(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
30 avril 2009 (30.04.2009)

PCT

(10) Numéro de publication internationale
WO 2009/053402 A1

(51) Classification internationale des brevets :
H04L 29/06 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2008/064310

(22) Date de dépôt international :
22 octobre 2008 (22.10.2008)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0707414 23 octobre 2007 (23.10.2007) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **THALES** [FR/FR]; 45 rue de Villiers, F-92200 Neuilly Sur Seine (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **VIRAVAU, Philippe** [FR/FR]; 13, Rue Villedo, F-75001 Paris (FR). **HIRSCH, Jeremy** [FR/FR]; 12, Boulevard de la Paix, F-92400 Courbevoie (FR).

(74) Mandataires : **DUDOUIT, Isabelle** etc.; Immeuble Visium, 22, Avenue Aristide Briand, F-94117 Arcueil (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : 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, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(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,

[Suite sur la page suivante]

(54) **Title:** DEVICE AND METHOD MAKING IT POSSIBLE TO INTERCEPT COMMUNICATIONS IN A NETWORK

(54) **Titre :** DISPOSITIF ET PROCEDE PERMETTANT D'INTERCEPTER DES COMMUNICATIONS DANS UN RESEAU

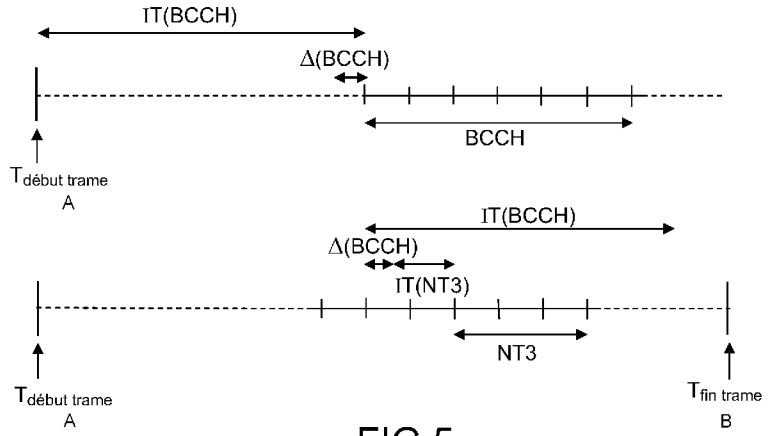


FIG.5

A $T_{frame\ start}$
B $T_{frame\ end}$

(57) **Abstract:** Method for intercepting communications exchanged between a first terminal and a second terminal, characterized in that it comprises a step of synchronizing the communication exchanges over the traffic channel, comprising a step where the instants of sending of bursts responsible for the allocation of the resources for the communication are determined and a step of calling the demodulator in the intervals of samples liable to contain these bursts so as to obtain the characteristics of intercepted communication or the communication on which the synchronization has been performed.

[Suite sur la page suivante]

WO 2009/053402 A1

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).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

(57) Abrégé : Procédé pour intercepter des communications échangées entre un premier terminal et un deuxième terminal, caractérisé en ce qu'il comporte une étape de synchronisation des échanges de communication sur le canal de trafic, comprenant une étape où l'on détermine les instants d'émission des bursts responsables de l'allocation des ressources pour la communication et une étape d'appel du démodulateur dans les intervalles d'échantillons susceptibles de contenir ces bursts afin d'obtenir les caractéristiques de la communication interceptée ou sur laquelle la synchronisation a été effectuée.

DISPOSITIF ET PROCEDE PERMETTANT D'INTERCEPTER DES COMMUNICATIONS DANS UN RESEAU

L'invention concerne un dispositif et un procédé permettant d'intercepter des communications dans un réseau où les mobiles communiquent entre eux en utilisant, par exemple, une liaison satellite.

De manière plus générale, elle s'applique dans tous les réseaux de communication qui utilisent un canal de diffusion (dit de « broadcast ») et des canaux de trafic, ces canaux étant utilisés pour la communication entre différents systèmes ou équipements.

Dans les réseaux de communication utilisant le lien satellitaire pour transmettre des informations d'un premier mobile vers un autre mobile, une grande partie des informations relatives au mobile, en particulier les identifiants IMSI (abrégé anglo-saxon de International Mobile Subscriber Identity),et IMEI (abrégé anglo-saxon de International Mobile Equipment Identity) ne sont pas disponibles via les canaux dits de diffusion, plus connus sous l'acronyme anglo-saxon « broadcast », mais via les canaux de trafic. Cela implique de se synchroniser avec précision sur ces canaux de trafic et d'en extraire l'information disponible pour connaître le contenu échangé durant la communication.

Dans l'art antérieur, différents mécanismes d'interception active des communications sont opérationnels pour les communications mobiles de type GSM (Global System Mobile). Les dispositifs qui utilisent ce principe sont plus connus sous le nom de « IMSI Catcher ».

Il existe aussi des systèmes d'interception passifs permettant d'obtenir l'ensemble des informations transmises en clair par le mobile et par le satellite sur les canaux dits de diffusion ou « broadcast ». Néanmoins, ces systèmes ne sont pas capables de se synchroniser sur les canaux de trafic et donc d'exploiter les informations issues de ces canaux.

Les systèmes d'interception connus à ce jour n'exploitent que les informations échangées entre le réseau et le mobile sur les canaux de broadcast, ce qui ne permet pas d'obtenir les caractéristiques des mobiles interceptés telles que l'IMSI, l'IMEI, la capacité de chiffrement du mobile.

Les systèmes de l'art antérieur ne permettent pas non plus « d'interroger » les mobiles interceptés à volonté afin d'acquérir leurs caractéristiques.

La demande de brevet WO 2006/111974 divulgue un procédé et un dispositif permettant d'intercepter des échanges entre un mobile et un réseau. Si certaines informations ne sont pas échangées, elles ne seront jamais décodées.

L'objet de la présente invention concerne un dispositif et un procédé qui permettent une synchronisation fine et précise sur les canaux de trafic. L'invention permet aussi de forcer des mobiles connectés sur un réseau à passer sur un autre réseau afin de pouvoir être interceptés.

L'objet de l'invention concerne un procédé pour intercepter des communications échangées entre au moins un premier terminal et un deuxième terminal caractérisé en ce qu'il comporte une étape au cours de laquelle au moins un signal identique à celui ou ceux émis par l'un des deux terminaux est émis au moyen d'un dispositif d'interception et une étape de synchronisation des échanges de communication sur le canal de trafic, comprenant une étape où l'on détermine les instants d'émission des bursts responsables de l'allocation des ressources pour la communication et une étape d'appel du démodulateur dans les intervalles d'échantillons susceptibles de contenir ces bursts afin d'obtenir les caractéristiques de la communication interceptée ou sur laquelle la synchronisation a été effectuée.

Selon un mode de réalisation, le signal émis par le dispositif d'interception simule un canal de diffusion identique à celui qui est émis par un des deux terminaux.

Dans le cas où un terminal est un satellite, le signal émis simule avec une puissance suffisante un canal de diffusion "broadcast" identique à celui émis par le satellite, les mobiles tentent de s'accrocher sur ce signal fictif, l'étape suivante consiste à interroger lesdits mobiles.

Selon un autre mode de réalisation, au moment où un autre mobile transmet sa capacité de chifffrement à un réseau, un dispositif d'interception génère un signal de perturbation permettant de neutraliser les messages envoyés par le mobile et émet un message virtuel indiquant au réseau que le mobile ne dispose pas de capacité de chiffrement, le module dédié aux canaux montants entre le mobile et le réseau décodent les informations émises par le mobile au réseau et le module dédié aux canaux descendants décode les informations émises par le réseau.

Le procédé exploite, par exemple, les informations de type IMSI, TMSI présentes dans la communication interceptée.

L'invention concerne aussi un dispositif permettant d'intercepter une ou plusieurs communications entre deux équipements comportant en combinaison au moins un dispositif de synchronisation adapté à déterminer les instants d'émission des créneaux ou « bursts » responsables de l'allocation des ressources pour la communication et un moyen permettant de générer un appel du démodulateur dans les intervalles d'échantillons susceptibles de contenir ces créneaux ou « bursts » afin d'obtenir les caractéristiques de la communication interceptée ou sur laquelle la synchronisation a été effectuée.

D'autres caractéristiques et avantages de la présente invention apparaîtront mieux à la lecture de la description d'un exemple de réalisation donné à titre illustratif et nullement limitatif annexé des figures qui représentent :

- La figure 1 représente un exemple d'organisation de la couverture en faisceaux,
- La figure 2 un exemple d'architecture de système selon l'invention,
- La figure 3, un exemple détaillé du module permettant l'interception des communications,
- La figure 4, le principe de synchronisation sur les canaux de trafic (NT et FACCH) à partir des informations contenues dans le message AGCH,
- La figure 5, le positionnement des bursts NT3 utilisés pour la synchronisation précise,
- La figure 6, la synchronisation symbole sur les bursts FACCH3 de type 0 et 1,
- La figure 7, un schéma de synchronisation temporelle en mode duplex,
- La figure 8, une synchronisation automatique en mode mono voie,
- Les figures 9 et 10, une application du procédé pour perturber des signaux émis.

Afin de mieux faire comprendre l'invention, la description qui suit est donnée dans le cadre d'un système spatial de radiotéléphonie mobile par satellite. Le système utilise, deux et à terme trois satellites géostationnaires. Dans la description, ce système est désigné sous le nom « Thuraya ».

L'invention n'est nullement limitée à ce type de système, et peut fonctionner aussi dans tout système de communication comprenant un canal de diffusion ou

« broadcast », un canal de trafic, et plusieurs mobiles communiquant entre eux ou encore un mobile et un satellite.

Le principe repose sur l'utilisation de deux téléphones mobiles de taille équivalente à un mobile GSM (Global System Mobile) classique et fonctionnant sous deux modes possibles : le mode GSM classique lorsque la zone dans laquelle se trouve le mobile est couverte par le réseau et le mode « Thuraya » lorsque la zone dans laquelle se trouve le mobile est couverte uniquement par le réseau Thuraya. Les deux modes sont bien entendus sélectionnables au choix par l'utilisateur (GSM seul ou préférentiel, THURAYA seul ou préférentiel). Il est possible d'appeler ou d'être appelé par n'importe quel téléphone, mais on peut également transmettre des SMS, des données jusqu'à 9,6 kbits/s, ainsi que des FAX.

La liaison de service exploite la bande L. La polarisation est circulaire gauche et les fréquences de fonctionnement sont :

- La bande 1,525 – 1,559 GHz pour la liaison descendante ou « downlink » satellite vers mobile,
- La bande 1,6265 – 1,6605 GHz pour la liaison montante « uplink » ou liaison montante.

Un canal fréquentiel descendant est toujours appairé à un canal fréquentiel montant, les deux canaux étant espacés de 101,5 MHz. L'espacement entre canaux adjacents est de 31,25 kHz.

La couverture spatiale pour la bande L est organisée en multiples faisceaux, ou spot-beams de 700 km de diamètre environ. Un exemple de couverture géographique est donnée sur la figure 1.

Les fréquences sont attribuées aux faisceaux à la configuration initiale (ou lors des reconfigurations du réseau). L'allocation minimale par spot est une « sous-bande » correspondant à 5 canaux contigus montants et descendants. L'un des canaux est dédié au « broadcast » et l'allocation de ressources de communication (liaison descendante) ou à l'émission de requêtes d'accès (liaison montante). C'est le canal de « broadcast » qui permet au mobile de se synchroniser sur le réseau (pour permettre l'inscription et l'utilisation de ressources dédiées). Voici l'inventaire des canaux logiques multiplexés sur ce canal dit de « broadcast » :

- Le FCCH (*Frequency Correction CHannel*) transmet des paquets qui aident les terminaux à se synchroniser en fréquence.
- Le GBCH (*GPS Broadcast CHannel*) transmet les éphémérides des

satellites GPS, ainsi que l'heure GPS.

- Le BCCH (*Broadcast Control CHannel*) transmet les informations générales relatives à la configuration du système (positions des canaux, offsets TDMA, consignes d'accès…).
- Le CBCH (*Cell Broadcast CHannel*) est utilisé pour la diffusion de SMS adressés à l'ensemble des mobiles d'un faisceau.
- Le RACH (*Random Access CHannel*) permet l'émission des requêtes initiales des mobiles selon le protocole d'accès ALOHA.
- Le CCCH (*Common Control CHannel*) contient tout ou partie des sous-canaux logiques suivants :
- Le PCH (*Paging CHannel*) pour la diffusion des messages de *paging* (précède la réception d'un appel ou d'un SMS).
- L'AGCH (*Access Grant CHannel*) pour l'attribution de ressources dédiées aux terminaux émetteurs de requêtes initiales.
- Le BACH (*Broadcast Alerting CHannel*) pour la diffusion de messages d'alerte à forte puissance.
- Le CICH (*Common Idle CHannel*) sur lequel aucun signal n'est émis afin de permettre au mobile de calibrer le bruit ambiant.

Tous ces canaux sont bien entendu descendants, à l'exception du RACH qui est montant. De plus, tous ces canaux sont permanents, à l'exception du CBCH qui est dynamiquement crée puis supprimé par le système en fonction des besoins de diffusion de SMS dans le faisceau.

Les autres canaux sont des canaux de trafic et permettent de relayer les échanges dédiés entre les mobiles et le réseau (mise en place de la communication, échange de paramètres, voix, FAX, données). Les canaux de trafic sont les suivants :

- Le TCH3 (Traffic CHannel) destiné aux communications téléphoniques, qui est couplé à un FACCH3 (Fast Associated Control CHannel),
- Le TCH6 destiné aux télécopies ou aux transmissions de données à 2.4 et 4.8 kbit/s, qui est associé à un FACCH6,
- Le TCH9 destiné aux communications de télécopie à 2.4, 4.8 ou 9.6 kbit/s ainsi qu'aux transmissions de données à 9.6 kbit/s, qui est associé à un FACCH9.

Ces canaux sont tous bidirectionnels.

La figure 2 schématise un intercepteur selon l'invention composé par exemple de 4 fonctions principales :

- Fonction de perturbation GSM (« Perturbateur GSM »1): cette fonction a notamment pour objectif de neutraliser un réseau GSM de manière à forcer les mobiles THURAYA sous couverture GSM à passer en mode THURAYA. A titre d'exemple, cette fonction est schématisée sur la figure 3 par le module « Perturbateur GSM » constitué d'un perturbateur GSM de type WinPower et d'une antenne Bande GSM.
- Fonction de perturbation THURAYA, 2: cette fonction a pour objectif de neutraliser un réseau THURAYA de manière à forcer les mobiles 5 THURAYA sous couverture THURAYA, donc fonctionnant en mode thuraya, à passer en mode GSM.
- Fonction d'interception des mobiles THURAYA connectés sur le réseau GSM classique ou fonction « Catcher GSM » 3 : cette fonction a pour but d'intercepter les mobiles Thuraya connectés sur le réseau GSM.
- Fonction d'interception des mobiles THURAYA connectés sur le réseau THURAYA ou « Catcher THURAYA », 4 : cette fonction a, notamment, pour but d'intercepter les mobiles Thuraya connectés sur le réseau Thuraya. Cette fonctionnalité du dispositif selon l'invention est détaillée en relation avec les figures 2, 3, 4 et 5.

L'architecture comprend un amplificateur faible bruit, 6, ou LNA (Low Noise Amplifier) permettant de basculer sur les différentes fonctionnalités du système selon l'invention et des antennes GSM pour la voie montante et la voie descendante, 7, 8 et des antennes L pour les voies montantes et descendantes, 10, 11. Le satellite est référencé 12.

Les canaux FACCH descendants permettent au réseau de transmettre des informations à la MES lors d'une transaction (appel, *location update*…). Ces canaux ne sont actifs qu'après l'allocation des ressources par le réseau (c'est-à-dire après l'échange RACH/AGCH). Sur ces canaux, se trouvent, par exemple, des informations sur le chiffrement utilisé lors de la communication. Suivant le type de communication établie la longueur de ces *bursts* peut être de 3, 6 ou 9 IT (Intervalle Temporel).

Fonction « interception »

Cette fonction a pour but d'intercepter les signaux émis par les mobiles THURAYA situés à portée d'un intercepteur selon l'invention schématisé à la figure 3 (quelques mètres à quelques kilomètres suivant le type d'antenne et les obstacles situés entre le mobile et l'intercepteur) ainsi que les signaux émis par le réseau à destination des mobiles. L'intercepteur est constitué d'un module dédié à la démodulation et au décodage des canaux montants (communication des mobiles vers le satellite), d'un module dédié à la démodulation et au décodage des canaux descendants (satellite vers mobiles), et d'un module dédié à l'émission du signal correspondant au spotbeam virtuel (un signal « leurre » qui permettra « d'accrocher » les mobiles voulus pour leur soutirer des informations). Les modules sont décrits en figure 3.

Le module dédié aux canaux descendants est composé des éléments suivants :

- Une antenne bande L (« Antenne Bande L DownLink (1550 MHz) », référencée 20 sur la figure) dirigée vers le satellite et un amplificateur faible bruit, ou LNA (*Low Noise Amplifier*), 21, permettant de capter les signaux émis par le satellite 12 avec une puissance suffisante pour décoder sans erreur les informations reçues,
- Un module de réception dans la bande L descendante (comprise entre 1,525 et 1,559 GHz) avec une bande instantanée d'au moins 156.25 kHz de large de manière à intercepter en une seule fois les 5 canaux fréquentiels (descendants) de 31.25 kHz de large correspondant à un faisceau. Le module est, par exemple, un récepteur composé d'un châssis 22, d'un module RF alpha 23 et d'un oscillateur local LO alpha 24, permettant de transposer le signal radio vers une fréquence intermédiaire FI compatible de la carte d'acquisition 25, d'un module FN 26 et ST 27 permettant de contrôler le récepteur à partir d'un microcontrôleur, par exemple un PC intitulé PC0 28.
- le module d'acquisition numérique 25 permettant de numériser au moins 156.25 kHz de bande (descendante) en instantané, composé par exemple de la carte d'acquisition 25 et du PC 28. La carte d'acquisition 25 doit disposer de 2 convertisseurs Analogique/Numériques 29, 30, d'un convertisseur Numérique/Analogique 31 (DAC pour Digital to Analogic Converter) et d'un moyen de synchronisation temporelle 32 entre les voies de réception et d'émission.

- Un module de décodage 33 des signaux THURAYA capable de décoder simultanément le canal de *broadcast* (BCCH), le canal d'allocation de ressources (AGCH) et les canaux de communications (NTx) de chaque mobile connecté au moment de l'acquisition (le procédé ne cherche pas à décrypter les communications chiffrées, mais il décode toutes les informations transmises en clair). Ce module est schématisé par le PC nommé « PC1 : Décodage Thuraya, lien descendant (signal Satellite) ».
- Un moyen 34_1 d'envoi des informations décodées en clair vers la fonction de « leurrage ». Il peut s'agir par exemple d'une liaison Ethernet accompagnée d'un moyen d'échange de type client/serveur entre les éléments du système. Les différentes lignes 34_1, 34_2, 34_3, sont schématisées pour des raisons de simplification en une seule ligne 34 qui les regroupe.

Le module dédié aux canaux montants est composé des éléments suivants :

- Une antenne bande L omnidirectionnelle 35 permettant de capter les signaux émis par les téléphones mobiles avec une puissance suffisante pour décoder sans erreur les informations transmises par ces derniers,
- Un module de réception dans la bande L montante (comprise entre 1,6265 et 1,660 GHz) avec une bande instantanée d'au moins 156.25 kHz de large de manière à intercepter en une seule fois les 5 canaux fréquentiels (montants) de 31.25 kHz de large correspondant à un faisceau. Le module présenté présent sur le châssis comprend un module RF alpha 36 et un oscillateur local LO alpha 37 permettant de transposer le signal radio vers une fréquence intermédiaire FI compatible de la carte d'acquisition.
- Le module d'acquisition précité pour la liaison descendante.
- Un module de décodage des signaux THURAYA capable de décoder simultanément le canal de signalisation des mobiles (RACH) et les canaux de communications (NTx) de chaque mobile connecté au moment de l'acquisition (le procédé décode toutes les informations transmises en clair et enregistre les données cryptées d'une communication à la fois). Ce module est schématisé par le PC nommé « PC2 : Décodage Thuraya, lien montant (Mobile THURAYA) », 38.
- Un moyen d'envoi des informations 34_2 décodées en clair vers la fonction de « leurrage ». Le moyen d'envoi est schématisé par les lignes reliant les

différents éléments du système. Il peut s'agir par exemple d'une liaison Ethernet accompagnée d'un moyen d'échange de type client/serveur entre les éléments du système.

Le module dédié à l'émission du signal correspondant au spotbeam virtuel est composé des éléments suivants :

- Une antenne bande L 39 permettant d'émettre le signal correspondant au spotbeam virtuel et reçu par les téléphones mobiles avec une puissance suffisante pour que ces derniers s'accroche sur ce signal à la place du signal émis par le satellite,
- Un amplificateur 40 permettant d'amplifier le signal à émettre (schématisé par le triangle). Une puissance de quelques milliwatts est nécessaire pour permettre l'accrochage des mobiles Thuraya sur le spotbeam virtuel.
- Un module d'émission dans la bande L descendante (comprise entre 1,5625 et 1,5659 GHz) avec une bande instantanée d'au moins 156.25 kHz de large de manière à émettre en une seule fois les 5 canaux fréquentiels de 31.25 kHz de large correspondant à un faisceau. Sur le châssis pré mentionné, il comporte un module Tx 41 et un oscillateur local LO alpha 42 permettant de transposer le signal radio vers une fréquence intermédiaire FI compatible de la carte d'acquisition.
- Un module d'émission d'un signal analogique permettant d'émettre au moins 156.25 kHz de bande en instantané. Ce module est par exemple composé de la carte précitée et du PC 28. La carte d'acquisition doit disposer des 2 convertisseurs Analogique/Numériques (ADC pour Analogic to Digital Converter sur la figure), d'un convertisseur Numérique/Analogique (DAC pour Digital to Analogic Converter sur la figure) et du moyen de synchronisation temporelle entre les voies.
- Un module de codage des signaux THURAYA capable de coder simultanément le canal de *broadcast* (BCCH), le canal d'allocation de ressources (AGCH) et les canaux de communications (NTx) du chaque mobile cherchant à ce connecter sur le signal correspondant au spotbeam virtuel. Ce module est schématisé par le PC 39 nommé « PC3 : Générateur Spot-Beam Thuraya ».
- Un moyen de réception des informations décodées par les modules de réception décrits précédemment. Le moyen de réception est schématisé par

les lignes 34_3 reliant les différents éléments du système. Il peut s'agir d'une liaison Ethernet avec un switch Ethernet 1 Gb/s accompagnée d'un moyen d'échange de type client/serveur entre les éléments du système.

L'intercepteur est synchrone en temps sur les 3 modules précités grâce à une référence de date unique fixée par la carte d'acquisition.

Le « Catcher THURAYA » est capable de fonctionner selon 3 modes :

Un mode dit « actif » : le dispositif d'interception 19 se fait passer pour un *spotbeam* réel en simulant avec une puissance suffisante un canal de « broadcast » rigoureusement identique à ceux qui sont émis par le satellite. Les mobiles tentent donc de s'inscrire sur ce *spotbeam* fictif, ce qui permet à l'intercepteur (une fois les mobiles inscrits) de les « interroger » grâce à des requêtes appropriées sur les canaux de communication FACCH (demande d'IMSI, d'IMEI, de position GPS…). La technique permet de localiser, d'identifier et d'intercepter l'ensemble des caractéristiques des mobiles présents dans la zone de couverture. Pour réaliser ce mode :

- Le module 50, 51 dédié à l'émission du signal correspondant au spotbeam virtuel pré mentionné génère le signal de « broadcast » (BCCH) virtuel.
- Le mobile s'accroche sur ce signal de « broadcast » et émet un RACH pour demander l'inscription sur ce spotbeam virtuel. Le module intercepte, démodule et décode ce RACH.
- Le module répond au mobile en lui attribuant le canal fréquentiel voulu (pour les échanges de trafic) via un message de type AGCH adapté au contenu du RACH émis par le mobile.
- Le mobile s'inscrit sur ce canal de trafic (TCH3 + FACCH3).
- Le module transmet les messages dédiés au mobile intercepté pour l'amorce de la communication (autorisation d'inscription du mobile, choix du chiffrement) via des messages de type FACCH3.
- Le mobile transmet l'ensemble des informations nécessaires (capacité de chiffrement, identification).
- Le module peut alors envoyer des messages de type FACCH3 pour établir des requêtes auprès du mobile, par exemple :
  - Demande d'envoi des identifiants (TMSI, IMSI, IMEI),
  - Demande d'envoi de position GPS.

Un mode dit « semi-actif » : les échanges entre le réseau composé d'un ou plusieurs terminaux et le mobile sont suivis en mode « passif » jusqu'à l'établissement de la communication. Au moment où le mobile transmet sa capacité de chiffrement (A5/1 ou A5/2 dans la plupart des cas), l'intercepteur émet un signal de perturbation (qui permet de neutraliser le message envoyé par le mobile) avant de transmettre – à la place du mobile – un « ordre » de non-chiffrement (cela se traduit par l'émission d'un signal contenant un message signifiant que le mobile ne supporte que le mode A5/0, algorithme de non-chiffrement). Cette technique permet de suivre le reste de la communication en mode « passif » puisque les échanges ne seront pas chiffrés. Pour réaliser ce mode :

- Le module dédié à l'émission du signal correspondant au spotbeam virtuel génère le signal de perturbation permettant de neutraliser les messages envoyés par le mobile, et émet les messages virtuels indiquant au réseau Thuraya que le mobile ne dispose pas de capacité de chiffrement,
- Le module dédié aux canaux montants décode les informations transmises par les mobiles au réseau ainsi que les messages émis par le module d'émission (ces informations sont dans ce cas toujours transmises en clair),
- Le module dédié aux canaux descendants décode les informations émises par le réseau Thuraya.

Un mode dit « passif » : l'intercepteur 19 démodule et décode en permanence les messages en clair (i.e. non chiffrés), sans intervenir directement sur les échanges entre le mobile et le satellite. Notons que l'intercepteur 19 est capable de se synchroniser sur les canaux de « broadcast » ainsi que sur les canaux de trafic de type FACCH et NT lorsqu'une communication est amorcée (à partir des informations décodées sur les canaux de « broadcast » BCCH et AGCH/PCH) afin d'extraire le maximum d'informations venant du mobile.

Le fonctionnement du mode passif est le suivant :

- Le module de démodulation et de décodage des canaux descendants veille en permanence le canal BCCH (pour avoir les dernières informations sur le réseau) et le canal AGCH.
- En parallèle, le module de démodulation et de décodage des canaux montants veille en permanence le canal RACH.

- Dès qu'une requête de communication est envoyée par un mobile sur le canal RACH, elle est démodulée et décodée.
- Le module recherche ensuite le message d'allocation de communication correspondant sur le canal AGCH grâce au numéro aléatoire unique attribué au RACH qui doit être le même pour le message AGCH associé. L'association du message AGCH au message RACH associé est confirmée par la valeur du paramètre « GPS discriminator » qui est un identifiant contenu lui aussi dans les deux messages.
- Le module récupère alors dans le message AGCH les paramètres temporels et fréquentiels du canal qui a été attribué au mobile ayant demandé la communication.
- Le module se synchronise sur le canal décrit, comme le montrent les figures 4 et 5.
- Une fois synchronisé, le module démodule et décode en permanence les messages de trafic (type NT et FACCH) échangés entre le mobile et le réseau sur le canal de trafic. Le contenu de ces messages est analysé et les informations sensibles sauvegardées. Voici les informations auxquelles on peut ainsi avoir accès :
  - TMSI, IMSI.
  - Position GPS.
  - Numéro appelé.
  - Chiffrement utilisé (A5/x), clés SRES et RAND utilisés.
  - Type de service demandé (appel, SMS, mise à jour de position GPS…).

- Lorsque la communication se termine, un détecteur d'activité basé sur le calcul du nombre de trames de bruit de confort permet de stopper le suivi.

Le train binaire correspondant aux informations chiffrées est, lui, enregistré dans un fichier dédié.

Pour exécuter les étapes de décodage du trafic descendant et du trafic montant, le procédé exécute différentes étapes dont l'étape de synchronisation selon l'invention détaillée ci-après.

Canaux descendants

Les canaux FACCH descendants permettent au réseau de transmettre des informations au téléphone satellite ou « MES » (abrégé anglo-saxon de Mobile Earth Station) lors d'une transaction (appel, *location update*…). Ces canaux ne sont actifs qu'après l'allocation des ressources par le réseau (c'est-à-dire après l'échange RACH/AGCH). Sur ces canaux, se trouvent en particulier des informations sur le chiffrement utilisé lors de la communication. Suivant le type de communication établie la longueur de ces *bursts* peut être de 3, 6 ou 9 IT (Intervalle Temporel).

Synchronisation temporelle

Les créneaux ou « *bursts* » NT3 sont envoyés à des instants définis dans le message AGCH, responsable de l'allocation des ressources temporelles et fréquentielles pour la communication Thuraya.

Pour éviter de consommer des ressources inutilement, le conditionneur de trafic n'est appelé que lorsqu'une attribution de canal a été détectée. On considère qu'une communication est détectée lorsqu'on reçoit un message de type « *Immediate Assignment* » (message de type DC6). Ce message contient en particulier les paramètres suivants :

- la fréquence attribuée en *downlink* et en *uplink*,
- les IT utilisés en *downlink* et en *uplink (*c'est-à-dire le numéro du time slot dans la trame TDMA*)*,
- le type de canal alloué (NT3 NT6 ou NT9),
- la raison de l'attribution d'un canal dédié (appel entrant, appel sortant, « *location update* »…),
- la référence du RACH correspondant à la requête de la MES.

Grâce à tous ces paramètres, il est possible de tracer la transaction entre la MES et le réseau, de se synchroniser sur les IT voulus et d'enregistrer l'échange (voix, fax…).

La figure 4 représente le principe de suivi d'une communication en fonction des paramètres décodés dans les créneaux DC6 (AGCH/PCH).

La synchronisation est prise par rapport au début des *bursts* BCCH (par analogie à la synchronisation des RACH). Les éléments nécessaires au calcul de la position temporelle sont les suivants :

- Le numéro d'IT qui marque le début des *bursts* BCCH dans les trames qui en contiennent (fourni en nombre d'IT dans le segment 2Abis des *bursts* BCCH),
- Le numéro d'IT qui marque le début des *bursts* NT3 dans les trames qui en contiennent (fourni en nombre d'IT dans le message « Immediate Assignment »),
- L'affinement de la position temporelle du début des *bursts* BCCH (fourni en nombre de symboles dans le segment 1A des *bursts* BCCH).

Le temps de début des *bursts* NT3 (par rapport au début d'une trame contenant le BCCH de référence) vaut alors, par exemple, exprimé en ms :

$$T_{départ}(NT3) = (40 - IT_{départ}(BCCH) \times \frac{5}{3}) + IT_{départ}(NT3) \times \frac{5}{3} + \Delta_{départ}(BCCH) \times \frac{1}{23.4}$$

où 5/3 est la durée en ms d'un intervalle temporel, IT, et 23.4 est la vitesse symbole en kbds.

Grâce à ce calcul, l'intervalle d'échantillons susceptible de contenir un *burst* NT3 est déterminé et donc, il est possible d'appeler le démodulateur uniquement dans cet intervalle. Cet appel est répété pour chaque trame à partir du début de la communication : chacune est susceptible de contenir, soit un *burst* NT3 (FACCH3/TCH3), soit un *burst* DKAB (bruit de confort). Le démodulateur est capable de faire la différence par une série de tests discriminatoires sur la modulation utilisée et l'énergie des bursts comme il est mentionné dans la suite de la description.

Le traitement est arrêté dès que le démodulateur détecte un nombre de *bursts* « inconnus » (sous-entendu différents des NT3 ou des DKAB) trop important (10 typiquement). La communication est considérée comme étant terminée.

La date de début des NT3 en voie descendante est calculée en date absolue (par rapport au début de l'acquisition). Cette date est ensuite utilisée pour réaliser le décodage des NT3 en voie montante qui ne dispose pas d'autre référence de temps que celle du début de l'acquisition.

Démodulation

La séparation du canal de trafic n'est réalisée qu'aux instants où le canal est actif. Le principe consiste donc à ne séparer que la partie du signal contenant le *burst* NT3, NT6 ou NT9.

La démodulation des *bursts* NT3 diffère selon le type de *burst* NT3 émis. En effet, les *bursts* peuvent être de type FACCH3, TCH3 ou bien DKAB. Les *bursts* FACCH3 sont quant à eux de 2 types : type 0 et type 1. Chaque type de burst est envoyé en alternance (type0, type1, type 0,…) par paquet de 4 *bursts* pour former un message complet.

De plus, le système envoie au mobile une valeur appelée *Timing Advance* permettant au mobile de se synchroniser temporellement par rapport à sa position géographique (principe équivalent au *Timing Advance* en GSM). Ce décalage est en général de quelques ms. Il est donc nécessaire pour l'intercepteur de réaliser une première synchronisation symbole pour se synchroniser parfaitement avec les canaux de trafic associés.

Les séquences de synchronisation sont très courtes pour ce type de *burst*, et par expérience il est connu que la synchronisation symbole est difficile voire impossible à réaliser sur des *bursts* NT3 de type 0 (la séquence associée donne lieu à trop d'ambiguïtés). En revanche les résultats obtenus sur les *bursts* NT3 de type 1 sont sans ambiguïté. Avantageusement, le procédé réalise une synchronisation symbole uniquement sur les *bursts* NT3 de type 1. Cette synchronisation est ensuite gardée comme référence pour les autres *bursts*. A l'apparition d'un burst NT3 de type 1, une synchronisation est de nouveau réalisée (elle permet en outre de vérifier d'éventuelles dérives de synchronisation).

Si les *bursts* ne sont pas de type FACCH3 (modulation π/4-CBPSK), une identification du type de *burst* est ensuite réalisée. Il faut en effet identifier s'il s'agit d'un *burst* de trafic (modulé en π/4-CQPSK), d'un *burst* DKAB ou encore de la fin de la communication. L'identification est basée, par exemple, sur les critères suivants :

- EQM des symboles démodulés (si celle-ci est supérieure à un seuil pour N *bursts* consécutifs, la communication est considérée comme ayant été interrompue),
- Répartition statistique des symboles démodulés (25% de symboles dans chaque quadrant de la constellation),

- Energie du signal dans les zones DKAB (zones appelées EchantillonDebutDKAB et EchantillonFinDKAB).

Ces critères permettent alors d'identifier les *bursts* suivants : TCH3, DKAB, BURST NULL (plus d'émission).

A titre d'exemple, la figure 6 représente la synchronisation d'un *burst* FACCH3 de type 0 et de type 1. Le *burst* FACCH3 de type 1 ne présente qu'un maximum autour de la zone de synchronisation, ce qui n'est pas le cas du *burst* de type 0.

Cas des canaux de trafics montant

Les canaux montants de signalisation dédiée transmettent des informations qui nous renseignent sur l'identité du mobile (TMSI, IMSI, IMEI ou IMEISV), sa capacité de chiffrement (A5/1 à A5/7). Ces données transitent au moins lors de la mise sous tension ou lors de l'établissement d'un appel.

L'objectif est de capturer ces données lors de la transmission des messages de signalisation sur les canaux de signalisation rapide FACCH3.

Synchronisation temporelle

Comme pour la voie descendante, la démodulation nécessite la connaissance de la position (temporelle et fréquentielle) des *bursts* NT3, position transmise en voie descendante dans le *burst* AGCH décrivant l'allocation des ressources fixées par le réseau. Il est donc à ce niveau impératif d'obtenir une démodulation duplex parfaitement synchronisée entre la voie *downlink* et la voie *uplink*. Dans ce cas, le démodulateur voie montante reçoit la date absolue de début des *bursts* de signalisation dédiée par rapport à la date de début de l'acquisition. Lorsque cette date est connue, le démodulateur fonctionne de la même manière que celui de la voie descendante.

La figure 7 schématise le principe de synchronisation temporelle en mode duplex.

Il est plus facile de réaliser des acquisitions simplex, que ce soit en voie montante ou en voie descendante. Afin d'augmenter le nombre de tests sur antenne, un mode dit « mono voie » réalise de manière aveugle la synchronisation temporelle et fréquentielle des canaux de signalisation et de trafic dédié. Cette technique est résumée dans le schéma fonctionnel décrit à la figure 8.

Une première étape consiste à réaliser une détection d'énergie dans les 4 canaux de trafic possible en voie montante (le niveau de bruit est estimé en prenant le spectre d'énergie la plus faible parmi les 4 canaux). Cette détection donne le numéro de canal dans lequel aura lieu l'émission des *bursts*. Une séparation de ce

canal est ensuite réalisée, puis une identification du type de *burst*. Cette identification est réalisée en réalisant l'intercorrélation du signal reçu avec l'ensemble des séquences possibles pour les *bursts* de type FACCH3 (procédé qui sera généralisé aux bursts de type FACCH6 et FACCH9). En sortie de cet identifieur, le type de canal utilisé est obtenu ainsi que la position temporelle du *slot* TDMA. La démodulation est ensuite réalisée en se déplaçant à chaque fois d'une trame TDMA.

Application à la perturbation d'une communication

Selon un mode de fonctionnement, le système peut fonctionner en mode « actif » et émettre un signal permettant de perturber une communication.

Fonction de perturbation Thuraya : cette fonction a pour objectif de neutraliser une communication Thuraya en cours, après synchronisation sur les canaux de communication. La synchronisation sera effectuée selon les étapes décrites précédemment.

Le mode utilise l'antenne bande L pour émettre une forme d'onde avec une puissance suffisante pour perturber les messages émis par le mobile en cours de communication.

Le fonctionnement de ce mode comporte, par exemple, les étapes suivantes :

- Le module de démodulation et de décodage des canaux descendants veille en permanence le canal BCCH (pour avoir les dernières informations sur le réseau) et le canal AGCH (pour intercepter les messages d'établissement de communication).
- Lorsque le module détecte un message d'allocation de communication sur le canal AGCH, il récupère alors dans le message AGCH les paramètres temporels et fréquentiels du canal qui a été attribué au mobile ayant demandé la communication.
- Le module se synchronise sur le canal décrit, comme le montrent les figures 4 et 5. Une fois synchronisé, le module d'émission du signal perturbateur prend le relais et neutralise les messages de trafic (type NT et FACCH) échangés entre le mobile et le réseau sur le canal de trafic montant comme il est représenté aux figures 9 et 10.

Le procédé et le dispositif selon l'invention reposant sur le principe actif de l'interception, le procédé consiste notamment) leurrer le mobile en émettant un signal équivalent du satellite, présentent les avantages suivants :

- il est possible d'interroger un mobile et d'obtenir toutes les informations sur ce dernier,
- les mobiles satellites peuvent de plus se connecter automatiquement sur un réseau GSM dès que ce dernier est présent dans la zone où se trouve le mobile. Le réseau GSM peut alors être neutralisé pour forcer le mobile à se connecter sur le réseau satellite,
- en fonctionnement normal, l'invention ne nécessite pas de module de chiffrement.

REVENDICATIONS

1 – Procédé pour intercepter des communications échangées entre au moins un premier terminal et un deuxième terminal, caractérisé en ce qu'il comporte une étape au cours de laquelle au moins un signal de simulation identique à celui ou ceux émis par l'un des deux terminaux est émis au moyen d'un dispositif d'interception et une étape de synchronisation des échanges de communication sur le canal de trafic, comprenant une étape où l'on détermine les instants d'émission des bursts responsables de l'allocation des ressources pour la communication et une étape d'appel du démodulateur dans les intervalles d'échantillons susceptibles de contenir ces bursts afin d'obtenir les caractéristiques de la communication interceptée ou sur laquelle la synchronisation a été effectuée.

2 – Procédé selon la revendication 1, caractérisé en ce que le signal émis est un signal de simulation de canal de diffusion avec une puissance suffisante identique à celui émis par un terminal satellite, et en ce qu'un mobile tente de s'inscrire sur ledit signal et en ce qu'il comporte une étape d'interrogation dudit mobile.

3 – Procédé selon la revendication 2, caractérisé en ce que ledit procédé exploite les informations de type IMSI, TMSI présentes dans la communication interceptée.

4 – Procédé selon la revendication 1, caractérisé en ce que le signal émis par l'intercepteur est émis après établissement d'une communication entre un mobile terminal et un réseau, et en ce qu'au moment où un mobile transmet par message sa capacité de chiffrement, le signal émis est un signal adapté à neutraliser ledit message, et en ce que le mobile dédié aux canaux montants entre le mobile et le réseau décode les informations émises par le mobile au réseau, et le module dédié aux canaux descendants décode les informations émises par le réseau.

5 – Procédé selon la revendication 1, caractérisé en ce que les bursts considérés sont les bursts NT3 et en ce que le temps de début desdits bursts NT3 est déterminé en tenant compte du numéro IT qui marque le début des bursts BCCH

dans les trames et du numéro IT qui marque le début des bursts NT3 dans les trames.

6 – Procédé selon la revendication 5, caractérisé en ce que le temps de début des *bursts* NT3, par rapport au début d'une trame contenant le BCCH de référence, vaut alors, par exemple, exprimé en ms :

$$T_{départ}(NT3) = (40 - IT_{départ}(BCCH) \times \frac{5}{3}) + IT_{départ}(NT3) \times \frac{5}{3} + \Delta_{départ}(BCCH) \times \frac{1}{23.4}$$

où 5/3 est la durée en ms d'un intervalle temporel, IT, et 23.4 est la vitesse symbole en kbds.

7 – Procédé selon l'une des revendications 5 ou 6, caractérisé en ce qu'il utilise les bursts NT3 de type 1.

8 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'après avoir intercepté le message échangé entre les deux terminaux, il comporte en outre une étape où le message d'allocation de communication sur un canal est détecté, une étape de récupération des paramètres temporels et fréquentiels du canal attribué à un mobile, une étape de synchronisation sur le canal trouvé et une étape d'émission d'un signal perturbateur qui prend le relais sur les messages de trafic échangés entre un premier terminal et le réseau sur le canal de trafic montant.

9 – Dispositif permettant d'intercepter une ou plusieurs communications entre deux équipements comportant en combinaison au moins un module d'émission d'un signal identique à celui émis par l'un des deux équipements, un dispositif de synchronisation (32) adapté à déterminer les instants d'émission des créneaux ou « bursts » responsables de l'allocation des ressources pour la communication et un moyen permettant de générer un appel du démodulateur dans les intervalles d'échantillons susceptibles de contenir ces créneaux ou « bursts » afin d'obtenir les caractéristiques de la communication interceptée ou sur laquelle la synchronisation a été effectuée.

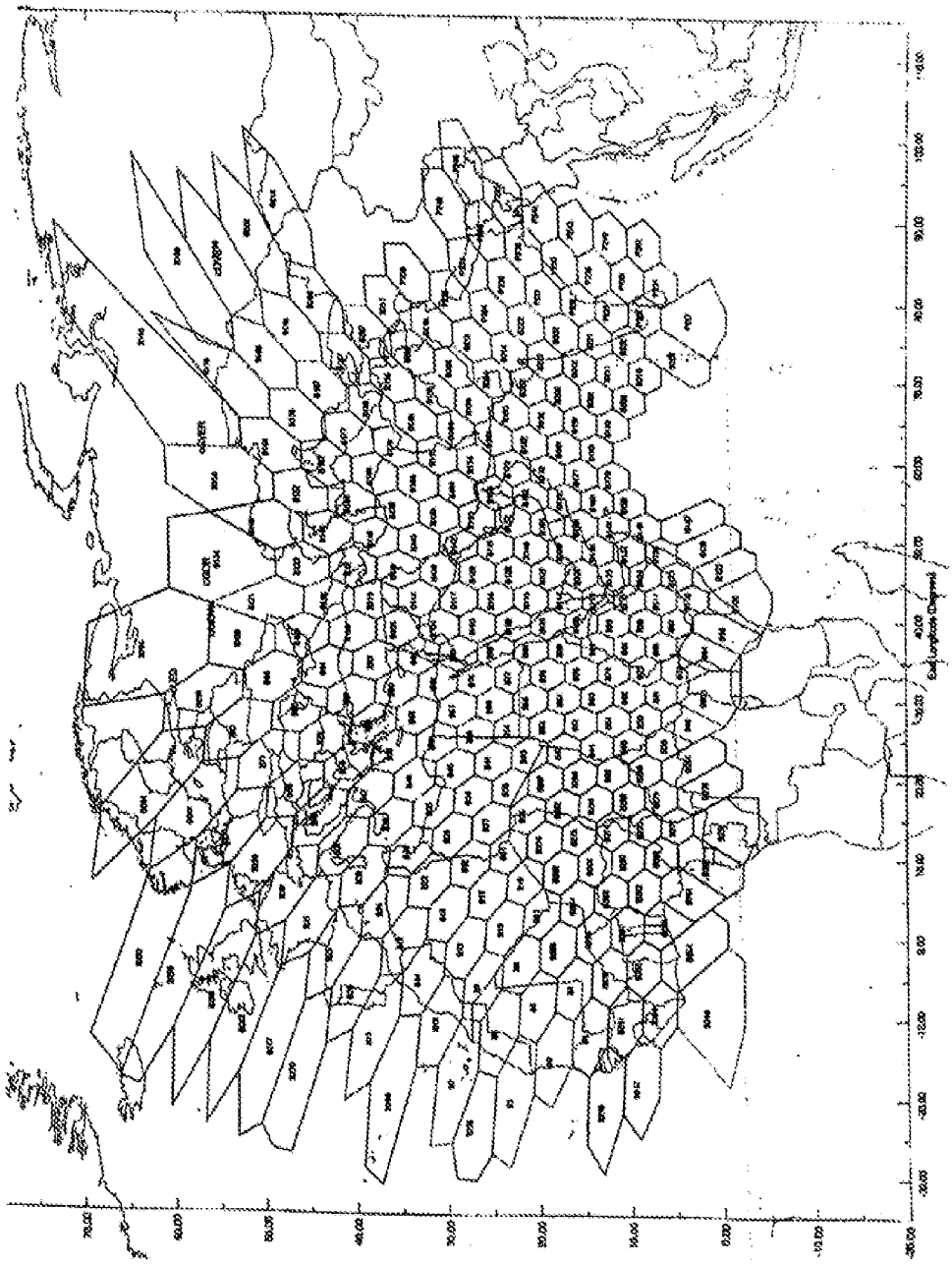


FIG.1

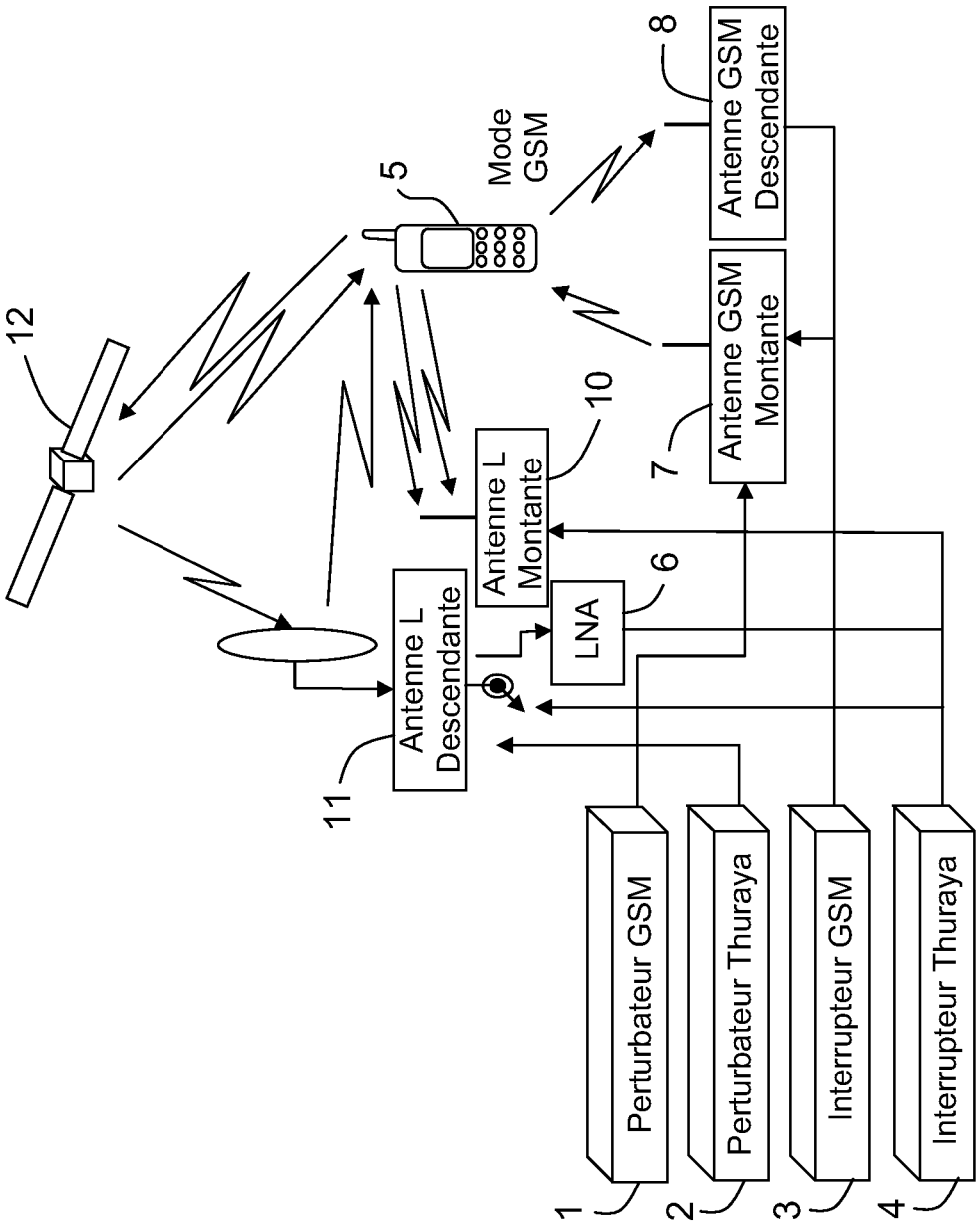

12
5
Mode GSM
8
Antenne GSM Descendante
Antenne GSM Montante
7
10
Antenne L Montante
LNA
6
Antenne L Descendante
11
Perturbateur GSM
Perturbateur Thuraya
Interrupteur GSM
Interrupteur Thuraya
1
2
3
4

FIG.2

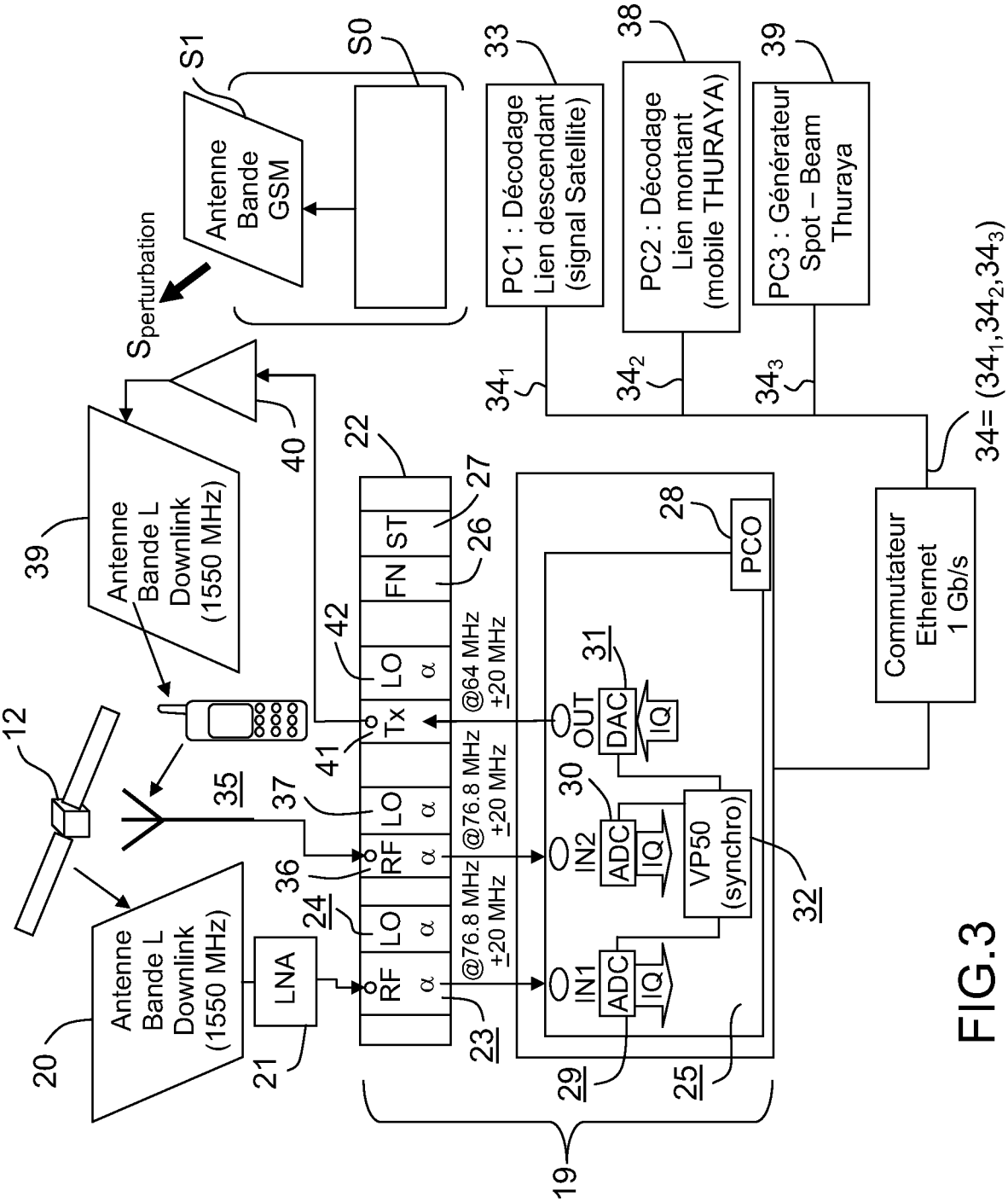

S1
S0
Antenne Bande GSM
Sperturbation
33
PC1 : Décodage Lien descendant (signal Satellite)
38
PC2 : Décodage Lien montant (mobile THURAYA)
39
PC3 : Générateur Spot – Beam Thuraya
34= (34$_1$,34$_2$,34$_3$)
34$_1$
34$_2$
34$_3$
Commutateur Ethernet 1 Gb/s
28
PCO
22
27
26
FN
ST
42
LO
α
41
Tx
@64 MHz ±20 MHz
31
OUT
DAC
IQ
30
IN2
ADC
IQ
@76.8 MHz ±20 MHz
37
RF
LO
α
36
24
23
IN1
ADC
IQ
VP50 (synchro)
32
29
25
19
12
35
39
Antenne Bande L Downlink (1550 MHz)
40
20
Antenne Bande L Downlink (1550 MHz)
LNA
21

FIG.3

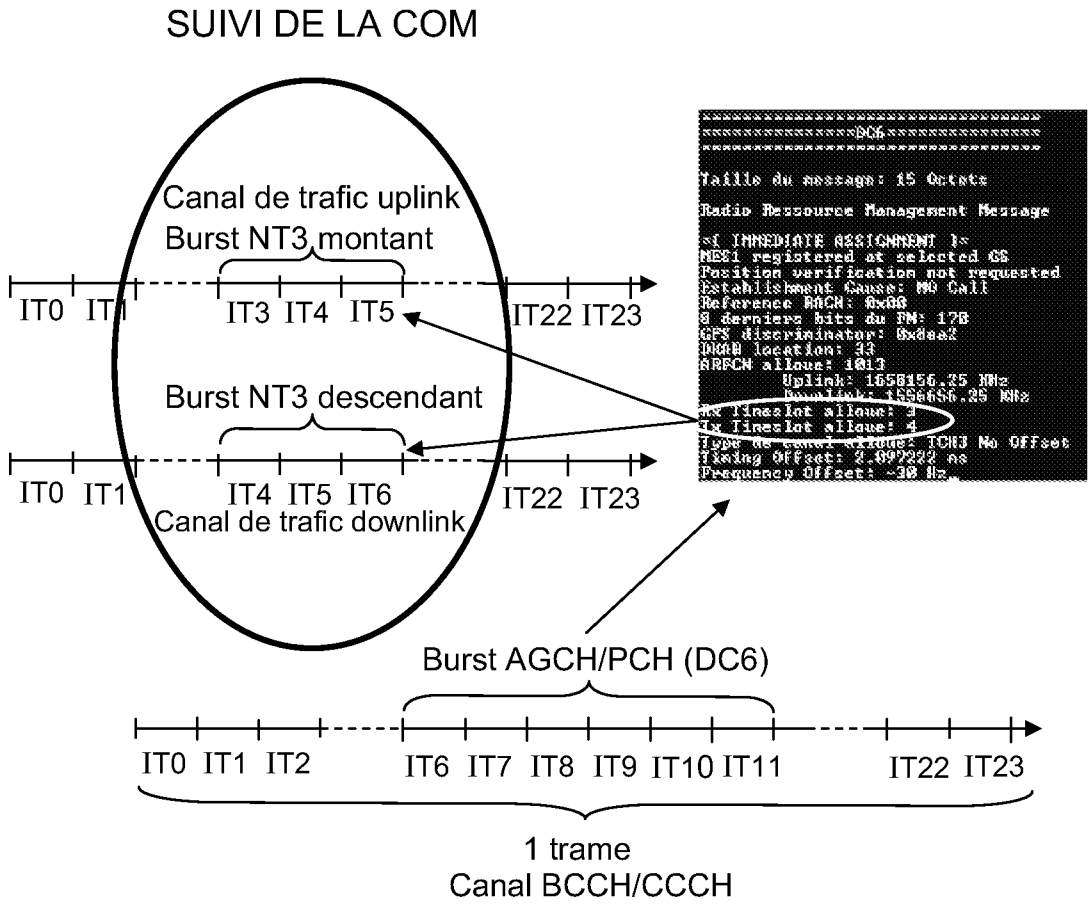

SUIVI DE LA COM
Canal de trafic uplink
Burst NT3 montant
IT0 IT1
IT3 IT4 IT5
IT22 IT23
Burst NT3 descendant
IT0 IT1
IT4 IT5 IT6
IT22 IT23
Canal de trafic downlink
Taille du message: 15 Octets
Radio Ressource Management Message
MES1 registered at selected CS
Position verification not requested
Establishment Cause: MO Call
Reference AACH: 0xA8
8 derniers bits du FN: 178
GPS discriminator: 0xdaa2
DRAN location: 33
ARFCH alloue: 1013
Uplink: 1658156.25 MHz
Downlink: 1596656.25 MHz
Burst AGCH/PCH (DC6)
IT0 IT1 IT2
IT6 IT7 IT8 IT9 IT10 IT11
IT22 IT23
1 trame
Canal BCCH/CCCH

FIG.4

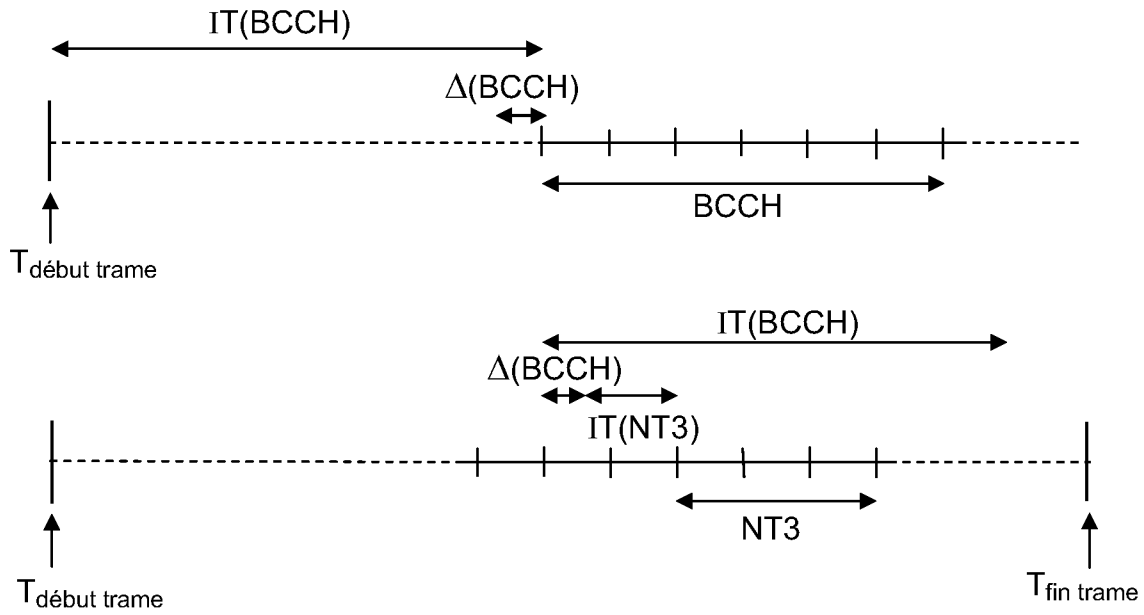
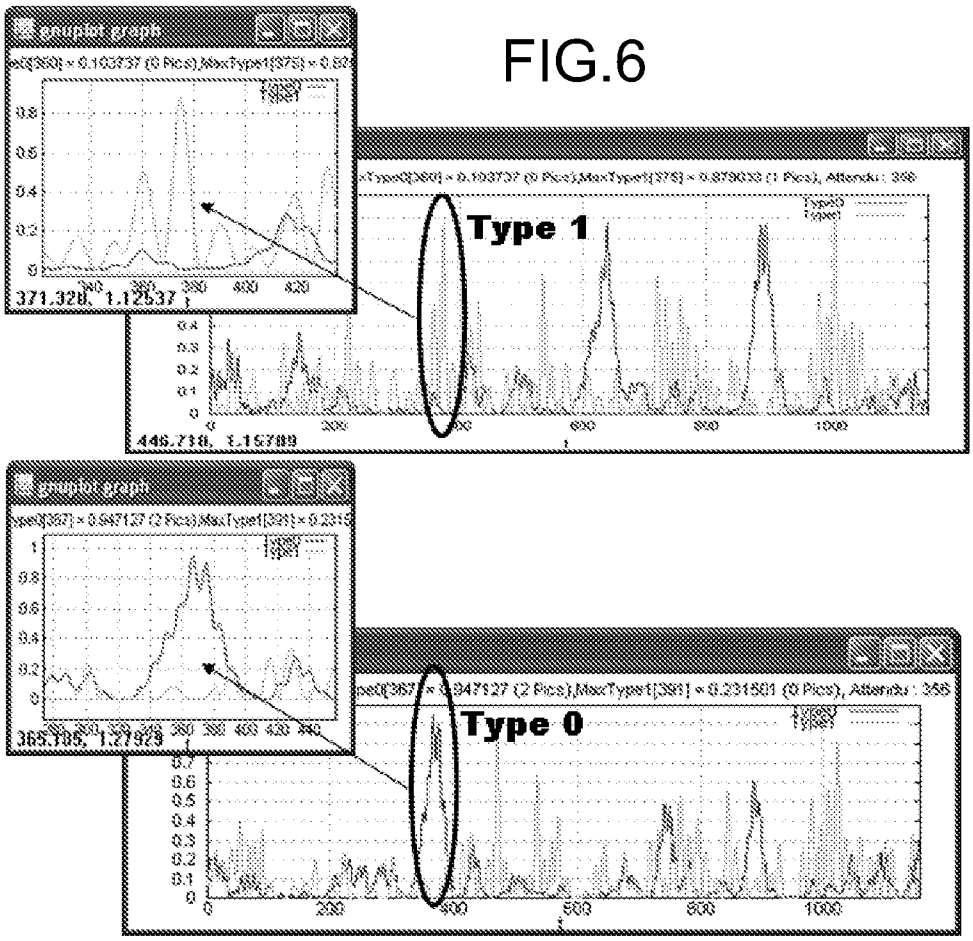

IT(BCCH)
Δ(BCCH)
BCCH
T début trame
IT(BCCH)
Δ(BCCH)
IT(NT3)
NT3
T début trame
T fin trame

FIG.5

FIG.6


gnuplot graph
Type 1
gnuplot graph
Type 0

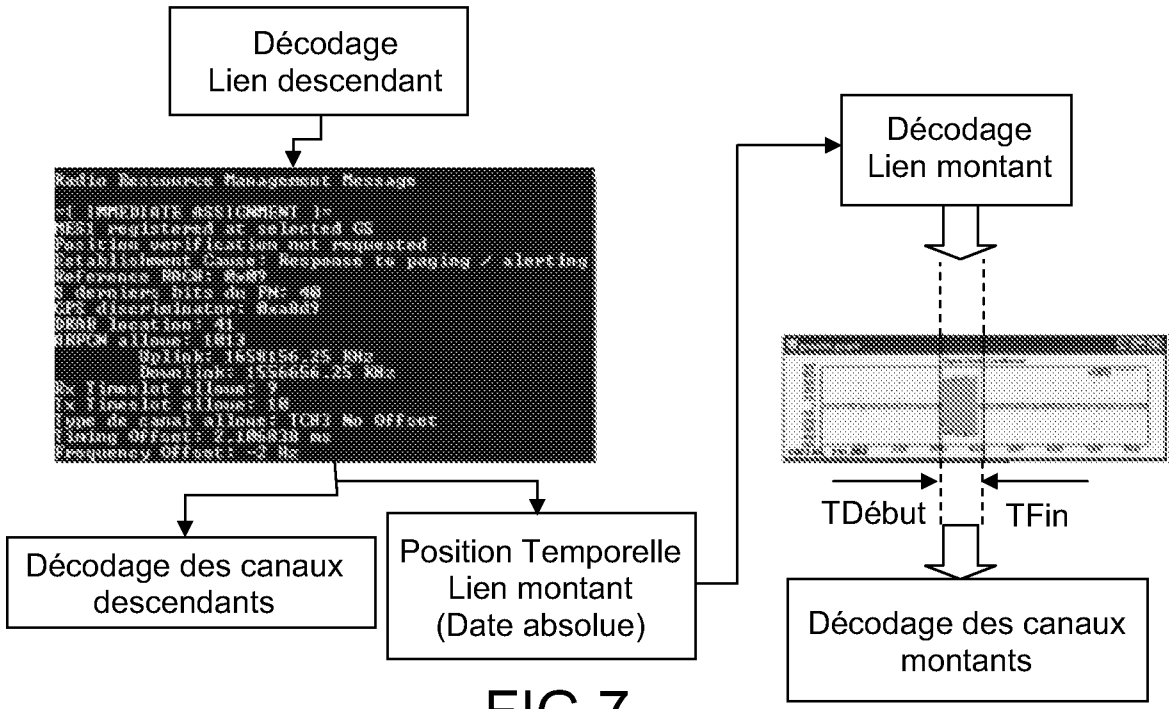

Décodage
Lien descendant
Décodage
Lien montant
TDébut
TFin
Décodage des canaux
descendants
Position Temporelle
Lien montant
(Date absolue)
Décodage des canaux
montants

FIG.7

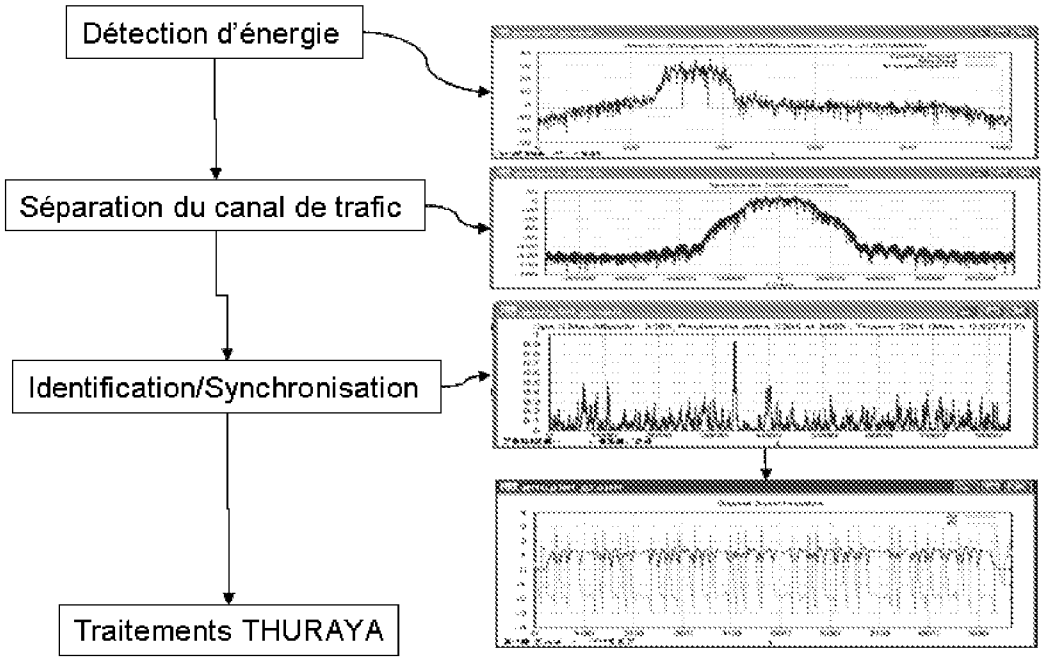

Détection d'énergie
Séparation du canal de trafic
Identification/Synchronisation
Traitements THURAYA

FIG.8

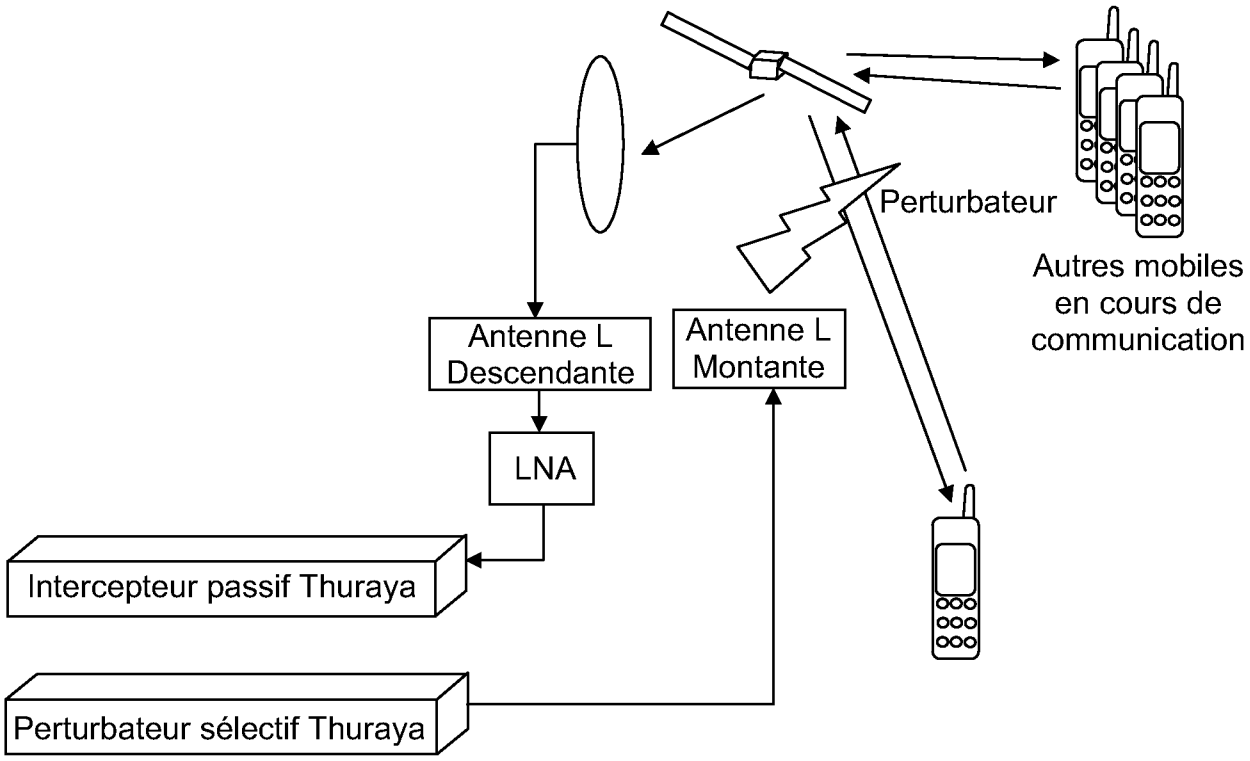

Perturbateur
Autres mobiles
en cours de
communication
Antenne L
Descendante
Antenne L
Montante
LNA
Intercepteur passif Thuraya
Perturbateur sélectif Thuraya

FIG.9

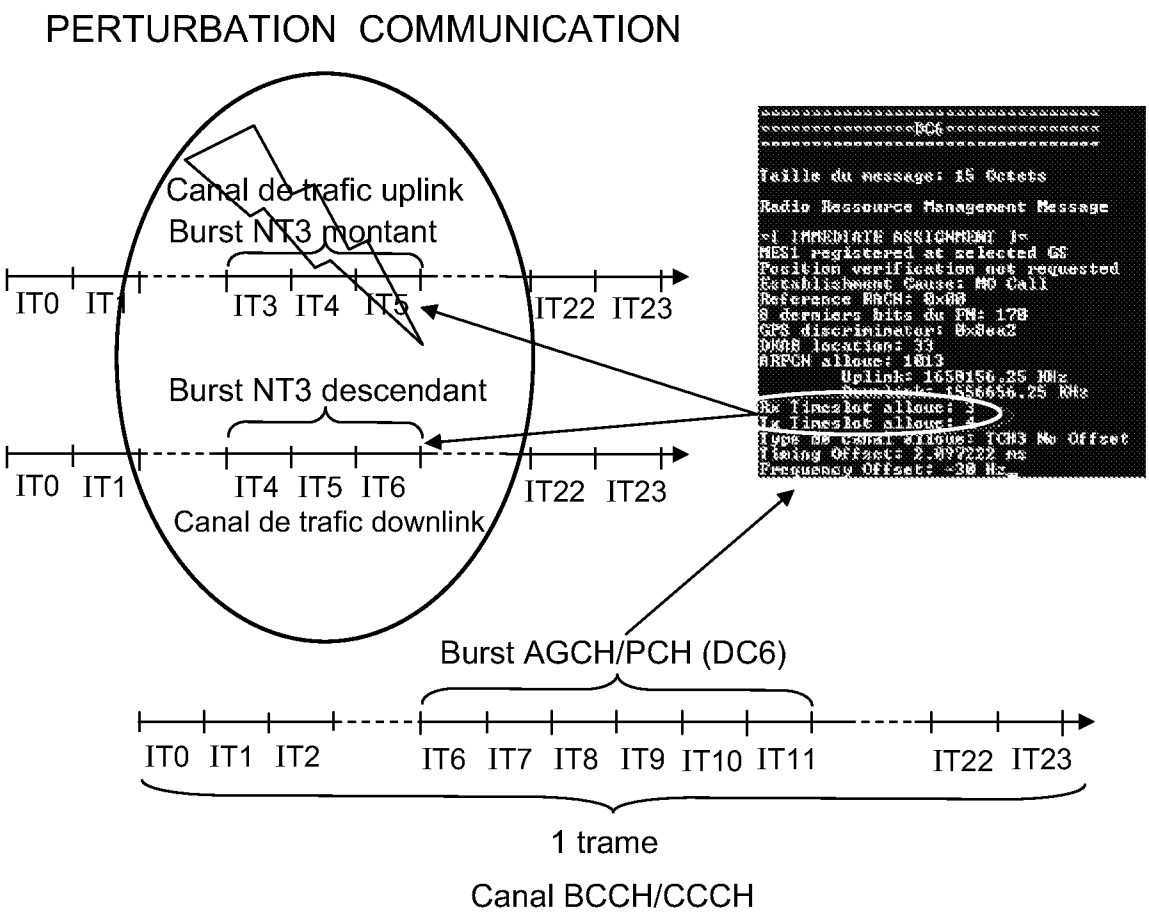

PERTURBATION COMMUNICATION
Canal de trafic uplink
Burst NT3 montant
IT0 IT1 IT3 IT4 IT5 IT22 IT23
Burst NT3 descendant
IT0 IT1 IT4 IT5 IT6 IT22 IT23
Canal de trafic downlink
Taille du message: 15 Octets
Radio Ressource Management Message
Burst AGCH/PCH (DC6)
IT0 IT1 IT2 IT6 IT7 IT8 IT9 IT10 IT11 IT22 IT23
1 trame
Canal BCCH/CCCH

FIG.10

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/064310

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04M H04L H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2006/111974 A (ELTA SYSTEMS LTD [IL]; GILOH BENJAMIN [IL]) 26 October 2006 (2006-10-26) abstract page 1, lines 2,3 page 2, lines 4-24 page 4, line 4 - page 5, line 17 page 7, lines 19-27 page 8, lines 13-30 page 9, lines 20-29 page 11, lines 10-20 page 14, line 10 - page 24, line 16 figures claims ----- -/--	1-9

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 février 2009	16/02/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Dejonghe, Olivier

3

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/064310

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FR 2 869 189 A (THALES SA [FR]) 21 October 2005 (2005-10-21) abstract page 3, lines 1-25 page 4, lines 32-34 page 6, line 25 - page 7, line 12 figures claims	1-9
A	DE 197 49 388 A1 (SIEMENS AG [DE]) 20 May 1999 (1999-05-20) the whole document	1-9
A	WO 2007/088344 A (M M I RES LTD [GB]; MARTIN PAUL MAXWELL [GB]; DOLBY RIKI BENJAMIN [GB]) 9 August 2007 (2007-08-09) the whole document	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2008/064310

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006111974 A	26-10-2006	AU 2006238431 A1	26-10-2006
		CA 2605623 A1	26-10-2006
		EP 1894321 A1	05-03-2008
		HK 1112338 A1	24-10-2008
		JP 2008537431 T	11-09-2008
		KR 20080017307 A	26-02-2008
		US 2008287123 A1	20-11-2008
FR 2869189 A	21-10-2005	AT 377333 T	15-11-2007
		CN 1973564 A	30-05-2007
		DE 602005003121 T2	21-08-2008
		EP 1747695 A1	31-01-2007
		WO 2005112497 A1	24-11-2005
		ES 2296164 T3	16-04-2008
		US 2008020749 A1	24-01-2008
DE 19749388 A1	20-05-1999	NONE	
WO 2007088344 A	09-08-2007	EP 1992103 A1	19-11-2008
		US 2009023424 A1	22-01-2009

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2008/064310

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04M H04L H04B

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela estréalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	WO 2006/111974 A (ELTA SYSTEMS LTD [IL]; GILOH BENJAMIN [IL]) 26 octobre 2006 (2006-10-26) abrégé page 1, ligne 2,3 page 2, ligne 4-24 page 4, ligne 4 - page 5, ligne 17 page 7, ligne 19-27 page 8, ligne 13-30 page 9, ligne 20-29 page 11, ligne 10-20 page 14, ligne 10 - page 24, ligne 16 figures revendications ----- -/--	1-9

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
9 février 2009	16/02/2009

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Dejonghe, Olivier

3

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	FR 2 869 189 A (THALES SA [FR]) 21 octobre 2005 (2005-10-21) abrégé page 3, ligne 1-25 page 4, ligne 32-34 page 6, ligne 25 - page 7, ligne 12 figures revendications	1-9
A	DE 197 49 388 A1 (SIEMENS AG [DE]) 20 mai 1999 (1999-05-20) le document en entier	1-9
A	WO 2007/088344 A (M M I RES LTD [GB]; MARTIN PAUL MAXWELL [GB]; DOLBY RIKI BENJAMIN [GB]) 9 août 2007 (2007-08-09) le document en entier	1-9

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2008/064310

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2006111974 A	26-10-2006	AU 2006238431 A1	26-10-2006
		CA 2605623 A1	26-10-2006
		EP 1894321 A1	05-03-2008
		HK 1112338 A1	24-10-2008
		JP 2008537431 T	11-09-2008
		KR 20080017307 A	26-02-2008
		US 2008287123 A1	20-11-2008
FR 2869189 A	21-10-2005	AT 377333 T	15-11-2007
		CN 1973564 A	30-05-2007
		DE 602005003121 T2	21-08-2008
		EP 1747695 A1	31-01-2007
		WO 2005112497 A1	24-11-2005
		ES 2296164 T3	16-04-2008
		US 2008020749 A1	24-01-2008
DE 19749388 A1	20-05-1999	AUCUN	
WO 2007088344 A	09-08-2007	EP 1992103 A1	19-11-2008
		US 2009023424 A1	22-01-2009