الجمـهورية الجزائرية الديمقراطية الشعبيـة
وزارة التعليم العالي والبحث العلمي
جـامعـة سعـيـدة د. مـولاي الطـاهـر
كـلـيـة العلوم
قسم: الإعلام الآلي

Mémoire de Master

Spécialité : sécurité Informatique et cryptographie

Thème
Sécurité de protocole de routage Adhoc AODV

Présenté par :

Boulghit Yassine

Boucif Abdelkader

Dirigé par :

Mr. Henoune Mohammed Mokhtar

Promotion 2023 - 2024

ملخص

الشبكة اللاسلكية المخصصة هي عبارة عن مجموعة من العقد المتنقلة التي تشكل شبكة مؤقتة ذات هيكل متغير وتعمل بدون محطة أساسية وبدون إدارة مركزية، وتكون الاتصالات متعددة القفزات ممكنة هناك بفضل بروتوكولات توجيه محددة. تعد المحاكاة أداة أساسية لدراسة أداء بروتوكولات التوجيه في هذه الشبكات

سنساهم في هذه الدراسة في تأمين بروتوكول التوجيه AODV عن طريق المحاكاة ضمن OMNET ++ وINET Framework لحماية طوبولوجيا البروتوكول وتأمين المسارات بين العقد اقترحنا استخدام SAODV الذي يضمن حماية البيانات المتبادلة عبر الشبكة.

الكلمات المفتاحية : AODV, OMNET,الأمن, SAODV

Abstract

An ad-hoc Wireless network is a collection of mobile nodes forming a temporary network with variable topology and operating without a base station and without centralized administration, multi-hop communications are possible there thanks to specific routing protocols. Simulation is an essential tool for studying the performance of routing protocols in these networks.

In this study we will contribute to securing the AODV routing protocol by simulation under OMNET ++ and the INET Framework; To protect the topology of the protocol and secure the paths between the nodes we have suggested using SAODV that ensures the protection of data exchanged over the network.

Keywords : AODV, OMNET, Security, SAODV

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, les communications multi sauts y sont possibles grâce à des protocoles de routage spécifiques. La simulation est un outil indispensable pour étudier la performance des protocoles de routage dans ces réseaux.

Dans cette étude nous contribuerons à sécuriser le protocole de routage AODV par la simulation sous OMNET ++ et du INE Framework, Pour protéger la topologie du protocole et sécuriser les chemins entre les nœuds nous avons suggéré d'utiliser le protocole de routage SAODV qui permet d'assurer la protection des données échangées sur le réseau.

Mots clés : AODV, OMNET, Sécurité, SAODV

DÉDICACES

JE DÉDIE CE TRAVAIL À :

MA MÈRE, MON PÈRE, MES FRÈRES,

ET ENCADREUR : MESSIEURS

HENOUNE MOHAMED MOKHTAR ET

TOUS MES PROFESSEURS ET COLLÈGUES DE PROMOTION.

« YASSINE »

ALA MÉMOIRE DE MA GRAND-MÈRE

ALA PLUS BELLE CRÉATURE QUE DIEU A CRÉÉE SUR TERRE,

ÀCET SOURCE DE TENDRESSE, DE PATIENCE ET DE GÉNÉROSITÉ,

ÀMA MÈRE !ET PÈRE

AMON GRAND FRÈRE

ÀTOUS MES FRÈRES ET SŒURS, AINSI QUE LEURS ENFANTS

ET ENCADREUR : HENOUNE MOHAMED MOKHTAR

ÀTOUS MES AMIS ET COLLÈGUES

ATOUS LES ÉTUDIANTS DE LA PROMOTION

A TOUS CEUX QUI, PAR UN MOT, M'ONT DONNÉ LA FORCE DE CONTINUER

« ABDELKADER »

Remerciements

Nous tenons à exprimer notre profonde gratitude à notre promoteur, Monsieur « Henoune Mohammed Mokhtar »

Pour nous avoir encadrés durant cette année, ainsi que pour ses conseils judicieux.

Nos remerciements vont également aux membres du jury pour l'honneur qu'ils nous

Font en acceptant d'examiner et de juger notre travail.
Nous remercions aussi tous ceux, et celles qui ont contribué de près ou de loin pour

L'accomplissement de ce modeste travail.

Table des matières

Table des figures

Liste des tableaux

Glossaire:

MANET: Mobile Ad hoc Networks.

OSI: Open Systems Interconnection.

TTL: Time to Live.

DSR: Dynamic Source Routing.

DSDV: Destination-Sequenced Distance Vector.

AODV: Ad-hoc On Demand Distance Vector.

SAODV: Secure Ad hoc On-Demande Distance Victor.

TORA: Temporally-Ordered Routing Algorithm.

OLSR: Optimized Link State Routing Protocol.

RREQ: Route Request.

RREP: Route Reply.

RERR: Route Error.

RREP-ACK: Route Reply Ack knowledge.

OMNeT: Objective Modular Network Test-bed.

Introduction générale :

Le développement technologique qu'a vue le monde d'aujourd'hui à toucher tous les domaines, particulièrement le secteur de la communication qui connaît une évolution considérable avec l'apparition de la technologie sans fil.

La technologie sans fil permet l'établissement d'une communication sans fil dans des environnements mobiles qui offrent une grande flexibilité d'emploi. En particulier, ils permettent la mise en réseau des sites dont le câblage serait trop onéreux à réaliser, voire même impossible. Les réseaux mobiles sans fil, peuvent être classés en deux classes : les réseaux avec infrastructure ou cellulaire et les réseaux sans infrastructure (Adhoc). Plusieurs systèmes utilisent le modèle cellulaire et connaissent un très fort épanouissement à l'heure actuelle, mais requièrent une importante infrastructure matérielle fix.

Un réseau ad hoc peut être défini comme une collection d'entités mobiles interconnectées par une technologie sans fil formant un réseau temporaire sans l'aide de toute administration centralisée ou de tout support fixe. Aucune supposition ou limitation n'est faite sur la taille du réseau ou sur la mobilité de ses nœuds, cela veut dire qu'il est possible que le réseau ait une taille très énorme.

Dans un réseau ad hoc les sites mobiles doivent former un tout pour réaliser les tâches facilement, dont les autres réseaux ne les permettent pas. Les applications des réseaux Ad hoc sont nombreuses, on cite l'exemple classique de leur application dans le domaine militaire et les autres applications de tactique comme les opérations de secours et les missions d'exploration. Du fait que la propagation de la portée des ondes radio des hôtes soit limité, et afin que le réseau Ad hoc reste connecté, (c'est à dire tout unité mobile peut atteindre toutes autre), Il se peut que l'hôte destination ne soit pas dans la portée de communication de l'hôte source, ce qui nécessite l'emploi d'un routage saut par saut pour acheminer les paquets de messages à la bonne destination. [1]

Ce mécanisme d'acheminement de paquet ou le routage, consiste à utiliser des protocoles de routage tel que le protocole réactif AODV capables d'assurer la connexion entre n'importe quelle paire de nœuds appartenant au réseau à tout moment. Ce protocole doit prendre en considération les changements topologiques ainsi que les autres caractéristiques du réseau ad hoc (bande passante, nombre de liens, ressources du réseau etc.).

Le protocole de routage AODV n'assure pas la sécurité de routage contre les différentes attaques, donc d'autres mécanismes doivent être mis en œuvre afin d'améliorer sécurité de routage et la disponibilité de réseau. Parmi les solutions proposées on peut citer ARAN, SAODV. Ce dernier est étudié dans notre mémoire. Pour cela on a subdivisé le travail en Cinque chapitres.

CHAPITRE I

Généralités sur les réseaux ad hoc

I.1 LES RESEAUX AD HOC:

I.1.1 Définition :

Les réseaux mobiles Ad Hoc appelés généralement MANET (Mobile Ad Hoc Network) sont devenus de plus en plus populaires ces dernières années, en raison de l'importance des domaines d'application des réseaux Ad Hoc. Ils sont un nouveau type de réseaux basés sur la technologie sans fil. Les réseaux Ad Hoc sont des systèmes autonomes qui communiquent avec des ondes radios qui se propagent entre les différents nœuds mobiles sans infrastructure. Il n'y a aucune limitation de taille dans un réseau Ad Hoc, il peut contenir des dizaines ou des milliers de nœuds. La communication entre les nœuds de réseaux MANET nécessite des protocoles de routage à cause de topologie dynamique et l'absence d'administration centrale [2].

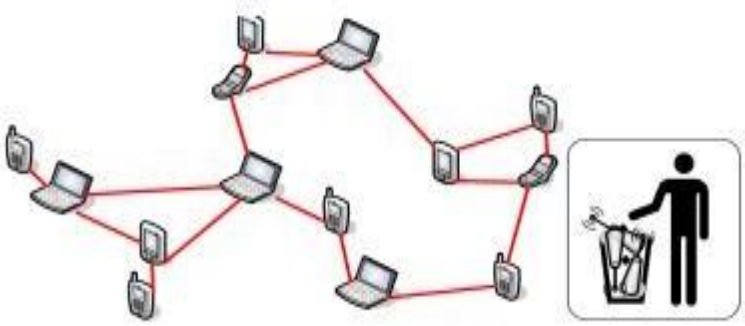

Figure I.1 : Réseau sans fil sans infrastructure (Ad Hoc).

I.1.2 Caractéristique des réseaux Ad Hoc :

Les réseaux mobiles Ad Hoc sont caractérisés par ce qui suit :

- **Sans infrastructure :**

Les réseaux ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructures préexistantes et de tout genre d'administration centralisée. Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue [3].

- **Mobilité et topologie dynamique :** Les unités mobiles du réseau se déplacent d'une façon libre et arbitraire, par conséquent la topologie du réseau peut changer à des instants imprévisibles, d'une manière rapide et aléatoire. Les liens de la topologie peuvent être mono ou bidirectionnels [4].

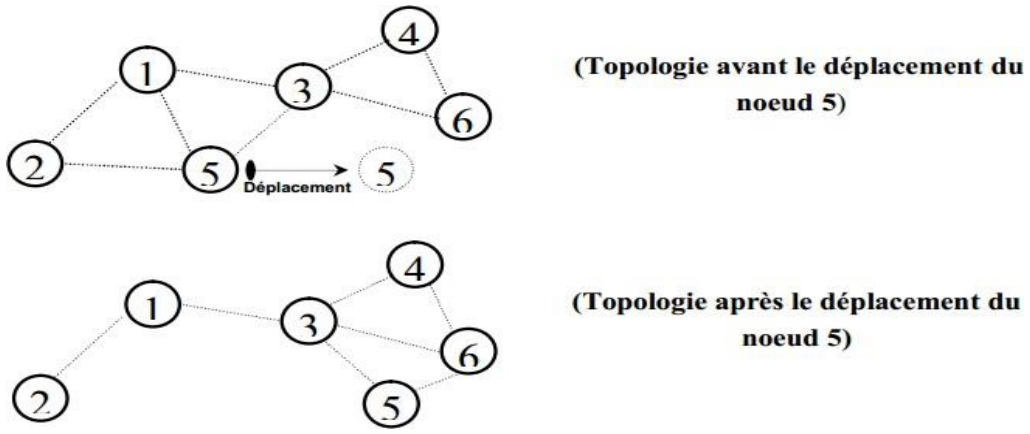

Figure I.2 : Changement de la topologie d'un réseau Ad Hoc

• Contraintes de ressources :

Les nœuds disposent de ressources d'alimentation et de capacités de calcul et de stockage limités, d'où une gestion efficace est nécessaire pour avoir une longue durée de vie, de routage devrait être maintenu à un minimum [4].

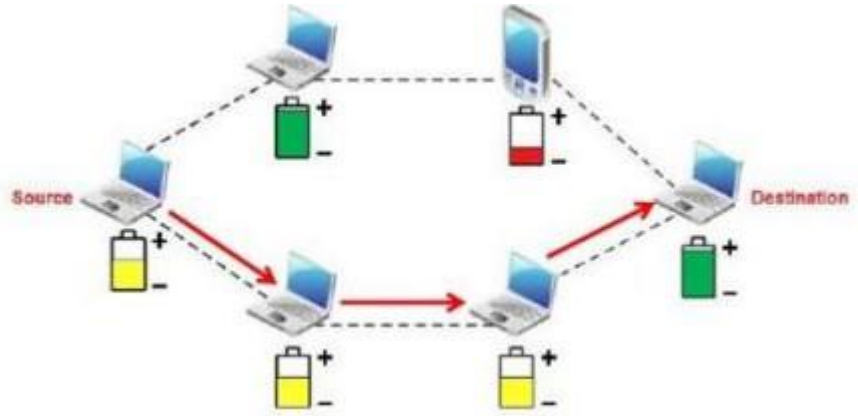

Figure I.3 : durée de vie de batterie des nœuds

• Bande passante limitée :

La communication dans les réseaux Ad Hoc se base sur le partage d'un medium sans fil (onde radio). Ce qui induit une bande passante modeste, pour chaque hôte du réseau [4].

• **Interférences :** Dans un réseau Ad Hoc, les liens radio ne sont pas isolés. Ceci peut impliquer que deux transmissions simultanées sur une même fréquence ou sur fréquences proches peuvent interférer et provoquer des erreurs de transmission. Un grand nombre de paquets peuvent être endommagés et perdus lors du transfert [4].

- **Sécurité physique limitée :**

Les terminaux ne sont pas protégés, ils sont menacés de vol ou de destruction, donc les nœuds d'un réseau Ad Hoc n'ont pas la même protection physique que les nœuds d'un réseau filaire. En effet, ceux d'un réseau Ad Hoc sont censés être mobiles et parfois complètement autonomes, c'est notamment le cas des réseaux de capteurs où les nœuds sont souvent lâchés, dans un environnement particulier et parfois hostile, sans aucune surveillance particulière [4].

- **Sécurité et Vulnérabilité :**

Les réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité que les réseaux filaires. Pour les réseaux Ad Hoc, le principal problème ne se situe pas tant au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau [4].

I.1.3 les avantages des réseaux ad Hoc :

- **Pas de câblages :** L'une des caractéristiques des réseaux Ad Hoc est l'absence d'un câblage, en effet, on élimine toutes les connexions filaires et on les remplace par des connexions radio [5][4].

- **Déploiement facile :** L'absence du câblage donne plus de souplesse et permet de déployer un réseau Ad Hoc facilement et rapidement, cette facilité peut être justifiée par l'absence d'une infrastructure préexistante permettant ainsi d'économiser tout le temps de déploiement et d'installation du matériel nécessaire [5][4].

- **Mobilité permise** : Comme l'indique leurs noms et à l'image des réseaux sans fils avec infrastructure, les réseaux mobiles Ad Hoc permettent une certaine mobilité à leurs nœud set de ce fait, ces derniers peuvent se déplacer librement à condition de ne pas s'éloigner trop les uns des autres pour garder leur connectivité [5][4]

- **Coût :** Le déploiement d'un réseau Ad Hoc ne nécessite pas d'installer des stations de base.

Les mobiles sont les seules entités physiques nécessaires pour se déployer [6][4].

I.1.4 Les inconvénient des réseaux ad Hoc :

● **Topologie non prédictible :** L'activité permanant et les déplacements fréquents des nœuds d'un réseau Ad Hoc rendent son étude très difficile. La raison est bien connue le changement rapide de sa topologie du au déplacement des nœuds [6].

● **Capacités limitées :** Dans un tel réseau Ad Hoc la configuration de la portée de communication des nœuds est importante. En effet il faut qu'elle soit suffisante pour assurer la connectivité du réseau, mais plus on accroit la portée des mobiles plus les communications 7 demandent de l'énergie.

Il faut donc trouver un compromis entre la connectivité du réseau et la consommation énergétique [7].

● **Taux d'erreur important :** Les risques de collision augmente avec le nombre de nœud qui partagent le même médium par conséquent plus la portée augmente plus le risque de collision n'est important [7].

● **Sécurité :** Un autre choix des réseaux Ad Hoc et qui attire la curiosité des chercheurs et des spécialistes de ce domaine est la notion de sécurité un réseau Ad Hoc tel que définit précédemment ne permet pas d'assurer la confidentialité de l'information échanger entre les nœuds contrairement en réseau filaire [8].

I.1.5 Domaines d'applications :

● Les réseaux Ad Hoc sont utilisés dans toutes les applications où le déploiement d'une architecture centralisée est contraignant, voire impossible. En effet, la robustesse, le coût réduit et le déploiement rapide qu'ils présentent leur confèrent un accès à une large palette d'applications dont :

● **Les applications militaires :** Les réseaux Ad Hoc ont été utilisés la première fois par l'armée. En effet ce type de réseaux est la solution idéale pour maintenir une communication sur un champ de bataille entre les différentes troupes unités d'une armée [9][10].

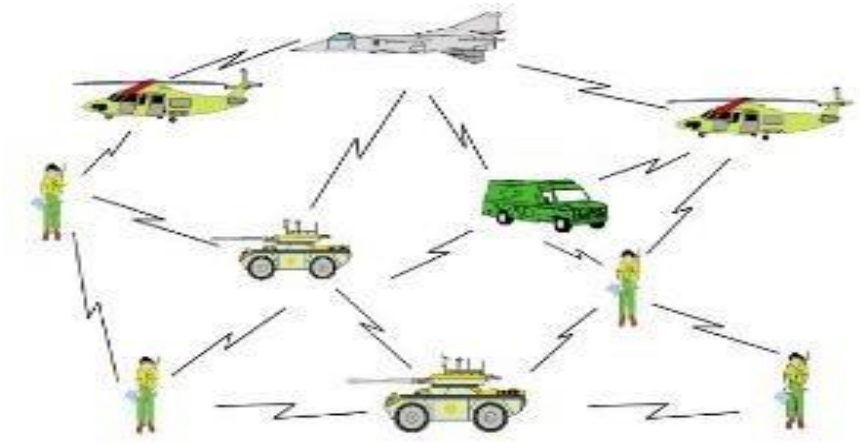

Figure I.4 : Les applications militaires de réseau Ad Hoc

- **Les opérations de secours :** Dans les zones touchées par les catastrophes naturelles (cyclone, séisme, etc.), le déploiement d'un réseau Ad Hoc est indispensable pour permettre eux unités de secours de communiquer [9][10].

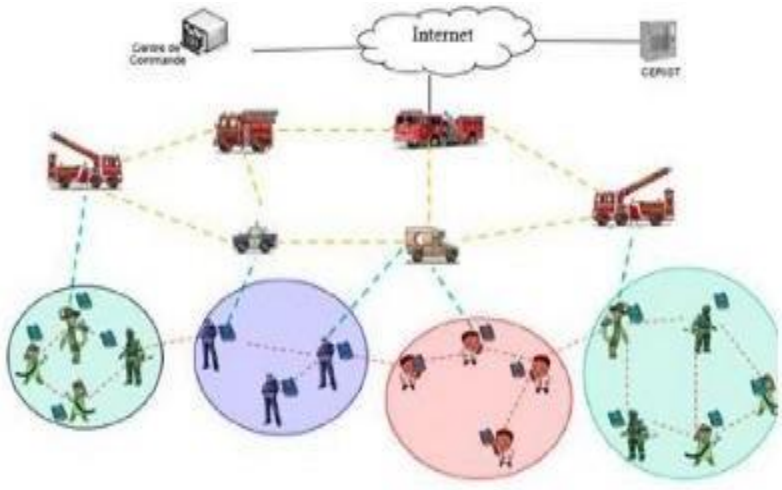

Figure I.5 : applications de secours des réseaux Ad Hoc.

- **L'utilisation à des fins éducatives** : Le déploiement d'un réseau Ad Hoc lors d'une conférence ou d'une séance de cours est très judicieux car cela permet aux chercheurs et étudiants de partager des ressources (fichiers, accès à internet…etc.) et de communiquer sans avoir besoin d'une quelconque infrastructure [11].
- **Applications industrielles :** Des scénarios plus complexes dans le domaine industriel appelés réseaux de capteurs peuvent former un MANET pour s'adapter à différents environnements. Un exemple d'une telle application est la formation d'un MANET pour la surveillance médicale, la détection des Feux de forêt, la surveillance des volcans…etc. [9].
- **Mise en œuvre des réseaux véhiculaires :** Sur un réseau routier les véhicules peuvent avoir besoin de communiquer entre eux ou avec leur environnement afin de partager des informations dans le but de gérer et réguler le trafic routier. Les réseaux Ad Hoc sont alors la solution idéale [9].

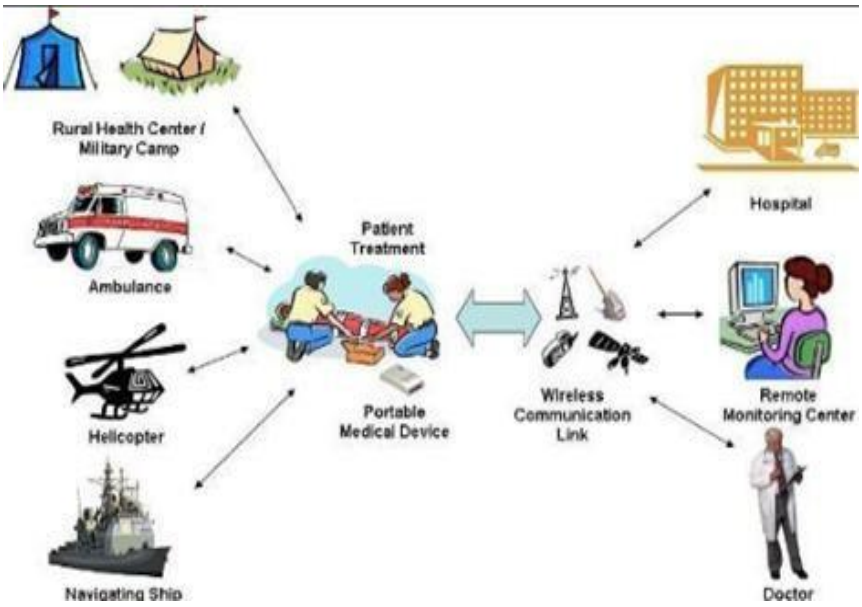

Figure I.6 : domaine d'application des réseaux Ad Hoc

I.2 LE ROUTAGE :

I.2.1 DEFINITION :

Le routage est une m´méthode d'acheminement des informations vers la bonne destination à travers un réseau de connexion donnée, il consiste à assurer une stratégie qui garantit, à n'importe quel moment, un établissement de routes qui soient correctes et efficaces entre n'importe quelle paire de nœuds appartenant au réseau, ce qui assure l'échange des messages d'une manière continue [12]

I.2.2 LE ROUTAGE DANS LES MANETS :

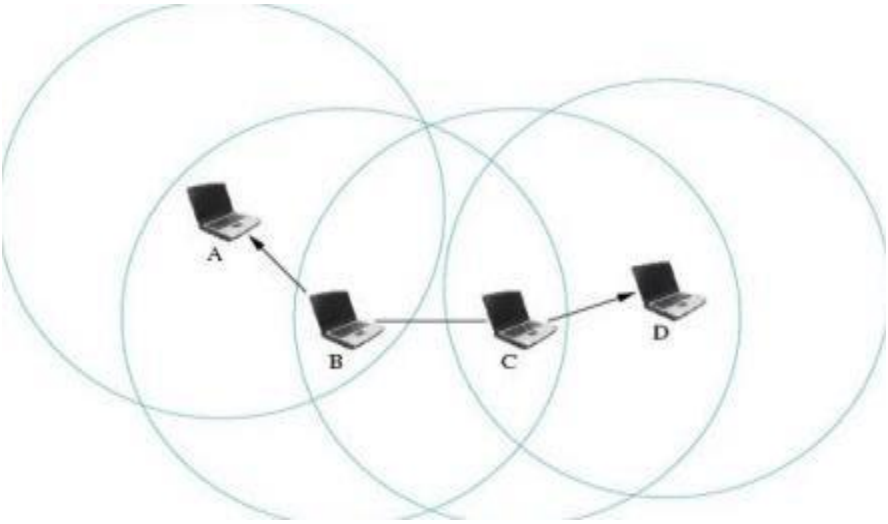

Figure I.7 : Le chemin utilisé dans le routage entre la source et la destination.

Le routage joue un rôle très important dans les MANET puisque tous les services supportés, unicast ou multicast, se basent sur des communications multi-sauts pour l'acheminement des données. Pour réaliser les échanges, les protocoles de routage utilisent des informations locales, sur le voisinage immédiat, ou globales, concernant tout le réseau, pour déterminer les nœuds qui participent à l'acheminement des données de communications, les protocoles de routage peuvent être séparés en Proactif, Réactif et Hybride [13].

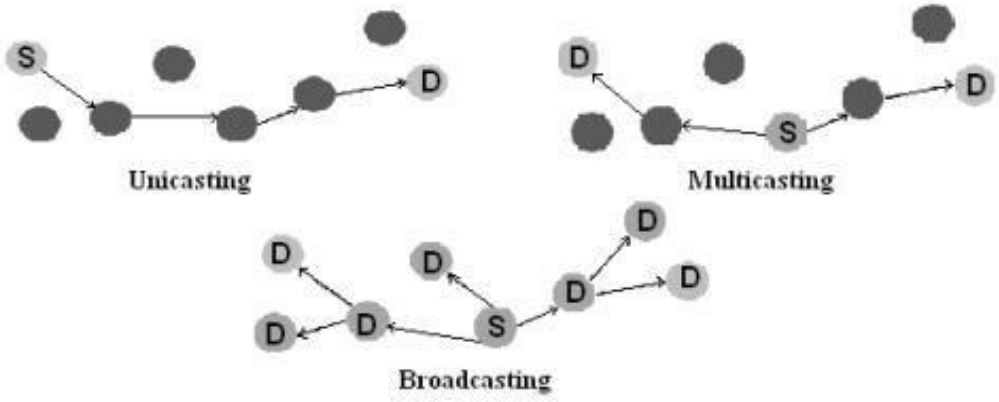

Figure I.8 : Illustration du routage unicast, multicast et broadcast

L'objectif principal des protocoles de routage est l'établissement et la maintenance des chemins, pour que les données soient correctement délivrées dans le réseau [14]. La conception des protocoles de routage pour les MANETS est loin d'être un problème simple. Des nouvelles approches de routage sont nécessaires pour effectuer un routage de données sûr et efficace. L'instabilité du médium de communication sans fil, la limitation d'énergie et de la bande passante, ainsi que la mobilité des nœuds introduisent plus de difficulté et de complexité à la conception des protocoles de routage pour les MANETS. Nous expliquerons, dans la section suivante, les propriétés requises pour les protocoles de routage dans les MANETS.

I.2.3 Propriétés requises pour les protocoles de routage dans les réseaux Ad Hoc :

Les propriétés que doivent vérifier les protocoles de routage pour les MANETS peuvent être résumés dans les points suivant :

- **Implémentation distribuée :** les MANETS sont des systèmes autonomes et auto organisés. Les protocoles de routage doivent être distribués en ne reposant plus sur une administration centralisée [5].
- **Optimisation de la consommation d'énergie :** dans un réseau Ad Hoc les nœuds ont besoin que leurs données soient acheminées par plusieurs nœuds intermédiaires pour qu'ils arrivent à leurs destinations. Une réduction en nombre de nœuds dégrade les performances du réseau comme elle peut aussi causer son partitionnement. Pour prolonger la durée de vie de chaque nœud et donc du réseau complet, la consommation d'énergie doit être prise en considération dans la conception des protocoles de routage [5].

- **Robustesse :** les pertes des paquets sont fréquentes dans les MANETS et elles sont dues aux collisions, à la mobilité des nœuds et à leurs durées de vie limitées. De ce fait, les protocoles de routage doivent être conçus pour continuer à fonctionner correctement même en présence des pertes [5].
- **Convergence rapide :** après la rupture d'un chemin, un protocole de routage doit rétablir un nouveau chemin le plutôt possible [5].
- **Élimination des boucles de routage :** comme les chemins sont maintenus de manière distribuée, la possibilité de création de boucles dans un chemin reste un problème sérieux. Le bouclage des paquets provoque une perte considérable en bande passante et en énergie. Les protocoles de routage doivent éviter/détecter la formation de boucles [5].
- **Support des liens unidirectionnels :** dans les MANETS, il y a certains facteurs comme l'hétérogénéité des capacités de transmission des nœuds qui engendrent des liens unidirectionnels. Un protocole de routage doit pouvoir fonctionner même en présence de liens unidirectionnels [5].
- **Sociabilité :** les protocoles de routage doivent fonctionner efficacement même si la taille du réseau grandisse. Cela n'est pas facile à réaliser, car établir un chemin entre deux nœuds mobiles devient couteux en termes du temps requis, nombre d'opérations, et bande passante dissipée, quand le nombre de nœuds augmente [5].
- **Optimisation des métriques :** parmi les métriques qui méritent d'être considérées lors de la conception des protocoles de routage pour les MANETS, on peut citer :

-Taux de délivrance maximal.

-Plus court chemin. -Consommation d'énergie minimale.

-Minimum de charge de routage (bande passante).

-Stabilité des chemins [5]

I.2.4 Services de routage dans les réseaux Ad Hoc :

Les réseaux Ad Hoc étant de nature multi-sauts, le protocole de routage détermine une route entre un nœud source et un nœud destination. De par la faible bande passante offerte par les réseaux Ad Hoc et du fait de la diffusion des données, les protocoles de routage actuellement utilisés dans les réseaux filaires ne peuvent être utilisés, sans modifications, dans les réseaux MANETS. De fait, des nouveaux protocoles de routage ont dû être développés [2].

Pour être réellement opérationnel dans un environnement mobile, le protocole de routage prend en compte trois phases :

- **Dissémination de l'information de routage :** elle permet de connaître suffisamment d'éléments sur la topologie pour choisir un chemin atteignant le nœud de destination. Suivant la quantité d'informations échangées, les nœuds obtiennent une vue plus ou moins précise de la topologie du réseau. Le protocole de routage se voit dans l'obligation d'optimiser l'envoi de ces informations, car elles sont fortement consommatrices en bande passante [2].
- **Sélection du chemin :** une fois les informations de routage obtenues, le protocole de routage peut sélectionner une route parmi l'ensemble obtenu en fonction de certains critères. Pour les protocoles Meilleur effort (« Best Effort »), le critère est de minimiser le nombre de sauts du chemin. Ainsi, parmi l'ensemble des routes qui lui sont proposées, le protocole choisit celle traversant le plus faible nombre de nœuds. Les routes choisies doivent être dépourvues de boucles. La présence de boucles rend inefficace le chemin sélectionné puisque le paquet ne pourra pas atteindre la destination consommant inutilement de la bande passante. En effet, un 12 paquet de données transitant sur un chemin, possédant une boucle, va tourner en rond tant que la boucle est présente. Pour éviter qu'un paquet de données tourne indéfiniment, le paquet est détruit lorsqu'il atteint la limite imposée par le champ TTL présent dans le protocole IP. Un protocole de routage peut créer deux sortes de boucles : les boucles temporaires et les boucles permanentes [2]. Les premières ont lieu pendant le transfert d'un message de routage. Durant ce temps, des stations peuvent être mises à jour et d'autres non, d'où la possible apparition d'une boucle. Elle dure au maximum la durée de traversée du réseau par un message de routage.

  Les boucles permanentes, quant à elles, sont dues au phénomène du bouclage à l'infini [2]. Ces boucles peuvent consommer énormément de bande passante.

- **Maintenance des routes :** dans un environnement mobile, la topologie du réseau ne cesse d'évoluer avec le temps. De fait, les routes sont amenées à changer avec le déplacement des nœuds. Une route doit éviter de rester longtemps interrompue, car les paquets ne pourraient atteindre leur destination. Le protocole de routage doit donc tenir compte de ces changements et mettre à jour les routes qui viennent à être coupées [2].

I.2.5 Les contraintes de routages dans les réseaux Ad Hoc :

L'étude et la mise en œuvre d'algorithmes de routage pour assurer la connexion des réseaux Ad Hoc au sens classique du terme (tout sommet peut atteindre tout autre), est un problème complexe. L'environnement est dynamique et évolue donc au cours du temps, la topologie du réseau peut changer fréquemment. Il semble donc important que toute conception de protocole de routage doive étudier les problèmes suivants :

- **Minimisation de la charge du réseau :** l'optimisation des ressources du réseau renferme deux autres sous problèmes qui sont l'évitement des boucles de routage, et l'empêchement de la concentration du trafic autour de certains nœuds ou liens [3].
- **Bon acheminement des données :** le fait que les chemins utilisés pour router les paquets de données puissent évoluer, ne doit pas avoir d'incident sur le bon acheminement des données. L'élimination d'un lien, pour cause de panne ou pour cause de mobilité devrait, idéalement, augmenter le moins possible les temps de latence [3].
- **Assurer un routage optimal :** la stratégie de routage doit créer des chemins optimaux et pouvoir prendre en compte différentes métriques de coûts (bande passante, nombre de liens, ressources du réseau, etc.). Si la construction des chemins optimaux est un problème dur, la maintenance de tels chemins peut devenir encore plus complexe, la stratégie de routage doit assurer une maintenance efficace de routes avec le moindre coût possible [3].
- **Le temps de latence :** la qualité des temps de latence et de chemins doit augmenter dans le cas où la connectivité du réseau augmente [3].

I.3 CLASSIFICATION DES PROTOCOLES DE ROUTAGE :

Suivant la classification des protocoles de routage dans les réseaux ad hoc, les protocoles de routage peuvent être séparés en deux catégories, les protocoles proactifs et les protocoles réactifs. Les protocoles proactifs établissent les routes à l'avance en se basant sur l'échange périodique des tables de routage, alors que les protocoles réactifs cherchent les routes à la demande.

D'autres classes existent tel que : les protocoles de routage hybrides qui combinent les deux approches précédentes afin de tirer avantage de deux

catégories citées précédemment, tout en réduisant leur limitation, on cite aussi les protocoles géographiques, hiérarchique, à qualité de service et multicast. Comme il est illustré dans la figure 1.9

Suivant la manière de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent classer en deux familles de protocoles :

- **État des liens : TORA, OLSR et TBRPF**
- **Vecteur de distance : DSR, DSDV et AODV**.

Suivant le moment de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent être séparés en :

- **Proactif : DSDV, OLSR et TBRPF** adoptent ce comportement. Les protocoles proactifs établissent les routes à l'avance en se basant sur l'échange périodique des tables de routage.
- **Réactif (sur demande) : TORA et AODV** adoptent ce comportement. Les protocoles réactifs cherchent les routes à la demande. **AODV** est en fait une version réactive de **DSDV**.
- **Hybride :** les protocoles hybrides définissent deux zones où ils combinent le comportement proactif à l'intérieur d'une zone et le comportement réactif entre les zones. Par exemple **DSR**, qui est réactif à la base mais qui peut être optimisé s'il adopte un comportement proactif

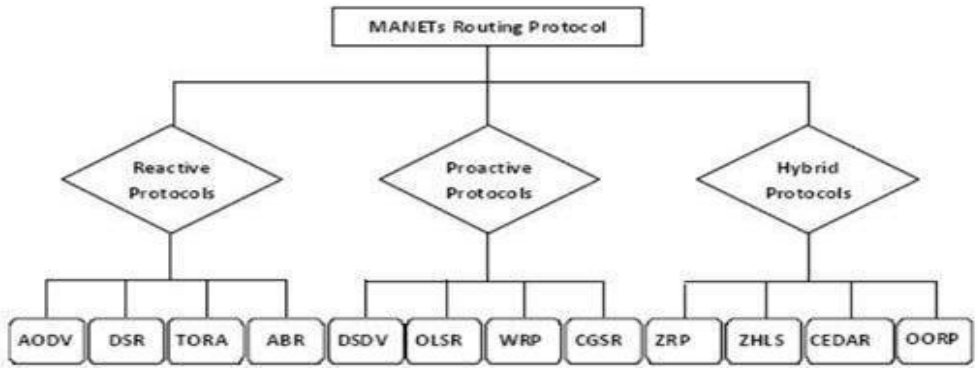

Figure I.9 : la classification des protocoles de routage

I.3.1 Les protocoles de routage proactifs :

I.3.1.1Définition :

Les protocoles de cette catégorie sont basés sur les algorithmes classiques d'état de liens et de vecteur de distance. Les protocoles de routage proactifs essaient de maintenir les meilleurs chemins existants, vers toutes les destinations possibles au niveau de chaque nœud du réseau. Les routes sont sauvegardées même si elles ne sont pas utilisées [1].

I.3.1.2 Avantages :

- ✓ Pas de temps de réaction.
- ✓ Adaptés aux réseaux denses de taille moyenne.
- ✓ Adaptés aux réseaux à forte mobilité.

I.3.1.3 Inconvénients :

- ✓ Trafic de contrôle important.
- ✓ Capacité d'échange du réseau limitée.

I.3.2 Protocole de routage réactif :

I.3.2.1 Définition :

Les protocoles réactifs adoptent des algorithmes classiques tels que le routage par vecteur de distance. Les routes sont établies uniquement sur demande et seules les routes en cours d'utilisation sont maintenues. Lorsqu'un nœud veut envoyer des paquets, une étape de découverte de route est initiée par la diffusion d'un message de recherche de route. Tout nœud qui reçoit ce message et qui ne dispose pas d'informations à propos de la destination, il diffuse à son tour le message. Ce mécanisme est appelé mécanisme d'inondation [16].

I.3.2.2 Avantages :

- ✓ Trafic de contrôle faible.
- ✓ Adaptés aux grands réseaux.
- ✓ Consommation énergétique réduite.

I.3.2.3 Inconvénients :

- ✓ Temps de réaction long.
- ✓ Problème en cas de forte mobilité des nœuds.

I.3.3 Les protocoles de routage hybrides (les zones) :

I.3.3.1 Définition :

Les protocoles de routage hybrides combinent les deux approches de routage réactif et proactif. Dans ce type de protocole, on peut garder la connaissance locale de la topologie jusqu'une certaine distance (nombre prédéfini de sauts) par un échange périodique de trame de contrôle.

Autrement dit par une technique proactive. Les routes vers des nœuds plus lointains sont obtenues par schéma réactif, c'est-à-dire par l'utilisation de paquets de requête en diffusion. Avec ce système, on dispose immédiatement des routes dans notre voisinage proche, et lorsque la recherche doit être étendue plus loin, elle en est optimisée [17].

I.3.3.2 Avantages et inconvénients des protocoles hybrides :

Le protocole hybride est un protocole qui se veut comme une solution mettant en commun les avantages des deux approches précédentes en utilisant une notion de découpage du réseau. Cependant, il rassemble toujours quelques inconvénients des deux approches proactives et réactives [6].

I.4 CONCLUSION :

Dans ce chapitre nous avons présentés les réseaux ad hoc ainsi le routage et la classification du routage dans les réseaux ad hoc.

CHAPITRE II

Le protocole de routage AODV (Ad Hoc On demande Distance Vector)

II.1 PRESENTATION :

AODV (Adhoc On-demande Distance Victor), qui a été normalisé dans la RFC 3561. AODV a fait l'objet de nombreux travaux. Comme DSR, il s'agit d'un protocole réactif, et donc il existe des similitudes importantes entre les deux protocoles. Néanmoins, AODV n'utilise pas de routage par la source, et utilise des numéros de séquence afin de déterminer si un message est plus récent ou ancien que l'information déjà connue. En outre, une métrique est utilisée afin de pouvoir utiliser une meilleure route si elle devient disponible, il s'agit d'une métrique comptant simplement le nombre de sauts [3].

II.2 TABLE DE ROUTAGE :

AODV maintient les chemins d'une façon distribuée en gardant une table de routage, au niveau de chaque nœud de transit appartenant au chemin cherché. Une entrée de la table de routage contient essentiellement :

- L'adresse IP de la destination.
- Le nœud suivant.
- La distance en nombre de nœud (i.e. le nombre de nœud nécessaire pour atteindre la destination).
- Le numéro de séquence destination qui garantit qu'aucune boucle ne peut se former.
- Liste des voisins actifs (origine ou relais d'au moins un paquet pour la destination pendant un temps donné).
- Le temps d'expiration de l'entrée de la table.
- Un tampon de requête afin qu'une seule réponse soit envoyée par requête.
- A chaque utilisation d'une entrée, son temps d'expiration est remis à jour (temps courant + active route time) [3].

II.3LES MESSAGES DE CONTROLE DE PROTOCOLE AODV :

Les mécanismes de découverte et de maintenance de routes peuvent s'effectuer par le biais des messages de contrôles suivants :

- **RREQ (Route Requêt) : Message de demande de route.**
- **RREP (Route Replay) : Message de réponse à un RREQ.**
- **RERR (Route Erreur) : Message qui signale la perte d'une route.**

Le format des paquets est donné ci-dessous :

II.3.1 Message de demande de route RREQ :

Il contient essentiellement les champs suivants : [2]

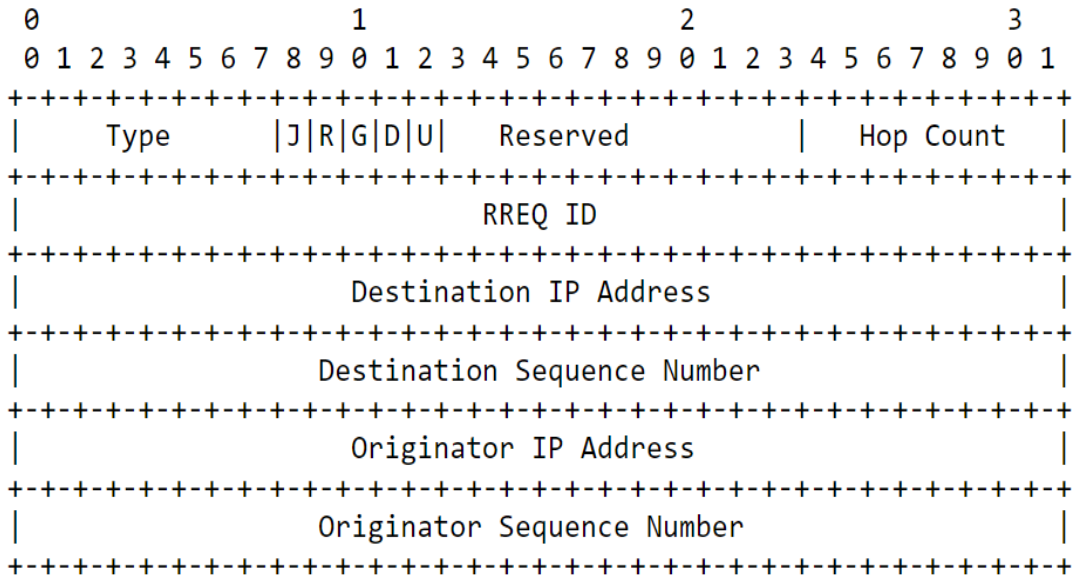

Figure II.1 : Format du message RREQ

- ✓ **Type (8 bits)** : ce champ indique le type de paquet, dans ce cas il prend la valeur 1.
- ✓ **Flags (drapeaux) (5 bits) :** ce champ contient cinq flags (J, R, G, D, U) tel que :
- ✓ **J (Join flag) et R (Repaire flag) :** sont réservés pour le multicast.
- ✓ **G (Gratuits RREP flag) :** indique si un message RREP spécifique doit être envoyé à la destination dans le cas où un nœud intermédiaire possède un chemin à la destination.
- ✓ **D (Destination only flag) :** ce drapeau indique si seulement la destination qui doit répondre à la requête ou pas.
- ✓ **U (Unknownsequencenumber) :** indique le numéro de séquence de la destination est inconnu
- ✓ **Reserved (11 bits) :** initialisé à la valeur 0 et ignoré à la réception du message.
- ✓ **Hop Count (8 bits) :** il contient le nombre de sauts parcourus par RREQ.
- ✓ **RREQ ID :** il identifie la requête parmi les requêtes envoyées par la même source.
- ✓ **Destination IP Address :** l'adresse IP de destination pour laquelle une route est désirée.

- ✓ **Destination Séquence Number :** Le dernier numéro de séquence reçu dans le passé par le créateur pour n'importe quelle route vers la destination.
- ✓ **Originator IP Adress** : l'adresse IP de la source de la requête.
- ✓ **OriginatorSequenceNumber :** Le nombre de séquence courant de la source contenue dans la table de routage de ce nœud s.

II.3.2 Message de réponse à un RREQ par RREP :

Il contient essentiellement les champs suivants : [3]

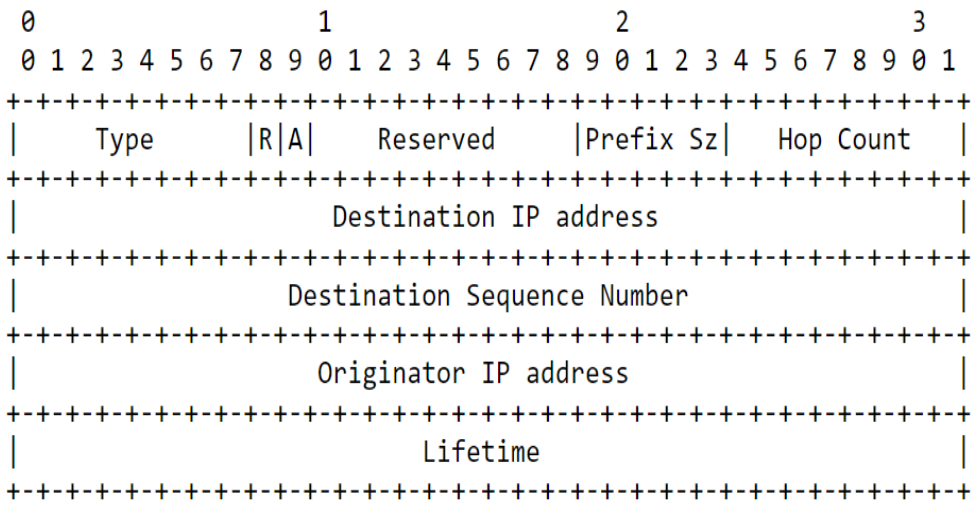

Figure II.2 : Format du message RREP

- ✓ **Type (8 bits) :** ce champ indique le type de paquet, dans ce cas il prend la valeur 2.
- ✓ **Flags (drapeaux) (2 bits) :** ce champ contient deux flags :
- ✓ **R (Repair flag) :** utilisé pour le multicast.
- ✓ **A (Acknowledgmentrequired) :** indique si la source doit envoyer un acquittement pout les messages RREP.
- ✓ **Reserved (9 bits) :** initialisé à la valeur 0 et ignoré à la réception du message.
- ✓ **Préfix Sz (5 bits) :** si la valeur de ce champ est différente de zéro, ce dernier indique que le nœud prochain peut être utilisé pour chaque nœud demandant cette destination et qui possède la même valeur de Préfix Sz. 23
- ✓ **Hop Count (8 bits) :** il contient le nombre de sauts entre la source jusqu'à la destination.

- ✓ **Destination IP Address** : l'adresse IP de la destination du paquet RREQ.
- ✓ **Destination SequenceNumber :** le numéro de séquence de la destination associé à cette route.
- ✓ **Originator IP Addresse :** l'adresse IP du nœud qui crée la requête.
- ✓ **Life time :** le temps pour lequel chaque nœud qui reçoit RREP considère que la route est valide.

II.3.3 Message de perte de route RERR :

Un message d'erreur de route contient essentiellement les champs suivants : [3]

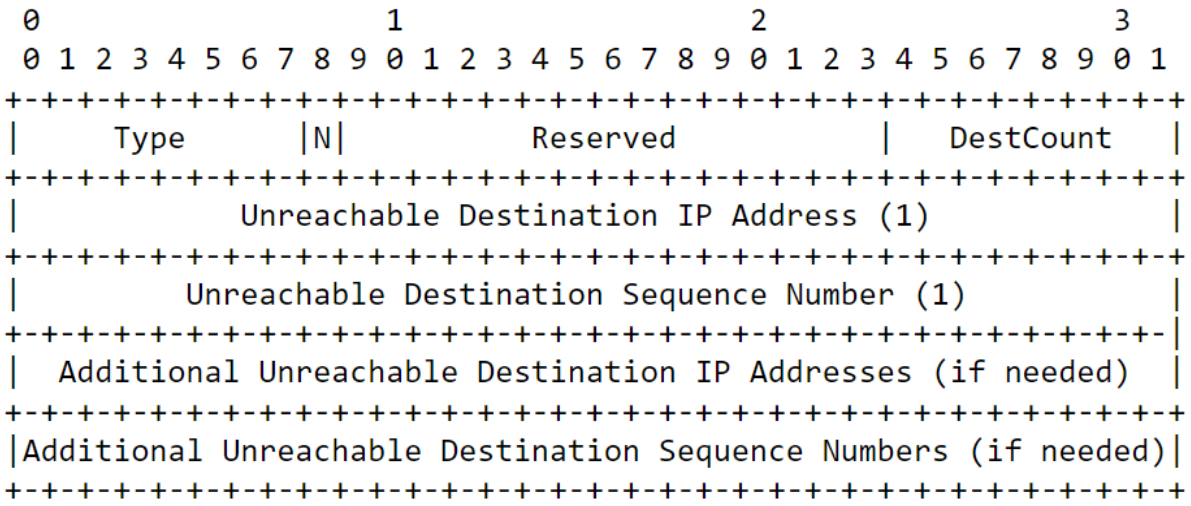

Figure II.3 : Format du message RERR

- ✓ **Type (8 bits) :** la valeur de ce champ prend 3 dans le message RRER.
- ✓ **Flag (1 bits) :** il contient un drapeau (N : No delete flag), celui-ci est indicatif lorsqu'un nœud est capable de réparer le lien, et informe les nœuds suivants qu'ils ne doivent pas supprimer le chemin.
- ✓ **Reserved (15 bits) :** initialisé à la valeur 0 et ignoré à la réception du message.
- ✓ **Dest Count (8 bits) :** il indique le nombre de destinations inaccessibles incluses dans ce message, ce champ doit être supérieur ou égal à un.
- ✓ **Unreachable Destination IP Address :** l'adresse IP des destinations inaccessibles pour la raison de cassure de lien.
- ✓ **Unreachable Destination SequenceNumber** : le nombre de séquence de la liste des destinations inaccessibles qui se trouve dans le champ Unreachable Destination IP Address.

II.4 LE PRINCIPE DE NUMERO DE SEQUENCE :

La circulation inutile des paquets de messages, qui peut arriver avec le DBF (Distribution de Bellman Ford), est intolérable dans les réseaux mobiles Ad Hoc, caractérisés par une bande passante limitée et des ressources modestes. L'AODV utilise les principes de numéro de séquence afin d'éviter le problème des boucles infinie et des transmissions inutiles de changent fréquemment ce qui fait que les routes maintenues par certains nœuds, deviennent invalide. Les numéros de séquence permettent d'utiliser les routes les plus nouvelles ou autrement dit les plus fraiches (fresh routes), un nœud les mis à jour chaque fois qu'une nouvelle information provenant d'un message RREQ, RREP ou RERR, il incrémente son propre numéro de séquence dans les circonstances suivantes :

- ✓ Il est lui-même le nœud destination et offre une nouvelle route pour l'atteindre.
- ✓ Il reçoit un message AODV (RREQ, RREP, RERR) contenant de nouvelles informations sur le numéro de séquence d'un nœud destination.
- ✓ Le chemin vers une destination n'est plus valide [3].

II.5 FONCTIONNEMENT DU PROTOCOLE AODV :

AODV, est un protocole de routage réactif à vecteur de distance qui s'inspire de DSDV. Contrairement à celui-ci, il ne construit pas a priori la table de routage mais réagit à la demande et essaie de trouver un chemin avant de router les informations. Tant que la route reste active entre la source et la destination, le protocole de routage n'intervient pas, ce qui diminue le nombre de paquets de routage échangés entre les nœuds constituant le réseau [2]

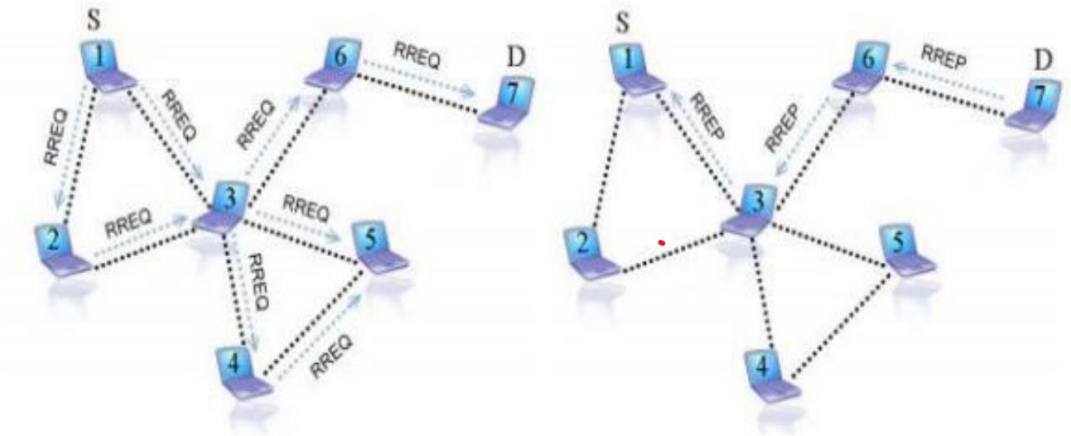

Figure II.4 : les deux requêtes RREQ et RREP utilisées dans le protocole AODV

Lorsqu'un nœud S essaie de communiquer avec un nœud D, l'échange de messages se fait en plusieurs étapes décrites ci-dessous à l'aide de l'exemple de la figure

II.5.1 Découverte de route :

Lorsqu'un nœud source a besoin d'une route vers une certaine destination (e.g: le nœud 1 dans la figure II.5 désire envoyer des données au nœud 5) et qu'aucune route n'est disponible (la route peut être non existante, avoir expiré ou être défaillante), la source 1 diffuse en broadcast (voir figure II.5 a) un message de demande de route RREQ (Route REQUEST), ce message contient un identifiant (RREQ_ID) associé à l'adresse de la source (@SRC) qui servira à identifier de façon unique une demande de route. Le nœud 1 enregistre cet identifiant de paquet RREQ ([RREQ_ID, @SRC]) dans son historique (buffer) et l'associe à un time qui décomptera sa durée de vie au-delà de laquelle cette entrée sera effacée. Quand un nœud intermédiaire (cas des nœuds 2 et 4 dans la figure II.5 b) qui n'a pas de chemin valide vers la destination reçoit le message RREQ, il ajoute ou met à jour le voisin duquel le paquet a été reçu. Il vérifie ensuite qu'il ne l'a pas déjà traité en consultant son historique des messages traités. Si le nœud s'aperçoit que la RREQ est déjà traitée, il l'abandonne et ne la rediffuse pas Sinon, il met à jour sa table de routage à l'aide des informations contenues dans la requête afin de pouvoir reconstruire ultérieurement le chemin inverse vers la source, il incrémente ensuite le nombre de sauts HC (Hop Count) dans la demande de route et la rediffuse. Il est à noter qu'AODV utilise le principe des numéros de séquence pour pouvoir maintenir la cohérence des informations de routage. Ce numéro, noté SN (SequenceNumber), est un champ qui a été introduit pour indiquer la fraicheur de l'information de routage et garantir l'absence de boucles de routages. À la réception d'un paquet RREQ (figure II.5 c), la destination 5 ajoute ou met à jour dans sa table de routage un chemin vers le nœud voisin duquel il a reçu le paquet (nœud 4) ainsi qu'un chemin vers la source 1. La destination 5 génère ensuite une réponse de route RREP qu'elle envoie en unicast vers le prochain saut en direction de la source (voir figure 1.16c). Notons qu'un nœud intermédiaire peut aussi générer un RREP si la requête l'autorise à le faire (bit destination only de la RREQ mis à 0) et qu'il dispose déjà dans sa table de routage d'un chemin valide vers la destination 5. Les nœuds intermédiaires qui reçoivent la RREP (cas du nœud 4 dans la figure II.5 d) vont mettre à jour le chemin qui mène à la destination dans leur table de routage et retransmettre en unicast le message (après avoir incrémenté le nombre de sauts) vers le nœud suivant en direction de la source sachant que cette information a été obtenue lors du passage de la RREQ. Lorsque la réponse de route atteint la source (nœud 1 dans l'exemple), un chemin 26

bidirectionnel est établi entre la source et la destination (voir figure 1.5) et la transmission de paquets de données peut débuter [2].

II.5. 2 Maintenance des routes :

Afin de maintenir les routes, une transmission de messages HELLO est effectuée. Ces messages sont en fait des réponses de route (RREP) diffusés aux voisins avec un nombre de sauts égal à un. Si au bout d'un certain temps, aucun message n'est reçu d'un nœud voisin, le lien en question est considéré défaillant. Alors, un message d'erreur RERR (Route ERROR) se propage vers la source et tous les nœuds intermédiaires vont marquer la route comme invalide et au bout d'un certain temps, l'entrée correspondante est effacée de leur table de routage. Le message d'erreur RERR peut être diffusé ou envoyé en unicast en fonction du nombre de nœuds à avertir de la rupture de liaison détectée. Ainsi, s'il y en a un seul, le message est envoyé en unicast sinon, il est diffusé. AODV à l'avantage de réduire le nombre de paquets de routage échangés étant donné que les routes sont créées à la demande et utilise le principe du numéro de séquence pour éviter les boucles de routage et garder la route la plus fraîche. Cependant, l'exécution du processus de création de route occasionne des délais importants avant la transmission de données [2].

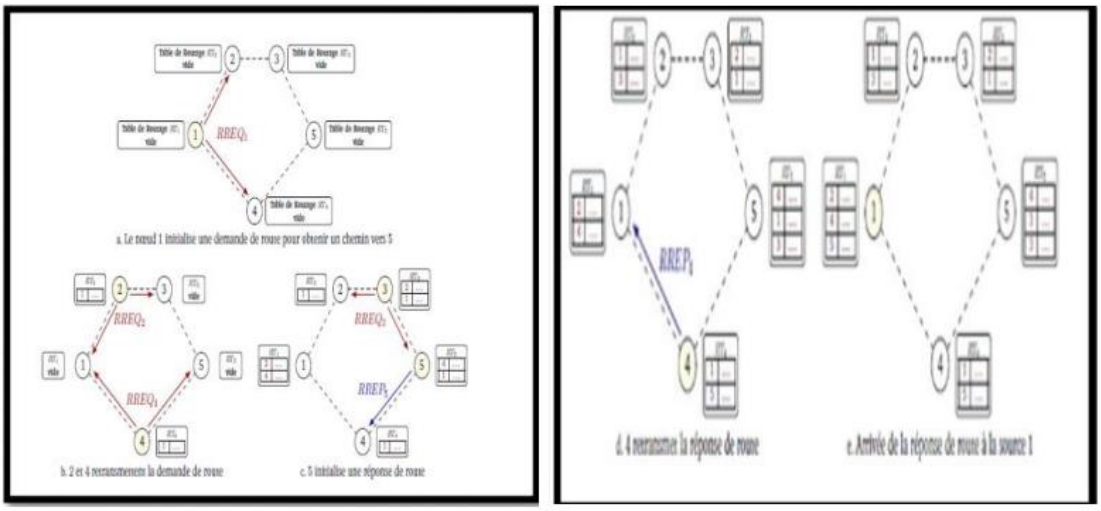

Figure II.5 : Coupure de route et envoie du RERR dans AODV

II.5.3 Gestion des numéros de séquence :

Il n'y a pas de numéro de séquence unique pour le réseau car il serait impossible de déterminer en permanence sa valeur de manière distribuée. Chaque nœud possède donc son propre numéro de séquence permettant de dater les informations provenant de lui seul. Un numéro de séquence est incrémenté dans les cas suivant : [2]

- Avant de commencer une découverte de route, un nœud incrémente son numéro de séquence.

- Avant d'envoyer une réponse RREP, le nœud met à jour son numéro de séquence en utilisant le plus grand entre le numéro de séquence actuel et de celui indiqué comme numéro de séquence destination dans la requête RREQ reçue.

- En cas de rupture d'un lien, pour chaque route passant par le lien, le numéro de séquence associé à la destination de la route est incrémenté avant d'envoyer la réponse RREP informant de la rupture du lien

II.6 ÉVALUATION :

Comme tout protocole réactif, AODV souffre d'un délai lors de l'envoi des premiers paquets vers une destination non connue. L'utilisation des numéros de séquence crée aussi une certaine complexité, mais a l'avantage de permettre de fortement limiter les retransmissions inutiles. Ajouté au fait que l'approche réactive du protocole ne pèse que peu sur la charge du réseau, il en résulte qu'AODV n'a que peu d'impact sur celle-ci. Les messages HELLO périodiques restent cependant nécessaires. Une différence majeure d'AODV par rapport à DSR est le fait qu'un nœud intermédiaire sur une route peut modifier la route d'une source à une destination. C'est notamment le cas si un lien est rompu et que le nœud intermédiaire parvient à trouver une route alternative ou si une meilleure route devient disponible entre le nœud intermédiaire et la destination. On peut parler de réparation locale du lien et d'optimisation locale de la route car ces informations n'ont pas à être remontées jusqu'à la source. Cette différence fait qu'AODV est plus adapté que DSR dans le cas d'une importante mobilité des nœuds, cela permet notamment à chaque source de choisir une route en fonction de critères qui lui sont propres, comme une métrique particulière ou encore le choix d'éviter certains nœuds ou liens. Le routage par la source de DSR reste néanmoins intéressant de par le fait qu'il permet à la source de contrôler exactement quelle route est utilisée [2].

II.7 LIMITATION DU PROTOCOLE AODV :

Dans le protocole AODV, les routes sont établies en fonction du « nombre minimal des sauts » (le plus court chemin), cependant, si le nombre des communications augmente le principe du plus court chemin n’est plus le critère optimal du choix des routes, il est préférable alors d’utiliser d’autres métriques qui ont un effet significatif sur la connectivité et la durée de vie du réseau [2].

II.8 Propriétés d'AODV :

II.8.1 Les avantages d'AODV :

- L'un des avantages d'AODV est l'utilisation de numéro de séquence dans les messages. Ces numéros de séquences permettent l'éviter les problèmes de boucles infinies et sont essentiels au processus de mis à jour de la table de routage

- Un autre avantage est le rappel de l'adresse IP du nœud origine dans chaque message. Ceci permet de ne pas perdre la trace du noeud à l'origine de l'envoi du message lors des différents relais

- Le protocole de routage AODV n'a pas besoin de système administratif central pour contrôler le processus de routage. Les protocoles réactifs comme AODV ont tendance à réduire le contrôle de la circulation des messages généraux au coût de l'augmentation de la latence à trouver de nouveaux itinéraires (routes).

- AODV réagit assez rapidement aux changements topologiques dans le réseau et met à jour uniquement les nœuds affectés par ces changements.

- Les messages HELLO assure le maintien de routes en communiquant seulement avec les voisins directs, donc ils ne provoquent pas une surcharge sur le réseau.

- Le protocole de routage AODV économise de la mémoire aussi bien que l'énergie. Le nœud de destination répond une seule fois à la première demande et ignore le reste. La table de routage maintient au plus une entrée par destination. Si un nœud doit choisir entre deux trajets, le trajet récent avec un numéro de séquence de destination plus grand, est toujours choisi [18].

- Si une entrée de table de routage n'est pas utilisée récemment, l'entrée est expirée après un certain délaite la route devient invalide. La route invalide est supprimée après un délai. : les paquets d'erreur (RERR)atteignent tous les nœuds utilisant le lien coupé situant sur la route vers toute destination.

II.8.2 Les inconvénients d'AODV :

- Un inconvénient d'AODV est qu'il n'existe pas de format générique des messages. Chaque message a son propre format : RREQ, RREP, RERR.

- Il est possible qu'une route valable soit expirée. La détermination d'un temps d'expiration raisonnable est difficile, parce que les nœuds sont mobiles ce qui nécessite de relancer le processus de découverte de route et l'envoi des RREQ avec un taux différent selon la mobilité du réseau.

- En outre, AODV recueille une quantité très limitée d'informations de routage, l'acquisition désinformations de routage sont obtenue uniquement des paquets de contrôles. Ceci provoque une inondation de découverte de route plus fréquemment, ce qui peut entraîner d'importantes surcharges réseau. Les inondations incontrôlées génèrent de nombreuses transmissions redondantes qui peuvent provoquer ce qu'on appelle

« Broadcast Storm » La performance du protocole AODV se conduisant mal dans de plus grand s réseaux. La principale différence entre les petits et les grands réseaux est la longueur moyenne des chemins. Un long chemin est plus vulnérable aux ruptures de lien et requiert une charge de contrôle élevé pour son entretien [18].

- En outre, comme la taille d'un réseau grandit, diverses mesures de performance commencent à diminuèrent raison de l'augmentation du travail administratif, que l'on appelle la charge administrative.

- AODV est vulnérable à toutes sortes d'attaques, car il repose sur l'hypothèse que tous les nœuds vont coopérer. Sans cette coopération, aucune route ne peut être établie et aucun paquet ne peut être transmis. Il existe deux principaux types de nœuds non coopératifs : malveillants et égoïstes. Les nœuds malveillants sont soit défectueux et ne peuvent pas suivre le protocole, ou sont intentionnellement malveillant et essaient d'attaquer le réseau.

- L'égoïsme est la non coopération dans de certaines opérations de réseau, par exemple :

Suppression de paquets qui peuvent affecter les performances, mais peuvent économiser la batterie.

II.9 Vulnérabilités dans AODV :

Le protocole AODV est très efficace en tant que service de réseau, mais il a beaucoup de vulnérabilités, signifie que ce protocole peut facilement être attaqué. AODV n'est pas si sécurisé. AODV est conçu pour un réseau idéal signifie pour un réseau n'ayant aucun nœud malveillant. Pour un réseau n'ayant aucun nœud malveillant le protocole AODV est le plus efficace. Mais nous savons tous que rien n'est idéal, autrement dit qu'il y a certains nœuds incommodes partout. Quelques nœuds gourmands peuvent exister aussi ce qui met en échec l'objectif de l'utilisation du réseau. Afin de lancer une attaque contre le protocole de routage AODV, il suffit de faire des modifications dans les messages RREQ, RREP, RERR comme suit [19] :

➢ Les numéros de séquence peuvent être modifiés.

➢ Le nombre de sauts peuvent être modifié. (Principale attaque est la formation des boucles dans le réseau « Looping »).

➢ Modification des routes (attaque Blackhole, des informations erronées sur le chemin).

➢ Tunneling (warm Hole).

➢ Spoofing (collecte d'information sur le routage) pour préparer une attaque ultérieurement.

II.10 Les différentes attaques de routage AODV :

II.10.1 Le modèle d'un attaquant :

La première étape pour sécuriser un système est l'identification de la nature des éventuels attaquants. Dans les réseaux ad hoc, nous pouvons classifier un attaquant selon les dimensions suivantes :

• **Interne vs. Externe :** L'attaquant interne est perçu comme un membre normal du réseau et peut communiquer avec les autres membres. La présence des attaques internes est très problématique et difficile à détecter, car elle annule le niveau de sécurité assuré par les techniques cryptographiques. L'attaquant externe est considéré par les nœuds membres comme un intrus et est donc limité dans la diversité des attaques qu'il peut provoquer [20].

• **Malveillant vs Rationnel** : Un attaquant malveillant n'a pas d'intérêts personnels à travers ses attaques et a pour but le dysfonctionnement du réseau. Par conséquent, il peut employer tous les moyens sans tenir compte des coûts correspondants et des conséquences. Par contre, un attaquant rationnel cherche un profit personnel, et ainsi, on peut prévoir les cibles d'attaques et les moyens employés.

• **Passif vs. Actif :** L'attaquant passif écoute simplement les informations qui sont échangées entre les nœuds tandis que l'attaquant actif agit sur les informations qui sont échangées. Il peut les falsifier, les modifier, voire même les détruire

II.10.2 Attaque de largage de paquets : Dans une attaque d'abandon de paquet, les messages de routage reçus sont simplement abandonnés par l'attaquant. Cela peut être détecté en surveillant si un nœud voisin diffuse des paquets vers la destination finale ou non. Pour activer la surveillance des nœuds voisins, il est nécessaire de conserver la table des voisins.

Cette attaque est disponible sous différentes formes. Les différentes sous-catégories sont les suivantes :

Si un attaquant veut appliquer une attaque de suppression de paquets sur les messages RREQ qu'il reçoit, les messages RREQ peuvent également être supprimés de manière sélective par un attaquant interne. De tels types d'abus par des attaquants sont de nature similaire aux nœuds égoïstes. Si un attaquant s'inquiète de l'application de cette attaque sur les messages RREP, cela peut être le cas d'une perturbation d'itinéraire. Cette attaque peut également s'appliquer à d'autres paquets de données et empêchera le nœud affecté de prendre des paquets de données des nœuds voisins pendant une courte période de temps. Après avoir reçu le message RREQ, un attaquant peut apporter des modifications comme augmenter l'ID RREQ, changer l'adresse IP de destination avec une autre adresse IP, ajouter le numéro de séquence source par un, mettre une adresse IP inexistante à la place de l'adresse IP source. Après cela, un faux message peut être transmis par un attaquant.

Lorsque tous les voisins d'un attaquant reçoivent le faux message RREQ, ils modifient le saut suivant du nœud source vers le nœud inexistant car le faux message RREQ a un numéro de séquence source plus grand. En raison d'une adresse IP de destination inexistante, le faux message se rendra aux nœuds extrêmes du réseau ad hoc. Chaque fois qu'un nœud nécessite l'envoi de paquets de données vers le nœud source, il suivra la route créée à l'aide du faux message RREQ. En raison d'un nœud inexistant, les paquets de données peuvent être abandonnés. Avec l'aide de mécanismes de réparation locaux dans le protocole AODV, cette attaque ne peut pas totalement séparer le nœud victime. Chaque fois qu'un nœud observe une livraison infructueuse de paquets de données, les nœuds recommencent le processus de découverte d'itinéraire [20]

II.10.3 Attaque par numéro de séquence :

La fraîcheur de la route couplée à un nœud sera indiquée en utilisant le numéro de séquence. Si un attaquant transmet un paquet de contrôle AODV avec un grand numéro de séquence du nœud compromis, la route sera dirigée vers le nœud compromis. Le numéro de séquence peut être réduit pour restreindre la mise à jour dans la table ou augmenté pour renouveler les tables de route inverse d'autres nœuds. Cette attaque peut également s'appliquer à la fois au numéro de séquence source ou au numéro de séquence de destination. Un message RREQ peut être identifié de manière unique par l'ID RREQ avec l'adresse IP source. La combinaison de cela montre la fraîcheur d'un message RREQ. À tout moment, un nœud ne considère que la première copie d'un message RREQ. Si un autre nœud accepte l'ID RREQ augmenté avec l'adresse IP source, cela signifie que le nœud

acceptera le faux message RREQ. L'attaque par numéro de séquence ne peut prendre en compte que le champ de numéro de séquence, disponible dans le message RREQ [21].

II.10.4 Attaque de modification de champ :

Comme on le sait, le paquet de données sera envoyé avec l'en-tête. Dans le processus de superposition, les paquets de données passent par différentes couches et ajoutent des en-têtes en conséquence. L'attaque de modification de champ est responsable de la modification des valeurs de champ dans l'en-tête au niveau de la couche réseau. Comme ci-dessus, l'attaque par numéro de séquence modifie le champ de numéro de séquence, par conséquent, on peut dire que l'attaque par numéro de séquence fait partie de l'attaque de modification de champ. Les autres champs qu'un attaquant peut modifier sont mis en évidence ci-dessous. Le tableau ci- dessous montrera l'impact du champ modifié pendant le processus de routage normal.

Champ de message RREQ	**Modifications**
RREQ ID	**Pour rendre acceptable ou inacceptable un faux message RREQ, l'attaquant augmente ou diminue l'ID RREQ.**
Type	**Le type de message sera modifié.**
Hop Count	**Pour invalider la mise à jour, le nombre de sauts sera diminué ou augmenté pour mettre à jour les tables de routage inversé des autres nœuds**
Destination IP Address	**Remplacer par une autre adresse IP**
Source IP Address	**Remplacez par une autre adresse IP pour modifier l'itinéraire inverse**

Tableau II.1 : Attaque de modification de champ sur le champ de message RREQ

Lorsque plusieurs champs ont été modifiés par l'attaquant, cela montre des répercussions immédiates sur la sécurité du réseau. Pour garantir l'absence de boucle dans AODV, un nœud après avoir reçu un message RREQ modifie sa table de routage inverse. Cette modification se produit uniquement si le numéro de séquence source est supérieur à la valeur dans sa table de routage ou si le numéro de séquence source est égal mais la valeur du nombre de sauts est inférieure à celle de la table de routage pour le message RREQ. Pour affecter la table de routage des autres nœuds, un attaquant interne peut également impliquer la modification de ces champs. La même procédure sera utilisée pour un message RREP. Dans ce cas, si le numéro de séquence de destination dans le message

RREP est supérieur à la valeur un dans sa table de routage ou le numéro de séquence de destination est le même mais que le nombre de sauts plus un est inférieur à la valeur dans la table de routage, un nœud source ou un nœud intermédiaire modifie sa table de routage avant. Maintenant, prenez le point de vue de l'attaquant, si le numéro de séquence de destination dans le message RREP est supérieur à celui de sa table de routage, ou si les numéros de séquence de destination sont les mêmes, mais le nombre de sauts dans le message RREP plus un est plus petit que celui dans sa table de routage, l'attaquant peut contenir le message RREP légitime en augmentant le numéro de séquence de destination [21].

II.10.5 Attaque d'ajout de champ :

Dans cette attaque, un attaquant peut construire un message RREQ sans recevoir de message RREQ. Pour lancer cette attaque, il est nécessaire de collecter des informations d e base pour créer de faux messages RREQ (par exemple, en écoutant le trafic). En théorie, pour perturber le processus de routage, l'attaquant peut ajouter n'importe quel champ dans un message RREQ [21].

II.11Conclusion :

Dans ce chapitre nous avons présentés les réseaux ad hoc ainsi le routage et la classification du routage dans les réseaux ad hoc. Finalement on a présenté le fonctionnement et le comportement de chacun des protocoles AODV dans les réseaux ad hoc. AODV est un protocole de routage à la demande, il est utilisé principalement pour les réseaux sans fil. Ce protocole est le plus populaire des protocoles réactifs, son fonctionnement est basé sur la découverte de route et la maintenance de ces routes en utilisant des paquets de contrôle.

CHAPITRE III

Généralités sur La sécurité dans les réseaux ad hoc

III.1 Introduction :

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

III.2 Les risques liés à la sécurité informatique : [23] [22]

III.2.1 Analyse de risque en sécurité :

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

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

1. Détermination des fonctions et données sensibles des réseaux sans fil ad hoc.

2. Recherche des exigences de sécurité fondées sur les propriétés de la sécurité.

3. Étude des vulnérabilités.

4. Étude des menaces et quantification de leur probabilité d'occurrence ou de leur faisabilité.

5. Mesure du risque encouru en fonction des vulnérabilités mises en lumières et des menaces associées.

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

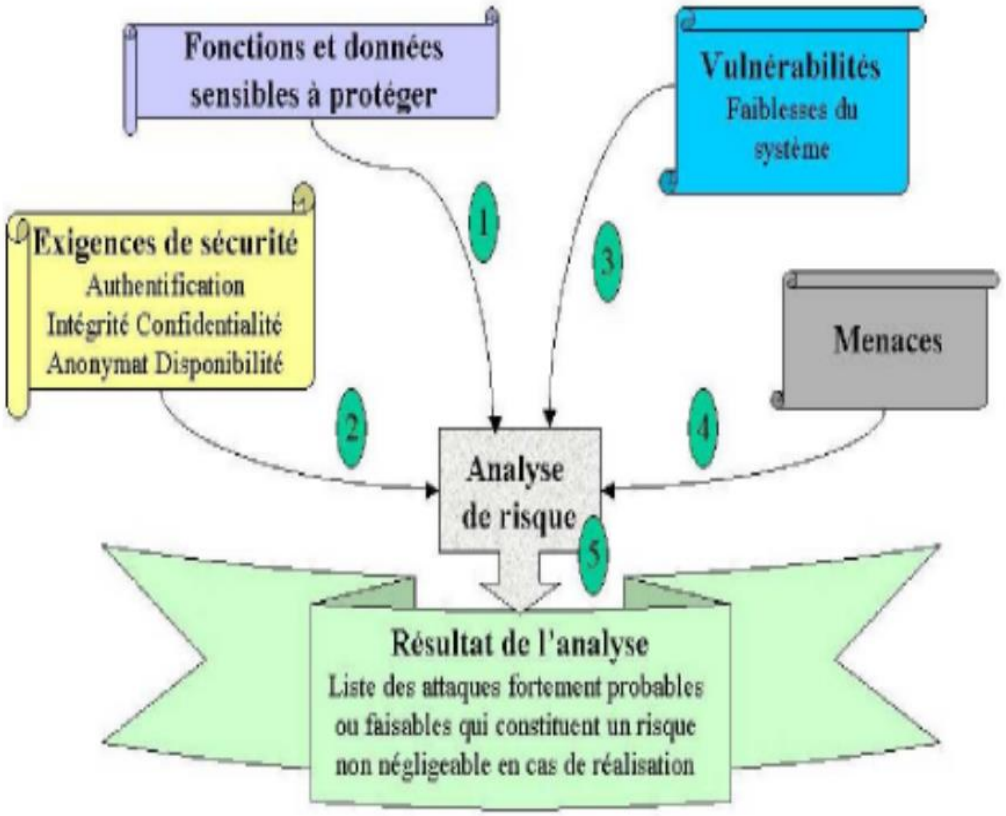

Figure III.1 : Les étapes de l'analyse de risque

III.3 Exigence de la sécurité dans les réseaux ad hoc :[23]

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

III.3.1 Contraintes de la sécurité :

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

¬ **Caractéristiques des nœuds :** les nœuds eux-mêmes sont des points de vulnérabilité du réseau car un attaquant peut compromettre un élément laissé sans surveillance. De plus, certains éléments peuvent avoir de faibles capacités de calculs.

¬ **Gestion de l'énergie :** L'énergie doit être conservée au maximum pour cela les nœuds chercheront le plus souvent à se mettre en veille, ce qui provoque donc une minimisation de l'activité de l'ensemble du réseau.

¬ **L'absence d'infrastructure centralisée :** cette caractéristique du réseau ad hoc qui pénalise la gestion des accès aux ressources du réseau.

¬ **La technologie sans fil :** Les perturbations dues à l'environnement radio peuvent entrainer des diminutions de débit et bande passante.

¬ **Mobilité :** Les éléments étant fortement mobiles, leur sécurité physique est moins assurée.

¬ **Les mécanismes de routage :** sont d'autant plus critiques dans les réseaux ad hoc que chaque entité participe à l'acheminement des paquets à travers le réseau. De plus, les messages de routage transitent sur les ondes radio.

III.3.2 Les besoins de sécurité :[24]

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

¬ **Disponibilité :** Est une propriété difficile à gérer dans les réseaux sans fil ad hoc vu les contraintes qui pèsent sur ce type de réseau :

-Topologie dynamique.

-Limitation des ressources énergétiques sur quelques nœuds.

-Communications sans fil pouvant être facilement brouillées ou perturbées.

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

¬ **Authentification :** L'authentification des entités apparait donc comme la pierre angulaire d'un réseau sans fil ad hoc sécurisé. Elle permet d'identifier et contrôler d'identité des participants afin d'interdire aux intrus d'injecter des messages falsifies en erronés

¬ **Confidentialité des données :** La confidentialité consiste le secret des messages échangés et ne pas les révéler aux adversaires et assurer la protection de l'information contre toute divulgation accidentelle ou malveillante aux parties non autorisées. Sans ce mécanisme, un nœud malveillant peut accéder aux

informations secrètes transites dans le réseau, et provoque le disfonctionnement du routage des données.

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

⎫ L'aspect sans fil qui permet à n'importe qui d'écouter les conversations au sein du réseau.

⎫ L'aspect sans infrastructure préexistante fait qu'un nœud ne peut pas faire des suggestions sur les chemins à emprunter par les différentes données, ce qui permet de ne pas faire confiance aux nœuds intermédiaires.

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

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

⎫ Les attaques visant à modifier le contenu des messages.

⎫ La faible fiabilité des liaisons filaires.

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

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

III.4 Les attaques contre les réseaux Ad Hoc :[25] [23]

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

Voici quelques attaques les plus courantes :

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

Un nœud malicieux a la capacité d'usurper l'identité d'un nœud valide du réseau, il peut lors du mécanisme de découverte de route répondre au nœud initiateur avec un message de type route replay en annonçant un chemin, avec un cout minimal, vers le nœud demandé. Le nœud émetteur mettra alors sa table de routage à jour

avec cette fausse route. Les paquets de données de nœud émetteur vers le nœud destinataire transiteront par le nœud malicieux qui pourra tout simplement les ignorer. Les paquets sont captés et absorbés par le nœud malicieux.

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

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

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

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

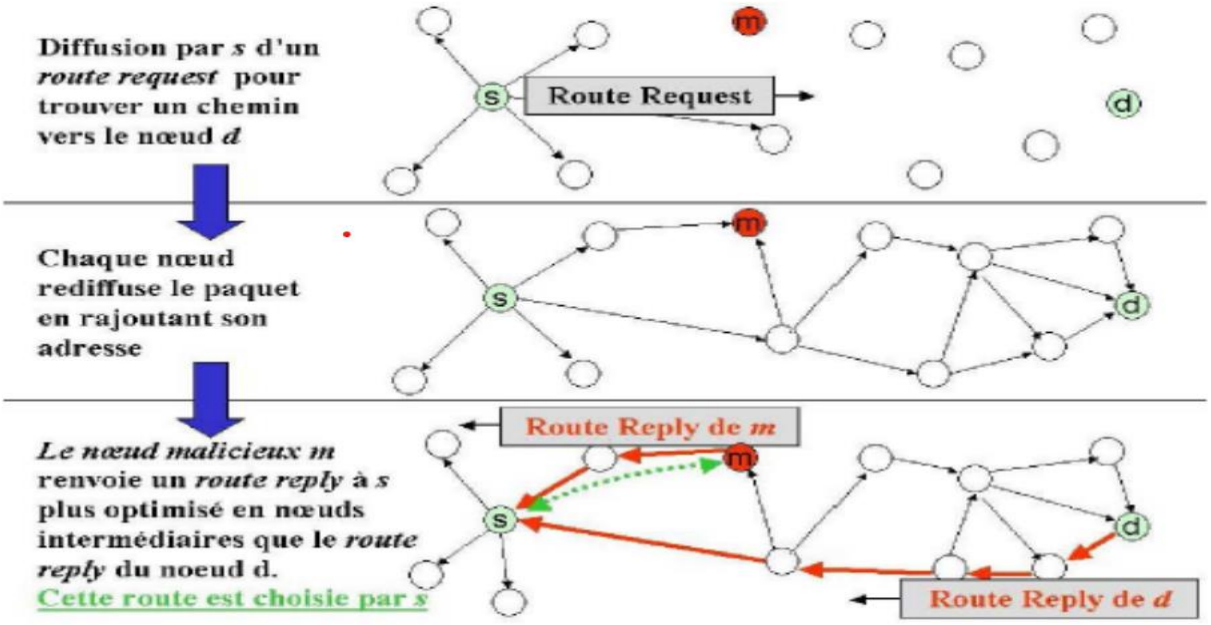

Figure III.2 : Attaque blackhole

III.4.2 Attaque du trou de ver (Worm Hole) :

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

première requête qui arrive aux nœuds intermédiaires qui est transmise de route. L'objectif pour l'attaquant est alors de faire passer ses requêtes avant les autres.

La figure ci-dessous illustre le principe de Worm Hole :

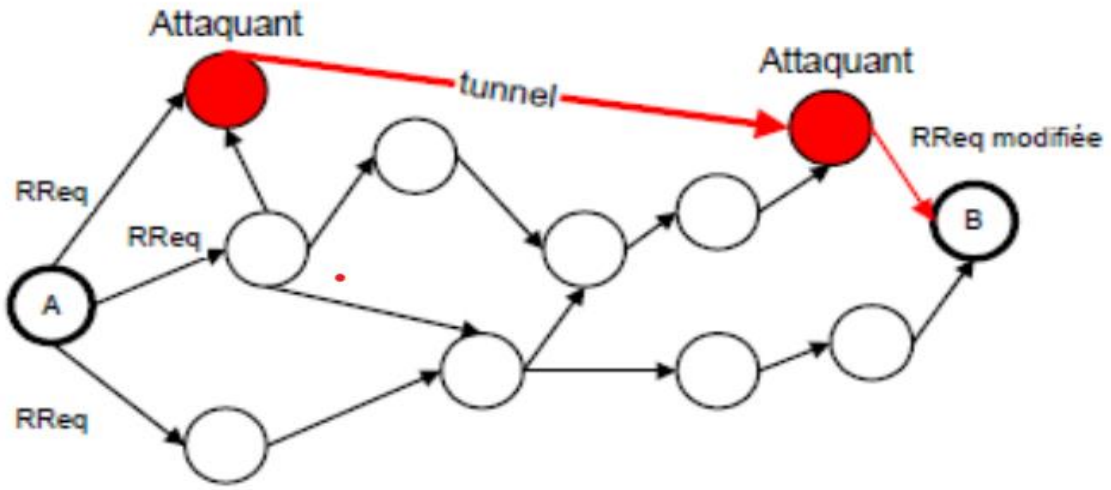

Figure III.3 : Attaque par un trou de ver

III.4.3 Attaque par usurpation d'identité [24] :

L'attaquant falsifie les informations relatives à l'identité afin d'isoler un nœud auquel il a volé l'identité et donner une fausse vue de la topologie du réseau.

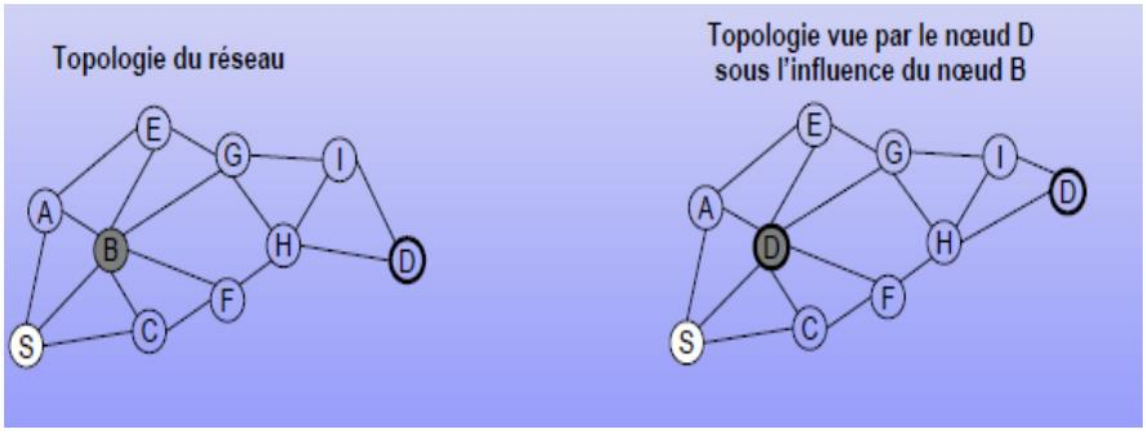

Figure III.4 : Attaque par usurpation d'identité

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

Les attaques contre les protocoles de routage des réseaux Ad Hoc peuvent avoir pour but de modifier le protocole lui-même, pour que le trafic passe par un nœud contrôle par l'adversaire. Une attaque peut aussi avoir pour but d'empêcher la

formation du réseau, obliger les nœuds à mémoriser des routes incorrectes, et en général perturber la topologie du réseau. Les attaques au niveau de routage peuvent être classées en deux catégories :

- Général incorrecte de trafic.

- Relayage incorrecte de trafic.

III.6 Etat de l'art des solutions pour la sécurité :[23] [24]

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

III.6.1 Solution pour l'authentification :

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

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

• Cryptographique symétrique (clé secrète) :

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

• Cryptographie asymétrique (clef publique) :

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

Exemple d'algorithmes asymétrique :

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

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

III.6.2 Solution pour l'intégrité et l'authentification des messages :

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

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

III.6.3 Solution pour la confidentialité :

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

III.6.4 Solution pour l'intégrité physique des nœuds :

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

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

III.6.5 Solution pour disponibilité :

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

III.6.6 Solution pour la sécurisation du routage :

Le mécanisme de cryptographie tel que les cryptographies à clé symétrique, clé public ou chaine de hach

Age 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 fonctionnelle 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.7 Conclusions :

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

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

CHAPITRE IV :

Le protocole de routage SAODV (Secure Ad hoc On-Demande Distance Victor)

IV. 1 Introduction :

Le SAODV, fruit d'une évolution constante dans le domaine de la sécurité des réseaux mobiles, est bien plus qu'un simple mécanisme de routage. Il incarne l'équilibre subtil entre la réactivité nécessaire pour s'adapter aux changements rapides de la topologie du réseau et la robustesse indispensable pour contrer les menaces potentielles, telles que les attaques par déni de service ou l'interception de données sensibles.

Dans un réseau Adhoc, du point de vue du protocole de routage, il existe deux types de messages : les messages de routage et les messages de données. Chacun a une nature différente et des besoins de sécurité différents. Les messages de données sont de bout en bout et peuvent être protégés en utilisant n'importe quel système de sécurité de bout en bout. En revanche, les messages de routage sont envoyés aux voisins directs, sont traités, éventuellement modifiés, puis renvoyés.

IV 2. Fonctions de sécurité :

Avant de concevoir une extension au protocole, qui assure la sécurité de l'AODV, il est nécessaire de réfléchir aux besoins en matière de sécurité et aux problèmes qui ne peuvent tout simplement pas être résolus. La principale difficulté à ne pas pouvoir éviter est qu'il peut y avoir des nœuds malveillants qui ne respectent pas les protocoles (ils falsifieront les paquets AODV, écouteront les autres, répondront aux paquets dans leurs propres intérêts, signaleront des erreurs là où il n'y en a pas, etc.).

Il est nécessaire d'avoir l'intégrité, l'authentification. Mais qu'en est-il de la confidentialité ? Eh bien, elle peut être nécessaire pour des scénarios avec des besoins de sécurité très élevés, mais cela n'a pas de sens si le scénario est un réseau ad hoc public auquel tout le monde peut se joindre à tout moment. Par conséquent, cela n'est pas pris en compte dans l'extension de protocole SAODV.

IV.3 Les défauts du protocole AODV :

1. Un nœud malveillant peut emprunter l'identité d'un nœud S en forgeant une RREQ avec son adresse comme adresse de l'expéditeur.

2. Lorsqu'un nœud malveillant transmet une RREQ généré par le nœud S pour découvrir une route vers D, en réduisant le champ du nombre de sauts, il augmente les chances d'être dans le tracé de l'itinéraire entre S et D, pour pouvoir analyser la communication entre eux. Une variante consiste à incrémenter le numéro de séquence de destination pour faire croire aux autres nœuds qu'il s'agit d'une route « fraîche ».

3. Emprunter l'identité d'un nœud D en forgeant une RREP avec son adresse comme adresse de destination.

4. Emprunter l'identité d'un nœud en forgeant une RREP qui prétend que le nœud est la destination et, pour accroître l'impact de l'attaque, il prétend être un leader d'un sous réseau SN avec un grand numéro de séquence et l'envoyer à ses voisins. De cette manière, il est devenu (au moins localement) un trou noir pour le sous-réseau SN entier.

5. Potentiellement, ne pas acheminer certaines RREQ et RREP, ne pas répondre à certaines RREQ et ne pas transférer certains messages de données. Ce genre d'attaque est particulièrement difficile à détecter car les erreurs de transmission ont le même effet.

6. Forger un message RERR prétendant qu'il est le nœud S et l'envoyer à son voisin D. Le message RERR a un très haut numéro de séquence de destination (DSN) pour l'une des destinations inaccessibles (U). Cela pourrait provoquer D à mettre à jour le numéro de séquence de destination correspondant à U avec la valeur DSN et, par conséquent mettre en échec les futures découvertes de routes effectuées par D pour obtenir une route vers U (car le numéro séquence de destination de U sera beaucoup plus petit que celui stocké dans la table de routage de D).

7. Selon AODV [26], l'originaire d'une RREQ peut mettre un numéro de séquence de destination beaucoup plus grand que le réel. En outre, les numéros de séquence se remettent à zéro quand ils atteignent la valeur maximale autorisée par la taille du champ. Ceci permet une attaque très facile dans le cas un attaquant est capable de fixer le numéro de séquence d'un nœud à toute valeur désirée par simple envoi de deux messages RREQ au nœud

IV.4Sécurisation d'AODV :

Supposons qu'il y a un sous-système de gestion des clés qui permet à chaque nœud ad hoc d'obtenir des clés publiques des autres nœuds du réseau. De plus, chaque nœud ad hoc est capable de bien vérifier l'association entre l'identité d'un nœud ad hoc donné et la clé publique de ce nœud. La réalisation de cela est dépendante du système de gestion des clés.

Deux mécanismes sont utilisés pour sécuriser les messages AODV : les signatures numériques pour authentifier les champs non-mutables des messages et les chaînes de hachage pour sécuriser l'information de nombre de sauts (la seule information mutable dans les messages). Pour les informations non-mutables, l'authentification est effectuée de façon bout en bout mais le même genre de techniques ne peut pas être appliqué à l'information mutable.

Les informations relatives aux chaînes de hachage et la signature sont transmises avec le message AODV comme une extension du message qui sera référencé par Signature Extension.

IV.5Les extensions SAODV :

Les figures indiquent le format des SAODV Signature Extensions (page suivante) :

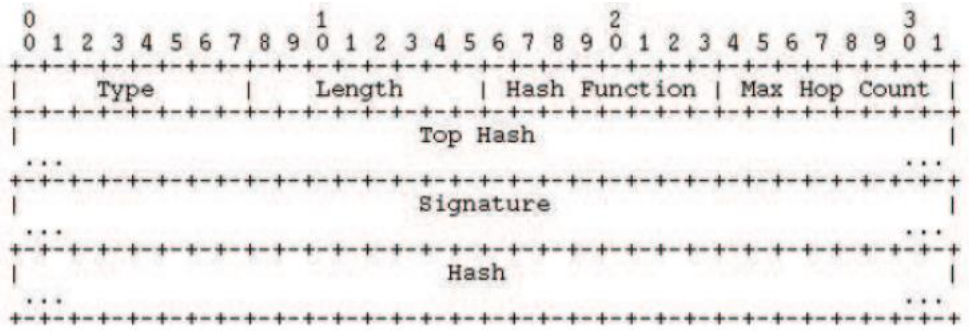

Figure IV.1 : RREQ (Single) Signature Extension

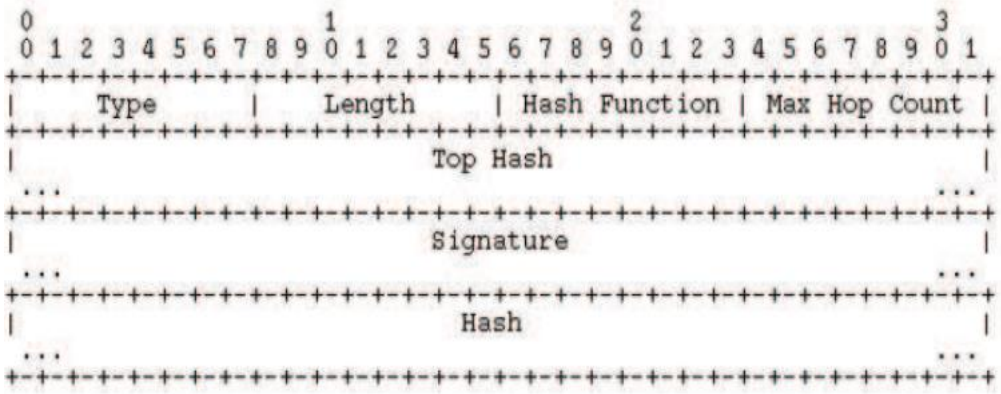

Figure IV.2 : RREP (Single) Signature Extension

Champ	Valeur
Type	64 dans RREQ-SSE et 65 dans RREP-SSE
Length	La longueur de données types spécifiques, sans les champs Type et Length
Hash fonction	La fonction de hachage utilisée pour calculer les champs Top hash et Hash
Max hop count	Le nombre de sauts maximal
Top Hash	Le hash correspondant au Max hop count pour l'authentification du compteur de sauts. Ce champ est variable et est multiple de 32bit.
Signature	La signature de tous les champs dans le paquet AODV qui sont avant ce champ sauf le champ compteur de sauts. Ce champ est variable et est multiple de 32bit.
Hash	Le hash correspondant au compteur de sauts actuel. Ce champ est variable et est multiple de 32bit.

Tableau IV.1 RREQ et RREP Signature Extension Fields

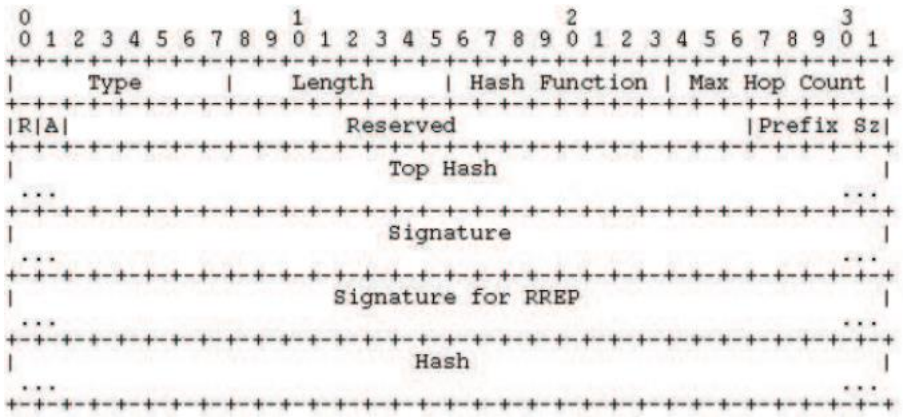

Figure IV.3 RREQ Double Signature Extension

Champ	Valeur
Type	66
Length	La longueur de données types spécifiques, sans les champs Type et Length
Hash fonction	La fonction de hachage utilisée pour calculer les champs Top hash et Hash
Max hop count	Le nombre de sauts maximal
R	Drapeau de réparation pour RREP
A	Drapeau de nécessité d'acquittement
Reserved	Émis 0 ; ignoré à la réception
Top Hash	Le hash correspondant au Max hop count pour l'authentification du compteur de sauts. Ce champ est variable et est multiple de 32bit
Signature	La signature de tous les champs dans le paquet AODV qui sont avant ce champ sauf le champ compteur de sauts. Ce champ est variable et est multiple de 32bit.
Signature for RREP	La signature qu'un nœud intermédiaire doit mettre dans RREP-DSE lorsqu'il répond à une demande de route vers le nœud ayant émis cette RREQ-DSE. Ce champ est variable et est multiple de 32bit
Préfix size	La taille du préfix pour RREP
Hash	Le hash correspondant au compteur de sauts actuel. Ce champ est variable et est multiple de 32bit.

Tableau IV.2 : champs RREQ Double Signature Extension

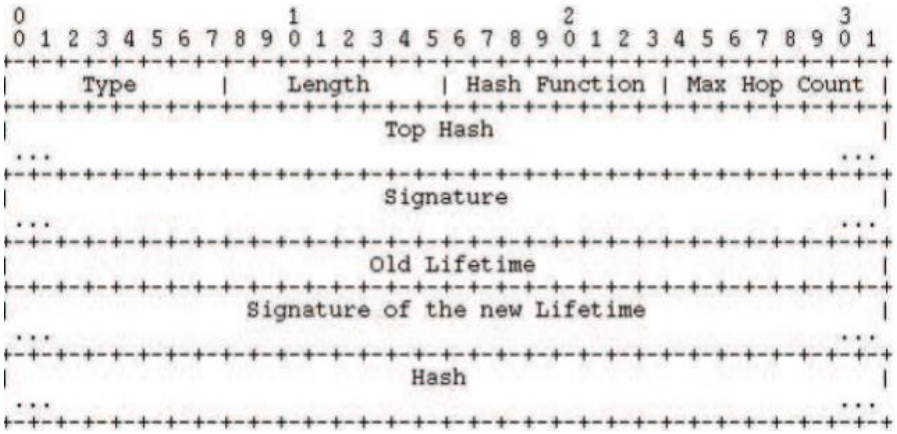

Figure IV.4 RREP Double Signature Extension

Champ	Valeur
Type	67
Length	La longueur de données types spécifiques, sans les champs Type et Length
Hash fonction	La fonction de hachage utilisée pour calculer les champs Top hash et Hash
Max hop count	Le nombre de sauts maximal
Top Hash	Le hash correspondant au Max hop count pour l'authentification du compteur de sauts. Ce champ est variable et est multiple de 32bit.
Signature	La signature de tous les champs dans le paquet AODV qui sont avant ce champ sauf le champ compteur de sauts. Ce champ est variable et est multiple de 32bit.
Old life time	Life time qui était dans la RREP générée par la destination finale
Signature of the new Life time	La signature de la RREP avec life time actuel (celui de la route dans le nœud intermédiaire). Cette signature est générée par ce nœud. Ce champ est variable et est multiple de 32bit.
Hash	Le hash correspondant au compteur de sauts actuel. Ce champ est variable et est multiple de 32bit

Tableau IV.3 : Champs RREP Double Signature Extension

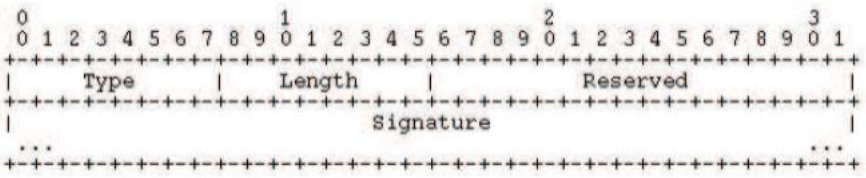

Figure IV.5 RERR Signature Extension

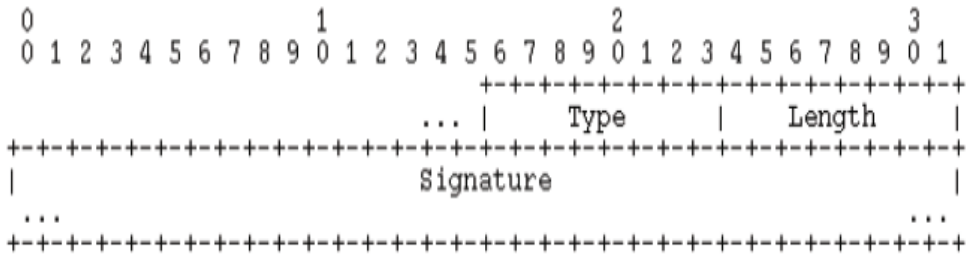

Figure IV.6 : RREP-ACK Signature Extension

Champ	Valeur
Type	**68 dans RERR-SE et 69 dans RRER-ACK-SE**
Length	**La longueur de données types spécifiques sans les champs Type et Length de l'extension**
Reserved	**(Seulement dans RERR-SE) Émis à 0 ; ignoré à la réception**
Signature	**La signature de tous les champs dans le paquet AODV qui sont avant ce champ sauf le champ compteur de sauts. Ce champ est variable et est multiple de 32bit.**

Tableau IV.4 RERR et RREP-ACK Signature Extension Fields

IV.6 Chaînes de hachage SAODV :

SAODV utilise les chaînes de hachage pour authentifier le nombre de sauts des messages RREP et RREQ de telle manière qu'il permet à chaque nœud qui reçoit le message (soit un nœud intermédiaire ou la destination finale) de vérifier que le nombre de sauts n'a pas été modifié par un attaquant. Cela empêche une attaque de type 2. Une chaîne de hachage est formée par l'application d'une fonction de hachage à plusieurs reprises sur un nombre aléatoire.

Chaque fois qu'un nœud initie un message RREQ ou RREP, il effectue les opérations suivantes :

· Générer un nombre aléatoire (seed).

· Définir le champ Max_Hop_Count à la valeur Time olive (à partir de l'en-tête IP)

Max_Hop_Count = Time olive

· Définir le champ Hash à la valeur de seed.

Hash = seed

· Définir le champ Hash_Fonction à l'identifiant de la fonction de hachage qu'il va utiliser.

Les valeurs possibles sont présentées dans le Tableau 2.1.

Valeur	Hash fonction
0	**Réservé**
1	**MD5HMAC96**
2	**SHA1HMAC96**
3-127	**Réservé**
128-255	**Dépend de l'implémentation**

Tableau IV.5 les valeurs du champ Hash Function

Hash Function = h ·

Calcule Top_Hash par le hachage de seed, Max_Hop_Count fois.

Top_Hash = Max_Hop_Count(seed)

Où :

– h est une fonction de hachage.

– h i (x) est le résultat de l'application de la fonction h à x, i fois.

En outre, chaque fois qu'un nœud reçoit un message RREQ ou RREP, il effectue les opérations suivantes afin de vérifier le nombre de sauts :

· Appliquer la fonction de hachage h, Maximum_Hop_Count–Hop Count fois sur la valeur du champ Hash et vérifie que la valeur résultante soit égale à la valeur contenue dans le champ Top_Hash.

Top_Hash == hMax_Hop_Count−Hop_Count (Hash)

· Avant la rediffusion d'une RREQ ou la transmission d'une RREP, un nœud applique la fonction de hachage sur la valeur Hash dans Signature Extension pour tenir compte du nouveau saut.

$$Hash = h\ (Hash)$$

Le champ Hash_Fonction indique quelle fonction de hachage doit être utilisée pour calculer le hachage. Tenter d'utiliser une fonction de hachage différente crée juste un faux hachage sans apporter aucun avantage à un nœud malveillant. Les champs Hash_Fonction, Max_Hop_Count, Top_Hash et Hash sont transmis avec le message AODV dans Signature Extension. Et, comme il sera expliqué plus tard, tous les champs sauf le champ Hash sont signés pour protéger leur intégrité.

IV.7 Signatures numériques SAODV :

Les signatures numériques sont utilisées pour protéger l'intégrité des données non mutables dans les messages RREP et RREQ. Cela signifie que SAODV signe tout sauf le nombre de sauts du message AODV et Hash de l'extension SAODV.

Le problème principal dans l'application de signature numérique c'est qu'AODV permet aux nœuds intermédiaires de répondre aux messages RREQ s'ils ont une route « assez fraiche » à la destination. Même si cela rend le protocole plus efficace, il le rend aussi plus difficile à sécuriser. Le problème est que le nœud intermédiaire qui génère un message RREP doit être en mesure de le signer au nom de la destination finale. Et, en plus, il est possible que la route stockée dans le nœud intermédiaire soit créée comme chemin inverse après avoir reçu un message RREQ (ce qui signifie qu'il n'a pas la signature pour la RREP).

Pour résoudre ce problème, SAODV propose deux alternatives. La première (et aussi la plus évidente) est que, si un nœud intermédiaire ne peut pas répondre à un message RREQ parce qu'il ne peut pas signer son message RREP, il se comporte exactement comme s'il n'avait pas la route et retransmet le message RREQ. La seconde est que, chaque fois qu'un nœud génère un message RREQ, il inclut aussi les drapeaux RREP, la taille préfixe et la signature qui peut être utilisée (par un nœud intermédiaire qui crée un chemin inverse à l'origine de la RREQ) pour répondre à une RREQ qui demande le nœud qui a initié le premier RREQ. En outre, quand un nœud intermédiaire génère un message RREP, la durée de vie de la route a changé à l'origine. Par conséquent, le nœud intermédiaire doit inclure les deux durées de vie (l'ancienne est nécessaire pour vérifier la signature de la destination de la route) et signer la nouvelle durée de vie. De cette façon, l'information originale de la route est signée par la destination finale et la durée de vie est signée par le nœud intermédiaire.

Pour distinguer les différents messages d'extension SAODV, ceux qui ont deux signatures sont appelés RREQ et RREP Double Extension Signature.

Quand un nœud reçoit une RREQ, il vérifie d'abord la signature avant de créer ou mettre à jour une route inverse vers cet hôte. Seulement si la signature est vérifiée, la route sera stockée. Si la RREQ a été reçue avec une Double Signature Extension (RREQ-DSE) alors le nœud stocke également la signature de la RREP et la durée de vie (qui est la valeur « durée de vie de la route inverse ») dans l'entrée de la route dans la table de routage. Un nœud intermédiaire ne répondra à une RREQ avec une RREP que si elle remplit les exigences d'AODV et le nœud a la signature correspondante et l'ancienne durée de vie pour les mettre dans les champs Signature et Old Life time de la RREP Double Extension Signature (RREP-DSE). Sinon, il retransmet la RREQ.

Quand une RREQ est reçue par la destination elle-même, elle ne répondra avec une RREP que si elle remplit les exigences d'AODV. Cette RREP sera envoyé avec une RREP Single Signature Extension.

Quand un nœud reçoit une RREP, il vérifie d'abord la signature avant de créer ou mettre à jour une route à cet hôte. Seulement si la signature est vérifiée, la route sera stockée avec la signature de RREP et la durée de vie.

L'utilisation de signatures numériques empêche les scénarios d'attaque 1 et 3.

IV.8Messages d'erreur SAODV :

En ce qui concerne les messages RERR, on peut penser que la bonne approche pour les sécuriser devrait être similaire à la façon dont sont les autres messages AODV (signant l'information non-mutable et trouver un moyen de sécuriser les informations mutables). Néanmoins, les messages RERR ont une grande quantité d'informations modifiables. En outre, il n'est pas clair quel nœud a annoncé la RERR et quels nœuds ne font que la transmettre. La seule information pertinente est qu'un nœud voisin est en train d'informer un autre nœud qu'il ne va pas être en mesure de router les messages vers certaines destinations du tout.

Cette proposition [27] (SAODV) stipule que chaque nœud (produisant ou retransmettant un message RERR) utilise les signatures numériques pour signer le message tout entier et que tout voisin qui le reçoit, vérifiera la signature. De cette façon, on peut vérifier que l'expéditeur du message RERR est vraiment celui qu'il prétend être. Et, puisque les numéros de séquence de destination ne sont pas signés par le nœud correspondant, un nœud ne doit jamais mettre à jour un numéro de séquence de destination de sa table de routage en se basant sur un message RERR

(Ce qui empêche un nœud malveillant de lancer une attaque de scénario 6). L'implémentation d'un mécanisme qui permettra aux numéros de séquence de destination d'un message RERR d'être signés par leurs nœuds correspondants va ajouter trop de surcharges par rapport à l'avantage de l'utilisation de cette information. Bien que les nœuds ne fassent pas confiance aux numéros de séquence de destination dans un message RERR, ils vont les utiliser pour décider s'ils doivent invalider une route ou non. Cela ne va conférer aucun avantage supplémentaire à un nœud malveillant.

Cette proposition [27] (SAODV) stipule que chaque nœud (produisant ou retransmettant un message RERR) utilise les signatures numériques pour signer le message tout entier et que tout voisin qui le reçoit, vérifiera la signature. De cette façon, on peut vérifier que l'expéditeur du message RERR est vraiment celui qu'il prétend être. Et, puisque les numéros de séquence de destination ne sont pas signés par le nœud correspondant, un nœud ne doit jamais mettre à jour un numéro de séquence de destination de sa table de routage en se basant sur un message RERR (ce qui empêche un nœud malveillant de lancer une attaque de scénario 6). L'implémentation d'un mécanisme qui permettra aux numéros de séquence de destination d'un message RERR d'être signés par leurs nœuds correspondants va ajouter trop de surcharges par rapport à l'avantage de l'utilisation de cette information. Bien que les nœuds ne fassent pas confiance aux numéros de séquence de destination dans un message RERR, ils vont les utiliser pour décider s'ils doivent invalider une route ou non. Cela ne va conférer aucun avantage supplémentaire à un nœud malveillant.

IV.9 Conclusion :

Dans SAODV, deux mécanismes sont utilisés pour sécuriser les messages AODV : les signatures numériques pour authentifier les champs non mutables des messages et les chaînes de hachage pour sécuriser les informations de nombre de sauts (la seule information mutable dans les messages). Pour les informations non mutables, l'authentification est effectuée de façon bout en bout mais le même genre de techniques ne peut pas être appliqué à l'information mutable.

Bien que SAODV soit bien sécurisé, il présente un défaut en ce qui concerne les performances pendant le traitement de paquets SAODV car il applique fréquemment des algorithmes de cryptographie asymétrique connus par leur lenteur de calcul ce qui dégrade largement le temps de réponse du protocole de routage.

CHAPITRE V

Résultats et Simulation

V.1 Introduction :

Ce chapitre a pour objectif de comparer le fonctionnement du protocole de routage AODV, en termes de temps de découverte de routes en deux cas :

- En utilisant du le protocole AODV ordinaire sans le sécuriser
- Utiliser le protocole de routage SAODV (Secure Ad hoc On-Demande Distance Victor)

Afin d'évaluer les performances de protocoles sélectionnés pour l'étude, dans ce chapitre, nous allons présenter principalement les outils utilisés pour réaliser notre simulation, puis les différentes étapes permettant de mettre en œuvre le protocole à l'aide de simulateur OMNET et du INET Framework, et enfin, on discute les résultats obtenus.

V.2 OMNET ++

5.2.1 Définition :

OMNET ++ est un environnement de simulation d'événements discrets orienté objet, basé sur C ++, utilisé pour simuler des réseaux, des systèmes multiprocesseurs et d'autres systèmes discrets. Grâce à son architecture modulaire, OMNET ++ est largement utilisé dans divers domaines d'application, tels que : modélisation des protocoles de communication, modélisation de réseaux filaires et sans fils. En général, il peut être utilisé pour tout système d'événement discret pouvant être conçu en fonction des entités de communication en envoyant des messages. OMNET++ fournit des outils pour la création et la configuration des modèles de réseaux (les fichiers NED et INI) et des outils pour l'exécution des programmes ainsi que pour l'analyse des résultats de simulation. [40]

Figure V.1 : Le lancement du simulateur OMNET++

V.2.2 Architecture de OMNETt++ :

Les modèles OMNET++ constituent en un ensemble de modules hiérarchiquement emboités tel qu'il est montré dans la (Figure 5.2) :

L'architecture d'OMNET++ est hiérarchique composé de modules. Un module peut être soit module simple ou bien un module composé. Les feuilles de cette architecture sont les modules simples qui représentent les classes C++. Pour chaque module simple correspond un fichier .cc et un fichier.h. Un module composé est composé de simples modules ou d'autres modules composés connectés entre eux. Les paramètres, les sous modules et les ports de chaque module sont spécifiés dans un fichier. Ned. La communication entre les différents modules se fait à travers les échanges de messages.

Les messages peuvent représenter des paquets, des trames d'un réseau informatique, des clients dans une file d'attente ou bien d'autres types d'entités en attente d'un service. Les messages sont envoyés et reçus à travers des ports qui représentent les interfaces d'entrer et de sortie pour chaque module. La conception d'un réseau se fait dans un fichier. Ned et les différents paramètres de chaque module sont spécifiés dans un fichier de configuration (.ini). OMNET++ génère à la fin de chaque simulation deux nouveaux fichiers omnet.vec et omnet.sca qui permettent de tracer les courbes et calculer des statistiques [41]

- La modélisation des protocoles de communications
- La modélisation des réseaux filaires et sans fils
- La modélisation des systèmes répartis
- L'architecture Hardware

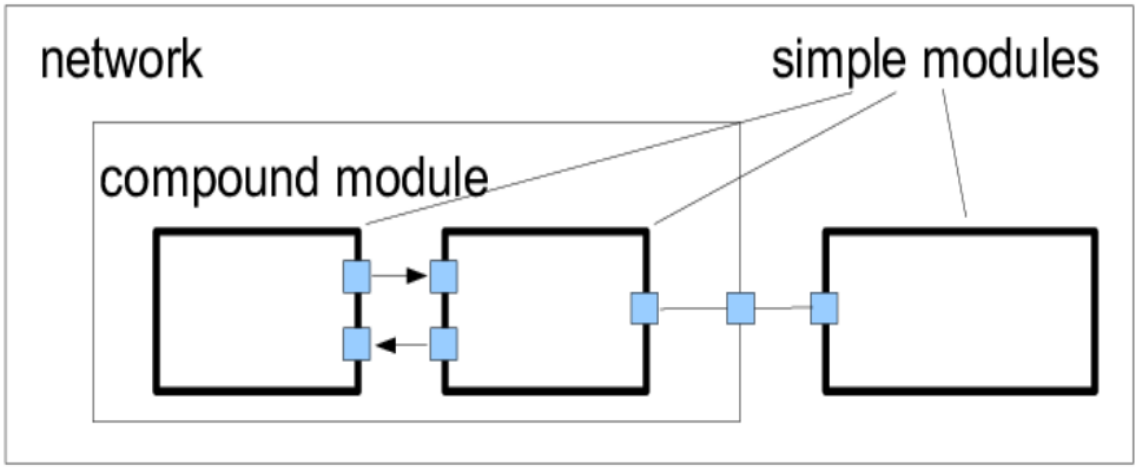

Figure V.2 : Architecture modulaire du simulateur OMNET++

V.2.3 Les principaux fichiers d'OMNET++ :

OMNET++ est composé par différents principaux fichiers [42] sont :

V.2.3.1Fichier (.NED) :

Utilise le langage NED (Network Description) de description de réseaux. Il peut être utilisé en deux modes : Mode Graphique ou Mode Texte qui permettent de décrire les paramètres et les ports du module. Les erreurs commises sont indiquées en temps réel par un point rouge situé à la gauche du code Un exemple de fichier Ned en mode "source" & "Graphique" sont présentés dans la (Figure 5.3) et (Figure 5.4).

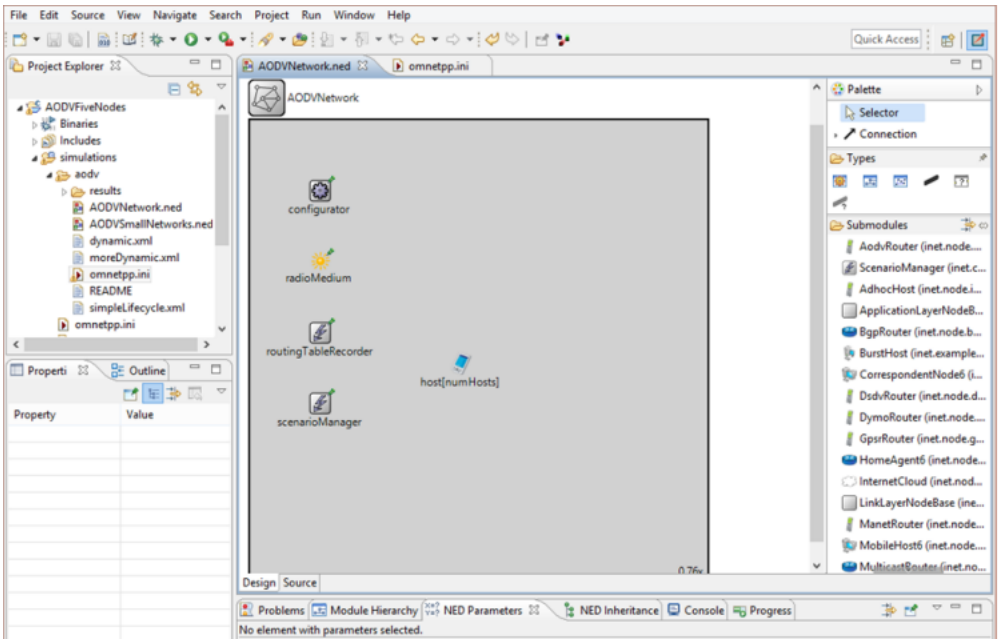

Figure V.3 : Ficher Ned en mode graphique

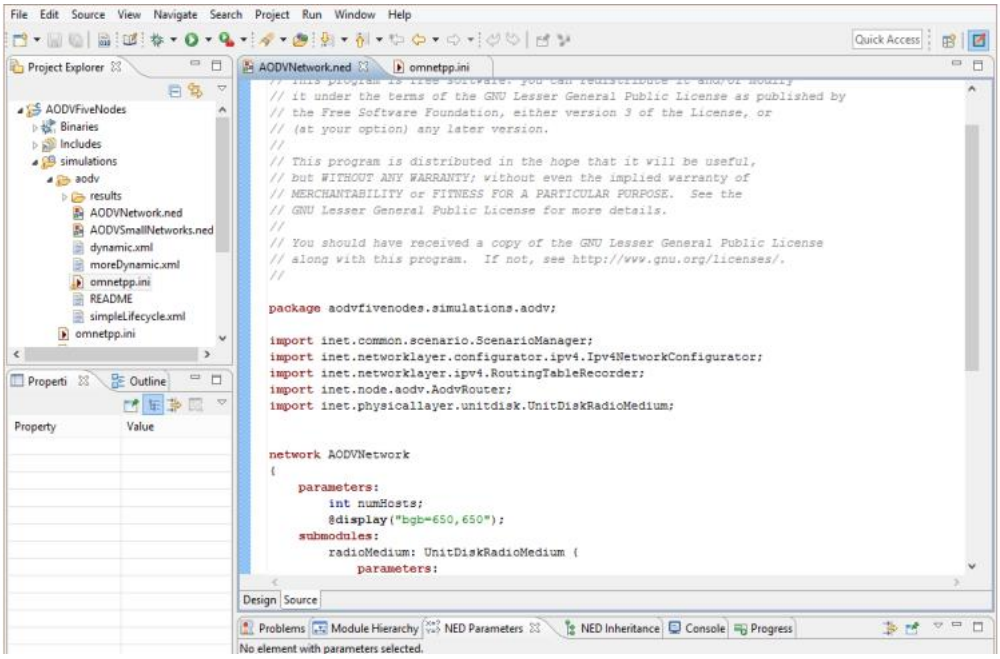

Figure V.4 : Fichier Ned en mode texte

V.2.3.2Fichier(.ini) :

Est lié étroitement avec le fichier NED. Permet à l'utilisateur d'initialisé les paramètres des différents modules ainsi la topologie du réseau. Voici un exemple présenté ci-dessous :

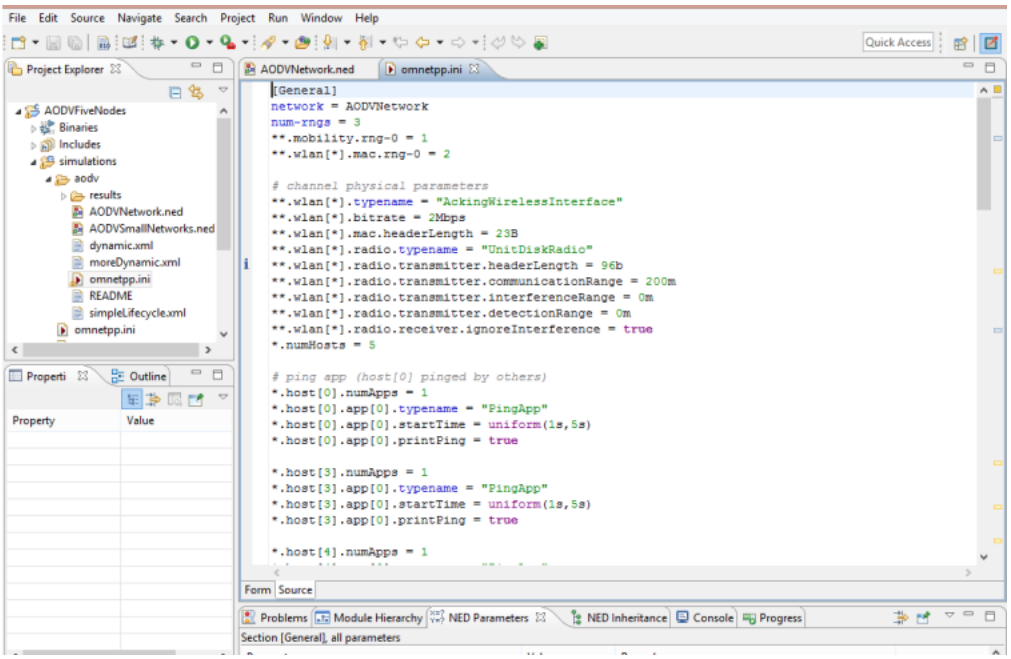

Figure V.5 : Exemple d'un fichier *.ini

V.2.3.3Fichier(.msg) :

Les modules communiquent en échangeant des messages. C'est dernier peuvent être déclarés dans un fichier dont l'extension est(.msg) ou l'on peut ajouter des champs de données. OMNET++ traduira les définitions de messages en classes C++ le diagramme suivant peut donner une idée plus détaillée sur le développement d'exécution d'une simulation sous OMNET++.

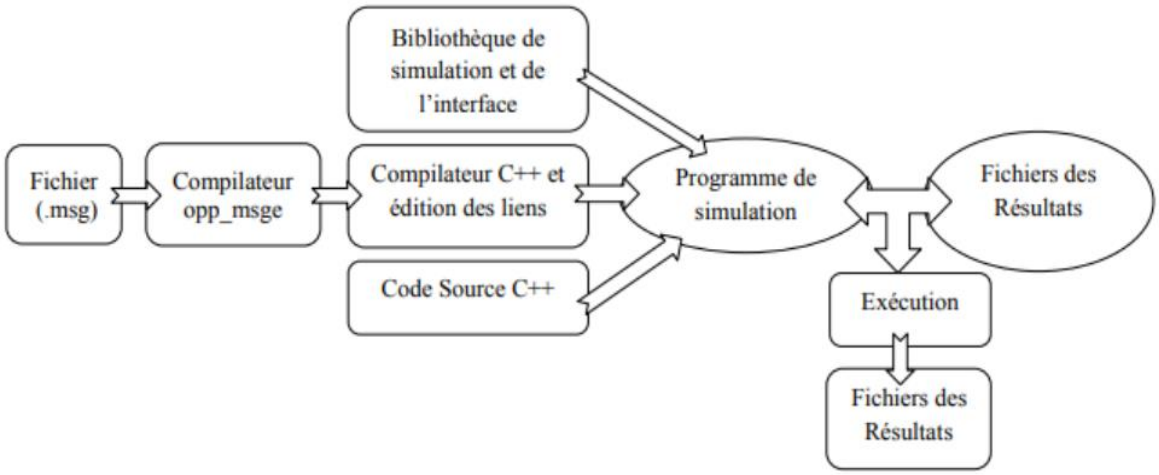

Figure V.6 : Exécution d'une simulation sous OMNeT++

V.2.4 Structure d'un nœud mobile dans OMNET++ :

Dans OMNET++, un nœud mobile a une structure [43] représentée par (Figure 5.7)

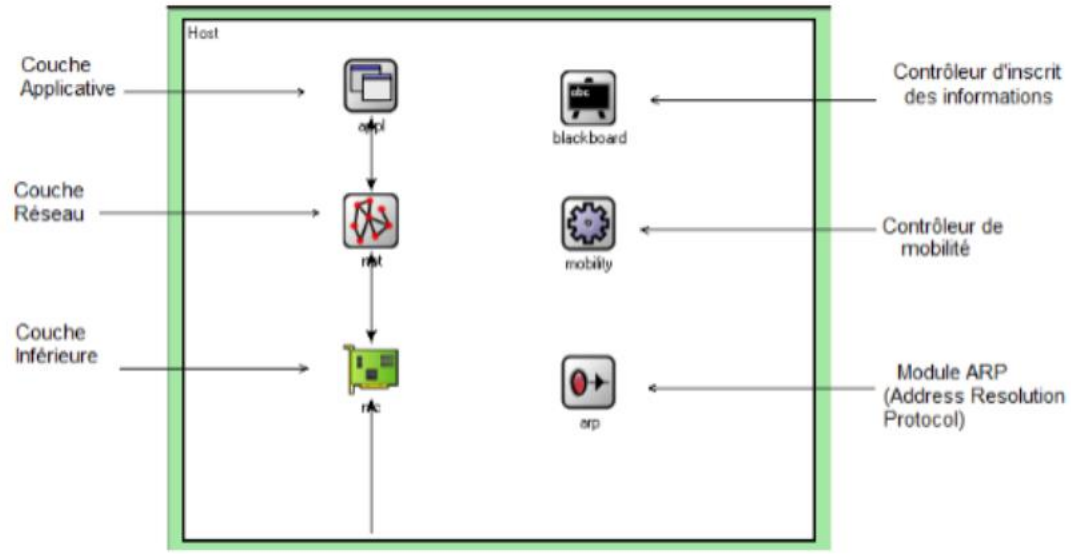

Figure V.7 : Structure d'un nœud mobile dans OMNET++

V.3 INET Framework :

INET est considéré comme la bibliothèque de modèles standard d'OMNeT++. Elle était basée initialement sur le paquetage IP Suite développé à l'université Karlsruhe puis maintenu par l'équipe d'OMNeT++ en lui ajoutant des correctifs et de nouveaux modèles.

Elle contient actuellement des modèles de protocoles pour la suite TCP/IP (IPv4, IPv6, TCP, SCTP, UDP, …), des modèles de la couche liaison pour les réseaux filaires et sans fils (Ethernet, PPP, IEEE802.11, …), des modèles MPLS avec signalisation RSVP et LDP, un support à la mobilité et plusieurs autres protocoles et composants.

Ses modules sont organisés dans des paquetages qui sont à leurs tours organisés selon les couches du modèle OSI (exemple : inet. Applications, inet. Transport, …).

Du point de vue architectural, INET respecte le concept modulaire d'OMNeT++ : les protocoles sont représentés par des modules simples dont les interfaces externes sont décrites par des fichiers NED et le comportement est implémenté à l'aide de classes C++. Les nœuds sont construits par composition de plusieurs modules simples.

D'autres modules (qui n'implémentent pas de protocoles) sont utilisés pour assurer des tâches spécifiques au cours de la simulation :

On en trouve côté nœud, le module Interface Table qui contient la table des interfaces réseau (eth0, wlan0, …), les tables de routage Routin Table et RoutingTable6 pour IPv4 et IPv6 respectivement et le module Notification Board qui facilite la communication entre les différents modules.

Au niveau réseau, on cite le module Flat Network Configuration qui sert à attribuer les adresses IP aux différents nœuds et de configurer un routage statique, le module Scenario Manager qui contrôle les expériences de simulation et la planification d'évènements et le module Channel Control requis pour les simulations sans fil et permet de garder la trace des nœuds à l'intérieur d'une zone d'interférences avec d'autres nœuds.

En ce qui concerne l'interaction entre ses différents éléments, INET gère la communication entre les différentes couches de protocoles via un processus d'encapsulation/décapsulation avec Control Info comme un objet attaché au message pour véhiculer une information additionnelle à la couche prochaine.

Un mode d'appel direct est suivi pour lier les autres modules, souvent en communication. Cela, est assuré par son module Notification Board qui joue le rôle d'intermédiaire entre le module où les évènements apparaissent et les modules qui sont intéressés par ces évènements. Son fonctionnement est basé sur le concept publication/abonnement selon lequel les modules peuvent s'abonner à des catégories de changements (exemple : un tableau de routage change d'état, un canal de communication devient libre). Quand l'un des changements se produit, le module hôte (exemple : Table de routage, couche physique) informe le module Notification Board, qui à son tour, diffuse l'information vers tous les modules à cette catégorie de changement.

INET constitue aujourd'hui un Framework incontournable pour OMNeT++. La richesse de ses modèles et la réutilisabilité de ses composants lui ont garanti un large déploiement chez la communauté OMNeT++ et lui ont permis d'être le socle sur lequel se basent plusieurs extensions telle que CoRE4INET l'extension INET implémentant le protocole TT Ethernet.[44]

V.3.1 Catalogue de modeles :

Les composants de modèle suivants [45] (protocoles, applications et autres modèles) sont disponibles pour INET Framework :

	Protocol	Projet
Application	CBR/VBR , HTTP, File Transfer , DHCP…	INET
Transport	TCP,UDP,SCTP,RTp,RTCP	INET
Reseaux	IPv4, ICMPV4 ,ARP ,IGMPv3 ,IPv6	INET
Routage	link-state routing , OSPFv2(1) , OSPF(2) , BGPv4 , BGP(2) ,RIP	INET
Manet Routage	AODV , DYMO , GPSR , DSDV, DSR,OLSR	INET
Fils	PPP, Ethernet, STP ,RSTP ,TTE ,802.1avb ,EPON , TDM/WDm-PON	INET
Sans fils	802.11 , 802.11p , 802.1e ,802.15.4, LTE(User-Plane) ,LTE(Control-Plane)	INET
Mobility/Envirenment	Various Mobility Models	INET

Tableau V.1 : La liste des principaux composants de modèle disponible dans INET FW

V.4 Les Avantages et Les Inconvénients :

V.4.1 Avantages :

Architecture modulaire permettant l'intégration de nouveau modèle.

- Utilisation du C++ pour le développement du noyau.
- Les classes de base du simulateur peuvent être étendue et personnalisées.
- Conception de modèle rapprochant de la réalité.
- La mise en route avec ce simulateur est assez simple grâce à une conception claire du simulateur. [41]
- Il fournit également une puissante bibliothèque d'interfaces graphiques pour l'animation et la gestion du débogage.

V.4.2 Inconvénients :

- Peu de modèles pour les réseaux sans fil
- Il y a un manque cruel de protocoles disponibles dans la bibliothèque comparée à d'autres simulateurs. [41]

Partie De La Simulation :

Objectifs de la simulation : Le but de notre expérimentation est d'analyser la propriété « temps moyen d'établissement de routes ». Ce délai de découverte de routes est en fonction de plusieurs paramètres tels que la taille du réseau (le nombre de nœuds dans le réseau), la mobilité des nœuds du réseau. Dans nos simulations, on évalue cette propriété des protocoles AODV, SAODV en tenant compte du nombre et de la mobilité des nœuds du réseau. Si un nœud veut communiquer avec un autre et n'a pas une entrée dans sa table de routage pour cette destination spécifique, une procédure de découverte de route est initiée. Le temps pris pour découvrir cette route est important pour qualifier le protocole de routage. Ce qui nous intéresse est le temps entre l'envoi de la RREQ et la réception de la RREP correspondante ce qui est qualifié comme temps de découverte de route. Quand un nœud doit transmettre un paquet de données, il consulte d'abord sa table de routage pour s'assurer qu'il existe une entrée pour cette destination. S'il n'y a pas d'entrée, il stocke le paquet et diffuse le message RREQ. Après avoir reçu le message RREP, le nœud source transmet les paquets mémorisés. Les protocoles notent dans leurs fichiers de sortie le temps des découvertes. En consultant ces fichiers, il est possible de déterminer la moyenne de la « Route Discovery »

Les paramètres de simulation utilisés dans ces deux scénarios sont :

Nombre de nœuds	**5, 10,40**
Le Temps de simulation	**600s**
Bit rate	**2Mbps**
Transmission range	**200m**
Surface de simulation	**1000m*1000m**
Le protocole de routage	**AODV, SAODV**
Interfaces de routage	**Wlan**
Traffic type	**UDP App Basic**
Placement des nœuds	**Uniforme**

Différentes vitesses utilisées :

```
[Config humain]
    extends = Static
    # mobility
    **.host[*].mobility.angleDelta = normal(0deg, 30deg)
    **.host[*].mobility.speed = normal(2mps, 0.01mps)
[Config thon]
    extends = Static
    # mobility
    **.host[*].mobility.angleDelta = normal(0deg, 30deg)
    **.host[*].mobility.speed = normal(50)
[Config voiture]
    extends = Static
    # mobility
    **.host[*].mobility.angleDelta = normal(0deg, 30deg)
    **.host[*].mobility.speed = normal(80)
[Config avoin]
    extends = Static
    # mobility
    **.host[*].mobility.angleDelta = normal(0deg, 30deg)
    **.host[*].mobility.speed = normal(120)
```

Le Statique (Statique) représenté par :

```
# lifecycle
**.hasStatus = true
[Config Static]

**.host[*].mobility.typename = "StationaryMobility"

**.aodv.activeRouteTimeout = 3s

**.host[*].mobility.changeInterval = normal(5s, 0.1s)

**.host[*].mobility.angleDelta = normal(0deg, 30deg)
```

Topologie en 5 NŒUDS :

Dans ce scénario, trois nœuds source (S) envoyer des données aux nœuds (D), La destination des nœuds d'envoi :

```
*.host[0].app[0].destAddr = "host[1](ipv4)"

*.host[3].app[0].destAddr = "host[2](ipv4)"

*.host[4].app[0].destAddr = "host[3](ipv4)"
```

Et comme il n'y a pas de chemin établi préalablement entre le nœud source et le nœud destination dans chaque cas, cela nécessite de lancer le processus de découverte de routes par la diffusion des nœuds (S) d'un message de demande de route (RREQ) à ses voisins, y compris le numéro de séquence de cette destination. La demande de route est inondée en quelque sorte par le réseau jusqu'à ce qu'elle atteigne un nœud qui a une route à la destination où

La destination elle-même, comme illustré dans la figure suivante :

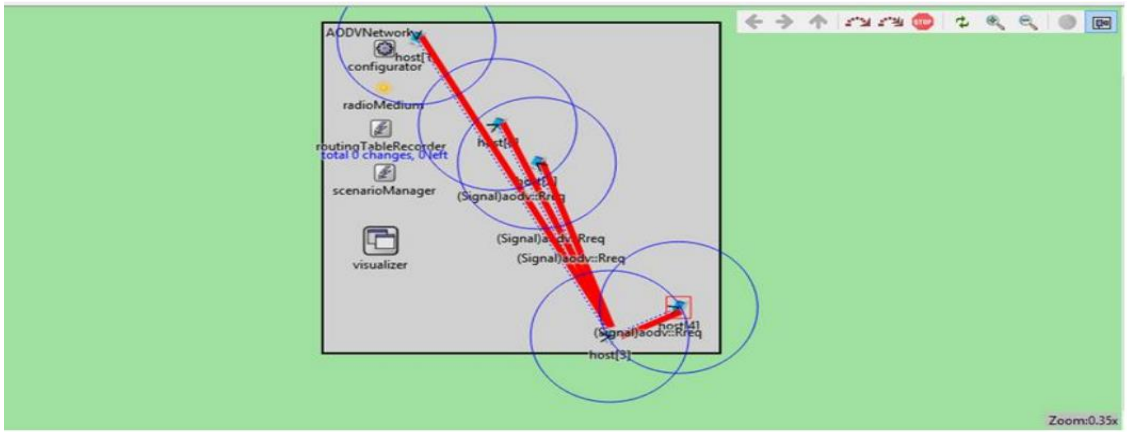

Figure V.8 : Lancement de la simulation

Une fois la simulation terminée, nous avons calculé le temps moyen entre la première RREQ envoyé par nœud source (S) et la RREP reçu depuis le nœud destination (D) pour chaque nœud dans et chaque vitesses (1.25mps/ 50mps/ 80mps/ 120mps) ce qui est illustré dans la figure suivante

Ensuite, dans le même scénario nous Secure, spécifiquement le protocole AODV en saodv mode transport. (La partie de la charge utile du paquet) sont cryptées et / ou authentifiées car dans le protocole AODV tous les nœuds sont à la fois routeurs et terminaux. Ceci est appliquer pour chaque voisin

Si (S) va envoyer paquets de routage à (D) et (C) est un nœud intermédiaire, alors dans ce cas le chemin entre (S) et (C) sera sécurisé et le chemin entre (C) et (D) sera aussi sécurisé, ainsi le chemin entre (D) et (C) devient systématiquement sécurisé. Dans ce cas, les paquets seront protégés de bout en bout

Comme nous savons que SAODV est utilisé pour assurer l'intégrité sans connexion, l'authentification de l'origine des données pour les et fournir une protection contre les rediffusions

La première étape pour protéger l'intégrité consiste à créer des hachages à l'aide d'un algorithme de hachage à clé, également connu sous le nom d'algorithme de code d'authentification de message (MAC). L'algorithme de hachage standard génère un hachage basé sur un message, tandis que l'algorithme de hachage à clé génère un hachage basé à la fois sur le message et la clé secrète partagée entre les voisins.

Le hachage est ajouté au paquet RREQ ou RREP et ce dernier est envoyé aux voisins un par un. A la réception du paquet de contrôle, le voisin recrée le hachage avec la clé partagée et S'assurer que les deux hachages correspondent, offrant ainsi une protection de l'intégrité du package La fonction de hachage SHA offre plus de sécurité que MD5

Dans cette simulation, nous avons utilisé l'algorithme de code d'authentification de message de hachage ((HMAC-SHA-1), qui effectue deux hachages liés :

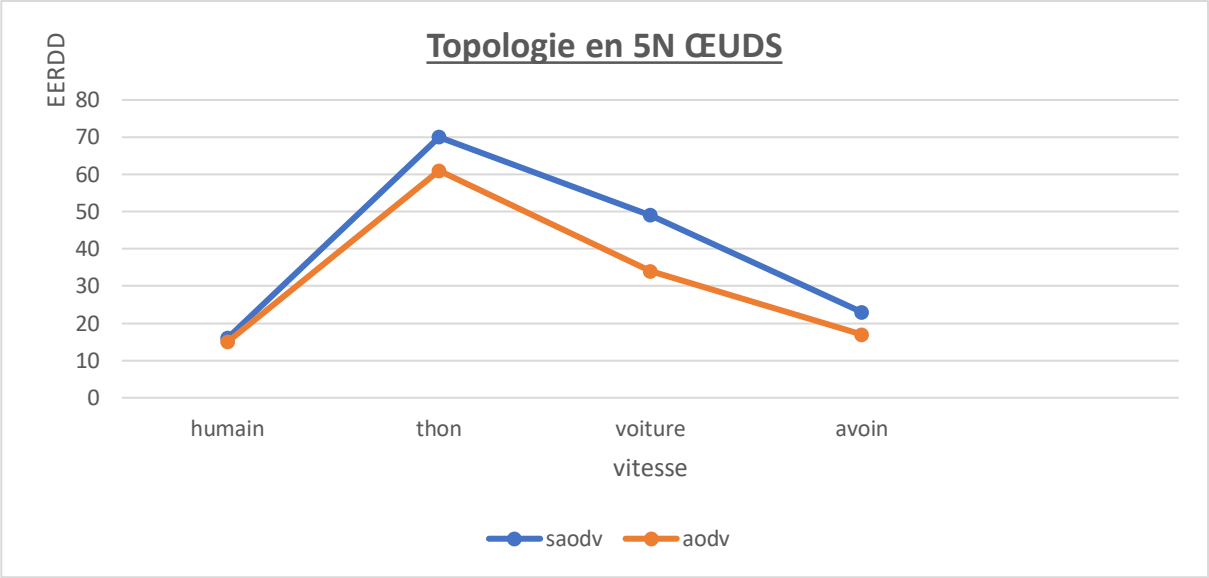

Figure V.12 : Le temps moyen entre RREQ et RREP Pour chaque Vitesse (m/s) (Avec AODV ET SAODV)

Aodv :

Dans le cas ‘’Humain ‘’, la surface de simulations est grande et la vitesse de déplacement des nœuds est faible, c’est difficile pour Host (0) et Host (3) de trouver un chemin vers leurs destinations durant le temps de la simulation. Dans ce scénario Host (4) est le seul à avoir reçu une route replay (RREP) depuis sa destination Host (3). Ce qi explique le faible temps de découverte de route.

Et dans le cas de ‘’ thon’’ la vitesse de déplacement des nœuds est supérieure par rapport à la vitesse ‘’Humain’’ En raison de la vitesse du thon, les nœuds peuvent se rapprochés dans plusieurs cas puis ils se détournent, ce qui permet de construire plusieurs routes durant la simulation cela explique l’augmentation, du temps moyen entre RREQ et la RREP comme illustré dans la figure (5.12). Au contraire dans le cas de ‘’voiture’’ et ‘’ avion’’ leurs grande vitesse de mouvements a donnée de la place pour faire converger les nœuds rapidement comme le montre la figure (5.12), c'est ce qu'il explique la diminution de temps moyen entre RREQ et RREP pour le "voiture" et le "avion".

Avec l’utilisation SAODV :

On remarque dans ce graphe que le temps moyen entre RREQ et RREP avec l'utilisation d’SAODV augmente par rapport au cas de routage sans l'utilisation d’SAODV, par un taux différent d'une vitesse à l'autre. À mesure que la vitesse de déplacement des nœuds augmente, la différence du temps moyen entre RREQ et RREP dans le cas où le protocole SAODV s'applique et le cas ordinaire augmente.

Topologie en 10N ŒUDS :

```
*.host[2].app[0].destAddr = "host[1](ipv4)"
*.host[3].app[0].destAddr = "host[2](ipv4)"
*.host[4].app[0].destAddr = "host[3](ipv4)"
*.host[8].app[0].destAddr = "host[3](ipv4)"
*.host[9].app[0].destAddr = "host[3](ipv4)"
```

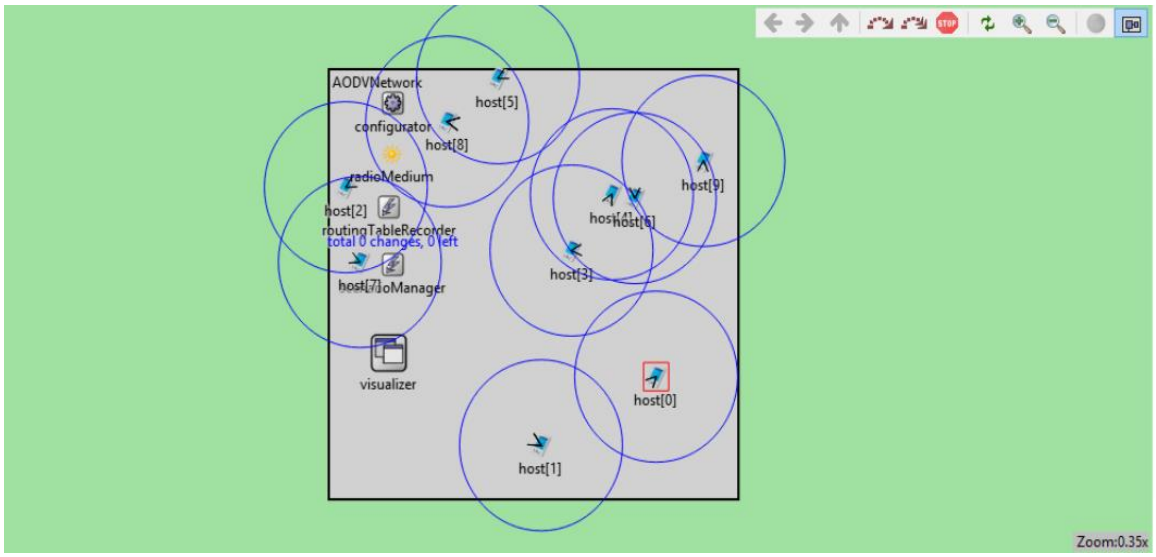

Figure V.13 : Topologies du réseau Avant lancement de la simulation

Dans le premier courbe, le réseau n'est pas protégé, ce qui signifie que le protocole saodv n'est pas appliqué. Alors que dans le second courbe, le protocole saodv sera appliqué aux messages de contrôle des nœuds du protocole AODV.

Et comme il n'y a pas de chemin entre les nœuds source et de destination dans chaque cas, cela nécessite de découvrir un chemin par la diffusion des nœuds (S) d'un message de demande de route à ses voisins.

Encore quand la simulation terminée, nous avons calculé le temps moyen entre la première RREQ envoyé par un nœud (S) et la première RREP qui a reçu depuis le nœud (D) pour chaque nœud dans les quatre vitesses (1.25mps/50mps/80mps/120mps) qui est illustré dans la figure suivante :

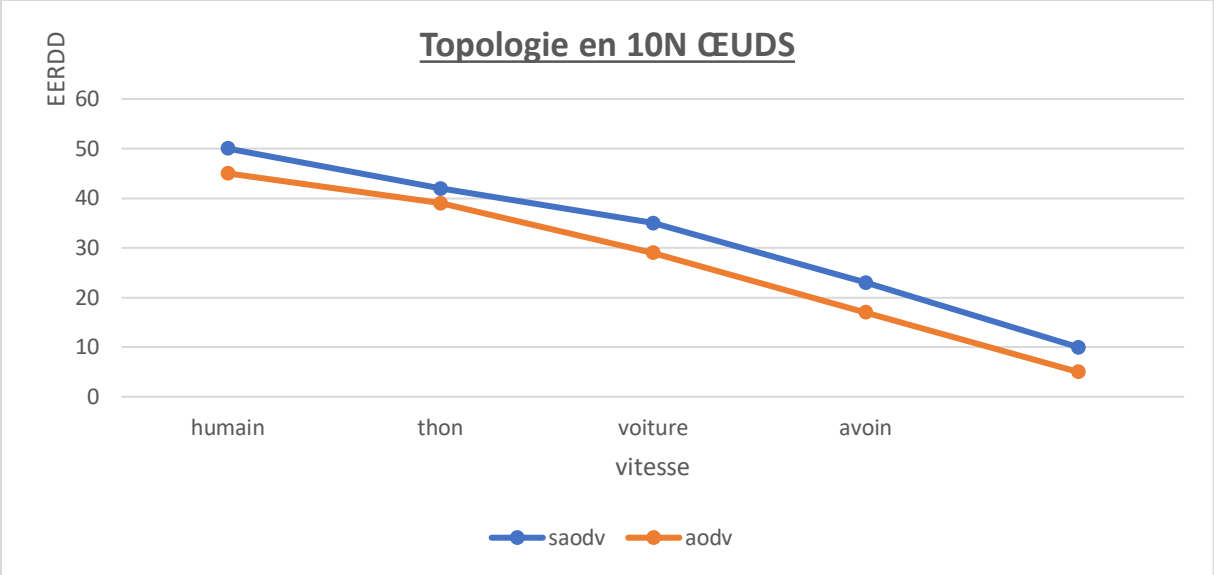

Figure V.17 : Le temps Moyen entre RREQ et RREP Pour chaque Vitesse (m/s) (Avec saodv et aodv)

Aodv :

On remarque qu'au fur et à mesure que la vitesse de déplacement des nœuds augmente, le temps moyen entre RREQ et RREP diminue. Puisque le réseau est dense les routes sont construites fréquemment ce qui augmente le temps de découverte de routes par rapport au scénario de 5 nœuds.

Avec l'utilisation d'SAODV :

On remarque dans ce graphe que le temps moyen entre RREQ et RREP avec l'utilisation d'SAODV a augmenté par rapport au cas de routage sans l'utilisation d'SAODV, par un taux différent d'une vitesse à l'autre. À mesure que la vitesse de déplacement des nœuds augmente, la différence du temps moyen entre RREQ et RREP dans le cas où le protocole SAODV s'applique et le cas normal augmente. La différence du temps moyen entre RREQ et RREP d'une vitesse à l'autre dans le cas où le protocole saodv s'applique et le cas qu'il n'est pas applicable dans le de réseau à 5 nœuds est inférieur à la différence du temps moyen entre RREQ et RREP dans le cas où le protocole saodv s'applique et le cas qu'il n'est pas applicable dans le de réseau de 10 nœuds.

Topologie en 40N ŒUDS :

Nous appliquerons les mêmes étapes précédentes à un réseau de 40 nœuds Dans ce réseau, Cinque nœuds (S) envoient des données aux nœuds (D),

La destination des nœuds d'envoi :

```
*.host[2].app[0].destAddr = "host[1](ipv4)"
*.host[3].app[0].destAddr = "host[2](ipv4)"
*.host[4].app[0].destAddr = "host[3](ipv4)"
*.host[8].app[0].destAddr = "host[3](ipv4)"
*.host[9].app[0].destAddr = "host[3](ipv4)"
*.host[10].app[0].destAddr = "host[1](ipv4)"
*.host[12].app[0].destAddr = "host[2](ipv4)"
*.host[14].app[0].destAddr = "host[4](ipv4)"
*.host[15].app[0].destAddr = "host[5](ipv4)"
*.host[17].app[0].destAddr = "host[5](ipv4)"
```

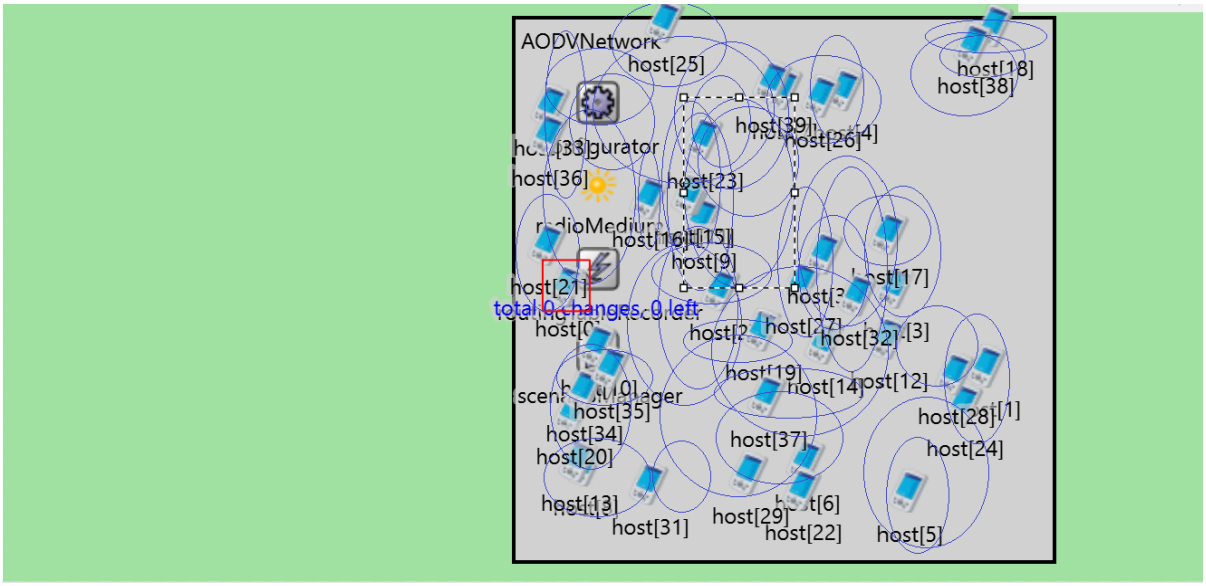

Figure V.13 : Topologie du réseau Avant lancement de la simulation

Et comme il n'y a pas de chemin entre les nœuds source et de destination dans chaque cas, cela nécessite de découvrir un chemin par la diffusion des nœuds (S) d'un message de demande de route à ses voisins.

Encore quand la simulation terminée, nous avons calculé le temps moyen entre la première RREQ envoyé par un nœud (S) et la première RREP qui a reçu depuis le nœud (D) pour chaque nœud dans les quatre vitesses (1.25mps/50mps/80mps/120mps) qui est illustré dans la figure suivante :

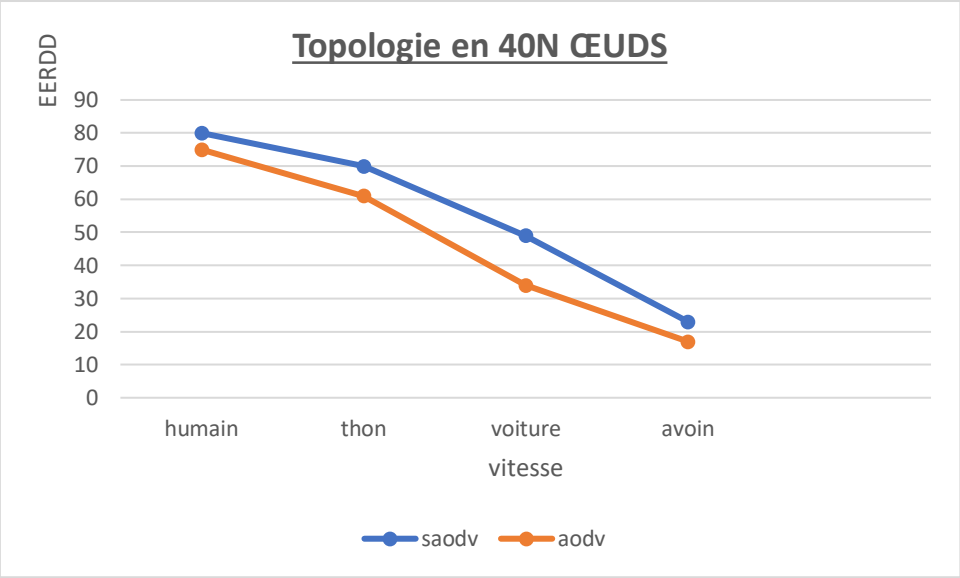

Figure V.17 : Le temps moyen entre RREQ et RREP Pour chaque Vitesse (m/s)

On remarque dans ce graphe que le temps moyen entre RREQ et RREP avec l'utilisation d'saodv a augmenté par rapport au cas de routage sans l'utilisation saodv, par un taux différent d'une vitesse à l'autre.

AODV :

- **Latence** : La latence de découverte de route est généralement faible en raison du petit nombre de nœuds.
- **Surcharge** : La surcharge est minimale puisque le trafic de contrôle est limité
- Peut diminuer si les chemins de routage deviennent instables ou s'il y a une congestion dans le réseau.

SAODV :

- **Latence** : La latence peut être légèrement supérieure à celle d'AODV en raison du temps supplémentaire nécessaire pour les opérations cryptographiques.
- **Surcharge** : Une légère augmentation de la surcharge due aux signatures numériques et à la vérification des messages.
- Peut également diminuer, mais l'intégrité des données est mieux protégée contre les attaques

Dans les deux scénarios, SAODV fournit une sécurité accrue par rapport à AODV mais au coût d'une surcharge de routage plus élevée, d'une consommation d'énergie accrue et d'un délai de bout en bout plus long. Dans un petit réseau de 5 nœuds, ces surcoûts sont moins prononcés, tandis que dans un réseau de 40 nœuds, l'impact de la sécurité sur les performances est plus significatif.

Conclusion :

En raison de diverses applications sensibles des réseaux Adhoc, la cohésion et l'intégrité du réseau doit être assurée, mais garantir une sécurité complète dans un tel réseau est couteuse si les nœuds sont très mobiles et le réseau es dense.

V.5 Conclusion générale :

Les Manets se présentent comme des réseaux sans fil dans lesquels les équipements peuvent avoir des configurations différentes, et qui doivent coopérer pour assurer l'existence de tels réseaux et la communication entre les équipements du réseau. Les Manets utilisent le lien radio. Ceci permet à un nœud malicieux d'interférer facilement pour perturber le fonctionnement du réseau.

Les protocoles de routage présentent des défis difficiles dans la sécurisation du routage, et donc la sécurité de ces réseaux est un prérequis pour leurs déploiements.

Il faut non seulement éviter de nombreuses attaques, mais aussi assurer la fiabilité des routages du réseau, car il existe plusieurs attaques qui ont comme but de surcharger le protocole, ce qui donne des effets néfastes sur le comportement du protocole.

Parmi ces attaques ; les attaques contre le protocole de routage AODV qui incluent attaque de largage de paquets, attaque par numéro de séquence, attaque de modification de champ ainsi attaque d'ajout de champ. Ce type d'attaques peut représenter une menace importante pour dégrader le bon fonctionnement du protocole.

Dans notre mémoire on a évalué une extension au protocole AODV qui garantit la protection des paquets de routage, en termes de EERDD suivant diffèrent scenario en variant la mobilité et la densité du réseau Manet. On a constaté que SAODV est relativement pénalise les performances du réseau par rapport au ADOV. Ceci est acceptable vue les garanties offertes par SAODV.

Bibliographie

- [1] : Y. MELOUK, S. MOUHLI, Sécurité contre les attaques liées aux identités dans les réseaux Ad hoc, mémoire de fin d'études, Faculté des Sciences Exactes, Département d'Informatique, Université ABDERRAHMANE Mira Bejaïa, 2015/2016.
- [2] Hemaizia Zineb, Aissaoui Bouthaina." Un protocole de routage optimisé dans les réseaux Ad Hoc" Mai 2016
- [3] Fatima AMEZA."Les technologies sans fil : Le routage dans les réseaux ad hoc (OLSR et AODV)", Licence 2007.
- [4] Nadjette & Hanane MOUICI & BOUKHALFA. "L'impact des attaques sur la fiabilité des réseaux ad hoc", Master 2-2015.
- [5] Melle. Saloua CHETTIBI ; "Protocole de routage avec prise en compte de la consommation d'énergie pour les réseaux mobile Ad Hoc". Université Mentouri Constantine, 2008.
- [6] Nadir BOUKHECHEM, « Routage dans les réseaux mobiles Ad Hoc par une approche à base d'agents ». Promotion 2007-2008.
- [7] Ameza Fatima, Assam Nassima, Atmani Mouloud, Le routage dans les réseaux Ad Hoc (OLSR et AODV), Licence en informatique, Université Abderrahmane Mira BÉJAÏA, 2007.
- [8] Mohamed Ali AYACHI, Contributions à la détection des comportements malhonnêtes dans les réseaux Ad Hoc AODV par analyse de la confiance implicite, Thèse de doctorat : Université de Rennes 1, 24/02/2011.
- [9] Ahizoune Ahmed, Un protocole de diffusion des messages dans les réseaux véhiculaires, Thèse de Maîtrise ès sciences (M. Sc.) de l'Université de Montréal, Avril 2011.
- [10] Nadir BOUCHAMA, Qualité de Service dans les Réseaux Mobiles Ad Hoc, Centre de Recherche sur l'Information Scientifique & Technique, Division Théorie & Ingénierie des Systèmes Informatiques (DTISI), 08/06/2010
- [11] Nabila LABRAOUI, La sécurité dans les réseaux sans Fil Ad Hoc, Thèse de DOCTORAT, Université de Tlemcen, 2012
- [12]M elle BESSAIH Aldja M me BOUCHAKEL Siham. "Routage et simulation dans les réseaux mobiles ad hoc", 2017, Université A/Mira de Béjaia.

- [13] Ait Ali Kahina, Modélisation Et Etude De Performances Dans Les Réseaux VANET. Thèse de doctorat de l'Université de Technologie de Belfort-Montbéliard, 16 /10/ 2012.
- [14] R. Meraihi ; "Gestion de la qualité de service et contrôle de topologie dans les réseaux ad hoc" ; Thèse de doctorat, École nationale supérieure des télécommunications, Paris, 2004.
- [15] Khadîdja AYAD, Sécurité du routage dans les réseaux Ad Hoc mobile, Thème de MAGISTER Option : Informatique Répartie et Mobile, 14 /11/ 2012
- [16] Amadou Adama Ba., Protocole de routage basé sur des passerelles mobiles pour un accès Internet dans les réseaux véhiculaires, Thèse de doctorat, l'université de Montréal, Avril 2011.
- [17] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, 2006 Springer
- [18] International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.2, Issue.3, May June 2012 pp-728-732
- [19] https://www.rfc-editor.org/rfc/pdfrfc/rfc3561.txt.pdf
- [20] Y. Yahia Tène, "Traffic Encryptions Keys distribution modeles in Mobile Ad hoc Networks (Distribution de clés dans un réseau dynamique)", mémoire de magister de l'Université M'hammed Bougara, Boumerdes, 2011
- [21] https://sg.inflibnet.ac.in/bitstream/10603/207580/12/12_chapter3.pdf
- [22] Cours sur internet « Les réseaux mobiles Ad hoc et les protocoles de routage ».
- [23] Loufti NUAYMI Valérie Gay rand « La sécurité dans les réseaux Ad hoc », université ENST Bretagne
- [24] Omar Cheikhrouhou « La sécurité des réseaux Ad hoc », mémoire d'ingénieur d'état en informatique, Ecole Sfax tunisien, 2005.
- [25] Livre « La sécurité dans les réseaux sans fil et mobiles » sous la direction de Hakima CHAOUCHI et Maryline Laurent-Maknavicius, Lavoisier ,2007.
- [26] E. Perkins, E. M. Belding-Royer, and S. R. Das. Ad hoc on-demand distance vector (AODV) routing. Internet Request for Comments RFC 3561, Nov. 2003.
- [27] M.G Zapata. Securing and Enhancing Routing Protocols. Submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy Doctorate in Computer Architecture and Technology Computer Architecture Department (DAC) for Mobile Ad hoc Networks. Barcelona, March 2006