(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 600 23 659 T2** 2006.08.10

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 157 574 B1**
(21) Deutsches Aktenzeichen: **600 23 659.5**
(86) PCT-Aktenzeichen: **PCT/US00/01451**
(96) Europäisches Aktenzeichen: **00 903 372.1**
(87) PCT-Veröffentlichungs-Nr.: **WO 2000/044190**
(86) PCT-Anmeldetag: **20.01.2000**
(87) Veröffentlichungstag der PCT-Anmeldung: **27.07.2000**
(97) Erstveröffentlichung durch das EPA: **28.11.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **02.11.2005**
(47) Veröffentlichungstag im Patentblatt: **10.08.2006**

(51) Int Cl.[8]: ***H04Q 7/38*** (2006.01)
H04Q 7/22 (2006.01)

(30) Unionspriorität:
237392 **26.01.1999** **US**

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(73) Patentinhaber:
Qualcomm, Inc., San Diego, Calif., US

(74) Vertreter:
WAGNER & GEYER Partnerschaft Patent- und Rechtsanwälte, 80538 München

(72) Erfinder:
FAUS, Juan, San Diego, US; ACKERMAN, Janet, Longmont, US; MUELLER, T., Phillip, Niwot, US

(54) Bezeichnung: **ANORDNUNG UND VERFAHREN ZUM BEREITSTELLEN EINES ZUGANGS ZU EINEM DRAHTLOSEN KOMMUNIKATIONSDIENST FÜR EINE GRUPPE VON TEILNEHMERN, DIE EIN SET VON MODEMS TEILEN**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

Hintergrund der Erfindung

I. Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich auf Teilnehmerauthentisierung bzw. Teilnehmerauthentifizierung in einem drahtlosen Kommunikationssystem. Genauer gesagt bezieht sich die vorliegende Erfindung auf Teilnehmerauthentisierung in einem drahtlosen Kommunikationssystem, wo sich eine Gruppe von Teilnehmern eine Reihe von. Modems teilt.

II. Verwandte Technik

[0002] Um den Betrug und den Diebstahl von drahtlosen Kommunikationsdiensten zu verhindern und, um die Teilnehmer von einem drahtlosen Kommunikationsdienst richtig zu berechnen, haben drahtlose Kommunikationsdienstanbieter (wie zum Beispiel zellulare Telephonieanbieter) einen Mechanismus zum Authentisieren bzw. zum Authentifizieren ihrer Teilnehmer geschaffen. Dieser Mechanismus vertraut auf die Tatsache, dass jeder Teilnehmer in dem System eine einzigartige Authentisierungsinformation (UAI = unique authentication information) für jeden Transceiver, der dem Teilnehmer gehört, hat.

[0003] Diese Authentisierungsinformation ist notwendig, um Zugriff zu einem drahtlosen Kommunikationssystem zu erlangen. Auf diese Art und Weise ist die Authentisierungsinformation irgendwie analog zu einer Personenidentifizierungsnummer (PIN = personal identification number), die für das Erlangen des Zugriffs zu seinem Bankkonto über einen Geldautomaten benutzt wird.

[0004] Jede Authentisierungsinformation des Teilnehmers besteht aus statischen Authentisierungsdaten und aus dynamischen Authentisierungsdaten. Eine elektronische Seriennummer (ESN = electronic serial number) und eine Mobilidentifizierungsnummer (MIN = mobile identification number) sind zwei Beispiele für statische Authentisierungsdaten. Geteilte Geheimdaten (SSD = shared secret data) ist ein Beispiel für dynamische Authentisierungsdaten. Statische Authentisierungsdaten bleiben, wie der Name schon sagt, über die Zeit konstant. Auf der anderen Seite können dynamische Authentisierungsdaten verändert werden, während ein Teilnehmer sich aktiv mit einem Anruf beschäftigt, und dass während des Aufbauens eines Anrufs oder während des Registrierens mit einer Basisstation, etc.

[0005] In traditionellen, drahtlosen Kommunikationssystemen hat jeder Teilnehmer seine eigene Teilnehmereinheit (oder Transceiver), wie zum Beispiel ein zellulares Telefon, und jeder Teilnehmer ist für das Zahlen für alle Anrufe, die von seinem Mobiltelefon getätigt wurden, verantwortlich.

[0006] Weiterhin hat jede Teilnehmereinheit ein Modem verbunden mit einer Antenne für das Senden von Hochfrequenzsignalen (HF = RF = radio frequency) zu und Empfangen von HF-Signalen von einer Basisstation innerhalb des drahtlosen Kommunikationssystems. Somit gibt es in konventionellen, drahtlosen Kommunikationssystemen ein Eins-zu-eins-Verhältnis zwischen Modems und Teilnehmern. Wegen diesem Eins-zu-eins-Verhältnis wird die einzigartige Authentisierungsinformation eines Teilnehmers in dem Modem innerhalb des Mobiltelefons des Teilnehmers gespeichert. Durch das Speichern der Authentisierungsinformation im Modem des Teilnehmers, kann das Modem den Authentisierungsprozess auf eine Art und Weise durchführen, die für den Teilnehmer transparent ist, und das Modem kann nach Bedarf die dynamische Authentisierungsinformation des Teilnehmers aktualisieren und Aufrecht erhalten. Infolge dessen muss sich der Teilnehmer sich selbst nicht mit der Bereitstellung seiner Authentisierungsinformation belasten.

[0007] Jedoch gibt es in gewissen drahtlosen Kommunikationssystemen (wie zum Beispiel in einem konzentrierten Teilnehmersystem, dass hierin später beschrieben wird) nicht nur ein Eins-zu-eins-Verhältnis zwischen Teilnehmern und Modem-Systemen. In solch einem System ist es erwünschenswert, dass der Authentisierungsprozess für die Teilnehmer transparent ist, und zwar auf die gleiche Weise, wie der Authentisierungsprozess für Teilnehmer in einem System transparent ist, wo es eine Eins-zu-eins-Übereinstimmung zwischen Teilnehmern und Modem-Systemen gibt.

[0008] Deswegen wird ein System und ein Verfahren benötigt, auf transparente Art und Weise Zugriff zu einem drahtlosen Kommunikationsdienst vorzusehen, wo es kein Eins-zu-eins-Verhältnis zwischen Teilnehmern und Modems gibt. Weiterhin sollten das System und das Verfahren mit existierenden drahtlosen Kommunikationssystemen kompatibel sein.

[0009] Weiterhin wird die Aufmerksamkeit auf das Dokument US-A-5 781 856 gezogen, dass ein Zellulartelefon konzentriertes Teilnehmersystem (concentrated subscriber system) beschreibt. Das konzentrierte Teilnehmersystem beinhaltet eine Gruppe von Teilnehmereinheiten verkoppelt mit einer Steuerung eines konzentrierten Teilnehmersystems. Die Steuerung des konzentrierten Teilnehmersystems sieht ein Hochfrequenz-Interface zum Standardbasisstationstransceiver eines zellularen Telefonsystems vor: Jede Teilnehmereinheit hat eine einzigartige elektronische Seriennummer. Die Steuerung des konzentrierten Teilnehmersystems beinhaltet eine Gruppe von Modulator-Demodulator-Systemen (Modems)

und einen HF-Transceiver und ein Antennensystem, dass so eingestellt ist, um genügend Information zu senden, um vielfache Telefonanrufe über beide, lange und kurze Distanzen, durchzuführen. Die Steuerung sieht ein Modem vor, dass entwickelt wurde, um einen Telefonanruf mit Kodierungsinformationen, die die elektronischen Seriennummern beinhalten, zu handhaben.

[0010] Auch wird die Aufmerksamkeit auf EP-A-0 532 227 gezogen, dass eine sichere, zellulare Telephonieanordnung offenbart, wo die Mobileinheit ein Geheimnis führt, dass ihr von dem Dienstanbieter zugewiesen wurde und, dass dem Anbieter bekannt ist aber keiner anderen Basisstation.

[0011] Gemäß der vorliegenden Erfindung ist ein Verfahren zum Vorsehen von einer Gruppe von Teilnehmern mit Zugriff zu einem drahtlosen Kommunikationsdienst in einem konzentrierten Teilnehmersystem, wie dargelegt in den Ansprüchen 1 und 11, wie auch ein konzentriertes Teilnehmersystem, wie dargelegt in Anspruch 20, vorgesehen. Bevorzugte Ausführungsbeispiele der Erfindung sind in den abhängigen Ansprüchen offenbart.

Zusammenfassung der Erfindung

[0012] Die. vorliegende Erfindung bewältigt das oben identifizierte Problem. Gemäß einem Aspekt der Erfindung sieht ein Verfahren vor, auf transparente Art und Weise den Zugriff zu einem drahtlosen Kommunikationsdienst zu einer Gruppe von Teilnehmern, die eine Gruppe von Modems teilen, vorzusehen, wo jeder Teilnehmer in der Gruppe mit einer Teilnehmereinheit versehen ist und jeder Teilnehmer in der Gruppe bzgl. statischer und dynamischer Authentisierungsinformation assoziiert wird.

[0013] In einem Ausführungsbeispiel beinhaltet das Verfahren folgende Schritte: (a) Detektieren der Aktivierung von einer der Teilnehmereinheiten; (b) Auswahl eines Modems aus dem Satz von Modems; (c) Koppeln der aktivierten Teilnehmereinheit mit dem ausgewählten Modem, wodurch der Verkehr zwischen der aktivierten Teilnehmereinheit und dem ausgewählten Modem fließen kann; und (d) Vorsehen dynamischer Authentisierungsinformation für das ausgewählte Modem, wobei die dynamische Authentisierungsinformation geliefert an das ausgewählte Modem die dynamische Authentisierungsinformation ist, die mit dem Teilnehmer assoziiert ist, für den die aktivierte Teilnehmereinheit vorgesehen ist.

[0014] In einem anderen Ausführungsbeispiel beinhaltet das Verfahren folgende Schritte: (a) Detektieren eines ankommenden Anrufs, adressiert an einen der Teilnehmer in der Gruppe; (b) Bestimmen eines angerufenen Teilnehmers, wobei der angerufene Teilnehmer, der Teilnehmer in der Gruppe ist, an den der eventuell ankommende Anruf adressiert ist; (c) Auswahl eines verfügbaren Modems aus dem Satz von Modems; (d) Koppeln, der für den angerufenen Teilnehmer vorgesehenen Teilnehmereinheit mit dem ausgewählten Modem, wodurch der Verkehrsfluss zwischen der Teilnehmereinheit und dem ausgewählten Modem, ermöglicht wird; und (e) Vorsehen dynamischer Authentisierungsinformation an das ausgewählte Modem, wobei die dynamische Authentisierungsinformation, geliefert an das ausgewählte Modem, die mit dem angerufenen Teilnehmer assoziierte dynamische Authentisierungsinformation ist.

[0015] Zweckmäßigerweise kann jedes Ausführungsbeispiel weiterhin folgende Schritte enthalten: Speichern der dynamischen Authentisierungsinformation, die jedem Teilnehmer in der Gruppe zugewiesen wird, in einer Datenbank; Speichern, der an das ausgewählte Modem gelieferten dynamischen Authentisierungsinformation in dem ausgewählten Modem; Modifizieren der dynamischen Authentisierungsinformation, gespeichert in dem ausgewählten Modem, ansprechend auf das ausgewählte Modem, welches von einer Basisstation eine Aktualisierungsbefehlsnachricht empfängt; Speichern der modifizierten dynamischen Authentisierungsinformation in dem ausgewählten Modem; und Speichern der modifizierten dynamischen Authentisierungsinformation in der Datenbank. Auf diese Weise wird die dynamische Authentisierungsinformation, die in der Datenbank gespeichert wurde, immer dann aktualisiert, wenn eine Aktualisierung von einem Modem empfangen wurde.

[0016] Zusätzlich kann das Verfahren gemäß beiden Ausführungsbeispielen weiterhin den Schritt des Speicherns der statischen Authentisierungsinformation assoziiert mit jedem Teilnehmer in der Gruppe in jedes der Modems beinhalten.

[0017] Die Erfindung sieht auch ein konzentriertes Teilnehmersystem vor. Das konzentrierte Teilnehmersystem gemäß einem Ausführungsbeispiel beinhaltet ein Transceiversystem zum Senden von HF-Wellenfrequenzsignalen an eine Basisstation und zum Empfangen von HF-Wellenfrequenzsignalen von einer Basisstation; eine Vielzahl von Modems, wobei jedes der Vielzahl von Modems mit dem erwähnten Transceiversystem gekoppelt ist; eine Vielzahl von Teilnehmereinheiten, deren jeder einzigartige statische und dynamische Authentisierungsinformation zugewiesen ist; ein Schalter bzw. Switch, gekoppelt mit jedem Modem und gekoppelt mit jeder Teilnehmereinheit; ein Steuersystem in Verbindung mit dem Schalter und jedem Modems; und eine Datenbank zum Speichern von Authentisierungsinformation, wobei die Datenbank für das Steuersystem zugreifbar ist. Das Steuersystem bestimmt ein verfügbares Modem aus dem Satz von Modems, wenn

eines der Teilnehmereinheiten aktiviert wurde. Weiterhin weist das Steuersystem den Schalter an, um die aktivierte Teilnehmereinheit mit dem verfügbaren Modem zu verbinden, aus der Datenbank die gespeicherte dynamische Authentisierungsinformation, assoziiert mit der erwähnten einen der Vielzahl von Teilnehmereinheiten zu entnehmen, und das verfügbare Modem mit der entnommenen Authentisierungsinformation zu beliefern. Auf diese Weise wird die Authentisierungsinformation assoziiert mit der aktivierten Teilnehmereinheit zum Modem, das den Anruf handhabt, geliefert. Infolge dessen kann das Modem, das den Anruf handhabt, auf transparente Art und Weise die Teilnehmereinheit auf die gleiche Weise authentisieren, wie in einem konventionellen drahtlosen Kommunikationsdienst.

[0018] Weitere Merkmale und Vorteile der vorliegenden Erfindung, wie auch die Struktur und Operation der verschiedenen Ausführungsbeispiele der vorliegenden Erfindung, werden im Detail weiter unten mit Bezug zu den beiliegenden Zeichnungen beschrieben.

Kurze Beschreibung der Figuren

[0019] Die beiliegenden Zeichnungen, die hierin inkorporiert wurden und einen Teil der Spezifikation bilden, zeigen die vorliegende Erfindung und dienen, zusammen mit der Beschreibung weiter die Prinzipien der Erfindung zu erklären und einem Fachmann zu ermöglichen die Erfindung zu produzieren und zu verwenden. In den Zeichnungen bezeichnen gleiche Bezugsnummern identische oder funktional ähnliche Elemente. Zusätzlich identifiziert die links außen liegende Ziffer(n) einer Bezugsnummer die Zeichnung, in der die Bezugsnummer zuerst erschienen ist.

[0020] Fig. 1 ist eine Zeichnung eines zellularen Telefonsystems, konfiguriert auf eine Art und Weise, die mit der Verwendung von CDMA Funkwellenmodulationstechniken konsistent ist.

[0021] Fig. 2 zeigt ein Beispiel eines Authentisierungsprozesses.

[0022] Fig. 3 zeigt ein Ausführungsbeispiel eines Mobiltelefonsystems mit einem Vielen-zu-Vielen-Verhältnis zwischen Teilnehmern und Modems.

[0023] Fig. 4 zeigt den Operationsfluss eines Steuersystems eines konzentrierten Teilnehmersystems, gemäß einem Ausführungsbeispiel.

[0024] Fig. 5 zeigt den Operationsfluss eines Steuersystems eines konzentrierten Teilnehmersystems, gemäß einem alternativen Ausführungsbeispiel.

Detaillierte Beschreibung der bevorzugten Ausführungsbeispiele

[0025] Ein System und ein Verfahren zur Durchführung von Teilnehmerauthentisierung in einem drahtlosen Kommunikationssystem ist vorgesehen. In der Folgenden Beschreibung sind verschiedene Prozeduren, Anordnungen und Systeme im Detail beschrieben. Dies beinhaltet die Beschreibung eines zellularen Telefonsystems, dass gemäß einer speziellen, Codemultiplex-Vielfachzugriffs-Zellular-Spezifikation und -Protokoll (CDMA = code division multiple access) operiert. Es wird dem Fachmann ersichtlich sein, dass die vorliegende Erfindung innerhalb einer Vielfalt von zellularen oder drahtlosen Kommunikationssystemen ausgeübt werden kann, obwohl das beschriebene Ausführungsbeispiel bevorzugt ist. Zusätzlich ist auch die Verwendung einer elektronischen Seriennummer (ESN = electronic serial number) beschrieben, um eine Teilnehmereinheit zu identifizieren und zu pagen. Es wird ebenso ersichtlich sein, dass andere einzigartige Identifikationscodes für den ESN ausgetauscht werden können, und zwar beinhaltend Mobilidentifikationsnummer (MIN) oder noch allgemeiner eine Teilnehmereinheitsidentifikationsnummer (SUIN = subscriber unit identification number). In anderen Versionen werden bekannte Strukturen und Systeme in Blockform vorgesehen. Dies wird gemacht, um die unnötige Verschleierung der Offenbarung der vorliegenden Erfindung zu vermeiden.

[0026] Fig. 1 ist eine Zeichnung eines zellularen Telefonsystems **100** konfiguriert auf eine Art und Weise die mit der Verwendung von CDMA-Funkwellenmodulationstechniken konsistent ist. Eine Implementation für ein solches CDMA-Zellulartelefonsystem ist beschrieben im U.S. Patent Nr. 4,901,307 ('307) mit dem Titel "Spread Spectrum Multiple Access Communication System Using a Satellite or Terrestrial Repeater" und im U.S. Patent Nr. 5,103,459 ('459) mit dem Titel "System and Method for Generating Signal Waveforms in a CDMA Cellular Telephone System", beide dem Rechtsnachfolger der vorliegenden Erfindung zugeordnet, und deren Offenbarungen sind inkorporiert hierin durch Bezugnahme. Zusätzlich ist eine Implementation für ein CDMA-Zellulartelefonsystem in der Spezifikation IS-95 von der Telecommunication Industry Association (2001 Pennsylvania Avenue, Suite 800, Washington, DC 20006) beschrieben mit dem Titel "Mobile Station-Base Station Compatibility Standard for Dual Mode Wideband Spread Spectrum Cellular System" (IS-95), der auch hierin inkorporiert wurde durch Bezugnahme.

[0027] Fig. 1 zeigt zwei Teilnehmer **102** und **104** unter Verwendung eines konventionellen, zellularen Telefonsystems **100**. Konventionell ist Teilnehmer **102** in Besitz des zellularen Telefons (nachfolgend Mobiltelefon) **106** und Teilnehmer **104** ist in Besitz des Mo-

biltelefons **108**. In dem zellularen Telefonsystem **100** werden alle Anrufe, die vom Mobiltelefon **106** gemacht wurden, dem Teilnehmer **102** in Rechnung gestellt. Auf ähnliche Weise werden alle Anrufe, die vom Mobiltelefon **108** gemacht wurden, dem Teilnehmer **104** in Rechnung gestellt.

[0028] Mobiltelefon **106** beinhaltet ein Modem **110**. Auf ähnliche Weise beinhaltet Mobiltelefon **108** ein Modem **112**. Die Modems **110** und **112** sind unter anderem dafür verantwortlich Hochfrequenzsignale (HF) von den Basisstationen **120**, **122** und **124** zu empfangen und zu den Basisstationen **120**, **122** und **124** zu senden. Vorzugsweise senden und empfangen die Modems **110** und **112** HF-Signale, die gemäß den CDMA-Spreizspektrumstechniken, die in den oben referenzierten Patenten '459 und '307 und Spezifikation IS-95 beschrieben wurden, moduliert.

[0029] Die Basisstationen **120**, **122** und **124** kommunizieren mit dem Mobiltelefonvermittlungsstelle (MTSO = mobile telephone switching office) 130 auf verschiedene Art und Weise einschließlich am Boden verlegte Drähte oder Mikrowellenverbindungen. MTSO **130** leitet den Verkehr, den es von den Basisstationen **120**, **122** und **124** empfängt, zum öffentlichen Telefonnetzwerk (PSTN = public switched telephone network) **140** oder zu anderen Zellstandorten **150**. Generell kommunizieren die Mobiltelefone **106** und **108** nicht direkt miteinander.

[0030] Um Betrug und Diebstahl zu vermeiden und eine richtige Abrechnung sicher zu stellen, muss ein Teilnehmer im System **100**, wie zum Beispiel Teilnehmer **102**, authentisiert werden, bevor der Teilnehmer Zugriff zum zellularen Telefonsystem **100** bekommt. Infolge dessen bekommt jeder Teilnehmer **102** und **104** im System **100** eine einzigartige Authentisierungsinformation (UAI = unique authentication information), die für die Authentisierungszwecke benutzt wird. So wird ein Teilnehmer, wie zum Beispiel Teilnehmer **102**, ohne gültiger, einzigartiger Authentisierungsinformation, der Zugriff zum Mobiltelefonsystem **100** verweigert. Da der Teilnehmer **102** sein eigenes Mobiltelefon **106** hat und, weil das Mobiltelefon **106** ein Modem **110** hat, wird die UAI des Teilnehmers **102** in dem Modem **110** gespeichert. Infolge dessen kann der Authentisierungsprozess vom Modem **110** auf eine Art und Weise, die für den Teilnehmer **102** transparent ist, gehandhabt werden. Das gleiche gilt für Teilnehmer **104**. Dieses sieht einen Nutzen für die Teilnehmer **102** und **104** vor, da keiner der Teilnehmer **102** und **104** sich mit der Teilnahme in dem Authentisierungsprozess belasten muss. Natürlich, da die UAI des Teilnehmers **102** in dem Mobiltelefon **106** gespeichert ist, muss der Teilnehmer **102** aufpassen, sein Mobiltelefon **106** nicht zu verlieren. Andernfalls könnte es dazu kommen das Teilnehmer **102** für Telefonanrufe für das Mobiltelefon **106** zahlen muss, die der Teilnehmer **102** nicht gemacht oder autorisiert hat. Das gleiche gilt für Teilnehmer **104**.

[0031] Eine UAI eines Teilnehmers besteht aus statischen Authentisierungsdaten und dynamischen Authentisierungsdaten. In einem Ausführungsbeispiel beinhalten die statischen Authentisierungsdaten eine elektronische Seriennummer (ESN) und einen Authentisierungsschlüssel (A-Key = A-Schlüssel), und die dynamischen Authentisierungsdaten beinhalten geteilte Geheimnisdaten (SSD) und einen Zählwert. Der Zählwert weist daraufhin, wie oft die dynamischen Authentisierungsdaten aktualisiert worden sind. Vorzugsweise behält jeder Teilnehmer im System **100** eine einzigartige ESN. Somit identifiziert eine ESN auf einzigartige Art und Weise einen Teilnehmer und ein spezifisches Mobiltelefon. Jegliche Anrufkosten assoziiert mit einer ESN werden dem Teilnehmer, der durch diese ESN identifiziert wird, in Rechnung gestellt.

[0032] Statische Authentisierungsdaten, wie der Name schon sagt, bleiben konstant über die Zeit. Auf der anderen Seite können die dynamischen Authentisierungsdaten während ein Teilnehmer aktiv in einem Anruf ist, diesen initiiert oder beendet oder sich registriert, geändert werden.

[0033] Fig. 2 zeigt ein Beispiel eines Authentisierungsprozesses **200**, bei dem der Teilnehmer **102** einbezogen ist. Wenn der Teilnehmer **102** wünscht einen Anruf zu platzieren, sendet das Modem **110** in das Mobiltelefon **106** eine Zugriffsnachricht **202** zu einer Basisstation, wie die Basisstation **120**. Vorzugsweise beinhaltet die Zugriffsnachricht **202** die ESN des Teilnehmers, so dass die Basisstation **120** bestimmen kann, dass der Anruf von einem autorisierten Mobiltelefon ausgegangen ist. Basisstation **120** antwortet auf die Zugriffsnachricht **202** durch Senden einer Challenge- bzw. Aufforderungsnachricht **204** zum Modem **110**. Modem **110** muss dann auf die Aufforderungsnachricht **204** durch Senden einer Antwortnachricht **206** zur Basisstation **120** antworten. Wenn die UAI in dem Modem **110** gültig ist, dann ist das Modem **110** dazu in der Lage korrekt auf die Aufforderungsnachricht **204** zu antworten. In diesem Fall ordnet die Basisstation **120** einen Verkehrskanal über den der Anruf platziert werden kann zu und weist das Mobiltelefon **106** an seine SSD und seinen Zählwert zu aktualisieren. Wenn jedoch das Modem **110** keine gültige UAI hat, wird das Modem **110** auf die Aufforderungsnachricht **204** inkorrekt antworten. Als Resultat lehnt die Basisstation **120** den Zugriff des Teilnehmers **102** zum zellularen System **100** ab. Infolge dessen, so lang wie Modem **110** die momentane UAI des Teilnehmers **102** hat, kann der Teilnehmer **102** Anrufe unter Verwendung des zellularen Systems **100** platzieren.

[0034] Wie oben angegeben beinhaltet die UAI des Teilnehmers **102** statische und dynamische Authenti-

sierungsinformation. Die statische Authentisierungsinformation bleibt konstant über die Zeit. Jedoch, während des Vorgangs eines Telefonanrufs, kann die Basisstation **120** eine oder mehrere geteilte Geheimnisdaten (SSD) Aktualisierungsnachrichten **210** zum Modem **110** senden. Eine SSD-Aktualisierungsnachricht ist eine Befehlsnachricht, dass die aktuellen SSD nicht über die Luft bzw. Luftschnittstelle gesendet werden. Ansprechend auf den Empfang einer SSD-Aktualisierungsnachricht modifiziert das Modem **110** die dynamische Authentisierungsinformation des Teilnehmers **102**. Auf diese Weise ändert sich die UAI des Teilnehmers **102** über die Zeit.

[0035] Wie oben beschrieben gibt es ein Eins-zu-eins-Verhältnis zwischen Teilnehmer und Modems im konventionellen zellularen System **100**. Zum Beispiel ist das Modem **110** assoziiert mit Teilnehmer **102** und das Modem **112** ist assoziiert mit dem Teilnehmer **104**. Wie oben dargestellt sieht das Mobiltelefonsystem **100** einen Vorteil aus diesem Eins-zu-eins-Verhältnis durch Speichern eines UAI's eines Teilnehmers in dem Modem assoziiert mit dem Teilnehmer. Zusätzlich hält das Modem die UAI des Teilnehmers aufrecht. Das heißt, das Modem aktualisiert/modifiziert die dynamische Authentisierungsinformation des Teilnehmers gemäß der SSD-Aktualisierungsnachricht **210**, die von einer Basisstation **120**, **122** oder **124** empfangen wurde. Auf diese Weise müssen die Teilnehmer innerhalb des zellularen Systems **100** sich nicht mit dem Erinnern und Aufrecht erhalten von deren UAI belasten. Infolge dessen ist der Teilnehmerauthentisierungsprozess **200** transparent für den Teilnehmer.

[0036] Fig. 3 zeigt ein Ausführungsbeispiel eines Mobiltelefonsystems **300** mit einem Vielen-zu-Vielen-Verhältnis zwischen Teilnehmer und Modems. Im speziellen zeigt Fig. 3 ein konzentriertes Teilnehmersystem (CSS = concentrated subscriber system) **306** über das die Teilnehmer **302(1)** bis **302(X)** die Modems **310(1)** bis **310(Y)** teilen, wobei X und Y beides positive Integerzahlen sind und vorzugsweise X größer Y ist. Die vorliegende Erfindung wird mit Bezug auf Fig. 3 beschrieben. Jedoch ist die vorliegende Erfindung nützlich in – anderen Ausführungsbeispielen von Mobiltelefonsystemen mit einem Vielen-zu-Vielen-Verhältnis zwischen Teilnehmern und Modems.

[0037] CSS **306** ermöglicht den Teilnehmern **302** die Modems **310** zu teilen. Das System operiert auf der Voraussetzung, dass zu jedem Zeitpunkt die Wahrscheinlichkeit, dass mehr als Y der X-Teilnehmer **302** in einem Anruf beteiligt sind, extrem klein ist. CSS **306** beinhaltet einen Schalter bzw. Switch **308**, ein Steuersystem **314**, ein oder mehrere Modems **310**, ein Modeminterfacesystem **318**, ein Speichersubsystem **316**, ein Antenneinterfacesystem **320** und eine Antenne **322**. Ein Transceiversubsystem wird in dem CSS durch die Antenne **322**, Antenneinterfacesystem **320** und Modeminterfacesystem **318** gebildet. Viele Transceiversubsysteme sind auf dem Fachgebiet bekannt und eine Implementation eines Transceiversubsystems ist beschrieben in dem ebenfalls anhängigen U.S. Patent Nr. 5,737,687 mit dem Titel "Self-Attenuating RF Transceiver System Using Antenna and Modem Interface and Cable Link", dem Rechtsnachfolger der vorliegenden Erfindung zugeordnet und hierin durch Bezugnahme inkorporiert.

[0038] Das Antenneninterfacesystem **320** empfängt Hochfrequenzsignale von einer Basisstation, wie zum Beispiel Basisstation **120**, über Antenne **322** und sendet diese Signale über das Modeminterface **318** zur Modembank **312**, die die Modems **310(1)** bis **310(Y)** aufweist. Um die Kosten für die Entwicklung des CSS **306** zu reduzieren, sind die Modems **310** vorzugsweise in Struktur und Funktionalität zu den Modems **110** und **112**, die in den Mobiltelefonen **106** und **108** entsprechend benutzt werden, ähnlich. Schalter **308** verkoppelt selektiv die Teilnehmereinheiten **304** mit den Modems **310**.

[0039] Steuersystem **314** empfängt Informationen von und sieht Informationen für die Modems **310** vor und steuert die Operation des Schalters **308** unter Verwendung der Information, die im Speichersubsystem **316** gespeichert wurde. Die Konfiguration und Operation des CSS **306** ist im weiteren Detail beschrieben im U.S. Patent Nr. 5,781,856 mit dem Titel "Concentrated Subscriber System for Wireless Local Loop" eingereicht am 10. Januar 1994, dem Rechtsnachfolger der vorliegenden Erfindung zugeordnet und die Offenbarung davon ist hierin durch Bezugnahme inkorporiert.

[0040] Wie in Fig. 3 gezeigt ist jede Teilnehmereinheit **304(1)**–(X), die mit dem Schalter **308** gekoppelt ist, mit einem entsprechenden Teilnehmer **302(1)**–(X) assoziiert. Zum Beispiel ist die Teilnehmereinheit **304(1)** mit dem Teilnehmer **302(1)** assoziiert und Teilnehmereinheit **304(2)** ist mit dem Teilnehmer **302(2)** assoziiert. Vorzugsweise fehlt es den Teilnehmereinheiten **304** generell an der Schaltung, die notwendig ist, um Funkwellen zu senden und zu empfangen und Daten von digital zu analogem Format zu modulieren und zu demodulieren. Das heißt, die Teilnehmereinheiten **304** haben kein Modem. Teilnehmereinheiten **304** bestehen im Wesentlichen aus einem Lautsprecher und einem Mikrofon. Vorzugsweise sind die Teilnehmereinheiten **304** Standardtelefonsets, die benutzt werden, um konventionellen, auf Draht basierenden, Pulscode modulierten Telefondienst vorzusehen und haben twisted pair bzw. verdrilltes Paar- oder PBX-Verbindungen. Während die Teilnehmereinheiten **304** als gekoppelt direkt zum Schalter **308** gezeigt sind, werden alternative Verfahren zum Austausch von Information zwischen Teilnehmereinheiten **304** und Schalter **308** in Erwägung gezogen, einschließlich einer vereinfachten Form von Funkwellen

basierender Kommunikation.

[0041] Wenn ein Teilnehmer **302**, wie zum Beispiel Teilnehmer **302(1)**, wünscht, einen Telefonanruf zu platzieren, aktiviert Teilnehmer **302(1)** seine assoziierte Teilnehmereinheit **304(1)**. Die Aktivierung der Teilnehmereinheit **304(1)** entspricht normalerweise dem Abnehmen bzw. Entfernen eines Handapparats (nicht gezeigt) von einer Gabel (nicht gezeigt) wie bei einem Standard, drahtgebundenen Telefon.

[0042] Steuersystem **314** detektiert, wann die Teilnehmereinheit **304(1)** aktiviert wurde. Beim Detektieren der Aktivierung der Teilnehmereinheit **304(1)** bestimmt das Steuersystem **314**, ob ein Modem **310** für den Prozess eines Telefonanrufs verfügbar ist. Jedes Modem **310** kann nur einen Telefonanruf gleichzeitig bearbeiten. Somit ist ein Modem nur dann verfügbar, wenn es nicht schon gerade einen Anruf verarbeitet. Wenn ein Modem **310** nicht verfügbar ist, sieht das Steuersystem **314** ein schnelles, Besetzt-Signal für die Teilnehmereinheit **304(1)** vor. Andernfalls sieht das Steuersystem **314** ein wähltonartiges Signal für die aktivierte Teilnehmereinheit **304(1)** vor. Das verfügbare Modem ist dann ausgewählt den Telefonanruf zu verarbeiten. Das heißt, das Steuersystem **314** verbindet das verfügbare Modem mit der Teilnehmereinheit **304(1)** über den Schalter **308**.

[0043] Wenn jemand einen Anruf auf einen der Teilnehmereinheiten **304(1)**–(X) platziert, wird der Anruf zur Basisstation **120** geleitet. Beim Detektieren eines Anrufs für eine der Teilnehmereinheiten **304(1)**–(X) sendet die Basisstation **120** eine Page-Nachricht zum CSS **306** über einen Paging-Kanal. Die Page-Nachricht beinhaltet einen Teilnehmereinheitidentifikator. Vorzugsweise beinhaltet der Teilnehmeridentifikator eine elektronische Sicherheitsnummer (ESN), die die Teilnehmereinheit **304**, für die der Anruf bestimmt ist, identifiziert. Als alternative könnte anstelle der ESN auch die MIN benutzt werden.

[0044] Um eingehende Anrufe zu detektieren, wählt das Steuersystem **314** ein oder mehrere Modems **310(1)**–(Y) aus, um den Paging-Kanal nach Page-Nachrichten abzuhören. Auf diese Modems wird sich im Weiteren als "Paging-Modems" bezogen. Wenn eines der Paging-Modems eine Page-Nachricht empfängt, sieht das Paging-Modem die ESN, die in der Page-Nachricht für das Steuersystem **314** enthalten ist, vor. Auf diese Weise detektiert das Steuersystem **314** eingehende bzw. ankommende Anrufe und ist informiert über die Teilnehmereinheit **304**, zu der der Anruf adressiert ist.

[0045] Bei einem Detektieren eines eingehenden Anrufs für eine der Teilnehmereinheiten **304**, zum Beispiel Teilnehmereinheit **304(3)**, bestimmt das Steuersystem **314**, ob die Teilnehmereinheit **304(3)** im On-Hook oder im Off-Hook bzw. aufgelegt oder abgenommen Zustand ist. Das Steuersystem **314** fragt den Schalter **308** ab, um zu bestimmen, ob die Teilnehmereinheit **304(3)** Off-Hook ist. Wenn die Teilnehmereinheit **304(3)** im Off-Hook ist, dann ist die Teilnehmereinheit **304(3)** "besetzt" und kann den Anruf nicht annehmen. In diesem Fall sendet das Steuersystem **314** ein Besetzt-Signal (oder eine Anrufverweigerungsnachricht) zur Basisstation **120**. Wenn die Teilnehmereinheit **304** nicht Off-Hook ist, wählt das Steuersystem **314** ein verfügbares Modem aus, wie zum Beispiel das Modem **310(1)**, um den Anruf zu verarbeiten und weist den Schalter **308** an, die Teilnehmereinheit **304(3)** mit dem ausgewählten Modem **310(1)** zu verkoppeln.

[0046] Wie die Teilnehmer **102** und **104** im Mobiltelefonsystem **100** sind die Teilnehmer **302(1)**–(X) jede für sich assoziiert mit der einzigartigen Authentisierungsinformation (UAI), einschließlich der statischen Authentisierungsinformation und der dynamischen Authentisierungsinformation (DAI). Die UAI, welche mit jedem Teilnehmer **302(1)**–(X) assoziiert ist, wird in einer Datenbank **317** im Speichersubsystem **316** gespeichert. Weiterhin, bevor eines der Modems **310(1)**–(Y) einen Telefonanruf im Auftrag von einem der Teilnehmer **302(1)**–(X) bearbeitet, muss der Teilnehmer **302** zuerst gemäß des Authentisierungsprozesses, der in Fig. 2 gezeigt ist, authentisiert werden. Das heißt, das Modem **310**, das einen Telefonanruf im Auftrag von einem der Teilnehmer **302** verarbeitet, muss auf korrekte Weise auf die Aufforderungsnachricht **204**, die von der Basisstation **120** gesendet wurde, antworten. Damit das Modem **310** erfolgreich auf die Aufforderungsnachricht **204** antwortet, und dabei den Teilnehmer **302** authentisiert, muss das Modem **310** Zugriff zu der UAI des Teilnehmers **302** haben.

[0047] In einem ersten Ausführungsbeispiel ist jedes Modem **310** der statischen und dynamischen Authentisierungsinformation des Teilnehmers **302** versehen, wenn CSS **306** initialisiert wird. In einem zweiten Ausführungsbeispiel ist jedes Modem **310** nur mit der statischen Authentisierungsinformation jedes Teilnehmers **302** versehen, wenn CSS **306** initialisiert wird.

[0048] In dem zweiten Ausführungsbeispiel sieht das Steuersystem **314** eine dynamische Authentisierungsinformation des Teilnehmers **302** für ein Modem **310** vor, und zwar auf einer Wenn-Benötigt-Basis. Das heißt, wenn ein spezielles Modem ausgewählt wurde, um einen ausgehenden oder eingehenden Anruf zu verarbeiten, sieht das Steuersystem **314** die adäquate dynamische Authentisierungsinformation für das spezielle Modem **310** vor. Zum Beispiel, wenn das Steuersystem **314** detektiert, dass die Teilnehmereinheit **304(3)** aktiviert ist und das ein Modem verfügbar ist, um einen ausgehenden Anruf zu verarbeiten, dann holt sich das Steuersystem **314** die DAI entsprechend dem Teilnehmer **302(3)** von der Daten-

bank **317** und sieht anschließend die geholte DAI dem verfügbaren Modem vor. Als ein anderes Beispiel, wenn das Steuersystem **314** einen eingehenden Anruf gerichtet auf die Teilnehmereinheit **304(5)** detektiert, dann holt das Steuersystem **314** die DAI entsprechend dem Teilnehmer **302(5)** von der Datenbank **317** und sieht anschließend die geholte DAI einem verfügbaren Modem vor, um den Anruf zu verarbeiten.

[0049] In einem dritten Ausführungsbeispiel sind die Modems **310** nicht mit der statischen Authentisierungsinformation jedes Teilnehmers versehen, wenn CSS **306** initialisiert wird. Stattdessen sieht das Steuersystem **314** beide, die statischen und die dynamischen Authentisierungsdaten, für die Modems **310**, wenn es notwendig ist, vor. Es ist notwendig die Authentisierungsinformation einem Modem **310** vorzusehen, wenn ein Modem **310** ausgewählt wurde, um einen ausgehenden oder eingehenden Anruf im Auftrag eines speziellen Teilnehmers **302** zu verarbeiten oder, wenn das Modem **310** ausgewählt wurde, um den Paging-Kanal zu überwachen.

[0050] Während des Verlaufs eines Anrufs kann die Basisstation **120** eine oder mehrere SSD-Aktualisierungsnachrichten **210** zum Modem, das den Anruf handhabt, senden. Ansprechend auf den Empfang der SSD-Aktualisierungsnachricht **210** modifiziert das Modem, welches den Anruf handhabt, eine lokale Kopie der DAI des Teilnehmers. In einem Ausführungsbeispiel meldet das Modem nach der Modifizierung seiner lokalen Kopie der DAI des Teilnehmers sofort dem Steuersystem **314** die Modifikation, sodass das Steuersystem **314** die Masterkopie der DAI des Teilnehmers, die in der Datenbank **317** gespeichert ist, aktualisieren kann. In einem anderen Ausführungsbeispiel informiert das Modem das Steuersystem **314** über die Modifikationen) am Ende des Anrufs. In jedem Fall ist das Steuersystem **314** mit der neuen dynamischen Authentisierungsinformation des Teilnehmers versehen.

[0051] In einem Ausführungsbeispiel speichert das Steuersystem **314**, beim Empfang einer neuen dynamischen Authentisierungsinformation eines Teilnehmers, sie in der Datenbank **317**, und, wie oben beschrieben, sieht diese Information zum Modem **310** auf eine Wenn-Benötigt-Basis vor. In einem alternativen Ausführungsbeispiel sieht das Steuersystem **314**, beim Empfang einer dynamischen Authentisierungsinformation eines Teilnehmers, sie zu jedem Modem **310** vor.

[0052] Fig. 4 zeigt den Operationsfluss des Steuersystems **314** gemäß einem Ausführungsbeispiel. Der Prozess beginnt im Schritt **402**, wo das Steuersystem **314** bestimmt, ob einer der Teilnehmer **302** wünscht einen ausgehenden Anruf zu platzieren. Das Steuersystem **314** bestimmt dies durch Bestimmung, ob einer der Teilnehmereinheiten **304** aktiviert worden ist. Wenn das Steuersystem **314** die Aktivierung einer Teilnehmereinheit **304** detektiert, geht die Steuerung über zum Schritt **404**, andernfalls geht die Steuerung über zum Schritt **412**.

[0053] Im Schritt **404** bestimmt das Steuersystem **314**, ob eines der Modems **310(1)**–(Y) verfügbar ist, um einen Anruf zu verarbeiten. Wenn ein Modem **310** verfügbar ist, geht die Steuerung über zum Schritt **406**, andernfalls sendet das Steuersystem **314** ein Besetzt-Signal zu der aktivierten Teilnehmereinheit (Schritt **410**). Der Prozess fährt anschließend fort mit Schritt **412**.

[0054] Im Schritt **406** wählt das Steuersystem **314** eines der verfügbaren Modems aus, um den Anruf zu verarbeiten und versieht das ausgewählte Modem mit der Authentisierungsinformation aus der Datenbank **317**. Wie oben dargestellt speichert das Steuersystem **314** die Authentisierungsinformation für jeden Teilnehmer **302(1)**–(X) in der Datenbank **317**. In einem Ausführungsbeispiel versieht das Steuersystem **314** das ausgewählte Modem mit nur den dynamischen Authentisierungsdaten. In diesem Ausführungsbeispiel ist jedes Modem der statischen Authentisierungsinformation jedes Teilnehmers beim Zeitpunkt der CSS-306-Intitialisierung versehen. In einem anderen Ausführungsbeispiel versieht das Steuersystem **314** das Modem mit beidem, statische und dynamische Authentisierungsinformation.

[0055] Das Steuersystem **314** bestimmt, welche Authentisierungsinformation von welchem Teilnehmer es zum gewählten Modem vorsehen muss, basierend auf die Teilnehmereinheit **304**, die dazu verwendet wird den Anruf zu platzieren. Wenn zum Beispiel die Teilnehmereinheit **304(3)** Off-Hook geht, dann wird die Authentisierungsinformation des Teilnehmers **302(3)** dem gewählten Modem vorgesehen. Das gewählte Modem **310** wird dann mit der Teilnehmereinheit **304(3)** über den Schalter **308** (Schritt **408**) verkoppelt. Beim Verkoppeln mit der Teilnehmereinheit **304(3)** kann das gewählte Modem **310** den Anruf für die Teilnehmereinheit **304(3)** verarbeiten. Das heißt, das gewählte Modem empfängt Daten von der Teilnehmereinheit **304(3)** und sendet diese zur Basisstation **120**, und empfängt den Verkehr von der Basisstation **120** und sendet diesen zur Teilnehmereinheit **304(3)**. Nach dem Schritt **408** geht die Steuerung in den Schritt **412** über.

[0056] Im Schritt **412** bestimmt das Steuersystem **314**, ob es einen eingehenden Anruf für eine der Teilnehmereinheiten **304(1)**–(X) gibt. Wie oben beschrieben, wenn es einen eingehenden Anruf für einen der Teilnehmereinheiten **304(1)**–(X) gibt, empfangen die Paging-Modems eine Page-Nachricht von der Basisstation **120**. Die Page-Nachricht enthält eine einzigartige ESN (oder MIN), die identifiziert, welche Teil-

nehmereinheit **304(1)**–(X) gerade angerufen wird. Wenn ein Paging-Modem eine Page-Nachricht empfängt, versieht das Paging-Modem das Steuersystem **314** mit der ESN in der Page-Nachricht. Auf diese Weise bestimmt das Steuersystem **314**, wann es einen eingehenden Anruf für einen der Teilnehmereinheiten **304(1)**–(X) gibt. Wenn es keine eingehenden Anrufe gibt, geht die Steuerung über in Schritt **424**, andernfalls geht die Steuerung über in den Schritt **414**.

[0057] Angenommen ein eingehender Anruf ist gerichtet an die Teilnehmereinheit **304(2)** (das heißt, die ESN in einer Page-Nachricht identifiziert die Teilnehmereinheit **304(2)**), bestimmt das Steuersystem **314**, ob die Teilnehmereinheit **304(2)** gerade verwendet wird, (das heißt, Off-Hook ist) (Schritt **414**). Wenn die Teilnehmereinheit **304(2)** benutzt wird, dann sendet das Steuersystem **314** ein Besetzt-Signal oder eine Page-Verweigerungsnachricht zur Basisstation **120** (Schritt **422**) und anschließend geht die Steuerung über in den Schritt **424**. Wenn die Teilnehmereinheit **304(2)** nicht benutzt wird, geht die Steuerung über in den Schritt **416**.

[0058] In Schritt **416** wählt das Steuersystem **314** ein verfügbares Modem, um den Anruf zu verarbeiten, und im Schritt **418** wird das ausgewählte Modem mit der Authentisierungsinformation von der Datenbank **317** versehen. Wie oben beschrieben speichert das Steuersystem **314** die Authentisierungsinformation für jeden Teilnehmer **302(1)**–(X) in der Datenbank **317**. In einem Ausführungsbeispiel versieht das Steuersystem **314** das ausgewählte Modem mit nur den dynamischen Authentisierungsdaten. In diesem Ausführungsbeispiel ist jedes Modem mit der statischen Authentisierungsinformation jedes Teilnehmers zum Zeitpunkt der CSS-**306**-Initialisierung versehen. In einem anderen Ausführungsbeispiel versieht das Steuersystem **314** das Modem mit beidem, der statischen und der dynamischen Authentisierungsinformation.

[0059] Das Steuersystem **314** bestimmt, welche Authentisierungsinformation von welchem Teilnehmer dem ausgewählten Modem basierend auf die Teilnehmereinheit **304**, die in der Page-Nachricht empfangen von der Basisstation **120** identifiziert wird, vorgesehen wird. In diesem Beispiel enthält die Page-Nachricht die ESN assoziiert mit der Teilnehmereinheit **304(2)**. Somit wird die Authentisierungsinformation des Teilnehmers **302(2)** an das ausgewählte Modem geliefert, welches dann mit der Teilnehmereinheit **304(2)** über den Schalter **308** (Schritt **420**) verkoppelt wird. Beim Verkoppeln der Teilnehmereinheit **304(2)** kann das ausgewählte Modem den Anruf des Teilnehmers verarbeiten. Das heißt, das ausgewählte Modem empfängt die Daten von der Teilnehmereinheit **304(2)** und sendet diese der Basisstation **120**, und empfängt den Verkehr von der Basisstation **120** und sendet ihn zur Teilnehmereinheit **304(2)**. Nach dem Schritt **420** geht die Steuerung über in Schritt **424**.

[0060] Im Schritt **424** bestimmt das Steuersystem **314**, ob ihm ein Modem **310** die aktualisierte, dynamische Authentisierungsinformation eines Teilnehmers geschickt hat. Wie oben erklärt kann ein Modem **310**, das einen Anruf für einen speziellen Teilnehmer **302** verarbeitet, ab und zu eine SSD-Aktualisierungsnachricht **210** von der Basisstation **120** empfangen. Ansprechend auf den Empfang einer solchen Nachricht von der Basisstation **120** aktualisiert das Modem **310** die DAI des Teilnehmers lokal und liefert anschließend, zu einem gewissen Punkt, die aktualisierte DAI an das Steuersystem **314**.

[0061] Wenn das Steuersystem **314** eine aktualisierte DAI von einem der Modems **310** nicht empfangen hat, dann kehrt die Steuerung zurück zu Schritt **402**. Andernfalls geht die Steuerung über zum Schritt **426**. In Schritt **426** aktualisiert das Steuersystem **314** die Datenbank **317** mit der empfangenen, aktualisierten DAI. Nach dem Schritt **426** geht die Steuerung zurück zum Schritt **402**, wo der Prozess sich selbst wiederholt.

[0062] Fig. 5 zeigt den Operationsfluss des Steuersystems **314** gemäß einem zweiten Ausführungsbeispiel. Der Prozess beginnt im Schritt **501**, wo das Steuersystem **314** die Modems **310** initialisiert. Das heißt, das Steuersystem **314** versieht jedes Modem **310** mit der statischen und dynamischen Authentisierungsinformation von jedem Teilnehmer **302**. Nach dem Schritt **501** geht die Steuerung über zum Schritt **502**. Im Schritt **502** bestimmt das Steuersystem **314**, ob eine der Teilnehmereinheiten **304** aktiviert worden ist. Wenn das Steuersystem **314** die Aktivierung einer Teilnehmereinheit **304** detektiert, geht die Steuerung über zum Schritt **504**, andernfalls geht die Steuerung über zum Schritt **512**.

[0063] Im Schritt **504** bestimmt das Steuersystem **314**, ob eines der Modems **310(1)**–(Y) verfügbar ist, um einen Anruf zu verarbeiten. Wenn ein Modem **310** verfügbar ist, geht die Steuerung über zum Schritt **508**, andernfalls sendet das Steuersystem **314** ein Besetzt-Signal zu der aktivierten Teilnehmereinheit (Schritt **510**) und der Prozess geht anschließend weiter im Schritt **512**.

[0064] Im Schritt **508** wählt das Steuersystem **314** eines der verfügbaren Modems aus, um den Anruf zu verarbeiten, und koppelt anschließend die aktivierte Teilnehmereinheit zum ausgewählten Modem über Schalter **308**. Beim Verkoppeln der aktivierten Teilnehmereinheit kann das ausgewählte Modem, Daten von der aktivierten Teilnehmereinheit empfangen und sendet die Daten zur Basisstation **120**. Nach Schritt **508** geht die Steuerung über zum Schritt **512**.

[0065] Im Schritt **512** bestimmt das Steuersystem **314**, ob es einen eingehenden Anruf für eine der Teilnehmereinheiten **304(1)**–(X) gibt. Wenn es keine eingehenden Anrufe gibt, geht die Steuerung über zum Schritt **524**, andernfalls geht die Steuerung über zum Schritt **514**.

[0066] Angenommen ein eingehender Anruf ist an die Teilnehmereinheit **304(2)** gerichtet, (das heißt, die ESN in einer Page-Nachricht identifiziert die Teilnehmereinheit **304(2)**), dann bestimmt das Steuersystem **314**, ob die Teilnehmereinheit **304(2)** gerade verwendet wird (das heißt, Off-Hook ist) (Schritt **514**). Wenn die Teilnehmereinheit **304(2)** verwendet wird, sendet das Steuersystem **314** anschließend ein Besetzt-Signal oder eine Page-Verweigerungsnachricht zur Basisstation **120** (Schritt **522**), und anschließend geht die Steuerung über zum Schritt **524**. Wenn die Teilnehmereinheit **304(2)** nicht verwendet wird, geht die Steuerung über zum Schritt **516**.

[0067] Im Schritt **516** wählt das Steuersystem **314** ein verfügbares Modem aus, um den Anruf zu verarbeiten. Anschließend verkoppelt das Steuersystem **314** das ausgewählte Modem mit der Teilnehmereinheit **304(2)** über den Schalter **308** (Schritt **520**). Beim Verkoppeln der Teilnehmereinheit **304(2)** kann das ausgewählte Modem den Anruf für den Teilnehmer verarbeiten. Das heißt, das ausgewählte Modem empfängt Daten von der Teilnehmereinheit **304(2)** und sendet sie zur Basisstation **120**, und empfängt Verkehr von der Basisstation **120** und sendet ihn zur Teilnehmereinheit **304(2)**. Nach dem Schritt **520** geht die Steuerung über zum Schritt **524**.

[0068] Im Schritt **524** bestimmt das Steuersystem **314**, ob ihm ein Modem **310** die aktualisierte, dynamische Authentisierungsinformation eines Teilnehmers gesendet wurde. Wie oben erklärt, kann ein Modem **310**, das einen Anruf verarbeitet, ab und zu eine SSD-Aktualisierungsnachricht **210** von der Basisstation **120** empfangen. Ansprechend auf den Empfang einer solchen Nachricht von der Basisstation **120** aktualisiert das Modem **310** die DAI des Teilnehmers lokal und liefert anschließend, zu einem gewissen Punkt, die aktualisierte DAI zum Steuersystem **314**. Wenn das Steuersystem **314** keine aktualisierte DAI von einem der Modems **310** empfangen hat, dann kehrt die Steuerung zum Schritt **502** zurück. Andernfalls geht die Steuerung über zum Schritt **526**. Im Schritt **526** liefert das Steuersystem **314** die aktualisierte DAI zu den anderen Modems. Die Steuerung geht dann zurück zum Schritt **502**.

[0069] Während verschiedene Ausführungsbeispiele der vorliegenden Erfindung oben beschrieben wurden, sollte es verstanden werden, dass sie nur als Beispiel präsentiert wurden, und nicht limitierend. Somit sollte der Umfang und Rahmen der vorliegenden Erfindung nicht durch irgendein oben beschriebenes Beispiel der Ausführungsbeispiele limitiert werden, sondern sollten nur definiert sein gemäß den folgenden Ansprüchen und deren Äquivalenzen.

Patentansprüche

1. Ein Verfahren zur Bereitstellung für eine Gruppe von Teilnehmern (**302**) den Zugriff zu einem drahtlosen Kommunikationsdienst in einem konzentrierten Teilnehmersystem (concentrated subscriber system), wobei jeder Teilnehmer (**302**) in der Gruppe von Teilnehmern mit einer Teilnehmereinheit (**304**) ausgestattet ist, wobei jeder Teilnehmer (**302**) in der Gruppe von Teilnehmern mit statischer und dynamischer Authentisierungsinformation bzw. Authentifizierungsinformation assoziiert ist, und wobei die Gruppe von Teilnehmern eine Vielzahl von Modems (**310**) teilen, wobei die folgenden Schritte vorgesehen sind:
(a) Detektieren der Aktivierung von einer der Teilnehmereinheiten (**304**);
(b) Auswahl eines Modems aus der Vielzahl von Modems (**310**);
(c) Koppeln der aktivierten Teilnehmereinheit (**304**) mit dem ausgewählten Modem (**310**), wodurch der Verkehr zwischen der aktivierten Teilnehmereinheit und dem ausgewählten Modem fließen kann; und
(d) Vorsehen dynamischer Authentisierungsinformation für das erwähnte ausgewählte Modem (**310**), wobei die erwähnte dynamische Authentisierungsinformation geliefert an das ausgewählte Modem die dynamische Authentisierungsinformation ist, die mit dem Teilnehmer (**302**) assoziiert ist, für den die aktivierte Teilnehmereinheit (**304**) vorgesehen ist.

2. Verfahren nach Anspruch 1, wobei ferner der folgende Schritt vorgesehen ist: Speichern der dynamischen Authentisierungsinformation, assoziiert mit jedem Teilnehmer in der Gruppe in einer Datenbank (**317**).

3. Verfahren nach Anspruch 2, wobei ferner der folgende Schritt vorgesehen ist: Entnahme der dynamischen Authentisierungsinformation aus der Datenbank (**317**), wobei die aus der Datenbank (**317**) entnommene Authentisierungsinformation die dynamische Authentisierungsinformation ist, die mit dem Teilnehmer assoziiert ist, für den die aktivierte Teilnehmereinheit (**304**) vorgesehen ist.

4. Verfahren nach Anspruch 3, wobei die an das ausgewählte Modem (**310**) gelieferte dynamische Authentisierungsinformation die dynamische Authentisierungsinformation ist, die aus der Datenbank (**317**) entnommen wurde.

5. Verfahren nach Anspruch 4, wobei ferner der folgende Schritt vorgesehen ist: Speichern der an das ausgewählte Modem gelieferten dynamischen Authentisierungsinformation in dem ausgewählten Modem (**310**).

6. Verfahren nach Anspruch 5, wobei ferner die folgenden Schritte vorgesehen sind:
Modifizieren der dynamischen Authentisierungsinformation, gespeichert in dem ausgewählten Modem (**310**), ansprechend auf das ausgewählte Modem; welches von einer Basisstation (**120**) eine Aktualisierungsnachricht empfängt; und
Speichern der modifizierten dynamischen Authentisierungsinformation in dem ausgewählten Modem (**310**).

7. Verfahren nach Anspruch 6, wobei ferner der folgende Schritt vorgesehen ist: Speichern der modifizierten dynamischen Authentisierungsinformation in der Datenbank (**317**).

8. Verfahren nach Anspruch 1, wobei ferner der folgende Schritt vorgesehen ist: Speichern der statischen Authentisierungsinformation assoziiert mit jedem Teilnehmer (**302**) in der Gruppe in jeder der Vielzahl von Modems (**310**).

9. Verfahren nach Anspruch 1, wobei ferner der folgende Schritt vorgesehen ist: Bestimmen ob eines der Vielzahl von Modems (**310**) zur Verarbeitung eines Anrufs verfügbar ist.

10. Verfahren nach Anspruch 9, wobei ferner der folgende Schritt vorgesehen ist: Übertragen eines Besetztsignals zu der aktivierten Teilnehmer- bzw. Subscribereinheit (**304**), wenn keines der Vielzahl von Modems zur Verarbeitung eines Anrufs verfügbar ist.

11. Verfahren zum Versorgen einer Gruppe von Teilnehmern in einem konzentrierten Teilnehmersystem (**306**) mit Zugriff zu einem drahtlosen Kommunikationsdienst, wobei jeder Teilnehmer (**302**) in der Gruppe von Teilnehmern mit einer Teilnehmereinheit (**304**) ausgestattet ist, wobei ferner jeder Teilnehmer in der Gruppe von Teilnehmern mit statischer und dynamischer Authentisierungsinformation bzw. Authentifizierungsinformation ausgestattet ist, und wobei ferner die Gruppe der Teilnehmer eine Vielzahl von Modems (**310**) teilen, wobei die folgenden Schritte vorgesehen sind:
(a) Detektieren eines ankommenden bzw. eingehenden Anrufs, adressiert an einen der Teilnehmer (**302**) in der Gruppe;
(b) Bestimmen eines angerufenen Teilnehmers (**302**), wobei der angerufene Teilnehmer der Teilnehmer in der Gruppe ist, an den der erwähnte ankommende Anruf adressiert ist;
(c) Auswahl eines verfügbaren Modems (**310**) aus der Vielzahl von Modems (**310**);
(d) Koppeln der für den angerufenen Teilnehmer vorgesehenen Teilnehmereinheit (**304**) mit dem ausgewählten Modem, wodurch der Verkehrsfluss zwischen der Teilnehmereinheit (**304**), vorgesehen für den angerufenen Teilnehmer und dem ausgewählten Modem (**310**), ermöglicht wird; und
(e) Vorsehen dynamischer Authentisierungsinformation an das ausgewählte Modem, wobei die dynamische Authentisierungsinformation, geliefert an das ausgewählte Modem (**310**), die mit dem angerufenen Teilnehmer assoziierte dynamische Authentisierungsinformation ist.

12. Verfahren nach Anspruch 11, wobei ferner der folgende Schritt vorgesehen ist: Speichern der mit jedem Teilnehmer in der Gruppe assoziierten dynamischen Authentisierungsinformation in einer Datenbank (**317**).

13. Verfahren nach Anspruch 12, wobei ferner der folgende Schritt vorgesehen ist: Entnahme dynamischer Authentisierungsinformation aus der Datenbank (**317**), wobei die aus der Datenbank (**317**) entnommene dynamische Authentisierungsinformation die dynamische Authentisierungsinformation ist, die mit dem angerufenen Teilnehmer (**302**) assoziiert ist.

14. Verfahren nach Anspruch 13, wobei die an das ausgewählte Modem (**310**) gelieferte dynamische Authentisierungsinformation die dynamische Authentisierungsinformation ist, die aus der Datenbank (**317**) entnommen wurde.

15. Verfahren nach Anspruch 14, wobei ferner der folgende Schritt vorgesehen ist: Speichern der erwähnten dynamischen Authentisierungsinformation, geliefert an das ausgewählte Modem in dem ausgewählten Modem (**310**).

16. Verfahren nach Anspruch 15, wobei ferner die folgenden Schritte vorgesehen sind:
Modifizieren der erwähnten dynamischen Authentisierungsinformation, gespeichert im ausgewählten Modem (**310**), und zwar ansprechend auf den Empfang einer Aktualisierungsnachricht von einer Basisstation (**120**) durch das ausgewählte Modem; und
Speichern der modifizierten dynamischen Authentisierungsinformation in dem ausgewählten Modem (**310**).

17. Verfahren nach Anspruch 16, wobei ferner der folgende Schritt vorgesehen ist: Speichern der modifizierten dynamischen Authentisierungsinformation in der Datenbank (**317**).

18. Verfahren nach Anspruch 11, wobei ferner der folgende Schritt vorgesehen ist: Speichern der statischen Authentisierungsinformation, assoziiert mit jedem Teilnehmer in der Gruppe in jedem der Vielzahl von Modems (**310**).

19. Verfahren nach Anspruch 11, wobei ferner die folgenden Schritte vorgesehen sind:
Bestimmen ob die Teilnehmereinheit (**304**), vorgesehen für den angerufenen Teilnehmer, sich im Ge-

brauch befindet; und
Senden eines Besetztsignals an die Basisstation (**120**), wenn die Teilnehmereinheit (**304**), vorgesehen für den angerufenen Teilnehmer (**304**), in Gebrauch ist.

20. Ein konzentriertes Teilnehmersystem (concentrated subscriber system) (**306**), welches Folgendes aufweist:
ein Transceiversystem (**322**, **320**, **318**) zum Senden von HF-Wellenfrequenzsignalen an eine Basisstation und zum Empfang von HF-Wellenfrequenzsignalen von einer Basisstation (**120**);
eine Vielzahl von Modems (**310**), wobei jedes der Vielzahl von Modems mit dem erwähnten Transceiversystem (**322**, **320**, **318**) gekoppelt ist;
eine Vielzahl von Teilnehmereinheiten (**304**), deren jeder einzigartige statische und dynamische Authentisierungsinformation zugewiesen ist;
einen Schalter bzw. Switch (**308**), gekoppelt mit jedem der Vielzahl von Modems (**310**) und gekoppelt mit jeder der Vielzahl von Teilnehmereinheiten (**304**);
ein Steuersystem (**314**) in Verbindung mit dem Schalter (**308**) und jedem der Vielzahl von Modems; und
eine Datenbank (**317**) zum Speichern von mindestens der dynamischen Authentisierungsinformation, wobei die Datenbank (**317**) für das Steuersystem (**314**) zugreifbar ist, wobei
das Steuersystem (**314**) für Folgendes geeignet ist: ein verfügbares Modem (**310**) aus der Vielzahl von Modems zu bestimmen, wenn eine der Vielzahl von Teilnehmereinheiten (**304**) aktiviert ist, ferner den Schalter (**308**) anzuweisen, eine der erwähnten Vielzahl von Teilnehmereinheiten mit dem erwähnten verfügbaren Modem zu verbinden, aus der Datenbank (**317**) die gespeicherte dynamische Authentisierungsinformation, assoziiert mit der erwähnten einen der Vielzahl von Teilnehmereinheiten (**304**) zu entnehmen, und das verfügbare Modem mit der entnommenen gespeicherten dynamischen Authentisierungsinformation zu beliefern.

21. Das konzentrierte Teilnehmersystem (**306**) nach Anspruch 20, wobei dann wenn das konzentrierte Teilnehmersystem (**306**) initialisiert ist, das Steuersystem geeignet ist, jedes der Vielzahl von Modems mit der statischen Authentisierungsinformation entsprechend jeder der Vielzahl von Teilnehmereinheiten zu beliefern.

22. Das konzentrierte Teilnehmersystem (**306**) nach Anspruch 20, wobei das erwähnte verfügbare Modem geeignet ist, die dynamische Authentisierungsinformation geliefert an dieses, vom Steuersystem (**314**) zu modifizieren, und zwar ansprechend auf den Empfang einer Nachricht von der Basisstation (**120**), wobei das verfügbare Modem ferner geeignet ist um die modifizierten dynamische Authentisierungsinformation an das erwähnte Steuersystem (**314**) zu übertragen.

23. Das konzentrierte Teilnehmersystem (**306**) nach Anspruch 22, wobei das Steuersystem (**314**) geeignet ist, die erwähnte modifizierte dynamische Authentisierungsinformation in der Datenbank (**317**) zu speichern.

Es folgen 5 Blatt Zeichnungen

Anhängende Zeichnungen

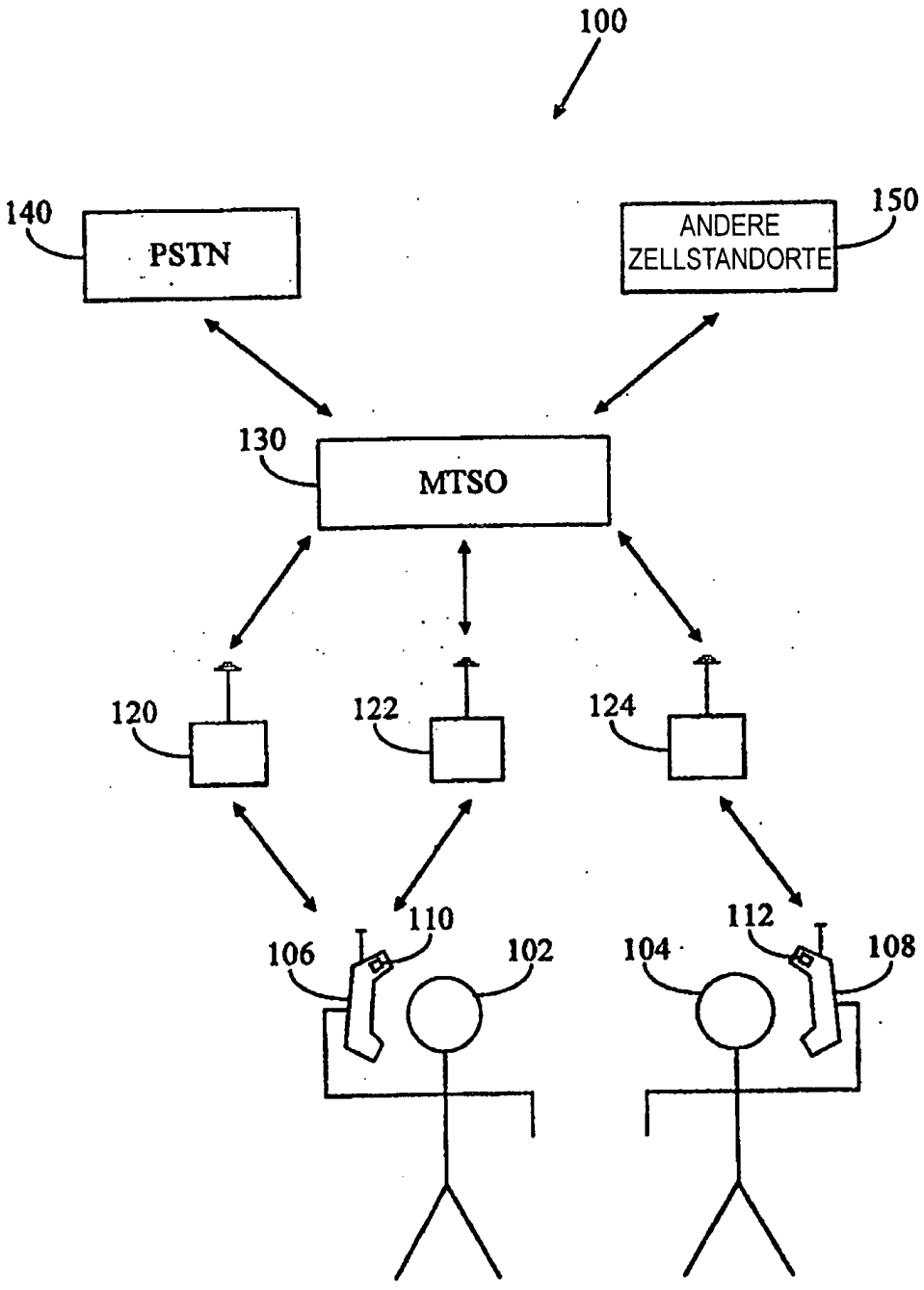

FIG. 1

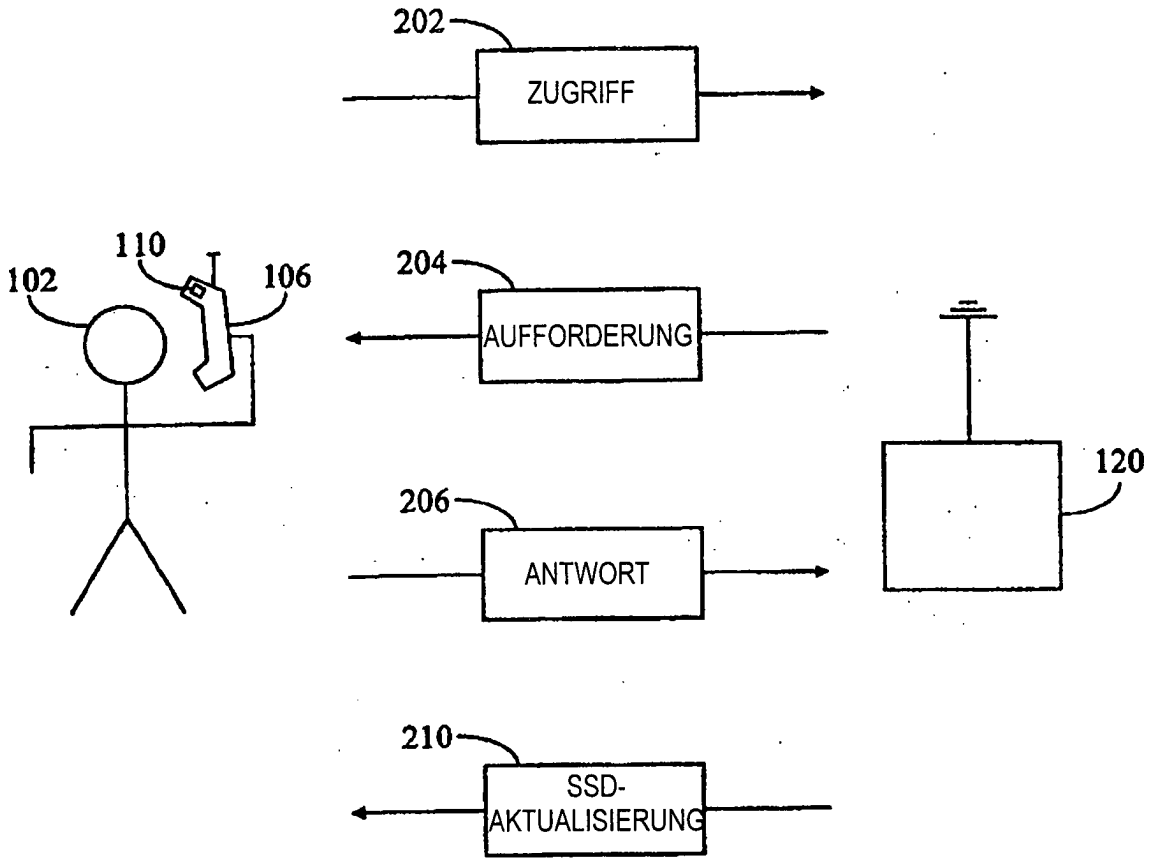
202
ZUGRIFF
110
102
106
204
AUFFORDERUNG
120
206
ANTWORT
210
SSD-
AKTUALISIERUNG

FIG. 2

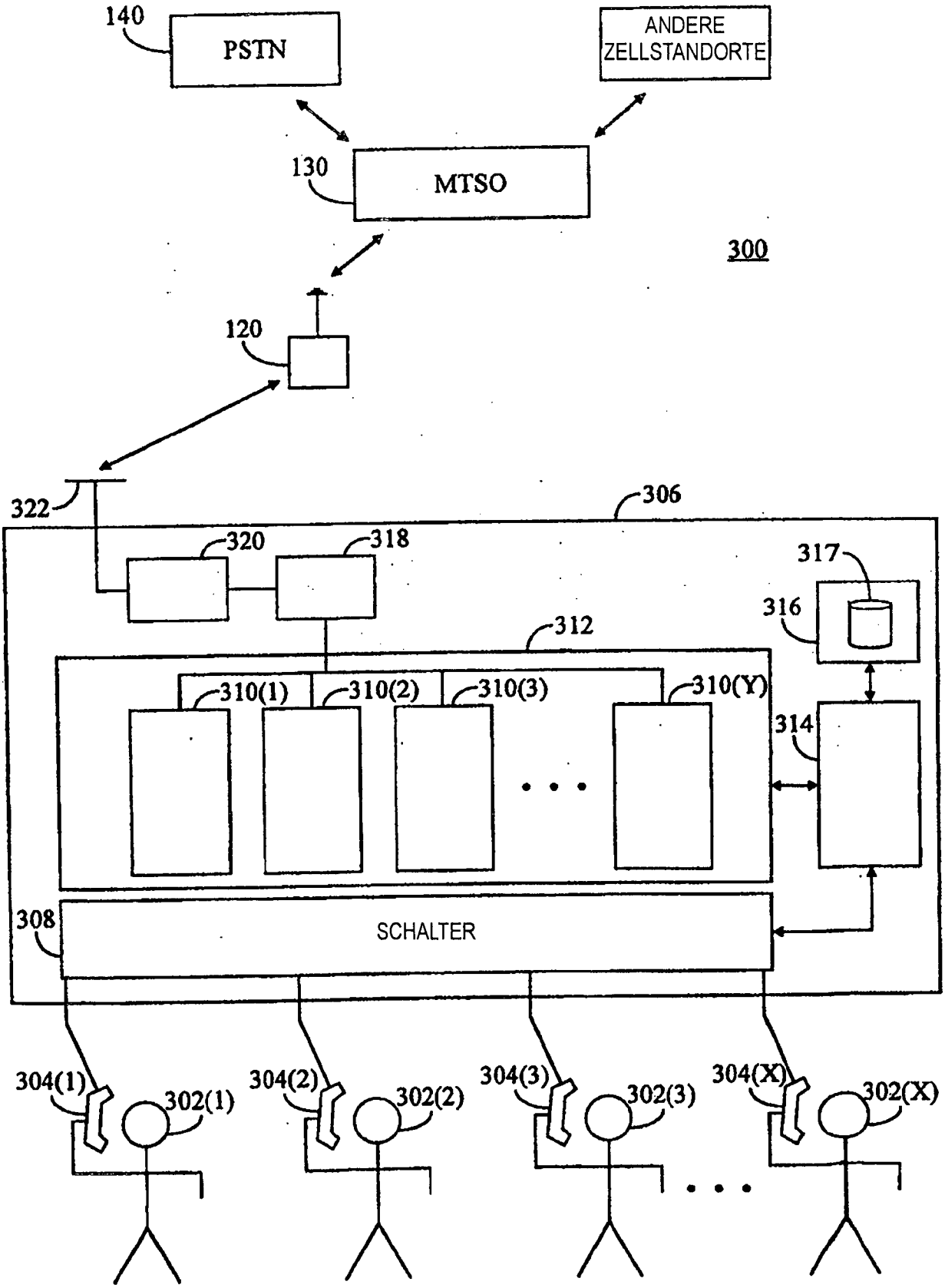
140
PSTN
ANDERE ZELLSTANDORTE
130
MTSO
300
120
322
306
320
318
317
316
312
310(1)
310(2)
310(3)
310(Y)
314
308
SCHALTER
304(1)
302(1)
304(2)
302(2)
304(3)
302(3)
304(X)
302(X)

FIG. 3

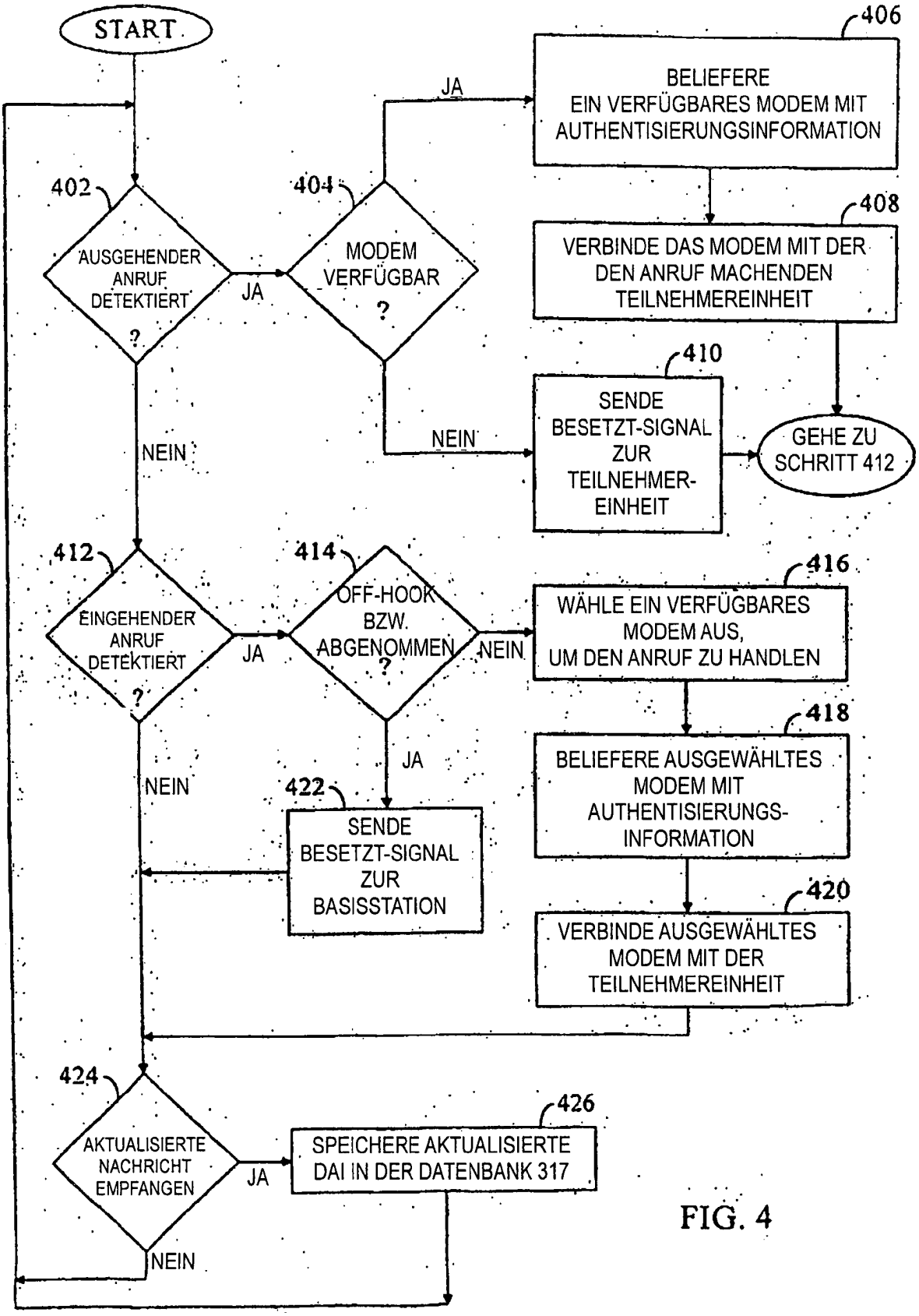
START
402
AUSGEHENDER ANRUF DETEKTIERT ?
JA
404
MODEM VERFÜGBAR ?
JA
406
BELIEFERE EIN VERFÜGBARES MODEM MIT AUTHENTISIERUNGSINFORMATION
408
VERBINDE DAS MODEM MIT DER DEN ANRUF MACHENDEN TEILNEHMEREINHEIT
NEIN
410
SENDE BESETZT-SIGNAL ZUR TEILNEHMER-EINHEIT
GEHE ZU SCHRITT 412
NEIN
412
EINGEHENDER ANRUF DETEKTIERT ?
JA
414
OFF-HOOK BZW. ABGENOMMEN ?
NEIN
416
WÄHLE EIN VERFÜGBARES MODEM AUS, UM DEN ANRUF ZU HANDLEN
418
BELIEFERE AUSGEWÄHLTES MODEM MIT AUTHENTISIERUNGS-INFORMATION
420
VERBINDE AUSGEWÄHLTES MODEM MIT DER TEILNEHMEREINHEIT
NEIN
JA
422
SENDE BESETZT-SIGNAL ZUR BASISSTATION
424
AKTUALISIERTE NACHRICHT EMPFANGEN
JA
426
SPEICHERE AKTUALISIERTE DAI IN DER DATENBANK 317
NEIN

FIG. 4

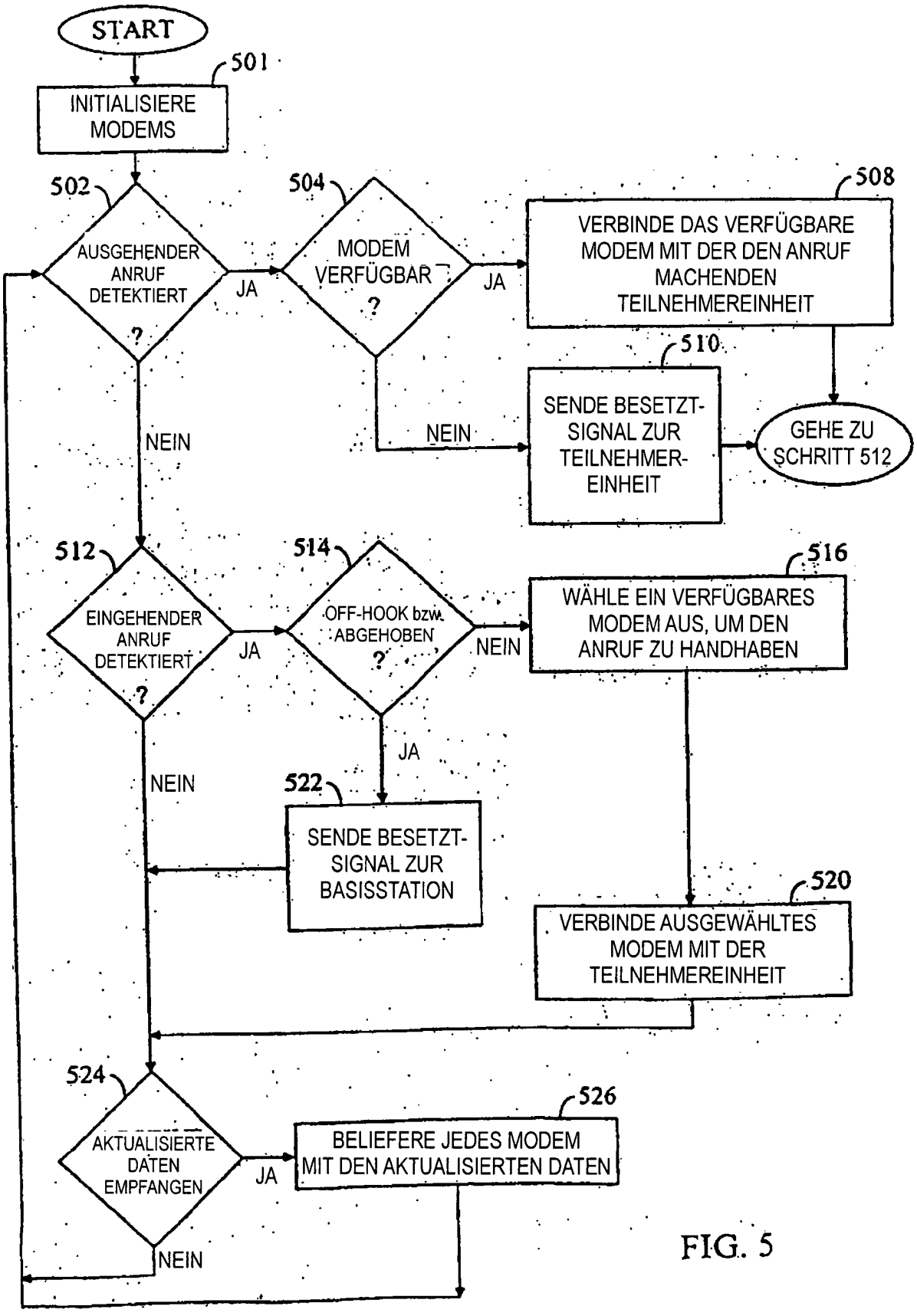
START
501
INITIALISIERE MODEMS
502
AUSGEHENDER ANRUF DETEKTIERT ?
JA
504
MODEM VERFÜGBAR ?
JA
508
VERBINDE DAS VERFÜGBARE MODEM MIT DER DEN ANRUF MACHENDEN TEILNEHMEREINHEIT
NEIN
510
SENDE BESETZT-SIGNAL ZUR TEILNEHMER-EINHEIT
NEIN
GEHE ZU SCHRITT 512
512
EINGEHENDER ANRUF DETEKTIERT ?
JA
514
OFF-HOOK bzw. ABGEHOBEN ?
NEIN
516
WÄHLE EIN VERFÜGBARES MODEM AUS, UM DEN ANRUF ZU HANDHABEN
JA
NEIN
522
SENDE BESETZT-SIGNAL ZUR BASISSTATION
520
VERBINDE AUSGEWÄHLTES MODEM MIT DER TEILNEHMEREINHEIT
524
AKTUALISIERTE DATEN EMPFANGEN
JA
526
BELIEFERE JEDES MODEM MIT DEN AKTUALISIERTEN DATEN
NEIN

FIG. 5