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

(11) EP 2 665 214 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
20.11.2013 Bulletin 2013/47

(51) Int Cl.:
H04K 3/00 *(2006.01)*

(21) Application number: **12167929.4**

(22) Date of filing: **14.05.2012**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(71) Applicant: **Gemalto M2M GmbH**
81541 München (DE)

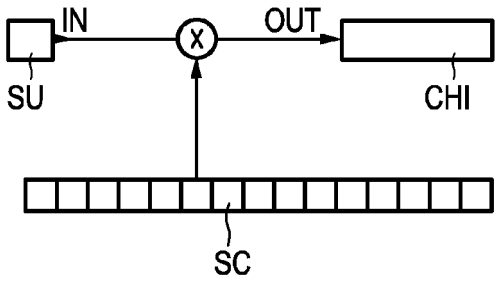
(72) Inventors:
- **Breuer, Volker**
  16727 Bötzow (DE)
- **Duchstein, Henrik**
  13158 Berlin (DE)

(74) Representative: **Eisenführ, Speiser & Partner**
Anna-Louisa-Karsch-Strasse 2
10178 Berlin (DE)

(54) Method of detecting a jamming transmitter affecting a communication user equipment,device and user equipment and system with the user equipment

(57) Method of detecting a jamming transmitter, affecting a communication user equipment, wherein said communication user equipment (UE) is adapted for communication with a component of a cellular radio network (RN) having a number of user equipments (UE) and a number of base stations (BNS) for communication in a communication band on a communication channel of predetermined frequency range, providing the user equipment (UE) in a start up mode for achieving a connected mode of a communication radiolink with the component of the radio network (RN), wherein in the start up mode of said user equipment (UE) it is determined that a connected mode of the communication radiolink cannot be established, and wherein jamming detection steps are provided.

FIG. 2



EP 2 665 214 A1

Description

[0001] The present invention relates to a method of detecting a jamming transmitter affecting a communication user equipment according to the preamble part of claim 1. The present invention also relates to a device configured to execute said method and a system of the device with the user equipment with interfaces to the user equipment and with an application, in particular to execute the method.

[0002] Contemporary cellular radio networks known since many years are now meanwhile based on different technologies. The broadest coverage still is held by the global system for mobile communications according to the so called GSM standard. A user equipment in such cellular network can move freely and may be handled over to various cells of the GSM networks as e.g. described in GSM standard specification 3GPP ETSI TS 51.010 or the like.

[0003] Contemporary radio networks are based on a cellular code division multiple access CDMA as e.g. realized in the universal mobile telecommunication system UMTS. Networks implementing these standards are increasingly important for security applications like camera systems or the like. Also other technologies are known for use in a cellular radio network like TDMA based technologies like WCDMA, HSPA, EV-DO or the like 3G-(UMTS) technologies; CDMA based technologies like IS-technologies or the like 2G, 3G technologies; and LTE or WiMax based technologies and the like 4G-technologies. Generally, a user equipment in radio networks can be subject of being affected by a jamming transmitter - jamming in this context generally is performed by an instrument preventing a user equipment from receiving signals from its base station. In use the jammer effectively disables cellular phones mostly by broad frequency interference with communication frequencies of the user equipment at high power level. Whereas some jammer applications are meant to be legal e.g in places where phone calls are to be suppressed due to silence conditions. Other jammers are applied during misuse e.g. to interrupt security applications of user equipment or the like. Jammers are available for jamming GSM- and also UMTS- and LTE- frequencies. However, jamming detecting and preventing solutions are known up to date basically only against GSM-jammers. In this regard, it should be recognized that primary aim of an anti-jamming solution is to undoubtedly detect a jamming attack; however, it is also desirable to prevent the same.

[0004] In WO2005/112321 a method for jamming detection in a GSM mobile telecommunications network is described comprising the steps of, at a user equipment registered with the mobile telecommunications network: a) measuring a signal power level in at least one of a plurality of communication channels between the user equipment and a base station within a band of operation of the mobile telecommunications network; b) checking whether the signal power level in said at least one communication channel is greater than a threshold MNPL and, if so, attempting to decode a Base Station Identity Code BSIC broadcast by the base station in said communication channel; c) repeating steps a) and b) for a certain number of channels; d) signaling a jammed condition report JDR message to the base station if said BSIC cannot be decoded for said number DCMN of channels. This method suffers from the fact that usually a signaling of a jammed condition report JDR message to the base station is not possible due to the jammed condition; thus the jammed condition remains unanswered.

[0005] An anti-jamming solution is known from WO 2007/019814 which however also is restricted to the GSM standard. Therein a method for detecting a jamming transmitter affecting a communication terminal is described wherein receipt radio channel signal levels are evaluated at periodic intervals on a signalling channel. In the case that the communication terminal detects a radio channel signal level that exceeds a predefined threshold value in the signalling channel but is nevertheless unable to decode a message content of a message, then this state is interpreted as an interference state and an alarm signal is emitted. The problem related with this GSM anti-jamming solution is its fundament on a predefined threshold value in the signalling channel and the receipt of a message content. These features are somewhat specific for the GSM technology, however, less suited in the UMTS technology. More specifically it turns out that an anti jamming solution in the frame of a cellular code division multiple access based radio network is much more demanding. The state of dealing with disturbances in a communication frequency band of a user equipment is more or less a usual state of operation for a user equipment within a cellular code division multiple access based radio network. In particular, intracell and intercell interferences are generally accepted in a CDMA based radio network as long as a signal can be decoded. Thus, the state of operation naturally is permanently disturbed due to the CDMA based technology.

[0006] The specific reason is as follows: a communication user equipment UE and a number of base node stations BNS are the basic components of a CDMA based radio network. The radio network RN may work in either a frequency division duplex FDD or also a time division duplex TDD mode. Once a communication link in a serving cell coverage area is provided between the communication user equipment and a serving base node station sBNS a communication signal unit SU is correlated with a pseudonoise spread code SC in a serving cell coverage area CA of a serving base node station and transmitted as a pseudonoise chip CHI in a multiple shared communication frequency channel. Thus, interferences of multiple base node stations and user equipments in the communication frequency channel are spectrally located between an upper frequency and a lower frequency of a communication frequency band. Consequently, a broad band "jamming like" interference in the multiple shared communication frequency channel can not be consid-

ered as an extraordinary event but is on the contrary part of the usual state of operation. Such situation may also occur each time the number of users changes in said frequency band. The similar situation may also occur when a user equipment has a comparatively large or a comparatively small distance to a base node station. Also a similar situation may occur when a user equipment is in the reach of two base node stations in particular vice versa when two user equipments belong to the same or neighbouring cells of the CDMA based radio network. In conclusion, an anti-jamming solution to be successfully implemented in a CDMA based radio network technology is more sophisticating.

[0007] In WO 00/62437 a concept for improving jammer detection sensitivity in a CDMA based communication network is provided wherein spectral analysis data are used to identify jamming signals having power spectral density characteristics which are distinguishable from those of legitimate subscriber transmissions in the wireless system's frequency band. By using several base stations located near the jamming transmitter, and by comparing the power spectral densities received at those base stations, the location of the jamming transmitter is estimated. Additionally, such spectral analysis data is used to detect aberrant receive spectrum characteristics which may indicate a hardware malfunction or failure. The spectral analysis uses a model of a real-input-data FFT and complex-input-data FFT for a CDMA signal bandwidth C of approximately 1.25 MHz and is based on the assumption that a jammer detection threshold will be set relative to a "noise floor", and it can be concluded that the jammer detection threshold will be the same for the two cases of a FFT. The (in-band) power spectral density P will be the same for either technique, with the power spectral density equaling P/C. But because the jammer power divided equally between a I and a Q branch, the jammer power will be 3dB less for the real-input-data FFT than in the case of the complex-input-data FFT.

[0008] Nevertheless, generally and as compared to the above mentioned GSM solution of WO 2007/019814 and WO2005/112321 a predefined threshold value for a signal level of a specific signalizing channel for a user equipment per se cannot be defined. Either the channel and/or the signal level is continuously changing depending on the surroundings of the network. Also, a message content as such can not be received unless a pseudonoise spread code is received by the communication user equipment. Consequently, without pseudonoise spread code neither transmission nor a content of a message is possible unless - the pseudonoise spread code is known to the user equipment.

[0009] In 3GPP TS 25.133 in Chapter 4.2.2.1 a measurement and evaluation of cell selection criteria S of a serving cell is described, wherein the user equipment shall measure the CPICH Ec/Io and CPICH RSCP level of the serving cell and evaluate the cell selection criterion S defined in 3GPP TS 25.304 ("UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode"). After a certain period a user equipment is considered to be "out of service area" and shall perform actions according to 3GPP TS 25.331("RRC Protocol Specification"). On transition of the user equipment to another cell and if a user equipment cannot find a suitable UTRA cell, then it is considered to be "out of service area" and shall perform actions according to 3GPP TS 25.331. Thus, in principle, if no suitable cell according to its power level is found, the user equipment shall be considered to be out of service. This procedure demands for measuring one or more power levels.

[0010] Although a jamming-detection concept can be advantageously also be based identifying contents of messages or on measuring power levels, primarily it is desirable to have an anti-jamming concept which is less dependent on sophisticated measurement of signal strength or power and thus is more reliable. In particular in a CDMA based radio network decoding and despreading procedures have to be taken into account when a comparison of power levels is taken as a basis for a jamming-detection and could be avoided. Also, all the above mentioned approaches suffer from the fact that a jamming situation can only be detected rather than prevented. However, jamming preventing solutions are highly desirable for UMTS and also LTE standards.

[0011] In this regard, it should be recognized that primary aim of an anti-jamming solution is to undoubtedly detect a jamming attack but nevertheless preventing the same shall be possible as well. At least a rather early detection of a jamming attack can help to prevent the same. Usually, jamming results in a user equipment loosing connection to the base station; thus camping of an user equipment in the certain cell is no more possible. Technically speaking, the user equipment falls back from a connected mode to an idle mode. The above jamming approaches have the aim to detect a jamming situation only in the idle mode. It is known e.g. that the idle mode still preserves certain operations as the user equipment is still registered in the radio network, that is when the user equipment (UE, also referred to as a mobile station MS) is switched on but has no dedicated channel allocated. Thus, the mobile station is not able to make or receive a call. In particular certain idle mode tasks are still possible to provide a radio subsystem link control. As outlined above, a jamming detection in the idle mode is rather late and thus limits the chances to prevent a jamming situation.

[0012] Also, when --at a later time T2-- the ability to receive a signal or camp on a cell is broken, it can only be guessed, what had been the exact status and communication conditionsat an earlier time T1-- prior to the jamming occurred, i.e. at a time T1 where the UE/MS was synchronized to a cell or received a certain message, thus camping on a cell has been possible. Still, comparing the overall received signal conditions of e.g. the unbiased power for later time instants, might indicate that a power is high but the ability to decode or receive a certain ded-

icated signal or common signal transmitted by a BTS (in GSM) or nodeB station (in CDMA) is not decodable. Hence the result of this comparison can lead to the indication of jamming detection.

[0013] Nevertheless in certain circumstances a mobile phone, module or M2M device needs to switch off its receiver/radio frequency (RF) front-end, e.g. if carried by an aircraft. Furthermore it needs to be noted that a similar situation could occur, once an M2M device is switched on for the first time. Hence, after switching on a receiver of an user equipment and when the user equipment is pending a while in the idle mode and then synchronization to a cell is not achieved --although sufficient power for a suitable cell is detected-- still no jamming indication can reliably be provided; an undisturbed measurement or threshold required in principle in the jamming detection algorithms, still is missing. The lack of a mere power reference measurement at least partially precludes the usage of the above mentioned jamming algorithms. Indicating jamming indeed could be misleading when de facto a power level above a suitable level for the technology used by the M2M device is detected, but said band or channel would belong to a not supported technology or a technology not supported in that band by the device. I.e. in a search, when finding a band with high power and being unable to detect or decode an associated communication technology by the UE itself; when this is the only available information, using jamming detection algorithms is not sufficient for so far to indicate a jamming situation reliably. A solution for the above mentioned problem in general, is in particular neither for leaving an airplane mode and/or a temporary receiver inactivity nor for the first activation, known yet.

[0014] This is where the invention comes in, the object of which is to provide an improved method of detecting a jamming transmitter affecting a communication user equipment wherein the communication user equipment and a number of base node stations are adapted to be components of a cellular radio network like e.g. frequency division duplex or time division duplex mode or GPRS cellular radio network. In particular it is an object of the invention to provide a method of detecting a jamming transmitter rather early, in particular prior to the user equipment falling back into the idle mode. A further object of the invention is to provide an improved communication module, in particular user equipment, adapted to execute the method of detecting a jamming transmitter affecting the communication user equipment, in particular to detect the jamming situation already whilst the communication user equipment is in a start up mode. In particular the method and the communication module shall be adapted to detect a jamming warning before a jammed situation is to be accepted; in particular it shall be discriminated between an out of service state of the user equipment and a jamming warning situation. It is still another object of the invention to provide such method and device with a more elaborated anti-jamming concept allowing also detection of a jamming transmitter on a broad frequency range. In particular it is an object of the invention to provide an effective and reliable method and device for detecting a jamming transmitter affecting a communication user equipment and while nevertheless being less dependent on sophisticated measurement of signal strength or power.

[0015] As regards the method, the object is achieved by the method of the invention as claimed in claim 1.

[0016] As regards the device, the object is achieved by particular preferred development of the user equipment as claimed in claim 16.

[0017] A communication user equipment UE is adapted for communication with a component of a cellular radio network RN having a number of user equipments UE and a number of base node stations BNS. Preferably the cellular radio network RN provides a synchronization channel SCH for synchronization of the user equipment UE to a cell of the cellular radio network RN, and wherein the detection device is provided in the neighborhood or part of the user equipment. Said communication user equipment UE and a number of base node stations BNS are components of a cellular radio network RN, in particular in a code division multiple access CDMA based radio network (like a frequency division duplex FDD or time division duplex TDD mode) or a GPRS or LTE network.

[0018] Preferably a pseudonoise spread code SC is for spreading a communication signal unit SU and a synchronization of the user equipment UE to a cell of the cellular radio network RN is determined during a cell search from a synchronization channel according to a 3G technology or other synchronization is provided in a GPRS or the like 2G technology. In particular the cellular radio network RN provides a synchronization channel SCH for synchronizing and a dedicated channel DCH for communicating, for a communication radiolink of the user equipment UE to a cell of the cellular radio network RN and the user equipment UE is in a start up mode of a communication radiolink. Preferably the start up mode comprises a synchronization mode and the communication radiolink is on a dedicated channel DCH and synchronization cannot be established and/or a dedicated channel DCH cannot be established.

[0019] Preferably a jamming detection device is provided in the neighborhood or part of the user equipment.

[0020] The invention starts from the consideration that the user equipment per se and without further measures cannot distinguish between a normal mode frequency disturbance due to interferences originating from the CDMA system as outlined in the introduction on the one hand and a loss of service availability due to external disturbing factors which in the specific situation usually cannot be fixed. Basically this also holds for all technologies in the start of a start up mode of a user equipment when there is no reference for orientation. Basically for detecting a jamming transmitter affecting a communication user equipment and while nevertheless being less dependent on sophisticated measurement or compari-

son of signal strength or power the invention provides an alternative concept for nevertheless actively and reliably detecting a jamming situation even in a start up mode is suggested.

[0021] The instant concept of jamming detection and/or warning according to the invention is based on providing the user equipment UE in a start up mode of a communication radiolink with the component of the radio network RN. In the start up mode of said user equipment (UE) it is determined that a connected mode of the communication radiolink cannot be established.

[0022] Thus, according to the invention in the start up mode of said user equipment UE the steps are provided:

- measuring a power level in the radiolink at least at the predetermined frequency range, in particular in at least the band and/or channel, and determining whether the power level is above a threshold level to establish a communication link.

[0023] On the other hand, preferably, measuring a power level in the radiolink, in particular a band and/or channel, and determining whether the power level is below a threshold level to establish a communication link can be used for providing an out-of-service indication.

[0024] Further, according to the invention in the start up mode of said user equipment UE the steps are provided:

- receiving a location information with regard to a position of the communication user equipment;
- receiving a coverage information of deployment of radio network at the position;
- indicating a jamming transmitter in case the coverage information is positive with regard to the supported communication capability of the user equipment at the position of the communication user equipment.

[0025] The invention starts from the consideration that the problem of jamming detection due to the lack of an undisturbed earlier or other reference signal can be transferred into another problem. Namely the invention recognized that the signal measured during a start up mode (also referred to as idle mode) leading to an unsuccessful connection attempt-although power which is detected should be sufficient for connection-

- may be due to jamming
- or just the case of being in a location where the technologies supported by the UE are not deployed, i.e. an out-of-service (OOS) situation.

[0026] Hence in that situation it is rather a location determination problem e.g. the question is to be answered: Is a GSM mobile in Europe and currently jammed or in Japan where GSM is not deployed?

[0027] In short terms, the invention follows in general to combine the measurement on the power distribution in the received band being unable to decode, with location information compared to a stored list on the deployment of the technologies supported. Hence, if energy is detected in a band and the band is designated to GSM in that area e.g., it is likely that the M2M device is interfered, i.e. jammed.

[0028] The method and developed configurations thereof as outlined above may be implemented by digital circuits of any preferred kind, whereby the advantages associated with the digital circuits may be obtained. In particular one or more method steps or features of the method can be implemented by one or more means for functionally executing the method step. A single processor or other unit may fulfil the functions of several means recited in the claims - this in particular holds for a user equipment according to the concept of the invention. The concept also leads to a computer program product storable on a storage device and adapted for executing the method when executed on a device. The units of Power Spectral Density (PSD) are extensively used in this document. PSD is a function of power versus frequency and when integrated across a given bandwidth, the function represents the mean power in such a bandwidth- this holds generally for GSM and CDMA. When the mean power is normalized to (divided by) the chip-rate it represents the mean energy per chip, which is specific for CDMA. Some signals are directly defined in terms of energy per chip, (DPCH_E_c, E_c, OCNS_E_c and S-CCPCH_E_c) and others defined in terms of PSD (I_o, I_{oc}, I_{or} and $\hat{I}_{or}$). There also exist quantities that are a ratio of energy per chip to PSD (DPCH_E_c/I_{or}, E_c/I_{or} etc.). This is the common practice of relating energy magnitudes in communication systems and can be used related to channels for both GSM and CDMA based technologies; a channel or chip related PSD is also referred to as a biased energy, whereas the total wide power at an antenna is referred to as unbiased power.

[0029] It can be seen that if both energy magnitudes in the ratio are divided by time, the ratio is converted from an energy ratio to a power ratio, which is more useful from a measurement point of view. It follows that an energy value per chip of X dBm/3.84 MHz can be expressed as a mean power per chip of X dBm. Similarly, a signal PSD of Y dBm/3.84 MHz can be expressed as a signal power of Y dBm.

[0030] E.g. DPCH - Ec/Io is the ratio of the transmit energy per PN (pseudonoise) chip of the DPCH (dedicated physical channel) to the total transmit power spectral density at the NodeB antenna connector. Ec/Io is the ratio of the average transmit energy per PN chip for different fields or physical channels to the total transmit power spectral density at the Node B antenna connector.

[0031] In general terms for 3G and 2G e.g. the Ec (respectively RSCP)/ **Io** (respectively RSSI - total receive

power) is the received energy per chip divided by the power density in the band. 'Io' includes the power of specified cell as it indicates total receive power. As a result, Ec/Io is deteriorated by increasing 'Io'.

[0032] The concept of the invention also leads to a device for a user equipment, in particular device reportingly connectable to an application layer, configured to execute the method of detecting a jamming, affecting the communication user equipment in a start up mode, wherein the detection device has

- a power measuring unit adapted for measuring a power level in the radiolink at least at the predetermined frequency range, in particular in at least the band and/or channel, and determining whether the power level is above a threshold level to establish a communication link;

- a receiving unit adapted for receiving a location information with regard to a position of the communication user equipment and adapted for receiving a coverage information of deployment of radio network at the position;

- a comparator for indicating a jamming transmitter in case the coverage information is positive with regard to the supported communication capability of the user equipment at the position of the communication user equipment.

[0033] The concept also leads to a system of the device and a communication user equipment (UE) adapted for communication with a component of a cellular, in particular code division multiple access (CDMA) and/or TDMA and/or LTE and/or GPRS based, radio network (RN) having a number of user equipments (UE) and a number of base node stations (BNS), in particular wherein the cellular radio network (RN) provides a synchronization channel (SCH) for synchronizing and a dedicated channel (DCH) for communicating, for a communication radiolink of the user equipment (UE) to a cell of the cellular radio network (RN) and the user equipment (UE) is in a start up mode of a communication radiolink, preferably wherein the detection device is provided in the neighborhood or part of the user equipment.

[0034] These aspects of the invention and further developments thereof are further outlined in the dependent claims. Thereby the mentioned advantages of the proposed concept are even more improved. In particular several methods to serve as example for different ways to retrieve the position location with or without additional measurement are described.

[0035] Particular preferred the start up mode is an idle mode. Most preferably the start up mode also comprises a synchronization mode. The communication radiolink is preferably on a dedicated channel (DCH). In particular when a connected mode of the communication radiolink cannot be established synchronization cannot be established and/or a dedicated channel (DCH) cannot be established.

[0036] In a particular preferred development one or more good-reference parameters are provided for indicating that the communication user equipment UE is capable of communicating in the cellular radio network RN by means of a communication indicator as further parameter.

[0037] Particular preferred is that the location information comprises determining a position of the communication user equipment. In particular determining comprises measuring or estimating. In particular receiving a coverage information of deployment of radio network at the position comprises receiving information with regard to a specific location like a sub-way or the like out-of-service (OOS) location. Preferably receiving a coverage information of deployment of radio network at the position comprises information about a communication technology deployed, preferably from a stored data item, like e.g. a stored list or the like.

[0038] According to a preferred development the further steps are provided:

- measuring the radiolink at least of predetermined frequency range by providing a power distribution of the radiolink at least of predetermined frequency range,

- analyzing the power distribution in terms of a characteristic item of the power distribution indicative of at least the predetermined frequency range.

[0039] In a particular preferred development thus the device for a user equipment further comprises:

- a link measuring unit adapted for measuring the radiolink at least of predetermined frequency range by providing a power distribution of the radiolink at least of predetermined frequency range,

- an analyzing unit for analyzing the power distribution in terms of a characteristic item of the power distribution indicative of at least the predetermined frequency range.

[0040] Also preferably in the method the steps are provided;

- retrieving a characteristic feature of a position related undisturbed power distribution of at least the predetermined frequency range, wherein

- the characteristic feature is associated with the analyzed characteristic item of the measured power distribution at the measured position, and

- comparing one or more characteristic features and associated characteristic items and verifying wheth-

er they do not correspond at least in a significant degree and in case of non-correspondence, indicating a jamming transmitter.

[0041] Accordingly the device for a user equipment further comprises preferably comprises:

- a location measuring unit adapted for measuring a position of the communication user equipment and retrieving a characteristic feature of a position related undisturbed power distribution of at least the predetermined frequency range, wherein
- the characteristic feature is associated with the analyzed characteristic item of the measured power distribution at the measured position; and
- a comparator adapted for comparing one or more characteristic features and associated characteristic items and verifying whether they do not correspond at least in a significant degree and in case of non-correspondence, indicating a jamming transmitter.

[0042] The power distribution is preferably a frequency related power distribution wherein preferably the item and feature is frequency related.

[0043] Preferably in a first aspect of development the radiolink is measured for at least predetermined frequency range of one or more bands and/or channels and the power distribution is analyzed at least in the predetermined frequency range across a number of separate bands and/or channels. More particular measuring the radiolink provides an unbiased power distribution across available communication bands and/or channels of the, in particular entire, supported antenna range. This approach is rather easy to be implemented and can form the basis for a certain variance analysis of e.g. generally available bands and/or channels due to the separation of bands and/or channels. Preferably the item is a variance of separate bands and/or channels and analyzing the unbiased power distribution is in terms of a variance of separate bands and/or channels.

[0044] Preferably in a first aspect of development the radiolink is measured for at least predetermined frequency range of one or more bands and/or channels and the power distribution is analyzed at least in the predetermined frequency range inside of at least one band and/or channel. More particular measuring the radiolink provides a biased power distribution in a supported communication band and/or channel of the communication radiolink. This approach is particular reliable as also biased band jammers can be detected. Preferably the item is a shape like a dip, a width, a steepness and the like item of distribution in the band and/or channel and analyzing the biased power distribution is in terms of a said shape and the like item of distribution in the band and/or channel. Also a characteristic feature and/or item can be additionally or alternatively a technology parameter like a statement of technology supported frequencies relative to a position of the user equipment.

[0045] Measuring the radiolink can be provided preferably for one or more additional technology relevant parameters, wherein the technology is selected from the group comprising:

- GSM based technologies like GPRS, EDGE and the like 2G-technologies,
- TDMA based technologies like WCDMA, HSPA, EV-DO or the like 3G-(UMTS)technologies,
- CDMA based technologies like IS-technologies or the like 2G, 3G technologies,
- LTE or WiMax based technologies and the like 4G-technologies.

[0046] A characteristic feature of a technology can be retrieved from a preloading, stored, downloaded, or in-use collected or the like gathered undisturbed power distribution, in particular in a list or the like look-up-table. In particular a characteristic feature and/or item can be a shape like dip, width, steepness and the like and/or technology parameter like a binary statement of technology supported frequencies relative to a position of the user equipment.

[0047] Preferably measuring a position of the communication user equipment provides for at least estimating, in particular identifying, a location of the user equipment, in particular by one or more of software, hardware or MMI measures, in particular selected from the group comprising of: MMI input, GPS module, cell measurement, signaling run time or interference or the like measurement adapted to provide some indication to an actual position of the user equipment e.g. also those exemplified in the detailed description.

[0048] For a more complete understanding of the invention, the invention will now be described in detail with reference to the accompanying drawing. The detailed description will illustrate and describe what is considered as a preferred embodiment of the invention. It should of course be understood that various modifications and changes in form or detail could readily be made without departing from the spirit of the invention. It is therefore intended that the invention may not be limited to the exact form and detail shown and described herein, nor to anything less than the whole of the invention disclosed herein and as claimed hereinafter. Further the features described in the description, the drawing and the claims disclosing the invention may be essential for the invention considered alone or in combination. In particular, any reference signs in the claims shall not be construed as limiting the scope of the invention. The wording "comprising" does not exclude other elements or steps. The wording "a" or "an" does exclude a plurality. Whereas in the following the concept of the invention is exemplifying de-

scribed by using the example of a CDMA based cellular radio network and terminology assigned thereto, it should nevertheless be understood that the general concept as claimed is not restricted to a specific technology but, also not explicitly mentioned in the example, embraces also other kinds of technologies like GSM, LTE or the like.

[0049] In the drawing:

Fig. 1 shows a simplified symbolic graphic of a structure of a CDMA based radio network as an example; nevertheless it should be understood that the graphic in other form also basically holds to address the start up (idle mode) and jamming situation with regard to a GSM or LTE based technology;

Fig. 2 is a graphic illustrating the correlation of a pseudonoise spread code SC with a communication signal unit SU to provide a pseudonoise chip CHI in a multiple shared communication frequency channel of a CDMA based radio network;

Fig. 3 a flow diagram illustrating the concept of the invention, wherein a preferred combination is exemplified of on the one hand a measurement on the power distribution in the received band unable to be decoded and on the other hand with a location information compared to a stored list on the deployment of the technologies supported;

Fig. 4 a scheme of a module for illustrating the concept of the invention on a device.

[0050] Fig. 1 shows in principle a cellular code division multiple access CDMA based radio network RN. The radio network RN allows for several transmitters - here referred to as a user equipment UE - to send information simultaneously over a single communication channel. This allows several user equipments UE to share a bandwidth of different frequencies. The CDMA based network can employ a spread spectrum technology and a special coding scheme - e.g. a frequency division duplex FDD or time division duplex TDD mode can allow multiple users to be multiplexed over the same physical channel. The spread spectrum signalling has a much higher data bandwidth than the data being communicated. The CDMA based radio network RN provides a set of at least one base node station - here e.g. the serving base node station sBNS and the further base node station BNS, which are within reach of the user equipment UE. E.g. a communication link 1 in a serving cell #1 coverage area CA1 of the sBNS#1 is provided between the communication user equipment #1 and the assigned serving base node station sBNS#1. As the user equipment UE#1 is also in the cell coverage area CA2 of the base node station BNS#2, the base node station BNS#2 and the serving base node station sBNS#1 form an active set of base node stations, which are both in reach of the user equipment UE#1. In the present embodiment the sBNS#1 has the strongest communication link 1.

[0051] The communication link 1 is adapted for transmitting a signal comprising multiple communication signal units SU between the communication user equipment UE#1 and the serving base node station sBNS#1. As exemplified in Fig. 2A the communication signal unit SU forms the input of a spreading code operation, wherein the signal unit SU is correlated with a pseudonoise spread code sSC in the serving cell coverage area CA1 of the serving base node station sBNS#1. The output signal of the spreading code operation is a so called pseudonoise chip CHI formed by the spreading encryption manipulating the original signal unit SU by means of the serving spreading code sSC. This can be performed either by an additive or multiplicative or other modified spreading operation as in principle known in the art.

[0052] As a result, the pseudonoise chip CHI is transmitted in a multiple shared communication frequency channel as indicated in the communication link 1 of Fig. 1 and can be transmitted or received by the user equipment UE#1 only when the serving pseudonoise spread code sSC is known by the user equipment UE#1. Once, the spreading code SC, i.e. the pseudonoise spread code is known, a signal unit can be received or transmitted by the user equipment UE#1.

[0053] The pseudonoise spread code SC is received by the communication user equipment UE#1 as a serving pseudonoise spread code sSC as shown in Fig. 1 in a so called serving downlink channel sCPICH. The CPICH contains 150 bit in one UMTS radio frame, which are either all zeros or in the case that space time transmit diversity is employed is a pattern of alternating ones and zeros for transmissions on the sBNS second antenna. The first antenna of a base node station always transmits all zeros for a CPICH. The CPICH downlink channel has a constant power and is of a known bit sequence. Its power is usually between 5 % and 15 % of the total BNS transmit power. A common CPICH power is of 10 % of the typical total transmit power of 43 dBm. The CPICH can be used for measurements of signal quality.

[0054] As outlined in 3GPP ETSI TS25.214 during the cell search, a user equipment UE searches for a cell and determines the downlink spreading code and frame synchronization of that cell. The cell search is typically carried out in three steps:

Step 1: Slot synchronization

Step 2: Frame synchronization and code-group identification

Step 3: Spreading-code identification

[0055] During the third and last step of the cell search procedure, the UE determines the exact primary spread-

ing code used by the found cell. The primary spreading code is typically identified through symbol-by-symbol correlation over the CPICH with all codes within the code group identified in the second step. After the primary spreading code has been identified, the Primary CCPCH can be detected. And the system- and cell specific BCH information can be read. If the user equipment UE has received information about which spreading codes to search for, steps 2 and 3 above can be simplified. Once the spreading code for a CPICH is known, the channel can be used for measurements of signal quality, usually with RSCP and E_c/I_0 as will be shown below. Timing and phase estimations can also be made, providing a reference that helps to improve reliability when decoding other channels from the same Node B.

[0056] In the UMTS cellular communication system, received signal code power RSCP denotes the power measured by a receiver on a particular physical communication channel. It is used as an indication of signal strength, as a handover criterion, in downlink power control, and to calculate path loss. In CDMA systems, a physical channel corresponds to a particular spreading code, hence the same. While RSCP can be defined generally for any CDMA system, it is more specifically used in UMTS. Also, while RSCP can be measured in principle on the downlink as well as on the uplink, it is only defined for the downlink and thus presumed to be measured by the UE and reported to the Node B.

[0057] In the instant embodiment, a jammer affects the user equipment UE#1 by interfering with the multiple shared communication frequency channel as located in a communication frequency band. Frequency bands FB I to XIX are known in the UMTS standard, each having a bandwidth of approximately 60MHz. Each frequency band comprises several communication frequency channels, each having a bandwidth of 5 MHz. For each frequency channel, therefore the noise floor of approximately -110 dBm can be defined based on a relative noise floor of -174 dBm/Hz. With this noise floor of -174 dBm/Hz integrated via the bandwidth of 5 MHz (66dB) one can calculate -174 dBm/Hz * 5MHz = - 174 dBm + 66 dB - 110 dBm.

[0058] A staple power for an out of jamming region user equipment UE#10 is a piled up staple with a rather small amount of CPICH power, a larger amount of signal code power dedicated to the user equipment and a main portion of shared signal power. The latter is used by several user equipments in the same 5 MHz bandwidth of the communication frequency channel. Nevertheless, information can be retrieved for each user equipment according to the pseudonoise spread code provided by the serving base node station and also the further base node station to each of the user equipments.

[0059] Once the number of user equipments changes in a coverage area CA1 of the service base node station 1 the shared signal power may vary rather often. However, as the serving pseudonoise spread code SSC is available for the user equipment UE#10 even upon variation of the shared signal power, user equipment UE#10 can uphold the communication link to the serving base node station sBNS#1. The reason for this is that even upon variation of the shared signal power nevertheless the CPICH power can be detected by the user equipment UE#10. The CPICH power normally is located not more than 24 dB below the upper level of the staple power. Thus, due to the spread code gain (sf=256) value of ideally not less than CPICH_Ec/Io=-24dB power and pseudonoise spread code SC can be detected by the user equipment UE#10 during normal operation. Considering real implementations the standard TS 25.133 requires values of CPICH_Ec/Io not less than -20dB.

[0060] In the case the distance between serving base node station sBNS#1 and user equipment UE#10 is diminished like e.g. the distance between sBNS#1 and UE10 the cell selection criteria power parameters Ec/Io ratio --in the standard denoted as CPICH Ec/Io as well as the received signal code power CPICH RSCP will increase-- thus overall the signal quality will increase. However, in the case the distance between UE#10 and sBNS#1 is enlarged - e.g. by moving to UE#20 - the biased parameter Ec/Io, i.e. ratio CPIHC Ec/Io and the received signal code power CPICH RSCP of the sBNS#1 will decrease but instead of those of the BNS#2 will increase. Thus, upon a situation, the soft-handover may occur between sBNS#1 and BNS#2 by moving UE#10 to UE#20. This situation is described e.g. in 3GPP TS25.133.

[0061] Distinct from those normal operation interferences in the communication frequency channels is the situation shown in Fig. 1 due to the presence of a jammer J.

[0062] The presence results in a user equipment UE#1 received staple power. Additional to the CPICH power the dedicated signal code and the shared signal power a large pile of jamming power on top of the staple power is detected by UE#1. The CPICH power therefore is not anymore in the spread code gain and consequently cannot be detected anymore. This situation is to be distinguished from the out of range situation as described in TS25.133 chapter 4.2.2.1. Namely, in the presently described situation of Fig. 1 the biased parameters are not detectable whereas the unbiased parameters have increased. The increase is due to the jamming power of jammer J. In the "out of service area" situation the unbiased parameters decrease as the biased parameters also decrease.

[0063] In principle this situation can be used to detect a jamming transmitter affecting the user equipment UE#1 when also an unbiased received wideband power within the bandwidth of the communication user equipment receiver at the communication user equipment UE#1 antenna connector is measured. Upon verifying the condition that the biased parameters --namely the Ec/Io and RSCP-- are not detectable and the unbiased parameter RSSI has increased a first indication of a jamming transmitter is given.

[0064] However, this demands for comparison of power levels of different points of time; namely before and after the jamming situation. However, due to the timespan in between the different points of time the user equipment UE#1 may have fallen back into the idle mode and thus loosing the communication link cannot be prevented anymore. Also in a start up mode no earlier reference is available. According to the concept of the invention this situation can be used already to provide an effective concept of detecting a jamming transmitter affecting the user equipment UE#1 without detecting and comparing power levels.

[0065] In particular according to the concept of the invention detection of a jamming situation is possible in a start up mode of the user equipment, said communication user equipment UE is adapted for communication with a component of a cellular code division multiple access CDMA based radio network RN having a number of user equipments UE and a number of base node stations BNS.

[0066] As a rather simple prerequisite it can be made sure, that the user equipment indeed is in a UMTS communication modus and the received signal strength is a signal of a CDMA based radio network. Here it is verified whether a respective UMTS communication indicator is set. E. g. a UMTS communication indicator can be on hold by means of a binary value stored or some setting of a user equipment which is indicative that the user equipment is capable and in reach of a UMTS communication signal. However, this might not be available. More importantly, as described in 3GPP TS 25.124 Chapter 4.3 in detail, for the dedicated channels DCH, synchronisation primitives are used to indicate the synchronisation status of radio links, both in uplink and downlink. However such primitive might also be not executable or may not work due to jamming in the start up phase.

[0067] The concept starts from the consideration that the problem of jamming detection due to the lack of an undisturbed earlier or other reference signal can be transferred into another question/problem. Namely the invention recognized that the signal measured during a start up mode, in particular idle mode, leading to an unsuccessful connection attempt-although power which is detected should be sufficient for connection may be due to jamming or just the case of being in a location where the technologies supported by the UE are not deployed (out-of-service OOS). Hence in that situation it is rather a location determination problem i.e. the question: is a GSM mobile in Europe and currently jammed or in Japan where GSM is not deployed ? In short terms, the invention follows in general to combine the measurement on the power distribution in the received band being unable to decode, with location information compared to a stored list on the deployment of the technologies supported. Hence, if energy is detected in a band and the band is designated to GSM in that area e.g., it is likely that the M2M device is interfered/jammed.

[0068] Besides the example named the concept generally embraces the general combination of a method for positioning in conjunction with measurements/decoding attempts on UE receiver bands to evaluate whether said radio bands are disturbed by purpose hence the so called jamming to prevent said mobile from connection loss. The jamming detection method of this approach is exemplified with regard to the following Fig. 2 for combination of these aspects.

[0069] Fig. 2 shows a flow chart wherein in step S1 a communication user equipment UE is provided without powering such that in principle it is connectable to a cellular radio network RN as depicted in Fig. 1 once powered. The communication in the network thus in principle can be accomplished in a communication band on a communication channel for a predetermined frequency range, namely the frequency range of a dedicated channel DCH e.g.. In step S2 the communication user equipment is in a switched off state UE RX off. This state usually occurs once the user equipment has been switched off, namely a power source of the user equipment has been disconnected or switched off. This sometimes is provided during night times or when the user equipment resides on an airplane or another location where no transmission is necessary or allowed. In step S3 the user equipment is switched on, this means a power source of the user equipment is connected to a receiver of the antenna of the user equipment. Thereby the user equipment begins to work through the procedural steps of a start up mode in order to arrive at an idle mode and for finally achieving a connected mode of a communication radio link with the component of the radio network. In step S4 a band and/or channel search is started as one procedural step of the start up mode, wherein all frequency bands for communication --as far as allowed by the capability of the user equipment-- are scanned by the receiver. In particular, in the example given in Fig. 1 the available communication frequency bands may comprise all UMTS communication frequency bands FB I to XIX. However, depending on the capability of the user equipment, further bands may be scanned within other technologies than the UMTS technology, e.g. GPRS or LTE technology related frequency bands and/or channels may be scanned. This is in particular the case when, e.g., the user equipment relies on a combination of UMTS and GMS and a LTE technology.

[0070] A communication frequency of a synchronization channel and/or dedicated channel in the end is spectrally located between an upper frequency and a lower frequency of a communication frequency band, e.g. a frequency band FB I to XIX as it is basically known for the UMTS standard. The bands lie in the range of between 700 MHz to 2700 MHz; in the European Union e.g. a frequency band I at 2100MHz is provided. The band provides a duplex distance for uplink and downlink channel of 190 MHz and provides a sequence of channels of 60 MHz width. Thus, each duplex channel has a 5 MHz width in a band. In LTE the number of duplex channels increases and each has a width of 10 or 20 MHz. The data rates in such kind of rather broad frequency chan-

nels in UMTS standard are meanwhile upgraded according to HSDPA or HSUPA. Longer term developments of UMTS to 4G-speed increase for downlink to of 100 Mbits/sec and 50 Mbits for uplink.

[0071] Once a band and/or channel is successfully allocated by the user equipment, the synchronization process to a respective cell at the location of the user equipment starts, as indicated above; the typical cell synchronization and code identification is provided in step S5. If this step is successful in the YES-path the user equipment in step S6 can turn to normal operation which means the user equipment is in idle mode and once a dedicated channel e.g. a dedicated channel DPCCH for voice or a dedicated data channel DPDCH for a data transfer is synchronized, the user equipment is connected mode.

[0072] However, in the case, one or more steps of the synchronization procedure to a synchronization channel and/or a dedicated channel fails in step S5, then according to the concept of the invention it is determined that a connected mode of a communication radio link cannot be established.

[0073] Thus, as a consequence, in step S7 a power level in the radio link is measured for at least the predetermined frequency range of the channel or band. In the embodiment a threshold level to establish a communication link is provided and it is determined whether the measured power level is above the threshold level to establish a communication link. In this case if in step S7 a measured power level is well below the threshold, thenfollowing the NO-path, in step S8 an OOS (out of service) indication can be outputted. Thus, obviously the user equipment is at a location wherein the power is too low as to sufficiently build up a communication link. A corresponding transmit power control error can be outputted. In step S9 for evaluating jamming a precondition is given in if defined.

[0074] However, in the case of following the YES-path, a power level measured is well above a threshold level to establish a communication link. This result will be taken as an indication for jamming along the YES-path following a step S7 with consideration of step S9. Thus, here an Ec/Io value can be measured --as biased power-- e.g. for a DPCH channel or DPCCH channel. Once, at least one out of number of bands is detected with sufficient power for a suitable cell connection the YES-path is to be followed as follow-up of step S7.

[0075] In GSM or CDMA this can be a channel specific RSCP value. However, also in step S7 the total received wide band power can be measured like e.g. an RSSI value. Although a wide band power measurement is less indicative of a biased jamming situation in the band and/or channel here a choice nevertheless is possible in a varied embodiment.

[0076] In step S10 a position estimate is executed by one or more of a number of preferred location means which can be selected according to the demands of the specific application. E.g. a GPS module or other measuring means can be used. Also a signal run time or interference in a cell or the like cell measurement can be used. Also, a location of the user equipment can be provided by means of an MMI (man machine interface) which input can be used for further steps in the procedure.

[0077] According to a first aspect of the concept the instant embodiment provides for a jamming detection using positioning. The first aspect method as outlined above can give the answer to the question of being in an area with deployed technologies not supported by the UE or being jammed can also be analyzed; positioning can be achieved by using of systems which allow a global positioning analysis. Such modules are known as GPS or radio services with regional pattern like WLAN (IEEE 802.11d-2001), world clock signals, i.e. in Germany the DCF77 is in use at 77kHz having a coverage area of 2000km hence being remarkable for Europe.

[0078] E.g. IEEE 802.11d-2001 or 802.11d is an amendment to the IEEE 802.11 specification that adds support for "additional regulatory domains". This support includes the addition of a country information element to beacons, probe requests, and probe responses. The country information elements simplifies the creation of 802.11 wireless access points and client devices that meet the different regulations enforced in various parts of the world. The amendment has been incorporated into the published IEEE 802.11-2007 standard.

[0079] In the same manner as above using additional hardware for positioning A-GPS has to be considered. A-GPS should be world wide available, by the achieved position it can be matched whether the radio communication is not available as technology not deployed or jammed. If A-GPS is also received but not decidable too, also this can be used as some jamming indication.

[0080] Generally beyond the instant embodiment a device for analyzing such jamming situations may be equipped with additional hardware or connected to said hardware being in the position for doing a location estimate on every means that is available, and comparing this to information identifying whether the supported technologies by the UE should be available in the determined area. As a consequence in case the UE detects that there is power in y out of z supported receiver bands which would be sufficient for having a suitable cell (a suitable cell is defined as a cell which could provide a service according to the radio conditions) it activates a hardware being in the position to identify the global position with one of the methods mentioned above, e.g. said world time signal where the usage may be limited to one or more of said signals. I.e. only for areas not supported or for areas where a technology used by the UE is supported. Furthermore if energy is detected in said band it should belong to that technology.

[0081] Certain confidence levels in case of radio shape analysis and/or variance analysis may be provided/calculated.

[0082] In step S9 a second condition is provided by the step S11 of evaluating to be in area of location --as de-

termined by the position estimate-- where coverage in one of the bands and/or channels should be available. Thus the at least predetermined frequency of the radio link as measured and identified with X mentioned above is identified to have sufficient power for a suitable cell connection and also should be available at the location of the user equipment. As a consequence in step S12 in general it can be determined that at the actual location with coverage is provided for built up of a communication connection in the predetermined frequency range.

[0083] However, to make this conclusion more reliable the concept of the invention provides a second aspect. Therein, according to step S13 a data base or the like is provided with technologies supported regions in certain bands in countries ITU. The characteristic feature of undisturbed power distribution of at least the predetermined frequency range according to the technology supported in the countries ITU regions can be used for identifying and associating the measured power distribution in step S13. Those are available for making a reliable decision in step S12. As it will be clear from the details following the power distribution measured in S12, a power distribution can be analyzed in terms of characteristic items of the power distribution indicative of at least the predetermined frequency range.

[0084] According to a second aspect of the concept the instant embodiment provides for detection by identifying normal bands according to ITU (international telecommunications union) in step S13. An M2M receiver itself has in a possible scanning mode a broader reception capability than the radio chip which is the limiting factor for the supported technologies carrying the spreading modulation and coding schemes of the communication technology within the M2M device; this means a receiver has the ability to receive the unbiased power in a large frequency spectrum and analyzing the energy distribution over the supported frequency range. It needs to be noted that according to WARC each ITU region has its own band plan and technologies being deployed there. Hence an undisturbed area in such a region shows a certain characteristic especially recognizable in the area where the transmitter of base-stations are operating. In these areas there will be a certain power distribution with a certain variance as not all bands are used in one place (e.g. there is a re-use for GSM). In addition the duplex technologies also have certain characteristics for receive and transmit bands. However, in a jamming signal the variance between separate channels is lower.

[0085] Hence, according to the concept upon reception of signals in the supported bands/technologies being above the level that is required for a suitable/detectable cell the mobile shall analyze the unbiased power of the entire range supported by its receiver and compare the shape to stored references of undisturbed WARC areas having different deployments or basic characteristics.

[0086] In a more advanced state the variance measured across the bands supported by the UE shall be analyzed. Jammed UE receiver bands have a higher nearly equal power distribution whilst BS transmitter bands due to re-use and coverage assumptions rather have a higher variance. Not all carriers are used in an area and even if so the power is different due to deployment of the base stations in different distances from the receiver.

[0087] Consequently, within step S12, one or more characteristic features of a position related undisturbed power distribution can be compared with a characteristic item of a measured power distribution according to a corresponding analysis in the at least predetermined frequency range. Generally --in the case the characteristic features and associated characteristic items do not correspond at least in a significant degree-- in step S12 a reliable conclusion can be taken that a jamming transmitter is affecting the communication user equipment.

[0088] As a follow up in the YES- path in step S13 a jamming indication can be given e.g. to an application in step S14. The application in step S14 may use this information for further measures, e.g. by outputting a warning or providing safety measures to protect a user equipment within an M2M system.

[0089] The process as such or relevant parts as described may be activated or deactivated.

[0090] Generally the concept can be implemented with a method of combining radio measurements and positioning analysis for jamming detection, a device supporting said functionality, a computer program executing such functionality, an internal or external application controlling and triggering such method, a service centre providing support for such a method, any instance in or connected to the device supporting the method. A respective device is shown schematically in Fig. 3.

[0091] The user equipment 100 comprises a module 10 for mobile communication with cellular radio network RN via an air interface, namely by means of an antenna 20 connected to a receiver. The receiver and also a power source for powering the user equipment is not shown in detail. The user equipment is provided with a SIM card 1 for authentication in the radio network RN and a storage means 2. Further the user equipment 100 has an interface connection 30 between the module 20 and an application 40. On the interface connection 30 AT-commands can be transmitted for signaling between the module 20 and the application 40. The application 40 can be realized by means of a software- or hardware-layer, in particular by any kind of device for connection to the cellular network by the module 10. E.g. the application 40 can be formed by some kind of a sensor- or supervision-device or metering device or other apparatus.

[0092] In particular, the interface connection 30 can be used for transmitting a jamming warning and/or jamming detection indication to an application 40 once the module 10 has detected a jamming transmitter by means of the method described above. The module 10 thus is adapted for executing one or more method steps according to the embodiment shown in Fig. 3. In particular, the module 10 provides a power measuring unit 11 and a power analysis unit 12. Further, the module provides for a link meas-

uring unit 13 and a link analyzing unit 14. Last but not least the module 10 also provides a location measuring unit 15 and a location analyzing unit 16.

[0093] The power measuring unit 11 is adapted for measuring a power level in the radio link via the antenna 20 and a corresponding receiver sensory for a power level in the radio link at least at the predetermined frequency range, namely in particular in at least the band and/or channel as found during cell search. An analyzing unit 12 provides for a comparator measure for determining whether the power level measured is above a threshold level to establish a communication link. A respective threshold level can e.g. be stored in the storage means 2 or be submitted to the module 10. A respective threshold level also can be stored according to a setting or other received network frame.

[0094] The link measuring unit 13 is adapted for measuring the radio link at least at the predetermined frequency range by providing a power distribution of the radio link at least of a predetermined frequency range. The power distribution can be provided as a function of frequency and is transferred to the analyzing unit 14 of the module 10. The analyzing unit 14 is adapted for analyzing the power distribution in terms of a characteristic item of the power distribution indicative of at least the predetermined frequency range. Thus, in the analyzing unit 14 the width, steepness, dips and the like shape parameters of the power distribution can be determined. Also in particular a dip or gap in the distribution can be determined to result from the duplex distance between an uplink and downlink channel or other separation of channels; thus is an important feature / item to discriminate between an undisturbed power spectrum and a jamming spectrum. Further, the analyzing unit can also provide further characteristic features which have no direct relation to the frequency; but nevertheless all of these shape features can be used to characterize the power distribution with essential and mostly strong features thereof.

[0095] A location measuring unit 15 is adapted for measuring a position of the communication user equipment as indicated above. An analyzing location unit 16 is adapted for retrieving a characteristic feature of a position related undisturbed power distribution of at least the predetermined frequency range. The undisturbed location related power distribution e.g. can be stored directly in the SIM card 1 but also in a storage means 2 of the user equipment.

[0096] As shown in Fig. 3 the storage 2 of lookup information can be accomplished. In case of the usage of stored pre-knowledge information i.e. received unbiased power radio shape analysis, said information is stored on the SIM card 1 or within the UE 100 itself. The information matching the current position with the areas where the supported technologies by the UE are provided can be done by stored information held in the UE. Either in the UE directly or in the SIM card. I.e. in which countries are the supported bands designated to e.g. GSM; this is a simple table.

[0097] All relevant parameters used may be settable by AT commands and updatable via AT commands or radio communication. I.e. in case of radio shape analysis when the target is known of an aircraft delivery the expected undisturbed radio shape of power distribution could be send to the UE 100 via radio communication from a service centre which in case of conditions as above come true may be used for said analysis.

Claims

1. Method of detecting a jamming transmitter, affecting a communication user equipment, wherein

   - said communication user equipment (UE) is adapted for communication with a component of a cellular radio network (RN) having a number of user equipments (UE) and a number of base stations (BNS) for communication in a communication band on a communication channel of predetermined frequency range,
   - providing the user equipment (UE) in a start up mode for achieving a connected mode of a communication radiolink with the component of the radio network (RN), wherein in the start up mode of said user equipment (UE) it is determined that a connected mode of the communication radiolink cannot be established, and wherein the steps are provided:
   - measuring a power level in the radiolink at least at the predetermined frequency range, in particular in at least the band and/or channel, preferably communication channel, and determining whether the power level is above a threshold level to establish a communication link;
   - receiving a location information with regard to a position of the communication user equipment;
   - receiving a coverage information of deployment of radio network at the position;
   - indicating a jamming transmitter in case the coverage information is positive with regard to the supported communication capability of the user equipment at the position of the communication user equipment.

2. Method according to claim 1, wherein one or more good-reference parameters comprise indicating that the communication user equipment (UE) is capable of communicating in the cellular radio network (RN) by means of a communication indicator as further parameter.

3. Method according to claim 1 or 2 wherein the location information comprises determining, preferably measuring or estimating, a position of the communication user equipment.

4. Method according to one of the preceding claims wherein receiving a coverage information of deployment of radio network at the position comprises receiving information with regard to a specific location like a sub-way or the like out-of-service (OOS) location.

5. Method according to one of the preceding claims wherein receiving a coverage information of deployment of radio network at the position comprises information about a communication technology deployed, preferably from a stored data item, like e.g. a stored list or the like.

6. Method according to one of the preceding claims further comprising the steps of:

- measuring the radiolink at least of a predetermined frequency range by providing a power distribution of the radiolink at least of predetermined frequency range,
- analyzing the power distribution in terms of a characteristic item of the power distribution indicative of at least the predetermined frequency range.

7. Method according to one of the preceding claims further comprising the steps of:

- retrieving a characteristic feature of a position related undisturbed power distribution of at least the predetermined frequency range, wherein
- the characteristic feature is associated with the analyzed characteristic item of the measured power distribution at the measured position, and
- comparing one or more characteristic features and associated characteristic items and verifying whether they do not correspond at least in a significant degree and in case of non-correspondence, indicating a jamming transmitter.

8. Method as claimed in one of the preceding claims wherein the radiolink is measured for at least predetermined frequency range of one or more bands and/or channels and the power distribution is analyzed at least in the predetermined frequency range across a number of separate bands and/or channels.

9. Method as claimed in one of the preceding claims wherein measuring the radiolink provides an unbiased power distribution across available communication bands and/or channels of the, in particular entire, supported antenna range, in particular wherein the item is a variance of separate bands and/or channels and analyzing the unbiased power distribution is in terms of a variance of separate bands and/or channels.

10. Method as claimed in one of the preceding claims wherein the radiolink is measured for at least predetermined frequency range of one or more bands and/or channels and the power distribution is analyzed at least in the predetermined frequency range inside of at least one band and/or channel.

11. Method as claimed in one of the preceding claims wherein measuring the radiolink provides an biased power distribution in a supported communication band and/or channel of the communication radiolink, in particular wherein the item is a shape of distribution in the band and/or channel and analyzing the biased power distribution is in terms of a shape of distribution in the band and/or channel.

12. Method as claimed in one of the preceding claims wherein measuring a power level in the radiolink, in particular a band and/or channel, and determining whether the power level is below a threshold level to establish a communication link is for providing an out-of-service indication.

13. Method as claimed in one of the preceding claims wherein measuring the radiolink provides one or more additional technology relevant parameters, wherein the technology is selected from the group comprising:

- GSM based technologies like GPRS, EDGE and the like 2G-technologies,
- TDMA based technologies like WCDMA, HSPA, EV-DO or the like 3G-(UMTS)technologies,
- CDMA based technologies like IS-technologies or the like 2G, 3G technologies,
- LTE or WiMax based technologies and the like 4G-technologies.

14. Method as claimed in one of the preceding claims wherein a characteristic feature is retrieved from a preloading, stored, downloaded, or in-use collected or the like gathered undisturbed power distributions, in particular in a list or the like look-up-table.

15. Method as claimed in one of the preceding claims wherein determining a position of the communication user equipment provides for at least estimating, in particular identifying, a location of the user equipment, in particular by one or more of software, hardware or MMI measures, in particular selected from the group comprising of: MMI input, GPS module, cell measurement, signaling run time or interference or the like measurement.

16. Device for a user equipment, in particular device reportingly connectable to an application layer, configured to execute the method of detecting a jamming,

affecting the communication user equipment in a start up mode as claimed in any of the claims 1 to 14, wherein the detection device has

- a power measuring unit adapted for measuring a power level in the radiolink at least at the predetermined frequency range, in particular in at least the band and/or channel, and determining whether the power level is above a threshold level to establish a communication link;
- a link measuring unit adapted for measuring the radiolink at least of predetermined frequency range by providing a power distribution of the radiolink at least of predetermined frequency range,
- an analyzing unit for analyzing the power distribution in terms of a characteristic item of the power distribution indicative of at least the predetermined frequency range;
- a location measuring unit adapted for measuring a position of the communication user equipment and retrieving a characteristic feature of a position related undisturbed power distribution of at least the predetermined frequency range, wherein
- the characteristic feature is associated with the analyzed characteristic item of the measured power distribution at the measured position;
- a comparator adapted for comparing one or more characteristic features and associated characteristic items and verifying whether they do not correspond at least in a significant degree and in case of non-correspondence, indicating a jamming transmitter.

FIG. 2

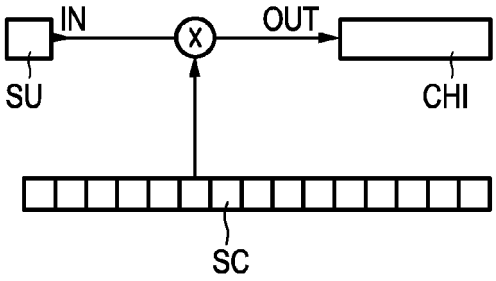
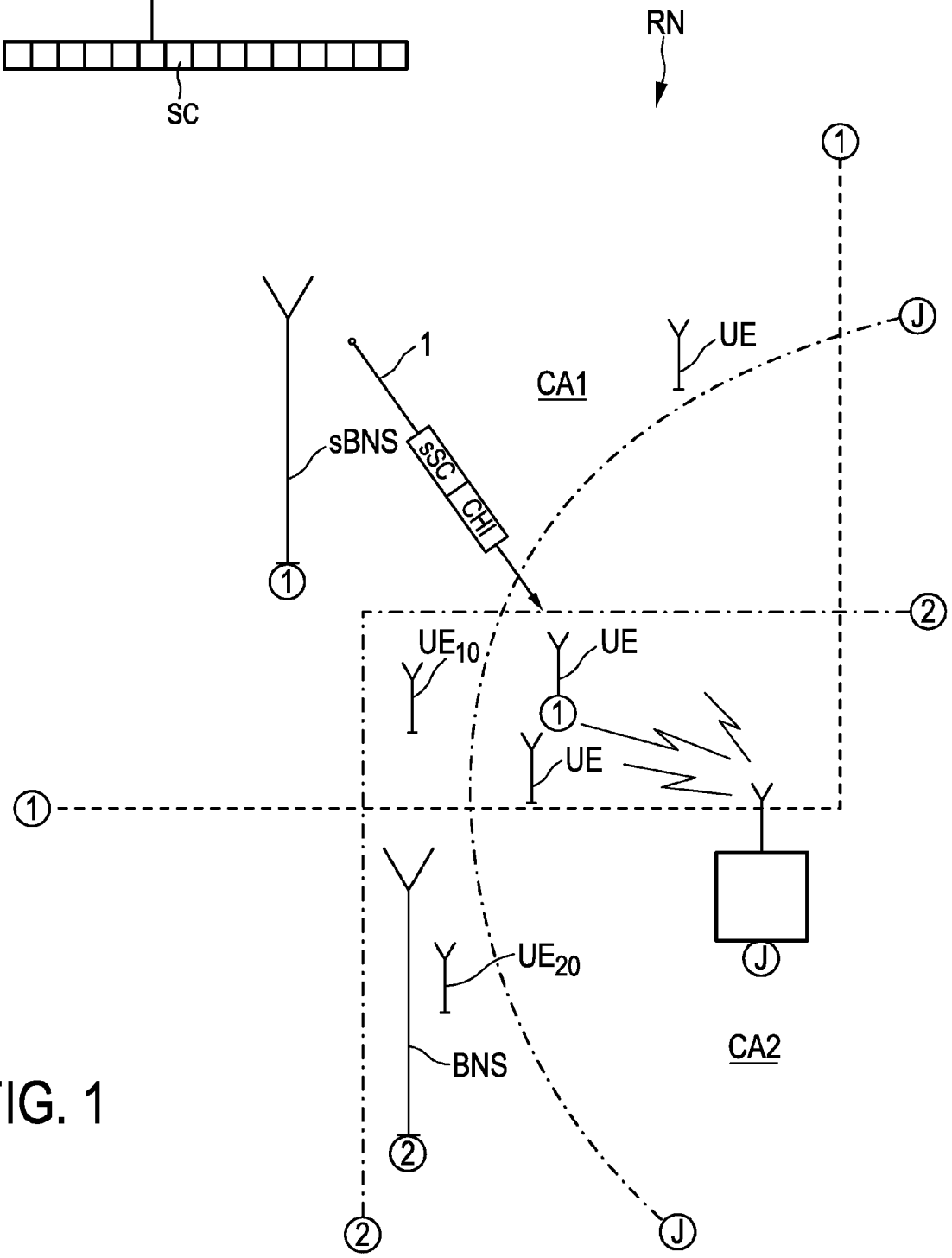

IN
X
OUT
SU
CHI
SC

FIG. 1


RN
1
J
UE
CA1
1
sBNS
sSC
CHI
1
2
UE10
UE
1
UE
1
J
UE20
CA2
BNS
2
2
J

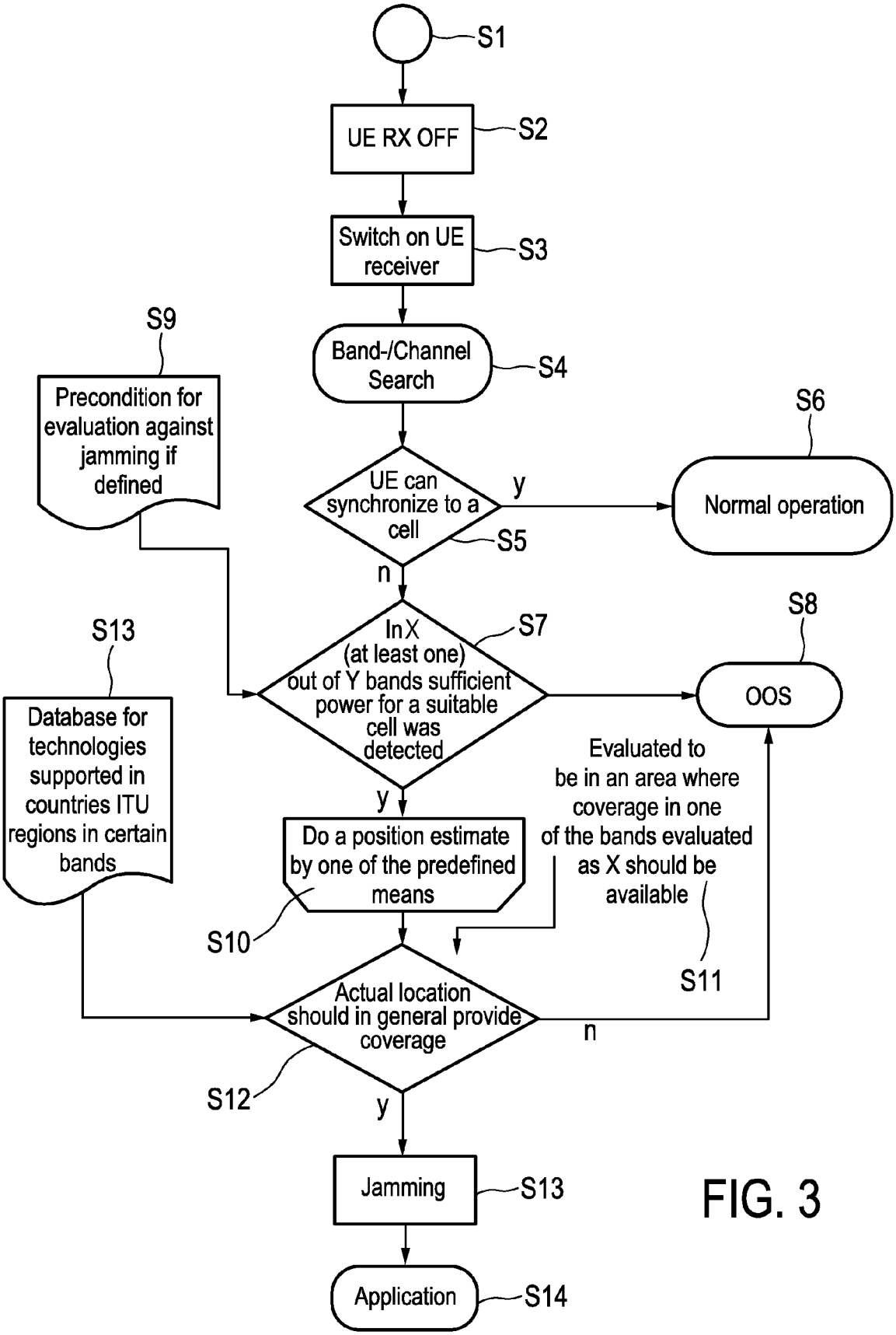

S1
UE RX OFF
S2
Switch on UE receiver
S3
Band-/Channel Search
S4
S9
Precondition for evaluation against jamming if defined
UE can synchronize to a cell
S5
y
S6
Normal operation
n
S13
Database for technologies supported in countries ITU regions in certain bands
In X (at least one) out of Y bands sufficient power for a suitable cell was detected
S7
S8
OOS
y
Do a position estimate by one of the predefined means
S10
Evaluated to be in an area where coverage in one of the bands evaluated as X should be available
S11
Actual location should in general provide coverage
n
S12
y
Jamming
S13
Application
S14

FIG. 3

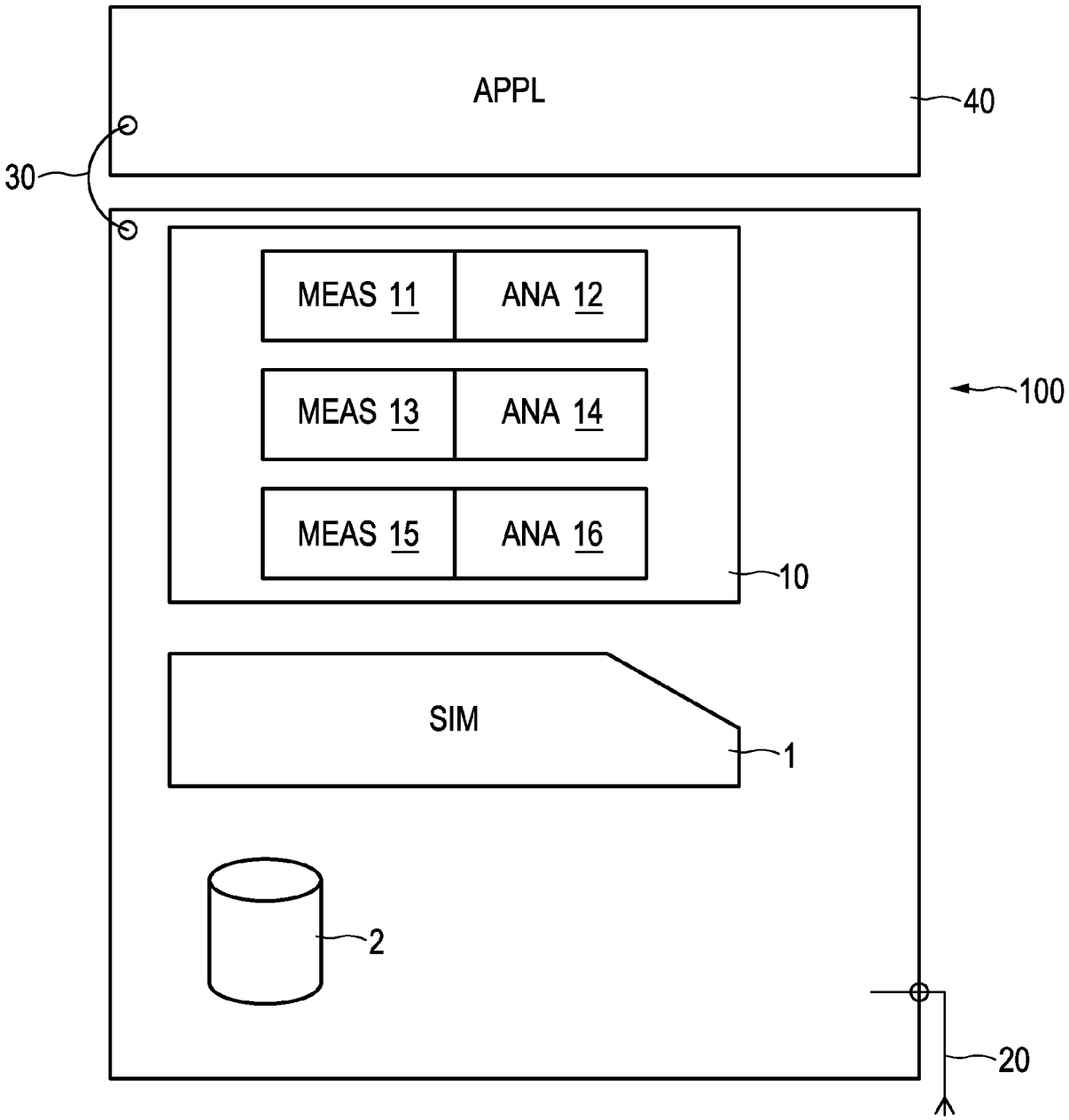

APPL
40
30
MEAS 11
ANA 12
MEAS 13
ANA 14
MEAS 15
ANA 16
10
100
SIM
1
2
20

FIG. 4

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 12 16 7929

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	GB 2 481 720 A (VODAFONE PLC [GB]) 4 January 2012 (2012-01-04) * abstract * * page 1, line 1 - page 9, line 12 * * page 47, line 1 - page 59, line 29 * -----	1-16	INV. H04K3/00
X	US 2004/005858 A1 (CERVINKA ALEXANDRE [CA] ET AL) 8 January 2004 (2004-01-08) * abstract * * paragraph [0003] - paragraph [0008] * * paragraph [0013] - paragraph [0046] * * figures 1-2 * -----	1-16	
E	EP 2 453 582 A1 (CINTERION WIRELESS MODULES GMBH [DE]) 16 May 2012 (2012-05-16) * abstract * * paragraph [0008] * * paragraph [0012] - paragraph [0028] * * paragraph [0032] - paragraph [0049] * * figures 1-3 * -----	1-16	TECHNICAL FIELDS SEARCHED (IPC) H04K

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	26 November 2012	Dujardin, Corinne

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 12 16 7929

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

26-11-2012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2481720 A	04-01-2012	NONE	
US 2004005858 A1	08-01-2004	CA 2392326 A1	03-01-2004
		US 2004005858 A1	08-01-2004
		US 2004005872 A1	08-01-2004
		US 2005017899 A1	27-01-2005
EP 2453582 A1	16-05-2012	EP 2453582 A1	16-05-2012
		WO 2012066052 A1	24-05-2012
		WO 2012066053 A1	24-05-2012

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 2005112321 A **[0004] [0008]**
- WO 2007019814 A **[0005] [0008]**
- WO 0062437 A **[0007]**