MINISTRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECEHERCHE SCIENTIFIQUE

UNIVERSITE FERHAT ABBAS – SETIF
UFAS ALGERIE

MEMOIRE

Présenté à la Faculté des Sciences de l'Ingénieur
Département d'Informatique
Pour l'Obtention du Diplôme de

MAGISTER en INFORMATIQUE

Option : Sciences et Technologies de l'Information et de la Communication (STIC)

Par

Mme : Zidani Ferroudja

Thème

Solution d'authentification et de gestion de clés pour le standard 802.11i des réseaux WiFi

---

Soutenu le : devant la commission d'examen :

Dr Abdelouahab .Moussaoui	M.C	UFAS	Président
Dr Abdallah Boukerram	M.C	UFAS	Rapporteur
Dr Makhlouf Alliouat	C.C	UFAS	Examinateur
Dr Chabane Khentout	C.C	UFAS	Examinateur
Dr Mabrouk Nekkache	C.C	UFAS	Examinateur

Dédicaces

Je dédie ce modeste travail

A tous ceux qui me sont les plus chers : mon mari, mon père, ma mère, ma sœur Saida et mes deux frères Mounir et Lamine.

A toute la famille,

A mes amies et collègues

Et à tous ceux qui m'ont aidé.

Remerciements

Je remercie tout d'abord le bon dieu pour m'avoir donné le courage et la santé pour accomplir ce travail.

Mes vifs remerciements accompagnés de toute ma gratitude vont ensuite à mon encadreur Boukerram Abdellah, maître de conférence à l'université de Setif, pour avoir accepté de m'encadrer et pour ses conseils.

Je remercie également les membres de Jury qui ont accepté de juger mon travail.

Enfin, je remercie ma famille et mes ami(e)s pour leur aide et leur soutien précieux durant cette année.

Résumé

La transmission radio rend les réseaux sans fil, commodes d'usage, facile à déployer, et économique, mais soulève par contre des problèmes de la sécurité, dues à la nature ouverte des supports de transmission utilisés. Ajouté à cela les exigences de sécurité doivent être vérifiées notamment l'anonymat et la protection à long terme des données. Dans cette optique, on a proposé une méthode d'authentification EAP/AH (méthode d'Authentification Hybride) qui, basée sur le chiffrement symétrique et asymétrique permet d'assurer outre les services de sécurité classique l'anonymat et la protection à long terme des données.
Dans ce mémoire on a identifié les vulnérabilités du 802.11i, un standard développé pour améliorer la sécurité des réseaux 802.11 au niveau MAC en proposant une nouvelle architecture de sécurité appelée RSN (Rubust Security Network) dont l'apport est essentiellement dans l'utilisation du standard 802.1x pour l'authentification et un contrôle d'accès, le 4-way handshake pour la génération des clés fraîches de session et le protocole AES (Advenced Encryption Standard) pour le cryptage. Dans RSN l'une des méthodes d'authentification qui s'appuis sur 802.1x/EAP est exécutée pour établir une clé maître (PMK) entre la station et le serveur d'authentification, cette dernière sera par la suite utilisée dans la procédure de gestion de clés (4-way handshake) pour fournir une authentification mutuelle entre le point d'accès et le client et la génération des clés temporaires de session. Toute fois a cause du protocole EAP qui ne contient aucun mécanisme pour vérifier l'intégrité des messages de notification, l'attaque « Man-In-The-Middle » peut contourner tout type de méthode d'authentification, pour cela on a modifié le 4-way handshake de sorte à faire un seul processus avec la méthode d'authentification EAP/AH, cela a permit d'éviter, outre l'attaque contre les messages de notification, l'attaque par force bute contre le deuxième message du 4-way handshake.
Du fait que la mobilité est l'un des avantages des réseaux sans fil, des protocoles doivent être mis en œuvre pour une réauthentification rapide et efficace. Pour cela, on a aussi proposé une solution d'authentification pour le roaming, basé sur notre modification pour le 4-way handshake, permet à un client mobile d'obtenir une clé maître quand il change de point d'accès du même sous réseau sans exécuter le processus d'authentification.

Mots clefs: sécurité, WiFi, 802.11i, méthode d'authentification, 4-way handshake, roaming

Abstract

The transmission radio makes the wireless networks, dressers of use, easy to open out, and economic, but raises problems of the security, due to the nature opened of the used transmission media. Added to it the requirements of security must be verified notably anonymity and the long-term protection of data. In this optics, we proposed a method of authentification EAP/AH (Authantification Hybid méthod) which, based on the symmetrical and asymmetric ciphering permits to assure besides the classic of secutity services anonymity and the long-term protection of data.
In this dissertation we identified the vulnerabilities of the 802.11i, a standard developed to improve the security of the networks 802.11 in the MAC level whith proposing a new architecture of security named RSN (Rubust Security Network) whose contribution is essentially in the use of the standard 802.1x for the authentification and a control of access, the 4 way handshake for the generation of the cool keys of session and the AES protocol (Advenced Encryption Standard) for the encryption. In RSN one of the authentification methods that himself supports out of 802.1x/EAP are executed to establish a main key (PMK) between the station and the server of authentification, this last will be used thereafter in the procedure of management of keys (4-way handshake) to provide a mutual authentification between the access point and the customer and the generation of the temporary keys of session.
All time because of the EAP protocol that contains no mechanism to verify the integrity of the notification messages, the attack " Man-In-Tea-Middle" can get round all type of authentification method, for it we modified the 4 way handshake in order to make only one process with the method of authentification EAP/AH, it has permitted to avoid, besides the attack against the messages of notification, the attack by strength stumbles against the second message of the 4-way handshake.
Because the mobility is one of the advantages of the wireless networks, some protocols must be put of it. uvre for a fast and efficient réauthentification. For it, we also proposed a solution of authentification for the roaming, based on our modification for the 4-way handshake, allows a mobile station to get a main key when it changes access point of the same under network without executing the process of authentification.

Keywords: **Security, WiFi, 802.11i, method of authentification, 4-way handshake, roaming,**

ملخص

إن نضام الإرسال على موجات الراديو يجعل شبكات الإعلام الآلي اللاسلكية سهلة الاستعمال و البسط، و اقتصادية، لكنه يطرح مشاكل أمنية ناتجة عن طبيعة النواقل المستعملة.زيادة على هذا، متطلبات على المستوى الأمني يجب أن تكون متوفرة ، خاصة الحماية و الوقاية الطويلة المدى للمعلومات.

في هذا النطاق اقترحنا طريقة التعرف Protocole d'Authentification Hybride (EAP/AH)
. المتمركز على الشفرة المتناضرة و اللامتناضرة يوفر زيادة على الخدمات الأمنية المعروفة، الحماية و الوقاية الطويلة المدى للمعلومات.

في هذه المذكرة تعرفنا على نقاط ضعف نضام 802.11i المنجز خصيصا لتحسين أمن الشبكات 802.11 على المستوى MACباقتراح هندسة جديدة للحماية تسمى RSN (Rubust Security Network) تساهم خاصة في استخدام أنظمة 802.1 x لمراقبة العبور و التعرف، و نضام 4 way handshake لإنتاج مفاتيح (Session)، و نظام AES (Advenced Encryption Standard) للشفرة .في RSN، إحدى طرق التعرف المركزة على نظامEAP /802.1 x تطبق لإنتاج مفتاح أساسي (PMK) بين Station و Serveur التعرف، الذي يستعمل في ما بعد في منهاج تسيير المفاتيح (4 way handshake) لإعطاء تعرف متبادل بين Point d'accès.و Station لإنتاج مفاتيح (Session) مؤقتة . بما أن نضام EAP لا يملك أي وسيلة لمراقبة هيئة الرسائل الإعلانية فإن هجوم « Man-In-The-Middle » قد يستطيع أن يشكل خطر على كل طرق التعرف ، و لهذا أحدثنا تغيير في ال 4 way handshake من أجل الحصول على Processus واحد مع طريقة التعرف EAP/AH و هذا يسمح من جهة بمنع هجوم ضد الرسائل الإعلامية و من جهة اخرى الهجوم بالقوة ضد الرسالة الثانية لـ 4 way handshake .

بما أن التحرك من المزايا الأساسية للشبكات اللاسلكية فمن الواجب إنجاز أنظمة التعرف السريع و المضمون، في هذا النطاق اقترحنا أيضا حلا للتعرف ل(Roaming) المتمركز على التغيير الذي أحدثناه على ال(4 way handshake) و الذي يسمح لـ Station متحركة بالحصول على مفتاح رئيسي (PMK)عندما تبدل Point d'accès في نفس جزء الشبكة بدون تطبيق التعرف .

كلمات المفتاح: **أمن، WiFi، i 802.11، طريقة التعرف، 4 way handshake ، التحرك**

Table des matiéres

Introduction générale

Chapitre I : Réseaux sans fil et réseaux de mobiles

I.1. Introduction 4

I.2. Réseaux de mobiles et réseaux sans fil 4

I.3. Réseaux sans fil vs réseaux filaire 4

I.3.1. Avantages 4

I.3.2. Inconvénients 5

I.4. Classifications des réseaux 6

I.4.1. Classification suivant la distance séparant les terminaux mobiles 6

I.4.2 Classification suivant l'infrastructure 10

Chapitre II : Les réseaux WiFi

II.1. Introduction 12

II.2. Architecture du réseau 802.11 12

II.3. Modèle en couche 13

1. La couche physique 13

2. La couche liaison de données 16

2.1. Introduction 16

2.2. La structure des trames MAC 802.11 16

2.3. Quelques fonctionnalités de la couche MAC : 17

2.3.1. Accès au support 17

2.3.2. Mobilité 21

2.3.3. Le contrôle d'erreur 23

2.3.4. L'économie d'énergie 23

2.4. Les évolutions de la couche MAC 24

II.4 . Les équipements WIFI : 24

II.5. Conclusion 26

Chapitre III : La sécurité dans les réseaux WiFi

III.1. Introduction : 27

III.2. Les attaques d'un réseau WiFi : 27

2.1. Le War Driving: 27

2.2. L'espionnage: 27

2.3. L'intrusion 28

2.4. Le déni de service (DoS) 29

2.5. La modification de messages 29

Les attaques MIM (Man-In-The-Middle) 29

III.3. Cryptographie et services de sécurité 30

Introduction 30

1. Confidentialité : 30
2. Intégrité du message : 32
3. Authentification: 33
III. 4. Les Protocoles de sécurité 802.11 36
4.1.2. Mécanisme de gestion des clés WEP : 37
4.1.3. Quelques vulnérabilités du WEP 38
4.2. 802.11i: 39
4.2.2. Déférence entre WPA ET WPA2: 40
4.2.3. Architectures WPA 40
4.2.4. Une connexion complète : 41
Phase 1 : Mise en accord sur la politique de sécurité 41
Phase 2 : Authentification 802.1X 42
A. Le protocole IEEE 802.1X 42
La structure d'IEEE 802.1X : 42
B. EAP 43
Phase 3 : Hiérarchie et distribution des clés 45
Le 4-way handshake : 46
Phase 4 : Chiffrement et intégrité au sein d'une RSNA 49
4.2.5. Les faiblesses de WPA/WPA2 54
III.5. Méthodes d'authentification 57
5.1. Introduction 57
5.2. Etude de quelques méthodes existantes 57
1. EAP/TLS 57
2. EAP-TTLS 60
3. EAP-MD5 61
Chapitre IV: Proposition d'une solution d'authentification et de gestion de clés
IV.1.Introduction 63
IV.2. EAP/AH (méthode d'Authentification Hybride) 64
Suppositions : 64
Processus d'échange de messages 64
IV.3.Procédure de gestion de clés de session 65
IV.4. Evaluation 67
a. Méthode d'authentification EAP/AH 67
Procédure de gestion des clés de session : 69
Architectures de RSN et de la solution proposée 69
IV.5. Le roaming 70
5.1. Etude de l'existant 70
5.2. Proposition 70
Conclusion 73
Perspectives 73
Bibliographie 75
Glossaire 79

Introduction générale

Les réseaux sans fil sont séduisants par le fait que leur transmission s'effectue par ondes électromagnétiques et non pas par câble. La communication sans fil a levé toutes les restrictions des réseaux filaires et fournit l'accès omniprésent à l'internet. De plus, l'augmentation dans la flexibilité a beaucoup motivé les technologies de réseau sans fil. Aujourd'hui, le déploiement de réseaux locaux sans fil (WLANS) est plus économe et effectif, qu'installer le réseau de câble. Avec la promotion du marché des technologies de mise en réseau sans fil, services et applications ont énormément augmentés.

La nature ouverte de support de transmission des réseaux sans fil, les rend bien plus vulnérables que les réseaux conventionnels. En effet, ce mode de transmission a pour effet d'avoir la possibilité d'intercepter les données envoyées et/ou reçues sur le support et par la suite de pouvoir modifier et rejouer les données. L'intrus peut également injecter, saturer ou endommager les équipements du réseau.

Les architectures de 802.11 [1] intègrent par défaut un mécanisme de contrôle d'accès et un chiffrement WEP [2]. Cependant, ces mécanismes ne résistent pas suffisamment à plusieurs attaques [3] : de la falsification de l'identité à la récupération de la clé de chiffrement. Par conséquence, le groupe de travail 802.11i [4] a été mis en place. L'architecture 802.11i appelée aussi RSN (Robust Secure Network) fournit une amélioration de la sécurité réseau au niveau MAC, elle utilise le standard IEEE 802.1X [5] pour l'authentification et le calcul d'une clé maître, le 4-way handshake pour une meilleure gestion des clés de session et permet la définition de multiples protocoles de sécurité radio : WEP, TKIP et CCMP, et des éléments d'information permettant de choisir l'un des protocoles définis.

Le standard 802.1X s'appuie sur l'encapsulation EAP (Extensible Authentification Protocol) [6] pour mettre en relation le serveur d'authentification et le système à authentifier par l'intermédiaire d'un point d'accès dans le cas des réseaux 802.11. Le protocole EAP réalise une enveloppe générique pour de multiple méthode d'authentification. Plusieurs méthodes d'authentification pour les LAN sans fil, ont été proposées, mais chacun de ces approches a une certaine limitation. En autre, la majorité ne fournit pas tous les services de sécurité ; notamment l'échange anonyme et la protection à long terme des données qui sont important dans l'environnement sans fil. En plus, la plupart des méthodes sont construites pour répondre à l'anonymat sont victimes de l'attaque MIM (Man-In-The-Middle) [7].

La procédure de gestion de clés (4-way handshake) permet de dériver les clés temporaires de session à partir de la clé maître obtenue lors du processus d'authentification 802.1X/EAP, et toutes les informations nécessaires à leurs calcul sont transmises en clair. Le second message du 4-Way Handshake peut être sujet à des attaques par force brute.

Dans ce mémoire, on à proposé une méthode EAP/AH (méthode d'Authentification Hybride), qui en combinant le chiffrement symétrique et asymétrique permet d'assurer l'ensemble des services d'authentification.

Tous les mécanismes d'authentification se terminent par une notification de succès ou d'échec à l'aide du message *EAP-Success* ou *EAP-Echec*. Due au protocole EAP lui-même, ce message ne contient aucune information qui conserve son intégrité et donc il est possible pour l'intrus de forger son propre message *EAP-Success* et de se subtiliser au point d'accès. Tout le trafic réseau du client va donc passer par lui. [8]

Afin de palier a cette problématique, on a indiqué le sucées de la phase d'authentification par un message contenant la clé maître (PMK), envoyée du client vers le serveur. De ce fait, le nombre de messages échangés lors de la phase de la hiérarchie et distribution des clés est réduit. Cela a permit d'éviter, outre l'attaque contre les messages de notification, l'attaque par force brute contre le deuxième message du 4-way handshake.

La mobilité est l'un des avantages des réseaux sans fil, des protocoles doivent être mis en œuvre pour une réauthentification rapide et efficace. Notre proposition d'authentification et de gestion de clé nous a amené à suggérer une solution d'authentification pour le roaming d'une station entre les points d'accès du même sous réseau. Elle consiste à dériver les clés maitres à partir de celle obtenue lors de sa première authentification.

Plan du mémoire

Ce mémoire est composé d'une introduction, d'une conclusion, d'une annexe et de quatre chapitres.

Le premier chapitre présente des généralités sur les réseaux mobiles et leurs caractéristiques, ainsi que deux différentes classifications des réseaux mobiles tout en faisant apparaître la position du Wi-Fi par rapport aux réseaux sans fil ;

Le deuxième chapitre décrit en détail la norme 802.11 sur laquelle repose un réseau WiFi, en se concentrant sur la couche MAC qui offre autres les fonctions d'une couche MAC classique (allocation du support, adressage, formatage des trames) des fonctionnalités supplémentaires telles que la sécurité des communications, l'économie d'énergie, la fragmentation, le réassemblage, le contrôle d'erreur ou encore comment assurer une bonne qualité de service, en particulier pour les communication multimédias ;

Le troisième est structuré en trois sections :

En section 1 on cite les différentes attaques susceptibles d'atteindre un réseau WiFi dans son mode infrastructure;

La section 2 est consacrée à une présentation détaillée de la cryptographie, les différentes techniques de cryptage des messages et la vérification de leurs intégrité ;

La section 3 dresse un état de l'art des solutions de sécurité des réseaux WiFi:

On présente le protocole WEP, première solution de sécurité proposée par le standard 802.11. Puis on analyse le standard 802.11i on se focalisant sur le standard IEEE 802.1X et son utilisation avec le protocole EAP et le 4-way handshake qui fournit une authentification mutuelle entre le point d'accès et le client et permet la génération des clés temporaires de session.

On termine le chapitre trois par la description de quelques méthodes d'authentification, on a examiné les avantages et les inconvénients de ces dernières.

Le dernier chapitre présente en détail notre proposition d'authentification et de gestion de clés pour le standard 802.11i des réseaux WiFi dans leur mode infrastructure, ainsi que notre solution d'authentification pour le roaming.

CHAPITRE I

Réseaux sans fil et réseaux de mobiles

I.1. Introduction

Après avoir développé tout un ensemble de réseaux filaires exploitant des supports de communication "cuivre" et/ou "fibre", pour la transmission de flux divers (données numériques, sons, images ...), les opérateurs télécoms et les fournisseurs de service marquent un intérêt de plus en plus fort pour la mise en oeuvre de réseaux sans fils, offrant la possibilité à l'utilisateur de se déplacer dans une zone spécifique tout en restant connecté au réseau.

Les réseaux mobiles permettent de connecter plusieurs composants mobiles en utilisant des mediums non filaires, c'est pour cela qu'on les appèlent aussi réseaux sans fil (*Wireless network*). Les réseaux sans fil utilisent les ondes radioélectriques (radio ou infrarouges) comme medium de transmission.

L'objectif principal des réseaux mobiles est de permettre à leurs utilisateurs de se déplacer tout en restant connecté dans une zone géographique plus ou moins étendu (zone de couverture), et d'accéder au réseau de n'importe où et à n'importe quel moment (communication *ubique*).

Les environnements sans fil offrent une grande flexibilité d'emploi. En particulier, ils permettent la mise en réseau des sites dont le câblage serait trop onéreux à réaliser dans leur totalité, voire même impossible

I.2. Réseaux de mobiles et réseaux sans fil

Les termes mobile et sans fil sont souvent utilisés pour décrire les systèmes existants, tels que le GSM, IS-95, IEEE 802.11, Bluetooth, etc. Toutefois, il est important de distinguer les deux catégories de réseaux que recoupent les concepts de mobile et de sans fil, de façon à éviter toute confusion [9].

Les réseaux de mobiles : Un utilisateur mobile est défini théoriquement comme un utilisateur capable de communiquer à l'extérieur de son réseau d'abonnement tout en conservant une même adresse.

Les réseaux sans fil : Le concept de sans fil est étroitement associé au support de transmission. Un système est dit sans fil s'il propose un service de communication totalement indépendant de prises murales. Dans cette configuration, d'autres moyens d'accès sont exploités, tels que l'infrarouge ou les ondes hertziennes. Réseaux filaire

I.3. Réseaux sans fil vs réseaux filaire

L'environnement mobile offre beaucoup d'avantages par rapport à l'environnement habituel. Cependant, de nouveaux problèmes peuvent apparaître.

I.3.1. Avantages

- **Mobilité**

L'utilisateur des réseaux sans fil a la possibilité de se déplacer dans le réseau tout en gardant la même adresse. Il peut accéder aux services offerts par le réseau de n'importe où et à n'importe quel moment. Cela nécessite d'une part des mécanismes de localisation de l'utilisateur, et d'autre part une gestion de la mobilité assurant la continuité des communications en cours de déplacement (*handover*).

- **Moins de fils**

Dans les réseaux mobiles, les fils sont supprimés ou moins utilisés, ça répond bien aux situations où le câblage est difficile (zones rurales, bâtiments historique,...) ou dans des situations où l'on veut réaliser un réseau temporellement (réunion de travail, conférences,...).
L'utilisation des fils est remplacée par l'utilisation des liaisons infrarouges ou des ondes radio comme canaux de communication. Les liaisons infrarouges sont très utilisées dans le cadre des télécommandes et communications courtes distances où les éléments sont en vue directe, mais sont très sensibles aux perturbations. Les ondes radio sont les plus utilisées, elles offrent une meilleure pénétration des obstacles et des débits et portées plus importants que les liaisons infrarouges.

- **Coût**

Si leur installation est parfois un peu plus coûteuse qu'un réseau filaire, les réseaux sans fil ont des coûts de maintenance très réduits ; sur le moyen terme, l'investissement est facilement rentabilisé.

- **Evolutivité**

Les réseaux sans fil peuvent être dimensionnés au plus juste et suivre simplement l'évolution des besoins.

I.3.2. Inconvénients

Faire transiter des informations sans support (ou canal) physique se révèle très pratique. Cependant les données émises le sont dans toutes les directions et sans contrôle. Cela aura plusieurs impacts :

- **La sensibilité à l'environnement**

Dans un environnement physiquement vierge, la transmission ne posera aucun problème. Par contre, s'il commence à y avoir trop d'obstacles physiques tels que des murs ou des structures métalliques, la transmission deviendra perturbée voire impossible (atténuation du signal).

- **Interférences**

On va en effet envoyer des ondes à des endroits où cela n'est pas nécessaire. Cela pourra brouiller d'autres transmissions et pourra empêcher celles-ci.

- **Débit et portée faibles**

L'une des limites de la communication sans fil vient de la relative faiblesse de la bande passante des technologies utilisées. Plusieurs facteurs limitent la portée d'une transmission sans fil, comme la faible puissance du signal, les obstacles qui empêchent, atténuent, ou réfléchissent les signaux.

- **La consommation d'énérgie**

Les équipements sans fil sont destinés à être portable et donc à utiliser des batteries. Ils doivent alors être capables de gérer leur consommation énergétique.

▪ **Difficulté de détection des collisions (Problème de la station cachée)**

Un problème spécifique du monde sans fil est le problème de la station cachée. Deux stations situées chacune à l'opposé d'un point d'accès (AP) ou d'une autre station peuvent entendre l'activité de cet AP mais ne pas s'entendre l'une l'autre du fait que la distance entre les deux est trop grande ou qu'un obstacle les empêche de communiquer entre elles.

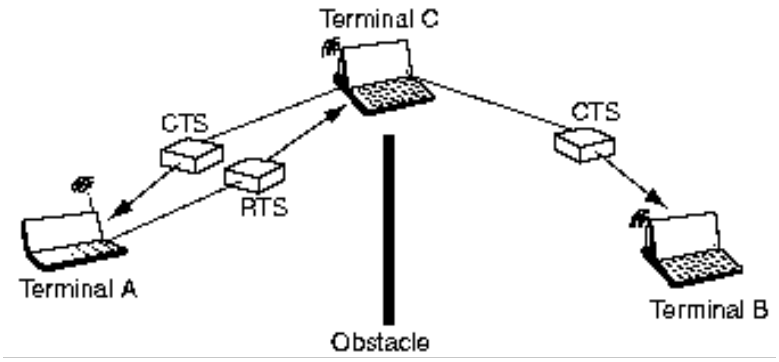

Figure 1 : Problème de la station cachée [2]

La figure 1 illustre une station A cachée de la station B mais pas de la station C. Si A transmet des informations à C et que B désire faire de même, il y aura une collision car B n'a pas détecter la transmission entre A et C.

▪ **Non sécurisé**

Les réseaux sans fil offrent de nouvelles failles aux pirates. De part la nature immatérielle du support physique, l'écoute clandestine sur un réseau sans fil est facile. Il faut donc protéger l'accès aux ressources sans fil et aux informations qui circulent dans les trames.

I.4. Classifications des réseaux

Nous présentons dans cette section deux différentes classifications englobant tous les types de réseaux sans fil : une classification suivant la distance séparant les terminaux mobiles et l'autre selon l'infrastructure du réseau.

I.4.1. Classification suivant la distance séparant les terminaux mobiles

On peut classifier les réseaux sans fil suivant les distances qui séparent les terminaux tout en permettant à ces derniers de rester connectés. Ces distances forment des zones géographiques offrant une connectivité aux terminaux, plus communément appelées zones de couverture ou cellule. La figure 2 décrit les différentes catégories de réseaux définies en fonction de la taille de la zone de couverture et la figure 3 les normes existantes.

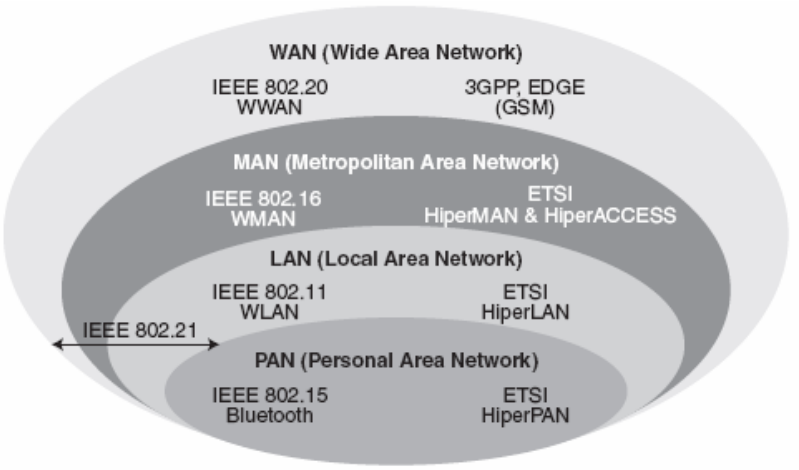

Figure 2 : Catégories de réseaux sans fil [2].

Les principales normes sont IEEE 802.15, pour les petits réseaux personnels (WPAN, Wireless Personal Area Network) d'une dizaine de mètres de portée, IEEE 802.11, ou WiFi, pour les réseaux WLAN (Wireless Local Area Network), IEEE 802.16 [10], pour les réseaux WMAN (Wireless Metropolitan Area Network) atteignant plus de dix kilomètres, et IEEE 802.20, pour les réseaux WWAN (Wireless Wide Area Network), c'est-à-dire les très grands réseaux. [2]

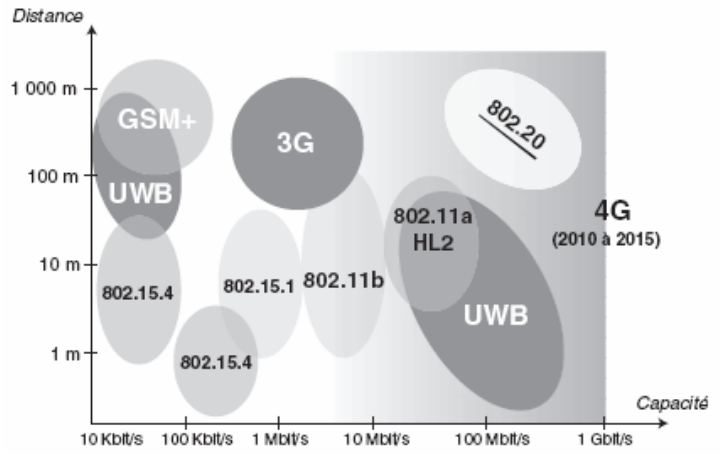

Figure 3 : Principales normes des réseaux sans fil [2].

A. Réseaux personnels sans fil (WPAN)

Le réseau personnel sans fils (appelé également réseau individuel sans fils ou réseau domotique sans fil et noté WPAN pour Wireless Personal Area Network concerne les réseaux sans fil d'une faible portée (quelques dizaines de mètres). Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes. Parmi les technologies WPAN on peut citer :

- **Bluetooth :** nom commercial de la norme IEEE 802.15.1 [11], Bluetooth est aujourd'hui présent dans de nombreux dispositifs. Malgré un débit de 1 Mb/s et une portée d'environ 30 mètres,

Bluetooth offre de nombreuses possibilités grâce à la faible consommation de ses équipements. On trouve des composants Bluetooth dans beaucoup d'ordinateurs portables mais aussi dans de nombreux périphériques (appareils photo, téléphones portables, assistants personnels, ...). La norme IEEE 802.15.3 [12] (Bluetooth2 ou UWB) est une évolution de la norme Bluetooth permettant des débits plus rapides et intégrant des mécanismes de sécurité très limités.

- **ZigBee** : avec un débit plus faible que Bluetooth, la norme IEEE 802.15.4 [13] (ZigBee) a comme objectif de consommer extrêmement peu d'énergie, de telle sorte qu'une petite batterie puisse tenir presque toute la durée de vie de l'interface, mais avec une vitesse extrêmement faible.

B. Réseaux locaux sans fil (WLAN)

Les réseaux locaux sans fil sont en train de devenir les solutions les plus courantes pour de nombreuses entreprises. Ces dernières permettent des gains intéressants qui découlent de la disparition des câbles. Les WLAN (Wireless LAN) commencent aussi à se développer dans les campus universitaires et les zones publiques tels que les gares, les aéroports, permettant à toute personne munie d'un ordinateur portable d'accéder à des services publics d'information ou encore à se connecter sur Internet à travers le réseau local. Plusieurs normes de WLAN ont été développées, nous citons dans se qui suit les deux principales : IEEE 802.11 et Hiperlan.

- **La norme IEEE 802.11**

La norme IEEE 802.11, qui a vu le jour en 1997, est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN ou Ethernet sans fil). Ce dernier est utilisé pour remplacer les réseaux LANs ou comme prolongation de l'infrastructure des LANs. La norme IEEE 802.11 est la norme initiale à partir de laquelle un certain nombre de normes dérivées ont été créées afin de répondre à des objectifs d'interopérabilité ou de sécurité. [2, 14]

Il existe aujourd'hui quatre propositions, dont les débits sont de 11 Mbit/s (IEEE 802.11b ou WiFi) et 54 Mbit/s (IEEE 802.11a ou WiFi 5 et IEEE 802.11g). Une quatrième proposition, provenant des travaux du groupe IEEE 802.11n, devrait augmenter le débit, qui pourrait atteindre 320 Mbit/s. Les fréquences utilisées se placent dans la bande 2,4-2,483 5 MHz pour les extensions b et g et dans la bande 5,15-5,3 MHz pour 802.11a. [2]

WiFi

Le nom Wi-Fi (contraction de Wireless Fidelity), parfois notée à tort WiFi, correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance, anciennement WECA (Wireless Ethernet Compatibility Alliance), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage (et pour des raisons de marketing) le nom de la norme se confond aujourd'hui avec le nom de la certification. Ainsi un réseau Wi-Fi est en réalité un réseau répondant à la norme 802.11. [2, 14, 15]

Logo officiel 

- **Hiperlan (High Performance Radio LAN)**

Hiperlan est une norme européenne, la première version (Hiperlan1) [16] a été définie en juillet 1998 par le comité RES-10 du projet BRAN (Broadband Radio Access Networks) de l'ETSI (European Télécommunications Standards Institute). Elle exploite la bande de fréquence 5 à 6,25 GHz en offrant un débit théorique de 20 Mbp/s. Une seconde version (Hiperlan2) [17] permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres.

A présent, la majorité des WLANs sont actuellement basés sur la norme IEEE 802.11, la norme européenne n'a jamais vu le jour industriellement.

Les bandes de fréquences:

WiFi utilise deux bandes de fréquences, la bande ISM (Industrial, Scientific and Medical), située dans les 2,4 GHz, pour 802.11b et 802.11g, et la bande U-NII (Unlicensed-National Information Infrastructure), située dans les 5 GHz, pour 802.11a.
Ces deux bandes sont dites sans licence, signifiant qu'il n'y a pas d'autorisation à demander ni d'abonnement à payer pour les utiliser. Elles sont toutefois réglementées en France par l'ART (Autorité de régulation des télécommunications), qui a imposé certaines contraintes pour leur utilisation et n'en a libéré qu'une partie pour les réseaux WiFi, l'autre partie ne pouvant être utilisée que sous certaines conditions.

Un inconvénient des bandes de fréquences vient du fait qu'elles ne sont pas utilisées en totalité dans WiFi, y compris la bande ISM, mais sont divisées en sous-bandes, ou canaux, sur lesquelles ont lieu les transmissions. Ces canaux étant relativement proches, leur choix doit être effectué de façon rigoureuse afin de prévenir toute interférence. [18]

C. Réseaux métropolitains sans fil WMAN (norme IEEE 802.16)

Le réseau métropolitain sans fils (WMAN pour Wireless Metropolitan Area Network) visent à remplacer les modems ADSL, que l'on trouve sur les réseaux téléphoniques fixes, pour donner à l'utilisateur final des débits importants pour du hertzien, jusqu'à plusieurs mégabits par seconde. Ces réseaux forment ce que l'on appelle la boucle locale radio (BLR). Plusieurs normes sont proposées suivant la fréquence utilisée. La norme IEEE 802.16, est plus connue sous son nom commercial *WiMax.*

D. Réseaux étendus sans fil (WWAN)

Le réseau étendu sans fil (WWAN pour Wireless Wide Area Network) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil.

Les réseaux à grande étendue se sont principalement développés sous l'égide d'organismes internationaux tels que l'UIT (Union Internationale des Télécommunications). Les principaux standards sont le *GSM* (Global System for Mobile communication), le *GPRS* (General packet Radio Service), Edge, l'*UMTS* (Universal Mobile Telecommunications System) et le cdma2000.

La norme concurrente provenant de l'IEEE est IEEE 802.20, ou *MBWA* (Mobile Broadband Wireless Access), dont l'objectif est de concurrencer les standards des opérateurs de téléphonie mobile par un coût très avantageux. Le nom commercial des produits provenant de cette norme sera *Wi-Mobile*.

I.4.2 Classification suivant l'infrastructure

A. Réseaux sans fil avec infrastructure

Dans ce mode de fonctionnement, le réseau est obligatoirement composé d'un point d'accès appelé station de base (SB), muni d'une interface de communication sans fil pour la communication directe avec les sites ou unités mobiles (UM). Une station de base couvre une zone géographique limitée dite portée ou *cellule* (comme le montre la figure 4). Une unité mobile est rattachée à un moment donné qu'à une station de base lui offrant tous les services tant que l'UM est à l'intérieure de la zone de couverture de la SB. Cette dernière fait office de pont entre réseau filaire et réseau sans fil, permettant de relier une UM à une unité connecté à un site fixe. La SB est aussi le point de passage de la transmission d'une UM à une autre. Si les deux UMs dépendent de la même SB, la trame est simplement relayée par la SB. Si les deux UMs sont à deux SB différentes, une trame échangée entre les deux UMs doit être relayée par le réseau filaire qui relie les deux points d'accès. Les points d'accès peuvent être répartis sur tous le réseau filaire, agrandissant d'autant la couverture du réseau sans fil. Au cours de communication, une UM peut sortir de la zone de couverture de son point d'accès, entrant dans une autre zone (*handover*). Pour assurer la continuité de la communication, l'ancienne SB envoie les informations de l'UM à la nouvelle SB qui va allouer un canal de communication à l'unité mobile.

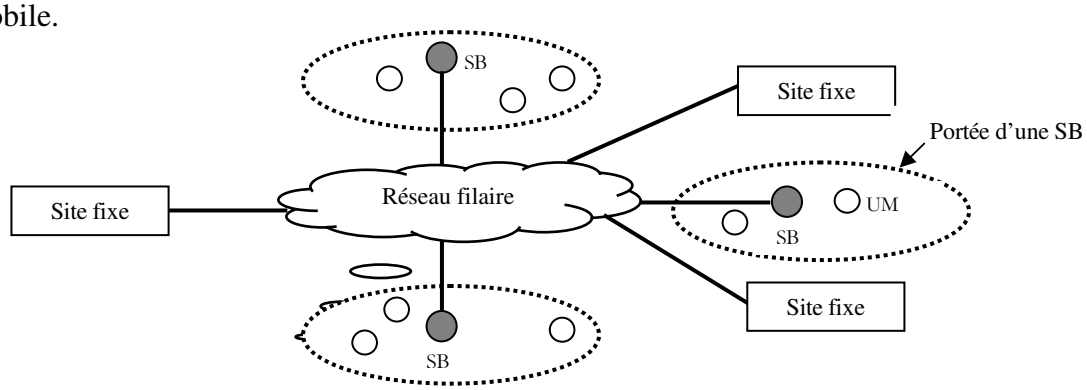

Figure 4 : Le modèle des réseaux mobiles avec infrastructure.

B. Réseaux sans fil sans infrastructure (ad hoc)

Il s'agit d'un mode Point à Point, ne nécessitant pas de points d'accès. Il permet de connecter les stations (dites dans ce cas nœuds), quand aucun point d'accès n'est disponible. L'absence d'infrastructure oblige les nœuds à jouer le rôle de routeurs.

La figure 5 montre l'exemple du nœud A qui peut envoyer au nœud C malgré que ce dernier ne soit pas dans sa portée. Pour ce faire, il envoie les messages au nœud B qui va les envoyer au nœud C.

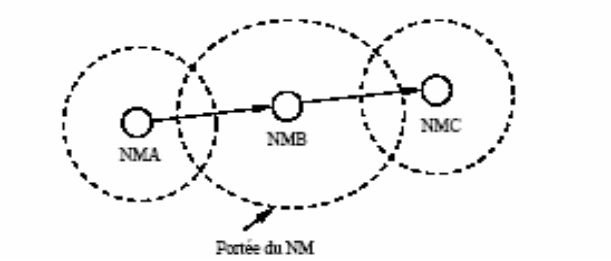

Figure 5 : Exemple de réseaux ad hoc

CHAPITRE II

Les réseaux WiFi

II.1. Introduction

Comme il a été précisé plus haut dans le document, par WiFi, nous désignerons un réseau répondant à la norme 802.11.

II.2. Architecture du réseau 802.11

Du point de vue de l'architecture, 802.11 définit deux modes d'opération : le mode infrastructure BSS (Basic Service Set) et le mode ad-hoc IBSS (Independant Basic Service Set). La topologie du mode ad-hoc est très simple et l'ensemble des stations communique directement par paires, sans aucune fonction de relais de messages. Le mode infrastructure est beaucoup plus répandu que le mode ad-hoc et il définit un élément central, le point d'accès (AP)

Quoiqu'un LAN sans fil puisse être constitué par une seule cellule, avec un seul point d'accès, (et peut également travailler sans point d'accès), la plupart des installations seront constituées par plusieurs cellules, où les points d'accès sont reliés ensemble par un *système de distribution* (DS). Ce DS est dans la majorité des cas un LAN Ethernet. Les communications entre points d'accès peuvent aussi être hertziennes, on parle dans ce cas de WDS (Wireless DS). [2, 19, 20]

Généralement les réseaux sans fil 802.11 sont déployés en regroupant plusieurs points d'accès rapprochés, pour former une zone de couverture étendue composée des cellules de couverture contiguës. Ce réseau étendu est appelé ESS (*Extended Service Set*) et les points d'accès qu'il contient coopèrent entre eux pour acheminer les messages entre les cellules desservies.

La figure suivante montre un réseau 802.11 avec les composants déjà décrits :

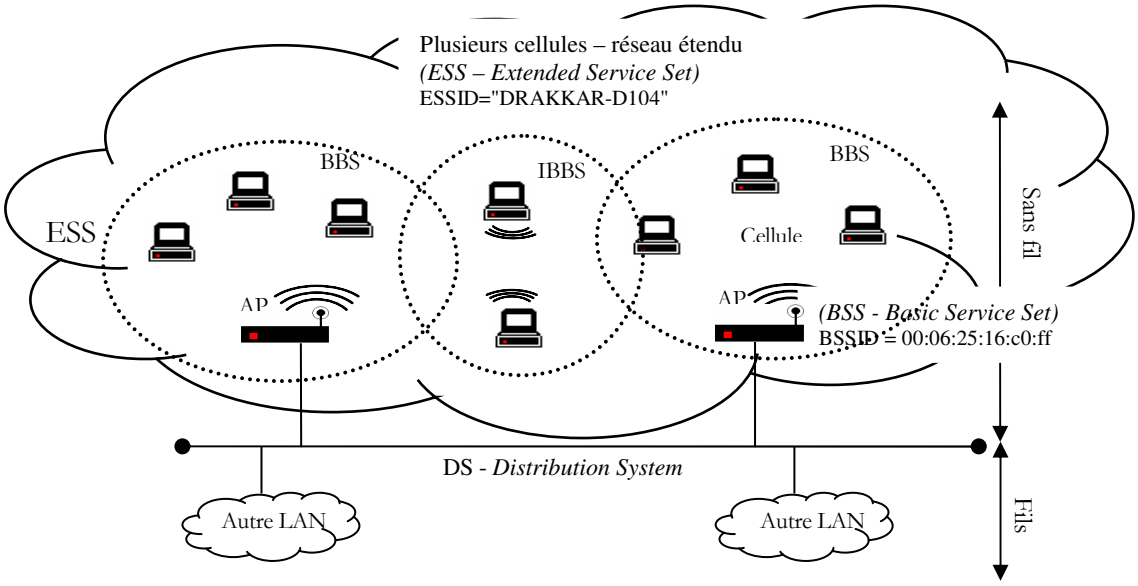

Figure 6 : Architecture type d'un WLAN 802.11

Les noeuds mobiles peuvent errer (roam) entre les APs, il est alors possible d'avoir une couverture sans coupure .Cette mobilité est réalisé par la mise en place d'une technique de *handover (Roaming).*

On va maintenant introduire quelques éléments de terminologie présents dans le standard 802.11. Chaque réseau indépendant (de type BSS ou IBSS) comporte un identificateur appelé *SSID* (Service Set ID), qui est une chaîne de maximum 32 caractères. Dans le cas d'un réseau étendu, cet identificateur est appelé *ESSID* (Extended Service Set ID) ; les cellules qui le forment sont alors identifiées par le BSSID, qui est l'adresse physique du point d'accès de la cellule respective. [19]

II.3. Modèle en couche

La norme 802.11, comme toutes les normes définies par le comité 802, couvre les deux premières couches du modèle OSI [21]: la couche physique (niveau 1) et la couche liaison de données (niveau 2). [1, 15,19, 22].

<table>
<tr><td rowspan="2">Couche 2 OSI
Liaison de données</td><td colspan="6">802.2 Logical Link Control (LLC)</td></tr>
<tr><td colspan="6">802.11 Meduim Access Control (MAC)</td></tr>
<tr><td>Couche1 OSI
Physique (PHY)</td><td>DSSS</td><td>FHSS</td><td>IR</td><td>Wi-Fi
802.11b</td><td>Wi-Fi
802.11g</td><td>Wi-Fi5
802.11a</td></tr>
</table>

Figure 7: modèle en couches de l'IEEE 802.11 [22]

1. La couche physique

Pour la couche physique, le standard initial publié en 1997 [23], proposait trois techniques de transmission : FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum) et IR (InfraRed). Les deux premières fonctionnent dans la bande de fréquences de 2,4 Ghz et peuvent offrir un débit maximal de 1 ou 2 Mbps. La version *802.11b* publié en 1999 [1] a retenu que le deuxième type de transmission physique et y apporte des améliorations dans HR/DSSS (High Rate Direct Sequence Spread Spectrum) pour obtenir des débits pouvant aller jusqu'à 11 Mbps. La version *802.11a* [24] choisit quant à elle d'utiliser une autre technique de transmission appelée OFDM; elle change également la bande de fréquences utilisée à 5 Ghz (Bande U-NII), avec des débits de transmission jusqu'à 54 Mbps. Le même débit maximum caractérise aussi la dernière version du standard, *802.11g* [25], apparue en 2001 et qui utilise la modulation OFDM dans la bande de 2,4 Ghz pour rester compatible avec les équipements 802.11b existants. Une synthèse de ces technologies est présentée dans la table 1. [19]

La bande de fréquences utilisée, que ce soit 2,4 Ghz pour 802.11b et 802.11g (WiFi) ou 5Ghz pour 802.11a (WiFi 5) est repartie sur plusieurs plages de fréquences, appelées *canaux.*
La bande de 2,4 Ghz est divisée en 14 canaux de 22 MHz chacun, la largeur de bande étant de 83,5 MHz, on ne peut placer bout à bout 14 canaux de 22 MHz sans les faire se chevaucher, c'est pour cela qu'on ne peut utiliser que trois canaux distincts donc trois réseaux. Les canaux 1,6 et 11 sont souvent choisis (Voir la figure 8).

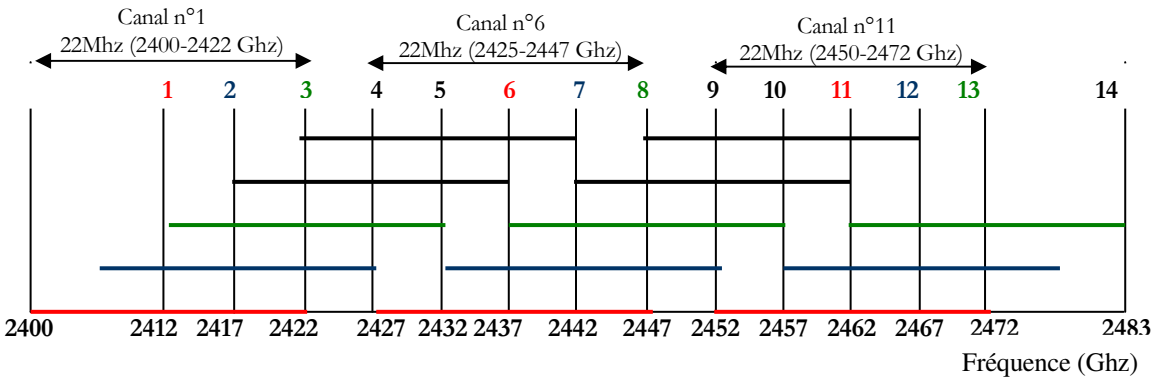

Figure8 : Les canaux de transmission dans 802.11b

Standard	Technologie de la couche physique	Bande de fréquences	Débit maximum
802.11	Modulation FHSS (élément de spectre avec saut de fréquences)	Bande de 2,4 Ghz (2.400 – 2.4835GHz) 75 canaux de 1 Mhz	1 ou 2 Mbps
	Modulation DSSS (élément de spectre à séquence directe)	Bande de 2,4 Ghz (2.400 – 2.4835GHz) 14 canaux de 22 Mhz de recouvrant	
	IR (Infrarouge)		
802.11b	HR/DSSS (High Rate / Haut Débit) basé sur la modulation CCK (complimentary code Keying)	Bande de 2,4 Ghz (2.400 – 2.4835GHz) 14 canaux de 22 Mhz de recouvrant	1, 2, 5.5, 11 Mbps
	DSSS pour la compatibilité avec le 802.11 original		
802.11a	Modulation OFDM (Multiplexage par division en fréquences orthogonales)	Bande de 5 Ghz (5.15 – 5.825GHz) 12 canaux de 20 Mhz indépendantes	6, 9, 12, 18, 24, 36, 48, ou 54 Mbps
8.2.11g	Modulation OFDM	Bande de 2,4 Ghz (2.400 – 2.4835GHz) 14 canaux de 22 Mhz de recouvrant	1, 2, 5.5, 11 Mbps : 6, 9, 12, 18, 24, 36, 48, ou 54 Mbps
	Modulation DSSS avec CCK pour la compatibilité avec le 802.11b		

Tab. 1: Les couches physiques des protocoles 802.11 a, b et g [19].

Couche	Standard	Objet du standard
	802.1	Norme générale. Le fonctionnement inter-réseaux (réseaux pontés). Séparation des deux couches OSI *Physique* et *Liaison* en trois sous couches *LLC, MAC et PLS*
LLC – Link Layer Control	802.2	Définition et spécifications de la couche contrôle de liaison
Contrôle d'accès au medium (*MAC - Media Access Control*) et Couche physique *(PLS - Physical Layer Signaling)*	802.3	Les réseaux locaux en bus logique (Ethernet) avec la méthode d'accès CSMA/CD
	802.4	Les réseaux locaux en bus à jeton (*Token Bus LAN*)
	802.5	Les réseaux locaux en anneau à jeton (*Token Ring LAN*)
	802.6	Les réseaux métropolitains (*MAN*)
	802.11	Les réseaux locaux sans fil (*Wireless LAN*)
	802.12	Les réseaux basés sur la priorité de la demande
	802.15	Réseaux personnels sans fil (*Wireless PAN*)
	802.16	Les réseaux métropolitains sans fil (*Wireless MAN*)
	802.17	Les réseaux *Resilient Packet Ring (Token Ring* amélioré)
	802.22	Les réseaux sans fil régionaux (*Wireless RAN*)

Tab. 2 : Les protocoles 802 [19]

2. La couche liaison de données

2.1. Introduction

La couche liaison de données en 802.11 est composée, à l'instar d'autres normes de la famille 802**,** de deux sous-couches : le contrôle de la liaison logique *LLC* (Logical Link Control) et le contrôle d'accès au medium *MAC* (Medium Access Control).

La couche LLC (Logical Link Control) normalisée 802.2 [26] permet de relier un WLAN 802.11 à tout autre réseau respectant l'une des normes de la famille 802. Un récapitulatif des standards 802 est présenté dans la table 2.

La couche MAC 802.11 est comparable à la couche Ethernet 802.3 [27] **:** elle implante la politique d'accès. Cependant, cette couche MAC est spécifique à l'IEEE 802.11 car elle offre autres les fonctions d'une couche MAC classique (allocation du support, adressage, formatage des trames) des fonctionnalités supplémentaires telles que la sécurité des communications, l'économie d'énergie, la fragmentation, le réassemblage, le contrôle d'erreur ou encore comment assurer une bonne qualité de service, en particulier pour les communication multimédias .La couche MAC est donc en quelque sorte le « cerveau » du 802.11. [2, 19, 14]

2.2. La structure des trames MAC 802.11

La figure 9, présente le format standard d'une trame MAC 802.11. Les données sont placées dans le champ *Données*, d'une longueur variable. Les stations source et destination ainsi que les points d'accès utilisés pour relayer la trame sont identifiées par leurs adresses physiques, sur 6 octets, dans les champs de type @.

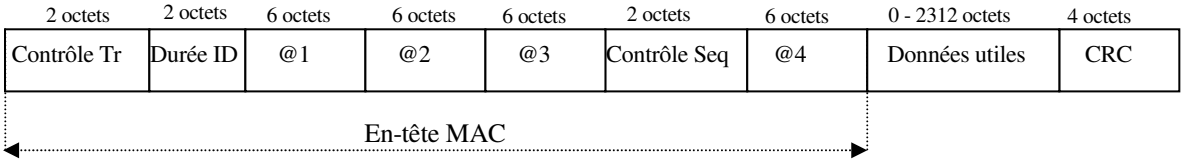

Figure 9 : La structure d'une trame MAC 802.11

Il y a trois types de trames qui sont envoyées parmi les stations d'un réseau sans fil 802.11. Ce type, codé dans le champ *Contrôle Tr*, catégorise les trames en :

- Trames de données ;
- Trames de contrôle, utilisées pour coordonner l'accès au médium. Dans cette catégorie entrent les trames d'acquittement - ACK (*Acknowledgement*) - ou les trames RTS (*Request to Send*) et CTS (*Clear to Send*), dont le rôle est d'éviter les collisions avec des stations plus éloignées. À cause de leur caractère de contrôle, cette catégorie de trames est prioritaire pour l'accès au medium.
- Trames de management. Celles-ci ont la même priorité d'accès au medium que les trames de données. Leur rôle est l'échange des informations relatives strictement au protocole 802.11 (synchronisation, scanning, authentification, association) entre les stations du réseau sans-fil.

2.3. Quelques fonctionnalités de la couche MAC :

2.3.1. Accès au support

Le 802.11 dispose de trois méthodes pour accéder au canal. Ces trois méthodes se nomment CSMA/CA, RTS/CTS et Polling. CSMA/CA et RTS/CTS sont des méthodes dites DCF (Distributed Coordination Function) car la gestion de l'accès au canal est laissée aux stations. A contrario, Polling est une méthode PCF (Point Coordination Function) ou l'accès au canal est géré par un point d'accès. [2, 19, 20]

Description du mode DCF

CSMA

Le protocole CSMA fonctionne ainsi : une station voulant transmettre sonde le support de transmission. S'il est occupé (une autre transmission est en cours), alors la station reporte sa transmission pour plus tard. S'il est libre, alors la station peut émettre. Ce type de protocole est très efficace lorsque le support n'est pas surchargé, dans la mesure où il permet aux stations d'émettre avec un minimum d'attente, mais il existe toujours un risque pour que deux stations émettent en même temps après avoir détecté un support libre et créent ainsi une collision.

Il faut alors détecter ces collisions pour que la couche MAC puisse retransmettre la trame sans avoir à repasser par les couches supérieures, ce qui engendrerait des retards significatifs. L'Ethernet utilise un algorithme appelé CSMA/CD (CSMA *with Collision Detection*) qui permet un une station d'émettre et d'écouter au même temps sur le média de communication afin de s'assurer qu'il n'y a pas de collision avec un paquet émis par une autre station. [2, 20]

Si ces mécanismes de détection de collision sont bons sur un réseau local câblé, ils ne peuvent pas être utilisés dans un environnement sans fil, ceci pour deux raisons principales :

- Implémenter un mécanisme de détection de collision demanderait l'implémentation d'une liaison radio full duplex, capable de transmettre et de recevoir simultanément, ce qui augmenterait le prix.
- Dans un environnement sans fil, on ne peut pas être sûr que toutes les stations ont un lien radio entre elles (ce qui est l'hypothèse de base du principe de détection de collision), car une station peut croire que le canal est libre alors qu'une station "cachée" est en train de transmettre.

Pour pallier ces problèmes, 802.11 utilise un mécanisme d'évitement de collision associé à un système d'accusé de réception : le CSMA/CA. Les autres éléments importants sont les espaces intertrames et le temporisateur d'émission.

Les espace intertrames, ou IFS (Inter Frame Spacing), correspondent à un intervalle de temps entre l'émission de deux trames. Il en existe trois types selon 802.11 [2]:

- SIFS (Short Initial inter-Frame Spacing), représente le plus cours des IFS et permet de séparer deux trames d'un même dialogue (envoie de données, Ack, etc.).

- PIFS (PCF IFS), utilisé par le point d'accès pour bénéficier d'une priorité supérieur, dans le cas de réseaux à accès au support mixte DCF/PCF.
- DIFS (DCF IFS), utilisé en DCF (c'est à dire en CSMA/CA) lorsqu'une station veut initier une communication

SIFS < PIFS < DIFS

La temporisation d'émission, appelé NAV (Network Allocation Vector) permet d'éviter les collisions en retardant les émissions de toutes les stations qui détectent que le support est occupé.

Le protocole CSMA/CA

Le principe général de la méthode CSMA/CA est : chaque station, après que le médium devient libre, attend une durée fixe DIFS suivie de processus de *Backoff* qui permet de gérer les collisions et garantir la même probabilité d'accès pour chaque station au support.

Le processus de Backoff (Backoff process) consiste, dans un premier temps, à calculer un nombre aléatoire (ce qui empêche les stations multiples de saisir le médium en même temps) compris entre zéro et CW (Contention Windows, fenêtre de contention). Ce nombre est ensuite multiplié avec une durée appelée *slot time*. Le résultat de la multiplication permet à la station d'initialiser un *Backoff time* dont la valeur est donnée par la formule :

Backoff time = Random (0, CW) x SlotTime ;

Où Random(0, CW) est une valeur aléatoire entière uniformément distribuée sur [0, CW] avec CW (Contention Window) la fenêtre de contention vérifiant CWmin ≤ CW ≤ Cwmax =1023. Initialement on a : CW= CWmin = 15 dans 802.11. SlotTime est une durée fixe (9µs dans 802.11a).

Les stations par la suite décrémentent leurs b*ackoff time*. Dés que le b*ackoff time* de l'une d'elles atteint zéro (Souce 1 dans notre exemple), elle émet. Les autres stations, dés quelles détectent le regain d'activité sur le canal stoppent la décrémentation de leurs *Backoff time* et entrent en période de *defering*.

Un paquet de donnée est séparé de son acquittement par un SIFS qui est plus court que le DIFS. Les stations en période de *defering* ne pourront reprendre la décrémentation de leurs b*ackoff time* que si le canal est à nouveau libre pendant DIFS. Le fait que SIFS soit plus court empêche que la décrémentation ne reprenne de manière inopportune entre les données et leur acquittement.

Lorsque les données de la Station 1 ont été acquittées et que DIFS s'est écoulé sans activité sur le canal, les autres stations peuvent reprendre la décrémentation de leurs *Backoff time*. [2, 20]

La figure ci-dessous montre le principe de backoff et de defering, l'envoi et l'acquittement d'une trame :

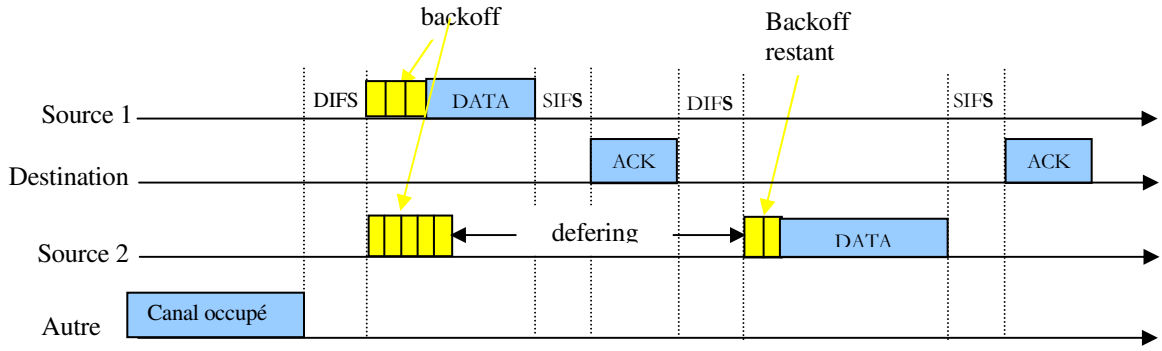

Figure 10 : Le backoff et le defering

Chaque trame doit être acquittée par la station de destination. Lorsqu'une trame n'est pas acquittée, la station retransmet la trame après avoir attendu DIFS et un processus de *Backof.*

La probabilité d'avoir des collisions sur le canal dépend de la dimension de la fenêtre de contention CW. Plus la fenêtre est grande, plus la probabilité que les temps d'attente de deux stations soient identiques est faible. Cependant une fenêtre de contention trop importante nuit aux performances car les temps d'attente sont plus longs. La solution consiste à contrôler dynamiquement la dimension de la fenêtre de contention. CW est donc recalculé en fonction du nombre de collisions détectées sur le canal. A chaque collision détectée, la formule est la suivante :

CW i= 2CWi-1+1 (15, 31, 63, 127, 255, 511, 1023)

Le mécanisme RTS/CTS

Le mécanisme de réservation RTS/CTS permet de résoudre le problème de la station cachée (voir chapitre I Figure 1).

Lorsqu'une station désire transmettre une trame, elle commence par envoyer une trame RTS (Request To Send) après avoir attendu un temps DIFS et un temps aléatoire.

La trame RTS contient la durée de la transmission (champ Duration). Chaque station, hormis la station destinatrice, sait alors que le canal est réservé et pour combien de temps. Afin de savoir quand elles pourront recommencer à émettre, les stations utilisent un NAV (Network Allocation Vector). Le NAV est initialisé à partir de la durée transmise par la trame RTS. Lorsqu'une station reçoit un RTS qui lui est destiné, elle attend SIFS et envoie une trame CTS. Une station n'ayant pas reçu de RTS, car trop éloignée de la station émettrice, peut recevoir le CTS et configurer son NAV.

Le mécanisme utilisé par RTS/CTS peut laisser penser qu'il est moins performant que CSMA/CA car il nécessite l'envoi de deux trames avant de pouvoir émettre de l'information. Cela est vrai mais seulement dans le cas où la longueur des données est petite. Le fait qu'avec RTS/CTS les collisions ne peuvent survenir que pendant l'envoi de la trame RTS garantit que de longues trames ne seront pas à répéter suite à une collision. Pour optimiser les transmissions un *RTS*

threshold (seuil) a été introduit : Lorsque les trames à envoyer sont petites c'est CSMA/CA qui est utilisé. Dans le cas où les trames sont plus grandes qu'un certain seuil (RTS Threshold), c'est alors RTS/CTS qui est utilisé.

La figure 11 illustre le processus d'émission d'une trame lorsque la station destination est cachée.

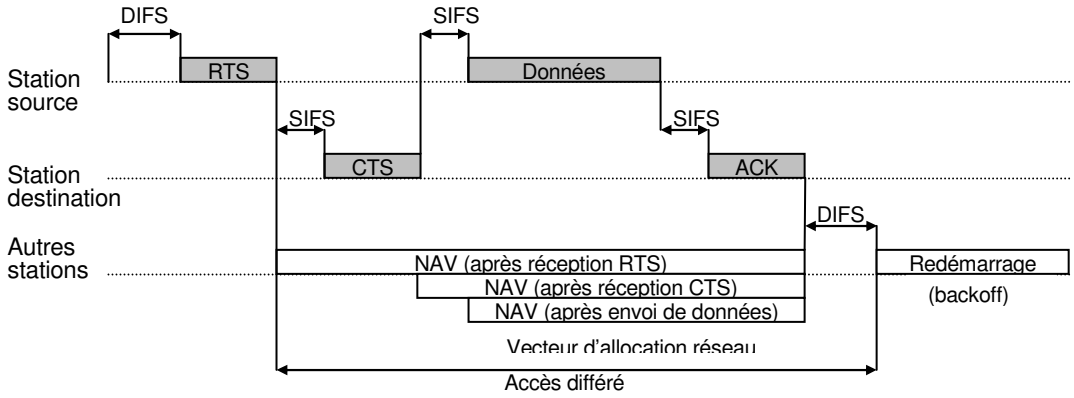

Figure 11 : Transmission en utilisant les trames *RTS/CTS* [2]

Polling

La méthode du Polling est une méthode PCF (Point Coordination Function), elle nécessite un point de coordination (PC, Point Coordination). Le point de coordination est un point d'accès, le Polling ne fonctionne donc pas dans un réseau ad hoc.

Le principe de base de la PCF est de centraliser la gestion de l'accès au médium d'une cellule. C'est le point d'accès qui indiquera à chacun des stations qui lui sont rattachées quant elles doivent émettre leurs paquets. Le backoff aléatoire devient ainsi en partie inutile. Durant toute la phase ou le point d'accès impose l'ordre des transmissions, il n'y a pas de contention pour l'accès au canal ; on parle de Contention-Free Period (CFP)

Dans chaque cycle de la PCF, une période de DCF est conservée et permet aux stations n'implémentant la PCF de continuer à accéder au canal. C'est la C*ontention Period* (CP). La cohabitation entre les stations implémentant la PCF et celle ne l'implémentant pas est assurée grâce au temporisateur PIFS; Lorsque le point d'accès désire commencer une CFP, il attend PIFS avant de transmettre le beacon. Comme les stations en mode DCF ne peuvent émettre qu'après un temps DIFS, le point d'accès est certain de prendre le contrôle car DIFS est plus grand que PIFS. [28]

Le Polling, contrairement à CSMA/CA et RTS/CTS, permet de garantir *la qualité de Service*, de ce fait il est utilisée pour la transmission des donnés temps réel, telles que la voix ou la vidéo.

2.3.2. Mobilité

Le fait qu'un terminal doit pouvoir se déplacer et donc passer d'une cellule à une autre a conduit à la mise en place d'une technique de handover (roaming).

Le roaming est le processus de mouvement d'une cellule vers une autre sans perdre la connexion au réseau. Cette fonction est similaire au "handover" des téléphones portables, mais avec deux différences majeures [20]:

- Sur un WLAN, qui est basé sur une transmission par paquets, la transition d'une cellule à une autre doit être faite entre deux transmissions de paquets, contrairement à la téléphonie où la transition peut subvenir au cours d'une conversation. Ceci rend le roaming plus facile dans les LANs sans fil.
- Dans un système vocal, une déconnexion temporaire peut ne pas affecter la conversation, alors que dans un environnement de paquets, les performances seront considérablement réduites à cause de la retransmission qui sera exécutée par les protocoles des couches supérieures.

Analyse du processus d'association et de handoff dans le protocole 802.11 :

A. L'association au réseau

Une station doit s'associer auprès d'un point d'accès pour pouvoir envoyer et recevoir des trames. Cette procédure d'association a lieu au moment de la première connexion de la station au point d'accès et se répète quasiment à l'identique chaque fois que la station se reconnecte au même réseau sans-fil. La connexion à un réseau sans-fil comporte deux phases :

- Découverte des points d'accès présents dans le voisinage et choix de l'AP cible ;
- Authentification et association auprès du point d'accès choisi.

Le scan

Premièrement, la station doit trouver les points d'accès potentiels auxquels elle peut se connecter. Ceci se réalise par une phase de découverte qui s'appelle *scan*. Le standard spécifie deux types de scan : *actif* et *passif*.

Dans le scan actif, la station diffuse des trames *Probe Request* et attend des trames de réponse *Probe Response*. Dans le mode passif, la station n'envoie aucune trame et écoute uniquement le médium pour intercepter des trames *Beacon* qui sont envoyées périodiquement par les points d'accès.

Une fois que le scan est fait, la station possède la liste des points d'accès qui lui sont accessibles. Les informations contenues dans les trames *Probe Response* ou *Beacon* envoyées par les points d'accès sont utilisées par la station pour choisir celui auquel elle va essayer de s'associer. En général, la station va choisir le point d'accès qui a le meilleur indicateur SNR (*Signal to Noise Ratio*)[1]. [19, 20].

[1] Ce paramètre indique la puissance du signal reçu à la réception d'une trame, rapporté au bruit présent sur le canal de communication.

L'authentification et l'association

Après que la station a choisi un point d'accès candidate pour s'associer avec, elle va initier la procédure d'authentification. Les méthodes et mécanismes d'authentification seront détaillés dans le prochain chapitre.

Après que la station est authentifiée auprès du point d'accès, elle initie le dernier échange de trames de cette phase d'initialisation. La station envoie une trame *Association Request* et le point d'accès répond avec une trame *Association Response*. Si la réponse est positive, la station et le point d'accès peuvent commencer à s'échanger entre eux des trames de données.

B. Le transfert d'association

Un handoff a lieu quand une station s'éloigne de son point d'accès courant et entre dans la couverture d'un autre AP dont la qualité du signal est meilleure. On peut identifier trois phases différentes dans le déroulement d'un handoff (voir la figure12) ; la première est celle où la station s'aperçoit que le signal de l'AP courant est en baisse ; la deuxième et la troisième sont en grandes lignes les mêmes que la connexion initiale au réseau : la découverte des points d'accès et la réassociation. [19,20].

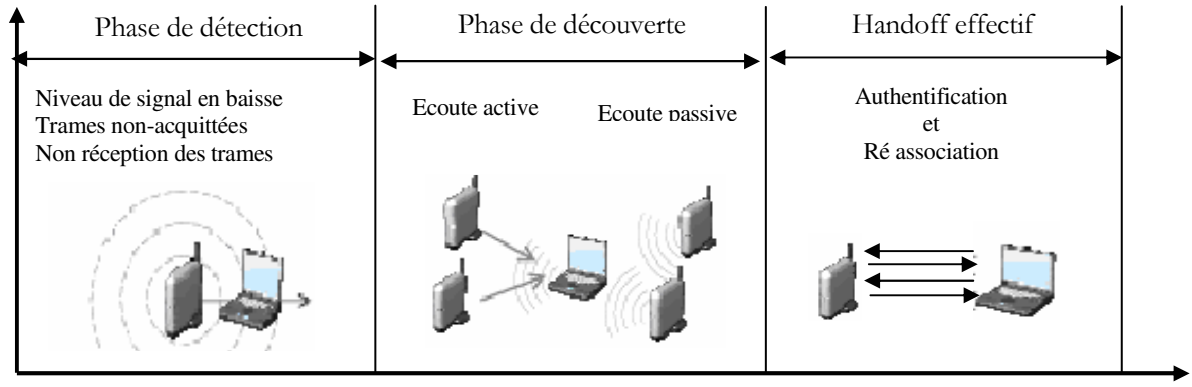

Figure 12 : Les phases du handoff dans 802.11 [19]

Le standard ne spécifie pas le moment où le client détecte la nécessité d'initier un scan, mais la plupart des implémentations présentes dans les équipements 802.11 le font au moment ou la qualité du lien descend en dessous d'une certaine valeur. En initiant le scan, la station essaie de découvrir d'autres AP qui appartiennent au même réseau (c'est-à-dire qui ont le même ESSID) et dont la puissance du signal reçu est meilleure. [19]

Le processus de ré association est similaire au celui de l'association initiale. L'élément nouveau para rapport à l'association initiale est la spécification de l'ancien point d'accès de la station dans la trame *Reassociation Request*.

Cet élément nouveau peut être utilisé pour un échange supplémentaire de messages entre les deux points d'accès (l'ancien et le nouveau), conformément aux spécifications d'un document récent de

l'IETF - la recommandation 802.11f[2] [29]. Ainsi, le nouveau AP envoie à l'ancien un message *IAPP MOVE Notify* et la réponse consiste dans un message *IAPP MOVE Response*. Le but de ce message est l'échange des informations regardant la station mobile, comme par exemple des informations de sécurité permettant une authentification plus rapide au nouveau point d'accès. [19]

Le même document recommande au nouveau point d'accès point d'accès d'envoyer une trame de mise à jour au niveau 2. Cette trame contient comme adresse source dans son en-tête LLC l'adresse MAC de la station mobile. Son rôle est la mise à jour des tables des équipements actifs de niveau 2, comme les ponts et commutateurs, pour que les trames destinées à la station soient acheminées vers sa nouvelle localisation. [19,20]

2.3.3. Le contrôle d'erreur

Contrairement à l'Ethernet qui ne s'occupe pas du contrôle d'erreur et laisse les couches supérieures s'en occuper, la couche Mac du 802.11 calcule, pour chaque paquet envoyé, un code de Contrôle de redondance Cyclique (CRC) de 32 bits. Ce code est calculé à partir de l'ensemble des bits du paquet à envoyé et il est rajouté à celui-ci. Ainsi en recevant un paquet, il suffit d'effectuer le même calcul que l'émetteur pour obtenir le CRC du paquet, puis de comparer ce résultat au CRC envoyé par l'émetteur.

2.3.4. L'économie d'énergie

Les réseaux sans fil sont généralement en relation avec des applications mobiles, et dans ce genre d'application, l'énergie de la batterie est une ressource importante. C'est pour cette raison que le standard 802.11 donne lui-même des directives pour l'économie d'énergie et définit tout un mécanisme pour permettre aux stations de se mettre en veille pendant de longues périodes sans perdre d'information.

L'idée générale, derrière le mécanisme d'économie d'énergie, est que le point d'accès maintient un enregistrement à jour des stations travaillant en mode d'économie d'énergie, et garde les paquets adressés à ces stations jusqu'à ce que les stations les demandent, ou jusqu'à ce qu'elles changent de mode de fonctionnement. Les points d'accès transmettent aussi périodiquement (dans les trames "balise") des informations spécifiant quelles stations ont des trames stockées par eux. Ces stations peuvent ainsi se réveiller pour récupérer ces trames balise, et si elles contiennent une indication sur une trame stockée en attente, la station peut rester éveillée pour demander à récupérer ces trames.

Les trames de multicast et de broadcast (trames destinées à toutes les stations du réseau) sont stockées par le point d'accès et transmises à certains moments (à chaque DTIM) où toutes les stations en mode d'économie d'énergie qui veulent recevoir ce genre de trames devraient rester éveillées. [20]

[2] 802.11f consiste principalement dans la spécification du protocole de communication inter-points d'accès - IAPP (*Inter Access Point Protocol*).

2.4. Les évolutions de la couche MAC

La première version du standard 802.11 publiée en 1997, a définit la couche MAC en y intégrant un certain nombre de fonctionnalités. Toutefois de nombreuses améliorations ont été apportées à cette couche, au fil du temps [14, 15, 30] :

- 802.11c : Traite du fonctionnement de pont, équipement reliant deux LAN. Elle analyse les procédures de connexion entre les points d'accès.
- 802.11d : établit la liste des règles à suivre selon les pays pour pouvoir émettre sur telle ou telle fréquence : éviter tel ou tel canal, limiter la puissance, etc. Le 802.11d permet aussi aux constructeurs de savoir facilement comment configurer leurs produits en fonction des pays auxquels ils sont destinés.
- 802.11e : Ratifié fin 2005, Apporte des modifications à la couche MAC afin d'améliorer la Qualité de Service (QoS). Elle prévoit des communications planifiées, dans des intervalles de temps ou aucun trafic n'est transmis. Ces optimisations visent à utiliser des services de téléphonie sur IP (ToIP) et de diffusion de vidéo en continu.
- 802.11f : La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole Inter-Access point roaming protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée itinérance (ou roaming en anglais)
- 802.11h : validé en septembre 2003, traite de la gestion du spectre et de la puissance afin de les rendre conformes aux normes européennes.
- 802.11i : Gère le mécanisme d'authentification et de sécurité au niveau de la couche MAC. Elle résout notamment les faiblesses du protocole WEP (Wired Equivalent Privacy) qui est la solution de sécurité offerte par la première version de la couche MAC. Le 802.11i a été ratifié le 24 juin 2004.
- 802.11k : Apporte des améliorations dans le domaine de la mesure des ressources radio, dans le but d'arriver à une meilleure gestion du réseau. Elle définit quelles sont les informations qu'il faut rendre disponibles pour la gestion et la maintenance des WLAN.
- 802.11s : Groupe de travail pour les réseaux maillés.
- Etc.

II.4 . Les équipements WIFI :

Il existe différents types d'équipement pour la mise en place d'un réseau sans fil WiFi [15] :

Les adaptateurs ou cartes d'accès sont des cartes réseaux permettant de se connecter à un réseau WiFi. Ces adaptateurs sont disponibles dans de nombreux formats : carte PCMCIA, carte PCI, adaptateur USB, carte Compact Flash ou SD, ...). On appelle station tout équipement possédant une telle carte.

Les bornes d'accès encore appelées AP (Access Point) font office de station de base. Elles se comportent comme des routeurs et peuvent être relie au réseau filaire ou à une connexion ADSL.

Les ponts (bridge) permettent de relier deux réseaux entre eux (deux immeubles par exemple).

Les antennes servent à amplifier le signal. Elles se connectent aux points d'accès.

- **Antenne Omni :** le signal est émis de façon égale dans toutes les directions.
- **Antenne Patch :** Emission dans un rayon de 180°
- **Antenne Yagi :** Emission de 15 à 60 degrés.
- **Antenne Parabole :** Focalisée sur un point précis

Les connecteurs d'antennes relient les antennes au point d'accès. L'objectif est de réduire au maximum les pertes de signal.

II.5. Conclusion

Dans ce chapitre, on a présenté la norme 802.11 sur laquelle repose un réseau WiFi. Cette norme couvre les deux premières couches du modèle OSI: la couche physique et la couche liaison de données (MAC) qui a un rôle crucial en définissant des fonctionnalités avancées telles que la sécurité des communications, l'économie d'énergie, le contrôle d'erreur ou encore comment assurer une bonne qualité de service. Le WiFi, qui utilise les ondes radio comme support de transmission, présente plusieurs avantages par rapport aux réseaux locaux filaires notamment la simplicité d'installation et la mobilité. Cependant, il est confronté à plusieurs problèmes de sécurité. Le chapitre suivant dresse un état de l'art de la sécurité d'un réseau WiFi dans son mode infrastructure.

CHAPITRE III

La sécurité dans les réseaux WiFi

III.1. Introduction :

Les réseaux 802.11ont introduit de nouveaux besoins de sécurité en comparaison aux réseaux fixes. En effet, le manque de protection physique des points d'accès au réseau et la transmission sur des liens radios sont les causes principales de la vulnérabilité des réseaux sans fil**.**

Pour permettre aux réseaux sans fil d'avoir un trafic aussi sécurisé que dans les réseaux fixes, le groupe de travail 802.11 a mis au point le protocole WEP (Wired Equivalent Privacy), dont les mécanismes s'appuient sur le chiffrage des données et l'authentification des stations.

D'après le standard, WEP est optionnel, et les terminaux ainsi que les points d'accès ne sont pas obligés de l'implémenter. Comme nous allons le voir, la sécurité n'est pas garantie avec le WEP, et un attaquant peut casser les clés de chiffrement sans trop de difficulté. La Wi-Fi Alliance, une association promouvant et certifiant les équipements Wi-Fi, a développé un deuxième mode de protection, le WPA (Wi-Fi Protected Access) [31], qui résout ces problèmes, au moins pour quelques années. Enfin, le groupe de travail 802.11 a créé un groupe spécifique, IEEE 802.11i, qui propose une solution pérenne, normalisée en juin 2004.

Avant de présenter ces trois protocoles de sécurité, Nous allons tout d'abord voir les différentes attaques susceptibles d'atteindre un réseau WiFi dans son mode infrastructure, puis les principaux services de la sécurité informatique ainsi que les techniques utilisées pour les assurer.

III.2. Les attaques d'un réseau WiFi :

2.1. Le War Driving:

Le War Driving (la guerre en voiture) est une forme de piratage consiste, comme son nom l'indique à se promener en voiture avec une antenne WiFi et à noter la position et les caractéristiques de tous les points d'accès que l'on puisse trouver. Des logiciels tel que *NetStumbler* permettent d'automatiser la tâche, et peuvent être relies à un module GPS[3] pour que la position exacte soit enregistrée.

Cette pratique permet aux initiés de repérer les différents endroits où se trouvent les réseaux, et de les exploiter afin de réaliser toute les catégories d'attaques contre le WiFi : l'espionnage, l'intrusion, la modification de messages, le déni de service et la relecture. [14]

2.2. L'espionnage:

La première attaque qui vient à l'esprit qu'on on parle des technologies sans fil est l'écoute : un pirate se poste à proximité et surveille les échanges. On dit qu'il *"sniffe"* le réseau sans fil. Dans les réseaux filaires, ceci est rendu difficile par le fait qu'il faut d'abord se brancher physiquement au réseau. Avec le WiFi, chacun peut écouter ce qui est transmis par les autres. Il suffit de disposer d'un adaptateur gérant le mode *promescuous*, c'est-à-dire capable de lire tous les messages et pas

[3] Global positioning System : système de localisation par satellite.

uniquement ceux qui lui sont adressés. Puis utiliser un logiciel d'analyse de réseau, du type Ethereal par exemple pour « sniffer » tout ce qui se passe sur le réseau. [14]

2.3. L'intrusion

L'intrusion consiste à s'introduire au sein du réseau WiFi pour consulter voire modifier les données du système informatique (bases de données, fichier, e-mails…) ou encore pour profiter de la connexion à Internet.

Si aucune sécurité n'est mise en œuvre l'intrusion est trivial il suffit de s'associer à l'un des points d'accès du réseau. En revanche, si l'association impose un mécanisme d'identification avant d'autoriser l'ouverture d'une session sur le réseau, le pirate aura essentiellement deux options [14] :

- Ouvrir une nouvelle session en se faisant passer pour un utilisateur légitime ;
- Détourner une session existante (hijaking).

2.3.1. Attaque de dictionnaire

Pour la première option, le pirate doit parvenir a tromper le mécanisme d'identification ; par exemple si les utilisateurs sont identifier avec un mot de passe il suffit de trouver le mot de passe valable, pour cela le pirate a plusieurs possibilités : si les mots de passe sont échangés en claire, il suffit d'attendre qu'un utilisateur légitime se connecte et d'espionner l'envoi de son mot de passe. S'ils sont cryptés, il peut essayer de s'attaque a l'algorithme de cryptage.

Une autre technique, consiste à essayer des millions de mots de passe jusqu'à trouver le bon. Certain logiciels permettent d'essayer les mots de passe les plus probables on utilisant les mots du dictionnaire, et en les modifiant légèrement, on parle d'attaque de « dictionnaire ».

Il existe deux variantes de l'attaque de dictionnaire :

L'attaque en ligne : L'utilisateur cherche à se connecter au système en essayant successivement chaque mot de passe jusqu'à trouver le bon.

L'attaque hors ligne : De nombreux protocoles d'authentification fonctionnent de la façon suivante : le serveur envoie un « défi » (texte aléatoire) à l'utilisateur qui utilise ce « défi » ainsi que son mot de passe pour générer la réponse, selon un algorithme précis. Le serveur utilise le même algorithme pour vérifier la validité de la réponse. L'attaque de dictionnaire hors ligne fonctionne ainsi : Le pirate enregistre le dialogue d'une authentification réussie. Il possède alors le défi et la réponse, correcte, de l'utilisateur. Hors connexion, il essaye des millions de mots de passe avec le même défi et le même algorithme jusqu'à ce qu'il trouve la même réponse que celle donnée par l'utilisateur.

L'attaque *par dictionnaire* est souvent une méthode utilisée en complément de ***l'attaque par force brute*** qui consiste à tester de manière exhaustive les différentes possibilités de mots de passe. Cette dernière est particulièrement efficace pour des mots de passe n'excédant pas 5 ou 6 caractères.

Idéalement, les mots de passe doivent être assez longs et complexes pour qu'il soit impossible de les deviner en quelques tentatives, le système doit détecter et bloquer les attaques de dictionnaire en ligne, et il doit également utiliser un protocole d'authentification invulnérable aux attaques de dictionnaire hors ligne.

2.3.2. Attaque de relecture

Une autre façon d'ouvrir une nouvelle session consiste à enregistrer les paquets émis par une station légitime ou moment ou elle se connecte, puis de les émettre à l'identique un peu plus tard.

Une façon d'éviter les risques de relectures consiste à imposer qu'un compteur soit incrémenté à chaque paquet échangé.

2.3.3. Détourner une session existante :

Il existe des adaptateurs WiFi dont on peut changer l'adresse MAC, ce qui permet à un pirate de facilement détourner des sessions : il lui suffit d'espionner le réseau en attendant l'arriver d'un utilisateur légitime .Une fois que celui-ci s'est identifie, le pirate regarde son adresse MAC et configure son propre adaptateur WiFi pour imiter cette adresse on parle de *spoofing* de l'adresse MAC.

2.4. Le déni de service (DoS)

Le déni de service a pour but d'empêcher le réseau de fonctionner normalement pour ce faire :

Le pirate peut attaquer le réseau en émettant des ondes radio pour brouiller les Communication Ou inonder le réseau de fausses requête d'association, dé-association ou dé-authentification (*Airjack*) pour le saturer ou forcer les utilisateurs à se reconnecter pour faire une attaque d'intrusion. Le pirate peut aussi mettre les utilisateurs en attente en envoyant des paquets CTS. [14]

2.5. La modification de messages

Les attaques MIM (Man-In-The-Middle)

Ce type d'attaque consiste à dévier toutes communications entre deux ordinateurs, pour les faire transiter par la machine attaquante. Les attaques MIM peuvent aussi servir de base pour toutes les attaques décrites précédemment : espionner le trafic réseau, démarrer une nouvelle session, prendre le contrôle d'une session existante ou encore empêcher le réseau de fonctionner (DoS). [14]

III.3. Cryptographie et services de sécurité

Dans ce qui suit nous présentant les mécanismes cryptographiques les plus utilisées pour assurer : la confidentialité, l'intégrité, l'authentification et la non répudiation.

Introduction

La cryptographie est une science qui se base sur les mathématiques pour *crypter* et *décrypter* des informations considérées comme confidentielles. Elle permet de stocker et de transmettre ces informations d'une manière sécurisée [32].

Le *Cryptage* appelé aussi *chiffrement* est la fonction qui permet de transformer un texte en clair et lisible en un texte incompréhensible dit texte crypté ou chiffré en utilisant une clé. La fonction inverse, appelée *Décryptage*, n'est possible que par le destinataire possédant la clé adéquate. [33] Ces mécanismes se basent sur des fonctions mathématiques qui associent une clé (nombre, mot, …) au passage du texte en clair au texte chiffré et vis versa.

Les protocoles cryptographiques ont pour objectif de sécuriser un échange en respectant les propriétés fondamentales suivantes :

- Confidentialité : seul le destinataire d'un message peut en prendre connaissance.
- Intégrité : un message ne peut être modifié à l'insu du destinataire.
- Authentification : l'identité de l'expéditeur est vérifiée.
- Non-répudiation : lier une personne à un document i.e. l'expéditeur ne peut pas nier avoir émis un message une fois celui-ci reçu par son destinataire.

1. Confidentialité :

Elle a pour rôle d'assurer le secret du message afin que seul son destinataire légitime puisse en prendre connaissance [33, 34].

Elle s'appuie sur différents types d'algorithmes :

- symétriques ou à clé secrète,
- asymétriques ou à clé publique,
- et hybrides.

Chiffrement à clé secrète

Le chiffrement à clé secrète appelé aussi chiffrement symétrique, repose sur le partage entre deux interlocuteurs en communication d'une même clé secrète qui sert à paramétrer l'algorithme à la fois pour le chiffrement et le déchiffrement (Figure13). Deux interlocuteurs désirant communiquer des données confidentielles doivent partager une clé secrète K, l'émetteur envoie par exemple un message M chiffré avec la clé K ($\{M\}_K$), à la réception, le récepteur récupère le message M en déchiffrant le message reçu avec la clé K.

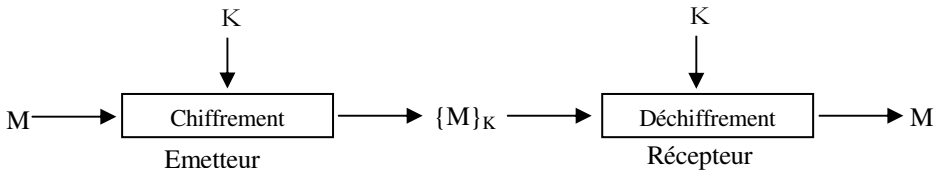

Figure 13 : Le chiffrement symétrique

Le chiffrement symétrique a l'avantage d'être rapide. Cependant, il peut être assez onéreux en raison de la difficulté de la distribution sécurisée de la clé. Comme exemples d'algorithmes de chiffrement symétrique, on trouve DES, IDEA, AES et RC4. [33, 34]

Chiffrement à clé publique

Le but de ce genre de cryptographie est de résoudre le problème de la distribution des clés secrètes employée dans la cryptographie symétrique. Introduite par Diffie et Hellman en 1975 avec l'algorithme connu sous le nom de Diffie-Hellman, ce procédé utilise deux clés : une publique à partager pour le cryptage et l'autre privée à garder secrète pour le décryptage.

Les deux clés sont établies soit par leur propriétaire, soit par une autorité à laquelle il est rattaché. Elles sont, généralement, liées par des relations mathématiques, mais il reste difficile de deviner la clé privée à partir de la clé publique. Cela est dû au choix de clés de grande taille. [33]

Un émetteur voulant envoyer une donnée confidentielle, chiffre le message à envoyer en utilisant la clé publique de récepteur ($\{M\}_{pk}$), puis ce dernier est le seul à pouvoir récupérer le message en le déchiffrant avec sa clé privée (sk) (voir Figure ci-dessous).

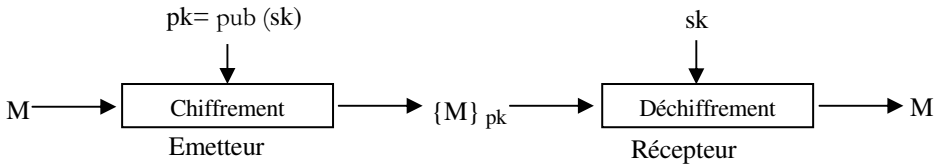

Figure 14 : Le chiffrement asymétrique

L'intérêt du chiffrement asymétrique réside dans la possibilité de diffuser la clé de cryptage sans renoncer à la confidentialité des messages. Parmi les algorithmes utilisant la cryptographie asymétrique, notons : RSA (Rivest Shamir Adelman), Elgamel, Diffie-Hellman, DSA (Digital Signature Algorithm). [33, 34]

Cryptographie hybride

C'est une combinaison des meilleures fonctionnalités des deux types de cryptographie précités. La cryptographie hybride consiste à créer d'abord une clé de session qui est une clé secrète à usage unique. Pour le cryptage et le décryptage c'est la clé de session qui est employée par un algorithme symétrique, donnant ainsi une rapidité aux deux processus. [33]

Comme nous l'avons déjà vu précédemment, la clé secrète doit être transmise. Pour garantir la confidentialité de la clé, la cryptographie hybride utilise un algorithme asymétrique à clé publique pour crypter la clé de session.

Les deux clés associées à l'algorithme à clé publique (la clé publique et la clé privée) sont créées par le propriétaire ou par une autorité à laquelle ce dernier se rattache (entreprise, …). Par contre la clé de session associée à l'algorithme à clé secrète est soit crée par l'expéditeur aléatoirement, soit par les deux parties en même temps. [33]

Parmi les algorithmes utilisant la cryptographie hybride, il y a PGP (Pretty Good Privacy), GnuPG (GNU Privacy Guard) et SSL (Secure Socket Layer) qui est un protocole plus qu'un algorithme. [33, 34]

2. Intégrité du message :

Une des conditions les plus élémentaires pour une communication sécurisée est que les messages échangés ne doivent, en aucun cas, faire l'objet de modification ou d'altération durant la communication.

Le rôle de cette fonctionnalité (*intégrité du message*) est de détecter toute modification apportée au message. A cette fin, l'utilisation des fonctions de hachage est nécessaire. [33, 34]

Fonction de hachage

Une fonction de hachage appelée aussi fonction de hachage à sens unique est une fonction mathématique qui permet de transformer une chaîne de longueur variable en une chaîne de taille inférieure et fixe appelée empreinte, condensé ou haché. Elle offre les propriétés suivantes :

Soit h une fonction de hachage à sens unique, M le message à hacher tel que h (M) = H (H : le condensé) Alors :

- Etant donnée M, il est facile de calculer H
- Etant donné h, il est difficile de trouver M (h a sens unique)
- Etant donné M, il est difficile de trouver un autre message M' tel que :
  h (M) = h (M') (Résistance en collision).

La fonction de hachage assure que, si l'information était échangée en qui que ce soit, même d'un seul bit, une sortie totalement différente serait produite.

Il existe deux types de fonction de hachages à sens unique : les fonctions de hachage avec clé et celle sans clé. Les fonctions de hachage sans clé peuvent être calculées par n'importe quel entité. La valeur calculée dans ce cas ne dépend que du message initial, alors que les fonctions de hachage avec clé sont en fonction de message initial et d'une clé de hachage : seuls ceux qui possèdent la clé peuvent calculer la valeur de hachage correspondante au message initial (voir la section 3.3).

Parmi les fonctions de hachage les plus utilisées, notons : MD5 (Message Degest 5), SHA-1 (Standard Hash Algorithm - 1) …. [8, 33]

3. Authentification:

L'authentification nous permet de s'assurer de l'identité des parties concernées [33, 34]. Il existe plusieurs techniques :

3.1. Avec un algorithme à clé publique

Chaque partie possède une paire de clés publique/privée (pkA/skA, pkB/skB). Le fait que l'expéditeur crypte le message *M* avec sa clé secrète *skA*, est un moyen d'affirmer qu'il est le propriétaire de la clé publique *pkA*. [33]

3.2. Avec un algorithme à clés symétriques

Idem que le précédent sauf que c'est la même clé.

3.3. Avec un MAC (Message Authentication Code)

C'est un code qui peut être généré de deux manières différentes, avec :

a) Une clé symétrique :

Le code de hachage signé avec la clé secrète est une manière de s'assurer de l'identité de l'expéditeur, car il détient la bonne clé secrète. L'expéditeur A crypte un message ***M*** avec sa clé secrète générant le message *C*. On constitue alors un code *MAC* qui peut être tout simplement le dernier octet du message C. Et il ne reste au destinataire B que de faire le même enchaînement et de comparer le *MAC* trouvé et celui reçu. [33]

b) Une fonction de hachage

C'est le même principe, sauf que dans ce cas on ne crypte pas avec la clé *K*, mais elle entre avec un message *M* dans la composition du code de hachage *MAC*. L'émetteur calcul le condensé du message M: H = MAC (K, M) (Figure 15, étape 1), ensuite il envoie le message M avec le condensé H calculé (Figure 15**,** étape 2). A l'arrivée, le récepteur vérifie l'origine du message reçu comme suit : Il calcul le condensé du message reçu en utilisant la même clé K (Figure 15, étape3) et il le compare avec le condensé reçu (Figure 15**,** étape4). Si les deux condensés sont égaux, le message est dit authentique sinon le message recu a été changé ou a été fabriqué par un autre expéditeur.

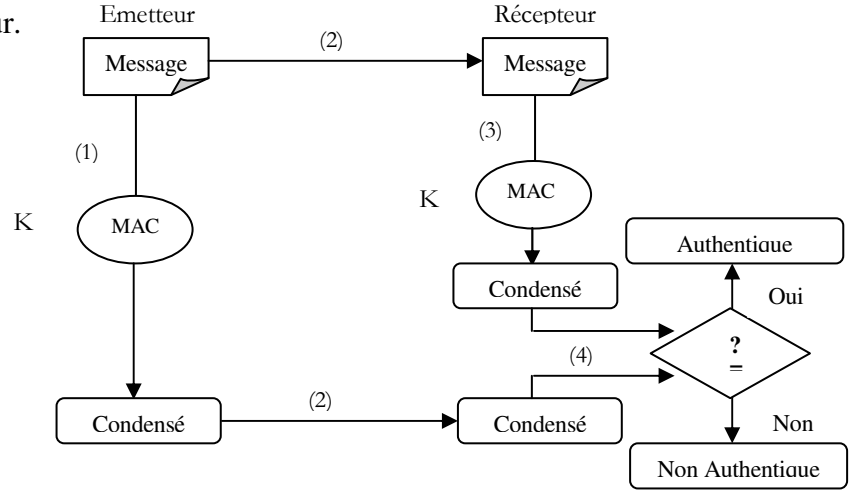

Figure 15 : Authentification avec le MAC (*avec fonction de hachage*)

3.4. Avec une signature digitale :

L'une des utilisations de la cryptographie à clé publique est qu'elle permet l'établissement des signatures numériques. Ces dernières offrent au destinataire la possibilité de vérifier l'authenticité de l'expéditeur (origine exacte).

Ces signatures sont liées aux informations qu'elles attestent, donc, difficiles à falsifier. Elles apportent aussi l'authentification et l'identification des parties concernées et la non répudiation en cas de désaveu de la part de l'expéditeur.

Le principe de la signature numérique est qu'elle est le résultat du cryptage du document et d'autres informations concernant l'expéditeur avec sa clé privée, affirmant ainsi son authenticité. [33]

Pour signer un message M, l'émetteur calcule le condensé H de M en utilisant une de fonction de hachage h tel que H = h (M) (Figure16, étape1) puis le chiffre avec sa clé privée (Figure16, étape 2). Le résultat de cette transformation est appelé *signature numérique* du message M. Lors de la réception du message et la signature, le récepteur vérifie la signature comme suit : Tout d'abord, il calcule le condensé de message reçu en utilisant la même fonction de hachage h (Figure16, étape 4) puis déchiffre la signature en utilisant la clé publique de l'émetteur (Figure16, étape 5). Les deux condensés obtenus sont comparés (Figure16, étape 6). S'ils concordent, alors on peut s'assurer que le message et son origine sont authentiques et on garantit la non répudiation.

Une signature numérique fournit les services suivants : l'authentification, l'intégrité des données et la non répudiation.

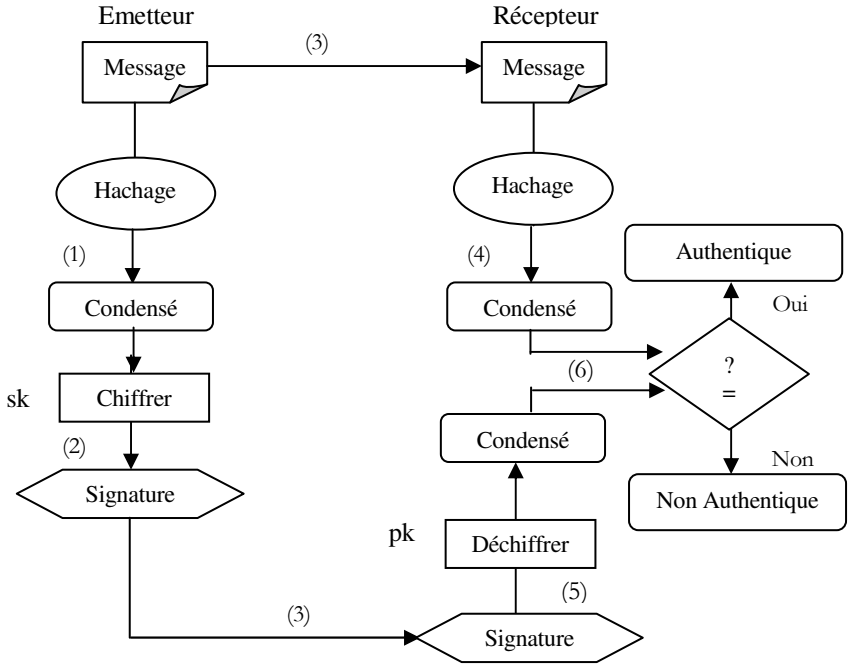

Figure 16 : La signature numérique

Comme toutes les clés publiques sont distribuées dans l'annuaire, elles risquent d'être interceptées et remplacées par d'autres clés. Il est donc possible de fabriquer de fausses signatures. Alors il faut lier la clé publique avec son propriétaire. Ce qui a donné naissance aux *certificats a clés publiques*.

Certificat à clé publique

Un certificat, validé par une autorité de certification (AC), est l'équivalent d'une carte d'identité. Il repose sur les mêmes principes. Il permet de justifier de l'identité d'un individu (ou d'une entité) sur présentation du certificat. Quand deux entités veulent établir une connexion sécurisée entre elle, elles échangent juste leurs certificats. Le certificat contient l'identité et la clé publique de cette entité. De ce fait, les interlocuteurs auront une information qui prouve l'appartenance réelle d'une clé publique à son propriétaire supposé.

En outre, les certificats peuvent également contenir d'autre information comme la durée pour laquelle le certificat est valide qui est fixé par l'autorité de certification. Les interlocuteurs doivent renouveler leurs certificats quand la durée de vie expire.

Les certificats numériques permettent aux individus et aux organisations de sécuriser les transactions, professionnelles et personnelles, effectuées sur les réseaux de communication. Ils peuvent être utilisés pour signer des documents, chiffrer des informations et contrôler l'accès à des applications. [8, 34]

III. 4. Les Protocoles de sécurité 802.11

4.1. Le protocole WEP

4.1.1. Fonctionnement

Le WEP, première solution de sécurité à avoir été intégrée dans le standard 802.11 est un protocole élaborée en 1999 dans le but d'offrir aux réseaux sans fil un moyen d'authentification, de confidentialité et de contrôle d'intégrité. Ces principes se basent sur un système à clé symétrique, la même clé étant utilisée pour chiffrer et déchiffrer les données. Cette clé de 40 ou 104 bits est partagée par tous les clients du réseau et par le point d'accès.

Le mécanisme de chiffrement et de contrôle d'intégrité du WEP se base sur l'algorithme RC4 conçu en 1987 par Ronald Rivest. L'algorithme RC4 (Ron's Code 4) réalise le chiffrement des données en mode flux (stream cipher). [2, 14, 35]

Le chiffrement et le contrôle d'intégrité comme l'illustre la figure 17 se déroulent comme suit :

1. La clé partagée K de 40 ou 104 bits est concaténée avec un vecteur d'initialisation (IV) de 24 bits (IV : Initialisation Vector qui change à chaque trame envoyée), formant ainsi une clé de 64 ou 128 bits appelée *Key Scheduling Algorithme*(KSA) :
KSA = [IV‖ K]. Où ‖ est l'opération concaténation.

En parallèle on effectue, avec un CRC 32, un calcul d'intégrité ou ICV (Integrity Check Value) sur les données qui sont, ensuite, concaténées avec cet ICV ; [M ‖ CV (M)].

2. L'algorithme RC4 est appliqué sur la clé KSA pour produire une série pseudo aléatoire de bits d'une longueur égale à la longueur de la trame, nommée KeyStream (KS) :
KS = RC4 [IV‖K].

3. Un XOR (opération logique de OU exclusif) est appliqué bit à bit entre la KeyStream et les données concaténées avec l'ICV, formant les données cryptées :
C = [M ‖ ICV (M)] + RC4 [IV ‖ K]. Où + est l'opération XOR.

4. Les données chiffrées sont transmises et l'IV est rajouté à la trame.

Le chiffrement n'est appliqué que sur les données de la trame MAC, l'en-tête, l'IV et le CRC sont transmis en clair.

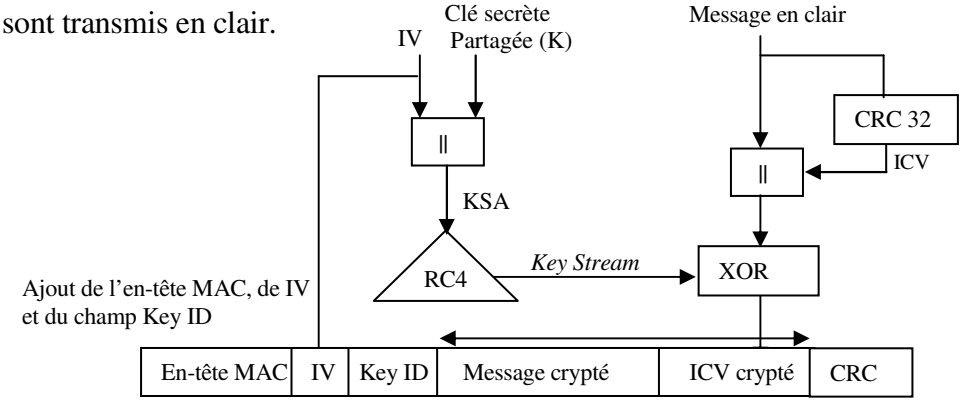

Figure 17: Le cryptage et le contrôle d'intégrité WEP

Le déchiffrement et le contrôle d'intégrité se déroulent en plusieurs étapes comme précédemment, mais en sens inverse :

1. La clé partagée est concaténée avec l'IV de la trame reçue, puis l'ensemble est soumit à l'algorithme RC4 pour donner la bonne séquence pseudo aléatoire qui a été utilisé pour le chiffrement.
2. On effectue un XOR entre cette séquence aléatoire et les données chiffrées reçues. On obtient les données et l'ICV en clair de la façon suivante :

$$C + RC4[IV \| K] = [M \| ICV(M)] + RC4[IV \| K] + RC4[IV \| K]$$
$$= [M \| ICV(M)] + (RC4[IV \| K] + RC4[IV \| K])$$
$$= [M \| ICV(M)]$$

3. On effectue un contrôle d'intégrité (ICV') sur ces données en clair que l'on compare avec l'ICV reçu. Si ICV'=ICV on peut être sûr des données.

Deux techniques d'authentification sont associées au WEP [2, 14]:

Authentification par système ouvert

Le système ouvert est essentiellement une authentification « nulle ». Tout client qui demande une authentification avec cet algorithme sera authentifié si le point d'accès destinataire utilise l'authentification par système ouvert. Ce mode d'authentification est mis en place là où la facilité d'utilisation est prioritaire, ou encore là où la sécurité n'est pas cruciale pour un administrateur de réseau. On peut quand même utiliser le mécanisme WEP pour chiffrer les données, quand on utilise l'authentification par système ouvert. L'authentification par système ouvert est la configuration par défaut.

Authentification par clé partagée

Cette technique, basée sur un secret partagé, se déroule en quatre étapes :

1. La station envoie une requête d'authentification au point d'accès.

2. Lorsque le point d'accès reçoit cette trame, il envoie un texte en clair 128 bits (défi) généré par l'algorithme WEP.

3. La station chiffre cette valeur avec la clé partagée.

4. Le point d'accès déchiffre le texte reçu avec le même secret et confirme l'authentification de la station si la vérification est correcte et la station peut alors s'associer, sinon il répond par un message négatif.

4.1.2. Mécanisme de gestion des clés WEP :

Le standard IEEE 802.11 fournit 2 mécanismes qui permettent de sélectionner une clef lorsque l'on crypte ou décrypte les données [14] :

a. La rotation de clé :

La norme 802.11 autorise que jusqu'à quatre clés WEP soit définie. Une seule est utilisée pour le cryptage (la clé « active ») mais toutes peuvent être utilisées pour le décryptage. Pour changer de clé WEP, il suffit donc de rajouter une nouvelle clé WEP dans tous les points d'accès, sans

l'activer, puis d'installer progressivement la nouvelle clé WEP dans toutes les stations, en l'activant et enfin l'activer dans les points d'accès.

b. Les clés individuelles

Une clé WEP « individuelle » est configure sur chaque poste, puis les configurer dans chacun des AP, en les associant aux adresses MAC des postes en question. Ceci permet d'améliorer la sécurité en évitant qu'une même clé soit utilisée par tout le monde pour leurs communications. Cependant une clé partagée doit être installé pour le trafic broadcast et multicast.

4.1.3. Quelques vulnérabilités du WEP

Le WEP présente de nombreuses failles de sécurité ; notamment sur la gestion de clés (tous les utilisateurs ont la même clé). En effet, le WEP ne définit aucun moyen pour gérer les clés de chiffrement. C'est à l'administrateur de WLAN de créer les clés, de les distribuer, de les archiver/stocker d'une manière protégée, de clarifier qui a telles ou telles clés cryptographiques et de révoquer les clés compromises. Les spécifications de WEP n'ont pas pris en charge ces problématiques.

Plusieurs problèmes résident dans le protocole WEP lui-même [14, 36, 37]:

- Comme les clés WEP sont partagées, la confidentialité de la communication n'est pas assurée.
- En raison de l'utilisation d'un vecteur d'initialisation relativement court (24 bits), il est fort probable que, après une courte période de temps sur un réseau sans fil actif, le vecteur IV sera réutilisé (pas de protection contre le rejeu des messages). Cela pourrait faciliter une attaque contre le système visant à récupérer du texte en clair.
- Avec WEP, la station mobile n'authentifie pas le point d'accès. Elle ne peut donc pas vérifier si elle s'accorde avec le vrai point d'accès dans le réseau WLAN.
- *Spoofing* de l'authentification : le principe de l'authentification avec WEP est que le point d'accès envoie un challenge de 128 octets en clair et que l'utilisateur doit lui renvoyer chiffré. Si la réponse de l'utilisateur est correcte, alors le point d'accès considère que la station possède la clé du WEP. L'attaque peut être réalisée en interceptant le message en clair et la réponse cryptée. Ensuite, l'attaque déduit RC4 (IV, K) et il demande à s'authentifier.
- Le contrôle d'intégrité souffre aussi de sérieuses failles dues à l'utilisation de l'algorithme CRC32 choisi pour cette tâche. Cet algorithme est fréquemment utilisé pour la détection d'erreurs mais n'a jamais été considéré cryptographiquement sûr pour du contrôle d'intégrité à cause de sa linéarité. [35]

Soit C le paquet crypté et C' le paquet obtenu après modification de C de la manière suivante :

$C' = C + [E \| CRC(E)]$ /E est une séquence aléatoire de même longueur que M/
$= [M \| CRC(M)] + R(IV, K)] + [E \| CRC(E)]$
$= [M + E + CRC(M) + CRC(E)] + R(IV,K)$

OR l'algorithme CRC est linéaire ie $CRC(A + B) = CRC(A) + CRC(B)$ alors :

C' = [M + E + CRC(M+E)] + R(IV,K)
C' = [M' + CRC (M')] + R (IV, K) / on pose M' =M + E

- Faiblesse de l'algorithme RC4 au sein du protocole WEP due à la construction de la clé. En 2001, Scott Fluhrer, Itsik Mantin et Adi Shamir publièrent leur fameux article sur la sécurité WEP : *Weaknesse in the Key Scheduling Algorithme of RC4* [38]; dans lequel ils détaillaient une attaque reposent sur le fait que pour certaines valeurs de la clé, il est possible pour les 1er bits de la suite chiffrante de dépendre uniquement de quelques bits de la clé.

Ces vulnérabilités furent exploitées par des outils de sécurité telle : Airsnort, WEPCrack, Air crack, permettant de retrouver la clé WEP en analysant une importante quantité de trafic chiffré. [39]

4.2. 802.11i:

4.2.1. Introduction:

Le WEP souffre en effet de nombreuses failles qui le rendent peu recommandable comme la sécurité est importante, par conséquence le groupe de travail 802.11i à été mis en place pour développer une solution de sécurité nettement plus sur.

Malheureusement entre la découverte des failles du WEP et la finalisation de la norme 802.11i, il s'est écoulé plusieurs années. En 2002 la WiFi Alliance a donc publié une solution de sécurité appelée Wireless Protected Access (WPA), qui est un sous ensemble du 802.11i. Cette version de WPA peut être considérée comme une norme de deuxième génération.

En Juin 2004, la version finale de la norme 802.11i fut adoptée et le nom commercial WPA2 [40] fut choisi par la Wi-Fi Alliance. Cette norme de troisième génération, introduit des changements fondamentaux comme la séparation de l'authentification utilisateur et le chiffrement/contrôle d'intégrité des messages, cela permettant une architecture de sécurité robuste passant à l'échelle et convenant parfaitement tant aux entreprises qu'aux particuliers. La nouvelle architecture pour les réseaux sans fil est appelée RSN (Robust Security Network).

Dans RSN l'association entre toute station est construite sur une association/authentification solides appelle RSNA. RSNA utilise 802.1X pour l'authentification et le calcul d'une clé maître, nommée PMK (Pairwise Master Key), le 4-way handshake pour une meilleure gestion des clés de session et deux types de protocoles pour assurer la confidentialité des données : TKIP (Temporal Key Integrity Protocol) et CCMP (Counter-mode/CBC-MAC Protocol). [8, 39, 41]

L'IEEE 802.11i a aussi défini une architecture temporaire TSN (Transitional Security Network) dans laquelle les équipements RSN et les systèmes WEP peuvent coexister permettant ainsi aux utilisateurs de mettre à jour leurs équipements.
Un TSN supporte les architectures antérieures, c'est à dire pré-RSN, en particulier les mécanismes suivants, importés de la norme IEEE 802.11 [8, 14,39, 41] :

- Open Authentification;
- Shared Key Authentification;
- WEP (Wired Equivalent Privacy).

4.2.2. Déférence entre WPA ET WPA2:

Le protocole WPA 2 inclut quelques différences très significatives avec WPA :

Le WPA et le WPA2 sont identique de point de vue de leur architecture globale et donc de leur mis en œuvre. Le WPA repose sur un algorithme de cryptage défini par le protocole TKIP (Temporal Key Integrity Protocole) alors que WPA2 repose, au choix, sur TKIP ou sur un autre algorithme de cryptage appelé Advanced Encryption Standard (AES).

Une autre différence importante est que le WPA n'est pas compatible qu'avec les réseaux de type infrastructure et non les réseaux Ad Hoc, quand au WPA2, il peut sécuriser les deux types de réseau. [14]

Une autre innovation du WPA2 est la *Pre-authentification* et le *Key caching* ; introduites comme solution d'authentification pour le roaming. Ces deux notions sont détaillées en chapitre IV.

4.2.3. Architectures WPA

La norme IEEE 802.11i définit deux modes de fonctionnement [14] :

WPA Personal :

Le mode « WPA personnel » permet de mettre en oeuvre une infrastructure sécurisée basée sur le WPA sans mettre en oeuvre de serveur d'authentification. Le WPA personnel repose sur l'utilisation d'une clé partagée, appelées *PSK* pour *Pre-shared Key*, renseignée dans le point d'accès ainsi que dans les postes clients. Contrairement au WEP, il n'est pas nécessaire de saisir une clé de longueur prédéfinie. En effet, le WPA permet de saisir une « *passphrase* » (*phrase secrète*), traduite en *PSK* par un algorithme de hachage.

Inconvénient :

- Si le mot de passe qui est choisi est trop court, un pirate peut lancer une attaque hors ligne pour le retrouver ;
- La clé est partagée, tous les utilisateurs peuvent espionner le trafic des autres utilisateurs ;
- Contrairement au WEP, aucun mécanisme de rotation de clé n'est prévu, ce qui la rend trop lourde à gère pour les grand réseaux.

WPA Enterprise :

Le mode entreprise impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification, généralement un serveur RADIUS (Remote Authentication Dial-in User Service), et d'un contrôleur réseau (le point d'accès). Cette solution est actuellement ce qu'il y a de plus sûr en terme de sécurité d'authentification forte.

4.2.4. Une connexion complète :

Un contexte de communication sécurisé s'effectue en quatre phases (voir la Figure 18) :

- La mise en accord sur la politique de sécurité ;
- L'authentification 802.1X ;
- La dérivation et la distribution des clés ;
- Le chiffrement et l'intégrité au sein d'une RSN.

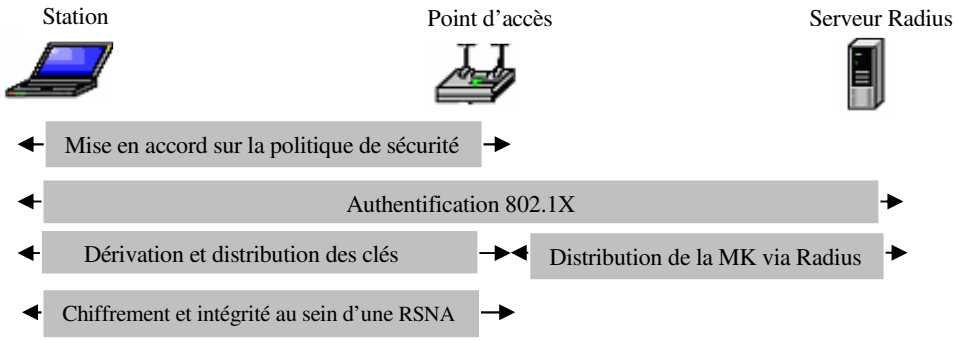

Figure 18 : Les phases opérationnelles du 802.11i [39]

Phase 1 : Mise en accord sur la politique de sécurité

La première phase perrmet aux deux parties communicantes de s'accorder sur la politique de sécurité à utiliser. Un point d'accès diffuse dans ses trames *beacon* ou *Probe Response* (suivant un message Probe Request du client) des éléments d'information, ou IE (Information Element), afin de notifier au client 802.1x les indications suivantes [39, 41]:

- Les méthodes d'authentification supportées (802.1X, clé pré-partagée (PSK)),
- Le protocole de sécurité pour le chiffrement du trafic vers une seule destination (unicast) (CCMP, TKIP, etc.)
- Le protocole de sécurité pour le chiffrement du trafic en diffusion (multicast) (CCMP, TKIP, etc.)
- Le support de la pré-authentification permettant aux utilisateurs de se pré-authentifier avant de basculer sur un nouveau point d'accès pour un handover en douceur.

La figure 19 illustre cette première phase :

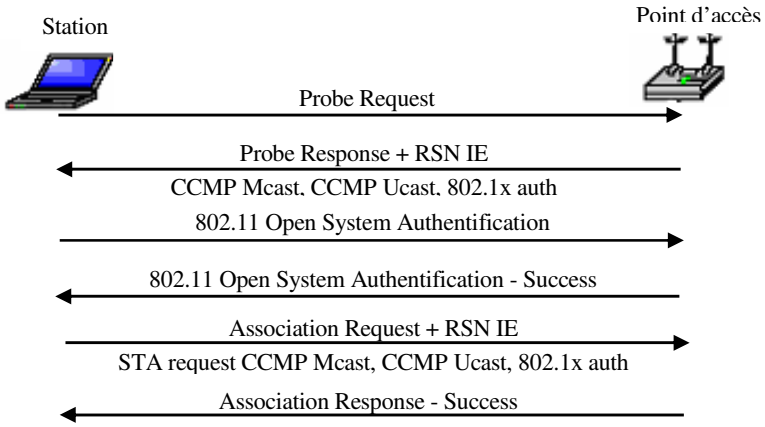

Figure 19 : La mise en accord sur la politique de sécurité [39]

Après avoir détecté l'AP le plus proche, le client envoie une requête d'authentification. Puisque, avec le WPA et le WPA2, l'AP devraient toujours être en mode « ouvert », cette authentification est toujours positive (au sens WiFi, pas au sens 802.1x). La réponse du client aux politiques de sécurité supportées est incluse dans le message *Association Request* validé par le message *Association Response* du point d'accès.

Phase 2 : Authentification 802.1X

A. Le protocole IEEE 802.1X

Introduit en 2001, le standard 802.1x fournit un contrôle d'accès réseau basé sur port, il fournit l'authentification des stations attachées au LAN. Un port désigne une entité supervisant le trafic échangé entre un visiteur (le client) et le réseau de communication auquel il désire accéder. Un port non authentifié bloque tous les paquets qui ne transportent pas le protocole d'authentification EAP. [39, 42, 43]

La structure d'IEEE 802.1X :

Le 802.1x utilise un modèle qui s'appuie sur trois entités fonctionnelles :

Le client (suplicant) : c'est un poste de travail (terminal informatique) demandant un accès au réseau.

L'authentificateur (authentificator) : c'est l'unité qui contrôle et fournit la connexion au réseau, dans les réseaux sans fil, le point d'accès joue le rôle d'authentificateur.

Le serveur d'authentification (AS) : il réalise la procédure d'authentification avec l'authentificateur et valide la demande d'accès. Le serveur d'authentification peut être soit un serveur Radius dédier ou – par exemple pour les particulier – un simple processus fonctionnant sur le point d'accès).

Comme l'illustre la figure 20, la station et l'authentificateur ont un PAE (Port accès entity) qui traite les protocoles et algorithmes d'authentifications. Le PAE authentificateur contrôle le statut autorisé/non-autorisé de son *Port Contrôlé* dépendamment des résultats de processus d'authentification. Avant que le client soit authentifié, l'authentificateur utilise le port non contrôlé

pour communiquer avec le PAE client et bloquer tous le trafic à l'exception des messages IEEE 802.1X. [39, 42, 43]

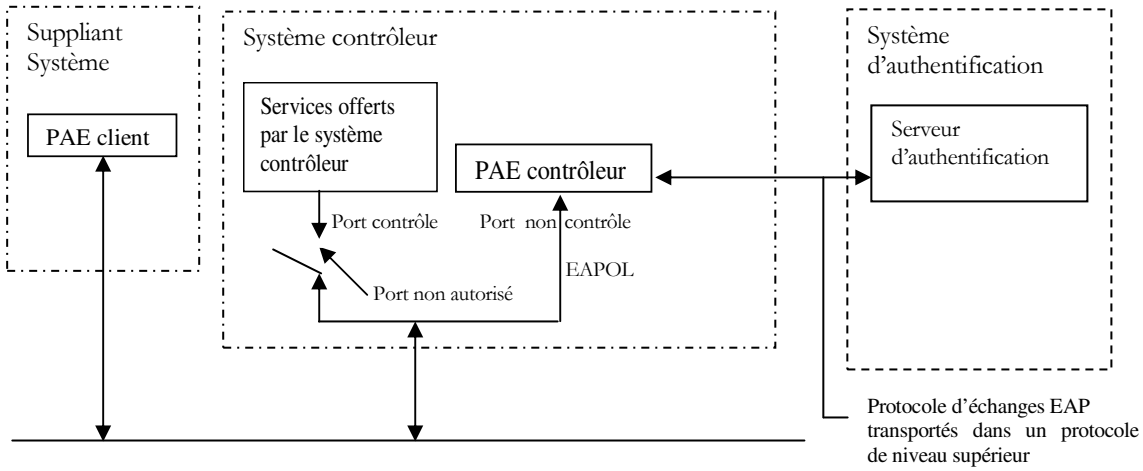

Figure 20 : Architecture d'authentification 802.1X [43]

Le standard IEEE 802.1X emploie le protocole EAP qui réalise une enveloppe générique pour de multiples méthodes d'authentification,

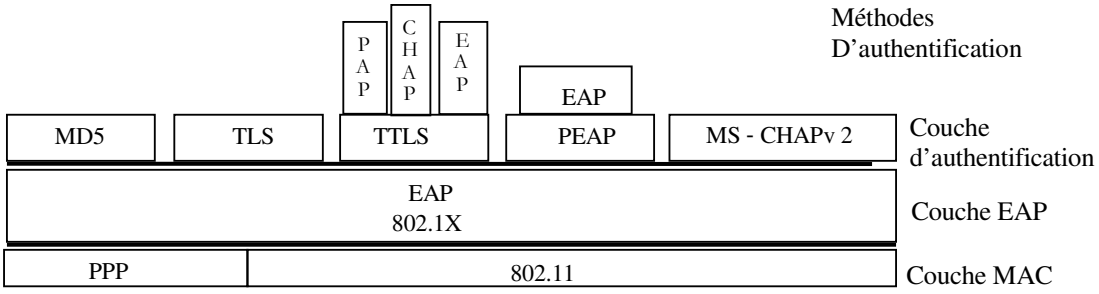

Figure 21 : la pile EAP

B. EAP

EAP est un protocole originalement développé pour PPP comme alternative aux méthodes d'authentification basées sur mot de passe. Contrairement à ces prédécesseurs, EAP ne définit pas de méthode d'authentification particulière mais il définit un moyen de transport général pour les échanges d'authentification. Il repose sur le paradigme de communication challenge-response. [42]

La figure suivante illustre le format du paquet EAP :

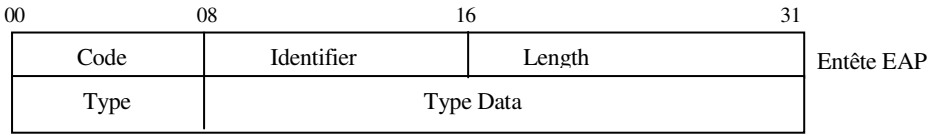

Figure 22 : Le format du message EAP [42]

Le champ « Code » indique s'il s'agit d'une requête, d'une réponse, d'un succès ou d'un échec. La requête et la réponse sont étiquetées par le même « Identifier » compris entre 0 et 255 et elles

ont une longueur totale codée sur deux octets. Le champ « Length » représente la longueur du paquet EAP. Le champ « Type », dans des paquets de requêtes ou de réponses, désigne le protocole d'authentification transporté d'où le nom extensible

Les messages EAP sont eux même encapsulé, le protocole EAP Over LAN (EAPOL) transporte les paquets EAP entre la station et le point d'accès en faisant appelle au message suivant [8, 41,42] :

- EAPoL-Start : permet au client de prévenir l'authentificateur qu'il souhaite se connecter ;
- EAPoL-Packet : ce sont ces paquets qui encapsulent les paquets EAP.
- EAPoL-Key : permet l'échange de clé de cryptage.
- EAPoL-Logoff : permet au client de demander la fermeture de sa session.

Le serveur l'authentification et le point d'accès communiquent en utilisant le protocole RADUIS ; les messages EAP sont transportés comme des attribut par le protocole RADUIS qui contient un mécanisme pour vérifier l'authenticité et l'intégrité des paquet échangés de fait que chaque point d'accès 802.11i, jouant le rôle d'authenticateur, partage un secret avec le serveur RADIUS avec lequel il communique. [8, 41,42]

Le format d'un paquet RADUIS est illustré par la figure23 ci-dessus ; le champ Authentificator contient un résumé HMAC-MD5 du paquet, calculé avec le secret partagé.

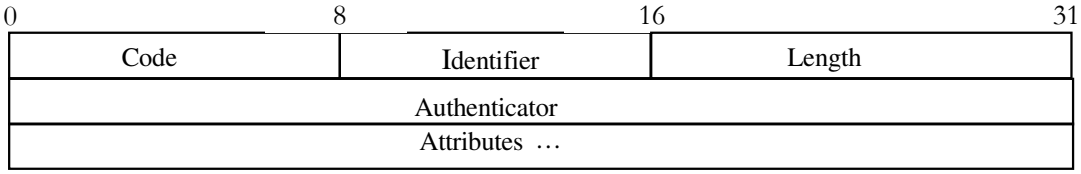

Figure 23 : Format d'un paquet RADUIS

Comme le montre la figure 24, l'insertion d'une station mobile dans un environnement 802.1X se déroule de la manière suivante [39, 8, 42] :

Après la phase d'association avec le point d'accès, le client envoie le message EAPOL –Start au point d'accès pour initialiser le processus d'authentification. Le point d'accès, envoie au terminal une requête d'identité EAP-Request/Identity. La station mobile produit en retour une réponse EAP-Response/Identity. Cette réponse comporte l'identité du client et les méthodes d'authentification supportées.

A ce moment, le point d'accès transmet au serveur d'authentification le message EAP Response/Identity encapsulé dans une requête RADIUS. À partir de ce moment, les échanges dépendent de la méthode d'authentification choisie afin de générer une clé maîtresse (Pairwise Master Key – PMK) si elle est génératrice de clés.

Durant l'échange des messages EAP (requêtes et réponses) entre le serveur d'authentification et la station mobile, le point d'accès agit comme un simple relais passif.

Le serveur d'authentification prend la décision d'accepter ou de refuser l'accès au réseau, comme, on aura 3 cas a cité :

Si l'authentification est réussie, RADUIS envoie le message EAP-Success à la station mobile pour indiquer le succès de la procédure d'authentification. Le *port contrôlé* passe alors à l'état autorisé.

Si l'authentification a échoué le message EAP-Failure sera envoyé, dans ce cas le port reste dans l'état non autorisé.

Si l'authentification est réussie et la station mobile veut se déconnecter de point d'accès courant, elle lui envoie un paquet EAPOL-Logoff, le port contrôlé transite alors à l'état non autorisé.

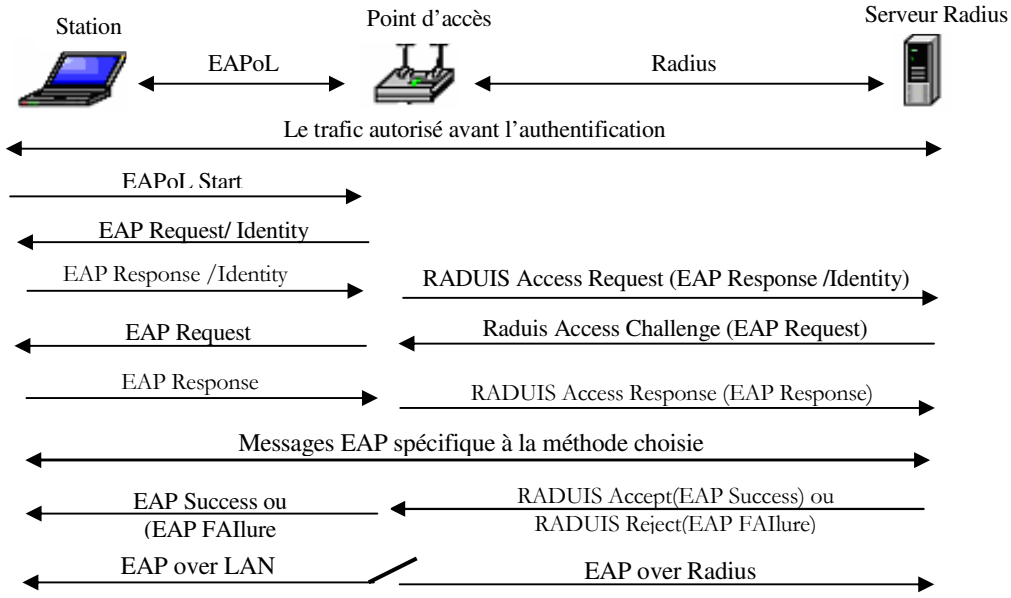

Figure 24 : Echange de messages 803.1x et EAP [8]

Si l'authentification de client se termine avec succès le *port contrôlé* de l'authentificateur est commuté dans l'état autorisé et le client est autorisé à avoir un accès complet au service réseau.

Phase 3 : Hiérarchie et distribution des clés

La sécurité des transmissions repose essentiellement sur des clés secrètes. Dans RSN, chaque clé à une durée de vie limitée et de nombreuses clés sont utilisées, organisées dans une hiérarchie. Quand un contexte de sécurité est établi après une authentification réussie, des clés temporaires (de sessions) sont créées et régulièrement mises à jour jusqu'à la fermeture du contexte. [39]

La génération et l'échange des clés est le but de cette troisième phase. Deux poignées de main (Handshake) ont lieu pour dériver les différentes clés (Figures 26 et 28) :

- Le 4-Way Handshake pour la dérivation de la PTK (Pairwise Transient Key) et de la GTK (Group Transient Key),
- Le Group Key Handshake pour le renouvellement de la GTK.

La dérivation de la PMK (Pairwise Master Key) dépend de la méthode d'authentification choisie :

Si la PSK (Pre-Shared Key) est utilisée, PMK = PSK. La PSK est générée à partir de la phrase secrète (composée de 8 à 63 caractères) ou directement à partir d'une chaîne de 256 bits, cette méthode est adaptée pour les particuliers n'ayant pas de serveur d'authentification,

Si un serveur d'authentification est utilisé, la PMK est dérivée de la MK issue de l'authentification 802.1X. [39]

Comme l'illustre la Figure 25 la PMK en elle même n'est jamais utilisée pour le chiffrement ou le contrôle d'intégrité. Néanmoins, elle est utilisée pour la génération de clés de chiffrement temporaires, pour le trafic à destination d'une machine il s'agit de la PTK (Pairwise Transient Key). La taille de la PTK dépend du protocole de chiffrement choisi : 512 bits pour TKIP et 384 bits pour CCMP.

La PTK, comme le montre la figure 25 consiste en plusieurs clés temporelles dédiées [39,41]:

- KCK (Key Confirmation Key – 128 bits) : Clé pour authentifier les messages (MIC) Durant le 4-Way Handshake et le Group Key Handshake,
- KEK (Key Encryption Key – 128 bits) : Clé pour la confidentialité des données durant le 4-Way Handshake et le Group Key Handshake,
- TK (Temporary Key – 128 bits) : Clé pour le chiffrement des données (utilisé pour le calcul des données d'intégrité dans le protocole CCMP)
- TMK (Temporary MIC Key – 2x64 bits) : Clé pour l'authentification des données (utilisée seulement par Michael dans TKIP). Une clé dédiée est utilisée pour chaque sens de communication.

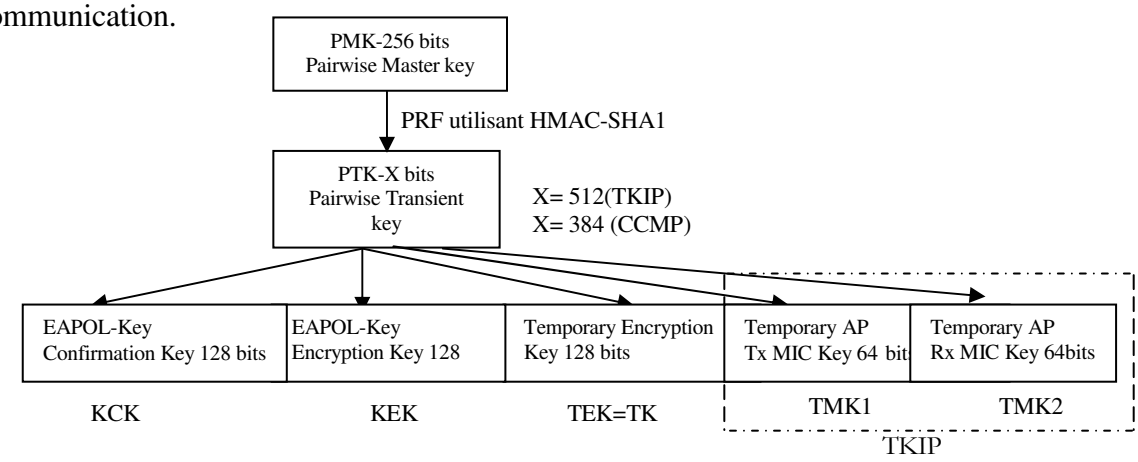

Figure 25 : Hiérarchie de clé Pairwise [39]

Le 4-way handshake :

Le 4-Way Handshake, initié par le point d'accès, permet :

- De confirmer la connaissance de la PMK par le client,
- De dériver une nouvelle PTK,
- D'installer les clés de chiffrement et d'intégrité,
- De chiffrer le transport de la GTK,
- De confirmer la suite de chiffrement choisie.

La négociation de la PTK

Quatre messages EAPOL-Key sont échangés entre le client et le point d'accès durant le 4-Way Handshake (Voir Figure 26) **;**

Le point d'accès initie le premier message en choisissant un nombre aléatoire ANonce puis l'envoie au client sans le chiffrer et l'authentifier. Le client génère ensuite son propre nombre aléatoire SNonce et est maintenant en mesure de calculer la PTK et de dériver les clés temporelles, il envoie donc SNonce et le MIC calculé sur le second message en utilisant la clé KCK. Quand le point d'accès reçoit le deuxième message, il peut extraire SNonce (car le message n'est pas chiffré) et calculer la PTK puis dériver les clés temporelles. Il est maintenant en mesure de vérifier la valeur du MIC contenu dans le second message, il s'assure ainsi que le client connaît la PMK et a correctement dérivé la PTK puis les clés temporelles.

Le troisième message est envoyé par le point d'accès au client et contient la GTK (chiffrée avec la clé KEK), dérivée d'une GMK et d'un GNonce aléatoire (Figure 27), accompagnée d'un MIC calculé sur le troisième message en utilisant la clé KCK. Quand le client reçoit ce message, le MIC est vérifié pour s'assurer que le contrôleur connaît la PMK et qu'il a correctement dérivé la PTK puis les clés temporelles.

Le dernier message acquitte la réussite de tous le Handshake et indique que le client a correctement installé les clés et qu'il est prêt à commencer le chiffrement des données. Après réception du message, le point d'accès installe ses clés et vérifie la valeur du MIC.

De cette façon, le client mobile et le point d'accès ont obtenus, calculés et installés les clés de chiffrement et d'intégrité et sont maintenant en mesure de communiquer sur un canal sûr pour le trafic à destination d'une machine ou en diffusion [39,41, 44].

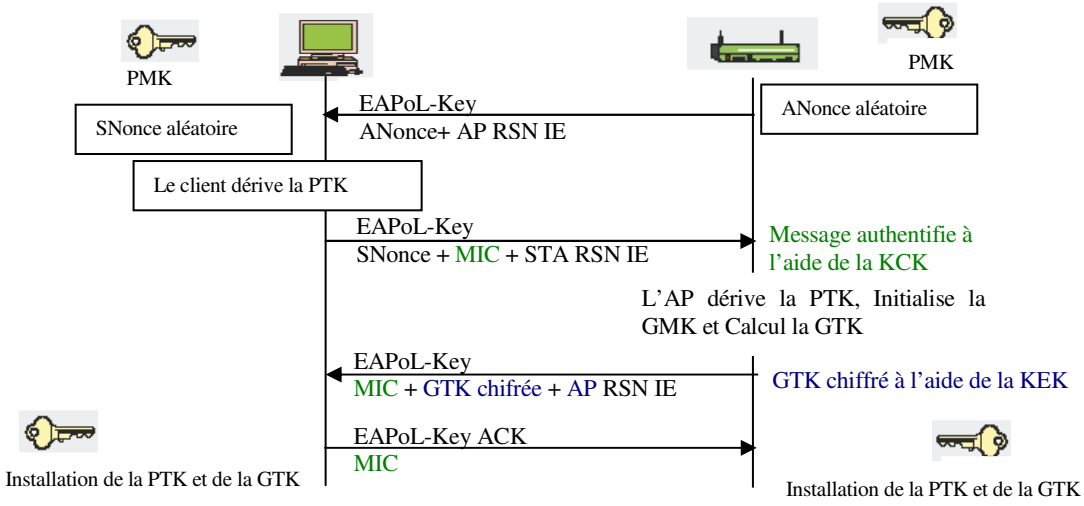

Figure 26 : 4-way Handshake [39]

La PTK est dérivée de la PMK, d'une chaîne de caractère fixe (pairwise key expansion), de l'adresse MAC du point d'accès (AP_Mac), de l'adresse MAC du client (STA_Mac) et d'ANonce et SNonce à l'aide de la fonction PRF de la façon suivante [39] :

PTK = PRF-X (PMK, Pairwise key expansion, Min (AP_Mac, STA_Mac) || Max (AP_Mac, STA_Mac) || Min (ANonce, SNonce) || Max (ANonce, Snonce)).

La fonction PRF

La fonction PRF est une fonction cryptographique appliquée sur trois paramètres : un secret, un label ("string") et une valeur aléatoire ("seed"). Sa représentation peut prendre la forme : PRF(secret, label, seed). Le string *label* nous permet d'utiliser la fonction PRF pour générer différentes clés en utilisant le même secret. Par exemples, PRF(secret, label 1, seed) et PRF(secret, label 2, seed) sont deux résultats différents.

Le trafic en diffusion est protégé par une autre clé, la GTK (Group Transient Key), générée à partir d'une clé maîtresse GMK (Group Master Key), d'une chaîne fixe, de l'adresse MAC du point d'accès et d'un nombre aléatoire GNonce. La longueur de la GTK dépend du protocole de chiffrement – 256 bits pour TKIP et 128 bits pour CCMP. La GTK est divisée en des clés temporelles dédiées [39] :

- GEK (Group Encryption Key) : Clé pour le chiffrement des données (utilisée par CCMP pour l'authentification et le chiffrement et par TKIP).
- GIK (Group Integrity Key) : Clé pour l'authentification des données (utilisée seulement par Michael avec TKIP).

Cette hiérarchie peut être résumée en Figure 27 suivante :

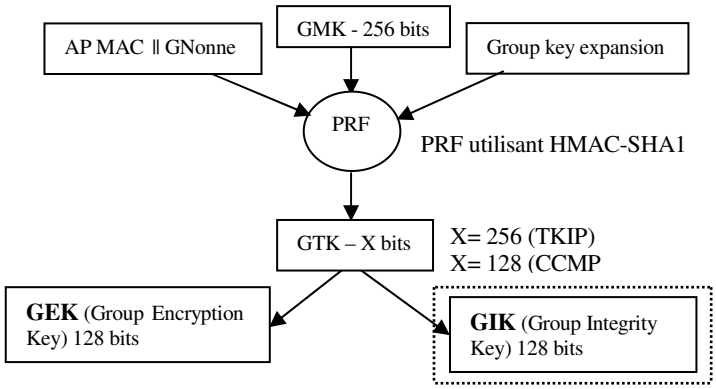

Figure 27 : Hiérarchie de clé de groupe [39]

Deux messages EAPOL-Key sont échangés entre le client et le point d'accès durant le Group Key Handshake. Cette poignée de main se base sur les clés temporelles générées durant le 4-Way Handshake (la KCK et la KEK). Ce processus est illustré en Figure 28.

Le Group Key Handshake est seulement nécessaire en cas de dé-association d'un client ou lors du renouvellement de la GTK suite à une demande client. Le contrôleur initie le premier message en choisissant le nombre aléatoire GNonce et en calculant une nouvelle GTK. Il envoie la GTK chiffrée (en utilisant la KEK), le numéro de séquence de la GTK et le MIC calculé sur ce message grâce à la KCK au client. Quand le message est reçu par le client, le MIC est vérifié et la GTK

déchiffrée. Le second message acquitte la réussite du Group Key Handshake en envoyant le numéro de séquence de la GTK et le MIC calculé sur ce second message. Après réception du message, le point d'accès installe la nouvelle GTK ; après avoir vérifié la valeur du MIC. [39,41]

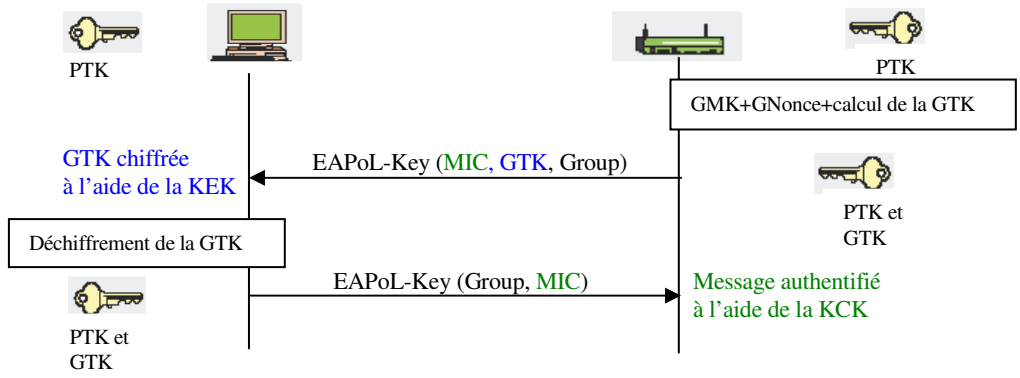

Figure 28 : Livraison d'une nouvelle clé de groupe [39]

Phase 4 : Chiffrement et intégrité au sein d'une RSNA

Toutes les clés générées précédemment sont utilisées dans les protocoles de chiffrement et d'intégrité au sein d'une RSNA :

- TKIP (Temporal Key Hash)
- CCMP(Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol),
- WRAP (Wireless Robust Authenticated Protocol).

Dans TKIP le MIC est calculé sur le MSDU (*MAC Service Data Unit*) tandis que dans CCMP il est calculé sur le MPDU (*MAC Protocol Data Unit*). Le MSDU représente un paquet de données avant sa fragmentation alors que le MPDU représente les multiples unités de données après fragmentation. [39]

TKIP

Tout comme le WEP, TKIP est basé sur l'algorithme de chiffrement RC4 mais il existe seulement pour une raison : afin de permettre une mise à jour aux systèmes à base de WEP pour bénéficier d'un protocole plus sécurisé. TKIP est nécessaire pour la certification WPA et est inclue de manière optionnel dans le RSN 802.11i. TKIP procure des corrections pour chaque faille du WEP détaillée précédemment [39]:

- L'intégrité des messages : un nouveau MIC (Message Integrity Code) basé sur l'algorithme Michael, qui est bien plus puissant que le contrôle d'intégrité de WEP ;
- IV : nouvelle méthode de sélection de valeur des vecteurs d'initialisation (IV), réutilisation de l'IV en temps que compteur anti-rejeu (TSC, ou TKIP Sequence Counter) et augmentation de la taille de l'IV (48 bits) pour éviter sa réutilisation,
- Per Packet Key Mixing : pour obtenir des clés en apparence non liées,
- Gestion de clé : nouveau mécanisme pour la génération et la distribution des clés.

Le schéma TKIP de mixage des clés est divisé en deux phases :

La phase1 implique les champs statiques – la clé de session secrète (TEK ou GEK, selon le type de trafic), l'adresse MAC du transmetteur TA (incluse pour éviter la collision d'IV) et les 32 bits de poids fort de l'IV.

La phase 2 implique la sortie de la phase 1 et les 16 bit de poids faible de l'IV, changeant ainsi tous les bits du champ *Per Packet Key* pour chaque nouvel IV.

La valeur de l'IV commence toujours à 0 et est incrémenté de 1 pour chaque paquet transmis, tout message ayant un TSC inférieur ou égal au message précédent doit être rejeté. La sortie de la phase 2 et une partie de l'IV étendu (ainsi qu'un octet factice) sont l'entrée de l'algorithme RC4, ce dernier générant une suite chiffrante que l'on XOR avec le texte en clair de la MPDU, le MIC calculé sur le MPDU et le vieux ICV issu du WEP (voir la Figure 29).

Le calcul du MIC utilise l'algorithme Michael développé par Niels Ferguson. Il a été créé pour TKIP et dispose d'un niveau de sécurité voulu de 20 bits (cet algorithme n'utilise pas de multiplications pour des raisons de performance car il se doit d'être supporté sur des vieux équipements pour permettre leur mise à jour vers WPA). Le MIC est calculé en utilisant l'adresse source (SA), l'adresse destination (DA), le texte en clair MSDU et la GIK ou TMK appropriée (dépendant du sens de la communication, une clé différente étant utilisée pour la transmission et la réception).Ce MIC est rajouté à la fin de message non crypté et crypté avec lui.

De fait que le MIC est sur 20 bit (2^{20} = 1048576) cela le rend vulnérable à une attaque brutale : le pirate peut envoyer des milliers de paquets dans le but que certain soient pris pour des paquets valables. Des contre-mesures sont nécessaires pour éviter la construction du MIC.

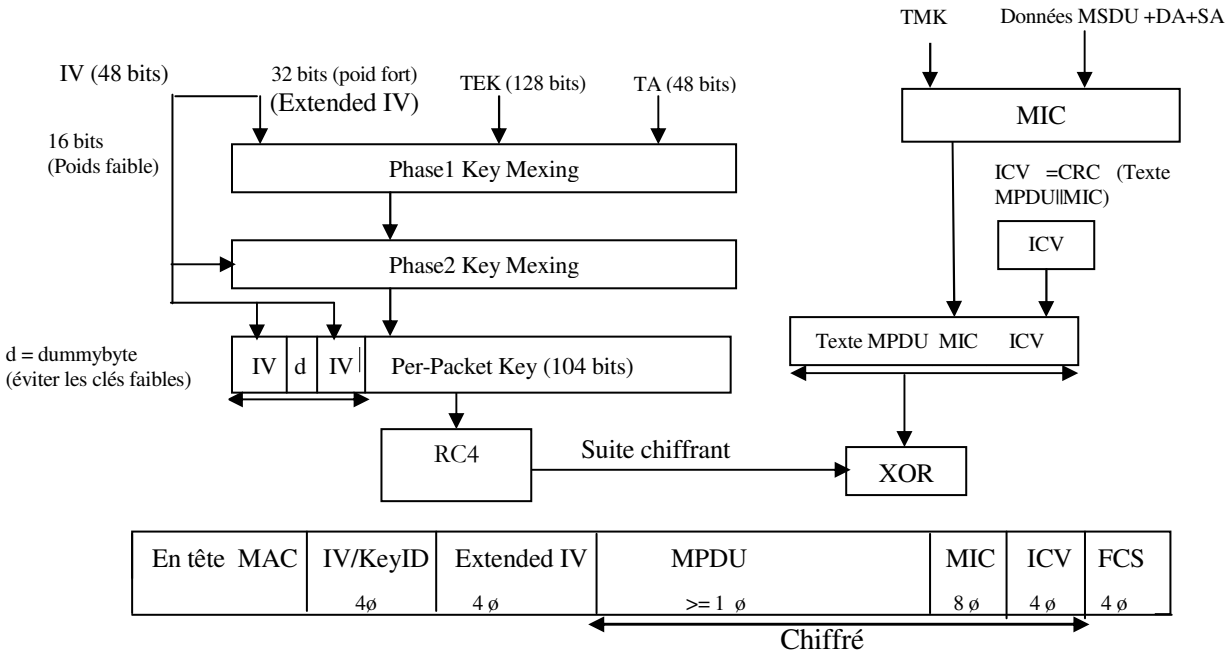

Figure 29 : Schéma TKIP de mixage des clés et de chiffrement [39]

CCMP

Le protocole CCMP (CCM Protocol) est basé sur le chiffrement par bloc AES (Advanced Encryption Standard) dans son mode d'opération CCM avec une taille de clé et de bloc de 128 bits.

AES est à CCMP ce que RC4 est à TKIP mais contrairement à TKIP, qui a été fait pour s'accommoder du matériel WEP existant, il n'est pas un compromis de sécurité mais une nouvelle architecture de protocole. CCMP utilise le mode d'opération CCM, qui combine les atouts du mode CM (Counter Mode) pour la confidentialité et de CBC-MAC (Cipher Block Chaining-Message Authentification Code) pour l'authentification et l'intégrité. [14, 39]

AES

Le protocole AES fait parti des algorithmes de cryptage « par bloc » : il prend un bloc de 128 bits et à l'aide d'une clé de cryptage (de 128, 192 ou 256 bits, au choix) il fabrique un nouveau bloc de 128 bits, crypté. Ce nouveau bloc à un aspect tout a fait aléatoire et imprévisible, ce qui fait la force d'AES. Le protocole AES définit comment récupérer le bloc original à partir du bloc crypté et de la clé de cryptage. [14]

Principe de Counter-Mode (CM)

On définit par mode la stratégie d'utilisation d'un algorithme de cryptage. Le *Counter-Mode* (CM) est un mode très apprécié pour les algorithmes par bloc, son principe est le suivant :

1. Un compteur est incrémenté sans arrêt ;
2. Ce compteur lui-même est crypté avec l'algorithme de cryptage par bloc ;
3. Ceci produit un flux infini de bits pseudo aléatoire, un peut comme RC4. Ce flux est simplement combiné avec le message, grâce à l'opération XOR.

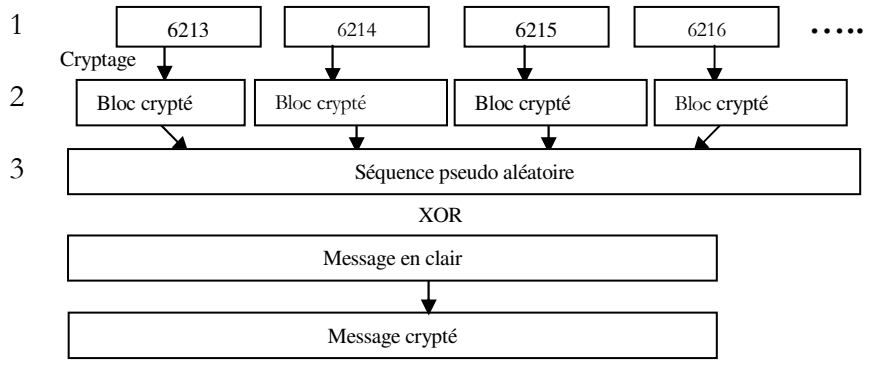

Figure 30 : Le Counter-Mode (mode compteur) [14]

Avec le Counter-Mode, un algorithme par bloc est transformé finalement en un algorithme par flux. La position d'un bit crypté correspond donc à celle de ce bit non crypté, le pirate s'il sait comment tromper le système de contrôle d'intégrité (comme le cas du WEP), peut modifier le message à l'endroit de son choix. IL faut donc que l'algorithme de contrôle d'intégrité soit très sur. [14]

Le code CBC :

Après avoir découpé le message en bloc de 128 bits chacun, le code CBC est calculé de la façon suivante [14] :

- Le premier bloc du message est crypté avec AES
- Ce bloc crypté est combiné avec le deuxième bloc non crypté, grâce à l'opération XOR ;
- Le résultat est lui-même crypté avec AES et ainsi de suite, bloc par bloc.

Le code CBC qui résulte de ce calcul a la longueur d'un bloc. Sa valeur est complètement imprévisible. Il s'agit donc d'un excellent code de contrôle d'intégrité, son principal défaut est qu'il, est gourmand en puissance de calcule. En outre, il ne peut fonctionner que si le message à une longueur égale à un multiple de la taille des blocs. Le protocole CCMP utilisé par WPA/AES résout ce problème en complétant le message avec des zéro (*padding*).

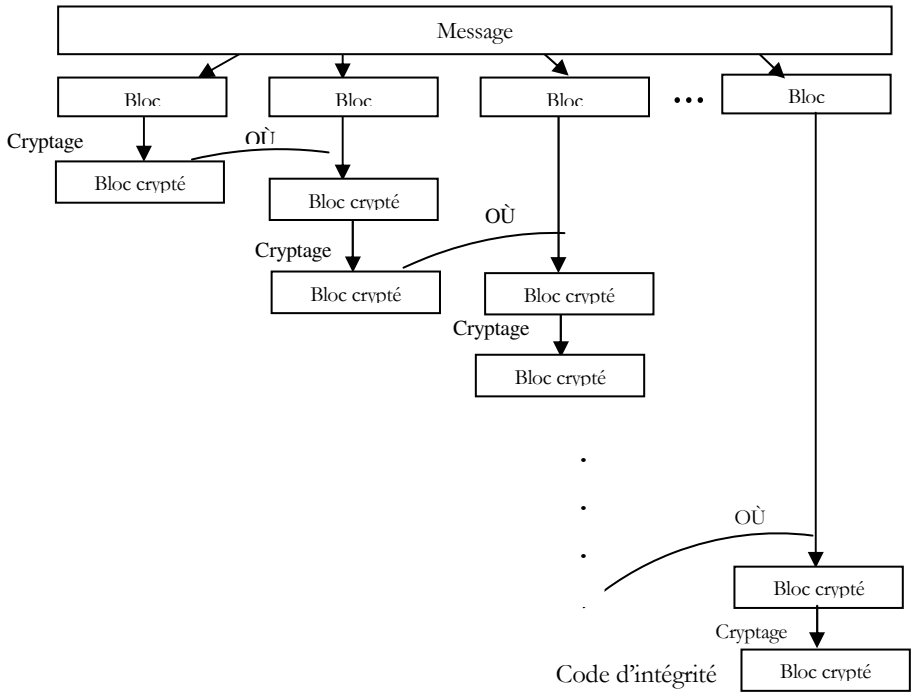

Figure 31 : Le code d'intégrité CBC [14]

Le protocole CCMP ajoute 16 octets au MPDU : 8 octets pour l'en-tête CCMP (figure 32) et 8 octets pour le MIC. L'en-tête CCMP est un champ non chiffré inclue entre l'en-tête MAC et la partie des données chiffrées contenant les 48 bits du PN (Packet Number = IV étendu) et le Group Key KeyID (utile uniquement pour le trafic de groupe, comme pour TKIP) ; Le PN est incrémenté de un pour chaque MPDU. Il est utilisé pour crypter et calculer le CBC de chaque message, afin que deux massages identiques envoyés avec la même clé ne donne jamais le même résultat .Le PN est séquentiel il est également utilisé pour éviter les attaque de relecture. [14]

PN0	PN1	Rsv	Key ID	PN2	PN3	PN4	PN5
1 octet	1 octet	1 octet	1 octet	1 octet	1 octet	1 octet	1 octet

Figure 32 : L'en-tête CCMP

Des en-têtes protégés :

Une originalité de CCMP est que le MIC est calculé sur l'ensemble de message plus l'en-tête CCMP et MAC, hormis les champs modifiables qui sont remplacés par des zéro. Ceci est le cas si une stratégie de qualité de service est mise en œuvre et que la priorité du paquet peut être modifiée en fonction de l'état de réseau. Les champs de l'en-tête MAC utilisés construit l'AAD (Additional Authentification Data).

Chiffrement CCMP :

Voyons maintenant comment CCMP effectue le chiffrement et le calcul de MIC:

Le calcul du MIC utilise l'algorithme CBC-MAC qui chiffre un bloc aléatoire de départ (obtenu grâce au champ Priority, à l'adresse source du MPDU et au PN incrémenté) et XOR les blocs suivants constitués à partir de donnée MPDU, l'en-tête CCMP et quelques champs de l'en-tête MAC (AAD) pour obtenir un MIC final sur 64 bits (le MIC final fait 128 bits mais les 64 bits de poids faible sont écartés). Le MIC est alors concaténé aux données en clair pour le chiffrement AES en mode compteur (CM). [14, 39, 41]

Ce compteur est construit sur une valeur aléatoire identique à celle utilisée pour le MIC combinée à un compteur incrémenté de 1 pour chaque bloc.

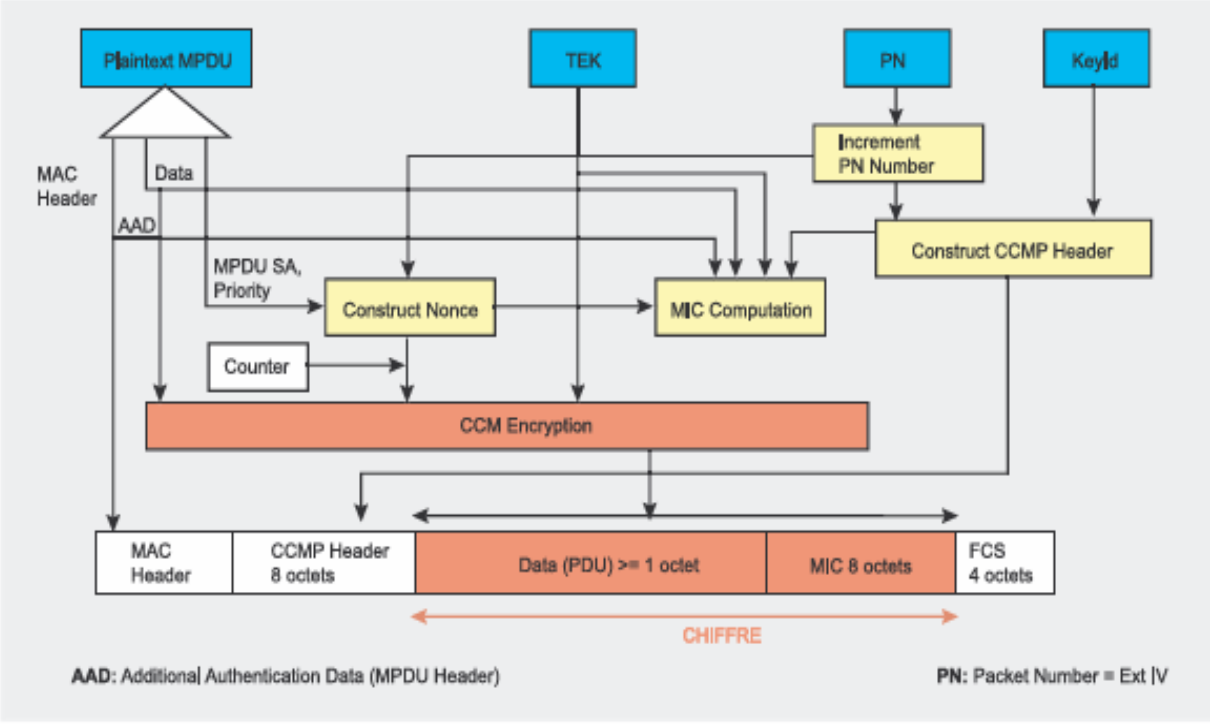

Figure 33 : Chiffrement CCMP [39]

Avant d'analyser quelques failles dans 802.11i, rappelons quelques règles de protection élémentaires [14, 41]:

a. Réduire la visibilité du système

La première étape pour éviter la compromission d'un WLAN consiste à réduire sa visibilité aux sources extérieures. On peut avoir recours aux techniques suivantes :

a.1 Limiter les débordements

Une première mesure de protection contre les attaques du réseau sans fil consiste à s'assurer que les ondes radio ne débordent pas sur l'extérieur de l'entreprise. Cette protection doit être pensée au moment de l'audit de site et de déploiement, en positionnant correctement les points d'accès pour que le niveau de signal soit très faible à l'extérieur des locaux.

a.2. Masquer le SSID

Cacher le nom du réseau, ou SSID, de telle sorte qu'un utilisateur ne voie pas le réseau et ne puisse donc pas s'y connecter. Cette mesure de sécurité n'est hélas que provisoire. Si un attaquant écoute le réseau suffisamment longtemps, il finira bien par voir passer le nom du réseau puisqu'un utilisateur qui souhaite se connecter doit donner ce SSID.

b. Le filtrage par adresse MAC

Les points d'accès permettent généralement dans leur interface de configuration de gérer une *liste de droits d'accès* (appelée ACL) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil en activant ce Filtrage des adresses MAC. Même si cette précaution est un peu contraignante, de fait que les paquets qui contiennent les adresses MAC sont transmis en clair et les entrées dans la liste ACL peuvent facilement être obtenues par un logiciel sniffer comme *kismet*. Un utilisateur non autorisé peut usurper ces adresses MAC et tenter d'accéder au point d'accès**,** il est quand même recommandé d'utiliser cette mesure de sécurité car elle permet de réduire le risque d'attaques ponctuelles.

4.2.5. Les faiblesses de WPA/WPA2

Quelques faiblesses ont été découvertes dans WPA/WPA2 depuis leur sortie,

Les risques avec l'authentification 802.1X

Une authentification à sens unique

Le premier problème de 802.1X réside dans son traitement asymétrique d'authentification entre la station et le point d'accès. Selon le standard, le port devient contrôlé après le succès de la phase d'authentification qui n'est pas applicable pour la station dont le port reste toujours à l'état authentifié. L'authentification à sens unique expose la station à plusieurs attaques ; notamment "*MIM*" et "*DoS*". [8, 42]

a. L'attaque "MIM"

L'intrus agit comme un légitime point d'accès pour la station et comme un client authentifié pour le réseau. En effet, dans l'architecture 802.1X, la station n'accepte que les requêtes EAP du point d'accès et ne lui répond que par des réponses EAP. Par conséquent, le point d'accès

n'accepte aucune requête EAP de la station. Cette menace peut être éliminés si une authentification mutuelle forte est rendu effectif, le protocole d'authentification (par exemple, EAP/TLS) devez empêche un adversaire de forger, modifier et rejouer les messages d'authentification. Dans la section suivante, on détail ce protocole et on montrera comment un pirate, si la méthode d'authentification n'est pas efficace, pourra réaliser une attaque MIM et récupérer la PMK et peut même prendre le contrôle totale d'une session (session hidjaking). [8, 42, 45]

L'attaque "*Man-In-The-Middle*" peut contourner tout type de mécanisme d'authentification de niveau supérieur et le rend inefficace quel qu'il soit. Cette faille vient de protocole EAP lui-même puisque il ne contient aucune mesure pour l'intégrité. En effet, tous les mécanismes d'authentification se terminent par une notification de succès ou d'échec envoyée du serveur à la station à l'aide du message *EAP-Success* ou *EAP-Echec*. Malheureusement, ce message ne contient aucune information qui conserve son intégrité et donc il est possible pour l'intrus de forger son propre message *EAP-Success* et de se subtiliser au point d'accès. Tout le trafic réseau de client va donc passer par lui. [8]

b. Le détournement d'une session :

Le détournement d'une session (session hidjaking) peut exister même si une authentification sûr est réalise. Après qu'un poste légitime ait complété une authentification prospère, l'adversaire, pourrait déconnecter un poste en forgeant les messages de dé-authentication ou dé-association, et reprend la session avec le point d'accès de la part du poste légitime. Cependant l'adversaire pour interagir aura besoin d'obtenir les informations d'authentification, telles que la PTK. [8, 42,45]

c. L'attaque DoS " Denial-of-Service"

Parmi les attaques qui ont toujours lieu avec 802.1X ; nous rencontrons l'attaque Déni de Service (DoS). Le but de cette attaque est d'empêcher l'accès aux ressources du réseau. Il peut se réaliser en engorgeant le réseau avec du trafic inutile afin d'étrangler sa capacité de servir et de répondre aux besoins de ses légitimes utilisateurs.

Avec les réseaux 802.11 sans fil, DoS peut se réaliser facilement**.** Il peut intervenir à plusieurs niveaux ; notamment au niveau physique et au niveau de liaison. En effet, comme tout réseau mobile, les fréquences radio de 802.1X peuvent dépasser plus ou moins largement le bâtiment dans lequel se trouve l'antenne d'émission (point d'accès), et donc l'attaque DoS peut s'effectuer facilement. Ce qui permet à l'intrus d'avoir accès au moyen de transport du réseau ;

Au niveau liaison, Il y a plusieurs attaques du DOS qui exploitent les messages EAP sans protection dans l'authentification 802.1X, un adversaire peut forger le message EAPOL-Start à maintes reprises pour empêcher l'authentification 802.1X de réussir, et forger les messages EAPOLFailure et EAPOL-Logoff afin de déconnecter le client.

Puisque les trames de gestion et trames du contrôle sont déprotégé dans un WLAN, un adversaire peut forger facilement ces trames pour lancer une attaque du DOS. Parmi les attaques les plus effectif sur les trames de gestion consiste à forge et à maintes reprises l'envoie des trames de dé-authentication ou dé- association. [8, 45]

Les failles dans le 4-Way Handshake

a. Attaques par dictionnaire et force brute hors ligne

La vulnérabilité la plus exploitable est une attaque contre la clé PSK utilisée dans WPA/WPA2. Comme déjà mentionné précédemment, la PSK est une alternative à la génération de la PMK par des échanges 802.1X basés sur un serveur d'authentification. La PSK est une chaîne de caractères de 256 bits ou une phrase secrète comprise entre 8 et 63 caractères de laquelle on extrait la chaîne de caractères par un algorithme connu.

La PTK est dérivée de la PMK en utilisant le 4-Way Handshake et toutes les informations nécessaires à son calcul sont transmises en clair. La force de la PTK repose uniquement sur la valeur de la PMK, qui dans le cas de la PSK repose sur la force de la phrase secrète l'ayant générée. Comme souligné par Robert Moskowitz, le second message du 4-Way Handshake peut être sujet à des attaques par dictionnaire et force brute hors ligne [39].

L'utilitaire cowpatty a été créé pour exploiter cette faiblesse et son code source fut repris et amélioré par Christophe Devine dans Aircrack afin de réaliser des attaques par force brute ou dictionnaire sur la PSK du WPA. [46]

Pour réaliser cette attaque, un attaquant doit capturer les messages du 4-Way Handshake en scrutant passivement les trames du réseau sans fil ou en utilisant l'attaque par dé-authentification (décrite précédemment) pour accélérer le processus. En fait, seul les deux premiers messages sont requis pour tester les choix de PSK. Sachant que la PTK = PRF-X (PMK, Pairwise key expansion, Min (AP_Mac, STA_Mac) ‖ Max (AP_Mac, STA_Mac) ‖ Min (ANonce, SNonce) ‖ Max (ANonce, Snonce)) où la PMK est égale à la PSK dans notre cas. Après la transmission du second message, l'attaquant connaît ANonce (grâce au 1er message) et SNonce (grâce au 2ème message) et peut commencer à choisir une PSK pour calculer la PTK et dériver les clés temporelles. Si la PSK est correctement choisie, le MIC du second message peut être obtenu avec la KCK correspondante, sinon un nouveau choix doit être effectué.

b. DoS :

Dans l'autre coté He [44] explique comment une attaque de type DoS est possible contre le 4-way handshake. L'attaque peut être réalisée en se faisant passer pour un point d'accès et composant le message 1 puis l'envoyer au client. Le pirate envoie un faux message 1 au client après le message 2 de 4-way handshake. Le client calcule la nouvelle PTK correspondante au nonce (ANonce) du nouveau message 1 reçu, ce qui provoquera le blocage de handshake suivant car la PTK est différente de celle calculée par le point d'accès. [45]

III.5. Méthodes d'authentification

5.1. Introduction

Le succès du concept EAP vient de fait que le protocole EAP, comme c'est déjà explique dans la section présidente, se résume à encapsuler les données servant à l'authentification et les méthodes EAP prennent en charge l'authentification en mettant en forme et en interprétant ces données d'authentification. Il ressort de cette séparation que les protocoles faisant appel à une authentification par EAP ne sont plus attachés à une méthode EAP particulière. Ainsi, en cas de failles de sécurité découvertes sur une méthode EAP, il suffit de changer de méthode EAP ; les protocoles s'appuyant sur EAP sont conservés.

A ce jour, plus d'une quarantaine de méthodes EAP existent, mais seulement six d'entre elles sont standardisées à l'IETF (Internet Engineering Task Force) : EAP-MD5 [6] et EAP-TLS [47], EAP-OTP (One-Time-Password) et EAP-GTC (Generic Token Card) [6], qui sont simples d'usage, mais ne proposent qu'une authentification unilatérale ou encore EAP-SIM (Subscriber Identity Modules) [48], et EAP-AKA (Authentication and Key Agreement) [49] qui ont été spécifiées pour fonctionner dans les environnements GSM/UMTS et qui sont plutôt prévues pour fonctionner à l'aide de cartes à puce. [50]

Une méthode d'authentification EAP utilise différents éléments pour identifier un client : login / mot de passe ; certificat électronique ; biométrie ; puce (SIM). Certaines méthodes combinent plusieurs critères (certificats et login/mot de passe etc.) généralement se sont des méthodes à base de tunnel comme TTLS et PEAP. [8, 14]

Dans ce qui suit on décrit et on évalue les méthodes suivantes :

- **EAP-TLS** : authentification mutuelle entre le client et le serveur Radius par le biais de certificats (côté client et côté serveur) ;
- **EAP-TTLS** [51]: authentification mutuelle du client et du serveur Radius par le biais d'un certificat côté serveur, le client peut utiliser un couple login/mot de passe ;
- **EAP-MD5** : pas d'authentification mutuelle entre client et le serveur Radius, le client s'authentifie par mot de passe ;

5.2. Etude de quelques méthodes existantes

1. EAP/TLS

La méthode EAP-TLS, issue du protocole TLS (Transport Layer Security) [52], fournit l'authentification mutuelle du client et de serveur à travers l'usage des certificats numérique. TLS est conçu pour fournir une authentification sûre et une confidentialité des données en faisant usage de la fiabilité de la Couche transport de la pile TCP/IP. Il fournit la sécurité à tout protocole d'application des couches supérieures.

Processus d'échange de messages

Comme l'illustre la figure 34, la négociation EAP-TLS commence typiquement entre la station et le point d'accès. Après la phase d'association, le point d'accès envoie une requête d'authentification au client. Le client répond avec son identifiant (nom de machine ou login), ce message est relayé par le point d'accès vers le serveur d'authentification.

A ce moment, le serveur d'authentification initie le processus d'authentification de TLS en envoyant le message EAP-TLS/start. Le client répond par le paquet EAP-Response contenant le message *ClientHello*. Ce message contient, entre autre, la version du protocole TLS supportée, un nombre aléatoire, un identifiant de la session et une suite cryptographique (fonctions de hachage, algorithmes de chiffrement) supportés par le client dans un ordre décroissant de préférence.

Si le serveur ne supporte aucun des suites cryptographiques envoyées par le client, il arrête la négociation. Autrement, il doit répondre par un paquet EAP-Request contenant le message *ServerHello* qui contiendra une suite cryptographique choisit de la liste envoyée par le client, un nombre aléatoire utilisée comme une entrée pour le processus de génération de clés et d'un identifiant de session (en fonction de celui proposé par le client). Le message hello du serveur est suivi par son certificat contenant sa clé publique, par une demande du certificat du client et par le message *ServerHelloDone* afin d'indiquer la fin de son hello.

Le client répond par un paquet EAP-Response contenant les messages : *certificat* s'il en a un sinon un message contenant "no certificates", le *ClientKeyExchange* comportant une valeur aléatoire de 48 octets appelée *premaster secret* qu'il génère chiffrée avec la clé publique du serveur qui la déchiffre en utilisant sa clé privée pour obtenir le *premaster secret*. Ce secret est utilisé avec les valeurs aléatoires qui se sont échangée pour générer la même *master_secret* par le client et le serveur qui l'utilise dans la génération des clés symétriques utilisées dans le chiffrement et dans le calcul du MAC durant l'échange des données.

Si le client est certifié, il envoie également un message de confirmation explicite : *CertificateVerify*. Ce message inclut un condensé de tous les messages envoyés/reçues depuis le message *ClientHello*. Ce condensé est ensuite chiffré avec la clé privée du client qui envoie le résultat au serveur. Le serveur authentifie le client en vérifiant son certificat ainsi que sa signature appliquée sur le condensé des messages de la négociation.

Après l'envoie du message *ChangeCipherSpec* afin de déclencher le chiffrement des échanges selon les choix effectués dans la phase précédentes, le client le fait suivre immédiatement du message *Finished* qui est un condensé de tous les messages de la négociation y compris la *premaster secret* en employant les attributs cryptographiques qui viennent d'être négociés.

Si le client s'est correctement authentifié, le serveur répond par un paquet EAPRequest dont le champ de données encapsule les messages *ChangeCipherSpec*et, et *Finished* de TLS qui est généré de la même façon utilisée par le client. Le client authentifie le serveur en vérifiant que le condensé est identique à celui qu'il avait envoyé dans son message *Finished*.

Le client envoie ensuite un paquet EAP-Response dont le champ de données est vide et le serveur répond par le massage EAP-Success.

Le client et le serveur définissent en fonction des valeurs aléatoires qui se sont échangées et la *premaster secret* une clé de chiffrement principale « *master_secret* » utilisée pour la session. [8, 14, 47, 53]

A la fin de la phase d'authentification, le serveur envoie la clé de chiffrement (PMK) au point d'accès dans un message Raduis dédié à cet effet. [8, 14, 47, 53]

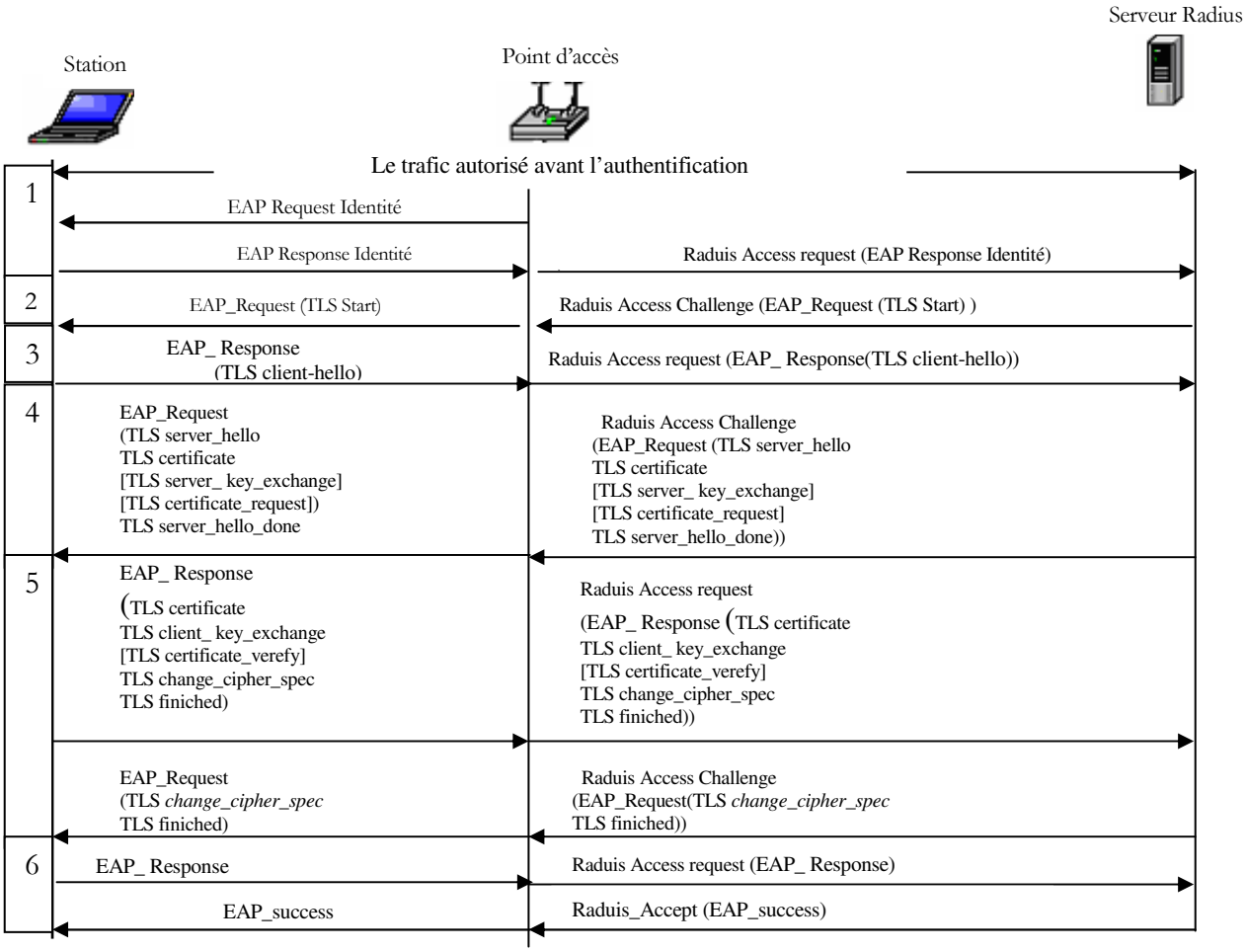

Figure 34 : Échanges EAP-TLS [8]

Analyse

La méthode EAP-TLS assure une authentification sûr et efficace à l'aide de certificats numériques. L'utilisation du certificat protège les entités contre plusieurs attaques ; notamment l'attaque MIM (*Man-In-The-Middle*). Cependant, durant le déroulement d'une session EAP-TLS, le serveur est relié à l'Internet et donc peut vérifier l'identité et la validité du certificat du client et de contrôler si le certificat est révoqué ou non alors que le client peut ne pas avoir aucune connexion Internet et donc il ne peut pas suivre la chaîne de certification et vérifier si le certificat du serveur a été révoqué ou non. Néanmoins, le client peut achever cette opération après l'établissement de la session EAP-TLS.

L'utilisation des certificats avec EAP-TLS exige une infrastructure à clé publique (PKI). Cette infrastructure ne peut pas être toujours déployée dans plusieurs types d'entreprises. En effet, elle nécessite la distribution des certificats aux clients et la révocation de celles qui ne sont plus valides. En plus, elle entraîne un surplus important en terme de gestion et de ressources machines et humaines. Notons que le certificat du client passe en clair sur le réseau et donc EAP/TLS n'offre pas la protection d'identité. [8, 14, 53]

Enfin, l'absence de l'intégrité et du chiffrement des messages de notification de la session EAP/TLS (échec ou succès) rend possible la réalisation des attaques de type DoS et MitM. Un intrus peut toujours remplacer le massage EAP-Success par le massage EAP-Echec et vice versa. [14, 8]

2. EAP-TTLS

Fonctionnement

EAP-TTLS est un Internet Draft définissant une méthode qui utilise le protocole EAP et le tunnel TLS dans le but d'établir une session authentifiée et sécurisée entre le client et le serveur d'authentification. Elle étend l'EAP-TLS et elle est presque aussi sûre que la méthode EAP-TLS, tout en simplifiant le déploiement des certificats. Les certificats ne sont en effet nécessaires que sur le serveur d'authentification. L'authentification du client peut se réaliser par d'autres moyens que le certificat ; mot de passe (CHAP [54], MSCHAPv2 [55]) ou carte à puce.

EAP-TTLS distingue deux phases d'authentification :

- Tunnel TLS, c'est une session TLS avec l'authentification du serveur par un certificat valide. Elle sert à protéger les échanges de la deuxième phase.
- Identification du client par le serveur en utilisant une méthode simple ((CHAP, MSCHAPv2), carte à puce, etc.).

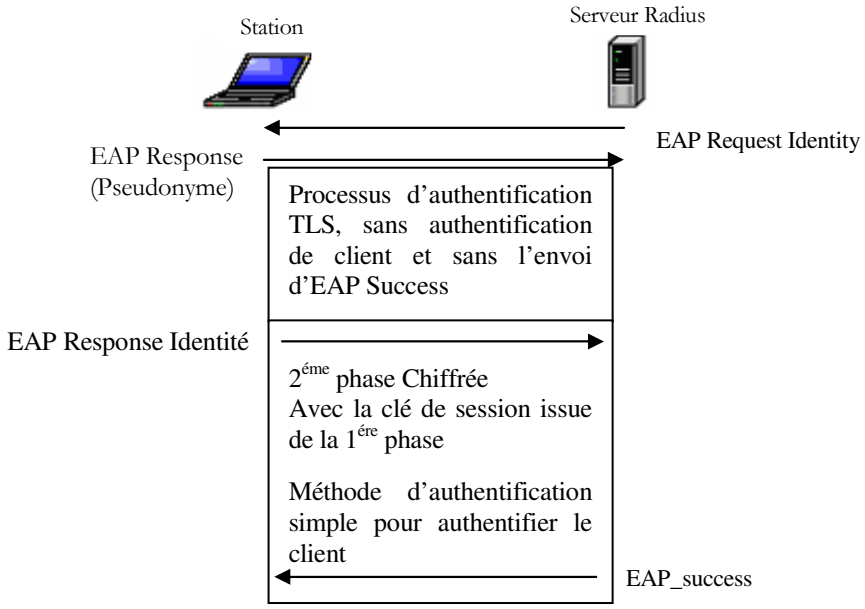

Figure 35 : Échanges EAP-TTLS

Durant la première phase, le processus d'authentification EAP/TLS, permet en plus de l'authentification du serveur par le client l'établissement d'un tunnel en utilisant la clé de session dérivée de ce processus. Ce tunnel est utilisé dans la deuxième phase, pour l'authentification de client. Si le client souhaite cacher son identité, il donne un pseudonyme dans le message EAP Response-Identity de la première phase.

Analyse

EAP-TTLS a un avantage par rapport à EAP-TLS, elle assure la protection de la notification du mécanisme d'authentification et de l'identité du client grâce au tunnel TLS établi durant la première phase. Ce tunnel garantit la confidentialité des échanges pour la deuxième phase. Ce qui donne l'avantage à l'administrateur du réseau de choisir une simple méthode d'authentification pour ses utilisateurs (mot de passe transit en clair dans le Tunnel TLS) et donc de supprimer la complexité de gestion liée aux certificats et à l'infrastructure à clé publique.

En revanche, EAP-TTLS n'est pas toujours protégée contre l'attaque *Man-In-The-Middle*, le pirate peut essayer de créer un tunnel avec le client et un tunnel avec le serveur. Il peut donc avoir accès à la méthode d'authentification « interne » utilisée qui est souvent très vulnérable en procédant de la façon suivante [14,8] :

Le pirate configure son poste pour se comporter comme un point d'accès (même SSID qu'un AP légitime) ; Lorsqu'un client cherche à se connecter à lui, le pirate ne redirige pas encore les paquets à un AP légitime, il se comporte comme le serveur d'authentification et envoie un faut certificat au client pour établir un tunnel sécurisé ;

Si le client ne vérifie pas rigoureusement le certificat qui lui est envoyé, il peut croire avoir affaire au serveur d'authentification légitime. Il utilise alors le tunnel crée entre lui et le pirate pour négocier la méthode EAP interne ;

Au ce moment, le pirate négocie lui-même TTLS avec le serveur d'authentification, via un AP légitime. Cette étape est possible puisque aucune authentification n'est exigée du côté de l'intrus. Au sein de ce tunnel, il redirige tout le trafic EAP interne et fini par accéder au réseau.

A l'issue de cette attaque, non seulement le pirate est accepter complètement sur le réseau, avec ses propres clés de cryptage temporaire, mais en plus il a vu passer la négociation EAP interne en clair. Or cette négociation interne est généralement très simple et vulnérable : par exemple, avec PAP, le mot de passe est envoyé en clair à l'intérieur de tunnel, avec EAP/MD5, le pirate peut faire une attaque de dictionnaire hors ligne, etc. [14]

3. EAP-MD5

Description

La méthode EAP-MD5 se base sur le protocole CHAP (Challenge Handshake Authentication Protocol) qui vise à authentifier un client en utilisant le principe de défi-réponse. EAP-MD5 nécessite une clé partagée entre client et serveur d'authentification. Cette clé consiste généralement

en un mot de passe associé à un nom d'utilisateur ou à une identité (par exemple une adresse IP ou MAC).

Comme l'illustre la figure 36, l'authentification avec EAP/MD5 se déroule comme suit [50]:

1) Après l'association et la phase EAP standard de demande d'identification, le serveur émet une requête EAP-MD5 sous forme d'un texte de défi ou challenge (étape 3) ;
2) Le client doit répondre à cette requête en calculant un hash à partir de ce défi et de la clé partagée avec le serveur. Le hash est retourné dans un message EAP (étape 4) ;
3) Le serveur effectue le même calcul de hash que le client et compare les deux hash. Deux hash identiques signifient que le client possède la bonne clé, ce qui conduit au succès de l'authentification et à l'émission d'un message d'acceptation (étape 5a). Sinon, l'authentification échoue et le serveur rejette la demande (étape 5b). En fonction de cette décision, le point d'accès autorise ou non le client à accéder au réseau.

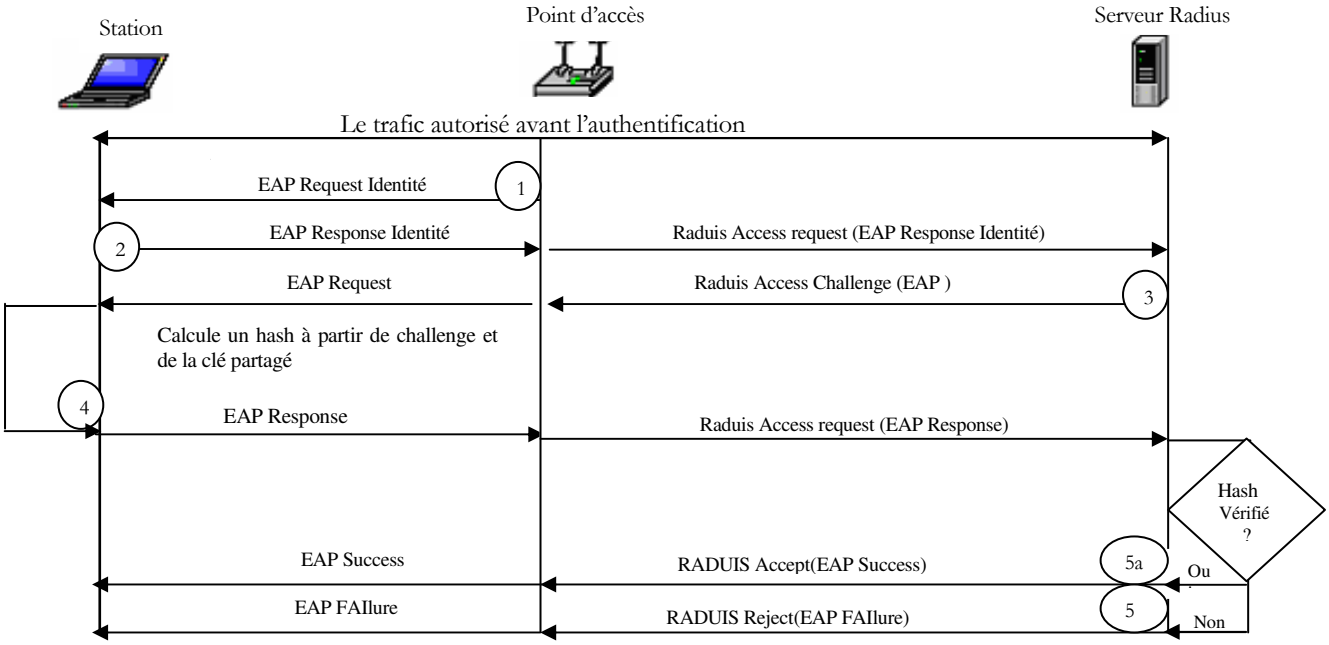

Figure 36 : Échanges EAP-MD5 [50]

Analyse

Les échanges sont non chiffrés. Le challenge texte et son résultat chiffré transitent en clair sur le réseau. Cette méthode est vulnérable aux attaques de dictionnaire et par force brute, MIM et session hijacking. [50]

Enfin, EAP-MD5 est une méthode d'authentification unilatérale dans la mesure où le client s'authentifie auprès du serveur, mais ne peut pas authentifier le serveur. Il n'est donc pas possible avec cette méthode de détecter de faux serveurs EAP et donc des points d'accès malveillants (contrôlés par des intrus). [50]

CHAPITRE IV

Proposition d'une solution d'authentification et de gestion de clés

IV.1.Introduction

Comme nous l'avons vu précédemment, la méthode EAP-TLS bien que très efficace souffre de la lourdeur de gestion due a l'infrastructure à clé publique (PKI) et EAP-MD5 qui présente l'avantage d'être léger est victime de plusieurs attaque du fait de l'authentification unilatérale. Plusieurs autres méthodes d'authentification pour les LANs sans fil, ont été proposées, mais chacune a une certaine limitation. En autre, la majorité ne fournit pas tous les services de sécurité ; notamment l'échange anonyme et la protection à long terme des données qui sont important dans les environnements sans fil et la plupart des méthodes construites pour répondre à l'anonymat comme EAP/TTLS sont victimes de l'attaque Man-In-The-Middle.

Dans ce qui suit, nous proposons une méthode EAP/AH (Authentification Hybride), qui combine le chiffrement symétrique et asymétrique. La clé partagée est utilisée pour l'authentification mutuelle alors que les clés publiques sont utilisées pour générer une clé pour chaque session.

Or la clé publique doit être authentifiée. C'est à dire, il faut que le serveur ait une preuve que la clé publique est bien la sienne. Autrement dit, il faut que le serveur ait un certificat signé par une autorité de confiance et que le certificat contienne à la fois le nom du serveur et sa clé publique. L'usage de certificat empêche plusieurs attaques ; notamment l'attaque MIM. Avec la méthode EAP/AH, le serveur envoie toujours sa clé publique mais avec l'absence totale du certificat. Par conséquent, le serveur peut envoyer une clé temporaire non authentifiée par un certificat. Dans ce chapitre, nous montrons comment le serveur et le client s'authentifient via la clé partagée, comment ils établissent des clés dynamiques pour chaque session et comment ils luttent contre les différents types d'attaques.

Dans l'architecture RSN, après la phase d'authentification 802.1X/EAP, vient la phase de la Hiérarchie et distribution des clés (4-way handshake) qui fournit une authentification mutuelle entre le client et le point d'accès et permet de générer des clés temporaires pour le chiffrement et le contrôle d'intégrité des données. On a proposé de modifier le 4-way handshake de sorte à faire avec la méthode d'authentification EAP/AH une seule phase, cela va permettre d'éviter outre l'attaque contre les messages de notification l'attaque par force bute contre le deuxième message de cette phase.

La mobilité est l'un des avantages majeurs d'un réseau sans fil, partant de notre modification pour la procédure de gestion de clés (4-way handshake) on a proposé une solution d'authentification pour le roaming.

IV.2. EAP/AH (méthode d'Authentification Hybride)

Suppositions :

On suppose que les crédits du client sont enregistrés dans une base de données du serveur sous forme de triplets : {Id client, PSK, Code}. *Id client*, désigne l'identité du client, est utilisé pour identifier le triplet. Il correspond aux valeurs de la clé secrète partagée et d'un pseudo.
Dans ce qui suit on utilise :
- F pour designer une fonction cryptographique, qui à partir d'un certain nombre de paramètres génère une clé (par exemples HMAC-SHA-1 ou HMAC-MD5).
- h pour désigner une fonction de hachage à sens unique pour assurer l'intégrité des messages échangés.

La méthode EAP/AH est basée sur l'algorithme Diffie-Hellman. L'algorithme Diffie-Hellman permet à deux entités de générer une clé secrète. Cette dernière est utilisée dans notre méthode :

- Par le client et le serveur durant le processus d'authentification afin de réduire la charge de calcule cryptographique en utilisant le chiffrement à clé symétrique ;
- Par le client pour transmettre les clés de sessions aux points d'accès auxquels il veut s'associer.

Processus d'échange de messages

Quand le point d'accès envoie une requête d'identité au client (EAP/AH Request Identity), celui-ci, selon l'algorithme Deffie Helmen, va envoyer un paquet de réponse au serveur dont le champ de données contiendra deux grands entiers premiers entre eux, *n* et *g*, tels que n>g>1.

Le serveur, après réception des valeurs n et g génère une valeur x aléatoire qui lui servira de clé secrète et calcule sa clé publique *Ps*. $Ps = g^x \bmod n$;

De la même manière, le client de son coté calcule sa clé publique *Pc*, mais au lieu de générer une clé privée aléatoirement, il utilise la clé *PSK* partagée avec le serveur. On aura :
$Pc = g^{psk} \bmod n$.

Le serveur envoie un message contenant sa clé publique (Ps) au client, ce dernier utilise *Ps* pour calculer le secret commun *Kc* de la façon suivante:

$$Kc = F(Ps^{PSK}, code)$$
$$= F((g^x \bmod n)^{PSK}, code)$$
$$= F(g^{x\,PSK} \bmod n, code).$$

On a introduit le *code* pour éviter une attaque par force brute pour récupérer la *PSK*.

Le client par la suite, au lieu d'envoyer a son tour sa clé publique au serveur afin qu'il puisse calculer la clé *Kc*, envoie son identité *Id client* et un nombre aléatoire *randc* chiffrés avec la clé publique du serveur (*Ps*) et un cadencé de toutes les données échangées calculé en utilisant la clé *Kc*: MIC = h (Kc.XOR.Ps, code, randc, Id client, Id serveur, n, g).

A la réception, le serveur utilise sa clé privée *x* pour déchiffrer le message reçu, puis récupère la *PSK* correspondante à la valeur de *Id client*. De cette façon, il pourra calculer la clé publique du client (*Pc*) puis le secret commun *Kc* :

$$\begin{aligned} Kc &= F(Pc^{x}, code) \\ &= F((g^{psk} \bmod n)^{x}, code) \\ &= F(g^{psk\,x} \bmod n, code) \\ &= F(g^{x\,psk} \bmod n, code). \end{aligned}$$

Le serveur procède par la suite à la vérification du MIC qui lui permet de :

- S'assurer que le client à bien reçu la clé *Ps* car dans le calcule de *Kc*, on a introduit la clé *Ps* envoyée par le serveur pour éviter l'attaque MIM. Si nous supposons qu'un intrus a envoyé sa clé publique à la place de celle du serveur, cet intrus sera obligé aussi de savoir la valeur de la clé *PSK* et celle du *code*. Il n'y a donc que les entités qui ont les valeurs du *PSK* et du *code* qui puissent calculer le secret *Kc* et avoir un MIC correcte ;
- D'authentifier le client du fait que seuls ceux qui possèdent la *PSK* et *code* correspondants à *Id client* envoyé, peuvent calculer le MIC.

Si le MIC est correct, le serveur va s'authentifier a son tour : il utilise la clé *Kc* pour chiffrer un nombre qu'il génère aléatoirement (*rands*) et calculer le MIC sur toutes les données envoyées/reçues. MIC = h (Kc. XOR.Ps, Code, rands, randc, Id client, Id serveur, n, g).

Sinon il envoi un message indiquant l'arrêt de la procédure d'authentification (EAP/AH (échec)) ;

A la réception, le client utilise la clé *Kc* pour déchiffrer le *rands* et authentifier le serveur en comparant le MIC reçu par celui qu'il a calculé. Le serveur est correctement authentifié uniquement en cas de MICs identiques;

En cas de sucées, le client calcule deux clés : une clé de session PMK = F(Kc, rands, randc, Id client, Id serveur) et E = F (Kc, randc) et génère un nombre aléatoire SNonce. Puis, à la place du message *EAP-Success,* envoie SNonce et la clé *PMK* cryptée avec la clé *E* (EAP/AH response (SNonce, $\{PMK\}_E$). On a calculé la clé E qui sera utilisée pour transmetre les clés PMKs du client vers le serveur pour éviter de trop exposer la clé Kc.

Le serveur calcule E et la PMK, vérifie que le client a bien calculé la *PMK* puis l'envoie avec SNonce au point d'accès.

La vérification de la clé *PMK* du client étant effectuer par le serveur, reste à authentifié le point d'accès et dérivé les clés temporelles de session.

IV.3.Procédure de gestion de clés de session

Le point d'accès génère un nombre aléatoire ANonce, puis calcule la clé PTK : PTK = PRF-X (PMK, Pairwise key expansion, Min (AP_Mac, STA_Mac) || Max (AP_Mac, STA_Mac) || Min (ANonce, SNonce) || Max (ANonce, SNonce)). La PTK, comme c'est illustré en figure 25 consiste en plusieurs clés temporelles dédiées.

Ensuite, il génère la clé de groupe *GTK* dérivée d'une *GMK* et d'un GNonce aléatoire (voir Figure 27), envoi le nombre ANonce, la *GTK* chiffrée avec la clé *KEK* et un MIC calculé sur l'ensemble de message a envoyé en utilisant la clé *KCK*.

Quand le client reçoit ce message, récupère le nombre pseudo aléatoire ANonce, calcule la PTK, déchiffre la GTK puis vérifie le MIC pour s'assurer que le point d'accès connaît la PMK et qu'il a correctement dérivé la PTK puis les clés temporelles.

Le dernier message acquitte la réussite de tous le Handshake et indique que le client a correctement installé les clés et qu'il est prêt à commencer le chiffrement des données. Après réception du message, le point d'accès installe ses clés et vérifie la valeur du MIC.

Le processus d'authentification EAP/AH et de gestion de clés est illustré par la figure suivante :

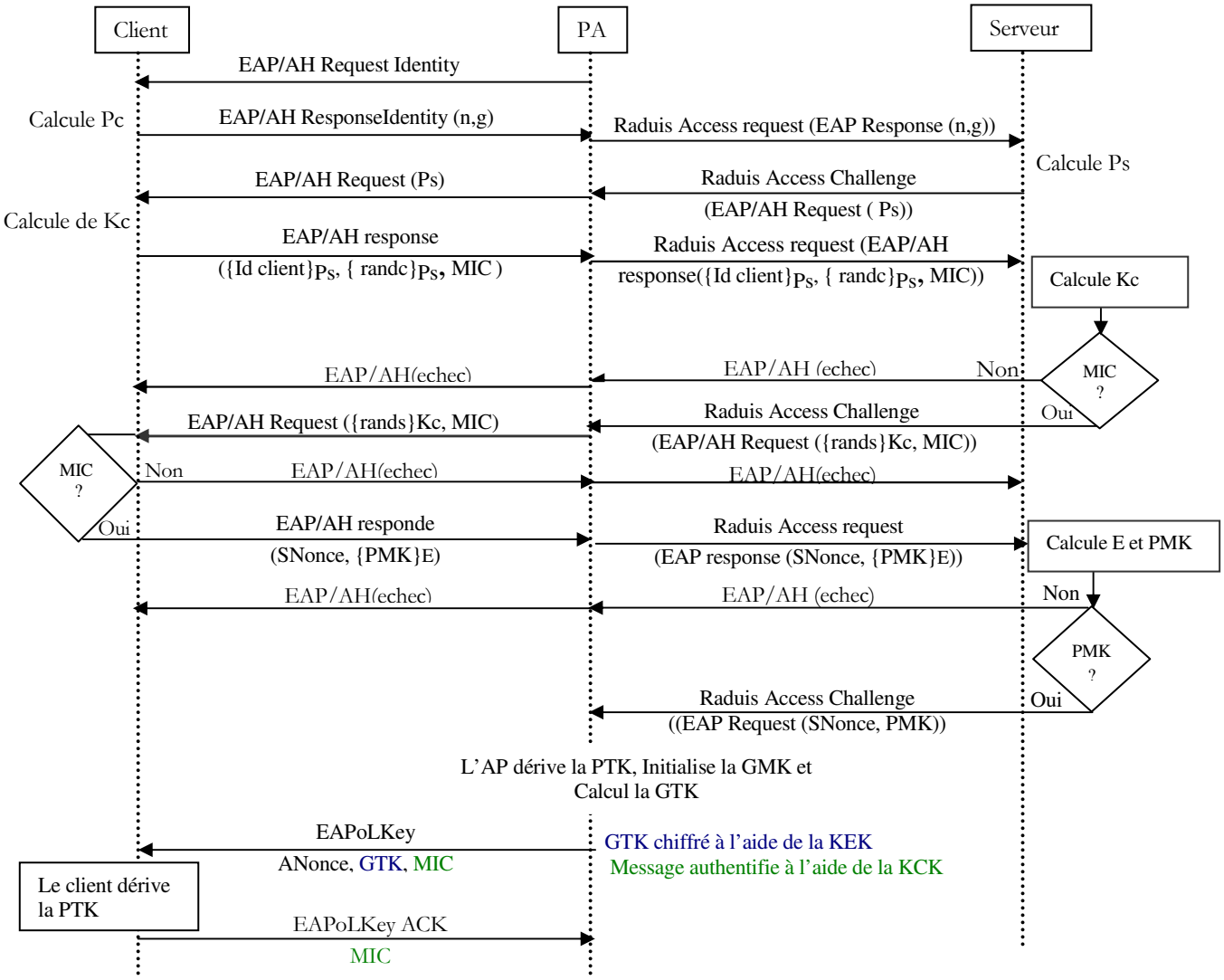

Figure 37 : Echanges EAP/AH et gestion de clés

IV.4. Evaluation

a. Méthode d'authentification EAP/AH

La méthode EAP/AH permet de vérifier les propriétés d'authentification suivantes :

Authentification mutuelle :

La méthode EAP/AH permet une authentification mutuelle entre le serveur et le client qui se base sur une clé partagée.

Efficacité contre les attaques par dictionnaire :

Avec EAP-MD5, il est possible de réaliser une attaque par dictionnaire car un espion peut avoir accès au texte en clair et au hash correspondant et se servir de ces informations pour découvrir la clé partagée. Avec EAP/AH, cette attaque n'est plus possible à cause du calcul des messages de contrôle d'intégrité (que ce soit les MICs calculés par le serveur ou ceux calculés par le client) en faisant intervenir des données qui se sont échangées cryptées (*rand c* et *Id client*) et l'introduction du *code* dans le calcule de la clé *Kc*.

Robustesse à l'attaque de l'homme du milieu (MIM) :

L'authentification mutuelle, l'introduction des clés publiques et *code* qui peut être un nombre ou un nom, sorte d'une deuxième clé partagée, dans le calcule des messages d'intégrité et dans le calcul du *Kc* permet d'éviter cette attaque. Si on se sert uniquement de la *PSK* dans le calcule du secret commun (Kc) on aura : Kc = F (Ps^{PSK}). L'intrus peut envoyer sa clé publique puis récupérer *randc* et *Id client*. Sachant que la valeur du message d'intégrité calculé par le client est : MIC = h (Kc.XOR.Ps, code, randc, Id client, Id serveur, n, g), si on calcule ce message d'intégrité sans la valeur du *code*, on aura : MIC = h (Kc.XOR.Ps, randc, Id client, Id serveur, n, g). Avec un utile rapide, le pirate peut faire une attaque par force brute sur ce MIC pour récupérer la clé *Kc* puis la même attaque sera réalisée pour avoir la valeur de la clé *PSK* (car Kc = F (Ps^{PSK})) sans que le serveur ou le client se rendent compte.

Résistance contre les attaques de rejeu :

L'utilisation des nombres aléatoires (rands, randc) et des clés dynamiques et temporelles permet de garantir la fraîcheur des messages échangés.

Outre les avantages cités, EAP/AH assure d'autres services d'authentification à savoir :

La protection d'identité :

L'identité du client « *Id client* » est envoyée cryptée à l'aide de la clé publique temporaire du serveur, qui seul possède la clé privée. Ce qui permet de cacher tout indice sur le client concerné.

La protection à long terme des données :

La majorité des méthodes d'authentifications y compris celles qu'on a cité dans le chapitre précédant, ne fournissent pas la protection à long terme des données parce qu'elles utilisent toujours la même clé dans la dérivation des clés de sessions. Si un intrus arrive à récupérer la clé partagée, il peut alors déchiffrer toutes les sessions déjà établies.

Avec le protocole EAP/AH, ce n'est pas le cas puisque le serveur et le client utilisent pour le calcule de la clé PMK une clé partagée et un nombre aléatoire (*randc*) anonyme et temporaire généré durant chaque session et cela grâce à l'utilisation de clés asymétriques dynamiques.

Par conséquent, si un intrus arrive à retrouver la clé partagée, il ne peut pas reproduire la clé de la session correspondante. Si l'intrus arrive à avoir la clé partagée, il doit casser encore l'algorithme de chiffrement asymétrique utilisé (Deffie Hellman) ou récupérer la clé privée temporaire du serveur. Même s'il arrive à récupérer la clé privée Deffie Hellman, l'intrus ne peut pas déchiffrer que la session concernée. Les anciennes sessions restent protégées.

Protection des messages de notification :

Tous les mécanismes d'authentification se terminent par une notification de succès ou d'échec envoyée du serveur à la station à l'aide du message *EAP-Success* ou *EAP-Echec* qui ne contiennent aucune information qui conserve leur intégrité et donc il est possible pour l'intrus de forger son propre message *EAP-Success* et de se subtiliser au point d'accès. Tout le trafic réseau de client va donc passer par lui. Avec EAP/AH cette attaque n'est plus possible car le message *EAP-Success* est remplacé par un message contenant la clé maitre de session (PMK)

Le tableau suivant résume une comparaison entre la méthode EAP/AH et les autres méthodes d'authentification.

	EAP/TLS	**EAP/TTLS**	**EAP/MD5**	**EAP/AH**
Authentification mutuelle	Oui	Oui	Non	Oui, grâce à une clé partagée
Méthode d'authentification	Certificat X.509	Méthodes EAP, MS-CHAP, OTP,…	Clé partagée (PSK)	Algorithme Diffie-Hellman et PSK
Infrastructure PKI exigée	Oui	Oui	Non	Non
Protection de l'identité du client	Non	Oui	Non	Oui, car : -Id client est crypté -Introduction de Ps dans le calcule de Kc
Vulnérabilité à l'attaque *Man-In-The-Middle*	Non	Oui	Oui	Non, grâce à : -Introduction de Ps dans le calcule de Kc -code qui évite l'attaque par force brute.
Protection des Messages de notification	Non	Non	Non	Oui, on indiquant le succès par l'envoie de la PMK.
Protection à long terme de données	Non	Non	Non	Oui, en utilisant des clés dynamiques et leurs introduction dans le calcule de la clé Kc

Tab.3 : Comparaison entre EAP/TLS, EAP/TTLS, EAP/MD5 et EAP/AH

Procédure de gestion des clés de session :

Architectures de RSN et de la solution proposée

Cette procédure, qui est une modification du 4-Way Handshake, permet d'éliminer l'attaque par force brute contre la *PSK* et même la *PMK*, en faisant éliminer le message 2 du 4-way handshake et faire vérifier que le client a la bonne PMK par le serveur.

Les figures 38 et 39 montrent une comparaison entre l'architecture d'authentification et de gestion de clés RSN et la solution proposée pour cette dernière :

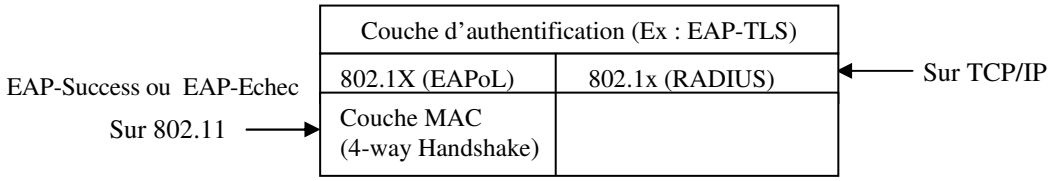

Figure 38 : Architecture RSN d'authentification et de gestion de clés

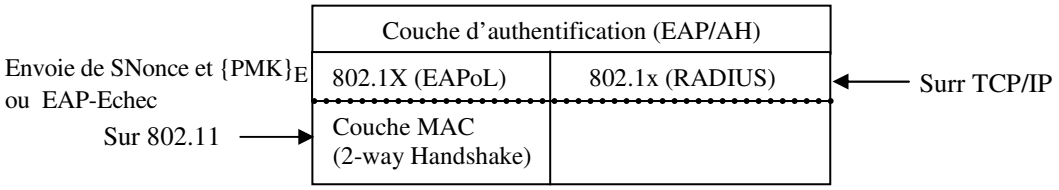

Figure 39 : L'Architecture d'authentification et de gestion de clés proposée pour RSN

L'architecture d'authentification et de gestion de clé de RSN et de la solution proposée se compose de 3 couches :

1. La couche supérieure d'authentification. 802.11i utilise EAP/TLS par exemple, notre proposition utilise EAP/AH

2. La couche centrale d'authentification (802.1X), repose sur la couche 802.11 entre le client et le point d'accès, et sur TCP/IP entre le point d'accès et le serveur d'authentification. Cette couche authentifie le client avec le serveur et permet l'échange du PMK. Le message EAP-Success de la méthode d'authentification utilisée dans RSN est remplacé par un message permettant au serveur de vérifier la PMK du client

3. la couche d'authentification MAC implique le 4-way handshake dans RSN qui laisse le point d'accès et le client s'authentifié mutuellement et le 2-way handshake dans notre proposition qui laisse le client authentifie le point d'accès.

IV.5. Le roaming

5.1. Etude de l'existant

Le standard 802.11i a introduit quelques solutions d'authentification pour le roaming. La première solution consiste à l'établissement d'une nouvelle association et authentification 802.1x/EAP à chaque fois que la station change du point d'accès. Mais cette solution est très lente et n'assure pas une connectivité continue.

Une autre solution est que la station et le Point d'accès gardent la PMK déjà négociée dans leur cache. Quand la station revient à ce Point d'accès, réemploi la PMK et saute les étapes de l'authentification 802.1x, en commençant directement la négociation des clés de session (unicast et multi-diffusion) par le protocole de gestion de clés (4-way handshake, et le Group key handshake) ce qui réduit le temps de ré association. L'inconvénient est que les points d'accès sont des dispositifs limités en ressources et ne peuvent pas stocker plusieurs PMK.

La troisième solution améliore le roaming et le fast roaming. Cette solution consiste en une pre-authentification qui signifie que la station négocie l'authentification avec les nouveaux points d'accès avant de laisser le point d'accès en cour, sans association. La station stock les PMKs négociés et utilisera une quand elle va vers un nouveau point d'accès. Quand la station quitte le courant point d'accès, elle s'associe à un prochain point d'accès, en utilisant parmi les PMKs stockées et négociées auparavant celle qui correspond à ce dernier afin qu'ils négocient les clés de session.

Dans ce qui suit, on présente notre proposition d'authentification pour le roaming. Elle consiste à dériver les PMKs de chaque point d'accès auquel la station veut s'associer a partir de celle obtenue lors de son authentification/association avec le premier point d'accès. Dans cette section on va montrer comment cela est possible sans qu'aucun point d'accès ou autre ne puisse avoir les PMKs utilisées lors de tous les roamings de la station.

5.2. Proposition

On suppose qu'a la fin de la méthode d'authentification EAP/AH, le serveur stocke une base de données qui contiendra pour chaque client i déjà associé à un point d'accès, un enregistrement sous la forme Li : $\{\{PMK\}_E$, Id client, Id PA, PMK, rands , randc , E, Valt, I, Seuil$\}$ où :

- PMK est la clé de session qui a servi pour la dérivation des clés PTK et GTK du point d'accès en cour, ie celui dont l'adresse MAC est Id PA ;
- Id PA est l'adresse MAC du point d'accès courant ;
- E : clé qui a été générée lors de l'authentification EAP/AH par le serveur et le client, elle sera utilisée pour crypter toutes les PMKs échangées entre ses derniers ;
- rands, randc sont les nombres aléatoires qui se sont échangés cryptés par le serveur et le client lors de l'authentification et leurs valeurs changent à chaque roaming selon la procédure SALT ;

- Valt: initialement, il aura la valeur Max (rands, randc) – Min (rands, randc) et pour chaque nouvelle PMK calculée pour un roaming vers un nouveau point d'accès, ce Valt est recalculé par la procédure SALT suivante :

SALT :
Début
 Si rands > randc alors
  rands ← Valt;
  Valt ← *f* (rands, randc);
 Sinon
    randc ← Valt;
    Valt ← *f* (randc, rands);
 Fsi
  I : I +1 ;
Fin.

Ou *f* est une fonction mathématique génératrice de nombres aléatoires.

- Seuil : correspond au nombre de fois possible qu'une station peut changer de point d'accès sans entamer l'authentification EAP/AH. Ce paramètre peut être configuré par l'administration réseau.
- I : compris entre 1 et Seuil, sa valeur est incrémentée pour chaque roaming en exécutant la procédure SALT.

Quand un client i déjà authentifié, désire s'associer à un nouveau point d'accès dont l'adresse MAC est « Id PA_N », au lieu d'exécuter la méthode d'authentification EAP/AH auprès du serveur, pour avoir une PMK, il génère une autre pour ce nouveau point d'accès de la façon suivante : PMK_N = F(Id PA, Id PA_N, PMK, Valt), puis envoie un message contenant la nouvelle PMK (PMK_N) et la PMK du courant point d'accès cryptées avec la clé E au nouveau point d'accès, accompagné d'un nombre aléatoire SNonce ($\{PMK_N\}_E$, ($\{PMK\}_E$, SNonce).

Le nouveau point d'accès ajoute son adresse MAC au message puis le relaye vers le serveur. Ce dernier utilise la valeur de $\{PMK\}_E$ comme indexe à l'enregistrement Li du client i qui désire s'associer au nouveau point d'accès, ce qui lui permet de calculer la PMK_N et de vérifier celle calculée par le client, si elle correspond, le client est alors authentifié et la PMK_N est envoyée au nouveau point d'accès. Le reste de ce processus est identique à celui décrit dans IV.3 de la section précédente.

Le serveur envoie un message au point d'accès identifié par IdPA lui indiquant qu'il ne devrait plus envoyer ou recevoir des données du client i.

Le client et le serveur, mettent à jour l'enregistrement : ils remplacent la PMK par celle qui vient d'être calculée (PMK_N), Id PA par Id PA_N de nouveau point d'accès, puis exécute la procédure SALT pour calculer les valeurs du *I*, *randc*, *rands* et du *Valt* pour le prochain roaming.

Le client est obligé d'exécuter le processus d'authentification dans le cas ou le Valt est nulle ou la valeur de I a atteint le seuil maximum fixé par l'administrateur (I = Seuil). Si on veut par exemple pour certaines stations dont on sait que la mobilité est très faible, exécuter le processus d'authentification à chaque changement du point d'accès, on met Seuil à 1.

On voit bien que même si on connaît l'ancienne PMK on ne pourra pas en déduire la nouvelle du fait que cette dernière est calculée en fonction de la valeur de *Valt* aléatoire calculée à l'aide d'une fonction de génération de nombres aléatoires qui à comme paramètres *rands* et *randc* connus uniquement du le client et du serveur.

La figure suivante résume tous le processus d'authentification, de gestion de clés et d'authentification pour le roaming d'un client :

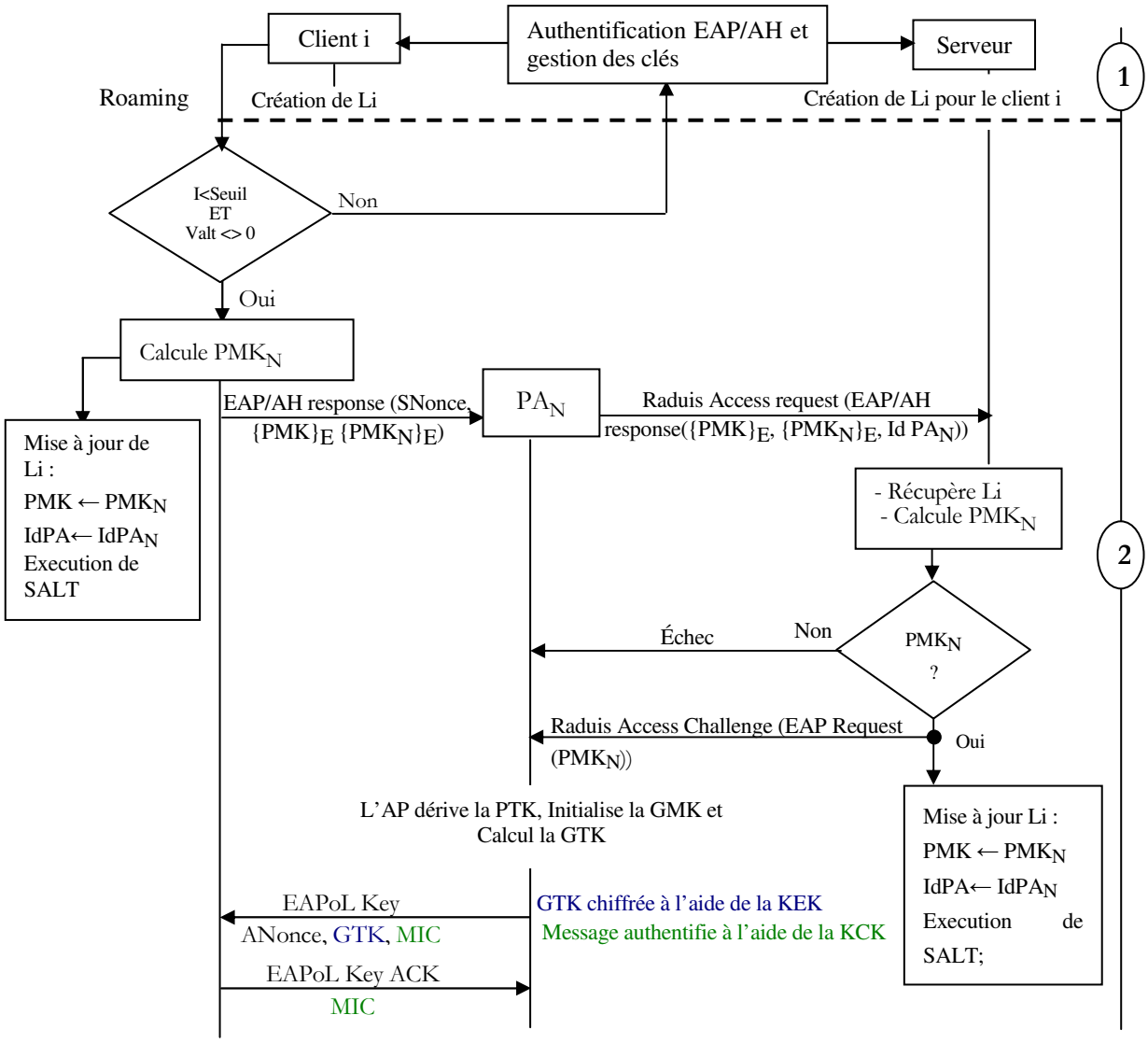

Figure 40 : processus d'authentification et de roaming

1 – Exécution du processus d'authentification et de gestion de clés indiqué en figure 37. Une fois authentifiés le client et le serveur, chacun de son coté crée l'enregistrement Li {{PMK}$_E$, Id client, Id PA, PMK, rands ,randc , E, Valt, I,Seuil}.

2 : A chaque fois que le client i change de zone de couverture ie de point d'accès, génère une nouvelle PMK en fonction des valeurs de l'enregistrement Li et si le seuil fixé par l'administrateur est atteint ou la valeur de Valt devient nulle, le client doit exécuter à nouveau le processus d'authentification et de gestion de clés.

CHAPITRE V

Conclusion perspectives

Conclusion

La transmission radio rend les LANs sans fil commode à usage, facile à déployer, et probablement plus économique, en même temps elle soulève beaucoup de problèmes de sécurité. Due à la nature ouverte de ce support de transmission, d'autres exigences de sécurité doivent être vérifiéés notamment l'anonymat et la protection à long terme des données. Le standard 802.11i à été développé pour améliorer la sécurité des réseaux 802.11 au niveau MAC en proposant une l'architecture RSN (Rubust Security Network) qui utilise le standard IEEE 802.1X pour l'authentification et le contrôle d'accès, le 4-way handshake pour la génération des clés de session et l'algorithme AES (Advenced Encryption Standard) pour le cryptage. Le standard IEEE 802.1X utilise le protocole EAP (Extensible Authentification Protocol) qui réalise une enveloppe générique pour de multiples méthodes d'authentification comme EAP/TLS et EAP/TTLS. La résistance de la phase d'authentification de la norme 802.11i aux déférentes attaques dépend de la méthode d'authentification utilisée, dans cette optique, on a proposé une méthode d'authentification EAP/AH, basée sur une clé partagée et un algorithme de chiffrement asymétrique (Diffie-Hellman) permet d'assurer l'ensemble des services d'authentification.

Contrairement aux méthodes d'authentification utilisée dans RSN, le sucées de la méthode EAP/AH est indiqué par un message contenant la clé maitre PMK cryptée, envoyée du client vers le serveur. Cela a permit d'éviter l'attaque contre les messages de notification. Après la phase d'authentification, Le 4-way handshake permet au point d'accès et au client de s'authentifié mutuellement et de générer les clés temporelles. Dans notre proposition d'authentification, la validité de la clé maitre du client est confirmé par le serveur au lieu du point d'accès, ce qui a réduit le nombre de messages de la phase de la hiérarchie et distribution des clés. L'attaque par force brute contre le deuxième message du 4-way handshake est de ce fait éliminée.

La mobilité est l'un des avantages des réseaux sans fil, notre proposition d'authentification et la modification du 4-way handshake nous a permit d'obtenir une solution d'authentification pour le roaming d'une station entre les points d'accès du même sous réseau. Cette solution permet une réauthentification rapide du fait que la station obtient la clé maître pour quelques points d'accès vers lesquels elle roam sans se ré authentifier auprès du serveur.

Perspectives

Ce travail gagnerait davantage, une fois l'implémentation effectuée sur un réseau mobile LAN sans fil. Les résultats expérimentaux, permettraient d'évaluer les performances sécuritaires de l'infrastructure logicielle proposée.

Nous nous attendions sans aucun doute, à la fameuse problématique : faut-il multiplier ou plutôt limiter, le nombre de points d'accès dans de tels réseaux : beaucoup de points d'accès, rendent complexes les contrôles d'authentification, peu de points d'accès génèrent des goulets d'étranglement à l'entrée des réseaux.

Bibliographie

[1] IEEE Standards for Information Technology. Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Supplement to 802.11-1997, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band. IEEE Std. 802.11-1999.

[2] G. PUJOLLE, Les Réseaux, Chapitre 21. Eyrolles, 2006.
http://www.editions-eyrolles.com/Chapitres/9782212119879/Chap21_Pujolle.pdf

[3] W. Arbaugh, N. Shankar, Y. Wan, Your 802.11 Wireless Network has No Clothe, http://www.cs.umd.edu/~waa/wireless.pdf , 2001

[4] IEEE Standard for Information technology – Telecommunications and Information exchange between systems – Local and metropolitan area networks – Specific requirements, Part 11, Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Std 802.11i-2004.

[5] IEEE Draft P802.1X/D11, Standards for local and metropolitan area networks: Standard for port based network access control, Mars 2001.

[6] B. Aboba et al., PPP Extensible Authentication Protocol (EAP), RFC 3748, June 2004

[7] Nokia Research Center, Man-In-The-Middle attacks in tunneled authentication protocols, http://www.saunalahti.fi/~asokan/research/mitm.html, October 2002

[8] M. Badra, Le transport et la sécurisation des échanges sur les réseaux sans fil, Thèse de doctorat, l'Ecole Nationale Supérieure des Télécommunications, 2004

[9] K. AL AGHA, G. PUJOLLE, G. VIVIER, Réseaux de mobiles et réseaux sans fil. Eyrolles, 2001

[10] IEEE, IEEE Std 802.16-2001, IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems, April 2002.

[11] IEEE Standard for Information technology -Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements. Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs). June 2002.

[12] IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements. Part 15.3 : Wireless Medium Access Control (MAC) and Physical Layer (PHY). september 2003.

[13] IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements. Part 15.4 : Wireless Medium Access Control (MAC) and Physical Layer (PHY). October 2003.

[14] A. Géron, WiFi Déploiement et sécurité, Dunod, 2006

[15] M. Lucarelli, Repères pour le WiFi, http://crdp.ac-paris.fr/d_tice/res/wifi2006fin.pdf, mars/avril 2006

[16] ETSI. Broadband Radio Access Networks (BRAN) ; HIgh PErformance Radio Local Area Network (HIPERLAN) Type 1 ; Functional specification. Technical Report, July 1998.
[17] ETSI. Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview. Technical Report, 2000.

[18] A vormales, G. Pujolle, Wi-Fi par la pratique. Eyrolles, 2002, 2004

[19] L. S. PAUN, Gestion de la mobilité dans les réseaux ambiants, Thèse de doctorat, INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE, Novembre 2005.

[20] INSA, Les réseaux locaux sans fil (RLANs). Département Télécommunications, Année 2006-2007

[21] ANSI/ISO. Information Processing Systems - Basic Reference Model for Open Systems Interconnection (OSI). ISO/IEC 7498-1:1994.

[22] M. Terré, WiFi, Mars 2007

[23] IEEE Standards for Information Technology. Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification. ISO/IEC DIS 8802-11:1997, IEEE Std. 802.11-1997.

[24] IEEE Standards for Information Technology. Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification – Amendment 1: High-speed Physical Layer in the 5 GHz Band. ISO/IEC DIS 8802-11:1999/Amd 1:2000(E), IEEE Std. 802.11a-1999.

[25] IEEE Standards for Information Technology. Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification – Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band. IEEE Std. 802.11g-2003.

[26] IEEE Standards for Information Technology. Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 2: Logical Link Control (LLC). ISO/IEC 8802-2:1998, IEEE Std. 802.2-1998.

[27] IEEE Standards for Information Technology. Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications. ISO/IEC DIS 8802-3:2002, IEEE Std. 802.3-2002.

[28] P. Mühlethaler, 802.11 et les réseaux sans fil, chapitre5. Eyrolles, 2002.

[29] IEEE Standards for Information Technology. IEEE Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation. IEEE Std. 802.11f-2003.

[30] V.Jérôme, Hybridation entre les modes ad-hoc et infrastructure dans les réseaux de type Wi-Fi, Mémoire d'Ingéniorat, Universit´e Libre de Bruxelles, 2006.

[31] Wi-Fi Protected Access, http://www.wi-fi.org/knowledge_center/wpa

[32] M. Parizeau, Introduction à la cryptographie, 2001

[33] A. MOKHTARI, La Sécurité dans les Échanges et la Sauvegarde des Données. DEA M.I.S.I. Université de Versailles. 2000 – 2001. rapStageDEA.pdf
[34] M. Riguidel, La sécurité des réseaux et des systèmes, E N S T P A R I S, 2 0 0 6 - 2 0 0 7

[35] N. Borisov, I. Goldberg, and D. Wagner, Intercepting Mobile Communications: The Insecurity of 802.11, Juillet 2001. http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

[36] W. A. Arbaugh. An inductive chosen plaintext attack against WEP/WEP2. IEEE Document 802.11-01/230, May 2001.

[37] J. R. Walker. Unsafe at any key size; an analysis of the WEP encapsulation. IEEE Document 802.11-00/362, Oct. 2000.

[38] S. Fluhrer, I. Mantin and A. Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, 2001, http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf.

[39] G. Lehembre, Sécurité Wi-Fi – WEP, WPA et WPA2, Dossier N° 1, 2006.
http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_FR.pdf

[40] Wi-Fi Protected Access 2, http://www.wi-fi.org/knowledge_center/wpa2

[41] G. Pujolle, Sécurité Wi-Fi, Chapitre 5, Groupe Eyrolles, 2004.
http://www.editions-eyrolles.com/Chapitres/9782212115284/chap5_Pujolle.pdf

[42] Arunesh Mishra and William A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard", UMIACS-TR-2002-10, University of Maryland, February 2002.

[43] J. CHEN, M. JIANG, AND Y. LIU, WIRELESS LAN SECURITY AND IEEE 802.11I, NATIONAL TSING HUA UNIVERSITY, IEEE Wireless Communications • February 2005. WC02-124-post.pdf

[44] C. He and J. C. Mitchell. Analysis of the 802.11i 4-Way Handshake. In Proceedings of the Third ACM International Workshop on Wireless Security (WiSe'04), Philadelphia, PA, October, 2004. http://byte.csc.lsu.edu/~durresi/7502/reading/p43-he.pdf

[45] C. He, J. C. Mitchell, "Security Analysis and Improvements for IEEE 802.11i," In Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSS '05), Internet Society, February 2005.

[46] S. Fogie, Cracking Wi-Fi Protected Access (WPA), Part 2.2005

[47] Aboba, B., and Simon, D. PPP EAP TLS authentication protocol. RFC 2716, October, 1999.

[48] H. Haverinen, J. Salowey, Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM), IETF RFC 4186, January 2006.

[49] J. Arkko, H. Haverinen, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), IETF RFC 4187, January 2006.

[50] Cheikhrouhou O., Laurent-Maknavicius M., Ben Jemaa M., « Nouvelle méthode d'authentification EAP-EHash », 12ème Colloque Francophone sur l'Ingénierie des Protocoles CFIP'2006, Tozeur, Tunisie, Octobre 2006.

[51] P. Funk, S. Blake-Wilson, EAP Tunneled TLS Authentication Protocol (EAP-TTLS), draft-ietf-pppext-eap-ttls-05.txt, Internet-Draft, July 2004 (expired)

[52] T. Dierks & E. Rescorla, The Transport Layer Security (TLS) Protocol, Version 1.1. RFC 4346, Avril 2006.
[53] Kwang-Hyun Baek, Sean W. Smith, David Kotz, A Survey of WPA and 802.11i RSN Authentication Protocols, November 2004

[54] W., Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[55] G., Zorn, "Microsoft PPP CHAP Extensions, Version 2", RFC 2759, January 2000.

Glossaire

1G – La téléphonie mobile de 1re Génération est analogique. Elle n'est pas conçue pour l'échange de données.

2G – La téléphonie mobile de 2e Génération est numérique et bien plus performante que la 1G. Exemples : GSM, CDMA, CDPDÉ

2.5G – Des technologies telles que le GPRS ou l'EDGE ont été conçues pour permettre la navigation sur Internet ou encore l'échange de contenu multimédia en reposant sur les réseaux de la 2G. On appelle ceci la téléphonie de génération «deux et demi ».

3G – La troisième génération de téléphonie vise des débits bien supérieurs à la 2.5G, et aspire à l'universalité. Exemples : UMTS, CDMA2000…

802.1x – Norme de l'IEEE pour le contrôle d'accès à un réseau. Le contrôle est exercé au niveau d'un port, d'un commutateur, ou pour chaque association dans un AP. Ce standard repose sur l'EAP, et l'authentification des utilisateurs est généralement réalisée par un serveur RADIUS.

802.11 – Norme connue par l'IEEE en 1997 pour les réseaux locaux sans fil, et constamment améliorée depuis. Elle définit trois couches physiques (infrarouge, FHSS et DSSS sur les fréquences de 2,4 GHz) et une couche MAC offrant de nombreuses fonctionnalités : partage du média, fragmentation, économie d'énergie, sécurité…

A

AAA – Un serveur AAA (Autorisation, Authentification, Accounting) gére l'authentification des utilisateurs, leurs autorisations et la comptabilisation de leurs connexions (voir aussi RADIUS).

Ad Hoc – Dans un réseau Wi-Fi de type Ad Hoc, les stations communiquent directement entre elles plutôt que par le biais d'un AP (voir aussi Infrastructure).

AES – Advanced Encryption Standard. Algorithme de cryptage symétrique extrêmement rapide et sûr. La norme de sécurit. WPA2 repose sur le TKIP ou l'AES.

AP – Access Point (point d'accès) : borne Wi-Fi composant l'ossature d'un réseau sans fil. En mode Infrastructure, tout utilisateur doit passer par un AP pour accéder au réseau sans fil : tout son trafic est alors relayé par l'AP auquel il est « associé ».

B

BLR – Boucle Locale Radio : ensemble de technologies permettant de relier par les ondes radio un abonné à un opérateur (téléphonie, Internet…). Parmi les technologies de BLR les plus utilisées, on compte le LMDS, le MMDS et le Wimax.

Broadcast – Trafic réseau adressé à tout le monde (voir aussi Multicast et Unicast).

BSS – Basic Service Set. Un réseau Wi-Fi composé d'un seul AP.

BSSID – Identifiant d'un BSS. Il s'agit d'un nombre de 48 bits, égal à l'adresse MAC de l'AP en mode Infrastructure, ou aléatoire en mode Ad Hoc.

C

CBC – Cipher Block Chaining. Algorithme produisant un MIC à partir d'un message, en utilisant un algorithme de cryptage par bloc. Le CBC est utilisé par le WPA/AES. Le CBC est souvent appelé le CBC-MAC (CBC-Message Authentication Code).

CCK – Complementary Code Keying. Modulation radio utilisée par le HR-DSSS.

CCM – Counter-Mode with CBC-MAC. Mode d'utilisation d'un algorithme de cryptage par bloc (ex. AES), mêlant le Counter-Mode (CM) et le CBC.

CCMP – CCM Protocol. Protocole pour le 802.11i sur AES

Cellule – Zone couverte par le signal d'un point d'accés Wi-Fi (voir aussi BSS).

CFP – Contention Free Period. Période de partage d'un média sans risque de collision. Les modes PCF et EPCF définissent une période CFP entre chaque balise.

CM – Counter-Mode : mode d'utilisation d'un algorithme de cryptage par bloc tel que l'algorithme AES. Le CM résulte en un algorithme de cryptage par flux.

Collision – On parle de «collision » lorsque deux stations émettent un paquet en même temps : généralement, les deux paquets sont alors perdus (voir aussi CSMA).

CRC – Code de Redondance Cyclique. Code d'intégrité assez simple (voir aussi MIC).

CSMA – Carrier Sense Multiple Access. Stratégie de partage d'un média trés simple : chaque station vérifie que le média soit libre pendant une durée minimale plus un temps aléatoire avant d'émettre un paquet. Ceci permet de limiter les collisions.

CSMA/CA – CSMA with Collision Avoidance. Variante du CSMA utilisée notamment par les modes DCF et EDCF du Wi-Fi : le récepteur envoie un accusé de réception (ACK) pour chaque paquet reçu : les collisions peuvent ainsi être détectées a posteriori, et les paquets concernés peuvent être réémis.

CSMA/CD – CSMA with Collision Detection. Variante du CSMA utilisée notamment par l'Ethernet. Chaque station écoute le média pendant qu'elle émet un paquet, et peut ainsi détecter si une autre station émet un paquet en même temps (collision).

CTS – Clear To Send (voir RTS/CTS).

CW – Collision Window (ou Contention Window). Durée maximale de l'attente aléatoire d'une station avant l'émission d'un paquet en mode CSMA.

D

DCF – Distributed Coordination Function. Stratégie de partage des ondes employée par défaut en Wi-Fi : elle repose sur le CSMA/CA et le mécanisme RTS/CTS.

DoS – Deny of Service. Une attaque de déni de service consiste à empêcher les utilisateurs d'accéder aux services du réseau. Le Wi-Fi est particuliérement vulnérable aux attaques DoS.

DS – Distribution System. Il s'agit du lien entre les AP d'un réseau Wi-Fi de type Infrastructure. Généralement le DS est le réseau filaire auquel sont reliés les AP, mais il peut également s'agir d'un lien sans fil (voir aussi WDS).

DSSS – Direct Sequence Spread Spectrum. Modulation radio utilisée par le 802.11b et le 802.11g. Grâce à la technique de chipping, le spectre radio occupé par le signal est étalé, ce qui permet d'atteindre des débits plus élevés et de mieux résister au bruit

E

EAP – Extensible Authentication Protocol. Protocole très générique permettant l'identification d'utilisateurs selon diverses méthodes (mot de passe, certificat, carte à puce…). Normalisé par l'IETF comme extension du protocole PPP, l'EAP est maintenant également à la base du 802.1x, lui-meme à la base du WPA.

EAPoL – EAP over LAN. Protocole défini par l'IEEE pour le 802.1x. Il permet l'échange de paquets EAP sur un réseau local (LAN).

ESS – Extended Service Set. Réseau Wi-Fi de type Infrastructure, pouvant être composé de plusieurs BSS.

ESSID – Identifiant d'un ESS, souvent noté simplement «SSID ». Il s'agit d'un nom composé au maximum de 32 caractères.

ETSI – European Telecommunications Standards Institute. Institut européen des normes de télécommunication, similaire à l'IEEE.

F

FHSS – Frequency Hopping Spread Spectrum. Modulation radio qui consiste à sauter régulièrement d'un canal d'émission à un autre. Cette technique permet de mieux résister aux interférences localisées dans le spectre. Elle a été plus ou moins abandonnée par le Wi-Fi, mais est à la base du Bluetooth et du HomeRF

Fragmentation – Lorsqu'un paquet à émettre parvient à la couche réseau Wi-Fi, il peut être découpé en plusieurs fragments si sa taille dépasse un seuil fixe. Chaque fragment est ensuite envoyé indépendamment, avec ses propres en-têtes Wi-Fi. Le paquet avant la fragmentation s'appelle le MSDU. Les fragments dotés de leur en-tête MAC s'appellent les MPDU.

G

GEK – Group Encryption Key, clé de chiffrement pour le trafic en diffusion (aussi utilisée pour l'intégrité des données dans CCMP)

GIK – Group Integrity Key, clé d'intégrité pour le trafic en diffusion (utilisé dans TKIP)

GMK – Group Master Key. En 802.11i, clé maîtresse dont est dérivée la clé GTK.

GPS – système mondial de positionnement).Système de radiorepérage qui détermine la position d'un véhicule ou d'un appareil mobile, en se servant d'une constellation de satellites en orbite autour de la Terre. Le système mondial de positionnement est une application civile du système de repérage NAVSTAR (Navigation System using Time and Ranging) mis au point par l'armée américaine. Les signaux émis par les satellites, au nombre de 24, sont captés par un appareil récepteur installé dans un mobile. Le système détermine par triangulation la position du mobile, à l'aide de données géographiques informatisées, en fonction du temps et de la distance parcourue par un des satellites en orbite

GPRS – General Packet Radio Service. L'une des premières technologies de 2.5G.

GSM – Global System for Mobile Communication. Technologie de 2G.

GTK – Group Transient Key. En 802.11i, clé dérivée de la clé GMK et servant au cryptage et contrôle d'intégrité du trafic broadcast et multicast (voir aussi PTK).

H

Hachage – Une fonction de hachage (ex. MD5) produit un nombre imprévisible à partir d'un message. Deux messages identiques donneront le même «hash », tandis que deux messages différents, meme trés proches, donneront deux hash sans lien entre eux.

Half-Duplex – Communication entre deux stations, chacune ne pouvant pas simultanément émettre et recevoir (voir aussi Full-Duplex).

Hand-over – On parle de hand-over (passer la main), en mode Infrastructure, lorsqu'une station passe d'un AP à un autre, de façon transparente pour l'utilisateur.

Hotspot – Zone d'accès à l'Internet par le Wi-Fi, en général payant.

HR-DSSS – High Rate DSSS. Version améliorée du DSSS introduite avec le 802.11b, permettant d'atteindre des débits plus élevés que le 802.11 DSSS grâce au CCK.

I

IBSS – Independent BSS. Réseau composé de plusieurs stations en mode Ad Hoc.

ICV – Integrity Check Value. Code d'intégrité du WEP.

IEEE – Institute of Electrical and Electronics Engineers. Organisation professionnelle fondé en 1963, regroupant les professionnels des télécommunications, de l'électronique, de l'électricité et de l'informatique.

IETF – Internet Engineering Task Force. Organisme informel à l'origine des principaux standards de l'Internet.

IGC – Infrastructure à Gestion de Clé. Une IGC est une organisation et des moyens techniques permettant la création, la distribution et la maintenance de clés cryptographiques, utiles pour divers services de sécurité.

Infrastructure – Dans un réseau Wi-Fi de type Infrastructure, chaque station est associée à un AP et ne communique que par son intermédiaire (voir aussi Ad Hoc).

ISO – International Organization for Standardization.
ITU – International Telecommunication Union. Organisme responsable de recommandations et de la Normalisation du téléphone et des systèmes de communication de données, pour les organisations de télécommunications publiques et privées.

K

KCK – Key Confirmation Key, clé d'intégrité utilisée pour protéger les échanges de clé.
KEK – Key Encryption Key, clé de confidentialité utilisée pour protéger les échanges de clé.

L

LAN – Local Area Network. Réseau de dimension « locale » : réseau d'entreprise, réseau familial, etc. (voir aussi PAN, MAN, WAN).
LLC – Logical Link Control. Couche réseau définie par l'IEEE (802.2), au-dessus de la couche MAC. Elle sert d'interface unique entre les couches 2 et 3 du modèle OSI.

M

MAC – Media Access Control. Couche réseau définie par l'IEEE en bas de la deuxième couche du modèle OSI. Elle gére notamment le partage du média entre plusieurs stations, et varie selon la technologie utilisée (Wi-Fi, Ethernet…).

MAC – Message Authentication Code (voir aussi MIC).

MAN – Metropolitan Area Network. Réseau de l'échelle d'un campus ou d'une ville. Il est généralement composé de multiples LAN reliés entre eux (voir aussi PAN, LAN, WAN).

MD5 – Message Digest 5. Algorithme de hachage très utilisé (voir aussi Hachage).

MIC – Message Integrity Code. Nombre calculé à partir d'un message et envoyé avec celui-ci. Le récepteur peut ainsi s'assurer que le message n'a pas été modifié.

Michael – Algorithme de contrôle d'intégrité utilisé par TKIP (voir aussi MIC).

MiM – Man in the Middle (également noté MitM). Une attaque MiM consiste pour un pirate à s'interposer entre deux stations du réseau, à leur insu, de façon à espionner leurs échanges, voire à les modifier.

MK – Master Key, clé maîtresse connue du client 802.1x et du serveur d'authentification à l'issu du processus d'authentificatio 802.1x.

MPDU – MAC Protocol Data Unit (voir Fragmentation).

MSDU – MAC Service Data Unit (voir Fragmentation).

Multicast – Trafic réseau adressé à un groupe de stations (voir aussi Broadcast et Unicast).

O

OFDM – Orthogonal Frequency Division Multiplexing. Modulation radio utilisée notamment par le 802.11a et le 802.11g. Elle consiste à diviser un canal radio en de multiples canaux, et à utiliser tous ces canaux simultanément.

OSI – Open Systems Interconnection. Connu par l'ISO, le modèle OSI définit comment les protocoles réseaux doivent être organisés en couches superposées. Bien qu'il ne soit pas utilisé tel quel, le modèle OSI reste un modèle de référence.

P

PAE – Port Access Entity, port logique 802.1x.

PAN – Personal Area Network. Réseau de trés petite taille, centré autour d'une personne. Par exemple, un PDA et un ordinateur interconnectés forment un PAN.

PCF – Point Coordination Function. Stratégie de partage des ondes définie par le 802.11 (optionnelle). Deux phases alternent sans cesse : dans la première, l'AP donne la parole

successivement à chaque station. Dans la seconde, le mode DCF est utilisé. Le PCF permet de gérer quelques aspects de la QoS, mais le 802.11e va bien plus loin.

PEAP – Protected EAP. Méthode d'authentification EAP établissant un tunnel TLS au sein duquel une autre authentification EAP est réalisée, et ainsi protégée (voir aussi TTLS).

PKI – Public Key Infrastructure (voir aussi IGC).

PMK – Pairwise Master Key. En 802.11i, clé maîtresse dont est dérivée la clé PTK.

PSK – Pre Shared Key (voir WPA-Personal).

PTK – Pairwise Transient Key. En 802.11i, clé dérivée de la clé PMK et servant au cryptage et contrôle d'intégrité du trafic unicast.

R

RADIUS – Remote Authentication Dial In User Service. Protocole de type AAA. Un réseau d'entreprise sécurisé par le WPA repose généralement sur un serveur RADIUS.

RC4 – Rivest Cipher 4 (ou Ron's Code 4). Algorithme de cryptage par flux : il produit un flux de bits pseudo aléatoires, à partir d'une clé. Ces bits sont combinés aux bits d'un message, avec l'opération XOR. Le WEP et le TKIP reposent sur RC4.

RLAN – Radio LAN. Réseau local reposant sur une technologie radio (ex. Wi-Fi).

Roaming – Un accord de roaming entre deux opérateurs permet aux clients de l'un d'utiliser le réseau de l'autre.Certains utilisent également le mot «roaming » pour parler de hand-over

RSN – Robust Security Network. Réseau Wi-Fi sécurisé par le 802.11i (voir TSN).

RSNA – Robust Security Network Association, association de sécurité utilisée dans RSN

RSN IE – Robust Security Network Information Element, champ contenant les informations RSN inclues dans les trames Probe Response et Association Request.

RTS/CTS – Request to Send/Clear to Send. Lorsqu'un paquet de données doit être envoyé, si sa taille dépasse un seuil donné (le RTS Threshold), une requete RTS est d'abord envoyée pour demander la permission. Si le récepteur autorise l'envoi du paquet, il renvoie une réponse CTS à l'émetteur. Ce mécanisme permet de réduire les collisions dues aux stations qui ne sont pas à portée les unes des autres et ne peuvent donc pas savoir si elles risquent de prendre la parole en même temps.

S

Sniffer – Enregistrer les paquets échangés entre des stations Wi-Fi dans le but de superviser (ou de pirater) le réseau.

SSID – Service Set Identifier (voir ESSID).

Station – Tout équipement capable de se connecter à un réseau (ordinateur, PDA…).

T

TK – Temporary Key, clé pour le chiffrement des données à destination d'une machine (unicast) (utilisé pour le calcul des données d'intégrité dans le protocole CCMP).

TKIP – Temporal Key Integrity Protocol. Protocole de sécurité Wi-Fi reposant sur RC4, et conçu pour résoudre tous les problémes du WEP sans avoir à changer de matériel. Le WPA repose sur TKIP. Le WPA2 repose sur TKIP ou CCMP.

TMK – Temporary MIC Key, clé pour l'authenticité des données du trafic à destination d'une machine (unicast) (utilisé dans TKIP).

TLS – Transport Layer Security. Protocole permettant de mettre en place un tunnel sécurisé entre un client et un serveur. TLS est standardisé par l'IETF, et issu du protocole SSL conçu par Netscape.

TSC – TKIP Sequence Counter, compteur anti-rejeu utilisé dans TKIP (basé sur l'IV étendu).

TSN – Transitional Security Network. Réseau Wi-Fi mixte, acceptant les stations sécurisées par le 802.11i ou le WEP. Il s'agit d'une étape de transition vers le RSN.

TTLS – Tunneled TLS. M.thode d'authentification EAP trés similaire à PEAP.

U

UIT – Organisation des Nations Unies pour les télécommunications. Fondée en 1865, elle compte quelque 180 pays membres. Son rôle est d'harmoniser le développement des télécommunications dans le monde. Le siège de l'UIT est à Genève.

Unicast – Trafic réseau adressé à une seule station (voir Broadcast et Multicast).

UWB – Ultra Wideband. Modulation radio consistant à émettre sur une trés large bande de fréquences. Â courte distance, il est possible d'atteindre des débits très élevés.

W

WAN – Wide Area Network. Réseau de dimension nationale ou mondiale, par exemple l'Internet (voir aussi PAN, LAN, WAN).

WarDriving – Promenade en voiture pour détecter des réseaux Wi-Fi.

WDS – Wireless Distribution System. Connexion sans fil entre AP (voir aussi DS).

WECA – Wireless Ethernet Compatibility Alliance (voir Wi-Fi Alliance).

WEP – Wired Equivalent Privacy. Premiére solution de sécurité du 802.11, reposant sur le RC4. Ses défauts sont nombreux et il vaut mieux passer au WPA ou WPA2.

Wi-Fi – Certification de la Wi-Fi Alliance pour les produits respectant la norme 802.11.

Wi-Fi Alliance – Association professionnelle internationale créée en 1999 afin de certifier les produits se voulant à la norme IEEE 802.11, ce qui permet d'assurer une bonne interopérabilité entre eux .

Wimax – Technologie de WMAN définie par le Wimax Forum à partir des normes IEEE 802.16 et ETSI HiperMAN.

WLAN – Wireless LAN. Réseau local sans fil (Wi-Fi, VFIRÉ). Voir RLAN.

WMAN – Wireless MAN. Réseau MAN sans fil (Wimax, BLR...).

WPA – Wireless Protected Access. Certification de la Wi-Fi Alliance pour les produits Wi-Fi compatibles avec la sécurit. TKIP définie par la norme 802.11i.

WPA-Personal – Certification pour les produits WPA que l'on peut configurer avec une clé secrète (PSK), partagée par tous les équipements du réseau, sans serveur d'authentification. On parle également de WPA/PSK.

WPA-Enterprise – Certification pour les produits WPA compatibles avec la norme 802.1x. L'architecture 802.1x implique la mise en place d'un serveur d'authentification (généralement de type RADIUS).

WPA2 – Certification de la Wi-Fi Alliance pour les produits Wi-Fi gérant la sécurité 802.11i complète, et notamment le CCMP/AES.

WPAN – Wireless PAN. Réseau PAN sans fil (Bluetooth, ZigBee...).

WWAN – Wireless WAN. Réseau WAN sans fil (2.5G, 3G, 802.20…).

X-Z

XOR – Exclusive Or. Le «ou exclusif » est une addition binaire sans retenue (1+1=0).

ZigBee – Technologie de WPAN à faible consommation électrique mais bas débit.