REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE KASDI MERBAH, OUARGLA

FACULTE DE NOUVELLE TECHNOLOGIE ET DE LA COMMUNICATION

DEPARTEMENT DE L'INFORMATIQUE

Projet de Fin d'Etudes

En vue de l'obtention du diplôme de

MASTER

Domaine : Informatique

Filière : Informatique

Spécialité : Informatique Fondamental

Présenter par: CHEBBAH Houssem & REZKI Boumediene

Thème

Etude de l'attaque BLACKHOLE dans Les réseaux sans fil décentralisés

Le : 25/06/2018

Devant le jury :

Encadreur	Dr. Ahmed Korichi	Maître de conférences « A »
Examinateur	Abdellkader Benmire	Maitre- assistant « A »
Examinatrice	Wassila Korichi	Maitre-assistant « A »

Année universitaire 2017/2018

Remerciements

Tout d’abord, Louange à Allah, le Clément et le Miséricordieux de m'avoir donné la force et le courage de mener à bien ce travail.

Notre vifs remerciements vont à mon encadreur « Dr.Ahmed Korichi», pour les orientations et les conseils qu’il a su me prodiguer durant l’évolution de notre projet.

nous voulons aussi remercier tous les professeurs qui ont contribué à ma formation.

Notre remerciements vont également à tous ceux et celles qui de près ou de loin nous ont apporté l'aide et l'encouragement.

CH.H & R.B

Dédicaces

Je dédie le présent travail à :

Mes parents qui m'ont toujours encouragé dans le chemin du savoir;

Mon grand-père et ma grand-mère, paternels et maternels;

Mes frères et sœurs;

Mes oncles et tantes, paternels et maternels;

Mes cousins, paternels et maternels;

Mes amis:

Toufik Gasmi, Khaled Sahli, Dayae Dehimi, Med Bekouche,

NasrAllh Allam, Laid Gouhmous, Med Benbeziane, Imad Djerbaoui, Bouhrira N.Imane et mon binôme Rezki Boumediene

A tous mes enseignants dans tous les paliers,

A toute ma promotion,

A toute personne qui m'a procuré de l'aide et du courage…

CHEBBAH Houssem

Dédicaces

Je dédie le présent travail à :

Mes parents qui m'ont toujours encouragé dans le chemin du savoir;

Mon grand-père et ma grand-mère, paternels et maternels;

Mes frères et sœurs;

Mes oncles et tantes, paternels et maternels;

Mes cousins, paternels et maternels;

Mes amis:

imad, momouh ,benouda(med) , karima, fouad, houssem, hatem, salim, amine, islam, saber, hayat, abdou, Sahli, Allam, Laid, Benbezianen, yacine, med, chnafa, med dahan, oussama, nasro, hamza, nidal, taher, youcef, fethi, mano, med arab, djilali,

sidahmed, sabri, tofik, alladine

A tous mes enseignants dans tous les paliers,

A toute ma promotion,

A toute personne qui m'a procuré de l'aide et du courage…

REZKI Boumediene

Résumé

Le présent travail étudie l'attaque blackhole comme un grand problème des réseaux sans fil décentralisés. Cette attaque est du type Déni de Service dans laquelle un nœud malicieux supprime les paquets en montrant un autre chemin vers le nœud destinataire et après il supprime tous les paquets au lieu de les transmettre au nœud déclaré comme destination. Selon les résultats obtenus, il est trouvé que le nœud malicieux a affecté le taux de livraison des paquets et le débit. Comme solution nous avons proposé l'IDS qui a surmonté ce problème en détectant ce nœud malicieux et en l'éliminant du réseau. Dans le futur nous conseillons d'auto-immuniser les protocoles ou de doter les nœuds de mécanisme de détection des nœuds malicieux.

Mots cles :blackhole, réseaux sans fil décentralisés, protocoles, IDS

Abstract

The present research studies the blackhole attack, which is major problem in wireless ad hoc networks. This attack is of DoS one where a malicious node drops packets by showing new path to destination node and after that drops all packets instead of transmitting to the node which is set to be destination. As per obtained results, it is found that the corrupted node affected the packet delivery ratio and throughput. As a solution, we proposed IDS to overcome this problem by detecting this malicious node by removing it from network. In future, we advise to auto-immune protocols or to give nodes the ability to detect malicious nodes.

Key words: blackhole, wireless ad hoc networks, protocols, IDS

Table des matières

Table des figures

Liste des abréviations

AODV	**A**d-Hoc **O**n-Demand **D**istance **V**ector protocol
CBR	**C**onstant **B**it **R**ate
CSMA/CA	**C**arrier **S**ense **M**ultiple **A**ccess / **C**ollision **A**voidance.
DOS	**D**enial **o**f **S**ervice
DSR	**D**ynamic **S**ource **R**outing.
DSRC	**D**edicated **S**hort **R**ange **C**ommunication.
E-E delay	**E**nd **to E**nd **d**elay
IDS	**I**ntrusion **D**etection **S**ystem
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers.
MAC	**M**edium **A**ccess **C**ontrol.
MANET	**M**obile **A**d hoc **N**etwork.
PDR	**P**acket **D**elivery **R**atio
RERR	**R**oute **Err**or
RREQ	**R**oute **Req**uest
RREP	**R**oute **Rep**ly
Wi-Fi	**W**ireless **F**idelity

Introduction générale

Introduction générale

Les réseaux sans fil décentralisés ont trouvé leur place significative dans les tendances récentes en ingénierie et en technologie. Les problèmes soulevés par une telle technologie et les défis qui l'attendent préparent le chemin vers d'excellentes opportunités de recherche et de développement.

En général, dans les réseaux sans fil, il y a deux principales architectures : réseaux infrastructure (simple saut) et les réseaux mobiles ad hoc (plusieurs sauts). Dans le premier cas, les utilisateurs sont reliés à des stations de base ou à des points d'accès avec une mobilité limitée à la zone de couverture de ces bases ou points d'accès. Dans le deuxième cas, les réseaux mobiles ad hoc (MANets) ont la capacité de communication et de mobilité en même temps et sans utiliser aucune infrastructure câblée. Ce type de réseaux est réellement un réseau à organisation automatique et il est adaptatif, pouvant être formé et déformé à la volée sans le recours à une administration centralisée.

Sujet

Dans les réseaux sans fil décentralisés, les nœuds mobiles sont le réseau, car ils doivent coopérer pour fournir les fonctionnalités généralement assurées par un réseau câblé (par exemple : routeur, serveur, switch, passerelle, pont …etc.) ce qui les rend très vulnérableset les confronteaux problèmes fondamentaux de sécurité qui à leur tour constituent l'un des défis les plus importants. Notre intérêt a été suscité par l'un des problèmes de sécurité touchant ce type de réseau, l'attaque blackhole, entre autres.

L'objectif

Dans le cadre de ce mémoire, nous allons implémenter une solution préventive aux problèmes causés par l'attaque blackhole qui touche les réseaux sans fil décentralisés.

Structure du mémoire

Pour mener à bien notre recherche, le présent travail comprend deux principales parties : une théorique et l'autre pratique.

La partie théorique se compose de deux chapitres :

-le premier, intitulé "**Les réseaux sans fil décentralisés** ", s'attache à élucider la notion de réseau sans infrastructure et ses types : Manets, Vanets, SPANs et HANets, en tant qu'applications civiles puis à décrire leur système de fonctionnement et leurs différents protocoles.

-le deuxième, intitulé "**La sécurité des réseaux sans fil décentralisés**", qui définit les mécanismes de base de la sécurité et met en relief les exigences de sécurité pour tels réseaux, et puis aborde les attaques auxquels ils sont soumis et en particulier le problème du trou noir (blackhole, objet de cette étude).

La partie pratique, comprenant un seul chapitre au titre de "**Implémentation**", est consacrée à l'étude poussée des mécanismes de l'attaque blackhole et à sa solution, aux simulations et interprétations des résultats.

Chapitre I

Les réseaux sans fil décentralisés

1 Introduction

Ce premier chapitre, en commençant par un historique assez informatif sur la naissance des réseaux sans fil décentralisés, s'attache à élucider la notion de réseau sans infrastructure et ses types : Manets, Vanets, SPANs et HANets et autres types, en tant qu'applications civiles puis à décrire leur système de fonctionnement, leurs normes, leurs différents protocoles et enfin à mettre en relief les problèmes techniques qu'ils rencontrent.

2 Historique

Le premier réseau de données sans fil été appelé "Packet Radio Network", il a été sponsorisé par DARPA (Defense Advanced Research Project Agency) au début des années 1970. Bolt, Beranek and Newman Technologies (BBN) and SRI International ont conçu,construit,et expérimenté ces premiers systèmes. Parmi les expérimentateurs on citeRobert Kahn, Jerry Burchfiel, et. Ray Tomlinson.Ces premiers systèmes à paquets radio ont précédé l'Internet, et vraiment ils ont été une partiede la motivation del'original Internet Protocol. Et puis,DARPA a expérimentéleprojet Survivable Radio Network (SURAN)durant les années 1980.Une autre troisième vague d'activité académique et de recherché a commencéau milieu des années 1990 avec l'avenue des cartes radio à la norme 802.11, bon marché et destinées aux ordinateurs personnels. De tels réseaux avaient des applications militaires mais des problèmes avec ces paquetsradio ont surgi, comme : (1) éléments volumineux, (2) faible débit, (3) incapacité de maintenir les liaisons pour une haute mobilité.

Leprojet n'a pas avancé jusqu'au début des années 1990 où les réseaux ad hoc sans fil ont pris naissance par les travaux de Charles Perkins de SUN MicroSystemset Chan Keong Toh à l'Université de Cambridge ont commencé séparément à travailler sur un autre Internet, celui des réseaux ad hoc sans fil. Le premier a développé le protocole DSDV (Destination Sequence Distance Vector) mais Toh proposa un protocole à la demande et ce n'est qu'en 1999 que le premier réseau ad hoc sans fil a fonctionné, puis AODV (Ad-hoc On-Demand Distance Vector) a été implémenté en 2005suivi du protocole DSR (Dynamic Source Routing) en 2007 et réalisé par David Johnson et Dave Maltz. [J. Burchfiel et al,1975]

D'autres informations sur l'historique sont disponibles dans [Ishu Varshney et al,2017]mais nous nous contentons desfaits donnés.

3 Généralités

3.1 Classifications des réseaux sans fil

Selon leur architecture, les réseaux sans fil se classent en deux grandes catégories: avec et sans infrastructure. [Bourai Amar et al,2014]

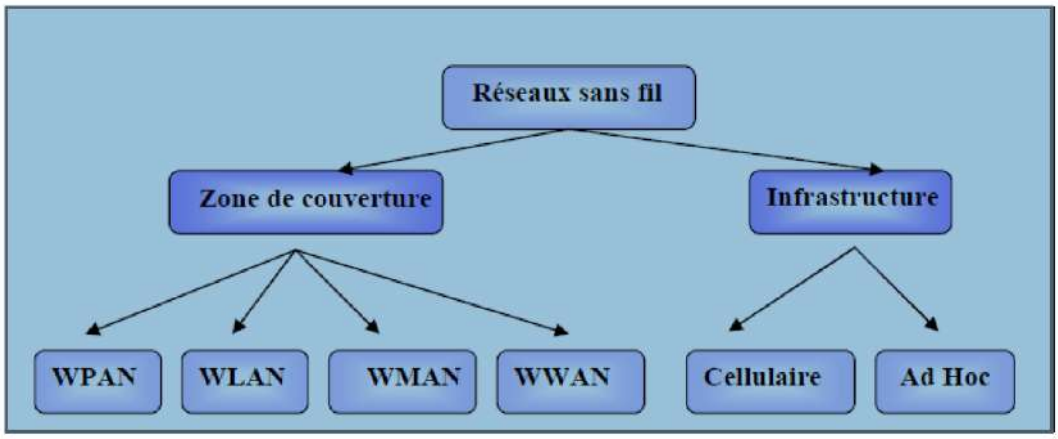

Figure 1.1: *Classification des réseaux sans fil.*

3.2 Exemples de réseaux sans fil

Les ordinateurs ou tous autres équipements prenant en charge la Wi-fi peuvent se connecter de deux manières.

L'illustration d'un simple réseau à infrastructure est la suivante :

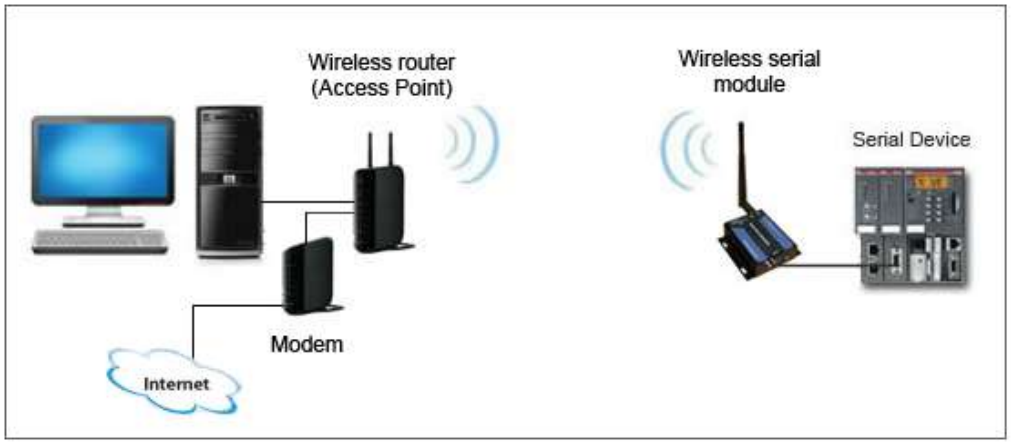

Figure 1.2*: Réseau sans fil avec infrastructure.*

Ce type de réseau nécessite un point d'accès, dans ce cas c'est le routeur sans fil.

Mais dans les réseaux sans fil et sans infrastructure, les équipements n'ont pas besoin d'un routeur tout en pouvant s'interconnecter en utilisant la Wi-fi.

***Figure 1.3**: Simple réseau sans fil sans infrastructure (Ad Hoc).*

3.3 Définition et comportement d'un réseau Ad-hocMobile

Selon [Ishu Varshney et al,2017], c'est une accumulation de nœuds, reliés sans fil, et qui peuvent dynamiquement former un réseau pour échanger des informations sans la préexistence d'une infrastructure qui est bénéfique pour la croissance dynamique de l'organisation.

Et selon [P.Visalakshi et al,2013] , un réseau mobile sans fil ad-hoc se comporte comme suit:

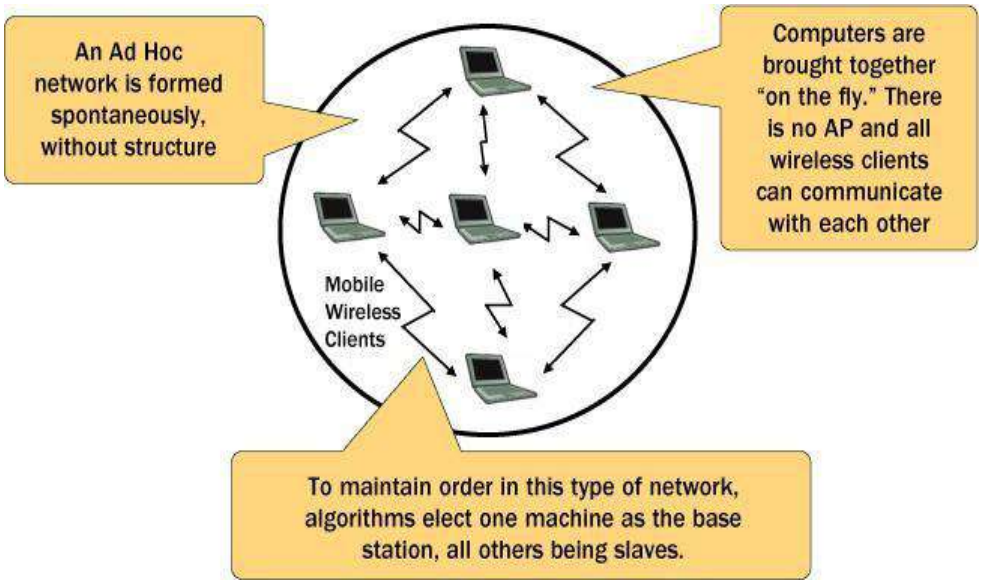

***Figure 1.4:** Comportement d'un réseau Ad-Hoc sans infrastructure.*

-se former spontanément et sans structure ;

-les nœuds sont interconnectés à la volée (pas de points d'accès) et tous les clients peuvent communiquer les uns avec les autres ;

-pour maintenir l'ordre dans ce type de réseau, des algorithmes choisissent un nœud comme serveur et tous les autres seront considérés comme des clients.

3.4 Diverses autres dénominations

Selon [Mshari Alabdulkarim,2017], les réseaux sans infrastructures sont désignés sous différents noms, entre autres un nom générique de MHWNs (Multi-Hop Wireless Networks), réseaux sans fil à sauts multiples qui sont des collections de nœuds qui communiquent sans fils en utilisant un signal radio et surtout en partageant un même canal.

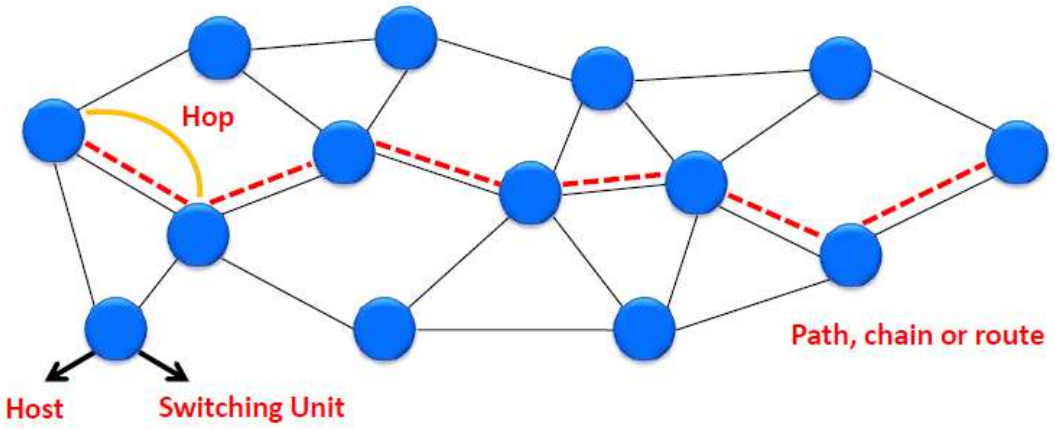

Figure 1.5: *Structure d'un réseau sans fil à sauts multiples.*

Ils sont alors dénommés : Packet Radio Network, Ad-hoc Network, Mobile Network, dans la même référence.

4 Les MANets et leurs applications

Un WANet (Wireless Network) ou MANet (Mobile Ad-Hoc Network) est un type décentralisé de réseau sans fil, il est dit aussi réseau spontané ou "à la volée" [Laura Feeny,2013], et qui a plusieurs applications dont :

4.1 Les VANets

4.1.1 Définition

Les réseaux véhiculaires ad hoc (VANets) sont un type particulier de réseaux mobiles ad hoc (MANets), où les véhicules sont simulés comme des nœuds mobiles. Les réseaux MANets et VANets se diffèrent en quelques détails. Dans VANets au lieu de se déplacer au hasard, les véhicules tendent à se déplacer d'une façon organisée. La communication avec les équipements de la route est caractérisée de manière assez exacte. De plus, la majorité des véhicules sont limités au niveau de leur mouvement, par exemple suivre une route bien définie.

Les réseaux véhiculaires sans fil contiennent deux entités: les véhicules et les points d'accès. Les points d'accès sont fixés et connectés généralement à l'Internet, et ils pourraient participer en tant que point de distribution pour les véhicules [Ines Chihi,2017].

4.1.2 Modes de communication dans les réseaux VANets

Dans les réseaux de véhicules, on peut distinguer deux modes de communication, les communications Véhicule-à-Véhicule (V2V) et les communications Véhicule-à-Infrastructure (V2I). Les véhicules peuvent utiliser un de ces deux modes ou bien les combiner s'ils ne peuvent pas communiquer directement avec les infrastructures. Dans cette section, nous présentons le principe et l'utilité de chaque mode [Ines Chihi, 2017] :

- **Mode de communication Véhicule-à-Véhicule (V2V)**

Ce mode de communication fonctionne suivant une architecture décentralisée, et représente un cas particulier des réseaux ad hoc mobiles, Il est basé sur la simple communication inter-véhicules ne nécessitant pas une infrastructure. En effet, un véhicule peut communiquer directement avec un autre véhicule s'il se situe dans sa zone radio, ou bien par le biais d'un protocole multi-sauts qui se charge de transmettre les messages de bout en bout en utilisant les nœuds voisins qui les séparent comme des relais. Dans ce mode, les supports de communication utilisés sont caractérisés par une petite latence et un grand débit de transmission. Les communications V2V sont très efficaces pour le transfert des informations concernant les services liés à la

sécurité routière et militaires, mais elles ne garantissent pas une connectivité permanente entre les véhicules.

- **Mode de communication de Véhicule à Infrastructure (V2I)**

Ce mode de communication permet une meilleure utilisation des ressources partagées et démultiplie les services fournis (par exemple: accès à Internet, échange de données de voiture-à-domicile, communications de voiture-à-garage de réparation pour le diagnostic distant, ...etc.) grâce à des points d'accès RSU (Road SideUnits) déployés aux bords des routes; ce mode est inadéquat pour les applications liées à la sécurité routière car les réseaux à infrastructure ne sont pas performants quant aux délais d'acheminement.

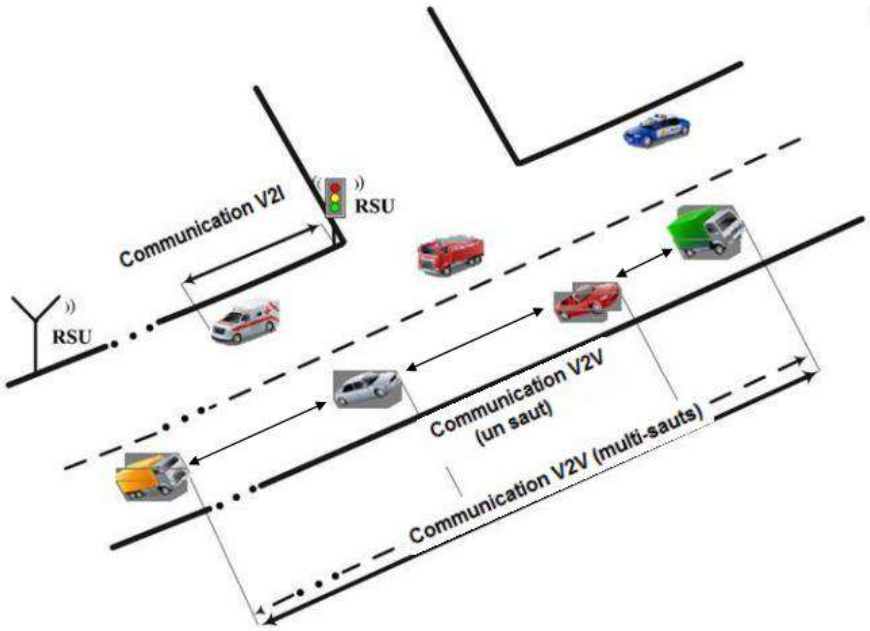

Figure 1.6: Les modes de communication dans les VANets.

4.2 Les SPANs

Les SPANs(Smart Phone Adhoc Networks) utilisent un hardware (Wi-fi et Bluetooth) et un software (protocole) pour former des réseaux peer-to-peer (pair-à-pair) sans se baser sur les réseaux cellulaires, les points d'accès, ou sur la traditionnelle infrastructure. Le dernier iphone 7.0 iOS d'Apple est prédit pour changer le monde car il va permettre de se connecter avec des millions de téléphones dans un réseau adhoc maillépair-à-pair.

4.3 HANets

Selon [Tie Qiu et al.,2017], les HANets (Heterogeneous Ad Hoc Networks), réseaux ad hoc hétérogènes, sont des composants importants de l'Internet des Things. Ils regroupent les réseaux de capteurs sans fil, les Smart Ad hoc Networks (SAN,Réseaux Ad hoc intelligents),réseaux Wi-Fi, les réseaux de télécommunications, les VANets, etc…

4.4 Autres applications

Les réseaux adhoc sans fil et sans infrastructure ont envahi d'autres domaines allant de la maison (éclairage intelligent), aux routes (réseaux d'éclairage publics), aux hôpitaux (réseaux pour le suivi des malades, alerte des médecins et infirmiers), à la libre nature (réseaux de secours durant les désastres), à la mer (pour remplacer les satellites),à l'industrie (réseaux de robots), etc.

5 Les systèmes pair-à-pair

En général, un système pair-à-pair (peer-to-peer) est un système d'échange de ressources entre deux utilisateurs (nœuds) sans passer par un serveur, ils se partagent alors la bande passante (bandwidth) qui sert de canal d'échange de toutes sortes de données.Un tel système est caractérisé par une importante volatilité des pairs (apparition/disparition imprévisible des pairs) et par une distribution géographique importante (d'où un asynchronisme et une communication non fiables).[Fabrice le Fessant,2008]

D'après [Claude Duvallet,2017], dans un système pair-à-pair,les nœuds ne jouent pas exclusivement les rôles de client ou de serveur mais peuvent assurer parallèlement les deux fonctions. Ils jouent aussi le rôle de routeur en passant les messages de recherche,voire les données vers leur(s) destinataire(s).

6 Les normesdes réseaux décentralisés

L'IEEE (Institute of Electrical and Electronics Engineers) définit les technologies relatives à ces types de réseaux. Il y a trois principales normes opérationnelles pour les réseaux locaux (LAN) : IEEE 802.11a, 802.11b et 802.11g. Ces normes appartiennent à la famille des protocoles 802.11 (Wi-fi). En 1992, la

norme 802.11a a été ratifiée par l'IEEE comme ayant un débit de 54 Mbps,mais le vrai débit est entre 17-28 Mbps. La norme la plus fréquemment déployée est la 802.11b, elle est utilisée par la plupart des zones sensibles (HotSpot). Pratiquement, sa vitesse de transmission réelle est de l'ordre de 4-7 Mbps.

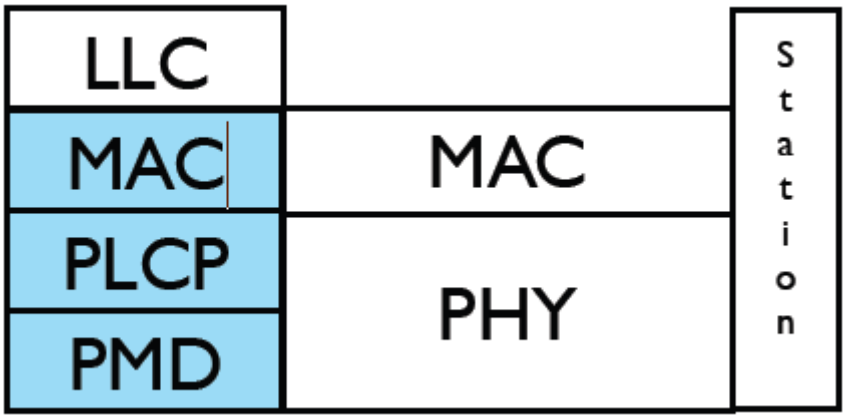

Figure 1.7: Architecture du protocole IEEE 802.11.

La couche physique (PHY) est composée de deux sous-couches :

- PMD (Physical Medium Dependent), Physique dépendant du support, encodage des données et émission;
- PLCP (Physical Layer Convergence Protocol),protocole de convergence de la couche physique, il écoute le support.

La couche de liaison comprend deux sous-couches : LLC et MAC.

- La sous-couche LLC (Logical Link Control), contrôle de liaison logique;
- La sous-couche MAC (Medium Access Control) : elle s'occupe de l'adressage des paquets, en particulier.

7 Protocoles des réseaux Ad Hoc

Selon [Dr.S.S.Dhenakaron et al.,2013], les protocoles de routage définissent un ensemble de règles qui contrôlent le parcours des paquets de messages à partir d'une source et vers une destination.Dans les MANets,c'est-à-dire les réseaux décentralisés, il existe différents types de protocoles de routage, chacun d'entreeux est

appliqué selon les circonstances du réseau. Il se classe en protocoles proactifs, protocoles réactif et protocoles hybrides (composant les deux précédents).

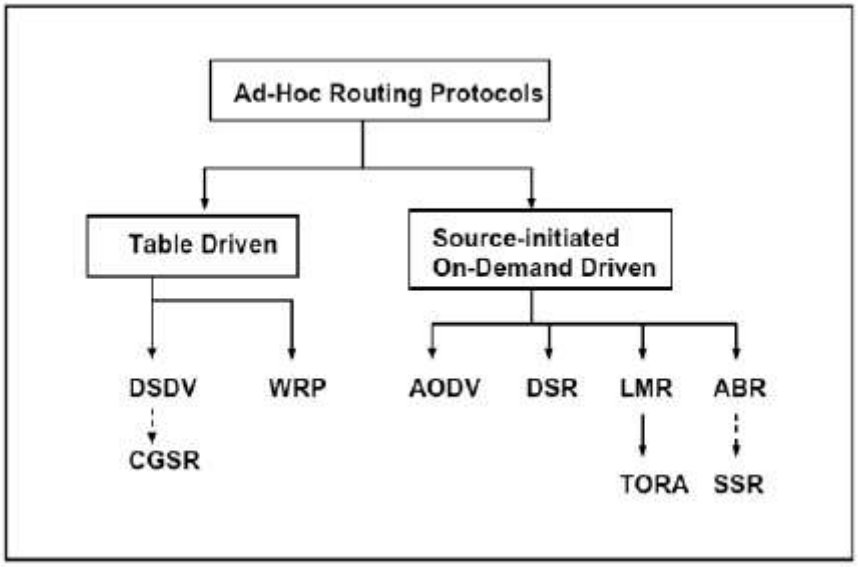

Figure 1.8: Arbre des protocoles dans les MANets.

7.1 Les protocoles proactifs

Dits aussi protocoles à table de routage où chaque nœud maintient une table de routage qui contient les informations sur la topologie du réseau même s'il n'en a pas besoin, cette table est périodiquement mise à jour lors du changement de la topologie. Parmi ces protocoles, on cite les protocoles : DSDV, OLSR, WRP et autres.

7.1.1 Le protocole DSDV (Dynamic destination-Sequenced Distance-Vector)

La table de routage contient la liste de toutes les destinations possibles et le nombre de sauts à chacune d'elles, elle est marquée par un numéro de séquence qui est généré par le nœud destinataire.

7.1.2 Le protocole WRP (Wireless Routing Protocol)

Ce protocole fait partie des protocoles qui utilisent la recherche de chemin.

7.2 Les protocoles réactifs

Connus aussi sous le nom de protocoles de routage à la demande. La découverte de route se fait à la demande du nœud source qui consulte sa table pour

une destination donnée.Ce type de protocoles utilise aussi la maintenance de route pour pallier aux ruptures de liaison augmentant ainsi le temps.

7.2.1 Le protocole DSR (Dynamic Source Routing)

Le destinataire détermine sa route à partir de la source et inclut les adresses des nœuds intermédiaires à l'enregistrement de route dans le paquet. Ce type de protocoles n'utilise pas le message HELLO (dit beacon).

7.2.2 Le protocole AODV (Ad hoc On demand Distance Vector)

Lorsqu'une source veut envoyer un paquet vers une destination, elle diffuse un paquet de demande de route dite RREQ(Route Request),les nœuds voisins à leur tour diffusent ce paquet vers leurs voisins jusqu'à ce qu'il arrive à destination. Durant cette opération, les nœuds intermédiaires enregistrent l'adresse du voisin à partir duquel la première copie du paquet diffusé est reçu. Ainsi, le chemin de retour est assuré.

Pour la maintenance de route, et lorsqu'un nœud se déplace il doit réinitialiser la découverte de route.

7.2.3 Le protocole ABR(Associativity-Based Routing)

Le protocole ABR(Routage basé sur l'associativité) définit une nouvelle métrique pour les réseaux ad hoc, le degré d'association de la stabilité. Dans ce protocole, la route est choisie sur la base de ce degré, ainsi chaque nœud annonce son existence par un message HELLO, son voisin met à jour sa table d'associativité en augmentant son compte,un haut degré (un nombre élevé de messages HELLO reçus) veut dire que le nœud émetteur est stable. Le compte d'un nœud qui sort du voisinage est remis à zéro.

7.2.4 Le protocole SSA (Signal Stability-based)

Le protocoleà signal stable SSA effectue la recherchede route sur la base de la puissance du signal, détectant ainsi les canaux faibles et forts.

7.2.5 Le protocole TORA (Temporary Ordered Routing Algorithm)

Le protocole TORA (Algorithme de Routage Temporairement Ordonné) établit un graphe direct acyclique de la route (de la source à la destination)

lorsqu'une liaison est faite, il établit un lien inverse. Il utilise alors un paramètre au nom de "Height" qui mesure la distance du nœud répondant à la requête de découverte de route.

7.3 Les protocoles hybrides

Ce sont une combinaison des protocoles proactifs et des protocoles réactifs qui résout deux sérieux problèmes, ainsi ils utilisent le mécanisme de découverte de route des protocoles réactifs et le mécanisme de maintenance de la table pour éviter la latence et le sur-débit du réseau. Ils conviennent aux grands réseaux ayant un grand nombre de nœuds.Parmi ce type de protocole, le protocole ZRP (Zone Routing Protocol), protocole de routage par zone, chaque nœud doit connaître ses voisins en premier lieu.

8 Les problèmes des réseaux Ad hoc

Les Docteurs [Baruch ,2008] ont classé les problèmes auxquels les réseaux Ad hoc ont fait face à cette date.

8.1 Les problèmes de routage

- Les routeurs sont mobiles;
- Les changements de liaison surviennent assez souvent (perte de paquets);
- Les événements de mise à jour sont souvent envoyés, d'où un grand nombre de contrôles;
- Les tables de routagepeuvent ne pas converger ;
- Il peut y avoir des boucles;

8.2 Les problèmes d'accès au canal

- L'accès au canal est distribué, c'est-à-dire pas de concept de station fixe;
- Très difficile d'éviter la collision de paquets;
- Très difficile de prendre en charge la qualité de service QoS;
- Le premier travail sur les paquets radio s'est fait sur la base du CSMA.

8.3 Les problèmes de mobilité

- La mobilité affecte la transmission du signal et par suite la communication;

- La mobilité affecte l'accès au canal;
- La mobilité affecte le routage (routes et paquets);
- La mobilité affecte la multidiffusion;
- La mobilité affecte les applications.

9 Conclusion

Les réseaux ad hoc sont des réseaux décentralisés qui portent généralement le nom de MANets, ils interviennent dans beaucoup de domaines, ils fonctionnent en peer-to-peer, ils ont plusieurs protocoles et sont exposés à de sérieux problèmes.

Chapitre II

La sécurité dans les réseaux sans fil décentralisés

1 Introduction

Dans ce chapitre, nous présentons les notions et les mécanismes de base de la sécurité, et puis on détermine les besoins en sécurité pour les réseaux décentralisés et les classes d'attaques auxquelles ils peuvent être exposés pour bien poser le problème du blackhole tout en décrivant l'état de l'art à ce sujet.

2 Les notions et mécanismes de base de la sécurité

2.1 La cryptographie

La cryptographie est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible; c'est ce qu'on appelle le chiffrement, qui à partir d'un texte en clair, donne un texte chiffré ou cryptogramme. Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré[Lazib Nassim et al.,2013].

2.2 Le chiffrement symétrique :

Dans le chiffrement symétrique, appelé aussi chiffrement à clé secrète, la même clé est utilisée pour le chiffrement et le déchiffrement. Deux interlocuteurs désirant communiquer des données confidentielles doivent partager une clé secrète (k). Cette même clé est utilisée par l'émetteur pour chiffrer le message et par le récepteur pour déchiffrer le message reçu. Lorsque l'utilisateur A envoie le message m chiffré avec la clé k ({m}k) vers l'utilisateur B, ce dernier est capable de le déchiffrer en utilisant la même clé k et récupérer m. Le chiffrement à clé symétrique a l'avantage d'être rapide en termes de calculs [Lazib Nassim et al.,2013].

2.3 Le chiffrement asymétrique

Dans le chiffrement asymétrique, appelé aussi chiffrement à clé publique, chaque interlocuteur détient un couple de clés : une clé visible clé publique et une clé secrète appelée clé privée. Si un texte est chiffré avec la clé publique de l'utilisateur A, il ne sera déchiffré que par la clé privée de A. Et s'il est chiffré avec la clé privée d'A, il ne sera déchiffré qu'avec la clé publique de A.

Le principal avantage de la cryptographie asymétrique est qu'elle permet à des utilisateurs n'ayant pas d'accord de sécurité préalable d'échanger des messages de manière sure. En effet, ces utilisateurs n'auront plus besoins d'établir un canal sécurisé pour s'échanger la clé. Ce type de cryptographie permet d'avoir une signature d'un utilisateur dans le but de s'authentifier et de s'assurer de son identité, en envoyant le message chiffré avec sa clé privée, tous les récepteurs peuvent vérifier la signature en utilisant sa clé publique pour le déchiffrer[Lazib Nassim et al.,2013].

2.4 Le hachage

Il consiste à déterminer une information de taille fixe et réduite (appelée une empreinte ou un condensé) à partir d'une donnée de taille indifférente [Lazib Nassim et al.,2013].

2.5 MAC (Message Authentification Code)

C'est un code accompagnant des données qui assure les mêmes fonctionnalités de la signature numérique, mais son implémentation se base sur l'utilisation de la clé secrète et sur des fonctions similaires à celles de hachage[Lazib Nassim et al.,2013].

2.6 La signature numérique

C'est un code numérique associé à un message électronique afin que les destinataires puissent en authentifier les origines et en vérifier l'intégrité. Son implémentation fait appel aux fonctions de hachage et à la clé privée du signataire[Lazib Nassim et al.,2013].

2.7 Le certificat numérique

C'est une structure de données permettant de prouver l'identité du propriétaire d'une clé publique. Les certificats numériques sont signés et délivrés par un tiers de confiance appelé l'autorité de certification (AC) [Lazib Nassim et al.,2013].

2.8 L'autorité

Les autorités sont des entités de confiance, qui sont responsables de l'établissement des clés, la gestion des identités et les qualités des nœuds dans un réseau.

3 Les besoins en sécurité

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

3.1 L'authentification

L'authentification permet de vérifier l'identité d'une entité ou d'un nœud dans le réseau. C'est une étape incontournable pour le contrôle de l'accès aux ressources réseau.

Sans l'authentification, un nœud malicieux peut facilement usurper l'identité d'un autre nœud dans le but de bénéficier des privilèges attribués à ce nœud ou d'effectuer des attaques sous l'identité de ce nœud et de nuire à la réputation du nœud victime.

Le schéma d'authentification centralisé, et connu sous le nom d'infrastructure à clé publique (PKI) ne peut être appliqué directement au réseau mobile Ad Hoc n'est pas possible pour des raisons de changement dynamique et fréquent de topologie réseau, car la disponibilité du service d'authentification est limitée en raison de la limite des capacités des nœuds (énergie, calcul, etc....) [Abderrazak Rachedi,2008].

3.2 La confidentialité

La confidentialité est un service essentiel pour assurer une communication privée entre les nœuds. C'est une protection contre les menaces qui peuvent causer la divulgation non autorisée d'informations alors qu'il faut veiller au caractère privé de l'information.

Elle est principalement basée sur la cryptographie, en particulier les algorithmes de chiffrement, symétrique ou asymétrique,mais le mécanisme de gestion des clés n'est pas adapté aux nœuds mobiles[Abderrazak Rachedi,2008]

3.3 L'intégrité

Ce service assure que le trafic de la source à la destination n'a pas été altéré ou modifié sans autorisation préalable pendant sa transmission. C'est la protection contre les menaces qui peuvent causer la modification non autorisée de la configuration du système ou des données. Les services d'intégrité visent à assurer le bon fonctionnement des ressources et la transmission.

Ces services assurent une protection contre la modification délibérée ou accidentelle et non autorisée des fonctions du système (intégrité du système) et de l'information (intégrité des données). Dans le réseau sans fil, le message peut être modifié pour des raisons non malicieuses, telles que la corruption du paquet au niveau de la propagation radio. Cependant, le risque qu'un nœud malicieux modifie le paquet est toujours présent. En fait, ce service peut être appliqué de manière indirecte avec des protocoles de sécurité qui assurent la confidentialité ou l'authentification [Abderrazak Rachedi,2008].

3.4 La non répudiation

La non-répudiation est la possibilité de vérifier que l'émetteur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues. En d'autres termes, la non-répudiation permet de garantir qu'une transaction (émission/réception/action) ne puisse pas être niée. Cela est très pratique pour détecter et isoler les nœuds compromis.

N'importe quel nœud qui reçoit un message (paquet) erroné peut accuser l'émetteur avec une preuve et cela permet de convaincre d'autres nœuds de la compromission du nœud émetteur. Généralement, la non-répudiation peut être atteinte seulement en utilisant la technologie du certificat numérique. En effet, cette technologie permet de prouver l'identité d'une personne qui possède sa propre clé privée [Abderrazak Rachedi,2008].

3.5 Autres services

Nous citons d'autres paramètres de sécurité utilisée dans l'analyse des aspects de sécurité réseau mobiles Ad hoc qui sont les suivants : la disponibilité, l'autorisation d'accès, le contrôle d'accès,la gestion des clés, l'anonymat, position/emplacement, complexité de calcul faible, auto-stabilisation, tolérance aux pannes et relations de confiance. [Abderrazak Rachedi,2008]

4 Classification des attaques dans les réseaux Ad hoc

Dans ce type de réseaux, la nature du support de transmission rend les réseaux plus vulnérables aux attaques. On peut classer les attaques dans ces réseaux en deux grandes catégories: les attaques actives et les attaques passives. [Lazib Nassim et al.,2013].

4.1 Les attaques actives

Un intrus tente de supprimer ou modifier les messages transmis sur le réseau. Il peut aussi injecter son propre trafic ou rejouer d'anciens messages pour perturber le fonctionnement du réseau ou provoquer un déni de service. [Lazib Nassim et al.,2013].

4.2 Les attaques passives

Les attaquants se limitent à l'écoute et l'analyse du trafic échangé. Ce type d'attaques est plus facile à réaliser (il suffit de posséder le récepteur adéquat) et il est 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. [Lazib Nassim et al.,2013].

En plus de cette classification, on peut citer encore deux autres classifications, la première classification se base sur l'objectif de l'attaquant, où on peut distinguer une attaque malveillante et une attaque rationnelle. Un attaquant malveillant n'a pas d'intérêts personnels à travers ses attaques et a pour but le dysfonctionnement du réseau. Par conséquent, il peut employer tous les moyens sans tenir compte des coûts

correspondants et des conséquences. Par contre, un attaquant rationnel cherche un profit personnel, et ainsi, on peut prévoir les cibles d'attaques et les moyens employés. [Lazib Nassim et al.,2013].

La dernière classification est ce qu'on nomme Interne vs. Externe : l'attaquant interne est perçu comme un membre normal du réseau et peut communiquer avec les autres membres. La présence des attaques internes est très problématique et difficile à détecter, car elle annule le niveau de sécurité assuré par les techniques cryptographiques. L'attaquant externe est considéré par les nœuds membres comme un intrus, et il est donc limité dans la diversité des attaques qu'il peut provoquer [Lazib Nassim et al.,2013].

5 Les attaques possibles dans les réseaux Ad hoc

Pour assurer une communication efficace dans ces réseaux, plusieurs protocoles de routage ont été conçus, mais ces réseaux sont vulnérables à plusieurs menaces en présence de nœuds malveillants. Donc les réseaux ad hoc ont besoin de sécurité pour mettre en œuvre l'environnement sans fil et servir les utilisateurs avec des applications sécurisées. Sans les mesures de sécurité adéquates dans le réseau, les informations peuvent ne jamais arriver à destination, ou devenir des menaces et devenir la cause d'accident [Ines Chihi,2017].

Dans cette section, nous examinons quelques attaques de routage dans ces réseaux.

5.1 L'attaque Déni de Service (DoS)

Selon [Sumra, LA., et al,2011], le but de ce type d'attaque est de rendre le réseau dysfonctionnel. L'attaque Déni de Service (DoS) consiste à rendre les différentes ressources indisponibles. Dans ce type d'attaques, l'entité malveillante peut bloquer le canal après la transmission des messages falsifiés et donc, interrompre la connexion réseau. L'attaque Déni de service peut être générée en diffusant à plusieurs reprises des faux messages avec des signatures non valides pour consommer la bande passante ou d'autres ressources du nœud ciblé.

5.2 L'attaque Black Hole (Trou noir)

Selon [Al-kahtani,2012], l'attaque « Black Hole » est dûe à un nœud malveillant qui prétend avoir une route optimale pour la destination et qui indique que le paquet devrait être acheminé par lui en transmettant de fausses informations de routage. L'impact de cette attaque est que le nœud malveillant peut soit détruire ou utiliser improprement les paquets interceptés sans les transmettre.

5.3 L'attaque « Worm Hole » (Trou de vers)

Dans [Perrig et Johnson,2003] un nœud malveillant reçoit les paquets de données à un point dans le réseau et les retransmet à un autre nœud malveillant en utilisant un lien «Worm Hole» à haut débit (tunnel) et par conséquence la communication de la source vers la destination passe par ces nœuds malveillants. L'impact de cette attaque est qu'elle empêche la découverte de routes valides et menace la sécurité de la transmission de paquets de données.

5.4 L'attaque « Sinkhole »

Dans [Ngai et Lyu,2006] ont définit l'attaque « Sinkhole » comme un nœud malveillant qui diffuse des fausses informations de routage de sorte qu'il peut facilement attirer tout le trafic réseau vers lui. L'impact de cette attaque est qu'elle rend le réseau compliqué et dégrade les performances du réseau, soit en modifiant les paquets de données ou en les détruisant.

5.5 L'attaque Sybil

Pour les chercheurs[Douceur, J.R.,2002],une attaque Sybil est un nœud malveillant qui crée un grand nombre de fausses identités afin de prendre le contrôle de tout le réseau et injecte de fausses informations dans le réseau afin d'endommager les nœuds légitimes. L'attaque Sybil a un fort impact sur la performance du réseau en créant une illusion sur l'existence de plusieurs nœuds dans le réseau. L'impact de cette attaque est que, après la falsification des identités ou des positions des autres nœuds dans le réseau, cette attaque peut conduire à d'autres types d'attaques.

6 Le problème du trou noir (BLACKHOLE)

Afin de comprendre cette attaque sur les réseaux Ad Hoc et les solutions proposées contre cette attaque, il est nécessaire de comprendre le fonctionnement général de protocole de routage.

On va étudier l'impact de cette attaque sur un protocole qui se basent sur des informations sur la topologie du réseau. Plusieurs protocoles de routages sont concernés par la notion de sécurité (AODV, DSR,TORA...), dans cette section nous donne une définition globale sure le protocole de routage AODV qu'on va utiliser dans notre implémentation.

6.1 Le fonctionnement général du protocole AODV

Ad hoc On demand Distance Vector (AODV) est un protocole de routage réactif ce qui signifie que les routes sont construites à la demande, si un nœud source veut envoyer des paquets de données vers un nœud destination, il doit établir et maintenir une route vers ce nœud destination durant le temps qu'il en fait usage. [Houda Hafi, 2010].

Le protocole AODV est basé sur l'utilisation des deux mécanismes "Découverte de route" et "Maintenance de route" (utilisés par le DSR), en plus du routage nœud-par-nœud, le principe des numéros de séquence et l'échange périodique du DSDV. Il utilise trois types de paquets de routage à savoir : RREQ (Route REQuest), RREP (Route REPly), RERR (RouteERRor).

6.1.1 Découverte des routes :

Avec le protocole AODV, chaque nœud doit maintenir une liste de ses voisins actifs. Cette liste est obtenue par un échange périodique des messages HELLO de chaque nœud avecses voisins immédiats. Quand un nœud source S veut envoyer des données à un destinataire Det qu'aucune route vers cette destination n'est stockée dans la table de routage de la source, lenœud S initialise une procédure de découverte de routes.

La source S envoie à ses voisins une demande de route RREQ qui contient l'adresse de S, l'identifiant de la requête, un compteur de séquence, l'adresse de D et

le compteur de nombre de sauts avec une valeur initiale zéro. 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 le RREQ et attend une période plus grande si aucune réponse n'est reçue, elle continuera la rediffusion du RREQ jusqu'à un nombre maximum de tentatives RREQ_RRTRIES (03 tentatives), si après RREQ_RETRIES tentatives d'établissement de route, il n'y a aucune réponse alors le processus est abandonné et un message d'erreur est signalé à l'application.

Après une certaine période d'attente (10 s), l'application demande la route et par conséquent l'opération de découverte de route est initiée. Chaque nœud qui reçoit le message RREQ recherche dans sa table de routage locale s'il existe une route vers le nœud D sinon le nœud qui traite la requête RREQ incrémente le nombre de sauts et la diffuse à nouveau. Lorsque la requête atteint la destination D ou un nœud qui connaît une route vers la destination, une réponse RREP est diffusée sur la même route de réception du RREQ (chemin inverse). La réponse RREP contient l'adresse source, l'adresse de destination, le nombre de sauts, un numéro de séquence de destination et la durée de vie du paquet. 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 [Houda Hafi, 2010].

6.1.2 Maintenances des routes

L'échange des messages HELLO entre les voisins immédiats permet de mettre à jour la liste des voisins de chaque nœud. Lorsqu'un nœud N détecte qu'un autre nœud Q n'est plus accessible(Q a quitté le réseau ou est hors porté radio), N procède à une mise à jour des liens dans sa table de routage. En effet, il recherche dans sa table de routage toutes les routes qui passent par le nœud Q et les détruit avant d'annoncer à ses voisins actifs que la route passant par le nœud Q n'est plus valide. Un message RERR est envoyé alors au nœud source. Ainsi, la mise à jour est diffusée à travers le réseau saut par saut et le nœud source initie une nouvelle procédure de recherche de route vers la destination. [Houda Hafi, 2010]

6.2 L'attaque du trou noir

Dans l'article [Houda Hafi, 2010] nous avons trouvées la description du problème du trou noir qui la suivante:

L'attaque de trou noire (BLACKHOLE en anglais) est une attaque de type DOS (Denial Of Service), dans laquelle un nœud corrompu utilise la vulnérabilité de route, pour découvre les paquets de protocole de routage a objective d'annoncer qu'il a le plus court chemin vers le nœud qui va intercepte les paquets.

Cette attaque vise à modifier le protocole de routage, donc ce trafic dérouler à travers un nœud spécifique qu'est contrôlé par l'attaquant. Pendant le processus de la découverte de la route, le nœud source envoyer un paquet de type RREQ(Route REQuest) vers les nœuds intermédiaires pour trouver un chemin frais vers la destination. Le nœud corrompu repend immédiatement la source que ces nœuds non pas réfère la table de routage.

Le nœud source suppose que le processus de la découverte de la route est complet, alors il ignore les autres RREP(Route REPly) messages des autres nœuds et sélectionne la route à travers le nœud corrompu pour envoyer les paquets. Le nœud corrompu fait ça par assignation d'un numéro de séquence élevé du paquet de repense. L'attaquant effacer les messages reçus à la place de retransmettre le, comme les conditions du protocole dit.

La figure ci-dessous illustre cette attaque où la source S veut transmettre des données vers la destination D, elle diffuse une requête RREQ, le paquet RREQ va être reçu par les nœuds N1,N2, N3.

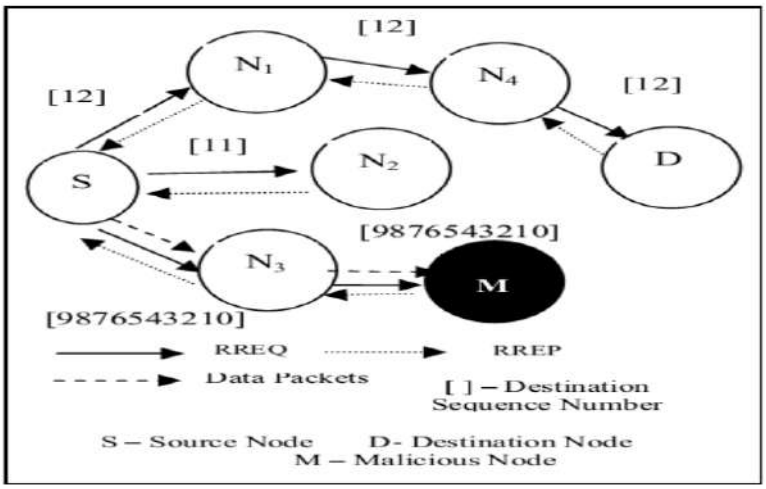

Figure 2.9: L'attaque Blackhole.

Supposons le nœud N3 a une route vers la destination dans sa table de routage, le nœudN3 génère un paquet de réponse RREP et mettre à jour sa table de routage par le nombre de sauts et le numéro de séquence de la destination.

Le numéro de séquence de la destination est un entier de 32 bits associé à chaque route et permet l'utilisation des routes les plus fraîches autrement dit les plus nouvelles. Une route estjugée fraîche que si la base du numéro de séquence de la destination est assez élevée. Le nœud N3va envoyer le paquet vers le nœud M, tant que les nœudsN1 et N2 n'ont pas une route vers la destination D, ils seraient à nouveau diffusé le message de contrôle RREQ.

Ainsi le paquet RREQ diffusé par le nœud N3devrait également être reçu par le nœud M (supposons M est un nœud malicieux). Donc le nœud M va générer un faux message de contrôle RREP et l'envoyer au nœud N3 avec un numéro de séquence de destination très élevé, qui serait ensuite envoyé au nœud S.

Cependant, tant que le numéro de séquence de destination est élevé, la route à partir du nœud N3 sera considéré comme plus fraiche et donc la source serait commencée à envoyer des paquets de données au nœud N3. Le nœud N3 serait envoyer les mêmes paquets au nœud malicieux. Le message de contrôle RREQ à partir du nœud N1, finirait par atteindre le nœud D(nœud de destination), ce qui générerait un message de contrôle RREP et la route du retour.

Toutefois, le nœud S a déjà reçu un paquet de réponse RREP avec numéro de séquence supérieur à celui de D, le nœud S ignore les deux véritables messages de

contrôle RREP. Pour chaque message de contrôle RREP reçu, la source devrait d'abord vérifier si elle possède une entrée pour la destination dans la table de routage ou non. S'il en trouve un, le nœud source vérifie si le numéro de séquence de destination dans le message de contrôle reçu est plus élevé que celui qu'il a envoyé dans la dernière RREQ ou non. Si le numéro de séquence de destination est plus élevé, la source met à jour sa table de routage avec le nouveau message RREP, sinon le message de contrôle RREP sera rejeté.

7 Etat de l'art

Au cours de la recherche bibliographique de ce mémoire, nous avons trouvées plusieurs études sur ce problème et des solutions proposées pour empêcher cette attaque, nous résumons les dans les paragraphes suivants.

[DengH et al.,2002] ont proposé une solution contre l'attaque 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 (FurtherRequest) afin de vérifier qu'il possède une route vers le nœud intermédiaire qui a envoyé le message de réponse, et qu'il a aussi une route vers le nœud destination. Le «next hop» répond avec un paquet de réponse de route (FurtherReply) qui comprend le résultat de contrôle. 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 reçue 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 et al.,2004] ont proposé deux solutions conçues pour cibler l'attaque blackhole 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 destination 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 des 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 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 inclus dans l'en-tête de chaque paquet. Le nœud dans cette situation a besoin d'avoir deux tables supplémentaires; la première table comprend les numéros de séquence du dernier paquet envoyé à chaque nœud dans le réseau. 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. Si ce n'est pas,

ce nœud est un nœud malveillant, alors un message d'alarme sera diffusé pour avertir le réseau sur ce nœud. Toutefois, les deux solutions ont le délai de bout en bout comme inconvénient.

[Houda Hafi, 2010] proposa un protocole basé sur l'utilisation d'un modèle de confiance capable d'assurer les échanges sécurisés dans les réseaux sans fil P2P. Dans le modèle proposé, et 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 l'une des équations ci-dessous, selon les valeurs stockées dans cette table, il décide si le nœud est un nœud de confiance ou bien non.

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, par conséquent, si on suppose que:

NB-D : le nombre des paquets de données reçus d'un nœud X

NB-RREQ : le nombre des paquets RREQ reçus d'un nœud X

NB-RREP : le nombre des paquets RREP reçus d'un nœud X

Si (NB-D+NB-RREQ > NB-RREP) alors : X est un nœud de confiance

Si ((NB-D+NB-RREQ != 0) and (NB-RREP >NB-D+NB-RREQ)) alors : X est un nœud connu

Si (NB-D+NB-RREQ=0) alors : X est un nœud inconnu et peut être un nœud BLACKHOLE

Dans ce qui suit, nous présentons l'idée générale du protocole:

Step 1: Le nœud source S commence la phase de découverte de route

Step 2: Chaque nœud intermédiaire reçoit un RREQ stocke le numéro de séquence de la source(SSN)

Step 3: Quand un nœud intermédiaire reçoit un RREP, il vérifie d'abord si le nœud existe dans le blackhole, si la condition est vraie, il le supprime directement. Sinon il passe à l'étape 4

Step 4: Dans cette étape il vérifie un bit rajouté au format du paquet RREP, pour éviter que plusieurs nœuds vérifient plusieurs fois le même paquet.

Si (le bit = 1) alors :

- Le RREP a été déjà vérifié par un nœud et le nœud suivant n'aura plus besoin de revérifier le paquet (dans ce cas le nœud est jugé soit de confiance, soit connu)

- Rediffuser RREP vers la source

Sinon (le bit =0)

Switch Etat du nœud

Case 1: Le nœud est jugé de Confiance

- Mettre le bit = 1

- Rediffuser RREP vers la source

Case 2 : Le nœud est jugé Connu

- Mettre le bit = 1

- Rediffuser RREP vers la source

Case 3 : Le nœud est Inconnu (Route non sécurisé, et le nœud peut être un blackhole)

Si (DSN>>SSN) (pour confirmer)

- Il ne le renvoie pas à la source

- Ajouter le nœud au black List

- Supprimer le RREP

Sinon

- Mettre le bit = 1

- Rediffuser RREP vers la source

Fin si

[Irshad. U et al.,2010] ont fait une étude sur l'attaque de trou noir dans les réseaux Mobile Ad hoc (MANET). Ils ont proposé comme solution l'utilisation de deux protocole de routage proactif : comme OLSR et réactif comme AODV, ensuite ils ont comparé les résultats des deux protocoles. Ils se sont basés sur le fait " les réseaux Mobile Ad hoc fonctionnent sans un administrateur central, cette caractéristique vulnérable peut être exploitée par un attaquant au sein de réseaux". Les chercheures ont utilisé le simulateur OPNET comme l'outil de mesure de performance du réseau Ad hoc. Le résultat de cette étude est la simulation de l'attaque de trou noir par l'AODV et OLSR et prendre les critères Delay, Throughput, Network Load, comme des critères de mesure de l'effet de l'attaque de trou noir.

[Subash Chandra Mandhata et al. 2011] ont présenté un algorithme pour détecter l'attaque 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 paquets) 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 soupçonné d'être un nœud malveillant et 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.

[H. A. Esmaili et al,2011] ont fait une étude sur la performance du protocole de routage AODV sous l'attaque de trou noir, ils proposèrent la mesure de l'effet de l'attaque du trou noir sur le réseau ad hoc à l'aide d'AODV comme un protocole de

routage. Les chercheurs ont utilisé la simulation comme l'outil de mesure de performance de réseau Ad hoc, et ils ont choisi l'outil de simulation de réseau OPNET. Les résultats de cette étude sont résumés dans les point suivants:

- Simulation d'un seul nœud malicieux dans un environnement de 46 nœuds mobiles

- Simulation de deux nœuds malicieux dans le même environnement

- Simulation de trois nœuds malicieux dans le même environnement

- Simulation de quatre nœuds malicieux dans le même environnement

[Romina Sh et al,2011] ont fait une étude sur le protocole de routage AODV dans les réseaux mobile Ad hoc, ils proposèrent de "modifier le protocole de routage AODV pour empêche l'attaque du trou noire et muserai l'impact de l'attaque du trou noir sur les réseaux mobile Ad hoc et compare avec le protocole modifie de AODV" à partir d'un problématique "à cause du vulnérabilité de sécurité de protocole de routage, les réseaux mobiles Ad hoc ne sont pas protégés de l'attaque de nœud malicieux, comme l'attaque de trou noir". Les chercheurs utilisent le simulateur OPNET comme l'outil de mesure de performance de réseau Ad hoc. Les résultats de cette étude sont résumés dans les trois point suivant:

- Simulation du protocole de routage AODV sans l'attaque de trou noir.

- Simulation de l'attaque du trou noire dans les réseaux mobiles Ad hoc

- Simulation de l'algorithme pour empêcher l'attaque de trou noire.

[Nisha et al,2016] ont misé sur l'une des premières techniques appliquée dans les réseaux : la détection de l'intrusion qui s'appuie sur la collecte d'informations réseau et sur leur audit. Ce système, IDS, contrôle la circulation des paquets. Chaque nœud mobile exécute IDS indépendamment des autres pour observer le comportement des nœuds voisins, cherchant localement des signes d'intrusion, et prenant la décision pour avertir le système de toute attaque comme il peut aussi demander des données des nœuds voisins.

Leur test a été exécuté comme suit : un blackhole envoie un message RREP sans vérifier les tables, avec l'aide d'IDS il va vérifier le paquet RREP du nœud

blackhole pour le chemin minimal et le numéro de séquence le plus élevé. IDSAODV va supprimer la première requête RREP du blackhole et choisir un autre paquet de la destination., comme il va aussi trouver un autre chemin vers la destination.

8 Conclusion

À partir de ce chapitre, on peut considérer que la sécurité des réseaux décentralisés consiste en six types d'opération: authentification d'un utilisateur, intégrité des données, la disponibilité, confidentialité des données, la non-répudiation et le contrôle d'accès. Malgré sa, les réseaux sans fil décentralisés restent toujours vulnérables à des attaques comme l'attaque de trou noir qui a un grand effet sur le déroulement de réseau à cause de l'environnement ouvert de ces réseaux. Pour cela, plusieurs recherches ont été développés pour trouver des solutions à ce problème.

Dans le chapitre suivant, nous essayons de proposer un modèle de simulation pour l'attaque de trou noir sur un réseau ad hoc avec le protocole AODV et un modèle de simulation pour la même attaque avec un protocole AODV modifié et le proposer comme une solution de ce problème, en utilisant le simulateur de réseau NS 2.

Chapitre III

Implémentation

1 Introduction

L'état de l'art dans le chapitre précédent a présenté un échantillon des solutions au problème de l'attaque blackhole qui constitue une menace courante pour les réseaux sans fils décentralisés. Dans ce chapitre nous allons présenter notre contribution, à la hauteur de notre compréhension et de nos moyens. Nous commençons par l'environnement de travail qui va nous permettre d'implémenter et l'attaque et sa solution, puis nous décrivons le simulateur utilisé à cette fin ainsi que le script de la simulation à appliquer pour avoir les résultats des scénarii destinés à voir les effets de l'attaque et de la solution proposée.

2 L'environnement de travail

Pour réaliser ce travail de recherche, nous avons testé différents systèmes d'exploitation et différents simulateurs. Ainsi, Windows n'a pas été encourageant, de même le simulateur OMNET++ (versions 4.3,4.4 et 5.0). Mais, Linux dans sa version Ubuntu 14.04 et Network Simulator NS 2.35 (patché à IDSAODV) ont donné des résultats.

3 Présentation du simulateur NS 2

NS2 (Network Simulator 2) est un outil de simulation open-source qui fonctionne sous Linux et Windows (Cygwin). Implémenté en C++ et OTcl (Object Tool Command Language), en C++ il prend en charge les fonctions de bas niveau et en OTcl il fait office d'interface avec les autres langages.

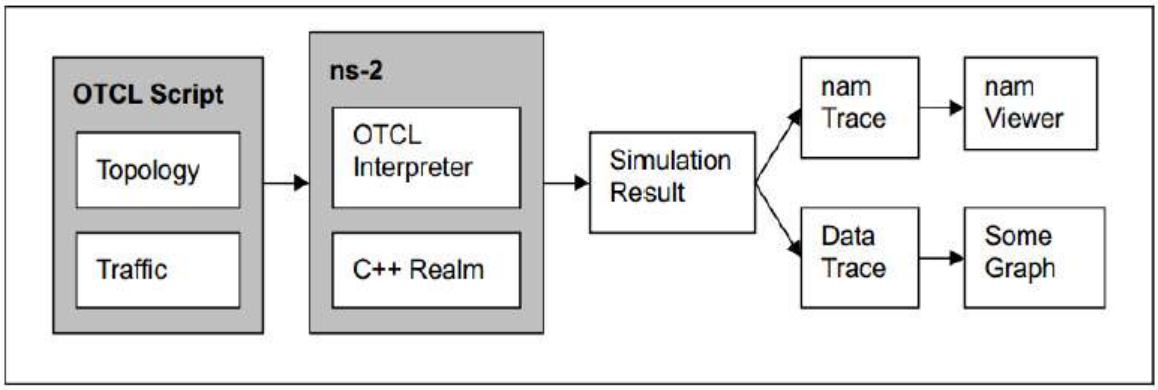

Figure 10: Architecture de NS 2

L'OTcl sert à décrire la topologie du réseau (nœuds, liaisons) et du trafic réseau (cheminement des paquets). NS2 interprète les scripts TCL et utilise la base de données de C++ sur les réseaux (C++Realm), il s'occupe ainsi des protocoles, des couches réseau et de leur simulation.

Le fonctionnement général de ce système se présente comme suit :

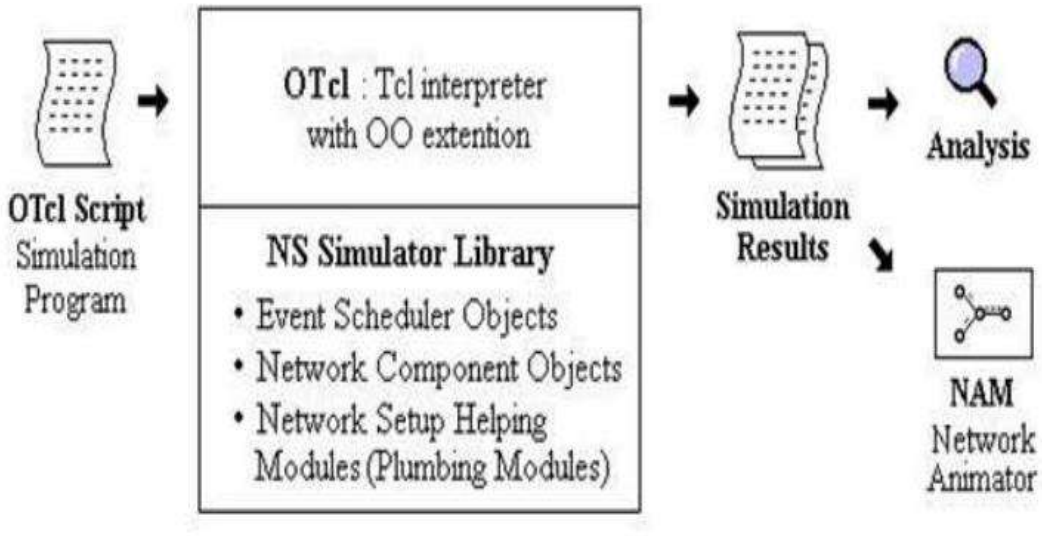

Figure 3.2: Détail de fonctionnement du système OTcl – NS2.

4 Description d'une simulation

Le script OTcl est un fichier.TCL généré par un quelconque éditeur de texte et interprété par l'OTcl, il comprend en général les parties suivantes :

4.1 Définition des options de simulation

Les options de simulation sont : le canal de transmission, le modèle de propagation, le type d'antenne, le type de couche liaison, type de file d'interface, le nombre maximum de paquets dans la file, le type d'interface réseau, le type MAC, le protocole de routage et le nombre de nœuds mobiles.

La définition de chaque option se fait par la commande set val () pour affecter une valeur à la variable qui lui correspond.

Exemple : set val(ll) LL, affecte à la variable ll relative au type de couche de liaison la valeur LL.

Cette partie est obligatoire au début de chaque simulation car tout nœud mobile se compose des éléments réseau détaillésen la figure suivante :

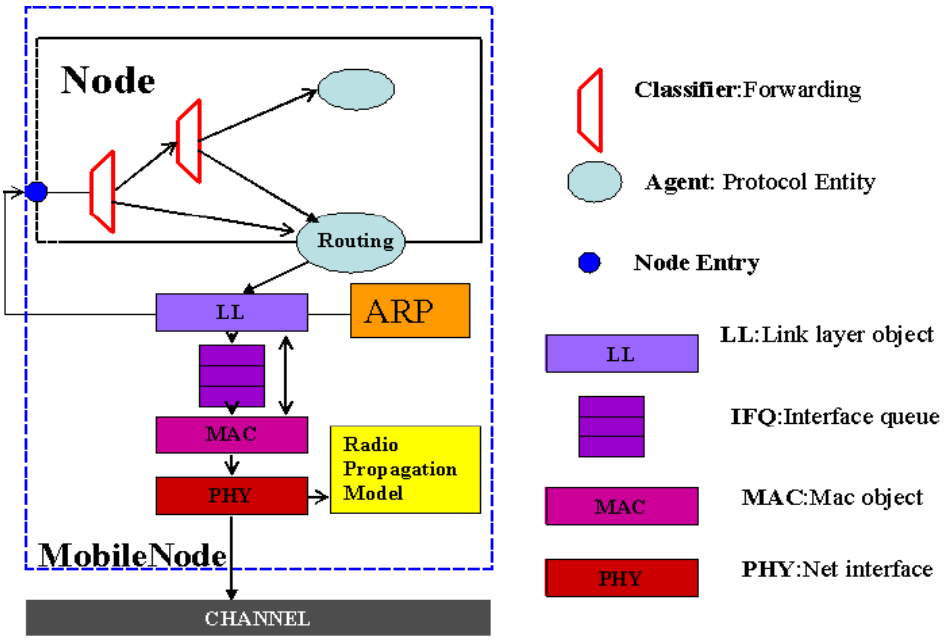

Figure3.3: Composants réseau d'un nœud mobile

4.2 L'initialisation des variables globales

-une nouvelle instance du simulateur : set ns_ [new simulator]

-l'option de traçage : $ns_ use-newtrace , nouvelle trace des événements

-créer le fichier trace : set tracefd [open fichiertrace.tr w]

-comment écrire dans le fichier trace : $ns_ trace-all &tracefd

-comment créer la trace d'une animation : set namtrace [open nomfichier.nam w]

-comment écrire dans le fichier animation : $ns_ namtrace-all-wireless $namtrace $val(x) $val(y)]

-préciser la topographie et l'initialiser : set topo [new Topography]

$topo load_flat_grid 500 500

-créer un gestionnaire des opérations : create-god $val(nn), nn=nombre de nœud ;

Cette commande est essentielle car elle attache les nœuds au canal décrit plus haut.

4.3 La configuration des nœuds

La configuration des nœuds utilise les options de simulation comme suit :

```
set chan_1_ [new $val(chan)]

$ns_ node-config -adhocRouting $val(rp) \

                          -llType $val(ll) \

                          -macType $val(mac) \

                         -ifqType $val(ifq) \

                          -ifqLen $val(ifqlen) \

                         -antType $val(ant) \

                          -propType $val(prop) \

                          -phyType $val(netif) \

                          -channel $chan_1_ \

                          -topoInstance $topo \

                          -agentTrace ON \

                          -routerTrace ON \

                          -macTrace OFF \

                          -movementTrace ON


# Pour créer les nœuds avec les paramètres spécifiés

for {set i 0} {$i < $val(nn) } {incr i} {

      set node_($i) [$ns_ node]

      $node_($i) random-motion 1;# enablerandom motion

       }
```

4.4 Autres déclarations et initialisations

Les positions initiales des nœuds doivent être déclarées, au moyen de leurs coordonnées, X, Y et Z (si nécessaire), par la commande $node_(n) set X_ 50.0 par exemple ;

Déclarer les couleurs des nœuds, si nécessaire, par

```
$ns_ at .01 "$node_(1) colorblue" ;
```

Décrire la mobilité des nœuds : **#Set destination format is "setdest<x><y><speed>"**

$ns_ at 0.01 "$node_(0) setdest 50.0 50.0 0.0"
$ns_ at 5.0 "$node_(0) setdest 350.0 350.0 0.0"
$ns_ at 6.0 "$node_(0) setdest 1.0 350.0 0.0"
$ns_ at 7.0 "$node_(0) setdest 50.0 50.0 0.0"

Et autres opérations.

5 Lescaractéristiques du protocole AODV

5.1 Principales fonctionnalités

5.1.1 Les fonctions de gestion de la table de routage :

rt_resolve (Packet *p) : résolution de paquets ;

rt_update : mis-à-jour de la route ;

rt_down : annuler route ;

rt_local_repair : initialiser le paquet et marquer la route et envoyer RREQ ;

rt_ll_failed : échec de route ;

5.1.2 Gestion des voisins (neighbors)

nb_insert : insérer un voisin ;

AODV_Neighbor*nb_lookup : chercher un voisin ;

nb_purge : purger les voisins ayant de très long délais d'attente ;

5.1.3 Gestion de la diffusion (broadcast) ID

forward : transférer/dispatcher les paquets

sendHello : envoyer message d'aknowlegdment

sendReply : envoyer des réponses

sendError : envoyer un message d'erreur

5.1.4 Gestion de la réception de paquets

AODV ::recvAODV : classer les paquets entrants

AODV ::recvRequest , si un nœud reçoit un paquet de type REQUEST, il fait appel à cette fonction

AODV ::recvReply , si un nœud reçoit un paquet de type REPLY , il appelle cette fonction

AODV ::recvError : utilisée si un nœud reçoit un message ERROR

AODV ::recvHello : à la réception d'un message HELLO , commence la recherche dans la liste des voisins, si non présent il est inséré dans la table de routage

5.2 Le messaging

AODV procède par échange de messages, qui est une qualité de tout agent.

Quatre types de messages sont lui sont associés :

-HELLO : bienvenue, qui est l'équivalent de ACK (aknowledgment) classique :

-RREQ : Route Request : demande de route ;

-RREP : Route Reply : réponse de route ;

-RERR : Route Error : erreur de route.

5.3 Structures de RREQ et de RREP

- Format de RREQ

Scr_ Address	Scr_ Sequence	Broad cast_id	Dest_ Address	Dest_ Sequence	Hop Count

Figure 3.4: Structure d'une demande de route

- Format de RREP

Scr_ Address	Dest_ Address	Dest_ Sequence	Hop Count	Life Time

Figure 3.5: Structure d'une réponse de route

5.4 Les modes de propagation

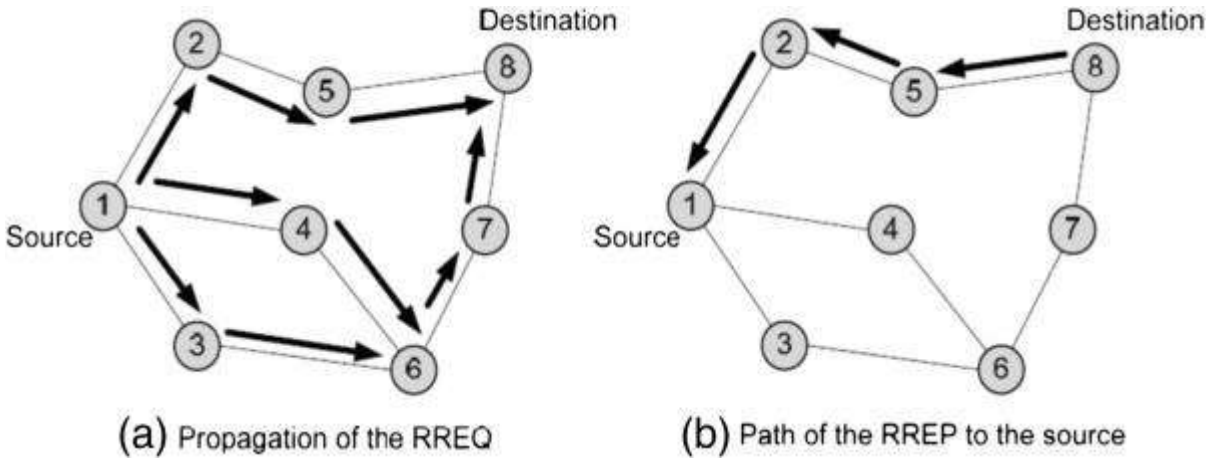

Figure 11: Modes de propagation de RREQ et RREP selon AODV.

6 L'attaque BlackHole dans le protocole AODV

6.1 Principe de suppression de paquets

L'attaque BlackHole (trou noir)ousuppression de paquets (packetdropping) résulte d'une fausseRREQ comportant un très grand numéro de séquence et émise par le nœud malicieux. Le nœud source insère ce numéro dans la table de routage et le considère comme le plus court chemin vers la destination en ignorant les paquets des autres nœuds donnant ainsi la chance au nœud malicieux d'être sa destination préférée et continue de lui envoyer des paquetsque ce dernier supprime, donc n'arrivant jamais aux autres.

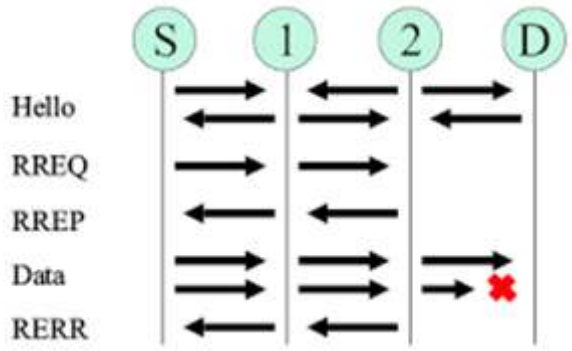

Figure 3.7 : Comportement d'un nœud malicieux

6.2 Effets du blackhole

Le blakhole affecte les métriques du réseau, en particulier il cause des modifications sures :

-le débit (Throughput) ;

-le délai entre la source et la destination (End-to-End Delay) :

-le taux ou la fraction de livraison de paquets (Packet Delivery Ratio/Fraction) .

6.3 L'implémentation d'un nœud malicieux

L'implémentation d'un nœud malicieux nécessite la mise-à-jour des fichiers dépendants (dependencies) du protocole AODV, ces fichiers dépendants sont montrés dans les figures suivantes :

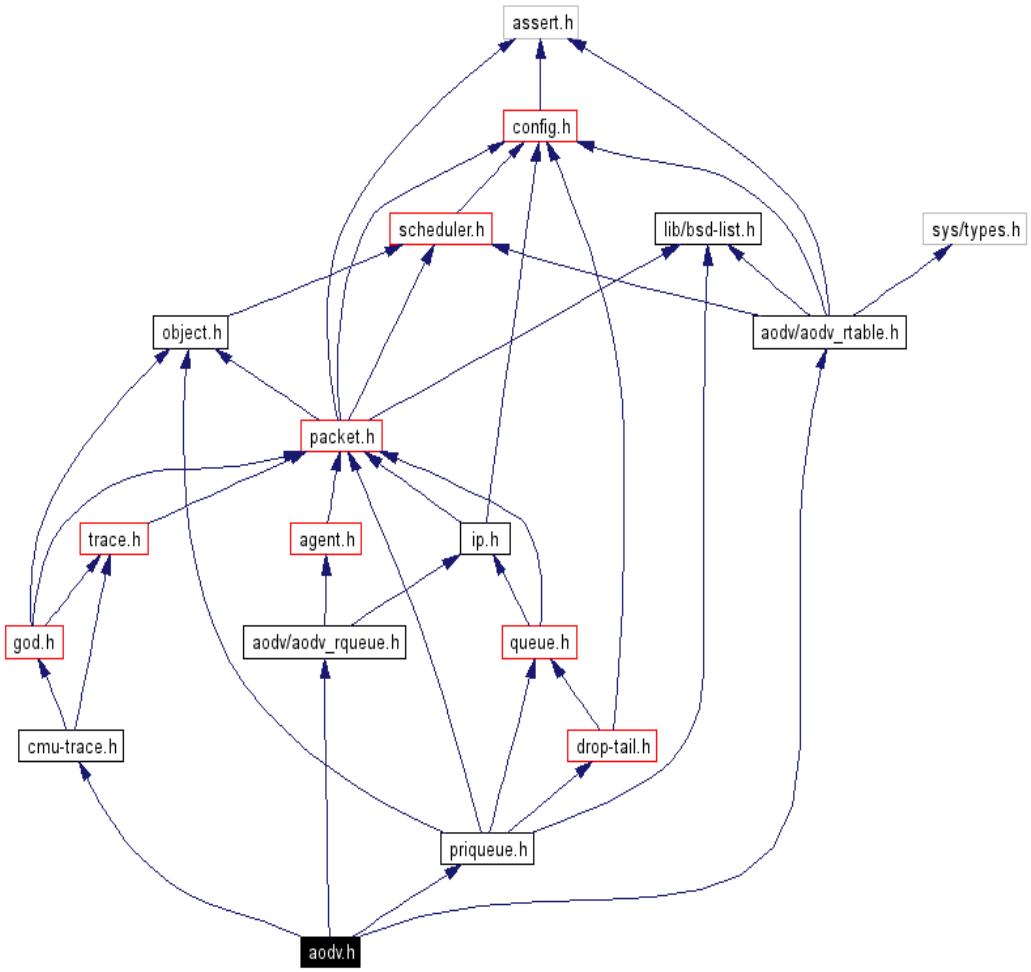

Figure 12.8: Fichiers dépendants de aodv.h

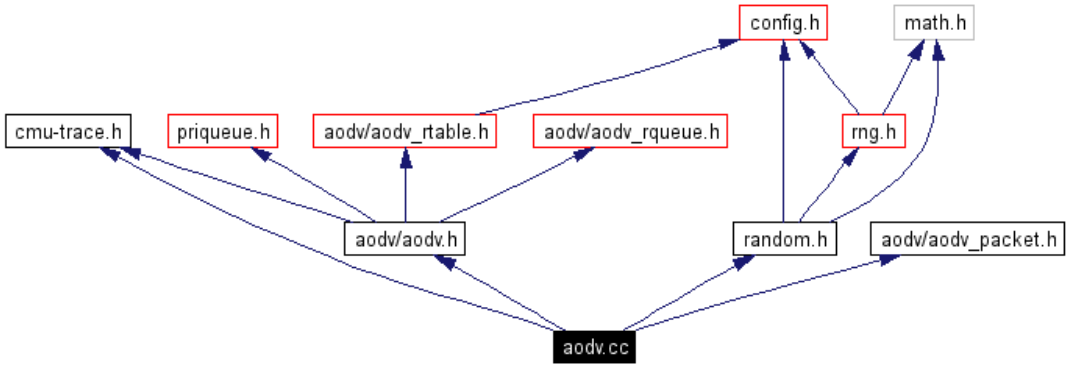

Figure3.9: Fichiers dépendants de aodv.c

Dans le fichier*aodv.h* (header)

Lignes 215 ou 216, déclarer le nœud malicieux : **bool malicieux** ;

Dans le fichier aodv.cc (source c++) :

Fonction AODV : ligne 152, initialiser **malicieux = false ;**

Fonction command ; ligne 85, effectuer le test :

If (strcmp(argv[1], 'malicieux')==0)
{
Malicieux = true ;
Return TCL_OK ;
}

Fonction resolve, ligne 449, effectuer le test :

If (malicieux==true)
{
Drop(p,DROP_MAL) ;
}

Dans le fichier cmu-trace.h, ligne 81 définir :

#define DROP_MAL 'MAL'

Dans le fichier TCL, caractériser le nœud malicieux :

$ns_ at 0 0 '$node_(3) colorred'

$node_(3) color 'red'

$ns_ at 0 0 '[$node_(3) set ragent_] malicieux'

7 Les scénarii des simulations

Le scénario 1 : c'est le scénario dans lequel est injecté un nœudblackhole parmi les nœuds du réseau pour voir son comportement de par ses effets.

Le scénario 2 : c'est le scénario qui teste la solution IDS pour montrer qu'il neutraliseles effets du blackhole.

8 Les paramètres de simulation

Les deux scénarios ont été exécutés sous les paramètres suivants:

Paramètres	Définition
Protocole	AODV,IDSAODV
Couche MAC	IEEE 802.11
Durée de la simulation	20s
Mobilité des nœuds	Fixé
Zone de simulation	4000x2000
Taille des paquets	512 bytes
Sources de trafic	CBR/UDP
Nombre de nœuds	11
Version NS-2	2.35 patché

9 Les simulations

9.1 Blackhole en action

Figure3.10: Action du blackhole

9.2 Actions de l'IDS sur le blackhole

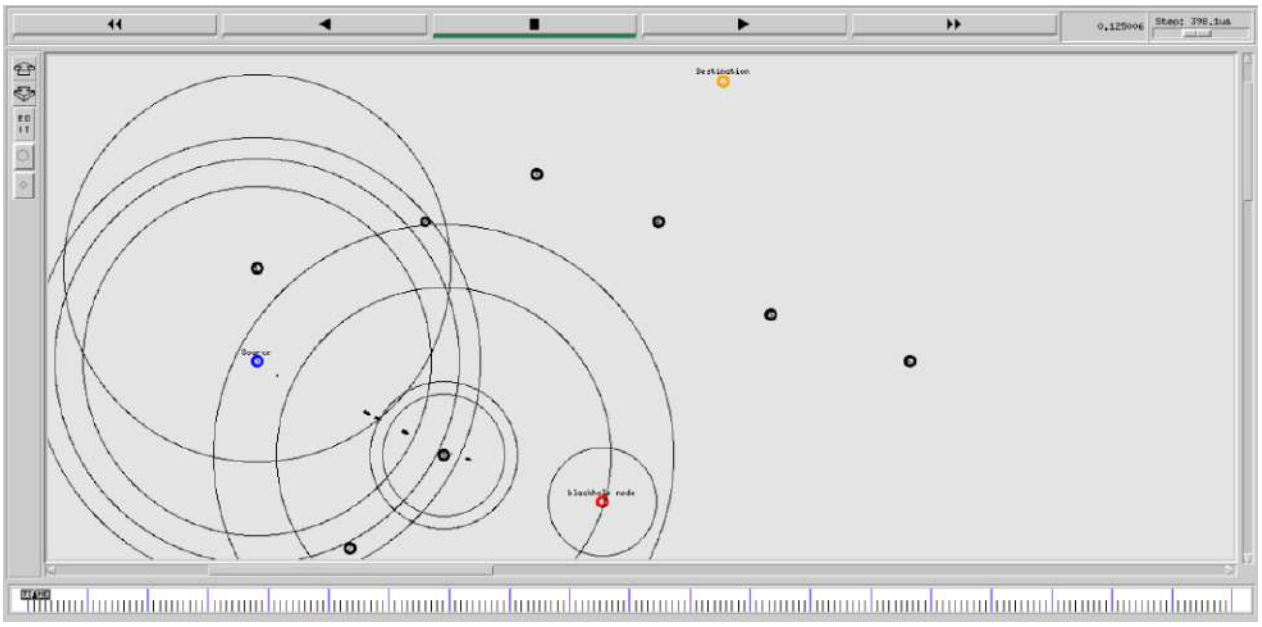

Figure3.11: L'IDS détectant le blackhole

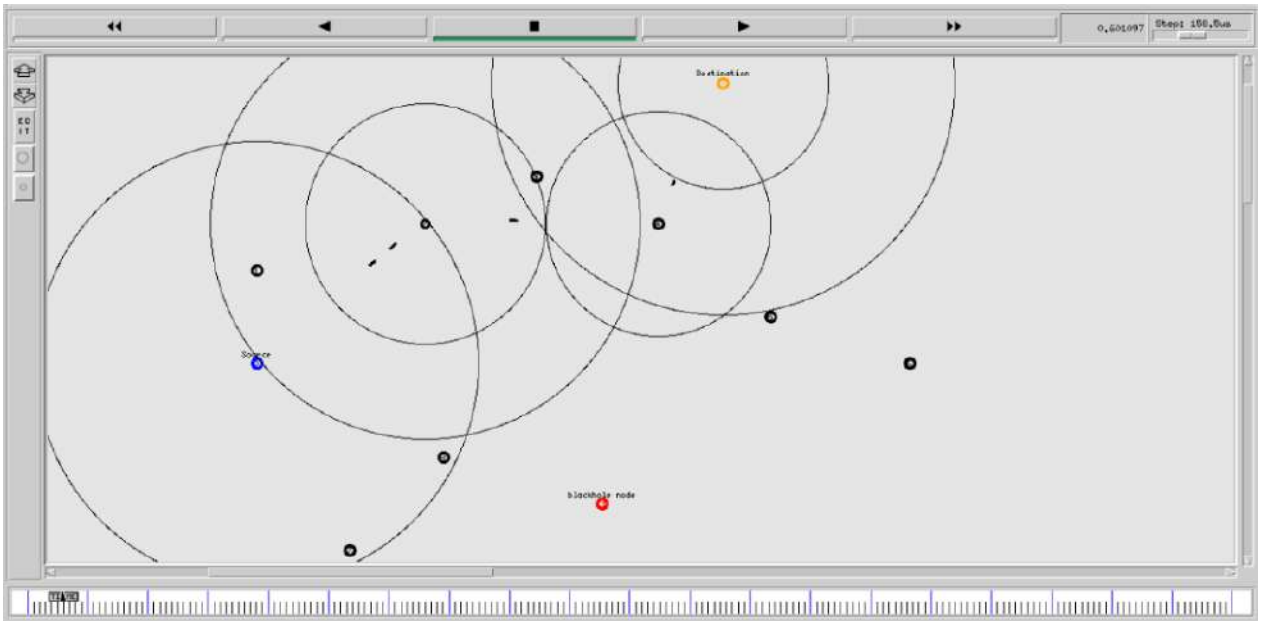

Figure 3.12: L'IDS changeant de route vers la destination

10 Le traçage

NS2 et OTcl donnent 2 formes de traces lesquelles sont définies dans un *fichier .tr*.

Ce fichier résultat a le format prédéfini suivant :

Event	Time	From node	To node	Pkt type	Pkt size	Flags	Fid	Src addr	Dst addr	Seq num	Pkt id

Figure 3.13: format d'un fichier trace

Où :

Event : type d'événement enregistré, il est l'une des quatre valeurs :

r : receive = réception ; + : enfilement ; - :défilement ; d :dropped = supprimé.

Time : temps où l'événement a eu lieu

FromNode : du Nœud, nœud en entrée de l'événement

To node, vers Nœud, nœud en sortie de l'événement

Pkt type : type de paquet, par exemple CBR, TCP

Pkt size : taille du paquet, en octets

Flags : drapeaux, booléens

FiD : flow ID, identificateur de flux ;

SrcAdr : adresse source,donnée par node.port

Dest Adr : adresse de destination, donnée par node.port

SeqNumber : numéro de séquence du paquet dans la couche liaison

Pkt ID : numéro de paquet

11 Résultats

Après avoir procédé aux simulations, nous avons obtenu les résultats sous forme de métriques sujettes à des comparaisons entre les effets du blackhole et les effets de l'IDS sur le blackhole. Un moniteur Sink a été attaché au nœud destinataire N°10 pour quantifier les données reçues à son niveau et qui sont les suivantes, dans chaque cas:

11.1 Effets du blackhole

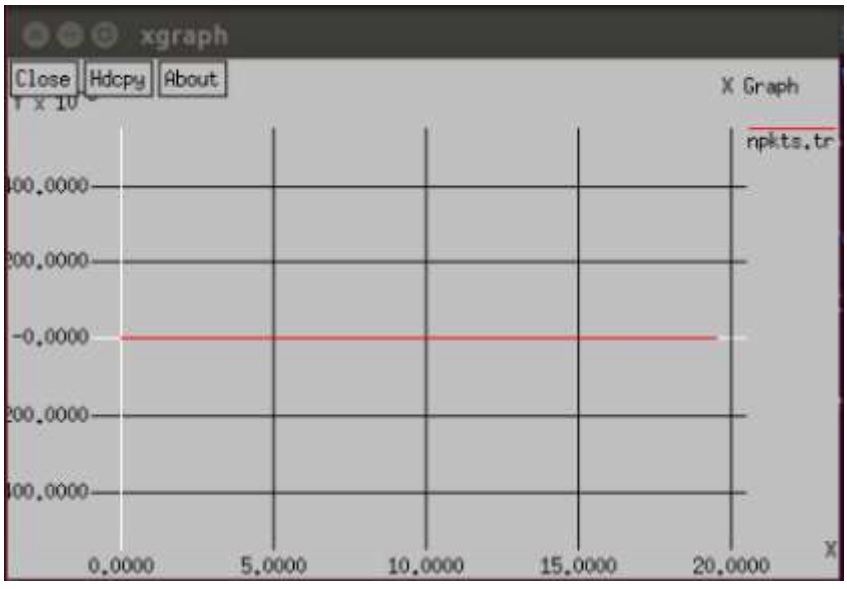

Figure3.14: Le nœud destinataire ne recevant aucun paquet

Interprétation :

Le blackhole a supprimé les paquets envoyés vers le nœud destinataire.

11.2 Effets de l'IDS

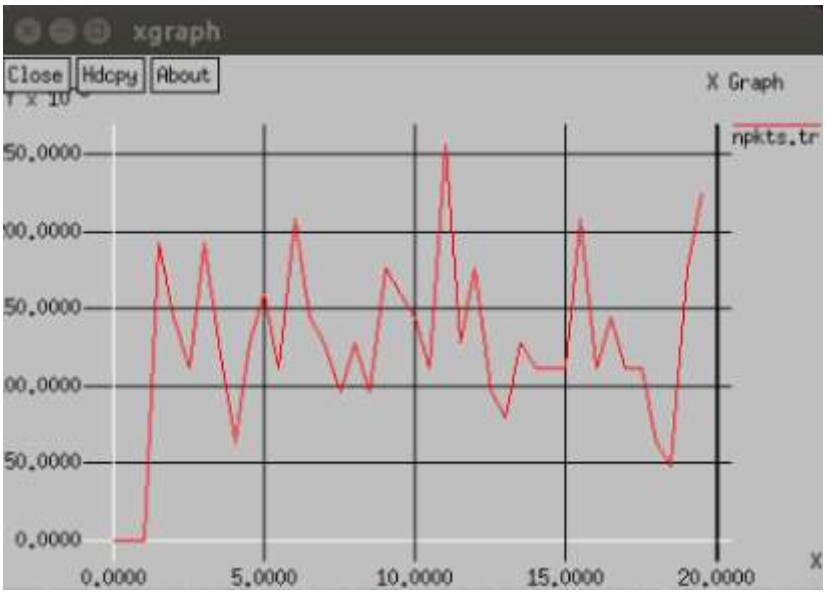

Figure 3.15: Le nœud destinataire recevant des paquets

***Interprétation* :**

Les paquets arrivent à leur destinataire, l'IDS a contourné l'attaque blackhole.

12 Conclusion

Dans ce chapitre, nous avons élaboré deux différents scénarios, l'un pour montrer les effets du blackhole, l'autre pour montrer les effets de l'IDS sur le blackhole. L'IDS a permis au nœud destinataire de recevoir des paquets en présence du blackhole, ceci confirme l'action préventive de l'IDS et sa capacité de conserver l'état normal du réseau.

Conclusion générale

Conclusion générale et perspectives

Les réseaux sans fil décentralisés sont l'option du futur en matière de coûts (sans infrastructure) et en connectivité. A l'opposé de ces avantages, l'inconvénient de la vulnérabilité risque de les anéantir. Aux diverses formes d'attaque auxquels ils peuvent être soumis se sont opposées des solutions.

Le présent travail a concerné l'une de ces attaques qu'est le blackhole (trou noir) et pour la comprendre de près, nous avons compris qu'elle se déroulait au niveau du protocole de routage et qu'elle est simulable, alors nous l'avons implémentée au même titre que sa solution.

Comme nous l'avons souligné au premier chapitre, les problèmes inhérents aux réseaux sans fils décentralisés sont assez sérieux et les touchent sur plusieurs plans laissant comprendre qu'ils resteront un domaine de recherche ouvert allant de leur conception jusqu'à leur exploitation.

Notre humble expérience nous a permis d'entrevoir des propositions pour l'avenir entre autres :

-auto-immuniser les protocoles ;

-doter les nœuds (en tant qu'agents) de la capacité de détection d'un voisin malicieux.

Références bibliographiques

[Abderrazak Rachedi,2008] Abderrazak Rached, Contributions à la sécurité dans les réseaux mobiles ad hoc,Université d'Avignon,2008.

[Al-kahtani,2012] Al-kahtani, M.S, "Survey on security attacks in Vehicular Ad hoc Networks(VANETs)", in Signal Processing and Communication Systems (ICSPCS), 2012 6thInternational Conference on, pp. 1-9, December 2012, Gold Coast, Australia. PrintISBN: 978-1-4673-2392-5.

[Al-Shurman et al.,2004] Al-Shurman M, S Moo Yoo and S.Park, Black hole Attack in Mobile Ad Hoc Networks, ACM Southeast Regional Conference, 2004.

[Bourai Amar et al,2014] Bourai Amar,Bentabet Abdel Hamid,La localisation dans les réseaux de capteurs , Mémoire de fin d'études, Université Boubakeur Belkaid, Tlemcen, 2014.

[Claude Duvallet,2014] Claude Duvallet,Les réseaux pair-à-pair (peer-to-peer),Cours SMB 214-215,Université du Havre,2014

[DengH et al.,2002] Deng H., Li W. and Agrawal, D.P., Routing security in wireless ad hoc networks, Communications Magazine IEEE, October 2002.

[Douceur, J.R.,2002] Douceur, J.R., "The sybil attack, in Peer-to-peer Systems", IPTPS '01 RevisedPapers from the First International Workshop on Peer-to-Peer Systems, pp. 251-260,March 2002, Springer-Verlag London, UK, ISBN: 3-540-44179-4.

[Dr.S.S.Dhenakaron et al..,2013] Dr.S.S.Dhenakaron,A.Parvathavarthini , An overview of routing protocols in Mobile Ad Hoc Network, International Journal of Advanced Research in

Computer Science and Software Engineering, Février 2013.

[Fabrice Le Fessant,2008] Fabrice Le Fessant,Pair-à-pair: architecture et services, INRIA,Saclay,2008.

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

[Houda Hafi, 2010] Houda Hafi, "Protocole pour la sécurité des réseaux sans fil peer to peer ", thèse de Magister, université de UKM Ouargla, 2010.

[Ines Chihi,2017] Ines Chihi, Étude de l'attaque « Black Hole » sur le protocole de routage VADD (Vehicule-Assisted Data Delivery), Mémoire, Université du Québec à Trois-Rivières, Juillet 2017.

[Irshad. U et al.,2010] Irshad. U, Shoaib UR Rehman, "Analysis of Black Hole Attack onMANETs Using Different MANET Routing Protocols", Master thesis,School of Computing Blekinge Institute of Technology, Sweden, 2010

[Ishu Varshney et al,2017] Ishu Varshney Shahjahan Ali, Study on MANet : concepts, features and applications, ELK Asia Pacific Journal, 2017.

[J. Burchfiel et al,1975] J. Burchfiel; R. Tomlinson; M. Beeler, Functions and structure of a packet radio station , National Computer Conference and Exhibition, Mai 1975.

[Laura Feeny,2013] Laura Feeny, Spontaneous Networking, IEEE Communications, 2013.

[Lazib Nassim et al.,2013] LAZIB Nassim et MAJOR Nassim,Les mécanismes de sécurité dans les réseaux véhiculaires (VANET), Mémoire,Université Abderrahmane MIRA de Béjaia, Faculté des Sciences Exactes,Département Informatique, 2013.

[Mshari Alabdulkarim,2017] Mshari Alabdulkarim,Ad hoc networks,King Saud University,2017.

[Ngai et Lyu,2006] Ngai, E.C.H., L. Jiangchuan, and M.R. Lyu, "On the Intruder Detection for SinkholeAttack in Wireless Sensor Networks in Communications", 2006. ICC '06. IEEEInternational Conference on, Vol. 8, pp. 3383 - 3389, June 2006. Print ISSN: 1550-3607.

[Nisha et al,2016] Nisha, Simranjit Kaur,Sandeep Kumar Arora,Analysis of blackhole effect and prevention through IDS in Manet,American Journalof Engineering Research, Volume 02,issue 10,2016

[P.Visalakshi et al,2013] P.Visalakshi,Mahish Mishram.Yusuf H and Snenasish Maitym,Ad hoc network – An overviezw , International Journal of Modern Engineering Research (IJMER), 2013.

[Perrig et Johnson,2003] Hu, Y.-C., A. Perrig, and D.B. Johnson, "Packet leashes: a defense against worrnholeattacks in wireless networks", in INFOCOM 2003. Twenty-Second Annual JointConference of the IEEE Computer and Communications. IEEE Societies, pp. 1976-1986,March 2003, San Francisco, CA, Print ISBN: 0-7803-7752-4.

[Romina Sh et al,2011] Romina Sh, Rajesh Sh, "Modified AODV Protocol To Prevent BlackHole Attack in Mobile Ad- hoc Network", International Journal OFInnovative Research & Development, Vol 2 Issue 4, April 2013.

[Subash Chandra Mandhata et al. 2011] Subash Chandra Mandhata, Dr.Surya Narayan Patro, "A countermeasure to Black hole attack on AODV-based Mobile Ad-HocNetworks", International Journal of Computer & CommunicationTechnology (IJCCT), 2011.

[Sumra, LA., et al,2011] Sumra, LA., et al. "Classes of attacks in VANET" In Electronics, Communicationsand Photonics Conference (SIECPC), 2011 Saudi International: IEEE, pp. 1-5, April2011. Print ISBN: 978-1-4577-0068-2.

[Tie Qiu et al.,2017] Tie Qiu,Ning Chen,Keqiu Li,Daji Qiao, Zhangjie, Heterogenous Networks . Architecture,advances and challenges,Elsevier,2017.