Réseaux Ad-Hoc

Cours systèmes de communications

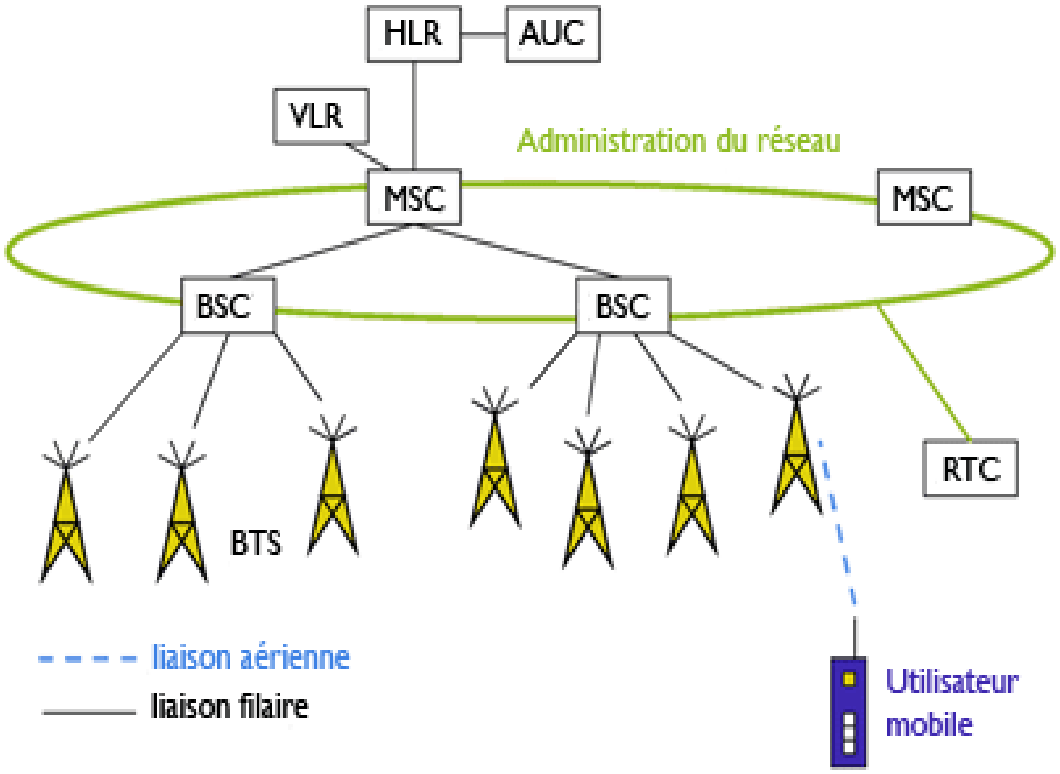
M1 SMART'COM

Introduction

- Les réseaux de téléphonie mobile que nous utilisons aujourd'hui souffrent de lacunes en termes de débit, de consommation, de flexibilité, de sécurité.
- C'est pourquoi de nouvelles architectures de réseaux sont proposées, qui vont des réseaux radio maillés aux réseaux ad hoc.

Réseaux sans fil à stations de base (1)

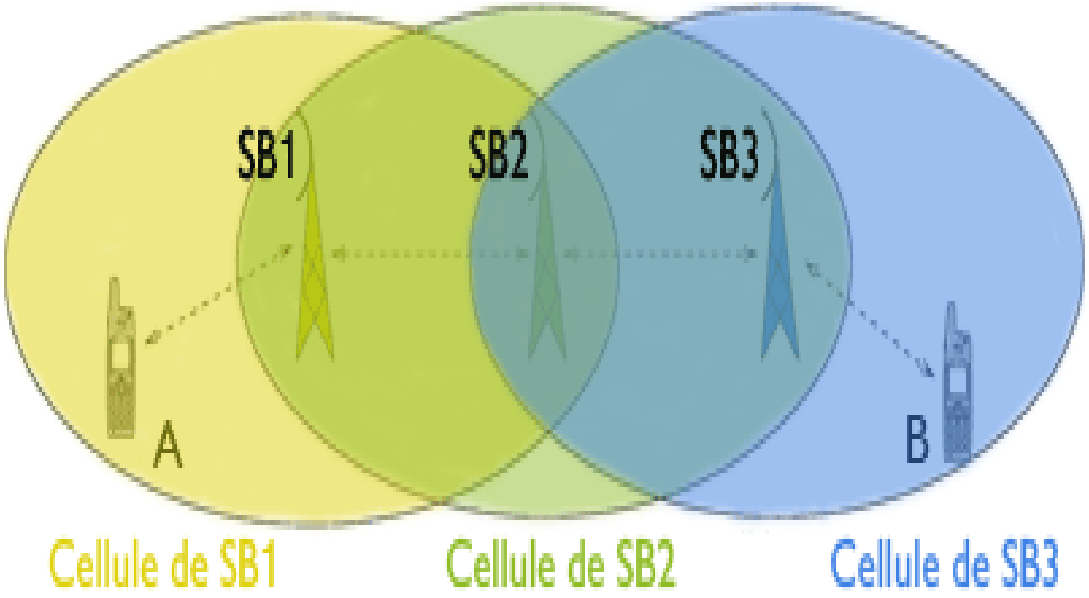
- Exemple GSM



Réseaux sans fil à stations de base (2)

- Ils souffrent d'un coût de déploiement important.
- Les prix des licences
- Une infrastructure fixe interconnectée de manière filaire.
- La nécessité de perpétuellement faire évoluer la configuration du réseau pour offrir la meilleure qualité de service possible

Mesh Networks: Réseau maillé (1)



Mesh Networks: Réseau maillé (2)

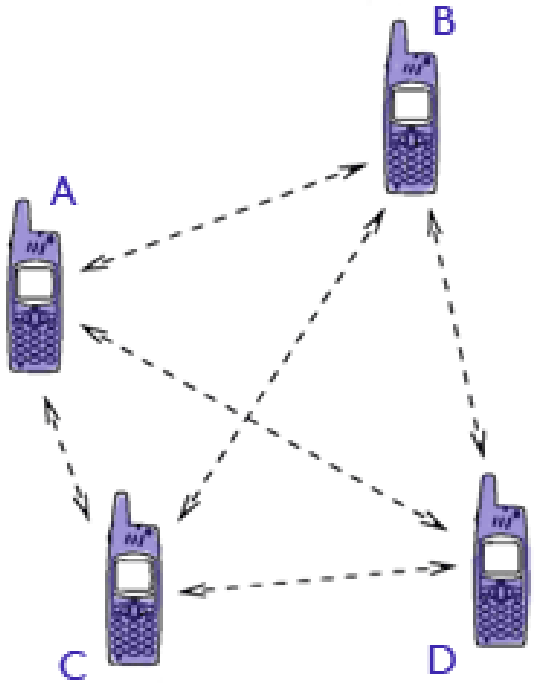
- Un ensemble de stations de base qui couvrent la zone visée.
- Les stations de base agissent comme des relais radio pour les communications des mobiles. Dans un réseau radio maillé, chaque mobile est rattaché à la station de base la plus proche, avec laquelle il communique exclusivement.
- Cette station de base peut ainsi faire office de chef d'orchestre et organiser les communications « au mieux » afin d'éviter les pertes de et d'optimiser l'utilisation de la bande passante

Réseau Ad-hoc: Définition (Wikipédia)

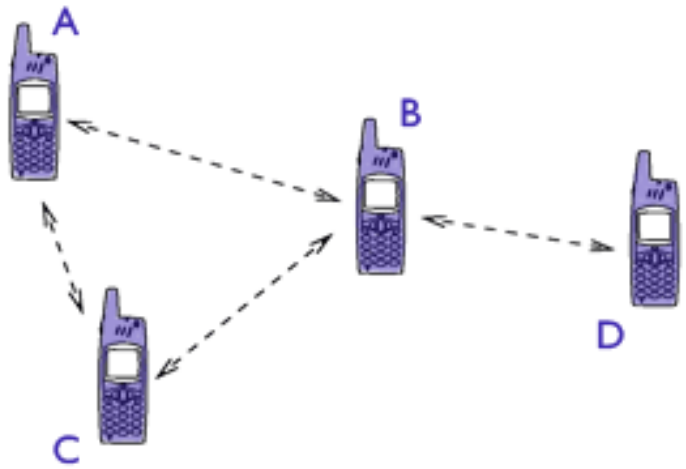
- Les **réseaux *ad hoc*** sont des réseaux sans fil capables de s'organiser sans infrastructure définie préalablement.
- Les réseaux ad hoc, dans leur configuration mobile, sont connus sous le nom de réseau mobile Ad-hoc
- Chaque entité (*node*) communique directement avec sa voisine.
- Pour communiquer avec d'autres entités, il lui est nécessaire de faire passer ses données par d'autres qui se chargeront de les acheminer.

Réseau Ad-hoc: Graphe

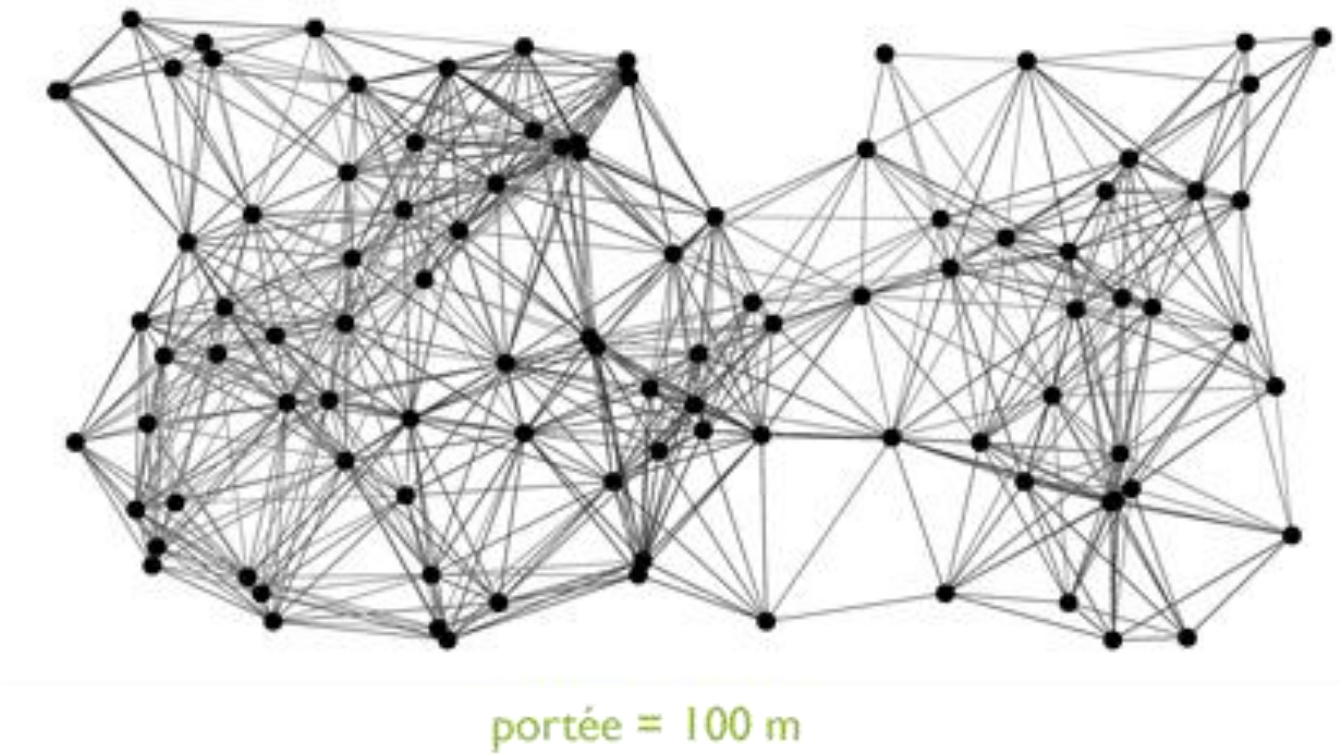
- Graphe complet
- Communications ad hoc simple saut.



- Graphe non-complet



Réseau Ad-hoc: l'équilibre entre la connexité du réseau et la consommation énergétique.



une portée de 100m assure la connexité mais engendre plus de consommation énergétique qu'une portée de 67m qui est suffisante pour la connexité du réseau.

Mobile Ad-hoc Networks: MANET

- MANET: est le nom d'un groupe de travail de l'**Internet Engineering Task Force (**IETF), créé en 1998/1999, chargé de standardiser des protocoles de routage basés sur la technologie IP pour les réseaux ad hoc.

Les caractéristiques des réseaux ad hoc (1)

- **L'absence d'infrastructure centralisée**
  - Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue
- **Une topologie dynamique**
  - Les unités mobiles du réseau, se déplacent d'une façon libre et arbitraire. Par conséquent la topologie du réseau peut changer, à des instants imprévisibles, d'une manière rapide et aléatoire. Les liens de la topologie peuvent être unis ou bidirectionnels.

Les caractéristiques des réseaux ad hoc (2)

- **La contrainte d'énergie**
  - Les équipements mobiles disposent de batteries limitées
  - Une partie de l'énergie est déjà consommée par la fonctionnalité du routage.
- **Une bande passante limitée**
  - Une des caractéristiques primordiales des réseaux basés sur la communication sans fil est l'utilisation d'un médium de communication partagé.

Les caractéristiques des réseaux ad hoc (3)

- **L'hétérogénéité des nœuds**
  - Un noeud mobile peut être équipé d'une ou plusieurs interfaces radio ayant des capacités de transmission variées et opérant dans des plages de fréquence différentes.
  - les noeuds peuvent avoir des différences en terme de capacité de traitement (CPU, mémoire) de logiciel et de mobilité (lent, rapide).

Les caractéristiques des réseaux ad hoc (4)

- **Sécurité et Vulnérabilité**
  - tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau.
  - Les possibilités de s'insérer dans le réseau sont plus grandes
- **Multihops**
  - plusieurs nœuds mobiles peuvent participer au routage

Les domaines d'applications des réseaux mobiles ad hoc

- Les services d'urgence
- Le travail collaboratif et les communications dans des entreprises ou bâtiments
- Applications commerciales
- Réseaux de senseurs
- Le cadre informatique

Les protocoles de routage dans les réseaux ad hoc

- Suivant la manière de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent être classés en trois catégories:
  - Protocoles réactifs: ne calculer une route qu'à la demande d'une application
  - Protocoles proactifs: entretiennent toutes les routes du réseau par l'échange de trames périodiques de contrôle.
  - Protocoles hybrides: combinent les idées des protocoles proactifs et réactifs pour tirer profit des avantages de chacun d'eux.

Réseaux Ad-Hoc: Services de sécurité (1)

- Contrôle d'accès
  - empêcher les nœuds étrangers d'accéder au réseau.
  - Le contrôle d'accès donne aux nœuds légitimes un moyen de détecter les messages provenant de sources externes au réseau
- Authentification
  - s'assurer de l'identité des entités en cours de communication.
  - le destinataire sera sûr que le message provient de la source prétendue.

Réseaux Ad-Hoc: Services de sécurité (2)

- Confidentialité
  - assurer que l'information ne peut pas être interprétée par des tiers non autorisés.
  - Les informations de routage doivent aussi, dans certains cas, rester secrètes.
- Intégrité
  - assurer que la modification des données transmises sera détectée. On utilise souvent les fonctions de hachage pour assurer l'intégrité

Réseaux Ad-Hoc: Services de sécurité (3)

- Non-répudiation
  - empêcher un nœud de nier l'envoi ou bien la réception d'un message.
- Fraîcheur
  - garantir que les données présentes échangées sur le réseau sont viables.
  - permet de lutter contre la réinjection d’anciens messages interceptés par un attaquant

Réseaux Ad-Hoc: Services de sécurité (4)

- Disponibilité :
  - assurer la présence des services du réseau même en présence d'attaques de déni de service.
  - Ces attaques peuvent se présenter au niveau de différentes couches d'un réseau ad hoc.
  - La disponibilité donne aussi une assurance sur la réactivité et le temps de réponse du réseau

Les attaques possibles dans les protocoles de routage

- Les attaques passives
  - l'intrus intercepte et analyse le trafic pour déterminer les relations entre les nœuds et éventuellement déterminer les nœuds importants dans le fonctionnement du réseau .
  - Ces informations peuvent être une préparation pour lancer une attaque active.
  - Par exemple une attaque par déni de service ciblant les nœuds importants peut faire tomber le réseau (mettre en disfonctionnement).
- Les attaques actives
  - l'intrus tente de perturber le fonctionnement du réseau en supprimant, en modifiant, en fabriquant des paquets ou en rejouant d'anciens paquets.

les attaques actives les plus connues (1)

- Relais sélectif de paquets (Selective forwarding) :
  - Un nœud décide de ne pas transmettre les données de certains nœuds. La raison peut être aussi bien d'ordre énergétique, que liée à une attaque.
- Attaque du trou noir :
  - Un noeud falsifie les informations de routage pour forcer le passage des données par lui-même.
  - Sa seule mission est ensuite de ne rien transférer, créant ainsi une sorte de puits ou « trou noir » dans le réseau.

les attaques actives les plus connues (2)

- Attaque du trou de ver :
  - Cette variante du trou noir consiste à réinjecter les paquets absorbés en un autre point (souvent distant) du réseau. Pour des distances plus longues que la couverture normale d'une transmission sans fil d'un hop, un attaquant peut s'arranger pour faire arriver ses paquets plus rapidement que par une route multi-hops. Il suffit pour lui d'utiliser un réseau externe câblé ou un transfert sans fil directionnel à forte puissance.
- Attaque de l'identité multiple :
  - Un noeud se fait passer pour plusieurs nœuds potentiellement distants, créant des incohérences dans les tables de routage des noeuds voisins.

les attaques actives les plus connues (2)

- Attaque par chantage :
  - Un nœud malicieux fait annoncer qu'un autre nœud légitime est malicieux pour éliminer ce dernier du réseau. Si le nœud malicieux arrive à attaquer un nombre important de nœuds, il pourra perturber le fonctionnement du réseau.
- Privation de mise en veille :
  - Elle a pour but de consommer toutes les ressources de la victime en l'obligeant à effectuer des calculs ou à recevoir ou transmettre des données inutilement.

les attaques actives les plus connues (3)

- Brouillage radio :
  - Il consiste à perturber le canal radio en envoyant des informations inutiles sur la bande de fréquences utilisées. Ce brouillage peut être temporaire, intermittent ou permanent.
  - De même, son champ d'action doit être pris en compte ; son effet est-il limité à quelques nœuds ou est-il suffisamment puissant pour bloquer le réseau tout entier ?

les attaques actives les plus connues (4)

- Attaque de l'inondation de HELLO :
  - De nombreux protocoles de routage utilisent des paquets « HELLO » pour découvrir les nœuds voisins et ainsi établir une topologie du réseau.
  - La plus simple attaque pour un intrus consiste à envoyer un flot de tels messages pour inonder le réseau et empêcher d'autres messages d'être échangés. De plus, s'il parvient à émettre à une portée suffisante, des nœuds distants vont ajouter l'intrus comme nœud voisin dans leurs routes et fausser ainsi complètement le routage de l'information dans le réseau