FI000110736B

(12) **PATENTTIJULKAISU**
PATENTSKRIFT

(10) **FI 110736 B**

(45) Patentti myönnetty - Patent beviljats **14.03.2003**

(51) Kv.lk.7 - Int.kl.7
H04L 9/28, H04Q 7/38

(21) Patenttihakemus - Patentansökning **20001734**

(22) Hakemispäivä - Ansökningsdag **01.08.2000**

(24) Alkupäivä - Löpdag **01.08.2000**

(41) Tullut julkiseksi - Blivit offentlig **02.02.2002**

SUOMI – FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN

(73) Haltija - Innehavare

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

(72) Keksijä - Uppfinnare

1 •Niemi,Valtteri, Topeliuksenkatu 32 G 11, 00290 Helsinki, SUOMI - FINLAND, (FI)
2 •Niemelä,Kari, Löylykuja 3 as. 2, 90650 Oulu, SUOMI - FINLAND, (FI)
3 •Hamiti, Shkumbin, Leenankuja 2 K 115, 02230 Espoo, SUOMI - FINLAND, (FI)
4 •Sebire,Guillaume, Postimiehenkatu 16 A 16, 00150 Helsinki, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud: Kolster Oy Ab
Iso Roobertinkatu 23, 00120 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning

Datansiirtomenetelmä, tilaajapäätelaite ja GPRS/EDGE-radioliityntäverkko
Dataöverföringsförfarande, abonnentterminal och GPRS/EDGE-radioanslutningsnät

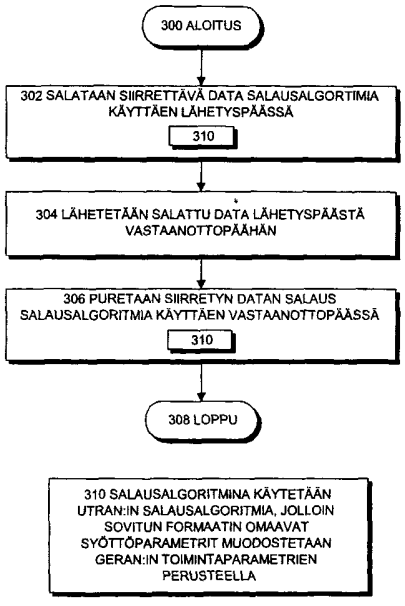
(56) Viitejulkaisut - Anförda publikationer

FI B 105964 (H04L 9/14), FI B 105385 (H04Q 7/38), WO A 9939525 (H04Q 7/22)

(57) Tiivistelmä - Sammandrag

Keksinnön kohteena on menetelmä siirtää dataa matkapuhelinjärjestelmän GPRS/EDGE-radioliityntäverkon GERAN ja tilaajapäätelaitteen välillä, sekä menetelmää käyttävä tilaajapäätelaite sekä GERAN. Menetelmässä (302) salataan siirrettävä data salausalgo- ritmia käyttäen lähetyspäässä, (304) lähetetään salattu data lähetyspäästä vastaanottopäähän; ja (306) puretaan siirretyn datan salaus salausalgoritmia käyttäen vastaanottopäässä. Salausalgoritmina käytetään universaalin matkapuhelinjärjestelmän laajakais- taista koodijakoista monikäyttömenetelmää käyttävän radioliityntäverkon UTRAN salausalgoritmia, jolloin salausalgoritmin vaatimat sovitun formaatin omaavat syöttöparametrit muodostetaan GPRS/EDGE-radioliityntäverkon GERAN toimintaparametrien perusteella.

Uppfinningen avser ett förfarande med vars hjälp i ett mobiltelefonsystems GPRS/EDGE-radioanslutningsnät data överföres mellan GERA och en abonnentapparat, samt en abonnentapparat och en GERA som använder sig av sagda förfarande. Vid sagda förfarande (302) schiffreras i sändningsänden den data som skall överföras med hjälp av en schiffreringsalgoritm, (304) sändes sagda schiffrerade data från sagda sändningsände till en mottagningsände; och (306) deschiffreras den överförda datans schiffrering i sagda mottagningsände med hjälp av en schiffreringsalgoritm. Som schiffreringsalgoritm användes en schiffreringsalgoritm i ett universalt mobiltelefonsystem, som använder sig av ett bredbandigt kodindelat multianvändningsförfarande för ett radioanslutningsnät UTRAN, varvid de av sagda schiffreringsalgoritm krävda matningsparametrarna i ett överenskommet format, bildas på basen av GPRS/EDGE-radioanslutningsnätets GERAN funktionsparametrar.



Datansiirtomenetelmä, tilaajapäätelaite ja GPRS/EDGE-radioliityntäverkko

Ala

Keksintö liittyy menetelmään siirtää dataa matkapuhelinjärjestelmän GPRS/EDGE-radioliityntäverkon GERAN (General Packet Radio Service/Enhanced Data Rates for GSM Evolution) ja tilaajapäätelaitteen välillä, tilaajapäätelaitteeseen ja GPRS/EDGE-radioliityntäverkkoon GERAN.

Tausta

Siirrettäessä dataa GERAN:ista tilaajapäätelaitteeseen ja päinvastoin, on siirrettävä data turvallisuussyistä salattava ennen siirtoa. Salaaminen vaikeuttaa signaloinnin ja käyttäjän datan salakuuntelua. Siirrettävä data salataan salausalgoritmia käyttäen lähetyspäässä, ja salattu data lähetetään lähetyspäästä vastaanottopäähän, jossa siirretyn datan salaus puretaan salausalgoritmia käyttäen. Sekä lähetys- että vastaanottopäässä käytetään samaa salausalgoritmia.

Salausalgoritmin tuottama salausmaski liitetään XOR-operaatiolla (looginen eksklusiivinen TAI -operaatio) salattavaan dataan, joten salaaminen ei sinänsä lisää lähetettävien bittien määrää. Tämä voidaan ilmaista kaavalla

$$C = M \oplus P \tag{1}$$

jossa C on salattu data, M on salausmaski, P on salaamaton data, ja $\oplus$ on XOR-operaatio.

Salausalgoritmi tarvitsee syöttöparametreja, jotta algoritmin tuloksena saatava salausmaski on erilainen kullekin käyttäjälle ja kullekin käyttökerralle. Tärkein parametri on salausavain, jonka pituus on esimerkiksi 128 bittiä. Kullekin käyttäjälle käytetään eri salausavainta ja siten eri salausmaskia. Ongelmaksi kuitenkin muodostuu se, että samaa salausmaskia ei saa käyttää kahta kertaa erisisältöisille datoille. Tällainen kielletty tilanne voidaan kuvata kaavalla:

$$\begin{array}{rl} & P_1 \oplus M = C_1 \\ \oplus & P_2 \oplus M = C_2 \\ \hline & P_1 \oplus P_2 = C_1 \oplus C_2 \end{array} \tag{2}$$

jossa P_1 ja P_2 ovat erisisältöisiä salaamattomia datoja, sekä C_1 ja C_2 ovat erisisältöisiä salattuja datoja. Kuten nähdään, niin mahdollinen sala-

kuuntelija voi poistaa maskin suorittamalla erisisältöisten samalla maskilla salattujen datojen kesken XOR-operaation, ja siten murtaa salauksen.

Tämän takia salausalgoritmissa käytetään myös muita parametreja, esimerkiksi universaalin matkapuhelinjärjestelmän (UMTS) laajakaistaista koodijakoista monikäyttömenetelmää käyttävän radioliityntäverkon (UTRAN) salausalgoritmi käyttää syöttöparametreinaan ajan mukaan muuttuvaa laskuriparametria, suuntaparametria (nouseva siirtotie/laskeva siirtotie) ja beareriparametria.

GERAN:issa käytettävän salausalgoritmin rakennetta ei ole vielä päätetty. Sen tulee kuitenkin täyttää ainakin seuraavat vaatimukset:

- Implisiittinen salauksen synkronointi, etenkin kanavanvaihdon yhteydessä.
- Samanlainen lähestymistapa sekä reaaliaikaisissa että ei-reaaliaikaisissa palveluissa.
- Inkrementaalinen redundanssi.
- Useiden eri käyttäjien multipleksaaminen samalle aikavälille.
- Useiden eri radiobearereiden multipleksaaminen samalle tilaajapäätelaitteelle.
- Moniaikavälitoiminnan (multislot operation) mahdollistaminen.

Keksinnön lyhyt selostus

Keksinnön tavoitteena on tarjota parannettu menetelmä siirtää dataa matkapuhelinjärjestelmän GPRS/EDGE-radioliityntäverkon GERAN ja tilaajapäätelaitteen välillä, parannettu tilaajapäätelaite, sekä parannettu GPRS/EDGE-radioliityntäverkko GERAN. Keksinnön eräänä puolena esitetään patenttivaatimuksen 1 mukainen menetelmä siirtää dataa matkapuhelinjärjestelmän GPRS/EDGE-radioliityntäverkon GERAN ja tilaajapäätelaitteen välillä. Keksinnön eräänä puolena esitetään patenttivaatimuksen 17 mukainen tilaajapäätelaite. Keksinnön eräänä puolena esitetään patenttivaatimuksen 33 mukainen GPRS/EDGE-radioliityntäverkko GERAN. Keksinnön edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Keksintö perustuu siihen, että UTRAN:in salausalgoritmia käytetään sellaisenaan uudelleen GERAN:issa. Tämä on mahdollista määrittelemällä salausalgoritmin sisäinen toiminta mustaksi laatikoksi, ja muokkaamalla salausalgoritmin vaatimia syöttöparametreja GERAN:in asettamien vaatimusten mukaan.

Keksinnön mukaisella menetelmällä ja laitteistolla saavutetaan useita parannuksia. Uuden salausalgoritmin suunnittelu on erittäin vaativa operaatio. Keksinnön mukaisesti toimittaessa GERAN:ia varten ei tarvitse suunnitella uutta salausalgoritmia, vaan voidaan käyttää jo valmiiksi suunniteltua UTRAN:in salausalgoritmia. Täten säästyy merkittävä työmäärä ja sen aiheuttamat tuotekehityskustannukset. Keksintö myös helpottaa sellaisten tilaajapäätelaitteiden, joilla voidaan ottaa yhteyttä sekä UTRAN:iin että GERAN:iin, suunnittelua.

Kuvioiden lyhyt selostus

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

Kuvio 1A esittää esimerkkiä solukkoradioverkon rakenteesta;

Kuvio 1B esittää tarkemmin solukkoradioverkkoa lohkokaaviona;

Kuvio 1C esittää piirikytkentäistä yhteyttä;

Kuvio 1D esittää pakettikytkentäistä yhteyttä;

Kuvio 2 kuvaa esimerkkiä solukkoradioverkon tiettyjen osien protokollapinoista;

Kuvio 3 on vuokaavio havainnollistaen menetelmää siirtää dataa;

Kuvio 4 havainnollistaa salauksen suorittamista lähetyspäässä ja salauksen purkua vastaanottopäässä.

Sovellusmuotojen selostus

Kolmannen sukupolven, kuten UMTS, matkapuhelinjärjestelmiin spesifikaatioita kehittää 3GPP (Third Generation Partnership Project), jonka kotisivuilta osoitteessa http://www.3gpp.org löytyy järjestelmän yleiseen rakenteeseen ja salaukseen liittyviä spesifikaatioita, joihin tutustumalla alan ammattilainen saa hyvän, keksinnön käytön mahdollistavan kuvauksen. Erityisesti tähän otetaan viitteeksi salaukseen liittyvät spesifikaatiot:

- 3G TS 33.102 V3.2.0: Security Architecture
- 3G TS 25.301 V3.4.0: Radio Interface Protocol Architecture
- 3G TS 33.105 V3.3.0: Cryptographic Algorithm Requirements.

Viitaten kuvioihin 1A ja 1B selostetaan tyypillinen radiojärjestelmän rakenne ja sen liittymät kiinteään puhelinverkkoon ja pakettisiirtoverkkoon. Kuvio 1B sisältää vain sovellusmuotojen selittämisen kannalta oleelliset lohkot, mutta alan ammattilaiselle on selvää, että tavanomaiseen solukkoradioverkkoon sisältyy lisäksi muitakin toimintoja ja rakenteita, joiden tar-

kempi selittäminen ei tässä ole tarpeen. Keksinnön kohteena oleva radiojärjestelmä käyttää GPRS/EDGE-radioliityntäverkkoa GERAN. Termillä GERAN tarkoitetaan GSM-järjestelmän (Global System for Mobile Communication) TDMA/136-järjestelmän (Time Division Multiple Access) ja EDGE-järjestelmän evoluutiota, jonka tarkoituksena on tarjota täydet kolmannen sukupolven (UMTS/WCDMA/cdma2000) matkapuhelinpalvelut.

GERAN on siis eräässä mielessä GSM-pohjaisten GPRS:n tai EGPRS:n (Enhanced General Packet Radio Service), ja laajakaistaista koodijakoista monikäyttömenetelmää (Wideband Code Division Multiple Access) käyttävän universaalin matkapuhelinjärjestelmän UMTS välimuoto, jossa radioliityntäverkon rakenne on hahmotettu UMTS-tyylisesti ja radioliityntäverkkoa kutsutaan esimerkiksi GERAN:iksi ja jossa radiorajapinta on kuitenkin GSM--pohjainen normaali radiorajapinta tai EDGE-modulaatiota käyttävä radiorajapinta. EGPRS on GSM-pohjainen pakettikytkentäistä siirtoa hyödyntävä järjestelmä. EGPRS käyttää EDGE-tekniikkaa tiedonsiirtokapasiteetin lisäämiseksi. Normaalisti GSM:ssä käytettävän GMSK-moduloinnin (Gaussian Minimum-Shift Keying) lisäksi voidaan käyttää 8-PSK (8-Phase Shift Keying) -modulointia pakettidatakanaville. Tavoitteena on lähinnä toteuttaa ei-reaaliaikaisia tiedonsiirtopalveluita kuten tiedoston kopiointia ja Internet-selaimen käyttöä, mutta myös reaaliaikaisia palveluita pakettikytkentäisesti esimerkiksi puheen ja videokuvan siirtoon.

Kuvioiden 1A ja 1B kuvaus pohjautuu lähinnä UMTS:ään. Matkapuhelinjärjestelmän pääosat ovat ydinverkko (Core Network) CN, universaalin matkapuhelinjärjestelmän maanpäällinen radioliityntäverkko (UMTS Terrestrial Radio Access Network) UTRAN ja tilaajapäätelaite (User Equipment) UE. CN:n ja UTRAN:in välinen rajapinta on nimeltään Iu, ja UTRAN:in ja UE:n välinen radiorajapinta on nimeltään Uu.

UTRAN muodostuu radioverkkoalijärjestelmistä (Radio Network Subsystem) RNS. RNS:ien välinen rajapinta on nimeltään Iur. RNS muodostuu radioverkkokontrollerista (Radio Network Controller) RNC ja yhdestä tai useammasta B-solmusta (Node B) B. RNC:n ja B:n välinen rajapinta on nimeltään Iub. B-solmun kuuluvuusaluetta eli solua merkitään kuviossa 1A C:llä. RNS:ää voidaan myös kutsua perinteisemmällä nimellä tukiasemajärjestelmä (Base-Station System, BSS). Radiojärjestelmän verkko-osa käsittää siis radioliityntäverkon UTRAN ja ydinverkon CN.

Kuviossa 1A esitetty kuvaus on hyvin abstrakti, joten sitä selvennetään kuviossa 1B esittämällä, mikä GSM-järjestelmän osa suunnilleen vastaa mitäkin UMTS:in osaa. On huomattava, että esitetty kuvaus ei ole mitenkään sitova, vaan suuntaa antava, sillä UMTS:in eri osien vastuut ja toiminnot ovat vielä suunnittelun alla.

Tilaajapäätelaite 150 voi olla esimerkiksi kiinteästi sijoitettu, ajoneuvoon sijoitettu tai kannettava mukana pidettävä päätelaite. Tilaajapäätelaite 150 tunnetaan myös nimellä liikkuva asema MS. radioliityntäverkon infrastruktuuri UTRAN muodostuu radioverkkoalijärjestelmistä RNS eli tukiasemajärjestelmistä. Radioverkkoalijärjestelmä RNS muodostuu radioverkkokontrollerista RNC eli tukiasemaohjaimesta 102 ja sen ohjauksessa olevasta ainakin yhdestä B-solmusta B eli tukiasemasta 100.

Tukiasemassa B on multiplekseri 116, lähetinvastaanottimia 114, ja ohjausyksikkö 118, joka ohjaa lähetinvastaanottimien 114 ja multiplekserin 116 toimintaa. Multiplekserillä 116 sijoitetaan useiden lähetinvastaanottimien 114 käyttämät liikenne- ja ohjauskanavat siirtoyhteydelle 160.

Tukiaseman B lähetinvastaanottimista 114 on yhteys antenniyksikköön 112, jolla toteutetaan kaksisuuntainen radioyhteys Uu tilaajapäätelaitteeseen 150. Kaksisuuntaisessa radioyhteydessä Uu siirrettävien kehysten rakenne on tarkasti määritelty.

Tukiasemaohjain RNC käsittää ryhmäkytkentäkentän 120 ja ohjausyksikön 124. Ryhmäkytkentäkenttää 120 käytetään puheen ja datan kytkentään sekä yhdistämään signalointipiirejä. Tukiaseman B ja tukiasemaohjaimen RNC muodostamaan tukiasemajärjestelmään kuuluu lisäksi transkooderi 122. Tukiasemaohjaimen RNC ja tukiaseman B välinen työnjako ja fyysinen rakenne voivat vaihdella toteutuksesta riippuen. Tyypillisesti tukiasema B huolehtii edellä kuvatulla tavalla radiotien toteutuksesta. Tukiasemaohjain RNC hallinnoi tyypillisesti seuraavia asioita: radioresurssien hallinta, solujen välisen kanavanvaihdon kontrolli, tehonsäätö, ajastus ja synkronointi, tilaajapäätelaitteen kutsuminen (paging).

Transkooderi 122 sijaitsee yleensä mahdollisimman lähellä matkapuhelinkeskusta 132, koska puhe voidaan tällöin siirtokapasiteettia säästäen siirtää matkapuhelinjärjestelmän muodossa transkooderin 122 ja tukiasemaohjaimen RNC välillä. Transkooderi 122 muuntaa yleisen puhelinverkon ja radiopuhelinverkon välillä käytettävät erilaiset puheen digitaaliset koodausmuodot toisilleen sopiviksi, esimerkiksi kiinteän verkon 64 kbit/s muodosta solukkora-

dioverkon johonkin muuhun (esimerkiksi 13 kbit/s) muotoon ja päinvastoin. Tässä ei tarkemmin kuvata vaadittavia laitteistoja, mutta voidaan kuitenkin todeta, ettei muulle datalle kuin puheelle suoriteta muunnosta transkooderissa 122. Ohjausyksikkö 124 suorittaa puhelunohjausta, liikkuvuuden hallintaa, tilastotietojen keräystä ja signalointia.

Ydinverkko CN muodostuu UTRAN:in ulkopuolisesta matkapuhelinjärjestelmään kuuluvusta infrastruktuurista. Kuviossa 1B kuvataan ydinverkon CN piirikytkentäiseen siirtoon kuuluvista laitteista matkapuhelinkeskus 132.

Kuten kuviosta 1B nähdään, niin kytkentäkentällä 120 voidaan suorittaa kytkentöjä (kuvattu mustilla palloilla) sekä yleiseen puhelinverkkoon 134 matkapuhelinkeskuksen 132 välityksellä että pakettisiirtoverkkoon 142. Yleisessä puhelinverkossa 134 tyypillinen päätelaite 136 on tavallinen tai ISDN-puhelin (Integrated Services Digital Network). Pakettisiirto suoritetaan Internetin 146 välityksellä matkapuhelinjärjestelmään liittyvästä tietokoneesta 148 tilaajapäätelaitteeseen 150 liitettyyn kannettavaan tietokoneeseen 152. Tilaajapäätelaitteen 150 ja kannettavan tietokoneen 152 yhdistelmän asemasta voidaan käyttää WAP-puhelinta (Wireless Application Protocol).

Pakettisiirtoverkon 142 ja kytkentäkentän 120 välisen yhteyden luo tukisolmu 140 (SGSN = Serving GPRS Support Node). Tukisolmun 140 tehtävänä on siirtää paketteja tukiasemajärjestelmän ja yhdyskäytäväsolmun (GGSN = Gateway GPRS Support Node) 144 välillä, ja pitää kirjaa tilaajapäätelaitteen 150 sijainnista alueellaan.

Yhdyskäytäväsolmu 144 yhdistää julkisen pakettisiirtoverkon 146 ja pakettisiirtoverkon 142. Rajapinnassa voidaan käyttää internet-protokollaa tai X.25-protokollaa. Yhdyskäytäväsolmu 144 kätkee kapseloimalla pakettisiirtoverkon 142 sisäisen rakenteen julkiselta pakettisiirtoverkolta 146, joten pakettisiirtoverkko 142 näyttää julkisen pakettisiirtoverkon 146 kannalta aliverkolta, jossa olevalle tilaajapäätelaitteelle 150 julkinen pakettisiirtoverkko 146 voi osoittaa paketteja ja jolta voi vastaanottaa paketteja.

Pakettisiirtoverkko 142 on tyypillisesti yksityinen internet-protokollaa käyttävä verkko, joka kuljettaa signalointia ja käyttäjän dataa. Verkon 142 rakenne voi vaihdella operaattorikohtaisesti sekä arkkitehtuuriltaan että protokolliltaan internet-protokollakerroksen alapuolella.

Julkinen pakettisiirtoverkko 146 voi olla esimerkiksi maailmanlaajuinen Internet, johon yhteydessä oleva päätelaite 148, esimerkiksi palvelintietokone, haluaa siirtää paketteja tilaajapäätelaitteelle 150.

Kuviossa 1C kuvataan, kuinka tilaajapäätelaitteen 150 ja yleisen puhelinverkon päätelaitteen 136 välille luodaan piirikytkentäinen siirtoyhteys. Kuvioissa kuvataan vahvennetulla viivalla, miten data kulkee järjestelmän läpi radiorajapinnassa 170, antennista 112 lähetinvastaanottimeen 114 ja sieltä multiplekserissä 116 multipleksattuna siirtoyhteyttä 160 pitkin kytkentäkenttään 120, jossa on muodostettu kytkentä transkooderiin 122 menevään ulostuloon, ja sieltä edelleen matkapuhelinkeskuksessa 132 tehdyn kytkennän kautta yleiseen puhelinverkkoon 134 kytkettyyn päätelaitteeseen 136. Tukiasemassa 100 ohjausyksikkö 118 ohjaa multiplekseria 116 siirron suorittamisessa, ja tukiasemaohjaimessa 102 ohjausyksikkö 124 ohjaa kytkentäkenttää 120 oikean kytkennän suorittamiseksi.

Kuviossa 1D kuvataan pakettikytkentäinen siirtoyhteys. Tilaajapäätelaitteeseen 150 on nyt kytketty kannettava tietokone 152. Vahvennettu viiva kuvaa, kuinka siirrettävä data kulkee palvelintietokoneelta 148 kannettavalle tietokoneelle 152. Tietoa voidaan siirtää tietysti myös päinvastaisessa siirtosuunnassa, siis kannettavalta tietokoneelta 152 palvelintietokoneelle 148. Data kulkee järjestelmän läpi radiorajapinnassa eli Um-rajapinnassa 170, antennista 112 lähetinvastaanottimeen 114 ja sieltä multiplekserissä 116 multipleksattuna siirtoyhteyttä 160 Abis-rajapinnassa pitkin kytkentäkenttään 120, jossa on muodostettu kytkentä tukisolmuun 140 menevään ulostuloon Gb-rajapinnassa, tukisolmusta 140 data viedään pakettisiirtoverkkoa 142 pitkin yhdyskäytäväsolmun 144 kautta kytkeytyen julkiseen pakettisiirtoverkkoon 146 kytkeytyneeseen palvelintietokoneeseen 148.

Kuvioissa 1C ja 1D ei ole selvyyden vuoksi kuvattu tapausta, jossa siirretään samanaikaisesti sekä piiri- että pakettikytkentäistä dataa. Tämä on kuitenkin täysin mahdollista ja yleistä, sillä piirikytkentäisen datan siirrosta vapaata kapasiteettia voidaan joustavasti ottaa käyttöön pakettikytkentäisen siirron toteuttamiseksi. Myös sellainen verkko voidaan rakentaa, jossa verkossa ei siirretä ollenkaan piirikytkentäistä dataa vaan ainoastaan pakettidataa. Tällöin verkon rakennetta voidaan yksinkertaistaa.

Tarkastellaan vielä uudestaan kuviota 1D. UMTS-järjestelmän eri kokonaisuudet - CN, UTRAN/GERAN, RNS/BSS, RNC/BSC, B/BTS - on hahmotettu kuvioon katkoviivalla toteutetuilla laatikoilla. Ydinverkkoon CN kuuluu pakettikytkentäympäristössä tukisolmu 140, pakettisiirtoverkko 142 ja yhdyskäytäväsolmu 144.

Edellä kuvatun lisäksi GPRS:ssä tunnetaan kaksi erityistä elementtiä: kanavakoodekkiyksikkö CCU (Channel Codec Unit) ja pakettikontrolliyksikkö PCU (Packet Control Unit). CCU:n tehtäviin kuuluu kanavakoodaus mukaanlukien FEC (Forward Error Coding) ja lomitus, radiokanavan mittaustoiminnot kuten vastaanotetun signaalin laatutaso, vastaanotetun signaalin vastaanottoteho, ja informaatio liittyen ajastuksen edistämistekijän (timing advance) mittauksiin. PCU:n tehtäviin kuuluu LLC-kehyksen (Logical Link Control) segmentointi ja uudelleenkokoaminen (re-assembly), ARQ-toiminnot (Automatic Repeat Request), PDCH:n (Packet Data Channel) skedulointi, kanavansaantikontrolli (channel access control), ja radiokanavan hallintatoiminnot. CCU 182 sijaitsee tukiasemassa 100, ja toteutuksesta riippuen sen voidaan katsoa olevan aikavälikohtainen tai lähetinvastaanotinkohtainen yksikkö. CCU:hun 182 on Abis-rajapinnan kautta yhteydessä PCU 180. PCU voi sijaita tukiasemassa 100 tai tukiasemaohjaimessa 102. Kuviossa 1C on kuvattu PCU:n 180 sijoitus tukiasemaohjaimeen 102, mutta selvyyden vuoksi sijoitusta tukiasemaan 100 ei ole kuvattu.

Kuviossa 1D kuvataan myös tilaajapäätelaitteen UE rakennetta esillä olevan sovelluksen kannalta mielenkiintoisilta osiltaan. Tilaajapäätelaite UE käsittää antennin 190, jonka välityksellä lähetinvastaanotin 192 vastaanottaa signaalin radiotieltä 170. Tilaajapäätelaitteen UE toimintaa ohjaa ohjausyksikkö 194, joka tyypillisesti on mikroprosessori tarvittavine ohjelmistoineen. Myös myöhemmin esitettävät protokollakäsittelyt suoritetaan kyseisillä ohjelmistoilla. Tilaajapäätelaite UE käsittää kuvattujen osien lisäksi myös käyttöliittymän, joka muodostuu tyypillisesti kaiuttimesta, mikrofonista, näytöstä ja näppäimistöstä, ja akun. Näitä ei kuitenkaan tässä tarkemmin kuvata, koska ne eivät ole esillä olevan keksinnön kannalta kiinnostavia.

Tässä ei myöskään tämän tarkemmin kuvata tukiaseman B lähetinvastaanottimen rakennetta, eikä myöskään tilaajapäätelaitteen UE lähetinvastaanottimen rakennetta, koska alan ammattilaiselle on selvää, miten kyseiset laitteet toteutetaan. Voidaan esimerkiksi käyttää normaalia EGPRS:n mukaista radioliityntäverkon lähetinvastaanotinta ja tilaajapäätelaitteen lähetinvastaanotinta. Esillä olevan sovelluksen kannalta on vain tärkeää, että radioyhteys 170 voidaan toteuttaa, sillä sovelluksen edellyttämä toiminta suoritetaan sitten ylemmillä OSI-mallin (Open Systems Interconnection) tasoilla, erityisesti kolmoskerroksessa.

Kuviossa 2 kuvataan EGPRS:n ohjaustason (Control Plane) pakettiprotokollapinoja. Todettakoon tässä, että sovellusmuodot eivät kuitenkaan ole rajoittuneet EGPRS:ään. Protokollapinot on muodostettu ISO:n (International Standardization Organization) OSI-mallin (Open Systems Interconnection) mukaisesti. OSI-mallissa protokollapinot jaetaan kerroksiin. Kerroksia voi periaatteessa olla seitsemän. Kuviossa 2 on kuvattu kunkin verkkoelementin osalta, mitä pakettiprotokollan osia kyseisessä verkkoelementissä käsitellään. Verkkoelementit ovat tilaajapäätelaite MS, tukiasemajärjestelmä BSS ja tukisolmu SGSN. Tukiasemaa ja tukiasemaohjainta ei ole kuvattu erikseen, koska niiden välille ei ole määritetty rajapintaa. Tukiasemajärjestelmälle BSS määrätty protokollakäsittely voidaan siis periaatteessa jakaa vapaasti tukiaseman 100 ja tukiasemaohjaimen 102 kesken, käytännössä ei kuitenkaan transkooderille 122, vaikka se tukiasemajärjestelmään BSS kuuluukin. Verkkoelementit MS, BSS ja SGSN on erotettu niiden välisillä rajapinnoilla Um ja Gb.

Kussakin laitteessa MS, BSS, SGSN oleva kerros viestii toisessa laitteessa olevan kerroksen kanssa loogisesti. Ainoastaan alimmat, fyysiset kerrokset viestivät toistensa kanssa suoraan. Muut kerrokset käyttävät aina seuraavan, alemman kerroksen tarjoamia palveluita. Viestin on siis fyysisesti kuljettava pystysuunnassa kerroksien välillä, ja ainoastaan alimmassa kerroksessa viesti kulkee vaakasuunnassa kerrosten välillä.

Varsinainen bittitason tiedonsiirto tapahtuu alinta ensimmäistä eli fyysistä kerrosta RF, L1 käyttäen. Fyysisessä kerroksessa määritellään mekaaniset, sähköiset ja toiminnalliset ominaisuudet fyysiseen siirtotiehen liittymiseksi. Seuraava toinen kerros eli siirtoyhteyskerros käyttää fyysisen kerroksen palveluita luotettavan tiedonsiirron toteuttamiseksi huolehtien esimerkiksi siirtovirheiden korjauksesta. Radiorajapinnassa 170 siirtoyhteyskerros jakautuu RLC/MAC-alikerrokseen (Radio Link Control/Medium Access Control) ja LLC-alikerrokseen (Logical Link Control) eli loogiseen linkkikontrolliprotokollaan. Kolmas kerros eli verkkokerros tarjoaa ylemmille kerroksille riippumattomuuden tiedonsiirto- ja kytkentätekniikoista, joilla hoidetaan laitteiden välinen yhteys. Verkkokerros huolehtii esimerkiksi yhteyden muodostuksesta, ylläpidosta ja purusta. GSM:ssä verkkokerrosta nimitetään myös signalointikerrokseksi. Sillä on kaksi päätehtävää: viestien reititys (routing), ja useiden itsenäisten yhteyksien mahdollistaminen samanaikaisesti kahden entiteetin välillä.

Verkkokerros käsittää istunnonhallinta-alikerroksen SM (Session management) ja liikkuvuudenhallinta-alikerroksen GMM (GPRS Mobility Management).

Liikkuvuudenhallinta-alikerros GMM huolehtii tilaajapäätelaitteen käyttäjän liikkumisesta aiheutuvat seuraukset, jotka eivät suoraan liity radioresurssienhallintaan. Kiinteän verkon puolella tämä alikerros huolehtisi käyttäjän valtuuksien tarkastamisesta ja verkkoon kytkemisestä. Solukkoradioverkoissa tämä alikerros siten tukee käyttäjän liikkuvuutta, rekisteröitymistä ja liikkumisen aiheuttaman datan hallintaa. Lisäksi tämä alikerros tarkastaa tilaajapäätelaitteen identiteetin ja sallittujen palveluiden identiteetit. Tämän alikerroksen viestiensiirto tapahtuu tilaajapäätelaitteen MS ja tukisolmun SGSN välillä.

Istunnonhallinta-alikerros SM hallitsee kaikkia pakettikytkentäisen puhelun hallintaan liittyviä toimintoja, mutta se ei havaitse käyttäjän liikkumista. Istunnonhallinta-alikerros SM perustaa, ylläpitää ja vapauttaa yhteydet. Sillä on omat proseduurinsa tilaajapäätelaitteen 150 aloittamille ja siihen päättyville puheluille. Tämänkin alikerroksen viestiensiirto tapahtuu tilaajapäätelaitteen MS ja tukisolmun SGSN välillä.

Tukiasemajärjestelmässä BSS istunnonhallinta-alikerroksen SM ja liikkuvuudenhallinta-alikerroksen GMM viestit käsitellään läpinäkyvästi, eli niitä vain siirretään edestakaisin.

Tunnetun tekniikan mukaisesti looginen linkkikontrolliprotokolla LLC toteuttaa luotettavan salaavan loogisen linkin SGSN:n ja MS:n välille. LLC on itsenäinen ja alemmista kerroksista riippumaton, jotta radiorajapinnan muuttuminen vaikuttaisi matkapuhelinverkon verkko-osaan mahdollisimman vähän. Loogisen linkkikontrolliprotokollan palvelut sisältävät: erittäin luotettavan loogisen linkin vastekerrosten (peer entities) välillä, tuen vaihtelevan mittaisille informaatiokehyksille, tuen sekä kuitatulle että kuittaamattomalle tiedonsiirrolle, kukin kehys sisältää yksikäsitteisen lähettävän tai vastaanottavan tilaajapäätelaitteen tunnisteen, tuen erilaisille palvelukriteereille kuten tiedonsiirron erilaisille prioriteeteille, siirrettävän tiedon ja käyttäjän identiteetin salauksen. Um- ja Gb-rajapintojen välillä LLC-data siirretään loogisen linkkiprotokollan välitystoiminnolla (Logical Link Control Protocol Relay) LLC RELAY. Tässä hakemuksessa kuvatun ratkaisun mukaisesti salausta ei suoriteta LLC-alikerroksessa, vaan MAC-alikerroksessa tai RLC-alikerroksessa. Myös muut LLC-alikerroksen tehtävät voidaan siirtää muille kerroksille, jolloin LLC-alikerros voidaan poistaa kokonaan.

MAC-taso on vastuussa seuraavien tehtävien suorittamisesta: datan ja signaloinnin multipleksoiminen sekä nousevan siirtotien (tilaajapäätelaitteelta verkko-osaan päin) että laskevan siirtotien (verkko-osasta tilaajapäätelaitteelle päin) yhteyksillä, nousevan siirtotien resurssipyyntöjen hallinta sekä laskevan siirtotien liikenteen resurssien jako ja ajoitus. Myös liikenteen priorisoinnin hallinta kuuluu tälle tasolle. RLC-taso huolehtii LLC-tason datan eli LLC-kehyksien välittämisestä MAC-tasolle; RLC pilkkoo LLC-kehykset RLC-datablokeiksi, jotka se välittää MAC-kerrokselle. Nousevan siirtotien suunnassa RLC rakentaa RLC-datablokeista LLC-kehyksiä, jotka se siirtää LLC-kerrokselle. Fyysinen taso toteutetaan Um-rajapinnassa radioyhteydellä, esimerkiksi GSM:n määritellyllä radiorajapinnalla. Fyysisellä tasolla suoritetaan esimerkiksi kantoaallon modulointi, lomitus ja virheenkorjaus lähetettävälle datalle, synkronointi ja lähettimen tehon säätö.

BSSGP-taso (Base Station Subsystem GPRS Protocol) kuljettaa ylempien kerrosten datan lisäksi reititykseen ja palvelun laatuun liittyvää informaatiota BSS:n ja SGSN:n välillä. Tämän informaation fyysisen kuljettamisen suorittaa FR-taso (Frame Relay). NS (Network Service) välittää BSSGP-protokollan mukaiset sanomat.

Kun nyt on kuvattu esimerkki matkapuhelinjärjestelmän rakenteesta ja siinä käytettävistä protokollapinoista, voidaan tarkastella salauksen toteuttamista GERAN:ia käyttävässä matkapuhelinjärjestelmässä. Kuviossa 4 kuvataan miten datavuo kulkee lähettävästä päästä vastaanottavaan päähän Lähettävä pää on kuvion vasemmalla puolella ja siitä on erotettu pystykatkoviivalla oikealla puolella sijaitseva vastaanottava pää. GERAN:issa salaus suoritetaan edellä kuvatussa pakettikontrolliyksikössä 180, ja tilaajapäätelaitteessa ohjausyksikössä 194. Salaus suoritetaan kuvattuihin protokollapinoihin sijoitettua toiminnallisuutta käyttäen. Tarvittava toiminnallisuus voidaan toteuttaa esimerkiksi yleiskäyttöisessä prosessorissa suoritettavana ohjelmistona, jolloin vaaditut toiminnallisuudet toteutetaan ohjelmistokomponentteina. Myös laitteistototeutus on mahdollinen, esimerkiksi ASIC:ina (Application Specific Integrated Circuit) tai erilliskomponenteista rakennettuna ohjauslogiikkana.

Salausalgoritmi 400 on universaalin matkapuhelinjärjestelmän laajakaistaista koodijakoista monikäyttömenetelmää käyttävän radioliityntäverkon UTRAN salausalgoritmi, joka tunnetaan myös nimellä f8. Salausalgoritmi on musta laatikko, jolloin sen toteutus on täsmälleen samanlainen sekä GPRS/EDGE-radioliityntäverkossa GERAN että laajakaistaista koodijakoista

monikäyttömenetelmää käyttävässä radioliityntäverkossa UTRAN. Tämä tarkoittaa käytännössä sitä, että samaa salausalgoritmin toteutusta, oli se sitten toteutettu ASIC:ina tai ohjelmistona, voidaan käyttää sekä GERAN:issa että UTRAN:issa.

UTRAN:issa on sovittu formaatti salausalgoritmin syöttöparametreille. Sovittu formaatti määrittää syöttöparametrien lukumäärän ja kunkin parametrin pituuden. UTRAN:in syöttöparametrit on määritelty edellä mainituissa 3GPP:n spesifikaatioissa. Ne ovat: salausavain, ajan mukaan muuttuva laskuriparametri, suuntaparametri (nouseva siirtotie/laskeva siirtotie) ja beareriparametri. Lisäksi tarvitaan salausmaskin 412 pituuden ilmoittava parametri, joka ei sinänsä vaikuta salausalgoritmin 400 sisäiseen toimintaan, vaan ainoastaan ilmoittaa kuinka monta tuotettua symbolia avainvirrasta otetaan salausmaskiin 412.

Salaamaton data 414 yhdistetään XOR-operaatiolla 416 salausmaskin 416 kanssa, jolloin saadaan salattu data 418.

Vastaanottopäässä salaus puretaan käyttäen samankaltaista toimintaa kuin lähetyspäässä, eli salausmaski 412 yhdistetään XOR-operaatiolla 416 vastaanotettuun salattuun dataan 418, jolloin saadaan alkuperäinen salaamaton data 414.

Lähetys- ja vastaanottopään täytyy olla synkronoituneita keskenään siinä mielessä, että tietyn datan 414 salaamiseen käytettyjä salausalgoritmin 400 parametreja 402, 404, 406, 408, 410 täytyy myös käyttää kyseistä salaamatonta 414 dataa vastaavan salatun datan 418 salauksen purkamiseen. Tämän toteuttaminen voi edellyttää lähetys- ja vastaanottopään välistä signalointia. Sitä, kuten ei myöskään datan modulointia ja kanavakoodausta, ei kuvata tässä tarkemmin, koska ne eivät ole keksinnön kannalta oleellisia, vaan alan ammattilaiselle jo ennestään tunnettuja toimenpiteitä. Keksinnön kannalta riittää todeta, että lähetyspää käsittää välineet 400, 416 salata vastaanottopäälle lähetettävä data salausalgoritmia 400 käyttäen, ja vastaanottopää käsittää vastaavasti välineet 400, 416 purkaa lähetyspäältä vastaanotetun datan salaus salausalgoritmia 400 käyttäen. Koska GERAN:in ja tilaajapäätelaitteen välinen yhteys on kaksisuuntainen voivat molemmat toimia sekä lähetys- että vastaanottopäinä. Siten GERAN ja tilaajapäätelaite käsittävät molemmat sekä salausvälineet että salauksen purkuvälineet.

GPRS/EDGE-radioliityntäverkko GERAN käsittää välineet 402, 404, 406, 408, 410 muodostaa salausalgoritmin 400 vaatimat sovitun formaatin

omaavat syöttöparametrit GPRS/EDGE-radioliityntäverkon GERAN toiminta-parametrien perusteella. Tilaajapäätelaite UE käsittää samat välineet 402, 404, 406, 408, 410. Selvyyden vuoksi kuviossa 4 sekä salausalgoritmin 400 parametreja että niiden käsittelyyn tarvittavia välineitä kuvataan samoilla viitenumeroilla 402, 404, 406, 408, 410. Käytännössä kyseiset välineet toteutetaan edullisesti ohjelmallisesti tilaajapäätelaitteen UE ohjausyksikössä 194 tai GPRS/EDGE-radioliityntäverkon GERAN pakettikontrolliyksikössä 180.

	RLC-protokolla	**MAC-protokolla**
Laskuriparametri 402: pituus 32 bittiä	- RLC-sekvenssinumero: pituus 7 tai 11 bittiä, arvoalue 0-127 tai 0-2047. - Symboli, jolla määritellään onko salattava data kakkoskerroksen signalointitason dataa vai muuta dataa: pituus 1 bitti, arvo 1. - Hyperkehysnumero: pituus 24 tai 20 bittiä.	- Laajennettu TDMA-kehysnumero: pituus 28 bittiä, arvoalue 0-(2^{28}-1) - Aikavälinumero: Pituus 3 bittiä, arvo 0-7. - Symboli, jolla määritellään onko salattava data kakkoskerroksen signalointitason dataa vai muuta dataa: pituus 1 bitti, arvo 1.
Suuntaparametri 404: pituus 1 bitti, arvo 0/1		
Beareriparametri 406: pituus 5 bittiä		
Pituusparametri 410: pituus 16 bittiä	Arvo hyötykuorman pituus, tai täyden lohkon pituus ilman radiobeareritunnistetta sekä RLC-sekvenssinumeroa	Arvo täyden lohkon pituus.
Salausavainparametri 408: pituus 128 bittiä		

Taulukko 1

Taulukossa 1 kuvataan miten GERAN:in toimintaparametreista saadaan vaaditun formaatin omaavat syöttöparametrit käyttäjätason dataa siirrettäessä. Taulukon vasemmanpuoleisimmassa sarakkeessa kuvataan UT-

RAN:in vaatimat parametrit. Keskimmäisessä sarakkeessa kuvataan vaihtoehto, jossa salaus suoritetaan RLC-protokollakerroksessa, ja oikeanpuolimmaisessa sarakkeessa kuvataan vaihtoehto, jossa salaus suoritetaan MAC-protokollakerroksessa.

UTRAN:in suuntaparametri 404 määrittää siirtosuunnan, johon salattava data siirretään. Arvo 0 merkitsee nousevaa siirtosuuntaa ja arvo 1 laskevaa siirtosuuntaa. Suuntaparametria 404 voidaan käyttää sellaisenaan myös GERAN:issa.

UTRAN:issa beareriparametri 406 määrittää käytetyn radiobeareritunnisteen. Tämä mahdollistaa sen, että saman käyttäjän käyttäessä samanaikaisesti useaa eri radiobeareria, jotka on multipleksattu samaan fyysisen kerroksen kehykseen, voidaan kuitenkin käyttää samaa salausavainta 408. Beareriparametria 406 voidaan käyttää sellaisenaan GERAN:issa.

UTRAN:issa pituusparametrilla 410 määritetään haluttu avainvirran pituus eli salausmaskin 412 pituus. Pituusparametria 410 voidaan käyttää sellaisenaan GERAN:issa. RLC-protokollaa käytettäessä sen arvo on hyötykuorman pituus, tai täyden lohkon pituus ilman radiobeareritunnistetta sekä RLC-sekvenssinumeroa. MAC-protokollaa käytettäessä sen arvo on täyden lohkon pituus, jolloin radiobeareritunniste ei sisälly tietovuohon, vaan sovitaan ennen siirron aloittamista.

UTRAN:issa salausavainparametri 408 määrittää salausavaimen. Salausavainparametria 408 voidaan käyttää sellaisenaan GERAN:issa.

UTRAN:issa laskuriparametri 410 on ajan mukaan muuttuva 32-bittinen laskuri, joka muodostetaan esimerkiksi hyperkehysnumerosta ja RLC-sekvenssinumerosta. Alkuperäisessä GSM-järjestelmässä laskuriparametrina käytetään TDMA-kehysnumeroa, joka on 22 bitin mittainen. Tämä aiheuttaa sen, että laskuriparametri saavuttaa maksimiarvonsa jo noin 3,5 tunnin salauksen jälkeen. Laskuriparametrin pyörähtäessä ympäri maski alkaa saada samoja arvoja kuin mitä se on jo saanut, ja salaus voidaan murtaa, ellei oteta käyttöön uutta salausavainta.

Laskuriparametria 410 ei voida sellaisenaan käyttää GERAN:issa, vaan sen sisältöä on muutettava pituuden pysyessä 32 bittinä. RLC-protokollaa käytettäessä laskuriparametri 410 muodostetaan RLC-sekvenssinumerosta, symbolista jolla määritellään onko salattava data kakkoskerroksen signalointitason (signalling plane) dataa vai muuta dataa, sekä hyperkehysnumerosta. Hyperkehysnumeron pituus voi olla 24 bittiä, jolloin

RLC-sekvenssinumeron pituus on 7 bittiä, tai sitten hyperkehysnumeron pituus voi olla 20 bittiä, jolloin RLC-sekvenssinumeron pituus on 11 bittiä. Yhden bitin symboli, jolla määritellään onko salattava data kakkoskerroksen signalointitason dataa vai muuta dataa, saa tässä tapauksessa arvon 1 salattavan datan ollessa muuta dataa kuin kakkoskerroksen signalointitason dataa. Käytännössä RLC-protokollaa käytettäessä laskuriparametrin teholliseksi pituudeksi tulee 31 bittiä, yhden bitin symbolin ollessa vakio.

MAC-protokollaa käytettäessä laskuriparametri 410 muodostetaan laajennetusta TDMA-kehysnumerosta, aikavälinumerosta, sekä symbolista jolla määritellään onko salattava data kakkoskerroksen signalointitason dataa vai muuta dataa. TDMA-kehysnumeron pituutta on siis laajennettu 28 bitin mittaiseksi. Yhden bitin symboli, jolla määritellään onko salattava data kakkoskerroksen signalointitason dataa vai muuta dataa, saa tässä tapauksessa arvon 1 salattavan datan ollessa muuta dataa kuin kakkoskerroksen signalointitason dataa. Aikavälinumero voi olla vakio, jos vain yhtä aikaväliä käytetään. Käytännössä MAC-protokollaa käytettäessä laskuriparametrin teholliseksi pituudeksi tulee 28 bittiä, yhden bitin symbolin ja aikavälinumeron ollessa vakioita. Tämäkin on vielä 64 kertaa enemmän kuin nykyisen GSM:n laskuriparametrin sykli ja siten käytännössä hyvin riittävä.

Laajennetulle TDMA-kehysnumerolle käytetään samaa ideaa kuin hyperkehysnumerolle. Nykyisessä GSM-järjestelmässä TDMA-kehysnumeron 11 merkitsevintä bittiä käytetään monikehyksen laskentaan. Nämä 11 bittiä muodostavat T1-laskuriosan, jota laajentamalla 16-bittiseksi saadaan laajennettu TDMA-kehysnumero. Pituudeltaan 5-bittinen T2-laskuriosa ja 6-bittinen T3-laskuriosa voidaan säilyttää laajennetussa TDMA-kehysnumerossa.

RLC-protokollaa käytettäessä salataan käyttäjän hyötykuorma, ei kuitenkaan radiobeareritunnistetta, eikä RLC-lohkon otsikkoa RLC-sekvenssinumeron perillemenon varmistamiseksi. Toinen mahdollisuus on salata käyttäjän hyötykuorma sekä lohkon otsikko, ei kuitenkaan RLC-sekvenssinumeroa eikä radiobeareritunnistetta. MAC-protokollaa käytettäessä salataan koko MAC-lohko.

Taulukossa 2 kuvataan miten GERAN:in toimintaparametreista saadaan vaaditun formaatin omaavat syöttöparametrit kakkoskerroksen signalointitason dataa siirrettäessä. Salaus on tällöin suoritettava MAC-protokollakerroksessa.

Suuntaparametria 404, pituusparametria 410 ja salausavainparametria 408 voidaan käyttää kakkoskerroksen signalointitason dataa siirrettäessä samalla tavalla kuin siirrettäessä muuta dataa.

Kakkoskerroksen signalointitason datalle ei ole olemassa radiobeareritunnistetta, siten beareriparametrille 406 annetaan jokin vakioarvo, esimerkiksi "00000". Tälle vakioarvolle voidaan määritellä myös erityinen merkitys, joka selitetään hieman myöhemmin.

	MAC-protokolla
Laskuriparametri 402: pituus 32 bittiä	Laajennettu TDMA-kehysnumero: pituus 28 bittiä, arvoalue 0-(2^{28}-1) - Aikavälinumero: Pituus 3 bittiä, arvo 0-7. - Symboli, jolla määritellään onko salattava data kakkoskerroksen signalointitason dataa vai muuta dataa: pituus 1 bitti, arvo 0.
Suuntaparametri 404: pituus 1 bitti, arvo 0/1	
Beareriparametri 406: pituus 5 bittiä	Arvo "00000"
Pituusparametri 410: pituus 16 bittiä	Arvo täyden lohkon pituus
Salausavainparametri 408: pituus 128 bittiä	

Taulukko 2

Kakkoskerroksen signalointitason datalle laskuriparametri 410 muodostetaan samalla tavalla kuin muulle datalle MAC-protokollaa käytettäessä, eli laskuriparametri 410 muodostetaan laajennetusta TDMA-kehysnumerosta, aikavälinumerosta, sekä symbolista, jolla määritellään onko salattava data kakkoskerroksen signalointitason dataa vai muuta dataa. Yhden bitin symboli, jolla määritellään onko salattava data kakkoskerroksen signa-

lointitason dataa vai muuta dataa, saa tässä tapauksessa arvon 0 salattavan datan ollessa kakkoskerroksen signalointitason dataa. Koko MAC-lohko salataan.

Tietenkin yhden bitin symbolin mahdolliset arvot voitaisiin määritellä toisinkin päin, eli arvo 1 tarkoittaisi, että salattava data on kakkoskerroksen signalointitason dataa, ja arvo 0 tarkoittaisi, että salattava data on muuta dataa.

Seuraavaksi selostetaan keksinnön vaihtoehtoisia edullisia suoritusmuotoja.

Eräässä edullisessa suoritusmuodossa yksi beareriparametrin arvoista on varattu signalointitason salattavalle datalle. Tämä on juuri yllämainittu taulukossa 2 kuvattu vakioarvo, esimerkiksi "00000". Tällä menettelyllä voidaan siis korvata symboli, jolla määritellään onko salattava data kakkoskerroksen signalointitason dataa vai muuta dataa. Arvo "00000" määrittelee, että salattava data on kakkoskerroksen signalointitason dataa, ja mikä tahansa muu arvo määrittelee käytetyn radiobeareritunnisteen. Kuten jo edellä todettiin, ei kakkoskerroksen signalointitason datalle käytetä radiobeareritunnistetta. Tämän menettelyn etuna on se, että laskuriparametrin tehollinen pituus kasvaisi yhdellä bitillä, haittana taas se, että yhdelle radiobeareritunnisteelle olisi määriteltävä erikoismerkitys.

Erässä edullisessa suoritusmuodossa käytettäessä MAC-protokollaa tallennettava tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta tallennetaan tilaajapäätelaitteeseen UE seuraavaa yhteyttä varten, yleensä käytännössä tilaajapäätelaitteen UE SIM-kortille (Subscriber Identity Module). Tässä sovelletaan UTRAN:ista tunnettua hyperkehysnumeroiden hallintaa. Jos samassa yhteydessä on käytetty useita radiobeareita, niin tallennetaan se laajennettu TDMA-kehysnumero, joka on ehtinyt saada suurimman arvon. Tällöin uutta yhteyttä aloitettaessa vain yksi arvo tarvitsee kommunikoida, ja tuota arvoa käytetään aloittamaan uuden yhteyden salaus. UTRAN:issa kyseinen arvo tunnetaan nimellä START. Edullisesti tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta käsittää tietyn määrän laajennetun TDMA-kehysnumeron merkitsevimpiä bittejä. Vastaavasti RLC-protokollaa käytettäessä tieto viimeisestä käytetystä hyperkehysnumerosta tallennetaan tilaajapäätelaitteeseen UE seuraavaa yhteyttä varten. Tallennettava tieto viimeisestä käytetystä hyperkehysnumerosta käsittää edullisesti tietyn määrän hyperkehysnumeron merkitsevimpiä bittejä. Kuvattu laajennetun

TDMA-kehysnumeron ja/tai hyperkehysnumeron tallennus seuraavaa yhteyttä varten voidaan toteuttaa myös GPRS/EDGE-radioliityntäverkossa GERAN, edullisimmin pakettikontrolliyksikössä 180. Tallennuspaikan valintaan vaikuttaa se miten kyseisen tallennetun arvon signalointi tilaajapäätelaitteen ja GPRS/EDGE-radioliityntäverkon GERAN välillä uutta yhteyttä muodostettaessa voidaan helpoimmin ja tehokkaimmin toteuttaa. Yhdellä tallennetulla START-arvolla hoidetaan sekä RLC-protokollaa että MAC-protokollaa käyttävät yhteydet samalle käyttäjälle, eli käytetyistä arvoista tallennetaan maksimi.

Eräässä edullisessa suoritusmuodossa tilaajapäätelaitteen UE yhteyden vaihtuessa GPRS/EDGE-radioliityntäverkon GERAN ja laajakaistaista koodijakoista monikäyttömenetelmää käyttävän radioliityntäverkon UTRAN välillä, tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta tai hyperkehysnumerosta ilmoitetaan uudelle radioliityntäverkolle, ja salausalgoritmin 400 salausavainsyöttöparametrina 408 uudessa radioliityntäverkossa käytetään samaa salausavainsyöttöparametria 408 kuin vanhassa radioliityntäverkossa. Tällä menettelyllä vältetään se, että samaa maskia 412 käytettäisiin erisisältöisille salaamattomille datoille 414. Ilman kyseistä menettelyä yhteyden vaihtuessa, esimerkiksi kanavanvaihdon johdosta, jouduttaisiin aina suorittamaan uuden salausavaimen käyttöönoton edellyttämä signalointi tilaajapäätelaitteen UE ja GPRS/EDGE-radioliityntäverkon GERAN välillä. Periaatteessa tämä menettely voidaan toteuttaa kahdella tavalla, joko niin että tilaajapäätelaite käsittää välineet 190, 192, 194 ilmoittaa tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta tai hyperkehysnumerosta uudelle radioliityntäverkolle tilaajapäätelaitteen UE yhteyden vaihtuessa GPRS/EDGE-radioliityntäverkon GERAN ja laajakaistaista koodijakoista monikäyttömenetelmää käyttävän radioliityntäverkon UTRAN välillä, tai GPRS/EDGE-radioliityntäverkko GERAN käsittää välineet 180 vastaanottaa tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta tai hyperkehysnumerosta tilaajapäätelaitteelle UE tilaajapäätelaitteen UE yhteyden vaihtuessa GPRS/EDGE-radioliityntäverkon GERAN ja laajakaistaista koodijakoista monikäyttömenetelmää käyttävän radioliityntäverkon UTRAN välillä.

Kuvatut menettelyt toteutetaan edullisesti siten, että tallennettava tai ilmoitettava tieto käsittää tietyn määrän merkitsevimpiä bittejä, ja ennen tiedon käyttämistä uudessa radioyhteydessä tai radioliityntäverkossa kyseisistä merkitsevimmistä biteistä muodostetun luvun arvoa kasvatetaan yhdellä. Tällöin vältytään jälleen saman salausmaskin 412 käyttämiseltä kahdesti erisi-

sältöisiin salaamattomiin tietoihin 414. Tämä toteutetaan niin, että joko tilaajapäätelaite UE tai GPRS/EDGE-radioliityntäverkko GERAN käsittää välineet 402 kasvattaa yhdellä kyseisistä merkitsevimmistä biteistä muodostetun luvun arvoa ennen tiedon käyttämistä uudessa radioyhteydessä tai uuden radioliityntäverkon yhteydessä. Esimerkiksi siirryttäessä GERAN:ista UTRAN:iin voitaisiin tallentaa 20 merkitsevintä bittiä, ja siirryttäessä UTRAN:ista GERAN:iin 17 merkitsevintä bittiä. Näin erot vähemmän merkitsevien osien välillä jäävät merkityksettömiksi, ja varmistutaan siitä, ettei samaa salausmaskia 412 käytetä kahdesti.

Seuraavaksi kuvion 3 vuokaavioon viitaten esitetään toimenpiteet, jotka suoritetaan menetelmässä siirtää dataa matkapuhelinjärjestelmän GPRS/EDGE-radioliityntäverkon GERAN ja tilaajapäätelaitteen UE välillä. Menetelmän suorittaminen aloitetaan lohkosta 300.

Lohkossa 302 salataan siirrettävä data salausalgoritmia 400 käyttäen lähetyspäässä.

Lohkossa 304 lähetetään salattu data lähetyspäästä vastaanottopäähän.

Lohkossa 306 puretaan siirretyn datan salaus salausalgoritmia 400 käyttäen vastaanottopäässä.

Lohkon 310 sijoituksella sekä lähetys- että vastaanottopäähän kuvataan sitä, että salausalgoritmina 400 käytetään universaalin matkapuhelinjärjestelmän laajakaistaista koodijakoista monikäyttömenetelmää käyttävän radioliityntäverkon UTRAN salausalgoritmia 400, jolloin salausalgoritmin 400 vaatimat sovitun formaatin omaavat syöttöparametrit 402, 404, 406, 408, 410 muodostetaan GPRS/EDGE-radioliityntäverkon GERAN toimintaparametrien perusteella.

Kuten oheisista patenttivaatimuksista käy ilmi, niin menetelmää voidaan muunnella käyttäen jo edellä kuvattuja tilaajapäätelaitteen UE ja GPRS/EDGE-radioliityntäverkon GERAN edullisia toteutusmuotoja.

Vaikka keksintöä on edellä selostettu viitaten oheisten piirustusten mukaiseen esimerkkiin, on selvää, ettei keksintö ole rajoittunut siihen, vaan sitä voidaan muunnella monin tavoin oheisten patenttivaatimusten esittämän keksinnöllisen ajatuksen puitteissa.

Patenttivaatimukset

1. Menetelmä siirtää dataa matkapuhelinjärjestelmän GPRS/EDGE-radioliityntäverkon GERAN ja tilaajapäätelaitteen välillä, käsittäen:

(302) salataan siirrettävä data salausalgoritmia käyttäen lähetyspäässä;

(304) lähetetään salattu data lähetyspäästä vastaanottopäähän;

(306) puretaan siirretyn datan salaus salausalgoritmia käyttäen vastaanottopäässä;

t u n n e t t u siitä, että (310) salausalgoritmina käytetään universaalin matkapuhelinjärjestelmän laajakaistaista koodijakoista monikäyttömenetelmää käyttävän radioliityntäverkon UTRAN salausalgoritmia, jolloin salausalgoritmin vaatimat sovitun formaatin omaavat syöttöparametrit muodostetaan GPRS/EDGE-radioliityntäverkon GERAN toimintaparametrien perusteella.

2. Patenttivaatimuksen 1 mukainen menetelmä, jossa salausalgoritmin syöttöparametreille sovittu formaatti määrittää syöttöparametrien lukumäärän ja kunkin parametrin pituuden.

3. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, jossa salausalgoritmi on musta laatikko, jolloin sen toteutus on täsmälleen samanlainen sekä GPRS/EDGE-radioliityntäverkossa GERAN että laajakaistaista koodijakoista monikäyttömenetelmää käyttävässä radioliityntäverkossa UTRAN.

4. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, jossa syöttöparametrit käsittävät laskuriparametrin.

5. Patenttivaatimuksen 4 mukainen menetelmä, jossa laskuriparametri käsittää symbolin, jolla symbolilla määritellään onko salattava data kakkoskerroksen signalointitason dataa vai muuta dataa.

6. Patenttivaatimuksen 1 mukainen menetelmä, jossa syöttöparametrit käsittävät beareriparametrin, ja yksi beareriparametrin arvoista on varattu signalointitason salattavalle datalle.

7. Patenttivaatimuksen 4 mukainen menetelmä, jossa suoritettaessa salausalgoritmi protokollapinon MAC-kerroksessa laskuriparametri käsittää laajennetun TDMA-kehysnumeron.

8. Patenttivaatimuksen 7 mukainen menetelmä, jossa laajennettu TDMA-kehysnumero pohjautuu GSM:n T1-laskuriosan laajentamiseen.

9. Patenttivaatimuksen 7 mukainen menetelmä, jossa tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta tallennetaan tilaajapäätelaitteeseen seuraavaa yhteyttä varten.

10. Patenttivaatimuksen 9 mukainen menetelmä, jossa tallennettava tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta käsittää tietyn määrän laajennetun TDMA-kehysnumeron merkitsevimpiä bittejä, ja ennen tiedon käyttämistä uudessa radioyhteydessä laajennetun TDMA-kehysnumeron muodostamiseksi kyseisistä merkitsevimmistä biteistä muodostetun luvun arvoa kasvatetaan yhdellä.

11. Patenttivaatimuksen 4 mukainen menetelmä, jossa suoritettaessa salausalgoritmi protokollapinon MAC-kerroksessa laskuriparametri käsittää aikavälinumeron.

12. Patenttivaatimuksen 4 mukainen menetelmä, jossa suoritettaessa salausalgoritmi protokollapinon RLC-kerroksessa laskuriparametri käsittää hyperkehysnumeron.

13. Patenttivaatimuksen 12 mukainen menetelmä, jossa tieto viimeisestä käytetystä hyperkehysnumerosta tallennetaan tilaajapäätelaitteeseen seuraavaa yhteyttä varten, ja ennen tiedon käyttämistä uudessa radioyhteydessä hyperkehysnumeron muodostamiseksi kyseisistä merkitsevimmistä biteistä muodostetun luvun arvoa kasvatetaan yhdellä.

14. Patenttivaatimuksen 13 mukainen menetelmä, jossa tallennettava tieto viimeisestä käytetystä hyperkehysnumerosta käsittää tietyn määrän hyperkehysnumeron merkitsevimpiä bittejä.

15. Patenttivaatimuksen 1 mukainen menetelmä, jossa tilaajapäätelaitteen yhteyden vaihtuessa GPRS/EDGE-radioliityntäverkon GERAN ja laajakaistaista koodijakoista monikäyttömenetelmää käyttävän radioliityntäverkon UTRAN välillä, tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta tai hyperkehysnumerosta ilmoitetaan uudelle radioliityntäverkolle, ja salausalgoritmin salausavainsyöttöparametrina uudessa radioliityntäverkossa käytetään samaa salausavainsyöttöparametria kuin vanhassa radioliityntäverkossa.

16. Patenttivaatimuksen 15 mukainen menetelmä, jossa ilmoitettava tieto käsittää tietyn määrän merkitsevimpiä bittejä, ja ennen tiedon käyttämistä uudessa radioliityntäverkossa kyseisistä merkitsevimmistä biteistä muodostetun luvun arvoa kasvatetaan yhdellä.

17. Matkapuhelinjärjestelmän tilaajapäätelaite (UE) käsittäen:

välineet (416) salata matkapuhelinjärjestelmän GPRS/EDGE-radioliityntäverkolle GERAN lähetettävä data salausalgoritmia (400) käyttäen

välineet (416) purkaa matkapuhelinjärjestelmän GPRS/EDGE-radioliityntäverkolta GERAN vastaanotetun datan salaus salausalgoritmia (400) käyttäen;

tunnettu siitä, että salausalgoritmi (400) on universaalin matkapuhelinjärjestelmän laajakaistaista koodijakoista monikäyttömenetelmää käyttävän radioliityntäverkon UTRAN salausalgoritmi (400), ja tilaajapäätelaite (UE) käsittää välineet (402, 404, 406, 408, 410) muodostaa salausalgoritmin (400) vaatimat sovitun formaatin omaavat syöttöparametrit GPRS/EDGE-radioliityntäverkon GERAN toimintaparametrien perusteella.

18. Patenttivaatimuksen 17 mukainen tilaajapäätelaite, jossa salausalgoritmin (400) syöttöparametreille sovittu formaatti määrittää syöttöparametrien lukumäärän ja kunkin parametrin pituuden.

19. Jonkin edellisen patenttivaatimuksen 17-18 mukainen tilaajapäätelaite, jossa salausalgoritmi (400) on musta laatikko, jolloin sen toteutus on täsmälleen samanlainen sekä GPRS/EDGE-radioliityntäverkossa GERAN että laajakaistaista koodijakoista monikäyttömenetelmää käyttävässä radioliityntäverkossa UTRAN.

20. Jonkin edellisen patenttivaatimuksen 17-19 mukainen tilaajapäätelaite, jossa syöttöparametrit käsittävät laskuriparametrin (402).

21. Patenttivaatimuksen 20 mukainen tilaajapäätelaite, jossa laskuriparametri käsittää symbolin, jolla symbolilla määritellään onko salattava data kakkoskerroksen signalointitason dataa vai muuta dataa.

22. Patenttivaatimuksen 17 mukainen tilaajapäätelaite, jossa syöttöparametrit käsittävät beareriparametrin (406), ja yksi beareriparametrin (406) arvoista on varattu signalointitason salattavalle datalle.

23. Patenttivaatimuksen 20 mukainen tilaajapäätelaite, jossa suoritettaessa salausalgoritmi (400) protokollapinon MAC-kerroksessa laskuriparametri (402) käsittää laajennetun TDMA-kehysnumeron.

24. Patenttivaatimuksen 23 mukainen tilaajapäätelaite, jossa laajennettu TDMA-kehysnumero pohjautuu GSM:n T1-laskuriosan laajentamiseen.

25. Patenttivaatimuksen 23 mukainen tilaajapäätelaite, jossa tilaajapäätelaite (UE) käsittää välineet tallentaa tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta seuraavaa yhteyttä varten.

26. Patenttivaatimuksen 25 mukainen tilaajapäätelaite, jossa tallennettava tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta käsittää tietyn määrän laajennetun TDMA-kehysnumeron merkitsevimpiä bittejä, ja tilaajapäätelaite (UE) käsittää välineet (402) kasvattaa yhdellä kyseisistä merkitsevimmistä biteistä muodostetun luvun arvoa ennen tiedon käyttämistä uudessa radioyhteydessä laajennetun TDMA-kehysnumeron muodostamiseksi.

27. Patenttivaatimuksen 20 mukainen tilaajapäätelaite, jossa suoritettaessa salausalgoritmi (400) protokollapinon MAC-kerroksessa laskuriparametri (402) käsittää aikavälinumeron.

28. Patenttivaatimuksen 20 mukainen tilaajapäätelaite, jossa suoritettaessa salausalgoritmi (400) protokollapinon RLC-kerroksessa laskuriparametri (402) käsittää hyperkehysnumeron.

29. Patenttivaatimuksen 28 mukainen tilaajapäätelaite, jossa tilaajapäätelaite (UE) käsittää välineet tallentaa tieto viimeisestä käytetystä hyperkehysnumerosta seuraavaa yhteyttä varten.

30. Patenttivaatimuksen 29 mukainen tilaajapäätelaite, jossa tallennettava tieto viimeisestä käytetystä hyperkehysnumerosta käsittää tietyn määrän hyperkehysnumeron merkitsevimpiä bittejä, ja tilaajapäätelaite (UE) käsittää välineet (402) kasvattaa yhdellä kyseisistä merkitsevimmistä biteistä muodostetun luvun arvoa ennen tiedon käyttämistä uudessa radioyhteydessä hyperkehysnumeron muodostamiseksi.

31. Patenttivaatimuksen 17 mukainen tilaajapäätelaite, jossa tilaajapäätelaite käsittää välineet (190, 192, 194) ilmoittaa tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta tai hyperkehysnumerosta uudelle radioliityntäverkolle tilaajapäätelaitteen (UE) yhteyden vaihtuessa GPRS/EDGE-radioliityntäverkon GERAN ja laajakaistaista koodijakoista monikäyttömenetelmää käyttävän radioliityntäverkon UTRAN välillä, ja käyttää salausalgoritmin (400) salausavainparametrina (408) uuden radioliityntäverkon yhteydessä samaa salausavainparametria (408) kuin vanhan radioliityntäverkon yhteydessä.

32. Patenttivaatimuksen 31 mukainen tilaajapäätelaite, jossa ilmoitettava tieto käsittää tietyn määrän merkitsevimpiä bittejä, ja tilaajapäätelaite (UE) käsittää välineet (402) kasvattaa yhdellä kyseisistä merkitsevimmistä biteistä muodostetun luvun arvoa ennen tiedon käyttämistä uuden radioliityntäverkon yhteydessä.

33. Matkapuhelinjärjestelmän GPRS/EDGE-radioliityntäverkko GERAN käsittäen:

välineet (416) salata tilaajapäätelaitteelle (UE) lähetettävä data salausalgoritmia (400) käyttäen

välineet (416) purkaa tilaajapäätelaitteelta (UE) vastaanotetun datan salaus salausalgoritmia (400) käyttäen;

t u n n e t t u siitä, että salausalgoritmi (400) on universaalin matkapuhelinjärjestelmän laajakaistaista koodijakoista monikäyttömenetelmää käyttävän radioliityntäverkon UTRAN salausalgoritmi (400), ja GPRS/EDGE-radioliityntäverkko GERAN käsittää välineet (402, 404, 406, 408, 410) muodostaa salausalgoritmin (400) vaatimat sovitun formaatin omaavat syöttöparametrit GPRS/EDGE-radioliityntäverkon GERAN toimintaparametrien perusteella.

34. Patenttivaatimuksen 33 mukainen GPRS/EDGE-radioliityntäverkko, jossa salausalgoritmin (400) syöttöparametreille sovittu formaatti määrittää syöttöparametrien lukumäärän ja kunkin parametrin pituuden.

35. Jonkin edellisen patenttivaatimuksen 33-34 mukainen GPRS/EDGE-radioliityntäverkko, jossa salausalgoritmi (400) on musta laatikko, jolloin sen toteutus on täsmälleen samanlainen sekä GPRS/EDGE-radioliityntäverkossa GERAN että laajakaistaista koodijakoista monikäyttömenetelmää käyttävässä radioliityntäverkossa UTRAN.

36. Jonkin edellisen patenttivaatimuksen 33-35 mukainen GPRS/EDGE-radioliityntäverkko, jossa syöttöparametrit käsittävät laskuriparametrin (402).

37. Patenttivaatimuksen 36 mukainen GPRS/EDGE-radioliityntäverkko, jossa laskuriparametri (402) käsittää symbolin, jolla symbolilla määritellään onko salattava data kakkoskerroksen signalointitason dataa vai muuta dataa.

38. Patenttivaatimuksen 37 mukainen GPRS/EDGE-radioliityntäverkko, jossa syöttöparametrit käsittävät beareriparametrin (406), ja yksi beareriparametrin (406) arvoista on varattu signalointitason salattavalle datalle.

39. Patenttivaatimuksen 36 mukainen GPRS/EDGE-radioliityntäverkko, jossa suoritettaessa salausalgoritmi (400) protokollapinon MAC-kerroksessa laskuriparametri (402) käsittää laajennetun TDMA-kehysnumeron.

40. Patenttivaatimuksen 39 mukainen GPRS/EDGE-radioliityntäverkko, jossa laajennettu TDMA-kehysnumero pohjautuu GSM:n T1-laskuriosan laajentamiseen.

41. Patenttivaatimuksen 39 mukainen GPRS/EDGE-radioliityntäverkko, jossa GPRS/EDGE-radioliityntäverkko GERAN käsittää välineet tallentaa tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta seuraavaa yhteyttä varten.

42. Patenttivaatimuksen 41 mukainen GPRS/EDGE-radioliityntäverkko tilaajapäätelaite, jossa tallennettava tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta käsittää tietyn määrän laajennetun TDMA-kehysnumeron merkitsevimpiä bittejä, ja GRPS/EDGE-radioliityntäverkko GERAN käsittää välineet (402) kasvattaa yhdellä kyseisistä merkitsevimmistä biteistä muodostetun luvun arvoa ennen tiedon käyttämistä laajennetun TDMA-kehysnumeron muodostamiseksi.

43. Patenttivaatimuksen 36 mukainen GPRS/EDGE-radioliityntäverkko, jossa suoritettaessa salausalgoritmi (400) protokollapinon MAC-kerroksessa laskuriparametri (402) käsittää aikavälinumeron.

44. Patenttivaatimuksen 36 mukainen GPRS/EDGE-radioliityntäverkko, jossa suoritettaessa salausalgoritmi (400) protokollapinon RLC-kerroksessa laskuriparametri (402) käsittää hyperkehysnumeron.

45. Patenttivaatimuksen 44 mukainen GPRS/EDGE-radioliityntäverkko, jossa GPRS/EDGE-radioliityntäverkko GERAN käsittää välineet tallentaa tieto viimeisestä käytetystä hyperkehysnumerosta seuraavaa yhteyttä varten.

46. Patenttivaatimuksen 45 mukainen GPRS/EDGE-radioliityntäverkko, jossa tallennettava tieto viimeisestä käytetystä hyperkehysnumerosta käsittää tietyn määrän hyperkehysnumeron merkitsevimpiä bittejä, ja GRPS/EDGE-radioliityntäverkko GERAN käsittää välineet (402) kasvattaa yhdellä kyseisistä merkitsevimmistä biteistä muodostetun luvun arvoa ennen tiedon käyttämistä hyperkehysnumeron muodostamiseksi.

47. Patenttivaatimuksen 33 mukainen GPRS/EDGE-radioliityntäverkko, jossa GPRS/EDGE-radioliityntäverkko GERAN käsittää välineet (180) vastaanottaa tieto viimeisestä käytetystä laajennetusta TDMA-kehysnumerosta tai hyperkehysnumerosta tilaajapäätelaitteelle (UE) tilaajapäätelaitteen (UE) yhteyden vaihtuessa GPRS/EDGE-radioliityntäverkon GERAN ja laajakaistaista koodijakoista monikäyttömenetelmää käyttävän radioliityntäverkon

UTRAN välillä, ja käyttää salausalgoritmin (400) salausavainparametrina (408) vastaanotetun tiedon mukaista salausavainparametria (408).

48. Patenttivaatimuksen 47 mukainen GPRS/EDGE-radioliityntäverkko, jossa ilmoitettava tieto käsittää tietyn määrän merkitsevimpiä bittejä, ja GRPS/EDGE-radioliityntäverkko GERAN käsittää välineet (402) kasvattaa yhdellä kyseisistä merkitsevimmistä biteistä muodostetun luvun arvoa ennen tiedon käyttämistä.

Patentkrav

1. Förfarande för överföring av data mellan ett GRPS/EDGE-radioaccessnät GERAN och en abonnentterminal i ett mobilsystem, omfattande:

(302) kryptering av data som sänds genom att använda en krypteringsalgoritm i sändarändan;

(304) sändning av krypterad data från sändar- till mottagarändan;

(306) dekryptering av sänd data genom att använda en krypteringsalgoritm i mottagarändan;

k ä n n e t e c k n a t av att (310) som krypteringsalgoritm används en krypteringsalgoritm för radioaccessnätet UTRAN som använder det universala mobiltelekommunikationssystemets bredbandiga CDMA-teknik, varvid de av krypteringsalgoritmen erfordrade inmatningsparametrarna av ett överenskommet format bildas på basis av funktionsparametrarna för GRPS/EDGE-radioaccessnätet GERAN.

2. Förfarande enligt patentkrav 1, där det överenskomna formatet för krypteringsalgoritmens inmatningsparametrar bestämmer antalet inmatningsparametrar och respektive parameters längd.

3. Förfarande enligt något av de föregående patentkraven, där krypteringsalgoritmen är en svart låda, varvid dess implementering är exakt den samma både i GRPS/EDGE-radioaccessnätet GERAN och i radioaccessnätet UTRAN som använder bredbandig CDMA-teknik.

4. Förfarande enligt något av de föregående patentkraven, där inmatningsparametrarna omfattar en räknarparameter.

5. Förfarande enligt patentkrav 4, där räknarparametern omfattar en symbol som bestämmer huruvida data som krypteras är data av det andra skiktets signaleringsplan eller annan data.

6. Förfarande enligt patentkrav 1, där inmatningsparametrarna omfattar en bärarparameter och ett av bärarparametervärdena reserverats för signaleringsplanets data som skall krypteras.

7. Förfarande enligt patentkrav 4, där räknarparametern omfattar ett utvidgat TDMA-ramnummer vid genomförande av krypteringsalgoritmen i MAC-skiktet i en protokollstack.

8. Förfarande enligt patentkrav 7, där det utvidgade TDMA-ramnumret baserar sig på utvidgning av T1-räknardelen i GSM.

9. Förfarande enligt patentkrav 7, där information om det senast använda utvidgade TDMA-ramnumret lagras i abonnentterminalen för nästa för-

bindelse.

10. Förfarande enligt patentkrav 9, där informationen om det senast använda utvidgade TDMA-ramnumret vilken lagras omfattar ett bestämt antal av de mest betydelsefulla bitarna av det utvidgade TDMA-ramnumret och innan informationen används i en ny radioförbindelse för att bilda ett utvidgat TDMA-ramnummer ökas värdet på talet som bildats av nämnda mest betydelsefulla bitar med ett.

11. Förfarande enligt patentkrav 4, där räknarparametern omfattar ett tidsluckenummer vid genomförande av krypteringsalgoritmen i MAC-skiktet i en protokollstack.

12. Förfarande enligt patentkrav 4, där räknarparametern omfattar ett hyperramnummer vid genomförande av krypteringsalgoritmen i RLC-skiktet i en protokollstack.

13. Förfarande enligt patentkrav 12, där information om det senast använda hyperramnumret lagras i abonnentterminalen för nästa förbindelse och innan informationen används i en ny radioförbindelse för att bilda ett hyperramnummer ökas värdet på talet som bildats av nämnda mest betydelsefulla bitar med ett.

14. Förfarande enligt patentkrav 13, där informationen om det senast använda hyperramnumret vilken lagras omfattar ett bestämt antal av de mest betydelsefulla bitarna av hyperramnumret.

15. Förfarande enligt patentkrav 1, där information om det senast använda utvidgade TDMA-ramnumret eller hyperramnumret meddelas till det nya radioaccessnätet, då abonnentterminalens förbindelse växlar mellan GRPS/EDGE-radioaccessnätet GERAN och radioaccessnätet UTRAN som använder bredbandig CDMA-teknik, och samma krypteringsnyckelinmatningsparameter som i det gamla radioaccessnätet används som krypteringsnyckelinmatningsparameter för krypteringsnyckeln i det nya radioaccessnätet.

16. Förfarande enligt patentkrav 15, där informationen som meddelas omfattar ett bestämt antal mest betydelsefulla bitar och innan informationen används i en ny radioförbindelse ökas värdet på talet som bildats av nämnda mest betydelsefulla bitar med ett.

17. Abonnentterminal (UE) i ett mobilsystem, omfattande:

medel (416) för kryptering av data som sänds till ett mobilsystems GRPS/EDGE-radioaccessnät GERAN genom att använda en krypteringsalgoritm (400),

medel (416) för dekryptering av data som mottagits från mobilsystemets GRPS/EDGE-radioaccessnät GERAN genom att använda en krypteringsalgoritm (400);

kännetecknad av att krypteringsalgoritmen (400) är en krypteringsalgoritm för radioaccessnätet UTRAN som använder det universala mobiltelekommunikationssystemets bredbandiga CDMA-teknik, och abonnentterminalen (UE) omfattar medel (402, 404, 406, 408, 410) att bilda de av krypteringsalgoritmen (400) erfordrade inmatningsparametrarna av ett överenskommet format bildas på basis av funktionsparametrarna för GRPS/EDGE-radioaccessnätet GERAN.

18. Abonnentterminal enligt patentkrav 17, där det överenskomna formatet för krypteringsalgoritmens (400) inmatningsparametrar bestämmer antalet inmatningsparametrar och respektive parameters längd.

19. Abonnentterminal enligt något av de föregående patentkraven 17-18, där krypteringsalgoritmen (400) är en svart låda, varvid dess implementering är exakt den samma både i GRPS/EDGE-radioaccessnätet GERAN och i radioaccessnätet UTRAN som använder bredbandig CDMA-teknik.

20. Abonnentterminal enligt något av de föregående patentkraven 17-19, där inmatningsparametrarna omfattar en räknarparameter (402).

21. Abonnentterminal enligt patentkrav 20, där räknarparametern omfattar en symbol som bestämmer huruvida data som krypteras är data av det andra skiktets signaleringsplan eller annan data.

22. Abonnentterminal enligt patentkrav 17, där inmatningsparametrarna omfattar en bärarparameter (406) och ett av bärarparameterns (406) värden reserverats för signaleringsplanets data som skall krypteras.

23. Abonnentterminal enligt patentkrav 20, där räknarparametern (402) omfattar ett utvidgat TDMA-ramnummer vid genomförande av krypteringsalgoritmen (400) i MAC-skiktet i en protokollstack.

24. Abonnentterminal enligt patentkrav 23, där det utvidgade TDMA-ramnumret baserar sig på utvidgning av T1-räknardelen i GSM.

25. Abonnentterminal enligt patentkrav 23, där abonnentterminalen (UE) omfattar medel att lagra information om det senast använda utvidgade TDMA-ramnumret för nästa förbindelse.

26. Abonnentterminal enligt patentkrav 25, där informationen om det senast använda utvidgade TDMA-ramnumret vilken lagras omfattar ett bestämt antal av de mest betydelsefulla bitarna av det utvidgade TDMA-ramnumret och

abonnentterminalen (UE) omfattar medel (402) att öka värdet på talet som bildats av nämnda mest betydelsefulla bitar med ett innan informationen används i en ny radioförbindelse för att bilda ett utvidgat TDMA-ramnummer.

27. Abonnentterminal enligt patentkrav 20, där räknarparametern (402) omfattar ett tidsluckenummer vid genomförande av krypteringsalgoritmen (400) i MAC-skiktet i en protokollstack.

28. Abonnentterminal enligt patentkrav 20, där räknarparametern (402) omfattar ett hyperramnummer vid genomförande av krypteringsalgoritmen (400) i RLC-skiktet i en protokollstack.

29. Abonnentterminal enligt patentkrav 28, där abonnentterminalen (UE) omfattar medel att lagra information om det senast använda hyperramnumret för nästa förbindelse.

30. Abonnentterminal enligt patentkrav 29, där informationen om det senast använda hyperramnumret vilken lagras omfattar ett bestämt antal av de mest betydelsefulla bitarna av hyperramnumret och (UE) omfattar medel (402) att öka värdet på talet som bildats av nämnda mest betydelsefulla bitar med ett innan informationen används i en ny radioförbindelse för att bilda ett hyperramnummer.

31. Abonnentterminal enligt patentkrav 17, där abonnentterminalen (UE) omfattar medel (190, 192, 194) att meddela information om det senast använda utvidgade TDMA-ramnumret eller hyperramnumret till det nya radioaccessnätet, då abonnentterminalens (UE) förbindelse växlar mellan GRPS/EDGE-radioaccessnätet GERAN och radioaccessnätet UTRAN som använder bredbandig CDMA-teknik, och som krypteringsnyckelparameter (408) för krypteringsalgoritmen (400) använda samma krypteringsnyckelparameter (408) i samband med det nya radioaccessnätet som i det gamla radioaccessnätet.

32. Abonnentterminal enligt patentkrav 31, där informationen som meddelas omfattar ett bestämt antal mest betydelsefulla bitar och abonnentterminalen (UE) omfattar medel (402) att öka värdet på talet som bildats av nämnda mest betydelsefulla bitar med ett innan informationen används i samband med en ny radioförbindelse.

33. GRPS/EDGE-radioaccessnät GERAN i ett mobilsystem, omfattande:

medel (416) för kryptering av data som sänds till en abonnentterminal (UE) genom att använda en krypteringsalgoritm (400),

medel (416) för dekryptering av data som mottagits från en abonnentterminal (UE) genom att använda en krypteringsalgoritm (400);

kännetecknat av att krypteringsalgoritmen (400) är en krypteringsalgoritm (400) för radioaccessnätet UTRAN som använder det universala mobiltelekommunikationssystemets bredbandiga CDMA-teknik, och GRPS/EDGE-radioaccessnätet GERAN omfattar medel (402, 404, 406, 408, 410) att bilda de av krypteringsalgoritmen (400) erfordrade inmatningsparametrarna av ett överenskommet format på basis av funktionsparametrarna för GRPS/EDGE-radioaccessnätet GERAN.

34. GRPS/EDGE-radioaccessnät enligt patentkrav 33, där det överenskomna formatet för krypteringsalgoritmens (400) inmatningsparametrar bestämmer antalet inmatningsparametrar och respektive parameters längd.

35. GRPS/EDGE-radioaccessnät enligt något av de föregående patentkraven 33-34, där krypteringsalgoritmen (400) är en svart låda, varvid dess implementering är exakt den samma både i GRPS/EDGE-radioaccessnätet GERAN och i radioaccessnätet UTRAN som använder bredbandig CDMA-teknik.

36. GRPS/EDGE-radioaccessnät enligt något av de föregående patentkraven 33-35, där inmatningsparametrarna omfattar en räknarparameter (402).

37. GRPS/EDGE-radioaccessnät enligt patentkrav 36, där räknarparametern (402) omfattar en symbol som bestämmer huruvida data som krypteras är data av det andra skiktets signaleringsplan eller annan data.

38. GRPS/EDGE-radioaccessnät enligt patentkrav 37, där inmatningsparametrarna omfattar en bärarparameter (406) och ett av bärarparameterns (406) värden reserverats för signaleringsplanets data som skall krypteras.

39. GRPS/EDGE-radioaccessnät enligt patentkrav 36, där räknarparametern (402) omfattar ett utvidgat TDMA-ramnummer vid genomförande av krypteringsalgoritmen (400) i MAC-skiktet i en protokollstack.

40. GRPS/EDGE-radioaccessnät enligt patentkrav 39, där det utvidgade TDMA-ramnumret baserar sig på utvidgning av T1-räknardelen i GSM.

41. GRPS/EDGE-radioaccessnät enligt patentkrav 39, där GRPS/EDGE-radioaccessnätet GERAN omfattar medel att lagra information om det senast använda utvidgade TDMA-ramnumret för nästa förbindelse.

42. GRPS/EDGE-radioaccessnät enligt patentkrav 41, där informationen om det senast använda utvidgade TDMA-ramnumret vilken lagras omfattar ett bestämt antal av de mest betydelsefulla bitarna av det utvidgade TDMA-ramnumret och GRPS/EDGE-radioaccessnätet GERAN omfattar medel (402) att öka värdet på talet som bildats av nämnda mest betydelsefulla bitar med ett innan informationen används för att bilda ett utvidgat TDMA-ramnummer.

43. GRPS/EDGE-radioaccessnät enligt patentkrav 36, där räknarparametern (402) omfattar ett tidsluckenummer vid genomförande av krypteringsalgoritmen (400) i MAC-skiktet i en protokollstack.

44. GRPS/EDGE-radioaccessnät enligt patentkrav 36, där räknarparametern (402) omfattar ett hyperramnummer vid genomförande av krypteringsalgoritmen (400) i RLC-skiktet i en protokollstack.

45. GRPS/EDGE-radioaccessnät enligt patentkrav 44, där GRPS/EDGE-radioaccessnätet GERAN omfattar medel att lagra information om det senast använda hyperramnumret för nästa förbindelse.

46. GRPS/EDGE-radioaccessnät enligt patentkrav 45, där informationen om det senast använda hyperramnumret vilken lagras omfattar ett bestämt antal av de mest betydelsefulla bitarna av hyperramnumret och GRPS/EDGE-radioaccessnätet GERAN omfattar medel (402) att öka värdet på talet som bildats av nämnda mest betydelsefulla bitar med ett innan informationen används för att bilda ett hyperramnummer.

47. GRPS/EDGE-radioaccessnät enligt patentkrav 33, där GRPS/EDGE-radioaccessnätet GERAN omfattar medel (180) att motta information om det senast använda utvidgade TDMA-ramnumret eller hyperramnumret till abonnentterminalen (UE), då abonnentterminalens (UE) förbindelse växlar mellan GRPS/EDGE-radioaccessnätet GERAN och radioaccessnätet UTRAN som använder bredbandig CDMA-teknik, och som krypteringsnyckelparameter (408) för krypteringsalgoritmen (400) använda krypteringsnyckelparametern (408) enligt mottagen information.

48. GRPS/EDGE-radioaccessnät enligt patentkrav 47, där informationen som meddelas omfattar ett bestämt antal mest betydelsefulla bitar och GRPS/EDGE-radioaccessnätet GERAN omfattar medel (402) att öka värdet på talet som bildats av nämnda mest betydelsefulla bitar med ett innan informationen används.

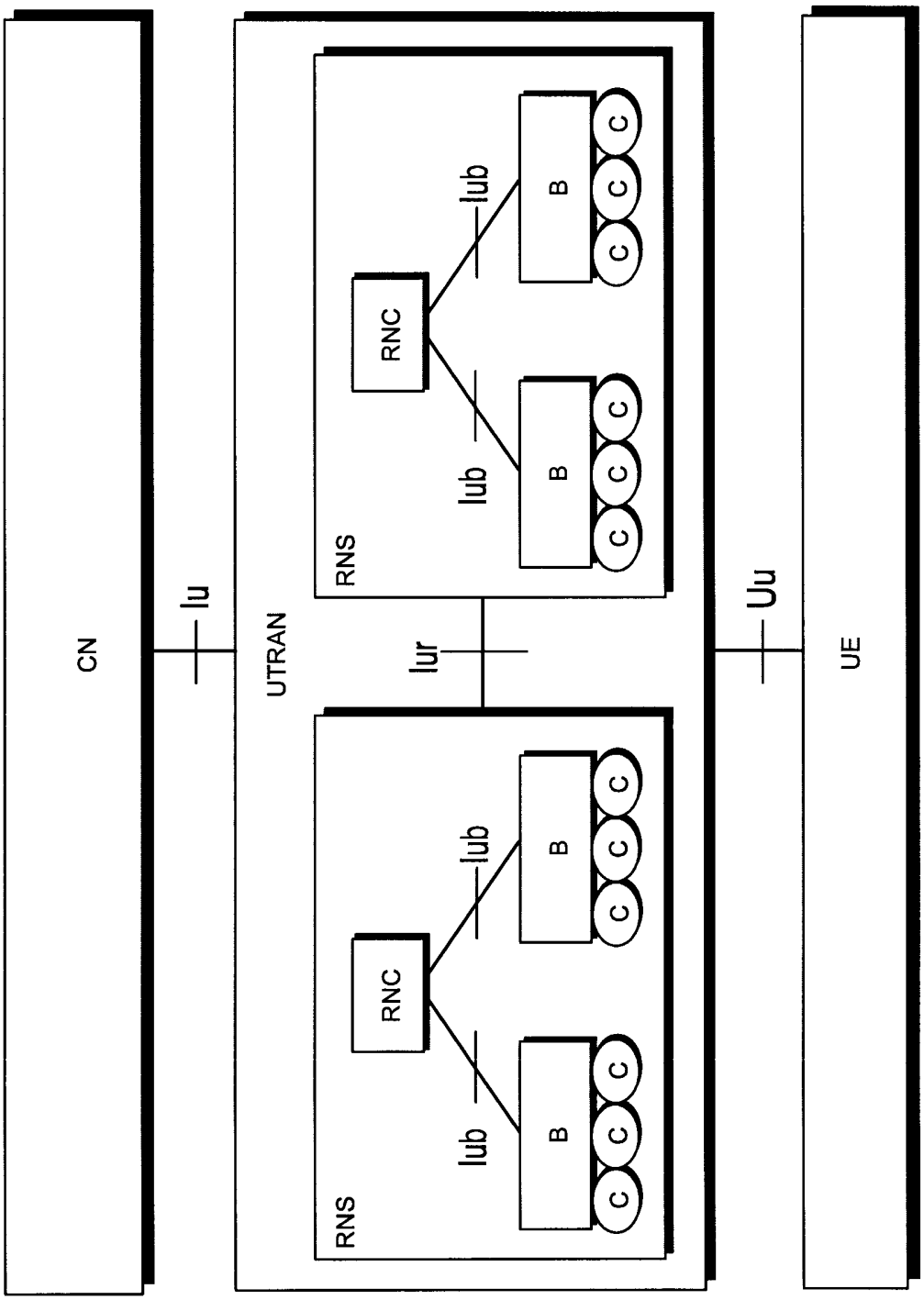


Fig 1A

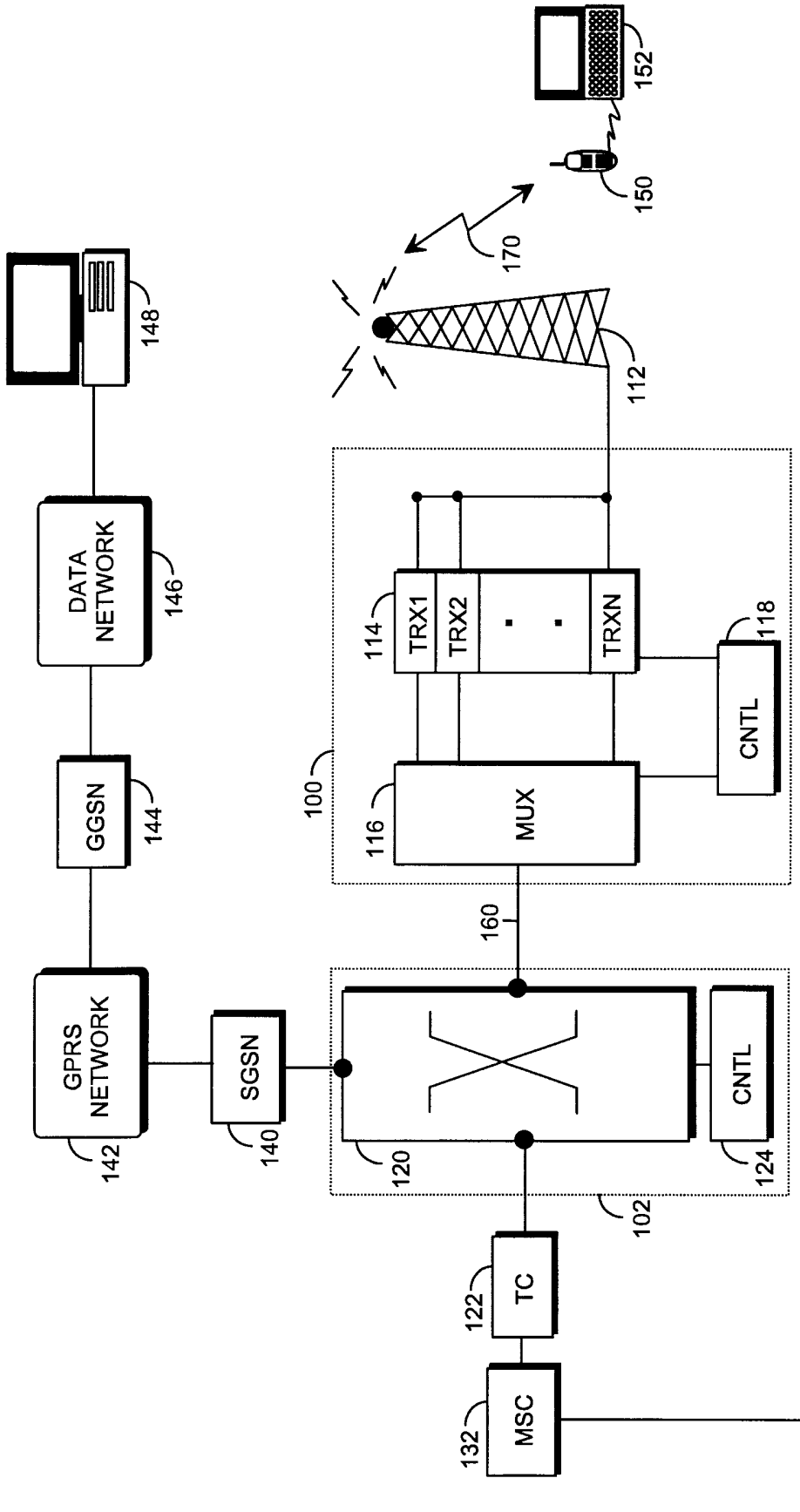

152
150
170
112
148
DATA NETWORK
146
114
TRX1
TRX2
TRXN
118
CNTL
100
116
MUX
GGSN
144
160
GPRS NETWORK
142
SGSN
140
120
CNTL
124
102
136
122
TC
132
MSC
PSTN
134

Fig 1B

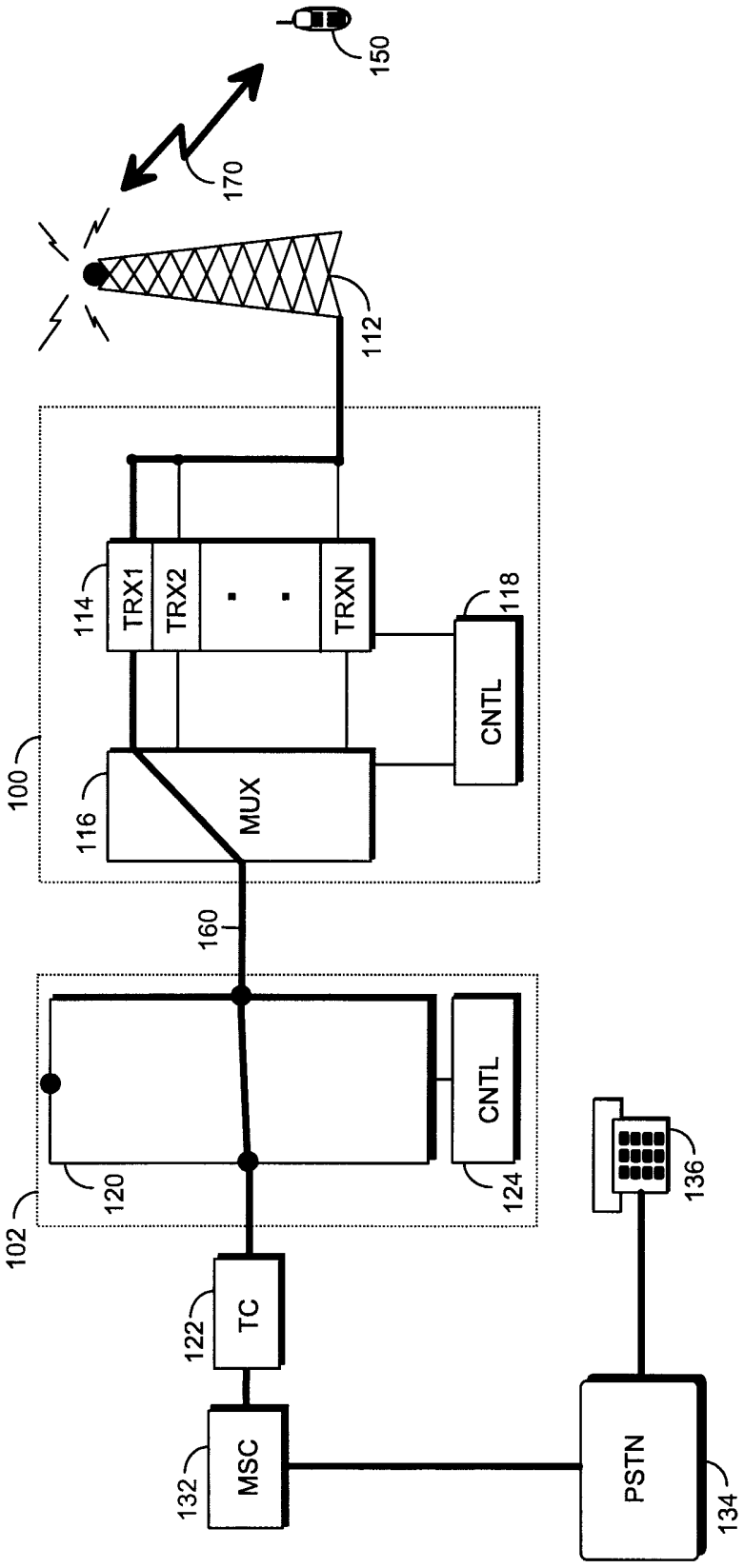

150
170
112
114
TRX1
TRX2
TRXN
118
CNTL
100
116
MUX
160
120
CNTL
124
102
136
122
TC
132
MSC
PSTN
134

Fig 1C

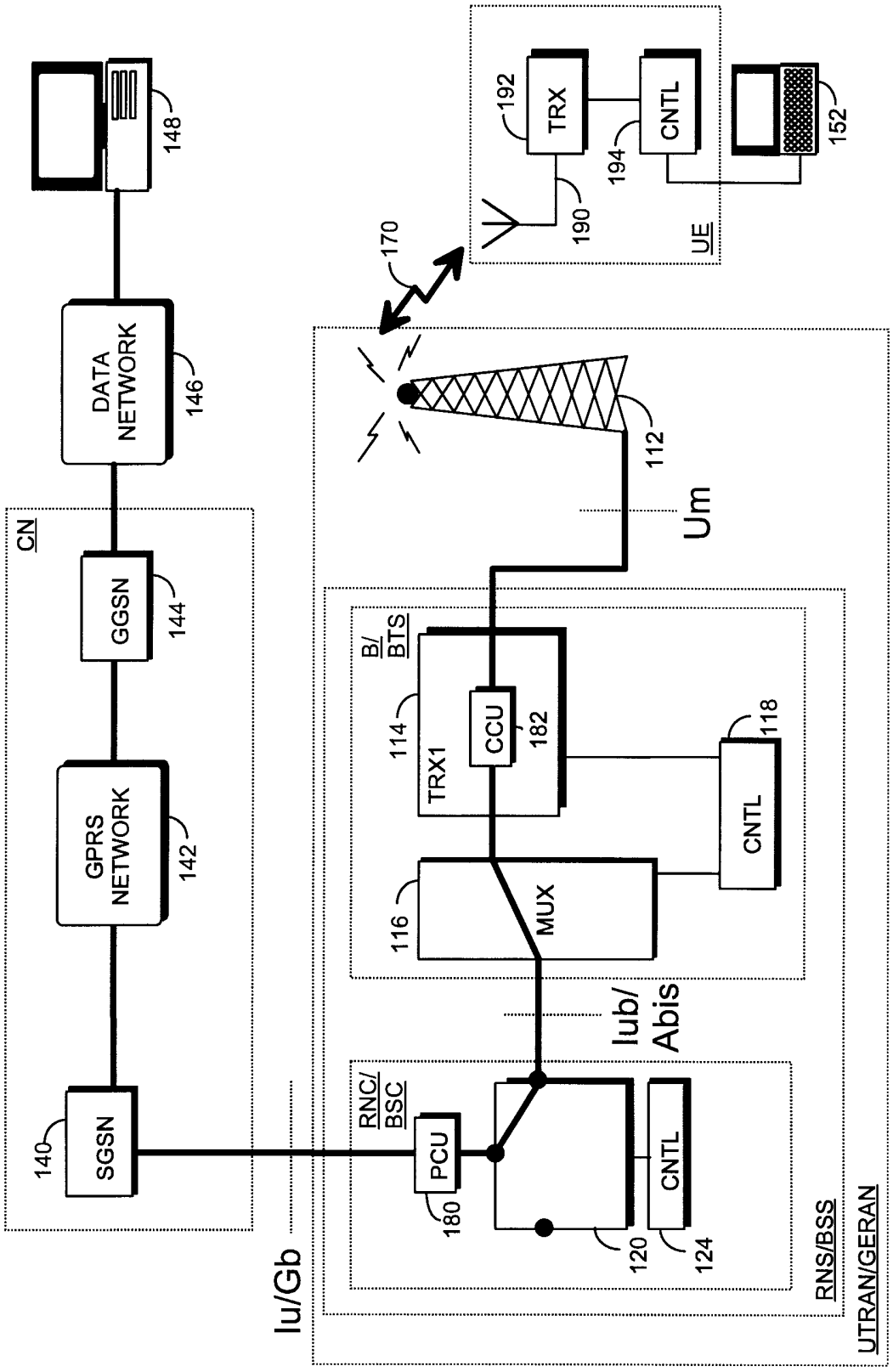

148
DATA NETWORK
146
GGSN
144
GPRS NETWORK
142
SGSN
140
CN
Iu/Gb
170
192
TRX
194
CNTL
190
UE
152
112
Um
B/ BTS
114
TRX1
CCU
182
118
CNTL
116
MUX
Iub/ Abis
RNC/ BSC
PCU
180
CNTL
120
124
RNS/BSS
UTRAN/GERAN

Fig 1D

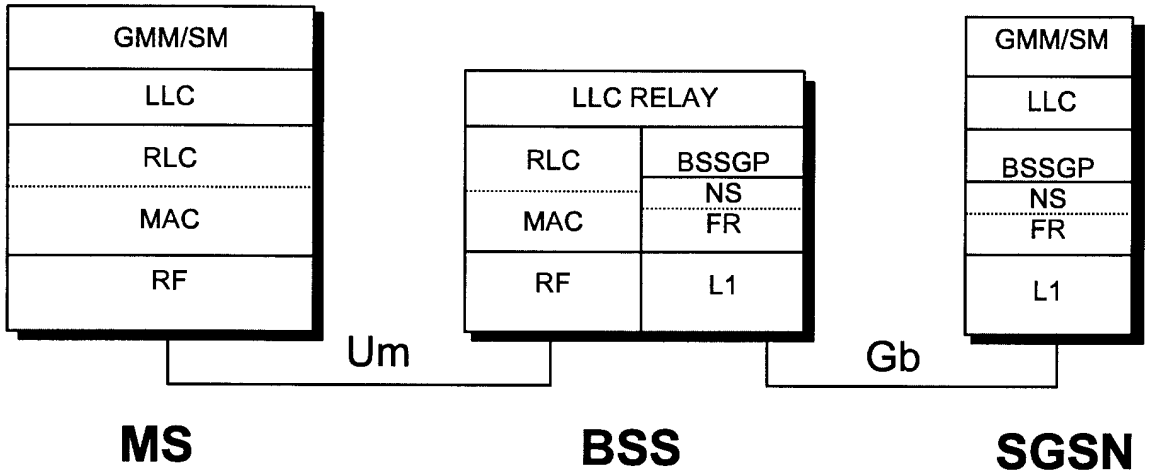
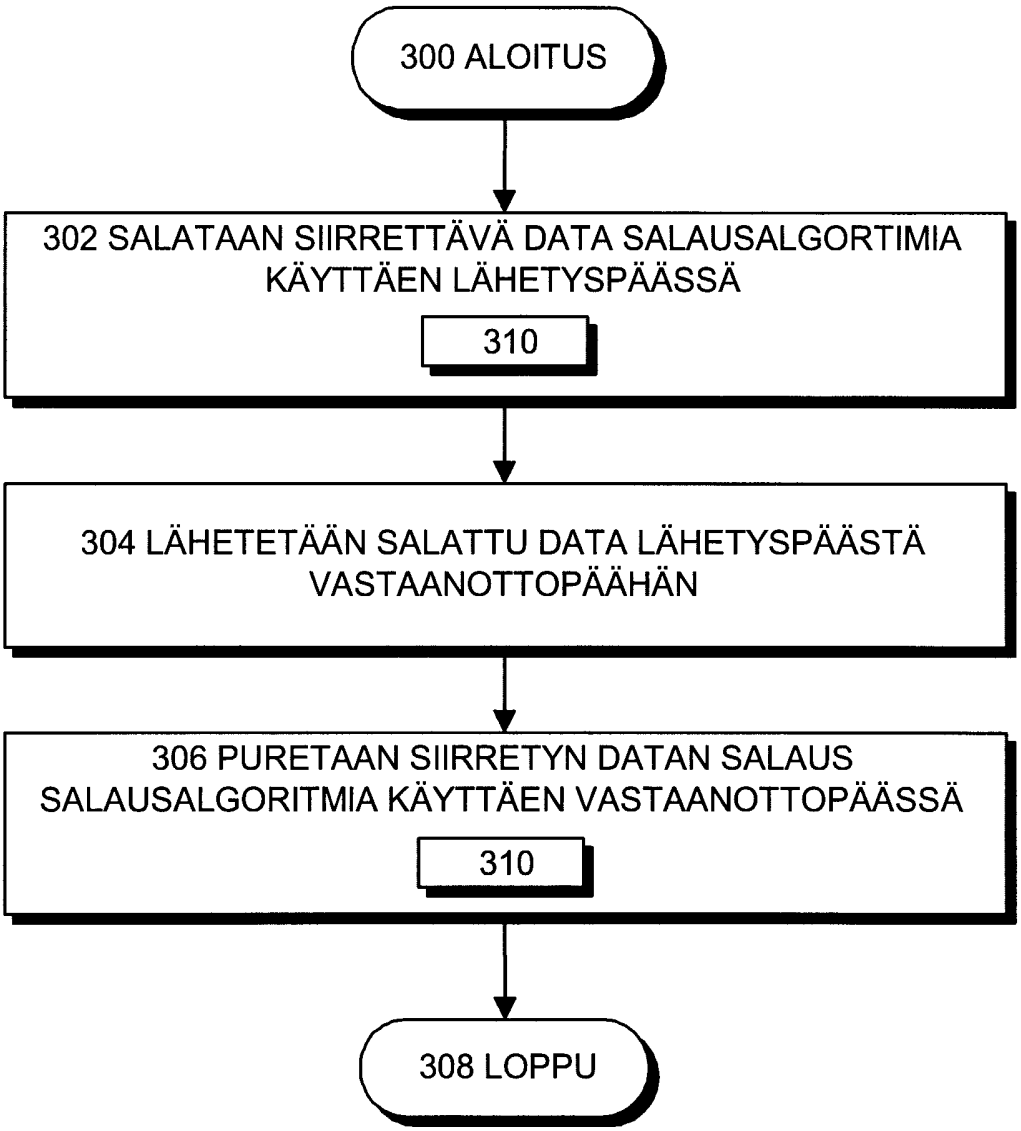

GMM/SM
LLC
RLC
MAC
RF
LLC RELAY
RLC
BSSGP
NS
MAC
FR
RF
L1
GMM/SM
LLC
BSSGP
NS
FR
L1
Um
Gb
MS
BSS
SGSN

Fig 2



310 SALAUSALGORITMINA KÄYTETÄÄN UTRAN:IN SALAUSALGORITMIA, JOLLOIN SOVITUN FORMAATIN OMAAVAT SYÖTTÖPARAMETRIT MUODOSTETAAN GERAN:IN TOIMINTAPARAMETRIEN PERUSTEELLA

Fig 3

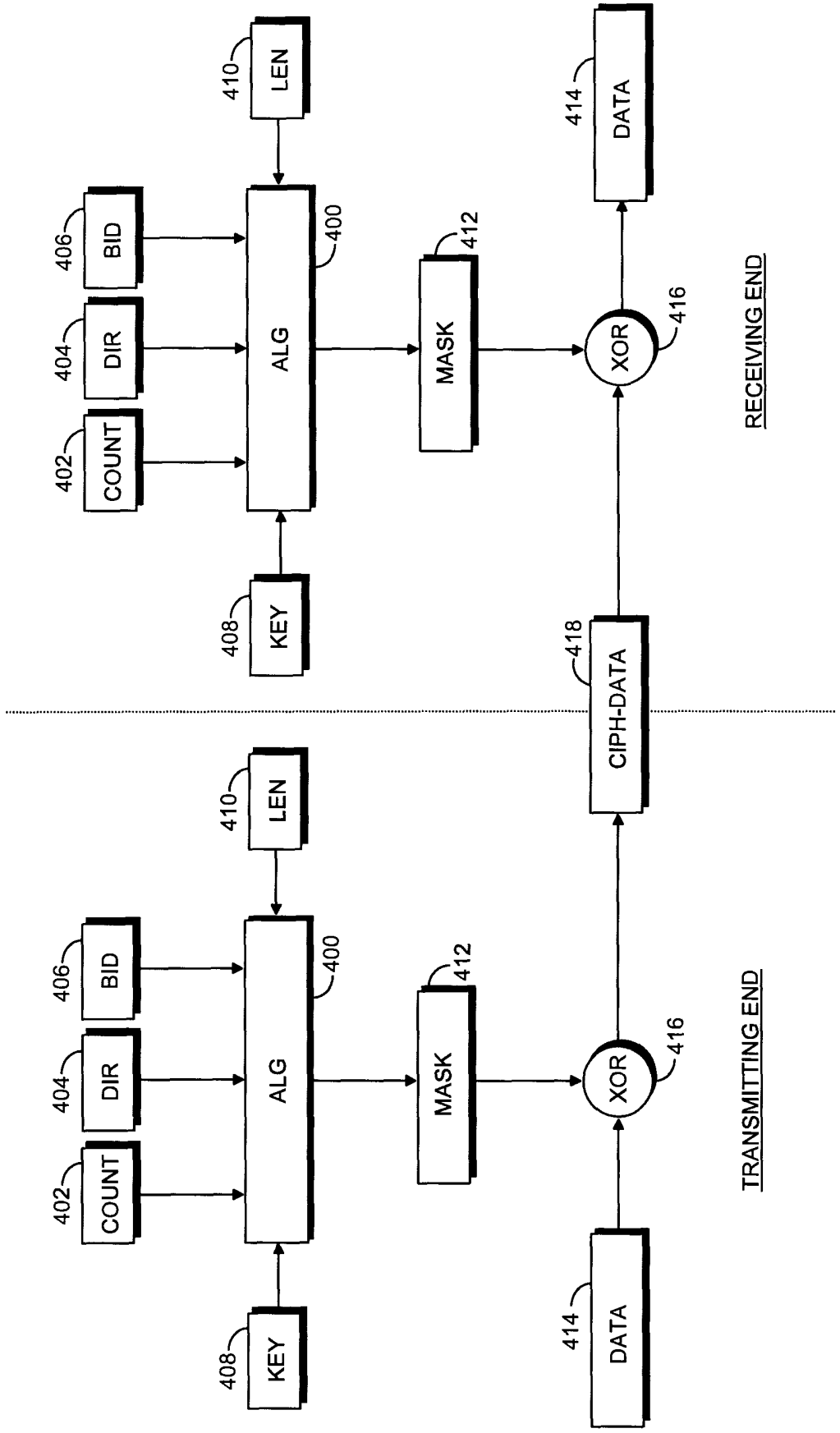

TRANSMITTING END
RECEIVING END
COUNT
DIR
BID
KEY
LEN
ALG
MASK
XOR
DATA
CIPH-DATA
402
404
406
408
410
412
414
416
418
400

Fig 4