(19) SUOMI - FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN
FINNISH PATENT AND REGISTRATION OFFICE

(10) **FI 20002608 A7**

(12) **JULKISEKSI TULLUT PATENTTIHAKEMUS**
PATENTANSÖKAN SOM BLIVIT OFFENTLIG
PATENT APPLICATION MADE AVAILABLE TO THE PUBLIC

(21) Patenttihakemus - Patentansökan - Patent application 20002608

(51) Kansainvälinen patenttiluokitus - Internationell patentklassifikation - International patent classification
H04L 7/08
H04L 9/16
H04L 9/18
H04L 29/08

(22) Tekemispäivä - Ingivningsdag - Filing date **28.11.2000**

(23) Saapumispäivä - Ankomstdag - Reception date **28.11.2000**

(41) Tullut julkiseksi - Blivit offentlig - Available to the public **29.05.2002**

(43) Julkaisupäivä - Publiceringsdag - Publication date **14.06.2019**

(71) Hakija - Sökande - Applicant

1 •**Nokia Corporation,** Helsinki, Keilalahdentie 4, 02150 ESPOO, SUOMI - FINLAND, (FI)

(72) Keksijä - Uppfinnare - Inventor

1 •**Relander, Rasmus,** Helsinki, SUOMI - FINLAND, (FI)
2 •**Kantola, Raimo,** Helsinki, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud - Agent

Kolster Oy Ab, Salmisaarenaukio 1, 00180 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning - Title of the invention
Päästä-päähän -tahdistuksen ylläpitäminen tietoliikenneyhteydellä
Upprätthållande av från terminal till terminal - synkronisering med en telekommunikationsförbindelse

(57) Tiivistelmä - Sammandrag - Abstract

Menetelmä ja järjestely päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä (PDN), jolloin siirrettävän tiedon toistoviivettä voidaan kasvattaa lisäämällä yksi tai useampia ylimääräisiä kehyksiä (72) siirrettävään kehysjonoon (75), jolloin järjestely käsittää välineet (MS, TE) tietoliikenneyhteyden vastaanottavassa päässä vastaanotetun kehyksen salauksen purkamisessa kulloinkin käytettävän kehystä vastaavan alustusvektorin arvon määrittämiseksi vastaanotettujen kehysten lukumäärän perusteella ja välineet (GW, TE) toistoviiveen säätämiseksi, jotka on sovitettu merkitsemään toistoviiveen kasvattamiseksi lisättävä kehys ylimääräiseksi kehykseksi, jolloin välineet (MS, TE) alustusvektorin arvon määrittämiseksi on sovitettu laskemaan vastaanotettujen kehysten lukumäärään vain ylimääräiseksi merkitsemättömät kehykset.(Kuvio 1)

Uppfinningen avser ett förfarande och ett arrangemang för att upprätthålla en point to point -synkronisering för en datatrafikförbindelse, över vilken överföres data i ramar i väsentligen realtid under användning av en synkroniserad point to point -kryptering, vilken synkroniseras genom att stundtals sända synkroniseringsvektorer i sagda ramar, varvid åtminstone en del av sagda datatrafikförbindelse bildas av en paketkopplad förbindelse (PDN), varvid repetitionsfördröjningen, för den information som skall sändas, kan ökas genom att lägga till en eller flera extra ramar (72) i den ramkö (75) som skall överföras, varvid sagda arrangemang omfattar don (MS, TE) för definiering av värdet på en i samband med dechiffreringen av kryptningen i den mottagande änden mottagen rams formatteringsvektor, på basen av de mottagna ramarnas antal, samt don (GW, TE) för reglering av sagda repetitionsfördröjning, vilka är anpassade att markera en vid ökningen av sagda repetitionsfördröjning använd ram som en extra ram, varvid donen (MS, TE) för definiering av värdet på en formatteringsvektor är anpassade att till antalet mottagna ramar enbart räkna de som extra ramar markerade ramarna.

Päästä-päähän -tahdistuksen ylläpitäminen tietoliikenneyhteydellä

Keksinnön tausta

Keksintö liittyy menetelmään ja laitteeseen päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä.

Tietoliikennejärjestelmissä kuten viranomaisverkossa on erittäin tärkeää, ettei liikenteen salakuuntelu ole mahdollista. Ilmatierajapinta on tyypillisesti salattu, joten vaikka radioliikennettä valvotaan, ulkopuolinen ei pysty purkamaan sitä. Infrastruktuurissa liikennettä ei kuitenkaan välttämättä salata, joten liikenne kuten puhe voidaan purkaa käyttäen kyseisen järjestelmän koodekkia. Vaikka ulkopuolinen ei periaatteessa pysty kuuntelemaan puhevuota infrastruktuurin sisältä, tämä on kuitenkin vaativimmille käyttäjille mahdollinen turvallisuusriski. Siksi on kehitetty ratkaisu, jossa puhe voidaan salata päästä-päähän -salauksella. Esimerkkinä päästä-päähän -salauksen mahdollistavasta järjestelmästä on TETRA-järjestelmä (TErrestrial Trunked RAdio).

Päästä-päähän -salauksen perusajatuksena on se, että verkon käyttäjä kuten viranomaisorganisaatio suorittaa liikenteen salauksen ja salauksen purun itsenäisesti ja käytettävästä siirtoverkosta riippumattomasti esimerkiksi päätelaitteiden yhteydessä.

Esimerkiksi TETRA-järjestelmässä päästä-päähän -salausta käytettäessä lähettäjä koodaa ensin 60 ms:n ääninäytteen TETRA-koodekkia käyttäen, josta syntyy selväkielinen näyte. Lähettävä päätelaite luo tiettyä avainsarjaa käyttäen salatun näytteen. Salattu näyte lähetetään sitten verkolle. Vastaanottaja purkaa salatun näytteen käyttämällä samaa avainsarjaa, jolloin saadaan taas selväkielinen näyte.

Salauksen murtamisen ehkäisemiseksi avainsarjaa muutetaan jatkuvasti, joten jokainen 60 ms:n ääninäytteen käsittävä kehys on salattu omalla avainsarjallaan. Molempien avainsarjakehittimien on siis sovittava siitä, mitä avainsarjaa on käytettävä jokaiselle kehykselle. Tämä tehtävä kuuluu tahdistuksen ohjaukselle. Tehtävää varten käytetään tahdistusvektoreja, joita lähetetään päätelaitteiden välillä puhekaistalla olevan signaalin avulla.

Avainsarjakehitin luo avainsarjan tietyn avaimen ja alustusvektorin perusteella. Avaimet jaetaan jokaiselle päätelaitteelle, joka osallistuu salattuun puheluun. Tämä on osa päätelaitteen asetuksia. Uusi avainsarja luodaan siis kerran 60 millisekuntia kohti. Jokaisen kehyksen jälkeen alustusvektoria muutetaan. Yksinkertaisin vaihtoehto on inkrementoida sitä yhdellä, mutta jokainen

salausalgoritmi päättää itse inkrementointitavastaan, joka voi olla monimutkaisempikin salausten murtamisen ehkäisemiseksi.

Tahdistusohjauksen tehtävä on varmistaa, että molemmat päät tietävät, millä alustusvektorilla kukin kehys on salattu. Jotta salaaja ja avaaja pääsisivät yhteisymmärrykseen alustusvektorin arvosta, puheenvuoron alussa lähetetään tahdistusvektori. Joskus kyseessä saattaa olla myös ryhmäpuhelu, johon on voitava liittyä puheenvuoron aikanakin. Tämän vuoksi tahdistusvektoria lähetetään jatkuvasti esimerkiksi 1-4 kertaa sekunnissa. Tahdistusvektori sisältää alustusvektorin lisäksi mm. avaimen tunnuksen ja CRC-virheentarkastuksen, joten päätelaite voi varmistaa tahdistusvektorin eheyden. Vastaanottaja laskee siis kuinka monta kehystä on lähetetty tahdistusvektorin jälkeen ja avainsarjakehitin luo uuden alustusvektorin viimeksi vastaanotetun alustusvektorin ja kehysten lukumäärän perustella.

Tiedonsiirtoverkko saattaa käsittää yhden tai useampia pakettikytkettyjä yhteyksiä, esimerkiksi IP (Internet Protocol) -yhteyksiä, joissa tieto siirretään esimerkiksi IP-puhetekniikalla (voice over IP, VoIP). Eräs standardiprotokolla tosiaikaisen tiedon kuten äänen ja videokuvan siirtämiseen esimerkiksi IP-verkossa on RTP (Real Time Protocol). IP-verkko aiheuttaa tyypillisesti vaihtelevan viiveen pakettien siirrossa. Esimerkiksi puheen ymmärrettävyyden kannalta viiveen vaihtelu on hyvin haitallista. Tämän korvaamiseksi RTP siirron vastaanottopää puskuroi tulevat paketit jitterpuskuriin ja toistaa ne tiettyyn toistoaikaan. Ennen toistohetkeä tullut paketti osallistuu alkuperäisen signaalin uudelleen rakentamiseen. Toistohetken jälkeen tullut paketti on käyttämätön ja hylätty.

Tosiaikainen sovellus vaatii toisaalta mahdollisimman pienen päästä-päähän -viiveen, ja näin halutaan pienentää toistoviivettä. Toisaalta pitkä toistoviive sallii pitkän ajan pakettien saapumiselle, ja näin voidaan hyväksyä enemmän paketteja. Toistoviiveen arvoa on näin säädettävä jatkuvasti verkon olosuhteiden mukaan. Useimmilla RTP-algoritmeilla on toiminne, joka säätää toistoviiveen automaattisesti verkko-olosuhteiden mukaan äänen laadun parantamiseksi. Toistoviiveen siirtäminen esimerkiksi 60 ms eteenpäin tapahtuu siten, että IP-yhdyskäytävä luo 60 ms:n korvaavan paketin. Toisin sanoen lisätään siirrettävän kehysvuon sisälle ylimääräinen kehys.

Ongelmana yllä kuvatussa järjestelyssä on se, että jos käytetään tahdistettua päästä-päähän -salauskoodausta ja kehysvuohon lisätään ylimääräinen kehys, on tämän seurauksena vastaanottopään kehyslaskuri yhden ke-

hyksen etuajassa verrattuna tuleviin kehyksiin eikä vastaanottopään avainsarja enää vastaa lähetyspään avainsarjaa.

Toistoviiveen kasvattamisella esimerkiksi puheenvuoron keskellä on siis se seuraus, että päästä-päähän -tahdistus menetetään, eikä salattu puhe ole enää dekoodattavissa. Tämä jatkuu kunnes lähetyspää lähettää uuden tahdistusvektorin, joka tahdistaa vastanottopään. Tämä ilmiö voidaan välttää siten, että esimerkiksi semidupleksipuheluissa toistoviivettä vaihdetaan vain puheenvuorojen jälkeen. Jos puheenvuorot ovat pitkiä, voidaan toistoviivettä tällöin muuttaa epäedullisen harvoin: puheenlaatu saattaa olla huono koko puheenvuoron loppuun asti, koska toistoviivettä ei voida vaihtaa aiemmin. Edelleen esimerkiksi dupleksipuheluissa, joissa ei ole puheenvuoroja ja joissa päätelaite lähettää jatkuvasti, toistoviivettä ei voida vaihtaa ollenkaan koko puhelun aikana, jos halutaan välttää tahdistuksen menetys.

Keksinnön lyhyt selostus

Keksinnön tavoitteena on siten kehittää menetelmä ja menetelmän toteuttava laitteisto siten, että yllä mainitut ongelmat saadaan ratkaistua. Keksinnön tavoite saavutetaan menetelmällä ja järjestelmällä, joille on tunnusomaista se, mitä sanotaan itsenäisissä patenttivaatimuksissa 1, 7, 13 ja 22. Keksinnön edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Keksintö perustuu siihen, että jos toistoviivettä kasvatetaan tiedon lähetyksen kuten puheenvuoron tai puhelun aikana, merkitään toistoviiveen kasvattamiseksi lisättävä kehys ylimääräiseksi kehykseksi ja lasketaan vastaanottopäässä vastaanotettujen kehysten lukumäärään vain ylimääräiseksi merkitsemättömät kehykset, jolloin toistoviiveen kasvattamiseksi lisätyt ylimääräiset kehykset eivät sekoita päästä-päähän -salauksessa käytettävää kehyslaskuria ja tiedon salauksen purkuun ja siten dekoodaukseen ei tule aukkoja.

Keksinnön mukaisen menetelmän ja järjestelmän etuna on se, että ne mahdollistavat toistoviiveen kasvattamisen myös tiedon lähetyksen aikana ilman, että tämän seurauksena salatun tiedon dekoodaus häiriintyisi.

Kuvioiden lyhyt selostus

Keksintöä selostetaan nyt lähemmin edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirroksiin, joista:

Kuvio 1 esittää lohkokaavion TETRA-järjestelmän rakenteesta;

Kuvio 2 esittää lohkokaavion päästä-päähän -salauksen toiminnasta;

Kuvio 3 esittää vastaanottajan suorittamaa alustusvektorin laskemista;

Kuvio 4 esittää kaavion RTP-paketin rakenteesta;

Kuvio 5 esittää RTP-algoritmin toimintaa;

Kuvio 6 esittää kaavion RTP-pakettien tulotodennäköisyydestä siirtoajan funktiona ja

Kuvio 7 esittää kaavion toistoviiveen kasvattamisesta.

Keksinnön yksityiskohtainen selostus

Keksintöä on seuraavassa kuvattu esimerkinomaisesti TETRA-järjestelmän yhteydessä. Keksintöä ei kuitenkaan ole tarkoitus rajoittaa mihinkään tiettyyn tietoliikennejärjestelmään tai tiedonsiirtoprotokollaan. Keksinnön sovellukset myös muihin järjestelmiin ovat alan ammattimiehelle ilmeisiä.

Kuviossa 1 on esitetty esimerkki TETRA-järjestelmän rakenteesta. Vaikka kuviossa ja seuraavassa selityksessä on viitattu TETRA-järjestelmän mukaisiin verkkoelementteihin, ei tämä mitenkään rajoita keksinnön soveltamista myös muihin tietoliikennejärjestelmiin. On huomattava, että kuviossa on esitetty vain keksinnön ymmärtämisen kannalta olennaisia elementtejä ja järjestelmän rakenne saattaa poiketa esitetystä ilman, että sillä on merkitystä keksinnön perusajatuksen kannalta. On myös huomattava, että todellisessa matkaviestinjärjestelmässä voi kutakin elementtiä olla mielivaltainen määrä. Päätelaitteet MS (Mobile Station) ovat yhteydessä tukiasemiin TBS (TETRA Base Station) radioteitse. Päätelaitteet MS voivat myös ns. suorakanavamoodissa viestiä suoraan keskenään käyttämättä tukiasemia TBS. Jokainen tukiasema TBS on kytketty yhteysjohdolla johonkin kiinteän siirtoverkon TETRA-keskuksista DXT (Digital Exchange for TETRA). TETRA-keskukset DXT on kytketty kiinteällä yhteydellä toisiin keskuksiin ja TETRA-solmukeskukseen DXTc (Digital Central Exchange for TETRA, ei esitetty), joka on keskus, johon on kytketty muita keskuksia DXT ja/tai muita solmukeskuksia DXTc vaihtoehtoisten liikennereittien aikaansaamiseksi. Mahdolliset ulkoiset liitäntärajapinnat esimerkiksi yleiseen puhelinverkkoon PSTN (Public Switched Telephone Network), digitaaliseen monipalveluverkkoon ISDN (Integrated Services Digital Network), yritysvaihteeseen PABX (Private Automatic Branch Exchange) ja pakettivälitteiseen dataverkkoon PDN (Packet Data Network) voivat sijaita yhdessä tai useammassa keskuksessa DXT. Edellä mainituista liitäntärajapin-

noista on kuviossa esitetty liitäntä pakettivälitteiseen dataverkkoon PDN yhdyskäytävän GW avulla. Yhdyskäytävän GW tehtävä on muuttaa keskukselta DXT tuleva piirikytketty data pakettiverkkoon PDN meneväksi pakettikytketyksi dataksi ja päinvastoin. Pakettivälitteiseen dataverkkoon PDN kytketty päätelaite TE voi näin olla yhteydessä TETRA-verkkoon. Yhdyskäytävä GW voi olla erillinen verkkoelementti tai esimerkiksi keskuksen DXT osa. Lisäksi kuviossa on esitetty keskukseen DXT kytketty käyttöpaikkajärjestelmä DS (Dispatcher System), joka muodostuu käyttöpaikan ohjaimesta DSC (Dispatcher Station Controller) ja siihen liitetystä työasemasta DWS (Dispatcher Workstation). Käyttöpaikanhoitaja ohjaa päätelaitteiden MS puheluita ja muita toimintoja työaseman DWS välityksellä.

Kuviossa 2 on havainnollistettu päästä-päähän -salauksen toimintaa. Päästä-päähän -salausta käytettäessä lähettäjä 20 koodaa ensin 60 ms:n ääninäytteen TETRA-koodekkia käyttäen, josta syntyy selväkielinen näyte (P). Päätelaite luo P:n pituista avainsarjaa (KSS, Key Stream Segment) avainsarjakehittimessä 21. Salattu näyte (C) saadaan suorittamalla binäärinen XOR-operaatio lohkossa 22:

$$C = P \text{ xor } KSS$$

Salattu näyte lähetetään sitten siirtoverkolle 29. Vastaanottaja 30 suorittaa saman XOR-operaation lohkossa 28 käyttämällä samaa avainsarjaa, josta syntyy taas selväkielinen näyte P.

$$P = C \text{ xor } KSS$$

Salauksen murtamisen ehkäisemiseksi avainsarjaa KSS muutetaan jatkuvasti, joten jokainen kehys on salattu omalla avainsarjallaan. Molempien avainsarjakehittimien 21 ja 27 on siis sovittava siitä, mitä avainsarjaa on käytettävä kullekin kehykselle. Tämä tehtävä kuuluu tahdistuksen ohjaukselle 23 ja 26. Tehtävää varten käytetään tahdistusvektoreja, joita lähetetään päätelaitteiden välillä puhekaistalla olevan signaalin avulla.

Avainsarjakehitin (EKSG, Encryption Key Stream Generator) 21 ja 27 luo avainsarjan (KSS) salausavaimen (CK, Cipher Key) ja alustusvektorin (IV) perusteella. Uusi avainsarja luodaan siis kerran 60 millisekuntia kohti.

KSS = EKSG (CK, IV)

Jokaisen kehyksen jälkeen alustusvektoria muutetaan. Yksinkertaisin vaihtoehto on inkrementoida sitä yhdellä, mutta jokainen salausalgoritmi päättää itse inkrementointitavastaan, joka voi olla monimutkaisempikin salausten murtamisen ehkäisemiseksi.

Tahdistusohjauksen 23 ja 26 tehtävä on varmistaa, että molemmat päät 20 ja 30 tietävät, millä alustusvektorilla jokainen kehys on salattu. Jotta salaaja 20 ja avaaja 30 pääsisivät yhteisymmärrykseen alustusvektorin arvosta, puheenvuoron alussa lähetetään tahdistusvektori (SV). Joskus kyseessä saattaa olla myös ryhmäpuhelu, johon on voitava liittyä puheenvuoron aikanakin. Tämän vuoksi tahdistusvektoria lähetetään jatkuvasti n. 1-4 kertaa sekunnissa. Tahdistusvektori sisältää alustusvektorin lisäksi mm. avaimen tunnuksen ja CRC-virheentarkastuksen, joten päätelaite voi varmistaa tahdistusvektorin eheyden.

Vastaanottaja 30 laskee siis kuinka monta kehystä (n) on lähetetty tahdistusvektorin jälkeen. Vastaanottajan 30 avainsarjakehitin 27 luo uuden alustusvektorin IV viimeksi vastaanotetun alustusvektorin ja kehysten lukumäärän perustella. Vastaanottajan suorittamaa alustusvektorin IV laskemista on havainnollistettu kuviossa 3, jossa on esitetty siirrettävä kehysjono. Kukin kehys käsittää kaksi puhelohkoa P1 ja P2, kuten kuviossa on esitetty yhden kehyksen osalta. Esitetyssä jonossa kehykset 1, 6, 12 ja 13 sisältävät toisessa puhelohkossaan tahdistusvektorin SV, joissa ilmoitetaan alustusvektorin IV numero.

Molempien päiden 20 ja 30 on sovittava siitä, miten puhelu salataan. Tahdistuksen ohjausyksiköt 23 ja 26 molemmissa päissä kommunikoivat keskenään U-varastettujen puhelohkojen avulla. Lähettävä päätelaite käyttää hyväkseen yhtä tai kahta puhelohkoa kehyksen sisältä omaan tarkoitukseensa. Tämä tapahtuu lohkossa 24. Tämä ilmaistaan vastaanottavalle päätelaitteelle asettamalla tarkoituksenmukaisesti 3 ensimmäistä ohjausbittiä kehyksen sisällä. Siten infrastruktuuri 29 ymmärtää, että kyseessä on päätelaitteesta-päätelaitteeseen -tieto, ja se siirtää tietoja sen perusteella läpinäkyvästi muuttamatta niitä. Sen lisäksi vastaanottava päätelaite havaitsee, ettei ko. puhelohkossa ole puhetietoja, eikä välitä niitä koodekille, vaan käsittelee niitä tarkoituksenmukaisesti, toisin sanoen lohkossa 25 suodatetaan tahdistuksenohjaustieto tahdistuksenohjaukselle 26, ja luo korvaavan äänen varastetun pu-

heen sijaan. Puhelohkon varastaminen hävittää 30 ms pituisen puheen. Tämä aiheuttaisi tauon puheessa, joten sen laatu huononisi ja sitä olisi vaikeampi ymmärtää. Tämän välttämiseksi TETRA-koodekki sisältää korvausmekanismin. Todellisuudessa käyttäjä ei koe puheen puuttumista haitallisena, mikäli puhelohkoja ei varasteta enemmän kun 4 kertaa sekunnissa. Salausavaimet CK jaetaan jokaiselle päätelaitteelle, joka osallistuu salattuun puheluun. Tämä on osa päätelaitteen asetuksia.

Kuviossa 1 esitetty pakettikytkentäinen dataverkko PDN voi olla esimerkiksi Internet, jossa käytetään TCP/IP protokollia. TCP/IP on tiedonsiirtoprotokollaperheen nimi, jota käytetään lähiverkon sisällä tai lähiverkkojen välillä. Protokollat ovat IP (Internet-protokolla), kuljetusprotokolla TCP (Transmission Control Protocol) ja tietosähkeprotokolla UDP (User Datagram Protocol). Perheeseen kuuluu myös muita protokollia tiettyjä palveluja, kuten tiedostosiirtoa, sähköpostia, etäkäyttöä ym., varten.

TCP/IP-protokollat on jaettu kerroksiin: yhteyskerros, verkkokerros, kuljetuskerros ja sovelluskerros. Yhteyskerros vastaa päätelaitteen fyysisestä liittymisestä verkkoon. Se koskee lähinnä verkkokorttia ja ajuria. Verkkokerrosta kutsutaan usein Internet- tai IP-kerrokseksi. Kerros vastaa pakettien siirtämisestä verkon sisällä ja mm. reitityksestä koneesta toiseen IP-osoitteen perusteella. IP tarjoaa TCP/IP-protokollaperheessä verkkokerroksen. Kuljetuskerros tarjoaa datavuopalvelun kahden päätelaitteen välillä sovelluskerrosta varten ja ohjaa vuot päätelaitteessa oikeaan sovellukseen. Internetprotokollassa on kaksi siirtoyhteyskäytäntöä: TCP ja UDP. Siirtokerroksen toinen tehtävä on ohjata paketit oikeaan sovellukseen porttinumeroiden perusteella. TCP tarjoaa luotettavan datavuon päätelaitteesta toiseen. TCP pilkkoo datan sopivankokoisiksi paketeiksi, kuittaa vastaanotetut paketit ja valvoo, että lähetetyt paketit kuitataan vastaanotetuiksi toisessa päässä. TCP vastaa luotettavasta siirrosta päästä-päähän, eli sovelluksen ei tarvitse huolehtia siitä. UDP on toisaalta paljon yksinkertaisempi protokolla. UDP ei vastaa tietojen perilletulosta, vaan tätä vaadittaessa sovelluskerroksen on huolehdittava siitä. Sovelluskerros vastaa kunkin sovelluksen omasta tiedonkäsittelystä.

RTP on Internetin standardiprotokolla tosiaikaisen tiedon, kuten äänen ja videokuvan siirtämiseen. Sitä voidaan käyttää mediatilauspalvelua tai vuorovaikutteista palvelua kuten IP-puheluita varten. RTP koostuu mediaosasta ja ohjausosasta. Jälkimmäistä kutsutaan RTCP:ksi (Real Time Control Protocol). RTP:n mediaosasta löytyy tukea tosiaikaisille sovelluksille. Tämä si-

sältää aikatuen, kadon havaitsemisen, turvallisuustuen ja sisällön tunnistamisen. RTCP mahdollistaa tosiaikaiset konferenssit erikokoisten ryhmien sisällä ja sen lisäksi päästä-päähän -palvelun laadun arvioinnin. Se tukee myös useamman mediavuon tahdistusta. RTP on suunniteltu siirtoverkosta riippumattomaksi, mutta Internet-verkossa RTP käyttää yleensä IP/UDP:tä. RTP-yhteyskäytännöllä on monia piirteitä, jotka mahdollistavat päästä-päähän tosiaikaisen tiedonsiirron. Jokaisessa päässä audiosovellus lähettää säännöllisesti audiotietoja pieninä näytteinä, jotka voivat olla pituudeltaan esimerkiksi 30 ms. Jokaiseen näytteeseen liitetään RTP-otsikko. RTP-otsikko ja tiedot taas pakataan UDP- ja IP-pakettiin.

RTP-otsikossa tunnistetaan paketin sisältö. Tämän kentän arvoa käyttämällä ilmaistaan, mitä koodausmenetelmää käytetään (PCM, ADPCM, LPC jne.) RTP-paketin hyötykuormassa. Internetissä, kuten muissa pakettiverkoissa, paketit voivat saapua mielivaltaisessa järjestyksessä, myöhästyä vaihtelevan ajan tai jopa kadota kokonaan. Tämän estämiseksi jokaiselle paketille tietyssä vuossa annetaan oma järjestysnumero ja aikaleima, jonka perusteella vastaanotettu vuo järjestyy uudelleen alkuperäisen vuon mukaan. Järjestysnumeroa kasvatetaan yhdellä jokaista pakettia kohti. Järjestysnumeroiden avulla vastaanottaja pystyy havaitsemaan puuttuvan paketin ja myös arvioimaan pakettihukan.

Aikaleima on 32 bittinen numero. Sillä ilmaistaan näytteenoton aloitushetki. Sen laskemiseen on käytettävä monotonisesti ja lineaarisesti ajan mukana kasvavaa kelloa. Kellon taajuus on valittava siten, että se on sisällölle sopiva, tarpeeksi nopea värinän laskemiseksi ja tahdistuksen mahdollistamiseksi. Esimerkiksi käytettäessä PCM-A-laki-koodaustapaa kellotajuus on 8000 Hz. Lähetettäessä 240-tavun pituisia RTP-paketteja, joka vastaa 240 PCM-näytettä, aikaleimaa kasvatetaan 240:llä jokaista pakettia kohti. RTP-otsikon pituus on 3 - 18 sanaa (32-bittinen sana). Kuviossa 4 on havainnollistettu RTP-paketin muotoa. Kenttien merkitys on seuraava: V: versio; käytetty RTP:n versio, nykyisin 2. Täyte: paketissa on täytetavuja; viimeinen tavu ilmoittaa, montako. Laajennus: paketin jälkeen tasan yksi otsakelaajennus. PM: palvelulähteiden määrä ilmoittaa, monenko lähteen tuottamaa informaatiota paketissa on. Merkitsintä voidaan käyttää ilmoittamaan merkittävistä tapahtumista esimerkiksi kehysten rajoista. HT: hyötykuorman tyyppi ilmoittaa hyötykuormassa olevan median tyypin. Sarjanumeroa kasvatetaan yhdellä jokaista lähetettyä datapakettia kohti. Se auttaa havaitsemaan pakettihukan ja epäjär-

jestyksen. Alkuarvo on satunnainen. Aikaleima kertoo ensimmäisen tavun näytteistyshetken. Sitä käytetään tahdistukseen ja värinän laskemiseen. Alkuarvo on satunnainen. SSRC: satunnaisesti valittu tahdistuslähteen tunniste. Ilmoittaa lähteiden yhdistyspisteen tai alkuperäisen lähettäjän, jos on vain yksi lähde. CSRC-lista tässä paketissa mukana olevien lähteiden lista.

Internet aiheuttaa vaihtelevan viiveen äänipakettien siirrossa. Puheen ymmärrettävyyden kannalta viiveen vaihtelu on hyvin haitallista. Tämän korvaamiseksi RTP:n vastaanottopää puskuroi tulevat paketit jitterpuskuriin ja toistaa ne tiettyyn toistoaikaan. Ennen toistohetkeä tullut paketti osallistuu alkuperäisen signaalin uudelleen rakentamiseen. Toistohetken jälkeen tullut paketti on käyttämätön ja hylätty.

Kuvio 5 havainnollistaa RTP-algoritmin toimintaa. Kuviossa kirjain t viittaa paketin lähetysajankohtaan, kirjain a vastaanottoajankohtaan ja p toistoajankohtaan. Yläindeksit ilmaisevat paketin numeroa ja alaindeksit puheenvuoron numeroa. K:nnessa puheenvuorossa paketit saapuvat vastaanottopäähän vaihtelevan siirtoajan jälkeen. RTP-algoritmi toistaa ne sitten oikealla hetkellä. (K+1):nnessä puheenvuorossa paketit 1 ja 2 vaihtelevat järjestystä, ja paketti 4 saapuu toistohetkensä jälkeen, joten se hylätään. RTP-algoritmi palauttaa paketit oikeaan järjestykseen, toistaa ne oikealla hetkellä, ja ilmaisee esimerkiksi korjaustoimenpiteitä varten, mitkä paketit puuttuvat tai ovat myöhästyneet. Toistoviive on aika t(toistoviive) = t(toisto) – t(lähetys). RTP-algoritmi huolehtii siitä, että toistoviive jää vakioksi koko puhevuoron aikana.

IP-paketin viive IP-verkon läpi t=t(tulo) – t(lähtö) koostuu kahdesta tekijästä. L on kiinteä viive, joka riippuu siirtoajasta ja keskimääräisestä jonotusajasta. J on taas vaihteleva viive, joka riippuu vaihtelevasta jonotusajasta IP-verkon sisällä, ja joka aiheuttaa jitterin. IP-verkon vastaanottopäässä on jitterpuskuri, joka tallentaa paketit muistiinsa, mikäli siirtoaika t < t(toistoviive). Toistoviiveen määritteleminen on kompromissiratkaisu. Tosiaikainen sovellus vaatii toisaalta mahdollisimman pienen päästä-päähän -viiveen, ja näin halutaan pienentää toistoviivettä. Toisaalta pitkä toistoviive sallii pitkän ajan pakettien saapumiselle, ja näin voidaan hyväksyä enemmän paketteja. Toistoviiveen arvoa on näin säädettävä jatkuvasti verkon olosuhteiden mukaan. Kuvio 6 havainnollistaa tätä. Paketti, jonka siirtoaika t < L+ J voidaan hyväksyä, kun taas paketti, jonka siirtoaika t > L + J on hylättävä. Kasvattamalla J:tä voidaan näin kasvattaa hyväksyttyjen pakettien määrää. Toistoviivettä voidaan säätää

esimerkiksi aloittamalla pienellä arvolla, ja kasvattamalla sitä säännöllisesti, kunnes myöhässä olevien pakettien osa jää tietyn rajan, esimerkiksi 1%, alle.

Useimmilla RTP-algoritmeilla on toiminne, joka säätää toistoviiveen automaattisesti verkko-olosuhteiden mukaan äänen laadun parantamiseksi. Toistoviiveen siirtäminen esimerkiksi 60 ms eteenpäin tapahtuu siten, että RTP-vastaanotossa luodaan 60 ms:n korvaava puhepaketti ennen kun puhevuo jatkuu. Toisin sanoen lisätään puhevuon sisälle ylimääräinen kehys. Kuviossa 7 on esitetty kehysjono 75, johon lisätään yksi tai useampia ylimääräisiä kehyksiä 72 ja edelleentoimitusta varten saadaan kehysjono 76. Toistoviiveen siirtäminen 60 ms taaksepäin tapahtuu puolestaan siten, että RTP-vastaanotossa kokonainen puhekehys hävitetään.

Kuviossa 1 RTP-siirto tapahtuu siis yhdyskäytävän GW ja päätelaitteen TE välillä pakettiverkon PDN yli. Yhdyskäytävän GW tehtävä on muuntaa keskukselta DXT PCM-linjaa pitkin tuleva piirikytketty puhe (tai muu data) IP-puhepaketeiksi ja päinvastoin. TETRA-infrastruktuurissa siirretään puhedataa kehyksissä, joten luonnollinen RTP-paketti sisältäisi yhden kehyksen puhedataa. Tällöin yhdessä RTP-paketissa olisi 60 ms puhetta, ja se vastaisi suoraan yhden puhekehyksen sisältöä. Toinen mahdollisuus on käyttää RTP-pakettia, joka sisältää vain puolikehyksen puhedataa (30 ms). Puolikehyspaketilla on seuraavat ominaisuudet verrattuna kokonaiskehyspakettiin: 1) Yhdyskäytävän vastaanottaessa puolikehyspaketteja sen täytyy odottaa, että kaksi pakettia on saapunut ennen ISI-kehyksen lähetyksen alkua. Molempia puhelohkoja koskevat ohjausbitit (BFI, C- tai U-varkaus) ovat nimittäin kehyksen alussa ja yhdyskäytävän täytyy määritellä ne puolikehyspakettien tyypin perusteella. 2) RTP-paketin kadotessa vain 30 ms puhetta puuttuu verrattuna 60 ms:in. Äänen laatua optimoitaessa on paketin pituus kompromissi kahden hahmottamisnäkökohdan välillä. Toinen ääripää on lyhyt paketti, jonka seurauksena puuttuvien pakettien määrä kasvaa kääntäen verrannollisesti pakettien kokoon, ja vääristymät tapahtuvat näin useammin. Toinen ääripää on pitkä paketti, jolloin vääristymät tapahtuvat harvemmin mutta jolla todennäköisyys kokonaisen foneemin häviämisestä ja näin ollen puheen ymmärrettävyyden huononemisesta kasvaa varsinkin kun paketin pituus on yli 20 ms. Jälkimmäinen raja on nimittäin lyhyin foneemin pituus. 3) Kaistanleveyden kannalta pitkä paketti on kuitenkin tehokkaampi, sillä otsikoiden (Ethernet + IP + UDP + RTP) pituus (36-40 tavua) on hyötykuorman pituuteen verrattuna (18 tavua/puhelohko tai 36 tavua/puhekehys) jo pitkä. Otsikoiden osuutta paketis-

sa voidaan pienentää käyttämällä kahta tekniikkaa. Multipleksauksen avulla voidaan useita puhekanavia pakata samaan RTP-pakettiin ja näin pienentää otsikoiden osuutta. Tämä on varsin kiinnostavaa keskuksesta-käyttöpaikkaan-yhteyttä varten, sillä kaikki ryhmäpuhelut ja yksilöpuhelu voidaan näin lähettää samassa paketissa. Toinen tekniikka, joka soveltuu sarjayhteyksiin, on otsikoiden kompressio. Sen avulla voidaan IP/UDP/RTP-otsikkoa pienentää huomattavasti (2-4 tavuihin) ja näin säästää kaistanleveyttä. Paremman äänenlaadun saavuttamiseksi on lyhyt RTP-paketti (30 ms) näin ollen edullisempi.

Puhelohkoja voidaan varastaa kehyksen sisältä joko verkon (C-varastettu) tai käyttäjän (U-varastettu) tarkoitukseen. Esimerkiksi päästäpäähän -salausta käytettäessä päätelaitteet varastavat yhden puhelohkon omaan tarkoitukseensa 1 - 4 kertaa sekunnissa tahdistusvektorin välittämiseen kuten edellä on selitetty.

ACELP-koodekkeja tuetaan RTP-standardissa ja monessa IP-puhepäätelaitteessa, mutta TETRA-kohtaista ACELP:iä ei RTP-standardi tue. Puheen siirtämistä varten voidaan käyttää RTP-pakettia, jossa on esimerkiksi seuraavat asetukset: RTP-versio 2, ei täytettä, ei laajennusta, ei CRSC lähteitä, ei merkitsintä, kuorman tyyppi: 8 (sama kuin A-laki), aikaleima kasvaa 240 yksiköllä jokaista pakettia kohti. Tämä vastaa TETRA:n 8000 Hz näytteenottokelloa ja 30 ms näytteenpituutta. Hyötykuormassa esiintyvät seuraavat tiedot: kolme ensimmäistä bittiä ilmaisevat, onko kehysvirhebitti (BFI) asetettu, onko hyötykuormassa ääni vai data, ja onko mahdollisesti kyseessä C- tai U-varastettu puhelohko; muut ensimmäisen tavun bitit eivät ole käytössä; seuraavat 137 bittiä ovat varsinaista dataa, ja ne vastaavat yhtä puhelohkoa. Hyötykuorman loput bitit ovat 0.

Edellä kuvattu yhdyskäytävän GW toiminta piirikytketyn ja pakettikytketyn yhteyden välillä on vain eräs mahdollinen toteutustapa ja yhdyskäytävän GW toiminta voi poiketa tästä ilman, että sillä on merkitystä keksinnön perusajatuksen kannalta.

Kuviossa 1 esitetty päätelaite TE voi olla puhepäätelaite tai datapäätelaite ja keksintöä voidaan soveltaa esimerkiksi ääniyhteyksiin, kuvayhteyksiin tai datayhteyksiin, jotka vaativat reaaliaikaista tiedonsiirtoa. Päätelaite TE voi olla esimerkiksi matkaviestin, käyttöpaikan työasema, tukiasema tai jokin muu verkkoelementti. Päätelaite TE ei ole välttämättä suoraan kytketty pakettiverkkoon PDN vaan päätelaitteen TE ja pakettiverkon PDN välillä voi olla esimerkiksi toinen TETRA-verkko. Tällöin myös pakettiyhteyden PDN toisessa

päässä on yhdyskäytäväelementti. Välissä voi olla myöskin jokin muu yhteys tai useampia pakettiyhteyksiä. Jos päätelaite TE on kuvion 1 mukaisesti kytketty suoraan pakettiverkkoon PDN, toimii se RTP-siirron toisena osapuolena olennaisesti samalla tavoin, kuin jo edellä on kuvattu yhdyskäytävän GW osalta.

Keksinnön mukaisesti suoritetaan pakettiyhteyden PDN vastaanottavassa päässä GW tai TE toistoviiveen kasvatus tiedon lähetyksen, esimerkiksi puheenvuoron tai puhelun, aikana, siten, että merkitään toistoviiveen kasvattamiseksi lisättävä kehys 72 ylimääräiseksi kehykseksi ja edelleen tietoliikenneyhteyden vastaanottavassa päässä lasketaan vastaanotettujen kehysten lukumäärään n vain ylimääräiseksi merkitsemättömät kehykset, jotta oikea alustusvektorin arvo saadaan selville kuten edellä on selitetty. Esimerkinä voidaan tarkastella tilannetta, jossa kuviossa 1 matkaviestimen MS ja päätelaitteen TE välillä on puhelu, joka kulkee pakettiyhteyden PDN kautta RTP-protokollan mukaisesti. RTP-protokollan mukainen tiedonsiirto tapahtuu tällöin protokollaa tukevien yhdyskäytävän GW ja päätelaitteen TE välillä. Tällöin yhdyskäytävä GW on pakettiyhteyden PDN vastaanottava pää päätelaitteelta TE tulevan liikenteen suhteen. Kun RTP-algoritmin mukaisesti havaitaan tarve kasvattaa toistoviivettä, lisätään yhdyskäytävässä GW yksi tai useampia ylimääräisiä kehyksiä 72 vastaanotettuun kehysjonoon 75 ja lähetetään näin saatu kehysjono 76 edelleen matkaviestimelle MS. Lisättävät ylimääräiset kehykset 72 lisäksi merkitään yhdyskäytävässä GW siten, että vastaanottaja eli tässä tapauksessa matkaviestin MS tunnistaa ne ylimääräisiksi kehyksiksi eikä laske niitä mukaan vastaanotettujen kehysten lukumäärään n. Tällöin matkaviestimen MS salausalgoritmi pysyy oikeassa tahdissa. Vastaavalla tavalla päätelaite TE, joka on pakettiyhteyden PDN vastaanottava pää matkaviestimeltä MS tulevan liikenteen suhteen, merkitsee toistoviiveen kasvattamiseksi mahdollisesti lisättävät ylimääräiset kehykset 72. Tällöin seuraavaksi salauksen purkuun ja toistettavaksi edelleensiirrettävästä kehysjonosta pystytään päätelaitteen TE salauksen purussa erottamaan ylimääräiset kehykset, joita ei lasketa mukaan vastaanotettujen kehysten lukumäärään n. Toistoviiveen ohjaus päätelaitteessa TE tapahtuu siis kuvion 2 kaavioon viitaten ennen suodatinlohkoa 25. Toistoviiveen kasvattamiseksi lisättävä kehys voidaan merkitä ylimääräiseksi kehykseksi jollakin ennalta sovitulla tavalla. Tapa, jolla merkintä tehdään, ei ole merkityksellinen keksinnön perusajatuksen kannalta. Tärkeintä on, että tietoliikenneyhteyden vastaanottava osapuoli pystyy tunnistamaan

ylimääräiset kehykset. Merkintä voidaan tehdä esimerkiksi käyttämällä erityistä tähän tarkoitukseen varattua parametria, joka välitetään ylimääräisen kehyksen 72 toisessa puhelohkossa, joka on C-varastettu. Merkintä voidaan tehdä jokaiseen ylimääräiseen kehykseen tai jos lähetetään useita ylimääräisiä kehyksiä peräkkäin, on myös mahdollista, että merkintä on vain ensimmäisessä ylimääräisessä kehyksessä ja samalla ilmoitetaan sitä seuraavien ylimääräisten kehysten lukumäärä.

Alan ammattilaiselle on ilmeistä, että tekniikan kehittyessä keksinnön perusajatus voidaan toteuttaa monin eri tavoin. Keksintö ja sen suoritusmuodot eivät siten rajoitu yllä kuvattuihin esimerkkeihin vaan ne voivat vaihdella patenttivaatimusten puitteissa.

Patenttivaatimukset

1. Menetelmä päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta, jossa määritetään tietoliikenneyhteyden vastaanottavassa päässä vastaanotettujen kehysten lukumäärän perusteella vastaanotetun kehyksen salauksen purkamisessa kulloinkin käytettävä kehystä vastaava alustusvektorin arvo, ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä, jolloin siirrettävän tiedon toistoviivettä voidaan kasvattaa lisäämällä yksi tai useampia ylimääräisiä kehyksiä siirrettävään kehysjonoon, t u n n e t t u siitä, että

merkitään toistoviiveen kasvattamiseksi lisättävä kehys ylimääräiseksi kehykseksi ja

lasketaan vastaanotettujen kehysten lukumäärään vain ylimääräiseksi merkitsemättömät kehykset.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että

toistoviiveen kasvatus suoritetaan pakettikytketyn yhteyden vastaanottavassa päässä.

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, t u n n e t t u siitä, että pakettikytketty yhteys käyttää Internet-protokollaa.

4. Patenttivaatimuksen 1, 2 tai 3 mukainen menetelmä, t u n n e t t u siitä, että tietoliikenneyhteys kuuluu TETRA-järjestelmään.

5. Jonkin patenttivaatimuksista 1–4 mukainen menetelmä, t u n n e t t u siitä, että toistoviiveen kasvattamiseksi lisättävä ylimääräinen kehys käsittää varastetun puhelohkon, jolloin mainittu merkintä tehdään varastettuun puhelohkoon.

6. Jonkin patenttivaatimuksista 1–5 mukainen menetelmä, t u n n e t t u siitä, että salaus suoritetaan avainsarjan avulla, jonka luomisessa käytetään alustusvektoria.

7. Järjestely päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä (PDN), jolloin siirrettävän tiedon toistoviivettä voidaan kasvattaa lisäämällä yksi tai useampia ylimääräisiä kehyksiä (72) siirrettävään kehysjonoon (75), jolloin järjestely käsittää

välineet (MS, TE) tietoliikenneyhteyden vastaanottavassa päässä vastaanotetun kehyksen salauksen purkamisessa kulloinkin käytettävän kehystä vastaavan alustusvektorin arvon määrittämiseksi vastaanotettujen kehysten lukumäärän perusteella, t u n n e t t u siitä, että järjestely käsittää lisäksi

välineet (GW, TE) toistoviiveen säätämiseksi, jotka on sovitettu merkitsemään toistoviiveen kasvattamiseksi lisättävä kehys ylimääräiseksi kehykseksi, jolloin välineet (MS, TE) alustusvektorin arvon määrittämiseksi on sovitettu laskemaan vastaanotettujen kehysten lukumäärään vain ylimääräiseksi merkitsemättömät kehykset.

8. Patenttivaatimuksen 7 mukainen järjestely, t u n n e t t u siitä, että välineet (GW, TE) toistoviiveen säätämiseksi sijaitsevat pakettikytketyn yhteyden (PDN) vastaanottavassa päässä.

9. Patenttivaatimuksen 7 tai 8 mukainen järjestely, t u n n e t t u siitä, että pakettikytketty yhteys (PDN) käyttää Internet-protokollaa.

10. Patenttivaatimuksen 7, 8 tai 9 mukainen järjestely, t u n n e t t u siitä, että tietoliikenneyhteys kuuluu TETRA-järjestelmään.

11. Jonkin patenttivaatimuksista 7–10 mukainen järjestely, t u n n e t t u siitä, että toistoviiveen kasvattamiseksi lisättävä ylimääräinen kehys (72) käsittää varastetun puhelohkon, jolloin välineet (GW, TE) toistoviiveen säätämiseksi on sovitettu tekemään mainittu merkintä varastettuun puhelohkoon.

12. Jonkin patenttivaatimuksista 7–11 mukainen järjestely, t u n n e t t u siitä, että salaus suoritetaan avainsarjan avulla, jonka luomisessa käytetään alustusvektoria.

13. Verkkoelementti päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta, jossa määritetään tietoliikenneyhteyden vastaanottavassa päässä vastaanotettujen kehysten lukumäärän perusteella vastaanotetun kehyksen salauksen purkamisessa kulloinkin käytettävä kehystä vastaava alustusvektorin arvo, ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä (PDN), jolloin

verkkoelementti (GW, TE) on sovitettu tarvittaessa kasvattamaan siirrettävän tiedon toistoviivettä lisäämällä yhden tai useampia ylimääräisiä kehyksiä (72) siirrettävään kehysjonoon (75), t u n n e t t u siitä, että

verkkoelementti on lisäksi sovitettu merkitsemään toistoviiveen kasvattamiseksi lisättävä kehys ylimääräiseksi kehykseksi.

14. Patenttivaatimuksen 13 mukainen verkkoelementti, t u n n e t t u siitä, että verkkoelementti sijaitsee pakettikytketyn yhteyden (PDN) vastaanottavassa päässä.

15. Patenttivaatimuksen 13 tai 14 mukainen verkkoelementti, t u n n e t t u siitä, että toistoviiveen kasvattamiseksi lisättävä ylimääräinen kehys (72) käsittää varastetun puhelohkon, jolloin verkkoelementti on sovitettu tekemään mainittu merkintä varastettuun puhelohkoon.

16. Patenttivaatimuksen 13, 14 tai 15 mukainen verkkoelementti, t u n n e t t u siitä, että pakettikytketty yhteys (PDN) käyttää Internet-protokollaa.

17. Jonkin patenttivaatimuksista 13–16 mukainen verkkoelementti, t u n n e t t u siitä, että tietoliikenneyhteys kuuluu TETRA-järjestelmään.

18. Jonkin patenttivaatimuksista 13–17 mukainen verkkoelementti, t u n n e t t u siitä, että salaus suoritetaan avainsarjan avulla, jonka luomisessa käytetään alustusvektoria.

19. Patenttivaatimuksen 17 tai 18 mukainen verkkoelementti, t u n n e t t u siitä, että verkkoelementti on TETRA käyttöpaikan työasema.

20. Jonkin patenttivaatimuksista 13–18 mukainen verkkoelementti, t u n n e t t u siitä, että verkkoelementti on tukiasema.

21. Jonkin patenttivaatimuksista 13–18 mukainen verkkoelementti, t u n n e t t u siitä, että verkkoelementti on mediayhdyskäytävä.

22. Verkkoelementti, joka käyttää tietoliikenneyhteyttä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä (PDN), jolloin siirrettävän tiedon toistoviivettä voidaan kasvattaa lisäämällä yksi tai useampia ylimääräisiä kehyksiä (72) siirrettävään kehysjonoon (75), jolloin

verkkoelementti (TE, MS) on sovitettu määrittämään vastaanotetun kehyksen salauksen purkamisessa kulloinkin käytettävän kehystä vastaavan alustusvektorin arvon vastaanotettujen kehysten lukumäärän perusteella, t u n n e t t u siitä, että

verkkoelementti on lisäksi sovitettu, kun toistoviiveen kasvattamiseksi lisättävät kehykset on merkitty ylimääräisiksi kehyksiksi, laskemaan

vastaanotettujen kehysten lukumäärään vain kehykset, joita ei ole merkitty ylimääräisiksi.

23. Patenttivaatimuksen 22 mukainen verkkoelementti, t u n n e t t u siitä, että toistoviiveen kasvattamiseksi lisättävä ylimääräinen kehys (72) käsittää varastetun puhelohkon, jolloin mainittu merkintä on varastetussa puhelohkossa.

24. Patenttivaatimuksen 22 tai 23 mukainen verkkoelementti, t u n n e t t u siitä, että pakettikytketty yhteys (PDN) käyttää Internet-protokollaa.

25. Patenttivaatimuksen 22, 23 tai 24 mukainen verkkoelementti, t u n n e t t u siitä, että tietoliikenneyhteys kuuluu TETRA-järjestelmään.

26. Jonkin patenttivaatimuksista 22–25 mukainen verkkoelementti, t u n n e t t u siitä, että salaus suoritetaan avainsarjan avulla, jonka luomisessa käytetään alustusvektoria.

27. Patenttivaatimuksen 25 tai 26 mukainen verkkoelementti, t u n n e t t u siitä, että verkkoelementti on TETRA käyttöpaikan työasema.

28. Jonkin patenttivaatimuksista 22–26 mukainen verkkoelementti, t u n n e t t u siitä, että verkkoelementti on tukiasema.

29. Jonkin patenttivaatimuksista 22–26 mukainen verkkoelementti, t u n n e t t u siitä, että verkkoelementti on matkaviestin.

Patentkrav

1. Förfarande för att upprätthålla en point-to-point -synkronisering på en telekommunikationsförbindelse, över vilken data överförs i ramar väsentligen i realtid och genom användning av en synkroniserad point-to-point -kryptering, vari värdet på en formatteringsvektor motsvarande ramen som skall användas vid dechiffreringen av den mottagna ramens kryptering bestäms på basis av antalet ramar som mottagits i telekommunikationsförbindelsens mottagande ända, och varvid åtminstone en del av telekommunikationsförbindelsen bildas av en paketkopplad förbindelse, varvid repetitionsfördröjningen för den information som skall överföras kan ökas genom att lägga till en eller flera extra ramar i den ramkö som skall överföras, k ä n n e t e c k n a t av att

ramen som skall läggas till för att öka repetitionsfördröjningen markeras som en extra ram och

till antalet mottagna ramar räknas endast omarkerade ramar.

2. Förfarande enligt patentkrav 1, k ä n n e t e c k n a t av att

ökningen av repetitionsfördröjningen utförs i den paketkopplade förbindelsens mottagande ända.

3. Förfarande enligt patentkrav 1 eller 2, k ä n n e t e c k n a t av att den paketkopplade förbindelsen använder ett Internet-protokoll.

4. Förfarande enligt patentkrav 1, 2 eller 3, k ä n n e t e c k n a t av att telekommunikationsförbindelsen hör till TETRA-systemet.

5. Förfarande enligt något av patentkraven 1-4, k ä n n e t e c k n a t av att den extra ramen som skall läggas till för att öka repetitionsfördröjningen omfattar ett stulet talblock, varvid nämnda markering görs i det stulna talblocket.

6. Förfarande enligt något av patentkraven 1-5, k ä n n e t e c k n a t av att krypteringen utförs med hjälp av en nyckelserie, vid skapandet av vilken används en formatteringsvektor.

7. Arrangemang för att upprätthålla en point-to-point -synkronisering på en telekommunikationsförbindelse, över vilken data överförs i ramar väsentligen i realtid och genom användning av en synkroniserad point-to-point -kryptering, och varvid åtminstone en del av telekommunikationsförbindelsen bildas av en paketkopplad förbindelse (PDN), varvid repetitionsfördröjningen för den information som skall överföras kan ökas genom att lägga till en eller flera extra ramar (72) i den ramkö (75) som skall överföras, varvid arrangemanget omfattar

don (MS, TE) för att bestämma värdet på en formatteringsvektor motsvarande ramen som skall användas vid dechiffreringen av krypteringen av ramen som mottagits i telekommunikationsförbindelsens mottagande ända på basis av antalet mottagna ramar, k ä n n e t e c k n a t av att arrangemanget dessutom omfattar

don (GW, TE) för reglering av repetitionsfördröjningen, vilka är anordnade att markera ramen som skall läggas till för att öka repetitionsfördröjningen som en extra ram, varvid donen (MS, TE) för att bestämma värdet på formatteringsvektorn är anordnade att till antalet mottagna ramar räkna endast omarkerade ramar.

8. Arrangemang enligt patentkrav 7, k ä n n e t e c k n a t av att donen (GW, TE) för reglering av repetitionsfördröjningen är belägna i den paketkopplade förbindelsens (PDN) mottagande ända.

9. Arrangemang enligt patentkrav 7 eller 8, k ä n n e t e c k n a t av att den paketkopplade förbindelsen (PDN) använder ett Internet-protokoll.

10. Arrangemang enligt patentkrav 7, 8 eller 9, k ä n n e t e c k n a t av att telekommunikationsförbindelsen hör till TETRA-systemet.

11. Arrangemang enligt något av patentkraven 7-10, k ä n n e t e c k n a t av att den extra ramen (72) som skall läggas till för att öka repetitionsfördröjningen omfattar ett stulet talblock, varvid donen (GW, TE) för reglering av repetitionsfördröjningen är anordnade att göra nämnda markering i det stulna talblocket.

12. Arrangemang enligt något av patentkraven 7-11, k ä n n e t e c k n a t av att krypteringen utförs med hjälp av en nyckelserie, vid skapandet av vilken används en formatteringsvektor.

13. Nätelement för att upprätthålla en point-to-point -synkronisering på en telekommunikationsförbindelse, över vilken data överförs i ramar väsentligen i realtid och genom användning av en synkroniserad point-to-point -kryptering, vari värdet på en formatteringsvektor motsvarande ramen som skall användas vid dechiffreringen av krypteringen av den mottagna ramen bestäms på basis av antalet ramar som mottagits i telekommunikationsförbindelsens mottagande ända, och varvid åtminstone en del av telekommunikationsförbindelsen bildas av en paketkopplad förbindelse (PDN), varvid

nätelementet (MS, TE) är anordnat att vid behov öka repetitionsfördröjningen för informationen som skall överföras genom att lägga till en eller

flera extra ramar (72) i ramkön (75) som skall överföras, k ä n n e t e c k n a t av att

nätelementet dessutom är anordnat att markera ramen som skall läggas till för att öka repetitionsfördröjningen som en extra ram.

14. Nätelement enligt patentkrav 13, k ä n n e t e c k n a t av att nätelementet är beläget i den paketkopplade förbindelsens (PDN) mottagande ända.

15. Nätelement enligt patentkrav 13 eller 14, k ä n n e t e c k n a t av att den extra ramen (72) som skall läggas till för att öka repetitionsfördröjningen omfattar ett stulet talblock, varvid nätelementet är anordnat att göra nämnda markering i det stulna talblocket.

16. Nätelement enligt patentkrav 13, 14 eller 15, k ä n n e t e c k n a t av att den paketkopplade förbindelsen (PDN) använder ett Internetprotokoll.

17. Nätelement enligt något av patentkraven 13-16, k ä n n e t e c k n a t av att telekommunikationsförbindelsen hör till TETRA-systemet.

18. Nätelement enligt något av patentkraven 13-17, k ä n n e t e c k n a t av att krypteringen utförs med hjälp av en nyckelserie, vid skapandet av vilken används en formatteringsvektor.

19. Nätelement enligt något av patentkraven 17 eller 18, k ä n n e t e c k n a t av att nätelementet är en arbetsstation i TETRA driftstället.

20. Nätelement enligt något av patentkraven 13-18, k ä n n e t e c k n a t av att nätelementet är en basstation.

21. Nätelement enligt något av patentkraven 13-18, k ä n n e t e c k n a t av att nätelementet är en media-gateway.

22. Nätelement som använder en telekommunikationsförbindelse, över vilken data överförs i ramar väsentligen i realtid och genom användning av en synkroniserad point-to-point -kryptering, och varvid åtminstone en del av telekommunikationsförbindelsen bildas av en paketkopplad förbindelse (PDN), varvid repetitionsfördröjningen för den information som skall överföras kan ökas genom att lägga till en eller flera extra ramar (72) i den ramkö (75) som skall överföras, varvid

nätelementet (TE, MS) är anordnat att bestämma värdet på en formatteringsvektor motsvarande ramen som skall användas vid dechiffreringen av den mottagna ramens kryptering på basis av antalet mottagna ramar, k ä n n e t e c k n a t av att

nätelementet dessutom är anordnat att, när ramarna som skall läggas till för att öka repetitionsfördröjningen är markerade som extra ramar, till antalet mottagna ramar endast räkna ramar som inte har markerats som extra.

23. Nätelement enligt patentkrav 22, k ä n n e t e c k n a t av att den extra ramen (72) som skall läggas till för att öka repetitionsfördröjningen omfattar ett stulet talblock, varvid nämnda markering finns i det stulna talblocket.

24. Nätelement enligt patentkrav 22 eller 23, k ä n n e t e c k n a t av att den paketkopplade förbindelsen (PDN) använder ett Internet-protokoll.

25. Nätelement enligt patentkrav 22, 23 eller 24, k ä n n e t e c k n a t av att telekommunikationsförbindelsen hör till TETRA-systemet.

26. Nätelement enligt något av patentkraven 22-25, k ä n n e t e c k n a t av att krypteringen utförs med hjälp av en nyckelserie, vid skapandet av vilken används en formatteringsvektor.

27. Nätelement enligt något av patentkraven 25 eller 26, k ä n n e t e c k n a t av att nätelementet är en arbetsstation i TETRA driftstället.

28. Nätelement enligt något av patentkraven 22-26, k ä n n e t e c k n a t av att nätelementet är en basstation.

29. Nätelement enligt något av patentkraven 22-26, k ä n n e t e c k n a t av att nätelementet är en media-gateway.

Fig. 1

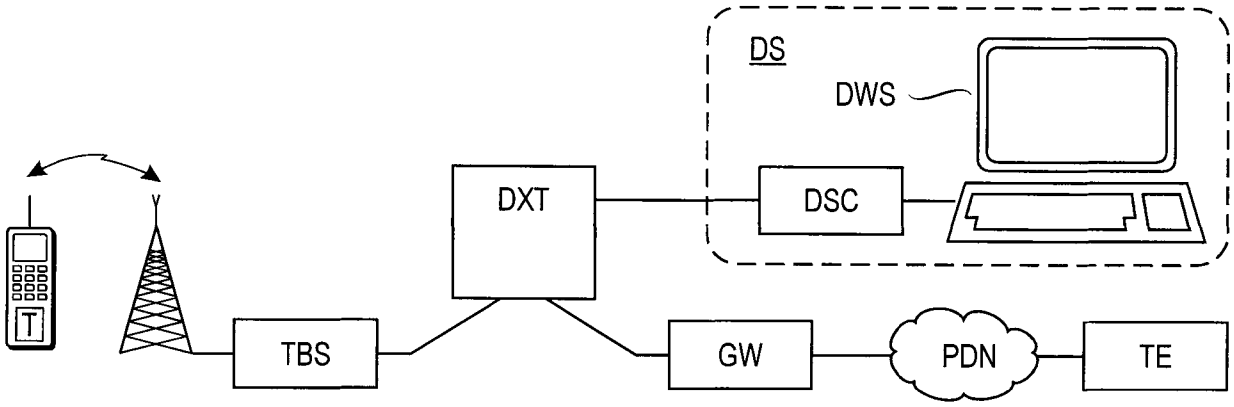


Fig. 3

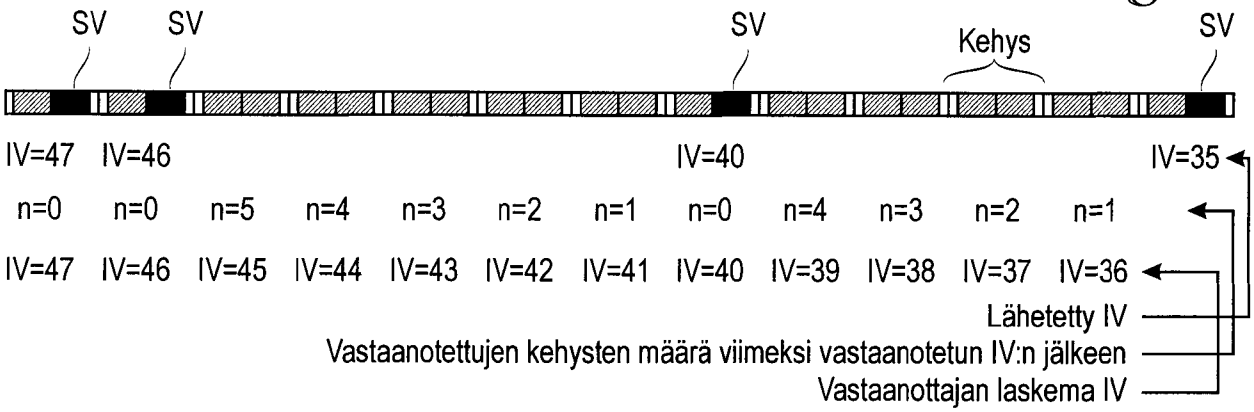
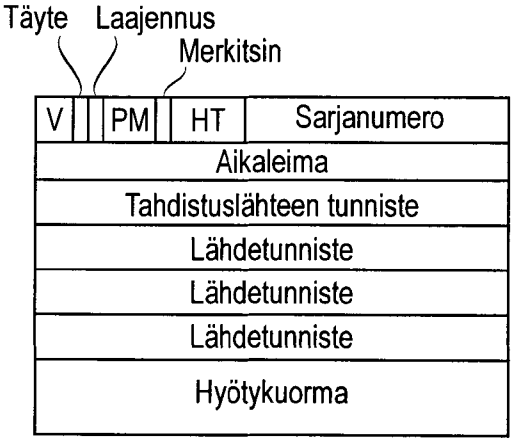


Fig. 4



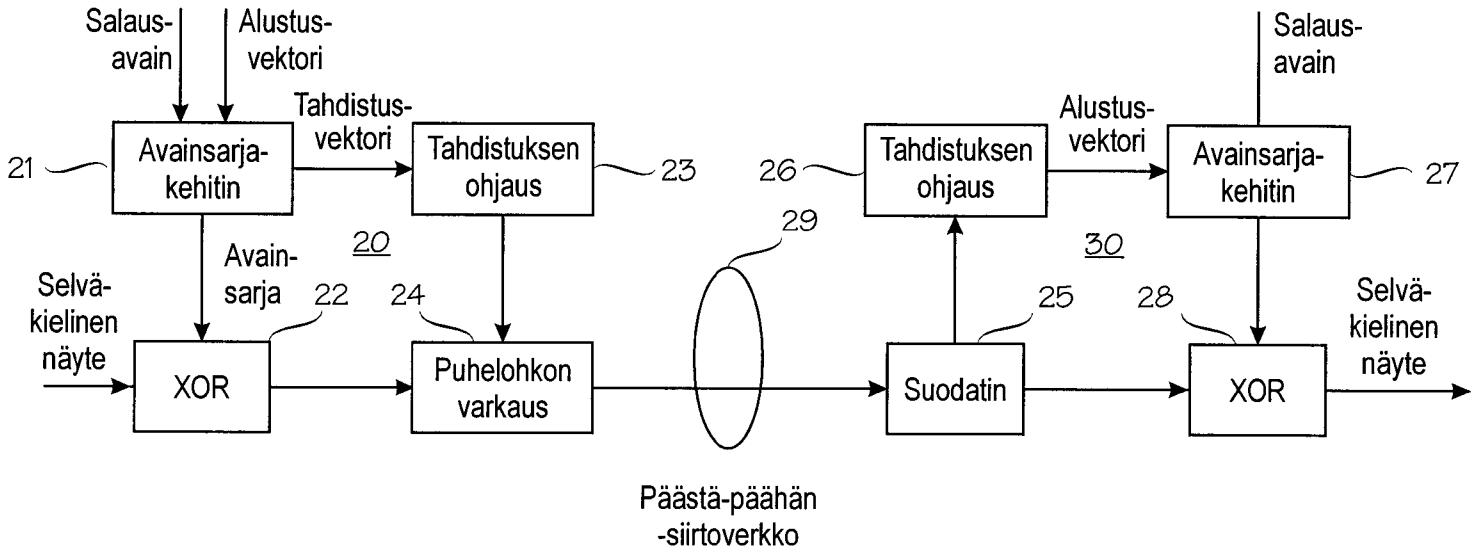


Fig. 2

Fig. 5

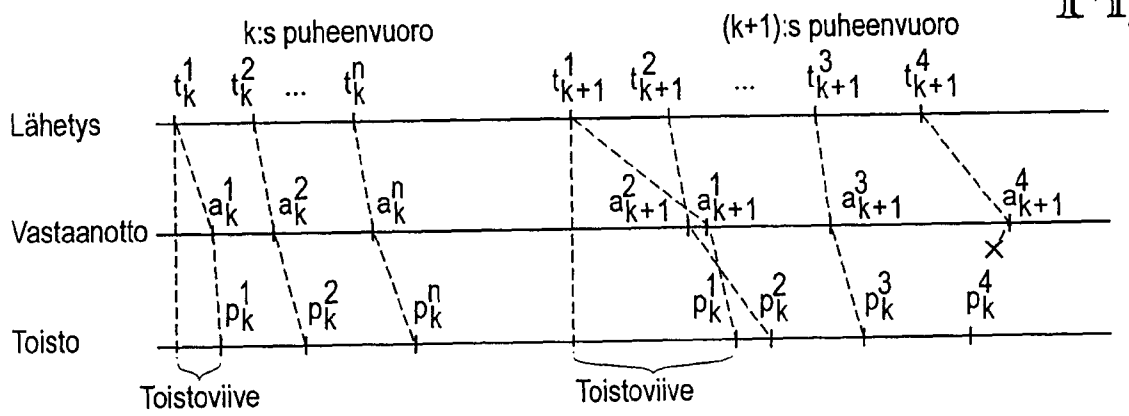


Fig. 6

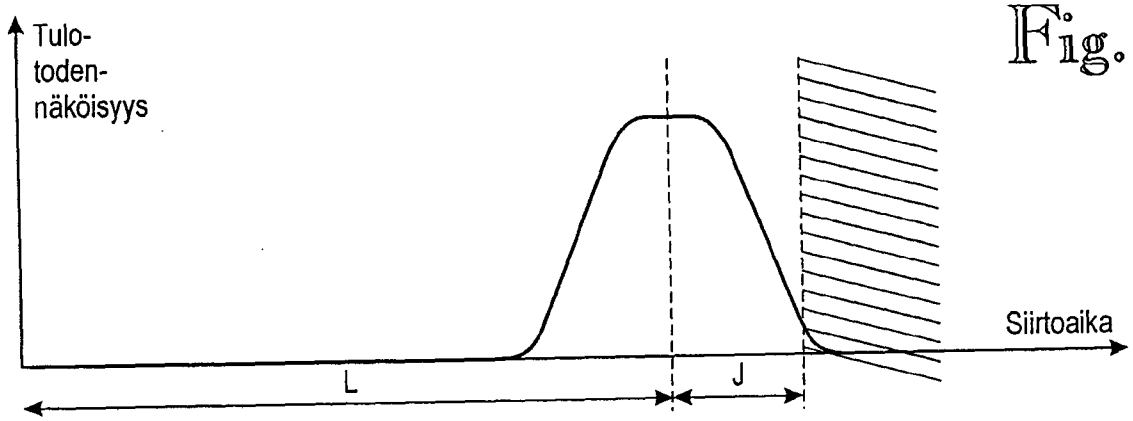
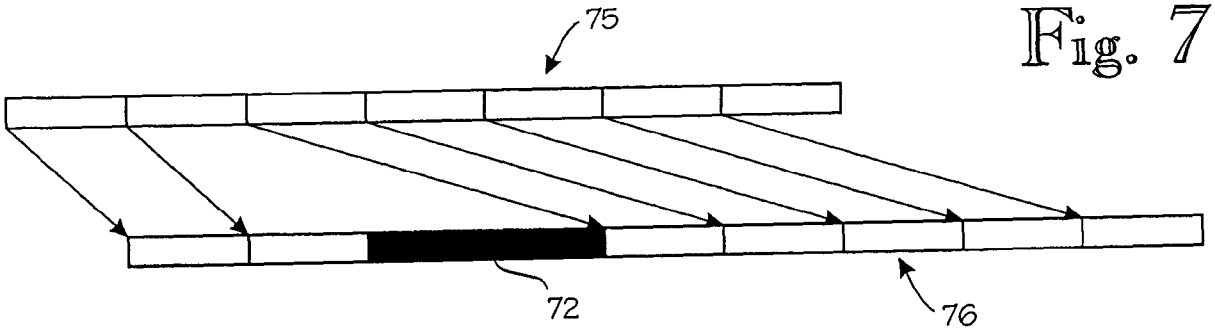


Fig. 7



PATENTTI- JA REKISTERIHALLITUS **TUTKIMUSRAPORTTI**
Patentti- ja innovaatiolinja

PATENTTIHAKEMUS NRO	LUOKITUS
20002608	HYV.NÄHT. H04L7/08, H04L9/16, H04L9/18, H04L29/08

TUTKITTU AINEISTO
Patenttijulkaisukokoelma (FI, SE, NO, DK, DE, CH, EP, WO, GB, US), tutkitut luokat H04L, H04K
Tiedonhaut ja muu aineisto EPODOC -tietokanta

VIITEJULKAISUT

Kategoria*)	Julkaisun tunnistetiedot	Koskee vaatimuksia
A (julk. 19.1.2001) A	WO-A1-0156249 (H04L29/06), (tiivistelmä) US-A-5943376 (H04L7/00), (tiivistelmä, vaatimus 1 ja 2)	

*) X Patentoitavuuden kannalta merkittävä julkaisu yksinään tarkasteltuna
Y Patentoitavuuden kannalta merkittävä julkaisu, kun otetaan huomioon tämä ja yksi tai useampi samaan kategoriaan kuuluva julkaisu
A Yleistä tekniikan tasoa edustava julkaisu, ei kuitenkaan patentoitavuuden este

Päiväys	Tutkija
17.12.2001	Jouko Berndtson