République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mouloud Mammeri De Tizi-Ouzou
Faculté de Génie Electronique et Informatique
Département d'Informatique

Mémoire

De fin d'etudes

En vue de :

L'obtention du Diplôme Master en informatique

Option : Système Informatique

Thème

Etude et simulation des attaques dans les réseaux ad hoc

Présenté par :

M^elle^ DERRICHE Ouiza

Proposé par :

M^me^ : BOURKACHE .G

Promotion 2010/2011

Résumé

Résumé

Un réseau ad-hoc sans fil est une collection de nœuds mobiles formant un réseau temporaire à topologie variable et fonctionnant sans station de base et sans administration centralisée.

Dans un réseau ad hoc, les nœuds sont connectés via des liens sans fil qui sont Particulièrement vulnérables aux différentes attaques possibles. Cela se justifie par les Contraintes et les limitations physiques, qui font que le contrôle des données transférées doit être minimisé. En plus des menaces qui viennent du fait que les communications sans fil sont transmises par ondes radios et peuvent être écoutées par des personnes non autorisées.

Notre travail s'inscrit dans le cadre de l'étude du problème de la sécurité dans les réseaux mobiles Ad hoc. Afin de mener cette étude, nous avons principalement effectué tout d'abord une étude sur les attaques liés aux protocoles de routage et principalement l'attaque Blackhole.

Nous avons ensuite proposé un nouveau protocole de routage afin de simuler cette attaque. Une fois le protocole conçu et implémenté, nous avons proposé par la suite
Une solution afin de contrecarrer cette attaque.

Mots- clés :

MANET, Protocoles de routage à la demande (AODV,…), Sécurité, Attaques Blackhole, NetWork Simulator NS2.

Abstract

Abstract

An ad-hoc network is a collection of wireless mobile nodes forming a temporary network topology and variable operating without base station and without centralized administration.

In an ad hoc network, nodes are connected via wireless links that are particularly vulnerable to various attacks possible. This is justified by the Constraints and physical limitations that make control of the transferred data must be minimized. In addition to the threats that come from the fact that wireless communications are transmitted by radio waves and can be listened to by unauthorized persons.

Our work is part of the study the problem of security in mobile ad hoc networks. To conduct this study, we first performed primarily a study of attacks associated with routing protocols, mainly the attack Blackhole.

We then proposed a new routing protocol to simulate the attack. Once the protocol designed and implemented, we proposed the following one solution to counter the attack.

Keywords:

MANET routing protocols on demand (AODV ...), Security, Blackhole Attacks, Network Simulator NS2.

Dédicace

Je dédie ce modeste travail à :

Mes parents.

Mes grands parents.

Mon frère Akli.

Toutes mes sœurs et ma tente Yamina.

Mes neveux et mes nièces.

Tous mes amis (es) et a toutes leurs familles.

Tous mes collèges du département informatique.

Et à tous qui me sont chers.

Ouiza

Remerciement

Initialement, ce mémoire n'aurait pas été réalisé sans la bénédiction du ***Bon Dieu*** *qui m'a permis de m'instruire et Qui a récompensé mes prières.*

Je voudrais tout d'abord exprimer mes profonds remerciements à ma famille pour leur soutien inconditionnel, merci pour m'avoir encouragé, supporté et pour avoir accepté tant de sacrifices durant cette période.

Je tiens à témoigner ma sincère gratitude à ma promotrice de mémoire, et ce pour de multiples raisons. Tout d'abord, je lui suis reconnaissante d'avoir dirigé mes travaux de recherche tout en me laissant libre d'explorer des pistes à ma guise. De plus, je la remercie pour ses conseils avisés tout

au long de ce mémoire ainsi que pour avoir été présente et motivante.

J'adresse aussi mes très sincères remerciements à tous les membres de jury pour l'intérêt qu'ils témoignent à mon travail par la lecture de manuscrit et leur présence à la soutenance publique de mon memoire de master.

Je ne peux conclure ces remerciements sans exprimer ma reconnaissance à tous ceux qui m'ont aidé et encouragé durant ce projet.

Liste des figures

Liste des figures

Liste des figures

Liste des tableaux

Liste des abréviations

BLR	Boucle Local Radio
SB	Station de Base
UM	Unité Mobile
BSS	Basic station service
GSM	Global System for Mobile Communication
GPRS	General Packet Radio Service
UMTS	Universal Mobile Telecommunication System
MANET	Mobile Ad hoc Network
AODV	Ad hoc On Demand Distance Vector
OLSR	Optimized Link State Routing
DSDV	Dynamic Destination Sequenced Distance-Vector Routing Protocol
ABR	Associative Based Rounding
SSR	Signal Stability based Rounding
RDMAR	Relative Distance Micro Discovery Ad hoc Routin Protocol
DSR	Dynamic Source Routing
FSR	Fisheeye State Routing Protocol
SN	Sequence number

Liste des abréviations

DBF	Distributed Bellman Ford
DREAM	Distance Routing Effect Algorithm For Mobility
MPR	Multipoint Relaying
MID	Multiple Interface Declaration
HNA	Host and Network Association
TC	Topology Control
ANSN	Advertised Neighbor Sequence Number
MID	Multiple Interface Declaration
RREQ	Route Request Message
RREP	Route Reply Message
TORA	Temporary Ordering Routing Algorithm
DAG	Directed Acyclic Graph
ZRP	Zone Routing Protocol
IARP	Intra-Zone Routing Protocol
IERP	Inter-Zone Routing Protocol
BRP	Broadcast Resolution Protocol
NS	Network Simulator

SOMMAIRE

Introduction generale

Introduction générale

L'essor des technologies sans fil, offre aujourd'hui de nouvelles perspectives dans le domaine des télécommunications. L'évolution récente des moyens de la communication sans fil a permet la manipulation de l'information à travers des unités de calculs portables qui ont des caractéristiques particulières (une faible capacité de stockage, une source d'énergie autonome..) et accèdent au réseau à travers une interface de communication sans fil. Comparant avec l'ancien environnement (l'environnement statique), le nouvel environnement résultant appelé l'environnement mobile, permet aux unités de calcul, une libre mobilité et il ne pose aucune restriction sur la localisation des usagers. La mobilité (ou le nomadisme) et le nouveau mode de communication utilisé, engendrent de nouvelles caractéristiques propres à l'environnement mobile : une fréquente déconnexion, un débit de communication et des ressources modestes, et des sources d'énergie limitées.

Le domaine des réseaux mobile ad hoc, suscite de plus en plus d'intérêt ces dernières années. La particularité de ce type du réseau est qu'il n'a besoin d'aucune installation fixe à l'inverse d'autres types de réseaux sans fil. Ils sont faciles et rapides à déployer et ils peuvent opérer de façon autonome ou être connectés à d'autres types de réseaux.

D'autre part, les réseaux mobiles ad hoc sont plus touchés par le paramètre de sécurité, que les réseaux filaires classiques. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé

Toutefois, malgré ces handicaps spécifiques, les réseaux *ad hoc* présentent des avantages indéniables, comme par exemple leur déploiement immédiat et leur faible coût d'utilisation du point de vue financier. Pour exploiter efficacement les possibilités des réseaux ***ad hoc***, il reste à proposer des solutions permettant de surmonter leurs handicaps.

Introduction générale

Le présent travail rentre dans le cadre de l'étude et la simulation des attaques dans les réseaux mobile ad hoc et plus précisément l'attaque trou de noir ***(Blackhole***) en utilisant le simulateur NS2 dans le but d'améliorer la sécurité de ces réseaux.

Pour la réalisation de ce travail de recherche, nous avons suivi le plan suivant :

- Le premier chapitre est consacré à définir un certain nombre de notions fondamentales qui permettront de mieux appréhender les différentes parties du mémoire.
- Puis le deuxième chapitre, est dédié à l'étude des différents protocoles de routage.
- Le troisième chapitre fera office d'une étude détaillé du problème de sécurité dans les Manet.
- Le quatrième chapitre sera consacré à la description de l'environnement de l'implémentation et de simulation de notre attaque.
- Le dernier chapitre porte sur la simulation de notre attaque en proposant un nouveau protocole de routage.

Enfin une conclusion générale présente nos perspectives et conclut ce travail.

Première Partie : Etat de l'art

Routage et Sécurité dans les réseaux ad hoc.

Deuxième Partie :
le simulateur NS et notre Contribution

Proposition d'un nouveau protocole de routage pour simuler L'attaque Blackhole dans un réseau ad hoc

Chapitre I : introduction aux réseaux ad hoc

Introduction :

La dernière décennie a connu une véritable révolution en matière de nouvelles technologie ; notamment dans le secteur de la communication. L'évolution des moyens de communication sans fils a permet la réalisation de l'objectif des réseaux « ***l'accès à l'information n' importe où et n'importe quand*** », en utilisant des unités de calcules portables possédant quelques caractéristiques .L'environnement résultant nommé l'environnement mobile, qui offre une libre mobilité (nomadisme) et qui permet l'accès a l'information dés que le besoin se fait sentir.

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 a l'aide de leurs interfaces sans fils.

Les réseaux Ad hoc sont idéaux pour les applications caractérisées par une absence d'une infrastructure préexistante, telles que les applications militaires et les autres applications de tactique comme les opérations de secours (incendies, tremblement de terre, etc.) et les missions d'exploration.

Ce présent chapitre à pour le but de donner un bref aperçu sur les réseaux sans fils , puis présenter l'environnement mobile et quelque concepts de base de cet environnement, Par la suite, nous nous focaliserons sur l'étude des caractéristiques des réseaux mobiles ad hoc , leurs avantages, leurs handicaps et leurs domaines d'applications.

I.1.Concept de base :

I.1.1.Réseau sans fils :

I.1.1.1.Définition d'un réseau sans fil :

Les réseaux sans fil jouent un rôle crucial au sein des réseaux informatiques.ils constituent un domaine de recherche de l'informatique la plus actif en offrant des solutions ouvertes pour la mobilité.

Qu'est ce qu'un réseau sans fil ?

Un réseau sans fil (Wireless LAN ou WLAN ou IEEE 802.11) est, comme son non l'indique, un réseau dans lequel au moins deux terminaux (nœud) peuvent échanger des informations sans aucune établissement d'une liaison filaire, ils utilisent des mediums radio ou infrarouge pour l'échange de l'information.

C'est un système de transmission des données, assurant une liaison indépendante de l'emplacement des périphériques informatique composant le réseau .ce qui donne a l'utilisateur la possibilité de se déplacer dans une zone géographique plus un moins étendu**.[3][2]**

I.1.1.2.Les catégories de réseaux sans fils :

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

a. **Réseaux personnels sans fils (WPAN)** : il concerne les réseaux sans fils de faible portée, de l'ordre de quelques dizaines de maitres. Plusieurs technologies exploitent les WPAN tel que la technologie bluetooth, la technologie ZigBee, la liaison infrarouge,…etc**. [16]**

b. **Réseaux locaux sans fils(WLAN)** : les WLAN couvrent l'équivalent d'un réseau local d'entreprise, sa portée et d'environ une centaine des mètres. différentes technologies utilisent les WPAN comme : le Wifi(ou IEEE 802.11), hiper LAN2 (High Performance Radio LAN 2.0),…etc.

c. **Réseaux métropolitains sans fils(WMAN) :** les WMAN sont basés sur la norme IEEE 802.16.ils sont connus sous le nom de Boucle Local Radio(BLR) qui offre un débit de 1 à 10M bit /s pour une portée de 4 à 10 Kilomètres.

d. **Réseaux étendus sans fils (WWAN) :** connu sous le nom de réseau cellulaire mobile. C'est un réseau sans fils le plus courant puisque les différents téléphones mobiles sont connectés à un réseau étendu sans fils. les principales technologies sont :

   GSM (*Global System for Mobile Communication)*, GPRS (*General Packet Radio Service*), UMTS (*Universal Mobile Telecommunication System*)…etc. **[16]**

I.2.L'environnement mobile :

Un environnement mobile est un système composé des unités de calcule mobiles permettant une libre mobilité en assurant la connexion avec le réseau indépendamment des facteurs : temps et lieu.

Les réseaux sans fils mobiles substituent aux habituels câbles des connexions aériennes via des ondes radios, infrarouge ou éventuellement des faisceaux laser **[7].** Cette définition, assez large, nous amène à considérer plusieurs types des réseaux sans fils :

I.2.1.Les réseaux sans fils avec infrastructure (cellulaire) :

Dans ce mode, le réseau sans fils est constitue de deux unités différentes : les «sites fixes » appelé station de base (SB), et les « sites mobiles » (UM) nommés aussi cellules.

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 constitue une cellule.la figure suivante présente un réseau sans fil avec infrastructure comportant 4 cellules(UM) :

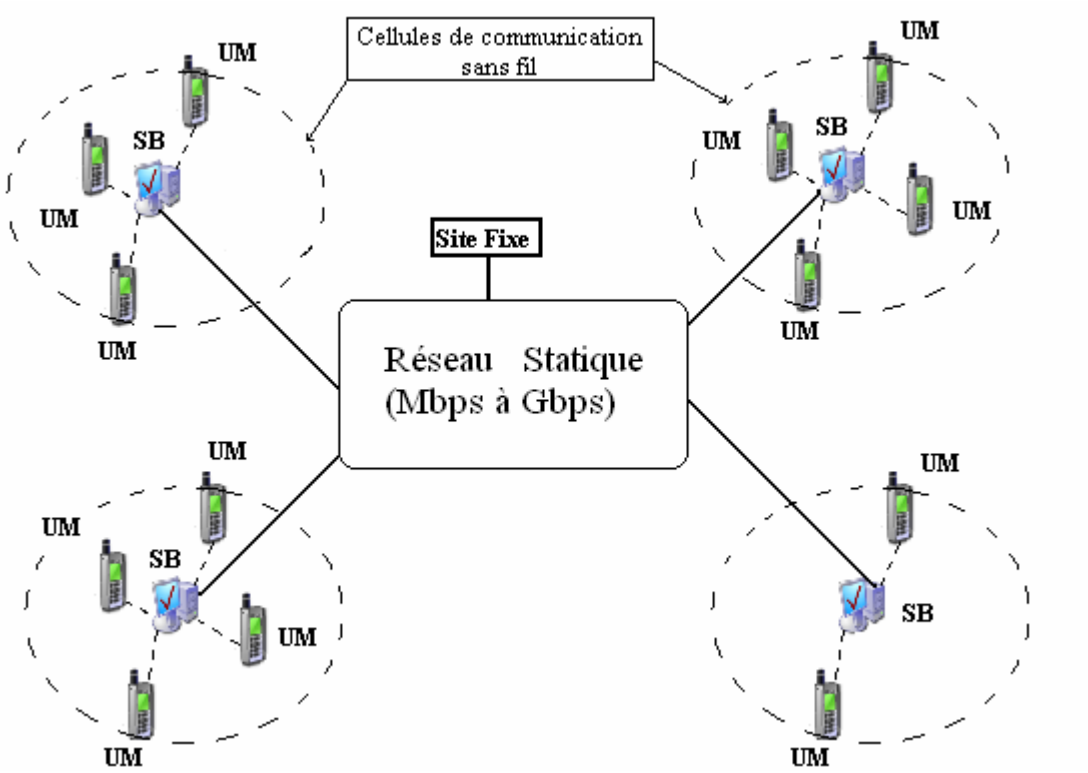


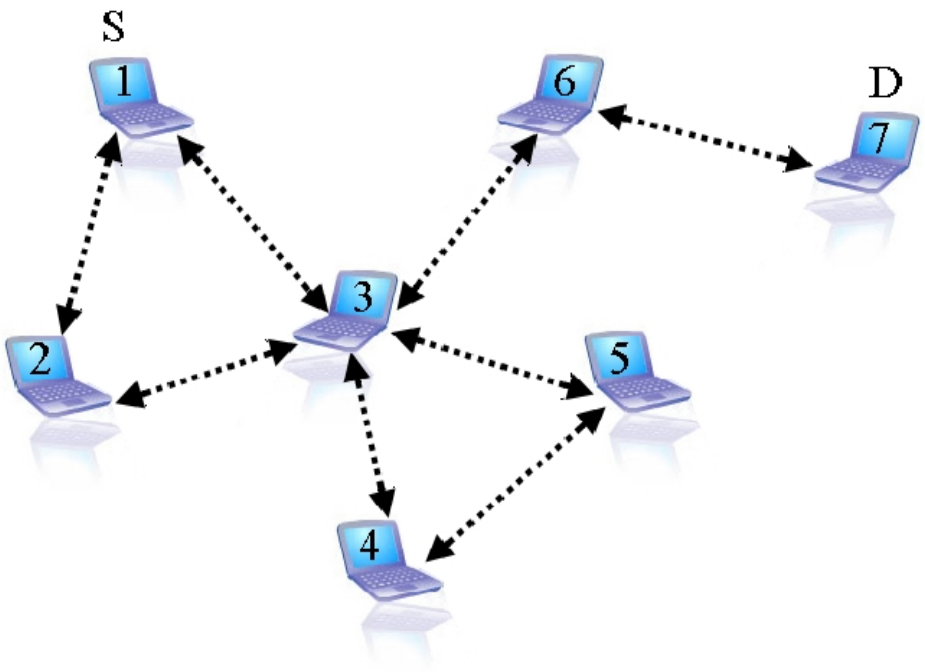
Figure 1.1. Réseau mobile ad hoc avec infrastructure

I.2.2.Les réseaux sans fils sans infrastructure (ad hoc) :

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 (cf. Figure I.2).

Exemple du réseau sans infrastructure est celui des **réseaux ad hoc** (MANET : Mobile Ad hoc Network) dont les unités mobiles utilisent les ondes radio pour communiquer entre eux sans l'aide d'une infrastructure préexistante ou administration centralisée**. [4]**

La figure I.2 présente un modèle sans infrastructure contenant 7 unités mobiles (7 UM) :



Figue 1.2 Réseau ad hoc.

I.3.Les réseaux mobiles ad hoc :

I.3.1.Définition ad hoc :

Un réseau mobile ad hoc appelés généralement MANET (Mobile Ad hoc Network), est un réseau sans fil formé par une collection d'entités mobiles (nœud), ayant la possibilité de communiquer entre eux sans passer par une autre infrastructure. **[1]**

C'est un réseau spontané i.e. que les équipements qui le compose sont capable de s'organiser en réseau sans aucune configuration initial. Cette caractéristique lui donne une

topologie instable qu'elle doit être découverte dynamiquement.de même, le changement de topologie sont fréquent lors de l'existence de réseau. **[6][4]**

La figure suivante montre le changement de topologie dans le réseau ad hoc :

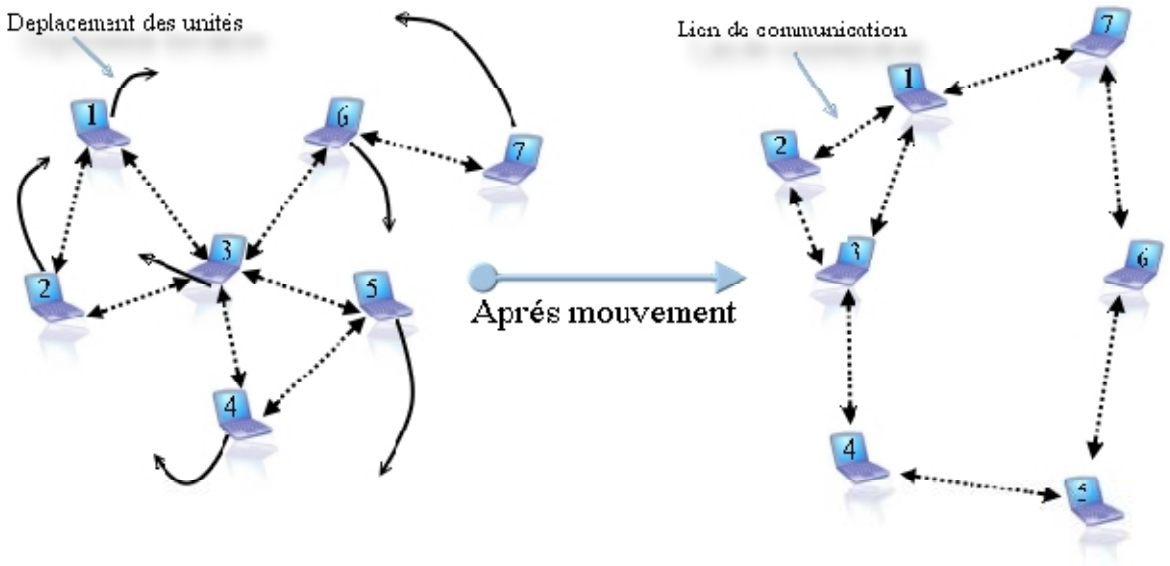


Figure 1.3. Le changement de la topologie des réseaux Ad Hoc

I.3.2.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 utilité dans plusieurs applications et services tel que : les opérations de secours, les bases de données parallèles ,l'enseignement a distance , les systèmes de fichiers repartis, les applications de calcul distribué ou méta-computing ,réseaux en mouvement(informatique embarquée et véhicules communicant), et les applications commerciales(un paiement électronique distant).**[9]**

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

I.3.3 .Caractéristique des Manet :

- **Bande passante limitée :** parmi les caractéristiques des réseaux sans fil est l'utilisation d'un medium de communication partagé, ce partage fait que la bande passante réservé a un hôte soit modeste.
- **Une topologie dynamique :** les entités mobiles du réseau, se déplacent d'une façon libre et arbitraire ce qui provoque le changement de topologie d'une manière rapide et aléatoire à des instants imprévisibles. (cf. Figure1.4)

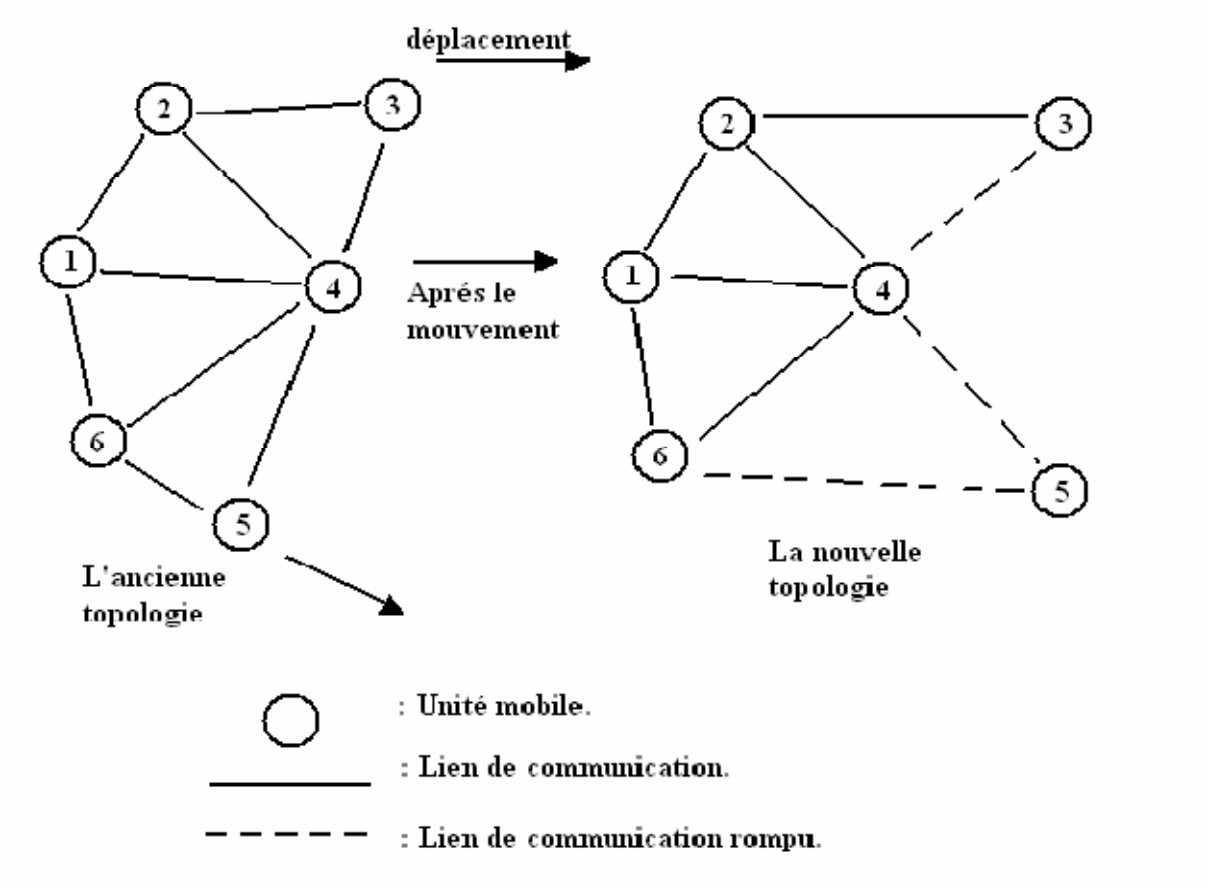


Figure 1.4. Les changements de topologie dans les réseaux mobiles Ad hoc.

- **Contrainte d'énergie :** les hôtes mobiles sont alimentés par des sources d'énergie autonome telle que les batteries ou des autres sources consommables. le paramètre d'énergie doit être pris en compte dans tout le contrôle fait par le système.
- **L'absence d'infrastructure :** dans les réseaux ad hoc, les hôtes se charge d'établir et de maintenir la connectivite du réseau d'une manière continue. L'absence d'infrastructure préexistante et d'une administration centralisée le distingue des autres réseaux mobiles.
- **Une sécurité physique limitée :** les réseaux ad hoc sont plus atteignable par le problème de sécurité, que les autres réseaux filaires classiques.
- **Erreur de transmission :** les erreurs de transmission radio sont plus fréquentes que dans les réseaux filaires.
- **Nœud caché :** ce phénomène est très particulier à l'environnement sans fil.

Deux stations sont dite cachées lorsqu'elles sont trop éloignés pour se détecter mais que leurs zones de transmission 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. (Figure 1.5)

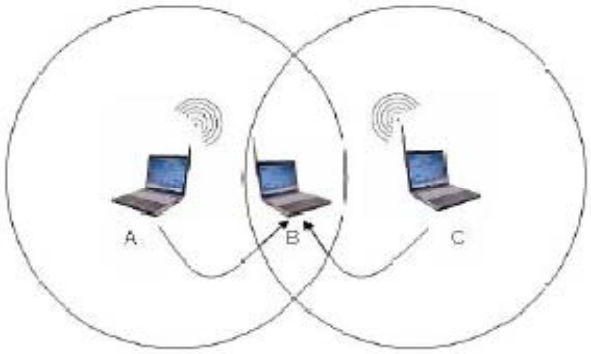


Figure 1.5. Illustration du problème des nœuds cachés.

I.3.4.Architecture ou topologie des réseaux ad hoc :

Les réseaux ad hoc peuvent être soit plate soit hiérarchique :

1. Architecture plate : dans cette architecture (voir figure. 1.6) tous les nœuds participent au routage des paquets étant donné qu'ils sont au même niveau.

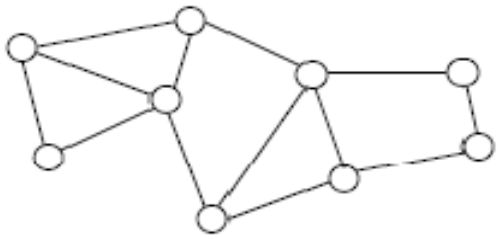


Figure 1.6. Architecture plate.

2 .Architecture hiérarchique : dans ce type (voir figure. 1.7) un groupe des nœuds mobiles sont réunis afin de formé des ensembles nommes « clusters ».dans chaque cluster un seul nœud se charge du routage des paquets. Ce dernier appelé maitre ou clusterhead.

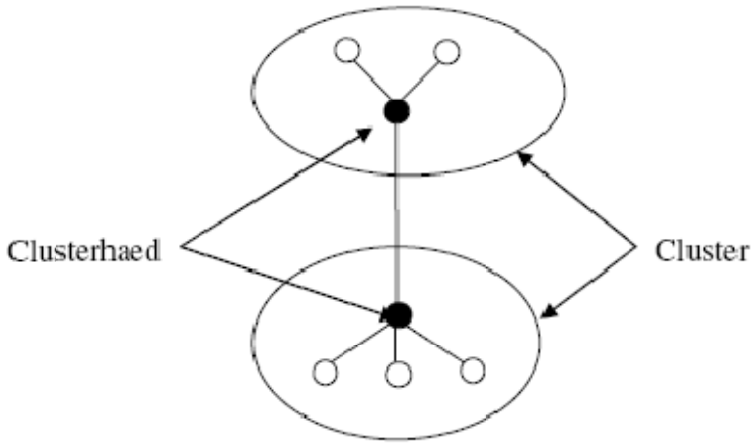


Figure 1.7. Architecture hiérarchique.

I.3.5.Les modes de communication dans les réseaux ad hoc :

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

- **La communication point à point « Unit cast »** : dans ce mode de communication le paquet est adresse à un seul nœud mobile.
- **La communication multi point « Multicast »** : contrairement au Unicast, un paquet est adressé à un ensemble des unités mobiles dans le réseau.
- **La diffusion Broadcast** : un paquet est adressé à toutes les unités composant le réseau.

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

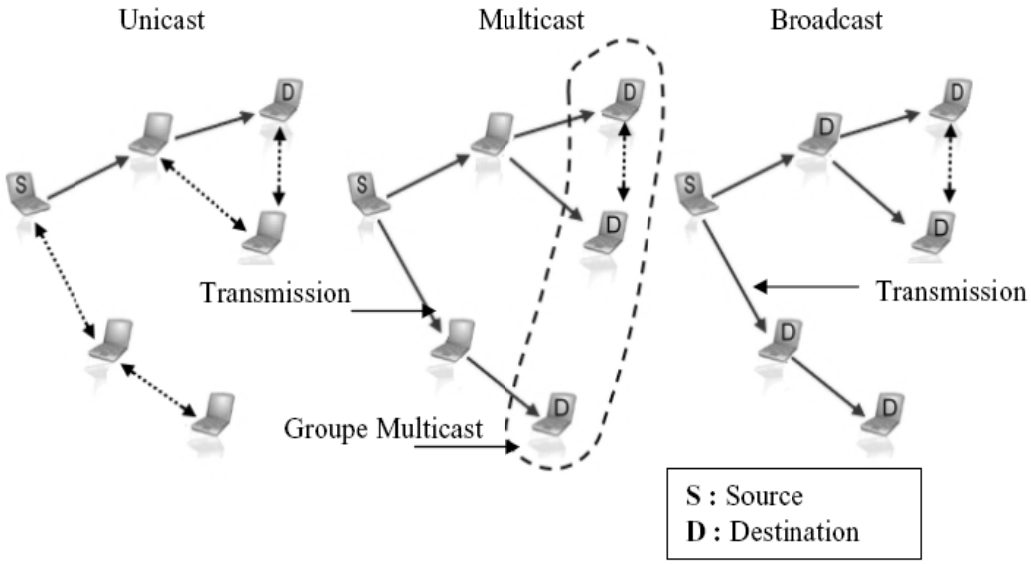


Figure 1.8. **Modes de communication d'un réseau mobile ad hoc.**

I.3.6.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.
- Faible cout.
- L'indépendance, technique et commerciale, vis-à-vis de ports d'accès. **[10]**
- La rapidité de mise en place.
- La robustesse : un réseau évolutif et dynamique. **[7]**

I.3.7.Les handicaps des réseaux ad hoc :

Il existe beaucoup des 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 redandance.

2. la mobilité des nœuds :

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

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

4. les problèmes liés au routage : le problème de routage est l'un des problèmes majeur 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 modestes capacités de calcul et de sauvegarde et de changements rapides de topologies. **[12]**

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, disponibilité et elle concerne deux points, la sécurité des données transitant sur le réseau est limité étant donné que le media de transmission est partagé par tout les nœuds de réseau, et la sécurité du routage. Ces deux aspects comportent quelques vulnérabilités et sont exposés à plusieurs différentes attaques.

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.

Le concept de réseau ad hoc est très prometteur comme nouveau mode de télécommunication propre à compléter et à étendre les systèmes de communication existants. C'est la rencontre des problèmes pratiques, comme la qualité de service, la consommation des terminaux, le routage…etc.

Le problème de routage constitue le problème le plus important dans ce type de réseau, ou l'environnement impose de nouvelles limitations par rapport aux environnements classiques.

Effectivement, le routage est un facteur important dans les réseaux mobiles ad hoc. Le routage et les protocoles de routage feront objet du prochain chapitre.

Chapitre II

le Routage et les Protocoles de Routage dans Ad hoc

Chapitre II *:* Le routage et les protocoles de routage dans ad hoc.

Introduction :

Comme nous avons déjà vu, Les MANETs sont des réseaux auto-organisés sans aucune infrastructure fixe qui manipule la communication entre les nœuds mobiles.

Cette absence d'infrastructure pose un certain nombre de problèmes non triviaux. En particulier, afin d'assurer la transmission des informations d'un bout à l'autre du réseau, les terminaux mobiles doivent avoir la capacité de retransmettre les données. Cependant, les spécificités du lien radio ainsi que la mobilité potentielle des utilisateurs rendent les protocoles de routage utilisés dans les réseaux usuels peu performants.

C'est pourquoi La gestion d'acheminement des données, ou routage, implique l'établissement d'une certaine architecture globale qui doit tenir compte de tous les facteurs et limitations physiques imposés par l'environnement tel que le changement imprévisible de la topologie et la versatilité du médium physique afin que les protocoles de routage résultat ne dégradent pas les performances du système.

Ce présent chapitre entre dans le cadre de l'étude des protocoles de routages les plus connu pour se faire, nous commençons d'abord par une bref définition du routage ainsi les difficultés de se dernier, ensuite nous décrirons les protocoles de routage et leurs classification, enfin nous introduisons quelques protocoles de chaque classification. Notons que ces protocoles de routage ne cessent pas d'être évolués par des groupes de travail spécialisé dans les environnements mobiles.

II.1.Définition de routage :

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**. [12][13].**

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 2.1**)

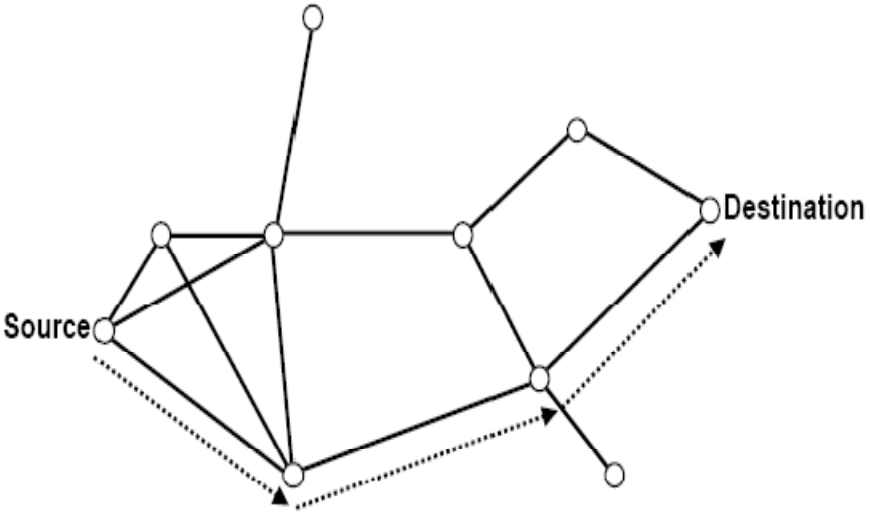


Figure 2.1. Exemple de routage dans un réseau ad hoc.

II.2.Acheminement de l'information dans un réseau ad hoc :

Un réseau ad hoc est un système de communication assurant l'acheminement d'une donnée entre les unités du réseau via les ondes radio, pour se faire il fait appel au deux types d'acheminement : l'envoi direct et le routage.

II.2.1.L'envoi directe (sans intermédiaire): dans ce type, la donnée est envoyée directement de l'émetteur vers le nœud de destinataire sans faire appel aux nœuds intermédiaires.

II.2.2.Envoie par routage : c'est la contre partie de l'envoie directe, les nœuds sont relativement éloignées. Pour la transmission d'une donnée de la source vers un autre nœud qui n'est pas dans sa portée de transmission, il fait appel à une autre station (nœud intermédiaire) qui joue le rôle d'un routeur**. [16]**

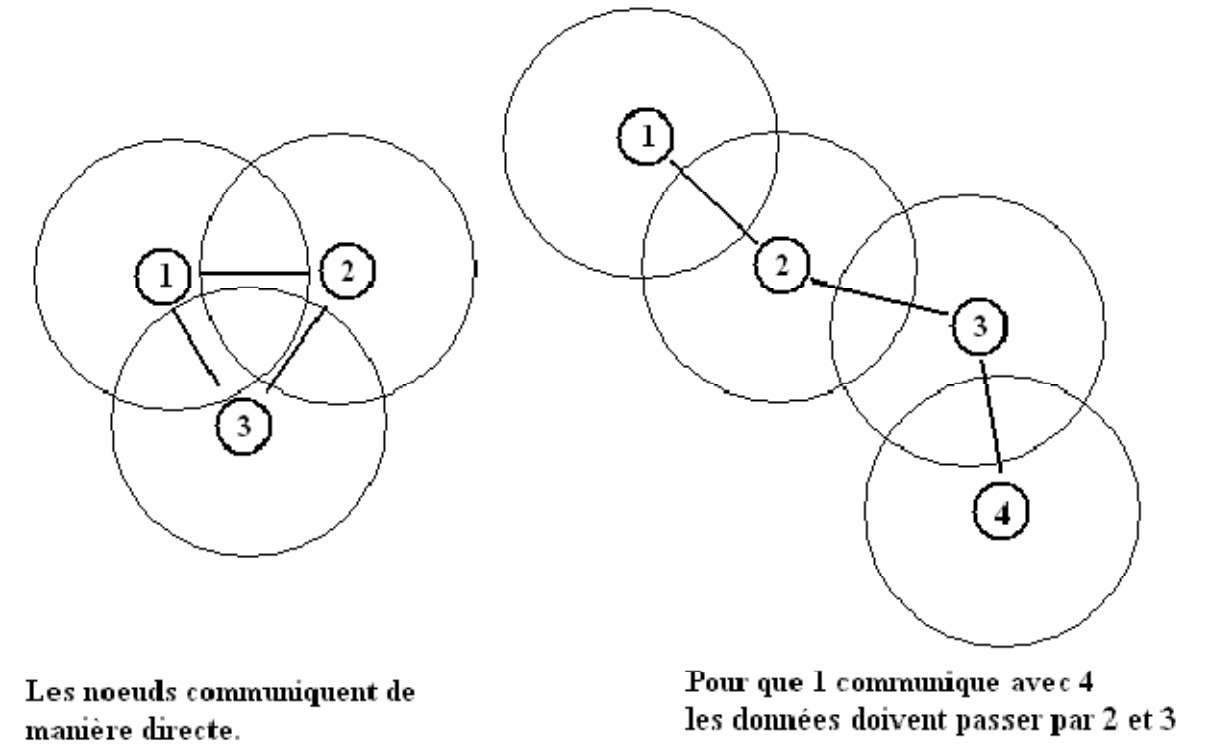


Figure 2.2. La communication entre stations dans les réseaux mobiles Ad hoc.

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

De fait que le réseau ad hoc est défini par une collection de nœuds mobiles et qui sont tout le temps en mouvement, l'interconnexion entre les nœuds peut changer à tout moment.

Dans le cas ou le nœud destinataire se trouve dans la portée du nœud émetteur , le routage est indispensable , mais il se peut qu'un hôte destination soit hors de la portée de communication d'un hôte source , ce qui nécessite l'emploi d'un routage par les stations intermédiaires afin de pouvoir transiter les paquets de message à la bonne destination**.[14]**

Vu les modestes capacités de calcule et de sauvegarde dont est caractérisé un réseau ad hoc, les méthodes d'acheminement utilisée avec la taille du réseau évolutive sont délicates à adaptés et plus complexes à mettre en œuvre.

II.4.Les contraintes de routage dans les réseaux ad hoc :

Le problème consiste à mettre en œuvre d'algorithmes de routage pour garantir la transmission des données dans les réseaux ad hoc.

L'environnement est dynamique, la topologie évolue constamment en fonction des mouvements des mobiles. Il semble donc important que toute conception de protocoles de routage doive tenir compte de limitations physiques imposés par l'environnement afin d'améliorer les performances de système :

- **La minimisation de la charge du réseau** : l'optimisation des ressources du réseau engendre deux autres problèmes l'évitement des boucles de routage, et l'empêchement de la concentration du trafic autour de certaines stations ou lien**. [20]**

- **Offrir un support pour pouvoir effectuer des communications multipoints fiables** : vu que les chemins employés pour le routage des paquets sont capable 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**. [13][14]**

- **Assurer un routage optimal** : le routage doit concevoir des chemins optimaux en tenant compte de différents métriques de couts (bande passante, nombres de liens, délai de bout en bout,…etc.) et il doit assurer une maintenance efficace de routes avec le moindre cout possible **[21].**

- **Le temps de latence** : La qualité des temps de latence et de chemins doit augmenter dans le cas où la connectivité du réseau augmente. **[17]**

II.5.La classification des protocoles de routage.

Le but de toute stratégie de routage est de mettre en œuvre une bonne gestion d'acheminement qui soit efficace et robuste. Pour se faire les protocoles de routage ad hoc s'appuient sur deux modèles de fonctionnement : les protocoles proactifs et les protocoles réactifs. On peut les distinguer par la manière utilisée pour la création et la maintenance des routes lors de transmission des données entre le nœud source et le nœud de destination**. [17][19]**

Les protocoles de routages proactifs établissent les routes à l' avance en se basant sur l'échange périodique de la table de routage tandis que les protocoles de routages réactifs cherchent les routes à la demande.

D'autre classes existent tel que : les protocoles de routage hybrides qui combinent les deux approches précédentes afin de tirer avantages de deux catégories citées précédemment, tout en réduisant leurs limitations, on cite aussi les protocoles géographique, hiérarchique et à qualité de service et multicast. **[19][20]**

La figure ci-dessous illustre les deux grandes classes suivant la façon de découverte et la maintenance des chemins.

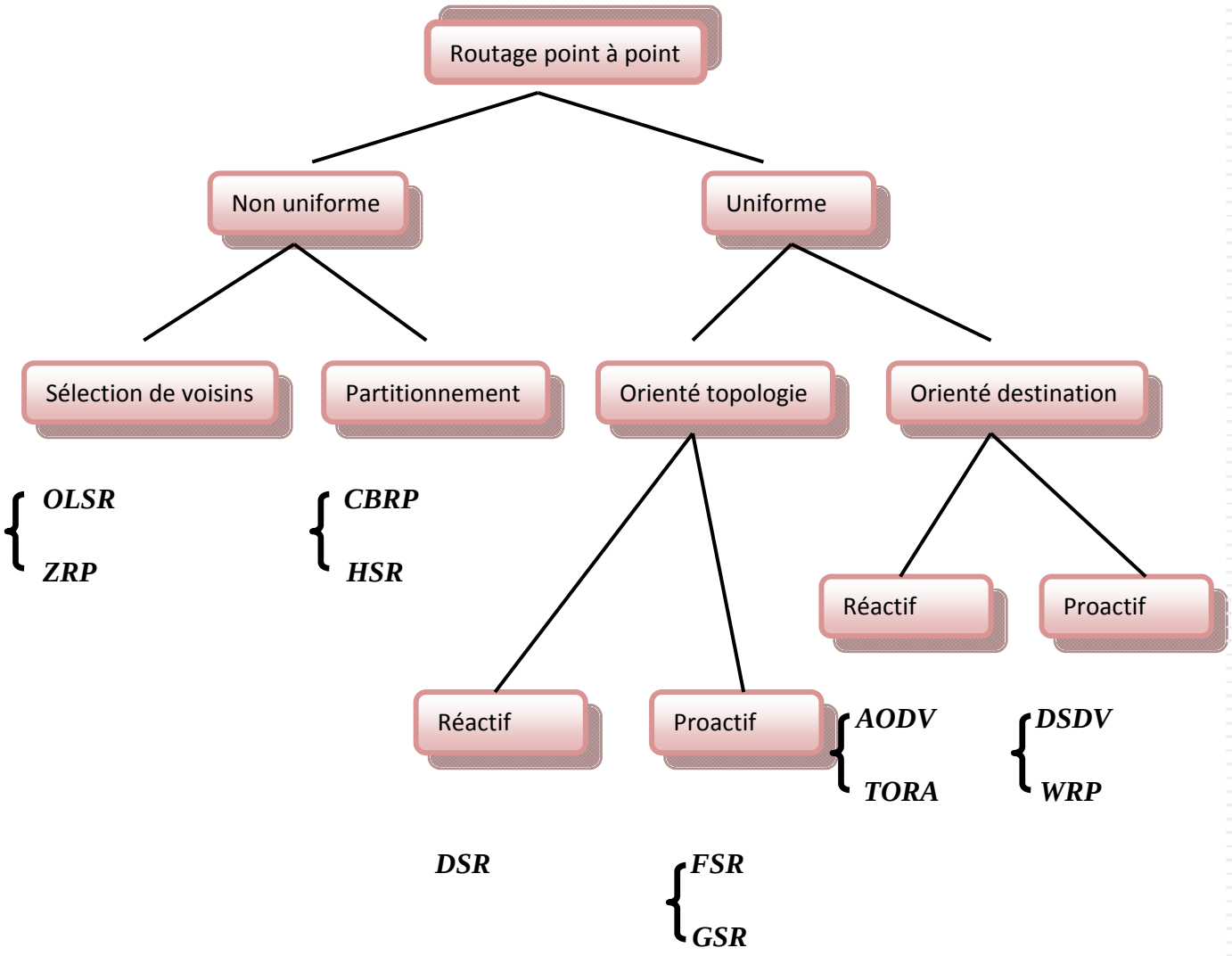


Figure 2.3. Classification des protocoles de routage

Le tableau présenté précédemment présente une taxonomie des protocoles de routage dans le réseau ad hoc ces derniers différencient en premier lieu par le niveau d'implication des nœuds dans le routage.

Type	**Description**
Uniformes	tous les nœuds du réseau jouent le même rôle pour la fonction de routage
Non uniformes	une structure hiérarchique est donnée au réseau et que seuls certains nœuds assurent le routage.
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.
Les protocoles orientés Topologie	chaque nœud utilise comme données l'état de ses connexions avec ses nœuds voisins ; cette information est ensuite transmise aux autres nœuds pour leur offrir une connaissance plus précise sur la topologie du réseau.
Les protocoles orientés Destinations	connus sous le nom de Distance Vector Protocoles, ils maintiennent pour chaque nœud destination une information sur le nombre de nœuds qui les en séparent (la distance) et éventuellement sur la première direction à emprunter pour y arriver.

Tableau 2.1. Une taxonomie des protocoles de routage.

II.5.1.Protocoles de routage proactifs :

Les protocoles de routage 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 fondamental sont utilisée dans cette catégories 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**. [10]**

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**. [10]**

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 et leur mobilité et le cout du maintien les informations de routage et de topologie qui augmente la consommation de la bande passante.

Parmi les protocoles les plus aboutis on cite: OLSR (optimized Link State Routing), DSDV (Dynamic Destination Sequenced Distance-Vector Routing Protocol), FSR (Fisheeye State Routing Protocol).

II.5.2.Protocoles de routage 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 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 récolté les réponses reçues**. [9]**

Plusieurs protocoles appartiennent à cette catégorie, les plus connu :

DSR (Dynamic Source Routing), ABR (associative based rounding), SSR (signal stability based rounding), AODV (Ad hoc On Demand Distance Vector), RDMAR (Relative Distance Micro Discovery Ad hoc Routin Protocol)…etc.

Avantages et inconvénients des protocoles réactifs : ce type de Protocol 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.5.3.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) et CBRP.

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 découpe du réseau.

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

II.5.4.Protocoles de routage uniforme :

Tous les nœuds du réseau possèdent le même rôle, importance et fonctionnalité (**figure 2.4**). Le routage des paquets dépend de la position du nœud.

Deux catégories sont distinguée : les protocoles orientés topologie, plus connus sous le nom de Link-State Protocol et les protocoles orientés destination connu sous le nom de distance Vector Protocol.

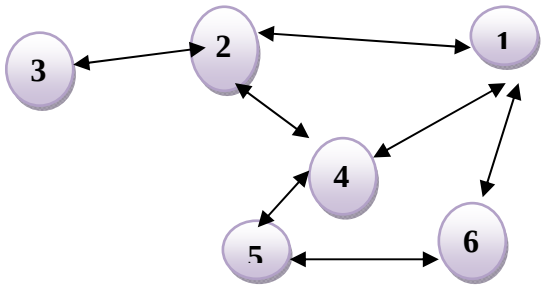


Figure 2.4. Le routage uniforme.

II.5.5.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.5.5.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'ont pas besoin de table de routage ce qui élimine les paquets de contrôle pour maintenir cette table en permettant le gain de la bande passante et l'économie d'énergie des nœuds.

II.6.Etude de quelques protocoles de routage :

II.6.1.Les protocoles de routage proactifs :

II.6.1.1.Le protocole DSDV :

a. Définition :

Le protocole DSDV (Dynamic Destination –Seconced Distance-Vector)**,** 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) **[23].** 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 nouvelles routes et les anciennes et éviter la formation de boucle de routage.

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

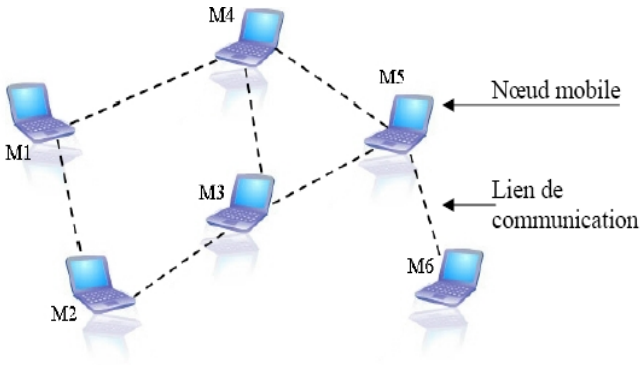


Figure 2.5. Exemple de routage.

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

Destination	Nombre de sauts	Prochain nœud	Numéro 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 2.2.Table de routage du nœud M1de la figure 2.5.

b. Fonctionnement :

Vu le changement dynamique de la typologie 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 étiquetée 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 lorsque une route est demandée.
- Elimine les deux problèmes de boucle de routage et celui du « counting to infinity ».
- 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.

- **Inconvénients :**

- Le gaspillage de la bande passante : dans le cas ou il n'y 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.6.1.3. Le protocole DREAM (Distance Routing Effect Algorithm For Mobility) :

Le protocole DREAM est un protocole de routage proactif basé sur les informations des localisations des unités mobiles dont, chaque station maintient une table de localisation incluant les coordonnées géographique de toutes les destinations qui permet de définir la direction ainsi la distance vers chaque destination**.[22][23]**

Chaque nœud du réseau ad hoc, échange périodiquement des messages de contrôle pour prévenir tous les autres nœuds de sa localisation.

Lors de transmission d'un paquet de données, chaque nœud consulte sa table de localisation. Si ce dernier possède des informations récentes sur la localisation du nœud destination, il choisit un ensemble de nœuds voisins qui se trouvent dans la même direction source/destination. Dans le cas contraire, les données sont inondées dans le réseau entier**.[17]**

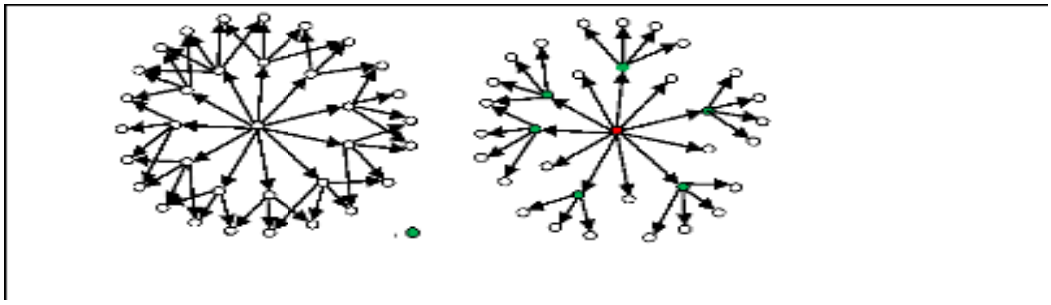
Le protocole Dream assure une meilleure fiabilité de fait que plusieurs copies d'un même paquet de données arrivent à la destination.

II.6.1.4.Le protocole OLSR :

a. Définition :

Le protocole OLSR (Optimized Link State Routing) est un protocole de routage proactifs soumis au groupe MANET de l'IETF, est, comme son nom l'indique, une version optimisé d'un sous ensemble de protocole de routage bien connu : le routage par état de lien optimisé (Link State Routing) ou chaque nœud découvre ses voisins, et informe tout le réseau de son voisin par la diffusion**. [29][17]**

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 (MultPoint Relaying), dans lequel chaque nœud ne déclarent qu'une sous partie de leurs voisinage, ainsi le nombre de message passant par les MPR voir réduit par apport à une inondation classique (**Figure 2.6**). **[29]**



a) b)

a) : Transmission par inondation pure.

b) : transmission avec les MPR.

Figure 2.6.le relais multipoint

Le protocole OLSR utilise quatre (04) types de messages :

- **HELLO** : utilisé pour la détection de voisinage.
- **TC** (**Topology Control**) : permet la diffusion des informations de topologie.
- **MID (Multiple Interface Déclaration)** : permettent de publier la liste des interfaces de chaque nœud.
- **HNA (Host and Network Association)** : utilisés pour déclarer les sous-réseaux et hôtes joignables par un nœud jouant le rôle de passerelle.

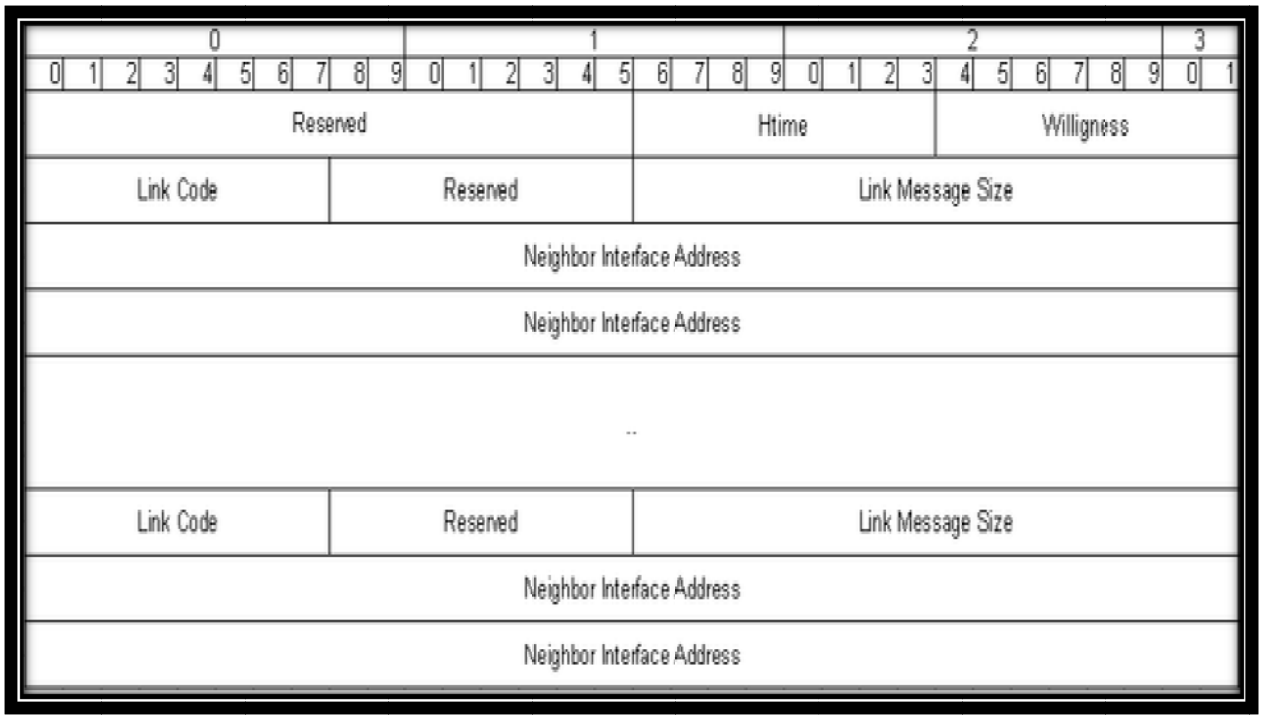
Ainsi OLSR effectue deux actions principales :

- La détection de voisinage, grâce à l'envoi de messages HELLO et à la détermination des MPRs.
- Le contrôle de la topologie, effectuée par l'intervention des messages TC, MID et HNA et aboutissant à une table de routage globale dans chaque entité mobile**. [29]**

- **Message HELLO :**

OLSR propose un mécanisme de détection de voisinage, cela est du à l'envoie périodiquement du message « HELLO » contenant des informations sur les voisins connus et l'état des liens avec ceux-ci. Ce dernier transmet plusieurs informations et a plusieurs utilités.il sert d'abord à découvrir l'ensemble du réseau.il expédie ensuite l'état et le type de lien (symétrique/asymétrique) entre l'expéditeur et son voisin. Enfin, il spécifie le MPR choisi par l'expéditeur.

Diagramme :



- « Reserved » : Ce champ doit contenir « 0000000000000000 »
- « Htime » : Intervalle d'émission des messages HELLO
- « Willigness » : permet de forcer le passage d'un nœud en MPR
- « Link Code » : Code identifiant le type de lien (pas d'information, symétrique, asymétrique, etc.) entre l'expéditeur et les interfaces listées (« Neighbor Interface Address »)

Remarque :

Les messages HELLO ne sont destinés qu'aux nœuds voisins (à un saut) de l'expéditeur, ils doivent donc ne jamais être routés par un MPR.

- **Le relais multipoint MPR :**

Le concept de relais multipoint vise à réduire significativement l'ensemble de retransmission 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 saut. L'ensemble choisit dit le MPR.

Grâce 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.

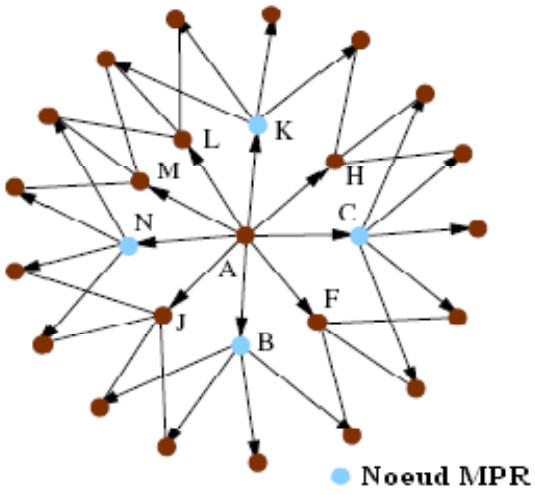


Figure 2.7. Le relais multipoints.

- **Messages TC :**

Le message TC (Topology Control) permet au MPR de lister l'ensemble de ses voisins choisi come étant MPR. Cela sert essentiellement à mettre en place la table de routage.

Diagramme TC :

- « Reserved » : Ce champ doit contenir « 0000000000000000 »
- « ANSN (Advertised Neighbor Sequence Number) » : Entier incrémenté à chaque changement de topologie. Il permet de ne pas tenir compte des informations obsolètes, pour tenir les tables le plus à jour possible.
- « Advertised Neighbor Main Address » : Adresse IP de nœuds à un saut. L'ensemble des nœuds publiés dans les messages TC est un sous-ensemble des voisins à un saut. La version par défaut recommande de publier les "MPR-Selectors", c'est-à-dire les voisins pour lesquels le nœud courant est un relai MPR.

- **Les messages MID (Multiple Interface Déclaration) :**

Ces messages sont émis que par un nœud qui a des interfaces OLSR multiples, afin d'annoncer des informations sur la configuration de ses interfaces au réseau. Un message MID contient une liste d'adresses, L'adresse **I_if_addr** correspond à une interface ainsi que **I_main_addr** est l'adresse principale du nœud émetteur. La diffusion de ces messages se fait par les relais multipoints afin de minimiser le nombre de messages circulants sur le réseau

b. La table de routage :

Chaque nœud maintient une table de routage qui permet le routage des paquets de données vers n'importe qu'elles destination présentés dans le réseau. Le calcule de la table de routage s'appui sur les informations de voisinage, celles de la topologie tout en les combinant avec les associations des interfaces.

La mise à jour de la table de routage se fait à chaque modification des informations de voisinage ou de topologie.la table de routage possède le format suivant :

-R_dest1	R_next1	R_dist1	R_if_id
- R_dest2	R_next2	R_dist2	R_if_id2
-			
-			
-			
-			
- R_destN	R_nextN	R_distN	R_if_idN

- **R_next** : est l'identifiant du prochain saut pour atteindre le nœud identifié par R_dest.
- **R_if_id** : est l'identifiant de l'interface locale par laquelle le nœud peut atteindre R_dest.
- **R_dist** : est la distance estimée en nombre de sauts séparant R_dest du nœud local.

Les entrées dans la table de routage correspondent à tous les nœuds dont le nœud local peut calculer une route valide. Les autres destinations dont la route est partiellement connue, ou possédant un lien cassé, ne sont pas enregistrées dans la table de routage.

c. Avantage et inconvénient :

Le protocole OLSR offre plusieurs fonctionnalités tout en optimisant des routes en termes de nombres de sauts, il permet ainsi de minimiser le nombre de message de contrôle grâce au

concept de sélection de MPR et offre la possibilité de communiquer entre le réseau MANET et un réseau filaire (messages 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 :

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 le 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**. [31][26]**

Vu la densité des réseaux ad hoc, les routes changent 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**. [31]**

b. Les types des messages dans AODV:

Le protocole AODV fonctionne en utilisant trois (03) types de messages :

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

Nombre de sauts1	Num. seq. Destination	@destination	Broadcast id	Num. seq. Source	@source

Figure 2.8. Format d'un message RREQ.

- les messages de réponse de route **RREP** (Route Reply Message) sous la forme ci-après :

@source	@destination	Num. seq. destination	Nombre de sauts2	life time

Figure 2.9. 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 le RREP.

Life time : un temps en milliseconde pour lequel le nœud recevant le RREP 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 l'lorsqu' un nœud source désire établir une route vers la destination sur laquelle il ne possède pas encore d'information dans sa table de routage. Chaque nœud maintient deux compteurs, « node sequence number » et « broadcast_id ».

La source broadcaste un message de type route request RREQ a travers le réseau, contenant les champs suivants :

source_addr	**source_sequence_#**	**broadcast_id**
dest_addr	dest_sequence_#	Hop_cnt

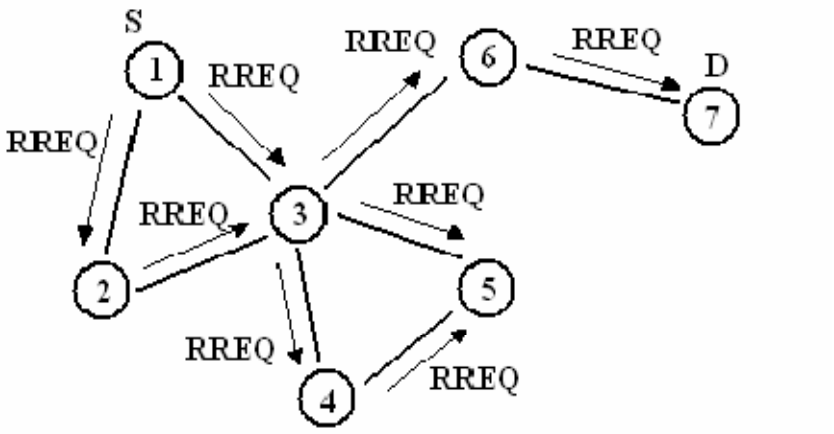
Ou la paire <source_addr, broadcast_id> est une identification du message RREQ, et le champ broadcast_id est incrémenté à chaque envoie de message RREQ.

Lorsque un nœud reçoit le message RREQ, il émet un paquet route reply RREP si il est la destination. Sinon s'il possède une route vers la destination avec un numéro de séquence supérieur ou égale à celui indiqué 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 nœuds 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 de la découverte de la route par AODV :



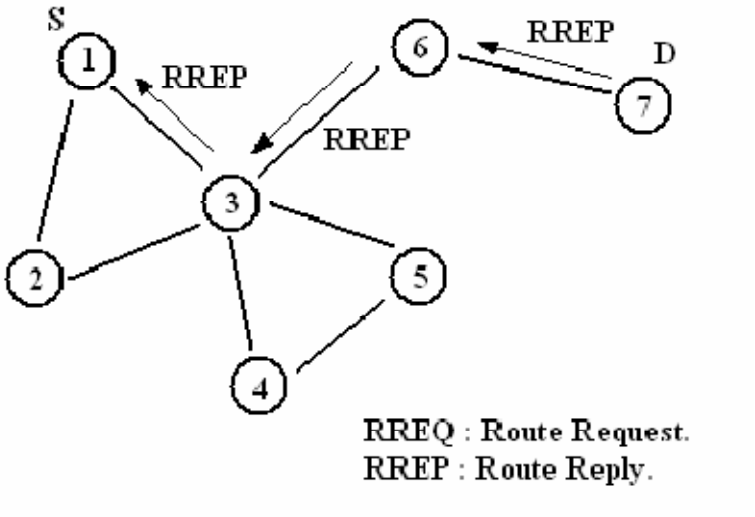


Figure 2.10. le processus de la decouverte de la route par AODV.

d. Maintenance de la route :

Lors de la transmission périodique des données de la source vers la destination la route est considéré active. Une fois la source s'arrête d'émettre des paquets de données, 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 le message HELLO permettant de vérifié la connectivité des routes. Si pendant un laps (période) de temps, trois messages HELLO ne sont

pas reçu, 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. Apres la réception de RERR, si la source désire toujours la route, il peut ré initier un processus de la découverte de la route.

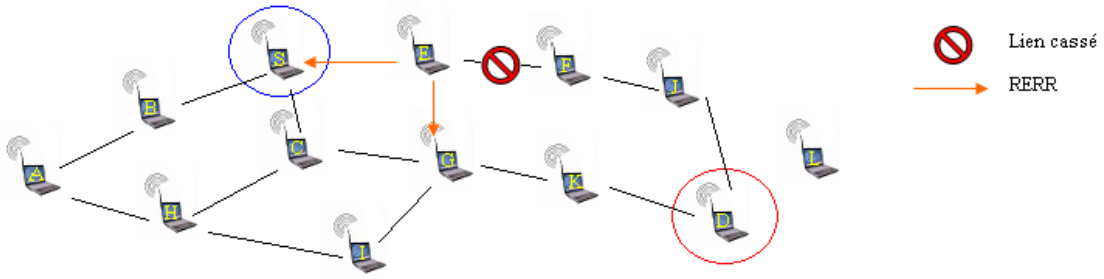


Figure 2.11.Maintenance de route dans AODV

e. Avantages et inconvénients :

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 boucles 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, RERR.

II.6.2.2.Le protocole TORA :

L'Algorithme de Routage Ordonné Temporairement ou TORA (Temporary Ordering Routing Algorithme) est un protocole de routage conçu afin de résoudre le problème de changement dynamique de la topologie dans les réseaux ad hoc, pour cela il a opté pour la mémorisation de plusieurs chemins vers la destination, ce qui minimise l'effet de changement fréquent de la topologie sur le routage des données**. [17]**

Du fait que TORA est un protocole réactive, les routes entre le nœud source et nœud destinataire sont crées à la demande.la notion d'optimisation des chemins est très élémentaire, les longs chemins peuvent être employés afin d'éviter le contrôle causé par la recherche de nouveaux chemins.

L'algorithme TORA s'appuie sur une technique de routage dite « inversement de liens » (Link Reversal), et basé sur l'utilisation de propriété « orientation destination » des graphes acycliques orientés ou DAG (Directed Acyclic Graph).ce dernier peut être orienté destination dans le cas de l'existence d'un chemin vers la destination. Comme il peut devenir non orienté destination si au moins un lien (ou plus) devient défaillant. Dans ce cas l'algorithme utilise le concept de « inversement de liens » permettant la transformation du graphe précédent, en un graphe orienté destination pendant un certains temps fini**. [28]**

Dans le but de maintenir le DAG orienté destination, TORA utilise la taille de nœud qui est échangé par chaque nœud avec ses voisins directes. Un liens est toujours orienté du nœud possédant la plus grande taille vers celui de la plus petite taille.

II.6.2.3. Le protocole DSR :

DSR ou (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 atteindre la destination**. [28][30]**

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 l'orsqu'une route n'est plus valide et d'en informer la source**. [28]**

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**. [28]**

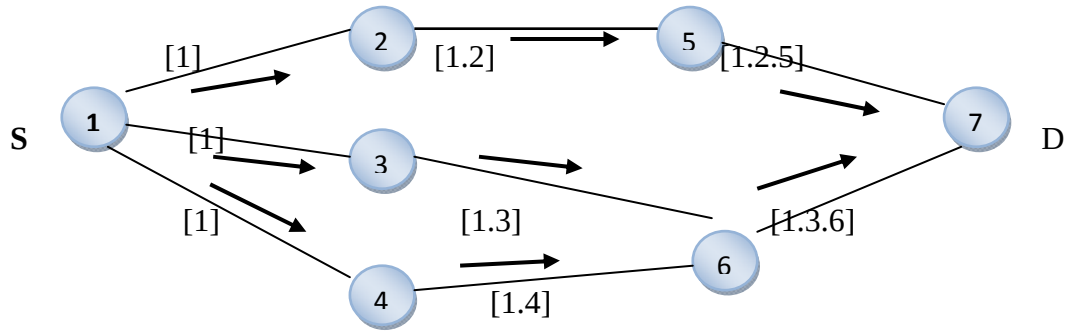


Figure 2.12. La transmission de RREQ.

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

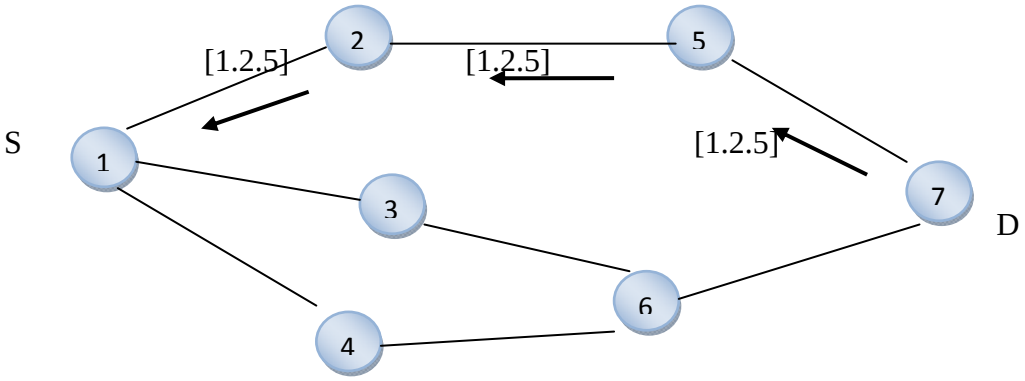


Figure 2.13. Renvoi du chemin par DSR.

b. Le mécanisme de maintenance de la route :

Dans le protocole DSR, chaque nœud est responsable de la confirmation de réception du paquet au nœuds suivant, si pas de réponse sur un paquet de données, une erreur est détectés 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.

c. Avantages 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.6.3.Les protocoles de routage hybrides :

II.6.3.2. protocole ZRP :

Le protocole ZRP (Zone Routing Protocol), est un protocole de routage dit hybride, combinant simultanément un schéma proactif et un schéma réactif afin de combler les problèmes issus de ces deux approches et tirer profil de leurs avantages. Pour se faire il se base sur le concept de décomposition du réseau en plusieurs zones nommés « zone de routage ».

Notant qu'une zone peut être vue comme un sous ensemble du réseau, c'est unités se situent à une distance inférieure ou égale au rayon de la zone.

Le fonctionnement du protocole ZRP s'appuie sur :

- Le protocole **IARP** (Intra-Zone Routing Protocol) : c'est un protocole de routage proactif permettant à chaque nœud de maintenir une table de routage avec ses nœuds voisins au sein d'une même zone.
- Le protocole **IERP** (inter-Zone Routing Protocol) : un protocole réactif assurant le routage vers les nœuds extérieurs de la zone.
- Le protocole **BRP** (Broadcast Resolution Protocol) : employé en association avec le protocole IERP dans le but de minimiser les effets d'une inondation des RREQ dans une zone en s'appuyant sur les routes établit par IARP.

Découverte de la route :

Si le nœud destinataire se trouve dans la zone de nœud source, dans ce cas le chemin est connu. Dans le cas inverse une requête de la recherche de la route est diffusée à tous les nœuds. Cette requête est transmise jusqu'aux nœuds périphériques à l'aide de protocole BRP.

Le nœud périphérique renvoie un paquet RREP au nœud source si ce dernier possède la route. Autrement ils diffusent la requête a leurs propres nœuds periphériques.ce processus se répète jusqu'à atteindre la destination.

Conclusion :

Ce chapitre a axé le fonctionnement et le comportement de quelques protocoles de routage qui ont été proposés afin d'assurer la fonction de routage et comprendre les divers stratégies d'acheminement des données dans les réseaux mobiles ad hoc.

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 fut l'objet du prochain chapitre.

Chapitre III

La Sécurité Dans les Réseaux Ad hoc

Chapitre III : La sécurité dans les réseaux ad hoc

Introduction :

La sécurité dans les réseaux mobiles ad hoc est un challenge en raison des caractéristiques de ces réseaux. L'absence d'une gestion centrale des fonctionnalités du réseau rend ces réseaux beaucoup plus vulnérables aux attaques. De plus, les protocoles de sécurité qui existent actuellement ne sont pas conçus pour un tel environnement (dynamique). Ils ne prennent pas la contrainte des ressources en considération car non seulement l'environnement est dynamique, mais les ressources sont aussi limitées (mémoire, capacité de calcul et surtout énergie), ce qui complique d'avantage la problématique.

Cependant, en raison de l'importance des domaines d'application des réseaux mobiles ad hoc comme les opérations militaires (communication entre les avions, les voitures et le personnel et opérations de secours, situations d'urgence en cas de sinistre, etc.), il faut relever le défi, car concevoir un mécanisme de sécurité infaillible pour les réseaux mobiles ad hoc est nécessaire.

III.1 les risques liés à la sécurité informatique.

III.1.1 Analyse de risque en sécurité :

Les coûts 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 coûts 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 suivants pouvant servir de base à une étude de risque :

1. Détermination des fonctions et données sensible des réseaux ad hoc tel que le routage, la configuration, la gestion d'énergie, et les mécanismes de la sécurité**. [32][35]**
2. La recherche des exigences de sécurité fondées sur les propriétés de la sécurité. [**32]**
3. Etude des vulnérabilités.

4. Etude des menaces ainsi leurs occurrences**. [35]**
5. Mesure du risque encouru en fonction des vulnérabilités mises en lumière et des menaces associées.

La figure 3.1 retrace les différentes phases de ce processus :

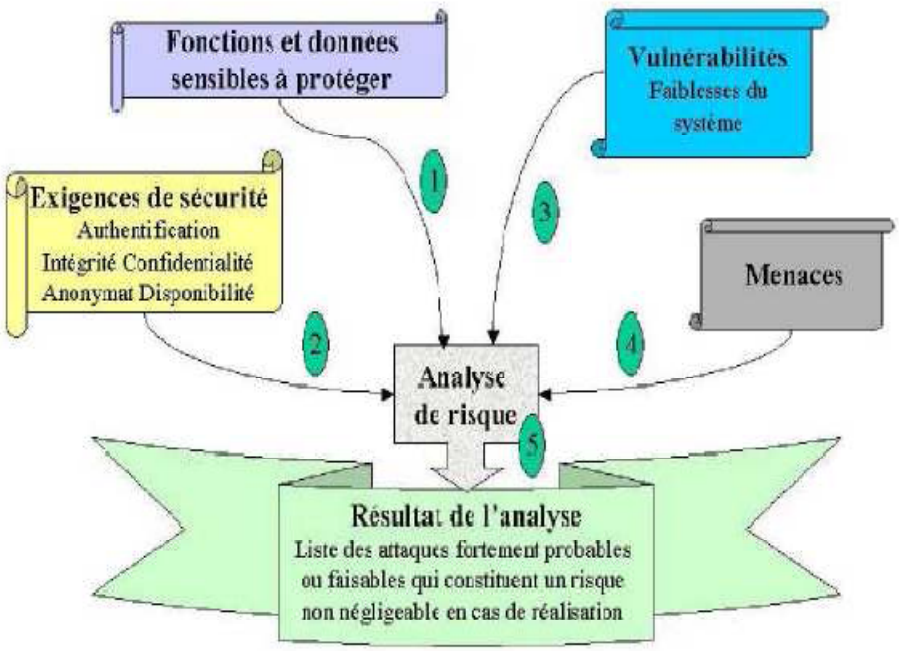


Figure 3.1. **Les différentes étapes de l'analyse de risque.**

III.1.2. Exigence de la sécurité dans les réseaux ad hoc :

Déterminer les exigences de sécurité d'un système donné revient tout d'abord à appréhender les différentes contraintes pesant sur ce système. Cette phase nous permet par la suite d'aboutir à l'ensemble des critères de sécurité**. [34]**

III.1.2.1. Contraintes de la sécurité :

Les contraintes de la sécurité sont réparties en six grands thèmes traitant :

- **La spécificité des nœuds** : les nœuds eux-mêmes sont des points de vulnérabilité du réseau car un attaquant peut compromettre un élément laissé sans surveillance**. [32]** De plus, Certains élément peuvent posséder de faibles capacités de calcule.
- **Gestion d'énergie** : l'énergie doit être conservé au maximum pour cela les nœuds cherchent le plus souvent à se mettre en veille, ce qui provoque donc une minimisation de l'activité de l'ensemble des nœuds. **[32]**
- **L'absence d'infrastructure fixe** : cette caractéristique du réseau ad hoc qui pénalise la gestion des accès aux ressources du réseau.
- **La technologie sans fil** : la diminution du débit de la bande passante due aux différentes perturbations des ondes radio.
- **La mobilité** : les entités sont fortement mobiles, leur sécurité physique est moins assurer.
- **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. **[32]**

III.1.2.2. Les besoins de la sécurité :

A l'instar de la sécurité des réseaux traditionnels câblés, les réseaux mobiles ad hoc sont exposés à un grand nombre de vulnérabilités, surtout au niveau routage**. [34]**

III.1.2.2.1. Disponibilité : vise à assurer la persistance d'un service. Cette propriété est difficile à gérer dans les réseaux mobiles ad hoc vu les contraintes qui pèsent sur ce type de réseau :

- Topologie dynamique.
- Limitation des ressources énergétiques sur quelques nœuds.
- La perturbation de la communication sans fils.

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 (les DoS). **[32][36]**

III.1.2.2.2. Authentification : l'authentification des entités apparait comme la pierre angulaire d'un réseau sans fil ad hoc sécurisé. Elle permet d'identifier et contrôler l'identité des participants afin d'interdire aux intrus d'injecter des messages falsifiés et erronés**. [37]**

III.1.2.2.3 Confidentialité des données : la confidentialité consiste à préserver 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 transitées dans le réseau, et provoquer le disfonctionnement du routage des données. **[39]**

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.

III.1.2.2.4. Intégrité : elle permet de garantir que les messages échangés n'ont pas été altérées ou modifier de manière inattendue. **[38]**

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.

III.1.2.2.5. Non répudiation ou irrévocabilité : assure qu'une entité ne puisse nier avoir effectué une activité (i.e. un message envoyé ne sera pas nié par son expéditeur).

III.1.2.2.6. Fiabilité : vise à assure 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**. [32]**

III.2.Vulnérabilité et attaques existantes dans les réseaux ad hoc :

L'utilisation accrue de connexion sans fil dans les réseaux ad hoc aggrave la préoccupation de l'ensemble de sécurité, et rend le réseau sans fil plus vulnérable aux attaques qu'un réseau filaire. Dans un réseau filaire, un intrus a besoin d'avoir accès physique à une machine du réseau. Alors que sur un réseau sans fil l'intrus est capable d'écouter tout

les messages échangés l'essentiel qu'il se trouve dans la zone de transmission. Cela lui donne la possibilité de perturber facilement les communications en injectant ses propres messages**.[41]**

En général, les attaques menées à l'encontre des communications dans les réseaux ad hoc sont classées en deux catégories : passives et actives. Dans le premier mode, l'attaquant n'intervient pas dans la communication mais il se contente d'écouter et analyser le trafic échangé. A l'inverse, les attaques actives permettent d'agir sur la gestion, la configuration et l'exploitation du réseau. Un attaquant est donc capable de supprimer ou injecter des messages erronés, modifier les protocoles de routages et le bon fonctionnement du réseau. **[38][42]** voici quelques attaques les plus courantes :

III.2.1. Attaque du trou de vers (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 vers 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.

Cette attaque facilite la mise en place d'une autre attaque nommée ***rushing attack*** dans le but de profiter du fait que dans la plupart des protocoles de routage, lors de la découverte de routes, c'est la première requête qui arrive aux nœuds intermédiaires qui est transmise. L'objectif pour l'attaquant est alors de faire passer ses requêtes avant les autres**.[39][40]**

La figure ci-dessous illustre le principe de wormhole :

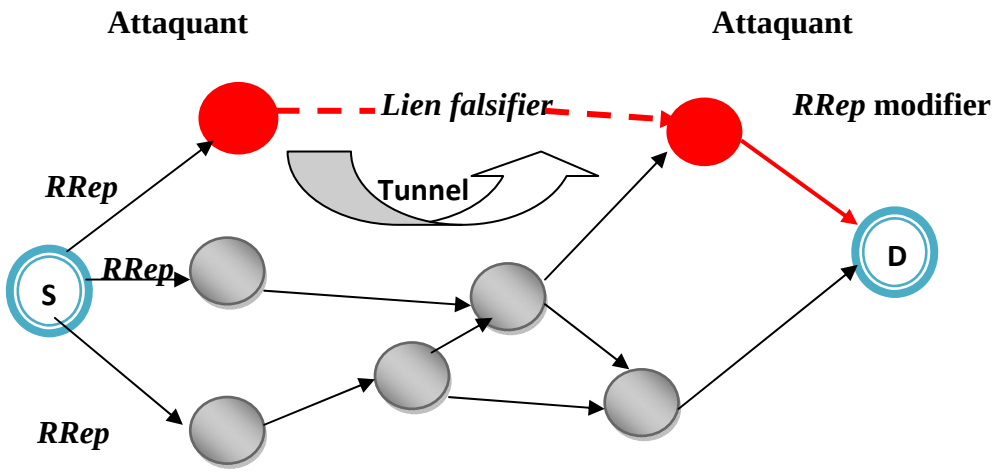


Figure 3.2. Attaque par un trou de vers.

III.2.2. 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 du 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 (voir La figure3.3).

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

- ***Grayholes* :** ne laisse passer que les paquets de routage, le paquet transmis est choisi pour favoriser une partie du trafic**. [43]**
- ***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.

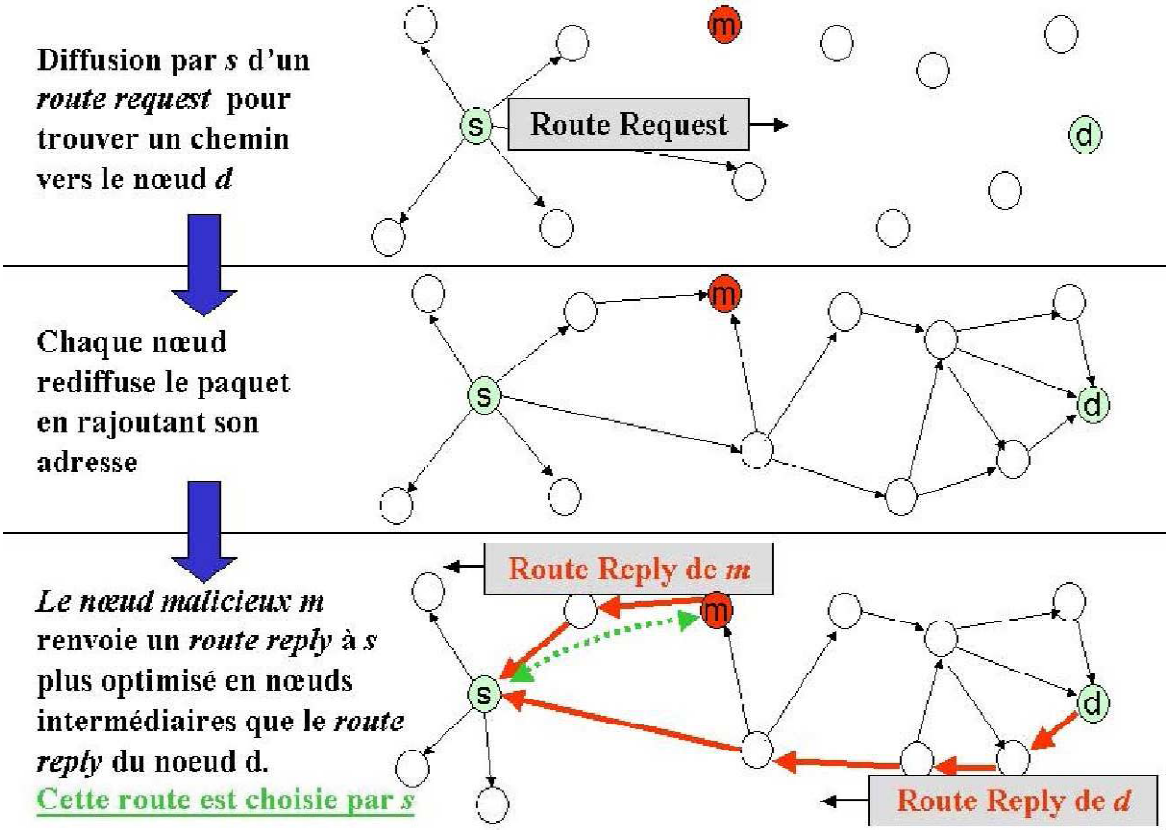


Figure 3.3. Attaque Blackhole.

III.2.3. Attaque par usurpation d'identité : 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 (voir figure 3.4). **[44]**

Topologie vue par le nœud D

Sous l'influence du nœud B

Topologie du réseau

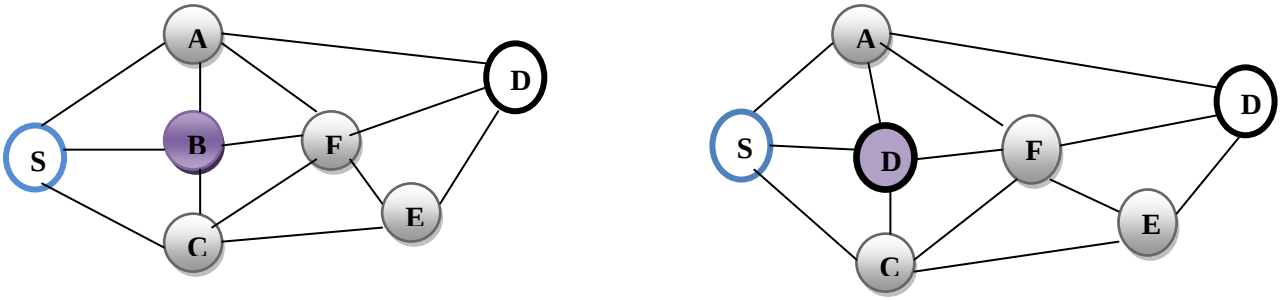


Figure 3.4. Attaque par usurpation d'identité.

III.2.4. Attaque par harcèlement ou déni de service (Denial service) : la plus facile à réaliser par un attaquant, son principal but est de rendre le service indisponible en s'attaquant au fournisseur de service lui-même (indisponibilité de serveur). **[33][34]**

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 routages 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. **[32]**

III.2.5 Les attaques liées aux protocoles de routage :

III.2.5.1. Attaques ciblant les protocoles réactifs et proactifs :

1. Attaques ciblant les protocoles réactifs:

- Attaque par précipitation.
- Attaque par falsification des paquets Route Reply.
- Attaque par falsification des paquets Route Request (numéro de séquence, Destination, nombre de saut.).
- Attaque par non diffusion des paquets Route Error.

2. Attaques ciblant les protocoles proactifs:

- Attaque par altération des tables de routage ou de la topologie.
- Attaque par surcharge des tables de routage ou de la topologie.

III.2.5.2. Classification des attaques :

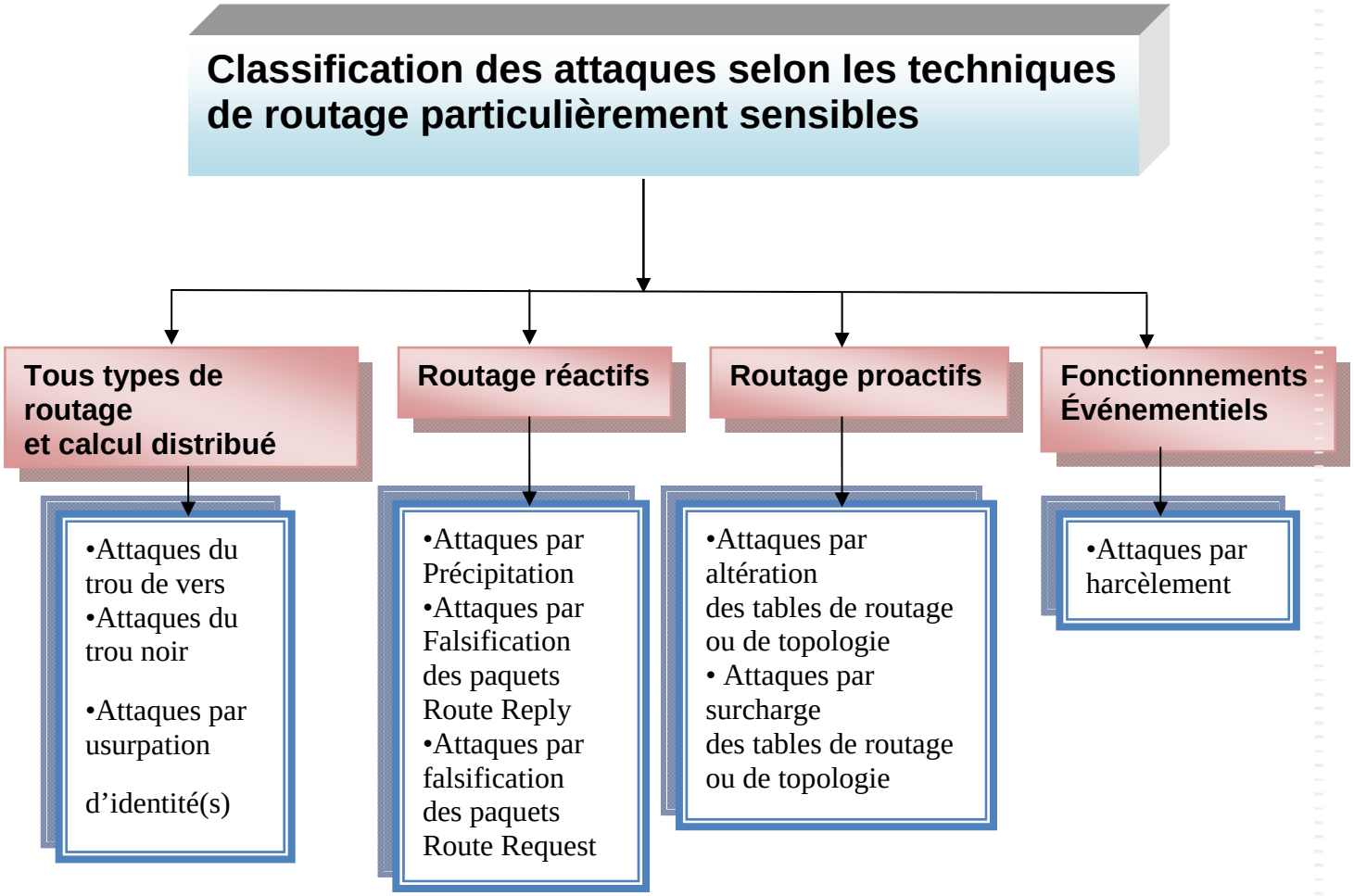


Figure 3.5. Classification des attaques dans les réseaux ad hoc.

Tout les attaques citées précédemment concernent tout les protocoles de routage, il existe par ailleurs d'autre qui exploitent précisément des vulnérabilités spécifiques à certains protocoles de routage. Nous détaillons ces attaques pour les protocoles de routage AODV et OLSR.

III.2.5.3. Vulnérabilité du protocole de routage AODV :

Comme nous avons vu précédemment, le protocole AODV est un protocole de routage réactif ou chaque nœud compte sur la collaboration des autres entités pour le bon déroulement de mécanisme de routage.

L'absence de mécanisme de sécurité dans ce protocole, permet aux nœuds malicieux d'effectuer plusieurs attaques parmi-elles on cite :

- **Suppression du trafic de routage** : plusieurs paquets peuvent être rejetés à cause des nœuds comportant comme des nœuds égoïstes. Ce comportement peut être du à la capacité de calcule ou à la limitation de l'énergie**. [47]**
- **Attaque par consommation des ressource** : cette attaque est du à l'envoi successive des paquets RREQ et RERR dans le but de surcharger le réseau afin de consommer inutilement la bande passante disponible et l'énergie des différents nœuds**. [45][48]**
- **Attaque par modification de numéro de sequence** : l'attaquant répond à une requête RREQ en envoyant un paquet RREP contenant un numéro de séquence plus grand pour favorisée sa requête. De plus, touts les autres nœud génèrent et propagent des fausses informations en insérant l'attaquant dans leur route active**. [45]**

Le tableau suivant présente la conséquence des différentes attaques possibles affectant les paquets de contrôle du protocole AODV :

Champ	**Attaque**
Id_source	Fabriquer un message avec l'identité d'un nœud légitime.
Id_destination	L'attaquant crée des routes vers des destinations inexistantes pour consommer l'énergie du réseau (déni de service).
Id_Broadcast	Ce champ permet d'identifier la requête d'une manière unique et de supprimer une demande déjà traitée. L'adversaire incrémente ce champ pour invalider toute les futures requêtes venant d'un nœud légitime. Décrémenter ce champ dans une requête valide empêche la mise à jour de la table de routage des nœuds intermédiaires car la requête sera considérée comme une demande déjà traitée.
Nbr_saut	Quand le nœud malicieux reçoit un paquet, il suffit qu'il positionne le nombre de saut à 0 pour se présenter comme relai à faible coût.

Num de seq	Un numéro de séquence élevé force la mise à jour au niveau des nœuds récepteurs du paquet. En manipulant ce champ l'adversaire peut injecter de fausses informations de topologie.

Tableau 3.1. Attaques contre le protocole AODV.

III.2.5.4. Vulnérabilité du protocole de routage OLSR :

Dans le protocole de routage proactif OLSR, chaque nœuds génère correctement des messages HELLO et TC ainsi il sauvegarde une vue générale sur la topologie du réseau en se basant sur les messages qu'il reçoit. Ces derniers peuvent subir des modifications pendant la diffusion à travers des différentes attaques. Le protocole OLSR est vulnérable aux deux catégories d'attaques : la génération incorrecte du trafic et le relayage de trafic incorrecte.

- **La génération incorrecte du trafic** : Il inclut quelques attaques unitaires qui touchent les messages de contrôle HELLO et TC du protocole OLSR.

- **Génération incorrecte des messages HELLO** : inclut des attaques sur les messages de contrôle HELLO, deux attaques existantes : usurpation d'identité et usurpation de lien**. [48]**

  - **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 tout les nœuds voisin de l'adversaire ajoutent le nœud identifié dans le message HELLO a la liste de leur voisins direct.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 (voir figure3.6)**. [49]**

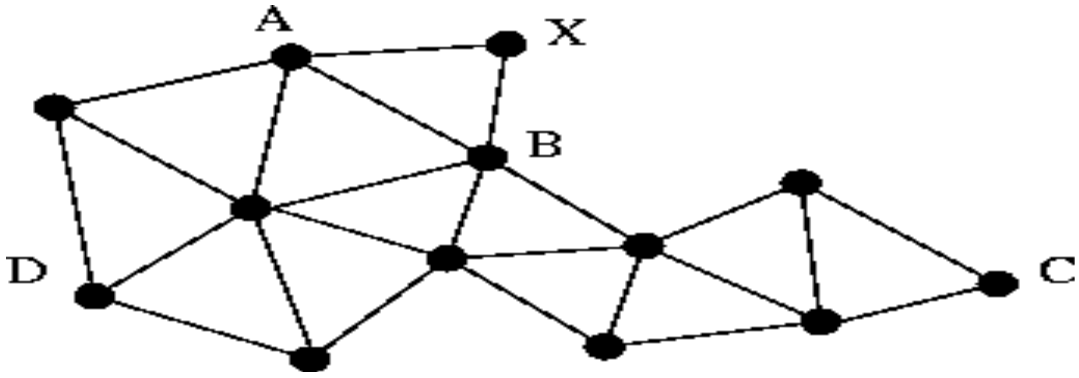


Figure 3.6. Usurpation d'identité dans OLSR.

Dans la figure ci-dessus le nœud X envoie des messages avec C comme origine, les nœuds A et B vont annoncer leur voisinage avec C. Ensuite le nœud X va choisir A et/ ou B comme MPRs avec l'identité de C, ces deux MPRs vont déclarer qu'ils peuvent fournir une connectivité vers C ce qui entraine des conflits de route vers C et une perte de connectivité.

- **Usurpation de lien (*Link spoofing)***: consiste à gérer un ensemble d'information erroné sur l'état du lien (Link Type) avec les voisins ou des relations de voisinages insignifiantes dans les messages de contrôle HELLO. Ce qui entraine des difficultés de sélectionner les MPRs pour les nœuds présents dans le voisinage de l'adversaire et par conséquent peut entraîner une redirection de tous les trafics des nœuds ciblés vers l'adversaire.

Le plus grand risque de ces attaques est la sélection de l'attaquant comme unique et seul MPR du nœud cible, car l'attaquant pourra par la suite de contrôler tous les flux des messages expédiés.

La figure suivante présente ce type d'attaque :

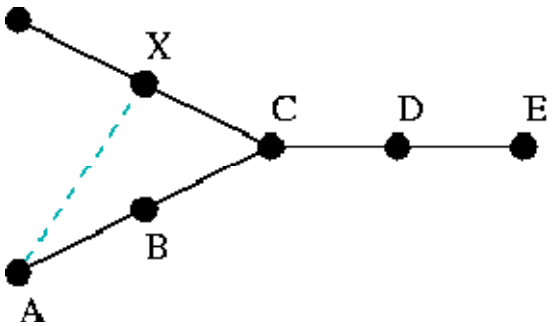


Figure 3.7. Usurpation de lien dans OLSR.

Dans la figure X déclare un lien symétrique avec A. le nœud C va choisit donc les nœuds X et D comme MPRs au lieu de X, B et D. par conséquent les messages de E ne vont pas joindre A.

- **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 vérifié si l'origine d'un message TC est un nœud MPR. Cette attaque permet de définir des routes passantes par l'adversaire. **[49]**

  - **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 type 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 liens existants qui conduit au même résultat de la suppression de message TC**. [49]**

& Le relayage de trafic incorrect :

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

Dans cette attaque, un nœud adversaire supprime une partie ou tous les messages 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 apparaître**. [50]**

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.3.Etat de l'art des solutions pour la sécurité :

S'il est clair que les problématiques de sécurité posées par les réseaux sans fil ad hoc sont réelles et complexe, elles ne restent heureusement 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.3.1.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 nécessité de concevoir des schémas ou des protocoles qui s'adaptent a ce changement de la topologie dans les manetes**. [32]**

Une première ligne de défense pour contrecarrer les 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 propose pour l'authentification, l'inconvénient commun entre ces solution est l'utilisation des algorithmes cryptographique asymétrique (a clé public**). [42][53]**

& **Cryptographie 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**. [51][53]**
Deux modèles basant sur la clé secrète :

- ***The Key agreement*** : Les participants s'entendent sur une clé secrète. Les recherches en matière de Key agreement dans les réseaux ad hoc se focalisent sur la manière d'établir une clé commune entre plusieurs participants qui ne se connaissent pas a priori. Cette clé leur permet de s'authentifier et de communiquer d'une manière sécurisée. La mise en place de cette clé peut se faire de manière distribuée**. [56]**

- ***The Duckling Security Policy Model*** : Le modèle d'authentification élaboré par RossAnderson et Franck Stajano**. [56]**

Les algorithmes symétriques les plus connus sont : Diffie-Hellman

Autre algorithme comme : Le **DES** (*Data Encryption Standard*), le **3DES** (prononcé « Triple DES »), et **l'AES** *(Advanced Encryption Standard).*

& **Cryptographie asymétrique (clef publique) :** chaque entité considère une paire de clés complémentaires et sont générée simultannement.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**. [54][51][50]**

Exemple d'algorithmes asymétrique :

L'infrastructure à clé publique auto-organisée **PKI *(Public Key Infrastructure***) : Une infrastructure de gestion de clés (IGC) ou PKI *(public key infrastructure)* 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'initialisation 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 sûre une clé publique à Une entité (utilisateur, serveur, etc**.). [56][52]**

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

En plus d'utilisation de ces solutions pour la gestion de la clé, une autre technique a été proposée comme chaine de hashage, TESLA (Time Efficient Stream Loss-tolerant Authentication) et IDHC**. [56][51]**

III.3.2.Solution pour la sécurisation du routage : le mécanisme de cryptographie tel que le cryptographie à clé symétrique, clé public ou chaine de hashage 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.3.3.Solution pour renforcement de coopération des nœuds : afin d'éviter le problème des nœuds égoïste dans les réseaux ad hoc trois solution sont mise en place pour renforcer la coopération de chacun des nœuds : Les solutions base sur le système de réputation, Les solutions basée sur le modèle de « micro-payement », et d'autre solution existantes**. [55]**

- **Les solutions basées sur le système de réputation :** les deux solutions fondées sur le système de réputation sont :

CORE : Utilisé pour imposer la coopération entre les nœuds. Il se base sur une technique de surveillance distribuée. Ce mécanisme de coopération n'empêche pas un nœud de nier la coopération ou de dévier d'un comportement légitime mais s'assure que les entités se conduisant mal soient punies en leur refusant graduellement les services de communication**.[32][56]**

CONFIDANT : détecte les nœuds malveillants grâce à un mécanisme d'observation qui fournit un rapport sur différent type d'attaque : les nœuds malveillants sont isolés et ne peuvent plus être sollicités pour le routage des paquets**. [56]**

- **La solution basées sur le modèle de « micro-payement** » : il se focalise sur le principe suivant : les nœuds qui profitent du réseau (émetteurs et /ou récepteurs) payent les nœuds 'fournisseurs de services' **(**nœuds intermédiaires). De cette façon, tout nœud doit servir les autres pour être servi lui-même.

Une autre solution consiste à utiliser ***la cryptographie à seuil*** afin d'exclure collectivement les nœuds égoïstes. De plus, exige qu'un nœud intermédiaire (lui-même aussi

surveillé par ses propres voisins) change de route s'il juge que le nœud à qui il transfère des données est égoïste**. [51]**

III.3.4.Solutions 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 AuthenticationCode). 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. **[53]**

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

III.3.5.Solutions pour la Confidentialité

La confidentialité dans les réseaux ad hoc est d'abord traitée par l'utilisation de transmission par saut de fréquences, *frequency hoping*. Les données sont transmises sur une séquence de fréquences définies pseudo-aléatoirement. L'attaquant doit connaître 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 donnée qu'une des contraintes des réseaux ad hoc est de devoir être adaptables 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**. [56]**

III.3.6.Solutions 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 le corrompre. 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. **[32]**

III.3.7.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.

Conclusion :

Ce chapitre montre à quel point les réseaux sans fil ad hoc constituent, de par leur nature, un formidable challenge pour la sécurité informatique.

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

Deuxième Partie :
le simulateur NS et notre Contribution

Proposition d'un nouveau protocole de routage pour simuler L'attaque Blackhole dans un réseau ad hoc

Chapitre IV

Environnement de simulation NS2

Chapitre IV : Environnement de simulation NS2

Introduction :

Dans ce présent chapitre nous allons essayer de présenter le simulateur NS2, que nous allons utiliser pour évaluer les performances du protocole qu'on à proposé.

Pour se faire, Nous allons tout d'abord, éclaircir certaines fonctionnalités du Simulateur NS2. Tel que la prise en charge des réseaux (sans fil et câblés), et son adaptation aux réseaux mobiles ad hoc, ainsi que la simulation proprement dite. Celle-ci comprend plusieurs phases : implémentation, scénario de simulation, et autres mesures tel que la connectivité, la charge et la mobilité.

IV.1.Environnement de simulation :

IV.1.1.le simulateur NS2 :

NS2 est un outil logiciel de simulation de réseaux informatiques, il est parmi les simulateurs les plus utilisés, afin de simuler et étudier les performances des protocoles réseau. Il offre une plateforme de développement de nouveaux protocoles et permet de les tester**. [61]**

C'est un simulateur a événement discret oriente objet, développé dans le cadre du projet VINT (Virtual Inter Network Testbed) qui est dirigé par l'université de Californie du sud et est financé par le DARPA en collaboration avec Xerox PARC et LBNL. Le but de ce projet est la construction d'un simulateur réseau qui offre des outils et des méthodes innovatrices dans un environnement proche de la réalité. Ce simulateur essaie de répondre aux questions de mise à l'échelle (simulation de grandes topologies) et d'interaction entre protocoles dans des services intégrés à l'Internet (problèmes d'hétérogénéité)**.[60][63**]

NS2 couvre un très grand large nombre d'applications, protocoles, types réseaux et des éléments de réseaux, il est basé sur deux langages : un Orienté Objet simulateur écrit en C++ et un langage orienté objet OTCL (Object TCL) dérivé du TCL (Tool Command Langage) qui permet à l'utilisateur de décrit sous forme d'un script les conditions de la simulation : topologie du réseau, caractéristiques des liens physiques, protocoles utilisés, communications…etc. La simulation doit d'abord être saisie sous forme de fichier texte que

NS utilise pour produire un fichier trace contenant les résultats. NS est fourni avec différents utilitaires dont des générateurs aléatoires et un programme de visualisation : NAM (Network Animator) permettant une représentation du graphe du réseau sur lequelle nous pouvons voir circuler les paquets, suivre le niveau des files d'attente, etc. **[63] [61]**

NS est un simulateur développé et distribué gratuitement à partir de ce lien : **http://www-mash.cs.berkeley.edu/ns.**

Dans ce qui suit nous allons présenter quelques concepts de base concernant la simulation.

IV.2.Présentation du simulateur NS2 :

NS-2 est un simulateur développé en C++ et en OTcl ; Le pacquage inclus une hiérarchie de classe compilée d'objets écrits en C++ et une hiérarchie de classe interprétée d'objets écrits en OTcl. La question qui se pose pourquoi l'utilisation de deux langages ? Tout simplement c'est par ce que NS exploite deux raisonnements distincts. D'une part, la simulation doit être efficace afin de manipuler les bits, les entêtes des paquets ainsi pour implémenter des différents algorithmes aptes de parcourir plusieurs types de données. Cette tache nécessite une rapidité d'exécution qui est offerte par le $C^{++.}$ D'autre part, le changement rapide des scénarios de simulation, la configuration des objets et la gestion des événements, impose l'utilisation l'OTcl. **[63][60][62]**

La figure ci-dessous montre la double hiérarchie de classes dans NS:

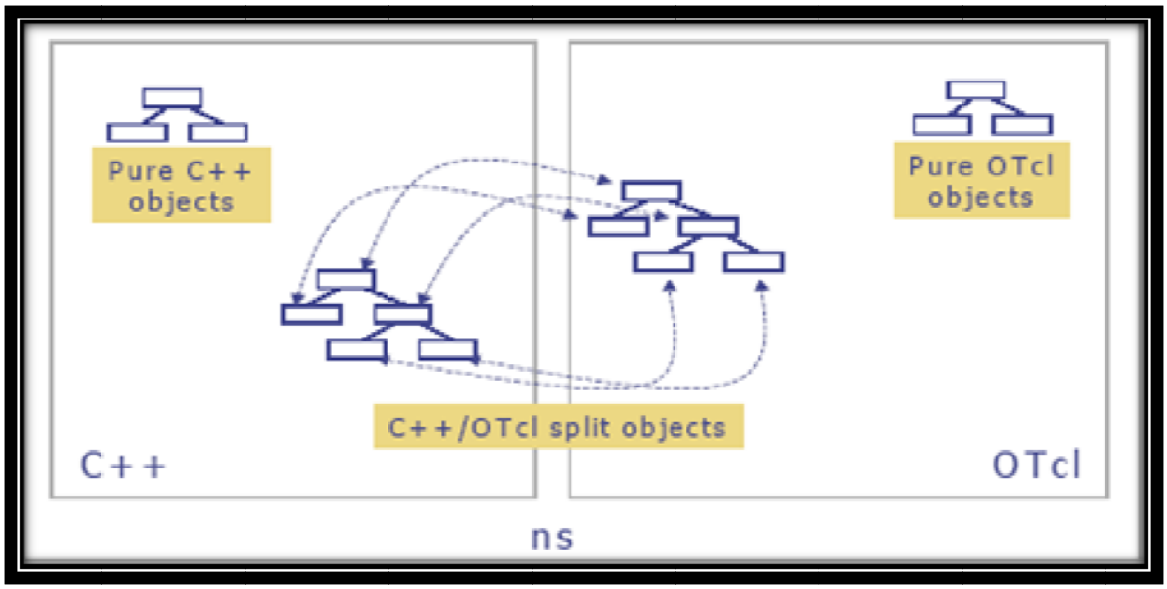


Figure 4.1. Dualité C++/ OTcl dans NS

1. Les instructions de base en OTCL :

1.1. Conventions :

nom { } signifie une fonction ou méthode OTcl. Elle se nomme dans ce langage des "Instance procédure".

nom ( ) signifie une fonction ou méthode C++.

"_" Dans le code, ce caractère est appliqué comme suffixe au nom des variables; il indique une variable d'instance.

1.2. Les substitutions :

- Substitution de variable : $<variable>

Le contenu d'une variable est obtenu en faisant précéder le nom de variable par le symbole $

- Substitution de commande : [<commande>]

La substitution de commande permet de remplacer la commande par son résultat. Les caractères entre les crochets doivent constituer un script Tcl valide. Le script peut contenir un nombre quelconque de commandes séparées par des retours à la ligne et des ";".

- Anti-slash substitution: "\"

Il est utilisé devant les caractères '**retour à la ligne'**, '**$'**,' **['** pour indiquer de les interpréter comme des caractères ordinaires.

1.3. Les Inhibitions :

Il existe plusieurs façons d'empêcher l'analyseur syntaxique de donner une interprétation spéciale aux caractères tel que '**$'** ou '**;'**. Ces techniques se nomment inhibitions. OTcl fournit deux formes d'inhibitions:

- double quotte (") inhibe les séparations de mots et de commandes. Il reste les substitutions de variable et de commande. Les caractères espaces, tabs, retour à la ligne et point-virgule sont traités comme des caractères ordinaires.

- accolade inhibe toutes les substitutions et tous les caractères spéciaux. Les caractères compris entre les crochets sont considérés comme un mot.

1.4. Quelques exemples des instructions de bases d'OTCL :

- Assigner une valeur à une variable : **set a 10**
- Lire le contenu d'une variable et l'assigner a une autre variable : **set b $a**
- Ouvrir un fichier : **set f [open file w]**
- Imprimer le contenu d'une variable dans un fichier : **puts $f "$b"**
- Opération arithmétiques : **set a [expr $b (+-*/) $c]**
- Structure de contrôle : **if {$a==$b}{……}**

  for {set i 1} {$i<=10} {set i [expr $i+1]} {……}
- Définir une fonction: **proc fonction {param1 param2….} {**

  global a b

  …….

  Return [expr $a + $param1] }

  Set c [fonction $param1 $param2…]

- Instancier une classe: **set obj [new Class1/Class2/Class3]**
- Appeler une méthode d'un objet sans retour:**$obj method param1 param2 …**
- Et avec retour : **set a [$obj method param1 param2……]**
- Assigner une valeur à un attribut d'un objet : **$obj set attrib 10**
- Lire le contenu de l'attribut d'un objet : **set a [$obj set attrib]**

2. Le fonctionnement de NS :

Le simulateur NS fonctionne en utilisant deux éléments essentiels :

- **Un interpréteur** : permettant la création de modèle de simulation après avoir rassembler les différents outils nécessaires pour la simulation.
- **Un moteur de simulation** : effectuant des calculs nécessaire pour les différents modèles construit par l'utilisateur via l'interpréteur.

La figure ci-après montre les différentes phases de procédure de simulation :

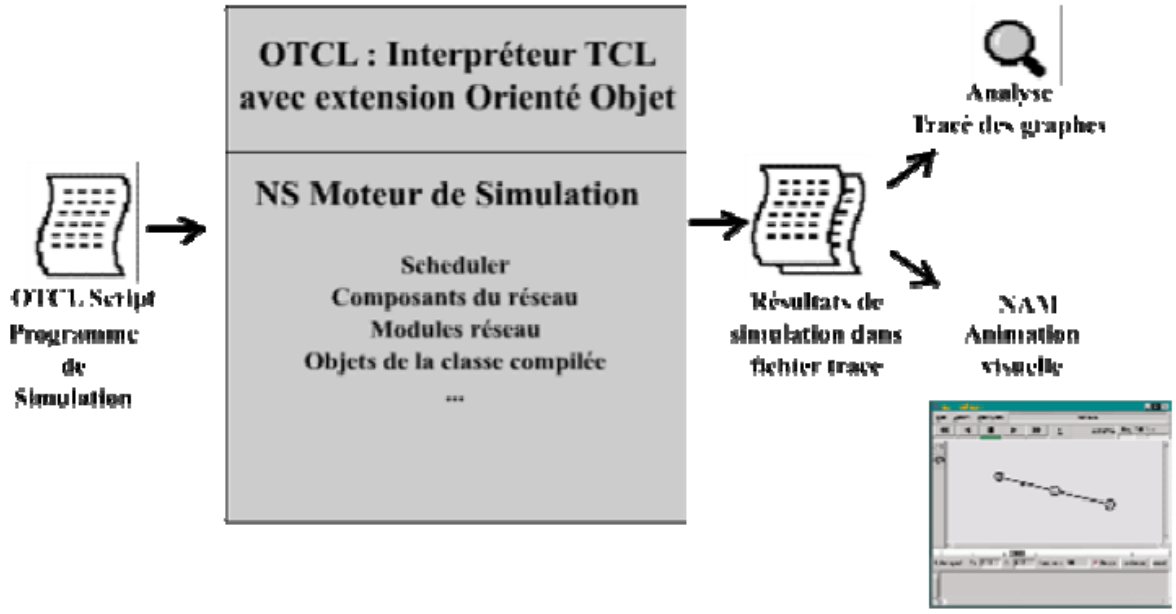


Figure 4. 2. Simulation sous NS2.

La simulation est décrite comme suit :

- Un fichier de script OTCL décrivant l'environnement et les conditions de simulation, est passé à l'interpréteur TCL de NS-2.
- L'interpréteur crée le modèle de simulation et assemble les différents éléments nécessaires à l'étude de la simulation. Par la suite, il fait appel au moteur de simulation qui effectue alors les calculs applicables à l'environnement décrit dans le fichier de script.
- A l'issue de ces calculs, des informations sur les mouvements des nœuds, sur ceux des paquets ainsi que des données sur l'état de ces nœuds au cours de la simulation sont enregistrées dans un fichier de traçage.

- Ce fichier peut par la suite être lu ou interprété, selon les cas, pour une visualisation de la simulation ou pour tracer des graphes sur une étude quelconque relative à la simulation.

3. Les composants d'un modèle :

Le modèle de réseau NS est constitué de :

- Nœud de réseau : c'est endroit ou est générer le trafic.
- Des liens de communication entre les différents nœuds du réseau.
- Des agents de communication représentants les protocoles de niveau transport (TCP, UDP) ; ces agents sont reliées aux nœuds et connectés l'un à l'autre, ce qui permet un échange de données (connexion TCP, flux UDP). **[60]**
- Applications qui génèrent le trafic de données selon certaines règles, et se servant des agents de transport (CBR : Constant Bit Rate). **[60]**

4. Modèle de mobilité dans NS :

Vu le changement dynamique et aléatoire dans ce type de réseaux, le simulateur NS met en œuvre plusieurs types de modèle de simulation Grâce à ces modèles, nous pourrons mesurer ce facteur important, qui est la mobilité. Et de ce fait, nous permettre d'évaluer le comportement du protocole de routage ad hoc. Parmi ces modèles de mobilités nous retrouvons :

& Random Waypoint Model (RWM):

Dans ce modèle la mobilité des nœuds est typiquement aléatoire. En effet, la destination et la vitesse de chaque nœud mobile, désirant se déplacer, est aléatoire, et est limité à un intervalle bien déterminé.

Après son déplacement le nœud mobile s'immobilise pour un temps fini, puis se déplace à nouveau de la même manière que la première fois, et cela jusqu'à la fin de la simulation.

& Random Direction Model (RDM) :

De la même façon que le modèle précédant (RWM), le choix de la destination ainsi la vitesse du chaque nœud est aléatoire. À la différence que dans le modèle RDM le nœud en Déplacement doit atteindre les bornes de la surface de simulation, puis s'immobilise.
Une fois le nœud immobile, et dans un intervalle de 180° par rapport à la position D'arrêt (borne atteinte), le nœud mobile peut entreprendre à nouveau son mouvement aléatoire.

& Modified Random Direction Model (MRDM):

C'est une modification de la version RDM. Cette dernière permet aux nœuds mobiles, en déplacement, de ne pas forcement atteindre les bornes de la surface de simulation.

Le modèle RWM répond bien aux caractéristiques des réseaux mobiles ad hoc en offrant une mobilité aléatoire aux nœuds mobiles appartenant au réseau. Contrairement aux modèles RDM et MRDM qui, d'une manière indirecte, conditionne le mouvement des nœuds.

5. Outils utilisés par NS-2 :

NS-2 fournit quelques outils importants pour les besoins de simulation tel que :

- **NAM (Network Animator)** : NAM est un outil de visualisation qui présente deux intérêts principaux : représenter la topologie d'un réseau décrit avec NS-2, et afficher temporellement les résultats d'une trace d'exécution NS-2. Il est capable aussi de représenter des paquets TCP ou UDP, la rupture d'un lien entre nœuds, ou encore de représenter les paquets rejetés d'une file d'attente pleine.

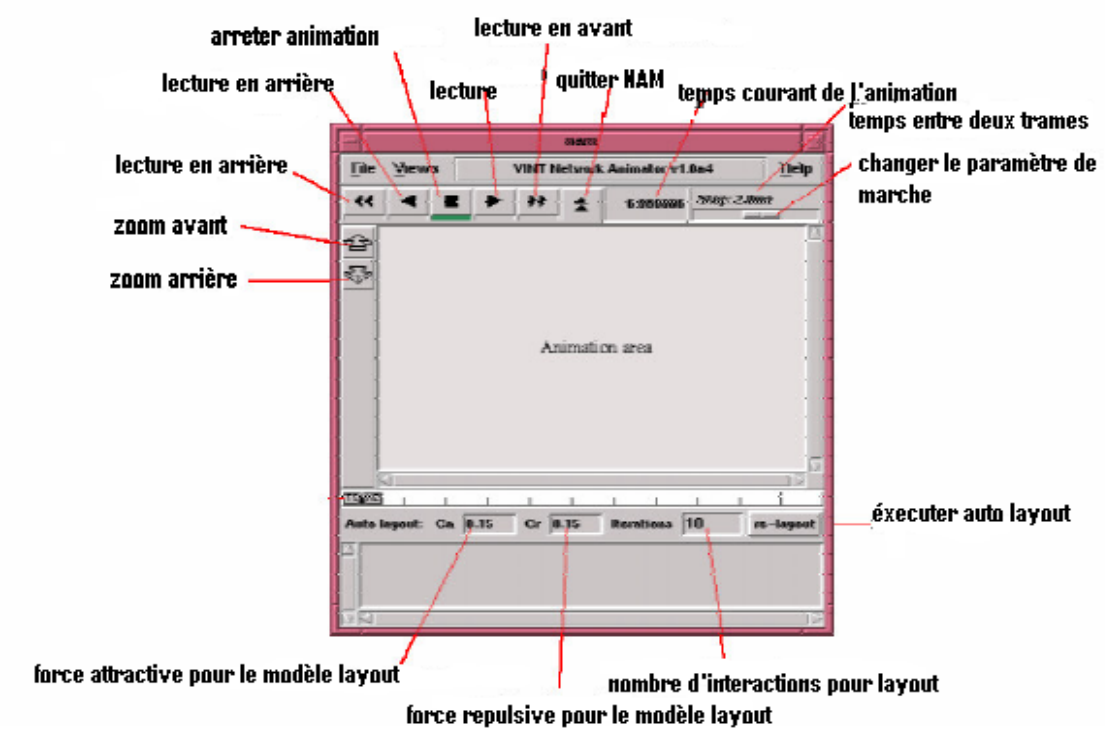


Figure 4.3. Fenêtre d'animation NAM.

- **Xgraph** : permet de tracer les résultats d'une simulation sous forme de courbes.
- **Gt-itm** : c'est un générateur de graphes qui facilite la création de grands réseaux.
- **Sgb2ns** : permet de convertir les informations fournies par gt-itm en des instructions pouvant être interprétées sur l'interface OTCL du simulateur.

6. Techniques de simulation

La simulation des différents protocoles de routage des réseaux 802.11 s'appuie sur quatre étapes indépendantes :

6.1. Pré-simulation

Durant cette phase, nous allons générer le script principal en OTCL à faire passer à NS2 ; ce script est généré automatiquement à partir de plusieurs modèles de scripts TCL pour les configurations et la manipulation de fichiers, ainsi qu'un script OTCL contenant le code de

génération du trafic sur le réseau et un autre script OTCL, contenant les instructions définissant le mouvement des nœuds dans le réseau. L'ensemble des ces

Fichiers constitue un "scénario" de simulation.

```
##########################simulation Setup####################
set SIMULATION_ID sim1
set SIMULATION_TIME 600
set SIMULATION_COUNT10
set SEED 1.0
set AGENT_TRACE ON
set ROUTER_TRACE ON
set MAC_TRACE OFF
set MOVEMENT_TRACE OFF
########################## Mobility############################
Setup
set MAX_SPEED 5
set PAUSE_TIME 0
########################## MAC/LLC Setup#######################
set MAC_TYPE Mac/802_11
set ANTENNA_TYPE Antenna/OmniAntenna
set INTERFACE_QUEUE Queue/DropTail/PriQueue
set MAX_QUEUE_SIZE 50
set NET_INTERFACE Phy/WirelessPhy
set CHANNEL_TYPE Channel/WirelessChannel
set PROPAGATION_MODEL Propagation/TwoRayGround
set LINK_LAYER LL
```

6.2 Simulation

Durant cette phase, NS2 va simuler les différents scénarios pendant une durée bien fixée. Le résultat de ces simulations se trouve dans des fichiers de trace générés par NS2. Le fichier de trace généré par NS2, est un fichier texte très volumineux avec plusieurs millier de lignes et ayant une taille de plusieurs centaine de Mo. Une ligne typique d'un fichier de trace se présente ainsi (Il n'y a pas de retour à la ligne) :

s -t 10.000000000 -Hs 0 -Hd -2 -Ni 0 -Nx 5.00 -Ny 2.00 -Nz 0.00 –Ne -1.000000 -Nl AGT -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 0.0 - Id 1.0 -It cbr -Il 1000 –If 2 -Ii 2 -Iv 32 -Pn cbr -Ps 0 -Pa 0 -Pf 0 -Po 0

Cette ligne correspond à l'émission **(s)** à l'instant 10.000000000 **(-t)** d'un paquet de donnée CBR **(-It)** par le nœud 0 **(-Is)** se trouvant dans la position (5.00, 2.00) **(-Nx,-Ny)** à destination du nœud 1 **(-Id)**. Le nexthop auquel le nœud 0 va envoyer ce paquet est le nœud 2 **(-Hd)**. Ce paquet est émis avec un TTL = 32 **(-Iv)**.

Cette ligne décrit un événement bien précis lors de la simulation, détecté à un instant mesuré au nano-seconde près.

Quatre types d'événement sont possibles :

- **s_** émission d'un paquet (send)
- **r_**réception d'un paquet (receive)
- **f_**routage d'un paquet (forward)
- **d_**perte d'un paquet (drop)

6.3 -Post-simulation

Dans cette phase, nous allons récupérer les fichiers de trace NS2 et en extraire les résultats que nous voulions visualiser ou interpréter. Cette extraction ainsi que toute autre opération de calcul est assurée par plusieurs scripts en langage AWK (Aho, Weinberger, & Kernighan.).

Le listing ci dessus est un extrait du script AWK pour le calcul et l'extraction des résultats.

$1 == "s" && $19 == "AGT" && $33==0.0){if(control[$41]== 0){start[$41]=$3;control[$41]=1;} }($1 == "r" && $19 == "AGT" && $33==0.0)

{star=start[$41];delay=$3-star;printf star;printf " "; printf delay;printf "\n";}

Cette partie du code comptabilise le délai de bout en bout d'un paquet émis avec une

Priorité = 0.

6.4 Exploitation

Une fois les résultats sont calculés, les scripts AWK les enregistrent dans des fichiers que nous pouvons ensuite sauvegarder ou bien utiliser avec d'autres programmes pour tracer des courbes ou bien effectuer d'autres calculs.(MatLab, Exel,Xgraph, GnuPlot,etc).

La figure suivante illustre les différentes techniques de simulation :

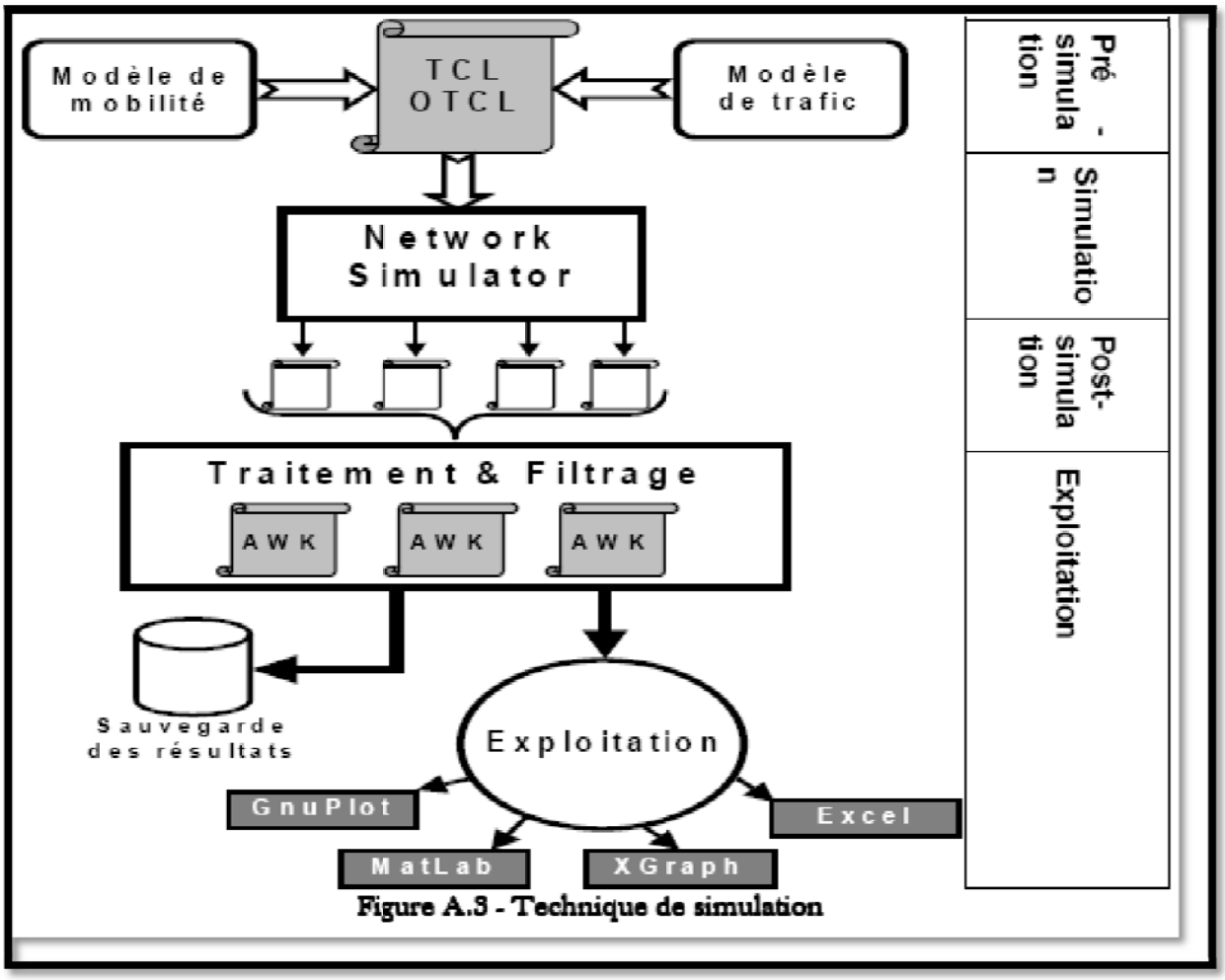


Figure A.3 - Technique de simulation

Conclusion :

Ce chapitre nous a permit de présenter d'une façon détaillée l'environnement de simulation NS2.

Le prochain chapitre décrit l'implémentation du l'attaque ***Blackhole*** dans le simulateur NS2.

Chapitre V

Simulation de l'attaque Blackhole

Chapitre V : Simulation de l’attaque Blackhole.

Introduction :

La simulation de l’attaque Blackhole à été faite sous Network Simulator 2 (version ns-2.34). Nous avons récupérer le code source du protocole de routage réactif AODV auquel on a apporté des ajouts et des modifications pour lui permettre de simuler l’attaque ***Blackhole***.

V.1.présentation de l’attaque trou de noir (Blackhole) dans le protocole AODV :

V.1.1. principe de Blackhole :

Dans les réseaux ad hoc qui utilise le protocole de routage réactif AODV, l’attaque Blackhole absorbe tout le trafic du réseau et supprime tout les paquets de contrôle.

Afin de mieux expliquer le principe de cette attaque, on ajoute un nœud malicieux à la figure suivante **:**

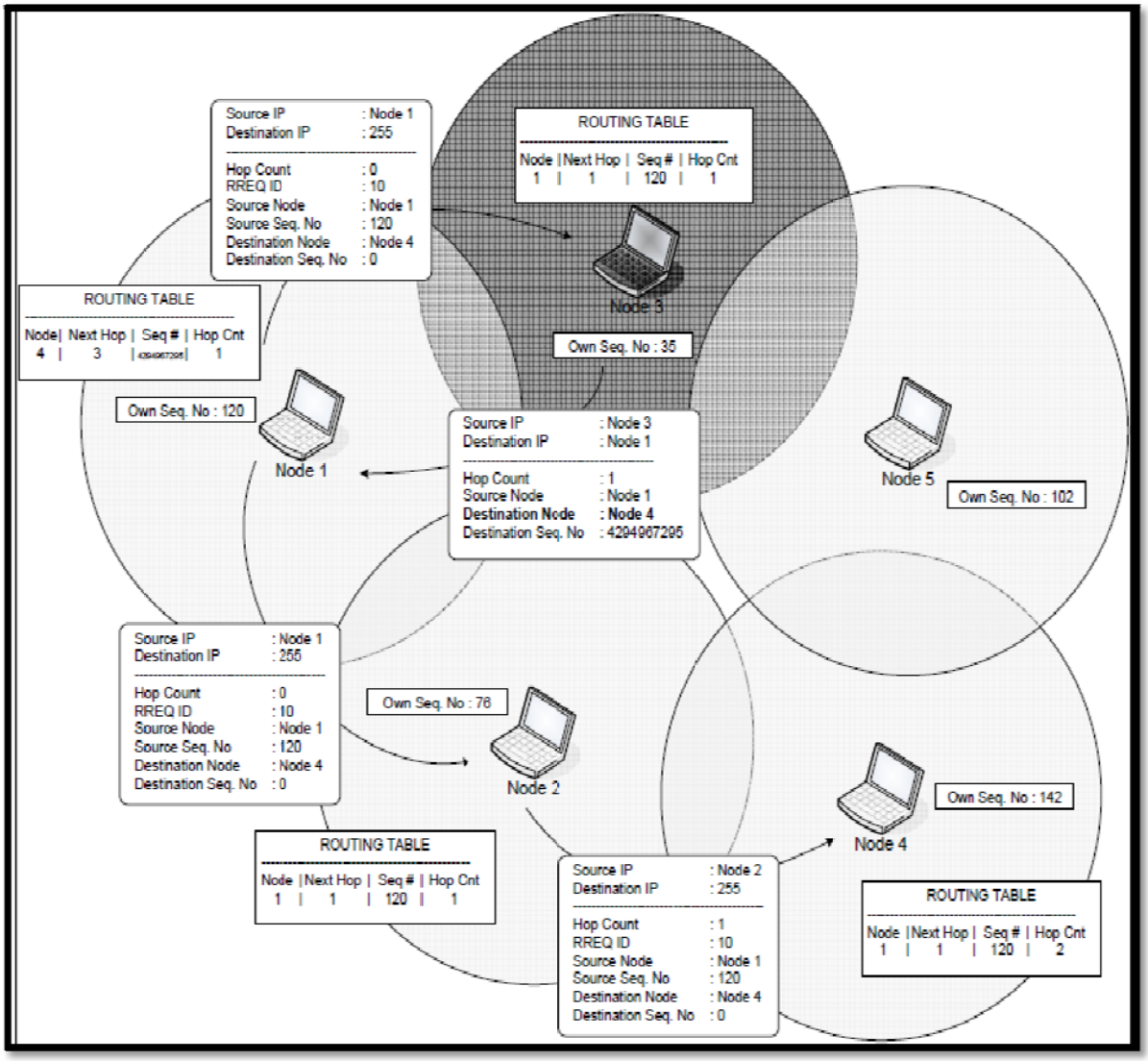


Figure 5. 1. Illustration de l'attaque Blackhole.

La figure montre que le « **nœud 3** » est le nœud malicieux. Quand le « **nœud 1** » envoie un message RREQ au « **nœud 4** », le « **nœud 3 »** va répondre immédiatement au **« nœud 1**» avec un message RREP contenant le plus grand numéro de sequence.

Le « **nœud 1** » considère que le « **nœud 3 »** comme un voisin du nœud destinataire ce qui lui permet d'ignorer les paquets RREP envoyé par le « **nœud 2 ».**

Le « **nœud 1 »** va donc commencer à envoyer ses données au « **nœud 3 »** en espérant atteindre la destination « **nœud 4** » mais le nœud malicieux « **nœud 3**» supprime tout les paquets envoyés.

V.2.Un nouveau protocole de routage pour simuler l'attaque Blackhole :

Afin d'implémenter un nouveau protocole de routage unicast dans le simulateur NS2 nous avons effectué plusieurs modifications à différents niveaux.

Dans notre travail, nous avons utilisé les nœuds qui présentent un comportement trou noir « Blackhole » dans le réseau sans fil ad hoc qui utilise le protocole de routage réactif AODV. Ces nœuds doivent utiliser le nouveau protocole implémenté.

Les principales étapes à suivre pour mettre en œuvre ce nouveau protocole sont décrites en détails dans la section ci-dessous :

Tout les protocoles de routage dans NS sont installés dans le répertoire des **"ns-2.34 ".**

On commence tout d'abord notre travail en dupliquant le protocole AODV dans ce répertoire et changer le nom de répertoire par **"blackholeaodv"**. Ensuite on modifie tout les fichiers étiquetés **"aodv "** dans ce répertoire par **"blackholeaodv**" tels que ***blackholeaodv.cc***, ***blackholeaodv.h, blackholeaodv.tcl, blackholeaodv_rqueue.cc, blackholeaodv_rqueue.h*** etc.

Le point clé de notre travail est que le protocole **AODV** et **blackholeaodv** enverra tout les deux le même paquet de contrôle. Par conséquent, nous n'avons pas copié le fichier ***"aodv_packet.h"*** dans le répertoire **blackholeaodv**. De plus, on change tout les classes, fonctions, structures, variables et constantes dans tout les fichiers, sauf le fichier ***"aodv_packet.h".***

Apres avoir effectué tout les changements cités précédemment, on doit changer deux fichiers utilisés par NS2 pour intégrer le nouveau protocole **blackholeaodv** dans le simulateur. Ces deux fichiers sont :

- le fichier ***"\tcl\lib\ ns-lib.tcl"*** où des agents du protocole sont codés comme une procédure. Quand un nœud utilise le protocole **"blackholeaodv",** cet agent est prévue au début de la simulation et il est affecté à des nœuds qui vont utiliser le nouveau protocole **"blackholeaodv".**

La procédure agent du protocole **"blackholeaodv"** est montrée dans la figure

Ci-après :

```
blackholeAODV {
set ragent [$self create-blackholeaodv-agent $node]
}
Simulator instproc create-blackholeaodv-agent { node } {
set ragent [new Agent/blackholeAODV [$node node-addr]]
$self at 0.0 "$ragent start"     # start BEACON/HELLO Messages
$node set ragent_ $ragent
return $ragent
     }
```

Figure 5.2.le code ajouté dans le fichier "*\tcl\lib\ ns-lib.tcl*".

- Le fichier **"*\makefile*"** dans le répertoire de **"ns-2.34 "** où on ajoute les lignes suivantes :

```
blackholeaodv/blackholeaodv_logs.o blackholeaodv/blackholeaodv.o \
blackholeaodv/blackholeaodv_rtable.oblackholeaodv/

blackholeaodv_rqueue.o \
```

Figure 5.3.ligne à ajouté au "*\makefile*"

Remarque : après chaque implémentation, on doit recompiler NS2 pour avoir les fichiers objet.

Jusqu'à présent, nous avons mis en place un nouveau protocole de routage nommé **" blackholeaodv ".** Mais les comportements Black Hole n'ont pas encore été mis en œuvre dans ce nouveau protocole de routage. Pour ajouter un comportement Black Hole dans ce nouveau protocole nous avons fait mêmes des changements dans **blackholeaodv/ blackholeaodv.cc** fichier C + +.

Ces changements sont décrits comme suit :

Lorsque un paquet est reçu par la fonction "***recv*"** de **"aodv/aodv.cc"**, il sera acheminé selon son type :

- Si le paquet est un paquet de gestion AODV, il sera envoyé à la fonction ***"recvAODV".***
- Si le paquet reçu est un paquet de données, le protocole AODV l'expédie à l'adresse de destination, mais se comporter comme un trou noir qu'il supprime toutes les données.

Le code suivant montre que la première condition ***"if "*** permet au nœud de recevoir le paquet de données s'il est la destination. La condition ***"else"*** supprime tout les paquets.

```
if ( (u_int32_t)ih->saddr() == index)
forward((blackholeaodv_rt_entry*) 0, p, NO_DELAY);
else
drop(p, DROP_RTR_ROUTE_LOOP);
```

Figure 5.4. Condition "*if* "pour accepter ou refuser un paquet.

Si le paquet est un paquet de gestion AODV, La fonction "***recv*"** l'envoie à la fonction "***recvblackhole*AODV"** qui fait appel au fonction "***recvRequest*"** s' il s'agit d'un paquet RREQ, et a la fonction "***recvReply*"**dans le cas de paquet RREP.

Ce processus est illustrer avec le principe ***"case"*** décrit ci-dessous :

```
recvRequest(p);
break;
case AODVTYPE_RREP:
recvReply(p);
break;
case AODVTYPE_RERR:
recvError(p);
break;
case AODVTYPE_HELLO:
recvHello(p);
break;
default:
fprintf(stderr, "Invalid blackholeAODV type (%x)\n", ah>ah_type);
exit(1);
```

Figure 5.5. Condition *"case"* pour choisir le type de message de contrôle.

Dans notre cas nous allons considérer la fonction RREQ parce que le comportement Trou noir est réalisé quand le nœud reçoit un paquet malicieux RREQ.

Lorsque le nœud malveillant reçoit un paquet RREQ, il envoie immédiatement un paquet RREP s'il possède un chemin récent vers la destination.il tente donc de tromper les nœuds en envoyant un tel paquet RREP.

Numéro de séquence le plus élevé du protocole AODV est **4294967295**, valeur entière de 32 bits non signé. Les valeurs de paquet RREP envoyé par le nœud malicieux sont fixés à :

- **« 4294967295 »** pour le numéro de sequence.
- **« 1 »** pour le nombre de sauts.

  Le message erroné RREP de l'attaque Blackhole est montré dans la figure suivante :

```
sendReply(rq->rq_src,                    // IP Destination
                  1,                     // Hop Count
                  index,                 // Dest IP Address
                  4294967295,            // Highest Dest Sequence Num
                  MY_ROUTE_TIMEOUT,      // Lifetime
                  rq->rq_timestamp);     // timestamp
```

Après tous les changements sont finis, nous avons recompilé tous les fichiers NS-2 pour créer des fichiers objet.

Ayant achevé la compilation, nous avons un nouveau banc d'essai pour simuler l'attaque Black hole.

V.3.Test du Blackhole AODV :

Nous allons tester l'implémentation du l'attaque Blackhole. Pour se faire nous allons utiliser NAM (Network Simulator) de NS2.

Afin de tester l'implémentation on utilise deux simulations :

- Le premier scenario sans le nœud malicieux Blackhole.
- Le deuxième scenario avec l'ajout du nœud malicieux Blackhole.

Le résultat de simulation est comparé avec NAM.

V.4.Paramètre de simulation :

Pour étudier la faisabilité ainsi que l'efficacité de notre attaque, nous l'avons implémenté dans un outil de simulation : **NS2** le Network Simulator2.

Pour cela nous avons utilisé :

- Le logiciel de simulation des réseaux sans fil Network Simulator ns-2.34.

- Le protocole de routage réactif *AODV*.

- Le modèle de mobilité ***way point*** avec une vitesse maximale de 20m/s.

- Un modèle de génération de trafic CBR (Constante Bit Rate).

- Notre simulation se déroule sur une surface de 670m x 670m.

- Un nombre de nœuds égal à 50.

- La portée radio de chaque nœud est de 250m

- la bande passante du canal radio est de 2Mb/s

- La durée de chaque simulation effectuée est de 900s

- La taille de la partie utile des paquets de données est de 512octets

-Nous avons utilisé le modèle de la couche MAC : 802.11 qui est inclus dans le NS.

-Le protocole de transport utilisé est (TCP).

V.5.Proposition une solution pour contrecarrer l'attaque Blackhole :

Dans le protocole AODV normal, lorsqu'un nœud reçoit un paquet RREP il vérifie d'abord la valeur de numéro de séquence dans sa table de routage. Le paquet RREP est accepté s'il contient un RREP_seq_no plus élevé à celui de la table de routage. Notre solution consiste à vérifier si RREP_seq_no est supérieure à la valeur seuil qui est mise à jour dynamiquement dans les intervalles de temps. Si RREP_seq_no est supérieur à la valeur seuil, le nœud est soupçonné d'être malveillant et il est ajouté à la liste noire.

Quand un nœud détecte ce nœud malveillant il envoie un paquet ALARM pour ses voisins contenant les paramètres du l'attaquant. En outre, si un nœud reçoit le paquet RREP de ce dernier, ce paquet sera tout simplement ignoré et ne sera jamais traité.

Ainsi, de cette façon, le nœud malveillant est isolé du réseau par le paquet ALARM. Les réponses provenant du nœud malveillant sont bloqués, ce qui entraîne moins du Routages généraux.

Conclusion :

Dans ce chapitre nous avons présenté la dernière étape de notre travail qui consiste en étude de l’attaque Blackhole qui trouble le fonctionnement des protocoles de routage réactif plus précisément le protocole de routage AODV. Ensuite, nous avons implémenté un nouveau protocole de routage afin de simuler cette attaque. Puis on a proposé une solution pour contrecarrer cette attaque.

Conclusion et perspectives

Conclusions et perspectives

Conclusion :

Les réseaux mobiles ad hoc, sont des réseaux composés des nœuds pouvant être en mobilité permanente rendant ainsi la topologie du réseau dynamique. Ce sont des systèmes totalement distribués qui offrent beaucoup d'avantage à leur utilisation et révèlent une architecture prometteuse pour assurer une communication ***"n'importe où et n'importe quand"*** vu leurs caractéristiques d'auto-organisation et le déploiement rapide et économique. Cependant, cette classe souffre de plusieurs types d'attaques qui perturbent et handicapent son fonctionnement tel qu'ils deviennent incapables de découvrir des routes sécurisées pour pouvoir transmettre les données d'une manière fiable et confidentielle.

Dans ce projet de fin d'étude, nous nous sommes intéressés au problème de la sécurité dans les réseaux mobiles et spécialement des réseaux mobiles ad hoc. Ce problème qui n'a jamais cessé de susciter des préoccupations du fait qu'ils sont exposés à des menaces supplémentaires par rapport aux réseaux filaires. En général, ces menaces viennent du fait que les communications sans fil sont transmises par ondes radios et peuvent être écoutées par des personnes non autorisées.

Nous avons étudié l'une des attaques qui touche le protocole de routage réactif AODV : l'attaque ***trou de noir*** ou ***Blackhole***. Nous avons aussi développé un nouveau protocole de routage qui permet de simuler cette attaque qui perturbe le bon fonctionnement des réseaux ad hoc.

En fin nous avons proposé une solution qui permet à ces protocoles de résister contre cette attaque. Cette solution consiste à identifier l'attaquant puis l'isoler du réseau.

Perspectives :

Dans la continuité du travail présenté, nous pourrions approfondir notre étude afin d'implémenter la solution présenté et proposé d'autre solutions pour contrecarrer ces types d'attaques.

Bibliographie

Bibliographie

[1] Jean Carle, Olivier FRAUZAC, Florent NOLOT , LIFT- CRESTIC.

[2] ALAGHA Khaldom, Guillaune Vivier , Reseaux mobiles & reseaux sans fils,Eyrolles, Septembre 2001.

[3] Di GALLO Fedéric, WIFI l'essentiel qu'il faut savoir, 2003.

[4] C. Marabet , these doctorat en science, Amelioration du service A lternative Best Effort(ABE and WABE) pour le transport de flux sur les réseaux ad hoc,2004.

[5] Frédiric Guinand- Brice Onfroy, 76058, le Havre, France,

Frediric- guinaud@ univ-lehavre.fr.

onfroy-brice@g mail.com

[6] Guilhen Paroux, une plate pour les échanges pair à pair sur les réseaux mobiles ad hoc, France telécom R & D.

[7] Cyber Networks, livre Blanc Sécurité des systemes sans fils, version 2.0, 2004.

[8] Jim Geier, les reseaux sans fils first-Step, PEARSON.

[9] T.Lemlouma, projet de recherche le routage dans les easeaux ad hoc, 2000.

[10] S.Sivavakeesar, G.Pavlon,Damien Masson,Koffi N guetta, reseaux ad hoc : etude bibliographique,2005.

[11] Laure GONNORD , Y ves.GERARD ,Securité dans les réseaux ad hoc.

[12] DUTREIGE Janathan et TIMMER MANS Thomas, Reseau ad hoc, 2006.

[13] Bouam, Jalel Ben-Othman, Protocole de sécurisation des données à base de routage dans les réseaux ad hoc, laboratoire CNRS- Pri SM

Bibliographie

[14] Reseaux ad hoc mobiles : acces au medium, routage et qualité de service, DEA. IFA, université de marne- la – Vallée.

http : //www.lgm.univ.mlv.fr

http ://www.quill.net.

[15] IUP.GMI.D'AVIGNON, BABETNET Florent, Sécurité dans les réseaux ad hoc mobiles, cahier de charges.

[16] Sedrati Maamar, Aouragh Lamia, Belami Azeddine, Etude des performances des protocoles de routage dans les réseaux mobiles ad hoc, Battna, 2007.

[17] Adolf Abdallah, conseption d' un protocole de routage sécurisé à l'aide de proceseur sécurisés embarqués pour les réseaux ad hoc, Université de Limoges, 2006.

[18] Jean Carle, Oliviers FLAUZAC, Réseaux Hétérogenes intelligents pour situation de crise, Rapport sur l'etat de l'art des algorithmes de routage, LIFL Cre STIC, LIFL CReSTIC, 2008.

[19] V.Kumar,Fr Carrez, J-Riganati, Technologie clés pour les réseaux radio ad hoc,Révue des télécommunication d'Alcatel, 3eme trimestre, 2001.

[20] Fanilo Harivélo, Pascal Anelli, IREMIA, Equité pour réseau ad hoc WiFi, univérsité de la Réunion , BP 7151, 15 Avenue R.Cassin, France.

Email : Fanilo. Harivelo@univ_reunion.fr

: Pascal. Anelli@univ_reunion.fr

[21] Frédériques Laforest, Frédéric le Mouel, Système d'information péevasifs, Master recherche.

fréderique. laforest@insa-lyon.fr

Bibliographie

http:// liris.cnrs.fr/frederique.laforest.

[22] E. Fleury,Plan CongDuc, S.Frenot, Protocole de télécommunication- Evolution de l'internet, INSA de Lyon – DEA Disic

Eric.Fleury@iniria.fr

Stéphan.Frénot@insa-lyon.fr

[23] Anelise Munaretto Fonseca, Les réseaux ad hoc

Anelise.munaretto@lip6.fr

anelise@lri.fr

[24] E. Fleury, S. Fréot, Protocoles de télécommunication- Evolution de l'internet-, INSA de Lyon- DEADISIC.

EricFleury.Stéphane.Frenot@insa-lyon.fr

[25] H.Labiod, Reseaux ad hoc mobiles et réseaux de capteurs sans fils,collection IC2, Lavoisier.

[26] Isabelle Guérin Lassous, Réseaux ad hoc MIF 11.

Isabelle Guerin.Lassous@ens-Lyon.fr

http ://perso.ens-Lyon.fr/isabelle.guerin-lassous

[27] Alexandre Pocquet, Les attaques sur le routage dans les réseaux ad hoc, CREC Saint-cyr-Laboratoire MACCLA IRISA- Equipe ARMOR.

alexandrepocquet@stc.fr

[28] Johnson, D, Hu, Y and Maltz, D, The Dynamic Source Routing (DSR) for mobile Ad hoc network for IPV4, IETF ? RFC 4728, 2007.

Bibliographie

[29] Clausen.T, and Jacquet. P, « Optimized Link State Routing Protocol (OLSR)», IETF ? RFC 3626(2003).

[30] David Elorrieta, Protocole de routage pour l'interconnexion des réseaux ad hoc et UMTS, université libre de Bruxelles.

[31] C.Castelluccia and G.Montenegro « protecting AODV against impersonation Attaks », ACM SIGMONILE mobile comp and commun Rev.Archive, Vol 6,July 2002 PP 108-109.

[32] Allam. I , les modelles de cooperation dans dans les réseaux ad hoc, 2009.

[33] M.Mehdi, A.Anou, S.Zair, M.Bensebti and M.Djebari, La Sécurité dans les Réseaux Ad Hoc, 2007.

Mmehdi_m@hotmail.com**,** Anou@uReach.com**,** szair@hotmail.com, m_bensebti@hotmail.com and Djebarim@hotmail.com

[34] Julien Thomas, Détection de la malveillance et réactions dans les réseaux ad hoc Bibliographie, École Nationale Supérieure des Télécommunications , 31 Janvier 2007.

[35] Marine Minier , sécurité et réseau ad hoc.
marine.minier@insa-lyon.fr

[36] Jérôme LEBEGUE, Christophe BIDAN et Bernard JOUGA, Supélec Rennes – Equipe SSIR, les réseaux ad hoc : problémes de sécurité et sollution potentielles, 13 octobre 2005

[37] Hassiba-Asmaa ADNANE, la confiance dans le routage ad hoc : etude du protocole OLSR, le grade de docteur de l'université de Rennes, 2009.

[38] Adolf Abdallah, Conception d'un protocole de routage réactif sécurisé à l'aide de processeurs sécurisés embarqués pour les réseaux ad hoc, universite de Limoges, 2006.

[39] BERNARD TOURANCHEAU, les réseaux sans fil et les problémes de la sécurité,2009.

[40] Michel Riguidel, la securité des réseaux et des systémes.2006.

[41] YihChun Hu, Adrian Perrig, David B. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, Carnegie Mellon University.

Bibliographie

Email: yihchun@cs.cmu.edu
perrig@cmu.edu
dbj@cs.rice.edu

[42] JAVIER BONNY MOUNIR KRICHANE, Securing Ad Hoc Networks Using Ariadne, Swiss Institute of Technology (EPFL) Lausanne, Switzerland, March 29, 2004, javier.bonny | mounir.krichane @epfl.ch

[43] ADJIDO Idjiwa, BENAMARA Radhouane, BENZIMRA Rebecca, GIRAUD Laurent, Protocole de routage ad hoc sécurisé dans une architecture clusterisée, Université Pierre et Marie Curie (Paris VI) Paris, France.
{idjiwa.adjido, rebecca.benzimra, radhouane.benamara, laurent.giraud}@etu.upmc.fr.

[44] G Florin, S Natkin, LA SÉCURITÉ, CNAM- Cedric.

[45] Guibadj Rym Nesrine , Mehar Sara, SRS_AODV (Secure Routing Scheme for AODV), Ecole nationale Supérieure de formation en Informatique ESI , Alger, Algérie.
Email : g_nesrym@hotmail.com s.mehar123@gmail.com

[46] Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong, A New Routing Attack in Mobile Ad Hoc Networks, Department of Computing and Information Technology,
Fudan University, Shanghai, 200433, China,
Email:
Pyi_edu@yahoo.com.cn, zldai@guanghua.sh.cn, szhang@fudan.edu.cn,
ypzhong@fudan.edu.cn

[47] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, Department of Computer Science, IACC 258 North Dakota State University, Fargo, ND 58105.
Email: Huirong.fu@ndsu.nodak.edu

[48] Jarmo V. E. M¨ols¨a, CROSS-LAYER DESIGNS FOR MITIGATING RANGE ATTACKSIN AD HOC NETWORKS, Helsinki University of Technology P.O. Box 3000, FI-02015 HUT, Finland.

Bibliographie

Email: jarmo.molsa@tkk.fi

[49] Céline Burgod, Etude des vulnérabilités du protocole de routage OLSR, 26 septembre 2007.

[50] Jérôme LEBEGUE, Christophe BIDAN et Bernard JOUGZ, Supélec Renne – SSIR, avenue de la Boulais 35510 CESSION SEVIGNE.

[51] *Mr* Abdesselem BEGHRICHE, De la Sécurité à la E-Confiance basée Sur la Cryptographie à Seuil dans les Réseaux sans fil Ad hoc, *2008/2009*

[52] C_eline BURGOD , Contribution a la sécurisation du routage dans les reseaux ad hoc, le 12 octobre 2009.

[53]ALIOUANE Lynda *, BADACHE ** Nadjib* CERIST, L'Authentification dans les Réseaux Ad Hoc, ** LSI, USTHB, BP 32, EL-Alia, Bab-Ezzouar, 16111, Alger.
E-mail :{lyn_f35@yahoo.fr, badache@wissal.dz

[54] M. Mehdi, A. Anou, S.Zair, M.Bensebti and M.Djebari, La Sécurité dans les Réseaux Ad Hoc, Département électronique, Université de BLIDA, ALGERIE.
E-mail:
Mmehdi_m@hotmail.com
Anou@uReach.com
szair@hotmail.com
,m_bensebti@hotmail.com
Djebarim@hotmail.com

[55] ANDRIAMADY Miarisoa Faniry, TARIFICATION ET RÉSEAUX AD-HOC, Décembre 2003.

[56] Val_erie Gayraud1, Lout_ Nuaymi2, Francis Dupont2, Sylvain Gombault2, and Bruno Tharon2, la Securite dans les Reseaux Sans Fil Ad Hoc,
Thomson R&I, Security Lab,1, Avenue de Belle-Fontaine, 35551 Cesson Sevigne
E- mail : valerie.gayraud@thomson.net

Bibliographie

[57] E.M.Royer & C.K.Toh. "A review of current routing Protocols for ad hoc mobile wireless networks". IEEE personal communication magazine, Avril 1999.

[58] Nabil Tabbane, Sami Tabban, Ahmed Mehaoua, Simulation et mesure des performances du protocole de routage AODV,

University of Versailles St-Quentin-en-Yvelines– 45, av. des Etats-Unis 78035 Versailles– France

Email: Ahmed.Mehaoua@prism.uvsq.fr

Email: Nabil.Tabbane@supcom.rnu.tn

[59] C. E. Perkins, E. M. Royer, and S. R. Das, "Ad Hoc on Demand Distance Vector (AODV) Routing". URL: http://www.ietf.org/internet-drafts/draft-ietfmanet-aodv-11.txt, IETF Internet Draft, June 2002. (Work in progress).

[60] Thomas Noël , LA MOBIILIITE DANSS LESS RESSEAUX IP, Université Louis Pasteur de Strasbourg.

[61] Introduction au simulateur réseau NS2, Youssef BADDI (home) , Date de publication : 21/03/2011 , Dernière mise à jour : 21/03/2011.

[62] Introduction à l'utilisation de NS (Network Simulator), Pascal Anelli , Marceau Coupechoux, Eric Horlait, Naceur Malouch.

[63] NS-2: Principes de conception et d'utilisation , P. Anelli & E. Horlait,Version 1.3.

Annexe

Annexe

Annexe A: Exemple de scénario de mobilité

```
## This scenario file uses node index of 0 instead of 1.
# nodes: 50, pause: 600.00, max speed: 20.00  max x = 670.00, max y: 670.00
#
set god_ [God instance]
$node_(0) set X_ 252.959383262454
$node_(0) set Y_ 480.272299375307
$node_(0) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(0) 50
$node_(1) set X_ 447.033548437227
$node_(1) set Y_ 379.340645138333
$node_(1) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(1) 50
$node_(2) set X_ 129.469733929631
$node_(2) set Y_ 507.518401755946
$node_(2) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(2) 50
$node_(3) set X_ 574.845617050158
$node_(3) set Y_ 382.429117192086
$node_(3) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(3) 50
$node_(4) set X_ 317.790700854626
$node_(4) set Y_ 351.879165210758
$node_(4) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(4) 50
$node_(5) set X_ 91.769762053791
$node_(5) set Y_ 447.260435096250
$node_(5) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(5) 50
$node_(6) set X_ 189.397567002070
$node_(6) set Y_ 666.615379415942
$node_(6) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(6) 50
$node_(7) set X_ 159.689552011708
$node_(7) set Y_ 507.188267856695
$node_(7) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(7) 50
$node_(8) set X_ 348.494544350072
```

$node_(8) set Y_ 251.459314377492
$node_(8) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(8) 50
$node_(9) set X_ 284.448702676317
$node_(9) set Y_ 537.892111352142
$node_(9) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(9) 50
$node_(10) set X_ 248.074693516807
$node_(10) set Y_ 444.138255000018
$node_(10) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(10) 50
$node_(11) set X_ 375.080379244203
$node_(11) set Y_ 596.569237866879
$node_(11) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(11) 50
$node_(12) set X_ 25.597569100883
$node_(12) set Y_ 659.529081920520
$node_(12) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(12) 50
$node_(13) set X_ 464.461349254387
$node_(13) set Y_ 273.672262617690
$node_(13) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(13) 50
$node_(14) set X_ 433.667336643911
$node_(14) set Y_ 169.541728221962
$node_(14) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(14) 50
$node_(15) set X_ 200.241500207942
$node_(15) set Y_ 459.264905744794
$node_(15) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(15) 50
$node_(16) set X_ 159.070809865854
$node_(16) set Y_ 664.702849462329
$node_(16) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(16) 50
$node_(17) set X_ 62.937168085856
$node_(17) set Y_ 592.738146821758
$node_(17) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(17) 50
$node_(18) set X_ 164.244577407663
$node_(18) set Y_ 263.178668605791
$node_(18) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(18) 50
$node_(19) set X_ 382.003052289924
$node_(19) set Y_ 323.315387585511
$node_(19) set Z_ 0.000000000000
#$ns_ initial_node_pos $node_(19) 50
$node_(20) set X_ 257.881517791492
$node_(20) set Y_ 444.940220687773
$node_(20) set Z_ 0.000000000000

#$ns_ initial_node_pos $node_(20) 50
$node_(21) set X_ 246.053534130641
$node_(21) set Y_ 422.126095511148
$node_(21) set Z_ 0.000000000000
$node_(22) set X_ 38.118889016937
$node_(22) set Y_ 628.056586420566
$node_(22) set Z_ 0.000000000000
$node_(23) set X_ 75.441482820031
$node_(23) set Y_ 296.000406808428
$node_(23) set Z_ 0.000000000000
$node_(24) set X_ 402.996806831712
$node_(24) set Y_ 321.495016950673
$node_(24) set Z_ 0.000000000000
$node_(25) set X_ 48.126502042949
$node_(25) set Y_ 441.115695848648
$node_(25) set Z_ 0.000000000000
$node_(26) set X_ 279.551603094611
$node_(26) set Y_ 123.567984862980
$node_(26) set Z_ 0.000000000000
$node_(27) set X_ 67.116102692442
$node_(27) set Y_ 12.548409961688
$node_(27) set Z_ 0.000000000000
$node_(28) set X_ 445.063001813653
$node_(28) set Y_ 115.242604735391
$node_(28) set Z_ 0.000000000000
$node_(29) set X_ 453.664105810337
$node_(29) set Y_ 54.614604943629
$node_(29) set Z_ 0.000000000000
$node_(30) set X_ 238.810589910364
$node_(30) set Y_ 520.780208502779
$node_(30) set Z_ 0.000000000000
$node_(31) set X_ 67.163014905318
$node_(31) set Y_ 13.873591447389
$node_(31) set Z_ 0.000000000000
$node_(32) set X_ 636.022813550163
$node_(32) set Y_ 520.827120715654
$node_(32) set Z_ 0.000000000000
$node_(33) set X_ 68.488196391018
$node_(33) set Y_ 204.833403183899
$node_(33) set Z_ 0.000000000000
$node_(34) set X_ 371.607329253799
$node_(34) set Y_ 135.651211296336
$node_(34) set Z_ 0.000000000000
$node_(35) set X_ 218.706994631288
$node_(35) set Y_ 337.630142527334
$node_(35) set Z_ 0.000000000000
$node_(36) set X_ 656.478332323983
$node_(36) set Y_ 287.195191334300
$node_(36) set Z_ 0.000000000000
$node_(37) set X_ 542.463545711233

$node_(37) set Y_ 358.085661301154
$node_(37) set Z_ 0.000000000000
$node_(38) set X_ 422.846402630636
$node_(38) set Y_ 91.170540065894
$node_(38) set Z_ 0.000000000000
$node_(39) set X_ 25.715803551861
$node_(39) set Y_ 409.324734677992
$node_(39) set Z_ 0.000000000000
$node_(40) set X_ 378.365731400194
$node_(40) set Y_ 568.179349263094
$node_(40) set Z_ 0.000000000000
$node_(41) set X_ 97.410395702519
$node_(41) set Y_ 131.212134066196
$node_(41) set Z_ 0.000000000000
$node_(42) set X_ 659.349889328987
$node_(42) set Y_ 123.126199254379
$node_(42) set Z_ 0.000000000000
$node_(43) set X_ 540.536868744187
$node_(43) set Y_ 367.715620764547
$node_(43) set Z_ 0.000000000000
$node_(44) set X_ 21.305548240845
$node_(44) set Y_ 637.947264758699
$node_(44) set Z_ 0.000000000000
$node_(45) set X_ 498.927754830742
$node_(45) set Y_ 10.655437605198
$node_(45) set Z_ 0.000000000000
$node_(46) set X_ 91.073463736451
$node_(46) set Y_ 369.464623298302
$node_(46) set Z_ 0.000000000000
$node_(47) set X_ 378.371058369745
$node_(47) set Y_ 112.379012289290
$node_(47) set Z_ 0.000000000000
$node_(48) set X_ 337.411887780374
$node_(48) set Y_ 207.298812923860
$node_(48) set Z_ 0.000000000000
$node_(49) set X_ 123.034449894488
$node_(49) set Y_ 428.485351828819
$node_(49) set Z_ 0.000000000000

Annexe B : Exemple de scénario de trafic

 # 1 connecting to 2 at time 176.70898653413587
#
set udp_(0) [new Agent/UDP]
$ns_ attach-agent $node_(1) $udp_(0)
set null_(0) [new Agent/Null]
$ns_ attach-agent $node_(2) $null_(0)
set cbr_(0) [new Application/Traffic/CBR]
$cbr_(0) set packetSize_ 512
$cbr_(0) set interval_ 4.0

```
$cbr_(0) set random_ 1
$cbr_(0) set maxpkts_ 10000
$cbr_(0) attach-agent $udp_(0)
$ns_ connect $udp_(0) $null_(0)
$ns_ at 176.70898653413587 "$cbr_(0) start"
#
# 1 connecting to 3 at time 127.93667922166023
#
set udp_(1) [new Agent/UDP]
$ns_ attach-agent $node_(1) $udp_(1)
set null_(1) [new Agent/Null]
$ns_ attach-agent $node_(3) $null_(1)
set cbr_(1) [new Application/Traffic/CBR]
$cbr_(1) set packetSize_ 512
$cbr_(1) set interval_ 4.0
$cbr_(1) set random_ 1
$cbr_(1) set maxpkts_ 10000
$cbr_(1) attach-agent $udp_(1)
$ns_ connect $udp_(1) $null_(1)
$ns_ at 127.93667922166023 "$cbr_(1) start"
#
# 2 connecting to 3 at time 79.371595438277154
#
set udp_(2) [new Agent/UDP]
$ns_ attach-agent $node_(2) $udp_(2)
set null_(2) [new Agent/Null]
$ns_ attach-agent $node_(3) $null_(2)
set cbr_(2) [new Application/Traffic/CBR]
$cbr_(2) set packetSize_ 512
$cbr_(2) set interval_ 4.0
$cbr_(2) set random_ 1
$cbr_(2) set maxpkts_ 10000
$cbr_(2) attach-agent $udp_(2)
$ns_ connect $udp_(2) $null_(2)
$ns_ at 79.371595438277154 "$cbr_(2) start"
#
# 8 connecting to 9 at time 130.49074511532243
#
set udp_(3) [new Agent/UDP]
$ns_ attach-agent $node_(8) $udp_(3)
set null_(3) [new Agent/Null]
$ns_ attach-agent $node_(9) $null_(3)
set cbr_(3) [new Application/Traffic/CBR]
$cbr_(3) set packetSize_ 512
$cbr_(3) set interval_ 4.0
$cbr_(3) set random_ 1
$cbr_(3) set maxpkts_ 10000
$cbr_(3) attach-agent $udp_(3)
$ns_ connect $udp_(3) $null_(3)
$ns_ at 130.49074511532243 "$cbr_(3) start"
```

```
#
# 8 connecting to 10 at time 37.95315322370881
#
set udp_(4) [new Agent/UDP]
$ns_ attach-agent $node_(8) $udp_(4)
set null_(4) [new Agent/Null]
$ns_ attach-agent $node_(10) $null_(4)
set cbr_(4) [new Application/Traffic/CBR]
$cbr_(4) set packetSize_ 512
$cbr_(4) set interval_ 4.0
$cbr_(4) set random_ 1
$cbr_(4) set maxpkts_ 10000
$cbr_(4) attach-agent $udp_(4)
$ns_ connect $udp_(4) $null_(4)
$ns_ at 37.95315322370881 "$cbr_(4) start"
#
# 9 connecting to 10 at time 127.20229852348672
#
set udp_(5) [new Agent/UDP]
$ns_ attach-agent $node_(9) $udp_(5)
set null_(5) [new Agent/Null]
$ns_ attach-agent $node_(10) $null_(5)
set cbr_(5) [new Application/Traffic/CBR]
$cbr_(5) set packetSize_ 512
$cbr_(5) set interval_ 4.0
$cbr_(5) set random_ 1
$cbr_(5) set maxpkts_ 10000
$cbr_(5) attach-agent $udp_(5)
$ns_ connect $udp_(5) $null_(5)
$ns_ at 127.20229852348672 "$cbr_(5) start"
#
# 9 connecting to 11 at time 29.031284241486009
#
set udp_(6) [new Agent/UDP]
$ns_ attach-agent $node_(9) $udp_(6)
set null_(6) [new Agent/Null]
$ns_ attach-agent $node_(11) $null_(6)
set cbr_(6) [new Application/Traffic/CBR]
$cbr_(6) set packetSize_ 512
$cbr_(6) set interval_ 4.0
$cbr_(6) set random_ 1
$cbr_(6) set maxpkts_ 10000
$cbr_(6) attach-agent $udp_(6)
$ns_ connect $udp_(6) $null_(6)
$ns_ at 29.031284241486009 "$cbr_(6) start"
#
# 10 connecting to 11 at time 144.90353608732275
#
set udp_(7) [new Agent/UDP]
$ns_ attach-agent $node_(10) $udp_(7)
```

```
set null_(7) [new Agent/Null]
$ns_ attach-agent $node_(11) $null_(7)
set cbr_(7) [new Application/Traffic/CBR]
$cbr_(7) set packetSize_ 512
$cbr_(7) set interval_ 4.0
$cbr_(7) set random_ 1
$cbr_(7) set maxpkts_ 10000
$cbr_(7) attach-agent $udp_(7)
$ns_ connect $udp_(7) $null_(7)
$ns_ at 144.90353608732275 "$cbr_(7) start"
#
# 11 connecting to 12 at time 117.24698354361905
#
set udp_(8) [new Agent/UDP]
$ns_ attach-agent $node_(11) $udp_(8)
set null_(8) [new Agent/Null]
$ns_ attach-agent $node_(12) $null_(8)
set cbr_(8) [new Application/Traffic/CBR]
$cbr_(8) set packetSize_ 512
$cbr_(8) set interval_ 4.0
$cbr_(8) set random_ 1
$cbr_(8) set maxpkts_ 10000
$cbr_(8) attach-agent $udp_(8)
$ns_ connect $udp_(8) $null_(8)
$ns_ at 117.24698354361905 "$cbr_(8) start"
#
# 11 connecting to 13 at time 110.05241760520842
#
set udp_(9) [new Agent/UDP]
$ns_ attach-agent $node_(11) $udp_(9)
set null_(9) [new Agent/Null]
$ns_ attach-agent $node_(13) $null_(9)
set cbr_(9) [new Application/Traffic/CBR]
$cbr_(9) set packetSize_ 512
$cbr_(9) set interval_ 4.0
$cbr_(9) set random_ 1
$cbr_(9) set maxpkts_ 10000
$cbr_(9) attach-agent $udp_(9)
$ns_ connect $udp_(9) $null_(9)
$ns_ at 110.05241760520842 "$cbr_(9) start"
#
#Total sources/connections: 6/10
#
```

Annexe C: simblackhole.tcl

```
# ======================================================================
#                         Define options
# ======================================================================

set val(chan)         Channel/WirelessChannel              ;#Channel Type
set val(prop)         Propagation/TwoRayGround             ;# radio-propagation
model
set val(netif)        Phy/WirelessPhy                      ;# network interface type
set val(mac)          Mac/802_11                           ;# MAC type
set val(ifq)          Queue/DropTail/PriQueue              ;# interface queue type
set val(ll)           LL                                   ;# link layer type
set val(ant)          Antenna/OmniAntenna                  ;# antenna model
set val(ifqlen)       150                                  ;# max packet in ifq
set val(nn)           50                                   ;# total number of mobilenodes
set val(nnaodv)       49                                   ;# number of AODV mobilenodes
set val(rp)           aodv                                 ;# routing protocol
set val(x)            670                                  ;# X dimension of topography
set val(y)            670                                  ;# Y dimension of topography
set val(cstop)        451                                  ;# time of connections end
set val(stop)         900                                  ;# time of simulation end
set val(cp)           "scen-670x670-50-600-20-1.tcl"       ;#Connection Pattern
set val(cc)           "connection cbr-50-10-4-512.tcl"     ;#CBR Connections

# ======================================================================
# ======================================================================

# Initialize Global Variables
set ns_     [new Simulator]
```

```
# création des fichiers traces
$ns_ use-newtrace
set tracefd [open sim1forBlackHole.tr w]
$ns_ trace-all $tracefd

# création des fichiers traces pour nam
set namtrace  [open sim1forBlackHole.nam w]
$ns_ namtrace-all-wireless $namtrace $val(x) $val(y)

# set up topography object
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)

# Create God
create-god $val(nn)

# Create channel #1 and #2
set chan_1_ [new $val(chan)]
set chan_2_ [new $val(chan)]

#############################################################################
#############################################################################

# configure node, please note the change below.
$ns_ node-config   -adhocRouting $val(rp) \
                   -llType $val(ll) \
                   -macType $val(mac) \
                    -ifqType $val(ifq) \
                   -ifqLen $val(ifqlen) \
                   -antType $val(ant) \
```

```
                -propType $val(prop) \
                -phyType $val(netif) \
                -topoInstance $topo \
               -agentTrace ON \
               -routerTrace ON \
               -macTrace ON \
               -movementTrace ON \
                -channel $chan_1_

        # Creating mobile AODV nodes for simulation
        puts "Creating nodes..."
        for {set i 0} {$i < $val(nnaodv)} {incr i} {
        set node_($i) [$ns_ node]
        $node_($i) random-motion 0      ;#disable random motion
        }

        # Creating Black Hole nodes for simulation

        $ns_ node-config            -adhocRouting blackholeAODV
        for {set i $val(nnaodv)} {$i < $val(nn)} {incr i} {
        set node_($i) [$ns_ node]
        $node_($i) random-motion 0       ;#disable random motion
        $ns_ at 0.01 "$node_($i) label \"blackhole node\""
        }

        # Adding connection pattern which is created using setdest, parameters shown
below

        # ./setdest -n 20 -p 1.0 -M 20.0 -t 500 -x 750 -y 750 > scen1forAODV-n20-t500-
x750-y750
```

```
puts "Loading random connection pattern..."
set god_ [God instance]
source $val(cp)
# CBR Connections generated by cbrgen
source $val(cc)
# Define initial node position
for {set i 0} {$i < $val(nn) } {incr i} {
$ns_ initial_node_pos $node_($i) 30
}
# CBR connections stops
for {set i 0} {$i < 9 } {incr i} {
$ns_ at $val(cstop) "$cbr_($i) stop"
}
# Tell all nodes when the simulation ends
for {set i 0} {$i < $val(nn) } {incr i} {
$ns_ at $val(stop).000000001 "$node_($i) reset";
}

# Ending nam and simulation
$ns_ at $val(stop) "finish"
$ns_ at $val(stop).0 "$ns_ trace-annotate \"Simulation has ended\""
$ns_ at $val(stop).00000001 "puts \"NS EXITING...\" ; $ns_ halt"

**********PROCEDURE FINISH**********

proc finish {} {
global ns_ tracefd namtrace
$ns_ flush-trace
close $tracefd
```

```
close $namtrace
exec nam sim1forBlackHole.nam &
exit 0
}
puts "Starting Simulation..."
$ns_ run
```