OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(12) (19) (CA) **Demande-Application**

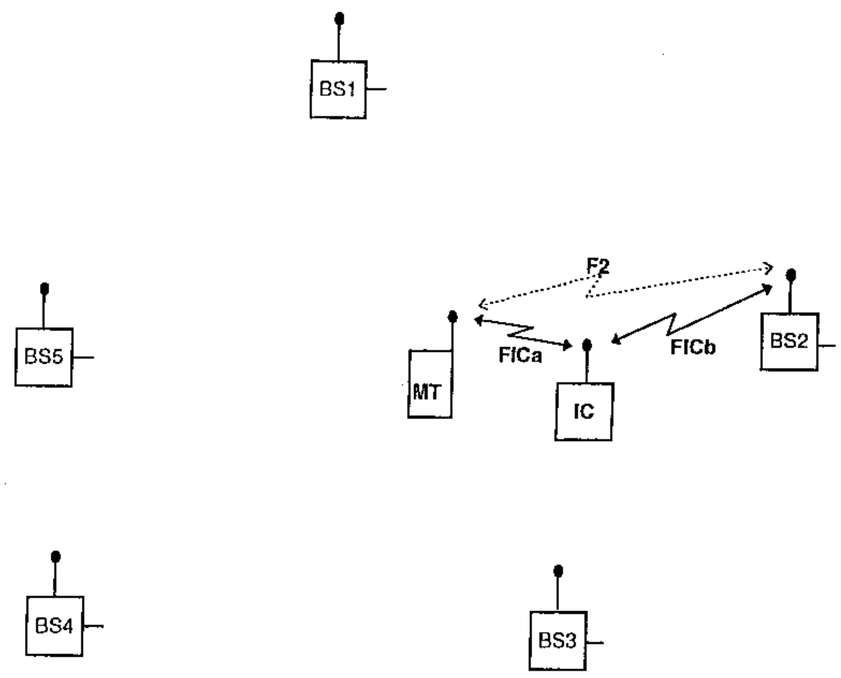
(21) (A1) **2,286,964**
(22) 1999/10/20
(43) 2000/04/23

(72) WILHELM, MICHAEL, DE
(71) ALCATEL, FR

(51) Int.Cl.[6] H04Q 7/34
(30) 1998/10/23 (198 48 915.3) DE

(54) **AMELIORATION DE LA PROTECTION DES TELEPHONES MOBILES CONTRE L'ECOUTE ELECTRONIQUE**

(54) **IMPROVING THE SECURITY OF MOBILE TELEPHONES AGAINST EAVESDROPPING**



(57) A method of detecting an eavesdropping device (IC) which is interposed between a mobile telephone (MT) and a base station (BS2) and which accepts, as a purported base station, a call from the mobile telephone (MT) and then forwards it, as a purported mobile telephone, to the base station (BS2) involves storing data of the base stations (BS1, ..., BS5) used by the mobile telephone (MT) in the mobile telephone (MT). When a new connection is set up to a base station (BS2), the data newly determined during this connection setup are compared with the data to be expected for this base station (BS2) in view of the stored data. If the data differ, an error signal is generated in the mobile telephone (MT). This error signal may initiate a release of the connection with this base station (BS2) or trigger an alarm message to the user. This improves the security of, e.g., GSM mobile stations against eavesdropping.

Abstract of the Disclosure

A method of detecting an eavesdropping device (IC) which is interposed between a mobile telephone (MT) and a base station (BS2) and which accepts, as a purported base station, a call from the mobile telephone (MT) and then forwards it, as a purported mobile telephone, to the base station (BS2) involves storing data of the base stations (BS1, ..., BS5) used by the mobile telephone (MT) in the mobile telephone (MT). When a new connection is set up to a base station (BS2), the data newly determined during this connection setup are compared with the data to be expected for this base station (BS2) in view of the stored data. If the data differ, an error signal is generated in the mobile telephone (MT). This error signal may initiate a release of the connection with this base station (BS2) or trigger an alarm message to the user. This improves the security of, e.g., GSM mobile stations against eavesdropping.

Improving the Security of Mobile Telephones against Eavesdropping

This invention relates to a method of detecting an eavesdropping device which is interposed between a mobile telephone and a base station and which accepts, as a purported base station, a call from the mobile telephone and then forwards it, as a purported mobile telephone, to the base station, as well as to a program module for carrying out this method and to a mobile telephone equipped with such a program module.

Telephoning with digital mobile telephones as are known from the GSM (Global System for Mobile Communications) is considered secure against eavesdropping, since all radio communications between a mobile telephone and a base station are encrypted. In an article entitled "Handys abhörsicher?", published in the journal c't 1998, No. 5, page 92, and in an article entitled "Aus der Luft gegriffen", published in the journal FOCUS, 38/1997, pages 220/221, eavesdropping devices, so-called IMSI catchers (IMSI = International Mobile Subscriber Identity) are described with which mobile telephone calls can possibly be intercepted after all.

These eavesdropping devices act vis-à-vis a mobile telephone like a base station of the mobile radio network. If the eavesdropping device is the strongest transmitter in the vicinity, the mobile telephone will use it as a base station during the next outgoing call. Since, during call establishment, each base station can determine how the radio communication will be encrypted, the eavesdropping device will choose the unencrypted mode. As the eavesdropping device is no genuine base station, it will log on to an adjacent base station as a purported mobile telephone and simply forward the intercepted call as if the latter originated from a mobile telephone.

From EP 0 822 726 A2 it is known to improve security in a radiocommunications network by storing the propagation delay between a fixed telephone and its serving base station at the base station. If the propagation delay measured during another call attempt differs from the stored propagation delay, the telephone will be denied access to the base station.

It is the object of the invention to provide a method of detecting the interposition of the above-described eavesdropping device, a program module for carrying out the method, and a mobile telephone equipped with such a program module.

To attain this object, the invention provides a method of the kind referred to at the beginning which is characterized in that characteristic data of the base stations used by the mobile telephone are stored in the mobile telephone, that when a new connection is set up to a base station, the data newly determined during

this connection setup are compared with the data to be expected for said base station in view of the stored data, and that if the data differ, an error signal is generated in the mobile telephone.

If the newly determined data differ markedly from the stored data as is the case for an interposed eavesdropping device, this error signal may trigger a visual, audible, or mechanical alarm message from the mobile telephone to the user, or the mobile telephone will change to another base station. This measure improves the security of, e.g., GSM mobile stations against eavesdropping. The alarm message can also be transmitted to a center, e.g. for further investigations, possibly using further alarm messages from other mobile subscribers to determine the exact geographical position of the eavesdropping device.

The characteristic data are preferably the propagation delays or the transmitting power assigned by the base station to the mobile telephone. Also, an unencrypted mode desired by the base station can be used as a trigger for the error signal. Further characteristic data could be, for example, the identity of the radio cells or base stations, the response times to enquiries, the geographical distance to the base station, and statistics about the calls conducted with the mobile telephone.

Preferably, these characteristic data are stored in dependence upon the distance between the mobile telephone and the base station so as to be able to interpolate characteristic data for intermediate distances.

If the characteristic data are stored in groups each relating to at least three base stations separated by a distance from each other, interdependent data, such as the propagation delays to the respective base station, can be obtained.

If the mobile telephone communicates a determined difference between the data together with information about its geographical position via the base station to a center, the latter, possibly using further messages received from other mobile telephones, can determine the exact geographical position of the eavesdropping device.

According to a further aspect, the invention also relates to hardware and software modules for carrying out the method described.

Further advantages of the invention are apparent from the following description and the accompanying drawings. According to the invention, the aforementioned features and the features described below can be used alone or in arbitrary combinations. While particular embodiments of the invention are described, it is to be understood that the description is made only by way of example and not as a limitation to the scope of the invention.

In the drawings:

Fig. 1 shows highly schematically a mobile radio network with several base stations, a mobile telephone, and an eavesdropping device;

Fig. 2 shows highly schematically the internal structure of the eavesdropping device of Fig. 1; and

Fig. 3 is an exemplary flowchart for a method carried out in accordance with a program module to detect the eavesdropping device and determine its geographical position using the mobile telephone.

Fig. 1 shows a mobile radio network with several base stations BS1 to BS5 and an eavesdropping device IC ("IMSI catcher"). This eavesdropping device IC acts vis-à-vis a mobile station or mobile telephone MT like a base station of the mobile radio network. In the embodiment shown it is assumed that the mobile telephone MT would have selected the base station BS2 as the strongest station for the establishment of a call over the radio link F2 if the eavesdropping device IC were not present or not active. Since the eavesdropping device IC is the strongest transmitter in the vicinity of the mobile telephone MT, however, the mobile telephone MT will use it as a supposed base station BS' (Fig. 2) during the next outgoing call. Accordingly, the link FICa to the eavesdropping device IC is established. Since during a connection setup each base station can determine how the radio communication will be encrypted, the eavesdropping device IC will select the unencrypted mode. Via a facility REC provided in the eavesdropping device IC, the conversation can then be listened to or recorded. Via the link FICb, the eavesdropping device IC will log, as a purported mobile telephone MT' (Fig. 2), on to the

adjacent base station BS2 and simply forward the intercepted call.

To improve the security against eavesdropping by means of such a device IC, the mobile telephone MT incorporates a hardware or software module that operates, for example, according to the flowchart shown in Fig. 3.

After a radio link has been established between the mobile station MT and a base station (step 1), characteristic data of this base station, such as propagation delays or the transmitter power assigned by this base station to the mobile telephone MT, are determined by the mobile telephone MT (step 2). These newly determined data are compared (step 3) in the mobile telephone MT with the data determined during previous connections with this base station, which were stored in the mobile telephone MT. If this comparison indicates that the newly determined data lie within permissible limits, these data will be stored in the mobile telephone MT (step 4) and the setting up of the connection between the mobile station MT and the base station will continue (step 5). The permissible limits used in step 3 may be preset or be determined using statistical functions, for example.

If, however, a significant difference between the newly determined data and the stored data is detected in step 3, an error signal will be generated and the program will branch to step 6, in which the mobile telephone MT determines its geographical position, absolutely or relative to the base station. This geographical position, together with the determined difference

between the data, is communicated via this base station to a center (step 7). There, the exact geographical position of the eavesdropping device IC can be determined based on this message, possibly together with further messages received from other mobile telephones. The mobile telephone MT will then release the connection with the base station (step 8) and establish a new connection to another base station. It is also possible for the user to receive an alarm message and then decide whether to release or maintain the connection.

In the embodiments of Figs. 1 and 2, the propagation delays between mobile telephone MT and base station BS2 are significantly increased by the combined radio link FICa and FICb via the interposed eavesdropping device IC. Therefore, the comparison with the shorter propagation delays determined during previous connections without an interposed eavesdropping device IC will indicate a marked difference, so that the connection will be released.

Patent Claims

1. A method of detecting an eavesdropping device (IC) which is interposed between a mobile telephone (MT) and a base station (BS2) and which accepts, as a purported base station (BS'), a call from the mobile telephone (MT) and then forwards it, as a purported mobile telephone (MT'), to the base station (BS2), c h a r a c t e r i z e d i n that data of the base stations (BS1, ..., BS5) used by the mobile telephone (MT) are stored in the mobile telephone (MT), that when a new connection is set up to a base station (BS2), the data newly determined during this connection setup are compared with the data to be expected for said base station (BS2) in view of the stored data, and that if the data differ, an error signal is generated in the mobile telephone (MT).

2. A method as claimed in claim 1, characterized in that the error signal initiates the release of the connection to said base station (BS2).

3. A method as claimed in claim 1, characterized in that the error signal triggers an alarm message to the user.

4. A method as claimed in claim 1, characterized in that as the data, propagation delays, and/or the transmitting power assigned by the base station (BS2) to the mobile telephone (MT), and/or the mode of encryption specified by the base station (BS2) are used.

5. A method as claimed in claim 1, characterized in that the data include the identities of radio cells and/or of the base stations.

6. A method as claimed in claim 1, characterized in that the data are stored in dependence upon the distance between the mobile telephone (MT) and the base station (BS2).

7. A method as claimed in claim 6, characterized in that the data are stored in groups each relating to at least three base stations separated by a distance from each other.

8. A method as claimed in claim 1, characterized in that the mobile telephone (MT) communicates a determined difference between the data together with information about its geographical position to a center.

9. A program module for carrying out the method claimed in any one of the preceding claims.

10. A mobile telephone (MT) comprising processor-controlled circuits for carrying out the method as claimed in any one of claims 1 to 8 and a program module as claimed in claim 9.

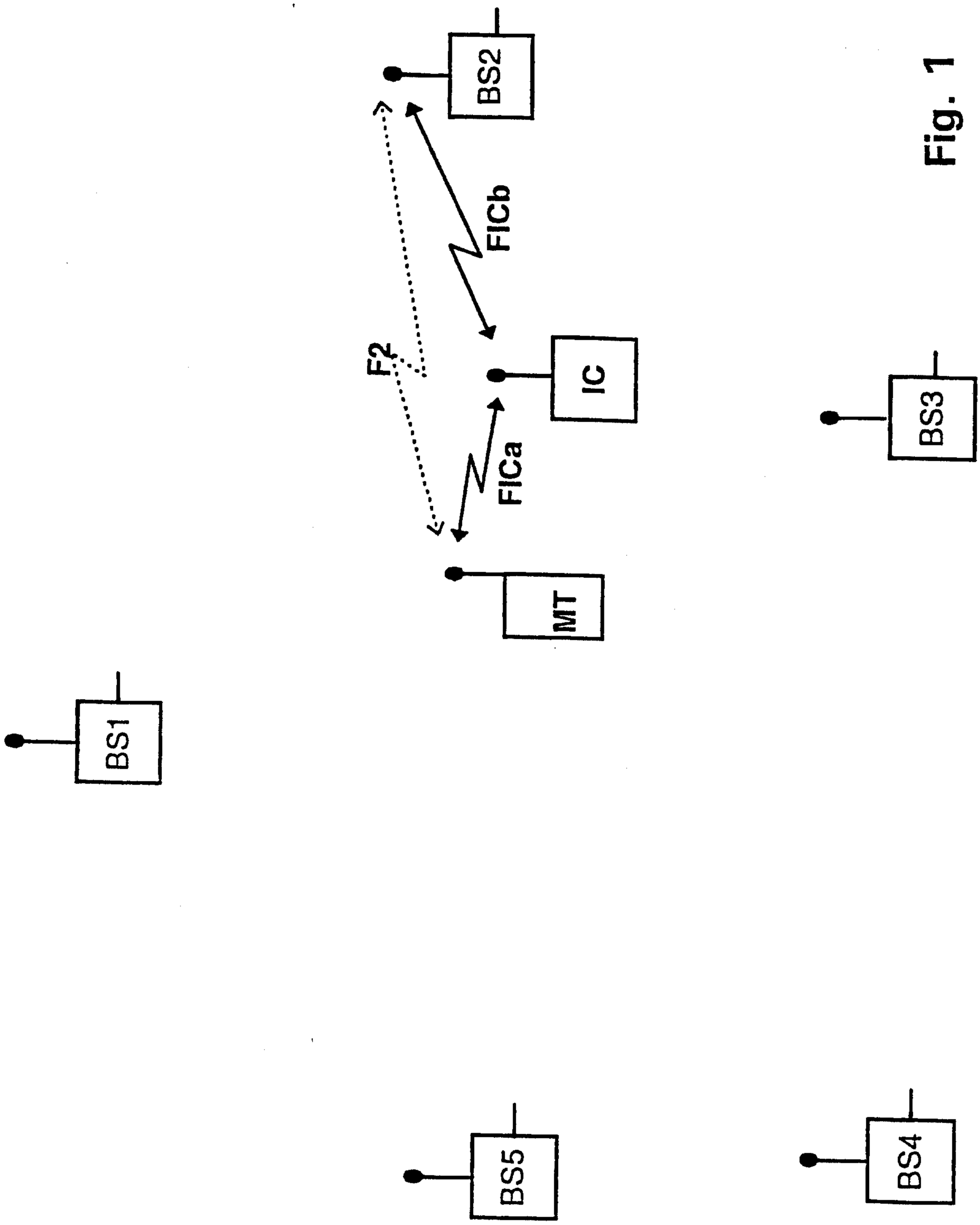


Fig. 1

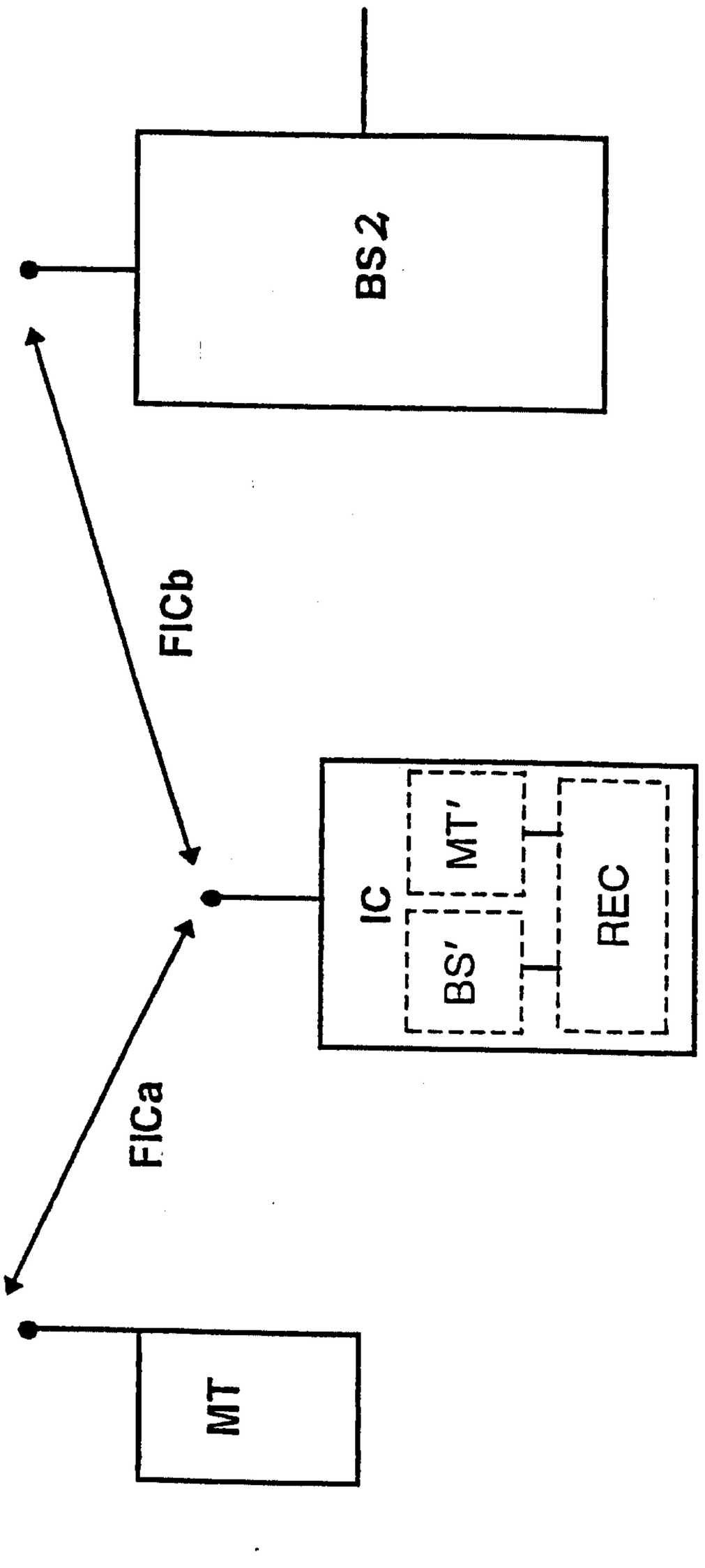


Fig. 2

Fig. 3