Sécurité dans les réseaux WIFI 802.11

Constantin Yamkoudougou
Ingénieur Réseaux Télécoms & Sécurité

28 mars 2005

1 Définitions et abréviations

PDU : Protocol Data Unit, données et un entête de protocole réseau formant un tout. Il s'agit par exemple une trame au niveau 2 du modèle OSI.
WEP-PDU :PDU chiffrée par le protocole WEP
RC4 : Algorithme de génération de clés secondaires à partir d'un vecteur d'initialisation et d'une clé maître. Cet algorithme a été créé par R. Rivest du MIT et de la société RSA.

AP : Access Point - Point s'accès
STA : station
BSS : Basic Sub Set est une cellule de base ayant pour station de base, un point d'accès. L'ensemble des stations (ternimaux WIFI, ordinateurs) appartenant à un même BSS communiquent par le point d'accès de leur cellule.
ESS : Extended Sub Set. Un ESS est un réseau étendu constitué de plusieurs BSS reliées entre elles et possédant plusieurs systèmes de distributions.
PPP : Point-to-Point Protocol
EAP : Extensible Authentication Protocol
RADIUS : Remote Authentication Dial In User Server
RSN : Robust Security Network - concept introduit dans les spécifications du standard 802.11i pour améliorer la sécurité du WIFI.
Association : On appelle association, l'établissement d'un canal de communication entre deux éléments du réseau 802.11. Dans le mode ad-hoc, il s'agit d'un lien entre deux stations et en mode BSS c'est le lien entre une station et un point d'accès.
CRC : Cyclical Redundancy Code - technique de détection d'erreur par calcul linéaire
MAC : Medium Access Control- couche liaison de données
MIC : Message Integrity Code.
WEP : Wireless Equivalent Protocol est le protocole de base de sécurité des réseau de première génération.

TSC : Temporal Sequence Counter-Compteur introduit dans le spécifications 802.11i dans les protocole TKIP et CCMP
MSDU : SDU (Service Data Unit) de niveau MAC.
DSSS : Direct Sequence Spread Spectrum
FHSS : Frequency hoping Spread Spectrum
OFDM : Orthogonal Frequency Division Multiplex.
CSMA / CA : carrier sense multiplex access / collision avoidance
CSMA/ CD : carrier sense multiplex access / collision detection
CBC-MAC : Cipher Block Chaining - Message Authentication Code. **CCMP** :CBC-MAC Protocol.

2 Généralités sur les réseaux 802.11

2.1 Qu'est ce que le WIFI ?

WIFI est l'acronyme anglais de Wireless Fidelity. Le WIFI d ésigne ainsi génériquement les réseaux sans fil du standard 802.11 sans aborder les différentes variantes de ce standard.

2.2 Quelle sont les typologies d'architectures déployées ?

On distingue deux modes de fonctionnement des réseaux WIFI : le mode **infrastructure** et le **mode ad hoc**. Le mode infrastructure correspond à un mode où l'élément central de la communication est la borne WIFI. Dans ce mode,c'est la borne ou point d'accès qui gère l'ensemble des communications entre toutes les stations du qui lui sont reliées. Le mode ad hoc est un mode de fonctionnement où chaque station est autonome et fait office de relais pour les autres stations. Ce dernier mode est plutôt destiné à des usages de type militaire ou dans des cas où un backbone ne peut être figé.

2.3 Quels sont les débits ?

Les débits sont variables selon la version utilisée. Pour le WIFI de version 802.11b, le débit maximum est de 11 Mbits/s. Il est de 54 Mbits/s pour le 802.11a ou 802.11g dans la bande des 5Ghz

2.4 Quelles sont les fréquences utilisées ?

Considérons l'exemple d'un abonné au réseau radio mobile GSM. En France, si celui-ci est abonné chez Orange ou SFR, il communiquera sur une bande de fréquences de 800 à 900 Mhz alors que chez Bouygues il communiquera plutôt dans la bande des 1800 à 1900 Mhz. Il en est de même pour le WIFI. Les ordinateurs reliés à une borne WIFI utilisent une bande de

fréquences de 2,4GHz à 5Ghz qui leur est réservée. En général les émetteurs utilisés dans les bornes WIFI et les cartes réseaux des ordinateurs sont de très faible puissance (quelques milliwatts), ce qui fait que les communications sont limitées à quelques dizaines de mètres.. Un nouveau standard appeé WIMAX dans la bande des 3Ghz est en train d'émerger et a fait l'objet de consultation de l'Autorité de Régulation des Télécommunications pour un usage au niveau métropolitain.

2.5 Quelles technologies de gestion du spectre de fréquences sont utilisées ?

Ils utilisent des technologies à étalement du spectre à saut de fréquence (FHSS) et à étalement du spectre en séquence directe (DSSS) à cause de leur résistance aux bruits radioélectriques. Le 802.11a utilise la technologie OFDM dans la bande de fréquence des 5 Ghz.

ref http ://grouper.ieee.org/groups/802/11/

2.6 Quelle est le protocole d'accès au medium radio ?

Dans un réseau local d'accès radio, le nombre de stations n'est pas figé et la réservation statique de ressources radio s'avère coûteuse à cause de la rareté des fréquences dans une bande donnée. Le 802.3, ancêtre du 802.11 utilise une méthode d'accès au médium physique à détection de contention appelée CSMA/CD. Une station avant d'émettre écoute le médium filaire pour voir s'il n'y a pas une station en train d'émettre une trame. Lorsque le médium est libre, elle émet sa trame et continue d'écouter le support afin de s'assurer que la transmission a réussi. Lorsqu'une collision est détectée, il y a temporisation, puis réémission au bout d'un temps aléatoire. Dans le cas de la 802.11, une écoute de la grande diversité des fréquences serait fastidieuse. C'est pourquoi dans le 802.11 la notion d'acquittement à été introduite dans le CSMA/CA. Lorsqu'une station transmet une trame, elle reoit en retour un ACK (ACKnowledgement) de la station réceptrice pour s'assurer que la réception s'est bien déroulée.

http ://grouper.ieee.org/groups/802/11/

2.7 Quelles sont les enjeux de sécurité ?

Les problèmes de sécurité du WIFI sont liés au support de communication dont on ne peut donner une limite précise dans un espace donné. En effet, lorsque l'on déploie le WIFI dans un appartement donné, on peut légitimement craindre que les autres voisins du même palier ne se connectent frauduleusement au réseau. Ce problème ne se posait pas dans les réseaux

câblés où les chemins sont bien définis et encastrés dans des murs ou protégés par des goulottes. Il est donc indispensable de sécuriser non seulement l'accès mais aussi les informations circulant sur le réseau.

3 Sécurité des réseaux WIFI de première génération

La sécurité des réseaux de première génération repose sur le protocole WEP.

3.1 Quel est le mécanisme de chiffrement utilisé dans le WEP ?

Deux longueurs de clés sont spécifiées dans le standard 802.11b. La première est de 40 bits pour le WEP de première version. Cette restriction a été imposée initialement par le gouvernement américain soucieux de contrôler et d'accéder facilement au contenu des paquets chiffrés en procédant notamment dans le pire des cas par des attaques de type force brute. Il s'est avéré très rapidement par la suite que la puissance de calcul disponible dans la plupart des entreprises permettait de faire ce type d'attaque avec un investissement relativement peu coûteux. Cela a conduit à la spécification d'une nouvelle longueur de clé de 104 bits pour la deuxième version du WEP dont on peut brièvement rappeler le fonctionnement.
Avant d'être soumis à l'algorithme RC4 pour la génération de clés de session de chiffrement des payloads de trames réseau, les clé initiales de 40 ou 104 bits sont concaténées à un vecteur d'initialisation de 3 octets de long pour obtenir une clé de base de 64 ou 128 bits. Le RC4 est utilisé en tant que stream cipher pour la génération de clés de session beaucoup plus longue de 64 ou 128 bits. Cette longueur est égale à la taille du payload de la trame à chiffrer à laquelle il faut ajouter la taille du CRC.

Une WEP-PDU transmise sur un réseau WIFI est le résultat d'une addition modulo 2 d'une clé de session et d'une PDU. Le vecteur d'initialisation est le même aussi bien pour le chiffrement que le déchiffrement. L'identifiant des clés de 40 ou 104 bits est codé sur deux bits selon la structure du protocole, ce qui ne permet de changer en théorie de clé que 4 fois. Ces identifiants ainsi que le vecteur d'initialisation sont transmis en clair sur l'interface radio.

3.2 Quelles sont les attaques possibles sur le WEP ?

On se restreint volontairement aux attaques cryptographiques possibles sur le WEP en ne tenant pas compte des failles intrinséques au protocole 802.11b telles que la diffusion en clair de SSID (Sub System ID) sur les trames balises (beacon frames) qui permettent de faire du spoofing de point d'accès ou de station. Les attaques possibles sur le WEP sont des attaques

à clairs connus pour les clés de session, les attaques par rejeu et enfin les attaques sur l'algorithme RC4. Les autres types d'attaques sont traitées dans d'autres fiches.

3.3 Oscar peut-il faire des attaques à PDU clairs connus ?

Il s'agit du cas où Oscar possède quelques résultats de trames connues sans pouvoir les choisir. Il lui suffit dans ce cas de tester l'ensemble des opérations d'arithmétiques modulo 2 entre la PDU claire et la PDU chiffrée pour tomber sur la clé. On peut gager que c'est ce qui se passe dans la réalité parce que le WEP et les algorithmes de cryptographie en général ne sont pas secrêt.

3.4 Comment se fait l'authentification par le protocole WEP

L'authentification d'une station appartenant à un réseau 802.11b se fait en trois passes. La station envoit une demande d'association au point d'accès. Le point d'accès lui transmet un nonce chiffré. La station déchiffre le nonce et le transmet de nouveau au point d'accès en le rechiffrant avec une clé de session WEP. Le point d'accès accepte l'association si le nonce est identique au nonce initialement transmis.

3.5 Comment attaquer le protocole d'authentification dans le WEP ?

Si Oscar a la possibilité d'écouter et de sauvegarder l'ensembles des trames transmises lors du protocole d'authentification, il lui suffira de rejouer cette séquence lors d'une requête d'association exprimée par une station du réseau pour se faire passer pour un point d'accès.

3.6 Comment faire une attaque sur le calcul du CRC

Dans le protocole WEP, une trame est considérée comme étant intègre lorsqu' après son déchiffrement, le résultat du calcul du CRC du payload de cette trame est identique au CRC acheminé avec cette trame. Dans la mesure où le CRC est liénaire, il suffira pour un attaquant de modifier le contenu d'une trame avec une parité de bits qui permet de retrouver une somme identique à celle du CRC transmis par voie radio. Par exemple la suite binaire 0000 ou 0110 donnera le même résultat en terme de calcul de CRC.

3.7 Y a-t-il intérêt à faire des attaques par force brute ?

Pour référence, aujourd'hui le DES [ref1] de complexité 2^{56} ne présente plus de résistance suffisante en recherche exhaustives. Il est évident qu'une attaque par recherche exhaustive devient intéressante si d'aventure une clé de 40 bits était choisie pour le WEP.

ref1 http ://www.itl.nist.gov/fipspubs/fip46-2.htm

3.8 Qu'est ce que l'algorithme RC4 ?

L'algorithme a été créé par R. Rivest pour la société RSA Data Security. Il est utilisé comme stream cipher dans des produits commerciaux tels que Lotus Notes mais aussi dans des standards IETF tels que TLS qui est la version standardisée du protocole SSL de la société Netscape. L'algorithme comporte deux étapes : une phase d'initialisation de la s-box S, puis la phase de génération des suites chiffrantes S_z dont l'ensemble forme une clé de session dans le cas du WEP .

3.8.1 Comment est initialisé l'algorithme RC4 ?

On suppose que l'utilisateur possède une clé k d'initialisation décomposable en une suite k_0 ..... k_{l-1} de l mots de n bits. n = 8 (taille d'un octet) en général dans le domaine des réseaux. On effectue les itérations suivantes :

Pour z s'incrémentant de de 0 à $2^n - 1$

$K_z = k_{z \bmod l}$.

$S_z = z$.

On initialise j.

$j = 0$.

Pour i s'incrémentant de 0 à $2^n - 1$

$j = j + S_i + K_i \bmod 2^n$.

$S_i \leftarrow S_j$ (il s'en suit une permutation de S_i et S_j)

$S_j \leftarrow S_i$

On réinitialise i et j avant le calcul des clés de session .

i=0, j=0

3.8.2 Comment sont généré les clés par RC4 ?

i et j étant définis précédemment et réinitialisés à 0, ils évoluent désormais comme suit

$i = i + 1 \bmod 2^n$

$j = j + S_i \bmod 2^n$

$S_i \leftarrow S_j$

$S_j \leftarrow S_i$

Les octets de suites chiffrante ou de clé de session sont obtenus par la suite de $S_{S_i+S_j \bmod 2^n}$

ref http ://csrc.nist.gov/wireless/S09_IEEE802.11Procedures-ncwv2.pdf

3.9 Y a-t-il des attaques connues sur l'algorithme RC4 ?

La plupart des attaques décrites précédement reposent sur la facilité relative de récupération d'une clé de session. On peut donc raisonnablement pour aller plus loin se poser une question sur l'algorithme RC4. Etant donné la découverte d'une ou plusieurs clés de session, quelle information Oscar peut-il avoir sur les clés WEP de 40 ou 104 bits sachant que l'algorithme utilisé est le RC4. Parmi les attaques qui ont été menées sur le RC4, on peut citer celles d'Andrew Roos de 1995 et les plus récentes de Serge Mister et E. Tavares.

3.10 clés faibles générés par RC4

En septembre 1995, Andrew Roos publia dans le sci.crypt newsgroup un article sur une classe de clés faibles pour l'algorithme RC4. Ces clés sont celles dont les premiers octets présentent une forte corrélation selon la relation suivante :

$$k_0 + k_1 = 0 \bmod 2^n$$

. En effet, une entrée donnée S_z ne subit au maximum q'une seule permutation. La probabilité que cette permutation aît lieu pour une entrée S_z de la s-box S calculée par Andrew Roos est de de 1/e. Dans le cas du WEP, k_0 et k_1 appartiennent au vecteur d'initialisation. Selon cet article, la complexité d'un attaque serait réduite de $2^{5,1}$ ce qui ne représente pas un gain énorme un dans un espace de clés de complexité 2^{128} si le vecteur d'initialisation n'est pas connu. En revanche, la complexité se réduirait de 2^{18} pour Oscar, s'il a déjà mené les attaques decrites ci-dessus et possède une clé de session.

ref http ://www.esat.kuleuven.be/ psourady/research/mypapers/paulv2a.pdf

3.11 autres attaques sur RC4

La plupart des attaques sur RC4 exploite les faiblesses du vecteur d'initialisation ou un espace de clés faibles comme par exemple celui de Fluhrer, Itsik Mantin, Adi Shamir [ref1] ou encore comme celle de Grosul et Wallach sur des clé très longues de 2048 bits [ref2].

ref1 http ://citeseer.ist.psu.edu/fluhrer01weaknesses.html
http ://www.wisdom.weizmann.ac.il/ itsik/RC4/rc4.html
ref 2 http ://www.wisdom.weizmann.ac.il/ itsik/RC4/Papers/GrosulWallach.ps

3.12 Peut-on sécurisé un réseau 802.11b ?

La sécurité des réseaux de première génération repose sur le WEP qui utilise un algorithme de génération d'une suite chiffrante construite à partir de l'algorithme RC4. La sécurité du WEP n'est pas fiable à cause des nombreuses attaques à clairs connus, par rejeu et usurpation d'identité possible dans ce type de réseaux. La deuxième génération encore connu sous le nom de WPA (wireless Project Allinace) utilise le protocole 802.11i est scensé apporter plus de sécurité. Il est conseillé d'utiliser un mécanisme de confidentialité de type tunnel chiffrant tel que IPSec si l'on souhaite réellement sécuriser les flux réseaux et de compartimenter les flux WIFI dans des réseaux virtuels (vlan) spécifiques.

4 Sécurité des réseaux de 2ème génération

L'une des options de sécurité dans les nouvelles générations des réseaux WIFI est l'utilisation du protocole 802.1x basé sur EAP pour la sécurisation des réseaux 802.1x. Ce protocole n'est pas récent. Il a été introduit par le groupe 802.11i en tant protocole ouvert au support d'autres protocoles d'authentification par login - mot de passe, par RADIUS (RFC RFC3580), par fonction de hachage MD5 ou par certificats dans TLS (RFC2716) ou encore par du One time pad.. Ce parcours traite d'abord du concept de Robust Security Network introduit dans la sécurité des réseaux WIFI de dernière génération avant d'aborder les protocoles 802.1x, EAP-TLS, et enfin le protocole TKIP et CCMP.

4.1 Qu'est ce que le concept de Robust Security Network (RSN) dans les réseaux 802.11 ?

Dans le standard 802.11i la sécurité repose sur le concept de RSN. L'authentification se fait par le standard IEEE 802.1X qui assure également les mécanismes de distribution des clés.

Un RSN ajoute de nouvelles composantes de sécurité par rapport à la sécurité des réseaux de première génération, c'est-à-dire :

- Un mécanisme d'authentification amélioré pour les point d'accès et les stations
- Des algorithmes de dérivation de clés
- Des algorithmes de chiffrement améliorés comme CCMP et optionnellement TKIP.

Le RSN introduit deux nouveaux éléments dans l'architecture 802.11.

Un serveur d'authentification que l'on notera AS par la suite. C'est une entité séparée ou intégrée dans l'AP. Elle est chargée d'assurer l'authentifi-

cation des éléments de l'ESS ou de fournir des informations aux éléments du RSN pour qu'ils s'authentifient entre eux. Cette authentification peut être mutuelle et est assurée par une méthode de type EAP. Le 802.11i ne spécifie pas de méthode d'authentification particulière à utiliser. L'authentification par le protocole 802.1x n'est pas une authentification formelle en soit. Elle doit être perçue comme une enveloppe supportant des algorithmes et des méthodes d'authentification plus spécifiques déjà cités plus haut.

Le concept de port 802.1X. Dans le contexte des réseaux 802.11, c'est l'acceptation ou le refus de l'établissement d'un canal de communication entre le demandeur et les autres ressources du réseau dont le point d'accès constitue une passerelle. Pendant la phase d'authentification, le port est ouvert. Les seuls échanges possibles sont ceux qui sont entre le serveur d'authentification, l'authentifiant et le demandeur. Le port est fermé lorsque le demandeur est authentifié.

4.2 Comment est utilisé le protocole 802.1x dans les mécanismes d'authentification des réseaux 802.11 ?

Pour une compréhension du protocole, il est nécessaire de définir les trois acteurs intervenant dans ce protocole : Le demandeur, l'authentifiant et l'authentificateur qui est le Serveur d'authentification (SA) déjà défini précédemment.

Le demandeur est une station cliente voulant accéder au réseau c'est-à-dire à un BSS ou ESS donné.

L'authentifiant est l élément BSS ou ESS qui demande au demandeur de prouver qu'il est digne de confiance dans le protocole d'authentification. Typiquement l'authentifiant est un point d'accès dans une architecture en mode infrastructure. L'authentifiant fait appel à un service d'authentification qui est une entité tierce telle qu'un serveur RADIUS appartenant au même réseau que l'authentifiant.

L'authentificateur est l'entité tierce dans l'exemple du serveur RADIUS à qui l'authentifiant passe la main pour exécuter un protocol d'authentification donné. L'authentifiant attend le résultat de l'authentificateur afin de décider s'il ferme ou non le port 802.1x pour que le demandeur puisse accéder au réseau. Le fonctionnement de 802.1x est similaire à celui d'un interrupteur électrique.

4.3 Comment est utilisé le protocole EAP dans les mécanismes d'authentification des réseaux 802.11 ?

EAP est le protocole d'authentification conçu pour PPP (point to point protocol), le protocole d'échange utilisé dans le réseau téléphonique afin de

pouvoir acheminer un trafic de trames sur des circuits commutés. EAPoL (EAP over Lan) est la variante implémentée pour l'authentification sur un réseau local comme le 802.11.

Dans le cas du protocole 802.11i, il est nécessaire de distinguer deux types d'authentification via EAP :

- Un protocole d'authentification écrit par le groupe 802.11i dont les canaux de distribution des clés ne sont pas explicitement définis. En l'occurrence le standard stipule l'usage d'un canal MPPE propre à Microsoft. Ce protocole est à clé secrète. La clé partagée est le PMK (Pairwaise Master Key)
- L'utilisation de protocoles d'authentification et/ou de chiffrement déjà connus tels que SSL, TLS, OTP (protocole à masques jetables One Time Pad) ou encore les protocoles sur la base de fonctions de hachage.

4.3.1 Authentification par PMK

Dans ce scénario, le demandeur et l'authentificateur, s'authentifient mutuellement par le protocole EAP et génèrent par la suite des clés de session à partir d'une clé maîtresse PMK (Pairwise Master Key). La clé PMK est générée par l'authentificateur qui en transmet une copie au demandeur en vue des chiffrements et des authentifications futures. Elle est ensuite transmise par canal secret à l'authentifiant. Le standard 802.11i ne donne aucune précision par rapport à ce canal, ce qui pourrait donner lieu à des implémentations incompatibles entre équipementiers. Un protocole subséquent à quatre passes (4 handshake) utilisant un format EAPOL-Key du protocole EAP pour l'échange de clé permet de confirmer l'existence de la PMK et de faire des dérivations de clés secondaires à partir de la PMK

4.3.2 Exemple d'authentification via EAP-TLS [ref 2]

Lorsque le protocole sous-jacent est TLS [ref 1], la suite des échanges se fait selon le schéma ci-dessous dans lequel seules les phases essentielles du protocole sont mentionnées.

- Phase 1 : Probe request : demande d'identité à la station voulant accéder au réseau
- Phase 2 : réponse de la station en déclinant son identité et l'ensemble des protocoles d'authentification supportés.
- Phase 3 : phase où le point d'accès transmet l'identité du demandeur au serveur d'authentification.
- Phase 4 : négociation du protocole TLS entre le demandeur et l'authentificateur.
- Phase 5 : démarrage du Hello TLS

– Phase 6 : réponse du serveur avec transmission de certificat et requête optionnelle du certificat client.
– Phase 7 : vérification certificat serveur, échange de clés par le protocole Diffie hellman.

ref1 http ://www.faqs.org/rfcs/rfc2246.html ref 2 http ://www.faqs.org/rfcs/rfc2716.html

4.4 Qu'est ce que le Protocol TKIP dans les réseaux WIFI 802.11 ?

Le protocole TKIP (Temporary Key Integrity Protocol) est une amélioration apportée au protocole WEP dans la nouvelle norme 802.11i afin d'assurer une compatibilité avec les réseaux de premières génération déjà déployés de manière importante. L'objectif de TKIP est de pallier un certain nombre de failles de sécurité découvertes dans le WEP comme les attaques par rejeu et la linéarité du CRC. Les points importants de ce protocole sont :

– Le calcul systématique d'un code de contrôle d'intégrité (MIC) des adresses MAC source, destination et du payload des trames 802.11.

– L'introduction d'un compteur (TSC) afin dempêcher les attaques par rejeu.

– L'extension du vecteur d'initialisation (IV) de 32 bits, plus long que celui du WEP initial calculé sur 3 octets.

– L'introduction d'une fonction cryptographique de mixage permettant de combiner TSC et clé WEP avant la génération de suites chiffrantes par l'algorithme RC4.

4.5 Quelle est la structure d'un paquet 802.11 avec TKIP ?

La structure des trames [ref 1] intègre désormais des compteur dans le cas du protocole TKIP. Ce compteur appelé TSC est codé sur 32 bits. Comme le TSC est mis à jour pour chaque paquet, il faudra attendre 2^{32} transmissions pour qu'une tentative d'attaque tombe sur le même numéro de TSC. La nouvelle structure de trame montre également que le nombre de clés WEP interchangeables dans le protocole WEP n'a pas changé. Ce nombre est toujours codé sur deux bits.

TKIP introduit aussi la notion de fonction de mixage. La fonction de mixage permet une génération de clés WEP de 104 bits en intégrant un compteur. Cela évite l'utilisation de clés statiques comme dans la première version du protocole. Le reste du protocole WEP est inchangé dans le fond.

Il s'agit notamment de la transmission du vecteur d'initialisation et du calcul d'un MIC à partir d'une fonction de hachage au lieu d'un CRC linéaire.

ref 1source : norme 802.11i

4.6 TKIP améliore-t-il la sécurité du WEP ?

La réponse est affirmative dans la mesure où il empêche le rejeu en introduisant un numéro de séquence à l'instar de protocoles plus élaborés tels que TCP. Si nécessaire, les payloads (MSDU) sont fragmentés en incrémentant le TSC pour chaque fragment et l'on accepte que les paquets arrivent uniquement dans l'ordre. Les attaques à clair choisis sont toujours possibles, mais n'apportent que peu d'informations dans la mesure où la fonction de mixage permet un renouvellement en temps réel des clés avant l'entrée de l'algorithme RC4. On peut dire que le maillon faible de ce protocole est l'absence de mécanisme de gestion et de stockage des clés utilisées avant l'accès à la fonction de mixage.

4.7 qu'est ce que le protocole CCMP dans les réseaux 802.11 ?

Le protocole CCMP est une des options de sécurité spécifiée par le groupe 802.11i afin de remplacer le protocole WEP. CCMP [ref1] utilise un mécanisme de chiffrement qui repose sur l'algorithme AES [ref 2]. AES possde différents modes d'utilisation. Le mode choisi pour le 802.11 est le " **counter mode with CBC-MAC (CCM)**". Le **counter mode** assure la confidentialité et CBC-MAC assurant l'intégrité et l'authentification. Contrairement à TKIP, CCMP est obligatoire dans les implémentations de 802.11i.

5 Références documentaires complémentaires

Standard IEEE 802.11i
http ://www.netcraftsmen.net/welcher/papers/wlansec01.html
http ://www.wi-fi.org/OpenSection/secure.asp ?TID=2
http ://www.hp.com/sbso/productivity/howto/it_wifisecurity/
http ://www.ieee802.org/1/files/public/docs2000/ieee_plenary.PDF
http ://www.urec.cnrs.fr/securite/CNRS/vCARS2003/DOCUMENTS/saccavini.pdf
http ://ditwww.epfl.ch/publications-spip/article.php3 ?id_article=821