



F 1000111583B



SUOMI – FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN

(12) PATENTTIJULKAISU
PATENTSKRIFT

(10) FI 111583 B

(45) Patentti myönnetty - Patent beviljats 15.08.2003

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

H04L 9/32, 29/06

(21) Patentihakemus - Patentansökning 991493

(22) Hakemispäivä - Ansökningsdag 30.06.1999

(24) Alkupäivä - Löpdag 30.06.1999

(41) Tullut julkiseksi - Blivit offentlig 31.12.2000

(73) Haltija - Innehavare

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

(72) Keksijä - Uppfinnare

1 •Solala, Erkki, Halimajärventie 53, 36100 Kangasala As., SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud: Nokia IPR-osasto

PL 226
00045 Nokia Group

(54) Keksinnön nimitys - Uppfinningens benämning

Lisenssinvalvonta yhdyskäytäväpalvelimessa
Licenskontroll vid en gateway server

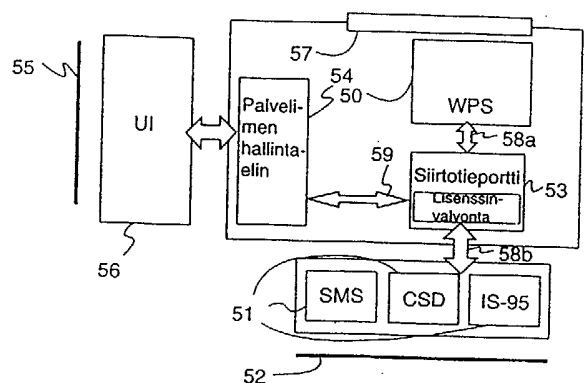
(56) Viitejulkaisut - Anförda publikationer

US A 5485460 (G06F 13/00), US A 5915087 (G06F 11/00)

(57) Tiivistelmä - Sammandrag

Keksintö koskee yhdyskäytäväpalvelinta viestin vastaanottamiseksi päätteeltä ja käsittäen protokollapinon (50) viestin käsittelemiseksi tietyn protokollapinon mukaisesti. Palvelin lisäksi käsittää lisenssinvalvontavälineet (53) viestin pääsyoikeuden tulla palvelimeen ennen kuin viestin sallitaan mennä protokollapinoon (50) valvomiseksi. Keksintö koskee myös menetelmää ja tietokoneohjelmatuotetta päätteeltä palvelimessa vastaanotetun viestin pääsyoikeuden valvomiseksi palvelimessa.

Uppfinningen avser en gatewayserver för mottagning av ett meddelande från en terminal och omfattande en protokollstack (50) för bearbetning av meddelandet enligt en bestämd protokollstack. Servern omfattar vidare tillståndskontrollmedel (53) för kontroll av meddelandets accessrätt till inträde i servern innan meddelandet tillåts passera till protokollstacken (50). Uppfinningen avser även en metod och en dataprogramprodukt för att, i en server, kontrollera accessrätten för ett meddelande som i servern mottagits från en terminal.



Lisenssinvalvonta yhdyskäytäväpalvelimessa

- 5 Esillä oleva keksintö koskee lisenssinvalvontaa yhdyskäytäväpalvelimessa viestin oikeuden tulla palvelimeen valvomiseksi. Se soveltuu erityisesti matkaviestintäprotokollalle, kuten WAP:lle (Wireless Application Protocol), liikkuvan päätteen mahdollistamiseksi päästä Internetiin yhdyskäytäväpalvelimen välityksellä.
- 10 Termiä "Internet" käytetään yleisesti kuvaamaan tietoa, sisältöä, johon voidaan päästä käsiksi käyttämällä päätettä, tyypillisesti PC:tä, joka on liitetty modeemin välityksellä tietoliikenneverkkoon. Sisältö voidaan tallentaa moniin eri paikkoihin, jotka ovat etäällä yhteyden ottavasta tietokoneesta, vaikka jokainen etäpaikoista on myös yhdistetty tietoliikenneverkkoon. Sisältö voidaan rakentaa käyttämällä
- 15 HTML:ää (HyperText Mark-up Language). Internetin tekee toimivaksi vakiotietojärjestelmän spesifikaatio, joka käyttää useita protokollia, kuten TCP:tä (Transfer Control Protocol), UDP:tä (User Datagram Protocol) ja IP:tä (Internet Protocol) tietovirran ohjaamiseksi Internetin lukuisien eri komponenttien ympäri. TCP ja UDP koskevat virheiden estämistä ja korjaamista lähetetyssä Internet-
- 20 datassa. IP koskee datan strukturointia ja reitittämistä. Tämän lisäksi voidaan tarjota muita sovelluskohtaisia protokollia Internetin kautta saatavissa olevien erilaisten tietojen hallitsemiseksi ja manipuloimiseksi, esimerkiksi HTTP HTML-sisältöön pääsemiseksi, FTP tiedostoihin pääsemiseksi tai SMTP sähköpostiin pääsemiseksi.
- 25 Internet on rakennettu fyysisesti tietoliikenne- ja dataliikenneverkkojen hierarkiasta, esimerkiksi lähiverkoista (Local Area Network eli LAN), alueellisista puhelinverkoista ja kansainvälisistä puhelinverkoista. Nämä verkot on liitetty sisäisesti ja ulkoisesti niin kutsutuilla "reitittimillä", jotka vastaanottavat tietoa
- 30 lähdeisäntäkoneelta tai edelliseltä reitittimeltä lähetysketjussa ja reitittävät sen kohdeisäntäkoneelle tai seuraavalle reitittimelle lähetysketjussa.
- Matkapuhelinten käytön lisääntyessä kasvaa niin kutsutun liikkuvan Internet-liitynnän tarve, jossa liityntä tapahtuu kannettavasta tietokoneesta, joka on liitetty
- 35 matkapuhelimeen, tai integroidusta tietokone/matkapuhelinlaitteesta. Tällaisen liitynnän tarkoitus on tyypillisesti hankkia sisältöä Internetistä. On myös ehdotettu tarjota Internet-liityntä kehittyneisiin liikkuviin päätteisiin, niin kutsuttuihin kommunikaattoreihin ja älypuhelimiin esim. WAP-protokollan (Wireless

Application Protocol) avulla. WAP:lla on arkkitehtuuri, jossa on protokollapino, jolla on sovelluskerros (jota kutsutaan nimellä Wireless Application Environment eli WAE), istuntokerros (jota kutsutaan nimellä Wireless Session Protocol eli WSP), yhteystapahtumakerros (jota kutsutaan nimellä Wireless Transaction Protocol eli WTP), turvallisuuskerros (jota kutsutaan nimellä Wireless Transport Layer Security eli WTLS) ja kuljetuskerros (jota kutsutaan nimellä Wireless Datagram Protocol eli WDP), kuten kuviossa 1 on esitetty. Yläpuolella olevat kerrokset sekä muut palvelut ja sovellukset pääsevät jokaiseen arkkitehtuurin kerrokseen. Nämä protokollat on suunniteltu toimimaan useiden eri siirtotiepalvelujen yli, kuten SMS (Short Message Service), CSD (Circuit Switched Data), GPRS (General Packet Radio Service) jne. WAP-arkkitehtuuria ja protokollakerroksia kuvaava spesifikaatio on saatavissa osoitteesta <http://www.wapforum.org/>.

Internetiin pääseminen käsittää yleensä istuntojen pitämisen päätteeksi, kuten liikkuvan päätteeksi ja palvelimen välillä. Istunto on sarja vuorovaikutuksia päätteeksi ja palvelimen välillä, jolla on hyvin määritelty alku ja loppu ja joka käsittää sovitut ominaisuudet. Tyypillisesti istunto käsittää vastekerroksen, joka ilmoittaa toiselle vastekerrokselle halun järjestää istunto, jotka molemmat vastekerrokset neuvottelevat istunnon ominaisuuksista, jotka vastekerrokset ottavat osaa moninlaisiin yhteystapahtumiin, ja yhden vastekerroksen päättäessä istunnon. Ominaisuudet, joista neuvotellaan, ovat tyypillisesti vaihdettavien pakettien pituus, merkkijoukot, jotka voidaan ymmärtää ja manipuloida, ja protokollien versiot, joita tullaan käyttämään. Yhteystapahtuma on vuorovaikutuksen perusyksikkö ja se voi sisältää informaation pyytämisen ja vastaanottamisen, käynnissä olevan istunnon kumoamisen ja käynnissä olevan istunnon tilanteen ilmoittamisen vastekerrokselle. Kaikkien istuntojen piteiden istunnon muodostamiseksi ja päättämiseksi sekä kaikkien yhteystapahtumien seurauksena vastekerros generoi ja vastaanottaa tapahtumia. Tapahtumalähteitä (istuntoja ja yhteystapahtumia) on monia.

Toimenpiteitä, jotka sovellus voi herättää tapahtumien generoimiseksi, kutsutaan palveluprimitiiveiksi. Palveluprimitiivit esittävät loogista tiedonvaihtoa ja ohjausta istuntokerroksen ja muiden kerrosten välillä. Ne koostuvat käskyistä ja niiden vastaavista tiettyyn tarjottuun palveluun liittyvistä vastauksista. Palveluprimitiivin herättäminen vastekerroksessa viestintäyhteyden toisella puolella johtaa tapahtuman generoimiseen vastekerroksessa yhteyden toisella puolella. Palveluprimitiiveja on läsnä kaikissa viestintäprotokollissa.

Aktiivinen istunto voi käsittää monia yhteystapahtumia ja voi näin generoida monia tapahtumia. Riippuen nopeudesta, jolla sovellus voi käsitellä tapahtumia, jotka tulevat sen vastekerrokselta, voi käydä niin, että yhteystapahtumia on
5 enemmän kuin se voi käsitellä, ja niin se vastaanottaa enemmän tapahtumia kuin se voi käsitellä. Tässä tapauksessa tapahtumat asettuvat jonoon ja odottavat käsittelyä tuon istunnon yhteydessä. Samaan istuntoon yhteydessä olevat tai liittyvät tapahtumat täytyy yleensä käsitellä määrättyssä järjestyksessä. Joissakin
10 protokolissa istuntoa voidaan lykätä, jossa tilassa mitään yhteystapahtumia ei sallita lukuun ottamatta pyyntöä jatkaa tai lopettaa.

WAP:ssa viestintä kerrosten välillä ja yksiköiden välillä istuntokerroksen sisällä saadaan myös aikaan palveluprimitiivien avulla.

15 Useimmat yhteystapahtumat ovat joko tarjonta- tai imutyypisiä (pyyntö-vastaus). Tarjontatyyppisissä yhteystapahtumissa vastekerros lähettää tietoa, jota ei olla erityisesti pyydetty, ja imutyypisissä yhteystapahtumissa vastekerros erityisesti pyytää vastaanottamaan tietoa toiselta vastekerrokselta.

20 Päätteet, kuten henkilökohtaiset tietokoneet, hankkivat tietoa Internetistä palvelimen kautta kuten yhdyskäytäväpalvelimen. Internet käyttää HTTP:tä, joka on yksinkertainen pyyntö-vastaus -protokolla. Lähes ainoa tapahtuma on HTTP-pyyntö. Palvelimen käyttöjärjestelmä ajaa useita sovelluksia ja luo näin useita säikeitä niiden käsittelemiseksi, esimerkiksi välipalvelimia ja postipalvelimia.

25 Sovellukset käyttävät käytettävissä olevia säikeitä sitä mukaa, kun niitä tarvitaan. Siinä tapauksessa, että Internet-liityntä tapahtuu PC:llä, on tarkoituksenmukaista luoda säie palvelimeen dynaamisesti käsittelemään jokainen pyyntö, koska pyynnöt ovat riippumattomia toisistaan. Kun pyyntö on kerran käsitelty, säie on päättänyt toimintansa ja se lopetetaan.

30

Viestintäjärjestelmässä, joka käsittää yhdyskäytäväpalvelimen ja lukuisia liikkuvia päätteitä, istunnon muodostaminen vaatii suhteellisen suuren määrän kaistanleveyttä, koska päätteen ja palvelimen on neuvoteltava monista istuntoon liittyvistä ominaisuuksista. Lisäksi tietoa, joka on ainutlaatuista tietyille avatulle
35 istunnolle, voidaan menettää, jos istunto lopetetaan. Tästä ainutlaatuisesta tiedosta olisi voitu neuvotella yhteystapahtumien tuloksena. Se voi olla esimerkiksi jokin pelin tila. Jotta vältetään istuntojen avaamiselta ja sulkemiselta vaadittaessa ja uusien istuntojen muodostamiselta aina kun niitä tarvitaan,

istunnot voidaan pitää auki pitkän aikaa, jopa passiivisessa tilassa niin, että niitä voidaan jatkaa tarvittaessa. Istunto voi pysyä auki päiviä tai jopa viikkoja, kunnes se suljetaan tai kunnes pääte ei enää vastaanota tehoa esimerkiksi akusta.

Palvelimessa oleva sovellus käyttää käyttöjärjestelmän säikeidenhallintapalvelua ja luo useita säikeitä näiden istuntojen hallitsemiseksi.

WAP:ssa yhdyskäytäväpalvelin on tyypillisesti portti päätteen sallimiseksi päästä Internetiin. Yhdyskäytäväpalvelimen tarjoaa esimerkiksi palvelun tarjoaja, ja käyttäjät voivat päästä yhdyskäytäväpalvelimeen ostamalla lisenssin tai useita lisenassejä palvelun tarjoajalta. Näin ollen on tarve toteuttaa ratkaisu yhdyskäytäväpalvelimessa yhdyskäytäväpalvelimelle pääsyn valvomiseksi. Samoin yhdyskäytäväpalvelin toteutetaan tavallisesti tietokoneohjelmana, joka tietokoneeseen ladattuna toimii yhdyskäytäväpalvelimena. Siten yhdyskäytäväpalvelimen valmistaja, ts. tietokoneohjelman tekijä, voi myydä lisenassejä palvelun tarjoajalle, joka rajoittaa käyttäjien määrää, jota palvelun tarjoaja pystyy palvelemaan ostamatta lisää lisenassejä valmistajalta. Täten on tarve toteuttaa ratkaisu yhdyskäytäväpalvelimessa palvelimella käytössä olevien kokonaislisenassien määrän valvomiseksi.

Nyt on keksitty yhdyskäytäväpalvelin, jossa lisenassinvalvonta suoritetaan viestillä, joka saapuu yhdyskäytäväpalvelimeen ennen kuin sen sallitaan mennä edelleen protokollapinon, ts. lisenassinvalvonta suoritetaan protokollapinon alapuolella yhdyskäytäväpalvelinhierarkiassa. Viestin lähettäjän tunnistus tarkistetaan pääsyoikeuden määrittämiseksi. WAP-yhdyskäytävä- tai välipalvelimessa tarjotaan vielä erityisemmin WAP-pinon alapuolella ja siirtoteiden yläpuolella siirtotieportti, joka suorittaa lisenassinvalvonnan ja jonka kautta kaikki siirtoteiltä tuleva tietoliikenne kulkee ennen protokollapinon menemistä.

Esillä olevaa keksintöä voidaan käyttää viestin pääsyoikeuden valvomiseksi kummassakin yllä mainitussa tilanteessa, nimittäin sen valvomiseksi, että palvelun tarjoaja ei ylitä yhdyskäytäväpalvelimen valmistajalta ostamiensa lisenassien määrää ja sen valvomiseksi, että käyttäjäyksikkö, joka on ostanut useita lisenassejä palvelun tarjoajalta, ei ylitä tuota lisenassien määrää.

Keksinnön eräessä edullisessa suoritusmuodossa vastaanotetaan datagrammeja tai datapaketteja tietyn siirtotien kautta. Tällä datapaketilla on lähettäjän osoite, jota kutsutaan myös lähdeosoitteeksi, etäosoitteeksi tai tilaajaosoitteeksi. Lisäksi jokaisella datapaketilla on lähettäjän porttinumero, jotka kutsutaan myös

lähdeportti-, etäportti- tai tilaajan porttiedoksi. Esillä olevan keksinnön eräässä suoritusmuodossa sekä lähettäjän osoite että porttinumero tarkistetaan lähettäjän tunnistamiseksi lisenssinvalvontatarkoitusta varten.

- 5 Lisenssit lasketaan istunnoittain, ts. valvomalla samanaikaisia istuntoja samalta lisenssinhaltijalta. Lisenssiä kohti olevan istunnon aikana sallittavien yhteystapahtumien määrää ei ole rajoitettu, vaan lisenssinvalvonnassa on kysymys siitä, kuinka monen istunnon sallitaan suorittaa yhteystapahtumia samanaikaisesti. Eräässä tietyssä suoritusmuodossa istunnoille annetaan
- 10 aikaikkuna, jonka aikana lisenssi on varattu, ja ellei tuossa istunnossa aikaikkunan sisällä ole tietoliikennettä, lisenssi tuolle istunnolle vapautetaan. Seuraavan kerran, kun on tarve yhteystapahtumien suorittamiseksi tuossa istunnossa, on otettava käyttöön uusi lisenssi.
- 15 Keksinnön erään ensimmäisen aspektin mukaisesti tarjotaan palvelin viestin vastaanottamiseksi päätteeltä ja joka käsittää protokollapinon viestin käsittelemiseksi tietyn protokollapinon mukaisesti, joka palvelin lisäksi käsittää: lisenssinvalvontavälineet viestin pääsyoikeuden tulla palvelimeen ennen kuin viestin sallitaan mennä protokollapinon valvomiseksi.
- 20 Yhdessä tietyssä suoritusmuodossa keksintö käsittää yhdyskäytäväpalvelimen, joka palvelee useita liikkuvia päätteitä. Se voi olla WAP-yhdyskäytävä. Esimerkiksi käskyjä, kuten WAP-pyyntöjä, voidaan lähettää lyhytsanomaviesteissä (SMS:n generoimissa) ja lähettää WAP/HTTP-
- 25 yhdyskäytävään. Yhdyskäytävä tulkitsee nämä WAP-verkkopaketteina ja suorittaa tarvittavat HTTP-yhteystapahtumat alkuperäpalvelimella. Tämän jälkeen se lähettää takaisin WAP-viestin samalla siirtotiellä, ts. tuloksen sisältävänä SMS-viestinä.
- 30 Keksinnön erään toisen aspektin mukaisesti tarjotaan menetelmä päätteeltä palvelimessa vastaanotetun viestin pääsyoikeuden valvomiseksi palvelimessa, ja jossa protokollapino käsittelee viestin, jossa menetelmässä:
tarkistetaan viestin oikeus tulla palvelimeen ennen kuin viestin sallitaan mennä protokollapinon.
- 35 Keksinnön erään kolmannen aspektin mukaisesti tarjotaan tietokoneohjelmatuote päätteeltä palvelimessa vastaanotetun viestin pääsyoikeuden valvomiseksi

palvelimessa, ja jossa protokollapino käsittelee viestin, joka tietokoneohjelmatuote käsittää:

konekieliset ohjelmavälineet viestin pääsyoikeuden tulla palvelimeen ennen kuin viestin sallitaan mennä protokollapinoon valvomiseksi.

5

Keksintö toteutetaan edullisesti ohjelmistona, joka tietokoneeseen ladattuna toimii yhdyskäytäväpalvelimena esillä olevan keksinnön mukaisesti.

Keksintöä käsitellään seuraavassa yksityiskohtaisesti viittaamalla oheisiin

10 piirustuksiin, joissa

kuvio 1 esittää protokollapinojen järjestelyä WAP:ssa (Wireless Application Protocol),

kuvio 2 esittää viestintäjärjestelmää,

15 kuvio 3 esittää laitteistoon sisällytettyä yhdyskäytäväpalvelinta,

kuvio 4 esittää esillä olevan keksinnön mukaisen yhdyskäytäväpalvelimen toiminnallista lohkoakaaviota ja

kuvio 5 esittää lisenssinvalvonnassa suoritettavia vaiheita vuokaaviona.

20 Seuraavassa esimerkissä viestintää kuvataan viittaamalla yllä mainittuun WAP:iin (Wireless Application Protocol). Olisi huomattava, ettei keksintö rajoitu WAP:in käyttöön, ja muita protokollia ja spesifikaatioita voidaan käyttää.

Kuvio 2 esittää viestintäjärjestelmää, joka käsittää lukuisia liikkuvia päätteitä 2, 25 joilla on liityntä Internetiin 4. Liikkuvat päätteet lähettävät signaaleja 6, jotka langaton verkko 8 vastaanottaa ja jotka lähetetään sen kautta. Langaton verkko voi olla useita eri verkkojärjestelmiä, kuten GSM, CDMA IS-95, TDMA IS-136 ja UMTS, ja se voi käyttää eri tyyppistä viestintää yhden ja saman järjestelmän sisällä, esim. SMS, GPRS tai HSCSD-viestintää GSM:n sisällä. Näin voidaan 30 käyttää useita eri siirtoteitä signaalien 6 lähettämiseksi. Verkon 8 vastaanottamat WAP-pyyntö 6 reititetään väli- tai yhdyskäytäväpalvelimeen 12. Palvelin 12 kääntää WAP-pyyntö 6 HTTP-pyyntöiksi ja sallii näin liikkuvien päätteiden 2 pyytää tietoa WWW-palvelimelta 14 ja näin selata Internetiä 4. Välipalvelin koodaa ww-palvelimelta 14 saadun tiedon sopivaan muotoon, ja langaton verkko 35 lähettää sen sitten liikkuvalla päätteelle 2, joka pyysi sitä. Vastaus käsittää WML:n (Wireless Mark-up Language) WAP:n mukaisesti. WML on nimiöperusteinen näyttökieli, joka tarjoaa navigointitukea, tiedonsyötön, hyperlinkkejä, teksti- ja kuvaesityksen ja lomakkeita. Se on HTML:ää muistuttava

selauskieli. Liikkuva pääte 2 käsittelee ja käyttää tiedon. Jos WWW-palvelin 14 tarjoaa sisällön WAP/WML-muodossa, palvelin 12 voi hakea tällaisen sisällön suoraan WWW-palvelimesta 14. Jos WWW-palvelin kuitenkin tarjoaa sisällön WWW-muodossa (kuten HTML), suodatinta voidaan käyttää kääntämään sisällön WWW-muodosta WAP/WML-muotoon.

WAP soveltuu useisiin eri järjestelmiin, mukaan lukien GSM-900, GSM-1800, GSM-1900, CDMA IS-95, TDMA IS-136, laajakaistainen IS-95 ja kolmannen sukupolven järjestelmät, kuten IMT-2000, UMTS ja W-CDMA.

Vaikka kuviossa 2 esitetään tietoa haettavan Internetistä, välipalvelin itse voi sisältää halutun tiedon. Esimerkiksi tilaaja voi hakea tietoa välipalvelimen tiedostojärjestelmästä.

WWW-palvelimen 14 lisäksi liikkuvat päätteet voivat viestiä WTA-palvelimen 18 (Wireless Telephony Application) kanssa.

Kuvio 3 esittää laitteistoon, kuten tietokoneeseen 20, sisällytettyä yhdyskäytäväpalvelinta. Tietokoneella 20 on dynaaminen muisti, käsittelyteho ja muisti kaikkien niiden ohjelmien tallentamiseksi, joita tarvitaan yhdyskäytäväpalvelimen toteuttamiseen, kuten sovellusohjelma, protokollapinot ja käyttöjärjestelmä. Tietokone 20 käsittää käyttöliittymän, kuten näppäimistön 22 ja näytön 23 ja palvelinohjelman 24. Palvelinohjelmalla 24 on sovellusohjelma 26 alapuolisen protokollan tapahtumien käsittelemiseksi, kuten pyynnön hakea WML palvelimelta käsittelemiseksi, ja protokollapinot, kuten WAP-protokollapino 28 ja HTTP-protokollapino 30. Sovellusohjelma 26 ohjaa tiedon virtaa mukaan lukien käskyt, pyynnöt ja informaatio tietokoneen ja eri verkkojen välillä, mukaan lukien puhelinverkko 32, Internet 34 ja tietoverkko ja piirikytkentäiset tietoverkot 35. Sovellusohjelma 26 voi lisäksi ajaa ohjelman, joka voidaan nähdä näytöllä 23 ja jota voidaan ohjata näppäimistöllä 22 (ja esim. hiirellä). Tietokone 20 viestii Internetin 34 kanssa HTTP-protokollapinon 30 ja rajapinnan 36 välityksellä. Tietokone 20 viestii puhelinverkon 34 ja tietoverkon 35 kanssa rajapintojen 38 ja 40 välityksellä. Palvelinohjelma 24 käsittää myös yhdyskäytävän 42, joka konvertoi HTTP:n ja WAP:in välillä. SMS-sanomanvälitys voidaan tarjota dataliittymän kautta asianmukaisen laitteiston välityksellä operaattorin verkkoon.

Sovellusohjelmassa 26 ja WAP-protokollapinossa 28 olevat yksittäiset säikeet 44 käyttävät prosessoreita 46 tietokoneessa 20 tarvittavien käsittelytehtävien

suorittamiseen. Säikeiden varaamisen prosessoreille tarjoaa tietokoneen 20 käyttöjärjestelmässä 50 olevat säikeistyspalvelut 48.

5 Kuten kuviossa 1 on esitetty, WAP-pino on rakennettu niin kutsuttujen siirtoiteiden päälle (jotka tarjoavat datagrammipalveluja). Nämä siirtotiet voivat olla esimerkiksi SMS tai CSD. Siirtoteilla on omat protokollansa ja ne on toteutettu protokollapinototeutusten kautta.

10 Kuvio 4 esittää esillä olevan keksinnön mukaisen yhdyskäytäväpalvelinhierarkian toiminnallista kaaviota (joka on sisällytetty ohjelmistoon) ainakin siinä laajuudessa, että keksintö ymmärretään. Yhdyskäytäväpalvelin sisältää WPS:n (Wireless Protocol Stack) 50, kuten kuviossa 1 esitetty WAP-pino. WPS:n alapuolella ovat eri siirtotiesovittimet 51, jotka pääsevät eri siirtoteille siirtotieajureiden 52 kautta.

15

Siirtotiesovittimen toiminto on määritelty Wireless Datagram Protocol – spesifikaatiossa, ts. WAP:n WDP-spesifikaatiossa. Siinä siirtotiesovittinta kutsutaan nimellä sovituskerros tai tunneli (Adaptation Layer or Tunnel). Sovituskerros on WDP-protokollan kerros, joka kohdentaa WDP-
20 protokollatoiminnot suoraan tiettyyn siirtotiehen. Sovituskerros on eri jokaiselle siirtotielle ja se käsittelee tuon siirtotiepalvelun tiettyjä kykenevyyksiä ja ominaisuuksia. Lisäksi tunneli päättyy WAP-yhdyskäytävässä tai –palvelimessa ja siirtää WDP-paketit WAP-välipalvelimelle/-palvelimelle tunnelointiprotokollan välityksellä, joka on rajapinta siirtotiepalvelua tukevan yhdyskäytävän ja WAP-
25 välipalvelimen/-palvelimen välillä.

Sovituskerros tai siirtotiesovitin on täten komponentti, joka liittää WAP-palvelimen langattomaan verkkoon. Tukeakseen useita eri siirtoteitä, yhdyskäytäväpalvelimella on näin oltava useita eri siirtotiesovittimia 51.

30

Kaikki tieto WAP-päätteeltä tulee yhdyskäytäväpalvelimeen siirtotien kautta, jota kuviossa kuvataan siirtotieajureilla 52 ja siirtotiesovittimilla 51. Siirtotiesovittimelta tieto tulee WAP-pinoon 50, joka voi sisältää kaikki tai vain joitakin kuviossa 1 esitetystä protokollakerroksista. Esillä olevan keksinnön mukaisesti on
35 ymmärretty suorittaa lisenssinvalvonta suoraan yhdyskäytävään tulevasta tiedosta ennen kuin se menee protokollapinoon 50. Tämän suorittamiseksi tarjotaan toiminnallisesti WPS:n 50 ja siirtotiesovittimien 51 välillä siirtotieportti 53, jonka kautta kaikki datagrammiliikenne siirtotiesovittimen ja WPS:n välillä

kulkee. Näin ollen siirtotieportti 53 suorittaa lisenssinvalvonnan, ts. tarkistaa, onko jokaisella tulevilla datapaketeilla pääsyoikeus vai ei, jolloin paketin joko sallitaan mennä protokollapinoon käsiteltäväksi tai se hylätään.

- 5 WDP-spesifikaatio määrittelee palveluprimitiivin T-DUnitdata, jota käytetään tiedon lähettämiseen. Se käsittää muun muassa seuraavat parametrit:
- 1) *Lähdeosoitteen (Source Address)*, joka on lähettäjän osoite ja WDP-kerrokselle pyynnön tekevän laitteen ainutlaatuinen osoite. Lähdeosoite voi olla MSISDN-numero (Mobile Station ISDN –numero), IP-osoite (annettu
10 numeroina esim. 153.226.0.56 tai symboleina esim. mycomputer.company.subsidiary.com), X.25-osoite tai muu tunniste. Siten lähdeosoitteen parametrin pituus voi vaihdella sen mukaan, mikä lähde on.
 - 2) *Lähdeportti (Source Port)*, joka on pyynnön esittävän viestintäinstanssin lähdeosoitteeseen liittyvä sovellusosoite tai porttinumero. Lähettäjän
15 porttinumero on 16 bittinen luku.
 - 3) *Käyttäjätiedot (User Data)*, jotka ovat WDP-protokollan kuljettamat käyttäjätiedot. WDP-kerrokseen jätettyä tai sieltä vastaanotettua datayksikköä kutsutaan myös palveludatayksiköksi (Service Data Unit). Tämä on kokonainen datan yksikkö (viesti, paketti, pakkaus), jonka ylempi kerros
20 (lähettäjällä) on jättänyt WDP-kerrokseen lähetettäväksi. WDP-kerros lähettää palveludatayksikön ja toimittaa sen kohteeseensa manipuloimatta sen sisältöä.

25 *Lähdeosoitteen ja lähdeportin* parametrit ovat osa WAP-viestin otsikko-osuutta, ja *käyttäjätiedot* ovat viestin varsinainen hyötykuorma tai tiedot.

Lisenssin valvontaa varten siirtotieportti lukee sekä *lähdeosoitteen* että *lähdeportin* informaation jokaisessa datapaketeissa, joka vastaanotetaan siirtotieportissa 53 siirtotiesovittimen 51 kautta. Jokainen tilaajaosoitteen
30 (lähdeosoite) ja tilaajaportin (lähdeportti) yhdistelmä muodostaa samanaikaisen istunnon ja vaatii näin yhden lisenssin. Tämä tarkoittaa, että sama pääte voi kuluttaa enemmän kuin yhden lisenssin esimerkiksi, jos käyttäjä käyttää samanaikaisesti kahta eri sovellusta päätteessä hakemalla palvelun yhdyskäytäväpalvelimen välityksellä (esim. pankkisovelluksen ja
35 kalenterisovelluksen). Tilaajan portin numeron (lähdeportti) käyttö lähettäjän tunnistamiseksi on myös tarpeen estämään jotakuta käyttämästä välipalvelinkonetta lisenssitarkastuksen (UDP-siirtotiellä) kiertämiseksi, jossa tapauksessa useat päätteet voisivat mennä välimuistipalvelimen kautta

yhdyskäytävään, jolloin lähdeosoite olisi aina sama. Lähdeportin informaatio datapakettissa olisi kuitenkin eri.

5 Lisenssit lasketaan istunnoittain, ts. valvomalla samanaikaisia istuntoja samasta
lisenssilähitteestä. Yhteystapahtumien määrää ei ole rajaa, vaan
lisenssinvalvonnassa on kysymys siitä, kuinka monen istunnon sallitaan suorittaa
yhteystapahtumia samanaikaisesti. Edullisesti esillä olevan (keksinnön) eräässä
suoritusmuodossa on tarjottu määrätyn kokoinen aikaikkuna, jonka aikana
10 (istunto) tarvitsee lisenssin yhteystapahtumien suorittamiseksi. Aikaikkuna voi
olla esimerkiksi 10 minuuttia. Tämä tarkoittaa, että kun istunto muodostetaan,
varataan yksi lisenssi (mikä tehdään jokaiselle *lähdeosoitteen ja lähdeportin*
yhdistelmälle). Jos mitään dataa ei saavu yhdyskäytäväpalvelimeen tuon
istunnon yli tuon aikaikkunan kuluessa, ts. 10 minuutin aikana, lisenssi
vapautetaan. Seuraavan kerran, kun tuo istunto haluaa suorittaa
15 yhteystapahtuman, tarvitaan uusi lisenssi, ts. tuon datan tuossa istunnossa
sallitaan päästä ohi vain, jos tuolle lisenssinhaltijalle on vielä vapaa lisenssi.

Aikaikkunan idea lisenssintarkistuksessa on, että yhdyskäytäväpalvelin hyväksyy
viimeisen kymmenen minuutin aikana datapaketteja ainoastaan Y:stä eri
20 samanaikaisesta istunnosta. Jos datapaketti vastaanotetaan samanaikaisesta
istunnosta Y+1, tilaajalle (ts. WAP-päätteelle) lähetetään WCMP (Wireless
Control Message) –viesti 'Destination Unreachable (address unreachable)'
(Kohde Saavuttamaton (osoite saavuttamaton)).

25 Samanaikaisten istuntojen maksimilukumäärä Y määritetään tarkistamalla
lisenssintallennustiedoston sisältö (joka on tallennettu palvelintietokoneeseen
normaalilla tavalla), kun palvelin käynnistetään. Lisenssintallennustiedosto
sisältää salattuja lisenssimerkkijonoja. Jokainen lisenssimerkkijono sallii tietyn
määrän samanaikaisia istuntoja, esim. 5/10/30/100 tai 1000 samanaikaista
30 lisäistuntoa.

Vaiheet, jotka suoritetaan siirtotieportissa datapaketin pääsyoikeuksien
tarkistamiseksi, kuvataan seuraavassa kuvion 5 yhteydessä. Vaiheessa 60
datapaketti vastaanotetaan siirtotieportissa siirtotiesovittimen kautta. Vaiheessa
35 61 lähettäjän osoite ja porttinumero luetaan datapakettista. Siirtotieportti
käsittelee etäosoitteen (lähdeosoite) formatoimattomana binaaritietona, joka on
riippumaton siitä, onko se MSISDN, IP-osoite, X.25-osoite vai muu tunniste.
Vaiheessa 62 nykyinen aika T liitetään viestiin. Tätä tarkoitusta varten palvelin

pitää kelloa kuten tietokoneet normaalisti. Seuraavaksi vaiheessa 63 tehdään tarkistus jo varattujen lisenssien listasta tai tiedostosta, jotta nähdään, onko jokin varaus tai merkintä vanhempi kuin sallittu aikaikkuna, joka tässä esimerkissä on 10 minuuttia. Jos tällainen merkintä löydetään, merkintä poistetaan listasta tai tiedostosta, ja lisenssi vapautetaan. Vaiheessa lasketaan myös käytössä olevien merkintöjen lukumäärä C, ts. käytössä olevien lisenssien lukumäärä. Vaiheessa 64 tehdään tarkistus, jotta nähdään, onko lisenssi jo olemassa istunnolle, jossa datapaketti vastaanotettiin (ts. onko kulunut vähemmän kuin 10 minuuttia viimeisestä yhteystapahtumasta tuon istunnon aikana). Jos 'kyllä, merkinnässä oleva aika päivitetään syöttötiedostossa, ja datapaketin käsittely sallitaan, jolloin datapaketin sallitaan mennä protokollapinoon (vaihe 65). Jos vastaus vaiheessa 64 tehtyyn tarkistukseen on 'ei', kysymys on uudesta samanaikaisesta istunnosta, missä tapauksessa menemme vaiheeseen 66.

Vaiheessa 66 tarkistetaan, onko tietyn lisenssinhaltijan käytössä olevien lisenssien C lukumäärä pienempi kuin lisenssinhaltijan ostamien lisenssien lukumäärä Y. Jos 'kyllä', mennään vaiheeseen 67, jossa uusi lisenssi otetaan käyttöön, ts. uusi merkintä tehdään syöttölistaan, C:hen lisätään yksi, ja viestin käsittely sallitaan, jolloin datapaketin sallitaan mennä protokollapinoon. Jos vastaus vaiheeseen 66 on 'ei', jolloin tietyn lisenssinhaltijan käytössä olevien lisenssien lukumäärä C on yhtä suuri (tai suurempi, mitä sen ei pitäisi olla) kuin lisenssinhaltijan ostamien lisenssien lukumäärä Y, siirtotieportti lähettää tilaajapäätteelle WCMP-viestin (Wireless Control Message Protocol) sisällön "Destination Unreachable" (kohde saavuttamaton) kanssa, ja datapaketti hylätään (vaihe 68). Vaiheeseen 66 liittyen, samanaikaisten istuntojen maksimimäärä, ts. lisenssinhaltijan ostamien lisenssien lukumäärä Y määritetään tarkistamalla lisenssintallennuslistan (esim. erillinen tiedosto) sisältö, kun palvelin käynnistetään. Lisenssintallennustiedosto sisältää salattuja lisenssimerkkijonoja. Jokainen lisenssimerkkijono sallii esim. 5/10/30/100 tai 1000 samanaikaista lisäistuntoa.

Jos oletetaan, että kaikki datapaketit ovat tulleet tunnetusta ja voimassaolevasta tilaajaosoitteesta, silloin yllä selitetyt vaiheet riittävät lisenssinvalvonnan suorittamiseksi. Tämä voi olla hyvä lähestymistapa siihen valvontatarkoitukseen, ettei palvelun tarjoaja ylitä yhdyskäytäväpalvelimen valmistajalta ostettujen lisenssien määrää. Palvelun tarjoaja saattaa kuitenkin haluta rajoittaa pääsyä viesteihin, jotka tulevat vain tietyiltä ennalta määritetyiltä päätteiltä. Tuota tarkoitusta varten erillinen tarkistus saatetaan tehdä pitämällä

yhdyskäytäväpalvelimessa listaa (tai erillistä tiedostoa) sallituista osoitteista ja porttinumeroista yleensä ja koskien tiettyä lisenssiä, jolloin jos osoite ja porttinumero eivät vastaa mitään sallittua lisenssiä, silloin viesti hylätään ja virheilmoitus palautetaan. Tuo tarkistus voidaan tehdä täysin erillisenä kuvion 5
5 iisenssinvaivontatarkisukseksi ja suoritetaan vaiheen 61 jälkeen kuviossa 5.

Palatkaamme kuvioon 4, jossa siirtotieportilla 53 on yhteys palvelimen hallintaelimeen 54, joka ohjaa palvelintoimintaa. Palvelimen hallintaelin 54 saa ohjaukskäskyjä ylläpitäjältä 55, jonka sallitaan ohjata palvelintoimintaa
10 käyttöliittymällä 56, kuten kuviossa 3 esitetyillä näppäimistöllä 22 ja näytöllä 23. Yhteys Internetiin, kuten WWW-palvelimeen, tapahtuu rajapinnan 57 kautta.

Siirtotieportin 53 ja WPS:n 50 välillä on rajapinta 58a, joka on rajapinta WDP-datagrammien lähettämiseksi ja vastaanottamiseksi ja tiedon hakemiseksi
15 siirtotiesovittimesta 51. Lisäksi datagrammit siirretään siirtotieportin ja siirtotiesovittimen välillä rajapinnan 58b yli. Palvelimen hallintaelimen 54 ja siirtotieportin 53 välillä on lisäksi rajapinta 59 palvelimen ja siirtotieportin 53 toiminnan ohjaamiseksi ja konfiguroimiseksi. Ylläpitäjä 55 voi muuttaa lisenssinhaltijan ostamien tai hallussapitämien lisenssien määrää käyttöliittymän
20 56 välityksellä.

Kuviossa 4 esitetyt eri toimenpiteet ja toiminnalliset lohkot toteutetaan edullisesti ohjelmistolohkoina, jotka prosessori 46 ajaa soittosäikeillä 44 sovellusohjelmassa 26 ja protokollapinossa 28.

25 Esillä oleva keksintö julkaisee menetelmän, jolla lisenssinvalvontaa voidaan käsitellä yksinkertaisella tavalla suorittamalla se protokollapinon alapuolella (huomioon ottaen palvelinhierarkia). Esillä olevalla keksinnöllä vältetään WAP-yhdyskäytäväpalvelimessa tarve käyttää monia erillisiä lisenssijärjestelmiä WAP-
30 protokollan kaikille yhdistelmille. Lisenssinvalvontajärjestelmä voidaan myös toteuttaa WAP-pinon yläpuolella tai sisällä, mut tämä johtaisi erillisiin lisenssinvalvontajärjestelmiin eri protokollayhdistelmille. Etätilaaja ts. pääte voi ottaa yhteyden WAP-palvelimeen käyttämällä mitä tahansa kerrosta tai käyttämällä protokollien monia yhdistelmiä. Esimerkiksi, kun katsotaan kuviota 1,
35 protokollayhdistelmät WDP+WTLS (palveluille, jotka vaativat ainoastaan datagrammin kuljetuksen turvallisesti), WDP+WTP (sovelluksille, jotka vaativat ainoastaan yhteystapahtumapalveluita ilman turvallisuutta), WDP+WTP+WSP (sovelluksille, jotka eivät vaadi turvallisuutta, mutta muuten normaaleja WAP-

istuntoja), WDP+WTLS+WTP (sovelluksille, jotka vaativat ainoastaan yhteystapahtumapalveluja turvallisesti) ja WDP+WTLS+WTP+WSP (täydellinen WAP-pino) ovat kaikki mahdollisia, ja ne vaatisivat kaikki oman lisensoinnin laskemisjärjestelmän, jos ne toteutetaan pinon yläpuolella. Jos lisenssivalvonta toteutettaisiin WAP-pinon yläpuolella tai sisällä, syntyisi myös ongelma siitä, että kaikki protokollat eivät käytä istuntoja lainkaan, ja se tulisi ratkaista. Esimerkiksi samanaikaisten WSP-istuntojen maksimimäärää rajoittavan lisenssintijärjestelmän toteuttaminen on helppoa, mutta on myös yhteydetön WSP-protokolla, joka ei käytä istuntoja lainkaan. Esillä oleva keksintö ratkaisee tämän ongelman yleisellä tavalla tarkistamalla etäosoitteen ja etäporttitiedon protokollapinon alapuolella jokaisessa datapaketissa.

Keksintö voidaan toteuttaa ohjelmistona, joka ladattuna tietokoneeseen toimii yhdyskäytäväpalvelimena esillä olevan keksinnön mukaisesti. Keksinnön mukaisen lisenssinvalvonnan toiminnallisuus voidaan ohjelmoida esimerkiksi C- tai Java-ohjelmointikielelle tai mille tahansa muulle ohjelmointikielelle.

Tässä selityksessä on esitetty keksinnön toteutusta ja suoritusmuotoja esimerkkien avulla. Alan ammattimiehelle on ilmeistä, ettei keksintö rajoitu edellä esitettyjen suoritusmuotojen yksityiskohtiin ja että keksintö voidaan toteuttaa muussakin muodossa poikkeamatta keksinnön tunnusmerkeistä. Esimerkiksi, vaikka edellä esitetty liittyy Internetiä selaaviin liikkuviin päätteisiin tai WAP-välipalvelimeen, on ymmärrettävä, että viestintä voi olla eri tyyppistä mukaan lukien tiedon lähettäminen ja vastaanottaminen, yhteystapahtumien hoitaminen, kuten rahoitustapahtumien, sähköpostin tai viestien lähettäminen ja vastaanottaminen. Toimenpiteiden valikoimaan kuuluu pääsy palveluihin, esimerkiksi säätiedotukset, uutiset, osakehinnat, lentoaikataulut, soittoäänien lataus, pankkipalvelut mukaan lukien tiedon hankinta ja maksut. Se voi esiintyä muissakin viestintäympäristöissä kuin Internet ja sitä voidaan käyttää myös muiden protokollapinojen kuin WAP:n kanssa. Täten esitettyjä suoritusmuotoja tulisi pitää valaisevina, muttei rajoittavina. Siten keksinnön toteutus- ja käyttömahdollisuuksia rajoittavatkin ainoastaan oheistetut patenttivaatimukset. Niin muodoin vaatimusten määrittelemät erilaiset keksinnön toteutusvaihtoehdot, myös ekvivalenttiset toteutukset kuuluvat keksinnön piiriin.

Patenttivaatimukset

1. Menetelmä päätteeltä palvelimessa vastaanotetun viestin pääsyoikeuden valvomiseksi palvelimessa, ja jossa protokollapino (50) käsittelee viestin, jossa menetelmässä:

5 tarkistetaan viestin oikeus tulla paiveiimeen ennen kuin viestin saiiitaan mennä protokollapinoon (50).

2. Patenttivaatimuksen 1 mukainen menetelmä, jossa viesti on datapaketti, joka käsittää

10 lähettäjän osoitteen, joka määrittelee päätteen osoitteen, porttinumeron, joka määrittelee päätteellä viestin lähettävän instanssin sovellusosoitteen ja

käyttäjätiedot mukaan luettuna viestin sisällön, ja lisäksi menetelmässä

15 luetaan sekä lähettäjän osoite että porttinumero datapaketista päätteen tunnistamiseksi.

3. Patenttivaatimuksen 1 mukainen menetelmä, jossa menetelmässä lisäksi:

20 viestitään viestejä tietyn langattoman verkon kanssa ja sovitetaan langattomasta verkosta vastaanotettuja viestejä protokollapinolle (50), ja sovittamisen jälkeen suoritetaan pääsyoikeuden tarkistaminen.

4. Patenttivaatimuksen 2 mukainen menetelmä, jossa menetelmässä lisäksi:

25 muodostetaan istunto palvelimen ja päätteen välille ja vastaanotetaan datapaketti istunnon kuluessa,

varataan lisenssi istunnolle vasteena pääsyoikeuden olemassaolon määrittämiseksi ja

30 seurataan aikaa, joka kului siitä, kun viimeinen datapaketti saapui yhdessä istunnossa ja vapautetaan lisenssi istuntoa varten, milloin ennalta määritely aika on kulunut siitä, kun viimeinen datapaketti saapui istunnossa.

5. Patenttivaatimuksen 2 mukainen menetelmä, jossa menetelmässä lisäksi:

tallennetaan lisenssinhaltijan ostamien pääsyoikeuslisenssien lukumäärä (Y) ja

35 vastaanotetaan lisenssi (C) jokaista datapaketista löytyvää eri lähettäjän osoitteen ja porttinumeron yhdistelmää varten ja

valvotaan, ettei varattujen lisenssien lukumäärä (C) ylitä ostettujen pääsyoikeuslisenssien lukumäärää (Y).

6. Patenttivaatimuksen 1 mukainen menetelmä, jossa menetelmässä lisäksi:
viedään viesti protokollapinoon (50) vasteena sallitun pääsyn
määrittämiselle ja
5 hylätään viesti vasteena kielletyn pääsyn määrittämiselle.
7. Patenttivaatimuksen 6 mukainen menetelmä, jossa menetelmässä lisäksi:
palautetaan virheilmoitus päätteelle vasteena hylätylle viestille.
- 10 8. Patenttivaatimuksen 4 mukainen menetelmä, jossa milloin lisenssi on
vapautettu tiettyä istuntoa varten ja datapaketti saapuu jälleen tuossa istunnossa,
suoritetaan pääsyoikeuden tarkistus vastavastaanotetulle datapaketilte ja
varataan uusi lisenssi, kun pääsy sallitaan.
- 15 9. Patenttivaatimuksen 4 mukainen menetelmä, jossa milloin datapaketti saapuu
ennen kuin mainittu ennalta määritelty aika on kulunut, suoritetaan
pääsyoikeuden tarkistus vastavastaanotetulle datapaketilte ja sallitaan pääsy jo
varatun lisenssin perusteella uutta lisenssiä varaamatta.
- 20 10. Minkä tahansa edellä esitetyn patenttivaatimuksen mukainen menetelmä,
jossa päätteet käsittävät liikkuvia päätteitä, esimerkiksi matkapuhelimia, jotka
tukevat WAP:ia (Wireless Application Protocol).
11. Palvelin viestin vastaanottamiseksi päätteeltä ja käsittäen protokollapinon
25 (50) viestin käsittelemiseksi tietyn protokollapinon mukaisesti, joka palvelin lisäksi
käsittää:
lisenssinvalvontavälineet (53) viestin pääsyoikeiden tulla palvelimeen
ennen kuin viestin sallitaan mennä protokollapinoon (50) valvomiseksi.
- 30 12. Patenttivaatimuksen 11 mukainen palvelin, jossa viesti on datapaketti
käsittäen
lähettäjän osoitteen, joka määrittelee päätteen osoitteen,
porttinumeron, joka määrittelee päätteellä viestin lähettävän instanssin
sovellusosoitteen ja
35 käyttäjätiedot mukaan lukien viestin sisällön,
ja palvelin lisäksi käsittää
välineet (53) sekä lähettäjän osoitteen että porttinumeron lukemiseksi
datapaketilte päätteen tunnistamiseksi.

13. Patenttivaatimuksen 11 mukainen palvelin, jossa palvelin lisäksi käsittää
siirtotiesovittimen (51) viestien viestimeksi tietyn langattoman verkon
kanssa ja langattomasta verkosta vastaanotettujen viestien sovittamiseksi
5 protokollapinolle (50), ja jossa lisenssinvalvontavälineei (53) on sijoitettu
toiminnallisesti protokollapinon (50) alapuolelle ja siirtotiesovittimen (51)
yläpuolelle palvelinhierarkiassa.
14. Patenttivaatimuksen 12 mukainen palvelin, jossa palvelin lisäksi käsittää
10 kytkentävälineet (50 – 52) istunnon muodostamiseksi palvelimen ja
päänteen välille ja datapaketin vastaanottamiseksi istunnon kuluessa,
varaamisvälineet (53) lisenssin varaamiseksi istuntoa varten vasteena
sille, että lisenssinvalvontavälineet (53) ovat määritelleet pääsyoikeuden
olemassaolon ja
15 ajoitusvälineet (53) viimeisen datapaketin saapumisesta yhdessä
istunnossa kuluneen ajan seuraamiseksi ja lisenssin vapauttamiseksi istuntoa
varten, milloin ennalta määriteltä aika on kulunut siitä, kun viimeinen datapaketti
saapui istunnossa.
- 20 15. Patenttivaatimuksen 12 mukainen palvelin, jossa palvelin lisäksi käsittää
tallennusvälineet lisenssinhaltijan ostamien pääsyoikeuslisenssien
määrän (Y) tallentamiseksi ja
välineet lisenssin (C) varaamiseksi datapaketista löytyvää jokaista eri
lähettäjän osoitteen ja porttinumeron yhdistelmää varten ja
25 välineet sen valvomiseksi, ettei varattujen lisenssien lukumäärä (C) ylitä
ostettujen pääsyoikeuslisenssien lukumäärää (Y).
16. Patenttivaatimuksen 11 mukainen palvelin, jossa palvelin lisäksi käsittää
välineet (53) viestin viemiseksi protokollapinoon (50) vasteena sallitun pääsyn
30 määrittämislle ja viestin hylkäämiseksi vasteena kielletyn pääsyn
määrittämislle.
17. Patenttivaatimuksen 16 mukainen palvelin, jossa palvelin lisäksi käsittää
välineet (53) virheilmoituksen palauttamiseksi päätteelle vasteena hylätylle
35 viestille.
18. Minkä tahansa patenttivaatimuksen 11-17 mukainen palvelin käsittäen
yhdyskäytäväpalvelimen, joka palvelee lukuisia liikkuvia päätteitä.

19. Patenttivaatimuksen 18 mukainen palvelin käsittäen WAP-yhdyskäytävän.

20. Tietokoneohjelmatuote päätteeltä palvelimessa vastaanotetun viestin
5 pääsyoikeuden valvomiseksi palvelimessa, ja jossa protokollapino (50) käsittelee viestin, joka tietokoneohjelmatuote käsittää:

konekieliset ohjelmavälineet (53, 56, 63) viestin pääsyoikeuden tulla palvelimeen ennen kuin viestin sallitaan mennä protokollapinoon (50) valvomiseksi.

Patentkrav

1. En metod för att, i en server, kontrollera accessrätten för ett meddelande som i servern mottagits från en terminal och där meddelandet bearbetas av en protokollstack (50), där metoden omfattar:
 - 5 kontroll av meddelandets rätt till inträde i servern innan meddelandet tillåts passera till protokollstacken (50).

2. En metod enligt patentkrav 1 där meddelandet är ett datapaket omfattande avsändarens adress som specificerar terminaladressen,
 - 10 ett portnummer som specificerar applikationsadressen till den instans som sänder meddelande vid terminalen och
 - användardata inklusive meddelandets innehåll,
 - och metoden omfattar vidare
 - läsning av både avsändarens adress och portnummer i datapaketet i syfte att
 - 15 identifiera terminalen.

3. En metod enligt patentkrav 1 där metoden vidare omfattar:
 - att meddelanden kommuniceras med ett bestämt trådlöst nätverk och de från det trådlösa nätverket mottagna meddelandena anpassas till
 - 20 protokollstacken (50), och efter anpassningen utförs en kontroll av accessrätten.

4. En metod enligt patentkrav 2 där metoden vidare omfattar:
 - att en session upprättas mellan server och terminal och datapaketet mottas under sessionen,
 - 25 att ett tillstånd reserveras för sessionen som en respons på att accessrättens befintlighet fastställts och
 - att följa den tid som förflutit sedan det sista datapaketet anlant under en session och frigöra tillståndet för sessionen när en på förhand bestämd tid förflutit sedan det sista datapaketet anlant under sessionen.
 - 30

5. En metod enligt patentkrav 2 där metoden vidare omfattar:
 - att lagra ett antal (Y) accessrättstillstånd som köpts av en tillståndsinnehavare och
 - att reservera ett tillstånd (C) för varje olika kombination av
 - 35 avsändaradress och portnummer som kan påträffas i datapaketet och
 - att kontrollera att antalet reserverade tillstånd (C) inte överskrider antalet köpta accessrättstillstånd (Y).

6. En metod enligt patentkrav 1 där metoden vidare omfattar:
att föra meddelandet till protokollstacken (50) som en respons på
fastställd tillåten access och
att avvisa ett meddelande som en respons på fastställd nekad access.
- 5
7. En metod enligt patentkrav 6 där metoden vidare omfattar:
att ett felmeddelande återförs till terminalen som en respons på ett avvisat
meddelande.
- 10
8. En metod enligt patentkrav 4, där, när tillståndet har frigjorts för en bestämd
session och ett datapaket på nytt anländer under sessionen, en kontroll av
accessrätten utförs för det nyligen anlända datapaketet och ett nytt tillstånd
reserveras efter att access tillåts.
- 15
9. En metod enligt patentkrav 4, där, när datapaketet anländer före den nämnda
förbestämda tiden har förflutit, en kontroll av accessrätten utförs för det nyligen
mottagna datapaketet och access tillåts på basis av det redan reserverade
tillståndet utan att reservera nytt tillstånd.
- 20
10. En metod enligt vilket som helst av de tidigare nämnda patentkraven i vilken
terminalerna omfattar mobila terminaler, till exempel mobiltelefoner, som stöder
WAP (Wireless Application Protocol).
- 25
11. En server för mottagning av ett meddelande från en terminal och omfattande
en protokollstack (50) för bearbetning av meddelandet enligt en bestämd
protokollstack, där servern vidare omfattar:
tillståndskontrollmedel (53) för kontroll av meddelandets accessrätt till
inträde i servern innan meddelandet tillåts passera till protokollstacken (50).
- 30
12. En server enligt patentkrav 11 där meddelandet är ett datapaket som omfattar
avsändarens adress som specificerar terminalens adress,
ett portnummer som specificerar applikationsadressen till den instans
som sänder meddelandet vid terminalen och
användardata inklusive meddelandets innehåll,
- 35
- och servern dessutom omfattar
medel (53) för läsning av både avsändarens adress och portnummer i
datapaketet i syfte att identifiera terminalen.

13. En server enligt patentkrav 11 där servern vidare omfattar
en bäraradapter (51) för kommunikation av meddelanden med ett
bestämt trådlöst nätverk och för att anpassa meddelanden mottagna från det
trådlösa nätverket till protokollstacken (50) och där tillståndskontrollmedlen (53)
5 funktionellt i serverhierarkin har placerats under protokollstacken (50) och ovanför
bäraradaptern (51) .
14. En server enligt patentkrav 12 där servern vidare omfattar
kopplingsmedel (50-52) för upprättandet av en session mellan server och
10 terminal och för mottagning av datapaketet under sessionen,
reserveringsmedel (53) för att reservera ett tillstånd för sessionen som en
respons på att tillståndskontrollmedlen (53) har fastställt accessrättens
befintlighet och
tiduppföjningsmedel (53) för att följa den tid som förflutit sedan det sista
15 datapaketet anlänt under en session och frigöra tillståndet för sessionen när en
på förhand bestämd tid förflutit sedan det sista datapaketet anlänt under
sessionen.
15. En server enligt patentkrav 12 där servern vidare omfattar
20 lagringsmedel för att lagra ett antal (Y) accessrättstillstånd som köpts av
en tillståndsinnehavare och
medel för att reservera ett tillstånd (C) för varje olika kombination av
avsändaradress och portnummer som kan påträffas i datapaketet och
medel för att kontrollera att antalet reserverade tillstånd (C) inte
25 överskrider antalet köpta accessrättstillstånd (Y).
16. En server enligt patentkrav 11, där servern vidare omfattar medel (53) för att
föra meddelandet till protokollstacken (50) som en respons på fastställd tillåten
access och för att avvisa meddelandet som en respons på fastställd nekad
30 access.
17. En server enligt patentkrav 16, där servern vidare omfattar medel (53) för att
återföra ett felmeddelande till terminalen som en respons på ett avvisat
meddelande.
35
18. En server enligt vilket som helst av patentkraven 11-17 som omfattar en
förmedlingsnodsserver som betjänar en mångfald av mobila terminaler.

19. En server enligt patentkrav 18 som omfattar en WAP-gateway.
20. En dataprogramprodukt för att, i en server, kontrollera accessrätten för ett meddelande som i servern mottagits från en terminal och där meddelandet
- 5 bearbetas av en protokollstack (50), där dataprogramprodukten omfattar:
- maskinläsbara programmedel (53, 56, 63) för kontroll av meddelandets accessrätt till inträde i servern innan meddelandet tillåts passera till protokollstacken (50).

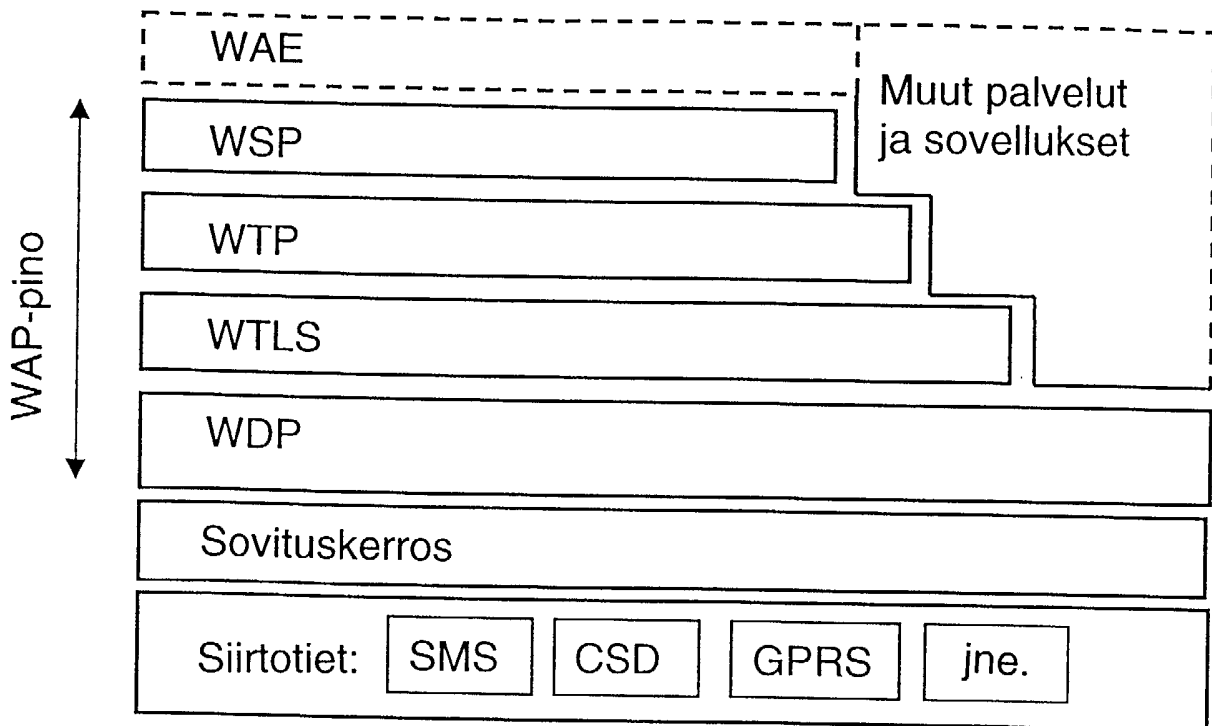


Fig. 1

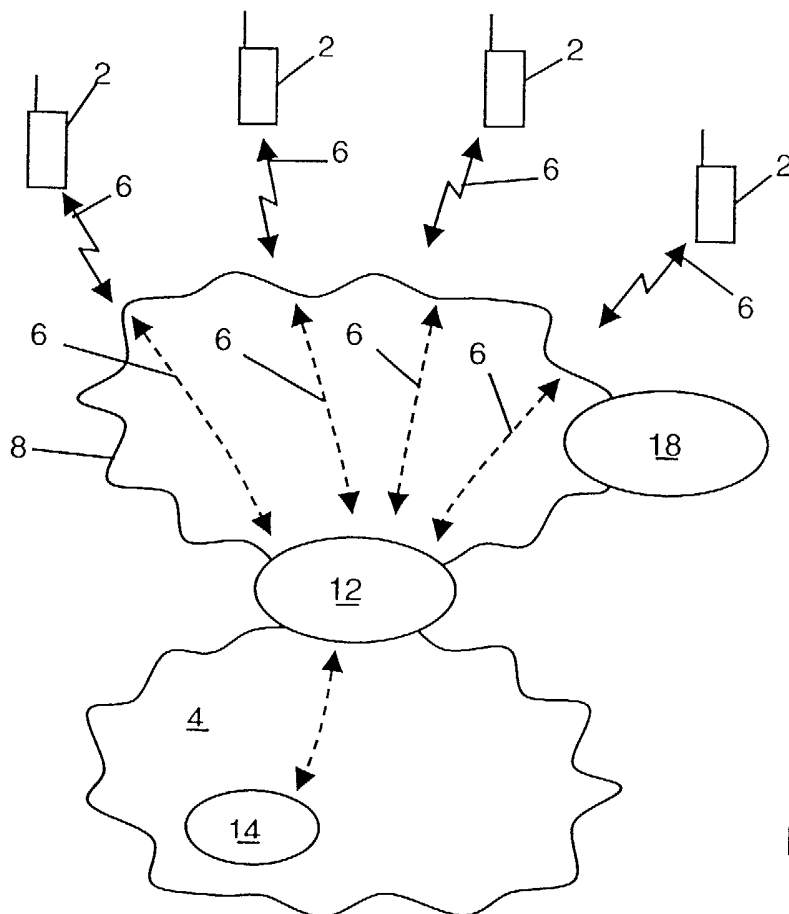


Fig. 2

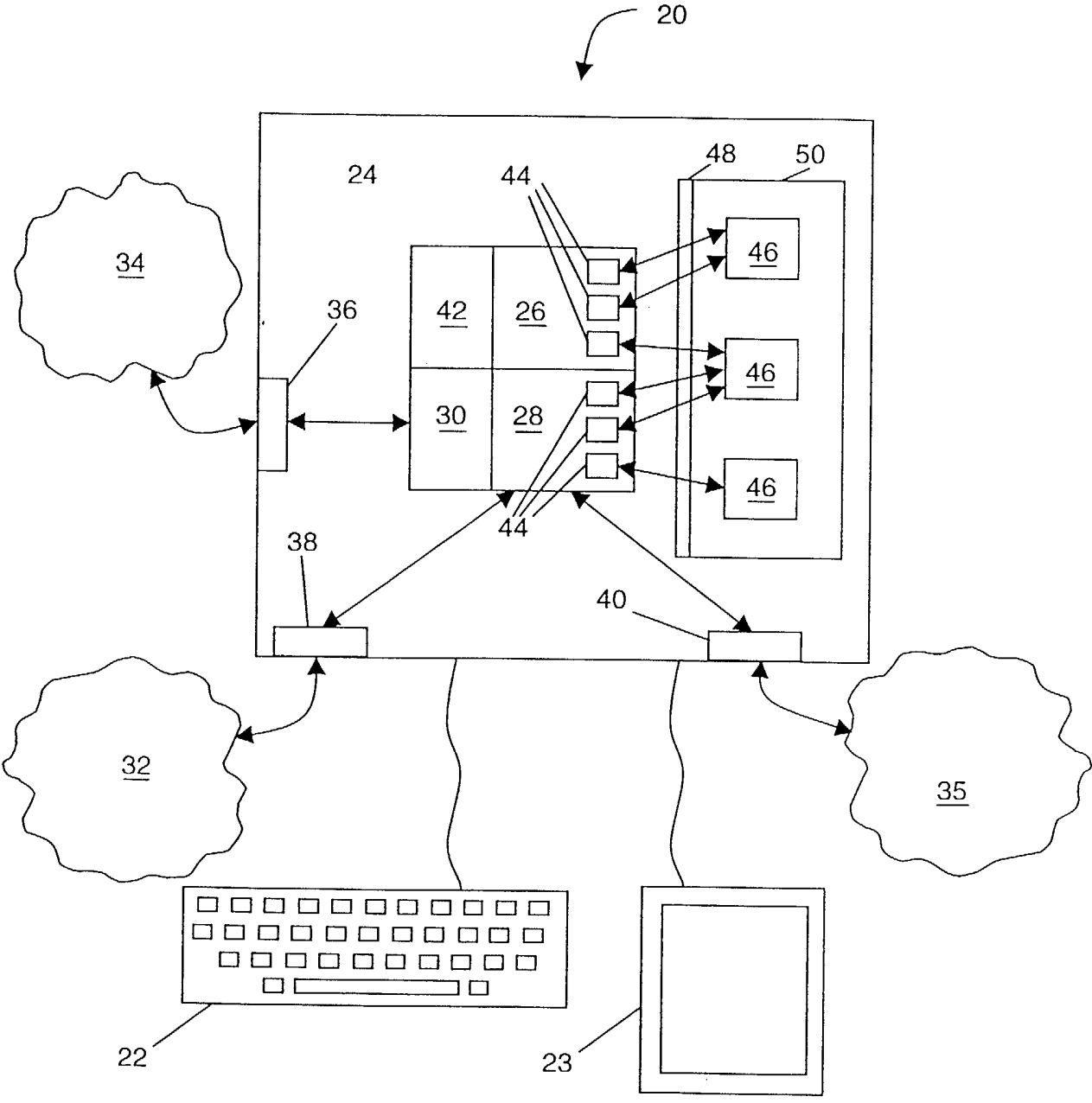


Fig. 3

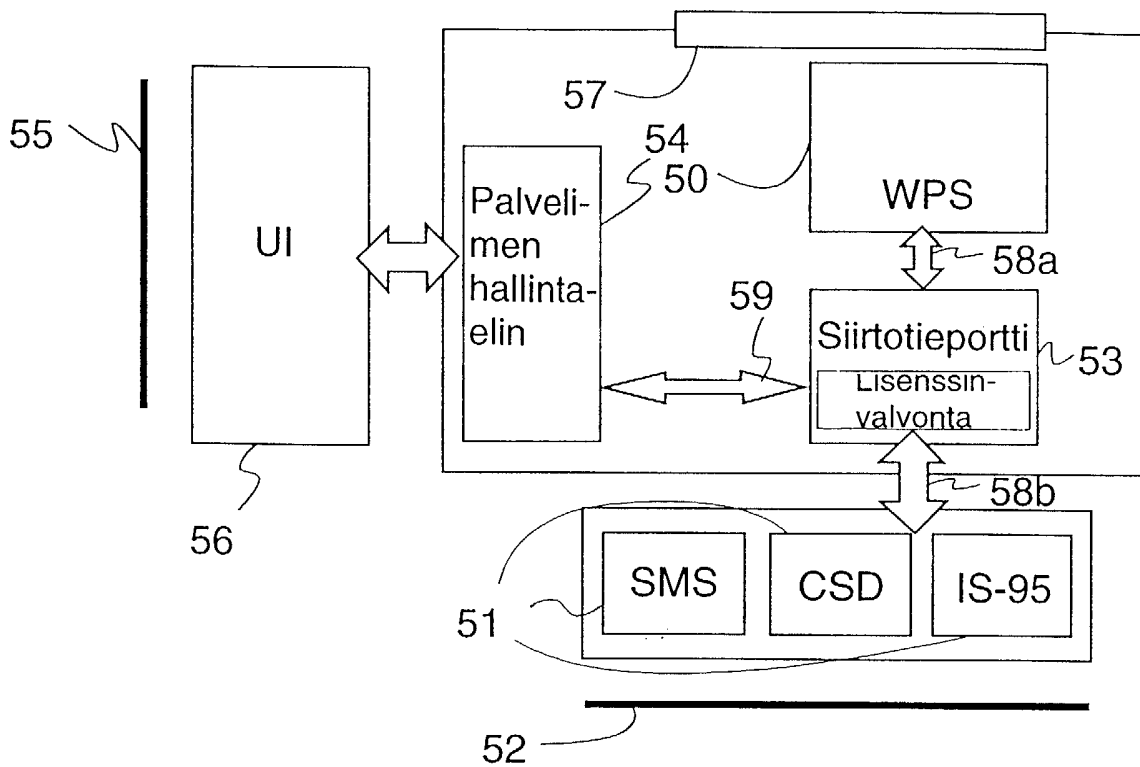


Fig. 4

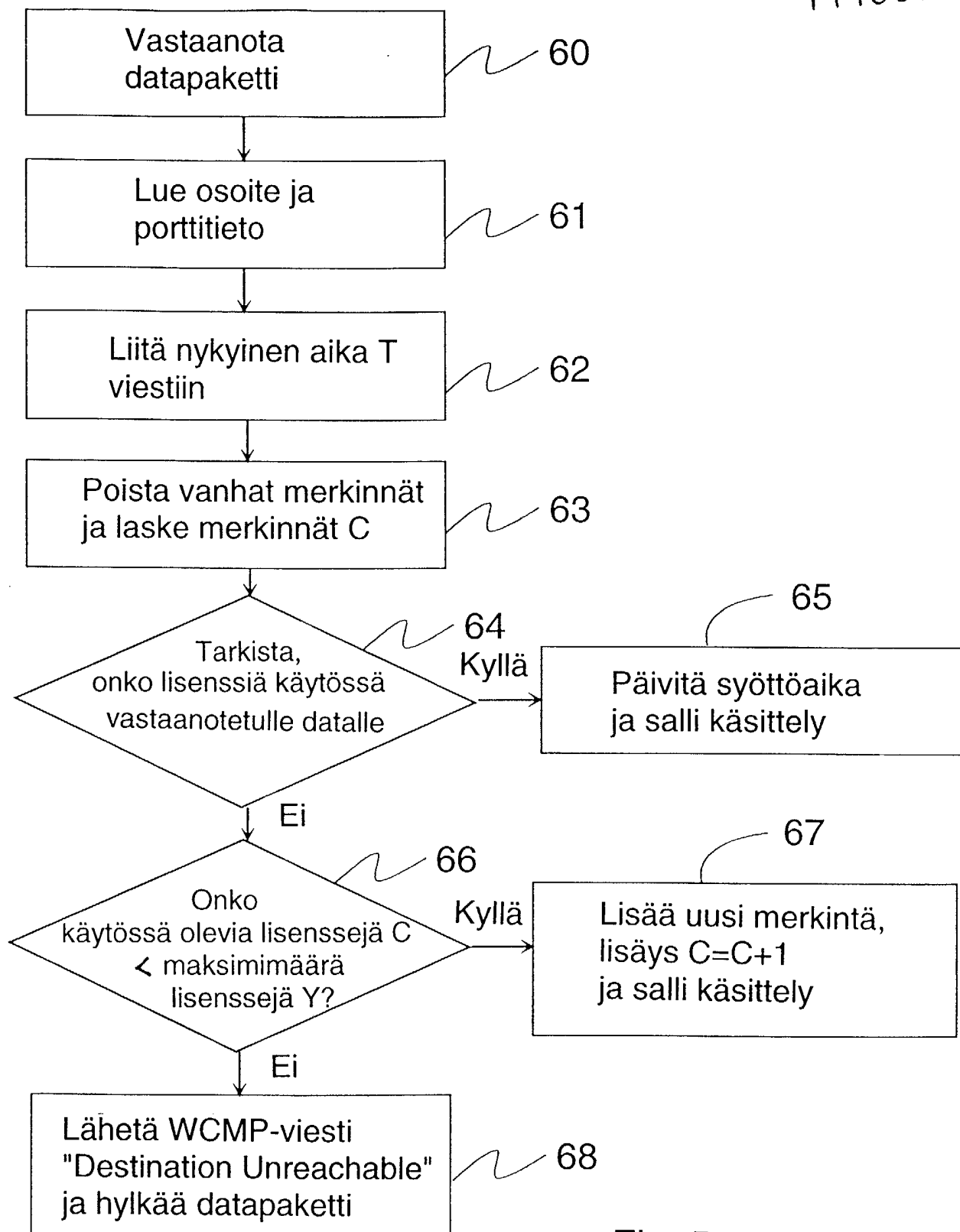


Fig. 5