TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikka
Tietoliikennetekniikka

Tutkintotyö

Tommi Salo

PUHEENSALAUS TIEDONSIIRTOVERKOSSA

Työn ohjaaja Ari Rantala
Työn teettäjä Instasec Oy, valvoja Samu Lentonen
Tampere 2005

Tekijä:	Tommi Salo
Työn nimi:	Puheensalaus tiedonsiirtoverkoissa
Päivämäärä:	21.4.2005
Sivumäärä:	49 sivua
Hakusanat:	puheensalaus, kaistanleveys, voip
Koulutusohjelma:	Tietotekniikka
Suuntautumisvaihtoehto:	Tietoliikennetekniikka

Työn ohjaaja:	Ari Rantala
Työn teettäjä:	Suunnittelupäällikkö Samu Lentonen Instasec Oy, Tampere

Tarpeellisen tietoturvatason saavuttaminen on yksi tietoliikenneverkkojen keskeisimmistä haasteista. Tämän insinöörityön tarkoituksena on kuvata menetelmiä, joilla riittävä tietoturvan taso saavutetaan, kun halutaan salata ja siirtää puhetta tietoliikenneverkoissa.

Työssä tutustutaan puheen koodauksessa, siirrossa ja salauksessa käytettäviin tekniikoihin. Työssä keskitytään tarkastelemaan yleisimmin käytössä olevia pakettiverkon tekniikoita.

Koska nykypäivänä on myös tarvetta mukana kannettavalle salauslaitteelle, on tarpeen tutustua myös digitaalisen puheensiiron tarvitsemiin siirtokaistanleveyksiin ja niiden laskentatapoihin. Työssä lasketaan eri puheenkoodausmenetelmillä koodattujen puheiden kaistantarpeita, jotta suunnittelussa osataan ottaa huomioon eri siirtoverkkotekniikoiden rajoittuneet kapasiteetit.

Author:	Tommi Salo
Name of work:	Speech encryption in communication networks
Date:	21.4.2005
Pages:	49 pages
Keywords:	Speech encrypt, band width, voip

Thesis Supervisor:	Ari Rantala
Commissioning Company:	Designer Manager Samu Lentonen Instasec Oy, Tampere

The major challenge in communications network is to achieve necessary stage in data security. Purpose of this engineer work is to describe processes which adequate data security level is reached when wants to encrypt and transfer speech in communications networks.

In this engineer work we get to know technologies which are used in speech coding, data transfer and encryption. We concentrate in this work to study most common packet network technologies in use.

Because now a day there is need for portable cryptology it is necessary to get to know also digital speech transmission band width and their calculation customs. In this work we calculate with different speech coding methods coded speeches band needs so that engineering can take into account different transfer network technologies limited capacities.

SISÄLLYSLUETTELO

TIETOLIIKENTEEN JA SALAUSTEKNIIKAN LYHENTEET

3DES	*Data Encryption Standard*. USA:ssa kehitetty symmetrinen salausalgoritmi. Parannettu versio perus DES:stä, salataan kolmesti eri avaimilla.
AES	*Advanced Encryption Standard*. DES algoritmin seuraajaksi valittu salausstandardi.
DES	*Data Encryption Standard*. USA:ssa kehitetty symmetrinen salausalgoritmi. Julkaistu vuonna 1977.
ETSI	European Telecommunications Standards Institute.
IAB	*Internet Architecture Board*. Internet-standardit hyväksyvä elin.
IP	*Internet Protocol*. TCP/IP:n verkkokerroksen yhteyskäytäntö.
ITU	Eurooppalainen teleliikenteen standardointijärjestö. Vastaa eri jäsenmaiden kansallisten määräysten harmonisoinnnista.
IETF	*Internet Engineering Task Force*. Internet-verkon vapaaehtoiseen kehittämistyöhön osallistuvista henkilöistä muodostuva ryhmä. IAB:n alainen.
ITU-T	ITU:n alaosasto, joka vastaa puhelin- ja teleliikenteen suosituksista
PCM	*Pulse Code modulation*. Tekniikka äänen muuttamiseksi analogisesta digitaaliseksi
RSA	Epäsymmetrinen salausalgoritmi. Saanut nimensä keksijöiltään Rivest, Shamir ja Adleman mukaan.
TCP	*Transmission Control Protocol.* TCP/IP:n kuljetuskerroksen yhteyskäytäntö.
TETRA	*Trans-Europe Trunked Network.* Langaton viranomaisverkko.
TLL 1-4	Valtionhallinnossa käytössä oleva tietoturvaluokkaluokitus

1 JOHDANTO

Vaikka paketteina kulkevan puheen salakuuntelu ei ole aivan helppoa, ip-puheen ja pakettiverkkojen käytön lisääntyessä myös välineet paranevat ja vakoilu yleistyy. Liikenteen salaus on vakio-ominaisuus monissa tuotteissa, muttei kaikissa. Myös laitteiden antamaan salauksen tasoon kannattaa kiinnittää huomio.

Työssä on tarkoitus selvittää eri siirtoteiden tarjoamia kapasiteetteja ja tekniikoita, kun halutaan tehdä puheensalaus yhteyden päästä päähän. Työssä selvitetään tekniikoita, joita voidaan hyödyntää, kun halutaan suunnitella mukana kuljetettavaa puheensalainta.

Nykypäivänä on tarvetta salata tietoliikenneyhteyksiä yhä enenevässä määrin kun ulkoiset uhat ovat realisoituneet. Myös valtionhallinnon määräykset edesauttavat tarvetta puheensalauksen lisäämiseen. Valtionhallintoihin tuleva määräys määrää että tietoturvaluokan TLL 4 ja korkeampien asioiden käsittely puhelimessa ilman salausta on kielletty.

2 INSTASEC YRITYKSENÄ

Instasec Oy on Tamperetta pääpaikkanaan pitävä teknologiayritys. Sillä on toimipisteet Tampereella ja Espoossa. Instasec Oy kuuluu Insta-konserniin ja on 100% Instrumentointi Oy:n omistama. Yritys kehittää ja toimittaa turvallisia tietoliikenneratkaisuja ja -palveluja, joiden avulla asiakkaat voivat toteuttaa uudenlaisia liiketoimintamalleja ja tehostaa toimintaansa. Instasec Oy keskittyy innovatiivisiin, räätälöityihin ja erikoistuneisiin teknologiaratkaisuihin, kuten puolustus- ja valtionhallinnon erikoissovellukset, viranomaisten mobiiliverkot (TETRA), tietoturvatuotteet ja kriisinhallintajärjestelmät. Ratkaisuille on tyypillistä erittäin korkeat tietoturvavaatimukset. /21/

Instasec Oy toimittaa tietoliikenne- ja tietoturvaratkaisuja Puolustusvoimien ja valtionhallinnon järjestelmiin. Instasec:n tietoturva-asiantuntemus ulottuu uhka-analyysin tekemisestä ohjelmistoista ja laitteista koostuvien tietoturvajärjestelmien kokonaistoimituksiin. /21/

Yksi esimerkki tietoliikenneratkaisuista on Puolustusvoimien sanomanvälitysjärjestelmä, joka tarjoaa edistyksellisiä viestintätoimintoja COTS-ympäristössä mahdollistaen yhteydenpidon erilaisten verkkojen, protokollien ja laitteiden välillä tukien mm. TCP/IP:tä, sanomalaiteverkkoa, digitaalisia kenttäradioita, TETRAa, faksia, sähköpostia ja modeemeja. /21/

3 PUHEEN KÄSITTELY JA PAKKAUS

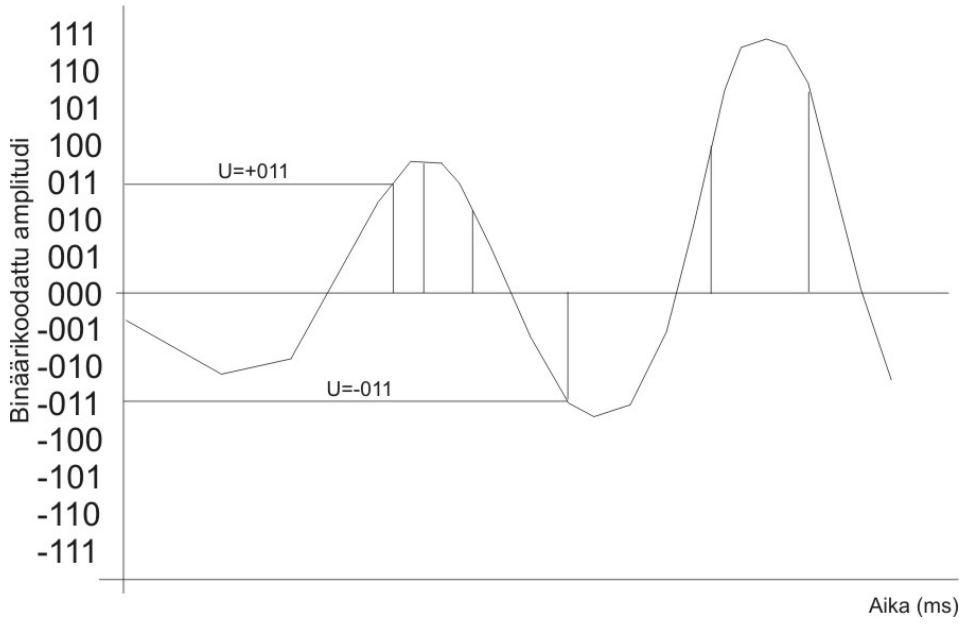
3.1 Datan koodaus PCM (Pulse Code Modulation)

Ennen kuin ääntä voidaan käsitellä, se pitää muuttaa analogisesta digitaaliseen muotoon. Analoginen data muuntuu diskreettiin muotoon, kun siitä otetaan näytteitä. PCM-moduloinnissa (Pulse Code Modulation) otetaan siis analogisesta signaalista näyte, jolle annetaan signaalin amplitudia ilmaiseva digitaalinen arvo. Diskreetti data muodostuu yksittäisistä symboleista. Numeeriseen muotoon koodatun äänen aitouden tunne säilyy sitä paremmin, mitä lyhyempi on näytteenottojen väliaika ja mitä pienempi on näytteenottojen väliaika. Aaltomuodon mukainen mallinnus eli näytteenotto ja sitä seuraava koodaus muuntavat analogisen datan numeeriseen muotoon. Analogisen suureen kvantisoidut näytearvot ovat symbolijoukko eli diskreettiä dataa. Koodekki muuttaa äänen PCM-koodiksi. /1/

3.1.1 Näytteenotto

Digitoidun signaalin laatuun merkittävästi vaikuttava tekijä on muunnoksessa käytetty näytteenottotaajuus eli se, kuinka monta näytettä sekunnissa analogisesta signaalista otetaan. Näytteistetystä signaalista saadaan sitä tarkempi ja parempi kuva, mitä suurempaa näytteenottotaajuutta käytetään. Nyquistin teoreeman mukaan näytteenottotaajuus pitää olla vähintään kaksi kertaa niin suuri kuin näytteistettävän signaalin korkein taajuus. Toisaalta liian suuren näytteenottotaajuuden käyttäminen lisää tarpeettomasti talletettavan datan määrää tuomatta uutta informaatiota tutkittavasta kohteesta. Käytännössä näytteenottotaajuus määrätään aina tutkittavan signaalin perusteella: hitaasti muuttuville signaaleille riittää pieni näytteenottotaajuus. /11/

Digitoinnin ensimmäinen vaihe on analogisen signaalin mittaaminen määrävälein. Toimenpidettä kutsutaan näytteenotoksi ja se ratkaisee, kuinka tarkkaan analogisen signaalin pienet tasovaihtelut saadaan otettua prosessiin mukaan. Mitä karkeampi mittaus on, sitä pienempi on koko prosessin dynamiikka eli pienimmän ja suurimman muutoksen välinen ero. Analogisen signaalin luonteeseen kuuluu, että vaikka sen tason vaihteluille on olemassa selvät rajat, voi se saada näiden rajojen välissä äärettömän monta erilaista arvoa eli A/D-muunnoksessa pitäisi käyttää mitta-asteikkoa, jossa on äärettömän monta porrasta. /1/ Kuvassa 1 esitetty PCM-koodauksen periaate.



Kuva 1. PCM-koodauksen periaate /3/

Tämä ei kuitenkaan ole mahdollista, vaan mitta-asteikon porrastus on rajallinen ja saatu mittatulos on siksi aina pyöristettävä sopimaan tähän porrastukseen. /12/

Puheen pakkaaminen tapahtuu audiokoodekeilla, joita on käytettävissä useita erilaisia. ITU-T:n määrittämistä G.7xx-sarjan koodekeista vanhin on G.711, joka julkaistiin vuonna 1981. Tällä koodauksella on perinteisesti hoidettu koodaus perinteisessä puhelinverkoissa. Koodekki vaatii kaistaa 64 kilobittiä sekunnissa. Tehokkaampia pakkauksia on käyttämällä esimerkiksi G.723.1- ja G.729-koodekeissa, joiden kaistantarve vaihtelee 5,4 - 8:aan kilobittiin sekunnissa.

3.1.2 Puheenkoodausmenetelmiä

Verkon yleisestä ruuhkautumisesta, reitityksestä ja kytkennästä aiheutuu puskurointiviiveitä. Yksi keino parantaa viiveitä on vähentää liikennettä datan pakkausalgoritmeilla. Puheen digitoinnissa ja pakkauksessa käytetään yleensä ITU-T:n määrittelemiä standardeja. Yksi puhekaista vie muutamasta kilobitistä 64 kilobittiin sekunnissa riippuen käytetystä puheenkoodausmenetelmästä. Pääsääntöisesti voidaan sanoa, että puheen laatu heikkenee siirryttäessä tiukempiin pakkauksiin, mutta pyrkimys on käyttää tehokasta tiivistystä ilman että puheen ymmärrettävyys heikkenee.

Puheen pakkaamiseen on määritelty useita erilaisia pakkausmenetelmiä. Alla on osa ITU-T:n määrittelemistä puheenkoodausstandardeja.

G.711: PCM - vanhin kansainvälinen standardi, joka on määritelty, miten PCM-koodi muodostetaan puhelinverkkoon. Siirtokaistan tarve 64 kb/s, ei pakkausta. G.711 on myös määritelty standardiksi ISDN päätelaitteille. Pitää sisältyä myös H.323- ja SIP-standardien implementointeihin. /14/

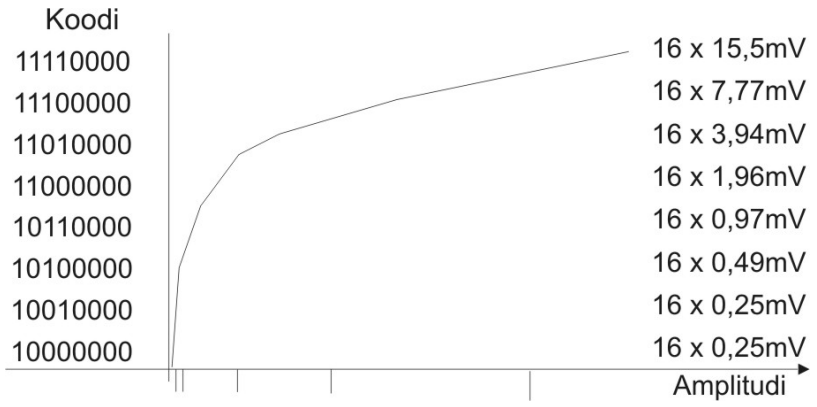
Näytteitä otetaan 8000 näytettä/s kunkin näytteen ollessa 8 bitin mittainen. Näytteen amplitudi tallennetaan 8 bitin mittaisena Kaistantarve muodostuu siis 8 b x 8000 = 64 kb/s. Näytteistettävä taajuus voi siis G.711 koodekilla olla 0 – 4kHz:iin. /3/

Tästä standardista on kaksi muotoa, A-Law ja u-Law. A-Law sovelletaan Euroopassa ja u-Law sovelletaan Yhdysvalloissa ja Kanadassa. Molemmat toimivat suurin piirtein samalla tavalla., joten alla esitetty Euroopassa käytettävää A-law-mallia. /14/

A-Law G.711 PCM-kooderi muuntaa 13-bittisen PCM-näytteen 8-bittiseksi (logaritminen muoto). Saatu 13-bittinen arvo ”tiivistetään” 8 bittiin logaritmisella askelluksella, jolloin 8 bitin tarkkuudella saavutetaan 13 bitin dynamiikka. /14/

Puhe digitalisoidaan 13 bitin A/D-muuntimella, jolloin saamme ± 4096 askelta koko välille ja yhden askeleen pituus on 0,125 mV. /14/

Saatu 13-bittinen arvo ”tiivistetään” 8 bittiin logaritmisella askelluksella, jolloin saavutetaan 13 bitin dynamiikka. Vastaanottaja avaa tiivistyksen vastakkaisella toimenpiteellä. /14/



Kuva 2. G.711 A-law’n kompessiokäyrä /14/

Puheenkoodauksessa pyritään aikaansaamaan mahdollisimman hyvä tiivistys ilman, että puheen ymmärrettävyys kärsii. Tähän tavoitteeseen pääsy vaatii koodausta erilaisilla matemaattisilla malleilla, jolloin linjalle lähetetään A/D-muunnoksen näytteen sijaan kyseisen mallin

tarvitsemat parametriarvot. Seuraavassa luvussa esitetty kolme menetelmää: ADPCM, LPC ja CELP.

3.1.2.1 ADPCM

Menetelmä on PCM-moduloinnin muunnelma, jossa lähdetään olettamuksesta, että vierekkäiset näytteet poikkeavat toisistaan hyvin vähän ja sen sijaan, että lähetetään näyte sellaisenaan, lähetetään näytteiden välistä erotusta kuvaava arvo. /14/

ADPCM-menetelmässä sisään tuleva analoginen signaali suodatetaan ja siitä otetaan A/D-muuntimella näyte n_i. Tämän jälkeen lasketaan näytteestä n_i-1 muodostetun laskennallisen näytteen x_{i-1} ja näytteen n_i välisen erotuksen Dn. Erotuksesta Dn muodostetaan muutosta kuvaava 4-bittinen koodi. Jos käytössämme on 16-bitin muunnos niin saadaan menetelmällä 4:1 pakkaus. PCM-koodauksella 64 kb/s nopeudella siirrettävä puhe voidaan siirtää 16 kb/s siirtotiellä. /14/

3.1.2.2 LPC ja CELP

LPC-menetelmissä puheesta otetaan lyhyt näyte, jota verrataan joukkoon tunnettuja malleja. Parhaiten soveltuvan mallin indeksi tai osoitetieto välitetään vastaanottajalle, joka tämän perusteella muodostaa synteettisen äänen. LPC perustuu PCM-koodauksen tavoin siihen, että puheesta otetaan näytteitä nopeudella 8000 näytettä sekunnissa. Kukin näyte on 8-bittinen, joten koodekille tulevan bittivirran nopeus on 64 kb/s. Bittivirta jaetaan segmentteihin siten, että kukin segmentti edustaa 22,5 ms:n näytettä ja segmentissä näitä on 180 kappaletta. Kukin segmentti käsitellään digitoinnissa omana kokonaisuutenaan. /14/

Äänen muodostamiseksi tarvitaan tietoa siitä, millä voimakkuudella ääntä lähdetään tuottamaan. Seuraavaksi on tehtävä päätös siitä, onko

kyseessä vokaali vai konsonantti. Tämä voidaan päätellä tutkimalla äänen voimakkuutta ja taajuutta, koska vokaalit ovat amplitudiltaan suurempia kuin konsonantit ja konsonanttien taajuudet ovat vokaaleja suuremmat. Vokaaleja varten on osattava säätää taajuus ja lopuksi tarvitaan artikulointia varten joukko suodatusparametreja. Kaikkiaan yhdestä näytteestä saadaan 54 bitin sanoma kuvaamaan näytettä ja se lähetetään purettavaksi vastaanottajalle. /14/

CELP- menetelmä käyttää samaa menetelmää kuin LPC-menetelmä, mutta sen lisäksi siinä huomioidaan puheen ja mallin välinen virhe, ja virheistä muodostetaan oma mukautuva mallisto, jolla laajennetaan staattista mallistoa. Staattisessa mallistossa on 1024 vektoria, jotka kuvaavat mahdollisia ääninäytteitä ja koodauksessa valitaan se näyte, joka parhaiten sopii äänestä otettuun näytteeseen. Menetelmä on suhteellisen vaativa ja sen vuoksi puheen koodaus reaaliajassa tapahtuu yleensä laitetasolla. /15/

G.721: ADPCM (Adaptive Differential Pulse Code Modulation) - kaistantarve 32 kilobittiä sekunnissa.

G.722: SB-ADPCM (Sub-Band Adaptive Differential Pulse Code Modulation) - PCM:ää paremmalla näytteenottotaajuudella toimiva ja korkealuokkaisemman äänen antava menetelmä, siirtokaistan tarve 48, 56 tai 64 kb/s

G.723.1: Dual Rate Speech Coder, kaistantarve 5.3 tai 6.4 kb/s

G.728: PCM + LD-CELP (Pulse Code Modulation with Low-Delay Code Excited Linear Prediction) - kaistantarve 16 kb/s

G.729: CS-ACELP - Conjugate Structure Algebraic Code Excited Linear Prediction, kaistantarve 8 kb/s

Taulukkoon 1 on kerätty ITU-T:n standardoimia puheenpakkaus-menetelmiä.

Taulukko 1. G.7XX standardin bittinopeuksia /27/

Standardi ITU-T	Koodausmenetelmä	Bittinopeus/ kb/s
G.711	PCM	64
G.721	ADPCM	32
G.722	ADPCM	64
G.723	ADPCM	20, 40
G.723.1	LD-CELP	5.3, 6.4
G.726	ADPCM	16, 24, 32, 40
G.727	ADPCM	16, 24, 32, 40
G.728	LD-CELP	16
G.729	CELP	8

.

4 SALAUS- JA TODENNUSMENETELMÄT

Analogisella puheensekoittajalla salataan puheviesti muuntelemalla eri tavoin siirrettävää viestiä taajuuden ja ajan suhteen. Taajuuskaista voidaan jakaa osiin, joita vaihdetaan keskenään tai puheesta otetut lyhyet jaksot lähetetään eri järjestyksessä. Taajuuksien vaihto tapahtuu avaimen ohjaamana mahdollisimman satunnaisesti. Tänä päivänä analoginen puheensekoitus ei anna enää riittävää turvaa salakuuntelua vastaan. /3/

Digitaalisilla salausmenetelmillä voidaan tiedonsiirrossa varmistaa luottamuksellisuus tiedon eheys ja tunnistaa käyttäjä. Digitaalisilla salamenetelmillä voidaan salata puhetta, dataa tai kuvaa, kaikkea mikä on digitaalisessa muodossa. /3/

Salausalgoritmilla tarkoitetaan salauksessa käytettyä salakirjoitusmenetelmää. Salausalgoritmilla saatetaan tarkoittaa myös sitä ohjelmakoodia, jota käytetään viestin salakirjoituksessa. Jos viestin salakirjoittamisen ja viestin purkaminen suoritetaan täsmälleen samalla tavalla, algoritmista käytetään nimitystä involuutio. /13/

Salausalgoritmi mahdollistaa erilaisten salausmoodien käytön, jolloin viesti voidaan salata samalla salausalgoritmilla useilla eri tavoilla. Käytettävissä olevat moodit riippuvat salausalgoritmista. Taulukossa 2 on esitetty yleisimmät käytettävissä olevat salausmoodit: /13/

Taulukko 2. Salausalgoritmien salausmoodit /13/

Salausmoodit	
Salausmoodi	Kuvaus
ECB (*Electronic Codebook*)	Salakirjoittaa viestin normaalisti. Viestin jokainen lohko salakirjoitetaan samalla tavalla.
CBC (*Cipher Block Chaining*)	Sama kuin edellinen, mutta ennen lohkon salakirjoitusta sitä muutetaan salasanoman edellisen lohkon mukaan.
CFB (*Cipher Feedback*)	Salakirjoittamisen suorittava lohko muodostetaan edellisestä salakirjoittamisen suorittaneesta lohkosta sekä avaimesta.
OFB (*Output feedback*)	Salakirjoittamisen suorittava lohko muodostetaan edellisestä salakirjoittamisen suorittaneesta lohkosta sekä avaimesta.

Kaikki salausmoodit (paitsi ECB) käyttävät lohkon salakirjoittamiseen edellisiä salakirjoitettuja lohkoja muuttamalla selväkielisanoman lohkolla ennen sen salakirjoitusta. /13/

Salauksen hyvyys riippuu kolmesta tekijästä: salausalgoritmin vahvuudesta, salausavaimen pituudesta ja avainten vaihdon tiheydestä.

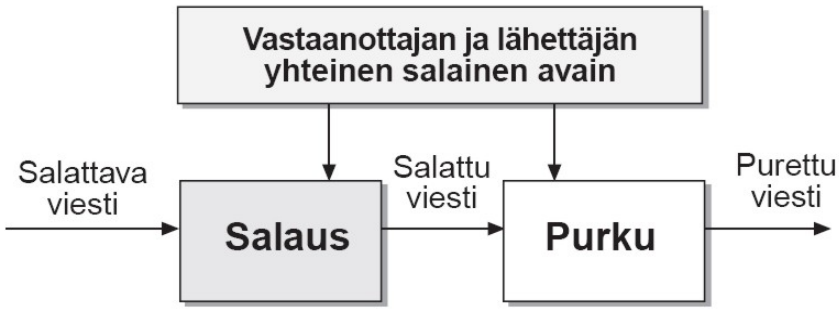
4.1 Symmetrinen salaus

Symmetrisessä salauksessa viestin salauksen purkamiseen tarvittava avain on suoraan johdettavissa salausavaimesta. Käytännössä symmetrisissä salausalgoritmeissa viesti salataan ja salaus puretaan samalla avaimella (kuva 3). Symmetriset salausalgoritmit jaetaan yleisesti jono- ja lohkosalausmenetelmiin. /24/

Symmetristen salausmenetelmien merkittävin etu on salausmenetelmän nopeus. Erityisesti symmetristä salausta varten rakennetut

laitetoteutukset pääsevät satojen megatavujen läpimenoaikoihin sekunnissa. Symmetrinen salaus on myös menetelmänä perinteinen, joten symmetristen salausjärjestelmien toteuttamisella on pitkä historia.

Ongelmana symmetrisessä salauksessa on avainten hallinta, sillä sekä viestin lähettäjällä että vastaanottajalla tulee olla tiedossaan sama salausavain. Avaimen välittämiseen osapuolien välillä tarvitaan jokin turvallinen menetelmä. Tällaisia menetelmiä ovat esimerkiksi avaimen toimittaminen henkilökohtaisesti (esimerkiksi levykkeellä) tai avaimen välittäminen salattuna (epäsymmetrinen salaus). /24/



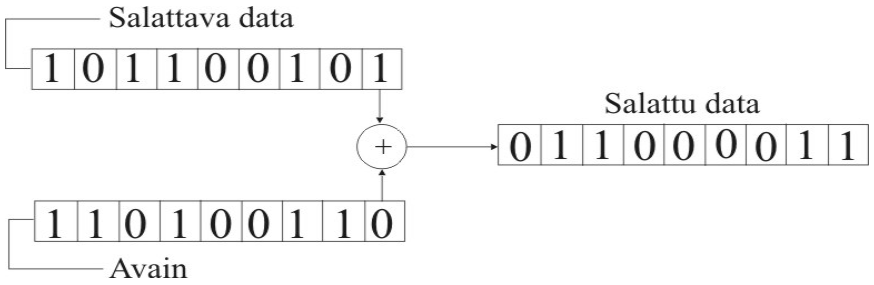
Kuva 3. Symmetrisen salauksen periaate /24/

4.1.1 Jonosalaus

Jonosalauksessa käytetään avain- ja selkodataparia, joille tehdään bitti bitiltä modulo 2 yhteenlasku eli XOR-operaatio (kuva 4). Salaustulos on ykkönen, jos datan ja avaimen biteistä toinen on ykkönen, ja nolla, jos biteillä on sama arvo. Sanoma avataan tekemällä sama operaatio salatun datan ja avaimen kesken. /3/

Jos tavoitellaan suurta salausnopeutta, mutta yksinkertaista rakennetta, on jonosalaus tähän hyvä ratkaisu. Hyviä ja vapaasti käytettäviä jonosalaajia on vain muutamia. Jonosalaimia käytetään lähinnä

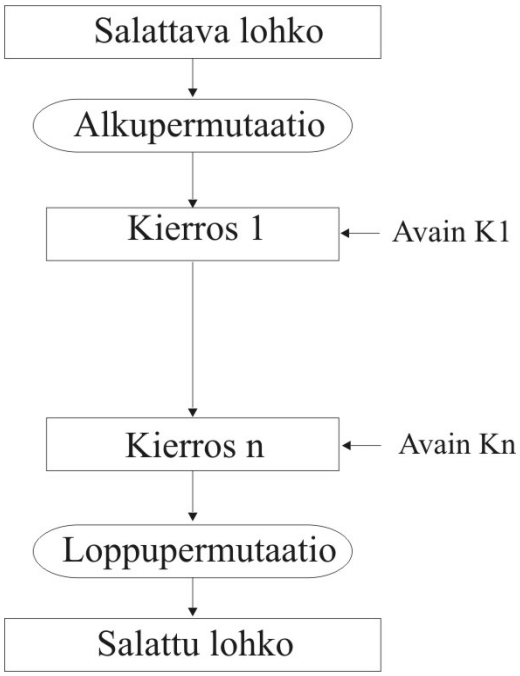
sulautetuissa laitteissa eivätkä valmistajat mielellään julkaise niiden toimintaperiaatetta. /6/



Kuva 4. Jonosalauksen periaate. /3/

4.1.2 Lohkosalaus

Lohkosalaajissa algoritmeille syötetään useampi bitti tai merkki kerrallaan eli lohkoina. Yleensä nämä lohkot ovat 64 tai 128 bitin kokoisia. Salaus tapahtuu siis lohko kerrallaan. Jos salattavan tiedon pituus on pienempi kuin lohkonpituus, lisätään tiedon perään täytettä. Alussa ja lopussa lohko permutoidaan eli bittien järjestys sekoitetaan. /13/



Kuva 5. Lohkosalauksen periaate. /3/

4.1.3 DES

Symmetrisistä salausalgoritmeista tunnetuin lienee edelleen laajasti käytetty DES (Data Encryption Standard), joka on tunnettu myös nimellä DEA (Data Encryption Algorithm) DES käyttää neljää erilaista salausmoodia (ECB, CBC, CFB ja OFB). DES-algoritmi perustuu lohkosalaukseen, joka käyttää 64 bitin lohkoja ja 56-bittistä avainta. DES on ollut 1970-luvulta lähtien maailmanlaajuinen standardi ja sen johdannaiset, kuten 3DES, ovat edelleen laajasti käytössä. 3DES on salausalgoritmi, jossa sama tieto salataan kolmeen kertaan peräkkäin eri salausavaimella. DES-algoritmia, varsinkaan alhaisilla avainten pituuksilla käytettynä, ei voida enää pitää riittävän turvallisena kaikkiin käyttötarkoituksiin. DES-salaus on onnistuttu murtamaan läpikäymällä avainavaruus. /13/

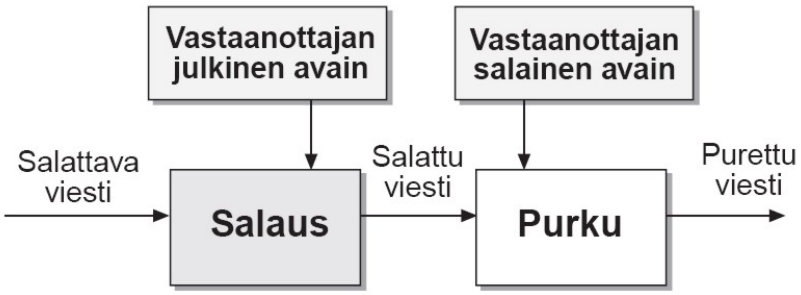
4.1.4 AES

DES-algoritmin seuraajaksi on valittu AES (Advanced Encryption Standard), joka on USA:n hallituksen ja yksityisen sektorin kehitystyön tuloksena syntynyt standardi. AES:n salausalgoritmina käytetään Rijndaelia, jonka kehitti kaksi belgialaista tutkijaa, Joan Daemen ja Vincent Rijmen. Rijndael on siis yhdistelmä heidän nimistään ja on lohkosalaukseen perustuva symmetrinen salausalgoritmi. AES-standardin mukaiset avainpituudet ovat 128, 192 ja 256 bittiä. Valintaprosessin yhteydessä Rijndaelin todettiin estävän kaikki tunnetut lineaarisen ja differentiaalisen analyysin muodot. Menetelmä on kuitenkin niin uusi, ettei sen kaikkia heikkouksia tunneta. /16/

Muita yleisesti käytössä olevia symmetrisiä salausalgoritmeja ovat mm. IDEA (International Data Encryption Algorithm), Blowfish, RC5 ja CAST. /24/

4.2 Epäsymmetrinen salaus

Epäsymmetrisessä salauksessa käytetään avainparia, joista toinen avain on julkinen (public key) ja toinen vastaavasti yksityinen (private key) (kuva 6). Avaimet ovat vaihtokelpoisia siten, että julkisella avaimella salattu viesti voidaan avata kyseessä olevan avainparin yksityisellä avaimella ja päinvastoin. Esimerkiksi salattaessa sähköpostiviestejä viesti salataan vastaanottajan julkisella avaimella, jolloin vastaanottaja avaa viestin omalla yksityisellä avaimellaan. Koska vastaanottajan yksityinen avain on ainoastaan vastaanottajan hallinnassa, kolmas osapuoli ei pysty purkamaan hänen julkisella avaimellaan salattua viestiä. /16/



Kuva 6. Asymmetrinen salauksen periaate. /24/

Epäsymmetristä salausta voidaan käyttää myös viestin eheyden varmistamiseen siten, että viestin lähettäjä salaa viestin omalla yksityisellä avaimellaan, jolloin viestin vastaanottaja voi varmistua viestin lähettäjästä purkamalla salaus käyttäen lähettäjän julkista avainta.

Epäsymmetrisen salauksen merkittävimpiä etuja symmetrisiin salausalgoritmeihin verrattuna on avaintenhallinnan yksinkertaisuus. Julkisen avaimen algoritmien heikkoutena pidetään salauksen hitautta. Lisäksi julkisen avaimen salauksessa avainten pituudet pidetään huomattavasti pidempinä kuin salaisen avaimen algoritmeissa.

Epäsymmetrisen salauksen avainpituuksia ei voi verrata symmetrisiin salausmenetelmiin. RSA:ta murrettaessa ei tarvitse kokeilla kaikkia mahdollisia avaimia. Riittää kun kokeillaan niitä, jotka täyttävät avaimelta vaadittavat matemaattiset ominaisuudet. Esimerkiksi kaikki parilliset luvut voidaan jättää kokeilematta, koska ne eivät ole alkulukuja. Siksi epäsymmetristen avainten on oltava pidempiä kuin vastaavan turvatason antavat symmetriset avaimet. /6/

Epäsymmetrisen salauksen kehittivät Whitfield Diffie ja Martin Hellman. /16/

4.2.1 RSA

Suosituimman epäsymmetrisen salausalgoritmin kehittivät kuitenkin Ron Rivest, Adi Shamir ja Leonard Adleman. Algoritmin nimeksi tuli tekijöiden mukaan RSA. Se julkaistiin vuonna 1978. Sen vahvuus perustuu suurten lukujen tekijöiden jakamisen vaikeuteen. Algoritmin menestys on puolestaan perustunut yksinkertaiseen ideaan ja helppoon toteutettavuuteen. RSA on patentoitu Yhdysvalloissa, mutta patentti vanheni syksyllä 2000. RSA on siirtosalaaja ja siinä käytetään yleensä 1024 – 4096-bittisiä avaimia. Mitä suurempaa avainta käytetään, sitä hitaampi se on. /13/

RSA-menetelmässä salaaminen ja avaaminen perustuu siihen, että sanomalohko korotetaan erittäin suureen potenssiin modulolaskentaa käyttäen. RSA-menetelmässä valitaan aluksi kaksi suurta jaotonta lukua p ja q, joiden tulo $pq = n$. Seuraavassa esitetty avainparin luominen. /22/

1. Valitaan kaksi erittäin suurta alkulukua, luvut p ja q
2. Lasketaan luku $n = pq$
3. Lasketaan phi, $\Phi = (p\text{-}1)(q\text{-}1)$
4. Valitaan pariton luku e, joka on $1 < e < \Phi$
5. Lasketaan luku $d = e\text{-}1 \bmod \Phi$
6. Julkinen avain on $\{n, e\}$, salainen avain on d

Salaus: $c = m^e \bmod n$

Purku: $m = c^d \bmod n$

Seuraavassa esimerkki, jossa laskettu RSA:n julkinen- ja salainen avain pienillä luvuilla. /22/

1. $p = 47$, $q = 71$
2. $n = pq = 3337$
3. Lasketaan phi, $\Phi = 46 * 70 = 3220$
4. Valitaan $e = 79$

5. Lasketaan $d = 79^{-1} \bmod 3220 = 1019$
6. Julkinen avain on n ja e, salainen avain d, hylätään p ja q.

Salattu viesti $m = 688$, $68879 \bmod 3337 = 1570 = c$.

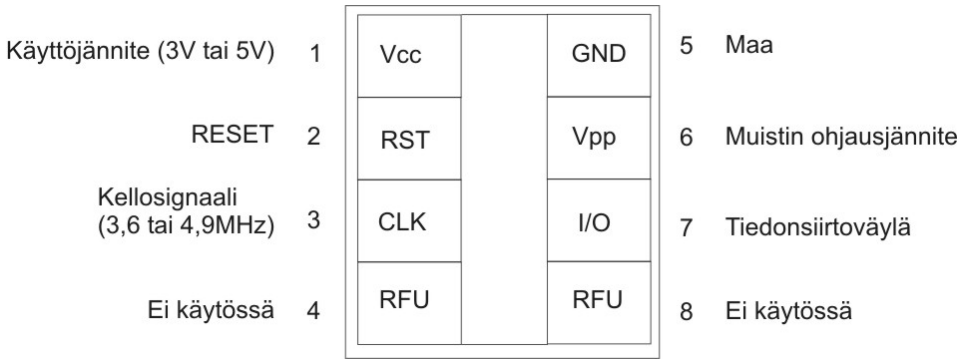
Avattu viesti $c = 1570$, $15701019 \bmod 3337 = 688 = m$.

RSA-menetelmän turvallisuus perustuu siihen, että modulusta n ei voi alkutekijöihin p ja q niiden suuruuden takia. Moduluksen tulee olla vähintää 1024 bitin pituinen luku. Alkulukujen p ja q valinnassa on noudatettava tiettyjä sääntöjä, jotta ratkaisemisessa ei voida käyttää oikotietä. Sitä mukaan kun alkutekujöihin jakoon keksitään tehokkaampia keinoja, on pidennettävä avaimia. /3/

RSA-576 selvitettiin joulukuussa 2003. /17/

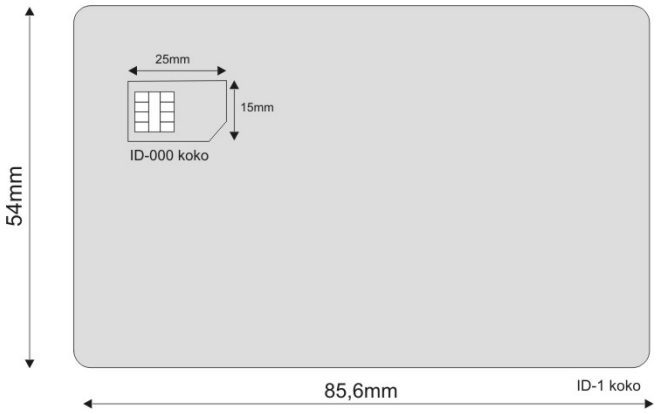
4.3 Toimikortti

Toimikortit sopivat hyvin salasanojen sekä salaustunnistusten turvallisiksi säilytyspaikoiksi, joten niitä voidaan käyttää käyttäjän tunnistetietojen tallentamiseen. Toimikortilla voidaan toteuttaa käyttäjän todentaminen. Toimikortin sijoittaminen laitteeseen toimii käyttäjän autentikointivälineenä. Myös käyttäjäkohtaiset parametrit voidaan sijoittaa kortille. Tietojen tallentamisen lisäksi toimikortit pystyvät suorittamaan matemaattisia toimintoja ja ohjelmia, joten niiden avulla voidaan toteuttaa salausta ja monenlaisia tunnistusprotokollia. Toimikortille kytkeydytään kahdeksalla standardoidulla kontaktinastalla. Toimikorttien fyysiset mitat ja sirun nastajärjestys on määritelty ISO 7816 -standardiperheessä. Toimikortti saa tarvittavan ulkoisen käyttöjännitteen liitännän kautta (kuva 7). /6/



Kuva 7. Toimikortin prosessorin kontaktinastat. /6/

Toimikortti on luottokortin kokoinen ns. ID-1 koko (kuva 8), johon mikropiiri on upotettu.



Kuva 8. ID-1 kokoinen toimikortti. /6/

Setec:n tarjontaa /23/:

PKI	RSA-apuprosessori
Kortti	SetCard™
EEPROM-muistia	16 kilotavua
Avaimen pituus max	1024 bittiä
Lisäalgoritmit	DES, 3DES, DESX

5 SIIRTOVERKOT

5.1 PSTN siirtoverkkona

Vanhin vertailtavista siirtoverkkotekniikoista on analoginen piirikytkentäinen puhelinverkko ja siihen tarkoitettu modeemi. Tämän päivän modeemit siirtävät teoriassa jopa 56 kb/s operaattorilta käyttäjälle (downlink), mutta tämä vaatii, että yhteyden toisessa päässä pitää olla digitaaliseen verkkoon kytketty laite. Jos molemmissa päissä on analoginen modeemiliittymä, voi siirtonopeus olla maksimissaan 33,6 kb/s. Muunnos analogisesta digitaaliseen tehdään PCM-moduloinnilla, jonka näytteenottotaajuus ja kvantisointikohina rajoittavat siirtonopeutta. Vaikka käytössä on digitaalinen puhelinverkko, modeemiyhteydet käyttävät tätä analogiverkon tavoin. /14/

Modeemi on siirtotien ominaisuuksiin mukautuva laite ja tästä seuraa, että modeemeille annetut nimelliset nopeudet eivät käytännössä vastaa saatuja arvoja. Modeemi, jonka nopeus on 33,6 kb/s, vaatii erittäin hyvänlaatuisia yhteyksiä toimiakseen edes lähellä maksiminopeutta. Kun yhteyttä muodostetaan, niin modeemit tutkivat siirtotien todellisen kaistanleveyden ja signaali/kohinasuhteen kaistan sisällä usealla taajuusalueella. Tämä tapahtuu siten, että modeemit lähettävät toisilleen tunnetulla tasolla ja taajuudella olevan signaalin, jonka perusteella vastaanottaja voi määritellä yhteyden laadun ja suurimman käytettävissä olevan kaistanleveyden. Siirron aikana modeemit tekevät myös nopeudenvaihdoksia ja olosuhteiden huonontuessa voi siirtonopeudet pudota jopa 4,8 kb/s asti. /14/

Teoreettisena rajana on pidetty 35 - 40 kb/s nopeutta Shannonin mallin mukaan. Rajoittavina tekijöinä piirikytkentäisessä siirtoverkossa

voidaan pitää verkon signaali-kohinasuhdetta, verkossa käytettyjä erillaisia muuntimia ja erilaisia epälineaarisuuksia. /18/

5.2 Ilmatie siirtoverkkona

5.2.1 GSM-Data

GSM-verkon perustiedonsiirtopalvelu on GSM-data. GSM-data on piirikytkentäinen tiedonsiirtotekniikka, jonka avulla matkapuhelinliittymällä on mahdollista soittaa datapuheluita. GSM-datan suurin mahdollinen tiedonsiirtonopeus on 14,4 kb/s. / 7/

5.2.1.1 HSCSD

HSCSD (High Speed Circuit Switched Data) on GSM-verkon nopea piirikytkentäinen tiedonsiirtotekniikka, joka on käytettävissä GSM-verkossa. /7/

HSCSD-tiedonsiirtotekniikka mahdollistaa datapuhelun soittamisen matkapuhelinliittymällä. HSCSD:n suurin mahdollinen tiedonsiirtonopeus GSM-verkossa on 57,6 kb/s. Käytännön tiedonsiirtonopeus jää teoreettisen huippunopeuden alle. Todellinen nopeus riippuu päätelaitteesta, verkon liikennemäärästä ja kuuluvuudesta. Parhaimmillaan HSCSD-tekniikalla päästään käytännössä noin 40 kb/s –nopeuksiin. /7/

HSCSD-pohjautuu GSM-verkon GSM-dataan. Lisänopeus saavutetaan tehokkaammalla radiokoodauksella ja usean rinnakkaisen GSM-verkon puhekanavan käyttämisellä. /7/

5.2.1.2 GSM:n salaus

GSM-verkossa radiorajapinnan salaus tehdään A5-salauksella. Salaukseen käytetään laskettavaa *kc*-salausavainta, joka syötetään algoritmiin. Salausavain *kc* vaihtuu jokaisella yhteydellä. Käyttäjän puolella A5 sijaitsee puhelinlaitteessa ja verkon puolella tukiasemasassa. A5-algoritmi on määritetty epäjulkiseksi. GSM-verkossa on on määritetty seitsemän erilaista A5-algoritmia. Tällä hetkellä on käytännössä toteutettu kaksi, A5/1 ja A5/2. A5/1 on hyvän suojan antava versio ja A5/2 on helpommin murrettavissa. Salausavaimen *kc* pituus on 64 bittiä, mutta 10- bittiä on nollaa, joten tehollinen avaimen pituus on 54 bittiä. Suomessa algoritmista käytetään versiota A5/1. /29/

GSM-verkossa radioliikenne tukiaseman ja puhelimen välillä liikkuu salattuna. Tukiasemasta eteenpäin kaikki data liikkuu GSM-järjestelmän runkoverkossa normaalissa tilanteessa salaamattomassa muodossa, ellei näihin yhteyksiin ole asennettu tapauskohtaisesti jotain lisäsalausta. /29/ Uusi suositus GSM-salaukseen on A5/3 (kts. EDGE:n salaus 5.2.3.1). /30/

5.2.2 GPRS

GPRS-tekniikka (General Packet Radio Service) on GSM-verkon pakettikytkentäisen tiedonsiirron perustekniikka, joka on käytettävissä kaikkialla GSM-verkossa. GPRS-tekniikka on liittymän peruspalveluna kaikkien matkapuhelinasiakkaiden käytössä. GPRS-tekniikan hyödyntäminen edellyttää, että käytössä on GPRS-tekniikkaa tukeva puhelin. /7/

GPRS:n pakettidatan liikennekanavilla on määritty neljä kanavakoodausluokkaa CS-1, CS-2, CS-3 ja CS-4. CS-1 käyttää tehokkainta kanavakoodausta ja sen datanopeus on hitain. Sen sijaan CS-4 luokalla päästään 21,4 kb/s. Taulukossa 3 on esitetty kanavakoodausluokkien datanopeudet. GPRS-tekniikan suurin

mahdollinen teoreettinen nopeus on n. 160 kbit/s kun käytetään kahdeksaa aikaväliä kanavakoodauksella CS-4, mutta pakettidatan ohjauskanaville käytetään aina kanavakoodausluokkaa CS-1. /4/ Tällöin nopeus jää maksimissaan noin 72 kb/s.

Taulukko 3. GPRS-verkon nopeuden koodaustaulukko /4/

Koodaus	Maksimi datanopeus kb/s
CS-1	9,05
CS-2	13,4
CS-3	15,6
CS-4	21,4

Käytännössä GPRS:n kuten muidenkin pakettikytkentäisten tekniikoiden nopeus riippuu verkon ominaisuuksien ja kuormituksen lisäksi käytettävästä tietoliikennekortista/ puhelimesta. Siksi käytännön tiedonsiirtonopeus jää aina teoreettisten huippuarvojen alle. GPRS-tekniikalla saavutetaan parhaimmillaan noin 40 kbit/s siirrettäessä tietoa verkosta puhelimelle ja noin puolet tästä siirrettäessä tietoa puhelimelta verkkoon. /7/

GPRS-tekniikka toimii yhteen GSM-verkon EDGE-tekniikan ja UMTS-verkon pakettikytkentäisen tiedonsiirtopalvelun kanssa. /7/

5.2.2.1 GPRS:n salaus

GPRS-salaukseen on määritelty A5-salausalgoritmi GEA3. Algoritmiin on määritelty 64 – 128-bittinen avainpituus. Tämän hetken määritys on 64-bittinen avainpituus. GEA3 perustuu lohkosalausalgoritmiin nimeltä F8, joka perustuu salauskerneliin nimeltä KASUMI. Algoritmi on epäjulkinen. /30/

5.2.3 EDGE

EDGE (Enhanced Data Rates for GSM Evolution) on nopea pakettikytkentäinen GSM-verkon tiedonsiirtotekniikka. EDGE vastaa palveluiltaan GPRS-tekniikkaa, mutta GPRS:ää merkittävästi tehokkaamman radiotekniikan ja –koodauksen ansiosta EDGE:n avulla on mahdollista saavuttaa huomattavasti GPRS:ää suurempi tiedonsiirtonopeus (taulukko 4). /7/

EDGE-tekniikka on otettu käyttöön GSM-verkossa suurimmissa kaupungeissa ja palvelun käyttöalue laajenee jatkuvasti GSM-verkon uudistustöiden mukana. EDGE:n palvelualueen laajenemisen mukana nopeat tiedonsiirtoyhteydet ovat käytössä monilla alueilla, joille UMTS-verkkoa ei ensi vaiheessa rakenneta. /7/

EDGE-tekniikka on liittymän peruspalveluna6 kaikkien matkapuhelinasiakkaiden käytössä. EDGE-tekniikan hyödyntäminen edellyttää, että käytössä on EDGE-tekniikkaa tukeva tietoliikennekortti/puhelin. /7/

EDGE-tekniikan suurin teoreettinen nopeus GSM-verkossa on 236,8 kb/s. EDGE:n nopeus riippuu verkon ominaisuuksien ja kuormituksen lisäksi käytettävästä tietoliikennekortista/puhelimesta. Toistaiseksi nopein tarjolla oleva puhelin tukee huippunopeutta 236,8 kb/s verkosta puhelimelle, mutta puhelimelta verkkoon suurin mahdollinen nopeus on vain puolet tästä eli 118,4 kb/s. Käytännön tiedonsiirtonopeudet jäävät teoreettisten huippuarvojen alle. Käytännössä EDGEllä saavutetaan parhaimmillaan n. 150 kb/s nopeus siirrettäessä tietoa verkosta puhelimelle ja noin puoleen tästä siirrettäessä tietoa puhelimelta verkkoon. EDGE-tekniikka toimii yhteen GSM-verkon GPRS-tekniikan ja UMTS-verkon pakettikytkentäisen tiedonsiirtotekniikan kanssa. /7/

EDGE:n käyttämiä kanavakoodausluokkia kutsutaan nimellä MSC (modulation and coding scheme). Luokat MCS-1 – MCS-4 käyttävät GSM:n modulointia, kun luokat MCS-5 – MCS-9 käyttävät 8-PSK modulaatiota. Taulukossa 4 on esitetty EDGE:n datanopeuksia eri koodausluokilla. /25/

Taulukko 4. EDGE:n datanopeuksia eri koodausluokilla. /25/

Koodausluokka	**Datanopeus/ aikaväli (kb/s)**
MSC-9	59,2
MSC-8	54,4
MSC-7	44,8
MSC-6	29,6
MSC-5	22,4
MSC-4	17,6
MSC-3	14,8
MSC-2	11,2
MSC-1	8,8

5.2.3.1 EDGE:n salaus

EDGE:n salaus perustuu samaan algoritmiin A5/3, kuin uusi GSM suositus. Myös A5/3 algoritmi on epäjulkinen. Avaimen pituus *kc* on säädettävissä välillä 64 bittä – 128 bittiä, mutta nykyinen suositus on 64 bittiä. /30/

5.2.4 TETRA

TETRA (TErrestrial Trunked RAdio) on viranomaisten käyttöön tarkoitettu kansainvälinen radioverkko ja se on ETSI:n määrittelemä standardi. Standardin pohjaksi on luotu yhteistyöelin Tetra MoU (Memorandum of Understanding) joka perustettiin vuonna 1994. Nykyään siihen kuuluu noin sata organisaatiota, jotka edustavat laitevalmistajia, operaattoreita ja palveluntarjoajia. Suomesta Tetra

MoU:hun kuuluu mm. Instasec ja Nokia. Tetra on GSM:n kaltainen, mutta suurelta yleisöltä suljettu verkko. Se on tällä hetkellä poliisin, palokunnan ja muiden viranomaisten käytössä. Suomessa määrityksen mukaista verkkoa kutsutaan viranomaisverkoksi eli Virveksi. /9/

Tetra-taajuudet on jaettu neljän aikavälin muodostamiin kehyksiin. Puheen koodauksen nopeus on 7,2 kb/s sisältäen virheenkorjauksen. Datan raakabittinopeus (cross bit rate) on 36 kb/s neljää aikaväliä käytettäessä. Tästä arvosta, suojausluokasta ja aikavälien jaottelusta riippuen voidaan hyötydataan käyttää 2,4 – 28,8 kb/s. Tetran datasiirrossa käytetään samoja periaatteita kuin GSM:n HSCSD:ssä tai GPRS:ssä eli siinä on nopeudeltaan muuttuva datasiirto riippuen käytettävästä kanavakoodauksesta ja aikavälien lukumäärästä. Piirikytkentäisen datansiirron lisäksi Tetra-järjestelmään on määritelty myös pakettikytkentäiset yhteydet. Tetra-verkko tukee IP-protokollia Ipv4 ja Ipv6. /9/

5.2.4.1 Tetran salaus

Tetran ilmatiesaluksessa salataan radiolaitteen ja tukiaseman välinen liikenne. Tetra-standardissa radiorajapinnan salausmääritys jakautuu kolmeen luokkaan. Standardi ei määrittele käytettävää salausalgoritmia, mutta TETRA MoU suosittelee IDEA-algoritmia. Luokkien määrittelyt ovat seuraavat: /26/

Ilmatiesalaus (Air interface encryption - AIE)

Luokka 1 - Salaamaton

Digitaalinen TETRA koodaus tarjoaa vakio digitaalisen ”suojauksen” ilman staattisia tai dynaamisia avaimia. Käytännössä on taso, jossa ei ole salausta.

Luokka 2 - SCK

Ilmatie on salattu vahvalla ETSI:n määrittelemällä salausalgoritmilla ja staattisella salausavamilla (static cipher key (SCK)). Pysyvä avain tarkoittaa tässä tapauksessa, että salausavain on ohjelmoitu TETRA-radioon.

Luokka 3 - DCK/CCK

Kolmas luokka on vahvin ja ilmatie on salattu ETSI:n määrittelemällä salausalgoritmilla ja *johdetulla* salausavaimella (DCK-derived cipher key)

Perus-salausavain (CCK- common cipher key) avain liikenteensalaukseen tukiasemalta TETRA-radiolle. Avain on yksilöllinen joka tukiasemalla ja vaihtuu säännöllisesti.

Taulukossa 5 on kuvattu käyttäjän datanopeudet käytettäessä eri salausluokkia.

Taulukko 5. Tetran nopeusluokat /9/

Suojaus	1 aikaväli kb/s	2 aikaväliä kb/s	3 aikaväliä kb/s	4 aikaväliä kb/s
Luokka 1	7,2	14,4	21,6	28,8
Luokka 2	4,8	9,6	14,4	19,2
Luokka 3	2,4	4,8	7,2	9,6

6 INTERNET-SIIRTOPROTOKOLLAT

Digitoidun puheen pakkaus IP-paketteihin tuo vielä oman lisänsä kokonaiskuormaan. Pakkaamaton PCM-puhe kulkee normaalisti yhdellä 64 kb:n ISDN-kanavalla, mutta VoIP-muodossa kaistantarve nousee helposti 90 kb/s. G.723.1:n 5.3 kb/s voi nousta jopa 20 kb/s.

6.1 IP-protokolla

IP-protokolla (Internet Protocol) on TCP/IP-protokollaperheen perusta. Kaikki muut TCP/IP:n protokollat toimivat sen päällä. IP-protokollan keskeisin tehtävä on loogisten osoitteiden lisääminen datavirtaan, jolloin muodostuu yhdessä kuljetustason porttinumeron kanssa yhteyden indentifioivat socketit. IP-protokolla toimii verkkokerroksessa ja tarjoaa yhteydettömän (connectionless) palvelun kuljetuskerrokselle, eli se ei pidä yhteyksiä tietokoneiden välillä eikä varmista viestin perille pääsyä, vaan lähettää viestit halutulle tietokoneelle. /13/

IP:n oleellinen tehtävä on siirtää kehyksissään oleva data paikasta toiseen. Tämän mahdollistaa IP-osoite, joka annetaan jokaiselle verkkoon liitettävälle laitteelle.

6.1.1 IP-protokollan viestit

IP-protokollan viestit (datagrammit) kulkevat verkossa paketteina. Viesti lähetetään joko yhdessä paketissa tai se voidaan jakaa useampaan eri pakettiin. Pakettiin kuuluu otsikkotiedot sekä sisältö eli hyötykuorma. IP-protokollan pakettien otsikkotiedot ovat kuvattu kuvassa 9. /13/

<table>
<tr><th colspan="8">IP-prokollan otsikkotiedot</th></tr>
<tr><td colspan="2">1. tavu</td><td colspan="2">2. tavu</td><td colspan="2">3. tavu</td><td colspan="2">4. tavu</td></tr>
<tr><td>Versio</td><td>IHL</td><td colspan="2">Palvelun tyyppi</td><td colspan="4">Paketin koko</td></tr>
<tr><td colspan="4">Tunniste</td><td>Liput</td><td colspan="3">Sijainti viestissä</td></tr>
<tr><td colspan="2">TTL</td><td colspan="2">Protokolla</td><td colspan="4">Tarkistussumma</td></tr>
<tr><td colspan="8">Lähdeosoite</td></tr>
<tr><td colspan="8">Kohdeosoite</td></tr>
<tr><td colspan="6">Optiot</td><td colspan="2">Täyte</td></tr>
<tr><td colspan="8">Data</td></tr>
</table>

Kuva 9. IP-protokollan otsikkotiedot. /13/

Versio - (4 bittiä) kertoo protokollan version

IHL – (4 bittiä) kertoo otsikon pituuden laskettuna 32 bitin osissa (pituus jaettuna 32:lla)

Palvelun tyyppi – (8 bittiä) käytetään viestin tärkeysjärjestyksen merkitsemiseen.

Paketin koko – (16 bittiä) kertoo paketin koon tavuina laskettuna. Suurin mahdollinen koko on 65 535 tavua

Tunniste – (16 bittiä) sisältää yksilöllisen pakettinumeron. Kenttä käytetään lohkottaessa datagrammeja.

Liput – (3 bittiä) käytetään lohkottaessa

Sijainti viestissä – (13 bittiä) käytetään lohkottaessa

TTL – (8 bittiä) kertoo paketin elinajan (*time to live*). Aina kun pakettiin osallistuva laite vastaanottaa ja lähettää sen eteenpäin, elinaikaa vähennetään yhdellä. Jos kentän arvoksi tulee nolla, paketti tuhotaan.

Protokolla – (8 bittiä) kertoo, mitä protokollaa paketin sisältö käyttää. Yleisimmät protokollat ovat ICMP, TCP ja UDP

Tarkistussumma – (16 bittiä) varmistetaan, että paketin otsikkotiedot eivät ole muuttuneet kuljetuksen aikana. tarkistus suoritetaan jokaisessa pakettia käsittelevässä laitteessa (esim. reitittimet ja palvelimet)

Lähdeosoite – (32 bittiä) kertoo lähettäjän IP-osoitteen.

Kohdeosoite – (32 bittiä) kertoo vastaanottajan IP-osoitteen.

Optiot – (max. 320 bittiä) lisämääritykset. Ei yleisessä käytössä. /13/

Täyte – Lisätään tarvittaessa siten, että otsikkotietojen pituus on jaollinen luvulla 32

6.2 TCP-protokolla

Kuljetuskerroksen TCP-protokolla (Transmission Control Protocol) on yhteydellinen protokolla (connection oriented) joten se varmistaa, että sen lähettämät tiedot saapuvat perille eli se tarjoaa sovelluksille päästä päähän luotettavan palvelun. Tämä tapahtuu siten, että vastaanottaja lähettää jokaisesta saamastaan viestistä kuittauksen lähettäjälle, jossa se kertoo, kuinka paljon tietoa se on vastaanottanut. Jos lähettäjä ei saa kuittausta viestiinsä tai ilmoitettu tietomäärä on liian pieni, matkalla hukkuneet tiedot lähetetään uudelleen. TCP-protokolla käyttää lähde- ja kohdeosoitteina porttinumeroita. Jokaisella TCP-protokollaa käyttävällä ohjelmalla on oma portti, jota se käyttää yhteyteen. /13/

6.2.1 TCP-protokollan viestit

TCP-protokollan viesti lähetetään IP-pakettien sisältönä. TCP-protokollan viestit lähetetään paketteina samalla tavalla kuin IP-protokollankin viestit. TCP- paketin otsikkotiedot ovat kuvattu kuvassa 10.

<table>
<tr><th colspan="6">TCP-protokollan otsikkotiedot</th></tr>
<tr><td colspan="2">1. tavu</td><td colspan="2">2. tavu</td><td colspan="1">3. tavu</td><td>4. tavu</td></tr>
<tr><td colspan="3">Lähdeportti</td><td colspan="3">Kohdeportti</td></tr>
<tr><td colspan="6">Järjestysnumero</td></tr>
<tr><td colspan="6">Kuittausnumero</td></tr>
<tr><td>HLEN</td><td>Varattu</td><td colspan="2">Kontrollibitti</td><td colspan="2">Vastaanottoikkunan koko</td></tr>
<tr><td colspan="3">Tarkistusumma</td><td colspan="3">Kiirellisen tiedon määrä</td></tr>
<tr><td colspan="3">Optiot</td><td colspan="3">Täyte</td></tr>
<tr><td colspan="6">Data</td></tr>
</table>

Kuva 10. TCP-protokollan otsikkotiedot. /13/

Lähdeportti – (16 bittiä) kertoo paketin lähettäneelle ohjelmalle kuuluvan porttinumeron.

Kohdeportti – (16 bittiä) kertoo paketin vastaanottavalle ohjelmalle kuuluvan porttinumeron.

Järjestysnumero – (32 bittiä) kertoo viestin ensimmäisen tavun järjestysnumeron, eli monesko lähettäjän tällä yhteydellä lähettämä tavu se on.

Kuittausnumero – (32 bittiä) käytetään kuittausviesteissä merkitsemällä siihen järjestysnumero, jonka lähettäjä olettaa olevan seuraavassa vastaanottajan lähettämässä viestissä.

HLEN - (4 bittiä) kertoo otsikkotietojen pituuden laskettuna 32 bitin osissa.

Varattu – (6 bittiä) tulee aina olla täynnä nollia

Konrollibitti – (6 bittiä) sisältää kuusi pakettia koskevaa lippua. Jos lippua vastaava bitti on 1, lippu on voimassa.

Konrollibitit					
1	2	3	4	5	6
URG	ACK	PSH	RST	SYN	FIN

Kuva 11. TCP-protokollan kontrollibitit. /13/

URG-lippu, paketissa on *kiireellisen tiedon määrä* kentän osoittama määrä kiireellistä tietoa.

ACK-lippu, kyseessä kuittausviesti, jolloin *kuittausnumero*-kentän sisältämä tieto tulee käsitellä.

PSH-lippu, paketissa oleva tieto tulee antaa ohjelmalle jolle se on tarkoitettu välittömästi ilman puskurointia.

RST-lippu, aiheuttaa yhteyden nollautumisen

SYN-lippu, paketti on yhteydenavauspyyntö

FIN-lippu, paketin lähettäjä haluaa lopettaa

Vastaanottoikkunan koko – (16 bittiä) kertoo, kuinka paljon tietoa lähettäjä voi lähettää saamatta kuittausta aikaisemmin lähetettyihin tietoihin.

Tarkistussumma – (16 bittiä) sisältää tarkistussumman, jolla pyritään varmistamaan että paketin tiedot eivät ole tahattomasti muuttuneet.
Optiot – sisältää erilaisia lisämäärityksiä paketille
Täyte – lisätään tarvittaessa, jotta otsikkotietojen koko olisi jaollinen 32:lla. /13/

6.3 UDP-protokolla

UDP-protokolla (User datagram Protocol) on yhteydetön, TCP-protokollaan verrattuna hyvin kevyt protokolla. Sovellukset, joilta ei vaadita luotettavuutta, voivat käyttää kuljetustason protokollana UDP-protokollaa kuten esimerkiksi puhesovellukset. UDP-protokolla käyttää IP-osoitteita ja portteja samalla tavalla kuin TCP-protokollakin. Myös porttien määrä on sama (0-65 535). /13/

6.3.1 UDP-protokollan viestit

UDP-protokollan otsikkotiedot			
1. tavu	2. tavu	3. tavu	4. tavu
Lähdeportti		Kohdeportti	
Paketin koko		Tarkistussumma	
Data			

Kuva 12. UDP-protokollan otsikkotiedot. /13/

Lähdeportti – (16 bittiä) kertoo paketin lähettäneen ohjelman porttinumeron.
Kohdeportti – (16 bittiä) kertoo paketin vastaanottavan ohjelman porttinumeron.
Paketin koko – (16 bittiä) kertoo paketin koon tavuina.
Vähimmäiskoko on 8 tavua ja enimmäiskoko 65 535 tavua.

Tarkistussumma – (16 bittiä) lasketaan IP-paketin lähde- ja kohdeosoitteista sekä protokollanumerosta, UDP-paketin otsikkotiedoista ja sisällöstä sekä UDP- paketin pituudesta. /13/

6.4 RTP-protokolla

RTP on UDP-protokollan päälle rakennettu protokolla, joka helpottaa reaaliaikaisten palvelujen kuten puheen ja kuvan reaaliaikaisen siirron. RTP-protokolla lisää UDP-pakettiin lisäotsakkeen, jonka avulla paketit voidaan helposti vastaanottaa oikeassa järjestyksessä ja esittää oikeaan aikaan. /2/

6.4.1 RTP-protokollan viestit

<table>
<tr><td colspan="8">RTP-protokollan otsikkotiedot</td></tr>
<tr><td colspan="2">1. tavu</td><td colspan="2">2. tavu</td><td colspan="2">3. tavu</td><td colspan="2">4. tavu</td></tr>
<tr><td>V</td><td>P</td><td>X</td><td>CC</td><td>M</td><td>PT</td><td colspan="2">Järjestysnumero</td></tr>
<tr><td colspan="8">Aikaleima</td></tr>
<tr><td colspan="8">Synkronisointilähteen tunniste (SSRC)</td></tr>
<tr><td colspan="8">Osallisten lähteiden tunnisteet (CSRC)</td></tr>
</table>

Kuva 13. RTP-protokollan viestit /20/

V versio - (2 bittiä) kertoo RTP version

P täyte – (1 bitti) kertoo, sisältääkö paketti täytemerkkejä.

X laajennus - (1 bitti) kertoo, onko otsikkolaajennus käytössä.

CC- (4 bittiä) CSRC-laskuri

M- (1 bitti) merkki, käyttö riippuu hyötykuormasta

PT- (7 bittiä) kertoo kuljetettavan hyötykuorman tyypin ja kuinka vastaanottavan sovelluksen tulee sitä käsitellä. Taulukossa 6 muutamia hyötykuormatyypejä.

Taulukko 6. RTP-protokollan hyötykuorman tyyppejä. /20/

PT	Kuorman tyyppi
2	G.721
4	G.723
9	G.722
18	G.728

Järjestysnumero – (16 bittiä) kertoo paketin järjestysnumeron. Arvoa kasvatetaan joka kerta kun RTP-paketti lähetetään.
Aikaleima – (32 bittiä), kertoo RTP-paketin aikaleiman
Synkronointilähteen tunniste – (32 bittiä) kertoo synkronisointilähteen
Osallisten lähteiden tunnisteet – (32 bittiä)

6.5 TCP/IP-yhteyden nopeuteen vaikuttavat tekijät

TCP/IP-yhteydessä on pidettävä mielessä kunkin protokollan lähettämän datayksikön koko. Tärkeimmät määritykset ovat IP-protokollan MTU (Maximum Transmission Unit) Ja TCP:n MSS (Maximum Segment Size). Ethernet verkossa MTU on yleensä 1500 bittiä. Se määräytyy verkkokortin suurimman kehyskoon 1518 bitin perusteella. Nykyisin myös käytetään MTU:n tilalla PMTU määritystä (Path Maximun Transmission Unit). Siinä IP:n käyttämä datagrammin maksimikoko määräytyy koko oman ja etäjärjestelmän välisen yhteyden perusteella. PMTU arvoksi tulee yhteyden välityskyvyltään heikoimman yhteysvälin MTU esim. reititin. Siirtoviiveen osalta yleissääntönä voidaan sanoa, että yli 150 millisekunnin yksisuuntainen viive tekee puheen laadusta käytännössä käyttökelvottoman. /8/

7 VOIP-PROTOKOLLAT

Ip-puhe eli Voip (Voice over internet protocol) ei ole itsenäinen standardi vaan kokoelma erilaisia tekniikoita ja niiden käyttötapoja. VoIP kuvaa tekniikkaa, jonka avulla missä tahansa TCP (Transmission Control Protocol) -verkossa välitetään puhetta IP (Internet Protocol) -protokollan mukaisesti paikasta toiseen. Erilaisia ratkaisumalleja on useita. Tässä esitellään kaksi yleisintä standardia ja kahden eri standardointijärjestön tuotosta eli H.323 ja SIP.

Ensimmäinen Voip-toimintoja määritellyt standardointi oli ITU-T:n (ITU Telecommunication standardization sector) H.323-suositus. Sen ensimmäinen versio julkaistiin vuonna 1996. Se kattaa puheyhteyksien lisäksi video- ja dataneuvottelut, ja siihen perustuvat esimerkiksi Microsoft NetMeeting ja monet kaupalliset videoneuvotteluohjelmat. H.323 on laajassa käytössä myös pelkkää puhetta siirtävissä järjestelmissä. /28/

7.1 H.323

H.323 on puhelinmaailmasta lähtöisin oleva standardi. H.323-määrittelyt ovat laajoja, ja niistä on julkaistu vuodesta 1996 lähtien lukuisia versioita, eikä eri toimittajien tuotteiden yhteensopivuus ole ollut käytännössä kovin hyvä. /28/

H.323-standardin mukaisessa verkossa signalointi tapahtuu neljällä siirtoprotokollalla, jotka ovat RAS (käyttäjien rekisteröinti ja tilatieto), Q.931 (huolehtii puhelun muodostuksesta ja lopetuksesta), H.245 (kanavien käyttö ja kapasiteetti) sekä H.235 (turvallisuus ja käyttäjän tunnistus). /28/

7.2 SIP (Session Initiation Protocol)

SIP-protokolla kehitettiin alun perin ryhmälähetysten hallintaa varten, mutta sen on havaittu sopivan myös muihin käyttötarkoituksiin, joista ehkä eniten on puhuttu Internet-puhelujen signaloinnista. SIP:n kehittäjät näkevät sen myös protokollana, jonka avulla mobiili maailma yhdistetään tehokkaasti Internetiin. SIP-protokollan vahvuus on erityisesti siinä, että se on perustoiminnoiltaan kohtuullisen yksinkertainen ja helposti laajennettavissa. SIP-protokolla osoittaa käyttäjää puhelinnumeron tai sähköpostiosoitteen muotoisella osoitteella. SIP-protokolla perustaa, ohjaa ja purkaa kutsut. SIP hyödyntää onnistuneesti monia jo aikaisemmin hyväksi havaittuja Internet-tekniikoita, kuten URL:ää, HTTP-tyyppisiä sanomia, MIMEä, DNS:ää ja XML:ää. SIP:n tarkoitus on pystyä tekemään yhtä yksinkertainen mekanismi puheluiden ja yhteyksien luontiin kuin mitä tavallisen puhelun ottaminen on. SIP on sovellustason protokolla, joka mahdollistaa päästä päähän tai monipiste- yhteydet. SIP on IETF:n määrittelemä standardi. /2/

SIP ei ota kantaa IP-puheen kannalta epäolennaisiin toimintoihin kuten koodekkien neuvotteluihin, joten yhteys saadaan muodostumaan muutaman paketin vaihdolla. Jos SIP havaitsee, että yhteyden toisessa päässä on H.323-laite, yhteydenotto jätetään tämän käytännöillä loppuun vietäväksi. SIP:n etuna pidetään sitä, että se on ympäristöltään ja toteutukseltaan kevyt verrattuna H.323:n puhelinkeskusmaailmaan, jonka lukuisat toiminnot ovat tehneet standardista raskaan ja vaikeaselkoisen. Myös Microsoft on korvannut H.323:n SIPillä Windows XP -sukupolven tuotteissaan. /2/

SIP koostuu seuraavista tehtävistä: /27/

1. *Käyttäjän sijainti* (*User Location*). Eli etsii verkosta päätelaitteen, jonka kanssa halutaan keskustella. Käyttäjän sijainti ilmaistaan URL:llä, SIP URL, jota vastaava sijaintitieto, yleensä IP-osoite, on pystyttävä selvittämään.

2. *Käyttäjän ominaisuudet* (*User capability Exchange*). Minkä tyyppisiä yhteyksiä vastaanottaja pystyy käsittelemään selvitetään SDP:llä (Session Description Protocol). Se määrittää keskustelukumppanin saatavuuden; käyttäjä on voinut paitsi sulkea laitteensa, myös ilmoittaa olevansa varattu, eikä siis halua ottaa vastaanottaa puheluita.

3. *Käyttäjän saavutettavuus* (*User availability*). Käyttäjän tavoitettavuus ko. Hetkellä. Keskustelu voi myös päätyä ei-puhemoodiin, eli esimerkiksi pikaviestintään tekstillä tai sähköpostiin.

4. *Yhteyden avaus* (*Call setup*). Yhteyden avaamiseen tarvittavien parametrien alustaminen puhelun eri päissä. Käynnistää istunnon hälyttämällä vastapäätä ja vaihtamalla tarvittavat parametrit keskustelukumppanin kanssa istunnon aikana.

5. *Puhelun hallinta* (*Call handling*). Meneillään olevien puheluiden siirto ja lopetus. SIP hoitaa puhelun hallinnan, esimerkiksi siirtää sen toiseen laitteeseen, vaihtaa koodekkeja, jos keskustelukumppanit haluavat ottaa vaikkapa videon käyttöön, ja lopuksi purkaa istunnon.

7.3 H.323:n ja SIP:n erot

Molemmat protokollat käyttävät video- ja äänivuon siirtoon RTP-protokollaa IP:n päällä. Taulukossa 7 on esitetty muutamia standardien eroja.

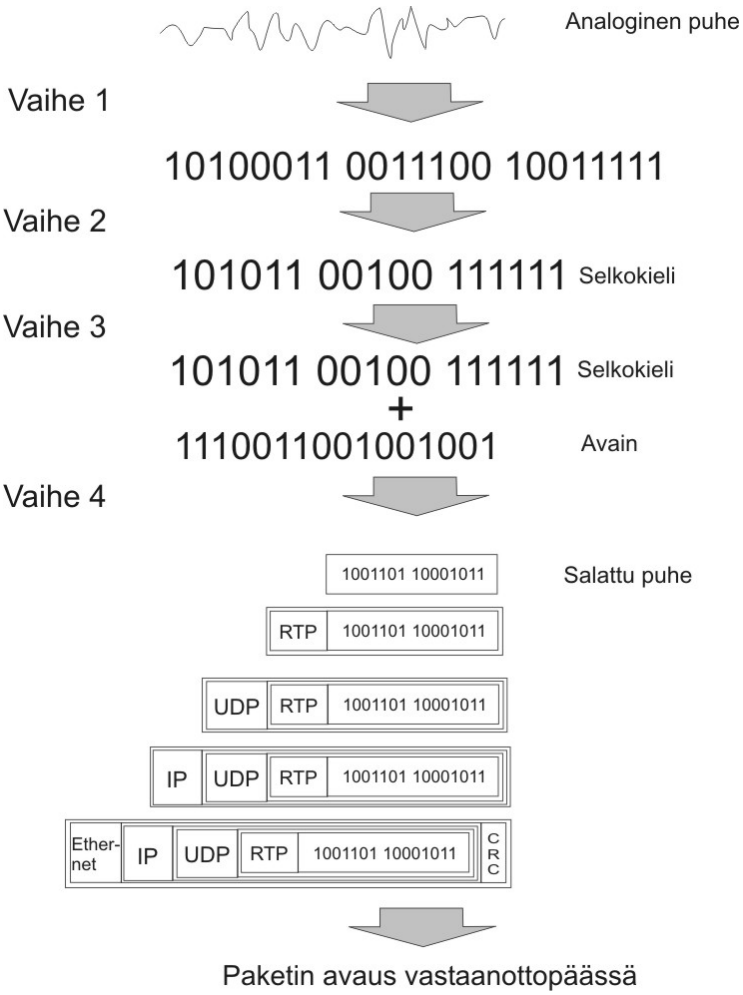
Taulukko 7. H.323- ja SIP-protokollien erot /2/

	PSTN	H.323	SIP
Arkkitehtuuri		Protokollapino	Elementti
Standardoija	ITU	ITU	IETF
Kuljetuskerros	Analoginen kaapeli, PCM multipleksaus	Suurimmaksi osaksi TCP	Suurimmaksi osaksi TCP
Merkinannon koodaus	Äänikoodit päätelaitteeseen	ASN.1	Esitetty ASCII-merkeillä, muistuttaa HTTP-protokollan koodausta
Osoitteisto	Puhelinnumero	Omat tunnisteet	Sähköpostiosoitteen näköinen SIP URL
Käyttötarkoitus	Äänipuhelut	Ääni- ja kuvapuhelut	Verkkomultimedia, IP-puhelut

8 PUHELIIKENNE IP-VERKOSSA

Edellä esitettyjen lukujen pohjalta voidaan muodostaa lähetettävä salattu paketti. Kuvassa 14 on yksinkertaistettuna esitetty salatun paketin muodostamisen vaiheet lähetettäväksi IP-paketiksi verkkoon. IP- paketin muodostuksessa on käytetty UDP-protokollaa, joka kevyempänä protokollana tarvitsee vähemmän kaistanleveyttä kuin TCP-protokolla.

8.1 Paketin kehystys



Kuva 14. Salatun IP-paketin muodostus

Vaihe 1: Analoginen puhe näytteistetään ja muutetaan digitaaliseksi dataksi.
Vaihe 2: Digitaaliseksi muutettu puhe pakataan valitulla puhekoodekilla.
Vaihe 3:Pakattu puhe salataan valitulla symmetrisellä salaus-menetelmällä.
Vaihe 4: Salattu puhe (nettodata) kehystetään. Kehykset sisimmäisistä uloimpiin. Suluissa ilmoitettu, kuinka paljon kehys tuo lisää kuormaa tavuissa. /19/

- RTP-protokolla (12 tavua)
- UDP-protokolla (8 tavua)
- IP-protokolla (20 tavua)
- Ethernet-kehystys ja CRC (18 tavua)

IP-pakettien otsikot ja kontrollipaketit on myös mahdollista pakata. Tällöin lähetetään vain muuttuneet kentät. Pakkauksella saadaan niiden osuus tippumaan kymmenesosaan, jolloin ne vievät 2- 4 tavua, 40 tavun sijaan. Esimerkiksi kun verrataan G.729 koodekilla pakattua puhetta niin ero on yli 40% tehokkaampi kaistankäyttö pakatuilla otsikkokentillä.

8.2 Tarvittava siirtokaista

Käytettäessä Voip-protokollia puheensalauksessa voidaan yhteyden tarvitsema siirtokaistantarve laskea. Laskelmat ovat suuntaa antavia, mutta kertovat, kannattaako yhteyttä edes ajatella salattavaksi standardi Voip-protokollien päällä hitailla yhteyksillä. Seuraavat kaavat /19/ ovat käytössä tarvittavaa siirtokaistaa laskettaessa.

Puhepaketin koko = (Ethernet-kehys) + (IP/UDP/RTP kehykset) + (nettopuhe)
Puhepaketteja sekunnissa (pps) = koodekin datanopeus/ nettopuhe
Kaistanleveys = Puhepaketin koko * pps

Esimerkki on laskettu koodekilla G.729, jonka bittinopeus on 8 kb/s ja puhenäytteen pituutena on käytetty 20 ms. Esimerkin otsikko- ja kontrollipaketteja ei ole pakattu.

Kun puhenäytteitä otetaan 20 ms:n välein niin paketteja tulee 50 pakettia sekunnissa. Tällöin nettopuhe on koodekin bittinopeus 8 kb /50 = 160 bittiä

Puhepaketin koko = 144 b + 320 b + 160 b = 624 b
Puhepaketteja sekunnissa (pps) = 8000 b/ 160 b = 50
Kaistanleveys = 624 b * 50 = 31 200 b/s

Siirtokaistan tarpeeseen on myös mahdollista vaikuttaa näytteen pituudella. Mitä pidempi näyte on, sitä pienempi on kaistan tarve. Kääntöpuolena asiassa on se, että kun pitempi paketti hukkuu se on helpommin korvilla havaittavissa.

Taulukkoon 8 on laskettu eri koodekkien tarvitsemia siirtokaistanleveyksiä.

Taulukko 8. Eri koodekkien tarvitsema siirtokaista

Puhekoodekki	Bittinopeus	Näytepituus	Kaistanleveys RTP	Kaistanleveys cRTP
G.711 (PCM)	64 kb/s	10 ms	110,4 kb/s	81,6 kb/s
	64 kb/s	30 ms	79,4 kb/s	69,9 kb/s
G.723.1 (ACELP)	5,3 kb/s	10 ms	51,7 kb/s	22,9 kb/s
	5,3 kb/s	30 ms	20,8 kb/s	11,2 kb/s
G723.1 (MP-MLQ)	6,4 kb/s	10 ms	52,8 kb/s	24,0 kb/s
	6,4 kb/s	30 ms	21,9 kb/s	12,3 kb/s
G.726 (ADPCM)	32 kb/s	10 ms	78,4 kb/s	49,6 kb/s
	32 kb/s	30 ms	47,5 kb/s	37,9 kb/s
G.729 (CS-CELP)	8 kb/s	10 ms	54,4 kb/s	25,6 kb/s
	8 kb/s	30 ms	23,5 kb/s	13,9 kb/s

9 YHTEENVETO

Verkon yli toteutettu puheensalaus toteutettuna yleisimmin käytetyillä VoIP-protokollilla tarvitsee kaistaa niin paljon, että sitä ei ole mahdollista toteuttaa varmasti kaikkein hitaimmilla siirtoteillä kuten PSTN:llä ja hitaimmilla ilmasiirtoteillä kuten GSM-data, GPRS ja Tetra-verkoissa. Tehokkaimmilla puheenpakkausmenetelmillä se on mahdollista hyvissä olosuhteissa, mutta kun siirtokaista pienenee olosuhteiden huonontuessa, tulee toiminnasta epävarmaa. Kun siirtokaistaa on tarpeeksi, ei yhteyden muodostaminen ja sen pitäminen yllä tuota ongelmia.

Jos hitaammilla siirtoteillä halutaan tehdä salattu puheyhteys päästä päähän, pitää siirtokuormaa pienentää. Yksi mahdollisuus tähän on epästandardin toiminnan toteuttaminen esimerkiksi jättämällä Voip-protokollan vaatima kehystys pois ja toteuttaa päästä päähän salaus modeemipääteyhteyden avulla. Tällöin laitteiden välille muodostetaan tavallinen pääteyhteys, joka salataan halutulla algoritmilla. Tämä toteutustapa pudottaa verkon siirtokuormaa jopa 70%, mutta samalla menetetään Voip-protokollien tuoma etu, esimerkiksi yhteensopivuus muiden valmistajien laitteiden kanssa ja pakettiverkko

Yksi mahdollisuus laitteen toteuttamiseen on, että laitteesta suunnitellaan ns. combo-laite, jolloin laitteessa on nopeita pakettiverkkoja varten Voip-standardin mukainen puheenkäsittely ja hitaita yhteyksiä varten salattu pääteyhteys.

Joka tapauksessa, jos operaattorien tekniseen tukeen on uskominen niin omatoiminen salaus on jollain lailla toteutettava, sillä he eivät pakettiverkkoa salaa tällä hetkellä mitenkään.

LÄHDELUETTELO

Painetut lähteet

1 Uotila, Pekka. Tietoliikenteen tekniikka. Gummerus 2000. 238 s.

2 Kehittyvä IP-protokolla. Prosessori 5/2002, s. 66-69.

3 Hämeen-Anttila Risto. Tietoliikennejärjestelmät. Edita 1996. 293 s.

4 Andersson Christoffer. GPRS and 3G Wireless Applications. Robert Ipsen 2001. 317 s.

6 Järvinen Petteri. Salausmenetelmät. Docendo 2003. 380 s.

8 Hakala Mika. Tietoverkon rakentaminen. Docendo 2002. 325 s.

9 Tetra on viranomaisverkkojen aatelia. Prosessori 11/2002, s. 58-62

13 Ruohonen, Mika. Tietoturva. Docendo 2002. 428 s.

14 Granlund Kaj Tietoliikenne. Gummerus 2003. 436 s.

15 Granlund Kaj. Tietoliikenne. Gummerus 1999. 352 s.

18 Uusi nopeampi nopeusluokka. Prosessori 12/1996, s. 51-53

19 Cisco Systems, Voice Over IP-Per Call Bandwidth Consumption. Document ID 7934. 9 s.

24 Salausarsenaali hyötykäyttöön. Prosessori 4/2005. s. 88-90

25 EDGE tuo suuret GSM-datanopeusluokat, Prosessori 10/2002. s. 71-75

26 Heikkonen Kimmo, You and Your Tetra Radio. Edita 2004. 97 s.

27 IP-puhetta kaikille, Tietokone 7-8/2004.

28 Puhetta IP-kanavaan, Prosessori 1/2001. s. 76-79

29 Penttinen Jyrki, GSM-tekniikka. WSOY 1999. 349 s.

Sähköiset lähteet

7 Elisa Oyj. [www-sivu]. [viitattu 10.4.2005] Saatavissa: http://matkaviestinta.elisa.fi

11 Oulun yliopiston fysikaalisten tieteiden laitos. [www-sivu]. [viitattu 4.4.2005] Saatavissa: http://physics.oulu.fi

12 Chameleon Oy. [www-sivu]. [viitattu 4.4.2005] Saatavissa: http://www.chameleon.fi

16 Viestintävirasto. [www-sivu]. [viitattu 1.3.2005] Saatavissa: http://www.ficora.fi/

17 RSA laboratories. [www-sivu]. [viitattu 4.4.2005] Saatavissa: http://www.rsasecurity.com

20 Network Sorcery. [www-sivu]. [viitattu 10.4.2005] Saatavissa: http://www.networksorcery.com/enp/protocol/rtp.htm

21 Instrumentointi Oy [www-sivu] [viitattu 7.4.2005] Saatavissa: www.insta.fi

22 Riikonen Pekka. RSA Algorithm [www-sivu].[viitattu 9.4.2005] Saatavissa: http://iki.fi/priikone/docs/rsa.pdf

23 Setec Oy [www-sivu]. [viitattu 31.3.2005] Saatavissa: www.setec.com

30 The 3rd Generation Partnership Project. [www-sivu] [viitattu 17.4.2005} Saatavissa: http://www.3gpp.org