(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 051 053 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
08.11.2000 Patentblatt 2000/45

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

(21) Anmeldenummer: **00107879.9**

(22) Anmeldetag: **12.04.2000**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **03.05.1999 DE 19920222**

(71) Anmelder:
Rohde & Schwarz GmbH & Co. KG
D-81671 München (DE)

(72) Erfinder:
- **Frick, Joachim**
  86391 Stadtbergen (DE)
- **Bott, Rainer**
  82346 Andechs (DE)

(74) Vertreter:
Graf, Walter, Dipl.-Ing. et al
Mitscherlich & Partner
Patent- u. Rechtsanwälte,
Sonnenstrasse 33
80331 München (DE)

(54) Verfahren zum Identifizieren des Benutzers eines Mobiltelefons oder zum Mithören der abgehenden Gespräche

(57) Zum Identifizieren und Abhören eines Mobiltelefons in einem öffentlichen digitalen zellularen Mobilfunknetz wird folgendes Verfahren benutzt:

in räumlicher Nähe zum Mobiltelefon (MS) wird eine virtuelle Basisstation (VBTS) mit einem damit verbundenen Test-Mobiltelefon (TMS) betrieben;
mittels des Test-Mobiltelefons (TMS) werden durch eine Zellenabfrage über die dem gewählten Standort zugeordnete Netz-Basisstation (BTS1) mit der höchsten Leistung die Liste (BA) aller dem Standort benachbarten Basisstationen ermittelt;
davon wird dann eine Basisstation (BTS2) ausgewählt, die der dem gewählten Standort zugeordneten Basisstation (BTS1) höchster Leistung benachbart ist;
auf deren Kanalfrequenz (BCCH) wird anschließend die virtuelle Basisstation (VBTS) mit einer Leistung, die beim Mobiltelefon (MS) größer ist als die der dem Standort zugehörigen Netz-Basisstation (BTS1), und mit einem Bereichscode, der von dem dem Standort zugehörigen Bereichscode (LAC) abweicht, betrieben;
damit wird das Mobiltelefon (MS) veranlaßt, auf die virtuelle Basisstation (VBTS) zu wechseln und ihre Parameter (IMSI, IMEI) mit dieser auszutauschen.

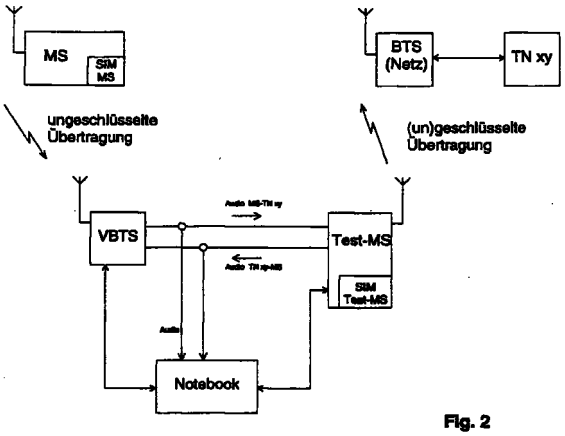

Fig. 2

EP 1 051 053 A2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Identifizieren des Benutzers eines Mobiltelefons in einem öffentlichen digitalen zellularen Mobilfunknetz sowie zum Mithören von abgehenden Gesprächen dieses Mobiltelefons.

[0002] Bei modernen öffentlichen digitalen zellularen Mobilfunknetzen besteht im öffentlichen Interesse oftmals die Notwendigkeit, den Benutzer eines Mobiltelefons durch Ermittlung seiner IMSI (International Mobile Subscriber Identity (Internationale Mobilteilnehmerkennung)) bzw. der IMEI (International Mobile Station Equipment Identity (Mobilgerätekennung)) des von ihm benutzten Mobiltelefons zu identifizieren oder sogar die Gespräche dieses Benutzers abzuhören.

[0003] Es ist daher Aufgabe der Erfindung, den hierzu berechtigten öffentlichen Diensten, wie z. B. Polizei, ein Gerät und ein damit ausführbares Verfahren zur Verfügung zu stellen, mit dem in einem digitalen zellularen Mobilfunknetz beliebige Benutzer von Mobiltelefonen identifiziert und deren Gespräche abgehört werden können.

[0004] Diese Aufgabe wird ausgehend von einem Verfahren laut Oberbegriff des Hauptanspruches durch dessen kennzeichnende Merkmale gelöst. Vorteilhafte Weiterbildungen insbesondere bezüglich des Abhörens solcher identifizierter Mobiltelefone und auch bezüglich einer einfachen Geräteeinheit zum Ausführen eines solchen Verfahrens ergeben sich aus den Unteransprüchen.

[0005] Die Erfindung wird im Folgenden anhand schematischer Zeichnungen am Ausführungsbeispiel des bekannten GSM-(Global System for Mobile Communications)-Mobilfunknetzes näher erläutert.

[0006] Die in der nachfolgenden Beschreibung benutzten Abkürzungen und Begriffe sind geformt (ETR 350 GSM 01.04) und werden in der entsprechenden Normvorschrift beispielsweise GSM05.02 näher erläutert. Sie sind außerdem in dem Buch "The GSM System for Mobile Communications" von Michel MOULY und Marie-Bernadette PAUTET näher erläutert, die nachfolgend verwendeten Abkürzungen sind außerdem im INDEX dieses Buches erläutert.

[0007] Für die Identifizierung des Benutzers eines Mobiltelefons, das in einem öffentlichen zellularen Mobilfunknetz betrieben wird, ist die Bestimmung der IMSI- bzw. IMEI-Nummer eine wichtige Kenngröße.

[0008] Um diese Identifikationskriterien zu erfassen, ist erfindungsgemäß eine virtuelle Basisstation VBTS vorgesehen, ein vorzugsweise mobiles Gerät, das wie eine übliche Netz-Basisstation BTS aufgebaut ist und genauso wie diese betreibbar ist. Diese VBTS steht in unmittelbarer Verbindung mit einem Test-Mobiltelefon TMS. Diesen beiden Geräten ist außerdem eine Auswerteinrichtung vorzugsweise in Form eines Notebooks zugeordnet.

[0009] Zur Identifizierung eines Mobiltelefons und zur Abfrage relevanter Parameter, wie z.B. der gewünschten IMSI- und IMEI-Nummern des ausgewählten Mobiltelefons MS wird die VBTS in möglichst räumlicher Nähe des Mobiltelefons MS aufgestellt, so daß bezüglich der VBTS annähernd die gleiche Zellumgebung herrscht wie bei der zu identifizierenden MS, wie dies in Figur 1 schematisch dargestellt ist. Es sei angenommen, daß das Mobiltelefon MS die Basisstation BTS 1 mit dem momentan höchsten Leistungspegel als Betriebszelle ausgewählt hat. Die MS mißt im Normalfall (eingeschalteter Zustand, eingebucht auf die Betriebszelle und Betrieb im IDLEMODE) nur die Pegel der Nachbarzellen, die ihr von der Betriebszelle BTS1 über die sogenannte BA-Liste (Liste der in der Umgebung des MS-betriebenen Basisstationen mit den zugehörigen Kontrollkanälen BCCH) mitgeteilt werden. Damit die MS die zur Identifikation benutzte VBTS wahrnimmt und in ihre Pegelmeßroutine aufnimmt, muß die VBTS eine Kontrollkanalfrequenz BCCH aus dieser BA-Liste der Basisstation BTS 1 abstrahlen.

[0010] Dazu muß zunächst eine Zellenabfrage (Cell Monitormg) durchgeführt werden und zwar wie folgt:

[0011] Am Standort des VBTS, der möglichst nahe am MS ist, werden die Parameter der Basisstation BTS1 in das Test-Mobiltelefon TMS über eine entsprechende Datenschnittstelle eingelesen und die so empfangene BA-Liste ausgewertet. Aus dieser BA-Liste wird eine der BTS1 benachbarte Basisstation BTSx mit der zugehörigen Kontrollkanalfrequenz BCCH entweder manuell oder automatisch ausgewählt und die Parameter dieser benachbarten Basisstation, beispielsweise BTS2, werden in die VBTS eingelesen und entsprechend modifiziert von dieser abgestrahlt. Durch die Wahl einer benachbarten Zelle BTS2 anstelle von BTS1 wird vermieden, daß laufende Gespräche eventuell abgebrochen werden.

[0012] Die am Standort der MS empfangene TX-Leistung der VBTS muß höher als die der Basisstation BTS1 sein, um das Radio-Kriterium C1 für einen Zellenwechsel (Cell-Reselect) zu erfüllen. Dies wird durch entsprechende Senderleistung des VBTS und/oder durch räumliche Nähe der VBTS zur zu identifizierenden MS erreicht.

[0013] Wenn diese Radiokriterien erfüllt sind, so kann die MS einen Zellenwechsel auf die VBTS vornehmen.

[0014] Im GSM-Netz sind vom Netzbetreiber verschiedene räumlich benachbarte Basisstationen zu sogenannten LAC zusammengefaßt, wie dies für LAC1 und LAC2 in Figur 1 dargestellt ist. Nur wenn ein Wechsel eines Mobiltelefons (im Idle Mode) von LAC1 zu LAC2 erfolgt, ist ein Parameteraustausch zwischen MS und BTS möglich.

[0015] Aus diesem Grunde strahlt die VBTS einen von den Zellen in der Nachbarschaft der MS unterschiedlichen LAC ab. Dies wird dadurch erreicht, daß bei der Zellenabfrage mittels des TMS von allen Zellen in der Nachbarschaft der LAC ermittelt wird und dann

ein von diesen LAC unterschiedlicher LAC (LAC-VBTS) abgestrahlt wird. Damit wird erreicht, daß mit dem Einbuchen der zu identifizierenden MS bei VBTS die MS auch tatsächlich ihre relevanten Parameter wie IMSI, IMEI und dergleichen Kennungen an die VBTS überträgt und in dieser dann entsprechend ausgewertet werden können.

[0016] Solange die VBTS abstrahlt und die Radio-Kriterien für die MS erfüllt sind, bleibt die MS auf der VBTS eingebucht und ist damit vom öffentlichen Netz, also der ihr zugehörigen Basisstation BTS1, abgetrennt. Nach Abschluß der Identifikation der MS soll diese aber im Normalfall möglichst sofort wieder auf die BTS1 oder eine andere Basisstation des öffentlichen Netzes zurückkehren, um wieder erreichbar zu sein. Um dies auch ohne Abschalten des Senders VBTS zu erreichen, wird wie folgt vorgegangen:

[0017] Bei allen Mobiltelefonen MS des GSM-Systems ist ein sogenannter downlink signaling counter DSC vorgesehen, nach der GSM-Norm 05.08 6.5 muß gesteuert durch diesen DSC die MS eine neue Basisstation auswählen, wenn der DSC den Wert Null erreicht. Der DSC wertet dabei die Daten aus, die im Rufkanal PCH (Paging Channel) übertragen werden. Wenn die dort übertragenen Daten richtig decodiert werden, erhöht sich der Zählerstand von DSC um 1, wenn die Decodierung jedoch fehlerhaft ist, wird der Zählerstand um 4 erniedrigt.

[0018] Dies wird gemäß der Erfindung ausgenutzt, um die identifizierte MS wieder in das Netz zurückzuzwingen, indem der VBTS für eine gewisse Zeit auf dem PCH fehlerhafte Daten sendet und so der DSC im MS bis auf Null zurückgestuft wird und dann die MS einen Zellenwechsel durchführen muß, also vom VBTS wieder auf die Netz-Basisstation BTS1 zurückkehrt.

[0019] Um einen solchen Zellenwechsel nur für ausgewählte MS zu erzwingen, ist noch Folgendes vorgesehen:

[0020] Gewisse MS, von der VBTS bestimmt, sollen auf der VBTS weiter campen, alle anderen MS sollen nach der Abfrage relevanter Parameter durch die VBTS wieder auf die BTS1 oder eine andere BTSx des öffentlichen Netzes zurückkehren. Um die Cell-Reselection der MS im Erfassungsbereich möglichst gezielt einsetzen zu können, muß die Anzahl der Paging Groups maximiert werden. So können ein oder mehrere bestimmte Mobiles auf der VBTS weiterhin campen, während alle anderen eine Cell Reselection auf die BTS in der Umgebung durchführen.

[0021] Die Anzahl der Paging Groups kann über die Parameter BS_AG_BLKS_RES und BS_PA_MFRMS auf dem CCH eingestellt werden. (GSM 05.02) und wird über den BCCH abgestrahlt.

[0022] Die Paging Group einer MS wird durch die 3 letzten Ziffern der IMSI (auf der SIM-Karte abgelegt) bestimmt. (GSM 05.02 6.5.2, 6.5.3). Da die VBTS die IMSI der gerade eingebuchten MS kennt, werden nun auf dieser speziellen Paging Group für eine gewisse Zeit fehlerhafte Daten gesendet, die den DSC der MS auf 0 dekrementieren lassen und die MS zu einer Cell Reselection zwingen.

[0023] Nach erfolgter Cell Reselection auf eine BTSx des öffentlichen Netzes werden vom MS weiterhin die benachbarten Zellen (über die BA-Liste von BTSx definiert) pegelmäßig ausgewertet. Falls in der BA-Liste von BTSx sich auch der Kanal der VBTS befindet und die VBTS immer noch sendet, so wird die MS für die VBTS wahrscheinlich immer noch das beste Radio-Kriterium errechnen und eine Cell Reselection (frühestens nach 5sec) wieder auf die VBTS machen. Um dieses dauernde Hin und Her zwischen VBTS und BTS und die damit verbundene Signalisierungsbelastung der VBTS zu minimieren, wird die BA-Liste der VBTS modifiziert.

[0024] Am Standort der VBTS werden mit dem Zell-Monitor die BA-Listen der Nachbarzellen eingelesen und aus diesen Daten wird eine (oder mehrere) Nachbarzelle(n) ermittelt, deren BA-Liste den Kanal der VBTS nicht enthält. Diese Zelle wird dann in die BA-Liste der VBTS eingetragen und über den BCCH abgestrahlt. Dabei kann es, vor allem in Gebieten mit vielen räumlich kleinen Zellen, Zellen geben, von denen aus die MS erst nach dem Umweg über 2 oder mehr Zellen wieder eine Zelle erreicht, deren BA-Liste den Kanal der VBTS enthält. So können Verweildauern von 1 Min. bis zu unendlich erreicht werden, in denen die MS die VBTS nicht mehr aufsucht.

[0025] Mit der erfindungsgemäßen Anordnung einer virtuellen Basisstation können auch die abgehenden Gespräche der so identifizierten Mobilstation MS abgehört werden, wie dies Figur 2 zeigt. Es wird wieder von dem ersten Verfahrensschritt ausgegangen, nach welchem die abzuhörende MS auf der virtuellen Basisstation VBTS eingebucht hat, d.h. sie ist in dieser Zeit vom eigentlichen Netz und den Netz-Basisstationen BTS nicht erreichbar und kann auch nicht angerufen werden.

[0026] Das Test-Mobiltelefon TMS wird durch geeignete Maßnahmen auf einer benachbarten Netz-Basisstation eingebucht. Wegen der räumlichen Nähe zur VBTS würde die TMS an sich auf letzterer einbuchen, aus diesem Grunde muß durch geeignete Maßnahmen ein Einbuchen auf einer Netz-Basisstation erzwungen werden.

[0027] Ein Ruf der abzuhörenden MS kommt bei der VBTS an. Um die Verschlüsselung im GSM-Netz zu umgehen, signalisiert die VBTS der MS, die Verschlüsselung auszuschalten. Die gerufene Telefonnummer wird erfaßt und der Test-MS übergeben. Die Test-MS wählt dann diese Telefonnummer an, dabei wird gleichzeitig die Sprachsignalverbindung zwischen VBTS und Test-MS durchgeschaltet. Das Gespräch wird auf Kosten der SIM-Karte in der Test-MS geführt. Da dies eine normale SIM-Karte ist, kann die Übertragung zwischen Test-MS und Netz-BTS sowohl verschlüsselt als auch ungeschlüsselt sein. Die SIM-Karte in der MS wird

mit keinen Gebühren belastet.

[0028] Bucht die Test-MS anstatt mit den Daten ihrer SIM-Test-MS mit den Daten der SIM-MS im öffentlichen Netz ein, so können für diese MS auch ankommende Gespräche mitgehört werden. In diesem Fall kommt der Ruf für die MS bei der Test-MS an, wird erfaßt und über die VBTS zur MS weitergeleitet. Die SIM-Karte der MS wird mit den Gebühren belastet.

[0029] Die aufgebaute Verbindung kann nun mit einer geeigneten Abhöreinrichtung, beispielsweise über den eingebauten Lautsprecher eines Notebooks, mitgehört werden. Vorzugsweise werden die beiden Audio-Pfade

$$MS \rightarrow TN\ xy\ (= L) \text{ und } TN\ xy \rightarrow MS\ (=R)$$

an die Stereoeingänge des Notebooks als Stereosignal angeliefert. Damit ist über die Gesprächsrichtung eine eindeutige Zuordnung der Gesprächspartner möglich.

[0030] Mithörmöglichkeiten bestehen über die eingebauten Stereolautsprecher oder über einen extern anzuschließenden Kopfhörer.

[0031] Weiterhin kann das Gespräch gleichzeitig mitgeschnitten und als Protokoll abgespeichert werden (Zuordnung IMSI $\rightarrow$ File). Dieses Protokoll kann dann später ausgewertet werden.

Patentansprüche

1. Verfahren zum Identifizieren eines Mobiltelefons (MS) in einem öffentlichen digitalen zellularen Mobilfunknetz,
dadurch gekennzeichnet,

daß in räumlicher Nähe zum Mobiltelefon (MS) eine virtuelle Basisstation (VBTS) mit einem damit verbundenen Test-Mobiltelefon (TMS) betrieben wird,
mittels des Test-Mobiltelefons (TMS) durch eine Zellenabfrage über die dem gewählten Standort zugeordnete Netz-Basisstation (BTS1) mit der höchsten Leistung die Liste (BA) aller dem Standort benachbarten Basisstationen ermittelt werden,
davon eine Basisstation (BTS2) ausgewählt wird, die der dem gewählten Standort zugeordnete Basisstation (BTS1) höchster Leistung benachbart ist,
und auf deren Kanalfrequenz (BCCH) dann die virtuelle Basisstation (VBTS) mit einer Leistung, die beim Mobiltelefon (MS) größer ist als die der dem Standort zugehörigen Netz-Basisstation (BTS1), und mit einem Bereichscode, der von dem dem Standort zugehörigen Bereichscode (LAC) abweicht, betrieben wird,
und damit das Mobiltelefon (MS) veranlaßt wird, auf die virtuelle Basisstation (VBTS) zu wechseln und ihre Parameter (IMSI, IMEI) mit dieser auszutauschen.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,

daß nach dem Einbuchen des Mobiltelefons (MS) auf der virtuellen Basisstation (VBTS) auf dem Rufkanal (PCH) durch die virtuelle Basisstation so lange fehlerhafte Daten gesendet werden, bis das Mobiltelefon (MS) einen Basisstationwechsel ins öffentliche Netz vornimmt.

3. Verfahren nach Anspruch 2,
dadurch gekennzeichnet,

daß aus der bei der Zellenabfrage gewonnenen Liste (BA) aller benachbarten Basisstationen mindestens eine Nachbar-Basisstation ermittelt wird, deren Liste (BA) den von der virtuellen Basisstation (VBTS) benutzten Kanal nicht enthält, und diese Basisstation dann in die von der virtuellen Basisstation abgestrahlte Liste (BA) eingetragen wird.

4. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,

daß zum Abhören der von dem identifizierten Mobiltelefon (MS) abgehenden Gespräche das Test-Mobiltelefon (TMS) so eingestellt wird, daß es auf einer Netz-Basisstation (BTS) einbucht,
und bei einem bei der virtuellen Basisstation (VBTS) ankommenden Ruf des abzuhörenden Mobiltelefons (MS) die gerufene Telefonnummer erfaßt und an das Test-Mobiltelefon (TMS) übergeben wird, das dann seinerseits diese Telefonnummer im Netz anwählt und gleichzeitig die Gesprächsverbindung zwischen dem Test-Mobiltelefon (TMS) und der mit dem abzuhörenden Mobiltelefon (MS) verbundenen virtuellen Basisstation (VBTS) herstellt, über die dann die aufgebaute Verbindung abhörbar ist.

5. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,

daß zum Abhören der beim identifizierten Mobiltelefon (MS) ankommenden Gespräche das Test-Mobiltelefon (TMS) mit den Daten des Mobiltelefons (MS) im öffentlichen Netz einbucht, so daß ein bei dem Test-Mobiltelefon (TMS) ankommender Ruf für das abzuhörende Mobiltelefon (Ms) über die virtuelle Basisstation (VBTS) an das Mobiltelefon weitergeleitet wird.

6. Anordnung zum Ausführen eines Verfahrens nach einem der vorhergehenden Ansprüche, **gekennzeichnet durch**

eine als virtuelle Basisstation einsetzbare Basisstation (VBTS) mit einem GSM-normgerechten Aufbau, die über eine Leitung unmittelbar verbunden ist mit einem Test-Mobiltelefon (TMS), wobei an dieser Leitungsverbindung eine Auswerteinrichtung zum Auswerten der bei der virtuellen Basisstation (VBTS) ankommenden Daten und/oder zum Abhören der auf dieser Leitung geführten Gespräche angeschlossen ist.

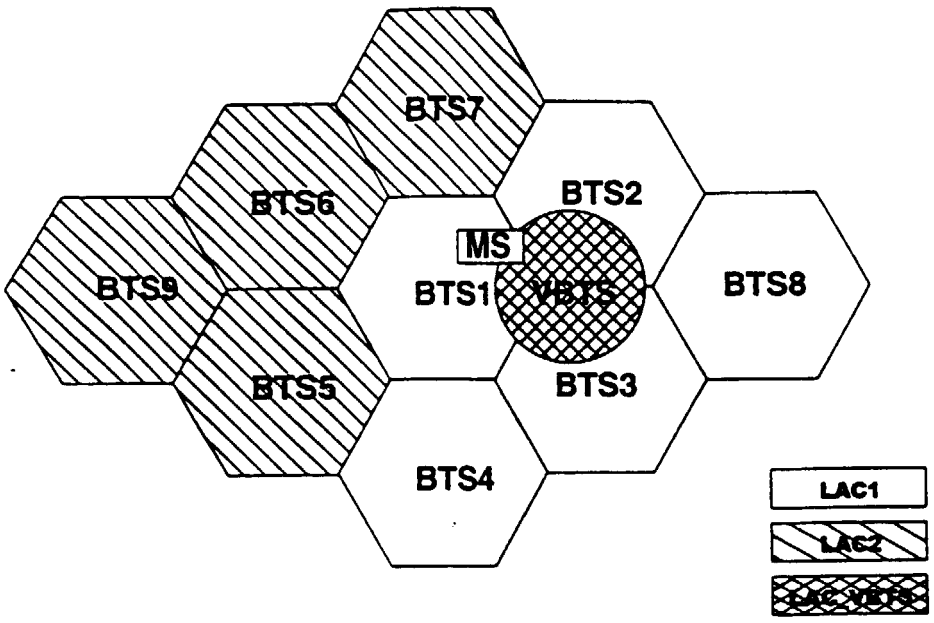
BTS7
BTS6
BTS2
MS
BTS9
BTS1
VBTS
BTS8
BTS5
BTS3
BTS4
LAC1
LAC2

Fig. 1

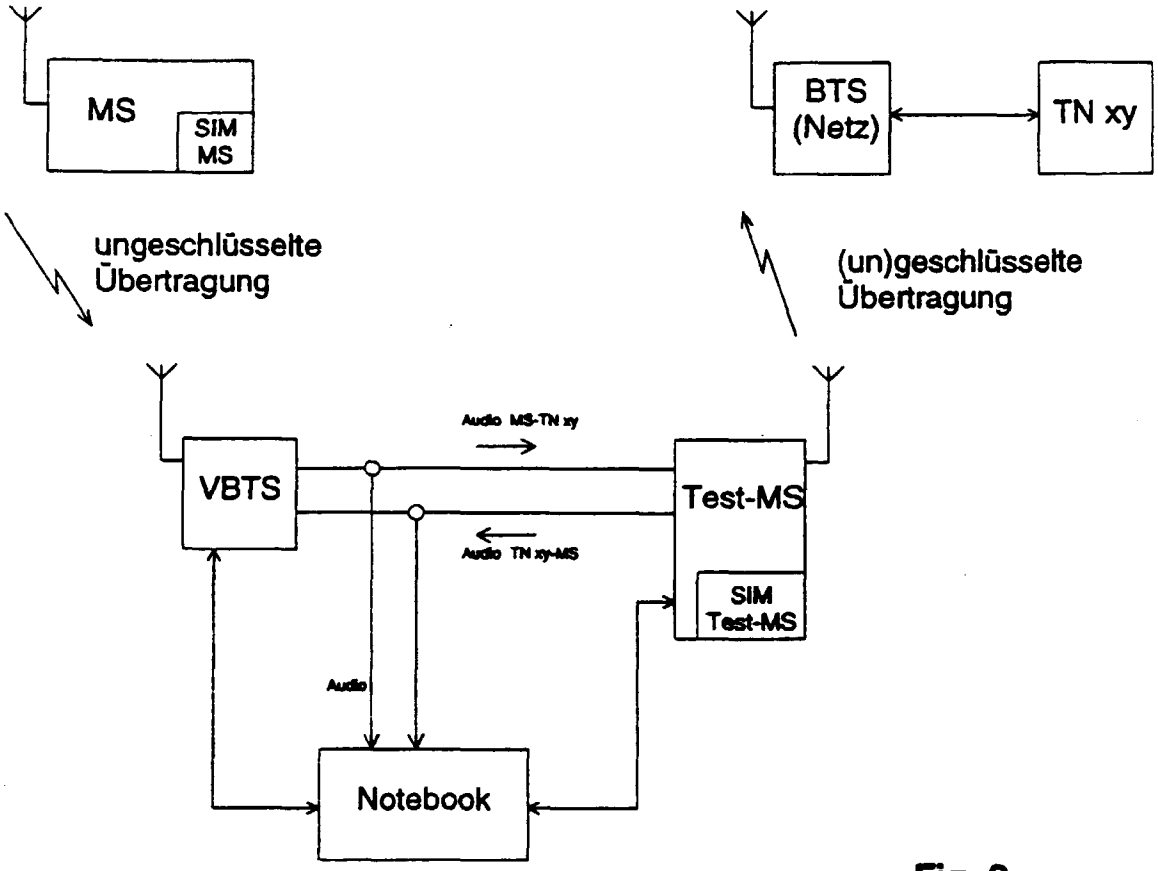
MS
SIM
MS
BTS
(Netz)
TN xy
ungeschlüsselte
Übertragung
(un)geschlüsselte
Übertragung
Audio MS-TN xy
VBTS
Test-MS
Audio TN xy-MS
SIM
Test-MS
Audio
Notebook

Fig. 2