(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 146 776***

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

(21) **N° d'enregistrement national :** **23 02492**

(51) Int Cl[8] : ***H 04 L 9/08*** *(2023.01), H 04 L 9/32, H 04 W 74/00*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 17.03.23.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 20.09.24 Bulletin 24/38.

(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) :** BALE Sylvain et AUFFRAY Michel.

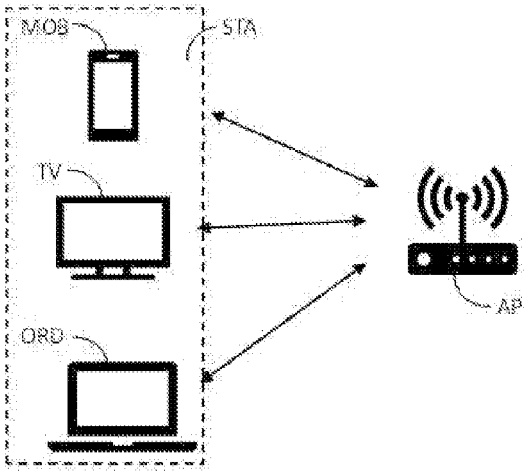
(73) **Titulaire(s) :** ORANGE Société anonyme.

(74) **Mandataire(s) :** REGIMBEAU.

(54) Connexion multi-profils d'une station à un point d'accès d'un réseau de télécommunication sans-fil.

(57) Procédé de connexion d'une station à un point d'accès d'un réseau de télécommunication sans-fil comportant une phase d'authentification dans lequel ladite station (STA) utilise une clé pour transmettre un message (m2) vers ledit point d'accès (PA), et dans lequel ledit point d'accès vérifie l'intégrité dudit message en utilisant une pluralité de clés stockées, et, si une clé stockée parmi ladite pluralité permet de vérifier ladite intégrité, attribue un profil d'accès à ladite station, correspondant à ladite clé stockée.

Figure pour l'abrégé : Fig. 1



FR 3 146 776 - A1

Description

Titre de l'invention : Connexion multi-profils d'une station à un point d'accès d'un réseau de télécommunication sans-fil

DOMAINE DE L'INVENTION

[0001] La présente invention concerne le domaine de la connexion d'une station à un point d'accès d'un réseau de télécommunication sans-fil, en particulier d'un réseau de type Wi-Fi.

[0002] Elle concerne plus particulièrement l'attribution d'un profil à une station, définissant ses droits au sein du réseau de télécommunication.

[0003] Dans un réseau domestique, il a été proposé plusieurs mécanismes pour la gestion des droits d'une station donnée et le contrôle d'accès.

[0004] Par exemple, l'adresse physique de la station, par exemple son adresse MAC (« Medium Access Control ») peut être utilisé pour identifier une station donnée et ainsi distinguer des profils différents en fonction des stations au niveau du point d'accès. Toutefois, cette méthode présente l'inconvénient d'être incompatible avec les mécanismes d'adresses MAC dynamiques (« MAC address randomization »).

[0005] Une autre méthode consiste à créer plusieurs réseaux de télécommunication distincts, chacun correspondant à un profil distinct. Typiquement, un premier réseau Wi-Fi confère tous les droits aux stations connectées, et un second réseau Wi-Fi, dit « invités » (« guest »), confère des droits minimaux, par exemple l'accès à un réseau extérieur (Internet) sans permettre l'accès aux ressources locales connectées au réseau Wi-Fi.

[0006] Cette méthode présente toutefois de nombreux inconvénients.

[0007] Ainsi, chaque réseau de télécommunication déployé occupe nécessairement un emplacement sur le spectre de la bande de fréquences utilisée. L'ajout même d'un seul réseau « invité » génère des interférences sur les bandes de fréquences Wi-Fi induisant d'une part la congestion du réseau et d'autre part une consommation énergétique accrue.

[0008] En outre, elle permet difficilement de proposer plus de deux profils distincts, d'autant plus que chaque réseau de télécommunication déployé, comme on l'a vu, consomme les ressources disponibles. La granularité de la gestion des droits d'accès est donc nécessairement très faible.

[0009] Une autre méthode consiste à déporter la gestion des droits d'accès dans une couche applicative. Les utilisateurs doivent ainsi se connecter sur un portail web captif et saisissent des identifiants et mots de passe correspondant à leur profil.

[0010] Cette méthode présente l'inconvénient de nécessiter une étape supplémentaire pour

les utilisateurs des stations et donc d'impacter l'expérience utilisateur. De plus, elle laisse l'accès libre à la couche physique du réseau de télécommunication, ce qui génère une vulnérabilité aux attaques et malveillances envers ce réseau et envers le point d'accès.

[0011] Il existe donc un besoin d'améliorer les propositions actuelles de l'état de la technique.

Résumé de l'invention

[0012] À ces fins, selon un premier aspect, la présente invention peut être mise en œuvre par un procédé de connexion d'une station à un point d'accès d'un réseau de télécommunication sans-fil comportant une phase d'authentification dans lequel ladite station utilise une clé pour transmettre un message vers ledit point d'accès, et dans lequel ledit point d'accès vérifie l'intégrité dudit message en utilisant une pluralité de clés stockées, et, si une clé stockée parmi ladite pluralité permet de vérifier ladite intégrité, attribue un profil d'accès à ladite station, correspondant à ladite clé stockée

[0013] Il est ainsi possible de définir une pluralité de clés, chaque clé pouvant correspondre à un utilisateur ou à un groupe d'utilisateurs, indépendamment des stations qu'ils peuvent utiliser.

[0014] Le mécanisme proposé est aisé à configurer pour l'administrateur qui, dans le cadre d'un déploiement familial, n'est pas nécessairement informaticien, et il est en outre transparent pour chaque utilisateur qui n'a juste qu'à connaître et paramétrer un mode de passe, de la même façon que dans les mécanismes habituels.

[0015] Si un utilisateur possède plusieurs stations, l'utilisateur d'un même mot de passe lui permettra d'obtenir le même profil d'accès pour chacune de ses stations.

[0016] Suivant des modes de réalisation préférés, l'invention comprend une ou plusieurs des caractéristiques suivantes qui peuvent être utilisées séparément ou en combinaison partielle entre elles ou en combinaison totale entre elles :

- ladite phase d'authentification est conforme à la norme IEEE 802.11i et ladite clé est une clé primaire, PMK.

En particulier, l'invention s'applique particulièrement bien aux réseaux Wi-Fi en mode de sécurité WPA2-Personnal, ce qui permet un usage familial, notamment sans déploiement d'un serveur Radius.

- ledit message est un second message d'un processus de poignée de main à 4 voies. Ainsi, le mécanisme est complétement transparent du point du vue des stations, et implique une modification mineure pour les points d'accès.
- ledit profil d'accès correspond à un réseau local virtuel. Il est ainsi possible d'apporter une grande flexibilité des droits d'accès et de déporter la configuration des droits d'accès sur la configuration de réseaux locaux virtuels ap-

propriés.

- ledit profil d'accès détermine un accès à un réseau extérieur et/ou aux ressources locales connectées audit réseau local sans-fil. On peut ainsi gérer, par exemples, des profils visiteurs (pouvant se connecter au réseau extérieur mais pas aux ressources locales), des profils « enfants » (pouvant se connecter aux ressources locales mais pas au réseau extérieur), etc.
- ledit point d'accès parcourt ladite pluralité en testant chaque clé stockée pour vérifier l'intégrité dudit message jusqu'à ce qu'une clé donnée vérifie ladite intégrité, et attribue ledit profil correspondant à ladite clé donnée.

Il est possible d'ordonner les clés de façon que les premières stockées soient les plus communes afin de minimiser les temps moyens de connexion au réseau.

[0017] Un autre aspect de l'invention concerne un point d'accès à un réseau de télécommunication sans-fil, comprenant un processeur configuré pour permettre la connexion d'une station à la suite d'une phase d'authentification dans lequel ledit point d'accès reçoit de la part de ladite station un message, et dans lequel ledit point d'accès vérifie l'intégrité dudit message en utilisant une pluralité de clés stockées, et, si une clé stockée parmi ladite pluralité permet de vérifier ladite intégrité, attribuer un profil d'accès à ladite station, correspondant à ladite clé stockée, ledit profil d'accès étant utilisé pour ladite connexion.

[0018] Un autre aspect de l'invention concerne un programme d'ordinateur apte à être mis en œuvre sur un point d'accès à un réseau de télécommunication sans fil, le programme comprenant des instructions de code qui, lorsqu'il est exécuté par un processeur, réalise les étapes du procédé tel que précédemment défini.

[0019] Un autre aspect de l'invention concerne un support de données sur lequel a été mémorisé au moins une série d'instructions de code de programme pour l'exécution d'un procédé tel que précédemment défini.

[0020] D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui suit d'un mode de réalisation préféré de l'invention, donnée à titre d'exemple et en référence aux dessins annexés.

BREVE DESCRIPTION DES FIGURES

[0021] Les dessins annexés illustrent l'invention :

la [Fig.1] illustre un contexte de mise en œuvre d'un procédé

[0022] la [Fig.2] schématise un chronogramme d'un échange entre une station et un point d'accès selon un mode de réalisation du procédé.

[0023] DESCRIPTION DETAILLEE DE MODES DE REALISATION DE L'INVENTION

[0024] La [Fig.1] illustre un contexte de mise en œuvre d'un réseau de télécommunication permettant de connecter une ou plusieurs stations à un point d'accès.

[0025] Ce réseau de télécommunication peut être un réseau local sans fil, communément appelé WLAN pour « Wireless Local Area Network » en anglais.

[0026] Ce réseau local sans-fil peut être conforme aux protocoles Wi-Fi, ou wifi, tels que spécifiés dans les documents normatifs de l'IEEE de la famille 802.11 (ou ISO/CEI 8802-11).

[0027] Un tel réseau est identifié par un identifiant de réseau SSID (pour « service set identifier ». En mode infrastructure (connexion d'une station à un point d'accès), il sert à identifier le point d'accès sans-fil.

[0028] Les stations peuvent être de différentes natures, leur commun étant de disposer de moyens permettant la connexion au réseau. Il s'agit essentiellement de composants de radiocommunication et de composants électroniques et informatiques permettant la mise en œuvre des piles protocolaires nécessaires à la gestion des protocoles associés au réseau et à la réception et à l'émission de paquets de données.

[0029] Sur la [Fig.1], trois types de stations STA sont représentés : un ordinateur ORD, un terminal mobile de communication, MOB, et un téléviseur connecté TV.

[0030] Le terminal mobile MOB est typiquement un téléphone intelligent de type « smartphone » ou une tablette numérique…. L'ordinateur peut être un ordinateur fixe (ou « desktop » selon le vocabulaire en langue anglaise) ou portable (ou « laptop »).

[0031] Le téléviseur TV peut être nativement connecté ou l'être par le truchement d'un dispositif associé tel que par exemple une clé HDMI connecté au téléviseur.

[0032] Un exemple de dispositif externe communiquant avec un téléviseur TV est Chromecast. Le Chromecast est un appareil lecteur de flux multimédias (passerelle multimédia) en temps réel développé et commercialisé par Google. L'appareil se branche sur le port HDMI d'un téléviseur et communique, par connexion Wi-Fi, avec un autre appareil connecté à Internet (ordinateur, smartphone, tablette…), afin d'afficher sur le téléviseur le contenu multimédia reçu depuis une application compatible avec la technologie Google Cast, depuis le navigateur Google Chrome présent sur un ordinateur, ou depuis certains appareils Android.

[0033] Bien évidemment d'autres types de stations STA peuvent être amenés à se connecter à un réseau local sans-fils. On peut notamment citer les objets connectés qui, dans le cadre de l'internet des objets (IoT pour « Internet of Things »), se connectent entre eux ou à un serveur afin de déployer l'ensemble de leurs fonctionnalités.

[0034] Selon un mode infrastructure de déploiement, les stations se connectent au réseau local sans fil via un ou plusieurs points d'accès PA. Ces points d'accès agissent comme des concentrateurs, au travers desquels les flux de données depuis/vers les stations transitent obligatoirement.

[0035] Ces points d'accès permettent donc le contrôle de l'accès au réseau local sans fil par les stations STA. Celles-ci doivent s'identifier auprès d'un point d'accès et celui-ci, le

cas échéant, leur accorde les droits correspondant à son profil. Si elle ne peut s'identifier correctement, la station ne peut pas accéder au réseau local sans-fil.

[0036] Ce réseau local sans fil peut être un réseau domestique, c'est-à-dire correspondant au domicile d'un utilisateur.

[0037] Le réseau local sans fil peut également être un réseau d'entreprise, notamment pour des petites entreprises (PME/TPE), des lieux accueillants le public (restaurants, bars, cafés…), etc.

[0038] Les points d'accès peuvent également être de différentes natures, notamment en fonction du type de lieu dans lequel est déployé le réseau local sans fil.

[0039] Un point d'accès peut être un dispositif dédié, commercialisé en tant que tel. Il peut également former une passerelle vers un réseau extérieur tel qu'internet.

[0040] A titre d'exemple, les boitiers permettant l'accès à internet depuis un environnement domestique offrent habituellement la fonction de point d'accès Wi-Fi.

[0041] Par exemple, dans un environnement domestique, le point d'accès peut être embarqué dans un boitier de connexion à internet, communément appelé « box internet » ou passerelle domestique.

[0042] La connexion d'une station à un point d'accès nécessite une phase d'authentification de cette station STA auprès du point d'accès PA.

[0043] Dans le cadre d'un réseau Wi-Fi, le mode de sécurité WPA2-Personnal peut être utilisé. De nombreux équipements sont compatibles à ce mode de sécurité. Il est particulièrement adapté à un environnement familial, dans lequel l'accès est contrôlé par des phrases secrètes (ou « mots de passe ») et non pas par des serveurs d'authentification tels que des serveurs Radius.

[0044] D'autres mode de sécurité sont également envisageables, tels que par exemple WPA3-Personnal.

[0045] Cette phase d'authentification peut être une poignée de main en 4 passes (ou « 4-way handshake » selon la terminologie plus commune en anglais), telle que définie par la norme IEEE 802.11i. Cette norme définie un mécanisme d'authentification communément appelé WPA2 (pour « Wi-Fi Protected Access 2 », accès protégé pour Wi-Fi 2).

[0046] Toutefois, d'autres mécanismes peuvent être possibles, notamment de futures évolutions des protocoles définis pour les normes Wi-Fi ou pour d'autres familles de protocoles qui pourraient par exemple en être issus.

[0047] Ce mécanisme est un échange de 4 messages transitant entre une station STA et un point d'accès PA qui permet de :

- confirmer la connaissance mutuelle d'une clé commune et d'ainsi assurer une certaine forme d'authentification, et de
- dériver et installer des clés temporelles sur la station et sur le point d'accès et

de fournir l'assurance de l'utilisation de nouvelles clés de chiffrement et d'intégrité.

[0048] Cette clé commune peut être une clé PMK (pour « Pairwise Master Key » en anglais).

[0049] Un mode de déploiement d'un réseau local sans fil est nommé mode « personnel » ou PSK pour « Pre-Shared Key » en anglais ou clé pré-partagée). Dans ce mode de déploiement, la clé maître PMK est calculée préalablement par l'utilisateur de la station et le point d'accès.

[0050] Typiquement, cette clé maître PMK dérive de la PSK (communément appelée phrase secrète). La phrase secrète peut être configurée par un administrateur au sein des paramètres du point d'accès.

[0051] L'administrateur peut la communiquer aux utilisateurs potentiels du réseau local qui peuvent la saisir lors de leurs tentatives de connexion au réseau local. Beaucoup de stations disposent d'un système d'exploitation offrant la possibilité de stocker la phrase secrète de sorte que l'utilisateur n'ait pas à la saisir à nouveau.

[0052] La phrase secrète peut contenir 8 à 63 caractères ASCII ou 64 symboles hexadécimaux (256 bits). Si une phrase secrète sous forme de caractères ASCII est utilisée, elle est convertie vers une clé maître PMK de 256 bits, en appliquant par exemple une fonction de dérivation de clé PBKDF2.

[0053] Ce mécanisme de dérivation PBKDF2 (abréviation de « Password-Based Key Derivation Function 2 », fonction de dérivation de clé basée sur un mot de passe ») est par exemple décrit dans la page wikipedia associée : https://fr.wikipedia.org/wiki/PBKDF2.

[0054] Dans un autre mode de déploiement, un serveur d'authentification peut être mis en place et ce dernier dérive la clé maître et la distribue aux stations et aux points d'accès. Ce serveur d'authentification peut être conforme à la norme IEEE 802.1X

[0055] Dans le procédé proposé, une pluralité de clés primaires (PMK par exemple) peut être définie, chacune étant associée à un profil d'accès au réseau local sans-fil. Le point d'accès a alors la connaissance de l'ensemble de ces clés primaires tandis que chaque station n'a connaissance que d'un (ou plus généralement d'un sous-ensemble) de ces clés primaires.

[0056] Ainsi, un administrateur peut communiquer à chaque station une clé primaire, ou une phrase secrète correspondant, qui corresponde au profil qu'il souhaite lui attribuer.

[0057] Il est ainsi possible de définir autant de profil que souhaité, simplement en provisionnant dans le point d'accès une clé primaire et d'associer cette clé primaire aux droits d'accès (et autres paramètres) correspondant à ce profil.

[0058] La clé maître PMK n'est jamais directement utilisé pour le chiffrement ou le contrôle d'intégrité. Elle est utilisée pour la génération de clés de chiffrement temporaires,

PTK, pour les échanges entre un point d'accès PA et une station STA donnés.

[0059] La clé temporaire PTK (pour « Pairwise Transcient Key ») comporte en fait plusieurs clés temporelles, chacune ayant un usage dédié :

- la clé de confirmation de clés, KCK (pour « Key Confirmation Key »), qui est principalement utilisée lors de la poignée de main en 4 passes (4-way handshake),
- la clé de chiffrement de clés, KEK (pour « Key Encryption Key),
- la clé temporaire TK (pour « Temporary Key »),
- la clé MIC temporaire, TMK (« Temporary MIC Key »).

[0060] La clé temporaire PTK est dérivée de la clé maître PMK, d'une chaîne de caractères fixe, de l'adresse MAC du point d'accès, de l'adresse MAC de la station, et de deux nombres aléatoires générés un par la station et l'autre par le point d'accès.

[0061] La [Fig.2] illustre le mécanisme de 4-way handshake proposé.

[0062] Dans un premier message $m_1$le point d'accès PA transmet un premier nombre aléatoire à la station STA qui souhaite s'authentifier. Selon la norme 802.11i, ce nombre aléatoire s'appelle « Anonce ».

[0063] Dans une étape E1, la station STA génère un second nombre aléatoire, appelé « Snonce » selon la norme 802.11i.

[0064] A partir de deux nombres aléatoires, de la clé maître PMK, et des adresses MAC, le point d'accès PA peut déterminer la clé temporaire PTK.

[0065] La station STA peut alors transmettre un message m_2 vers le point d'accès PA contenant le second nombre aléatoire, Snonce, et un code d'intégrité, MIC (pour « Message Integrity Check ») en utilisant la clé de confirmation de clés, KCK (issue de la clé temporaire PTK).

[0066] Ce message m_2 n'est pas chiffré. A sa réception, dans une étape E2, le point d'accès peut donc extraire le second nombre aléatoire, Snonce. Il peut alors calculer elle-même, de la même façon que le point d'accès, une clé temporaire PTK.

[0067] Dans le procédé proposé, le point d'accès dispose d'une pluralité de clés communes. Ces clés communes peuvent être des clés primaires PMK à partir desquelles, il peut dériver autant de clés temporaires PTK qu'il y a de clés primaires PMK.

[0068] Il n'existe par ailleurs pas de limites théoriques au nombre de clés communes mémorisés dans un point d'accès et donc utilisable par une station, et donc aucune limite au nombre de profils d'accès possibles.

[0069] A partir de cette clé temporaire, le point d'accès peut alors vérifier l'intégrité du message reçu. Cette vérification peut consister à vérifier l'intégrité du champ d'intégrité MIC contenu dans le second message. Il peut ainsi s'assurer que la station STA connaît bien la clé primaire PMK car elle a pu correctement dériver la clé temporaire PTK, puis les clés temporelles (clé de confirmation de clés, KCK) ayant

permis la génération du code d'intégrité, MIC.

[0070] Le point d'accès peut vérifier l'intégrité du message m_2 en utilisant une pluralité de clés stockées.

[0071] Il peut vérifier l'intégrité du message de façon itérative avec les clés de la pluralité stockée. Si une clé testée ne permet pas de vérifier l'intégrité, alors une nouvelle clé est testée (flèche rebouclant sur l'étape E2, sur la [Fig.2]). Si une clé testée permet de vérifier l'intégrité du message, alors les tests peuvent s'interrompre et cette clé est sélectionnée. Si aucune clé ne permet de vérifier l'intégrité du message m_2 alors la connexion de la station STA est rejetée.

[0072] Ces clés stockées peuvent être des clés primaires PMK.

[0073] Selon un mode de réalisation, la pluralité de clés stockés est mémorisée au sein du point d'accès PA sous forme d'une liste. Le point d'accès PA peut parcourir la liste et vérifier l'intégrité du message m_2 reçu de la station pour chaque clé de la liste jusqu'à ce qu'une clé permette effectivement de vérifier l'intégrité du message.

[0074] Le point d'accès peut alors stopper le parcours de la liste car on peut supposer que chaque clé n'est stockée qu'une fois dans la liste.

[0075] Il peut alors attribuer un profil d'accès à la station, correspondant à cette clé stockée.

[0076] Ainsi, le point d'accès peut mémoriser un ensemble de correspondance entre une clé et un profil.

[0077] Le profil peut être stocké sous la forme d'un identifiant de profil, ou bien d'un ensemble de paramètres qui le définissent. Ces paramètres sont typiquement des droits d'accès.

[0078] L'identifiant de profil peut définir, directement ou indirectement, un réseau local virtuel. Ce réseau virtuel peut être de type VLAN pour « Virtual Local Area Network ». Ce réseau local virtuel permet de définir des droits d'accès au réseau local sans-fil pour la station concernée, avec la granularité souhaitée.

[0079] La mémoire du point d'accès peut contenir un ensemble d'associations sous la forme du tableau suivant :

[0080] [Tableaux1]

PMK1	VLAN1
PMK2	VLAN2
PMK3	VLAN3

[0081] Chaque clé est ainsi associée à un réseau virtuel correspondant au profil d'accès correspondant à la clé et définissant les droits d'accès de la station au réseau.

[0082] Respectivement, dans l'exemple du Tableau 1, la clé maître PMK1 est associée à un réseau local virtuel VLAN1, la clé maître PMK2 est associée à un réseau local virtuel

VLAN2 et la clé maître PMK3 est associée à un réseau local virtuel VLAN3.

[0083] On peut tout à fait prévoir que plusieurs clés soient associées à un même profil. Cela peut être le cas si l'on souhaite prévoir des évolutions dans les droits d'accès et pouvoir gérer ces évolutions simplement en modifiant les associations sans avoir à changer les clés maîtres communiqués aux différents utilisateurs et, paramétrés dans les différentes stations d'un parc informatique/domotique.

[0084] Les profils peuvent correspondre à des membres d'une famille (parents, enfants…) et à des visiteurs, pour un réseau domestique. Ils peuvent correspondre à différents rôles au sein d'une entreprise de type TPE/TPE, etc.

[0085] En particulier, les profils d'accès peuvent régir l'accès à un réseau extérieur au réseau local privé (Internet, extranet…), à certaines ressources locales (disques durs connectés, imprimante connectée…), etc.

[0086] Certains profils peuvent n'avoir accès qu'au réseau Internet, accessible à travers du réseau local, mais pas aux ressources locales connectées au réseau local. Cela peut par exemple le cas d'un visiteur, auquel on confère un accès gratuit à Internet et à une ressource particulière (type imprimante) mais dont on ne veut pas qu'il puisse accéder aux données personnelles de la famille ou de l'entreprise.

[0087] Inversement, certains profils peuvent n'avoir accès aux ressources locales mais pas à Internet. Cela peut par exemple être le cas d'un enfant en dessous d'un certain âge, pour un réseau domestique.

[0088] Également, les ressources locales peuvent être catégorisées, de sorte que certaines ressources peuvent n'être accessibles que pour certains profils.

[0089] En résumé, toutes sortes de configuration sont envisageables dans le cadre du procédé de connexion proposé, qui propose donc une très grande souplesse dans la gestion des droits d'accès.

[0090] Un profil d'accès peut être attribué aisément à un utilisateur en lui fournissant la phrase secrète, ou clé maître, associée. Le mécanisme est donc extrêmement simple à mettre en place, et la même phrase secrète peut être utilisé par un utilisateur sur l'ensemble de ses stations, de sorte à obtenir ainsi un même profil d'accès.

[0091] En outre, ce mécanisme est indépendant de l'adresse physique (MAC) de chaque station, et ne souffre donc pas de la problématique des adresses physiques dynamiques comme certaines propositions de l'état de la technique.

[0092] Les réseaux locaux virtuels peuvent être déployés en amont, par exemple lors de l'initialisation d'un des points d'accès du réseau de télécommunication sans-fil. Ils peuvent également être déployés par un point d'accès lorsque celui-ci reçoit un message d'une station correspondant à un réseau local virtuel.

[0093] Lorsqu'une station détermine un profil d'accès pour une station donnée, elle peut donc vérifier si le réseau local virtuel correspondant est déployé, et si non, déclencher

son déploiement.

[0094] Un message m_3 peut alors être transmis à la station STA, conformément aux spécifications de la norme IEEE 802.11i.

[0095] Ce troisième message m_3 contient une clé temporaire de groupe, GTK (« Group Transcient Key »), chiffrée avec la clé de chiffrement de clés, KEK, et dérivée d'une clé maître de groupe, GMK (« Group Master Key ») et d'un nombre aléatoire « GNonce », ainsi qu'un champ d'intégrité, MIC, calculé sur le contenu de ce troisième message.

[0096] A réception de ce troisième message m_3, la station initie une étape E3 de vérification de l'intégrité du message reçu. Cette vérification peut consister à vérifier l'intégrité de ce champ d'intégrité MIC. Cela permet de s'assurer que le point d'accès connaît bien la clé maître PMK et qu'il a correctement dérivé la clé temporaire PTK puis les clés temporelles (notamment la clé de chiffrement de clés, KEK).

[0097] Le 4e message, m_4, permet d'acquitter la réussite de l'ensemble de la phase d'authentification « 4-way handshake ». Il indique que la station a correctement installé les clés et qu'il est prêt à commencer le chiffrement des données. A sa réception, la station et le point d'accès savent que chaque partie a obtenu, calculé et installé les diverses clés de chiffrement du protocole.

[0098] A ce stade, le point d'accès peut effectivement connecter la station STA au réseau local virtuel correspondant.

[0099] Dans ce mode de réalisation basé sur les spécifications de la norme IEEE 802.11i, on voit donc qu'uniquement l'étape E2, mise en œuvre par le point d'accès PA est modifié. Le protocole en lui-même n'est pas modifié et la station STA n'est pas non plus impactée.

[0100] Ainsi, la section 8.5.3.2 de la norme IEEE 802.11i, décrit une étape a) de dérivation d'une clé maître PTK, une étape b) de vérification du champ MIC du message 2 (c'est-à-dire du message m_2 tel que précédemment décrit).

[0101] Une étape c) peut être prévue pour si l'authentificateur gèrent plusieurs clés maître, PTK, reprendre à l'étape a) en essayant une nouvelle clé maître PTK.

[0102] Différents profils peuvent être définis pour les différents membres de la famille, notamment pour les enfants mineurs par exemple, mais le contrôle d'accès vise également à interdire l'accès au réseau pour des tiers qui seraient à l'extérieur du domicile mais dans la portée radio des points d'accès.

[0103] Dans ces diverses situations, différents profils peuvent être définis, notamment pour le public autorisé à utiliser le réseau local (ou non), le personnel de l'entreprise, etc.

[0104] Les clés primaires (ou les phrases secrètes permettant de les générer) peuvent être partagés de façon connue en soi, mais chacune de façon différenciée à des utilisateurs distincts : chaque utilisateur disposera alors d'une clé primaire, qu'il pourra utiliser

avec sa station STA, afin d'obtenir l'accès au réseau local avec des droits d'accès conférés par son profil. La station peut notamment se connecter à un réseau local virtuel correspondant à ce profil et déterminée par la clé primaire saisie par l'utilisateur.

[0105] Bien entendu, la présente invention n'est pas limitée aux exemples et au mode de réalisation décrits et représentés, mais est défini par les revendications. Elle est notamment susceptible de nombreuses variantes accessibles à l'homme de l'art.

Revendications

[Revendication 1] Procédé de connexion d'une station à un point d'accès d'un réseau de télécommunication sans-fil comportant une phase d'authentification dans lequel ladite station (STA) utilise une clé pour transmettre un message (m_2) vers ledit point d'accès (PA), et dans lequel ledit point d'accès vérifie l'intégrité dudit message en utilisant une pluralité de clés stockées, et, si une clé stockée parmi ladite pluralité permet de vérifier ladite intégrité, attribue un profil d'accès à ladite station, correspondant à ladite clé stockée.

[Revendication 2] Procédé selon la revendication précédente dans lequel ladite phase d'authentification est conforme à la norme IEEE 802.11i et ladite clé est une clé primaire, PMK.

[Revendication 3] Procédé selon la revendication précédente, dans lequel ledit message est un second message d'un processus de poignée de main à 4 voies.

[Revendication 4] Procédé selon l'une des revendications précédentes dans lequel ledit profil d'accès correspond à un réseau local virtuel.

[Revendication 5] Procédé selon l'une des revendications précédentes dans lequel ledit profil d'accès détermine un accès à un réseau extérieur et/ou aux ressources locales connectées audit réseau local sans-fil.

[Revendication 6] Procédé selon l'une des revendications précédentes, dans lequel ledit point d'accès parcourt ladite pluralité en testant chaque clé stockée pour vérifier l'intégrité dudit message jusqu'à ce qu'une clé donnée vérifie ladite intégrité, et attribue ledit profil correspondant à ladite clé donnée.

[Revendication 7] Point d'accès (PA) à un réseau de télécommunication sans-fil, comprenant un processeur configuré pour permettre la connexion d'une station (STA) à la suite d'une phase d'authentification dans lequel ledit point d'accès reçoit de la part de ladite station (STA) un message (m_2), et dans lequel ledit point d'accès vérifie l'intégrité dudit message en utilisant une pluralité de clés stockées, et, si une clé stockée parmi ladite pluralité permet de vérifier ladite intégrité, attribuer un profil d'accès à ladite station, correspondant à ladite clé stockée, ledit profil d'accès étant utilisé pour ladite connexion.

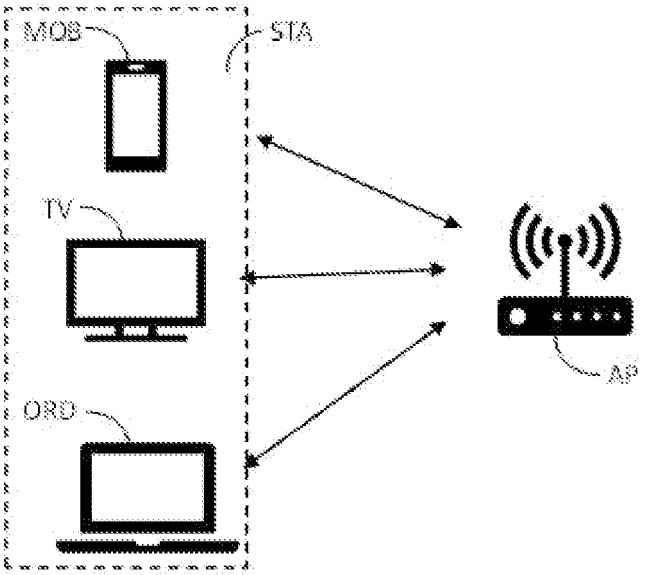
[Revendication 8] Boitier d'accès à Internet comprenant un point d'accès selon la revendication précédente.

[Revendication 9] Programme d'ordinateur apte à être mis en œuvre sur un point d'accès à un réseau de télécommunication sans fil, le programme comprenant des instructions de code qui, lorsqu'il est exécuté par un processeur, réalise

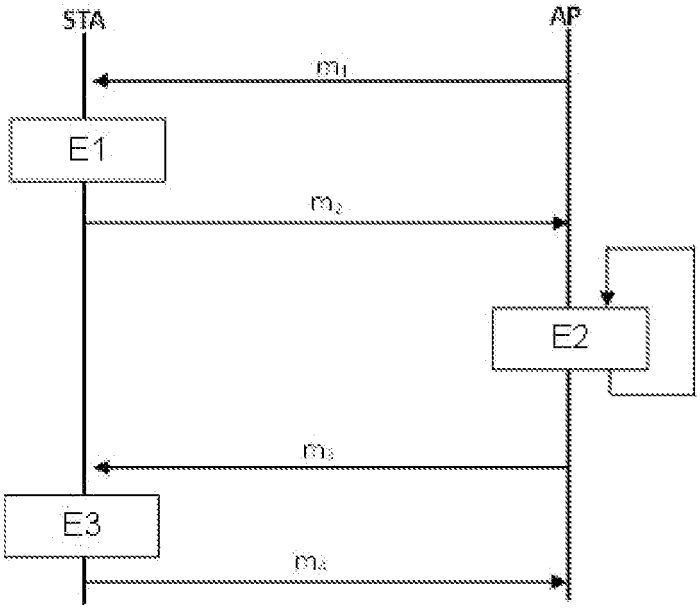
les étapes du procédé défini dans les revendications 1 à 6.

[Revendication 10] Support de données sur lequel a été mémorisé au moins une série d'instructions de code de programme pour l'exécution d'un procédé selon l'une des revendications 1 à 6.

[Fig. 1]



[Fig. 2]



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 917042
FR 2302492

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 2018/131519 A1 (LE SCOUARNEC NICOLAS [FR] ET AL) 10 mai 2018 (2018-05-10) * figure 3 * * alinéas [0065] - [0070] * -----	1-10	H04L 9/08 H04L 9/32 H04W 74/00
X	US 2006/107050 A1 (SHIH CHIH-HENG [TW]) 18 mai 2006 (2006-05-18) * alinéas [0019] - [0022] * -----	1-10	
A	US 2021/099876 A1 (NEIPRIS EDWARD W [US] ET AL) 1 avril 2021 (2021-04-01) * figure 4B * * alinéas [0016], [0019], [0020], [0024] - [0033], [0045], [0046] * -----	1-10	
A	US 2022/060899 A1 (HARDING MUIR LEE [US] ET AL) 24 février 2022 (2022-02-24) * figure 2A * * alinéas [0027], [0028], [0071] * -----	1-10	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04W

Date d'achèvement de la recherche	Examinateur
26 septembre 2023	Kufer, Léna

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

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2302492 FA 917042

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 26-09-2023
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
US 2018131519 A1	10-05-2018	BR 102017023626 A2	29-05-2018
		CA 2983550 A1	04-05-2018
		CN 108023731 A	11-05-2018
		EP 3319295 A1	09-05-2018
		JP 2018110378 A	12-07-2018
		KR 20180050233 A	14-05-2018
		MY 181840 A	08-01-2021
		RU 2017138066 A	06-05-2019
		US 2018131519 A1	10-05-2018
		US 2020287720 A1	10-09-2020
US 2006107050 A1	18-05-2006	TW I268083 B	01-12-2006
		US 2006107050 A1	18-05-2006
US 2021099876 A1	01-04-2021	CA 3152918 A1	08-04-2021
		EP 4038925 A1	10-08-2022
		IL 291779 A	01-06-2022
		JP 2022550181 A	30-11-2022
		KR 20220076491 A	08-06-2022
		US 2021099876 A1	01-04-2021
		US 2022322091 A1	06-10-2022
		WO 2021067082 A1	08-04-2021
US 2022060899 A1	24-02-2022	EP 4201090 A1	28-06-2023
		JP 2023540264 A	22-09-2023
		US 2022060899 A1	24-02-2022
		WO 2022046798 A1	03-03-2022

EPO FORM P0465