NORGE

(12) **PATENT**

(19) NO (11) **300249** (13) B1

(51) Int Cl^6 H 04 B 7/26, H 04 Q 7/22, 7/38, 7/06

Patentstyret

(21) Søknadsnr	914357	(86) Int. inng. dag og søknadsnummer	29.01.91, PCT/SE91/00066
(22) Inng. dag	07.11.91	(85) Videreføringsdag	07.11.91
(24) Løpedag	29.01.91	(30) Prioritet	09.03.90, SE, 9000856
(41) Alm. tilgj.	07.11.91		
(45) Meddelt dato	28.04.97		

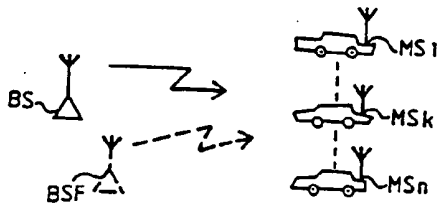
(73) Patenthaver Telefonaktiebolaget L M Ericsson, S-126 25 Stockholm, SE
(72) Oppfinner Paul Wilkinson Dent, Stehag, SE
Alex Krister Raith, Kista, SE
Jan Erik Åke Steinar Dahlin, Järfälla, SE
(74) Fullmektig Oslo Patentkontor AS, 0306 OSLO

(54) Benevnelse **Fremgangsmåte for utførelse av tilhørighetskontroll mellom en basisstasjon og en mobilstasjon i et mobilradiosystem**

(56) Anførte publikasjoner DE A1 3405381

(57) Sammendrag

En fremgangsmåte for å utføre en tilhørighetskontroll i et mobilt telefonsystem, i hvilket en ekte basestasjon (BS) betjener et antall mobilstasjoner (MS1-MSn). Det er tidligere kjent å utføre en enveisrettet kontroll fra basestasjonen (BS) til en oppringende mobilstasjon (MSk). En falsk basestasjon (BSF) kan herved utføre en falsk tilhørighetskontroll ved å samle en rekke RAND-responspar. For å unngå dette, innføres ytterligere én enkelrettet tilhørighetskontroll basestasjon-mobilstasjon, og dessuten en tilhørighetskontroll fra mobilstasjonen. I en utførelsesform av fremgangsmåten, utelukkes den enveisrettede kontrollen og den kun den dobbelrettede tilhørighetskontrollen gjennomføres.



Oppfinnelsen omhandler en fremgangsmåte for utførelse av en tilhørighetskontroll mellom en basisstasjon og en mobilstasjon i et mobilradiosystem, spesielt i et cellulært mobiltelefonsystem. Den foreslåtte fremgangsmåte kan også tilpasses for andre mobilradiosystem, eksempelvis personsøkersystem ("paging system").

I f.eks. et cellulært mobiltelefonsystem skjer en tilhørighetskontroll innen en samtale oppkobles mellom mobilstasjonen og basisstasjonen. Basisstasjonen ber om informasjon fra mobilstasjonen om dennes identitet ved å beordre denne til å sende et identifikasjonsnummer. Mobilstasjonen er dermed tvunget til å vise sin identitet for basisstasjonen slik at denne vet om mobilstasjonen har rett til sende ut en samtale over systemet og slik at basisstasjonen og sentralen vet hvilken mobilstasjon som skal debiteres for den påfølgende oppkoblede samtalen.

Mobilstasjonen må på sin side vite sikkert om den kommuniserer med en ekte basisstasjon, dvs. en basisstasjon som virkelig kan formidle samtalen i det tilfellet av at mobilstasjonen er den oppringende part (mobilstasjonen er A-abonnent), og om korrekt debitering finner sted.

For å utføre en tilhørighetskontroll er det tidligere kjent å danne tilhørighetssignaler, "Resp."-signaler, i basisstasjonen og mobilstasjonen. Et tilfeldig tall (RAND) sendes ut fra basisstasjonen til mobilstasjoner innenfor basisstasjonens dekningsområde. Den oppringende mobilstasjon svarer med et visst signal (Resp. 1). Basisstasjonen danner på samme måte ut fra det tilfeldige tallet og den oppringende mobilstasjonens identitet samme signal Resp. 1. Normalt stemmer disse overens og basisstasjonen beordrer mobilstasjonen til en talekanal.

I den ovenfor nevnte kjente fremgangsmåte for tilhørighetskontroll dannes således et RAND-responspar for en viss

mobilstasjon, dvs. for et visst mottatt tilfeldig tall RAND dannes i mobilstasjonen et visst responssignal og en basisstasjon kan altså motta en rekke slike responssignaler for en rekke tilfeldige tall. Dette innebærer at det kan opprettes en "falsk" basisstasjon som sender ut en rekke forskjellige tilfeldige tall og mottar tilsvarende rekke (forskjellige) responssignaler. Den falske basisstasjonen kan derved opprette et mobilabonnement som ikke rettmessig kan sende samtaler over systemet. Denne ulempe eller brist ved den kjente tilhørighetskontrollen kommer av at kontrollen er enveisrettet på den måten at det er kun basisstasjonen som krever det responssignal som avgjør mobilstasjonens tilhørighet.

Ifølge foreliggende fremgangsmåte er tilhørighetskontrollen toveisrettet, dvs. at det ikke er kun basisstasjonen som krever identitet fra mobilstasjonen, men også mobilstasjonen krever identitet fra basisstasjonen.

Formålet med foreliggende oppfinnelse er således å fremskaffe en forbedret fremgangsmåte for tilhørighetskontroll, slik at manipulering med falsk basisstasjon med den hensikt å få tilgang til mobiltelefonsystemets tilhørighetskode umuliggjøres.

Fremgangsmåten er karakterisert ved den karakteristiske delen til krav 1 og 5. Utførelsesformer av den foreslåtte fremgangsmåten fremgår av patentkrav 2-4 og 6-7.

Oppfinnelsen skal beskrives nærmere med henvisning til vedføyde tegninger, der:

figur 1 viser skjematisk kommunikasjon mellom to basisstasjoner og et flertall mobile stasjoner;

figur 2 viser et flytskjema som illustrerer en utførelse av den foreslåtte fremgangsmåte;

figur 3 viser i et blokkskjema inngangs- og utgangsstørrelser ved en tilhørighetsalgoritme som inngår

i en mobilstasjon;

figur 4 viser et flytskjema for en annen utførelse av den foreslåtte fremgangsmåten.

Figur 1 viser en ekte basisstasjon BS som lytter ved å sende ut tilfeldige tall over en gitt kontrollkanal til et antall mobilstasjoner MS1-MSn. Av disse er det én mobilstasjon MSk som svarer og vil opprette en samtale over en viss talekanal. Slik som beskrevet ovenfor utføres på kjent måte en enveisrettet tilhørighetskontroll ved at basisn krever et svar Resp. 1 fra mobilstasjonen MSk. Dette vil bli beskrevet nærmere i forbindelse med figur 2. Ettersom forbindelsen på dette stadiet er enveisrettet, kan en falsk basisstasjon BSF som angitt ovenfor innhente svar fra en rekke mobilstasjoner ved utsending av ovenfor nevnte tilfeldige tall RAND. Basisstasjonen BSF kan derved opprette en bank av RAND-responssvar som siden kan utnyttet urettmessig av en mobilstasjon.

For å umuliggjøre dette foreslås en tilhørighetsfremgangsmåte som fremgår av flytskjemaet ifølge figur 2.

En ekte basisstasjon BS lytter til et antall mobilstasjoner MS1-MSn innenfor sitt dekningsområde ved å sende ut et tilfeldig tall RAND, blokk 1.

En gitt mobilstasjon som ønsker å opprette en samtale, svarer med et signal Resp. 1, blokk 2. Dette signalet dannes i mobilstasjonens mikroprosessor utfra et antall inndata PIN, ESN og DN i tillegg til det mottatte tilfeldige tallet RAND, se figur 3, der PIN er lik mobilstasjonens personlige identifikasjonsnummer, ESN er lik mobilstasjonens elektroniske serienummer, DN er lik det nummer som slås. Mobilstasjonen MSk er derved en A-abonnent. Mikroprosessoren 13 avgir deretter Resp. 1-signalet som består av et 18 biters AUTH-signal og et 8 biters RANDC-signal, som sendes til basisstasjonen.

Basisstasjonen beregner Resp. 1 på tilsvarende måte, blokk 3, ut fra de innkommende signalene AUTH og RANDC, og foretar en sammenligning med verdien til det oversendte Resp-signalet, blokk 4, hvilket signal er beregnet av mobilstasjonen. Dersom disse overensstemmer med hverandre, beordrer basisstasjonen mobilstasjonen til en viss tildelt talekanal, blokk 5, og forbindelsen etableres på kjent måte, blokk 6. Ovenfor beskrevne fremgangsmåte er kjent fra før.

Ifølge den foreslåtte fremgangsmåte danner nå basisstasjonen et svarsignal Resp. 2 utfra et nytt tilfeldig tall RAND 2 og ut fra mobilstasjonens personlige identifikasjonsnummer PIN, hvilket er kjent i basisstasjonen (blokk 2, 3). Både Resp. 2 og RAND 2 sendes til mobilstasjonen, blokk 7. Mobilstasjonen danner en verdi for Resp. 2 ut fra sitt PIN og det mottatte tilfeldige tall RAND 2, blokk 8. En sammenligning foretas nå i mobilstasjonen, blokk 9, mellom mottatt Resp. 2 og den beregnede verdien for Resp. 2. Dersom disse to verdiene stemmer overens, danner mobilstasjonen en verdi resp. 3, og overfører denne til basisstasjonen, blokk 10. Resp. 3 dannes ut fra RAND 2 og PIN i mobilstasjonen. Basisstasjonen beregner Resp. 3 på samme måte ut fra RAND 2 og PIN, som er kjente i basisstasjonen, blokk 11. Deretter foretas en sammenligning, blokk 12, mellom mottatt og beregnet verdi for Resp. 3. Dersom verdiene er i overensstemmelse med hverandre, fortsetter oppkoblingen til en opprettet taleforbindelse.

Fremgangsmåtetrinnene ifølge blokk 7, 8 og 9 innebærer en tilhørighetskontroll i hvilken mobilstasjonen avgjør om basisstasjonen er ekte, ettersom verifisering av det utsendte signalet Resp. 2 fra basisstasjonen skjer i mobilstasjonen og mot en verdi Resp. 2 som er beregnet i mobilstasjonen. Signalet Resp. 2 fra basisstasjonen kan derfor betraktes som et svarsignal fra denne. Den ovenfor beskrevne fremgangsmåte utgjør den vesentlige forskjellen sammen-

lignet med den kjente tilhøringhetsfremgangsmåten ifølge blokk 2, 3 og 4.

Kontrollen ifølge blokk 10, 11 og 12 utgjør hovedsakelig en gjentakelse av fremgangsmåte ifølge blokk 2, 3 og 4, dvs. kontroll fra basisstasjonen på om mobilstasjonen er tilhørig.

Den vesentlige forskjellen relativt den kjente tilhørighetsfremgangsmåten (blokk 1-4) består i at også mobilstasjonen krever et svar Resp. 2 fra basisstasjonen og verifiserer dette ifølge blokk 7-9. En falsk basisstasjon må derfor vite eksakt hvordan en beregning av dette svarsignal skal utføres. Kontrollen blir derved dobbelrettet.

Tilhørighetskontrollen ifølge blokkene 2, 3 og 4 kan utføres på en generell kontrollkanal i mobilradiosystemet, og tilhørighetskontrollen ifølge blokkene 7-12 kan utføres på den talekanal som ble opprettet mellom basisstasjonen BS og mobilstasjon MSk (blokk 5 og 6).

Figur 4 viser et blokkskjema over de første trinnene under det tilfellet av at det kun utføres en dobbelrettet tilhørighetskontroll. Trinnene ifølge blokk 1-3 erstatter derved trinnene ifølge blokk 1-6. I dette tilfellet utføres ingen enkelrettet (og kjent) tilhørighetskontroll forut for den dobbelrettede kontrollen. En oppringende mobilstasjon, f.eks. MSk, ber om en forbindelse fra basisstasjonen BS. Ved mottagning av denne anropsforespørsel søker basisstasjonen BS opp en ledig talekanal og beordrer mobilstasjonen MSk til denne ledige kanal. Derved er en ledig forbindelse etablert over talekanalen uten at det har blitt utført noen tilhørighetskontroll. Deretter følger selve tilhørighetskontrollen på samme måte som beskrevet ovenfor i forbindelse med blokk 7-12 i figur 2, dvs. kun én dobbelrettet tilhørighetskontroll er blitt utført.

P a t e n t k r a v

1. Fremgangsmåte for utførelse av tilhørighetskontroll mellom en basisstasjon (BS) og en mobilstasjon (MSk) i et mobilradiosystem der basisstasjonen før oppkobling av en forbindelse sender en forespørsel om mobilstasjonens tilhørighet og beordrer denne til å sende et første svarsignal (Resp. 1) som i basisstasjonen anvendes for å konstatere mobilstasjonens tilhørighet,
k a r a k t e r i s e r t v e d at etter at mobilstasjonens tilhørighet er konstatert (2, 3, 4) i basisstasjonen sendes det ut (7) et andre svarsignal (Resp. 2) fra basisstasjonen til mobilstasjonen som så danner (8) et tilsvarende andre svarsignal (Resp. 2) for å konstatere (9) basisstasjonens tilhørighet innen forbindelsen opprettes.

2. Fremgangsmåte som angitt i krav 1,
k a r a k t e r i s e r t v e d at etter at tilhørigheten av basisstasjonen (BS) er etablert, sender mobilstasjonen et tredje svarsignal (Resp. 3) til basisstasjonen som på nytt konstaterer mobilstasjonens tilhørighet innen forbindelsen opprettes.

3. Fremgangsmåte ifølge krav 1,
k a r a k t e r i s e r t v e d at nevnte andre svarsignal (Resp. 2) dannes fra et tilfeldig tall (RAND 2) produsert i basisstasjonen, og mobilstasjonens identifikasjonsnummer (PIN), og ved at basisstasjonens tilhørighet konstateres ved å sammenligne (9) nevnte svarsignal med et signal som produseres i mobilstasjonen og som er avhengig av det mottatte tilfeldige tall (RAND 2) og identifikasjonsnummeret (PIN) som er tilgjengelig i mobilstasjonen.

4. Fremgangsmåte ifølge krav 2 eller 3,
k a r a k t e r i s e r t v e d at nevnte tredje svar-

signal (Resp. 3) som sendes til basisstasjonen dannes fra nevnte tilfeldige tall (RAND 2) og fra nevnte mobilstasjons identifikasjonsnummer (PIN), ved at nevnte signal sendes til basisstasjonen, og ved at nevnte basisstasjon danner et tilsvarende signal på samme måte fra nevnte tilfeldige tall (RAND 2) og mobilstasjonens identifikasjonsnummer (PIN) som er tilgjengelig i nevnte basisstasjon, og ved at en sammenligning (12) utføres i basisstasjonen mellom det dannede signal og det sendte signal slik at ved overensstemmelse mellom nevnte signaler blir det opprettet en taleforbindelse.

5. Fremgangsmåte for å utføre en tilhørighetskontroll mellom en basisstasjon (BS) og en mobilstasjon (MSk) i et mobilradiosystem etter at mobilstasjonen har bedt om og blitt tildelt en forbindelse over en gitt kanal, k a r a k t e r i s e r t v e d at det i basisstasjonen (BS) dannes et første svarsignal (Resp. 2), som sendes til mobilstasjonen (MSk) som så danner et tilsvarende svarsignal (Resp. 2) for å konstatere basisstasjonens tilhørighet og dersom dennes tilhørighet konstateres, sender mobilstasjonen et andre svarsignal (Resp. 3) til basisstasjonen, som danner tilsvarende svarsignal og konstaterer mobilstasjonens tilhørighet innen forbindelse opprettes.

6. Fremgangsmåte ifølge krav 5, k a r a k t e r i s e r t v e d at nevnte andre svarsignal (Resp. 2) dannes fra et tilfeldig tall (RAND 2) produsert i basisstasjonen og fra mobilstasjonens identifikasjonsnummer (PIN), og ved at basisstasjonens tilhørighet konstateres ved å sammenligne (9) nevnte svarsignal med et signal som produseres i mobilstasjonen og som er avhengig av det mottatte tilfeldige tall (RAND 2) og identifikasjonsnummeret (PIN) som er tilgjengelig i mobilstasjonen.

7. Fremgangsmåte ifølge krav 5,
k a r a k t e r i s e r t v e d at nevnte andre svarsignal (Resp. 3) som sendes til basisstasjonen dannes fra nevnte tilfeldige tall (RAND 2) og fra nevnte mobilstasjons identifikasjonsnummer (PIN), ved at nevnte signal sendes til basisstasjonen, og ved at nevnte basisstasjon danner et tilsvarende signal på samme måte fra nevnte tilfeldige tall (RAND 2) og mobilstasjonens identifikasjonsnummer (PIN) som er tilgjengelig i nevnte basisstasjon, og ved at en sammenligning (12) utføres i basisstasjonen mellom det dannede signal og det av stasjonen mottatte signal, slik at ved overensstemmelse mellom nevnte signaler blir det opprettet en taleforbindelse.

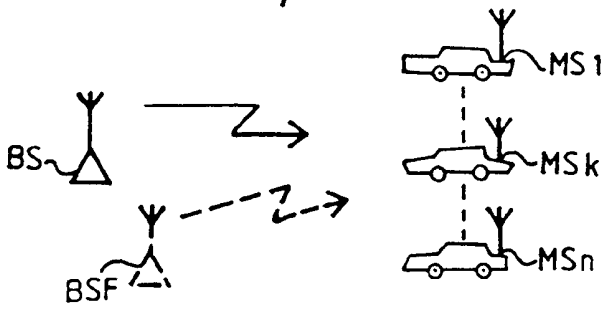


Fig.1

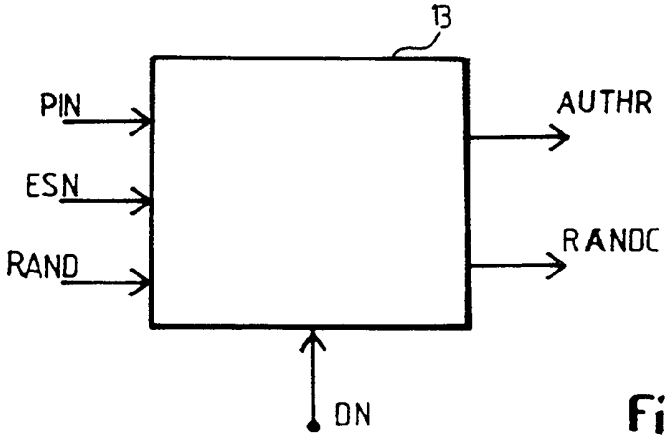


Fig 3

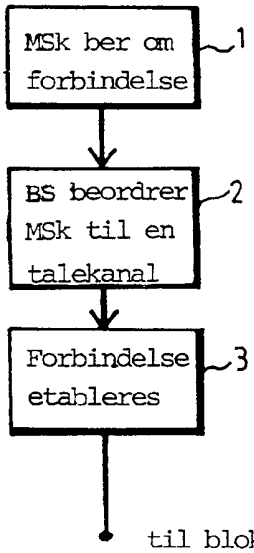


Fig.4

til blokk 7, Fig. 2

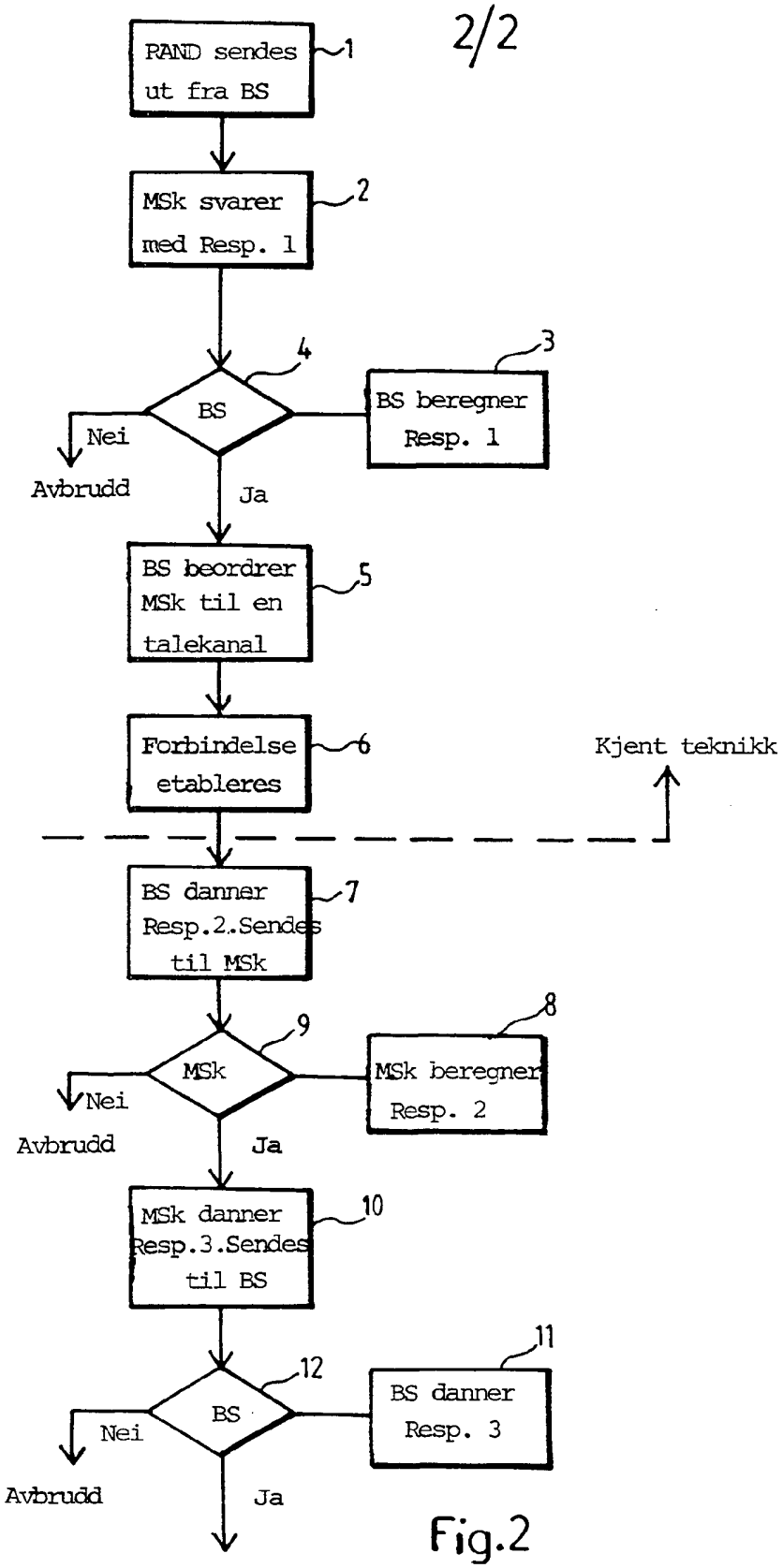

RAND sendes ut fra BS
1
MSk svarer med Resp. 1
2
BS
4
BS beregner Resp. 1
3
Nei
Avbrudd
Ja
BS beordrer MSk til en talekanal
5
Forbindelse etableres
6
Kjent teknikk
BS danner Resp.2.Sendes til MSk
7
MSk
9
MSk beregner Resp. 2
8
Nei
Avbrudd
Ja
MSk danner Resp.3.Sendes til BS
10
BS
12
BS danner Resp. 3
11
Nei
Avbrudd
Ja

Fig.2