Couche liaison

WLAN

Objectifs

- Pouvoir expliquer la différence entre les termes WLAN, 802.11 et Wi-Fi
- Savoir citer les avantages et les inconvénients des WLAN
- Pouvoir expliquer le lien entre 802.11 et le modèle OSI
- Savoir expliquer les critères pour le choix de canaux
- Pouvoir expliquer le problème d'accès au medium dans le cadre d'un WLAN
- Savoir expliquer les différents problèmes de sécurité posés par les réseaux Wi-Fi
- Pouvoir citer les différents protocoles utilisés pour sécuriser les réseaux Wi-Fi, expliquer leur fonctionnement et leurs faiblesses

Définitions

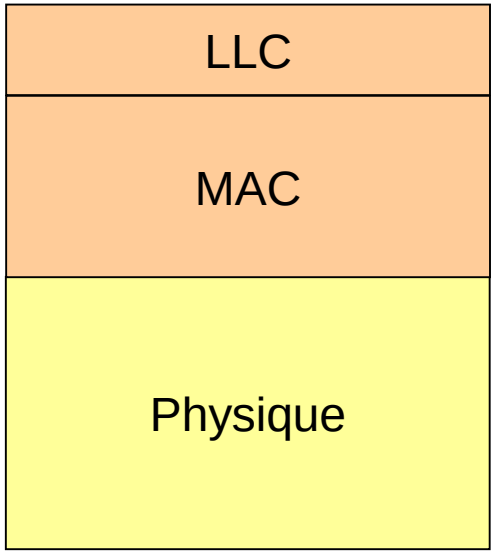
- WLAN: Wireless Local Area Network (réseau local sans fil)
  - Type de réseau
- 802.11: décrit les caractéristiques d'un WLAN
  - Standard international
- Wi-Fi: Wireless Fidelity, marque créée par la Wi-Fi Alliance
  - Initialement le nom d'une certification pour la compatibilité des équipements
  - Technologie / ensemble de protocoles basé sur les standards 802.11

Avantages et inconvénients

- Avantages
  - Mobilité
  - Facilité et coût d'installation
  - Adapté à toutes les plateformes
- Inconvénients
  - Débit faible et partagé
  - Problèmes liés à la transmission radio (interférences, couverture)
  - Sécurité

Lien avec le modèle OSI

- 802.11 définit les couches Physique et Liaison
- La couche liaison est divisée en 2 sous-couches:
  - MAC
  - LLC
- But initial de LLC: cacher les différences entre les versions à la couche supérieure
- Concrètement: identifie seulement le protocole de la couche supérieure



Normes principales

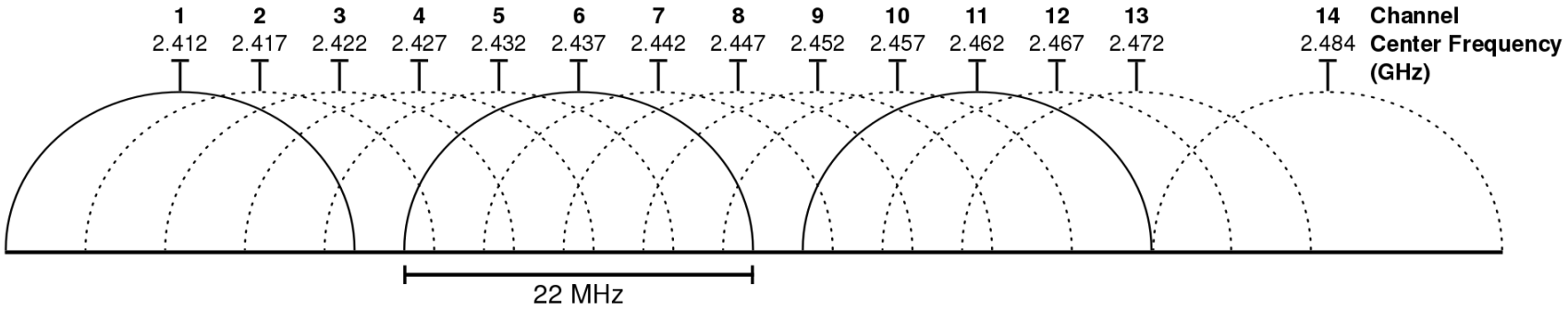
Norme	Débit maximal théorique	Bande de fréquences	Commentaire
IEEE 802.11	2 Mb/s	2.4 GHz	Première norme
IEEE 802.11b	11 Mb/s	2.4 GHz	Compatible avec 802.11g. Peu utilisée
IEEE 802.11g	54 Mb/s	2.4 GHz	Très populaire
IEEE 802.11a	54 Mb/s	5 GHz	Portée plus faible, mais moins d'interférences
IEEE 802.11n	600 Mb/s	2.4 GHz ou 5 GHz	Utilise le MIMO (Multiple Input Multiple Output)

Choix de canal

- Les bandes de fréquences sont divisées en canaux
- Nombre de canaux utilisés :
  - 802.11b: 1
  - 802.11g: 1
  - 802.11a: 1
  - 802.11n: 1 ou 2
- Le choix des bons canaux est important pour éviter de mauvaises performances

Choix de canal: 802.11b/g/n (2.4GHz)

- 13 canaux en Europe + canal 14 seulement au Japon
- Chevauchement des canaux: bruit dans les canaux voisins
- Utilisation du même canal
  - Inconvénient: partage de la bande passante
  - Avantage: permet aux mécanismes de détection de collision de fonctionner
- Idéalement: 5 canaux d'écart pour éviter les interférences
  - Canaux les plus utilisés: 1, 6 et 11



Choix de canal: 802.11a/n (5GHz)

- 19 canaux en Europe
- Pas d'interférences mutuelles
- 802.11n peut utiliser un ou deux canaux
  - 5GHz: rien de spécial
  - 2.4GHz: les deux canaux doivent être séparés de 20 MHz
    - Par exemple 1 et 5 ou 6 et 10
    - Un seul réseau 802.11n à 2.4 GHz bloque 9 des 13 canaux

Accès au medium

- Pratiquement impossible de transmettre et écouter en même temps
  - Le signal reçu peut être très faible par rapport au signal émis
  - CSMA/CD ne peut pas être utilisé
- Les collisions doivent être évitées plutôt que détectées
- La méthode la plus courante est CSMA/CA (Carrier Sense Multiple Access Collision Avoidance):
  1. Ecouter le canal avant de transmettre
  2. Si le canal est libre pendant l'intervalle DIFS: transmission
  3. Si le canal est occupé: attente d'un délai aléatoire
  4. Une fois la trame transmise: attente d'un délai aléatoire
  5. Acquittement des trames après chaque transmission (intervalle SIFS entre la réception de la trame et l'acquittement)

Trames de gestions 802.11

- Trois types de trames: données, contrôle et gestion
- Contrôle: utilisées pour l'accès au medium et les acquittements
- Session: utilisées pour la communication avec l'AP
- Scanning (trouver un réseau):
  - Scanning actif: Probe request et Probe response
  - Scanning passif: Beacon (envoyé régulièrement par l'AP)
- Authentification (prouver son identité):
  - Authentication
- Association (négocier les conditions):
  - Association request
  - Association response

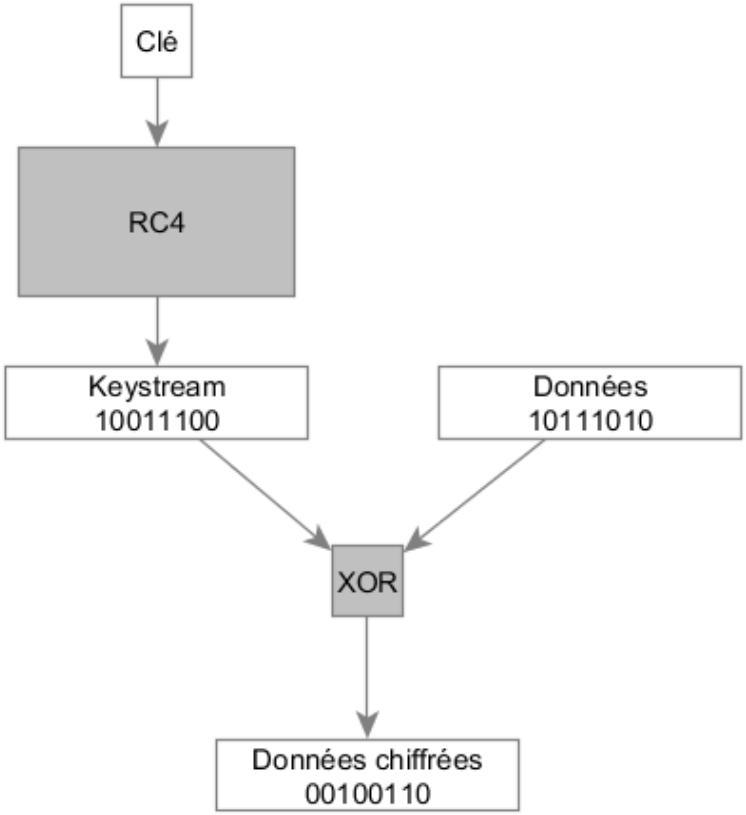
Sécurité Wi-Fi

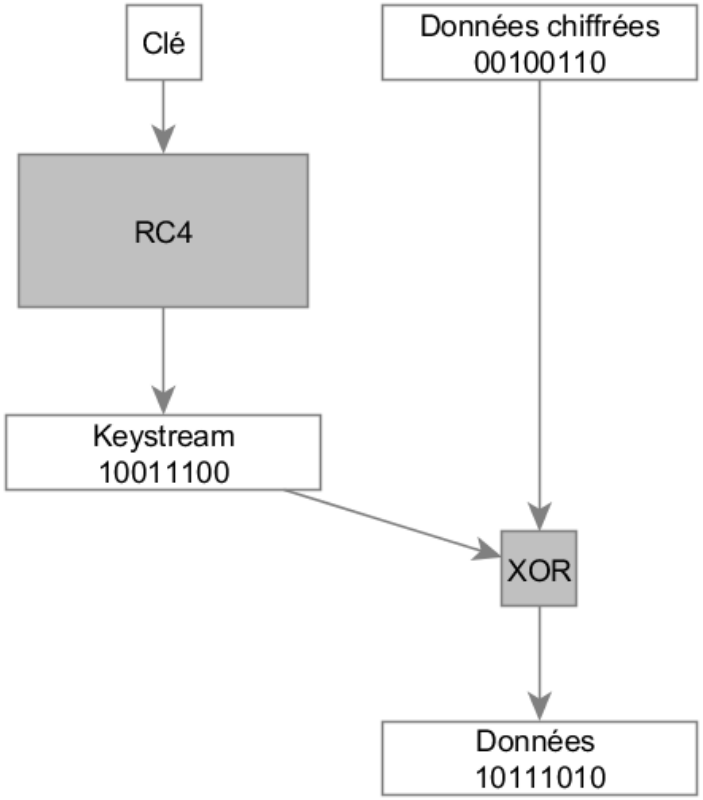
- Aucun chiffrement (p.ex. free hotspot)
  - Équivalent à un hub
- Ecoute passive et analyse du trafic
  - Trafic visible
  - Mode monitor
  - Informations dans les Probe Request
- Problème du déni de service
  - Par définition les réseaux sans fil sont vulnérables aux attaques par déni de service
  - En créant du bruit, on empêche un réseau sans fil de fonctionner
  - La disponibilité ne peut pas être garantie

WEP – RC4

- Chiffre les données en utilisant l'algorithme de chiffrement par flot **RC4:**
  - prend en entrée une **clé**
  - génère une séquence de bits pseudo-aléatoire aussi longue que les données à chiffrer: le **keystream**
  - le keystream chiffre les données en effectuant une opération XOR
  - comme l'opération XOR est son propre inverse, les données chiffrées peuvent être déchiffrées en les XORant à nouveau avec le keystream
- La clé utilisée peut être dérivée du mot de passe de plusieurs manières, qui sont propriétaires

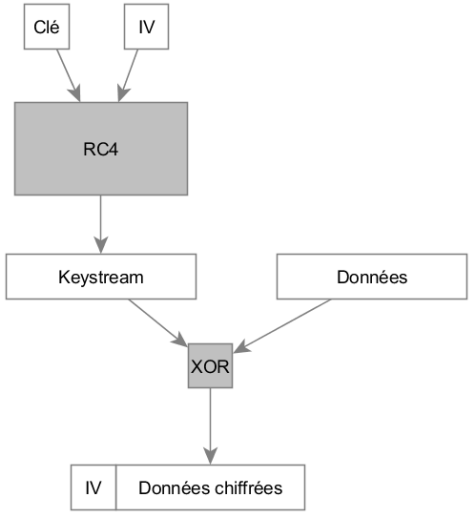
WEP – RC4

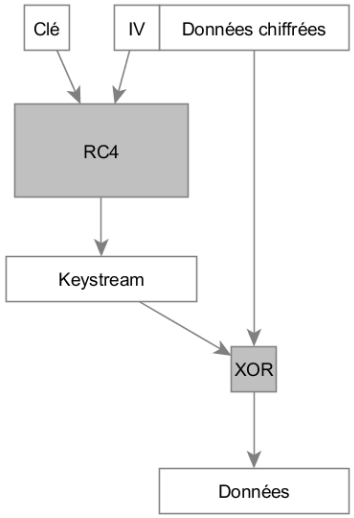

Clé
RC4
Keystream
10011100
Données
10111010
XOR
Données chiffrées
00100110


Clé
Données chiffrées
00100110
RC4
Keystream
10011100
XOR
Données
10111010

WEP – RC4 et IV

- Problèmes:
  - Si un keystream est utilisé plusieurs fois, on peut obtenir des informations sur les données
  - Si le keystream est découvert (p.ex. en utilisant un texte clair connu) il permet de déchiffrer des données
- Utilisation d'un vecteur d'initialisation (IV) pour rendre la clé unique
- L'IV est envoyé avec les données pour qu'elles puissent être déchiffrées





WEP - Confidentialité

- Faiblesses:
  - L'IV n'est pas assez long (24 bits)
    - En une heure environ, tous les IV auront été utilisés
  - La norme concernant les IV n'est pas assez stricte:
    - Pas obligatoire
    - Pas forcément aléatoire (incrémentation p.ex.)
  - RC4 est vulnérable aux attaques par réutilisation du keystream
- Des outils utilisent ces faiblesses pour retrouver la clé
- Capture du trafic en mode monitor
- Même si on a le mot de passe, le trafic n'est pas déchiffré automatiquement
- Déchiffrement du trafic avec le mot de passe ou la clé

WEP - Authentification

- Il est nécessaire de s'authentifier auprès de l'AP pour que les trames envoyées soient acceptées:
  1. Open System
  2. Shared Key
- Dans le cas de l'Open System il s'agit juste d'une requête d'authentification envoyée à l'AP, suivie d'une réponse positive
- Dans le cas du Shared Key, les étapes suivantes ont lieu:
  1. Demande d'authentification par la station
  2. Envoi d'un texte clair par l'AP
  3. Envoi du texte chiffré avec la clé par la station
  4. Envoi d'un message de succès par l'AP

WEP - Authentification

- Shared Key semble plus sûr, mais en réalité, il expose un keystream
- Le texte clair et le texte chiffré ont circulé sur le réseau, il suffit de les XORer entre eux pour obtenir un keystream valable:
  - L'AP envoie le texte clair 01110101
  - La station le chiffre en utilisant la clé et renvoie le texte chiffré 10110010, avec l'IV utilisé
  - Un attaquant capture ces deux messages, il effectue l'opération 01110101 XOR 10110010
  - Il sait maintenant que le keystream correspond à cet IV est 11000111

WEP - Integrité

- Le contrôle d'intégrité de WEP, CRC, présente également des faiblesses:
  - Il n'utilise pas de clé
  - Il est linéaire
- Ces propriétés permettent de créer des trames illisibles mais valides sans connaitre la clé de chiffrement

WPA - Confidentialité

- WPA ajoute une couche supplémentaire par rapport à WEP, en utilisant l'algorithme TKIP
- TKIP génère la clé utilisée par RC4 pour générer le keystream en se basant sur plusieurs éléments:
  - Passphrase
  - SSID du réseau
  - Eléments échangés pendant l'authentification
- Chaque keystream est unique
- Récupérer la passphrase seule ne permet pas de déchiffrer le trafic
- Pour déchiffrer le trafic, il faut avoir capturé les informations échangées pendant l'authentification

WPA - Confidentialité

- Si l'authentification n'a pas été interceptée, possible d'envoyer une trame de désauthentification, pour forcer la station à se réauthentifier
- Les trames de désauthentification ne sont pas sécurisées et peuvent être envoyées par n'importe qui
- Une attaque par dictionnaire peut être utilisée pour retrouver la passphrase
- Certains outils, comme Wireshark, déchiffrent automatiquement le trafic s'ils détectent des messages d'authentification

WPA – Integrité

- WPA utilise également un nouveau contrôle d'intégrité: MIC
  - Protégé cryptographiquement
  - Utilise une clé dépendant des informations échangées pendant l'authentification
  - Plus robuste que le CRC

WPA2

- Un nouvel algorithme est utilisé pour chiffrer les données: AES
  - Contrairement à RC4, c'est un algorithme de chiffrement sûr
- Les clés de chiffrement sont construites à partir d'une passphrase et d'informations échangées pendant l'authentification
- La passphrase est vulnérable aux attaques par dictionnaire
- Comme pour WPA, en retrouvant la passphrase et en capturant les messages d'authentification, on peut déchiffrer le trafic
- L'intégrité est également assurée en utilisant AES, avec la même clé que celle utilisée pour chiffrer les données

WPA2 Enterprise

- Utilise également AES pour chiffrer et vérifier l'intégrité des données
- L'authentification se fait de manière plus complexe, avec une étape supplémentaire lors de l'authentification
- Les messages envoyés lors de l'authentification sont chiffrés, il n'est donc pas possible de les récupérer
- Il n'y a pas de passphrase, donc pas d'attaque par dictionnaire