République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université AMO de Bouira

Département d'Informatique

Mémoire de Master

en Informatique

Spécialité : *Génie Système Informatique(GSI)*

Thème

PROPOSITION D'UN MÉCANISME DE SÉCURITÉ POUR FAIRE FACE A UNE ATTAQUE ACTIVE DE TYPE BLACK HOLE DANS UN RESEAU SANS FIL.

Encadré par

— Dr. DEMOUCHE Mouloud

Réalisé par

— TELDJOUNE Said

— KERROUA Arezki

2019/2020

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 notre encadreurs Mr. DEMMOUCHE MOULOUD, pour Ses conseils et orientations tout au long d'élaboration de ce travail et pour leurs aides précieuses.

Nous tenons également à remercier Mr. YAHIAOUI Kais et Madame MAHFOUD Zohra pour avoir accepté d'etre Jury, pour l'honneur qu'ils nous font en participant à l'évaluation de ce travail.

Enfin, nous adressons nous remerciement à Tous Les Enseignants de L'université de Akli Mohand Oulhadj pour leurs soutien et leurs bonne volonté à l'aide.

Dédicaces

Je dédie ce modeste travail : A mes parents, mes frères, mes sœurs, toute ma famille et mes amis.

TELDJOUNE said.

Dédicaces

Je dédie ce modeste travail :

A mes parents, mes frères et toute ma famille ainsi que mes amis.

KERROUA Arezki.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AC	Access Control
ACS	Anonymous Communication Scheme
AODV	Adhoc on Demand Distance Vector
ARP	Address Resolution Protocol
AS	Autonomous System
BLR	boucle locale radio
BTS	Base Transceiver Station
CBRP	Cluster Based Routing Protocol
CCK	Complementary Code Keying
CA	Certificate Authority
DDOS	Distributed Denial of Service
DNS	Domain Name System
DRI	Data Routing Information
DSR	Dynamic Source Routing
DOS	Denial Of Service
DPIS	Dummy Packet Injection Scheme
EDCF	Energy Dissipation Circulation Function
EDGE	Enhanced Data Rates for GSM Evolution
EFM	Egress Filtering Method
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
EUTRAN	Evolved Universal Terrestrial Radio Access Network

GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HiperLAN 2	High Performance LAN 2.0
HSDPA	High Speed Downlink Packet Access
HTTPS	Hypertext Transfer Protocol Secure
IAPP12	Inter Access Point Protocol
IDS	Intrusion Détection System
IEEE	Institute of Electrical and Electronics Engineers
IFM	Ingress Filtering Method
IP	Internet Protocol
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
MANET	Mobile Ad hoc NETwork
MITM	Man In The Middle
NS	Network Simulator
OFDMA	Orthogonal Frequency Division Multiple Access
OLSR	Optimized Link State Routing
OTcl	Object Tool Command Language
PC	Personal Computer
PDA	Assistant Numérique Personnel
P2P	peer to peer
RERR	Route Error
RREP	Route Reply
RREQ	Route Request
RRS	Random Routing Scheme
REQ	Request
SC-FDMA	Single Carrier Frequency Division Multiple Access
SIM	Subscriber Identity/Identification Module

SMS	Short message service
SPM	Spoofing Prevention Method
SSL	Secure socket layer
SB	Stations de Base
TCP	Transmission Control Protocol
TFN	Tribal Flood Network
TLS	Transport Layer Security
TORA	TemporallyOrdered Roufing Aigorithm
TV	Télévision
UCAD	Université Cheikh Anta Diop
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
WIFI	WIreless FIdelity
Wimax	Worldwide interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network
WWAN	Wireless Wide Area Network
ZRP	Zone Routing Protocol

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.

Les réseaux mobiles ad hoc ou MANET (Mobile Ad hoc NETworks) définis par la RFC 2501 (Scott Corson et al., 1999), sont des réseaux sans fil qui ne bénéficient ni d'une infrastructure préexistante, ni d'une administration centralisée pour assurer les échanges d'informations et les services fournis aux utilisateurs. La topologie de ces réseaux se forme au gré de l'apparition et du mouvement des nœuds. Ces derniers communiquent avec leurs voisins par des liaisons sans fil point à point et assurent eux-mêmes la fonction de routage. En conséquence, il n'existe aucune hiérarchie entre les nœuds et aucun service réseau ne peut prétendre être centralisé.

Un réseau ad hoc est donc un système autonome de nœuds mobiles. Ce système peut fonctionner de manière isolée ou s'interfacer avec des réseaux fixes au travers de passerelles pour devenir un réseau d'extrémité. Compte tenu de l'évolution rapide des performances des réseaux sans fil et des besoins grandissants des utilisateurs, l'utilisation des MANET, aussi appelés réseaux spontanés, semble appelée à se développer. Ainsi, ces réseaux répondent au besoin d'échange d'informations, par exemple, entre les participants d'une réunion, entre les acteurs d'une opération de secours, entre les intervenants d'un chantier de construction, ou encore entre les éléments engagés sur un champ de bataille, etc.

Ces réseaux sont par nature plus vulnérables et plus difficiles à protéger que les réseaux filaires. En effet, dans un réseau sans fil, l'accès aux données échangées est immédiat pour tout nœud équipé d'une interface réseau adaptée, alors qu'il faut disposer d'une connexion physique dans un réseau filaire. De plus, la mise en œuvre de certains mécanismes de sécurité développés pour les réseaux filaires est délicate, voire impossible dans les MANET. En raison de leur caractère spontané, ces derniers ne peuvent bénéficier des mécanismes de sécurité s'appuyant sur l'infrastructure, comme un pare-feu ou un serveur d'authentification.

En conséquence, chaque nœud constitue un point de vulnérabilité qui ne peut compter que sur ses propres ressources et ses services pour se protéger. Outre les vulnérabilités déjà identifiées dans les réseaux filaires et souvent accentuées dans le contexte ad hoc, ces réseaux possèdent des vulnérabilités qui leur sont propres comme celles spécifiques à la couche physique et celles spécifiques à la couche réseau (Albers et al., 2002). De plus, l'observation des attaques dirigées vers les systèmes d'information nous montre que, quelles que soient les techniques de prévention mises en place, il existe toujours des failles exploitables pour celui qui les traque.

Nous proposons de renforcer les mécanismes de sécurité préventifs existants en leur adjoignant un Système de Détection d'Intrusions (IDS, Intrusion Detection System) adapté aux caractéristiques des MANET.Notre étude offre principalement un état de l'art des travaux de recherche qui ont été faits et qui se font à l'heure actuelle dans le but de résoudre le problème de l'attaque du trou noir dans les Reseau Sans fil.

Nous proposons un nouveau Protocole idsAODV qui essaye de sécuriser le routage et d'optimiser les performances. Le reste du mémoire est organisé comme suit :

- Dans le chapitre 1, nous donnons des généralités sur les réseaux Sans Fil.
- Dans le chapitre 2, nous présentons les attaques qui existe dans les réseaux sans fil, nous discutons des besoins et des solution de sécurité .
- Dans le chapitre 3 , nous présentons la simulation du l'attaque du trou noir ainsi que la Solution Proposé.

On termine notre travail par une conclusion et des perspectives.

Chapitre 1

Les réseaux sans fil

1.1 Introduction

Dans cette partie de travail nous visions à donner un aperçu sur les réseaux sans fil, nous commençons par définir les réseaux sans fil et citer les catégories de ce réseau, en suite nous allons définir le réseau Ad Hoc ainsi que la Topologie et les principaux caractéristiques de ce réseau, Enfin nous donnons les domaines d'application de ce réseau.[1]

1.2 Définition de réseau sans fil

En anglais wireless network est un réseau dans lequel au moins deux terminaux (ordinateur portable, PDA, etc.) peuvent communiquer sans liaison filaire. Les réseaux sans fil sont basés sur une liaison utilisant des ondes radioélectriques (radio et infrarouges) [2].

1.3 Les catégories des réseaux sans fil

Les réseaux sans fil peuvent être classés selon deux normes. Le premier est la couverture du réseau. Selon la norme, il existe quatre catégories : réseau personnel, réseau local, réseau métropolitain et réseau étendu.

Le deuxième critère est l'infrastructure et le modèle utilisés. Concernant cette norme, nous pouvons diviser les réseaux sans fil en : réseaux avec infrastructure et réseaux sans infrastructure, comme le montre la figure suivante [2].

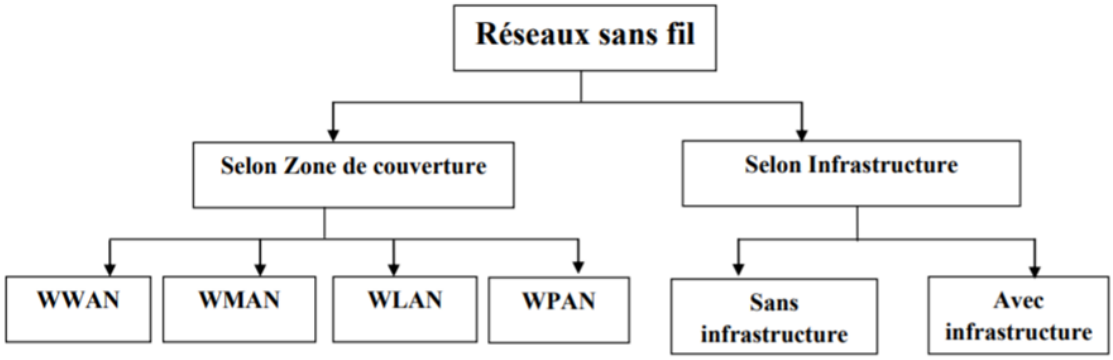


FIGURE 1.1 – Classification des réseaux sans fils

1.4 Selon la zone de couverture

Les réseaux sans fil sont généralement divisés en plusieurs catégories, en fonction de la zone géographique (appelée zone de couverture) qui assure la connectivité [1] :

* Les réseaux personnels sans fil (WPAN : Wireless Personnel Area Network) telle que les réseaux Bluetooth et Infrarouge.
* Les réseaux locaux sans fil (WLAN : Wireless Local Area Network) telle que les réseaux WIFI.
* Les réseaux métropolitains sans fil (WMAN : Wireless Metropoletan Area Network) telle que les réseaux à diffusion WiMax.
* Les réseaux étendus sans fil (WWAN : Wireless Wide Area Network), telle que les réseaux cellulaires.

1.4.1 Réseaux personnels sans fil (WPAN)

Aussi connu sous le nom de réseau personnel sans fil ou réseau domestique sans fil, et appelé Wireless Personal Area Network (WPAN) en anglais , il s'agit d'un réseau sans fil à très courte distance, environ 10 mètres. Ils sont le plus souvent utilisés pour communiquer avec les matériaux présents sur une personne, tels que les écouteurs et les téléphones

portables. Ils sont également utilisés pour connecter des périphériques informatiques entre eux sans liaison filaire : par exemple, pour connecter une imprimante ou un PDA (assistant numérique personnel) à un ordinateur, ou pour communiquer avec deux machines proches l'une de l'autre [3].

Il existe plusieurs technologies permettant la mise en oeuvre de tels réseaux qui sont :

Bluetooth

La norme Bluetooth (prise en charge par IEEE 802.15.1) est une technologie à vitesse moyenne qui peut atteindre une vitesse maximale théorique de 1 Mbps (effectivement environ 720 Kbps) avec une faible consommation d'énergie. Bluetooth utilise la bande de fréquences 2,4 GHz et a une portée de 10 à 30 mètres. Cette technologie permet de créer un réseau de 8 appareils communiquant simultanément. La petite taille du composant Bluetooth peut être insérée dans un clavier et une souris sans fil, des kits mains libres ou casque et d'autres appareils, ainsi que la transmission de données entre un PC et un PDA (assistant numérique

* **les caractéristiques de Bluetooth**

  Dans les versions commercialisées en 2015 (4.0 et 4.1), largement utilisées, essentiellement dans les appareils mobiles comme les téléphones portables, la liaison Bluetooth présente les caractéristiques suivantes :

  - très faible consommation d'énergie
  - très faible portée (sur un rayon de l'ordre d'une dizaine de mètres)
  - faible débit, suffisant cependant pour le son stéréo de qualité
  - très bon marché et peu encombrant.

  En conséquence, il apparaît sur les appareils qui dépendent souvent de la batterie, dans l'espoir d'échanger de petites quantités de données à courte distance :

  - Téléphone portable, principalement utilisé pour connecter des écouteurs ou échanger des fichiers, voire comme modem.
  - ordinateurs portables, essentiellement pour communiquer avec les téléphones portables (pour servir de modem, pour sauvegarder les carnets d'adresses, pour l'envoi de SMS, etc.

- Divers périphériques (tels que des claviers) pour faciliter la saisie sur les appareils sans clavier.
- périphériques spécialisés à destination médicale (électrocardiogramme, oxymètres, glucomètres) ou environnementale (thermomètres, hygromètres....).[5]

ZigBee

Il est également connu sous le nom de norme IEEE 802.15.4 et permet d'accéder à des liaisons sans fil à faible coût et à très faible consommation d'énergie, ce qui le rend particulièrement adapté à une intégration directe dans de petits appareils. Electronique (capteurs, appareils électroménagers ...). Le réseau ZigBee peut fournir jusqu'à 250 Kbit / s dans la bande de fréquence classique de 2,4 GHz [6].

Liaisons infrarouges

Avant l'avènement des technologies radio telles que le Wi-Fi et le Bluetooth, il était encore possible d'utiliser l'infrarouge pour transmettre des données sans fil entre deux appareils. IrDA est une technologie largement utilisée dans les années 1990 et au début des années 2000, en particulier sur les téléphones, les PDA et les ordinateurs portables. IrDA utilise des signaux infrarouges (comme les télécommandes TV, par exemple) pour transmettre entre deux appareils. L'opération est très simple : La fréquence du rayonnement infrarouge (invisible pour l'homme) émis par la lampe permet de travailler en binaire. L'infrarouge présente plusieurs inconvénients : la portée est limitée (entre 5 mètres et 1 mètre), le périphérique doit être aligné (environ 15 ° de cône), et il n'y a aucun obstacle pour séparer les deux appareils. À l'heure actuelle, l'utilisation des ordinateurs a presque complètement disparu, mais de nombreuses entreprises utilisent toujours l'infrarouge pour leurs télécommandes (dans le monde de l'audio / vidéo, l'infrarouge est omniprésent). La raison est simple : la technologie est bien maîtrisée, est efficace et consomme peu [7].

1.4.2 Réseaux locaux sans fil (WLAN)

WLAN pour Wireless Local Area Network est un réseau qui peut couvrir le réseau équivalent du réseau local de l'entreprise, c'est-à-dire que la couverture est d'environ cent mètres. Il permet de relier entre eux les terminaux existant dans la zone de couverture [8], par exemple :

IEEE 802.11, WiFi (Wireless Fidelity)

IEEE 802.11 [30] est un standard de réseau sans fil local proposé par l'organisme de standardisation Américain IEEE. La technologie 802.11 est généralement considérée comme la version sans fil de 802.3 (Ethernet). La technologie 802.11 a connu beaucoup d'évolutions, notamment la 802.11.a et la 802.11b qui proposent une amélioration de la norme initiale en introduisant la modulation CCK (Complementary Code Keying) dans la bande des 2,4 GHz. Deux nouveaux débits sont alors disponibles, 5,5 Mbits/s et 11 Mbits/s sur une portée de quelques dizaines de mètres environ [8].

— **Normes associées à l'IEEE 802.11**

Dans ce qui suit, nous donnons une description des principales problématiques traitées par les groupes de travail de 1' IEEE 802.11.

- **L'IEEE 802.11e : la qualité de service**

  L'IEEE a chargé le groupe de travail802.lle d'améliorer la couche MAC 802.11 pour y inclure des mécanismes de qualité de service, afin de permettre un meilleur support des applications sensibles aux phénomènes de latence, telles que les applications de voix ou vidéo. Le groupe de travail n'a pas encore finalisé le standard 802.1le, mais a réussi à mettre en œuvre quelques solutions intermédiaires intéressantes, tel qu'EDCF11 qui réalise un contrôle d'admission simple et efficace. Les efforts se poursuivent encore afin d'aboutir à un ensemble d'outils pratiques et efficaces qui permettent d'étendre et de développer les applications Wi-Fi [9].

- **L'IEEE 802.11 f : les han do vers**

  L'objectif du groupe 802.11 fest de développer la technologie permettant la mobilité inter-cellules des stations Wi-Fi, tout en préservant les performances

du réseau et en maintenant la connectivité des stations lors du déplacement.

Ainsi, la plupart des réseaux sans fil pourront désormais jouer le rôle de réseaux mobiles, en adoptant la norme 802.11 f, qui équipe actuellement la plupart des interfaces WiFi. Ces dernières permettent de réaliser des handovers ou relève intercellulaire qui désigne la possibilité de passer d'une cellule à une autre sans interruption de la communication. Le protocole retenu par le groupe de travail 802.11 f est IAPP12, qui fait communiquer les différents points d'accès d'un même réseau ESS, de façon à permettre à un utilisateur mobile de passer d'une cellule à une autre sans perte de connexion. [9]

- **L'IEEE 802.1ln : le haut débit**

  L'IEEE 802.11n est un groupe de travail au sein de l'IEEE, mis en place en 2003. Les raisons qui ont suscité la création de ce groupe sont les suivantes [10] :
  — Les réseaux Wi-Fi (standards 802.11 b, g et a) offrent une portée limitée.
  — Les réseaux Wi-Fi sont très sensibles aux phénomènes de réflexion d'ondes, ainsi qu'aux interférences ayant comme origine d'autres unités sans fil.
  — Les réseaux Wi-Fi sont beaucoup plus lents, en termes de débits, qu'Ethernet.

- **L'IEEE 802.lli : la sécurité**

  Dans les réseaux Wi-Fi, le support est partagé. Tout ce qui est transmis peut donc être intercepté. L'incapacité de garantir un trafic aussi sécurisé que dans les réseaux fixes constitue un obstacle pour l'essor de la technologie Wi-Fi. C'est pourquoi l'IEEE a mis en place le groupe de travail IEEE 802.lli, dont la mission est la mise au point d'une architecture de sécurité robuste, qui prend en compte les spécificités des réseaux sans fil [10].

Les réseaux HiperLAN 2 (High Performance LAN 2.0)

Ils sont issus des standards européens développés par l'ETSI (European Telecommunications Standards Institute) .Ainsi : Hiperlan 1 fournit une vitesse de 20 Mbit / s, HiperLAN 2 permet d'obtenir une vitesse théorique de 54 Mbps dans une centaine de zones 5 150-5300 MHz [10] Compteurs électriques dans la gamme de fréquences.

1.4.3 Les réseaux métropolitains sans fil (WMAN)

(WMAN pour Wireless Metropolitan Area Network), également connu sous le nom de Loop Locale Radio (BLR), est une technologie informatique utilisée dans ce réseau. Il ne faut pas oublier qu'en plaçant une antenne parabolique sur le toit d'un bâtiment, le BLR peut transmettre la voix et les données à haut débit par voie aérienne pour accéder à Internet et au téléphone. Par exemple, le type de réseau WMAN, dont le plus connu est [11] :

les réseaux Wimax (Worldwide interoperability for Microwave Access)

WMAN est basé sur la norme IEEE 802.16 et fournit un débit utile de 1 à 10 Mbit / s dans une plage de 4 à 10 kilomètres. Par conséquent, ce type de connexion est principalement utilisé par les opérateurs télécoms [11].

1.4.4 Le réseau étendu sans fil (WWAN)

Le réseau étendu sans fil WWAN utilisé dans le réseau étendu sans fil est également appelé réseau cellulaire mobile. Étant donné que tous les téléphones mobiles sont connectés à un réseau étendu sans fil, ils constituent le réseau sans fil le plus populaire. Les principales technologies sont les suivantes [12] :

GSM (2G)

Au début du 20e siècle, le réseau GSM (Global System for Mobile Communications) était la norme de téléphonie mobile la plus utilisée. La norme GSM autorise une vitesse maximale de 9,6 kbps, ce qui permet la transmission de la voix et de petites quantités de données numériques, telles que des messages texte ou des messages multimédias. Le réseau cellulaire repose sur l'utilisation d'une station émettrice-réceptrice centrale au niveau de chaque cellule, appelée station de base (BTS : Base Transceiver Station). Plus le rayon de cellule est petit, plus la bande passante disponible est grande. Ainsi, quel que soit le terminal utilisé lors de la communication avec la station de base, la carte SIM peut identifier chaque utilisateur. La communication entre la station mobile et la station de base a lieu via une liaison radio communément appelée interface radio. [7]

GPRS (2.5G)

GPRS (General Packet Radio Service) est une technologie de communication sans fil à commutation de paquets utilisée dans les réseaux GSM. La connexion au service GPRS est toujours ouverte pour fournir aux utilisateurs de terminaux mobiles la même disponibilité réseau que le réseau d'entreprise. GPRS fournit une connexion IP de bout en bout du terminal GPRS à n'importe quel réseau IP. Le terminal peut être efficacement intégré au réseau Internet. La vitesse «utile» est d'environ 40 Kb / s (vitesse maximale : 171 Kb / s), l'une ou l'autre est quatre fois supérieure à celle du GSM. [3]

EDGE (2.75G)[13]

«Evolved EDGE» vise à apporter de nombreuses améliorations à EDGE. En divisant par deux l'intervalle de temps de transmission (de 20 millisecondes à 10 millisecondes), le délai peut être réduit. En utilisant deux porteuses, des débits de symboles plus élevés et un codage plus complexe (32QAM et 16QAM au lieu de 8-PSK), la bande passante théorique maximale a été développée à 1 Mbit / s et le délai a été réduit à 80 ms.) Et le code Turbo pour améliorer la correction des erreurs. D'autre part, la qualité du signal peut être améliorée en utilisant une antenne dipôle. EDGE Evolution peut être mis en œuvre progressivement grâce à des mises à jour logicielles.

UMTS (3G) [14]

La version initiale de l'UMTS "3GPP R99" (normalisée en 1999 et achevée en 2001) permet au débit de données maximal théorique de la liaison descendante (téléchargement) d'être de 1,920 Mb / s, ce qui est nettement supérieur au débit initial du GSM. 9,6 kb / s, supérieur à la vitesse maximale fournie par la variante GSM optimisée pour la transmission de données (GPRS et EDGE) : EDGE est de 384 kb / s.

Les débits UMTS varient suivant le lieu d'utilisation et la vitesse de déplacement de l'utilisateur4. Pour la première génération de l'UMTS (celle disponible en France de 2005 à 2009), les débits maximum descendants (download) étaient de :

- 144 kb/s pour une utilisation mobile en mouvement rapide (voiture, train...) et en zones rurales loin de l'antenne ;
- 384 kb/s pour une utilisation piétonne ;

— jusqu'à 2 000 kb/s depuis un point fixe (terminal immobile) et dans des conditions idéales.

HSDPA (3G+)

14.4Mbps

LTE-Advanced (4G) : 1Gbps / 100Mbps

Un réseau LTE est un réseau cellulaire composé de milliers de cellules radio utilisant la même fréquence radio, grâce au codage radio OFDMA (de la station de base au terminal) et SC-FDMA (du terminal au terminal). basé sur). Cela permet d'allouer une largeur de spectre plus grande pour chaque cellule qu'en 3G, allant de 3 à 20 MHz, de sorte que chaque cellule dispose d'une bande passante et d'un débit plus importants.

Le réseau se compose de deux parties : la partie radio (eUTRAN) et le cœur de réseau "EPC" (noyau de paquets évolué). [15]

1.5 Selon l'infrastructure

L'environnement mobile est un système composé de sites mobiles qui permet aux utilisateurs d'accéder aux informations où qu'ils se trouvent. Les réseaux mobiles ou sans fil peuvent être divisés en deux catégories : les réseaux avec infrastructure et les réseaux sans infrastructure.

1.5.1 Réseaux cellulaires (avec infrastructure)

Ce type de réseaux se compose des éléments suivants [16] :

* Les "sites fixes" du réseau filaire.
* Les "sites mobiles", réseaux sans fils.

Certains sites fixes (appelés stations de base (SB)) ont des interfaces de communication sans fil pour une communication directe avec des sites mobiles situés dans une zone géographique limitée (appelées cellules), comme illustré dans la figure suivante :

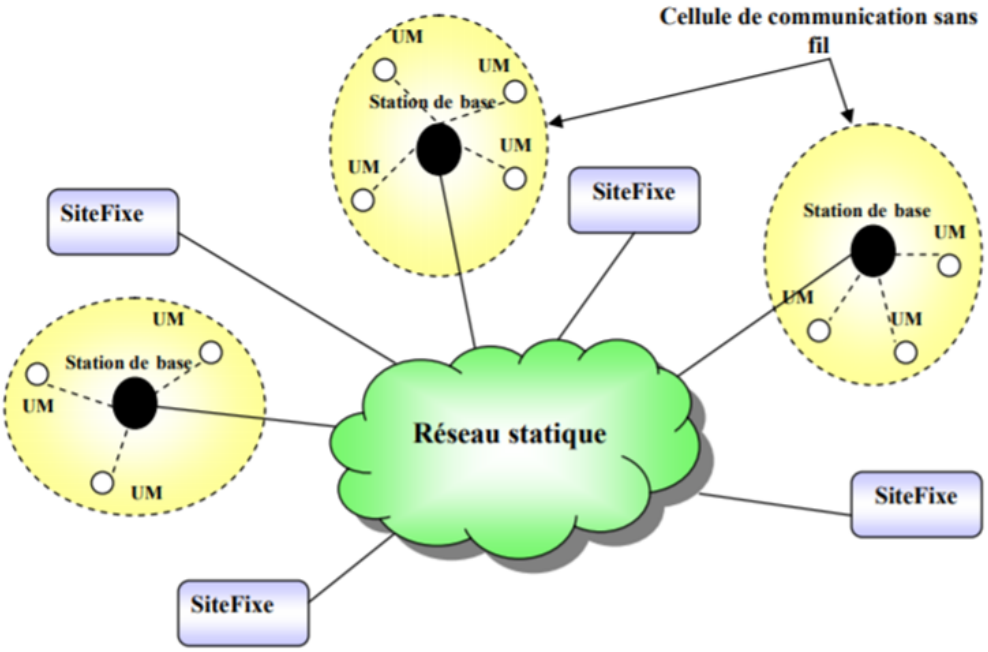


FIGURE 1.2 – Le modèle des réseaux mobiles avec infrastructure

Chaque station de base a une cellule correspondante à partir de laquelle l'unité mobile peut envoyer et recevoir des messages. Les sites fixes sont connectés les uns aux autres via un réseau de communication filaire. A un moment donné, l'unité mobile ne peut se connecter directement qu'à une seule station de base. Il peut communiquer avec d'autres sites via le site directement connecté à.

Principe de fonctionnement La configuration standard d'un système de communication cellulaire est une grille hexagonale. Au départ, une zone ne peut être couverte que par une seule cellule.Lorsque la concurrence devient importante pour l'attribution des canaux, la cellule est généralement divisée en sept cellules plus petites, comme le montre la figure 1.3.

Les cellules adjacentes de la grille doivent utiliser des fréquences différentes, ce qui est différent du risque que la grille de l'autre côté de la grille puisse utiliser la même fréquence sans interférence. [3]

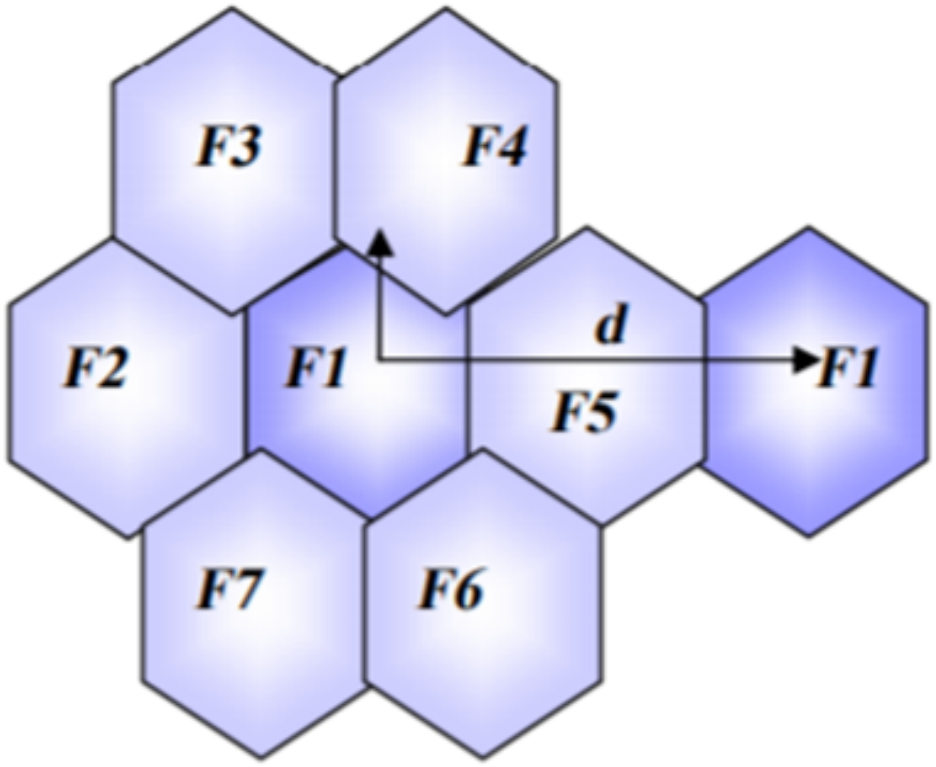


FIGURE 1.3 – Le principe de réutilisation de fréquence [3]

1.5.2 Réseaux ad hoc (sans infrastructure)

Ces dernières années, le développement de la technologie de transmission sans fil a ouvert de nouvelles perspectives dans le domaine des télécommunications. Le réseau mobile ad hoc est un nouveau type de réseau basé sur cette technologie. [1]

L'évolution récente des moyens de communication sans fil a permis la manipulation d'informations au travers d'unités de calcul portables aux caractéristiques bien particulières (faible capacité de stockage, source d'énergie autonomie, puissance limitée, etc.) qui accèdent au réseau par le biais d'une interface de communication sans fil.

1. **Définition d'un réseau mobile adhoc**

Dans le modèle de réseau ad hoc ou MANET (Mobile Ad hoc NETwork), l'entité «site fixe» n'existe pas, tous les sites du réseau sont mobiles et communiquent directement avec leurs interfaces de communication sans fil. . Le manque d'infrastructure ou d'un réseau filaire composé de stations de base obligera les unités mobiles à se comporter comme des routeurs, participant à la découverte de chemin et à la maintenance des autres hôtes du réseau. Ensuite, MANET est composé d'unités mobiles relativement denses, qui peuvent se déplacer dans n'importe quelle zone, et son seul moyen de communication est d'utiliser une interface sans fil, sans avoir besoin d'une infrastructure existante ou d'une gestion centralisée. [17]

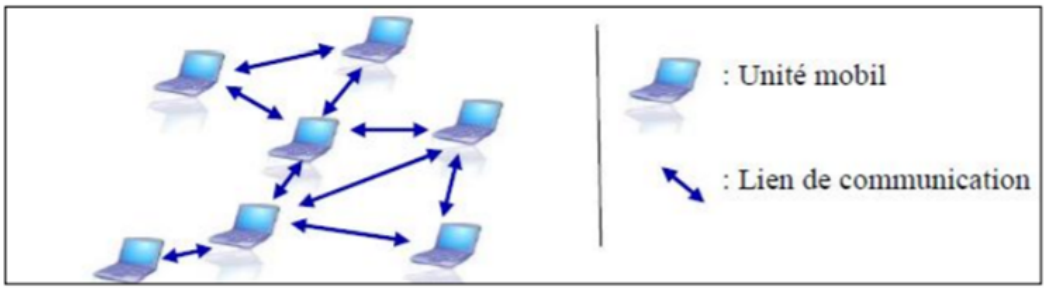


FIGURE 1.4 – Réseau en mode ad hoc. [17]

— Contrairement aux réseaux basés sur des communications cellulaires, l'unité mobile elle-même forme l'infrastructure du réseau de manière et maintient sa connectivité de manière décentralisée. Les informations sont transmises via le téléphone mobile actuel.
— Un réseau ad hoc doit être facilement déployé, les nœuds peuvent rejoindre et quitter le réseau de manière complètement dynamique sans avertir le réseau, et lorsque cela est possible, cela n'interrompra pas la communication entre les autres nœuds du réseau.

2. **Modélisation d'un réseau mobile ad hoc**

Un réseau ad hoc peut être modéliser par un graphe Gt = (Vt,Et) ou Vt représente l'ensemble des nœuds (i.e. les unités ou les hôtes mobiles) du réseau et Et modélise l'ensemble les connections qui existent entre ces nœuds (voir la fi-

gure1.5). Si e = (u,v) appartient à Et, cela veut dire que les nœuds u et v sont en mesure de communiquer directement a l'instant t.[1]

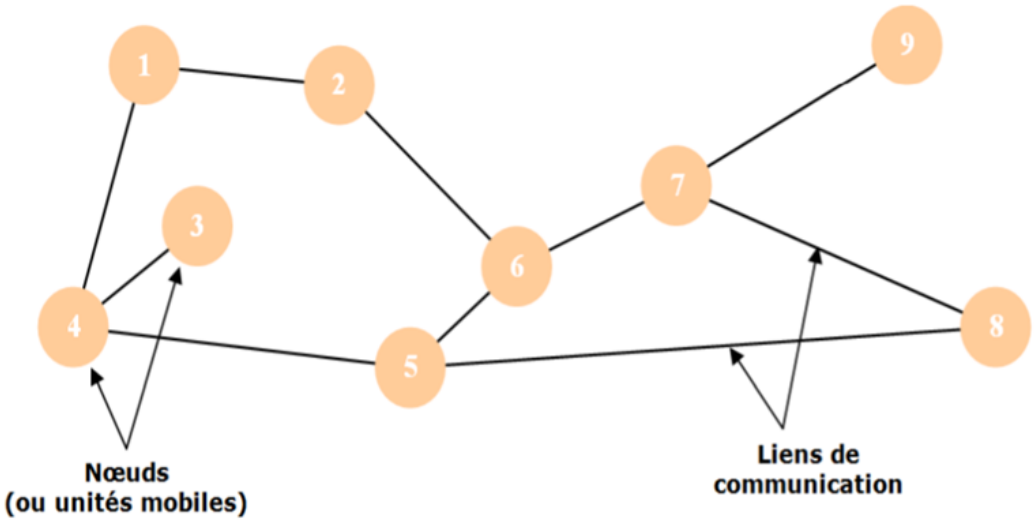


FIGURE 1.5 – La modélisation d'un réseau ad hoc. [1]

3. Topologie d'un réseau mobile ad hoc

La topologie des réseaux ad hoc est dynamique et décentralisé. Il peut changer de manière aléatoire et l'unité mobile peut se déplacer à volonté. Par conséquent, la déconnexion de ces unités est très fréquente [18].

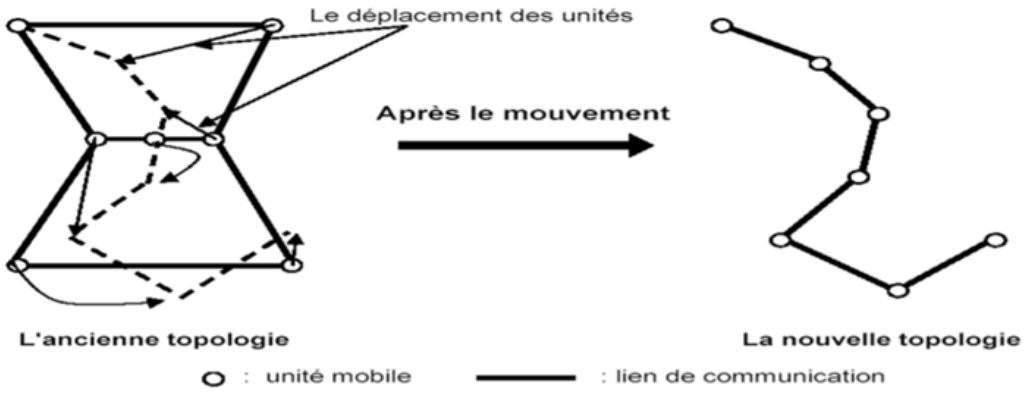


FIGURE 1.6 – Le changement de la topologie d'un réseau mobile ad hoc [18].

4. **Caractéristiques des réseaux ad hoc**

On peut distinguer six grandes caractéristiques [1], [19], [20] :

- **Mobilité (Une topologie dynamique)**

  La mobilité des nœuds est évidemment une caractéristique très particulière des réseaux ad hoc. Cette mobilité est intrinsèque au fonctionnement du réseau.

  un réseau ad hoc, la topologie du réseau peut changer rapidement, de manière aléatoire et imprévisible, et la technologie de routage réseau traditionnelle basée sur des routes préétablies ne fonctionnera pas correctement.

- **Liaisons sans fil (Une bande passante limitée)**

  Bande passante limitée : l'une des caractéristiques de base des réseaux de communication sans fil est l'utilisation de supports de communication partagés. Ce partage rend la bande passante réservée à l'hôte modérée.

- **Autonomie des nœuds (Des contraintes d'énergie)**

  La consommation d'énergie est le principal problème des équipements fonctionnant sur des sources d'alimentation indépendantes. L'appareil utilise un mode de gestion de l'énergie, le protocole implémenté dans le réseau ad hoc doit donc prendre en compte ce problème, ce qui est très important [8].

- **Vulnérabilité (Une sécurité physique limitée)**

  Par rapport aux réseaux filaires traditionnels, les réseaux mobiles ad hoc sont plus affectés par les paramètres de sécurité. Les contraintes et restrictions physiques le prouvent, ce qui signifie que le contrôle des données transmises doit être minimisé.

- **L'absence d'infrastructure**

  La différence entre les réseaux ad hoc et les autres réseaux mobiles réside dans le manque d'infrastructure préexistante et de tout type de gestion centralisée. L'hôte mobile est responsable de l'établissement et du maintien continus des connexions réseau.

- **Les interférences**

  Il y a beaucoup d'interférences entre les hôtes dans le réseau des hôtes et même entre leurs propres ondes (dans le cas de la réflexion des ondes). Ils augmentent le nombre d'erreurs de transmission et réduisent les performances.

5. **Applications des réseaux ad hoc**

Les réseaux ad hoc peuvent être utilisés dans toute application où le déploiement d'une infrastructure de réseau filaire est trop strict. Cela peut être dû au fait qu'il est difficile à mettre en place ou parce que le temps d'installation du réseau ne justifie pas un câblage permanent. [1]

Les applications militaires

Le réseau Ad Hoc était à l'origine utilisé par les militaires. En fait, ce type de réseau est une solution idéale pour maintenir les communications sur le champ de bataille entre différents groupes et forces. [21]

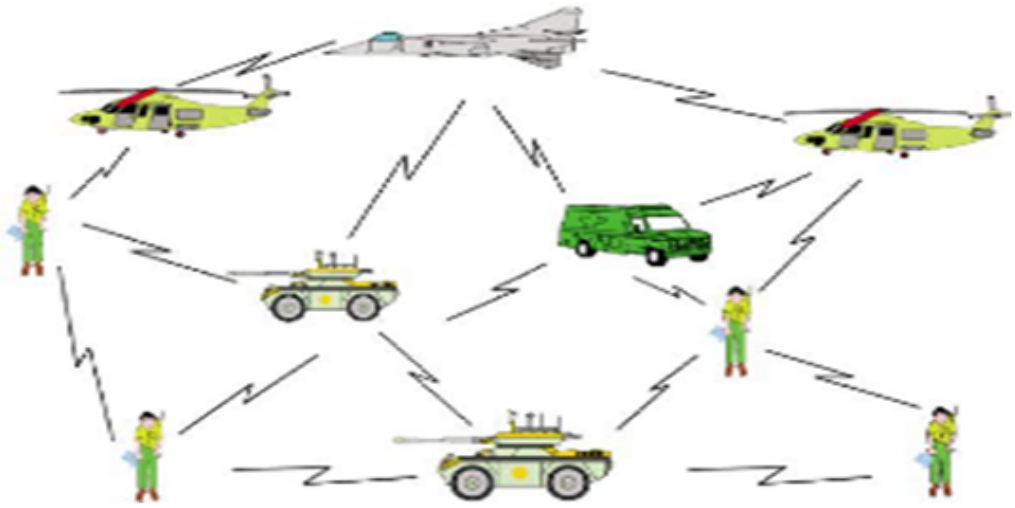


FIGURE 1.7 – Les applications militaires.

Les opérations de secours

Dans les zones touchées par des catastrophes naturelles (ouragans, tremblements de terre, etc.), le déploiement de réseaux ad hoc est indispensable pour permettre

aux unités de secours de communiquer. [21]

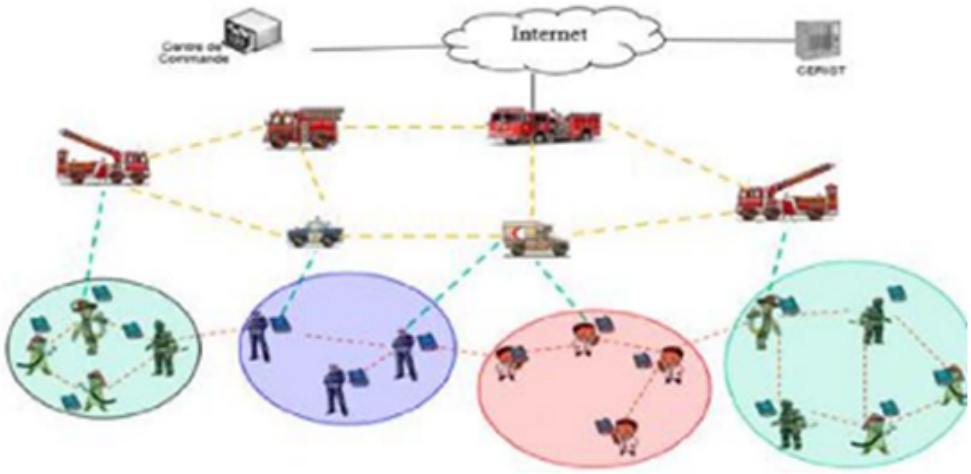


FIGURE 1.8 – Les opérations de secours.

Applications industrielles

La plupart des sites industriels ou commerciaux disposent de réseaux sans fil, en particulier dans les environnements de production. En règle générale, les installations de fabrication ont de nombreux appareils électroniques interconnectés. Le câblage peut provoquer un chaos spatial, non seulement causant des risques pour la sécurité, mais également endommageant la fiabilité. L'utilisation de réseaux sans fil élimine bon nombre de ces problèmes. Si la connexion prend la forme d'une communication sans fil auto-organisée, elle augmentera de nombreux aspects bénéfiques, y compris la mobilité. Vous pouvez facilement déplacer l'appareil et reconfigurer le réseau en fonction des nouvelles exigences. [22]

Domaine de la santé

En cas d'urgence, l'échange d'informations multimédias (audio, vidéo et données) entre le patient et l'appareil est très utile. Les personnes transportées à l'hôpital par ambulance peuvent utiliser le réseau temporaire pour envoyer des informations. Dans de nombreux cas, si le médecin a la vidéo et pas seulement les données, le médecin est très approprié pour diagnostiquer et préparer le traitement pour le patient. [23]

L'utilisation à des fins éducatives

Déployer un réseau Ad Hoc dans une conférence ou un cours est très judicieux, car il permet aux chercheurs et étudiants de partager des ressources (fichiers, accès Internet, etc.) sans aucune infrastructure pour communiquer. [23]

1.6 Conclusion

Les réseaux informatiques sans fil peuvent être divisés en deux catégories : les réseaux avec une infrastructure fixe existante et les réseaux sans infrastructure. La deuxième catégorie tente d'étendre le concept de mobilité à tous les composants environnementaux, toutes les unités de réseau de cette catégorie.

Les réseaux ad hoc se déplacent librement et il n'y a pas d'administration centralisée, dans le prochain chapitre nous traiterons de diverses attaques sur les réseaux sans fil

Chapitre 2

Les attaques des réseaux sans fil

2.1 Introduction

La sécurité des réseaux informatiques est devenue un enjeu croissant du fait des évolutions que personne aujourd'hui ne cherche à nier. Pour procéder à une attaque, une personne mal intentionnée cherche par différentes techniques à connaître le réseau et ses faiblesses. Ces faiblesses à exploiter dans le but par exemple de récupérer des informations, modifier le comportement d'un réseau ...

Ce chapitre permet de définir les différents types d'attaques, en suite nous allons définir Les principales attaques contre les réseaux sans fil.

2.2 Attaque

Tentative d'évitement des contrôles de sécurité sur un serveur. Le succès de l'attaque dépend de la vulnérabilité du serveur attaqué, mais si elle réussit, l'attaquant aura un accès illimité au serveur et pourra faire ce qu'il veut (vol, destruction de données ...)[24].

2.2.1 Types d'attaques

Les attaques informatiques dans les réseaux sans fil peuvent être vue sous 2 angles différents : [25]

* selon l'action malicieuse.
* selon le type de nœud.

Classification des attaques selon l'action malicieuse (active ou passive)

— les attaques passives : consistent à écouter sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais une prévention est possible.

— les attaques actives : consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau. Noter qu'une attaque active peut être exécutée sans la capacité d'écoute. De plus, il n'y a généralement pas de prévention possible pour ces attaques, bien qu'elles soient détectables.

Classification des attaques selon le type du nœud(Interne ou Externe)

Il est plus difficile de repérer une attaque informatique interne qu'une attaque informatique externe [26] :

- Les attaques informatiques internes sont plus difficiles à détecter que les attaques informatiques externes.
- En général, c'est la principale difficulté pour détecter ces attaques informatiques internes, et le contrevenant possède des informations d'identification valides et légales. Par conséquent, il est difficile de détecter les intrusions car le système fonctionnera de manière tout à fait normale.
- Une autre difficulté est que la montée en puissance des applications et des supports au sein de l'entreprise peut entraîner des fuites ou des pertes de données.
- Selon les experts de la sécurité réseaux Il est difficile d'évaluer les dommages de ces attaques informatiques internes. Compte tenu des résultats d'autres problèmes, c'est-à-dire que les utilisateurs les utilisent rarement ou ne les utilisent pas, il n'est pas surprenant que les appareils utilisés dans le cloud (en particulier les appareils personnels) soient contrôlés, et notamment les appareils personnels ne sont que peu ou insuffisamment contrôlés. [26]

2.2.2 Profils et capacités des attaquants

Comme leurs attaques, les pirates ont des profils variés et leurs actions peuvent répondre à des motivations financières, politiques ou morales. Ce qui suit est une liste des principaux fichiers de configuration des hackers, il est préférable de faire attention à [27].

* Non seulement l'attaquant peut être classé selon les connaissances de l'attaquant, mais l'attaquant peut également être classé selon la capacité d'attaque dans une situation claire. Par conséquent, nous pouvons calculer la capacité suivante [28] :
  - transmission de messages sans capacité d'écoute (IP SPOOFING ...).
  - Écoutez et envoyez des messages.
  - Écouter et interrompre la communication (blocs de paquets, DOS et DDOS ...).
  - Écouter, déranger et transmettre des informations.
  - Écouter, interrompre et transmettre des informations.
* ne autre caractéristique utilisée par les pirates est que, en raison de l'asymétrie de ces informations, elles sont saisies à sens unique ou bidirectionnel. En fait, la plupart des canaux de transmission sur Internet ou sur tout autre réseau hétérogène sont à sens unique et empruntent des chemins différents selon les règles de routage. Par conséquent, de nombreux protocoles de sécurité sont également unidirectionnels, il est donc nécessaire d'établir plusieurs canaux pour permettre l'échange duplex [29].

2.2.3 Outils des attaquants

- Procédures et scripts de test de vulnérabilité et d'erreur de configuration.
- Injectez du code pour accéder à la machine de la victime (cheval de Troie).
- Échangez des techniques d'attaque via des forums et des publications.
- Par exemple, utilisation massive de ressources pour détruire des clés.
- L'attaquant utilise des outils pour se rendre anonyme et invisible sur le réseau.[30]

2.2.4 Protections contre ces attaques

- Contrôle d'accès aux ressources (également physiquement).

- Pare-feu : filtre les trames entre le réseau externe et le réseau interne.
- Audit : étudiez le fichier journal pour identifier les anomalies.
- Logiciel antivirus (2/3 des attaques sont des virus).
- Programme de test de vulnérabilité et de mauvaise configuration (Satan).
- Détection d'intrusion : détecte le comportement anormal de l'utilisateur ou les attaques connues. [25]

2.2.5 Les principales attaques contre les réseaux sans fil

Attaque Denial of Service

Une attaque par déni de service (en anglais Denial-of-Service attack , abrégé en DOS) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés [31].

Les attaques par déni de service trouvent leur origine dans la culture Hacker, il s'agit d'une forme d'amusement partagée par des accros de l'informatique. Elle consiste à importuner d'autres internautes en postant des contenus offensifs, répugnants ou tordus sur des forums de discussion [32].

ATTAQUES DOS (Denial-of-service attack) se présente par :

* Saturation de la bande passante pour empêcher toute communication
* débordement des tables de routages des nœuds servant de relais.
* épuisement des batteries des nœuds ayant une capacité réduite de batterie.

Attaque Spoofing

Dans le monde informatique, spoofing d'identité fait référence à une identité volée, lorsqu'une personne se fait passer pour une autre personne, organisation ou entreprise dans le but d'accéder à des informations personnelles sensibles, notamment les noms d'utilisateur et les mots de passe, les informations bancaires et les numéros de carte de crédit. spoofing d'identité fait à la fois partie de la configuration de l'hameçonnage et d'une technique permettant d'accéder directement à l'ordinateur ou au réseau informatique d'un individu ou d'une organisation.[33]

Attaque Hello flood

Certains protocoles de routage dans un réseau sans fil exigent des nœuds pour diffuser des messages Hello, à eux-mêmes annoncé à leurs voisins. Un nœud qui reçoit un tel message peut supposer qu'il est dans une plage de l'expéditeur. Certains nœuds de mauvaise conduite dans le flot de réseau continu le paquet Hello. Sans la maintenance de l'intervalle de Hello. Il crée les perturbations dans le fonctionnement du réseau. Cette activité détourne l'action du nœud légitime dans le réseau.[34]

Attaque Sniffing

Sniffing en termes généraux fait référence à enquêter secrètement sur quelque chose afin de trouver des informations confidentielles. Du point de vue de la sécurité de l'information, le Sniffing fait référence à l'exploitation du trafic ou à l'acheminement du trafic vers une cible où il peut être capturé, analysé et surveillé. Le Sniffing est généralement effectué pour analyser l'utilisation du réseau, résoudre les problèmes de réseau, surveiller la session à des fins de développement et de test [35].

FIGURE 2.1 – L'attaque sniffing

Attaque man in the middle

Man in the middle attack (en abrégé MITM) est une attaque cryptographique sur un canal de communication par un tiers malveillant, qui contrôle un canal de communication confidentiel ou personnel entre deux ou plusieurs points de communication. Dans cette

cyberattaque, l'attaquant peut contrôler (lire, modifier, intercepter, changer ou remplacer) le trafic de communication entre les victimes. Mais en utilisant le protocole MITM, l'attaquant non authentifié ne laisse aucun indice ou trace de son interception de cette cybercriminalité, bref l'attaquant reste invisible pour les victimes.[36]

Attaque Sybil

Les attaques Sybil sont bien connues dans l'environnement des réseaux peer-to-peer, filaires et sans fil. Dans sa forme de base, les pairs représentant l'attaquant vont générer autant d'identités que possible et les traiter comme de multiples pairs dans le système [37] pour perturber le comportement normal du système.

Le nombre d'identités qu'un attaquant peut générer dépend uniquement de la capacité de l'attaquant, qui est limitée par la bande passante requise pour répondre aux demandes simultanées d'autres pairs dans le système et la mémoire requise pour stocker les informations de routage du serveur. Les autres pairs correspondant à chaque identité Sybil générée et les ressources informatiques nécessaires pour traiter les requêtes simultanées sans retard significatif. Avec la forte croissance du matériel (Par exemple, en termes de stockage et de puissance de traitement) et la diffusion à grande échelle d'Internet haut débit à des vitesses de bande passante élevées, même les attaquants fonctionnant sur du matériel «basique» peuvent causer des dommages, ce qui est important pour les grands systèmes. [38]

Attaque wormholle

Les attaques Wormhole sont une attaque sérieuse contre les réseaux sans fil. Deux ou plusieurs attaquants sont connectés via une liaison hors canal à grande vitesse appelée liaison trou de ver. Lors d'une attaque par un ver, deux attaquants forment un «tunnel» pour transmettre des paquets de données et les rediffuser sur le réseau. Cette attaque a un impact important sur les réseaux sans fil, en particulier les protocoles de routage. Lorsque les messages de contrôle de routage sont acheminés dans la mauvaise direction, le mécanisme de routage peut provoquer confusion et destruction. Le tunnel formé entre deux assaillants en collusion s'appelle un lien de trou de ver. [39]

La figure 2.2 montre le fonctionnement de l'attaque par trou de ver. Le paquet de données reçu par le noeud S2 est rejoué par le noeud S9, et vice versa. Généralement, il faut quelques sauts pour un paquet de données d'un emplacement près de S2 à un emplacement près de S9. Les paquets transmis près de S2, qui traverse le trou de ver, atteindront S9 avant que le paquet ne passe par plusieurs sauts dans le réseau. L'attaquant peut tromper S1 et S10 en leur faisant croire qu'ils sont voisins en transmettant des messages de routage, puis supprimer sélectivement le message de données pour interrompre la communication entre S1 et S10.

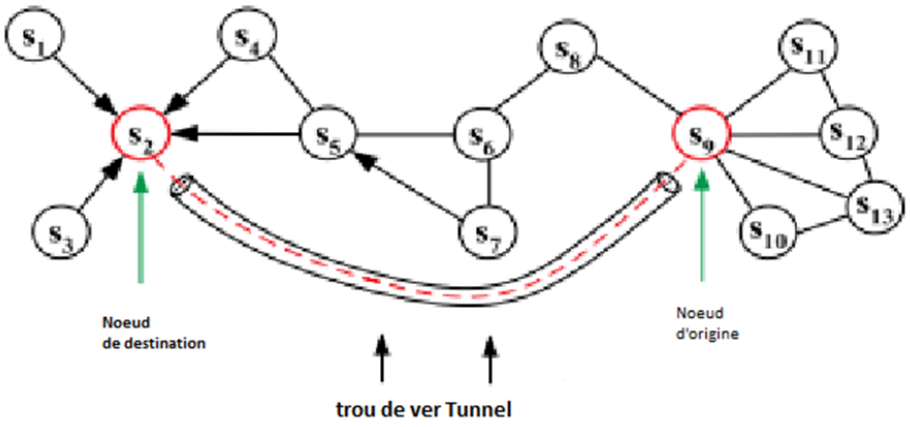


FIGURE 2.2 – Attaque de trou de ver dans le protocole de routage.[**?**]

Attaque BLACKHOLE

Une attaque de BLACKHOLE est une attaque active conçue pour rejeter certains messages de routage reçus par un nœud. L'abandon de paquets peut être effectué d'une manière qui n'augmente pas la suspicion d'attaques de nœuds. Il a des variantes plus ou moins similaires, mais des objectifs différents. Dans ces variantes, on peut citer [40] :

- **boucle de routage (routing loup) :** permet aux nœuds de créer des boucles dans le réseau .
- **trou gris (Gray hole) :** autorise uniquement le routage des paquets de données à transmettre et à transférer des données.
- **courrier noir (Black mail) :** permettant à un nœud attaquant d'isoler un autre nœud en envoyant des messages d'erreur (tels que des erreurs de routage).

2.3 Les protocoles de routage dans les réseaux Mobile adhoc (MANET)

Le routage peut être défini comme un échange de données entre deux hôtes dans un réseau. La méthode de routage consiste à transmettre le paquet vers son nœud de destination en utilisant le chemin optimal. Cet itinéraire est mesuré selon différentes métriques telles que le trafic, la sécurité, etc.

2.3.1 Catégorie des Protocoles de routages

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 .

La figure 2.3 ci-dessous présente une classification des protocoles de routage pour réseaux Ad-hoc

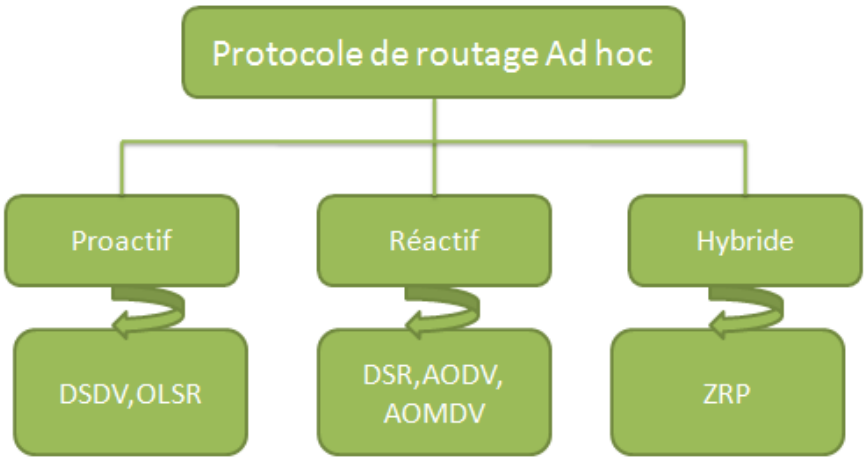


FIGURE 2.3 – Classification des protocoles de routage

Les protocoles de routage proactifs

Dans ce type de protocoles de routage, l´établissement de routes se fait a l'avance. Chaque nœud met a jour régulièrement les données de routage de manière a obtenir le plus court chemin (nombre de nœuds intermédiaires, ou bien nombre de sauts) vers tous les nœuds du réseau. De ce fait, si un nœud veut transmettre un paquet vers une destination, il consulte sa table de routage qui lui indique le chemin a suivre.[41]

Ce protocole utilise deux principales méthodes :

- Méthode Etat de Lien (Link State).
- Méthode du Vecteur de Distance (Distance Vector).

Les protocoles de routage proactifs

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.[41]

Ces protocoles peuvent être classifiés en deux catégories : routage source et routage saut-par-saut 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. [42]

Les protocoles de routage proactifs

Cette catégorie de protocoles est une combinaison d'un protocole réactif et d'un protocole proactif. Ce type de protocoles adopte une approche proactive pour avoir des informations sur les voisins les plus proches, qui se trouvent au maximum a deux sauts du nœud mobile et utilise une approche réactive au-delà de cette limite, afin de chercher des routes. L'un des protocoles utilises dans ce type est, ZRP (ZoneRouting Protocol) et CBRP (Cluster Based Routing Protocol).l'idée principale derrière ces protocoles est de réduire la surcharge de contrôle et la latence causée par la découverte d'itinéraire . [43][44]

2.3.2 Le Problème du 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.

2.3.3 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 [45][46].

2.3.4 Gestion de la table de routage du Protocole AODV

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

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. Ce message contient :

- l'adresse source.
- Le numéro de séquence source.
- L'ID de la demande.
- l'adresse de destination.
- numéro de séquence de destination.
- le nombre de saut. [67][68]

source	Num.seq Source	Broadcast id	Destination	Num.seq Destination	Nombre desaut

TABLE 2.1 – Le format de RREQ

Réponse de route RREP(ROUTE REPly)

C'est 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.

- l'adresse source.
- l'adresse de destination.
- numéro de séquence de destination.
- le nombre de saut. [47][48]

- Temps en millisecondes pour lequel les nœuds recevant la RREP et ils considèrent la route valide. [47][48]

source	Destination	Num.seq Destination	Nombre desaut	Life time

TABLE 2.2 – Le format de RREP

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 [49][50].

2.3.5 Les mécanismes d'AODV

Découverte de route

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 avec ses voisins immédiats. Quand un nœud source S veut envoyer des données à un destinataire D et qu'aucune route vers cette destination n'est stockée dans la table de routage de la source, le nœud S initialise une procédure de découverte de routes.[51]

- Un nœud diffuse une requête de route (RREQ) pour connaître la route vers une certaine destination si celle-ci n'est pas connue au préalable, Le champ numéro de séquence de destination du paquet RREQ, contient la dernière valeur connue du numéro de séquence, recopiée de la table de routage. Si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut.
- Après la diffusion du RREQ, la source attend le paquet réponse de route (RREP). Si ce dernier n'est pas reçu durant une certaine période (appelée RREP_WAIT_TIME), 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.[52]

- Chaque nœud qui reçoit le message RREQ recherche dans sa table de routage locale s'il existe une route vers le nœud destinataire sinon le nœud qui traite la requête RREQ incrémente le nombre de sauts et la diffuse à nouveau. [51]
- Lorsque la requête atteint la destination ou un nœud qui connaît une route vers la destination, une réponse RREP (Route REPly) est diffusée sur la même route de réception du RREQ (chemin inverse).[52]

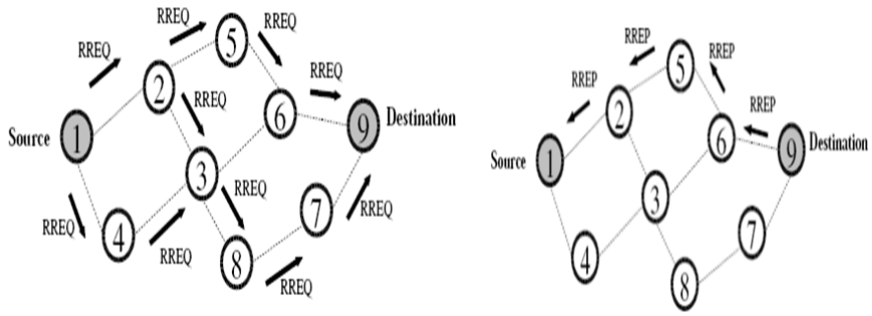


FIGURE 2.4 – (a) Inondation de RREQ, (b) revoie du RREP dans AODV.

Maintenance de route

L'échange des messages HELLO entre les voisins immédiats permet de mettre à jour la liste des voisins de chaque nœud.Chaque noeud dans AODV maintient une liste des ses voisins. Avec une cadence d'une fois par seconde . Si un noeud ne reçoit pas d'un voisin trois messages HELLO consécutifs (pas de messages pendant trois secondes) le lien avec le voisin est considéré invalide. [53]

Si un lien entre deux noeuds est invalide (à cause de la mobilité ou la défaillance d'un noeud), les noeuds utilisant se lien sont prévenus par un message d'erreur (RERR) , ils vont alors diffusés une autre requêtte.

La figure suivante illustre la coupure d'un lient entre deux noeuds et l'envoi du RERR dans AODV. [51]

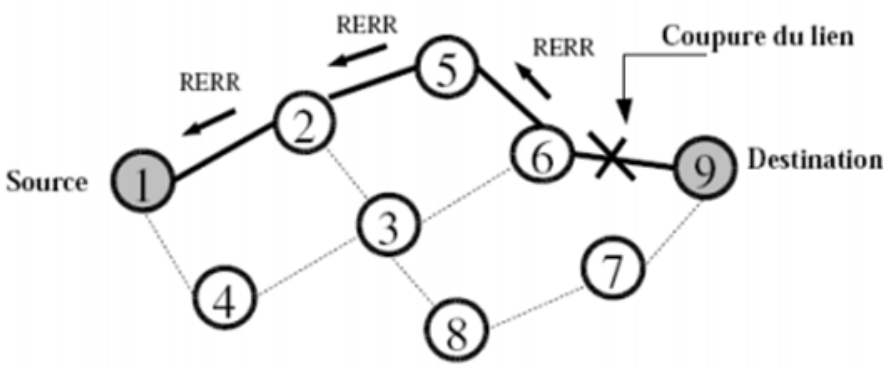


FIGURE 2.5 – Coupure de route et envoie du RERR dans AODV.

La maintenance peut être résumée dans les trois points suivants [54] :

- Des messages HELLO périodiques pour détecter les coupures de liens.
- Si la source se déplace, la procédure de détermination de route peut être ré initié.
- Si un nœud intermédiaire ou la destination se déplacent, un RREP spécial est émis au nœud source (reconstruisant la route au passage).

2.3.6 Les avantages d'AODV

⋆ L'AODV a un avantage dans en haut sur les protocoles simples qui doivent garder le trajet entier de l'hôte source à l'hôte de destination dans leurs messages. Le RREQ et les messages RREP, qui sont responsables de la découverte de trajet, n'augmentent pas de façon significative l'aérien de ces messages de contrôle. [55]

⋆ AODV réagit relativement vite aux changements topologiques dans le réseau et le fait d'actualiser seulement les hôtes qui peuvent être affectés par le changement, en utilisant le message RRER. Bonjour les messages, qui sont responsables de la maintenance de trajet, sont aussi limités pour qu'ils ne créent pas inutile en haut dans le réseau.[56]

⋆ Le protocole AODV est un protocole de routage plat, il ne nécessite aucun système administratif central pour gérer le processus de routage.[55]

⋆ Le protocole AODV jouera mieux dans les réseaux avec la circulation statique avec le nombre de source et les paires de destination est relativement petit pour chaque hôte.[56]

⋆ Le protocole AODV est une boucle libre et évite le compte au problème d'infinité, qui étaient typiques au vecteur de distance classique routing des protocoles, par l'usage des nombres d'ordre.[56]

2.3.7 Description de l'attaque BLACKHOLE dans le protocole AODV

Dans le protocole AODV, lorsqu'il n'y a pas de route vers une cible donnée dans la table de routage du nœud d'envoi, il lancera une demande de découverte de route en diffusant le message RREQ. A ce moment, l'attaquant peut intervenir en créant un BLACKHOLE dans le réseau. Ensuite, nous présenterons en détail Des trous noirs apparaissent dans le protocole AODV.

Spécification de l'attaque de BlackHole dans AODV

Les attaques BlackHole ou par perte de paquets sont le résultat de fausses RREQ avec de très grands numéros de série émis par des nœuds malveillants. Le nœud source insère ce numéro dans la table de routage et le considère comme le chemin le plus court vers la destination , tout en ignorant les paquets de données provenant d'autres nœuds, de sorte que le nœud malveillant ait la possibilité de devenir sa destination préférée et de continuer à lui envoyer des paquets de données. Dernière suppression, donc cela n'arrivera jamais à d'autres.[52]

L'attaque vise à modifier le protocole de routage afin que le trafic se propage à travers des nœuds spécifiques contrôlés par l'attaquant. Dans le processus de découverte de route, le nœud source envoie des paquets de données de type RREQ (Route REQuest) au nœud intermédiaire pour trouver une nouvelle route vers la destination. Le nœud endommagé renverra immédiatement les informations à la source indiquant que ces nœuds ne font pas référence à la table de routage.[57]

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.[58]

Le nœud source suppose que le processus de découverte d'itinéraire est terminé, il ignore donc les autres messages RREP (route REPly) des autres nœuds et choisit l'itinéraire via le nœud endommagé pour envoyer le paquet de données. Le nœud endommagé accomplit cela en attribuant un numéro de séquence élevé au paquet repensé. L'attaquant effacera les messages reçus au lieu de les renvoyer selon les conditions du protocole.[59]

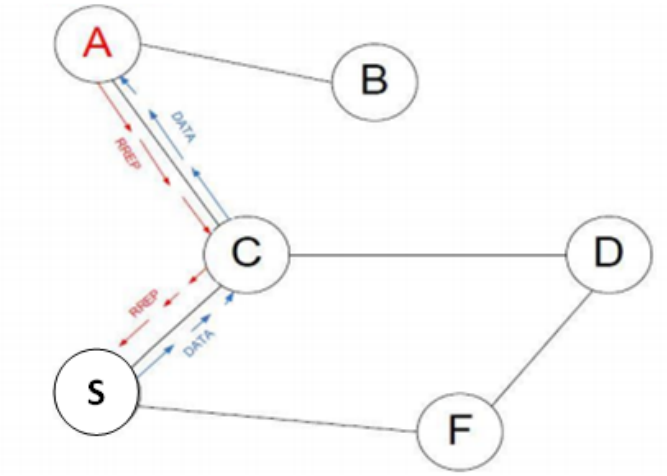


FIGURE 2.6 – Spécification de l'attaque de BlackHole dans AODV.

Dans l'attaque de BLACKHOLE AODV, comme vous pouvez le voir sur la figure 3.4, le nœud malveillant «A» découvre d'abord la route active entre le nœud émetteur «S» et le nœud de destination «D». Après cela, le nœud malveillant «A» envoie un message RREP qui contient l'adresse de destination usurpée comprenant un petit nombre de sauts et un grand numéro de séquence que la normale au nœud «C». Le nœud «C» transmet RREP au nœud émetteur «S». L'expéditeur utilise maintenant cette route pour envoyer les informations et de cette manière, le nœud malveillant recevra les informations. Et les informations seront alors sup-

primées. De cette manière, l'émetteur et le nœud récepteur ne seront plus en situation de diffuser des informations en état d'attaque de BLACKHOLE.[52]

2.3.8 Conclusion

Les réseaux Sans Fils sont par nature plus sensibles aux problèmes de sécurité. L'intrusion sur le support de transmission est plus facile en menant des attaques qui peuvent brouiller les bandes de fréquences utilisées. D'autre part. En plus, on remarque que le routage pose des problèmes spécifiques tel que la possibilité d'être exposée à des attaques qui peuvent détourner le trafic en transit. Pour garantir une transmission efficace des paquets et au même temps pallier à l'inconvénient de la sécurité.

Chapitre 3

Etude de l'attaque BlackHole et la solution proposée

3.1 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. Plusieurs protocoles ont été proposés au niveau ad hoc.

Dans ce chapitre nous allons présenter le protocole utilisé ainsi que l'environnement de travaille choisi et la solution proposée.

3.2 Travaux et solutions proposées pour l'attaque du BlackHole

3.2.1 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** [60]

  ont proposé une solution pour résoudre l'attaque du BLACKHOLE en modifiant le protocole AODV. Dans cette méthode, chaque nœud intermédiaire doit inclure les informations de prochain saut « next hop » lors de l'envoi de paquets RREP.

  Une fois que la source reçoit le paquet RREP et avant d'envoyer le paquet, elle va extraire l'adresse du prochain saut « next hop » et lui envoyer une nouvelle demande de route (FurtherRequest), c'est pour vérifier si elle a une route vers le nœud intermédiaire qui envoie le message de réponse .

  La source vérifie les informations du paquet FRREP et fonctionne selon les règles suivantes :

  — 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.

  — 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 an d'isoler le nœud malveillant.

  — 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 an d'isoler le nœud malveillant.

Le mécanisme proposé est efficace pour détecter les attaques Blackhole, mais l'envoi de paquets FRREQ du nœud source au « next hop » et l'attente des paquets FRREP du « next hop » augmentera la charge de routage « overhead ». La distance entre la source et « next hop » est importante, en particulier lorsque ce mécanisme est appliqué sur un réseau à grande échelle et que la distance entre la source et le nœud malveillant est longue.

- La solution proposée par **Al-Shurman** [61]

  a proposé deux solutions à l'attaque BLACKHOL dans le protocole AODV.

  La première solution proposée est de trouver plus d'un itinéraire (au moins trois itinéraires différents) jusqu'à la destination. La source utilise ces trois routes pour envoyer des paquets RREQ au nœud de destination. La destination, les nœuds malveillants et les nœuds intermédiaires répondront à ce paquet.

  La deuxième solution proposée utilise le numéro de séquence contenu dans l'en-tête de chaque paquet de données. Dans ce cas, le nœud doit avoir deux tables supplémentaires. Le premier tableau contient le numéro de séquence du dernier paquet envoyé à chaque nœud du réseau, et le deuxième tableau contient le numéro de séquence reçu de chaque expéditeur.

  Dans la phase de réponse d'itinéraire, le nœud intermédiaire ou la cible doit contenir le numéro de séquence du dernier paquet de données reçu de la source qui a lancé la demande d'itinéraire. Une fois que la source a reçu ce RREP, elle extraira le dernier numéro de série et le comparera à la valeur enregistrée dans le tableau. S'il correspond, il sera transmis, sinon ce sera un nœud malveillant, puis un message d'alerte sera diffusé pour avertir le réseau sur ce nœud.

- **Houda Ha** [52]

  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 la confiance d'un nœud, chaque nœud du réseau maintient une table d'activité, qui stocke l'identifiant d'un nœud, le nombre de paquets de données, le nombre de demande de routage de paquets (RREQ) et le reçu du nœud Le nombre de paquets de réponse (RREP).

  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 .
- **H.A.Esmaili** [62]

  font une étude sur la performance du protocole de routage AODV sous l'attaque de BLACKHOLE, Ils ont proposé un objectif qui utilise AODV comme protocole de routage, qui attaque les réseaux ad hoc, et définit une solution basée sur les problèmes suivants pour améliorer la sécurité de ces réseaux : les réseaux ad hoc mobiles sont efficaces pour de nombreux types de réseaux Les attaques (telles que les attaques de trous noirs) sont vulnérables.

- **Romina Sharma** [63]

  a étudié le protocole de routage AODV dans les réseaux mobiles Ad hoc. Ils ont suggéré : Modifier le protocole de routage AODV pour éviter les attaques de trous noirs et mesurer l'impact de cette attaque sur le réseau. Mobile Ad hoc et le comparer avec AODV selon les questions suivantes Comparez les protocoles modifiés : en raison des failles de sécurité dans le protocole de routage, les réseaux mobiles Ad hoc ne peuvent pas être protégés contre les attaques de nœuds malveillants, telles que les attaques. Du BLACKHOLE.

Les chercheurs ont proposé des améliorations au protocole AODV pour contrer les attaques coopératives de trous noirs.

Dans le contenu suivant, nous introduirons des hypothèses sous lesquelles notre schéma est fonctionnel, et nous détaillerons notre approche de sécurité contre l'attaque du BLACKHOLE.

3.2.2 Solution proposée

Dans la plupart des applications des réseaux sans ls, 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.

Description de la Solution proposée

nous nous somme inspiré de la solution IDS (Intrusion Détection System) publier par dokurer 2006 [64] qui est un autre Protocole AODV modifié qui est conçu pour réduire les effets néfastes des attaques par BLACKHOLE. Le protocole d'atténuation est mise en œuvre en modifiant le mécanisme de mise à jour du routage dans le Protocole AODV.

Le processus consistant à ignorer la première voie d'établissement est ajouté au protocole logiquedans le processus de mise à jour du routage.

La stratégie principale est que lorsque le réseau est sous attaque, de multiples RREP provenant d'un chemin différent sont générés.

Ce protocole suppose que le premier message RREP qui arrive à un nœud provient d'un nœud malveillant, et donc la méthode d'atténuation dans idsAODV est d'ignorer ce RREP pour éviter Le Nœud Malicieux .l'entrée de l'itinéraire est mise à jour dans la table d'acheminement.Cette méthode permet d'éviter Le Malicieux Nœud (Blackhole).

en suivant cette algorithme :

Étape 1 : Le nœud source envoi une Requête broadcaste RREQ qui contiennent l'adresse source, l'ID de la demande, le numéro de séquence source, l'adresse de destination.

Étape 2 : Les nœuds voisins reçoivent la requête RREQ, vérifiés dans la table de routage et si la table est vide , elle transmettra la requête pour atteindre la destination.

Étape 3 : Le nœud de destination reçoit la requête RREQ, et génère le la requête RREP qui se compose de l'adresse source, de l'adresse de destination, numéro de séquence de destination, nombre de sauts et durée de vie.

Étape 4 : Le nœud de destination diffuse ensuite le contrôle RREP en unicast vers le même itinéraire utilisé pour la requête RREQ. Le nœud source reçoit le contrôle RREP de tous les nœuds intermédiaires.

Étape 5 : La source utilise la première requête RREP pour lancer le transfert de données.

Étape 6 : Si une deuxième Requête RREP arrive, il passe à la nouvelle route puisqu'il est supposer que le BLACKHOLE ne perde pas de temps à vérifier la table d'acheminement et le RREP La requête du BLACKHOLE arrive plus tôt que la destination réelle

3.3 Simulation de la solution IDSAODV

3.3.1 Environnement de Simulation

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 ont donné des résultats.

3.3.2 Présentation de Network Simulation 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.

3.3.3 Implémentation du protocole blackhole AODV et IDS AODV dans NS2.35

Création du Nœud Malicieux (Blackhole)

Etape 1 :

nous devons mettre en œuvre un nouveau protocole de routage dans ns 2.35. La mise en œuvre d'un nouveau protocole de routage unicast MANET dans le NS-2 est décrite dans la référence. [65].

Tous les protocoles de routage dans le simulateur de réseau 2.35 sont installés dans le répertoire de "ns-2.35". Nous dupliquons d'abord le protocole AODV dans le répertoire ns-2.35 et changeons le nom de ce répertoire en "blackholeaodv".

Dans ce répertoire blackholeaodv, le nom de tous les fichiers étiquetés "aodv" est changé en "blackholeaodv", par exemple blackholeaodv.cc, blackholeaodv.h, blackholeaodv.tcl etc. Tous les noms de classes, fonctions, variables et constantes du répertoire blackholeaodv ont changé.

Pour intégrer le nouveau protocole blackholeaodv dans le simulateur NS-2.35, nous avons modifié deux fichiers qui sont utilisés globalement dans ce simulateur. Dans le fichier **" ns-lib.tcl"**, nous ajoutons d'abord les lignes indiquées dans les figure 3.1 pour créer la procédure d'agent pour le BLACKHOLE.

```
if {$rtAgentFunction_ != ""} {
        set ragent [$self $rtAgentFunction_ $node]
} else {
        switch -exact $routingAgent_ {
            DSDV {
                    set ragent [$self create-dsdv-agent $node]
            }
            DSR {
                    $self at 0.0 "$node start-dsr"
            }
            AODV {
                    set ragent [$self create-aodv-agent $node]
            }
            blackholeAODV {
                    set ragent [$self create-blackholeaodv-agent $node]
            }
```

(a)

```
        return $ragent
}

Simulator instproc create-aodv-agent { node } {
        #  Create AODV routing agent
        set ragent [new Agent/AODV [$node node-addr]]
        $self at 0.0 "$ragent start"     ;# start BEACON/HELLO Messages
        $node set ragent_ $ragent
        return $ragent
}

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

(b)

FIGURE 3.1 – Ajout de l'agent blackhole.

Etape 2 :

Dans aodv.cc, la fonction "recv" traite le paquet en fonction du type de paquet. Si le type de paquet est un paquet acheminé par la route AODV, tel que RREQ, RREP, RERR, il envoie le paquet à la fonction "recvAODV". Lorsque le type de paquet reçu est un paquet de données, le protocole AODV l'envoie à l'adresse de destination.

Dans la figure , la première condition "if" permet au nœud de recevoir des paquets de données s'il est la destination et la condition "else" consomme tous les paquets restants comme un nœud blackhole comme illustré dans la figure 3.2.

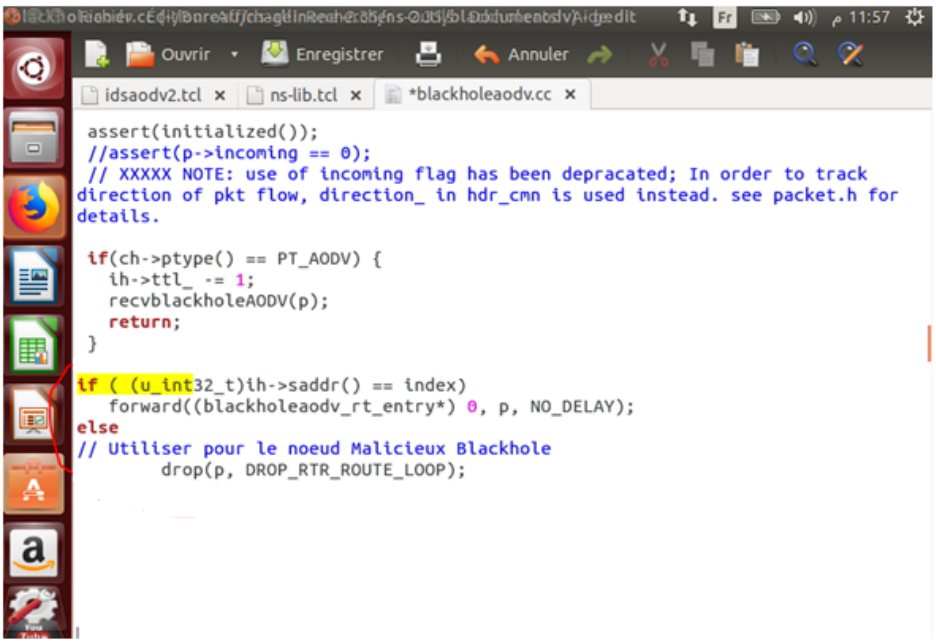


FIGURE 3.2 – montrant le fonctionnement ajoutée a la méthode recevoir.

Etape 3 :

Pour générer le comportement du BLACKHOLE, nous devons modifier le fichier blackholeaodv.cc en ajoutant le faux RREP. Le faux message RREP indique qu'il a le numéro de séquence le plus élevé, que le numéro de séquence est 4294967295 et que le nombre de sauts est 1.le numéro de séquence le plus élevé du protocole AODV est 4294967295, valeur entière non signée de 32 bits .

Les lignes de la figure 3.3 sont ajoutées au fichier aodv.cc pour générer les caractéristiques du nœud de BLACKHOLE.

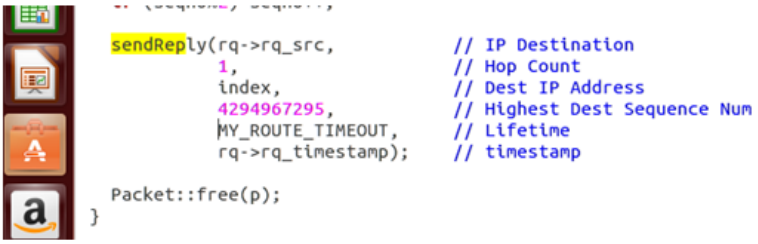
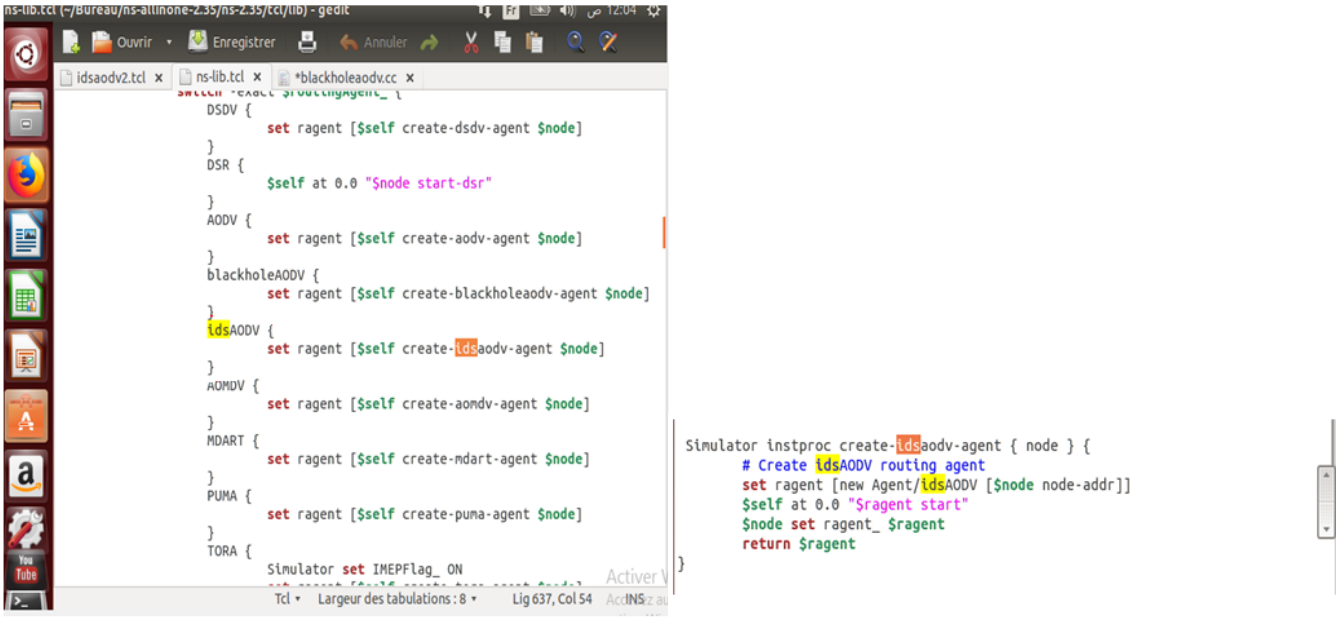


FIGURE 3.3 – Le faux RREP de BLACKHOLE.

Création du Protocole IDSAODV

Etape 1 :

nous avons dupliqué le protocole "AODV", en le changeant en "idsAODV" comme nous l'avons fait dans "blackholeaodv". pour la solution, nous avons dû modifier la fonction de réception RREP (recv Reply) et créer un mécanisme de sauvegarde RREP. Ce mécanisme de sauvegarde RREP compte le deuxième message RREP. Dans un premier temps, nous avons changé le nom de tous les fichiers dans le répertoire "aodv" cloné en idsAODV. Pour intégrer le nouveau protocole bds AODV dans le simulateur NS-2.35, le fichier " nslib. tcl" est d'abord modifié, où les agents de protocole sont codés, comme le montre la figure 3.4.



(a) (b)

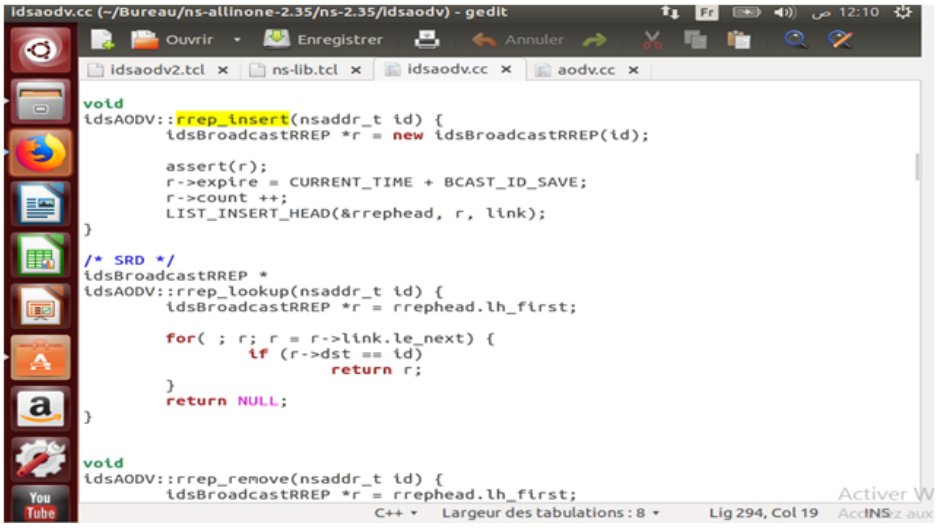
FIGURE 3.4 – Ajout du protocole proposé.

Etape 2 :

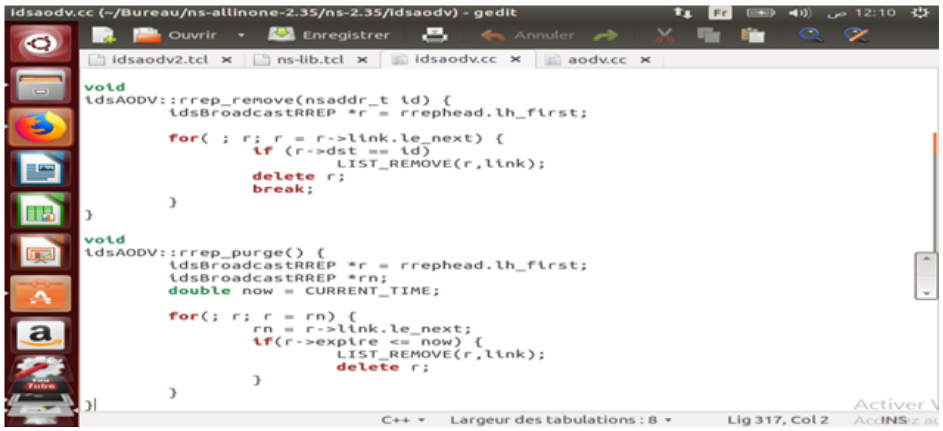
Pour détecter les attaques par BLACKHOLE, nous créons un mécanisme de sauvegarde RREP dans la fonction recv Reply du fichier idsAODV.cc qui est présenté à la figure 3.5.

Dans le mécanisme de sauvegarde des RREP, la fonction "rrep_insert" est utilisée pour ajouter des messages RREP, la fonction "rrep_lookup" est utilisée pour recher-

cher tout message RREP existant, la fonction "rrep_remove" supprime tout enregistrement de message RREP provenant d'un nœud défini et la fonction "rrep_purge" doit être supprimée périodiquement de la liste si elle a expiré.



(a)



(b)

FIGURE 3.5 – Mécanisme de sauvegarde des RREP dans le protocole idsAODV.

Etape 3 :

Nous vérifions d'abord si le message RREP est arrivé pour lui-même, s'il est arrivé pour lui-même alors la fonction recherche le message RREP si elle a la solution la fonction de réception du message RREP est déjà arrivée. S'il n'est pas arrivé, elle insère le message RREP pour son adresse de destination et revient de la fonction.

Si le message RREP est déjà arrivé ou mis en cache pour la même adresse de destination, la fonction RREP normale est alors exécutée. Si le message RREP n'est pas arrivé pour lui-même, le nœud transmet le message à son voisin approprié.

Les blocs de code représentés à la figure 3.6 montrent comment le idsAODV s'exécute.

```
void
idsAODV::recvReply(Packet *p) {
//struct hdr_cmn *ch = HDR_CMN(p);
        struct hdr_ip *ih = HDR_IP(p);
        struct hdr_aodv_reply *rp = HDR_AODV_REPLY(p);
        idsaodv_rt_entry *rt;
        char suppress_reply = 0;
        double delay = 0.0;
        int count;

        idsBroadcastRREP *r = rrep_lookup(rp->rp_dst);

#ifdef DEBUG
        fprintf(stderr, "%d - %s: received a REPLY\n", index, __FUNCTION__);
#endif // DEBUG


        if (r == NULL) {
                count = 0;
                rrep_insert(rp->rp_dst);
        } else {
                r->count++;
                count = r->count;
        }

        /*
```

FIGURE 3.6 – la fonction de réception du protocole idsAODV.

3.3.4 Visualisation des résultats sous NS2.35

Paramètre de simulation

Le tableau (TAB 3.1) contient les paramètres réseau sur lequel les simulations sont été effectuées pour la simulation du protocole Aodv sans noeud malicieux entre le noeud 0 (source) et le noeud 3 (destination) .

Paramètre	Valeurs
Simulateur	NS2.35
Protocole	AODV
Nombre de Noeud	7
Nombre de Noeud Malicieux	0
Temps de simulation (ms)	99
Temps d'arriver des paquets(sec)	Exponentiel
Terrain de simulation	800*541

TABLE 3.1 – Paramètres de simulation pour le Protocole AODV sans Blackhole

On peut visualiser le placement des nœud dans la figure 3.7 :

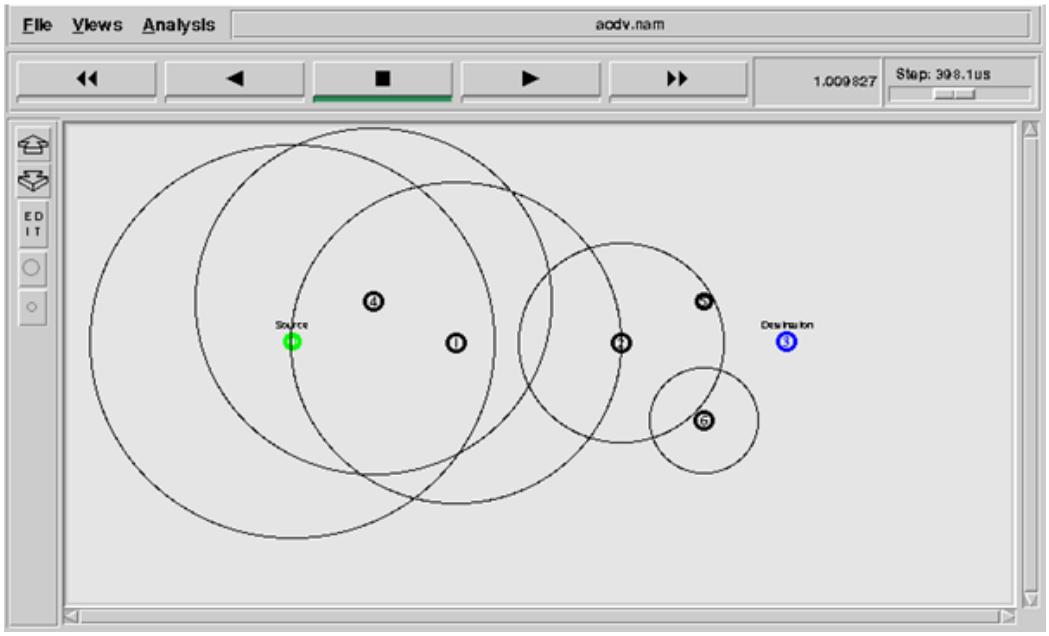


FIGURE 3.7 – Simulation du AODV sans Blackhole.

on a eu comme résultat le nombre de paquet envoyé : 1238 , le nombre de paquet reçu : 1238 , le taux de paquet perdu est de 0% ,comme le montre la figure 3.8 :

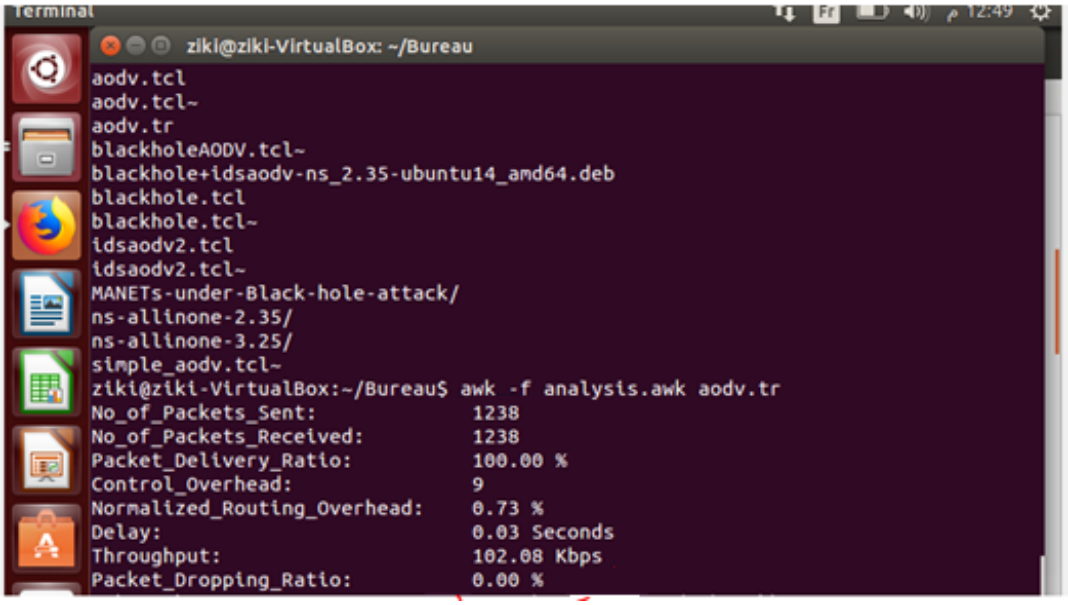


FIGURE 3.8 – Le taux de paquets envoyée et Reçu .

Le tableau (TAB 3.2) contient les paramètres réseau sur lequel les simulations sont été effectuées pour la simulation du protocole Aodv avec le nœud malicieux entre le nœud 0 (source) et le nœud 3 (destination) .

Paramètre	Valeurs
Simulateur	NS2.35
Protocole	AODV,blackholeAODV
Nombre de Noeud	7
Nombre de Noeud Malicieux	1
Temps de simulation (ms)	99
Temps d'arriver des paquets(sec)	Exponentiel
Terrain de simulation	800*541

TABLE 3.2 – Paramètres de simulation pour le Protocole AODV sans Blackhole

On peut visualiser le placement des nœud ainsi que le blackhole dans la figure 3.9 :

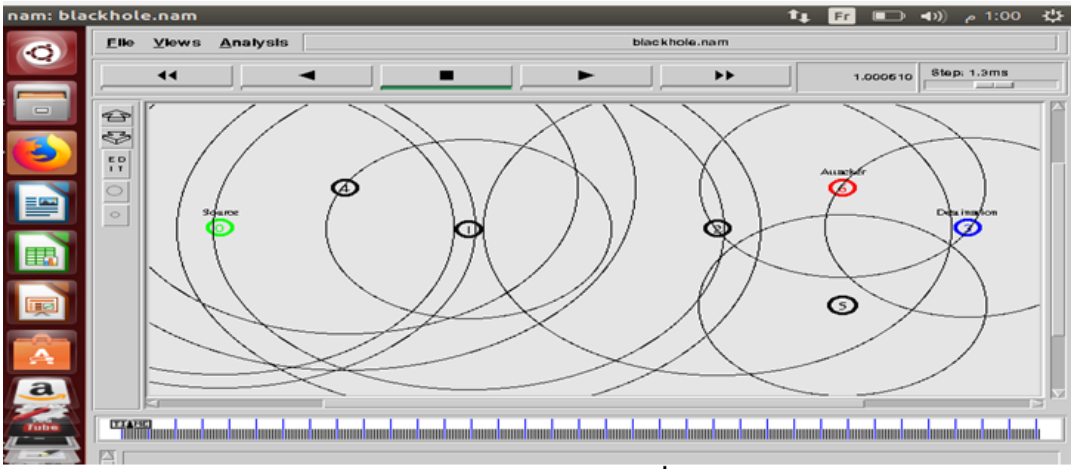


FIGURE 3.9 – Simulation du AODV Avec le Blackhole.

on a eu comme résultat le nombre de paquet envoyé : 1238 , le nombre de paquet reçu : 1 , le taux de paquet perdu est de 99% ,comme le montre la figure 3.10 :

```
ziki@ziki-VirtualBox:~/Bureau$ awk -f analysis.awk blackhole.tr
No_of_Packets_Sent:              1238
No_of_Packets_Received:          1
Packet_Delivery_Ratio:           0.08 %
Control_Overhead:                9
Normalized_Routing_Overhead:     900.00 %
Delay:                           0.00 Second
Throughput:                      0.00 Kbps
Packet_Dropping_Ratio:           99.92 %
```

FIGURE 3.10 – Le taux de paquets supprimer par le blackhole.

Le tableau (Table 3.3) contient les paramètres réseau sur lequel les simulations sont été effectuées pour la simulation du protocole idsAODV qui contient la solution proposé, entre le nœud 0 (source) et le nœud 3 (destination) .

Paramètre	Valeurs
Simulateur	NS2.35
Protocole	idsAODV
Nombre de Noeud	1
Nombre de Noeud Malicieux	0
Temps de simulation (ms)	99
Temps d'arriver des paquets(sec)	Exponentiel
Terrain de simulation	800*541

TABLE 3.3 – Paramètres de simulation pour le Protocole idsAODV

On peut visualiser le placement des nœud ainsi que le blackhole en utilisant le protocole idsAODV qui contient la solution proposé dans la figure 3.11 ,3.12 :

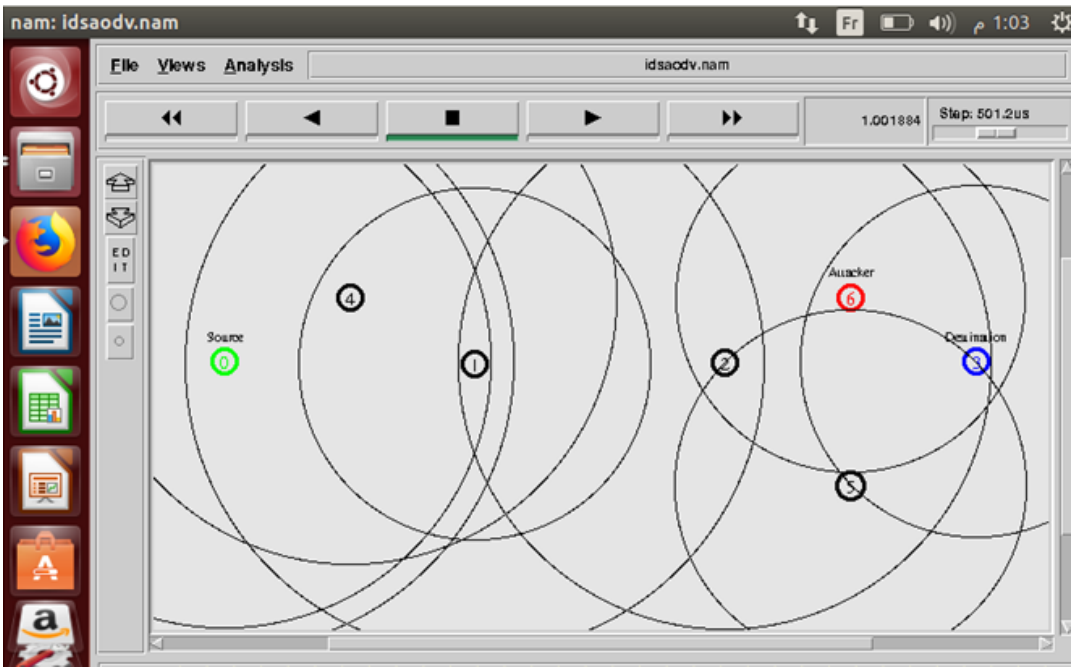


FIGURE 3.11 – Simulation du idsAODV .

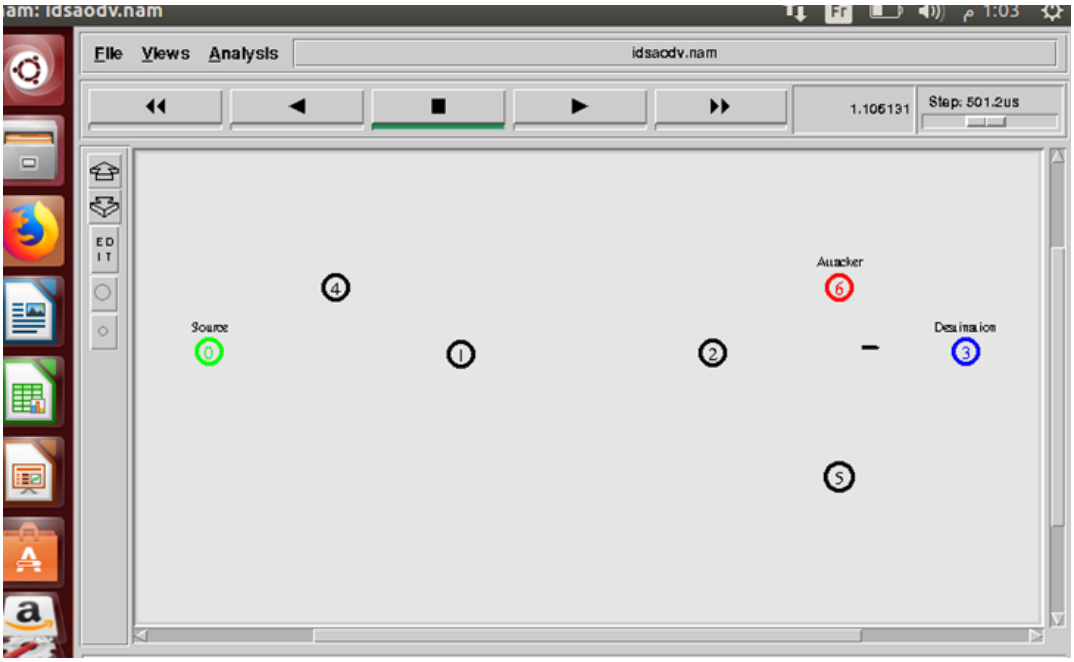


FIGURE 3.12 – montrant l'arrivage du paquet vers la destination.

on a eu comme résultat le nombre de paquet envoyé : 1238 , le nombre de paquet reçu : 1238 , le taux de paquet perdu est de 0% ,comme le montre la figure 3.13 :

```
ziki@ziki-VirtualBox:~/Bureau$ awk -f analysis.awk idsaodv.tr
No_of_Packets_Sent:              1238
No_of_Packets_Received:          1238
Packet_Delivery_Ratio:           100.00 %
Control_Overhead:                10
Normalized_Routing_Overhead:     0.81 %
Delay:                           0.03 Seconds
Throughput:                      102.08 Kbps
Packet_Dropping_Ratio:           0.00 %
ziki@ziki-VirtualBox:~/Bureau$
```

FIGURE 3.13 – Le taux de paquets envoyer et reçu a la présence du nœud malicieux.

3.4 conclusion

Dans ce chapitre, nous avons mené des expériences sur le trac de données, dans le premier cas, nous avons envoyé le trac sans aucune attaque. Dans le second cas, nous avons introduit une attaque BlackHole sur les données envoyées, empêchant ainsi la réception des données. dans le second cas, nous avons intégré l'attaque et la solution proposée pour ce problème, qui s'est avérée efficace .

Conclusion générale et perspectives

La sécurité dans les réseaux sans fil est un challenge très intéressant, notamment dans les réseaux ad hoc où l'accès au médium physique est totalement libre. Les données transmises par les nœuds peuvent être interceptées ou modifiées. Les protocoles de routage multi-sauts dans les MANETs sont susceptibles á divers types d'attaque suite á la coopération des nœuds et aussi au manque d'une relation de confiance préalable entre eux.

L'attaque de trou noir black hole est une attaque active qui affecte le protocole de routage AODV, le nœud malveillant supprime tous les paquets des données détournées vers lui. Les notions présentées dans cette mémoi s'articulent autour de ce cadre.

Nous nous somme focalisés sur cette attaque dont le but d'isoler des noeuds 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 olutions proposées par les chercheurs nous ont poussés à chercher une autre solution.

Nous avons proposé un modèle permettant de mesurer l'impact de cette attaque sur ces fonctions réseau et simulé ce travail sous NS-2. Ensuite, nous avons réalisé un ensemble de simulations et présenté et expliqué les résultats obtenus.

Au terme de ce travail de recherche, on peut dire que la protection des protocoles de routage dans les réseaux ad hoc reste un réel défi. D'un point de vue, il sera

utile d'améliorer et d'optimiser de plus en plus les solutions de sécurité existantes pour rendre les réseaux ad hoc , plus fiables, plus efficaces et plus sécurisés pour le public.

Bibliographie

[1] BRAHIMI. Cour Réseau mobile. 2019-2020 . UNIVERSITE BOUIRA.

[2] Samir Athmani ; «Protocole de sécurité pour les réseaux de capteurs sans fil ». Thèse de Magistère ; Université de Hadj Lakhdar-Batna ; Juillet 2010.

[3] Boudjaadar Amina « Plateforme basée Agents pour l'aide à la conception et la simulation des réseaux de capteurs sans fil ». Thèse de Magistère ; Université de Skikda ; 2009/2010.

[4] https://www.epfl.ch/campus/associations/list/robopoly/kit-prisme-extension/module-bluetooth/, 26 mars 2020

[5] http://grouper.ieee.org/groups/802/15/Bluetooth/profile$_1 0_b .pdf, 26 mars 2020$

[6] J.Lanford-Home RF : Bringing Wireless Connectivity home-Intel Home RF technology Tutorial ; Avril 1999.

[7] ABOURA Wissam et BENHABIB Imane , Etude et caractérisation de la couche physique du standard IEEE802.16/WIMAX , Octobre 2013.

[8] K. Al Agha, G. Pujolle et G. Vivier. « Réseaux de mobiles et réseaux sans fil ». Paris : Édition Eyrolles, 2001 ,

[9] P. Roshan, et J. Leary « Réseaux WiFi : notions fondamentales ». Paris : CampusPress, Cisco Press, 2004.

[10] G. Pujolle, O. Salvatori et J. Nozick. « Les Réseaux, Édition 2005 ». Paris : Édition Eyrolles, 2004.

[11] https://web.maths.unsw.edu.au/ lafaye/CCM/wireless/wman.htm ,26 mars 2020.

[12] http://www.commentcamarche.net, site de documentation informatique 28 mars 2020.

[13] http://developer.att.com/devcentral/toolstechnologies/network/docs/DataCapabilitiesGPRStoHSDPA.pdf 28 mars 2020.

[14] Rapport sur la couverture et la qualité des services mobiles en France métropolitaine - p.12 à 15, et p.20, La variabilité des performances des réseaux mobiles.

[15] https://www.howtogeek.com/273745/what-is-4g-lte/ , 29 mars 2020.

[16] Tayeb Lemlouma. Le Routage dans les Réseaux Mobiles Ad Hoc. Mini projet proposé par Dr. Nadjib Badache septembre 2000.

[17] Messaoud Belloula ; « La géolocalisation dans les réseaux de capteurs sans fil ; Etude de cas : Utilisation en agriculture ».Thèse de Magistère ; Université Hadj Lakhder-Batna.

[18] Belkheir Khaled et Haned Ahmed ; « Réseaux WiFi ad hoc ». Mémoire d'ingéniorat ; Institut de télécommunication d'Oran ; Juin 2008.

[19] Lemlouma, T. (2000). Le routage dans les réseaux ad-hoc, Mémoire de maîtrise, Université des Sciences et de la Technologie Houari Boumèdiene.

[20] Mémoire ROUTAGE DANS LES RESEAUX MOBILES Ad Hoc PAR UNE APPROCHE A BASE D'AGENTS Présenté par : Mr BOUKHECHEM Nadhir Promotion 2007-2008.

[21] KHADIDJA AYAD Mémoire MAGISTER Thème "Sécurité du routage dans les réseaux Ad Hoc mobile" Option : Informatique Répartie et Mobile Présenté par : 14 Novembre 2012.

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

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

[24] paragraph https ://www.securiteinfo.com/divers/lexique.shtml 4 mai 2020

[25] https://www.securiteinfo.com/conseils/introsecu.shtml 4 mai 2020.

[26] https://www.ivision.fr/securite-informatique-les-attaques-informatiques-internes-en-forte-progression/ 16 mai 2020.

[27] https://www.amecsi.com/10-profils-de-pirates-informatiques/ 16 mai 2020.

[28] Lokbani, A. C., Lehireche, A., Hamou, R. M. (2013, June). Experimentation of Data Mining Technique for System's Security : A Comparative Study. In International Conference in Swarm Intelligence (pp. 248-257). Springer, Berlin, Heidelberg.

[29] Khader Mohamed EL Amine -Bourbig Mokhtar Conception Et Implémentation D'un Systeme De Détection D'intrusion Par Les Abeilles Sociales UNIVERSITE Dr. TAHAR MOULAY SAIDA Juin 2018.

[30] http://xenod.free.fr/0$_L a_s ecurite_i nformatique.htm Outils des attaquants 15 mai 2020.

[31] DDoS attacks and defense mechanisms : classification and state-of-the-art Christos Douligeris , Aikaterini Mitrokotsa page 653 et 654.

[32] Albert de Mereuil et Annabel-Mauve ANATOMIE D'UNE CYBER-ATTAQUE CONTRE UNE ENTREPRISE : COMPRENDRE ET PRÉVENIR LES ATTAQUES PAR DÉNI DE SERVICE Bonnefous 2016/1 N° 123 — pages 5 à 14.

[33] Classification of Spoofing Attack Types , Johannes Rossouw , Ivana Lukcin, Alexander Rügamer , Xabier Zubizarret,van der Merwe Fraunhofer Institute for Integrated Circuits IIS, May 2018.

[34] L'impact des attaques sur la fiabilité des réseaux ad hoc.par Nadjette Hanane MOUICI BOUKHALFA Laarbi tebessi -Tebessa- Algérie - Sécurité et réseaux informatiques -Master 2- 2015.

[35] Conception et déploiement d'un réseau informatique pour la transmission des données.par Pamphil KAZADI Notre Dame du Kasayi - Licence 2015

[36] Man-in-the-middle-attack : Understanding in simple words, Avijit Mallik Rajshahi University of Engineering Technology, Abid Ahsan Rajshahi University of Engineering Technology, Mhia Md Zaglul Shahadat Rajshahi University

of Engineering Technology, Jia-Chi Tsou China University of Technology , January 2019.

[37] John Douceur and Judith S. Donath. The Sybil attack. In IPDPS, pages 251–260, Washington,DC, USA, 2002. IEEE.

[38] Wormhole Attack in Wireless Sensor Network, Rajshree Pandey and R. A. KHAN , Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow , January 2014.

[39] MÉMOIRE DE FIN D'ÉTUDES Université A/Mira de Béjaïa Sécurité dans les réseaux Ad Hoc Wormhole P49.

[40] Tseng, F. H., Chou, L. D., Chao, H. C. (2011). A Survey of BlackHole Attacks in Wireless Mobile Ad Hoc Networks. Human-centric Computing and Information Sciences, 1(4), pp. 1-16.

[41] Misra, P. (1999). Routing Protocols for Ad Hoc Mobile Wireless Networks.Courses Notes, available at :$//$www.cse.wustl.edu/ jain/cis788-99/ftp/adhoc$_r outing/(lastaccessedonJuly$2015).

[42] Bilandi, N., Verma, H. K. (2012). Comparative Analysis of Reactive, Proactive and Hybrid Routing Protocols in MANET. International Journal of Electronics and Computer Science Engineering, 1(3), pp. 1660-1667.

[43] Jhaveri, R. H., Patel, S. J., Jinwala, D. C.2012). DoS Attacks in Mobile Ad Hoc Networks : A Survey. In Second International Conference on Advanced Computing Communication Technologies, pp. 535-541.

[44] Perkins, C., Belding-Royer, E., Das, S. (2003). Ad Hoc On-demand Distance Vector (AODV) Routing, No. RFC 3561.

[45] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., Nemoto, Y.(2007). Detecting Blackhole Attack on AODV-based Mobile Ad HocNetworks by Dynamic Learning Method. International Journal of Network Security, 5(3), pp. 338-346.

[46] 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,

[47] C.Seghiri, “Protection contre l’attaque de trou noir dans les réseaux mobiles adhoc,” Mémoire d’ingéniera Informatique, Université Bejaia, 2010.

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

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

[50] Mr BOUKHECHEM Nadhir, ROUTAGE DANS LES RESEAUX MOBILES AD HOC PAR UNE APPROCHE A BASE D’AGENTS thèse de Magister, Université de constantine Faculté des sciences et science de l’ingénieur, 2007-2008.

[51] Houda HAFI, Protocole pour la sécurité des réseaux sans fil peer to peer thèse de Magister, Université Kasdi Merbah – Ouargla,juin 2012.

[52] Mohamed Ali Ayachi. Contributions à la détection des comportements malhonnêtes dans les réseaux ad hoc AODV par analyse de la confiance implicite.Cryptographie et sécurité [cs.CR]. Université Rennes 1 ; Université Européenne de Bretagne ; Université 7 Novembre à Carthage, 2011. Français.

[53] Harris SIMAREMARE A DEVELOPMENT OF SECURE AND OPTIMIZED AODV ROUTING PROTOCOL USING ANT ALGORITHM , UNIVERSITE DE HAUTE ALSACE ÉCOLE DOCTORALE JEAN-HENRI LAMBERT,November 2013

[54] Benabdallah Karima, Optimisation d’un protocole de routage AODV dans les Réseaux de capteur sans fil thèse de master , Université Aboubakr Belkaïd Tlemcen , 2016-2017.

[55] Rahul Sharma, Naveen Dahiya, Divya Upadhyay ,article An Analysis for Black Hole Attack in AODV Protocol and Its Solution, Computer Science Engineering, Amity University, Noida, India , April 2013.

[56] CHEBBAH Houssem REZKI Boumediene, Etude de l’attaque BLACKHOLE dans Les réseaux sans fil décentralisés, UNIVERSITE KASDI MERBAH, OUARGLA, 2017/2018.

[57] Pradish, Patel, Sachin. (2013). Performance Evaluation of Routing Protocol like AODV and DSR under Black Hole Attacks. Performance Evaluation, 3(1), 1487-1491.

[58] Ms Monika Y, Sambare, Mr Santosh S. (2013). A Survey on Detection of Blackhole Attack using AODV Protocol in MANET.

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

[60] Al-Shurman and S.Moo-Yoo and S.Park, "Blackhole Attack inMobile Ad Hoc-Networks,"ACM Southeast Regional Conference,2004.

[61] 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.

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

[63] Dokurer, S., Erten, Y. M., Acar, C. E. (2007). Performance Analysis of Ad-hoc Networks under Black Hole Attacks. Proceedings of IEEE SoutheastCon, pp. 148-153.

Résumé

Un réseau ad hoc est une collection de noeuds 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 noeuds participent à la fonction du routage qui consiste à trouver un chemin entre les noeuds source et destination à travers des noeuds intermédiaires pour faire acheminer ces paquets. Un noeud 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 noeud 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 Si une deuxième Requête RREP arrive à la source, il passe à la nouvelle route puisqu'il est supposer que le BLACKHOLE ne perde pas de temps à vérifier la table d'acheminement et le RREP La requête du BLACKHOLE arrive plus tôt que la destination réelle

Mots clés :réseaux Ad hoc,sécurité des réseaux ad hoc, AODV, BLACKHOLE.

Abstract

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 were interested in the blackhole attack in a network running the AODV protocol, this attack consists of removing or redirecting the absorbed traffic to another node. To prevent this attack, we have proposed a solution If a second RREP Request arrives at the source, it switches to the new route since it is assumed that the BLACKHOLE does not waste time checking the routing table and the RREP The BLACKHOLE request arrives earlier than the actual destination.

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