(19) SUOMI - FINLAND
(FI)

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

(10) **FI 20021684 A7**

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

(21) Patenttihakemus - Patentansökan - Patent application 20021684

(51) Kansainvälinen patenttiluokitus - Internationell patentklassifikation - International patent classification
H04L 12/46
H04L 9/32
H04Q 7/22
H04Q 7/32
H04L 12/56 (2006.01)
H04L 12/70 (2013.01)

(22) Tekemispäivä - Ingivningsdag - Filing date **20.09.2002**

(23) Saapumispäivä - Ankomstdag - Reception date **20.09.2002**

(41) Tullut julkiseksi - Blivit offentlig - Available to the public **21.03.2004**

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

(71) Hakija - Sökande - Applicant

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

(72) Keksijä - Uppfinnare - Inventor

1 • **Haverinen, Henry,** Tampere, SUOMI - FINLAND, (FI)
2 • **Ahmavaara, Kalle,** Espoo, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud - Agent

Kolster Oy Ab, Iso Roobertinkatu 23, 00120 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning - Title of the invention
Osoitteen verifiointi tietoliikennejärjestelmässä
Verifiering av en adress i ett telekommunikationssystem

(57) Tiivistelmä - Sammandrag - Abstract

Keksintö liittyy IP-osoitteen verifioimiseen tietoliikennejärjestelmässä, jossa tiedonsiirtoyhteys voidaan muodostaa julkiseen matkaviestinverkkoon paikallisen verkon kautta. Päätelaitteessa muodostetaan paikallisessa verkossa allokoidun IP-osoitteen käsittävä signalointiviesti, jossa ainakin mainittu IP-osoite on eheyssuojattu. Signalointiviesti lähetetään päätelaitteesta julkiseen matkaviestinverkkoon paikallisen verkon kautta käyttäen signalointiviestin kantavan IP-datagrammin lähdeosoitteena allokoitua IP-osoitetta. Julkisessa matkaviestinverkossa tarkastetaan vastaanotetun IP-datagrammin käsittämän signalointiviestin käsittämän IP-osoitteen eheys. Julkisessa matkaviestinverkossa verrataan IP-datagrammin lähde-IP-osoitetta signalointiviestin sisältämään IP-osoitteeseen, jos signalointiviestin käsittämää IP-osoitetta ei ole eheystarkastuksen perusteella muokattu. IP-osoitetta käytetään päätelaitteen tunnisteena julkisessa matkaviestinverkossa, jos IP-datagrammin lähde-IP-osoite on sama kuin signalointiviestin käsittämä IP-osoite.(Kuvio 2)

Uppfinningen avser verifiering av en IP-adress i ett telekommunikationssystem, i vilket en dataöverföringsförbindelse kan bildas till ett offentligt mobiltelefonnät via ett lokalt nät. I en terminalapparat bildas ett signaleringsbudskap bestående av en i sagda lokala nät allokerad IP-adress, där åtminstone sagda IP-adress är helhetsskyddad. Sagda signaleringsbudskap sänds från terminalapparaten till sagda offentliga mobiltelefonnät via ett lokalt nät genom att som signaleringsbudskapets bärande IP-datagrams källadress använda den allokerade IP-adressen. I sagda offentliga mobiltelefonnät granskas helheten hos IP-adressen som omfattas av det i sagda signaleringsbudskap mottagna IP-datagrammet. I sagda offentliga mobiltelefonnät jämförs IP-datagrammets käll-IP-adress med den i sagda signaleringsbudskap ingående IP-adressen, ifall den i sagda signaleringsbudskap ingående IP-adressen inte på basen av sagda helhetsgranskning har modifierats. Sagda IP-adress används son identi-fieringstecken för terminalapparaten i sagda offentliga mobiltelefonnät, ifall IP-datagrammets käll-IP-adress är den samma som den i sagda signaleringsbudskap ingående IP-adressen.

Osoitteen verifiointi tietoliikennejärjestelmässä

Keksinnön tausta

Keksintö liittyy päätelaitteelle osoitetun osoitteen verifioimiseen, erityisesti osoitteen verifioimiseen tietoliikennejärjestelmässä, joka käsittää paikallisen langattoman liityntäverkon ja julkisen matkaviestinverkon (PLMN; Public Land Mobile Network).

Peittoalueeltaan erittäin kattavia ja käyttäjän liikkuvuutta hyvin tukevia julkisia matkaviestinverkkoja varten kehitetyt datapalvelut ovat kehittyneet huomattavasti viime vuosina. Pakettivälitteinen GPRS-palvelu (General Packet Radio Service) tarjoaa GSM-verkkoja varten tehokkaan datavälityksen, jossa radiokapasiteettia on varattuna ainoastaan pakettien siirron aikana. 3GPP:n (Third Generation Partnership Project) standardoima kolmannen sukupolven UMTS-järjestelmä (Universal Mobile Telecommunications System) tulee tarjoamaan GSM/GPRS-verkkojakin suuremman datan välityskapasiteetin.

PLMN-verkkojen tarjoamien datapalveluiden lisäksi on kehitetty useita erilaisia langattomia paikallisia verkkoja, jotka tarjoavat hyvin rajallisella peittoalueelta laajakaistaisen langattoman datasiirtopalvelun. Eräitä tällaisia tekniikoita ovat IEEE 802.11 –pohjaiset WLAN-verkot. Näitä paikallisia verkkoja voidaan käyttää tarjoamaan erilaisissa aktiivikohdissa (hot spot), kuten toimistoissa tai lentokentillä, erittäin nopean datansiirron ja pääsyn Internetiin. Myös langattomien lähiverkkojen ja PLMN-verkkojen konvergoitumista on tapahtunut. Esimerkiksi GSM-teknologiaan perustuvia tukiasemia voidaan käyttää toimiston tietojärjestelmässä langattoman yhteyden järjestämiseen toimiston lähiverkkoon. Toisaalta myös langattomia lähiverkkoja varten on suunniteltu verkkoelementtejä, joiden avulla paikallinen verkko voi hyödyntää PLMN-verkkoa. Esimerkiksi IEEE 802.11-standardin mukaisia WLAN-verkkoja ja GSM-verkkoja varten on kehitetty verkkoelementtejä, joiden avulla WLAN-verkon kautta päästään GSM-verkon tarjoamiin todentamis- ja laskutuspalveluihin. PLMN-verkkojen ja langattomien lähiverkkojen yhteistoimintaa on suunniteltu myös pidemmälle niin, että langattomien lähiverkkojen tarjoaman radiorajapinnan kautta voitaisiin käyttää PLMN-verkkojen palveluita. UMTS-järjestelmässä, jota kutsutaan myös 3GPP-järjestelmäksi (3GPP System), langaton lähiverkko voisi toimia yhtenä liityntäalijärjestelmänä.

Kun päätelaite muodostaa yhteyttä langattoman lähiverkon liityntäpisteeseen (Access Point), langattomasta lähiverkosta voidaan muodostaa yhteys julkisessa matkaviestinverkossa todentamispalveluita tarjoavaan verk-

koelementtiin. Verkkoelementti voi todentaa päätelaitteen esimerkiksi SIM-yksikön (Subscriber Identity Module) laskeman todentamisvasteen perusteella. Tällöin päätelaite identifioidaan ja todennetaan julkisessa matkaviestinverkossa PLMN-verkossa käytettävän yhden tai useamman tunnisteen, esimerkiksi GSM-verkon IMSI-tunnisteen (International Mobile Subscriber Identity) perusteella. Tällöin IMSI-tunniste verifioidaan esimerkiksi GSM-järjestelmän todentamismekanismeja käyttäen. Kun päätelaite on todennettu, sille voidaan allokoida IP-osoite, johon käyttäjä- ja/tai signalointidatan siirto päätelaitteeseen/-sta perustuu. Tämä aiheuttaa turvallisuusongelman, sillä vilpillinen päätelaite voi siepata päätelaitteen ja julkisen matkaviestinverkon välisiä signalointiviestejä ja korvata viesteihin oma IP-osoitteensa. Julkinen matkaviestinverkko ei havaitse, että paketti ei tule oikeasta päätelaitteesta, vaan se vastaa vilpillisen päätelaitteen IP-osoitteeseen ja näin ollen vilpillinen päätelaite voi häiritä verkon toimintaa. Erityinen ongelma on tilanteessa, jossa päätelaite rekisteröityy julkiseen matkaviestinverkkoon paikallisen verkon kautta. Jos rekisteröintiviesti siepataan, julkinen matkaviestinverkko rekisteröi päätelaitteen IP-osoitteeksi vilpillisen päätelaitteen valitseman osoitteen. Tällöin päätelaitteen liikenne ohjautuisi vilpilliselle päätelaitteelle. Tällöin kaappaaja saisi kaiken oikealle päätelaitteelle tarkoitetun liikenteen, joka saattaa olla käytettävästä protokollasta riippuen jopa selväkielistä (näin olisi esimerkiksi IEEE 802.11i –protokollaa käytettäessä).

Keksinnön lyhyt selostus

Keksinnön tavoitteena on kehittää sellainen menetelmä ja menetelmän toteuttava laitteisto, että edellä mainittu epäkohta voidaan välttää. Keksinnön tavoitteet saavutetaan menetelmällä, tietoliikennejärjestelmällä, päätelaitteella ja verkkoelementillä, joille on tunnusomaista se, mitä sanotaan itsenäisissä patenttivaatimuksissa. Keksinnön edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Keksinnön mukaisesti päätelaitteessa muodostetaan paikallisessa verkossa allokoidun IP-osoitteen käsittävä signalointiviesti, jossa ainakin mainittu IP-osoite on eheyssuojattu. Signalointiviesti lähetetään päätelaitteesta julkiseen matkaviestinverkkoon paikallisen verkon kautta käyttäen signalointiviestin kantavan IP-datagrammin lähdeosoitteena allokoitua IP-osoitetta. Julkisessa matkaviestinverkossa tarkastetaan vastaanotetun IP-datagrammin käsittämän signalointiviestin käsittämän IP-osoitteen eheys. Julkisessa matkaviestinverkossa verrataan IP-datagrammin lähde-IP-osoitetta signalointiviestin sisäl-

tämään IP-osoitteeseen, jos signalointiviestin käsittämää IP-osoitetta ei ole eheystarkastuksen perusteella muokattu. IP-osoitetta käytetään päätelaitteen tunnisteena julkisessa matkaviestinverkossa, jos IP-datagrammin lähde-IP-osoite on sama kuin signalointiviestin käsittämä IP-osoite.

IP-osoitteen eheyssuojauksella tarkoitetaan sitä, että signalointiviesti varustetaan sellaisella eheyden tarkastuskoodilla, että julkisessa matkaviestinverkossa havaitaan, jos IP-osoitetta on muutettu. Tyypillisesti paikallinen verkko on lisensioimattomalla taajuusalueella toimiva langaton (WLAN) tai langallinen lähiverkko (LAN) keksinnön sovellusaluetta niihin kuitenkaan rajoittamatta.

Keksinnön mukaisen ratkaisun etuna on, että IP-kerroksen yhteyksien edelleenlähetykset ja uudelleenreititykset voidaan havaita. Tällöin voidaan havaita, että pakettien lähettäjä ei olekaan päätelaite, vaan paketit siepannut kolmas osapuoli, jota ei tarvitse palvella. Vaikka kolmas osapuoli korvaisi myös signalointiviestin käsittämän IP-osoitteen omalla osoitteellaan, muuttunut IP-osoite havaittaisiin julkisessa matkaviestinverkossa. Ratkaisu parantaa turvallisuutta paikallisten verkkojen ja julkisten matkaviestinverkkojen yhteistoiminnassa.

Keksinnön erään edullisen suoritusmuodon mukaisesti julkinen matkaviestinverkko on UMTS-verkko ja päätelaite käsittää UMTS-tilaajan tunnistusyksikön USIM (Universal Subscriber Identity Module), johon on tallennettu eheysavaimen laskemiseen tarvittava algoritmi ja salainen avain. Tällöin signalointiviestin käsittämän IP-osoitteen eheys tarkastetaan vertaamalla päätelaitteen USIM-yksikössä lasketun eheysavaimen perusteella laskettua eheyden tarkastuskoodia (MAC-I) julkisen matkaviestinverkon todentamiskeskuksessa lasketun eheysavaimen avulla laskettuun odotettuun eheyden tarkastuskoodiin (XMAC-I). Tämä suoritusmuoto mahdollistaa 3GPP:n standardien mukaisten päätelaitteita ja verkkoelementtejä varten jo määritettyjen todentamistoimintojen, erityisesti eheyden tarkastamistoimintojen, käyttämisen IP-osoitteeen verifioinnissa. Tällöin voidaan myös pitkälti hyödyntää jo määritettyjä signalointiviestejä, eikä suuria muutoksia standardeihin tarvita.

Kuvioiden lyhyt selostus

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

Kuvio 1a esittää erästä julkisen matkaviestinverkon ja paikallisen verkon käsittävää tietoliikennejärjestelmää;

Kuvio 1b havainnollistaa matkaviestimen rakennetta;

Kuvio 2 esittää vuokaaviona keksinnön erään edullisen suoritusmuodon mukaista menetelmää;

Kuvio 3 esittää signalointikaaviona keksinnön erään edullisen suoritusmuodon mukaista todentamisprosessia; ja

Kuvio 4 havainnollistaa erään edullisen suoritusmuodon mukaista signalointiviestiä.

Keksinnön erään edullisen suoritusmuodon yksityiskohtainen selostus

Viitataan kuvioon 1a, jossa on esitetty erään edullisen suoritusmuodon mukaista verkkoarkkitehtuuria, jossa julkisena matkaviestinverkkona on UMTS-verkko PLMNW ja paikallisena verkkona on laajakaistaliityntäverkko BAN. Paikallinen verkko BAN on erään edullisen suoritusmuodon mukaisesti jonkin IEEE 802.1x-standardin mukaista käyttäjän todentamista ja verkkoonpääsynvalvontaa käyttävä langaton lähiverkko, kuten IEEE 802.11*i*-standardin mukainen langaton lähiverkko. Keksintöä voidaan kuitenkin soveltaa myös muissa IEEE 802-pohjaisissa langattomissa lähiverkoissa tai muuntyyppisissä paikallisissa, tyypillisesti lisensioimattomalla taajuuskaistalla toimivissa verkoissa BAN, esimerkiksi BRAN-standardin (Broadband Radio Access Network) mukaisessa verkossa tai Bluetooth-verkossa. BRAN-standardit käsittävät tyyppien 1 ja 2 HIPERLAN-standardit (High Performance Radio Local Area Network), HIPERACCESS- ja HIPERLINK-standardit. Julkinen matkaviestinverkko voi olla UMTS-verkon sijaan esimerkiksi GSM/GPRS-verkko.

Paikallinen verkko BAN ja UMTS-verkko PLMNW voivat kommunikoida IP-pohjaisen (Internet Protocol) verkon IPNW kautta. UMTS-verkko PLMNW käsittää GERAN-pääsyverkon, UTRAN-pääsyverkon ja GSM/GPRS-ydinverkkoon perustuvan UMTS-ydinverkon CN (Core Network) tai ainakin osittaisia toiminnallisuuksia niistä. Kuvion 1a mukaisesti paikallinen verkko BAN voi toimia yhtenä UMTS-verkon liityntäverkkona, siitä voidaan järjestää yhteys myös muihin verkkoihin, kuten julkiseen Internetiin. BAN käsittää liityntäpisteiksi AP kutsuttuja liityntälaitteita, jotka tarjoavat radiopääsyn matkaviestimelle MS ja näin ollen päättävät laajakaistaradioyhteyden.

Liityntäpiste AP hallitsee radiorajapintaa käytettävän radioteknologian mukaisesti, erään edullisen suoritusmuodon mukaisesti IEEE 802.11-standardin mukaisesti. IEEE 802.11 -spesifikaatiot määrittävät sekä fyysisen kerroksen että MAC-kerroksen protokollat tiedonsiirrolle radiorajapinnan yli. Tiedonsiirrossa voidaan käyttää infrapunaa tai kahta hajaspektritekniikkaa (Di-

rect Sequence Spread Spectrum DSSS, Frequency Hopped Spread Spectrum FHSS). Molemmissa hajaspektritekniikoissa käytetään 2,4 gigahertsin kaistaa. MAC-kerroksella käytetään ns. CSMA/CA-tekniikkaa (Carrier Sense Multiple Access with Collision Avoidance). AP huolehtii myös radiorajapinnan datavirtojen silloittamisesta (Bridging) tai reitittämisestä muihin verkkosolmuihin ja muista verkkosolmuista.

Kuvion 1a mukaan paikallinen verkko BAN käsittää myös ohjauslaitteen tai yhdyskäytävälaitteen BANGW (BAN Gateway). BANGW toimii yhdyskäytävänä AP:n ja UMTS-verkon PLMNW välisessä datansiirrossa. Nämä toiminnot voidaan suorittaa yhdessä tai useammassa loogisessa tai fyysisessä solmussa, jota voidaan kutsua muillakin nimillä kuin ohjauslaite tai yhdyskäytävälaite, esimerkiksi liityntäkontrolleri (Access Controller). BANGW myös allokoi IP-osoitteita matkaviestimelle MS ja tallentaa ja toimittaa UMTS-verkkoon PLMNW liittyvää verkkoinformaatiota sitä tarvitseville matkaviestimille MS. BANGW myös vastaanottaa ja tallentaa tietoja sen kautta käytettävissä olevista muista verkoista, ainakin UMTS-verkosta PLMNW. BANGW muodostaa veloitusinformaatiota siirrettävän datan perusteella ja siirtää sitä laskutuspalvelimelle esimerkiksi AAA-protokollan (Authentication, Authorization and Accounting) mukaisesti.

Erään vaihtoehtoisen suoritusmuodon mukaisesti kaikki tai osa BANGW:n toiminnallisuudesta voidaan toteuttaa liityntäpisteessä AP. Liityntäpisteiden toiminta poikkeaa tällöin kuvion 1a liityntäpisteistä AP siten, että liityntäpisteet on kytketty IP-verkkoon IPNW, esimerkiksi Internetiin, eikä erillistä liityntäpisteitä ohjaavaa ohjauslaitetta (BANGW) välttämättä tarvita. Esimerkiksi IEEE 802.1x-standardin mukaista käyttäjän todentamista ja verkkoon pääsynvalvontaa tukeva AP tyypillisesti käyttää AAA-protokollaa ja voi siten kommunikoida suoraan todentamispalvelimien ja laskutuspalvelimien kanssa sekä muodostaa myös veloitusinformaation siirrettävän datan tai yhteysaikojen perusteella.

UMTS-ydinverkko CN käsittää UMTS-verkkoon liittyneitä matkaviestimiä palvelevan operointisolmun SGSN (Serving GPRS Support Node) ja yhdyskäytävätukisolmun GGSN (Gateway GPRS Support Node), joka tarjoaa yhdyskäytävätoiminnan ulkopuolisiin verkkoihin, kuten Internetiin tai yrityksen intranetiin. PLMNW voi käsittää myös piirikytkentäisiä palveluita tarjoavan matkaviestinkeskuksen 3GMSC ja muita kuviossa 1a esittämättömiä tunnettuja

verkkoelementtejä, kuten lyhytsanomapalvelukeskuksen ja UMTS-laskutusjärjestelmän elementtejä.

UMTS-radiopääsy voi olla järjestetty GSM/EDGE-radiopääsyverkon GERAN kautta tai WCDMA-pohjaisen UTRAN-verkon kautta, johon seuraavassa kuvatut esimerkit pohjautuvat. Radioalijärjestelmä käsittää UTRAN-verkon tapauksessa radioverkko-ohjaimen RNC (Radio Network Controller) ja tukiasemia BS, joita voidaan kutsua myös B-solmuiksi (Node B).

UMTS-verkko PLMNW voi käsittää todentamispalvelimen AS, joka tarjoaa UMTS-matkaviestintilaajien todentamispalveluita ja edullisesti myös laskutuspalveluita paikallisille verkoille BAN. Näin UMTS-verkon tilaajatietoja ja todentamispalveluita voidaan käyttää paikallisessa verkossa BAN vierailevien tunnistusyksikön USIM (Universal Subscriber Identity Module) käsittävien matkaviestimien MS palvelemiseksi. Matkaviestimen MS käyttäjällä ei välttämättä tarvitse olla ennalta sovittua sopimusta paikallisen verkon BAN operaattorin kanssa. Tällöin paikallisen verkon BAN tarjoamasta langattomasta yhteydestä voidaan laskuttaa matkaviestinverkon PLMNW kautta. UMTS-verkon PLMNW operaattori voi myöhemmin hyvittää verkon BAN operaattoria verkon käytöstä. Vaikka todentamispalvelin AS on kuviossa 1a esitetty erillisenä elementtinä, se voidaan hyvin toteuttaa esimerkiksi osana palvelusolmua BSN, operointisolmua SGSN tai yhdyskäytävätukisolmua GGSN.

Jos PLMNW ei ole matkaviestimen MS kotiverkko HPLMNW, eli MS verkkovierailee myös verkossa PLMNW, vierailtavasta verkosta on kommunikoitava todentamista ja laskuttamista varten matkaviestimen MS USIM-yksikön ilmaiseman IMSI-tunnisteen mukaiseen kotiverkkoon HPLMNW. Kotiverkko HPLMNW käsittää kyseisen tilaajan tilaajatiedot sisältävän kotirekisterin HLR, jonka yhteydessä tyypillisesti on myös todentamisvektorit laskeva todentamiskeskus AuC. Kuviossa 1a ei ole esitetty muita kotiverkon HPLMNW elementtejä, kuten matkaviestinkeskusta 3GMSC tai operointisolmua SGSN, joiden kautta yhteys kotirekisteriin/todentamiskeskukseen HLR/AuC tyypillisesti järjestetään. UMTS-spesifikaatioissa vierailtavaa verkkoa kutsutaan myös termillä SN (Serving Network) ja kotiverkkoa termillä HN (Home Network).

Kuten kuviossa 1b on havainnollistettu, matkaviestin MS käsittää muistia M, käyttöliittymän UI, lähetinvastaanottimen TxRx langattoman tiedonsiirron järjestämiseksi, ja yhden tai useamman prosessorin käsittävän keskusprosessointiyksikön CPU (Central Processing Unit). Muistissa M on haihtumaton osuus keskusprosessointiyksikköä CPU kontrolloivien sovellusten ja mui-

den säilytettävien tietojen tallentamiseksi ja haihtuva osuus käytettäväksi tilapäistä datan prosessointia varten. Keskusprosessointiyksikössä CPU suoritettavilla tietokoneohjelmakoodeilla voidaan aikaansaada matkaviestin MS toteuttamaan keksinnölliset välineet, joiden eräitä suoritusmuotoja on havainnollistettu kuvioissa 2 ja 3. On myös mahdollista käyttää kovo-ratkaisuja tai kovo- ja ohjelmistoratkaisuiden yhdistelmää toteuttamaan keksinnölliset välineet. MS voi olla esimerkiksi integroitu kommunikointilaite, sylimikro (laptop computer), yhdistettynä radiopääsyn tarjoavaan laitteistoon (esim. WLAN-kortti), tai PDA-laitteen ja matkapuhelimen yhdistelmä.

Erään edullisen suoritusmuodon mukainen matkaviestin MS käsittää UMTS-järjestelmälle spesifisen tilaajan tunnistusyksikön USIM. Matkaviestimessä MS käytettävä tunnistusyksikkö voi olla erilainen matkaviestinverkosta riippuen, GSM-verkoissa käytetään tunnistusyksikköä SIM. MS:n käsittämien kortinlukuvälineiden (ei esitetty) avulla CPU voi hyödyntää tunnistusyksikön USIM käsittävää UICC-korttia (Universal Integrated Circuit Card) 3GPP-spesifikaatioiden mukaisesti. UICC-korttia voidaan vaihtaa matkaviestimestä MS toiseen. USIM on kotiverkon HPLMNW operaattorin luovuttama ja kotiverkon HPLMNW kotirekisterissä HLR on tallennettuna tiedot USIM:stä. USIM käsittää tilaajan tunnistetiedon IMSI (International Mobile Subscriber Identifier), joka edustaa tilaajaa verkossa ja toimii näin ollen matkaviestimen MS käyttäjän tunnisteena. Matkaviestimen MS laiteosalla TE voi olla myös oma laitetunnisteensa IMEI (International Mobile Equipment Identity), joka ei kuitenkaan ole relevantti keksinnön kannalta.

Eräänä tunnistusyksikön USIM tehtävänä on toteuttaa yhteyden muodostamiseen UMTS-verkossa PLMNW tarvittava AKA-toiminnallisuus (Authentication and Key Agreement) matkaviestimen MS puolelta. Tätä tarkoitusta varten USIM käsittää myös salaisen avaimen K, algoritmin f3 salausavaimen CK muodostamiseksi, algoritmin verkosta PLMNW lähetetyn todentamisvasteen AUTN tarkastamiseksi ja algoritmin f2 verrattavan todentamisvasteen RES (Response) muodostamiseksi (jos AUTN on verifioitu). USIM muodostaa salaisen avaimen K ja julkisesta matkaviestinverkosta PLMNW vastaanotetun haasteen RAND perusteella myös eheysavaimen IK käyttäen algoritmia f4. Eheysavainta IK käytetään todentamaan matkaviestimestä lähetettävien ja vastaanotettavien signalointiviestien eheys algoritmia f9 käyttäen. Vastaavasti, samaa satunnaislukua RAND käyttäen, UMTS-verkon PLMNW todentamiskeskuksessa AuC muodostetaan todentamisvektori AV (RAND,

XRES, CK, IK, AUTN). IK ja CK siirretään onnistuneen todentamisen jälkeen UMTS-verkossa radioverkko-ohjaimelle RNC, joka suorittaa salaukseen ja datan eheyden tarkastamiseen liittyvät toiminnot matkaviestimeltä vastaanotetuille ja lähetettäville tiedoille. Tunnettujen AKA-toimintojen muiden yksityiskohtien tarkemman kuvauksen osalta viitataan 3GPP-spesifikaatioon 3GPP TS 33.102 "*3G Security; Security Architecture (Release 5)*", v. 5.0.0, kesäkuu 2002, sivut 1 - 49.

Erään edullisen suoritusmuodon mukaisesti paikallisen verkon BAN kautta voidaan käyttää UMTS-verkon PLMNW tiedonsiirtopalveluita. Tällöin UMTS-verkko käsittää tunnettujen UMTS-liityntäverkon verkkoelementtien lisäksi Iu-rajapintaa tukevan palvelusolmun BSN (Broadband Service Node) yhtä tai useampaa paikallista verkkoa BAN varten. Tässä suoritusmuodossa onnistuneen todentamisen jälkeen (jonka joko BSN tai todentamispalvelin AS suorittaa) MS voi käyttää myös vierailtavan UMTS-verkon PLMNW palveluita paikallisen verkon BAN ja palvelusolmun BSN kautta. Palvelusolmun BSN toiminta vastaa monelta osin palvelevan radioverkko-ohjaimen RNC toimintaa. Palvelusolmua BSN ei voida kuitenkaan järjestää hallitsemaan paikallisen verkon radioresursseja, joten tavanomainen Iub-rajapinta korvataan I4-rajapinnalla paikalliseen verkkoon BAN, jolloin BSN kommunikoi matkaviestimen MS kanssa paikallisen verkon BAN kautta. Palvelusolmun BSN toimintoja ovat:

- UTRAN-verkkoa varten määritettyjen RRC-signalointiprotokollien (Radio Resource Control) suorittaminen mahdollisesti BAN-spesifisten rajoitusten mukaisesti
- Korkeampien kerrosten UMTS-datavirtojen, kuten loogisten kanavien tai kuljetuskanavien, multipleksointi IP-pohjaisiin siirtopolkuihin (esimerkiksi UDP/IP-tunneliin) BAN-verkkoon ja demultipleksointi BAN–verkosta
- Radioyhteyksien hallinta
- UMTS-salauksen järjestäminen
- UMTS IP-otsikkokenttien kompressointi
- UMTS RLC-kerroksen (Radio Link Control) uudelleenlähetykset

Palvelusolmun BSN toiminnot voivat mahdollisesti myös sisältää paikallisen verkon BAN resurssien käytön seuraamisen BAN-operaattorin laskutuksen tarkistamiseksi. Paikallinen verkko BAN voi olla usean UMTS-verkon hyödyntämä. Paikallinen verkko BAN voi olla kytkettynä useaan palvelusolmuun BSN ja BSN voi olla kytketty yhteen tai useampaan paikalliseen verk-

koon BAN. BSN voidaan jakaa erillisiin käyttäjätason (User Plane) yhdyskäytävä- ja ohjaustason (Control Plane) palvelintoimintoihin. BSN voi olla kytketty operointisolmuun SGSN, matkaviestinkeskukseen MSC (Mobile Switching Centre) ja mahdollisesti muihin UMTS ydinverkon elementteihin standardin lurajapinnan kautta. BSN voi olla myös kytketty muihin BSN-solmuihin tai UTRAN-verkon RNC-elementteihin Iur-signalointirajapintojen kautta yhteysvastuun vaihtamisen tukemiseksi UTRAN-verkon sisällä tai UTRAN-verkkojen välillä.

Tässä suoritusmuodossa MS sisältää välineet paikallisen verkon BAN alempien kerrosten (L1, L2) toteuttamiseksi ja välineet UMTS-verkon kanssa kommunikointiin paikallisen verkon kautta. Erään edullisen suoritusmuodon mukaisesti MS on kaksitoimipäätelaite (Dualmode Terminal), joka kykenee kytkeytymään paikallisen verkon BAN lisäksi myös UMTS-verkkoon UTRAN:n tukiasemien (Node B) kautta. Jotta matkaviestin MS kykenee muodostamaan yhteyden UMTS-verkkoon paikallisen verkon BAN kautta, on siinä oltava lisäksi seuraavat toiminnot:

- 3GPP-spesifikaatioiden määrittämien UMTS:n korkeampien kerrosten signalointiprotokollien toteuttaminen. Näitä protokollia ovat RRC (Radio Resource Control), istunnon hallinta (Session Management) ja liikkuvuuden hallinta (Mobility Management).

- UMTS-käyttäjätason protokollien rajoitetun toiminnallisuuden suorittaminen ja käyttäjätason datan kommunikoiminen solmun BSN kanssa mahdolliset paikallisen verkon BAN aiheuttamat rajoitukset huomioiden. Näitä protokollia ovat RLC (Radio Link Control) ja PDCP (Packet Data Control Protocol).

- Korkeampien UMTS-kerrosten datavirtojen multipleksoiminen alempien kerrosten UDP/IP-pohjaisen kommunikaatioon ja käänteisesti vastaanotetun datan demultipleksoiminen päinvastoin UMTS-datavirroiksi.

Myös UMTS-verkon PLMNW palvelusolmu BSN tai todentamispalvelin AS käsittävät välineet, joilla myöhemmin kuvioiden 2 ja 3 yhteydessä havainnollistettu keksinnöllinen toiminnallisuus voidaan toteuttaa. BSN ja AS käsittävät prosessointiyksiköt, joissa suoritettava tietokoneohjelmakoodi voi aikaansaada keksinnölliset toiminnot. Myös kovo-toteutuksia tai ohjelmisto- ja kovo-toteutuksien yhdistelmää voidaan käyttää.

Kuviossa 2 on havainnollistettu keksinnön erään edullisen suoritusmuodon mukaista menetelmää vuokaavion avulla. Matkaviestimelle MS allokoidaan paikallisessa verkossa BAN IP-osoite tyypillisesti sen jälkeen, kun se

on todennettu. Päätelaitteessa muodostetaan 201 allokoidun IP-osoitteen käsittävä signalointiviesti, jossa ainakin IP-osoite on eheyssuojattu. Tällöin signalointiviesti varustetaan sellaisella eheyden tarkastuskoodilla, että julkisessa matkaviestinverkossa PLMNW havaitaan, jos IP-osoitetta on muutettu. Tyypillisesti koko signalointiviesti on eheyssuojattu, eli eheyssuojauskoodi on laskettu koko viestin perusteella. Matkaviestin MS lähettää 202 eheyssuojatun IP-osoitteen käsittävän signalointiviestin julkiseen matkaviestinverkkoon PLMNW paikallisen verkon kautta käyttäen signalointiviestin kantavan IP-datagrammin lähde-IP-osoitteena allokoitua IP-osoitetta. Julkisessa matkaviestinverkossa PLMNW tarkastetaan 203, 204 vastaanotetun IP-datagrammin käsittämän signalointiviestin käsittämän IP-osoitteen eheys. Jos IP-osoitetta on eheystarkastuksen 203, 204 perusteella muokattu, signalointiviesti sivuutetaan 205. On mahdollista, että myös myöhemmät signalointiviestin sisältämästä IP-osoitteesta vastaanotetut paketit hylätään.

Jos IP-osoitetta ei ole muokattu, julkisessa matkaviestinverkossa PLMNW verrataan signalointiviestin käsittävän 206, 207 IP-datagrammin lähde-IP-osoitetta signalointiviestin sisältämään IP-osoitteeseen. Jos ne eivät ole samoja, IP-datagrammin lähdeosoitetta on muutettu. Tällöin signalointiviesti hylätään 205, koska kolmas osapuoli on voinut siepata viestin. Jos IP-datagrammin lähde-IP-osoite on sama kuin signalointiviestin käsittämä IP-osoite, käytetään 208 IP-osoitetta päätelaitteen tunnisteena julkisessa matkaviestinverkossa. Edellä havainnollistettu toiminnallisuus luonnollisesti vaatii, että matkaviestin MS ja julkinen matkaviestinverkko PLMNW ovat samassa IP-osoiteavaruudessa, eli verkko-osoitteiden muunnosta (NAT; Network Address Translation) ei voida käyttää. Eheyssuojauksen lisäksi on myös mahdollista, että signalointiviesti salataan päätelaitteessa ja signalointiviestin salaus puretaan julkisessa matkaviestinverkossa. Tämä edelleen parantaa turvallisuutta.

Kuviossa 3 on havainnollistettu signalointikaaviona erästä edullista suoritusmuotoa, jossa matkaviestin MS siirtyy käyttämään UMTS-verkon PLMNW palveluita paikallisen verkon BAN kautta. Tämä tarve aiheutuu esimerkiksi matkaviestimen MS siirtyessä pois PLMNW:n tukiasemien BS peittoalueelta, käyttäjän aloitteesta tai automaattisesti siirryttäessä paikallisen verkon BAN liityntäpisteiden AP peittoalueelle, esimerkiksi toimistoon. Jotta matkaviestimelle MS voidaan tarjota palveluita paikallisessa verkossa BAN, se täytyy ensin todentaa 301. Todentaminen 301, joka suoritetaan matkaviestimen MS ja UMTS-verkon PLMNW elementin, edullisesti palvelusolmun BSN tai to-

dentamispalvelimen AS, välillä, voi perustua IETF:n RFC-dokumentissa 2284 *"PPP Extensible Authentication Protocol (EAP)"*, maaliskuu 1998, määritettyyn EAP-protokollaan. Matkaviestimelle MS voidaan suorittaa, sen pyytäessä yhteydenmuodostusta paikallisen verkon kautta, täydellinen AKA-mekanismin mukainen todentaminen tai jo aiemmin UMTS-verkossa PLMNW matkaviestimelle tarjottua yhteyttä varten muodostettuja todentamistietoja hyödyntävä todentaminen. Täydellinen todentaminen voidaan toteuttaa käyttäen IETF:n Internet-luonnoksessa *"EAP AKA Authentication"*, lokakuu 2001, J. Arkko ja H. Haverinen, esitettyä EAP (Extensible Authentication Protocol) AKA-todentamista, joka määrittelee UMTS:n AKA-todentamismekanismia hyödyntävän EAP-protokollan.

Koska matkaviestimellä MS on tai on aiemmin ollut aktiivinen yhteys UMTS-verkon PLMNW kautta, matkaviestimelle aiemmin suoritetussa AKA-todentamismekanismissa matkaviestimeen MS ja UMTS-verkkoon PLMNW on muodostettu jaettu salaisuus eheysavain IK. Näin ollen myös todentaminen 301 voi perustua eheysavaimen IK perusteella matkaviestimessä MS ja palvelusolmussa BSN tai todentamispalvelimessa AS laskettujen eheyden tarkastuskoodien vertailemiseen. Aiempaan matkaviestimelle UMTS-verkossa PLMNW tarjottuun yhteyteen liittyvät todentamistiedot saadaan esimerkiksi radioverkko-ohjaimesta RNC. Tällöin todentaminen saadaan suoritettua nopeammin verrattuna siihen, että suoritettaisiin täydellinen todentaminen.

Kun matkaviestin MS on todennettu, sille voidaan allokoida 302 paikallisessa verkossa (liityntäpisteessä AP tai ohjauslaitteessa BANGW) IP-osoite, joka välitetään 303 matkaviestimelle MS. Nyt matkaviestin MS voi kommunikoida UMTS-verkon palvelusolmun BSN kanssa suorittaen RRC-protokollaa UDP/IP-protokollapinoa hyödyntäen. MS voi pyytää yhteysvastuun siirtoa UMTS-verkosta PLMNW solun päivitysviestillä (Cell Update). Erään edullisen suoritusmuodon mukaisesti solun päivitysviestistä verifioidaan IP-osoite. Tällöin MS muodostaa 304 eheyden tarkastuskoodin MAC-I erään edullisen suoritusmuodon mukaisesti UMTS-järjestelmää varten määritetyllä tavalla eheysavaimen IK, eheyssekvenssinumeron (COUNT-I), verkosta saadun satunnaisluvun (FRESH), suuntabitin (DIRECTION) ja [Cell Update]-viestin perusteella algoritmia f9 käyttäen, kuten 3GPP-spesifikaatiossa 3GPP TS 33.102 *"3G Security; Security Architecture (Release 5)"*, v. 5.0.0, kesäkuu 2002, kappaleessa 6.5.3, on kuvattu. Eheysavain IK on saatu tunnistusyksiköstä USIM tai eheyden UMTS-verkkoon suuntautuvan yhteyden signalointiviesteistä var-

mistavasta toiminnosta. Solun päivitysviesti (Cell Update) edullisesti käsittää myös MS:lle allokoidun IP-osoitteen, ja MAC-I lasketaan 304 huomioiden IP-osoite. Solun päivitysviesti voi myös olla salattu. MS muodostaa 305 eheyden tarkastuskoodin MAC-I ja IP-osoitteen käsittävän solun päivitysviestin. Viestiin lisätään tarvittavat alempien kerrosten otsikkokentät, kuten IP-datagrammin vaatimat IP-otsikkokentät. IP-datagrammin lähde-IP-osoitteena käytetään MS:lle vaiheessa 302 allokoitua IP-osoitetta, joka on siis myös ylemmän kerroksen signalointiviestissä. Näin muodostettu IP-datagrammi välitetään 306 UMTS-verkon PLMNW palvelusolmulle BSN.

Palvelusolmu BSN muodostaa 307 odotetun datan eheyden tarkastuskoodin XMAC-I. BSN voi tämän jälkeen tarkastaa 308 vastaanotetun signalointiviestin käsittämän IP-osoitteen eheyden tarkastamalla, ovatko eheyden tarkastuskoodit MAC-I ja XMAC-I identtisiä. Näin voidaan varmistaa, onko signalointiviestiä muutettu sen siirron aikana. Jos eheyden tarkastuskoodit MAC-I ja XMAC-I ovat identtisiä, viestiä ei ole muokattu ja näin ollen myös sen sisältämää IP-osoitetta ei ole muutettu. Tässä tapauksessa BSN voi verrata 309 vastaanottamansa IP-datagrammin lähde-IP-osoitetta IP-datagrammin käsittämän solunpäivitysviestin sisältämään IP-osoitteeseen. Jos ne ovat samoja, IP-osoite on verifioitu ja sitä voidaan käyttää UMTS-verkossa matkaviestimen MS tunnisteena. Vaiheessa 310 voidaan IP-osoitteen verifioinnin jälkeen suorittaa vasteena solun päivitysviestille UMTS-järjestelmän mukainen palvelevan radioverkon vaihto (SRNS Relocation), jonka tuloksena ydinverkossa kytketään käyttäjädatavirta paikallisen verkon BAN kautta kulkevaksi aiemman radioverkko-ohjaimen RNC sijaan. BSN voi UMTS-verkon kannalta toimia kuin RNC suorittaessaan palvelevan radioverkon vaihtoa. Tunnettua radioaliverkon vaihtoa on kuvattu 3GPP-spesifikaatiossa 3GPP TS 22.060, v.5.0.0, tammikuu 2002, "*General Packet Radio Service (GPRS); Service Description; Stage 2 (Release 5)*" kappale 6.9.2.2, sivut 74-89.

Tällöin IP-osoite tallennetaan ainakin palvelusolmuun BSN ja se sidotaan matkaviestimen MS U-RNTI-tunnisteeseen. Matkaviestimen MS ja palvelusolmun BSN välille muodostetaan looginen PDCP-yhteys, johon UMTS-verkon PLMNW ydinverkon datan siirtokonteksti sidotaan.

On huomioitava, että kuvio 3 on vain eräs esimerkki ja IP-osoitteen verifiointi voidaan toteuttaa myös muilla tavoin ja muissa tilanteissa. Esimerkiksi eheyden tarkastamiskoodit MAC-I, XMAC-I voidaan muodostaa (302, 305) kuviosta 3 poikkeavassa kohdassa. IP-osoitteen verifiointi voidaan suorit-

taa milloin tahansa matkaviestimen IP-osoitteen muuttuessa, eli tyypillisesti aina paikallisen verkon BAN allokoidessa matkaviestimelle MS IP-osoitteen.

Kuviossa 4 on havainnollistettu erään edullisen suoritusmuodon mukaista IP-datagrammia 41, joka voidaan lähettää matkaviestimen MS ja UMTS-verkon PLMNW välillä vaiheessa 202 ja viestissä 306. IP-datagrammi 41 käsittää IP-otsikkokentän 42, UDP-otsikkokentän 43, mahdollisia muita otsikkokenttiä 44 ja signalointiviestin 45. Muita otsikkokenttiä 44 voivat olla esimerkiksi kuviossa 3 havainnollistetussa tilanteessa MS:n ja BSN:n välillä käytettävän multipleksointikerroksen ja RLC-kerroksen (Radio Link Control) otsikkokentät. IP-otsikkokenttä 42 käsittää MS:lle allokoidun lähde-IP-osoitteen 46. IP-osoite 47 sijaitsee myös signalointiviestissä 45, joka käsittää myös eheyden tarkastuskoodin MAC-I 48. Signalointiviesti 45 voi olla esimerkiksi RRC-protokollan mukainen ja sisältää UMTS-verkossa PLMNW käytettävän solunpäivitysviestin (Cell Update), johon on lisätty IP-osoite 47. Vaihtoehtoisesti IP-osoite 47 voi sijaita RRC-viestin ulkopuolella, jolloin voidaan käyttää täysin 3GPP-spesifikaatioidan mukaista viestirakennetta. Tällöin ei voida käyttää RRC-viestissä 3GPP-spesifikaatioissa määriteltyä eheyden tarkistuskoodia vaan tarvitaan erillinen IP-osoitteen eheyden tarkastuskoodi, joka sijaitsee RRC-viestin ulkopuolella.

Edellä on havainnollistettu suoritusmuotoja, joissa matkaviestin MS voi paikallisen verkon BAN kautta käyttää UMTS-verkon PLMNW palveluita tukisolmun BSN kautta. Keksintöä voidaan soveltaa kuitenkin myös muuntyyppisissä paikallisen verkon ja julkisen matkaviestinverkon yhteistoimintakonfiguraatioissa ja yhteydenmuodostustilanteissa. Eräitä muita konfiguraatioita, joissa keksintöä voidaan soveltaa ovat:

Paikallinen verkko BAN voi olla suoraan yhteydessä julkisen matkaviestinverkon PLMN operointisolmuun SGSN tai yhdyskäytävätukisolmuun GGSN, esimerkiksi tunnelointitekniikoita käyttäen. Tällöin SGSN tai GGSN suoraan palvelisi myös paikallisessa verkossa BAN vierailevia matkaviestimiä MS. Nämä konfiguraatiot voidaan toteuttaa monella eri tavoin; paikalliseen verkkoon BAN voidaan lisätä julkisen matkaviestinverkon elementteihin (esim. SGSN, GGSN, RNC) liittyviä toimintoja tai käyttäjä-/signalointidata voidaan välittää paikallisen verkon BAN kannalta täysin läpinäkyvästi matkaviestimen MS ja SGSN:n tai GGSN:n välillä. Esimerkiksi yhdyskäytäväsolmua GGSN voitaisiin pitää liityntäpisteenä Internetiin myös paikallisessa verkossa BAN vierailleville matkaviestimille MS, myös julkisen matkaviestinverkon tarjoamia laskutus-

ja tilaajanhallintapalveluita voitaisiin käyttää. Eräässä konfiguraatiossa käytetään IP-liikkuvuustekniikoita (Mobile IP) verkkovierailevaa matkaviestintä MS varten paikallisen verkon BAN ja julkisen matkaviestinverkon välillä.

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

Patenttivaatimukset

1. Menetelmä IP-osoitteen verifioimiseksi tietoliikennejärjestelmässä, joka käsittää ainakin yhden langattoman paikallisen verkon, ainakin yhden julkisen matkaviestinverkon, ja ainakin yhden langattoman päätelaitteen, joka käsittää välineet tiedonsiirtoyhteyden muodostamiseksi paikallisen verkon kanssa ja välineet tiedonsiirtoyhteyden muodostamiseksi julkiseen matkaviestinverkkoon paikallisen verkon kautta, joka menetelmä käsittää:

allokoidaan paikallisessa verkossa päätelaitteelle IP-osoite, t u n n e t t u siitä, että

muodostetaan päätelaitteessa mainitun IP-osoitteen käsittävä signalointiviesti, jossa ainakin mainittu IP-osoite on eheyssuojattu,

lähetetään päätelaitteesta signalointiviesti julkiseen matkaviestinverkkoon paikallisen verkon kautta käyttäen signalointiviestin kantavan IP-datagrammin lähdeosoitteena mainittua IP-osoitetta,

tarkastetaan julkisessa matkaviestinverkossa vastaanotetun IP-datagrammin käsittämän signalointiviestin käsittämän IP-osoitteen eheys,

verrataan julkisessa matkaviestinverkossa IP-datagrammin lähde-IP-osoitetta signalointiviestin sisältämään IP-osoitteeseen vasteena sille, että signalointiviestin käsittämää IP-osoitetta ei ole muokattu, ja

käytetään IP-osoitetta päätelaitteen tunnisteena julkisessa matkaviestinverkossa vasteena sille, että IP-datagrammin lähde-IP-osoite on sama kuin signalointiviestin käsittämä IP-osoite.

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

mainittu signalointiviesti on päätelaitteessa ja julkisen matkaviestinverkon radioresursseja ohjaavassa verkkoelementissä toteutettavan radioresurssien ohjausprotokollan viesti.

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

mainittu signalointiviesti on yhteyden modifiointipyyntöviesti, kuten solun päivityspyyntöviesti (Cell Update), joka lähetetään päätelaitteesta vasteena sille, että päätelaitteelle julkisen matkaviestinverkon kautta tarjottu yhteys täytyy siirtää paikallisen verkon kautta tarjottavaksi.

4. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

salataan signalointiviesti päätelaitteessa, ja

puretaan signalointiviestin salaus julkisessa matkaviestinverkossa.

5. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

julkinen matkaviestinverkko on UMTS-verkko ja päätelaite käsittää UMTS-tilaajan tunnistusyksikön USIM (Universal Subscriber Identity Module), johon on tallennettu eheysavaimen laskemiseen tarvittava algoritmi ja salainen avain, jolloin

tarkastetaan signalointiviestin käsittämän IP-osoitteen eheys vertaamalla päätelaitteen USIM-yksikössä lasketun eheysavaimen perusteella laskettua eheyden tarkastuskoodia (MAC-I) julkisen matkaviestinverkon todentamiskeskuksessa lasketun eheysavaimen avulla laskettuun odotettuun eheyden tarkastuskoodiin (XMAC-I).

6. Tietoliikennejärjestelmä, joka käsittää ainakin yhden paikallisen verkon, ainakin yhden julkisen matkaviestinverkon ja ainakin yhden langattoman päätelaitteen, missä

päätelaite on järjestetty muodostamaan tiedonsiirtoyhteyden ainakin langattoman paikallisen verkon kanssa,

paikallinen verkko on järjestetty allokoimaan päätelaitteelle IP-osoitteen, t u n n e t t u siitä, että

päätelaite on järjestetty muodostamaan mainitun IP-osoitteen käsittävä signalointiviesti, jossa ainakin mainittu IP-osoite on eheyssuojattu,

päätelaite on järjestetty lähettämään signalointiviesti julkiseen matkaviestinverkkoon paikallisen verkon kautta käyttäen signalointiviestin kantavan IP-datagrammin lähdeosoitteena mainittua IP-osoitetta,

julkinen matkaviestinverkko on järjestetty tarkastamaan vastaanotetun IP-datagrammin käsittämän signalointiviestin käsittämän IP-osoitteen eheys,

julkinen matkaviestinverkko on järjestetty vertamaan IP-datagrammin lähde-IP-osoitetta signalointiviestin sisältämään IP-osoitteeseen vasteena sille, että signalointiviestin käsittämää IP-osoitetta ei ole muokattu, ja

julkinen matkaviestinverkko on järjestetty käyttämään IP-osoitetta päätelaitteen tunnisteena vasteena sille, että IP-datagrammin lähde-IP-osoite on sama kuin signalointiviestin käsittämä IP-osoite.

7. Langaton päätelaite, joka on järjestetty muodostamaan tiedonsiirtoyhteyden ainakin langattoman paikallisen verkon kanssa, joka päätelaite on järjestetty muodostamaan tiedonsiirtoyhteyden langattoman paikallisen verkon kanssa ja muodostamaan tiedonsiirtoyhteyden julkiseen matkaviestinverkkoon paikallisen verkon kautta, t u n n e t t u siitä, että

päätelaite on järjestetty muodostamaan paikallisessa verkossa allokoidun IP-osoitteen käsittävä signalointiviesti, jossa ainakin mainittu IP-osoite on eheyssuojattu,

päätelaite on järjestetty lähettämään signalointiviesti julkiseen matkaviestinverkkoon paikallisen verkon kautta käyttäen signalointiviestin kantavan IP-datagrammin lähdeosoitteena mainittua IP-osoitetta,

8. Verkkoelementti julkista matkaviestinverkkoa varten, joka on järjestetty siirtämään tietoja julkisen matkaviestinverkon ja paikallisen verkon välillä, joka verkkoelementti on järjestetty vastaanottamaan paikallisen verkon kautta päätelaitteelta signalointiviestin, t u n n e t t u siitä, että

verkkoelementti on järjestetty tarkastamaan vastaanotetun IP-datagrammin käsittämän signalointiviestin käsittämän IP-osoitteen eheys,

verkkoelementti on järjestetty vertamaan signalointiviestin sisältämän IP-datagrammin lähde-IP-osoitetta signalointiviestin sisältämään IP-osoitteeseen vasteena sille, että signalointiviestin käsittämää IP-osoitetta ei ole muokattu, ja

verkkoelementti on järjestetty käyttämään IP-osoitetta päätelaitteen tunnisteena vasteena sille, että IP-datagrammin lähde-IP-osoite on sama kuin signalointiviestin käsittämä IP-osoite.

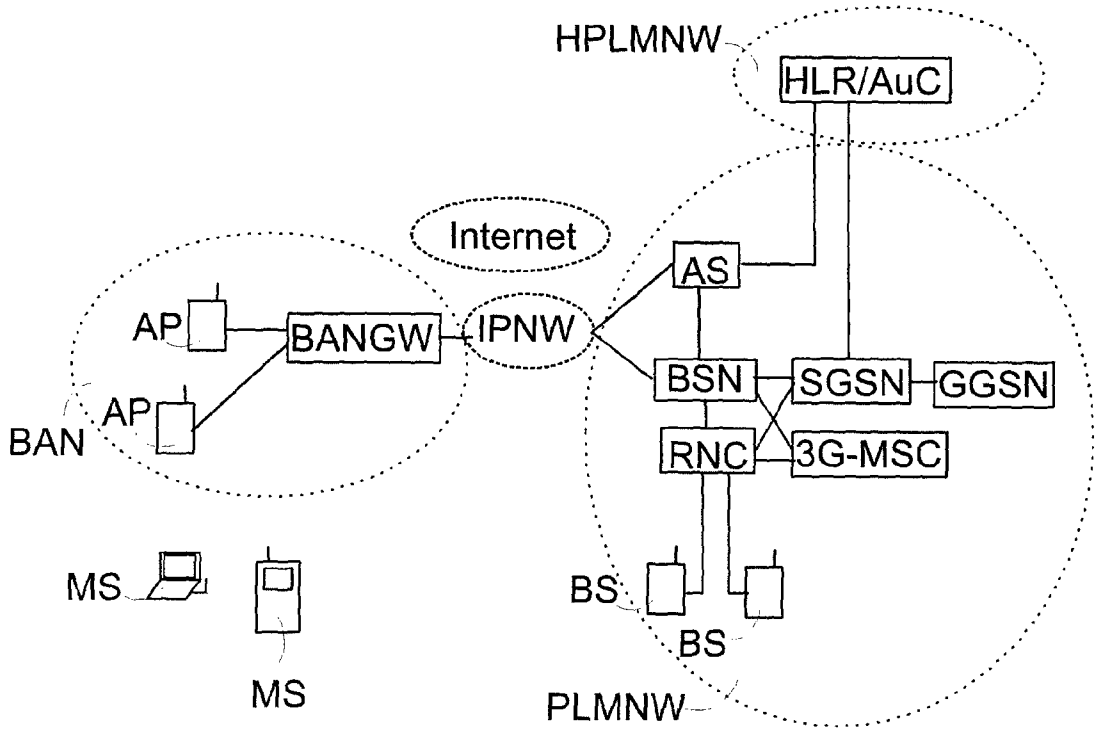
HPLMNW
HLR/AuC
Internet
AS
AP
BANGW
IPNW
BSN
SGSN
GGSN
AP
BAN
RNC
3G-MSC
MS
BS
BS
MS
PLMNW

Fig. 1a

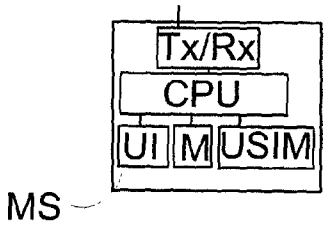
Tx/Rx
CPU
UI
M
USIM
MS

Fig. 1b

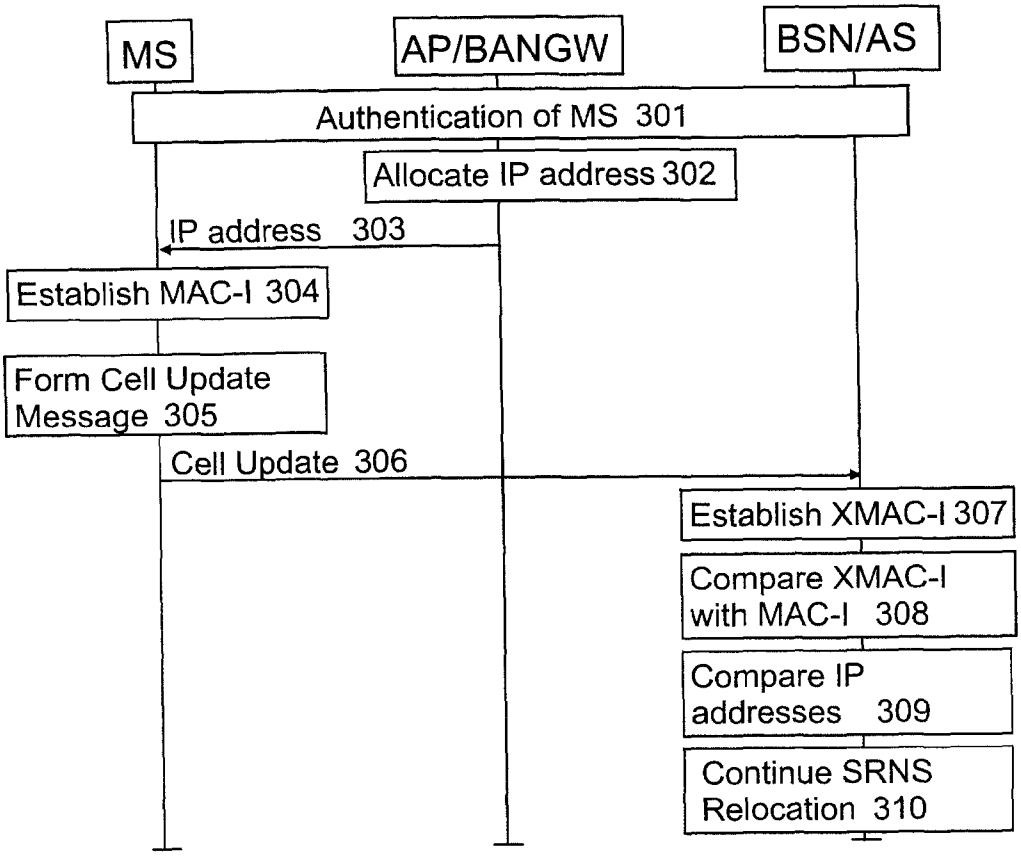
MS
AP/BANGW
BSN/AS
Authentication of MS 301
Allocate IP address 302
IP address 303
Establish MAC-I 304
Form Cell Update Message 305
Cell Update 306
Establish XMAC-I 307
Compare XMAC-I with MAC-I 308
Compare IP addresses 309
Continue SRNS Relocation 310

Fig. 3

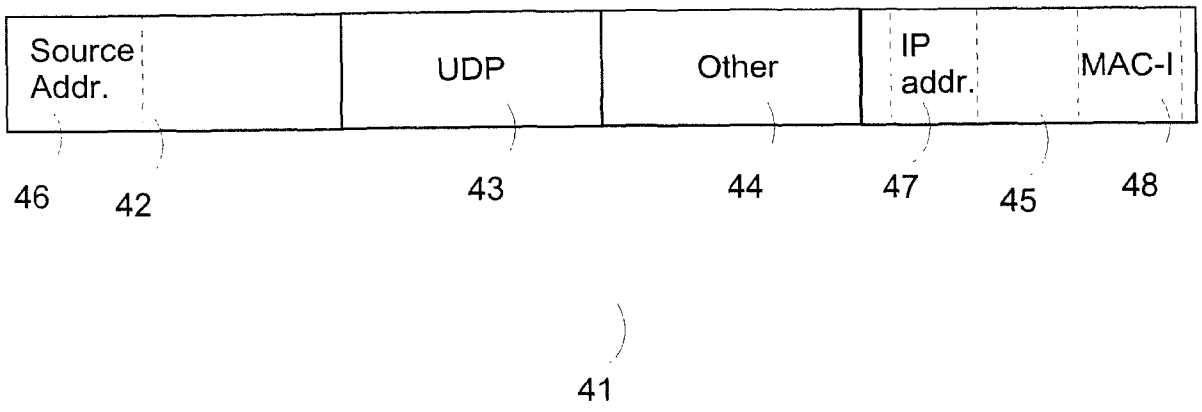
Source Addr.
UDP
Other
IP addr.
MAC-I
46
42
43
44
47
45
48
41

Fig. 4

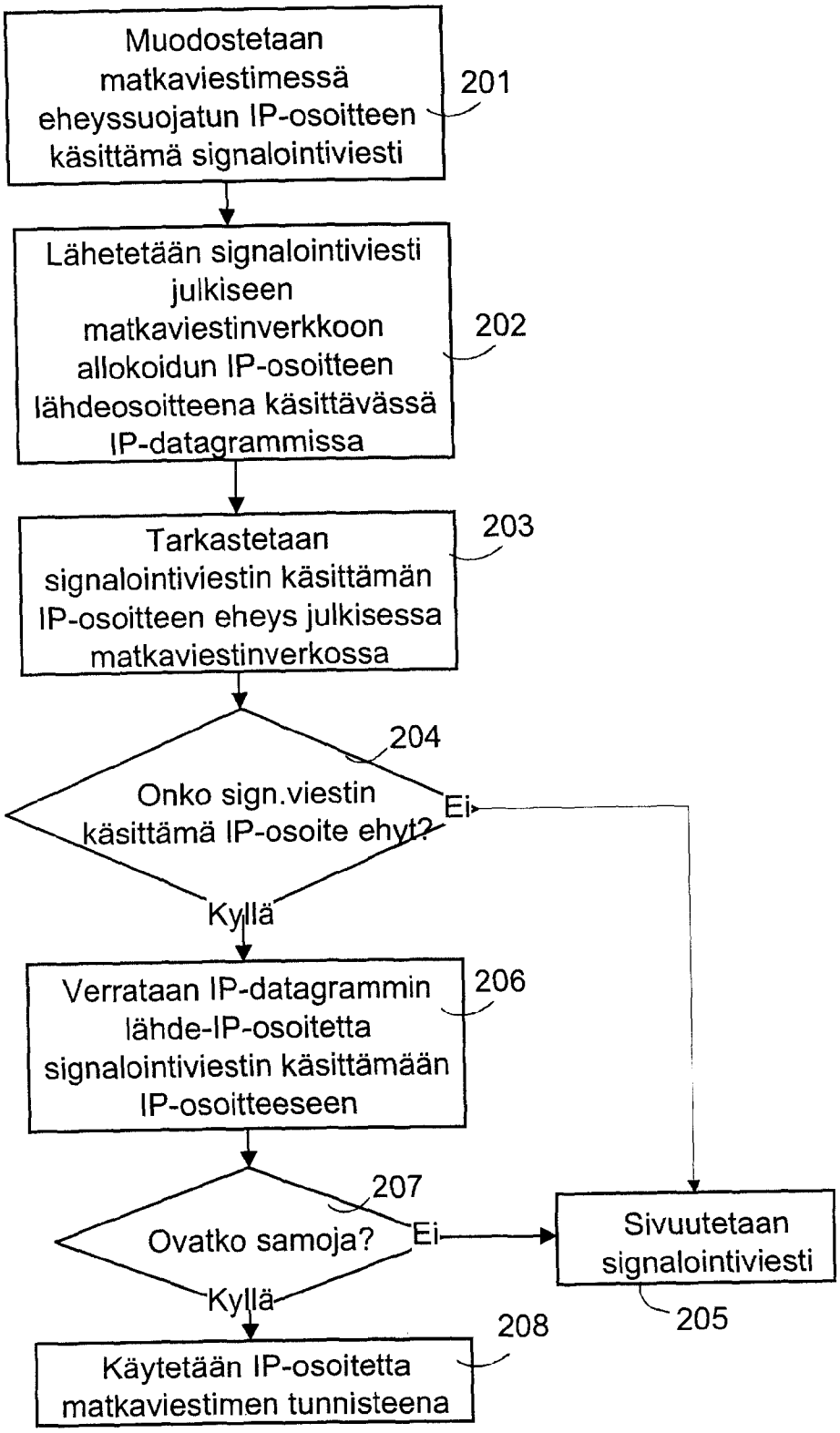
Muodostetaan matkaviestimessä eheyssuojatun IP-osoitteen käsittämä signalointiviesti
201
Lähetetään signalointiviesti julkiseen matkaviestinverkkoon allokoidun IP-osoitteen lähdeosoitteena käsittävässä IP-datagrammissa
202
Tarkastetaan signalointiviestin käsittämän IP-osoitteen eheys julkisessa matkaviestinverkossa
203
204
Onko sign.viestin käsittämä IP-osoite ehyt?
Ei
Kyllä
Verrataan IP-datagrammin lähde-IP-osoitetta signalointiviestin käsittämään IP-osoitteeseen
206
207
Ovatko samoja?
Ei
Kyllä
Sivuutetaan signalointiviesti
205
208
Käytetään IP-osoitetta matkaviestimen tunnisteena

Fig. 2