République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Faculté des Sciences Exactes et Sciences de la Nature et de la Vie

Université de Tébessa

Département des mathématiques et informatique

MEMOIRE DE MASTER

Domaine: Informatique
Filière : Mathématiques / Informatique
Option : Réseaux et sécurité informatique

THÈME :

L'impact des attaques sur la fiabilité du routage dans les réseaux Ad Hoc

Présenté par :

M^{elle} Hanane BOUKHALFA.
M^{me} Nadjette MOUICI.

Devant le jury:

Président :	**M^{r}** Tarek NOUIOUA.	M.A.A	Université de Tébessa
Encadreur :	**M^{r}** Rachid MAHMOUDI.	M.A.A	Université de Tébessa
Examinateur :	**M^{r}** Samir TAG.	M.A.A	Université de Tébessa

Date de soutenance : 29/05/2016.

Note : **Menton :**

Remerciements

Nous tenons tout d'abord à remercier notre encadreur monsieur Rachid MAHMOUDI pour la confiance qu'il nous a accordée, ainsi que pour toute l'aide et tous les encouragements qu'il nous a apporté dans les moments les plus difficiles.

Nous adressons nos sincères remerciements à tous les professeurs et tout le personnel de département mathématiques et d'informatiques, et surtout les membres de jury, pour son rôle d'examinateur.

Nous remercions également nos familles ainsi que nos amis pour leurs soutiens durant toute la période de rédaction de ce mémoire.

Résumé

Réseau Mobile Ad Hoc (MANET) est l'un des domaines le plus vaste pour la recherche et l'examen du réseau sans fil. Les réseaux Ad Hoc sont des nœuds mobiles communiquent sans infrastructure, à travers des ondes radio. Ces réseaux sont utilisés dans plusieurs domaines comme les applications militaires, les opérations de secours, les applications industrielles, les réseaux véhiculaires...etc. Une exigence essentielle dans MANET est la sécurité des réseaux, les réseaux Ad Hoc plus vulnérable aux différentes attaques telles que l'attaque par l'inondation (Flooding). L'inondation de réseau est un type de déni de service (DoS) sur MANET. Son but peut conduire à des surcharges dans le réseau, ce qui permet une dégradation des performances, à cause de circulation des paquets non valides. Dans ce mémoire nous allons essayer de réaliser ce type d'attaque « RREQ Flooding » sous le protocole réactif AODV. Nous avons analysé dans ce travail l'impact de cette attaque en utilisant le simulateur OPNET. Les tests montrent que ce type d'attaque peut dégrade la performance du réseau jusqu'à 600%.

Mots clés : réseau, protocole de routage, AODV, OPNET, Sécurité, AD HOC, Flooding, simulation.

Abstract

Mobile Ad Hoc Network (MANET) is one of the largest areas for research and review of the wireless network. Ad Hoc networks of mobile nodes communicate without infrastructure, through radio waves. These networks are used in many fields such as military applications, emergency operations, industrial application, vehicular networks.... An essential requirement in MANET is the security of Ad Hoc networks, Ad Hoc networks more vulnerable to various attacks such as the attack by inundation (Flooding). Flooding is a type of denial of service (DoS) on MANET. Its purpose can lead to overloading of the network, enabling performance degradation, due to movement of invalid packets. In this paper we will try to achieve this type of attack RREQ Flooding as reactive AODV protocol. We analyze in this work the impact of this attack by using the OPNET simulator. Tests show that this type of attack can degrade network performance up to 600%.

Key words: Network, Protocol of routing, AODV, OPNET, Security, Ad Hoc, Flooding, simulation.

مـــــــلـــــــخـــــــص

الشبكة المتحركة Ad Hoc (MANET) هي واحدة من أوسع مجالات البحث واختبار الشبكات اللاسلكية.
شبكات Ad Hoc هي عبارة عن مجموعة من العُقَد المتحركة متصلة فيما بينها بدون بنية تحتية، عن طريق موجات الراديو. هذه الشبكات مستعملة في العديد من المجالات مثل التطبيقات العسكرية وعمليات الطوارئ، والتطبيقات الصناعية وشبكات المركبات ... الخ، احتياج مهم في شبكات MANET هو امن الشبكات Ad Hoc. شبكات Ad Hoc تعاني من عدة هجومات مثل الهجوم بالفيضانات (gnidoolF)، وهذه الشبكات أكثر عرضة للهجمات المختلفة مثل هجوم الفيضانات (gnidoolF). الفيضانات في الشبكة هو حرمان من الخدمة (DoS) في MANET. الهدف منه يمكن أن يقود إلى إثقال الشبكة، مما يسمح الى تدهور الأداء بسبب حركة الحزم غير الصالحة.
في هذه المذكرة حاولنا انشاء هذا النوع من الهجوم "RREQ gnidoolF"، تحت نطاق البروتوكول AODV. حللنا في هذا العمل تأثير هذا الهجوم باستخدام برنامج المحاكاة OPNET، وقد أثبتت التجارب أن هذا النوع من الهجمات، يمكن أن يؤدي إلى تراجع الأداء الجيد للشبكة بنسبة تصل حتى 600 ٪.

الكلمات المفتاحية:

شبكة، بروتوكول التوجيه، AODV ،OPNET ، الحماية، Ad Hoc، الفيضانات، المحاكاة.

Liste des figures

Chapitre 1 Généralités sur les Réseaux AD HOC et Les Protocoles de routage

Chapitre 2 Sécurité et Attaques des réseaux Ad Hoc

Chapitre 3 Simulation et simulateur

Chapitre 4 Attaque par inondation dans Réseau Ad Hoc

Chapitre 5 L'impact de l'attaque RREQ Flooding sur la fiabilité de protocole de routage AODV dans les réseaux Ad Hoc.

Chapitre 6 Tests et résultats

Premier scénario

Deuxième scénario

Troisième Scénario

Liste des tableaux

Table des matières

Chapitre2 : Sécurité et Attaques des réseaux Ad Hoc

Chapitre3 : Simulations et simulateurs

Chapitre4 : Attaque par inondation (Flooding) dans Réseau Ad Hoc

Chapitre5 : L'impact de l'attaque RREQ Flooding sur la fiabilité de protocole de routage AODV dans les réseaux Ad Hoc.

Chapitre6 : Tests et résultats

Liste d'abréviation

ACA	Autonome Component Architecture.
AHFA	Ad Hoc Flooding Attack.
AODV	Ad Hoc On-demand Distance Vector.
ATM	Asynchronous Transfer Mode.
CBQ	Class Based Queuing.
CBR	Constant Bit Rate.
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance.
CSMA/CD	Carrier Sense Multiple Access/Collision Detection.
DDoS	Distributed Denial of services.
DoS	Denial of services.
DRR	Disaster Risk Reduction.
DSDV	Destination Sequenced Distance Vector.
DSR	Dynamic Source Routing.
DVMPR	Destination Sequenced Multi Point Relay.
FAP	Flooding Attack Prevention.
FDDI	Fiber Distributed Data Interface.
FTP	File Transfert Protocol.
GPRS	General Packet Radio Service.
GSM	Global System for Mobile Communications.
GSR	Global State Routing.
GUI	Graphical User Interface.
HLA	high Level Architecture.
IEEE	Institute of Electrical and Electronics Engineers.
IERP	IntEr zone Routing Protocol.
INET	Inter networking.
IP	Internet Protocol.
J-SIM	Java Simulator.
MAC	Media Access Control.
MAC-OS	Macintosh Operating System.
MANET	Mobile Ad Hoc Network.
MPR	Multi Point Relay.
NED	Network Editor Graphic.
NS	Numéro de séquence.
NS-2	Network Simulator-2.
OLSR	Optimized Link State Routing Protocol.
OMNET++	Objective Modular Network Tested in C++.
OPNET	Optimized Network Engineering Tools.
OSI	Open System Interconnexion.
OTcl	Object Tool Command Language.
PDA	Personal Digital Assistant.
Perl	Practical Extraction and Report Language.

PRNET	Packet Radio Network.
QoS	Quality Of Service.
RCSF	Réseaux de Capteurs Sans Fils.
RCSF	Réseau de Capteur Sans Fil.
RERR	Route Error Message.
RREP	Route Reply Message.
RREQ	Route Request Message.
RRFA	Route Request Flooding Attack.
RTP	Real-time Transport Protocol.
RUV	Run User Virtual.
SRM	Scalable Reliable Multicast.
SURAN	Survivable Adaptative Radio Network.
TC	Topology Control.
Tcl	Tool Command Language.
TCP	Transmission Control Protocol.
TelNet	Telecommunication Network.
UDP	User Data Protocol.
UIT	Union Internationale des Telecommunications.
UMTS	Universal Mobile Telecommunications System.
VANET	Vehicule Ad Hoc Network.
VoIP	Voice Over Internet Protocol.
WIFI	Wireless Fidelity.
WIMAX	Worldwide Interoperability for Microwave Access.
WLAN	Wireless Local Area Network.
WMAN	Wireless Metropolitan Area Network.
WPAN	Wireless Personal Area Network.
WWAN	Wireless Wide Area Network.
ZRP	Zone Routing Protocol.

Introduction générale :

Le développement de la technologie sans fil ouvre de nouvelles perspectives dans le domaine des télécommunications. Les réseaux mobiles basés sur la technologie sans fil connaissent aujourd'hui une forte expansion. Les réseaux mobiles (MANET) offrent une grande flexibilité d'emploi, ils permettent aux utilisateurs de se déplacer librement tout en continuant normalement leurs communications.

Il existe deux types de réseaux mobiles, les réseaux mobiles avec infrastructure et les réseaux mobiles Ad Hoc. Les réseaux Ad Hoc en contrepartie n'ont besoin d'aucune infrastructure fixe préexistante.

Les nœuds se déplacent librement dans une certaine zone géographique et forment ensemble d'une manière dynamique un réseau interconnecté. Pour pouvoir communiquer entre eux chaque unité mobile doit jouer le rôle d'un routeur et d'un terminal, et doit retransmettre les paquets des autres unités mobiles.

En effet à cause de la mobilité des nœuds il est très difficile de localiser une destination à un instant donné. Plusieurs protocoles de routage pour les réseaux Ad Hoc ont été développés, chaque protocole essaye de maximiser les performances du réseau. Les algorithmes de routage pour les réseaux Ad Hoc peuvent se classer en trois catégories, les protocoles proactifs, les protocoles réactifs et les protocoles Hybrides.

Les protocoles de routage Ad Hoc offrent un grand problème de sécurité entre les entités communiquées. Les réseaux Ad Hoc sont vulnérables à différents types d'attaques, comme les attaques d'inondation, Trou noir, trou de ver, etc., qui sont lancés forcement avec des nœuds malveillants ou attaquants. Il n'existe pas des études complètes sur l'impact de ces attaques dans les réseaux Ad Hoc, On a décidé dans notre mémoire d'entamer le sujet des effets de l'attaque Flooding sur la fiabilité de routage dans les réseaux Ad Hoc.

- ## Problématique

Le grand problème qui se trouve dans le réseau Ad Hoc, est la sécurité. Notre étude offre principalement une analyse sur l'impact des attaques sur la fiabilité du routage dans les réseaux ad hoc. Parmi les attaques qui peut toucher la sécurité des réseaux Ad Hoc, est l'attaque de Flooding, parce qu'elle dégrade le bon fonctionnement des réseaux Ad Hoc.
On peut résumer la problématique de notre travail comme suit :

- Comment créer un réseau Ad Hoc et activer le protocole AODV dans ce réseau, et générer une attaque Flooding sur ce réseau?
- Quelles sont les métriques appropriées pour analyser l'impact de dégradation de la performance de réseau attaqué par Flooding?
- Quelle est la méthode utilisée pour détecter l'impact de cette attaque sur le réseau ?
- Identification de différents paramètres influant sur la puissance de l'attaque et l'attaquant ?

- **Objectif de ce travail**

Dans le cadre de ce mémoire, nous nous intéresserons au problème de sécurité dans les réseaux Ad Hoc et en particulier le problème de Flooding. Dans cette vision nous allons essayons d'analyser ce problème par approche de simulation sous OPNET, par les étapes suivantes :

- Création et simulation de l'attaque Flooding, (inondation de réseau par des paquets à des destinations hors réseau) sur un réseau Ad Hoc routé par le protocole de routage réactif AODV.
- Analyser l'impact de cette attaque à travers des métriques de performances.
- Comparaison des résultats de simulation par des scénarios sans attaques et d'autres avec attaques, pour démontrer ces effets sur Ad Hoc,
- Création de plusieurs scenarios en modifiant à chaque fois un paramètre tel que nombre d'attaquants, nombre de fois de tentative de découverte de route.

- **Organisation du mémoire :**

Nous avons organisé notre mémoire en six chapitres :

Le premier chapitre nous détaillons l'étude sur les réseaux Ad Hoc. Ainsi nous commençons par une présentation des caractéristiques, avantages et inconvénients de ce type de réseaux en plus nous décrivons les principaux protocoles de routage proposés et leur Classification dans ce type de réseau.

Le deuxième chapitre nous introduisons, les concepts et les terminologies fondamentales de la sécurité.sa définition, ces principaux objectifs. Où cette partie sera consacrée à l'étude des exigences de la sécurité, les différentes vulnérabilités liées aux protocoles de routage Ad Hoc, ainsi que les types d'attaques qui peuvent les menacées.

Le troisième chapitre nous commençons par détailler des différents types des simulateurs « NS-2, OMNET++, JSIM, OPNET », et comparaison entre eux, pour garantir notre choix « OPNET », et les critères générale de utiliser un simulateur.

Le quatrième chapitre nous allons présenter l'attaque Flooding, ses types et leur principe ainsi que ces effets, la deuxième partie on a présenté quelques travaux connexes. Enfin on a expliqué notre contribution.

Le cinquième chapitre nous allons présenter la description de l'attaque Flooding, et les étapes de création sous OPNET, et définir les paramètres de base pour obtenir cette attaque.

Le sixième chapitre présente tous les tests et les résultats sous forme de graphes, à travers de trois scenarios on teste l'impact de l'attaque, dans le premier scénario on teste l'effet de nombre d'attaquants, dans le deuxième scenario on teste l'influence de nombre de tentative de découverte de la route sur la puissance de l'attaque, et en fin on teste la performance réseau par l'attaquant le plus puissant dans le troisième scenario.

Chapitre 1 :

Généralités sur les Réseaux AD HOC Et Les Protocoles de routage

1. Introduction

L'évolution récente de la technologie dans le domaine de la communication sans fil et l'apparition des unités de calcul portables poussent aujourd'hui plusieurs domaines de recherches.

Dans ce chapitre, nous allons présenter des généralités sur les réseaux sans fil et les deux classes qui le constituent (mode infrastructure et mode sans infrastructure) et les principaux concepts liés à ce type. Nous donnons ensuite le concept des réseaux Ad Hoc et les caractéristiques différentes à ces réseaux et leurs domaines d'application. Dans la deuxième partie de ce chapitre, nous présentons le routage dans les réseaux Ad Hoc en définissant quelques protocoles de routage les plus connus dans ce domaine.

2. Réseaux informatiques

Les réseaux informatiques sont des réseaux de communication, nés du besoin d'interconnecter un ensemble des équipements terminaux situés à distance les uns des autres. Pratiquement, ils misent à la disposition de ces équipements des ressources afin de transporter les données d'une source à un ou plusieurs destinataires selon des règles bien définies. **[1]**

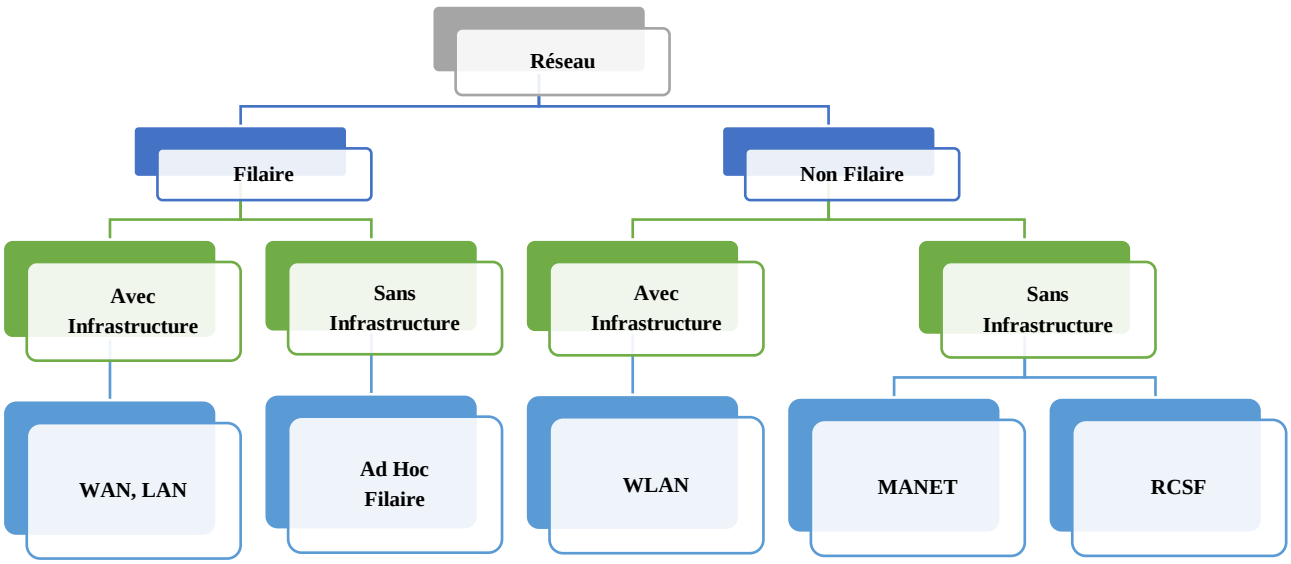


Figure 1.1: Classification des réseaux de communication. **[20]**

3. Réseaux sans fil

3.1. Définition

Un réseau sans fil (Wireless network) c'est un cas particulier des réseaux informatiques, dans lequel au moins deux équipements (ordinateur, PDA, imprimante, routeur…), peuvent communiquer sans liaison filaire. Néanmoins, il recourt à des ondes radios comme un support de transmission. Il est plutôt considéré comme une extension de réseau filaire existant, et non pour le remplacer, offrant l'avantage d'une connectivité sans fil. **[1]**

Figure 1.2 : Réseau sans fils**. [24]**

3.2. Type des réseaux sans fil

Les réseaux mobiles ou sans fil, peuvent être classés en deux catégories : les réseaux avec infrastructure (cellulaire) et les réseaux sans infrastructure (Ad Hoc).

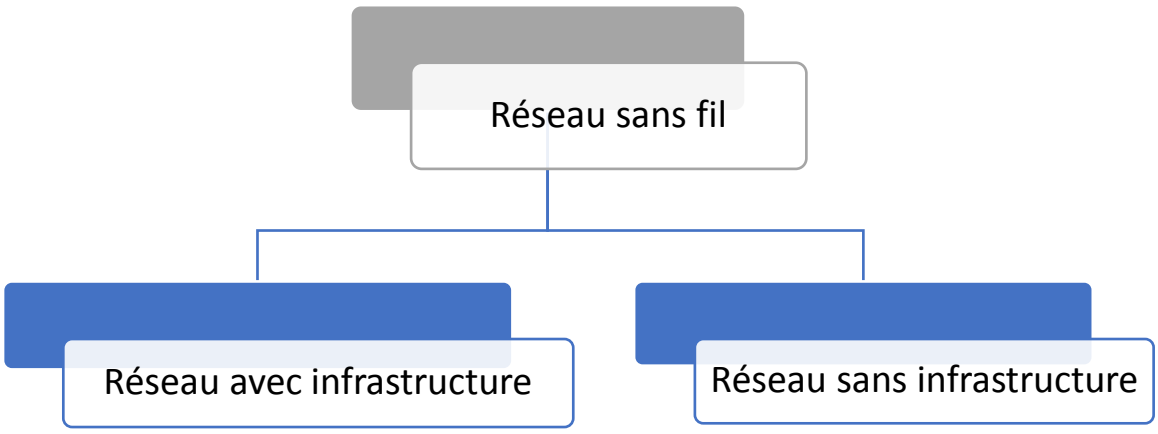


Figure 1.3: Types des réseaux sans fil. **[2]**

3.2.1. Réseaux avec infrastructure

Les réseaux de communications cellulaires sont Basée sur une topologie centralisée, cette technologie consiste à découper un territoire en zone (cellules), chacune est desservie par une station de base (le point central). Toutes les communications doivent passer par ce point central qui a pour rôle de les acheminer à leurs destinations. **[2]**

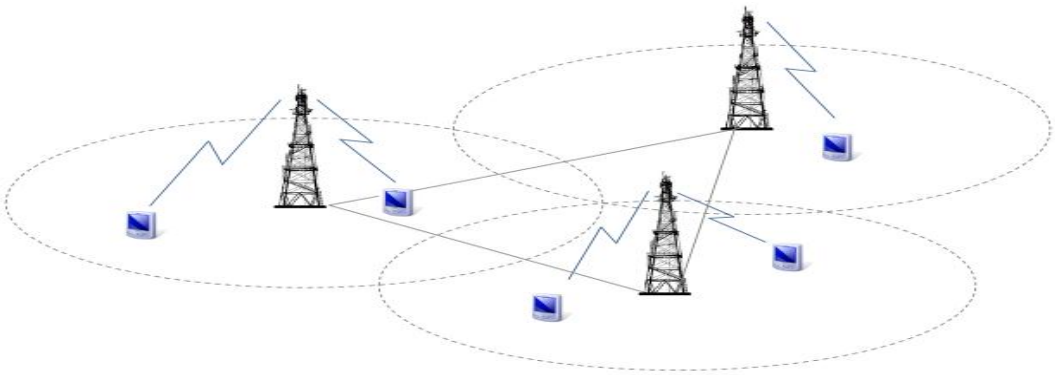


Figure 1.4 : Mode avec infrastructure. **[2]**

3.2.2. Réseaux sans infrastructure

Les réseaux Ad Hoc mobiles MANET (**M**obile **Ad Hoc NET**works) ne nécessitent pas une infrastructure fixe (des antennes relais ou satellite), pour acheminer les messages d'un nœud vers un autre. Le principe des réseaux Ad Hoc est basé sur la coopération entre les différents nœuds du réseau. En effet, chaque nœud communique directement avec ses voisins, qui se chargent de retransmettre les messages jusqu'à leur destination. **[2]**

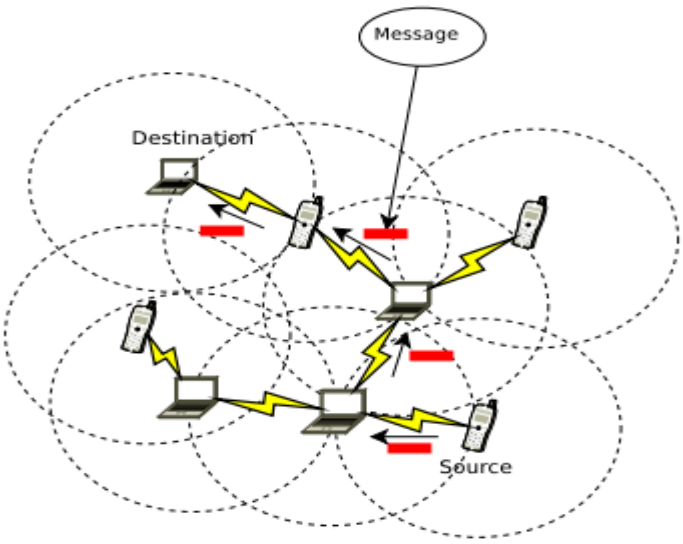


Figure 1.5 : Mode sans infrastructure. **[22]**

3.3. Avantages et inconvénients des réseaux sans fil

Les réseaux sans fil présentent plusieurs avantages et aussi des inconvénients.

Avantages	Inconvénients
• L'usage facile dans les endroits à câblage difficile. • La réduction du temps de déploiement et d'installation. • La réduction des coûts d'entretien. • L'augmentation de la connectivité. • La réduction de l'encombrement.	• Obligation de respecter les réglementations relatives aux transmissions radioélectriques. • Sensibilité aux interférences. • Problèmes liés au franchissement des obstacles. • Difficultés de contrôler la propagation du signal, donc difficultés de contrôler la sécurité du réseau.

Tableau 1.1 : Les avantages et les inconvénients d'un réseau sans fil. **[24]**

4. Différentes technologies sans fil

Il existe plusieurs technologies sans fil qui permettent la mise en place de réseaux sans fil .Ces technologies peuvent être classifiées selon les normes des réseaux sans fil utilisés:**[4]**

- **L'IEEE 802.15 (Bluetooth) :** utilise les ondes radio dont la bande de fréquence est située entre 2,4 et 2,4835 GHz. Cette technologie est destinée à la communication entre différents appareils à très courte distance (souris sans fil).

- **l'IEEE 802.11 (Wi-Fi) :** est la norme la plus utilisé à ce jour dans les réseaux maillés sans fil. Elle a été conçue pour des réseaux de courtes distances (une centaine de mètres en moyenne). Il existe plusieurs versions de cette norme selon la bande de fréquence utilisée. La version IEEE 802.11a a une bande de fréquence située autour de 5 GHz, l'IEEE 802.11b et IEEE 802.11g opèrent sur 2,4 GHz. L'IEEE 802.11n peut fonctionner aussi bien avec la bande 2,4 GHz qu'avec 5 GHz. Les débits varient de 1 à 54 Mbps suivant la norme et ses éventuelles extensions. C'est la technologie qu'on utilise dans nos travaux.

- **l'IEEE 802.16 (WIMAX)** : est de plus en plus prisée dans les RMSF. Elle permet des connexions de plusieurs dizaines de kilomètres avec des débits pouvant atteindre 100 Mbps. Elle est destinée au WMAN. **[4]**

Figure 1.6 : Type des réseaux sans fils**. [5]**

5. Réseaux Ad Hoc

Les réseaux Ad Hoc représentent la deuxième catégorie des réseaux sans fil sans infrastructure.

5.1. Historique

L'histoire des réseaux Ad Hoc a commencé en 1972 avec une initiative du département de la défense américaine qui a subventionné le projet PRNET (Packet Radio Network). Par la suite, ce projet a donné naissance au projet SURAN (Survivable Adaptative Radio Network) au début des années 90. Le but de ces deux projets était de créer un réseau sans fil et sans infrastructure capable d'acheminer les données par voie radio souvent utilisée dans le domaine militaire.

L'introduction du standard 802.11 par l'IEEE a ouvert les portes pour une utilisation des réseaux Ad Hoc dans les applications civiles. **[5]**

5.2. Définition

Les réseaux Ad Hoc, appelés aussi MANET (Mobile Ad Hoc Network) sont formés dynamiquement par un grand nombre de stations mobiles (nœuds) qui se connectent sans utiliser d'infrastructure existante en utilisant comme moyen de communication des interfaces sans fil (ondes radio).

Les nœuds interagissent et peuvent coopérer pour s'échanger des services. Ces nœuds sont donc libres de se déplacer, impliquant une grande variabilité de la topologie du réseau. Chaque nœud est capable de communiquer directement avec ses voisins (se trouvant dans la zone de portée de leur antenne), voisins par lesquels passent les informations pour communiquer avec des nœuds plus éloignés donc peuvent servir comme relais (voisins) aux autres nœuds du réseau. **[6]**

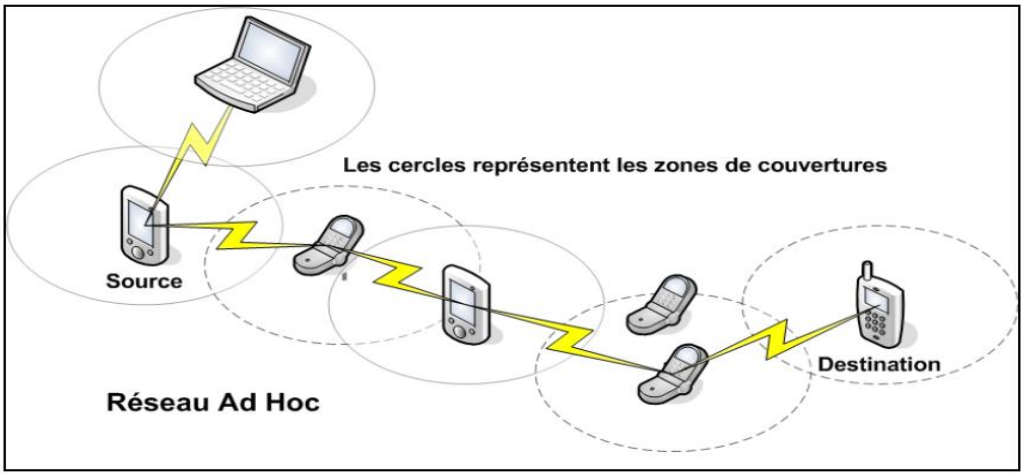


Figure 1.7 : Exemple d'un réseau Ad Hoc simple**. [7]**

5.3. Caractéristiques des réseaux Ad Hoc

Les réseaux Ad Hoc héritent des mêmes propriétés et problèmes liés aux réseaux sans fil. Les réseaux Ad Hoc sont caractérisés par ce qui suit : **[8]**

- **Multi sauts (Multi Hopping)** : la propriété grâce à laquelle chaque nœud du réseau peut atteindre les autres nœuds hors portée radio grâce au protocole de routage. **[8]**

- **Auto-configuration :** l'absence d'une entité centrale d'administration exige que les nœuds doivent s'auto-configurer et s'auto-organiser afin de garantir la flexibilité et l'adaptabilité requises. **[8]**
- **Energie :** la plupart des nœuds Ad Hoc (ordinateur portable, PDA et capteurs) sont limités en matière d'énergie ce qui affecte la durée de vie de ces nœuds surtout si on considère la nature collaborative des protocoles de routage Ad Hoc**. [8]**

- **Qualité de service (QoS : Q**uality **O**f **S**ervice**) :** les applications gourmandes en ressources et surtout celles qui exigent une exécution en temps réel (VoIP, jeux en ligne...etc.) représentent un vrai défi pour les réseaux Ad Hoc. Le caractère versatile des nœuds et les ressources d'énergie limitées pourraient nuire à la qualité de service (QoS) offerte à travers un réseau AD HOC. **[8]**

- **Sans infrastructure:** Les MANET ne dépendent donc pas d'une infrastructure préétablie. Chaque nœud opère comme un routeur indépendant, il est responsable de l'établissement et le maintien d'une connectivité continue. **[9]**

- **Bande passante limitée:** La communication dans les réseaux Ad Hoc se base sur le partage d'un médium sans fil (onde radio). Ce qui induit une bande passante modeste pour chaque hôte du réseau. **[9]**

- **Interférences:** Dans un réseau Ad Hoc, les liens radio ne sont pas isolés, par exemple : deux transmissions simultanées sur une même fréquence, ou sur des fréquences proches pouvant interférer et provoquer des erreurs de transmission. Un grand nombre de paquets peuvent être endommagés et perdus lors du transfert. **[9]**

- **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 unis ou bidirectionnels. **[25]**

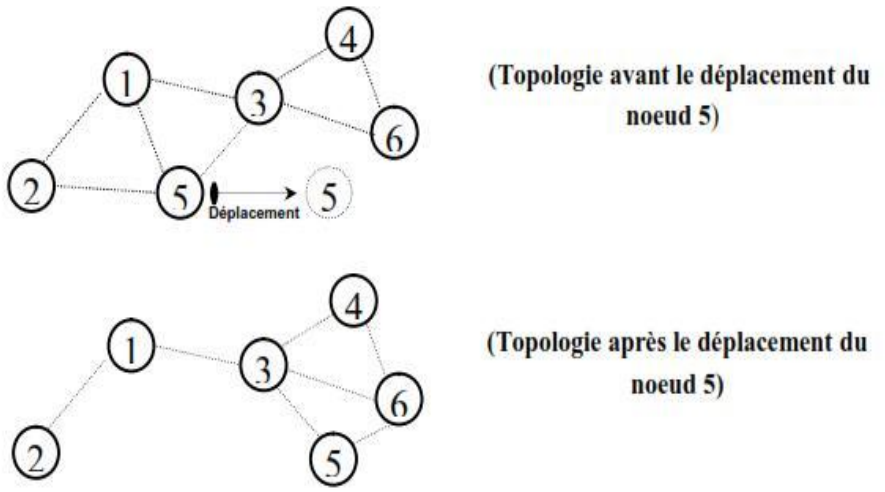


Figure 1.8 : Changement de la topologie d'un réseau Ad Hoc**. [25]**

- **Contraintes de ressources :** Les nœuds disposent de ressources d'alimentation et de capacités de calcul et de stockage limitées. D'où une gestion efficace est nécessaire pour avoir une longue durée de vie, le trafic de routage devrait être maintenu à un minimum. **[25]**

- **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. **[25]**

- **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. **[25]**

5.4. Avantages et les inconvénients des réseaux Ad Hoc

Les réseaux Ad Hoc se caractérisent par plusieurs avantages et inconvénients :

5.4.1. Avantages des réseaux Ad Hoc

- **Pas de câblages :** L'une des caractéristiques des réseaux Ad Hoc est l'absence d'un câblage et ce en éliminant toute les connexions filaires qui remplacées par des connexions radio. **[24]**

- **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 justifié par l'absence d'une infrastructure préexistante permettant ainsi d'économiser tout le temps de déploiement et d'installation du matériel nécessaire. **[24]**

- **Consommation énergétique** : Un mobile émet plus de message en modes Ad Hoc qu'en mode infrastructure puisqu'il doit à la fois transmettre ses propres paquets mais également les paquets des autres mobiles pour lesquels il fait travail de routeur. **[24]**

- **Permet la mobilité :** Comme l'indique leur nom et à l'image des réseaux sans fils avec infrastructure, les réseaux mobiles Ad Hoc permettent une certaine mobilité à leurs nœuds, 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. **[3]**

- **Coût :** Le déploiement d'un réseau Ad Hoc ne nécessite pas d'installer des stations de base. Les mobiles sont les seules entités physique nécessite, pour déployer un tel réseau ce qui conduit à la réduction de son coût d'une manière significative. **[3]**

5.4.2. Inconvénients 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. **[26]**

- **Capacités limitées** : Dans un tel réseau Ad Hoc la configuration de la portée de communication des nœuds est important. 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 demandent de l'énergie. Il faut donc trouver un compromis entre la connectivité du réseau et la consommation énergétique. **[26]**

- **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. **[26]**

- **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. **[15]**

5.5. Domaines d'applications des réseaux mobiles Ad Hoc

La particularité du réseau Ad Hoc qu'il n'a pas besoin d'aucune installation fixe, ceci lui permet d'être rapide et facile à déployer.

Les réseaux Ad Hoc sont utilisés dans toutes les applications où le déploiement d'une architecture décentralisée est contraignant, voire impossible. En effet, la robustesse, le coût réduit et le déploiement rapide, confèrent un accès à une large palette d'applications dont : **[9]**

- **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 différents groupes et les unités d'armée. **[9]**

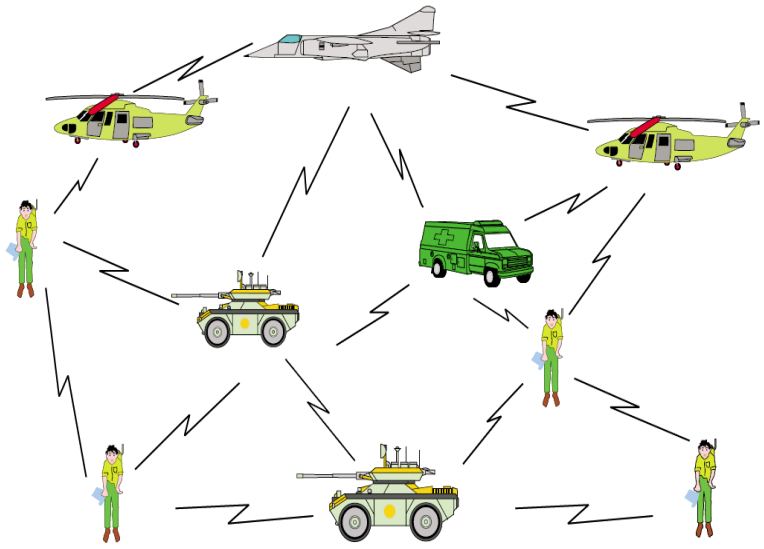


Figure 1.9 : Les applications militaires. **[17]**

- **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 aux unités de secours de communiquer. **[9]**

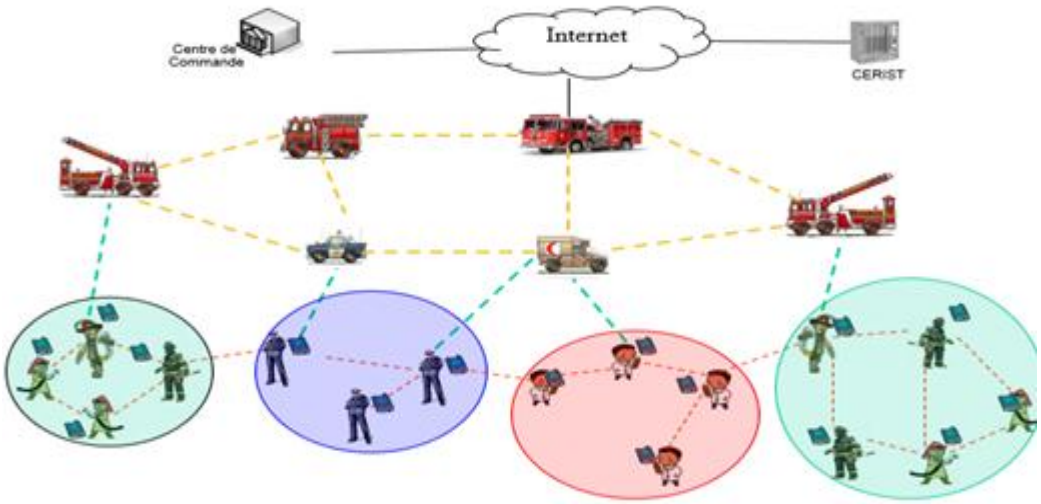


Figure 1.10 : Les opérations de secours. **[17]**

- **Applications industrielles** : Des scénarios plus complexes dans le domaine industriel, appelés réseaux de capteurs (Sensor Networks) 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]**

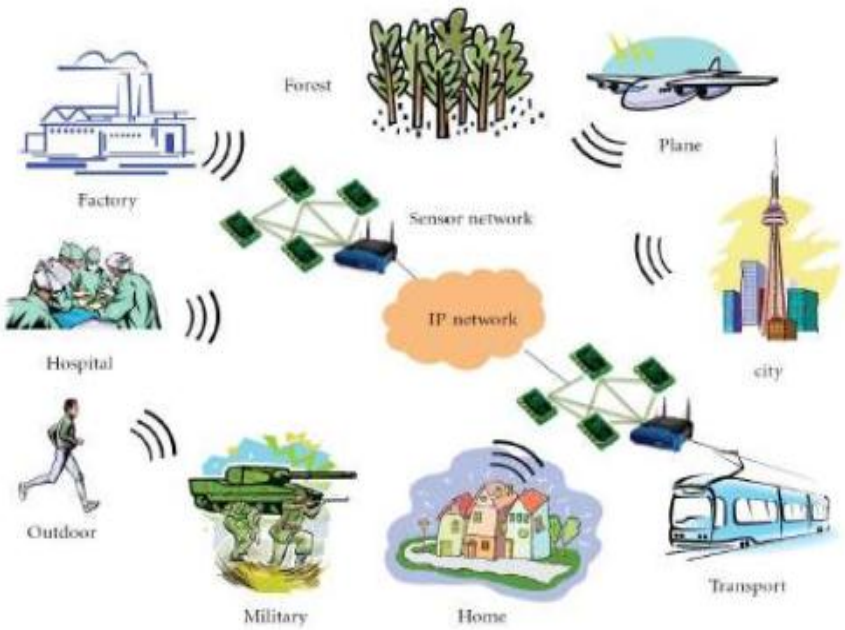


Figure 1.11 : Quelques domaines d'application pour les RCSF. **[20]**

- **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]**

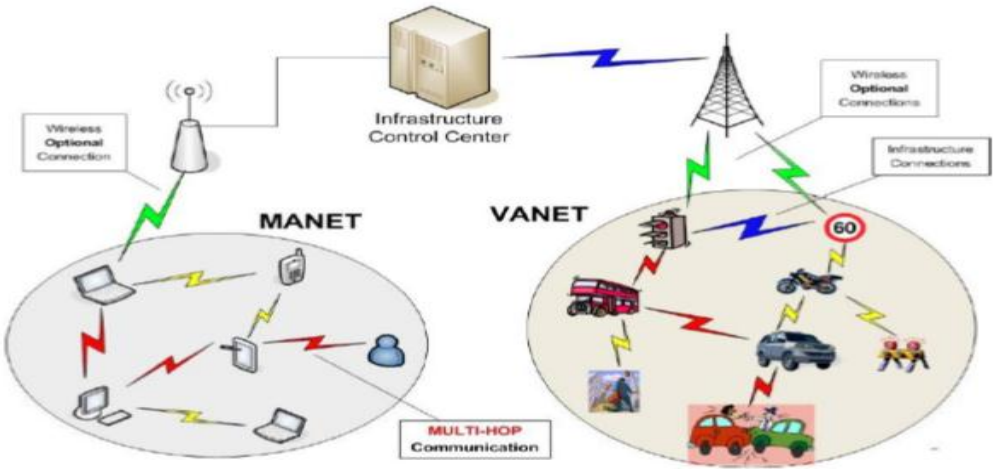


Figure 1.12 : Nœud représentes les réseaux VANET. **[14]**

- **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. **[27]**

6. Comparaison entre les deux types de réseaux sans fil

Les deux types des réseaux sans fil présentent pour chacun d'eux des spécifications l'un par rapport à l'autre.

Réseau avec infrastructure	Réseau sans infrastructure
Avec point d'accès.	Pas de point d'accès.
Performances élevées d'un point d'accès pour couvrir des zones étendues.	Les connexions sont limitées.
Pas d'interférences.	Dans un réseau Ad Hoc comptant un grand nombre d'ordinateurs, les interférences de ces derniers augmentent dans la mesure, où chacun d'entre eux tente d'utiliser le même canal de fréquence.
Bande passante élevée.	Bande passante limitée.
Coûteux.	Besoin seulement d'ordinateurs.
Topologie de réseau statique.	Topologie de réseau très dynamique avec multi-sauts.

Tableau 1.2 : Comparaison entre les deux types des réseaux sans fil**. [28]**

7. Routage dans les réseaux Ad Hoc

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**. [10]**

7.1. Classification des protocoles de routage dans les réseaux Ad Hoc

Ce sont principalement des régimes à base topologique qui utilisent une approche réactive, proactive ou hybride pour créer des itinéraires.

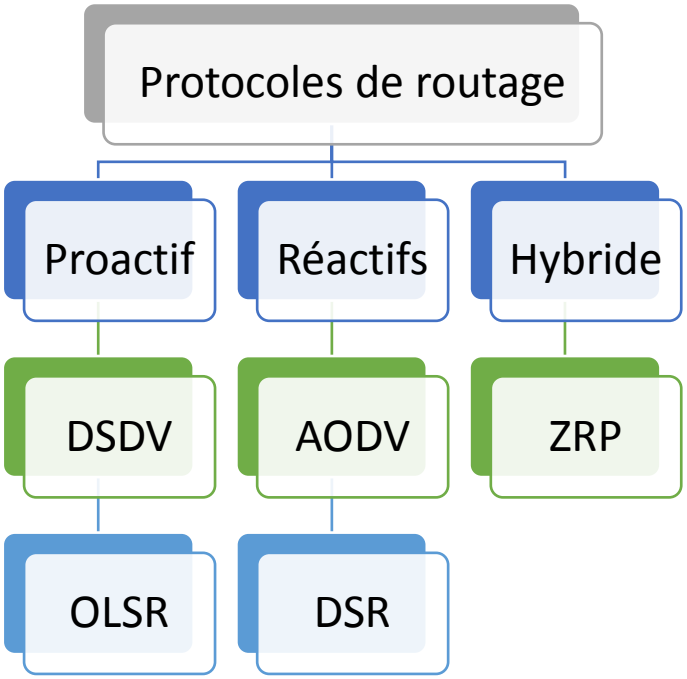


Figure 1.13 : Les protocoles de routage dans les MANET. **[28]**

7.1.1. Protocoles réactifs

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. **[11]**

- **Avantages et inconvénients des protocoles réactifs**

Dans le cas d'un protocole réactif, aucun message de contrôle ne charge le réseau pour des routes inutilisées. Ce qui permet de ne pas gaspiller les ressources du réseau (cela permet d'économisé de la bande passante et de l'énergie). Mais la mise en place d'une route par inondation, peut être coûteuse et provoquer des délais importants avant l'ouverture de la route. **[3]**

a) Le protocole AODV (Ad Hoc On-demand Distance Vector)

Ce protocole crée les routes au besoin et utilise le principe du numéro de séquence, afin d'utiliser les routes les plus nouvelles. En plus, il utilise le nombre de sauts comme métrique pour choisir entre plusieurs routes disponibles.

Trois types de paquets sont utilisés par AODV : les paquets de requête de route RREQ (Route Request Message), les paquets de réponse de route RREP (Route Reply Message) et les paquets d'erreur de route RERR (Route Error Message). En plus de ces paquets, AODV invoque des paquets de contrôle HELLO qui permettent de vérifier la connectivité des routes. AODV repose sur deux mécanismes : découverte de route et maintenance de route.

La découverte de route permet de trouver une route pour atteindre une destination, et **la maintenance de rout**e permet de détecter et signaler les coupures de routes, provoquées éventuellement par la mobilité des nœuds. **[12]**

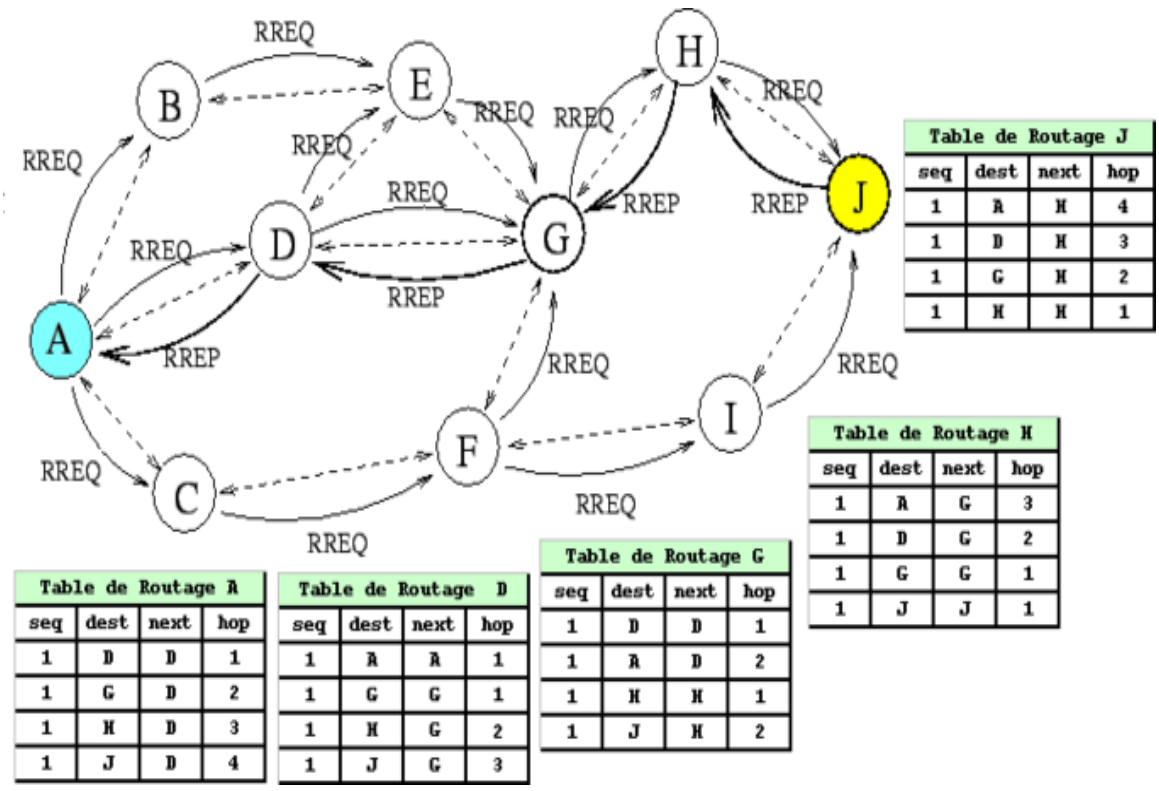
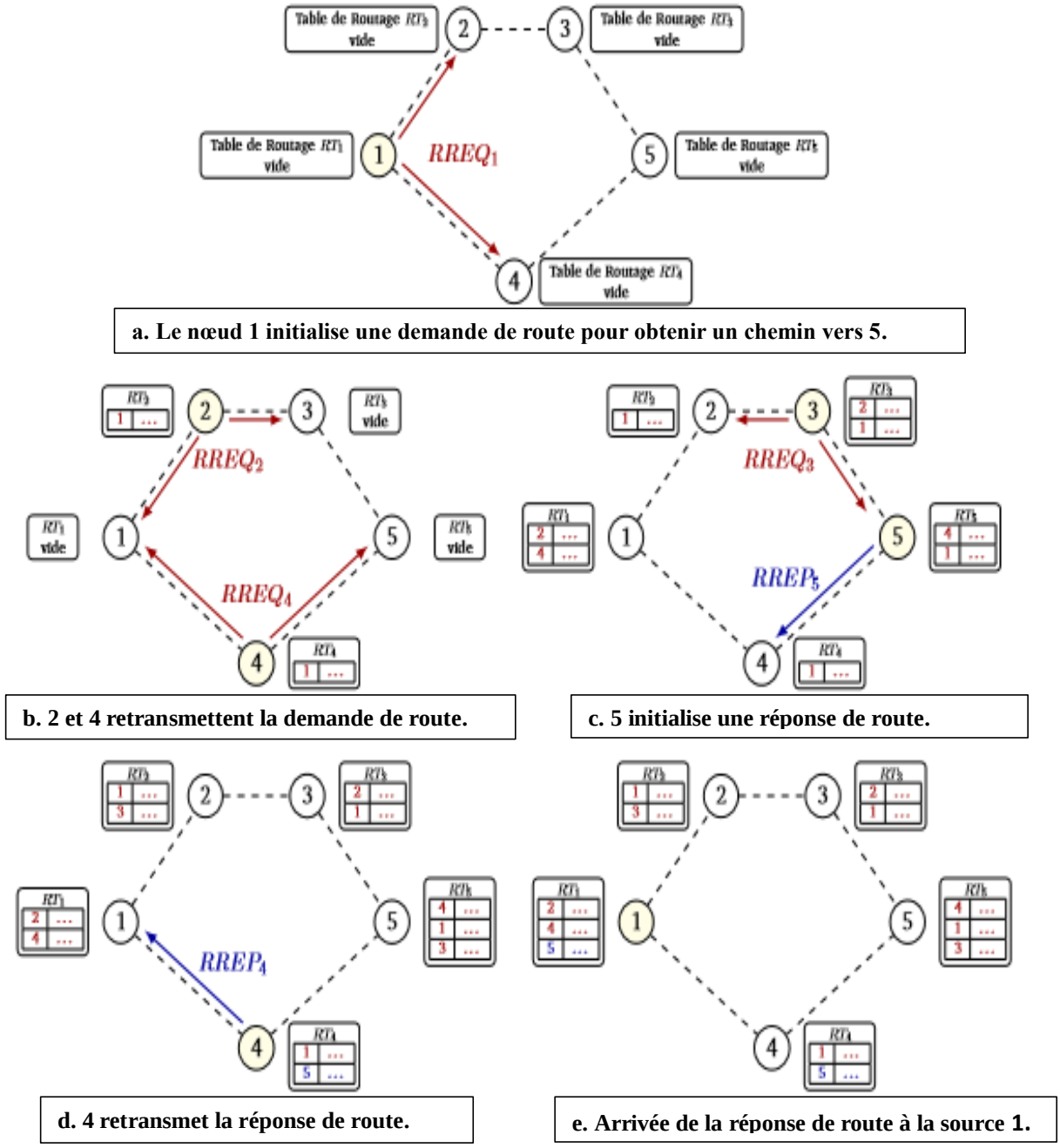


Figure 1.14 : Fonctionnement de protocole AODV**. [12]**



a. Le nœud 1 initialise une demande de route pour obtenir un chemin vers 5.

b. 2 et 4 retransmettent la demande de route.

c. 5 initialise une réponse de route.

d. 4 retransmet la réponse de route.

e. Arrivée de la réponse de route à la source 1.

Figure 1.15: Exemple d'établissement de route entre 1 et 5. **[15]**

Une entrée de la table de routage contient essentiellement :

1) L'adresse de la destination.
2) Adresse du nœud suivant.
3) La distance en nombre de sauts (le nombre de nœuds nécessaires pour atteindre la destination).
4) Le numéro de séquence de la destination.
5) Le temps d'expiration de chaque entrée dans la table.

A chaque utilisation d'une entrée, son temps d'expiration est remis à jour (temps courant + active route time).

Si une nouvelle route est nécessaire, ou qu'une route disparaît, la mise à jour de ces tables s'effectue par l'échange de trois types de messages entre les nœuds :

- RREQ Route Request, un message de demande de route.
- RREP Route Reply, un message de réponse à un RREQ.
- RERR Route Error, un message qui signale la perte d'une route.

Format général d'une RREQ :

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

Format général d'une RREP :

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

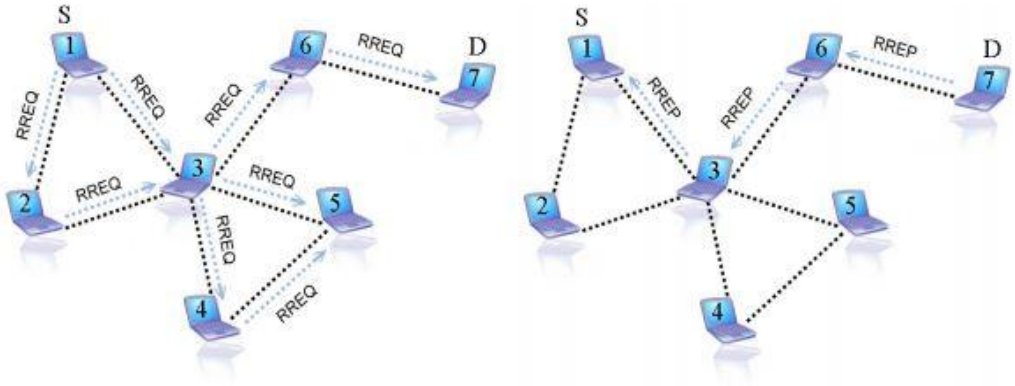


Figure 1.16 : Les deux requêtes RREQ et RREP utilisées dans le protocole AODV**. [28]**

Le protocole AODV exécute lui aussi une procédure de maintenance des routes, cette procédure se fait par l'émission périodique d'un message "HELLO". Le lien entre deux nœuds voisins sera considéré comme défaillant dans le cas où les messages "HELLO" ne sont pas reçus.

Les défaillances des liens sont généralement dues à la mobilité du réseau Ad Hoc. Les mouvements des nœuds qui ne participent pas dans le chemin actif n'affectent pas la consistance des données de routage.

Le protocole AODV maintient les adresses des voisins à travers lesquels les paquets destinés à un certain nœud arrivent. Un voisin est considéré actif, pour une destination donnée, s'il délivre au moins un paquet de donnée sans dépasser une certaine période (appelée : active time out period). Une entrée de la table du routage est active, si elle est utilisée par un voisin actif. Le chemin reliant la source et la destination, en passant par les entrées actives des tables de routage, est dit un chemin actif.

Lorsqu'un nœud reçoit un paquet en Broadcast, il met à jour ses informations de connectivité locale pour s'assurer qu'elles incluent ce voisin. **[12]**

b) Le protocole DSR (Dynamic Source Routing)

Ce protocole crée les routes à la demande comme le protocole AODV. Il utilise la technique « routage à la source », dans laquelle celle-ci inclut dans l'entête du paquet la route complète, par laquelle un paquet doit passer pour atteindre sa destination.

Les nœuds intermédiaires entre la source et la destination n'ont pas besoin de maintenir à jour les informations sur la route traversée puisque la route complète est insérée dans l'entête du paquet.

Le DSR est composé de deux mécanismes : la découverte et la maintenance de la route. Le premier permet de chercher les routes nécessaires à la demande, tandis que le second permet de s'assurer de la maintenance des routes tout au long de leur utilisation. **[12]**

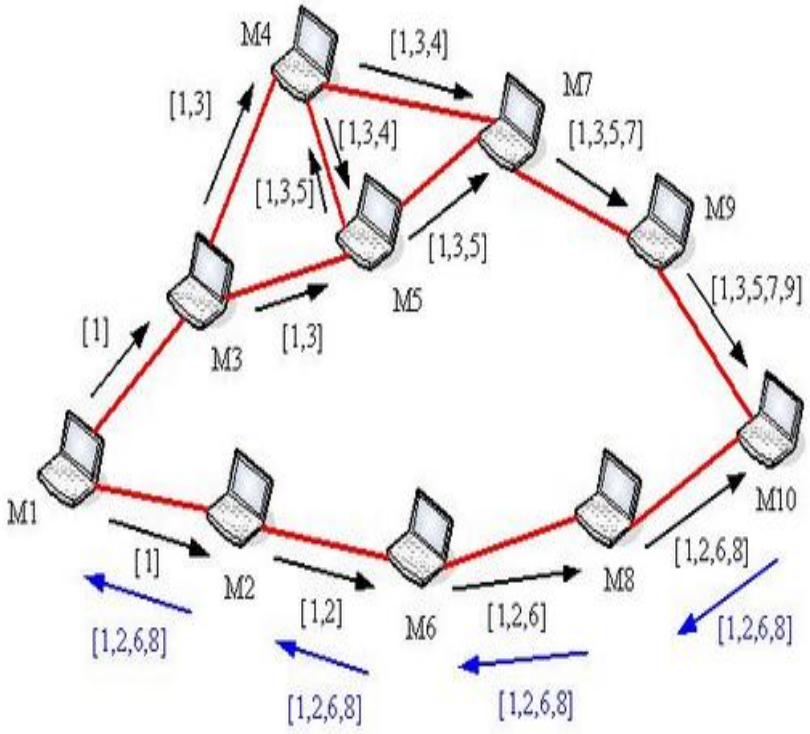
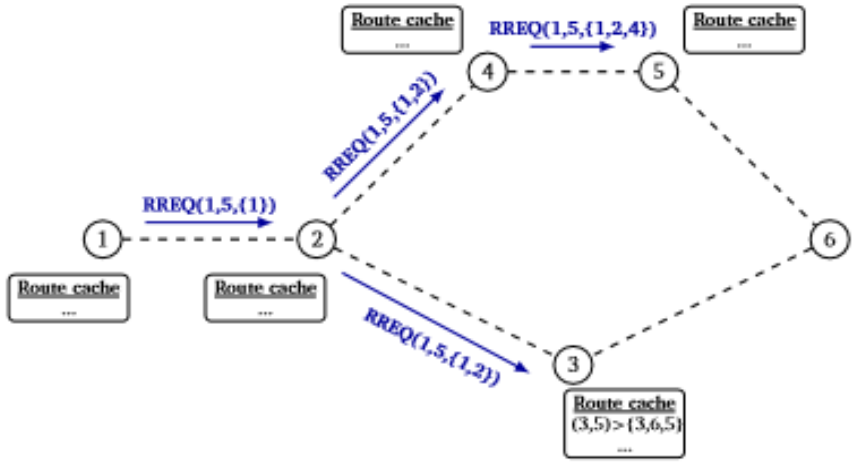
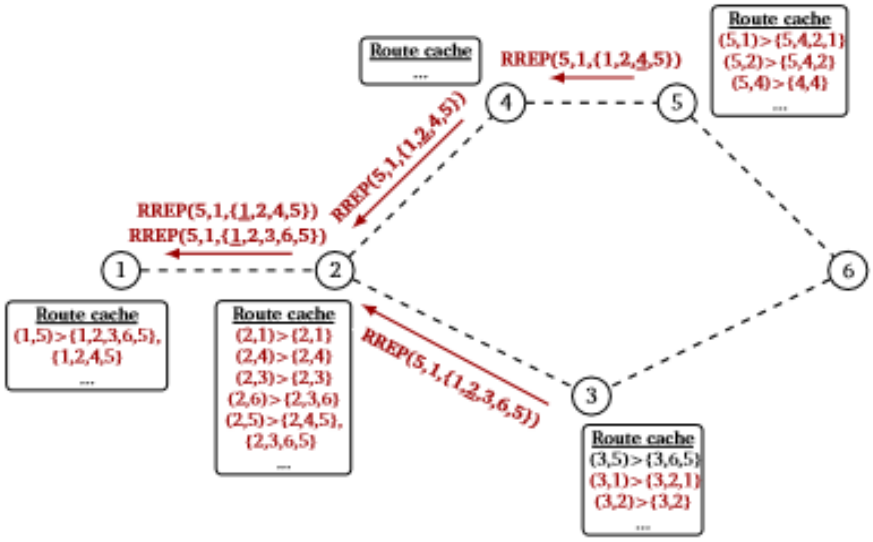


Figure 1.17 : Fonctionnement du DSR**. [28]**



a. Propagation de la demande de route



b. Propagation de la réponse de route

Figure1.18 : Fonctionnement du DSR entre 1 et 5. **[15]**

Afin d'assurer la validité des chemins utilisés, le DSR exécute une procédure de maintenance de routes :

- Quand un nœud détecte un problème fatal de transmission, à l'aide de sa couche de liaison, un message erreur de route (route error) est envoyé à l'émetteur original du paquet.
- Le message d'erreur contient l'adresse du nœud qui a détecté l'erreur et celle du nœud qui le suit dans le chemin.
- Lors de la réception du paquet erreur de route par l'hôte source, le nœud concerné par l'erreur est supprimé du chemin sauvegardé, et tous les chemins qui contiennent ce nœud sont tronqués à ce point-là. Par la suite, une nouvelle opération de découverte de routes vers la destination, est initiée par l'émetteur.

L'utilisation du technique « routage source », fait que les nœuds de transit n'aient pas besoin de maintenir les informations de mise à jour pour envoyer les paquets de données, puisque ces derniers contiennent toutes les décisions de routage.

Dans ce protocole, il y a une absence totale de boucle de routage, car le chemin source destination fait partie des paquets de données envoyés. **[12]**

7.1.2. Protocoles proactifs

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. **[16]**

- **Avantages et inconvénients des protocoles proactifs**

Avec un protocole proactif, les routes sont disponibles immédiatement lors du besoin. Ainsi l'avantage d'un tel protocole est le gain de temps lors d'une demande de route. Le problème est que, les changements de routes peuvent être plus fréquents que la demande de la route. Dans ce cas-là, le trafic induit par les messages de contrôle et de mise à jour des tables de routage peut être important et partiellement inutile. Car seules certaines routes seront utilisées par les applications en général. Ce qui gaspille la capacité du réseau sans fil en termes de bande passante. **[3]**

a) Le protocole DSDV (Destination Sequenced Distance Vector)

Le protocole DSDV est basé sur l'algorithme distribué de Bellman-Ford .Chaque nœud du réseau maintient dans sa table de routage un ensemble d'informations pour chaque destination contenant : **[8]**

- L'adresse du destinataire : l'identifiant du prochain nœud vers cette destination.
- Le nombre de sauts (nœuds) pour l'atteindre.
- Le plus grand numéro de séquence reçu pour cette destination, il est utilisé pour permettre au nœud mobile de faire la distinction entre les anciennes routes et les nouvelles routes découvertes.

Afin de maintenir la consistance des tables de routage dans une topologie qui change rapidement, chaque nœud du réseau transmet périodiquement sa table de routage à ses voisins directs. Lors d'une nouvelle diffusion, le nœud incrémente un numéro de séquence et le transmet avec sa table de routage. Celui-ci est utilisé par les autres nœuds pour valider la mise à jour de leur table de routage et éviter les boucles. Afin de limiter le trafic occasionné par toutes ces mises à jour, il existe deux types de mise à jour :

- Des mises à jour complètes : qui n'est rien autre que la mise à jour périodique, c'est- à-dire que le nœud transmet la totalité de sa table de routage vers ses voisins.
- Des mises à jour incrémentales : cette mise à jour n'est faite qu'en cas d'événements (Apparition d'un nouveau voisin, disparition d'un nœud ...etc.), et dans ce cas il n'y a que l'entrée concernant le nœud en question dans la table de routage qui change. Cette mise à jour est aussi dite mise à jour partielle.

La mise à jour se fait à travers la transmission d'un paquet généralement contenant :

- Le nouveau numéro de séquence, incrémenté, du nœud émetteur.
- L'adresse de la destination.
- Le nombre de sauts séparant le nœud de la destination.

Le numéro de séquence (des données reçues de la destination) tel qu'il a été estampillé par la destination. **[8]**

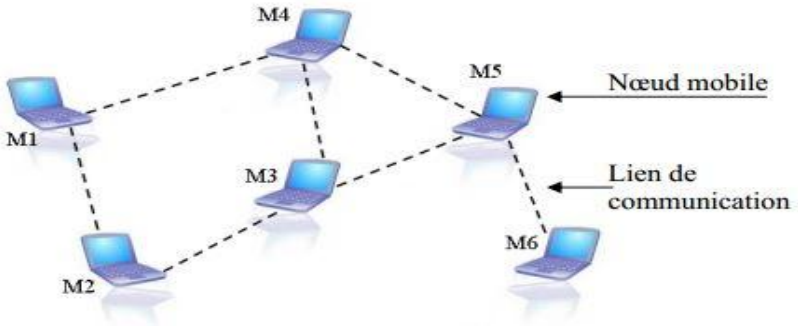
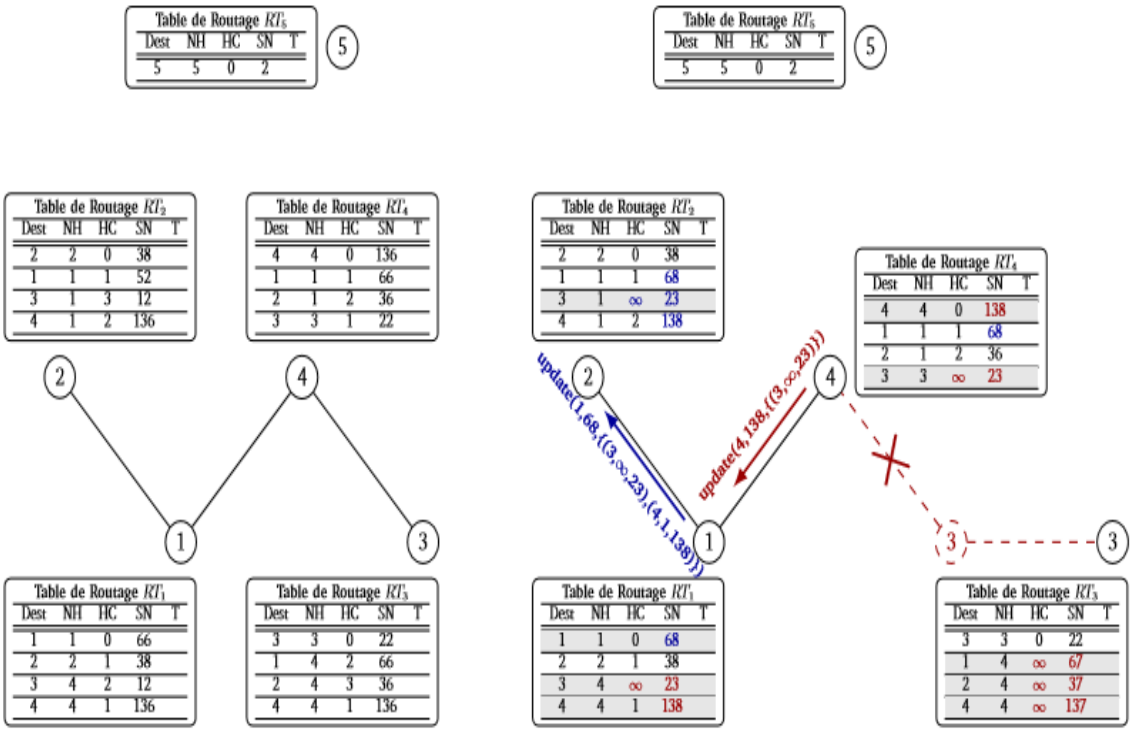


Figure 1.19 : Exemple d'un réseau Ad Hoc**. [28]**

Si l'on considère que le DSDV est le protocole de routage utilisé dans la figure 1.19, la table de routage correspondante au nœud M1 ressemblera à la suivante : **[8]**

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

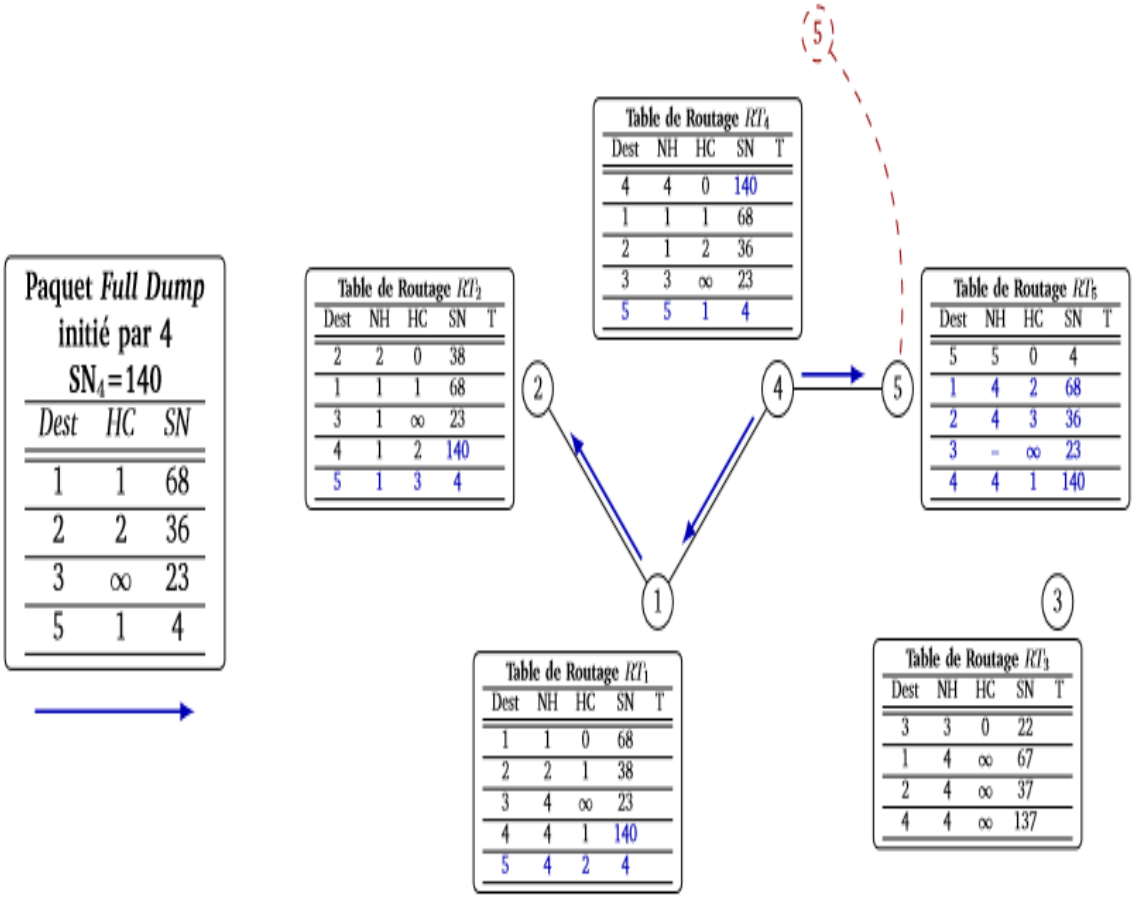
Tableau 1.3 : Table de routage du nœud M1 du graphe de la figure 1.19. **[8]**



a. Après échanges de messages de mises à jour, les tables de routage se sont stabilisées

b. Modification suite au déplacement du nœud 3

Figure 1.20 : Mise à jour incrémentale. **[15]**



a. Paquet de mise à jour émis par le nœud 4

b. Propagation du paquet et répercussion sur les tables de routage

Figure 1.21 : Mise à jour complète (full dump). **[15]**

Ainsi tout nœud, qui a subi une mise à jour, compare les données de routage reçus avec les siennes, et la route la plus récente (celle avec la plus grande valeur du numéro de séquence) sera utilisée.

Si deux routes ont le même numéro de séquence, alors la route qui possède la meilleure métrique est celle qui sera utilisée. La métrique utilisée dans le calcul des plus courts chemins est, tout simplement, le nombre de nœuds intermédiaires existants sur ce chemin. Un lien rompu est matérialisé par une valeur infinie de sa métrique (une valeur plus grande que la valeur maximale permise par la métrique).

Parmi les inconvénients du protocole DSDV, est qu'il est très lent, du fait qu'il doit attendre la mise à jour transmise par le destinataire pour modifier l'entrée adéquate dans la table de distance. **[8]**

b) Le protocole OLSR (Optimized Link State Routing Protocol)

OLSR est un protocole proactif qui repose sur l'échange régulier d'informations sur la topologie du réseau et aussi un protocole à état de liens qui construit des routes du plus court chemin.

L'algorithme est optimisé par la réduction de la taille et du nombre des messages échangés. Seuls des nœuds particuliers, les MPR (Multi Point Relay) diffusent des messages de contrôle sur la totalité du réseau. Le MPR est le nœud sélectionné par un de ses voisins immédiats pour retransmettre ses messages à travers le réseau. L'ensemble des MPRs d'un nœud est choisi parmi les voisins immédiats, de manière à permettre d'atteindre tous les nœuds situés exactement à 2 sauts.

Tous les nœuds envoient périodiquement des messages HELLO à leurs voisins immédiats sur chacune de leurs interfaces. Ces messages permettent à chaque nœud de maintenir à jour toutes les informations nécessaires au choix des relais multipoints et effectuer le calcul des tables de routage.

Le routage vers les stations éloignées de plus d'un saut se fait grâce aux MPR, qui diffusent périodiquement des messages de contrôle de la topologie TC (Topology Control) contenant la liste de leurs MPRs. Ces messages servent à maintenir dans chaque station une table de la topologie du réseau. La table de routage est construite et mise à jour à partir des informations contenues dans la table des interfaces voisines et la table de la topologie, en utilisant un algorithme du plus court chemin.

La métrique prise en compte est le nombre de sauts. **[6]**

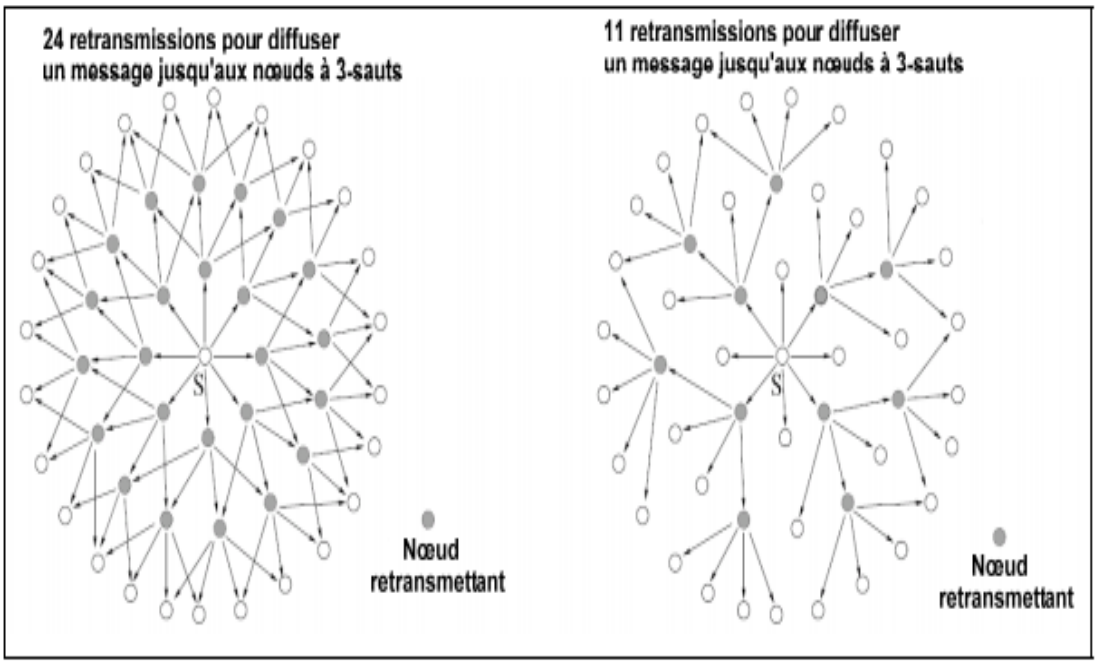


Figure 1.22 : Diffusion par inondation classique vs inondation par relais multipoints. **[21]**

7.1.3. Protocoles hybrides

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. **[13]**

- **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. **[3]**

a) Le protocole ZRP (Zone Routing Protocol)

ZRP est un protocole de routage dit hybride. Il met en place, simultanément, un routage proactif et un routage réactif, afin de combiner les avantages des deux approches. Pour ce faire, il passe par un concept de découpage du réseau en différentes zones, appelées (zones de routage).

Une zone de routage pour un nœud S, est définie par son (rayon de zone). Ce rayon correspond au nombre de sauts maximum existants entre le nœud D et S (figure 1.23).

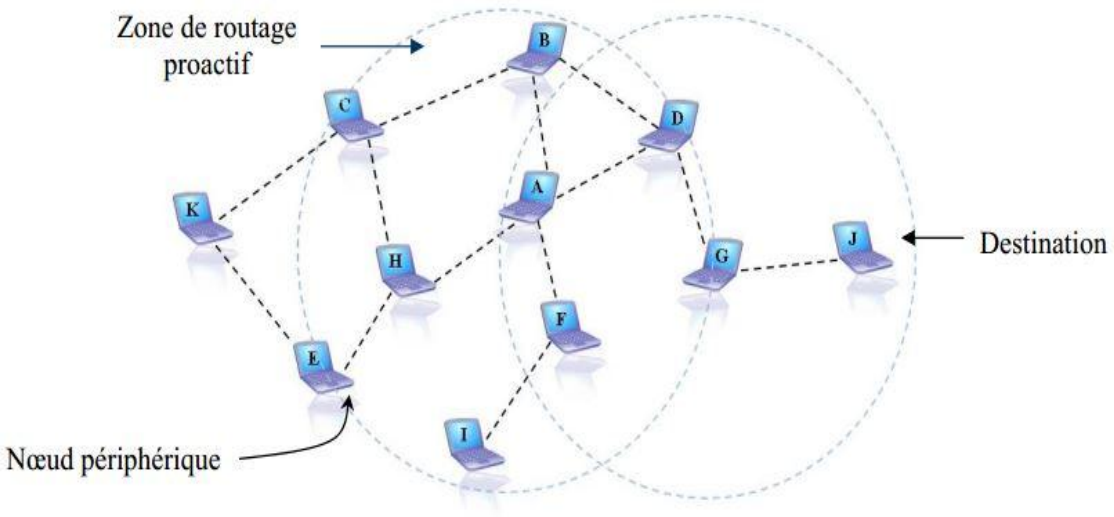


Figure 1.23 : Une zone de routage. **[28]**

Le routage au sein d'une zone se fait de manière proactive, et le routage vers les nœuds extérieurs de la zone se fait de façon réactive.

8. Comparaison

8.1. Comparaison entre type de routage

Le tableau ci-dessous présente une comparaison entre les différents types de routage Ad Hoc :

Routage proactif		Routage réactif		Routage Hybride
Avantages	**Inconvénients**	**Avantages**	Inconvénients	
- Pas de temps de réaction. -Adaptés aux réseaux denses de taille moyenne. -Adaptés aux réseaux à forte mobilité.	-Trafic de contrôle important. -Capacité d'échange du réseau limitée. -Consommation énergétique plus importante.	-Trafic de contrôle faible. -Adaptés aux grands réseaux. -Consommation énergétique réduite.	-Temps de réaction long. -Problème en cas de forte mobilité des nœuds.	Combine les deux techniques proactives et réactive.

Tableau 1.4 : Comparaison entre les protocoles proactifs, réactifs et hybride**. [29]**

8.2. Comparaison entre les protocoles de routage

Le tableau ci-dessous présente une comparaison entre les différents protocoles de routage Ad Hoc en mettant l'accent sur les différences et les propriétés de chacun des protocoles.

Contrainte de performance	DSDV	OLSR	AODV	DSR	ZRP
Catégorie	Proactif	Proactif	Réactif	Réactif	Hybride
Route sans cycle	Oui	Oui	Oui	Oui	Oui
Routes multiples	Oui	Non	Non	Non	Oui
Multicast	Oui	Oui	Oui	Non	Oui
Surcharge réseau	Minimale	Minimale	Modérée	Modérée	Modérée
Diffusion périodique	Possible	Possible	Possible	Possible	Possible
Principale caractéristique	Des informations sur les destinations avec un numéro de séquence. Envoi périodique aux voisins.	Messages de contrôle pour la détection de liaison, détection des voisins (MPR), et un calcul des routes.	Découverte des routes, avec une recherche, à la poursuite du chemin.	Demande et découverte des routes, des routages à la source, et la maintenance de route.	Chaque nœud identifié les voisins, pour découvrir les routes, IERP est utilisé à la demande pour chercher les routes.

Tableau 1.5 : Tableau comparatif des différents protocoles de routage Ad Hoc. **[28]**

9. Conclusion

Après avoir abordé le concept général de la communication sans fil, nous avons cité une description pour les réseaux sans fil avec une explication de leurs types, nous nous sommes intéressés beaucoup plus à une catégorie de réseaux sans fil qui sont les réseaux Ad Hoc.

Pour cela, nous avons traité les réseaux Ad Hoc qui sont un type particulier de réseaux MANET avec des détails sur leurs caractéristiques et l'intérêt qu'apporte ce type de réseaux.

Une des contraintes des réseaux MANET est le problème d'acheminement des données entres les nœuds mobiles du réseau.

Dans ce chapitre, nous avons cité les différents types de protocoles de routage dans les réseaux Ad Hoc dans la deuxième partie.

Chapitre 2 :

Sécurité et attaques dans les Réseaux AD HOC.

1. Introduction

Aujourd'hui, les réseaux filaires peuvent assurer un niveau de sécurité très élevé. Mais dans les réseaux sans fil, les défauts de sécurité apparaissent souvent même si des précautions ont été prises, ils vont intégrer dans un futur proche toutes les situations de notre vie quotidienne. Le concept et la nature des réseaux Ad Hoc les rendent facilement vulnérables à différents types d'attaques. Ce qui rend la tâche encore plus difficile est que les nœuds du réseau se chargent eux-mêmes de la fonction de routage des données. Favorisé par la nature vulnérable des communications sans fil, n'importe qui peut se connecter sur le réseau et écouter les messages de contrôle échangés. Il pourra ensuite les supprimer, les modifier, ou mener d'autres attaques plus complexes, ce qui met en danger tout le réseau. Les protocoles de routage proposés dans le cadre du travail du groupe MANET offre un acheminement optimal des données mais n'offre aucun système de sécurité.

Dans ce chapitre, nous allons mettre le point sur le problème de sécurité des protocoles de routage. Au début de ce chapitre nous introduisons les concepts et les besoins fondamentales de la sécurité. Nous donnons sa définition, ces principaux objectifs, et présentons des différentes types d'attaques.

2. Sécurité informatique

La sécurité informatique est un ensemble de techniques assurant que les ressources (matérielles ou logicielles), d'un système d'information d'une organisation donnée, sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient. **[30]**

3. Sécurité dans les réseaux informatiques

3.1. Définition

La sécurité des réseaux informatiques est un sujet essentiel, pour favoriser le développement des échanges dans tous les domaines. Un seul mot « Sécurité » recouvre des aspects très différents à la fois techniques, organisationnels et juridiques. L'attitude des utilisateurs vis à vis des problèmes de sécurité est souvent irrationnelle, ce qui ne contribue pas à simplifier le débat. **[17]**

3.2. Besoins de sécurité Ad Hoc

Les besoins de base en sécurité pour les réseaux mobiles Ad Hoc sont plus ou moins les mêmes que pour les réseaux filaires ou sans fil avec infrastructure. Les services de sécurité sont basés sur quatre concepts fondamentaux : l'**authentification** des utilisateurs, la **confidentialité**, l'**intégrité** des données et du trafic du réseau, et enfin la **non répudiation** des utilisateurs et disponibilité de système. **[18]**

- **Authentification**

L'authentification permet de vérifier l'identité d'une entité ou d'un nœud dans le réseau. Sans l'authentification, un nœud malicieux peut facilement usurper l'identité d'un autre nœud dans le but de bénéficier des privilèges attribués à ce nœud ou d'effectuer des attaques sous l'identité de ce nœud et de nuire à la réputation du nœud victime. **[18]**

- **Confidentialité**

La confidentialité est un service essentiel pour assurer une communication privée entre les nœuds. C'est une protection contre les menaces qui peuvent causer la divulgation non autorisée d'informations alors qu'il faut veiller au caractère privé de l'information. Elle est principalement basée sur la cryptographie, en particulier les algorithmes de chiffrement. **[18]**

- **Intégrité**

Ce service assure que le trafic de la source à la destination n'a pas été altéré ou modifié sans autorisation préalable pendant sa transmission. Les services d'intégrité visent à assurer le bon fonctionnement des ressources et la transmission. Donc le récepteur d'un message s'assure que le message reçu est le même que le message envoyé. **[19]**

- **Non-répudiation**

La non-répudiation est la possibilité de vérifier que l'émetteur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. En d'autres termes, la non-répudiation permet de garantir qu'une transaction (émission/réception/action) ne puisse pas être niée. Cela est très pratique pour détecter et isoler les nœuds compromis. **[18]**

- **Disponibilité :**

La disponibilité consiste à assurer la continuité du service fourni par un nœud même en présence d'une attaque. Pour cela, la protection contre les menaces qui peuvent causer la perturbation des fonctions du réseau est nécessaire pour assurer à tous les nœuds l'accès aux ressources réseau comme le routage, l'accès aux données, etc. ... **[18]**

4. Vulnérabilités et l'attaques dans les réseaux Ad Hoc

Dans un réseau Ad Hoc toute les entités peuvent participer au routage, donc il n'y a pas de barrières pour un nœud malicieux de causer des perturbations dans le trafic circulant. L'intérêt de l'attaquant vise essentiellement à compromettre la confidentialité et l'intégrité des informations en transit. Ou de manière plus générale, à perturber le bon fonctionnement du processus de routage pour dominer le réseau. **[16]**

La vulnérabilité des réseaux Ad Hoc est liée à la technologie sans fil sous-jacente. Quiconque possédant le récepteur adéquat peut potentiellement écouter ou perturber les messages échangés. Et ceci, même s'il se trouve dans un lieu public, à l'extérieur du bâtiment où se déroulent les échanges.

- **Les nœuds** eux-mêmes sont des points de vulnérabilités du réseau car un attaquant peut compromettre un élément laissé sans surveillance.
- **L'absence d'infrastructure fixe** pénalise l'ensemble du réseau dans la mesure où il faut faire abstraction de toute entité centrale de gestion pour l'accès aux ressources.
- **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.

En fin, ces réseaux héritent de toutes les vulnérabilités propres aux technologies sans fil WLAN et WPAN. **[42]**

4.1. Classification des attaques dans les réseaux Ad Hoc

Les environnements des réseaux Ad Hoc présentent de grands défis, ce type de réseaux a hérité à la fois des problèmes de sécurité des réseaux câblés et aussi ceux des réseaux sans fil. S'ajoute à cela, la nature des réseaux Ad Hoc qui se caractérise par une architecture Peer-to-Peer ouverte, une topologie dynamique et extensible, des ressources limitées et un canal radio accessible par tout le monde. **[21]**

Les attaques sur les réseaux Ad Hoc sont généralement divisées en deux catégories :

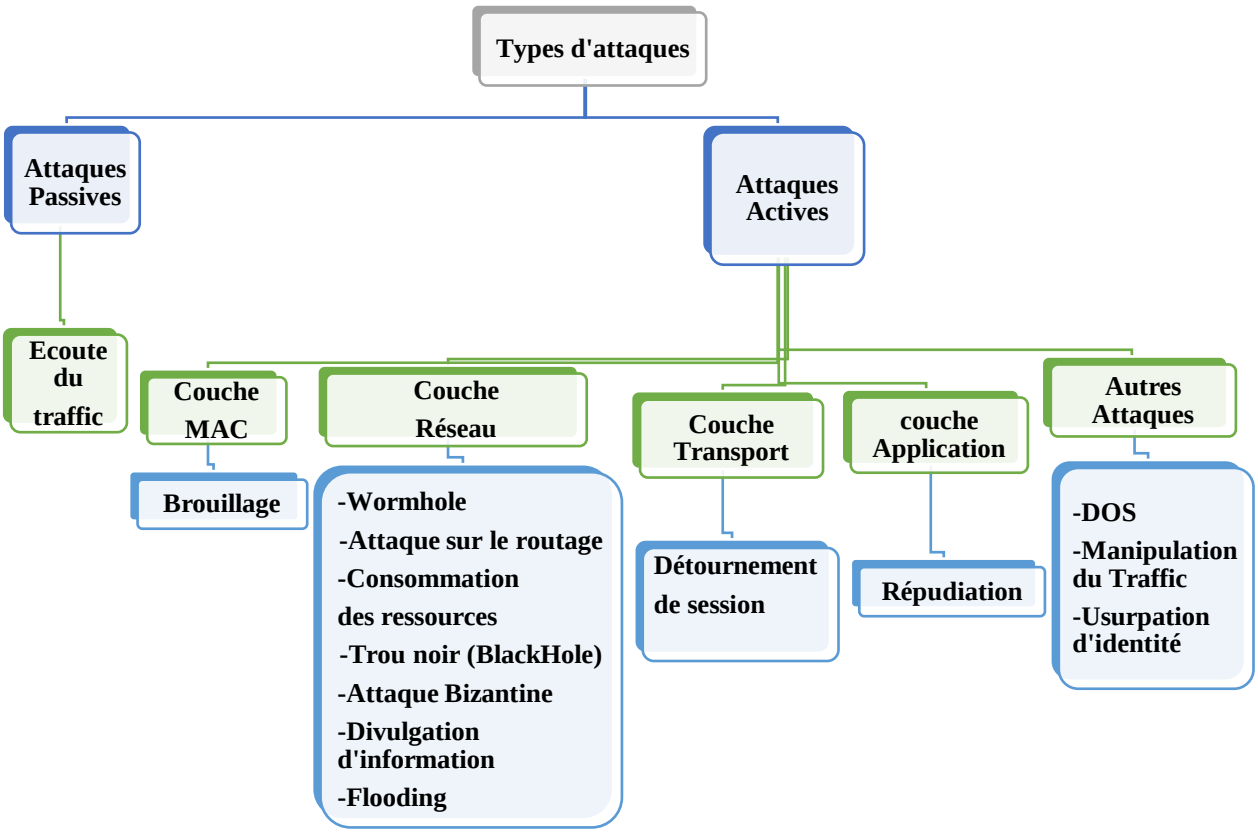


Figure 2.1 : Classification des attaques dans les réseaux Ad Hoc par rapport aux couches OSI**. [21][13]**

4.1.1. Attaque passive ou active

Dans les réseaux Ad Hoc, selon le niveau d'intrusion des actions menées par un attaquant, on distingue généralement deux catégories d'attaques : les attaques passives et les attaques actives. **[16]**

- **Attaques passives** : Principalement des attaques d'écoute de données.

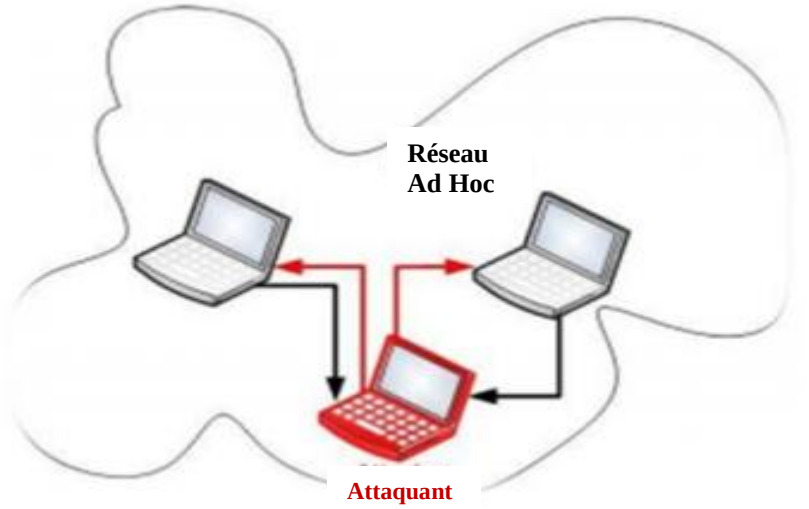


Figure 2.2 : Attaque passive. **[6]**

- **Attaques actives** : Des attaques pour lesquelles un attaquant doit modifier, altérer ou générer des messages. **[16]**

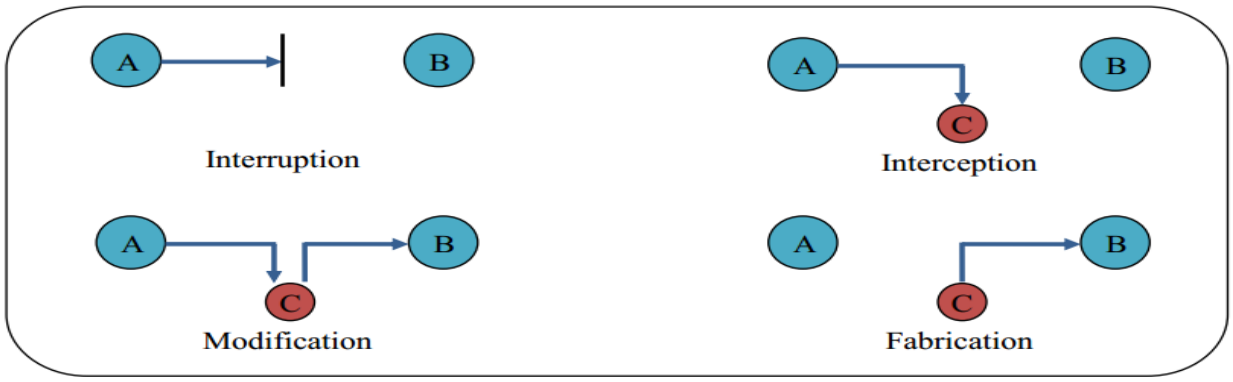


Figure 2.3 : Attaque active. **[29]**

- **Interruption** : Vise la disponibilité des données.
- **Interception** : Vise la confidentialité des données.
- **Modification** : Vise l'intégrité des données.
- **Fabrication** : Vise l'authenticité des données.

4.1.2. Attaque externe ou interne

En outre, selon le domaine d'appartenance d'un nœud, les attaques actives peuvent elles-mêmes être classées en deux catégories, à savoir les attaques externes et internes.

- **Attaque externe**

Les attaques externes sont réalisées par des nœuds qui n'appartiennent pas au réseau. **[16]**

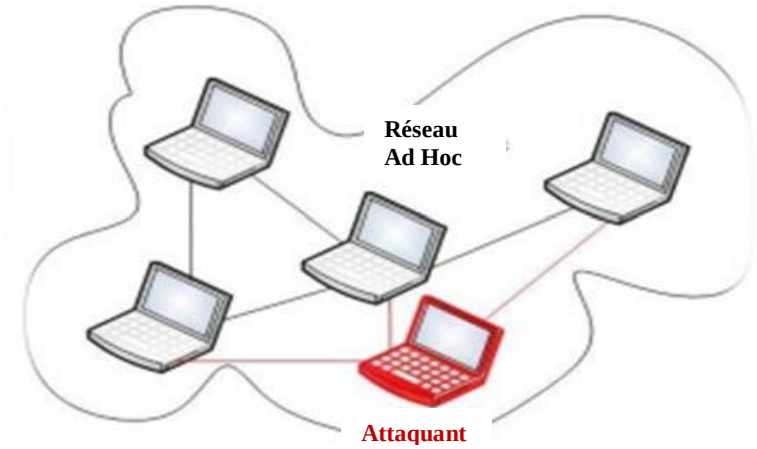


Figure 2.4 : Attaque externe**. [6]**

- **Attaque interne**

Les attaques internes sont menées par des nœuds compromis qui sont autorisés à participer au fonctionnement du réseau. Etant donné que les attaquants font d'ores et déjà partie du réseau de nœuds autorisés, les attaques internes sont généralement plus pernicieuses et difficiles à détecter que les attaques externes**. [16]**

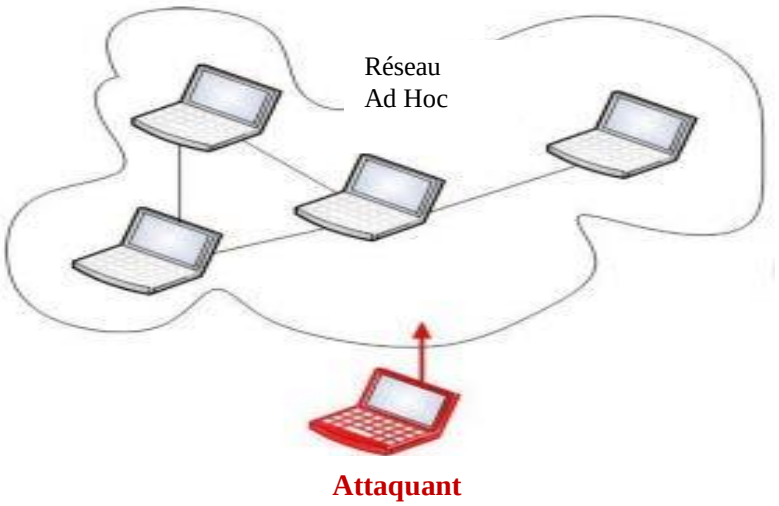


Figure 2.5 : Attaque interne**. [6]**

4.1.3. Attaque individuelle ou attaque distribuée

En effet, les attaques peuvent être de type individuelles ou par collusion ou appelée également distribuée. Les attaques individuelles sont menées par un seul nœud attaquant. Puisque les capacités de communication et de calcul de l'attaquant sont en général similaires à celles des autres nœuds du réseau, ces attaques demeurent relativement simples, et sont d'autant plus limitées que des mécanismes de sécurité sont mis en œuvre.

En revanche, rien n'empêche à des nœuds attaquants de mutualiser leurs informations et leurs ressources, en exploitant les connexions qu'ils ont entre eux. Ces attaques par collusion, issues de plusieurs nœuds répartis à différents endroits dans le réseau, sont généralement plus évoluées et plus dangereuses. Par ailleurs, en raison de l'intervention de plusieurs nœuds intermédiaires, leur détection et l'identification précise de leur origine sont rendues plus complexes. **[16]**

5. Principes d'attaques et d'attaquants

Une attaque peut être définie comme une tentative d'accès illégale à une ressource du système. Les attaques visent essentiellement les liens de communication et les entités du réseau afin de s'autoriser à récupérer et manipuler les données échangées. Un attaquant est une personne qui s'intéresse au fonctionnement du réseau dans le but de s'adjuger les moyens et le pouvoir de déjouer la sécurité du système. Cela est possible par la maitrise des techniques utilisées pour le sécuriser, et ainsi causer son dysfonctionnement partiel ou total par l'usurpation d'identités et la compromission de ses nœuds. L'existence d'un nœud compromis est très problématique car cela nécessite de revoir complètement la politique de sécurité appliquée. **[29]**

- **Objectifs des attaques**

Un attaquant peut opérer à deux niveaux : s'attaquer aux informations échangées entre les nœuds et s'attaquer aux nœuds eux-mêmes. Les objectifs et les motivations d'un attaquant sont multiples, on cite les principaux :

- Obtenir un accès au système.
- **Espionnage** : récupérer les données qui circulent sur le réseau.
- **Perturbation** : injection de données erronées, génération de fausses alertes, dénis de services….etc.
- **Détournement :** la compromission des nœuds et leur détournement de leurs fonctions initiales. **[29]**

6. Présentation de quelques attaques

6.1. Usurpation d'identité (Spoofing)

Consiste à se faire passer pour quelqu'un d'autre en utilisant son identité. L'attaquant se présente en utilisant l'identité d'un nœud légitime et peut ainsi communiquer avec les nœuds du réseau sans être rejeté. **[16]**

6.2. Les dénis de services (DOS)

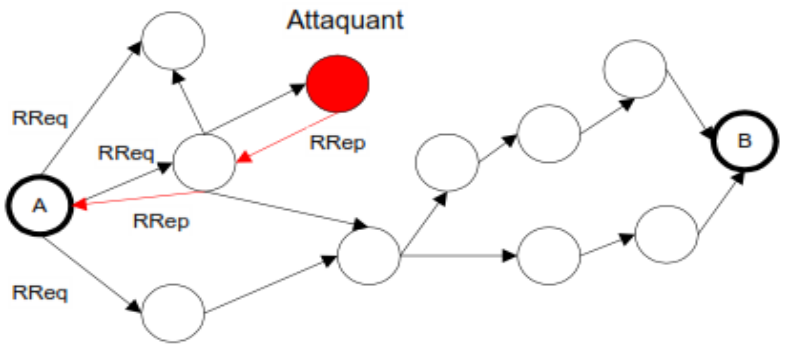
Denial of services (DoS), apparaissent comme les attaques les plus faciles à réaliser par un attaquant. Les modèles de dénis de services qui suivent se dégagent plus particulièrement dans le cas de réseau sans fil Ad Hoc :

- Brouillage du canal radio pour empêcher toute communication.
- Tentative de débordement des tables de routages des nœuds servant de relais.

Non-coopération d'un nœud au bon fonctionnement du réseau dans le but de préserver son énergie. L'égoïsme d'un nœud est une notion propre aux réseaux Ad Hoc. Un réseau Ad Hoc s'appuie sur la collaboration sans condition de ses éléments. **[16]**
Parmi les types d'attaques DOS, on cite l'attaque par inondation « Flooding ».

6.3. Attaque du trou noir (blackhole)

Dans une attaque blackhole, le nœud malveillant essaye d'attirer vers lui le plus de chemins possibles permettant le contrôle de la plus part des données circulant dans le réseau. Pour ce faire, l'attaquant doit apparaître aux autres comme étant très attractif, en présentant des routes optimales. L'attaquant se place généralement à un endroit stratégique et supprime tous les messages qu'il doit retransmettre ou bien permet la mise en œuvre d'une autre attaque. Créant ainsi une sorte de puits ou «trou noir » dans le réseau. **[16]**



RReq : demande de route

RRep : réponse de route

Figure 2.6 : Exemple de l'attaque du trou noir. **[15]**

6.4. Les attaques trou de ver (Wormhole)

Dans une attaque wormhole, un attaquant reçoit des paquets dans un point du réseau, puis les encapsule vers un autre attaquant pour les réintroduire dans le réseau. Dans ce genre d'attaque, les adversaires coopèrent pour fournir un canal à basse latence pour la communication en utilisant une radio pour communiquer avec une puissance plus élevée et des liens à longue portée. Ceci favorise les nœuds voisins à acheminer leurs données à travers l'attaquant. **[16]**

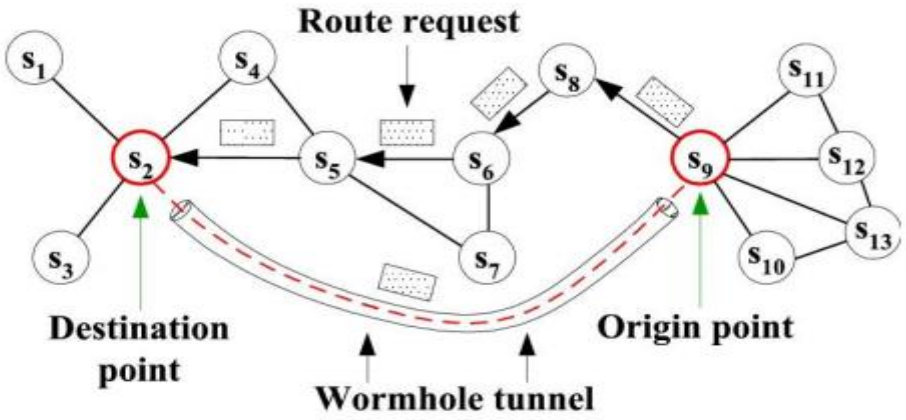


Figure 2.7 : Attaque WormHole dans MANET. **[31]**

6.5. Brouillage (jamming)

Le jamming est une attaque très connue qui s'en prend à la communication sans fil. En effet, vu la sensibilité du média sans fil au bruit, un nœud peut provoquer un déni de service en émettant des signaux à une certaine fréquence pour interférer avec les fréquences radio employées par les nœuds du réseau. **[16]**

7. Comparaison entre les différentes attaques :

Type d'attaque	Objectif ciblé	Mécanisme de sécurité
• **Attaques passives**	Analyse du trafic	- Authentification des messages. - Cryptographie. - Partitionnement.
• **Jamming**	Déni de service	- Détection précoce d'une quantité excessive de paquets émis sur le réseau.
• **Sinkhole**	Disponibilité	- Cryptographie. - Authentification de la source.
• **Wormhole** • **Blackhole**	L'intégrité Confidentialité Fraicheur	-Authentification des messages.

Tableau 2.1 : Comparaison entre les différentes attaques**. [29]**

8. Exigences de sécurité des réseaux Ad Hoc

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. Les spécificités des réseaux sans fil Ad Hoc sont multiples. On peut les répartir en six grands thèmes traitant des caractéristiques des nœuds, de la gestion de l'énergie, des caractéristiques du réseau, des technologies sans fil sous-jacentes, de la mobilité et de la configuration. **[32]**

8.1. Caractéristiques des nœuds

Les participants peuvent posséder des systèmes hétérogènes qui doivent s'interconnecter facilement. Certains éléments peuvent avoir de faibles capacités de calculs. **[32]**

8.2. Gestion de l'énergie

L'énergie doit être conservée au maximum pour éviter d'incessantes recharges du système qui diminuent sa mobilité. Les nœuds chercheront donc à se mettre en veille le plus souvent possible, ce qui provoquera alors une diminution de réactivité de l'ensemble du réseau. **[32]**

8.3. Caractéristiques du réseau

La charge du réseau doit être distribuée équitablement entre les éléments en tenant compte de leur capacité respective. Chaque élément d'un réseau ad hoc est autonome et possède à la fois les fonctionnalités de relais et de point de communication. L'administration de ces éléments reste interne au réseau. L'absence d'infrastructure centralisée sera une contrainte très forte pour la gestion des accès aux ressources du réseau. **[32]**

8.4. Technologie sans fil

Les perturbations dues à l'environnement radio peuvent entraîner des diminutions de débit et de bande passante. Les réseaux sans fil Ad Hoc héritent de l'architecture propre aux technologies WLAN et WPAN, et notamment des couches physiques et liaison de données de ces technologies. **[32]**

8.5. Mobilité

Les éléments étant fortement mobiles, leur sécurité physique est moins assurée que pour un poste de travail fixe. La topologie du réseau peut changer d'autant plus rapidement que les nœuds sont mobiles. Des liens asymétriques peuvent se créer lorsqu'un élément muni d'un récepteur particulièrement sensible est capable de capter les émissions d'un autre nœud qui est hors de portée du premier élément. **[32]**

8.6. Configuration

L'auto configuration permet aux nœuds de s'intégrer facilement dans un réseau. Elle facilite la gestion du réseau car l'interconnexion des éléments ne nécessite qu'un minimum d'intervention technique externe. Cette fonctionnalité est de plus en plus nécessaire pour un déploiement à grande échelle des réseaux sans fil Ad Hoc. **[32]**

9. Classification des solutions de sécurité

Il n'est pas dans nos objectifs de citer les différents types d'attaques sur les environnements sans fil comme nous venons de le voir, mais nous envisageons d'en proposer des solutions qui permettent soit d'empêcher définitivement l'attaque, soit d'en amoindrir l'effet. Dans cette vision, nous présentons les différentes solutions possibles qui peuvent être hiérarchisées sur trois niveaux.

9.1. Le niveau organisationnel

A ce niveau, il faut s'organiser pour gérer correctement ses réseaux sans fil. Il s'agit donc d'adopter une politique de sécurité adaptée aux besoins, aux métiers et aux objectifs de l'entreprise et qui doit être définie par l'organisme concerné. Ce niveau se voit nécessaire dans le cas des grandes organisations ; par contre, il peut être dépassé dans le cas des petits établissements.

9.2. Le niveau physique

Il s'agit de sécuriser l'accès physique aux équipements sans fil de l'établissement (points d'accès, portables, PDA, …etc.)

9.3. Le niveau protocolaire

Dans ce niveau, il faut sécuriser le trafic qui circule dans le réseau sans fil. La collection d'attaques présentées dans la section précédente entraine la disposition des services de sécurité qui sont obligatoires à l'exploitation équitable des réseaux sans fil et plus particulièrement des réseaux Ad Hoc. **[42]**

10. Conclusion

Les réseaux Ad Hoc constituent de par leur nature, un formidable challenge pour la sécurité informatique. Ce sujet va devenir d'autant plus critique que le développement de tels réseaux va rapidement s'amplifier.

La sécurité est un service très important complémentaires qui doit assurer les besoins fondamentale de l'intégrité, la confidentialité, la non répudiation et l'authentification …etc. dans les réseaux Ad Hoc, parce que les réseaux Ad Hoc menés à plusieurs types d'attaques, qui ont différents buts (Suppression, Modification, Interception, Fabrication), ou pour perturber le bon fonctionnement de réseau.

La solution de sécurité peut être classée sous plusieurs niveaux (organisationnel, physique et protocolaire).

Chapitre 3 :

Simulations Et Simulateurs.

1. Introduction

La simulation constitue actuellement l'outil le plus pratique pour évaluer le comportement d'un système complexe dont la formalisation à l'aide de méthodes analytiques est difficile .Pour tester les performances d'un réseau mobile on a souvent recours à la simulation. En effet il serait trop couteux, voire impossible, de mettre en place un réseau à des fins de test pour certains critères. Par exemple, tester les applications sur des réseaux de grande envergure n'est possible en réalité que si l'on dispose de moyens matériels importants.

Cependant, dans le cadre d'une simulation, il suffit de changer les paramètres de simulation correspondant à la taille de réseau. Nous présentons dans ce chapitre, quelques simulateurs les plus utilisées.

2. Simulation

La simulation est une technique de modélisation du monde réel, elle est une technologie moderne très importante et elle permet de représenter le fonctionnement d'un système que l'on veut observer. La modélisation de ce système consiste à répertorier plusieurs grandeurs intéressantes, que nous appelons variable. On définit alors l'état d'un système comme l'ensemble des valeurs que prennent ces variables à un instant donné.

La simulation est couramment utilisée pour mesurer les performances d'un réseau informatique, et plus particulièrement les performances d'un protocole. Elle est nécessaire quand l'expérimentation est trop coûteuse et l'étude théorique trop complexe ou quand on souhaite valider des hypothèses. **[64]**

3. Simulateur

Un simulateur de réseau est un programme, logiciel qui imite le fonctionnement d'un réseau informatique. Dans les simulateurs, le réseau informatique est généralement modélisée à l'aide des dispositifs, le trafic, …etc. et les performances sont analysées. En règle générale, les utilisateurs peuvent ensuite personnaliser le simulateur pour répondre à leurs besoins d'analyse spécifiques. **[60]**

4. Simulation de réseau et un simulateur

D'une manière générale, des simulateurs de réseaux tentent de modéliser les réseaux du monde réel. L'idée principale est que si un système peut être modélisé, alors les caractéristiques du modèle peuvent être modifiées et les résultats correspondants peuvent être analysés. Comme le processus de modification du modèle est relativement pas cher que la mise en œuvre réelle complète, une grande variété de scénarios peut être analysé à faible coût (par rapport à apporter des modifications à un véritable réseau).

Cependant, si tous les détails sur les réseaux sont bien modélisés, ils seront assez près afin de donner au chercheur un aperçu significatif dans le réseau sous test, et comment les changements auront une incidence sur son fonctionnement. **[61]**

5. Type des simulateurs

Différents types de simulateurs réseaux peuvent être caractérisé et basé sur plusieurs critères, comme commercial ou gratuit ou ils sont simple ou complexe.

5.1. Simulateurs commerciaux et open source

5.1.1. Simulateurs commerciaux

Certains des simulateurs de réseaux sont de nature commerciale qui signifie qu'ils ne fourniraient pas le code source de son logiciel ou les packages affiliés aux utilisateurs gratuitement. Tous les utilisateurs doivent payer pour obtenir la licence d'utiliser leur logiciel ou payer pour commander des forfaits spécifiques pour leurs propres besoins d'utilisation spécifiques (OPNET simulateur commercial). **[61]**

- L'avantage est qu'il a généralement complète et mise à jour des documentations.
- Ils peuvent être constamment maintenus par certains membres du personnel spécialisé dans cette société. **[61]**

5.1.2 Simulateurs Open Source

Le simulateur de réseau source ouvert est désavantageux, dans cet aspect, il n'y a pas assez de gens spécialisés qui travaillent sur la documentation. Ce problème peut être grave lorsque les différentes versions viennent avec beaucoup de nouvelles choses et il deviendra difficile de retracer ou de comprendre les codes précédents sans documentation appropriée. Au contraire, le simulateur de réseau open source a l'avantage que tout est très ouvert et tout le monde ou l'organisation peut contribuer et trouver des bogues dans elle (NS-2, NS-3 simulateurs open source). **[61]**

- L'interface est également ouverte pour l'amélioration future.
- Il peut aussi être très flexible et refléter les plus récents développements de nouvelles technologies d'une manière plus rapide que les simulateurs de réseaux commerciaux.
- Le manque de suffisamment de documentation systématique et complète et le manque de soutien de contrôle de version peut conduire à un problème grave et peut limiter l'applicabilité et la vie en temps des simulateurs de réseau open source. **[61]**

	Les simulateurs réseaux
Commercial	OPNET, QualNet
Open source	NS2, NS3, OMNET++, SSFNet, J-Sim

Tableau 3.1 : Les simulateurs réseaux. **[61]**

5.2 Complexe ou simple

Actuellement, il y a une grande variété de simulateurs de réseaux, allant des simples aux plus complexes. Minimalement, un simulateur de réseau devrait permettre aux utilisateurs de représenter une topologie de réseau, de définir les scénarios, en spécifiant les nœuds sur le réseau, les liens entre les nœuds et le trafic entre les nœuds. Des systèmes plus complexes peuvent permettre à l'utilisateur de spécifier tout ce qui concerne les protocoles utilisés pour traiter le trafic de réseau. Les applications graphiques permettent également aux utilisateurs de visualiser facilement le fonctionnement de leur environnement simulé.

Certains d'entre eux peuvent être à base de texte et peut fournir une interface moins visuelle ou intuitive, mais peut permettre à des formes plus avancées de personnalisation. D'autres peuvent être la programmation orientée et peut fournir un cadre de programmation qui permet aux utilisateurs de personnaliser pour créer une application qui simule l'environnement de mise en réseau pour les tests. **[61]**

6. Simulateurs réseaux les plus utilisés

Plusieurs simulateurs pour réseaux informatique sans fil ont été proposés ces dernières années, parmi lesquels NS-2, GloMoSim, JiST/SWANS, GTSNetS, OMNet++, Opnet, …etc. Ces simulateurs offrent tous un environnent avarice de programmation pour l'implémentation et l'évaluation des performances des protocoles de communication.

6.1 NS2 (Network Simulator-2)

6.1.1. Présentation du Simulateur NS-2

Network Simulator (NS-2) est un simulateur à événements discrets orienté objet, écrit en C++ avec une interface qui utilise le langage OTcl (Object Tool Command Langage). A travers ces deux langages il est possible de modéliser tout type de réseau et de décrire les conditions de simulation : La topologie réseau, le type du trafic qui circule, les protocoles utilisés, les communications qui ont lieu ...etc. Le langage C++ sert à décrire le fonctionnement interne des composants de la simulation. Pour reprendre la terminologie objet, il sert à définir les classes. Quant au langage OTcl, il fournit un moyen flexible et puissant de contrôle de la simulation comme le déclenchement d'événements, la configuration du réseau, la collecte de statistiques, …etc. **[41]**
Toute simulation sous NS-2 se base sur un modèle composé des éléments suivants :

- **Nœuds du réseau** : Nœuds d'extrémités où le trafic est généré ou consommé plus les nœuds de routage (nœuds intermédiaires).
- **Liens de communications** entre ces nœuds**.**
- **Agents** : représentent les protocoles au niveau transport (TCP, UDP), ces agents sont connectés aux nœuds et sont attachées les uns aux autres pour permettre l'échange de données.
- **Application** : qui génère le trafic des données. **[41]**

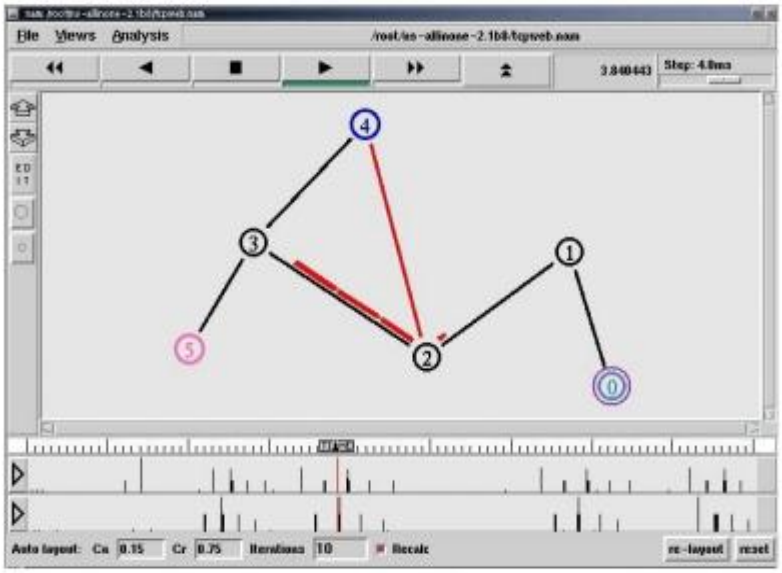


Figure 3.1 : Interface de simulateur NS-2. **[62]**

6.1.2. Avantages NS-2

Network Simulator offre plusieurs avantages comme :

- Un logiciel de simulation multicouche.
- Un outil complètement libre pour plusieurs plateformes.
- Possibilité d'ajouter des composants à la demande.
- Développement orienté objet.
- Du fait de sa popularité, de nombreux protocoles sont à priori disponibles pour NS-2.

- L'analyse des résultats est en général peu aisée, le résultat de la simulation étant essentiellement composé d'un fichier retraçant l'ensemble des envois, réceptions et suppressions de paquets. Un certain nombre de scripts ont été développés (ou sont en cours de développement) pour faciliter cette analyse.

- Les capacités de NS-2 ouvrent le champ à l'étude de nouveaux mécanismes au niveau des différentes couches de l'architecture réseau. Alors il est devenu l'outil de référence pour les chercheurs du domaine qui peuvent ainsi partager leurs efforts et échanger leurs résultats de simulations. **[16]**

- Il est open source et gratuit.
- Il englobe les contributions de plusieurs chercheurs.
- Il peut être étendu à d'autres modèles grâce à sa conception orientée objet et son implémentation en C++.
- Il est riche en modèles et en protocoles pour les deux environnements filaires et sans fil. **[41]**

6.1.3 Les composants disponibles dans NS-2

La liste des principaux composants actuellement disponible dans NS2 sont représentés par catégorie dans le tableau suivant :

Application	Web, Ftp, Telnet, générateur de trafic (CBR…).
Transport	TCP, UDP, RTP, SRM
Routage	Statique, dynamique (vecteur distance) et routage multipoint (DVMRP, PIM, AODV).
Gestion de file d'attente	RED, DropTail, Token bucket,
Discipline de service	CBQ, SFQ, DRR, fair queueing.
Système de service	CSMA/CD, CSMA/CA, Lien point à point.

Tableau 3.2 : Les principaux composants de NS-2**. [32]**

6.2. OMNet++ (Objective Modular Network Tested in C++)

6.2.1. Présentation du Simulateur OMNet ++

OMNET ++ a été à la disposition du public depuis Septembre 1997 et dispose actuellement d'un grand nombre d'utilisateurs. Contrairement ns-2 et ns-3, OMNET ++ est non seulement conçu pour les simulations de réseau. Il peut être utilisé pour la modélisation de multiprocesseur, des systèmes matériels distribués et évaluation des performances des systèmes logiciels complexes. Cependant, il est le plus souvent utilisé pour la simulation des réseaux informatiques. **[62]**

OMNeT ++ est un simulateur open source, l'environnement d'architecture à base de composants modulaire et ouvert pour la simulation d'événements discrets. Il est gratuit pour un usage académique et sans but lucratif. **[60]**

OMNeT ++ est actuellement gagne en popularité en tant que plate-forme de simulation de réseau dans la communauté scientifique, ainsi que dans les industriels, et la construction d'une grande communauté d'utilisateurs. **[60]**

OMNeT ++ fonctionne sur Linux, d'autres systèmes Unix et Windows, plates-formes de système d'exploitation. **[60]**

OMNET ++ distribution a été développé en utilisant l'approche orientée composants qui favorise les modèles structurés et réutilisables. En outre, OMNET ++ possède une vaste interface graphique utilisateur (GUI) et le soutien du renseignement. **[62]**

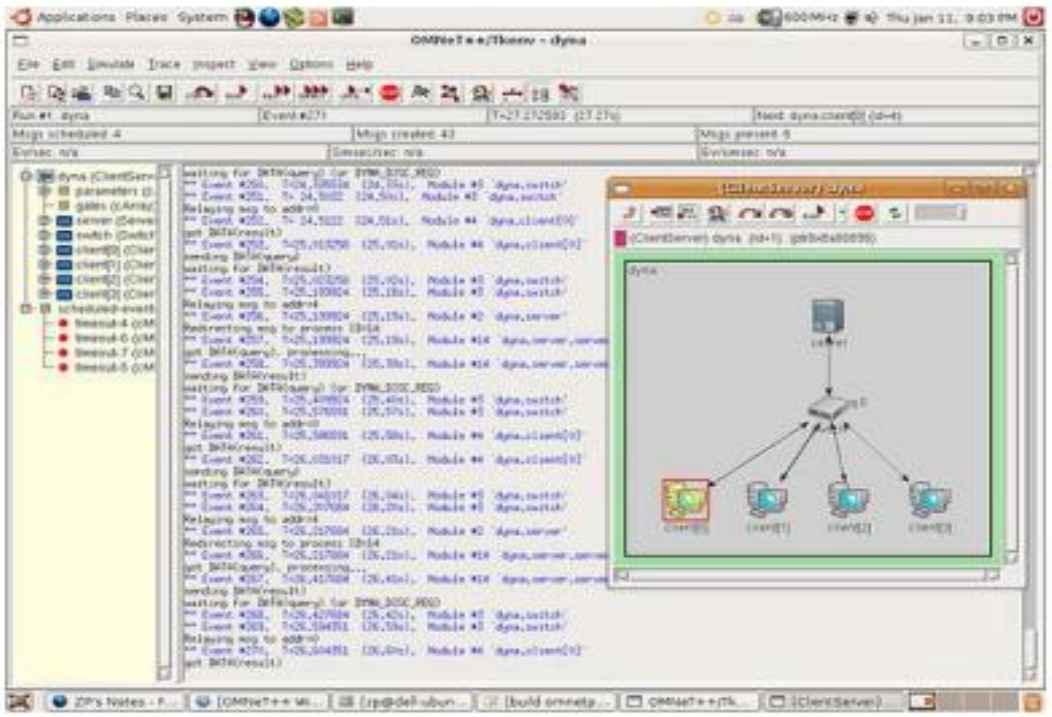


Figure 3.2 : Interface de simulateur NS-2**. [62]**

6.2.2. Composants OMNet++

OMNeT ++ est composé de :

- **Editeur graphique de réseau**: Un éditeur graphique de réseau (NED) pour permettre la construction d'une topologie graphique, la création de fichiers dans la description du langage réseau (NED).
- **Bibliothèque Kernel:** Une bibliothèque noyau de simulation contient les définitions des objets utilisés pour la création de la topologie
- **Interface de ligne de commande**: Comprend les interfaces graphiques et de ligne de commande pour l'exécution de simulation
- **Un outil de documentation de modèle pour la documentation** : Deux types de modules existent : modules simples et des modules composés. **[60]**

6.3. J-Sim (Java Simulator)

6.3.1. Présentation du Simulateur J-Sim

J-Sim est un système de simulation basé sur Java et qui sert à construire des modèles réseaux et les analyser par rapport aux références de données expérimentales. J-Sim a été conçu principalement pour la biomédecine et la physiologie, mais son moteur de calcul est tout à fait générale et s'applique à plusieurs domaines scientifiques. Les modèles J-Sim peuvent mélanger les Formules aux dérivées partielles, Formules implicites, les intégrales, sommations, les événements discrets et du code procédural selon le cas à étudier. **[63]**

Son organisation est similaire à celle de OMNeT ++. J-Sim est un simulateur de temps réel axé sur les processus, autrement dit, une simulation fonctionne de la même manière comme un véritable système, en ce sens que les exécutions d'événements sont effectuées en temps réel, par opposition aux points fixes de temps en simulation d'événements discrets. **[60]**

Comme dans NS-2, deux langues sont utilisées dans J-Sim: Java pour décrire et mettre en œuvre des modèles et un langage de script pour construire, configurer et / ou contrôler la simulation lors de l'exécution. J-Sim a été conçu pour soutenir les langages de script (Tcl, Perl ou Python), cependant, la mise en œuvre disponible est basée sur Tcl. J-Sim fournit Tcl commandes spécifiques, les (RUV) des commandes virtuelles d'exécution, pour simplifier la manipulation et la configuration des composants de réseau lors de la simulation d'exécution. J-Sim comprend la plate-forme INET qui est dédié à la simulation des réseaux. **[60]**

6.3.2. Composants de J-Sim

J-Sim est un logiciel gratuit de mise en œuvre de charge pour la simulation d'une architecture à base de composants :

- **L'Autonome Component Architecture (ACA) :** Les ACA imite la conception du circuit et de fabrication modèle intégrée en termes de la façon dont les composants sont spécifiés, conçus et assemblés.

- **Internetworking (INET)**: J-Sim comprend cette plate-forme INET spécifique, dédié au réseau de simulation, mais ne se limite pas à ce domaine. **[60]**

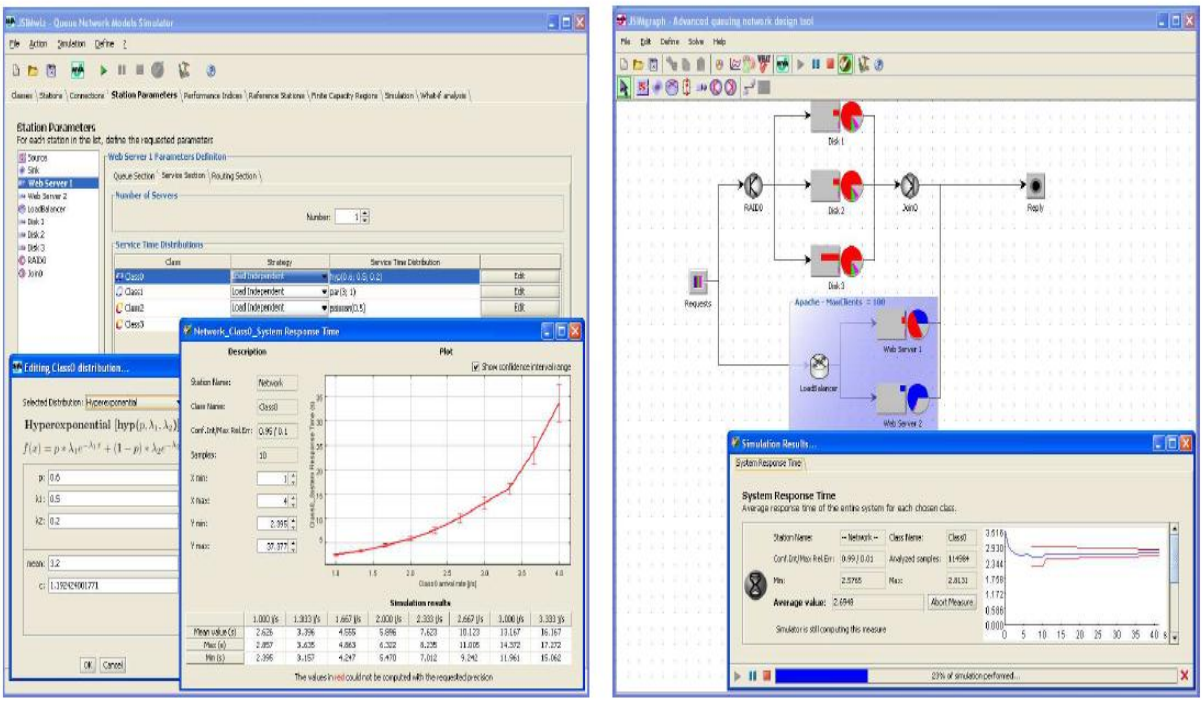


Figure 3.3 : L'interface graphique de simulateur J-Sim. **[65]**

6.4. OPNET (Optimized Network Engineering Tools)

6.4.1. Présentation du Simulateur OPNET

OPNET est un environnement de simulation qui permet la modélisation de réseaux de communication grâce à ses bibliothèques de modèles (routeurs, commutateurs, stations de travail, serveur, etc.) et de protocole (TCP/IP, FTP, FDDI, Ethernet, ATM, …etc.). Le module de radio Opnet permet la simulation des réseaux de radiocommunication (hertzien, téléphonie cellulaire et satellitaire).**[63]**

Il fournit un environnement mondial pour modéliser, simuler et évaluer les performances de tous les types de câble et réseaux de communication sans fil et des systèmes distribués. Il est disponible sur Windows 2000, XP, Linux et les plates-formes Solaris. **[60]**

L'environnement OPNET inclut des outils graphiques pour les scénarios et les modèles conception, simulation de scénarios, la collecte des données et l'analyse des données. Une simulation au sein de OPNET est représentée par un projet, y compris un ensemble de scénarios. Ce projet est créé par l'éditeur de projet a également connu sous le nom de l'interface centrale OPNET. **[60]**

Toutes les fonctionnalités disponibles peuvent être consultées à partir de cet éditeur. Il fournit un accès à d'autres éditeurs qui proposent des fonctions, y compris le nœud et le processus la création du modèle, la construction de formats de paquets, et la création de filtres et paramètres.

OPNET offre de nombreuses fonctions supplémentaires, y compris un haut niveau Architecture (HLA) module, qui permet la communication entre les différents simulateurs. **[60]**

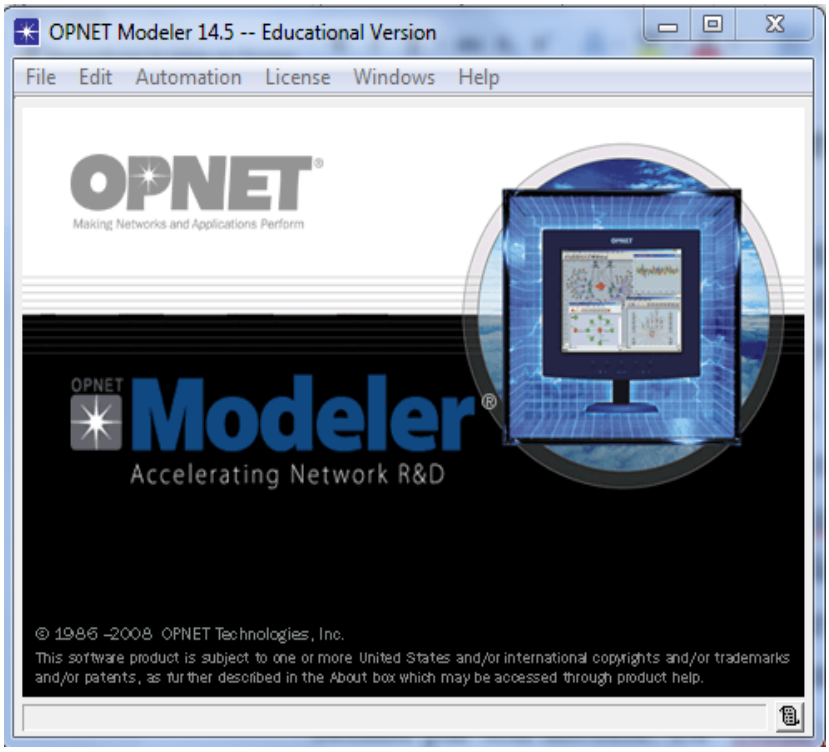


Figure 3.4: L'interface de simulateur OPNET**.**

6.4.2. Domaines de modélisation de Simulateur OPNET

OPNET permet la modélisation hiérarchique en définissant un réseau comme un ensemble de sous-modèles représentant des sous-réseaux ou des nœuds. La modélisation est constituée de trois domaines (Network domain, Node domain et Process domain). **[60]**

- **Le domaine réseaux (Network domain)** : est le niveau le plus élevé de la hiérarchie d'Opnet. Il permet de définir la topologie du réseau en y installant des routeurs, des hôtes, des équipements tels que des switch, reliés entre eux par des liens.

Chaque entité de communication (appelé nœud) est entièrement configurable et est définie par son modèle. **[63]**

- **Le domaine nœud (Node domain) :** permet quant à lui de définir la constitution des nœuds (routeur, stations de travail, hub, …etc.). Le modèle est défini à l'aide de blocs appelés modules. **[63]**

- **Le domaine processus (Process domain) :** est le niveau dans lequel on définit le rôle de chaque module programmable. Un module possède par défaut un processus principal, auquel peuvent s'ajouter des processus fils accomplissant une sous-tâche précise. **[63]**

Opnet fournit des mécanismes permettant à tous les processus créés à l'intérieur d'un domaine processus de communiquer entre eux, via un bloc de mémoire partagée, ou l'ordonnancement d'interruptions logicielles. **[63]**

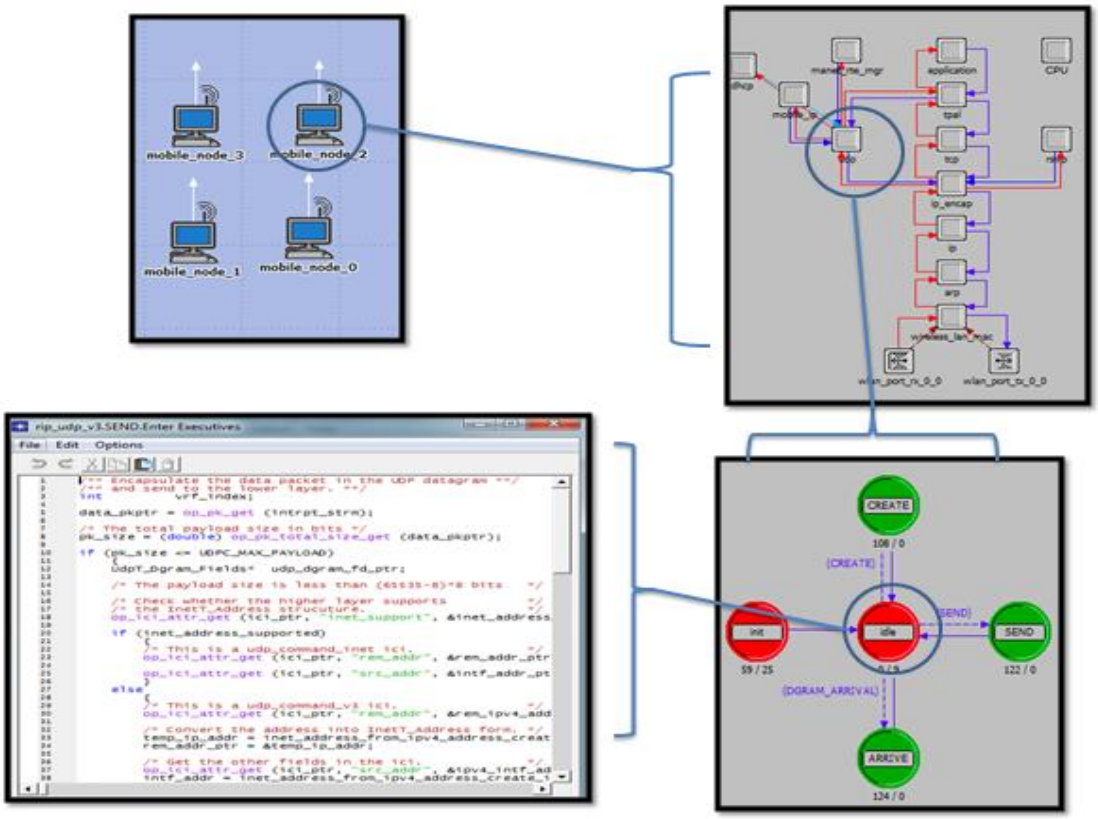


Figure 3.5: Domaine de modélisation de OPNET.

7. Comparaison entre quelques simulateurs

Plusieurs simulateurs existent tel que NS-2, J-Sim, OPNET, OMNET++. Pour cela, une brève étude comparative entre ces simulateurs est présentée dans le tableau 4.3 :

Fonctionalités	OMNet++	NS-2	OPNET	J-Sim
Langage supporté	C++	C++/OTCL	C++/Java	Java
License	Open source	Open source	Commercial	Open source
GUI support	Bon	Pauvre	Excellent	Bon
Temps nécessaire pour apprendre	Modérer	Longue	Longue	Modérer
Plate-forme	Linux, mac-os, unix	Unix, mac-OS, Microsoft window Cygwin	C, C++, OPNET modeler software	Matlab
Les outils disponibilité d'analyse	✓	✓	✓	✓
Les outils de visualisation	✓	✓	✓	✓
Possibilité de conception et modifié les scénarios	✓	✓	✓	✓
Création des fichiers traçant	✓	✓	✓	✓
Interaction avec les systèmes réels	✓	✓	✓	✓
Communication avec d'autres modules			✓	
Possibilités rapides de simulation			✓	

Tableau 3.3: Comparaison entre différents simulateurs réseaux**. [60]**

8. Critères de choix d'un simulateur

Il existe une multitude de simulateurs de réseaux, certains plus spécialisés, d'autres généralistes. Le choix du simulateur est basé sur plusieurs critères : **[64]**

- **Bibliothèque de modèles** : Typiquement les protocoles implémentés dans le simulateur. Si l'on souhaite utiliser un protocole déjà inclus dans la bibliothèque, il est alors inutile de l'implémenter.

- **Fiabilité du simulateur et des protocoles simulés** : La fiabilité des protocoles inclus dans le simulateur est primordiale pour rendre la mesure de performances d'un protocole la plus fidèle à la réalité.

- **Performances brutes :** Se mesurent en temps d'exécution et en utilisation de la mémoire. Si on souhaite simuler un réseau comportant un grand nombre de nœuds, le temps d'exécution doit rester raisonnable et la mémoire utilisée adaptée à la machine exécutant le simulateur.
- **Facilité d'extension :** La facilité d'ajout de nouveaux modèles au simulateur est primordiale pour en évaluer les performances.

- **Mesure de performances :** Certains simulateurs incluent la génération automatique statistique en fonction de différentes métriques.

- **Type de réseau :** Architecture (filaire ou Ad Hoc) ou ses applications.

- **Licence de distribution :** Définit les droits d'utilisation du logiciel, les droits de diffusion (Duplication) et les droits de modification. **[64]**

9. Conclusion

Simulation de réseau est la méthode la plus utile et couramment utilisé pour évaluer les différentes topologies de réseau sans mise en œuvre du monde réel. Simulateurs de réseau sont largement utilisés par la communauté des chercheurs pour évaluer les nouvelles théories et hypothèses.

Il y a un certain nombre de simulateurs de réseaux (NS-2, OMNET ++, OPNET, J-Sim). Par conséquent, la sélection d'un simulateur de réseau pour évaluer le travail de recherche est une tâche cruciale pour les chercheurs.

Une comparaison des simulateurs présentés par rapport aux critères d'évaluation définis est présentée dans le Tableau 3.3.

Chapitre 4 :

Attaque par inondation (Flooding) dans Les Réseaux Ad Hoc.

1. Introduction

Le réseau Ad Hoc est plus vulnérable à des attaques par déni de service (DOS) lancé avec force à travers des nœuds malveillants ou attaquant.

L'inondation est une des opérations les plus fondamentales dans les réseaux Ad Hoc mobiles, l'inondation est l'opération normale qui est habituellement utilisé pour la diffusion de paquets de commande. La plupart des principaux protocoles de routage comme DSR, AODV, ZRP etc… reposent sur les inondations pour la diffusion de découverte de route, la maintenance des routes et des paquets de mise à jour de la topologie. L'inondation est une fonction très fréquemment invoquée dans les MANET.

Dans ce chapitre nous intéressons vers l'attaque par inondation « Flooding » dans le protocole AODV des réseaux Ad Hoc.

Mobiles Ad Hoc Networks (MANET) sont nouveau paradigme des réseaux sans fil offrant une mobilité illimitée à des nœuds sans infrastructure fixe ou centralisée. Chaque nœud participant au réseau agit comme routeur pour acheminer les données de la source à la destination. Cette caractéristique rend MANET plus vulnérables aux attaques de routage. L'attaque par inondation est une attaque qui consomme plus de ressources, comme la bande passante, la puissance de la batterie…etc. Les protocoles de routage réactifs comme AODV et DSR utilisés dans MANET reposent sur les inondations des paquets de RREQ pour la découverte de route, ce qui rend plus facile pour le nœud malveillant de lancer l'attaque par inondation en inondant les paquets de demande d'itinéraire (RREQ) dans le réseau.

2. L'inondation

L'inondation ou la diffusion simple consiste à répéter un message dans tout le réseau. Un nœud qui initie l'inondation envoie le paquet à tous ses voisins directs. De même, si un nœud quelconque du réseau reçoit le paquet pour la première fois, il le rediffuse à tous ses voisins, ainsi de proche en proche le paquet inonde le réseau (Figure 4.1).

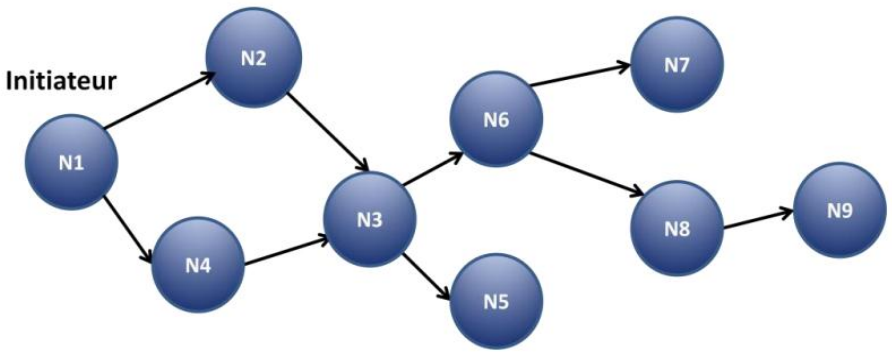


Figure 4.1. Mécanisme d'inondation. **[32]**

Durant l'inondation les nœuds peuvent appliquer des traitements de contrôle dans le but d'éviter certains problèmes, tels que le bouclage et la duplication de messages. Le mécanisme d'inondation est utilisé généralement dans la première phase du routage, plus exactement dans la procédure de découverte des routes, et cela dans le cas où le nœud source ne connaît pas la localisation exacte de la destination. **[32]**

3. Types d'attaques par inondation (Flooding)

Les nœuds malveillants peuvent également interrompre le fonctionnement normal dans le processus de transmission de paquets par inondation des nœuds cibles avec d'énormes paquets inutiles. Les nœuds qui sont sous des attaques d'inondation sont incapables de recevoir ou de transmettre des paquets, de même que tous les paquets qui leur sont destinés sont rejetés du réseau. **[32]**

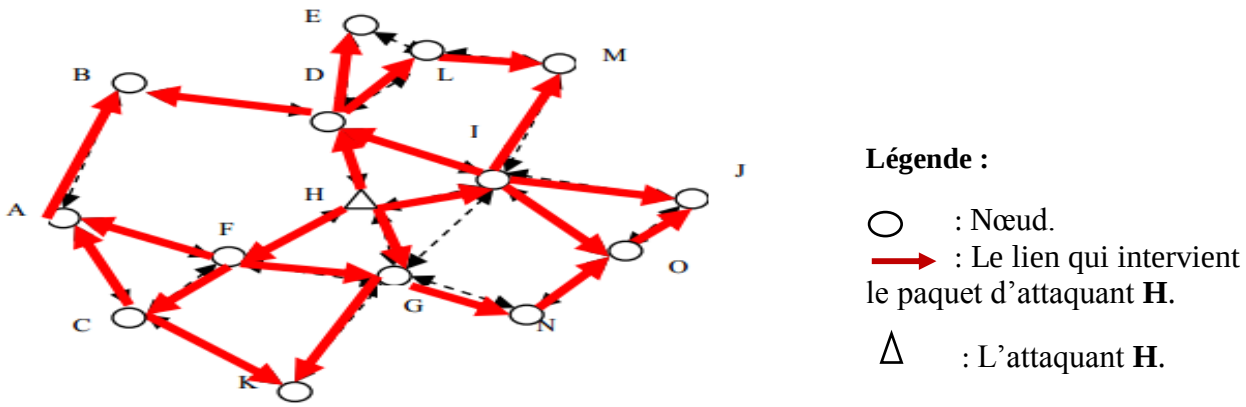


Figure 4.2: Attaque par inondation (Flooding)**. [39]**

3.1. But de l'attaque Flooding

Dans les attaques Flooding, l'attaquant épuise les ressources du réseau, telles que la bande passante et de consommer les ressources d'un nœud, comme la puissance de calcul et la batterie ou de perturber le fonctionnement de routage pour provoquer une grave dégradation des performances du réseau. Par exemple, dans le protocole AODV, un nœud malveillant peut envoyer un grand nombre de RREQs dans une courte période à un nœud de destination, qui n'existe pas dans le réseau. Parce que personne ne répondra aux RREQs, ces RREQs inonderont l'ensemble du réseau. En conséquence, toute la puissance de la batterie de nœud, ainsi que la bande passante réseau sera consommée et pourrait conduire à un déni de service (DOS). **[39]**

3.2. Types de Flooding

L'Attaque Flooding peut être commencé par inonder le réseau avec de faux RREQ ou paquet de données, menant au blocage du réseau et réduit la probabilité de transmission de données du réel nœud. Dépend Sur quel type de paquet utilisé pour inonder dans le réseau est classé en trois catégories, sont Hello Flooding, RREQ Flooding Et Data Flooding. **[42]**

3.2.1. Hello Flooding

Certains protocoles de routage dans un réseau sans fil exigent des nœuds pour diffuser des messages Hello, à eux-mêmes annoncé à leurs voisins. Un nœud qui reçoit un tel message peut supposer qu'il est dans une plage de l'expéditeur. Certains nœuds de mauvaise conduite dans le flot de réseau continu le paquet Hello. Sans la maintenance de l'intervalle de Hello. Il crée les perturbations dans le fonctionnement du réseau. Cette activité détourne l'action du nœud légitime dans le réseau. **[42]**

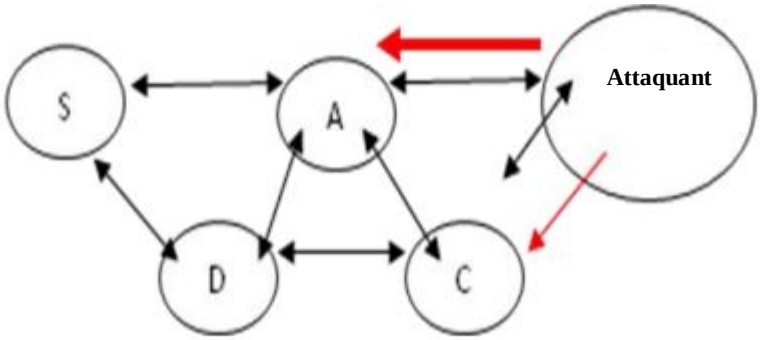


Figure 4.3: L'attaque Hello Flooding**. [42]**

3.2.2. RREQ Flooding

Dans ce type d'attaque, le nœud inondeur diffuse plusieurs paquets RREQ pour le nœud qui existent ou non existent dans le réseau. Dans ce type d'attaque Flooding, l'attaquant désactive le taux de RREQ, Pour activer l'inondation par des paquets RREQ, donc il consomme de la bande passante du réseau. **[40]**

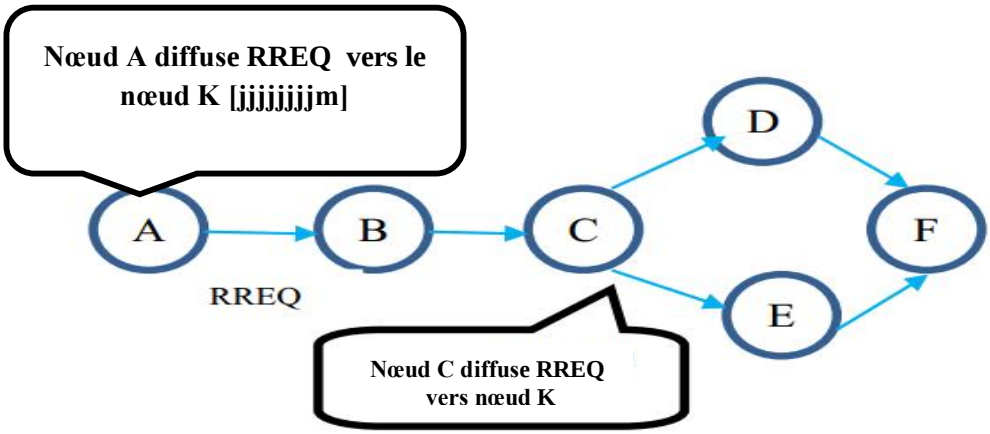


Figure 4.4: L'attaque RREQ Flooding**. [40]**

3.2.3. Data Flooding

En DATA Flooding (données d'inondation), des paquets de données sont utilisées pour inonder le réseau. Dans ce nœud malveillant l'inondeur construit un chemin d'accès à tous les nœuds puis envoyer la grande quantité de paquets de données fausses, et ce paquet de données fausses échouent les ressources du réseau. **[40]**

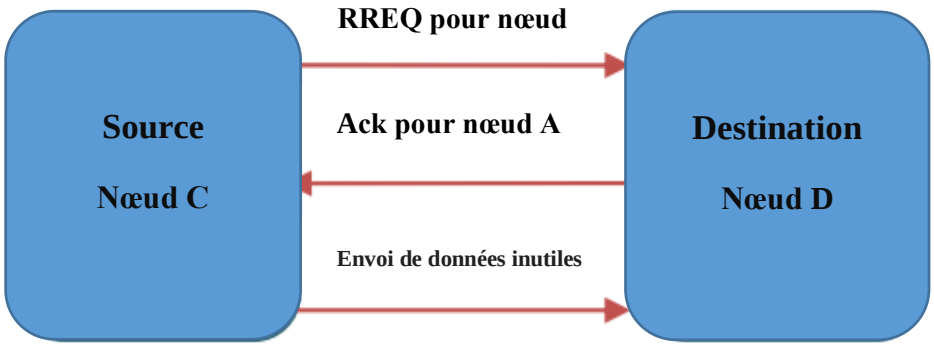


Figure 4.5 : L'attaque DATA Flooding. **[40]**

- **Ack :** L'acquittement**.**

4. Des vulnérabilités dans AODV

Les attaques par saturation peuvent incroyablement réduire les performances du protocole de routage réactif et affecter un nœud dans des manières suivantes :

- Dégrader les performances dans un tampon (buffer).
- Dégrader les performances dans l'interface sans fil.
- Dégrader les performances dans des paquets RREQ. **[43]**

Des vulnérabilités dans AODV est conçu pour une utilisation dans les réseaux, où la communication est produit sur la base de la confiance mutuelle entre les nœuds et peut supposer qu'il n'y a pas de nœud intrus malveillant. Prenant le fonctionnement de AODV, essentiellement son processus de découverte de route, il est plus vulnérable aux attaques par déni de service. Dans la procédure de découverte de route de AODV diffuse un paquet de RREQ (contenant une émission ID, les adresses de source et destination, et le numéro de séquence de destination), et attendre pendant un certain temps pour obtenir un RREP ou un autre paquet de contrôle (RREQ, RREP, RERR, Hello). Si ce temps était à expiration, le nœud peut essayer même processus une fois de plus pour obtenir un itinéraire valide. AODV ne fournit aucun mécanisme de sécurité de telle sorte que DOS (l'attaque de Flooding) peut se faire facilement. **[43]**

5. Effets de Flooding

L'attaque Flooding peut sérieusement dégrader les performances des protocoles de routage réactifs et affecter un nœud dans les routes :

5.1. Affecter les performances dans un tampon (buffer)

Le tampon utilisé par le protocole de routage peut déborder depuis un protocole réactif a pour tamponner les paquets de données pendant le processus de découverte de route. **[44]**

5.2. Dégrade la performance dans l'interface sans fil

Selon la conception de l'interface sans fil, le tampon utilisé par la carte d'interface réseau sans fil peut déborder en raison du grand nombre de RREQ être envoyer. Pareillement, des paquets de données authentiques peuvent être supprimés si le routage des paquets a la priorité sur les paquets de données**. [44]**

5.3. Dégrader les performances dans des paquets RREQ

Puisque les paquets RREQ sont diffusés dans l'ensemble du réseau, l'augmentation du nombre de paquets RREQ donne les résultats de réseau (dans la couche MAC des collisions, la congestion dans le réseau seront affectés, des retards pour les paquets de données, TCP sensibles aux temps d'aller-retour). **[44]**

5.4. Dégrade la performance dans la durée de vie de MANET

Les nœuds MANET sont susceptibles comme la puissance et la bande passante limitée, le paquet de l'attaquant (Route Request Flooding Attack) peut réduire la durée de vie du réseau par le biais de transmissions RREQ inutiles, ainsi que les frais généraux supplémentaires d'authentification d'un grand nombre de RREQs, si elle est utilisée. **[44]**

6. Travaux connexes

6.1. Les auteurs **[42]** représentent des œuvres proposées par divers auteurs sur les attaques Flooding. Leurs contribution dans cet article est qu'ils ont présenté les détails de comparaison des différents systèmes à base de compteurs.

Ils concentrent sur de diverses approches pour surmonter l'attaque de Flooding en utilisant le système de rediffusion basé par différents compteurs. Ces systèmes sont efficaces pour développer la valeur seuil appropriée de sorte que le paquet de rediffusion de nœud à ses voisins et forment un itinéraire et augmentent également la joignabilité, économiser la rediffusion et la latence moyenne. Le résultat d'exécution de ses travaux donne meilleur impact pour surmonter l'attaque de Flooding.

6.2. Les auteurs **[56]** expliquent le principe de L'attaquant (s) qui peut inonder le noeud attaqué avec des paquets d'ordures à des fins de colmatage. L'attaquant (s) peut atteindre cet objectif en ; soit des nœuds de Flooding avec demande redondante ou aléatoire par des paquets Route (RREQ), des paquets de données, ou les deux. L'attaque de Flooding malveillant; soit par un seul attaquant ou plusieurs attaquants de collaboration, peuvent être classés dans les cas possibles suivants :

Cas 1: Un attaquant, faisant semblant d'être un nœud source, choisit d'inonder en générant des paquets RREQ excessifs. Ici, l'attaquant choisit de garder la même adresse source dans tous les paquets RREQ comme représenté sur la figure 4.6.

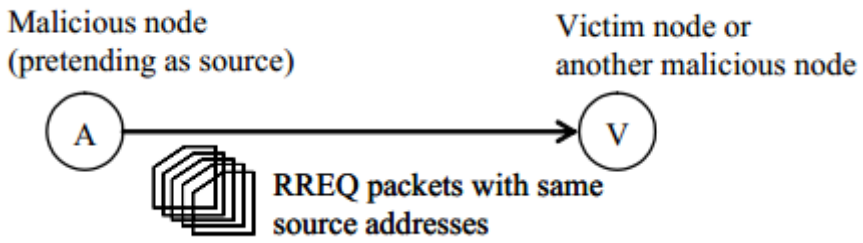


Figure 4.6: Cas 1, un attaquant inonde les paquets RREQ avec adresse source redondant. **[56]**

Cas 2: Un attaquant, prétendant à nouveau être le nœud source, choisit d'inonder en générant des paquets RREQ excessifs avec des adresses sources différentes, se faisant passer comme le montre la figure 4.7.

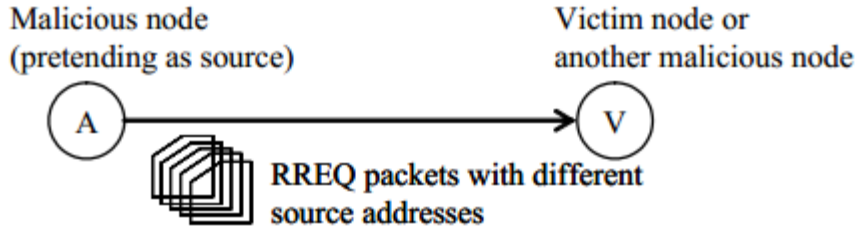


Figure 4.7: Cas 2, Un attaquant inonde les paquets RREQ avec des adresses sources différentes. **[56]**

Cas 3: Un attaquant choisit d'inonder en générant des paquets de données excessives au lieu de paquets RREQ. Le cas est expliqué plus loin dans la figure 4.8.

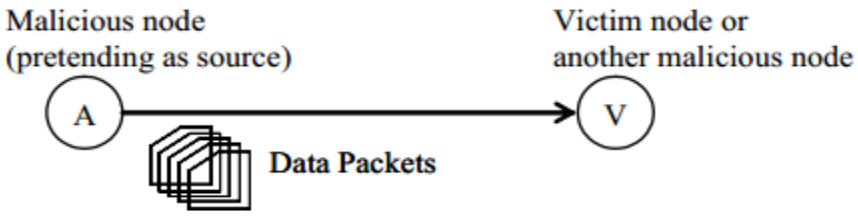


Figure 4.8 : Cas 3, Un attaquant inonde beaucoup de paquets de données. **[56]**

Cas 4-1: Un attaquant peut mener une attaque de collaboration avec un autre attaquant. Dans ce cas, l'un d'eux attaque le nœud de la victime (ou un autre nœud malveillant) avec des paquets RREQ avec des adresses sources redondantes, tandis que son homologue attaque le nœud de la victime (ou un autre nœud malveillant) avec des paquets de données comme le montre la figure 4.9.

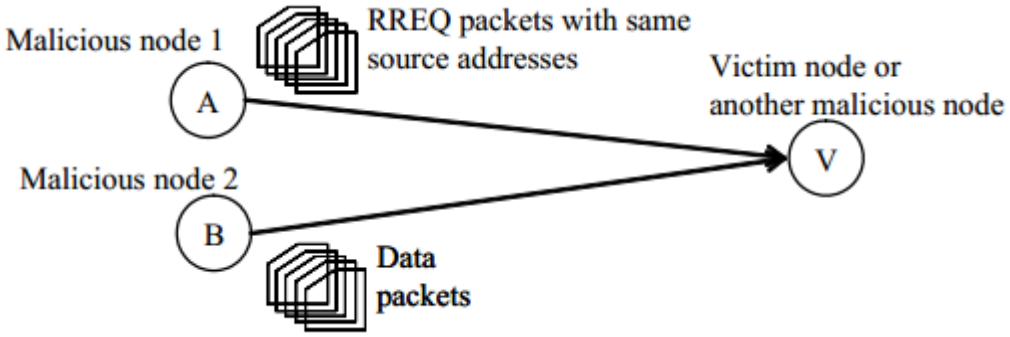


Figure 4.9 : Sous-cas 4-1, Une attaque concertée est menée en combinant cas 1 et 3. **[56]**

Cas 4-2: Ceci est encore un cas de mener des attaques de collaboration. Dans ce cas, l'un d'eux attaque le nœud de la victime (ou un autre nœud malveillant) avec des paquets RREQ ayant des adresses sources différentes, tandis que son homologue attaque le nœud de la victime (ou un autre nœud malveillant) avec des paquets de données comme le montre la Figure 4.10.

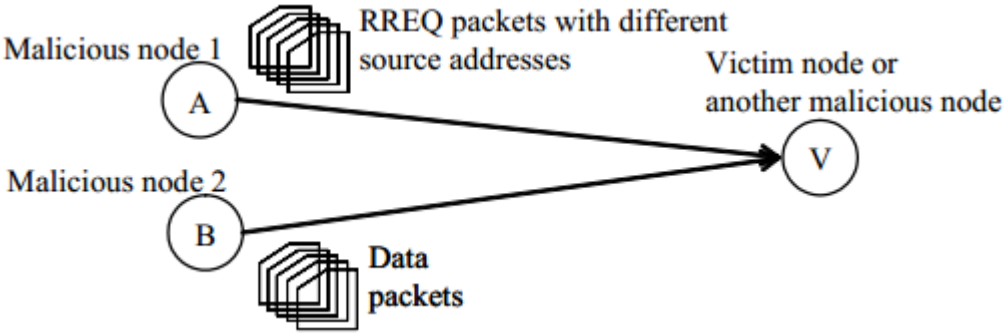


Figure 4.10 : Sous-cas 4-2, Une attaque concertée est menée en combinant cas 2 et 3. **[56]**

Les attaques mentionnées ci-dessus sont menées afin d'obstruer et de paralyser le nœud de la victime et éventuellement le réseau complet.

Dans cet article les auteurs proposent un mécanisme de défense menée dans les réseaux mobiles Ad Hoc. Le schéma proposé améliore la quantité de traitement de paquets légitime à chaque nœud. Les résultats de simulation montrent que le schéma proposé améliore également le rapport de bout en bout de la livraison des paquets.

6.3. Les auteurs **[51]** expliquent l'attaque de Flooding par la Route Request (RREQ), est une sorte d'attaque de déni de service, qui vise à inonder le réseau avec un grand nombre de RREQs vers les destinations du réseau. Dans cette attaque, le noeud malveillant va générer un grand nombre de RREQs, éventuellement dans la région des centaines ou des milliers de RREQs, dans le réseau jusqu'à ce que le réseau est saturé avec RREQs et incapable de transmettre des paquets de données. Beaucoup de différents protocoles de routages réactifs (sur demande) proposés pour MANET peuvent souffrir de ce genre d'attaque.

Dans un protocole de routage dynamique à la demande, on utilise généralement un procédé "de découverte de route" pour obtenir dynamiquement une route lorsqu'un noeud tente d'envoyer un paquet de données à une destination pour laquelle il ne connaît pas encore l'itinéraire. La découverte de l'itinéraire fonctionne en inondant le réseau avec la route paquets demande (RREQ) de contrôle.

Un nœud qui reçoit un RREQ rediffuse, à moins qu'il a déjà vu d'un autre voisin où il a une itinéraire vers la destination indiqué dans le RREQ. Si le RREQ reçu est un double, il sera abandonné. Si un noeud a la route, car il est la destination ou qu'il a appris dans une autre découverte de route, il répond à la RREQ avec une itinéraire réponse (RREP) paquet qui est acheminé à l'expéditeur d'origine du RREQ.

Un inconvénient de **Blind** processus de découverte de route basée sur l'inondation est la surcharge élevé des paquets de contrôle. Chaque RREQ initié par un résultat de nœuds dans n émissions dans le MANET, où n est le nombre de nœuds dans le MANET. Comme nous le savons, dans un réseau sans fil Ad Hoc où les infrastructures filaires ne sont pas réalisables, l'énergie et la bande passante la conversation sont les deux éléments clés présentant des défis de recherche.

Bande passante limitée rend un réseau facilement congestionné par des signaux de commande du protocole de routage. Comme la mobilité et la charge du réseau augmente, les paquets de contrôle RREQ utilisés pour les découvertes d'itinéraire peuvent consommer plus de bande passante que les paquets de données.

Nœuds malveillants pourraient exploiter cette faiblesse potentielle des protocoles de routage. Les pirates peuvent lancer beaucoup plus de paquets de contrôle de RREQ que les nœuds normaux de consommer des ressources de réseau. Puisque les paquets de contrôle sont une priorité plus élevée des paquets de données à transmettre, puis à des charges élevées, l'utilisation du canal sans fil peut être complètement dominée par les paquets de contrôle utilisés pour les découvertes d'itinéraire. Dans cette situation, la communication en cours de validité ne peut pas être conservé et les nœuds de réseau normaux ne peut pas être servi, il conduit à une sorte d'attaque par déni de service.

Dans certains protocoles à la demande, par exemple AODV, un noeud malveillant peut remplacer la restriction posée par RREQ_RATELIMIT (limite d'initier / RREQs expédition) en augmentant ou le désactiver. Un nœud peut le faire en raison de son autocontrôle sur ses paramètres. La valeur par défaut pour le RREQ_RATELIMIT est 10. Un nœud compromis peut choisir de définir la valeur du paramètre RREQ_RATELIMIT à un nombre très élevé.

Cela lui permet d'inonder le réseau avec de faux RREQs et conduit à une sorte d'attaque DoS. Dans ce type d'attaque DoS un noeud non malveillant ne peut pas servir assez d'autres nœuds en raison du réseau de charge imposée par les faux RREQs. Cela permettra non seulement conduire à l'épuisement des ressources du réseau, comme la mémoire (des entrées de la table de routage), mais aussi conduire à un gaspillage de bande passante et le gaspillage du temps de traitement de nœuds.

Les auteurs proposent un mécanisme de filtrage distribué pour réduire de telles situations et pour réduire la perte de débit. Le mécanisme proposé a pu empêcher ce genre spécifique d'attaque de DOS et n'emploie pas n'importe quelle largeur de bande passante additionnelle de réseau.

6.4. Les auteurs **[50],** expliquent la nouvelle attaque DOS, appelé Ad Hoc Flooding attaque peut entraîner un déni de service lorsqu'il est utilisé contre les protocoles à la demande de routage pour les réseaux mobiles Ad Hoc, L'intrus diffuse masse Route Demande de paquets pour épuiser la bande passante de communication et les ressources des nœuds de sorte que la communication entre les nœuds valides ne peut être maintenue. Le paquet injecté est un paquet de faux. Le nœud attaquant met sa propre valeur définie dans le paquet RREQ afin de rendre cette attaque plus dangereuse.

Le Flooding RREQ dans l'ensemble du réseau va consommer beaucoup de ressources du réseau. Pour réduire la congestion dans un réseau, le protocole AODV adopte la méthode suivante : Il limite le nombre de messages, provenant d'un nœud à RREQ_RATELIMIT messages RREQ par seconde. Après la diffusion d'un RREQ, un nœud attend un RREP. Si une route n'est pas reçue dans aller-retour millisecondes, le nœud peut essayer à nouveau de découvrir une route en diffusant une autre RREQ, jusqu'un maximum de temps de nouvelle tentative à la valeur maximum TTL. Dans l'attaque de Flooding, le nœud d'attaque viole les règles ci-dessus pour épuiser la ressource réseau.

Tout d'abord, l'attaquant choisit de nombreuses adresses IP qui sont pas dans le réseau, si l'attaquant connaît le champ d'adresse IP dans les réseaux. Étant donné qu'aucun des nœuds ne peut répondre à des paquets RREP pour ces RREQ, le chemin inverse dans la table de routage du nœud sera conservé plus longtemps. L'attaquant peut sélectionner des adresses IP aléatoires si elle ne connaît pas la portée des adresses IP.

Deuxièmement, l'attaquant provient successivement des messages masse RREQ pour ces adresses IP vides. L'attaquant tente d'envoyer RREQ excessive sans tenir compte de la limite de demande de taux par seconde. L'attaquant renverra les paquets RREQ sans attendre le RREP ou temps aller-retour, si elle utilise ces adresses IP. Le TTL de RREQ est configuré pour un maximum sans utiliser l'expansion méthode de recherche de l'anneau. Dans les attaques des Flooding, l'ensemble du réseau sera pleine de paquets RREQ que l'attaquant envoie. La largeur de bande de communication est vidée par les paquets RREQ inondées et les ressources des nœuds sont épuisées en même temps. Par exemple, le stockage de la table de routage est limité. Si les paquets RREQ masse arrivent à un nœud dans un court intervalle de temps, le stockage de table de routage dans le nœud sera épuisé, de sorte que le nœud ne serait pas en mesure de recevoir de nouveaux paquets RREQ. En conséquence, un des nœuds légitimes ne seront pas en mesure de mettre en place des chemins pour envoyer des données.

La figure 4.11 montre un exemple de l'attaque d'Inondation par RREQ. Nœud de **8** est un attaquant et inonde RREQ masse des paquets sur les réseaux de sorte que les autres nœuds ne peuvent pas créer des chemins entre eux.

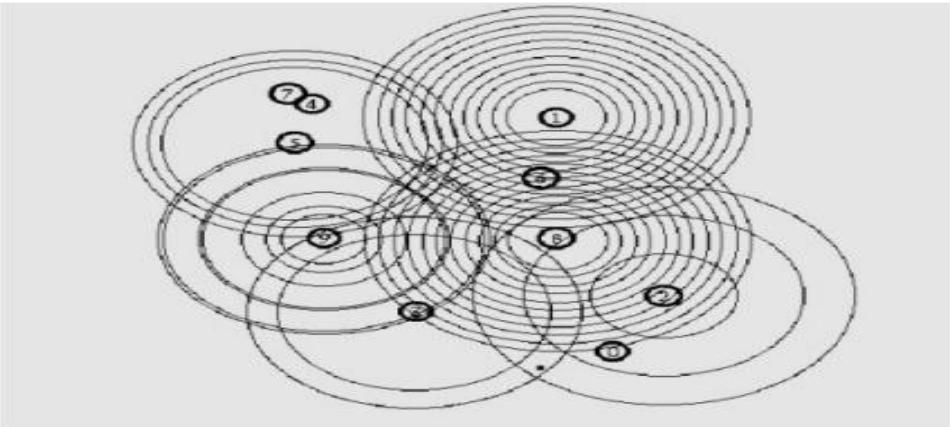


Figure 4.11 : L'attaque de Flooding. **[50]**

Les auteurs proposent une technique simple et efficace pour sécuriser le protocole de routage (AODV) contre les attaques Flooding. Pour faire face à une attaque contre les inondations, ils ont proposé une Technique de défense de Voisin pour (AODV). Cela rend AODV plus robuste. La technique proposée a été conçu pour isoler l'attaquant Flooding avec l'utilisation de minuteries, la valeur de sommet et technique d'alarme avec « hello ».

Ils ont simulé son travail dans un Simulateur réseau NS-2.33 (NS-2) avec des temps de pause par l'intermédiaire d'un nombre différent de nœuds malveillants.

Ils ont comparé les performances de NDTAODV avec AODV en situation normale ainsi que, en présence d'attaques malveillantes. Ils ont examiné Fraction Packet Delivery (PDF), Moyenne ou Average Throughput (AT) et Normalized Routage Load (LNR) pour comparer les performances des NDTAODV et AODV.

6.5. Dans ce travail **[49]**, le comportement d'attaque Flooding et son impact sur les performances de protocole AODV est étudié. Le simulateur de réseau NS2 est utilisé pour évaluer l'impact de l'attaque sur les inondations de protocole AODV.

Dans ce travail, l'attaque de Flooding est simulée dans ns2 en employant l'approche basée par temporisateur dans le protocole de cheminement d'AODV.
Selon le RFC la limite de taux pour RREQ est définie en tant que 10 par sec.
Ceci est recouvert en employant la fonction de générateur d'inondation.
Cette fonction continuera à produire du RREQ indépendamment de la limite de taux.
Par conséquent sur une certaine période de temps le réseau a plus de nombre de RREQ visant la destination D.

La source produisant du Flooding de RREQ est le noeud H comme montré dans Figure 4.12.

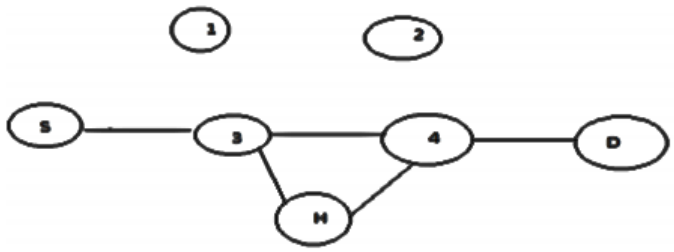


Figure 4.12 : Modèle de L'attaque Flooding (**H** nœud attaquant). **[49]**

Ici la source est S et la destination D qui est observée sous la circulation normale.
Le nœud **H** d'attaquant envoie le RREQ visant la destination D et a également annoncé RREQ au nœud 3 et 4 pour atteindre l'extrémité D. le AODV () est modifiés pour le temporisateur () et la fonction d'émission (). Le paramètre de RATE_LIMIT est incrémenté.
Le nouvel agent est créé pour l'AODV modifié et attaché au nœud attaquant H.

Cette étude de l'attaque de Flooding dans le protocole d'acheminement d'AODV et son impact de performances en termes de consommation de largeur de la bande passante, la fin à l'extrémité retarde, et le rapport de la livraison de paquet a été discuté. Le même a été simulé en utilisant NS-2 et les résultats sont analysés en détail.

7. Contribution

Notre contribution consiste à créer une attaque RREQ Flooding par une autre technique difficile à détecter, par les logiciels de détection et d'élimination d'attaques.

Notre idée se focalise sur la création d'un attaquant avec le moindre changement des paramètres de configuration, on essaye de créer l'attaquant par la technique de changement de l'adresse IP de destination, le champ d'adresse IP de destination de l'attaquant est affectés par une adresse IP de destination inconnue, à la différence des travaux précédemment cités dans ce domaine, les attaquants sont créés par la modification des paramètres d'AODV tel que TTL, RREQ_RATELIMIT…etc. Ces paramètres ont des valeurs par défaut standards qui rend la détection des modifications facile.

Par contre les nœuds dans les réseaux Ad Hoc routés par un protocole de routage réactif comme AODV, n'ont pas les connaissances sur les adresses de réseau (manque de table de routage sur le réseau globale), qui rend la détection et l'élimination des attaquants difficiles.

Chaque attaquant essaye d'emmètre chaque une seconde (1s) un paquet de donnée, comme l'adresse de destination est hors plage, il consomme plusieurs tentatives de découverte de nouvelle route, ces paquets de découverte de route RREQ inondent le réseau, jusqu'à l'expiration de leurs durée de vie (TTL), ce qui agrandis la surcharge sur le réseau par des trafiques indésirables.

Pour analyser l'impact de cette attaque sur la fiabilité de réseau, on essaye de choisir les meilleures métriques, qui mesurent l'influence de l'attaque. Ces métriques sont :

Métriques AODV (Route Traffic Received, Packet Dropped, Route Request Sent)

Métriques WIRELESS (Delay, Throughput, Load)

La méthode d'évaluation qu'on essaye de choisir est d'exécuter la simulation d'un réseau Ad Hoc sans attaques, et le comparer avec le même réseau subit par une attaque externe, par l'attaquant(s) créé(s), avec des graphes des statistiques des métriques cités précédemment, on compare l'impact d'attaque Flooding sur les performances de réseau.

8. Conclusion

Dans ce chapitre on a présenté le principe de l'inondation et leur type et ses effets sur les performances de réseau, et ensuite on a cité quelques travaux connexes de ce domaine, et enfin on a expliqué le principe de notre participation dans ce domaine ainsi la différence entre notre contribution et les travaux réalisés précédemment.

Dans le prochain chapitre on explique la réalisation de cette contribution sous le simulateur OPNET.

Chapitre 5 :

L’impact d’attaque RREQ Flooding sur la fiabilité de protocole de routage AODV.

1. Introduction

AODV est un protocole de routage réactif, dans les réseaux Ad Hoc, ces réseaux sont vulnérable par plusieurs types d'attaques, parmi ces attaques on distingue l'attaque d'inondation « Flooding », que l'on a pris dans ce travail pour simuler l'impact de cette attaque sur la fiabilité de routage dans les réseaux Ad Hoc, en utilisant le simulateur OPNET Modeler 14.5.

OPNET Modeler 14.5 est une mise à jour logicielle à la version 14.0. Cette version contient de nouvelles fonctionnalités et des améliorations aux capacités existantes. Cette version met également en œuvre des suggestions et corrige de nombreux problèmes logiciels signalés dans les versions antérieures.

2. Création de l'attaque Flooding sous OPNET MODELER

2.1. Simulation de l'attaque

Nous avons essayé de créer l'attaque du Flooding, par inonder le paquet RREQ vers destination inconnu, en utilisant le protocole AODV en but de cette attaque de perturber le bon fonctionnement de réseau

Pendant le déclenchement de processus de découverte de la route de protocole, le nœud source diffuse un paquet de type RREQ (Route REQuest) vers les nœuds voisins pour choisir un chemin récent vers la bonne destination, qui n'existe pas réellement parmi les nœuds de réseau.

Le nœud source d'attaque qui joue le rôle d'une source qui initie l'envoie des paquets RREQ pour découvrir la route, et il n'intéresse pas de la réception d'une réponse, avec un paquet RREP, parce que son but est la surcharge de réseau, pour dégrader ses performance.

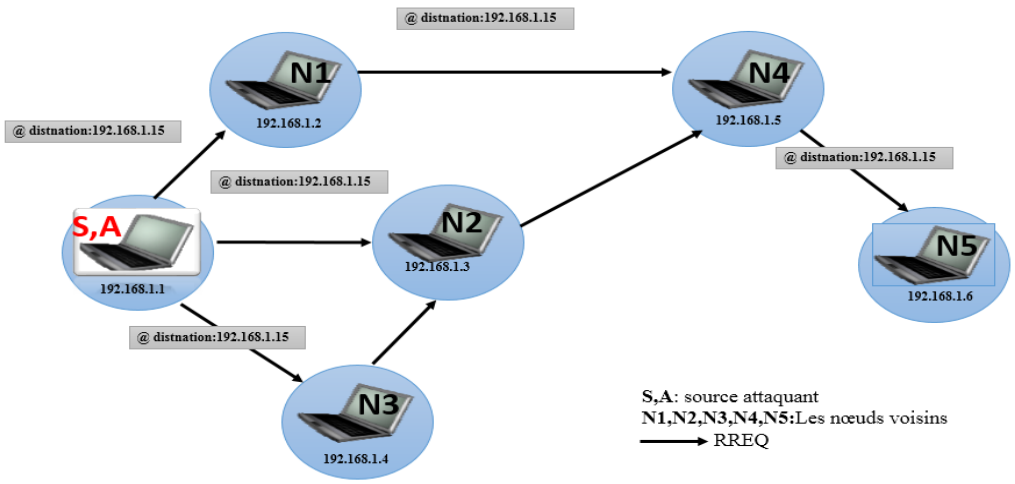


Figure 5.1 : L'attaque Flooding.

2.2. Simulation d'un attaquant

Pour créer un attaquant dans un réseau Ad Hoc, le changement des paramètres ci-dessous permet de changer un nœud normal à un nœud attaquant par RREQ Flooding, voir les figures 5.6 et 5.7.

- **Paramètre AODV**

a. Route Requests Retries : Cet attribut spécifie le nombre maximum de fois un nœud va essayer à nouveau de découvrir une route en diffusant une autre requête RREQ.

- **Paramètres IP :**

a. Adresses: Représente l'Adresse IP de l'interface. L'Adresse IP devrait être indiqué dans l'exemple pointillé de notation décimale : 198.24.46.89

b. Le masque de sous-réseau (Subnet Mask): Le masque sous réseau de l'interface. Le masque de sous réseau devrait être indiqué dans le pointillé décimal notation par exemple. 255.255.255.0.

- **Paramètre de génération du trafic de MANET**

Attribut composé qui contient tous les attributs modèles reliés par génération crue de paquet de MANET.

a. Temps de départ (Time_Start (secondes)): Temps pour commencer la génération de paquet.

b. L'adresse IP de destination : L'adresse IP de destination auquel des paquets devraient être envoyés. Ceci doit être une Adresse IP inconnu dans le réseau (adresse hors plage des adresses qui existent dans le réseau).

2.3. Réalisation sous OPNET 14.5

Dans la suite, on va présenter les étapes suivis pour la création de cette attaque et le choix des paramètres du réseau à configurer.

- **Création du projet**

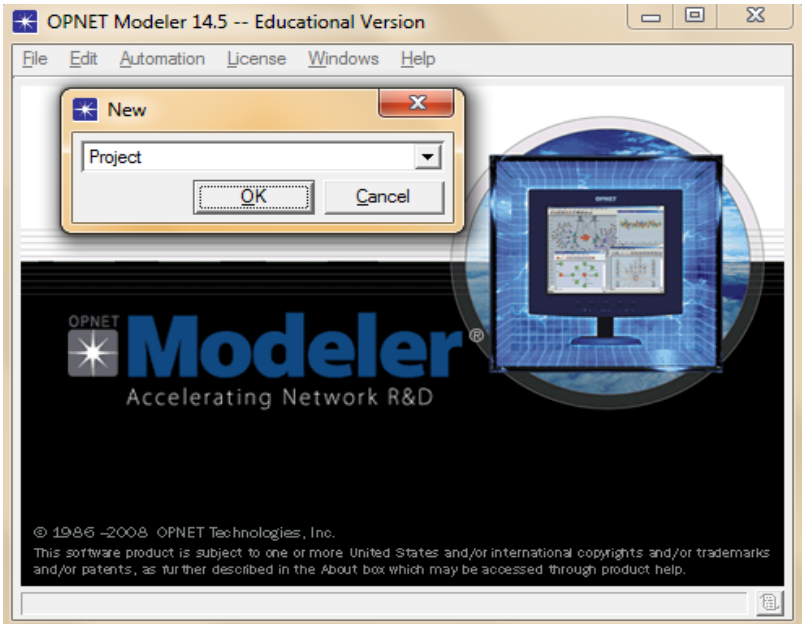


Figure 5.2 : Nouveau projet sous OPNET.

- Cette utilitaire présent de première interface d'OPNET 14.5 de création de nouveau projet.
- Un projet est en fait constitué d'un ensemble de scénario reliés les uns aux autres, chacun montrant un aspect différent du réseau.

Figure 5.3 : Utilitaire de Création de réseau sans fil sous OPNET.

- Pour créer un réseau Ad Hoc, nous allons définir sa topologie initiale, sa taille, le lieu et la mobilité.
- Dans notre exemple, nous choisissons la technologie : Ad Hoc comme modèle.

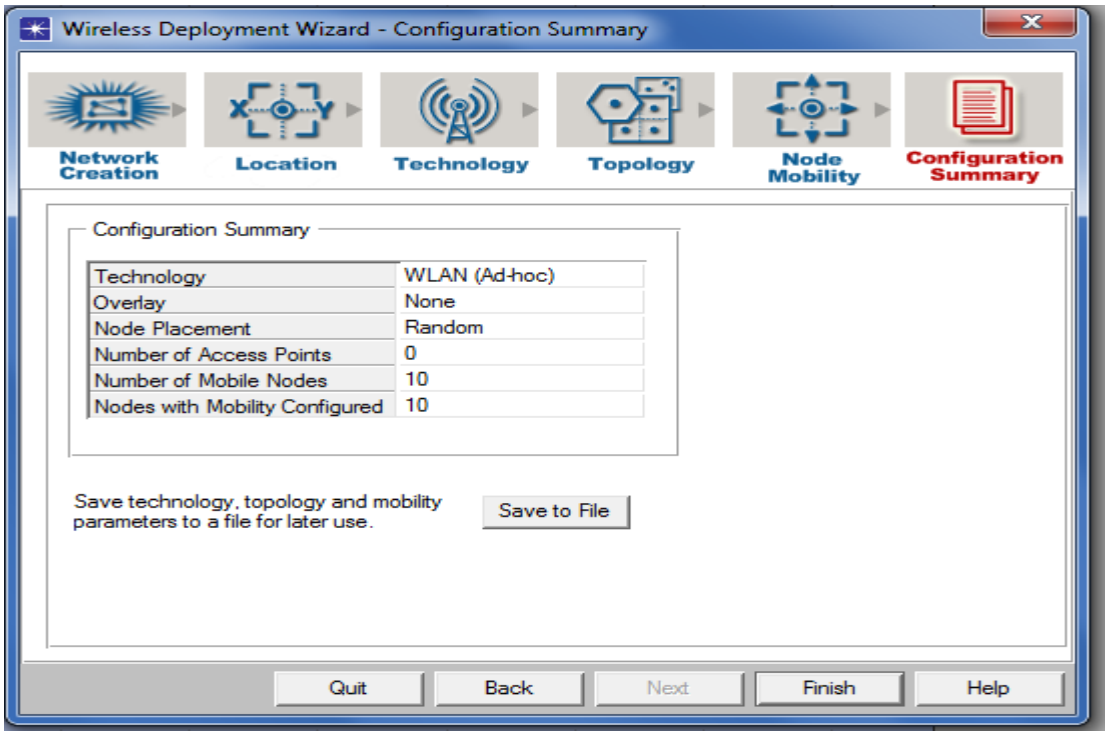


Figure 5.4 : Configuration de réseau sous OPNET.

➢ Cet interface représente les choix des paramètres de réseau crée. On a choisi le type de réseau, le nombre des nœuds, la mobilité trajectoire et le mode de déplacement des nœuds. On peut alors choisir de commencer par un nouveau scénario vide.

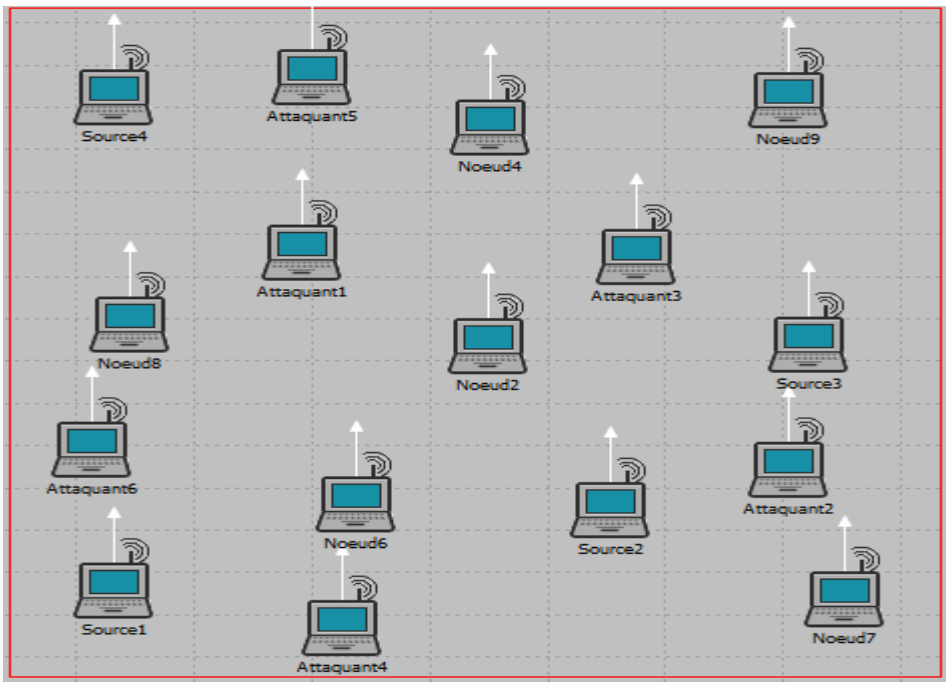
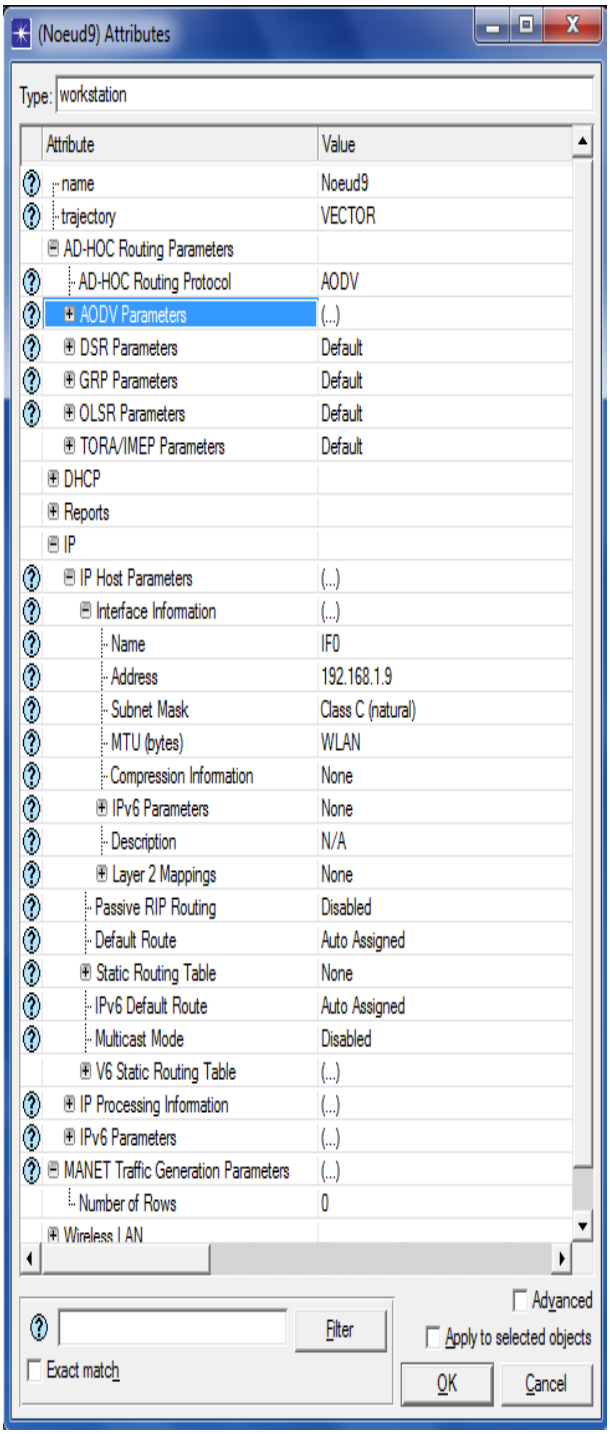


Figure 5.5 : L'interface de projet.

➢ Dans la figure 5.5 l'interface de projet créé consiste un réseau Ad Hoc contient plusieurs nœuds bien configurée.

Dans cette topologie nous avons un réseau Ad Hoc avec 10 nœuds (4 nœuds sources de paquets et 6 nœuds consommatrices), ce réseau attaqué par 6 attaquants.



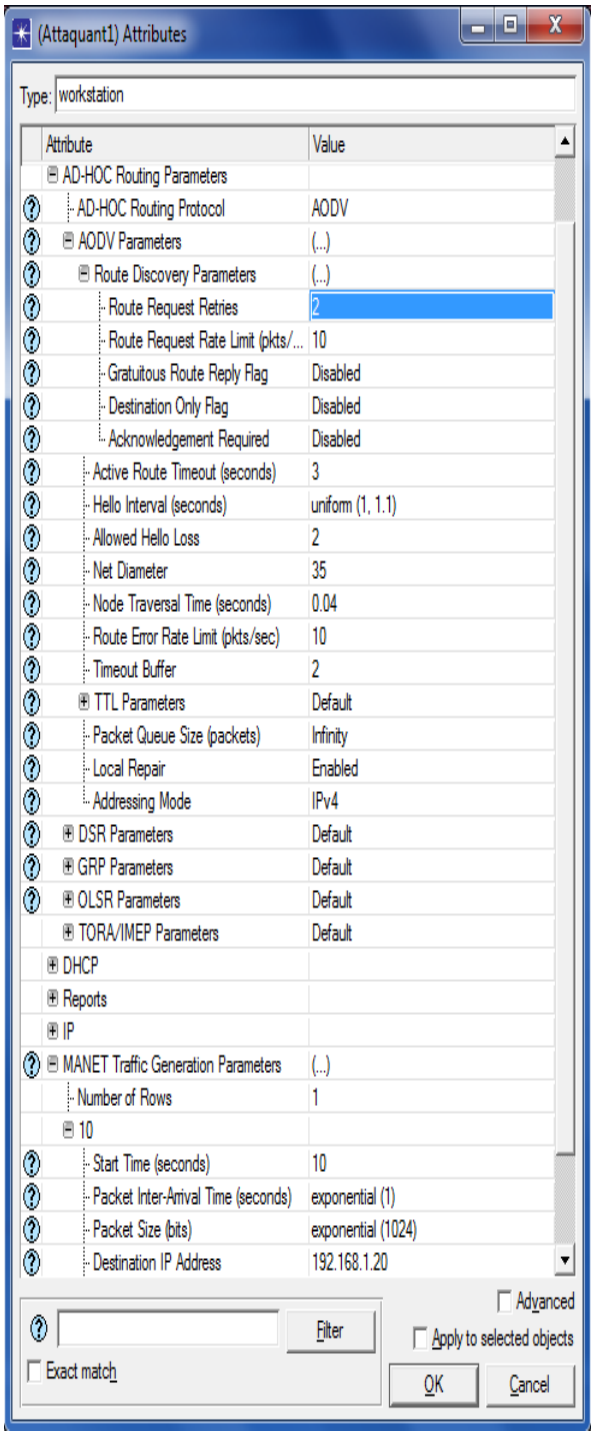


Figure 5.6 : Paramètre par Défaut d'un nœud**.**

Figure 5.7 : Paramètre d'un nœud attaquant.

- Dans la figure 5.6, la configuration d'un nœud consommatrice par défaut (Protocole de routage AODV, Adresse IP = 192.168.1.9, Masque de sous réseau = Classe C).
- Pour les nœuds sources de paquets on ajoute les paramètres suivants (Number of rows = 1).
- Dans la figure 5.7, la configuration d'un nœud attaquant (Adresse IP de destination inconnu, Start Time = 10 s, Route Request Retries = 2, Number of rows = 1).

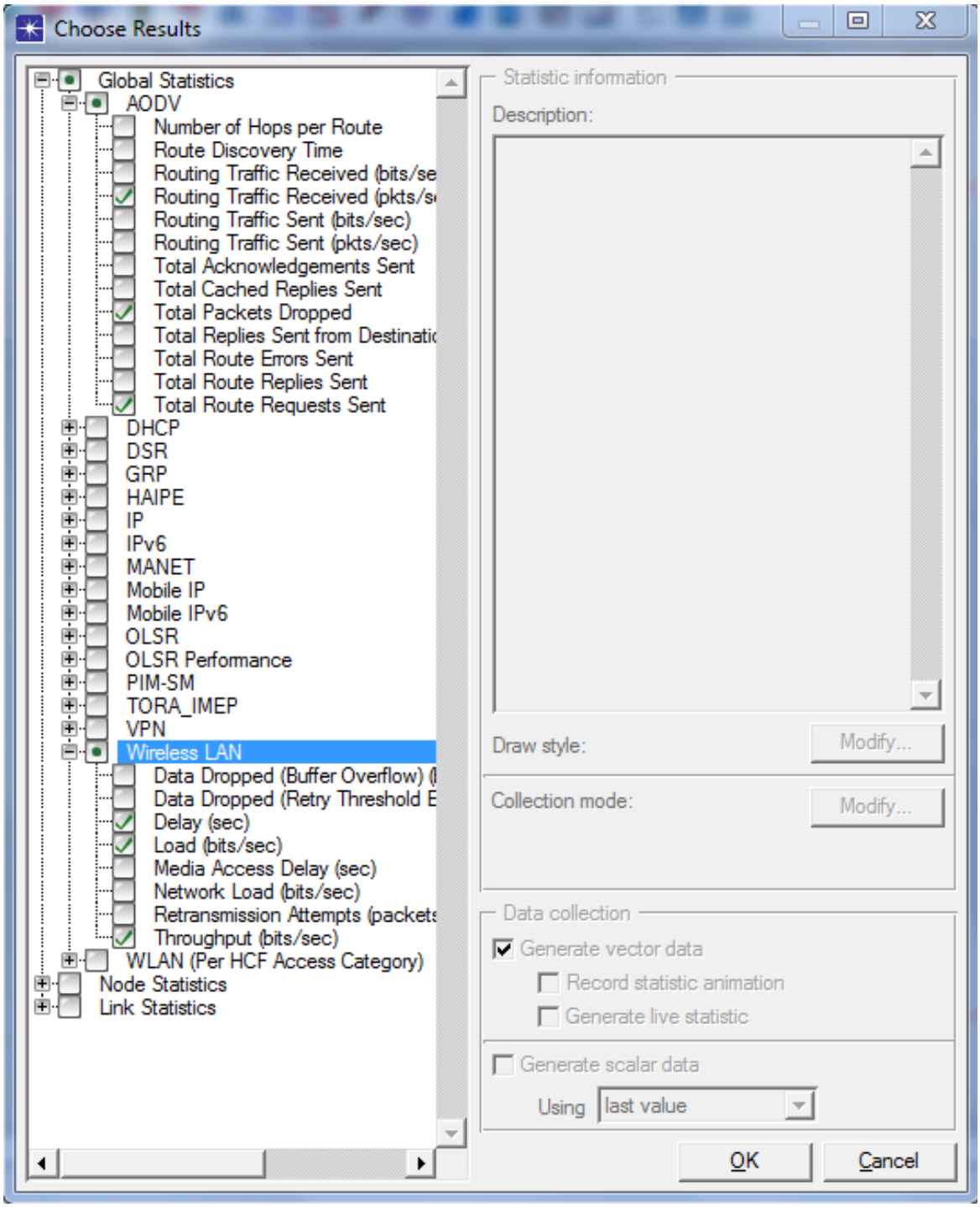


Figure 5.8 : Métriques Globales.

- Cette fenêtre permet de choisir les métriques qui mesurent l'impact de l'attaque Flooding.

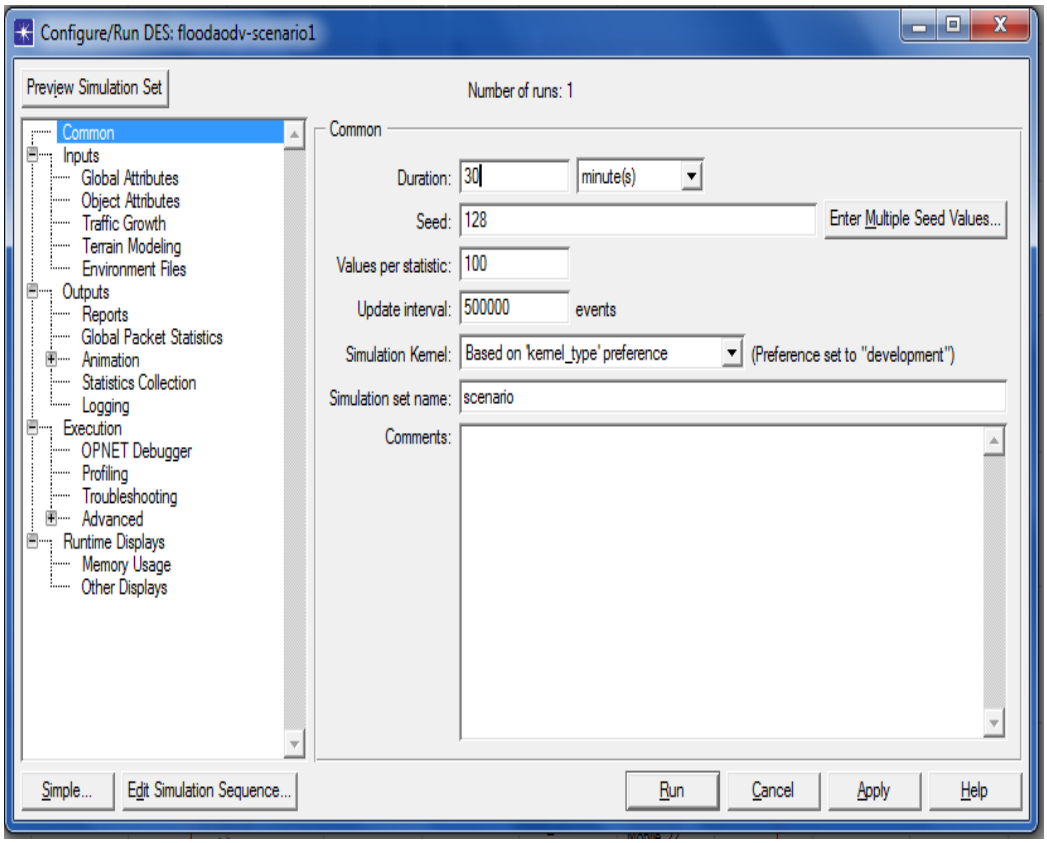


Figure 5.9 : Fenêtre d'exécution**.**

➢ Par cette fenêtre dans la figure 5.9, on peut lancer l'exécution de simulation et de choisir quelques paramètres de l'exécution, tel que le temps de simulation (30 minutes).

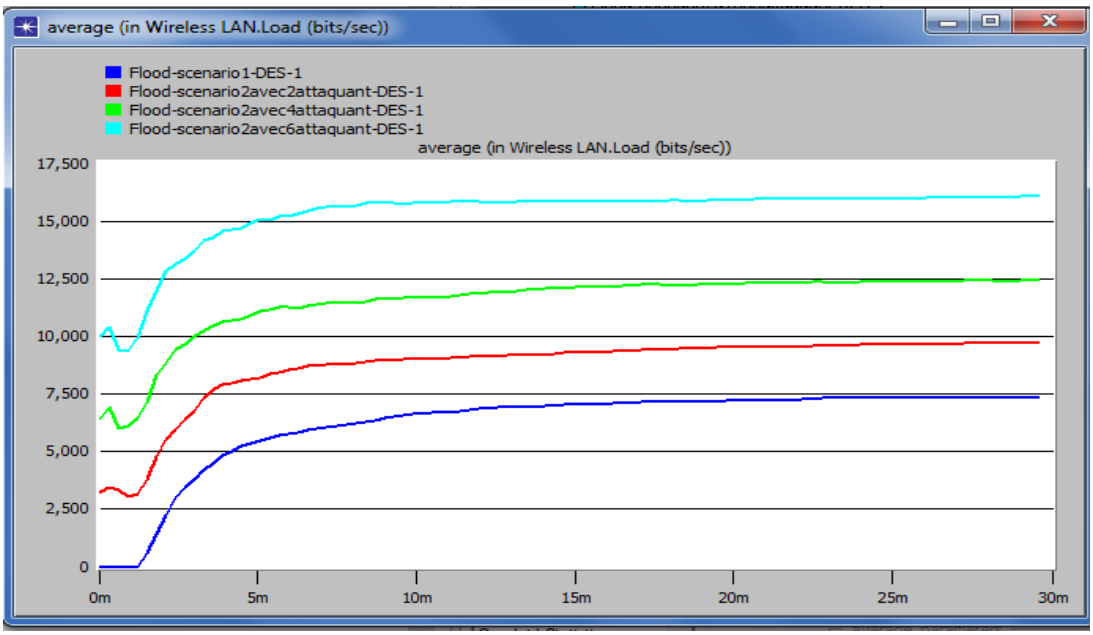


Figure 5.10 : Graphe des résultats.

➢ Le graphe 5.10 représente les résultats obtenus après l'exécution des scénarios.

A travers deux scénarios, on simule notre contribution, dans ces scénarios on augmente le nombre d'attaquants, et on configure le nombre maximum de tentative pour essayer de découvrir la route **ROUTE REQUEST RETRIES,** pour voir l'impact de cette attaque sur le réseau**.**

En conclure cette recherche, On a créé un scénario résultat, qui est la concaténation entre tous ces paramètres, pour augmenter le taux d'impact sur la fiabilité de routage dans le réseau Ad Hoc.

3. Conclusion

L'objectif principal de ce chapitre est de présenter la réalisation de notre contribution, nous essayons de simuler un réseau Ad Hoc, ainsi des nœuds attaquants, où l'attaquant est d'origine un nœud normale avec modification des paramètres de sorte que ce nœud génère périodiquement, des paquets indésirables, surcharger le réseau, cette création se base essentiellement sur la demande de route, pour une adresse hors plage de réseau.

Cette réalisation faite par le simulateur OPNET 14.5, on a montré dans la deuxième partie, les étapes d'implémentation de notre contribution.

Chapitre 6 :

Tests Et Résultats.

1. Introduction

Pour voir à quel degré l'attaque peut influencer le réseau, à travers des scénarios choisis suivant : (Nombre d'attaquants, le nombre de tentative de découverte la route) et de réaliser un scénario résultat qui est la combinaison entre les deux paramètres, pour obtenir la meilleur dégradation dans le réseau.

Comparer les résultats après l'exécution des scénarios avec attaques et les résultats de scénario de réseau sans attaques pour voir l'impact de ce dernier.

2. Métriques pour analyser l'impact

Dans cette section nous expliquons les différents indicateurs de l'impact requises sur la fiabilité de routage dans les réseaux Ad Hoc et l'augmentation de l'impact selon :

- L'augmentation de nombre d'attaquants.
- La minimisation de **ROUTE REQUEST RETRIES**.

Les métriques qui ont choisis pour analyser l'impact de la dégradation de performance du réseau sont des métriques globales inclus dans les deux groupes des métriques suivantes :

- **Métriques AODV**: Routing traffic received, Packet dropped, Total route requests sent.
- **Métriques Wireless LAN**: Delay, Load, Throughput.

2.1. Métriques AODV

Ces métriques sont importantes, pour analyser la fiabilité de réseau.

• **Routing traffic received** : le trafic reçu à travers le réseau, indique la quantité globale des trafics reçu par les nœuds mobiles. Le protocole de routage AODV estime la quantité du trafic reçu en fonction de paquets par seconde.

• **Packet dropped :** les paquets perdus, détermine le nombre de paquet si aucune route n'est trouvée à la destination, cette statistique représente tout le nombre de paquets d'application jetés par tous les nœuds dans le réseau.

• **Total route requests sent :** le nombre total de paquets envoyés de demande d'itinéraire par tous les nœuds dans le réseau au cours de découverte de route.

2.2. Métriques Wireless LAN

- **Delay** : est le temps moyen pour traverser le paquet de bout en bout à l'intérieur du réseau. Cela comprend le temps de génération du paquet de l'expéditeur jusqu'à la réception du paquet ou l'inverse, est exprimé en secondes.

- **Load :** est la charge du réseau, Il indique la quantité de la circulation dans tout le réseau. Il représente le trafic de données totales en bits par seconde reçues par l'ensemble du réseau de couche supérieure acceptée et en attente de transmission.

- **Throughput** : est le débit, il est le rapport de la quantité totale de données qui atteint le récepteur de l'expéditeur, c'est représenté en paquets par secondes.

3. Simulation et Résultats

3.1. Premier scénario

Dans le premier scénario, nous choisissons le changement de nombre d'attaquants, nous fixons tous les paramètres et le nombre des nœuds globales, et le nombre des nœuds émetteurs, le premier courbe représente le cas par default (sans attaquants), les autres représentent les cas de 2, 4, 6 attaquants.

Paramètre choisis pour la simulation	
Modèle de mobilité	Default Random way point
Placement des nœuds	Random
Nombre de nœuds	10
Nombre de nœuds attaquants	0, 2, 4, 6
Dimension du terrain	1000 m x 1000 m
carte de communication	802.11g (54 Mbps)
Le temps de simulation	30 minutes
Paramètre du protocole AODV	Par défaut
Vitesse	5 m/s
Taille de paquets	1024 bits

Tableau 6.1: Paramètres de premier scénario de la simulation.

3.1.1. Graphes d'AODV dans le premier scénario

- **Trafic reçu router par AODV (AODV routing traffic received (Packets/sec))**

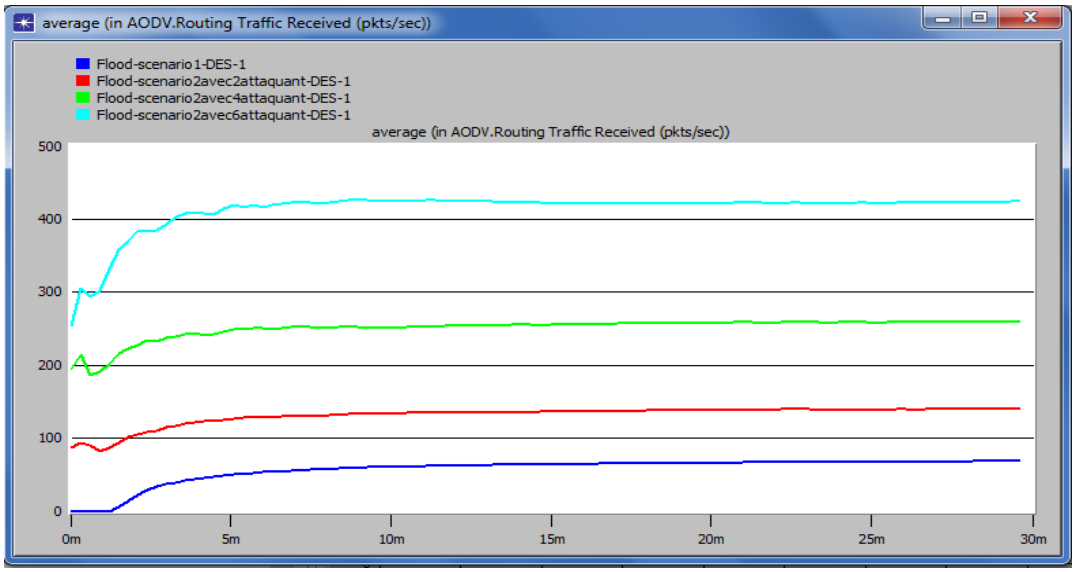


Figure 6.1: Trafic reçu routé par AODV **(**Paquets/sec).

➢ On a remarqué dans la première courbe que plus le nombre d'attaquants augmentent, la quantité moyenne de trafic reçu augmente, cette augmentation représente des surcharges indésirables sur le réseau, parce que la différence entre les données valides et les données non valides presque quatre fois (400%).

- **Total des paquets perdus (AODV Total packets dropped)**

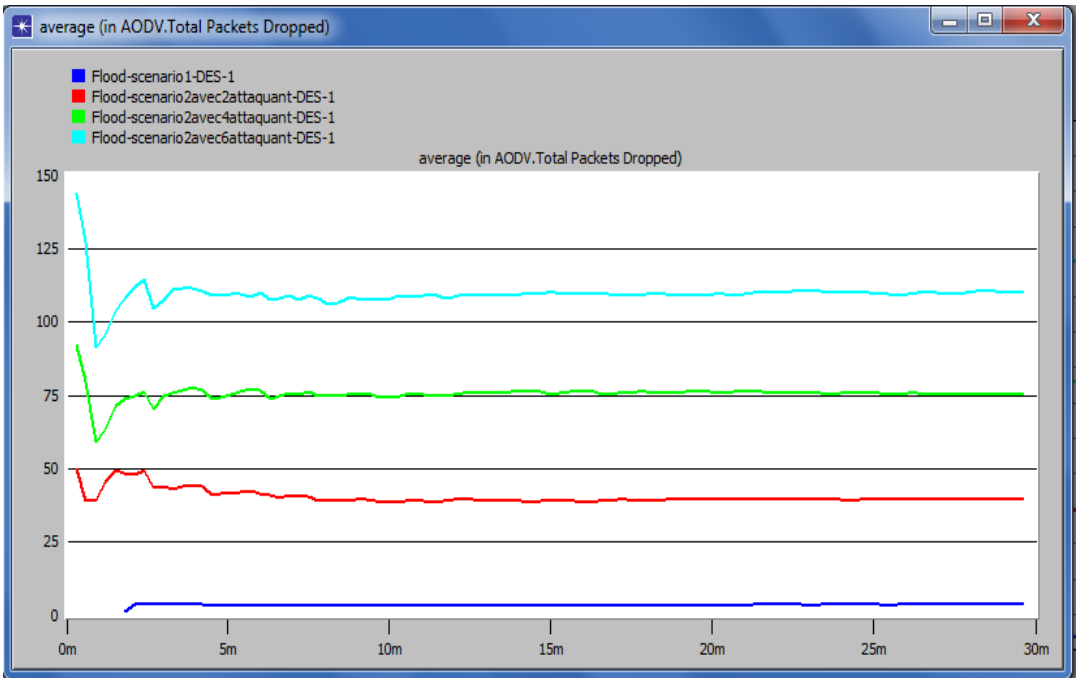


Figure 6.2 : Total des paquets perdus.

- Il est clair dans la figure 6.2 que plus le nombre d'attaquants augmentent, l'impact sur perte des paquets augmente, puisque dans la première courbe (bleu) la perte des paquets est faible parce que il n'existe pas aucune attaque, vise à vie aux autres courbes que la perte des paquets s'augmente est considéré importante en raison de l'augmentation des intrusions.

- **Total route demande paquets envoyés (Total Route Requests Sent)**

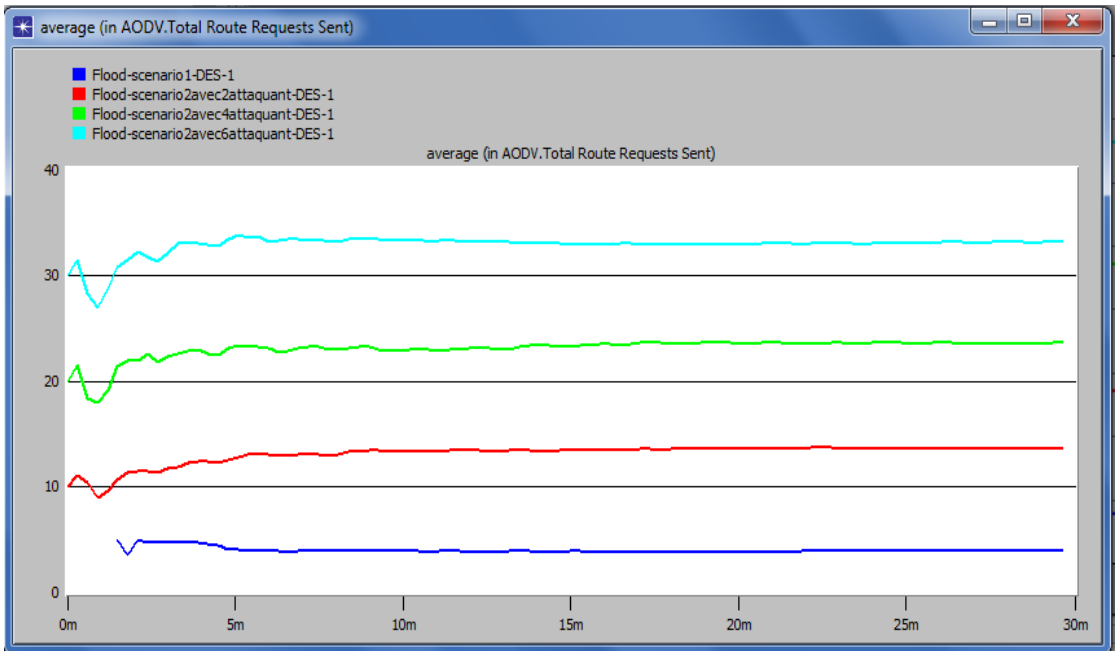


Figure 6.3 : Total route demande paquets envoyés.

➢ La figure 6.3 démontre que le nombre total d'itinéraire demande des paquets envoyés par tous les nœuds dans le réseau au cours de découverte de route augmente en fonction de l'augmentation des nombres d'attaquants.

3.1.2. Les graphes de Wireless dans le premier scénario

- **Bout en bout (Delay (sec))**

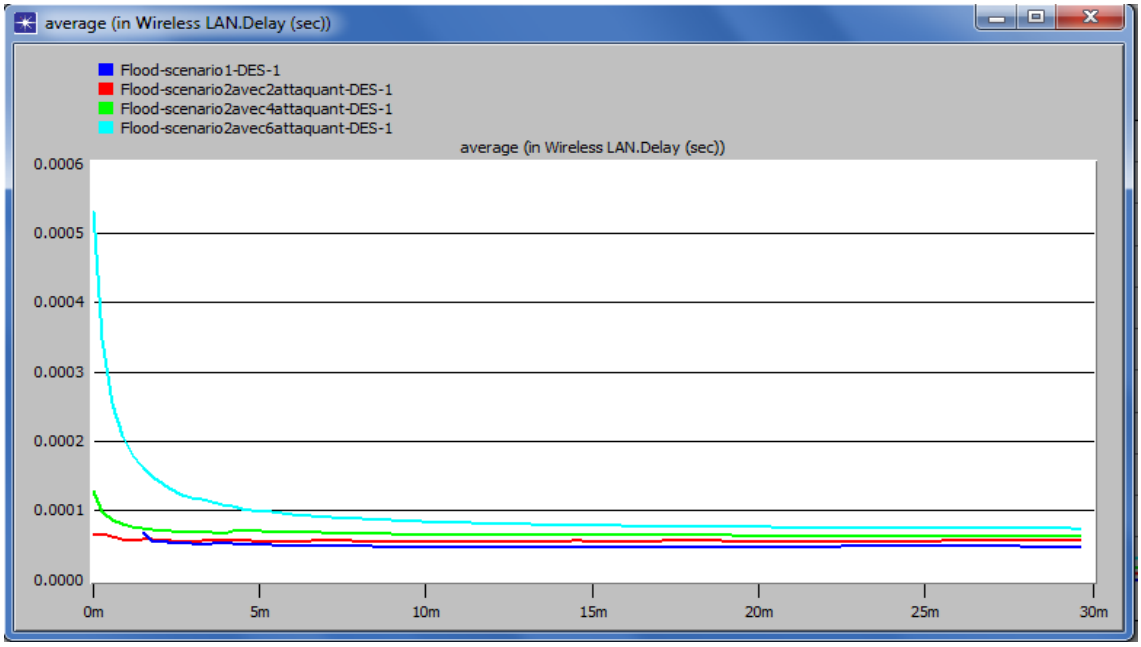


Figure 6.4: Bout en bout. (sec)

➢ Les graphes de temps de bout en bout du protocole AODV avec attaque est élevé par rapport AODV sans attaque. Le fonctionnement de Flooding augmente le délai de bout en bout car il diffuse une fausse information de découvrir la route.

- **Charge de réseau (Load)**

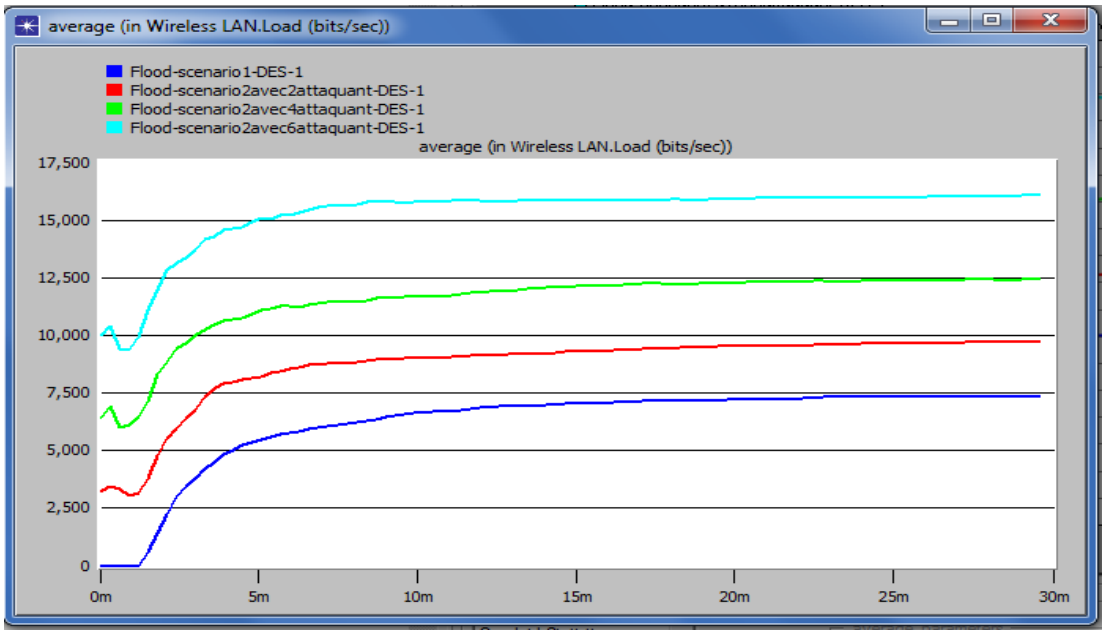


Figure 6.5: Charge de réseau (bits /sec).

➢ Le graphique de la charge réseau du protocole AODV avec attaquants et sans présence d'un nœud malveillant a été montré dans la Figure 6.5. La charge du réseau d'AODV avec attaque est très élevée par rapport à AODV sans attaque.

- **Débit (Throughput (bits/sec))**

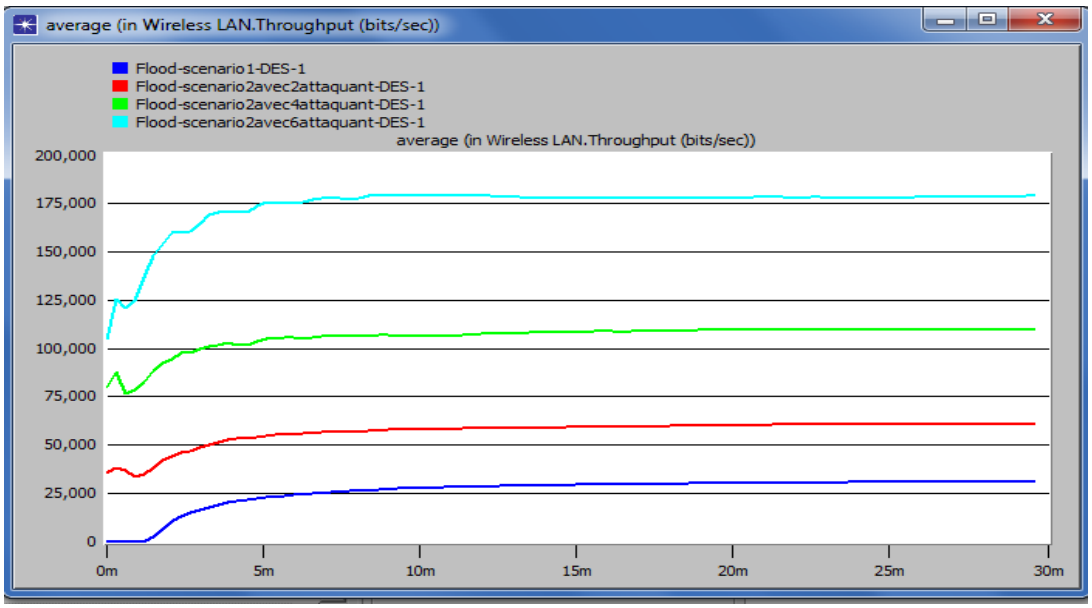


Figure 6.6 : Débit (bits/sec).

➢ Dans la Figure 6.6 pour la courbe la plus haute qui représente le réseau avec 6 attaquants, son débit est très élevé par rapport au cas sans attaquants, à cause des paquets générés par les nœuds malveillants. Le pourcentage de gaspillage de débit est presque à 600% de débit valide.

3.2. Deuxième scénario

Dans le deuxième scénario, nous choisissons le changement de paramètre correspondant au nombre de tentative de découverte d'une nouvelle route, qui représente le nombre de paquet RREQ.

Le nombre de tentative par défaut égale à 5 dans les autres cas chaque fois nous décrémentons le nombre par 1.

Paramètre choisis pour la simulation	
Modèle de mobilité	Default Random way point
Placement des nœuds	Random
Nombre de nœuds	10
Nombre de nœuds attaquants	2
Route Request Retries	5, 4, 3, 2
Dimension du terrain	1000 m x 1000 m
carte de communication	802.11g (54 Mbps)
Le temps de simulation	30 minutes
Paramètre du protocole AODV	Par défaut
Vitesse	5 m/s
Taille de paquets	1024 bits

Tableau 6.2 : Paramètres de deuxième scénario de la simulation.

3.2.1. Graphes d'AODV dans deuxième scénario

- **Trafic reçu router par AODV (AODV routing traffic received (Packets/sec))**

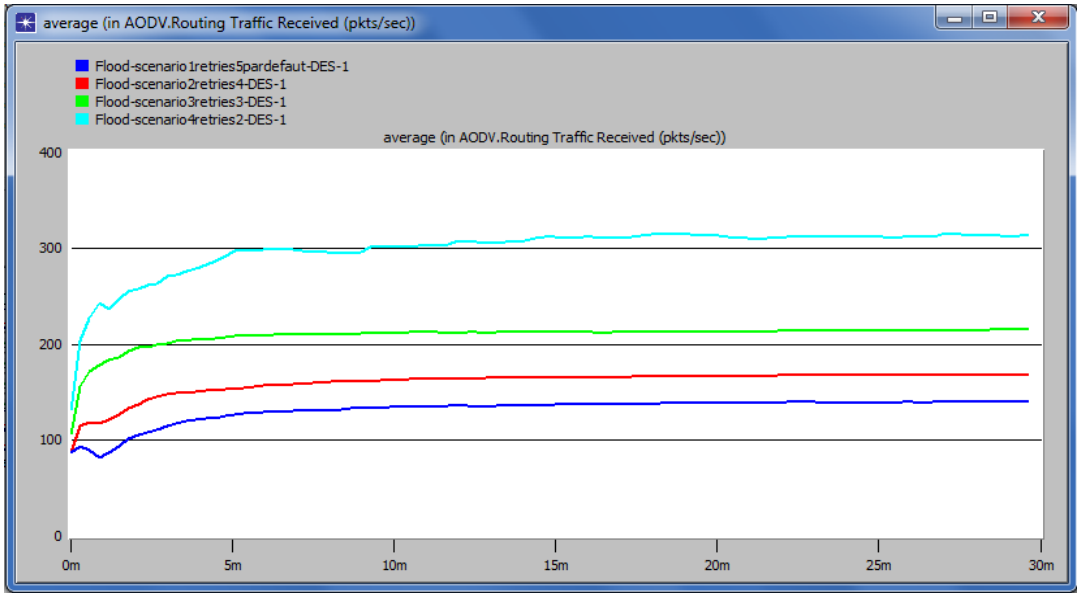


Figure 6.7: Trafic reçu routé par AODV (Paquets/sec)

➢ Cette métrique désigne le routage de trafic total reçu (en paquets /seconde), de tous les nœuds dans le réseau. On a distingué dans la figure 6.7 qu'il existe une grande différence, car l'attaquant diffuse un grand nombre des paquets invalides dans le réseau, avec un nombre de tentative de découverte de route minimum. L'impact sur le trafic reçu augmente ce qui donne une surcharge sur le réseau parce que la différence entre les données valides et les données non valides presque 100%.

- **Total des paquets perdus (AODV Total packets dropped)**

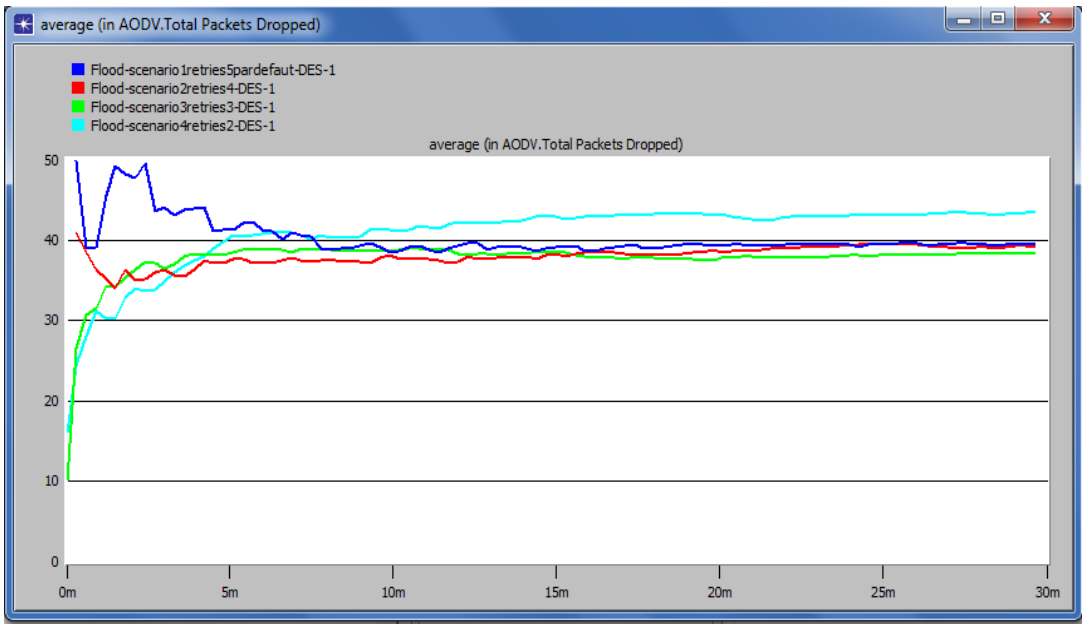


Figure 6.8 : Total des paquets perdus.

➢ Dans la figure 6.8, la métrique des paquets perdus n'est pas influencé beaucoup par la réduction de nombre de tentative de découverte de la route, par rapport aux d'autres métriques.

- **Total route demande paquets envoyés (Total Route Requests Sent (paquets))**

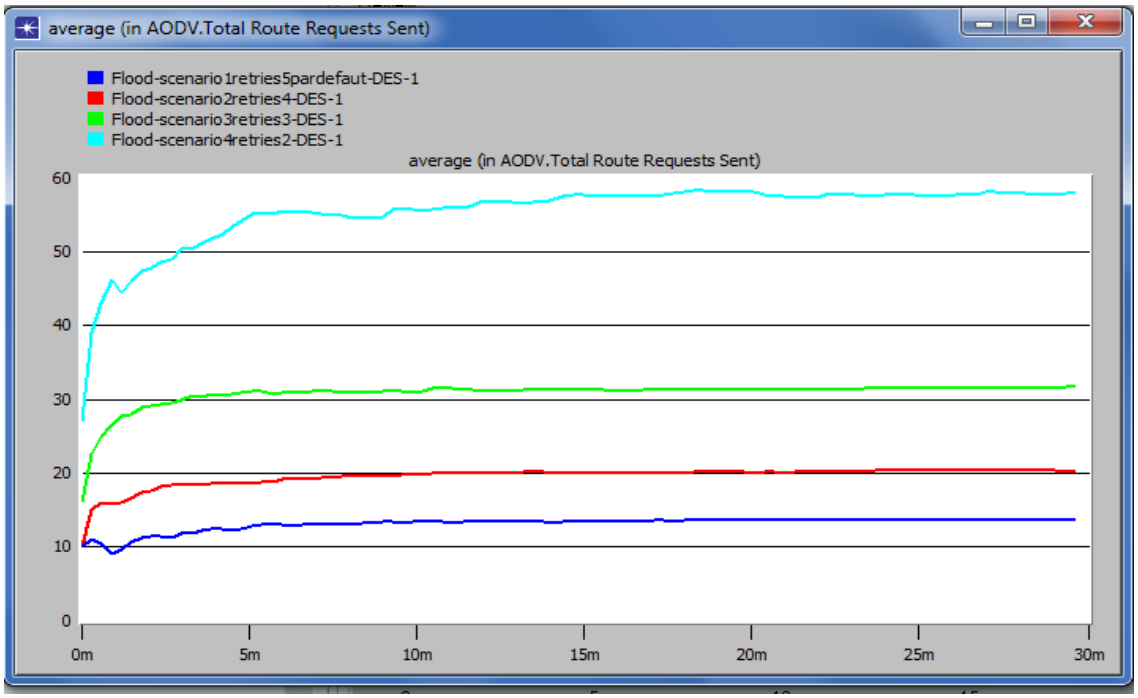


Figure 6.9: Total route demande paquets envoyés (paquets).

➢ On a remarqué dans la figure 6.9 que le total moyen envoyé de route demandé dans le réseau augmente considérablement quand les attaquants diminuent le nombre de tentative de découverte de route.

3.2.2. Graphes de Wireless dans deuxième scénario

- **Bout en bout (Delay (sec))**

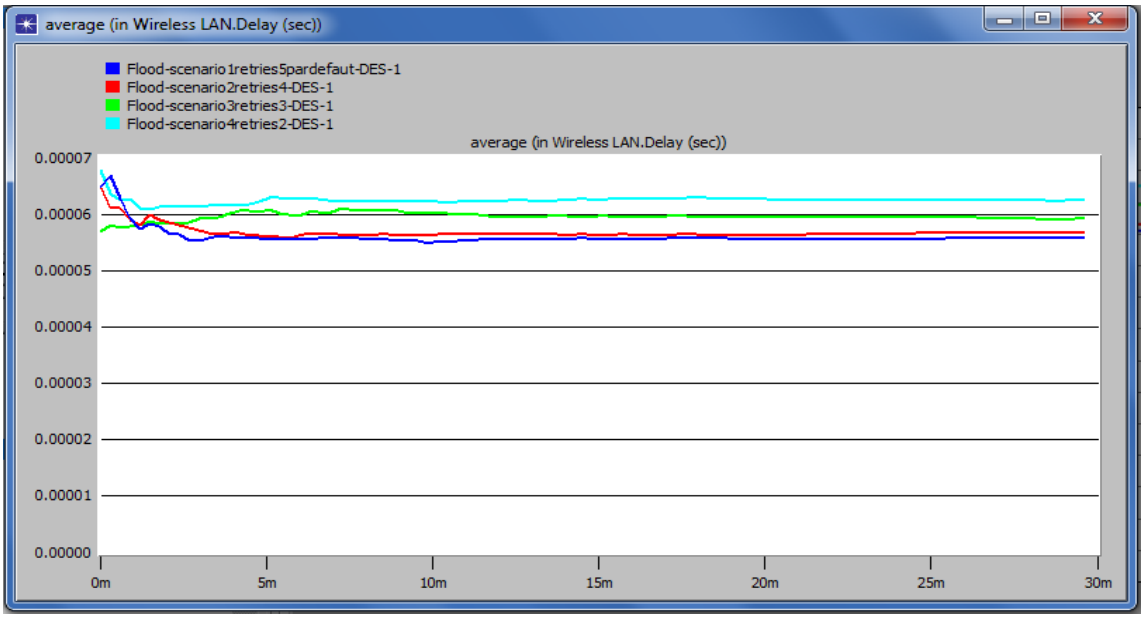


Figure 6.10 : Bout en bout (sec)

➢ Les graphes de bout en bout du protocole AODV avec le nombre des attaquants fixes, mais le nombre de tentatives de découverte de la route diminue dans chaque cas illustré dans la figure 6.10. La dégradation de temps bout en bout n'est pas clair, car l'unité de mesure est très réduite (1/100000s).

- **Charge de réseau (Load)**

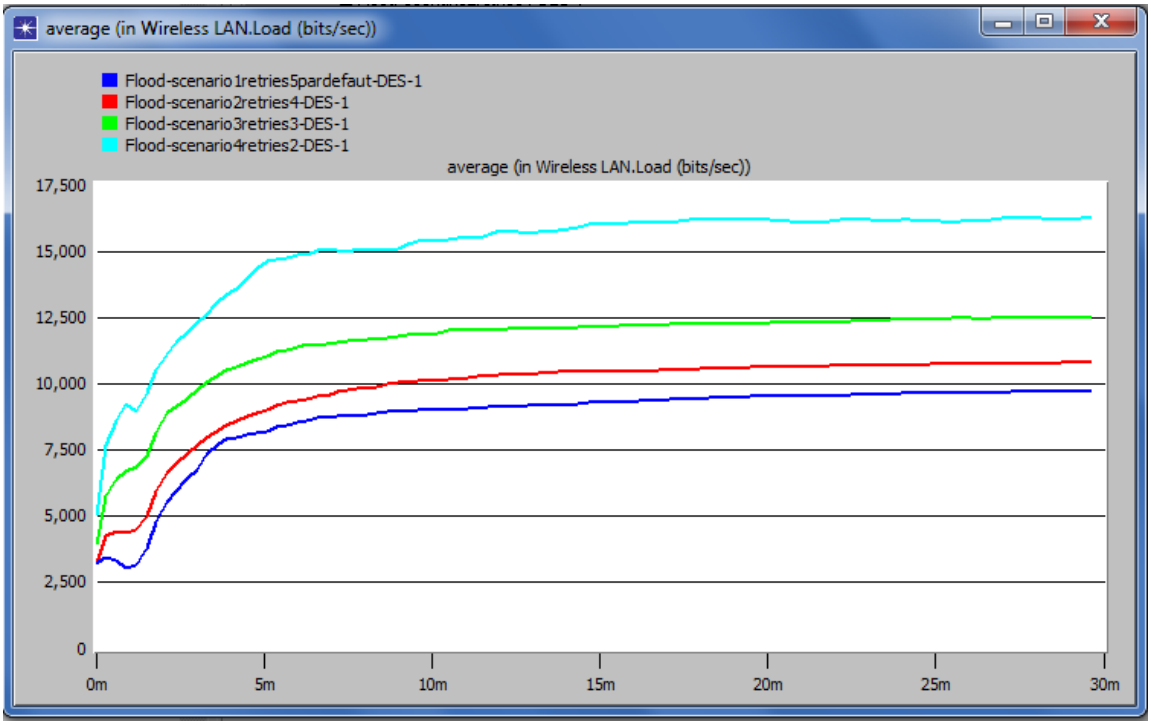


Figure 6.11 : charge de réseau (bits/sec).

➢ Cette métrique représente la charge total dans le réseau (bits / s). Le graphe de la figure 6.11 démontre que l'influence sur la charge de réseau agrandis lorsque les attaquants essayent moins de nombre de tentative de découverte de route.

- **Débit (Throughput (bits /s))**

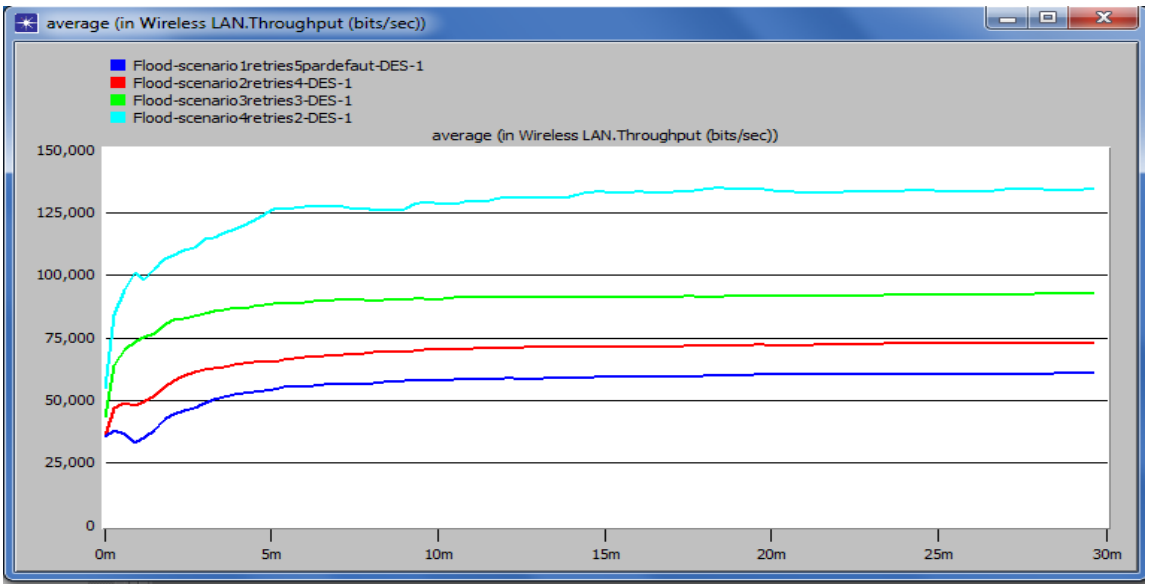


Figure 6.12: Débit (bits / sec).

➢ Parmi les métriques importants qui identifient la performance dans les réseaux Ad Hoc, le débit puisqu'il est limité. On a remarqué une dégradation dans la fiabilité de réseau à cause de l'utilisation total de la bande passante du réseau par les attaquants avec la minimisation de nombre de tentative de découverte de la route à chaque fois (plus de 100%).

3.3. Troisième Scénario

Dans le troisième scénario, nous concaténons le changement les paramètres des deux scenarios précédant (nombre des attaquants = 6 et nombre de tentative de découverte de la route = 2), ces paramètres d'après les scénarios précédents donnent l'impact le plus important sur le réseau.

Tous ces paramètres sont appliqués sur le protocole AODV.

Paramètre choisis pour la simulation	
Modèle de mobilité	Default Random way point
Placement des nœuds	Random
Nombre de nœuds	10
Nombre de nœuds attaquants	6
Nombre de tentative de découverte de route	2
Dimension du terrain	1000 m x 1000 m
carte de communication	802.11g (54Mbps)
Le temps de simulation	30 minutes
Paramètre du protocole AODV	Par défaut
Vitesse	5 m/s
Taille de paquets	1024 bits

Tableau 6.3 : Paramètres de troisième scénario de la simulation.

3.3.1. Les graphes d'AODV dans le troisième scenario

- **Trafic reçu router par AODV (AODV routing traffic received (Packets/sec))**

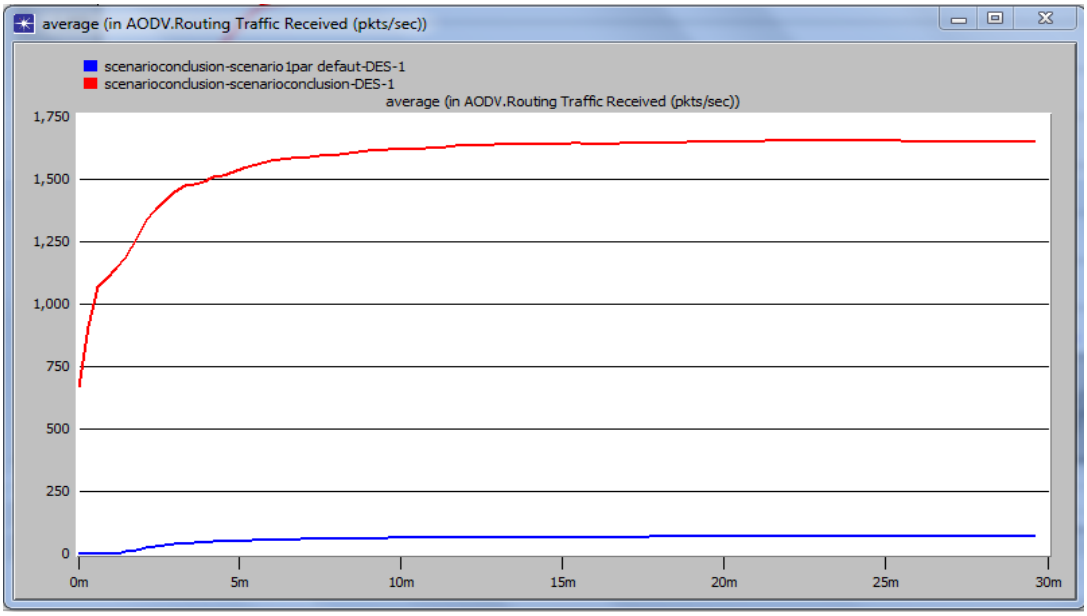


Figure 6.13 : Trafic reçu routé par AODV (Paquets/sec).

➢ On remarque que le trafic reçu agrandis que lorsqu'on fait combinaison entre les grand nombre d'attaquants et le minimum de nombre de tentative de découverte de la route. On conclue l'impact de réseau très élevé.

- **Total des paquets perdus (AODV Total packets dropped)**

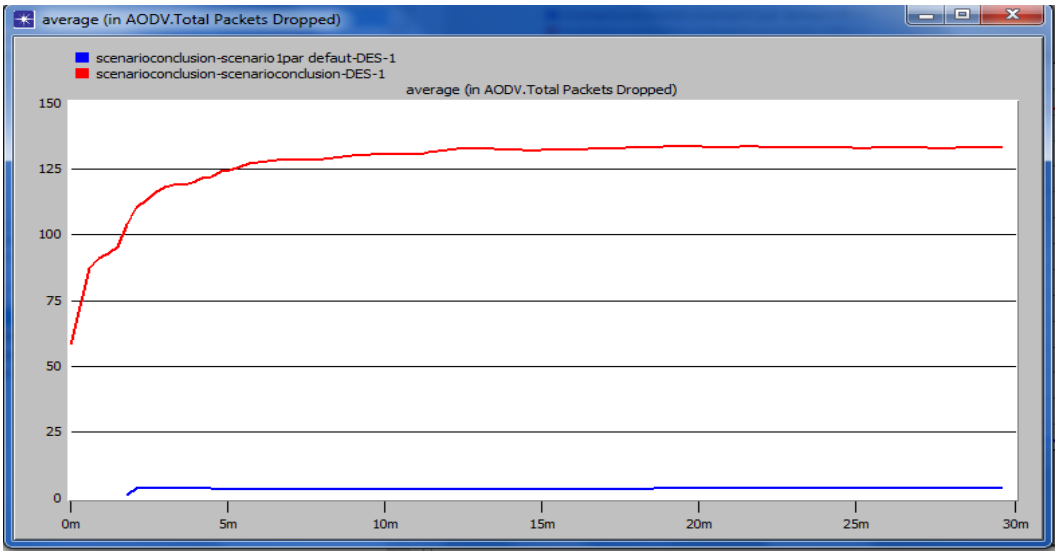


Figure 6.14 : Total des paquets perdus.

➢ Le nombre total des paquets perdus indique les conditions du trafic dues aux performances du protocole de routage. Le nombre de paquets perdus à travers le réseau et la performance du protocole AODV.

En remarquant dans le graphe 6.14 : la première courbe (bleu) initialement la perte des paquets est faible et plus tard sa valeur est maintenue constante, parce qu'il n'existe pas aucun attaquant.

Dans le cas de la seconde courbe (rouge) la perte des paquets beaucoup agrandisse par rapport premier courbe (bleu).

- **Total route demande paquets envoyés (Total Route Requests Sent (paquets))**

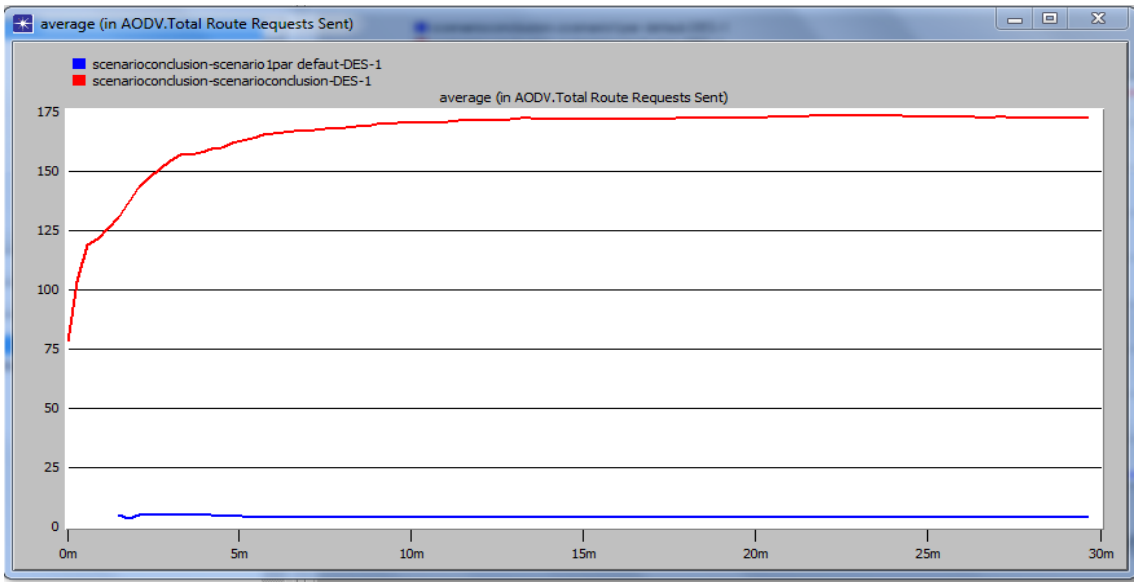


Figure 6.15 : Total route demande paquets envoyés.

➢ On a constaté dans la figure 6.15 à travers concaténation entre l'augmentation du nombre de nœuds malicieux = 6 et minimisation de nombre de la tentative de la découverte de route = 2, que le fonctionnement de Flooding augmente le total RREQ.

3.3.2. Graphes de Wireless dans troisième scénario

- **Bout en bout (Delay (sec))**

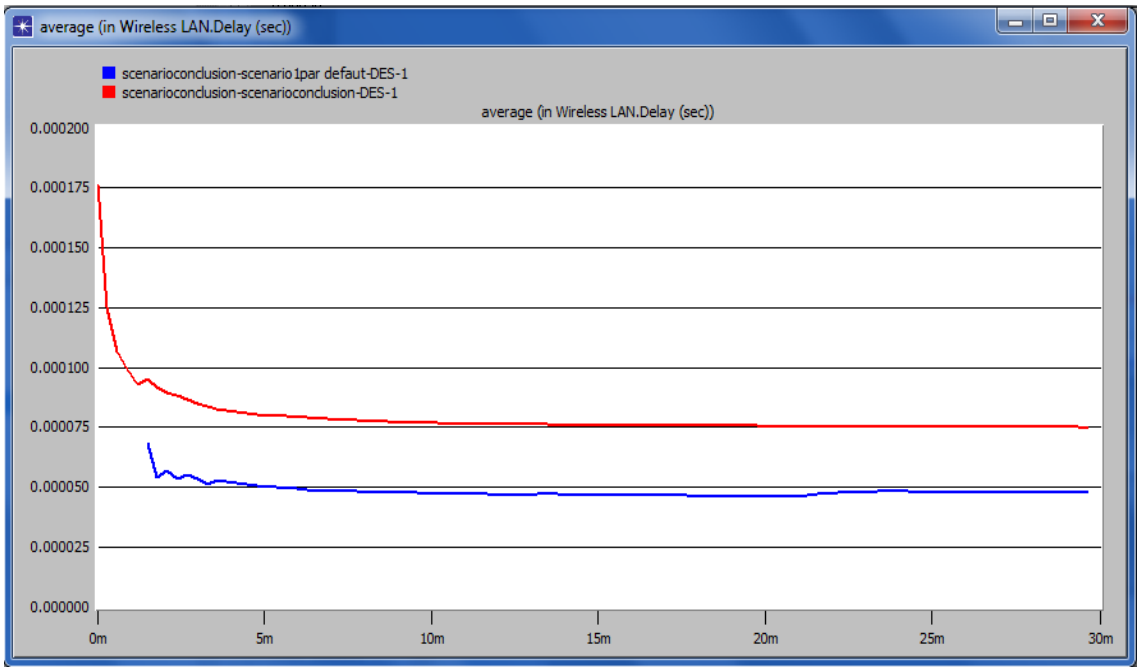


Figure 6.16: Bout en bout (sec)

➢ Les graphes 6.16 de bout en bout du protocole AODV avec attaque Flooding est élève par rapport AODV sans attaque.

- **Charge de réseau (Load)**

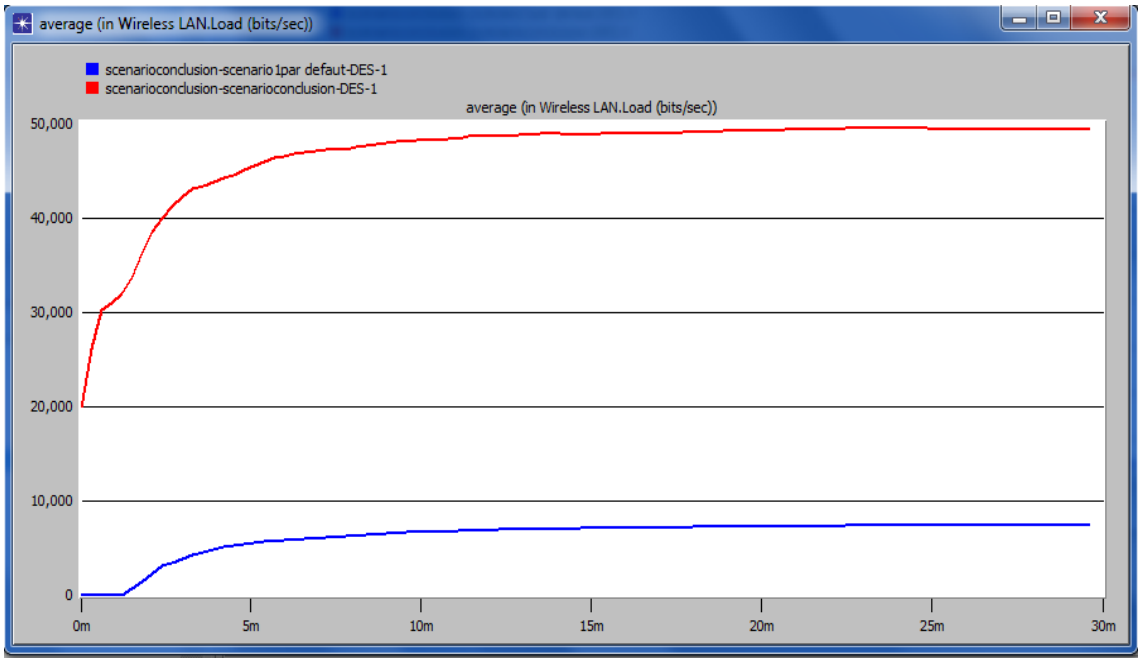


Figure 6.17: Charge de réseau (bits/sec)

➢ La charge total dans le réseau (bits / s) dans Le graphe de la figure 6.17 est très élevé avec les attaques Flooding par rapport un réseau sans des attaquants.

- **Débit (Throughput (bits/s))**

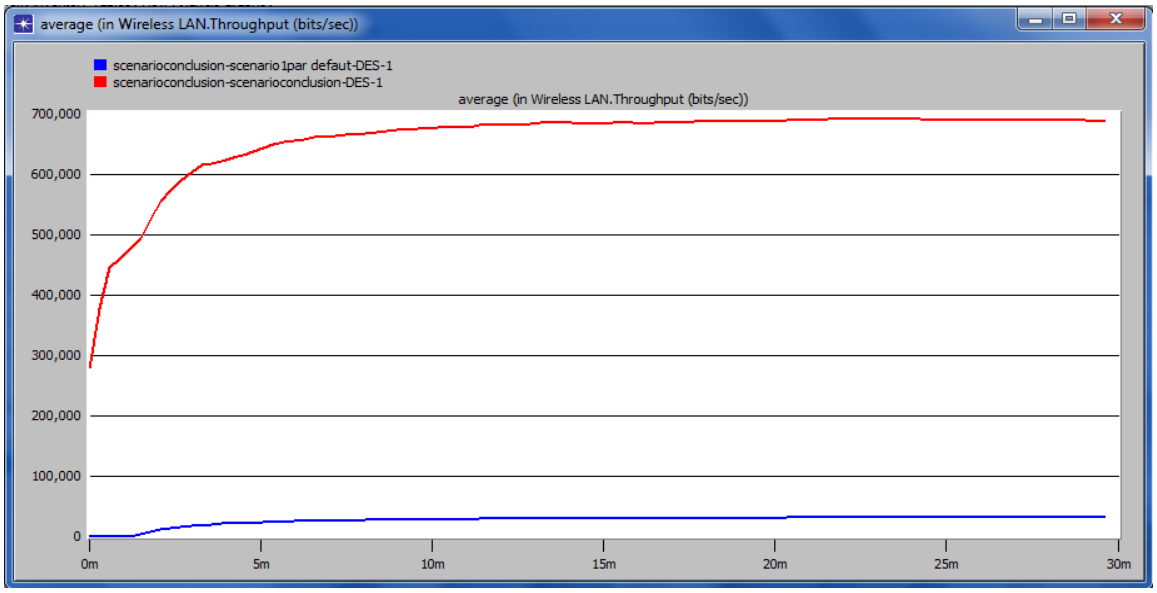


Figure 6.18: Débit (bits / sec)

➢ Le débit (bits/sec) est le nombre total des bits de données livrés de la couche LAN sans fil, jusqu'aux couches supérieures dans tous les nœuds du réseau. Dans la figure 6.18, la quantité totale des données qui arrive à la destination de la source (Throughput) est égale à 50,000 bits/second pour AODV dans premier courbe (bleu) sans attaques mais dans la deuxième courbe (rouge) avec les attaques égale 700,000 bits/second .On conclue l'impact d'attaque Flooding sur le débit augmente considérablement sur le réseau.

4. Conclusion

Dans ce chapitre, nous avons simulé et analysé l'impact d'attaque Flooding sur la fiabilité du routage dans les réseaux ad hoc à travers adresse de destination inconnu, de façon à changer et jouer sur les paramètres (ROUTE REQUEST RETRIERS), et le nombre d'attaquants. Mais le reste des paramètres (RREQ_RateLimit, TTL,…etc.) et les autres caractéristiques (nombre de nœuds, vitesse de mobilité, Diamètre de réseau,…etc.) restent inchangés.

D'après les résultats obtenus dans les 3 scenarios de simulation, nous remarquons que la surcharge sur les réseaux Ad Hoc avec attaquants augmente considérablement, il dégrade le bon fonctionnement de AODV, à travers les graphes de tests résultant de la simulation des scénarios, les courbes des graphes montrent que les métriques de performances dégradent toujours avec l'attaque de RREQ Flooding, on prend quelques métriques comme Paquets perdus, le trafic reçu, la charge de réseau, le débit …etc. Ces métriques sont apparais les plus importants pour nous comme des métriques de mesure de performance de réseau.

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. Ces équipements sont libres de se déplacer dans le réseau, d'y rentrer et de le quitter à volonté; ce qui donne le caractère spontané à ce type de réseaux. De plus, ces réseaux ne favorisent pas l'existence d'une quelconque autorité de contrôle ou de gestion, ce qui confère aux équipements les mêmes rôles dans le fonctionnement du réseau.

Pour assurer la communication entre les équipements du réseau, les MANETs utilisent le lien radio. Ceci permet à un nœud malicieux de se traverser facilement pour perturber le fonctionnement du réseau.

Les réseaux Ad Hoc présentent des challenges difficiles dans la sécurisation du routage.

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

Un exemple spécifique de l'une de ces attaques est l'attaque de Flooding RREQ. Ce type d'attaque peut représenter une menace importante pour dégrader le bon fonctionnement du réseau.

Ce mémoire a été principalement axé sur l'étude de l'impact de cette attaque sur les MANETs. Nous avons proposé une simulation pour l'attaque de Flooding RREQ. Nous sommes intéressés à ses effets au niveau de routage, plus précisément nous avons basé spécifiquement l'étude de l'impact de cette attaque sur le protocole AODV.

Nous sommes intéressés à l'analyse de l'attaque Flooding RREQ, nous avons proposé plusieurs scénarios permettant de mesurer l'impact de cette attaque sur le bon fonctionnement des réseaux, et nous avons les réalisé sous le simulateur de réseau OPNET 14.5.

Dans ce travail nous avons réalisé les tâches suivantes :

- La création d'un réseau Ad Hoc (MANET) sous OPNET14.5.
- L'activation de protocole de routage AODV sur ce réseau.
- La génération d'attaque de Flooding avec l'adresse IP de Destination inconnue.
- La réalisation des différents scénarios, le premier utilise l'adresse de destination inconnue et à chaque fois augmente le nombre d'attaquants, le deuxième utilise le paramètre ROUTE REQUEST RETRIES en minimise à chaque fois le nombre de tentative de découverte la route, et le troisième scénario c'est la combinaison entre les deux.
- Pour obtenir des résultats pour tester l'impact d'attaque sur ce réseau, des graphes représentent les métriques de performance de réseau sont générés pour chaque scénario.

➢ Perspectives

On peut ajouter et améliorer ce travail comme perspective plusieurs tâches concernant la détection et l'élimination d'attaque, les types d'attaques, les paramètres de l'attaquant …etc.
On peut les résumer comme suit :

- La détection des différents types d'attaques Flooding.
- L'élimination des nœuds attaquants détectées.
- Tester ce type d'attaque avec d'autres scénarios qui examinent l'effet sur la fiabilité de routage avec d'autres examination sur des nombres différents de nœuds, des vitesses de nœuds différents…etc.
- Identification d'autres paramètres qui augmentent l'impact de l'attaquant (TTL, RREQ_RATELIMIT,…etc.).
- L'extension de notre travail à d'autres types d'attaques, tels que trou noir, trou de ver, IP Spoofing, Sybille…etc.

REFERENCE BIBLIOGRAPHIQUE

[1] **Mohieddine KHEBBACHE**, Protocole de transport multicast fiable pour les réseaux sans fil, Mémoire En vue de l'obtention du diplôme de Magister en Informatique Option : Systèmes informatiques de communication(SIC), Université Hadj LAKHDAR -Batna-, 28/01/2014.

[2] **Ons BOUACHIR,** Conception et mise en œuvre d'une architecture de communication pour mini-drones civils, Thèse de doctorat, Université de Toulouse 3 Paul Sabatier, 02/12/2014.

[3] **Nadhir BOUKHECHEM,** Routage dans les réseaux mobiles Ad Hoc par une approche à base d'agents.

[4] **Akyildiz, I.F., Wang, X. and Wang, W. ,** Wireless mesh networks: a survey, Computer Networks, 47, 445-487, **2005**.

[5] **Yassine SNOUSSI**, Mécanisme de sécurité pour la famille de protocoles Ad Hoc OLSR organisés en grappes (clusters), maîtrise en génie concentration réseaux de télécommunications M.Ing, Université de MONTRÉAL, Soutenu le : 24/11/ 2011.

[6] **Abderrezak Rachedi,** Contributions à la sécurité dans les réseaux mobiles Ad Hoc, Spécialité : Networking and Internet Architecture, Université d'Avignon France, 2012.

[7] **TAHAR ABBES Mounir,** Proposition d'un protocole à économie d'énergie dans un réseau hybride GSM et AD HOC, présenter par pour obtenir LE diplôme de doctorat spécialité Informatique, 2011/2012.

[8] **Abderrezak BENYAHIA**, Adaptation de TCP aux réseaux sans fil, Mémoire de Magister Faculté des Sciences de l'Ingénieur ; Département d'Informatique ; Spécialité : systèmes informatiques de communication, Université Hadj Lakhdar -Batna-, 09/12/2012.

[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] **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.

[11] **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.

[12] **Guizani Badreddine,** Algorithme De Clusterisation Et Protocoles De Routage Dans Les Réseaux Ad Hoc, Thèse de doctorat de l'université de Technologie de Belfort-Montbéliard Tunisie, Avril 2012.

[13] **Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei,** A Survey on Attacks and Countermeasures inMobile Ad Hoc Networks , 2006 Springer .

[14] **Abdelaziz AOUES et Meryam HAMMOUDI** et **Youcef BENAISSA** et **Nadjet BENSAIDANE, Les** Réseaux Véhiculaires VANET, Département d'informatique L3 GTR Technologie Réseau, université des sciences et de la technologie Houari Boumediene, 2014/2015.

[15] **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.

[16] **Khadidja AYAD**, Sécurité du routage dans les réseaux Ad Hoc mobile, Thème de MAGISTER Option : Informatique Répartie et Mobile, 14 /11/ 2012.

[17] **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.

[18] **Abderrezak RACHEDI,** Contributions à la sécurité dans les réseaux mobiles Ad Hoc, Thèse de doctorat spécialité : Informatique, Université d'Avignon et des Pays de Vaucluse, 26 novembre 2008.

[19] **Valérie Gayraud, Loutfi Nuaymi, Francis Dupont, Sylvain Gombault et Bruno Tharon,** La Sécurité dans les Réseaux Sans Fil Ad Hoc ,2010.

[20] **KAZI TANI Chahrazad** et **Wiam BENHADDOUCHE,** Implémentation et test d'un protocole de prévention de l'attaque Clone dans un réseau de capteurs sans fil, Thème de Master en Informatique Option: Réseaux et systèmes distribués, 2013-2014.

[21] **Rachid ABDELLAOUI,** SU-OLSR une nouvelle solution pour la sécurité du protocole OLSR, Thèse de la maîtrise en génie concentration réseaux de télécommunications m.ing. , Université de Montréal, 05 /05/ 2009.

[22] **Boussad AIT-SALEM,** le Sécurisation des Réseaux Ad Hoc : Systèmes de Confiance et de Détection de Répliques, Thèse de doctorat Spécialité : Informatique, Université de LIMOGES, 12/07/2011.

[23] **Noureddine CHAIB,** La sécurité des communications dans les réseaux VANET, Thèse de Magister en Informatique Option : Ingénierie des systèmes informatiques (ISI), Université ELHADJ LAKHDER – BATNA.

[24] **Saloua CHETTIBI**, Protocole de routage avec prise en compte de la consommation d'énergie pour les réseaux mobile Ad Hoc, Université Ourgla, 2012.

[25] **Mohamed djihad BEN SALEM et Oussama BOUGOFFA**, Etude comparative de deux simulateurs pour les réseaux AD HOC sans fil, Mémoire de Master en Informatique Spécialité : Informatique Industriel, 14/06/2014.

[26] **Ameza Fatima, Assam Nassima, Atmani Mouloud,** Le routage dans les réseaux Ad Hoc (OLSR et AODV), Licence en informatique, Université Abderrahmane Mira BÉJAÏA, 2007.

[27] **Nabila LABRAOUI,** La sécurité dans les réseaux sans Fil Ad Hoc, Thèse de DOCTORAT, Université de Tlemcen, 2012.

[28] **Rima Bayaza,** master 2 Etude des protocoles de routage dans les réseaux VANET (Communication inter-véhiculesV2V 2014/2015.

[29] **Mohamed RAMDANI,** MÉMOIRE DE MAGISTER PROBLÈMES DE SÉCURITÉ DANS LES RÉSEAUX DE CAPTEURS AVEC PRISE EN CHARGE DE L'ÉNERGIE Par : Blida, Novembre 2013.

[30] **Zoulikha Zemali,** La sécurité de routage dans les réseaux Ad Hoc, master 2, 2014/2015.

[31] **Vimal Kumar Parganiha et Sanjivani Shantaiya et Somesh Dewangan,** Performance Evolution of MR-AODV for MANET Under Various Attacks, International Journal of Engineering Research & Technology (IJERT) IJERT ISSN: 2278-0181 - Vol. 3 Issue 3, Mars 2014.

[32] **Abdelmajid HAJAMI,** Sécurité du routage dans les réseaux sans fil spontanés : cas du protocole OLSR, THÈSE de doctorat ,12 Mai 2011.

[33] **Abdesselem BEGHRICHE,** De la Sécurité à la E-Confiance basée sur la Cryptographie à Seuil dans les Réseaux sans fil Ad Hoc, Université de Le Hadj Lakhdar-Batna, 2009.

[34] **Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Eli-zabeth M. Belding-Royer,** A secure routing protocol for Ad Hoc networks, In ICNP. IEEE Computer Society, 2002.

[35] **Manel Guerrero Zapata and N. Asokan, Douglas Maughan and Nitin H. Vaidya,** Securing Ad Hoc routing protocols, Workshop on Wireless Security, ACM, 2002.

[36] **P. Papadimitrato and Z. Haas,** Secure Routing for Mobile Ad Hoc Network, Conference SCS CNDS. In Proceeding of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), SanAntonio, TX January 27-31, 2002.

[37] **Yih-Chun Hu, David B. Johnson, and Adrian Perrig. Sead:** Secure efficient Distance vector routing for mobile wireless Ad Hoc networks. In WMCSA, IEEE Computer Society, 2002.

[38] **Yih-Chun Hu, Adrian Perrig, and David B. Johnson**, F**. Akyildiz, Jason Yi-Bing Lin, Ravi Jain, Vaduvur Bharghavan, and Andrew T. Campbell**, Ariadne: a secure On demand routing protocol for Ad Hoc networks. In Ian editors, MOBICOM, ACM, 2002.

[39] **Sarvesh Tanwar, Prema K.V.,** Threats & Security Issues in Ad Hoc network: A Survey Report, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, Janvier 2013.

[40] **Neha Kamdar, Vinita Sharma, Poorva Kakani,** Study of Various Attacks in MANET and Elaborative Discussion of RREQ Flooding Attack and Its Solutions, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (1) 104-107, 2016.

[41] **Houda HAFI,** Protocole pour la sécurité des réseaux sans fil peer to peer, Magister en Informatique, Université Kasdi Merbah Ouargla.

[42] **Ruchita Meher, Seema Ladhe , kamothe Navi,** Review Paper on Flooding Attack in MANET, Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 1(Version 2), India, pp. 39-46, Janvier 2014.

[43] **Khushboo Sawant et M.K Rawat et Lakshmi Narayan,** Survey of DOS Flooding Attacks over MANET Environment, Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 5 (Version 6), pp.110-115, Department of Computer Science & Engineering College of Technology Indore, India, May 2014.

[44] **Ujwala D. Khartad** et **R. K. Krishna Rajiv Gandhi,** Route Request Flooding Attack Using Trust based Security Scheme in Manet, College of Enginnering Research & Technolgy, Chandrapur India.

[45] **Pi Huang** et **Ian.W.Marshall, New** Flooding Control Schemes Applied In Route Initialization For The Ad Hoc On Demand Routing Protocols, Department of Electronic and Electrical Engineering, University College London.

[46] **M. Bani Yassein, M. Bani Khalaf ,** A Performance Comparison of Smart Probabilistic Broadcasting of Ad Hoc Distance vector (AODV), Department of Computing Science, Jordan University of Science and Technology.

[47] **Neetu Singh Chouhan** et **Prachi Jain,** Detection and prevention of Flooding attack in MANET using node reliability index University India, ISSN NO 2320-5407 International Journal of Advanced Research, 2013.

[48] **Neha Kamdar, Neeraj Paliwal ,** Performance Evaluation of Conditional Active RREQ Flooding-Filter Based Prevention Method for AODV in Manet, International Journal of Engineering Trends and Technology (IJETT) – Volume 15 Number 5 – ISSN: 2231-5381 Page 206,India, Sep 2014.

[49] **Examination of Impact of Flooding attack on MANET and to accentuate on Performance Degradation,** Bhuvaneshwari K. Scholar, A.Francis Saviour, Devaraj, J. Advanced Networking and Applications Volume: 04 Issue: 04 Pages: 1695-1699ISSN : 0975-0290 1695, Bangalore India, Janvier 2013.

[50] **Savita Gandhi2, Nirbhay Chaubey2, Naren Tada2, Srushti Trivedi2, Akshai Aggarwal**, NDTAODV: neighbor defense technique for ad hoc on-demand distance vector (AODV) to mitigate flood attack in MANETS, International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.1, DOI: 10.5121/ijcnc.2014.6102 19, Gujarat University, India, January 2014.

[51] **Jian-Hua Song, Fan Hong, Yu Zhang,** Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks,
College of Computer Science and Technology, IEEE, 2006.

[52] **Ping Yi et Zhoulin Dai et Shiyong Zhang et Yiping Zhong,** A New Routing Attack in Mobile Ad Hoc Networks, International Journal of Information Technology Vol. 11 No. 2, Department of Computing and Information Technology, Fudan University, Shanghai, 200433, Chine.

[53] **Charushila Choube, M. Murali,** Detection of Route Request Flooding Attack in MANET Using Session Based History Table, IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, www.ijiset.com ISSN 2348 – 7968 348, April 2015.

[54] **Sugata Sanyal, Ajith Abraham, Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia and Nirali Mody,** Security Scheme for Distributed DoS in Mobile Ad Hoc Networks.

[55] **Khushboo Sawant, Asst. Prof, HOD,** Novel Paradigm: Assessment of DOS Flooding Attack through Energy Aware Routing over MANET Environment, International Journal of Computer Applications (0975 – 8887) Volume 104 – No.14, October 2014.

[56] **HyoJin Kim, Ramachandra Bhargav Chitti, and JooSeok Song,** Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks**,** Journal of Information Processing Systems, Vol.7, No.1, March 2011 DOI: 10.3745/JIPS.2011.7.1.137.

[57] **Madhavi, S. et K. Duraiswamy,** flooding attack aware secure aodv, Journal of Computer Science, 9 (1): 105-113, ISSN 1549-3636, 2013.

[58] **Shishir K. Shandilya,** A Trust Based Security Scheme for RREQ Flooding Attack in MANET, International Journal of Computer Applications (0975 – 8887) Volume 5– No.12, August 2010.

[59] **Bhuvaneshwari et A. Francis Saviour et Devaraj,** Detection Scheme for Flooding attack in AODV based MANET, International Journal of Security, Privacy and Trust Management (IJSPTM) vol 2, No 3, PDS- A Profile based. Join 2013.

[60] **Vinita Mishra, Smita Jangale,** Analysis and comparison of different network simulators, International Journal of Application or Innovation in Engineering & Management (IJAIEM), ISSN 2319 – 4847 Special Issue for International Technological Conference, 2014.

[61] **Jianli Pan,** A Survey of Network Simulation Tools: Current Status and Future Development.

[62] **Attaur Rehman Khan, Sardar M. Bilal, Mazliza Othman,** A Performance Comparison of Network Simulators for Wireless Networks.

[63] **Rachid Haboub,** Proposition d'un protocole de routage sensible au contexte et sécurisé pour les réseaux Ad Hoc, Thèse de Doctorat Spécialité : Génie Informatique, Université Hassan II -Casablanca-, 21 /09/ 2013.