République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Master Recherche
en Informatique
Option
Réseaux et Systèmes Distribués
Thème

ÉTUDE, ANALYSE ET PROPOSITION D'UNE SOLUTION D'AUTHENTIFICATION ET DE GESTION DE CLÉS DU STANDARD 802.11i

---

Présenté par

M^r ***BOUGHANI*** **Rafik**
M^r ***YAHIA CHERIF*** **Fawzi**

Soutenu devant le jury composé de :

Président	M^r ***SLIMANI*** **Hachem**	**M.C.B U.Béjaia**
Rapporteur	M^eme ***ZIDANI*** **Ferroudja**	**M.A.B U.Béjaia**
Examinateur	M^r ***AISSANI*** **Sofiane**	**Enseignant (Doctorant) à l'U.Béjaia**
Examinateur	M^elle ***BOUADEM*** **Nassima**	**Enseignante (Doctorante) à l'U.Béjaia**

Promotion 2011/2012

Remerciements

On remercie dieu pour nous avoir donné du courage, de la patience, de la santé et beaucoup de volonté pour mener à terme ce mémoire de Master.

Nous tenons à remercier aussi Mme. ZIDANI Ferroudja, notre promotrice, pour sa sympathie, sa disponibilité, ses conseils et ses encouragements qui nous ont permis de mener à bien ce travail.

Nous tennons à exprimer notre gratitude aux membres de jury pour avoir accepté de juger ce travail.

Un grand merci à tous nos collègues en Master 2 et tous les enseignants du département Informatique, qui nous ont offert un environnement estudiantin extrêmement agréable.

Un merci pudique : à nos familles, pour leur soutien qui nous a poussé à chercher au fond de nous la volanté de faire toujours beaucoup plus, à nos amis et tous ceux qui ont contribué de près ou de loin à l'aboutissement de ce travail.

Dédicaces

Je dédie ce modeste travail à :

A mes parents,

A mes frères et soeurs,

A toute la famille,

A mes amis et collègues, et tous ceux qui m'ont aidé ;

A mon binôme Fawzi et sa famille.

BOUGHANI Rafik

Dédicaces

Je dédie ce modeste travail à :

A mes parents,

A mes frères et soeurs,

A toute la famille,

A mes amis et collègues, et tous ceux qui m'ont aidé ;

A mon binôme Rafik et sa famille.

YAHIA CHERIF Fawzi

Résumé

La transmission radio rend les réseaux sans fil commodes d'usage, faciles à déployer, et économiques, mais soulèvent par contre des problèmes de sécurité, dus à la nature ouverte des supports de transmission utilisés. En plus, les exigences de sécurité doivent être vérifiées notamment l'anonymat et la protection à long terme des données. 802.11i est un standard développé pour améliorer la sécurité des réseaux 802.11 au niveau MAC, en proposant une nouvelle architecture de sécurité appelée RSN (Robust 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'appuie 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 des 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. Dans ce mémoire, on a étudié le protocole 802.11i, tout en se concentrant sur la phase d'authentification et la phase de gestion de clés de ce protocole. Nous avons étudié les failles et vulnérabilités de ses dernières, et nous avons proposé de nouvelles solutions pour améliorer la sécurité de ce standard.

Mots-clés : *Cryptographie, sécurité, WiFi, 802.11i, 802.1x, EAP, 4-way handshake.*

Abstract

The Radio transmission makes the wireless networks convenient to practical use, easy to be spread, and economic. However, it raises security problems because of the open nature of the used transmission supports. In addition, the security demands should be checked especially the anonymity and the long time protection of the data. 802.11i is a standard which was developed to improve the network security 802.11 at the MAC level suggesting a new architecture of security called RSN (Robust Security Network) whose contribution is essentially in the use of the standard of 802.1x for the authentication and an access control, the four way handshake for the generation of the fresh keys of the session and the protocol AES (Advanced Encryption Standard) for encryption. In RSN, one of the methods of authentication which supports the 802.1x/EAP is carried out to establish a master key (PMK) between the station and the authentication server. The latter will be ; then, used in the management procedure of the keys (4-way handshake) to provide a mutual authentication between the access point and the client, and the generation of temporary keys of sessions. In this dissertation, we studied the protocol of 802.11i, concentrating on the authentication phase and the key management phase of this protocol. We studied the flaws and the vulnerabilities of these lasts, and we have proposed new solutions to enhance the security of the standard.

Keywords : *Cryptography, security, WiFi, 802.11i, 802.1x, EAP, 4-way handshake.*

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

AAD	**A**dditional **A**uthentication **D**ata
AES	**A**dvanced **E**ncryption **S**ystem
AKA	**A**uthentication and **K**ey **A**greement
AP	**A**ccess **P**oint
AVP	**A**ttribute-**V**alues **P**airs
BC	**B**oot **C**ounter
BLR	**B**oucle **L**ocale **R**adio
BSS	**B**asic **S**ervice **S**et
BSSID	**B**asic **S**ervice **S**et **ID**entifier
CBC	**C**ipher **B**lock **C**haining
CBC-MAC	**C**ipher **B**lock **C**haining **M**essage **A**uthentication **C**ode
CCM	**C**ounter Mode with **C**ipher Block Chaining **M**essage Authentication Code
CCMP	**C**ounter Mode with **C**ipher Block Chaining **M**essage Authentication Code **P**rotocol
CHAP	**C**hallenge **H**andshake **A**uthentication **P**rotocol
CPU	**C**entral **P**rocessing **U**nit
CRC	**C**yclic **R**edundancy **C**hecksum
CTR	**C**oun**T**e**R** Mode
DA	**D**estination **A**ddress
DoS	**D**enial **o**f **S**ervice
EAP	**E**xtensible **A**uthentication **P**rotocol
EAPoL	**E**xtensible **A**uthentication **P**rotocol **o**ver **L**AN
ETSI	**E**uropean **T**elecommunications **S**tandards **I**nstitute
FAST	**F**lexible **A**uthentication via **Se**cure **T**unneling
GEK	**G**roup **E**ncryption **K**ey
GHz	**G**ega **H**ert**z**

GIK	**G**roup **I**ntegrity **K**ey
GMK	**G**roup **M**aster **K**ey
GPRS	**G**eneral **P**acket **R**adio **S**ervice
GSM	**G**lobal **S**ytem for **M**obile communications
GTK	**G**roup **T**emporal **K**ey
GTKSA	**G**roup **T**emporal **K**ey **S**ecurity **A**ssociation
HIPERLAN	**HI**gh **PE**rformance **R**adio **L**ocal **A**rea **N**etwork
HomeRF	**H**ome **R**adio **F**requency
HP	**H**ewlett **P**ackard
IBM	**I**nternational **B**usiness **M**achines
IBSS	**I**ndependent **B**asic **S**ervice **S**et
ICV	**I**ntegrity **C**heck **V**alue
IE	**I**nformation **E**lement
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
IETF	**I**nternet **E**ngineering **T**ask **F**orce
IPv6	**I**nternet **P**rotocol **v**ersion **6**
ISM	**I**ndustrial, **S**cience and **M**edicine
ISO	**I**nternational **S**tandardization **O**rganization
IV	**I**nitialisation **V**ector
Kbps	**K**ilo **b**it **p**er **s**econd
KCK	**K**ey **C**onfirmation **K**ey
KEK	**K**ey **E**ncryption **K**ey
KHz	**K**ilo **H**ert**z**
LAN	**L**ocal **A**rea **N**etwork
LEAP	**L**ightweight **E**xtensible **A**uthentication **P**rotocol
MAC	**M**edium **A**ccess **C**ontrol
Mbps	**M**ega **b**it **p**er **s**econd
MD5	**M**essage-**D**igest algorithm **5**
MHz	**M**ega **H**ert**z**
MIC	**M**essage **I**ntegrity **C**ode
MITM	**M**an-**I**n-**T**he-**M**iddle
MK	**M**aster **K**ey
MPDU	**M**AC **P**rotocol **D**ata **U**nit
MS-CHAPv2	**M**icro**s**oft **C**hallenge **H**andshake **A**uthentication **P**rotocol **V**ersion **2**
MSDU	**M**AC **S**ervice **D**ata **U**nit)
OFDM	**O**rthogonal **F**requency **D**ivision **M**ultiplexing
OLSR	**O**ptimized **L**ink **S**tate **R**outing **P**rotocol

OSI	**O**pen **S**ystem **I**nterconnection
PAC	**P**rotected **A**ccess **C**redentials
PAE	**P**ort **A**ccess **E**ntity
PC	**P**ersonal **C**omputer
PDA	**P**ersonnal **D**igital **A**ssistant
PEAP	**P**rotected **E**xtensible **A**uthentication **P**rotocol
PKI	**P**ublic **K**ey **I**nfrastructure
PMK	**P**airwise **M**aster **K**ey
PMKSA	**P**airwise **M**aster **K**ey **S**ecurity **A**ssociation
PN	**P**acket **N**umber
PPP	**P**oint to **P**oint **P**rotocol
PRF	**P**seudo **R**andom **F**unction
PSK	**P**re-**S**hared **K**ey
PTK	**P**airwise **T**ransient **K**ey
PTKSA	**P**airwise **T**ransient **K**ey **S**ecurity **A**ssociation
QoS	**Q**uality **o**f **S**ervice
RADIUS	**R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice
RC4	**R**ivest **C**ypher **4**
RFC	**R**equest **F**or **C**omments
RSA	**R**ivest **S**hamir **A**delman
RSN	**R**obust **S**ecurity **N**etwork
RSNA	**R**obust **N**etwork **S**ecurity **A**ssociation
SA	**S**ource **A**ddress
SHA-1	**S**ecure **H**ash **A**lgorithm **1**
SID	**S**tation **ID**entifier
SIM	**S**ubscriber **I**dentity **M**odules
SMS	**S**hort **M**essage **S**ervice
SSID	**S**ervice **S**et **ID**entifier
STA	**STA**tion
TC	**T**ime **C**ounter
TDMA	**T**ime **D**ivision **M**ultiple **A**ccess
TK	**T**emporary **K**ey
TKIP	**T**emporal **K**ey **I**ntegrity **P**rotocol
TLS	**T**ransport **L**ayer **S**ecurity
TMK	**T**emporary **M**IC **K**ey
TMK	**T**ransient **M**aster **K**ey
TSC	**T**KIP **S**equence **C**ounter

TTAK	**T**KIP-mixed **T**ransmit **A**dress and **K**ey
TTLS	**T**unneled **T**ransport **L**ayer **S**ecurity
UMTS	**U**niversal **M**obile **T**elecommunications **S**ystem
USB	**U**niversal **S**erial **B**us
VoWLAN	**V**oice **o**ver **W**ireless **L**ocal **A**rea **N**etwork
W-CDMA	**W**ideband-**C**ode **D**ivision **M**ultiple **A**ccess
WECA	**W**ireless **E**thernet **C**ompatibility **A**lliance
WEP	**W**ired **E**quivalent **P**rivacy
Wi-Fi	**W**ireless **F**idelity
WIMAX	**W**orldwide **I**nteroperability for **M**icrowave **A**ccess
WLAN	**W**ireless **L**ocal **A**rea **N**etwork
WMAN	**W**ireless **M**etropolitan **A**rea **N**etwork
WPA	**W**i-Fi **P**rotected **A**ccess
WPAN	**W**ireless **P**ersonal **A**rea **N**etwork
WPA-PSK	**W**i-Fi **P**rotected **A**ccess-**P**re**S**hared **K**ey
WWAN	**W**ireless **W**ide **A**rea **N**etwork

LISTE DES TABLEAUX

TABLE DES FIGURES

INTRODUCTION GÉNÉRALE

Les réseaux sans fil (Wireless Networks) ont connu une véritable explosion depuis la fin des années 90, aussi bien dans la vie de tous les jours pour se connecter à l'internet que dans le monde de la recherche. Ils sont devenus populaires, en raison de leur mobilité, d'une grande disponibilité du matériels, avec une plus grande vitesse de transmission de données et à moindre coût. Ils permettent l'accès aux ressources du réseau sans avoir recours à utiliser une liaison câblée.

Le 802.11 est l'une des normes des réseaux locaux sans fil WLAN fixée par l'IEEE. Avec leurs extensions, ils ont été conçus pour offrir une transmission fiable de données sous diverses conditions environnementales défavorables. Récemment, le 802.11 est devenu l'une des technologies d'accès au réseau local sans fil.

Avec l'accéptation répandue et la mise en œuvre des réseaux 802.11, la préoccupation vient concernant la sécurité de ces réseaux, la transmission de données via une interface d'air plutôt qu'un conduit physique plus sûr, expose la sécurité du réseau à des vulnérabilités.

Le 802.11i est un amendement à la norme IEEE 802.11 ratifié en 2004, il est amené pour renforcer la sécurité dans les réseaux sans fil 802.11 (Wifi). Le 802.11i a introduit le concept du réseau de sécurité robuste RSN (Robust Security Network). Une RSN est définie comme un réseau de sécurité sans fil, qui autorise seulement la création d'associations RSN (RSNA). Une RSNA (Robust security Network Association) est une connexion logique entre entités communicantes établie à travers un schéma de gestion de clé appelé 4-way Handshake : un protocole qui s'assure que les entités partagent une même clé PMK (Pairwise Master Key), synchronise l'installation des clés temporaires et confirme la sélection et la configuration des protocoles de confidentialité des données et d'intégrité. La PMK est obtenue

du standard 802.1x lors de la phase d'authentification EAP, et qui précède le 4-way Handshake.

Le protocole 802.1x vise à fournir une authentification forte, ensuite une gestion et distribution de clé. Toutefois, il souffre de quelques problèmes de sécurité liés à ses spécifications, comme l'attaque man-in-the-middle, détournement de session et déni de service (DoS). En plus, d'autres attaques sont possibles, car EAP n'inclue aucune information d'intégrité à ses paquets transportés ; par exemple, à la fin du processus d'authentification, le point d'accès envoi un message de notification EAP pour indiquer le succès ou l'échec de ce processus. Le fait que cette notification n'inclue aucune protection d'intégrité de données, un attaquant peut facilement remplacer un EAP-échec en EAP-Succès et bloque l'accès au réseau WLAN.

D'autres part, He et Mitchell [49] ont démontré une attaque de déni de service contre le 4-way Handshake de 802.11i. L'attaque peut être réalisée en se passant pour un point d'accès, en composant des Message-1 et en les envoyant à la station. Un attaquant envoi un Message-1 forgé à cette station après le Message-2, la station est obligée de calculer une nouvelle PTK correspondant au nonce du nouveau message reçu, causant ainsi un blocage de 4-way Handshake.

L'objectif de ce travail est d'étudier et d'analyser la procédure d'authentification et de gestion de clé du standard de sécurité 802.11i, tout en se concentrant sur le mode infrastructure. Des différents travaux connexes basés sur ce sujet ont été menés par d'autres, et seront présentés et discutés, et ceci dans le but de proposer des nouvelles solutions d'amélioration pour renforcer la résistance de 802.11i aux diverses attaques.

Ce mémoire est organisé en quatre chapitres

Dans le ***chapitre 1***, nous présentons une description des réseaux sans fil : les motivations pour le sans fil, leurs classifications, les principales caractéristiques de ces réseaux. Nous présentons le standard 802.11 et nous terminons par la problématique des réseaux sans fil.

Dans le ***chapitre 2***, nous définissons quelques notions de base sur la sécurité, et quelques solutions et mécanismes utilisés pour sécuriser les réseaux 802.11. Nous présentons le standard 802.11i et nous clôturons ce chapitre par une analyse des vulnérabilités de ce standard.

Le ***chapitre 3*** présente un état de l'art sur les solutions d'authentification et de gestion de clé, basées sur les méthodes EAP et le 4-way Handshake, il présente une analyse des principales solutions proposées et nous les avons discutés pour ouvrir la voie vers le développement de

nouvelles solutions d'amélioration.

Le ***chapitre 4*** concerne notre contribution, nous allons présenter nos solutions proposées pour améliorer la sécurité de 802.11i, et nous allons analyser ces approches.

Enfin, nous concluons ce travail et nous dégageons quelques perspectives du travail.

CHAPITRE 1

LES RÉSEAUX SANS FIL ET LE STANDARD IEEE 802.11

1.1 Introduction

En raison de leur facilité de déploiement et de leur coût relativement faible, les réseaux sans fil sont de plus en plus utilisés, ils permettent de se connecter à l'Internet facilement et rapidement tout en se déplaçant. Les réseaux sans fil sont basés sur une liaison utilisant des ondes radioélectriques (Radio et Infrarouges), en lieu et place des câbles habituels. De ce fait, les réseaux sans fil sont les plus célèbres et les plus populaires.

Dans ce chapitre, nous aborderons l'intérêt des réseaux sans fil, les différentes normes et standards, les différentes technologies existantes de ces réseaux, et on termine par citer leurs avantages et inconvénients.

1.2 Définition d'un réseau sans fil

Un réseau sans fil (en anglais *Wireless network*) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux (ordinateur portable, assistants personnels, etc.) peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité".

Les réseaux sans fil sont basés sur une liaison utilisant des ondes hertziennes. Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée, ainsi que le

débit et la portée des transmissions. Les réseaux sans fil permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres. De plus, l'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes, comme c'est le cas avec les réseaux filaires (creusement de tranchées pour acheminer les câbles, équipements des bâtiments en câblage, goulottes et connecteurs), ce qui a valu un développement rapide de ce type de technologies [01].

1.3 Les motivations pour le sans fil

À l'apparition des réseaux sans fil à la fin des années 90, il est indiqué que leur but est de "fournir une connectivité sans fil aux machines automatiques, aux équipements, ou aux stations qui requièrent un déploiement rapide, pouvant être portables ou même dans la main, ou montés à bord de véhicules mobiles dans une zone délimitée". En effet, ces derniers font actuellement l'objet d'importants travaux de développement en raison de la flexibilité de leurs interfaces, qui permet à un utilisateur de se déplacer librement dans son entreprise ou dans son domicile tout en restant connecté. Ils sont dotés de capacités leur permettant de s'organiser et de se configurer de manière souple et, par conséquent, de se déployer rapidement.

La croissance continue du développement des technologies sans fil et des ordinateurs portables promet un avenir florissant pour les réseaux locaux sans fil WLANs (Wireless Local Area Networks), en particulier les systèmes IEEE 802.11 qui permettent d'atteindre des débits de plus de 500 Mbps avec la norme 802.11n.

Les réseaux sans fils constituent avant tout une alternative aux réseaux câblés. Leur compatibilité avec les réseaux câblés permet également de les ajouter comme extensions. Plusieurs facteurs ont poussé en puissance l'évolution de ce type de réseau, parmi lesquels nous pouvons citer :

- Utilisation croissante des terminaux portables en milieu industriel et logistique ;
- Besoin d'un accès permanent des populations nomades au système d'information de l'entreprise ;
- Réaliser des installations temporaires ;
- Réduire les coûts d'installation d'un réseau ;
- Mettre en place des réseaux en un temps très court ;
- Eviter le câblage de locaux, de liaisons inter-bâtiments ;

1.4 Classification des réseaux sans fil

Les normes dites « sans fil », la norme 802.11 en particulier, facilitent et réduisent le coût de connexion pour les réseaux de grande taille. Avec peu de matériel et un peu d'organisation, de grandes quantités d'informations peuvent maintenant circuler sur plusieurs centaines de mètres, sans avoir recours à une compagnie de téléphone ou de câblage. Ces technologies peuvent être classées en quatre parties (voir figure 1.1) :

- Les réseaux personnels sans fil (WPAN) ;
- Les réseaux locaux sans fil (WLAN) ;
- Les réseaux métropolitains sans fil (WMAN) ;
- Les larges réseaux sans fil (WWAN).

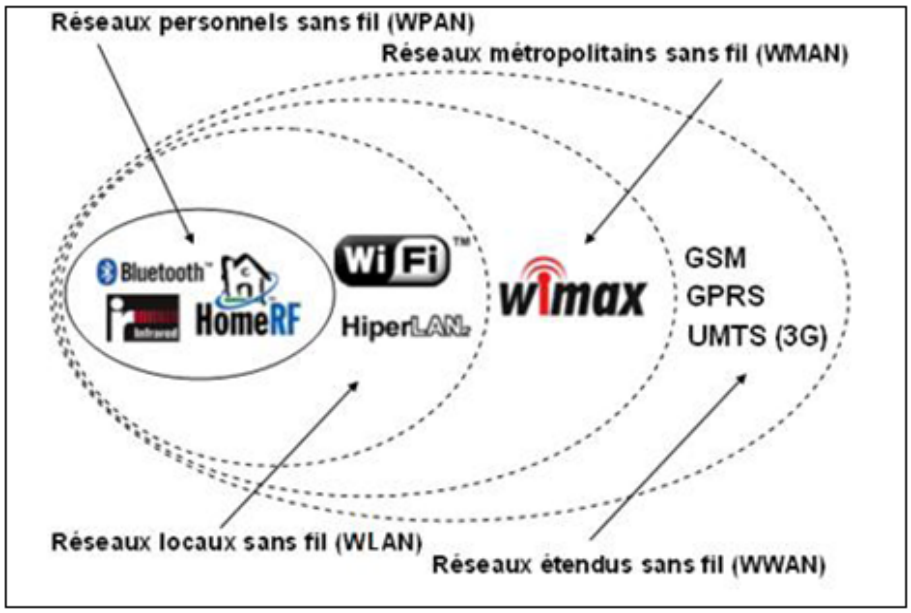

FIGURE 1.1 – Catégories des réseaux sans fil [01].

1.4.1 Réseaux personnels sans fil

Le groupe IEEE 802.15 intitulé WPAN (Wireless Personal Area Network), a été mis en place en Mars 1999, dans le but de réfléchir aux réseaux hertziens d'une portée d'une dizaine de mètres, avec pour objectif de réaliser des connexions entre les différents appareils d'un même utilisateur ou de plusieurs utilisateurs. Ce type de réseau peut interconnecter un PC portable, un téléphone portable, un Personal Digital Assistant (PDA) ou tout autre terminal de ce type [02]. Il existe plusieurs technologies utilisées pour les WPAN :

1.4.1.1 Bluetooth

Nom commercial de la norme IEEE 802.15.1, le Bluetooth est aujourd'hui présent dans de nombreux dispositifs. Malgré un débit de 1 Mbps 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, PDA, ...). La norme IEEE 802.15.3 (Bluetooth 2) est une évolution de la norme Bluetooth, permettant des débits plus rapides [03].

1.4.1.2 HomeRF

HomeRF est un standard développé en 1998 par le « Home Radio Frequency Working Group », consortium qui comprenait à l'origine Compaq, IBM, HP, Intel et Microsoft. Ce standard utilise la bande de fréquences proche de 2,4 GHz et offre un débit théorique de 1,6 Mbps partagé entre tous les utilisateurs connectés. Sa portée varie de 50 à 100 mètres. HomeRF est un des réseaux les plus perfectionnés, de part sa modulation et sa qualité de service [04].

1.4.1.3 ZigBee

Le ZigBee, définit par la ZigBee Alliance, est une technologie un peu similaire au Blue-Tooth : elle repose sur les ondes radio de 2,4 GHz, et son rôle est également de connecter des équipements entre eux, à faible distance. Toutefois, le ZigBee n'offre qu'un débit assez faible : 20 ou 250 Kbps. Son intérêt réside dans sa grande simplicité, son faible coût et sa consommation électrique extrêmement basse. Ceci le rend tout à fait adapté pour un grand nombre d'applications, telles que la connexion d'un clavier sans fil à un ordinateur ou l'ouverture d'une porte de garage. Le ZigBee n'est cependant pas conçu pour réaliser un véritable réseau sans fil [05].

1.4.1.4 Infrarouge

L'infrarouge est utilisé depuis de nombreuses années pour la communication direct entre deux équipements proches l'un de l'autre, tel que la télécommande et la télévision. Cependant, ces ondes ne sont pas capables de traverser les obstacles, et la puissance du signal se dissipe rapidement : la porté est donc faible. A courte distance, les débits peuvent toutefois être assez élevés [05].

1.4.2 Réseaux locaux sans fil

Les « Wireless Local Area Network » alias WLAN ou Réseaux locaux sans fil cherchent à offrir les mêmes prestations que les LANs d'entreprises, avec l'avantage de la suppression du câblage et le déplacement à l'intérieur d'un immeuble ou même l'extérieur, dans certaines zones, sans interruption de la session en cours. Plusieurs spécifications de WLAN ont été développées, nous citons dans se qui suit les deux principales : le WiFi et Hiperlan [08].

1.4.2.1 WiFi (IEEE 802.11)

Le WiFi (Wireless Fidelity) est un standard international décrivant les caractéristiques d'un réseau local sans fil WLAN, il est soutenu par l'alliance WECA (*Wireless Ethernet Compatibility Alliance*).

Grâce au WiFi, il est possible de créer des réseaux locaux sans fils à haut débit pour peu que l'ordinateur à connecter ne soit pas trop loin d'un point d'accès. Dans la pratique, le WiFi permet de relier des ordinateurs portables, des ordinateurs de bureau, des assistants personnels (PDA), ou tout type de périphérique à une liaison haut débit (supérieur à 11 Mbps) sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres) à plusieurs centaines de mètres en environnement ouvert [01].

Les réseaux Wi-Fi proviennent de la norme IEEE 802.11, qui définie une architecture cellulaire. Cette norme est le sujet de notre étude et elle sera détaillée dans la prochaine section 1.5.

1.4.2.2 HiperLAN

La technologie HiperLan (High Performance LAN) a été développée par l'ETSI(European Telecommunication Standards Institute), un organisme européen semblable à l'IEEE(Institute of Electronical and Electronical Engineers). Cette technologie, très proche de WiFi, n'a pas connu le succès, en grande partie du fait de l'écrasante avance commercial du WiFi. En outre, l'IEEE et l'ETSI n'ont pas réussi à se mettre d'accord pour permettre l'interopérabilité entre l'HiperLAN et le WiFi. L'HiperLAN/1 permet d'atteindre un débit de 20 Mbps et l'HiperLAN/2 monte à 54 Mbps. Les deux fonctionnent sur la bande de fréquence 5 GHz, et offre une portée similaire au WiFi [05].

1.4.3 Réseaux métropolitains sans fil

Les WMAN (Wireless Metropolitan Area Network)sont aussi connus sous le nom de Boucle Locale Radio (BLR), utilisés pour déployer des réseaux plus distants. Dans ce système, une antenne est fixée à proximité des zones d'habitation pour diffuser l'information vers des

antennes plus petites, installées aux sommets des immeubles, tout comme les antennes de télévision.

Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbps pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication [01].

1.4.3.1 WiMAX

Le WlMAX (Worldwide Interoperability for Microwave Access) est le consortium qui est chargé de la promotion des technologies de réseau sans fil métropolitains IEEE 802.16 et ETSI HiperMAN. Il prône la convergence de ces deux standards pour une technologie unique et interopérable. A ce titre, le consortium WiMAX a créer le label « WiMAX », qui certifie que l'équipement labellisé est approuvé selon les critères définis par le consortium, et qu'il est compatible avec les autres équipements labellisé, quelque soit le fabricant du matériel. De part leurs concepteurs communs, les normes HiperMAN et 802.16 sont très semblables [06].

1.4.4 Réseaux étendus sans fil

Les WWAN (Wireless Wide Area Network) connus aussi sous le nom des réseaux cellulaires, ce sont les réseaux sans fil les plus étendus permettant de relier des téléphones mobiles. Le principe général du modèle consiste à partager une zone géographique en un certain nombre de sous zones, appelées cellules. Les cellules sont généralement organisées sous forme hexagonale. Par la suite, il faut affecter une bande de fréquences à chacune des cellules pour éviter le problème d'interférence des signaux. Le mécanisme est simple, il suffit d'attribuer des fréquences différentes aux cellules adjacentes, mais il faut aussi utiliser un minimum de bande de fréquences [01]. Les principales technologies sont les suivantes :

1.4.4.1 GSM

Le GSM (Global Sytem for Mobile communications) est le système qui a permis l'accès à la téléphonie mobile grand public. Son débit relativement faible de 9,6 kbps le cantonne à des services de voix, même s'il a également popularisé le SMS (Short Message Service). Classiquement, dans le réseau GSM, les différents utilisateurs communiquent à tour de rôle, ils ont donc un slot de temps réservé : c'est la technique d'accès multiple à répartition dans le temps (TDMA : Time Division with Multiple Access). De plus, les utilisateurs communiquent non pas sur une fréquence fixe, mais sur plusieurs fréquences, car le GSM dispose de 124 fréquences porteuses de 200 kHz chacune, totalisant une bande de 25 MHz. À chaque slot correspond une fréquence : c'est la technique de saut de fréquences, pour limiter les erreurs de transmission [07].

1.4.4.2 GPRS

Les limitations en termes de débit du GSM ont conduit les professionnels à adopter de nouvelles techniques optimisant les infrastructures existantes, tout en minimisant le nombre de nouveaux équipements à installer pour développer le service de transmission de données.

Dans ce contexte s'est développé le GPRS (General Packet Ratio Service), qui introduit la communication par paquets pour les données, dérivé du modèle de communication IP (Internet Protocol). À la différence du GSM, le GPRS ne réserve pas de slots de temps par utilisateurs de manière fixe, au contraire, plusieurs de ces slots peuvent être alloués à un mobile selon la disponibilité de la BS (Base Station). L'optimisation permet d'atteindre des débits maximums réels de 50 Kbps.

Le but de cette nouvelle technologie est de permettre la transmission de données dans des conditions suffisantes (pour permettre d'accéder à Internet depuis son terminal sans subir les temps de chargement des pages Web). Le GPRS s'appuie sur une nouvelle infrastructure réseau qui prend en charge l'acheminement des données les plus volumineuses. Elle fonctionne donc en parallèle du réseau GSM classique. En conséquence, la voix conserve le mode de transmission GSM. Cette nouvelle architecture mixte GSM et GPRS est également appelée 2.5G au sens où elle améliore la 2G existante sans toutefois bouleverser son infrastructure [07].

1.4.4.3 UMTS

L'UMTS (Universal Mobile Telecommunication System) est un réseau mobile de troisième génération capable d'offrir des bénéfices significatifs à l'utilisateur en terme de services à valeur ajoutée, tels que l'accès Internet à haute vitesse, le téléchargement de fichiers (audio et vidéo) ou alors la visiophonie.

L'UMTS se base principalement sur la technique d'accès multiple large bande W-CDMA(Wideband-Code Division Multiple Access) pour y offrir ce type de service. Le système universel UMTS a été choisi dans le but de faire une distinction avec les systèmes de première et de deuxième génération, qui sont considérés comme des systèmes axés principalement sur le service de la voix.

Le réseau UMTS repose sur une architecture flexible et modulaire. Cette architecture n'est associée ni à une technique d'accès radio, ni à un ensemble prédéfini de services, ce qui assure sa compatibilité avec d'autres réseaux mobiles de deuxième et troisième génération et garantit son évolution. [07].

1.5 Le standard IEEE 802.11

1.5.1 Généralités

La première version de la norme IEEE 802.11 est définie en 1997. Des transmissions infrarouges étaient envisagées, les versions les plus récentes du standard sur la base desquelles sont construites l'essentiel des cartes d'interface commercialisées, s'adressent principalement à des transmissions radiofréquences. Pour définir cette norme, les concepteurs ont pris en considération les points suivants :

- Robustesse et simplicité de la technologie contre les défauts de communication, afin de pouvoir transmettre dans les meilleures conditions, tenant compte des considérations que le canal de transmission, en l'occurrence l'air, n'est pas aussi fiable que le câble, et qu'il est plus difficile à gérer. Ces caractéristiques ont été vérifiées par l'utilisation d'une approche distribuée du protocole de la couche MAC (Medium Acess Control).
- Utilisation du WLAN mondialement. C'est-à-dire le respect des différentes règles en usage dans les différents pays du monde.
- Totale compatibilité avec les anciens produits et les produits actuels, qui composent les réseaux LAN. C'est-à-dire que le passage du WLAN au LAN et vice-versa devra être transparent à l'utilisateur.
- Une sécurité acceptable pour le passage de l'information dans l'air.

Cette technologie très intéressante pourra prendre la relève des LANs au sein des entreprises, mais le principal problème vient de l'insécurité des échanges à travers les ondes radio qui propagent dans l'air. [08, 09]

1.5.2 La famille IEEE 802.11 et les standards 802.11

Le 802.11 est issu de la famille 802, qui est une série de spécifications pour les réseaux locaux. La figure 1.2 montre la relation entre les différents composants de la famille 802 et leurs emplacements dans le modèle OSI. Comme les spécifications 802, le standards IEEE 802.11 couvre les deux couches inferieures du modèle OSI (Open System Interconnexion) : la couche liaison de donnée et la couche physique. La couche MAC définit un ensemble de règles permettant d'accéder au médium et d'envoyer des données, les détails de la réception et de la transmission, sont traités au niveau de la couche physique. L'une des caractéristiques essentielles est qu'il définit une couche MAC commune à toutes les couches physiques. Ainsi différentes couches physiques peuvent être développées sans qu'il soit nécessaire de modifier le protocole d'accès au réseau. [10, 11]

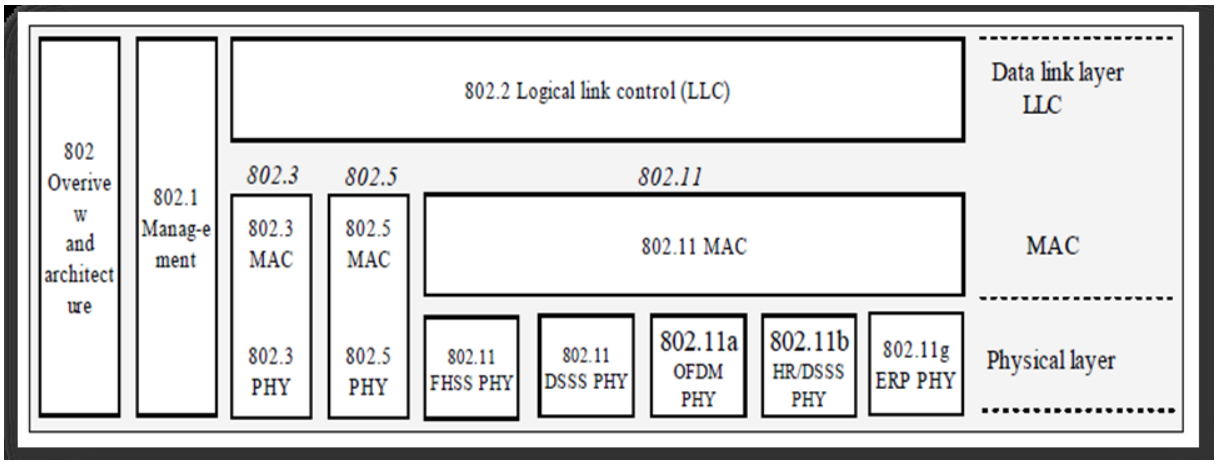

FIGURE 1.2 – Famille IEEE 802.11 [10].

1.5.3 Les normes IEEE 802.11

Depuis la première version de la norme 802.11, de nombreuses améliorations ont été apportées à cette norme initiale (avec un débit de 1 ou 2 Mbps), afin d'optimiser le débit (comme c'est le cas des améliorations apportés a la couche physique à savoir 802.11 a/b/g/n) ou bien préciser des éléments afin d'assurer une meilleure sécurité, ou une meilleure interopérabilité. Les extensions de la norme initiale sont :

- **802.11 - version 1999 :**Utilise la bande ISM (Industrial, Science and Medicine) des 2,4 GHz avec toujours des débits atteignant 2 Mbps. La bande de fréquences utilisées est partagée avec d'autres types de réseaux sans fil (Bluetooth en particulier) ainsi que de diverses applications des radios fréquences. [11]
- **802.11b :**Elle propose un débit théorique de 11 Mbps (environ 6 Mbps réels) avec une porté pouvant aller jusqu'à 300 mètre dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2,4GHz. [10]
- **802.11a :**Elle propose un débit théorique de 54Mbps (environ 30 Mbps effectifs) sur la bande des fréquences des 5GHz. Elle est non compatible avec la norme 802.11g. [12]
- **802.11g :**Elle propose un débit théorique de 54 Mbps (30 Mbps réels) sur la bande de fréquence des 2,4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que les matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b. [10]
- **802.11n :**Propose un débit de 540 Mbps de 50 mètres environ. Elle propose l'utilisation de deux bandes de fréquences 2,4 GHz (comme 802.11g) et 5 GHz (comme 802.11a). Comme 802.11g, cette norme reste compatible avec 802.11b. De plus, elle reprend les concepts de 802.11e pour la gestion de la Qualité de Service, de 802.11i pour la sécurité et de 802.11f pour la gestion des Handover. Cette norme a été ratifiée le 11 Septembre 2009 [06].

- **802.11c :**Elle apporte quelques précisions sur le fonctionnement d'un AP (Access Point) connecté à un réseau filaire. Ces précisions sont surtout utiles pour les constructeurs de matériels Wi-Fi ; et il n'est pas nécessaire de s'en soucier davantage [03].
- **802.11d :**L'objectif de cette extension est l'utilisation à l'échelle internationale des normes 802.11. Elle permet aux différents équipements d'ajuster automatiquement la bande de fréquence entre un client et un point d'accès, afin de s'adapter aux réglementations locales du pays [12].
- **802.11e :**C'est la norme de qualité de service (QoS) au niveau de la couche liaison de données. Elle permet de définir les besoins des différents paquets en termes de bande passante et de délai de transmission. La QoS est un point important, en particulier pour les applications multimédias (Voix/Téléphone *Voice over WLAN*, Vidéo,etc.). Elle s'applique sur la 802.11 a, b et g [12]
- **802.11f :**Cette norme est une recommandation à l'intention des vendeurs des points 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, quelque soit les marques des points d'accès présent dans l'infrastructure réseau. Cette possibilité est appelée roaming [10].
- **802.11h :**Elle vise à rapprocher la norme 802.11 du standard européens (HyperLAN/2) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie [10].
- **802.11i :**Le but de la norme 802.11i est d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuis sur l'Advanced Encryption System (AES) [13], et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g [10].
- **802.11j :**Propose une couche physique spécifique pour satisfaire à la réglementation japonaise. Très proche de 802.11a (OFDM (Orthogonal Frequency Division Multiplexing), 54 Mbps, etc.), elle travaille dans la bande 4,9 GHz - 5 GHz [06].
- **802.11k :**La norme 802.11k permet aux appareils compatibles de faire des mesures de signaux complètes pour améliorer l'efficacité des communications. Les avantages sont multiples tels que l'administration à distance de la couverture réseau, ou une amélioration du roaming automatique via des « site report » [14].
- **802.11s :**Propose une extension à la méthode d'accès au medium 802.11, ainsi qu'une méthode de routage pour les réseaux ad hoc de type Mech (réseau ad hoc maillés). La diffusion des routes est assurée par une méthode d'inondation et un algorithme très proche d'OLSR (Optimized Link State Routing Protocol) [06].
- **802.11r :**Elle a été élaborée de telle manière à utiliser des signaux infrarouges. Cette norme est désormais dépassée techniquement [10].

1.5.4 Topologies

Le réseau sans fil utilisant la norme 802.11 peut être déployé de deux manières différentes : Avec infrastructure ou sans infrastructure (mode Ad Hoc).

1.5.4.1 Réseau WLAN avec infrastructure

En mode Infrastructure, chaque station se connecte à un Point d'accès (AP) via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situées dans sa zone de couverture est appelé BSS pour « Basic Service Set » et constitue une cellule. Chaque BSS est identifié par un BSSID (BSS IDentifier), un identifiant de 6 octets (48 bits). Dans le mode infrastructure, le BSSID correspond à l'adresse MAC du point d'accès. Lorsque plusieurs points d'accès sont

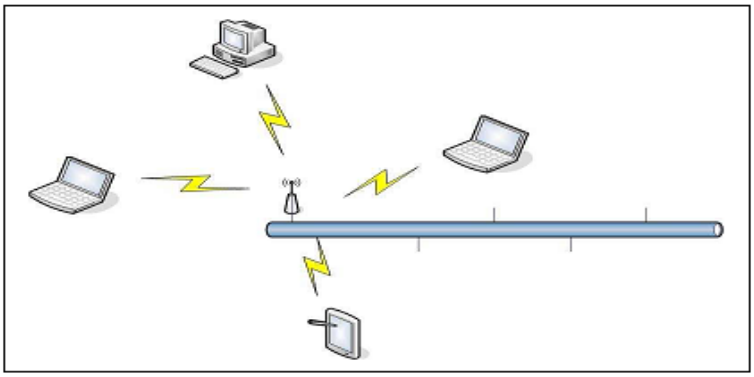

FIGURE 1.3 – Mode infrastructure avec un seul AP [14].

reliés entre eux (plusieurs BSS) par une liaison, ils forment un système de distribution (noté DS pour Distribution System). Celui-ci constitue un « Extended Service Set ». Le système de distribution (DS) peut être aussi bien un réseau filaire qu'un réseau sans fil [14], comme le montre la Figure 1.4.

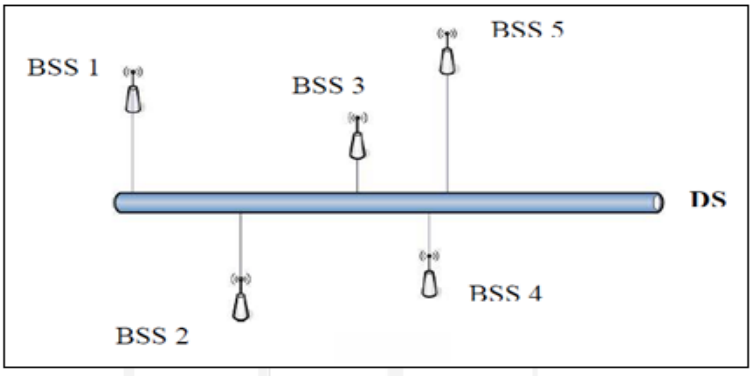

FIGURE 1.4 – Mode infrastructure avec plusieurs AP [14].

1.5.4.2 Réseau WLAN sans infrastructure

En mode Ad Hoc, les stations sans fil se connectent les unes aux autres afin de constituer un réseau point à point (peer to peer en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de routeur (voir la figure 4.3). L'ensemble formé par les différentes stations est appelé IBSS pour « independant basic service set ». Un IBSS est un réseau sans-fil constitué au minimum de deux stations et n'utilisant pas de point d'accès. L'IBSS constitue donc un réseau provisoire permettant à des personnes géographiquement proches d'échanger des données. Il est identifié par un Service Set IDentifier [14].

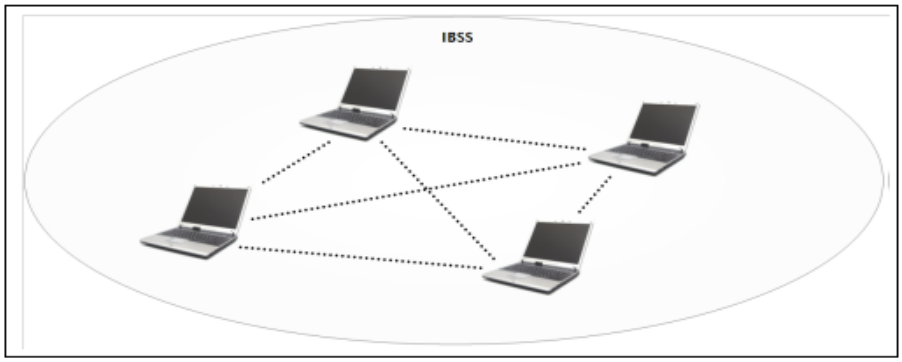

FIGURE 1.5 – Mode Ad Hoc [15].

1.6 Les avantages et les incovénients des réseaux sans fil

Voici les principaux avantages et inconvénients à déployer un réseau sans fil :

1.6.1 Les avantages des réseaux sans fil

Financier

Le réseau sans fil permet d'éviter l'obligation d'un câblage coûteux, qui peut se révéler rapidement obsolète, ou inutile en cas de déménagements de locaux.

Facilité et flexibilité

Dans le contexte d'un réseau temporaire, pour des formations, des expositions ou autre chantiers, pour couvrir des zones difficiles d'accès aux câbles, et relier des bâtiments distants.

Mobilité

Les réseaux sans fil offre une liberté de mouvement pendant des communications toute en maintenant les connexions.

1.6.2 Les incovénients des réseaux sans fil

Qualité et continuité du signal

Ces notions ne sont pas garanties du fait des problèmes pouvant venir des interférences du matériel et de l'environnement.

Qualité de service

La qualité de service est un élément essentiel dans un réseau. Les réseaux 802.11 posent de nombreux problème pour obtenir de la qualité de service. Tout d'abord, le débit réel du réseau n'est pas stable et peut varier dans le temps. Ensuite, le réseau étant partagé, les ressources sont divisées entre tous les utilisateurs se trouvant dans la même cellule. En ce qui concerne la première difficulté, les points d'accès Wi-Fi ont la particularité assez astucieuse de s'adopter à la vitesse des terminaux. Lorsqu'une station n'a plus la qualité suffisante pour émettre à 11 Mbps, elle dégrade sa vitesse à 5,5 puis 2, puis 1 Mbps [02].

Economie d'énergie

Les réseaux sans fil peuvent posséder des terminaux fixes ou mobiles. Le problème principal des terminaux mobiles concerne la batterie, qui n'a généralement que peu d'autonomie. Pour augmenter le temps d'activité de ces terminaux mobiles, le standard 802.11 prévoit un mode d'économie d'énergie [02].

1.7 Problématique de sécurité des réseaux sans fil

L'intérêt concernant la communication sans fil s'est considérablement développé avec l'émergence des réseaux hertziens. Nous utilisons dans notre vie de tous les jours les technologies sans fil dans le domaine informatique (la technologie Bluetooth, la norme 802.11 : le wifi). La demande des réseaux sans fil augmente de jour en jour en apportant avec elle de nouveaux problèmes liés à la communication y compris le problème de la sécurité relative aux transmissions radio-électriques. En effet, La transmission des données via une interface d'air plutôt que d'un conduit physique plus sûr apporte avec elle certaines vulnérabilités inhérentes à la sécurité, tels que l'écoute. Alors que les entreprises ont adopté les avantages de l'accès à leurs réseaux sans fil, ils ont également gardé le cap sur le maintien de leurs données sensibles au sein de leurs frontières. Il est principalement le besoin de la sécurité d'entreprise qui a entraîné le développement de méthodes et des protocoles de sécurité sans fil LAN, et ces progrès ont également eu un effet positif aux particuliers et aux petits cadres de fonction.

Il est essentiel de protéger son réseau sans fil, même si les données qui circulent n'ont

rien de confidentiel. En effet, un réseau sans fil non protégé peut permettre à n'importe quel utilisateur du voisinage de porter atteinte au réseau et de lancer un certains nombre d'attaques.

Dans le cadre de notre travail, la sécurité des réseaux sans fil sera discutée, nous insisterons donc sur les différentes attaques susceptible d'atteindre les réseaux 802.11, ainsi que les principales solutions qui ont été développées pour palier à celles-ci. Nous nous baserons sur la solution 802.11i qui est notre objet d'étude, pour le rendre plus robuste face aux attauqes du reseau.

1.8 Conclusion

Ce premier chapitre a été axé sur les concepts fondamentaux des réseaux sans fil. Ces dernières années, ce type de réseau a connu un essor considérable, et ceci revient aux multiples avantages qu'il offre (mobilité, fiabilité, etc.). Mais grâce à l'extrême d'usage libre que le wifi (802.11) offre aux utilisateurs « nomades », en assurant une continuité des services à la fois performante et économique via des terminaux adaptés, fiables et relativement peu coûteux (Laptop, PDA, etc.). Le Wifi est arrivée à surpassé ses autres concurrents, il est devenu un moyen dominant permettant de fournir une architecture de réseaux locaux sans fils.

Dans le prochain chapitre, nous aborderons la sécurité des réseaux sans fil 802.11, et nous détaillerons en particulier le standard 802.11i.

CHAPITRE 2

LA SÉCURITÉ DANS LES RÉSEAUX SANS FIL 802.11

2.1 Introduction

La sécurité de l'informatique ne se limite certes pas à celle du réseau, mais il est indéniable que la plupart des incidents de sécurité surviennent par le réseau. Ce chapitre est consacré à la sécurité des réseaux 802.11. Après un rappel de quelques notions de sécurité, nous présentons les attaques qui peuvent atteindre les réseaux 802.11 et les premières solutions utilisées, puis nous détaillons la norme de sécurité 802.11i. Enfin, nous clôturerons avec les vulnérabilités de ce standard.

2.2 Les exigences de la sécurité

Pour remédier aux failles des systèmes et protocoles informatiques et pour contrer les attaques du réseau, la sécurité informatique se base sur un certain nombre de services, qui permettent de mettre en place une réponse appropriée à chaque menace. Classiquement, la sécurité s'appuie sur les concepts de base suivant :

Identification

L'utilisateur d'un système ou de ressources diverses possède une identité qui détermine ses lettres de crédit et ses autorisations d'usage. Cette dernière peut être vérifiée de multiple manières, compte utilisateur (Login) d'un système d'exploitation ou techniques biométriques [02] tel que l'empreinte digitale, empreinte vocale.etc.

Authentification

Cette opération consiste à faire la preuve de son identité. Par exemple on peut utiliser un mot de passe, ou une méthode de défi basée sur une fonction cryptographique et un secret partagé. L'authentification peut être simple ou mutuelle selon les contraintes de l'environnement [02].

Confidentialité

C'est la garantie que les données échangées ne soient compréhensibles que pour les deux entités qui partagent un même secret. Cette propriété implique la mise en oeuvre de mécanismes et des méthodes de chiffrement [02].

Intégrité

L'intégrité des données consiste à prouver que les données n'ont pas été altérées ou modifiées durant la communication, elles peuvent être copiées, mais aucun bit ne doit avoir été changé [02]. Le chiffrement évite l'écoute indiscrètes, mais il ne protège pas contre la modification illicite des informations par un intervenant mal intentionné. La définition de mécanismes et de techniques est nécessaire pour assurer cette dernière.

Non répudiation

Les services de non-répudiation consistent à empêcher le démenti qu'un message a été reçu par une station qui l'a réclamé, ou empêcher le démenti par une station qui a émis un message de prétendre ne jamais l'avoir fait. La fonction de non-répudiation peut s'effectuer à l'aide d'une signature à clé privée ou publique ou par un tiers de confiance qui peut certifier que la communication a bien eu lieu [16, 17].

2.3 Les mécanismes cryptographiques

La cryptographie est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible ; c'est ce qu'on appelle le chiffrement, qui, à partir d'un texte en l'air, donne un texte chiffré ou cryptogramme. Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir de texte chiffré [18]. Son but est de répondre aux exigences de la sécurité. Pour cela, on utilise un certain nombre de mécanismes, nous allons voir dans ce qui suit, quelles sont les techniques que la cryptographie fournit pour réaliser ces mécanismes.

2.3.1 Chiffrement symétrique ou à clé secrète

Dans ce type de chiffrement, les clés de chiffrement et de déchiffrement sont identiques : c'est la clé secrète, qui doit être connue des tiers communicants et d'eux seuls. Ce procédé de chiffrement est dit symétrique [18, 19].

2.3.2 Chiffrement asymétrique ou à clé publique

Avec ce système de chiffrement, les clés de chiffrement et de déchiffrement sont distinctes et ne peuvent pas se déduire l'une de l'autre, l'une est publique qui doit être connue de tous, c'est pourquoi on parle de chiffrement à clé publique. Pour envoyer un message confidentiel à

un destinataire, l'émetteur le chiffre avec la clé publique du destinataire. A sa réception, ce dernier le déchiffrera avec sa clé privée qu'il est le seul à connaitre [18, 19].
Par ailleurs, le chiffrement asymétrique permet également de chiffrer en utilisant la clé secrète, cela permet donc la signature de messages.

2.3.3 Signature numérique

Appelée aussi signature électronique, est un procédé permettant à un destinataire de prouver le source et l'intégrité de message reçu. Ce qui implique que seul l'expéditeur doit être capable de générer la signature, donc d'assurer la non-répudiation de message signé [18, 20].

2.3.4 Certificat numérique

Ou certificat électronique, est un document électronique qui constitue la carte d'identité numérique d'une entité à qui il appartient, il renferme sa clé publique, ainsi qu'un certain nombre d'informations concernant cette entité. Ce document est signé par une autorité de certification ayant vérifié les informations qu'il contient [18, 19].

2.3.5 Fonction de hachage

C'est une fonction mathématique qui transforme un long message fourni en entrée, en un résumé de taille fixe, ce résumé est appelé condensé, haché ou empreinte. La fonction de hachage doit être résistante aux collisions, ce qui signifie qu'il est impossible en pratique de construire un seul haché à partir de deux messages complètement différents. D'autre part, il doit s'agir d'une fonction à sens unique, afin qu'il soit impossible de retrouver le message original à partir de condensé [20, 21]. Les algorithmes Secure Hash algorithm 1 (SHA-1) [22] et Message Digest algorithm 5 (MD5) [23], sont des fonctions de hachage utilisées fréquemment.

Le scellement

Comme la signature numérique, le scellement (Salting en anglais) fournit les services d'authentification de l'origine d'un message et l'intégrité des données, mais il ne fournit pas la non-répudiation. Ceci permet l'utilisation d'un sceau ou un code d'authentification de message. Ce code est le résultat d'une fonction de hachage à sens unique dépendant de l'entrée et d'une clé secrète.

Un moyen de générer le code, consiste à chiffrer l'empreinte avec un algorithme à clé sécrète. Une autre méthode, consiste à appliquer la fonction de hachage non pas seulement aux données à protéger, mais à un ensemble dépendant à la fois des données et de secret [18, 20].

2.4 Les différentes attaques susceptibles d'atteindre un réseau sans fils 802.11

Afin d'étudier et d'analyser le protocole 802.11i, il est important de caractériser les capacités d'un adversaire à porter atteinte à un réseau sans fil 802.11. Dans cette section, nous décrivons certaines formes d'attaques qui sont les plus répertoriées dans ces réseaux.

2.4.1 Ecoute passive et analyse du trafic

En raison des caractéristiques de communication sans fil, un adversaire peut facilement renifler et stocker tout le trafic dans un réseau local sans fil. Même lorsque les messages sont cryptés, il est important d'examiner si un adversaire peut apprendre des informations partielles ou totale de certains messages. Cette possibilité existe, si les champs communs de message sont prévisibles ou redondants ; de plus, les messages cryptés peuvent être générés sur les demandes de l'adversaire lui-même. Les paquets enregistrés et / ou des connaissances du texte en clair peuvent être utilisées pour révéler la clé de cryptage, décryptage des paquets complets, ou de recueillir d'autres informations utiles grâce à des techniques d'analyse de trafic [24].

2.4.2 Injection de message et écoute active

Un adversaire est capable d'insérer un message dans le réseau sans fil avec des équipements modérés, comme une station avec une carte réseau sans fil et un logiciel pertinent. Bien que le firmware (micrologiciel) de la plupart des cartes réseau sans fil peut limiter l'interface de composer des paquets à la norme 802.11, un adversaire est encore capable de contrôler n'importe quel champ d'un paquet à l'aide de techniques connus [09]. Par conséquent, il est raisonnable de supposer que l'adversaire peut générer un paquet choisi, modifier le contenu d'un paquet, et de contrôler complètement sa transmission. Si un paquet nécessite d'être authentifié, l'adversaire peut être capable de casser l'algorithme d'intégrité des données pour faire un paquet valide. L'adversaire peut aussi insérer un paquet rejeué, s'il n'ya pas de protection contre le rejeu ou s'il est capable de l'éviter [25]. En outre, en insérant des paquets bien choisis, l'adversaire pourrait être en mesure d'apprendre plus d'informations à partir de la réaction du système à travers l'écoute active.

2.4.3 Suppression de messages et interception

Si un adversaire est capable de faire la suppression de message, ce qui signifie qu'il est capable d'éliminer un paquet à partir du réseau avant qu'il n'atteigne sa destination. Cela pourrait se faire en interférant avec le processus de réception de paquets sur l'antenne du récepteur, par

exemple en provoquant des erreurs CRC (*Cyclic Redundancy Checksum*), de telle sorte que le récepteur abandonne le paquet. Ce processus est semblable aux erreurs ordinaires de paquet dues au bruit, mais peut être provoqué par un adversaire. L'interception des messages signifie que l'adversaire est capable de contrôler une connexion complètement. En d'autres termes, l'adversaire peut capturer un paquet avant que son récepteur le reçoit effectivement, et décider de supprimer le paquet ou le transmettre au récepteur, c'est plus dangereux que l'écoute et la suppression du message. En outre, elle diffère de l'écoute et du rejeu, parce que le récepteur ne reçoit pas le paquet avant que l'adversaire lui transmit. L'interception des messages peut sembler difficile dans les réseaux sans fil, parce que le destinataire légitime peut détecter un message dès que l'adversaire le fait. Toutefois, un adversaire déterminé a quelques moyens possibles pour réaliser l'interception des messages. Par exemple, l'adversaire peut utiliser une antenne directionnelle pour supprimer un paquet sur le côté du récepteur, tout en utilisant simultanément une autre antenne pour recevoir ce même paquet [24]. Depuis l'interception de messages est relativement difficile à réaliser, on considère cette possibilité que lorsque le dommage causé est relativement sévère.

2.4.4 La mascarade et point d'accès malveillant

A cause de la clarté des adresses MAC qui sont incluses dans tous les paquets transmis par des liaisons sans fil, un adversaire peut apprendre les adresses MAC valides par l'écoute. L'adversaire est également capable de modifier son adresse MAC à une valeur quelconque, car la plupart des firmwares fournissent l'interface pour le faire. Si un système utilise Adresse MAC comme seule information d'identification des périphériques sans fil, l'adversaire peut aussi se déguiser en toute station sans fil, ou en un point d'accès par usurpation de son adresse MAC, et en fonctionnant de façon appropriée en s'appropriant des moyens. Un adversaire est également en mesure d'installer son propre point d'accès, avec une adresse MAC fausse et un nom du réseau usurpé. Sinon, sans se passer pour d'autres, il est possible pour un AP malveillant de fournir un signal fort et tente de tromper une station sans fil en s'associant avec elle, et en divulguant des informations d'identification ou des données privées [24].

2.4.5 Le détournement de session

Nous considérons que l'adversaire peut être en mesure de détourner une session légitime après que les appareils sans fil ont fini de s'authentifier avec succès. Voici un scénario possible pour atteindre cet objectif. Tout d'abord, l'adversaire déconnecte un dispositif d'une session existante, puis se déguise en ce dispositif pour obtenir des connexions possibles sans l'attention d'autre appareils. Dans cette attaque, l'adversaire est capable de recevoir tous les paquets destinés à l'appareil détourné et d'envoyer des paquets au nom de l'appareil détourné. Cette

attaque pourrait en théorie de contourner tout mécanisme d'authentification dans le système. Toutefois, si la confidentialité des données et des protocoles d'intégrité sont utilisés, l'adversaire doit les briser afin de pouvoir lire le trafic crypté et d'envoyer des paquets valides. Ainsi, cette attaque contre l'authentification peut être prévenue par des mécanismes de confidentialité des données et d'intégrité suffisamment puissants [24].

2.4.6 Man-in-the-middle

Cette attaque est différente de l'interception de message, parce que l'adversaire doit participer à la communication continuellement. S'il existe déjà une connexion entre une station sans fil et le point d'accès (PA), l'adversaire doit briser cette connexion d'abord. Ensuite, l'adversaire se déguise en la station légitime pour s'associer avec le PA. Si le PA adopte des mécanismes pour authentifier la station, l'adversaire doit être en mesure d'usurper l'authentification. Et enfin, l'adversaire doit aussi se déguiser en PA pour tromper la station de s'associer avec lui. De même, si la station adopte un mécanisme pour authentifier le PA, l'adversaire doit usurper des informations d'identification du PA [24].

2.4.7 Déni de service

Les systèmes sans fil sont très vulnérables aux attaques par déni de service DoS (Denial of Service). Un adversaire est capable de rendre l'ensemble de service de base (BSS) indisponible, ou de perturber la connexion entre pairs légitimes. En utilisant les caractéristiques des réseaux sans fil, un adversaire peut lancer des attaques par déni de service de plusieurs façons [24]. Par exemple, le fait de forger des trames non protégés (par exemple, dé-authentification et désassociassion), en exploitant certaines faiblesses du protocole, ou de brouillage pure et simple de la bande de fréquence, sera un déni de service aux utilisateurs légitimes.

2.4.8 Attaque par dictionnaire et force brute

Ce sont des attaques qui visent les mots de passe gérer par les différents protocoles sans fil. L'attaque par force brute est une attaque qui théoriquement fonctionne à tous les coups. Elle consiste à essayer toutes les clés possibles, une à une, jusqu'à ce qu'on retrouve la clé utilisée pour le chiffrement.

Une autre attaque semblable est l'attaque par dictionnaire, Cette attaque est souvent utilisée en parallèle avec l'attaque par force brute, et consiste à essayer de retrouver un mot de passe en essayant tous les mots d'une liste contenant des mots souvent utilisés en tant que mot de passe [26]. Ces types d'attaque sont fréquemment mener contre les réseaux sans fils.

2.5 Les solutions de sécurité de 802.11

La norme 802.11 définit des solutions de sécurité pour les réseaux locaux sans fil qui permettent d'assurer l'identification et l'authentification des utilisateurs du réseau, la confidentialité et l'intégrité des données échangées sur ce réseau, et la non répudiation contribuant ainsi au respect de son intimité numérique. Parmi ces solutions, on cite :

2.5.1 Authentification

Il existe deux principaux modes d'authentification. Le premier est dit système ouvert d'authentification (en anglais *Open System Authentification*) qui ne produit aucune vérification. Le second dit à clé partagée (en anglais *Shared Key Authentification*), permet de s'assurer que la station qui souhaite s'authentifier possède bien la clé partagée.

Système ouvert d'authentification : Permet à une station de s'authentifier auprès d'une autre station. Pour cela, cette station envoie une requête d'authentification au point d'accès auprès duquel elle souhaite s'authentifier. Dans les systèmes d'authentification ouverts, la réponse à cette requête doit toujours être positive, pour autant que la station réceptrice accepte ce mode d'authentification sans contrôle. L'authentification est réalisée complètement en deux messages [27].

Authentification à clé partagée : Se base sur une clé secrète possédée par la station et le point d'accès, et sur un algorithme de chiffrement symétrique, donc un mode Challenge-réponse. Quand le point d'accès reçoit une requête d'authentification, il envoie un challenge à la station. La station chiffre le challenge avec l'algorithme de chiffrement choisi et sa clé secrète, puis transmet le résultat (une réponse) au point d'accès. Le point d'accès déchiffre la réponse à l'aide de la clé secrète et l'algorithme de chiffrement, et compare la valeur obtenue avec celle du challenge envoyé. Si les deux valeurs sont identiques, l'utilisateur est authentifié [27].

2.5.2 Contrôle d'accès

Le contrôle d'accès permet d'interdire les intrusions. Un système rattaché à d'autres systèmes et ne contrôlant pas les accès peut être une véritable menace pour l'intégrité du réseau. Pour cela, trois techniques ont été utilisées :

Identificateur de reseau(SSID) : Cet identificateur inclus dans la norme IEEE 802.11, permet de filtrer le trafic. Un trafic ne portant pas le même identificateur que le réseaux que l'on souhaite pénétrer est ignoré par ce dernier. Il est donc nécessaire de connaitre le nom du réseau qui est partagé secrètement, pour y pénétrer. Cette protection est en faite très sommaire, car le point d'accès envoie périodiquement en clair des trames indiquant l'identité du réseau, et une écoute de celui-ci permet de récupérer le SSID [27].

Mot de passe : La protection par mot de passe est bien connue. Une station cherchant à se connecter au réseau doit envoyer un mot de passe à la requête de ce réseau, ou plus généralement d'un point d'accès de celui-ci. Si le mot de passe est correct, l'accès est autorisé, sinon il est interdit. Cette protection est extrêmement simpliste, car il est facile de capturer le mot de passe par écoute passive [27].
Filtrage sur adresse MAC : Cette protection consiste à n'autoriser l'accès au réseau qu'à des stations présentant une adresse MAC prédéfinie est connue du réseau. Cette protection n'est pas non plus très difficile à contourner, car l'écoute passive du réseau permet de récupérer les adresses MAC autorisées. Ensuite, de nombreuses cartes radio permettent de modifier par logiciel leur adresse MAC [27].

2.5.3 Chiffrement

L'absence de chiffrement dans un réseau sans fil laisse l'ensemble des données qui transitent sur ce réseau à la merci d'une personne munie d'une carte Wifi et située dans le périmètre de réception des ondes émises par les autres équipements. En raison de la propagation des ondes, il est nécéssaire de protéger son réseau par un chiffrement approprié. Le protocole initialement proposé pour le chiffrement des communications entre éléments d'un réseau sans fil est le WEP (Wired Equivalent Privacy). Le WEP est une option proposée dans le standard IEEE 802.11 et, en plus de chiffrement, traite de l'authentification et de l'intégrité. L'évolution du chiffrement dans les réseaux sans fil est apparu avec le standard WPA (Wi-Fi Protected Access). Cette norme était initialement une norme intermédiaire avant la finition et la ratification de la norme IEEE 802.11i, qui a apporté un niveau de sécurité satisfaisant pour l'ensemble des exigences en matière de chiffrement, authentification et intégrité.

2.5.4 Contrôle d'intégrité

Parmi les mécanismes de contrôles d'intégrité des données utilisées, le CRC et MIC.
CRC : Le standard IEEE 802.11 définit un mécanisme sommaire d'intégrité des trames basé sur le CRC. Cette valeur est appelée ICV (Integrity Check Value) et est de longueur 4 octets. Les propriétés du CRC sont telles que le niveau de sécurité atteint est très faible. Il est ainsi possible pour un utilisateur mal intentionné de modifier une trame tout en mettant à jour le CRC, afin de créer une trame modifiée valide [28].
MIC : Un mécanisme d'intégrité beaucoup plus robuste appelé MIC. Ce champ a une longueur de 8 octets et permet de se prémunir contre le rejeu. L'utilisation de MIC est recommandée afin d'obtenir un niveau de sécurité plus élevé que l'utilisation d'une simple valeur de type CRC, présentant des propriétés cryptographiques trop faibles pour assurer l'intégrité des trames dans un réseau sans fil [28].

2.6 Les protocoles de sécurité du standard 802.11

La norme 802.11 a définit plusieurs protocoles destinés à fournir un environnement d'exploitation sécurisé. Dans cette section, nous décrivons chacun de ces mécanismes.

2.6.1 Le WEP

Le WEP est un protocole chargé du chiffrement des trames 802.11 utilisant l'algorithme symétrique RC4 (*Rivest Cypher* 4) avec des clés d'une longueur de 64 ou 128 bits. Le principe du WEP consiste à définir dans un premier temps une clé secrète de 40 ou 104 bits. Cette clé secrète doit être déclarée au niveau du point d'accès et des clients. La clé sert à créer un nombre pseudo aléatoire d'une longueur égale à la longueur de la trame. Chaque transmission de donnée est ainsi chiffrée en utilisant le nombre pseudo-aléatoire comme masque grâce à un OU-Exclusif entre le nombre pseudo-aléatoire et la trame [29].

La clé de session partagée par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations WiFi, il est nécessaire de les configurer en utilisant la même clé de session. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications. De plus, 24 bits de la clé servent uniquement pour l'initialisation, ce qui signifie que seul 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

Le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données. Pour autant, il est vivement conseillé de mettre au moins en oeuvre une protection WEP 128 bits, afin d'assurer un niveau de confidentialité minimum et d'éviter de cette façon 90% des risques d'intrusion.

2.6.2 Le WPA

Vu les faiblesses du WEP, la WiFi Alliance décida alors qu'elle ne voulait ni attendre la parution du 802.11i, ni accepter que chaque constructeur définisse sa propre solution. Sa conclusion fut qu'il était nécessaire d'avoir rapidement au moins une version allégée du futur 802.11i. C'est ainsi qu'elle définit la solution Wireless Protected Access (WPA) qui une version allégée du standard 802.11i. Il existe deux variantes du WPA : le WPA Personal, également appelé WPA-PreShared Key (WPA-PSK) et le WPA Enterprise.

Le WPA-PSK suppose la configuration d'une clé partagée dans tous les AP et équipements connectés au réseau. Le WPA Enterprise repose sur le protocole 802.1x [37] et un serveur d'authentification RADIUS (Remote Authentication Dial In User Service)[38].

Le WPA repose sur le cryptage TKIP (Temporal Key Integrity Protocol) qui a été conçu de telle sorte qu'il soit possible de le mettre en oeuvre dans les AP existants, par le biais d'une simple mise à jour de firmware. Tout en reposant encore sur l'algorithme RC4, comme le WEP, il corrige toutes les failles du WEP et peut être considéré comme robuste. L'intégrité des données est renforcée avec un contrôle d'intégrité des messages appelé MIC. Toutefois, il n'a été défini que pour servir de transition vers le 802.11i, qui est la solution la plus sûre[17].

2.6.3 Le 802.11i(WPA2)

Le 802.11i était la norme attendue pour améliorer la sécurité dans les réseaux sans fils vu les faiblesses du protocole WEP, mais pour sa finalisation, il a fallu passer beaucoup de temps ce qui a poussé la wifi alliance a publié une version légère du WPA2 à savoir WPA comme nous l'avons mentionné précédemment. Le 802.11i ou WPA2 (le nom commercial) a fini par être ratifié en juin 2004. Le WPA et le WPA2 sont identiques du point de vue de leur architecture globale et donc de leur mise en oeuvre.

La norme 802.11i complète le WPA avec une méthode de cryptage plus puissante encore : l'AES. Le WPA2 offre donc le choix du cryptage, contrairement au WPA qui impose TKIP. Une autre différence importante est que le WPA n'est compatible qu'avec les réseaux de type Infrastructure et non les réseaux Ad Hoc. Quant au WPA2, il peut sécuriser les deux types de réseau [17].

Dans ce qui suit, nous allons détailler la norme 802.11i, pour comprendre son fonctionnement, de pouvoir étudier les vulnérabilités présentes dans les mécanismes utilisés par celles-ci.

2.7 Le standard 802.11i

802.11i est un amandement comportant des améliorations par rapport au WEP, qui propose une nouvelle architecture de sécurité robuste en définissant de nouvelles methodes d'authentification et de chiffrement, il impliaque les trois entités suivantes :

- La station à authentifier appelée également Client d'accès (ou suplicant) : est l'entité qui tente d'accéder au réseau.
- Le Point d'Accès PA (ou authentificateur) : est l'entité intermédiaire contrôlant l'accès au réseau.
- Le Serveur d'Authentification : est l'entité qui prend les décisions d'autorisation.

La norme 802.11i utlise les trois moyens suivants :

- Le standard IEEE 802.1x qui permet de réaliser une authentification par contrôle de l'accès réseau et autoriser ou non une liaison physique entre un client et un point d'accès.
- Le processus de chiffrement basé sur l'algorithme AES permettant de réaliser le mode de sécurisation WPA2.
- Le processus de chiffrement TKIP permettant d'obtenir le mode de sécurisation WPA (moins robuste que WPA2).

2.7.1 RSN (Robust Network Security)

Un réseau sans fil qualifié de robuste (RSN, Robust Network Security) est définit comme un réseau dans lequel les stations communiquent d'une manière sécurisée au travers des associations de sécurité dénommées RSNA (Robust Network Security Association). Une RSNA est basée sur l'architecture IEEE 802.1x, qui fournit un service d'authentification et de gestion de clés. Le rôle d'une RSN est de garantir la sécurité et la mobilité, Intégrité et la confidentialité, ainsi que le passage à l'échelle et la flexibilité.

La notion de PAE

Chaque station utilise un port PAE (Port Access Entity) 802.1x pour la transmission des données. Ce port physique est utilisé pour fournir le contrôle d'accès dans 802.11i. Plus précisément, chaque port PAE est scindé en deux ports logiques qui sont connectés en parallèle sur ce port. Le premier port logique est dit "contrôlé" et peut prendre deux états "ouvert" ou "fermé" (Voir Figure 2.1), tandis que le second est toujours accessible "non contrôlé", mais il gère que les trames spécifiques à 802.1x [30, 31].

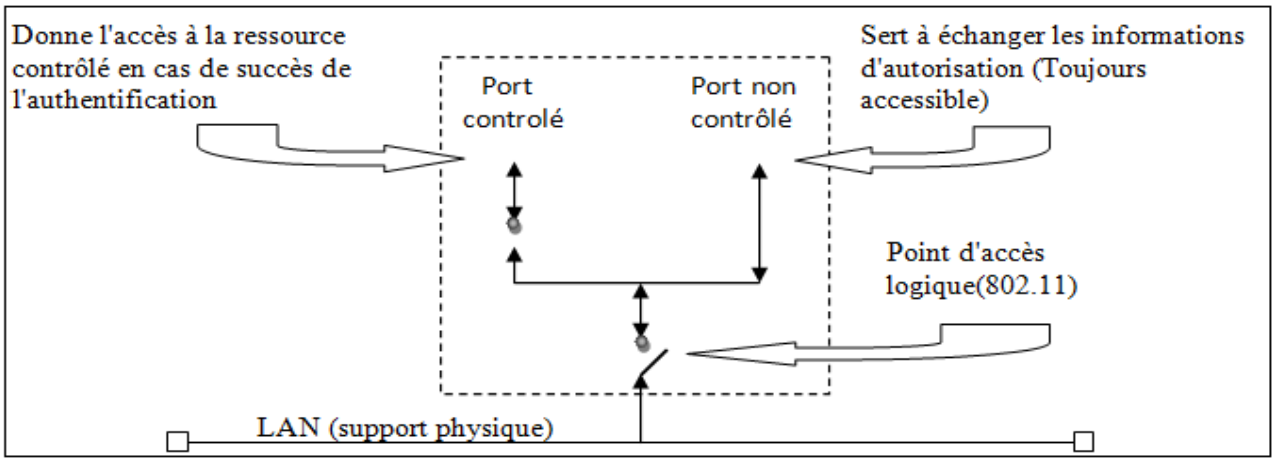

FIGURE 2.1 – PAE d'un point d'accès [32].

Une association de sécurité RSNA est établie entre deux ports PAE de deux entités de réseau, En fait, il existe trois types d'associations [32] :

- **Association PMKSA** (*Pairwise Master Key Security Association*) est établie entre une station et un point d'accès qui supporte la clé primaire PMK (Pairwise Master key) et d'autres informations comme la durée d'utilisation de PMK, adresse MAC de l'authenticateur, etc. PMK est utilisée pour la dérivation des clés temporaires pour le chiffrement de données.
- ***Association PTKSA*** (*Pairwise Transient Key Security Association*) est établie entre une station et un point d'accès qui contient la clé PTK (Pairwise Transient Key) et d'autres informations comme l'algorithme de chiffrement de données. Cette association est utilisée pour sécuriser le trafic unicast entre la station et le point d'accès.
- **Association GTKSA** (*Group Temporal Key Security Association*) établie entre les membres d'un groupe de stations. Dans un réseau 802.11 en mode infrastructure, une GTKSA est établie entre un point d'accès et un groupe de stations qui supportent la GTK (Group temporal Key) et d'autres informations nécessaires pour le chiffrement du trafic broadcast ou multicast envoyé de l'authentificateur vers les stations.

Dans la section qui suit, nous verrons ces associations dans les phases opérationnelles du 802.11i.

2.7.2 Les phases opérationnelles de 802.11i

Les changements fondamentaux introduits par la norme IEEE 802.11i comme la séparation de l'authentification utilisateur et le chiffrement/contrôle d'intégrité des messages, permettent une architecture de sécurité robuste RSN (Définit précédemment). Ces changements déterminent par conséquent les phases opérationnelles de 802.11i (voir la figure 2.2).

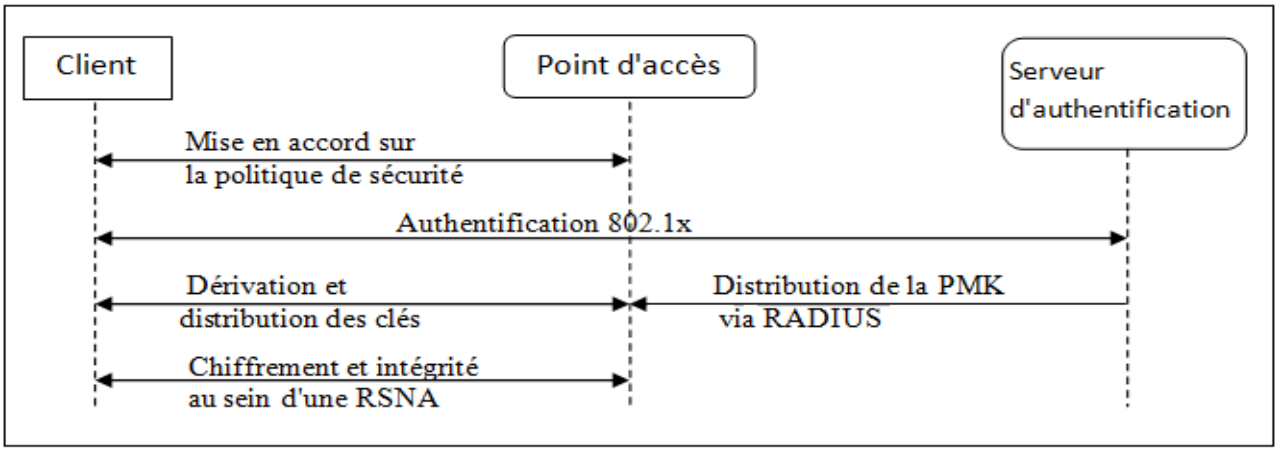

FIGURE 2.2 – Phases opérationnelles du 802.11i.

Un contexte de communication sécurisé s'effectue en quatre phases :

- La mise en accord (Négociation) 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 RSNA [02, 30, 33].

2.7.2.1 Phase 1 : Négociation d'une politique de sécurité

La première phase permet aux deux parties communicantes de s'accorder sur la politique de sécurité à utiliser. Les politiques de sécurité supportées par le point d'accès sont diffusées dans les trames *Beacon* et *Probe Response* (suivant un message *Probe Request* du client). Une authentification ouverte standard constitue l'étape suivante, cette authentification est toujours positive. 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. Les informations de la politique de sécurité sont envoyées dans le champ RSN IE (*Information Element*) détaillant :

- 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.) [02, 30, 33].

Cette phase est illustrée sur la figure suivante (figure 2.3) :

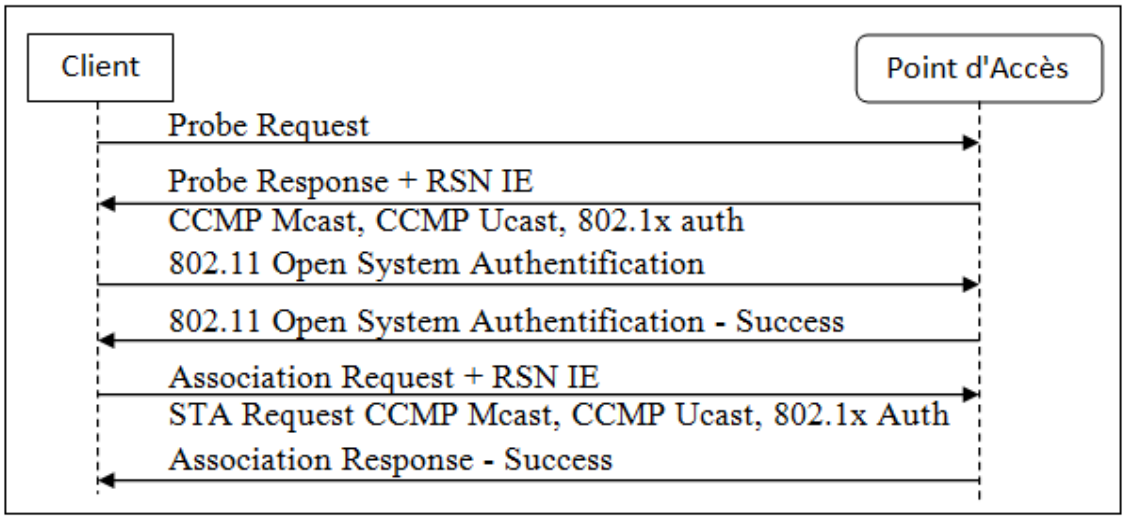

FIGURE 2.3 – Négociation de la politique de sécurité.

2.7.2.2 Phase 2 : Authentification 802.1x

La seconde phase consiste en l'authentification 802.1X basée sur EAP et la méthode spécifique choisie : EAP-TLS avec certificat client et serveur (nécessitant une infrastructure à clé publique), EAP-TTLS ou PEAP pour des authentifications hybrides (où le certificat est uniquement nécessaire côté serveur), etc. L'authentification 802.1X est initiée lorsque le point d'accès demande les données d'identification du client, la réponse du client contient alors la méthode d'authentification préférée. Différents messages dépendant de la méthode spécifique choisie sont alors échangés par la suite entre le client et le serveur d'authentification, afin de générer une clé maîtresse MK (*Master Key*). À la fin de la procédure, un message *Radius Accept* est envoyé du serveur d'authentification au point d'accès contenant la PMK, ainsi qu'un message final EAP Success pour le client (figure 2.4) [02, 30, 33].

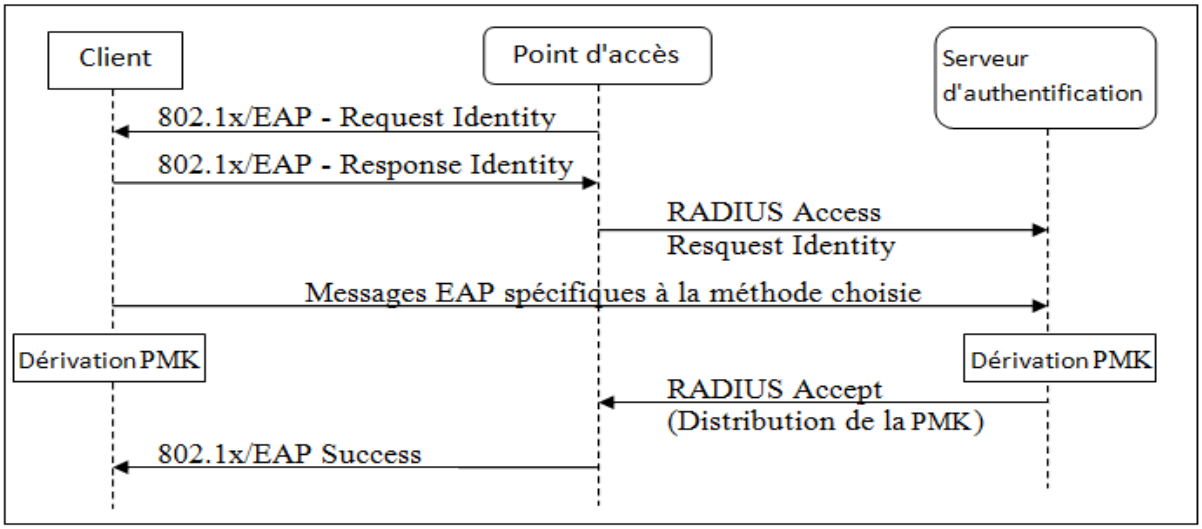

FIGURE 2.4 – Phase d'authentification 802.1x.

2.7.2.3 Phase 3 : Hiérarchie et distribution des clés

La sécurité des transmissions repose essentiellement sur des clés secrètes. Dans les RSN, chaque clé à une durée de vie limitée et de nombreuses clés sont utilisées. Après une authentification réussie, un contexte de sécurité est établi, des clés temporaires (*de sessions*) sont créées et régulièrement mises à jour jusqu'à la fermeture du contexte. 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 (voir la figure 2.5) :

- **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 [02, 30, 33].

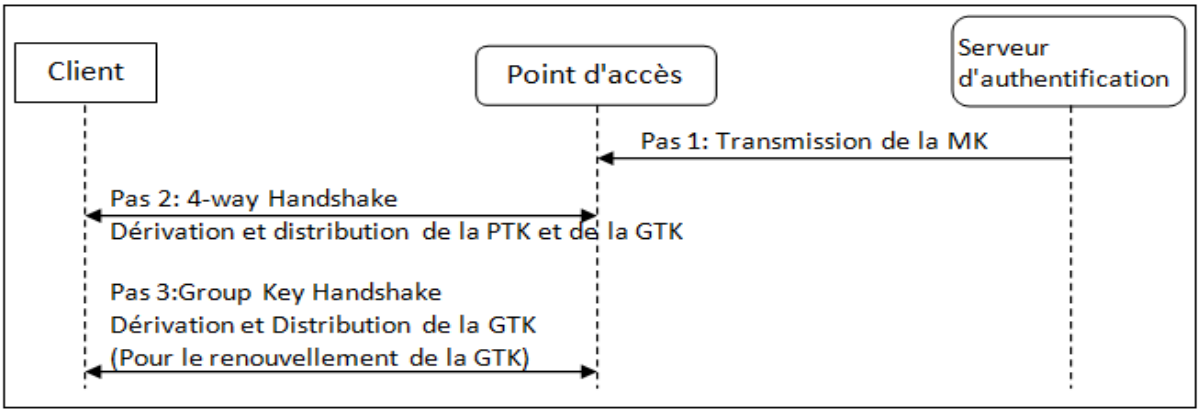

FIGURE 2.5 – Hiérarchie et distibution de clés.

La dérivation de la PMK dépend de la méthode d'authentification choisie :

– Si la PSK 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 (Phases 2).

La PMK est utilisé pour la génération des clés de chiffrement temporaire. Pour le trafic à destination d'une machine, la PTK (Pairwise transient Key) est utilisée, sa taille dépend de protocole de chiffrement choisi (chiffrement TKIP ou CCMP).

La PTK consiste en plusieurs clés temporelles dédiées (Voir la Figure 2.6) :

– **KCK** (*Key Confirmation Key*) : Clé pour authentifier les messages de contrôle d'intégrité (***MIC***) durant les deux poignées de main.
– **KEK** (*Key Encryption Key*) : Clé pour la confidentialité des données durant les deux poignées de main.
– **TK** (*Temporary Key*) : Clé pour le chiffrement des données (Utilisée dans TKIP ou CCMP).
– **TMK** (*Temporary MIC Key*) : Clé pour l'authentification des données (utilisée seulement dans TKIP) [02, 30, 33].

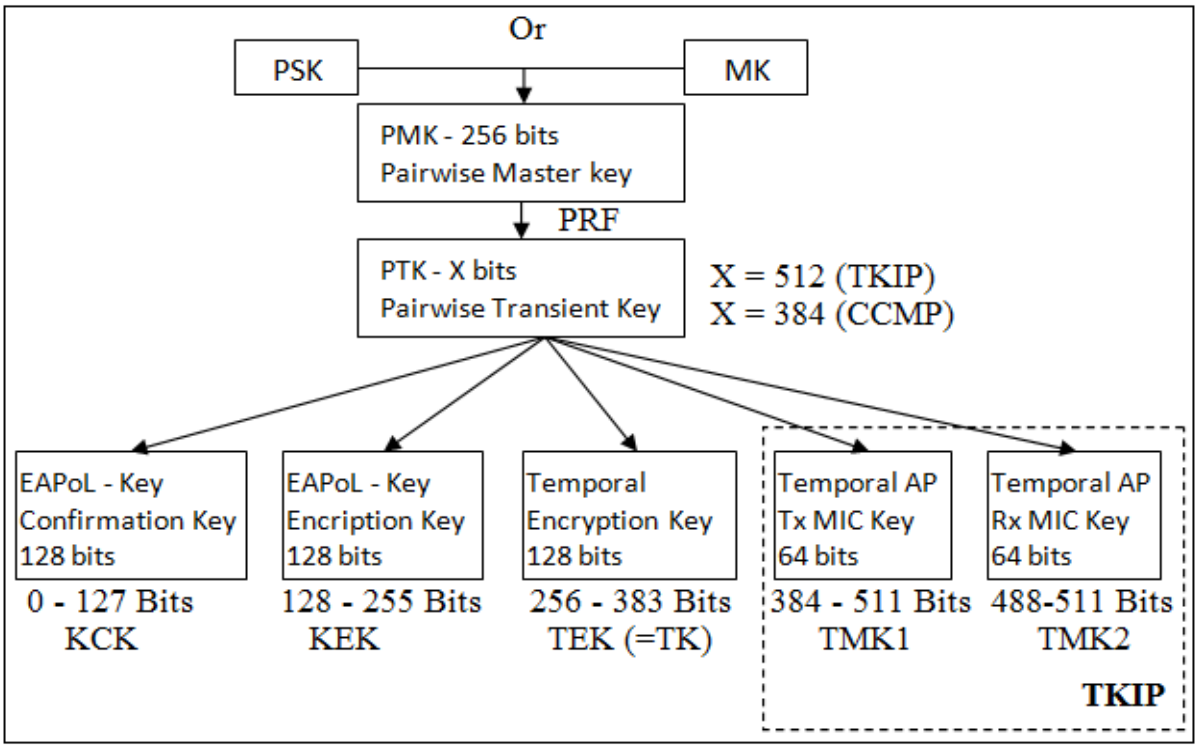

FIGURE 2.6 – Hiérarchie de clés.

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 PTK est dérivée de PMK, d'une chaine de caractères fixe, de l'adresse MAC du point d'accès (AP), de l'adresse MAC du client et de deux nombres aléatoires choisis : SNonce pour le client et ANonce pour le point d'accès, à l'aide de la fonction PRF(Pseudo Random Function).

Le 4-way Handshake est illustré à la figure ci-dessous (Figure 2.7).

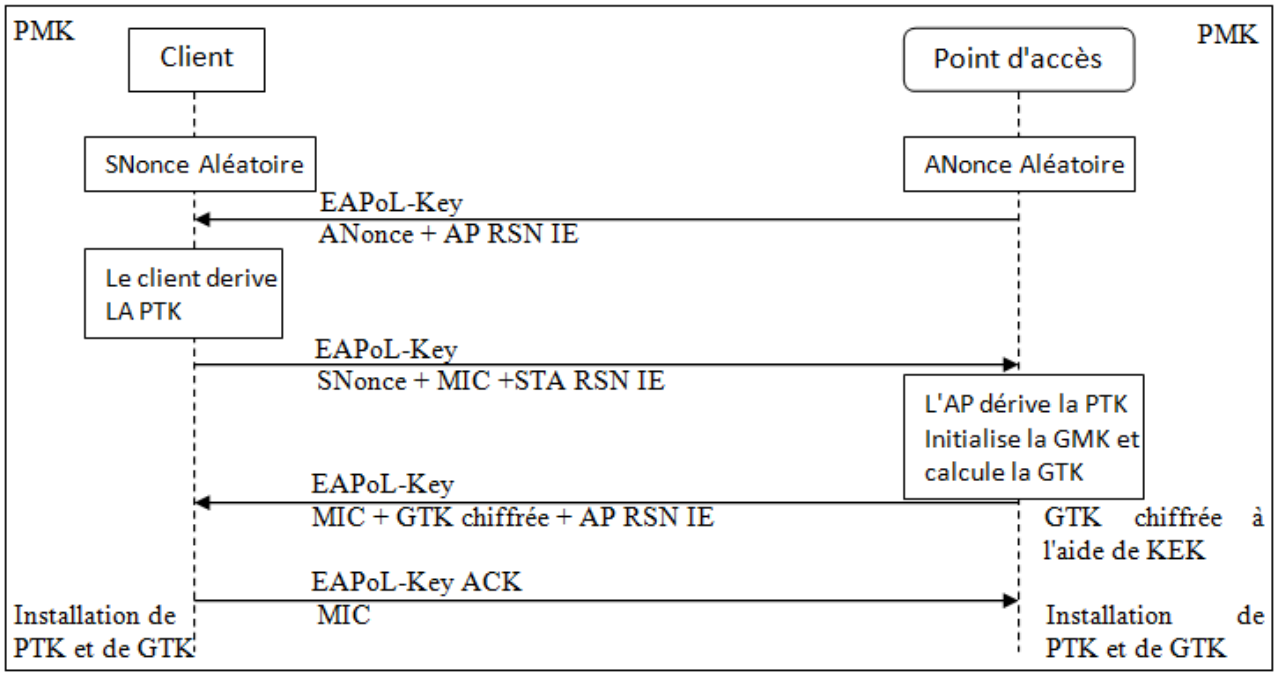

FIGURE 2.7 – 4-way Handshake

Le premier message est initie par le point d'accès en envoyant ANonce au client sans le chiffrer. Le client est maintenant en mesure de calculer la PTK et de dériver les clés temporelles. Ensuite, il envoie SNonce et le MIC calculé à l'aide de KCK dans un deuxième message. Le point d'accès en recevant ce dernier, il extrait SNonce (le message n'est pas chiffré), puis il calcule la PTK et dérive les clés temporelles. Il vérifie la valeur du MIC et il s'assure ainsi que le client connait PMK et a dérivé correctement la PTK et les clés temporelles.

Le troisième message est envoyé du point d'accès contenant GTK chiffré avec KEK. La GTK est calculée à ce niveau, à partir d'une clé maitresse GMK (Group Master Key), d'une chaine de caractères, de l'adresse MAC de point d'accès et d'un nombre aléatoire GNonce (voir la Figure 2.8). Un MIC est calculé sur ce message en utilisant la KCK, le client alors peut s'assurer que le point d'accès a correctement généré la PMK et dérivé PTK et 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. Le point d'accès reçoit le MIC et vérifie sa valeur pour commencer une session de communication sur un canal sûr [02, 30, 33].

La GTK es divisée en des clés temporelles dédiées :

- **GEK** (*Group Encryption Key*) : Clé pour le chiffrement de 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 TKIP).

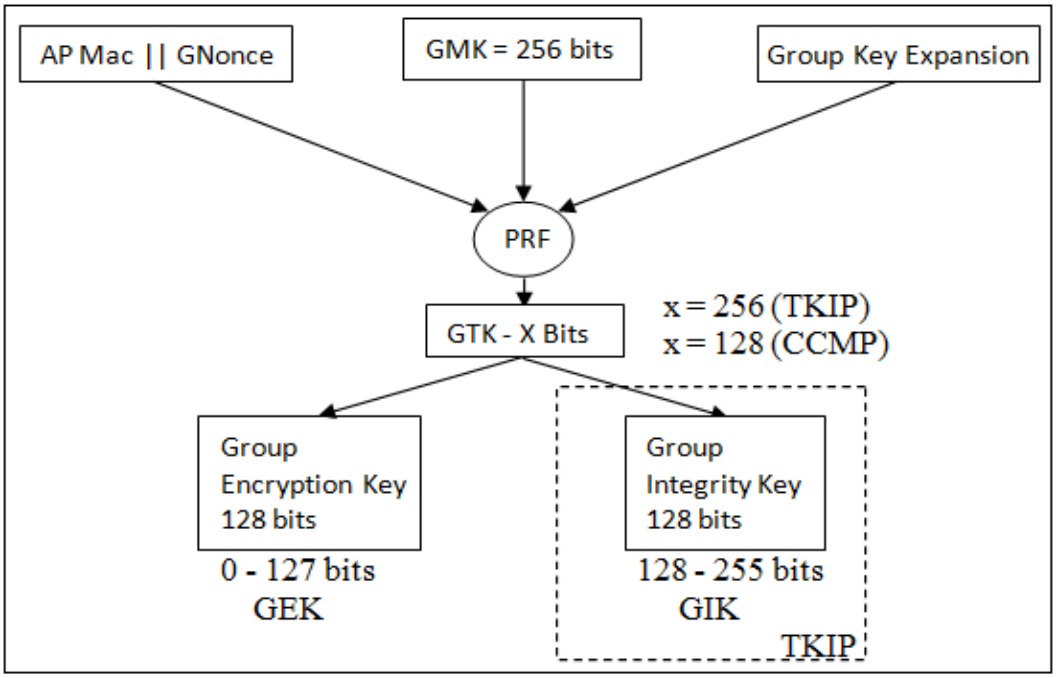

FIGURE 2.8 – Hiérarchie des clés de groupe.

La deuxième poignée de main **Group Key Handshake** se base sur les clés temporelles générées durant le 4-way Handshake (La KCK et la KEK). Elle est nécessaire en cas de désassociassion d'un client ou renouvellement de GTK. Le processus est illustré à la figure 2.9.

Le point d'accès envoi dans le premier message, la nouvelle clé GTK calculée et chiffrée avec KEK au client, ainsi que le numéro de séquence de GTK, l'adresse de groupe (Group) et le MIC de ce message calculé grâce à KCK..

Le second message acquitte la réussite de group Key Handshake en envoyant l'adresse du groupe de GTK et le MIC calculé sur ce message. A sa réception, le point d'accès vérifie la valeur de MIC et installe la nouvelle GTK Le point d'accès envoi dans le premier message, la nouvelle clé GTK calculée et chiffrée avec KEK au client, ainsi que le numéro de séquence de GTK, l'adresse de groupe (Group) et le MIC de ce message calculé grâce à KCK [30].

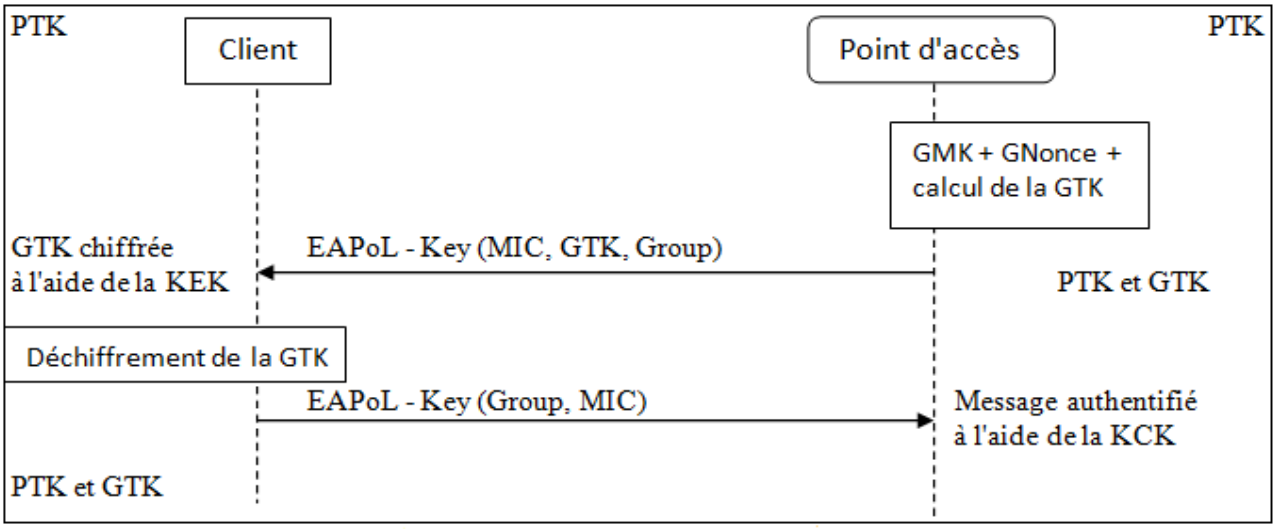

FIGURE 2.9 – Group Key Handshake.

2.7.2.4 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 Integrity protocol*),
- **CCMP** (*Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol*).

1) Le protocole TKIP :

TKIP est un Protocole de chiffrement destiné à améliorer le WEP, basé sur l'algorithme RC4, afin de permettre une mise à jour aux systèmes à base de WEP. Il procure des corrections pour chaque faille de WEP :

- L'intégrité des messages : un nouveau MIC basé sur l'algorithme Michael peut être implémenté de manière logicielle sur des processeurs lents,
- 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 pour éviter sa réutilisation,
- Per Packet Key Mixing : pour obtenir des clés en apparence non liées,
- Gestion des clés : nouveau mécanisme pour la génération et la distribution des clés.

Le chiffrement TKIP :

Le schéma TKIP de mixage des clés est divisé en deux phases. La phase 1 implique les champs statiques : la clé de session secrète TEK, l'adresse MAC du transmetteur TA (incluse pour éviter la collision de vecteur d'initialisation (IV)) et les 32 bits de poids fort de l'IV. La phase 2 implique la sortie de la phase 1 et les 16 bits de poids faible de l'IV, changeant ainsi

tous les bits du champ Per Packet Key pour chaque nouveau IV. La valeur de l'IV commence toujours à 0 et est incrémenté de 1 pour chaque paquet transmis, tout message ayant le compteur de séquence TKIP (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.

Le MPDU (MAC Protocol Data Unit) et le MSDU (MAC Service Data Unit) se réfèrent à un simple paquet de données, le MSDU représente un paquet de données avant sa sa fragmentation, alors que le MPDU représente les multiples unités de données après fragmentation

Le schéma de mixage des clés et de chiffrement est montré dans la figure ci-dessus (figure 2.10) :

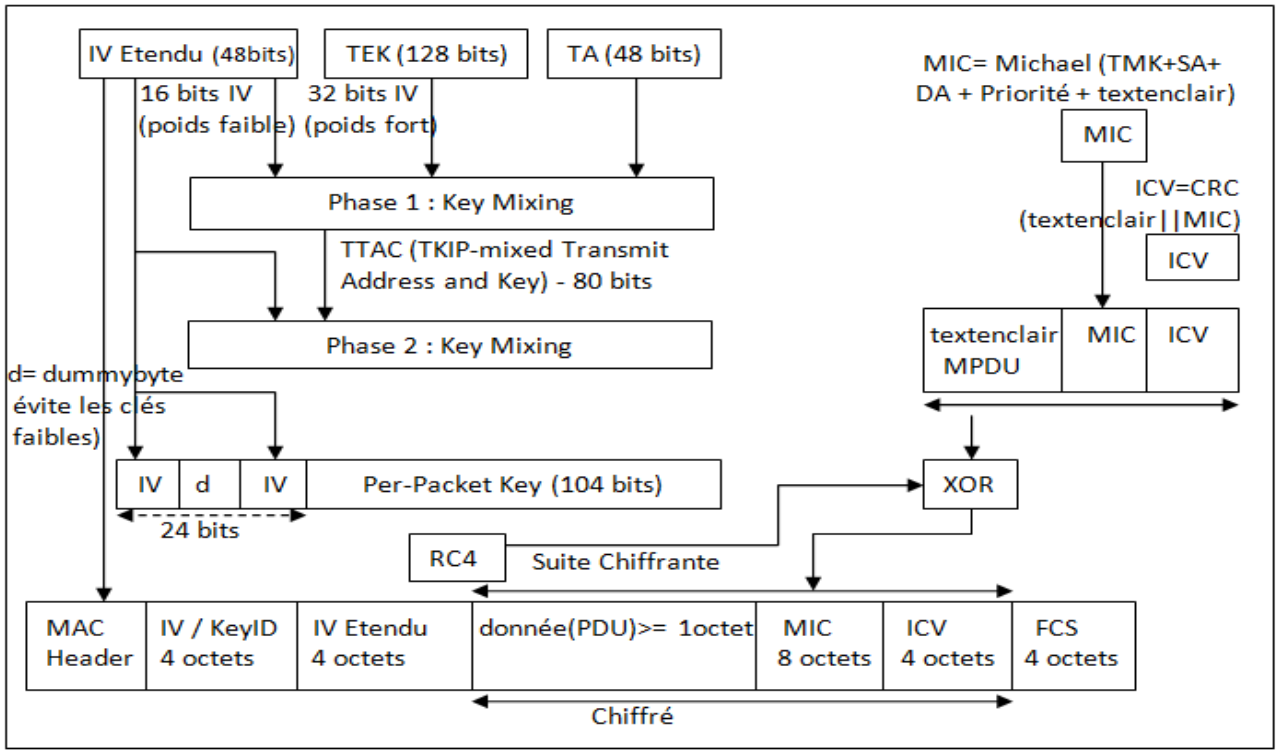

FIGURE 2.10 – Schéma TKIP de mixage et de chiffrement.

Le calcul de MIC :

Le calcul de MIC (Message Integrity Code) utilise l'algorithme Michael développé par Niels Ferguson. Il est crée pour TKIP et dispose d'un niveau de sécurité voulu de 20 bits. Le MIC est calculé en utilisant l'adresse source (SA), l'adresse destination (DA), le texte en clair MSDU et la TMK appropriée (dépendant du sens de la communication, une clé différente étant utilisée pour la transmission et la réception) [02, 30]. (voir la Figure 2.11).

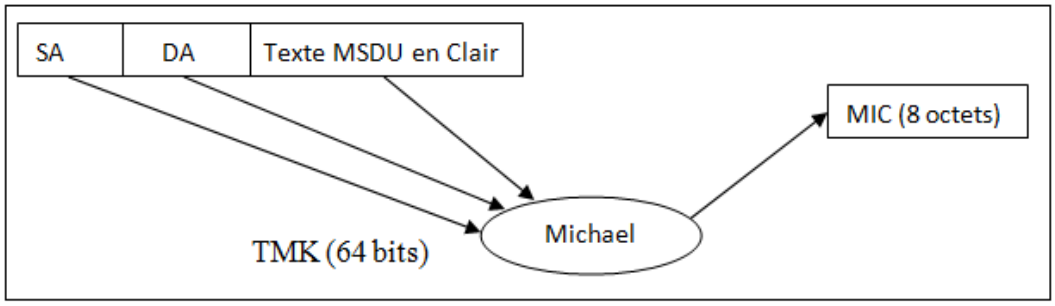

FIGURE 2.11 – Calcul de MIC (TKIP)

2) Le protocole CCMP :

Le protocole CCMP (Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol) est fondé sur AES, il utilise le mode d'opération CCM avec une taille de clé et de bloc de 128 bits, et qui combine les atouts du mode compteur CTR (CounTeR Mode) en combinaison avec la méthode d'authentification des messages appelée Cipher Block Chaining (CBC-MAC) permettant de produire un MIC.

Le protocole CCM utilise la même clé temporaire pour CTR et CBC-MAC, mais les IV sont différents, ce qui ne présente aucune faille de sécurité.

CCMP chiffre la charge utile d'une MPDU et encapsule le texte chiffré qui en découle en incrémentant le numéro de paquet PN (Packet number), afin d'obtenir un PN frais pour chaque MPDU.

Des champs de l'en-tête MAC sont utilisés pour construire l'AAD (Additional Authentification Data). CCM protège l'intégrité de ces champs ; en les masquant à 0, certains d'entre eux sont rendu silencieux. Le Nonce est construit à partir du PN, de l'adresse de la MPDU 2 et de la priorité de la MPDU. Il encode ensuite le nouveau PN et le KeyID dans l'en-tête CCMP de 8 octets [02, 30, 33].

Le schéma de chiffrement CCMP est illustrée sans la figure 2.12.

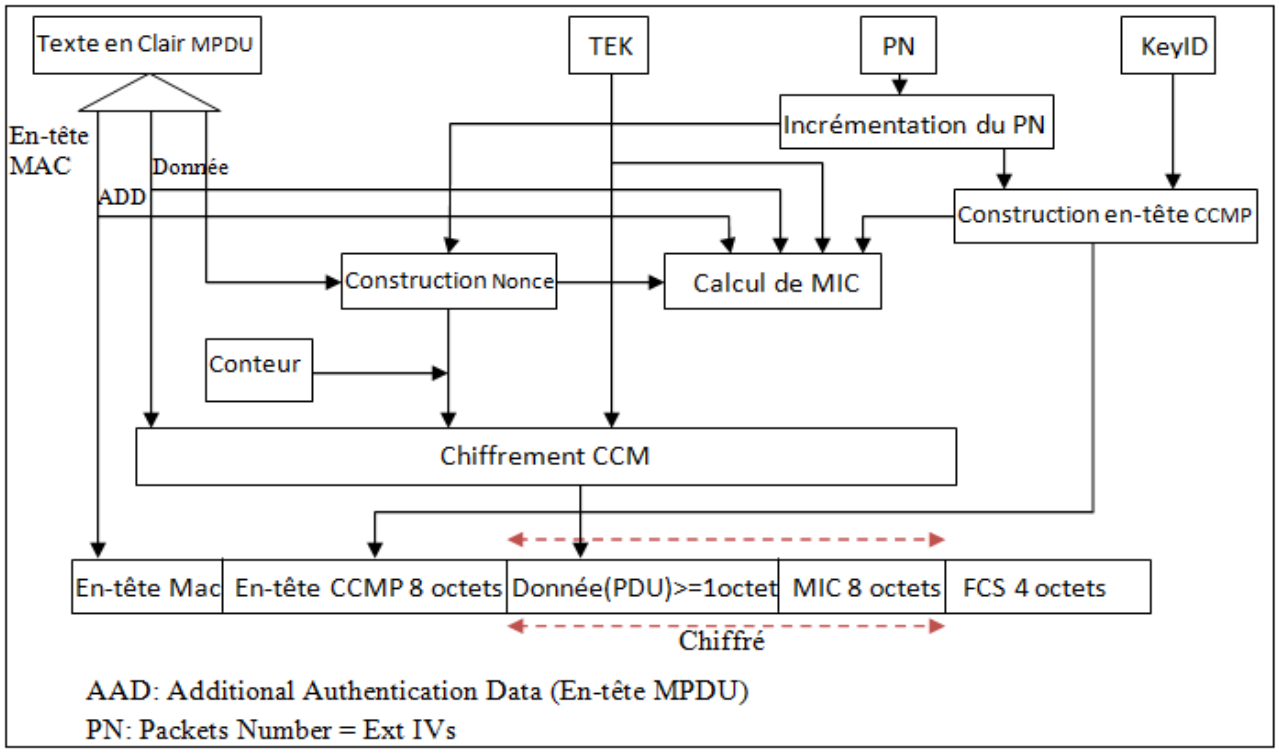

FIGURE 2.12 – Chiffrement CCMP

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 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. Ce compteur est construit sur une valeur aléatoire identique à celle utilisée pour le MIC combinée à un compteur incrémenté [30].

2.8 Analyse de la sécurité du 802.11i

Sur la base de la procédure complète d'établissement d'une RSNA, nous allons analyser la sécurité de la norme 802.11i en considérant les menaces détaillées à la section 2.4.

IEEE 802.11 a définit la façon dont les trames sont échangées entre STA et AP. Il existe trois types de trames d'IEEE 802.11, comme suit :

- Trames de données, qui encapsulent les paquets des protocoles de couche supérieure, tels que IP, elle contiennent des données d'application (par exemple, e-mails, pages Web).
- Les trames de gestion, qui comprennent les sondes d'information et balises, et des messages liés à la gestion d'association et les événements d'authentification.
- Les trames de contrôle, qui sont utilisées pour la demande et contrôler l'accès aux médias

sans fil, tels que l'envoi d'un accusé de réception après avoir reçu une trame de données.

Etant donné que les trames de gestion ne sont pas protégées dans un WLAN, un attaquant peut interférer la phase de négociation de la politique de sécurité. Plus précisément, cette phase est vulnérable à écoute passive/active, analyse de trafic, injection, interception et suppression de messages, la mascarade et PA malveillant. En effet, un attaquant peut envoyer des informations usurpées et des vues topologiques du réseau au client au nom de l'authentificateur (Point d'accès), et une fois que cela s'est produit, le client sera obligé d'utiliser des paramètres de sécurité inappropriés pour communiquer avec le point d'accès légitime, ou s'associer avec un PA malveillant.

Alternativement, un adversaire peut aussi forger les demandes d'association à un PA avec des capacités de sécurité éventuellement faibles, qui peut causer des problèmes si aucune autre protection n'est adoptée. La phase authentification 802.1x/EAP devraient prévenir de forger, modifier et rejouer les paquets d'authentification, si une authentification mutuelle forte a été implémenté. En outre, depuis que les informations d'identifications autres que l'adresse MAC sont fournies pour une authentification mutuelle réussie, l'attaquant ne peut pas se passer pour un AP (AP malveillant). Après que les deux entités sont authentifiées mutuellement et ils ont échangées un secret après la phase 2, la phase suivante résiste aussi à ces menaces. Dans le cas où l'authentification 802.1x/EAP n'a pas eu lieu, et qu'une PSK ou PMK cachée est utilisée, les deux entités peuvent s'authentifier en vérifiant la possession de celle-ci à la phase 3 qui prévient aussi de ces menaces.

Le détournement de session (*Session Hijacking*) peut exister même si de solide mécanismes d'authentification sont implémentés. Après qu'une station légitime a réussi son authentification, l'adversaire peut déconnecter cette station en forgeant des messages d'authentification et désassociassion et reprend la session avec l'AP au nom de la station légitime. Deux possibilités dans ce cas se présentent : Tout d'abord, si la session autorise l'adversaire seulement d'accepter les paquets, cela semble être juste de l'écoute, qui prévenu par le mécanisme de confidentialité de données. Autre, si la station exige l'adversaire pour interaction, l'adversaire a besoin d'obtenir les informations d'authentification comme la PTK, dans le but de générer un trafic acceptable. Dans l'ensemble, le détournement de session ne pose pas plus de danger que l'écoute et le déni de services sur la station.

L'attaque *Man-In-the-Middle* est possible dans les WLAN si aucun mécanisme n'est implémenté. Un attaquant se plaçant par exemple, entre le client et le serveur et interceptant tous les messages à leur passage. Vu du client, l'attaquant peut se comporter comme un point d'accès. Inversement, vu de point d'accès, il peut se comporter comme un client. si un

mécanisme d'authentification mutuelle n'est pas correctement implémenté dans la méthode EAP utilisée, l'adversaire est capable de lancer une attaque MITM et découvrir la PMK. Bien que cette vulnérabilité est considérée comme une faiblesse des protocoles d'authentification mutuelle spécifique à part 802.11i. N'importe implémentation de 802.11i devrait considérer attentivement ce problème

Le point d'accès 802.1x envoie un message EAP SUCCESS au client à la réception d'un message RADIUS ACCESS Accept. Ce message indique que l'authentification a réussi, mais il ne contient aucune information permettant de garantir son intégrité. le client peut passer inconditionnellement à l'état autorisé, sans qu'il soit porté attention à son état courant. Il est donc possible pour un attaquant de forger son propre paquet EAP SUCCES et de substituer au point d'accès 802.1x. Lorsque la norme est implémentée avec de forte mécanismes d'authentification mutuelle comme EAP-TLS, l'adversaire ne peut pas s'authentifier à une station ou un AP, car il ne possède pas des informations d'identification appropriées. Bien sûr, il peut suivre des informations entre stations et l'AP, mais du moment que les paquets d'authentification ne peuvent pas être modifier ou rejeuer, l'adversaire ne peut agir seulement comme un relais, ce qui provoque des dommages ne dépassant pas l'écoute.

Il existe plusieurs vulnérabilités au déni de service qui exploitent des message (EAP) non protégées dans 802.11i. Spécifiquement, un adversaire peut forger le message EAPoL-Start pour empêcher répétitivement l'authentification 802.1x de réussir, un message EAPoL-Success forgé met en place le port 802.1x sur la station sans authentification, et des messages forgés EAPoL-Failure et EAPoL-Logoff pour déconnecter le client. Une autre attaque est possible sur le 4-way Handshake, l'adversaire peut inonder la station avec le Message-1 usurpé et empêcher la réussite de la poignées de main.

Il existe encore d'autres vulnérabilités non citées des cette section, qui visent à nuire le bon fonctionnement des protocoles du 802.11i, et qui touchent à la sécurité des réseaux sans fils 802.11. Nous découvrirons quelques unes dans le chapitre qui suit à travers l'état de l'art qui expose ces dernières, ainsi les limites des solutions apportées.

2.9 Orientation de notre travail

Dans ce mémoire, nous nous concentrons principalement sur les mécanismes d'authentification et d'échange de clés dans le protocole 802.11i, qui constituent un portail d'accès à une session sécurisé, ce qui le rend une cible pour les pirates.

Nous allons étudier dans le chapitre suivant les solutions proposées pour l'amélioration des phases de l'authentification et de gestion de clés dans la norme802.11i, c'est à dire un état de l'art des améliorations faites sur ces derniers, afin de pouvoir les analyser et remédier à leurs failles et vulnérabilités et de proposer de nouvelles solutions de sécurité pour chaque phase du standard 802.11i.

Dans la phase d'authentification nous présentons un aperçu et une analyse du protocole EAP. Nous examinerons un certain nombre de méthodes EAP les plus courantes et les plus utilisés dans le contexte d'un réseau sans fil 802.11 et nous évaluerons leurs avantages en terme de niveau sécurité qu'elles offrent, et leur inconvénients en terme de susceptibilité à des types d'attaque. Ensuite, nous proposons une nouvelle méthode EAP appropriée pour les technologies sans fil.

Le processus complet de l'authentification dans le 802.11i est réalisé par le four Way Handshake. qui fournit une authentification mutuelle de client et du point d'accès, pour permettre de s'assurer que ce sont bien les entités annoncés lors de l'authentification EAP, tout en continuant avec la génération des différentes clés de session. Donc, l'importance de ces deux phases qui doivent être étudiées, analysées pour découvrir des menaces susceptibles de nuire la sécurité globale du réseau qui sera la base pour proposer de nouvelles améliorations de sécurité.

2.10 Conclusion

Au cours de ce chapitre, nous avons abordé les différents aspects liés à la sécurité dans les réseaux sans fil ainsi les différents attaques possibles sur ces réseaux. L'organisation internationale de standardisation (ISO) a défini le vocabulaire des services et des mécanismes de sécurité : l'authentification, l'intégrité, la non-répudiation, etc. Les solutions retenues actuellement pour faire face aux différents risques et menaces foisonnent. À titre d'exemple, nous avons décrit les attaques susceptibles d'atteindre les réseaux 802.11, ainsi une présentation des différentes solutions existantes, la norme de sécurité 802.11i est détaillée et nous avons analyser sa sécurité. La panoplie des protections est très vaste, elle s'accroît avec la créativité des attaquants ; par ailleurs, la technologie évolue et leur fournit des capacités de traitement toujours plus puissantes. La sécurité des réseaux 802.11 nécessite donc des études, analyses et propositions diverses pour continuer à lutter contre les menaces diverses de la sécurité.

CHAPITRE 3

SYNTHÈSE DES TRAVAUX ANTÉRIEURS

3.1 Introduction

La norme 802.11 a subi diverses modifications afin d'améliorer la sécurité des réseaux locaux sans fils. La norme 802.11i est la dernière norme pour les WLANs, elle a été lancée pour résoudre les problèmes des versions précédentes de sécurité, mais elle ne l'est pas entièrement.

Dans cette section, on verra un état de l'art des solutions qui ont été proposées pour colmater les brèches de sécurité laissées par la norme 802.11i, listées à travers l'analyse réalisée sur 802.11i dà la section 2.8. L'étude et l'analyse seront basées sur les propositions réalisées sur l'authentification et la gestion de clés.

3.2 Authentification et gestion de clés

La partie authentification est la plus sensible lorsque on veut établir une politique de sécurité. En effet, si l'authentification est bien faite, on pourra se permettre dénoyer à la machine authentifiée les clés à utiliser pour le reste des transmissions. Dans 802.11i, cela est réalisée par Le standard 802.1x qui fournit un cadre d'authentification basé sur EAP et par le 4-way Handshake pour la gestion de clés. La phase d'authentifications se termine en générant une clé primaire (PMK) qui servira dans la phase de 4-way Handshake pour la génération de clés temporaire, qui seront utilisées pour la confidentialité et l'intégrité des données. Nous Allons donc commencer par voir les solutions existantes pour les méthodes EAP, et le 4-way Handshake.

3.3 Extensible Authentification Protocol (EAP)

Le protocole EAP (Extensible Authentication Protocol) est une norme IETF (Internet Engineering Task Force) décrite dans le document RFC 3748, qui définit une infrastructure permettant aux clients d'accès réseau et aux serveurs d'authentification d'héberger des modules pour les méthodes et technologies d'authentification actuelles et futures.

EAP a été créé à l'origine comme extension du protocole PPP (Point to Point Protocol), afin de permettre le développement des méthodes arbitraires d'authentification de l'accès réseau. Avec les protocoles d'authentification PPP tels que CHAP (*Challenge Handshake Authentication Protocol*) [45], un mécanisme d'authentification spécifique est choisi au cours de la phase d'établissement de liaison. Au cours de la phase d'authentification, le protocole d'authentification négocié permet l'échange d'informations d'authentification du client qui se connecte.

Une fois l'accord négocié sur la méthode EAP, le protocole EAP permet l'échange ouvert de messages entre le client d'accès et le serveur d'authentification, lequel peut varier en fonction des paramètres de la connexion. La conversation est constituée de demandes et de réponses concernant les informations d'authentification. La méthode EAP détermine la longueur et les détails de la conversation d'authentification [34].

3.3.1 Type de paquets EAP

EAP définit quatre types de paquets pouvant être échangés entre le client et le serveur d'authentification (par l'intermédiaire du contrôleur d'accès, bien sûr) :

- **Paquet requete** : envoyé par le serveur d'authentification, il demande au client de fournir une information précise, comme son identité ou bien une preuve de cette identité, selon une méthode d'authentification choisie par le serveur (mot de passe, certificat électronique.etc.).
- **Paquet Réponse** : envoyé par le client en réponse à une requête. Le contenu de la réponse dépend de la méthode d'authentification requise par le serveur. Si le client ne gère pas la méthode d'authentification requise, il le signale et en profite éventuellement pour suggérer une liste de méthodes qu'il est capable de gérer. Le serveur d'authentification peut alors choisir l'une de ces méthodes et renvoyer une nouvelle requête au client. Si aucune méthode ne lui convient, c'est un échec.
- **Paquet Succès** : envoyé par le serveur d'authentification pour indiquer au client qu'il a été correctement authentifié. Au passage, le contrôleur d'accès ouvre le port d'accès au

réseau.

- **Paquet Echec** : envoyé par le serveur d'authentification, comme son nom l'indique, si le client n'a pas pu être authentifié.

3.3.2 Les méthodes associées à EAP

Une méthode d'authentification EAP utilise différents éléments pour identifier un client tel que :

- login / mot de passe ;
- certificat électronique ;
- biométrie
- puce (SIM)
- Etc.

Certaines méthodes combinent plusieurs critères (certificats et login/mot de passe etc.), En plus de l'authentification, EAP gère la distribution dynamique des clés de chiffrement. Dans ce qui suit, on va présenter les méthodes EAP les plus courantes.

3.3.2.1 EAP-TLS

La méthode EAP-TLS [35] est issue du protocole TLS (Transport Layer Security) [36], qui est conçu pour établir un tunnel sécurisé entre un client et un serveur. La mise en place d'un tunnel TLS commence par une première phase appelée la « négociation » ou « poignée de main » (handshake) : le serveur envoie son certificat électronique au client, et celui-ci fait de même. Le client est donc en mesure de s'assurer de l'identité du serveur, et vice versa ce qui garanti une authentification mutuelle.

À ce moment, le client génère une clé de cryptage symétrique. Il utilise ensuite la clé publique contenue dans le certificat du serveur pour crypter un message contenant la clé symétrique. Il l'envoie au serveur, qui est le seul à pouvoir décrypter le message et obtenir la clé symétrique. En effet, lui seul possède la clé privée correspondant à son certificat.

À la fin de la négociation TLS, le client s'est assuré de l'identité du serveur (et éventuellement vice versa), et une clé de cryptage symétrique a été secrètement échangée. Par la suite, les données échangées entre le client et le serveur sont cryptées grâce à cette clé symétrique [17].

L'organigramme suivant (figure 3.1) montre le fonctionnement de cette méthode :

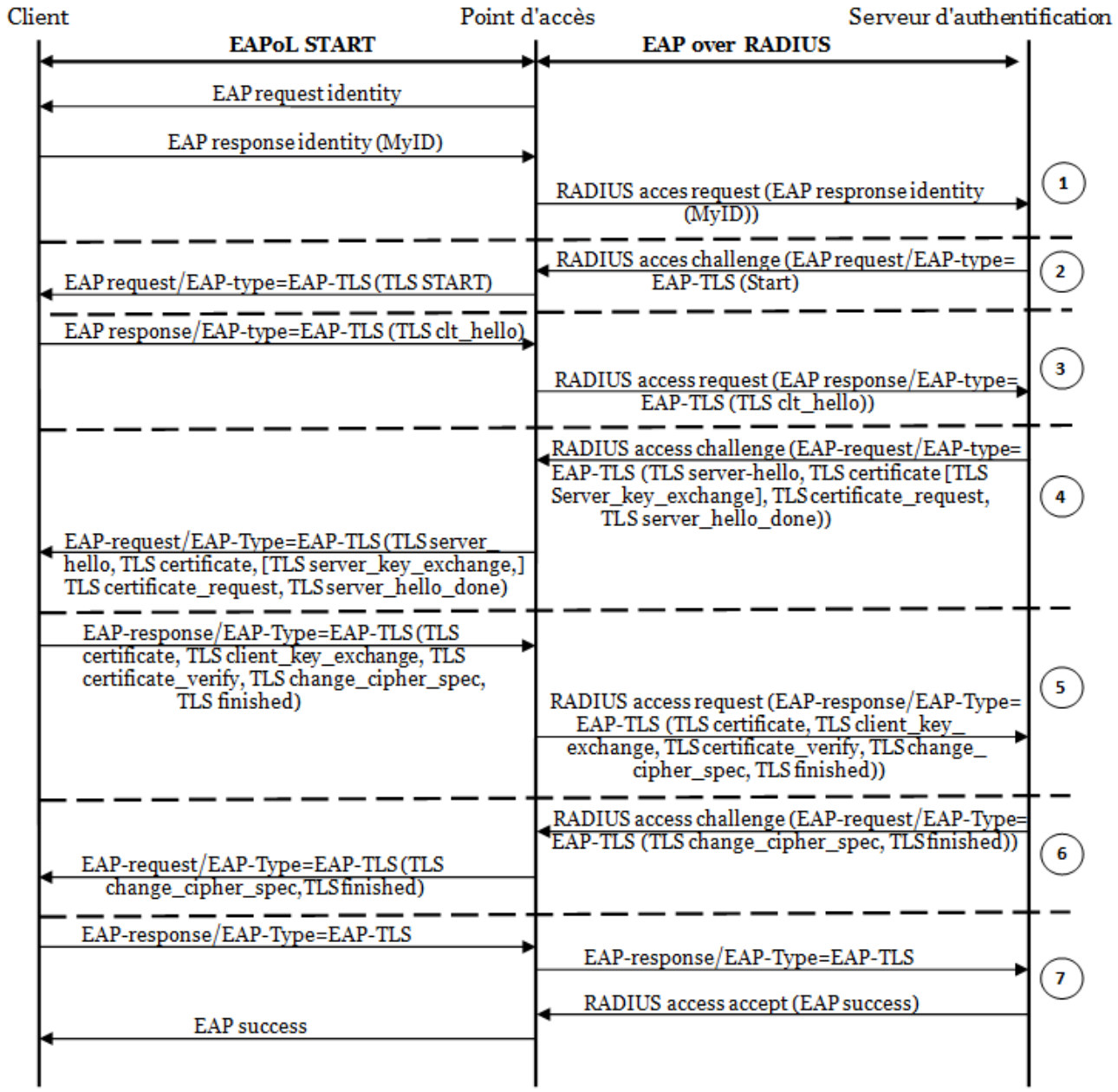

FIGURE 3.1 – Échanges EAP-TLS dans un contexte IEEE 802.11 (en cas de succès)[35, 16].

1. Le PA envoi une requête d'authentification au client. Le client répond avec son identifiant (MyID), ce message est relayé par le point d'accès vers le serveur Radius.
2. Le serveur RADIUS initie le processus d'authentification TLS par le message *TLS start*.
3. Le client répond avec un message *clt_hello*, qui contient :
   - La version TLS du client ;
   - Un identifiant de session (sessionID) ;
   - Un nombre aléatoire (défi ou challenge) ;
   - Les types d'algorithmes de chiffrement supportés par le client.
4. Le serveur renvoie une requête contenant un message *server_hello* suivi :
   - De son certificat (x509) et de sa clé publique ;
   - De la demande du certificat du client ;
   - D'un message *server_hello_done*. Un message server_hello contient :
     - Version TLS du serveur ;
     - Un nombre aléatoire ;
     - Un identifiant de session (choisit en fonction de celui proposé par le client) ;
     - Un algorithme de chiffrement choisi parmi la liste des algorithmes de chiffrement supporté par le client.
5. Le client vérifie le certificat du serveur et répond avec son propre certificat et sa clé publique.
6. Le serveur et le client, chacun de son côté, définissent une clé de chiffrement principale utilisée pour la session. Cette clé est dérivée des valeurs aléatoires que se sont échangées le client et le serveur. Les messages *change_cipher_spec* indiquent la prise en compte du changement de clé. Le message *TLS_finished* termine la phase d'authentification TLS (TLS handshake), dans le cas d'EAP-TLS la clé de session ne sert pas à chiffrer les échanges suivants.
7. Si le client a pu vérifier l'identité du serveur (avec le certificat et la clé publique), il renvoie une réponse EAP sans donnée. Le serveur retourne une réponse *EAP success*.

3.3.2.2 EAP-TTLS

EAP-TTLS (EAP - Tunneled Transport Layer Security ou tunnel de sécurité de la couche transport EAP) [39] est la version EAP signée par l'éditeur FUNK. Elle se différencie de la solution EAP-TLS par le fait que les certificats numériques ne sont pas nécessaires sur le poste client (optionnel). Le serveur s'authentifie auprès du client par un certificat et le client s'authentifie dans le tunnel par un couple identifiant/mot de passe, certificat, etc. selon la méthode d'authentification interne choisie (voir figure 3.2).

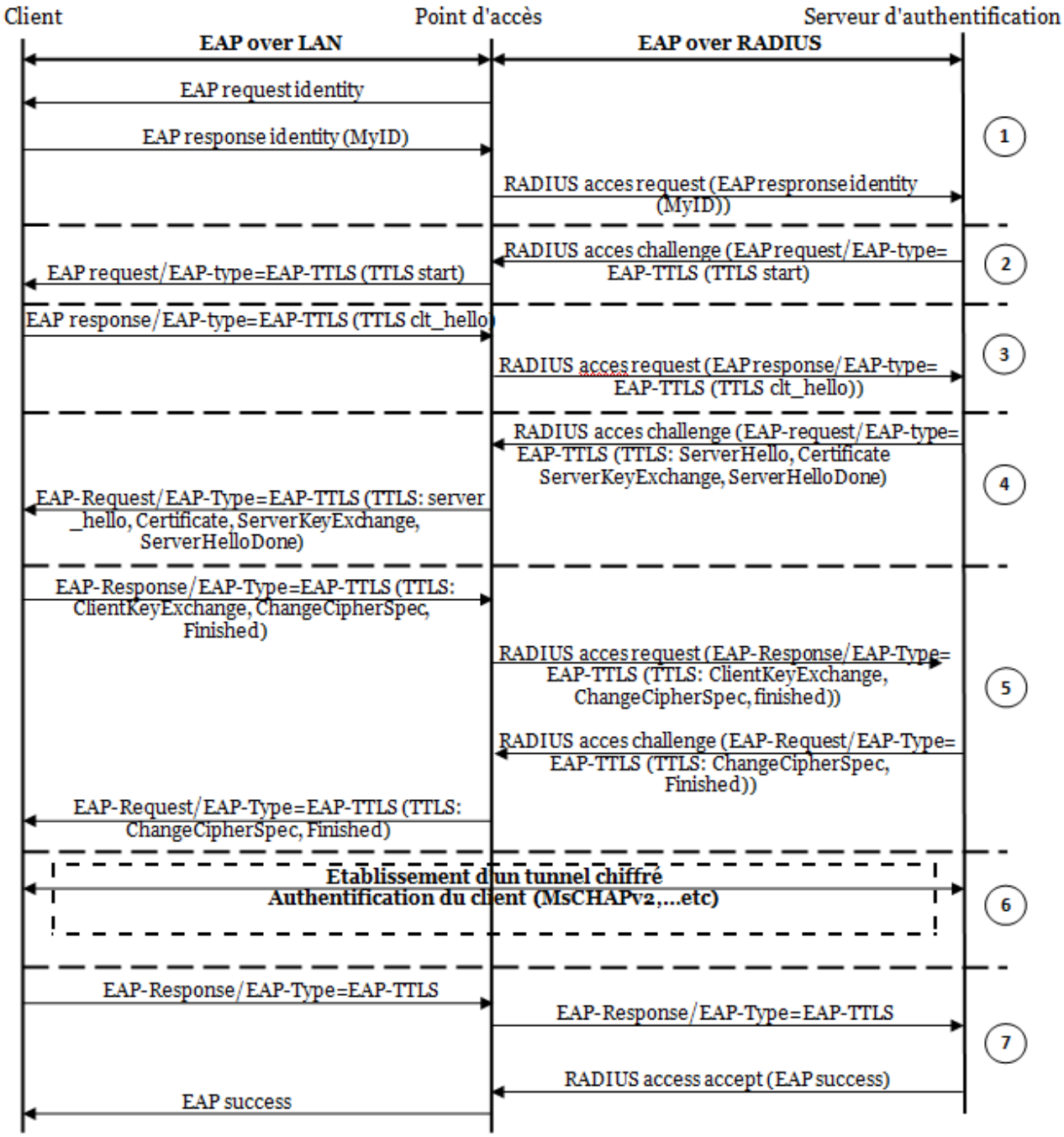

FIGURE 3.2 – Échanges EAP-TTLS dans un contexte IEEE 802.11 (en cas de succès)[39, 41].

Les échanges de 1 à 4. sont presque similaire à ceux d'EAP-TLS. Le client authentifie le serveur par l'intermédiaire d'un certificat (étape 4).
5. Cette étape diffère d'EAP-TLS, car le client n'a pas besoin de fournir de certificat pour s'authentifier, la clé qui sert à chiffrer la session peut donc être créée directement. À la fin de cette étape, le TLS handshake est terminé, les échanges suivants seront donc chiffrés par la clé de session.
6. L'établissement d'un tunnel TLS permet de chiffrer les échanges, le client fournit donc ses identifiants (login/mot de passe) au serveur en utilisant par exemple MS-CHAPv2.
7. Similaires à EAP-TLS.

L'argument de vente de FUNK est que les certificats PKI ne sont nécessaires que sur le serveur d'authentification, et non sur les postes clients. Cette solution est généralement considérée comme presque aussi sûre que EAP-TLS, tout en simplifiant le déploiement [40].

3.3.2.3 EAP-PEAP

PEAP [42] est un projet de RFC de l'IETF réalisé par Cisco Systems, Microsoft et RSA (Rivest Shamir Adelman) Security. PEAP utilise un certificat numérique pour l'authentification du serveur. Pour l'authentification utilisateur, PEAP supporte diverses méthodes d'encapsulation EAP au sein d'un tunnel TLS protégé.

Puisque la méthode PEAP est toujours utilisée conjointement avec une autre méthode EAP, on précise toujours le nom de cette méthode interne, par exemple PEAP-TLS ou PEAP-MD5. Toutefois, aux yeux du contrôleur d'accès et de tout observateur extérieur, une seule méthode d'authentification est utilisée : EAP-PEAP [17].

Le mode de fonctionnement est semblable à celui de EAP-TTLS (voir figure 3.3).

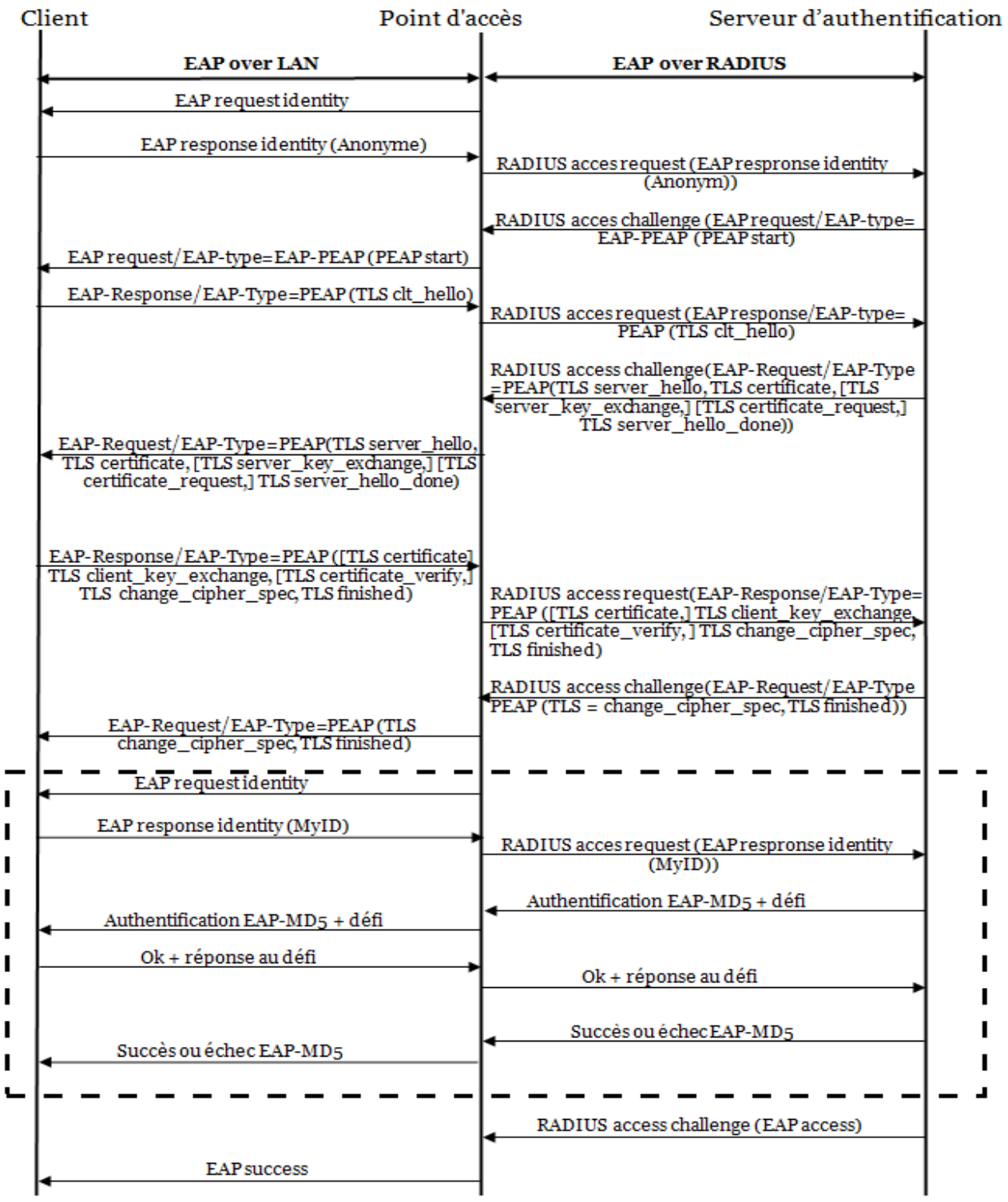

FIGURE 3.3 – Échanges EAP-PEAP-MD5 dans un contexte IEEE 802.11 (en cas de succès)[17, 43]

3.3.2.4 EAP-MD5

EAP-MD5 [44] est l'une des méthodes d'authentification les plus simples d'EAP, elle est très simple à mettre en place et son mécanisme d'authentification est semblable à la méthode CHAP [45]. Chaque utilisateur possède un mot de passe associé à un nom d'utilisateur qu'il utilise pour s'authentifié auprès d'un serveur d'authentification avec le mécanisme de défi/réponse. Comme l'illustre la figure 3.4, l'authentification avec EAP/MD5 se déroule comme suit :

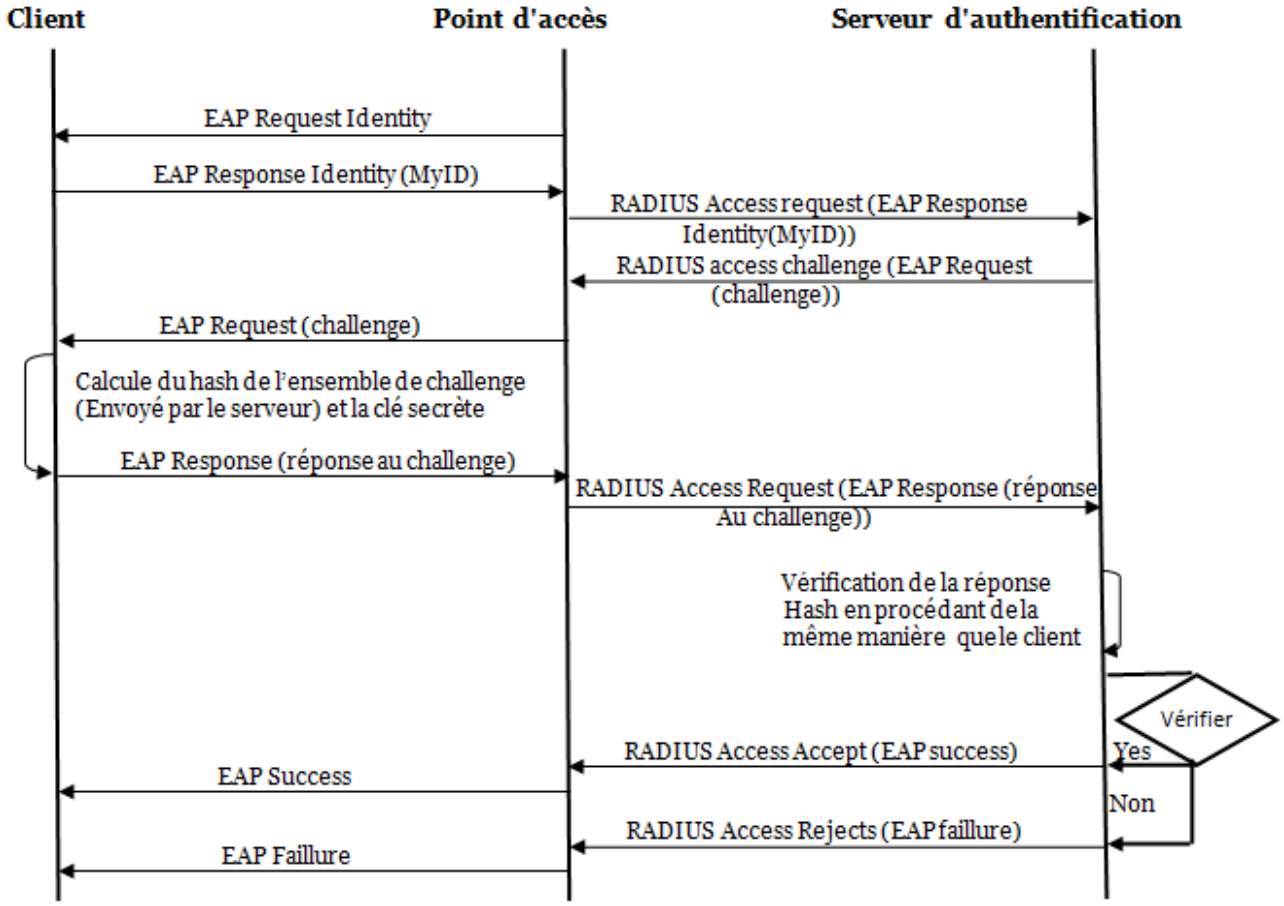

FIGURE 3.4 – Échanges EAP-MD5 dans un contexte IEEE 802.11 [41].

Le serveur d'authentification envoi un défi (Challenge) au client et celui-ci le chiffre via l'algorithme de hachage MD5 et le renvoi au serveur. À la réception de la réponse du défi, le serveur récupère dans sa base de donnees, le mot de passe correspondant au nom d'utilisateur du message reçu, et l'utilise pour faire le même calcul fait par le client, et si les résultats sont identiques, alors le serveur lui renverra un message *EAP success* indiquant la réussite de l'authentification au client, sinon il renverra un message *EAP faillure* indiquant l'échec de l'authentification [41].

3.3.2.5 Cisco LEAP

Cisco Systems a développé sa propre méthode EAP de manière à pouvoir proposer une solution complète (cartes clients, points d'accès, serveur Radius). Malgré tout, les équipements Cisco supportent d'autres types d'authentification (PEAP, EAP-TLS. Etc.).

Cisco LEAP (Lightweight) s'appuie sur une authentification, via un serveur, de type « challenge/réponse » et basée sur un couple « identifiant/mot de passe ». Avec LEAP, l'authentification mutuelle repose sur un secret partagé : une clé dérivée du mot de passe de connexion de l'utilisateur, qui n'est connu que du client et du serveur.

Le serveur RADIUS envoie au client un test d'authentification. Le client utilise un algorithme de hachage à sens unique sur le mot de passe fourni par l'utilisateur, pour générer une réponse au test avant son envoi au serveur RADIUS. À partir des informations de sa base de données utilisateurs, le serveur RADIUS crée sa propre réponse et la compare à celle du client. Lorsque le serveur RADIUS a authentifié le client, le processus recommence dans l'autre sens pour permettre au client d'authentifier le serveur RADIUS. Une fois les deux processus achevés, le client reçoit un message de confirmation EAP-Success du serveur RADIUS [46].

3.3.2.6 EAP-FAST

EAP-FAST (EAP-Flexible Authentication via Secure Tunneling) [37] est une autre méthode d'authentification par tunnel, publiée en février 2004 par Cisco sous la forme d'un draft IETF. Cisco vise à résoudre une faille de sécurité dans son protocole propriétaire LEAP (les mécanismes d'attaque par dictionnaire utilisés avec succès contre LEAP). Il est très similaire à TTLS : un tunnel est créé pour protéger une authentification interne. Mais il y a une différence de taille : le tunnel peut être établi avec un algorithme de cryptage symétrique et non avec TLS. Ceci présente essentiellement deux intérêts :

- Il n'est pas nécessaire d'installer un certificat sur le serveur ;
- La création du tunnel est plus rapide avec un algorithme symétrique qu'avec TLS (d'où le jeu de mot avec fast, qui signifie « rapide ») [40, 17].

3.3.2.7 EAP-SIM

EAP-SIM (EAP-Suscriber Identity Modules) [48] permet à un utilisateur de s'identifier grâce à la carte SIM de son téléphone portable GSM. Celle-ci peut être connectée à l'ordinateur via une clé USB, par exemple, ou directement intégrée dans l'adaptateur WiFi. Pour que l'identification puisse fonctionner, le serveur d'authentification doit être relié à l'opérateur

mobile de l'utilisateur : il ne sert alors que d'intermédiaire entre le client et le serveur d'authentification de l'opérateur mobile. Cette solution a sans doute peu d'intérêt pour la plupart des entreprises dans le contexte d'un réseau WiFi (à part pour les opérateurs mobiles qui déploient des hotspots), mais il s'agit encore d'une nouvelle preuve de la convergence entre la téléphonie et les technologies de l'information. Par ailleurs, d'autres drafts ou RFC ont été écrits pour des méthodes d'identification liées à la téléphonie : EAP-SIM 6 pour l'identification SIM passant par un réseau IPv6 (Internet Protocol version 6) et EAP-AKA (Authentification and Key Agreement) pour l'identification par un réseau UMTS [17].

3.3.3 Analyse critique

Toutes les méthodes EAP qui ne génère pas une clé secrète pour le cryptage de la session, seules ne peuvent pas résister contre une attaque de type Man-In-The-Middle qui est décrite comme suit :

Un pirate s'intercale entre un suplicant et un point d'accès et va servir juste d'un relai de paquet EAP entre les deux extrémités (le pirate n'a pas besoin de comprendre quoi que sa soit du contenu de paquet qu'il transporte). Une foi que les deux extrémités s'authentifie (avec certificat ou mot de passe), un paquet de type EAP succès va donc être délivré par le serveur d'authentification autorisant le client à s'accéder au réseau, le pirate ne relai pas ce paquet au suplicant, il le garde chez lui et il configure son adaptateur WiFi avec l'adresse MAC (spoofing d'adresse MAC) du suplicant et accède au réseau.

Voici un exemple de cette attaque sur une méthode à base de certificat :

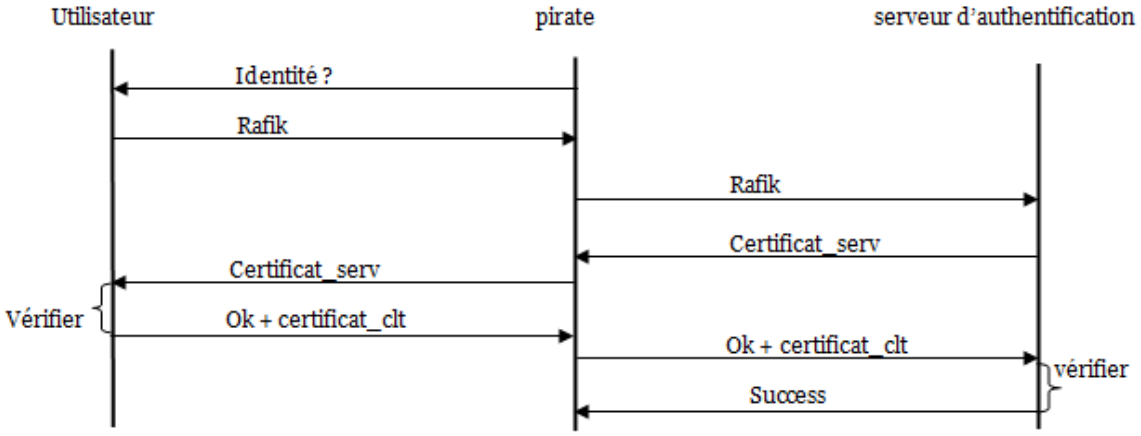

FIGURE 3.5 – Exemple d'attaque MITM contre les méthodes EAP à base du certificat.

On voit que le pirate n'a aucunement besoin de comprendre quoi que ce soit au contenu des

paquets EAP qu'il transporte, or le pirate fini par se faire accepter. Le seul mécanisme pour lutter contre cette attaque et le cryptage de la session avec une clé qui sera générée durant l'exécution de la méthode d'authentification. Alors la méthode d'authentification à choisir pour le protocole de sécurité 802.11i doit être génératrice de clé. Sachant que le pirate ne comprend pas le contenu des paquets EAP échangés entre le suplicant et le serveur d'authentification alors il ne va pas connaitre la clé générée et qui serai utilisé pour le cryptage de la session, ce qui rend cette attaque inutile. Les méthodes à base de tunnel (TLS, TTLS, PEAP, FAST) sont des méthodes génératrice de clés, une raison pour les utilisés.

La méthode EAP-MD5 offre l'avantage de ne pas nécessiter beaucoup de ressources pour son traitement. De plus elle n'exige pas d'infrastructure de gestion de certificats ou de clés publiques (comme le requiert EAP-TLS), mais elle n'est pas utilisée aujourd'hui car elle est reconnue comme vulnérable aux attaques par dictionnaire et aux attaques par force brute vu qu'elle ne prévoit aucun mécanisme pour changer la clé. 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) d'où elle est sensible aux attaques de type Man-In-The-Middle (MITM).

Le fonctionnement de la méthode LEAP est similaire au fonctionnement de d'EAP-MD5 donc elle est vulnérable aux attaques par dictionnaire. LEAP contrairement à EAP-MD5 assure l'authentification mutuelle d'où la possibilité de détecter les faux serveurs.

La méthode EAP-TLS offre un niveau de sécurité élevé puisqu'elle permet l'authentification mutuelle. Elle est robuste face aux attaques de l'homme du milieu (Man-In-The-Middle), puisqu'elle repose sur la cryptographie asymétrique (certificats : avec les certificats il n'est pas possible d'usurper une identité donc un pirate ne peut pas se comporter comme un AP légitime). L'inconvénient majeur de cette méthode est qu'elle repose sur une infrastructure de gestion de clé (PKI - Public Key Infrastructure) pour assurer la gestion des certificats côté client et côté serveur. Or les PKI sont extrêmement coûteuses et complexes en termes de gestion et de maintenance. En outre, il est d'usage, pour les certificats électroniques, de vérifier la non révocation d'un certificat auprès d'une autorité ou d'un serveur miroir avant de l'utiliser pour authentifier l'entité.

La méthode EAP-PEAP répond aux problèmes de sécurité EAP en créant préalablement un canal sécurisé dont le cryptage et l'intégrité sont assurés par TLS. Ensuite, une nouvelle négociation EAP est établie avec une autre méthode EAP (tel que MD5, TLS,etc.) pour

authentifier la tentative d'accès du client, ce qui offre une sécurité très élevé.

La méthode EAP-PEAP offre un avantage présenté par le fait que le client peut être authentifié par mot de passe, on supprime donc la complexité de gestion liée aux certificats des clients, tout en proposant une authentification mutuelle, mais dans une grande entreprise dont les puissants matériels sont disponible vaut mieux utiliser des certificats pour authentifié les suplicants.

La différence principale entre EAP-PEAP et EAP-TTLS vient de la manière d'encapsuler les échanges lors de la deuxième phase. Pour EAP-PEAP, les données échangées entre le client et le serveur au travers du tunnel TLS sont encapsulées dans des paquets EAP. EAP-TTLS utilisent des AVP (Attribute-Values Pairs) encapsulées dans des paquets EAP-TTLS, le format AVP d'EAP-TTLS est compatible avec le format AVP du serveur RADIUS, ce qui simplifie les échanges entre le serveur EAP-TTLS et le serveur RADIUS qui contient les informations relatives aux utilisateurs, dans le cas où les informations ne sont pas directement stockées sur le serveur EAP-TTLS. PEAP et TTLS ont une vulnérabilité un peu spécial de type Man-In-The-Middle : le pirate peut essayer de créer un tunnel avec le client et un tunnel avec le serveur. Il peut alors avoir accès à la méthode d'authentification « interne » utilisée. Voici comment il peut procéder :

- Le pirate configure sont poste pour se comporter comme un AP (même SSID qu'un AP légitime) ;
- Lorsqu'un client cherche à se connecter à lui avec la méthode PEAP ou TTLS, le pirate ne redirige pas encore les paquets à un AP légitime. Au contraire, il se comporte comme le serveur d'authentification et envoie un faux 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 créé entre lui et le pirate pour négocier la méthode EAP interne ;
- À ce moment, le pirate négocie lui-même un tunnel PEAP ou TTLS avec le serveur d'authentification, via un AP légitime. Au sein de ce tunnel, il redirige tout le trafic EAP interne et fini par accéder au réseau.

À l'issue de cette attaque, non seulement le pirate est accepté complètement sur le réseau, avec ses propres clés de cryptage, mais en plus il a vu passer la négociation EAP interne en clair.

Une solution pour éviter cette attaque consiste à mettre en place un certificat sur le poste de chaque utilisateur et à configurer le serveur d'authentification pour qu'il vérifie bien la

validité du certificat. Dans ce cas, on perd l'un des avantages de PEAP et TTLS qui était d'éviter la lourdeur administrative d'EAP/TLS. Cependant, cela empêchera le pirate de créer un tunnel avec le serveur d'authentification. Le client doit aussi vérifier le certificat du serveur et rejeter ainsi chaque faux certificat.

La méthode EAP-FAST est capable de créer le tunnel d'authentification en utilisant un algorithme symétrique, il permet de se dispenser du certificat du serveur d'où la souplesse du système (comme il y'a pas des opérations de gestion des certificats tel que l'ajout des certificats sur chaque station). Mais un nouveau problème se pose : pour établir un tunnel avec un algorithme symétrique, il faut que le serveur partage une clé avec chaque clientl ; Ces clés sont stockées dans des fichiers protégés par un mot de passe : les PAC (Protected Access Credentials). Pour mettre en place un système basé sur EAP-FAST, il faut donc commencer par utiliser un outil pour générer un PAC pour chaque utilisateur et installer le bon PAC sur le poste de chaque utilisateur. On se rend donc compte que ce système est tout aussi lourd à gérer qu'EAP-TLS.

3.3.4 Comparaison des différentes approches

Nous présentons ci-dessus un tableau comparatif des méthodes d'authentification EAP citées précédemment pour le standard 802.11i :

Méthode / Critère	MD5	TLS	TTLS	PEAP	FAST
Authentification du serveur	Non	Cetificat	Certificat	Certificat	login/mot de passe
Authentification de client	Hachage de mot de passe	Certificat	Certificat ou login/mot de passe	Certificat ou login/mot de passe	login/Mot de passe
Authentification mutuelle	Non	Oui	Oui	Oui	Oui
Génération automatique clés	Non	oui	Oui	Oui	Oui
Certificat du serveur	Non	Oui	Oui	Oui	Oui
Certificat du client	Non	Oui	Oui	Oui	Oui
Protection de l'identité de l'utilisateur	Non	Non	Oui	Oui	Oui
Protection contre les attaques de dictionnaire	Non	Oui	Oui	Oui	Oui
Protection contre les attaques MITM	Non	Oui	Oui	Oui	Oui
Protection contre le rejeu	Non	Oui	Oui	Oui	Oui

TABLE 3.1 – Comparaison des principales méthodes EAP.

Nous pouvons déduire que toutes les méthodes proposées souffrent d'un manque et d'insuffisances, malgré ce qu'elle offre et apporte comme avantages.

3.4 Le 4-way Handshake

La génération et la distribution de clés gérées par le 4-way Handshake est vulnérable à l'attaque de déni de service. En effet, le Massage-1 contenant la valeur aléatoire ANonce est envoyé en clair par le point d'accès, et comme il n'existe pas de mécanismes de protection à ce niveau, un attaquant est capable de capturer et d'usurper ce message. Il offre ainsi l'opportunité à l'attaquant d'inonder le client avec ce message, et empêcher totalement ou partiellement le déroulement de la phase. C'est la problématique traitée les diverses solutions décrites dans la section ci-dessous(section 3.4.1). Deux formes d'attaque existent [49, 50, 51] :

1) Attaque aprés le Message-1 :

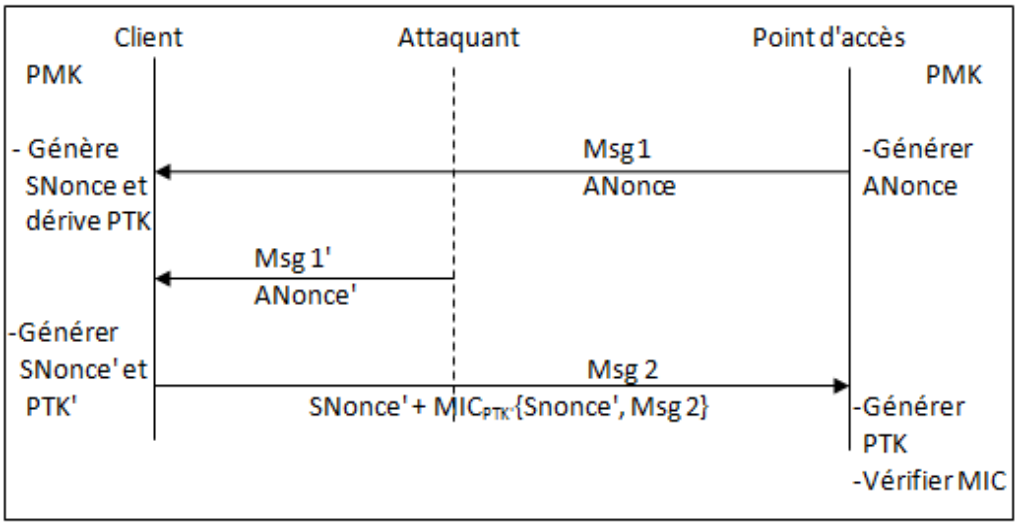

FIGURE 3.6 – Illustration de l'attaque après le Message-1.

La figure 3.6 montre l'attaque du 4-way handshake avec le Message-1 sur le client. L'attaquant envoi un message forgé qui contient une nouvelle valeur ANonce' au client, avant qu'il ait le temps d'envoyer le Message-2 au point d'accès. Cela cause au client de régénérer une nouvelle valeur SNonce', et d'en tirer une nouvelle valeur PTK soit PTK', à base de ANonce' reçu de l'attaquant. Lorsque le client envoi le Message-2 au point d'accès, la vérification du MIC va échouer car PTK est différente de PTK'. Par conséquent, le 4-way Handshake est incomplet [49, 50].

2) Attaque aprés le Message-2 :

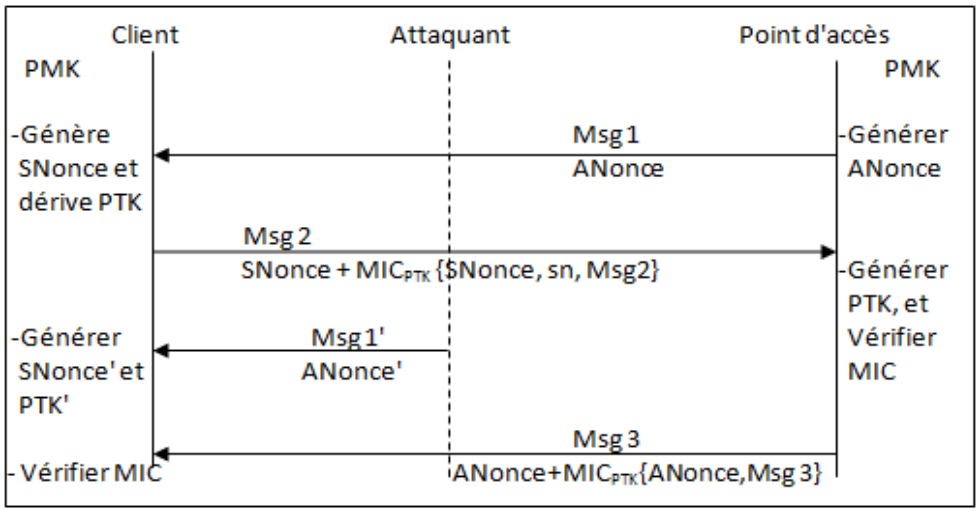

FIGURE 3.7 – Illustration de l'attaque après le Message-2.

Dans cette situation (Figure 3.7), l'attaquant envoi un Message-1 forgé après l'envoi du Message-2 par le client. Dans ce cas, le client est obligé de générer un nouveau SNonce' et dériver une nouvelle PTK', basé sur le nouveau ANonce' de l'attaquant, et enfin stocke la nouvelle PTK'. Une fois que le client a reçu le message-3 du PA, il vérifiera son MIC avec la PTK'. Etant donné que la nouvelle PTK' est différente de la PTK utilisée par le PA, la vérification du MIC échoue, et le client ne parvient à être authentifier. L'attaquant peut également choisir d'inonder le client avec le Message-1 usurpé. En conséquence, le client connaitra un épuisement de mémoire, car il a besoin de ré-stocker la nouveau ANonce, SNonce et PTK à chaque fois qu'il reçoit le message-1 usurpé [50].

3.4.1 Solutions existantes

3.4.1.1 Chiffrement de ANonce

Jafri et Li Ho [52] proposent une solution qui repose sur le chiffrement de la valeur ANonce avant son envoi, et ceci en utilisant le chiffrement AES (Voir Figure 3.8).

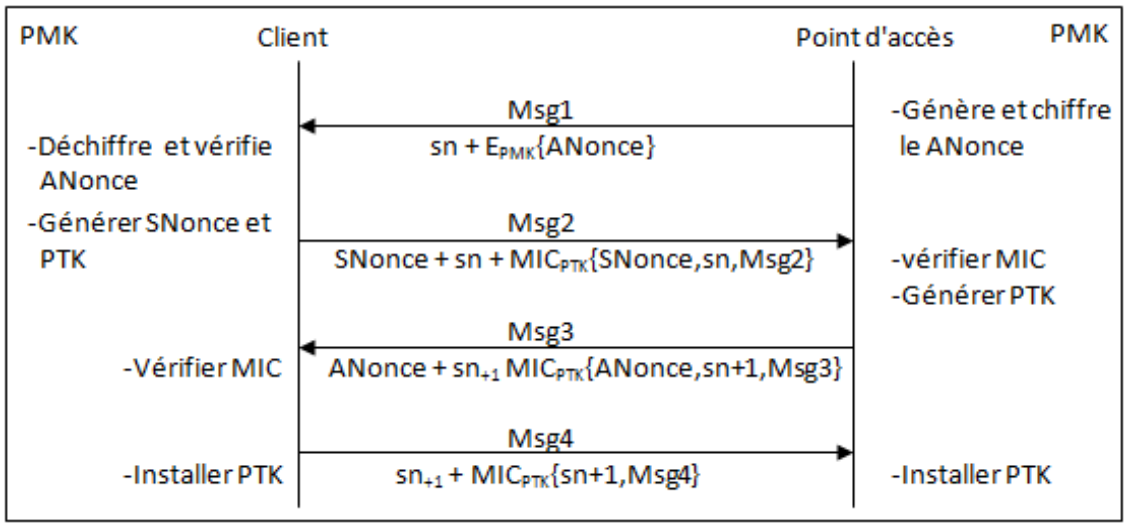

FIGURE 3.8 – Chiffrement de ANonce

À l'étape initiale de 4-way Handshake, le point d'accès (PA) et le client devraient déjà avoir possession de la clé PMK. Lorsque le PA génère ANonce, il l'utilisera comme clé pour chiffrer cette valeur avant de l'envoyer au client. Une fois que le Message-1 est reçu par le client, il va déchiffrer le texte chiffré pour obtenir le ANonce. Si la PMK des deux parties sont les mêmes, le texte chiffré sera bien déchiffré et qui donnera une valeur correcte de ANonce. Ensuite le ANonce sera conservé et utilisé pour calculer la clé PTK.

Discussion :

La proposition de chiffrer le ANonce du point d'accès permet au client de recevoir et de stocker seulement les messages légitimes. De cette façon, le chiffrement de ANonce peut éliminer la menace d'épuisement de mémoire et l'échec de 4-way Handshake causé par le Message-1.

Le cryptage ne concerne que les Message-1, et ne nécessite pas le calcul du MIC et la vérification de l'intégrité, c'est l'avantage de cette solution vu que le temps pris par le chiffrement est petit, qui permet au client de se débarrasser des messages d'un attaquant et de ne pas les traiter en offrant moins de charge. Mais la présente solution présente une nouvelle vulnérabilité, la PMK utilisée est vulnérable, il est possible à un attaquant d'obtenir cette clé en capturant les messages-1 lors de 4-way Handshake, et d'effectuer un attaque de dictionnaire ou force brute : car il est en possession du chiffré $E_{PMK}\{ANonce\}$ et de ANonce envoyé en clair dans le message-3.

La solution proposée à travers cet article peut dissuader l'attaque de déni de service (Dos) de Message-1 de 4-way Handshake, toutefois, elle pourrait ouvrir la possibilité à un attaquant d'obtenir la clé PMK et de compromettre la sécurité globale.

3.4.1.2 Le 2-way Handshake amélioré

Liu et Al [53] proposent un nouveau schéma pour remplacer le 4-way Handshake original nommé 2-way Handshake, basée sur deux messages MsgA et MsgB (voir Figure 3.9).

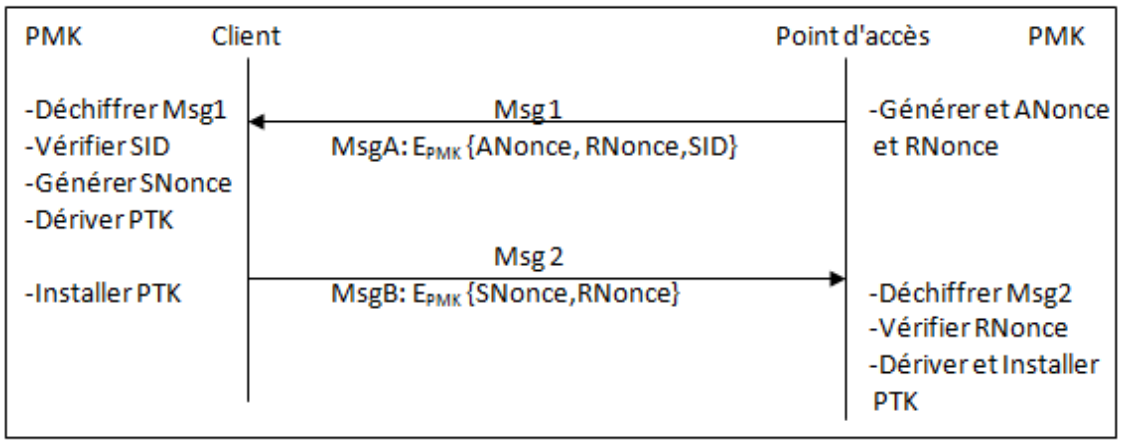

FIGURE 3.9 – 4-way Handshake amélioré

Le MsgA est envoyé par le point d'accès chiffré avec la PMK contenant ANonce et RNonce génères à son niveau, ainsi le SID (Station IDentifier : information d'identification du client c.à.d. l'adresse MAC). Le ANonce est le même que l'original de 4-way Handshake, tandis que

le RNonce est un grand nombre aléatoire généré par le point d'accès.

Le client en recevant le MsgA, il le déchiffre et récupère ses informations, pour comparer le SID reçu avec son propre SID, afin de vérifier si le point d'accès est légitime. Si c'est le cas, il génère son SNonce puis calcule sa PTK à base de ANonce reçu.

Un MsgB sera envoyé par la suite au PA contenant le SNonce du client et le RNonce reçu dans le MsgA, le tout chiffré avec sa clé PMK en utilisant le même algorithme de chiffrement utilisé par le PA. Ensuite, le PA à besoin seulement de vérifier la valeur de RNonce reçu et celle généré précédemment avant de dériver et d'installer la PTK.

Discussion

Ce protocole ne comporte pas de MIC, donc il utilise moins de traitement en réduisant l'échange d'information entre le client et le point d'accès. Mais il repose sur la vérification de SID par le client et de RNonce par le point d'accès. Les MsgA et MsgB sont chiffrés, ce qui empêche l'attaquant de forger ces messages pour lancer un déni de service (DoS), il n'y pas une fuite d'informations à travers l'attaque passive, les deux messages comportent tous les deux un Nonce, ce qui peut atténuer l'attaque par rejeu.

La sécurité de ce protocole dépend de la PMK comme elle est utilisée directement pour chiffrer les messages. Ainsi, la force de cette clé doit être suffisamment solide pour résister au taux de réussite de l'attaque par dictionnaire ou par force brute. La solution repose principalement sur le chiffrement des deux messages, un chiffrement symétrique qui consomme en temps de traitement, car chaque entité est contraint et forcé à chiffrer et à déchiffrer pendant la phase de 4-way Handshake.

3.4.1.3 Authentification de Message-1

He et Mitchell [49] proposent, comme c'est illustré par la figure 5, une méthode d'authentification de Message-1 pour assurer son intégrité. Le concept de base est d'ajouter un MIC au Message-1 du point d'accès, qui empêchera l'attaquant de forger ce dernier.

Comme il y'a un certain secret commun (PMK) partagé entre le point d'accès et le client, il est utilisé par le PA pour dériver une première clé PTK' avec une valeur spécifique Nonce, et qui est ensuite utilisé seulement pour calculer le MIC sur le Message-1.

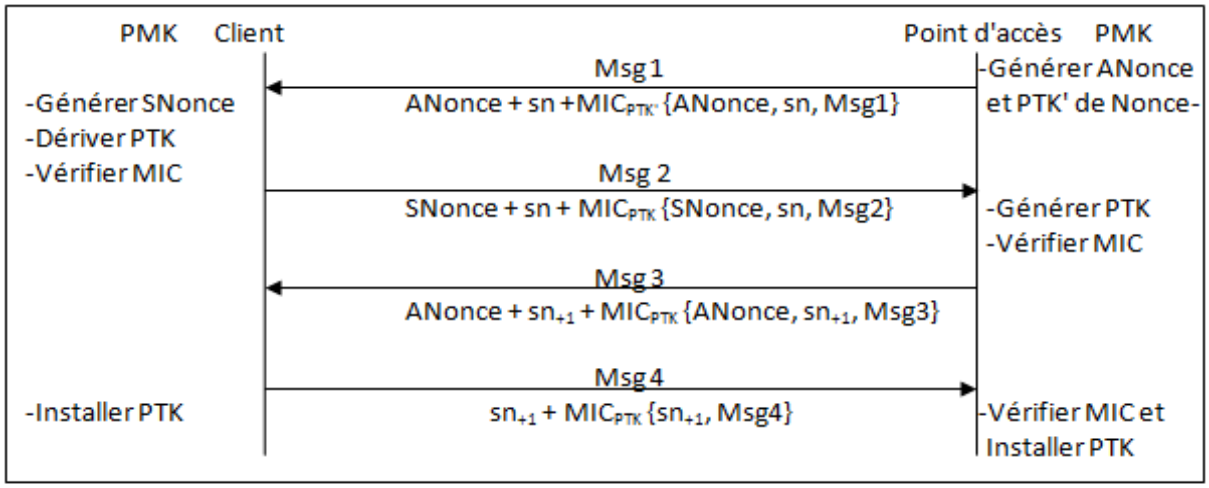

FIGURE 3.10 – Authentification de Message-1

Le Message-1 et le Message-3 se ressembleront, et un bit de sécurité intégré aux messages aura le rôle de les distinguer les.

Discussion

Si la PMK est générée grâce à la phase de l'authentification de 801.1x, elle sera à l'abri des attaquants et résoudrait le problème. Par contre, si ce n'est pas le cas et que la PSK ou une PMK cachée (une clé partagée secrètement) est utilisée pour le calcul de MIC, le Message-1 authentifié est toujours vulnérable aux attaques par rejeu, de fait que cette clé est statique pour une durée relativement longue. Elle impose au PA d'accroitre le numéro de séquence afin de renforcer le contrôle des messages reçus pour se défendre contre les attaques par rejou.

L'authentification de Message-1 permettra au client de traiter que les messages authentifiés qui lui sont adressés, ce qui évite l'attaque par inondation.

3.4.1.4 Réutilisation de Nonce

Dans cette méthode proposée par **He et Mitchell** [49], le client réutilisera les mêmes valeurs de SNonce jusqu'a la fin de 4-way Handshake légitime, et que la PTK soit installée dans les deux cotés (client et point d'accès). Cet approche nécessite que le client stocke le SNonce, et en tire une PTK basé sur le SNonce stocké et le ANonce reçu ; quand il reçoit le Message-3 du point d'accès, il dérive la PTK encore une fois de SNonce stocké et de ANonce' reçu de Message-3 pour vérifier son MIC.

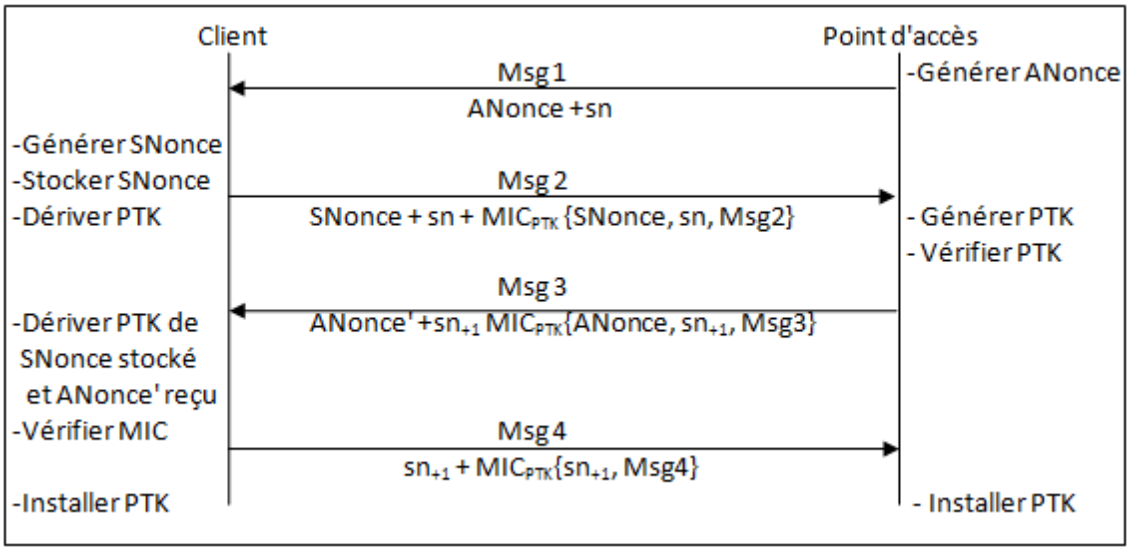

FIGURE 3.11 – Réutilisation de Nonce

Discussion :

La solution est robuste contre l'attaque d'épuisement de la mémoire, le client n'est pas obligé de stocker à chaque fois le SNonce généré pour chaque Message-1 reçu. Il besoin seulement de son premier SNonce généré.

Cependant, plus de puissance de calcul sur le coté de client dû au fait que le calcul de la PTK est effectuée deux fois. De plus, un attaquant est capable de jouer le Message-1 en inondation sur le client, elle pourra conduire à l'épuisement CPU et au blocage du 4-way Handshake.

3.4.1.5 Solution statique et dynamique du 4-way Handshake :

Rango et Al [50] proposent trois solutions statiques pour le 4-way Handshake, et une solution Dynamique qui s'appuie sur ces trois solutions.

a) Solution statique :

Sa méthodologie est similaire à la méthode réutilisation de Nonce décrite à la section 3.4.1.4, le client ne stocke pas la valeur de PTK. Au lieu de cela, il stocke le SNonce et recalcule la PTK à base de SNonce stockée et de ANonce contenant dans le Message-3.

Discussion :

La solution évite les risques de l'épuisement de mémoire en évitant de stocker que le SNonce, par contre, il peut y avoir un épuisement de CPU lors de calcul de la PTK.

b) La solution statique avec une variante compromise :

Cette solution nécessite au client de stocker les trois valeurs : ANonce, SNonce et PTK (voir figure 3.12). À la réception de Message-3, le client compare le ANonce reçu avec le ANonce stocké, si les deux correspondent, il procède à la vérification du MIC de Message-3 en utilisant la PTK stockée. Si ce n'est pas le cas, la PTK sera calculé avec la nouvelle valeur ANonce reçu pour vérifier le MIC.

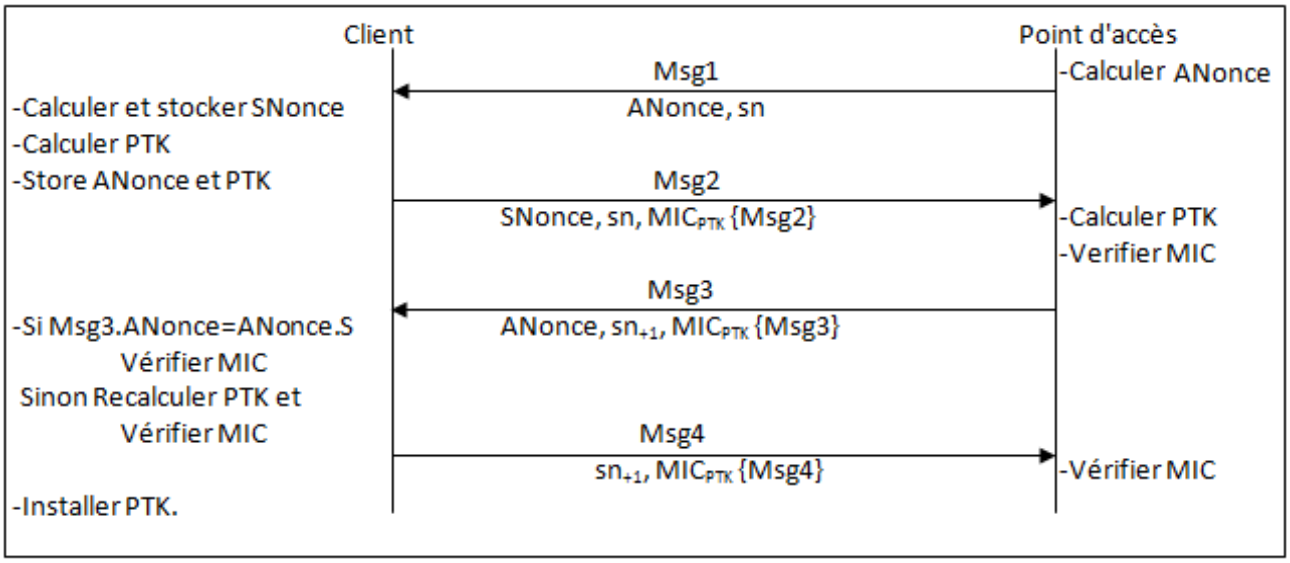

FIGURE 3.12 – Solution statique avec une variante compromise

Discussion :

Cette solution se base sur le stockage de trois valeurs nécessaires dans le protocole 4-way Handshake, ce qui provoque un épuisement de mémoire, non seulement pendant un scenario d'attaque de déni de service, mais aussi au cours du scenario normal sans attaque. Par contre, cette solution diminue le calcul de PTK après la réception de Message-3, ce qui réduit le risque de l'épuisement CPU. Le Message-1 reste toujours sans protection contre le déni de service.

c) Solution statistique avec une variante compromise et libération de mémoire :

Cette solution porte une amélioration à la solution présentée précédemment (solution b), dans le but de résoudre l'épuisement mémoire qu'elle peut provoquer sans qu'une attaque soit menée contre cette dernière. Elle consiste à libérer l'espace mémoire associe au stockage de ANonce et SNonce si la station ne reçoit pas de nouveaux Message-1. En d'autres termes, si le client reçoit un Message-3 après l'envoi de Message-2, il peut supprimer ANonce et SNonce. A ce point, elle peut vérifier la valeur de MIC sans vérifier la valeur de ANonce.

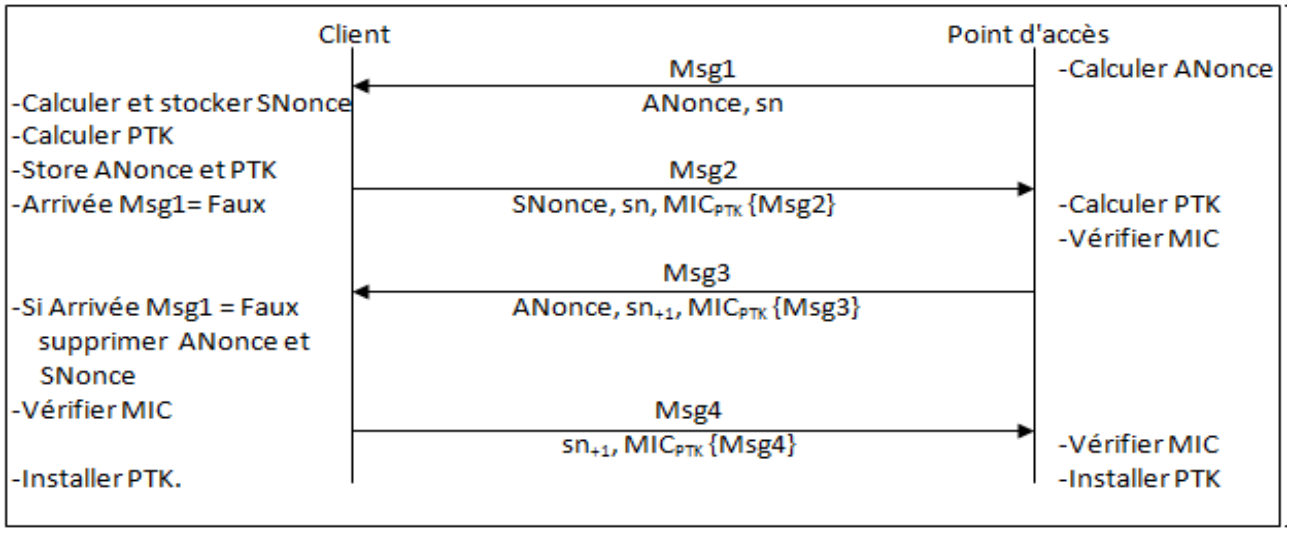

FIGURE 3.13 – Solution statique avec une variante compromise et libération mémoire

Discussion :

La solution proposée essaye de réduire le stockage mémoire quand un scenario d'attaque n'est pas présent. Pour utiliser ce type de solution, quelques mécanismes sont nécessaires pour avoir conscience des scenarios d'attaques, afin de libérer de l'espace mémoire. Elle est moins performante que le 4-way Handshake original.

d) Solution dynamique :

C'est une solution qui unifie les solutions statiques, propose d'adapter un module logiciel intelligent supplémentaire qui surveille les paramètres des systèmes : mémoire, contrôle la charge CPU et les niveaux de seuil pour basculer d'une solution à une autre sur la base de la valeur du seuil.

Discussion :

La solution peut éviter avec succès les attaques par déni de services, et les attaques par saturation, mais l'intégration d'un module logiciel peut amener à d'autres problèmes, par exemple, le taux de traitement et la charge CPU nécessaire pour le fonctionnement de module avec les entités impliquées, son intégration avec le protocole 4-way Handshake.

3.4.1.6 Mécanisme du cookie

Eum et Al [54] éliminent le stockage des paramètres ANonce et la PTK correspondante sur le coté du client, afin d'atténuer à l'attaque épuisement de mémoire, qui engendre un blocage de 4-way Handshake.

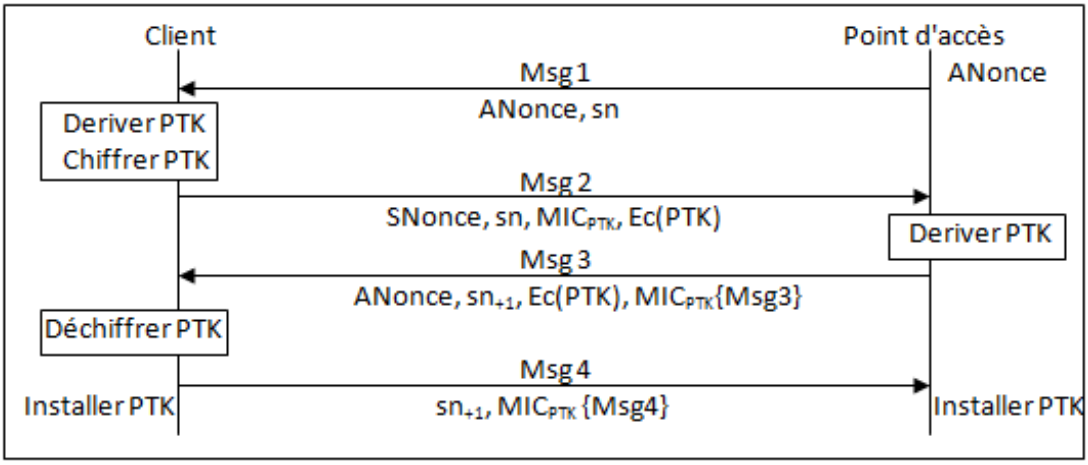

FIGURE 3.14 – Chiffrement de cookie

Au début, le point d'accès envoi le Message-1 au client avec le nombre aléatoire généré ANonce. Lorsque le client reçoit ce message, il génère à son tour son nombre aléatoire SNonce, puis dérive sa clé PTK. Le client ne stocke pas le SNonce et la PTK, mais consiste de chiffrer la PTK à l'aide d'une clé secrète propre au client, de mettre le chiffré et le SNonce du client dans un cookie, et d'envoyer le tout au point d'accès (PA) dans le Message 2. Un MIC est calculé à l'aide de PTK est ajouté au Message 2.

Le PA, après avoir reçu le Message 2, il tire également sa PTK de son ANonce généré, et en utilisant le MIC, il peut vérifier qu'il a la même PTK que celle dérivée par le client. Le Message-3 est envoyée par le PA contenant le même cookie contenu dans le Message-1, ainsi que le ANonce du client, et en ajoutant toujours un MIC pour assurer l'intégrité de ce dernier. Quand le client reçoit le cookie, il déchiffre à l'aide de la même clé secrète utilisée pour chiffrer la PTK dérivée à son niveau, puis il vérifie le MIC de message reçu avec la PTK déchiffrée. Un Message-4 est envoyé au point d'accès comme un message d'acquittement, que PTK est installé correctement.

Discussion :

La proposition élimine le stockage des paramètres ANonce et PTK, un attaquant ne peut pas mener une attaque de déni de service de type épuisement mémoire au niveau du client. Cependant, elle a besoin de puissance du calcul pour le processus de chiffrement et de déchiffrement du cookie. En plus, elle nécessite que le client ait une clé secrète.

Bien que cette solution résout l'épuisement mémoire, mais elle expose le 4-way Handshake à d'autres vulnérabilités. En effet, la clé PTK est envoyée dans le cookie à travers le Message-2

et le Message-3. Un adversaire peut intercepter le cookie et ensuite essayer de le déchiffrer, grâce à une attaque par dictionnaire où force brute sur la clé secrète.

Le temps pris par le chiffrement et le déchiffrement du cookie est très petit, donc acceptable, et il peut être négligé. Par contre, la vulnérabilité du blocage est toujours présente, car l'attaquant peut inonder le client avec le Message-1, ce dernier n'est pas authentifie ; le client dérive et chiffre la PTK et inonde à son tour le Point d'Accès (PA) avec le Message-2, ainsi un épuisement de calcul CPU peut être provoqué au niveau des deux côtes.

3.4.1.7 Three-way Handshake

Altunbasak et Owen [55] proposent une version modifiée de 4-way Handshake (voir figure 3.15), elle supprime le dernier message-4. Le point d'accès attend une période de temps après l'émission de Message-3 à la station. Si le point d'accès ne reçoit pas une copie du Message-2 de la station durant cette période, il installe la PTK. La station installe ses clés après la réception du message-3 du PA. Par contre, si le PA reçoit des Message-2, il réémit le Message-3 après un certain nombre de fois. Pareil pour la station, qui attend une période de temps après réception du Message-3, avant d'installer la PTK.

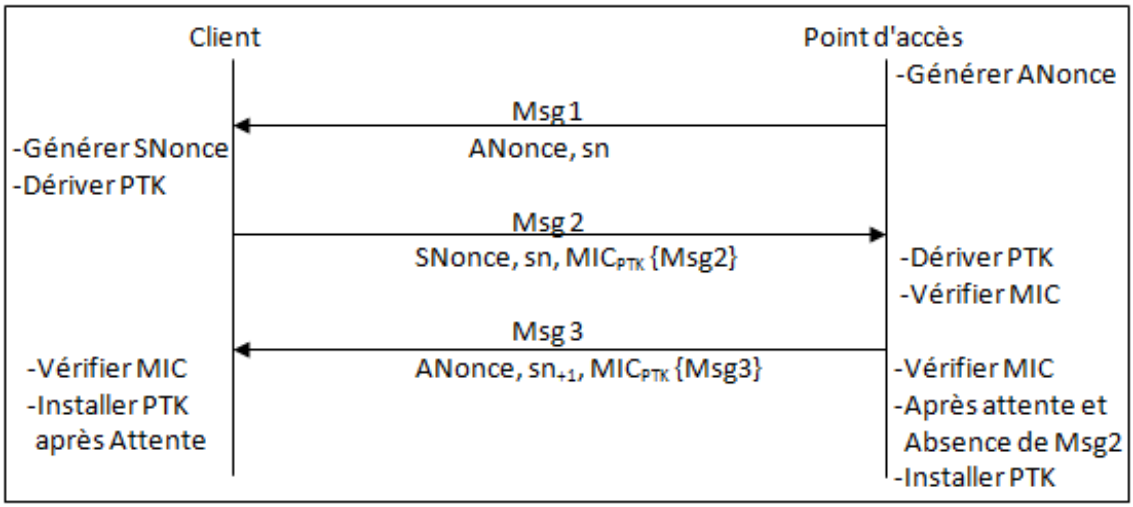

FIGURE 3.15 – Three way Handshake

Discussion :

Bien que la solution adoptée par les auteurs permet de réduire le nombre de message à trois au lieu de quatre du 4-way Handshake original, qui réduit la charge de traitement mais elle ne résout pas l'attaque du blocage, qui existe toujours. Les auteurs n'ont pas traité cette attaque de déni de service, le Message-1 constitue toujours une menace, car ce dernier ne peut pas être pas authentifié et aucun contrôle ne se fait sur celui-ci. Un attaquant peut inonder le

client avec ce Message-1, et peut bloque définitivement le 4-way Handshake.

L'idée de supprimer le Message-4 de 4-way Handshake présente une autre forme d'attaque de type déni de service, car un attaquant peut envoyer des Message-2 pendant la durée d'attente du PA jusqu'a le nombre de fois autorisée, pour le bloquer ensuite. Pareil pour la station, jusqu'a ce que le PA et la station ne sont plus autorisés à s'échanger des messages. En outre, le temps d'attente oblige les deux entités à attendre son expiration pour pouvoir installer les clés.

3.4.1.8 Two way Handshake

Altunbasak et Owen [24] proposent un autre protocole pour réduire le nombre de messages échangés pour établir une PTK. Un nombre aléatoire est utilisé ainsi que deux compteurs. Le point d'accès génère un ANonce et calcule après F(ANonce), où F() est une fonction connu publiquement ; il utilise le résultat de cette fonction dans le calcul de la PTK au lieu de SNonce du client, ce qui permet au PA de calculer la PTK avant l'envoi du premier Message-1 à la station.

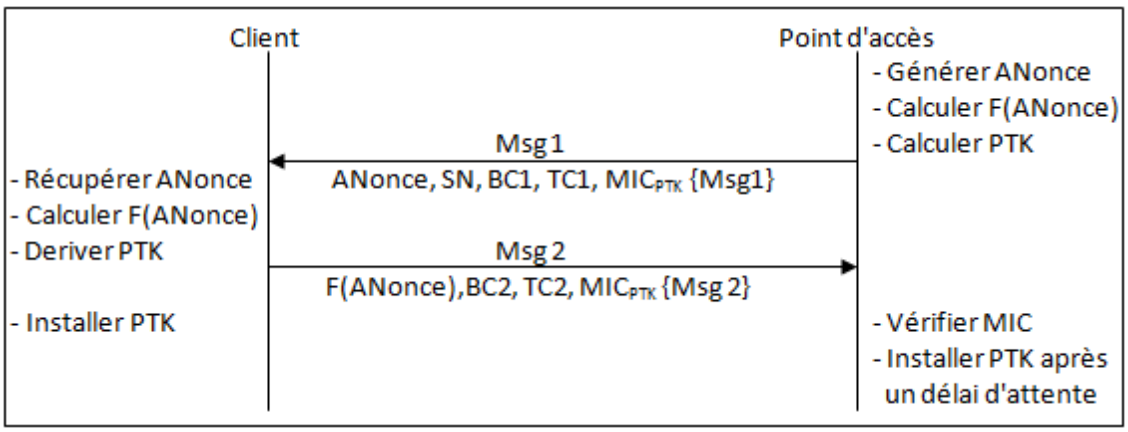

FIGURE 3.16 – Two way Handshake

Dans le Message-1, le PA envoi le ANonce en clair, et calcule le MIC sur le message entier à l'aide de la PTK. Deux champs sont inclus dans ce message pour prévenir l'attaque de rejeu : Boot Counter (BC) et Time Counter (TC). Quand la station reçoit le Message-1, elle calcule son SNonce qui est égale à F(ANonce), et calcule la PTK correspondante. La station vérifie après le MIC et contrôle les valeurs des compteurs contre l'attaque par rejeu.

Initialement les valeurs des compteurs sont à zéro, Le compteur Boot Counter (BC) est incrémenté à chaque fois que le point d'accès ou la station commence le 4-way Handshake. Tandis que le compteur Time Counter (TC) est incrémenté à chaque fois que le point d'accès

ou la Station envoi un message.

Chaque message que la station reçoit dans le 2-way Handshake doit avoir la valeur du compteur du temps (TC) supérieur à la valeur local du compteur du temps, et la valeur du compteur du démarrage et supérieur ou égale à la valeur locale de compteur de démarrage (BC).

Discussion :

L'avantage de la solution proposée est la réduction du nombre de messages pour le calcul de la PTK. Elle permet de pré-calculer la PTK avant l'envoi de Message-1. Cette réduction offre moins de temps de traitement sur la station et le point d'accès. Le protocole utilise aussi les compteurs pour atténuer les attaques par rejeu.

Le désavantage de leur utilisation est l'insignifiance de la synchronisation de la station et du point d'accès, les valeurs BC et TC sont synchronisées pour pouvoir contrôler un message reçu.

3.4.2 Comparaison des diverses solutions

Nous avons comparé les solutions proposées pour faire face aux vulnérabilités et les attaques qui menacent la sécurité du 4-way handshake, cette comparaison est montrée dans le tableau 3.2. suivant :

Critère \ Solution	Consomation mémoire sur le client	Consomation CPU sur le client	Le blocage 4-way Handshake	Attaque de dictionnaire ou force brute	Délai d'installation de PTK	Attaque par rejou	Supposition (Hypothèse)
Chiffrement de ANonce	ANonce et PTK	Déchiffrement ANonce Dérivation PTK	Robuste	Oui, sur PMK	Client :T(DE) +T(PTK) PA :T(CH)+ T(PTK)	Robuste	Utilisation de l'algorithme AES
Two way Handshake amélioré	PTK	Déchiffrement MsgA, Dérivation PTK et Chiffrement MsgB	Robuste	Oui, sur PMK	Client :T(DE)+ T(PTK)+T(CH) PA :T(CH)+ T(PTK)+T(DE)	Robuste	Le PA connait le SID de client
Authentification de Message-1	ANonce et PTK	Calcul PTK' et Dérivation PTK	Robuste	Robuste	Client :T(PTK') +T(PTK) PA :T(PTK')+ T(PTK)	Faible	Un Nonce partagé entre le client et PA
Réutilisation de Nonce (Solution statique)	ANonce, SNonce et PTK	2 * Dérivation PTK	Faible	Robuste	Client : 2*T(PTK) PA : T(PTK)	Faible	Non
Sol. Sta. avec une variante compromise	ANonce, SNonce et PTK	Dérivation PTK et Dérivation PTK si ANonce.stocké ≠ ANonce.reçu	Faible	Robuste	Client : T(PTK) (1x ou 2x) PA : T(PTK)	Faible	Non
Sol. Sta. avec une variante compromise et libération mémoire	SNonce, ANonce et PTK	Dérivation PTK et Dérivation PTK si ANonce.stocké ≠ ANonce.reçu	Faible	Robuste	Client :T(PTK) (x1 ou x2) PA :T(PTK)	Faible	Nécéssite un mécanisme de contrôle d'arrivée de messages
Solution dynamique	SNonce, ANonce et PTK	Dérivation PTK (1x ou 2x)	Faible	Robuste	Client :T(PTK)+ T(CH)+ T(DE) PA :T(PTK)	Faible	Module logiciel
Mécanisme de cookie	Non	Dérivation PTK, Chiffrement PTK et Déchiffrement PTK	Faible	Oui ; sur PTK	Client :T(PTK)+ T(CH)+ T(DE) PA :T(PTK)	Faible	Clé secrète propore au client
Three way Handshake	ANonce et PTK	Dérivation PTK	Faible	Robuste	Client :T(PTK)+ T(Att) PA :T(PTK)+ T(Att)	Faible	Nbre de fois autorisé à réémettre le message-3
Two way Handshake	PTK	Dérivation PTK	Robuste	Robuste	Client :T(PTK) PA :T(PTK)+ T(Att)	Robuste	Le choix de F() par les deux entités

TABLE 3.2 – Tableau comparatif de diverses solutions pour le 4-way Handshake.

A travers cette comparaison, on peut facilement déduire que les solutions qui sont proposées contre les attaques DoS ne sont pas suffisantes. Par exemple :

- La réutilisation de Nonce évite l'attaque de déni de service de type épuisement de mémoire, mais elle engendre un épuisement CPU si un attaquant inonde le client avec le Message-1 (plus de calcul est nécessaire à cause de re-calcul de la PTK). Où :
- Le 2-way Handshake Amélioré réduit le coût de la communication et le temps de calcul, et offre une fiable gestion de clé, mais la PTK est vulnérable aux attaques par dictionnaire où force brute.

Comme on peut le constater, chaque solution à des frais en terme de mémoire ou en puissance de calcul, ou vulnérabilités à de nouvelles attaques. Malgré l'intérêt que présentent ces solutions, les divers schéma de sécurité ne sont pas parfait contre l'attaque de déni de service sur le 4-way Handshake, qui est dû principalement au Message-1 non protégé.

3.5 Conclusion

Dans ce chapitre, on a présenté les principales méthodes EAP proposées pour répondre aux exigences de l'authentification et de la sécurité du standard 802.11i. Plusieurs solutions sont proposées pour divers problèmes, mais beaucoup d'entre eux sont restés irrésolus. Une comparaison a montré l'existence des insuffisances de sécurité, où des attaques comme l'attaque main-in-the-middle et le détournement de session menacent la sécurité globale du réseau sans fil. Pour atténuer les attaques de déni de services lors de la phase de génération de clé de 4-way Handshake, diverses solutions ont été présentées ; à l'exemple de 2-way Handshake Amélioré qui dépend exclusivement du secret PMK. Toutefois, la PMK est vulnérable à l'attaque par dictionnaire, ainsi la génération de clé est mise en péril.

Nous concluons sur la note que les mécanismes d'authentification et de gestion de clé sont toujours insuffisants et vulnérables aux divers attaques. Le chapitre suivant a pour but de présenter nos propositions d'amélioration de la sécurité de la norme 802.11i.

CHAPITRE 4

PROPOSITION DE SOLUTIONS DE SÉCURITÉ POUR L'AUTHENTIFICATION ET LA GESTION DE CLÉS DU STANDARD 802.11I

4.1 Introduction

Ce chapitre sera consacré à la présentation de nos protocoles de sécurité destinés aux standard 802.11i, à savoir des propositions pour l'authentification EAP, et amélioration du protocole 4-way Handshake qui complète l'authentification mutuelle entre le client et le point d'accès, génère et distribue les clés de sessions. La comparaison et l'analyse de ces propositions va constituer le second objectif dans la section 4.3.

4.2 Présentation des solutions proposées

Nous allons d'abord présenter les améliorations pour l'authentification EAP, ensuite pour le 4-way Handshake.

4.2.1 Présentation des améliorations EAP proposées

4.2.1.1 La solution KeyID

Nous proposons ici une nouvelle méthode EAP-KeyID qui se veut simple, et basée sur des clés symétriques. Elle permet l'authentification mutuelle, la mise en place d'une clé maître, et tire avantage des méthodes EAP-TLS, TTLS, PEAP, FAST (*authentification et génération d'une clé maitresse*) et EAP-MD5 (*simplicité*) en évitant les vulnérabilités détectées dans ces méthodes. Pour cela, **EAP-KeyID** suppose qu'une clé **pwd** est pré-partagée entre chaque

client et le serveur EAP, et reprend le principe du protocole CHAP [45] qui est léger dans son traitement.

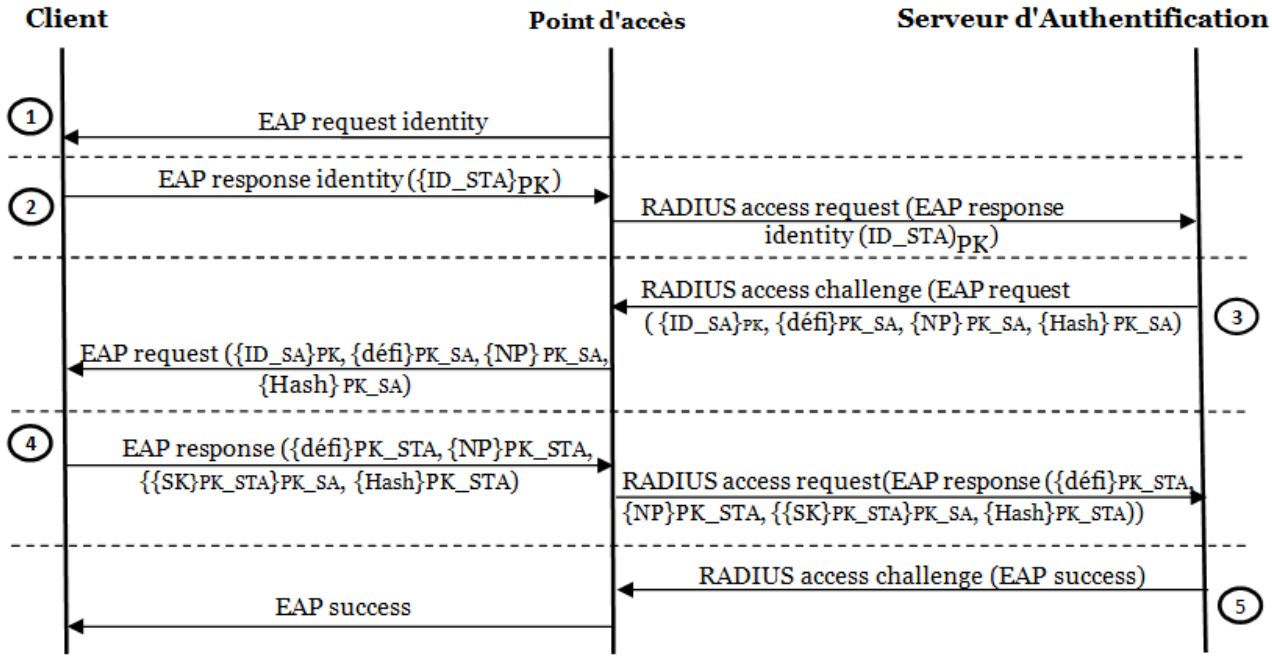

FIGURE 4.1 – Échanges EAP-KeyID dans un contexte IEEE 802.11 (En cas de succès).

Le suplicant dérive une clé **PK** (*Primary Key*) de la clé pré-partagé **pwd**. Après avoir reçu la demande d'identification de l'authentificateur, le suplicant répond à cette requête avec son identité chiffrée avec la clé **PK**, l'authentificateur à son tour relai cette requête au serveur d'authentification (**SA**).

Après avoir reçu l'identité du suplicant (le message 2), le serveur EAP dérive la **PK** de la clé pré-partagé **pwd** et l'utilise pour déchiffrer l'identité du suplicant. Une fois le **SA** a récupéré son identité, il l'utilise avec la clé pré-partagé **pwd** pour former une nouvelle clé PK_{SA} de la manière suivante :
PK_{SA} = f(ID_{STA} || pwd) ; où f() est une fonction de hachage basée sur le scellement (voir section 2.3.5), et || est une concaténation.

Le serveur d'authentification génère un défi (challenge) et le chiffre avec PK_{SA}, le **SA** associe à ce message un numéro unique **NP** qui n'est censé être utilisé qu'une et une seule fois, et qui est incrémenté à chaque paquet pour contrer les attaques par rejeu, ce **NP** est chiffré aussi avec la clé PK_{SA}. Le SA calcule le haché de l'ensemble de Défi, NP, ID_{STA}, ID_{SA}, PK_{SA} comme suit :

$$Hash = (défi||NP||ID_{STA}||ID_{SA}||PK_{SA})$$

Le message qui sera envoyé (Le message 3 de la figure 4.1) au suplicant est comme suit :

$$((ID_{SA})_{PK}, (défi)_{PK_{SA}}, (NP)_{PK_{SA}}, (Hash)_{PK_{SA}}).$$

A la réception du message 3, le suplicant ayant déjà généré la clé **PK**, il récupère l'identité du SA en la déchiffrant avec la clé PK(ID_{SA}) et l'utilise avec la clé pré-partagée pwd pour générer une nouvelle clé secrète PK_{STA}.

Le suplicant ayant déjà généré la PK_{SA} en combinant son identité avec la clé secrète pré-partagée pwd déchiffre le défi reçu (chiffré), ainsi que le NP et le Haché avec la PK_{SA}, puis il calcule le haché de l'ensemble de défi, NP, ID_{STA}, ID_{SA}, PK_{SA} et compare les résultats (Entre le hachage reçu et le haché calculé localement), s'ils sont identiques alors le serveur est bien authentifié.

Le suplicant à son tour génère un défi pour s'authentifié auprès du serveur, il le crypte avec la clé PK_{STA} et il calcul le hashé de l'ensemble de défi, **NP**, ID_{STA}, ID_{SA} et PK_{SA}, comme le SA. Le NP sera utilisé par le suplicant après incrémentation. Avant d'envoyer le message4, le suplicant génère une clé secrète **SK** (*Session Key*) et la chiffre avec la clé PK_{STA} puis chiffrer le tout avec PK_{SA}. Le message 4 est donc comme suit :

$$((défi)_{PK_{STA}}, (NP)_{PK_{STA}}, (SK_{PK_{STA}})_{PK_{SA}}, (Hash)_{PK_{STA}}).$$

A la réception du message 4, le **SA** effectue le même calcul que le suplicant et ainsi compare les résultats, s'ils sont identiques alors le suplicant est authentifié. La clé secrète **SK** va servir au cryptage des données durant la session.

4.2.1.2 EAP-TLS Améliorée :

La méthode d'authentification à utiliser doit répondre à certaines exigences telles que :

- Authentification mutuelle ;
- Protection contre les attaques Man-In-The-Middle ;
- Génération automatique de clés de session ;
- Résistance à l'attaque de dictionnaire ;
- Protection de l'intégrité des échanges durant l'authentification ;
- Assurer la confidentialité des échanges durant l'authentification ;

- Protection de l'identité de l'utilisateur ;

Notre solution se base essentiellement sur la méthode d'authentification EAP-TLS qui assure :

- L'authentification mutuelle : le client s'authentifie chez le serveur avec son certificat et réciproquement.
- EAP-TLS est une méthode génératrice de clé, d'où elle est robuste face aux attaques MITM.
- EAP-TLS comme nous venons de le mentionner est génératrice de clé, cette clé symétrique est générée par le client et envoyer au serveur d'authentification via le tunnel TLS.
- EAP-TLS est résistant aux attaques par dictionnaire grâce au tunnel qu'il établie.
- Les échange entre le serveur d'authentification et le suplicant sont envoyer via un tunnel ce qui garantit la confidentialité et l'intégrité de données.

Dans notre amélioration, on chiffre l'identité de l'utilisateur avec la clé publique du serveur, mais après avoir vérifié son certificat (le client après la vérification du certificat s'assurera qu'il s'adresse bien à un serveur d'authentification légitime, donc il lui délivre son identité). **EAP-PEAP** et **EAP-TTLS** assure la protection de l'identité du suplicant, mais le mécanisme suivi est un peu lent : utilisation d'une méthode d'authentification à l'intérieur d'une autre méthode d'authentification, donc trop de message EAP à gérer (par exemple le message **EAP-SUCCESS** ou **EAP-FAILLURE** sera doublé, le premier sera envoyé à l'achèvement de l'exécution du processus d'authentification de la méthode interne, puis un autre à l'achèvement de l'exécution du processus d'authentification de la méthode externe). A noter que c'est le message résultant de la méthode externe qui va donner l'accès au réseau pour le suplicant (dans le cas du succès d'authentification).

Notre solution est présentée dans le schéma suivant :

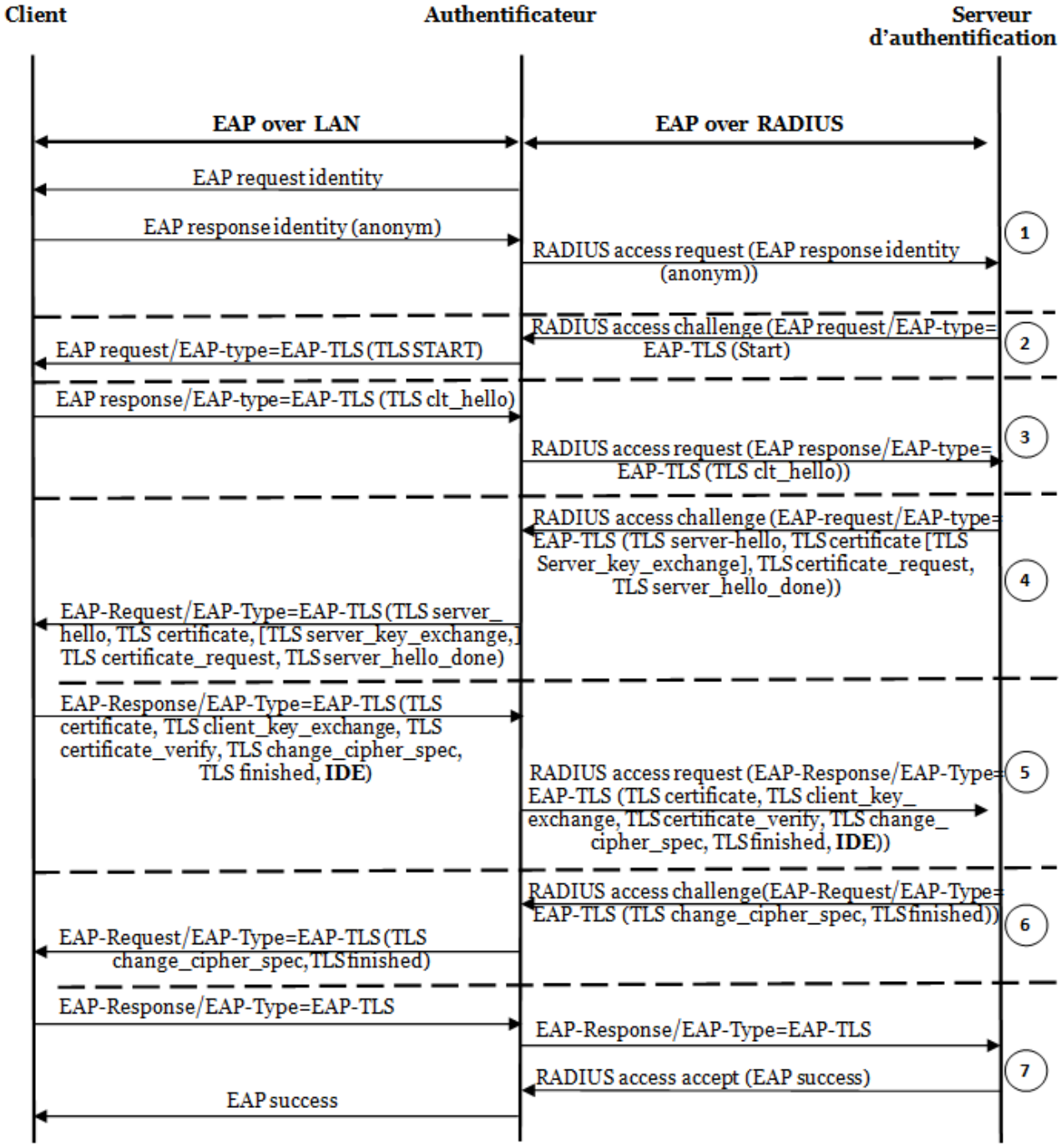

FIGURE 4.2 – Échanges EAP-TLS Amélioré dans un contexte IEEE 802.11 (en cas de succès)

IDE : un message crypté avec la clé publique du serveur d'authentification qui contient l'identité du client.

La différence est dans l'étape 5, où on a ajouté un nouveau message crypté avec la clé public du serveur d'authentification qui contient l'identité du suplicant.

4.2.2 Présentation des solutions 4-way Handshake proposées

Dans 4-way Handshake, quatre messages sont échangés : le Message-1 et le Message-3 transportent le Nonce généré par le point d'accès, le Message-3 transporte le Nonce généré par le client et le Message-4 est un acquittement pour indiquer la réussite du 4-way Handshake. Pendant que les messages 2, 3, et 4 sont protégés par le MIC calculé avec la PTK fraichement générée, le message-1 n'est pas protégé.

Le problème principal dans la procédure de 4-way Handshake est l'incapabilité de différencier un nouveau Message-1 provenant de point d'accès légitime ; et les messages générés par un adversaire (attaquant). D'autres problèmes sont à résoudre, tels que l'épuisement mémoire dû au stockage de ANonce et PTK ; l'épuisement CPU et les autres attaques discutées précédemment. Donc, un contrôle peut être ajouté au Message-1 pour attenuer ces attaques. Dans le cadre de notre travail, des modifications ont été apportées afin d'atténuer les attaques de déni de service visant cette poignée de main, la prémunir des attaques du rejeu, protéger les clés de sessions contre les attaques de dictionnaire ou force brute. Nous avons défini deux solutions pour la dérivation de clés dans 802.11i, à savoir le 4-way Handshake avec hachage et le 3-way Handshake avec hachage.

4.2.2.1 Solution 1 :4-way Handshake avec hachage

Cette proposition se base sur l'utilisation d'une fonction de hachage pour authentifier et assurer l'intégrité du Message-1, et d'empêcher un attaquant de le forger.

A l'étape initiale de 4-way Handshake, le point d'accès et le client devraient avoir connaissance de PMK, elle est utilisée pour authentifier le message-1, et de permettre au client de traiter que les messages authentifiés venant du point d'accès légitimes.

Le principe de base de la solution est présenté dans la figure 4.3 suivante :

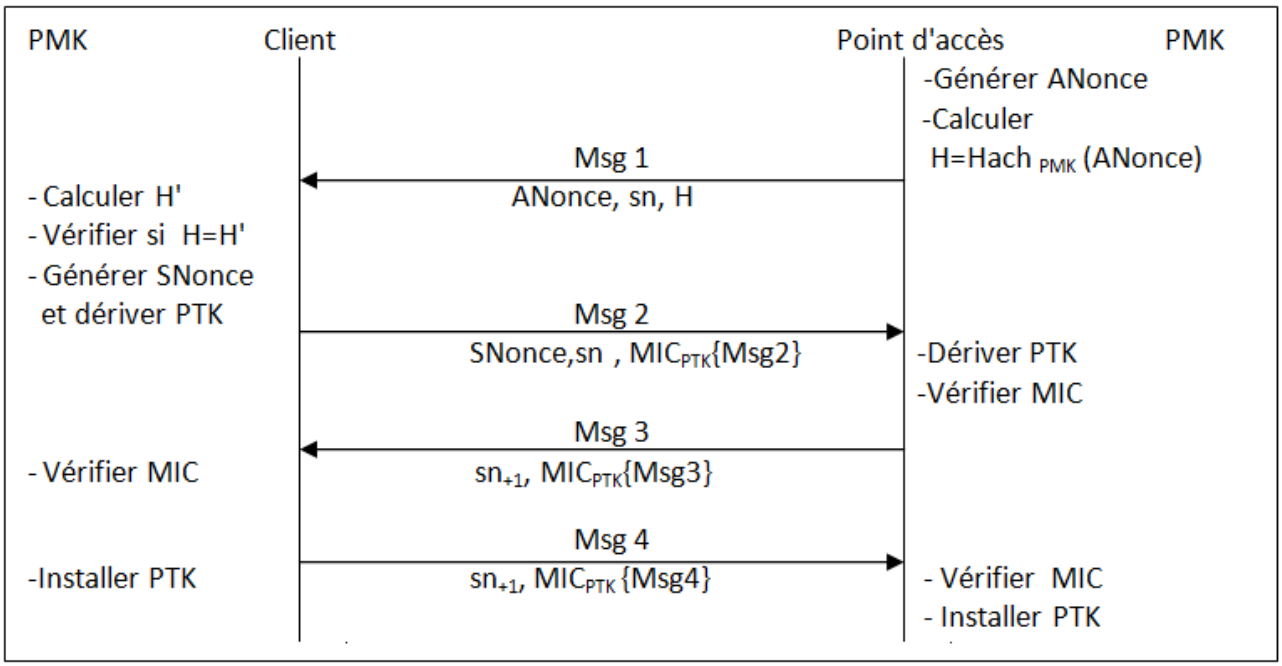

FIGURE 4.3 – 4-way Handshake avec hachage.

Lorsque le point d'accès génère le ANonce, il calcule le haché de ANonce à l'aide d'une fonction de Hachage connue par les deux entités par exemple SHA-1 ou SHA-2, et ceci en utilisant la clé secrète PMK, c'est à dire : Hash $\mathsf{PMK}_{(\mathrm{ANonce})}$. Cette technique est appelée scellement. Ce haché sera envoyé au client, avec le ANonce généré par le point d'accès. Une fois que le client a reçu le Message-1, il calcule le Haché à base de sa PMK et de ANonce reçu, soit H'. Ensuite, il vérifie si le H reçu est égale au H' calculé à son niveau. Si les deux entités sont légitimes et partagent la même clé PMK, ils devraient avoir H=H' et la procédure 4-way Handshake continue. Dans le cas contraire, il s'agit d'un message forgé et ne sera pas traiter. Le client, après avoir authentifier le Message-1, il génère son nombre SNonce, dérive la clé PTK de ANonce reçu, puis envoi un Message-2 au PA. La suite de la solution est similaire au 4-way Handshake original. Après avoir reçu le SNonce du client, le point d'accès procède a la dérivation de PTK et vérifie le MIC du message. De même pour le client, en recevant le Message-3, il s'assure bien que le PA a bien généré la PTK en vérifiant le MIC, il installe ensuite la PTK. Le Message-4 est envoyé au PA pour lui permettre d'installer la PTK.

4.2.2.2 Solution 2 :Three way Handshake avec hachage

Nous proposons aussi une autre variante de la solution précédente, qui réduit le nombre de messages échangés entre le client et le point d'accès. Une solution améliorée qui se base sur le principe du Message-1 de la solution 1, un principe qui consiste à insérer un code

d'authentification dans le Message-1, afin de l'authentifier. Ce code est calculer à l'aide d'une fonction de hachage en utilisant le nombre aléatoire ANonce et la clé PMK.

De plus, nous proposons cette solution pour renfoncer la résistance du Message-l à l'attaque par rejeu, en ajoutant le compteur sn au calcul de hache. La solution conclue le processus d'établissement de PTK en trois messages au lieu de quatre. La figure 4.4 illustre le protocole proposé.

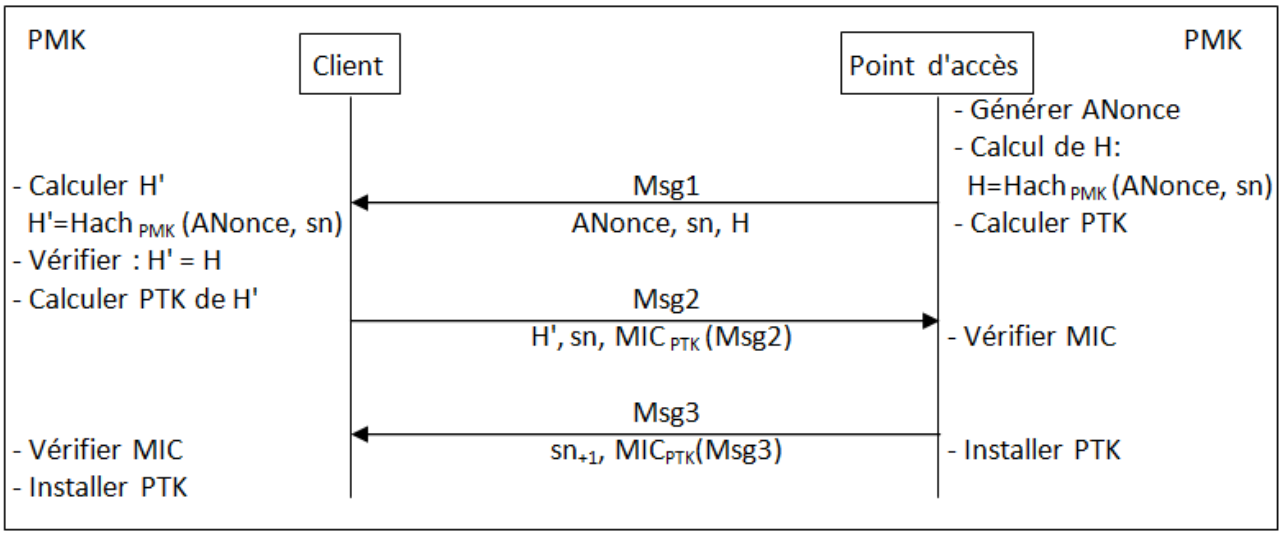

FIGURE 4.4 – Three-way Handshake avec hachage.

Dans ce Three way Handshake proposé, le PA calcule un ANonce, un haché sera ensuite calculé de ce ANonce, de sn à l'aide d'une fonction de hachage en utilisant la clé secrète PMK, soit H. La PTK est calculer avant l'envoi du premier message, en utilisant le H comme valeur aléatoire à la place de SNonce, vu que la plupart des fonction de hachage sont génératrices des nombre aléatoire. Le Message-1 est envoyé alors au client, contenant le hachée H, sn et le ANonce. A sa réception, le client récupère le ANonce pour calculer le hachée de la même manière que le PA, soit H'. Le client ensuite procède à la vérification de H et H'. Dans le cas d'une verification positive, le client dérive sa PTK en utilisant aussi le haché H' comme SNonce. Un Message-2 est envoyé ensuite au PA, inclue le haché H et le MIC calculé sur ce message, à l'aide de PTK. Le PA en le recevant, il vérifie son MIC, et envoi un troisième message au client avec un MIC calculé sur ce dernier. Après, il installe la PTK, idem pour le client, il vérifie le MIC est installe ces clés.

4.2.2.3 Le choix de la méthode de hachage et le scellement

Les deux méthodes utilisent une fonction de hachage pour hacher le ANonce. Donc son choix est crucial, il est impératif de choisir une fonction qui permet de garder les performances de la procédure originale de 4-way Handshake, ou bien encore de les améliorer. Ce type de fonction serve à rendre plus rapide l'identification de données, et elles ne coûtent qu'un temps négligeable, elle permet de protéger la PMK utilisée pour assurer l'authenticité et l'intégrité de message-1. La motivation pour leurs utilisations dans ces solution proposées, est qu'il est très difficile de trouver le contenu du message à partir de la signature en un temps raisonnable, car les fonctions de hachage ne permettent pas de remonter à l'origine du message à partir du haché.

La technique de scellement utilisée dans ces solutions, permet de renforcer la sécurité de la PMK, et d'éviter son exposition à des attaques susceptibles de l'atteindre telles que les attaques de dictionnaire ou force brute. La clé PMK est mélangée à la valeur aléatoire ANonce pour générer une empreinte (Haché) qui sera ensuite utilisée pour vérifier l'origine du Message-1.

La fonction de hachage doit aussi être capable de générer une valeur aléatoire à partir des entrées PMK et de ANonce. Et pour cela, il existe des fonctions pseudo génératrices de nombre aléatoire afin de générer un haché, qui peut être utilisé comme un nombre aléatoire au lieu de SNonce pour la génération de PMK.

4.3 Analyse et comparaison des approches

4.3.1 EAP proposés

La première méthode EAP-KeyID présente plusieurs avantages, à savoir :

- **Simplicité :** Basée sur la cryptographie symétrique, EAP-KeyID n'exige pas de traitements importants. Cette propriété est essentielle dans les réseaux sans fil puisque les nœuds présentent des ressources limitées en termes de batterie, de puissance de calcul et de capacité mémoire.
- **Authentification rapide :** Comme EAP-MD5, EAP-KeyID est basée sur un mécanisme de défi/réponse et par conséquent exige peu d'échanges de messages. Le nombre réduit des messages échangés rend l'authentification rapide. Cette propriété est importante dans les réseaux sans fils puisque les nœuds peuvent à tout moment perdre leurs connexions, ce qui est très perturbant pour les méthodes d'authentification et oblige le mobile à réinitialiser la procédure.
- **Authentification mutuelle :** La méthode EAP-MD5 ne permet pas au client d'authen-

tifier le serveur, et donc de détecter un point d'accès frauduleux qui serait mis en place par une personne malveillante dans le but d'espionner les communications des mobiles. La méthode EAP-KeyID permet de se prémunir de cette attaque en permettant une authentification mutuelle qui se base sur une clé pré-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 pré-partagée. Avec EAP-KeyID, cette attaque n'est plus possible car le hash est chiffré avec la clé (soit $\mathsf{PK}_{\mathsf{STA}}$ ou $\mathsf{PK}_{\mathsf{SA}}$).
- **Protection contre les attaques de type Man-In-The-Middle :** EAP-KeyID est une méthode génératrice de clé (**SK**) et elle assure l'authentification mutuelle, ce qui rend les attaque MITM inutile parce que la session est cryptée avec la clé **SA** et les deux extrémités du réseau (suplicant et SA) s'authentifie mutuellement d'où un pirate ne peut pas se prendre pour un serveur légitime.
- **Protection de l'identité de l'utilisateur :** l'identité de l'utilisateur est chiffrée avec la clé PK ce qui permet de cacher l'identité de l'utilisateur aux pirates donc un pirate qui espionne un trafic ne sait pas quel utilisateur il espionne.
- **Protection contre les attaques par rejeu :** EAP-KeyID définit une valeur unique NP (compteur) chiffré pour chaque paquet échangé, afin de permettre de savoir si un paquet est ancien ou pas.

L'inconvénient majeur de la méthode EAP-KeyID est que la clé pré-partagée est statique, un mécanisme de changement de clé est exigé (on peut utiliser le mécanisme de rotation de clé dans le WEP).

La deuxième solution est une amélioration de la méthode EAP-TLS qui est une méthode très sûre et complète (vu qu'elle répond à la plupart des exigences), donc cette solution souffre du même problème que EAP-TLS est qu'elle repose sur une infrastructure de gestion de clé (PKI - Public Key Infrastructure) pour assurer la gestion des certificats côté client et côté serveur qui est très coûteuse.

4.3.2 Handshake proposés

Dans cette section, nous analysons les deux variantes de 4-way Handshake proposées, puis nous les comparons avec la version originale.

Dans la solutions 1 (première variante), le 4-way Handshake est amélioré en proposant la vérification de l'origine du Message-1, donc elle permet à la station cliente d'ignorer les

messages forgés d'un attaquant, ce qui évite l'attaque d'inondation et le blocage de 4-way Handshake, car le client vérifie simplement le haché envoyé dans le premier message avec celui calculé à son niveau. Cette solution permet aussi d'éviter l'épuisement de mémoire en authentifiant d'abord les messages reçus avant un éventuel stockage de ANonce et de PTK : seuls les paquets légitimes envoyés par le point d'accès seront reçus et stockés, alors que les autres messages envoyés par un attaquant seront abandonnés. De plus, l'épuisement de mémoire peut être dissuader en raison de la difficulté de forger des messages, en raison de la force du technique du scellement, impliquant à la fois le ANonce et la clé PMK dans l'entrée de la fonction du hachage, sans exposer cette clé PMK aux attaques de dictionnaire ou force brute.

Par contre, un attaquant peut intercepter un Message-1 envoyé par un PA et forge le sn du message puis il le rejoue auprès de la station. Cette limite est corrigée dans la solution 2 (deuxième variante), qui propose d'intégrer la valeur du compteur sn avec la valeur à hacher (ANonce et PMK). De cette façon, même si un attaquant réussit à forger le sn du Message-1, il ne peut composer un hache valide ; et le client le découvrira en vérifiant la validité du Message.

Le but de cette deuxième solution est de se prémunir contre l'attaque par rejeu, et de réduire le nombre du message à trois au lieu de quatre en offrant moins de communication. Cette réduction est proposée dans le but de préserver (garder) la même durée prise par la procédure de 4-way Handshake, vu que les deux solutions ont besoin davantage de calcul, pour calculer le haché. Mais ce délai supplémentaire n'est pas critique, car les fonctions du hachage sont développées avec l'exigence qu'elles prennent un temps négligeable pour le calcul du haché. Ce retard est raisonnable avec l'utilisation de haché pour générer la PTK ; au lieu de générer un SNonce en évitant un calcul de plus, et en évitant même de stocker le ANonce du PA.

Un tableau récapitulant l'analyse comparatif est réalisé sur les deux solutions proposées avec le 4-way Handshake. (voir le tableau 4.1)

Approche / Critère	4-way Handshake original	4-way Handshake avec mécanisme de hachage	Three way Handshake avec mécanisme de hachage
Consommation mémoire sur le client	ANonce, PTK	ANonce, PTK	PTK
Consommation CPU sur le client	Dérivation PTK	Calcul de H et Dérivation PTK	- Calcul de H et Dérivation de PTK
Le blocage de Handshake	Faible	Faible	Robuste
Attaque de dictionnaire ou force brute	Robuste	Robuste	Robuste
Attaque par rejeu	Faible	Faible	Robuste
Suppositions	Non	Utilisation d'une fonction de hachage	Utilisation d'une fonction de hachage pseudo génératrice de nombres aléatoires

TABLE 4.1 – Tableau comparatif des solutions Handshake proposées.

4.4 Conclusion

Afin d'atténuer la vulnérabilité de l'authentification et la dérivation de clé du standard 801.11i, nous avons proposé des solutions EAP et 4-way Handshake : D'abord, nous avons proposé deux méthodes EAP, la première reposant sur le principe de défi/réponse et une clé pré-partagée, la deuxième est une amélioration d'EAP-TLS reposant sur les certificats.

Deuxièmement, nous avons adopté un mécanisme de hachage dans deux solutions d'amélioration de la sécurité de 4-way Handshake : une variante qui vérifie l'authenticité de Message-1, basé sur la difficulté de calcul de l'inverse de la fonction de hachage. La deuxième variante réduit le nombre de messages à trois au lieu de quatre, en utilisant le haché comme un nombre aléatoire, et en protégeant le Message-1 contre les attaques par rejeu , en assurant sont intégrité avec l'ajout du numéro de séquence du message au calcul du haché. Une analyse et une comparaison de ces approches ont été réalisées pour soulever leurs points forts et leurs limites.

CONCLUSION GÉNÉRALE ET PERSPECTIVES

Le WiFi et la sécurité dans les réseaux sans fils ont posé beaucoup de problèmes. L'utilisateur ne savait pas que choisir pour mettre en place une solution simple et compatible avec un minimum de matériels. Aujourd'hui les solutions normalisées arrivent enfin à maturité et les protocoles de sécurités sont de plus en plus rodés. Cependant, des failles dans les implémentations sont toujours possibles et des failles dans les configurations sont souvent présentes. La politique de l'autruche, ne rien faire tant que l'on a rien détecté, est généralement coûteuse et « sécuriser après » est souvent trop tard. Si la sécurité reste un choix volontaire, elle demeure essentielle et sécuriser de façon fiable et efficace un réseau sans fil est désormais possible.

Dans ce mémoire, nous nous sommes focalisés sur la sécurité des réseaux 802.11 (WiFi), plus particulièrement en mode infrastructure. Les failles de sécurité du courant standard 802.11 sont nombreuses, et afin de remédier à celles-ci, le groupe de travail IEEE a proposé la norme 802.11i connu aussi sous le nom «WPA2». Cependant, il ne parvient pas à sécuriser entièrement les WLANs. Dans ce dernier, des menaces ont été identifiées au niveau de la phase d'authentification 802.1x/EAP et au niveau de la phase de gestion de clé (4-Way Handshake). Toutes les méthodes EAP décrites dans ce mémoire présentent des défauts et des limites, et la procédure de dérivation de clés dans ce standard, gérée par le 4-way Handshake utilise des messages non protégés ce qui le rend sensible à certaines attaques que nous avions analysées.

L'objectif de ce travail, étant d'étudier et d'analyser quelques méthodes EAP et le 4-way Handshake, dans le but de les examiner, d'apprendre plus sur leurs failles, d'identifier les types d'attaques possibles sur ces dernières et de proposer des améliorations à leurs niveaux. Des travaux antérieurs ont été présentés, et des tableaux comparatifs ont été établis. Nous avons présenté deux solutions d'amélioration EAP, la première se base sur une clé pré-partagée et

l'authentification par le mécanisme de défi/réponse. La deuxième solution est une amélioration de la méthode EAP-TLS qui une méthode complète, mais qui ne permet pas de protéger l'identité de l'utilisateur, dans cette amélioration, on chiffre l'identité de l'utilisateur avec la clé public du serveur après la vérification de son certificat.

Nous avons aussi proposé deux variantes pour atténuer les attaques contre le 4-way Handshake. Leurs principes se reposent sur l'utilisation du scellement et ceci à l'aide d'une fonction de Hachage, pour authentifier le Message-1 et assurer son intégrité. Grace à ces études, analyses et propositions, nous avons contribué ainsi au développement des méthodes de sécurité, et d'avoir des réseaux sans fil plus sûr.

Comme perspectives de notre travail, nous allons continuer la simulation des solutions proposées, pour les analyser, détecter d'éventuelles vulnérabilités et évaluer leurs performances. Une implémentation des solutions a été entamée sous l'environnement java, nous allons tester les scenarios d'attaque possibles pour simuler les conditions d'un réseau typique et examiner les résultats obtenus, afin de valider ces propositions.

BIBLIOGRAPHIE

[1] F. Lemanque. *Tout sur les réseaux sans fil.* Dunod, Paris, 2009.

[2] G. Pujolle. *Sécurité Wi-Fi.* EYROLLES, Paris, 2004.

[3] Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA). *Sécurité des réseaux sans fil (Wi-Fi).* CERTA-2002-REC-002, Paris, 2008.

[4] L. Freytag. *Conception, réalisation et caractérisation d'antennes pour stations de base des réseaux de télécommunication sans fil.* Thèse de Doctorat en Informatique, UNIVERSITE DE LIMOGES, 2004.

[5] A. Géron. *WIFI : Déploiement et sécurité, la QoS et le WPA*. Dunod, Paris, 2006.

[6] M. Yazid. *Proposition d'un protocole d'accés au medium dans les réseaux locaux sans fil IEEE 802.11 à forte contraintes temporelles.* Thèse de Magister en Informatique, Université de A.Mira de Béjaia, 2009.

[7] C. Guellaut. *Prototype d'un système MIMO-MC-CDMA sur plateforme hétérogène.* Thèse de Doctorat en Informatique, Intstitut National des Sciences Appliquées de Rennes, 2009.

[8] R. Moawad. *QoS dans les WPAN, WLAN et WMAN.* Mémoire de DEA, Université Saint Joseph, Liban, 2004.

[9] M. Nehdi. *Evaluation de protocole EDCA*. Mémoire de fin d'étude, Ecole Superieure des Communications de Tunis, 2004.

[10] A. Ksentini. *Qualité de service dans les réseaux locaux sans fil basés sur la technologie IEEE 802.11.* Thèse de Doctorat en Informatique, Université de CERGY-PONTOISE, 2005.

[11] K. Runser. *Méthodologies pour la planification de réseaux locaux sans fil.* Thèse de Doctorat en Informatique et Information pour la Société Spécialité Télécommunications, Institut National des Sciences Appliquées de Lyon, 2005.

[12] Livre Blanc. *Sécurité des systèmes sans fil.* Livre Blanc version 2.0, 2004.

[13] U.S. National Institute of Standards and Technology (NIST). *Specification for Advanced Encryption Standard (AES).* Federal Information Processing Standards Publication 197 (FIPS PUB 197), 2001.

[14] M. Duchateau. *Analyse et simulation du déploiement d'un réseau sans fil à l'ULB.* Mémoire d'Ingénieur en Télécommunications, Université Libre de Bruxelles, 2005.

[15] A. V. D. Bossche. *Proposition d'une nouvelle méthode d'accès déterministe pour un réseau personnel sans fil à fortes contraintes temporelles.* Thèse de doctorat en informatique, Université de Toulouse II, 2007.

[16] G. Pujolle. *Les Réseaux.* EYROLLES, Paris, 2008.

[17] A. Géron. *WI-FI Professionnel : La norme 802.11, le déploiement, la sécurité.* Dunod 3eme Edition, Paris, 2009.

[18] Gh. Labouret. *Introduction à la cryptographie.* http ://www.labouret.net/crypto/#233, Consulté le 20 Mai 2012.

[19] S. Ghernaouti-Hélie. *Sécurité Informatique et Réseaux : Cours avec plus de 100 exercices corrigés.* Dunod 3e Edition, Paris, 2011.

[20] J. F. Pillion and J. P. Bay. *Tout sur la Sécurité Informatique.* Dunod 2e Edition, Paris, 2009.

[21] R. Rolland P. Barthelemy. *Cryptographie : Principes et mises en oeuvre.* Lavoisier, Cachan, 2005.

[22] National Institute of Standards and Technology (NIST). *Secure Hash Standard.* Information Processing Standards publication 180-1, 1995.

[23] R. Rivest. *The MD5 Message-Digest Algorithm.* 1992.

[24] C. He and J. C. Mitchell. *Security Analysis and Improvements for IEEE 802.11i.* Electrical Engeineering and Computer Science Departements. Université de Stanford, 2004.

[25] J. Bellardo and S. Savage. *802.11 Denial-of-Service attacks : real vulnerabilities and practical solutions.* In Proceedings of the USENIX Security Symposium, pages 15-28, 2003.

[26] Q. Stiévenart. *La cryptologie : Peut-on réellement cacher des informations ?* Athénée Royal de Waterloo, 2009.

[27] P. Muhlethaleer. *Securite dans les réseaux sans fil La norme IEEE 802.11.* INRIA, Renne, 2004.

[28] Sécurité des réseaux sans fil. *Agence nationale de la sécurité des systèmes d'information.* CERTA, Paris, 2008.

[29] F. Di Gallo. *WiFi L'essentiel qu'il faut savoir.* Extraits de sources diverses récoltées, 2003.

[30] G. Lehembre. *Sécurité WiFi - WEP, WPA et WPA2.* hakin9 N° 1/2006, 2006.

[31] L. Saccavini. *802.1x et la sécurisation de l'accès au réseau local.* INRIA , Renne, 2003.

[32] S. Ghernaouti-Hélie. *Sécurité informatique et réseaux : Cours et Exercices corrigés.* Dunod 2e Edition, Paris, 2008.

[33] M. Frikha. *Réseaux ad hoc.* LAVOISIER, Cachan, YEAR =.

[34] Microsoft Corporation. *Présentation du protocole EAP.* http ://technet.microsoft.com/fr-fr/library/bb457039.aspx, Consulté le 17 Mai 2012.

[35] B. Aboba and D. Simon. *PPP EAP-TLS Authentication Protocol.* RFC 2716, Octobre 1999.

[36] T. Dierks and C. Allen. *The TLS Protocol Version 1.0.* RFC 2246, 1999.

[37] Institute of Electrical and Electronics Engineers(IEEE). *802.1X Standard.* Part-Based network Access Control, 2001.

[38] C. Rigney, S. Willens, A. Rubens, and W. Simpson. *Remote Authentication Dial In User Service.* RFC 2865, 2000.

[39] P. Funk and S. Blake-Wilson. *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0).* RFC 5281, 2008.

[40] E. Doreau. *WI-FI : Etat de l'art des protocoles de secret et d'authentification.* Conservatoire National des Arts et Métiers (Informatique - Réseaux Systèmes et Multimédia), 2005.

[41] C. Saillard. *802.1X : Solution d'authentification sécurisée pour le futur réseau sans fil de l'Université Louis Pasteur.* Centre Réseau et Communication, Université Louis Pasteur, 2002.

[42] A. Palekar and Al. *Protected EAP Protocol (PEAP).* Work in Progress, 2004.

[43] Wikipedia. *EAP-PEAP.* http ://fr.wikipedia.org/wiki/Extensible_Authentication_Protocol, Consulté le 17 Mai 2012.

[44] B. Aboba, L. Blunk, J. Vollbretch, J. Carlson, and H. Levkowetz. *EAP-PEAP.* Extensible Authentication Protocol (EAP), RFC 3748, 2004.

[45] W. Simpson. *PPP Challenge Handshake Authentication Protocol (CHAP).* RFC 1994, 1996.

[46] S. Convery, D. Miller, S. Sundaralingam, M. Doering, P. Roshan, S. Albert, B. McMurdo, and J. Halpern. *Description détaillée de la sécurité pour les réseaux locaux sans fil.* Cisco SAFE, 2003.

[47] N. Cam-Winget, D. McGrew, J. Salowey, and H. Zhou. *The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST).* RFC 4851, 2007.

[48] J. Salowey H. Haverinen. *Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM).* RFC 4186, 2006.

[49] C. He and J. C. Mitchell. *Analysis of the 802.11i 4-Way Handshake.* In WiSe'04. 43-50, 2004.

[50] F. De Rango, D.C. Lentini, and S. Marano. *Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i.* In EURASIP Journal on Wireless Communications and Networking, 1-19, 2006.

[51] C. He and J. C. Mitchell. *Security Analysis and Improvements for IEEE 802.11i.* In NDSS, 2005.

[52] A. I. Jafri and Y. Li Ho. *ANonce Encryption in 802.11i 4-way Handshake Protocol.* Proceedings of MOMM2009, 2009.

[53] J. Liu, X. Ye, J. Zhang, and J. Li. *Security Verification of 802.11i 4-way Handshake Protocol.* In ICC 2008.1642-1647, 2009.

[54] S. Eu, S. Cho, H. Choi, and H. Choo. *A Robust Session Key Distribution in 802.11i.* In International Conference on Computational Sciences and Its Applications ICCSA0, 2008.

[55] H. Altunbasak and H. Owen. *Alternative Pair-wise Key Exchange Protocols for Robust Security Networks (IEEE 802.11i) in Wireless LANs.* Institue de technologie de Géorgie, IEEE 2004.

Résumé

La transmission radio rend les réseaux sans fil commodes d'usage, faciles à déployer, et économiques, mais soulèvent par contre des problèmes de sécurité, dus à la nature ouverte des supports de transmission utilisés. En plus, les exigences de sécurité doivent être vérifiées notamment l'anonymat et la protection à long terme des données. 802.11i est un standard développé pour améliorer la sécurité des réseaux 802.11 au niveau MAC, en proposant une nouvelle architecture de sécurité appelée RSN (Robust 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'appuie 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 des 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. Dans ce mémoire, on a étudié le protocole 802.11i, tout en se concentrant sur la phase d'authentification et la phase de gestion de clés de ce protocole. Nous avons étudié les failles et vulnérabilités de ses dernières, et nous avons proposé de nouvelles solutions pour améliorer la sécurité de ce standard.

Mots-clés : *Cryptographie, sécurité, WiFi, 802.11i, 802.1x, EAP, 4-way handshake.*

Abstract

The Radio transmission makes the wireless networks convenient to practical use, easy to be spread, and economic. However, it raises security problems because of the open nature of the used transmission supports. In addition, the security demands should be checked especially the anonymity and the long time protection of the data. 802.11i is a standard which was developed to improve the network security 802.11 at the MAC level suggesting a new architecture of security called RSN (Robust Security Network) whose contribution is essentially in the use of the standard of 802.1x for the authentication and an access control, the four way handshake for the generation of the fresh keys of the session and the protocol AES (Advanced Encryption Standard) for encryption. In RSN, one of the methods of authentication which supports the 802.1x/EAP is carried out to establish a master key (PMK) between the station and the authentication server. The latter will be ; then, used in the management procedure of the keys (4-way handshake) to provide a mutual authentication between the access point and the client, and the generation of temporary keys of sessions. In this dissertation, we studied the protocol of 802.11i, concentrating on the authentication phase and the key management phase of this protocol. We studied the flaws and the vulnerabilities of these lasts, and we have proposed new solutions to enhance the security of the standard.

Keywords : *Cryptography, security, WiFi, 802.11i, 802.1x, EAP, 4-way handshake.*