FI000102134B

(12) PATENTTIJULKAISU
PATENTSKRIFT

(10) FI 102134 B

(45) Patentti myönnetty - Patent beviljats 15.10.1998

(51) Kv.lk.6 - Int.kl.6
H 04Q 7/38

(21) Patenttihakemus - Patentansökning 915237

(22) Hakemispäivä - Ansökningsdag 06.11.1991

(24) Alkupäivä - Löpdag 29.01.1991

(41) Tullut julkiseksi - Blivit offentlig 06.11.1991

(86) Kv. hakemus - Int. ansökan PCT/SE91/00066

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

09.03.1990 SE 9000856 P

SUOMI-FINLAND

(FI)

Patentti- ja rekisterihallitus
Patent- och registerstyrelsen

(73) Haltija - Innehavare

1. **Oy L M Ericsson Ab**, 02420 Jorvas, (FI)

(72) Keksijä - Uppfinnare

1. **Dent, Paul Wilkinson**, Stehags Prästgård, 240 36 Stehag, Sverige, (SE)
2. **Raith, Alex Krister**, Sorögatan 19, 164 41 Kista, Sverige, (SE)
3. **Dahlin, Jan Erik Åke Steiner**, Såningsvägen 152, 175 45 Järfälla, Sverige, (SE)

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

(54) Keksinnön nimitys - Uppfinningens benämning

Förfarande att utföra behörighetskontroll mellan en basstation och en mobilstation i ett mobilradiosystem
Menetelmä käyttöoikeuskontrollin suorittamiseksi tukiaseman ja liikkuvan aseman välillä radiopuhelinjärjestelmässä

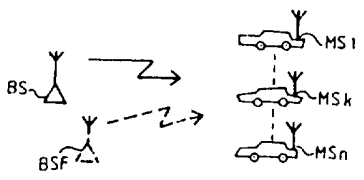
(56) Viitejulkaisut - Anförda publikationer

---

(57) Tiivistelmä - Sammandrag

Ett förfarande att utföra en behörighetskontroll i ett mobiltelefonsystem, i vilket en äkta basstation (BS) betjänar ett antal mobilstationer (MS1-MSn). Det är tidigare känt att utföra en enkelriktad kontroll från basstationen (BS) till en uppringande mobilstation (MSk). En falsk basstation (BSF) kan härigenom utföra en falsk behörighetskontroll genom att samla en mängd s k RAND-Responspar. För att undvika detta införs ytterligare en enkelriktad behörighetskontroll basstation-mobilstation och dessutom en behörighetskontroll från mobilstationen till basstationen. I ett utförande av förfarandet utesluts den enkelriktade kontrollen och endast den dubbelriktade behörighetskontrollen genomförs.

Menetelmä käyttöoikeusjärjestelmän suorittamiseksi radiopuhelinjärjestelmässä, jossa aito tukiasema (BS) palvelee joukkoa liikkuvia asemia (MS1-MSn). On aikaisemmin tunnettua suorittaa yksisuuntainen kontrolli tukiasemalta (BS) soitetulle liikkuvalle asemalle (MSk). Väärä tukiasema (BSF) voi tällöin suorittaa väärän käyttöoikeuskontrollin keräämällä joukon n.s. RAND-vastauspareja. Tämän välttämiseksi otetaan käyttöön vielä yksi yksisuuntainen käyttöoikeuskontrolli tukiasema-liikkuva-asema ja sitäpaitsi käyttöoikeuskontrolli liikkuvalta asemalta tukiasemalle. Menetelmän yhdessä suoritusmuodossa suljetaan pois yksisuuntainen kontrolli ja ainoastaan kaksisuuntainen käyttöoikeuskontrolli suoritetaan.



Förfarande att utföra behörighetskontroll mellan en basstation och en mobilstation i ett mobilradiosystem

Tekniskt område

Uppfinningen avser ett förfarande att utföra en behörighetskontroll mellan en basstation och en mobilstation i ett mobilradiosystem, speciellt i ett cellulärt mobiltelefonsystem. Det föreslagna förfarandet kan även tillämpas på andra mobilradiosystem, exempelvis pagingsystem.

Teknikens ståndpunkt

I exempelvis ett cellulärt mobiltelefonsystem sker en behörighetskontroll innan ett samtal uppkopplas mellan mobilen och basstationen. Basstationen begär information av mobilen om dennas identitet genom att beordra denna att sända ett identifikationsnummer. Mobilen är därvid tvungen att visa sin identitet för basen så att denna vet att mobilen är behörig att skicka ut ett samtal över systemet och att basstationen samt växeln vet vilken mobil som skall debiteras för det därefter uppkopplade samtalet.

Mobilstationen å sin sida måste veta säkert att den kommunicerar med en äkta basstation, dvs en basstation som verkligen kan förmedla samtal i det fall att mobilen är den uppringande parten (mobilen är A-abonnent), och att korrekt debitering sker.

För att utföra en behörighetskontroll är tidigare känt att i basstationen och mobilstationen bilda behörighetssignaler "Resp" -signaler. Ett slumptal (RAND) utsänds från basen till mobiler inom basstationens täckningsområde. Den uppringande mobilen svarar med en viss signal (Resp 1). Basstationen bildar på samma sätt ur slumptalet och den uppringande mobilens identitet samma signal Resp 1. Normalt överensstämmer dessa och basstationen beordrar mobilen till en talkanal.

Redogörelse för uppfinningen

I ovannämnda kända metod för behörighetskontroll bildas således ett RAND-Response par för en viss mobilstation, dvs för ett visst mottaget slumptal RAND bildas i mobilen en viss Responssignal och en basstation kan alltså motta en mängd sådana Responssignaler för en mängd olika slumptal. Detta innebär att en "falsk" basstation skulle kunna upprättas, som utsänder en mängd olika slumptal och mottar motsvarande mängd (olika) Responssignaler. Den falska basstationen kan därvid skapa ett mobilabonnemang som inte är behörigt att sända samtal över systemet. Denna nackdel eller brist hos den kända behörig-

hetskontrollen beror på att kontrollen är enkelriktad, nämligen så att det är endast basstationen som kräver den Responssignal som avgör mobilens behörighet.

Enligt föreliggande förfarande är behörighetskontrollen dubbelriktad, dvs det är ej endast basstationen som kräver identitet från mobilen, utan även mobilen kräver identitet från basstationen.

Ändamålet med föreliggande uppfinning är således att åstadkomma ett förbättrat förfarande för behörighetskontroll så att manipulering med falsk basstation i syfte att få tillgång till mobiltelefonsystemets behörighetskod omöjliggöres.

Förfarandet är därvid kännetecknat så som det framgår av patentkravet 1 och respektive 5. Utföringsformer av det föreslagna förfarandet framgår av de beroende patentkraven 2 - 4, 6 och 7.

Figurförteckning

Uppfinningen skall närmare beskrivas med hänvisning till bifogade ritningar där

figur 1 visar schematiskt kommunikation mellan två basstationer och ett flertal mobila stationer;

figur 2 visar ett flödesschema som illustrerar ett utförande av det föreslagna förfarandet;

figur 3 visar i ett blockschema ingångs- och utgångsstorheter till en behörighetsalgoritm ingående i en mobilstation;

figur 4 visar ett flödesschema över ett annat utförande av det föreslagna förfarandet.

Utföringsformer

Figur 1 visar en äkta basstation BS som lyssnar genom att sända ut slumptal över en viss kontrollkanal till ett antal mobiler MSl-MSn. Av dessa är det en mobil MSk som svarar och vill upprätta ett samtal över en viss talkanal. Såsom beskrivits ovan utförs på känt sätt en enkelriktad behörighetskontroll genom att basen kräver ett svar Resp 1 från mobilen MSk. Detta kommer att närmare beskrivas i samband med figur 2. Eftersom förbindelsen under detta skede är enkelriktad kan en falsk basstation BSF enligt ovan inhämta svar från en mängd mobiler vid utsändning av ovannämnda slumptal RAND. Basstationen BSF kan därvid skapa en bank av RAND-Responssvar som sedan obehörigt kan utnyttjas av en mobilstation.

För att omöjliggöra detta föreslås ett behörighetsförfarande som framgår av flödesschemat enligt figur 2.

En äkta basstation BS lyssnar på ett antal mobiler MSl-MSn inom sitt täckningsområde genom att utsända ett slumptal RAND, block 1.

En viss mobilstation MSk som vill upprätta ett samtal svarar med en signal Resp 1, block 2. Denna signal bildas i mobilens mikroprocessor ur ett antal indata PIN, ESN och DN förutom det mottagna slumptalet RAND, se figur 3, där PIN= mobilens personliga identifikationsnummer, ESN= mobilens elektroniska serienummer, DN= slaget nummer. Mobilstationen MSk är därvid en A-abonnent. Mikroprocessorn 13 avger därefter Resp l-signalen som består av en 18 bitars AUTHR-signal och en 8 bitars RANDC-signal, som sänds till basstationen.

Basstationen beräknar Resp 1 på motsvarande sätt, block 3, ur de inkommande signalerna AUTHR och RANDC och gör en jämförelse med det av mobilen beräknade och översända värdet på Resp-signalen, block 4. Om dessa överensstämmer beordrar basstationen mobilen till en viss tilldelad talkanal, block 5, och förbindelsen etableras på känt sätt, block 6. Ovan beskrivna förfarande är förut känt.

Enligt det föreslagna förfarandet bildar nu basstationen en svarssignal Resp 2 ur ett nytt slumptal RAND 2 och ur mobilens personliga identifikationsnummer PIN, vilket är känt i basstationen (block 2,3). Både Resp 2 och RAND 2 sänds till mobilen, block 7. Mobilstationen bildar ett värde på Resp 2 ur sitt PIN och det mottagna slumptalet RAND 2, block 8. Jämförelse görs nu i mobilen, block 9, mellan mottaget Resp 2 och det bildade värdet på Resp 2. Om dessa två värden överensstämmer bildar mobilen ett värde Resp 3 och överför detta till basstationen, block 10. Resp 3 bildas ur RAND 2 och PIN i mobilen. Basstationen bildar Resp 3 på samma sätt ur RAND 2 och PIN, vilka är kända i basstationen, block 11. Därefter görs en jämförelse, block 12, mellan mottaget och bildat värde på Resp 3. Om värdena överensstämmer fortsätter uppkopplingen till en upprättad talförbindelse.

Förfaringsstegen enligt block 7, 8 och 9 innebär en behörighetskontroll i vilken mobilen avgör om basstationen är äkta, eftersom verifiering av den från basstationen utsända signalen Resp 2 sker i mobilen och mot ett i mobilen beräknat värde Resp 2. Signalen Resp 2 från basstationen kan därför betraktas som en svarssignal från denna. Ovanstående förfarande utgör den väsentliga skillnaden jämfört med det kända behörighetsförfarandet enligt block 2, 3 och 4.

Kontrollen enligt block 10, 11 och 12 utgör väsentligen en upprepning av förfarandet enligt block 2, 3 och 4, dvs kontroll från basstationen att mobilen är behörig.

Den väsentliga skillnaden relativt det kändabehörighetsförfarandet (block 1-4) består i att även mobilen kräver ett svar Resp 2 från basstationen och verifierar detta enligt block 7-9. En falsk basstation måste därför exakt veta hur en beräkning av denna svarssignal skall utföras. Kontrollen blir därvid dubbelriktad.

Behörighetskontrollen enligt blocken 2, 3 och 4 kan utföras på en allmän kontrollkanal i mobilradiosystemet, och behörighetskontrollen enligt blocken 7-12 kan utföras på den talkanal som upprättades mellan basstationen BS och mobilen MSk (block 5 och 6).

Figur 4 visar ett blockschema över de första stegen i det fall att endast en dubbelriktad behörighetskontroll utförs. Stegen enligt block 1-3 ersätter därvid stegen enligt block 1-6 i figur 2. I detta fall utförs således ingen enkelriktad (och känd) behörighetskontroll före den dubbelriktade kontrollen. En uppringande mobil, exempelvis MSk begär en förbindelse hos basstationen BS. Vid mottagning av denna anropsbegäran söker basstationen BS upp en ledig talkanal och beordrar mobilen MSk till denna lediga kanal. Härigenom är en ledig förbindelse etablerad över talkanalen utan att någon behörighetskontroll har utförts. Därefter följer självabehörighetskontrollenpå det sätt som ovan är beskrivet i samband med block 7-12 i figur 2, dvs enbart en dubbelriktad behörighetskontroll har utförts.

Patentkrav

1. Förfarande för att utföra en behörighetskontroll mellan en basstation (BS) och en mobilstation (MSk) i ett mobilradiosystem, där basstationen före uppkoppling av en förbindelse sänder en förfrågan om mobilens behörighet och beordrar mobilen att sända en första svarssignal (Resp 1) som används för att i basstationen konstatera mobilens behörighet, k ä n n e t e c k n a t av att efter det att mobilens behörighet har konstaterats (2, 3, 4) i basstationen, utsändes från basstationen en andra svarssignal (Resp 2) till mobilen, som därvid bildar (8) en motsvarande andra svarssignal (Resp 2) för att konstatera (9) basstationens (BS) behörighet innan förbindelsen upprättas.

2. Förfarande enligt patentkrav 1, k ä n n e t e c k n a t av att efter att basstationens (BS) behörighet konstaterats, sänder mobilen en tredje svarssignal (Resp 3) till basstationen som igen konstaterar mobilens behörighet innan förbindelsen upprättas.

3. Förfarande enligt patentkrav 1, k ä n n e t e c k n a t av att den andra svarssignalen (Resp 2) bildas av ett slumptal (RAND 2) alstrat i basstationen och mobilens identifieringsnummer (PIN), och att basstationens behörighet konstateras genom jämförelse (9) av den andra svarssignalen med en signal alstrad i mobilen, som beror av det mottagna slumptalet (RAND 2) och det i mobilen tillgängliga identifieringsnumret (PIN).

4. Förfarande enligt patentkrav 2 eller 3, k ä n n e t e c k n a t av att den tredje svarssignalen (Resp 3) som sänds till basstationen bildas av slumptalet (RAND 2) och mobilens identifieringsnummer (PIN), vilken signal överförs till basstationen; och att basstationen bildar en motsvarande signal på samma sätt ur slumptalet (RAND 2) och det i basstationen tillgängliga identifieringsnumret (PIN) för mobilen; och att en jämförelse (12) utförs i basstationen mellan den bildade signalen och den överförda signalen så att vid överensstämmelse kan en talförbindelse upprättas.

5. Förfarande för att utföra behörighetskontroll mellan en basstation (BS) och en mobilstation (MSk) i ett mobilradiosystem efter det att mobilstationen har begärt och blivit tilldelad en förbindelse över en viss kanal, k ä n n e t e c k n a t av att i basstationen (BS) bildas en första svarssignal (Resp 2), den första svarssignalen (Resp 2) sänds till mobilen (MSk) som därvid bildar en motsvarande svarssignal (Resp 2) för att konstatera basstationens behörighet och, efter att en sådan behörighet konstaterats, sänder mobilen en

andra svarssignal (Resp 3) till basstationen, som bildar en motsvarande svarssignal och konstaterar mobilens behörighet innan en förbindelse upprättas.

6. Förfarande enligt patentkrav 5, k ä n n e t e c k n a t av att den första svarssignalen (Resp 2) bildas av ett slumptal (RAND 2) alstrat i basstationen och mobilens identifieringsnummer (PIN), och att basstationens behörighet konstateras genom jämförelse (9) av den första svarssignalen med en signal alstrad i mobilen, som beror på det mottagna slumptalet (RAND 2) och det i mobilen tillgängliga identifieringsnumret (PIN).

7. Förfarande enligt patentkrav 5, k ä n n e t e c k n a t av att den andra svarssignalen (Resp 3) till basstationen är bildas av slumptalet (RAND 2) och mobilens identifieringsnummer (PIN), vilken signal överföres till basstationen, och att basstationen bildar en motsvarande signal på samma sätt ur slumptalet (RAND 2) och det i basstationen tillgängliga identifieringsnumret (PIN) för mobilen; och att jämförelse (12) utförs i basstationen mellan signalen bildad i basstationen och den av basstationen mottagna signalen och att en talförbindelse upprättas då dessa signaler överensstämmer.

Patenttivaatimukset

1. Menetelmä käyttöoikeuskontrollin suorittamiseksi tukiaseman (BS) ja liikkuvan aseman (MSk) välillä radiopuhelinjärjestelmässä, jossa tukiasema ennen yhteyden kytkemistä lähettää kyselyn liikkuvan aseman käyttöoikeudesta ja määrää tämän lähettämään ensimmäisen vastaussignaalin (Resp 1), jota käytetään tukiasemalla liikkuvan aseman käyttöoikeuden toteamiseen, t u n n e t t u siitä, että sen jälkeen kun liikkuvan aseman käyttöoikeus on todettu (2, 3, 4) tukiasemalla, lähetetään (7) tukiasemalta toinen vastaussignaali (Resp 2) liikkuvalle asemalle, joka tällöin muodostaa (8) vastaavan toisen vastaussignaalin (Resp 2) tukiaseman (BS) käyttöoikeuden toteamiseksi (9) ennen yhteyden pystytystä.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että sen jälkeen kun tukiaseman (BS) käyttöoikeus on todettu, lähettää liikkuva asema kolmannen vastaussignaalin (Resp 3) tukiasemalle, joka jälleen toteaa liikkuvan aseman käyttöoikeuden ennen yhteyden pystytystä.

3. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että toinen vastaussignaali (Resp 2) muodostetaan satunnaisluvusta (RAND 2), joka on kehitetty tukiasemalla ja liikkuvan aseman identifiointinumerosta (PIN), ja että tukiaseman käyttöoikeus todetaan vertaamalla (9) toinen vastaussignaali liikkuvan aseman kehittämän signaalin kanssa, joka riippuu vastaanotetusta satunnaisluvusta (RAND 2) ja liikkuvalla asemalla saatavissa olevasta identifiointinumerosta (PIN).

4. Patenttivaatimuksen 2 tai 3 mukainen menetelmä, t u n n e t t u siitä, että kolmas vastaussignaali (Resp 3) tukiasemalle muodostetaan satunnaisluvusta (RAND 2) ja liikkuvan aseman identifiointinumerosta (PIN), joka signaali siirretään tukiasemalle; ja että tukiasema muodostaa vastaavan signaalin samalla tavoin satunnaisluvusta (RAND 2) ja tukiasemalla saatavilla olevasta liikkuvan aseman identifiointinumerosta (PIN); ja että vertailu (12) suoritetaan tukiasemalla muodostetun signaalin ja lähetetyn signaalin välillä siten, että yhtäpitävyyden yhteydessä puheyhteys voidaan pystyttää.

5. Menetelmä käyttöoikeuskontrollin suorittamiseksi tukiaseman (BS) ja liikkuvan aseman (MSk) välillä radiopuhelinjärjestelmässä sen jälkeen kun liikkuva asema on vaatinut ja sille on luovutettu yhteys tietyn kanavan kautta, t u n n e t t u siitä, että tukiasemalla (BS) muodostetaan ensimmäinen vastaussignaali (Resp 2), ensimmäinen vastaussignaali (Resp 2) lähetetään

liikkuvalle asemalle (MSk), joka tällöin muodostaa vastaavan vastaussignaalin (Resp 2) tukiaseman käyttöoikeuden toteamiseksi, ja sen jälkeen kuin tällainen käyttöoikeus on todettu, lähettää liikkuva asema toisen vastaussignaalin (Resp 3) tukiasemalle, joka muodostaa vastaavan vastaussignaalin ja toteaa liikkuvan aseman käyttöoikeuden ennen kuin yhteys pystytetään.

6. Patenttivaatimuksen 5 mukainen menetelmä, t u n n e t t u siitä, että ensimmäinen vastaussignaali (Resp 2) muodostetaan satunnaisluvusta (RAND 2), joka on kehitetty tukiasemalla, ja liikkuvan aseman identifiointinumerosta (PIN), ja että tukiaseman käyttöoikeus todetaan vertaamalla (9) ensimmäinen vastaussignaali ja liikkuvan aseman kehittämä signaali, joka riippuu vastaanotetusta satunnaisluvusta (RAND 2) ja liikkuvalla asemalla saatavilla olevasta identifiointinumerosta (PIN).

7. Patenttivaatimuksen 5 mukainen menetelmä, t u n n e t t u siitä, että toinen vastaussignaali (Resp 3) tukiasemalle muodostetaan satunnaisluvusta (RAND 2) ja liikkuvan aseman identifiointinumerosta (PIN), joka signaali siirretään tukiasemalle, ja että tukiasema muodostaa vastaavan signaalin samalla tavoin satunnaisluvusta (RAND 2) ja tukiasemalla saatavilla olevasta liikkuvan aseman identifiointinumerosta (PIN); ja että vertailu (12) suoritetaan tukiasemalla tukiaseman muodostetun signaalin ja tukiaseman vastaanotetun signaalin välillä siten, että yhtäpitävyyden yhteydessä pystytetään puheyhteys.

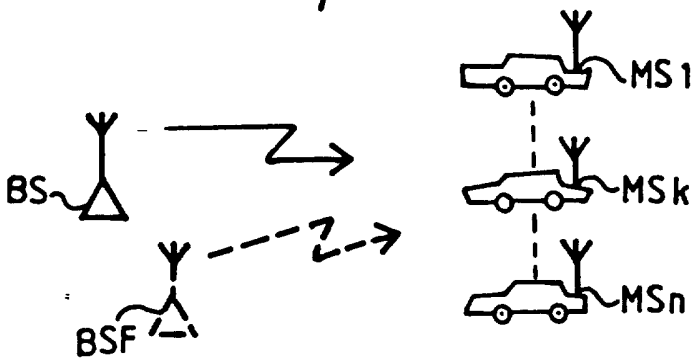


Fig.1

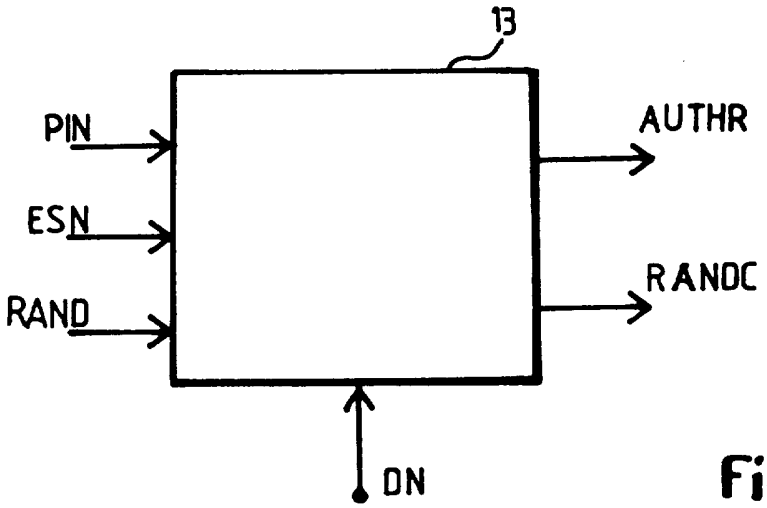


Fig 3

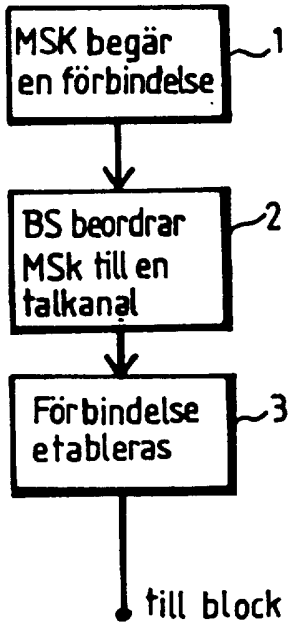


Fig.4

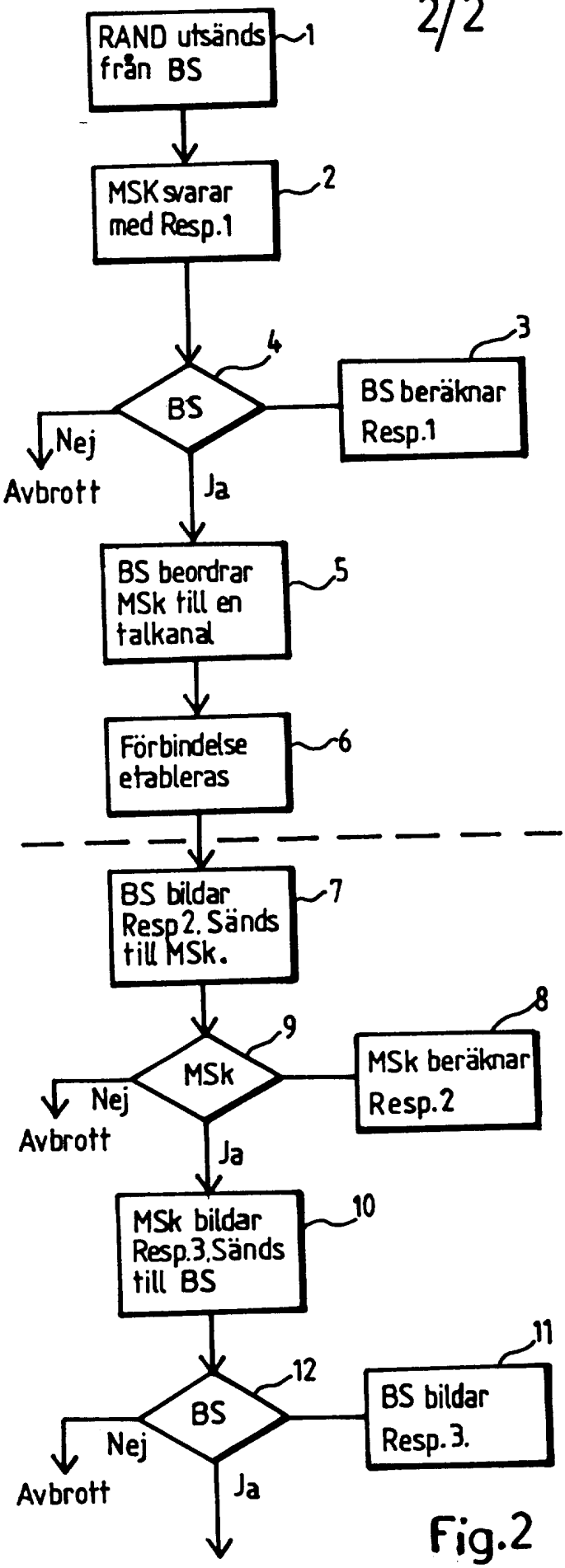

RAND utsänds från BS
1
MSK svarar med Resp.1
2
BS
4
BS beräknar Resp.1
3
Nej
Avbrott
Ja
BS beordrar MSk till en talkanal
5
Förbindelse etableras
6
Prior art
BS bildar Resp 2. Sänds till MSk.
7
MSk
9
MSk beräknar Resp.2
8
Nej
Avbrott
Ja
MSk bildar Resp.3. Sänds till BS
10
BS
12
BS bildar Resp.3.
11
Nej
Avbrott
Ja

Fig.2