Le Wi-Fi

Mathias Bigaignon, Mathieu Daumas, Victor Drouin Viallard

5 juin 2015

Table des matières

1 Introduction

1.1 L'origine du Wi-Fi

Le développement du Wi-Fi a été pour la première fois possible en 1985, peu après que le gouvernement ait permis l'accès libre à certaines bandes fréquences. C'est le point clé de sa création car le développement d'un protocole de réseau destiné au particuliers avait besoin de pouvoir utiliser simplement des bandes de fréquence sans avoir à obtenir de licences. Les premières utilisation de ces bandes de fréquences fûrent faites de manières indépendantes et de nombreux problèmes d'incompatibilité survenait entre les différents appareils.

1.2 Développement du Wi-Fi

Dès 1997, et pour accélérer le développement du Wi-Fi et son adoption par le grand public, les dirigeants de plusieurs industries se regroupèrent pour décider de l'adoption d'un standard commun. On comptait alors dans le commité créé de grands noms de l'industries électronique et informatique comme Nokia, Lucent, ou encore Cisco. C'est en 1997 que sort alors pour la première fois dans le commerce des appareils suivant la norme IEEE 802.11 créée par ce commité. A l'aube de l'an 2000 un large programme de certification fût alors lancé pour certifier les appareils du marché et facilliter d'avantage de développement de cette nouvelle norme de communication sans fil. Toujours dans le but d'être plus facillement adoptée par la société de consomation, la norme IEEE 802.11 est renommée Wi-Fi et débute son expension de part le monde.

2 Structure physique du Wi-Fi

2.1 Les différentes bandes de fréquences employées par le Wi-Fi

Le Wi-Fi profite dès sa création de l'utilisation sans license possible des bandes de fréquences libérées par l'état américain. Les différents standars du Wi-Fi (802.11a, 802.11b, 802.11g) emploient dès lors les bandes ISM et U-NII.

La première (ISM), dont la fréquence se situe de 2.4 GHz à 2.483.5 GHz, est utilisés par les standards 802.11b et 802.11. Néanmoins ce domaine est loin d'être constant d'un pays à l'autre et les constructeurs de matériel Wi-Fi doivent prendre en compte des variations de la largeur de bande lors de leur construction. Elles se situent néanmoins toutes aux alentours de 2.4 GHz.

La seconde (U-NII), a une largeur de bande plus grande de 300 MHz située aux alentours de 5GHz mais divisée en plusieurs sous-bandes et pour chacune d'entre elles les conditions d'utilisations émmisent par les organismes de réglementation des différents pays sont différents. La puissance des deux premières sous-bande est limitées de façon à ce que le Wi-Fi soit utiliser en intérieur. Pour la dernière la puissance permise est différente et permet l'utilisation du Wi-Fi pour des transmissions dans des endroits plus vastes. Mais là encore il n'y a pas qu'un seul pays donc qu'une seule norme, et chaque pays ne permet l'emploi que d'un nombre limité de ces bandes de fréquence. Un appareil validé pour l'Union Européenne ne sera donc pas nécessairement valide au Japon où seul la première sous-bande est utilisable.

2.2 Structure physique des ondes

Les conditions physiques font que la limitation de la largeur de bande utile pour le Wi-Fi oblige l'emploi de modulation pour permettre son utilisation sans intérference entre les différents appareils. Dès lors diffférnets types de modulation sont employés pour structurer ces ondes éléctromagnétiques.

2.2.1 L'étalement de spectre à séquence directe

Cette technique d'étalement de spectre, aussi utilisée dans les communication par satellite, utilise une bande de fréquence supérieur à celle réellement utile dans le but de rendre la transmission plus "resistante" aux altérations extérieures (bruit). Dans le même temps cela rend l'interception et l'altération volontaire du message par une entité tierce plus difficile. Cette resistance aux interférences permet le partage de la bande de fréquence entre plusieurs canaux de communication. C'est la méthode de modulation employée par la norme IEEE 802.11.

2.2.2 L'étalement de spectre par saut de fréquence

Le principe de cette modulation est simple : répartir le canal de communication entre plusieurs sous-canaux eux même répartis selon une configuration seulement connue de l'émetteur et du récepteur. Dans cette optique, le signal transmis et réparti est bien plus résistants aux altérations du bruit et son interception est elle aussi compliquée. Là encore la possibilité de partager par cette méthode une même bande de fréquence font qu'elle est employée (dans une forme particulière, sans saut de fréquence) par des versions plus récentes du Wi-Fi (normes 802.11g, 802.11n, 802.11ac) et cela permet des débits de communication plus élevés qu'avec la méthode d'étalement de spectre à séquence directe.

2.2.3 Le multiplexage par division orthogonale de fréquences

Ce procédé de codage consiste lui aussi en la répartition d'un signal en différentes sources porteuses, dont les fréquences sont orthogonales. Cette méthode consiste en l'utilisation de nombreuses porteuses orthogonales entre elles ce qu'il fait que même en étant employées pour des fréquences très proches, elles n'interfèrent pas entre elles. Grace à cela bruitage et interception sont atténués. Elle est employée pour les normes 802.11a, 802.11g, 802.11n, et par la norme 802.16e.

3 Les modes de connexion

Le Wi-Fi est utilisé selon différents modes de connexion qui sont décrit dans la suite.

3.1 Le mode infrastructure

] Il s'agit d'une mode employé pour établir des connections entre les différents appareils Wi-Fi. Ce mode s'appuie sur l'utilisation de points d'accès intermédiaires. Ce mode d'utilisation est majoritairement utilisé pour des réseaux locaux et chaque point d'accès y est placé intelligement de façon à recouvrir la zone à connecter. L'obligation des appareils connectés d'établir une connexion en passant par l'un des points d'accès - et en utilisant son identifiant unique - permet un contrôler plus facilement l'accès au réseau.

3.2 Le mode "pont"

Ce mode utilise à la manière du précédent un certain nombre de points d'accès mais ceux ci servent surtout à étendre un réseau filaire de plus grande envergure. Chaque connexion passe par le point de connexion, aussi appelé "pont", ce qui lui permet de les contrôler.

3.3 Le mode Ad-Hoc

C'est le mode de connexion utilisé pour connecter directement deux appareils entre eux. Les deux appareils choisissent au préalable un canal commun ainsi qu'un identifiant unique (voir une clé de chiffrement) et l'utilisent pour communiquer. Ce type de connexion permet également aux appareils de transmettre une connexion d'un appareil à un autre pour élargir la portée d'une connexion au delà de la portée réelle de l'emmeteur.

4 La structure des données

4.1 Contrôle de la lisaison logique (LLC)

La sous-couche employée par le Wi-Fi pour contrôler les connexion permet de fiabiliser le protocole MAC (décrit plus bas) en établissant un contrôle d'erreur et de flux. Elle dispose des types de transmission suivants :

- Type 1 : aucun contrôle donc pas de connexion ni utilisation d'ACK, seulement aiguillage des données vers les protocoles de couches supérieurs.
- Type 2 : ce type de transmission, similaire au précédent, effectue en plus un contrôle de séquence et de flux, et nécessite l'établissement d'une connexion avec ACK.
- Type 2 : mode dérivé du type 1 possédant en plus l'utilisation d'ACK dans le but d'être employé dans des réseaux industriel. Il ne nécessite cependant pas de connexion.

Les différents champs utilisés par la trame pour garantir la transmission des données et leur intégrité sont les suivants :

- DSAP (1o) : Désigne le protocole supérieur destinataire des données.
- SSAP (1o) : Désigle le protocole qui a transmis la trame courante.
- Contrôle
  - En mode information (2o) : Indique le numéro de trame envoyée et celui attendu.
  - En mode supervision (2o) : Indique le type de contrôle employé puis le numéro de la trame attendue.
  - En mode non numéroté (1o) : Indique une condition particulière.
- Données utiles sur un maximum de 1497 octets.

4.2 Contrôle d'accès au support (MAC)

Cette seconde partie de la couche structurelle des données transmises par le protocole Wi-Fi permet d'établir une interface entre la partie logicielle et la partie physique de la transmission. Elle peut varier selon les systèmes physiques employant la transmission (Ethernet, Token Ring, WLAN, etc.).

La méthode de contrôle d'accès employée par le Wi-Fi est le CSMA/CA (à la différence du CSMA/CD employé en Ethernet mais dont l'utilisation ne convient pas aux réseaux sans fils pour lesquels les appareils connectés ne peuvent directement connaître que l'état des appareils à portée d'emmission et donc ne peuvent pas savoir si l'appareil avec lequelle ils veulent se connecter est déjà en train de recevoir une transmission ou non). Pour ce mode de transmission la station emmetrice procède ainsi : tout d'abord elle vérifie que le réseau n'est pas encombré (sinon elle attend). Puis le cas échéant elle envoit un premier message type RTS (Request To Sent) à destination de la machine réceptrice. Si le récepteur n'est pas en état de congestion, il renvoit alors un message de type CTS (Clear To Send) à l'emmeteur qui peut alors envoyer ses données. Dans le RTS l'emmeteur précise entre autre la taille des données à envoyer ce qui permet au récepteur renvoyant le CTS de communiquer aux machines auquelles il est connecté le temps pendant lequel il sera occupé.

Comme expliqué dans le cours, le système de backoff exponentiel est employé pour éviter la congestion du réseau et pour permettre à plusieurs machine de communiquer avec une même autre. Dans ce mécanisme, si l'emmeteur tente l'envoi d'un RTS mais que le récepteur est occupé, alors il attend un temps aléatoire choisi dans une fenêtre dont l'étendue augmente à chaque nouvelle collision.

5 Sécurité des réseau Wi-Fi

5.1 Le contrôle des adresses MAC

La première sécurité employée par les réseaux informatique est celle du contrôle des adresses MAC (adresses physiques uniques associées à chaque matériel réseau). Chaque élément du réseau doit en posséder une (ordinateurs, routeurs, objets connectés divers) et leur filtrage permet de sélectionner les appareils autorisés à accéder au réseau. Le routeur ne conservant pas l'adresses MAC lorsqu'il transmet des données, ce système de filtrage ne fonctionne que pour des réseaux locaux, c'est pourquoi le mécanisme de filtrage par adresses IP est employé pour des réseaux de plus grande envergure.

5.2 Le WEP

Longtemps utilisé pour sécurisser les réseaux Wi-Fi sans fil, ce protocole visait à garantir la confidentialité des connexions établies sur un réseau sans fil de type Wi-Fi. Neanmoins l'algorithme de cryptographie qu'il utilise a récemment été cassé et son utilisation est obsolète.

5.3 Le WPA/WPA2

Le WPA (et sa version supérieure le WPA2) est un protocole développé après la découverte des faiblesses du WEP dans le but de le remplacer. Il respecte la norme IEEE 802.11i destinée à la sécurisation des connexion sur un réseau Wi-Fi ce qui lui permet d'être utilisable avec la plupart des carte Wi-Fi et points d'accès. Le WPA2 est une version ultèrieur certifiée par l'agence de certification Wi-Fi Alliance (celle qui depuis le début du Wi-Fi certifie les appareils Wi-Fi) et prend en charge le protocole CCMP.

Le CCMP est un mécanisme de chiffrement s'appuyant sur AES, lui même un sous-ensemble de Rijandael qui est un algorithme de chiffrement symétrique défini comme standard par les organisations gouvernementales américaines en 1997. Sur un bloc d'entrée fourni de 18 bits (ou 16 octets) la clé déduite est d'entre

128 bits et 256 bits. Ces 16 octets sont permutés suivant une table définie auparavent puis placé dans une matrice 4x4. Les lignes de cette matrice sont tournée vers la droite (la rotaton variant selon le numéro de la ligne). Elle subit une transformation linaire basée sur sa multiplication par des polynômes matriciels (cela garantissant une meilleur diffusion des coefficients de la matrice, c'est à dire une propagation des bits dans la structure). En fin d'algorithme, une matrice intermédiaire est obtenue en effectuant un OU binaire entre la matrice obtenue et une matrice préalablement définie, puis tout l'algorithme est ré-employé sur la matrice intermédiaire. Au total, entre 10 et 14 tours sont nécessaires pour générer les clés de 128 bits à 256 bits.

6 Conclusion

En conclusion le Wi-Fi est l'un des protocoles de communication sans fil qui s'est le plus répendu ces dernières années. Il a permi notamment la création de nombreux algorithmes de chiffrement libre destinés à sécuriser ses réseaux. Le Wi-Fi constitue ainsi aujourd'hui un moyen simple de se connecter au réseau Internet et sa sécurité, quand utilisé avec les bon algorithmes de choffrement, en font un rude concurent de la connexion ethernet qui était jusqu'alors utilisée. Il est de plus utilisé dans de plus en plus d'objets embarqués - car il est facile à mettre en place - comme les téléphones, les ballons sonde, etc.

7 Sources

- Articles wikipédia sur le Wi-Fi, le LLC, le DSSS, le FHSS, le WEP et le WPA/WPA23
- www.purplewifi.net pour l'histoire du Wi-Fi
- www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_FR.pdf pour la sécurité du Wi-Fi
- easytp.cnam.fr/terre/images/WiFi.pdf pour les couches physiques et le CSMA/CA