

①9 RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
COURBEVOIE

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

3 146 565

②1 N° d'enregistrement national : 23 02059

⑤1 Int Cl⁸ : H 04 W 12/50 (2023.01), H 04 B 7/14

⑫

DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 06.03.23.

③0 Priorité :

④3 Date de mise à la disposition du public de la demande : 13.09.24 Bulletin 24/37.

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

⑥0 Références à d'autres documents nationaux apparentés :

○ Demande(s) d'extension :

⑦1 Demandeur(s) : SOFTATHOME Société Anonyme — FR.

⑦2 Inventeur(s) : FERABOLI Quentin et GRAUL Alexis.

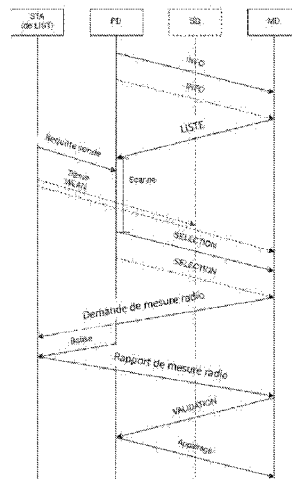
⑦3 Titulaire(s) : SOFTATHOME Société Anonyme.

⑦4 Mandataire(s) : IPAZ.

⑤4 PROCÉDE D'APPAIRAGE AUTOMATIQUE D'AU MOINS UN DISPOSITIF D'APPARIEMENT A UN RESEAU ET SYSTEME ASSOCIE.

⑤7 Procédé d'appairage automatique d'au moins un dispositif d'appariement (PD) à un réseau, le procédé comprenant les étapes suivantes:

- détection de dispositifs du réseau (AD) compatibles à l'appairage,
 - échange de données entre le dispositif d'appariement (PD) et un des dispositifs détectés compatibles du réseau (AD) devenant un dispositif direct (DD),
 - envoi au dispositif d'appariement (PD) d'une liste de dispositifs (STA),
 - surveillance des dispositifs de la liste (STA) grâce à la puissance du signal reçu par chacun d'entre eux, celui ayant la puissance reçue la plus élevée et dépassant un seuil prédéterminé étant le dispositif tiers de confiance (TTP STA),
 - surveillance du dispositif d'appariement (PD) via le dispositif tiers de confiance (TTP STA) grâce à la puissance du signal reçu, le dispositif d'appariement étant considéré comme fiable à l'appairage si son signal reçu dépasse un seuil prédéterminé,
 - envoi des informations de connexion.
- Figure pour l'abrégé : Fig. 3



FR 3 146 565 - A1



Description

Titre de l'invention : PROCÉDE D'APPAIRAGE AUTOMATIQUE D'AU MOINS UN DISPOSITIF D'APPARIEMENT A UN RESEAU ET SYSTEME ASSOCIE

Domaine technique

[0001] La présente invention concerne un procédé d'appairage automatique d'au moins un dispositif d'appariement à un réseau de communication via un dispositif tiers de confiance. Elle concerne aussi un système associé audit procédé.

Etat de la technique antérieure

[0002] La technologie Wi-Fi est aujourd'hui disponible dans une multitude de dispositifs de plus en plus grande et l'appairage de certains dispositifs se révèle contraignante à l'usage. Des dispositifs, ne disposant pas d'interface utilisateur, nécessitent parfois d'utiliser des méthodes telles que l'appairage WPS ou de passer par des applications tierces afin de transmettre les informations de connexion et de permettre l'appairage de nouveaux dispositifs à un réseau WLAN sécurisé utilisant par exemple la norme WPA2.

[0003] Dans le cas du WPS, il est nécessaire d'effectuer un appui bouton sur chaque dispositif impliqué dans le mécanisme d'appairage et dans un délai de deux minutes. Si les deux dispositifs se trouvent loin l'un de l'autre, cela peut rendre plus compliqué l'appairage à l'usage.

[0004] Dans le cas de l'utilisation d'une application, cela implique l'installation de ladite application et son utilisation avec un grand nombre d'appuis et d'entrées sur celle-ci.

[0005] Un exemple concret est l'appairage d'un décodeur ou d'un répéteur à une passerelle domestique haut débit. Aujourd'hui, la méthode la plus commune est le WPS, qui de plus, est de plus en plus abandonné par soucis de sécurité.

[0006] Le but de la présente invention est de résoudre au moins un de ces inconvénients par un nouveau procédé d'appairage automatique d'au moins un dispositif d'appariement à un réseau de communication.

Exposé de l'invention

[0007] Cet objectif est atteint avec un procédé d'appairage automatique d'au moins un dispositif d'appariement à un réseau de communication via un dispositif tiers de confiance situé à proximité dudit dispositif d'appariement, au moins un dispositif maître étant connecté audit réseau, le procédé comprenant les étapes suivantes :

[0008] - détection de dispositifs du réseau compatibles à l'appairage par le dispositif d'appariement,

[0009] - échange de données de connexion et d'identification entre le dispositif

- d'appariement et un des dispositifs détectés compatibles du réseau, le dispositif détecté compatible du réseau choisi pour l'échange devenant un dispositif direct,
- [0010] - envoi au dispositif d'appariement par le dispositif direct, une liste de dispositifs pouvant être considérés comme dispositif tiers de confiance,
- [0011] - surveillance des dispositifs de la liste par le dispositif d'appariement grâce à la puissance du signal reçu par chacun d'entre eux, celui ayant la puissance reçue la plus élevée et dépassant un seuil prédéterminé étant choisi comme le dispositif tiers de confiance,
- [0012] - surveillance du dispositif d'appariement par le dispositif direct via le dispositif tiers de confiance grâce à la puissance du signal reçu, le dispositif d'appariement étant considéré comme fiable à l'appairage si son signal reçu dépasse un seuil prédéterminé,
- [0013] - envoi des informations de connexion du dispositif maître par le dispositif direct au dispositif d'appariement fiable à l'appairage.
- [0014] La présente invention permet l'appairage sécurisé d'un dispositif WLAN à un dispositif WLAN maître, tel qu'une passerelle haut-débit, avec un minimum d'actions de la part de l'utilisateur. On entend par dispositif d'appariement, tous types de dispositifs pouvant être connectés à un dispositif maître. Afin d'appairer le dispositif d'appariement au dispositif maître, l'utilisateur utilise un dispositif WLAN tierce (tel qu'un téléphone portable) permettant d'authentifier le dispositif d'appariement auprès du dispositif maître pour que ce dernier fournisse les informations nécessaires à la connexion au dispositif d'appariement et permette son appairage. Le dispositif qui sert de dispositif tiers de confiance, doit se trouver à proximité du dispositif relais afin de valider que ce dernier peut accéder aux informations de connexion.
- [0015] Le but de l'invention est que l'utilisateur branche électriquement le dispositif d'appariement et qu'il se connecte automatiquement au dispositif maître, tel qu'une passerelle domestique par exemple. L'invention permet de minimiser au maximum le nombre d'interaction de l'utilisateur.
- [0016] L'invention offre une solution d'association de dispositifs tels qu'un répéteur ou un décodeur TV, cette association étant réalisée toujours au bon moment au bon endroit.
- [0017] L'invention ne nécessite pas d'écran, ni de boutons et permet la réduction des interactions pour appairer l'équipement. Elle facilite la procédure (pas de nécessité d'entrer les identifiants de connexion, l'action est simple : déplacer un appareil déjà connecté à ce même réseau vers l'appareil qu'on souhaite connecter).
- [0018] L'invention peut s'appliquer à tout protocole de communication permettant l'envoi chiffré de données et pouvant solliciter des mesures radio de leur environnement.
- [0019] L'invention peut être intégrée à tout type d'équipements disposant du Wi-Fi et peut être même normalisée afin d'étendre le nombre d'équipements compatibles avec la procédure.

- [0020] Dans un cadre plus restrictif, elle pourrait faciliter l'appairage d'équipements d'un même fabricant.
- [0021] La notion de proximité, qui est vérifiée par les deux équipements (celui qu'on souhaite appairer et celui de confiance) de manière symétrique sécurise la procédure et est protégé par le chiffrement des données envoyées.
- [0022] Cette proximité étant configurable, on peut imaginer deux scénarios : l'équipement de confiance peut être "coller" à l'équipement à appairer et agir comme un dispositif NFC ou bien l'équipement peut se trouver à moins d'un demi mètre (par exemple la poche de l'utilisateur final), ce dernier pouvant être averti par une notification via une application tierce de l'appairage. L'étape d'échange de données de connexion et d'identification entre le dispositif d'appariement et un des dispositifs détectés compatibles du réseau peut comprendre au moins une étape suivante :
- [0023] - envoi par le dispositif d'appariement au dispositif direct des données de connexion dudit dispositif d'appariement,
- [0024] - authentification des données de connexion du dispositif d'appariement reçue par le dispositif direct par le dispositif maitre,
- [0025] - envoi par le dispositif direct au dispositif d'appariement des données de connexion du dispositif maitre,
- [0026] - authentification des données de connexion du dispositif maitre par le dispositif d'appariement.
- [0027] Le dispositif direct peut correspondre au dispositif maitre ou à un dispositif relai.
- [0028] L'étape d'échange de données de connexion et d'identification entre le dispositif d'appariement et un des dispositifs détectés compatibles du réseau, peut également comprendre l'étape suivante :
- [0029] - envoi des informations d'identification du dispositif d'appariement au dispositif direct.
- [0030] Les échanges de données entre chaque dispositif peuvent être réalisés en fonction d'un type d'action, le type d'action correspondant à au moins une des actions suivantes:
- [0031] - information
- [0032] - liste
- [0033] - sélection
- [0034] - validation
- [0035] - requête
- [0036] - interrogation
- [0037] - réponse
- [0038] Les données de connexion peuvent comprendre au moins un certificat d'identification.

- [0039] Les données d'identification peuvent comprendre une adresse MAC du dispositif maitre et un nom du réseau.
- [0040] L'adresse MAC du dispositif maitre correspond au BSSID, « Basic Service Set Identifier » et le nom du réseau correspond au SSID, « Service Set Identifier ». L'adresse Mac, « Media Access Control » correspond à l'adresse physique d'un dispositif réseau.
- [0041] Les échanges de données entre chaque dispositif peuvent être réalisés par l'intermédiaire d'au moins une trame Wi-Fi standardisée.
- [0042] Ces trames Wi-Fi standardisées permettent l'envoi de données sans nécessité au transmetteur et au receveur d'être sur le même réseau WLAN.
- [0043] La trame Wi-Fi standardisée peut contenir au moins une donnée relative :
- [0044] - à un type d'action lié à l'envoi de la trame Wi-Fi standardisée,
- [0045] - aux données relatives à l'action.
- [0046] La liste de dispositifs peut être envoyée sous forme de trame Wi-Fi standardisée comprenant l'ensemble des adresses MAC des dispositifs de la liste, ainsi que le canal et la bande de fréquence utilisés par chaque dispositif de la liste.
- [0047] Ces données permettent au dispositif d'appariement d'analyser chacune des STA.
- [0048] Suivant un autre aspect de l'invention, il est proposé un système comprenant au moins un dispositif maitre connecté à un réseau, au moins un dispositif du système comprenant une unité de traitement configurée pour mettre en œuvre un procédé selon l'invention.
- [0049] Suivant encore un autre aspect de l'invention, il est proposé un produit programme d'ordinateur comprenant des instructions qui, lorsque le programme est exécuté par une unité de traitement dans l'au moins un dispositif du réseau, conduit celui-ci à mettre en œuvre le procédé selon l'invention.

Description des figures et modes de réalisation

- [0050] D'autres avantages et particularités de l'invention apparaîtront à la lecture de la description détaillée de mises en œuvre et de modes de réalisation nullement limitatifs, et des dessins annexés suivants :
- [0051] [Fig.1a] illustre une première configuration de système de dispositifs selon l'invention,
- [0052] [Fig.1b] illustre une deuxième configuration de système de dispositifs selon l'invention,
- [0053] [Fig.2] décrit l'étape de détection d'un équipement et échange des données de connexion du procédé selon l'invention.
- [0054] [Fig.3] décrit l'étape de sélection de du dispositif tiers de confiance et l'étape d'appairage du procédé selon l'invention.
- [0055] Ces modes de réalisation étant nullement limitatifs, on pourra notamment considérer

des variantes de l'invention ne comprenant qu'une sélection de caractéristiques décrites ou illustrées par la suite isolées des autres caractéristiques décrites ou illustrées (même si cette sélection est isolée au sein d'une phrase comprenant ces autres caractéristiques), si cette sélection de caractéristiques est suffisante pour conférer un avantage technique ou pour différencier l'invention par rapport à l'état de la technique antérieure. Cette sélection comprend au moins une caractéristique de préférence fonctionnelle sans détails structurels, et/ou avec seulement une partie des détails structurels si cette partie uniquement est suffisante pour conférer un avantage technique ou à différencier l'invention par rapport à l'état de la technique antérieure.

- [0056] On va tout d'abord décrire, en référence aux figures 1a et 1b, des configurations de systèmes de dispositifs appartenant à un même réseau internet dans lequel le procédé selon l'invention est appliqué. Chaque dispositif dispose d'un système qui est configurable par le biais d'une liste de paramètres. Ce système dispose également d'une mémoire permettant d'enregistrer des informations nécessaires à la suite de la procédure.
- [0057] Le dispositif relai SD que l'utilisateur souhaite appairer à un dispositif d'appariement PD dispose d'une fonctionnalité de point d'accès qui doit être active pendant la procédure ainsi qu'une fonctionnalité de point de connexion qui est également active afin d'effectuer l'appairage.
- [0058] La topologie des figures 1a et 1b comprend :
- [0059] - un dispositif d'appariement PD, « Pairing Device »,
- [0060] - un dispositif tiers de confiance TTP STA, et
- [0061] - un ensemble de dispositifs AD, « Authenticator Devices », qui correspond à un ensemble de dispositifs relais SD et maître MD connecté à un même réseau désigné par AD,
- [0062] La topologie du réseau AD peut comprendre :
- [0063] - soit un dispositif maître MD, « Master Device » (voir [Fig.1a]),
- [0064] - soit un dispositif maître MD et d'un ou plusieurs dispositifs relais SD, « Slave Device » pouvant faire office de relai (voir [Fig.1b]).
- [0065] Le dispositif qui communique en direct avec le dispositif d'appariement PD est désigné comme le dispositif direct DD, « Direct Device ». Le dispositif direct DD peut correspondre au dispositif maître MD (voir [Fig.1a]) ou à un dispositif relai SD (voir [Fig.1b]). Lorsque le dispositif direct DD correspond à un dispositif relai SD, le dispositif relai SD transfère automatiquement les informations reçues au dispositif maître MD et le dispositif maître MD transmet les informations au dispositif relai SD pour qu'il les envoie au dispositif d'appariement PD.
- [0066] En référence à la [Fig.2], on décrit l'étape de détection d'un équipement et échange des données de connexion du procédé selon l'invention.

- [0067] Le procédé selon l'invention est initié par le dispositif d'appariement PD. Le déclenchement peut se faire de manière automatique ou être lancé par l'utilisateur lui-même à l'aide d'un bouton logiciel ou matériel. La première étape du procédé consiste à la détection des dispositifs compatibles avec ladite invention.
- [0068] Chaque dispositif, supportant l'invention et l'ayant activé dans son système, doit émettre dans des trames balises « beacons » ou « probe responses » comportant les informations relatives au support de la procédure. Ces informations peuvent être transmises au travers d'un champ des trames cités précédemment dit « Vendor Information Element ». Les informations présentées sont le support ou non de la procédure, si le dispositif est maître MD ou dispositif relai SD du réseau auquel il appartient et un identifiant unique relatif à ce réseau.
- [0069] Le dispositif d'appariement PD analyse son environnement radio en effectuant un scan et enregistre en mémoire, l'ensemble des dispositifs supportant ladite invention. Les dispositifs détectés sont triés par la puissance du signal reçu par le dispositif d'appariement PD, du plus fort au plus faible. Ensuite, le dispositif d'appariement PD envoie à l'ensemble des dispositifs détectés ses données de connexion qui comprennent son certificat. Si aucun dispositif n'a été détecté la procédure est annulée.
- [0070] Chaque dispositif de l'invention doit au préalable détenir un certificat émis par un tiers de confiance avec un jeu de clés publique et privée. Les échanges de données entre chaque dispositif du réseau AD se font par l'intermédiaire de trames Wi-Fi standardisée de type « Public Action Frame ». La trame contient les données relatives :
- [0071] - au type d'action lié à l'envoi de la trame,
 - [0072] - aux données relatives à l'action.
- [0073] Le dispositif d'appariement PD transmet à l'ensemble des dispositifs détectés ses données de connexion qui comprennent son certificat ainsi que sa clé publique. Il envoie donc une trame « Public Action Frame » (PAF) avec pour type d'action l'initialisation de la procédure (Requête) et transmet en données son certificat et un numéro de séquence. La longueur du jeu de données du certificat pouvant excéder la taille d'une trame 802.11 MPDU, l'envoi peut se faire en plusieurs parties à l'aide de plusieurs trames PAF. Le numéro de séquence permet l'ordonnance des données afin de reconstituer le certificat par les dispositifs destinataires.
- [0074] Chaque dispositif ayant reçu une trame PAF avec comme type d'action Requête relaye au dispositif maître MD de son réseau les données reçues dans la trame et indique à quelle puissance le signal d'émission de la trame a été reçu. Si un dispositif maître MD reçoit la trame, il n'a pas besoin de relayer cette trame et est considéré comme le dispositif direct DD. Si les données ont été relayées par un ou plusieurs dispositifs relais SD de son réseau, le dispositif maître MD, lors de l'envoi d'une réponse vers le dispositif d'appariement PD, doit transmettre ses données au dispositif relai SD

ayant reçu la trame Requête au plus fort niveau de puissance mesuré de l'ensemble des dispositifs relais SD. Ce dispositif relais SD assure l'envoi des trames Wi-Fi standardisé PAF et via le protocole 802.11k pour la suite de la procédure et sert de relai vers le dispositif maître MD. Il est alors désigné comme étant le dispositif direct DD.

- [0075] Le dispositif maître MD de chaque réseau va tout d'abord authentifier le certificat afin de déterminer s'il a été fourni par un dispositif considéré comme de confiance pour valider la suite de la procédure. Le certificat émis par le dispositif d'appariement PD doit être rattaché à une organisation connue et validée par le dispositif maître MD. Si le certificat n'est pas valide, le dispositif ayant reçu la trame Requête ne répond pas au dispositif ayant envoyé cette même trame.
- [0076] Si le certificat est valide, le dispositif direct DD répond au dispositif d'appariement PD par une trame PAF pour transmettre à son tour son certificat. Cette trame a pour type d'action une réponse « Réponse » et transmet dans ses données son certificat et un numéro de séquence. Comme dans le cas de l'envoi d'une trame Requête, la taille de la trame PAF peut être insuffisante pour supporter la longueur totale du certificat, le numéro de séquence va servir à la reconstitution du certificat.
- [0077] Le dispositif d'appariement PD authentifie à son tour le certificat reçu afin de déterminer si le dispositif maître MD du réseau auquel il veut s'appairer a été fourni par un dispositif considéré comme de confiance, validant ainsi la suite de la procédure et pouvant faire l'envoi de ses informations. Le certificat émis par le dispositif maître MD doit être rattaché à une organisation connue et validée par le dispositif d'appariement PD pour être considéré de confiance. Si le certificat n'est pas valide, le dispositif d'appariement PD annule la procédure avec le dispositif direct DD ayant émis la trame Réponse. S'il n'y a plus de dispositifs compatibles valides, la procédure est annulée.
- [0078] Un type de trame supplémentaire est également présente afin de permettre le rejeu des deux trames d'actions précédentes dans des cas d'erreur comme un certificat ou une clé incomplets. Cette trame est définie par le type d'action « Interrogation » et doit indiquer la trame d'action qu'elle sollicite (Requête ou Réponse). Si au bout d'un nombre configurable d'envois de trame Interrogation, la complétion d'une des deux étapes précédentes n'a pas abouti, la procédure est terminée respectivement côté dispositif du réseau AD pour la trame Interrogation d'une trame Requête et côté dispositif d'appariement PD pour la trame Interrogation d'une trame Réponse, ce dernier annule la procédure pour le dispositif du réseau AD sollicité. Un nombre configurable de trames Interrogation reçus permet également d'empêcher des sollicitations abusives et d'ignorer toute trame Interrogation dépassant ce nombre.
- [0079] En référence à la [Fig.3], nous décrivons l'étape de sélection de du dispositif tiers de confiance et l'étape d'appairage du procédé selon l'invention.

- [0080] A partir de cette étape, le contenu de l'ensemble des trames envoyées avec des trames de type « Public Action Frame » PAF est crypté chiffré à l'aide de la clé publique du dispositif destinataire et signé par la clé privée du dispositif émetteur. Si un dispositif n'est pas capable de déchiffrer avec sa clé privée et authentifier par la signature l'émetteur une trame, la procédure est annulée pour le couple émetteur et destinataire, le dispositif d'appariement PD pouvant poursuivre la procédure avec un autre dispositif du réseau compatible ou l'annuler s'il n'y a plus de dispositifs compatibles disponibles.
- [0081] Le dispositif d'appariement PD envoie ses informations d'identification à au dispositif direct DD. Ces informations contiennent son BSSID et son SSID. Ces informations sont sauvegardées par le dispositif maitre MD en mémoire et seront réutilisées dans la suite de la procédure. Le dispositif d'appariement PD envoie ses informations à l'aide d'une trame contenant le type d'action Info (pour information), son BSSID et son SSID.
- [0082] Le dispositif d'appariement PD passe alors en attente de la réception des informations nécessaires pour la suite de la procédure, envoyées pour chaque dispositif du réseau AD qui ont reçu la trame Info. Un minuteur d'une durée configurable est déclenché au bout duquel, une fois terminé, le dispositif d'appariement PD peut de nouveau envoyer une trame Info et re-déclencher le minuteur. Le dispositif d'appariement PD peut répéter l'opération un nombre configurable de fois. Si la réception des informations n'aboutit pas, le dispositif d'appariement PD annule la procédure avec le dispositif direct DD avec lequel il communique.
- [0083] Le dispositif direct DD ayant reçu une trame INFO répond avec une liste de dispositifs (STA) dont l'un sera sélectionné comme dispositif tiers de confiance dans la suite de la procédure. La liste de dispositifs (STA) est donnée par le dispositif maitre MD.
- [0084] Le dispositif maitre MD crée donc une liste de dispositifs STA. Pour être présente dans la liste, le dispositif STA répond aux conditions suivantes :
- [0085] - Supporter le standard IEEE 802.11k (« Radio resource measurement »),
 - [0086] - Supporter le standard IEEE 802.11w (« Protected Management Frame »),
 - [0087] - Être associée en Wi-Fi à un des dispositifs de du réseau AD.
- [0088] Le support des standards IEEE 802.11k et IEEE 802.11w est annoncé à la connexion du dispositif STA lors de l'envoi d'une trame Requête d'association ou « Association Request ».
- [0089] Le dispositif direct DD envoie au dispositif d'appariement PD la liste des dispositifs STA avec une trame ayant une action de type « Liste ». Cette trame contient dans ses données l'ensemble des adresses MAC des dispositifs STA de la liste, ainsi que le canal et la bande de fréquence utilisés par chaque dispositif STA. Si plusieurs dis-

positifs du réseau AD envoie une trame Liste contenant une même adresse MAC, le dispositif d'appariement PD annule la procédure avec les dispositifs du réseau AD concernés.

- [0090] A la réception de la trame Liste, le dispositif d'appariement PD surveille chacun des dispositifs STA présents dans la liste et mesure la puissance reçue des signaux Wi-Fi qu'ils émettent. Si la puissance reçue mesurée d'un des dispositifs STA de la liste dépasse un seuil prédéterminé, le dispositif STA est alors désigné comme dispositif tiers de confiance (TTP STA, « trusted third party » STA). Le dispositif d'appariement PD arrête la surveillance des autres dispositifs STA et informe le dispositif direct DD. Si aucun dispositif STA n'est désigné comme dispositif tiers de confiance TTP STA après une durée configurable, le dispositif d'appariement PD passe à la liste de dispositif STA reçue dans la trame Liste du dispositif du réseau AD suivant en fonction de la puissance du signal reçu. Si toutes les listes ont été traitées, la procédure est annulée.
- [0091] Une fois le tiers de confiance TTP STA sélectionné par le dispositif d'appariement PD, ce dernier informe le dispositif direct DD de son choix. Le dispositif d'appariement PD transmet l'information grâce à une trame ayant une action de type « Sélection ». Cette trame contient les informations relatives au dispositif tiers de confiance TTP STA tel que son adresse MAC, le canal sur lequel il a été détecté, ainsi que le niveau de puissance à laquelle le dispositif d'appariement PD l'a mesuré.
- [0092] Le dispositif d'appariement PD passe alors en attente de la réception d'une trame « Validation » qui sera décrite plus bas. Un minuteur d'une durée configurable est déclenché au bout duquel, une fois terminé, le dispositif d'appariement PD peut de nouveau envoyer une trame Sélection et re-déclencher le minuteur. Le dispositif d'appariement PD peut répéter l'opération un nombre configurable de fois. Si la réception de la trame attendue n'aboutit pas, le dispositif d'appariement PD annule la procédure avec le dispositif direct DD et met fin à la procédure complète.
- [0093] A la réception de la trame Sélection, le dispositif maître MD vérifie si le dispositif tiers de confiance TTP STA appartient à la liste d'origine et si le niveau de puissance mesuré par le dispositif d'appariement PD est supérieur à un seuil prédéterminé. Si ces conditions sont remplies, le dispositif maître MD valide le dispositif de la liste STA comme étant dispositif tiers de confiance TTP STA. Le dispositif direct DD transmet l'information au dispositif d'appariement PD.
- [0094] Le dispositif d'appariement est alors surveillé à son tour par le dispositif direct DD via le dispositif tiers de confiance TTP STA grâce à la puissance du signal reçu via un protocole 802.11k. Le dispositif d'appariement PD est considéré comme fiable à l'appairage si son signal reçu dépasse un seuil prédéterminé.
- [0095] Une fois que le dispositif d'appariement est considéré comme fiable à l'appairage, les

informations de connexion du dispositif maître MD sont envoyées par le dispositif direct DD au dispositif d'appariement PD. Le dispositif d'appariement s'apparie au réseau.

- [0096] Typiquement au moins un des moyens du dispositif selon l'invention précédemment décrits, de préférence chacun des moyens du dispositif selon l'invention précédemment décrit sont des moyens techniques.
- [0097] Typiquement, chacun des moyens du dispositif selon l'invention précédemment décrits peuvent comprendre au moins un ordinateur, une unité centrale ou de calcul, un circuit électronique analogique (de préférence dédié), un circuit électronique numérique (de préférence dédié), et/ou un microprocesseur (de préférence dédié), et/ou des moyens logiciels.
- [0098] Bien sûr, l'invention n'est pas limitée aux exemples qui viennent d'être décrits et de nombreux aménagements peuvent être apportés à ces exemples sans sortir du cadre de l'invention.
- [0099] Bien entendu, les différentes caractéristiques, formes, variantes et modes de réalisation de l'invention peuvent être associées les unes avec les autres selon diverses combinaisons dans la mesure où elles ne sont pas incompatibles ou exclusives les unes des autres. En particulier toutes les variantes et modes de réalisation décrits précédemment sont combinables entre eux.

Revendications

- [Revendication 1] Procédé d'appairage automatique d'au moins un dispositif d'appariement (PD) à un réseau de communication via un dispositif tiers de confiance (TTP STA) situé à proximité dudit dispositif d'appariement, au moins un dispositif maitre (MD) étant connecté audit réseau, le procédé comprenant les étapes suivantes :
- détection de dispositifs du réseau (AD) compatibles à l'appairage par le dispositif d'appariement (PD),
 - échange de données de connexion et d'identification entre le dispositif d'appariement (PD) et un des dispositifs détectés compatibles du réseau (AD), le dispositif détecté compatible du réseau choisi pour l'échange devenant un dispositif direct (DD),
 - envoi au dispositif d'appariement (PD) par le dispositif direct (DD), une liste de dispositifs (STA) pouvant être considérés comme dispositif tiers de confiance (TTP STA),
 - surveillance des dispositifs de la liste (STA) par le dispositif d'appariement (PD) grâce à la puissance du signal reçu par chacun d'entre eux, celui ayant la puissance reçue la plus élevée et dépassant un seuil prédéterminé étant choisi comme le dispositif tiers de confiance (TTP STA),
 - surveillance du dispositif d'appariement (PD) par le dispositif direct (DD) via le dispositif tiers de confiance (TTP STA) grâce à la puissance du signal reçu, le dispositif d'appariement (PD) étant considéré comme fiable à l'appairage si son signal reçu dépasse un seuil prédéterminé,
 - envoi des informations de connexion du dispositif maitre (MD) par le dispositif direct (DD) au dispositif d'appariement (PD) fiable à l'appairage.
- [Revendication 2] Procédé d'appairage automatique selon la revendication 1, dans lequel l'étape d'échange de données de connexion et d'identification entre le dispositif d'appariement (PD) et un des dispositifs détectés compatibles du réseau (AD) comprend au moins une étape suivante :
- envoi par le dispositif d'appariement (PD) au dispositif direct (DD) des données de connexion dudit dispositif d'appariement (PD),
 - authentification des données de connexion du dispositif d'appariement (PD) reçue par le dispositif direct (DD) par le dispositif maitre (MD),
 - envoi par le dispositif direct (DD) au dispositif d'appariement (PD) des données de connexion du dispositif maitre (MD),

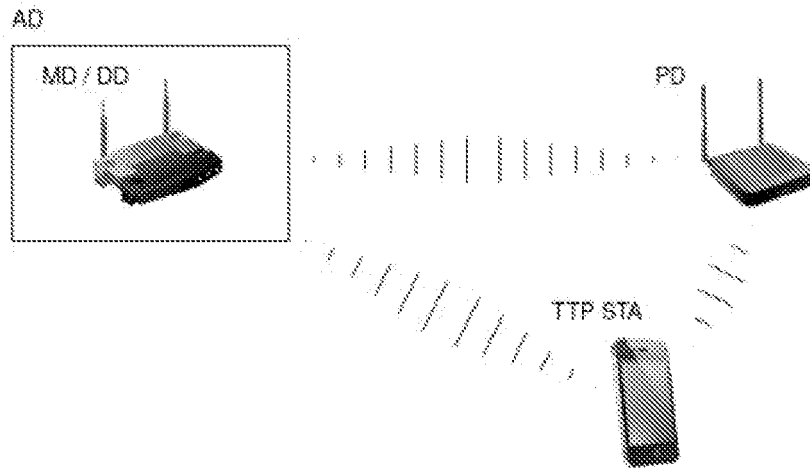
- authentification des données de connexion du dispositif maitre (MD) par le dispositif d'appariement (PD).
- [Revendication 3] Procédé d'appairage automatique selon l'une quelconque des revendications 1 à 2, dans lequel le dispositif direct (DD) correspond au dispositif maitre (MD) ou à un dispositif relai (SD).
- [Revendication 4] Procédé d'appairage automatique selon l'une quelconque des revendications 1 à 3, dans lequel l'étape d'échange de données de connexion et d'identification entre le dispositif d'appariement (PD) et un des dispositifs détectés compatibles du réseau (AD), comprend également l'étape suivante :
- envoi des informations d'identification du dispositif d'appariement (PD) au dispositif direct (DD).
- [Revendication 5] Procédé d'appairage automatique selon l'une quelconque des revendications 1 à 4, dans lequel les échanges de données entre chaque dispositif sont réalisés en fonction d'un type d'action, le type d'action correspondant à au moins une des actions suivantes :
- information
 - liste
 - sélection
 - validation
 - requête
 - interrogation
 - réponse
- [Revendication 6] Procédé d'appairage automatique selon l'une quelconque des revendications 1 à 5, dans lequel les données de connexion comprennent au moins un certificat d'identification.
- [Revendication 7] Procédé d'appairage automatique selon l'une quelconque des revendications 1 à 6, dans lequel les données d'identification comprennent une adresse MAC du dispositif maitre et un nom du réseau.
- [Revendication 8] Procédé d'appairage automatique selon l'une quelconque des revendications 1 à 7, dans lequel les échanges de données entre chaque dispositif sont réalisés par l'intermédiaire d'au moins une trame Wi-Fi standardisée.
- [Revendication 9] Procédé d'appairage automatique selon la revendication 8, dans lequel la trame Wi-Fi standardisée contient au moins une donnée relative :
- à un type d'action lié à l'envoi de la trame Wi-Fi standardisée,
 - aux données relatives à l'action.
- [Revendication 10] Procédé d'appairage automatique selon l'une quelconque des reven-

dications 1 à 9, dans lequel la liste de dispositifs (STA) est envoyée sous forme de trame Wi-Fi standardisée comprenant l'ensemble des adresses MAC des dispositifs (STA) de la liste, ainsi que le canal et la bande de fréquence utilisés par chaque dispositif de la liste (STA).

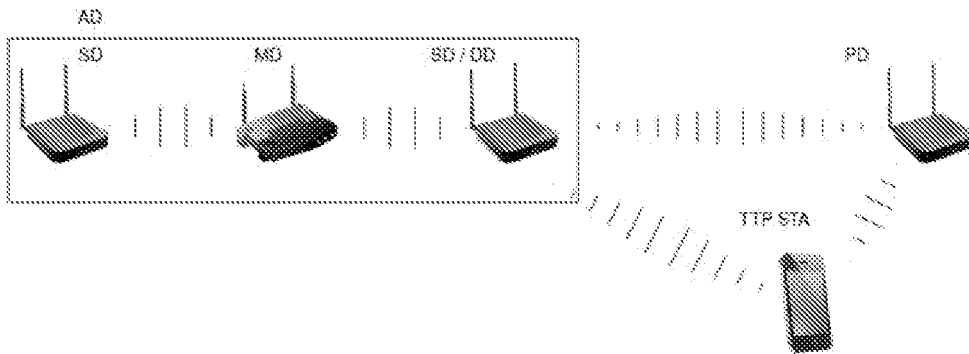
[Revendication 11] Système comprenant au moins un dispositif maître (MD) connecté à un réseau, au moins un dispositif du système comprenant une unité de traitement configurée pour mettre en œuvre un procédé selon l'une quelconque des revendications 1 à 10.

[Revendication 12] Produit programme d'ordinateur comprenant des instructions qui, lorsque le programme est exécuté par une unité de traitement dans l'au moins un dispositif du réseau, conduit celui-ci à mettre en œuvre le procédé selon l'une quelconque des revendications 1 à 10.

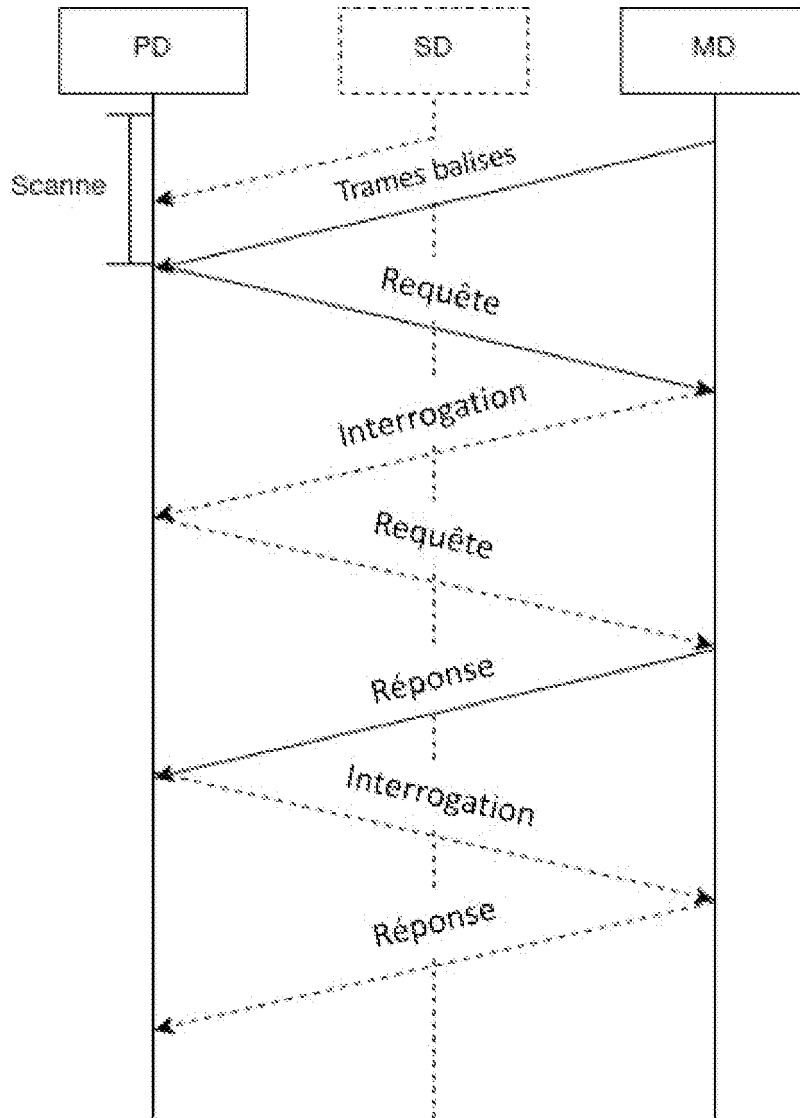
[Fig. 1a]



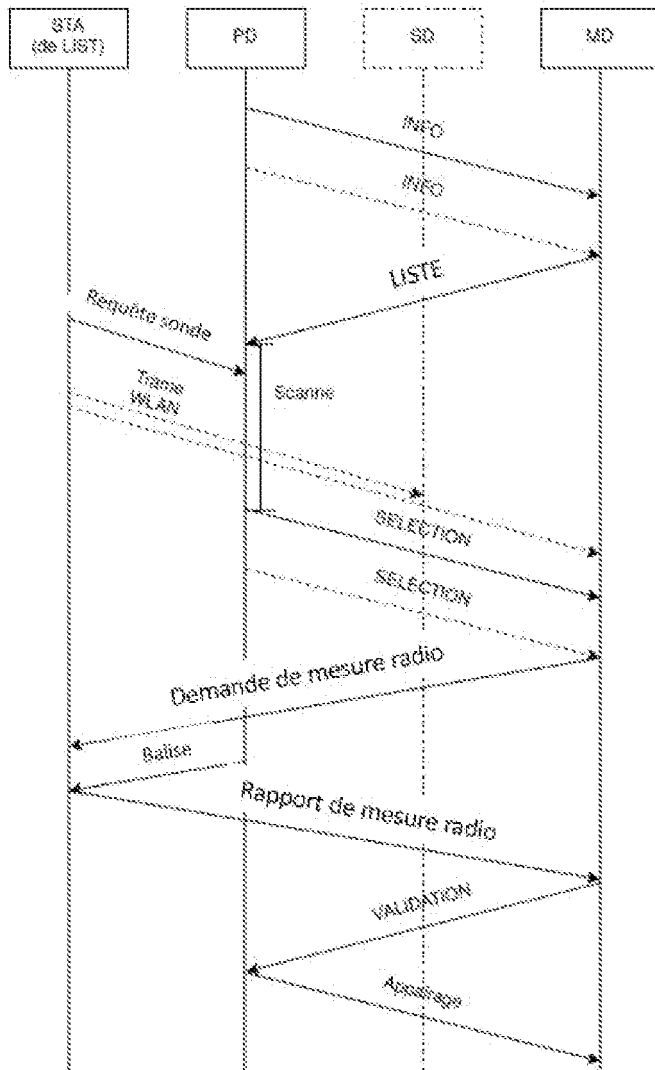
[Fig. 1b]



[Fig. 2]



[Fig. 3]



**RAPPORT DE RECHERCHE
PRÉLIMINAIRE**

N° d'enregistrement
national

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

FA 916610
FR 2302059

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	FR 3 109 692 A1 (ORANGE [FR]) 29 octobre 2021 (2021-10-29)	1-5, 7-12	H04B 7/14 H04W 12/50
Y	* alinéa [0107] - alinéa [0112]; figure 1 * * alinéa [0061] * * alinéa [0056] * * alinéa [0062] - alinéa [0065] * * alinéa [0124] * * alinéa [0092] - alinéa [0097] * -----	6	
Y	US 9 654 449 B2 (LINDTEIGEN TY B [US]; JONES JAMES CHESTER [US]; SAIFE INC [US]) 16 mai 2017 (2017-05-16) * colonne 8, ligne 4 - ligne 10 * -----	6	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04W
Date d'achèvement de la recherche		Examineur	
19 septembre 2023		Padilla Serrano, M	
CATÉGORIE DES DOCUMENTS CITÉS			
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire		T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant	

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2302059 FA 916610**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **19-09-2023**
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 3109692	A1	29-10-2021	AUCUN	

US 9654449	B2	16-05-2017	US 2014112472 A1	24-04-2014
			US 2016021069 A1	21-01-2016
