REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud MAMMERI de TIZI-OUZOU
Faculté de Génie Electrique et d'Informatique
Département d'Electronique

Mémoire

De fin d'études

En vue de l'obtention du Diplôme de Master En Electronique

Option : Réseaux et télécommunication

Thème

Sécurité et Routage dans les réseaux Ad hoc

Dirigé par :

M^r^ LAHDIR .M

Présenté par :

M^elle^ YAHI Siham

M^elle^ MALLEK Farida

Promotion : 2012/2013

Résumé

Le choix des éléments relais dans un réseau ad hoc mobile, nommé également Mobile Ad hoc Network : MANET, s'effectue par un protocole de routage. Le routage est la méthode d'acheminement des informations d'une source vers une destination à travers un réseau donné. Le problème du routage consiste à déterminer un acheminement optimal des paquets par rapport à certains critères de performance. Dans les réseaux ad hoc, il s'agit de trouver une méthode d'acheminement pour un grand nombre de nœuds dans un environnement caractérisé par des changements rapides de la topologie du réseau dus à la mobilité des hôtes, ainsi que d'autres caractéristiques comme l'absence d'infrastructure, la limitation de la bande passante, la limitation de source d'énergie, et les modestes capacités de traitement et de mémoire. La question actuelle n'est plus la recherche de la route optimale, mais la recherche du chemin le plus sûr. Plusieurs stratégies ont été proposées pour sécuriser les protocoles de routage ad hoc. Les mécanismes de sécurité utilisés dans les réseaux filaire et sans fil classiques et qui se basent sur une infrastructure centralisée ne sont pas appropriés à un réseau ad hoc complètement décentralisé. Les solutions qui ont été développées en essayant de les adapter à la nature des réseaux ad hoc s'avèrent coûteuses, lentes et consomment beaucoup de ressources (énergie, capacité de calcul et de stockage), ce qui dégrade les performances globales du réseau.

Mots clés : réseau Ad hoc, sans fil, routage, protocole de routage, proactif, réactif, simulateur NS2, AODV, DSDV, OLSR.

Je dédie ce modeste travail :

- *A la mémoire de mon père que Dieu le compte parmi ces fidèles ;*
- *A ma très chère mère ma source de tendresse qui a tout sacrifié pour moi ;*
- *A mon cher frère Kamel que Dieu le protège;*
- *A mes chères sœurs Wezna, Meriem et Lynda ;*
- *A mes cousins et cousines ;*
- *A mes chers amis ;*
- *A tous ceux qui ont apporté de l'aide de prés ou de loin pour la réalisation de ce travail.*

SIHAM

Sommaire

CHAPITRE III : La sécurité dans les réseaux Ad hoc

Aujourd’hui, les réseaux sans fil ont connu une forte expansion et sont de plus en plus populaires du fait de leur facilité de déploiement. L'évolution rapide de la technologie dans le domaine de la communication sans fil, a permis aux usagers munis d'unités de calcul portables d'accéder à l'information à n’importe quel moment depuis n’importe quel endroit. Cet environnement n'astreint plus l'usager à une localisation fixe, mais lui permet une libre mobilité tout en assurant sa connexion avec le réseau. Il offre des solutions ouvertes pour fournir des services essentiels là où l’installation d’infrastructures n’est pas possible.

Un réseau ad hoc est un ensemble autonome et coopératif de nœuds mobiles qui se déplacent et communiquent par une transmission sans fil qui ne suppose pas d'infrastructure préexistante. Le réseau ad hoc se forme de manière spontanée et provisoire dès que plusieurs nœuds mobiles se trouvent à portée radio les uns des autres. Les nœuds communiquent, selon la distance qui les sépare, par deux modes de communication : soit les nœuds mobiles peuvent directement communiquer (en transmission ad hoc) car ils sont à portée de transmission, soit ils doivent utiliser d'autres nœuds mobiles comme des relais pour acheminer les paquets à destination. Ainsi, chaque nœud est à la fois utilisateur final et routeur afin de relayer les paquets vers leur destination finale, en raison de la couverture limitée du champ radio disponible pour chaque nœud.

Le choix des éléments relais dans un réseau ad hoc mobile, nommé également Mobile Ad hoc Network : MANET, s'effectue par un protocole de routage. Le routage est la méthode d’acheminement des informations d’une source vers une destination à travers un réseau donné. Le problème du routage consiste à déterminer un acheminement optimal des paquets par rapport à certains critères de performance. Dans les réseaux ad hoc, il s’agit de trouver une méthode d’acheminement pour un grand nombre de nœuds dans un environnement caractérisé par des changements rapides de la topologie du réseau dus à la mobilité des hôtes, ainsi que d’autres caractéristiques comme l’absence d’infrastructure, la limitation de la bande passante, la limitation de source d’énergie, et les modestes capacités de traitement et de mémoire. La question actuelle n’est plus la recherche de la route optimale, mais la recherche du chemin le plus sûr. Plusieurs stratégies ont été proposées pour sécuriser les protocoles de routage ad hoc. Les mécanismes de sécurité utilisés dans les réseaux filaire et sans fil classiques et qui se basent sur une infrastructure centralisée ne sont pas appropriés à un réseau ad hoc complètement décentralisé. Les solutions qui ont été développées en essayant de les adapter à la nature des réseaux ad hoc s’avèrent coûteuses, lentes et consomment beaucoup de ressources (énergie, capacité de calcul et de stockage), ce qui dégrade les performances globales du réseau.

Dans ce travail, nous nous intéressons aux problèmes de sécurité des protocoles de routage dans les réseaux ad hoc. Pour cela, nous avons organisé notre mémoire en quatre chapitres ; dont le premier chapitre ; nous présenterons un aperçu général sur les réseaux ad hoc, leurs concepts, leurs caractéristiques, ainsi que leurs applications. Le deuxième chapitre se focalise sur les protocoles de routage dans les réseaux Ad hoc ;nous aborderons dans le troisième chapitre la problématique de la sécurité dans les réseaux ad hoc en expliquant les différents types d'attaques qui peuvent menacer le réseau ainsi que les services de base de sécurité existants et proposés pour faire face à ces menaces. Dans le quatrième chapitre nous décrirons l'outil de simulation NS2 et les éléments qui l'accompagnent pour la mise en œuvre de notre application ainsi ; nous faisons une étude comparative des deux protocoles AODV et DSDV effectuant différents tests et en interprétant ensuite les résultats obtenus.

Enfin ; nous terminerons notre travail par une conclusion générale.

I.1 Introduction :

Les réseaux mobiles sans fils engendrent deux catégories : les réseaux avec infrastructure basé sur une communication cellulaire et qui obéissent à une architecture client/serveur, et le modèle des réseaux sans infrastructure ou Ad hoc définit par une collection des stations mobiles communiquant à l'aide de leurs interfaces sans fils.

Dans ce chapitre nous avons donné un aperçu sur les réseaux sans fils, puis présenter l'environnement mobile et quelque concept de base de cet environnement, par la suite, nous nous focaliserons sur l'étude des caractéristiques des Ad hoc, leurs avantages, leurs inconvénients et leurs domaines d'applications.

I.2. Les réseaux sans fils :[1]

I.2.1.Définition :

Un réseau sans fils (Wireless LAN ou WLAN ou IEEE 802.11…) est comme son nom l'indique, un réseau dont lequel au moins deux terminaux peuvent échanger des informations sans aucune établissement d'une liaison filaire, ils utilisent des médiums radio ou infrarouge pour l'échange d'information.

C'est un système de transmission des données, assurant une liaison indépendante de l'emplacement des périphériques informatiques composant le réseau. Ce qui donne a l'utilisateur la possibilité de se déplacer dans une zone géographique plus au moins étendu.

I.2.2. Les catégories de réseau sans fils:

On distingue généralement plusieurs catégories de réseau sans fils, selon le périmètre géographique permettant une connectivité :

- R**éseaux personnels sans fil :** Les WPAN sont des réseaux sans fil de faible portée (quelques dizaines de mètres) à usage personnel, plusieurs technologies exploitent les WPAN tel que la technologie Bluetooth, technologie zigBee, la liaison infrarouge…etc.
- **Réseaux locaux sans fil :** Les WLAN couvrent l'équivalent d'un réseau local d'entreprise, sa portée est d'environ une centaine des mètres. Différentes technologies utilisent les WLAN comme : Wifi, hiper LAN2 (High Performance Radio LAN 2.0)…etc.

- **Réseaux métropolitains sans fil (norme IEEE 802.16) :** Les WMAN sont connus sous le nom la boucle locale radio (BLR) qui offre un débit de 1 à 10Mbit /s pour une portée de 4 à 10 Km.
- **Réseaux étendus sans fil :** Le réseau étendu sans fil est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes : **GSM (**Global System for Mobile Communication), **GPRS** (General Packet Radio Service), **UMTS** (Universal Mobile Telecommunication System),…etc

I.3. Environnements mobiles :[2] [11]

Un environnement mobile est un système composé de sites mobiles et qui permet à ses utilisateurs d'accéder à l'information indépendamment de leurs positions géographiques. Les réseaux mobiles ou sans fil, peuvent être classés en deux classes : les réseaux avec infrastructure et les réseaux sans infrastructure.

I.3.1.Les réseaux sans fils avec infrastructure (cellulaire):

Ce modèle est composé de deux ensembles d'entités distinctes :

1- Les "sites fixes" du réseau filaire.

2- Les "sites mobiles".

Les stations de base sont interconnectées entre eux via une liaison filaire, et chaque station de base peut communiquer directement avec les sites mobiles en utilisant une interface sans fil.

L'ensemble formé par le point d'accès et les stations situées dans sa zone s'appelle ensemble des services de base (BSS) et constitué une cellule. La figure (I.1) montre un réseau sans fil avec infrastructure :

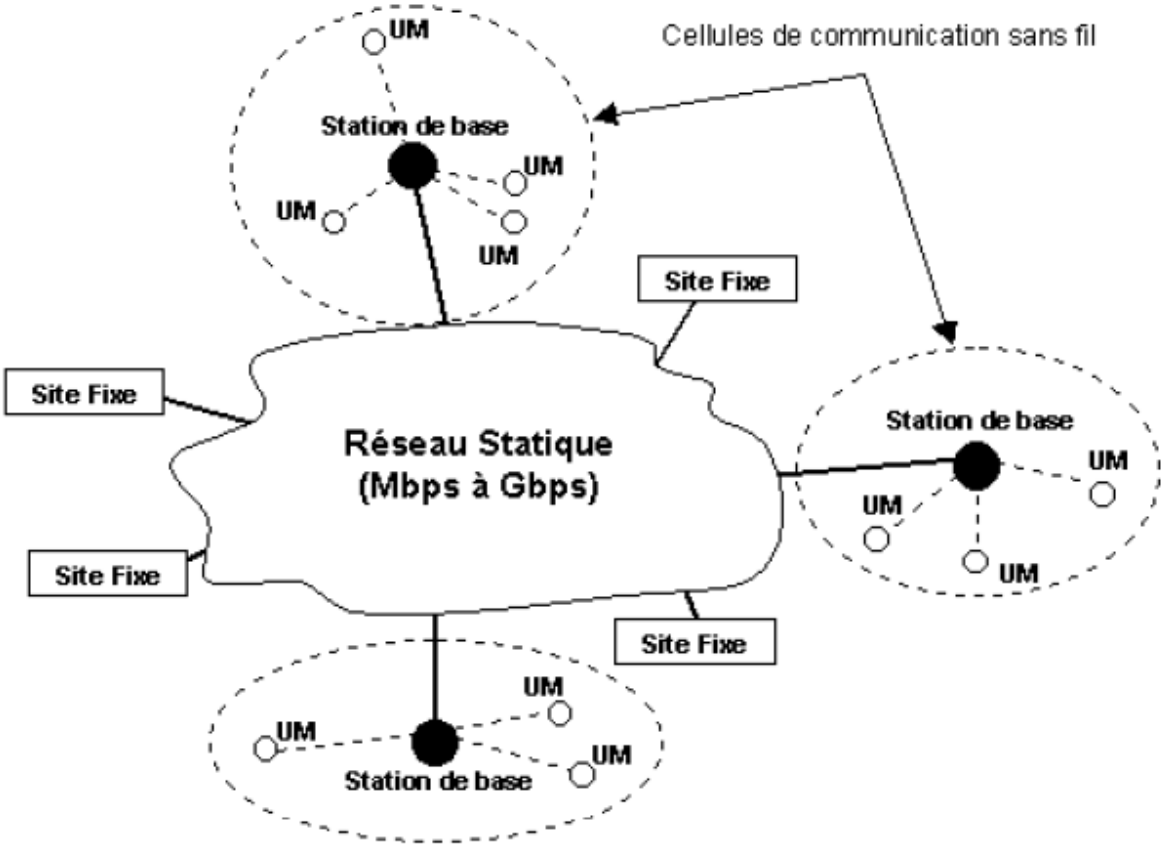


Figure I.1 : Le modèle des réseaux mobiles avec infrastructure

I.3.2. Les réseaux sans fils sans infrastructure (ad hoc) : [4]

Dans ce mode des réseaux les différents nœuds peuvent échanger des informations sans l'aide d'une station de base ; tout les nœuds du réseau sont mobiles et communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil.

Exemple du réseau sans infrastructure est celui des réseaux ad hoc dont les unités mobiles utilisent les ondes radio pour communiquer entre eux sans l'aide d'une infrastructure préexistante ou administration centralisée.

La figure (I.2) montre un modèle sans infrastructure contenant les unités mobiles :

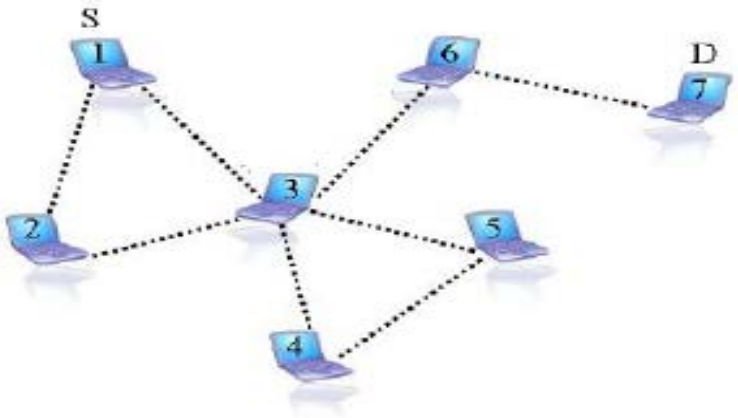


Figure1.2.Réseau Ad hoc

I.4. Les réseaux mobile ad hoc :[1][3]

I.4.1.Définition ad hoc :

Un réseau mobile ad hoc appelé généralement MANET (Mobile Ad hoc Network), est un réseau sans fil formé par une collection d'entités mobiles (nœuds), ayant la possibilité de communiquer entre eux sans passer par une autre infrastructure.

C'est un réseau spontané c'est un dire que les équipements qui le composent sont capable de s'organiser en réseau sans aucune configuration initiale. Cette caractéristique lui donne une topologie instable qu'elle doit être découverte dynamiquement ; de même le changement de topologie est fréquent lors de l'existence de réseau.

La figure (I.3) illustre le changement de topologie dans le réseau ad hoc :

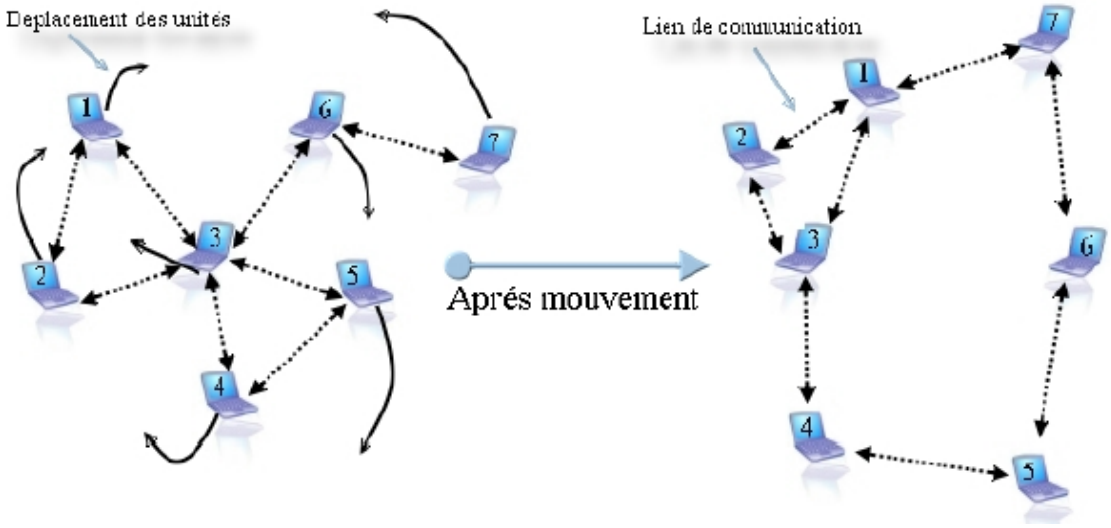


Figure I.3. Le changement de la topologie des réseaux ad hoc

I.4.2.Application des réseaux ad hoc :

Historiquement, les réseaux ad hoc ont été introduits dans le but d'améliorer les communications dans le domaine militaire. Cependant avec l'avancement des recherches dans le domaine des réseaux et l'émergence des technologies sans fil, les réseaux ad hoc ont montré leur utilités dans plusieurs applications et services tel que :

- Les services d'urgence : opération de recherche et de secours des personnes, tremblement de terre, feux, inondation, dans le but de remplacer l'infrastructure filaire.
- Le travail collaboratif et les communications dans des entreprises ou bâtiments : dans le cadre d'une réunion ou d'une conférence par exemple.
- Les bases de données parallèles.
- Applications commerciales : pour un paiement électronique distant ou pour l'accès mobile à l'Internet.
- Le télé-enseignement.

Généralement, les réseaux ad hoc sont plus utilisés dans les domaines nécessitant un déploiement d'infrastructure trop couteuse ou non fiable.

I.4. 3. Caractéristiques des MANET :[2]

Les r:éseaux Ad hoc sont caractérisés par :

1. La 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.

2. La bande passante limitée : Une des caractéristiques des réseaux basés sur la communication sans fil est l'utilisation d'un médium de communication partagé. Ce partage fait que la bande passante réservée à un hôte soit modeste.

3. Les contraintes énergétiques : Cela est dû au fait que chaque unité doit bien souvent embarquer une alimentation autonome telle que les batteries ou des autres sources consommables.

4. L'absence d'infrastructure : Les réseaux ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructure préexistante et d'une administration centralisée. Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue.

5. Une sécurité physique limitée : Les réseaux mobiles ad hoc sont plus atteignable par le problème de sécurité, que les réseaux filaires classiques.

6. erreur de transmission : Les erreurs de transmission radio sont plus fréquentes que dans les réseaux filaires.

7. Nœud caché : Ce phénomène est très particulier à l'environnement sans fil. Deux stations sont dite cachées lorsqu'elles sont trop éloignées pour se détecter mais que leurs zones de transmissions ne sont pas disjointes, par exemple si une station A tente d'émettre une trame a un nœud B situé a l'intersection de sa zone de transmission, cela provoque une collision.

La figure (I.4) montre le problème des nœuds cachés :

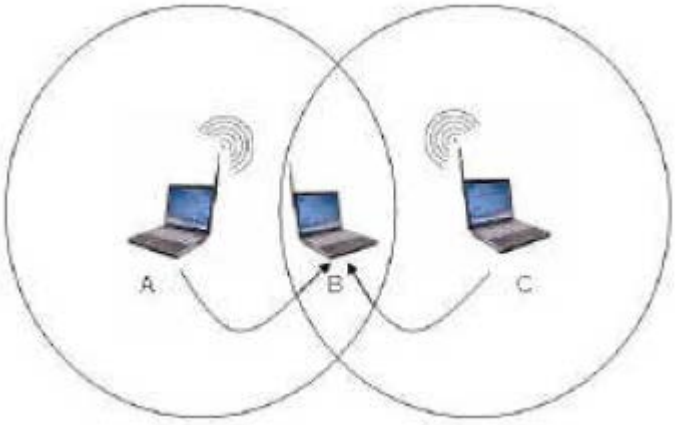


Figure I.4. Problème des nœuds cachés

I.4.4.Architecture ou topologies des réseaux ad hoc :

Les réseaux ad hoc peuvent être soit plate soit hiérarchique :

1. **Architecture plate** : dans cette architecture tous les nœuds participent au routage des paquets étant donnés qu'ils sont en même niveau.

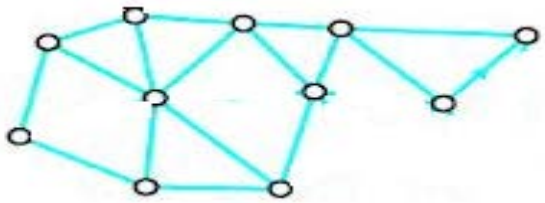


Figure I.5 Architecture plate

2 .Architecture hiérarchique : Dans ce type un groupe des nœuds mobile sont réunis afin de former des ensembles nommés « clusters » ; dans chaque cluster un seul nœud se charge du routage des paquets. Ce dernier appelé maitre ou clusterhead.

La figure (I.6) montre l'architecture hiérarchique :

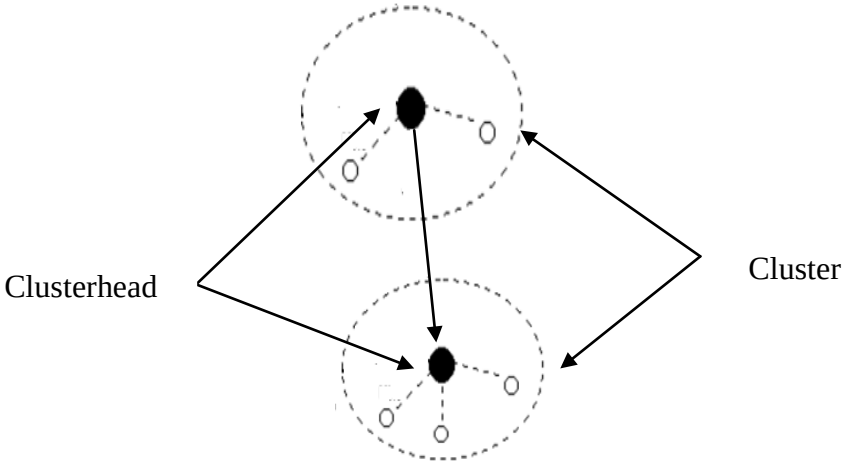


Figure I.6. Architecture hiérarchique

I.4.5. Les modes de communication dans le réseau ad hoc :

La communication dans les réseaux ad hoc se réalise en utilisant plusieurs modes qui sont :

- **La communication point a point « unicast » :** Dans ce mode de communication le paquets est adressé à un seul nœud mobile.
- **La communication multi point « multi cast »** : contrairement à l'unicast, un paquet est adressé à un ensemble des unités mobile dans le réseau.
- **La diffusion Broadcast** : un paquet est adressé à toutes les unités composant le réseau.

La figure suivante présente les trois modes de communication citée précédemment :

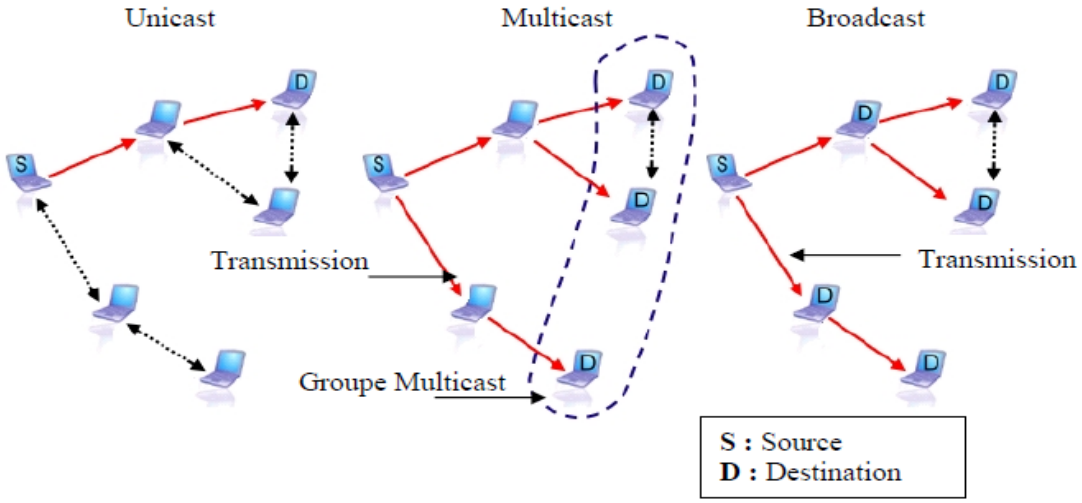


Figure I.7 Modes de communication d'un réseau mobiles ad hoc

I.4.6.Les avantages des réseaux ad hoc :

Les réseaux ad hoc offrent plusieurs avantages, citant :

- La tolérance aux pannes : la rupture d'un lien dans le réseau ad hoc est réparée par les autres nœuds en cherchant des nouvelles routes pour atteindre la destination.
- La mobilité des nœuds : la liaison sans fil permet aux nœuds de se déplacer dans le réseau.
- Un coût faible.
- L'indépendance technique et commerciale, vis-à-vis de point d'accès.
- La rapidité de mise en place.
- La robustesse : un réseau évolutif et dynamique.

I.4.7. Les inconvénients des réseaux ad hoc :[5]

Il existe beaucoup de problèmes techniques dans les réseaux ad hoc :

1. **Problèmes de transmission radio :** plusieurs problèmes liés a la transmission radio tel que :

- Augmentation de nombre d'erreurs sur la transmission.
- Amoindrissement des performances du lien radio.
- Diminution de débit de la liaison.
- La redondance.

2. La mobilité des nœuds :

- Modification de la topologie de réseau du à la densité des nœuds.
- Transformation du tracé des routes lors des échanges des paquets.

3. Consommation d'énergie : la durée de vie d'un équipement dépend de la durée de vie de la batterie, pour cela la consommation d'énergie doit obligatoirement diminuée.

4. Les problèmes liés au routage : le problème de routage est l'un des problèmes majeurs dans les réseaux ad hoc, il se pose sur l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modeste capacité de calcul, de sauvegarde et de changements rapides de topologies.

5. Problème de sécurité : la sécurité dans les réseaux ad hoc constitue l'une des préoccupations durant la planification, la mise en place ainsi la gestion du réseau. Cette dernière dépend de plusieurs paramètres tel que : authentification, confidentialité, intégrité et disponibilité ; elle concerne deux points, la sécurité des données transitant sur le réseau est limité étant donné que le média de transmission est partagé par tous les nœuds de réseau.et la sécurité du routage. Ces deux aspects comportent quelques vulnérabilités et sont exposés à plusieurs attaques.

I.5. Conclusion :

Ce chapitre nous a permet de présenter les notions nécessaires à la compréhension de l'environnement des réseaux sans fils. Ensuite, nous nous sommes intéressés plus aux réseaux mobiles ad hoc qui est l'objet de notre recherche. Ces réseaux présentent des avantages énormes, mais malheureusement beaucoup de problèmes restent à résoudre, notamment le problème du routage que nous verrons dans le chapitre suivant.

II.1. Introduction :

Afin de maintenir la communication, les nœuds d'un réseau ad hoc coopèrent pour la découverte et la maintenance des routes. Les informations de routage échangées entre les nœuds peuvent être une cible pour les attaques. En fait, il y a deux sources de risques pour les protocoles de routage : la première provient des attaques extérieures par l'insertion d'informations de routage falsifiées et le rejet des anciennes informations de routage. La deuxième, la plus sévère, provient des nœuds erronés appartenant au réseau qui peuvent réclamer des informations de routage falsifiées pour engendrer des boucles de routage ou détourner les données vers un nœuds particulier.

II .2. Routage dans les réseaux sans fil ad hoc :[6]

Le routage est un mécanisme a travers lequel on fait transiter une information donnée entre deux nœuds dans un réseau, il a pour but d'assurer une méthode qui garantit a n'importe quel moment, une identification de chemins qui soient correctes et efficaces entre un certains émetteurs vers un destinataire bien précis dans le réseau.

Vu les limitations de réseau ad hoc, le chemin établit doit être optimal et de qualité avec un minimum de contrôle ainsi la consommation de bande passante (voir figure II.1).

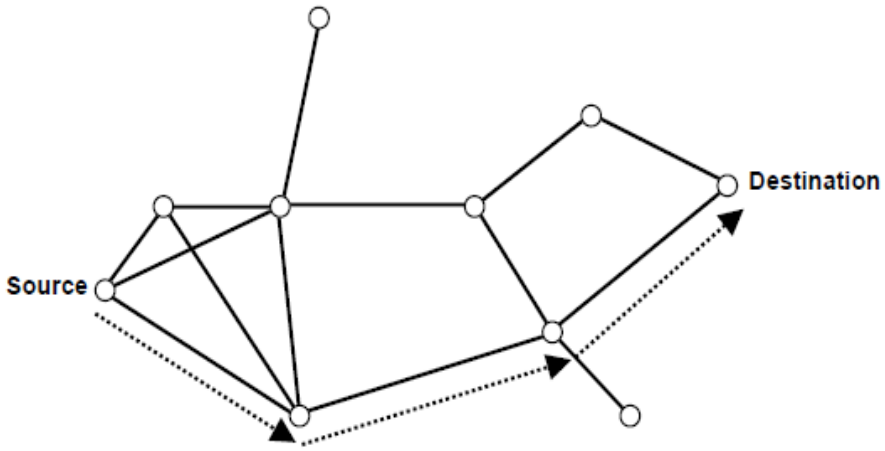


Figure II.1. Exemple de routage dans un réseau ad hoc

II .3. Contraintes de routage dans les réseaux ad hoc :

Le problème qui se pose dans le contexte des réseaux ad hoc est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde et de changements rapides de topologies.

Il semble donc important que toute conception de protocole de routage doive étudier les problèmes suivants :

- **La minimisation de la charge du réseau** : L'optimisation des ressources du réseau engendre deux autres problèmes : l'empêchement des boucles de routage, et empêchement de la concentration du trafic autour de certaines stations ou lien.
- **Offrir un support pour pouvoir effectuer des communications multipoints fiables :** Vu que les chemins employés pour les routages des paquets sont capables d'évoluer, ne doit pas perturber le bon acheminement des données. L'élimination d'un lien, pour raison de panne ou pour cause de mobilité devrait, idéalement accroitre le moins possible le temps de latence.
- **Assurer un routage optimal :** Le routage doit concevoir des chemins optimaux en tenant compte de différents métriques de coûts (bande passante, nombre de liens, délai de bout en bout,…etc.)et il doit assurer maintenance efficace de route avec le moindre coût possible.
- **Le temps de latence :** La qualité des temps de latence et de chemins doit augmenter dans le cas ou la connectivité du réseau augmente.

II.4.Classification des protocoles de routage :[7] [6]

Suivant la manière de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent être séparés en deux catégories, les protocoles proactifs et les protocoles réactifs. Les protocoles proactifs établissent les routes à l'avance en se basant sur l'échange périodique des tables de routage, alors que les protocoles réactifs cherchent les routes à la demande.

D'autres classes existent tel que : les protocoles de routage hybrides qui combinent les deux approches précédentes afin de tirer avantage de deux catégories citées précédemment, tout en réduisant leurs limitation, on cite aussi les protocoles géographiques, hiérarchique, à qualité de service et multicast.

II.4.1 Protocoles de routage proactifs :

Les protocoles de routages proactifs sont des protocoles qui tentent de maintenir à jour dans chaque nœud les informations de routage concernant tout les autres nœuds du réseau.

Quand un paquet doit être transmit, sa route est alors connu à l'avance et peut être immédiatement utilisée.

Du fait de changement topologique dans les réseaux ad hoc, la table de routage construite dans chaque nœud doit être mise à jour par l'envoie périodique d'un message par chaque nœud indiquant sa présence à tout ses voisins.

Deux méthodes fondamentales sont utilisées dans cette catégorie de protocoles proactifs : La méthode Link State et la méthode distance vector. Ces dernières sont aussi utilisée dans les réseaux filaires.

- **Link State** : dans cette méthode, chaque nœud a une vision global sur la topologie du réseau.
- **Distance Vector :** dans ce cas chaque nœud diffuse à ses voisins sa vision qui le sépare de tous les hôtes du réseau. Chaque nœud se charge à la recherche du chemin le plus court vers n'importe quelle destination.

- **Avantages et inconvénients des protocoles proactifs :**

La capacité des protocoles proactifs quelles disposent des routes immédiatement vers la destination, ainsi le gain de temps lors d'une demande de la route. Malheureusement ces protocoles atteignent rapidement leurs limites avec l'accoisement du nombre de nœud dans le réseau, leur mobilité et le cout du maintien les informations de routage et de topologie qui augmente la consommation de la bande passante.

Les principaux protocoles de cette classe sont : OLSR (Optimised State Routing).DSDV (Destination Sequenced Distance-Vector Protocol). FSR (Fisheye State Routing Protocol).

II.4.2 Protocoles de routages réactifs :

Appelés aussi « à la demande » créent et maintient les routes selon les besoins. Si un nœud veut communiquer avec une station distante sur laquelle aucune information n'est disponible au préalable, un processus de la localisation de la destination est lancé, ce

processus consiste à inonder une requête « RReq » (Route Request) dans le réseau et récolter les réponses reçues.

Parmi les protocoles qui appartiennent à cette catégorie on cite : DSR (Dynamic Source Routing), SSR (signal stability Based Rounding), AODV (Ad Hoc On Demand Distance Vector)

- **Avantages et inconvénients des protocoles réactifs :**

Ce type de protocole ne pas inonder le réseau par des paquets de contrôle, ce qui interdit le gaspillage des ressources du réseau et de ne pas conserver les routes non utilisées. Mais il nécessite en contre partie un certains temps pour établir la route avant de transmettre les données.

II.4.3 Protocoles de routage hybrides :

Il s'agit d'une combinaison des deux catégories cité précédemment afin de tirer profit de leurs avantages. Généralement, le réseau est divisé en deux régions. Un nœud utilise un protocole proactif pour le routage dans son voisinage proche (par exemple voisinage à deux ou trois sauts).

Au-delà de cette région prédéfinie, le protocole hybride fait appel aux techniques des protocoles proactifs pour la recherche des routes.

Exemples des protocoles hybrides : DSR (Dynamic Source Routing), ZRP (Zone Routing Protocol).

- **Avantages et inconvénient des protocoles hybrides :**

Le protocole hybride est un protocole qui se veut comme une solution mettant en commun les avantages des deux approches précédentes en utilisant une notion de découpage du réseau.

Cependant, ils cumulent toujours quelques inconvénients des deux approches proactives et réactives.

II.4.4 Protocoles de routage uniforme :

Tous les nœuds du réseau possèdent le même rôle, importance et fonctionnalité. Le routage des paquets dépend de la position du nœud.

Deux catégories sont distinguées : les protocoles orientés topologie, plus connus sous le nom de Link-State protocole et les protocoles orientés destination connu sous le nom de distance protocole. Figure suivante illustre le routage uniforme :

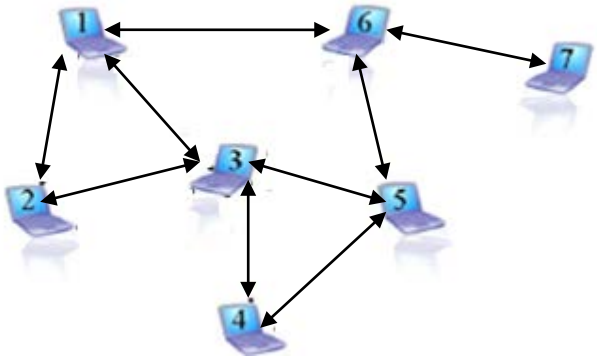


Figure II.2. Le routage uniforme

II.4.5 Protocoles de routage non uniforme :

Un protocole est dit non uniforme si une structure hiérarchique est donnée au réseau et que seuls certains nœuds interviennent directement dans la fonction de routage, on distingue deux cas :

- **Les protocoles à sélection de voisins** : Chaque nœud sous traite la fonction de routage à un sous ensemble de ses voisins directs.
- **Les protocoles à partitionnement** : le réseau est découpé en zones dans lesquelles le routage est assuré par un unique nœud maître.

II.4.6 Protocoles de routage géographique :

Les protocoles de routage géographique se basent sur la localisation de la destination pour assurer le routage des paquets, chaque nœud connait sa propre localisation à tout moment.

Ce type de protocole n'a pas besoin de table de routage, ce qui élimine les paquets de contrôle pour maintenir cette table en permettent le gain de la bande passante et l'économie d'énergie des nœuds.

II.5 Etude de quelques protocoles de routage : [8][15]

II.5.1 Les protocoles de routage proactifs :

II.5.1.1 Le protocole DSDV :

a. Définition :

Le protocole DSDV (Destination Sequenced Distance-Vector Protocol); est l'un des protocoles proactifs mis ou point par le groupe MANET, basé sur l'algorithme distribué de Bellman Ford (DBF : Distributed Bellman Ford), chaque station mobile dispose une table de routage ou chaque ligne doit identifier :

- L'une des destinations possibles.
- Le nombre de sauts pour y parvenir.
- Le nœud de voisin à traverser.
- Numéro de séquence (SN : séquence number) correspondant au nœud destination utilisé pour faire la distinction entre les nouvelle routes et les anciennes et éviter la formation de boucle de routage.

La figure suivante illustre la topologie d'un réseau ad hoc :

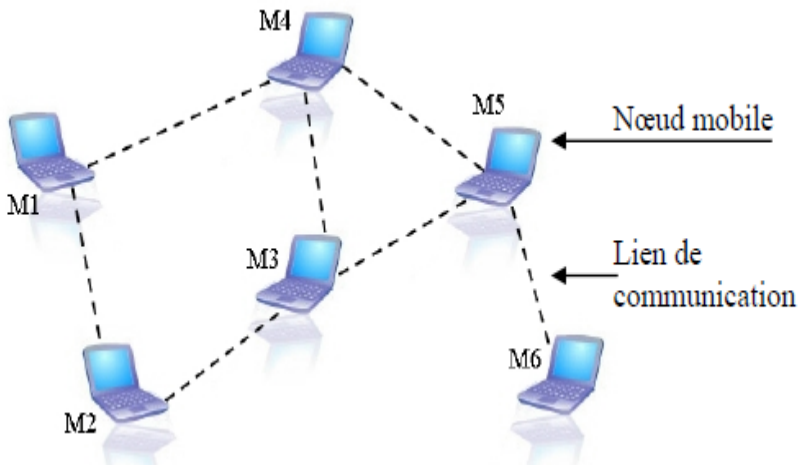


Figure II.3. Exemple de routage

La table de routage correspondante au nœud M1 de la figure ci-dessus est présentée comme suit :

Destination	Nombre de sauts	Prochain nœud	Nombre de séquence
M1	0	M1	NS1
M2	1	M2	NS2
M3	2	M2	NS3
M4	1	M4	NS4
M5	2	M4	NS5
M6	3	M4	NS6

Tableau II.1 : Le routage du nœud M1 de la figure II.3

b. Fonctionnement :

Vu le changement dynamique de la topologie dans les réseaux ad hoc, chaque nœud diffuse un paquet de mise à jour de table de routage contenant la destination accessible, nombre de saut pour atteindre la destination ainsi le numéro de séquence. Le nœud peut aussi transmettre périodiquement sa table de routage si cette dernière a subit des modifications par apport au dernier contenu envoyé.

Lors de la réception d'un paquet de mise à jour, chaque nœud le compare avec les données disponibles dans sa table de routage, la route utilisée est donc celle qui est étiqueté par la plus grande valeur du numéro de séquence (i.e. la route la plus récente).

c. Avantages et inconvénients :

- **Avantage :**
  - Le gain de temps lorsqu'une route est demandée.
  - Selon le chemin, DSDV maintient le meilleur chemin à la place de maintenir plusieurs chemins pour chaque destination, ce qui permet de réduire l'espace dans la table de routage.
- **Inconvénient :**
  - Le gaspillage de la bande passante : dans le cas ou il n'y a pas des changements de topologie du réseau.

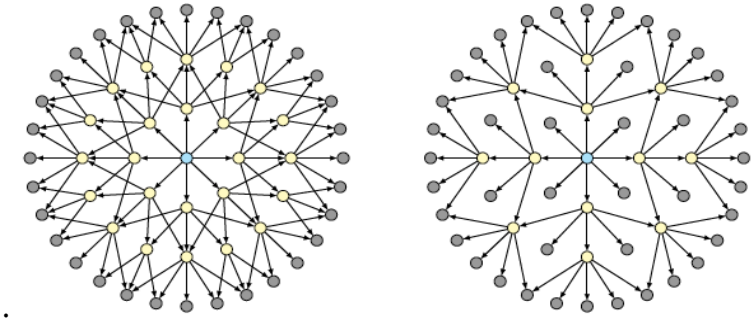
- Protocole très lent : un nœud doit attendre la mise à jour transmise par le destinataire pour modifier l'entrée.

II.5.1.2 Le protocole OLSR :[8] [3]

a. Définition :

Le protocole de routage OLSR, est comme son nom l'indique, un protocole à état de lien optimisé. OLSR offre des routes optimales en termes de nombre de sauts dans le réseau : le routage par état de lien optimisé (Link State Routing) ou chaque nœud découvre des voisins et informe tout le réseau de son voisin par la diffusion.

Son innovation réside en fait, dans sa façon à économiser la consommation de la bande passante et à réduire le nombre des messages de contrôle. Ceci est fait à l'aide de la technique de relais multipoints MPR (Multipoint Relaying), dans lequel chaque nœud ne déclare qu'une sous partie de leurs voisinages, ainsi le nombre de message passant par MPR.



(a) (b)

(a) : Transmission par inondation pure.

(b) : Transmission avec les MPR.

Figure II.4. Optimisation de relais multipoints

Le protocole OLSR utilise 4 types de messages :

- **Hello** : utilisé pour la détection de voisinage.
- **TC** (topology control) : diffuse les informations de topologie.

- **MID** (Multiple Interface Déclaration): permet de publier la liste des interfaces de chaque nœud.
- **HNA** (Host and Network Association) : utilisé pour déclarer les sous réseaux et hôtes joignables par un nœud jouant le rôle de passerelle.

b. Les relais multipoints :

Le concept de relais multipoint vise à réduire significativement l'ensemble de transmission inutiles et d'informations redondantes. Il consiste à choisir par chaque nœud un sous ensemble minimale des voisins symétrique (liens vérifié dans les deux sens) à un saut par l'envoi périodiquement des messages « hello » de tel sorte à pouvoir atteindre touts le voisinage à deux sauts. L'ensemble choisit dit le MPR.

Grace aux messages « hello », un nœud construit sa table des voisins ainsi que la liste des voisins qui l'ont choisi comme MPR dits ''MPR-sélecteurs''. De plus, afin de construire les tables de routage des paquets, chaque nœud broadcaste périodiquement des messages TC (topology control) qui contient la liste de ses MPR-sélecteurs.

La figure ci-après illustre le mécanisme de relais multipoint dans le protocole OLSR.

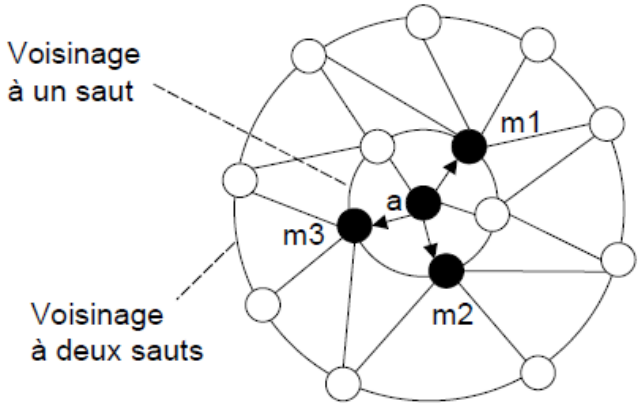


Figure II.5. Le relais multipoint

La station a choisi m1, m2 et m3 comme MPR. Quand (a) émet un message TC, il est seulement retransmis par m1, m2 et m3, qui le retransmettent à leur tour vers leur MPR.

c. L'état de liens :

Il existe quatre types de liens dans le protocole OLSR :

a. **Lien symétrique :** signifie que le lien a été vérifié dans les deux sens, et qu'il est donc possible d'envoyer les données en unicast sur ce lien.
b. **Lien asymétrique :** indique que le nœud reçoit les messages HELLO, venant de l'interface voisine, mais que le lien n'est pas encore valide dans l'autre sens.
c. **Lien MPR :** indique que ce nœud a choisi ce voisin comme relais multipoints, et que le lien est symétrique.
d. **Lien perdu :** signifie que le lien correspondant est perdu et n'est plus valide.

La figure suivante montre les types de liens dans le protocole OLSR :

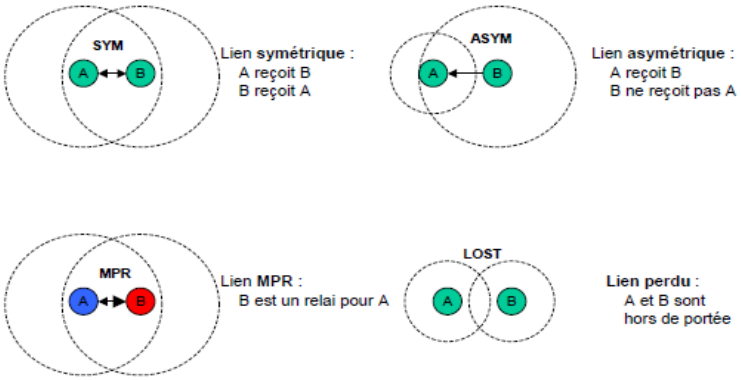


Figure II.6. L'état des liens

d. Fonctionnement du protocole OLSR :[6]

- **Détection de voisinages :**

Chaque nœud doit détecter avec qui, il a un lien symétrique direct. L'incertitude de la propagation radio peut rendre quelques liens asymétriques, par conséquent, tous les liens doivent être testés dans les deux sens afin d'être considérés valides. Pour accomplir cela, chaque nœud diffuse périodiquement des messages HELLO qui contiennent l'information concernant ses voisins et leur type de lien, les messages HELLO sont reçus par tous les voisins à un saut mais ne sont pas relayés aux autres nœuds. Chaque message HELLO contient (figure II.8):

- La liste des adresses des interfaces voisines, possédant un lien symétrique.
- La liste des adresses des interfaces voisines qui sont asymétriques.
- La liste des adresses des interfaces voisines qui sont choisies comme MPR.
- La liste des adresses des interfaces voisines qui viennent d'être perdues.

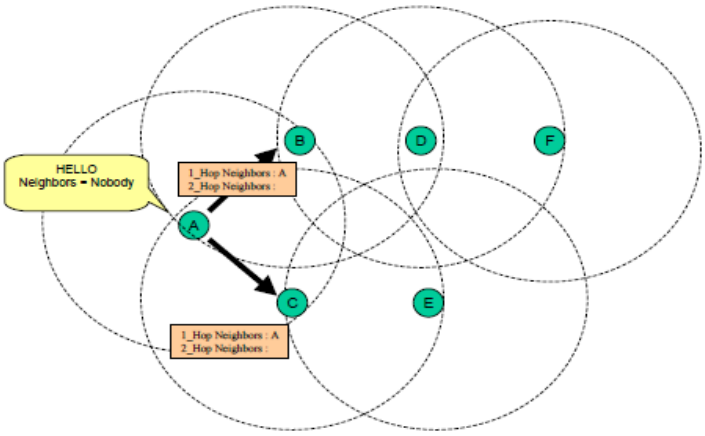


Figure II.8. La détection de voisinages.

Chaque nœud y publie la liste de ses voisins, il est possible pour un nœud d'acquérir des informations sur son voisinage à deux sauts. Par ailleurs, une fois qu'un nœud a effectué la sélection de ses MPRs. Il indique dans ses messages HELLO lesquels de ses voisins sont ses MPRs. Ceci permet à un nœud de savoir quels voisins l'ont choisi comme MPR, autrement son ensemble de MPR-selector.

- **Sélection de relais multipoints :**

Chaque nœud du réseau sélectionne d'une façon indépendante son ensemble de relais multipoints. Dans le but de construire la liste des voisins à deux sauts d'un nœud donné, il suffit de garder une trace de la liste des nœuds ayant des liens symétriques et trouvés dans les messages HELLO transmis par les voisins et reçus par ce nœud. Les relais multipoints d'un nœud sont décalés dans les messages HELLO, ainsi qu'à la réception des messages HELLO, chaque nœud met à jour sa table d'électeur MPR, dont laquelle il met les adresses des voisins qui l'ont choisi comme MPR avec un numéro de séquence.

L'élection des relais multipoints permet donc de réduire le nombre de retransmissions inutiles.

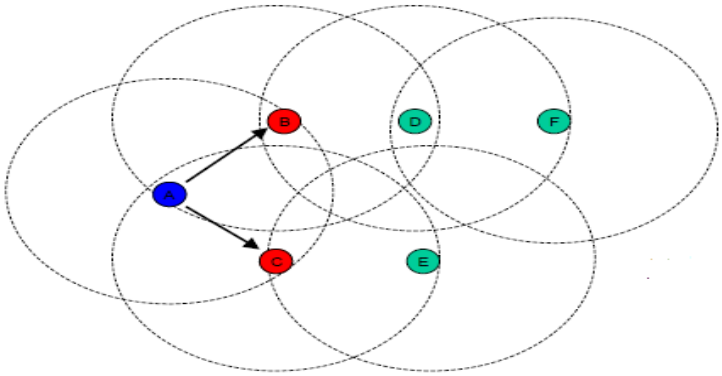


Figure II.9. La sélection des MPRs.

- **Diffusion de la topologie :**

Afin d'établir une base d'information, chaque nœud qui a été choisi comme MPR, diffuse des messages de contrôle spécifiques appelés : message de contrôle de topologie TC. Le message TC est envoyé périodiquement par chaque nœud dans le réseau afin de déclarer son ensemble d'élection MPR, c'est un dire le message TC contient la liste des voisins qui ont sélectionné l'émetteur comme MPR, ainsi ces informations vont aider les nœuds de construire leurs tables topologiques, à la base de cette table, la table de routage sera calculée.

La figure suivante montre la diffusion de la topologie dans le protocole OLSR.

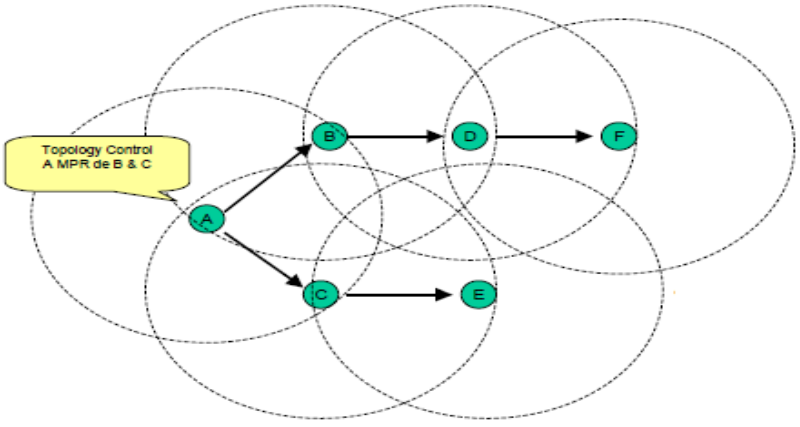


Figure II.10. Diffusion de la topologie

Chaque entrée dans la table topologique contient :

- L'adresse du nœud destinataire.

-L'adresse du nœud MPR qui offre le dernier saut au nœud destinataire.

-Numéro de séquence.

- La durée de vie.

- **Déclaration des interfaces multiples :**

Dans OLSR, un nœud qui contient plusieurs interfaces, émis périodiquement un type de message spécial appelé MID, dans lequel il liste toutes les adresses des interfaces rattachées à ce nœud ainsi que l'adresse principale associe.

Les informations contiennent dans le message MID sont collectées par tous les nœuds du réseau. Pour cela, chaque nœud contient un ensemble de triples de la forme (I_ if_ addr, I_ main_ addr, I_ time) pour chaque destination du nœud dont l'adresse principale est I_ main_ addr.

- **Calcul de la table de routage** : le calcul de la table de routage est basé sur les informations contenues dans la table des voisins et la table de topologie. De ce fait, si une de ces deux tables est modifiée alors la table de routage est recalculée pour mettre à jour les informations sur les routes vers toute destination dans le réseau.
- **Le calcul de route :** chaque nœud maintient une table de routage qui lui permet de router les paquets à toutes les destinations connues dans le réseau. Cette table est calculée en se basant sur la table des voisins et la table topologique. Chaque entrée dans la table de routage consiste en une adresse destinataire (R_ dest _ addr), adresse du saut suivant (R_ next_ addr) et le nombre de sauts (R_ dist) qui sépare la source de la destination. Pour le calcul de la table de routage, la procédure suivante sera exécutée par chaque nœud.

1. Toutes les entrées de la table de routage sont supprimées.
2. Tous les voisins symétriques à un saut seront insérés dans la table de routage avec distance de 1 (h= 1).
3. Pour chaque destination à plus d'un saut (h >1), la procédure suivante est exécutée pour chaque valeur de h, en commençant par h=1 et en incrémentant h par 1 à chaque itération. Cette boucle s'arrête lorsqu'il n'y a plus de nouvelles entrées dans la table de routage.
4. Pour chaque entrée dans la table topologique, si l'adresse de destination ne correspond à aucune adresse de destination dans la table de routage et l'adresse du last_hope_node correspond à une adresse destination dans la table de routage avec une distance h, on insère une nouvelle entrée dans la table de routage telle que :

- R_ dest_ addr égale à dest_ addr.
- R_ next_ addr égale à R_ next_ addr dont le R_ dest_ addr est égale à last_ hope.
- R_ dest = h+1.

Par la suite, la table de routage est complétée par l'ensemble des interfaces en ajoutant des entrées pour toutes les interfaces non présentes dans la table de routage. Finalement, on termine l'insertion des routes vers l'ensemble des associations des réseaux et les hôtes rattachés.

e. **Avantage et inconvénient :**

Le protocole OLSR offre plusieurs fonctionnalités tout en optimisant des routes en termes de protocoles de sauts, il permet ainsi de minimiser le nombre de message de contrôle grâce au concept de MPR et offre la possibilité de communiquer entre le réseau MANET et un réseau filaire (message HNA).

Malgré tout ces atouts le protocole OLSR est plus atteignable par le problème de sécurité qui inquiète plusieurs recherches afin de le protéger contre les différentes attaques.

II.6.2 Les protocoles de routage réactifs :[9]

II.6.2.1 Le protocole AODV :

a. Définition :

L'algorithme de routage AODV (Ad hoc On Demande Distance Vector) est un protocole de routage réactif présent essentiellement une amélioration du protocole proactif DSDV.

Le but avoué du protocole AODV est de fournir un service complètement orienté sur principe de la « route à la demande » : les nœuds ne maintiennent pas d'information de routage et ne s'échangent pas périodiquement leur table de routage.

Vu la densité des réseaux ad hoc, les routes échangent fréquemment ce qui fait que certaines route maintenu par certains nœuds devient invalide. Afin de maintenir l'information de routage la plus récente ou assurer la fraicheur des routes, AODV fait appel au concept «destination sequence number » ou le numéro de séquence.

b. Les types des messages dans AODV :

Le protocole AODV fonctionne en utilisant trois types de messages :

- Les messages de demande de route RREQ (Route Request Message).il est sous la forme ci-dessous :

@source	Num. seq. Source	Broadcast id	@destination	Num. seq. Destination	Nombre de sauts

Figure II.11. Format d'un message RREQ

- Les messages de réponse de routage RREP (Route Relay Message) sous la forme ci-après :

@source	@destination	Num. seq. destination	Nombre de sauts	life time

Figure II.12. Format d'un message RREP

Avec :

Broadcast id : un numéro séquentielle permettant d'identifiant une découverte de route lorsqu'il est pris avec l'adresse source i.e. <@source, Broadcast id>

Nombre de sauts1 : le nombre de sauts séparant la source du nœud traitant le paquet RREQ.

@destination : l'@IP du nœud pour lequel la route est recherchée.

Num. seq. Destination : le dernier numéro de séquence reçu par la source pour cette destination.

@source : l'@ du nœud qui a initié la découverte de route.

Num. seq. Source : le numéro de séquence courant utiliser dans l'entrée de la source.

Nombre de sauts2 : le nombre de sauts séparant la destination du nœud traitant RREQ.

Life time : un temps en milliseconde pour lequel le nœud recevant le RREQ considère la route comme étant active.

- Les messages d'erreur de route RERR (Route Error Message) pour signaler la perte d'une route.

En plus des messages cités précédemment AODV exploite des paquets de contrôle HELLO afin de vérifier la connectivité des routes.

c. Le processus de la découverte de la route par AODV :

Le processus de la découverte de chemin est lancé lorsqu'un nœud désire établir une route vers la destination sur laquelle il ne possède pas encore d'information de sa table de routage. Chaque nœud maintient deux compteurs, « node sequence number » et « Broadcast _ id ».

La source Broadcaste, un message de type route RREQ à travers le réseau, contenant les champs suivants :

Source _ addr	Source _ sequence_ #	Broadcast_ id
Dest_ addr	Dest_ sequence_ #	Hop_ cnt

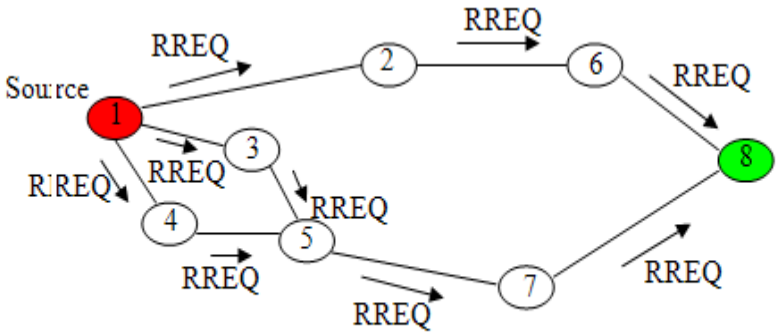
Ou la paire<source_ addr, Broadcast_ id> est une identification du message RREQ, et le champ broadcast_ id est incrémenté à chaque envoie de message RREQ.

Lorsqu'un nœud reçoit le message RREQ, il émet un paquet route reply RREP s'il est la destination ; sinon s'il possède une route vers la destination avec un numéro de séquence supérieur ou égale à celui indiquer dans RREQ, il transmit (unicast) un paquet RREP vers la source.

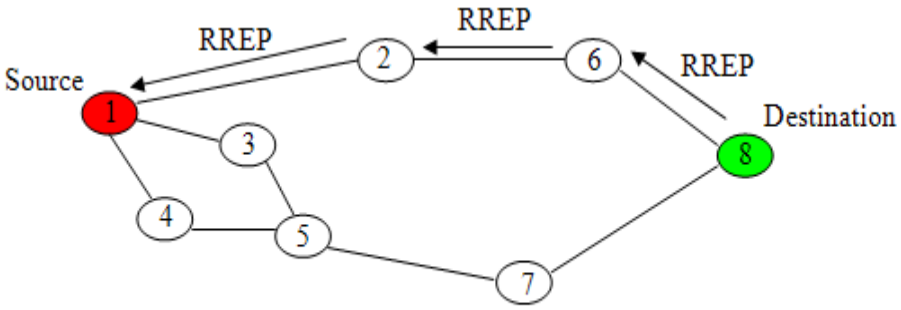
Dans le cas contraire, chaque nœud transmit RREQ à ses propres voisins après avoir incrémenté le compteur de saut « hop_ cnt » et gardant trace de l'adresse IP source, IP destination ainsi le broadcast_ id. si un nœud reçoit un paquet qui a déjà traité, il l'écarte et ne le transmit pas.

Les noeuds établissent des pointeurs de propagation vers la destination alors que les RREP reviennent vers la source. Une fois que la source a reçu RREP, des paquets de données peuvent être émis à la destination.

La figure suivante illustre le processus de la découverte de la route par AODV :



(a) La propagation du paquet RREQ (requête de route).



(b) Le chemin pris par le paquet RREP (requête de réponse).

Figure II.13. Processus de la découverte de la route par AODV

d. **Maintenance de la route :**

Lors de la transmission périodique des données de la source vers la destination, la route est considérée active. Une fois la source s'arrête d'émettre des paquets, le lien expirera et il sera effacé des tables de routage des nœuds intermédiaires. Si un lien se rompt alors qu'une route est active, AODV utilise un message HELLO permettant de vérifier la connectivité des routes. Si pendant un laps de temps, trois messages HELLO ne sont pas reçus, alors le lien vers la destination est considéré cassé. Il envoie donc un message d'erreur RERR à la source pour le notifier de la destination désormais inatteignable. Après la réception de RERR, si la source désire toujours la route, il peut ré initier un processus de la découverte de la route.

e. Avantage et inconvénient :

AODV utilise le concept de numéro de séquence, cet algorithme lui assure une utilisation efficace de la bande passante en minimisant la quantité d'information de contrôle sur le réseau et de se prévenir contre les boucle dans le réseau.

L'inconvénient de protocole AODV réside dans le fait, qu'il ne spécifie pas un format unique pour les messages : RREQ, RREP et RERR.

II.6.2.2 Le protocole DSR :[11]

a. Définition :

DSR (Dynamic Source Routing) est un protocole de routage réactif unicast, permet au réseau d'être auto-structurable et auto-configurable. Il est basé principalement sur la technique « routage source » dans laquelle la source des données détermine la séquence complète des nœuds à travers lesquels les paquets de données doivent être transités pour la destination.

DSR propose deux mécanismes fondamentaux : la découverte de la route « route discovery » et la maintenance de la route « route maintenance ». Le premier est mis en place quand le besoin apparait, tandis que le second permet de détecter lorsqu'une route n'est plus valide et d'en informer la source.

b. Le mécanisme de la découverte de la route :

Lorsque la source S veut initier un flux de données vers une destination sur laquelle aucune route ni disponible dans sa cache de route, il broadcaste un paquet route requête RREQ (S, D, L) ou L est une liste des nœuds traverser pour atteindre D. chaque nœud intermédiaire entre source et la destination qui reçoit RREQ non redondant ajoute son adresse à la liste existante dans RREQ et le diffuse à ses voisins.

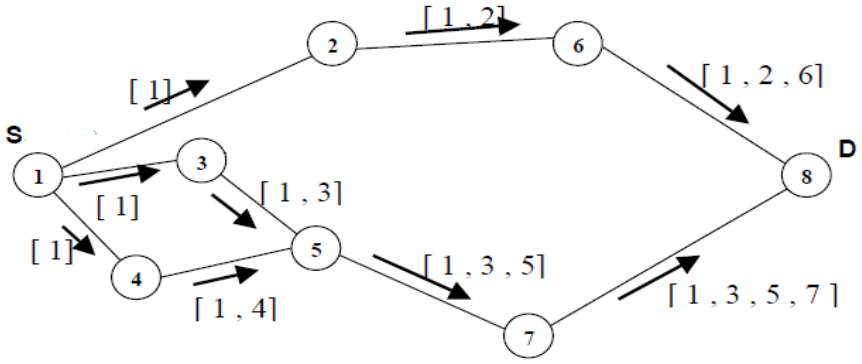


Figure II.14. La transmission de RREQ

Une fois le paquet atteint sa destination, il retourne à la source un paquet Route Reply (RREP). (Figure II.14)

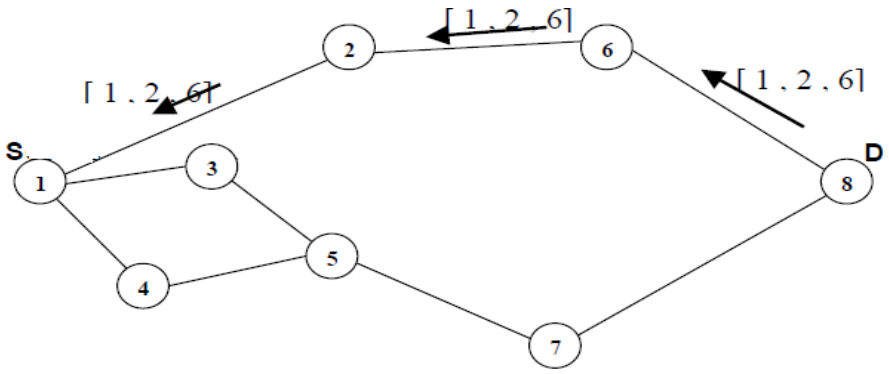


Figure II.15. Renvoi du chemin par DSR

c. Le mécanisme de maintenance de la route :

Dans le protocole DSR, chaque nœud est responsable de la configuration de réception du paquet au nœud suivant, si pas de réponse sur un paquet de données, une erreur est détecté et il sera récupérer par l'envoi d'un paquet route error (RERR) contenant l'adresse du nœud qui a détecté l'erreur et celle du nœuds qui le suit dans le chemin.

A la réception d'un RERR le nœud concerné par l'erreur est supprimé ainsi tout les chemins qu'ils le possèdent.

d. Avantage et inconvénients :

Le protocole de routage DSR offre plusieurs avantages potentiels pour les MANETs. En premier lieu il permet de réduire les frais de la bande passante par l'absence des messages de contrôle, il s'adapte mieux aux changements de la topologie du réseau.

Les faiblesses de ce protocole sont les liens asymétriques :

Route Reply ne peut pas prendre en sens inverse le trajet suivi par Route Request, pour revenir à la source, il lui faut aussi procéder par inondation.

II.7 Conclusion :

Dans ce chapitre nous avons présenté quelques protocoles de routage qui ont été proposé pour assurer le service de routage dans les réseaux mobiles ad hoc. Nous avons décrit leurs principales caractéristiques et fonctionnalités afin de comprendre les stratégies utilisées dans l'acheminement des données entre les différentes unités mobiles.

Cependant, afin que les services ''ad hoc'' soient exploitables, ils doivent se baser sur un réseau sécurisé. Le problème de la sécurité dans les réseaux ad hoc fait l'objet du prochain chapitre.

III.1 Introduction :

La sécurité des réseaux ad hoc présente un défi. En effet ces derniers possèdent des caractéristiques qui les rendent plus vulnérables aux attaques. Dans ce chapitre, nous énumérons ces caractéristiques et les vulnérabilités induites ainsi que les attaques possibles.

III.2 Les risques liés à la sécurité informatique : [12] [4]

III.2.1 Analyse de risque en sécurité :

Les couts d'un problème informatique peuvent être élevés et ceux de la sécurité le sont aussi. Il est nécessaire donc de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions et les couts associés. L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque. On obtient ainsi la liste de ce qui doit être protégé.

Afin de bien appréhender la problématique de la sécurité dans les réseaux mobiles ad hoc, les éléments suivant pouvant servir de base à une étude de risque :

1. Détermination des fonctions et données sensibles des réseaux sans fil ad hoc.
2. Recherche des exigences de sécurité fondées sur les propriétés de la sécurité.
3. Etude des vulnérabilités.
4. Etude des menaces et quantification de leur probabilité d'occurrence ou de leur faisabilité.
5. Mesure du risque encouru en fonction des vulnérabilités mises en lumières et des menaces associées.

La figure (III.1) retrace les différentes phases de ce processus :

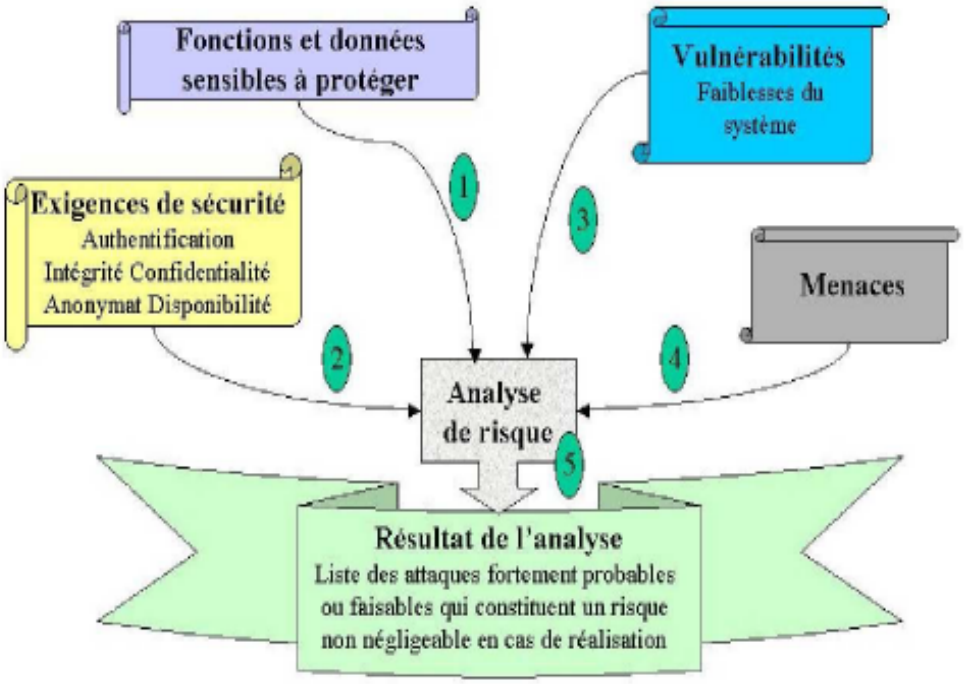


Figure III.1 Les étapes de l'analyse de risque

III.3 Exigence de la sécurité dans les réseaux ad hoc :[12]

Déterminer les exigences de sécurité d'un système nécessite d'appréhender l'ensemble des contraintes qui pèsent sur ce système. Cette étape permet par la suite de quantifier les critères de sécurité.

III.3.1 Contraintes de la sécurité :

Les contraintes de sécurité ad hoc sont multiples. On peut les répartir en six grands thèmes traitant :

- **Caractéristiques des nœuds :** les nœuds eux-mêmes sont des points de vulnérabilité du réseau car un attaquant peut compromettre un élément laissé sans surveillance. De plus, certains éléments peuvent avoir de faibles capacités de calculs.
- **Gestion de l'énergie :** L'énergie doit être conservée au maximum pour cela les nœuds chercheront le plus souvent à se mettre en veille, ce qui provoque donc une minimisation de l'activité de l'ensemble du réseau.

- **L'absence d'infrastructure centralisée :** cette caractéristique du réseau ad hoc qui pénalise la gestion des accès aux ressources du réseau.
- **La technologie sans fil :** Les perturbations dues à l'environnement radio peuvent entrainer des diminutions de débit et bande passante.
- **Mobilité :** Les éléments étant fortement mobiles, leur sécurité physique est moins assurée.
- **Les mécanismes de routage :** sont d'autant plus critiques dans les réseaux ad hoc que chaque entité participe à l'acheminement des paquets à travers le réseau. De plus, les messages de routage transitent sur les ondes radio.

III.3.2 Les besoins de sécurité :[14]

Les réseaux mobiles ad hoc sont exposés à un grand nombre de vulnérabilités, surtout au niveau de routage.

- **Disponibilité :** Est une propriété difficile à gérer dans les réseaux sans fil ad hoc vu les contraintes qui pèsent sur ce type de réseau:
  -Topologie dynamique.
  -Limitation des ressources énergétiques sur quelques nœuds.
  -Communications sans fil pouvant être facilement brouillées ou perturbées.

Plusieurs attaques ont pour but de remettre en cause cette propriété, pour cela le protocole de routage doit surmonter toute tentative d'attaque de type dénis de service(DoS).

- **Authentification :** L'authentification des entités apparait donc comme la pierre angulaire d'un réseau sans fil ad hoc sécurisé. Elle permet d'identifier et contrôler d'identité des participants afin d'interdire aux intrus d'injecter des messages falsifies en erronés
- **Confidentialité des données :** La confidentialité consiste le secret des messages échangés et ne pas les révéler aux adversaires et assurer la protection de l'information contre toute divulgation accidentelle ou malveillante aux parties non autorisées. Sans ce mécanisme, un nœud malveillant peut accéder aux informations secrètes transites dans le réseau, et provoque le disfonctionnement du routage des données.

La confidentialité reste un point crucial, en raison de plusieurs caractéristiques de réseau mobile ad hoc, parmi celles-ci on cite :

- ✓ L'aspect sans fil qui permet à n'importe qui d'écouter les conversations au sein du réseau.
- ✓ L'aspect sans infrastructure préexistante fait qu'un nœud ne peut pas faire des suggestions sur les chemins à emprunter par les différentes données, ce qui permet de ne pas faire confiance aux nœuds intermédiaires.

➢ **Intégrité :** elle permet de garantir que les messages échangés n'ont pas été altérés ou modifier de manière inattendue.

L'intégrité des données peut être remise en cause par plusieurs événements dont on note :

- ✓ Les attaques visant à modifier le contenu des messages.
- ✓ La faible fiabilité des liaisons filaires.

➢ **Non répudiation :** assure qu'une entité ne puisse nier avoir effectué une activité (i.e. un message envoyé ne sera pas nié par son expéditeur).

➢ **Fiabilité :** vise à assurer un réseau robuste permettant de gérer des problèmes d'engorgement. Différents processus sont mis en place afin de renforcer cette propriété telle que des procédures de secours.

III.4 Les attaques contre les réseaux Ad Hoc :[13] [12]

Un réseau sans fil est plus vulnérable aux attaques qu'un réseau filaire, car la transmission radio sont effectuées dans l'air. Sur un réseau filaire, un intrus nécessiterait d'avoir un accès physique à une machine du réseau, ou bien de se connecter aux câbles.

Voici quelques attaques les plus courantes :

III.4.1 Attaque du trou noir (blackhole) : son but est de retransmettre seulement une partie des paquets reçu ou de ne pas les transiter complètement.

Un nœud malicieux a la capacité d'usurper l'identité d'un nœud valide du réseau, il peut lors du mécanisme de découverte de route répondre au nœud initiateur avec un message de type route reply en annonçant un chemin, avec un cout minimal, vers le nœud demandé. Le nœud émetteur mettra alors sa table de routage à jour avec cette fausse route. Les paquets de données de nœud émetteur vers le nœud destinataire transiteront par le nœud malicieux qui pourra tout simplement les ignorer. Les paquets sont captés et absorbés par le nœud malicieux.

Cette attaque a plusieurs variantes ayant des objectifs différents. Parmi celles les plus connues :

Grayholes: ne laisse passer que les paquets de routage, le paquet transmis est choisi pour favoriser une partie du trafic.

Routing loop : permet à une entité de créer des boucles dans le réseau en imposant aux paquets de faire des détours ce qui provoque la consommation inutile de la ressource radio.

Black mail : permet à un nœud malveillant d'isoler un autre nœud.

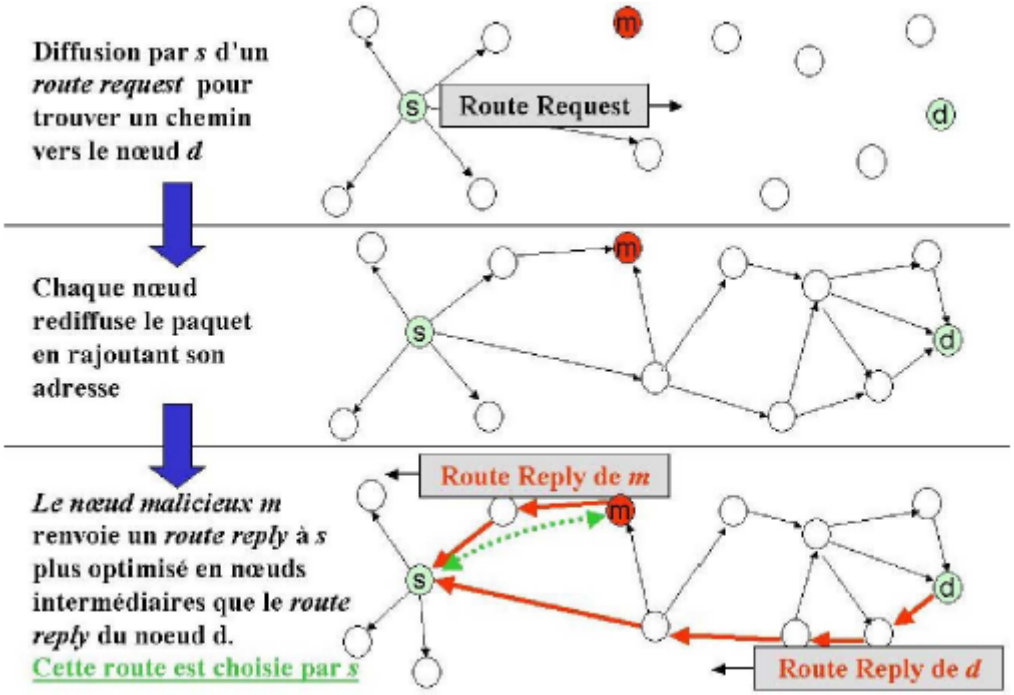


Figure III.2 Attaque blackhole

III.4.2 Attaque du trou de ver (wormhole) :

Appelée aussi le tunneling, cette attaque est réalisée lorsque plusieurs nœuds sont compromis. Elle consiste à construire un tunnel virtuel ou lien appelé lien de trou de ver entre deux nœuds. Ce lien peut être établit en utilisant par exemple, un câble d'Ethernet ou une transmission sans fil à long portée. Le premier nœud retransmet des paquets de données au nœud se trouvant à l'autre bout du tunnel qui se charge de les insérer dans le réseau. Lors de la découverte de route, c'est la première requête qui arrive aux nœuds intermédiaires qui est transmise de route. L'objectif pour l'attaquant est alors de faire passer ses requêtes avant les autres.

La figure ci-dessous illustre le principe de wormhole :

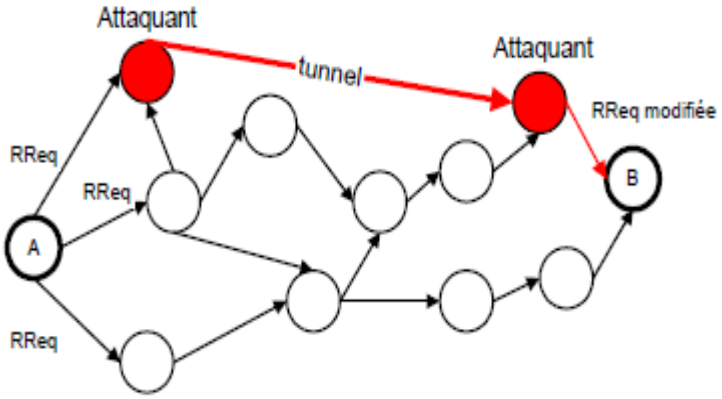


Figure III.3 Attaque par un trou de ver

III.4.3 Attaque par usurpation d'identité [14]: l'attaquant falsifie les informations relatives à l'identité afin d'isoler un nœud auquel il a volé l'identité et donner une fausse vue de la topologie du réseau.

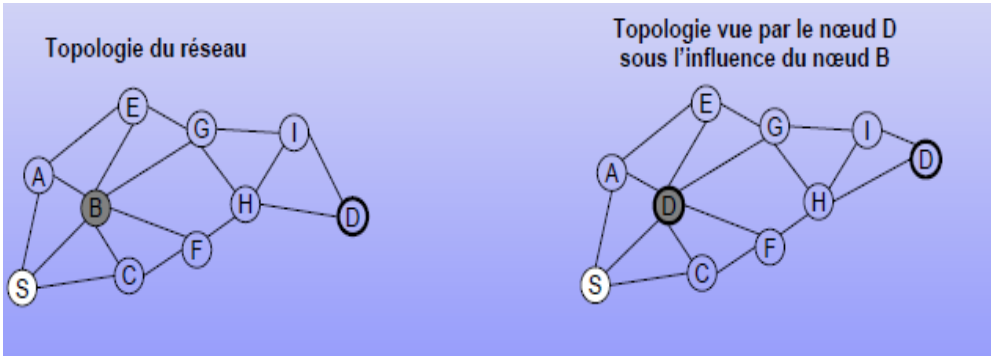


Figure III.4 Attaque par usurpation d'identité

III.4.4 Attaque par harcèlement ou déni de service : la plus facile à réaliser par un attaquant, son principal but est de rendre le service indisponible en attaquant au fournisseur de service lui-même (indisponibilité de serveur).

Voici quelques exemples de déni de service :

- Le brouillage du canal radio dans le but d'empêcher toute communication.
- Tentative de débordement des tables de routage des nœuds servant de relais
- L'absence de coopération d'un nœud au bon fonctionnement du réseau afin de protéger son propre énergie (un nœud égoïste).

- Dispersion et suppression du trafic en jouant sur les mécanismes de routage.
- Les attaques passives d'écoute et d'analyse du trafic constituent une menace certaine pour la confidentialité et l'anonymat.

III.5 Attaques contre les MANET au niveau de routage :

Les attaques contre les protocoles de routage des réseaux Ad Hoc peuvent avoir pou but de modifier le protocole lui-même, pour que le trafic passe par un nœud contrôle par l'adversaire. Une attaque peut aussi avoir pour but d'empêcher la formation du réseau, obliger les nœuds à mémoriser des routes incorrectes, et en général perturber la topologie du réseau.

Les attaques au niveau de routage peuvent être classées dans deux catégories :

- Général incorrecte de trafic.
- Relayage incorrecte de trafic.

II.5.1 Attaques contre le protocole OLSR :

Les protocoles de routage opérant selon deux phases distinctes : une phase de découverte de la topologie du réseau, puis une phase de retransmission des messages de données, ces opérations sont entièrement réalisées sons la responsabilité de sécurités. Au regard du protocole de routage OLSR, il est prévu que chaque nœud génère correctement des messages HELLO et TC, puis maintienne une vue de la topologie de réseau dérivé à partir des messages qu'il reçoit. Or comme les nœuds sont autonomes, des comportements déviants des règles définis par le protocole peuvent apparaitre et causer des déformations sur la vue de la topologie du réseau construite. Les attaques contre les protocoles OLSR peuvent être classées dans deux catégories :

- Génération incorrecte de trafic.
- Relayage incorrecte de trafic.

III.5.1.1 Génération incorrecte de trafic :

OLSR utilise deux différents de trafic de contrôle : les messages HELLO et TC. Dans cette section, nous monterons comment un intrus peut affecter la connectivité du réseau par la génération incorrecte des messages HELLO et TC.

a. **Génération incorrecte de message HELLO :** inclut des attaques sur les messages de contrôle HELLO, deux attaques existent : usurpation d'identité et usurpation de lien.

- **Usurpation d'identité (Identity spoofing)** : l'objectif de l'attaquant est d'identifier un autre nœud cible dans le champ « adresse logique » du message HELLO. Il en résulte que tous les nœuds voisins de l'adversaire ajoutent le nœud identifié dans le message HELLO à la liste de leurs voisins directs.de même tous les nœuds MPR de l'attaquant se comportent comme étant le dernier saut vers le nœud cible ce qui cause des conflits dans les annonces des routes.

Un nœud malveillant X peut envoyer des messages HELLO ayant une fausse origine C. en conséquence, d'autres nœuds pourrait, en se trompant, déclarant être voisins de nœud C, de se fait à travers leur message HELLO et TC. En outre, le nœud X choisit ses MPRs parmi ses voisins avec l'identité de nœud C ; de se fait, ces MPRs vont déclarer qu'ils sont voisins de C. avec perte de connectivité.

La figure suivante montre l'envoie des messages hello :

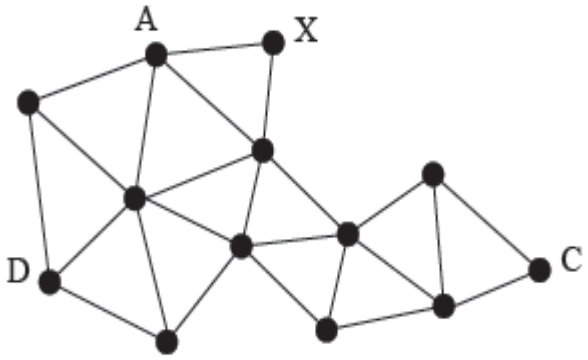


Figure III.5 Usurpation d'identité dans OLSR

- **Links spoofing dans le message HELLO :**

Les dommages au message HELLO inclurent la modification du contenu de message tel qu'insérer des voisins non existants, supprimer des voisins existants et modifier le statut des

voisins. L'insertion des voisins non existants peut affecter le choix des MPRs dans le voisinage de l'intrus et augmente la possibilité qu'un intrus soit choisi comme MPR, un intrus peut manipuler le trafic plus tard. La figure suivante montre link spoofing

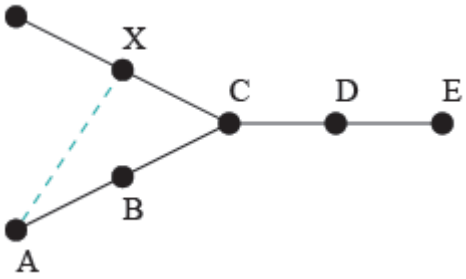


Figure III.6 Usurpation de lien dans OLSR

- Le nœud X déclare un lien symétrique avec A ;
- C choisit comme son MPR X, D au lieu X, D, B.
- Les messages de E ne vont pas joindre A.

b. Génération incorrecte des messages de contrôle TC :

Parmi les caractéristiques de protocole OLSR, seuls les nœuds MPR génèrent les messages de contrôle TC. Or un attaquant peut envoyer des messages TC sans d'être sélectionné comme MPR de fait qu'aucun mécanisme est mis en place afin de vérifier si l'origine d'un message TC est un nœud MPR. Cette attaque permet de définir des routes passantes par l'adversaire.

- **Usurpation d'identité (Identity spoofing) :** une usurpation de l'adresse source (originator Address) dans les messages TC a pour conséquence l'annonce incorrecte dans le réseau de relations de voisinage.
- **Usurpation de lien (Link spoofing) :** deux types d'altération sont distinguées : l'ajout d'un lien non existants qui permet de réduire la distance entre l'adversaire et le nœud cible à un saut seulement et la suppression de message TC.

III.5.1.2 Le relayage incorrecte de trafic :

- **Non retransmission des messages de données :**

Dans cette attaque, un nœud adversaire supprime une partie ou tous les massages de données qu'il reçoit des autres nœuds du réseau et qui ne lui sont pas destinés.

- **Non retransmission des messages de contrôle :**

Si un nœud adversaire est considéré comme étant un MPR par un de ses voisins et qu'il ne retransmet pas les messages de contrôle TC, alors des pertes de connectivité peuvent apparaitre.

Suite à cette attaque, tout nœud ciblé et voisin de l'adversaire devient non atteignable par les autres nœuds du réseau situés à plus de deux sauts (car les informations d'état de liens ne sont pas disséminées à travers le réseau).

III.6 Etat de l'art des solutions pour la sécurité :[12] [14]

Il est clair que les problématiques de sécurité posées par les réseaux sans fil ad hoc sont réelles et complexe, heureusement ; elles ne restent pas sans réponse. En effet, plusieurs solutions ont été mise en œuvre, permettant de sécuriser simplement et efficacement les réseaux ad hoc ou de se prémunir d'une utilisation néfaste. Parmi celles-ci on cite :

III.6.1 Solution pour l'authentification :

Le problème d'authentification dans les réseaux ad hoc est très compliqué a cause de l'absence d'une infrastructure centralisée, d'où la nécessite de concevoir des schémas ou des protocoles qui s'adaptent a ce changement de topologie dans les MANETs.

Une première ligne de défense pour contrecarrer qui attaques consiste à assurer les services d'authenticité et d'intégrité des informations qui sont échangées à l'aide de primitives cryptographiques. Plusieurs solutions ont été proposé pour l'authentification, l'inconvénient commun entre ces solution est l'utilisation des algorithmes cryptographique asymétrique (a clé public).

- **Cryptographique symétrique (clé secrète) :**

La cryptographie symétrique se base sur l'usage d'une même clé pour chiffrer et déchiffrer des données, ces clés sont appelées des clés symétriques (secrètes) ; très efficace et assez économe en ressources CPU. Cependant la complexité réside dans la mise en place de la même clé entre l'émetteur et le récepteur.

- **Cryptographie asymétrique (clef publique) :**

Chaque entité consiste une paire de clés complémentaires et sont générée simultanément ; une clé public connu par toutes les entités utilise pour la fonction de chiffrement des données et une clé privée connu seulement par une seule entité possédant la paire en question. Notons qu'un message chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante.

Exemple d'algorithmes asymétrique :

L'infrastructure à clé publique auto-organisée PKI (Public Key Infrastructure) : une infrastructure de gestion de clé (IGC) ou PKI prend en charge les aspects tant organisationnels que techniques afin d'assurer les fonctions suivantes : la génération de clés publiques/privées et leur distribution à leurs propriétaires à l'initiation d'une nouvelle entité dans la PKI, ainsi que la publication, révocation et validation de clés publiques. Les PKIs se basent généralement sur des certificats électroniques ont pour objectif de lier de façon sûr une clé publique à une entité (utilisateur, serveur, etc.).

Lorsque deux nœuds veulent transmettre des données, ils s'échangent leur liste de certificats afin d'établir une chaine de confiance entre eux.

III.5.2 Solution pour la sécurisation du routage :

Le mécanisme de cryptographie tel que les cryptographies à clé symétrique, clé public ou chaine de hachage sont les plus employé pour assurer un routage sécurisé. Plusieurs objectives mises en œuvre pour sécuriser le routage :

- la disponibilité : les routes peuvent être trouvées si elles existent.
- L'exactitude : une route en fonction doit au moins exister.
- La sureté : la route en fonction ne contient pas d'attaquant.
- Efficacité de ressource : les mécanismes de la sécurité de routage doivent être légers.

III.6.3 Solution pour l'intégrité et l'authentification des messages :

Les mécanismes permettant d'assurer l'intégrité et l'authentification des messages échangés par les différents nœuds d'un réseau sont l'utilisation de signatures numériques ou de MACs (Message Authentification Code). Les signatures numériques s'appuient sur la cryptographie à clé publique. Un nœud possède une clé publique qui sert à ses correspondants pour chiffrer des messages lui étant destinés et le nœud déchiffre les messages qu'il reçoit avec sa clé privée.

Dans le cas de la signature, le nœud utilise une clé privé (dédiée à la signature) pour signer un message. Le destinataire du message déchiffre la signature avec la clé publique.

III.6.4 Solution pour la confidentialité :

La confidentialité dans les réseaux ad hoc est d'abord traitée par l'utilisation de transmission par saut de fréquence, frequency hoping. Les données sont transmises sur une séquence de fréquence définie pseudo-aléatoirement. L'attaquant doit connaitre cette séquence pour pouvoir se synchroniser en réception. Une fois l'authentification des participants clairement établie, les outils cryptographiques permettent de rendre les communications confidentielles. Toutefois, étant donné qu'une des contraintes des réseaux ad hoc est de devoir être adaptable à des nœuds ayant de faibles capacités de calcul, la cryptographie symétrique sera préférée à la cryptographie à clé publique, cette dernière nécessitant beaucoup plus de puissance de calcul.

III.6.5 Solution pour l'intégrité physique des nœuds :

L'intégrité des nœuds du réseau est intensément lier à des capacités physiques de ce nœud à résister à des attaques qui permettraient à un attaquant de perturber le fonctionnement du nœud afin de la corrompe. De plus l'OS (Operating System) du nœud peut être modifié par un OS corrompu.

L'intégrité physique d'un système informatique est une notion très délicate à mettre en place par les fabricants.

III.6.6 Solution pour disponibilité :

Aucun mécanisme n'est efficace pour contrer le problème de déni de service sur le canal radio causer par un attaquant possédant des différents moyens dans le but de brouiller la totalité de spectre radio. Cependant la technique de saut de fréquence peut être utilisée contre les attaques ayant des faibles capacités.

III.7 Conclusions :

Quelle que soit l'application visée, un réseau ad hoc possède des exigences spécifiques en termes de sécurité, du fait de ses particularités : liens sans fil, contraintes d'énergie, limitation éventuelle de la bande passante.

Cette étude nous a permet d'analyser les différentes types d'attaques qui peuvent subir les réseaux ad hoc ainsi les diverses solutions proposées afin de contrecarrer ces attaques.

IV.1 Introduction :

Pour tester un protocole de routage on a recours souvent à la simulation. En effet, il serait très coûteux voire impossible de mettre en place un réseau à des fins de tests pour certains critères.

Dans ce chapitre nous présentons l'impact de la densité et la mobilité des nœuds sur le nombre des paquets perdus dans un réseau Ad hoc en utilisant les protocoles AODV et DSDV au moyen du simulateur NS2. Nous commençons tout d'abord par présenter l'outil de simulation NS2.

IV.2 Présentation de NS2 : [6] [9]

Le simulateur du réseau NS2 est un outil logiciel de simulation de réseaux informatiques. Il est principalement bâti avec les idées de la conception par objets, de réutilisation du code et de modularité. NS2 est écrit en C++ et utilise le langage OTCL (Object Tools Command Language) dérivé de TCL. A travers OTCL, l'utilisateur décrit les conditions de la simulation: la topologie du réseau, les caractéristiques des liens physiques, les protocoles utilisés, les communications qui ont lieu. La simulation doit d'abord être saisie sous forme de fichier que NS va utiliser pour produire un fichier contenant les résultats. Mais l'utilisation de l'Otcl permet aussi à l'utilisateur de créer ses propres procédures (par exemple s'il souhaite enregistrer dans un fichier l'évolution d'une variable caractéristique du réseau au cours du temps). Il contient des librairies pour la génération des fonctions (topologie, trafic, routage, MAC, LLC,...) et des outils graphiques pour faciliter l'interprétation (Xgraph) et la visualisation (network animator NAM) des résultats.

IV.3 Avantage du simulateur NS2 :

- ✓ Un logiciel de simulation multicouche.
- ✓ Possibilité d'ajouter des composants à la demande.
- ✓ Développement orienté objet.

Du fait de sa popularité, de nombreux protocoles sont à priori disponibles pour NS-2.

Les capacités de NS-2 ouvrent le champ à l'étude de nouveaux mécanismes au niveau des différentes couches de l'architecture réseau. Alors il est devenu l'outil de référence pour les chercheurs du domaine qui peuvent ainsi partager leurs efforts et échanger leurs résultats de simulations.

IV.4 Le processus de simulation :

Le processus de simulation en utilisant NS-2 est composé de trois phases principales :

- ✓ **Phase de préparation :** s'occupe de la génération des fichiers d'entrées. A cette étape, on introduit des fichiers de scripts Otcl qui décrivent l'environnement avec tous ses nœuds, leurs déplacements et leur trafic de données. Ces fichiers sont classés en deux catégories :
  - Fichiers de scénario qui décrivent les nœuds, leurs positions ainsi que leurs mouvements.
  - Fichiers de communication qui décrivent le trafic dans le réseau.
- ✓ **Phase de simulation :** pour lancer les simulations et générer les traces. Les deux fichiers obtenus de la phase de préparation sont introduits dans un script de lancement OTcl. Le script de simulation consiste à indiquer la topologie du réseau, à activer des traces aux endroits pertinents, à engendrer des événements particuliers à des instants donnés. A la fin de cette étape on obtient deux fichiers (journaux) appelé aussi « fichiers traces ». Le premier fichier sera traité par l'outil de visualisation NAM. Et le deuxième doit être filtré par un script awk afin d'afficher le résultat en utilisant l'outil Xgraph.

- ✓ **Phase d'analyse :** pour analyser les traces et générer les courbes. L'outil de visualisation NAM s'occupe du premier fichier trace. Deux éléments intéressants sont proposés à la visualisation : un dessin de la topologie du réseau étudié, et une visualisation dynamique du déroulement du programme dans le temps. Le deuxième fichier de trace sauvegarde tous les échanges de paquets effectués. Afin de dessiner les courbes en utilisant Xgraph, le fichier doit être filtré par un script awk pour ne garder que les informations pertinentes.

IV.5. Paramètres de simulation :

- **La perte des paquets** *:* C'est un élément crucial pour l'évaluation d'un protocole de routage. Afin de déterminer si un protocole est performant, il est utile de savoir s'il minimise au maximum la perte des paquets quelque soit la condition à la qu'elle il est confronté. Pour cela chacun des protocoles (DSDV, AODV) va être testé sous des conditions différentes afin de prédire lequel des deux est meilleurs dans un monde nomade. Ce paramètre va être testé en premier sous l'effet de la mobilité, en second par rapport au nombre de nœuds.

Nos simulations sont faites sur NS 2.35 sous Ubuntu 13.04. L'environnement étudié est un réseau de taille 950m x 950 m, de 4 nœuds et de 8 nœuds. Nous effectuons des simulations d'une durée de 60 secondes, pour avoir suffisamment de temps pour étudier la perte des paquets dans les réseaux ad hoc en utilisant les protocoles AODV et DSDV.

Les modèles utilisés dans la simulation sont standards et respectent les propriétés suivantes :

- **Modèle d'antenne** : il existe 2 types de modèle de simulation : l'antenne directionnelle qui nécessite que l'antenne d'émetteur soit pointée en direction de l'antenne réceptrice, et l'antenne omnidirectionnelle qui diffuse à 360° autour d'elle. Afin qu'un noeud puisse communiquer avec tous ses voisins dans n'importe quelle direction, nous avons choisi le modèle omnidirectionnel.

- **Modèle de propagation** : nous avons choisi le modèle Two-ray ground comme modèle de propagation afin de considérer la réflexion des signaux sur le sol, cela pour avoir des résultats plus justes et plus proches du cas réel.

- **Modèle de trafic** : pour le trafic généré nous avons plusieurs paramètres à définir. Nous avons choisi des sources de trafic à débit constant CBR (constant bit rate) dont le fonctionnement est assez simple : les paquets ont une taille fixe et sont envoyés à un rythme continu. L'intervalle d'envoi entre deux paquets est constant. De plus, la source d'un message n'essaie pas de savoir si son paquet a bien été reçu. Nous avons aussi fixé d'autres paramètres : la taille d'un paquet est égale à 125 octets et la fréquence d'envoi est de 1 paquets/0.015 seconde.

IV.6 Les scénarios de simulation :

Les deux protocoles étudiés sont exposés au même environnement en termes de nombre de nœuds, nombre de connexions de trafic, scénario de mobilité...etc. Après avoir créé les scénarios de mobilité et de trafic, nous avons comparé les performances de ces protocoles face à l'augmentation de nombre des nœuds et la mobilité.

IV.6.1 La perte des paquets a la présence de forte mobilité dans les protocoles AODV et DSDV:

- ✓ **Contexte de simulation :**

Le tableau suivant représente les paramètres de simulation :

Critère	Valeurs
Antenne	OmniAntinna : Omnidirectionnel
Nombre de noeuds	4
Type de la couche MAC	IEEE 802.11
Modèle de propagation radio	Two Ray Ground
Taille de réseau	950 x 950m
Temps de simulation	60 s
Taille de paquets	125 octet
L'intervalle de transmission	15 ms
Le paramètre simulé	La perte des paquets
Le protocole de routage	AODV, DSDV
Trafic	CBR

Tableau IV.1 : Les paramètres de simulation

La figure(IV.1) présente le scénario de simulation avec quatre nœuds dont les trois nœuds (n1 , n2 et n3) transmettent des paquets vers le nœud n0 :

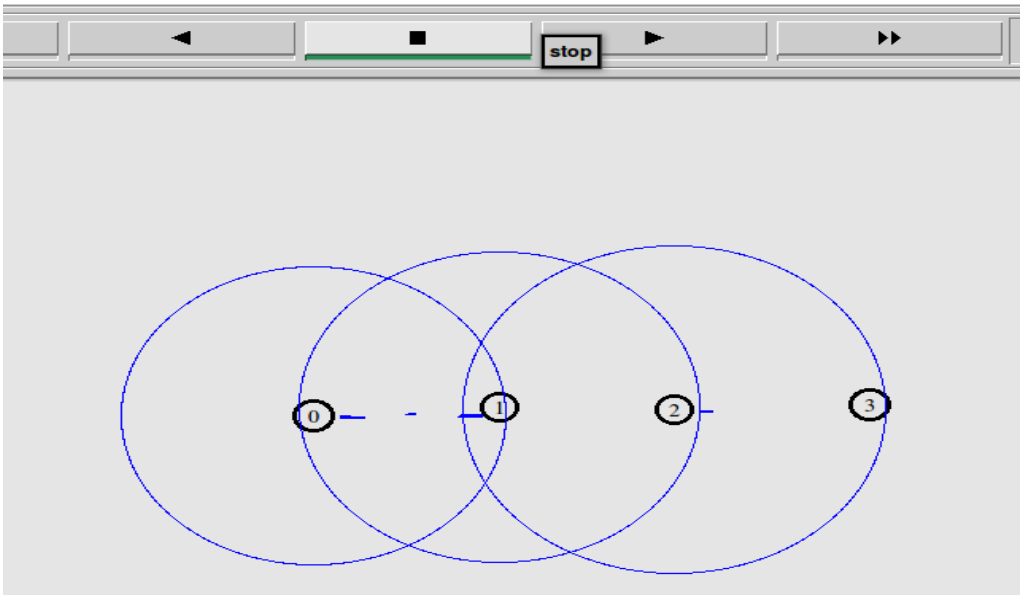


Figure IV .1 : Scénario de simulation avec quatre nœuds

- ✓ **Les résultats obtenus :**

1. **Dans le protocole AODV :**

Les graphes suivants présentent la perte des paquets par quatre nœuds dans le protocole AODV en fonction du temps de simulation dans le cas de présence de la mobilité :

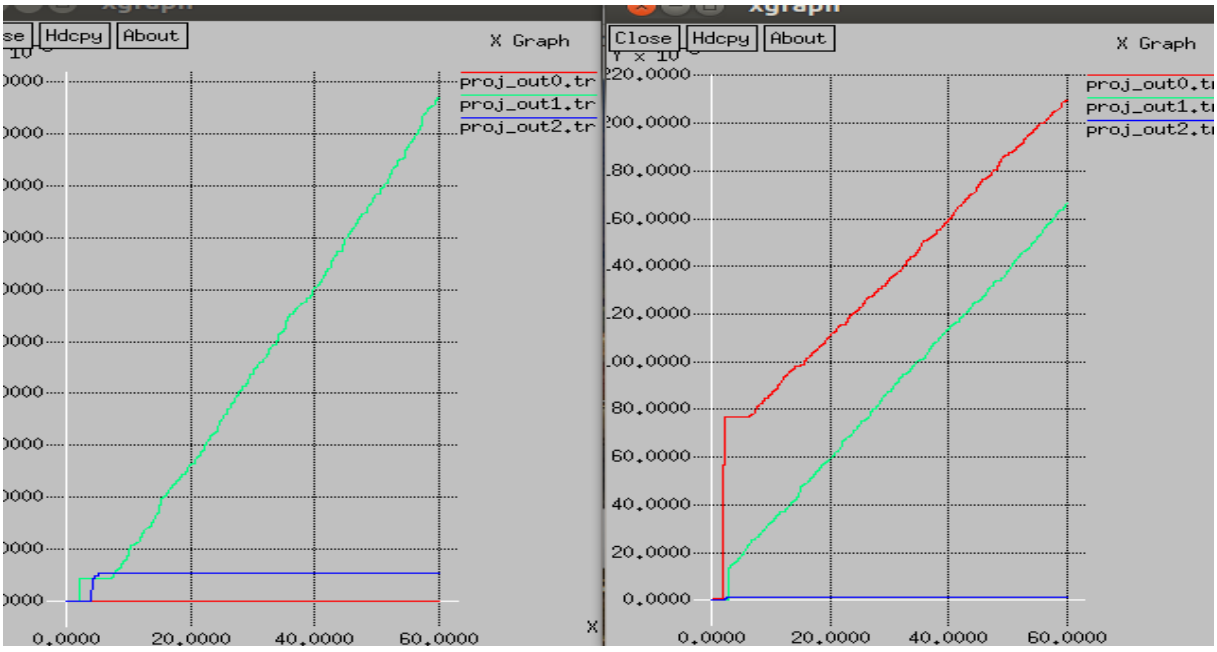


Figure IV .2 : Perte des paquets sans mobilité **Figure IV .3:** Perte des paquets avec mobilité

Avec :

Le nombre des paquets perdus par le nœud (n1).

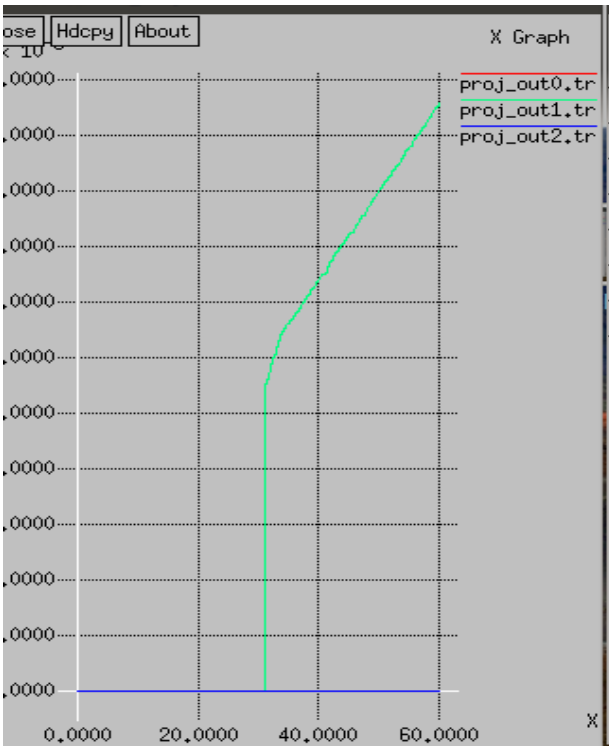
Le nombre des paquets perdus par le nœud (n2).

Le nombre des paquets perdus par le nœud (n3).

D'après ces graphes; nous remarquons que la présence de la mobilité dans le protocole AODV influence sur la perte des paquets.

2. **Dans le protocole DSDV :**

Les figures (IV.4), (IV.5) représentent les graphes obtenus par le protocole DSDV à la présence de la mobilité.



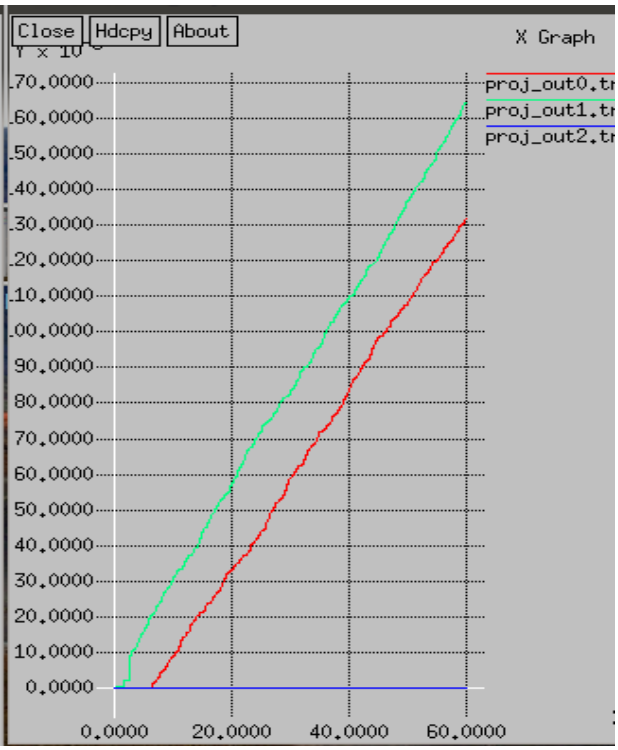


Figure IV.4: Perte des paquets sans mobilité **Figure IV.5:** Perte des paquets avec mobilité

D'après ces résultats ; nous remarquons que la mobilité influence même sur la perte des paquets dans le protocole DSDV

IV.6.2 La perte des paquets dans le cas d'augmentation de nombre des nœuds :

- ✓ **Contexte de simulation :**

On utilise le même contexte précédant juste on utilise 8 nœuds.la figure (IV.6) illustre le scénario de simulation de 8 nœuds :

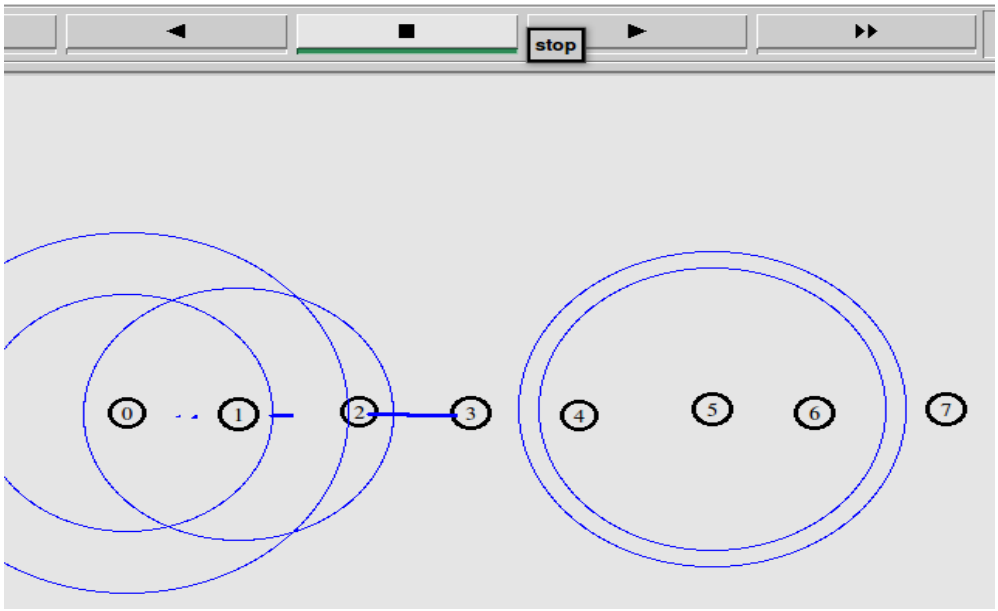


Figure IV.6: Scénario de simulation avec huit nœuds

- ✓ **Les graphes obtenus à l'utilisation des protocoles AODV et DSDV:**

Les graphes des figures suivantes illustrent l'influence de nombre des nœuds sur la perte des paquets en fonction de temps de simulation :

1. Dans le protocole AODV :

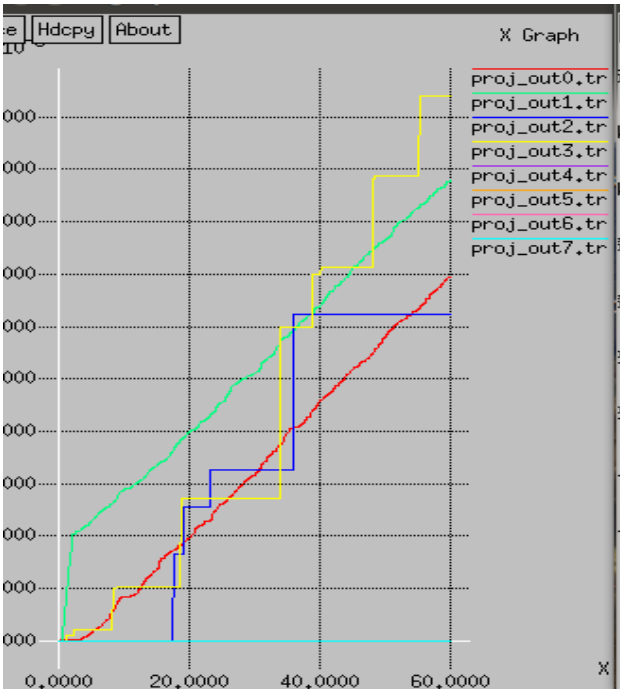


Figure IV.7: perte des paquets dans les 8 nœuds

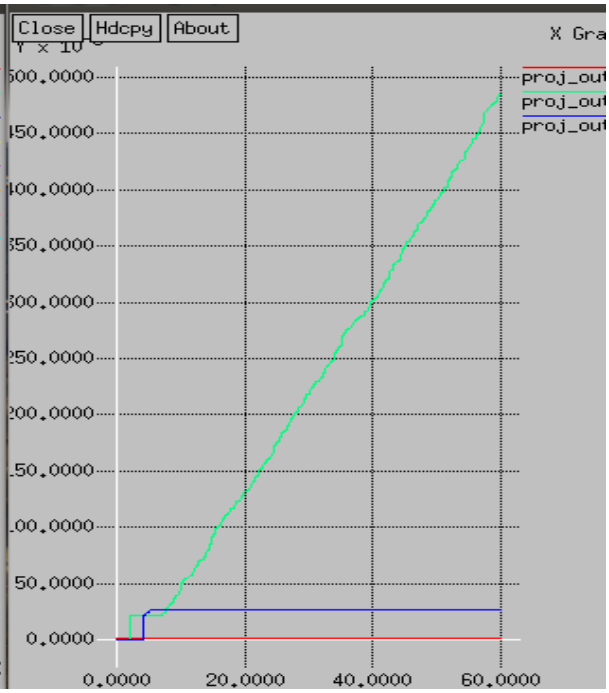


Figure IV.8: perte des paquets dans les 4 nœuds

Avec :

- Le nombre des paquets perdus par le nœud (n1).
- Le nombre des paquets perdus par le nœud (n2).
- Le nombre des paquets perdus par le nœud (n3).
- Le nombre des paquets perdus par le nœud (n4).
- Le nombre des paquets perdus par le nœud (n5).
- Le nombre des paquets perdus par le nœud (n6).
- Le nombre des paquets perdus par le nœud (n7).
- Le nombre des paquets perdus par le nœud (n8).

2. Dans le protocole DSDV :

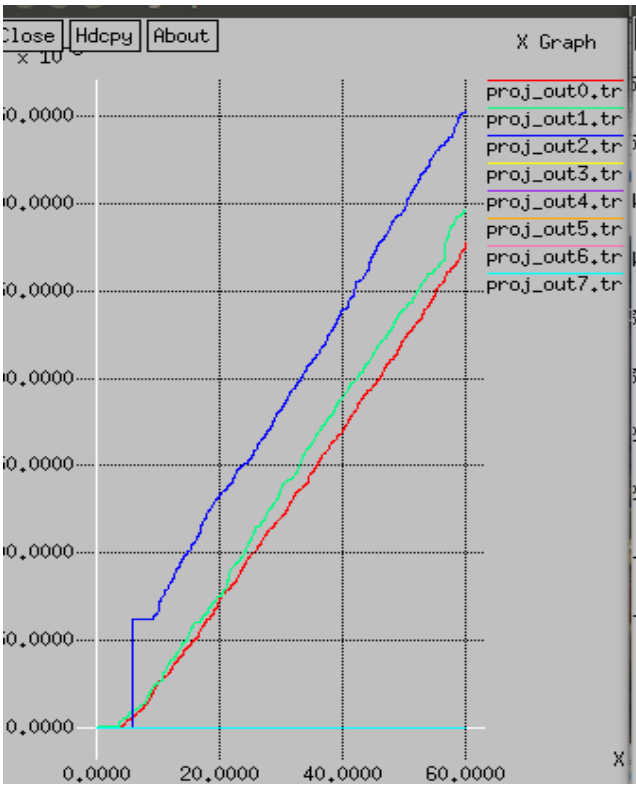


Figure IV.9: la perte dans les 8 nœuds

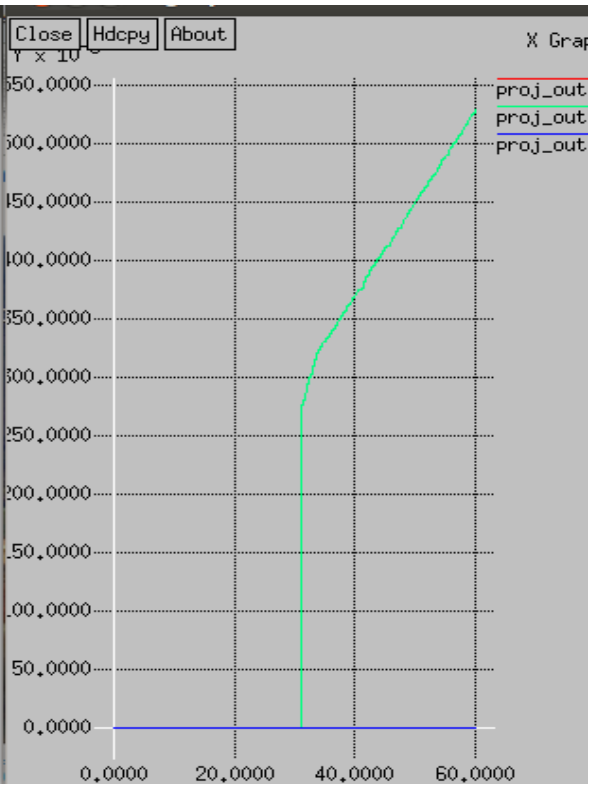


Figure IV.10:la perte dans 4 nœuds

D'après ces graphes on remarque que la perte des paquets augmentes à l'augmentation du nombre des nœuds quelque soit le type de protocole utilisé a cause de l'occupation de bande passante.

IV.6.3 Comparaison entre le protocole AODV et DSDV :

✓ Scénario de simulation :

Le tableau(IV.2) représente les paramètres de simulation utilisés pour comparer entre la perte des paquets dans AODV et DSDV.

paramètres	Valeurs
Antenne	OmniAntinna : Omnidirectionnel
Nombre de nœuds	8
Type de la couche MAC	IEEE 802.11
Modèle de propagation radio	Two Ray Ground
Taille de réseau	950 x 950m
Temps de simulation	60 s
Taille de paquets	4096 bit
L'intervalle de transmission	0.25s
Le paramètre simulé	La perte des paquets
Le protocole de routage	AODV, DSDV
Trafic	CBR

Tableau IV.2 : Les paramètres utilisés pour comparer entre AODV et DSDV

- ✓ **Les résultats dans l'absence de mobilité :**

Dans les graphes des figures (IV.11), (IV.12) on compare le nombre des paquets perdus dans AODV et DSDV dans l'absence de mobilité.

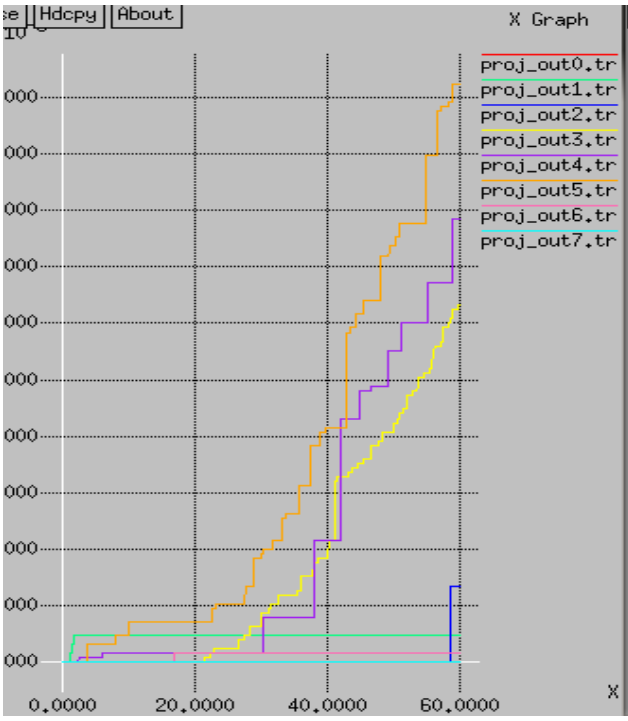


Figure IV.11: la perte dans AODV.

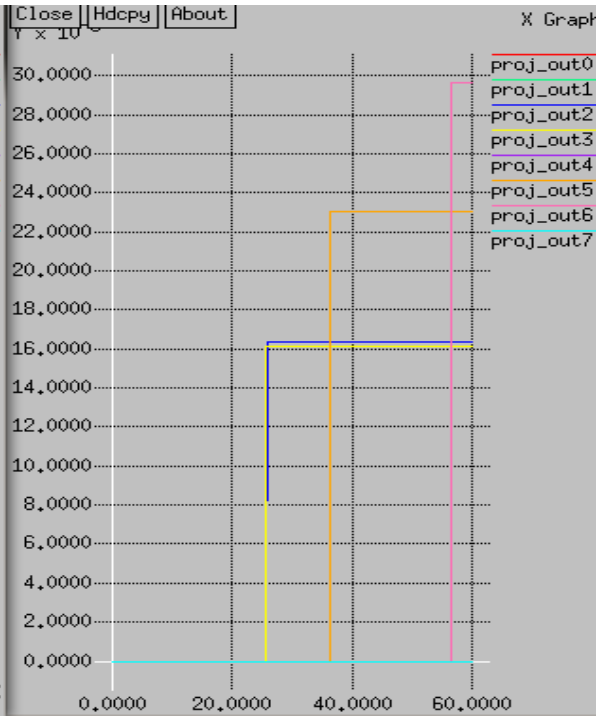


Figure IV.12: la perte dans DSDV

✓ **Les résultats dans la présence de mobilité :**

La figure suivante montre la mobilité des huit nœuds dans le scénario de simulation :

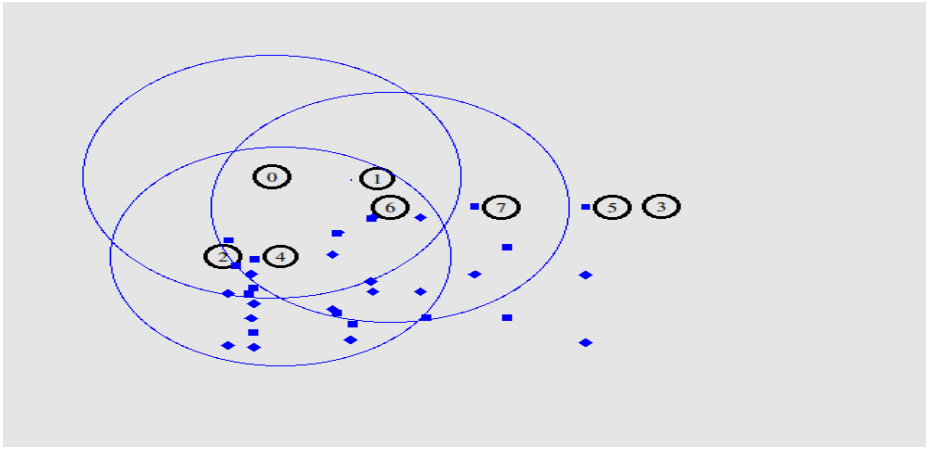


Figure IV.13 : le scénario de huit nœuds à la présence de mobilité

Les graphes suivants représentent la perte entre AODV et DSDV avec une forte mobilité :

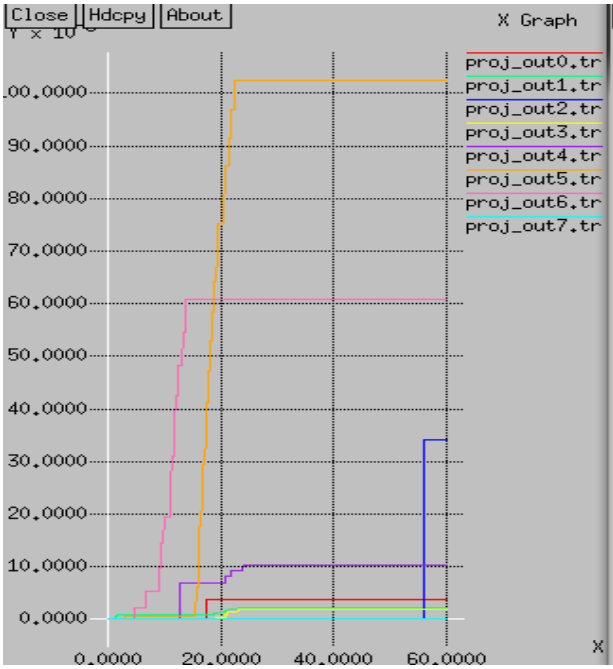


Figure IV.14: la perte dans AODV.

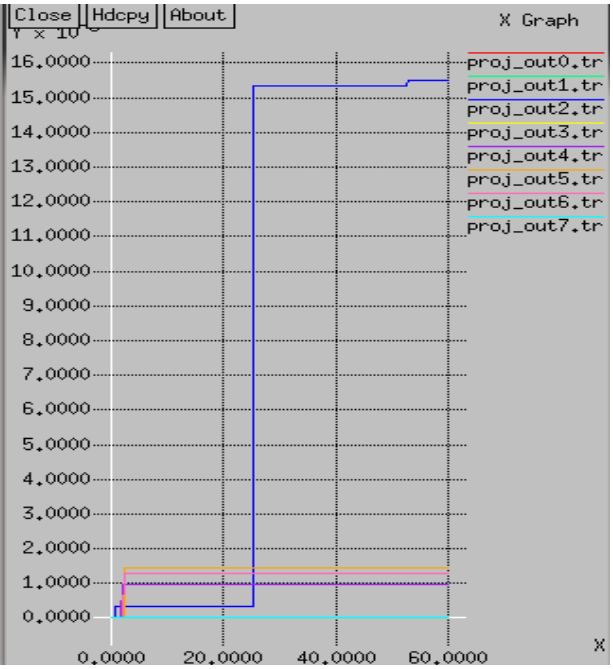


Figure IV.15: la perte dans DSDV

D'après ces résultats nous constatons que la perte des paquets est très importante dans les deux protocoles à la présence ou à l'absence de mobilité, mais si on compare entre eux ; on trouve que la perte est très forte à l'utilisation du protocole AODV à cause de diffusion des paquets de découverte de la route.

IV.7. Interprétation des résultats :

- **Mobilité :** Pour une forte mobilité et en tenant compte des résultats obtenus dans les graphes, on constate que le protocole DSDV minimise la perte des paquets qu'AODV.

- **Nombre des nœuds :** En utilisant UDP comme protocole de transport, on constate que la perte des paquets croit proportionnellement avec le nombre des nœuds quelque soit le protocole utilisé ; mais on remarque que la perte est très importante dans le protocole AODV que DSDV.

Donc d'après les observations, on dit que le protocole DSDV plus performent que AODV en terme de perte de paquets.

- **Perte des paquets :**

  On constate que la perte des paquets croit proportionnellement avec la mobilité et les nombres des nœuds mis en jeu ; ceci peut être interprété par la présence des nœuds intermédiaires qui coopèrent à la transmission des paquets, occupation de la bande passante du récepteur et par la non disponibilité d'une route ou simple perte au niveau de la file d'attente. De ce fait la perte sur le réseau plus dense est énorme par rapport à un réseau moins de nœuds quelque soit le protocole utilisé (AODV, DSDV).

IV.8.Conclusion :

Dans ce chapitre nous avons effectué une simulation sous NS-2 qui nous a permis de voir l'impact de la mobilité, le nombre de nœuds sur la perte des paquets pour les protocoles AODV et DSDV.

La sécurisation du routage dans les réseaux Ad hoc reste un problème majeur. Elle se heurte souvent à la difficulté de proposer des mécanismes relativement robustes face aux différentes attaques possibles, causées par les intrusions externes et les nœuds compromis sans pour autant affecter les performances globales du réseau ad hoc et des protocoles de routage de manière trop prononcée.

Dans ce travail, nous avons étudié les problèmes de sécurité dans les protocoles de routage des réseaux mobiles Ad hoc d'un point de vue théorique. Cette étude a révélé un nombre de difficultés liées à l'absence d'infrastructure centralisée, la contrainte d'énergie, la topologie dynamique, la bande passante, les ressources limitées,… etc. De nombreux travaux de recherche proposent des schémas de sécurité qui conviennent aux caractéristiques des réseaux ad hoc. Bien que des solutions répondent à un ensemble d'exigences de sécurité, il n'en demeure pas moins que les solutions les plus efficaces et les plus complètes sont coûteuses.

Notre travail nous a permis d'acquérir des connaissances sur l'utilisation de simulateur NS2 ; de simuler les deux protocoles de routage AODV et DSDV à l'utilisation des paramètres suivants : mobilité, nombre des nœuds et la perte des paquets. Les résultats obtenus nous permettrons de conclure que le protocole DSDV est plus performant qu'AODV en terme de perte de paquets dans le réseau ad hoc mobile et plus dense.

Nous conclurons que le choix d'un protocole de routage ne dépend pas seulement des paramètres cités précédemment mais aussi de plusieurs contraintes comme l'énergie, QOS,…etc et qu'il est intéressant de considérer et de combiner le maximum d'entre elles pour tirer les meilleurs profits.

Fonctions de hachage cryptographiques :

Pour garantir l'intégrité des messages, une fonction de hachage cryptographique peut être utilisée. C'est une fonction non réversible (*one-way*) produisant un condensé (appelé aussi empreinte

ou haché) ayant les propriétés suivantes :

– Unique et de taille fixe ;

– Il est impossible (techniquement parlant et dans un temps raisonnable) de retrouver le message

d'origine à partir du condensé ; Sachant un message donné et son empreinte en utilisant une fonction de hachage, il est très

difficile de générer un autre message qui donne la même empreinte (*weak collision resistance*); Il est impossible de trouver deux messages produisant le même condensé (*strong collision*

resistance).

Le temps négligeable pour le calcul du condensé constitue un avantage pour l'utilisation des fonctions de hachages cryptographiques. Ces fonctions sont utilisées entre autres pour la signature numérique (le condensé du message est calculé et lui seul est signé) et aussi pour des mécanismes d'authentification par mot de passe sans stockage de ce dernier.

Le format du message HELLO :

La Figure suivante présente le format des messages HELLO. Chaque message se compose en plusieurs sections qui correspondent à différents états de liens. La liste des adresses des interfaces voisins qui possèdent un lien symétrique sont listés dans les champs *Neighbor Interface Address*

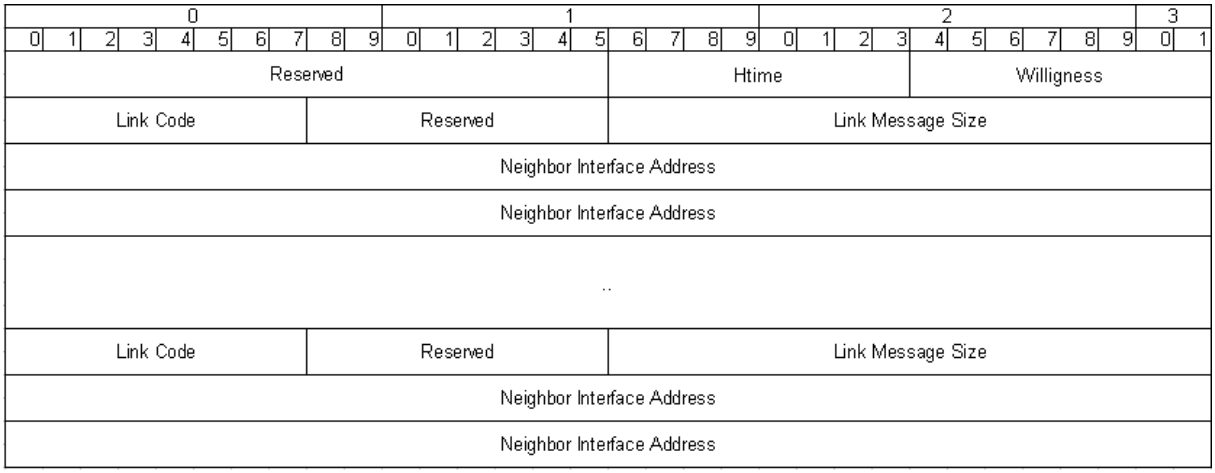


Figure ii : Format du message HELLO.

Le champ *Link Code* de taille 8 bits, contient à la fois les informations concernant les liens vers les nœuds voisins et le type de ces derniers.

Format de message TC :

Chaque message *TC* (*Voir* Figure iii), envoyé par un noeud *x* , contient la liste *MPRSel*(*x*) ainsi qu'un numéro de séquence (*ANSN*) associé au message. Ces messages permettent à chaque noeud de maintenir à jour sa table d'information sur la topologie et ainsi faciliter le calcul de sa table de routage.

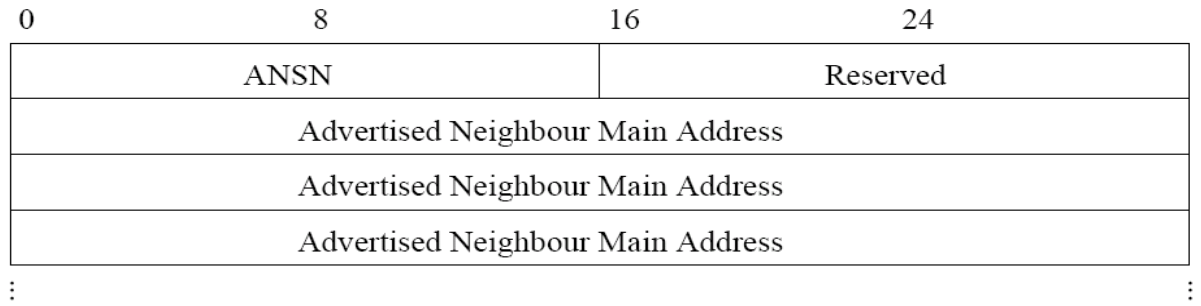


Figure iii : format du message TC

Denial Of Service – DoS :

Le but du DoS est de rendre le service indisponible en s'attaquant aux structures fournissant le service lui-même (indisponibilité du serveur, ...). Sur les réseaux ad hoc, l'absence de structure fait que le service (de routage, par exemple) est généralement réparti entre les entités. Les attaques du type DoS peuvent donc être appliquées sur les nœuds les plus faibles, parmi ceux e_ectuant le service.

Ces attaques sont généralement prises en compte dans les protocoles et peuvent être contrées, par exemple, soit en ayant peu de nœuds associés au service, et dans ce cas ces nœuds peuvent être renforcés, soit un grand nombre de nœuds, mais avec une technique de redondance matérielle. Ce genre d'attaque est étudié dans l'authentification du type Threshold.

L’inondation :

L'inondation ou la diffusion pure (*Broadcast*), consiste à faire propager un paquet (de données ou de contrôle) dans le réseau entier. Un nœud qui initie l'inondation envoie le paquet à tous ses voisins directs. De même, si un nœud quelconque du réseau reçoit le paquet, il le rediffuse à tous ses voisins.

Ce comportement se répète jusqu'à ce que le paquet atteigne tous les nœuds du réseau. Notons que les nœuds peuvent être amenés à appliquer, durant l'inondation, certains traitements de contrôle, dans le but d'éviter certains problèmes, tels que le bouclage et la duplication des messages.

Le mécanisme d'inondation est utilisé généralement dans la première phase du routage, plus exactement dans la procédure de découverte des routes, et cela dans le cas où le nœud source ne connaît pas la localisation exacte de la destination. Un paquet de requête de route est inondé par la source afin qu'il atteigne la station destination. Il faut noter que l'inondation est très coûteuse surtout dans le cas ou le réseau est volumineux (latence, surcharge des messages…etc.), c'est pour cela que les protocoles de routage essaient de minimiser au maximum la propagation des paquets inondés en rajoutant d'autres paramètres de diffusion.

Bibliographie

[1] BOULKAMH Chouaib « Prise en compte de la QoS par les protocoles de routage dans les réseaux Ad hoc », thèse de magistère, université de BATNA, 2008.

[2] HAGGAR BACHAR Salim « Les protocoles de routage dans les réseaux Ad hoc », rapport de stage, université de Reims ,2007.

[3] ABDELLAOUI Rachid «SU-OLSR une nouvelle solution pour la sécurité du protocole OLSR », la métrise en génie concentration réseaux de télécommunication, Université de QUEBEC, Mai 2009.

[4] Cours sur internet « Les réseaux mobiles Ad hoc et les protocoles de routage ».

[5] TOUBAL Adel ET Tiberranine Ferhat «Routage avec qualité de service dans les réseaux ad hoc »thèse d'ingénieur département informatique, Université de MOULOUD MAMMERI de TIZI OUZOU.

[6] AYAD Khadidja «Sécurité du routage dans les réseaux mobile Ad hoc », thèse de magistère, Ecole doctorale STIC à oued Smar ALGER, 2011 ,2012 .

[7] BEYDOUN Kamel «Conception d'un protocole de routage hiérarchique pour les réseaux de capteurs » thèse de doctorat, Université de franche compte, 2009

[8] DERRICHE Ouiza «Simulation des attaques dans les réseaux Ad hoc », thèse de Master en informatique, département informatique, université de Mouloud MAMMERI de Tizi Ouzou, 2010.2011.

[9] Mariam DAOUD «Analyse du protocole AODV », thèse DEA en informatique, faculté des sciences université Libanaise, 2005 ,2006.

[10] Jerome LEBEGUE, Bernard JOUGA et CHRISTOPHE BIDAN « Etat de l'art sur la sécurité des réseaux Ad hoc », thèse financée par une bourse DGA/CNRS ,2005 .

[11] LEMLOUMA Tayeb «Le routage dans les réseaux mobile Ad hoc », thèse d'octorat.

[12] Loutfi NUAYMI Valérie Gayrand «La sécurité dans les réseaux Ad hoc », université ENST Bretagne.

[13] Livre « La sécurité dans les réseaux sans fil et mobiles » sous la direction de Hakima CHAOUCHI et Maryline Laurent-Maknavicius, Lavoisier ,2007.

[14]Omar Cheikhrouhou « La sécurité des réseaux Ad hoc », mémoire d'ingénieur d'état en informatique, Ecole Sfax tunisien, 2005.

[15] Livre « Réseaux mobiles Ad hoc et réseaux de capteurs sans fil »sous la direction Houda Labiod, Lavoisier 2006.