

19 RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
COURBEVOIE

11 N° de publication :
(à n'utiliser que pour les
commandes de reproduction)

3 060 933

21 N° d'enregistrement national : 16 62475

51 Int Cl⁸ : H 04 W 52/28 (2017.01), H 04 W 4/02, 84/12, 80/08

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 15.12.16.

30 Priorité :

43 Date de mise à la disposition du public de la demande : 22.06.18 Bulletin 18/25.

56 Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

60 Références à d'autres documents nationaux apparentés :

Demande(s) d'extension :

71 Demandeur(s) : ORANGE Société anonyme — FR.

72 Inventeur(s) : BOUCADAIR MOHAMED et JACQUENET CHRISTIAN.

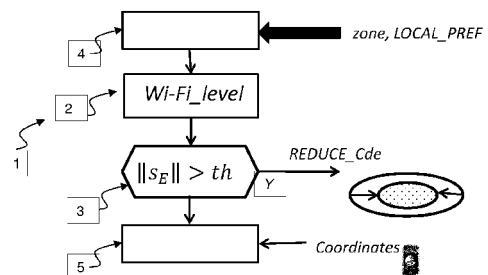
73 Titulaire(s) : ORANGE Société anonyme.

74 Mandataire(s) : ORANGE/IMT/OLPS/IPL/PAT.

54 PROCÉDE DE CONTROLE D'UN SIGNAL RADIO EMIS PAR UNE PASSERELLE, PASSERELLE ET PROGRAMME D'ORDINATEUR CORRESPONDANTS.

57 L'invention concerne un procédé de contrôle d'un signal radio émis par un dispositif pour adapter sa portée. Le procédé comprend :

- détermination (2) par un contrôleur d'un niveau (Wi-Fi_level) de signal radio émis par le dispositif en limite d'une zone déterminée,
- commande (REDUCE_Cde) par le contrôleur d'une adaptation (3) de la portée du signal radio émis par le dispositif en fonction de la comparaison du niveau de signal et d'un seuil déterminé.



FR 3 060 933 - A1



Procédé de contrôle d'un signal radio émis par une passerelle, passerelle et programme d'ordinateur correspondants.

Domaine de l'invention

Le domaine de l'invention est celui des télécommunications et plus particulièrement celui de l'adaptation de la portée du signal radio émis par une passerelle résidentielle ou des objets connectés (contexte de services déployés sur l'Internet des objets (Internet of Things)).

L'invention trouve donc des applications dans tout réseau de communication mettant en œuvre au moins une passerelle résidentielle (domestique ou d'entreprise) disposant d'un ou plusieurs composants radio de nature à émettre et recevoir des ondes de nature diverse : Wi-Fi, Bluetooth, NFC (Near Field Communication), 4G (3GPP LTE version 13 et au-delà), LoRa® WAN (Long Range Wide-area Network), etc.).

Art antérieur

Le réseau IP (« Internet Protocol ») est le support universel d'une multitude de services et applications.

Pour accéder à ces services ou applications, une passerelle résidentielle, encore appelée « box », HG pour « Home Gateway » ou CPE pour « Customer Premises Equipment », est classiquement installée chez un utilisateur. En d'autres termes, une passerelle résidentielle sert d'interface entre le réseau local de l'utilisateur et le réseau IP d'un opérateur. C'est donc l'élément concentrateur par lequel transite l'ensemble des connexions, le trafic caractéristique des différents services souscrits par le client, et qui supporte également un ensemble d'applications fournies par un opérateur de télécommunications.

Par exemple, une passerelle résidentielle permet à un utilisateur d'accéder à de multiples services IP permettant simultanément un accès à Internet, à des contenus vidéo (dont la diffusion de programmes télévisés) et à des services de voix (téléphonie sur IP, par exemple). L'offre commerciale correspondante est classiquement dite Triple Play et de manière plus large Multi-play.

En matière de connectivité, la passerelle résidentielle est raccordée d'un côté au réseau de l'opérateur et fournit côté client un ensemble d'interfaces variées : interfaces sans fil (par ex. WLAN, Bluetooth (marque déposée), etc.), prise RJ11 pour la téléphonie, prises RJ45 pour la télévision numérique et les ordinateurs, prises USB (Universal Serial Bus), port Ethernet.

Outre la fourniture de l'accès à l'ensemble des services (data, vidéo, voix) souscrits par le client, la passerelle résidentielle est également impliquée dans la gestion des fonctions qu'elle supporte (par exemple gestion des règles de translation d'adresses NAT (Network Address Translator), des filtres du pare-feu, etc.).

En matière d'applicatifs, la passerelle résidentielle intègre les logiciels utilisés pour les opérations de maintenance de la passerelle.

Un utilisateur qui veut accéder à Internet depuis un terminal, le fait très souvent en utilisant une communication sans fil, généralement de type IEEE 802.11 dit Wi-Fi (marque déposée),

établie entre son terminal et sa passerelle résidentielle.

Une telle passerelle comprend une interface d'administration, généralement accessible par le protocole HTTP (*HyperText Transfer Protocol*) mais cette interface est peu connue de la plupart des utilisateurs.

5 L'émergence des services reposant sur l'Internet des objets (IoT) est de nature à provoquer des failles sécuritaires importantes. En particulier, l'ensemble des services reposant sur l'exploitation d'objets connectés en réseau (réseau de capteurs de détection de mouvement, de détection de fumée, réseau de capteurs destinés à piloter le système d'éclairage d'une résidence, services de télémédecine reposant sur des capteurs destinés à surveiller en permanence un
10 ensemble de données biométriques, etc.) soulève inévitablement la question de la protection des données personnelles mais aussi de l'envoi d'instructions qui peuvent perturber le fonctionnement de ces objets dans leur environnement nominal.

En effet, la grande majorité des objets connectés embarquent des composants radio d'émission et de réception qui leur permettent de traiter les commandes en provenance d'un
15 contrôleur (par exemple, un Smartphone, une console locale, etc.) connecté quelque part sur l'Internet ou à l'intérieur de la zone de service délimitée par la portée du signal radio émis par la passerelle. Les composants radio sont également utilisés par ces objets connectés pour transmettre à un contrôleur soit de façon régulière (par exemple, collecte mensuelle du compteur d'électricité), soit de manière spontanée (par exemple, envoi d'une notification à un contrôleur lorsqu'un seuil de
20 données biométriques est sur le point d'être dépassé) l'ensemble des données qu'ils ont collectées. Ainsi, ces composants sont utilisés pour recevoir des instructions depuis un contrôleur telles que des instructions de mise en service, de mise en veille, etc.

Il est à ce titre primordial de préserver la confidentialité des données transmises ou reçues par ces objets connectés localisés au sein d'une zone de service. Et il est primordial de s'assurer en
25 particulier que les transmissions radio ne constituent pas un vecteur d'attaque de nature à provoquer le vol de ces données, à remettre en cause l'intégrité de ces données par des utilisateurs malveillants ou à commander d'une manière frauduleuse un objet connecté pour qu'il exécute des actions de nature contradictoire à son fonctionnement nominal et pouvant remettre en cause le bon fonctionnement du service fourni par l'objet.

30 Un risque emblématique (et avéré) de telles failles sécuritaires est celui lié à la présence d'une personne disposant d'un smartphone embarquant une fonction « contrôleur » capable de commander des objets connectés à proximité d'une résidence au sein de laquelle un réseau d'objets connectés (lampes) reposant sur la spécification LoRa[®] est déployé pour gérer le système d'éclairage : cette personne a théoriquement la capacité de piloter le système d'éclairage de ladite
35 résidence à sa guise, pour peu que les objets connectés se situent à portée de commande du contrôleur de cette personne. Dans ce contexte, la zone de service correspondant à la portée des signaux émis par les objets connectés ne peut se résumer à un espace isotrope : la gestion contrôlée

de la portée des signaux émis par de tels objets doit reposer sur une direction privilégiée de l'espace utilisé par les objets et leur contrôleur. Ces informations peuvent être échangées lors la première mise en service d'un objet connecté.

Ces failles de sécurité ont été révélées récemment lors d'une expérimentation avec un drone positionné à proximité de bâtiments équipés de lampes connectées. Des instructions ont été transmises par le drone aux lampes telles que : « éteindre toutes les lampes d'un étage, éteindre une partie des lampes, etc. ». Une attaque de ce type, menée en 2016, a fait l'objet d'articles dont celui accessible à l'adresse <https://www.engadget.com/2016/11/03/hackers-hijack-a-philips-hue-lights-with-a-drone/>. L'événement a été rapporté par le New York Times dans un article posté en ligne le 3 novembre 2016, et accessible à l'adresse http://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html?_r=0. Les produits visés dans cette attaque sont des lampes « Hue lights » commandées via une communication sans fil de type Zigbee. L'attaque a permis de montrer qu'en utilisant un drone situé à proximité de l'une des lampes, il avait été possible de répandre un virus contaminant dans le réseau de lampes et de commander ainsi l'allumage et l'extinction des lampes à partir d'un dispositif embarqué sur le drone.

Une telle attaque ciblait des lampes mais d'autres objets peuvent être visés.

De nombreux articles tels que l'article « *The Internet of Things Is Wildly Insecure -And Often Unpatchable* » accessible à l'adresse https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html et l'article accessible à l'adresse <https://events.ccc.de/congress/2014/Fahrplan/events/6166.html> font en outre état de la défaillance des solutions envisagées qui reposent sur des mécanismes de sécurité plus robustes ou sur un logiciel embarqué dans l'objet connecté pouvant être mis à jour régulièrement pour résoudre une faille sécuritaire. Cependant, il a été rapporté que le processus de mise à jour peut être défaillant et que les technologies actuelles ne supportent pas ou mal les fonctions requises pour ces solutions. Il faut noter que certaines implémentations utilisent des modèles de sécurité « simplifiés/simplistes » qui rendent la réalisation d'attaques possible. Par exemple, l'article « *Hacking into Internet Connected Light Bulbs* » accessible à l'adresse <https://www.contextis.com/resources/blog/hacking-internet-connected-light-bulbs/> expose comment le choix d'une même clé de sécurité avec un algorithme de chiffrement AES (Advanced Encryption Standard) peut sévèrement pénaliser le fonctionnement d'un réseau d'objets connectés.

Exposé de l'invention

L'invention a pour objet un procédé de contrôle d'un signal radio émis par un dispositif pour adapter sa portée. Le procédé comprend :

- détermination par un contrôleur d'un niveau de signal radio émis par le dispositif en limite d'une zone déterminée,
- commande par le contrôleur d'une adaptation de la portée du signal radio émis par le dispositif en fonction de la comparaison du niveau de signal et d'un seuil déterminé.

La zone est par défaut la zone couverte par le dispositif. Ce dispositif est par exemple une passerelle et cette passerelle embarque le contrôleur. Chaque passerelle, résidentielle ou pas, peut enregistrer des saisies d'un utilisateur. En particulier, la passerelle résidentielle enregistre une donnée descriptive de l'environnement de l'utilisateur de cette passerelle. La donnée descriptive de l'environnement peut consister en une information de dimension de l'environnement de l'utilisateur. Par exemple, il s'agit d'une distance entre la passerelle résidentielle et les murs extérieurs de la résidence de l'utilisateur. Cette distance délimite un volume considéré comme l'environnement de l'utilisateur qui détermine la zone.

Ainsi, connaissant la zone, la passerelle peut automatiquement ajuster sa portée à la limite de cette zone. En effet, connaissant sa puissance émise et un modèle de propagation, la passerelle peut déterminer la puissance à la limite de la zone. La passerelle peut ensuite ajuster la puissance émise pour que la puissance en limite de zone soit inférieure à un seuil minimal de réception admissible par un terminal qui veut s'associer à la passerelle.

Ainsi, même si un équipement électronique, par exemple un drone, peut s'approcher en limite de la zone, la résidence par exemple, il ne peut pas s'associer à la passerelle compte tenu que le signal rayonné à cette limite est inférieur au niveau de signal nécessaire pour établir une connexion.

Le dispositif peut être un objet connecté à un réseau local et contrôlé par un contrôleur. Une passerelle peut embarquer le contrôleur du dispositif ou être connectée à un tel contrôleur embarqué dans un équipement électronique tel un smartphone. La zone de rayonnement de l'objet peut alors correspondre à la zone déterminée, à une sous-zone de la zone déterminée ou à une zone différente. La zone de service de l'objet connecté peut être définie indépendamment de la zone de service d'une passerelle. Le procédé peut être activé par un objet connecté avec ou sans la présence d'une passerelle dans l'environnement utilisateur.

L'invention a en outre pour objet une passerelle résidentielle destinée à être connectée à un réseau de communication. La passerelle comprend :

- des moyens d'émission et de réception d'un signal radio,
- une mémoire pour mémoriser des données descriptives de l'environnement résidentiel d'un utilisateur de la passerelle définissant une zone,
- un calculateur pour déterminer le niveau de signal à la limite de la zone et pour comparer ce niveau à un seuil, le calculateur étant programmé pour commander l'adaptation de la portée du signal radio émis par la passerelle si le seuil est dépassé.

L'invention a en outre pour objet un système de communication comprenant une passerelle résidentielle pour le contrôle d'un signal radio émis par la passerelle. Le système est tel que la passerelle est selon un objet précédent.

Le procédé proposé apporte ainsi une solution robuste pour limiter les attaques contre un objet connecté (ou un ensemble d'objets connectés) sans faire d'hypothèse quant à la robustesse du

mécanisme de sécurité supporté ni sur le cycle de maintenance logicielle en contrôlant la portée des communications d'un tel objet connecté.

5 Selon un mode de réalisation de l'invention, la zone est déterminée en recevant et utilisant des informations de localisation transmises par un terminal mobile déplacé entre des points à la limite de la zone à délimiter.

Selon un mode de réalisation de l'invention, une passerelle résidentielle embarque le contrôleur.

Selon un mode de réalisation de l'invention, le procédé comprend en outre :

10 - enregistrement par la passerelle de données descriptives d'un environnement d'un utilisateur de cette passerelle pour déterminer les limites de la zone.

Selon un mode de réalisation de l'invention, le procédé comprend en outre :

15 - envoi d'une requête demandant sa localisation à tout terminal cherchant à s'associer à la passerelle,
- autorisation de l'association du terminal à la passerelle uniquement s'il est localisé dans la zone.

Selon un mode de réalisation de l'invention, le procédé comprend en outre :

20 - réception d'une requête d'association provenant d'un terminal comprenant la localisation de ce terminal,
- autorisation de l'association du terminal à la passerelle uniquement s'il est localisé dans la zone.

Selon un mode de réalisation de l'invention, le procédé comprend en outre :

- enregistrement par la passerelle résidentielle de préférences d'un utilisateur sur son environnement.

25 Chaque passerelle, résidentielle en particulier, peut enregistrer des préférences de l'utilisateur quant à son environnement. Les préférences sur l'environnement ont pour fonction de préciser des modalités de rayonnement de la passerelle résidentielle. Ainsi, l'utilisateur peut par exemple définir une plage horaire de rayonnement ou de non rayonnement de sa passerelle résidentielle ainsi qu'une durée de validité de ces préférences (période hors week-end). Les préférences ont des valeurs par défaut. Par défaut, elles peuvent autoriser l'adaptation de la portée
30 (puissance, fréquence, gain d'antenne, etc.).

Selon un mode de réalisation de l'invention le dispositif est un objet connecté. Le procédé comprend en outre :

35 - fourniture par le contrôleur à l'objet d'informations sur sa localisation,
- rejet par l'objet de toute requête ou commande venant du contrôleur si ce dernier est localisé en dehors de la zone déterminée.

Selon un mode de réalisation de l'invention, le dispositif embarque le contrôleur.

Selon un mode de réalisation de l'invention, la comparaison à un seuil est répétée.

La répétition de la comparaison à des instants plus ou moins réguliers permet une adaptation à des changements dans l'environnement, par exemple le déplacement d'un meuble qui a pour effet d'augmenter ou de diminuer l'atténuation du signal émis et donc de modifier la portée.

5 Une passerelle résidentielle selon l'invention est notamment adaptée à mettre en œuvre le procédé tel que décrit précédemment. Ainsi, une telle passerelle peut présenter les différentes caractéristiques relatives au procédé selon l'invention, ces caractéristiques pouvant être combinées ou prises isolément.

10 L'invention a en outre pour objet un ou plusieurs programmes d'ordinateur comportant des instructions pour la mise en œuvre d'au moins un procédé tel que décrit ci-dessus, lorsque ce ou ces programmes sont exécutés par un processeur.

L'invention a en outre pour objet un ou plusieurs supports d'informations, inamovibles, ou partiellement ou totalement amovibles, lisibles par un ordinateur, et comportant des instructions d'un ou plusieurs programmes d'ordinateur pour l'exécution des étapes d'au moins un procédé tel que décrit ci-dessus.

15 Les procédés selon l'invention peuvent donc être mis en œuvre de diverses manières, notamment sous forme câblée et/ou sous forme logicielle.

Liste des figures

20 D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante de modes de réalisation particuliers donnés à titre de simples exemples illustratifs et non limitatifs et des dessins annexés, parmi lesquels :

- la figure 1 est un schéma illustrant la zone de rayonnement ou zone de service d'une passerelle Wi-Fi,
- la figure 2 est un organigramme des principales étapes d'un procédé selon l'invention,
- les figures 3a-3d représentent des schémas illustrant un mode de réalisation selon lequel la 25 récupération de coordonnées de localisation d'un traceur associé à la passerelle permet de délimiter la zone,
- la figure 4 est un schéma illustrant la zone de rayonnement par défaut d'une passerelle Wi-Fi et la zone après optimisation, i.e., l'adaptation de sa portée et le positionnement de deux terminaux dont un TI (Terminal Interne) est dans la zone optimisée et l'autre TE (Terminal 30 Externe) est hors de la zone optimisée,
- les figures 5 et 6 sont des schémas d'échanges protocolaires selon des modes de réalisation de l'invention selon lesquels le procédé exige les coordonnées géographiques du terminal lors de son attachement au réseau ou les coordonnées géographiques du contrôleur lors de son association avec un objet connecté,
- 35 - la figure 7 est un schéma illustrant un mode de réalisation du procédé selon lequel des flux de terminaux sont redirigés vers un serveur en application de règles (*policy*),
- la figure 8 est un schéma de la structure simplifiée d'une passerelle résidentielle selon

l'invention adaptée à mettre en œuvre un procédé de contrôle selon l'invention.

Description de modes de réalisation de l'invention

Le principe général de l'invention repose sur l'adaptation de la portée du signal émis par un dispositif, en particulier une passerelle ou un objet connecté, pour diminuer le risque d'utilisation frauduleuse par un dispositif tiers. Un dispositif tiers peut être un drone qui s'approche à distance ou au plus près de l'environnement résidentiel. L'optimisation de la couverture à l'environnement résidentiel de l'utilisateur de la passerelle permet déjà de diminuer le risque précédent. La couverture peut bien entendu être limitée à une zone qui n'est pas identique à la résidence mais plus réduite ou plus étendue. Par exemple, cette zone peut être limitée à une pièce ou étendue à plusieurs pièces de plusieurs appartements.

La diminution de la portée du rayonnement revient à diminuer le niveau de signal pouvant être détecté dans cet environnement résidentiel. La zone couverte peut être restreinte, étendue, voire focalisée et donc la portée adaptée en modifiant par exemple la puissance émise, la fréquence d'émission ou par exemple en effectuant de la formation de voies ou du codage spatial. Le contrôle de la zone de couverture peut ainsi être réalisé à l'aide d'une pluralité d'antennes unidirectionnelles. Il peut bien entendu être mis en œuvre une combinaison de ces moyens pour adapter la zone couverte et donc la portée.

Ainsi, le contrôle du signal émis permet d'adapter la portée de ce signal et donc la zone couverte pour couvrir une zone de service dite optimale. La diminution de la portée peut ainsi permettre que l'énergie rayonnée ne soit plus suffisante pour qu'un dispositif tel qu'un drone puisse détecter le signal et se connecter de manière frauduleuse à un réseau distant via la passerelle ou seulement s'introduire dans un réseau local accessible via la passerelle.

La passerelle résidentielle peut en outre prendre en compte des préférences de rayonnement sur son environnement telles qu'exprimées par son utilisateur pour adapter la portée de son signal émis. La zone de rayonnement peut devenir nulle en coupant l'émission du signal, par exemple la nuit.

L'invention est décrite de manière plus détaillée dans le contexte d'une passerelle Wi-Fi, c'est-à-dire émettant un signal conforme à au moins l'un des standards de la famille IEEE802.11.

La figure 1 illustre de manière schématique la zone de service *Zdef* ou zone couverte par une passerelle qui définit la portée de cette passerelle. Il est bien entendu qu'en réalité la couverture ou portée ne suit pas une forme géométrique parfaite comme représentée sur la figure mais a un profil irrégulier qui dépend de l'environnement : murs, planchers, nature des murs et des planchers, distance aux murs, etc.

Les principales étapes de l'invention sont illustrées par l'organigramme de la figure 2. La description qui suit considère que le dispositif et la passerelle se confondent sauf indication contraire.

Le procédé 1 contrôle le signal radio émis par une passerelle CPE pour adapter sa portée. Il

est bien entendu qu'une passerelle peut émettre plusieurs signaux radio différents et qui peuvent être simultanés en fonction des capacités de la passerelle. Par exemple, la passerelle peut émettre un signal de type Wi-Fi simultanément avec un signal de type Bluetooth ou Zigbee. Le procédé peut être déployé pour contrôler plusieurs signaux émis par la même passerelle.

5 Le procédé 1 comprend la détermination 2 par la passerelle d'un niveau *Wi-Fi_level* de signal radio émis en limite d'une zone déterminée. Comme indiqué précédemment, selon un mode de réalisation le signal est celui émis par la passerelle. Selon un autre mode de réalisation, la passerelle contrôle le signal émis par un dispositif distinct. La fonction de détermination de la portée d'une interface radio locale et la fonction du contrôle d'une interface embarquée dans un
10 équipement tiers peuvent être co-localisées ou embarquées dans des équipements différents.

Selon un mode de réalisation, la passerelle affiche une zone, qui est par défaut la zone de couverture Wi-Fi. Généralement, une interface homme machine (IHM) peut permettre la saisie par l'utilisateur de données descriptives de l'environnement qui définissent la zone à prendre en compte. Selon un autre mode, les données descriptives sont récupérées par l'intermédiaire d'une
15 communication avec un traceur déplacé en limite de la zone à couvrir. D'autres interfaces de gestion peuvent être utilisées telles qu'un écran d'affichage en façade d'une passerelle ou une paire de lunettes intelligentes associée à la passerelle résidentielle.

Connaissant la zone, sa puissance émise et un modèle de propagation, la passerelle détermine le niveau de puissance émise à une distance qui correspond à la limite de la zone.

20 Le procédé 1 comprend en outre la comparaison 3 du signal émis en limite de zone à un seuil déterminé : $\|s_E\| > th$. Et si Y le signal émis s_E dépasse le seuil th alors la passerelle CPE commande *REDUCE_Cde* une adaptation de la portée du signal radio émis. La valeur du seuil peut être par défaut le seuil minimal de détection fixé par exemple dans un des standards IEEE 802.11.

Le procédé 1 peut en outre comprendre l'enregistrement 4 par la passerelle CPE de
25 données *zone* descriptives d'un environnement d'un utilisateur de cette passerelle.

Selon un mode de réalisation, l'utilisateur peut saisir des données descriptives de la résidence. L'utilisateur peut être plural, il ne s'agit pas forcément de la même personne physique qui utilise la passerelle et qui saisit les données de description. Les données descriptives de l'environnement permettent de déterminer les contours de l'environnement de l'utilisateur à
30 considérer. Les données peuvent comprendre un type de résidence (maison, appartement), un nombre de pièces à considérer, une surface globale au sol à considérer, un nombre d'étages à considérer, un nombre de pièces par étage à considérer, la localisation de la passerelle dans la résidence, etc. La limite de la zone est identifiée aux contours de l'environnement.

Selon un autre mode de réalisation illustré par les figures 3a-3d, la passerelle peut proposer
35 à l'utilisateur via une interface de gestion IHM un mode qui repose sur la récupération de coordonnées de localisation d'un terminal mobile ou traceur TR associé à la passerelle CPE. Ce traceur peut être un client Wi-Fi embarqué dans un terminal existant (smartphone, PC portable) ou

transporté par un drone, ou peut être un équipement dédié qui s'associe avec la passerelle CPE pour le seul besoin du calibrage Wi-Fi. Selon ce mode, une fois l'association *Assoc CPE TR* établie entre la passerelle CPE et le traceur, l'utilisateur est invité *START TRACE ?* à déplacer ou faire déplacer le traceur pour délimiter les contours de l'environnement et définir ainsi les données *zone*. Ainsi, le

5 traceur transmet régulièrement ses nouvelles coordonnées de localisation par exemple GPS (Global Positioning System) (ou des coordonnées ayant comme référence la localisation de la passerelle) qui permettent à la passerelle CPE de déterminer les contours de l'environnement et donc la limite de la zone de service souhaitée *Zsouv*. Connaissant sa localisation, par exemple ses propres

10 coordonnées de localisation, la passerelle peut positionner la zone par rapport à sa propre localisation. Une fois la phase de traçage terminée, la passerelle CPE invite *Optim. Wi-Fi ?* l'utilisateur à activer la procédure d'optimisation de la zone de couverture Wi-Fi. Une fois cette modification terminée *Wi-Fi optim*, la passerelle peut afficher la nouvelle zone de service *Zopt*.

Si la passerelle est déplacée, le changement de sa localisation permet automatiquement de déplacer la zone. Cependant, l'utilisateur peut être invité au déroulement d'une nouvelle étape

15 d'enregistrement par la passerelle CPE de données *zone* descriptives du nouvel environnement. Cette étape d'interaction avec l'utilisateur n'est pas nécessaire si la passerelle embarque un accéléromètre dont le but est d'ajuster la nouvelle localisation de la passerelle pour maintenir le rayonnement des interfaces radio à la zone de service définie au préalable par l'utilisateur.

Grâce à l'activation du procédé selon l'invention, un client optimise la portée du signal Wi-Fi de sa passerelle CPE comme illustré par la figure 4. Il a ainsi en particulier la possibilité de

20 limiter l'accès aux services offerts par ou via sa passerelle CPE aux seuls terminaux TI présents à l'intérieur de la zone de service et dûment habilités à bénéficier des services fournis par ou via la passerelle. Les terminaux TE externes à la zone de service ne sont plus en mesure d'initialiser des tentatives d'attachement radio avec la passerelle CPE.

25 Le traceur peut être utilisé pour vérifier si la nouvelle zone de service (c.-à-d. après optimisation) est conforme à la zone de service telle que renseignée par un utilisateur.

Une précaution supplémentaire ou alternative pour limiter l'accès aux services offerts par ou via la passerelle CPE aux seuls terminaux localisés dans une zone déterminée consiste à exiger les coordonnées géographiques du terminal lors de son attachement au réseau géré par la passerelle.

30 Cette procédure peut même être déployée si la passerelle CPE dispose de données descriptives de la zone mais ne dispose pas de mécanisme pour limiter la portée du signal radio à cette zone. Le procédé 1 peut ainsi interdire 5 toute autorisation d'association ou de connexion sous réserve de recevoir la localisation du terminal et que cette localisation soit comprise dans la zone.

Comme illustré par la figure 5, les coordonnées géographiques peuvent être fournies par le

35 terminal TE, TI dans le message de demande d'association *ASSOCIATION REQUEST(Coordinates)* ou sur demande explicite de la passerelle CPE comme illustré par la figure 6. Si la passerelle CPE ne reçoit pas les coordonnées du terminal dans le message de

demande d'association *ASSOCIATION REQUEST()*, la passerelle sollicite explicitement le terminal pour qu'il lui fournisse ses coordonnées. A cette fin, une demande d'identité *REQUEST IDENTITY(Type=Coordinates)* est envoyée au terminal avec un code précisant qu'il faut fournir les coordonnées en outre des informations de contrôle d'identité habituelles.

5 Sur réception des coordonnées venant du terminal, la passerelle CPE vérifie si le terminal se situe à l'intérieur ou à l'extérieur de la zone de service configurée par défaut ou configurée par l'utilisateur. Ainsi, l'accès aux services offerts par ou via la passerelle CPE n'est autorisé suite à cette vérification qu'aux terminaux situés à l'intérieur de la zone de service. Cette mesure renforce le contrôle assuré par le procédé 1 selon l'invention.

10 Le procédé 1 peut comprendre en outre l'enregistrement 4 par la passerelle résidentielle CPE de préférences *LOCAL_PREF* d'un utilisateur de cette passerelle CPE sur son environnement. Les préférences sur l'environnement ont pour fonction de préciser des modalités de rayonnement de la passerelle résidentielle.

15 Les préférences *LOCAL_PREF* d'un utilisateur de la passerelle résidentielle sont relatives à ses préférences en ce qui concerne l'activation ou la désactivation de l'interface Wi-Fi de sa propre passerelle résidentielle. Ainsi, *LOCAL_PREF* se rapporte aux plages d'activation de l'interface Wi-Fi de sa passerelle CPE.

20 Selon un mode de réalisation, les connexions provenant d'un terminal situé en dehors d'une zone de service sont relayées par la passerelle CPE vers un serveur dédié de l'opérateur d'un réseau de communication auquel accède la passerelle comme illustré par la figure 7. Ce serveur est responsable de la détection de fraude et de la collecte d'informations qui permettent d'identifier un utilisateur malveillant (collecte d'adresses MAC, simulation d'une tentative d'accès réussie au réseau, etc.). En référence à l'exemple illustré par la figure 7, la passerelle CPE redirige les connexions reçues d'un terminal TE vers un serveur *SERV* de l'opérateur à l'aide de filtres qui sont
25 activés dans la passerelle CPE. Le trafic issu du terminal externe TE est alors envoyé vers une plateforme P dédiée de l'opérateur pour des traitements plus avancés comme, par exemple, la collecte de données utiles pour identifier l'utilisateur TE, la sauvegarde d'une trace des tentatives de connexions frauduleuses, etc. Etant donné que la redirection vers une plateforme de l'opérateur peut consommer beaucoup de ressources de la passerelle CPE, cette procédure peut être
30 activée/désactivée à la demande, pour une partie du trafic, ou selon d'autres critères spécifiques à la passerelle CPE ou instruits par l'opérateur.

Dans le cas d'un réseau d'objets connectés, (fournissant un service reposant sur l'Internet des objets ou IoT (Internet of Things)), un contrôleur de la gestion de ces objets est utilisé pour rendre un service (gestion du système d'éclairage, gestion du système de chauffage, gestion des
35 détecteurs de fumée ou de mouvement, etc.) accessible au sein de la zone de service. Ce contrôleur peut être embarqué dans la passerelle ou dans un autre équipement électronique. La passerelle embarquant une fonction actionneur (« actuator ») ou contrôleur est capable de générer des

commandes destinées à modifier la portée des objets connectés au sein d'un réseau auquel la passerelle est également connectée. En effet, la très grande majorité des objets connectés embarquent un microcontrôleur MCU (ou Micro Controller Unit) et un régulateur LDO (Low Dropout Voltage). Le microcontrôleur MCU permet en particulier de gérer la puissance d'émission des composants radio mais également l'énergie consommée. Par exemple, on peut définir un « cycle de travail » (duty cycle) qui permet d'optimiser la consommation d'énergie de l'objet moyennant la définition et la configuration des états TX (Transmit), RX (Receive), idle (stand-by) ou mise en sommeil. Le régulateur LDO peut être paramétré pour permettre d'optimiser la durée de vie des batteries (par ex lorsque les batteries sont des piles AA ou AAA) embarquées dans l'objet en jouant notamment sur la puissance du signal émis. Le déploiement de tels objets connectés fut effectué d'abord dans un contexte industriel (réseaux de capteurs sur un site de production) puis métropolitain (gestion du système d'éclairage des sites olympiques de Pékin en 2008, par exemple) et puis peu à peu domestique. La portée des ondes générées par les objets connectés est ainsi calibrée par le contrôleur selon la zone de couverture du ou des services fournis par les objets. Si le contrôleur est embarqué dans une passerelle, les zones couvertes par ces objets peuvent constituer une sous-zone de la zone de service calibrée par la passerelle. Chaque objet est donc un dispositif dont le procédé peut adapter le signal émis.

Cette sous-zone est par exemple délimitée par la localisation des capteurs selon l'aménagement du logement et la nature du service qu'ils fournissent. Toutefois, les risques sécuritaires liés au déploiement d'un réseau d'objets connectés imposent que la zone de service ne soit pas un espace isotrope : en effet, une direction au sein de l'espace correspondant à la zone de service doit toujours être privilégiée pour s'assurer que seul le contrôleur de l'utilisateur est dûment habilité à envoyer des commandes vers l'ensemble des objets connectés placés sous sa responsabilité d'exploitation.

Cette précaution permet notamment de minimiser le risque d'attaques liées à la présence d'équipements (extérieurs) susceptibles de générer des commandes vers les objets connectés lorsque ces équipements sont localisés à proximité (par exemple un drone situé à proximité de la résidence de l'utilisateur) voire sont localisés dans la zone de service délimitée par la passerelle (par exemple, à cause de la présence d'un visiteur disposant d'un smartphone embarquant la fonction de contrôleur).

Le calibrage repose sur l'envoi par le contrôleur d'un premier message *SET_DIRECTION()* destiné à informer les objets connectés de la direction privilégiée dans l'espace au sein de la zone de service (nord, nord-est, est, sud, sud-ouest, etc.) pour communiquer avec le contrôleur en vertu de la localisation de l'objet connecté. Ensuite, le calibrage de la portée des signaux émis par les objets connectés repose sur l'envoi d'un message *SET_RANGE()* par le contrôleur.

Une variante consiste à inclure dans les messages de contrôle les coordonnées géographiques du contrôleur. La transmission de ces coordonnées permet à l'objet connecté de

vérifier si le contrôleur se situe dans la zone de service ou à l'extérieur sachant que l'objet connaît la zone de service. Les primitives utilisées pour communiquer ces coordonnées sont similaires à celles déjà décrites pour le cas de la passerelle CPE. Dans le cas où le contrôleur est localisé en dehors de la zone déterminée de service, l'objet connecté peut rejeter toute requête ou commande
5 du contrôleur et éviter ainsi une utilisation frauduleuse.

La figure 9 illustre la structure simplifiée d'une passerelle CPE résidentielle mettant en œuvre un procédé de contrôle selon l'un des modes de réalisation décrits ci-dessus.

La passerelle CPE selon un mode de réalisation de l'invention comprend une mémoire MEM comprenant par exemple une mémoire tampon (RAM), des moyens d'émission et de
10 réception EM/RE d'un signal radio et une unité de traitement μ P équipée par exemple d'un microprocesseur et pilotée par un programme d'ordinateur Pg mettant en œuvre le procédé de contrôle.

A l'initialisation, les instructions de code du programme d'ordinateur Pg sont par exemple chargées dans la mémoire tampon avant d'être exécutées par le microprocesseur de l'unité de
15 traitement μ P (calculateur). Le microprocesseur de l'unité de traitement μ P met en œuvre les étapes du procédé de contrôle selon les instructions du programme d'ordinateur Pg pour exécuter par l'unité de traitement μ P la détermination d'un niveau de signal radio émis par la passerelle CPE en limite d'une zone déterminée et la commande d'adaptation *REDUCE_Cde* de la portée du signal radio émis par la passerelle en fonction de la comparaison du niveau de signal et d'un seuil
20 déterminé.

A cette fin, la passerelle est telle que les moyens d'émission EM/RE sont adaptés pour adapter le signal émis en fonction de la commande d'adaptation *REDUCE_Cde*. La passerelle peut en outre comprendre une interface IHM pour que l'utilisateur saisisse les données *Zone* descriptives de son environnement résidentiel ainsi qu'un espace mémoire d'enregistrement de ces
25 informations.

Ces moyens sont pilotés par le microprocesseur de l'unité de traitement μ P.

Les exemples cités dans la description de modes de réalisation couvrent essentiellement le cas de réduction de la portée d'un signal radio, mais le procédé peut être appliqué pour des cas d'usage qui nécessitent l'augmentation de la portée d'un signal.

REVENDICATIONS

1. Procédé (1) de contrôle d'un signal radio émis par un dispositif pour adapter sa portée, caractérisé en ce que le procédé comprend :
 - détermination (2) par un contrôleur d'un niveau de signal radio émis par le dispositif en
5 limite d'une zone déterminée,
 - commande (*REDUCE_Cde*) par le contrôleur d'une adaptation (3) de la portée du signal radio émis par le dispositif en fonction de la comparaison du niveau de signal et d'un seuil déterminé.
2. Procédé (1) de contrôle d'un signal radio émis selon la revendication 1, dans lequel la zone est
10 déterminée en recevant et utilisant des informations de localisation transmises par un terminal mobile déplacé entre des points à la limite de la zone à délimiter.
3. Procédé (1) de contrôle d'un signal radio selon l'une des revendications 1 et 2, selon lequel une passerelle résidentielle embarque le contrôleur.
4. Procédé (1) de contrôle d'un signal radio selon la revendication 3, comprenant en outre :
15 - enregistrement (4) par la passerelle de données (*zone*) descriptives d'un environnement d'un utilisateur de cette passerelle pour déterminer les limites de la zone.
5. Procédé (1) de contrôle d'un signal radio émis selon l'une des revendications 3 et 4, comprenant en outre :
20 - envoi d'une requête demandant sa localisation à tout terminal cherchant à s'associer à la passerelle,
- autorisation de l'association du terminal à la passerelle uniquement s'il est localisé dans la zone.
6. Procédé (1) de contrôle d'un signal radio émis selon l'une des revendications 3 et 4, comprenant en outre :
25 - réception d'une requête d'association provenant d'un terminal comprenant la localisation de ce terminal,
- autorisation de l'association du terminal à la passerelle uniquement s'il est localisé dans la zone.
7. Procédé (1) de contrôle d'un signal radio selon l'une des revendications 3 à 6, comprenant en
30 outre :
- enregistrement (4) par la passerelle résidentielle de préférences (*LOCAL_PREF*) d'un utilisateur sur son environnement.
8. Procédé (1) de contrôle d'un signal radio émis selon l'une des revendications 3 à 7, selon
35 lequel la passerelle relaye une demande de connexion d'un terminal localisé en dehors de la zone vers un serveur d'un réseau auquel accède la passerelle pour que le serveur évalue s'il y a fraude et, en cas de demande frauduleuse, le procédé comprend une redirection du trafic du terminal vers une plateforme de service dédiée.

9. Procédé (1) de contrôle d'un signal radio selon l'une des revendications 1 à 8, selon lequel le dispositif étant un objet connecté, le procédé comprend en outre :
- fourniture par le contrôleur à l'objet d'informations sur sa localisation,
 - rejet par l'objet de toute requête ou commande venant du contrôleur si ce dernier est localisé en dehors de la zone déterminée.
10. Procédé (1) de contrôle d'un signal radio selon l'une des revendications 1 et 2, selon lequel le dispositif embarque le contrôleur.
11. Procédé (1) de contrôle d'un signal radio émis selon l'une des revendications 1 à 10 selon lequel la comparaison à un seuil est répétée.
- 10 12. Passerelle (CPE) destinée à être connectée à un réseau (AN) de communication comprenant :
- des moyens d'émission et de réception (EM/RE) d'un signal radio, caractérisée en ce qu'elle comprend en outre :
 - une mémoire (MEM) pour mémoriser des données descriptives de l'environnement résidentiel d'un utilisateur de la passerelle définissant une zone,
 - un calculateur (μ P) pour déterminer le niveau de signal à la limite de la zone et pour comparer ce niveau à un seuil et
- 15 en ce que le calculateur est programmé pour commander (*REDUCE_Cde*) l'adaptation de la portée du signal radio émis par la passerelle si le seuil est dépassé.
13. Système de communication comprenant une passerelle résidentielle (CPE) pour le contrôle d'un signal radio émis par la passerelle caractérisé en ce que la passerelle est selon la revendication 9.
- 20 14. Programme d'ordinateur comportant des instructions pour la mise en œuvre d'un procédé selon l'une quelconque des revendications 1 à 11 lorsque ce programme est exécuté par un processeur.

1/2

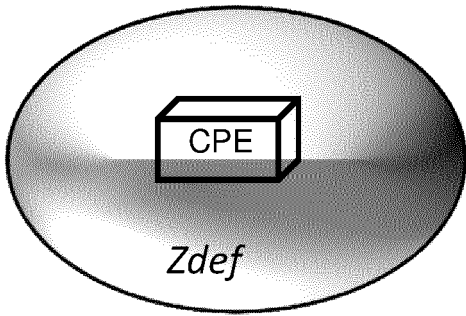


Fig.1

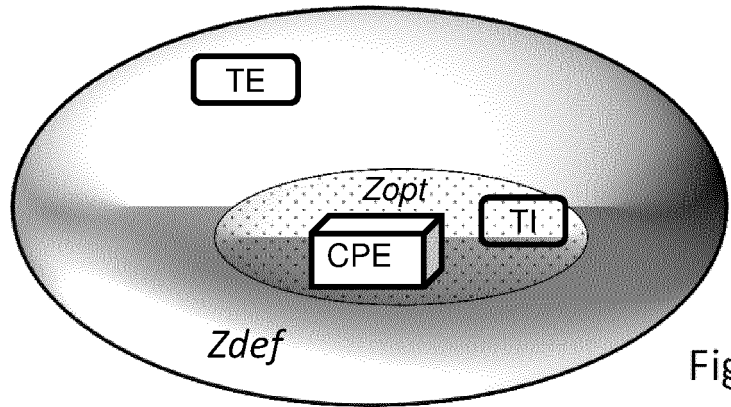


Fig.4

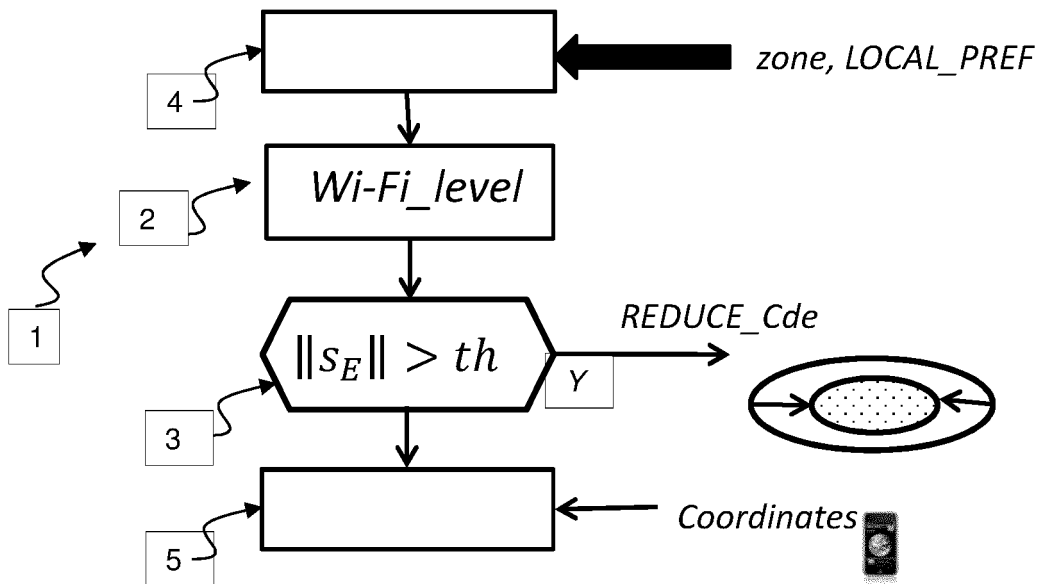


Fig.2

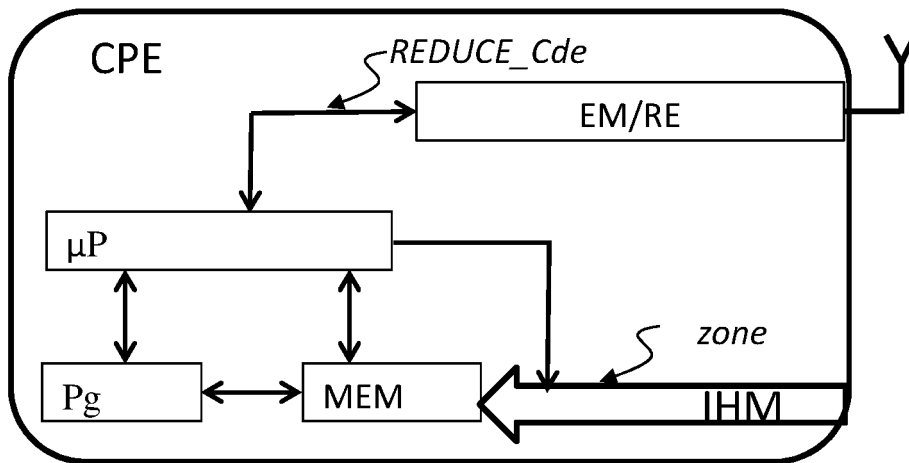


Fig.8

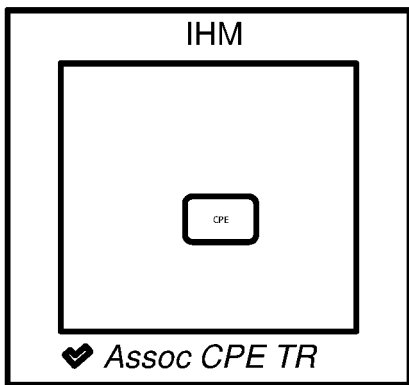


Fig.3a

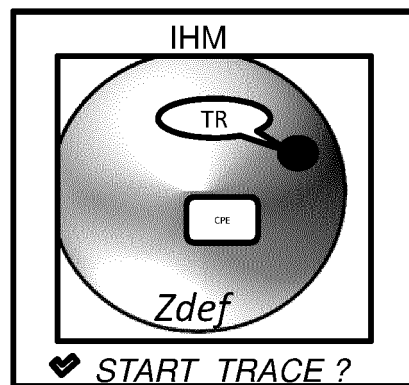


Fig.3b

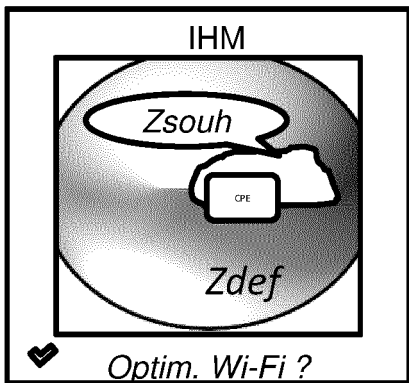


Fig.3c

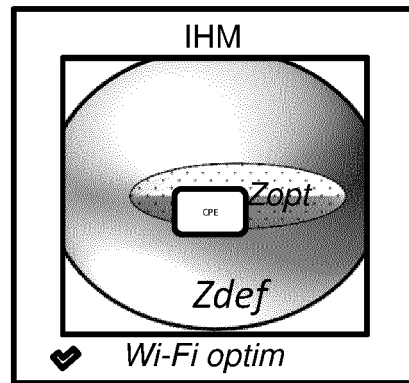


Fig.3d

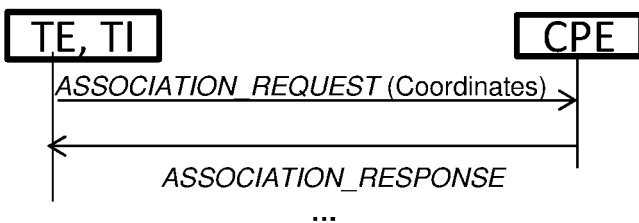


Fig.5

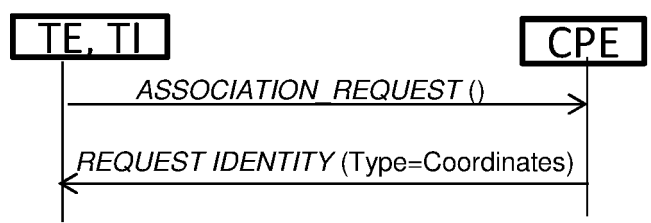


Fig.6

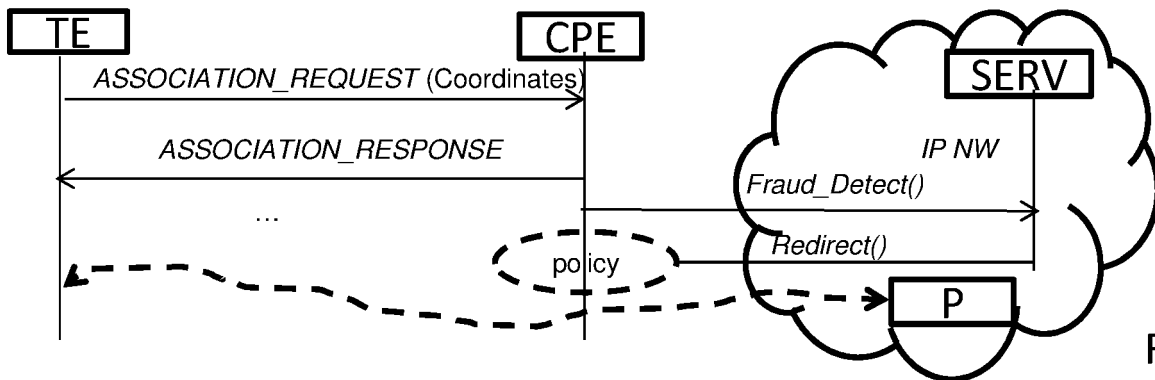


Fig.7



**RAPPORT DE RECHERCHE
PRÉLIMINAIRE**

N° d'enregistrement national

établi sur la base des dernières revendications déposées avant le commencement de la recherche

FA 834347
FR 1662475

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 2009/286496 A1 (YAVUZ MEHMET [US] ET AL) 19 novembre 2009 (2009-11-19)	1,12-14	H04W52/28
Y	* abrégé * * alinéas [0052] - [0054], [0078], [0115], [0123], [0125] - [0126] *	2-11	H04W4/02 H04W84/12 H04W80/08
X	US 2015/271764 A1 (AGRAWAL MEGHNA [US] ET AL) 24 septembre 2015 (2015-09-24)	1-7, 10-14	
Y	* abrégé * * alinéas [0002], [0004], [0043], [0045], [0048], [0054] - [0056], [0062], [0066] - [0067], [0071] * * figures 5-13 *	8,9	
Y	WO 2011/124810 A1 (FRANCE TELECOM [FR]; SONG SONGBO [FR]; MOUSTAFA HASSNAA [FR]) 13 octobre 2011 (2011-10-13) * abrégé * * page 2, lignes 23-31 * * page 10, lignes 30-37 * * page 12, lignes 11-14 * * page 14, lignes 25-30 * * revendications 1-15 *	2-11	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04W
Date d'achèvement de la recherche		Examineur	
16 août 2017		Yang, Betty	
CATÉGORIE DES DOCUMENTS CITÉS		T : théorie ou principe à la base de l'invention	
X : particulièrement pertinent à lui seul		E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.	
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie		D : cité dans la demande	
A : arrière-plan technologique		L : cité pour d'autres raisons	
O : divulgation non-écrite		
P : document intercalaire		& : membre de la même famille, document correspondant	

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1662475 FA 834347**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **16-08-2017**

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2009286496 A1	19-11-2009	AU 2009246492 A1	19-11-2009
		BR PI0912734 A2	13-10-2015
		CA 2722170 A1	19-11-2009
		CA 2928923 A1	19-11-2009
		CN 102027786 A	20-04-2011
		CN 104540206 A	22-04-2015
		EP 2311193 A2	20-04-2011
		JP 5350468 B2	27-11-2013
		JP 5752757 B2	22-07-2015
		JP 2011521563 A	21-07-2011
		JP 2014003680 A	09-01-2014
		KR 20110020250 A	02-03-2011
		RU 2010150744 A	27-06-2012
		TW 200952368 A	16-12-2009
		US 2009286496 A1	19-11-2009
		US 2014235288 A1	21-08-2014
		WO 2009140312 A2	19-11-2009
		US 2015271764 A1	24-09-2015
EP 3120624 A1	25-01-2017		
JP 2017516078 A	15-06-2017		
KR 20160136306 A	29-11-2016		
US 2015271764 A1	24-09-2015		
WO 2015142502 A1	24-09-2015		
WO 2011124810 A1	13-10-2011	AUCUN	