FI000111423B

(12) **PATENTTIJULKAISU**
PATENTSKRIFT

(10) **FI 111423 B**

(45) Patentti myönnetty - Patent beviljats **15.07.2003**

(51) Kv.lk.7 - Int.kl.7

H04L 9/12, 9/36, 9/32, H04Q 7/38

(21) Patenttihakemus - Patentansökning **20010282**

(22) Hakemispäivä - Ansökningsdag **14.02.2001**

(24) Alkupäivä - Löpdag **14.02.2001**

(41) Tullut julkiseksi - Blivit offentlig **29.05.2002**

(32) (33) (31) Etuoikeus - Prioritet

28.11.2000 FI 20002613 P

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 •Vialén,Jukka, Haltiantie 3 C, 02300 Espoo, SUOMI - FINLAND, (FI)
2 •Niemi,Valtteri, Tallberginkatu 3 as. 43, 00180 Helsinki, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud: Page White & Farrer Services, Suomen sivuliike
Runeberginkatu 5, 10 krs, 00100 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning

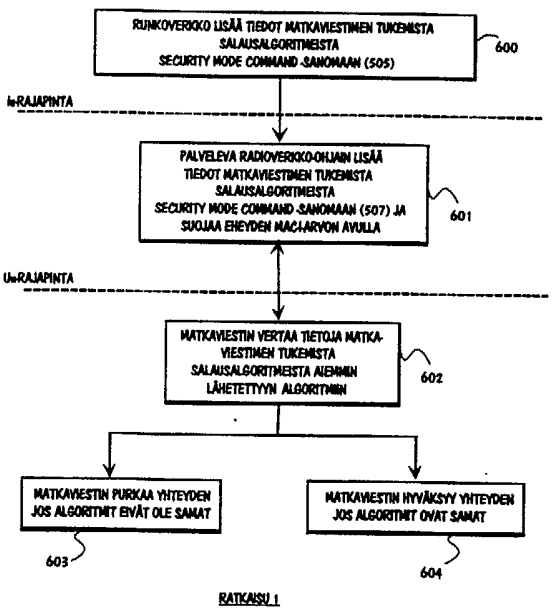
Järjestelmä kanavanvaihdon jälkeen tapahtuvan tietoliikenteen salauksen varmistamiseksi
Arrangemang för säkrande av enkryptad datakommunikation efter kanalbyte

(56) Viitejulkaisut - Anförda publikationer

WO A 0096206 (H04Q 7/38, H04L 9/32),
3G TS 33.102, v3.2.0, 3rd Generation Partnership Project (erityisesti kappaleet 6.4 ja 6.6), ftp://ftp.3gpp.org/specs/archive/33_series/33.102/33102-320.zip,
3G TS 35.201, v4.0.0, 3rd Generation Partnership Project, ftp://ftp.3gpp.org/specs/archive/35_series/35.201/35.201-400.zip

(57) Tiivistelmä - Sammandrag

Vilpillinen tunkeilija voi salakuunnella puhelua poistamalla salausalgoritmeihin liittyviä tietoja, kun monimuotomatkaviestin lähettää suojaamattoman merkinannon aloitussanoman, joka sisältää tällaisia tietoja, ilmarajapintaa pitkin matkaviestinjärjestelmään. Tällaiset yritykset voidaan estää maailmanlaajuisessa matkaviestinjärjestelmässä (UMTS-järjestelmässä), joka koostuu vähintään kahdesta radioliityntäverkosta, jotka tarjoavat matkaviestimille yhteyden vähintään yhteen ydinverkkoon, monimuotomatkaviestimestä ja vähintään yhdestä ydinverkosta. Kun yhteyttä avataan ensimmäiseen radioliityntäverkkoon, monimuotomatkaviestin lähettää suojaamattoman merkinannon aloitussanoman, joka sisältää tiedot niistä salausalgoritmeista, joita monimuotomatkaviestin tukee, kun se kommunikoi toisessa radioliityntäverkossa. Ensimmäinen radioliityntäverkko tallentaa osan tai kaikki näistä tiedoista. Sitten se muodostaa ja lähettää eheyssuojatun sanoman, joka sisältää tiedot niistä salausalgoritmeista, joita monimuotomatkaviestin tukee toisessa radioliityntäverkossa.



RATKAISU 1

En oärlig inkräktare kan tjuvlyssna på ett samtal genom att avlägsna information angående en krypteringsalgoritm, när en multimode mobilteleapparat skickar ett oskyddat inledande signaleringsmeddelande som innehåller denna information längs radiogränssnittet till mobiltelesystemet. Försöket kan förhindras i ett globalt mobiltelesystem (UMTS-system), som innefattar minst två radioaccessnät som ger mobilteleapparater access till minst ett huvudnät, en multimode mobilteleapparat och åtminstone etthuvudnät. När en förbindelse öppnas till ett första radioaccessnät, sänder multimode mobilteleapparaten ett oskyddat inledande signaleringsmeddelande som innehåller information om de krypteringsalgoritmer som multimode mobilteleapparaten stöder, då den kommunicerar i ett andra radioaccessnät. Det första radioaccessnätet sparar en del av eller all denna information. Därefter bildar och skickar det ett integritetsskyddat meddelande som innehåller information om krypteringsalgoritmerna som multimode mobilteleapparaten stöder i det andra radioaccessnätet.

JÄRJESTELMÄ KANAVANVAIHDON JÄLKEEN TAPAHTUVAN TIETOLIIKENTEEN SALAUKSEN VARMISTAMISEKSI

Keksinnön ala

Keksintö koskee yleisesti tietoliikenneverkon eheyden suojaamista.

Keksinnön tausta

Kolmannen sukupolven matkaviestinjärjestelmästä käytetään Euroopassa nimeä UMTS (Universal Mobile Telecommunications System, yleiseurooppalainen matkaviestinjärjestelmä). UMTS-järjestelmä on osa YK:n alaisen kansainvälisen televiestintäliiton ITU:n (International Telecommunications Union) IMT-2000-järjestelmää. UMTS/IMT-2000 on maailmanlaajuinen langaton multimedian välitykseen kykenevä järjestelmä, jonka avulla tiedonsiirto tulee olemaan nopeampaa (2 megabittiä sekunnissa) kuin nykyisissä matkaviestinverkoissa.

Kuvion **1** yksinkertaistetulla lohkokaaviolla kuvataan GSM (Global System for Mobile Communications, maailmanlaajuinen matkaviestinjärjestelmä) -verkkoa ja UMTS-verkkoa. Verkon tärkeimmät osat ovat käyttäjien päätelaitteet **100** ja verkko, johon kuuluvat GSM-tukiaseman alijärjestelmä (BSS, Base Station Subsystem) **105** ja UTRAN-verkko (UMTS terrestrial radio access network) **101**, sekä ydinverkko (core network) **104**. (UTRAN-verkko on laajakaistainen moniliityntäradioverkko, jonka määrittelytyötä tehdään parhaillaan 3GPP-projektissa (Third Generation Partnership Project).) Käyttäjän päätelaitteen ja UTRAN-verkon välistä ilmarajapintaa kutsutaan Uu-rajapinnaksi ja UTRAN-verkon ja kolmannen sukupolven ydinverkon välistä rajapintaa Iu-rajapinnaksi. GSM-tukiaseman alijärjestelmän (BSS) ja GPRS (general packet radio service, pakettikytkentäinen datapalvelu) -ydinverkon välistä rajapintaa kutsutaan Gb-rajapinnaksi ja GSM-tukiaseman alijärjestelmän (BSS) ja GSM-ydinverkon välistä rajapintaa A-rajapinnaksi. Käyttäjien päätelaitteet voivat olla monimuotopäätteitä, joita voidaan käyttää vähintään kahden eri radioliityntätekniikan avulla, joita tässä esimerkissä ovat UMTS ja GSM. UTRAN koostuu radioverkon alijärjestelmästä (RNS, radio network subsystem) **102**, joka puolestaan koostuu radioverkko-ohjaimesta (RNC, radio network controller) **103** ja yhdestä tai useammasta B-solmusta (ei kuvattu kuviossa 1). Rajapintaa kahden radioverkon alijärjestelmän (RNS)

välillä kutsutaan Iur-rajapinnaksi. Käyttäjän päätelaitteen ja GSM-tukiaseman alijärjestelmän (BSS) välistä rajapintaa kutsutaan yksinkertaisesti ilmarajapinnaksi. GSM-tukiaseman alijärjestelmä (BSS) koostuu tukiasemaohjaimista (BSC, base station controller) **106** ja varsinaisista tukiasemista (BTS, base transceiver station) **107**. Ydinverkkosolmut, esimerkiksi (GSM-)matkapuhelinkeskus (MSC, Mobile Switching Center) ja (GPRS-)tukisolmu SGSN (serving GPRS support node), voivat ohjata kummankin tyyppisiä radioliityntäverkkoja eli sekä UTRAN-verkkoja että tukiaseman alijärjestelmiä (BSS). Toinen mahdollinen verkkokonfiguraatio on sellainen, jossa jokaisella radioliityntäverkolla (UTRAN-verkolla ja tukiaseman alijärjestelmällä (BSS)) on oma ohjaava ydinverkkosolmunsa, matkapuhelinkeskuksensa (MSC), tukisolmunsa SGSN ja – vastaavasti – toisen sukupolven matkapuhelinkeskuksensa (MSC) ja tukisolmunsa SGSN sekä kolmannen sukupolven matkapuhelinkeskuksensa (MSC) ja tukisolmunsa SGSN – mutta, jossa kaikki nämä ydinverkkoelementit on liitetty yhteen ja samaan kotirekisteriin (HLR, home location register) (ei kuvattu kuviossa 1). Kotirekisteri sisältää kaikki pysyvät käyttäjätiedot, esimerkiksi käyttäjien laskutusta voidaan ohjata yhdestä paikasta käsin, siitäkin huolimatta, että käyttäjien päätelaitteet mahdollisesti kykenevät käyttämään useita eri radioliityntäverkkoja.

Seuraavassa käsitellään lyhyesti ilmarajapintoja koskevia yhteyskäytäntöjä, joita tarvitaan radioverkkopalveluiden perustamiseen, asetusten uudelleenmäärittelyyn ja purkamiseen. Ilmarajapintoja koskevien yhteyskäytäntöjen arkkitehtuuri liityntätasolla (access stratum) koostuu kolmesta eri yhteyskäytäntökerroksesta, jotka ovat järjestyksessä ylimmästä alimpaan seuraavat: radioverkkokerros (L3), siirtokerros (L2) ja fyysinen kerros (L1). Seuraavassa on esitelty kerrosten yhteyskäytäntöoliot. Radioverkkokerros koostuu ainoastaan yhdestä yhteyskäytännöstä, jota kutsutaan UMTS-ilmarajapinnassa radioresurssien ohjauskäytännöksi eli RRC-yhteyskäytännöksi (Radio Recourse Control protocol) ja toisen sukupolven GSM-ilmarajapinnassa radioresurssiyhteyskäytännöksi (RR, Radio Resource protocol). Siirtokerros koostuu useista UMTS-ilmarajapinnan yhteyskäytännöistä, joita kutsutaan PDCP-yhteyskäytännöksi (Packet Data Convergence Protocol, pakettidatan konvergenssiyhteyskäytäntö), BMC-yhteyskäytännöksi (Broadcast Multicast Control protocol, yleislähetys-ohjausta koskeva yhteyskäytäntö), radiolinkkien ohjauksen yhteyskäytännöksi (RLC, Radio Link Control protocol) ja siirtokanavan saantimenettelyn ohjauskäytän-

nöksi (MAC, Medium Access Control protocol). GSM/GPRS-ilmarajapinnassa kerros 2:n yhteyskäytännöt ovat siirtoyhteyden looginen ohjaus (LLC, Logical Link Control), matkaviestimen ja tukiasemajärjestelmän välinen D-kanavan siirtoyhteyskäytäntö (LAPDm, Link Access Protocol on the Dm Channel), radiolinkkien ohjauksen (RLC) yhteyskäytäntö ja siirtokanavan saantimenettelyn ohjauskäytäntö (MAC). Fyysinen kerros koostuu vain yhdestä "yhteyskäytännöstä", jolla ei ole mitään erityistä nimeä. Kussakin radioliityntätekniikassa käytetään omia ilmarajapintoja koskevia yhteyskäytäntöjä, mikä tarkoittaa esimerkiksi sitä, että GSM-ilmarajapintaa varten tarvitaan eri yhteyskäytäntö kuin UMTS-verkon Uu-rajapintaa varten.

UMTS-verkossa RRC-kerroksen avulla voidaan tarjota palveluita ylemmille kerroksille, toisin sanoen liitynnän esto -tasolle (NAS) palvelupisteiden kautta, joita käyttäjien päätelaitteiden puolella käyttävät ylemmän kerroksen yhteyskäytännöt ja UTRAN-verkon puolella Iu-rajapinnan toimintoja tukeva radioliityntäverkon merkinantokäytäntö (RANAP-yhteyskäytäntö, Radio Access Network Application Part). Kaikki ylemmissä kerroksissa tapahtuva merkinanto (liikkuvuuden hallinta, puhelunohjaus, yhteysjaksojen hallinta jne.) on kapseloitu RRC-sanomiksi, jotta ne voidaan siirtää ilmarajapinnan välityksellä.

Tietoliikenteessä on aina olemassa se ongelma, miten varmistaa, että vastaanotetun tiedon on lähettänyt sellainen lähettäjä, jolla on valtuudet käyttää järjestelmää, eikä järjestelmään päässyt tunkeilija, joka yrittää naamioitua lähettäjäksi. Ongelma on erityisen selkeä solukkojärjestelmissä, joissa ilmarajapinta sopii erinomaisesti salakuunteluun ja siirrettävien tietojen sisällön vaihtamiseen ylempiä lähetystasoja käyttämällä, jopa etäisyyksien takaa. Perusratkaisu tähän ongelmaan on kommunikoivien osapuolten todentaminen. Todentamisprosessilla pyritään tunnistamaan ja tarkistamaan kommunikoivat osapuolet niin, että molemmat osapuolet voivat tarkistaa toisen osapuolen tunnistustiedot ja että he voivat luottaa tunnistukseen riittävässä määrin. Todentaminen suoritetaan yleensä erityisessä menettelyssä yhteyden alussa. Sen avulla ei kuitenkaan voida riittävän hyvin suojata seuraavia sanomia luvattomalta muuntelulta, luvattomilta lisäyksiltä tai poistoilta. Siksi jokaisen sanoman käyttäjät on todennettava erikseen. Tämä voidaan tehdä lisäämällä sanomaan sanomantunnistuskoodi eli MAC-I-koodi lähettäjän päässä ja tarkistamalla MAC-I-arvo vastaanottajan päässä.

MAC-I-koodi on yleensä melko lyhyt bittijono, joka perustuu erityisellä tavalla suojattavaan sanomaan sekä salaiseen avaimeen, jonka tuntevat sekä sanoman lähettäjä että sen vastaanottaja. Salainen avain luodaan ja siitä sovitaan yleensä todentamisprosessin yhteydessä yhteyden alussa. Joissakin tapauksissa myös algoritmi, jota käytetään salaiseen avaimeen ja sanomaan perustuvan MAC-I-koodin laskemiseen, on salainen. Näin ei kuitenkaan yleensä ole.

Yksittäisten sanomien todentamisprosessia nimitetään usein eheyden suojaamiseksi. Merkinannon eheys voidaan suojata siten, että lähettävä osapuoli laskee lähetettävään sanomaan ja salaiseen avaimeen perustuvan MAC-I-arvon käyttämällä määritettyä algoritmia ja lähettää MAC-I-arvon sanoman mukana. Vastaanottava osapuoli laskee sanomaan ja salaiseen avaimeen perustuvan MAC-I-arvon uudelleen käyttämällä määritettyä algoritmia ja vertaa vastaanotettua MAC-I-arvoa ja laskennan tuloksena saatua MAC-I-arvoa toisiinsa. Jos nämä kaksi MAC-I-arvoa vastaavat toisiaan, vastaanottaja voi olla varma, että viesti on koskematon ja että sen lähettäjällä on valtuudet käyttää järjestelmää.

Kuviosssa **2** kuvataan, miten MAC-I-koodi lasketaan UTRAN-verkossa. UTRAN-verkossa käytettävän MAC-I-koodin pituus on 32 bittiä.

Lohkossa **200** käytettävä UMTS-eheysalgoritmi on yksisuuntainen kryptografinen toiminto, jonka avulla voidaan laskea MAC-I-koodi kuviossa **2** kuvattujen syöttöparametrien perusteella. Yksisuuntaisuus tarkoittaa, että MAC-I-koodin perusteella on mahdotonta selvittää niitä syöttöparametreja, joita ei vielä tunneta, vaikka kaikki muut paitsi yksi syöttöparametri tunnettaisiinkin.

MAC-I-koodin laskemisessa tarvittavat syöttöparametrit ovat varsinainen (koodauksen jälkeen) lähetettävä merkinantosanoma, salainen eheysavain, eheyssuojattavan sanoman järjestysnumero COUNT-I, siirtosuunnan - toisin sanoen sen, onko sanoma lähetetty nousevaa siirtotietä (käyttäjän päätelaitteesta verkkoon) vai laskevaa siirtotietä (verkosta käyttäjän päätelaitteeseen) – osoittava arvo ja verkon tuottama satunnaisluku FRESH. Järjestysnumero COUNT-I muodostetaan lyhyestä järjestysnumerosta (SN, sequence number) ja pitkästä järjestysnumerosta, jota kutsutaan hyperkehysluvuksi (HFN, hyper frame number). Yleensä ainoastaan lyhyt järjestysnumero lähetetään sanoman mukana; hyperkehysluku (HFN) päivite-

tään paikallisesti kunkin kommunikoivan osapuolen vastaanottaessa sanoman.

Laskentalohko **200** laskee MAC-I-koodin lisäämällä edellä mainitut parametrit eheysalgoritmiin, jota 3GPP:n vuoden -99 määrittelyiden mukaisesti kutsutaan f9-algoritmiksi. On mahdollista, että seuraavaksi julkaistavissa uusissa määrittelyissä on lisää algoritmeja. Ennen kuin eheyden suojaaminen aloitetaan, käyttäjän päätelaite ilmoittaa verkolle, mitä eheysalgoritmeja se tukee, minkä jälkeen verkko valitsee yhden näistä algoritmeista käytettäväksi yhteyttä varten. Vastaavanlaista tuettujen algoritmien mekanismia käytetään myös tietojen salauksessa.

Kuviossa **3** on kuvattu esimerkiksi ilmarajapinnan välityksellä lähetettävä sanoma. Sanoma on N-kerroksen yhteyskäytännön datayksikkö (PDU, protocol data unit) **300**, joka välitetään hyötyinformaationa N-1-kerroksen yhteyskäytännön datayksikölle (PDU) **301**. Tässä esimerkissä N-kerros kuvaa RRC-yhteyskäytäntöä ilmarajapinnassa ja N-1-kerros kuvaa radiolinkkien ohjauskerrosta (RLC). N-1-kerroksen yhteyskäytännön datayksikkö (PDU) on yleensä määrämittainen ja sen pituus riippuu fyysisestä kerroksesta (alin kerros, ei kuvattu kuviossa 2), käytettävästä kanavatyypistä ja parametreista, esimerkiksi modulaatiosta, kanavakoodauksesta ja kanavien lomituksesta. Jos N-kerroksen yhteyskäytännön datayksiköt (PDU:t) eivät ole tarkalleen samankokoisia kuin N-1-kerroksen tarjoama hyötyinformaatio, mikä on yleisin tapaus, N-1-kerros voi käyttää esimerkiksi segmentointi-, ketjutus- ja täytetoimintoja, joiden avulla N-1-kerroksen yhteyskäytännön datayksiköistä (PDU) voidaan tehdä määrämittaisia. Tässä sovelluksessa keskitymme N-kerroksen yhteyskäytännön datayksikköön (PDU), joka koostuu varsinaisista merkinantotiedoista ja eheystarkistustiedoista. Eheystarkistustiedot koostuvat MAC-I-koodista ja sanoman lyhyestä järjestysnumerosta (SN), jota tarvitaan vertaislaitteella MAC-I-koodin uudelleenlaskemiseen. Sanoman kokonaispituus on siten merkinantotiedot ja eheystarkistustiedot muodostavien bittien yhteispituus.

Kaaviossa **4** on kuvattu järjestelmien välinen kanavanvaihto radioliityntäverkosta GSM-tukiaseman alijärjestelmään. Yksinkertaisuuden vuoksi kaaviossa **4** on kuvattu vain yksi matkapuhelinkeskus. Käytännössä tarvitaan (2G- eli toisen sukupolven) GSM-matkapuhelinkeskus (MSC) ja (3G- eli kolmannen sukupolven) UMTS-matkapuhelinkeskus, jotka voivat olla fyysisesti joko yksi matkapuhelinkeskus tai kaksi erillistä matkapuhelinkeskusta

(MSC). Koska näiden kahden matkapuhelinkeskuksen (jos käytössä on kaksi erillistä yksikköä) välinen yhteistoiminta ei ole olennaista keksinnön kannalta, sitä ei kuvata seuraavassa.

Alussa käyttäjän päätelaitteen ja radioliityntäverkon, joka tässä esimerkissä on UTRAN-verkko, välillä on yhteys. Useiden eri parametrien, esimerkiksi naapurisolun kuormitustietojen ja käyttäjän päätelaitteelta saatavien mittausten perusteella, sekä sen perusteella, että läheisellä maantieteellisellä alueella on olemassa GSM-soluja ja että käyttäjän laitteessa on tarvittavat ominaisuudet (myös GSM-verkon tukemiseen), radioliityntäverkko voi käynnistää järjestelmien välisen kanavanvaihdon aiemmasta järjestelmästä tukiaseman alijärjestelmään (BSS). Ensiksi UTRAN pyytää käyttäjän päätelaitetta aloittamaan järjestelmien väliset GSM-kantoaaltojen mittaukset lähettämällä MEASUREMENT CONTROL –sanoman (mittauksen valvonta) **400,** joka sisältää erityisiä järjestelmien väliseen tietoliikenteeseen liittyviä parametreja. Kun kriteerit mittausraportin lähettämisestä (kuten MEASUREMENT CONTROL -sanomassa on kuvattu) täyttyvät, käyttäjän päätelaite lähettää MEASUREMNT RAPORT(S) –sanoman (mittausraportit) **401.** Sen jälkeen UTRAN-verkossa tehdään päätös järjestelmien välisestä kanavanvaihdosta. Kun päätös on tehty, palveleva radioverkko-ohjain (SRNC, serving radio network controller), joka sijaitsee UTRAN-verkossa, lähettää RELOCATION REQUIRED -sanoman (siirtopyyntö) **402** Iu-rajapinnan kautta (3G-)matkapuhelinkeskukseen (MSC). Kun sanoma on vastaanotettu, (2G-)matkapuhelinkeskus (MSC) lähettää HANDOVER REQUEST -sanoman (kanavanvaihtoyhteys) **403** kohteena olevalle tukiaseman alijärjestelmälle. Tämä sanoma sisältää sellaisia tietoja, kuten salausalgoritmin ja salausavaimen, joita käytetään yhteyttä varten, sekä matkaviestimen kyvykkyystiedot (classmark information), joiden perusteella tiedetään esimerkiksi, mitä salausalgoritmeja käyttäjän päätelaite tukee. Siten on mahdollista, että joko matkapuhelinkeskus (MSC) valitsee salausalgoritmin ja lähettää ainoastaan valitun algoritmin tukiaseman alijärjestelmälle (BSS) tai että matkapuhelinkeskus (MSC) lähettää listan mahdollisista salausalgoritmeista tukiaseman alijärjestelmälle (BSS), joka sitten tekee lopullisen valinnan. Käyttäjän päätelaite on lähettänyt matkaviestimen kyvykkyystiedot matkapuhelinkeskukselle (MSC) (UMTS-)yhteyden alussa. On myös mahdollista, että käyttäjän päätelaite lähettää matkaviestimen kyvykkyystiedot UMTS-radioliityntäverkolle (UTRAN-verkolle) (UMTS-)yhteyden alussa. Kun järjestelmien välinen kana-

vanvaihto UMTS-verkosta GSM-verkkoon käynnistetään, matkaviestimen kyvykkyystiedot lähetetään UTRAN-verkosta edelleen matkapuhelinkeskukselle (MSC). Kun GSM-tukiasemaohjain vastaanottaa sanoman, se tekee varauksen GSM-solusta, johon on viitattu, ja vastaa lähettämällä takaisin HANDOVER REQUEST ACK -sanoman (kanavanvaihtopyynnön kuittaus) **404**, joka osoittaa, että pyydettyä kanavanvaihtoa tukiaseman alijärjestelmään (BSS) tuetaan, sekä sen, mihin radiokanavaan (-kanaviin) käyttäjän päätelaite pitää ohjata. HANDOVER REQUEST ACK -sanoma **404** osoittaa myös, että pyydetty kanavanvaihtoalgoritmi on hyväksytty, tai siinä tapauksessa, että HANDOVER REQUEST -sanoma **403** sisälsi useita algoritmeja, se osoittaa, mikä kanavanvaihtoalgoritmi on valittu. Jos tukiaseman alijärjestelmä (BSS) ei tue mitään sille osoitetuista salausalgoritmeista, se palauttaa HANDOVER FAILURE -sanoman (kanavanvaihtovirhe) (sanoman **404** sijasta) ja matkapuhelinkeskus (MSC) ilmoittaa UTRAN-verkolle, että kanavanvaihdossa on tapahtunut virhe. Vaiheessa **405** (3G-)matkapuhelinkeskus (MSC) vastaa sanomaan, jonka UTRAN-verkossa sijaitseva palveleva radioverkko-ohjain on lähettänyt vaiheessa **402**, lähettämällä RELOCATION COMMAND -sanoman (siirtokomento) Iu-rajapinnan välityksellä. RELOCATION COMMAND -sanoman hyötyinformaatio sisältää mm. varattuja GSM-kanavia ja salaustapaa koskevia tietoja. UTRAN-verkko antaa käyttäjän päätelaitteelle käskyn suorittaa kanavanvaihto lähettämällä INTERSYSTEM HANDOVER COMMAND -sanoman (järjestelmien välinen kanavanvaihtokomento) **406**, joka sisältää kohteena olevan GSM-verkon kanavatiedot. Lisäksi mukana voi olla muitakin tietoja, kuten esimerkiksi GSM-salaustavan asetuksia koskevia tietoja, jotka osoittavat ainakin sen, mitä salausalgoritmia GSM-yhteyttä varten on käytettävä. Kun matkaviestin on kytkeytynyt varatuille GSM-kanaville, se yleensä lähettää neljä kertaa HANDOVER ACCESS -sanoman (kanavanvaihtoyhteys) **407** neljänä peräkkäisenä kerroksen 1 kehyksenä yhteyskohtaisen pääohjauskanavan (main DCCH) välityksellä. Nämä sanomat lähetetään salaamattomina GSM-saantipurskeina. Joissakin tilanteissa ei ole välttämätöntä lähettää HANDOVER ACCESS -sanomia, jos INTERSYSTEM HANDOVER COMMAND -sanomissa **406** osoitetaan niin. Päätelaite saattaa vastaanottaa PHYSICAL INFORMATION -sanoman (fyysiset tiedot) **408** vastauksena HANDOVER ACCESS -sanomaan. PHYSICAL INFORMATION -sanoma sisältää ainoastaan GSM-ajastuksen ennakkotiedot (GSM Timing Advance information).

PHYSICAL INFORMATION -sanoman vastaanotto saa aikaiseksi sen, että päätelaite lopettaa saantipurskeiden lähettämisen. HANDOVER ACCESS -sanomat - jos niitä käytetään - käynnistävät tukiasemajärjestelmän GSM-tukiasemaohjaimen, joka ilmoittaa tilanteesta (2G-)matkapuhelinkeskukselle lähettämällä HANDOVER DETECT -sanoman (kanavanvaihto havaittu) **409**.

Sen jälkeen, kun on luotu alemman kerroksen yhteydet, matkaviestin palauttaa HANDOVER COMPLETE -sanoman (kanavanvaihto suoritettu) **410** GSM-tukiaseman alijärjestelmälle yhteyskohtaisen pääohjauskanavan välityksellä (main DCCH). Kun verkko vastaanottaa HANDOVER COMPLETE -sanoman **410**, se purkaa vanhat kanavat, jotka tässä esimerkissä ovat UTRAN-kanavia. Kuviossa **4** on kuvattu kolme tämän purkuprosessin tuottamaa sanomaa, vaikka todellisuudessa tarvitaan monia muitakin verkkoelementtien välisiä sanomia, joita ei ole kuvattu kuviossa **4**. Nämä kolme sanomaa ovat ensinnäkin HANDOVER COMPLETE -sanoma **411**, joka lähetetään GSM-tukiaseman alijärjestelmältä matkapuhelinkeskukseen, ja toiseksi IU RELEASE COMMAND -sanoma (IU:n purkukomento) **412**, joka lähetetään Iu-rajapinnan välityksellä UTRAN-verkkoon tai tarkemmin sanottuna palvelevalle radioverkko-ohjaimelle. Kolmas sanoma on IU RELEASE COMPLETE (IU:n purku suoritettu) **413**.

Järjestelmien välisen kanavanvaihdon jälkeen käytettävä salausavain lasketaan muuntotoiminnon avulla sitä salausavainta käyttämällä, jota käytettiin UTRAN-verkossa ennen kanavanvaihtoa. Koska muuntotoiminto on sekä matkaviestimessä että matkapuhelinkeskuksessa, ilmarajapinnan kautta ei tarvitse suorittaa mitään lisäproseduureja. Kuten edellä on kuvattu, joko matkapuhelinkeskus (MSC) tai tukiaseman alijärjestelmä (BSS) valitsee GSM-salausalgoritmin, jota käytetään järjestelmien välisen kanavanvaihdon jälkeen, ja siitä ilmoitetaan matkaviestimelle (sanomien **405** ja **406** avulla). GSM-salausalgoritmin ominaisuudet (jotka sisältyvät GSM-matkaviestimen kyvykkyyden informaatioelementteihin) ovat nykyisten määrittelyjen mukaisesti läpinäkyviä UTRAN-verkon kannalta. GSM-matkaviestimen kyvykkyyden informaatioelementit lähetetään kuitenkin matkaviestimestä RRC-yhteyden avausproseduurin aikana UTRAN-verkkoon, josta ne lähetetään myöhemmin edelleen ydinverkolle, kun järjestelmien välinen kanavanvaihto GSM-verkkoon suoritetaan.

Kuvion **5** merkinantokaaviossa on kuvattu yleinen yhteydenavaus- ja turvatilan asetusproseduuri, jota käytetään 3GPP:n määrittelyjen mukai-

sessa UTRAN-verkossa. Kuviossa **5** on kuvattu ainoastaan kaikkein tärkein matkaviestimen ja palvelevan radioverkko-ohjaimen välinen merkinanto, johon sisältyy toisaalta radioliityntäverkon ja toisaalta palvelevan radioverkko-ohjaimen ja matkapuhelinkeskuksen tai palvelevan GPRS-tukisolmun merkinanto.

RRC-yhteyden avaaminen matkaviestimen ja palvelevan radioverkko-ohjaimen välille suoritetaan Uu-rajapinnan **500** avulla. RRC-yhteyden avaamisen aikana matkaviestin saattaa siirtää tietoja, kuten käyttäjän laitteen turvaamisvalmiudet ja ALOITUS-arvot (START), joita tarvitaan salaus- ja eheydensuojausalgoritmeja varten. Käyttäjän laitteen turvaamisvalmiudet sisältävät tiedot tuetuista (UMTS) salausalgoritmeista ja (UMTS) eheysalgoritmeista. Kaikki edellä mainitut arvot tallennetaan myöhempää käyttöä varten palvelevaan radioverkko-ohjaimeen vaiheessa **501**. Myös GSM-kyvykkyystiedot (matkaviestimen kyvykkyys 2 ja 3) siirretään matkaviestimestä UTRAN-verkkoon RRC-yhteyden avaamisen aikana, ja ne voidaan tallentaa myöhempää käyttöä varten palvelevaan radioverkko-ohjaimeen.

Seuraavaksi matkaviestin lähettää ylemmän kerroksen aloitussanoman **502** (joka voi olla esimerkiksi CM SERVICE REQUEST (CM-palvelupyyntö), LOCATION UPDATING REQUEST (sijainninpäivityspyyntö) tai CM RE-ESTABLISHMENT REQUEST (CM-yhteyden uudelleenmuodostuspyyntö)) palvelevan radioverkko-ohjaimen välityksellä *Iu*-rajapinnan kautta matkapuhelinkeskukselle. Ylemmän kerroksen aloitussanomaan sisältyvät esimerkiksi käyttäjän tunnistustiedot, KSI-tunniste (Key Set Identifier, avainsarjatunniste) ja matkaviestimen kyvykkyystiedot, joista käyvät ilmi esimerkiksi tuetut GSM-salausalgoritmit, kun järjestelmien välinen kanavanvaihto aiemmasta järjestelmästä GSM-verkkoon käynnistetään. Verkko käynnistää todentamisproseduurin, minkä vuoksi myös uusien suojausavainten **503** generointi aloitetaan. Seuraavaksi verkko päättää, mitkä ovat ne UMTS-eheysalgoritmit (UIA) ja UMTS-salausalgoritmit (UEA), joiden joukosta eheys- ja salausalgoritmi tätä yhteyttä varten on valittava **504**. Vaiheessa **505** matkapuhelinkeskus lähettää SECURITY MODE COMMAND -sanoman (turvatilakomento) palvelevalle radioverkko-ohjaimelle. Tässä sanomassa se ilmoittaa, mitä avainta (CK, cipherkey) ja eheysavainta on käytetty, sekä sen, mitkä ovat sallitut UMTS-eheysalgoritmit ja UMTS-salausalgoritmit.

Vaiheessa **501** tallennettujen käyttäjän laitteiden turvaamisvalmiuksien ja vaiheessa **505** matkapuhelinkeskukselta vastaanotetut mah-

dolliset UIA:t ja UEA:t sisältävän listan perusteella palveleva radioverkko-ohjain valitsee yhteyden aikana käytettävät algoritmit. Lisäksi se generoi satunnaisluvun FRESH, jota käytetään eheysalgoritmin (kuvio 2) ja salausalgoritmin syöttöparametrina. Lisäksi se käynnistää salauksen ja eheyden suojaamisen **506**.

Ensimmäinen eheyssuojattu sanoma SECURITY MODE COMMAND **507** lähetetään ilmarajapinnan kautta palvelevasta radioverkko-ohjaimesta matkaviestimeen. Sanomaan sisältyvät valittu UIA ja UEA sekä käyttäjän laitteen FRESH-parametri, jota käytetään jatkossa. Lisäksi SECURITY MODE COMMAND -sanomaan sisältyvät samat käyttäjän laitteen turvaamisvalmiudet, jotka on saatu käyttäjän laitteelta RRC-yhteyden avaamisen aikana **500**. Nämä tiedot lähetetään takaisin käyttäjän laitteelle siksi, että käyttäjän laite voi tarkistaa, että verkko on vastaanottanut tiedot oikein. Tämä mekanismi on tarpeellinen, koska RRC-yhteyden avaamisen **500** aikana lähetettäviä sanomia ei ole salattu eikä eheyssuojattu. MAC-I-koodi, jota käytetään eheyden suojaamiseen, liitetään SECURITY MODE COMMAND -sanomaan **507**.

Vaiheessa **508** matkaviestin vertaa, onko vastaanotetut käyttäjän laitteen turvaamisvalmiudet samat kuin RRC-yhteyden avausproseduurin **500** aikana lähetetyt turvaamisvalmiudet. Jos vertailun tulokset täsmäävät, matkaviestin voi olla varma siitä, että verkko on vastaanottanut turvaamisvalmiudet oikein. Muussa tapauksessa käyttäjän laite purkaa RRC-yhteyden ja siirtyy valmiustilaan.

Jos vertailun tulokset täsmäävät, matkaviestin vastaa lähettämällä SECURITY MODE COMPLETE -sanoman (turvatila suoritettu) **509**. Myös tämä sanoma on eheyssuojattu; matkaviestin generoi sanomaa varten MAC-I-koodin ennen kuin lähettää sanoman.

Kun palveleva radioverkko-ohjain vastaanottaa sanoman, se vahvistaa sen vaiheessa **510** laskemalla ensin XMAC-I-arvon (expected message authentication code, sanomantunnistuskoodin odotusarvo) ja vertaamalla sitten laskennan tuloksena saatua XMAC-I-arvoa vastaanotettuun MAC-I-arvoon. Jos arvot vastaavat toisiaan, palveleva radioverkko-ohjain lähettää matkapuhelinkeskukselle SECURITY MODE COMPLETE -sanoman **511**, joka sisältää esimerkiksi tiedot valitusta UIA:sta ja UEA:sta.

UTRAN-verkon ilmarajapinnassa eheyden suojaus on RRC-ohjauskäytännön toiminto käyttäjän päätelaitteen ja radioverkko-ohjaimen

välissä. RRC-ohjauskäytäntökerros suojaa kaiken ylempien kerrosten merkinannon eheyttä, koska kaikki ylempien kerrosten merkinanto siirretään hyötyinformaationa erityisissä RRC-sanomissa (esimerkiksi INITIAL DIRECT TRANSFER (aloittava suorasiirto)-, UPLINK DIRECT TRANSFER (nousevan siirtotien suorasiirto)- tai DOWNLINK DIRECT TRANSFER (laskevan siirtotien suorasiirto) -sanomassa). Ongelmana tässä on se, että todentamista ei voida suorittaa, ennen kuin ensimmäinen INITIAL DIRECT TRANSFER -sanomassa siirrettävä ylemmän kerroksen sanoma on lähetetty. Tästä on seurauksena se, että ensimmäisen ylemmän kerroksen sanoman, toisin sanoen liitynnän esto -tason (NAS) sanoman **502** eheyttä ei voida suojata.

Merkittävä ongelma aiheutuu siitä, että sanomien eheyttä ei ole vielä suojattu, kun ensimmäiset sanomat lähetetään RRC-yhteyden avauksen aikana (vaihe **500** kuviossa **5**). Koska sanoman eheyttä ei ole suojattu, on aina olemassa se vaara, että järjestelmään päässyt tunkeilija muuttaa vaiheen **500** sanomiin sisältyneet salausalgoritmitiedot arvoon "ei GSM-salausalgoritmeja käytössä". Kun kyseessä on GSM-verkko, ydinverkko vastaanottaa tämän tiedon matkaviestimen kyvykkyyttä koskevien informaatioelementtien mukana (kyvykkyys 2 ja 3), jotka sisältyvät RELOCATION REQUIRED -sanomaan (sanoma **402** kuviossa **4**). Kun käyttäjän laite suorittaa järjestelmien välisen kanavanvaihdon, esimerkiksi UTRAN-verkosta GSM-tukiaseman alijärjestelmään (BSS) (kuvio **4**), matkapuhelinkeskus tunnistaa, ettei käyttäjän laite tue mitään GSM-salausalgoritmeja, ja sen on muodostettava yhteys GSM-tukiaseman alijärjestelmään (BSS) ilman salausta. Tämän jälkeen järjestelmään päässeen tunkeilijan on helppo salakuunnella puhelua.

Keksinnön lyhyt yhteenveto

Keksinnön tavoitteena on luoda sellainen matkaviestinjärjestelmä, joka paljastaa vilpillisten järjestelmään päässeiden tunkeilijoiden yritykset poistaa salausalgoritmitietoja monimuotomatkaviestimen lähettäessä tällaisia tietoja sisältävän suojaamattoman merkinantosanoman ilmarajapinnan välityksellä matkaviestinjärjestelmään. Nykyisten määrittelyjen mukaisesti tämä merkinantosanoma on RRC CONNECTION SETUP COMPLETE -sanoma (RRC-yhteyden avaus suoritettu).

Järjestelmä koostuu vähintään kahdesta radioliityntäverkosta, jotka tarjoavat matkaviestimille yhteyden vähintään yhteen ydinverkkoon, mo-

nimuotomatkaviestimestä sekä vähintään yhdestä ydinverkosta. Avatessaan yhteyttä ensimmäiseen radioliityntäverkkoon monimuotomatkaviestin lähettää ainakin yhden suojaamattoman merkinantosanoman, joka sisältää tiedot niistä salausalgoritmeista, joita monimuotomatkaviestin tukee toisessa radioliityntäverkossa. Ydinverkko vastaanottaa tiedot salausalgoritmeista ensimmäisen radioliityntäverkon välityksellä, kun kanavanvaihto toiseen radioliityntäverkkoon käynnistetään (sanoma **402** kuviossa **4**). Ensimmäisessä radioliityntäverkossa on edistyksellisiä ominaisuuksia. Nimittäin kun monimuotomatkaviestin vastaanottaa ydinverkolta komentosanoman, jossa se pyytää monimuotomatkaviestintä salaamaan kaikki seuraavat ensimmäisessä radioliityntäverkossa siirrettävät tiedot, ensimmäinen radioliityntäverkko muodostaa eheyssuojatun komentosanoman, joka sisältää tiedot salausalgoritmeista, joita monimuotomatkaviestin tukee toisessa radioliityntäverkossa.

Suojattu komentosanoma koostuu hyötyinformaatiosta ja sanomantunnistuskoodista. Tiedot toisessa radioliityntäverkossa tuetuista algoritmeista sijaitsevat joko hyötyinformaatiossa tai näitä tietoja käytetään parametrina, kun sanomantunnistuskoodia lasketaan.

Kummassakin tapauksessa monimuotomatkaviestin pystyy päättelemään vastaanottamansa suojatun sanoman perusteella, vastaavatko sanomaan sulautetut tiedot niitä tietoja, jotka se lähetti edellisessä merkinantosanomassa. Jos monimuotomatkaviestimen lähettämät ja sen vastaanottamat tiedot eroavat toisistaan, on todennäköistä, että vilpillinen järjestelmään päässyt tunkeilija on muuttanut suojaustietoja. Siinä tapauksessa monimuotomatkaviestin käynnistää yhteyden purkamisen.

Kuvioluettelo

Keksintö on kuvattu yksityiskohtaisesti liitteenä olevien kuvioiden avulla, joissa

Kuvio **1** kuvaa yksinkertaistetun lohkokaavion avulla GSM- ja UMTS-radioliityntäverkkoja, jotka on kytketty samaan ydinverkkoon;

Kuvio **2** kuvaa, miten sanomantunnistuskoodi lasketaan;

Kuvio **3** kuvaa sanoman sisällön;

Kuvio **4** on merkinantokaavio, joka kuvaa järjestelmien välistä kanavanvaihtoa UMTS-verkosta GSM-verkkoon;

Kuvio **5** on merkinantokaavio, joka kuvaa yleistä yhteyden avaus- ja turvatilan asetusproseduuria, joita käytetään 3GPP:n määrittelyjen mukaisessa UTRAN-verkossa;

Kuvio **6** kuvaa prosessikaavion avulla menetelmän ensimmäistä keksinnön mukaista toteutusesimerkkiä;

Kuvio **7** kuvaa prosessikaavion avulla menetelmän toista keksinnön mukaista toteutusesimerkkiä;

Kuvio **8** kuvaa prosessikaavion avulla menetelmän kolmatta keksinnön mukaista toteutusesimerkkiä;

Kuvio **9** kuvaa prosessikaavion avulla menetelmän neljättä keksinnön mukaista toteutusesimerkkiä;

Kuvio **10** kuvaa menetelmän viidettä keksinnön mukaista toteutusesimerkkiä;

Kuvio **11** kuvaa menetelmän kuudetta keksinnön mukaista toteutusesimerkkiä.

Keksinnön yksityiskohtainen selostus

Seuraavassa kuvattavan menetelmän tarkoitus on lisätä tietoliikenneverkkojen ja erityisesti ilmarajapinnan kautta tapahtuvan merkinannon turvallisuutta.

On huomattava, että termeillä "päätelaite", "käyttäjän päätelaite", "matkaviestin" ja "käyttäjän laite" tarkoitetaan kaikilla samaa laitetta.

Suurimman osan merkinantosanomista, jotka lähetetään esimerkiksi käyttäjän päätelaitteen ja verkon välillä, täytyy olla eheyssuojattuja. Esimerkkejä tällaisista sanomista ovat RRC (radioresurssien ohjaus)-, MM (liikkuvuuden hallinta)-, CC (puhelunohjaus)-, GMM (GPRS-liikkuvuuden hallinta)- ja SM (yhteysjaksojen hallinta) -sanomat. Eheyden suojaaminen toteutetaan RRC-kerroksessa sekä käyttäjän päätelaitteessa että verkossa.

Yleensä kaikki RRC-sanomat eheyssuojataan, mutta joitakin poikkeuksiakin on. Poikkeustapaukset voivat olla seuraavia:

1. sanomat, jotka on osoitettu useammalle kuin yhdelle vastaanottajalle,
2. sanomat, jotka lähetetään ennen kuin yhteyttä varten on luotu eheysavaimet, ja
3. usein toistuvat sanomat sekä tiedot, joita ei tarvitse eheyssuojata.

Turvallisuuden kannalta on erityisen tärkeää eheyssuojata vaihtoehdossa 2 mainitut aloitussanomat tai vähintään niissä olevat kriittiset informaatioelementit. Kuten on jo mainittu, ellei sanomia ole eheyssuojattu, on aina olemassa se vaara, että järjestelmään päässyt tunkeilija muuttaa sanomaan **500** sisältyvät suojausalgoritmitiedot arvoon "ei suojausalgoritmeja käytössä".

On olemassa useita eri tapoja toteuttaa vaaditut toiminnot, joiden avulla turvallisuutta voidaan lisätä, mutta tässä on esitelty vain muutamia ratkaisuja.

Seuraavaksi keksintö kuvataan yksityiskohtaisesti neljän esimerkin ja kuvioiden **6 - 9** avulla.

Aluksi käyttäjän päätelaitteen ja UMTS-verkon välille muodostetaan yhteys. Sen jälkeen suoritetaan kanavanvaihto UMTS-verkosta GSM-verkkoon.

Kuviossa **6** kuvataan prosessikaavion avulla menetelmän yhtä keksinnön mukaista toteutustapaa. Oletetaan, että merkinanto vastaa tilannetta, joka on kuvattu kuviossa **5**, kunnes ydinverkko vastaanottaa sanoman **503**.

Lisäksi oletetaan, että käyttäjän päätelaite on kahta matkapuhelinjärjestelmää (UMTS/GSM) tukeva päätelaite, joka UMTS-tilassa lähettää ensimmäisen liitynnän esto -tason sanoman ilmarajapinnan kautta RRC INITIAL DIRECT TRANSFER -sanomassa (vastaa sanomaa **502** kuviossa **5**). Lisäksi oletetaan, että RRC-yhteyden avaaminen (**500**) on suoritettu, joten käyttäjän päätelaite on valmiustilassa eikä sillä ole RRC-yhteyttä, kun pyyntö ydinverkkoyhteyden avaamisesta vastaanotetaan.

Ydinverkko vastaanottaa GSM-kyvykkyystiedot aloitussanomassa **502** käyttäjän päätelaitteelta, joka tässä tapauksessa on matkaviestin. Tämä tieto kertoo, mitkä ovat matkaviestimen yleiset ominaisuudet GSM-tilassa sekä mitä GSM-salausalgoritmeja päätelaite tukee, kun se on GSM-tilassa. Termi "kyvykkyys" (classmark) liittyy tässä tapauksessa erityisesti GSM-järjestelmiin; muissa järjestelmissä saatetaan käyttää jotain muuta termiä.

Ydinverkon matkapuhelinkeskus lisää SECURITY MODE COMMAND -sanomaan **600** tiedot siitä, mitä salausalgoritmeja matkaviestin tukee. Sanoma lähetetään palvelevalle radioverkko-ohjaimelle *Iu*-rajapinnan kautta. Palveleva radioverkko-ohjain lisää matkaviestimen tukemia salausalgoritmeja koskevat tiedot sekä tiedot tukemistaan salausalgoritmeista SECURITY COMMAND -sanomaan (turvakomento) ennen sanoman koodaamista **601**. 32-bittinen MAC-I-koodi lasketaan ja lisätään koodattuun sanomaan.

Tämän koodatun sanoman lisäksi MAC-I-koodi perustuu moniin muihinkin parametreihin. Eheysalgoritmin laskemiseen tarvitaan seuraavia syöttöparametreja: koodattu sanoma, 4-bittinen järjestysnumero (SN), 28-bittinen hyperkehysluku (HFN), 32-bittinen satunnaisluku FRESH, 1-bittinen suuntatunniste DIR (direction identifier) ja - kaikkein tärkein parametri - 128-bittinen eheysavain. Lyhyt järjestysnumero (SN) ja pitkä järjestysnumero (HFN) muodostavat yhdessä eheyssarjanumeron COUNT-I (serial integrity sequence number).

Kun MAC-I-koodi lasketaan eheysalgoritmia ja edellä mainittuja parametreja käyttämällä, voidaan taata, ettei kukaan muu kuin lähettäjä voi lisätä oikeaa MAC-I-koodia merkinantosanomaan. Esimerkiksi COUNT-I-numero estää sen, että sama sanoma lähetettäisiin toistuvasti. Jos sama merkinantosanoma kuitenkin jostain syystä on lähetettävä toistuvasti, MAC-I-koodi on erilainen kuin se MAC-I-koodi, jota käytettiin edellisellä kerralla lähetetyssä merkinantosanomassa. Tämän tarkoituksena on suojata sanoma mahdollisimman tehokkaasti salakuuntelijoilta ja muilta vilpillisiltä tunkeilijoilta. Siten erityisesti tämän keksinnön osalta on tärkeää huomata, että myös matkaviestimen tukemia salausalgoritmeja koskevat GSM-tiedot, jotka lisätään SECURITY MODE COMMAND -sanomaan **507**, ovat eheyssuojattuja, jotta matkaviestin voi olla varma siitä, ettei tunkeilija ole muuttanut näitä tietoja.

Kun matkaviestin vaiheessa **602** vastaanottaa SECURITY MODE COMMAND -sanoman, tämän sanoman mukana vastaanotettuja tietoja matkaviestimen tukemista salausalgoritmeista verrataan matkaviestimen tukemia salausalgoritmeja koskeviin tietoihin, jotka matkaviestin lähetti aiemmin verkolle aloitussanomassa **502**. Vastaavasti - tekniikan tason mukaisesti - vastaanotettua käyttäjän laitteen (UMTS) turvaamisvalmiusparametria verrataan lähetettyyn käyttäjän laitteen turvaamisvalmiusparametriin. Jos vertailujen

tulokset täsmäävät, matkaviestin hyväksyy yhteyden **604**, muussa tapauksessa yhteys puretaan **603**.

Kuviossa **7** kuvataan prosessikaavion avulla menetelmän toista toteutustapaa.

Vaiheessa **700** matkaviestin lähettää INITIAL DIRECT TRANSFER -sanoman (vastaa sanomaa **502** kuviossa **5**) ydinverkolle radioliityntäverkossa olevan palvelevan radioverkko-ohjaimen välityksellä. Sanoma koostuu kahdesta pääosasta: RRC-osasta ja liitynnän esto -taso-osasta, joka on RRC:n kannalta läpinäkyvää hyötyinformaatiota. Lisäksi hyötyinformaatio-osa sisältää yhden seuraavista sanomista: CM SERVICE REQUEST (CM-palvelupyyntö), LOCATION UPDATING REQUEST (sijainninpäivityspyyntö), CM RE-ESTABLISHMENT REQUEST (CM-yhteyden uudelleenmuodostuspyyntö) tai PAGING RESPONSE (hakuvastaus).

Kun palveleva radioverkko-ohjain vastaanottaa sanoman **701**, se tallentaa sen ja lähettää hyötyinformaatio-osan tai liitynnän esto -taso-osan (NAS-osan) Iu-rajapinnan kautta edelleen ydinverkolle **702**. Ydinverkko vastaa normaalilla SECURITY MODE COMMAND -sanomalla **703**. Kuten edellisessä esimerkissä, MAC-I-koodi lasketaan matkaviestimeen lähetettävän sanoman suojaamiseksi. Sen jälkeen koodi lisätään sanomaan. MAC-I-koodi on erityisellä tavalla riippuvainen sanomasta, jota se suojaa. Seuraavassa suoritetaan koodin laskenta käyttämällä seuraavaa ketjutettua bittijonoa MESSAGE-parametrina:

MESSAGE = SECURITY MODE COMMAND + RRC CONNECTION REQUEST + RRC INITIAL DIRECT TRANSFER.

Sen jälkeen eheyssuojattu SECURITY MODE COMMAND -sanoma lähetetään matkaviestimeen **704**.

On tärkeää huomata, että tässä ratkaisussa ei ole välttämätöntä sisällyttää käyttäjän laitteen (UMTS-)turvaamisvalmiusparametria edellä mainittuun sanomaan. Molempia turvaparametreja eli käyttäjän laitteen turvaamisvalmiusparametria ja GSM-kyvykkyysparametria käytettiin kuitenkin syöttöparametreina MAC-I-koodia laskettaessa.

Tulevassa siirtosuunnassa, toisin sanoen matkaviestimellä on identtinen algoritmi MAC-I-koodin laskemiseen, jotta voidaan varmistaa, että vastaanotettu MAC-I-koodi on sama kuin laskennan tuloksena saatu koodi **705**. Matkaviestin onkin tallentanut aiemmin lähetetyt sanomat, RRC CONNECTION REQUEST -sanoman (**500**) ja RRC INITIAL DIRECT TRANSFER

-sanoman (**502**), jotta vastaanotetulle SECURITY MODE COMMAND -sanomalle voidaan laskea XMAC-I-koodi. Jos vastaanotettu MAC-I-koodi ja laskennan tuloksena saatava XMAC-I-koodi vastaavat toisiaan, matkaviestin olettaa, että verkko on vastaanottanut oikeat turvaamisvalmiutta ja GSM-kyvykkyyttä koskevat tiedot ja hyväksyy yhteyden **707.** Muussa tapauksessa yhteys puretaan **706**.

Ratkaisulla on yksi huono puoli, nimittäin koodatut RRC CONNECTION REQUEST (RRC-yhteyspyyntö)- ja RRC INITIAL DIRECT TRANSFER -sanomat täytyy tallentaa sekä palvelevan radioverkko-ohjaimen että matkaviestimen muistiin, kunnes SECURITY MODE COMMAND –sanoma on lähetetty/vastaanotettu. Mutta toisaalta tämän ratkaisun ansiosta on mahdollista jättää käyttäjän laitteen turvaamisvalmius pois tekniikan tason mukaisesta SECURITY MODE COMMAND -sanomasta ja tällä tavoin säästää sanoman tilaa 32 bitin verran.

Kuviossa **8** kuvataan prosessikaavion avulla kolmatta menetelmän toteutustapaa.

Tämä ratkaisu poikkeaa vain vähän toisesta ratkaisusta, toisin sanoen vain lohkot **801, 804** ja **805** poikkeavat kuvion **7** lohkoista. Tästä syystä kuvaamme näitä kahta lohkoa yksityiskohtaisemmin.

Vaiheessa **801** palveleva radioverkko-ohjain tallentaa ainoastaan sanoman hyötyinformaatio-osan, eikä koko sanomaa, myöhempää käyttöä varten. Toisin sanoen se tallentaa yhden seuraavista sanomista: CM SERVICE REQUEST (CM-palvelupyyntö), LOCATION UPDATING REQUEST (sijainninpäivityspyyntö), CM RE-ESTABLISHMENT REQUEST (CM-yhteyden uudelleenmuodostuspyyntö) tai PAGING REQUEST (hakupyyntö). Siten tässä ratkaisussa säästetään muistitilaa verrattuna toiseen ratkaisuun.

Vaiheessa **804** sanoman suojaamiseksi lasketaan MAC-I-koodi käyttämällä aiemmin tallennettua hyötyinformaatiota. Sanoma muodostetaan tässä tapauksessa seuraavasti:

> MESSAGE = SECURITY MODE COMMAND + UE SECURITY CAPABILITY + INITIAL DIRECT TRANSFER -sanoman liitynnän esto -taso-osa.

Ainoastaan SECURITY MODE COMMAND -sanoma lähetetään Uu-rajapinnan välityksellä matkaviestimeen. Tämä tarkoittaa, että sekä käyttäjän laitteen turvaamisvalmiuden turvaparametreja että GSM-matkaviestimen kyvykkyystietoja käytetään MAC-I-koodin laskemiseen, mutta niitä

ei tarvitse sisällyttää sanomaan. Tämä ei kuitenkaan millään tavalla alenna turvallisuuden tasoa.

Vaiheessa **805** matkaviestin laskee XMAC-I-koodin käyttämällä samoja MESSAGE-parametreja, joita verkko käytti vaiheessa **804**, eli parametreja, jotka oli tallennettu aiemmin käyttäjän laitteen turvaamisvalmiudesta ja INITIAL DIRECT TRANSFER -sanoman NAS-taso-osasta.

Kuviossa **9** kuvataan prosessikaavion avulla menetelmän neljättä toteutustapaa. Tämä ratkaisu on yhdistelmä ensimmäisestä ja kolmannesta ratkaisusta.

Kun yhteyttä muodostetaan matkaviestimen ja radioliityntäverkossa olevan palvelevan radioverkko-ohjaimen välille, radioverkko-ohjain vastaanottaa ja tallentaa käyttäjän laitteen turvaamisvalmiustiedot (UEC, user equipment capability information) muistiinsa myöhempää käyttöä varten **900**. Sen jälkeen matkaviestin lähettää ensimmäisen liitynnän esto -tason sanoman, joka sisältää esimerkiksi tiedot matkaviestimen tukemista salausalgoritmeista, hyötyinformaationa RRC INITIAL DIRECT TRANSFER -sanomassa radioliityntäverkolle, joka lähettää liitynnän esto -tason sanoman edelleen ydinverkolle **901**. Ydinverkon matkaviestinkeskus lisää matkaviestinparametrin tukemia salausalgoritmeja koskevat tiedot SECURITY MODE COMMAND -sanomaan ja lähettää sanoman *Iu*-rajapinnan välityksellä palvelevalle radioliityntäverkon radioverkko-ohjaimelle vaiheissa **902** ja **903**.

Vaiheessa **904** palveleva radioverkko-ohjain laskee MAC-I-koodin edellä kuvatulla tavalla ja lisää aiemmin kuvattuihin parametreihin MESSAGE-parametrin, joka muodostetaan seuraavasti:

MESSAGE = SECURITY MODE COMMAND + UE SECURITY CAPABILITY + GSM CLASSMARKS.

Samalla tavoin kuin edellisessä esimerkissä, sekä käyttäjän laitteen turvaamisvalmiuden turvaparametreja ja GSM-kyvykkyystietoja käytetään MAC-I-koodin laskemisessa, mutta niitä ei tarvitse sisällyttää sanomaan. Tämän ratkaisun etuna on se, että matkaviestimessä tai radioverkko-ohjaimessa ei tarvita lisämuistia.

On olennaisen tärkeää, että edellä kuvatuissa ratkaisuissa ydinverkko on 3G-verkkoelementti, jolloin se kykenee ohjaamaan vähintään UMTS-radioliityntäverkkoa ja valinnaisesti myös GSM-tukiaseman alijärjestelmää.

Tämän keksinnön toteuttaminen ja sovellustavat on selitetty edellä muutamien esimerkkien avulla. On kuitenkin painotettava, ettei keksintö rajoitu pelkästään edellä oleviin yksityiskohtaisiin sovellusesimerkkeihin ja että ammattihenkilöt voivat tehdä lukuisia muutoksia ja muokkauksia ilman, että keksinnön olennaisista piirteistä silti poikettaisiin. Kuvattuja sovellustapoja on pidettävä havainnollisina, mutta ei rajoittavina. Siksi ainoastaan liitteenä olevien patenttivaatimusten tulee rajoittaa keksintöä. Siten patenttivaatimuksissa kuvatut vaihtoehtoiset toteutustavat sekä myös muut vastaavat toteutustavat lasketaan kuuluviksi keksinnön käyttöalaan.

Esimerkiksi lähderadioliityntäverkko voi olla vaikkapa UTRAN-verkko, GSM-tukiaseman alijärjestelmä, GPRS-järjestelmä, GSM Edge -järjestelmä, GSM 1800 -järjestelmä tai jokin muu järjestelmä. Vastaavasti kohderadioliityntäverkko voi olla esimerkiksi UTRAN-verkko, GSM-tukiaseman alijärjestelmä, GPRS-järjestelmä, GSM Edge -järjestelmä, GSM 1800 -järjestelmä tai jokin muu järjestelmä.

Lisäksi tiedot monitoimimatkaviestimen tukemista GSM-turva-algoritmeista (A5/1, A5/2, A5/3 jne.) voidaan lisätä osana UMTS-järjestelmän "käyttäjän laitteen radioliityntäominaisuuksia" (UE Radio Access Capability). Vaihtoehtoisesti nämä tiedot voivat sijaita erillisessä informaatioelementissä tai jopa olla osa käyttäjän laitteen turvaamisvalmiusparametria. Käytännössä nämä tiedot täytyy lisätä RRC-yhteyden avausproseduuriin (katso vaihe **500** kuviossa **5**) sekä SECURITY MODE COMMAND -sanomaan (katso vaihe **507** kuviossa **5**). Kuten aiemmin kuvatuissa muissa mahdollisissa toteutustavoissa, myös tässä tapauksessa itse (tuettuja GSM-turva-algoritmeja koskevat tiedot sisältävän) "Inter-RAT-radioyhteysominaisuudet"-informaatioelementin lisääminen RRC SECURITY MODE COMMAND -sanomaan on vain yksi vaihtoehto ja tämä informaatioelementti tarjoaa merkinannolle otsikkotietoja, koska matkaviestin ei välttämättä tarvitse itse informaatioelementtiä, vaan ainoastaan vahvistuksen siitä, että verkko on vastaanottanut sen oikein. Seuraavassa kuvataan kolme vaihtoehtoista ratkaisua eli viides, kuudes ja seitsemäs esimerkki tämän menetelmän mukaisista toteutustavoista.

Viidennessä menetelmän mukaisessa toteutusesimerkissä määritellään yksi uusi RRC-informaatioelementti, joka sisältää vain GSM-salausalgoritmiominaisuuden. Tähän tarvitaan 7 bittiä. Tämä informaatioelementti lisätään sitten RRC SECURITY MODE COMMAND -sanomaan. Tämän ratkaisun

huono puoli on, että voidakseen koodata tämän uuden informaatioelementin mainittuun sanomaan UTRAN-verkon RRC-yhteyskäytännön on ensin dekoodattava GSM-kyvykkyys 2- ja 3 -informaatioelementit, joiden koodaus/dekoodaussäännöt eivät kuulu UTRAN-verkon RRC-yhteyskäytäntöön.

Kuviossa **10** kuvataan kuudetta menetelmän mukaista toteutusesimerkkiä. UTRAN-verkon puolella vastaanotettuja GSM-kyvykkyys 2- ja 3 -tietoja (RRC-informaatioelementtiä "Inter-RAT-radioyhteysominaisuudet" **1001**) sekä käyttäjän laitteen turvaamisvalmiuksia **1002** (sisältää tiedot tuetuista UTRAN-verkon turva-algoritmeista) käytetään MAC-I-koodin (ja XMAC-I-koodin) laskemiseen RRC SECURITY MODE COMMAND –sanomaa **1000** varten. Ratkaisu on pääpiirteiltään samanlainen kuin kuvion **9** ratkaisu, sillä poikkeuksella, että (matkaviestimen eikä ydinverkon (**902**)) GSM-kyvykkyystiedot on jo vastaanotettu ja tallennettu palvelevaan radioverkko-ohjaimeen RRC-yhteyden avausvaiheen aikana (**900**). Matkaviestimeen lähetettävä SECURITY MODE COMMAND -sanoma ei sisällä "käyttäjän laitteen turvaamisvalmiuksia" eikä "käyttäjän laitteen Inter-RAT-radioyhteysominaisuuksia"; näitä informaatioelementtejä käytetään ainoastaan laskettaessa MAC-I-koodia tätä sanomaa varten.

Kuudennen toteutustavan huono puoli on, että sellaisten ylimääräisten elementtien koodaaminen ("käyttäjän laitteen turvaamisvalmiudet" ja "käyttäjän laitteen Inter-RAT-radioyhteysominaisuudet"), joita käytetään MAC-I-koodin laskemiseen, täytyy olla suoraan määritelty. Jos niin ei voida tehdä, yksinkertaisempi toteutustapa kuvataan kuviossa **11** (menetelmän seitsemäs toteutustapa). Tässä koko koodattua RRC_CONNECTION_SETUP_COMPLETE-sanomaa käytetään MAC-I-koodin (ja XMAC-I-koodin) laskemiseen RRC_SECURITY_MODE_COMMAND-sanomaa **1000** varten (sen sijasta, että käytettäisiin ainoastaan kahta informaatioelementtiä kuten kuudennessa toteutustavassa). Käytännössä tämä tarkoittaa, että RRC-yhteyden avausproseduurin aikana (katso vaihe **500** kuviossa **5**), kun RRC_CONNECTION_SETUP_COMPLETE-sanoma lähetetään, matkaviestimen täytyy tallentaa kopio koodatusta sanomasta muistiinsa, kunnes se vastaanottaa SECURITY_MODE_COMMAND-sanoman ja on tarkistanut eheystarkistussumman. Verkon puolella (UTRAN-verkon ollessa kyseessä palvelevassa radioverkko-ohjaimessa) kopio vastaanotetusta (ei-koodatusta) RRC_CONNECTION_SETUP_COMPLETE-sanomasta täytyy säilyttää muistissa, kunnes MAC-I-koodi SECURITY_MODE_COMMAND-sanomaa varten

on laskettu. Toteutuksen kannalta on luultavasti melko helppoa tallentaa koko koodattu sanoma muistiin ennen kuin se lähetetään (käyttäjän laitteen puolella) tai heti sen vastaanottamisen jälkeen ja ennen kuin se on lähetetty edelleen dekooderille (UTRAN-verkon puolella). Siten MAC-I-koodi SECURITY_MODE_COMMAND-sanomaa varten laskettaisiin asettamalla MESSAGE-syöttöparametri eheysalgoritmiin seuraavasti:

MESSAGE = SECURITY_MODE_COMMAND +
RRC_CONNECTION_SETUP_COMPLETE

Menetelmän kuudenteen toteutusesimerkkiin verrattuna tämän toteutustavan huono puoli on, että ratkaisu vaatii hieman enemmän muistia sekä matkaviestimessä että verkon puolella. Matkaviestimen tukemat salausalgoritmit sisältyvät GSM-kyvykkyystietoihin.

Patenttivaatimukset

1. Matkaviestinjärjestelmä, jolle on tunnusomaista, että se koostuu seuraavista:

joukosta radioliityntäverkkoja, jotka tarjoavat matkaviestimille yhteyden vähintään yhteen ydinverkkoon;

monimuotomatkaviestimestä, joka lähettää ensimmäiseen radioliityntäverkkoon yhteyttä muodostaessaan vähintään yhden suojaamattoman merkinannon aloitussanoman sekä tiedot toisessa radioliityntäverkossa olevan monimuotomatkaviestimen tukemista salausalgoritmeista;

ydinverkosta, joka vastaanottaa salausalgoritmeja koskevat tiedot, ja jossa ensimmäinen radioliityntäverkko on mukautettu vastaanottamaan komentosanoman ydinverkolta, joka antaa monimuotomatkaviestimelle ohjeet suojata kaikki seuraavaksi siirrettävät tiedot:

muodostamaan ja lähettämään monimuotomatkaviestimelle eheyssuojatun komentosanoman, joka sisältää tiedot monimuotomatkaviestimen toisessa radioliityntäverkossa tukemista salausalgoritmeista, jolloin suojattu komentosanoma koostuu hyötyinformaatiosta ja sanomantunnistuskoodista, ja

jossa monimuotomatkaviestin on mukautettu päättelemään, vastaavatko eheyssuojatussa komentosanomassa vastaanotetut salausalgoritmeja koskevat tiedot monimuotomatkaviestimen tietoja, jotka se on lähettänyt merkinannon aloitussanomissa.

2. Patenttivaatimuksen 1 mukainen järjestelmä, jolle on tunnusomaista, että suojaamaton merkinannon aloitussanoma lähetetään suoritettaessa kanavanvaihto ydinverkosta, joka koostuu vähintään yhdestä matkaviestinliikenteen pakettivälitteisen liikenteen kytkentäelementistä, piirikytkentäisen matkaviestinliikenteen kytkentäkeskukseen.

3. Patenttivaatimuksen 1 mukainen järjestelmä, jolle on tunnusomaista, että ensimmäinen radioliityntäverkko liittää tiedot komentosanomassa vastaanotetuista salausalgoritmeista suojatun komentosanoman hyötyinformaatioon ja lisää hyötyinformaation algoritmiin laskemalla sanomantunnistuskoodin.

4. Patenttivaatimuksen 1 mukainen järjestelmä, jolle on tunnusomaista, että ensimmäinen radioliityntäverkko tallentaa suojaamattoman

monimuotomatkaviestimeltä vastaanotetun merkinannon aloitussanoman ja käyttää tätä sanomaa sanomantunnistuskoodin laskemisessa.

5. Patenttivaatimuksen 1 mukainen järjestelmä, jolle on tunnusomaista, että ensimmäinen radioliityntäverkko tallentaa suojaamattoman merkinannon aloitussanoman hyötyinformaation, jonka se on vastaanottanut monimuotomatkaviestimeltä, ja käyttää tätä hyötyinformaatiota sanomantunnistuskoodin laskemisessa.

6. Patenttivaatimuksen 1 mukainen järjestelmä, jolle on tunnusomaista, että ensimmäinen radioliityntäverkko tallentaa matkaviestimen ominaisuuksia koskevat tiedot, jotka se on vastaanottanut matkaviestimeltä yhteyden avaamisen aikana, ja käyttää näitä tietoja sekä ydinverkolta vastaanottamaansa komentosanomaan sulautettuja salausalgoritmeja koskevia tietoja sanomantunnistuskoodin laskemisessa.

7. Patenttivaatimuksen 1 tai 6 mukainen järjestelmä, jolle on tunnusomaista, että matkaviestin lähettää salausalgoritmeja koskevat tiedot yhteyttä avattaessa, ensimmäinen radioliityntäverkko tallentaa nämä tiedot ja käyttää niitä muodostaessaan suojatun komentosanoman.

8. Radioliityntäverkko, jolle on tunnusomaista, että se tarjoaa monimuotomatkaviestimille yhteyden vähintään yhteen ydinverkkoon,

jolloin radioliityntäverkko on mukautettu niin, että se

vastaanottaa ilmarajapinnan kautta monimuotomatkaviestimeltä suojaamattoman merkinantosanoman, joka sisältää tiedot monimuotomatkaviestimen toisessa radioliityntäverkossa tukemista salausalgoritmeista, ja lähettää tiedot edelleen ydinverkolle,

vastaanottaa ydinverkolta ensimmäisen komentosanoman, joka ohjeistaa monimuotomatkaviestimen suojaamaan kaikki seuraavat siirrettävät tiedot;

muodostaa toisen komentosanoman, joka sisältää hyötyinformaation ja sanomantunnistuskoodin,

laskee sanomantunnistuskoodin käyttämällä yhtenä laskentaparametrina tietoja monimuotomatkaviestimen toisessa verkossa tukemista salausalgoritmeista, ja

lähettää toisen komentosanoman monimuotomatkaviestimelle.

9. Patenttivaatimuksen 8 mukainen radioliityntäverkko, jolle on tunnusomaista, että salausalgoritmeja koskevat tiedot liitetään toisen komentosanoman hyötyinformaatioon.

10. Patenttivaatimuksen 8 mukainen radioliityntäverkko, jolle on tunnusomaista, että monimuotomatkaviestimeltä vastaanotettu suojaamaton merkinannon aloitussanoma tallennetaan ja että tätä sanomaa käytetään sanomantunnistuskoodin laskemisessa.

11. Patenttivaatimuksen 8 mukainen radioliityntäverkko, jolle on tunnusomaista, että monimuotomatkaviestimeltä vastaanotettu suojaamattoman merkinannon aloitussanoman hyötyinformaatio tallennetaan ja että tallennettua hyötyinformaatiota käytetään sanomantunnistuskoodin laskemisessa.

12. Patenttivaatimuksen 8 mukainen radioliityntäverkko, jolle on tunnusomaista, että monimuotomatkaviestimen tukemia salausalgoritmeja koskevat tiedot liitetään sanomaan, joka lähetettiin yhteyttä muodostettaessa ennen suojaamatonta merkinantosanomaa, ja että näitä tietoja käytetään sanomantunnistuskoodin laskemisessa.

Patentkrav

1. Mobiltelekommunikationssystem, k ä n n e t e c k n a t av att det består av

en mängd radioaccessnät som erbjuder mobilstationer åtkomst till minst ett kärnnät;

en multimodmobilstation som vid uppkoppling av en förbindelse till ett första radioaccessnät sänder minst ett oskyddat initialt signaleringsmeddelande och information om krypteringsalgoritmer som en multimodmobilstation i ett andra radioaccessnät stöder,

ett kärnnät som mottar informationen om krypteringsalgoritmerna, och där det första radioaccessnätet är anordnat att från kärnnätet motta ett kommandomeddelande som råder multimodmobilstationen att chiffrera all information som skall överföras näst;

att skapa och att till multimodmobilstationen sända ett integritetsskyddat kommandomeddelande som innehåller information om de krypteringsalgoritmer som multimodmobilstationen i det andra radioaccessnätet stöder, varvid det skyddande kommandommeddelandet består av nyttoinformation och en meddelandeautenticeringskod, och

där multimodmobilstationen är anordnad att dra en slutsats om den i det integritetsskyddade kommandomeddelandet mottagna informationen om krypteringsalgoritmerna motsvarar den information som multimodmobilstationen har sänt i de initiala signaleringsmeddelandena.

2. System enligt patentkrav 1, k ä n n e t e c k n a t av att det oskyddade initiala signaleringsmeddelandet sänds vid utförande av en handover från kärnnätet, som består av minst ett mobiltelekommunikationskopplingselement för paketförmedlande kommunikation, till en mobiltelekommunikationskopplingscentral för kretskopplad kommunikation.

3. System enligt patentkrav 1, k ä n n e t e c k n a t av att det första radioaccessnätet fogar informationen om de i kommandomeddelandet mottagna krypteringsalgoritmerna till nyttoinformationen i det skyddade kommandomeddelandet och lägger till nyttoinformationen i en algoritm genom att beräkna meddelandeautenticeringskoden.

4. System enligt patentkrav 1, k ä n n e t e c k n a t av att det första radioaccessnätet lagrar det från multimodmobilstationen mottagna oskyddade initiala signaleringsmeddelandet och använder detta meddelande vid beräkningen av meddelandeautenticeringskoden.

5. System enligt patentkrav 1, k ä n n e t e c k n a t av att det första radioaccessnätet lagrar det oskyddade initiala signaleringsmeddelandets nyttoinformation som det har mottagit från multimodmobilstationen och använder denna nyttoinformation vid beräkningen av meddelandeautenticeringskoden.

6. System enligt patentkrav 1, k ä n n e t e c k n a t av att det första radioaccessnätet lagrar information om mobilstationens egenskaper, vilken information det har mottagit från mobilstationen under förbindelseuppkopplingen, och använder denna information samt information om krypteringsalgoritmerna, vilken information finns införlivad i det från kärnnätet mottagna kommandomeddelandet, vid beräkningen av meddelandeautenticeringskoden.

7. System enligt patentkrav 1 eller 6, k ä n n e t e c k n a t av att mobilstationen sänder informationen om krypteringsalgoritmerna under förbindelseuppkopplingen, det första radioaccessnätet lagrar nämnda information och använder nämnda information vid skapandet av det skyddade kommandomeddelandet.

8. Radioaccessnät, k ä n n e t e c k n a t av att det erbjuder multimodmobilstationer åtkomst till minst ett kärnnät,

varvid radioaccessnätet är anordnat att

via ett luftgränssnitt från en multimodmobilstation motta ett oskyddat signaleringsmeddelande som innehåller information om krypteringsalgoritmer som en multimodmobilstation i ett annat radioaccessnät stöder och att sända informationen vidare till kärnnätet,

att från kärnnätet motta ett första kommandomeddelande som råder multimodmobilstationen att chiffrera all information som skall överföras näst;

att skapa ett andra kommandomeddelande som innehåller nyttoinformation och en meddelandeautenticeringskod,

att beräkna meddelandeautenticieringskoden genom att som en beräkningsparameter använda informationen om de krypteringsalgoritmer som multimodmobilstationen i det andra nätet stöder, och

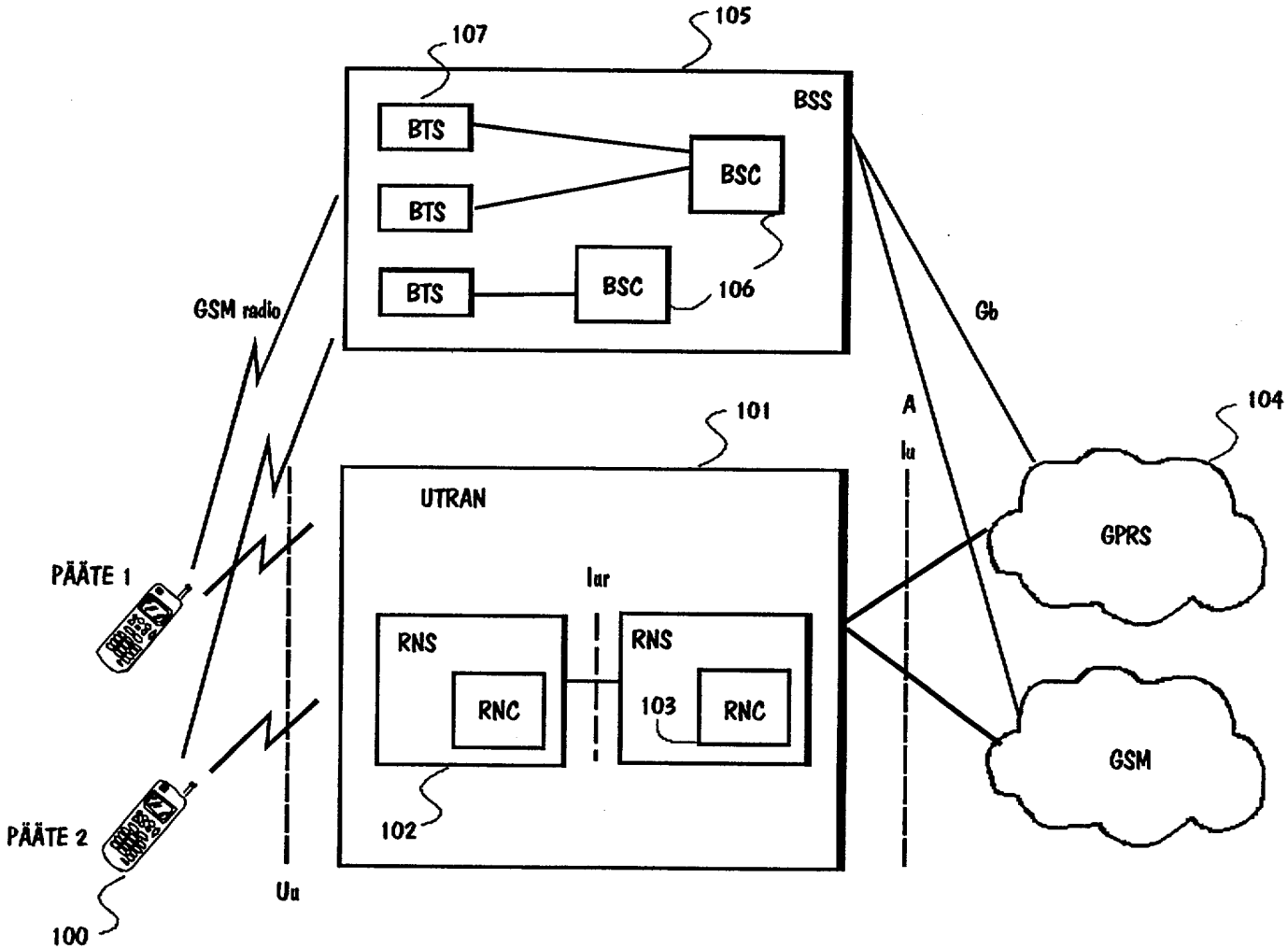
att sända det andra kommandomeddelandet till multimodmobilstationen.

9. Radioaccessnät enligt patentkrav 8, k ä n n e t e c k n a t av att informationen om krypteringsalgoritmerna fogas till nyttoinformationen i det andra kommandomeddelandet.

10. Radioaccessnät enligt patentkrav 8, k ä n n e t e c k n a t av att det från multimodmobilstationen mottagna oskyddade initiala signaleringsmeddelandet lagras och att detta meddelande används vid beräkningen av meddelandeautenticeringskoden.

11. Radioaccessnät enligt patentkrav 8, k ä n n e t e c k n a t av att det oskyddade initiala signaleringsmeddelandets nyttoinformation som har mottagits från multimodmobilstationen lagras och att den lagrade nyttoinformationen används vid beräkningen av meddelandeautenticeringskoden.

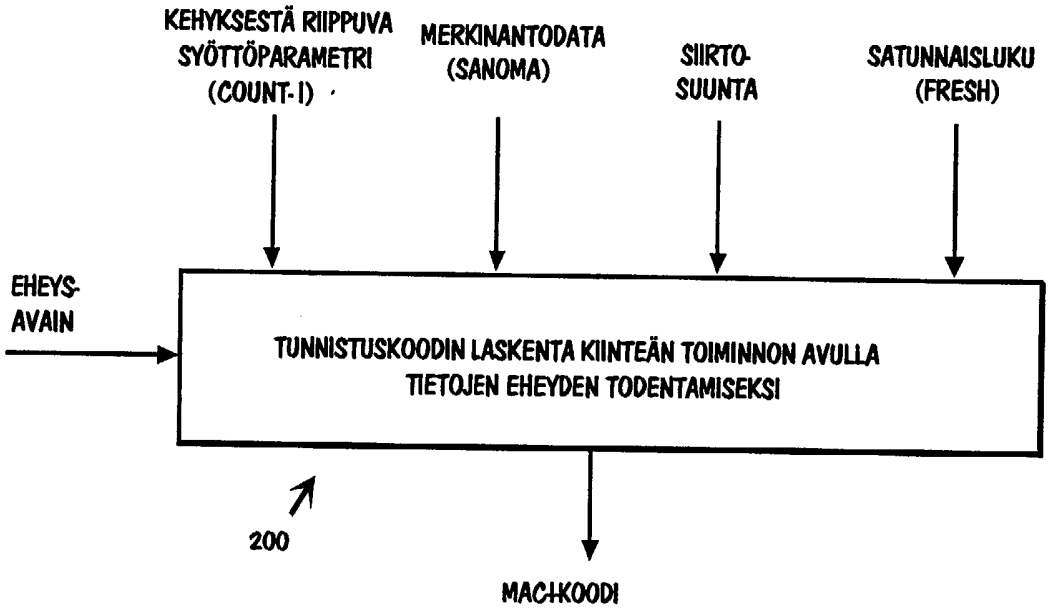
12. Radioaccessnät enligt patentkrav 8, k ä n n e t e c k n a t av att informationen om de krypteringsalgoritmer som multimodmobilstationen stöder fogas till ett meddelande som sändes vid förbindelseuppkopplingen före det oskyddade signaleringsmeddelandet och att denna information används vid beräkningen av meddelandeautenticeringskoden.



Kuvio 1

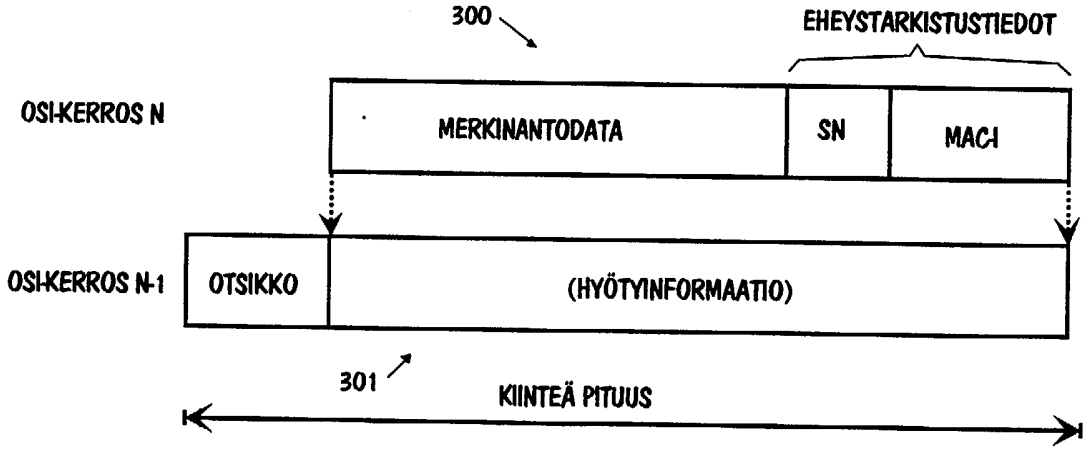
TEKNIIKAN TASO

RUNKOVERKOT



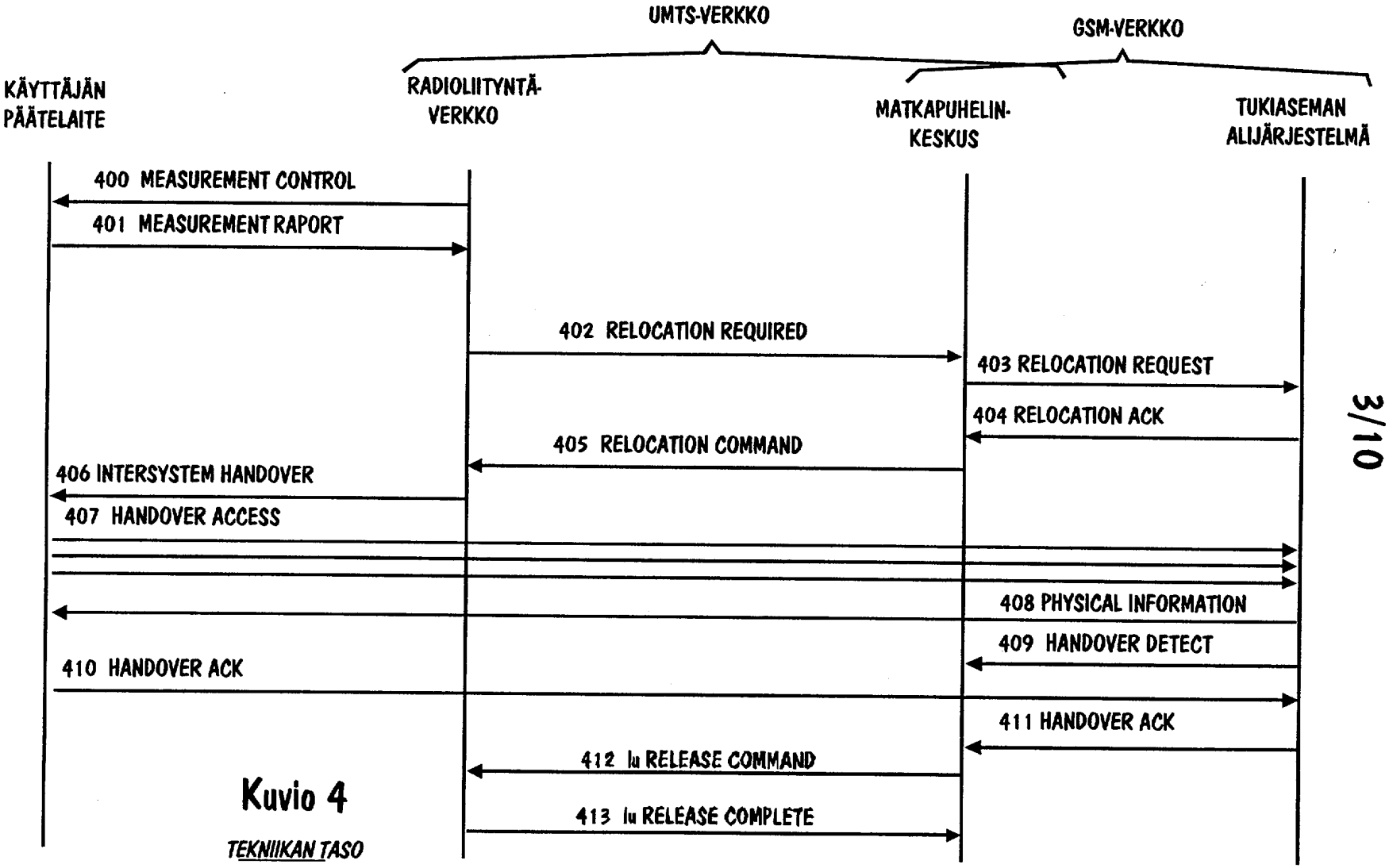
TEKNIIKAN TASO

Kuvio 2



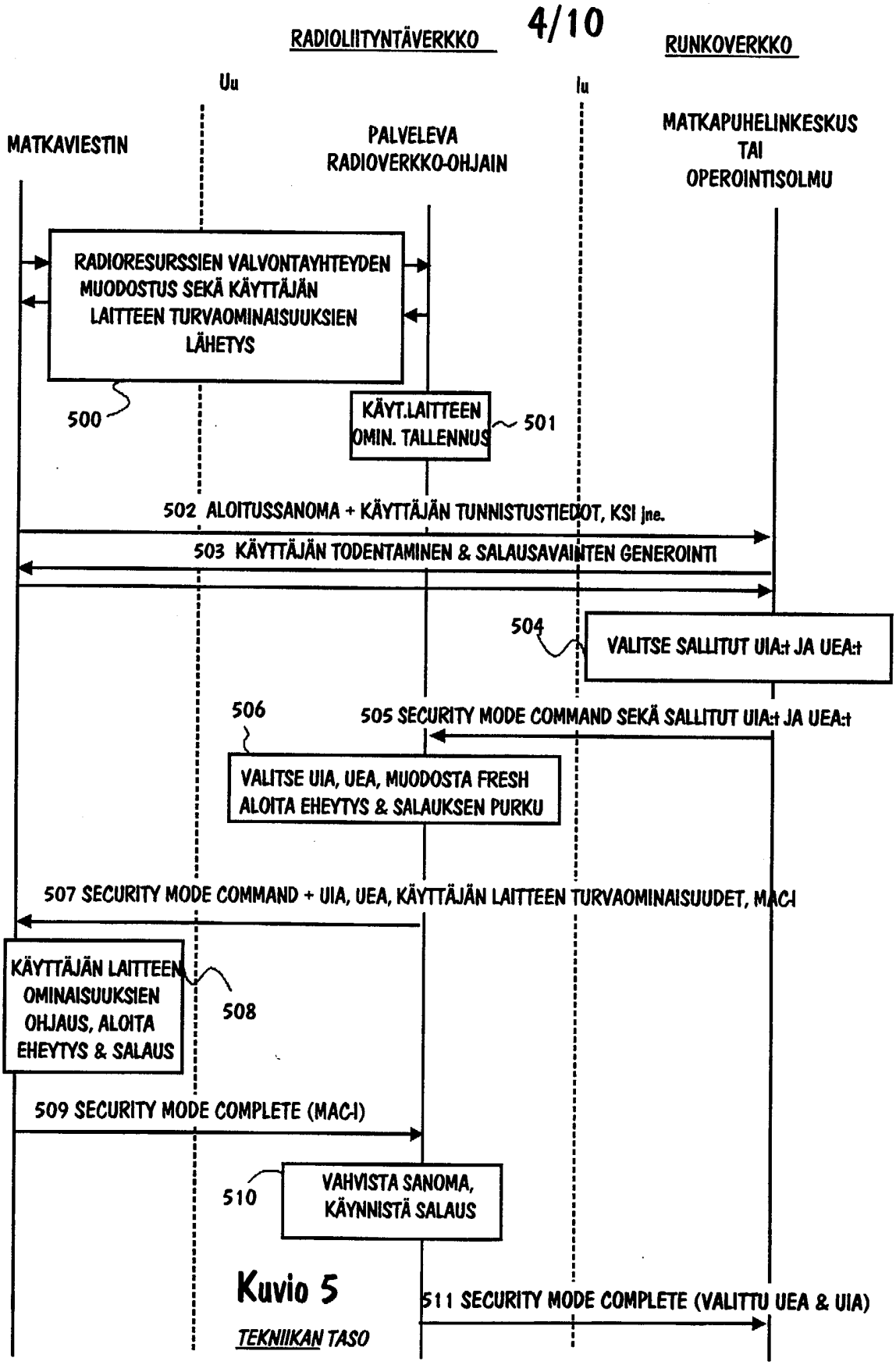
TEKNIIKAN TASO

Kuvio 3



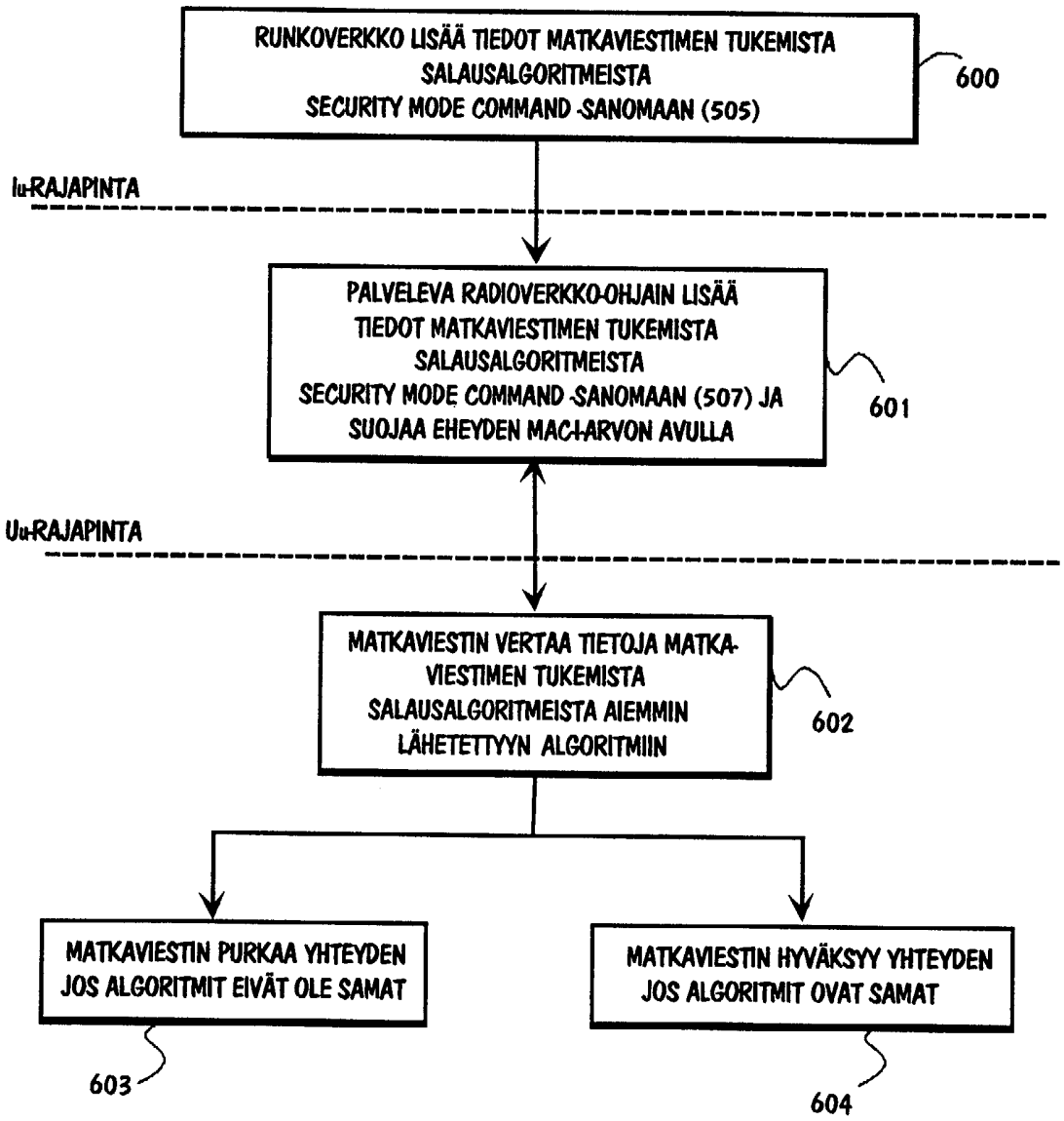
Kuvio 4

TEKNIIKAN TASO



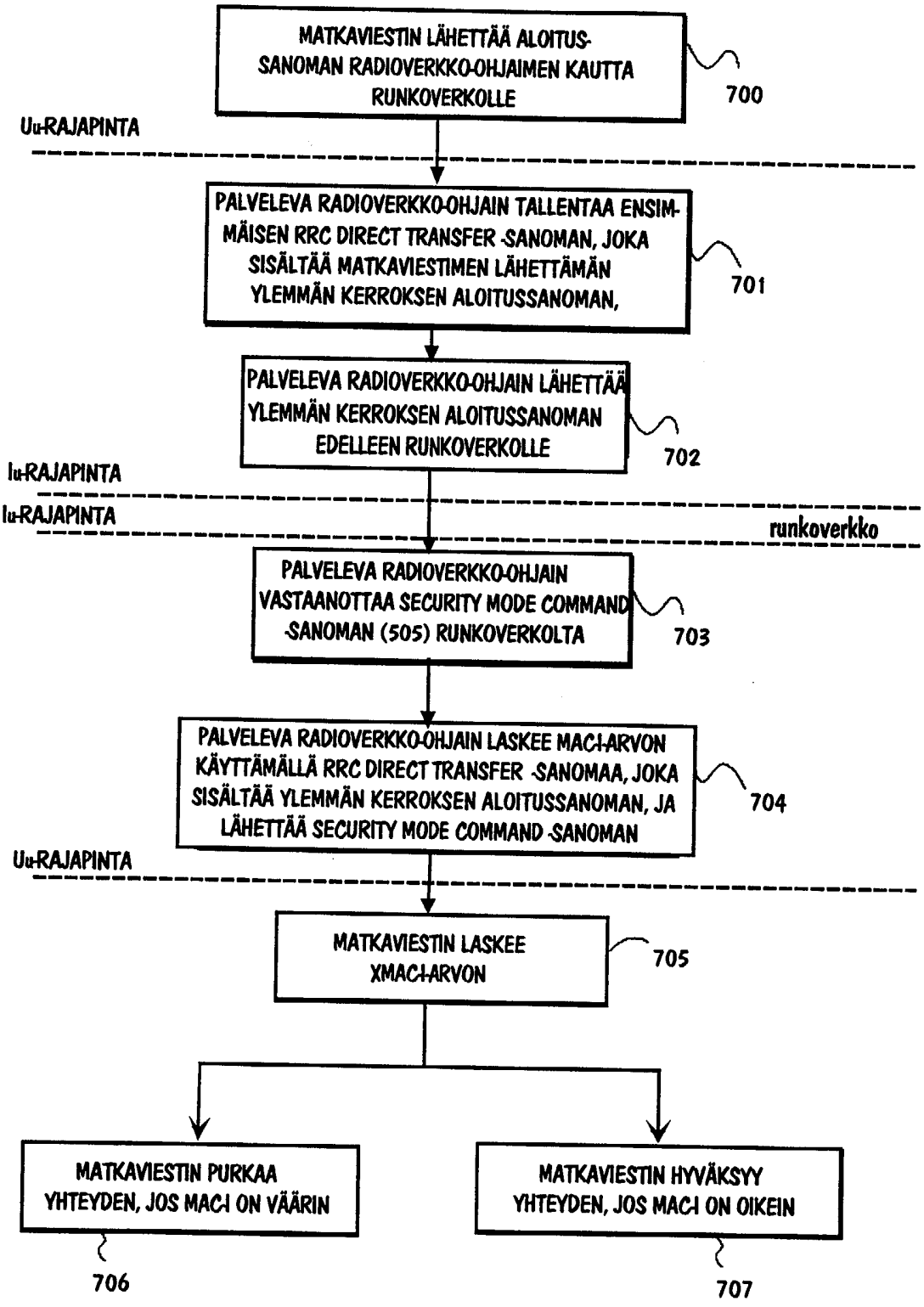
Kuvio 5

TEKNIIKAN TASO



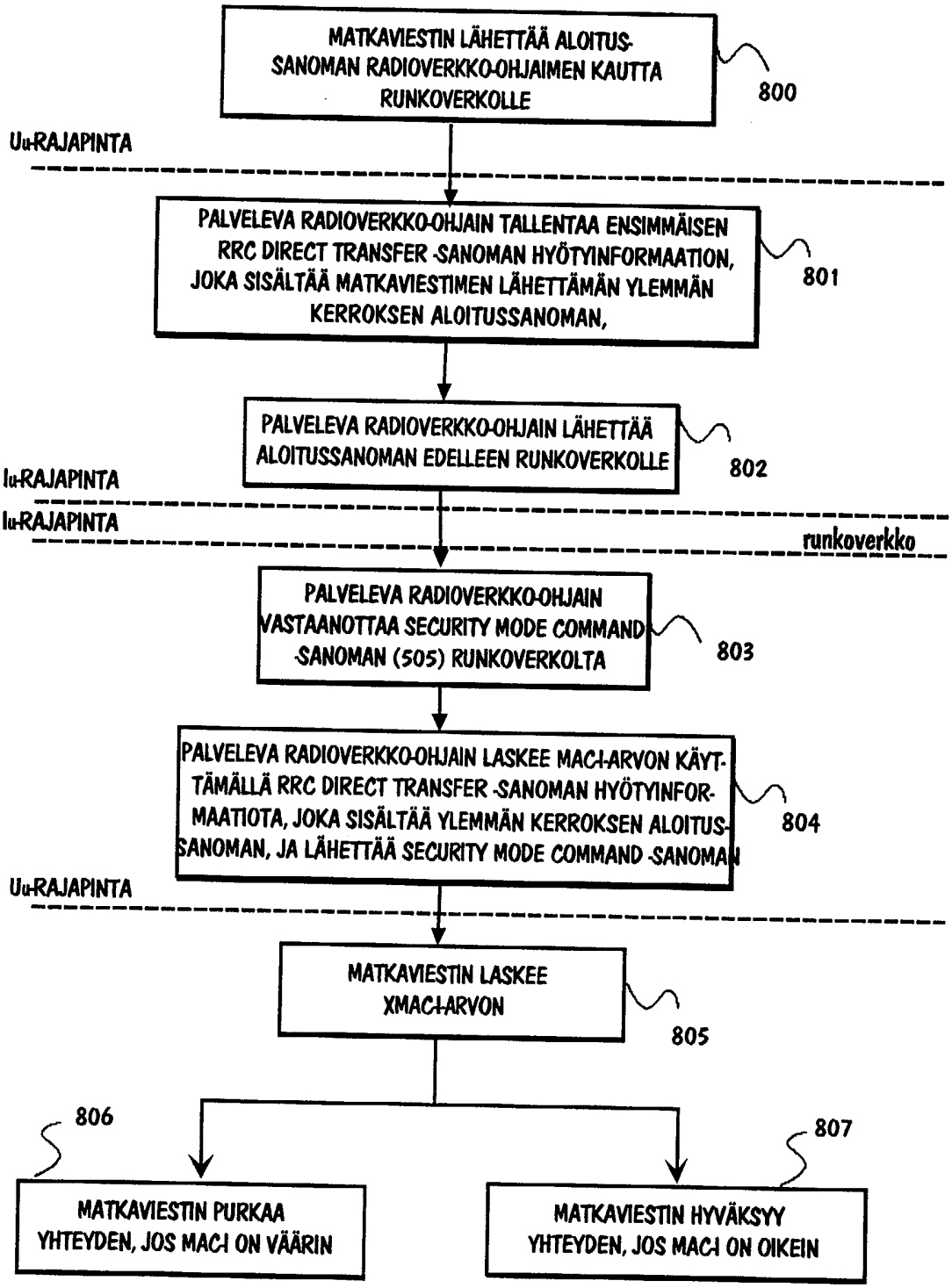
RATKAISU 1

Kuvio 6



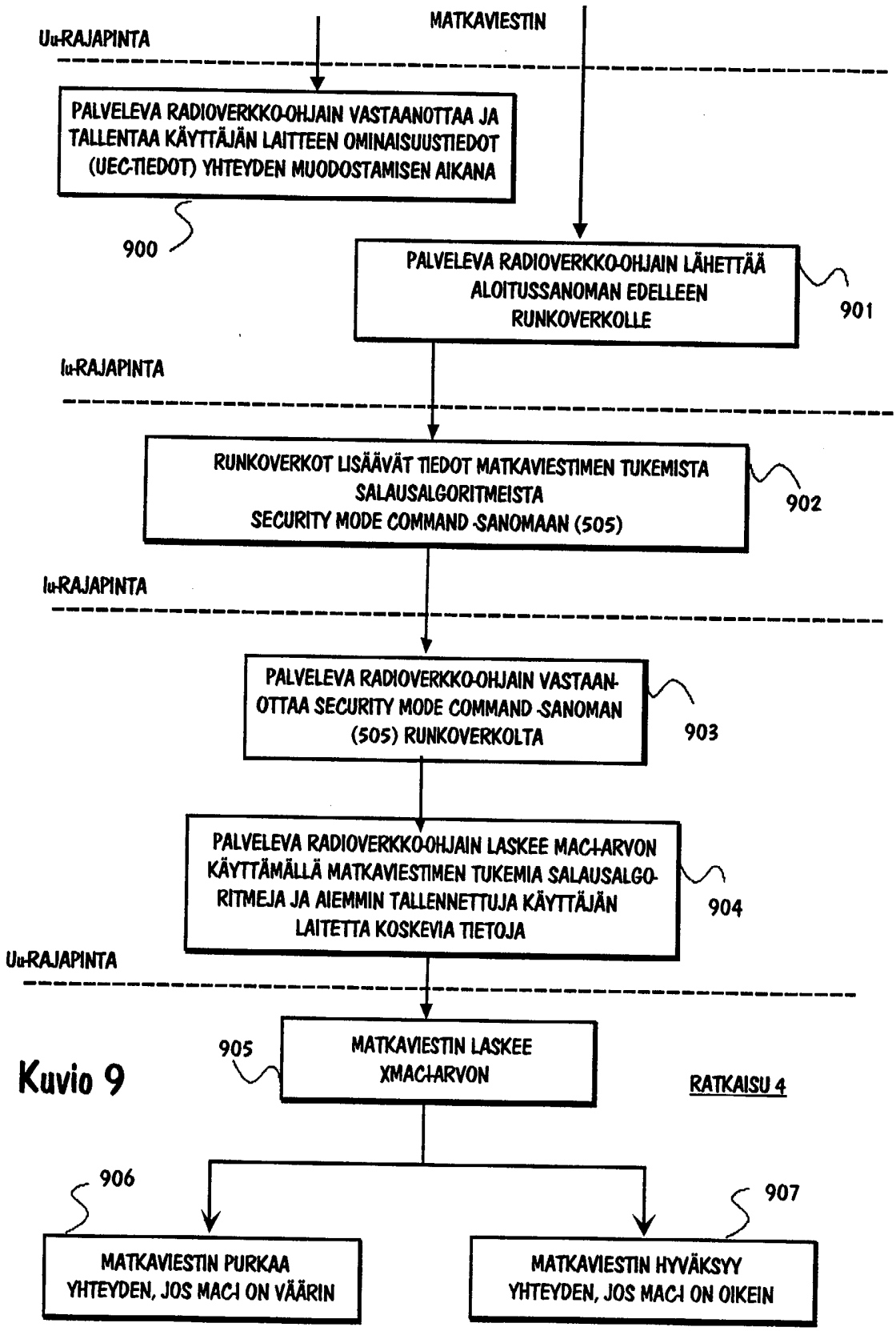
Kuvio 7

RATKAISU 2

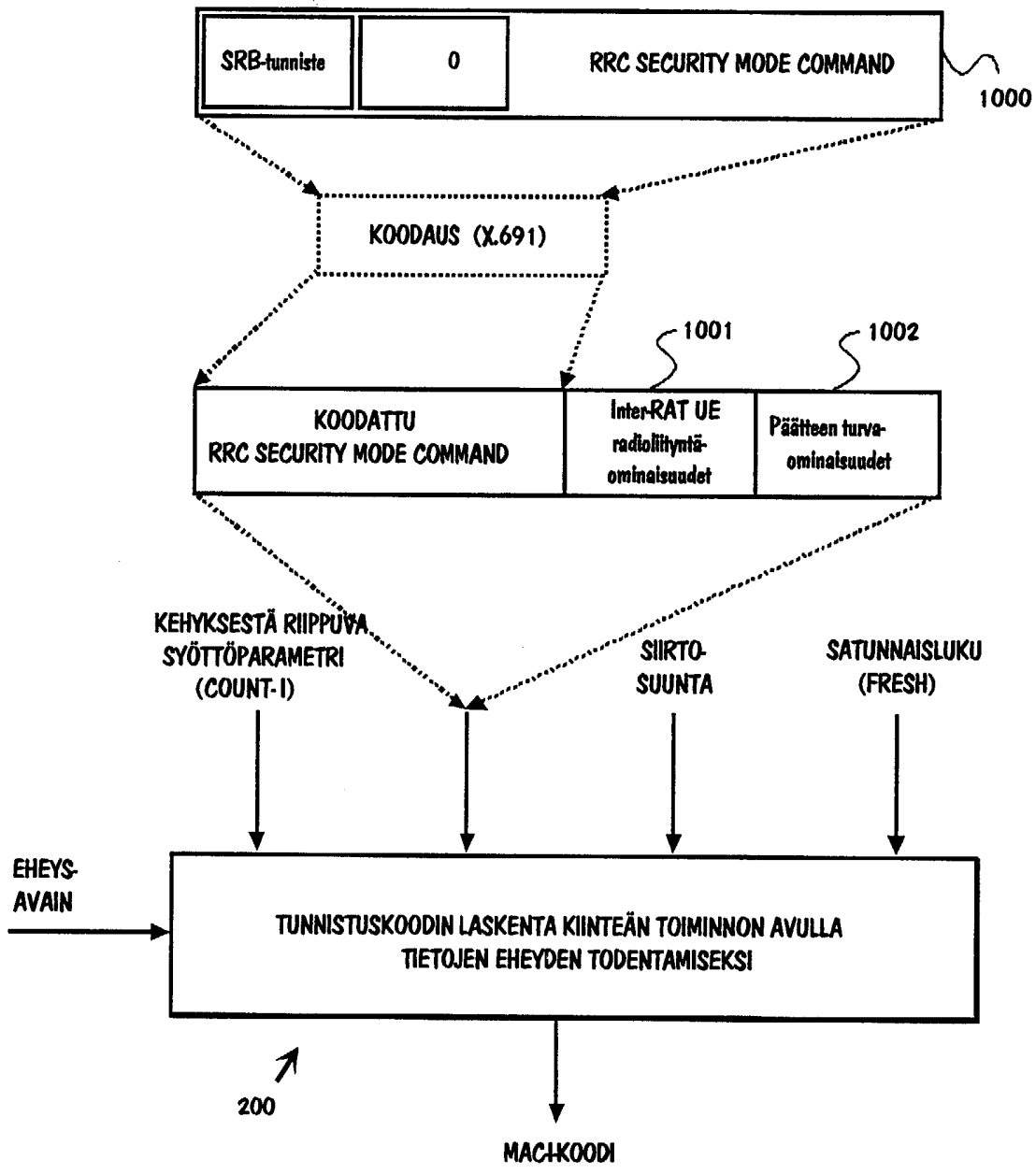


RATKAISU 3

Kuvio 8

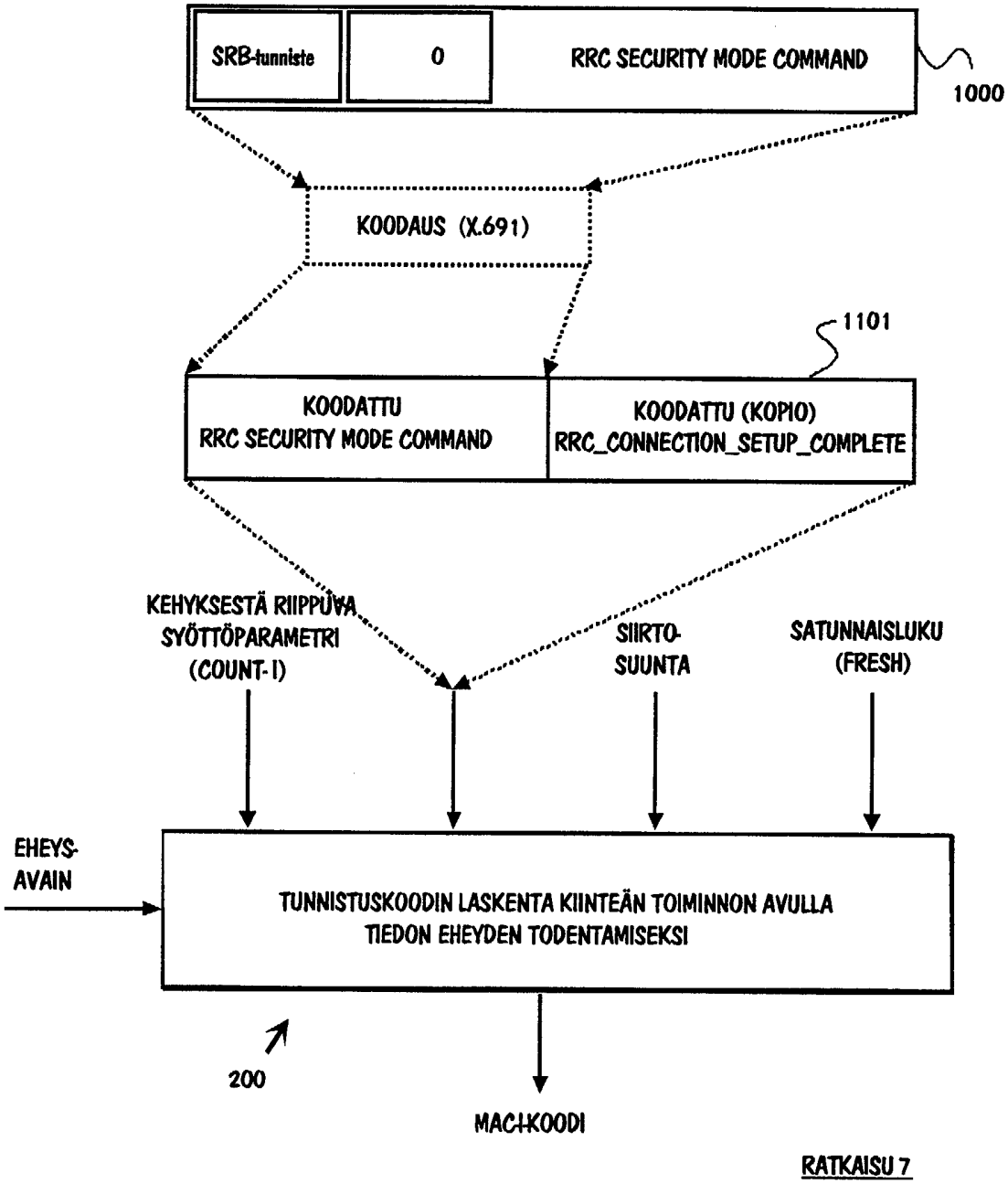

MATKAVIESTIN
Uu-RAJAPINTA
PALVELEVA RADIOVERKKO-OHJAIN VASTAANOTTAA JA TALLENTAA KÄYTTÄJÄN LAITTEEN OMINAISUUSTIEDOT (UEC-TIEDOT) YHTEYDEN MUODOSTAMISEN AIKANA
900
PALVELEVA RADIOVERKKO-OHJAIN LÄHETTÄÄ ALOITUSSANOMAN EDELLEEN RUNKOVERKOLLE
901
Iu-RAJAPINTA
RUNKOVERKOT LISÄÄVÄT TIEDOT MATKAVIESTIMEN TUKEMISTA SALAUSALGORITMEISTA SECURITY MODE COMMAND -SANOMAAN (505)
902
Iu-RAJAPINTA
PALVELEVA RADIOVERKKO-OHJAIN VASTAANOTTAA SECURITY MODE COMMAND -SANOMAN (505) RUNKOVERKOLTA
903
PALVELEVA RADIOVERKKO-OHJAIN LASKEE MAC-I-ARVON KÄYTTÄMÄLLÄ MATKAVIESTIMEN TUKEMIA SALAUSALGORITMEJA JA AIEMMIN TALLENNETTUJA KÄYTTÄJÄN LAITETTA KOSKEVIA TIETOJA
904
Uu-RAJAPINTA
905
MATKAVIESTIN LASKEE XMAC-I-ARVON
RATKAISU 4
906
MATKAVIESTIN PURKAA YHTEYDEN, JOS MAC-I ON VÄÄRIN
907
MATKAVIESTIN HYVÄKSYY YHTEYDEN, JOS MAC-I ON OIKEIN

Kuvio 9



RATKAISU 6

Kuvio 10


SRB-tunniste
0
RRC SECURITY MODE COMMAND
1000
KOODAUS (X.691)
1101
KOODATTU
RRC SECURITY MODE COMMAND
KOODATTU (KOPIO)
RRC_CONNECTION_SETUP_COMPLETE
KEHYKSESTÄ RIIPPUVA
SYÖTTÖPARAMETRI
(COUNT-I)
SIIRTO-
SUUNTA
SATUNNAISLUKU
(FRESH)
EHEYS-
AVAIN
TUNNISTUSKOODIN LASKENTA KIINTEÄN TOIMINNON AVULLA
TIEDON EHEYDEN TODENTAMISEKSI
200
MAC-I-KOODI
RATKAISU 7

Kuvio 11