Antti Tuominen

3G:n rakenne ja tietoturva

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

25.5.2014

Metropolia

Tekijä Otsikko Sivumäärä Aika	Antti Tuominen 3G:n rakenne ja tietoturva 32 Sivua 25.5.2014
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto	tietoverkot ja tietoliikenne
Ohjaaja	yliopettaja tri Tero Nurminen

Insinöörityön tavoitteena oli kerätä tietoa 3G:n yleisestä rakenteesta sekä käyttäjäkohtaisesta tietoturvasta. 3G-verkot ovat osa jokapäiväistä toimintaa, joten insinöörityön aihe on erittäin ajankohtainen. Aiheeseen tutustuttiin etsimällä tietoa useiden standardointijärjestöjen tietokannoista sekä kirjallisista lähteistä.

Insinöörityössä perehdyttiin 3G:n rakenteeseen sekä tietoturvaan käyttäjän näkökulman kannalta. Insinöörityössä tehtiin myös katsaus matkapuhelinverkkojen historiaan, jotta lukijalle muodostuisi yleiskuva matkapuhelinverkkojen tärkeimmistä kehitysvaiheista. Matkapuhelinverkkojen teoriaan perehdyttiin myös.

Työssä tutkittiin käyttäjän todennusta, tiedonkeruuta sekä verkon haavoittuvuutta. Vertailun vuoksi työssä on myös tutkittu, miten käyttäjän todennus tapahtuu 4G-verkossa ja miten se eroaa edellisestä sukupolvesta. Tutkimuksen aikana kävi ilmi, että 3G-verkot ovat hiljattain kehittymässä neljänteen sukupolveen, joten 4G-verkot ja niiden ominaisuuksia on myös työssä mainittu.

Insinöörityön tuloksena syntyi yleiskuva matkapuhelinverkkojen kolmannesta sukupolvesta sekä sen käyttämästä tietoturvasta. Työn tuloksena todettiin myös, että 4G-verkot ovat syrjäyttämässä 3G-verkot alan huipputeknologiana.

Avainsanat	3G, tiedonkeruu, televalvonta, UTRAN

Author Title Number of Pages Date	Antti Tuominen 3G architecture and security 32 pages 25 May 2014
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Telecommunications and Data Networks
Instructor	Dr Tero Nurminen, Principal Lecturer

The aim of this thesis is twofold: to investigate the structure of the 3G network and to gain an understanding about the information security features which interact with the network user. 3G networks and their usage are ubiquitous in everyday life, a key motivating factor behind this thesis. The information in this thesis is mainly gathered from the databases of various standardization organizations, as well as from books related to the field of 3G networking.

The security aspects discussed in this thesis relate to user authentication, lawful interception of user communications and the various vulnerabilities found within the 3G network. A brief history of mobile networks and related theory are also included. These are provided to give the user a general understanding of the important milestones and the pace of evolution within the network.

The current position of 3G technologies in Finland is very strong, but due to customer demand, network operators are slowly upgrading to 4G. In other words, the fourth generation of mobile networks is slowly but surely replacing the existing 3G network. For this reason, 4G networks and their various security features are also mentioned. In conclusion, it is clear that in a few years 4G will have completely overtaken 3G as the most used mobile technology in Finland.

Keywords	3G, Lawful Interception, UTRAN

Sisällys

Lyhenteet

3GPP	*3rd Generation Partnership Project*. Standardointijärjestöjen yhteistyöorganisaaito.
AUC	*Authentication Centre*. Matkapuhelinverkon todennuskeskus.
BS	*Base Station.* Tukiasema.
BSS	*Base Station Subsystem*. Matkapuhelinverkon tukiasemajärjestelmä.
BSC	*Base Station Controller*. Tukiasemaohjain.
CDMA	*Code Division Multiple Access.* Koodijakoinen kanavanvaraustekniikka.
DoS	*Denial of Service*. Palvelunesto hyökkäys.
eNB	*Evolved Node B*. E-UTRAN-radiorajapinnan tukiasema.
EIR	*Equipment Identity Register*. Laiterekisteri.
ETSI	*European Telecommunications Standards Institute*. Standardoimisjärjestö.
FDD	*Frequency Division Duplex*. Taajuusjakoinen dupleksointi.
FDM	*Frequency Division Multiplexing*. Taajuuskanavointi.
GGSN	*Gateway GPRS Support Node.* Yhdyskäytäväsolmu.
GSM	*Global System for Mobile Communications*. Matkapuhelinverkko.
HLR	*Home Location Register*. Kotirekisteri.
IMEI	*International Mobile Equipment Identity*. Matkapuhelimien laitetunnus.

IMSI	*International Mobile Subscriber Identity*. Matkapuhelimen SIM-kortille tallennettu yksilöllinen tunniste.
ITU	*The International Telecommunications Union*. Televiestintäliitto.
LEMF	*Law Enforcment Management Facilty*. Viranomaisten tietokanta.
LI	*Lawful Interception*. Viranomaisten keino kerätä televiestintätietoja käyttäjistä.
LTE	*Long Term Evolution*. GSM-matkapuhelinverkon neljännen sukupolven teknologia.
MIMO	*Multiple Input Multiple Output*. Useamman lähettimen ja vastaanottimen tekniikka.
MSC	*Mobile Switching Center*. Matkapuhelinverkon keskus.
OFDMA	*Orthogonal Frequency Division Multiple Access*. Usean käyttäjän mahdollistava kanavanjakotekniikka.
SIM	*Subscriber Identity Module*. Älykortti, joka sisältää tilaajan tunnistetiedot.
TDMA	*Time Division Multiple Access*. Aikajakoinen kanavanjakotekniikka.
TMSI	*Temporary Mobile Subscriber Identity*. Matkapuhelimen tilapäinen tilaajatunniste.
UMTS	*Universal Mobile Telecommunications System*. Kolmannen sukupolven matkaviestinstandardi.
VLR	*Visitor Location Register*. Matkapuhelinverkon vierailijarekisteri.
WCDMA	*Wideband Code Division Multiple Access.* UMTS-verkoissa käytettävä radiorajapinta.

1 Johdanto

Kolmannen sukupolven matkapuhelinverkot ovat olleet käytössä Suomessa jo yli 10 vuotta. Koska verkon käyttö on osa monen jokapäiväistä toimintaa, halusin tässä työssä perehtyä verkon rakenteeseen ja tietoturvaan.

Insinöörityön tavoitteena on tutkia 3G–verkon pääpiirteitä ja tietoturvaa. Ensin eritellään 3G-verkon arkkitehtuurin eri osa-alueet ja niiden sisältämät elementit. Tämän jälkeen siirrytään eri tiedonsiirtotekniikoihin, jotka ovat oleellinen seikka, jos halutaan ymmärtää miten ja mitä elementtejä verkossa turvataan.

Työssä tutkitaan myös, mitä tietoturva ominaisuuksia on säilytetty edellisen sukupolven verkkoon nähden ja miten niitä on muutettu. Työssä keskitytään lähinnä seikkoihin, jotka vaikuttavat käyttäjään, eli pääsääntöisesti todennukseen ja tiedonkeruuseen. Lopuksi mainitaan eri haavoittuvuuksia, joita verkosta löytyy, sekä verrataan nykyisen verkon tilannetta, uuteen juuri saapuneeseen neljännen sukupolven verkkoon.

Kolmannen sukupolven matkapuhelinverkot ovat nyt saavuttaneet huippunsa, ja on tullut aika kehittää matkapuhelinjärjestelmiä taas eteenpäin. 4G on jo saapunut Suomeen, ja työssä on rinnastettu eri omaisuuksia 3G:n ja 4G:n välillä.

2 Matkapuhelinverkkojen historia

Vuonna 1979 japanilainen Nippun Telephone and Telegraph (NTRR) perusti ensimmäisen matkapuhelinverkon. Pian tämän jälkeen 80-luvulla Yhdysvallat ja Skandinavia seurasivat mallia omilla verkoillaan. Ensimmäisen sukupolven verkot käyttivät analogista siirtotekniikka, jossa puhe muunnettiin korkeammalle taajuudelle, kun taas tulevissa sukupolvissa puhe koodataan kokonaan digitaaliseksi. Ensimmäisen sukupolven matkaviestittäjäjärjestelmä sisälsi automaattisen solukkojärjestelmän, joka hyödynsi kanavanvaihtoa, joka tarkoittaa sitä että puhelut eivät enää katkeilleet siirtyessä solusta toiseen. Samoin kutsuttaessa matkapuhelinta kutsujan ei tarvinnut tietää, missä päin verkkoa kutsuttava liikkui. Nämä verkot olivat myös ensimmäiset verkot, jotka tukivat kansainvälistä toimintaa, vaikka hyvin rajoitetusti. [15.]

Koska 1G:n kattavuus oli melko pienimuotoista, mutta onnistunutta, Euroopassa ruvettiin pohtimaan laajempaa, koko Euroopan kattavaa, matkapuhelinjärjestelmää. Yhteistyö lopulta synnytti GSM-järjestelmän (eng. Global System for Mobile communications) ensimmäisen version joka ilmesty markkinoille 1990-luvun alussa. Toisen sukupolven verkot tarjosivat perinteisiä puhepalveluita sekä tiedonsiirtoa alhaisilla nopeuksilla. Suurin muutos edelliseen sukupolveen verrattuna oli siirtyminen analogisesta siirtotekniikasta digitaaliseen siirtotekniikkaan. Tämä muutos digitaaliseen tarjosi madollisuuden parempaan datapalveluun sekä taajuusspektrin tehokkaampaan käyttöön. GSM:n ensimmäinen versio toimi 900 MHz:n alueella, johtaen nimeen GSM 900. Tulevan kahden vuosikymmenen aikana lukuisia parannuksia tehtiin GSM-järjestelmään ja yleinen terminologia muuttui 2G:stä 2.5G:hen. Järjestelmän parannukset, kuten GPRS (eng. General Packet Radio Service), jotka nostivat tiedonsiirtonopeuksia, nostivat myös verkon suosiota. [15.]

2.5G, eli GPRS, on pakettikytkentäinen laajennus GSM-verkkoon, ja se mahdollistaa tiedon siirtämisen ja vastaanottamisen GSM-verkossa. GPRS on siis eräänlainen Internetin laajennus GSM-järjestelmään. GPRS eroaa edellisistä datansiirtomenetelmistä siten, että tiedonsiirtokapasiteettia varataan vain silloin, kun yhteydellä siirtyy dataa. Edelliset järjestelmät olivat piirikytkentäisiä, ja ne vaativat avoimen yhteyden riippumatta siitä, jos dataa siirrettiin tai ei. [15.]

2G-verkkojen suuri menestys ja Internetin vakiintuminen osoitti, että käyttäjillä oli kasvava kysyntä tiedonsiirrolle. Tämä taivutti teleoperaattorit tutkimaan uusia ratkaisuja, jotka parantaisivat tiedonsiirtoa, samalla jättäen tilaa tulevaisuuden varalle. Suurin toiminnallinen ero edelliseen sukupolveen on, että 3G-verkot käyttävät pakettikytkentäistä tiedonsiirtoa. Tämä mahdollistaa nopeamman tiedonsiirron ja suuremman kapasiteetin, mikä taas loi operaattoreille tilaisuuden tarjota uusia sovelluksia, kuten langaton internet ja videopuhelut. [15.]

Älypuhelimien raskas päivittäinen käyttö osoitti, että 3G-verkkojen tarjoama tiedonsiirto ei riittäisi tulevaisuudessa. Tästä syystä neljännen sukupolven verkot ovat täysin pakettikytkentäisiä IP-verkkoja, jotka käsittelevät puheluita samalla tavalla kuin mikä tahansa muukin internetin läpi kulkeva data. 4G-järjestelmät toimivat sovussa nykyisten 2G- ja 3G-järjestäminen kanssa, mutta tulevaisuuden tavoite on korvata kaikki 4G:llä. [15.]

3 UMTS-verkko

3G-matkapuhelinverkko tunnetaan nimellä UMTS (eng. Universal Mobile Telecommunications System), ja se voidaan jakaa kolmeen osatekijään, jotka yhdessä muodostavat verkon: päätelaite, radioliityntäverkko/radiorajapinta UTRAN (eng. UMTS Terrestrial Radio Access Network) ja runkoverkko (eng. Core Network). Runkoverkko ja radioliityntäverkko ovat loogisia verkkoja, jotka vastaavat tiedonsiirrosta. Nämä kaksi verkkoa päätelaitteen kanssa muodostavat UMTS-matkapuhelinverkon eli kolmannen sukupolven matkapuhelinverkon.

3.1 Arkkitehtuuri

Päätelaite on laite, jolla käyttäjä kytkeytyy verkkoon. Päätelaite on lähes aina matkapuhelin, johtuen siitä että kyseessä on matkapuhelinverkko. Edellisissä verkkosukupolvissa päätelaite tunnistettiin nimellä Mobile Station (MS), mutta 3. sukupolven verkoissa tunniste on muutettu UE:ksi. Päätelaite koostuu vastaanottimesta, lähettimestä, antennista, SIM-kortista ja sen lukijasta. Jokaisella päätelaitteella on ainutlaatuinen tunniste, jonka avulle verkkoon kytkeydytään. [1.]

Radioliikenne päätelaitteen ja UMTS-verkon välillä kulkee UTRAN radioliityntäverkon läpi. UTRAN koostuu useasta radioverkko alijärjestelmästä (eng. Radio Network Subsystem, RNS), jotka ovat liitetty runkoverkkoon. Liityntäverkko sisältää tukiasemat (eng. Node B) ja radioverkko-ohjaimet (eng. radio network controller, RNC). Edellisessä sukupolvessa tukiasemat tunnettiin nimellä BTS (eng. Basestation) ja tukiasemaohjain nimellä BSC (eng. Base Station Controller). Yksi radioverkko-ohjain hallitsee yhtä tai useampaa tukiasemaa. [1.]

Tukiasemat vastaavat solujen sisäisestä viestinnästä kuten signaalin modulaatiosta ja koodauksesta. Tukiasemaohjaimet vastaavat kanavanvaihdosta, solujen siirtymisestä sekä puheluiden muodostamisesta [1.]

Runkoverkon (eng. Core Network) tehtävä on ohjata radioliityntäverkosta tuleva liikenne muihin verkkoihin, kuten julkiseen puhelinverkkoon tai internetiin. Runkoverkko vastaa laskutuksesta, käyttäjän todennuksesta, palvelun jakelusta sekä muista ohjaustehtävistä. [1.]

Runkoverkko koostuu seuraavista komponenteista:

MSC (eng. Mobile Switching Center) tunnetaan radiopuhelinkeskuksena. MSC:n tehtävä on käsitellä verkon sisäiset yhdistämispyynnöt ja ohjata tekstiviestien ja puheluiden yhdistykset. [1.]

GMSC (eng. Gateway Mobile Switching Center) on radiopuhelinkeskuksen yhdyskäytävä joka yhdistää MSC:n perinteiseen puhelinverkkoon PSTN (eng. Public Switched Telephone Network). [1.]

HLR (eng. Home Location Register) on kotirekisteri, joka sisältää liittymän tiedot jokaisesta käyttäjästä ja siitä, mitä käyttöoikeuksia heillä on verkon sisällä. Nämä tiedot on määritelty käyttäjän IMSI (eng. International Mobile Subscriber Identity) -tilaajatiedoissa. [1.]

VLR (eng. Visitor Location Register) on vierailijarekisteri, joka tilapäisesti tallentaa käyttäjän tiedot, kun käyttäjä vaeltaa esimerkiksi vieraan operaattorin alueella tai vieraassa maassa. [1.]

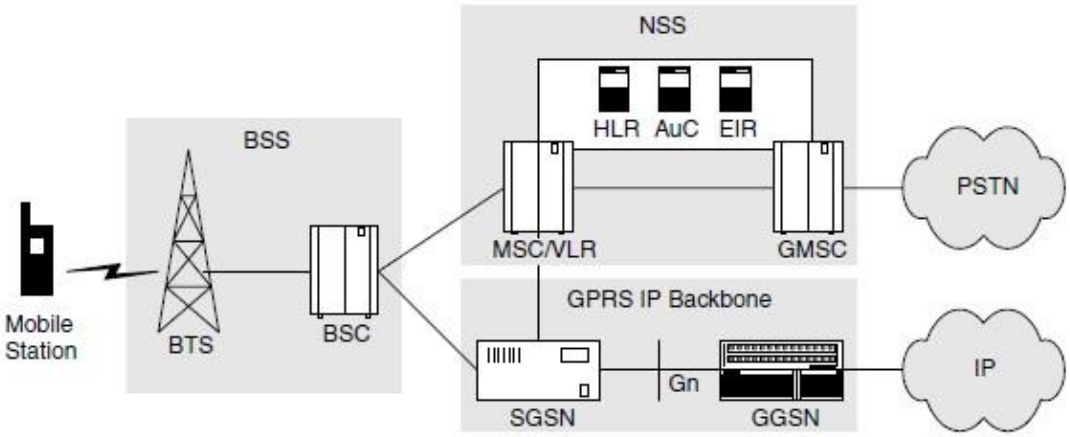
AuC (eng. Authentication Center) on todennuskeskus, joka suorittaa käyttäjän todennuksen SIM-kortin avulla. [1.]

SGSN (eng. Serving GPRS Support Node) on kytketty radioverkko-ohjaimeen ja toimii palvelevana pisteenä päätelaitteelle. SGSN vastaa pakettikytkentäisen tietoliikenteen todennuksesta ja reitityksestä. 3G-tekniikkassa SGSN tunnetaan myös nimellä 3G SGSN. [1.]

GGSN (eng. Gatway GPRS Support Node) toimii yhdyskäytävänä ulkoisiin verkkoihin. GGSN vastaanottaa muilta verkoilta liikennettä ja lähettää sen päätelaitteelle. GGSN myös välittää liikennettä, joka syntyy päätelaitteen toimesta, lähettäen sen enteenpäin.

3.2 Verkon kehitys

Kolmannen sukupolven matkaviestintäverkot tukevat kaikkia tietoliikennetyyppejä: puhetta, videota ja dataa. Johtava teknologia tämän kasvun takana on Internet-protokolla (IP), joka oli alun perin implementoitu GSM runkoverkkoon GPRS-laajennuksella joka tunnettiin 2.5G-verkkona. Kuva 1 esittää GPRS-verkon komponentit ja sen, miten ne on liitetty nykyiseen GSM-verkkoon. [10.]



Kuva 1. GPRS-verkon yleinen arkkitehtuuri [10.]

Gn-rajapinta kytkee SGSN:n (eng. Serving GPRS support node) ja GPRS yhdyskäytävän (eng. Gateway GPRS support node, GGSN) käyttäen tunnelointiprotokollaa GTP (eng. GPRS Tunneling Protocol). Tämän infrastruktuurin päätarkoitus on tarjota yhteyksiä ulkopuolisiin pakettikytkentäisiin verkkoihin, kuten internetiin tai yrityksen intranetiin. Teknologialla saadaan internetin käyttämä IP-protokolla käyttöön puhelinverkoissa, mikä mahdollistaa datapalvelujen käytön matkapuhelimella, kuten esimerkiksi sähköpostin lukemisen tai internetin selailun. Oleellinen osa pakettikytkentäistä teknologiaa on laskutuksen suorittaminen tiedon määrän mukaan, eikä sen mukaan, kuinka kauan yhteys on auki. [10.]

Kun GSM-verkosta siirrytään UMTS-verkkoon, yksi suurimmista muutoksista koskee radioliityntäverkkoa (RAN). Päätelaitteet kommunikoivat tukiasemien kanssa käyttäen koodinjakokanavointia (CDMA) ja sen laajakaistaista versiota WCDMA:ta (eng Wideband CDMA). UMTS-verkoissa on myös käytössä asynkroninen tiedonsiirtotapa ATM (eng. Asynchronous Transfer Mode). Nämä muutokset on tehty, jotta samassa

verkossa voidaan tukea puhe-, video- ja datapalveluja. Kuten kuvasta 2 myöhemmin nähdään, runkoverkko on pysynyt suurin piirtein samana kuin edellisessä sukupolvessa, lukuun ottamatta ohjelmistopäivityksiä. Nähdään myös, että IP-pohjainen teknologia ylettyy syvemmälle verkossa, koska radioverkko-ohjain (RNC) siirtää nyt dataa 3G SGSN:llä käyttäen IP-protokollaa. Seuraavaksi tutkitaan, mitkä kaikki komponentit ovat muuttuneet verkkojen kehittyessä 3G:hen ja miten. [10.]

WCDMA Tukiasemat

3GPP-spesifikaatiot määrittelevät tukiasemat termillä Node B, joka poikkeaa edellisen sukupolven Baste Station (BTS) -merkintätavasta. Virallisesti Node B on yksi kokonaisuus mikä palvelee yhtä solua. Tosin oikeassa maailmassa, johtuen ekonomisista syistä, tukiaseman alue on sekoroitu, ja tukee siten useita soluja kaikilta käytettäviltä taajuuksilta. Node B:n täytyy tukea WCDMA- ja ATM-tiedonsiirtomenetelmiä, joissa on käytössä osittain- tai täysin- synkroninen digitaalinen hierarkia (PDH tai SDH). [10.]

SDH on synkronoidulle tiedonsiirrolle standardoitu teknologia, joka helpottaa eri järjestelmien yhtyeenliitettävyyttä, koska kello on synkronoitu koko järjestelmän läpi. PDH on vanhempaa tekniikkaa, jota käytettiin kahden suoran liityntäpisteen välillä (eng. point-to-point). Tästä syystä kellon ei tarvitse olla synkronoitu koko järjestelmän sisällä, ja tämä aiheuttaa ongelmia järjestelmän yhteensopivuuden kanssa. [10.]

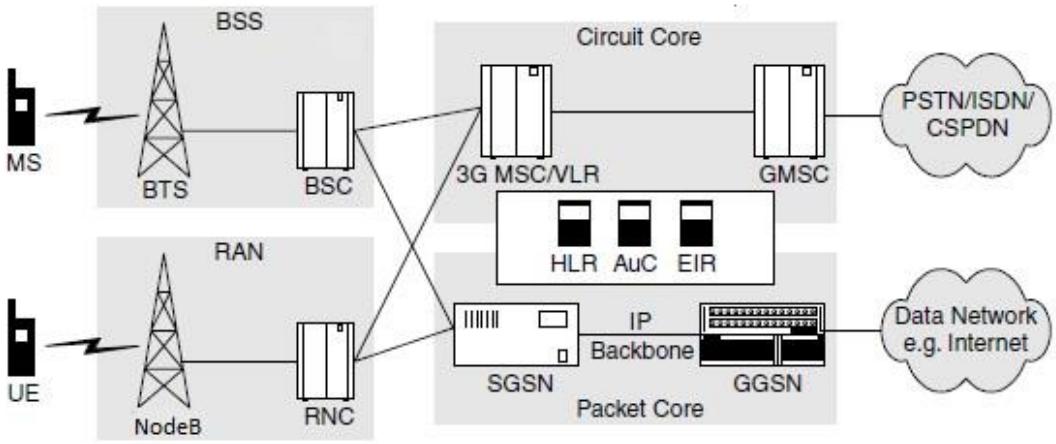
Toisin kuin GSM-järjestelmässä, solun koko ei ole vakio. CDMA-pohjaisissa puhelinverkoissa solut voivat "hengittää" (eng. Cell breathing). Tämä mekanismi mahdollistaa ylikuormitettujen solujen siirtävän osan kuormituksesta naapurisoluille. Ylikuormitetut solut kutistavat alueitansa samalla kun naapurisolut kasvattavat alueitansa kompensaationa. Näin liikennettä voidaan siirtää solusta soluun ja tasapainottaa kuormitusta. [10.]

Radioliityntäverkon ydin on myös korvattu uudella radioverkko-ohjaimella RNC. RNC ohjaa kaikkia tukiasemia jotka siihen on kytketty ja ylläpitää yhteyksiä sekä piirikytkentäiseen että pakettikytkentäiseen runkoverkkoon. Radioverkko-ohjain on kytketty puhelinkeskukseen (MSC) piiripuolella ja SGSN:ään pakettipuolella. Yksi muutos edellisen sukupolven tukiasemaohjaimeen on RNC:n kyky liittyä toiseen radioverkko-ohjaimeen. Melkein kaikki RNC:n tekemät päätökset ovat

sovelluspohjaisia, joten korkeampi prosessointikapasiteetti on tarvittu. Yksi esimerkki tästä on radioresurssien hallinta (eng. Radio resource management, RMM). [10.]

UTMS-evoluutio etenee julkaisujen (eng. release) mukaan. Ensimmäinen näistä julkaisuista oli Release 99 (R99), joka on nähtävissä kuvassa 2. Release 99 julkaistiin vuonna 2000, ja se määrittelee ensimmäiset UMTS 3G-verkot, jotka käyttävät CDMA:ta. UMTS R99-julkaisussa muutokset runkoverkkoon olivat minimaalisia ja koskivat lähinnä ohjelmistopäivityksiä, joiden avulla saavutettiin tuki uudelle radiorajapinnalle.

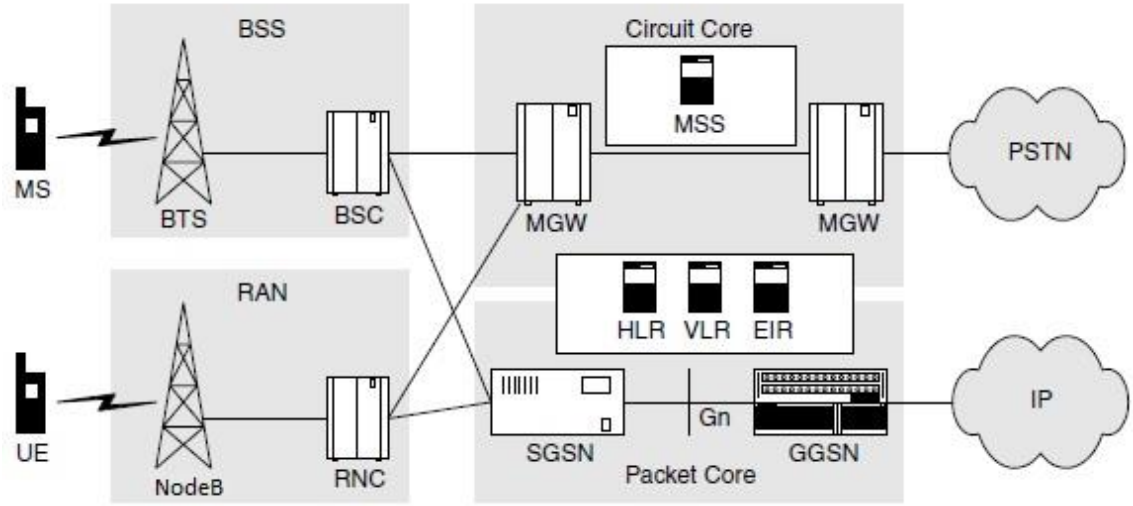
Yksi muutos oli kuitenkin MSC:n päivittäminen 3G MSC -järjestelmäksi. 3G MSC:n rooli oli täysin identtinen MSC:n nähden, mutta koska käytössä oli erilainen modulaatiotekniikka, tarvittiin yhteiskäyttötoiminta (eng. interworking function, IWF), jonka avulla yhteensopivuus 2G-järjestelmiin oli saavutettavissa. IWF tarvittiin radioliityntäverkon (RNC) ja MSC:n välille, ja sen tehtävänä oli hoitaa puheen koodaus 2G:lle yhteensopivaksi. Lisäksi tehtäviin kuului signalointi MSC:n ja RAN:in välillä RANAP -protokollalla. Käytännössä voidaan ajatella, että 3G MSC on IWF:n ja 2G MSC:n yhdistelmä. IWF tunnetaan myös mediayhdyskäytävänä (MGW), joka on erillinen laitteistoalusta, jota voidaan käyttää uudelleen tulevissa UMTS-julkaisuissa, kun ruvetaan siirtämään liikennettä TDM-, ATM- ja IP-teknologioilla. [10.]



Kuva 2. UMTS release 99 -matkapuhelinverkko [10.]

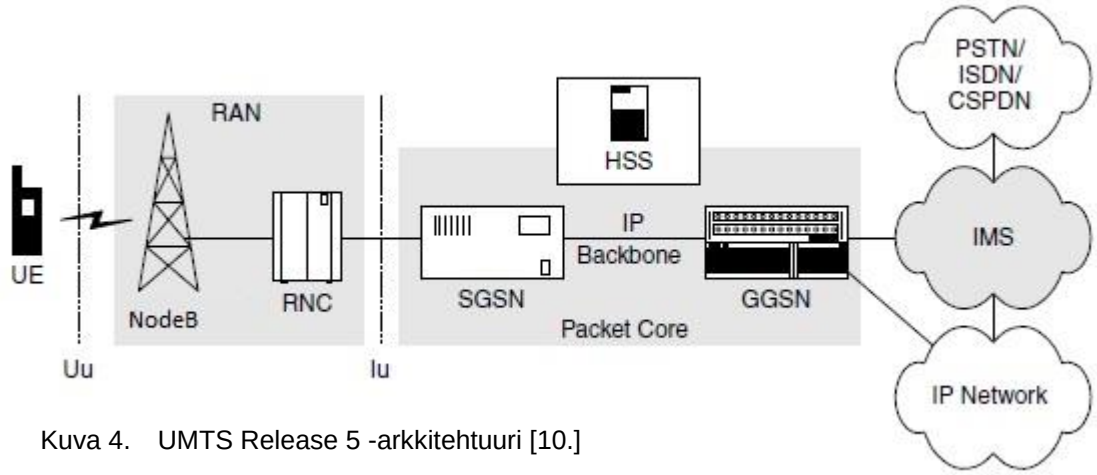
3.3 Verkon evoluutio

Seuraava askel evoluutiossa Release 99:n jälkeen oli Release 4, joka julkaistiin vuonna 2001 (kuva 3). Suurin muutos oli GSM-verkon ytimen infrastruktuurin muuttaminen IP-verkoksi joka perustuu IP-puhe protokollaan VoIP. Muutos johti MSC:n pilkkomisen kahdeksi eri komponentiksi: mediayhdyskäytäväksi (MGW) ja puhelinkeskuspalvelimeksi (eng MSC server, MSSC). Tämä ratkaisu on hyvin skaalatutuva, koska yksi MSS voi hallita useita MGW-laitteita. [10.]



Kuva 3. UMTS Release 4 -arkkitehtuuri [10.]

Näiden muutoksien jälkeen 3G-verkoissa oli useita internet pilviä, ja oli aika yhdistää ne yhdeksi Ii-verkoksi (eng. all-IP network). Release 5 (kuva 4), joka julkaistiin vuonna 2002 toteutti tämän tavoitteen. R5-arkkitehtuurissa määritettiin IP-multimedia-alijärjestelmä (eng. IP Multimedia Subsystem, IMS) jonka tarkoituksena oli tuoda internetpohjaisia palveluita muun muassa GPRS-verkkoon. IMS-alijärestlemän ansiosta IP-teknologia ylettyi nyt koko verkon yli, runkoverkosta tukiasemaan asti. Toinen merkittävä muutos oli kotirekisterin, vierailijarekisterin ja laiterekisterin yleistäminen yhdeksi alijärjestelmäksi nimeltä HSS (eng Home subscriber server). HSS on siis tietokanta, joka tukee IMS-verkossa olevia kokonaisuuksia, jotka käsittelevät puheluita. [10.]



Kuva 4. UMTS Release 5 -arkkitehtuuri [10.]

3.4 Fyysinen kerros

Puhelimien jatkuva kehitys on johtanut median käyttötapojen muuttumiseen. Nykypäivänä mediaa toistetaan reaaliajassa älypuhelimella verkon ylitse. Tämä nosti tarvetta tiedonsiirron nopeuden ja kapasiteetin kasvattamiseksi, sekä kaistanleveyden optimointiin jotta vasteaika saataisiin pienemmäksi. Verkon fyysisessä kerroksessa (eng. Physical Layer) on käytetty eri teknologioita, kuten MIMO (eng. Multiple In Multiple Out) ja WCDMA (eng. Wideband Code Division Multiple Access), joiden tarkoitus on ratkaista nämä ongelmat.

UMTS-verkot käyttävät pääsääntöisesti WCDMA-tekniikka radiorajapinnan tiedonsiirron standardina. WCDMA tukee FDD- (eng .Frequency –Division Duplexing) ja TDD- (eng. Time Division Duplexing) tekniikoita. WCDMA joka pohjautuu FDD-tekniikkaan hoitaa tiedonsiirron 5 MHz leveillä taajuuksilla, jotka on määritetty tukiaseman ja päätelaitteen käyttöön. Euroopan komissio on määrittänyt taajuudet 1920–1980 MHz paluusuunnan käyttöön ja taajuudet 2119–2170 MHz myötäsuunnalle. TDD-tekniikka eroaa FDD-tekniikasta siten, että samaa taajuusaluetta käytetään tiedonsiirron molempiin suuntiin. Tiedonsiirto tapahtuu vuorosuuntaisesti taajuusalueilla 1900–1920 ja 2020–2025 MHz. WCMDA lupaa teoreettisesti 2 Mbps:n tiedonsiirtonopeuden, mutta käytännössä enintään 394 kbps:n nopeuden. [3.]

MIMO-tekniikka on tietoliikenne antennitekniikka, jossa käytetään lähetykseen ja vastaanottoon samanaikaisesti useampaa kuin yhtä antennia. MIMO-tekniikka on suosittu ratkaisu 3. ja 4. sukupolven verkoissa, koska se tuo langattomaan tiedonsiirtoon useita parannuksia. Parannuksia on nähtävissä muun muassa linkin kantamaetäisyydessä ilman kaistanleveyden kasvattamista tai tehon (virrankulun) nostoa. MIMO-tekniikkaa voidaan hyödyntää kahdella tavalla: tiedonsiirtonopeuden maksimointiin tai tiedonsiirron luotettavuuden parantamiseen. On olemassa useita eri MIMO-malleja, joilla on päädytty näihin tavoitteisiin, pääsääntöisesti ne voidaan jakaa kolmeen eri tekniikkaan: spatial multiplexing, diveristy coding ja precoding. [2.]

Tiedonsiirtonopeuden maksimointiin käytetään MIO-SM -tekniikkaa (eng. MIMO Spatial Multiplexing). Kun vastaanottajalla on käytössä vähintään yhtä monta antennia kuin lähettäjällä, voidaan antennipareja käyttää yksilöllisesti. Lähetettävä viesti pilkotaan erillisiksi tietovirroiksi ja lähetetään rinnan samanaikaisesti samalla lähetyskanavalla. Pilkottu signaali saapuu vastaanottajalle epämääräisessä järjestyksessä, ja kun kaikki osat ovat saapuneet, voidaan signaali kasata yhdeksi kokonaisuudeksi. Tämä tekniikka nostaa tiedonsiirtokapasiteettia verrattuna siihen, jos käytettäisiin vain yhtä antennia. [2.]

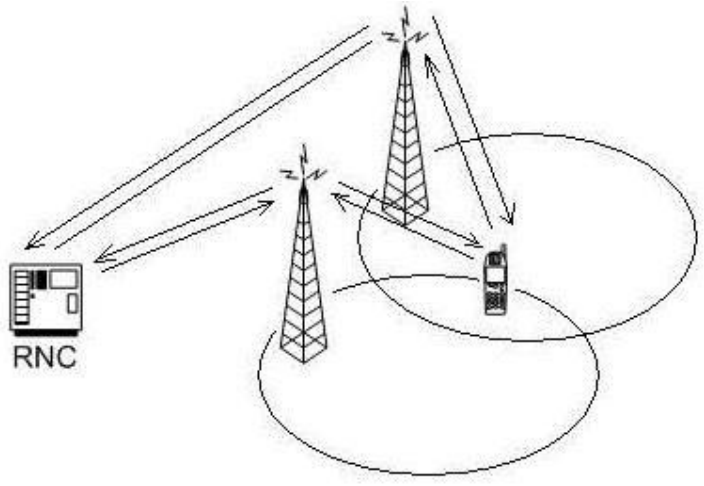
Jos tavoitteena on maksimoida tiedonsiirronluotettavuus kapasiteetin sijasta, voidaan käyttää aika-tilakoodausta (eng. space time coding , diversity coding). Tässä mallissa sama signaali lähetetään useammasta antennista samanaikaisesti. Menetelmä laskee virheiden todennäköisyyttä ja on hyvä ratkaisu, jos vastaanottimen antennimäärä ei ole tiedossa. [2.]

Precoding-tekniikalla on tarkoitus painottaa antenneista lähetettyjä signaaleita kanavatilojen mukaan (eng. Channel State Information, CSI). Jokaisella käytössä olevalla kanavalla on CSI-tietoja, joiden avulla voidaan soveltaa optimaaliset asetukset signaalin lähetykselle. Tämä on erittäin hyödyllistä, kun kyseessä on korkeat tiedonsiirtonopeudet. Tällä menetelmällä pyritään tuottamaan vastaanottajalle kokonaissignaali, jolla on paras mahdollinen signaali-kohinasuhde. [2.]

3.5 Solunvaihto

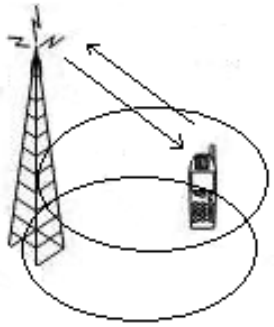
Matkapuhelimen liikkuessa alueelta alueelle on tarve suorittaa solunvaihtoja (eng. Handover), jotta yhteys matkapuhelinverkkoon pysyy yllä ja palvelunlaatu hyvänä. RNC seuraa tukiaseman saamaa matkapuhelinsignaalia, asettaen signaalin laadulle tietyt raja-arvot. Jos matkapuhelimensignaali kyseisellä kanavalla katsotaan olevan raja-arvoa heikompi, RNC suorittaa kanavanvaihdon, ja uudella alueella solunvaihdon. Vaihto onnistuu vain, jos parempi kanava on saatavilla. Solunvaihdon tärkein tehtävä on ylläpitää menossa olevia puheluita vaihdonaikana, estäen puhelun katkoksen siirron aikana. Matkapuhelin pitää jatkuvaa kirjaa radiolinkeistä ja lisää tai poistaa niitä muistista tarpeen mukaan. Tapauksia on kolme erilaista: soft handover, softer handover ja hard handover. [14.]

Soft Handover, Ns. ”pehmeä luovutus” (kuva 5) tapahtuu, jos matkapuhelimen kuuluvuus alueella on useampi samoilla taajuuksilla toimivia tukiasemasoluja, joihin matkapuhelin muodostaa samanaikaisen yhteyden. Koska matkapuhelin on kiinni useamassa tukiasemassa samanaikaisesti, onnistuu solunvaihto helposti. Kun yhteys tiettyyn tukiasemaan ei enää toimi tai on liian heikko, yhteys tukiasemaan katkaistaan, ja viestintä jatkuu muilla käytössä olevissa tukiasemayhteyksissä. [14.]



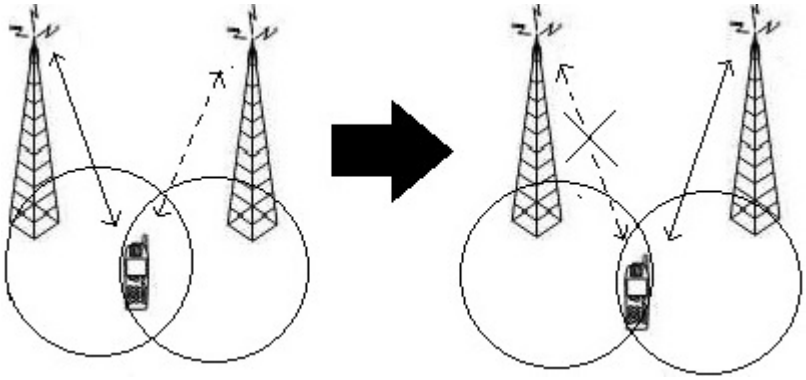
Kuva 5. Soft handover

Softer handover on erikoistilanne (kuva 6) jossa matkapuhelin muodostaa useamman yhteyden samaan tukisameaan. Näin voi käydä, jos matkapuhelin on saman tukiaseman kahden eri sektorin vaikutusalueella, ja yhteys samaan tukiasemaan muodostetaan kummankin sektorin kautta. [14.]



Kuva 6. Softer handover

Käytännössä hard handover (kuva 7) tarkoittaa sitä, että puhelimen muistista poistetaan kaikki vanhat radiolinkit ennen kuin uudet yhteydet uusiin tukiasemiin muodostetaan. Käyttäjä saattaa kokea lyhyen katkoksen yhteydessä vaihdon aikana. Tämänlainen solunvaihto tapahtuu aina, kun matkapuhelin siirtyy eri taajuudella toimivien solujen välillä. [14.]



Kuva 7. Päätelaite etsii uutta tukiasemayhteyttä ja katkaisee vanhan yhteyden ennen uuden muodostamista

3.6 Palvelunlaatu

Palvelunlaatu (eng. Qaulity of service) on termi, jolla tarkoitetaan tietoliikenteen luokittelua ja priorisointia. Käyttäjää ei kiinnosta, miten hänen haluamansa palvelut tarjotaan, mutta käyttäjää kiinnostaa, onko hän tyytyväinen palvelun laatuun. Tämä näkökulma on erittäin subjektiivinen, ja jos käyttäjä ei ole tyytyväinen, voi hän vaihtaa operaattoria. Verkon operaattoriin kannalta QoS vaatii paljon teknistä analyysiä ja osaamista kiertää haasteita tietyissä kustannusrajoitteissa. [11.]

3G-verkot tarjoavat monipuolisia palveluja, joista jokainen tarvitsee omat QoS-parametrinsa. Esimerkiksi multimediapuhelu saattaa sisältää puhetta ja videota, jolloin kummallekin tietovirralle täytyy määrittää QoS-parametrit. Jokainen palvelu asettaa tiettyjä vaatimuksia lähetystielle, jolla kyseistä palvelua kuljetetaan käyttäjälle. Julkisissa puhelinverkoissa kannetaan useita palveluja ja palvelupyyntöjä samanaikaisesti. Jokainen näistä palveluista sisältää omat parametrinsa tiedonlähetykselle. Koska verkon resurssit ovat rajallisia, QoS:n ideana on jakaa juuri tarpeeksi resursseja jokaiselle palvelulle/pyynnölle. Teoriassa olisi mahdollista tehdä erittäin monimutkaisia QoS-määritelmiä jokaiselle palvelulle, mutta tämä vain hankailuttaisi verkon toimintaa, koska mitä monimutkaisempia määritelmät ovat, sitä enemmän QoS-hallintaa tarvitaan verkossa tiedonsiirtämisen lisäksi. Tästä syystä UMTS käyttää yksinkertaista QoS mallia joka koostuu 4. liikenneluokasta ja muutamasta attribuutista joilla määritellään liikenteen pääpiirteet. Luokat ovat:

- QoS - conversational class
- QoS - streaming class
- QoS - interactive class
- QoS - background class [11.]

Sovellukset, jotka käyttävät conversational-luokkaa ovat puhe, VoIP ja videopuhelut. Koska reaaliaikaiset keskustelut käydään aina ihmisten välillä, tämä on ainoa luokka, jossa vaadittavat QoS-piirteet perustuvat käyttäjän kokemuksiin. Tässä liikenneluokassa liikenteelle on ominaista alhainen viive ja alhainen viiveen vaihtelu.

Viiveen maksimiarvo on suoraan riippuvainen siitä, paljonko käyttäjät kestävät viivettä. [11.]

Streaming-luokkaa käytetään kun käytössä on suoratoistoinen videotiedosto tai äänitiedosto. Tässä liikenneluokassa kyse on lähinnä yksisuuntaistaseista tiedonsiirrosta palveluntarjoajalta päätelaiteeseen. Yleensä vastaanottava päätelaite on aika-kohdistettu (eng. Time-alligned), ja tämä tapahtuu päätelaitteen sovelluksella, jolla kyseistä mediaa toistetaan. Vaatimukset viiveen vaihtelulle on siis asetettu päätelaitteen sovelluksen kautta. Koska tämä liikennetyyppi on pääsääntöisesti yksisuuntainen, pidemmät viiveet ovat hyväksyttäviä verrattuna conversational-liikenneluokkaan. [11.]

Interactive-liikenneluokka kuvastaa datakommunikaatiomallia, jonka parametrit määräytyvät käyttäjän pyyntö- ja vastauskuvioiden mukaan. Kun viesti saapuu kohteeseen, jää järjestelmä odottamaan vastausta tietyksi ajaksi. Tästä syystä kaikista tärkein attribuutti luokassa on edestakainen viive (eng. Round-trip delay time). Sovelluksia tässä luokassa ovat esimerkiksi internetin selailu ja hakutoiminnat tietokannoissa. [11.]

Background-liikenneluokassa käyttäjä ei odota tiedon saapumista tietyn ajanjakson aikana. Tiedonlähetys ja vastaanotto tapahtuvat taustalla käyttäjän huomaamatta. Esimerkkeinä tästä ovat sähköpostien ja tekstiviestien lähettäminen. Tämä luokka ei ole ajallisesti herkkä ja tärkein attribuutti on tietosisällön säilyttäminen. [11.]

3.7 Protokollat

Kuten aikaisemmin mainittiin, UMTS-arkkitehtuurin kokonaisuus koostuu kolmesta eri osasta: päätelaite, UTRAN-radiorajapinta ja runkoverkko. Päätelaitteen ja radiorajapinnan välissä on radiorajapinta Uu, kun taas rajapinta runkoverkon ja UTRAN:in välissä on Iu. On oleellista mainita rajapintojen toiminta, koska ne ovat selkeästi määrittelyjä standardeja, joiden mukaan eri valmistajat ja operaattorit ovat yhteensopivia kaikissa UMTS-verkoissa. [10.]

Radiorajapinta protokollat voidaan jakaa joko käyttäjätason (eng. user plane) tai hallintatason (eng. control plane) protokolleiksi. Nimensä mukaan käyttäjätason

protokollat kantavat käyttäjän dataa, kun taas hallintatason protokollat ylläpitävät yhteyksiä päätelaitteen ja verkon välillä. Protokollat koostuvat kolmesta eri kerroksesta: fyysisestä kerroksesta (eng. Physical layer, Layer 1), siirtoyhteyskerroksesta (eng. Data link layer, Layer 2) ja verkkokerroksesta (eng. Network Layer, Layer 3). Protokollapinon tarkoitus on asettaa ne palvelut käyttöön, joita tarvitaan tiedonvälitykselle. [10.]

Layer 1 -kerrokseen kuuluvat palvelut, joilla välitetään liikenne fyysisentason kanavia pitkin ylemmille kerroksille. Tähän kuuluu toimintoja, kuten kuljetuskanavien luonti laitteessa, virheidenhallinta ja palvelunlaadun mittaukset, kuten bittivirheet, signaali-kohinasuhde ja tehonsäätö. [10.]

Layer 2 -kerros on jaettu MAC- (eng. Medium Access Control), RLC- (eng. radio link control), PDCP- (packet Data Convergence Protocol) ja BMC (eng. Broadcast/Multicast Control) -osajärjestelmiin. MAC on verkon varaamisen ja itse liikennöinnin hoitava osajärjestelmä. RLC hoitaa siirron vastaanottavalle laitteelle ja välittää käyttäjän liikenteen sekä palvelunlaatuasetukset. Siirto voidaan saavuttaa kolmella eri tilalla: transparent modella (TM), unacknowledged modella (UM) ja acknowledge modella (AM). PDCP:n tehtävänä on pakata ja purkaa tietovirtoja, esimerkiksi internetliikennettä, sekä välittää käyttäjän dataa. BMC sovittaa lähetys ja monilähetyspalveluita radiorajapinnalla käyttäjän liikenteelle. [10.]

Layer 3 -kerros koostuu RRC-protokollasta, joka hoitaa radioresurssien hallinnan. RRC on radioverkonhallintaprotokolla, joka tarjoaa funktiot liittyen verkon transmission hallintaan ja ylläpitoon. Tähän liittyy muun muassa MAC-, RLC- ja PDCP-kerroksien hallinta. RRC:n päätehtävä on luoda ja ylläpitää tarvittavat radioyhteydet päätelaitteen ja verkon välillä. Tähän kuuluu muun muassa solujen valinta ja vaihtotoiminnat. RRC on siis hallinta protokolla päätelaitteen ja RNC:n välillä. RRC toimii yhteystyössä kaikkien kerroksien kanssa, jotta kaikki tarvittavat tiedot ovat saatavilla yhteyksien hallintaan. [10.]

4 3G:n tietoturva

Kuten muissakin järjestelmissä, käyttäjän toimintatavat ovat suurin haaste tietoturvasuunnittelussa. Käyttäjät olettavat helppokäyttöistä (eng. Ease of use) järjestelmää, jossa viestintä tapahtuu välittömästi ja vaivattomasti. Tämä rajaa pois pitkät käyttäjän syöttämät salasanat ja jatkuvat todennus ponnahdukset. On myös hyvin yleistä että käyttäjän päätelaite varastetaan tai katoaa, jolloin pitää olla mekanismi jolla sulkea kyseisen päätelaitteen kyky käyttää verkkoa. Päätavoitteet luotettavan järjestelmän suunnittelussa ovat estää järjestelmän laiton käyttö, tietojen luottamuksellisuuden säilyttäminen ja taata palveluiden käyttö oikeutetuille asiakkaille. [4.]

4.1 GSM-verkon ominaisuuksien säilyttäminen

Toisen sukupolven verkot oli suunniteltu tietoturva mielessä, verkko vastasi sen ajan tarpeisiin ja haasteisiin. Teknologian jatkuva kehitys on muuttanut matkapuhelinverkon tarpeita ja tästä alkoi kolmannen sukupolven verkkojen kehitys. Tärkeimpänä ratkaisuna oli päätös siitä, että 3G-verkko rakennetaan edellisen sukupolven päälle. Tämä tarkoitti sitä, että edellisen sukupolven teknologioiden turvallisuuden parantaminen on suotuisaa sen sijasta, että heitettäisiin kaikki pois ja aloitettaisiin alusta. Budjettisyistä tuskin kukaan operaattori olisi valmis aloittamaan puhtaalta pöydältä. Edellisen sukupolven päälle rakentaminen takaa myös korkeatasoisen yhteensopivuuden. [4.]

SIM-pohjainen todennus

Paikallinen (eng. home enviorment, HE) operaattori pystyi hallitsemaan verkon käyttöä älykortilla, joka tunnetaan termillä SIM (eng. Subscriber Identity Module). Sim-kortti on irrotettava turvallisuusmoduuli jona ylläpitäjänä/jakajana toimii paikallinen operaattori. SIM-pohjainen todennus on suotuisaa koska se täyttää aikaisemmin mainitun Ease of Use -ehdon. SIM-pohjainen todennus ei vaadi lisätoimenpiteitä käyttäjältä ja nelinumeroinen PIN-tunniste on yhtä helppo muistaa kuin oma henkilötunnus. [4.]

2G-verkon standardointi dokumenteissa SIM-kortin määritelmä kattoi koko laitteiston ja sen sisällä olevan ohjelmiston. UMTS verkkojen kehitysvaiheessa määritelmä muutettiin siten, että termi SIM kattaa vain ohjelmiston. SIM-kortin käyttämä laitteisto määriteltiin UICC:ksi. UICC vastaa rooliltaan vanhaa SIM-korttia, mutta siinä on uusi ominaisuus nimeltään USIM (eng. Universal Subscriber Identity Module). USIM sisältää tiedot verkon käyttäjän identiteetistä, jotta hänet voidaan todentaa, sekä parannettuja salaustoimintoja, kuten pidennetyt salausavaimet. Modernissa 3G-verkossa SIM-kortin sijasta on käytössä UICC, joka kostuu SIM:istä ja USIM:istä. [4.]

3G-verkko säilyttää myös pyyntö ja vastaus (eng. challenge and acknowledge) mekanismin joka perustuu salaiseen avaimeen SIM moduulin ja AuC:n välillä. Kyseinen ”keskustelu” on rajattu SIM Moduulin ja AuC:n väliseen paikalliseen verkkoon. Toisin sanoen, luottamuksellisen tiedon kulkureitti on minimissään, mikä hankaloittaa sen varastamista. [4.]

Radiorajapinta ja tilaajan tietoturva

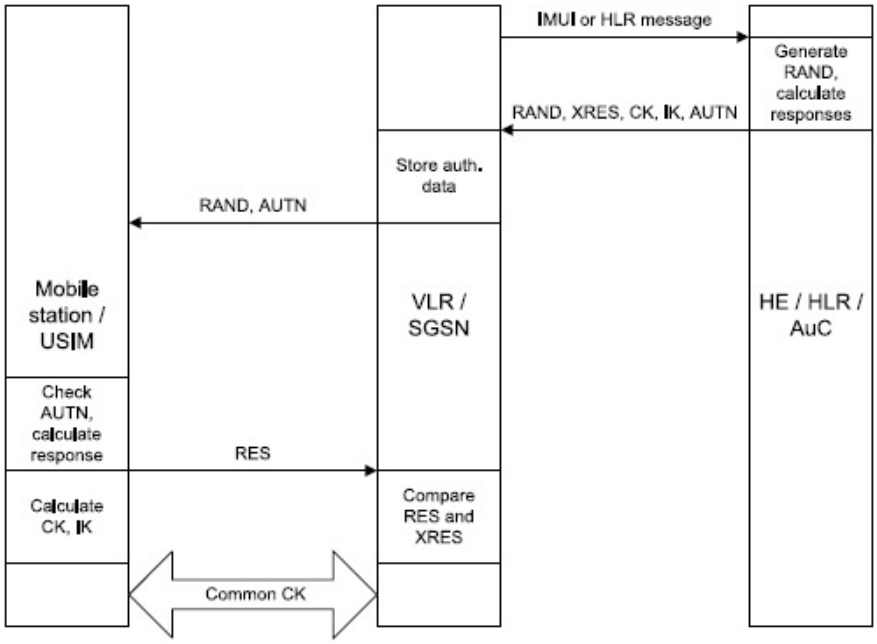
IMSI (eng, International Mobile Subscriber Identity) on numerosarja, joka on tallennettu puhelimen SIM-kortille. Jokaisella GSM/UMTS-verkon käyttäjällä on ainutlaatuinen numerosarja, jonka avulla käyttäjä voidaan tunnistaa. Päätelaite lähettää tämän numerosarjan verkkoon sisäänkirjautuessa, jonka jälkeen numerosarjaa verrataan operaattorin tietokantaan, jonka perusteella hänet todennetaan. Tietoturvasyistä IMSI-tunnusta ei lähetetä kuin verkon sisäänkirajutumisen yhteydessä, tämän jälkeen asiointi tapahtuu TMSI-tunnuksella. HLR-rekisteri todentaa IMSI-tunnuksen ja muuttaa sen väliaikaiseksi (eng. Temporary MSI, TMSI). TMSI on väliaikainen ja ainutlaatuinen sille alueelle jossa käyttäjä liikkuu. TMSI yleensä muuttuu kun käyttäjä liikkuu vierailijarekisteristä vierailijarekisteriin. TMSI vähentää oikean MSI:n altistusta radiorajapinnan yli ja täten estää tiedonkeräyksiä käyttäjän palveluista tai paikantamisesta. [4.]

4.2 Todennus

3G-verkon todennusprosessi alkaa aina päätelaitteen pyynnöstä. Todennusprosessi perustuu päätelaiteen USIM:n ja HLR:n tietokantaan tallennettuun K-avaimeen, jonka vain USIM ja HLR:n todennuskeskus AuC tietävät. Kuva 8 esittää todennusprosessin kokonaisuudessaan.

Päätelaitteen tunnistaminen alkaa, kun USIM lähettää IMSI-tiedot palvelevalle verkolle. Seuraavaksi palveleva verkko lähettää ”authentication data request”-pyynnön kotiverkon todennuskeskukselle jossa salattu K-avain ja IMSI-tiedot sijaitsevat. Näiden tietojen avulla todennuskeskus laskee todennusvektorit (eng. authentication vectors) joihin sisältyy numerosarja (eng. seqneunce number) SQN ja satunnainen numero RAND. Verkko lähettää päätelaitteelle vastauksena todennuspyyntö ”user authentication request”-sanoman joka sisältää parametrit RAND ja AUTN (eng authentication token). AUTN sisältää aikaisemmin mainitun SQN-numeron ja anonyymisen avaimen AK, joka on laskettu tietokannassa sijaitsevasta K-avaimesta ja satunnaisesta luvusta.

Saamansa RAND:n ja AUTN:n avulla päätelaitteen USIM suorittaa K-avaimella todennuslaskelmat. Päätelaite lähettää laskemansa arvon ”user authentication response” RES-viestillä. Seuraavaksi SN vertailee päätelaiteelta saamaansa RES-arvoa todennuskeskuksen generoimaan todennusvektoriin XRES. Jos arvot täsmäävät, käyttäjän todennus on suoritettu ja yhteys otetaan käyttöön. [5.]



Kuva 8. Päätelaitteen ja verkon suorittama todennusprosessi [5.]

Todennusprosessi on yritetty pitää niin salaisena kuin mahdollista. AuC:n luomassa todennusvektoreissa sekvenssinumero SQN on kasvava luku, jolla varmistetaan että sama numero ei esiinny toista kertaa. Satunnaisluku RAND on 128-bittinen, joka sisältyy myös todennusvektoriin. Laskennassa käytetään viittä eri funktiota, jotka ovat fi, f2,f3,f4 ja f5. Funktiot f2-f4 käyttävät parametreja K ja RAND, kun taas f1-funktio käyttää arvoja K, RAND, AMF ja SQN. [6.]

4.3 Telekuuntelu ja -valvonta

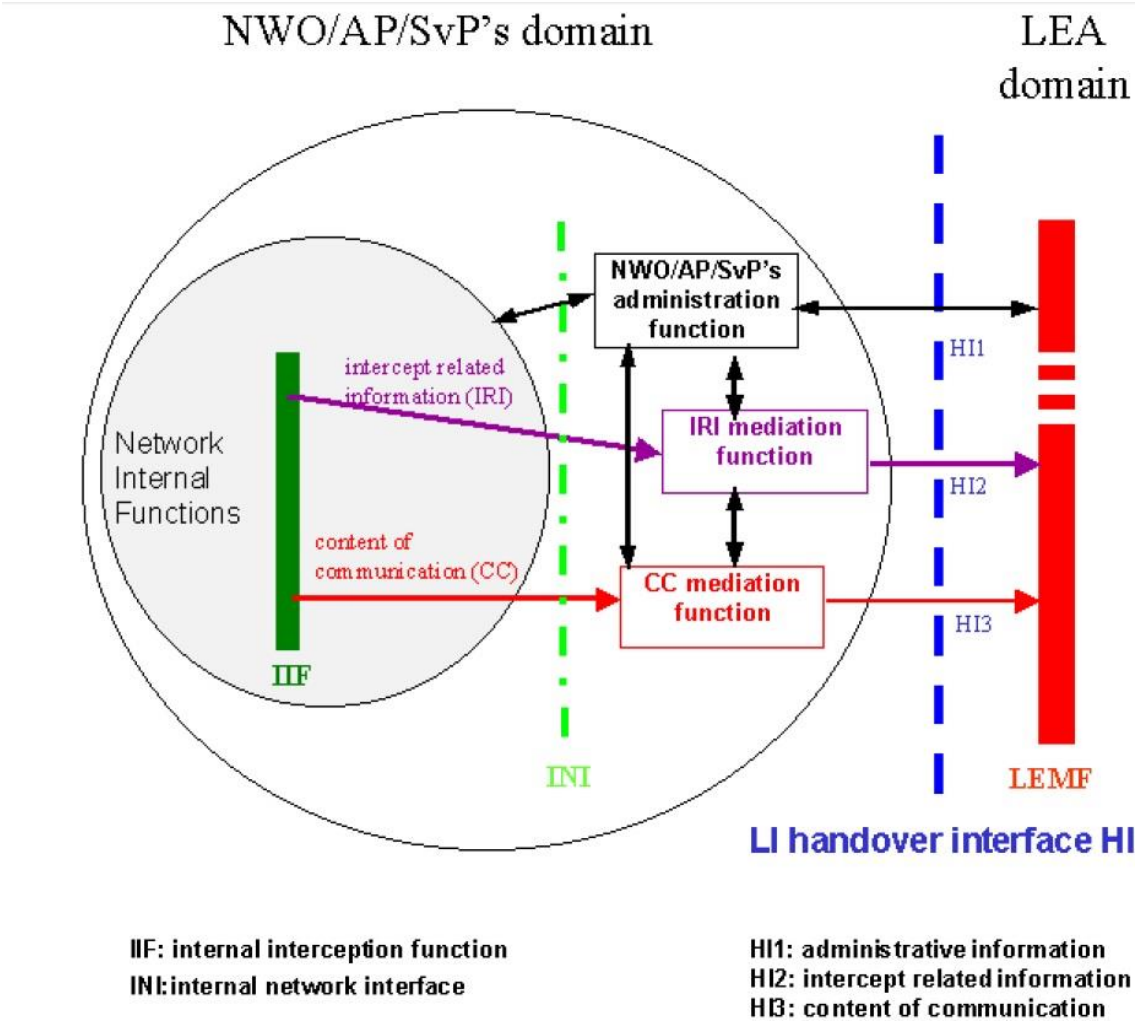
Telekuuntelu ja -valvonta (LI) on viranomaisten käytettävissä oleva menetelmä, jolla voidaan hankkia verkossa liikkuvien käyttäjien viestintätietoja. LI-järjestelmän luominen on aina ollut mahdollista, koska operaattorit ovat aina keränneet jonkintasoista tietoa puheluista, laskutus ja verkon ylläpito syistä. Tästä syystä LI-järjestelmän haasteet ovat enemmän lainsäädännöllisiä kuin teknisiä. Euroopan unioni on määrännyt julkisille puhelinoperaattoreille pakolliseksi tarjota viranomaisille tarvittavat tiedot telekommunikaatioiden seuraamiseen. [7.]

Telekuuntelu ja -valvonta käytännössä tarkoittaa viestintätietojen keräämistä. Viestintätiedot on jaettu kahteen eri tietotyyppiin: IRI ja CD. Viranomaiset voivat kerätä tietoja puhelun ja viestin sisällöstä, eli salakuunnella kaikkien viestien ja puheluiden sisältö reaaliajassa. Tämä tietotyyppi on IRI (eng. intercept related information), joka voi sisältää ääni-, video- tai tekstiviestejä. Toinen tietotyyppi, CD (eng. call data), sisältää puhelun tekniset tiedot: signalointitiedot (MAC osoitteet, taajuus), vastaajan ja soittajan puhelinnumerot, paikannustiedot sekä puheluiden kestot. [7.]

Tietojen luovuttaminen hoidetaan Handover-rajapinnan yli. Jotta tietojen luovuttaminen pysyisi mahdollisemman selkeänä, Handover-rajapinta on jaettu kolmeen osaan: HI1, HI2 ja HI3. HI1 sisältää hallinnolliset tiedot, HI2 sisältää IRI-tiedot ja HI3 sisältää CC-tiedot. Kuva 9 ilmaisee LI-järjestelmän yleisen arkkitehtuurin.

Uloin ympyrä kuvastaa verkonoperaattoria (eng. network operator, NWO). NWO sisältää verkon sisäiset toiminnat, rajapinnat ja tarvittavat funktiot CC- ja IRI-tietojen välitykselle. Sisempi ympyrä koostuu verkon sisäisistä toiminnoista, kuten liikenteen reitityksestä ja käsittelystä. Tällä tasolla toimivat myös IIF-funktiot (eng. Internal

Intercept Functions) joiden avulla tiedot lähetetään eteenpäin ja lopulta välittyvät H1-3 kanaville. Nämä kanavat puolestaan HI-rajapinnan avulla lähettävät tiedot viranomaisten tietokantaan LEMF (eng Law Enforcement Managment Facility). [8.]



Kuva 9. Telekuuntelu ja -valvonta ja sen rajapinnat [7.]

5 3G:n haavoittuvuudet

Kansainvälinen yhteistyöorganisaatio 3GPP, jonka tarkoitus on luoda maailmanlaajuisesti yhtenäiset tekniset määritelmät matkapuhelinverkkoja varten, on luokitellut mahdolliset tietoturvauhat 3G-järjestelmissä seuraavasti: luvaton pääsy tietoihin, tietojen luvaton käsittely, verkon häiritseminen ja väärinkäyttö sekä palveluiden luvaton käyttö. [9.]

Luvaton pääsy tietoihin koskee lähinnä liikenteen salakuuntelua ja naamioitumista. Hyökkääjä voi naamioitua verkkoelementiksi ja täten siepata käyttäjän liikenne, merkinanto- ja ohjaustietoja. On myös mahdollista, että hyökkääjä suorittaa liikenteen analysointia, josta voi saada selville sijainteja ja keskustelun pituuksia. Todennäköisintä kuitenkin on, että käyttäjän laite on varastettu ja hyökkääjän käytössä. [9.]

Tietojen luvaton käsittely käytännössä tarkoittaa tiedon eheyden murtamista. Hyökkääjä voi manipuloida tietoja, joita tarvitaan yhteyden muodostamiseen, joka voi johtaa salausmenetelmien manipulointiin. Jos tässä onnistutaan, hyökkääjä voisi teoriassa manipuloida käyttäjän liikennettä lisäämällä tai poistamalla siihen liittyviä attribuutteja. [9.]

Verkon ja palveluiden häiritseminen tai väärinkäyttö voi olla fyysistä tai virtuaalista. Hyökkääjä voi estää käyttäjän liikennettä etenemästä lähettämällä häiriösignaalia tai sabotoimalla verkkoa. Palvelunesto hyökkäykset (eng. Denail of Service, DoS) ovat myös mahdollisia. Vaikka USIM-kortti olisi lukittu, hätäpalveluihin soittaminen on vielä mahdollista, johtaen tilaisuuksiin aiheuttaa turhaa kuormitusta hätäpalveluille. [9.]

Palveluiden luvaton käyttö käytännössä tarkoittaa, että hyökkääjä saa todennettua itsensä palveluihin, jotka eivät muuten kuuluisi hänelle. Hyökkääjä naamioituu tukiasemana, joka palvelee käyttäjää ja toimii välikätenä todennusprosessissa, joka tapahtuu päätelaitteen ja AuC:n välillä. Kun todennus on suoritettu, hyökkääjä kaappaa käyttäjän yhteyden ja esiintyy taas päätelaitteena. [9.]

6 Tulevaisuus on 4G

6.1 Matkapuhelinverkkojen neljäs sukupolvi

Vaikka kolmannen sukupolven alku oli hidasta ja markkinointilausahdukset lupailivat liikoja, suosio on vahvasti kasvanut viimeisen vuosikymmenen aikana. Nykyään jokaisen taskusta löytyy älypuhelin ja mobiililaajakaistaliittymä. 3G-verkon käyttö on osa normaalia arkipäivää, ja tästä syystä on taas aika päivittää verkot uuteen sukupolveen, joka kestää nykyiset tiedonsiirtotarpeet nyt ja tulevaisuudessa.

Neljännen sukupolven verkot toimiviat IP-verkon tavoin, joten ne sopivat tiedonsiirtoon paljon paremmin. 4G-verkkojen LTE-tekniikka on myös hienostuneempaa, joten sen pitäisi kestää kauemmin kuin 3G:n, joka sai kaupallisen alkunsa noin kymmenen vuotta sitten. Täytyy kuitenkin muistaa, että uudet teknologiat tuovat uusia haasteita. 4G-verkkojen kattavuus ei ole vielä parhaimmalla tasolla, joten käyttäjät saattavat tietyillä alueilla pettyä kuuluvuuteen tai tiedonsiirtonopeuksiin. Meillä on töissä ollut 4G-mobiilitikkuja käytössä ja on huomattu, että kaupunkialueiden ulkopuolella kattavuus on heikkoa. Jos asiakas on vain puheliasta tyyppiä, voi hän säästää rahaa ja akkua, kun ei hän tarvitse 4G-dataliittymää.

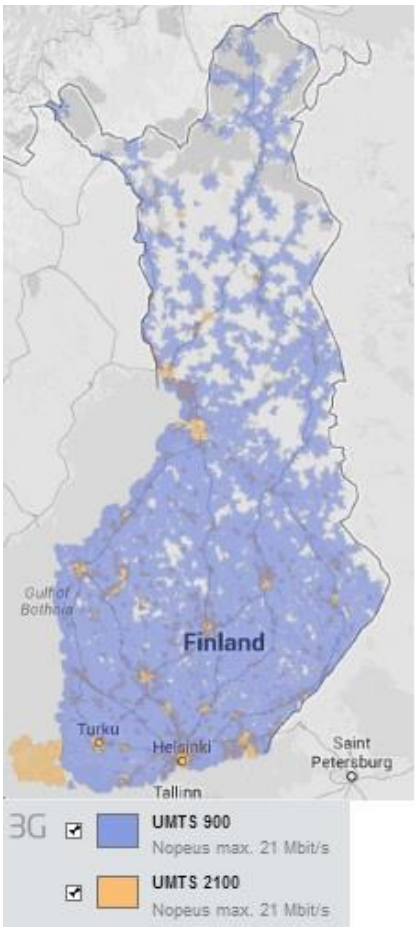
Kolmas sukupolvi toimi piiri- ja pakettikytkentäisesti ja pystyi tästä syystä käyttämään rinnakkain puhelu- ja datasiirtopalveluita. Neljännen sukupolven verkot ovat puhtaasti pakettikytkentäisiä, mikä tarkoittaa nopeampaa tiedonsiirtoa, mutta samalla tarkoittaa sitä, että se ei pysty käyttämään samanaikaisesti molempia verkkoja.

Näistä seikoista huolimatta 4G-verkot ovat korvaamassa 3G-verkkoja, varmasti mutta hitaasti. Uuden sukupolven verkot tarvitsevat uusia tukiasemia, jotta kattavuusalue kasvaisi ja uusia taajuuskaistoja on myös tulossa. Monissa kehitysmaissa aiotaan ohittaa 3G kokonaan ja hypätä suoraan 2G:stä 4G:hen, koska kustannukset vastaavat 3G-tekniikan hintoja.

Kuuluvuus Suomessa 4G vs 3G

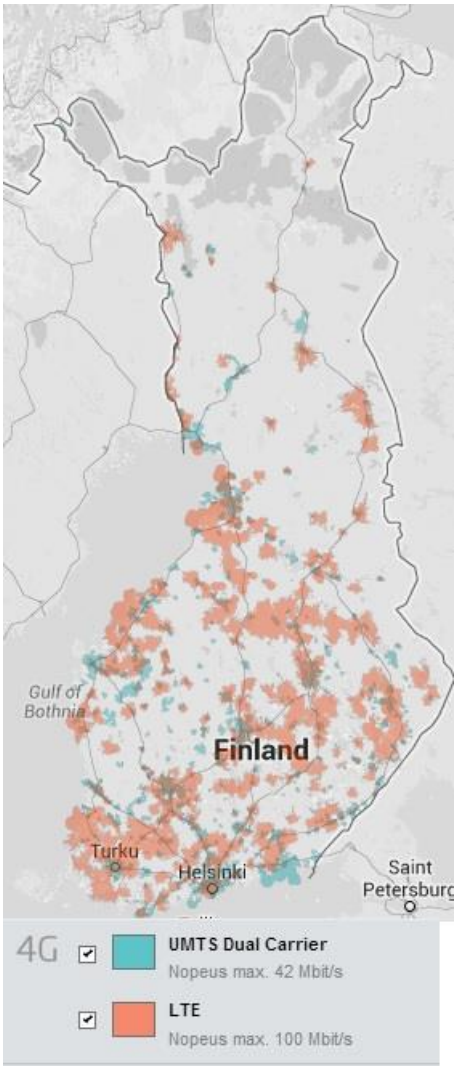
Puhelin- ja internetyhteyksien toimivuus matkaviestinverkoissa vaihtelee verkon kuuluvuuden mukaan. Viestintäviraston mukaan GSM-matkaverkko kattaa käytännössä lähes koko Suomen, kun taas 3G-matkaviestintäverkon kuuluvuus on määritelty hyvin laajaksi. 4G-verkkojen peitealue laajenee jatkuvasti, ja tällä hetkellä kuuluvuus on lähinnä tiheillä asuinalueilla. Tyypillisesti tukiaseman ja päätelaitteen välinen signaali on vahva tukiaseman läheisyydessä. Signaali heikkenee etäisyyden kasvaessa. Mitä heikompi signaali on vastaanotettavissa, sitä huonompi kuuluvuus on. [13.]

Tekijät, jotka vaikuttavat kuuluvuuteen, vaikuttavat signaalin voimakkuuteen. Kuuluvuuteen vaikuttavat tekijät ovat pääsääntöisesti joko fyysiseen sijaintiin liittyviä tai paikallisiin olosuhteisiin liittyviä. Fyysiseen sijaintiin vaikuttaa lähinnä etäisyys tukiasemaan ja alueen tiheys. Etäisyys tukiasemaan vaikuttaa, koska mitä kauempana tukiasemasta ollaan, sitä heikompi signaali on vastaanotettavissa. Tiheydellä tarkoitetaan, kuinka monta muuta käyttäjää alueella on saman solun palveluksessa. Jos yksi tukiasema on erittäin kuormitettu, laadunvalvonta saattaa asettaa rajoituksia tiedonsiirtonopeuksille, jotta kapasiteettia riittää kaikille, jotka ovat tukiasemassa kiinni sillä hetkellä. Tästä syystä yleensä yöaikaan, kun verkossa on vähiten käyttäjiä, on todennäköisempää saada koreammat tiedonsiirtonopeudet. Ympäristöolosuhteisiin kuuluvat seikat kuten rakenteelliset ja luonnolliset esteet sekä paikalliset sääolosuhteet. Seuraavalla sivulla on esitetty kuvat 10 ja 11, jotka kuvaavat Elisan 3G- ja 4G-verkkojen kuuluvuutta Suomessa. [13.]



Kuva 10. Elisa 3G-verkon kuuluvuus Suomessa [17.]

Kuten kuvasta 10 voidaan todeta, 3G-verkon kattavuus Suomessa on varsin laajaa. On selvää, että Pohjois-Suomessa kattavuus heikkenee sitä mukaa kun väestöntiheys laskee, etenkin maalaisalueilla. Mielenkiintoista on, että kuvan mukaan 3G:n kattavuutta esiintyy Pohjois-Suomessa, mutta vain isojen moottoriteiden läheisyydessä. Tämä luultavasti johtuu siitä, että harvat tukiasemat, jotka tältä alueelta löytyvät, sijaitsevat moottoriteiden vieressä. Yleensä datakaapelit kulkevat myös maan alla moottoriteiden vieressä, joten internetpalveluiden tarjoaminen ja niihin kytkeytyminen voidaan operaattorin kannalta hoitaa kustannustehokkaasti.



Kuva 11. Elisa 4G-verkon kuuluvuus Suomessa [17.]

Kuten kuvasta 11 voidaan päätellä, 4G-verkon kattavuus koskee vain tiheästi asuttuja alueita, kuten kaupunkeja. Tämä johtuu siitä, että operaattorit ovat vasta nyt panostamassa 4G-verkkojen laajentamiseen Suomessa. Olettaisin, että 3G-verkon kattavuus lopettaa laajentumisen nyt, kun LTE-teknologia on se, mihin operaattorit panostavat. Ei olisi kovin kustannustehokasta kasvattaa kummankin verkon kuuluvuutta samanaikaisesti.

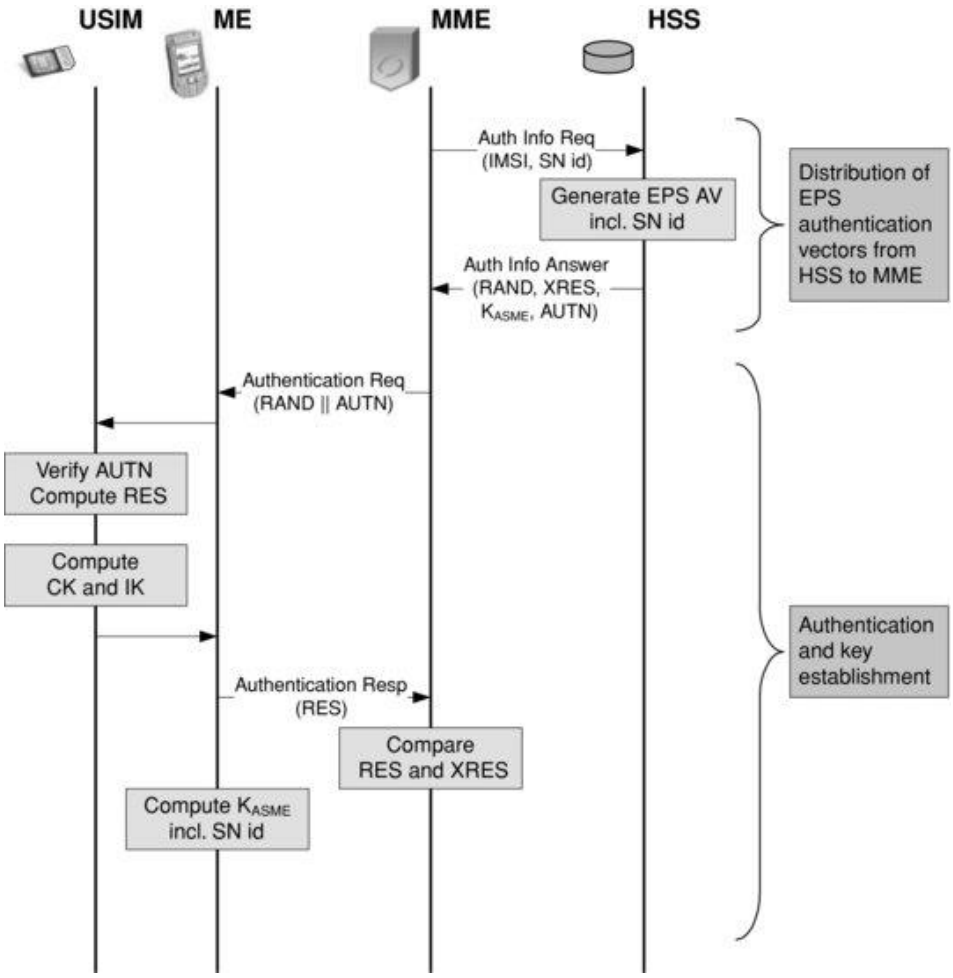
6.2 4G:n todennus

Vertausmielessä 3G-verkon todennusprosessiin otetaan tarkasteluun miten todennusprosessi tapahtuu 4G-verkoissa. Kuten 3G-verkoissa, 4G-verkon todennusprosessi alkaa aina päätelaitteen pyynnöstä. Päätelaiteen UICC:lle ja HSS:n tietokantaan on tallennettu salattu K-avain, jonka vain UICC ja HSS tietävät. K-avaimen perustella UICC ja HSS luovat kaksi muuta avainta: CK ja IK. UMTS käytti näitä avaimia suoraan salauksien ja eheyksien luomiseen, mutta LTE-verkot käyttävät niitä eri tavalla. LTE käyttää näitä avaimia luodakseen ASME-avaimen (eng. access security management entity), jonka tunnus on KASME. Tästä KASME-avaimesta runkoverkkoa ja päätelaitetta hallitseva MME luo vielä kolme avainta lisää: KNASenc, KNASint ja KeNB. [12.]

Tämä joukko avaimia on suurempi kuin GSM- tai UMTS-avaimet, ja hyödyt ovat selviä. Kun päätelaite irtautuu verkosta, UICC:n muistiin tallentuu CK- ja IK-arvot, kun taas MME tallentaa KASME-avaimen arvon. Tämä antaa verkolle mahdollisuuden suojata päätelaitteen seuraava pyyntö liittyä verkkoon, ominaisuus jota ei ollut edellisessä sukupolvessa. Salausavaimissa on myös käytössä hierarkkinen järjestelmä joka takaa että avaimet ovat kryptografisesti erillään. Tämä takaa sen, että hyökkääjä ei voi päätellä toista avainta toisesta. Tämä hierarkia on myös yhteensopiva vanhempien USIM-päätelaitteiden kanssa. K-, CK- ja IK-avaimet ovat 128-bittisiä, kun muut avaimet ovat 256-bittisiä. Nykyiset salausalgoritmit käyttävät 128-bittisiä avaimia jotka on johdettu 256-bittisten avainten vähiten merkitsevistä biteistä. Jos LTE-järjestelmien pitää joskus pidentää salausavaimia, onnistuu helposti 128 bittisen salauksen nosto 256-bittiin. [12.]

Kuten edellisessä kappaleessa todettiin, päätelaite ja runkoverkko todentavat toisensa pääsemällä yhteisymmärrykseen KASME-avaimen arvosta. Päätelaite aloittaa todennusprosessin ja runkoverkon hallintajärjestelmä MME vastaanottaa päätelaitteen IMSI -tunnuksen. Jotta prosessi jatkuisi, MME lähettää "Authentication Infrormation Request" -sanoman HSS-komponentille, joka sisältää IMSI-tunnuksen. IMSI-tunnuksen perusteella HSS etsii tietokannastaan K-avaimen ja laskee todennusvektorin johon kuuluu neljä elementtiä: RAND, AUTN, XRES ja KASME. RAND, AUTN ja XRES toimivat samalla tavalla kuin 3G-verkoissa, nyt vain välikätenä ei ole SGSN, vaan MME. GSM- ja UMTS-järjestelmissä perinteisesti AuC palauttaa useita todennusvektoreita kerrallaan minimoidakseen määrän viestejä, joita järjestelmän pitää

käsitellä. LTE-järjestelmässä näin ei tarvitse toimia koska KASME-avaimen muistiin jääminen on vähentänyt viestienmäärää, jota todennusprosessisissa muuten tarvittaisiin. Kuten kuvasta 12 nähdään, MME lähettää RAND- ja AUTN-parametrit päätelaitteelle, joka laskee omat arvonsa käyttäen K-avainta. Laskujen tulokset palautetaan verkolle "EMM Authentication Response" -sanomassa. Jos päätelaitteen laskemat arvot täsmäävät verkon odottamiin arvoihin, päätelaite on todennettu onnistuneesti. [12.]



Kuva 12. Päätelaitteen todennus LTE-järjestelmässä [12.]

6.3 4G:n tietoturva

Kuten kaikissa verkoissa, myös LTE-arkkitehtuuri on altis tietoturvauhkille. Kaikki radioliityntäprotokollat pysähtyvät tukiasematasolla, joten teoriassa niiden manipuloimien olisi mahdollista. Tämän lisäksi myös IP-protokollat ovat havaittavissa tukiasematasolla. LTE-järjestelmän turvaaminen fyysisesti on myös vaikeampaa, koska nyt on mahdollista sijoittaa pieniä tukiasemia (HeNB) koti- ja toimistotiloihin. Tämä nostaa mahdollisuuksia fyysisesti manipuloida tukiasemaa riippuen HenB:n sijainnista. Hyökkääjällä voi myös helpommin suorittaa mies välissä -hyökkäyksiä tämänlaiseen tukiasemaan. Koska kyseessä on nyt täysin IP-pohjainen teknologia, verkko on myös altis toisenlaisille hyökkäyksille. [16.]

On mahdollista huijata tukiasemaa lataamaan ja asentamaan väärennettyjä ohjelmistopäivityksiä tai aiheuttaa tietoturvariskejä yhteensopivuusongelmien kautta. LTE-verkot yhtyeentoimivat myös vanhojen järjestelmien kanssa, jotka eivät välttämättä ole 3GPP:n määritelmien alaisuudessa. Tämänlaiset järjestelmät, jotka ovat paljon vanhempia kuin LTE-jäjrestelmät, voivat aiheuttaa arvaamattomia tietoturvaukkoja, kun ne operoivat LTE-teknologioiden kanssa. On myös mahdollista, että näitä tietoturvaukkoja ei välttämättä huomata, koska vanhat järjestelmät saattavat toimia ihan hyvin omissa ympäristöissään. Verkossa on myös mahdollisuus käyttää palveluita, joiden luotettavuudesta ei voida olla hyvin varmoja. [16.]

LTE:ssä on lukuisia parannuksia todennuksen lisäksi. Yksi uusi ja mielenkiintoinen tietoturvaratkaisu on varmenteiden käyttö. Varmenteet sisältävät julkisen avaimen, jonka on allekirjoittanut luotettava osapuoli. Tällä menetelmällä esimerkiksi päätelaite luottaa varmenteeseen niin kauan kunnes luettava osapuoli pystyy todistamaan identiteettinsä sähköisellä allekirjoituksella, joka on osa varmennetta.

Varmenteiden ongelmana kuitenkin on niiden asennus ja ylläpito. On mahdotonta asentaa kaikki varmenteet lokaalisesti ja jossain vaiheessa ne täytyy taas uusia. Tästä syystä CMP-protokolla (eng Certificate Management Protocol) on kehitetty, ja sen

tehtävänä on tarjota kyky hakea, päivittää ja poistaa varmenteita, käyttäen keskitettyä palvelinta. Kaikki laitteet tulevat esiasennetun laitevalmistajavarmenteen kanssa, joka on käytössä jos operaattori ei ole vielä omaa varmennetta asentanut. [16.]

7 Yhteenveto

Insinöörityössä tutkittiin 3G-verkon pääpiirteitä ja tietoturvaan liittyviä yksityiskohtia. Yhteenvetona voidaan todeta, että matkapuhelinverkot ovat kehittyneet huimaa vauhtia ja jatkuvalle kehitykselle niin yleisestikin kuin tietoturvallisesti on tarvetta. Kolmannen sukupolven verkot vastaavat hyvin paljon edellistä sukupolvea, jota tässä työssä ei käsitelty.

Kävin läpi 3G-verkoissa käytettäviä tietoturvamenetelmiä ja keskityin lähinnä päätelaitteen ja käyttäjän tarvitsemaan tietoturvaan. Omasta mielestäni tämä on tärkein osa-alue 3G:n tietoturvan kannalta, koska suurin arvaamaton tekijä, kuten niin monessa muussakin asiassa, on ihminen. Työssä myös painotettiin uusimpia kehityksiä 3G:n tietoturvassa kuten telekuuntelu ja -valvonta, ja USIM-kortit. Vanhemmat teknologiat kuten GSM:n käyttämät SIM-kortit ja vanhemmat todennusprosessit eivät kuuluneet työn laajuuteen.

Koska 3G-verkon elinkaari parhaimpana puhelinverkkona on selkeästi takanapäin, mainitsin myös työn lopuksi neljännen sukupolven verkot ja miksi niitä tarvitaan. Lisäksi myös vertailtiin 3G- ja 4G-verkkojen kuuluvuutta Suomessa sekä miten käyttäjätodennus menetelmät eroavat toisistaan. Lopuksi on vielä mainittu mitä uusia tietoturvaominaisuuksia LTE-järjestemästä löytyy.

On selvää, että matkapuhelinverkkojen kehityspolku on ollut pitkä, ja muutoksia on tapahtunut paljon. Suurin osa näistä muutoksista on tehty koska matkapuhelimien kehitys on nostanut liikenteen määrää valtavasti. 12 vuotta sitten määritelty 3G-standardi on palvellut hyvin, ja vastasi niihin odotuksiin jotka verkolle asetettiin. Nyt kuitenkin ollaan tilanteessa johon 3G-verkko ei tarjoa riittävää ratkaisua.

Dataliikenteen räjähdysmäinen kasvu on osoittanut että 3G-verkko ja sen tarjoama kapasiteetti eivät enää pysty palvelemaan verkon käyttäjiä tehokkaasti. On myös huomattu, että aiemmista sukupolvista polveutuneet teknologiat ovat osoittautuneet

kömpelöiksi ja kalliiksi. Nyt ollaan tilanteessa jossa on suotuisampaa kehittää uusia teknologioita ja laitteita, eikä vain päivittää vanhoja teknologioita.

Kuten kaikessa tiedonsiirrossa, internet näyttäisi olevan ratkaisu myös matkapuhelinverkkojen jatkuvaan taisteluun nostaa tiedonsiirtokapasiteettia. 4G LTE-verkot ovat täysin pakettikytkentäisiä verkkoja, jotka ovat kytkeytyneet internettiin. Jos kerta tällä teknologialla voidaan saada tehokasta ja nopeata tiedonsiirtoa koteihin, miksi ei myös matkaviestintäjärjestelmiin. Kuten internetin kehityksestä voidaan nähdä, tiedonsiirto teknologiat ja niiden kapasiteetit kasvavat lähes vuosittain. On täysin loogista ajatella, että tätä samaa alustaa voitaisiin soveltaa yhtä menestyksellisesti myös matkapuhelinverkoissa.

Tietoturvan kannalta olisi myös suotuisaa siirtyä täysin IP-pohjaiseen ratkaisuun matkapuhelinverkoissa. Vaikka teknologian toteuttaminen onkin täysin uuttaa 4G-matkapuhelinverkossa, internet ja sen käyttö on vanhaa kauraa tietokonemaailmassa. Aiempia kokemuksia ja nykyisiä IP-pohjaisia tietoturva ratkaisuja voidaan soveltaa tietokonemaailmasta, ja voidaan täten paremmin suunnitella tulevia matkapuhelinjärjestelmiä. Tiedonsiirron tarve on ikuisessa kasvussa, ja se on ainakin selvää, että 4G-järjestelmät tulevat vielä kokemaan lukuisia muutoksia elinkaarensa aikana.

Lähteet

1 Overview of 3GPP Release 99. Verkkodokumentti. Third Generation Partnership Project. <http://www.3gpp.org/ftp/tsg_cn/tsg_cn/TSGN_23/Docs/PDF/NP-040010.pdf> Luettu 10.4.2014.

2 MIMO. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/MIMO> Luettu 5.4.2014.

3 W-CDMA (UMTS). Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/W-CDMA> Luettu 5.4.2014.

4 3G Security; Security Architecture. Verkkodokumentti. The European Telecommunications Standards Institute (ETSI). <http://www.etsi.org/deliver/etsi_ts/133100_133199/133102/11.05.01_60/ts_133102v110501p.pdf> Luettu 1.4.2014.

5 Vähä-Sipilä, Antti. 2000. Tampereen Yliopisto. Cyphering in GRPS and UMTS. Verkkodokumentti. <http://www.vähä-sipilä.fi/avs/gprs-umts-crypto-revised.pdf> Luettu 30.3.2014.

6 Algorithm Set for the 3GPP Authentication and Key Generation Functions. Verkkodokumentti. The European Telecommunications Standards Institute. <http://www.etsi.org/deliver/etsi_ts/135200_135299/135205/11.00.00_60/ts_135205v110000p.pdf> Luettu 30.3.2014.

7 Technical Aspects of Lawful Interception. 2008. Verkkodokumentti. International Telecommunications Union.<ttps://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000060002PDFE.pdf> Luettu 15.4.2014.

8 Lawful Interception (LI) Handover interface. Verkkodokumentti. European Telecommunications Standards Institute. <http://www.etsi.org/deliver/etsi_ts/101600_101699/101671/02.08.01_60/ts_101671v020801p.pdf> Luettu 15.4.2014.

9 3G security; Security threats and requirements. Verkkodokumentti. Third Generation Partnership Project <http://www.etsi.org/deliver/etsi_ts/121100_121199/121133/04.01.00_60/ts_121133v040100p.pdf> Luettu 15.4.2014.

10 Bannister, Jeffrey & Mather, Paul. 2004. Convergence Technologies for 3G Networks. John Wiley & Sons Ltd.

11 Kaaranen, Heikki & Ahtiainen Ari & Laittinen, Lauri & Naghian, Siamäk & Niemi, Valtteri. 2005. UMTS Networks Architecture, Mobility and Services. Wiley Ltd.

12 Cox, Christopher. 2012. An Introduction to LTE, LTE-Advanced and 4G Mobile Communications. John Wiley & Sons Ltd.

13 Matkaviestinverkon kuuluvuus. Verkkodokumentti. Viestintävirasto. <https://www.viestintavirasto.fi/internetpuhelin/toimivuus/kuuluvuus.html> Luettu 20.4.2014.

14 Handover. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Handover> Luettu 19.4.2014.

15 Penttinen, Jyrki. 2002. Kännyköinnin oppimäärä. WSOY.

16 Penttinen, Jyrki. 2011. The LTE / SAE Deployment Handbook. John Wiley & Sons Ltd.

17 Elisan kuuluvuus. Verkkodokumentti. Elisa Oy. <http://elisa.fi/kuuluvuus/> Luettu 19.4.2014.