(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
23 décembre 2004 (23.12.2004)

PCT

(10) Numéro de publication internationale
WO 2004/111970 A2

(51) Classification internationale des brevets[7] : G08C 17/02

(21) Numéro de la demande internationale : PCT/FR2004/001401

(22) Date de dépôt international : 4 juin 2004 (04.06.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
03/06907 6 juin 2003 (06.06.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **WAVECOM** [FR/FR]; Immeuble Bord de Seine I, 3, esplanade du Foncet, F-92442 Issy-les-Moulineaux Cedex (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **FABLET, Eric** [FR/FR]; 6, rue Pestalozzi, F-75005 Paris (FR).

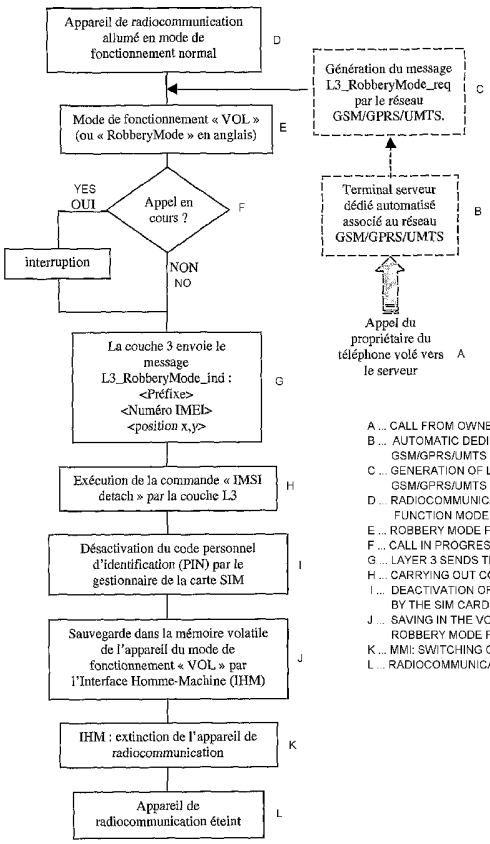
(74) Mandataire : **VIDON, Patrice**; Cabinet Patrice Vidon, 16B, rue de Jouanet, Boîte postale 90333, F-35703 Rennes Cedex 7 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE FOR PREVENTING THEFT OF A RADIOCOMMUNICATION DEVICE

(54) Titre : PROCEDE ET DISPOSITIF DE LUTTE CONTRE LE VOL D'UN APPAREIL DE RADIOCOMMUNICATION



A ... CALL FROM OWNER OF STOLEN TELEPHONE TO THE SERVER
B ... AUTOMATIC DEDICATED SERVER TERMINAL CONNECTED TO GSM/GPRS/UMTS NETWORK
C ... GENERATION OF L3_ROBBERYMODE_REQ MESSAGE BY GSM/GPRS/UMTS NETWORK
D ... RADIOCOMMUNICATION DEVICE SWITCHED ON IN NORMAL FUNCTION MODE
E ... ROBBERY MODE FUNCTION
F ... CALL IN PROGRESS?
G ... LAYER 3 SENDS THE MESSAGE L3_ROBBERYMODE_IND:
H ... CARRYING OUT COMMAND ΠIMSI DETACHΠ BY THE LAYER L3
I ... DEACTIVATION OF PERSONAL IDENTIFICATION NUMBER (PIN) BY THE SIM CARD MANAGER
J ... SAVING IN THE VOLATILE MEMORY OF THE DEVICE OF THE ROBBERY MODE FUNCTION BY THE MAN-MACHINE-INTERFACE (MMI)
K ... MMI: SWITCHING OFF THE RADIOCOMMUNICATION DEVICE
L ... RADIOCOMMUNICATION DEVICE SWITCHED OFF

(57) Abstract: The invention relates to a method and a device for preventing theft of a radiocommunication device. Such a method particularly comprises a step of calling the radiocommunication device, by the owner thereof once stolen and a step of transmission of at least one secret code, initiating an automatic execution of at least one specific operation, designed to prevent the use of the radiocommunication device and/or to alert at least one third party of the situation.

(57) Abrégé : L'invention concerne un procédé et dispositif de lutte contre le vol d'un dispositif de radiocommunication. Un tel procédé comprend en particulier une étape d'appel du dispositif de radiocommunication, par le titulaire de ce dernier, lorsqu'il a été dérobé, et une étape de transmission d'au moins un code confidentiel, entraînant la mise en oeuvre automatique d'au moins une opération spécifique destinée à empêcher l'utilisation du dispositif de radiocommunication et/ou à avertir au moins un tiers de la situation.

WO 2004/111970 A2

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* **:** ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

Procédé et dispositif de lutte contre le vol d'un appareil de radiocommunication.

1. Domaine de l'invention

Le domaine de l'invention est celui des radiocommunications.

Plus précisément, l'invention concerne la sécurisation d'appareils de radiocommunication, par exemple du type téléphone mobile. L'invention s'applique notamment, mais non exclusivement, à la lutte contre le vol de tels appareils.

2. L'art antérieur

Aujourd'hui, lorsqu'un individu se fait dérober son téléphone mobile, il est d'abord contraint de retrouver le numéro de téléphone du service de déclaration de vol de son opérateur, puis de trouver un autre téléphone (il n'a plus le sien !), et par exemple une cabine téléphonique publique, pour l'aviser de la situation. Une fois l'opérateur informé du vol par le propriétaire du téléphone mobile, un temps de latence d'environ trente minutes, voir plus, peut s'écouler avant que la désactivation à distance de la carte SIM (pour « Suscriber Identification Module » en anglais) de ce dernier ne soit effective.

Par conséquent, entre le moment où le téléphone mobile est dérobé à son propriétaire et le moment où le fonctionnement de ce dernier est neutralisé par l'opérateur, par une désactivation à distance de la carte SIM, il peut donc s'écouler jusqu'à plusieurs heures, durant lesquelles de nombreux appels téléphoniques coûteux peuvent être passés (appels téléphoniques à l'étranger, téléchargement haut débit de données multimédia, visiophonie, etc.).

De plus, si le propriétaire du téléphone mobile ne connaît pas le code unique d'identification de son téléphone portable, plus connu sous le nom de numéro IMEI (pour « International Mobile Suscriber Identity » en anglais), l'opérateur en charge de l'abonnement associé à ce téléphone ne disposera alors d'aucun moyen pour mettre ce dernier hors service à distance. Le téléphone volé reste alors définitivement utilisable et/ou revendable par le voleur.

Il n'existe pas à l'heure actuelle, d'autre solution que la solution précitée concernant la mise hors service à distance du téléphone mobile par l'opérateur en charge de l'abonnement de son propriétaire est connue à ce jour.

Cependant, une telle solution présente cependant pour inconvénients principaux d'une part que le propriétaire du téléphone soit dans l'obligation de connaître le numéro d'appel du service de déclaration des vols de son opérateur téléphone et d'autre part, qu'il ait connaissance ou en sa possession, le numéro d'identification international (numéro IMEI, ou « International Mobile Equipment Identity » en anglais) de son téléphone, sans lequel le fonctionnement de ce dernier ne pourra jamais être neutralisé.

3. Objectifs de l'invention

L'invention a notamment pour objectif de pallier ces inconvénients principaux de l'art antérieur.

Plus précisément, un objectif de l'invention est de fournir un dispositif ou appareil, et un procédé permettant d'obtenir rapidement et facilement la mise hors service d'un appareil de radiocommunication et/ou de sa carte SIM, suite à son/leur vol.

Ainsi, un objectif de l'invention est de fournir un dispositif et procédé permettant de limiter au maximum le délai séparant le moment où le propriétaire constate le vol de son téléphone mobile du moment où la mise hors service de celui-ci sera rendue effective.

Un objectif complémentaire de l'invention est de fournir un dispositif et procédé permettant à son propriétaire de s'affranchir de la connaissance de l'identifiant unique IMEI de l'appareil de radiocommunication pour mettre hors service celui-ci.

Un autre objectif de l'invention est de fournir un dispositif et un procédé qui permette à un individu de garder un contrôle à distance sur son appareil de radiocommunication, en particulier suite au vol de ce dernier.

Un objectif supplémentaire de l'invention est de fournir un dispositif et un procédé qui soient très simples et très rapides d'utilisation.

4. Caractéristiques principales de l'invention

Ces objectifs, ainsi que d'autres qui apparaîtront par la suite sont atteints à l'aide d'un procédé de lutte contre le vol d'un dispositif ou appareil de radiocommunication. Un tel procédé comprend avantageusement une étape d'appel du dispositif de radiocommunication, par le titulaire de ce dernier, lorsqu'il a été dérobé, et une étape de transmission d'au moins un code confidentiel, entraînant la mise en œuvre automatique d'au moins une opération spécifique destinée à empêcher l'utilisation du dispositif de radiocommunication et/ou à avertir au moins un tiers de la situation.

Préférentiellement, la ou les opérations spécifiques appartiennent au groupe comprenant :

- l'invalidation de la carte de contrôle (SIM) ;
- l'invalidation ou l'extinction dudit dispositif ;
- la transmission d'un message à un opérateur et/ou à un autre tiers ;
- l'émission de données de localisation ;
- l'interruption d'une communication ou d'une application en cours.

Avantageusement, le code confidentiel peut être transmis sous au moins une des formes suivantes :

- messages courts (SMS) ;
- codes DTMF ;
- messages vocaux.

De façon avantageuse, le code confidentiel est transmis au dispositif ou appareil de radiocommunication au moyen d'un autre terminal appartenant au groupe comprenant :

- téléphone mobile ;
- téléphone fixe ;
- appareil connecté à un réseau de communication du type Internet.

Dans un autre mode de réalisation de l'invention, le code confidentiel est avantageusement contenu dans un message protocolaire transmis au dispositif ou appareil de radiocommunication au moyen d'un terminal serveur dédié et automatisé.

L'utilisateur peut donc transmettre le code confidentiel à son téléphone

mobile qui lui a été dérobé, soit directement et personnellement en utilisant un autre téléphone mobile ou fixe, soit indirectement en sollicitant un terminal serveur dédié et automatisé mis à disposition par l'opérateur en charge de son forfait, ce terminal dédié ayant en charge de transmettre le message protocolaire contenant le code confidentiel et/ou un autre code secret à destination du terminal de communication volé.

De façon préférentielle, le procédé selon l'invention comprend une étape de désactivation du code d'identification personnel (PIN) en rentrant automatiquement un code erroné un nombre de fois supérieur au seuil autorisé.

Avantageusement, l'opération spécifique correspond à la génération d'un message de signalisation avec une en-tête spécifique, dans le cas du mode de réalisation utilisant un serveur dédié automatisé pour transmettre le message protocolaire au dispositif de radiocommunication.

De façon également avantageuse, le dispositif selon l'invention comprend au moins certaines des étapes suivantes de :

- réception par le dispositif de radiocommunication d'une requête et/ou d'un message, pour le déclenchement de la mise hors service ;
- passage de la couche IHM (Interface Homme-Machine) et/ou de la couche L3 dans l'état « mode vol » ;
- interruption de toute communication en cours et/ou verrouillage du dispositif ;
- transmission par l'appareil de radiocommunication d'un message à destination de l'opérateur en charge de l'abonnement téléphonique associé au dispositif dérobé ;
- exécution par la couche L3 (Layer 3 de la norme OSI) de l'appareil de radiocommunication de l'action IMSI_detach, pour la dés-inscription du dispositif de la base de données d'un enregistreur de localisation des visiteurs (VLR pour « Visitor Location Register » en anglais) ;
- mise dans l'état inactif du code personnel d'identité (code PIN) par le gestionnaire de la carte SIM du dispositif ;
- mémorisation d'une information représentative de l'état « volé » dans une

mémoire du dispositif ;

- extinction automatique du dispositif par coupure de l'alimentation électrique.

Le message à destination de l'opérateur comprend avantageusement :

- une en-tête prédéfinie signifiant le vol du dispositif ;
- le numéro IMEI, identifiant unique du dispositif.

De façon préférentielle, le procédé de lutte contre le vol selon l'invention comprend une étape de positionnement par des moyens de géo localisation intégrés au dispositif.

De façon également préférentielle, la mémoire de l'appareil est une mémoire non volatile programmable et réinscriptible du type appartenant au groupe comprenant :

- les mémoires EEPROM ;
- les mémoires FLASH.

Avantageusement, selon le procédé selon l'invention, on envoie trois fois un faux code PIN au dispositif, de façon à le verrouiller.

L'invention concerne également un dispositif de radiocommunication comprenant avantageusement des moyens de réception d'au moins un code confidentiel, émis par le titulaire du dispositif et/ou un autre terminal dédié automatisé, lorsqu'il a été dérobé, entraînant la mise en œuvre automatique d'au moins une opération spécifique destinée à empêcher son utilisation et/ou à avertir au moins un tiers de la situation.

De façon préférentielle, le dispositif de radiocommunication selon l'invention comprend en outre un menu de l'interface homme-machine spécifique permettant à l'utilisateur d'activer ou de désactiver un mode de fonctionnement spécifique de lutte contre le vol.

Avantageusement, lorsque le mode de fonctionnement spécifique de lutte contre le vol est activé, il comprend des moyens de demande de saisie systématique par l'utilisateur du code d'identification personnel (code PIN) et/ou d'un autre code secret propre au téléphone lui-même, de façon à autoriser ou ne pas autoriser l'appel.

Il est ici important de souligner que l'utilisation d'un deuxième code confidentiel doit permettre de dissuader encore un peu plus les voleurs qui jusqu'alors pouvaient revendre un téléphone volé en changeant la carte SIM neutralisée par une autre en fonctionnement. Ainsi, l'ajout et l'utilisation d'un second code secret rendraient impossible la réutilisation du téléphone dérobé, la carte SIM et le téléphone lui-même ayant été tous deux verrouillés à distance.

De façon préférentielle, le dispositif de radiocommunication selon l'invention met en œuvre le procédé précédemment décrit.

Dans un mode de réalisation particulier, le dispositif selon l'invention comprend avantageusement des moyens de communication sans fil avec une autre entité de radiocommunication dédiée. Ces moyens de communication permettent ainsi l'activation et/ou la désactivation du mode de fonctionnement spécifique de lutte contre le vol du dispositif au moyen d'échanges réguliers de mots de code. Ces échanges réguliers entre cette entité de radiocommunication dédiée et le téléphone mobile s'effectuent au moyen d'une communication asynchrone : le téléphone mobile émet des requêtes régulières possédant un premier mot de code vers l'entité de radiocommunication et reçoit normalement en retour par ladite entité un acquittement à cette requête contenant un autre mot de code. Cette communication selon un mode de requêtes/acquittements permet de tester la proximité du téléphone mobile.

Ainsi, dès lors que la distance entre le terminal dédié sans fil et le téléphone mobile dépassera un seuil prédéterminé, la communication sans fil, du type Bluetooth (marque déposée) par exemple, entre le terminal et le téléphone sera rompue, de même que lorsque le mot de code reçu par le téléphone mobile et contenu dans l'acquittement de ladite entité sera erroné un certain nombre prédéterminé de fois. Un « timer » sera alors déclenché. Lorsque ce dernier atteindra une durée prédéterminée correspondant à la durée pendant laquelle le téléphone mobile aura tenté de rétablir la communication avec le terminal dédié, ou de tester la validité du mot de code contenu dans l'acquittement, alors le procédé de lutte contre le vol sera activé, le téléphone mobile volé devenant alors inutilisable.

De façon également avantageuse, les moyens de communication sans fil utilisés comprennent une liaison sans fil du type Bluetooth (marque déposée), par exemple.

5. Liste des figures

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation préférentiel, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- la figure 1 est un diagramme correspondant à un premier mode de réalisation de l'invention et illustrant les différentes étapes et actions exécutées par l'appareil de radiocommunication suite à la réception d'un premier type de message de demande de mise hors service dudit appareil;
- la figure 2 est un diagramme correspondant à un deuxième mode de réalisation de l'invention et illustrant les différentes étapes et actions exécutées par l'appareil de radiocommunication suite à la réception d'un second type de message de demande de mise hors service dudit appareil ;
- la figure 3 est un diagramme correspondant à un quatrième mode de réalisation de l'invention mettant en œuvre une communication sans fil entre l'appareil de radiocommunication et une autre entité de radiocommunication sans fil.

6. Description de quatre modes de réalisation de l'invention

6.1 Rappel du principe général de l'invention

L'invention vise donc à permettre au propriétaire de l'appareil de radiocommunication, téléphone mobile ou autre terminal portable par exemple, de pouvoir désactiver lui-même, très simplement et très rapidement, l'utilisation de sa carte SIM et/ou de son téléphone.

De façon plus détaillée, le concept général de l'invention consiste à intégrer dans les couches dites d'interface homme-machine (IHM ou MMI pour « Man Machine Interface » en anglais) et de protocole de la couche 3 un mode de fonctionnement supplémentaire, dénommé dans la suite de la description « mode vol », ou « Robbery mode » en anglais.

Il est important de préciser que ce mode de fonctionnement « Robbery mode » est susceptible d'utiliser un ou deux nouveaux messages, dénommés « L3_RobberyMode_Req » et « L3_Robbery_Ind » qui n'existent pas à ce jour, suivant le mode de réalisation de l'invention, mais devraient être normalisés en termes de recommandations GSM et/ou GPRS et/ou UMTS et/ou autre norme de radiocommunication et/ou télécommunication futures.

L'équipement de radiocommunication devra entrer dans ce nouveau mode de fonctionnement, sous la contrainte de réception d'un stimulus précis déclenché à distance par le propriétaire de cet équipement qui peut ainsi garder le contrôle à distance sur celui-ci.

Différents modes de réalisation de l'invention sont techniquement envisageables pour permettre à l'équipement de radiocommunication (téléphone mobile GSM, GPRS, UMTS, PDA et autres terminaux portables) d'adopter le mode de fonctionnement « vol » précité. Quatre d'entre eux sont détaillés ci-dessous à titre d'exemples, d'autres variantes combinant ces quatre modes de réalisation possibles de l'invention pouvant être combinés indifféremment pour aboutir à d'autres modes de réalisation complémentaires.

6.2 Premier mode de réalisation préférentiel de l'invention

Dans un premier mode de réalisation préférentiel de l'invention, illustré de façon détaillé par le diagramme de la figure 1, le stimulus permettant à l'appareil de radiocommunication d'accéder au mode de fonctionnement « vol » provient d'un message de signalisation protocolaire émis par réseau de télécommunication mobile à destination de la couche 3 (dite L3) de l'appareil de radiocommunication. Ce message émis par le réseau de radiocommunication mobile est dénommé L3_RobberyMode_req.

Ce message est généré et adressé automatiquement par un terminal serveur dédié et attaché au réseau GSM/GPRS/UMTS, à l'appareil mobile ayant été dérobé, dès lors qu'un appel téléphonique du propriétaire est émis vers le mobile depuis n'importe quel autre téléphone mobile ou fixe, public ou privé, en composant un numéro spécial standardisé, par exemple, de la façon suivante :

<préfixe> <numéro ISDN de l'appareil mobile> <extension numérique secrète définie et connue uniquement du propriétaire de l'appareil>.

De façon plus précise, le préfixe précité correspond à un numéro d'adressage du terminal serveur dédié, lequel interprétera le numéro ISDN pour identifier formellement l'appareil mobile qui l'aura contacté.

Une fois ce message L3_RobberyMode_req reçu et reconnu par l'appareil mobile de radiocommunication, un système à états est activé sur l'appareil, puis déclenche l'exécution séquentielle des traitements suivants :

- passage des couches IHM (Interface Homme-Machine) et L3 dans l'état « mode vol » (ou « Robbery Mode », en anglais);
- interruption de toute communication en cours initiée par le voleur et verrouillage de l'appareil pour interdire l'établissement de toute autre communication ultérieure ;
- transmission par l'appareil de radiocommunication d'un message protocolaire dénommé L3_Robbery_ind issu de la couche L3 (niveau 3) à destination de l'opérateur en charge de l'abonnement téléphonique associé à l'appareil dérobé. Ce message standardisé comprend :
    - une en-tête prédéfinie signifiant le vol de l'appareil ;
    - le numéro IMEI, identifiant unique de l'appareil (téléphone mobile, par exemple) ;

  Ce message comprend en outre et de manière optionnelle le positionnement de l'appareil par localisation, dans l'hypothèse où cette fonction est implémentée sur l'appareil au moyen, par exemple, d'un système GPS (« Global Positionning System », en anglais) qui lui serait intégré.
- exécution par la couche L3 de l'appareil de radiocommunication de l'action IMSI_detach permettant de dés-inscrire proprement ledit appareil de la base de donnée de l'enregistreur de localisation des visiteurs VLR (pour « Visitors Location Register » en anglais) associée au centre de commutation du service mobile MSC (pour « Mobile Service Switching Center » en anglais) ;

- mise dans l'état inactif du code personnel d'identité ou code PIN (« Personnal Identity Number Code » en anglais) par le gestionnaire de la carte SIM de l'appareil, ce qui a pour conséquence d'obliger à l'utilisation de la clé de déblocage du code PIN de l'appareil (ou PUK pour « PIN Unblocking Key » en anglais) lors du rallumage de ce dernier. Pour rendre inactif le code PIN de l'appareil, le gestionnaire de la carte SIM fournit, en arrière-plan et de façon transparente pour l'utilisateur, trois fois à cette dernière un code PIN erroné de façon à la rendre inutilisable ;
- mémorisation du mode de fonctionnement, en l'occurrence du « mode vol » (ou « RobberyMode » en anglais), dans la mémoire non volatile programmable et réinscriptible de l'appareil (EEPROM, FLASH, par exemple). L'objectif premier de cette étape est d'interdire toute communication avec l'appareil, même après son rallumage lorsque celui-ci a été placé dans le mode de fonctionnement « vol » ou « RobberyMode ».
- extinction automatique de l'appareil de radiocommunication par coupure de l'alimentation électrique.

Ce premier mode de réalisation selon l'invention est très simple à mettre en œuvre dans un appareil de radiocommunication, dès lors que les deux nouveaux messages « L3_RobberyMode_Req » et « L3_Robbery_Ind » seront normalisés en termes de recommandations GSM et/ou GPRS et/ou UMTS et/ou autre norme de radiocommunication et/ou télécommunication futures.

Ce premier mode de réalisation selon l'invention offre en outre un confort particulier au propriétaire de ce dernier qui n'a plus à s'inquiéter des conséquences que l'utilisation frauduleuse et coûteuse que le vol de son appareil pourraient provoquer. Le propriétaire de l'appareil dispose en effet de tous les moyens simples pour neutraliser à distance le fonctionnement de ce dernier qui devient alors inutilisable et non revendable pour l'individu qui l'a dérobé, dans un délai de quelques minutes uniquement après le constat du vol. Ces moyens sont de plus indépendants de l'opérateur qui avait seul, suivant les solutions de l'art antérieur, la charge de la désactivation et/ou neutralisation de l'appareil de

radiocommunication. L'invention permet de gagner au moins le temps nécessaire pour la gestion d'une déclaration de vol et s'avère plus efficace.

6.3 Deuxième mode de réalisation possible de l'invention

Dans un deuxième mode de réalisation de l'invention, dont les étapes sont détaillées sur le diagramme de la figure 2, le stimulus permettant à l'appareil de radiocommunication d'accéder au mode de fonctionnement « vol » provient non plus d'un message de signalisation protocolaire émis par réseau de télécommunication mobile à destination de la couche 3 (dite L3) de l'appareil de radiocommunication, mais d'un message du type SMS (pour « Short Message Service » en anglais) transmis par le propriétaire à son appareil volé, au moyen d'un autre appareil de radiocommunication (autre téléphone mobile par exemple) ou bien d'un service d'envoi de message SMS accessible sur Internet.

Pour qu'un tel message SMS soit reconnu par l'appareil dérobé, son contenu doit être limité au code d'identification personnel du propriétaire (code PIN en anglais) ou à un autre code confidentiel. Lorsque l'appareil détecte la réception d'un message SMS contenant uniquement un numéro de code qu'il vérifie être celui de son propriétaire, un système à états est activé sur l'appareil, puis déclenche l'exécution séquentielle des traitements suivants :

- passage des couches IHM (Interface Homme-Machine) et L3 dans l'état « mode vol » (ou « Robbery Mode », en anglais);
- interruption de toute communication en cours initiée par le voleur et verrouillage de l'appareil pour interdire l'établissement de toute autre communication ultérieure ;
- transmission par l'appareil de radiocommunication d'un message protocolaire dénommé L3_Robbery_ind issu de la couche L3 (niveau 3) à destination de l'opérateur en charge de l'abonnement téléphonique associé à l'appareil dérobé. Ce message standardisé comprend :
    - une en-tête prédéfinie signifiant le vol de l'appareil ;
    - le numéro IMEI, identifiant unique de l'appareil (téléphone mobile, par exemple) ;

Ce message comprend en outre et de manière optionnelle le positionnement de l'appareil par localisation, dans l'hypothèse où cette fonction est implémentée sur l'appareil au moyen d'un système GPS (« Global Positionning System », en anglais) qui lui serait intégré.

- exécution par la couche L3 de l'appareil de radiocommunication de l'action IMSI_detach permettant de dés-inscrire proprement ledit appareil de la base de donnée de l'enregistreur de localsation des visiteurs VLR (pour « Visitors Location Register » en anglais) associée au centre de commutation du service mobile MSC (pour « Mobile Service Switching Center » en anglais) ;
- mise dans l'état inactif du code personnel d'identité ou code PIN (« Personnal Identity Number Code » en anglais) par le gestionnaire de la carte SIM de l'appareil, ce qui a pour conséquence d'obliger à l'utilisation de la clé de déblocage du code PIN de l'appareil (ou PUK pour « PIN Unblocking Key » en anglais) lors du rallumage de ce dernier. Pour rendre inactif le code PIN de l'appareil, le gestionnaire de la carte SIM fournit, en arrière-plan et de façon transparente pour l'utilisateur, trois fois à cette dernière un code PIN erroné de façon à la rendre inutilisable ;
- mémorisation du mode de fonctionnement, en l'occurrence du « mode vol » (ou « RobberyMode » en anglais), dans la mémoire non volatile programmable et réinscriptible de l'appareil (EEPROM, FLASH, par exemple). L'objectif premier de cette étape est d'interdire toute communication avec l'appareil, même après son rallumage lorsque celui-ci a été placé dans le mode de fonctionnement « vol » ou « RobberyMode ».
- extinction automatique de l'appareil de radiocommunication par coupure de l'alimentation électrique.

Ce deuxième mode de réalisation selon l'invention est également très simple à mettre en œuvre dans un appareil de radiocommunication. Il offre en outre un également confort particulier au propriétaire de ce dernier qui n'a plus à s'inquiéter des conséquences que l'utilisation frauduleuse et coûteuse que le vol de son appareil pourraient provoquer. Le propriétaire de l'appareil dispose en

effet, par simple envoi d'un message SMS, du moyen relativement simple pour neutraliser à distance le fonctionnement de ce dernier qui devient alors inutilisable et non revendable pour l'individu qui l'a dérobé, dans un délai de quelques minutes uniquement après le constat du vol.

Ce deuxième mode de réalisation présente en outre l'avantage de ne pas nécessiter l'introduction de deux nouveau messages aux normes GSM et/ou GPRS et/ou UMTS, et par conséquent, aucun nouveau développement côté réseau.

6.4 Troisième mode de réalisation possible de l'invention

Dans un troisième mode de réalisation de l'invention, avantageusement utilisé en combinaison avec l'un ou l'autre des deux précédents modes de réalisation décrits, une solution très simple, bien que probablement moins efficace, consiste à ajouter un menu supplémentaire au niveau de l'interface homme-machine (IHM), le choix de ce menu permettant d'activer le mode de fonctionnement « vol », ou « RobberyMode » directement au niveau de l'appareil. Le choix de ce menu permet alors à l'utilisateur d'anticiper un vol de son appareil (téléphone portable, PDA ou autre type d'appareil de radiocommunication) en imposant le verrouillage systématique des communications sortantes. Ainsi, à chaque fois qu'un utilisateur de cet appareil souhaite initier un appel, l'appareil dont le mode « vol » est activé demande systématiquement à l'utilisateur de saisir le code d'identification personnel (ou code PIN) normalement connu du seul propriétaire de la carte SIM contenu dans l'appareil.

Dans une variante de ce mode de réalisation, il est également possible d'envisager que l'utilisateur, lorsqu'il allume son téléphone mobile, doive saisir d'une part le code PIN dudit téléphone (en réalité de la carte SIM), mais également et d'autre part, un second code confidentiel qui serait indépendant de la carte SIM et propre au téléphone lui-même. Une telle variante, plus robuste en termes de dissuasion, offre pour avantage principal de permettre une double neutralisation : celle de la carte SIM et celle du téléphone lui-même qui devient alors invendable car inutilisable, même avec une nouvelle carte SIM non verrouillée.

6.5 Quatrième mode de réalisation possible de l'invention

Dans un quatrième mode de réalisation, le dispositif de radiocommunication selon l'invention comprend des moyens de communication sans fil avec une autre entité de radiocommunication dédiée. Ces moyens de communication peuvent être activés/désactivés au moyen d'un menu complémentaire (type MMI, par exemple) de l'interface homme-machine. Ils permettent en particulier d'activer et/ou de désactiver le mode de fonctionnement spécifique de lutte contre le vol du dispositif grâce à des par échanges réguliers de mots de code dont l'objectif consiste à tester régulièrement la continuité d'une communication sans fil (par liaison Bluetooth (marque déposée) par exemple) entre ce terminal et le téléphone. Ainsi, dès lors que le téléphone mobile sera dérobé, et donc éloigné du terminal dédié de communication sans fil, la connexion sera rompue. La rupture de la connexion sera alors détectée par le téléphone mobile ayant été dérobé, celui-ci activant alors automatiquement le procédé de lutte contre le vol qui neutralisera son fonctionnement.

En outre, le même processus de neutralisation du terminal de radiocommunication sera initié dès lors que les mots de code contenus dans les acquittements retransmis par l'entité de radiocommunication sans fil seront erronés un nombre de fois prédéterminé, égal à cinq, par exemple.

Il est donc nécessaire de préciser que l'entité de radiocommunication sans fil communiquant avec le téléphone mobile doit être nécessairement située à proximité du téléphone. Cette entité pourra prendre des formes diverses, comme celles appartenant au groupe comprenant par exemple :

- bracelet porté par l'utilisateur ;
- boucle de ceinture.

Ce quatrième mode de fonctionnement possible est décrit sur la figure 3.

6.6 Autres variantes de réalisation possible de l'invention

D'autres variantes du mode de réalisation de l'invention sont envisageables. Elles peuvent combiner les quatre modes de réalisation précités de façon que le propriétaire de l'appareil puisse provoquer à distance la mise hors service de ce dernier, indifféremment soit au moyen d'un appel téléphonique du propriétaire

émis vers le mobile depuis n'importe quel autre téléphone mobile ou fixe, public ou privé, en composant le numéro spécial standardisé :

<préfixe> <numéro ISDN de l'appareil mobile> <extension numérique secrète définie et connue uniquement du propriétaire de l'appareil>, soit directement par le mobile au moyen d'un message SMS dont le corps du message contient le code d'identification personnel (code PIN) ou bien un autre code confidentiel (celui du téléphone portable par exemple).

7. Avantages de la solution selon l'invention

Le procédé et dispositif de lutte contre le vol d'un appareil de radiocommunication, tels que proposés par l'invention présentent de nombreux avantages, dont une liste non exhaustive est donnée ci-dessous :

- indépendance par rapport à l'opérateur en charge de l'abonnement du propriétaire de l'appareil ayant été dérobé ;
- autonomie d'exécution de la mise hors service à distance de son appareil de radiocommunication pour le propriétaire de ce dernier ;
- simplicité, facilité et rapidité d'exécution de la mise hors service à distance de l'appareil, dès lors que son vol a été constaté par son propriétaire ;
- efficacité de la solution technique qui permet, à distance, de neutraliser l'appareil volé, sans aucune possibilité pour le voleur de pouvoir l'utiliser ;
- dissuasion auprès d'un voleur qui ne pourra désormais plus revendre et/ou utiliser l'appareil qu'il aura dérobé à son propriétaire, dès lors que ce dernier aura constaté le vol de l'appareil, puis exécuté la procédure de mise hors service de ce dernier ;
- faible coût de mise en œuvre de l'invention, seules des mises à jour et/ou amélioration au niveau logiciel étant nécessaires.

REVENDICATIONS

1. Procédé de lutte contre le vol d'un dispositif ou appareil de radiocommunication, caractérisé en ce qu'il comprend une étape d'appel dudit dispositif de radiocommunication, par le titulaire de ce dernier, lorsqu'il a été dérobé, et une étape de transmission d'au moins un code confidentiel, entraînant la mise en œuvre automatique d'au moins une première opération spécifique d'invalidation de la carte de contrôle (SIM), destinée à empêcher l'utilisation dudit dispositif de radiocommunication et/ou à avertir au moins un tiers de la situation.

2. Procédé de lutte contre le vol selon la revendication 1, caractérisé en ce que ladite étape de transmission d'au moins un code confidentiel entraîne également la mise en œuvre automatique d'au moins une seconde opération spécifique appartenant au groupe comprenant :

- l'invalidation ou l'extinction dudit dispositif ;
- la transmission d'un message à un opérateur et/ou à un autre tiers ;
- l'émission de données de localisation ;
- l'interruption d'une communication ou d'une application en cours ;

3. Procédé de lutte contre le vol selon l'une quelconque des revendications 1 et 2, caractérisé en ce que ledit code confidentiel peut être transmis sous au moins une des formes suivantes :

- messages courts (SMS) ;
- codes DTMF ;
- messages vocaux.

4. Procédé de lutte contre le vol selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ledit code confidentiel est transmis audit dispositif ou appareil de radiocommunication au moyen d'un autre terminal appartenant au groupe comprenant :

- téléphone mobile ;
- téléphone fixe ;
- appareil connecté à un réseau de communication du type Internet ;

5. Procédé de lutte contre le vol selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ledit code confidentiel est contenu dans un message protocolaire transmis audit dispositif ou appareil de radiocommunication au moyen d'un terminal serveur dédié et automatisé.

6. Procédé de lutte contre le vol selon l'une quelconque des revendications 1 à 5 caractérisé en ce qu'il comprend une étape de désactivation du code d'identification personnel (PIN) en rentrant automatiquement un code erroné un nombre de fois supérieur au seuil autorisé.

7. Procédé de lutte contre le vol selon l'une quelconque des revendications 1 à 6, caractérisé en ce que ladite opération spécifique correspond à la génération d'un message de signalisation avec une en-tête spécifique.

8. Procédé de lutte contre le vol selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il comprend au moins certaines des étapes suivantes de:

- réception par le dispositif de radiocommunication d'une requête et/ou d'un message, pour le déclenchement de la mise hors service ;
- passage de la couche IHM (Interface Homme-Machine) et/ou de la couche L3 dans l'état « mode vol » ;
- interruption de toute communication en cours et/ou verrouillage dudit dispositif ;
- transmission par l'appareil de radiocommunication d'un message à destination de l'opérateur en charge de l'abonnement téléphonique associé audit dispositif dérobé.
- exécution par la couche L3 de l'appareil de radiocommunication de l'action IMSI_detach, pour la dés-inscription dudit dispositif de la base de données d'un enregistreur de localisation des visiteurs (VLR) ;
- mise dans l'état inactif du code personnel d'identité (code PIN) par le gestionnaire de la carte SIM dudit dispositif ;
- mémorisation d'une information représentative de l'état « volé » dans une mémoire dudit dispositif.
- extinction automatique dudit dispositif par coupure de l'alimentation électrique.

9. Procédé de lutte contre le vol selon la revendication 8, caractérisé en ce que ledit message à destination de l'opérateur comprend :

- une en-tête prédéfinie signifiant le vol dudit dispositif ;
- le numéro IMEI, identifiant unique dudit dispositif ;

10. Procédé de lutte contre le vol selon l'une quelconque des revendications 1 à 9, caractérisé en ce qu'il comprend une étape de positionnement par des moyens de géo localisation intégrés audit dispositif.

11. Procédé de lutte contre le vol selon la revendication 10, caractérisé en ce que ladite mémoire de l'appareil est une mémoire non volatile programmable et réinscription du type appartenant au groupe comprenant :

- les mémoires EEPROM ;
- les mémoires FLASH.

12. Procédé de lutte contre le vol selon l'une quelconque des revendications 5 à 11 caractérisé en ce qu'on envoie trois fois un faux code PIN audit dispositif, de façon à le verrouiller.

13. Dispositif de radiocommunication, caractérisé en ce qu'il comprend des moyens de réception d'au moins un code confidentiel, émis par le titulaire dudit dispositif et/ou un autre terminal serveur dédié automatisé, lorsqu'il a été dérobé, entraînant la mise en œuvre automatique d'au moins une opération spécifique destinée à empêcher l'utilisation dudit dispositif de radiocommunication et/ou à avertir au moins un tiers de la situation.

14. Dispositif de radiocommunication selon la revendication 13, caractérisé en ce qu'il comprend un menu de l'interface homme-machine spécifique permettant à l'utilisateur d'activer ou de désactiver un mode de fonctionnement spécifique de lutte contre le vol dudit dispositif.

15. Dispositif de radiocommunication la revendication 14, caractérisé en ce que lorsque ledit mode de fonctionnement spécifique de lutte contre le vol est activé, il comprend des moyens de demande de saisie systématique par l'utilisateur du code d'identification personnel (code PIN), de façon à autoriser ou ne pas autoriser l'appel.

16. Dispositif de radiocommunication selon l'une quelconque des revendications 13 à 15, caractérisé en ce qu'il met en œuvre le procédé selon les revendications 1 à 12.

17. Dispositif de radiocommunication selon l'une quelconque des revendications 14 à 16, caractérisé en ce que qu'il comprend des moyens de communication sans fil avec un autre terminal dédié, lesdits moyens de communication permettant de ladite activation et/ou ladite désactivation dudit mode de fonctionnement spécifique de lutte contre le vol dudit dispositif par échanges réguliers de mots de code.

18. Dispositif de radiocommunication selon la revendication 17, caractérisé en ce que lesdits moyens de communication sans fil comprennent une liaison sans fil du type comprenant une liaison Bluetooth (marque déposée).

1/3

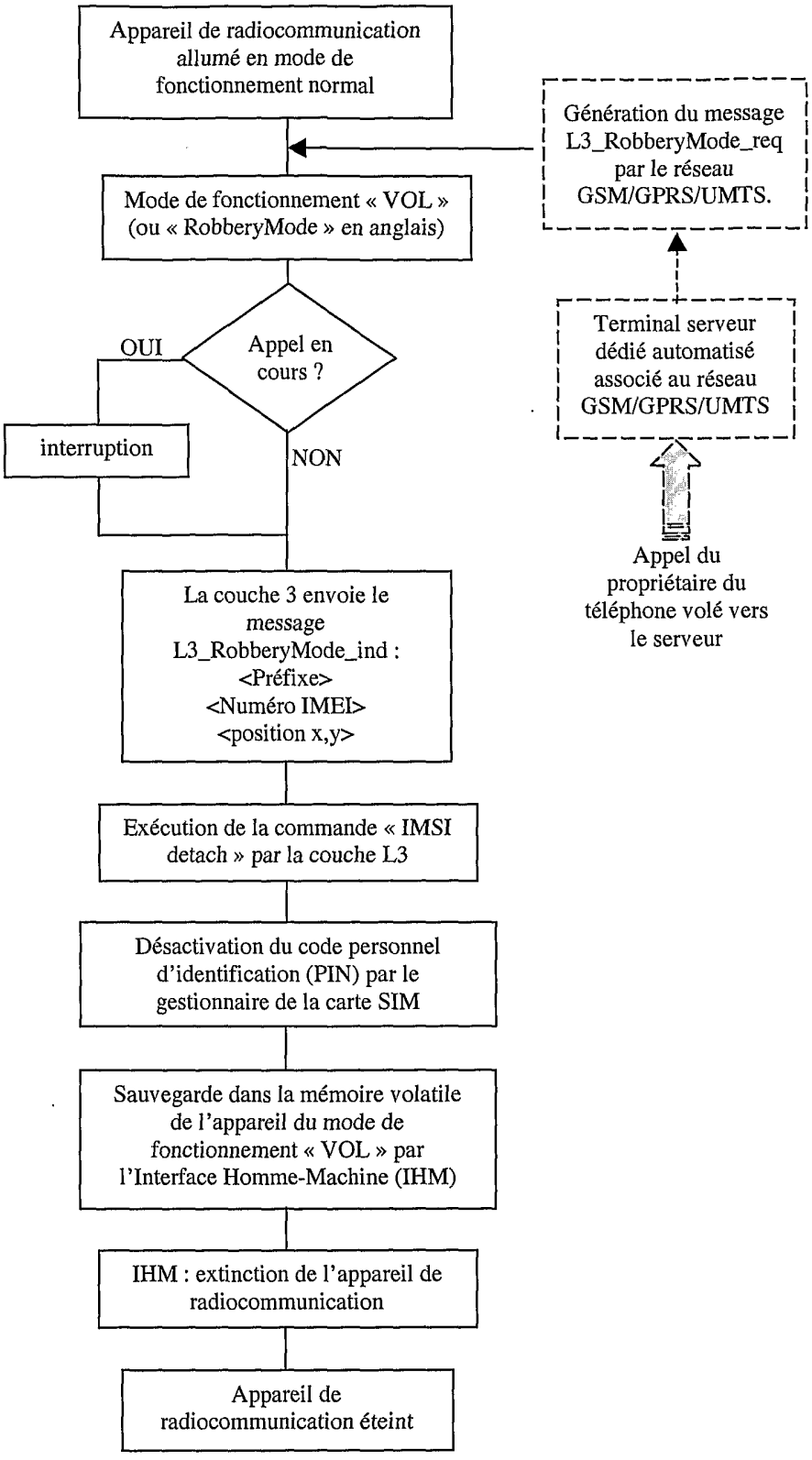

Appareil de radiocommunication allumé en mode de fonctionnement normal
Génération du message L3_RobberyMode_req par le réseau GSM/GPRS/UMTS.
Mode de fonctionnement « VOL » (ou « RobberyMode » en anglais)
Terminal serveur dédié automatisé associé au réseau GSM/GPRS/UMTS
OUI
Appel en cours ?
interruption
NON
Appel du propriétaire du téléphone volé vers le serveur
La couche 3 envoie le message L3_RobberyMode_ind : <Préfixe> <Numéro IMEI> <position x,y>
Exécution de la commande « IMSI detach » par la couche L3
Désactivation du code personnel d'identification (PIN) par le gestionnaire de la carte SIM
Sauvegarde dans la mémoire volatile de l'appareil du mode de fonctionnement « VOL » par l'Interface Homme-Machine (IHM)
IHM : extinction de l'appareil de radiocommunication
Appareil de radiocommunication éteint

Figure 1

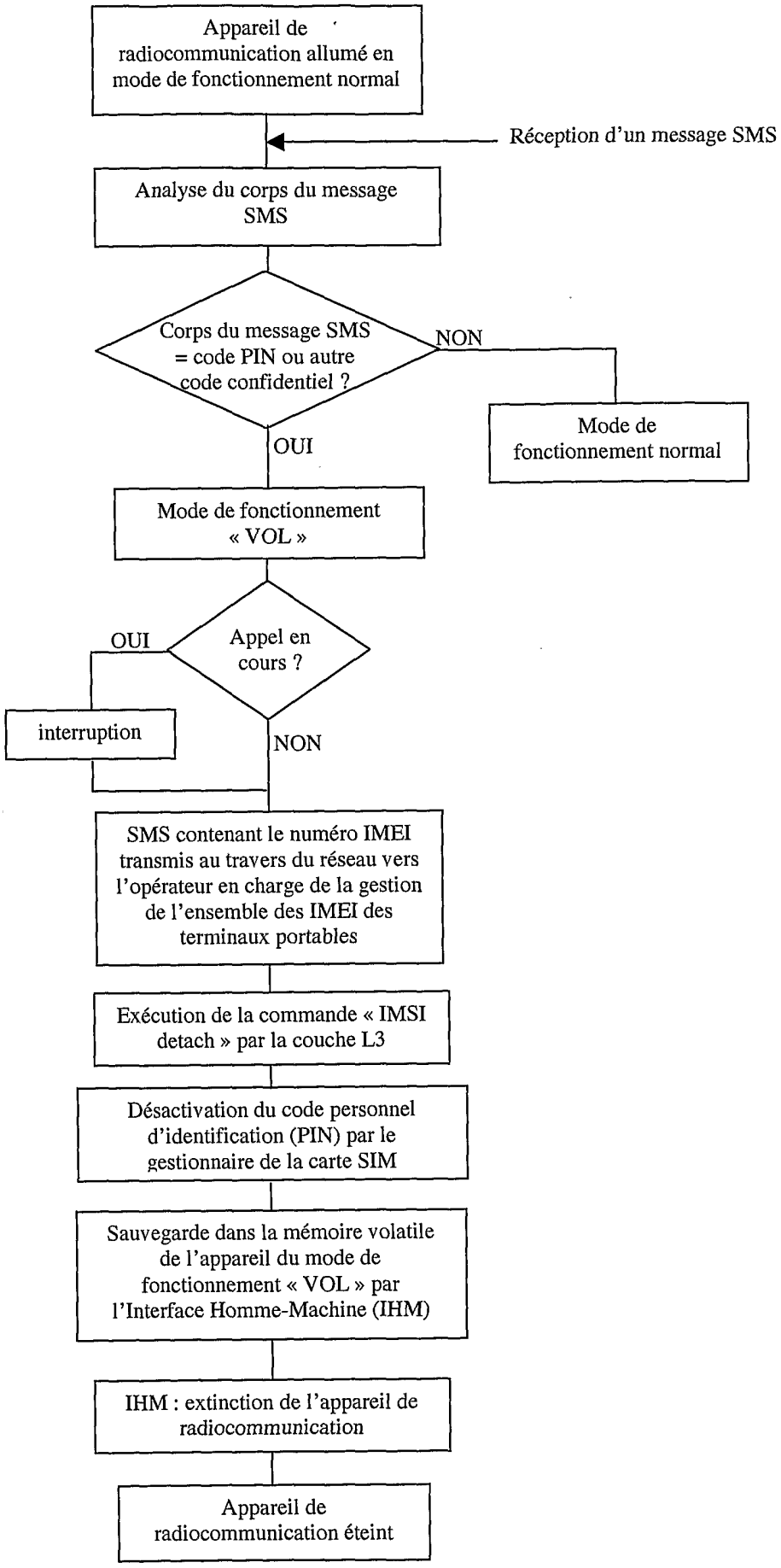

Appareil de radiocommunication allumé en mode de fonctionnement normal
Réception d'un message SMS
Analyse du corps du message SMS
Corps du message SMS = code PIN ou autre code confidentiel ?
NON
Mode de fonctionnement normal
OUI
Mode de fonctionnement « VOL »
Appel en cours ?
OUI
interruption
NON
SMS contenant le numéro IMEI transmis au travers du réseau vers l'opérateur en charge de la gestion de l'ensemble des IMEI des terminaux portables
Exécution de la commande « IMSI detach » par la couche L3
Désactivation du code personnel d'identification (PIN) par le gestionnaire de la carte SIM
Sauvegarde dans la mémoire volatile de l'appareil du mode de fonctionnement « VOL » par l'Interface Homme-Machine (IHM)
IHM : extinction de l'appareil de radiocommunication
Appareil de radiocommunication éteint

Figure 2

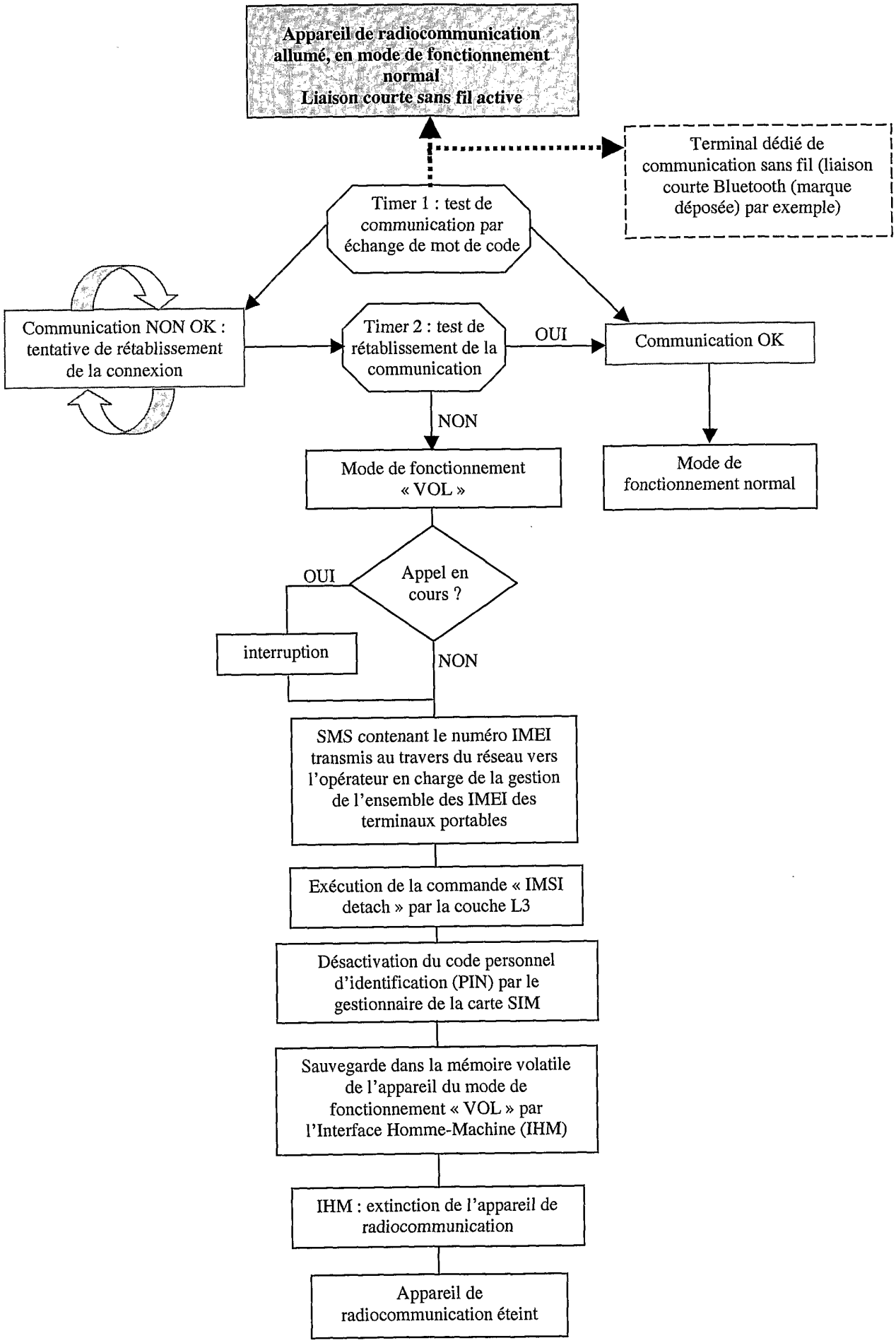

Appareil de radiocommunication allumé, en mode de fonctionnement normal
Liaison courte sans fil active
Terminal dédié de communication sans fil (liaison courte Bluetooth (marque déposée) par exemple)
Timer 1 : test de communication par échange de mot de code
Communication NON OK : tentative de rétablissement de la connexion
Timer 2 : test de rétablissement de la communication
OUI
Communication OK
NON
Mode de fonctionnement « VOL »
Mode de fonctionnement normal
Appel en cours ?
OUI
interruption
NON
SMS contenant le numéro IMEI transmis au travers du réseau vers l'opérateur en charge de la gestion de l'ensemble des IMEI des terminaux portables
Exécution de la commande « IMSI detach » par la couche L3
Désactivation du code personnel d'identification (PIN) par le gestionnaire de la carte SIM
Sauvegarde dans la mémoire volatile de l'appareil du mode de fonctionnement « VOL » par l'Interface Homme-Machine (IHM)
IHM : extinction de l'appareil de radiocommunication
Appareil de radiocommunication éteint

Figure 3