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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

PCT

(43) Date de la publication internationale
30 novembre 2006 (30.11.2006)

(10) Numéro de publication internationale
WO 2006/125885 A1

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

(21) Numéro de la demande internationale :
PCT/FR2006/001101

(22) Date de dépôt international : 16 mai 2006 (16.05.2006)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0505315 26 mai 2005 (26.05.2005) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **MALLEDANT, Matthieu** [FR/FR]; c/o France Telecom, 38/40 rue du Général Leclerc, F-92794 Issy les Moulineaux Cedex 9 (FR). **LANGLET, Patrick** [FR/FR]; c/o France Telecom, 38/40 rue du General Leclerc, F-92794 Issy les Moulineaux Cedex 9 (FR). **GILBERTAS, Claire** [FR/FR]; c/o France Telecom, 38/40 rue du Général Leclerc, F-92794 Issy les Moulineaux Cedex 9 (FR).

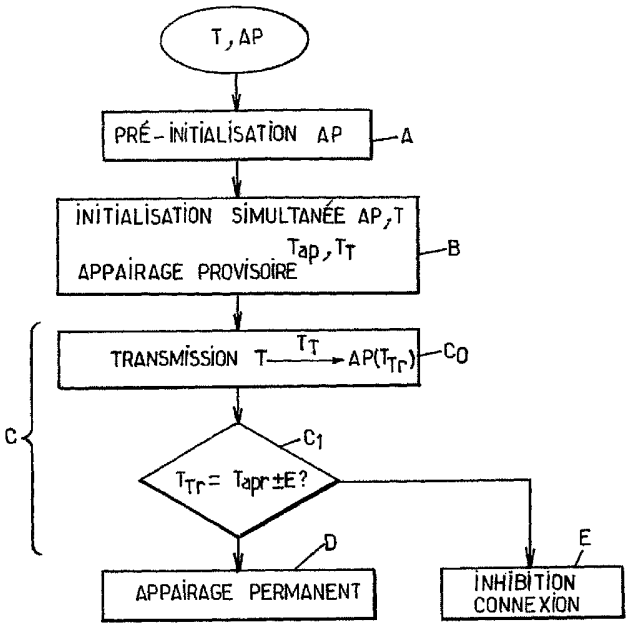
(74) Mandataires : **FRECHEDE, Michel** etc.; Cabinet Plasseraud, 52, rue de la Victoire, F-75440 Paris Cedex 09 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY,

[Suite sur la page suivante]

(54) Title: METHOD FOR CONTROLLING CONNECTION OF A PERIPHERAL TO AN ACCESS POINT, CORRESPONDING ACCESS POINT AND PERIPHERAL

(54) Titre : PROCEDE DE CONTROLE DE LA CONNEXION D'UN PERIPHERIQUE A UN POINT D'ACCES, POINT D'ACCES ET PERIPHERIQUE CORRESPONDANTS



A PRE-INITIALIZING
B SIMULTANEOUS AP, T INITIALIZING
C_0 TRANSMITTING VALUE OF STORED INITIALIZING
C_1 DURATION
D PERMANENT MATCHING
E INHIBITING CONNECTION

(57) Abstract: The invention concerns a method for controlling connection of a peripheral (T) to an access point (AP) in shared network. It consists in pre-initializing (A) the access point through a local command of that access point, the pre-initializing step enabling at least the access point to be configured to provisionally match the peripheral, simultaneously initializing (B) the access point (AP) and the peripheral (T) through a substantially concurrent local command of the access point respectively of the peripheral, locally measuring and storing the initializing duration (T_{ap}), (T_T) of each local command at the access point respectively at the peripheral, and, following provisional matching of the access point and the peripheral, transmitting and receiving (C_o), at least from the peripheral to the access point, the value of the stored initializing duration (T_T) and comparing (C_1) by equality comparison, the value of the locally measured initializing duration with the received initializing duration. If the received initializing duration (T_{Tr}) is substantially equal to the locally measured initializing duration (T_{ap}), the peripheral being accepted as recognized connection requesting peripheral, the follow-up of the peripheral connection is authorized by invoking (D) a permanent matching procedure. Otherwise, the connection follow-up is inhibited (E) at the access point. The invention is useful for managing control of connection of peripherals to an access point in shared network such as WIFI, Bluetooth, online Powerline Communication or the like.

[Suite sur la page suivante]

WO 2006/125885 A1

MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

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

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

— *avec rapport de recherche internationale*

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

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

(57) Abrégé : L'invention concerne un procédé de contrôle de la connexion d'un périphérique (T) à un point d'accès (AP) en réseau partagé. Il consiste à pré-initialiser (A) le point d'accès par une commande locale de ce point d'accès, l'étape de pré- initialisation permettant au moins de configurer le point d'accès pour appairer provisoirement le périphérique, à initialiser simultanément (B) le point d'accès (AP) et le périphérique (T) par une commande locale sensiblement concomitante en durée du point d'accès respectivement du périphérique, mesurer localement et mémoriser la durée d'initialisation (T_{ap}), (T_T) de chaque commande locale au niveau du point d'accès respectivement du périphérique, et, suite à un appairage provisoire du point d'accès et du périphérique, transmettre et recevoir (C_o), au moins du périphérique vers le point d'accès, la valeur de la durée d'initialisation mémorisée (T_T) et comparer (C_1) par comparaison d'égalité, la valeur de la durée d'initialisation mesurée localement à la durée d'initialisation reçue. Si la durée d'initialisation reçue (T_{Tr}) est sensiblement égale à la durée d'initialisation mesurée localement (T_{ap}), le périphérique étant admis comme périphérique demandeur de connexion identifié, on autorise la poursuite de la connexion du périphérique par appel (D) d'une procédure d'appairage permanent. Sinon, on inhibe (E) au moins au niveau du point d'accès, la poursuite de la connexion. Application à la gestion du contrôle de connexion de périphériques à un point d'accès en réseau partagé tel que WIFI, Bluetooth, Courants Porteurs en Ligne ou autres.

PROCEDE DE CONTROLE DE LA CONNEXION D'UN PERIPHERIQUE A UN POINT D'ACCES, POINT D'ACCES ET PERIPHERIQUE CORRESPONDANTS

L'invention concerne un procédé de contrôle de la connexion d'un périphérique à un point d'accès en réseau partagé, un point d'accès et un périphérique spécialement adaptés pour exécuter un tel procédé et le ou les produits de programme d'ordinateur permettant la mise en œuvre de ces derniers.

A l'heure actuelle la connexion d'un périphérique à un point d'accès en réseau partagé fait appel à une procédure de connexion sécurisée, pour les réseaux partagés tels que réseaux radio ou filaire répondant aux spécifications des recommandations 802.11, 802.15, 802.16, Bluetooth, RFId ou à Courant Porteur de Ligne par exemple. Cette procédure de connexion sécurisée est appliquée, une fois que le champ électromagnétique ou électrique support de la liaison en réseau partagé est détecté par le périphérique.

En principe, tout périphérique candidat est a priori en mesure de mettre en œuvre cette procédure de connexion sécurisée, indépendamment de l'existence ou non d'autres périphériques connectés au même point d'accès, pourvu que ce périphérique candidat dispose des habilitations nécessaires.

En particulier, après détection du champ support de la liaison en réseau partagé, tout périphérique habilité est en mesure de lancer une telle procédure sur simple transmission de son adresse MAC.

Des procédures de reconnaissance préalable ont été proposées plus récemment. Parmi celles-ci on peut citer :

– Le processus décrit par WO 02060151 propose un appairage automatique. Le dispositif décrit par le document précité comprend une mémoire pour enregistrer des clés d'appairage et un circuit de commande de la mémoire pour réaliser une procédure automatique de connexion à un appareil et fournir à ce dernier, désirant se connecter, une clé d'appairage. Cette procédure met en œuvre une phase de reconnaissance entre le dispositif de distribution des clés d'appairage et les

récepteurs de clés d'appairage, dans laquelle ce dispositif et un appareil récepteur de la clé d'appairage possèdent une première clé commune, pré-configurée en mémoire ou générée localement selon une méthode de calcul connue. Une comparaison de la clé commune permet au dispositif de distribution des clés d'appairage et à l'appareil récepteur de s'identifier mutuellement.

Le processus précité présente l'inconvénient d'une phase d'identification initiale basée sur une clé privée commune pré-configurée dans le dispositif de distribution des clés d'appairage et dans chaque appareil récepteur. La gestion des clés privées est, en général, lourde et peu adaptée à des appareils de grande diffusion. En outre, un appareil supplémentaire, le dispositif de distribution de clés d'appairage, est nécessaire pour appairer deux appareils.

– Le processus décrit par US 2003 200434 propose un procédé de reconnaissance entre deux appareils. Ce procédé consiste à mettre en marche les deux appareils, désigner l'un des appareils comme maître et l'autre comme esclave puis à les porter à proximité physique l'un de l'autre. L'appareil maître émet selon un diagramme de rayonnement spécifique, à portée réduite, de façon que l'appareil esclave puisse recevoir le signal porteur afin de transmettre une clé à ce dernier. L'appareil maître procède alors à un retour à son diagramme de rayonnement nominal et l'appareil esclave utilise la clé précédemment reçue pour s'authentifier auprès de l'appareil maître.

Ce processus précité présente deux inconvénients :

- Certaines technologies de liaison radio sont élaborées pour avoir un maximum de portée, de l'ordre de plusieurs centaines de mètres. C'est par exemple le cas de la technologie radio WIFI définie par la recommandation 802.11. Obtenir une portée de quelques centimètres au moyen de ces technologies se révèle impossible en pratique ;

- Le processus de connaissance entre les deux appareils étant basé uniquement sur la faible portée de la liaison radio utilisée pour la transmission de clé, il n'existe pas d'étape d'identification mutuelle. Ainsi, un utilisateur malveillant peut facilement obtenir qu'un appareil esclave s'appaire à son propre appareil maître, pour

peu que son appareil maître émette suffisamment fort pour dialoguer avec cet appareil esclave, qui tente de s'appairer.

La présente invention a pour objet de remédier aux inconvénients des techniques de l'art antérieur et d'améliorer ces dernières, en introduisant une phase d'identification, liée à une reconnaissance de périphérique demandeur de connexion identifié, auprès du point d'accès.

Un autre objet de la présente invention est en particulier la mise en œuvre d'une phase d'identification mutuelle permettant, d'une part, une reconnaissance du périphérique demandeur de connexion identifié, auprès du point d'accès, et, d'autre part, une reconnaissance du point d'accès demandé, auprès du périphérique, indépendamment d'une quelconque attribution d'une qualité de maître ou d'esclave à l'un de ces derniers.

Un autre objet de la présente invention est également d'introduire une sécurisation accrue de la procédure de connexion d'un périphérique à un point d'accès en réseau partagé, par l'introduction dans la phase d'identification, notamment mutuelle, d'un critère de rejet de toute nouvelle demande de connexion étrangère à la transaction.

Un autre objet de la présente invention est également d'introduire une sécurisation accrue de la procédure de connexion d'un périphérique à un point d'accès en réseau partagé, par l'introduction dans la phase d'identification, notamment mutuelle, d'un critère de poursuite de la connexion demandée, acceptée conditionnellement à l'absence de toute tentative de connexion étrangère dans un délai déterminé à compter d'une demande de connexion ayant satisfait au critère d'identification.

De manière générale, l'invention a pour objet un procédé de contrôle de la connexion d'un premier dispositif et d'un deuxième dispositif remarquable en ce qu'il consiste, au moins, à exécuter une commande locale d'initialisation pendant une certaine durée sur le premier et le deuxième dispositif. Suite à un appairage provisoire du premier et du deuxième dispositif, il consiste ensuite à échanger les valeurs de durées d'initialisation respectives du premier et du deuxième dispositif. Si

les durées d'initialisation du premier et du deuxième dispositif diffèrent d'une valeur inférieure à une valeur de seuil, la connexion est poursuivie. Sinon, la connexion est inhibée.

La présente invention a également pour objet un procédé de contrôle de la connexion d'un périphérique à un point d'accès en réseau partagé, remarquable en ce qu'il consiste au moins à pré-initialiser le point d'accès par une commande locale de point d'accès, l'étape de pré initialisation permettant au moins de configurer ce point d'accès pour appairer provisoirement un périphérique. Il consiste ensuite à initialiser simultanément le point d'accès et le périphérique par une commande locale sensiblement concomitante en durée du point d'accès respectivement du périphérique et à mesurer localement et à mémoriser la durée d'initialisation de chaque commande locale au niveau du point d'accès respectivement du périphérique. Suite à un appairage provisoire du point d'accès et du périphérique, il consiste à transmettre et recevoir au moins du périphérique vers le point d'accès, la valeur de la durée d'initialisation mémorisée et à comparer par comparaison d'égalité, au moins au niveau du point d'accès, la valeur de la durée d'initialisation mesurée localement à la durée d'initialisation reçue. Si la durée d'initialisation reçue est sensiblement égale à la durée d'initialisation mesurée localement, le périphérique est admis comme périphérique demandeur de connexion identifié et le procédé consiste alors à autoriser la poursuite de la connexion du périphérique par appel d'une procédure d'appairage permanent. Sinon, le procédé consiste à inhiber, au moins au niveau du point d'accès, la poursuite de la connexion.

L'invention a également pour objet un point d'accès en réseau partagé comportant au moins une interface de signal de liaison, une interface logicielle de gestion d'interface de signal de liaison remarquable en ce qu'il comporte au moins un module d'appairage point d'accès/périphérique relié à cette interface logicielle de gestion d'interface de signal de liaison et une base de données reliée au module d'appairage point d'accès/périphérique comportant, d'une part, des données temporaires, et, d'autre part, des données permanentes. Il comporte en outre un dispositif d'initialisation du point d'accès par une commande locale de ce point

d'accès. Le module d'appairage point d'accès/périphérique permet de mesurer localement et de mémoriser la durée d'initialisation du point d'accès par la commande locale, et, suite à un appairage provisoire de ce point d'accès et d'un périphérique, de recevoir au moins de ce périphérique une valeur de la durée d'initialisation mémorisée de ce périphérique, de comparer par comparaison d'égalité la valeur de la durée d'initialisation mesurée localement à la valeur de la durée d'initialisation mesurée reçue. Si la durée d'initialisation mesurée reçue est sensiblement égale à la durée d'initialisation mesurée localement, le périphérique est reconnu comme périphérique demandeur de connexion identifié et la poursuite de la connexion du périphérique est autorisée par appel d'une procédure d'appairage permanent. Sinon, la poursuite de la connexion est inhibée, au moins au niveau du point d'accès.

L'invention a également pour objet un périphérique connectable à un point d'accès en réseau partagé comportant au moins une interface de signal de liaison, une interface logicielle de gestion d'interface de signal de liaison remarquable en ce qu'il comporte au moins un module d'appairage périphérique/point d'accès relié à cette interface logicielle de gestion d'interface de signal de liaison et une base de données reliée au module d'appairage périphérique/point d'accès comportant, d'une part, des données temporaires, et, d'autre part, des données permanentes. Il comporte en outre un dispositif d'initialisation du périphérique par une commande locale de ce périphérique. Le module d'appairage périphérique/point d'accès permet de mesurer localement et de mémoriser la durée d'initialisation du périphérique par la commande locale, et, suite à un appairage provisoire de ce périphérique et de ce point d'accès, de recevoir au moins de ce point d'accès une valeur de la durée d'initialisation mémorisée de ce point d'accès, de comparer par comparaison d'égalité la valeur de la durée d'initialisation mesurée localement à la valeur de la durée d'initialisation mesurée reçue. Si la durée d'initialisation mesurée reçue est sensiblement égale à la durée d'initialisation mesurée localement, le point d'accès est reconnu comme point d'accès initialisé pour le périphérique demandeur d'accès et la poursuite de la connexion du périphérique est autorisée par appel d'une procédure d'appairage permanent.

Sinon, la poursuite de la connexion est inhibée, au moins au niveau du périphérique.

Le procédé, le point d'accès et le périphérique objets de l'invention trouvent application à la gestion du contrôle de connexion de périphériques à un point d'accès en réseau partagé mettant en œuvre des technologies aussi variées que les technologies WIFI, Bluetooth, Courants Porteurs en Ligne ou autres.

Ils seront mieux compris à la lecture de la description et à l'observation des dessins ci-après dans lesquels :

- la figure 1 représente un organigramme des étapes essentielles de mise en œuvre du procédé de contrôle de la connexion d'un périphérique à un point d'accès en réseau partagé conforme à l'objet de la présente invention ;
- la figure 2 représente, à titre illustratif, un détail de mise en œuvre spécifique des étapes d'initialisation simultanée et d'appairage provisoire, de transmission réciproque des valeurs de durée d'initialisation locale du point d'accès et du périphérique, au périphérique respectivement au point d'accès, et de comparaison de ces valeurs pour exécuter une identification mutuelle du périphérique demandeur d'accès et du point d'accès, dans un mode de mise en œuvre préférentiel non limitatif du procédé objet de l'invention représenté en figure 1 ;
- la figure 3a représente, à titre illustratif, un schéma synoptique par blocs d'un point d'accès en réseau partagé conforme à l'objet de la présente invention ;
- la figure 3b représente, à titre illustratif, un schéma fonctionnel d'un module d'appairage point d'accès/périphérique incorporé dans le point d'accès objet de l'invention, tel que représenté en figure 3a ;
- la figure 3c représente, sous forme d'un organigramme, les étapes essentielles d'un protocole de contrôle d'une connexion demandée par un périphérique tel que conduit par le module d'appairage point d'accès/périphérique représenté en figure 3b, dans la phase de pré-initialisation de ce dernier ;
- la figure 3d représente, sous forme d'un organigramme, les étapes essentielles d'un protocole de contrôle d'une connexion demandée par un

périphérique, tel que conduit par le module d'appairage point d'accès/périphérique représenté en figure 3b, dans la phase d'initialisation de ce dernier ;

- la figure 4a représente, à titre illustratif, un schéma synoptique par blocs d'un périphérique connectable à un point d'accès en réseau partagé conforme à l'objet de la présente invention ;

- la figure 4b représente, à titre illustratif, un schéma fonctionnel d'un module d'appairage périphérique/point d'accès incorporé dans le périphérique objet de l'invention tel que représenté en figure 4a ;

- la figure 4c représente, sous forme d'un organigramme les étapes essentielles d'un protocole de contrôle d'une connexion demandée par un périphérique, tel que conduit par le module d'appairage périphérique/point d'accès représenté en figure 4b.

Une description plus détaillée du procédé de contrôle de la connexion d'un périphérique à un point d'accès à un réseau partagé, objet de la présente invention, sera maintenant donnée en liaison avec la figure 1, puis avec la figure 2.

Le point d'accès et le périphérique constituent un premier et un deuxième dispositif.

En référence à la figure 1 précitée, le procédé objet de l'invention, consiste, au moins en une étape A, pour un périphérique T et un point d'accès AP en réseau partagé, à pré-initialiser le point d'accès AP par une commande locale de ce point d'accès.

L'étape de pré-initialisation exécutée à l'étape A représentée en figure 1 permet au moins de configurer le point d'accès AP pour appairer provisoirement un périphérique. L'étape A est suivie d'une étape B consistant à initialiser simultanément le point d'accès AP et le périphérique T par une commande locale sensiblement concomitante en durée du point d'accès AP respectivement du périphérique T et à mesurer localement et à mémoriser la durée d'initialisation T_{ap} pour le point d'accès AP respectivement la durée T_T pour le périphérique T de chaque commande locale au niveau du point d'accès, respectivement du périphérique T.

Suite aux opérations de mesure précitées et compte tenu de la configuration effectuée à l'étape A pour le point d'accès AP on procède alors à un appairage provisoire du point d'accès AP et du périphérique T.

D'une manière générale, on indique que la notion d'appairage provisoire recouvre la notion de configuration du point d'accès AP pour permettre à ce dernier d'échanger avec le périphérique T demandeur de la connexion certaines informations nécessaires à l'exécution d'une identification et de la poursuite de la connexion lorsque les critères d'identification ont été satisfaits, ainsi qu'il sera décrit ultérieurement dans la description. Cette notion d'appairage provisoire correspond donc à une notion spécifique d'appairage laquelle consiste en un échange de données techniques permettant d'exécuter une connexion limitée pour exécuter l'appairage provisoire.

L'appairage provisoire ayant été effectué entre le point d'accès AP et le périphérique T à l'étape B de la figure 1, le procédé objet de l'invention consiste alors à effectuer une étape consistant à transmettre et recevoir, à l'étape C_0 de la figure 1, au moins du périphérique vers le point d'accès, la valeur de la durée d'initialisation T_T mémorisée localement au niveau du périphérique T, cette opération étant notée :

$$\text{Transmission} \xrightarrow{T_T} AP\,(T_{Tr})$$

L'opération de transmission et de réception de la valeur de la durée d'initialisation mémorisée T_T localement au niveau du périphérique est suivie d'une opération C_1 consistant à comparer par comparaison d'égalité au moins au niveau du point d'accès AP la valeur de la durée d'initialisation mesurée localement du point d'accès AP, c'est-à-dire la durée d'initialisation T_{ap}, à la durée d'initialisation reçue T_{Tr} correspondant en fait à la durée d'initialisation du périphérique.

Sur la figure 1, l'opération de comparaison d'égalité est notée :

$T_{Tr} = T_{ap} \pm E$?

Dans cette relation on indique que E représente une tolérance en pourcentage de durée de la valeur de durée d'initialisation du point d'accès AP, c'est-à-dire de la durée T_{ap}.

Dans un exemple de mise en œuvre non limitative, la valeur de E peut être prise égale à 5 % de cette durée d'initialisation par exemple.

Si la durée d'initialisation reçue T_{Tr} est sensiblement égale à la durée d'initialisation mesurée localement T_{ap}, à la valeur de tolérance E près, alors en réponse positive au test C_1 le périphérique est admis comme périphérique demandeur de connexion identifié et le procédé objet de l'invention, consiste alors, en une étape D, à autoriser la poursuite de la connexion du périphérique T au point d'accès AP par appel d'une procédure d'appairage permanent.

Sinon, en réponse négative au test C_1 de la figure 1, le procédé objet de l'invention, le périphérique T demandeur de connexion n'étant pas reconnu comme périphérique demandeur de connexion identifié, le procédé objet de l'invention consiste à inhiber à l'étape E, au moins au niveau du point d'accès, la poursuite de la connexion.

On comprend en particulier que la comparaison d'égalité précédemment décrite peut en fait consister en une comparaison de la valeur de la différence des durées d'initialisation du premier et du deuxième dispositif à une valeur de seuil. Si cette valeur est inférieure à cette valeur de seuil, la connexion est poursuivie. Sinon la connexion est inhibée.

D'une manière plus spécifique, on comprend en particulier que, le procédé objet de la présente invention permet d'effectuer un codage du temps d'initialisation à l'initiative du seul utilisateur du périphérique T et du point d'accès AP. En effet, la commande locale concomitante en durée du point d'accès et du périphérique T permettant d'initialiser simultanément le point d'accès et le périphérique considéré permet d'appairer valablement le périphérique demandeur de connexion T au point d'accès AP choisi par l'utilisateur.

En effet, la durée d'initialisation peut être quelconque et laissée à l'initiative de l'utilisateur dans une plage de valeurs comprise entre 5 à 25 secondes par exemple.

Ainsi, l'utilisateur peut agir sensiblement simultanément dans la valeur de tolérance E précitée pour exécuter une connexion et en particulier une initialisation du point d'accès AP et du périphérique T qu'il souhaite connecter à ce dernier.

On comprend, en particulier, que le codage temporel de la durée d'initialisation simultanée du périphérique et du point d'accès AP permet, sous la volonté et l'action de l'utilisateur, d'attribuer une valeur commune sensiblement identique au point d'accès AP et au périphérique à connecter, ce qui permet de valider l'identification notamment du périphérique demandeur de connexion vis-à-vis du point d'accès AP.

On comprend en effet que dans l'hypothèse où un point d'accès AP a été pré-initialisé, un tiers indélicat muni d'un autre appareil périphérique par exemple ne peut bénéficier de l'initialisation du point d'accès réalisé pour un périphérique précédent, sauf à connaître bien entendu la valeur exacte, à la valeur de tolérance près, de la durée d'initialisation déjà exécutée.

Un mode de mise en œuvre préférentiel non limitatif du procédé de contrôle de connexion d'un périphérique à un point d'accès AP sera maintenant donné en liaison avec la figure 2.

D'une manière générale, on indique que l'étape B de la figure 1, relative à l'initialisation simultanée du point d'accès AP et d'un périphérique T peut comprendre en conséquence l'exécution de la commande locale par l'utilisateur à l'étape B_0, commande locale exécutée sur le point d'accès AP et sur le périphérique T pour enregistrer localement les durées d'initialisation T_{ap} respectivement T_T.

L'étape d'initialisation simultanée B_0 peut alors être suivie d'une étape B_1 d'appairage provisoire du point d'accès AP et du périphérique T. L'étape d'appairage provisoire précitée peut être mise en œuvre avantageusement par réduction de la portée en émission/réception du point d'accès AP par exemple. Cette technique sera décrite plus en détail ultérieurement dans la description en liaison avec un point d'accès conforme à l'objet de la présente invention.

L'étape C de la figure 1 consistant en l'étape de transmission C_0 et de comparaison C_1 précédemment décrite en liaison avec la figure précitée peut, dans un mode de mise en œuvre préférentiel non limitatif, être exécutée de façon que la transmission entre le point d'accès AP et le périphérique T de la valeur de la durée

d'initialisation mesurée localement et mémorisée est réciproque entre le point d'accès AP et le périphérique T.

Cette opération est alors représentée à l'étape C_{0I} de la figure 2 par les relations :

Transmission $T \xrightarrow{T_T} AP(T_{Tr})$

Transmission $AP \xrightarrow{T_{ap}} T(T_{apr})$

L'opération de transmission du périphérique T vers le point d'accès AP respectivement du point d'accès AP vers le périphérique T des valeurs de durée d'initialisation précitées peut avantageusement être exécutée par transmission d'un message de valeur comportant au moins la valeur de la durée d'initialisation mémorisée et par exemple l'identifiant au niveau lien de l'émetteur de ce message et d'un message d'acquittement, le message d'acquittement comportant au moins une référence au message de valeur. Le processus de transmission des messages précité sera décrit ultérieurement dans la description.

A l'étape C_I représentée en figure 2, on rappelle que :

- T_T désigne la valeur de la durée d'initialisation du périphérique T mesurée localement au niveau de ce périphérique ;
- T_{Tr} désigne la valeur de la durée d'initialisation du périphérique T transmise et reçue au niveau du point d'accès AP ;
- T_{ap} désigne la valeur de durée d'initialisation du point d'accès AP mesurée localement au niveau de ce dernier ;
- T_{apr} désigne la durée de la valeur d'initialisation du point d'accès AP transmise au périphérique T et reçue par ce dernier.

Dans ces conditions, l'autorisation de poursuite de la connexion est alors rendue avantageusement conditionnelle à l'identification mutuelle du périphérique demandeur d'accès identifié respectivement du point d'accès simultanément initialisé pour ce périphérique demandeur d'accès.

Dans ce but, une comparaison d'égalité de la valeur de la durée d'initialisation mémorisée localement et de la valeur de la durée d'initialisation

transmise est alors exécutée d'une part au niveau du point d'accès AP à l'étape C_{11} de la figure 2 et, d'autre part, au niveau du périphérique T à l'étape C_{12} de la même figure 2.

Les tests exécutés aux étapes C_{11} et C_{12} par comparaison d'égalité vérifient respectivement les relations :

$T_{Tr} = T_{ap} \pm E$

$T_{apr} = T_T \pm D$

Les valeurs de tolérance d'erreur E et D peuvent être différentes.

Sur réponse positive à l'étape C_{11} précitée et sur réponse positive à l'étape C_{12} précitée, c'est-à-dire lorsque la comparaison d'égalité de la valeur de la durée d'initialisation mémorisée localement T_{ap} respectivement T_T et de la valeur de la durée d'initialisation transmise, c'est-à-dire T_{Tr} respectivement T_{apr} sont satisfaits, alors le procédé de contrôle d'une connexion, objet de l'invention, est alors poursuivi par l'étape D de la figure 1 dans les conditions qui seront décrites ci-après.

Si au contraire, l'une des étapes de comparaison C_{11} ou C_{12} n'est pas satisfaite, c'est-à-dire sur réponse négative à l'une de ces deux étapes, alors une procédure de fin de connexion C_{13}, respectivement C_{14} est appelée, la poursuite de la connexion étant alors inhibée. Un mode de mise en œuvre spécifique de l'étape B d'appairage permanent de la figure 1 sera maintenant décrit en liaison avec la figure 2.

D'une manière générale, l'étape D précitée peut consister en une étape D_0 d'initialisation de l'appairage permanent. En effet, de manière avantageuse, l'étape consistant à autoriser la poursuite de la connexion du périphérique peut être rendue conditionnelle à l'absence, préalablement à l'appel de la procédure d'appairage permanent proprement dite, d'une nouvelle étape de pré-initialisation et/ou d'une étape d'initialisation simultanée entre le point d'accès AP déjà configuré pour un appairage provisoire et au moins un autre périphérique. Cette opération est représentée par l'étape D1 de la figure 2, notée $\exists$ T'_T visant à vérifier soit une tentative de connexion d'un autre périphérique à partir d'une durée quelconque différente de la durée d'initialisation du périphérique ayant initialisé le point d'accès

AP, cette opération étant représentée sur la figure 2 par une étape D_2 de fin de connexion sur existence d'une valeur T'_T différente de T_T.

De même l'étape consistant à autoriser la procédure de la connexion du périphérique peut comporter avantageusement un critère de rejet de toute nouvelle demande de connexion étrangère à une demande de connexion existante pour un périphérique demandeur de connexion identifiée.

Cette situation peut correspondre par exemple au cas où un premier périphérique ayant exécuté les opérations de pré-initialisation du point d'accès AP puis d'initialisation simultanée de ce périphérique et de ce point d'accès à un périphérique tiers disposant de la valeur de durée d'initialisation de ce périphérique, tente à nouveau de lancer une procédure d'initialisation simultanée à partir de la même durée d'initialisation.

L'existence d'une valeur T'_T égale ou non à T_T dans cette situation, c'est-à-dire en réponse positive au test D_1 de la figure 2, amène également à la fin de connexion de l'étape D_2 de la figure 2.

Au contraire, sur réponse négative au test D_1 de la figure 2, la poursuite de la connexion du périphérique considéré est exécutée par une étape D_3 désignée suite d'appairage permanent.

Ainsi que représenté sur la figure 2, l'étape D_3 peut comprendre préalablement à l'étape d'appel une procédure D_{30} de configuration d'appairage permanent au niveau du point d'accès, une étape D_{31} de chiffrement de paramètres descriptifs de configuration d'appairage permanent suivie d'une étape D_{31} de transmission des paramètres descriptifs de configuration d'appairage permanent chiffrés, du point d'accès AP vers le périphérique T appairé provisoirement.

Pour la mise en œuvre de l'étape de chiffrement D_{31}, le point d'accès AP est en mesure de collecter par le signal de liaison à courte portée par exemple toute clé de chiffrement envoyée par le périphérique T, lequel a bien entendu été identifié simultanément par exemple aux étapes C_{11} et C_{12}.

Pour ce qui concerne la mise en œuvre de l'étape D_1 de la figure 2, on indique que celle-ci peut être exécutée de la manière ci-après de manière avantageuse :

– Lors de l'étape de pré-initialisation du point d'accès AP, la commande locale exercée pour exécuter cette pré-initialisation peut permettre, outre la mise en configuration de ce dernier pour pouvoir appairer provisoirement un périphérique, de déclencher par exemple un compteur de temps pré-configuré de durée P_1 par exemple. Ce compteur de temps peut permettre de limiter dans le temps, au niveau du point d'accès AP, les étapes d'initialisation simultanées du périphérique T et du point d'accès AP puis d'appairage provisoire et finalement d'initialisation d'appairage permanent.

– De même lors de l'initialisation simultanée du périphérique T et du point d'accès AP par l'utilisateur par exécution d'une commande locale au niveau de chacun de ces derniers, la fin de la commande locale au niveau du périphérique T peut avantageusement déclencher un compteur de temps pré-configuré de valeur P_2 ayant pour objet de limiter dans le temps au niveau du périphérique T les opérations d'appairage et d'échange simultané par exemple des valeurs de temps écrites aux étapes B_1 et C_{01} de la figure 2.

On comprend ainsi que lorsque le point d'accès AP et le périphérique T se sont identifiés mutuellement par exemple ainsi que représenté aux étapes C_{01}, C_{11}, C_{12} de la figure 2, si, durant la période de compteur de temps P_1, le point d'accès AP a reçu plusieurs valeurs de durée d'initialisation de périphérique T_{Tr} ou si durant la deuxième période de compteur de temps P_2 le périphérique a reçu plusieurs valeurs de durée d'initialisation de point d'accès T_{apr} alors la procédure d'appairage se termine par un échec tel que représenté au test D_1 de la figure 2 décrit précédemment dans la description.

On comprend ainsi que le test D_1 précité permet bien de prévenir le cas de connexion d'un deuxième utilisateur malveillant qui essayerait d'appairer son périphérique sur le point d'accès AP considéré mais que ce mode opératoire permet

également de prévenir le cas d'un deuxième utilisateur qui essaierait de détourner la connexion du périphérique vers son propre point d'accès.

Une description plus détaillée d'un point d'accès en réseau partagé par un périphérique, point d'accès AP conforme à l'objet de la présente invention, sera maintenant donnée en liaison avec les figures 3a à 3d.

D'une manière générale, on indique que le point d'accès AP objet de l'invention, sera décrit pour un point d'accès en réseau partagé par liaison radio de manière non limitative, le point d'accès objet de l'invention, pouvant être mis en œuvre également dans d'autres technologies, telles que les courants porteurs de ligne sur réseau de distribution basse tension ou autre.

En conséquence, en référence à la figure 3a on indique que le point d'accès AP objet de l'invention, comporte au moins une interface de signal de liaison, dans le cas particulier de la figure 3a une interface radio portant la référence 1_0, et une interface logicielle de gestion d'interface de signal de liaison portant la référence 1_1 laquelle constitue, dans ce cas, une interface logicielle d'interface radio. L'interface de gestion de signal de liaison ou d'interface radio contient des éléments de programme informatique permettant de commuter les trames de l'interface radio précitée vers une autre interface radio ou vers une interface réseau.

Ainsi qu'on l'observera en outre sur la figure 3a, le point d'accès AP objet de l'invention, comporte également un module d'appairage point d'accès/périphérique portant la référence 1_2 relié à l'interface logicielle de gestion d'interface de signal de liaison 1_1. L'infrastructure ou interface logicielle 1_1 précitée permet en outre de remonter vers le module d'appairage point d'accès/périphérique 1_2 des informations déterminées ou d'inclure dans des trames radio, par exemple, des informations envoyées par le module d'appairage point d'accès/périphérique 1_2. L'interface logicielle 1_1 permet bien entendu d'assurer la gestion des messages de valeur de durée précédemment mentionnés dans la description, afin d'assurer la transmission de ces derniers vers le point d'accès AP, respectivement le périphérique T, ainsi que mentionné précédemment dans la description.

En outre, le point d'accès AP objet de l'invention, comporte une base de données 1_3 reliée au module d'appairage point d'accès/périphérique 1_2, cette base de données comportant d'une part des données temporaires et d'autre part des données permanentes.

La base de données 1_2 est structurée de façon qu'une partie de la base de données précitée soit volatile et permet au module d'appairage point d'accès/périphérique 1_2 de stocker et d'extraire des informations dont la nature est temporaire, tels que des identifiants de périphérique T candidats à une connexion par exemple, alors qu'une deuxième partie de la base de données 1_3 est non volatile et contient par exemple des fichiers de configuration relatifs au module d'appairage points d'accès/périphérique 1_2. Ces éléments de configuration sont des éléments de configuration radio lorsque le signal de liaison est un signal radio ou des éléments de configuration par courant porteur de ligne lorsque le signal de liaison est un signal par courant porteur de ligne.

En outre, le point d'accès AP comprend un circuit de pré-initialisation du point d'accès AP par l'intermédiaire d'une commande locale de ce point d'accès ce circuit de pré-initialisation portant la référence 1_4 sur la figure 3a.

En référence au procédé de contrôle de connexion objet de l'invention décrit précédemment dans la description, on indique que la pré-initialisation engendrée grâce au circuit d'initialisation 1_4 permet au moins de configurer le point d'accès AP pour appairer provisoirement un périphérique à ce dernier.

Le point d'accès AP comporte en outre un circuit d'initialisation lequel de manière avantageuse peut être constitué par le circuit de pré-initialisation 1_4 précédemment mentionné. Le circuit de pré-initialisation et d'initialisation 1_4 permet d'engendrer une commande locale de pré-initialisation respectivement d'initialisation du point d'accès AP, cette commande étant directement transmise au module d'appairage point d'accès/périphérique 1_2.

D'une manière générale, le module d'appairage point d'accès/périphérique 1_2 précité permet bien entendu la mise en œuvre du procédé objet de l'invention, et en particulier des étapes dévolues au point d'accès AP, telles que la mesure locale et la

mémorisation de la durée d'initialisation du point d'accès AP par la commande locale exécutée par l'intermédiaire du circuit d'initialisation 1_4, puis, suite à l'appairage provisoire du point d'accès AP et d'un périphérique T, de recevoir au moins du périphérique T précité une valeur de durée d'initialisation mémorisée engendrée par une commande locale d'initialisation et de comparer par comparaison d'égalité, la valeur de la durée d'initialisation mesurée localement, c'est-à-dire la durée d'initialisation T_{ap} décrite précédemment dans la description, à la valeur de la durée d'initialisation mesurée reçue, c'est-à-dire la durée T_{Tr} mesurée par le périphérique T. Enfin, le module d'appairage permet de conduire les décisions liées à la comparaison précitée. En particulier, si la durée d'initialisation mesurée reçue T_{Tr} est sensiblement égale à la durée d'initialisation mesurée localement T_{ap} et qu'elle est reçue de manière unique, le périphérique est alors reconnu comme périphérique demandeur de connexion identifié et la poursuite de la connexion du périphérique T est autorisée, par appel d'une procédure d'appairage permanent. Sinon, la poursuite de la connexion est inhibée au niveau du point d'accès AP.

En ce qui concerne le circuit de pré-initialisation et/ou d'initialisation 1_4 représenté en figure 3a, on indique que ce dernier peut être constitué par tout élément actionneur permettant d'engendrer un signal de commande locale d'initialisation au niveau du point d'accès AP.

En particulier, il peut être constitué par un circuit récepteur d'un signal engendré par un appareil de sélection de commande de télévision par exemple par commande infrarouge ou autre.

Dans un mode de mise en œuvre particulier non limitatif on indique que le circuit de pré-initialisation du point d'accès AP et le circuit d'initialisation constitué par le même circuit 1_4 sur la figure 3a du point d'accès AP sont avantageusement constitués par un bouton poussoir ou bouton de commande unique disposé sur le châssis du point d'accès AP.

On comprend, en particulier, que dans le cadre d'une utilisation domestique d'un point d'accès AP constitutif d'une passerelle d'accès en réseau partagé par un réseau WIFI par exemple, l'utilisateur domestique est alors amené à simplement

exercer un appui-relâchement pour étape de pré-initialisation du point d'accès AP puis un appui de durée déterminée, laissée à la seule initiative de l'utilisateur, et un relâchement de ce même bouton poussoir pour exécuter l'étape d'initialisation du point d'accès AP.

Enfin, dans un mode de mise en œuvre préférentiel non limitatif du point d'accès AP objet de l'invention, ce dernier peut comporter avantageusement, outre l'interface radio habituelle 1_0, cette interface radio pouvant être constituée par une interface radio à longue portée telle qu'une interface WIFI par exemple, une deuxième interface radio à courte portée portant la référence 1_5 sur la figure 3a.

L'interface radio courte portée peut être constituée avantageusement par une interface infrarouge, une interface Bluetooth ou autre dont les conditions de diagramme d'émission/réception peuvent alors être adaptées ainsi qu'il sera décrit ultérieurement dans la description.

On comprend, en particulier, que l'interface radio à longue portée et l'interface radio à courte portée peuvent alors être commutées pour la mise en œuvre du processus de contrôle de connexion conforme au procédé objet de la présente invention par l'intermédiaire du module d'appairage point d'accès/périphérique 1_2 représenté en figure 3a, pour assurer un appairage temporaire en liaison radio à courte portée, respectivement un appairage permanent en liaison radio en longue portée avec le périphérique T.

Le mode opératoire précité permet alors de sécuriser le processus de connexion par un contrôle effectif non seulement de l'identification du requérant de la connexion mais également par réduction de la portée des transactions, c'est-à-dire des échanges de message entre le point d'accès AP et le périphérique T demandeur de connection, pendant toute la durée du contrôle de la connexion.

Une description fonctionnelle du module d'appairage point d'accès/périphérique 1_2 intégré au point d'accès AP, objet de l'invention, décrit en figure 3a sera maintenant donnée en liaison avec la figure 3b.

D'une manière générale, on indique que le module d'appairage point d'accès/périphérique 1_2 est un module constitué par un programme informatique subdivisé le cas échéant en sous-modules.

De manière plus spécifique en référence à la figure 3b on indique que le module d'appairage point d'accès/périphérique 1_2 réunit un ensemble de fonctions, lesquelles sont supervisées par un organe de gestion non représenté en figure 3b. Cet organe de gestion permet d'articuler l'ensemble des fonctions précitées, c'est-à-dire de lancer les différentes fonctions au moment voulu et en particulier dans le cadre de la phase de pré-initialisation puis d'initialisation du point d'accès AP considéré.

Le module d'appairage point d'accès/périphérique 1_2 comprend les modules ci-après :

- module 1_{2a} de stockage/extraction de la base de données. Cette fonction permet aux différentes fonctions constitutives du module d'appairage 1_2 de stocker ou d'extraire de la base de données 1_3 des données telles que des identifiants de niveau 2 de périphérique ou des variables relatives à ces derniers ;
- module 1_{2b} Supervision/bouton-poussoir. Cette fonction permet de mesurer en particulier le temps d'appui, c'est-à-dire la durée d'initialisation T_{ap} exécuté par l'utilisateur du point d'accès AP sur le bouton-poussoir, c'est-à-dire la durée de la commande locale d'initialisation du point d'accès AP. La fonction précitée est en relation avec la fonction Stockage/extraction de la base de données 1_{2a} pour stocker le temps d'appui T_{ap}. Elle est également en relation avec une fonction 1_{2c} de gestion de connexion courte portée afin de paramétrer l'interface radio dès le relâchement du bouton poussoir dans le cadre de la phase de pré-initialisation pour le support d'une connexion courte portée. La fonction Supervision/bouton-poussoir est en outre en relation avec une fonction Envoi/réception de données radio 1_{2d} afin de transmettre au périphérique T par l'intermédiaire de la voie radio en mode courte portée pendant l'appairage provisoire le temps d'appui, c'est-à-dire la durée d'initialisation T_{ap} du point d'accès AP. Enfin, la fonction Supervision/bouton-poussoir 1_{2b} permet de déclencher le compteur de temps P_1 précédemment mentionné

dans la description et servant à protéger le point d'accès AP contre toute tentative d'un utilisateur indélicat ainsi que mentionné précédemment dans la description ;

– module Gestion connexion courte portée 1_{2c}. Cette fonction permet d'instaurer un dialogue avec l'infrastructure logicielle de gestion de l'interface du signal de liaison, c'est-à-dire avec l'interface logicielle 1_1 représentée en figure 3a, afin de paramétrer l'interface de signal de liaison en mode courte portée. Le paramétrage précité varie en fonction de la technologie radio utilisée. Pour une technologie de type IEEE 802.11, ce paramétrage consiste à activer un nom de réseau additionnel, tel que par exemple "Appairage", à fixer une modulation radio haute par exemple à 54 Mb/s et, optionnellement, à baisser la puissance radio d'émission et de réception de l'interface radio à courte portée ;

– module Envoi/réception de données radio 1_{2d}. Cette fonction envoie ou reçoit des données vers l'infrastructure logicielle 1_1 représentée en figure 3a ;

– module Identification périphérique 1_{2e}. Cette fonction est responsable de l'identification du périphérique T demandeur de connexion. Elle assure, en particulier, la réception du temps d'appui du point d'accès, c'est-à-dire la valeur d'initialisation locale T_{ap} du point d'accès AP, provenant de la fonction Supervision bouton-poussoir 1_{2b} d'une part, et le temps d'appui périphérique T_{Tr} valeur de la durée d'initialisation du périphérique T provenant de la fonction Envoi/réception de données radio 1_{2d}, d'autre part. La fonction Identification périphérique précitée dispose également du taux d'erreur E provenant de la fonction Stockage/extraction de la base de données 1_{2a}. A partir de ces données, la fonction Identification périphérique 1_{2e} est en mesure d'identifier le périphérique et permet alors de stocker dans la base de données 1_3 de la figure 3a, le résultat de cette identification. De plus, si le résultat de la comparaison est positif, un identifiant du périphérique T, tel que l'identifiant ou adresse au niveau lien de ce dernier, est également stocké.

Le cas échéant, la fonction précitée permet également de stocker dans la base de données 1_3 la valeur d'une variable Ch si cette dernière a été transmise par le périphérique T. On précise que la variable Ch précitée indique à quel type

d'application le périphérique T accèdera, une fois connecté, au point d'accès AP ou le type lui-même du périphérique ;

– module Analyse des clés 1_{2f}. Cette fonction collecte les clés de chiffrement provenant de la fonction Envoi/réception données radio 1_{2d} puis elle les analyse ainsi qu'il sera décrit ultérieurement dans la description. Si une seule clé de chiffrement est reçue d'un périphérique T identifié, cette clé est stockée dans la base de données 1_3 par l'intermédiaire de la fonction Stockage/extraction de la base de données 1_{2a} ;

– module Choix éléments de configuration 1_{2g}. Cette fonction permet d'extraire de la base de données 1_3, les éléments de configuration et la variable Ch envoyée optionnellement par le périphérique T. Les éléments de configuration permettent alors au périphérique T d'établir une connexion radio longue portée sécurisée par appairage permanent. La notion d'appairage permanent recouvre, bien entendu, la liaison sécurisée précitée à laquelle il est mis fin de la seule volonté de l'utilisateur. La fonction précitée sélectionne optionnellement les éléments de configuration à envoyer au périphérique T en fonction de la valeur de la variable Ch précitée ;

– module Chiffrement 1_{2h}. Cette fonction collecte, d'une part, par l'intermédiaire de la fonction Stockage/extraction de la base de données 1_{2a} la clé qui permet de chiffrer le message radio pour un périphérique donné et, d'autre, part, par l'intermédiaire de la fonction Choix éléments de configuration 1_{2g}, les éléments de configuration à transmettre au périphérique T. La fonction Chiffrement 1_{2h} précitée envoie ses données à la fonction Envoi/réception de données radio 1_{2d} pour transmission chiffrée des éléments de configuration au périphérique T ;

– module Gestion connexion longue portée 1_{2i}. Lorsque l'ensemble de la procédure d'identification est terminée, c'est-à-dire conformément au procédé objet de la présente invention telle que représentée en figure 1 par exemple, soit après appel et exécution de l'appairage permanent D et en particulier, d'exécution des étapes D_{30}, D_{31} et D_{32} de la figure 2, la fonction précitée est alors chargée de préparer la connexion longue portée du périphérique T. Dans ce but, elle agit en concertation

avec l'infrastructure logicielle de gestion des interfaces radio 1_1 de la figure 3a.

En référence à la figure 3b, on indique que les différents modules référencés à cette figure peuvent être implémentés sous forme de modules logiciels dont les interactions sont représentées sur la figure 3b précitée. Les modules précités sont alors constitués par des modules de produit de programme correspondants ou, le cas échéant, par un produit de programme unique par exemple.

Une description plus détaillée d'un protocole de contrôle d'une connexion demandée par un périphérique, tel que conduit par le module d'appairage point d'accès/périphérique 1_2 dans la phase de pré-initialisation de ce dernier, sera maintenant donnée en liaison avec la figure 3c.

Pour procéder à la pré-initialisation du point d'accès AP, un utilisateur exerce un appui sur le bouton-poussoir 1_4 de la figure 3a. Il peut bien entendu lancer la commande locale correspondante par tout moyen équivalent à ce bouton-poussoir. Cette étape est représentée à l'étape S_{ap01} de la figure 3c.

Dès le relâchement de l'opération de lancement de la commande de pré-initialisation précitée, c'est-à-dire dès le relâchement du bouton-poussoir 1_4 par exemple, une étape de configuration du point d'accès AP pour appairage provisoire est alors exécutée, cette étape étant référencée S_{ap02} sur la figure 3c. En outre, le relâchement du bouton-poussoir 1_4 provoque le démarrage du compteur de temps de valeur P_1 lequel a pour objet de limiter toute tentative de nouvelle réinitialisation ainsi que décrit précédemment dans la description.

Une description plus détaillée des étapes essentielles d'un protocole de contrôle de connexion demandé par un périphérique conduit par le module d'appairage point d'accès/périphérique 1_2 représenté en figure 3a, dans la phase d'initialisation de ce dernier sera maintenant donnée en liaison avec la figure 3d.

L'étape de pré-initialisation ayant été exécutée par l'utilisateur, ce dernier est ensuite amené à exécuter l'étape d'initialisation du point d'accès AP conjointement avec le périphérique T qu'il souhaite connecter.

L'étape d'initialisation et le déclenchement de la procédure d'identification sont alors engagés par une étape S_{ap1} déclenchée par un appui et un relâchement du

bouton de commande, bouton-poussoir 1_4 de la figure 3a, situé sur le point d'accès AP. Le temps d'appui sur le bouton-poussoir du point d'accès, c'est-à-dire la durée d'initialisation T_{ap} du point d'accès AP est comptabilisée par la fonction Supervision du bouton-poussoir 1_{2b}, représenté sur la figure 3b.

La valeur de cette durée est mémorisée à l'étape S_{ap2} par la fonction Stockage/extraction de la base de données 1_{2a} de la figure 3b.

Le module appairage point d'accès/périphérique 1_4 reçoit ensuite l'appairage du périphérique T sur le réseau radio ouvert temporairement pendant l'appairage provisoire, lors de la pré-initialisation du point d'accès AP décrit en figure 3c. L'appairage provisoire précité peut avantageusement de manière optionnelle être exécuté à travers la liaison courte portée mise en place suite au premier appui de l'utilisateur sur le bouton-poussoir 1_4, lors de l'exécution de l'étape de pré-initialisation. A titre d'exemple non limitatif, le réseau d'accès, dans ce cas, est un réseau de type IEEE 802.11 dont la portée est alors réduite en forçant le point d'accès à dialoguer avec un taux de modulation radio choisi le plus haut possible selon les possibilités radio du périphérique à 54Mb/s. A titre d'exemple la puissance d'émission et de réception radio dans cette situation est choisie par exemple égale à 1 milliwatt. Une modulation radio très haute combinée à une puissance d'émission/réception très basse, ainsi que décrit précédemment, permet de limiter l'écoute malveillante et l'espionnage des échanges radio. La portée restreinte du point d'accès AP dans cette situation permet en fait d'augmenter la sécurité et tous les messages radio suivants, jusqu'à l'étape finale précédant la mise en place de la liaison radio longue portée sont échangés grâce à la liaison radio courte portée.

Lorsque le processus de reconnaissance mutuel entre le point d'accès AP et le terminal T est mis en œuvre, ainsi que décrit précédemment dans la description en liaison avec la figure 2, alors en une étape S_{ap4} le module d'appairage point d'accès/terminal envoie par l'intermédiaire de la fonction Envoi/réception de données radio 1_{2d}, sur la liaison radio courte portée, la valeur de la durée d'initialisation du point d'accès, valeur T_{ap}, ainsi que de préférence son identifiant au niveau lien, c'est-à-dire son adresse MAC. L'envoi de cette variable peut optionnellement être exécutée

à travers un tunnel sécurisé. La variable de durée précitée T_{ap} et l'identifiant de niveau lien peuvent alors être envoyés dans un message de valeur tel que décrit précédemment dans la description par exemple.

A l'étape S_{ap5} le module d'appairage point d'accès/périphérique attend ensuite la réception de la valeur de durée d'initialisation du périphérique demandeur de connexion c'est-à-dire la durée T_T. En l'absence de réception de cette valeur de durée au bout d'une durée P_1 déclenchée par le compteur de temps précédemment mentionné dans la description, la procédure d'appairage se termine sur un échec. Cette situation est représentée par la branche NON de réponse au test S_{ap5} et de retour vers une situation de fin de connexion. De même, sur réception de plusieurs valeurs de durée d'initialisation de périphérique T_T au bout de la durée de compteur de temps P_1 ainsi que mentionné précédemment dans la description, la procédure d'appairage se termine également par un échec et un retour en fin de connexion.

Au contraire, sur réponse positive au test S_{ap5} la valeur d'initialisation du périphérique T_{Tr} étant reçue, la fonction Envoi/réception de données radio 1_{2d} transmet à la fonction Identification périphérique 1_{2e} la variable de durée d'initialisation T_{Tr} précitée. La fonction Identification périphérique 1_{2e} va alors appeler dans la base de données 1_3 la variable d'erreur E et procède à la vérification d'égalité permettant de vérifier l'identification réussie.

Si la relation de comparaison d'égalité est vérifiée ainsi que mentionné précédemment dans la description, la procédure se poursuit en réponse positive au test S_{ap6}. Sinon en l'absence de comparaison réussie et de vérification d'identité, la procédure d'appairage se termine par un échec par un retour à l'étape de fin de connexion.

L'étape de comparaison précédente étant vérifiée à la valeur vraie, la fonction Identification périphérique 1_{2e} permet à l'étape suivante S_{ap7} de stocker dans la base de données 1_3 l'identifiant au niveau lien du périphérique T. Le périphérique T est alors considéré comme reconnu et identifié comme périphérique ayant demandé la connexion, de la volonté même de l'utilisateur de ce dernier.

Lors de la transmission de la valeur de durée d'initialisation du périphérique valeur T_T et en présence de la variable Ch, mentionnée précédemment dans la description, cette variable, laquelle peut en outre indiquer le type de périphérique T concerné audiovisuel ou autre, est également consignée dans la base de données 1_3 avec l'identifiant au niveau lien du périphérique considéré.

L'étape suivante, étape S_{ap8} est une étape préconfigurée en temps au cours de laquelle le point d'accès AP collecte, par voie radio, les clés de chiffrement c'est-à-dire les clés publiques RSA qui vont permettre de chiffrer les données de configuration transmises au périphérique T candidat à la connexion.

L'étape suivante S_{ap9}, après écoulement du temps préconfiguré précité, consiste à transmettre, par l'intermédiaire de la fonction Envoi/réception de données radio 1_{2d} à la fonction d'analyse des clés 1_{2f}, la clé publique précitée. La fonction Analyse des clés procède alors à une analyse des clés transmises selon les règles suivantes :

a) les clés de chiffrement reçues d'un périphérique non identifié lors de l'étape S_{ap6} sont ignorées ;

b) si au moins deux clés de chiffrement sont reçues d'un périphérique identifié lors de l'étape S_{ap6}, alors les clés de chiffrement sont ignorées et la procédure d'appairage se termine sur un échec. Cette situation est représentée par la branche de réponse négative au test S_{ap9} de la figure 3d ;

c) si une seule clé de chiffrement est reçue d'un périphérique identifié lors de l'étape S_{ap6}, alors la clé de chiffrement est conservée et utilisée lors de l'étape suivante, notée S_{ap10}. Cette situation est représentée sur la figure 3d par la réponse positive au test de l'étape S_{ap9} ;

d) si aucune clé de chiffrement n'est reçue du périphérique identifié, la procédure d'appairage se termine alors sur un échec représenté par la réponse négative au test de l'étape S_{ap9}.

L'étape suivante S_{ap10} est celle dans laquelle la fonction Choix éléments de configuration 1_{2g} de la figure 3b permet de rechercher dans la base de données 1_3 les éléments de configuration possibles, l'identifiant du périphérique T et, lorsque cette

dernière est présente, la variable Ch. La variable précitée peut optionnellement permettre de discriminer les éléments de configuration à envoyer au périphérique identifié parmi l'ensemble des éléments de configuration possible. Le point d'accès AP utilise la clé de chiffrement reçue à l'étape S_{ap9} et l'algorithme de chiffrement associé à celle-ci pour chiffrer les informations de configuration et les envoyer au périphérique T candidat à la connexion.

L'étape S_{ap10} est alors suivie d'une étape S_{ap11} dans laquelle à partir des éléments de configuration choisis et communiqués par la fonction Choix éléments de configuration 1_{2g} à la fonction Gestion de connexion longue portée 1_{2i} cette dernière permet la mise en place de la configuration radio nécessaire à l'appairage longue portée, c'est-à-dire à l'appairage permanent du périphérique T. Cette opération peut être exécutée par exemple par la mise en place d'un nouveau nom de réseau ou d'une nouvelle clé de sécurité ou encore par vérification de la configuration déjà en place. La fonction Gestion de connexion courte portée 1_{2i} permet alors de désinstaller la configuration mise en place et notamment de désactiver le réseau radio temporaire pendant l'appairage provisoire créé lors du premier appui sur le bouton-poussoir 1_4 du point d'accès AP lors de l'étape de pré-initialisation de ce dernier.

Une description plus détaillée d'un périphérique connectable à un point d'accès en réseau partagé, conforme à l'objet de l'invention, sera maintenant donnée en liaison avec les figures 4a à 4c.

De même que dans le cas d'un point d'accès AP précédemment décrit, le périphérique objet de l'invention, sera décrit dans le cas de l'utilisation d'un signal de liaison constitué par un signal radio de manière non limitative.

En référence à la figure 4a, le périphérique sécurisé connectable à un point d'accès en réseau partagé, objet de l'invention, comporte une interface de signal de liaison 2_0 laquelle est constituée par une interface radio longue portée par exemple. Il comporte en outre une interface logicielle de gestion d'interface de signal de liaison 2_1 laquelle est constituée par une infrastructure logicielle de gestion de l'interface radio 2_0 précitée.

Le périphérique objet de l'invention, comporte en outre, ainsi que représenté sur la figure 4a, un module d'appairage périphérique/point d'accès 2_2 relié à l'interface logicielle de gestion d'interface de signal de liaison 2_1 et une base de données 2_3 reliée au module d'appairage périphérique/point d'accès 2_2. Selon une structure comparable à la base de données du point d'accès AP objet de l'invention, telle que décrite précédemment en liaison avec la figure 3a, la base de données 2_3 peut comporter avantageusement d'une part des données temporaires et, d'autre part, des données permanentes ainsi qu'il sera décrit ci-après.

En outre, et selon un aspect remarquable du périphérique connectable à un point d'accès en réseau partagé objet de l'invention, ce dernier comporte un circuit 2_4 d'initialisation du périphérique par une commande locale de ce périphérique.

Bien entendu, la notion de commande locale correspond à la notion d'une commande exercée localement sur le périphérique à la seule initiative de l'utilisateur demandeur d'une connexion pour ce périphérique.

De manière remarquable, le module d'appairage périphérique/point d'accès 2_2 intégré au périphérique objet de l'invention, permet de mesurer localement et de mémoriser la durée d'initialisation du périphérique par la commande locale puis, suite à un appairage provisoire de ce périphérique et d'un point d'accès AP tel que décrit précédemment dans la description, de recevoir au moins de ce point d'accès une valeur de la durée d'initialisation mémorisée de ce point d'accès par une commande locale d'initialisation et de comparer par comparaison d'égalité la valeur de la durée d'initialisation mesurée reçue correspondant à la valeur de la variable T_{apr} précédemment décrite dans la description. Si la durée d'initialisation mesurée reçue T_{apr} est sensiblement égale à la durée d'initialisation mesurée localement du périphérique la durée T_T alors le point d'accès AP est reconnu comme point d'accès initialisé pour le périphérique demandeur d'accès, ceci par la volonté exprimée de l'utilisateur du point d'accès AP et du périphérique T considéré. Le module d'appairage périphérique/point d'accès 2_2 permet alors d'autoriser la poursuite de la connexion du périphérique T demandeur de connexion par appel d'une procédure d'appairage permanent ainsi que décrit précédemment. Sinon, le module d'appairage

périphérique/point d'accès 2_2 permet d'inhiber au niveau du périphérique T la poursuite de la connexion.

D'une manière plus spécifique, on indique relativement au périphérique sécurisé, objet de la présente invention telle que représentée en figure 4a, que l'interface logicielle de gestion d'interface radio 2_1 constitutive de l'infrastructure logicielle précitée contient les éléments de programme informatique permettant d'envoyer et recevoir des trames d'une interface radio. Elle permet également de remonter vers le module d'appairage périphérique/point d'accès 2_2 des informations déterminées ou d'inclure dans les trames radio des informations envoyées par le module d'appairage périphérique précité. Bien entendu, l'interface logicielle ou infrastructure logicielle 2_1 permet d'assurer la gestion des messages radio tels que définis précédemment dans la description relativement à la mise en œuvre du procédé objet de la présente invention.

La base de données 2_3 est structurée de façon qu'une partie de la base de données est volatile et permet au module d'appairage périphérique/point d'accès 2_2 de stocker et d'extraire des informations dont la nature est temporaire, telles que les identifiants du point d'accès AP, et une deuxième partie non volatile contenant des informations de configuration relatives au module d'appairage périphérique/point d'accès, telles que nom de réseau prédéfini dans le cas de réseaux du type IEEE 802.11 par exemple.

En outre, en référence à la figure 4a, on indique que le circuit 2_4 d'initialisation peut être constitué par tout circuit récepteur de signal de télécommande, par exemple à partir d'une télécommande quelconque, de manière semblable au circuit d'initialisation du point d'accès AP. Toutefois, dans un mode de mise en œuvre préférentiel, le circuit d'initialisation 2_4 est avantageusement constitué par un bouton de commande disposé sur le châssis du périphérique T.

Enfin, en référence à la même figure 4a, on indique que le périphérique T, objet de l'invention, outre la première interface radio 2_0 constituant une interface de signal de liaison à longue portée comporte avantageusement une deuxième interface de signal de liaison 2_5 à courte portée. La première interface radio 2_0 et la deuxième

interface de radio 2_5 peuvent alors, selon une caractéristique avantageuse du périphérique objet de la présente invention, être commutés à l'initiative du module d'appairage périphérique/point d'accès 2_2 pour assurer l'étape d'appairage provisoire en liaison en courte portée respectivement un appairage permanent en liaison en longue portée avec le point d'accès, conformément au procédé objet de la présente invention. Un tel mode opératoire du périphérique T objet de la présente invention sera décrit ultérieurement dans la description.

En ce qui concerne le module d'appairage périphérique/point d'accès 2_2 on indique que ce dernier est essentiellement de nature logicielle. Les fonctions mises en œuvre par le module précité seront maintenant décrites en liaison avec la figure 4b, laquelle représente un schéma fonctionnel de ce dernier.

L'ensemble des fonctions mises en œuvre par le module d'appairage périphérique/point d'accès 2_2 sont avantageusement supervisées par un organe de gestion non représenté en figure 4b, lequel permet d'articuler l'ensemble des fonctions précitées, c'est-à-dire de lancer les fonctions selon un protocole défini, lequel sera décrit ultérieurement en liaison avec la figure 4c.

Le module d'appairage périphérique/point d'accès 2_2 comprend, ainsi que représenté en figure 4b :

- un module Stockage/extraction de la base de données 2_{2a}. Cette fonction permet aux différentes fonctions mises en œuvre par le module d'appairage périphérique/point d'accès 2_2 de stoker ou d'extraire de la base de données 2_3 des données telles que des identifiants au niveau 2 du point d'accès PA ou de variables utilisées par le périphérique T ;
- module Supervision/bouton-poussoir 2_{2b}. Cette fonction permet de mesurer le temps d'appui T_T, c'est-à-dire la valeur de la durée d'initialisation du périphérique exécutée par l'utilisateur sur le circuit tel qu'un bouton-poussoir 2_4. Cette fonction est en relation avec la fonction Stockage/extraction de la base de données 2_{2a} pour stocker le temps d'appui T_T précité. Elle est en outre en relation avec la fonction Gestion connexion courte portée 2_{2c} précédemment décrite afin de paramétrer l'interface radio dès le relâchement du bouton de commande 2_4 par

l'utilisateur pour assurer le support d'une connexion courte portée avec le point d'accès AP. La fonction Supervision/bouton-poussoir 2_{2b} est également en relation avec une fonction Collecte des variables 2_{2f} afin d'envoyer au point d'accès AP, par l'intermédiaire de la voie radio courte portée, par exemple, la durée d'initialisation du périphérique, c'est-à-dire la valeur T_T mémorisée localement. En outre, la fonction Supervision/bouton-poussoir 2_{2b} permet, de manière avantageuse, de déclencher le compteur de temps P_2 précédemment décrit dans la description pour la mise en œuvre du procédé afin de permettre la protection contre toute tentative de connexion non autorisée.

– module Gestion connexion courte portée 2_{2c}. Cette fonction permet d'instaurer un dialogue avec le module d'infrastructure logicielle de gestion d'interface radio 2_1, afin de paramétrer l'interface radio en mode courte portée par exemple. Ce paramétrage varie en fonction de la technologie radio utilisée. Pour une technologie radio de type IEEE 802.11, le paramétrage précité peut consister à se connecter sur un nom de réseau prédéfini, par exemple "Appairage", puis à fixer une modulation radio haute à 54 Mb/s et, optionnellement, à baisser la puissance radio d'émission et de réception de l'interface radio à courte portée 2_5 ;

– module Envoi/réception de données radio 2_{2d}. Cette fonction permet d'envoyer, respectivement de recevoir, des données vers l'infrastructure logicielle de gestion de l'interface radio 2_1 ;

– module Identification point d'accès 2_{2e}. Cette fonction permet d'assurer l'identification du point d'accès AP. Elle reçoit, d'une part, le temps d'appui ou durée d'initialisation du périphérique T_T, provenant de la fonction supervision bouton-poussoir 2_{2b}, et, d'autre part, le temps d'appui point d'accès, c'est-à-dire la durée d'initialisation du point d'accès transmise T_{apr} provenant de la fonction Envoi/réception données radio 2_{2d} précitée. La fonction Identification point d'accès 2_{2e} dispose également avantageusement d'un taux d'erreur D lequel peut être différent du taux d'erreur E appliqué au point d'accès AP et provenant de la fonction Stockage/extraction de la base de données 2_{2a}. A partir des données précitées, la fonction Identification point d'accès 2_{2e} est en mesure d'identifier le point d'accès AP

comme point d'accès pré-initialisé puis initialisé pour la connexion demandée et de stocker ensuite dans la base de données 2_3, le résultat de l'identification ainsi exécutée. Lorsque, en outre, le résultat l'identification est positif, l'identifiant au niveau lien du point d'accès AP identifié reconnu est également stocké dans la base de données 2_3 ;

- module Collecte des variables 2_{2f}. Cette fonction est en relation avec la fonction Supervision/bouton-poussoir 2_{2b} et la fonction Stockage/extraction de la base de données 2_{2a} afin de collecter la durée d'initialisation du périphérique temps d'appui du périphérique T_T et la valeur de la variable Ch précédemment mentionnée dans la description. Les variables précitées sont ensuite transmises à la fonction Envoi/réception données radio 2_{2d} pour transmission vers le point d'accès AP ;

- module Générateur de clés 2_{2g}. Cette fonction a pour objet d'engendrer une clé de chiffrement transmise ensuite à la fonction Envoi/réception données radio 2_{2d} pour transmission au point d'accès AP. Cette fonction est également chargée d'engendrer une clé de déchiffrement laquelle est stockée dans la base de données 2_3. On rappelle que lorsque la clé de chiffrement est transmise au point d'accès AP, cette clé de chiffrement est par exemple une clé publique alors que la clé de déchiffrement est au contraire une clé privée, laquelle peut être stockée dans la base de données 2_3 de manière sécurisée ;

- module Déchiffrement information de configuration 2_{2h}. Cette fonction est chargée de déchiffrer les éléments de configuration transmis par le point d'accès AP. Dans ce but, la fonction précitée est en relation avec la base de données 2_3 pour récupérer la clé de déchiffrement précitée. Après déchiffrement, les éléments de configuration précités sont envoyés à une fonction Gestion connexion longue portée 2_{2i} ;

- module Gestion connexion longue portée 2_{2i}. Cette fonction, lorsque l'ensemble de la procédure d'identification est terminée, a pour objet de préparer la connexion longue portée du périphérique T vers le point d'accès AP à partir des éléments de configuration reçus. Cette fonction opère en liaison avec l'interface ou infrastructure logicielle de gestion des interfaces radio.

Une description d'un protocole du mode opératoire d'un périphérique conforme à l'objet de la présente invention, tel que décrit en liaison avec les figures 4a et 4b sera maintenant décrit en liaison avec la figure 4c.

En référence à la figure précitée, la procédure d'identification est déclenchée par un appui puis un relâchement à l'étape S_{T1} du bouton de commande 2_4 situé sur le périphérique. Cette première étape correspond au déclenchement de l'initialisation du périphérique T. Le temps d'appui du bouton de commande 2_4 est comptabilisé par la fonction Supervision du bouton-poussoir 2_{2b} de la figure 4b, la valeur de cette durée étant la valeur T_T. Le relâchement du bouton de commande permet en outre au périphérique T de déclencher un compteur de temps, le compteur de temps P_2 précédemment décrit dans la description. En particulier, lorsque la reconnaissance mutuelle entre le point d'accès AP et le périphérique T est exécutée, toutes les étapes du procédé et du protocole représenté en figure 4c, jusqu'à l'étape de réception de la valeur de durée d'initialisation du point d'accès, valeur T_{apr}, doivent être exécutées dans la durée P2 déterminée par le compteur de temps précité.

A l'étape S_{T2} la durée d'initialisation du périphérique T_T est mise en mémoire par la fonction Stockage/extraction de la base de données 2_{2a}.

A l'étape suivante S_{T3}, le module d'appairage périphérique/point d'accès 2_2 met ensuite en place l'appairage provisoire sur un nom de réseau prédéfini avec le point d'accès en lien avec l'infrastructure logicielle de gestion des interfaces radio 2_1. De manière optionnelle, cet appairage provisoire peut être exécuté par l'intermédiaire de la liaison radio à courte portée 2_5. Dans l'exemple donné précédemment dans la description, le réseau d'accès dans cette situation est un réseau de type IEEE 802.11 dont la portée est réduite en forçant le périphérique à dialoguer avec un taux de modulation radio le plus haut possible selon les possibilités radio, par exemple 54 Mb/s et en utilisant la puissance d'émission et de réception radio la plus basse possible, par exemple 1 mW. Une modulation radio très haute combinée à une puissance d'émission/réception très basse permet de limiter l'espionnage des échanges radio. La portée restreinte permet en fait d'augmenter la sécurité des transactions et

tous les messages radio échangés jusqu'à l'étape finale d'initialisation sont échangés grâce à la liaison radio courte portée précitée.

L'étape suivante S_{T4} est mise en œuvre par la fonction Collecte des variables 2_{2f} laquelle permet la collecte de la variable T_T, de l'identification au niveau lien du périphérique T et, optionnellement, de la variable Ch. Ces variables sont alors transmises grâce à la fonction Envoi/réception de données radio sur la liaison radio vers le point d'accès AP. L'envoi de ces variables peut, le cas échéant, être exécuté par l'intermédiaire d'un tunnel sécurisé. Les variables précitées sont alors envoyées dans un message de valeur tel que décrit précédemment dans la description par exemple. Le périphérique T peut, optionnellement, transmettre la variable Ch indiquant à quel type d'application il accède une fois connecté au point d'accès AP, c'est-à-dire le type d'application ou le type de périphérique, tel qu'un périphérique audiovisuel par exemple, qu'il constitue.

L'étape suivante S_{T5} est une étape dans laquelle le module appairage périphérique/point d'accès 2_2 attend la réception de la valeur de durée d'initialisation du point d'accès, la valeur T_{apr}. Sur réponse négative au test de l'étape S_{T5}, c'est-à-dire en l'absence de réception de la valeur de durée précitée au bout de la durée P_2, la procédure d'appairage se termine sur un échec par retour à une situation de fin de connexion. En outre, sur réception de plusieurs valeurs d'initialisation de point d'accès T_{ap} au bout de durée P_2, la procédure d'appairage se termine également par un retour à une étape de fin de connexion sur un échec.

A l'étape S_{T6} suivante, sur réception du message de valeur contenant la variable de valeur de durée d'initialisation du point d'accès, variable T_{apr}, la fonction Envoi/réception données radio 2_{2d}, transmet à la fonction Identification point d'accès 2_{2e}, la valeur de la variable précitée. La fonction Identification point d'accès 2_{2e}, lit dans la base de données la variable d'erreur D et vérifie alors par comparaison d'égalité la relation :

$$T_{apr} = T_T \pm D.$$

Si la relation est vérifiée, la procédure se poursuit sinon, la procédure d'appairage se termine par un échec par un retour à un état de fin de connexion. Ces

opérations sont représentées par la réponse positive, respectivement négative, au test S_{T6} de la figure 4c.

On rappelle, conformément à un aspect remarquable du procédé et du protocole objets de la présente invention, que les valeurs d'erreur E et D appliquées pour les applications de reconnaissance mutuelles du point d'accès AP et du périphérique T peuvent être différentes et que la comparaison d'égalité précitée peut être effectuée en prenant comme référence la valeur de durée d'initialisation locale, c'est-à-dire la valeur T_{ap} de la durée d'initialisation du point d'accès AP, respectivement T_T du périphérique T, pour exécuter chaque comparaison au niveau du point d'accès AP, respectivement du périphérique T. Ainsi, par ce mode opératoire, les deux comparaisons sont rendues totalement indépendantes en l'absence de toute affectation de qualité d'appareil maître ou esclave à l'un et/ou l'autre des équipements point d'accès AP ou terminal T.

A l'étape S_{T7} la relation de comparaison précitée est vérifiée et la fonction Identification/point d'accès 2_{2e} permet de stocker dans la base de données 2_3 l'identifiant au niveau lien du point d'accès AP. Le point d'accès AP est maintenant considéré comme reconnu et identifié comme point d'accès choisi par l'utilisateur du périphérique T demandeur de connexion.

L'étape S_{T8} suivante est une étape dans laquelle le périphérique T engendre une clé de chiffrement grâce à la fonction Générateur de clé 2_{2g}, la clé de déchiffrement correspondante étant alors mémorisée dans la base de données 2_3. La clé de chiffrement est envoyée au point d'accès par l'intermédiaire de l'interface radio courte portée 2_5. La clé engendrée est une clé publique du système RSA par exemple, la clé de déchiffrement stockée étant alors la clé privée associée à cette clé publique et stockée de manière sécurisée.

L'étape suivante S_{T9} est une étape d'attente dans laquelle le périphérique T attend la réception des éléments de configuration relatifs à la connexion longue portée à établir. Sur réponse négative au test de l'étape S_{T9} si les éléments de configuration ne sont pas reçus au bout d'une durée déterminée, la procédure d'appairage se termine sur un échec par retour à une étape de fin de connexion. Au

contraire, sur réception des éléments de configuration, c'est-à-dire en réponse positive au test de l'étape S_{T9}, les éléments de configuration reçus sont ensuite déchiffrés par la fonction Déchiffrement/information de configuration 2_{2h} et envoyés à la fonction Gestion de connexion longue portée 2_{2i}. Cette situation est représentée sur réponse positive au test S_{T9} de la figure 4c.

L'étape suivante S_{T11} est une étape de mise en place de la connexion longue portée à partir des éléments de configuration et de la fonction Gestion de connexion longue portée 2_{2i} précitée. Cette connexion longue portée peut être mise en œuvre sur la base d'un nouveau nom de réseau fourni avec une clé de chiffrement fournie.

Suite à l'étape S_{T11}, alors la connexion entre le périphérique et le point d'accès AP est poursuivie.

En ce qui concerne l'échange des valeurs de durée d'initialisation entre le périphérique T et le point d'accès AP et réciproquement, on indique que les variables précitées peuvent être transmises dans le cadre de messages radio existants, tels que les champs supplémentaires dans les messages définis par la recommandation IEEE 802.11, "probe request" et "probe response" par exemple.

Toutefois les valeurs d'initialisation précitées peuvent faire l'objet d'envoi de messages spécifiques, en particulier sous forme d'un message de transmission de valeur d'une durée d'initialisation, entre un point d'accès en réseau partagé et un périphérique candidat à une connexion à ce point d'accès.

Un tel message comporte en particulier, outre un champ d'adresse du destinataire du message, un champ d'adresse de l'émetteur du message et au moins un champ d'identification du message, un champ de valeur de durée d'initialisation de l'émetteur du message. Il peut comporter en outre un champ de l'adresse au niveau lien de l'émetteur du message.

En particulier, la structure de données constitutive d'un tel message est représentée au tableau 1 ci-après.

Tableau 1

Champ	*Valeur du champ*
Adresse destination	Champ obligatoirement présent ; adresse du destinataire du message.
Adresse source	Champ obligatoirement présent ; adresse de l'émetteur du message.
Type du message	Champ obligatoirement présent ; ce champ prend la valeur "Envoi variable".
Longueur	Champ obligatoirement présent ; longueur du message.
Numéro de séquence	Champ obligatoirement présent ; numéro de séquence du message.
Variable 1	Champ obligatoirement présent ; cette variable contient la valeur Tap ou Tperiph suivant l'émetteur du message.
Variable 2	Champ optionnellement présent ; cette variable contient l'identification de niveau lien de l'émetteur du message.
Variable 3	Champ optionnellement présent ; Cette variable contient "Ch", variable présente uniquement si l'émetteur du message est un périphérique.

Le message de valeur ainsi constitué est envoyé par le point d'accès AP à l'étape S_{ap4} de la figure 3d et un message correspondant de valeur est envoyé à l'étape S_{T4} de la figure 4c avec, optionnellement, son identifiant au niveau lien et la variable Ch.

En outre, l'envoi du message de transmission de valeur précité fait l'objet de l'envoi d'un message d'acquittement d'un tel message de transmission de valeur de durée d'initialisation par l'équipement qui a reçu le message de transmission de valeur de durée d'initialisation.

Un tel message d'acquittement présente une structure de données telle que représentée au tableau 2 suivant.

Tableau 2

Champ	*Valeur du champ*
Adresse destination	Champ obligatoirement présent ; adresse du destinataire du message.
Adresse source	Champ obligatoirement présent ; adresse de l'émetteur du message.
Type du message	Champ obligatoirement présent ; ce champ prend la valeur "acquittement".
Longueur	Champ obligatoirement présent ; longueur du message.
Numéro de séquence	Champ obligatoirement présent ; numéro de séquence du message acquitté.

L'invention couvre enfin un programme d'ordinateur enregistré sur un support de mémorisation pour exécution par un ordinateur remarquable en ce que lors de l'exécution par l'ordinateur d'un point d'accès, ce programme d'ordinateur permet la mise en œuvre du procédé, au niveau du point d'accès, ainsi que décrit précédemment dans la description en liaison avec les figures 1 et 2.

On comprend en particulier que le programme d'ordinateur précité est alors implanté sur le point d'accès AP soit sous forme intégrée soit sous forme modulaire pour constituer un module d'appairage point d'accès/périphérique tel que le module 1_2 de la figure 3a dans un point d'accès tel que décrit en liaison avec les figures 3a et 3b et opérant selon les protocoles de pré-initialisation et d'initialisation décrits avec les figures 3c et 3d précédemment dans la description.

L'invention couvre également un programme d'ordinateur enregistré sur un support de mémorisation pour exécution par un ordinateur remarquable en ce que ce programme d'ordinateur, lorsqu'il est exécuté par l'ordinateur d'un périphérique, permet la mise en œuvre du procédé, au niveau de ce périphérique, ainsi que décrit précédemment dans la description en liaison avec la figure 1 et la figure 2.

En particulier on comprend que le programme d'ordinateur précité est implanté soit sous forme intégrée soit sous forme modulaire pour constituer un module d'appairage périphérique/point d'accès 2_2 tel que décrit en liaison avec la figure 4a dans un périphérique conforme à l'objet de la présente invention tel que

décrit précédemment dans la description en liaison avec les figures 4a, 4b et opérant selon le protocole décrit en liaison avec la figure 4c.

REVENDICATIONS

1. Procédé de contrôle de la connexion d'un premier dispositif et d'un deuxième dispositif, caractérisé en ce que celui-ci consiste au moins à :

– exécuter une commande locale d'initialisation pendant une certaine durée sur le premier et le deuxième dispositif ; et, suite à un appairage provisoire de ce premier et ce deuxième dispositif,

– échanger les valeurs de durées d'initialisation respectives du premier et du deuxième dispositif ; et, si les durées d'initialisation du premier et du deuxième dispositif diffèrent d'une valeur inférieure à une valeur de seuil,

– poursuivre la connexion ; sinon,

– inhiber la connexion.

2. Procédé selon la revendication 1, caractérisé en ce que pour le contrôle de la connexion d'un périphérique à un point d'accès en réseau partagé, ledit procédé consiste au moins à :

– pré-initialiser ledit point d'accès par une commande locale de ce point d'accès, l'étape de pré-initialisation permettant au moins de configurer ledit point d'accès pour appairer provisoirement un périphérique ; puis

– initialiser simultanément ledit point d'accès et ledit périphérique par une commande locale sensiblement concomitante en durée dudit point d'accès respectivement dudit périphérique, mesurer localement et mémoriser la durée d'initialisation de chaque commande locale au niveau dudit point d'accès respectivement dudit périphérique ; et, suite à un appairage provisoire dudit point d'accès et dudit périphérique,

– transmettre et recevoir, au moins dudit périphérique vers ledit point d'accès, la valeur de la durée d'initialisation mémorisée et comparer par comparaison d'égalité, au moins au niveau dudit point d'accès, la valeur de la durée d'initialisation mesurée localement à la durée d'initialisation reçue ; et, si la durée d'initialisation reçue est sensiblement égale à la durée d'initialisation mesurée

localement, ledit périphérique étant admis comme périphérique demandeur de connexion identifié,

– autoriser la poursuite de la connexion dudit périphérique par appel d'une procédure d'appairage permanent ; sinon,

– inhiber, au moins au niveau dudit point d'accès, la poursuite de la connexion.

3. Procédé selon la revendication 2, caractérisé en ce que la transmission entre ledit point d'accès et ledit périphérique de la valeur de la durée d'initialisation mesurée localement et mémorisée étant réciproque, l'autorisation de poursuite de la connexion est conditionnelle à l'identification mutuelle du périphérique demandeur d'accès identifié respectivement du point d'accès simultanément initialisé pour ce périphérique demandeur d'accès, par comparaison d'égalité de la valeur de la durée d'initialisation mémorisée localement et de la valeur de la durée d'initialisation reçue.

4. Procédé selon l'une des revendications 2 ou 3, caractérisé en ce que l'étape d'appairage provisoire entre ledit point d'accès et ledit périphérique consiste à réduire la portée en émission/réception d'au moins ledit point d'accès.

5. Procédé selon l'une des revendications 2 à 4, caractérisé en ce que l'étape consistant à autoriser la poursuite de la connexion dudit périphérique est conditionnelle à l'absence, préalablement à l'appel de la procédure d'appairage permanent, d'une nouvelle étape de pré-initialisation et/ou d'initialisation simultanée entre ledit point d'accès et au moins un périphérique.

6. Procédé selon l'une des revendications 2 à 5, caractérisé en ce que l'étape consistant à autoriser la poursuite de la connexion dudit périphérique comporte un critère de rejet de toute nouvelle demande de connexion étrangère à une demande de connexion existante pour un périphérique demandeur de connexion identifié.

7. Procédé selon l'une des revendications 1 à 6, caractérisé en ce que l'étape de transmission entre ledit point d'accès et ledit périphérique et/ou réciproquement est effectuée par transmission d'un message de valeur comportant au

moins ladite valeur de la durée d'initialisation mémorisée et l'identifiant au niveau lien de l'émetteur de ce message, et

– d'un message d'acquittement, ledit message d'acquittement comportant au moins une référence audit message de valeur.

8. Point d'accès à un réseau partagé, par un périphérique comportant une interface de signal de liaison, une interface logicielle de gestion d'interface de signal de liaison, caractérisé en ce que ledit point d'accès comporte au moins :

– un module d'appairage point d'accès/périphérique relié à ladite interface logicielle de gestion d'interface de signal de liaison ;

– une base de données reliée audit module d'appairage point d'accès/périphérique et comportant, d'une part, des données temporaires, et, d'autre part, des données permanentes ;

– des moyens de pré-initialisation dudit point d'accès par une commande locale de ce point d'accès, la pré-initialisation permettant au moins de configurer ledit point d'accès pour appairer provisoirement un périphérique ;

– des moyens d'initialisation dudit points d'accès par une commande locale de ce point d'accès, ledit module d'appairage point d'accès/périphérique permettant de mesurer localement et de mémoriser la durée d'initialisation dudit point d'accès par ladite commande locale, et, suite à un appairage provisoire de ce point d'accès et d'un périphérique, recevoir au moins de ce périphérique une valeur de la durée d'initialisation mémorisée de ce périphérique par une commande locale d'initialisation, comparer par comparaison d'égalité la valeur de la durée d'initialisation mesurée localement à la valeur de la durée d'initialisation mesurée reçue, et, si la durée d'initialisation mesurée reçue est sensiblement égale à la durée d'initialisation mesurée localement, ledit périphérique étant reconnu comme périphérique demandeur de connexion identifié, autoriser la poursuite de la connexion dudit périphérique par exécution d'une procédure d'appairage permanent ; sinon, inhiber au niveau dudit point d'accès la poursuite de la connexion.

9. Point d'accès en réseau radio partagé selon la revendication 8, caractérisé en ce que lesdits moyens de pré-initialisation dudit point d'accès et lesdits

moyens d'initialisation dudit point d'accès sont constitués par un bouton de commande unique disposé sur le châssis dudit point d'accès, ledit bouton de commande unique délivrant ledit signal de commande locale de pré-initialisation ou d'initialisation à l'initiative d'un utilisateur audit module d'appairage point d'accès/périphérique.

10. Point d'accès selon l'une des revendications 8 ou 9, caractérisé en ce que celui-ci comporte :

- une première interface radio à courte portée ; et
- une deuxième interface radio à longue portée, la première interface radio et la deuxième interface radio étant commutées par l'intermédiaire dudit module d'appairage point d'accès/périphérique pour assurer un appairage temporaire en liaison radio à courte portée respectivement un appairage permanent en liaison radio en longue portée avec ledit périphérique.

11. Périphérique connectable à un point d'accès en réseau partagé, comportant une interface de signal de liaison, une interface logicielle de gestion d'interface de signal de liaison, caractérisé en ce que ledit périphérique comporte au moins :

- un module d'appairage périphérique/point d'accès relié à ladite interface logicielle de gestion d'interface de signal de liaison ;
- une base de données reliée audit module d'appairage périphérique/point d'accès et comportant, d'une part, des données temporaires, et, d'autre part, des données permanentes ;
- des moyens d'initialisation dudit périphérique par une commande locale de ce périphérique, ledit module d'appairage périphérique/point d'accès permettant de mesurer localement et de mémoriser la durée d'initialisation dudit périphérique par ladite commande locale, et, suite à un appairage provisoire de ce périphérique et d'un point d'accès, recevoir au moins de ce point d'accès une valeur de la durée d'initialisation mémorisée de ce point d'accès par une commande locale d'initialisation, comparer par comparaison d'égalité la valeur de la durée d'initialisation mesurée reçue, et, si la durée d'initialisation mesurée reçue est

sensiblement égale à la durée d'initialisation mesurée localement, ledit point d'accès étant reconnu comme point d'accès initialisé pour ledit périphérique demandeur d'accès, autoriser la poursuite de la connexion dudit périphérique par exécution d'une procédure d'appairage permanent, sinon, inhiber au niveau dudit périphérique la poursuite de la connexion.

12. Périphérique selon la revendication 11, caractérisé en ce que lesdits moyens d'initialisation sont constitués par un bouton de commande disposé sur le chassis dudit périphérique, ledit bouton de commande délivrant ledit signal de commande d'initialisation à l'initiative d'un utilisateur audit module d'appairage périphérique/point d'accès.

13. Périphérique selon l'une des revendications 11 ou 12, caractérisé en ce que celui-ci comporte :

- une première interface de signal de liaison à courte portée ; et
- une deuxième interface de signal de liaison à longue portée, la première et la deuxième interface de signal de liaison étant commutées par l'intermédiaire dudit module d'appairage périphérique/point d'accès pour assurer une étape d'appairage temporaire en liaison en courte portée respectivement un appairage permanent en liaison en longue portée avec ledit point d'accès.

14. Message de transmission de valeur d'une durée d'initialisation entre un point d'accès en réseau partagé et un périphérique candidat à une connexion à ce point d'accès, caractérisé en ce que, outre un champ d'adresse du destinataire du message, un champ d'adresse de l'émetteur du message, celui-ci comporte au moins un champ d'identification du message, un champ de valeur de durée d'initialisation de l'émetteur du message.

15. Message d'acquittement d'un message de transmission de valeur d'une durée d'initialisation selon la revendication 14, caractérisé en ce que, outre un champ d'adresse du destinataire du message, un champ d'adresse de l'émetteur du message celui-ci comporte au moins un champ d'identification du message acquitté.

16. Programme d'ordinateur enregistré sur un support de mémorisation pour exécution par un ordinateur, caractérisé en ce que lors de l'exécution par

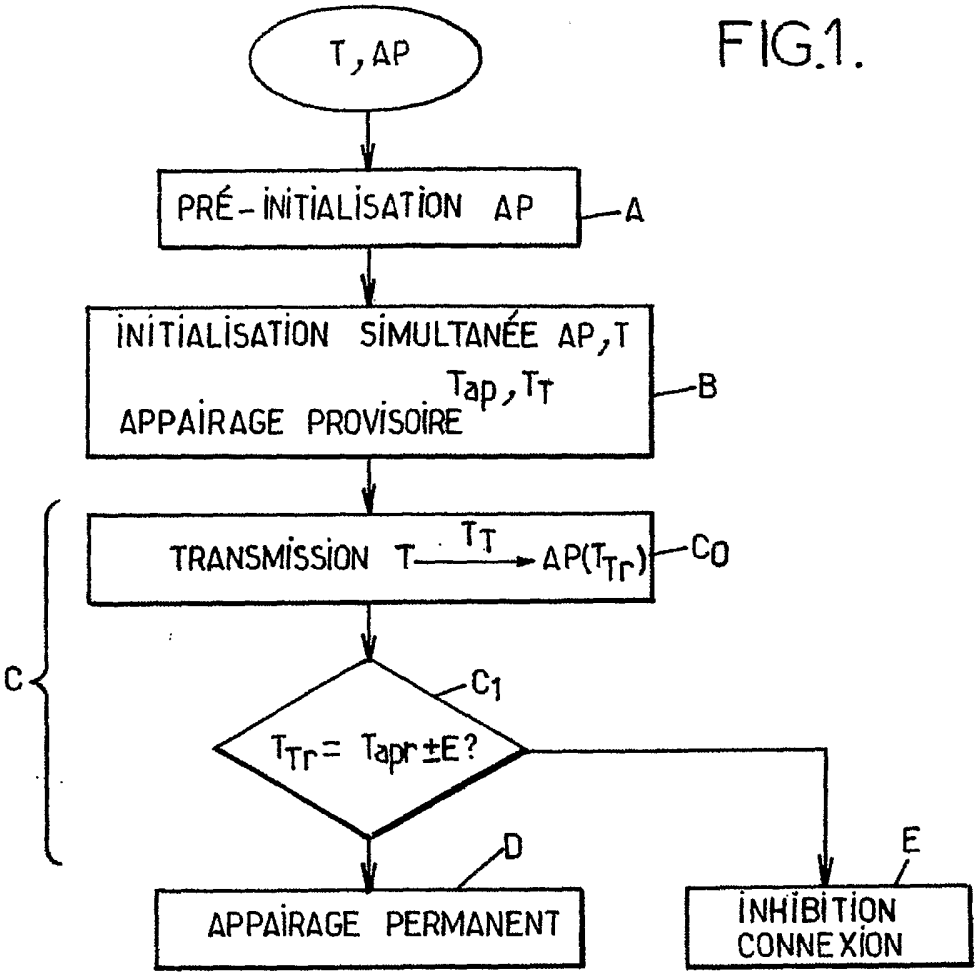
l'ordinateur d'un point d'accès, celui-ci permet la mise en œuvre du procédé, au niveau du point d'accès, selon l'une des revendications 1 à 7.

17. Programme d'ordinateur selon la revendication 16, caractérisé en ce que ledit programme d'ordinateur est implanté sur le point d'accès soit sous forme intégrée soit sous forme modulaire pour constituer un module d'appairage point d'accès/périphérique dans un point d'accès selon l'une des revendications 8 à 10.

18. Programme d'ordinateur enregistré sur un support de mémorisation pour exécution par un ordinateur, caractérisé en ce que lors de l'exécution par l'ordinateur d'un périphérique, celui-ci permet la mise en œuvre du procédé, au niveau périphérique, selon l'une des revendications 1 à 7.

19. Programme d'ordinateur selon la revendication 18, caractérisé en ce que ledit programme d'ordinateur est implanté soit sous forme intégrée soit sous forme modulaire pour constituer un module d'appairage périphérique/point d'accès dans un périphérique selon l'une des revendications 11 à 13.

FIG.1.


T, AP
PRÉ-INITIALISATION AP
A
INITIALISATION SIMULTANÉE AP, T
APPAIRAGE PROVISOIRE
Tap, TT
B
TRANSMISSION T
TT
AP(TTr)
Co
C
C1
TTr = Tapr ± E?
D
APPAIRAGE PERMANENT
E
INHIBITION CONNEXION

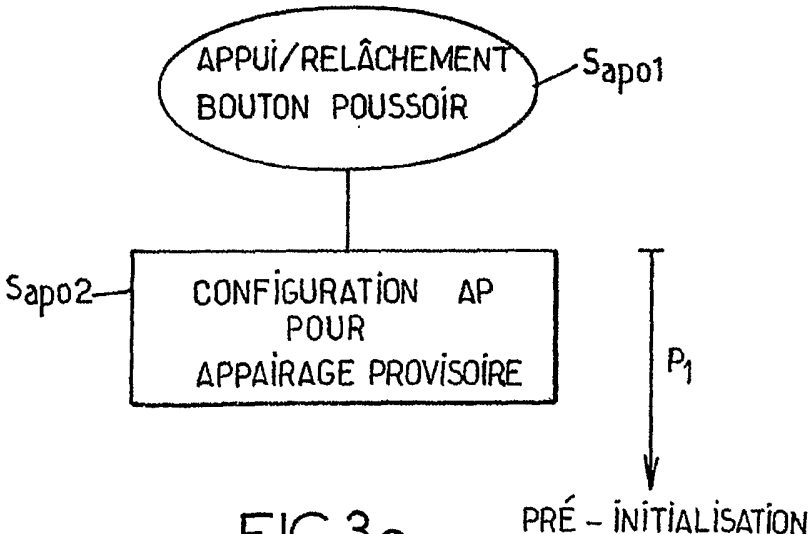

APPUI/RELÂCHEMENT BOUTON POUSSOIR
Sapo1
Sapo2
CONFIGURATION AP POUR APPAIRAGE PROVISOIRE
P1
PRÉ - INITIALISATION

FIG.3c.

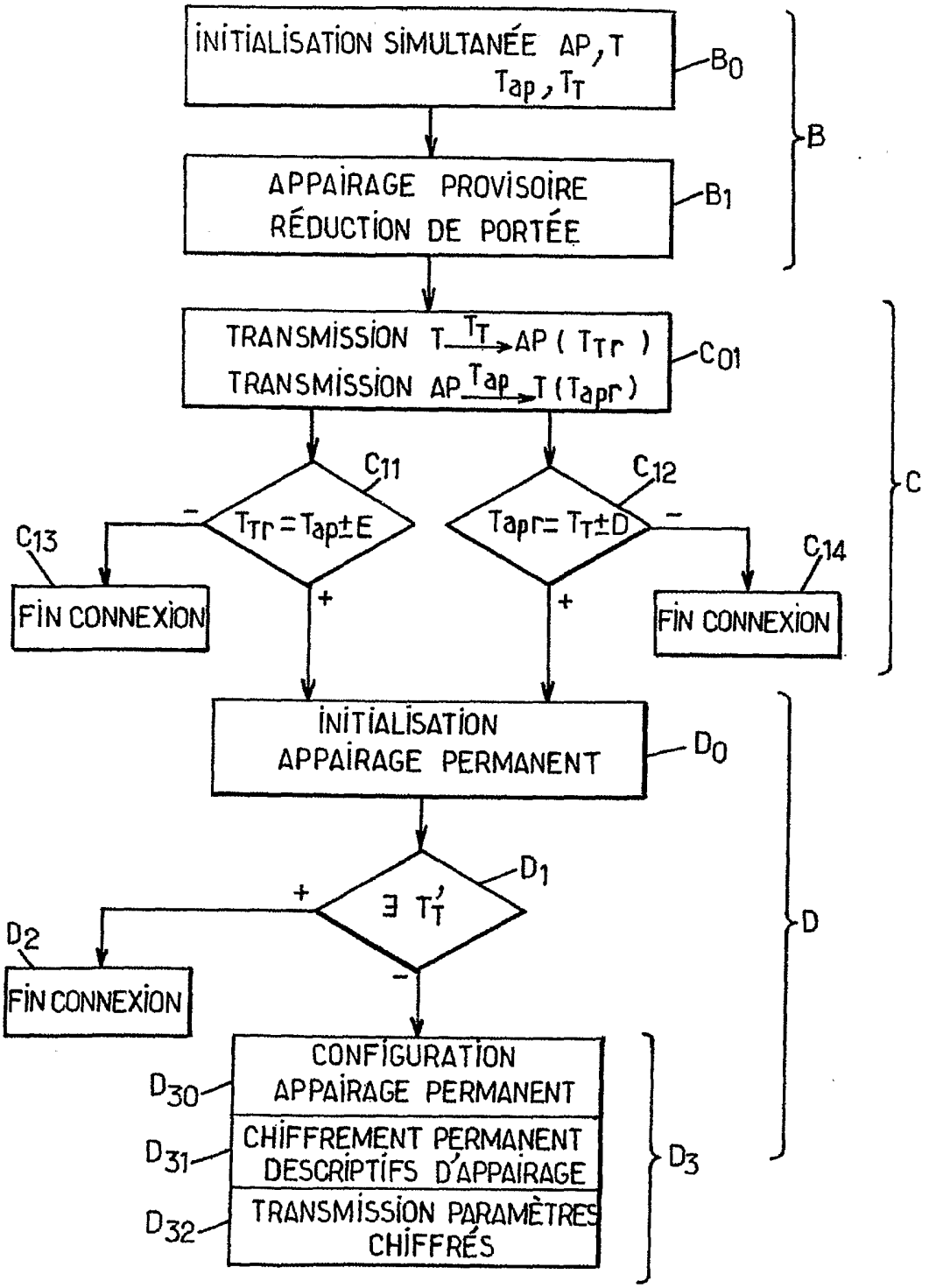

INITIALISATION SIMULTANÉE AP, T
Tap, TT
B0
B
APPAIRAGE PROVISOIRE
RÉDUCTION DE PORTÉE
B1
TRANSMISSION T TT AP (TTr)
TRANSMISSION AP Tap T (Tapr)
C01
C
C11
TTr = Tap±E
C12
Tapr = TT±D
C13
FIN CONNEXION
C14
FIN CONNEXION
INITIALISATION
APPAIRAGE PERMANENT
D0
D
D1
∃ T'T
D2
FIN CONNEXION
CONFIGURATION
APPAIRAGE PERMANENT
D30
CHIFFREMENT PERMANENT
DESCRIPTIFS D'APPAIRAGE
D31
TRANSMISSION PARAMÈTRES
CHIFFRÉS
D32
D3

FIG.2.

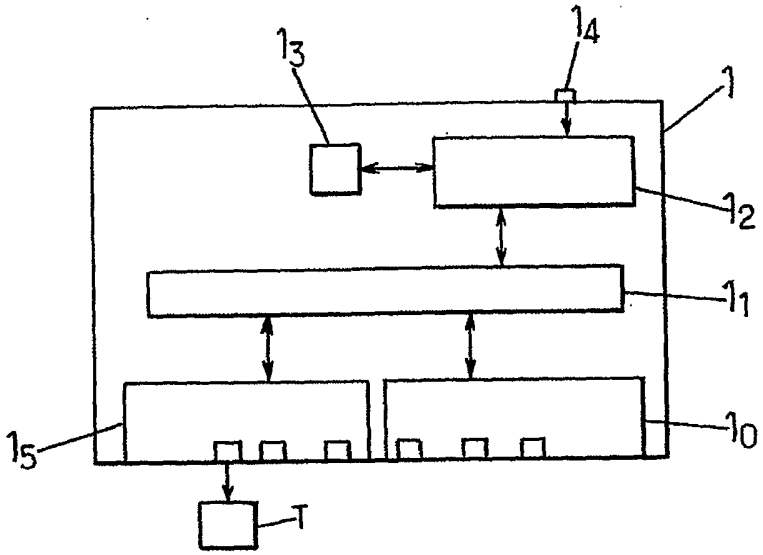

13
14
1
12
11
15
10
T

FIG.3a.

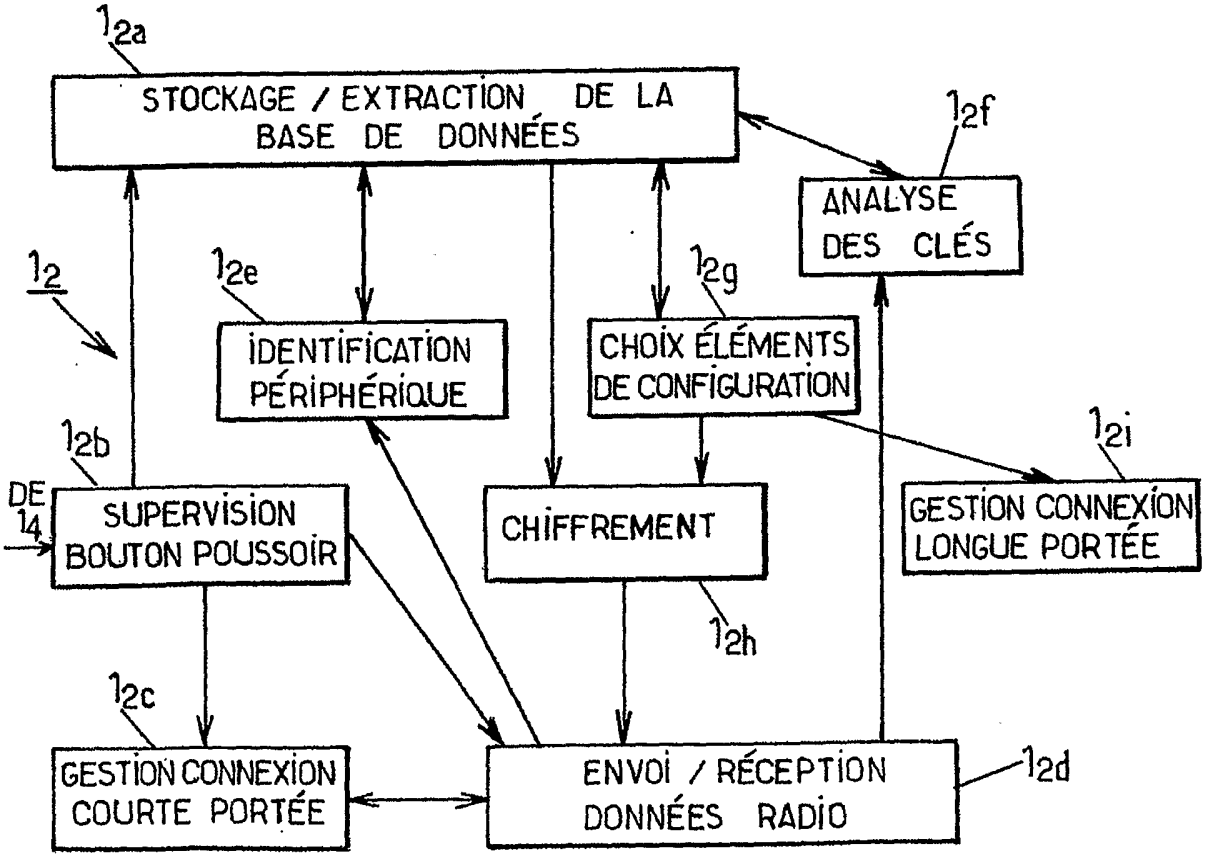

12a
STOCKAGE / EXTRACTION DE LA BASE DE DONNÉES
12f
ANALYSE DES CLÉS
12
12e
IDENTIFICATION PÉRIPHÉRIQUE
12g
CHOIX ÉLÉMENTS DE CONFIGURATION
12b
DE 14
SUPERVISION BOUTON POUSSOIR
CHIFFREMENT
12i
GESTION CONNEXION LONGUE PORTÉE
12h
12c
GESTION CONNEXION COURTE PORTÉE
ENVOI / RÉCEPTION DONNÉES RADIO
12d

FIG.3b.

FIG.3d.

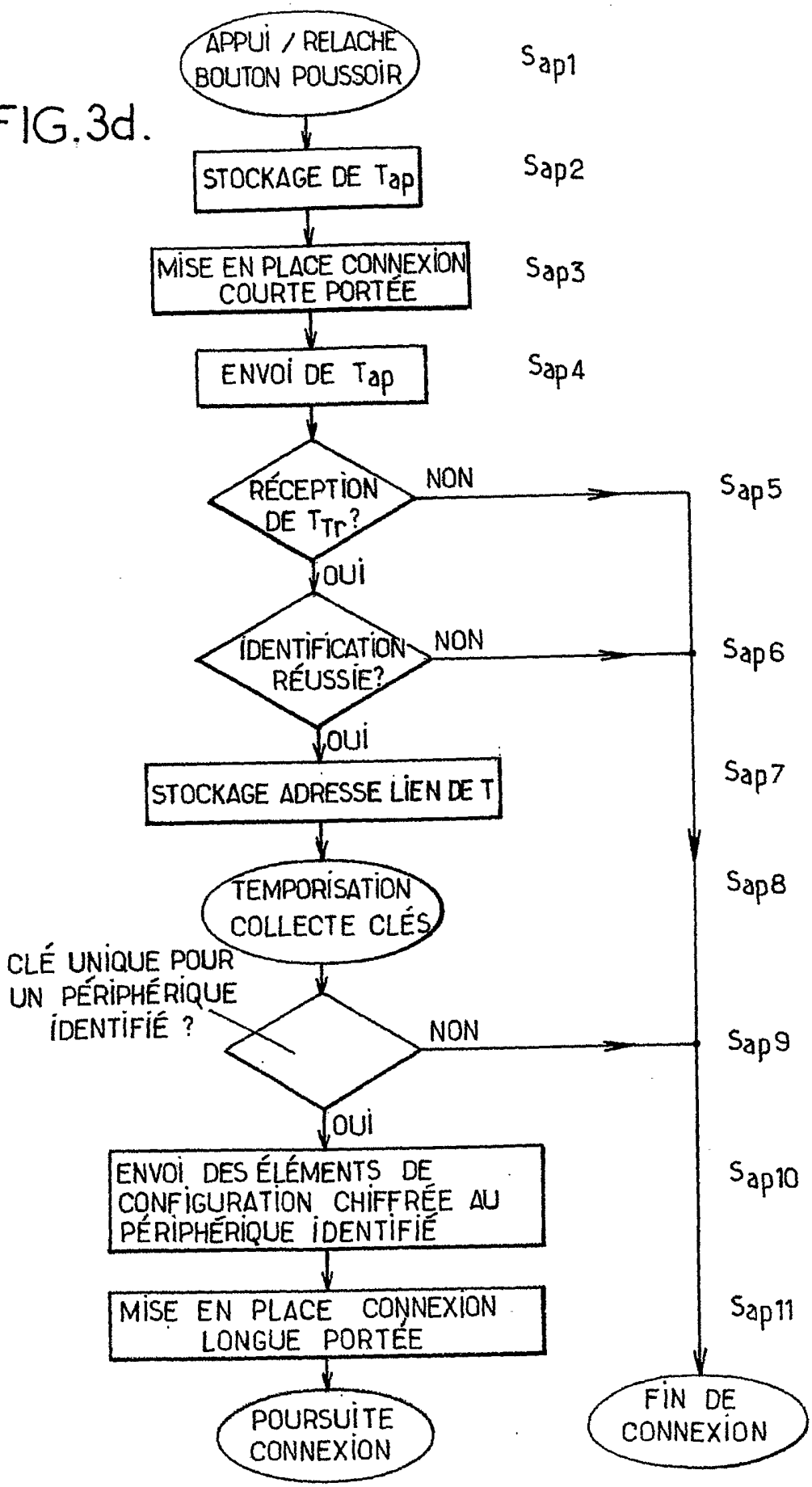
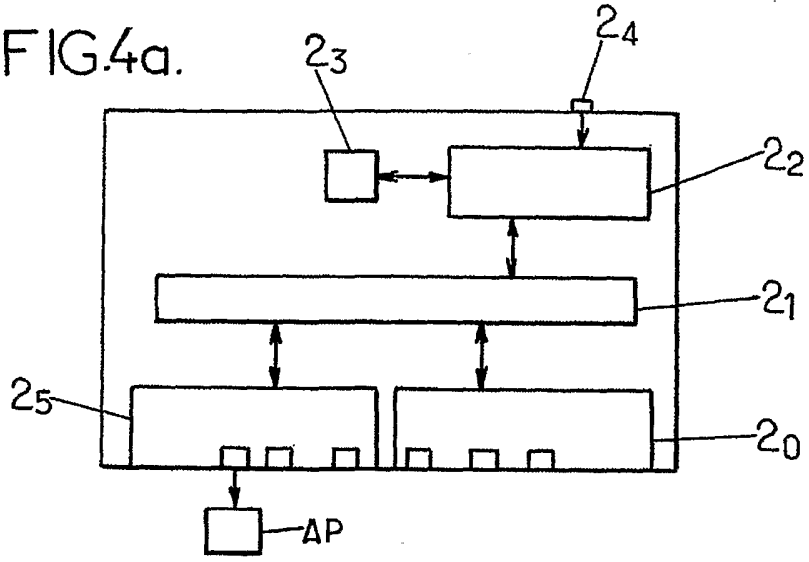

APPUI / RELACHE BOUTON POUSSOIR
Sap1
STOCKAGE DE Tap
Sap2
MISE EN PLACE CONNEXION COURTE PORTÉE
Sap3
ENVOI DE Tap
Sap4
RÉCEPTION DE TTr?
NON
Sap5
OUI
IDENTIFICATION RÉUSSIE?
NON
Sap6
OUI
STOCKAGE ADRESSE LIEN DE T
Sap7
TEMPORISATION COLLECTE CLÉS
Sap8
CLÉ UNIQUE POUR UN PÉRIPHÉRIQUE IDENTIFIÉ ?
NON
Sap9
OUI
ENVOI DES ÉLÉMENTS DE CONFIGURATION CHIFFRÉE AU PÉRIPHÉRIQUE IDENTIFIÉ
Sap10
MISE EN PLACE CONNEXION LONGUE PORTÉE
Sap11
POURSUITE CONNEXION
FIN DE CONNEXION

FIG.4a.


24
23
22
21
25
20
AP

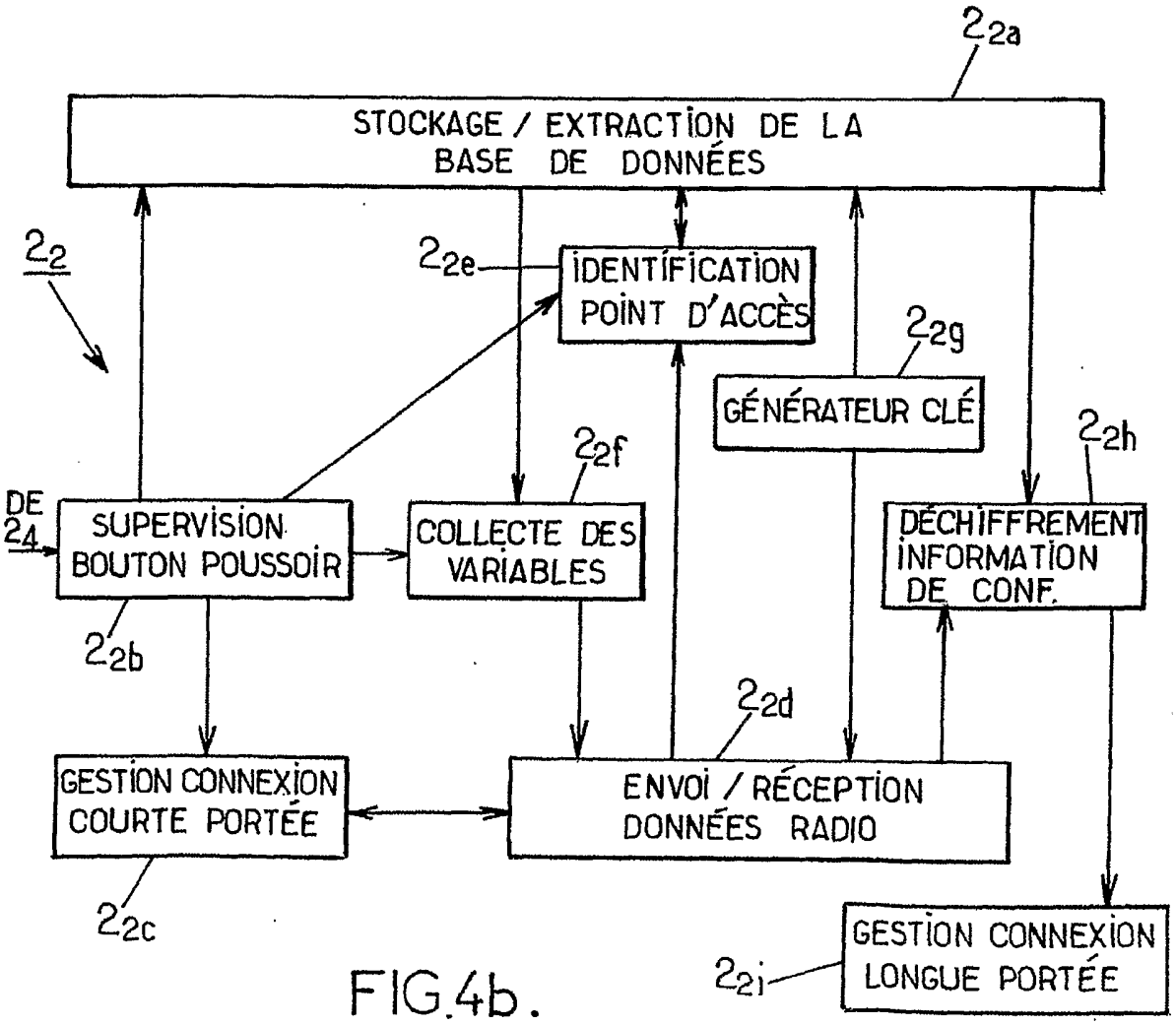

22a
STOCKAGE / EXTRACTION DE LA BASE DE DONNÉES
22
22e
IDENTIFICATION POINT D'ACCÈS
22g
GÉNÉRATEUR CLÉ
22h
22f
DE 24
SUPERVISION BOUTON POUSSOIR
COLLECTE DES VARIABLES
DÉCHIFFREMENT INFORMATION DE CONF.
22b
22d
GESTION CONNEXION COURTE PORTÉE
ENVOI / RÉCEPTION DONNÉES RADIO
22c
22i
GESTION CONNEXION LONGUE PORTÉE

FIG.4b.

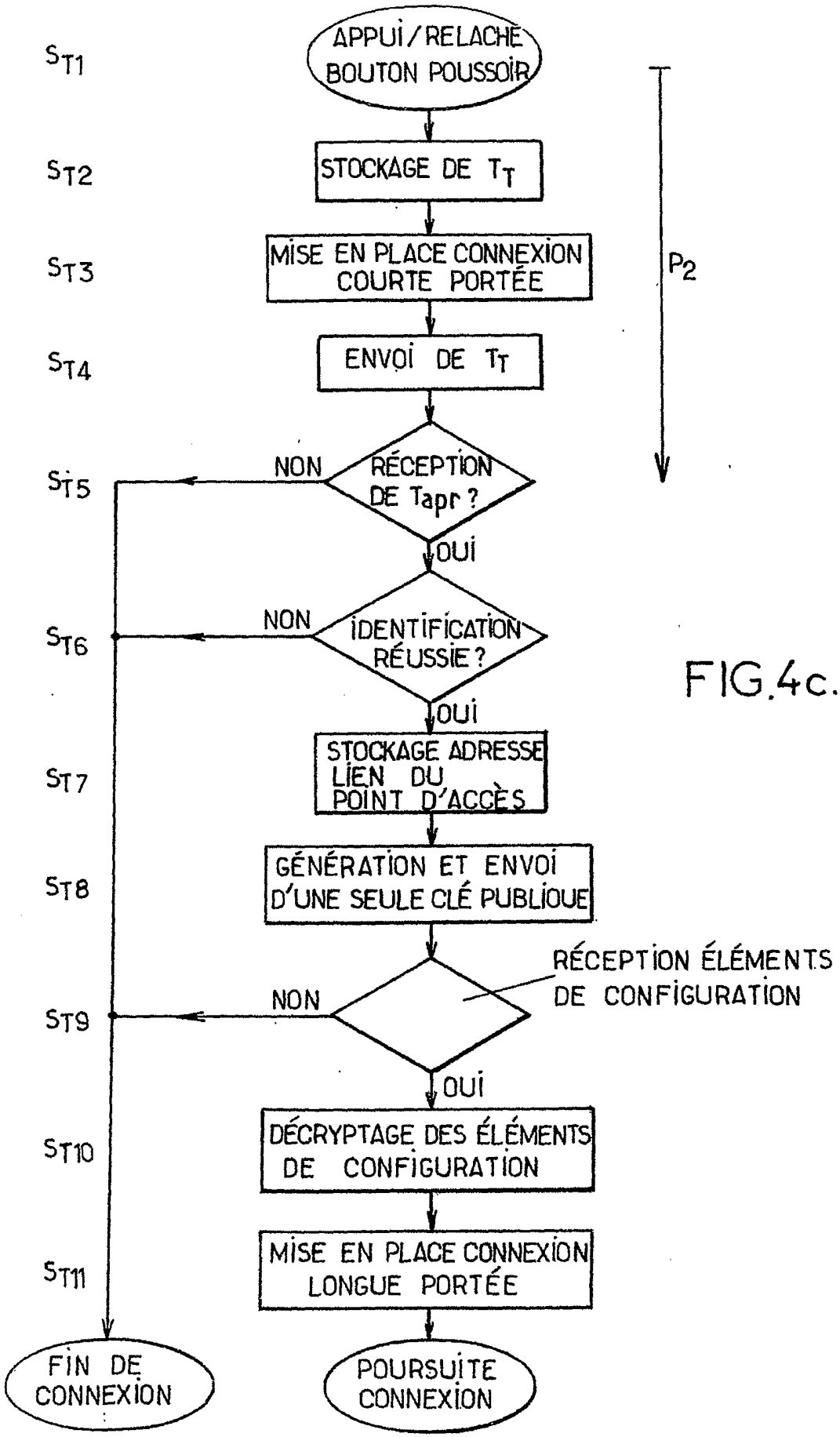

APPUI / RELACHE BOUTON POUSSOIR
STOCKAGE DE T_T
MISE EN PLACE CONNEXION COURTE PORTÉE
ENVOI DE T_T
RÉCEPTION DE Tapr ?
NON
OUI
IDENTIFICATION RÉUSSIE ?
NON
OUI
STOCKAGE ADRESSE LIEN DU POINT D'ACCÈS
GÉNÉRATION ET ENVOI D'UNE SEULE CLÉ PUBLIQUE
RÉCEPTION ÉLÉMENTS DE CONFIGURATION
NON
OUI
DÉCRYPTAGE DES ÉLÉMENTS DE CONFIGURATION
MISE EN PLACE CONNEXION LONGUE PORTÉE
FIN DE CONNEXION
POURSUITE CONNEXION
S_{T1}
S_{T2}
S_{T3}
S_{T4}
S_{T5}
S_{T6}
S_{T7}
S_{T8}
S_{T9}
S_{T10}
S_{T11}
P_2

FIG.4c.

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2006/001101

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06

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

B. FIELDS SEARCHED

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

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	TANENBAUM: "Computer networks" 2003, PRENTICE HALL , XP002362000 page 33, line 17 - page 33, line 18	15
A	EP 1 432 199 A (MITSUBISHI DENKI KABUSHIKI KAISHA) 23 June 2004 (2004-06-23) paragraphs [0011], [0012], [0019] - [0023]	1-19
A	HAARTSEN J C: "THE BLUETOOTH RADIO SYSTEM" IEEE PERSONAL COMMUNICATIONS, IEEE COMMUNICATIONS SOCIETY, US, vol. 7, no. 1, February 2000 (2000-02), pages 28-36, XP000908653 ISSN: 1070-9916 page 35, right-hand column, line 20 - page 35, right-hand column, line 28	1,8,11, 14-16,18

-/--

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 September 2006	25/09/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Goller, Wolfgang

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2006/001101

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 820 266 A (GEMPLUS) 2 August 2002 (2002-08-02) abstract claim 2	1,8,11, 14-16,18

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2006/001101

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1432199 A	23-06-2004	CN 1509012 A	30-06-2004
		JP 2004200785 A	15-07-2004
		US 2004114561 A1	17-06-2004
FR 2820266 A	02-08-2002	EP 1358748 A2	05-11-2003
		WO 02060151 A2	01-08-2002

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2006/001101

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

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

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

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

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

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

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	TANENBAUM: "Computer networks" 2003, PRENTICE HALL , XP002362000 page 33, ligne 17 - page 33, ligne 18	15
A	EP 1 432 199 A (MITSUBISHI DENKI KABUSHIKI KAISHA) 23 juin 2004 (2004-06-23) alinéas [0011], [0012], [0019] - [0023]	1-19
A	HAARTSEN J C: "THE BLUETOOTH RADIO SYSTEM" IEEE PERSONAL COMMUNICATIONS, IEEE COMMUNICATIONS SOCIETY, US, vol. 7, no. 1, février 2000 (2000-02), pages 28-36, XP000908653 ISSN: 1070-9916 page 35, colonne de droite, ligne 20 - page 35, colonne de droite, ligne 28	1,8,11, 14-16,18

-/--

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

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

* Catégories spéciales de documents cités:

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

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

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

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

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

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

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

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

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

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
15 septembre 2006	25/09/2006

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Goller, Wolfgang

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2006/001101

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	FR 2 820 266 A (GEMPLUS) 2 août 2002 (2002-08-02) abrégé revendication 2 _____	1,8,11, 14-16,18

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2006/001101

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 1432199	A	23-06-2004	CN	1509012 A	30-06-2004
			JP	2004200785 A	15-07-2004
			US	2004114561 A1	17-06-2004
FR 2820266	A	02-08-2002	EP	1358748 A2	05-11-2003
			WO	02060151 A2	01-08-2002