République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderahmane MIRA - BEJAIA -
Faculté de Technologie
Département D'électronique

جامعة بجاية
Tasdawit n'Bgayet
Université de Béjaïa

Mémoire de Fin d'Etudes

Présenté par

AIT ELHADJ Kahina
MAKHMOUKHEN Souhila

Pour l'obtention du Diplôme de Master Recherche

Filière : **Electronique**
Spécialité **: Télécommunication**

Thème

La sécurité des réseaux mobiles Ad hoc contre l'attaque du trou noir

Soutenu en public en date du : 22.06.2015

Devant le Jury:
Mr .BAADACHE Abderrahmane **Promoteurs**
Mr. BERRAH Smail

-KHIRDDINE Abdelkrim
-HAMADI Houria

Promotion 2014-2015

REMERCIEMENTS

Nous remercions Dieu, le tout puissant de nous avoir accordé santé, volonté, courage et patience qui nous ont été utiles tout le long de notre parcours.

Nous tenons à remercier nos encadreurs Mr. KHIREDDINE Abdelkrim et Melle. HAMADI Houria, pour leurs conseils et orientations tout au long d'élaboration de ce travail et pour leurs aides précieuses.

Nous tenons également à remercier Mr. BERRAH Smail pour avoir accepté de présider le jury, ainsi que, Mr. BAADACHE Abdarrahmane l'examinateur, pour l'honneur qu'ils nous font en participant à l'évaluation de ce travail.

Enfin, nous adressons nous remerciement à Mr. Ali Ait Mahamed " Directeur Operationnel Déploiement et Maintenance" Mr. HAROUN Farid "Service Transmission", Mr. DAHMOUN Abdelghafour de l'entreprise OOREDOO, Mr. BENDI El hadi et Mr.ZAIDI Mohand de nous avoir aidé à faire notre simulation, Mr. OUAMRI Mouhamed Amine doctorant à l'université de Bejaia, Mr.MEKHMOUKHE Abdenour, Mr. BAADACHE Abdarrahmane Docteur a l'université de Bejaia pour leurs soutien et leurs bonne volonté à l'aide.

Je dédie ce modeste travail :

A la lumière de mon chemin, mes parents qui m'ont donné la vie, le symbole de tendresse et l'école de mon enfance, qui ont veillé tout au long de ma vie a m'encourager à me donner de l'aide et à me protéger durant toutes les années d'études. Que dieu les gardes et les protège.

A mon frère et mes sœurs.

Et toute ma famille.

Aux étoiles de ma vie : mes amis.

A tous ceux qui me sont chères.

A tous ceux qui m'aiment.

A tous ceux que j'aime.

A toute la promotion télécommunication 2015.

A Chakib

MAKHMOUKHEN Souhila

Je dédie ce modeste travail :

A mes parents, mes frères, mes sœurs, toute ma famille et mes amis

AIT ELHADJ Kahina

Table des matières

Table des figures

Liste des tableaux

1G Première Génération
2G Deuxième Génération
3G Troisième Génération
4G Quatrième Génération

A

ACK Acknowledgement
ABR Associativlty Based Routing
AMPS Advanced Mobile Phone System
AODV Ad hoc On-Demand Distance Vector Routing Protocol

B

BLR Boucle Locale Radio
BS Base station

C

CBRP Clusfer Based Roufing Profocol
CDMA Code Division Multiple Access

D

DREAM Distance Routlng Effecl Aigorithm for Mobllity
DSDV Destination Sequenced Distance Vector
DSR Dynamic Source Routing Protocol

E

EDGE Enhanced Data Rates for GPRS Evolution
ETACS Extended Total Access Communication System

F

FSR Fisheye State Routing

G

GSM Global System for Mobile communications
GSR Global State Routing
GPRS General Packet Radio Service

H

HSDPA High Speed Downlink Packet Access
HSPA High Speed Packet Access
HSR Hierarchical State Routing
HSUPA High-Speed Uplink Packet Access

I

IEEE Institute of Electrical and Electronics Engineers

L

LAR LocatIon Alded Routing
LTE Long Term Evolution

M

MANET Mobile Ad-hoc Network
MMS Multimedia Messaging Service
MSS Mobile Support Station

N

NS Network Simulator

O

OLSR Optimized Link State Routing Protocol

R

RDMAR Relative Distance Micro-discovery Ad hoc Routing
RERR Route Error
RREP Route Reply
RREQ Route Request

S

SMS Short Message Service
SSR Signal Stabllity Roufing

T

TACS Total Access Communications System
TORA Temporally-Ordered Roufing Aigorithm
TTL Time To Live

U

USA United States of Amerique
UMTS Universal Mobile Telecommunication System
UM Unités Mobiles

W

WRP Wireless Routing Protocol
WLAN Wireless Local Area Network
WMAN Wireless Metropolitan Area Network
WPAN Wireless Personal Area Network
WRAN Wireless Regional Area Network
WRP Wlreless Routlng Protocol
WWAN Wireless Wide Area Network
WiMAX Worldwide interoperabilité for Microwave Access

Z

ZHLS Zone Based Hierarchical Link State
ZRP Zone Routing Protocole

Introduction Générale

Ces dernières années les réseaux sans fil ont connu une forte expansion, de plus en plus populaires du fait de leur facilité de déploiement ; ils offrent aujourd'hui des perspectives intéressantes dans le domaine des télécommunications.

L'évolution rapide de la technologie dans le domaine de la communication sans fil, a permis aux usagers munis d'unités de calcul portables d'accéder à l'information à n'importe quel moment depuis n'importe quel endroit. Cet environnement n'astreint plus l'usager à une localisation fixe, mais lui permet une libre mobilité tout en assurant sa connexion avec le réseau.

Les réseaux informatiques basés sur la communication sans fil peuvent être classés en deux catégories : les réseaux avec infrastructure fixe préexistante, et les réseaux sans infrastructure.

Dans la première catégorie les nœuds du réseau communiquent entre eux via un point d'accès, et sont basés sur un ensemble de sites fixes appelés stations de base, qui vont relier les différents nœuds mobiles entre eux pour former un réseau interconnecté.

La deuxième catégorie essaie d'étendre les notions de la mobilité à toutes les composantes de l'environnement, toutes les unités du réseau se déplacent librement et aucune administration centralisée n'est disponible. Les réseaux de cette catégorie sont appelés : les réseaux sans infrastructure ou Ad hoc.

Un réseau ad hoc peut être défini comme une collection d'entités mobiles qui sont dynamiquement interconnectées par une technologie sans fil formant un réseau temporaire pour répondre à un besoin ponctuel de communication sans l'aide de toute administration ou de tout support fixe.

Dans la plupart des cas, l'hôte destination ne se trouve pas obligatoirement dans la portée de communication directe de l'hôte source, ce qui nécessite l'emploi d'un routage interne par des nœuds intermédiaires afin de faire acheminer les paquets de messages à la bonne destination.

La gestion de l'acheminement de données ou le routage, consiste à assurer une stratégie qui garantit, à n'importe quel moment, la connexion entre n'importe quelle paire de nœuds appartenant au réseau.

Suivant la manière de création et de maintenance de routes, plusieurs protocoles de routage pour les réseaux Ad hoc ont été développés pour disséminer des informations de routage nécessaires à l'obtention et à la maintenance des routes. Suivant le type de dissémination de l'information, ces protocoles peuvent être répertoriés en trois grandes classes : proactifs , réactifs et hybrides.

Introduction Générale

Ces réseaux sont par nature, sensibles aux problèmes de sécurité. Plusieurs attaques peuvent être menées sur les différentes fonctionnalités du réseau ad hoc, en particulier la fonction de routage telles que : l'usurpation d'identité, la suppression des données, modification des messages, Blackhole, whormhole, et d'autres attaques peuvent aussi être menées dans un réseau ad hoc.

Pour sécuriser cette fonction, plusieurs efforts de recherche ont été entrepris ces dernières années visant à sécuriser l'opération de routage, pour proposer de multiples solutions, mais une protection parfaite est loin d'être évidente, à cause de la diversité des attaques possibles.

Dans notre travail, on s'est focalisé sur l'attaque de trou noir, dans laquelle un nœud malicieux supprime les paquets passant par lui au lieu de les acheminer vers son successeur dans un chemin reliant une source et une destination données. Notre solution consiste à vérifier le bon acheminement des messages par un nœud intermédiaire de coté, et de l'autre coté le principe des numéros de séquence. Ce mémoire est structuré autour de cinq chapitres : Le premier chapitre présente les différents types de réseaux sans fil ainsi que leurs classifications.

Au deuxième chapitre nous introduisons le concept des réseaux mobiles ad hoc, leurs caractéristiques, leurs applications, et les différentes classes de protocole de routage dans cet environnement.

Le troisième chapitre concerne l'analyse des services de sécurité exigée, et les différentes attaques possibles.

Le quatrième chapitre est consacré au développement des attaques liées aux protocoles du routage AODV. Nous spécifions l'attaque du trou noir menée sur ce protocole ainsi qu'une description des solutions proposées pour le sécuriser en première lieu, en second lieu pour notre proposition pour se protéger contre cette attaque.

Le dernier chapitre présente notre plateforme virtuelle de simulation ainsi que ses différentes étapes d'installation et de configuration afin de valider notre proposition. Les résultats de simulation sont aussi décrits dans ce chapitre pour montrer l'efficacité de la solution proposée .

On termine notre travail par une conclusion et des perspectives.

Chapitre 1

Réseaux sans fils

1.1 Introduction

Un réseau sans fil est un réseau informatique ou numérisé qui connecte différents postes ou systèmes entre eux par ondes radios. Le réseau sans fil peut être associé à un réseau de télécommunication pour réaliser des interconnexions entre nœuds.

Les réseaux mobiles sans fil, peuvent être classés en deux classes : les réseaux avec infrastructure qui utilisent généralement le modèle de la communication cellulaire, et les réseaux sans infrastructure. Plusieurs systèmes utilisent déjà le modèle cellulaire et connaissent une très forte expansion à l'heure actuelle.
Ce chapitre est consacré initialement à l'introduction des différentes notions élémentaires des réseaux sans fils, en particulier les réseaux de mobile (cellulaires).

1.2 Réseaux sans fil

1.2.1 Définition d'un réseau sans fil

Un réseau sans fils (en anglais wireless network) est un réseau dans lequel les différents éléments participants (ordinateur portable, téléphone portable...etc.) ne sont pas raccordés entre eux par un média physique .

La transmission des données se fait via les ondes hertziennes (radio ou infrarouge),ceci permet aux utilisateurs de se déplacer dans un périmètre de couverture pouvant aller d'une dizaine de mètres à quelques kilomètres [6].

1.2.2 Architectures des réseaux sans fils

Les architectures les plus courantes dans les réseaux sans fil peuvent classés en deux classes :

1. les réseaux avec infrastructure.

2. les réseaux sans infrastructure ou ad hoc .

Réseaux avec infrastructure

Le réseau mobile avec infrastructure intègre deux ensembles d'entités distinctes :
- Les « sites fixes » d'un réseau de communication filaire classique (wired network).

- Les sites mobiles (wireless network)

Certains sites fixes, appelés stations support mobile (MSS) ou station de base (BS) sont munis d'une interface de communication sans fil pour la communication directe avec les sites ou unités mobiles (UM), localisés dans une zone géographique limitée, appelée cellule (voir figure 1.1).

A chaque station de base correspond une cellule à partir de laquelle des unités mobiles peuvent émettre et recevoir des messages. Alors que les sites fixes sont interconnectés entre eux à travers un réseau de communication filaire, généralement fiable et d'un débit élevé. Les liaisons sans fil ont une bande passante limitée qui réduit sévèrement le volume des informations échangées. Dans ce modèle, une unité mobile ne peut être, à un instant donné, directement connectée qu'à une seule station de base.

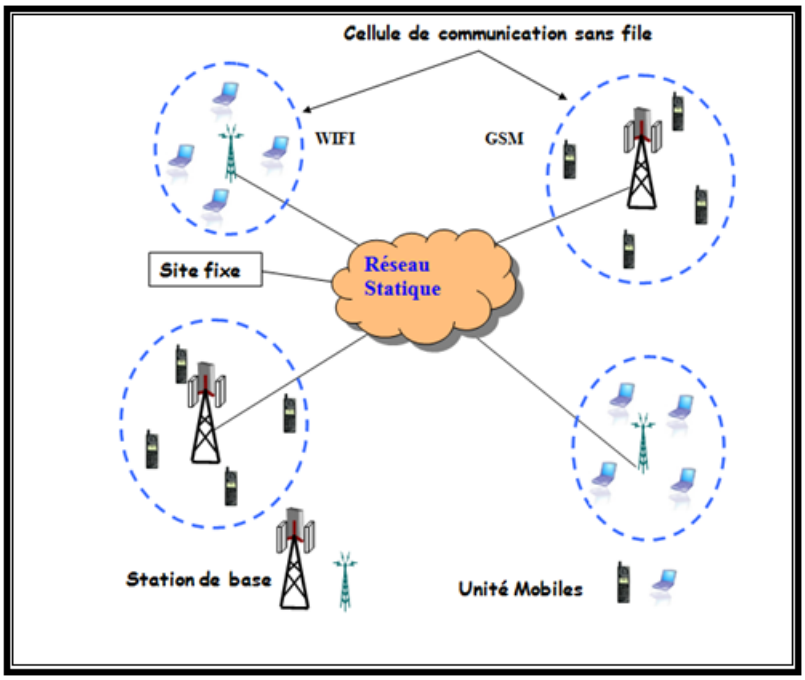

FIGURE 1.1 – Le modèle des réseaux mobiles avec infrastructure

Réseaux sans infrastructure

Le modèle de réseau mobile sans infrastructure préexistante ne comporte pas l'entité « site fixe », tous les sites du réseau sont mobiles et se communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil (voir figure 1.2). L'absence de l'infrastructure ou du réseau filaire composé des stations de base, oblige les unités mobiles à se comporter comme des routeurs qui participent à la découverte et la maintenance des chemins pour les autres hôtes du réseau

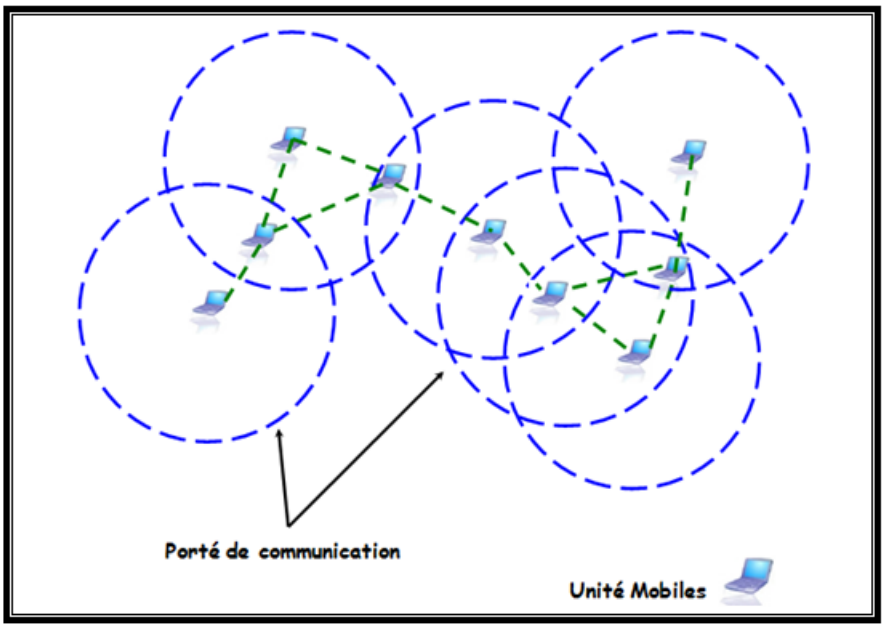

FIGURE 1.2 – Le modèle des réseaux mobiles sans infrastructure.

1.3 Classification des réseaux sans fils

1.3.1 Réseaux personnels sans fils (WPAN)

Le réseau personnel sans fil, concerne les réseaux d'une faible portée de l'ordre de quelques dizaines de mètres. Ce type sert généralement à relier des périphériques (imprimante, téléphone portable ...) ou bien à permettre la liaison sans fil entre deux machines très peu distantes. Les technologies les plus utilisées dans WPAN ont : l'infrarouge à100 Kbit/s et Bluetooth (802.15.1) environ 1 Mbit/s [1].

1.3.2 Réseaux locaux sans fils (WLAN)

Le réseau local sans fil est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre eux les terminaux présents dans la zone de couverture. Ils autorisent des débits allant de 2 à 54 Mbit/s. La technologie la plus utilisée dans ce types de réseau est wifi (802.11n)[1].

1.3.3 Réseaux métropolitains sans fils (WMAN)

Le réseau métropolitain sans fil est connu sous le nom de Boucle Locale Radio (BLR), permet à un particulier ou une entreprise d'être relié à son opérateur (téléphonie fixe, Internet, télévision...) via les ondes radio. Elle offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres. WiMAX (802.16) étant certainement le plus prometteur dans ce domaine [1].

1.3.4 Réseaux étendus sans fils (WWAN)

Le réseau étendu sans fil est également connu sous le nom de réseau cellulaire mobile dont la zone de couverture est très large, à l'échelle mondiale. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à ce réseau. Les débits, sont relativement faibles de quelques dizaines de kbit/s (10 à 380 kbit/s). Dans cette catégorie, on peut citer : GSM, GPRS, UMTS, LTE,LTE-Advenced [1].

1.3.5 Réseaux régional sans fils (WRAN)

L'objectif de ce type de réseaux est de couvrir une large surface géographique, ils peuvent avoir 50 kilomètres de rayon, ce qui permet, à partir d'une seule antenne, de connecter un très grand nombre d'utilisateurs. Cette norme a été élaborée pour offrir un accès large bande à de vastes régions n'importe où dans le monde ainsi que des communications rapides, fiables et sécurisées à des collectivités ayant des services insuffisants ou inexistants [1][2].

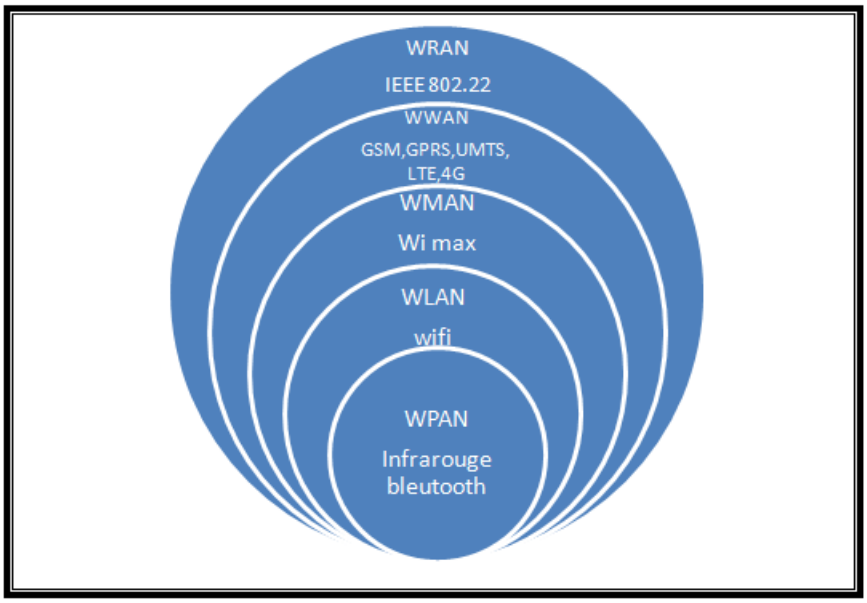

FIGURE 1.3 – Classification des réseaux sans fils

1.4 Réseaux de mobiles (réseaux cellulaires)

Un réseau de téléphonie mobile a une structure « cellulaire » qui permet de réutiliser de nombreuses fois les mêmes fréquences ; il permet aussi à ces utilisateurs en mouvement de changer de cellules (handover) sans coupure de communication [1].

Ces communications mobiles existent depuis un demi-siècle, mais c'est dans les années 80 qu'elles se sont vraiment développées. Les réseaux de mobiles connaissent un énorme succès. On trouve dans les réseaux mobiles des quatre générations : 1G, 2G, 3G, 4G. La 1G a disparu dans la plupart des pays, la 2G correspond au GSM, la 3G correspond a l'UMTS et la 4G au LTE-ADVENCED ou LTE-A [2].

1.4.1 Réseaux mobiles de première génération

La première génération de téléphonie mobile (notée 1G) possédait un fonctionnement analogique et été constituée d'appareils relativement volumineux. La bande de fréquence de fonctionnement est au tour de 450 MHz et de 900 MHz. Il s'agissait principalement des standards suivants :

AMPS

Apparu en 1976 aux USA, constitue le premier standard de réseau cellulaire. Possède de faibles mécanismes de sécurité rendant possible le piratage des lignes téléphoniques.

TACS

Est la version européenne du modèle AMPS. Utilisant la bande de fréquence de 900 MHz, ce système été utilisé en Angleterre, puis en Asie.

ETACS

Est une version améliorée du standard TACS développé au Royaume-Uni utilisant un nombre plus important de canaux de communication [3].

1.4.2 Réseaux mobiles de deuxième génération

La deuxième génération de réseau mobile est apparue vers les années 90. Elle a marqué une rupture avec la première génération de téléphones cellulaires grâce au passage de l'analogique vers le numérique. Il s'agit principalement des standards suivants : [4]

GSM

Cette norme autorise un débit maximal de 9,6 Kbit /s. Ce débit permet de transmettre la voix ainsi que des données numériques de faible volume, par exemple des messages textes(SMS) ou des messages multimédias (MMS)[6].

GPRS

C'est une évolution de la norme GSM, on parle généralement de 2,5G pour classifier ce standard. Cette norme autorise le transfert de données par paquets, avec des débits théoriques maximum de l'ordre de 171,2 Kbit/s, 40 Kbit/s en pratique. Grâce au mode de transfert par paquet, les transmissions de données n'utilisent le réseau que lorsque c'est nécessaire. Ce standard permet de facturer l'utilisateur au volume échangé plutôt qu'à la durée de connexion, ce qui signifie notamment qu'il peut rester connecter sans surcoût. GPRS à permis d'initier l'internet mobile [7].

EDGE

Le passage de 2G à la 3G est couteux car il faut déployer un nouveau réseau physique. Les operateurs ont donc cherché des alternatives. L'une d'entre elle est l'EDGE présentée comme la génération 2,75. Elle vise à optimiser la partie radio d'un réseau mobile sur la partie « données » afin d'augmenter les débits de téléchargements. En théorie EDGE permet d'atteindre des débits allant jusqu'à 384 Kbit/s, 100 Kbit /s en

pratique[8].

1.4.3 Réseaux mobiles de troisième génération

La troisième génération est apparue en 2000, elle désigne une génération de norme de téléphonie mobile. Elle est représentée principalement par la norme UMTS. Les premières applications grand public de la 3G sont l'accès à l'internet, le visionnage de vidéos, voire même d'émission de télévision et la visiophonie. Il n'existe pas un, mais plusieurs systèmes de troisième génération, parmi ceux-ci, l'UMTS, LTE, CDMA2000 [4].

UMTS

Est l'une des technologies de téléphonies mobile de 3éme génération, le procédé employé pour faire transiter la voix et les données a été entièrement reconsidéré. Ce nouveau standard permet d'atteindre un débit de 10 Mbit/s en réception et à 5 Mbit/s en émission. Afin de faire transiter toutes ces données, une nouvelle bande de fréquences a été allouée à l'UMTS dans le spectre, aux alentours de 2100 MHz. En 2011, l'UMTS est déjà déployé sur plus de (95 %) de la population [4][6].

3G+

Une génération intermédiaire entre la 3G et la 4G s'est mise en place avec des extensions de l'UMTS et une augmentation des débits, c'est-à-dire plus de 1 Mbit/s. Cette valeur est obtenue par la technologie HSDPA dans le sens descendant et par son successeur HSUPA dans le sens montant [2].

Cette génération intermédiaire est illustrée par les solutions HSDPA, HSUPA et LTE. Basée sur la technologie HSDPA, la 3G+ est une évolution du réseau 3G, qui permet une augmentation des débits pour le téléchargement et le transfert de données jusqu'à 14,4 Mbit/s en théorie et 3,6 Mbit/s en pratique.

1.4.4 Réseaux mobiles de quatrième génération

Ces réseaux HSPA+, sont si rapides que certains n'hésitent pas à le commercialiser sous le nom de 4G. Même la LTE qui est a la mode ces derniers mois est techniquement un réseau de troisième génération : elle n'atteint pas le seuil des Gbite, mais se limite a 300 Mbit/s. on l'appelle donc parfois 3.9G.

La LTE utilise néanmoins un grand nombre de bande de fréquences que les téléphones ne pourront pas tout prendre en charge : un téléphone pouvant se connecter n'importe

où dans le monde est encore un rêve.

La 4G est définie non seulement par un seuil de débit, mais aussi par l'abandon total du mode commuté c'est-à-dire, du canal voix. La LTE-Advanced sera le premier réseau à répondre techniquement à la définition originale des réseaux de la 4G [5].

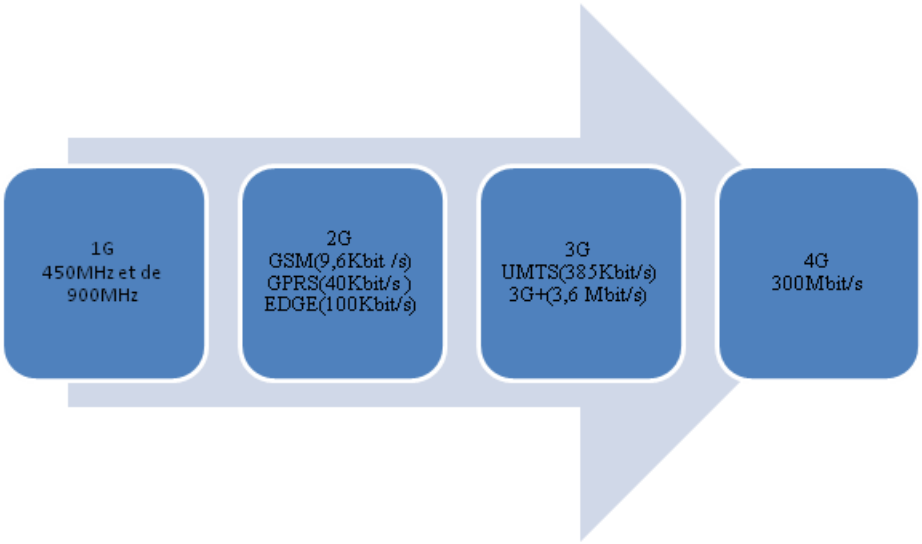

FIGURE 1.4 – générations de la téléphonie mobile

1.5 Conclusion

Dans ce chapitre nous avons étudiés les réseaux sans fils et les réseaux de mobiles de manière générale.
Dans le chapitre suivant, nous porterons toute notre attention sur le réseaux mobile ah-doc

Chapitre 2

Réseaux Mobile ad hoc

2.1 Introduction

Les systèmes de communication cellulaires sont basés essentiellement sur l'utilisation des réseaux filaires et la présence des stations de base qui couvrent les différentes unités mobiles du système, la contrepartie de ces réseaux sont des réseaux ad hoc qui se forment spontanément et qui s'organisent automatiquement sans avoir besoin d'une infrastructure existante. Dans ce chapitre, nous visons à donner un aperçu sur les réseaux ad hoc et quelques concepts liés à cette notion tels que le routage.

2.2 Historique

Le début des années 1970 voit, au sein du projet militaire Américain DARPA(The Defense Advanced Research Projects Agency), la naissance des premiers réseaux utilisant le médium radio .Ces réseaux disposaient déjà d'une architecture distribuée, partageaient le canal de diffusion en répétant des paquets pour élargir la zone de couverture globale. Par la suite, en 1983 les Sur vivable Radio Networks (SURAN) furent développés par DARPA.

L'objectif était de dépasser les limitations en particulier permettre le passage à des réseaux comportant énormément des nœuds, gérant la sécurité, l'énergie. Mais les recherches sur ces réseaux restaient exclusivement militaires. Ce n'est qu'avec l'arrivée du protocole IEEE 802.11 qui permet de bâtir des réseaux sans fils autour de stations fixes [18].

2.3 Présentation des Réseaux Mobiles ad hoc

Un réseau mobile ad hoc est constitué de station munie d'une interface de communication radio qui se propage entre les différents nœuds mobiles qui se déplacent librement dans un territoire quelconque, chaque nœud dans le réseau ad hoc doit se comporter comme un terminal, et aussi comme un routeur, dont le seul moyen de communication est l'utilisation des interfaces sans aucune infrastructure fixe préexistante [10][11][12].

2.4 Les caractéristiques des réseaux ad hoc

Les réseaux sans fil ad hoc se caractérisent principalement par ce qui suit :

- Absence d'infrastructure : Le réseau ad hoc ne dépend donc pas d'une infrastructure préexistante. Chaque nœud opère comme un routeur indépendant, il est responsable de l'établissement et le maintien d'une connectivité continue [9].

- Mobilité et topologie dynamique : Dans un réseau ad hoc, la topologie du réseau peut changer rapidement, de façon aléatoire, cela est dû au déplacement libre et aléatoire des unités mobiles du réseau, les liens de la topologie peuvent être unis ou bidirectionnels [7].

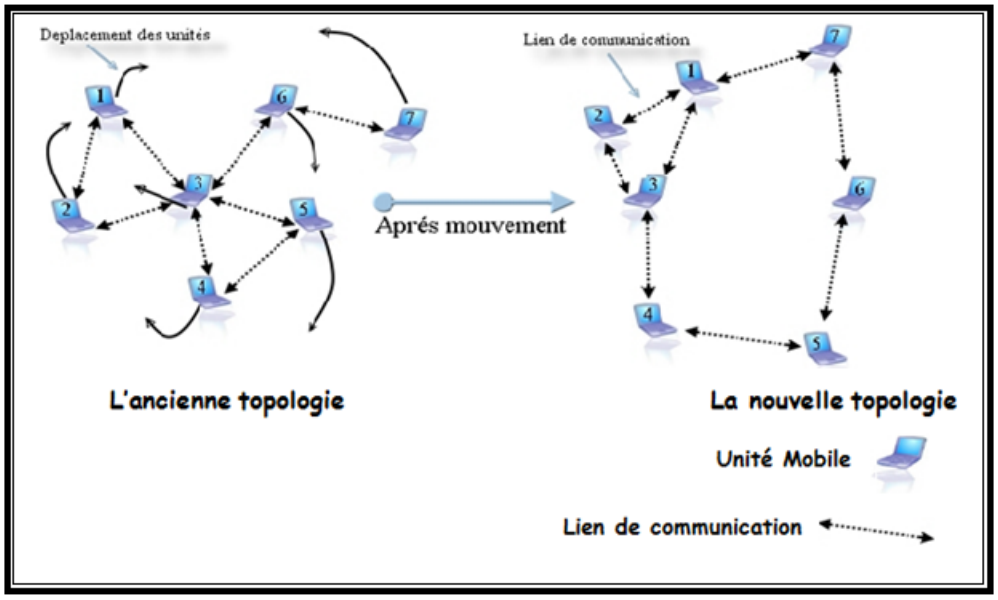

FIGURE 2.1 – Le changement de la topologie des réseaux Ad Hoc

- Bande passante limite : L'utilisation d'un médium de communication partagé est

une caractéristique primordiale des réseaux basés sur la communication sans fil. Ce partage fait que la bande passante réservée à un hôte soit modeste [8].

- Energie limite : Les nœuds dans un réseau ad hoc sont alimentés typiquement par des batteries dont la capacité en puissance est souvent limitée.Par conséquent, elle ne peut satisfaire les demandes d'énergies d'un nœud pour un fonctionnement normal durant une période de temps raisonnable [9].
Le paramètre d'énergie doit être pris en considération dans tout contrôle fait par le système [8].

- Sécurité physique limitée : Les réseaux mobiles ad hoc sont généralement plus vulnérables aux menaces de pertes d'informations et de sécurité que les autres réseaux filaires et cellulaires. Cette vulnérabilité est dûe essentiellement à la nature du médium de propagation sans fil qui rend possibles certaines attaques malicieuses allant de l'écoute clandestine passive aux interfaces actives [9].

Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé [10].

- Erreur de transmission et interférences : Dans un réseau ad hoc, les liens radio ne sont pas isolés. Ceci peut impliquer que deux transmissions simultanées sur une même fréquence ou sur des fréquences proches peuvent interférer et provoquer des erreurs de transmission [9][11].

2.5 Domaines d'utilisation des réseaux ad hoc

Le réseau Ad hoc n'a besoin d'aucune installation fixe, ceci lui permettant d'être rapide et facile à déployer. En effet, la robustesse, le coût réduit qui rend ce réseau très utilisé dans plusieurs domaines :
- Services Militaires : Les réseaux ad hoc ont été utilisés la première fois par l'armée. Lors d'interventions en milieu hostile, il peut être difficile ou trop encombrant d'utiliser un réseau à infrastructure ce type de réseaux est la solution idéale pour maintenir une communication sur un champ de bataille entre les différentes troupes d'une armée.
Les réseaux sans fils sont parfaitement bien adaptés à ce type d'environnement ou les déplacements restent peu rapides et peu soutenus [6][9].

- Les services d'urgence : Dans les zones touchées par les catastrophes naturelles, le déploiement d'un réseau ad hoc est indispensable pour permettre eux unités de secours de communiquer dans le but de remplacer l'infrastructure filaire [6][13].

- Applications de collaborations : Les utilisateurs professionnels ont besoin d'applications particulières lors d'échanges entre collaborateurs.

Ainsi, au cours de réunions ou de conférences, ces utilisateurs peuvent ressentir le besoin de former dans n'importe quel lieu un réseau pour s'échanger des informations, ou faire une vidéo conférence entre bureaux voisins. Les réseaux ad hoc sont bien appropries à ces besoins [9].

- Mise en œuvre des réseaux véhiculaires : sur un réseau routier les véhicules peuvent avoir besoin de communiquer entre eux ou avec leur environnement afin de partager des informations dans le but de gérer et réguler le trafic routier. Les réseaux ad hoc sont alors la solution idéale[6].

- Home network : partage d'applications et communications des équipements mobiles [14].

2.6 Les avantages et les inconvénients des réseaux ad hoc

• Avantages

- Un coût faible : parce que ce réseau ne nécessite pas l'installation de stations de base, les mobiles sont les seules entités physiques pour déployer un tel réseau.

- La rapidité de mise en place : l'absence d'une infrastructure permettant d'économiser tout le temps.

- Souplesse d'utilisation : puisque les seuls éléments peuvent tomber en pain sont les nœuds eux-mêmes.

- Extensible : Ce réseau est facile de l'étendre et d'augmenter sa taille, il suffit de procéder à quelques configurations au niveau du nœud lui-même.

- Si l'un des nœuds du réseau devient indisponible pour cause de défaillance ou de manque d'énergie, cela ne change rien ou presque pour les autres nœuds qui vont se réorganiser et continuer leurs communications [15][16].

• Inconvénients

- La sécurité des réseaux ad hoc est difficile à contrôler et d'assurer la confidentialité de l'information échangée entre les nœuds.

- Les signaux envoyés par les interfaces sans fils s'atténuent au fur et à mesure qu'ils s'éloignent de leur émetteur, un nœud dans les réseaux ad hoc ne peut donc pas communiquer avec un autre s'il est situé trop loin de lui, il doit alors passer par des nœuds

intermédiaires pour atteindre la destination désiré [15][16].

2.7 Le routage dans les réseaux mobiles ad hoc

Les communications dans les réseaux ad hoc constituent une tâche difficile à réaliser. En effet, en l'absence d'infrastructure, l'acheminement d'un paquet d'une source vers son nœud destination n'est pas aisé.Il s'agit de découvrir un chemin entre les deux nœuds qui sera amené à changer dans le temps et être découvert lors d'une prochaine communication.

Généralement, le routage est une méthode d'acheminement d'informations vers la bonne destination à travers un réseau de connexion donné, il consiste à assurer une stratégie qui garantit à n'importe quel moment, un établissement de routes qui soient correctes et efficaces entre n'importe quelle paire de nœuds appartenant au réseau, ce qui assure l'échange des messages d'une manière continue[10][17].

2.8 Notions fondamentales sur le routage

Vue à la difficulté de routage dans les réseaux Ad Hoc, les stratégies existantes utilisent une variété de techniques afin de résoudre ce problème. Suivant ces techniques plusieurs classifications sont apparues parmi lesquelles nous allons citer :

Routage hiérarchique ou plat

Le premier critère utilisé pour classifier les protocoles de routage dans les réseaux Ad Hoc concerne le type de vision qu'ils ont du réseau et les rôles qu'ils accordent aux différents mobiles

• **Les protocoles de routage à plat** considèrent que tous les nœuds sont égaux. La décision d'un nœud de router des paquets pour un autre dépendra de sa position. Permis les protocoles utilisant cette technique, on cite l'AODV (Ad Hoc On Demand Distance Vector) [62].
• **Les protocoles de routage hiérarchique** fonctionnent en confiant aux mobiles des rôles qui varient de l'un à l'autre. Certains nœuds sont élus et assument des fonctions particulières qui conduisent à une vision en plusieurs niveaux de la topologie du réseau [62].

2.8.1 Routage à vecteurs de distance

Dans un routage à vecteurs de distance, chaque nœud diffuse périodiquement sa table de routage à ses voisins, la table contient les adresses des nœuds destination du réseau et la distance en nombre de sauts pour atteindre chacun d'eux. Un nœud met sa table de routage à jour s'il trouve une route plus courte que celle qu'il a dans sa table, ou si le nœud par lequel il passe pour atteindre une destination donnée change la distance vers cette destination, ou encore s'il trouve un nœud inconnu (c'est-à-dire, qui n'existe pas dans sa table) [62].

2.8.2 Routage à état de liens

Dans un routage à état de liens, chaque nœud vérifie l'état des liaisons avec ces voisins (peut aussi calculer le coût de ces liens), et diffuse un paquet contenant ces informations à tout le réseau. Ces diffusions permettent à chaque nœud d'avoir une connaissance complète de la topologie du réseau [62].

2.9 Techniques du routage

On distingue, en général deux techniques de routage :
- le routage à la source .
- le routage saut par saut.

• **Routage à la source** Le routage à la source ou "source routing" consiste à indiquer dans le paquet routé l'intégralité du chemin que devra suivre le paquet pour atteindre sa destination. L'entête du paquet va donc contenir la liste des différents nœuds relayeurs vers la destination [62].
• **Routage saut par saut** Le routage saut par saut ou "hop by hop" consiste à donner uniquement à un paquet l'adresse du prochain nœud vers la destination. Ce type de routage est le routage le plus rependu dans l'Internet, c'est le système de routage par défaut. AODV fait partie des protocoles qui utilisent cette technique [62].

2.9.1 Routage uniforme ou non uniforme

Une autre méthode de classification est basée sur le rôle que jouent les nœuds dans un schéma de routage. Selon ce critère de classification, on distingue les protocoles de routage uniformes et non uniformes.

Dans un protocole de routage uniforme, tous les nœuds mobiles ont le même rôle, importance et fonctionnalité.

Dans un protocole de routage non uniforme, certains nœuds ont des fonctions de gestion et de routage particulières. Les protocoles non uniformes à leur tour peuvent être subdivisés selon l'organisation des nœuds mobiles et selon les stratégies de gestion et de routage en : des protocoles basés sur les zones, basés sur les clusters ou basés sur des nœuds noyaux [12].

2.10 Les protocoles de routage dans les réseaux ad Hoc

De nombreux protocoles et algorithmes ont été proposés pour rendre la communication dans les réseaux ad hoc plus efficace, dont la fonction principale est de fournir le chemin le plus court en termes de nombre de sauts entre une source et une destination de manière a ce que le nombre de messages générés soit minimum.

Le routage dans les réseaux Ad hoc est assez délicat étant donnée la nature changeante de la topologie de ce type de réseaux. Pour cela, de nombreux protocoles sont proposés pour résoudre le problème multi saut, chacun fondé sur différents concepts et reposant sur différentes hypothèses et intuitions [19][20].

2.11 Classification des protocoles de routage

Selon la manière de création et de maintenance de routes lors de l'acheminement des données, la classification des protocoles de routage se fait en fonction de la méthode de création et de maintenance de routes lors de l'acheminement des données.

Suivant les informations de routages échangés et les méthodes de calcul des routes utilisées, on distingue trois familles de protocoles de routage ad hoc : les protocoles de routage dits “proactifs“ et les protocoles de routage “réactifs“. Entre ces deux famille, une autre approche qui fait un mélange entre les deux approches précédentes, il s'agit des protocoles dits “hybrides“ qui utilisent à la fois les protocoles proactifs et les protocoles réactifs [6][13][10][9].

La figure ci-dessous présente une classification des protocoles de routage pour réseaux Ad-hoc

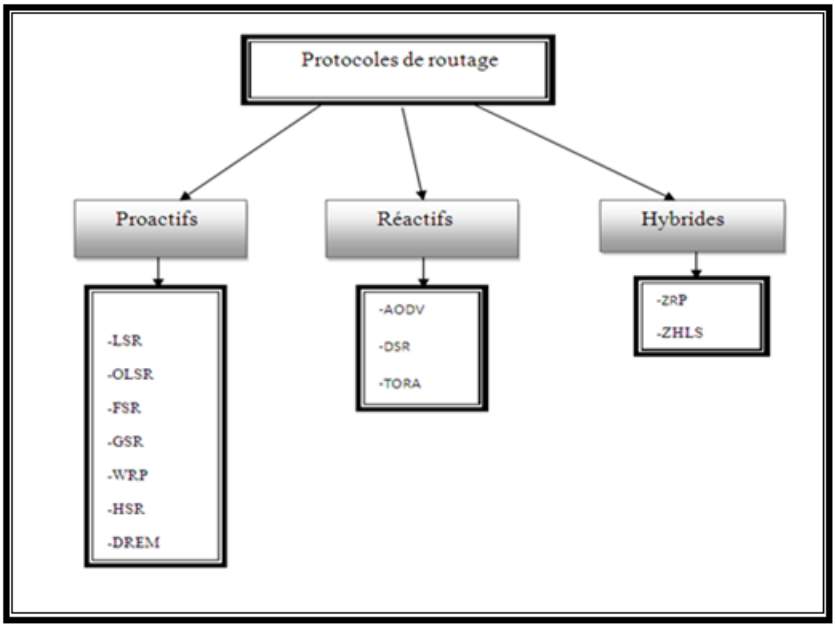

FIGURE 2.2 – Classification des protocoles de routage

2.11.1 Les protocoles de routage proactifs

Un protocole de routage est dit proactif si les procédures de création et de maintenance des routes durant la transmission des paquets de données sont contrôlées périodiquement. Ces protocoles essaient de maintenir les meilleurs chemins existants vers toutes les destinations possibles au niveau de chaque nœud du réseau, les routes sont sauvegardées et active dans quelques tables même si elles ne sont pas utilisées.

La mise à jour permanente de ces derniers est assurée par un échange continu des messages, lorsqu'un nœud reçoit un paquet de contrôle il met à jour ses tables de routages. Ainsi, de nouvelles routes seront construites sur la base des informations topologiques transportées par les trames de contrôle. Ce processus est déclenché aussi à chaque changement de topologie pour reconstruire à nouveau les routes.

Le trafic induit par les messages de contrôle et de mise à jour des tables de routage peut être important et partiellement inutile, ce qui gaspille la capacité du réseau sans fil. De plus, la taille des tables de routage croit linéairement en fonction du nombre de nœuds.

Parmi les protocoles de routages proactifs les plus connus on citera : DSDV, OLSR, FSR, WRP, GSR, HSR, LSR, DREAM...etc [6][13][22].

2.11.2 Les protocoles de routage réactifs

Les protocoles réactifs également appelés protocoles à la demande, se basent sur la découverte et le maintien des routes. Suite à un besoin, une procédure de découverte globale de routes est lancée. Ce processus s'arrête une fois la route trouvée ou toutes les possibilités sont examinées. Dès que la communication est établie, cette route est maintenue jusqu'à ce que la destination devienne inaccessible ou jusqu'à ce que la route ne soit plus désirée.

Ces protocoles peuvent être classifiés en deux catégories : routage source et routage saut-par-saut(voir l'annex 1). Dont les protocoles à routage source, les paquets de données portent dans leurs entêtes les adresses de tous les nœuds constituant le chemin à partir de la source jusqu'à la destination. De ce fait, les nœuds intermédiaires acheminent les paquets selon les informations qui se trouvent dans l'entête de chaque paquet de données. Cela veut dire que les nœuds intermédiaires n'ont pas besoin de maintenir des informations sur les chemins actifs.De plus, ils n'ont pas besoin de maintenir la connectivité avec leurs voisins.

Dans le routage saut-par-saut chaque paquet de données porte uniquement l'adresse de la destination et celle du saut prochain. De ce fait, chaque nœud intermédiaire utilise sa table de routage pour acheminer chaque paquet de données.

Le trafic de contrôle des protocoles réactifs est réduit, les nœuds du réseau ne génèrent aucun trafic de contrôle sans qu'il soit nécessaire. Ceci permet de réduire la charge du trafic dans le réseau.

Parmi les protocoles basés sur ce principe on cite : DSR, AODV, TORA..etc [22][23][24].

2.11.3 Les protocoles de routage Hybrides

Les protocoles de routage hybrides combinent les deux approches de routage réactif et proactif. Le routage à l'intérieur des zones est assuré par un protocole de routage proactif alors que le routage entre les zones est assuré par un protocole de routage réactif.

Ils utilisent un protocole proactif, pour apprendre le proche voisinage, ils disposent des routes immédiatement dans le voisinage. Au delà de cette zone prédéfinie, le protocole hybride fait appel aux techniques des protocoles réactifs pour chercher des routes. Avec ce découpage, le réseau est partagé en plusieurs zones, et la recherche de route en mode réactif peut être améliorée.

A la réception d'une requête de recherche réactive, un nœud peut indiquer immédiatement si la destination est dans le voisinage ou non, et par conséquent savoir s'il faut diriger la requête vers les autres zones sans déranger le reste de sa zone.

Il existe plusieurs protocoles hybrides on citera : ZRP et ZHLS [6][12][19].

2.12 Conclusion

Dans la première partie de ce chapitre, nous avons introduit le concept des réseaux ad hoc et les caractéristiques inhérentes à ces réseaux et domaines d'application. Dans la deuxième partie, un aperçu général sur le routage ad hoc en présentant quelques protocoles de routage les plus connus dans ce domaine et une classification pour ces protocoles existant.

Le prochain chapitre portera sur la notion de sécurité et les attaques ciblant les protocoles de routage et les solutions proposées pour les résoudre.

Chapitre 3

Sécurité des réseaux mobiles ad hoc

3.1 Introduction

La sécurité est un enjeu pour le déploiement des réseaux sans fil, qui de part leur nature, souffrent encore aujourd'hui de plusieurs problèmes.L'absence d'infrastructure centralisée dans les réseaux ad hoc soulève de nombreux problèmes de sécurité qui les rend susceptible aux différents attaques. Ces attaques peuvent parvenir par n'importe quelle station puisque toutes ces derniers se déplacent indépendamment, sont susceptibles d'être contournés et obtenus par les attaquants. Ce type de réseaux hérite à la fois des problèmes de sécurité des réseaux câblés et aussi ceux des réseaux sans fil .

Ces Problèmes sont dûs essentiellement à l'environnement sans fil et à la nature de ces réseaux, protocoles de routage.

3.2 Définition de la sécurité

La sécurité est un ensemble de techniques assurant que les ressources d'un système d'information d'une organisation donnée sont utilisées uniquement dans le cadre ou il est prévu qu'elles le soient [6].

3.3 Objectif de la sécurité

Les principaux objectifs de sécurité pour les réseaux Ad-hoc sont regroupés par :

- **Confidentialité des données**

La confidentialité consiste à refuser l'accès aux informations échangées entre deux nœuds dans le réseau par tout nœud malveillant ou non désiré. Son principe est d'assurer que seuls les acteurs de la transaction sont en mesure de comprendre les données secrètes échangées.

Des contrôles d'accès stricts doivent être mis en place pour garantir la confidentialité des données [25][26].

- **Intégrité des données**

C'est un service qui garantit que les données échangées n'ont pas été altérées durant leur transit dans le réseau de manière volontaire ou accidentelle contre toute modification ou altération par une personne non autorisée [6][26][27].

- **L'authentification de l'origine des données**

Dans un réseau, un adversaire peut facilement injecter des paquets additionnels, ainsi le récepteur doit s'assurer que les données reçues proviennent effectivement de la source supposée pour assurer que la communication entre ces derniers se fais d'une manière authentique [3][24].

- **Disponibilité**

La disponibilité garantit le fonctionnement en permanence des services et garantit l'accès des usagers à ces services.
Son principe permet de s'assurer que les services réseau désirés sont toujours disponibles même à la présence des attaques, le système qui assure la disponibilité dans un réseau ad hoc cherche à combattre les dénis de service et les nœuds qui se comportent mal tels que les nœuds égoïstes [6][25][26]

- **Le non répudiation de l'origine**

C'est un mécanisme destiné à prévenir que la source ou la destination désavoue ses actions ou nier l'envoi ou bien la réception d'un message [6][24][25].

- **La fraîcheur de données**

Garantir que les données présentes échangées sur le réseau sont viables. Ce service permet de lutter contre la réinjection d'anciens messages interceptés par un attaquant et de garantir que les données échangées sur le réseau sont actuelles [24][27].

3.4 Les mécanismes de sécurité

Un mécanisme de sécurité est un processus conçu pour détecter, prévenir ou réparer le réseau suite à des attaques ou des intrusions.
Il peut être indépendant de tout protocole ou être mis en ouvre de façon spécifique.

• La cryptographie

La cryptographie est la science d'écriture et de lecture de messages codés , elle joue un rôle essentiel dans toutes les communications sécurisée en chiffrant un message dit « texte clair » en un deuxième dit « texte crypté » à l'aide d'une clé en utilisant des moyens, matériels ou logiciels conçus à cet effet.

Les informations originales sont restituées à partir de celles codées. Cette opération inverse est nommée décryptage.

La cryptographie est un traitement fait sur une donnée qui sera transmise à un destinataire à travers un canal peu sur en présence d'adversaires. Le défi est que cette donnée atteigne sa destination sans qu'elle soit modifiée et espionnée [6].

• Les fonctions de Hachage

La fonction de hachage est une fonction permettant d'obtenir un condensé, appelé aussi empreinte, de longueur fixe à partir d'un texte de longueur arbitraire finie. Elle doit être telle qu'elle associée à un seul condensé à un texte en clair.

Cela signifie que la moindre modification du texte entraine la modification de son condensé. D'autre part, il doit agir d'une fonction facilement calculable et à sens unique afin qu'il soit impossible de retrouver le message original à partir du condensé. En expédiant un message accompagné de son haché, il est possible de garantir l'intégrité d'un message. C'est-à-dire le destinataire peut vérifier que le message n'a pas été altéré durant la communication [6].

• La signature numérique

La signature numérique est définie comme des « données ajoutées à un message », ou transformation cryptographique d'un message, permettant à un destinataire d'authentifier l'auteur d'un document électronique, garantir son intégrité et de le protéger contre la contrefaçon [6].

- **Vérification du Certificat Electronique**

Un certificat est un élément d'information qui prouve l'identité du propriétaire d'une clé publique, sont signés et transmis de façon sécuritaire par un tiers de confiance appelé autorité de certification.Lorsqu'un utilisateur désire communiquer avec un autre il lui suffit de se procurer le certificat du destinataire.

Il est donc possible de vérifier la validité du certificat en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière et en comparant ces deux résultats [6].

3.5 Les Attaques dans les réseaux Ad hoc

Le réseau Ad hoc est un environnement hostile qui est soumis à des attaques de différents types et dûe à la nature du réseau et ses spécificités la sécurité présente un véritable défi.

Un attaquant peut effectuer une variété d'attaques n'ayant pas forcément le même objectif ou motivations. Ainsi le choix d'une stratégie de sécurité doit se baser sur une modélisation de l'attaque, ceci afin d'éviter un déploiement excessif de moyens de protection conduisant à des solutions irréalistes [25][27].

3.6 Classification des attaques dans les réseaux ad hoc

Les attaques sont classifier selon plusieurs critères, Ceci est illustré dans la figure suivante

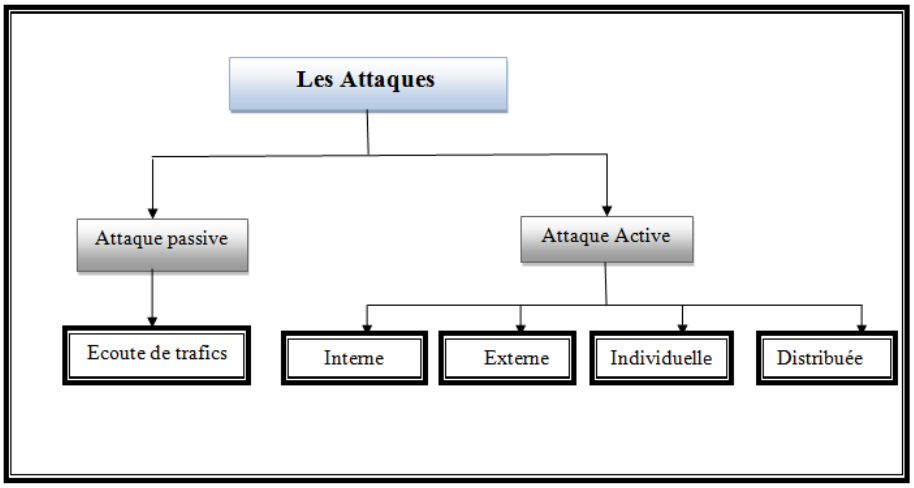

FIGURE 3.1 – Classifications des attaques dans les réseaux Ad-Hoc

3.6.1 Attaque Passive ou Active

- **Attaque Passive**

Les attaques passives se limitent à l'écoute et l'analyse du trafic échangé, une écoute se produit lorsqu'un attaquant capture un nœud et étudie le trafic qui le traverse sans en altérer le fonctionnement .Ce type d'attaques est plus facile à réaliser et difficile à détecter puisque l'intrus n'apporte aucune modification sur les informations échangées.

L'intention de l'intrus peut être la connaissance des informations confidentielles des utilisateurs ou bien la connaissance des nœuds importants dans le réseau, en analysant les informations de routage, pour se préparer à une attaque active. Un adversaire passif ne fait que menacer la confidentialité des données [6][24][25].

- **Attaque active**

Une attaque est active lorsqu'un nœud non autorisé altère des informations de routage en transit par des actions de modification, suppression, ou fabrication, ce qui conduit à des perturbations dans le fonctionnement du réseau. L'intrus peut aussi injecter son propre trafic ou rejouer d'anciens messages pour perturber le fonctionnement du réseau ou provoquer un déni de service [27][28].

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 Interne : Les attaquants internes sont des nœuds faisant légitimement partie du réseau, sont considérée comme la plus dangereuse du point de vue sécurité et

menées par des nœuds compromis qui sont autorisés à participer au fonctionnement du réseau.

Puisque l'attaquant qui capture un nœud, peut lire sa mémoire et avoir accès à son matériel et par conséquent peut s'authentifier comme un nœud légitime et émettre des messages aléatoires erronés sans qu'il soit identifié comme intrus, puisqu'il utilise des clés valides [6][25][27].

- Attaque Externe : Les attaquants externes sont réalisés par des nœuds qui n'appartiennent pas au domaine du réseau, seuls les nœuds ayant les autorisations nécessaires pourront accéder au réseau ou déchiffrer le contenu .

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 [6][29].

- Attaque individuelle ou attaque distribuée : Les attaques peuvent être de type individuelles ou par collusion ou appelée également distribuée :

Attaque individuelle : 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 [6].

Attaque Distribuée : Attaques distribuées 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 [6][25].

3.7 Les attaques liées aux protocoles de routages

3.7.1 Attaques par suppression des paquets

Dans ce type d'attaque, l'intrus supprime tous ou certains paquets. On peut trouver :

• Attaques Trou noir (Black holes)

Dans une attaque du trou noir, 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.

Le principe est d'insérer un nouveau nœud ou bien compromettre un nœud du réseau pour obliger un maximum de voisins à modifier leurs tables de routage et faire transiter leurs données émises par ce nœud malicieux pour les obliger à faire passer l'information par lui. Les informations reçues par ce dernier seront détruites et ne seront jamais réinsérées sur le réseau.

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. Le trafic absorbé peut être donc soit redirigé vers un autre nœud soit disparaître complètement.

La figure 3.2 représente un trou noir mis en place par un nœud malicieux X qui a modifié le routage pour que les clusters 1, 2, 3 et 4 fassent passer l'information par lui pour communiquer entre clusters. Dans ce cas de figure, le trou noir X ne retransmettra aucune information, empêchant toute communication entre les différents clusters [6][30][31].

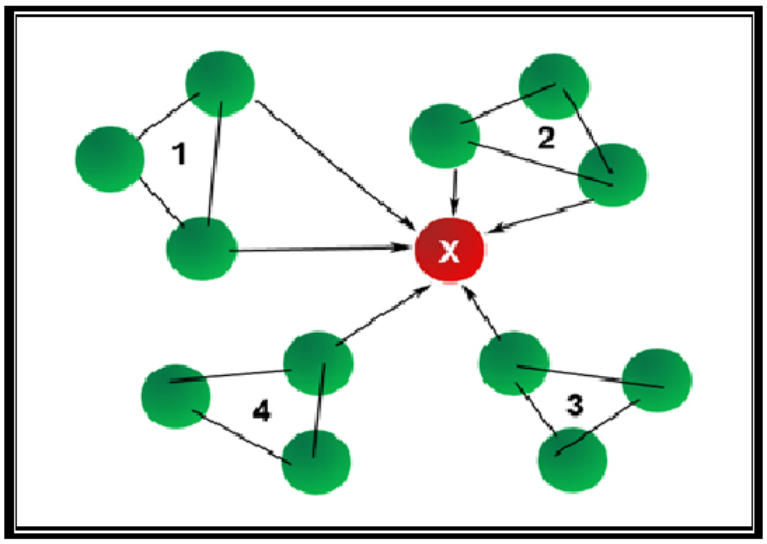

FIGURE 3.2 – Attaque Trou noir

- **Attaques Trou gris (Gray holes)**

L'attaque du trou gris est une variante améliorée de l'attaque du trou noir dans lequel l'attaquant supprime les paquets de données et transmet ceux de contrôle.

Contrairement au trou noir, le trou gris relaye certaines informations. Ce type d'attaque est ainsi plus difficile à détecter que l'attaque du trou noir, le capteur malicieux tant qu'il se comporte de manière normale ne peut être détecté.

Tout comme le principe de Blackhole, Greyhole attack procède à la modification des tables de routage des nœuds du réseau par l'insertion d'un nouveau nœud ou la compromission d'un nœud du réseau, mais à la différence que les informations récupérées par l'attaquant du trou gris ne seront pas toutes détruites et quelques informations non critiques seraient acheminées correctement. Ce comportement semble normal aux autres nœuds du réseau d'où la difficulté de sa détection [6][29][31].

- **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. (figure 3.3)

L'attaque du trou de ver est une attaque particulièrement difficile à contrer. Elle peut être lancée par un attaquant externe et être réussie même en présence d'un système d'authentification et de chiffrement.

Une version simple de cette attaque est de faire croire à deux de ses voisins qu'ils sont eux aussi voisins en relayant leurs paquets. Une version plus élaborée de cette attaque nécessite la présence d'au moins deux nœuds malveillants formant une collusion et se trouvant généralement dans des zones géographiquement séparées. Le but de cette version de l'attaque est de former un tunnel entre ces deux nœuds. Ce tunnel est construit de telle sorte que chaque paquet capturé à l'une des extrémités du tunnel soit relayé, à travers ce tunnel, vers le deuxième attaquant se trouvant à l'autre bout du tunnel en ignorant les nœuds intermédiaires [6][30].

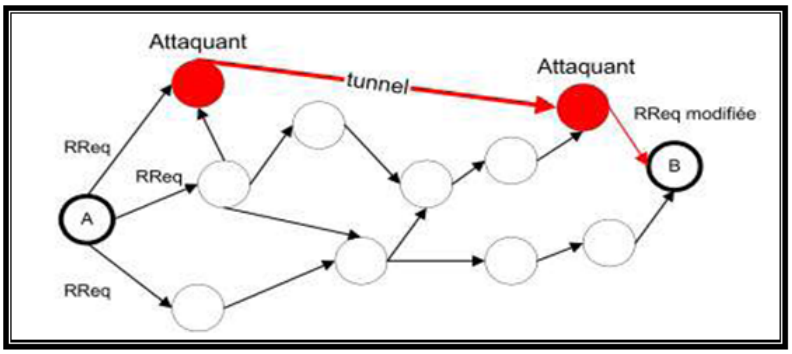

FIGURE 3.3 – Attaquede trou de ver

3.7.2 Attaques par modification des informations de routage

En absence de contrôle d'intégrité sur les messages transmis, un nœud malicieux peut rediriger le trafic vers lui ou causer un déni de service, simplement par la modification de certains champs de paquets de contrôle utilisés par les protocoles de routage dans le but de les tromper ces modifications peuvent concerner plusieurs informations de routage telles que les numéros de séquence ou le nombre de sauts.

Le nœud malhonnête peut jouer sur le numéro de séquence de la destination et/ou le nombre de saut dans une RREP en augmentant le premier et en diminuant le second. Ces paramètres sont pris en compte lors de la mise à jour du chemin vers la destination : une mise à jour est possible si le numéro de séquence reçu dans la demande de route est plus grand que celui stocké dans la table de routage ou les numéros de séquence sont égaux et le nombre de sauts reçu est plus petit que celui stocké dans la table de routage. Cette intervention permet de garder le chemin qui passe par le nœud malhonnête même si un autre chemin plus court est proposé par un autre nœud.

Dans cette attaque, l'intrus tente de convaincre l'expéditeur que le lien faible est fort ou qu'un nœud mort est vivant. Par conséquent, tous les paquets qui passent par ce lien ou ce nœud seront perdus [24][28][29][30][32].

3.7.3 Attaques par usurpation d'identité

Dans cette attaque, le nœud présente des identités multiples aux autres nœuds du réseau, créant ainsi des inconsistances dans les tables de routage des nœuds voisins. L'objectif de cette attaque est de faire passer le nœud malicieux pour plusieurs nœuds en lui endossant plusieurs identités, ce qui permet de créer plusieurs routes passant par ce nœud, qui ne sont en réalité qu'un seul chemin pour pouvoir lire et transmettre des messages en utilisant les coordonnées de sa victime[3][30][31] .

3.7.4 Attaques par fabrication des messages

A la réception d'une demande de route, les attaques par fabrication peuvent être effectuées sans avoir reçu de messages de contrôle, un nœud malicieux ajoute un nombre de nœuds virtuels au chemin durant la phase de découverte de route, le cout de ce chemin serait élevé et le trafic serait dirigé vers d'autres routes qui présentent un cout minimal. Il peut fabriquer un message d'erreur de route et déclarer autant de routes non-joignables ou des messages de mise à jour afin d'épuiser les ressources des autres nœuds ou de perturber le réseau [32][33].

3.8 Conclusion

Dans ce chapitre, nous avons présenté quelques attaques et leur classification dans les MANET et les attaques liées aux protocoles de routage qu'on a cité dans le chapitre précédant et nous avons montré comment ces attaques peuvent perturber le fonctionnement du réseau et dégrader ces performances.

Le prochain chapitre portera sur les solutions proposées pour lutter contre ce type d'attaque et problème de sécurité de routage dans les réseaux mobiles ad hoc.

Chapitre 4

Etude de l'attaque choisie

4.1 Introduction

La nature dynamique des réseaux ad hoc, les rendent plus vulnérables aux attaques de sécurité par apport aux réseaux fixes. Cependant il s'avère difficile de garantir la sécurité dans un réseau ou le medium de communication est ouvert et une autorité centrale de certificat est absente, et cela facilite l'interception, la modification ou même la fabrication des paquets pour l'injecter dans le but de perturber son fonctionnement ou le rendre non opérationnel.

La principale fonctionnalité des réseaux ad hoc est l'opération de routage. Elle contrôle et gère le trafic des messages dans le réseau son objectif principal est l'établissement d'un chemin entre une paire de nœuds de sorte que les messages puissent être acheminés, il permet aux nœuds de se connecter directement les uns aux autres pour relayer les messages par des sauts multiples.

Lors de la transmission d'un paquet d'une source vers une destination, il est nécessaire de faire appel à un protocole de routage qui acheminera correctement le paquet par le «meilleur » chemin. Plusieurs protocoles ont été proposés au niveau ad hoc. Afin de comprendre leur comportement dans des réseaux mobiles, nous nous sommes intéressés :

- 1ère étape : une étude théorique sur le protocole AODV, qui suppose que les nœuds sont dignes,

- 2éme étape : faire le choix d'une attaque sur ce protocole et lui trouver ensuite une solution pour l'éliminer ou bien pour l'éviter ou la supprimer.

4.2 Le choix de protocole

Certaines optimisations des protocoles réactifs ont été développées afin d'optimiser la connaissance des chemins ; ce sont des protocoles plus récents proposés dans le but d'assurer le service du routage dans les réseaux sans fil.

Dans cette catégorie de protocoles, la découverte d'un moyen d'acheminement des messages ne se font que lorsqu'un nœud désire communiquer avec un autre. La découverte de chemin se fait donc à la demande. Grace à cette méthode, les nœuds du réseau ne génèrent aucun trafic de contrôle sans qu'il soit nécessaire.

Ce choix se justifie par le fait que les protocoles de routage réactifs fonctionnent mieux que les protocoles proactifs car ils minimisent le trafic de contrôle.

La majorité des solutions proposées pour résoudre le problème de routage dans les réseaux ad hoc, appartiennent à cette classe de protocoles de routage. Elle créent et maintiennent les routes selon les besoins.
Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et cela dans le but d'obtenir une information spécifique, inconnue au préalable. Parmi les protocoles basés sur ce principe on cite un qui est plus connu est l'AODV [8][23][35] .

4.3 Le protocole AODV

AODV est un protocole réactif qui signifie que les routes sont construites à la demande.

Il maintient les chemins d'une façon distribuée en gardant une table de routage au niveau de chaque nœud appartenant au chemin de transit. Quand une application a besoin d'envoyer un flot de paquets dans le réseau et qu'une route est disponible dans la table de routage, AODV ne joue aucun rôle et s'il n'y a pas de route disponible, le protocole a pour tâche de trouver la meilleure route.

Le protocole AODV est basé sur l'utilisation des deux mécanismes

- Découverte de route.

- Maintenance de route.

Il utilise trois types de paquets de routage : RREQ, RREP, RERR [32][33][37] .

4.4 Gestion de la table de routage

AODV maintient une table de routage qui contient des informations utiles à l'acheminement des paquets, il utilise trois types de paquets de routage :

4.4.1 Demande de route RREQ (Route REQuest)

C'est le message d'interrogation des routes disponibles qui est diffusé lorsqu'un nœud détermine qu'il a besoin d'une route vers une destination et ne dispose pas d'une route disponible. C'est le cas lorsque la destination est inconnue ou lorsqu'une route précédemment valide dans sa table de routage expire ou est marquée invalide.

Source	Num.seq Source	Broadcast id	Destination	Num.seq Destination	Nombre de saut

TABLE 4.1 – Réponse de route RREQ

– ID : Un numéro de séquence identifiant de manière unique une demande de route lorsqu'il est associé à l'adresse de la source (@Src).
– D : Adresse IP de la destination à laquelle une route est demandée.
– SND : Le dernier numéro de séquence connu pour la destination.
– Src : Adresse IP de la source (nœud qui a initialisé la demande de route).
– SNS : Numéro de séquence actuel de la source qui sera associé à l'entrée de la table de routage dans les nœuds traitant le message RREQ [16][40].

4.4.2 Réponse de route RREP (Route REPly)

C'st le message indiquant au demandeur les routes disponibles. Lorsqu'une demande de route atteint la destination ou un nœud ayant un chemin valide vers la destination, celui-ci génère une réponse de route qui sera envoyé d'un nœud à un autre jusqu'à atteindre la source.

Source	Destination	Num.seq Destination	Nombre de saut	Life time

TABLE 4.2 – Réponse de route RREP

– D : Adresse IP de la destination à laquelle une route est demandée.
– SND : Numéro de séquence de la destination.
– Src : Adresse IP de la source, nœud qui a initialisé la demande de route RREQ.
– LifeTime : Temps en millisecondes pour lequel les nœuds recevant la RREP et ils considèrent la route valide [16][40].

4.4.3 Erreur de route RERR (Route ERRor)

Il indique une route erronée. Une erreur de route est envoyée à chaque fois que la rupture d'un lien rend inaccessible l'accès à une ou plusieurs destinations [19][42].

4.5 Les mécanismes d'AODV

Le mécanisme de routage dans AODV est constitué de deux parties : découverte et maintenance de route dont le principe est :

4.5.1 Découverte de route

Le processus de découverte de route est lancé lorsqu'un nœud sollicite un nœud destinataire, il vérifie d'abord sa table de routage s'il y a un chemin préexistant vers ce nœud destination ; alors il l'utilise pour envoyer le paquet.

Lorsque la source possède une route active vers la destination désirée, elle commence directement l'envoie de ses paquets de données vers cette destination, elle envoie à ses voisins une demande de route RREQ qui contient un identifiant (RREQ-ID) associé à l'adresse de la source qui servira à identifier de façon unique une demande de route.
Le nœud source enregistre cet identifiant de paquet RREQ dans son historique et l'associe à un timer qui décomptera sa durée de vie au delà de laquelle cette entrée sera effacée.

La source attendra une période "RREP-WAIT-TIMEOUT", si une réponse est reçue ; alors l'opération de découverte de route est terminée. Sinon, elle rediffuse une autre requête RREQ et attend une période plus grande si aucune réponse n'est reçue ; elle continuera la rediffusion jusqu'à un nombre maximum de fois avant de déclarer que la destination injoignable et un message d'erreur est signalé à l'application.

Les nœuds intermédiaires qui reçoivent la RREP vont sauvegarder l'identité de son prédécesseur afin de construire le chemin inverse qui contient :
- L'adresse source, - L'adresse de destination, - Le nombre de sauts, - Un numéro de séquence de destination , - La durée de vie du paquet et qui sera traversé par le paquet de réponse de route RREP et mettre à jour le chemin qui mène à la destination dans leur table de routage et retransmettre en unicast le message vers le nœud suivant en direction de la source sachant que cette information a été obtenue lors du passage de la RREQ.

La réponse RREP passe par la route inverse vers le nœud source S, ainsi chaque nœud sur cette route enregistre une entrée dans sa table de routage local vers le nœud destination avant de renvoyer le paquet. Une fois la source S reçoit le message, elle commence à envoyer les données vers D [32][33][39][41]

Ceci est illustré dans la figure suivante :

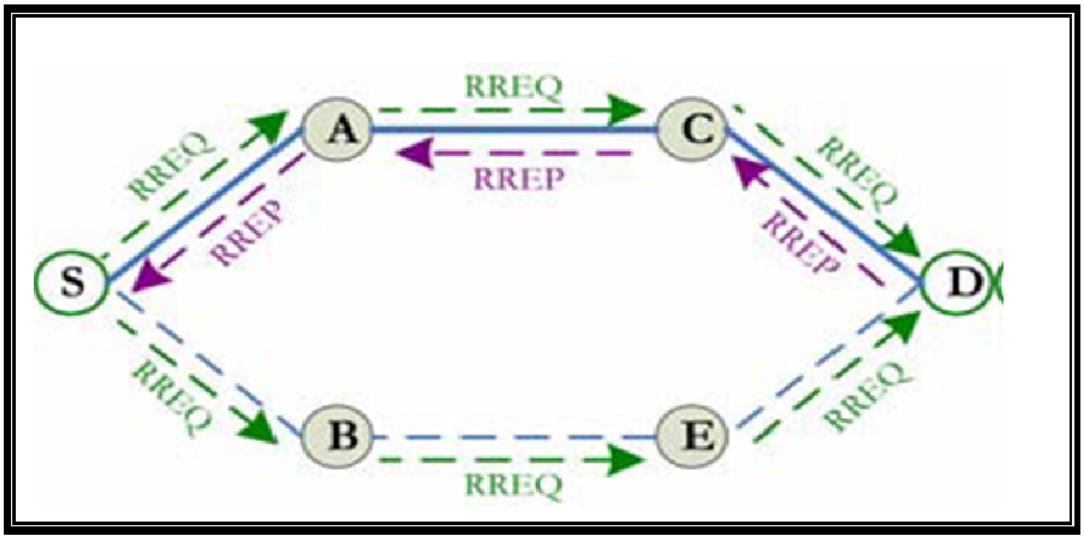

FIGURE 4.1 – Découverte de route dans le protocole AODV

4.5.2 Maintenance de route

Afin de maintenir des routes, une transmission périodique des messages HELLO entre voisins est effectuée pendant que la route est considérée active. Le lien entre deux nœuds voisins sera considéré comme défaillant dans le cas où trois messages "HELLO" ne sont pas reçus respectivement à partir de ces nœuds et il n'a pas reçu un message de contrôle autre que ce dernier pendant une certaine période de temps.
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.

Une fois le message HELLO reçu, la source initie un processus de découverte de chemin et tous les nœuds appartenant au chemin de retour ; et mettent à jour des liens dans leurs tables de routage. Ce message cherche toutes les routes qui passent par le nœud voisin et les détruit avant d'annoncer à ses voisins que la route passant par l'autre nœud n'est plus valide.

Les mouvements des nœuds qui ne participent pas dans le chemin actif n'affectent pas la consistance des données de routage. Une valeur de numéro de séquence égale à l'ancienne valeur du paquet RREP incrémentée de un, une valeur infinie de la distance.

Si le processus est échoué, le nœud destinataire envoie un paquet RERR vers sa liste des précurseurs qui le transmet aux voisins actifs jusqu'à ce qu'il arrive à la source saut-par saut ; et le nœud source initie une nouvelle procédure de recherche de route vers la

destination. Une fois reçu, la source peut relancer une nouvelle requête de découverte de route [7][35][37][39][41] .
Ceci est illustré sur la figure suivante :

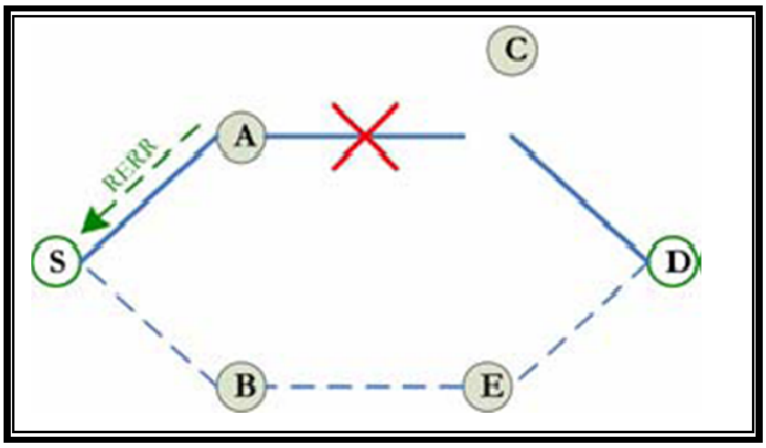

FIGURE 4.2 – Maintenance de route dans le protocole AODV

4.6 Les avantages d'AODV

Des études comparatives montrent que certains protocoles sont plus performants que d'autres selon les caractéristiques du réseau. Ces études ont montré que le protocole AODV semble convenir à des réseaux à forte mobilité et semble performant dans les réseaux de faible densité.

4.7 Description de l'attaque trou noir dans le protocole AODV

Dans le protocole AODV, quand un noud émetteur ne dispose pas d'une route dans sa table de routage vers une destination donnée, il lance une requête de découverte de route par la diffusion de message RREQ, à ce moment là l'attaquant peut intervenir en créant un trou noir dans le réseau. Dans ce qui suit nous allons détailler la présence d'un trou noir dans le protocole AODV [38][41].

4.7.1 Définition de l'attaque de trou noir

L'attaque du trou noir est parmi les attaques les plus connues, c'est le terme qui désigne une attaque dans laquelle un nœud malveillant supprime, ignore où effectue des changements sur tous les paquets qui passent par lui.

Pour mener une attaque, le nœud malicieux doit d'abord s'insérer dans le chemin de bout en bout, puis il supprime le trafic passant par lui. Les paquets de données sont captés et absorbés par le trou noir qui joue le rôle d'empêcher le trafic d'atteindre sa destination. [42][39][40].

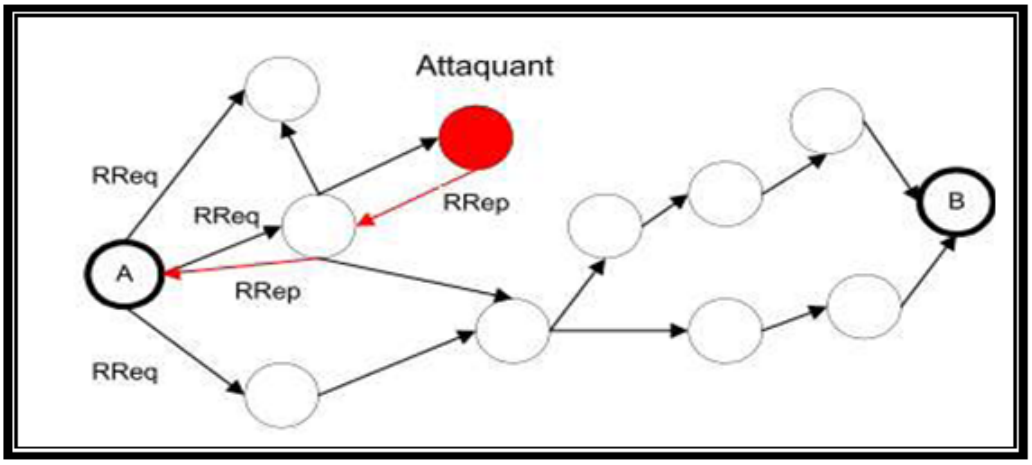

FIGURE 4.3 – l'attaque Black Hole

4.7.2 Spécification de l'attaque de trou noir dans AODV

Cette attaque vise à modifier le protocole de routage, ou le trafic déroulé à travers un nœud spécifique qu'il est contrôlé par l'attaquant et qui a la possibilité de violer la spécification du protocole de routage pour être dans le chemin reliant la source et la destination des données.

Elle peut s'effectuer au moment où un nœud source initie un processus de découverte de route en émettant un paquet RREQ vers les nœuds intermédiaires pour trouver un chemin frais vers la destination ; le nœud corrompu en le recevant va répondre par un paquet RREP avec un numéro de séquence non seulement erroné mais également élevé afin d'augmenter ses chances de faire partie de la route.

Si le paquet RREP atteint la source le premier par rapport aux réponses des nœuds légitimes, il peut ignorer les autres RREP messages des autres nœuds et sélectionner la route à travers le nœud corrompu pour envoyer les paquets et s'intégrer dans la route .Le trafic absorbé peut être donc soit rediriger vers un autre nœud soit disparaître complètement.

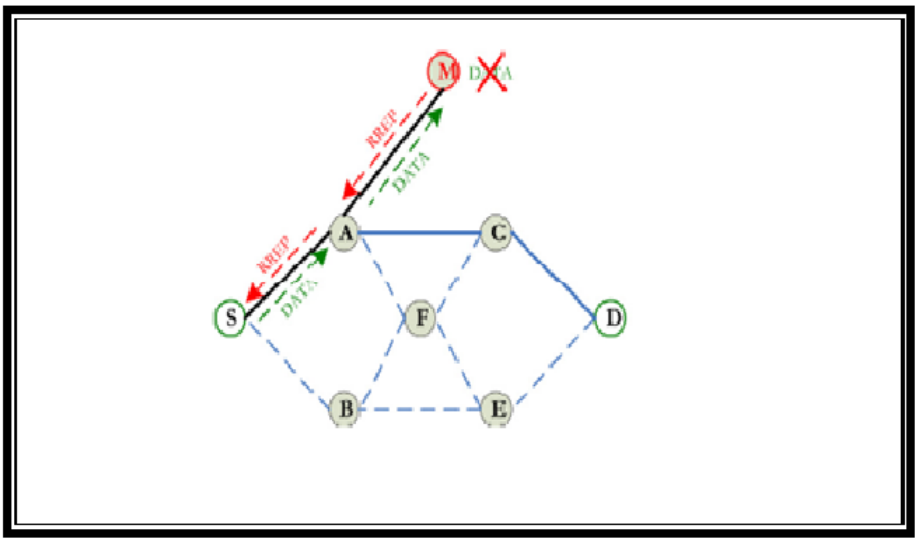

FIGURE 4.4 – Attaque de trou noir dans AODV

La figure ci-dessus montreque, le nœud malicieux M détecte l'existence d'une route active (S ,A,C,D) entre la source et la destination D, M envoie au nœud A un message de route replay (RREP) contenant l'adresse de la destination usurpée, une valeur de numéro de séquence relativement grande et une valeur de compteur de saut relativement petite . Le nœud A achemine ce message RREP à S et ce dernier met à jour sa table de routage. La nouvelle route (S,A,M) sera utilisée par S pour envoyer ses données et en arrivant à M, ces données seront supprimées. En conséquence, les nœuds S et D ne seront plus capables de communiquer en présence de cet attaquant [36][38][39][40][41][42].

4.8 Travaux et solutions proposées pour l'attaque du trou noir

4.8.1 Solutions existantes

Au cours de la recherche bibliographique de ce mémoire, nous avons trouvées plusieurs études sur ce problème ainsi que des solutions proposées que nous les résumons dans les paragraphes suivants :

Deng et al [51] ont proposé une solution contre l'attaque du trou noir en modifiant le protocole AODV. Dans cette méthode chaque nœud intermédiaire doit inclure l'information« next hop » quand il envoie un paquet RREP.

Une fois la source a reçu le paquet RREP et avant d'envoyer les paquets de données, il extrait l'adresse du « next hop » et lui envoie une nouvelle demande de route (Fur-

therRequest) ;ceci, afin de vérifier qu'il possède une route vers le nœud intermédiaire qui a envoyé le message de réponse.
La source vérifie les informations des paquets FRREP et agit selon les règles suivantes :
1) Si le « next hop » possède une route vers le nœud intermédiaire et la destination, la source établit la route reçu du nœud intermédiaire et commence l'envoi des données.

2) Si le « next hop » a une route vers la destination, mais n'a pas de route vers le nœud intermédiaire, la source suppose que le nœud intermédiaire est un nœud malicieux. Ensuite, elle initie l'envoi des données via la nouvelle route à travers le next hop et diffuse un message d'alarme dans le réseau afin d'isoler le nœud malveillant.

3) Si le « next hop » n'a pas de routes vers le nœud intermédiaire et la destination, la source lancera un nouveau processus de découverte de route, et envoie également un message d'alarme afin d'isoler le nœud malveillant.

Le mécanisme proposé est efficace dans la détection de l'attaque Blackhole, cependant, l'envoi d'un paquet FRREQ à partir du nœud source vers le « next hop» et l'attente du paquet FRREP du « next-hop » augmente la charge du routage « overhead » entre la source et le « next hop », surtout quand ce mécanisme est appliqué sur un réseau à grande échelle et la distance entre la source et le nœud malicieux est longue .

Al-Shurman [49] ont proposé deux solutions conçues pour cibler l'attaque BLACKHOL dans le protocole AODV.

- La première solution proposée consiste à trouver plus d'une route vers la destination (au moins trois routes différentes). La source envoie un paquet RREQ au nœud destinataire en utilisant ces trois routes. La destination, le nœud malicieux et les nœuds intermédiaires vont répondre à ce paquet.

Le nœud expéditeur met ses paquets de données dans un tampon jusqu'à ce qu'il reçoit plus d'une réponse RREP ; lorsque la source reçoit ces RREP, si les routes à destination ont des nœuds partagés, la source peut reconnaître une voie sûre vers la destination, et les paquets vont être transmis. Si aucuns nœuds partagés ne semblent être dans ces routes redondantes, l'expéditeur attendra une autre RREP jusqu'à ce qu'un chemin avec des nœuds partagés soit identifié ou le temps d'attente soit expiré.

Cette solution peut garantir à trouver une route sécurisé vers la destination, mais le principal inconvénient est le délai d'attente. Plusieurs paquets RREP doivent être reçues et traitées par la source. En outre, s'il n'y a pas de nœuds partagés entre les routes, les paquets ne seront jamais envoyés.

- La seconde solution proposée exploite le numéro de séquence inclu dans l'en-tête de chaque paquet. Le nœud dans cette situation a besoin d'avoir deux tables supplémen-

taires ; la première table comprend les numéros de séquence du dernier paquet envoyé à chaque nœud dans le réseau et la deuxième table contient le numéro de séquence reçu de chaque expéditeur.

Pendant la phase de réponse de route, le nœud intermédiaire ou la destination doivent inclure le numéro de séquence du dernier paquet reçu de la source qui déclenche la demande de route. Une fois la source reçoit ce RREP, il va extraire le dernier numéro de séquence, puis le comparer avec la valeur enregistrée dans sa table. Si elle correspond, la transmission aura lieu, sinon c'est un nœud malveillant, alors un message d'alarme sera diffusé pour avertir le réseau sur ce nœud.
Toutefois, les deux solutions proposées par **Al - Shurman** ont le délai de bout en bout comme inconvénient [37][42].

La solution proposée par **Houda Hafi** [32] propose un protocole basé sur l'utilisation d'un modèle de confiance capable d'assurer les échanges sécurisés dans les réseaux sans fil P2P.
Afin d'évaluer le degré de confiance d'un nœud, chaque nœud dans le réseau maintient une table d'activité, dans cette table il sauvegarde l'identifiant d'un nœud, le nombre des paquets de données, le nombre des paquets de demande de route(RREQ)et le nombre des paquets de réponse (RREP) reçus de ce nœud.

Quand un nœud légitime reçoit un paquet, selon le type du paquet reçu, il augmente le nombre dans sa table d'activité. Si le paquet reçu est de type RREP, il consulte sa table d'activité pour vérifier quelques équations, selon les valeurs stockées dans cette table, il décide si le nœud est un nœud de confiance ou ne l'est pas.

A chaque fois qu'un nœud BLACKHOLE reçoit un paquet de données, il le supprime directement, ainsi quand il reçoit un paquet RREQ, il répond en envoyant une fausse RREP sans consulter sa table de routage et il ne rediffuse pas le RREQ vers les autres nœuds. En se basant sur ce comportement, un nœud légitime ne recevra aucun paquet de données ou bien un paquet RREQ d'un nœud malicieux, il reçoit que des paquets de réponse RREP .

Dans la même année, **H.A.Esmaili** [54] font une étude sur la performance du protocole de routage AODV sous l'attaque de trou noir, ils proposent l'objectif qui a l'effet de cette attaque sur le réseau ad hoc à l'aide d'AODV comme protocole de routage et définissent une solution pour accroître la sécurité dans ces réseaux, à partir de la problématique : Mobile ad hoc networks sont faible aux nombreux types d'attaques comme l'attaque de trou noir.

Lalit Himral [61] ont proposé une méthode pour trouver les routes sécurisées et prévenir les nœuds malveillants dans les MANET en vérifiant s'il existe une différence importante entre le numéro de séquence du nœud source et celui du nœud intermédiaire

qui a envoyé la première RREP. En règle générale, la première réponse sera celle du nœud malveillant.

Celle-ci sera d'abord stockée comme la première entrée dans RR-table. Ensuite,comparée au numéro de séquence du nœud source, s'il existe une grande différence entre eux, il est certain que cette réponse vient d'un nœud malveillant, par conséquent elle sera immédiatement supprimer de la table.

1) Le nœud malveillant est identifié dans la phase initiale et il est retiré immédiatement.

2) Aucune modification n'est faite dans les autres opérations du protocole AODV.

3) Une meilleure performance en légère modification. Cependant la méthode ne peut pas trouver de multiples nœuds malicieux .

Un algorithme présenté dans **Subash** [59] pour détecter l'attaque du trou noir dans un MANET basé sur un prétraitement appelé Pre-Process-RREP, il est simple ainsi il ne change pas le fonctionnement de l'un des nœuds intermédiaires ou de destination. Il n'a même pas modifié le fonctionnement normal de l'AODV.

Le processus continue à accepter les paquets RREP et appelle un processus appelé Compare-Pkts (p1 paquets, p2 paquet) qui compare le numéro de séquence de destination des deux paquets et sélectionne le paquet avec un numéro de destination supérieur si la différence entre les deux numéros n'est pas sensiblement élevée.

Le paquet contenant exceptionnellement un numéro de séquence de destination élevé est soupçonnée d'être un nœud malveillante un message d'alerte contenant l'identification du nœud est généré et diffusé vers les nœuds voisins de sorte qu'il peut être isolé du réseau et peut maintenir une liste de ces nœuds malveillants .

Dans la même année, **H.A.Esmaili** [54] font une étude sur la performance du protocole de routage AODV sous l'attaque de trou noir, ils proposent l'objectif qui a l'effet de cette attaque sur le réseau ad hoc à l'aide d'AODV comme protocole de routage et définissent une solution pour accroître la sécurité dans ces réseaux, à partir de la problématique : Mobile ad hoc networks sont faible aux nombreux types d'attaques comme l'attaque de trou noir .

Romina Sharma [60] font une étude sur le protocole de routage AODV dans les réseaux mobile Ad hoc, ils proposent de : modifier le protocole de routage AODV pour empêcher l'attaque du trou noir et mesurer l'impact de cette attaque sur les réseaux mobile Ad hoc et le comparer avec le protocole modifie de AODV suivant la problématique : à cause de la vulnérabilité de sécurité des protocoles de routage, les réseaux mobile Ad

hoc ne sont pas protégés de l'attaque du nœud malicieux, telle que l'attaque du trou noir .

Les chercheurs proposent une amélioration du protocole AODV pour lutter contre l'attaque du trou noir coopérative.

Dans ce qui suit, nous introduirons des hypothèses sous lesquelles notre schéma est fonctionnel, et nous détaillerons notre approche de sécurité contre l'attaque du trou noir.

4.8.2 Solution proposée

Dans la plupart des applications des réseaux sans fils, l'emplacement des nœuds sur une zone de captage est souvent bidirectionnel, ce qui maintient régulièrement à jour l'état des liens et les informations de routage stockées sur les nœuds. Nous supposons que les nœuds du réseau aient :

- Une mémoire de stockage suffisante
- Y'a plusieurs chemins reliant un nœud avec ses voisins.

4.8.3 Description de la solution proposée

L'attaque BLACKHOLE comme nous l'avons déjà vu, est une attaque dans laquelle un nœud corrompu utilise la vulnérabilité de route, pour découvrir les paquets.le protocole de routage a pour objectif d'annoncer qu'il a le plus court chemin vers le nœud qui va intercepter les paquets.

Elle peut s'effectuer au moment où un nœud source initie un processus de découverte de route, ou en émettant un paquet RREQ pour trouver un nouveau chemin, quand le nœud corrompu reçoit ce message, il va répondre par un paquet RREP avec un numéro de séquence non seulement erroné mais également élevé par rapport au numéro de la source afin d'augmenter ses chances de faire partie de la route.Ceci est illustrée par la figure :

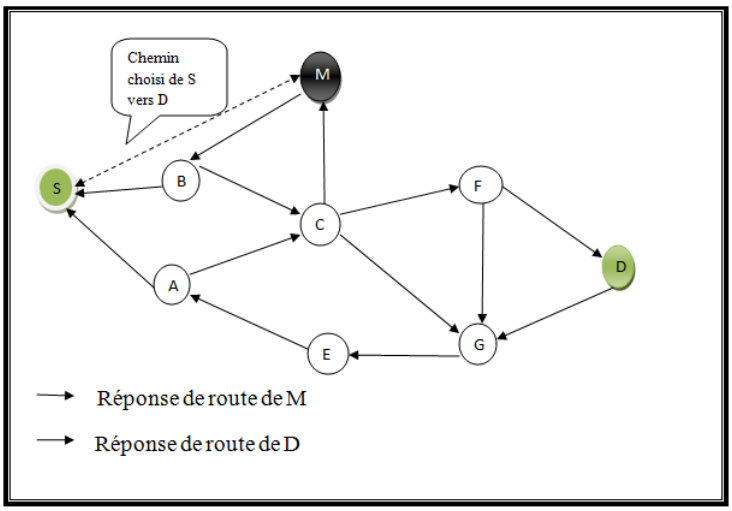

FIGURE 4.5 – Le trou noir répond par un message RREP

En effet, si son paquet RREP atteint la source le premier par rapport aux réponses des nœuds légitimes, il peut s'intégrer dans la route pour intercepter et contrôler une partie ou la totalité du trafic échangé au sein du réseau, de façon à pouvoir surveiller, bloquer ou même détourner certains flux du trafic.
Le trafic absorbé peut être donc soit redirigé vers un autre nœud soit disparaître complètement.

BLACKHOLE consiste à empêcher le trafic de se dérouler à travers un nœud contrôlé par l'attaquant. Ce dernier doit d'abord s'insérer dans le chemin de données ensuite, il repend immédiatement a la source que ces nœuds ne sont pas répertoriés dans sa table de routage.

Le nœud source suppose que le processus de la découverte de la route est complet, alors il ignore les RREP des autres nœuds et sélectionne la route à travers le nœud corrompu pour envoyer les paquets.
Le nœud corrompu fait ça pour assigner un numéro de séquence élevé du paquet de réponse.

L'attaquant efface et supprime les paquets passant par lui ou reçus au lieu de les retransmettre.

Pour éviter ce problème plusieurs solutions ont été proposées pour renforcer la sécurité dans les réseaux ad hoc contre cette attaque, notre approche de sécurité exploite sur :
- Le principe de multi-chemins pour vérifier le bon acheminement des paquets, le long du chemin de bout en bout
- Numéro de séquence.

Dans notre requête contre l'attaque du trou noir, nous nous somme inspiré des propositions citées précédemment, d'où nous avons choisi celle **d' Al-Sherman** et nous avons abouti aux résultats suivants :
L'information à transmettre est découpée au niveau du nœud source en plusieurs paquets REEQ de tailles fixes où chaque requête contient une empreinte de son message, qui est chiffré avec sa clé privée, puis le message et la signature seront envoyés sur des chemins différent,Ceci est illustré par la figure suivante :

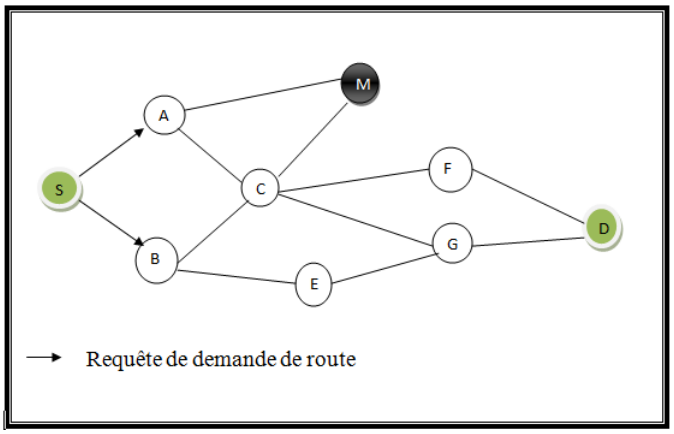

FIGURE 4.6 – Diffusion d'un message RREQ par la source

La destination, le nœud malicieux et les nœuds intermédiaires vont répondre à ce paquet en utilisant la clé publique de la source pour déchiffrer la signature après qu'elle ait recalculé l'empreinte du message et la comparé avec celle reçue.

Si les deux sont différentes alors c'est soit la source qui ne possède pas la bonne clé,ou c'est le message qui a subi des modifications en chemin.

Afin de transmettre intégralement l'information échangée entre la source et sa destination, le nœud expéditeur met ses paquets de données dans un tampon jusqu'à ce qu'il reçoit plus d'une réponse RREP et les traites.
Le nœud qui répond par RREP doit indiquer aussi :

- Le nœud suivant vers la destination,
- La source peut reconnaître une voie sûre vers la destination,
- Les paquets vont être transmis.

Si aucun nœud partagé ne semble être dans ces routes redondantes, l'expéditeur retransmet le message vers les autres voisins et attendra une autre RREP, jusqu'à ce qu'un chemin avec des nœuds partagés soit identifié ou que le temps d'attente soit expiré,Ceci

est illustré par :

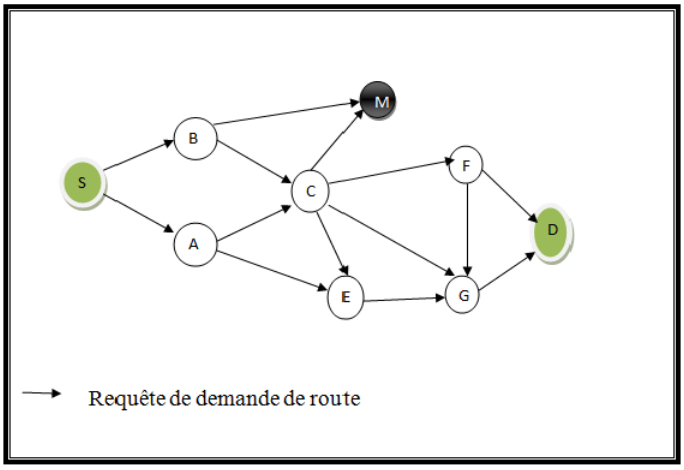

FIGURE 4.7 – Rediffusion de message de demande de route

Quand la source reçoit la réponse du premier nœud voisin, elle va le tester avec l'envoi d'un message de vérification au nœud suivant et elle attend un ACK (clé partagée) pendant un temps fixe ; si ce nœud répond pendant un temps inférieur ou égal au temps fixe, on doit vérifier que c'est le nœud désiré qui a répondu, si cette vérification est positive, le nœud transmet le RREP sinon il va l'ignorer ,ceci est illustré par la figure suivante :

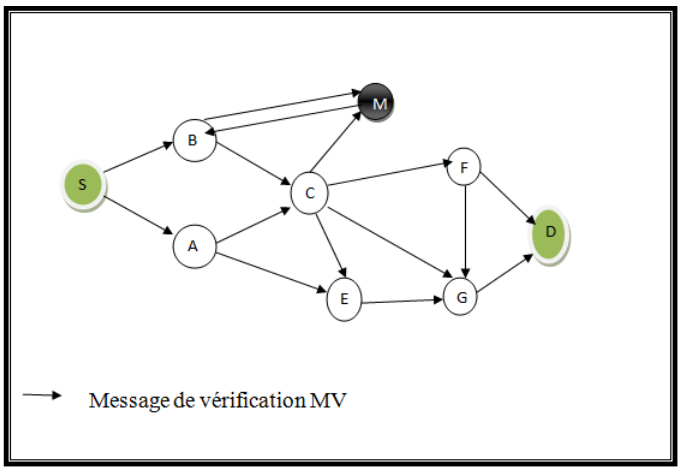

FIGURE 4.8 – Le noeud qui reçoit RREP envoie MV

Pour éviter l'inondation du réseau durant un temps trop long, le système associe à chaque requête un temporisateur TTL "Time To Live". Lorsque cette action ne corres-

pond pas à un résultat attendu, le nœud observateur comptabilise un échec de retransmission et si le nœud ne répond pas à temps le message sera rejeté.

4.9 Conclusion

Dans ce chapitre nous avons étudié le protocole AODV, ses mécanismes et ses différents messages délivrés soit par la source ou le destinataire, et aussi nous avons choisi d'étudier l'attaque de trou noir parmi toutes ces menaces.

Les auteurs ont donné plusieurs propositions pour la détection et la prévention de cette attaque, chacune a ses propres avantages et inconvénients, et à partir de ces solutions nous avons proposé une solution qui a étais une amélioration de l'une des solutions précédentes.
Dans notre solution, nous avons exploité sur :

- Le principe des multi-chemins conjointement avec des acquittements pour s'assurer que le paquet est bien acheminé,
- La surveillance de numéro de séquence ou l'envoie des acquittements pour confirmer la bonne réception des paquets,

Notre solution protège efficacement contre l'attaque de trou noir qui a un grand effet sur le déroulement de réseau à cause de l'environnement ouvert de ces réseaux.

Dans le chapitre qui suit nous avons proposé un modèle de simulation pour l'attaque de trou noire et de mettre le point sur notre protocole proposé et ses performances en utilisant le simulateur NS3.

Chapitre 5

Simulation et Analyse

5.1 Introduction

Pour tester les performances d'une solution apportée à un problème de communication dans un réseau, il n'est pas toujours possible d'accéder aux infrastructures nécessaires en raison de leurs coûts élevés. Rappelons que les réseaux ad hoc sont des réseaux qui englobent plusieurs unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces radio.

En effet, il serait très coûteux voir impossible de mettre en place un réseau à des fins de tests de certains critères. Pour remédier à ce problème et afin de tester les performances d'un nouveau protocole, on a recours à la simulation qui met à la disposition de l'utilisateur un environnement d'expérimentation.

La simulation permet de tester à moindre coût les nouveaux protocoles afin de connaitre leurs comportements dans tous les scénarios possibles et d'anticiper ainsi les problèmes qui pourront se poser dans le futur.

5.2 Présentatio de l'entreprise

Au cours de notre stage effectué à ooredoo (Bab zouar), nous avons pu assimiler la notion de réseau ah doc. Bien que nous voulions voir en réalité la sécurisation de ce réseau , cela nous a été impossible car la sécurité s'effectue au niveau de Oulade Fayet qui est un niveau tres sécurisé.

Comme nous n'avons pas pu faire par nous méme une sécurisation du réseau contre une attaque à l'entreprise, nous avons décider de fair une simulation, ce qui nous a pousser a faire une formation sur un simulateur que nous avons nous même choisit pour pouvoir introduire l'attaque que nous avons étudier et la solution que nous avons proposer.

5.3 Environnement de simulation

5.3.1 Introduction à la simulation

La simulation connait de nos jours un essor considérable. Ceci est du aussi bien à l'intérêt théorique que présente la modélisation des systèmes simulés, que par les besoins croissants de simuler par ordinateur des réalisations de plus en plus complexe. Ses applications sont innombrables.
Dans le cadre de ce travail, l'évaluation de performance du protocole de routage AODV sera abordée par les simulations sous, elle permet de présenter les contextes des simulations et les résultats obtenus pour sécurisé protocole AODV contre l'attaque de blackhole.

5.3.2 Système réel et objectif de simulation

La simulation est une technique de modélisation du monde réel. Elle permet de représenter le fonctionnement d'un système composé de différent centre d'activité, de mettre en évidence les caractéristiques de ceci et les interactions entre eux, de décrire la circulation de différents objets traités par ces processus et en fin d'observer le comportement du système dans son ensemble et dans son évolution dans le temps [15].

5.3.3 Simulateur

Un simulateur un programme qui met en œuvre un modèle de simulation par événements discrets. La tache première d'un simulateur est d'assurer que la chronologie des événements soit respectée. A chaque occurrence d'un événement, les actions qui sont associées à celui-ci sont exécutées [15].

5.3.4 Avantages et inconvénients de la simulation

Les avantages et les inconvénients sont donnés comme suite :

Avantages
- Observation des états du système ;
- Étude des points de fonctionnement d'un système ;
- Étude de l'impact des variables sur les performances du système ;
- Étude d'un système sans les contraintes matérielle.

Inconvénients
- La conception de modèle peut nécessiter des compétences spéciales ;
- Résultats pas forcément généralisable [15].

5.3.5 Choix du simulateur

Le choix du simulateur approprié à notre étude s'est fait parmi plusieurs : OMNET++, NS-3, OPNET Modeler ... Ces derniers diffèrent selon leurs caractéristiques à savoir :
• La plateforme sur laquelle ils s'exécutent (Linux, ...).
• Le type de licence d'utilisation (gratuit/payant, propriétaire/open source) .
• Leur compatibilité aux réseaux sans fils.

Afin d'implémenter notre protocole, nous avons utilisé le simulateur NS3 et nous avons effectué plusieurs modifications à plusieurs niveaux, tout d'abord nous avons implémenté l'attaque, puis nous avons intégré le protocole proposé AODV. Nous avons effectué ce choix choisi car il consomme moins d'énergie, il réduit le surcoût de routage et il est plus adaptable aux réseaux dynamiques [32][33].

5.4 Networks Simulator NS-3

5.4.1 Présentation du simulateur NS3

NS-3 est un outil logiciel de simulation à code source ouvert et à événements discrets permettant l'étude, la conception et la gestion des protocoles pour les réseaux informatiques.
Il est écrit en c++ et python,il contient des librairies pour la génération des fonctions (topologie, trafic, routage, ...) et des outils graphiques pour faciliter l'interprétation et la visualisation des résultats.
Pour des informations sur l'installation du NS-3 voir lannexe 2

5.4.2 Composants de la topologie

Un modèle de réseau sous NS se base sur un modèle composé des éléments suivant :

- Nœud : Le nœud est l'entité de communication qui constitue l'élément de base. Sa fonction est de recevoir des paquets, les examiner et les diriger vers ses interfaces sortantes.

- Lieu : Un lien est utilisé pour relier les nœuds. Il est défini par plusieurs paramètres comme : sa bande passante, le point d'entrée, la durée de vie de chaque paquet, etc.

NS-3 présente plusieurs types de liens, ainsi on peut distinguer des liens unidirectionnels ou bidirectionnels, des liens filaires et des liens non filaires pour modéliser les réseaux sans fils.

- Agent : Les agents de communication représentent des points terminaux, là où des paquets de la couche réseau sont construits ou consommés. Ces agents sont attachés aux nœuds et connectés l'un à l'autre, ce qui représente un échange de données pour rôle de fournir l'adresse de destination et les fonctions pour les paquets.

-Application : Les applications génèrent le trafic de données selon certaines lois, et se servent des agents de transport [14][15]

5.4.3 Avantages de NS3

Le Network Simulator offre plusieurs avantages comme :
- 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 fils ;
-Les résultats de simulation sont générés dans un fichier trace que l'utilisateur peut exploiter ;

5.5 Visualisation des résultats sous NS3

5.5.1 Paramètre de simulation

Le tableau (TAB .5.1) contient les paramètres réseau sur lequel les simulations sont été effectuées. Parmi l'ensemble des nœuds qui sont déployés dans un terrain de simulation 400*400, on choisit aléatoirement un seul nœud source qui génère des paquets, de taille 125 bits, selon une loi exponentielle de paramètre 1, pour un seul nœud destinataire choisi aussi aléatoirement. Un seul nœud malicieux qui joue le rôle du nœud qui mène l'attaque de trou noir, est choisi aléatoirement. La simulation a été effectuée dans un réseau qui utilise AODV comme protocole de routage.

Paramétres	Valeurs
Simulateur	NS3
protocole	AODV
Nombres de nœuds	5 noeuds
Nombre de nœuds malicieux	1
Temps de simulation (ms)	125
Temps d'arriver des paquets (sec)	Exponentielle
Taille des paquets ($bits$)	160
Terrain de simulation	400*400

TABLE 5.1 – Paramètres de simulation

5.5.2 Métriques de simulation

Du moment où l'impact du trou noir consiste à empêcher le trafic d'être délivrer à sa destination, nous avons pensé à mesurer le trafic envoyer par la source et celui par la destination ; cela pour savoir si le trou noir a supprimé les paquets qui ont passé par lui.

Donc, les deux métriques choisies sont définis comme suite :
• Trafic envoyé par la source : désigne le trafic (Paquets /sec) envoyé par le hôte source au hôte destinataire.
• Trafic reçu par la destination : désigne le trafic (paquets/sec) reçu par le nœud destinataire.

La simulation consiste à mesurer ces métriques dans les cas :
• Sans l'attaque
• Avec l'attaque et sans l'utilisation de la solution
• Avec l'attaque et l'utilisation de la solution

5.5.3 Déscution des résultats de simulation

Apres la simulation des paramètres nous avons obtenue les résultats suivants :
- Cas sans l'attaque
Apres simulation nous avons obtenu pour ce cas le taux de paquets perdu lors de la transmission des données dans le protocole AODV :

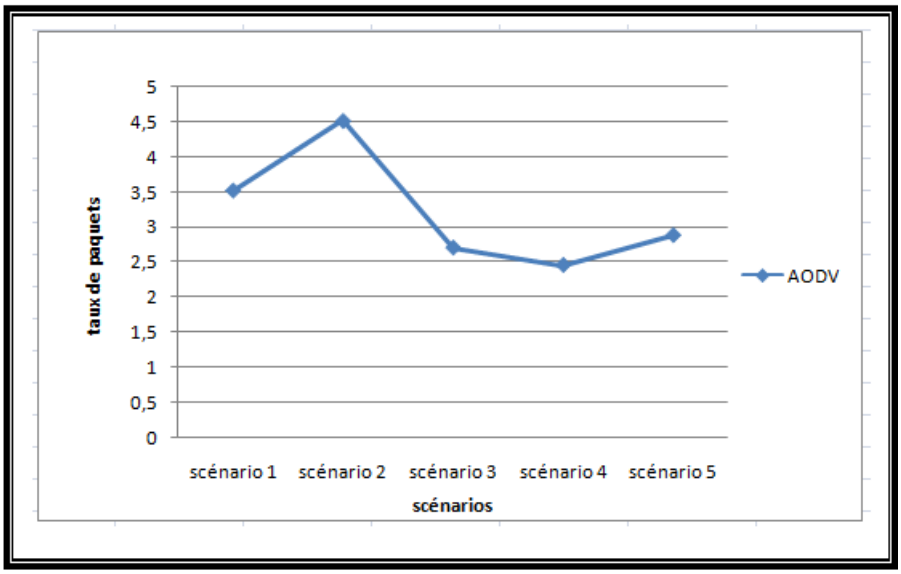

FIGURE 5.1 – Le taux de paquets perdu lors de la transmission des données dans le protocole AODV

La figure ci-dessus illustre le taux de paquets perdu lors de la transmission des données dans le protocole AODV

• **Commentaires :** Le taux de perte des paquets lors de la transmission est très faible cela traduit que le paquet envoyé par la source est presque reçu par la destination ce qui veut dire qu'aucun paquet n'a été supprimer dans ce réseau, ces pertes sont dûs à la mobilité des nœuds.

- Cas avec attaque et sans solution Le scénario de simulation obtenu est représentés comme suit :

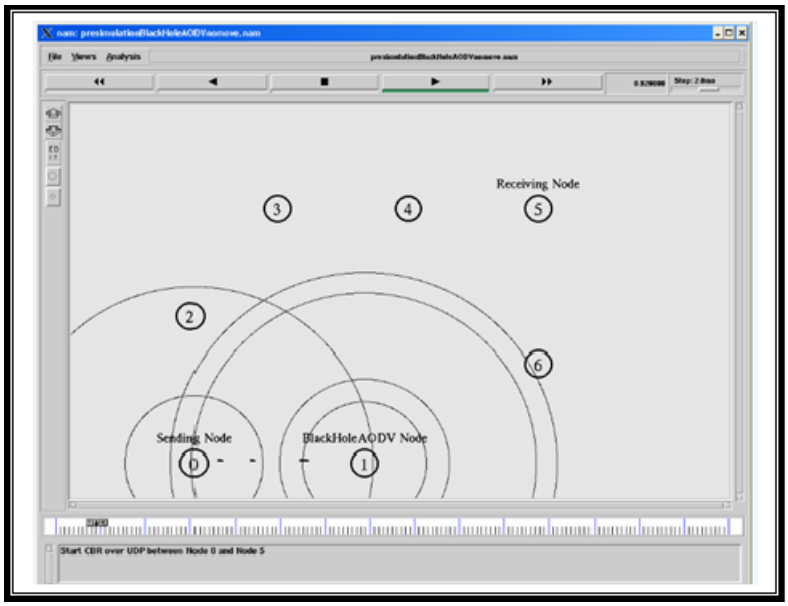

FIGURE 5.2 – Simulation du trou noir

•**Commentaire :** Lors de la transmission des paquets de données du noued source vers le nœud destinataire à travers des nœuds intermédiaires, l'attaque du trou noir s'inséré dans le chemin reliant la source et la destination, vise à capter et à absorber les paquets passant par lui, il va les supprimer et les empêcher d'arriver à la destination.

Les résultats de taux de paquets perdu lors de la transmission dans le protocole AODV avec l'attaque du trou noir sont illustrés comme suit :

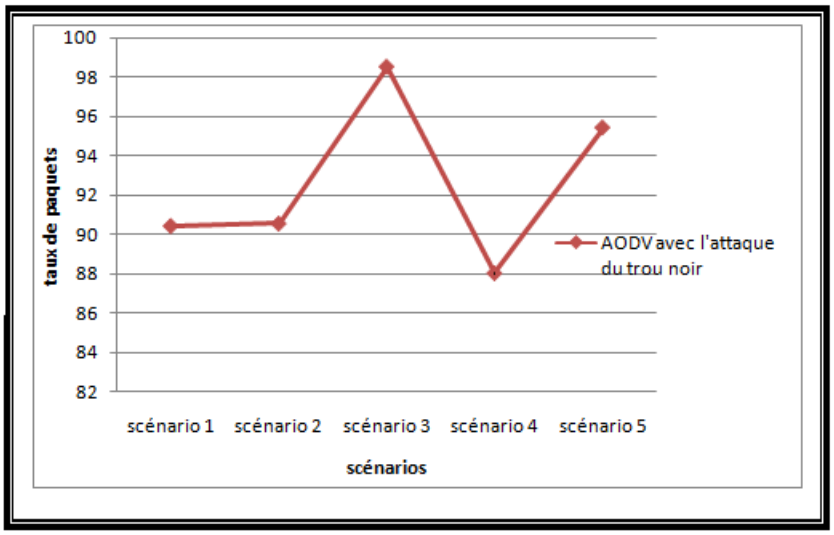

FIGURE 5.3 – Le taux de paquets perdu lors de la transmission dans le protocole AODV avec l'attaque du trou noir

La figure ci-dessus montre le taux de paquets perdu lors de la transmission dans le protocole AODV a cause l'attaque du trou noir.

• **Commentaire :** Durant la période de la simulation, le nœud source a bien généré le trafic mais ce dernier n'est pas été reçu par la destination, ceci a cause du nœud malicieux qui intercepte a chaque envoie les données ce qui empêche ces dernières d'arriver a leurs destination.

- Cas avec attaque et solution

Pour la Simulation de la solution du trou noir nous avons obtenu le scénario suivants :

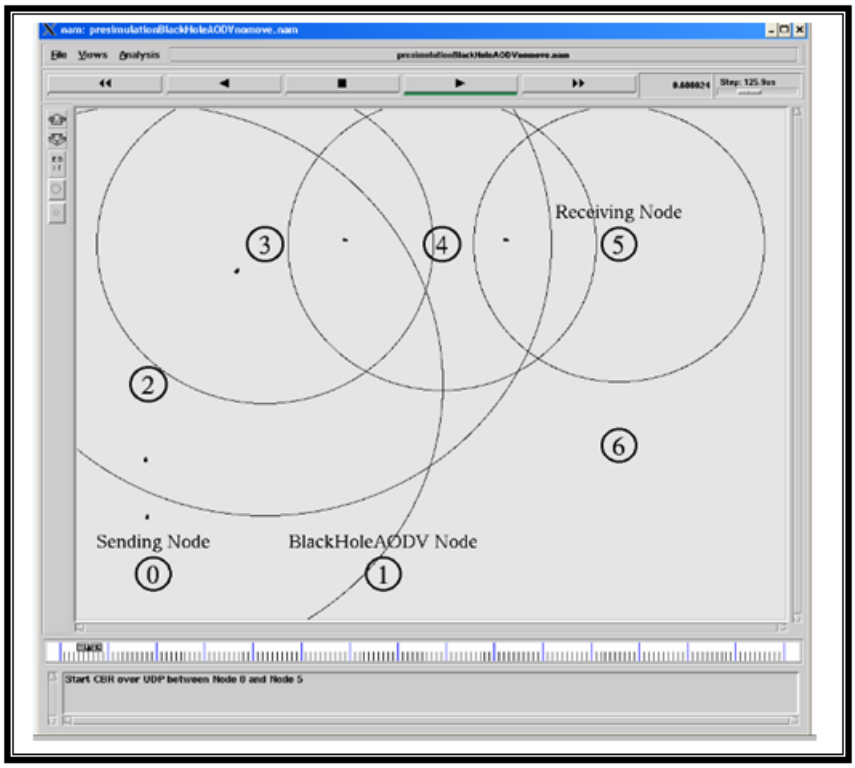

FIGURE 5.4 – Simulation de la solution du trou noir

• **Commentaire :** Dans ce scénario, à l'envoie des paquets de données du nœuds source destiné vers le nœud destinataire, le trou noir s'inséré dans le chemin reliant ces deux dernières pour empêcher les paquets d'être transmet, En repense de cette attaque, le noeud source cherche un autre chemin pour transmettre les paquets, ainsi les paquets sont transmet a la destination.

Pour le taux de paquets perdu lors de la transmission en appliquant la solution a l'attaque du trou noir, nous avons trouvé les résultats suivants :

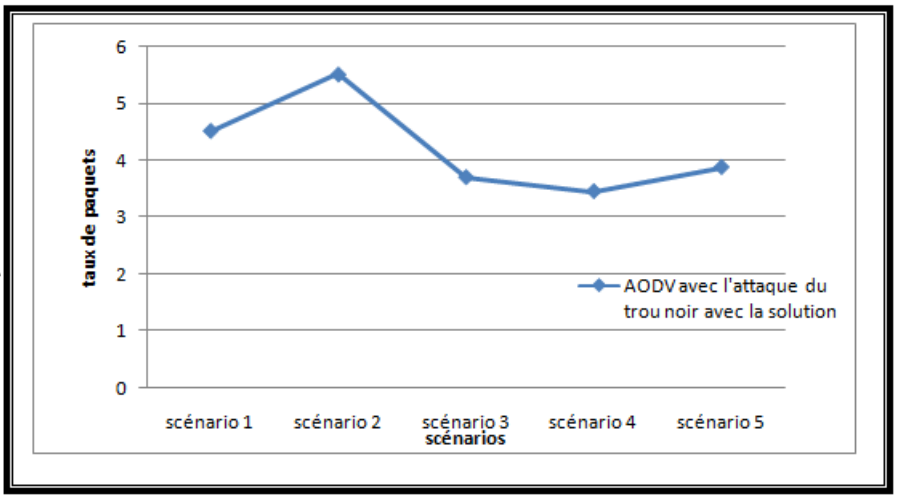

FIGURE 5.5 – Le taux de paquets perdu lors de la transmission en appliquant la solution a l'attaque du trou noir

La figure ci-dessus présente le taux de paquets perdu lors de la transmission en appliquant la solution a l'attaque du trou noir.

• **Commentaire :** Le trafic générer est transmet mais avec un taux de pertes légèrement plus élever que dans le premier cas ceci est due au chemins plus long empreinte par les données envoyer par la source vers la destination.

5.6 Conclusion

Dans ce chapitre nous avons fais des expériences sur un trafic de données, dans le premier scénario nous avons envoyé le trafic sans aucune attaque ; au deuxièmes scénario nous avons introduit l'attaque du trou noir sur les données envoyé se qui les a empêcher d'être reçues et au troisième nous avons intégrer l'attaque et la solution que nous avons proposé contre celle-ci, et elle s'est avérée efficace car nous avons retrouvé les données envoyées a la réception.

Conclusion Générale

Un réseau ad hoc est une collection de nœuds mobiles qui communiquent entre eux à travers des liaisons sans fil. Il présente l'avantage d'être facile, rapide et moins coûteux à déployer. Mais il est très vulnérable à plusieurs types d'attaques à cause de l'ouverture du médium de communication et l'absence d'une administration centralisée.

Les messages diffusés dans le réseau peuvent être interceptés, modifiés ou supprimés par le nœud malicieux, Ceci qui a de la sécurité des échanges dans un réseau ad hoc un défi pour les concepteurs des protocoles, en particulier ceux concernant le routage qui est la fonction la plus ciblée par les attaques qui visent les différents services de sécurité.

Vue les multitudes vulnérabilités des MANETs , plusieurs solutions ont été proposées pour sécuriser les différentes fonctions de ce réseau, mais à cause de la diversité des attaques une sécurité parfaite est loin d'être assurée est sa reste toujours un problème. De ce fait, des nouvelles solutions sont plus que nécessaires pour rendre le réseau plus résistant contre les différentes attaques possibles.

Dans un réseau ad hoc, un nœud source compte toujours sur des nœuds intermédiaires pour faire acheminer ses données au nœud destinataire, puisque aucun contrôle n'est fait sur l'acheminement des données. Un nœud intermédiaire qui fait partie du chemin de données peut être malicieusement introduit pour supprimer les données qui passent par lui ; ce comportement malicieux s'appelle attaque du trou noir.
Dans notre travail, nous nous sommes intéressés à la sécurité des protocoles de routage AODV dont l'objectif est de proposer des mécanismes de détection d'actions malhonnêtes pour consolider les protocoles de routage ad hoc et prévenir les attaques.

Nous nous somme focalisés sur cette attaque dont le but d'isoler des nœuds légitimes par l'absorption des paquets destinés à ces derniers après une spécification de la manière avec laquelle une telle attaque peut être menée. Les failles que nous avons détectées dont les solutions proposées par les chercheurs nous ont poussés à chercher une autre solution.

Notre solution consiste à trouver plusieurs chemins pour l'acheminement des données pour la protection contre l'attaque du trou noir à la réception.

Nous avons proposé un modèle qui permet de mesurer l'effet de cette attaque sur le fonctionnement de ces réseaux, et nous avons simulé ce travail sous NS-3. Ensuite, nous avons effectués un ensemble de simulations et nous avons présenté et interprété les résultats obtenus.

A la fin de ce travail de recherche, nous pouvons dire que la sécurisation des protocoles de routage dans les réseaux ad hoc reste un vrai challenge. En perspectives, il serait utile d'améliorer et d'optimiser de plus en plus les solutions de sécurité existantes afin de rendre les réseaux ad hoc plus fiables, plus performants et plus sécurisés à faible coût pour le grand public.

Bibliographie

Bibliographie

Bibliographie

[1] C.Sevrin, ‘‘*Réseaux et télécoms’’*, DUNOD, Normandie France, 2013.

[2] G.Pujolle, ‘‘*Les Réseaux*, ’’EYROLLES, Saint-Germain Paris, 2014.

[3] K.Alagha et G.Pujolle et G.Vivier, ‘‘*Réseaux de mobiles et réseaux sans fil,*’’ Paris, Eyrolles, 2001 (1G)

[4] K.Ibrahimi, ‘‘*Gestion des Ressources des Réseaux Mobiles de Nouvelle Génération par rapport à la Mobilité des Utilisateurs,’’* Thèse doctorat, UNIVERSITÉ MOHAMMED V – AGDAL Rabat, 2009.(2G)(3G)

[5] Y.Bouguen et Hardouin et Eric et Wolff et F.Xavier, ‘‘ *LTE et les réseaux 4G,’’* Editions Eyrolles, 2012.(4G)

[6] K.Ayad, ‘‘*Sécurité du routage dans les réseaux ad hoc Mobile*,’’ Thèse magister, Ecole nationale Supérieure en Informatique (ESI) Oued-Smar Alger, 2012.

[7] M.Dawoud, *‘‘Analyse du protocole AODV,’’* DEA d'informatique, Université Paul Sabatier – I.R.I.T, 2006.

[8] M.Tahar, ‘‘*Proposition d’un protocole à économie d’énergie dans un réseau hybrideGSM et AD HOC,’’* Thèse doctorat, 2012.

[9] N.J.Daujeard et R.Carsique et L.Lallemand,‘‘ Le routage dans les réseaux mobiles Ad hoc’’, INGENIEURS, 2002-2003.

[10] A.Bouzaher, ‘‘ *Approcheagent mobile pour l’adaptation des réseaux mobiles*,’’ Thèse magister, Université Mohamed Khider Biskra, 2011.

[11] R.Poovendran et L.Lazos, ‘‘A *graph theoretic framework for preventing the wormholeattack in wireless ad hoc network,’’* Wireless Networks (Kluwer Academic Publishers).Vol.1²3, No.27, pp.27-59,200

[12] N.Boukhechem, ‘‘*Routage dans les réseaux mobile par une approche a* base d’agent,’’ Thèse Magister en Informatique,’’ Université de Constantine, 2008.

[13] K.Oudidi, ‘‘ *Routage et Qualité de Service dans les réseaux sans fil spontanés’’*, Thèse doctorat, Université Mohammed V – Soussi Ecole Nationale Supérieure d’Informatique et d’Analyse des Systèmes (ENSIAS)- RABAT, 2010.

[14] B. Chouaib, ‘‘*Prise en Compte de la QoS par les Protocoles de Routage dans lesRéseaux Mobiles Ad Hoc,’’* ThèseMagister,Université El Hadj Lakhdar de Batna, 2008.

[15] M.djihad et O.B.Bensalem, ‘‘*Etude comparative de deux simulateurs pour lesréseaux ad-hoc sans fil,’’* Mémoire Master.Université Kasdi Merbah Ouargla, 2014.

[16] A.hajami, ‘‘*Sécurité du routage dans les réseaux sans fil spontanés : cas du protocole OLSR Université Mohammed V Souissi,’’* Thèse doctorat, Université Mohammed V Souissi**,** 2011.(avantage et inconvi 13)

[17] R.Haboub, *‘‘ Proposition d’un protocole de routage sensible au contexteetsécurisé pour les réseaux Ad-Hoc,’’*Thèse doctorat en informatique, Université Hassan II Casablanca, 2013.

[18] N.Tahir et N.Saadi, *‘‘Authentification dans les réseaux mobile ad hoc,’’* Mémoire master, Université Bejaia, 2010.

[19] A.Berraba et S.Bouklihacene et M.Lehsaine, *‘‘Evolutionary Engineering & DistributedInformation Systems Laboratory,’’* UDL de Sidi-Bel-Abbès, Algérie, 2 Laboratoire Systèmes et technologies de l'information et de la communication , 2014.

[20] F, Sailhan, *‘‘Localisation de ressources dans les réseaux ad hoc,’’* Computer Science, Université Pierre et Marie Curie-Paris VI, 2005.

[21] S.Maamar et L.Aouragh et L.Guettala et A.Bilami, *‘‘Etude des Performances des Protocoles deRoutage dans les Réseaux Mobiles Ad-Hoc,’’* Université El Hadj Lakhdar – Batna, 2007.

[22] S.Chettibi, *‘‘Protocole de routage avec prise en compte de la consommation D’énergie pour les réseaux mobiles ad-hoc,’’* Thèse magister en informatique, Université Mentouri Constantine, 2008.

[23] A.Riahla-med, *‘‘Conception et mise en œuvre d’un nouveau protocole deroutage Multi chemins sécurisé pour les réseaux ad hoc basé sur les colonies de fourmis,’’* Thèse magister, Université M’Hamed Bougara de Boumerdes, 2008.

[24] O.Cheikhrouhou, *‘‘ Sécurité des réseaux ad hoc,’’* Mémoire d’ingéniera en Informatiqu, l’Ecole Nationale d’Ingénieurs de Sfax, 2005.

[25] Y**.**Yahiatene, *‘‘traffic encryptions keys distribution models in mobile Ad Hoc networks (Distribution de clés dans un réseau dynamique),’’* Thèse magister, Université M’Hamed Bougara de Boumerdes, 2011.

[26] R.Abdellaoui, *‘‘SU-OLSR une nouvelle solution pour la sécurité du protocole OLSR,’’*Mémoire de maîtrise électronique, Montréal, École de technologie supérieure, 2009.

[27] N**.**LabraouiL, *‘‘ La sécurité dans les réseaux sans fil ad hoc,’’ ‘*Thèse doctorat, université de télécom Tlemcen, 2012.

[28] S.A.H Sedjelmaci, *‘‘mise en œuvre de mécanismes de sécurité bases sur les IDS pour lesréseaux de capteurs sans fil,’’* Thèse doctorat, Université de télécom Tlemcen, 2012.

[29] Y.Benabbassi, *‘‘ Application de la redondance pour la surveillance par réseau de capteursans fil,’’* Thèse doctorat, Université d’Oron, 2014.

[30] B.Ait-salem,*‘‘Sécurité des Calculs Distribués Multiparties Application: Sécuriser le Calcul Distribué des Confiances,’’*Université de Limoges, Laboratoire Limoges – France, 2009.

[31] D.Martins, *‘‘ Sécurité dans les réseaux de capteur sans fil Stéganographie et réseaux deconfiance,’’* Thèse doctorat, Université de Franche-Comté, 2010.

[32] H.Houd, ‘‘ Protocole pour la sécurité des réseaux sans fil Peer to Peer,’’ Thèsemagister**,** Université Kasdi Merbah – Ouargla, 2012.

[33] S.Maag et C. Grepet et A.Cavalli, *‘‘ Un Modèle de validation pour le protocole de Routage DSR,’’* Institut National des Télécommunications CNRS UMR 5157,rue Charles Fourier, F-91011 Evry Cedex, 2005.

[34] F.Ameza, *‘‘ Le routage dans les réseaux ad hoc OLSR et AODV,’’* Mémoire licence,Université de Bejaia, 2007.

[35] O.Smail, *‘‘Routage multipath dans les réseaux ad hoc,’’*Thèse doctorat, Université d’ORAN Mohamed Boudiaf, 2014.

[36] M.Frikha, *‘‘Réseaux ad hoc, routage, qualité de service et optimisation,’’LAVOISIER, 2010.*

[37] E.Belding-Royer,*‘‘Ad hoc On-Demand Distance Vector (AODV) Routing,’’* Nokia Research Center, University of California, Santa Barbara, July 2003.

[38] L.Bachiri et R.Bendadouche, *‘’ Approche de sécurité contre l’attaque Blackholedans les réseaux ad hoc,’’* Mémoire master en Informatique, Université Bejaia, 2014.

[39] L.Hamouche et F.Mezhod, *‘‘Sécurité contre l’attaque de trou noir dans les réseaux ad* hoc mobiles,’’ Mémoire master en informatique, Université Bejaia.

[40] C.Seghiri, *‘‘Protection contre l’attaque de trou noir dans les réseaux mobiles ad* hoc,’’ Mémoire d’ingéniera Informatique, Université Bejaia, 2010.

[41] A.Hammamouch et C.Bensaci, *‘‘ Protection contre l’attaque de suppression des paquetsdans les réseaux mobile ad hoc,’’* Mémoire master en informatique.Université Bejaia, 2011.

[42] L.etal et C.Licornes et L.Levier, *“Tableaux de bord de la sécurité réseau,”*2003.

[43] B.Nathalie et B.Benoit et T.Stéphane,*"Nouvelles Technologies Réseaux Les réseauxpeer-to-peer,"*Thèse ingénieur Informatique Réseaux, 2003.

[44] P.Marlier, “Sécurité du Peer-to-Peer”,[en ligne],www.labo-asso.com, 2007.

[45] R.Al king, "Localisation de sources de données et optimisation de requêtes réparties en environnement pair-à-pair," Thèse de doctorat, Université de Toulouse, 2010.

[46] S.Romina and S.Rajesh, *"Modified AODV Protocol To Prevent BlackHole Attack inMobile Ad- hoc Network,’’* International Journal OF Innovative Research & Development, Vol 2 Issue 4, April 2013.

[47] S.Mehta and H.Kabir,*"Network and System Simulation Tools for NextGenerationNetworks: a case study,''*Inha University Korea, 2010.

[48] S.C.Mandhata and Dr.S. N Patro, *"A counter nmeasure to Black hole attack on AODV- based Mobile Ad-Hoc Networks,"* International Journal of Computer & Communication Technology (IJCCT), 2011.

[49] Al-Shurman and S.Moo-Yoo and S.Park, *"Blackhole Attack inMobile Ad HocNetworks,"*ACM Southeast Regional Conference,2004.

[50] S.Androutsellis -Theotokis and D.Spinellis.*"A survey of peer-to-peer contentdistribution technologies,"* ACM Computing Surveys,December 2004.

[51] H.Deng and W.Li andD.P Agrawal, *"Routing security in wireless ad Hoc networks,"* Communications Magazine IEEE, October 2002.

[52] D.Guillaume et D.Juliette et D.Rida Kh, *"Approche Collaborative pour la détectiond'attaques dans les réseaux Pair à Pair"*, Groupement –GIS3SGS-, délivrable1, LORIA–INRIA, 2010.

[53] G.Pujolle, "Les Réseaux", EYROLLES, Paris-France, 1128, Edition 2008.

[54] H.A.Esmaili and M.R.Khalili and H. Gharaee, *"Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator,"*World of Computer Science and Information Technology Journal(WCSIT) Vol. 1, 2011.

[55] U.Irshad and S.U.Rehman, *"Analysis of Black Hole Attack onMANETs Using Different MANET Routing Protocols,"* Master thesis,School of Computing Blekinge Institute of Technology, Sweden, 2010.

[56] K.Lakshmi et al, *"Modified AODV Protocol against Blackhole Attacks in MANET,"*International Journal of Engineering and Technology Vol.2 (6), 2010, p 444.

[57] El Ghayam, Yassine, and Mohammed Erradi. "Distributed Context Management in Collaborative Environment." *New Technologies of Distributed Systems (NOTERE), 2011 11th Annual International Conference on*. IEEE, 2011.]

[58] Abdelhamid, Zebdi.*DZ-MAODV: Nouveau protocole de routage multicast pour les reseaux adhoc mobiles base sur les zones denses*.ProQuest, 2006.]

[59] Subash Chandra Mandhata, Dr.Surya Narayan Patro, "A counter

measure to Black hole attack on AODV- based Mobile Ad-Hoc Networks", International Journal of Computer & Communication Technology (IJCCT), 2011.

[60] RominaSh, Rajesh Sh, "Modified AODV Protocol To Prevent Black

Hole Attack in Mobile Ad- hoc Network", International Journal OF Innovative Research & Development, Vol 2 Issue 4, April 2013.

[61] Himral, Lalit, Vishal Vig, and Nagesh Chand. "Preventing aodv routing protocol from black hole attack." *Lalit Himral et al./International Journal of Engineering Science and Technology (IJEST)* 3.5 (2011).

[62] H.Assia et S.Chahrazed, *‘’ Protection contre l’attaque de trou noir dans les réseaux mobiles Ad,’’* Mémoire master en Informatique, Université Bejaia, 2014.

https://doc.ubuntu-fr.org/tutoriel/console_commandes_de_base

www.nsnam.org

www.ubuntu.com

1 Modélisation d'un réseau ad hoc

Un réseau ad hoc peut être modélisé par un graphe G(t) = [(V(t) ,E(t)] Où V(t) : représente l'ensemble des nœuds (i.e. les unités ou les hôtes mobiles) du réseau et E(t) modélise l'ensemble les connections qui existent entre ces nœuds.

Si e = (u,v) E(t), cela veut dire que les nœuds u et v sont en mesure de communiquer directement à l'instant t. La figure.1 suivante représente un réseau ad hoc de 10 unités mobiles sous forme d'un graphe :

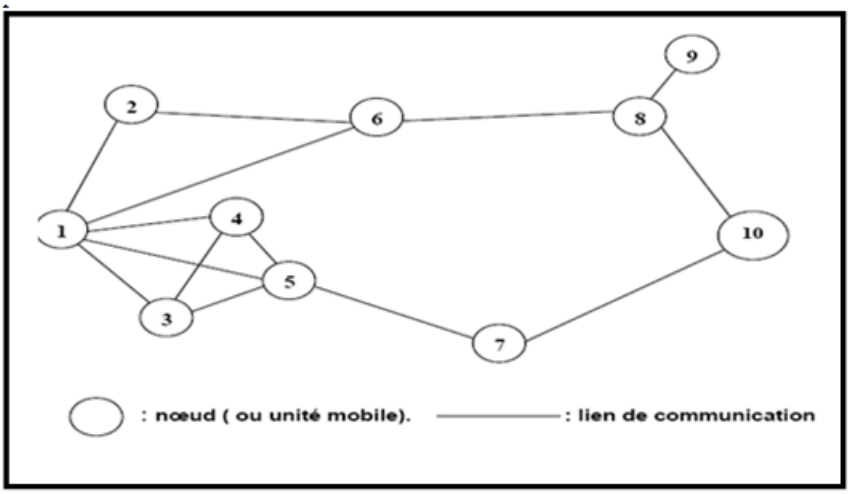

FIGURE 1 – La modélisation d'un réseau ad hoc

2 Modes de communication

Comme montre la figure3, la communication dans un réseau mobile ad hoc peut s'effectuer en trois modes :
• La communication point à point ou unicast, dans laquelle il existe une source qui communique avec une seule destination.
• La communication multipoints ou multicast, qui permet d'envoyer un message à un groupe de destinataires.
• La diffusion ou broadcast, qui consiste à envoyer un message à tous les nœuds.

3 Normes des réseaux ad hoc

Les réseaux sans fils ad hoc s'appuient sur les technologies sans fil conçues à l'origine pour des réseaux locaux sans fil à savoir :
•**Blutooth :** Elle a été lancée par Ericsson en 1994. Elle propose un débit théorique de l'ordre d'un mégabit pour une portée maximale d'une trentaine de mètre.
Le Bluetooth permet de créer un réseau de 8 appareils en communication simultanée. Son principal avantage est sa très faible consommation d'énergie.

•**HomRF :** Cette technologie a été lancée en 1988 par le HomRF Workin Group. Cette norme propose un débit théorique de 10 Mbit /s avec une portée d'environ 50 à 1OO mètre.

• **Norme 802.11 :** La 802.11 est une norme établie par l'IEEE en 1997, les débits possibles varient entre 1 et 54 Mbit/s. Les portées prévues varient entre quelques dizaines et quelques centaines de mètre.
Des extensions ont été publiées depuis, qui viennent lui ajouté des améliorations et des modes de fonctionnements plus performants. Les principales extensions et des modes de fonctionnements plus performants et sont les suivants : 802.11b, 802.11g, 802.11a, 802.22e, 802.11h, 802.11i.

• **HiperLAN :** HiperLAN est une norme européenne élaborée par l'ETSI (Européen Télécommunication Standards Institue), elle est divisée en deux catégories :

- HiperLAN1 permet un transfert autour de 20Mbit/s dans la gamme de fréquence de 5Ghz.
- HiperLAN2 permet d'obtenir un débit théorique de 54Mbit/s sur une zone d'une centaine de mètre dans une gamme de fréquences comprises entre 5150 et 5300 Mhz.

4 Installation de NS-3

Pour provenir à l'installation du NS-3, nous devons avoir une interface Linux, pour cela nous avons choisi de l'installer sur une machine virtuel et ceci en procédant de la manière suivante :
- Installation et configuration de Virtuelbox.
- Installation de Linux à partir du cite WWW.Ubuntu.com
- Téléchargement et mise en route de NS-3 à partir du cite www.nsnam.org

Une fois NS-3 télécharger, nous devons télécharger et installer les packages suivants pour faire le fonctionnement :

= Commentaire explicatif de la commande

Afficher le contenu de l'emplacement actuel pour pouvoir utiliser le raccourci de la touche tabulation qui permet de remplir le nom du fichier ou repertoire automatiquement :

ls
Accéder au repertoire Bureau/ où il y a le paquetage de NS-3 précédemment téléchergé : cd Bureau/

Mettre à jour Linux Ubuntu pour pouvoir passer à la prochaine étape sans risque d'erreur. Pour ce faire, il est nécéssaire d'utiliser le mode root grace à "sudo" puis taper le mot de passe root : sudo apt-get update

Installer les dépendances nécéssaires au bon fonctionnement de NS-3 :

sudo apt-get install gcc g++python python-dev mercurial bzr gdb valgrind gsl-bin libgsl0-dev libgsl0ldbl flex bison tcpdump sqlite3 libsqlite3-dev libxml2 libxml2-dev libgtk2.0-0 libgtk2.0-dev uncrustify doxygen graphviz imagemagick texlive texlive-latex-extra texlive-generic-extra texlive-generic-recommended texinfo dia texlive texlive-latex-extra texlive-extra-utils texlive-generic-recommended texi2html python-pygraphviz python-kiwi python-pygoocanvas libgoocanvas-dev python-pygccxml

Par mesure supplémentaire, il est préférable d'installer le géstionnaire de paquetage "Synaptic" puis le lancer afin de vérifier si les dependances sont bien à jours : sudo apt-get install synaptic sudo synaptic

Extraire le paquetage de NS-3 précédemment téléchergé : tar -xvf ns-allinone-3.23.tar.bz2

ls
Accéder au repertoire décompréssé : cd ns-allinone-3.23/

ls
Compiler (construire) NS-3 grace au scripte "build.py" : ./build.py –enable-examples –enable-tests

sudo synaptic

ls
cd ns-3.23/

ls

Résumé

Un réseau ad hoc est une collection de nœuds mobiles qui forment un réseau temporaire, interconnectés par un médium de communication sans fil sans recours à aucune infrastructure fixe ni administration centralisée. Il présente l'avantage d'être facile et moins coûteux à déployer, mais en contrepartie, il est vulnérable par plusieurs types d'attaques qui peuvent être menées sur les différentes fonctionnalités en particulier la fonction de routage.

Dans un tel réseau tous les nœuds participent à la fonction du routage qui consiste à trouver un chemin entre les nœuds source et destination à travers des nœuds intermédiaires pour faire acheminer ces paquets. Un nœud intermédiaire, qui participe à l'acheminent des données, peut se comporter malicieusement et supprimer les paquets passant par lui, au lieu de les acheminer au nœud suivant dans la route de données.

Dans notre travail, nous nous sommes intéressées à l'attaque de blackhole dans un réseau fonctionnant avec le protocole AODV, cette attaque consiste à supprimer ou redirigé le trafic absorbé vers un autre nœud. Pour empêcher cette attaque, nous avons proposé une solution basée surle principe de multi-chemins pour se protéger contre celle-ci. Une série de simulation ont été fait pour valider la solution proposée.

Mots clés : réseaux Ad hoc, sécurité des réseaux ad hoc, AODV, Trou noir

An ad hoc network is a collection of mobile nodes forming a temporary network, interconnected by a wireless communication medium without resort to any fixed infrastructure or centralized administration. It has the advantage of being easier and cheaper to deploy, but in return, it is vulnerable in many types of attacks that can be carried on the various features in particular the routing function.

In such a network all nodes are involved in routing function, which is to find a path between the source and destination nodes via intermediate nodes to route these packets. An intermediate node, which participates in the route data can behave maliciously and drop packets going through it instead of routing to the next node in the data path.

In our work, we are interested to the attack of theblack-hole in a network running AODV protocol, this attack is to remove absorbed or redirected traffic to another node. To prevent this attack, we proposed a solution based on the principle of multi- paths to protect against it. A series of simulations have been done to validate the proposed solution.

Key word: AD hoc Network, Security of Ad hoc networks, AODV, Blackhole