Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2685841 C 2013/06/11

(11)(21) 2 685 841

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2008/04/29
(87) Date publication PCT/PCT Publication Date: 2008/11/13
(45) Date de délivrance/Issue Date: 2013/06/11
(85) Entrée phase nationale/National Entry: 2009/10/30
(86) N° demande PCT/PCT Application No.: US 2008/061893
(87) N° publication PCT/PCT Publication No.: 2008/137417
(30) Priorités/Priorities: 2007/04/30 (US60/915,078);
2007/05/29 (US60/940,557)

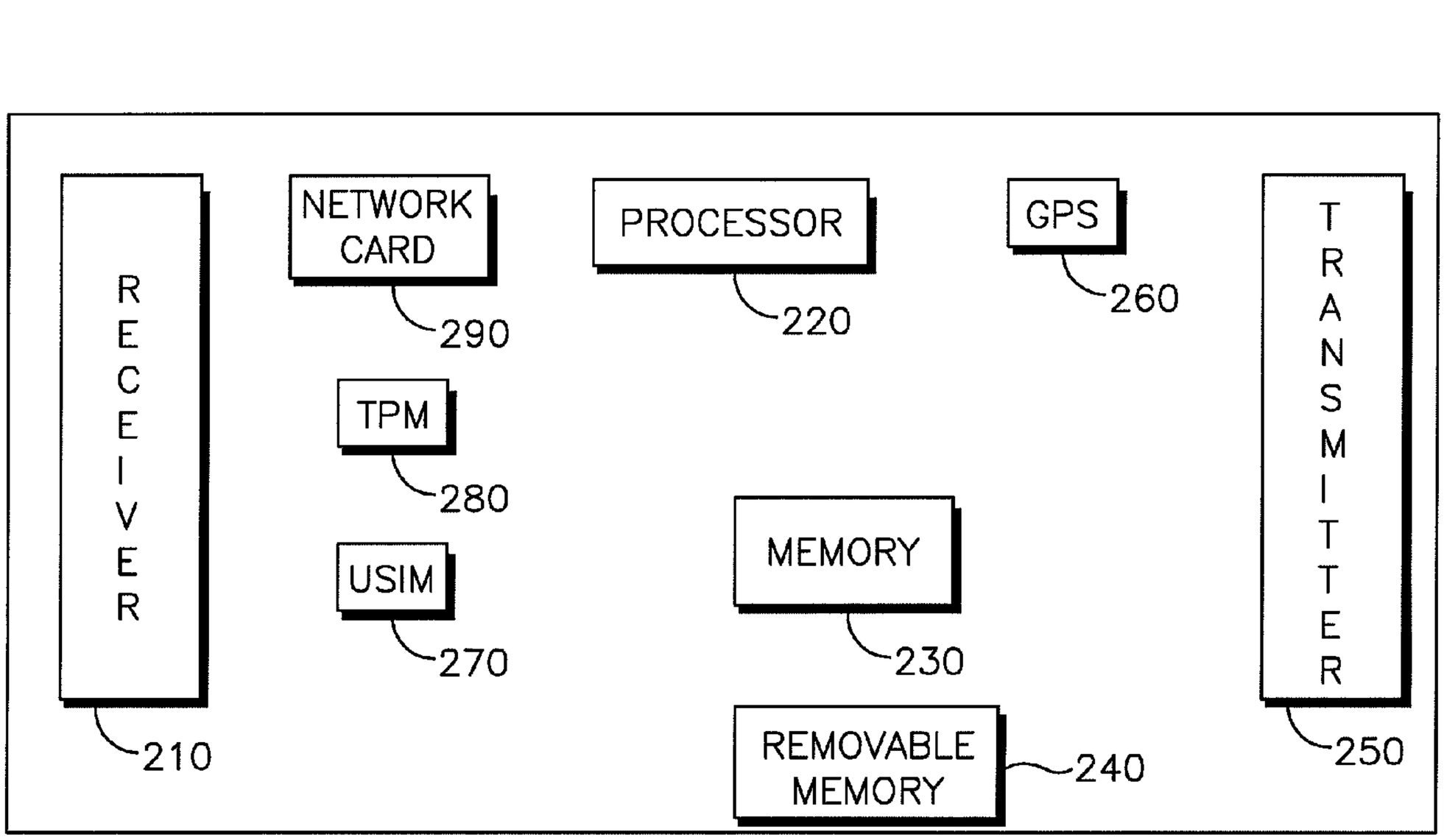
(51) Cl.Int./Int.Cl. *H04W 48/12* (2009.01)

(72) Inventeurs/Inventors:
MUKHERJEE, RAJAT P., CA;
SOMASUNDARAM, SHANKAR, US;
SHAH, YOGENDRA C., US;
CHITRAPU, PRABHAKAR R., US;
CHA, INHYOK, US;
OLVERA-HERNANDEZ, ULISES, CA

(73) Propriétaire/Owner:
INTERDIGITAL TECHNOLOGY CORPORATION, US

(74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : (e)NOEUD B A DOMICILE EQUIPE D'UNE NOUVELLE FONCTIONNALITE
(54) Title: A HOME (e)NODE-B WITH NEW FUNCTIONALITY



(57) Abrégé/Abstract:
A wireless communication device is configured as an in-home node-B (H(e)NB). The H(e)NB is configured to perform a locking function to control modification of carrier and user controlled parameters, and also configured to detect a change in location.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 November 2008 (13.11.2008)

PCT

(10) International Publication Number
WO 2008/137417 A3

(51) International Patent Classification:
H04W 48/12 (2009.01)

(21) International Application Number:
PCT/US2008/061893

(22) International Filing Date: 29 April 2008 (29.04.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/915,078	30 April 2007 (30.04.2007)	US
60/940,557	29 May 2007 (29.05.2007)	US

(71) Applicant *(for all designated States except US)*: **INTERDIGITAL TECHNOLOGY CORPORATION** [US/US]; 3411 Silverside Road, Concord Plaza, Suite 105, Hagley Building, Wilmington, Delaware 19810 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MUKHERJEE, Rajat, P.** [IN/CA]; 3620 Lorne Crescent, Apt. 717, Montreal, Québec H2X 2B1 (CA). **SOMASUNDARAM, Shankar** [IN/US]; 5 Andover Drive, Deer Park, New York 11729 (US). **OLVERA-HERNANDEZ, Ulises** [MX/CA]; 2 Rolland Laniel, Kirkland, Québec H9J 4A5 (CA). **SHAH, Yogendra, C.** [GB/US]; 10 Regency Court, Exton, Pennsylvania 19341 (US). **CHITRAPU, Prabhakar, R.** [US/US]; 135 Brochant Drive, Blue Bell, Pennsylvania 19422 (US). **CHA, Inhyok** [US/US]; 510 Southridge Circle, Yardley, Pennsylvania 19067 (US).

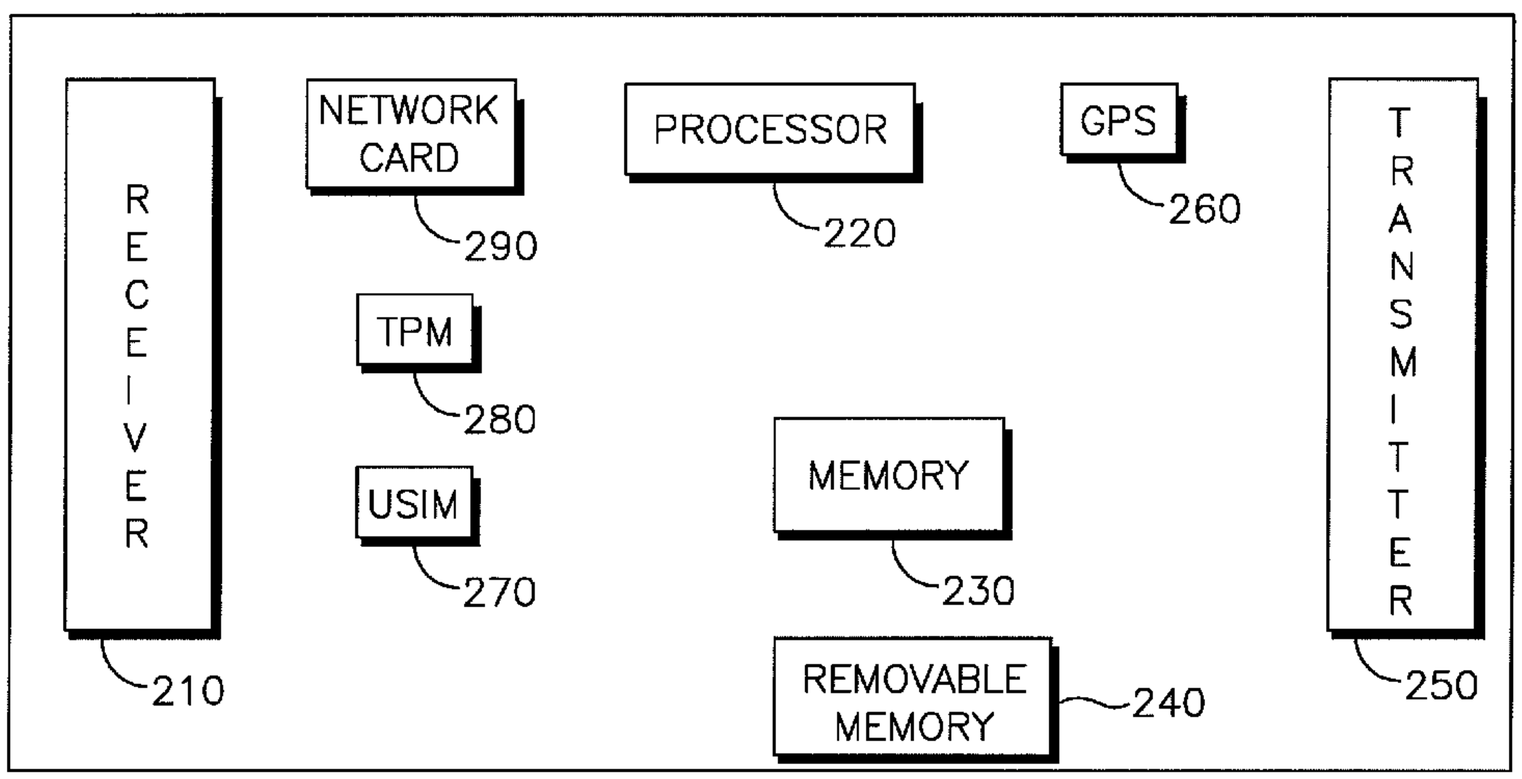
(74) Agent: **SOLOMON, Robert, I.**; Volpe and Koenig, P.C., 30 South 17th Street, United Plaza, Suite 1600, Philadelphia, Pennsylvania 19103 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: A HOME (e)NODE-B WITH NEW FUNCTIONALITY



(57) Abstract: A wireless communication device is configured as an in-home node-B (H(e)NB). The H(e)NB is configured to perform a locking function to control modification of carrier and user controlled parameters, and also configured to detect a change in location.

WO 2008/137417 A3

WO 2008/137417 A3

ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
2 April 2009

[0001] A HOME (e)NODE-B WITH NEW FUNCTIONALITY

[0002] FIELD OF INVENTION

[0003] The application relates to wireless communication networks, and more particularly, to an advanced in-home (e)Node-B (H(e)NB).

[0004] BACKGROUND

[0005] A goal of the Third Generation Partnership Project (3GPP) Long Term Evolution (LTE) program is to develop new technology, new architecture and new methods for LTE settings and configurations in order to provide improved spectral efficiency, reduced latency, and better utilization of radio resources for faster user experiences and richer applications and services with less cost. As part of these efforts, the 3GPP has introduced the concept of an in-home, evolved node B (called H(e)NB) for LTE networks. 3GPP is also considering the in-home NB (called HNB) for Release 8 wideband code division multiple access (WCDMA). The acronym H(e)NB is used in this application to refer to both a H(e)NB and a HNB.

[0006] The in-home (e)NB (H(e)NB) is preferably similar to a wireless local area network (WLAN) access point (AP). It gives users access to LTE services (it may also provide Wideband Code Division Multiple Access (WCDMA), Global System for Mobile Communication (GSM) Edge Radio Access Network (GERAN), and other cellular services) over extremely small service areas such as homes and small offices. This can be particularly useful in areas where LTE has not been deployed and/or legacy 3GPP radio access technology (RAT) coverage already exists. This may also be useful in areas where cellular services have yet to be deployed, or where coverage may be faint or non-existent for radio related reasons, such as in an underground metro or shopping mall. The subscriber, whether an individual or an organization, will be able to deploy a H(e)NB in an area where such service is desired. Figure 1 shows an example of a possible H(e)NB deployment.

[0007] Several issues should be addressed regarding the use of an H(e)NB. H(e)NB mobility is a potential problem. An H(e)NB could easily change location. A new location may pose a challenge if, for example, the operator who originally provided the H(e)NB did not offer coverage at the new location, thus a user may need to use a different operator and follow a location update procedure. An H(e)NB preferably would include high-level functions to implement detection of its own mobility as well as functions to implement other operator restrictions. All of this must be accomplished in a cost effective manner.

[0008] SUMMARY

[0009] An in-home node-B (H(e)NB) configured to perform a locking function to control modification of carrier and user controlled parameters, and also configured to detect a change in location.

[0010] BRIEF DESCRIPTION OF THE DRAWING

[0011] A more detailed understanding of the invention may be had from the following description of a preferred embodiment, given by way of example and to be understood in conjunction with the accompanying drawing wherein:

[0012] Figure 1 shows an example of a H(e)NB deployment;

[0013] Figure 2 illustrates an example embodiment of a H(e)NB and its respective components;

[0014] Figure 3 shows an embodiment of a relay station (RS) H(e)NB and its respective components; and

[0015] Figure 4 shows an example of a RS deployment.

[0016] DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

[0017] When referred to hereafter, the terminology "wireless transmit/receive unit (WTRU)" includes but is not limited to a user equipment (UE), a mobile station, a fixed or mobile subscriber unit, a pager, a cellular telephone, a personal digital assistant (PDA), a computer, or any other type of user device capable of operating in a wireless environment. When referred to hereafter, the terminology "base station" includes but is not limited to a Node-B, a site controller, an access point (AP), or any

other type of interfacing device capable of operating in a wireless environment. When referred to hereafter, the terminology "user" is interchangeable with "subscriber." When referred to hereafter, the terminology "operator" is interchangeable with "carrier," "wireless provider," and "wireless carrier." When referred to hereafter, the terminology "memory" refers to any computer-readable storage medium, examples of which include a read only memory (ROM), a random access memory (RAM), a nonvolatile random access memory (NVRAM), a register, cache memory, semiconductor memory devices, magnetic media such as internal hard disks and removable disks, magneto-optical media, and optical media such as CD-ROM disks, and digital video disks (DVDs). When referred to hereafter, the terminology "controlled" is interchangeable with "configurable." When referred to hereafter, the terminology "parameter" and "characteristic" are equivalent.

[0018] Figure 2 depicts an example embodiment of a H(e)NB 200 comprising a receiver 210, a processor 220, a memory 230, a removable memory 240, a transmitter 250, and a GPS device 260, an integrated or removable universal subscriber identifier module (USIM) module 270, a trusted platform module (TPM) 280 which is a secure hardware component that provides a secure storage and execution environment, and a network card 290 comprising a modem (baseband) processor. In alternative embodiments, the USIM module 270 may be implemented as an integrated or removable universal integrated circuit card (UICC), or as an embedded functionality implemented collectively by the processor 220, the TPM 280, and some of the internal memory 230. In an alternative embodiment, the network card 290 may be integrated into the processor 220. The processor 220, among other things, is configured to process one or more applications. In an alternative embodiment, the application processor may be a separate device.

[0019] In one embodiment, a H(e)NB has parameters that are configured by an operator (carrier, wireless provider, etc.) using conventional methods and parameters that may be configured by a subscriber (based upon proper authorization and/or authentication). The operator can configure parameters that control, restrict, and define the operation of the H(e)NB including, but not limited to a public land mobile

network identifier (PLMN ID) that should be broadcasted by the H(e)NB, H(e)NB supported services (basic voice service, emergency call support, high speed data support), security parameters used by the H(e)NB (such as whether it is locked, whether user data is protected, the security keys and algorithms used for performing these functions), the spectrum in which the H(e)NB operates, the location of operation, and/or the tariffs employed. Some of these parameters are only configurable by the operator. Such parameters are referred to as locked parameters, thus a H(e)NB can be locked in a manner similar to the way WTRUs (mobile phones, etc.) are locked by an operator. Referring to Figure 2, these parameters are handled by the processor 220 and may be stored in the memory 230. The TPM 280 may be used to securely store the parameters either within its own internal non volatile random access memory (NVRAM), or store encryption keys that have been used to encrypt these parameters, which are then stored encrypted in memory 230.

[0020] In Figure 2, the USIM module 270 may store the static configuration parameters and assist the H(e)NB in its self-configuration upon start-up. Additional parameters can also be included in a standard H(e)NB configuration independent of the specific services (LTE, GERAN, 3GPP, etc.) offered by the H(e)NB. Alternatively, some of the parameters may be stored either within the TPM 280 or in the memory 230 but encrypted by keys stored in the TPM 280.

[0021] H(e)NB parameters may be configured or modified using a locking (lock/unlock) function. The locking function manages access to H(e)NB parameters and comprises commands such as lock and unlock, and other procedures such as authentication, verification and similar capabilities. In one embodiment, this function, is included in a smart card or a removable memory module, and could be extended to serve both a WTRU and the H(e)NB, that is, a single smart card could provide this function for both a WTRU and an H(e)NB.

[0022] In another embodiment, the locking function ensures that the H(e)NB cannot be operated unless specific criteria for operation are met (specific parameters must be set in a specific manner or contain specific values). The locking function is enforced at the hardware level or by using trusted computing techniques that provide a

secure execution environment and a secure storage environment. Lockable parameters include but are not limited to the public land mobile network identifier (PLMN ID) that is broadcasted by the H(e)NB, H(e)NB supported services, security parameters used by the H(e)NB , the spectrum (frequency) in which the H(e)NB operates, the location of operation, and/or the tariffs employed.

[0023] In the event that a user attempts to reconfigure parameters of operation without the requisite authority the locking function will take one or more actions including, but not limited to forcing the H(e)NB to stop operating or shutting it down, reducing the offered services, restricting admission control, resetting configuration parameters by sending operational and maintenance (O&M) signaling or control plane (C-plane) signaling to the operator, sending warning messages to the operator, and/or directly contacting the operator.

[0024] As stated above, the H(e)NB may be configured such that only the original operator or vendor is able to change certain parameters (the H(e)NB is locked). In another embodiment, the operator specifies in the locking function that the H(e)NB is allowed to accept a WTRU only if it is subscribed with that operator. This may be indicated, for example, by the PLMN ID in messages sent by the WTRU. Thus, if the user changes operators, the user will not be able to use the H(e)NB until and unless the H(e)NB is unlocked and this parameter is changed.

[0025] In another embodiment, Open Mobile Alliance (OMA) mechanisms, such as client provisioning and device management (DM), are applied between the operator network and the H(e)NB. When the H(e)NB is configured and setup, there is an exchange of information between the network and the H(e)NB using OMA mechanisms so that specific capabilities are configured in the H(e)NB. In Figure 2, such OMA procedures may be performed by the processor 220.

[0026] In one embodiment, the “unlock” capability of the locking function (enforced, for example, at the hardware level or using trusted computing techniques) ensures that the H(e)NB can be “unlocked” when all requisite (predetermined) criteria for operation are met. Examples of such conditions include:

[0027] successful authentication of the H(e)NB and/or the (new) owner of the H(e)NB, and/or

[0028] successful verification of the context of the request for "unlocking" of the H(e)NB by its owner/operator, and/or

[0029] successful verification of the attestation by the H(e)NB of its platform trustworthiness.

[0030] Attestion means an attempt by the H(e)NB to 'attest to the trustworthiness of the platform of the H(e)NB to an appropriate network entity'. Verification means that entity's verification of such attestation from the H(e)NB. Referring to Figure 2, the parameters needed to "unlock" the H(e)NB may be stored in the USIM module 270. Alternatively, it may be stored within the TPM 280 or in the memory 230 but encrypted by keys stored in the TPM 280.

[0031] The "unlock" command and the parameters to be modified are forwarded from the Core Network/ radio network controller (RNC) to the H(e)NB via signaling such as new O&M signaling or C-plane signaling. In another embodiment, such commands and parameters are forwarded by the use of OMA DM.

[0032] An H(e)NB may be moved from one location to another. An H(e)NB has the capability to detect such location changes via a variety of mechanisms. Referring to Figure 2, such location change detection functionality may be implemented collectively by the processor 220 and the global positioning system (GPS) (or assisted GPS (A-GPS) or any other positioning device) 260. The USIM module 270 may securely store parameters and configuration files for the location change detection functionality. Alternatively, the TPM 280 may be used to either directly store such parameters and configuration files within it, or to store encryption keys that have been used to encrypt such parameters and files. The TPM 280 may also be used to protect the integrity of the software handling the location change detection functionality.

[0033] In one embodiment, the H(e)NB is programmed with the identifier or identifiers (ID)s of any surrounding macro-cell(s), such as LTE, GSM/edge radio network (GERAN) and the like and/or neighbor cells. The H(e)NB is programmed to detect neighbor cells and certain expected measurement values. Upon startup, if the

H(e)NB detects one or more pre-programmed cells and determines that the radio strength of one or more of these cells is within or close to expected measurement values, the H(e)NB assumes that its location has not changed significantly (for example, within the surrounding macro-cell). In another embodiment, the H(e)NB uses the location information provided by its onboard GPS, or from a WTRU that it is serving, or from a WTRU in a neighboring cell, and compares this information with its configured (stored) location parameter or parameters to determine if its location has changed. Referring to Figure 2, either the USIM module 270 or the TPM 270 (either directly or indirectly by storing encryption keys) may store the IDs of the macro-cell, the list of detected neighbor cells and other expected and real measurement values, and any location information or the WTRU-reported neighbor cell information. The processor 220 may perform any algorithms for the location change detection.

[0034] Alternatively, if the H(e)NB is unable to detect a pre-programmed cell, and/or the radio strength of any surrounding cell is significantly lower than the expected value, the H(e)NB will assume that either its neighbors have changed (assuming that the H(e)NB can determine that it has not moved), or that its location has changed. In the event that the H(e)NB is absolutely certain that it has not moved (all stored expected location parameters match all provided or measured location information and parameters), the detection of a change in a neighbor cell will trigger a request to the core network (CN) (using, for example, O&M signaling), to update its neighbor list. Referring to Figure 2, the signal measurement obtained from the receiver 210 may be processed by the processor 220, and a determination may be made by the processor 220 on whether the radio strength from any surrounding cell is significantly lower than the expected value. If such a determination is made, a notification of a detection of the change in a neighbor cell may be transmitted to the CN by the transmitter 250.

[0035] Alternatively, if the H(e)NB determines that its location might have changed (some stored expected location parameters match only some provided or measured location information and parameters) it will, depending on its connectivity and programmed configurations, implement by way of the processor 220, the

transmitter 250, the USIM module 270, and the TPM 280, any of the following location update mechanisms (procedures) either individually or in any combination:

[0036] contact the operator core network and report a change in location with an indication of the new location/new IP address, and any detected neighbors;

[0037] request updated neighbor list information;

[0038] institute a trigger locking mechanism;

[0039] broadcast an out of service alert message to the WTRUs attempting to connect to the H(e)NB;

[0040] continue operating or reconfigure its neighbor list on its own.

[0041] In one embodiment, the H(e)NB has a periodic timer, which, when it expires, causes the H(e)NB to contact the operator network and request an updated neighbor list. Referring to Figure 2, such a timer may be implemented by the TPM 280 or the processor 220 or collectively between them. The operator network will then give the H(e)NB an updated neighbor list based on any updated information it has and the H(e)NB will use this to understand the extent of change in its surroundings.

[0042] In another embodiment, the H(e)NB may include a position detection device, for example, a GPS chip(referred to as GPS 260 in Figure 2), that may provide the absolute location of the H(e)NB. Limited mobility of the H(e)NB preferably is supported. Consequently, the H(e)NB will have a range of coordinates within which it is able to operate. This range may include, multiple locations, examples of these locations include but are not limited to a home, an office, an alternative office, retail building, a commercial space, areas adjacent to homes, offices, retail buildings, commercial spaces etc.

[0043] In another mobility management embodiment, the H(e)NB defines an association between the H(e)NB and a serving Higher Network Node (HNN), which could be an RNC or the base station (BS) ID of a macro-cell. Each HNN advertises its own identity and the H(e)NB listens to the identity of the serving HNN and stores it internally. When the H(e)NB moves to a new location which is served by a different HNN, the H(e)NB detects this change by comparing the advertised HNN identity and its own stored value. If they differ, a H(e)NB location update procedure is initiated.

Referring to Figure 2, the processor 220, possibly with assistance from the GPS module 260, the USIM module 270 and/or the TPM 280,or any combination of these, may perform functionality to determine the absolute location of the H(e)NB or the relative location (in the form of neighbor-cell lists and HNN lists) and perform functions such as access-control and out-of-range reporting.

[0044] In another embodiment, the H(e)NB is programmed with a data base (H(e)NB DB) including, but not limited to WTRU information such as WTRU ID(s), expected values for certain WTRU parameters (power capability of the WTRU, support for Multiple Input Multiple Output (MIMO), modulation capability of WTRU, security algorithms supported by WTRU) and other similar characteristics of the WTRUs (for example: validation, authentication, etc.) in order to be connected or to request connection to the H(e)NB. Any element of the H(e)NB DB shall be considered H(e)NB DB "information" or "data." Referring to Figure 2, the processor 220, in conjunction with the memory 230, may handle such a database. Alternatively, the TPM 280 may also additionally be used to store some or all of the elements of the database in a secure manner.

[0045] Alternatively, the H(e)NB may acquire this information over time (a typical range is 0 to 5 minutes) from the WTRUs connecting to it. In a home setting and over some reasonably long periods of time (a typical range is 0 to 5 minutes), many if not most of the WTRUs connected to a given H(e)NB would be the same. Therefore, upon startup and after monitoring the WTRUs connected to it for a specified period of time, if the H(e)NB detects that a large amount of the WTRU IDs have changed, or that other WTRU characteristics vary from the expected values in the H(e)NB DB, the H(e)NB may assume that its location has changed.

[0046] If the H(e)NB suspects such a change, then the H(e)NB may assume that either there is a change in the IDs and other characteristics of the WTRUs that are connecting or requesting to connect to it, or that its location has changed. In the event that the H(e)NB is absolutely certain (e.g. using GPS, neighbor cell information provided by a WTRU) that it has not moved, such a detection of change in H(e)NB DB

information is, for example, communicated to the Core Network/RNC (e.g. using O&M signaling) by either sending an alert message indicating such change(or suspicion of change), or requesting verification that the perceived changes in the IDs or other characteristics of the WTRUs connected (or requested to connect) to the H(e)NB are valid. Referring to Figure 2, the processor 220 would perform the functions of determining the change in the ID and other characteristics, and then the transmitter 250 would wirelessly send the notification message to the network.

[0047] The H(e)NB can perform a secure and trusted method to determine its own location with certainty. Such methods comprise the use of location detection methods such as GPS or assisted GPS (A-GPS), for instance, where the GPS/A-GPS devices, the interface from the GPS device to the H(e)NB's processor, and the programs and data associated with the H(e)NB's processor in regard to the location processing, are secured and made trustworthy.

[0048] The H(e)NB may have a tamper detection circuit which is capable of detecting physical tampering of the H(e)NB. In the event that the H(e)NB detects tampering, it may send an alert message indicating such tamper detection (or suspicion of tampering) to the carrier, owner and/or core network.

[0049] In another embodiment, if the H(e)NB determines a possible change in its location, depending on its connectivity and programmed configurations, it can implement by way of the processor 220 in conjunction with possible assistance from the memory 230, the transmitter 250, the USIM module 270, and TPM 280, as illustrated in Figure 2, any of the mechanisms listed below either individually or in any combination or implement other possible schemes as one skilled in the art will recognize:

[0050] 1) contact the Operator Core Network/RNC and report the change in location (with an indication of new location/IP address etc.), detected changes of WTRU ID's or changes in other characteristics of the WTRUs in the H(e)NB cell, and/or request that the Core Network/RNC send an update for the database of expected WTRUs , respective IDs and characteristics;

[0051] 2) trigger a locking mechanism;

[0052] 3) broadcast an out of service alert message to the WTRUs attempting to connect to the H(e)NB; and

[0053] 4) continue to operate and/or reconfigure its list of expected WTRU ID's and other WTRU characteristics (e.g. power capability of the WTRU, support for MIMO, modulation capability of WTRU, security algorithms supported by WTRU).

[0054] In another embodiment, the H(e)NB 200 includes a periodic timer which upon expiration causes the H(e)NB 200 to contact the Operator network. The Operator network then provides updated information for the H(e)NB DB. The H(e)NB can also contain a position detection device (GPS, etc.) that provides it with its the absolute location. The H(e)NB can be moved within a certain range of coordinates (say between different rooms or offices) without triggering an update to the H(e)NB DB.

[0055] If a major change in location (outside the range of allowed coordinates) is indicated by the position detection device, the H(e)NB, depending on its connectivity and programmed configurations, will implement the following mechanisms either individually or in any combination:

[0056] contact the operator core network and report its change in location with an indication of a new location, a new IP address and new detected neighbors. The H(e)NB may request updated neighbor list information;

[0057] trigger a locking mechanism;

[0058] broadcast an out of service alert message to the WTRUs attempting to connect to the H(e)NB; and

[0059] continue operating and/or reconfigure its location.

[0060] In another embodiment, an H(e)NB uses the location information, provided by a WTRU that it is serving, to determine whether its location has changed.

[0061] Alternatively, the H(e)NB detects a change in its location based on the IP address assigned to it (for example, if an IP address is assigned using dynamic host configuration protocol (DHCP) and is different from the one assigned earlier, or if any of the IP addresses of the network router to which the H(e)NB connects changes). A detection based on these parameters will cause the H(e)NB to, depending on its connectivity and programmed configurations, implement by way of the processor 220

and the transmitter 250, with possible assistance from the USIM module 270 and the TPM 280, any of the following location update procedures, either individually or in any combination:

[0062] contact the operator core network and report a change in location with an indication of a new location, a new IP address and new detected neighbors. The H(e)NB may request updated neighbor list information;

[0063] trigger a locking mechanism;

[0064] broadcast an out of service alert message to the WTRUs attempting to connect to the H(e)NB; and

[0065] continue operating and/or reconfigure its location.

[0066] In another embodiment, when the H(e)NB detects a change in its IP connectivity, it will implement a mobility mechanism such as Internet Engineering Task Force (IETF) compliant Client Mobile IP or Proxy Mobile IP, in the H(e)NB. This enables the H(e)NB to report its location change to the operator core network via a public IP network. The mobility mechanism may be enhanced by including an additional indication of the new absolute location by using, for example, a GPS chip or location information obtained from the WTRUs connecting to the H(e)NB.

[0067] In a conventional wireless communications system, a Node-B (NB) or an evolved Node-B ((e)NB) is programmed (for example, by O&M procedures, etc.) with a neighboring cell list (NCL). This technique works because the NCL does not change very often and conventional NBs and (e)NBs do not change location. In comparison, an H(e)NB may frequently change location, but at the same time must flexibly continue operation without requiring operator intervention.

[0068] A WTRU may detect information about the cells to which it can connect. Additionally, a given WTRU may be able to connect to cells not in the NCL of a NB or (e)NB to which it is connected. However, while such additional cell connection information may be detected by the WTRU, the WTRU is typically directed by a NB or (e)NB to only collect measurement information from cells that are listed in that NB's or (e)NB's respective NCL and transmit this measurement information to the respective NB or (e)NB.

[0069] In contrast, the H(e)NB can use this detected cell information to dynamically create its neighboring cell list, the H(e)NB NCL. In one embodiment, the H(e)NB sends messages to its WTRUs requesting that each WTRU send information about the cells to which it can connect (detected cell information). The WTRU sends this information to the H(e)NB in its measurement report. This detected cell information may be part of an existing measurement report using existing messages and data structures, or a new message, new data structure or information element may be used to store and transmit this detected cell information. The H(e)NB receives the detected cell information from each WTRU, processes the detected cell information and uses the detected cell information to generate its NCL.

[0070] In another embodiment, the H(e)NB is able to detect the type and characteristics of the physical layer connection to the operator core network/RNC, for example, digital subscriber line (DSL), cable modem, T1 connection or wireless, and report (indicate) this to the operator. In addition, the H(e)NB may choose to change some of its parameters. For example, in one embodiment, the H(e)NB offers multiple types (e.g.: graded) and levels of service based on the type and or characteristics of its connectivity methods to the core network/RNC. The H(e)NB may change any one or more of such characteristics including but not limited to: services offered, admission control parameters, and number of users supported, based on the capabilities of the underlying physical layer connection. The H(e)NB may also change additional characteristics that include, but are not limited to data rate, guaranteed throughput, maximum throughput, bit error rate, quality of service, air interface signaling, and other similar capabilities. In addition, the operator may change, via the core network, H(e)NB parameters such as services and security, depending on the type of connectivity available to the H(e)NB. Referring to Figure 2, the processor 220, with assistance from the receiver 210, and possibly also from the USIM module 270, and the TPM 280, may determine the type of the connectivity of the WTRU 200 and coordinate any response actions thereof.

[0071] As mentioned above, certain parameters of the H(e)NB are user configurable, independent of O&M, C-plane or operator signaling. This is unlike e-NB

re-configuration, which is operator controlled only. In one example embodiment, a user is be able to change the power level at which the H(e)NB operates to give it greater coverage. The H(e)NB preferably is pre-configured with a maximum power limit. A user can configure the power level, up to the specified limit, independent of the operator. Preferably, the H(e)NB implements a mechanism that allows a user to change other parameters, such as services offered to non-subscribed pedestrians. To enable this type of reconfiguration, the H(e)NB implements a mechanism that offers the user a suitable interface over an IP network with facilities similar to those provided by a WLAN AP. Referring to Figure 2, the processor 220, in conjunction with the USIM module 270 and/or the TPM 280, may perform coordination of the user-initiated reconfiguration of the H(e)NB parameters.

[0072] In another embodiment, the H(e)NB can vary parameters such as modulation technology, rate, and power level transmitted such that they are all within defined thresholds depending on the number of transmission errors it encounters and the transmission rate.

[0073] Alternatively, a power control mechanism can be applied to an H(e)NB along with adaptive modulation and coding (AMC). This will assist the H(e)NB in maintaining the required QoS to a WTRU.

[0074] In one embodiment, additional procedures are defined which simplify H(e)NB actions or services. For example, filtering measurements at L1 are simplified by using linear filtering instead of logarithmic filtering (considering the limited range and environment in which the H(e)NB operates), features like fractional dedicated physical channel (F-DPCH) in release 6 3GPP are made optional by use of special IEs in the H(e)NB. Additionally, the front end radio frequency (RF) are made simpler by not using transmitter (Tx) diversity. Such simplification is possible because the H(e)NB operates in a less complex environment than an eNodeB. Essentially an H(e)NB operates as a very simple and basic cellular base station offering only those services that are required. Referring to Figure 2, such new Information Elements (IE's) may be created and/or handled by the processor 220 and the memory 230, possibly with assistance from the USIM module 270 and even the TPM 280.

[0075] In another embodiment, H(e)NB functionality and credentials are remotely setup and modified under the control of the Operator Core Network by way of O&M/C-plane/operator signaling. Such functionality may be very beneficial to reducing the cost of H(e)NBs and also to 'reuse' H(e)NB hardware by remotely re-provisioning or migrating the functions. Examples of such remotely configurable functionality and credentials includes functionality for the following: cellular communication, communication with the Operator Core Network/RNC, secure management of the H(e)NB's ID and other credentials, management of downloadable USIM credentials and executables, management of downloadable security policies and configuration parameters, management of neighbor cells and/or 'expected' UEs, or attestation of the trustworthiness of the H(e)NB, and any credentials that are required to support such functionality listed above. Additionally, this capability enables the functionality of the H(e)NB to be enhanced in the future with capabilities such as a relay capability for cooperative communications, assisting the Operator to reach target UEs through enhancements of the H(e)NB, use of multiple air interfaces such as GSM/GPRS/Edge, WCDMA HSPA, WLAN, WiMAX etc. based upon various QoS metrics measured and gathered by the H(e)NB. Referring to Figure 2, the processor 220 would perform the coordinating role in the provisioning of the parameters or executables.

[0076] Techniques similar to those defined by the Trusted Computer Group (TCG) such as the use of Trusted Computer Platform (TPM) and/or Mobile Trust Module (MTM) and related commands may be used to allow H(e)NB functionality and credentials to be remotely managed (provision-able or migrate-able). In one embodiment, these methods and techniques allow remote attestation of the integrity of the H(e)NB platform to the Operator or other authorized challengers, secure and migrate-able (under secure authorization) storage and management of credentials and cryptographic keys, and secure encryption/decryption capability. In another embodiment, each H(e)NB is equipped with a TPM or an MTM, and these secure embedded devices enable the H(e)NB to provide secure remote provisioning and the migration of functions and credentials. Referring to Figure 2, the TPM (or a Mobile Trusted Module (MTM)) 280 may perform such integrity-attestation functionality.

[0077] The functions set forth above preferably require specific messages between the H(e)NB and the operator core network/RNC. In one embodiment, this information is sent in dedicated messages, as part of other existing messages or as Information Elements (IEs) and may be a part of O&M signaling or may be a part of standard S1-mobile management entity(MME)/S1-user plane entity(UPE)/X2 type signaling or any other type of new signaling.

[0078] Such messages, by way of example, include:

[0079] "location update". This indicates such information as a change in location of an H(e)NB to the core network, an anticipated change, access restrictions associated with that location, service parameters, security parameters and commands from the core network;

[0080] "WTRU List." This indicates a list of the WTRU IDs and other characteristics of WTRUs that are connected or requesting to connect to the H(e)NB.

[0081] "type of connectivity". This indicates the type of connectivity, for example, DSL or cable, that the H(e)NB has with the operator along with other characteristics of the connection, such as quality of service (QoS) support;

[0082] "reconfigured parameters". User configurable parameters include: services offered by the H(e)NB, some specific radio resource control (RRC) parameters such as values for power control, and the like. Such user reconfiguration may be performed independent of the operator. The H(e)NB could indicate these reconfigured parameters to the operator core network/controlling entity/RNC in a new IE or message that contains the user-configurable parameters;

[0083] "handover and reselection parameters". This includes parameters for handover and reselection from an H(e)NB to a macro-cell. Other H(e)NBs could also be signaled in the H(e)NB; and

[0084] "H(e)NB platform and functionality attestation." This includes new parameters and information for secure remote attestation of the H(e)NB's platform and/or functionality authenticity and integrity to the Operator Core Network or other authorized challengers.

[0085] Referring to Figure 2, these messages may be handled by the processor 220, in conjunction with the memory 230, USIM module 270, and TPM 280, and any response messages to the network may be transmitted by the transmitter 250.

[0086] In another embodiment the location of an H(e)NB may be defined in terms of its neighboring HNNs or by the associated HNN. H(e)NB mobility management is facilitated by maintaining a database of the location of each H(e)NB. For this purpose, functional entities similar to home location register (HLR) and visiting location register (VLR) are created in the network. In one embodiment, each HNN contains a database of all served H(e)NBs (similar to VLR functionality). In another embodiment the database could be placed in the Core Network, for example the Mobile Switching Center (MSC) or Serving GPRS Support Node (SGSN).

[0087] In one embodiment, an example RS deployment is illustrated in Figure 4, a Relay Station (RS) 470 is a special kind of H(e)NB. A RS 470 is typically considered to act as a "helper node" to facilitate and improve the communications between a BS 460 (which plays the role of HNN in Figure-1) and one or more WTRUs (480, 482, 484). The RS 470 is similar to a typical H(e)NB in that it provides local coverage in a macro-cell served by a HNN. Similarly, a RS 470 is typically a physically small and inexpensive node that can be easily installed and configured. Precisely due to these reasons, a RS 470 may exhibit a mode of mobility similar to that of a typical H(e)NB. Therefore, some of the mobility management solutions for the typical H(e)NB are directly applicable and/or extensible to the RSs. An example of the internal components of an RS 300 is illustrated in Figure 3. The RS 300 contains a Processor 320, a trusted platform module 380, a USIM 370, a GPS 360, a memory 330, a removable memory (e.g. a smart card) 340, a transmitter 310 and a receiver 350.

[0088] In one embodiment, a RS 470 communicates with one or more HNNs (e.g. BS 460) via a wireless link 462 which may use the same spectrum and signaling schemes as that used for communications by a WTRU 480 as shown in Figure 4. In Figure 4, the WTRUs 480, 482, 484 are connected to the RS 470 via respective wireless links 472, 474 and 476. The WTRUs are also able to communicate wirelessly with the BS 460 via links 464, 466, and 468. The BS 460 may be connected to a HNN 450 via

link 452 which could be wireless or hard-wired. The RS 470 registers itself through a registration procedure, which includes the verification of credentials via mutual (two-way) or unilateral (one-way) authentication. The registration data is stored in a database in the network. The database resides in the HNN 450 or another node in the network such as in the home subscriber server (HSS) in a 3GPP network which also contains HLR and VLR databases. In another embodiment, this data resides in a core network element, such as an SGSN or Gateway GPRS Support Node (GGSN). In non-3GPP networks, similar nodes are identified for storing the registration data.

[0089] The registration process is performed either at the time of installation and periodically at regular intervals of time (for example once a day), or as a response to a request by the network, or other similar conditions. As part of the registration process, a candidate RS may be denied registration, for example, if the authentication fails. Similarly, an RS may decide not to register with a particular HNN based on several criteria, which may include but are not limited to authentication, restrictions imposed by the HNN on the operation of the RS, and any economic factors relating to the usage of the HNN.

[0090] Following the registration process, is the process of Attachment. This process is dynamic process that executes frequently, involves the current state of an RS and the HNNs that it is poised to communicate with. Procedures similar to GPRS attach/detach may be employed here. For example, as described in 3GPP TS 24.008-780, Section 4.7.3, the RS sends an ATTACH REQUEST MESSAGE, which contains a number of RS attributes, such as RS Identity, Radio Access Capabilities, Ciphering details, etc. The RS Identity may be permanent or temporary. The Radio Access Capabilities may include RF Power Class, Multiple Antenna capabilities, Interference Cancellation capabilities, Handover capabilities as well as support for other radio technologies supported (e.g. UMTS FDD, LTE, CDMA2000 etc) [See 3GPP TS 24.008-780, Section 10.5.5.12a]. The BS examines the ATTACH REQUEST message and if acceptable and deemed useful for cooperative purposes, will transmit an ATTCH ACCEPT message.

[0091] An RS may attach with one or more HNNs. When it is attached to multiple HNNs, diversity techniques may be used for improved communications within a multi cell system.

[0092] The data that describes the location of an RS may take a form similar to the data that describes H(e)NB location. This data includes but is not limited to identity of the HNN to which the RS is attached; identities of the HNNs to which the RS is attached; identities of HNNs which are in the radio reception range of the RS (even though the RS is not attached to any or all of them); and identities of other RSs which are in the radio vicinity of the RS under consideration.

[0093] When a RS changes its state of registration or attachment, a number of procedures may be invoked. For example, if a RS is moved from its present location, this may trigger a new registration/attachment procedure at the new location. Similar to the concept of Home Network and Visited Network in Cellular Systems for WTRUs, RSs may also have a Home Network. Thus, when a RS moves to a network that is not its Home Network, i.e. a Visited Network, then the registration/attachment procedure in the Visited Network may involve a communication between the Visited and Home Networks for the purpose of authenticating the RS. RS roaming procedures similar to WTRU roaming procedures in current cellular systems may be used.

[0094] In another embodiment, a RS experiences a failure and ultimately stops working (complete failure). In such a case, prior to complete failure, the RS may communicate with the HNN and possibly other nodes in the core network and inform them of the change of status. This will trigger a de-attachment procedure. In another embodiment, the RS may be solar-powered (full or partial). The RS may wish to conserve power by shutting itself down. In another embodiment, the RS may be battery or solar-powered (full or partial). This is a particularly attractive way to power a RS because RSs are small, expected to be deployed in large numbers and operate unattended. Alternatively, the RS may wish to conserve power by using Idle (or Sleep) mode procedures similar to those performed by a WRTU connected to a BS. When the RS is in Idle mode, power utilization is minimized. In such a case, prior to

transitioning to Idle mode, the RS may send a message to notify the BS indicating such a transition.

[0095] An RS, which is unattached and possibly unregistered in a particular location with any HNN, advertises itself, seeking to know if any HNN requires its services. Specifically, the RS listens to the radio beacon signals and determines the presence of HNNs. Depending on the results, it selects suitable radios (assuming a RS is capable of multiple radio modes, such as GSM, WCDMA, WLAN etc) and sends advertisement messages. If the RS is a single mode device (a special case), it will skip searching for the radios and immediately advertise itself. Since HNNs know the nature of their radio coverage and coverage holes, etc., they are in a position to determine whether or not they need relay help. Therefore, using such criteria, the BS may choose to use the help of an advertised RS and negotiate terms of a contract. The contract may involve duration of assistance, nature of assistance, modes of assistance, etc. Subsequently, the RS 'sells' its services which includes registering and attaching with the HNN and upon the completion of the contract, de-registers and de-attaches itself with the HNN. This solution provides for a deployment scenario where a number of 3rd party radio helper RSs are possible. It may also encourage a type of tier-2 radio coverage providers and a secondary market.

Embodiments

1. An in-home Node-B (H(e)NB) comprising a global positioning system(GPS) or Assisted-GPS (A-GPS) system configured to determine a location.

2. The H(e)NB of embodiment 1 comprising:

a processor configured to:

perform a locking function that locks and unlocks parameters including at least one of a carrier controlled parameter and a user controlled parameter, and modifies at least one of the carrier controlled parameters and the user controlled parameters;

detect the location of the H(e)NB; and

detect if the H(e)NB has moved from the location.

3. The H(e)NB of embodiment 2 further comprising:

a universal subscriber identifier module (USIM) configured to store static parameters and assist in configuration upon startup;

a memory;

a removable memory configured to contain the locking function and parameters;

a network card configured for connecting to an IP network

a transmitter; and

a receiver.

4. The H(e)NB of embodiment 3 further comprising:

a secure hardware component providing a secure storage and execution environment.

5. The H(e)NB as in any one of embodiments 2-4, wherein the carrier controlled parameter includes a public land mobile network identifier (PLMN ID) that should be broadcasted by the H(e)NB.

6. The H(e)NB as in any one of embodiments 2-5, wherein the carrier controlled parameter includes an H(e)NB supported service comprising at least one of basic voice service, emergency call support, and high speed data support.

7. The H(e)NB as in any one of embodiments 2-6, wherein the carrier controlled parameter includes a security parameter comprising at least one of a locked parameter indicator, a protected data indicator, a security key, and a security algorithm.

8. The H(e)NB as in any one of embodiments 2-7, wherein the carrier controlled parameter includes a spectrum indicator that indicates the operational frequency of the H(e)NB.

9. The H(e)NB as in any one of embodiments 2-8, wherein the carrier controlled parameter includes a location of operation indicator and a tariff indicator.

10. The H(e)NB as in any one of embodiments 2-9, wherein the carrier controlled parameter is a locked parameter.

11. The H(e)NB as in any one of embodiments 2-10, wherein the USIM contains one or more parameters.

12. The H(e)NB as in any one of embodiments 2-11, wherein the memory contains one or more parameters.

13. The H(e)NB as in any one of embodiments 2-12, wherein the removable memory contains one or more parameters.

14. The H(e)NB as in any one of embodiments 2-13, wherein the removable memory comprises the locking function.

15. The H(e)NB as in any one of embodiments 2-14, wherein the removable memory comprises the locking function in a WTRU.

16. The H(e)NB as in any one of embodiments 2-15, wherein the locking function allows operation of the H(e)NB based at least in part on parameter values.

17. The H(e)NB as in any one of embodiments 2-16, wherein the locking function is enforced at the hardware level or by using a secure execution environment provided by trusted computing techniques.

18. The H(e)NB as in any one of embodiments 2-17, wherein the locking function performs at least one of stopping, shutting down, reducing the offered services, restricting admission control, resetting configuration parameters by sending operational and maintenance (O&M) signaling or control plane (C-plane) signaling to the operator, sending warning messages to the operator, and directly contacting the operator, if a user attempts to reconfigure H(e)NB parameters without authority.

19. The H(e)NB as in any one of embodiments 2-17, wherein the locking function allows WRTUs to connect to the H(e)NB only if the WTRUs are subscribed with the H(e)NB carrier.

20. The H(e)NB as in any one of embodiments 2-18, wherein the locking function ensures that the H(e)NB can be unlocked when predetermined criteria for operation are met.

21. The H(e)NB of embodiment 20, wherein predetermined criteria includes:

successful authentication of the H(e)NB or the owner of the H(e)NB;

successful verification of the context of the unlocking request by its owner or operator; and

successful verification of the attestation by the H(e)NB of its platform trustworthiness.

22. The H(e)NB as in any one of embodiments 2-21, wherein a locking function unlock command or locking command, along with modified parameters are received from the core network or radio network controller via signaling.

23. The H(e)NB as in any one of embodiments 2- 22, wherein a locking function command, along with modified parameters are received via Open Mobile Alliance (OMA) Device Management (DM) mechanisms.

24. The H(e)NB as in any one of embodiments 2-23, wherein the H(e)NB detects a change in its location by comparing at least one of a surrounding macro-cell identifier and neighbor cell identifier along with a corresponding radio strength, with at least one of an expected macro-cell identifier parameter and an expected neighbor cell identifier, and an expected corresponding radio strength.

25. The H(e)NB as in any one of embodiments 2-24, wherein the H(e)NB detects a change in its location by comparing a stored location parameter with at least one of the GPS or A-GPS determined location, a served wireless transmit/receive unit (WTRU) location, and a neighboring cell WTRU location.

26. The H(e)NB as in any one of embodiments 2-25, wherein the H(e)NB transmits a request to update its neighbor list if a neighboring cell has changed and the H(e)NB location has not changed.

27. The H(e)NB as in any one of embodiments 2-26, wherein if the H(e)NB determines that its location might have changed, the H(e)NB will perform at least one of the following:

contact the operator core network and report a change in location with an indication of the new location/new IP address, and any detected neighbors

request updated neighbor list information;

institute a trigger locking mechanism;

broadcast an out of service alert message to the WTRUs attempting to connect to the H(e)NB;

continue operating or reconfigure its neighbor list on its own; and

upon expiration of a timer, request an updated neighbor list.

28. The H(e)NB as in any one of embodiments 2-27, wherein the H(e)NB can operate within a range of locations including:

a home;

an office;

an alternative office;

a retail building; and

an area adjacent to a home, office or retail building.

29. The H(e)NB as in any one of embodiments 2-28, wherein the H(e)NB initiates a location update procedure if a stored serving higher network node (HNN) identity is different from an advertised serving higher network node (HNN) identity.

30. The H(e)NB as in any one of embodiments 2-29, wherein at least one of the processor, the secure hardware component, the USIM, the memory, and the removable memory contains an information database (H(e)NB DB) comprising:

WTRU information further comprising:

a WTRU identifier (ID);

expected values for WTRU parameters including:

a power capability of the WTRU;

an indicator that the WTRU supports Multiple Input Multiple Output (MIMO);

a modulation capability of WTRU; and

security algorithms supported by WTRU;

validation information; and

authentication information.

31. The H(e)NB of embodiment 30, wherein the H(e)NB DB information is programmed.

32. The H(e)NB in any one of embodiments 30-31, wherein the H(e)NB DB information is acquired from WTRUs connected to the H(e)NB.

33. The H(e)NB as in any one of embodiments 30-32, wherein the H(e)NB sends a change alert message or requests verification of changed information, if the H(e)NB has not moved and the H(e)NB detects a change in the H(e)NB DB information.

34. The H(e)NB as in any one of embodiments 2-33, wherein the H(e)NB detects a change in its location by comparing a first assigned IP address with a second assigned IP address.

35. The H(e)NB as in any one of embodiments 2-34, wherein if the H(e)NB detects a change in its location, the H(e)NB performs at least one of the following:

contact the operator core network and report a change in location with an indication of a new location, a new IP address and new detected neighbors;

request updated neighbor list information;

trigger a locking mechanism;

broadcast an out of service alert message to the WTRUs attempting to connect to the H(e)NB;

continue operating and/or reconfigure its location; and

implement an Internet Engineering Task Force (IETF) mobility mechanism that enables the H(e)NB to report its location change via a public IP network.

36. The H(e)NB as in any one of embodiments 2-35, wherein the H(e)NB detects the type and characteristics of the physical layer connection to the operator core network (CN) or radio network controller (RNC) wherein the physical layer comprises at least one of Wideband Code Division Multiple Access (WCDMA) High Speed Packet Access (HSPA), Global System for Mobile Communication (GSM)

Edge Radio Access Network (GERAN), Wireless Local Area Network (WLAN) , Digital Subscriber Line (DSL), cable and Worldwide Interoperability for Microwave Access (WiMAX), based upon quality of service (QoS) metrics measured and gathered by the H(e)NB and using QoS parameters stored in the H(e)NB DB.

37. The H(e)NB as in any one of embodiments 2-36, wherein the H(e)NB changes at least one of

services offered, admission control parameters, and number of users supported,

based on the capabilities of the underlying physical layer connection.

38. The H(e)NB as in any one of embodiments 2-37, wherein the H(e)NB changes at least one of data rate, guaranteed throughput, maximum throughput, bit error rate, air interface signaling, and quality of service.

39. The H(e)NB as in any one of embodiments 2-38, wherein the processor is further configured to provide procedures to simplify H(e)NB actions or services.

40. The H(e)NB as in any one of embodiments 2-39, wherein the parameters are remotely configurable.

41. The H(e)NB as in any one of embodiments 2-40, wherein messages are sent and received that contain signaling information comprising at least one of the following:

a "location update" that indicates information including at least one of a change in location of a H(e)NB to the core network, an anticipated change, access restrictions associated with that location, service parameters, security parameters and commands from the core network;

a "WTRU list" that further comprises a list of the WTRU IDs that are connected or requesting to connect to the H(e)NB;

a" type of connectivity" that indicates the type of connectivity including DSL or cable, that the H(e)NB has with the operator and includes quality of service (QoS) support information;

"reconfigured parameters" that indicates user configurable parameters including: services offered by the H(e)NB, specific radio resource control (RRC) parameters further including values for power control.

"handover and reselection parameters" that specifies parameters for handover and reselection from an H(e)NB to a macro-cell or to another H(e)NB; and

"H(e)NB platform and functionality attestation" that specifies new parameters and information for secure remote attestation of the H(e)NB's platform or functionality, authenticity and integrity.

42. The H(e)NB as in any one of embodiments 2-41, wherein the messages are dedicated messages, part of existing messages or as Information Elements (IE)s.

43. A method for wireless communications comprising configuring a in-home Node-B (H(e)NB).

44. The method of embodiment 43 comprising locking and unlocking parameters, in a locking function, including at least one of a carrier controlled parameter and a user controlled parameter, and modifying at least one of the carrier controlled parameters and the user controlled parameters.

45. The method of embodiment 43 comprising detecting a location of the H(e)NB.

46. The method of embodiment 43 comprising detecting if the H(e)NB has moved from the location.

47. The method as in any one of embodiments 44-46, wherein the carrier controlled parameter includes:

a public land mobile network identifier (PLMN ID) that should be broadcasted by the H(e)NB;

an H(e)NB supported service comprising at least one of basic voice service, emergency call support, and high speed data support;

a security parameter comprising at least one of a locked parameter indicator, a protected data indicator, a security key, and a security algorithm;

a spectrum indicator that indicates the operational frequency of the H(e)NB;

a location of operation indicator; and

a tariff indicator.

48. The method as in any one of embodiments 44-47, wherein the carrier controlled parameter is a locked parameter.

49. The method as in any one of embodiments 44-48, further comprising storing the locking function and one or more parameters in a universal subscriber identifier module (USIM).

50. The method as in any one of embodiments 44-49, further comprising storing the locking function and one or more parameters in a removable memory.

51. The method as in any one of embodiments 44-50, further comprising storing the locking function and one or more parameters in a trusted platform module (TPM).

52. The method as in any one of embodiments 44-51, wherein the locking function further comprises allowing operation of the H(e)NB based at least in part on parameter values.

53. The method as in any one of embodiments 44-52, wherein the locking function further comprises enforcing the locking function at the hardware level or

enforcing the locking function by trusted computing techniques.

54. The method as in any one of embodiments 44-53, wherein the locking function further comprises performing at least one of stopping, shutting down, reducing the offered services, restricting admission control, resetting configuration parameters by sending operational and maintenance (O&M) signaling or control plane (C-plane) signaling to the operator, sending warning messages to the operator, and directly contacting the operator, if a user attempts to reconfigure H(e)NB parameters without authority.

55. The method as in any one of embodiments 44-54, wherein the locking function further comprises allowing wireless transmit/receive units (WTRU)s to connect to the H(e)NB only if the WTRUs are subscribed with the H(e)NB carrier.

56. The method as in any one of embodiments 44-55, wherein the locking function further comprises ensuring that the H(e)NB can be unlocked when predetermined criteria for operation are met.

57. The method as in any one of embodiments 44-56, wherein predetermined criteria includes:

authenticating the H(e)NB or the owner of the H(e)NB;

verifying a context of the unlocking request; and

verifying an attestation by the H(e)NB of its platform trustworthiness.

58. The method as in any one of embodiments 44-57, wherein the locking function further comprises receiving the unlock command or the locking command, along with modified parameters.

59. The method as in any one of embodiments 44-58, wherein the detecting a change in its location comprises comparing at least one of a surrounding macro-cell

identifier and neighbor cell identifier along with a corresponding radio strength, with at least one of an expected macro-cell identifier parameter and an expected neighbor cell identifier, and an expected corresponding radio strength.

60. The method as in any one of embodiments 44-59, wherein the detecting a change in its location comprises comparing a stored location parameter with at least one of the GPS or A-GPS determined location, a served wireless transmit/receive unit (WTRU) location, and a neighboring cell WTRU location.

61. The method as in any one of embodiments 44-60, further comprising transmitting a request to update its neighbor list if a neighboring cell has changed and the H(e)NB location has not changed.

62. The method as in any one of embodiments 44-61 further comprising performing at least one of the following, if the H(e)NB determines that its location might have changed:

contacting the operator core network and report a change in location with an indication of the new location/new IP address, and any detected neighbors

requesting updated neighbor list information;

instituting a trigger locking mechanism;

broadcasting an out of service alert message to the WTRUs attempting to connect to the H(e)NB;

continuing operating or reconfigure its neighbor list on its own; and

upon expiration of a timer, requesting an updated neighbor list.

63. A method for generating detected cell information by a WTRU comprising:

storing additional detected cell information;

receiving a request from a H(e)NB to transmit the detected cell information; and

transmitting the detected cell information to the H(e)NB.

64. A method for creating a neighboring cell list (NCL) in a H(e)NB comprising:

sending a request to a WTRU for detected cell information;

receiving the detected cell information from the WTRU; and

processing detected cell information to generate the NCL.

65. A Relay Station (RS) comprising an in-home Node-b (H(e)NB).

66. The RS of embodiment 65 comprising a global positioning system(GPS) or Assisted-GPS (A-GPS) system configured to determine a location.

67. The RS of embodiment 65 comprising a processor configured to

perform a locking function that locks and unlocks parameters including at least one of a carrier controlled parameter and a user controlled parameter, and modifies at least one of the carrier controlled parameters and the user controlled parameters;

detect the location of the H(e)NB; and

detect if the H(e)NB has moved from the location.

68. The RS as in any of embodiments 66-67, further comprising:

a universal subscriber identifier module (USIM) configured to store static parameters and assist in configuration upon startup;

a memory;

a removable memory configured to contain the locking function and parameters;

a transmitter; and

a receiver.

69. The RS as in any of embodiments 66-68, further comprising:

a secure hardware component providing a secure storage and execution

environment.

70. The RS as in any of embodiments 66-69, wherein the carrier controlled parameter includes:

a public land mobile network identifier (PLMN ID) that should be broadcasted by the H(e)NB;

an H(e)NB supported service comprising at least one of basic voice service, emergency call support, and high speed data support;

a security parameter comprising at least one of a locked parameter indicator, a protected data indicator, a security key, and a security algorithm;

a spectrum indicator that indicates the operational frequency of the H(e)NB;

a location of operation indicator; and

a tariff indicator.

71. The RS as in any of embodiments 66-70, wherein the carrier controlled parameter further includes:

a RS Identity;

a Radio Access Capability further comprising:

a RF Power Class;

a Multiple Antenna capability indicator;

an Interference Cancellation capability indicator; and

Handover capabilities; and

Ciphering details.

72. The RS as in any of embodiments 66-71, wherein at least one of the processor, the secure hardware component, the USIM, the memory, and the removable memory contains an information database (H(e)NB DB) comprising:

WTRU information further comprising:

a WTRU identifier (ID);

RS identities (IDs);

mode indicator that indicates if the RS is in idle mode;

expected values for WTRU parameters including:

a power capability of the WTRU;

an indicator that the WTRU supports Multiple Input Multiple Output (MIMO);

a modulation capability of WTRU; and

security algorithms supported by WTRU;

validation information; and

authentication information.

73. A method for conserving power by a relay station (RS) comprising:

entering idle mode; and

sending a mode indicator.

74. A method comprising obtaining services by a relay station (RS).

75. The method of embodiment 74 comprising listening to determine the presence of a higher network node (HNN).

76. The method of embodiment 74 comprising advertising to a HNN.

77. The method of embodiment 74 comprising receiving a contract for assistance including at least one of a duration of assistance, a nature of assistance and a mode of assistance.

78. The method of embodiment 74 comprising selling its services.

79. The method as in any one of embodiments 75-78, further comprising selecting a radio.

[0096] Although the features and elements of the present invention are described in the preferred embodiments in particular combinations, each feature or element can

be used alone without the other features and elements of the preferred embodiments or in various combinations with or without other features and elements of the present invention. The methods or flow charts provided in the present invention may be implemented in a computer program, software, or firmware tangibly embodied in a computer-readable storage medium for execution by a general purpose computer or a processor. Examples of computer-readable storage mediums include a read only memory (ROM), a random access memory (RAM), a register, cache memory, semiconductor memory devices, magnetic media such as internal hard disks and removable disks, magneto-optical media, and optical media such as CD-ROM disks, and digital video disks (DVDs).

[0097] Suitable processors include, by way of example, a general purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Arrays (FPGAs) circuits, any other type of integrated circuit (IC), and/or a state machine.

[0098] A processor in association with software may be used to implement a radio frequency transceiver for use in a wireless transmit receive unit (WTRU), user equipment (UE), terminal, base station, radio network controller (RNC), or any host computer. The WTRU may be used in conjunction with modules, implemented in hardware and/or software, such as a camera, a video camera module, a videophone, a speakerphone, a vibration device, a speaker, a microphone, a television transceiver, a hands free headset, a keyboard, a Bluetooth® module, a frequency modulated (FM) radio unit, a liquid crystal display (LCD) display unit, an organic light-emitting diode (OLED) display unit, a digital music player, a media player, a video game player module, an Internet browser, and/or any wireless local area network (WLAN) module.

* * *

CLAIMS

1. A Home evolved Node-B (HeNB) comprising:

a processor configured to:

initiate a platform validation procedure for validating the integrity of the HeNB; and

receive and maintain trust related credentials through a remote provisioning procedure on a condition that the platform validation is successful; and

trigger a locking function on a condition that the platform validation procedure is not successful.

2. The HeNB of claim 1, wherein the processor is a trusted processing module.

3. The HeNB of claim 1, wherein the processor includes a secure execution environment.

4. The HeNB of claim 1 wherein initiating the validation procedure includes sending an attestation of the platform's trustworthiness to a network entity.

5. The HeNB of claim 4 wherein the validation procedure is successful on a condition that verification successful message is received in response to the attestation.

6. The HeNB of claim 1 wherein initiating a validation procedure includes verifying a location of the HeNB.

7. The HeNB of claim 6 wherein verifying the location of HeNB is performed by verifying a current neighbor list.

8. The HeNB of claim 6 wherein verifying the location of HeNB is performed by using an Internet Protocol (IP) address.

9. A method of securing communication at a Home evolved Node-B (HeNB), the method comprising:

initiating a platform validation procedure for validating the integrity of the HeNB; and

receiving and maintaining trust related credentials through a remote provisioning procedure on a condition that the platform validation is successful; and

triggering a locking function on a condition that the platform validation procedure is not successful.

10. The method of claim 9 wherein initiating the validation procedure includes sending an attestation of the trustworthiness of the platform to a network entity.

11. The method of claim 10 wherein the validation procedure is successful on a condition that verification successful message is received in response to the attestation.

12. The method of claim 9 wherein initiating a validation procedure includes verifying a location of the HeNB.

13. The method of claim 12 wherein verifying the location of HeNB is performed by verifying a current neighbor list.

14. The method of claim 12 wherein verifying the location of HeNB is performed by using an Internet Protocol (IP) address.

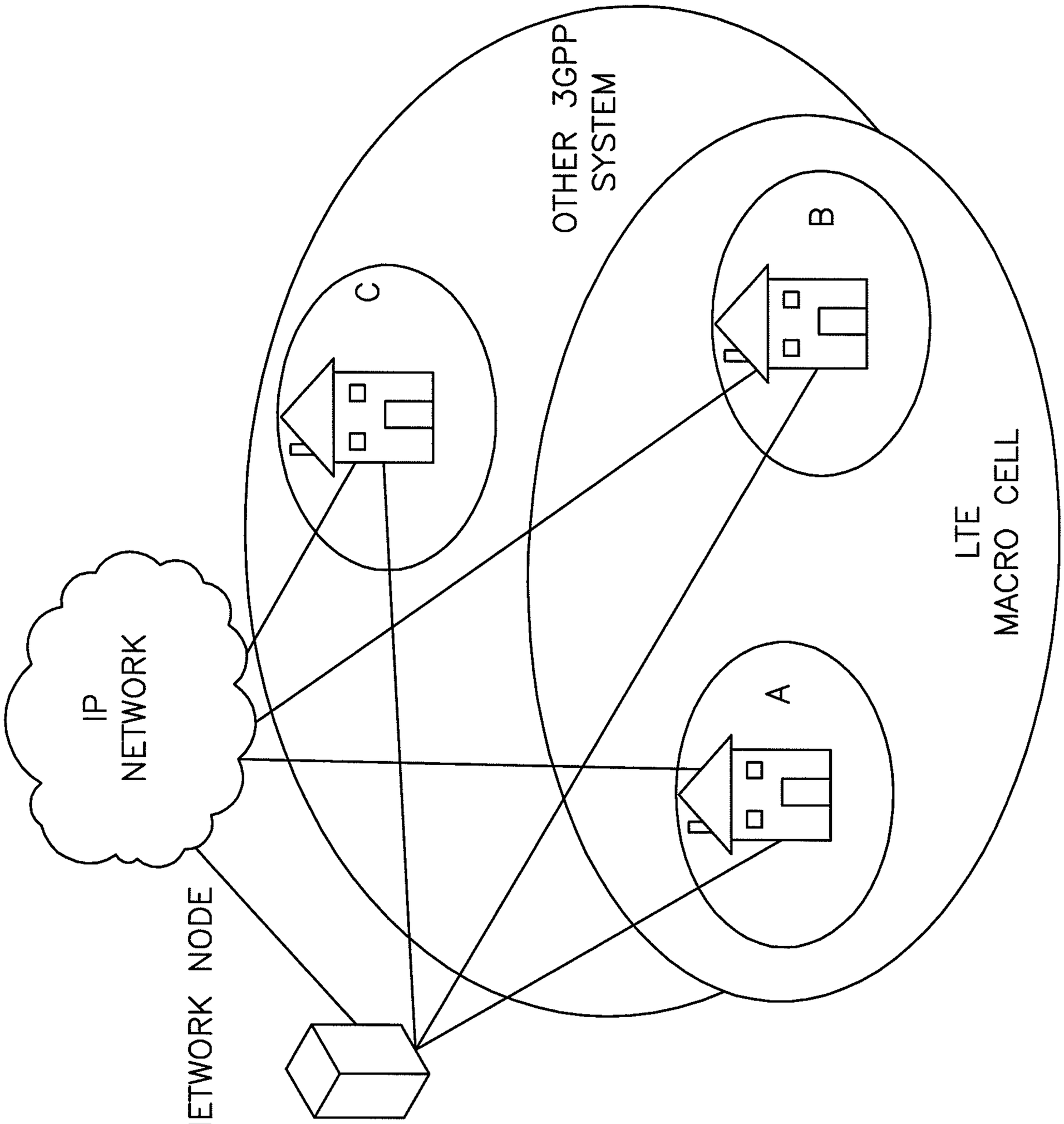

HIGHER NETWORK NODE
IP NETWORK
OTHER 3GPP SYSTEM
LTE MACRO CELL
A
B
C

FIG.1

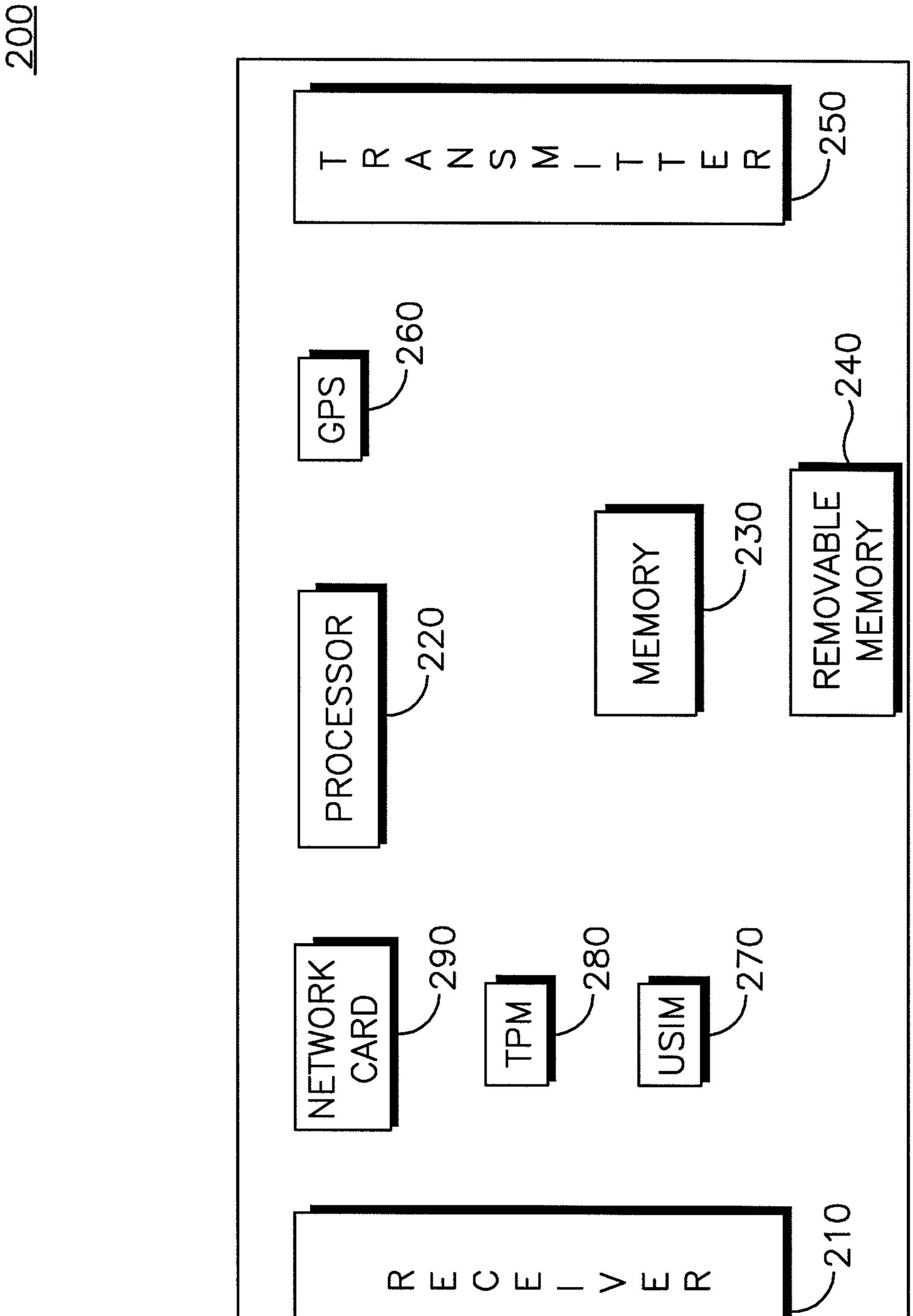

200
RECEIVER
210
TRANSMITTER
250
GPS
260
PROCESSOR
220
MEMORY
230
REMOVABLE MEMORY
240
NETWORK CARD
290
TPM
280
USIM
270

FIG.2

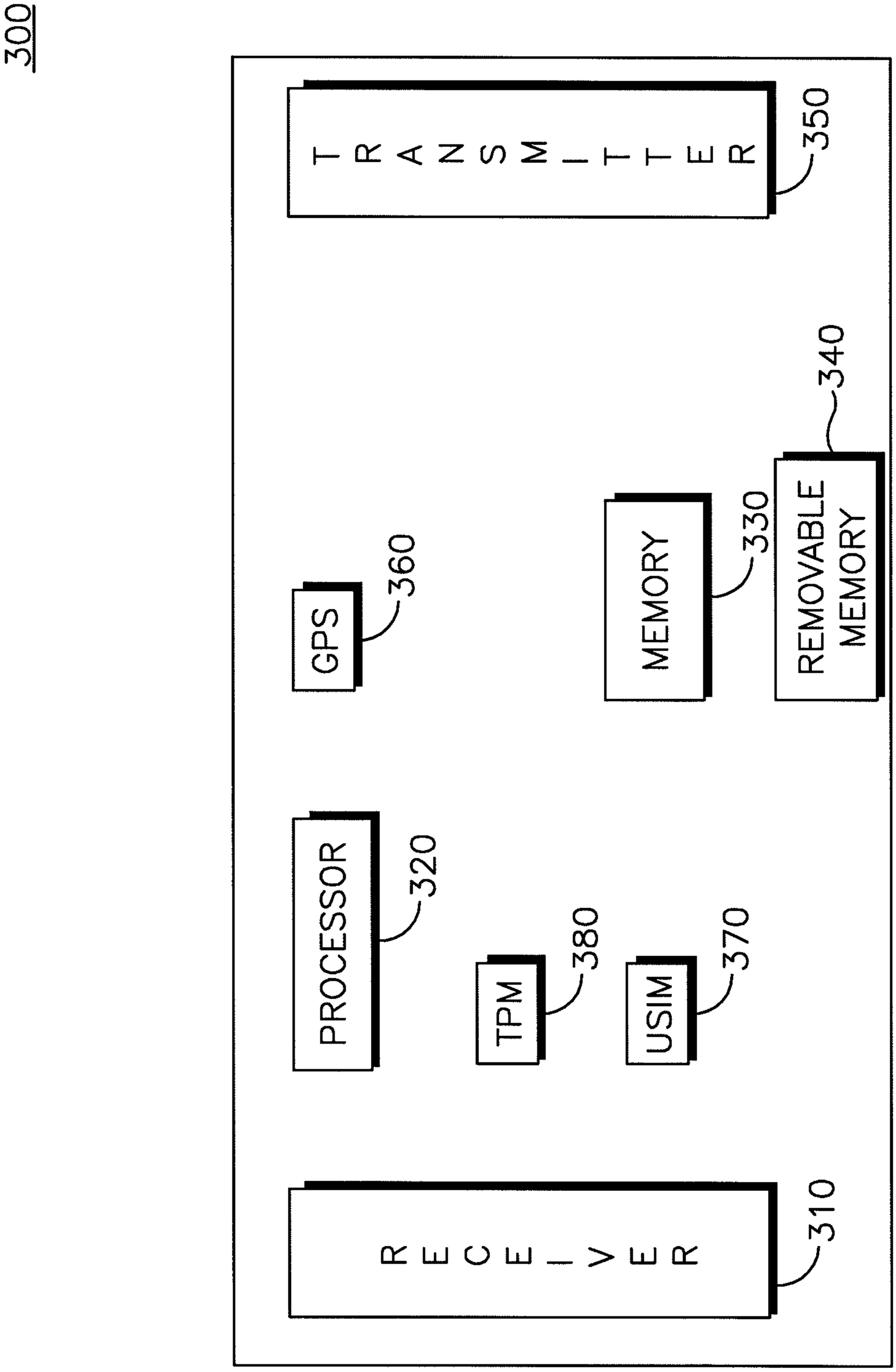

300
TRANSMITTER
350
GPS
360
MEMORY
330
REMOVABLE MEMORY
340
PROCESSOR
320
TPM
380
USIM
370
RECEIVER
310

FIG. 3

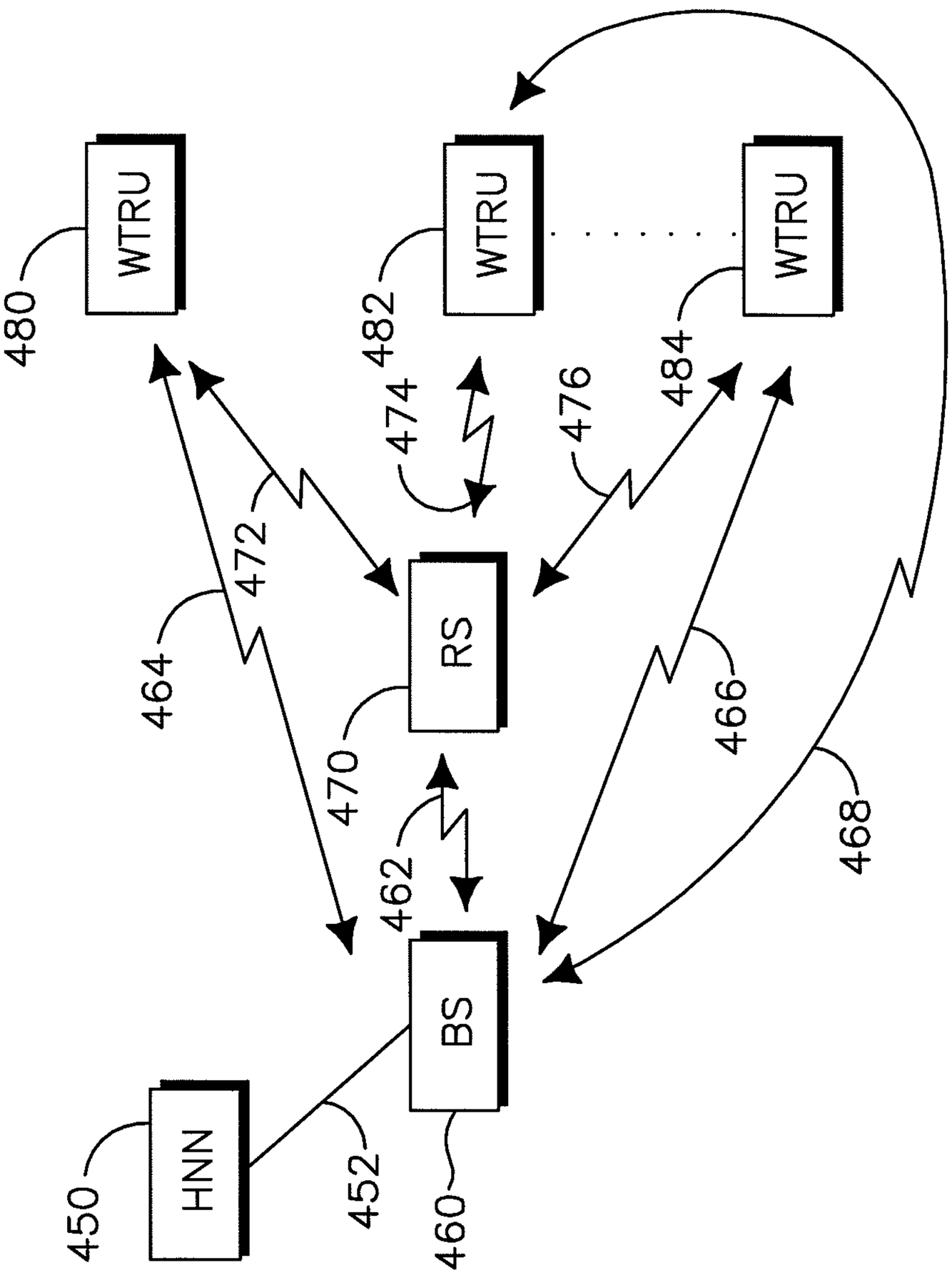
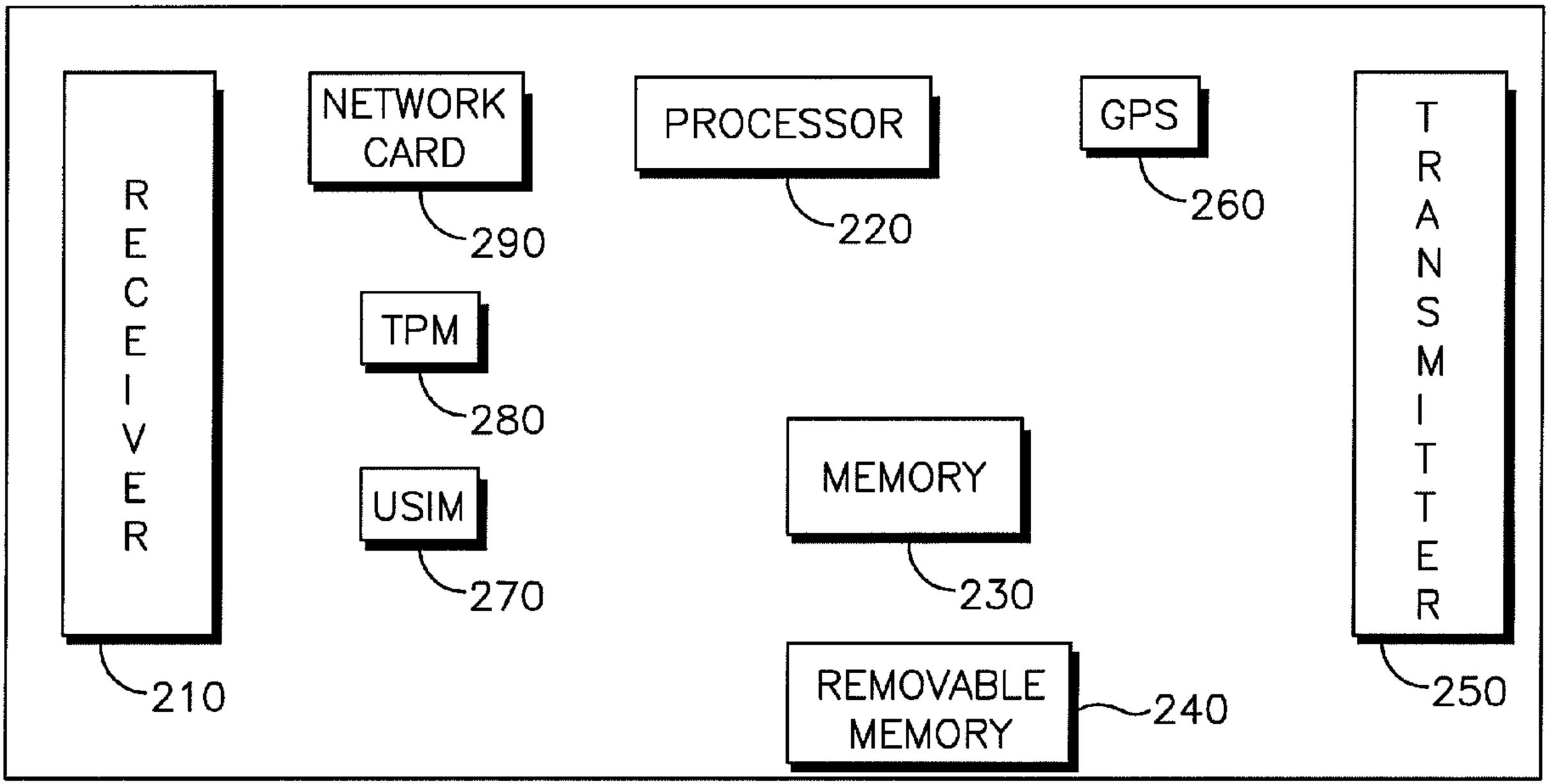

WTRU
480
WTRU
482
WTRU
484
474
476
464
472
RS
470
466
462
468
BS
HNN
450
452
460

FIG.4


RECEIVER
210
NETWORK CARD
290
TPM
280
USIM
270
PROCESSOR
220
MEMORY
230
REMOVABLE MEMORY
240
GPS
260
TRANSMITTER
250