

PROCEDE DE LOCALISATION DE DONNEES, SYSTEME DE CONTROLE, DISPOSITIF EMETTEUR

5 DOMAINE

Le domaine de l'invention concerne celui des procédés et des équipements permettant la localisation de données émises par un équipement aux fins de garantir leur intégrité. Le domaine de l'invention concerne les équipements émetteurs comportant une interface UWB pour émettre au moins
10 une donnée dont on souhaite garantir la provenance notamment par le contrôle de la position depuis laquelle elle est émise.

ETAT DE L'ART

Il existe des solutions permettant de sécuriser l'identité d'une
15 personne ou de contrôler l'intégrité d'une donnée émise par cette personne lors d'une transaction. La notion de transaction s'entend au sens large, lorsqu'un tiers est notamment sollicité dans une opération visant à obtenir des accès, des droits ou un contrôle des données échangées entre différentes entités comportant un module de communication électronique.

20 Il peut s'agir, par exemple, d'une délivrance d'accès à une salle au niveau d'une porte dont un utilisateur aurait préalablement émis une requête pour obtenir cet accès au moyen d'un dispositif de communication électronique.

Selon un autre exemple, le cas visé peut correspondre à celui d'une
25 vérification d'une alerte incendie émise par un détecteur de fumée dont on souhaite vérifier une mesure de capteur et sa position afin de valider ou non une intervention.

Enfin, selon un autre exemple, lors d'une transaction dans un lieu
30 donné, la certitude que la transaction est réellement effectuée depuis ce lieu peut suffire à autoriser la transaction à un utilisateur présent dans ce lieu.

Actuellement, ces situations sont solutionnées afin d'utiliser la position d'un utilisateur pour fiabiliser une transaction.

Dans ce sens, le document de brevet **US8869305** décrit une
35 solution dans laquelle une position est déterminée à partir d'un réseau sans fil de type Wifi ou par une liaison Bluetooth. La position peut être exploitée de manière absolue ou de manière relative. De manière absolue, la présente

solution vise à vérifier la connectivité locale avec un équipement, par exemple pour vérifier qu'il est bien localisé au sein d'un réseau wifi ou au moyen d'un contrôle de la position obtenue par un système GPS. De manière relative, c'est notamment le cas lorsqu'on souhaite vérifier qu'un utilisateur se situe, par
5 exemple, près de son casque audio ou son ordinateur. Une déduction peut être qu'un utilisateur se situe ou non dans son lieu de travail.

En ce qui concerne la localisation d'un appareil par sa connectivité sur un lieu, tel que décrit également dans le document de brevet **US200080096529**, un problème est que cette solution n'est pas précise et
10 qu'elle comporte un risque dans la fiabilité du contrôle de l'intégrité d'une donnée. En effet, la seule connectivité permet de remonter l'information qu'un utilisateur se situe dans une zone donnée, mais elle ne permet pas de connaître précisément sa localisation. De ce fait, une usurpation de l'identité lorsque la localisation est utilisée comme mot de passe peut être très
15 dangereuse. Cela présente un danger dans le contrôle de l'intégrité des données émises lorsque seule la position de l'équipement est utilisée pour valider une transaction.

Enfin, en ce qui concerne la localisation GPS, telle que décrit dans le document de brevet **US20060107008**, cette dernière n'est également pas
20 suffisamment précise pour permettre une large utilisation d'un contrôle d'intégrité d'une donnée par la position d'un équipement d'un utilisateur. De surcroît, la position GPS peut être difficilement obtenue dans un contexte d'un lieu cloisonné, fermé ou immergé au sein duquel l'équipement peut ne pas être détecté.

Par ailleurs, les solutions mobiles utilisant la localisation satellite de
25 type GPS traitent généralement les données relatives à la position acquise dans différents algorithmes. En conséquence, ces données peuvent être détectées, captées et/ou corrompues par un tiers. Ce fonctionnement autorise, par exemple, la possibilité de générer une fausse localisation afin d'usurper
30 une identité.

Il existe donc un besoin pour fournir une solution au problème suivant : localiser une donnée à produire afin d'assurer son intégrité, c'est-à-dire reconnaître la source de sa provenance en tant qu'équipement ou
utilisateur. Cette fonction de localisation d'une donnée devrait être
35 préférentiellement réalisée de manière fiable, c'est-à-dire sans permettre une

possible falsification de la localisation par un tiers. En outre, les solutions devraient permettre aussi un fonctionnement dans un environnement cloisonné ou fermé ne limitant pas la production d'une position précise de l'équipement.

5

RESUME DE L'INVENTION

Selon un premier aspect l'invention concerne un procédé de contrôle de l'intégrité d'au moins une donnée utile, ledit procédé comprenant :

- 10 ▪ Acquisition d'au moins un message dans la bande radio UWB provenant d'un émetteur au moyen d'une interface sans fil et d'un démodulateur UWB ;
- Décodage d'au moins une donnée utile, dite première information ;
- 15 ▪ Détermination d'une information de position, dite seconde information, de l'émetteur UWB à partir de plusieurs réceptions de messages émis par ledit émetteur ;
- Génération d'un couple de données comportant d'une part la première information et d'autre part la seconde information.

20 Un avantage de l'invention est de tirer un bénéfice de la localisation de l'émission d'un message UWB pour certifier l'intégrité d'une information donnée. Un avantage de la bande radio UWB est de permettre une localisation très précise de la source d'émission générant des messages UWB. Ainsi, il devient possible d'augmenter la sécurité du contrôle des messages dans des transactions diverses en corroborant la position de l'émission des données
25 avec une position attendue.

 Selon un mode de réalisation, l'acquisition comprend une réception d'une séquence d'impulsions radio, définissant des messages UWB, par une pluralité de balises, chaque balise étant localisée à une position prédéfinie.

30 Un avantage est de couvrir une zone donnée dans laquelle des transactions sont susceptibles d'intervenir. Un intérêt est de générer une information de localisation infalsifiable. Cette dernière peut par exemple comprendre un vecteur position dont les composantes sont des mesures de temps d'arrivée d'un signal ou des temps de vol. Ces données sont quasiment infalsifiables étant donné que la régénération d'un tel vecteur nécessiterait une
35 connaissance des données de réceptions dans chaque récepteur. En

particulier, il serait nécessaire d'usurper le signal au niveau de chaque récepteur en conservant une synchronisation entre les usurpations meilleure qu'une durée de l'ordre de la nanoseconde tout en empêchant le signal d'origine d'arriver à ces mêmes récepteurs.

5 De plus, selon un mode de réalisation, l'invention permet de générer un code, par exemple, tournant dans la date à chaque émission. Dans ces conditions, il devient impossible de deviner le message à l'avance et donc de réaliser une attaque par rejeu d'un message déjà reçu, plus connue sous le nom de « replay attack » ou « playback attack » dans la terminologie
10 anglosaxonne.

Le tiers souhaitant usurper un message daté devrait alors conduire une attaque simultanément au niveau de chaque récepteur en étant sur les lieux. Il devrait alors connaître l'architecture radio et l'agencement des balises de réception.

15 Selon un mode de réalisation, l'information de position de l'émetteur est déterminée par une méthode d'estimation :

- des temps d'arrivée des messages UWB afin d'en déduire des différences de temps de vol de ces derniers et/ou ;
 - des puissances d'arrivée des messages UWB et/ou ;
 - 20 ▪ des fréquences d'arrivée des messages UWB,
- au niveau desdites balises de réception.

Un avantage est d'obtenir une précision accrue de la position de l'émetteur par exemple en combinant différentes techniques de localisation.

25 Selon un mode de réalisation, lorsque les différences de temps d'arrivée des messages sont estimées, la localisation de l'émetteur étant déduite d'un calcul de trilatération entre les temps d'arrivée des différents messages UWB.

Un avantage est d'obtenir une position précise et fiable avec un temps de traitement court.

30 Selon un mode de réalisation, au moins un message UWB reçu comporte un identifiant de l'émetteur. Un avantage est de sécuriser le contrôle d'intégrité en vérifiant l'identification du dispositif émetteur et sa localisation.

35 Dans le cas d'un détecteur de fumée, l'identifiant peut être transmis en clair au niveau radio UWB, c'est-à-dire sans chiffrement. Dans d'autres cas, l'identification peut être déduite du lieu de réception des messages UWB émis.

Dans ce dernier cas, la transmission de l'identification du détecteur de fumée peut être optionnelle puisque par construction les messages UWB reçus déterminent le détecteur qui émet les trames. Généralement, les identifiants des détecteurs de fumée sont connus et leur position dans l'espace peut être
5 référencée et enregistrée dans une mémoire distante. Lorsque la position calculée par les balises de réception est fautive et ne correspond pas à la position théorique attendue, alors le message reconstruit comportant la position à partir des messages UWB est un faux message.

Selon un mode de réalisation, l'information de position calculée et
10 la donnée utile, et optionnellement l'identifiant de l'émetteur, sont associés par la génération d'une clef unique. Un avantage est de transférer des données sécurisées vers un serveur de contrôle ayant les capacités de contrôler l'intégrité de la donnée utile. Cette solution évite par exemple de communiquer la position en clair d'un utilisateur accédant à un service donné. Ainsi un
15 premier calcul est effectué au niveau du calculateur effectuant le calcul de position afin de générer une donnée intermédiaire ne restituant pas l'intégralité de la valeur de la position.

La génération d'un couple de données comportant la première information de données utiles et la seconde information de position peut être
20 interprétée comme une association de données. Cette association peut être réalisée, par exemple, par une opération combinant la première et la seconde information pour générer une tierce valeur ou bien un enregistrement des deux informations liées par une clef unique.

Selon un mode de réalisation, l'association entre l'information de
25 position calculée et la donnée utile comprend la génération d'un code résultant d'une opération :

- de codage des données par un algorithme d'encodage ;
- d'entrelacement, une permutation de données ou une opération permettant de générer un champ de données comportant les bits
30 de données de l'information de position et les bits de données issues des données utiles, et/ou ;
- de chiffrement des données entre elles au moyen d'une clef de chiffrement.

Un avantage est de ne pas communiquer en clair la position de l'utilisateur.

Selon un mode de réalisation, le procédé comprend l'émission d'un message de synthèse vers un serveur distant, le message de synthèse comportant :

- 5 ▪ la donnée utile et l'information de position calculée, ces informations pouvant être codées dans différents champs du message de synthèse et/ou ;
- la donnée utile et l'information de position calculée, ladite position calculée étant cryptée dans le message de synthèse et/ou ;
- 10 ▪ une clef unique permettant de déchiffrer l'information de position chiffrée dans un champ du message de synthèse et/ou ;
- un identifiant de l'émetteur UWB ayant émis le message et/ou ;
- un identifiant d'un équipement sur lequel une étiquette est agencée, ledit équipement et l'étiquette formant un dispositif
- 15 émetteur.

Un avantage est de communiquer à serveur distant des données permettant de vérifier l'intégrité de données utiles.

Selon un autre aspect, l'invention concerne un système de contrôle comportant :

- 20 ▪ Au moins une balise de réception comportant :
 - Une première interface sans fil configurée pour recevoir des signaux dans la bande UWB ;
 - Un module radio permettant de traiter les signaux reçus de manière à horodater la réception d'une pluralité de messages
 - 25 reçus et de démoduler en bande de base au moins une donnée utile ;
- Un calculateur pour déterminer une position de l'espace à partir de l'analyse d'une pluralité de propriétés issues des réceptions de messages provenant d'au moins un émetteur, lesdites propriétés
- 30 issues des réceptions étant corrélées de manière à déterminer une information de position d'un émetteur ;
- Une mémoire pour enregistrer au moins une valeur associant d'une part une information de position de l'espace calculée et d'autre part au moins une donnée utile.

Un avantage est de disposer d'un système complet permettant de sécuriser des transactions dans un lieu donné. Ainsi un lieu peut être équipé de balises visant à couvrir une zone donnée. L'information de position générée par une pluralité de balises est difficile à falsifier compte tenu que les données
5 utilisées pour retrouver la localisation dépendent de propriétés du signal radio et de la position des balises.

Selon un mode de réalisation, dans le système de l'invention :

- chaque balise comporte un composant pour horodater les messages UWB reçus ;
- 10 ▪ le calculateur détermine des écarts de temps de vol issus d'une pluralité de réception de messages provenant d'au moins un émetteur afin de déterminer l'information de position de l'émetteur.

Un avantage est d'obtenir un système fournissant une position
15 précise. Plus la position déterminée est précise, plus le système de l'invention permet d'offrir un service de contrôle de l'intégrité accru des données utiles.

Selon un mode de réalisation, le système de contrôle comprend en outre un second serveur distant, ledit serveur distant comportant une interface pour recevoir un message de synthèse généré par le calculateur et comportant
20 des moyens de calculs pour :

- décoder et contrôler l'information de position et ;
- générer un message visant à permettre ou interdire l'accès à un service vers un équipement donné,

le second serveur comportant, en outre, une interface pour émettre ledit
25 message vers l'équipement donné.

Un avantage est de sécuriser n'importe quel type de transaction dès lors qu'une donnée utile de la transaction peut être associée à une position pendant la transaction.

Selon un autre aspect, l'invention concerne un dispositif émetteur
30 comportant :

- Un équipement susceptible de générer au moins une donnée utile dans un contexte prédéfini et de transférer ladite donnée utile au moyen d'une première interface ;
- Une étiquette radio comportant une seconde interface pour recevoir
35 ladite au moins une donnée utile, ladite étiquette radio comportant

un modulateur UWB dans la bande UWB pour émettre un signal comportant ladite au moins une donnée utile.

Un avantage est de transformer un équipement existant en un équipement pouvant assurer l'intégrité de données émises lors de transactions avec des équipements tiers.

Selon un mode de réalisation, le dispositif émetteur comporte, en outre :

- Un module de réception radio pour recevoir un flux d'ondes radio ;
- Un redresseur pour convertir la puissance spectrale reçue par le module de réception radio en une tension ou un courant électrique ;
- Un accumulateur électrique ;
- Un module de gestion des capacités d'énergie pour déclencher l'émission d'un message dans la bande UWB à partir du modulateur UWB.

Un intérêt est de fournir un dispositif autonome en énergie qui soit alimenté par une source d'énergie radio installée dans un lieu couvrant les dispositifs émetteurs susceptibles d'y circuler.

BRÈVE DESCRIPTION DES FIGURES

D'autres caractéristiques et avantages de l'invention ressortiront à la lecture de la description détaillée qui suit, en référence aux figures annexées, qui illustrent :

- figure 1 : différentes étapes du procédé de l'invention mises en œuvre selon un mode de réalisation du procédé de l'invention ;
- figure 2 : un équipement émetteur selon un mode de réalisation de l'invention ;
- figure 3 : un exemple de trame de données comportant une association entre une localisation d'un équipement et une donnée émise par cet équipement ;
- figure 4 : une vue en perspective d'un lieu dans lequel sont agencées des stations réceptrices pour recevoir des messages provenant de dispositifs émetteurs selon différents modes de réalisation de l'invention ;
- figure 5 : une vue en perspective d'un lieu dans lequel est agencée une station réceptrice pour recevoir des messages provenant d'un

dispositif émetteur en mouvement selon un mode de réalisation de l'invention.

DESCRIPTION

5 On appelle dans la suite de la description une étiquette radio comportant un modulateur UWB, une étiquette radio émettant des signaux dans la bande UWB. L'étiquette 20 peut également être appelée « étiquette radio UWB » ou « étiquette UWB ». Elle est désignée par l'indice 20 dans les figures. Dans son interprétation la plus large, on appelle une étiquette radio
10 UWB une support électronique comportant à minima un modulateur et une antenne UWB. Cette dernière peut être intégrée électroniquement à d'autres étages électroniques d'un équipement EQ₁.

Dans la suite de la description, l'étiquette radio émet des messages M₁ sous la forme de séquences d'impulsions radio à bande ultra-large, dits
15 « messages UWB ». De tels messages UWB, formés par une séquence d'impulsions radio, sont également désignés par « Ultra Wide Band-Impulse Radio » ou UWB-IR dans la littérature anglo-saxonne.

Dans la suite de la description, le dispositif émetteur 1 de l'invention comprenant une étiquette UWB 20 peut être assimilé à l'étiquette 20 pour la
20 description des fonctions d'émission. Ainsi, pour la commodité du lecteur on évoquera l'émission de message M₁ d'une étiquette radio UWB 20 pour désigner également l'émission de message M₁ par un dispositif émetteur 1 comportant les briques fonctionnelles et les composants permettant de réaliser des émissions de messages M₁ dans la bande UWB. La notion d'« étiquette »
25 est donc toute relative dans la mesure où le dispositif émetteur 1 de l'invention réalise les fonctions d'émission en intégrant les caractéristiques nécessaires d'une étiquette radio UWB pour réaliser ces émissions. A cette fin, la figure 2 représente un dispositif émetteur 1 selon un mode de réalisation comportant une étiquette 20 ménagée de sorte qu'elle est physiquement liée à
30 l'équipement EQ₁, ledit équipement EQ₁ générant des données DATA₁ dont l'intégrité doit être sécurisée à partir du procédé de l'invention.

Dans la suite de la description, le procédé de l'invention vise à sécuriser l'intégrité d'au moins une donnée DATA₁ émise par un dispositif émetteur 1 ou plus spécifiquement par un équipement EQ₁ associé à une
35 étiquette radio UWB. La donnée est appelée donnée décodée ou donnée utile.

Elle peut comprendre une information minimale correspondant à un bit de donnée « 0 » ou « 1 » et n'est pas limitée en taille d'octets. Selon un mode de réalisation, les données utiles DATA₁ comprennent une pluralité d'octets.

5 La figure 1 représente un mode de réalisation du procédé de l'invention. Cette illustration représente les échanges entre différentes entités, à savoir un équipement EQ₁, une étiquette 20, des balises de réception 30, un serveur SERV₁ ou un équipement centralisant les différents messages M₁ afin de générer une information de localisation et un second serveur SERV₂, ainsi
10 que les différents messages émis entre elles. Selon un mode de réalisation l'équipement EQ₁ et l'étiquette UWB ne forme qu'un seul et même équipement comportant un modulateur et une antenne UWB.

 Un équipement EQ₁ comprend un ordinateur pour générer des données utiles DATA₁. Ces données peuvent être issues d'une mémoire et
15 peuvent correspondre, par exemple, à un identifiant stocké, une clé publique ou une valeur d'un paramètre. Ces données utiles DATA₁ peuvent également être issues d'un capteur collectant des données. Dans ce dernier cas, les données DATA₁ peuvent être des données brutes, des données filtrées ou traitées ou encore un résultat calculé issus des données collectées avec
20 d'autres paramètres. Enfin, ces données peuvent résulter d'opérations sur des données provenant d'une base de données, d'un serveur et acquises par une liaison filaire ou sans fil de l'équipement EQ₁.

 Selon un exemple de réalisation, le procédé comprend une étape de génération GEN_DATA₁ des données DATA₁ par exemple au moyen d'un
25 ordinateur. Les données générées sont émises vers l'étiquette UWB 20. A cette fin, une étape TRANS_MDATA₁ permet de communiquer les données DATA₁ à l'étiquette 20. Ces données DATA₁ peuvent être émises via une interface physique ou une interface sans fil selon les différents modes de réalisation du dispositif émetteur 1.

30 L'étiquette UWB 20 reçoit alors les données DATA₁. Le procédé comprend donc une étape de réception (non représentée) des données provenant de l'équipement EQ₁. Selon un mode de réalisation, les données qui seront modulées dans un message M₁ comprennent des données reçues DATA₁ de l'équipement EQ₁ et des données provenant de l'étiquette 20 telles
35 que les données TAG₁ qui codent ici un identifiant de l'étiquette 20 ou du

dispositif émetteur 1 lorsque l'étiquette 20 est électroniquement ou physiquement intégrée dans l'équipement EQ₁.

Lorsque les données DATA₁ à émettre par un équipement EQ₁ sont trop volumineuses pour être codées dans un seul message M₁ émis par l'étiquette 20, le procédé comprend une étape visant à segmenter les données DATA₁ en une pluralité de paquets DATA₁₁, DATA₁₂, ... DATA_{1k}, DATA_{1N}, k∈[1;N]. Un module de codage des données peut être configuré de manière à optimiser le codage des données DATA₁ au sein d'une pluralité de messages M₁. Des fonctions de redondance, d'entrelacement, ou de cryptage des données peuvent être mises en œuvre de sorte à générer des messages M₁ répondant à une configuration prédéfinie.

Le procédé de l'invention comprend, en outre, une étape de génération GEN_M₁ d'un message M₁ afin de coder et moduler les données DATA₁ et possiblement les données TAG₁ dans au moins un message UWB M₁. Le ou les message(s) M₁ sont alors ensuite transmis vers au moins une balise de réception 30, cette étape est notée TRANS_M₁. Le message M₁ est émis grâce à une antenne de l'étiquette 20.

Selon un mode de réalisation, les messages UWB émis par une même étiquette 20 peuvent être tous de tailles identiques. Certains champs sont prédéfinis, par exemple, le champ comportant l'identifiant de l'étiquette 20 : TAG₁ ou du dispositif émetteur 1. Les bits d'information inclus dans ce champ peuvent donc être identiques. Le champ correspondant aux données DATA₁ peut être fixe ou variable selon les modes de réalisation envisagés.

Selon un mode de réalisation, le procédé de l'invention comprend une étape de réception d'une pluralité de messages M₁ comportant au moins une donnée utile DATA₁.

Selon un premier mode de réalisation, la pluralité de réceptions est effectuée de manière séquentielle par une unique balise 30. Dans ce mode, des messages M₁ sont émis de manière séquentielle par l'étiquette 20. La figure 5 illustre un mode d'application de cette réalisation. La position de la balise 30 est connue dans l'espace et permet de déterminer un trajet de l'étiquette 20 par l'analyse d'une succession de réceptions de messages M₁ émis depuis différentes positions.

Selon un second mode de réalisation, la pluralité de réceptions de message M₁ est réalisée par un ensemble de balises 30_A, 30_B, 30_C réparties

sur une zone géographique donnée. Ce mode est illustré à la figure 3 par les trois blocs comportant un module de réception comportant une antenne pour recevoir des messages dans la bande UWB. Les positions de chaque balise 30 sont connues et permettent de définir, par exemple, un référentiel de base
5 afin de localiser une étiquette 20.

Le procédé comprend donc une étape de réception REC des messages UWB par les balises 30. Le procédé comprend une étape de démodulation des messages M_1 et une étape visant à horodater HORO l'arrivée des messages. Selon un exemple de réalisation, la qualité des
10 réceptions est estimée afin de réduire les fausses détections ou d'appliquer un filtrage particulier afin de réduire les erreurs lors de la démodulation des signaux. Chaque balise 30 réalise ces trois étapes de réception, de démodulation et d'horodatage des messages reçus M_1 . En outre, chaque balise 30 émet, à l'étape TRANS M_{2i} , $i \in \{A, B, C\}$, un message M_{2A} , M_{2B} , M_{2C} à un
15 calculateur $SERV_1$ centralisant les données émises notamment pour déterminer la position de l'étiquette. Selon un exemple, le calculateur $SERV_1$ est un serveur. Selon un mode de réalisation, les messages M_{2A} , M_{2B} , M_{2C} émis par chaque balise 30 comprennent donc des données $DATA_1$ de l'équipement EQ_1 , des données TAG_1 de l'étiquette 20 et des données
20 enrichies $HORO_1$ des balises 30 notamment comportant des temps d'arrivée de chaque message M_1 reçu.

Selon un mode de réalisation, le procédé de l'invention comprend ensuite une étape de réception REC des messages M_{2i} , $i \in \{A, B, C\}$ émis par chaque balise 30. Selon un mode particulier, le calculateur $SERV_1$ peut être
25 agencé dans l'une des balises 30.

Le procédé comprend une étape de traitement Δ_{Tvol} des différentes dates de réception des messages M_1 reçus par les différentes balises 30.

Selon un exemple de réalisation lorsqu'un même message UWB M_1 est reçu par plusieurs balises de réception 30, la position de l'étiquette UWB
30 20 peut être estimée en comparant les instants d'arrivée respectifs du message UWB sur chacune des balises 30 réceptrices. Notamment, la position de l'étiquette 20 peut être estimée, de manière connue, en calculant pour plusieurs paires de balises 30 des différences entre les instants d'arrivée (TDOA) du message UWB sur les balises 30 réceptrices de chaque paire.

Cette étape de calcul peut être réalisée à partir d'un horodatage de chaque message reçu M_1 par chaque balise de réception 30.

5 Dans cette étape, selon un exemple de réalisation, la qualité du signal reçu peut être prise en compte pour estimer si une donnée est prise ou non en compte dans un calcul.

Selon un mode de réalisation, les temps de vol des messages M_1 permettent de déterminer la localisation de l'étiquette 20, par exemple, au moyen d'un algorithme de trilatération estimant les différences de temps d'arrivée des messages. Un tel algorithme peut être connu de l'homme de l'art.

10 Selon d'autres modes de réalisation, l'estimation de la position d'une étiquette 20 est réalisée à partir d'une méthode d'estimation de position pouvant utiliser notamment, alternativement ou en complément, les puissances d'arrivée et/ou les fréquences d'arrivée des messages UWB au niveau desdites balises de réception 30. Toutefois, un intérêt de l'utilisation
15 des messages UWB est qu'ils permettent d'avoir des mesures d'instant d'arrivée très précises, ce qui permet également d'estimer la localisation de l'étiquette de manière très précise.

A cet effet, le procédé comprend une étape de détermination de la
20 localisation POS_1 ou plus généralement d'une information de localisation POS_1 . Cette information de localisation peut comprendre :

- une position reconstruite comportant des coordonnées de type GPS ;
- une localisation relative dans un repère de l'espace défini vis-à-
25 vis des positions de chaque balise ;
- un vecteur dont chaque composante correspond à une mesure de temps de vol entre l'étiquette et une balise donnée ou une mesure de date d'arrivée à chaque balise,
- etc.

30 Selon un mode de réalisation, le procédé de l'invention comprend une étape d'association de l'information de localisation POS_1 et des données $DATA_1$ et optionnellement des données de l'étiquette TAG_1 .

Afin de réaliser une association des données permettant de rendre
35 infalsifiable l'intégrité des données $DATA_1$, ces dernières peuvent être

associées de diverses manières de sorte qu'un tiers ne puisse reproduire cette association.

L'association des données de position et des données DATA₁ peut comprendre une étape de codage, d'entrelacement et/ou de cryptage des données entre elles.

Dans un autre mode de réalisation, l'information de position POS₁ peut définir une clef unique visant à restituer une valeur qualifiant si la position ou non est vérifiée. Ainsi, l'information de position n'est pas nécessairement transmise dès lors qu'une clef d'association permet de certifier que la position est validée.

Selon un mode de réalisation, l'information de position POS₁ permet de définir une clef de cryptage ou un mot de passe à transmettre à une application tierce. Selon un autre mode de réalisation, les différentes composantes d'un vecteur position peuvent être combinées afin de coder les données DATA₁.

La figure 2 représente un mode de réalisation d'un équipement EQ₁ associé avec une étiquette UWB 20. Cette association peut prendre différentes formes selon les cas d'applications de l'invention. On nomme le dispositif comportant l'équipement EQ₁ et l'étiquette 20 un dispositif émetteur 1. Selon un mode de réalisation, l'équipement EQ₁ intègre l'étiquette 20 au sens où une interface électronique et physique permet de faire échanger des données entre les deux entités. Un même bâti peut être utilisé pour les deux entités EQ₁ et 20.

Selon un autre exemple, les deux entités EQ₁, 20 peuvent être physiquement disjointes. Dans ce cas de figure l'étiquette UWB 20 communique avec l'équipement EQ₁ par le biais d'une interface sans fil.

Selon un mode de réalisation, l'équipement EQ₁ comporte une mémoire M, un calculateur K et un capteur C permettant de collecter une donnée DATA₁. Dans l'exemple de la figure 2, l'équipement EQ₁ comporte une interface physique 10 compatible d'une interface 26 d'une étiquette UWB. L'étiquette UWB 20 comporte un modulateur 25 et une antenne 21 pour émettre un signal dans la bande UWB. Les données DATA₁ sont acquises depuis l'interface 26 et modulées par le modulateur 25. Selon un mode de réalisation, une mémoire et un calculateur peuvent être intégrés dans

l'étiquette 20 pour traiter, stocker, mettre en forme les données provenant de l'interface 26. -

5 Selon un exemple de réalisation, l'étiquette UWB comporte une alimentation afin de fournir une tension aux différents composants. Selon un autre mode de réalisation, l'alimentation provient de l'équipement EQ₁. Elle peut être acheminée par un connecteur de l'interface 26.

10 Selon un mode de réalisation, l'étiquette 20 comporte un module de contrôle (non représenté) configuré pour piloter les émissions des messages UWB M₁. Selon un mode de réalisation, la période d'émission, la puissance d'émission, le codage des données, la modulation UWB, etc. sont configurés dans le module de contrôle pour réaliser les émissions de messages UWB M₁. Selon un mode de réalisation, les différentes fonctions énumérées peuvent être supportées par différents composants ou être mises en œuvre par le même composant.

15 Selon un exemple de réalisation, l'étiquette 20 comporte un module de réception radio 23 pour recevoir un flux d'ondes radio. Dans ce mode de réalisation, une balise émettrice (non représentée) d'un flux radio permet à l'étiquette 20 de collecter une énergie radio fréquence.

20 Selon un mode de réalisation, une balise émettrice d'un flux radio peut être une ou plusieurs stations d'alimentation électrique (non représentées) sans fil réparties sur la zone géographique couverte par les balises 30. Ans ce mode de réalisation, les stations d'alimentation électrique sans fil alimentent à distance les étiquettes 20 en énergie électrique.

25 Les balises émettrices, également dénommées « stations d'alimentation électrique sans fil », sont distinctes des balises 30 réceptrices. Rien n'exclut cependant, suivant d'autres exemples, d'avoir une ou plusieurs desdites stations d'alimentation électrique sans fil qui soient intégrées dans une ou plusieurs balises 30 réceptrices, de sorte qu'au moins un équipement dudit système d'estimation de position est à la fois une station d'alimentation électrique sans fil et une balise 30 réceptrice.

30 Selon le mode de réalisation de la figure 2, l'étiquette 20 comprend un redresseur 24 pour convertir la puissance spectrale reçue par le module de réception radio 23 en une tension ou un courant électrique. L'énergie convertie peut alors être stockée dans un accumulateur électrique (non représenté).

L'accumulateur électrique se comporte donc comme une batterie permettant de délivrer l'énergie nécessaire à l'émission de messages UWB.

5 Selon un mode de réalisation, le dispositif émetteur de l'invention pourrait également alimenter le capteur et/ou le calculateur, par exemple un microprocesseur, qui s'interfacent avec le modulateur UWB.

10 Selon un mode de réalisation, l'étiquette 20 comporte un module de gestion des capacités d'énergie (non représenté) pour déclencher l'émission d'un message dans la bande UWB à partir du modulateur UWB. Ce module de gestion peut être piloté de sorte à émettre un message dès qu'un niveau d'énergie électrique collecté est suffisant pour émettre un message UWB d'une taille donnée. Selon un mode de réalisation, différents seuils sont configurés pour émettre différents messages M_1 selon une configuration donnée. Selon un mode de réalisation, une gestion d'un aléa permet de générer des messages de manières aléatoires depuis l'étiquette UWB 20.
15 Selon un autre mode de réalisation, l'étiquette comporte une horloge permettant d'émettre les messages M_1 à des intervalles e temps réguliers pendant un laps de temps.

20 La figure 3 représente un exemple de trame émise par le serveur $SERV_1$ associant des données issues de l'équipement EQ_1 dans un champ F_2 , des données issues de l'étiquette UWB 20 dans un champ F_1 et des données relatives à l'information de position POS_1 de l'étiquette 20 dans un champ F_3 . Cet exemple de trame est une juxtaposition de champs non chiffrés dans un message M_{S1} émis vers un serveur distant $SERV_2$. Selon d'autres modes de réalisation, d'autres trames peuvent être construites à partir de ces données.
25 Selon un exemple de réalisation, une clef unique est transmise, la clef unique étant générée à partir d'une association entre les données $DATA_1$ et les informations de position POS_1 . Ainsi, le simple contrôle de la valeur de la clef unique peut être réalisé afin de certifier la provenance du message M_{S1} .

30 Dans les figures 4 et 5, un lieu 50 est représenté par un espace fermé. Il peut s'agir d'un hangar, d'une pièce, d'une usine, d'un hall, d'une galerie ou de tout autre lieu à priori partiellement ou totalement fermé par des murs et/ou un toit. Un tel lieu dispose généralement de moyens pour permettre de fixer des équipements aux murs ou au plafond.

35 L'invention sera décrite au travers d'exemples de réalisation dans un tel lieu. Toutefois, l'invention s'applique également à des lieux ouverts ou

publics dès lors que des supports permettant de fixer au moins une balise réceptrice 30 sont présents.

L'exemple de la figure 1 est détaillé au travers de plusieurs exemples de réalisation correspondant à différents cas d'application de l'invention. Dans cet exemple, une pluralité de balises réceptrices 30A, 30B, 30C, et plus généralement notées 30, sont agencées de sorte à recevoir des signaux UWB provenant d'un émetteur 20. Selon un mode de réalisation, les balises 30 font parties d'un système comportant des moyens configurés pour calculer par une méthode de trilatération une information de position de l'émetteur UWB 20 ou 1.

L'exemple de la figure 5 est détaillé et illustré au travers d'un exemple de réalisation correspondant à un cas d'application de l'invention. Dans cet exemple, une seule balise réceptrice 30 est agencée de sorte à recevoir des signaux UWB provenant d'un émetteur 20 qui évolue dans l'espace. Selon un mode de réalisation, la balise 30 est configurée pour calculer par une méthode de trilatération la position de l'émetteur 20 de signaux UWB dans une période de temps donné.

Dans les deux cas d'exemples des figures 4 et 5, le serveur $SERV_2$ peut comprendre une base de données comportant des données de références pouvant être utilisées pour corroborer les informations de position reçues du serveur $SERV_1$. Ainsi, selon un mode de réalisation, le serveur $SERV_2$ permet de valider l'intégrité des données utiles $DATA_1$ en fonction de l'identifiant TAG_1 de l'émetteur et en fonction de la position à laquelle les données $DATA_1$ ont été générées.

Selon un exemple de réalisation, le serveur $SERV_2$ émet un message M_3 permettant à l'utilisateur d'accéder à un service. Le message M_3 peut être émis vers un ordinateur, vers un serveur, vers un équipement connecté à internet ou même vers le dispositif émetteur 1. Selon le cas d'application, les droits permettant d'accéder à un service peuvent être délivrés à distance à partir du serveur $SERV_2$ ou depuis un autre serveur recevant une requête du second serveur $SERV_2$. Cela peut être le cas lorsqu'une opération nécessite une autorisation émanant d'un serveur de gestion de droits tels qu'un serveur bancaire ou tout autre serveur nécessitant à des informations relatives à l'utilisateur non partagées par le serveur $SERV_2$.

Présence dans les locaux

La figure 1 représente un premier utilisateur U_1 comportant un téléphone intelligent EQ_1 . Le premier utilisateur U_1 entre, par exemple, dans son lieu de travail, tel qu'une boutique. Lorsqu'il entre dans le lieu, il est
5 nécessaire que cette personne puisse accéder à différents services. Il peut être nécessaire qu'il dispose de droits informatiques particuliers afin d'activer différents équipements ou des services applicatifs. Il peut s'agir d'un terminal de paiement, d'un accès à un répertoire d'un serveur, ou encore d'un accès à un service de gestion de temps de travail d'un ensemble de vendeurs.

10 L'utilisateur U_1 porte une étiquette UWB 20 qui peut être associée au téléphone intelligent EQ_1 en étant par exemple fixée au téléphone. Dans ce cas, l'étiquette 20 peut, par exemple, être intégrée dans une housse ou dans une coque ou encore sous forme d'un sticker. Dans ce cas, le dispositif émetteur 1 de l'invention correspond au téléphone intelligent, à sa coque et à
15 l'étiquette 20.

Selon un autre exemple, l'étiquette UWB 20 est agencée dans un autre équipement. Dans ce dernier cas, c'est alors l'ensemble des équipements : étiquettes UWB 20 et téléphone intelligent EQ_1 qui correspond au dispositif émetteur 1 sans qu'ils soient nécessairement fixés l'un à l'autre.

20 Lorsque l'utilisateur U_1 est dans la boutique 50, l'étiquette UWB 20 émet un signal qui est reçu par chaque balise 30. Selon un mode de réalisation, un algorithme de trilatération exécuté par un calculateur $SERV_1$ permet de déterminer la position POS_{U_1} de l'étiquette UWB 20 à partir de chaque signal reçu depuis l'étiquette au sein de chaque balise 30. Ainsi, selon
25 un mode de réalisation, les données émises par l'étiquette 20 comprennent également au moins une donnée $DATA_1$ provenant du téléphone intelligent EQ_1 . Les données transmises du téléphone intelligent EQ_1 vers l'étiquette UWB 20 peuvent comprendre, par exemple, un identifiant ou encore des données provenant d'un service donné, tel qu'une requête pour accéder à un
30 service distant.

La liaison entre le téléphone intelligent EQ_1 et l'étiquette UWB 20 peut être une liaison sans fil telle qu'une liaison Bluetooth. Dans ce cas d'exemple, l'étiquette UWB comprend une interface de réception compatible, ici une interface Bluetooth. Tout autre type d'interface peut être utilisée selon
35 l'interface utilisée par l'équipement EQ_1 . Selon un autre mode de réalisation,

l'étiquette 20 peut être associée à un support ou une interface physique et/ou électronique permettant d'établir une liaison filaire avec le téléphone intelligent par exemple à partir d'une interface USB, USBC ou jack audio.

L'étiquette UWB 20 est alors en mesure d'émettre au moins un
5 message UWB qui sera reçu par les balises 30_A, 30_B, 30_C. Les données DATA₁ sont ensuite démodulées par chaque balise 30.

Un serveur SERV₁ peut être utilisé pour effectuer le calcul de la position POS₁ en récupérant les dates d'arrivée de chaque message M₁ démodulé provenant de chaque balise 30. Les données DATA₁ sont ensuite
10 associées à une information de position résultante d'une opération visant à comparer les différents temps de vol de chaque signal reçu par chaque balise 30.

L'information issue du téléphone intelligent EQ₁ peut alors être associée à une information de position de l'utilisateur U₁. Cette association
15 permet de contrôler que l'utilisateur U₁ est bien dans les lieux 50 de l'entreprise/ la boutique, et elle permet, en outre, de connaître sa position précisément. Ainsi, il apparaît que sa position POS_{U1} peut être utilisée comme un mot de passe pour accéder à un certain nombre de services. Un intérêt est de rendre cette information infalsifiable par un tiers qui n'est pas précisément
20 localisé dans les lieux. Un intérêt est de sécuriser le contrôle d'accès d'un utilisateur à des services sans pour autant qu'un mot de passe soit nécessairement utilisé par l'utilisateur U₁. L'identité de l'utilisateur U₁ est donc difficilement falsifiable.

Une application consiste à émettre comme donnée DATA₁ une clef
25 publique. Lorsque la position POS₁ est vérifiée par un équipement distant, tel qu'un serveur SERV₂ de gestion d'accès et de droits utilisateurs, alors ce dernier peut émettre un mot de passe chiffré avec la clef publique émise par l'étiquette UWB vers un équipement de contrôle d'accès. L'équipement de contrôle d'accès peut être un terminal de paiement, un ordinateur comportant
30 un service, ou tout autre équipement validant l'accès. Il peut s'agir également de l'équipement EQ₁ dans la mesure où ce dernier peut donner un accès à un service distant. L'équipement de contrôle d'accès décrypte le message chiffré avec une clef privée.

Un avantage est que pour permettre l'émission d'une clef publique chiffrée il est nécessaire d'être physiquement à une position ou dans une zone permise.

5 Une application concrète de ce mode de réalisation est un accès à un réseau Wifi lorsqu'on est dans une certaine zone couverte par ce réseau wifi et par une couverture UWB à partir de balises 30.

Il peut s'agir par exemple d'un hôtel dans lequel on peut accéder au réseau wifi sans avoir à rentrer de mot de passe et uniquement lorsqu'on se situe dans une chambre ou un salon dudit hôtel. Ainsi, un tiers ne peut accéder
10 au réseau sans être physiquement présent dans les lieux.

Le réseau wifi peut également être utilisé aux fins d'accroître le contrôle de l'intégrité des données émises. Dans ce cas, les données décrivant l'association entre les données $DATA_1$ et la localisation de l'utilisateur U_1 peuvent être corroborées avec une autre information de
15 localisation, par exemple, acquise depuis la connectivité wifi ou depuis une image issue d'une caméra. Cette option permet de sécuriser le contrôle de l'intégrité de l'information de position.

Ainsi, lorsque l'utilisateur U_1 est identifié au moyen d'une donnée émise qui est localisée, il peut alors accéder à des services.
20

Contrôle d'accès à une porte

La figure 4 représente un utilisateur U_2 ayant une puce électronique comportant une mémoire avec un identifiant. Cette puce électronique correspond à l'équipement EQ_1 . Cette puce électronique peut être intégrée par
25 exemple dans un badge B_1 d'entreprise comportant un support. L'identifiant peut être utilisé pour accéder à différents services au sein de son entreprise, tels que le paiement à la cantine, l'ouverture de lieux sécurisés, la réservation d'une salle, etc.

Selon un mode de réalisation, la mémoire de la puce électronique
30 comporte d'autres données telles que des identifiants, des mots de passe ou des clefs permettant d'accéder à des services.

Dans le cas de la figure 4, le badge B_1 comporte une mémoire stockant au moins un identifiant. Le badge B_1 comprend une interface permettant de communiquer avec une étiquette radio 20 comportant un

modulateur UWB apte à émettre des signaux et plus particulièrement des séquences d'impulsions dans la bande UWB.

Selon un exemple de réalisation, le badge B_1 peut être solidaire de l'étiquette de sorte qu'ils soient collés ensemble. Une interface physique peut
5 alors être réalisée entre la puce électronique et l'étiquette radio.

Selon un cas simple, l'équipement EQ_1 est une étiquette radio comportant une mémoire avec un identifiant.

Selon un autre exemple, le badge B_1 peut être désolidarisé de l'étiquette UWB. Dans ce cas une interface sans fil permet le transfert de
10 données du badge B_1 vers l'étiquette UWB 20. Une interface radio peut être réalisée de sorte que l'identifiant soit transmis spontanément à intervalles réguliers ou après un réveil ou une activation du badge B_1 .

Selon un autre exemple, l'utilisateur U_2 peut porter un bracelet comportant une étiquette UWB et un badge B_1 , les entités étant
15 désolidarisées.

Dans cet exemple, le dispositif émetteur 1 de l'invention est, par exemple, un badge plastique et une étiquette radio UWB 20 intégrée dans un autre équipement.

L'utilisateur U_2 s'approche de la porte 51 afin d'accéder à une salle
20 dont un contrôle d'accès autorise ou non une personne à y pénétrer.

Selon un premier cas d'exemple, l'identifiant codé est modulé par le modulateur UWB et l'antenne de l'étiquette UWB pour être transmis vers les différentes balises 30_A , 30_B , 30_C .

Chaque balise 30_A , 30_B , 30_C reçoit un signal décrivant un message
25 radio M_1 provenant de l'étiquette 20. Le message M_1 comporte à minima une donnée $DATA_1$ telle qu'un identifiant de l'utilisateur U_2 . Selon différents modes de réalisation, d'autres données peuvent être modulées et transmises dans le message M_1 . Chaque balise 30_A , 30_B , 30_C transmet alors les données provenant du signal démodulé, ainsi qu'au moins une information
30 d'horodatage vers un serveur $SERV_1$.

Selon un mode de réalisation, le serveur $SERV_1$ détermine par un algorithme prédéfini la position de l'étiquette 20 de l'utilisateur U_2 en combinant les différentes informations d'horodatage provenant de chaque démodulation de chaque balise 30_A , 30_B , 30_C .

Le serveur $SERV_1$ réalise une association entre, d'une part, la position POS_{U_2} ou des données décrivant cette position POS_{U_2} et, d'autre part, les données utiles $DATA_1$ démodulées.

5 Selon différents cas de figure, cette association peut prendre différentes formes :

- une génération d'une clef unique à partir des deux informations ; Cette clef unique peut être la clef d'une base de données associant les deux informations $\{POS_1, DATA_1\}$ et/ou ;
- une génération d'une clef cryptée à partir des deux informations ;
10 cela peut être réalisé par exemple par un algorithme combinant différentes opérations telles qu'un codage, un troncage, un entrelacement, des permutations de données, etc. Un algorithme basé sur une clef privée peut également être utilisé afin de chiffrer une donnée associant les deux informations.

15

Le serveur $SERV_1$ émet alors un message M_{S_1} à un serveur distant $SERV_2$ au moyen d'un accès PA_1 afin de requérir aux droits d'accès à la salle fermée par la porte 51. Le serveur $SERV_2$ reçoit alors le message M_{S_1} émis par le premier serveur $SERV_1$. La liaison de données entre les serveurs peut
20 être réalisée au travers d'un réseau tel que le réseau NET de la figure 4, qui peut être le réseau internet ou un réseau intranet. Selon un autre exemple, cette liaison est une liaison point à point.

Le serveur $SERV_2$ contrôle alors l'identifiant du dispositif émetteur
1. Selon un mode de réalisation, cet identifiant est associé à une position POS_1
25 ou une information relative à la position POS_{U_2} de l'utilisateur U_2 . En considérant que l'utilisateur U_2 dispose des droits d'accès, le serveur $SERV_2$ peut donc certifier que l'identité de la personne U_2 n'a pas été usurpée, et que l'utilisateur U_2 situé devant la porte 51 est bien le porteur de l'étiquette UWB
20 ayant les accès. Cette information de position POS_1 permet de contrôler
30 l'intégrité de l'identifiant transmis avec la demande d'accès.

Dans ce cas, une autorisation d'accès peut être transmise à un boîtier de verrouillage de la porte 51 qui est commandée, par exemple, par une commande numérique transmise à partir d'un réseau de données.

Localisation d'un compte utilisateur accédant à un réseau depuis une machine

La figure 4 représente un autre utilisateur U_3 accédant à un service offert par un ordinateur 52, ledit ordinateur 52 étant connecté à un réseau privé. L'étiquette 20 est associée à cet ordinateur 52. L'utilisateur U_3 se connecte à un service par le biais d'un identifiant et d'un mot de passe.

Dans ce cas d'application, on souhaite connaître à partir de quel ordinateur, l'utilisateur U_3 a ouvert une session et a effectué une action donnée. Il est alors possible de localiser de manière certaine l'identifiant de l'utilisateur émis lors de sa connexion.

De la même manière, une transaction donnée peut être localisée aux fins d'être autorisée ou non.

Dans ce mode de réalisation, l'étiquette UWB 20 peut être interfacée avec l'ordinateur 52 par une connectique physique telle qu'une carte SD, une prise USB, ou encore par une connectique sans fil telle qu'une liaison Wifi, RFID, Bluetooth, etc.

Contrôle d'un capteur autonome

La figure 4 illustre un quatrième exemple de cas d'usage de la présente invention.

Selon un mode de réalisation, un équipement connecté à un réseau, tel qu'internet comprend un capteur. Dans le cas d'exemple de la figure 4, il s'agit d'un détecteur de fumée 51. Ce détecteur 51 est associé à une étiquette 20 selon une interface physique ou sans fil. L'équipement émetteur EQ_1 correspond donc ici au détecteur de fumée 51 et à l'étiquette UWB 20.

Dans ce cas de figure, la configuration de l'équipement émetteur EQ_1 comprend la configuration des données à émettre vers l'étiquette 20 et de la période à laquelle ces émissions sont réitérées.

Certaines données $DATA_1$ émises ou stockées dans le détecteur de fumée 51 peuvent être émises vers l'étiquette UWB 20 selon cette configuration. Selon un exemple, l'identifiant du détecteur 51 peut être émis vers l'étiquette 20. Alternativement, ce dernier identifiant peut être stocké dans une mémoire de l'étiquette UWB 20 et être directement émis vers les balises 30.

Selon un exemple de réalisation, les données DATA1 comportent les données brutes collectées par un capteur. Selon un autre exemple, les données DATA1 correspondent à des données filtrées, par exemple dont la valeur d'un paramètre physique a dépassé un seuil donné. Selon un exemple
5 de réalisation, la donnée DATA1 correspond uniquement à un statut parmi une liste de statuts prédéfinis : {en marche, HS, alarme détectée, alimentation réduite, etc.}.

Ainsi, dans le cas o un détecteur de fumée détecte une fumée, il déclenche une alerte. L'alerte est émise notamment par l'intermédiaire de
10 l'étiquette UWB 20 vers les balises. Les balises avec le fonctionnement décrit précédemment démodulent les signaux et un calculateur SERV1 compare les temps de vol. Ainsi, la position du détecteur de fumée est reconstruite à partir d'un calculateur centralisant les différents messages UWB 20 reçus par
15 chaque balise. Un tel équipement peut être un serveur de données SERV1. Un intérêt est de localiser la donnée émise par le détecteur de fumée 51 de manière certaine. Ainsi, la localisation de la détection de fumée peut être corroborée avec l'alerte qui a été émise et reçue via un autre système de gestion des alertes dans un bâtiment.

Un serveur distant SERV2 peut par exemple réaliser les fonctions
20 de collecte de données provenant des différents systèmes et d'analyses visant à valider une décision.

La figure 5 représente une alternative de fonctionnement dans lequel ce n'est pas une position précise d'une étiquette qui est déterminée,
25 mais une trajectoire identifiée par un algorithme de trilatération. La méthode consiste à analyser les temps de vol successifs d'un même émetteur. Un intérêt de cette solution est de minimiser le nombre de balises utilisées et de relâcher la contrainte sur la précision de la position. Un cas d'application est la détection de la présence d'un individu dans une zone donnée. Il peut s'agir
30 par exemple d'un opérateur dans un hangar manipulant différents outils et effectuant un parcours.

La trilatération permet de s'assurer d'une position d'un utilisateur ayant effectué un déplacement et dont on souhaite vérifier la présence dans une zone par exemple.

Dans ce cas d'exemple, l'étiquette UWB peut être associée à un téléphone intelligent, une tablette, un terminal électronique sans fil visant à réaliser un inventaire d'un stock, etc.

L'étiquette UWB émet un signal à trois positions successives POS_a,
5 POS_b et POS_c, on suppose que l'utilisateur U₁ se déplace dans la zone
couverte par les balises 30. Dans cet exemple, les données DATA₁
comprennent par exemple un relevé de stock de pièces dans une allée d'un
hangar. Les différentes pièces d'un stock sont supposées être à une position
donnée. Ainsi, il est possible de corroborer un trajet d'un utilisateur équipé
10 d'une étiquette avec le relevé des stocks attendus.

Cas d'exemple d'un mode de réalisation d'un émetteur UWB

Selon un mode de réalisation, l'étiquette UWB 20 comprend un
module de communication 21 simplex. Par « simplex », on entend que le
15 module de communication est adapté uniquement à émettre des messages
UWB mais ne permet pas de recevoir des messages UWB émis par d'autres
équipements tiers.

Selon un exemple, le module 21 de communication simplex se
présente par exemple sous la forme d'un circuit électrique comportant des
20 équipements tels qu'une antenne, un amplificateur, un oscillateur local, un
mélangeur, un filtre analogique et tout autre équipement pouvant contribuer à
l'émission de signaux UWB.

Selon un exemple, le module 21 de communication simplex est
configuré pour émettre les messages UWB dans une bande de fréquences
25 centrée sur 4 gigahertz (GHz) et/ou centrée sur 7.25 GHz. Rien n'exclut
cependant de considérer des bandes de fréquences centrées sur d'autres
fréquences.

Les messages UWB, émis sous la forme de signaux
radioélectriques, présentent à un instant donné un spectre fréquentiel
30 instantané de largeur prédéterminée, par exemple comprise entre 500
mégahertz (MHz) et 2.5 GHz, ce qui correspond à des impulsions radio de
durées comprises respectivement entre quelques nanosecondes et quelques
dixièmes de nanosecondes.

Dans un mode de réalisation, le module 21 de communication
35 simplex est configuré pour émettre les messages UWB en utilisant une

modulation d'impulsion radio en tout ou rien (« On Off Keying » ou OOK dans la littérature anglo-saxonne) des bits à émettre, c'est-à-dire que les valeurs des bits à émettre sont encodées par une présence ou une absence d'impulsion radio. Par exemple, si à un instant donné le bit à émettre vaut « 1 »
5 alors le module 21 de communication simplex émet une impulsion radio, alors que si le bit à émettre vaut « 0 » ledit module 21 de communication simplex n'émet pas d'impulsion radio. De telles dispositions sont avantageuses en ce qu'elles permettent de réduire la consommation électrique nécessaire pour émettre un message UWB, puisque l'émission de bits à émettre à « 0 » ne
10 consomme presque pas d'énergie électrique.

Selon un autre mode de réalisation, une modulation en position d'impulsions radio (« Pulse Position Modulation » ou PPM dans la littérature anglo-saxonne) peut être mise en œuvre dans le procédé de l'invention. Par exemple, en considérant que les bits à émettre sous la forme d'impulsions
15 radio sont cadencés à une période prédéterminée T_c , alors à chaque période T_c , les impulsions sont émises avec un décalage par rapport à la période T_c , la valeur dudit décalage dépendant de la valeur du bit à émettre.

Selon un mode de réalisation, chaque impulsion radio à bande ultra-large peut être formée en multipliant un signal sinusoïdal par une
20 enveloppe d'impulsion. Dans ce cas, l'oscillateur local formant le signal sinusoïdal correspondant à la fréquence porteuse des impulsions radio peut rester activé de manière continue sur la durée du message UWB, et l'amplitude dudit signal sinusoïdal est modulée par ladite enveloppe d'impulsion. En dehors des instants d'émission d'impulsions radio, l'amplitude
25 du signal sinusoïdal est modulée par un signal de valeur nulle.

Le signal modulé obtenu après modulation d'amplitude du signal sinusoïdal est ensuite fourni en entrée de l'amplificateur, qui peut également rester activé pendant toute la durée du message UWB à émettre.

Un avantage de cette solution est de former de manière plus
30 précise la séquence d'impulsions radio à bande ultra-large, par rapport aux dispositifs émetteurs selon l'art antérieur dans lesquels les impulsions radio sont formées en fournissant le signal sinusoïdal directement en entrée de l'amplificateur, et en activant l'amplificateur au début de l'émission d'une impulsion radio et en désactivant ledit amplificateur à la fin de l'émission de
35 ladite impulsion radio. Dans ces dispositifs émetteurs selon l'art antérieur, les

enveloppes des impulsions radio sont moins précises, car elles dépendent de la précision avec laquelle les instants d'activation/désactivation de l'amplificateur peuvent être contrôlés, la forme de l'enveloppe de l'impulsion étant par ailleurs difficilement contrôlable.

5 En modulant le signal sinusoïdal par une enveloppe d'impulsion avant d'amplifier, les impulsions radio sont formées avant l'amplificateur. Ledit amplificateur ne forme donc plus les impulsions radio mais se contente d'amplifier lesdites impulsions radio préalablement formées. Il est à noter qu'il est néanmoins possible de désactiver l'amplificateur entre les impulsions radio
10 afin de réduire la consommation électrique de l'amplificateur.

 Selon un mode de réalisation, le module de contrôle 22 comporte un ou plusieurs processeurs et des moyens de mémorisation (disque dur magnétique, mémoire électronique, disque optique, etc.) dans lesquels est mémorisé un produit programme d'ordinateur, sous la forme d'un ensemble
15 d'instructions de code de programme à exécuter.

 Alternativement ou en complément, le module de contrôle 22 comporte un ou des circuits logiques programmables (FPGA, PLD, etc.), et/ou un ou des circuits intégrés spécialisés (ASIC).

 Selon un mode de réalisation, le module de contrôle 22 comporte
20 un ensemble de moyens configurés de façon logicielle (produit programme d'ordinateur spécifique) et/ou matérielle (FPGA, PLD, ASIC, composants électroniques discrets, etc.).

REVENDEICATIONS

1. Procédé de contrôle de l'intégrité d'au moins une donnée utile ($DATA_1$),
5 caractérisé en ce qu'il comprend :
 - Acquisition (REC) d'au moins un message (M_1) dans la bande radio UWB provenant d'un émetteur (1) au moyen d'une interface sans fil et d'un démodulateur UWB ;
 - Décodage d'au moins une donnée utile ($DATA_1$), dite première
10 information ;
 - Détermination d'une information de position (POS_1) de l'émetteur UWB (20), dite seconde information, à partir de plusieurs réceptions de messages (M_1, M_i) émis par ledit émetteur (1) ;
 - Génération d'un couple de données comportant d'une part la
15 première information ($DATA_1$) et d'autre part la seconde information (POS_1).

2. Procédé selon la revendication 1, caractérisé en ce que l'acquisition
20 comprend une réception d'une séquence d'impulsions radio, définissant des messages UWB, par une pluralité de balises (30), chaque balise (30) étant localisée à une position prédéfinie.

3. Procédé selon la revendication 2, caractérisé en ce que l'information de
25 position de l'émetteur (1) est déterminée par une méthode d'estimation :
 - des temps d'arrivée des messages UWB (M_1) afin d'en déduire des différences de temps de vol (Δ_{Tvol}) de ces derniers et/ou ;
 - des puissances d'arrivée des messages UWB (M_1) et/ou ;
 - des fréquences d'arrivée des messages UWB (M_1),
30 au niveau desdites balises de réception (30).

4. Procédé selon la revendication 3, caractérisé en ce que la localisation
35 de l'émetteur (1) est déduite d'un calcul de trilatération entre les temps

d'arrivée des différents messages UWB par une estimation des différences de temps d'arrivée des différents messages (M_1) reçus par les différentes balises (30).

- 5 5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'au moins un message UWB (M_1) reçu comporte un identifiant (TAG_1) de l'émetteur (1, 20).
- 10 6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que l'information de position calculée (POS_1) et la donnée utile ($DATA_1$), et optionnellement l'identifiant (TAG_1) de l'émetteur (1), sont associées par la génération d'une clef unique (K_1).
- 15 7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que l'information de position calculée (POS_1) est comparée à une information de position déduite d'un système de géolocalisation par Wi-Fi, par adresse IP, par RFID ou par GSM, ladite comparaison évaluant un écart de distance vis-à-vis d'un seuil prédéfini, ledit procédé comportant la génération d'un message M_3 dont un champ de données détermine une autorisation ou non à un service prédéfini.
- 20 8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que l'information de position calculée (POS_1) et la donnée utile ($DATA_1$) sont combinées pour générer un code résultant d'une opération :
 - 25 ▪ de codage des données par un algorithme d'encodage ;
 - d'entrelacement, une permutation de données ou une opération permettant de générer un champ de données comportant les bits de données de l'information de position (POS_1) et les bits de données issues des données utiles ($DATA_1$), et/ou ;
 - 30 ▪ de chiffrement des données entre elles au moyen d'une clef de chiffrement.
- 35 9. Procédé selon l'une quelconque des revendications 1 à 8, caractérisé en ce qu'il comprend l'émission d'un message de synthèse (M_{s1}) vers

un serveur distant (SERV₂), le message de synthèse (MS₁) comportant :

- 5 ▪ la donnée utile (DATA₁) et l'information de position calculée (POS₁) codées dans différents champs du message de synthèse (MS₁) et/ou ;
- la donnée utile (DATA₁) et l'information de position calculée (POS₁), ladite position calculée (POS₁) étant cryptée dans le message de synthèse (MS₁) et/ou ;
- 10 ▪ une clef unique permettant de déchiffrer l'information de position chiffrée dans un champ du message de synthèse (MS₁) et/ou ;
- un identifiant (TAG₁) de l'émetteur UWB (1, 20) ayant émis le message et/ou ;
- 15 ▪ un identifiant (ID₁) d'un équipement (EQ₁) sur lequel une étiquette (20) est agencée, ledit équipement (EQ₁) et l'étiquette (20) formant un dispositif émetteur (1).

10. Système de contrôle comportant :

- 20 ▪ Au moins une balise de réception (30) comportant :
 - Une première interface sans fil configurée pour recevoir des signaux dans la bande UWB ;
 - Un module radio permettant de traiter les signaux reçus de manière à horodater la réception d'une pluralité de messages reçus (M₁) et de démoduler en bande de base au moins une donnée utile (DATA₁) ;
- 25 ▪ Un calculateur (SERV₁) pour déterminer une position de l'espace (POS₁) à partir de l'analyse d'une pluralité de propriétés issues des réceptions de messages (M₁, $\sum M_i$) provenant d'au moins un émetteur (20), lesdites propriétés issues des réceptions étant corrélées de manière à déterminer une information de position
- 30 (POS₁) d'un émetteur (1, 20) ;
- Une mémoire pour enregistrer au moins une valeur associant d'une part une information de position de l'espace (POS₁) calculée et d'autre part au moins une donnée utile (DATA₁).

35 11. Système de contrôle selon la revendication 9 caractérisé en ce que :

- chaque balise (30) comporte un composant pour horodater les messages UWB (M1) reçus ;
- le calculateur (SERV₁) détermine des écarts de temps de vol (Δt_{vol}) issus d'une pluralité de réception de messages (M₁, $\sum M_i$) provenant d'au moins un émetteur (20) afin de déterminer l'information de position (POS₁) de l'émetteur (1, 20).

12. Système de contrôle selon l'une quelconque des revendications 9 à 10 caractérisé en ce qu'il comprend en outre un second serveur distant (SERV₂), ledit serveur distant (SERV₂) comportant une interface pour recevoir un message de synthèse (M_{S1}) généré par le calculateur (SERV₁) et comportant des moyens de calculs pour :

- décoder et contrôler l'information de position (POS₁) et ;
- générer un message (M₃) visant à permettre ou interdire l'accès à un service vers un équipement donné,

le second serveur (SERV₂) comportant, en outre, une interface pour émettre ledit message (M₃) vers l'équipement donné.

13. Dispositif émetteur (1) comportant :

- Un équipement (EQ₁) susceptible de générer au moins une donnée utile (DATA₁) dans un contexte prédéfini et de transférer ladite donnée utile (DATA₁) au moyen d'une première interface (10) ;
- Une étiquette radio (20) comportant une seconde interface (26) pour recevoir ladite au moins une donnée utile (DATA₁), ladite étiquette radio (20) comportant un modulateur UWB dans la bande UWB pour émettre un signal comportant ladite au moins une donnée utile (DATA₁).

14. Dispositif émetteur (1) selon la revendication 12, comportant en outre :

- Un module de réception radio (23) pour recevoir un flux d'ondes radio ;
- Un redresseur (24) pour convertir la puissance spectrale reçue par le module de réception radio (23) en une tension ou un courant électrique ;
- Un accumulateur électrique ;

- Un module de gestion des capacités d'énergie pour déclencher l'émission d'un message dans la bande UWB à partir du modulateur UWB.

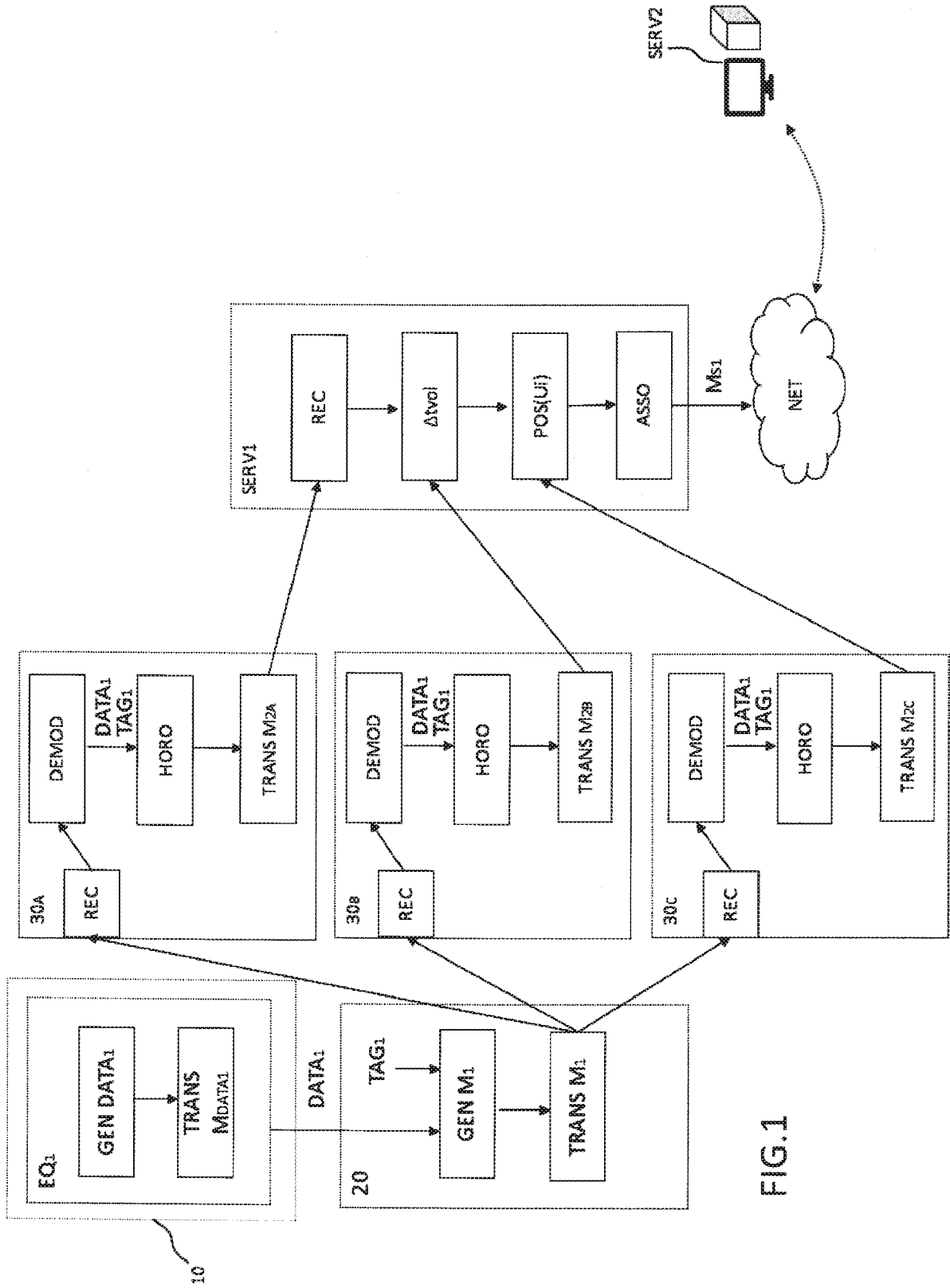


FIG. 1

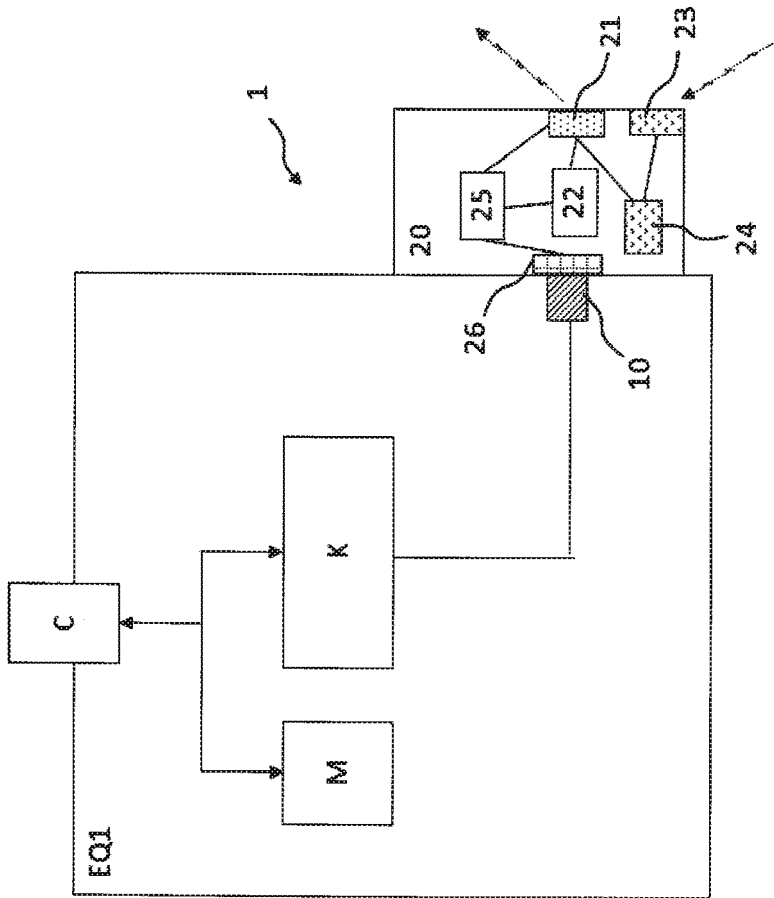


FIG.2

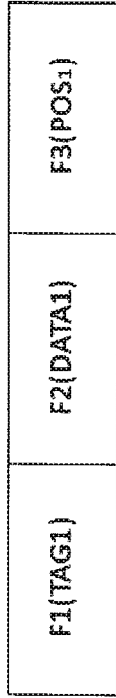


FIG.3

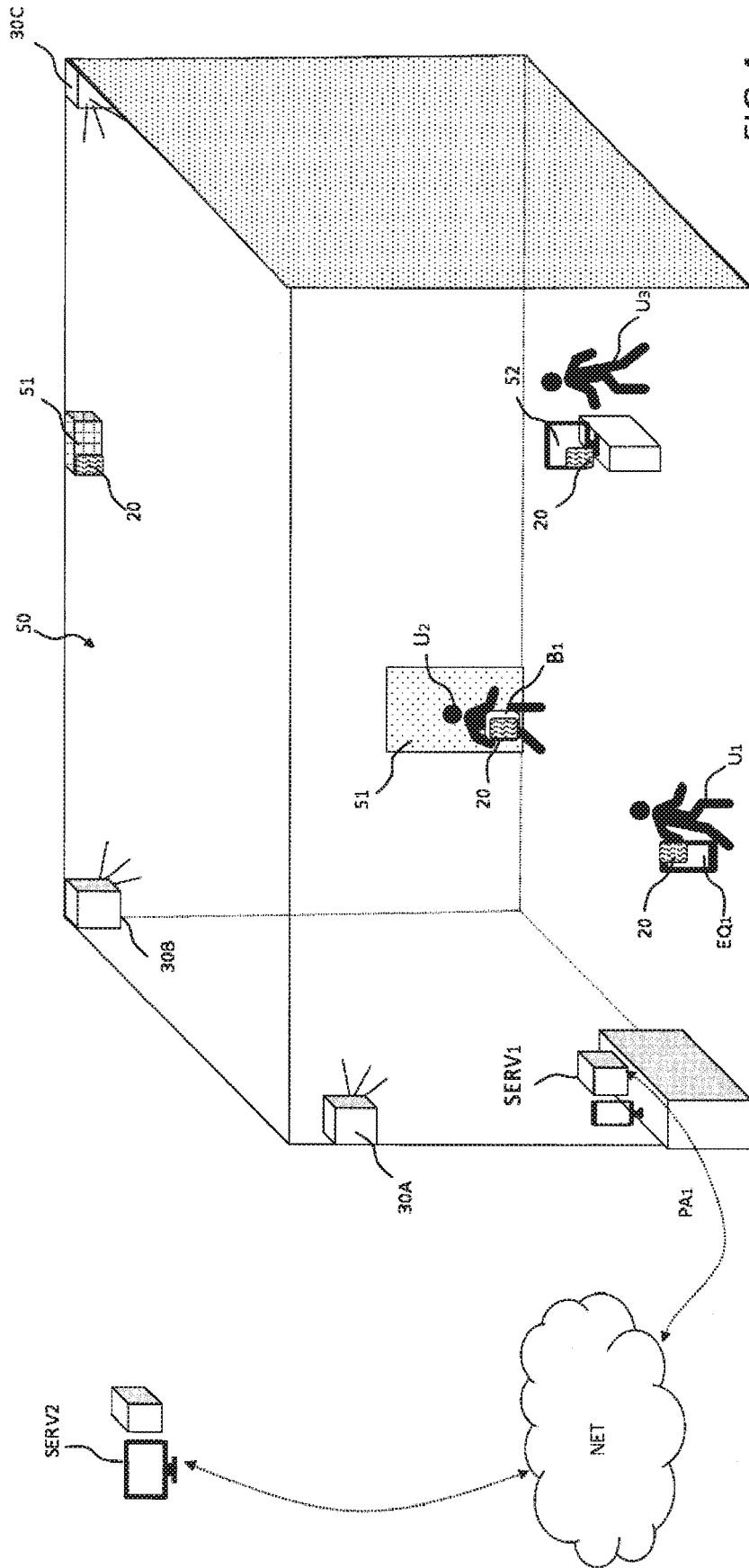


FIG.4

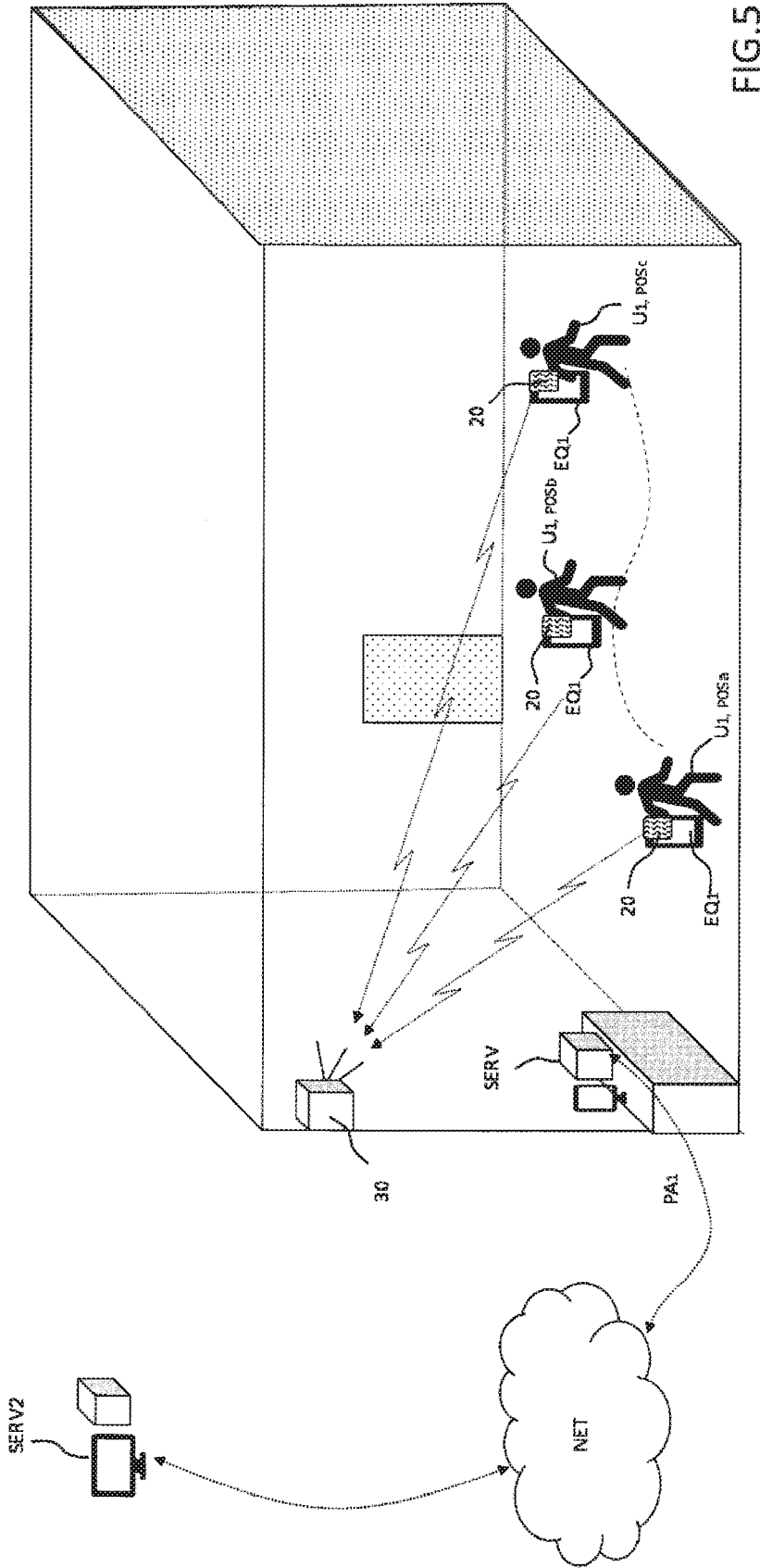


FIG.5



**RAPPORT DE RECHERCHE
PRÉLIMINAIRE**

N° d'enregistrement
national

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

FA 860071
FR 1800921

| 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 | | |
| Y | US 2008/186231 A1 (ALJADJEFF DANIEL [IL] ET AL) 7 août 2008 (2008-08-07) * figure 1 * * alinéas [0015] - [0017], [0021] - [0029] * * alinéas [0031] - [0034], [0035] - [0037], [0039] * * alinéas [0041] - [0048] * * alinéas [0059], [0067] - [0069] * ----- | 1-12,14 | G01S5/10 H04L9/14 H04L12/951 |
| Y | US 2008/030359 A1 (SMITH CURT [US] ET AL) 7 février 2008 (2008-02-07) * alinéas [0020], [0026] * * alinéas [0031], [0033], [0037] - [0042] * * alinéas [0046], [0047], [0050] * * alinéas [0062], [0066] * * alinéas [0072], [0073], [0077] * ----- | 1-8,12,14 | |
| Y | US 2015/355311 A1 (O'HAGAN JAMES [US] ET AL) 10 décembre 2015 (2015-12-10) * alinéa [0004] * * alinéas [0045], [0048], [0049] * * alinéas [0063], [0064] * * alinéa [0096] * ----- | 1 | DOMAINES TECHNIQUES RECHERCHÉS (IPC) G01S G07C G08B |
| X | US 2012/176272 A1 (HIRATA SEIICHIRO [JP] ET AL) 12 juillet 2012 (2012-07-12) * alinéas [0011] - [0014], [0023] - [0031], [0036] - [0046] * ----- | 13 | |
| Y | | 1 | |
| Y | US 2004/223556 A1 (CHOI YUN-HWA [KR]) 11 novembre 2004 (2004-11-11) * alinéas [0012] - [0030] * ----- | 1 | |
| | -/-- | | |
| Date d'achèvement de la recherche | | Examineur | |
| 27 juin 2019 | | Naddeo, Giovanni | |
| CATÉGORIE DES DOCUMENTS CITÉS | | | |
| X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire | | T : théorie ou principe à la base de l'invention 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. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant | |

1
EPO FORM 1503 12.99 (P04C14)



**RAPPORT DE RECHERCHE
PRÉLIMINAIRE**

N° d'enregistrement
national

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

FA 860071
FR 1800921

| 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 | | |
| Y | US 2016/259032 A1 (HEHN MARKUS [CH] ET AL) 8 septembre 2016 (2016-09-08) * alinéas [0040] - [0045] * * alinéas [0113] - [0127] * * alinéas [0163], [0172] * * alinéas [0227], [0256] - [0260], [0270], [0274] * | 10,11 | |
| Y | DE DOMINICIS C M ET AL: "High-precision UWB-based timestamping", PRECISION CLOCK SYNCHRONIZATION FOR MEASUREMENT CONTROL AND COMMUNICATION (ISPCS), 2011 INTERNATIONAL IEEE SYMPOSIUM ON, IEEE, 12 septembre 2011 (2011-09-12), pages 50-55, XP031974501, DOI: 10.1109/ISPCS.2011.6070150 ISBN: 978-1-61284-893-8 * le document en entier * | 11 | |
| Y | US 2005/135811 A1 (LEE JONG-HUN [KR] ET AL) 23 juin 2005 (2005-06-23) * alinéas [0019] - [0021] * * alinéas [0031] - [0035] * | 9 | DOMAINES TECHNIQUES RECHERCHÉS (IPC) |
| Date d'achèvement de la recherche | | Examineur | |
| 27 juin 2019 | | Naddeo, Giovanni | |
| 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 | |
| Y : particulièrement pertinent en combinaison avec un | | à la date de dépôt et qui n'a été publié qu'à cette date | |
| autre document de la même catégorie | | de dépôt ou qu'à une date postérieure. | |
| A : arrière-plan technologique | | D : cité dans la demande | |
| O : divulgation non-écrite | | L : cité pour d'autres raisons | |
| P : document intercalaire | | | |
| | | & : membre de la même famille, document correspondant | |

1

EPO FORM 1503 12.99 (P04C14)

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1800921 FA 860071**

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 **27-06-2019**

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 2008186231 A1 | 07-08-2008 | EP 2117546 A2 | 18-11-2009 |
| | | US 2008186231 A1 | 07-08-2008 |
| | | WO 2008110928 A2 | 18-09-2008 |
| ----- | | | |
| US 2008030359 A1 | 07-02-2008 | US 2008030359 A1 | 07-02-2008 |
| | | WO 2007145890 A2 | 21-12-2007 |
| ----- | | | |
| US 2015355311 A1 | 10-12-2015 | US 2015355311 A1 | 10-12-2015 |
| | | US 2017356978 A1 | 14-12-2017 |
| ----- | | | |
| US 2012176272 A1 | 12-07-2012 | JP 5761480 B2 | 12-08-2015 |
| | | JP 2011080946 A | 21-04-2011 |
| | | US 2012176272 A1 | 12-07-2012 |
| | | WO 2011043091 A1 | 14-04-2011 |
| ----- | | | |
| US 2004223556 A1 | 11-11-2004 | AUCUN | |
| ----- | | | |
| US 2016259032 A1 | 08-09-2016 | CN 107980100 A | 01-05-2018 |
| | | EP 3268765 A1 | 17-01-2018 |
| | | JP 2018510366 A | 12-04-2018 |
| | | US 2016259032 A1 | 08-09-2016 |
| | | US 2017003374 A1 | 05-01-2017 |
| | | US 2018196120 A1 | 12-07-2018 |
| | | WO 2016142837 A1 | 15-09-2016 |
| ----- | | | |
| US 2005135811 A1 | 23-06-2005 | JP 4134018 B2 | 13-08-2008 |
| | | JP 2005184830 A | 07-07-2005 |
| | | KR 20050063211 A | 28-06-2005 |
| | | US 2005135811 A1 | 23-06-2005 |
| ----- | | | |