Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

Hes·so

Téléinformatique – Ch. 21

Wireless

Vincent Magnin
vincent.magnin@hefr.ch

Objectifs

- Connaître les principales normes liées aux technologies sans fil.
- Savoir expliquer les différentes topologies et le matériel utilisé.
- Connaître les différents moyens de sécuriser une communication sans fil et en expliquer les avantages et les inconvénients.

Technologies sans fil

Il existe plusieurs types de liaisons sans fil, qui correspondent à des besoins et des problématiques différentes.

WPAN : Bluetooth (IEEE 802.15 standard), RFID, NFC...

Wi-Fi : IEEE 802.11 standard.

Mobile Broadband : 2G à la 5G.

Satellites : Starlink, liaisons satellitaires...

Classification des réseaux sans fil

WPAN

- Wireless Personal Area Network
- Réseau personnel à très petite échelle (moins d'un mètre).

WLAN

- Wireless LAN
- Réseau à échelle d'une pièce, d'un site, d'un bâtiment avec une portée jusqu'à quelques centaines de mètres.

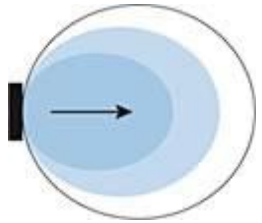
WWAN

- Wireless Wide Area Network
- Réseau étendu de plusieurs kilomètres en zone métropolitaine ou entre deux villes avec des relais d'ondes.

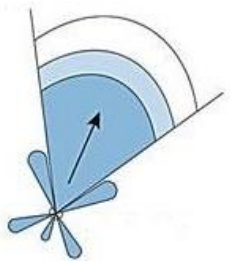
Types d'antennes

Antenne omnidirectionnelle : fournit une couverture à 360°, idéale pour les open-spaces, les halls, les salles de conférence et les espaces extérieurs.

Antenne directionnelle : concentre le signal dans une direction donnée. Cela permet d'améliorer la qualité du signal dans une certaine direction.



Antenne Yagi : antenne radio directionnelle pouvant être utilisée dans le cadre des réseaux Wi-Fi longue distance. Ces antennes sont généralement utilisées pour étendre la portée des hotspots en extérieur, dans une direction donnée.

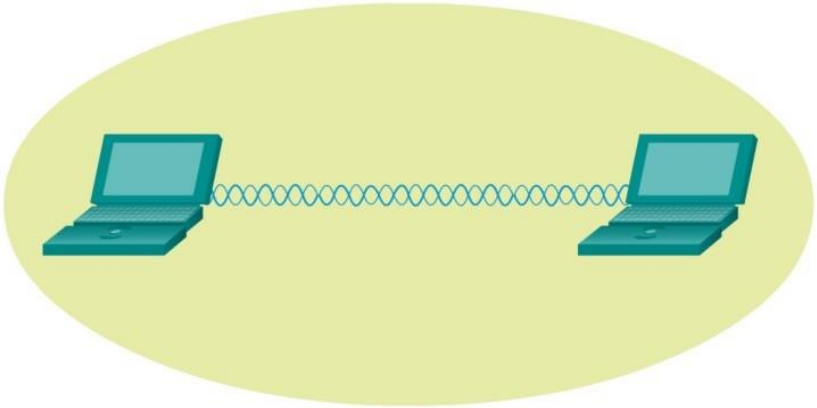


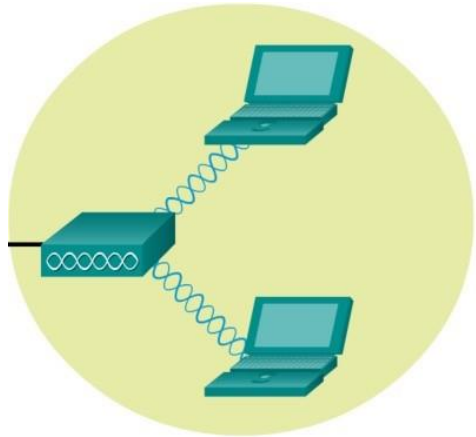
Topologies sans fil

Il existe 2 modes opératoires pour construire un réseau sans fil :

- Mode Ad-hoc : réseau sans fil où les stations se connectent les unes aux autres afin de constituer un réseau point à point.

- Mode infrastructure : des points d'accès (AP) comparables à des switchs gèrent les communications des clients. Ces bornes peuvent être reliées entre elles par le réseau filaire ou par réseau hertzien.

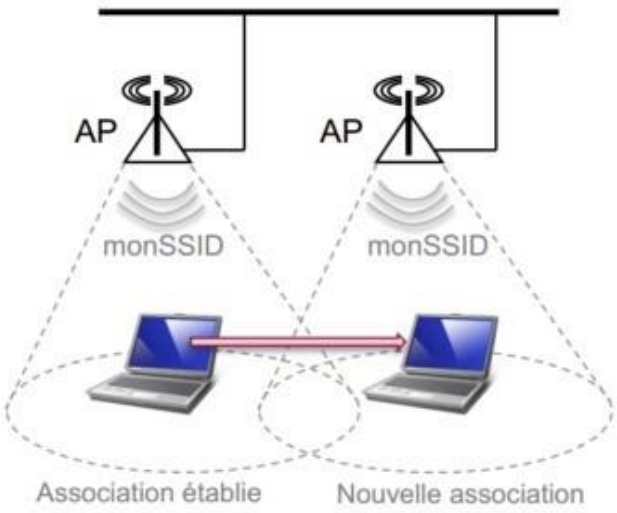




Roaming

Le roaming (itinérance) est le fait de changer de cellule pendant une communication. Cela engendre en général une courte perte de communication.

Le client change d'AP en fonction de la qualité du signal reçu. Le même principe est appliqué aux réseaux 4G et 5G où les mobiles sont en général connectés à 3 antennes en même temps et choisissent la meilleure.



Sécurité des réseaux sans fil

Il n'est pas possible de sécuriser de manière « physique » les réseaux sans fil : on ne peut pas (ou difficilement) limiter la propagation des ondes / des informations. C'est une porte d'entrée aux pirates (pas besoin d'accès physique).

Il existe de nombreuses menaces, comme l'interception, l'intrusion, le rogue AP, le DoS...

Il existe des protocoles d'authentification pour sécuriser l'accès à un réseau sans fil, comme WEP, WPA, WPA2 et WPA3.

La norme 802.1x/EPA a été créée pour généraliser le contrôle d'accès aux réseaux sans fil.

Sécurité des réseaux sans fil (2)

L'attaque par interception permet de capturer des données sans fil facilement au moyen d'interceptions illicites ou d'usurpation de l'identité de l'AP.

On peut réduire les risques d'interception par des mécanismes d'authentification et de confidentialité (chiffrement).

L'attaque par intrusion permet à des utilisateurs non autorisés d'accéder à des ressources du réseau.

On peut réduire les risques d'intrusion par des mécanismes d'authentification.

Sécurité des réseaux sans fil (3)

L'attaque par rogue AP permet à un AP non autorisé d'être installé par un utilisateur naïf ou délibérément, à des fins malveillantes.

On peut réduire les risques de rogue AP avec des logiciels de gestion de réseaux sans fil pour détecter des AP non autorisés.

L'attaque par DoS permet à un attaquant de lancer des interférences ou des messages spécifiques pour rendre le réseau inutilisable. Par exemple, on peut forcer la déconnexion des clients en usurpant l'identité de l'AP.

Les standards 802.11i et 802.11w permettent de contrer les attaques par DoS dans les réseaux sans fil.

Sécurisation préliminaire

Pour augmenter légèrement la sécurité d'un réseau sans fil, on peut procéder aux manipulations suivantes :

- Masquage du SSID : permet de cacher le SSID pour que seules les personnes le connaissant puissent se connecter au réseau

  → Problème : écoute du réseau pour trouver le SSID (Kismet, NetStumbler...).

- Filtrage des adresses MAC : autorise les clients à se connecter uniquement selon leur adresse MAC.

  → Problème : MAC spoofing (utilisation d'une fausse adresse MAC).

Références

- Ancien cours « Téléinformatique » (G. Waeber, S. Paccard, Q. Vaucher, N. Wirth).
- Ancien cours « Téléinformatique » (M. Roch-Neirey).