(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 125 376***

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **21 07683**

(51) Int Cl[8] : ***H 04 W 12/06*** *(2020.12), H 04 L 12/28, H 04 W 4/00, 84/12, H 04 L 29/06*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 16.07.21.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 20.01.23 Bulletin 23/03.

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

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *ORANGE Société Anonyme* — FR.

(72) **Inventeur(s) :** NAJMI Elyass et RALLE Hélène.

(73) **Titulaire(s) :** ORANGE Société Anonyme.

(74) **Mandataire(s) :** CABINET VIDON BREVETS ET STRATEGIE.

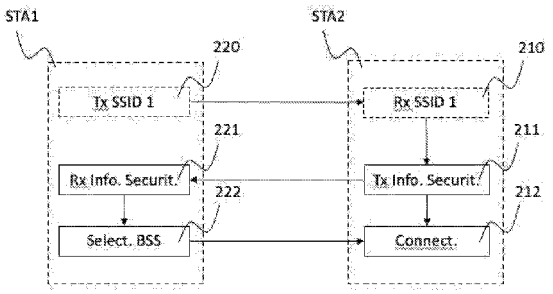
(54) Procédé de connexion entre une première station et une deuxième station dans un réseau de communication sans fil, première station, deuxième station, et programme d'ordinateur correspondants.

(57) Procédé de connexion entre une première station et une deuxième station dans un réseau de communication sans fil, première station, deuxième station, et programme d'ordinateur correspondants.

L'invention concerne un procédé de connexion entre une première station (STA1) et une deuxième station (STA2) dans un réseau de communication sans fil, selon lequel ladite deuxième station (STA2) met en œuvre :

la transmission (211), vers ladite première station (STA1), d'au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station (STA2),la connexion (212) avec un ensemble de services de base auquel appartient ladite première station (STA1), sélectionné par ladite première station en fonction de ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station.

Figure pour l'abrégé : Figure 2



FR 3 125 376 - A1

Description

Titre de l'invention : Procédé de connexion entre une première station et une deuxième station dans un réseau de communication sans fil, première station, deuxième station, et programme d'ordinateur correspondants.

[0001] 1. Domaine de l'invention

[0002] Le domaine de l'invention est celui des télécommunications.

[0003] Plus précisément, l'invention concerne la sécurisation de l'accès à un réseau sans fil, par exemple de type réseau d'accès local sans fil WLAN (« Wireless Local Access Network »).

[0004] 2. Art antérieur

[0005] Un réseau WLAN utilise notamment la technologie de transmission sans fil basée sur la norme de réseau radioélectrique IEEE 802.11 et ses évolutions, communément regroupées sous l'appellation Wi-Fi (en anglais « Wireless Fidelity »). Un tel réseau est communément appelé réseau Wi-Fi.

[0006] Classiquement, un réseau Wi-Fi en mode infrastructure comprend au moins deux stations dont un point d'accès/routeur (ou AP, en anglais « Access Point ») et un terminal client. Pour pouvoir se connecter au point d'accès, par exemple une Livebox – marque déposée, le terminal client doit disposer de trois paramètres : le nom du réseau Wi-Fi (en anglais SSID pour « Service Set Identifier »), une clé Wi-Fi, et un mode de sécurité compatible avec le mode de sécurité configuré au niveau du point d'accès.

[0007] On note que si ces trois paramètres sont validés et mémorisés par le terminal client, il peut se connecter au réseau Wi-Fi. Si l'un de ces trois paramètres change, la configuration n'est plus valide et la connexion peut être refusée.

[0008] Le mode de sécurité permet notamment de protéger les données échangées entre le terminal client et le point d'accès. Par exemple, le mode de sécurité défini par l'organisation « Wi-Fi Alliance » est de type WPA, en anglais « Wi-Fi Protected Access », notamment WPA2 ou WPA3.

[0009] Dans les bandes de fréquence autour de 2,4 GHz ou 5GHz, classiquement utilisées pour la transmission des signaux dans un réseau Wi-Fi, le mode de sécurité principalement utilisé est de type WPA2.

[0010] Dans la bande de fréquence autour de 6 GHz, prochainement utilisée pour la transmission des signaux dans un réseau Wi-Fi, le mode de sécurité recommandé est de type WPA3.

[0011] Un terminal client qui supporte le mode de sécurité WPA2 (ou une version antérieure) peut se connecter à un point d'accès qui supporte les deux modes de sécurité

WPA2 et WPA3. En revanche, un terminal client qui supporte le mode de sécurité WPA2 (ou une version antérieure) ne peut pas se connecter à un point d'accès qui supporte uniquement le mode de sécurité WPA3.

[0012] Un nouveau mode de sécurité, noté WPA3-TM (« Transition Mode »), a donc été défini par l'organisation « Wi-Fi Alliance », pour être utilisé dans des environnements où cohabitent des terminaux supportant le mode de sécurité WPA2 et des terminaux supportant le mode de sécurité WPA3.

[0013] Ainsi, lorsque le réseau, ou le point d'accès, doit gérer plusieurs modes de sécurité, le mode de sécurité à privilégier au niveau du point d'accès est le mode de sécurité WPA3-TM.

[0014] Un inconvénient de l'utilisation de ce mode de sécurité WPA3-TM est qu'il existe, pour certains terminaux (par exemple de type Smartphone, imprimante, TV connectée, etc) des problèmes d'interopérabilité avec les points d'accès activant le mode de sécurité WPA3-TM.

[0015] Il existe donc un besoin pour une nouvelle technique de sécurisation de l'accès à un réseau sans fil.

[0016] 3. Exposé de l'invention

[0017] L'invention propose une solution ne présentant pas l'ensemble des inconvénients de l'art antérieur, sous la forme d'un procédé de connexion entre une première station et une deuxième station dans un réseau de communication sans fil.

[0018] Selon l'invention, la deuxième station met en œuvre :

[0019]
- la transmission, vers ladite première station, d'au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station,
- la connexion avec un ensemble de services de base auquel appartient ladite première station, sélectionné par ladite première station en fonction de ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station.

[0020] Ainsi, selon l'invention, la deuxième station, par exemple un terminal client, peut informer la première station, par exemple un point d'accès, du ou des modes de sécurité qu'elle supporte. A réception de cette information, la première station peut choisir le mode de sécurité adapté pour la connexion entre la première station et la deuxième station, la deuxième station se connectant avec l'ensemble de services de base configuré avec ce mode de sécurité.

[0021] On rappelle à cet effet qu'un ensemble de services de base, en anglais BSS ou « Basic Service Set », est un ensemble formé par un point d'accès et les terminaux associées à ce point d'accès, selon une configuration particulière (comprenant par exemple le nom du réseau Wi-Fi et un mode de sécurité).

[0022] Ainsi, l'association de la deuxième station n'est mise en œuvre qu'avec un BSS

« compatible » avec le ou les modes de sécurité supporté(s) par la deuxième station, ce qui permet d'éviter les problèmes d'interopérabilité. En particulier, la deuxième station est associée avec le BSS présentant le niveau de sécurité le plus élevé parmi les modes de sécurité supportés par la deuxième station.

[0023] Par exemple, les modes de sécurité appartiennent au groupe comprenant :

[0024]
- le mode de sécurité WPA2 ;
- le mode de sécurité WPA3 ;
- d'autres modes de sécurité actuels ou à venir tel que le mode de sécurité WPA4.

[0025] Ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station peut notamment lister de façon exhaustive tous les modes de sécurité supportés par la deuxième station.

[0026] En variante, ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station correspond au nombre de modes de sécurité supporté par ladite deuxième station.

[0027] Ainsi, à titre d'exemple, si un seul mode de sécurité est supporté par la deuxième station, la première station déduira que le mode de sécurité supporté par la deuxième station est le WPA2. Si deux modes de sécurité sont supportés par la deuxième station, la première station déduira que les modes de sécurité supportés par la deuxième station sont le WPA2 et le WPA3. Si trois modes de sécurité sont supportés par la deuxième station, la première station déduira que les modes de sécurité supportés par la deuxième station sont le WPA2, le WPA3 et le WPA4, etc.

[0028] Selon un mode de réalisation particulier, la deuxième station met en outre en œuvre la réception d'un identifiant d'au moins un premier ensemble de services de base auquel appartient ladite première station, ledit au moins un premier ensemble de services de base étant configuré avec un premier mode de sécurité,

[0029] et ladite connexion comprend la réception d'une requête de routage vers ledit ensemble de services de base sélectionné, si l'ensemble de services de base sélectionné, dit deuxième ensemble de services de base, est configuré avec un deuxième mode de sécurité supporté par ladite deuxième station et présentant un niveau de sécurité supérieur audit premier niveau de sécurité.

[0030] Selon ce mode de réalisation, la deuxième station reçoit un identifiant d'au moins un premier ensemble de services de base. Par exemple, le premier ensemble de services de base est configuré avec le niveau de sécurité le plus bas (par exemple WPA2) et donc supporté par toutes les stations.

[0031] Si la première station, à réception de l'information représentative d'un mode de sécurité supporté par la deuxième station, détermine que la deuxième station supporte un deuxième mode de sécurité, offrant une meilleure protection que le premier mode

de sécurité configuré pour le premier ensemble de services de base, la solution proposée permet de router automatiquement la deuxième station vers le deuxième ensemble de services de base configuré avec ce deuxième mode de sécurité (supporté par la deuxième station).

[0032] Ce deuxième ensemble de services de base n'est, de préférence, pas visible pour l'utilisateur de la deuxième station, i.e. seul un identifiant dudit au moins un premier ensemble de services de base est affiché sur une interface (par exemple un écran) de la deuxième station. De cette façon, l'utilisateur de la deuxième station ne voit qu'un seul identifiant d'un premier BSS, et la première station peut se charger, si besoin, de router la deuxième station vers un deuxième BSS non diffusé, mais plus adapté (par exemple parce qu'il est configuré avec un niveau de sécurité plus élevé).

[0033] En affichant un seul BSS, on évite le risque que l'utilisateur de la deuxième station choisisse un « mauvais BSS » (i.e. celui présentant un mode de sécurité faible, ou non supporté par la deuxième station), ce qui conduirait à une dégradation de l'expérience client avec la réception de messages d'erreurs non cohérents et variés.

[0034] La solution proposée permet ainsi de router automatiquement la deuxième station vers le BSS sélectionné par la première station, en tenant compte de l'information représentative d'un mode de sécurité supporté par la deuxième station. Cette opération est donc transparente pour un utilisateur de la deuxième station.

[0035] Notamment, si la deuxième station est un terminal multi-bande, apte à émettre ou recevoir des signaux sur plusieurs bandes de fréquence dans un réseau Wi-Fi (par exemple une bande de fréquence autour de 6 GHz lorsqu'il est proche du point d'accès, ou une bande de fréquence autour de 2,4 GHz lorsqu'il s'éloigne du point d'accès), le changement de mode de sécurité inhérent au changement de bande de fréquence peut ainsi être exécuté rapidement et de façon transparente pour l'utilisateur, i.e. sans nuire à l'expérience utilisateur.

[0036] Par exemple, on peut considérer que la première station appartient à :

[0037]
- deux « premiers ensembles de services de base » : un premier BSS, noté BSS1, sur une bande de fréquence à 2,4 GHz, et un deuxième BSS, noté BSS2 sur une bande de fréquence à 5 GHz, présentant la même configuration, par exemple un nom de réseau Wi-Fi « SSID1 » et un mode de sécurité WPA2 ;
- un « deuxième ensemble de services de base » : un troisième BSS, noté BSS3, sur une bande de fréquence à 6 GHz, présentant une configuration différente, par exemple un nom de réseau Wi-Fi « SSID2 » et un mode de sécurité WPA3.

[0038] Les BSS1 et BSS2, associés chacun à une bande de fréquence distincte, forment un ensemble de services étendu, en anglais ESS pour « Extended Service Set », présentant un identifiant d'ensemble de services SSID commun. Au niveau de la couche de

contrôle de la liaison logique (en anglais LLC, pour « Logical Link Control », l'ESS apparaît comme un BSS unique pour chacune des stations.

[0039] Selon un mode de réalisation particulier, ladite connexion comprend en outre la transmission, à ladite première station, d'une réponse à ladite requête de routage autorisant le routage vers ledit deuxième ensemble de services de base et la connexion de ladite deuxième station avec ledit deuxième ensemble de services de base.

[0040] Ainsi, à réception d'une requête de routage, la deuxième station peut choisir de s'associer, ou non, avec le BSS identifié dans la requête de routage, et en informer la première station.

[0041] L'invention concerne également un procédé de connexion entre une première station et une deuxième station dans un réseau de communication sans fil correspondant, mis en œuvre par la première station.

[0042] Selon l'invention, la première station met en œuvre :

[0043]
- la réception, en provenance de ladite deuxième station, d'au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station,
- la sélection d'un ensemble de services de base auquel appartient ladite première station, en fonction de ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station.

[0044] Comme indiqué ci-dessus, la première station peut ainsi vérifier si le ou les modes de sécurité supportés par la deuxième station sont compatibles avec au moins un mode de sécurité d'un BSS auquel la première station appartient, afin que la deuxième station s'associe avec un BSS compatible avec un mode de sécurité que la deuxième station supporte, de préférence le BSS présentant le niveau de protection le plus élevé.

[0045] Selon un mode de réalisation particulier, un tel procédé comprend également, mis en œuvre par la première station :

[0046]
- la transmission d'un identifiant d'au moins un premier ensemble de services de base auquel appartient ladite première station, ledit au moins un premier ensemble de services de base étant configuré avec un premier mode de sécurité,

[0047]
- la transmission d'une requête de routage vers ledit ensemble de services de base sélectionné, si l'ensemble de services de base sélectionné, dit deuxième ensemble de services de base, est configuré avec un deuxième mode de sécurité supporté par ladite deuxième station et présentant un niveau de sécurité supérieur audit premier niveau de sécurité.

[0048] Ainsi, comme indiqué précédemment, la solution proposée permet de router automatiquement la deuxième station vers un BSS sélectionné par la première station, en tenant compte de l'information représentative d'un mode de sécurité supporté par la

deuxième station.

[0049] Comme le deuxième mode de sécurité offre une meilleure protection que le premier mode de sécurité, la deuxième station peut choisir de s'associer au premier BSS, ou d'être routée vers le deuxième BSS si elle supporte les premier et deuxième mode de sécurité.

[0050] En particulier, la première station met en œuvre la réception, en provenance de ladite deuxième station, d'une réponse à ladite requête de routage autorisant le routage vers ledit deuxième ensemble de services de base et la connexion de ladite deuxième station avec ledit deuxième ensemble de services de base.

[0051] Ainsi, comme indiqué ci-dessus, à réception d'une requête de routage, la deuxième station peut choisir de s'associer, ou non, avec le BSS identifié dans la requête de routage, et en informer la première station.

[0052] Selon un mode de réalisation particulier, ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station est transmise dans un champ de type « Robust Security Network Information Element ».

[0053] Un tel champ est notamment décrit dans le paragraphe 9.4.2.24 de la norme IEEE 802.11-2020.

[0054] En particulier, ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station est transmise dans un message de type « Probe Request ».

[0055] Un tel message est classiquement transmis de la deuxième station vers la première station, pour que la deuxième station puisse s'associer avec un BSS auquel appartient la première station. Ainsi, la solution proposée ne nécessite pas l'envoi de message supplémentaire.

[0056] En particulier, ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station peut être transmise dans un champ de type « Robust Security Network Information Element » inséré dans un message de type « Probe Request ».

[0057] L'invention concerne encore une première station d'un réseau de communication sans fil correspondante, comprenant :

[0058]
- des moyens de réception, en provenance d'une deuxième station dudit réseau, d'au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station,
- des moyens de sélection d'un ensemble de services de base auquel appartient ladite première station, en fonction de ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station.

[0059] En mode infrastructure, une telle première station est par exemple un point d'accès (passerelle, « set top box », etc). En mode ad-hoc, une telle première station est par

exemple un terminal client (smartphone, tablette, imprimante, télévision connectée, etc).

[0060] L'invention concerne par ailleurs une deuxième station d'un réseau de communication sans fil correspondante, comprenant :

[0061]
- des moyens de transmission, vers une première station dudit réseau, d'au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station,
- des moyens de connexion avec un ensemble de services de base auquel appartient ladite première station, sélectionné par ladite première station en fonction de ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station.

[0062] Une telle deuxième station est par exemple un terminal client (smartphone, tablette, imprimante, télévision connectée, etc).

[0063] L'invention concerne encore un ou plusieurs programmes d'ordinateur comportant des instructions pour la mise en œuvre d'un procédé de connexion tel que décrit ci-dessus lorsque ce ou ces programmes sont exécutés par au moins un processeur.

[0064] L'invention concerne enfin un ou plusieurs supports d'enregistrement lisibles par un ordinateur, sur lequel sont enregistrés un ou plusieurs programmes d'ordinateur comprenant des instructions de code de programme pour l'exécution d'au moins une étape d'un procédé de connexion tel que décrit ci-dessus, selon l'un quelconque des modes de réalisation. De tels supports d'enregistrement peuvent être n'importe quelle entité ou dispositif capable de stocker un programme.

[0065] 4. Liste des figures

[0066] D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation particulier, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

[0067] - la [Fig.1] illustre un exemple de réseau de communication Wi-Fi comprenant une première station STA1 et une deuxième station STA2 ;

[0068] - la [Fig.2] présente les principales étapes mises en œuvre par les première et deuxième stations STA1 et STA2 selon un mode de réalisation particulier de l'invention ;

[0069] - la [Fig.3] illustre un exemple d'échange de messages pour connecter les première et deuxième stations STA1 et STA2 selon un mode de réalisation particulier ;

[0070] - la [Fig.4] présente la structure simplifiée d'une première station selon un mode de réalisation particulier ;

[0071] - la [Fig.5] présente la structure simplifiée d'une deuxième station selon un mode de réalisation particulier.

[0072] 5. Description d'un mode de réalisation particulier

[0073] 5.1 Principe général

[0074] On se place dans le contexte d'un réseau de communication Wi-Fi mettant en œuvre au moins deux stations STA1 et STA2, comme illustré en [Fig.1]. Un tel réseau Wi-Fi peut fonctionner en mode infrastructure ou ad-hoc.

[0075] Le principe général de l'invention repose sur l'information, au niveau de la première station, du ou des modes de sécurité supportés par la deuxième station. De cette façon, la première station peut sélectionner un ensemble de services de base auquel elle appartient, configuré avec un mode de sécurité supporté par la deuxième station, pour que la deuxième station puisse s'associer avec un « bon » ensemble de services de base. En particulier, la première station sélectionne l'ensemble de services de base configuré avec le mode de sécurité supporté par la deuxième station offrant le niveau de sécurité le plus élevé.

[0076] On présente ci-après, en relation avec la [Fig.2], les principales étapes mises en œuvre par la première station STA1 et la deuxième station STA2 selon un mode de réalisation de l'invention.

[0077] Au cours d'une étape 211, la deuxième station STA2 transmet, vers la première station STA1, au moins une information représentative d'un mode de sécurité supporté par la deuxième station STA2. Par exemple, une telle information comprend une liste du ou des modes de sécurité supportés par la deuxième station STA2, un nombre de modes de sécurité supportés par la deuxième station STA2, etc.

[0078] La première station STA1 reçoit ainsi, au cours d'une étape 221, ladite au moins une information représentative d'un mode de sécurité supporté par la deuxième station STA2.

[0079] A réception de cette information, la première station STA1 peut sélectionner, au cours d'une étape 222, un ensemble de services de base auquel appartient la première station STA1, en fonction de ladite au moins une information représentative d'un mode de sécurité supporté par la deuxième station STA2.

[0080] Par exemple, si la deuxième station STA2 supporte un unique mode de sécurité, la première station STA1 sélectionne l'ensemble de services de base configuré avec ce mode de sécurité. La première station STA1 peut éventuellement informer la deuxième station STA2 de l'ensemble de services de base sélectionné, mais cette étape est facultative dans ce cas.

[0081] Si la deuxième station STA2 supporte plusieurs modes de sécurité, la première station STA1 sélectionne par exemple l'ensemble de services de base configuré avec le mode de sécurité présentant le niveau de sécurité le plus élevé. Dans ce cas, la première station STA1 informe la deuxième station STA2 de l'ensemble de services de base sélectionné.

[0082] La deuxième station STA2 peut ainsi se connecter, au cours d'une étape 212, avec

l'ensemble de services de base sélectionné par la première station STA1, sans passer par une connexion avec un autre ensemble de services de base qui offrirait un niveau de sécurité moins élevé par exemple.

[0083] Selon un mode de réalisation particulier, la première station STA1 diffuse au préalable dans le réseau Wi-Fi, au cours d'une étape 220, un identifiant d'au moins un premier ensemble de services de base auquel elle appartient, configuré avec un premier mode de sécurité. La deuxième station STA2, notamment, reçoit cet identifiant au cours d'une étape 210. Par exemple, ce premier mode de sécurité présente le niveau de sécurité le plus bas (par exemple WPA2), et peut donc être supporté par toutes les stations du réseau Wi-Fi.

[0084] Si la deuxième station STA2 supporte uniquement le premier mode de sécurité, la première station STA1 sélectionne le premier ensemble de services de base, configuré avec ce premier mode de sécurité. La deuxième station STA2 peut ainsi se connecter avec le premier ensemble de services de base sélectionné par la première station STA1.

[0085] Si la deuxième station STA2 supporte plusieurs modes de sécurité, la première station STA1 sélectionne un deuxième ensemble de services de base, configuré avec un deuxième mode de sécurité présentant un niveau de sécurité supérieur au premier mode de sécurité. Par exemple, la première station STA1 sélectionne le deuxième ensemble de services de base présentant le niveau de sécurité le plus élevé.

[0086] La première station STA1 peut alors transmettre à la deuxième station STA2 une requête de routage vers le deuxième ensemble de services de base sélectionné, si elle détecte que le deuxième mode de sécurité offre une meilleure protection que le premier mode de sécurité (par exemple le deuxième mode de sécurité est plus récent que le premier mode de sécurité). La première station STA1 peut ainsi décider de router la deuxième station STA2 vers un ensemble de services de base en tenant compte des capacités de la deuxième station STA2.

[0087] En d'autres termes, la première station STA1 selon ce mode de réalisation propose un premier ensemble de services de base, par exemple le BSS1 illustré en [Fig.1], qui peut être vu comme un BSS « de routage », dirigeant la deuxième station STA2 vers un BSS adapté selon le ou les modes de sécurité supportés par la deuxième station STA2, par exemple le BSS2 illustré en [Fig.1]. Pour que cela soit transparent pour l'utilisateur de la deuxième station STA2, l'utilisateur peut sélectionner l'unique BSS visible dans une interface de la deuxième station STA2. Par cette action, la deuxième station STA2 est dirigée vers un BSS adapté à un mode de sécurité supporté par la deuxième station STA2.

[0088] L'invention permet ainsi de garantir la connexion des stations qui ne supportent pas les nouveaux modes de sécurité et de router les stations qui supportent un nouveau mode de sécurité donné vers le « bon » BSS. Selon un mode de réalisation particulier,

elle permet de garantir une connexion de chaque station avec le BSS qui lui garantit le meilleur mode de sécurité supporté.

[0089] En particulier, lors de la découverte des réseaux visibles, l'utilisateur de la deuxième station ne voit que le BSS1, et peut connecter son terminal à ce BSS1. La configuration de sécurité permet a toutes les stations de pouvoir se connecter au BSS1 sans problème d'interopérabilité.

[0090] 5.2 Exemple de mise en œuvre

[0091] On décrit ci-après un exemple de mise en œuvre de l'invention, dans un réseau Wi-Fi en mode infrastructure. On considère selon cet exemple que la première station est un point d'accès / routeur, et la deuxième station un terminal client.

[0092] On considère également que le point d'accès appartient à au moins deux BSS ou ESS :

[0093]
- un premier BSS, noté BSS1, identifié par l'identifiant SSID1, et configuré avec un premier mode de sécurité présentant le niveau de protection le plus faible, par exemple de type WPA2. Le BSS1 permet de garantir l'interopérabilité avec une deuxième station qui ne serait pas mise à jour, par exemple une deuxième station supportant uniquement le premier mode de sécurité. Le BSS1 permet également le routage d'une deuxième station plus récente vers un BSS configuré avec un deuxième mode de sécurité présentant un niveau de protection plus élevé que le premier mode de sécurité, par exemple de type WPA3 ;
- un deuxième BSS, noté BSS2, identifié par l'identifiant SSID2, et configuré avec un deuxième mode de sécurité présentant un niveau de protection plus élevé que le premier mode de sécurité, par exemple de type WPA3. Le BSS2 est non visible par l'utilisateur de la deuxième station.

[0094] On note qu'une station supportant un mode de sécurité supporte également des modes de sécurité de niveau de sécurité inférieur. Par exemple une station supportant le mode de sécurité WPA3 supporte également les versions antérieures (ou présentant un niveau de sécurité inférieur) du mode de sécurité WPA3, et donc le mode de sécurité WPA2.

[0095] La [Fig.3] illustre un exemple de messages échangés entre le point d'accès AP et le terminal client STA2 selon cet exemple de mise en œuvre.

[0096] Classiquement, le point d'accès diffuse dans le réseau Wi-Fi une balise, en anglais « Beacon », portant des informations sur le réseau de communication. Une telle balise porte des informations permettant de connaître les caractéristiques d'un ensemble de services de base proposé par le point d'accès, par exemple l'identité du point d'accès, la bande de fréquence (2,4GHz, 5GHz, 6GHz), la largeur de bande (20MHz, 40MHz, 80MHz, 160MHz), etc.

[0097] Selon l'exemple illustré en [Fig.3], le point d'accès diffuse une balise 31 identifiant le premier ensemble de services de base BSS1, au moyen de l'identifiant SSID1.

[0098] Lorsqu'il cherche à se connecter au point d'accès AP, le terminal STA2 envoie une succession de trames Wi-Fi. Le terminal STA2 peut ainsi envoyer au point d'accès AP une information représentative du ou des modes de sécurité qu'il supporte, par exemple dans un message « Probe Request » 32.

[0099] Par exemple, lors de l'envoi de la trame « Probe Request » par le terminal STA2 vers le point d'accès AP dans l'ensemble de services de base BSS1 identifié par l'identifiant SSID1, un champ « RSN Information Element» est ajouté afin d'indiquer les modes de sécurité supportés par le terminal STA2.

[0100] Le point d'accès peut répondre au message « Probe Request » 32 en envoyant un message classique « Probe Response » 33 de la norme Wi-Fi au terminal STA2.

[0101] Si le point d'accès AP détermine que le terminal STA2 ne supporte que le premier mode de sécurité (WPA2), alors il sélectionne l'ensemble de services de base BSS1 et le terminal STA2 se connecte au BSS1.

[0102] Si le point d'accès AP détermine que le terminal STA2 supporte le deuxième mode de sécurité (WPA3), alors il redirige le terminal STA2 vers l'ensemble de services de base BSS2. Pour ce faire, comme illustré en [Fig.3], le point d'accès AP émet une requête de routage qui propose au terminal STA2 de se connecter sur le BSS2 identifié par l'identifiant SSID2, configuré avec le deuxième mode de sécurité offrant un niveau de sécurité supérieur au premier mode de sécurité (par exemple le deuxième mode de sécurité est plus récent que le premier mode de sécurité). Par exemple, une telle requête est émise sous la forme d'une nouvelle trame « Routing Request » 34. Selon un mode de réalisation particulier, la trame « Routing Request » émise par le point d'accès AP permet de donner au terminal STA2 les informations nécessaires pour qu'il puisse se connecter au BSS sélectionné. Par exemple, la trame « Routing Request » porte un identifiant du BSS sélectionné (par exemple un identifiant d'ensemble de services SSID), et un ou plusieurs champs classiques rencontrés dans les trames « probe response » / « association response ».

[0103] A réception de cette requête de routage, le terminal STA2 peut accepter de se connecter sur ce BSS2, ou décider de se connecter sur le BSS1. Il peut envoyer une réponse au point d'accès AP, par exemple dans une trame « Routing Response » 35, portant l'identifiant du BSS avec lequel il souhaite se connecter (SSID2 par exemple) et un champ « RSN Information Element». Selon un mode de réalisation particulier, la trame « Routing Response » émise par le terminal STA2 permet d'indiquer au point d'accès AP s'il accepte de se connecter avec le BSS sélectionné par l'AP ou non. Par exemple, la trame « Routing Response » porte une information de type « succès » si le terminal STA2 accepte de se connecter avec le BSS sélectionné par l'AP, « échec »

sinon. Le terminal STA2 peut également indiquer au point d'accès AP la ou les raisons pour lesquelles il refuse de se connecter au BSS sélectionné par le point d'accès, par exemple via un message de type « reason code » prenant l'une des valeurs prévues par la norme Wi-Fi.

[0104] La connexion se poursuit en échangeant des trames classiques telles que décrites dans la norme Wi-Fi, notamment au cours d'une procédure d'authentification 36, d'association 37 et d'échange de clés 38.

[0105] Par exemple, la procédure d'authentification 36 repose sur l'échange de messages d'authentification de type « Simultaneous Authentication of Equals (SAE) » entre le point d'accès AP et le terminal STA2.

[0106] Une fois l'authentification terminée, le terminal STA2 peut s'associer 37 (s'inscrire) au point d'accès/routeur pour accéder pleinement au réseau. L'association permet au routeur/point d'accès d'enregistrer chaque station afin que les trames soient correctement livrées. Par exemple, le terminal STA2 envoie au point d'accès une requête en association avec le BSS2 dans un message « Association Request (SSID2) ». Le point d'accès confirme l'association dans un message de réponse « Association Response (SSID2) ». Le terminal STA2 est donc routé vers le BSS2 avant la procédure d'association, ce qui lui permet de s'associer avec le « bon » BSS, par exemple celui configuré avec le mode de sécurité le plus élevé supporté par le terminal STA2.

[0107] Le terminal STA2 peut ensuite se connecter avec le point d'accès AP grâce à l'échange 38 de clés (« Key » 1, 2, 3, 4).

[0108] 5.3 Structures simplifiées d'une première station et d'une deuxième station

[0109] On présente désormais, en relation avec la [Fig.4], la structure simplifiée d'une première station selon au moins un mode de réalisation décrit ci-dessus.

[0110] Comme illustré en [Fig.4], une telle première station comprend au moins une mémoire 41 comprenant une mémoire tampon, au moins une unité de traitement 42, équipée par exemple d'une machine de calcul programmable ou d'une machine de calcul dédiée, par exemple un processeur P, et pilotée par le programme d'ordinateur 43, mettant en œuvre des étapes du procédé de connexion selon au moins un mode de réalisation de l'invention.

[0111] A l'initialisation, les instructions de code du programme d'ordinateur 43 sont par exemple chargées dans une mémoire RAM avant d'être exécutées par le processeur de l'unité de traitement 42.

[0112] Le processeur de l'unité de traitement 42 met en œuvre des étapes du procédé de connexion décrit précédemment, selon les instructions du programme d'ordinateur 43, pour :

[0113] • recevoir au moins une information représentative d'un mode de sécurité supporté par une deuxième station, en provenance de la deuxième station,

- sélectionner un ensemble de services de base auquel appartient la première station, en fonction de ladite au moins une information représentative d'un mode de sécurité supporté par la deuxième station.

[0114] On présente désormais, en relation avec la [Fig.5], la structure simplifiée d'une deuxième station selon au moins un mode de réalisation décrit ci-dessus.

[0115] Comme illustré en [Fig.5], une telle deuxième station comprend au moins une mémoire 51 comprenant une mémoire tampon, au moins une unité de traitement 52, équipée par exemple d'une machine de calcul programmable ou d'une machine de calcul dédiée, par exemple un processeur P, et pilotée par le programme d'ordinateur 53, mettant en œuvre des étapes du procédé de connexion selon au moins un mode de réalisation de l'invention.

[0116] A l'initialisation, les instructions de code du programme d'ordinateur 53 sont par exemple chargées dans une mémoire RAM avant d'être exécutées par le processeur de l'unité de traitement 52.

[0117] Le processeur de l'unité de traitement 52 met en œuvre des étapes du procédé de connexion décrit précédemment, selon les instructions du programme d'ordinateur 53, pour :

[0118]
- transmettre, vers une première station, au moins une information représentative d'un mode de sécurité supporté par la deuxième station,
- se connecter avec un ensemble de services de base auquel appartient la première station, sélectionné par la première station en fonction de ladite au moins une information représentative d'un mode de sécurité supporté par la deuxième station.

Revendications

[Revendication 1] Procédé de connexion entre une première station (STA1) et une deuxième station (STA2) dans un réseau de communication sans fil, caractérisé en ce que ladite deuxième station (STA2) met en œuvre :

- la transmission (211), vers ladite première station (STA1), d'au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station (STA2),
- la connexion (212) avec un ensemble de services de base auquel appartient ladite première station (STA1), sélectionné par ladite première station en fonction de ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station.

[Revendication 2] Procédé selon la revendication 1, caractérisé en ce qu'il comprend en outre la réception (210) d'un identifiant (SSID1) d'au moins un premier ensemble de services de base auquel appartient ladite première station (STA1), ledit au moins un premier ensemble de services de base étant configuré avec un premier mode de sécurité,
et en ce que ladite connexion comprend la réception d'une requête de routage (34) vers ledit ensemble de services de base sélectionné, si ledit ensemble de services de base sélectionné, dit deuxième ensemble de services de base, est configuré avec un deuxième mode de sécurité supporté par ladite deuxième station (STA2) et présentant un niveau de sécurité supérieur audit premier niveau de sécurité.

[Revendication 3] Procédé selon la revendication 2, caractérisé en ce que ladite connexion comprend en outre la transmission, à ladite première station, d'une réponse (35) à ladite requête de routage autorisant le routage vers ledit deuxième ensemble de services de base et la connexion de ladite deuxième station avec ledit deuxième ensemble de services de base.

[Revendication 4] Procédé selon l'une quelconque des revendications 2 et 3, caractérisé en ce qu'il comprend l'affichage, sur ladite deuxième station (STA2), dudit identifiant dudit au moins un premier ensemble de services de base uniquement.

[Revendication 5] Procédé de connexion entre une première station (STA1) et une deuxième station (STA2) dans un réseau de communication sans fil, caractérisé en ce que ladite première station (STA1) met en œuvre :

- la réception (221), en provenance de ladite deuxième station (STA2), d'au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station (STA2),
- la sélection (222) d'un ensemble de services de base auquel appartient ladite première station (STA1), en fonction de ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station.

[Revendication 6] Procédé selon la revendication 5, caractérisé en ce qu'il comprend également :

- la transmission (220) d'un identifiant (SSID1) d'au moins un premier ensemble de services de base auquel appartient ladite première station (STA1), ledit au moins un premier ensemble de services de base étant configuré avec un premier mode de sécurité,
- la transmission d'une requête de routage (34) vers ledit ensemble de services de base sélectionné, si ledit ensemble de services de base sélectionné, dit deuxième ensemble de services de base, est configuré avec un deuxième mode de sécurité supporté par ladite deuxième station et présentant un niveau de sécurité supérieur audit premier niveau de sécurité.

[Revendication 7] Procédé selon la revendication 6, caractérisé en ce qu'il comprend la réception, en provenance de ladite deuxième station (STA2), d'une réponse (35) à ladite requête de routage autorisant le routage vers ledit deuxième ensemble de services de base et la connexion de ladite deuxième station avec ledit deuxième ensemble de services de base.

[Revendication 8] Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station est transmise dans un champ de type « RSN Information Element ».

[Revendication 9] Procédé selon l'une quelconque des revendications 1 à 8, caractérisé en ce que ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station est transmise dans un message de type « Probe Request ».

[Revendication 10] Procédé l'une quelconque des revendications 1 à 9, caractérisé en ce que

ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station correspond au nombre de modes de sécurité supporté par ladite deuxième station.

[Revendication 11] Procédé l'une quelconque des revendications 1 à 10, caractérisé en ce que lesdits modes de sécurité appartiennent au groupe comprenant :

- le mode de sécurité WPA2 ;
- le mode de sécurité WPA3 ;
- une autre version du mode de sécurité WPA.

[Revendication 12] Programme d'ordinateur comportant des instructions pour la mise en œuvre d'un procédé selon l'une quelconque des revendications 1 à 11 lorsque ce programme est exécuté par un processeur.

[Revendication 13] Station d'un réseau de communication sans fil, dite deuxième station (STA2), comprenant :

- des moyens de transmission (211), vers une première station (STA1) dudit réseau, d'au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station (STA2),
- des moyens de connexion (212) avec un ensemble de services de base auquel appartient ladite première station (STA1), sélectionné par ladite première station en fonction de ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station.

[Revendication 14] Station d'un réseau de communication sans fil, dite première station (STA1), comprenant :

- des moyens de réception (221), en provenance d'une deuxième station (STA2) dudit réseau, d'au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station (STA2),
- des moyens de sélection (222) d'un ensemble de services de base auquel appartient ladite première station (STA1), en fonction de ladite au moins une information représentative d'un mode de sécurité supporté par ladite deuxième station.

[Fig. 1]

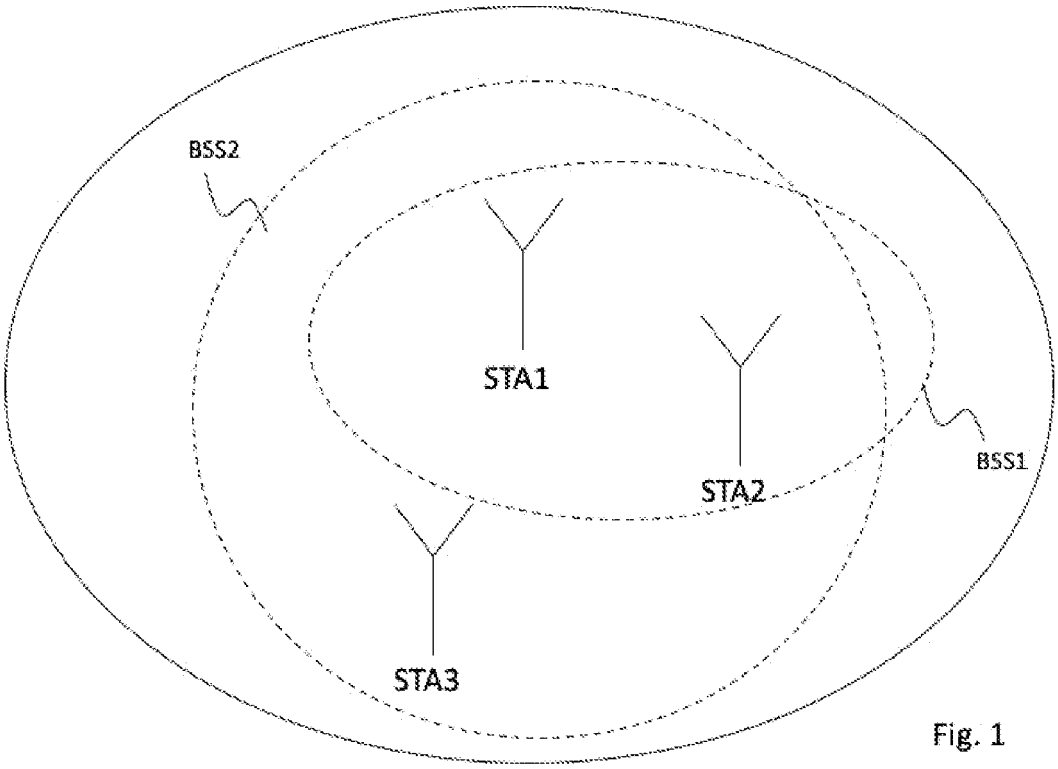


Fig. 1

[Fig. 2]

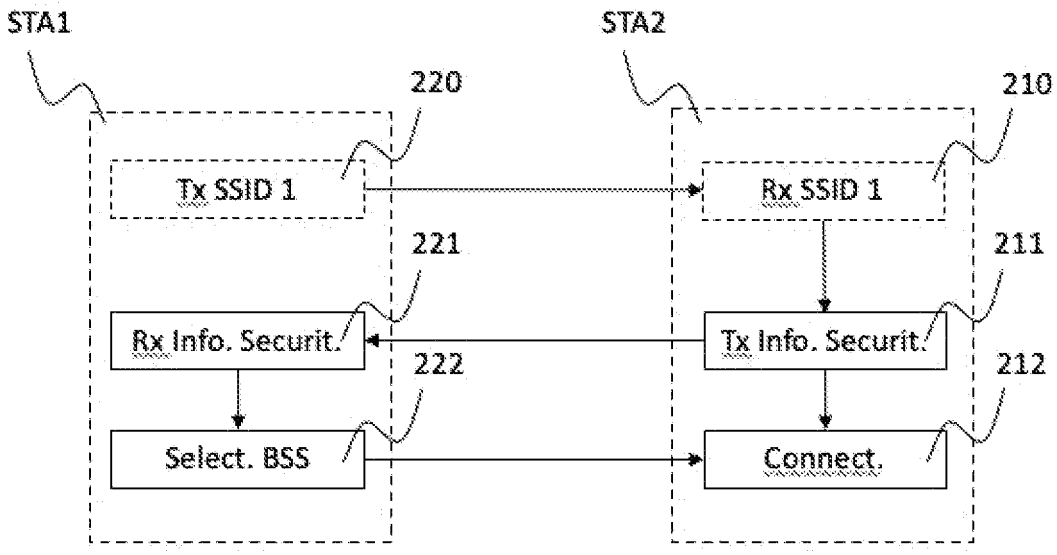


Fig. 2

[Fig. 3]

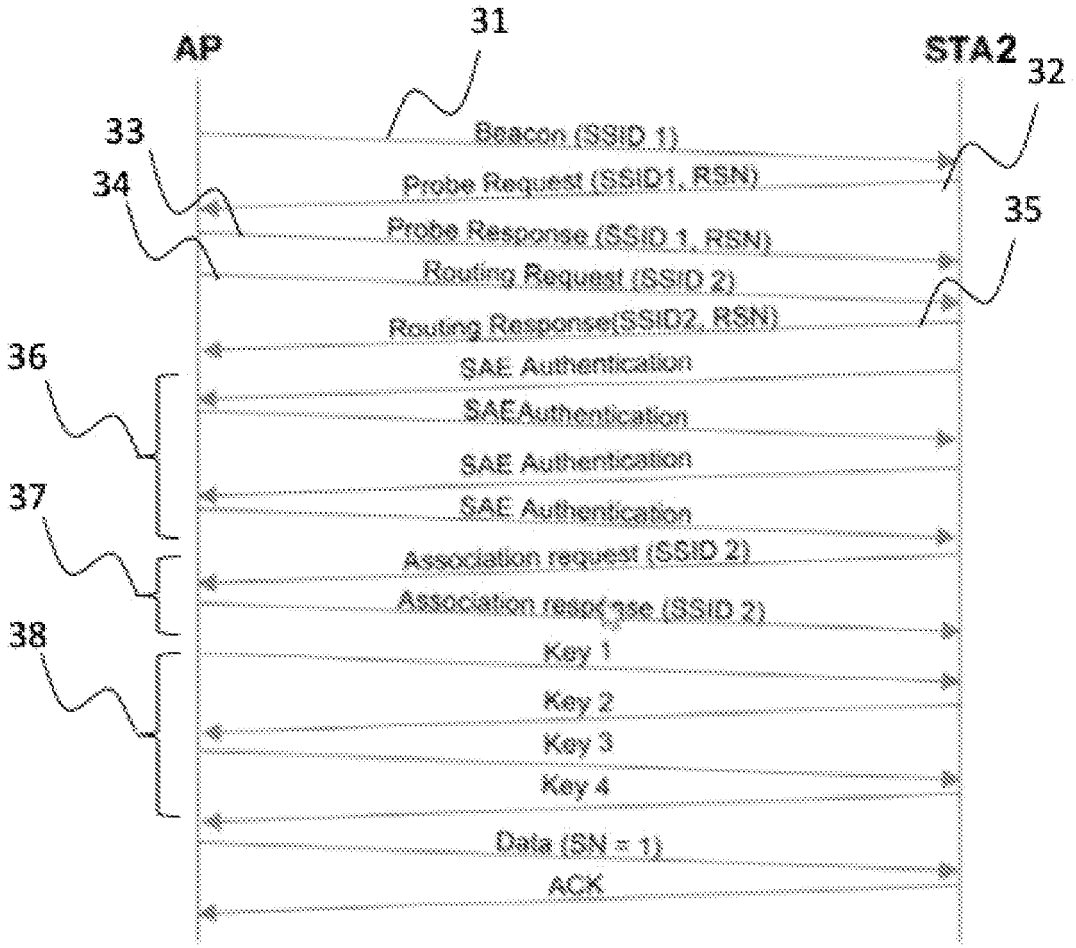


Fig. 3

[Fig. 4]

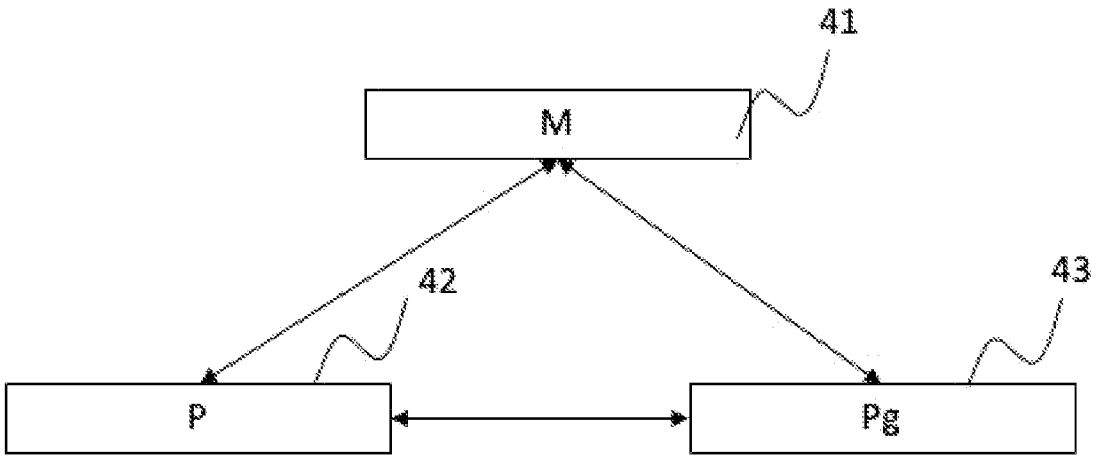


Fig. 4

[Fig. 5]

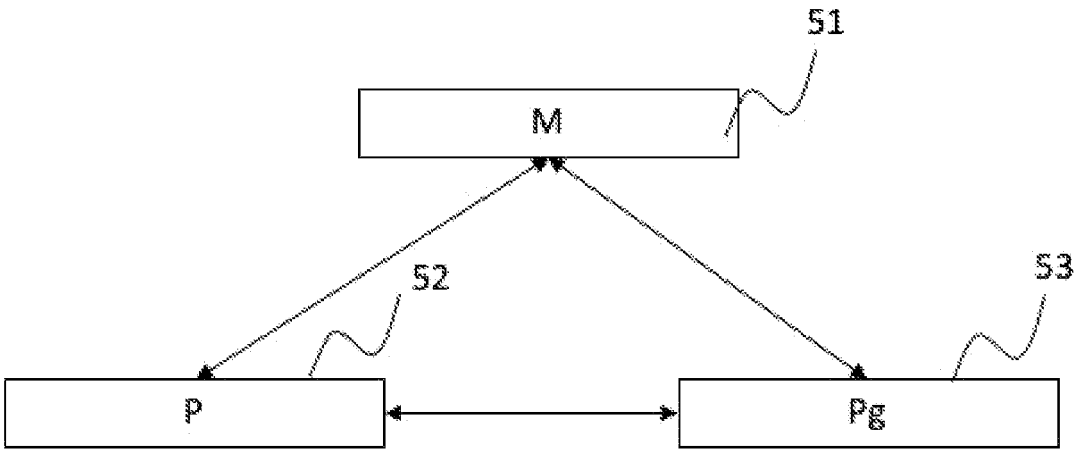


Fig. 5

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 898437
FR 2107683

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	LOUNIS KARIM ET AL: "WPA3 Connection Deprivation Attacks", 28 février 2020 (2020-02-28), COMPUTER VISION – ECCV 2020 : 16TH EUROPEAN CONFERENCE, GLASGOW, UK, AUGUST 23-28, 2020 : PROCEEDINGS; PART OF THE LECTURE NOTES IN COMPUTER SCIENCE ; ISSN 0302-9743; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PU, XP047549887, ISBN: 978-3-030-58594-5 [extrait le 2020-02-28] * le document en entier *	1-14	H04W12/06 H04L12/28 H04W4/00 H04W84/12 H04L29/06
A	Unknown: "WPA3 Encryption and Configuration Guide Introduction published 24.06.2021", , 24 juin 2021 (2021-06-24), XP055891749, Extrait de l'Internet: URL:https://documentation.meraki.com/@api/deki/pages/1310/pdf/WPA3+Encryption+and+Configuration+Guide.pdf?stylesheet=default [extrait le 2022-02-15] * page 2, alinéa WPA3 only – page 6, alinéa WPA3-Enterprise *	1-14	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04W
A	LAMERS ERIK ET AL: "Securing Home Wi-Fi with WPA3 Personal", 2021 IEEE 18TH ANNUAL CONSUMER COMMUNICATIONS & NETWORKING CONFERENCE (CCNC), IEEE, 9 janvier 2021 (2021-01-09), pages 1-8, XP033885364, DOI: 10.1109/CCNC49032.2021.9369629 [extrait le 2021-03-03] * le document en entier *	1-14	

-/--

Date d'achèvement de la recherche	Examinateur
1 mars 2022	Ghomrasseni, Z

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

3

EPO FORM 1503 12.99 (P04C14)

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 898437
FR 2107683

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		
A	Unknown: "WPA3 Specification Version 3.0", , 20 décembre 2020 (2020-12-20), XP055891724, Extrait de l'Internet: URL:https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v3.0.pdf [extrait le 2022-02-15] * page 24, alinéa 7 - page 26, alinéa 8 * -----	1-14	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)

Date d'achèvement de la recherche	Examinateur
1 mars 2022	Ghomrasseni, Z

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

3

EPO FORM 1503 12.99 (P04C14)