatiotapahtuman kulku. (Rackley 2007, 218)

4.3 WPA2-salaus

Kuten WPA, myös WPA2 tukee autentikointimetodeina EAP- sekä PSK-käytäntöjä. Salauksena WPA2 käyttää AES-standardiin perustuvaa CCMP-protokollaa (Counter Mode/CBC-MAC Protocol). AES mahdollistaa salausavaimen, jonka pituus voi olla joko 128-, 192- tai 256-bittiä. AES salaus sisältää 4 vaihetta, jotka muodostavan yhden

kierroksen. Kierros toistetaan joko 10, 12 tai 14 kertaa, riippuen salausavaimen pituudesta. AES-standardi nähdään erittäin turvallisena, josta kertoo myös se, että Yhdysvaltain hallitus käyttää sitä. AES:lle ei ole tunnettuja hyökkäysmetodeja ja analyysien perusteella vaadittaisiin 2^{120} operaatiota jotta AES avain voitaisiin murtaa. (Wi-Fi Alliance 2005, 5,10)

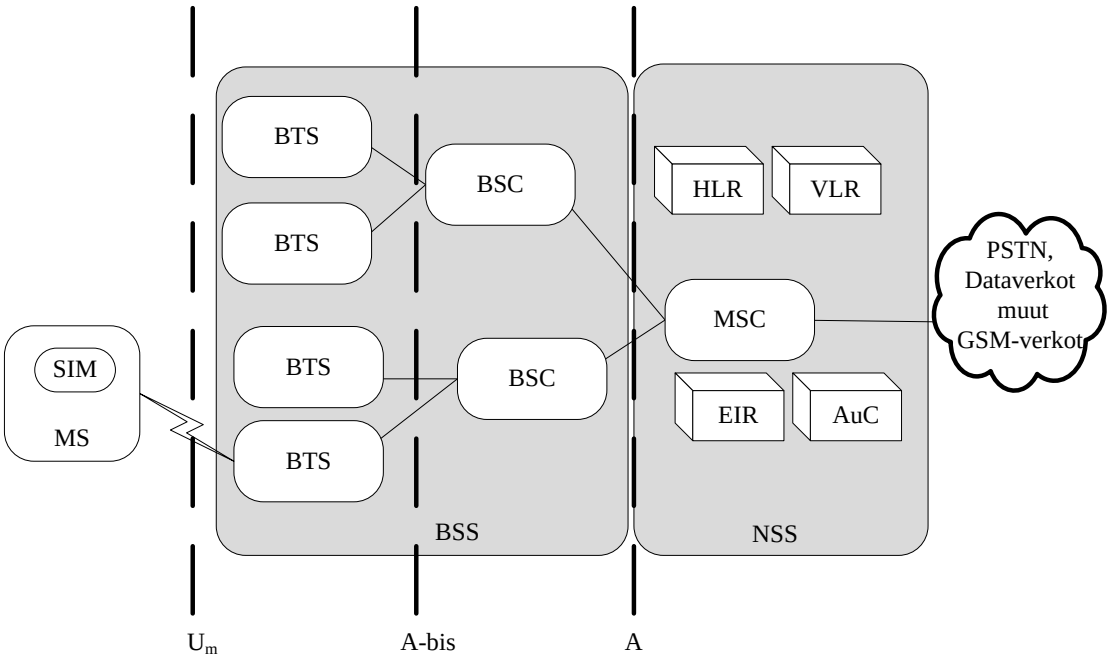
5 2G - GSM-VERKKO

Toisen sukupolven matkapuhelinverkkoa, GSM-verkkoa alettiin kehittää vuonna 1982, Groupe Special Mobile -työryhmän toimesta ja myöhemmin jatkettiin ETSI-organisaation toimesta. GSM-järjestelmä kehitettiin korvaamaan jokaisen maan kehittämän, kansalliset matkapuhelinverkot, jotka olivat keskenään epäyhteensopivia. (Imai 2005,92)

GSM-verkko voidaan jakaa kolmeen eri osaan. Ensimmäinen osa koostuu päätelaitteesta MS, joka kulkee henkilön mukana. Toinen osa, eli tukiasemajärjestelmä BSS hallitsee radiolinkit päätelaitteen MS ja kolmannen osan, verkko-osan NSS välillä. Lisäksi verkon toimintaan oleellisesti liittyy käyttö- ja kunnossapitokeskus OMC, joka valvoo verkon toimintaa ja suorittaa vaadittavat ylläpitotoimet. (Imai 2005, 93)

GSM-verkko voidaan jaotella osiin myös seuraavasti: radioliityntäverkko BSS, ydinverkko NSS sekä hallintaverkko OMSS. (Eberspächer, Bettstetter, Hartmann & Vögel 2009, 44)

Kuviossa 11 havainnollistetaan GSM-matkapuhelinverkon rakennetta lohkokaavion avulla. Katkoviivoilla merkityt kohdat kuvaavat verkon rajapintoja.



Kuvio 11: GSM-matkapuhelinverkon arkkitehtuuri. (Imai 2005, 94; GSM For Dummies)

Kuviossa 11 MS sisältää päätelaitteen (terminaali) sekä älykortin SIM (subscribers identity module). SIM-kortti tarjoaa käyttäjille liikkuvuutta, koska käyttäjä voi kirjautua verkkoon millä tahansa terminaalilla. Terminaali sisältää myös laitteen yksilöllisen tunnisteen, IMEI-koodin (International Mobile Equipment Identity). (Imai 2005, 94).
MS yhdistää tukiasemajärjestelmään BSS ilmarajapinnan U_m kautta. (GSM For Dummies)

Tukiasemajärjestelmä BSS koostuu kahdesta eri osasta, lähetin-vastaanotintukiasemasta BTS sekä tukiasemaohjaimesta BSC. Nämä viestivät keskenään standardoidun Abis-rajapinnan kautta. Koska Abis-rajapinta on standardoitu, se sallii eri valmistajien valmistamien komponenttien käytön samassa verkossa. (Imai 2005, 94)

BTS sisältää lähetin- ja vastaanotinlaitteiston ja se määrittelee solut sekä huolehtii radiolinkkiprotokollista MS:n kanssa. BSC sisältää tiedot radiokanavien kanavajaosta, kanavien asetuksista, taajuushypyistä sekä kanavanvaihdoista. BSC voi ohjata yhtä, tai useampaa tukiasemaa. BTS ja BSC yhdessä muodostavat radioliityntäverkon. (Eberspächer, ym. 2009, 43; Imai 2005, 94)

Verkko-osan NSS keskeisin osa on MSC. Se toimii kytkimenä, joka hoitaa datan edelleenlähetyksen sekä palveluominaisuuksien hallinnan ja on yhdistettynä kiinteään puhe-

linverkkoon, muuhun dataverkkoon ja/tai muihin GSM-verkkoihin. Se myös hallitsee matkaviestintilaajan rekisteröinnin, autentikoinnin, paikkatietojen päivityksen, kanavanvaihdot, puheluiden reitityksen sekä verkkovierailupuhelut (roaming). (Eberspächer, ym. 2009, 43; Imai 2005, 95)

5.1 GSM-verkon tietokannat

GSM-verkko sisältää myös useita erityyppisiä tietokantoja, jotka sijaitsevan verkon NSS-osassa. Näillä jokaisella on oma tehtävänsä, joita tässä kappaleessa käsitellään.

Kotirekisteri HLR sisältää hallinnollista tietoa jokaisesta kyseisen matkapuhelinverkon asiakkaasta ja liittymästä. Tiedot sisältävät mm. IMSI-numeron. Lisäksi HLR sisältää päätelaitteen kulloisenkin sijaintitiedon. (Imai 2005, 95; GSM For Dummies)

Vierasrekisteri VLR sisältää samat tiedot kuin kotirekisteri HLR, mutta sillä poikkeuksella että vierailijarekisterissä on kulloinkin kyseisen matkapuhelinverkon alueella olevien päätelaitteiden tiedot, jotka saadaan sekä päätelaitteelta, että vierailijan omasta HLR:stä. VLR ja HLR yhdessä MSC:n kanssa hallitsevat puheluiden reitityksen oikeaan päätelaitteeseen. (Imai 2005, 95)

EIR on laitetunnusrekisteri, johon tallennetaan laitetietoja ns. mustan listan päätelaitteista ja niiden IMEI-tunnuksista. EIR sisältää erilaisia kategorioita. Valkoiselle listalle pääsevät kaikki laitteet. Harmaalle listalle joutuvat laitteet, joiden toiminnalle operaattori on halunnut asettaa joitakin rajoituksia. Mustalle listalle listataan mm. varastetuksi tulleet matkapuhelimet. Listalla olevat päätelaitteet eivät pääse liittymään verkkoon.

AuC on tietokanta, joka sisältää parametreja sekä salausavaimen, joita käytetään autentikointiin sekä tiedonsiirron salaamiseen. (Imai 2005, 95–96; Eberspächer, ym. 2009, 46)

5.2 Salaus ja autentikointi GSM-järjestelmässä

GSM-järjestelmän suojaamisen tavoitteena oli tehdä järjestelmästä yhtä turvallinen, kuin lankapuhelinverkostakin ja estää puhelinkloonit. GSM-verkon tietoturva sisältää seuraavat näkökulmat:

- Asiakkaan/liittymän identiteetin varmentaminen
- Tiedon luotettavuus
- Asiakkaan/liittymän identiteetin luotettavuus

(Imai 2005, 96)

IMEI-koodin (International Mobile Station Equipment Identity) avulla tunnistetaan jokainen päätelaite yksilöllisesti. Siitä voidaan päätelaitteen valmistusmaa, valmistaja ja valmistuspäivä. EIR-tietokantaan vertailemalla, verkko voi päätellä onko laite, joka pyrkii liittymään verkkoon joko sallittu päästää verkkoon, tai onko se vanhentunut, varastettu tai muuten toimimaton verkossa ja täten estää sen pääsy verkkoon. (Eberspächer, ym. 2009, 46)

IMSI (International Mobile Subscriber Identity) on tunnus, joka yksilöi liittymän/asiakkaan. IMSI on tallennettuna SIM-kortille sekä AuC-tietokantaan. Se on enimmillään 15 desimaalilukua pitkä, ja koostuu kolmesta osasta:

- MCC (Mobile Country Code), kolme desimaalilukua, kansainvälisesti standardisoitu maatunnus
- MNC (Mobile Network Code), kaksi desimaalilukua, verkkotunnus, jokaisella operaattorilla on omansa
- MSIN (Mobile Subscriber Identification Number), enimmillään 10 desimaalilukua, identifioi liittymän/asiakkaan operaattorille.

(Eberspächer, ym. 2009, 47)

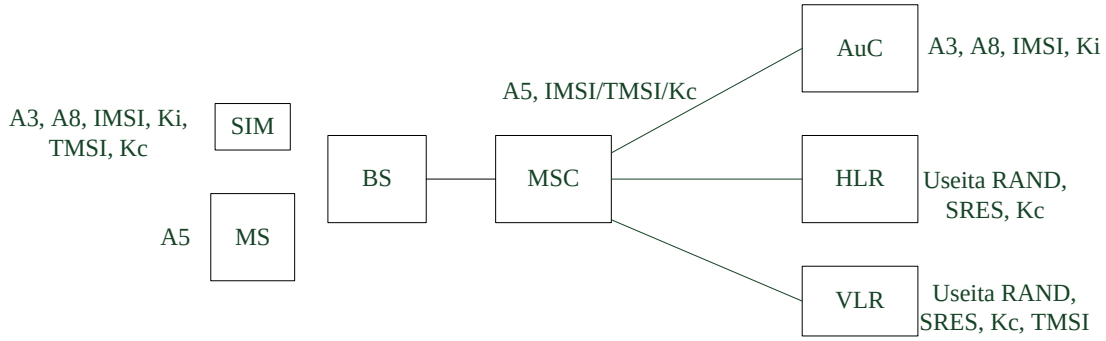
Liittymän/asiakkaan identifiointiin käytetään IMSI:n lisäksi 128-bittinen autentikaatioavainta K_i joka myös sijaitsee SIM-kortilla sekä AuC-tietokannassa. Kun päätelaite on kirjautunut GSM-verkkoon onnistuneesti, VLR korvaa IMSI-numeron TMSI-numerolla (Temporary Mobile Subscriber Identity), joka vaihtuu periodisesti, esimerkiksi kanavanvaihtojen yhteydessä. Näin lisätään tietoturvaa, kun liikennöintiin verkossa ei käytetä käyttäjän suoraa IMSI-numeroa vaan korvataan se tilapäisellä tunnuksella, joka vain

viittaa alkuperäiseen IMSI-numeroon. TMSI-numero tallennetaan SIM-kortille sekä VLR-rekisteriin. (Imai 2005, 96; Eberspächer, ym. 2009, 49)

Tiedonsiirron salaamiseen käytetään 64-bittistä salausavainta K_c. Algoritmeina käytetään A8-algoritmia salausavaimien luomiseen, A3-algoritmia autentikointiin ja A5-algoritmia tiedon salaamiseen. (Imai 2005, 96–97,100; Eberspächer, ym. 2009, 174,177)

RAND on 128-bittinen satunaisluku, jota käytetään autentikoinnissa ja SRES on 32-bittinen autentikointivastaus, joka koostuu RAND-luvusta sekä salausavaimesta K_i.

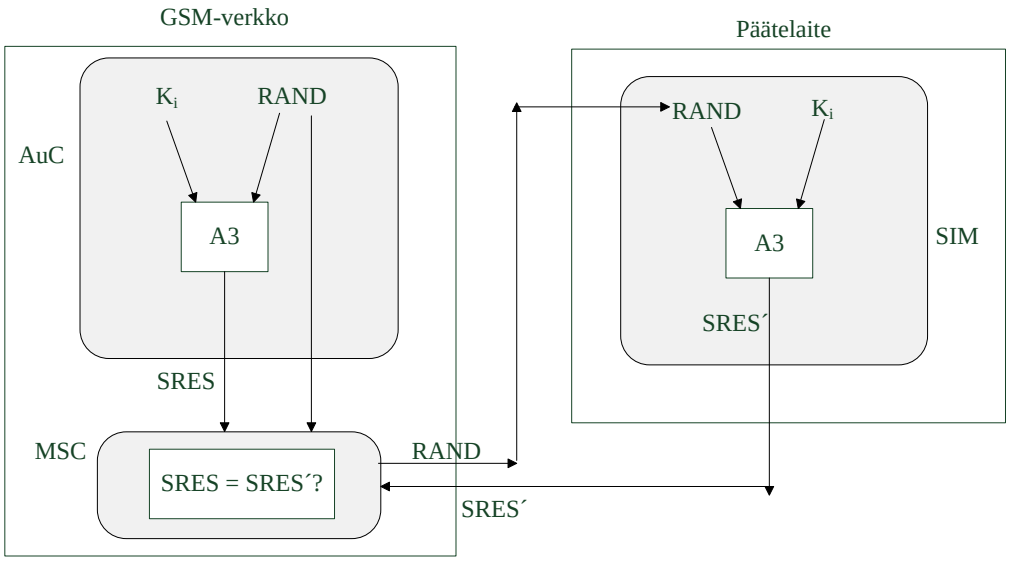
Kuvio 12 hahmottaa, missä kukin salausavain, numero ja algoritmi sijaitsevat.



Kuvio 12: GSM-verkon tietoturvaparametrien sijainnit verkossa. (Imai 2005, 97)

Päätelaitteen kirjautuminen verkkoon alkaa, kun GSM-verkosta MSC lähettää päätelaitteelle RAND-luvun, tai RAND-haasteen, johon päätelaitteen tulee vastata. Päätelaite ja SIM-kortti suorittavat RAND-luvulle sekä salaiselle avaimelle K_i , A3-algoritmin vaatimat toimenpiteet ja saavat aikaan vastauksen RAND-haasteeseen, SRES-viestin. Samalla myös MSC suorittaa laskutoimituksen samoilla parametreilla, jotka se on saanut AuC-tietokannasta ja vertaa päätelaitteen lähettämää SRES-viestiä omaansa. (Imai 2005, 99)

Kuviossa 13 esitetään autentikaatioprosessin vaiheet.

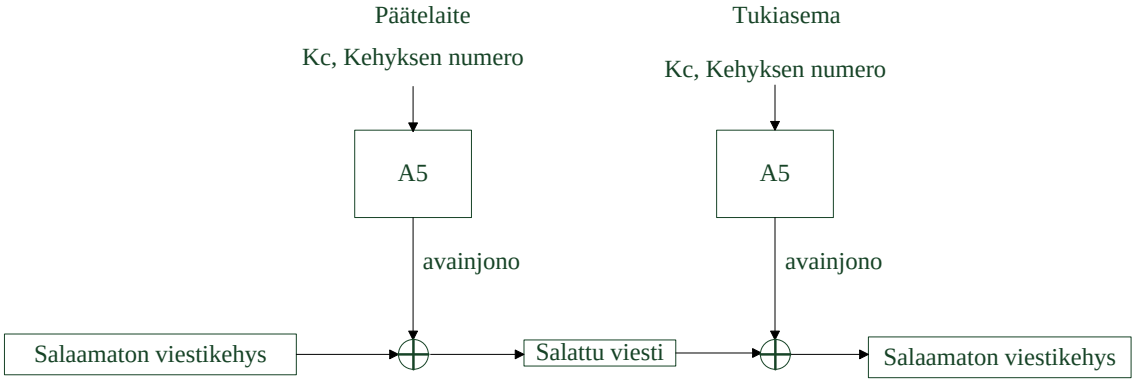


Kuvio 13: GSM-verkkon liittymän/asiakkaan varmentamisprosessi. (Imai 2005, 99)

Päätelaite käyttää samoja parametreja A8-algoritmin kanssa, tiedonsiirronsalaukseen käytettävän avaimen K_c luomiseen. Lisäksi tiedonsiirron salauksessa käytetään kulloinkin lähetettävän kehyksen 22-bittistä numeroa. (Imai 2005, 102)

Kehyksen numerosta ja K_c -avaimesta luodaan A5-algoritmilla 114-bittinen avainjono, joka XOR-operaation avulla yhdistetään bitti kerrallaan salaamattomaan viestikehykseen. Näin luodaan tiedon salaus radiotietä pitkin. (Imai 2005, 101–102)

Kuviossa 14 esitetään radiotien tiedonsiirron salauksen vaiheet päätelaitteelta BSC:lle.



Kuvio 14: Radiotien tiedonsiirron salauksen vaiheet. (Imai 2005, 102)

5.2.1 Tietoturvan heikkoudet

GSM-verkoissa autentikaatio tapahtuu yksipuoleisesti, eli vain käyttäjä tunnistautuu verkolle. Tästä seuraa se, että käyttäjä ei voi tietää onko hän liittynyt oikeaan verkkoon. Tämä mahdollistaa väärennettyjen tukiasemien väliintulon tai ns. mies keskellä -hyökkäyksen päätelaitteen ja oikean tukiaseman väliin. Lisäksi päästä päähän salausta ei GSM-verkoissa ole, vaan ainoastaan radiotie päätelaitteen ja tukiaseman välillä on salattu, jolloin tukiaseman ja tukiasemaohjaimen väli jää turvattomaksi, varsinkin kun usein näiden välinen yhteys on toteutettu radiolinkillä. Radiotien salaus voidaan myös poistaa operaattorin toimesta.(Bouška & Drahanský 2008, 3; Chandra 2005, 151)

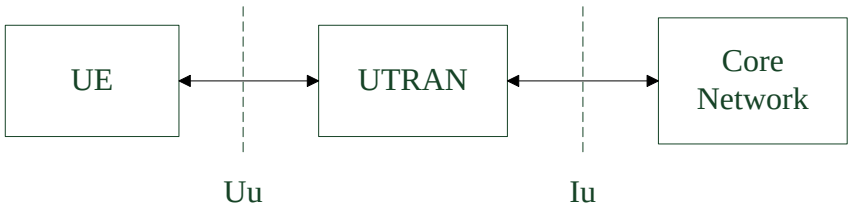
GSM:stä jätettiin myös salausalgoritmeja salaisiksi, jolloin ei voitu tutkia tai varmentaa algoritmien hyvyyttä. Lisäksi radiotien salauksessa käytettävät salausavaimet altistuvat ns. brute force -hyökkäyksille, joissa hyökkääjä kokeilee yhdistelmä yhdistelmältä läpi avaimia, kunnes löytää oikean. Nämä jätettiin tarkoituksella GSM-verkosta huolehtimatta, koska katsottiin että hyökkäysten ehkäisemiseen käytetyt resurssit olisivat olleet suurempia kuin saavutetut hyödyt. (Nyberg & Niemi 2003, 7–8)

6 3G - UMTS-VERKKO

Kun GSM-verkko julkaistiin markkinoille, ETSI aloitti jo seuraavan sukupolven, 3G-verkon kehittämisen ja suunnittelun. Tätä uutta järjestelmää kutsuttiin UMTS:ksi (Universal Mobile Telecommunications System). ETSIssä tätä kehittämistyötä varten luotiin SMG (Special Mobile Group) niminen komitea, joka myöhemmin jakaantui 12 alaryhmään. Myöhemmin 3G-tekniikan kehittämisestä on vastannut useiden tietoliikenneyhtiöiden rakentama 3GPP-ohjelma. (Korhonen 2003, 203)

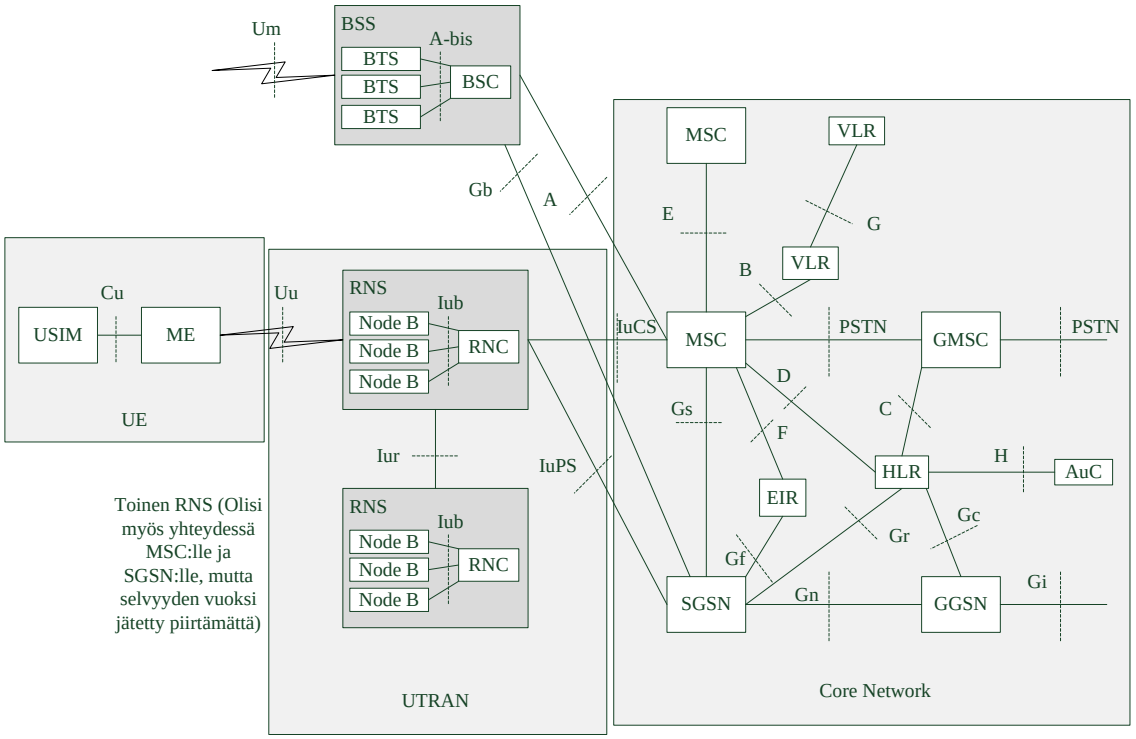
UMTS on rakennettu olemassa olevan GSM-infrastruktuurin päälle ja tukee sekä pakettikytkentäistä, että piirikytkentäistä tiedonsiirtoa. UMTS kuitenkin käyttää uusia tiedonsiirtomenetelmiä päätelaitteen ja tukiaseman välillä. UMTS-verkon tavoitteena on tarjota kustannustehokkaasti laajakaistaista, pakettikytkentäistä palvelua jopa 2 Mbps nopeudella. (4BA2. GSM and UMTS Security)

UMTS-verkko jaotellaan kolmeen osaan, kuten GSM-verkkokin. Osat ovat päätelaite UE (User Equipment), radioverkko-osa UTRAN (UMTS Terrestrial Radio Access Network) sekä ydinverkko CN (Core Network). Kuviossa 15 esitetään näiden osien väliset suhteet. Rajapinnat U_u sekä I_u on suunniteltu siten, että ne tukevat eri valmistajien laitteita. (Korhonen 2003, 206)



Kuvio 15: UMTS-verkon osat. (Korhonen 2003, 206)

Kuviossa 16 esitetään UMTS-verkon arkkitehtuuri. Katkoviivoilla on merkitty kukin rajapinta. Kuten kuviosta voidaan huomata, verkon ydinosassa on samoja osia kuin GSM-verkossakin sekä GPRS-verkossa, jota tässä työssä ei käsitellä. Sama ydinverkko voikin palvella sekä UMTS- että GSM-verkon radioverkkoa. (Korhonen 2003, 206–207)



Kuvio 16: UMTS-verkon arkkitehtuuri. (Korhonen 2003, 207, muokattu)

GMSC (Gateway MSC) on MSC joka sijaitsee kiinteän puhelinverkon ja muiden MSC:iden välissä. Se reitittää sisään tulevat puhelut oikealle MSClle ja HLRlle. SGSN (Serving GPRS Support Node) on keskeinen elementti pakettikytkentäisessä tiedonsiirrossa. Se pitää sisällään tilaajatietoja (mm. IMSI) sekä sijaintitietoja. GGSN (Gateway GPRS Support Node) vastaa toiminnaltaan piirikytkentäisen verkon GMSC:n toimintaa. Poikkeuksena on, että GGSN myös reitittää lähtevää liikennettä. Muut ydinverkon osat toimivat samaan tapaan ja ovat samoin nimetty kuin GSM-verkossakin. (Korhonen 2003, 212–213)

UTRAN, eli UMTS-verkon radioverkko-osa rajoittuu I_uCS- sekä I_uPS-rajapintoihin ja päätelaitteeseen UE (ME+USIM) yhteydessä olevaan U_u-rajapintaan. Se pitää sisällään RNC (Radio Network Controller) radioverkko-ohjaimen, jota GSM-verkossa vastaa BSC, sekä useita tukiasemia, joita UMTS-verkossa kutsutaan nimellä Node B. Nämä yhdessä muodostavat radioverkon alijärjestelmän, RNS (Radio Network Subsystem). (Korhonen 2003, 213–214)

6.1 Salaus ja autentikointi 3G-järjestelmässä

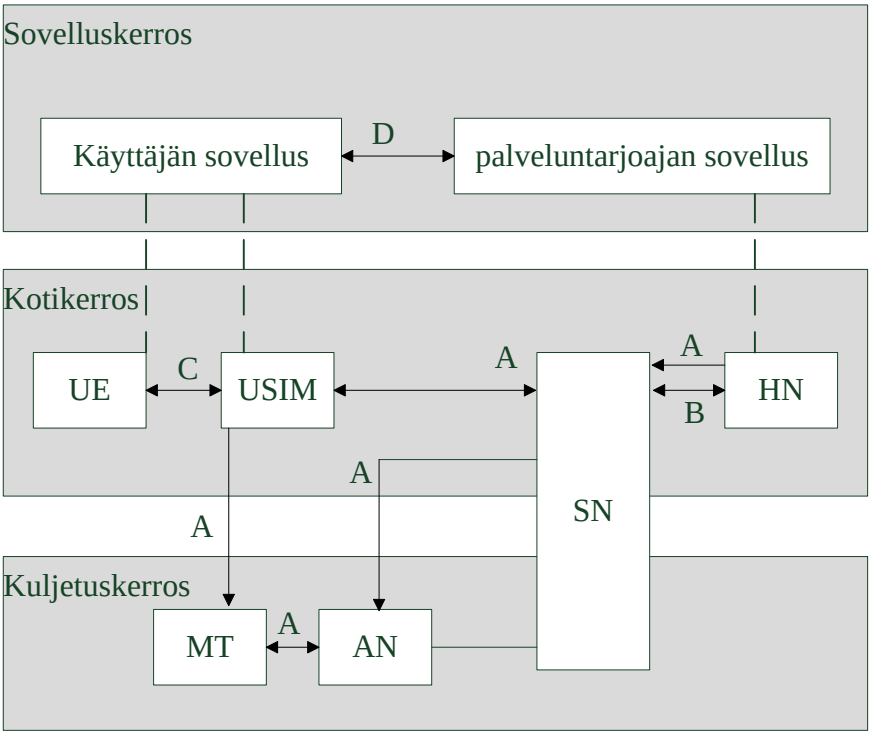
UMTS-järjestelmän tietoturvaominaisuuksia suunniteltiin GSM-järjestelmän pohjalta. Periaatteena oli se, että hyväksi todetut ominaisuudet otettiin suoraan käyttöön ja heikoiksi osoittautuneet suunniteltiin uudelleen. (Chandra 2005, 144)

GSM-järjestelmässä käyttöön otettua vaihtuvaa TMSI-tunnistetta käytetään myös UMTS-järjestelmässä. TMSI korvaa IMSI-numeron, jolloin käyttäjän ja liittymän arkaluontoiset tiedot pysyvät paremmin suojassa, kun IMSI-numeroa ei lähetetä radiotietä pitkin kuin vain tarvittaessa. (Chandra 2005, 145)

Salausavaimina käytetään myös GSM-järjestelmästä peräisin olevaa 128-bittistä K_i-avainta, joka sijaitsee AuC-tietokannassa sekä USIM-kortilla (UMTS Subsrcibers Identity Module). Autentikaatiomallikin muistuttaa läheisesti GSM-verkon vastaavaa, mutta tärkeänä uudistuksena UMTS-verkossa myös verkon on tunnistauduttava käyttäjälle. (Chandra 2005. 146)

Kuvio 17 kuvaa UMTS-järjestelmän tietoturvan osa-alueita. UMTS-järjestelmän tietoturva rakentuu viidestä eri ominaisuudesta: Näkyvyydestä ja muokattavuudesta, verkkoliitynnän turvallisuudesta A, jolla taataan käyttäjälle, että verkko on turvallinen liittyä, puhelinverkon liitynnän turvallisuudesta B, jolla taataan että verkon liityntä kiinteään verkkoon on suojattu, päätelaitteen turvallisesta yhteydestä C sekä sovellustason turvallisuudesta D. (4BA2. GSM and UMTS Security)

Kuviossa 17 SN on palveleva verkko, eli se verkko jossa kulloinkin matkapuhelin on, HN on kotiverkko, AN on liityntäverkko ja MT on puhelun reititystoimintaa verkosta toiseen. (4BA2. GSM and UMTS Security; Federal Communications Commission (ComCom))



Kuvio 17: UMTS-järjestelmän tietoturvan osa-alueet. (4BA2. GSM and UMTS Security)

Molemminpuoliseen autentikaatioon käytetään UMTS-järjestelmässä autentikaatiokvintettiä, joka koostuu käyttäjälle osoitetusta haasteesta RAND, käyttäjän vastauksesta XRES, salausavaimesta C_k sekä eheysavaimesta I_k sekä verkon autentikointimerkistä AUTN. UMTS sisältää myös uuden, tiedon eheysmekanismin, joka suojaa viestit päätelaitteen ja radioverkko-ohjaimen välillä. (4BA2. GSM and UMTS Security)

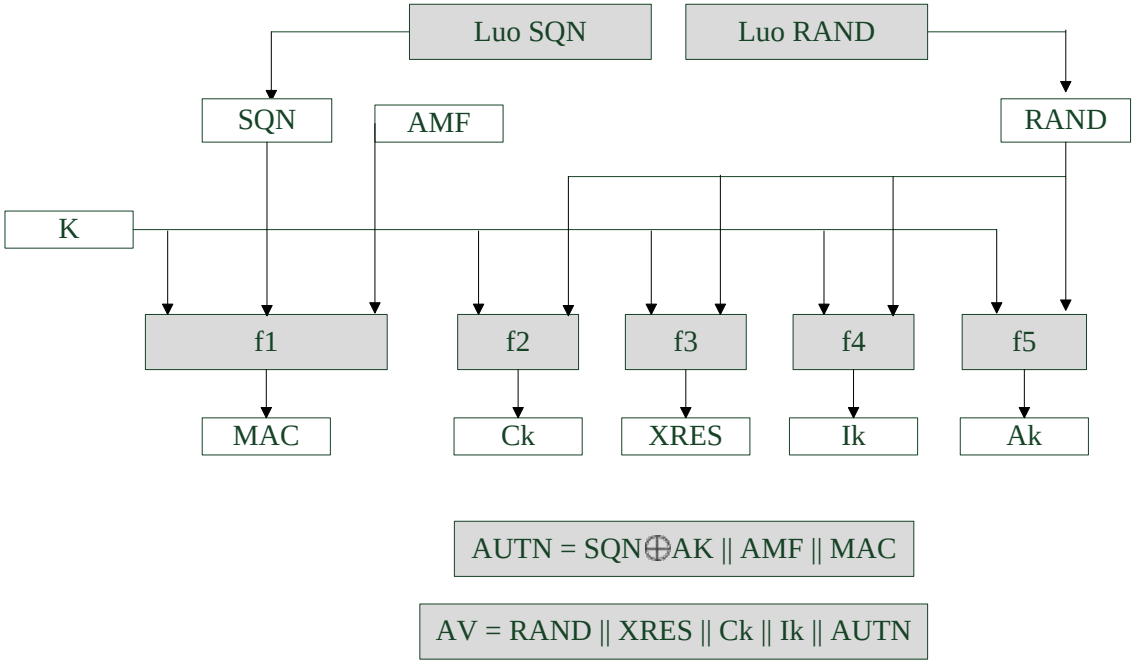
Autentikaatiomenettely alkaa, kun päätelaite UE, johon on asennettu SIM-kortti USIM, lähettää viestin tukiasemalle, ilmoittaakseen aikeistaan liittyä verkkoon. Tukiasema välittää viestin MSC:lle sekä VLR-tietokannalle, jotka määrittävät voiko kyseinen USIM sekä päätelaite liittyä verkkoon. Määrittäminen tapahtuu siten, että MSC lähettää kyselyn ko. USIM-kortin HLR-tietokannalle, tiedustellakseen autentikaatioon tarvittavia parametreja. (Chandra 2005, 146)

Ensimmäiseksi HLR luo satunaisluvun RAND sekä järjestysnumeron SQN. Tämän jälkeen se pyytää AuC-tietokannalta salausavainta K_i. Lisäksi tilaaja-avain K tarvitaan autentikaatiossa. Näillä parametreilla, sekä autentikaation hallintakentällä AMF lasketaan funktiot f1–f5. Parametrit lähetetään takaisin niitä pyytäneelle MSClle sekä VLR-tietokannalle jotka lähettävät edelleen RAND- sekä AUTN-parametrit valitusta autentikaatiovektorista päätelaitteen USIM-kortille. Kuten GSM-verkossakin, RAND-

parametri toimii haasteena, johon päätelaitteessa olevan USIM-kortin on vastattava oikein.(Chandra 2005, 147–148; Helsinki University of Technology 2003, 13)

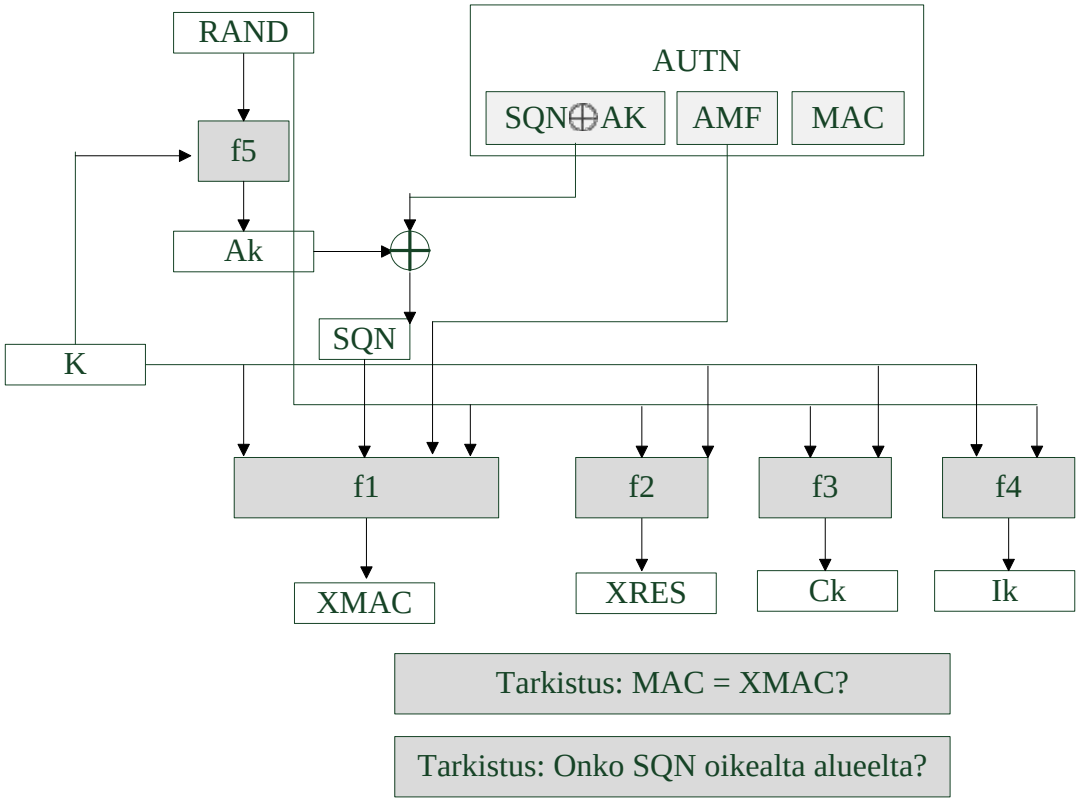
Funktiolla f1–f5 lasketaan parametrit autentikaatiovektorille AV lisäksi myös autentikointimerkille AUTN. Parametrit ovat MAC (Message Authentication Code), joka varmentaa viestin eheyttä sekä autentikointia, XRES, joka on odotettu tilaajan vastaus RAND-haasteeseen sekä salausavain Ck, eheysavain I_k ja nimettömyysavain A_k. (Chandra 2005, 147; 4BA2. GSM and UMTS Security)

Kuviossa 18 esitetään periaate, jolla HLR laskee autentikaatioparametrit fuktioilla f1–f5.



Kuvio 18: Autentikaatioparametrien laskeminen UMTS-järjestelmässä. (Chandra 2005, 148)

Kun päätelaite sekä sen sisällä oleva USIM-kortti ovat vastaanottaneet verkolta autentikaatioon vaadittavat RAND- sekä AUTN-parametrit, alkaa USIM laskea vastausta haasteeseen. Kuten kuviosta 18 ilmenee, AUTN-parametri sisältää useita parametreja jo itsessään, joita tarvitaan molemminpuoliseen autentikaatioon. Kuviossa 19 esitetään toimintaperiaate, jolla USIM laskee vastauksen verkon esittämään autentikaatiohaasteeseen. Lisäksi USIM varmentaa, että verkko, johon liitytään on luotettava. Tähän käytetään MAC- ja SQN-parametreja. (Chandra 2005, 148)

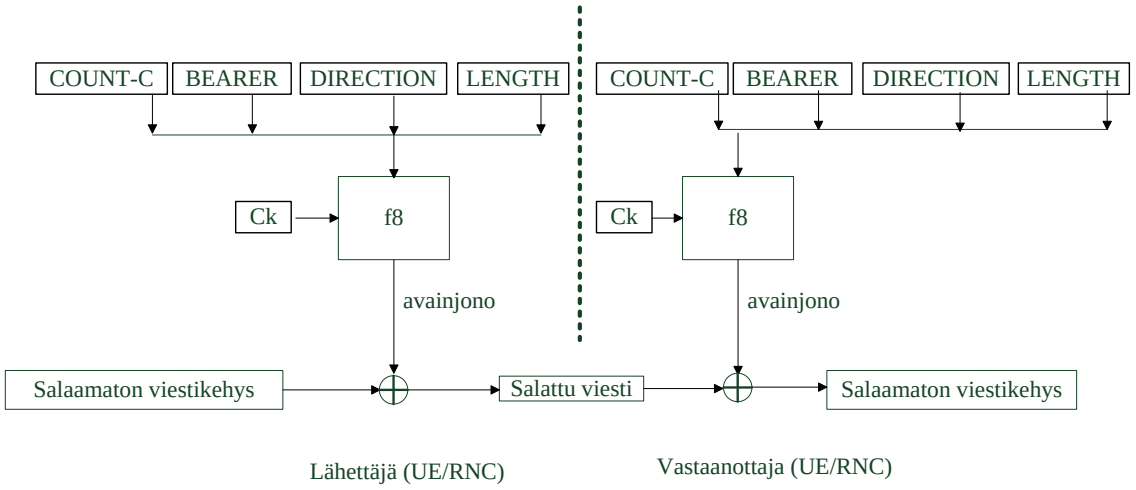


Kuvio 19: Päätelaitteen ja USIMin autentikaatiovastauksen luomisprosessi. (Chandra 2005, 148; 4BA2. GSM and UMTS Security)

Kun päätelaite ja USIM ovat tarkistaneet, että verkko on luotettava, lähetetään funktiolla f2 laskettu SRES-arvo takaisin verkkoon MSClle ja VLR-tietokannalle, jotka vertaavat sitä laskettuun XRES-arvoon. Näin käyttäjä sekä liittymä tunnistautuu verkolle. Mikäli arvot ovat samat, autentikointi on onnistunut ja verkon palveluita voidaan käyttää kyseisellä USIMillä. (Chandra 2005, 149)

Tiedon salaukseen UMTS käyttää KASUMI-algoritmia sekä 128-bittistä salausavainta Ck (Ciphering key). KASUMI-algoritmi tuo mukanaan huomattavan tietoturvan parannuksen verrattuna GSM-järjestelmässä käytettävään A5-algoritmiin. Tiedon salauksessa käytettävät muut parametrit ovat 32-bittinen COUNT-C, joka on salaussekvenssin numero, joka päivittyy jokaisen salattavan viestikehyksen kohdalla, sekä 5-bittinen BEARER, joka on uniikki tunniste jolla käytössä oleva siirtokanava tunnistetaan, 1-bittinen DIRECTION joka määrittää kumpaan suuntaan tiedonsiirtoa käydään (uplink/downlink) ja 16-bittinen LENGTH joka määrittää salausavainjonon pituuden. Nämä parametrit syötetään f8-algoritmiin ja tuloksena on avainjono, jolla salaamaton viesti XOR-operaation avulla salataan ja vastaanottajapäässä samalla operaatiolla saadaan salattu viesti avattua. Salaus suojaa radiotietä, välillä USIM - RNC.(Chandra 2005, 150)

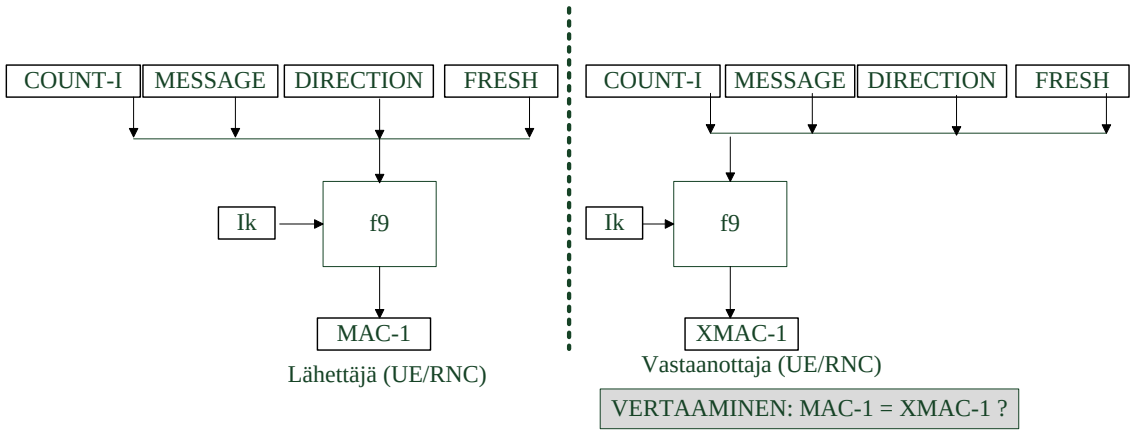
Kuvio 20 esittää tiedon salauksen toimintaperiaatteen.



Kuvio 20: UMTS-verkon radiotien tiedonsiirron salauksen toimintaperiaate. (Chandra 2005, 150)

Tiedon eheyttä UMTS-verkossa varmistetaan f9-algoritmin avulla luoduilla MAC-1-tunnuksilla. MAC-1-tunnus liitetään lähetettävän viestiin. Parametreina algoritmiin on 128-bittinen eheysavain I_k, 32-bittinen eheyssekvenssinumero COUNT-I, joka vaihtuu jokaisen lähetettävän viestikehyksen mukaan, DIRECTION bitti, jolla määritellään tiedonsiirron suunta (uplink/downlink), 32-bittinen FRESH, joka on jokaista yhteyttä varten luotu satunaisjono. Lisäksi parametrina toimii itse lähetettävä viesti. Vastaanottaja luo oman XMAC-1-tunnuksen ja vertaa sitä vastaanotetussa viestissä olleeseen MAC-1-tunnukseen. Mikäli ne ovat samat, viesti on eheä.(Chandra 2005, 151)

Kuvio 21 esittää tiedon eheyden varmistamisen toimintaperiaatteen.



Kuvio 21: UMTS-verkon tiedon eheyden varmistuksen toimintaperiaate. (Chandra 2005, 151; Helsinki University of Technology 2003, 16)

7 4G - LTE-JÄRJESTELMÄ

LTE (Long Term Evolution) kehitettiin tarjoamaan suurempaa järjestelmäkapasiteettia sekä peittoaluetta ja vähentämään kustannuksia. Tavoitteena oli myös parantaa käyttökokemusta suuremmalla tiedonsiirtokapasiteetilla ja pienemmillä viiveajoilla. Lisäksi LTE suunniteltiin siten, että se voidaan helposti käyttöönottaa olemassa olevan arkkitehtuurin rinnalle. (Ratasuk & Ghosh 2011, 10)

LTE-järjestelmän arkkitehtuuri on IP-pohjainen ja suunniteltu tukemaan tehokkaasti pakettikytkentäistä tiedonsiirtoa. Järjestelmä koostuu kahdesta pääosasta ja päätelaitteesta UE. Ensimmäinen osa on radioverkko-osa E-UTRAN joka pitää sisällään LTE-tukiasemia, joita kutsutaan eNB:ksi. (eNodeB). Toinen osa ydinverkko EPC (Evolved Packet Core) koostuu MME:stä (Mobility Management Entity), S-GW:stä (Serving Gateway) ja P-GW:stä (Packet Gateway). (Ratasuk & Ghosh 2011, 12–13)

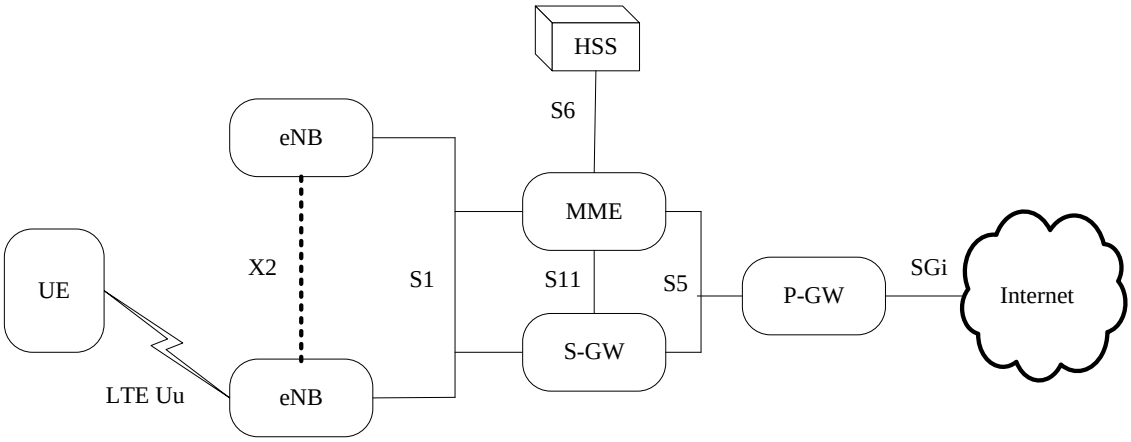
Tukiasemaosa eNB on huomattavasti kehittyneempi kuin UMTS-järjestelmän NodeB-tukiasema. ENB toimii autonomisena osana järjestelmää, huolehtien QoS-palveluista, kuormantasauksesta sekä kanavien sekä radiotien hallinnasta. ENB koostuu antenneista, radiomoduuleista, jotka moduloivat sekä demoduloivat lähetettävät ja vastaanotettavat signaalit sekä digitaalisista moduuleista, jotka käsittelevät kaikki lähetettävät ja vastaanotettavat signaalit ja toimivat liityntänä ydinverkkoon. Tukiasemat ovat toisiinsa yhteydessä X2 rajapinnan kautta, jonka avulla tukiasemat huolehtivat kanavanvaihdoista. Tukiasema on yhteydessä MMEn ja S-GWn kanssa S1 rajapinnan kautta. (Sauter 2010, 210–211)

MME huolehtii autentikoinnista verkossa sekä GSM- ja UMTS-verkkoihin yhdistämisestä. Autentikaatio tapahtuu yhdessä HSS-tietokannan kautta. Lisäksi MME voi hoitaa kanavanvaihtoa, mikäli tukiasemien välinen X2 rajapinta ei ole käytössä. Vaikka LTE on puhtaasti IP-pohjainen verkko, MME kuitenkin tukee myös perinteisiä tekstiviesti- sekä puhelupalveluita. MME on yhteydessä HSS-tietokantaan S6 rajapinnan kautta sekä S-GWn kanssa S11 rajapinnan kautta. MME päättää myös NAS (Non-Access Stratum) viestinnän päätelaitteen ja MMEn välillä. NAS hallitsee päätelaitteen mobiliteettia sekä tukee istunnon hallintatoimenpiteitä, luo ja ylläpitää IP-yhteyttä päätelaitteen ja P-GWn välillä. (Sauter 2010, 213; LteWorld)

S-GW huolehtii tiedonsiirrosta tukiasemien ja P-GW:n välillä. P-GW on reititin joka yhdistää verkon Internetiin. P-GW on vastuussa IP-osoitteiden jakamisesta päätelaitteille. P-GW on yhteydessä MMEn ja S-GWn kanssa S5 rajapinnan kautta ja Internetiin SGi rajapinnan kautta.(Sauter 2010, 214)

HSS-tietokanta sisältää samoja tietoja kuin GSM- sekä UTMS-verkon HLR-tietokanta. HSS ja HLR ovatkin fyysisesti yhdistetty, jolla taataan helppo verkosta toiseen siirtyminen. Tietojen hakuun tietokannasta käytetään DIAMETER-protokollaa. (Sauter 2010, 215)

Kuvio 22 esittää LTE-verkon osat sekä rajapinnat.



Kuvio 22: LTE-verkon arkkitehtuuri. (Sauter 2010, 208, muokattu)

7.1 Salaus ja autentikointi LTE-järjestelmässä

Ensimmäinen uusi tietoturvaominaisuus LTE-järjestelmässä on NAS-viestinnän salaus, jossa päätelaitteen ja MMEn välinen NAS-viestintä on salattua. Lisäksi kokonaan IP-pohjainen järjestelmä tarjoaa mahdollisuuden salata S1 rajapintojen välinen liikennöinti käyttämällä IPsec-protokollapinoa (Internet Protocol Security). Näiden uusien tietoturvaominaisuuksien lisäksi, LTE sisältää edellisten (GSM ja UMTS) verkkotekniikoiden tietoturvaominaisuuksia, kuten molemminpuolinen autentikaatio ja tilaajan identiteetin salaus käyttämällä tilapäistä identiteettiä jota LTEssä kutsutaan GUTI-parametriksi. (Kreher & Gaenger 2010, 34)

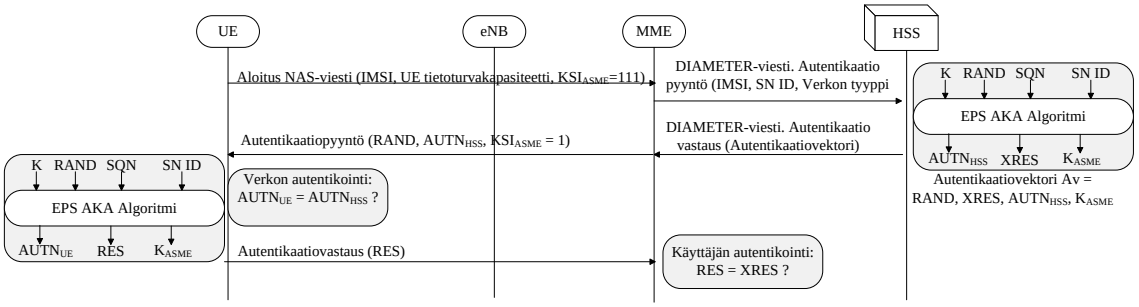
LTE käyttää useita eri salausavaimia liikennöinnissä. K_{eNB} on avain jonka päätelaite UE ja MME johtavat K_{ASME} avaimesta tai kanavavaihdon yhteydessä tukiaseman ja päätelaitteen välillä. Avainta käytetään vain radiotien (RRC) liikenteen sekä käyttäjäliikenteen (UP) salausavaimien johtamiseen. K_{NASint} avainta käytetään NAS-liikennöinnin eheyden varmentamiseen. K_{NASenc} avainta taas käytetään NAS-liikennöinnin salaamiseen. Nämä avaimet johdetaan K_{ASME} avaimesta. K_{UPenc} avainta käytetään käyttäjäliikenteen salaamisessa. Avain johdetaan K_{eNB} avaimesta. K_{RRCint} on avain, jolla varmistetaan radiotien liikenteen eheys. Avain johdetaan K_{eNB} avaimesta, kuten myös K_{RRCenc} avain joka huolehtii radiotien liikenteen salauksesta. (Kreher & Gaenger 2010, 34 – 35)

Käyttäjän autentikointi tapahtuu siten, että päätelaite lähettää MME:lle NAS-viestin, joka sisältää päätelaitteen tietoturvakapasiteetit, joita ovat mm. tuetut salaus- sekä eheysalgoritmit. Tämän jälkeen MME lähettää DIAMETER-viestin HSS-tietokannalle, tiedustellakseen autentikaatiotietoja kyseiselle päätelaitteelle. HSS sisältää salausavaimen K, joka on myös päätelaitteen USIM-kortilla. Salausavaimella K sekä tilaajatiedon avulla HSS luo salausavaimen K_{ASME}, autentikaatiomerkin AUTN sekä odotetun vastausviestin XRES. Lisäksi HSS luo satunaisluvun RAND. Nämä lähetetään takaisin MMElle joka johtaa K_{ASME} avaimesta salausavaimet K_{NASenc}, K_{NASint} sekä $K_{eNB.}$

Tämän jälkeen MME lähettää RAND- ja AUTN-parametrit päätelaitteelle, joka salausavaimen K, sekä RAND- ja AUTN-parametrien avulla laskee vastauksen RES, jonka se lähettää MME:lle. MME vertaa saamaansa RES arvoa XRES arvoon ja mikäli arvot ovat samat, päätelaite voi jatkaa toimintaansa verkossa. (Kreher & Gaenger 2010, 35–36)

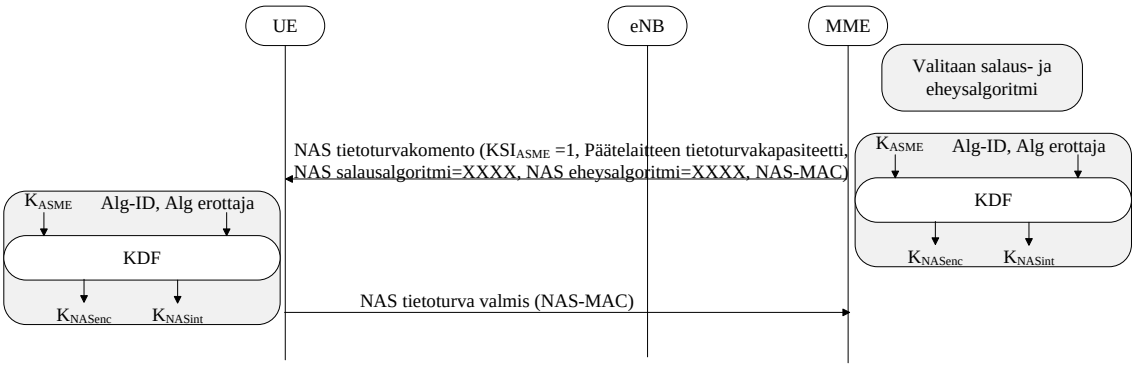
Salausavainten ja parametrien muodostamiseen käytetään EPS AKA-algoritmia (Evolved Packet System Authentication and Key Agreement) sekä KDF-funktiota (Key Derivation Function). (NMC Consulting Group)

Kuvio 23 esittelee autentikointitapahtuman periaatteen. Kuvio 24 esittää myös yllä esitetyn NAS-viestinnän autentikointi- ja eheysavaimien luontiprosessin.



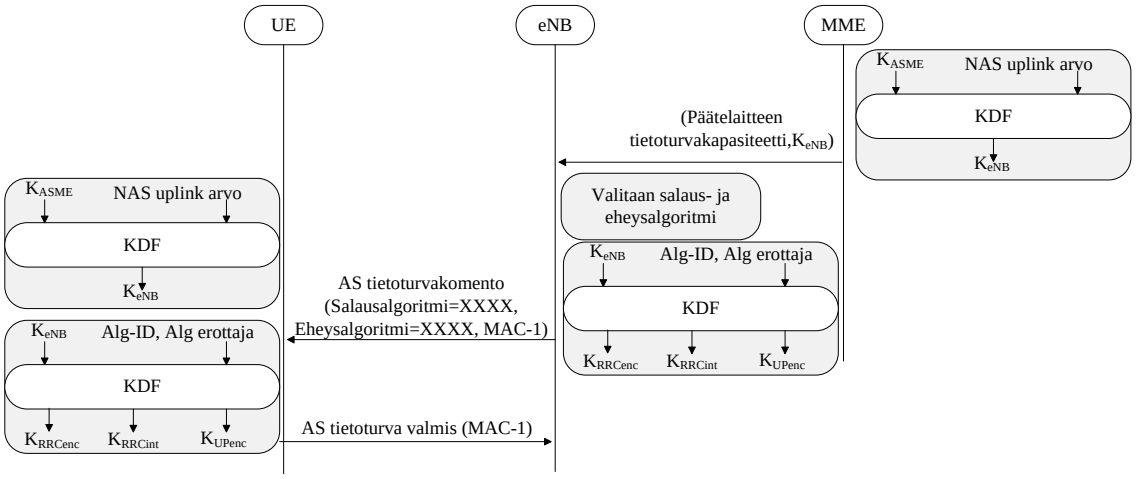
Kuvio 23: LTE-järjestelmän autentikaatioprosessi. (Kreher & Gaenger 2010, 36; NMC Consulting Group, muokattu)

Kun autentikaatioprosessi on suoritettu, luodaan salausavaimet ja -algoritmit tukiasemalle eNB. Näillä avaimilla salataan ja varmennetaan NAS-viestejä sekä RRC-viestejä. Kun salaus- ja eheysalgoritmeja asetetaan, päätelaite, tukiasema sekä MME sopivat käytettävän salausalgoritmin sekä eheysalgoritmin. (Sauter 2010, 254)



Kuvio 24: NAS-viestinnän salausalgoritmien luomisprosessi. (Kreher & Gaenger 2010, 37; NMC Consulting Group, muokattu)

Kuvio 25 esittää RRC-viestinnän salaus- ja eheysavaimien luontiprosessin.

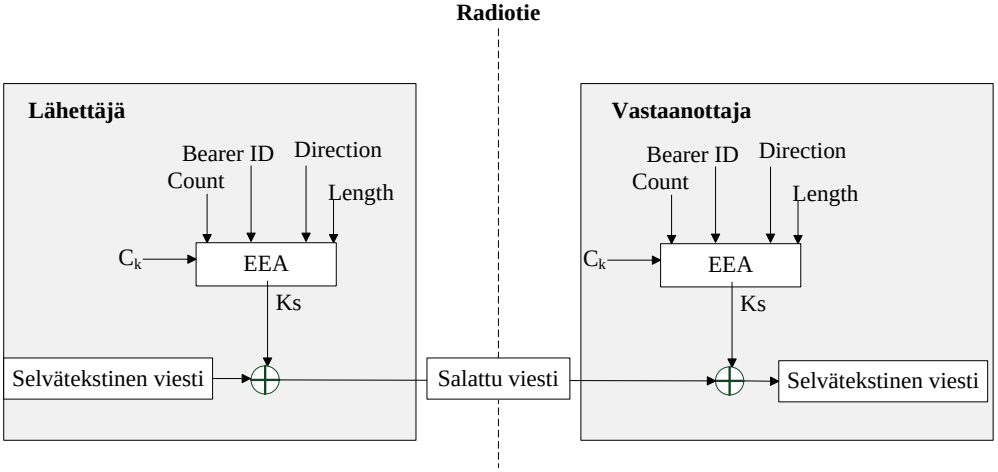


Kuvio 25: RRC-viestinnän salaus- ja eheysavaimien luontiprosessi. (Kreher & Gaenger 2010, 37; NMC Consulting Group, muokattu)

LTE-järjestelmä tukee kolmea EPS salausalgoritmia (EEA) viestien salaamisessa. Käytettävät algoritmit ovat SNOW 3G- ja AES-algoritmi. Kolmas algoritmi on nolla-algoritmi, jolloin salausta ei käytetä. Poiketen aikaisemmista järjestelmistä, LTE-laitteiden on ilmoitettava käyttäjälle onko ilmarajapinnan tietoliikenne salattua vai salaamatonta. (Cox 2012, 196–197)

Salausprosessissa lähettäjä luo näennäissatunaisen avainjonon EEA-algoritmilla, johon syötetään 128-bittinen salausavain C_k sekä muut IV-alustusmuuttujat. IV-alustusmuuttujia ovat 5-bittinen yksilöivä haltija ID (Bearer ID), 32-bittinen laskurin arvo Count, 1-bittinen tiedonsiirron suunnan osoittava merkki Direction ja salattavan viestin pituus Length. (Cox 2012, 197; ETSI/SAGE 2009)

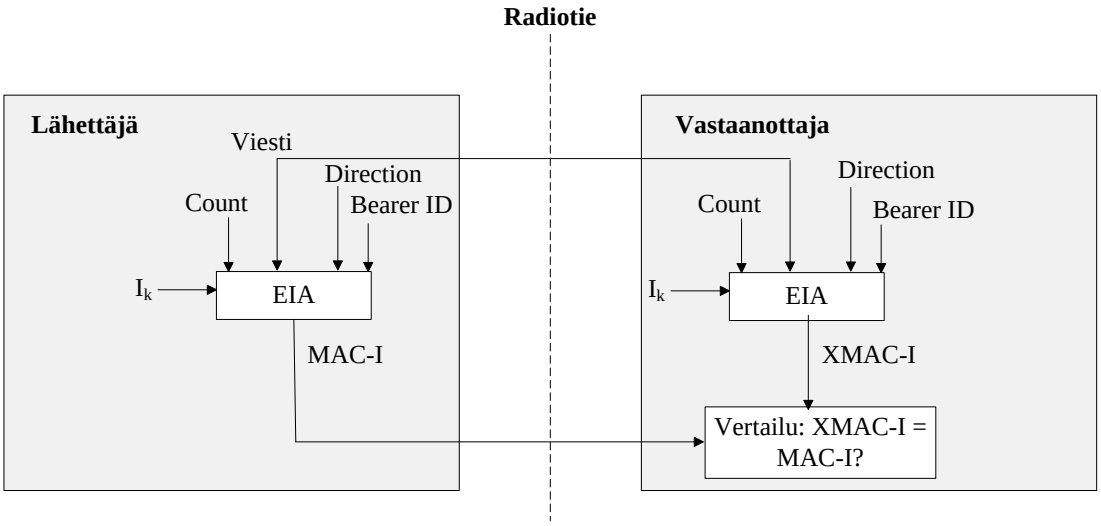
Kuviossa 26 esitetään salauksen periaate lähettäjän ja vastaanottajan välillä.



Kuvio 26: Viestin salaaminen LTE-järjestelmässä. (Cox 2012, 197, muokattu)

Viestien eheyden tarkistamiseen käytetään EPS eheysalgoritmeja (EIA). Kuten EEA-algoritmeissakin, myös EIA-algoritmeissa käytetään joko SNOW 3G- tai AES-algoritmeja. Algoritmin avulla lasketaan lähetettävälle viestille tarkistussumma MAC-I. Vastaanottaja laskee oman vastineensa XMAC-I ja vertaa näiden kahden summan arvoa toisiinsa. Mikäli arvot eivät täsmää, viesti tuhotaan. (Cox 2012, 197)

Kuvio 27 esittää viestin ehdeyden tarkistusprosessin.



Kuvio 27: Viestin ehdeyden tarkistusprosessi. (Cox 2012, 198, muokattu)

8 POHDINTA

Työssä tutustuttiin eri tietoliikennejärjestelmien salaus- ja autentikaatiomenetelmiin. Näihin tutustuttaessa oli selkeästi huomattavissa se, että tekniikan kehittyessä myös salaus- ja autentikaatiomenetelmät kehittyivät huomattavasti. Tietotekniikan kehittyessä yhä useammalla henkilöllä on taidot sekä tarvittavat laitteet ja resurssit murtaa yksinkertaiset suojausmenetelmät, joten uusia, vahvempia suojausalgoritmeja sekä -menetelmiä tarvitaan jatkossakin.

Työhön valittujen langattomien järjestelmien valinnassa on onnistuttu, koska tavoitteena oli esitellä yleisesti käytössä olevia järjestelmiä. Työtä olisi mahdollista jatkaa tulevaisuudessa jatkotutkimuksilla, koska työn ulkopuolelle jäi useita erilaisia järjestelmiä ja myös esitetyistä järjestelmistä on jokaisesta mahdollisuus tehdä oma, syvempi analyysi. Lisäksi työssä esitetyistä algoritmeista itsestään on mahdollista suorittaa erittäin laajoja tutkimuksia.

Tämä opinnäytetyö pohjautuu vahvasti eri lähteisiin, joten lähteiden luotettavuus on pyritty varmistamaan vertailemalla niitä muihin saatavilla oleviin aineistoihin. Lisäksi suurin osa lähdemateriaalista oli kirjoitettu englanniksi, joten käännöstyöhön on panostettu.

Matkapuhelinverkkojen suojaus on suurilta osin operaattorien harteilla, käyttäjän tehtäväksi jääkin näissä verkoissa asianmukaisen päätelaitteen ostaminen sekä asianmukaisen SIM-kortin asettaminen laitteeseen. Tässä työssä on kuitenkin huomattava että matkapuhelinverkkojen suojaus on kehittynyt huomattavasti eri verkkosukupolvien myötä ja tämä vaatii operaattoreilta lisää resursseja, suunnittelua ja paneutumista asiaan. Lisäksi usein verkkosukupolvia käytetään rinnakkain.

WLAN-verkkojen salaukseen voi kuluttaja vaikuttaa huomattavasti enemmän. Kotiverkossaan kannattaakin valita mahdollisimman vahva salaus jotta verkon tietoturva ei vaarannu. Salausavaimen asettamisessa on myös tarpeen huomioida se, että salausavaimesta muodostuu mahdollisimman monimutkainen yhdistelmä. Salaamattomia WLAN-verkkoja käytettäessä on hyvä miettiä miten verkkoa käyttää, koska kaikki tietoliikenne

voidaan kyseisissä verkoissa kaapata ja sitä voidaan lukea erittäin helposti. Näitä tietoja voidaan jälkikäteen käyttää rikollisessa toiminnassa hyväksi.

Bluetooth-laitteita käytettäessä on asetettava PIN-koodi aina, kun se on mahdollista. Lisäksi käyttäjän on nähtävä PIN-koodin asettamisessa se vaiva, että koodista tulee mahdollisimman monimutkainen yhdistelmä, eikä esimerkiksi numerosarja 1234. Lähes jokainen matkapuhelin on myös Bluetooth-laite. Mikäli kyseiselle ominaisuudelle ei ole tarvetta, voidaan tietoturvaa lisätä sammuttamalla Bluetooth-ominaisuus kokonaan.

RFID-järjestelmät ovat aiheuttaneet paljon vastarintaa epäilijöiden joukossa juuri niiden seurattavuuden takia. Suurimmat skeptikot ovat sitä mieltä, että valtiot ja yrityksen käyttävät tekniikkaa juuri sen takia, että voivat seurata ihmisten käyttäytymistä ja profiloida heidät mahdollisimman tarkasti. Lisäksi passeihin asennetut RFID-tunnisteet ovat mahdollisesti luettavissa ja seurattavissa, koska ne sisältävät henkilön yksilöivää tietoa yllin kyllin.(Banks, ym. 2007, 272–273)

Kirjoittaja itsekin on joutunut RFID-tunnisteen väärinkäytön uhriksi, kun eräästä liikkeestä ostetun tuotteen sisällä ollut tunniste aktivoitui toisessa liikkeessä. Aktivoituminen kävi ilmi siitä, että liikkeen varashälytinjärjestelmä toimi RFID-tekniikalla ja lukijan ohitse käveleminen laukaisi varashälyttimen.

RFID-järjestelmän käyttöönotossa tulevaisuuden viivakoodina onkin syytä huolehtia siitä, ettei kuluttajaa seurata ja profiloida tunnisteiden avulla. Myös yllä mainitun kaltaisien nolojen tilanteiden välttäminen on pyrittävä estämään. Yksi potentiaalinen toimenpide on tässä työssä esitetty tappokäsky. Lisäksi erilaisiin henkilökortteihin ja tunnisteisiin liitettävien RFID-tunnisteiden salaus- ja autentikointimetodeista on tehtävä tarpeeksi luotettavia.

Salaus ja autentikointi ovat kuitenkin vain osa kattavaa tietoturvaa. Ne ovat välttämättömiä, mutta myös käyttäjän toiminnalla verkossa on suuri rooli tietoturvassa. Käyttäjän on pidettävä hyvää huolta päätelaitteistaan ja myös mietittävä omaa verkossa käyttäytymistään. Kun yhä enemmän ja enemmän tietoa siirtyy tietoverkkoihin, käyttäjiltä vaaditaan suurta valveutuneisuutta siitä, mitä he itse verkkoon laittavat ja miten he käyttäytyvät, jottei heidän oma yksityisyytensä vaarantuisi.

LÄHTEET

Banks, J., Hanny, D., Pachano, M. A. & Thompson, L. G. 2007. RFID Applied. Hoboken, NJ, USA: John Wiley & Sons Ltd.

Bouška P. & Drahanský P. 2008. Communication Security in GSM Networks. Brno University of Technology. 2008 International Conference on Security Technology.

Chandra, P. 2005. Bulletproof Wireless Security: GSM, UMTS, 802.11 and Ad Hoc Security. Burlington, MA, USA: Newnes.

Cox, C. 2012. An Introduction to LTE - LTE, LTE-advanced, SAE and 4G Mobile communications. Iso-Britannia: John Wiley & Sons Ltd.

Eberspächer, J., Bettstetter, C., Hartmann C. & Vögel, H. 2009. GSM - Architecture, Protocols and Services. 3. Painos. Hoboken, NJ, USA: John Wiley & Sons Ltd.

Estevez-Tapiador, J. M., Hernandez-Castro, J. C., Peris-Lopez, P. & Ribagorda A. Lightweight Cryptography for Low-Cost RFID Tags. Teoksessa Kitsos P. & Zhang Y. Security in RFID and Sensor networks. 2009. Boca Raton, FL, USA: Auerbach Publications.

ETSI. 3GPP™ Algorithms. Luettu 28.10.2012.
http://www.etsi.org/website/ourservices/algorithms/3gppalgorithms.aspx

ETSI/SAGE. 2009. Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 1: UEA2 and UIA2 Specification. Luettu 28.10.2012.
http://serving.webgen.gsm.org/5926DA9A-2DD6-48E7-BAD4-50D4CD3AF30A/assets/uea2uia2d1v21.pdf

Federal Communications Commission (ComCom). Appendis “What is mobile termination?” PRESS RELEASE. Luettu 18.10.2012.
http://www.news.admin.ch/NSBSubscriber/message/attachments/1603.pdf

Gehrmann, C., Persson, J & Smeets, B. 2004. Bluetooth Security. Norwood, MA, USA: Artech House.

GSM For Dummies. GSM Network Architecture. Luettu 16.10.2012.
http://gsmfordummies.com/architecture/arch.shtml

Helsinki University of Technology. S-38.119 Tietoverkkotekniikan seminaari. Mobiili Internet. 2002. Luettu 2.1.2013. http://www.netlab.tkk.fi/opetus/s38119/k02/raportti.pdf

Helsinki University of Technology. Perttula, K-P. UMTS security. 2003. Luettu 24.10.2012.
http://www.netlab.tkk.fi/opetus/s38153/k2003/Lectures/g42UMTS_security.pdf

Imai, H. 2005. Wireless Communications Security. Norwood, MA, USA: Artech House, INC.

Kallonen, T. 2006. RFID-tekniikan käyttö betonielementtien tunnistamiseen. Lappeenrannan Teknillinen Yliopisto. Tietotekniikan osasto. Diplomityö.

Korowajczuk, L. 2011. LTE, WiMAX and WLAN Network Design, Optimization and Performance Analysis. Hoboken, NJ, USA: John Wiley & Sons Ltd.

Korhonen, J. 2003. Introduction to 3G Mobile Communications (Second Edition). 2. Painos. Norwood, MA, USA: Artech House

Kreher, R. & Gaenger, K. 2010. LTE Signaling: Troubleshooting and Optimization. Hoboken, NJ, USA: John Wiley & Sons Ltd.

LteWorld. Non-Access-Stratum (NAS) Protocol. Luettu 28.10.2012. http://lteworld.org/specification/non-access-stratum-nas-protocol

NMC Consulting Group. LTE Security. Luettu 28.10.2012. http://www.nmcgroups.com/files/download/NMC.LTE%20Security.v1.0.pdf

Nyberg, K. & Niemi, V. 2003. UMTS Security. West Sussex, Iso-Britania: John Wiley & Sons Ltd.

Opel, A. Otto-von-Guericke University of Magdeburg. Bluetooth Authentication - Authorisation - Encryption. 2003. Luettu 3.1.2012. http://www.toengel.net/studium/mm_and_sec/bluetooth.pdf

Pitkämäki, A. Tampereen Teknillinen Yliopisto. Essee: Bluetoothin Tietoturva-arkkitehtuuri. Luettu 6.1.2013. http://www.cs.tut.fi/kurssit/8306000/LTT/ap.pdf

Prasad, N. & Prasad A. 2005. 802.11 WLANs and IP Networking : Security, QoS, and Mobility. Norwood, MA, USA: Artech House.

Rackley, S. 2007. Wireless Networking Technology: From Principles to Successful Implementation. Jordan Hill, Iso-Britania: Newnes.

Ratasuk, R. & Ghosh, A. 2011. Essentials of LTE and LTE-A. New York, USA: Cambridge University Press.

RFID Lab Finland ry. RFID-tekniikan käyttämät taajuusalueet. Luettu 21.1.2013. http://www.rfidlab.fi/rfid-tekniikan-k%C3%A4ytt%C3%A4m%C3%A4t-taajuusalueet

Sauter, M. 2010. From GSM to LTE: An Introduction to Mobile Networks and Mobile Broadband. Hoboken, NJ, USA: John Wiley & Sons Ltd.

Subramanian, M., Gonsalves, T. & Rani, N. 2010. Network Management Principles and Practice. 1. Painos. Noida, Intia: Dorling Kidersley (India) Pvt. Ltd.

Technology Reports. Zugenmaier, A. & Hiroshi, A. Special Articles on SAE Standardization Technology: Security Technology for SAE/LTE. Luettu 28.10.2012. http://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol11_3/vol11_3_027en.pdf

Wireless Computing. 802.11b Security Mechanisms. Luettu 15.10.2012. http://www-cs-faculty.stanford.edu/~eroberts/courses/soco/projects/2003-04/wireless-computing/sec_80211.shtml

Wi-Fi Alliance. 2005. Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise. Luettu 16.10.2012. http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf

4BA. GSM and UMTS Security. Luettu 18.10.2012. http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group7/index.html

Jonsson, T. 2012. Pirkanmaan alueen jätelajittelututkimus. Paperi- tekstiili- ja kemiantekniikan koulutusohjelma. Tampereen ammattikorkeakoulu. Opinnäytetyö.

Toro, J. 2006. Bluetooth-tekniikka ja tietoturva. Tietotekniikan koulutusohjelma. Tampereen ammattikorkeakoulu. Opinnäytetyö.