Attaques existantes

- **Deux types d'attaques**
  - ✓ **attaques passives:** capter, lire, espionner…les données sans les modifier
  - ✓ **attaques actives:** modifier les données, perturber le bon fonctionnement du réseau…

Rq: on ne peut juger lesquelles sont les plus dangereuses (passives ou actives), tout dépend du contexte et du type de données à sécuriser.

- **Attaques possibles**

✓ il existe une multitude d'attaques possibles (on peut en compter facilement une centaine), chacune a ses propres techniques et objectifs (ping flooding, SMTP overflow, FTP bounce, DoS…etc). Nous aborderons les plus importantes (cours et TD).

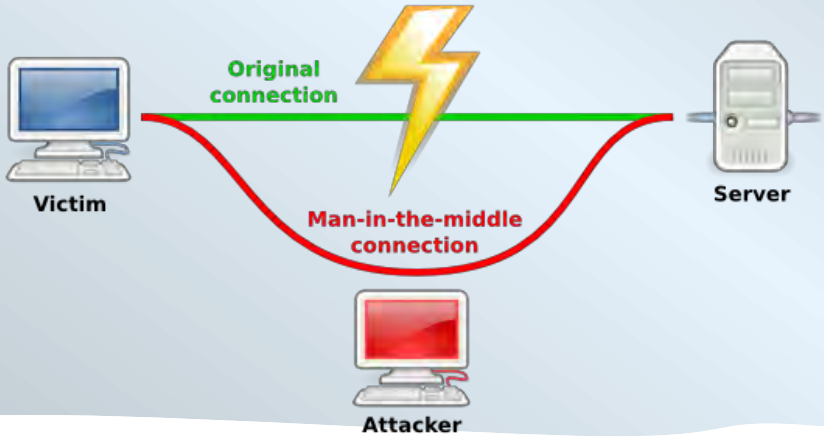
Rappel: Sécurité dans les réseaux sans fil

Les attaques que nous allons étudier concernent aussi bien les communications filaires que les communications sans fil, mais il est important de souligner qu'il y a des vulnérabilités spéciales au domaine du sans fil:

- ✓ Protection physique faible (vol facile des nœuds, perte, …)
- ✓ Capacités limitées (calcul, mémoire, énergie, …)
- ✓ Nature non filaire (brouillage, espionnage …)
- ✓ Nature provisoire des services

Attaques passives

- **Deux types d'attaques**
  - ✓ **Lecture de messages:** les données interceptées sont envoyées en clair (conversation téléphonique, email, fichiers, …) et peuvent contenir des informations sensibles ou confidentielles.
  - ✓ **Analyse de trafic:** si les données sont cryptées l'attaquant peut les analyser au moins et déterminer des informations intéressantes (emplacement et identités des machines, fréquences et longueur des messages, …)

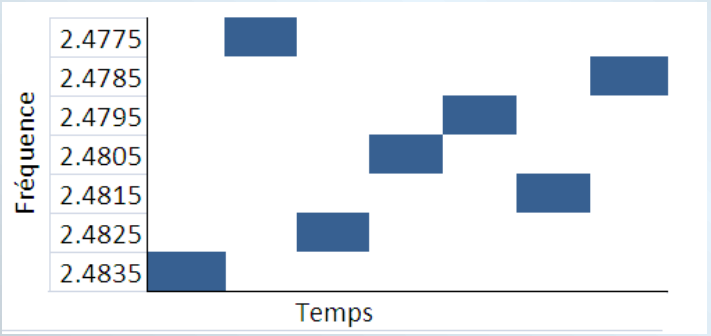


Ex: l'attaque Man in the middle

Attaques (1)

- **Jamming (brouillage)**
  - ✓ C'est une attaque de type Déni de service (DoS) dont le but est de mettre à plat une partie ou tout le système. Elle tente de perturber la communication par des interférences. Il existe:
    - ❖ Le *Constant jamming* : sans interruption
    - ❖ Le *Random jamming* : aléatoirement (ou même par intervalles)
    - ❖ Le *Reactive Jamming* : dès qu'il y a une communication
  - ✓ **Solution:**

Utilisation, par exemple, de la technique de saut de fréquences (ex: FHSS (Frequency Hopping Spread Spectrum))

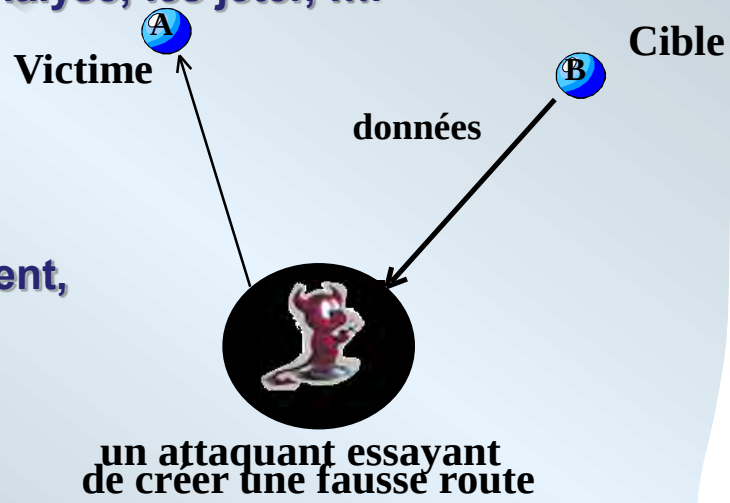


Attaques (2)

- **Tampering**
  - ✓ Capturer et accéder physiquement au nœud afin d'extraire toutes les informations (clés de cryptage, …)
- **Collision**
  - ✓ Comparable au *jamming* mais l'attaquant envoie son signal pendant une transmission
    - → Ceci crée une erreur de contrôle CRC
      - → Le message est détruit avec demande de retransmission
        - → Congestion et épuisement des batteries
  - ✓ Difficile à détecter (différencier les vraies des fausses collisions) et peut mener à un DoS

Attaques (3)

- **Blackhole (trou noir)**
  - ✓ Un nœud attaquant peut devenir trou noir s'il annonce qu'il a la meilleur métrique de routage (plus court chemin) (*en modifiant les tables de routage ou en communicant de fausses métriques par ex*)
    - → Les nœuds le choisiront pour router leurs paquets
      - → Il peut alors les engloutir pour analyse, les jeter, ….
- **Usurpation d'identité (*masquerade*)**
  - ✓ Un nœud malveillant se fait, tout simplement, passer pour un nœud de confiance
    - → **Solution:** Authentification



Attaques (4)

- **Boucle de routage**
  - ✓ Coopération de plusieurs nœuds adversaires pour créer des boucles dans le mécanisme de routage entre une source et une destination.
    - → Solution: utiliser des TTL (*Time To Live*) pour limiter le nombre de sauts
- **Attaque Sybille**
  - ✓ Un nœud malveillant prétend être plusieurs nœuds légitimes (identités multiples) à la fois
    - → Solution: L'authentification

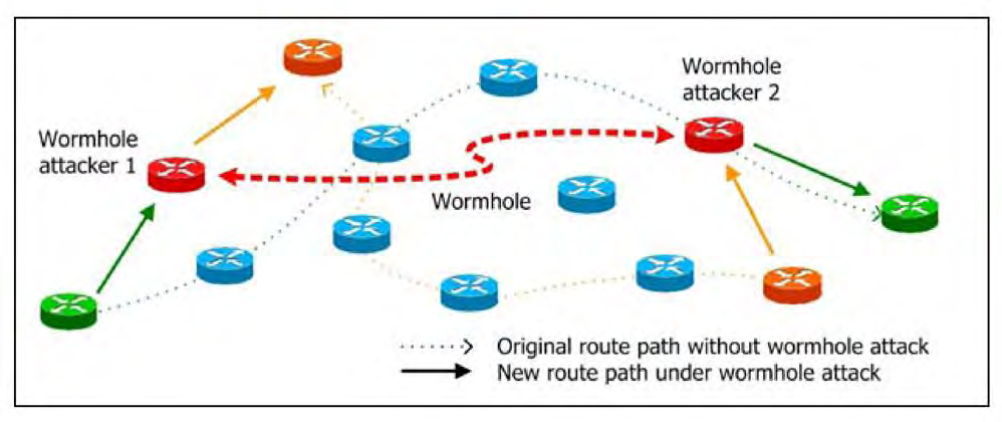
Attaques (5)

- **Réplication de nœuds**
  - ✓ Variante de l'attaque Sybille: capturer un nœud et construire des copies légitimes de ce nœud y compris de sa clé.
    - → Corruption de données
    - → DoS partiel ou total

- **Hello Flood**
  - ✓ Paquet HELLO est envoyé à l'origine pour la découverte du voisinage. Cette attaque inonde le réseau de paquets Hello en provoquant de fausses listes de voisins
    - → Solution: L'identification

Attaques (6)

- **Wormhole (trou de ver)**
  - ✓ Un nœud compromis enregistre les paquets et les envoie via un lien ou tunnel vers un autre nœud malicieux dans le réseau.



- **Forced Delay**
  - ✓ Un nœud malveillant retarde délibérément les paquets. Cette attaque est utilisée pour dégrader la qualité de service des applications dans les systèmes temps réel.

Attaques (7)

- **Désynchronisation**
  - ✓ L'attaquant envoie successivement à l'metteur et au récepteur des messages avec de faux numéros de séquence, ce qui les oblige à rompre leur synchronisation
    - → il faut contrôler l'identité et l'intégrité des paquets pour contrer cette attaque
- **Attaque injection de message**
  - ✓ L'attaquant fabrique un faux message conforme au format échangé et l'injecte dans le réseau
    - → Cette attaque peut avoir plusieurs objectifs (inondation, usurpation d'identité, …..)

Attaques (8)

- **Attaque par rejeu (replay)**
  - ✓ Même principe que l'attaque par injection, mais dans cette attaque, le message n'est plus fabriqué mais intercepté puis réinjecté dans le réseau.
- **Attaque par harcèlement**
  - ✓ Emission régulière et inutile de paquets pour augmenter la charge du réseau
    - → **Résultat : DoS**

Conclusion: la liste des attaques possible est encore longue, on a cité les plus communes, elle sera enrichie au TD, mais reste plusieurs attaques à connaitre pour avoir une vision globale, sachant qu'une bonne base en réseau est indispensable (attaque ARP, ICMP……)