République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A/MIRA de Bejaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Fin de cycle

En vue de l'obtention du diplôme de Master Professionnel en Informatique

Spécialité : Administration et Sécurité des Réseaux

Thème

Schéma de prévention contre l'attaque Wormhole dans les réseaux ad hoc

---

Réalisé par :

M^lle^ MAOUCHI Djamila
M^lle^ MENASRIA Aicha

Devant le jury composé de :

Président :	M^r^	D. TOUAZI
Rapporteur :	M^r^	A. BAADACHE
Examinateur :	M^r^	S. AISSANI

Promotion 2014/2015

Remerciements

Ce mémoire n'aurait pas pu être confectionné si Dieu le Tout Puissant nous a avait pas doté d'une santé physique et morale à chaque instant ; c'est pourquoi, nous le remercions à l'infini pour ce don inestimable dont il nous a gratifié.

Nous tenons -bien entendre à remercier particulièrement, notre cher encadreur, en l'occurrence le DR : Abderrahmane BAADACHE, de l'Université BEJAIA qui, par son encadrement ses précieux conseils, sa patience, sa générosité et enfin sa disponibilité ont fait que notre œuvre a été largement facilité : nous ne saurions l'oublier.

Nous tennons à exprimer notre gratitude aux membres de jury pour avoir accepté de juger ce travail.

Un énorme merci à nos familles et amis pour leurs éternel soutient et la confiance qu'ils ont en nos capacité.

Dédicaces

A mes chers parents qui m'ont éclairé le chemin de la vie par leur grand soutien et leurs encouragements, par leurs dévouements exemplaires et les énormes sacrifices qu'ils m'ont consentis durant mes études et qui ont toujours aimé me voire réussir .Je les remercie pour tout ce qu'ils mon fait,

Que dieu les gardes et les protèges,

A mon frère koussaila et mes sœurs,

A ma binôme Djamila qui m'a supporté durant le travail.et chez qui j'ai trouvé l'entente dont j'avais besoin,

A tous mes amis ,

AICHA

Dédicaces

A mes chers parents qui m'ont éclairé le chemin de la vie par leur grand soutien et leurs encouragements, par leurs dévouements exemplaires et les énormes sacrifices qu'ils m'ont consentis durant mes études et qui ont toujours aimé me voire réussir .Je les remercie pour tout ce qu'ils mon fait,

Que dieu les gardes et les protèges,

A mon frère Daoud et mes sœurs ,

A ma binôme Aicha qui m'a supporté durant le travail.et chez qui j'ai trouvé l'entente dont j'avais besoin,

A mon fiancé Salim,

A tous mes amis ,

DJAMILA

TABLE DES MATIÈRES

LISTE DES TABLEAUX

TABLE DES FIGURES

LISTE DES ABRÉVIATIONS

AODV	**A**d Hoc **O**n **D**emand **V**ector
ARAN	**A**uthenticated **R**outing for **A**d hoc **N**etworks
CA	**C**ertificate **A**uthority
COTA	**C**ell-based **O**pen **T**unnel **A**voidance
CPU	**C**entral **P**rocessing **U**nit
DoS	**D**enial **o**f **S**ervice
DSDV	**D**estination **S**equenced **D**istance **V**ector
DSR	**D**ynamic **S**ource **R**outing
GPS	**G**lobal **P**ositionning **S**ystem
GPSR	**G**reedy **P**erimeter **S**tateless **R**outing
IARP	**I**ntr**A**zone **R**outing **P**rotocol

IERP	**I**nt**E**rzone **R**outing **P**rotocol
IDS	**I**ntrusion **D**etection **S**ystem
IP	**I**nternet **P**rotocol
KA	**K**ey **A**greement
LBK	**L**ocal **B**roadcast **K**ey
LDAC	**L**ocalized **D**ecentralize **A**lgorithm for **C**ountering Wormholes
MAC	**M**edium **A**ccess **C**ontrol
MAD	**M**utual **A**uthenticated **D**istance-Bouding
MAE	**M**anet **A**uthentication **E**xtension
MANET	**M**obile **A**d hoc **NET**work
MAD	**M**utuelle **A**uthentique with **D**istance Bounding
MDS	**M**ulti-**D**imensional **S**caling
ND	**N**eighbor **D**iscovery
OLSR	**O**ptimized **L**ink **S**tate **R**outing
PDR	**P**acket **D**elevery **R**atio

PMF	**P**robability **M**ass **F**unction
PSR	**P**acket **S**ent **R**atio
RREP	**R**oute **REP**ly
RREQ	**R**oute **REQ**uest
RERR	**R**oute **ERR**uest
RSA	**R**ivest **S**hamir **R**outing
SAM	**S**tatistical **A**nalysis of **M**ulti-path
SAR	**S**ecurity **A**ware ad hoc **R**outing protocol
SEAD	**S**ecure **E**fficient **A**d hoc **D**istance vector routing protocol
SLPS	**S**ecure **L**ink **S**tate **P**rotocol
SMA	**S**ystem **M**odel **A**ssumption
SRP	**S**ecure **R**outing **P**rotocol
IUT	**I**nternational **U**nion of **T**elecommunication
TESLA	**T**ime **E**fficient **S**tream **L**oss tolerant **A**uthentication
TIK	**T**esla with **I**nstant **K**eys discolosure
ZRP	**Z**one **R**outing**P**rotocol

ZHLS **Z**one-bsed **H**ierarchical **L**ink **S**tate Protocol

INTRODUCTION GÉNÉRALE

Un réseau sans fil ad hoc est un ensemble de nœuds utilisant des liaisons sans fil pour communiquer. Il s'agit d'un réseau où le support de communication est ouvert et partagé, la mobilité est possible et l'infrastructure est complètement absente. Donc, les nœuds dans un tel réseau s'auto-organisent et coopèrent entre eux pour rendre possible la communication entre les nœuds qui sont hors portée de communication les uns des autres. Ce genre de réseau présente l'avantage d'être facilement et rapidement déployés avec un coût généralement pas coûteux. En contrepartie, il est relativement facile d'attaquer un réseau ad hoc à cause des caractéristiques inhérentes de ce dernier. En effet, un support de communication sans fil ouvert et partagé facilite considérablement l'interception, la modification ou même la suppression du trafic réseau en l'absence des contremesures de sécurité. En outre, la mobilité et l'absence d'infrastructure rendent impossible l'application des mécanismes de sécurité utilisés en filaire.

Plusieurs classes d'attaques, qui exploitent les différentes vulnérabilités au niveau de chacune des couches de la pile protocolaire, ont été présentées dans la littérature. La sécurité contre ces attaques consiste à garantir un certain nombre de services qui sont l'authentification des nœuds, l'intégrité et la confidentialité des données, la disponibilité du réseau, le contrôle d'accès au support de communication et l'anonymat. Bien que multiples, les travaux de recherche se focalisant sur le problème de la sécurité restent toujours limités en termes d'efficacité et de performance, ces travaux reposent sur des outils cryptographiques ou non cryptographiques pour la mise en œuvre de la première ligne de

défense, et utilise les systèmes de réputations et de détection d'intrusion comme deuxième ligne de défense.

Dans notre travail, nous nous sommes intéressés par l'attaque wormhole, dans laquelle un tunnel est établi entre deux nœuds malicieux dans le but de capter les paquets dans une zone et les rejouer dans une autre zone, ce qui affecte particulièrement les relations de voisinages entre les nœuds. Cela a un impact négatif bien évidement sur l'opération de routage et entraine en conséquence la dégradation de la performance du réseau. Pour lutter contre une telle attaque, nous avons proposé un schéma de prévention basé sur le découpage en zones du réseau. L'idée est qu'à chaque fois qu'un nœud envoi un paquet doit l'accompagné par l'identifiant de la zone, de cette façon, le récepteur est toujours tenu informer de la zone d'où provient le paquet reçu. Par simulation, nous avons montré l'efficacité de notre schéma et évaluer sa performance.

Notre mémoire est structuré autour de quatre chapitres. Les réseaux ad hoc, leurs caractéristiques ainsi que les protocoles de routages utilisés sont introduits dans le premier chapitre. Le deuxième chapitre, quant à lui, présente un état de l'art sur les différentes classes d'attaque ainsi que les solutions correspondantes proposées dans la littérature. Le chapitre trois est consacré à l'attaque wormhole, en y trouve la spécification de l'attaque et les différentes solutions de sécurité proposées pour y remédier. Nous décrivons notre schéma de sécurité et nous analysons les résultats de simulation dans le chapitre quatre. Le mémoire se termine par une conclusion qui récapitule notre travail et énumère les perspectives pour améliorer notre travail.

CHAPITRE 1

GÉNÉRALITÉS SUR LES RÉSEAUX AD HOC

1.1 Introduction

L'explosion des communications téléphoniques ou informatiques dans les dernières années a donné naissance à une utilisation plus croissante des réseaux de communication. Les environnements mobiles offrent une grande flexibilité d'emploi et ils peuvent être classés en deux catégories : les réseaux avec infrastructure qui utilisent généralement le modèle de la communication cellulaire, et les réseaux sans infrastructure ou ad hoc. Ces derniers, appelés généralement MANET (Mobile ad hoc Network) permettent aux utilisateurs de se déplacer librement tout en continuant normalement leurs communications, ils peuvent être déployés rapidement et ils n'ont besoin d'aucune infrastructure fixe préexistante.

Dans ce chapitre, nous présenterons les réseaux mobiles ad hoc, leurs caractéristiques ainsi que leurs principaux avantages. Nous présenterons par la suite quelques domaines applications d'un réseau ad hoc. Enfin, nous donnerons un aperçu général sur le routage et nous décriverons quelques protocoles de routage les plus connus.

1.2 Réseaux sans fil

Un réseau est dit sans fil s'il permet à ses utilisateurs d'accéder à l'information indépendamment de leurs position géographique. Pour communiquer entre eux les nœuds du réseau sans fils utilisent une interface de communication sans fil(médium radio ou

infrarouge) qui permet de propager les signaux sur une certaine distance. Les réseaux sans fils offrent une plus grande flexibilité d'emplois et un plus grand confort par rapport au réseaux statiques.

Nous pouvons distinguer deux classes de réseaux sans fils, les réseaux sans fils avec infrastructure de communication, et les réseaux sans fils sans infrastructure de communication ou les réseaux ad Hoc.

1.2.1 Les réseaux sans fils avec infrastructure

Un réseau sans fil avec infrastructure est basé sur un ensemble de sites fixes appelés stations de base qui sont interconnectés entre eux à travers un réseau de communication filaire, chaque station de base peut communiquer directement en utilisant une interface sans fil avec les nœuds mobiles se trouvant dans une zone géographique limitée comme le montre la figure suivante :

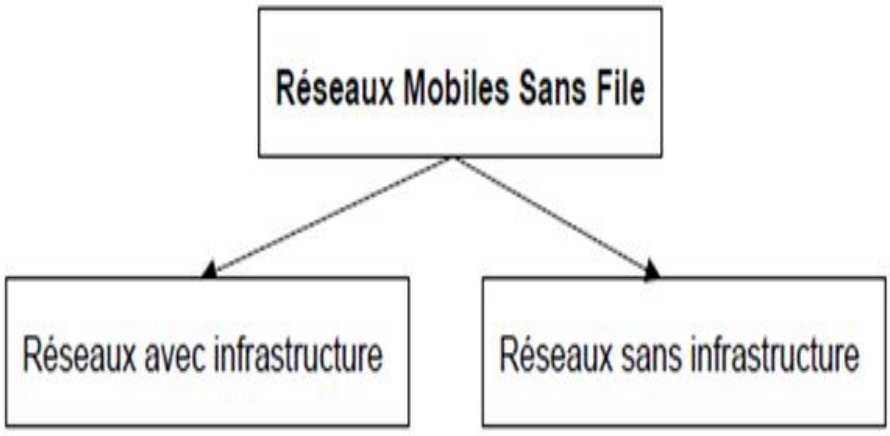

FIGURE 1.1 – Réseau sans fils avec infrastructure

Un nœud dans les réseaux sans fils avec infrastructures se connecte et communique avec les autres nœuds du réseau a travers la station de base la plus proche dans sa portée de communication, si le nœud mobile sort de la portée de cette station, il doit trouver une autre station de base pour continuer la communication. Les réseaux mobiles avec infrastructures coûtent chère car ils demandent le déploiement d'une importante

infrastructure fixe.

1.2.2 Les réseaux sans fils sans infrastructure

Ces réseaux sont constitués d'unités mobiles communiquant entre eux sans l'aide d'infrastructure fixe. Appelées communément ad hoc, elles ne nécessitent aucune structure physique pour être déployées et elles sont opérationnelles instantanément. Dans ce type de réseau tous les hôtes doivent coopérer pour gérer les communications entre eux (routage,contrôle de l'accès au media, etc)[1].

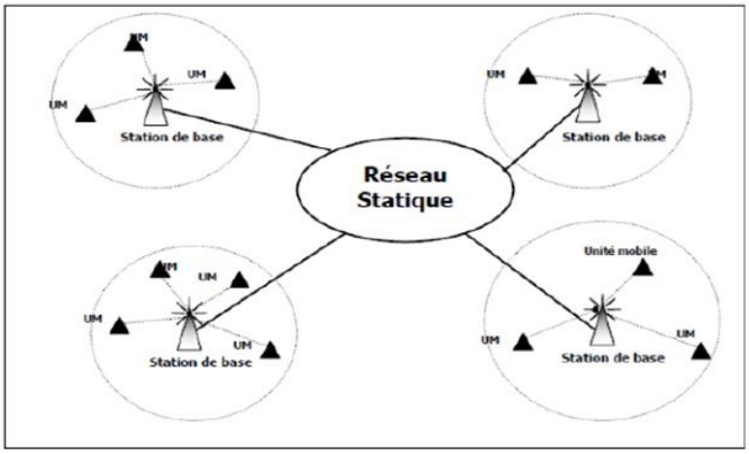

FIGURE 1.2 – Réseau sans fils sans infrastructure

1.3 Modélisation d'un réseau ad hoc

Un réseau mobile ad hoc consiste en une grande population, relativement dense, d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure préexistante ou administration centralisée [2].

Un réseau mobile ad hoc peut être modélisé par un graphe Gt = (Vt, Et) où : Vt : représente l'ensemble des nœuds du réseau, Et : représente l'ensemble des connexions qui existent entre ces nœuds. Si e = (u, v) ϵ Et, cela veut dire que les nœuds u et v sont en mesure de communiquer directement à l'instant t [3]. La figure 1.3 présente la modélisation d'un réseau ad hoc.

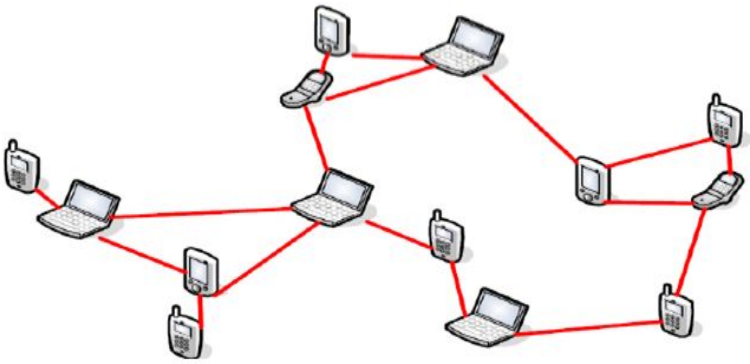

FIGURE 1.3 – Modélisation d'un réseau ad hoc.

1.3.1 Caractéristiques des réseaux ad hoc

Les réseaux mobiles ad hoc sont distingués par les caractéristiques suivantes :

- **Topologie dynamique :** Les nœuds du réseau sont autonomes et capables de se déplacer de manière arbitraire (voir la figure 1.4). Cette mobilité fait que la topologie réseau est dynamique, car elle peut changer à tout instant de façon imprévisible et aléatoire[4].

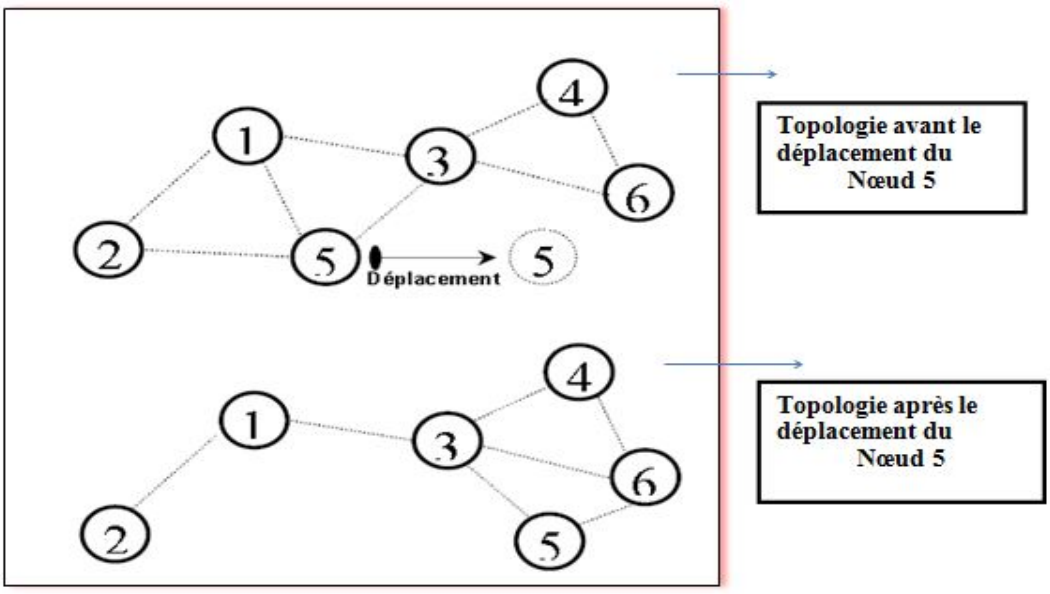

FIGURE 1.4 – Changement de la topologie d'un réseau ad hoc

- **Absence d'infrastructure :** Pas de station de base ou de point d'accès, tous les nœuds du réseau se déplacent dans un environnement distribué, sans point d'accès

ou un point de rattachement à l'ensemble du réseau [5].

- **Contrainte d'énergie :** Les hôtes mobiles sont alimentés par des sources d'énergie autonomes comme les batteries de capacité limité. Le paramètre d'énergie doit être pris en considération dans tout contrôle fait par le système [1].
- **Erreur de transmission :** Les erreurs de transmission radio sont plus fréquentes que dans les réseaux filaires.
- **Sécurité physique limitée :** Les réseaux sans fil sont généralement plus sensibles aux menaces physiques que les réseaux câblés. Les techniques existantes pour la sécurité des liaisons sont souvent appliquées au sein des réseaux sans fil pour réduire les risques d'attaques. Notons, cependant, un avantage dans le fait que le contrôle des réseaux MANET soit décentralisé s'ajoute à sa robustesse, contrairement aux problèmes pouvant survenir sur les points centraux dans les approches plus centralisées [6].
- **Qualité de service :** De nombreuses applications ont besoin de certaines garanties relatives par exemple au débit, au délai ou encore à la gigue. Dans ces réseaux ad hoc, ces garanties sont très difficiles à assurer. Ceci est dû à la nature du canal radio d'une part (interférences et taux d'erreurs élevés) et au fait que les liens entre les nœuds sont partagés [7].
- **Bande passante limitée :** Les nœuds dans les réseaux ad hoc utilisent une technologie de communication sans fil dont la bande passante reste modeste comparée aux technologies des réseaux filaires.
- **L'hétérogénéité des nœuds :** Un nœud mobile peut être équipé d'une ou plusieurs interfaces radio ayant des capacités de transmission variées et opérant dans des plages de fréquences différentes. Cette hétérogénéité de capacité peut engendrer des liens asymétriques dans le réseau. De plus, les nœuds peuvent avoir des différences en termes de capacité de traitement (CPU, mémoire), de logiciel, de taille (petit, grand) et de mobilité (lent, rapide). Dans ce cas, une adaptation dynamique des protocoles s'avère nécessaire pour supporter de telles situations.
- **La taille des réseaux ad hoc :** Elle est souvent de petite ou moyenne taille (une centaine de nœuds) ; le réseau est utilisé pour étendre temporairement un réseau filaire, comme pour une conférence ou des situations où le déploiement du réseau fixe n'est pas approprié (ex : catastrophes naturelles). Cependant, quelques applications

des réseaux ad hoc nécessitent une utilisation allant jusqu'à des dizaines de milliers de nœuds.

1.3.2 Avantages des réseaux ad hoc

Les réseaux ad hoc présentent plusieurs avantages, les plus importants sont :

- Les réseaux ad hoc peuvent être déployés dans un environnement quelconque.
- Déploiement facile, rapide et économique : ne nécessite aucun prérequis puisqu'il suffit de disposer un certain nombre de terminaux dans un espace pour créer un réseau ad hoc, et rapide puisqu'il est immédiatement fonctionnel dès lors que les terminaux sont présents.
- Coût d'exploitation du réseau ad hoc faible : aucune infrastructure n'est à mettre en place initialement et surtout aucun entretien n'est à prévoir.
- Tolérance aux pannes : les seuls éléments pouvant tombés en panne sont les terminaux, autrement dit, il n'y a pas de panne pénalisante de manière globale.

1.3.3 Applications des réseaux ad hoc

À cause de la facilité et la rapidité de déploiement des réseaux ad hoc, ces derniers sont utilisés dans plusieurs applications, dans ce qui suit, nous allons énumérer les applications fréquemment citées dans la littérature.

- **Applications de collaboration :** Les utilisateurs professionnels ont besoin d'applications particulières lors des échanges entre collaborateurs. Ainsi, au cours de réunions ou de conférences pour s'échanger des informations, ou faire une vidéo conférence entre bureaux voisins, les réseaux ad hoc sont bien appropriés à ces besoins.
- **Réseaux de capteurs :** Un réseau ad hoc peut servir à mettre en œuvre des applications environnementales telles que le suivi des mouvements des animaux, le contrôle des équipements à distance, la surveillance, etc.
- **Applications militaires :** Les réseaux ad hoc ont été utilisés pour la première fois par l'armée (voir la figure 1.5). En effet, ce type de réseaux est la solution idéale pour maintenir une communication sur un champ de bataille entre les différentes troupes d'une armée.

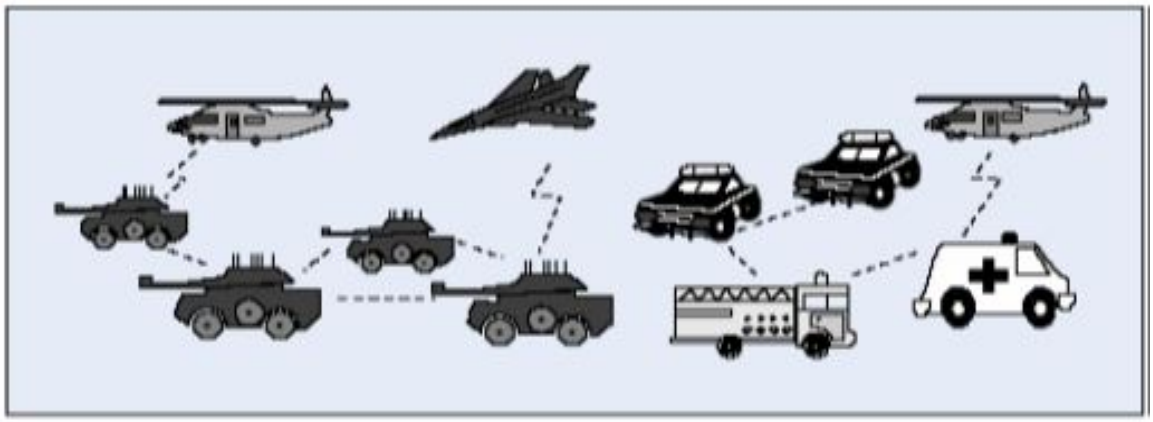

FIGURE 1.5 – Application militaire des réseaux ad hoc

- **Mise en œuvre des réseaux véhiculaires :** Sur un réseau routier, les véhicules peuvent avoir besoin de communiquer entre eux ou avec leur environnement afin de partager des informations, dans le but de gérer et réguler le trafic routier. Les réseaux ad hoc sont alors la solution la plus idéale.
- **Applications commerciales :** Pour un paiement électronique distant ou pour l'accès mobile à Internet.
- **Opérations de secours :** Dans les zones touchées par les catastrophes naturelles (cyclone, séisme, etc.), le déploiement d'un réseau ad hoc est indispensable pour permettre aux unités de secours de communiquer.

1.4 Routage dans les réseaux ad hoc

Le routage est le processus qui consiste à découvrir un chemin entre deux nœuds, source et destinataire. Un protocole de routage doit prendre en compte les contraintes des réseaux ad hoc pour construire et maintenir les routes entre les différents nœuds et s'adapter à la topologie changeante et imprévisible. Comme il est illustré dans la figure 1.6, globalement, trois familles de protocoles de routage ad hoc sont distinguées.

FIGURE 1.6 – Classification des protocoles de routage

1.4.1 Protocoles proactifs

Dans cette famille de protocoles, les chemins sont établis à l'avance. Les protocoles de routage proactifs tentent de maintenir à jour dans chaque nœud les informations de routage concernant tous les autres nœuds du réseau. Il nécessite ainsi que chaque nœud maintienne une table de routage pour stocker les informations de routage qui grandissent avec la taille du réseau. Ils répondent aux changements de topologie du réseau en propageant à chaque voisin les mises à jours des routes afin que chacun puisse maintenir une vue consistante du réseau. Malheureusement ces protocoles atteignent rapidement leurs limites avec l'accroissement du nombre de nœuds et de leur mobilité. Ce type de protocole de routage est ainsi limité à des réseaux de petite taille et fonctionnent mieux pour les réseaux qui ont une faible mobilité des nœuds.

Dans ce que suit, nous présenterons deux protocoles représentatifs de cette famille qui sont : DSDV et OLSR.

- **DSDV** est un protocole de routage proactif, dans lequel chaque nœud garde une table de routage qui donne pour chaque destination accessible dans le réseau :
  - Le nœud voisin à utiliser pour atteindre cette destination.
  - Un numéro de séquence qui est envoyé par le nœud destinataire et qui permet de distinguer les nouvelles routes des anciennes.
  - Le nombre de sauts (nœuds intermédiaires) pour atteindre cette destination.

Périodiquement, chaque nœud dans le réseau diffuse par inondation un paquet de mise à jour des tables de routage qui inclue les destinations accessibles et le nombre de sauts exigés pour atteindre chaque destination, avec le numéro de séquence lié à chaque route. Des paquets de mise à jour sont aussi diffusés immédiatement s'il y a un changement dans la topologie du réseau afin de propager les informations de routage aussi rapidement que possible. A la réception d'un paquet de mise à jour, chaque nœud le compare avec les informations existantes dans sa table de routage. Les routes les plus récentes (qui ont le plus grand numéro de séquence) avec la distance la plus courte sont gardées, les autres sont simplement ignorées [8].

- **OLSR** : Dans ce protocole, les nœuds ne déclarent qu'une sous-partie de leur voisinage grâce à la technique des relais multipoints. Cette technique permet d'optimiser la diffusion des messages de routage économisant une grande partie de la bande passante du réseau.

1.4.2 Protocoles réactifs

Les protocoles réactifs sont basés sur le principe qu'il n'y a aucune information sur la topologie du réseau entier, puisque cette dernière est en évolution constante. Donc, chaque fois qu'un nœud requiert de l'information sur une route pour une destination donnée, il initie un processus de découverte de route [9].

Les protocoles réactifs effectuent donc la mise à jour des routes sur demande. Ces protocoles tentent d'établir une route lorsqu'un nœud demande d'initier une communication avec un nœud pour lequel il n'y a aucune route. Ce type de protocoles est généralement basé sur l'inondation du réseau avec les messages de demande de route (RREQ)et les messages de réponse (RREP).

Ce type de protocole de routage est très efficace pour les réseaux de taille importante, mais le désavantage est le délai engendré par l'établissement d'une route avant de pouvoir émettre les paquets de données [10]. Les protocoles réactifs les plus connus pour les réseaux ad hoc sont : AODV et GPSR.

- **AODV** : AODV se base sur l'algorithme à vecteur de distance, et il ne demande la route que lorsque c'est nécessaire et ne maintient pas les routes vers les destinations qui ne sont pas utilisées dans les communications actives. Chaque nœud intermé-

diaire qui se trouve dans la route entre un nœud source et un nœud destination doit garder une table de routage qui contient :

- L'adresse de la destination.
- Le nœud suivant à utiliser pour atteindre la destination.
- La distance en nombre de nœud.
- Le numéro de séquence de la destination.
- Le temps d'expiration de l'entrée de la table.

AODV utilise trois types de messages pour créer et maintenir les routes, le RREQ pour demander une route, le RREP pour répondre à une requête de demande de route, et le RERR pour signaler une coupure de route.

- **GPSR** : est un protocole réactif basé sur les informations de localisation des unités mobiles. Le protocole GPSR utilise deux méthodes pour router les paquets : la méthode "greedy Forwarding", qui est utilisée tant que possible et la méthode "perimeter Forwarding", qui est applicable dans le cas où la première méthode échoue. La méthode "greedy forwarding" consiste à envoyer le paquet vers le nœud voisin le plus proche de la destination. La méthode " Perimeter Forwarding " est appliquée lorsque d'une part un nœud ne trouve aucun voisin plus proche que lui de la destination et d'autre part la destination ne se trouve pas à la portée de celui-ci [6].

1.4.3 Protocoles Hybrides

Les protocoles hybrides essaient de combiner les deux idées des protocoles proactifs et réactifs pour bénéficier de leurs avantages. Ils utilisent un protocole proactif pour connaître les voisins les plus proches et un protocole réactif au-delà de cette zone prédéfinie dans le but de réduire la charge des paquets de contrôle. Les protocoles hybrides cumulent aussi les inconvénients des protocoles proactifs et des protocoles réactifs à savoir les paquets de contrôle périodique, et le délai de découverte de route. Parmi les protocoles hybrides les plus connus, on cité ZRP et ZHLS.

- **ZRP** : a été introduit en 1997 par Haas et Pearlman, ZRP définit pour chaque zone de routage (*zone radius*), qui inclut tous les nœuds dont la distance minimale (en nombre de sauts) à ce nœud est d. Les nœuds qui sont exactement à distance d sont appelés nœuds périphériques. Pour trouver une route vers des nœuds situés à

une distance supérieure à d, ZRP utilise un protocole réactif, qui envoie une requête à tous les nœuds périphériques. Pour cela, ZRP utilise deux protocles : IARP et IERP. IARP permet, en utilisant une technique proactive, de trouver toutes les routes jusqu'à une distance d. IERP quant à lui, permet d'établir les routes vers les nœuds à plus de d sauts d'une façon réactive[10].

- **ZHLS** : allie une recherche proactive dans l'Intrazone et une recherche dans l'Interzone. Connaissant la topologie, chaque nœud détermine les routes pour joindre l'ensemble des nœuds de sa zone. Le routage dans l'interzone consiste à déterminer les nœuds frontières faisant liaison avec les zones voisines. Lorsqu'une zone a déterminé celles qui l'entourent, la totalité des nœuds du réseau propage cette information. De ce fait, chaque nœud détermine un chemin vers les autres zones du réseau. Lors de la recherche d'une route dont la destination est située dans l'Interzone, la source interroge l'ensemble des zones du réseau pour déterminer a quelle zone appartient la destination. Une fois la zone identifiée, la source peut envoyer vers cette zone des paquets qui arriveront à destination [11].

1.5 Tableaux récapitulatifs

Nous décriverons dans le tableau suivant les différentes classes de protocoles de routages pour les réseaux ad hoc.

Classes	***Caractéristiques***	***Avantages***	***Inconvénients***
Proactif	Calculer les routes à l'avance.	Transmission immédiate des données.	Utiliser beaucoup de paquets de contrôles.
Réactif	Calculer les routes à la demande.	Utiliser moins de paquets de contrôles .	Délai initial avant de commencer la transmission des données.
Hybride	Combinaison des deux approches précédentes.	Bénéficier des avantages des deux approches précédentes.	Cumuler les inconvénients des deux approches précédentes.

TABLE 1.1 – Les classes des protocoles de routage pour les réseaux ad hoc.

1.6 Conclusion

Dans ce chapitre, nous avons introduit les réseaux ad hoc, en particulier, leurs caractéristiques et avantages. Nous avons aussi présenté les protocoles de routage et décrit quelques exemples représentatifs de ces protocoles. Ce genre de réseau, bien que facile, rapide et moins coûteux à déployer, est vulnérable à plusieurs types d'attaques à cause de ces caractéristiques inhérentes qui sont l'ouverture et le partage du médium de communication, la mobilité et l'absence d'infrastructure. Un sérieux problème de sécurité est donc posé. Dans le chapitre suivant, nous allons établir un état de l'art sur la sécurité dans un tel réseau.

Protocoles	**Classes**	**Avantages**	**Inconvénients**
DSDV	**Proactif**	Fournit à tout moment des routes valables vers toutes les destinations du réseau.	L'inondation des paquets de mise à jour cause une charge de contrôle importante au réseau.
OLSR	**Proactif**	Economiser les ressources radio lors des diffusions grâce à l'utilisation des relais multipoints.	Ne fournit aucune spécification de sécurité à prendre en compte.
AODV	**Réactif**	Découvre les routes à la demande en inondant le réseau avec un paquet de requête.	Délai initial avant de commencer la transmission des données.
GPSR	**Réactif**	Utilise essentiellement une métrique de routage bien déterminée.	N'utilise pas la diffusion pour la recherche de routes ni pour l'acheminement des données, ce qui réduit davantage de signalisation.
ZRP	**Hybride**	Réduire le trafic généré lors de la diffusion de requêtes de localisation et Etablir des liens avec les nœuds situés dans l'interzone.	Moins efficace.
ZHLS	**Hybride**	Réduit le nombre d'information de contrôle échangé, pour déterminer un chemin.	Il suppose que le réseau est déjà divisé en zones, qui ne se chevauchent pas.

TABLE 1.2 – Les protocoles de routage pour les réseaux ad hoc.

CHAPITRE 2

SÉCURITÉ DANS LES RÉSEAUX AD HOC

2.1 Introduction

La sécurité est un enjeu majeur pour le déploiement des réseaux sans fil qui, à part leur nature, souffrent encore aujourd'hui de plusieurs problèmes. Les failles de sécurité apparaissent souvent même si des précautions ont été prises. Ceci peut affecter les services qui tournent dans les réseaux sans fil, notamment les protocoles de routage.

Dans ce chapitre, nous énumérerons les vulnérabilités des réseaux ad hoc, ensuite nous présenterons les objectifs de la sécurité, les attaques possibles ainsi que les solutions de sécurité proposées. Le chapitre s'achèvera par une conclusion.

2.2 Vulnérabilités & objectifs de sécurité

Plusieurs types de vulnérabilités ont été recensées dans les réseaux ad hoc. Certaines vulnérabilités sont liées à la technologie sans fil et d'autres aux caractéristiques de ces réseaux.

- Ouverture du support de communication : un message peut être écouté ou une fausse information peut être injectée dans le réseau.
- Absence d'infrastructure : cela rend impossible l'utilisation d'une entité centrale pour la gestion des accès aux ressources du réseau.

- Sécurité physique limitée : les nœuds sont aussi des points de vulnérabilité du réseau au moment où ils peuvent être dans des endroits non protégés physiquement, par exemple, un attaquant peut compromettre un terminal laissé sans surveillance.
- Équivalence des nœuds du réseau : tous les nœuds sont équivalents, alors un nœud malicieux peut modifier, ajouter ou supprimer les messages en transit, ce qui entraine une perturbation du réseau.
- Contrainte d'énergie : la consommation d'énergie constitue un problème important pour les équipements fonctionnant avec une alimentation autonome.

Les principaux objectifs de la sécurité sont :

- **Confidentialité** : La confidentialité est un service essentiel pour assurer une communication privée entre les nœuds. Elle empêche les données d'être consultées par des entités non autorisées. Des contrôles d'accès strict, doivent être mis en place, pour garantir la confidentialité des données dans les réseaux ad hoc. Étant donné que les communications sans fil transitent via l'air, elles sont donc, potentiellement accessibles à tout possesseur du récepteur adéquat.
- **Intégrité** : C'est un service qui garantit que les données n'ont pas été altérées pendant la transmission. Donc le récepteur d'un message s'assure que le message reçu est le même que le message envoyé. L'intégrité des données est une exigence importante pour les réseaux ad hoc. Elle peut être remise en cause par de nombreux évènements. Parmi ceux-ci, les attaques visant à modifier le contenu des messages et la faible fiabilité des liaisons sans fil. [12]
- **Authentification :** Il existe deux types d'authentification, l'authentification des entités et l'authentification des données. L'authentification des entités consiste à vérifier l'identité de l'autre partie communicante. Sans mécanisme d'authentification, un nœud malicieux peut usurper l'identité d'un nœud valide pour obtenir un accès aux ressources. D'autre part, l'authentification des données se focalise de fournir des garanties quant à l'origine des données.
- **Disponibilité :** Consiste à maintenir le bon fonctionnement du système. La topologie dynamique, la limitation des ressources sur certains nœuds, la facilité de brouillage des communications, font de la disponibilité une propriété difficile à gérer[13].
- **Non répudiation :** C'est un mécanisme destiné à prévenir, que la source ou la

destination désavoue ses actions ou nie qu'un échange a eu lieu.

- **Contrôle d'accès :** C'est la fonction qui consiste à se protéger contre les accès non autorisés.
- **Anonymat :** Des fois, même si le contenu de la communication est protégé, les identités des éléments qui prennent part dans la communication constituent une information sensible. Cette propriété a une importance majeure dans les applications civiles spécialement en termes de confidentialité.

2.3 Mécanismes de la sécurité

Plusieurs mécanismes ont été utilisés pour la mise en œuvre de la sécurité. Dans ce qui suit, nous allons décrire les mécanismes les plus utilisés.

2.3.1 Cryptographie

La cryptographie est l'opération qui consiste à chiffrer un message dit " texte clair " en un deuxième dit " texte crypté ", à l'aide d'une clé en utilisant des moyens matériels ou logiciels conçus à cet effet. Les informations originales sont restituées à partir de celles codées. Cette opération inverse est nommée déchiffrement ou décryptage (voir la figure 2.1). Il existe deux grandes familles d'algorithmes cryptographiques à base de clefs :

- Les algorithmes à *clef secrète* ou algorithmes symétriques.
- Les algorithmes à *clef publique* ou algorithmes asymétriques.

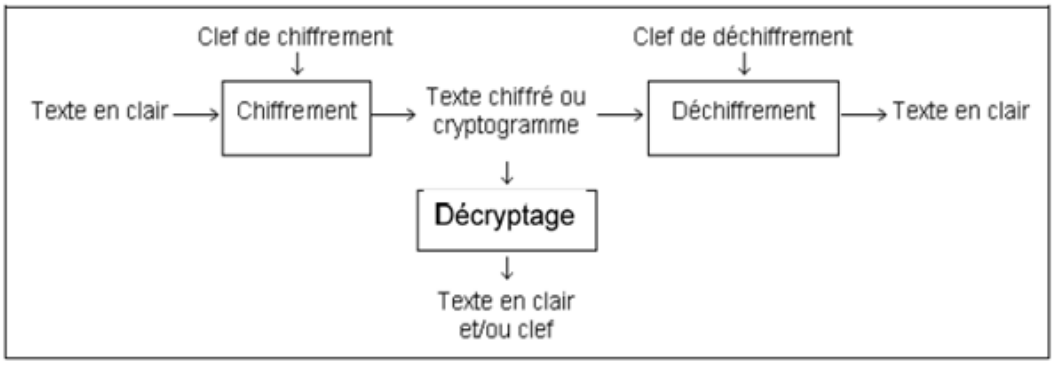

FIGURE 2.1 – Cryptographie

2.3.1.1 Chiffrement Asymétrique

Le concept de la cryptographie à clef publique illustrée dans la figure 2.2 fut inventé par Whitfield Diffie et Martin Hellmanen en 1976, afin de résoudre le problème de distribution des clefs, posé par la cryptographie à clef secrète. Cette technique utilise une paire de clés complémentaires : une clé publique qui chiffre les données et une clé privée pour les déchiffrer. La clé publique doit être diffusée à tous les correspondants dans le système, par contre la clé privée doit rester secrète au niveau de son propriétaire. Toute entité en possession d'une copie de la clé publique peut chiffrer les informations que seul le propriétaire de la clé privée pourra les déchiffrer.

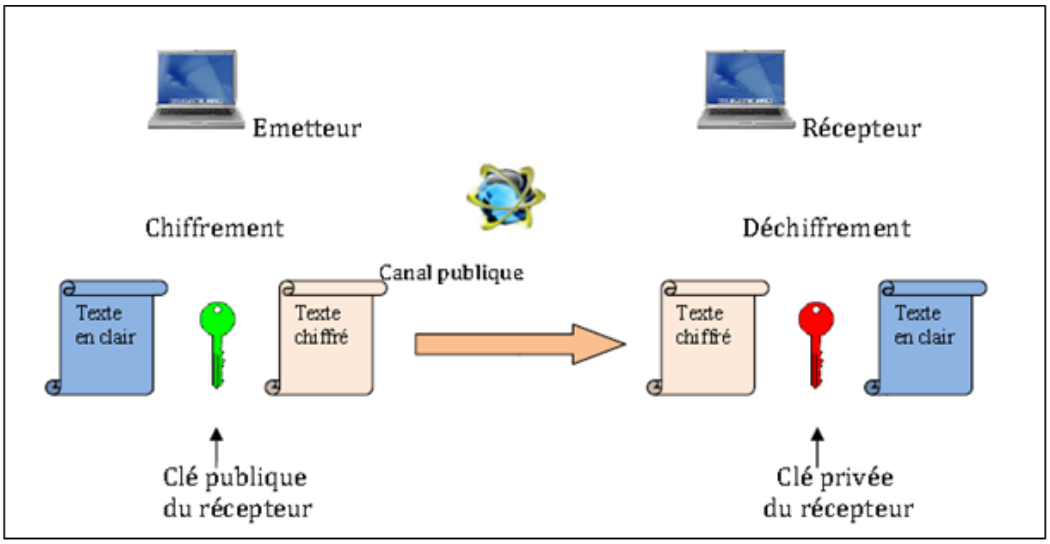

FIGURE 2.2 – Cryptographie Asymétrique

2.3.1.2 Chiffrement symétrique

Dans la cryptographie conventionnelle illustrée dans la figure 2.3, les clefs de chiffrement et de déchiffrement sont identiques. c'est la clef secrète, connue des tiers communicants et d'eux seuls, et qui doit être gardée secrète. Le procédé de chiffrement est dit symétrique.

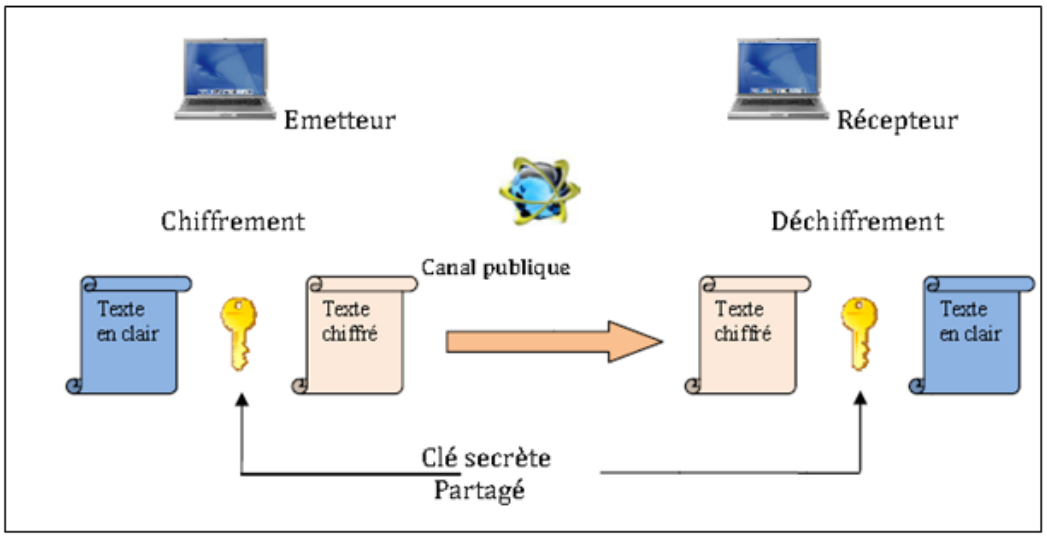

FIGURE 2.3 – Cryptographie symétrique

2.3.2 Fonction de hachage

Une fonction de hachage est une fonction permettant d'obtenir un condensé, appelé aussi empreinte ou haché, de longueur fixe à partir d'un texte de longueur arbitraire finie. La fonction de hachage doit être telle qu'elle associe un et un seul condensé à un texte en clair. Cela signifie que la moindre modification du texte entraine la modification de son condensé. D'autre part, il doit s'agir d'une fonction facilement calculable et à sens unique afin qu'il soit impossible de retrouver le message original à partir de son condensé. En expédiant un message accompagné de son haché, il est possible de garantir l'intégrité d'un message, c'est-à-dire que le destinataire peut vérifier que le message n'a pas été altéré durant la communication[14].

2.3.3 Chaînes de hachage

Les chaînes de hachage sont basées sur les fonctions de hachage à sens unique. La chaîne de hachage est obtenue en appliquant plusieurs fois la fonction de hachage h sur une donnée initiale.

2.3.4 Réputation

Chaque entité réseau encourage la collaboration d'autres entités en utilisant une métrique de coopération appelée réputation. La métrique de réputation est calculée sur la base des données recueillies localement par chaque nœud et peut se baser optionnellement sur l'information fournie par d'autres nœuds du réseau impliqués dans des échanges de messages avec les nœuds surveillés. Une note est attribuée à chaque entité, cette note sera augmentée chaque fois que l'entité participe au routage. Basé sur la réputation, un mécanisme de punition est adopté comme système de dissuasion pour empêcher un comportement égoïste en refusant graduellement les services de communication aux entités qui se conduisent mal. Les nœuds prouvés comme malveillants sont exclus du réseau. Cette décision est prise par une autorité centrale [15].

2.3.5 Signature numérique

La signature numérique est l'un des services réalisés grâce à la cryptographie asymétrique, elle est définie comme des " données ajoutées à un message ", ou transformation cryptographique d'un message, permettant à un destinataire de :

1. Authentifier l'auteur d'un document électronique.
2. Garantir son intégrité.
3. Protéger contre la contrefaçon (seul l'expéditeur doit être capable de générer la signature), assurer alors la non répudiation.

La signature numérique est basée sur l'utilisation conjointe d'une fonction de hachage et de la cryptographie asymétrique. La signature numérique comprend deux étapes :

1. Évaluation du condensé de message : l'émetteur commence par générer un condensé, qui est une représentation réduite et unique du message complet, à l'aide d'une fonction de hachage.
2. Signature du condensé : l'émetteur chiffre ce condensé avec un algorithme asymétrique, à l'aide de sa clé privée. Il obtient une signature numérique qu'il ajoute au message original et émettre l'ensemble, message et signature, sur le réseau. La figure 2.4 illustre le processus de la signature numérique.

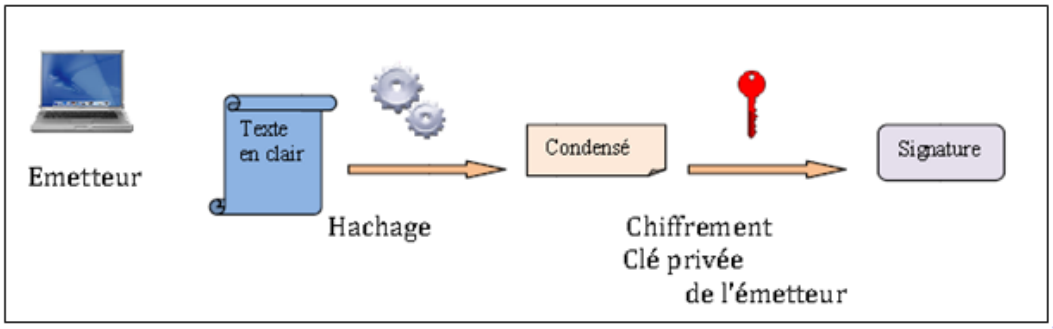

FIGURE 2.4 – Signature d'un message

Pour vérifier la signature, les trois étapes suivantes sont nécessaires.

1. Déchiffrement du condensé de message : le condensé est déchiffré avec la clé publique de l'émetteur.
2. Le destinataire doit réévaluer le condensé en utilisant le même algorithme de hachage que l'émetteur.
3. Comparaison des condensés : le condensé chiffré et le condensé évalué sont comparés. s'ils concordent, la signature est, de ce fait vérifiée et le destinataire peut alors avoir certitude que le message a été envoyé par l'émetteur et n'a pas été altéré. S'ils ne concordent pas, il est possible que le message n'ait pas été signé par l'émetteur ou que le message ait été altéré. Dans les deux cas, le message doit être rejeté.[16]

2.3.6 Certificat électronique

Un certificat est un élément d'informations qui prouve l'identité du propriétaire d'une clé publique. Les certificats sont signés et transmis, de façon sécurisée par un tiers de confiance appelé autorité de certification (CA). L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité, ainsi que de révoquer éventuellement des certificats avant cette date, en cas de compromission de la clé. La structure des certificats est normalisée par le standard X.509 de l'UIT, qui définit les informations contenues dans le certificat :

- Version.
- Numéro de série de l'autorité de certification.
- Algorithme de signature du certificat.

– Le nom de l'autorité de certification.
– La date de validité du certificat.
– Le propriétaire du certificat.
– La clé publique du propriétaire.

Lorsqu'un utilisateur désire communiquer avec un autre, il lui suffit, de se procurer le certificat du destinataire. Il est donc possible de vérifier la validité du certificat en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant, d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière et en comparant ces deux résultats. [16]

2.4 Classification des attaques dans les réseaux ad hoc

Les attaques contre un réseau ad hoc peuvent intervenir des nœuds malicieux qui ne sont pas une partie valide au réseau et qui tentent de joindre le réseau sans autorisation. Ces nœuds sont généralement appelés des nœuds externes. Les réseaux sont généralement protégés contre les nœuds malicieux grâce à l'utilisation de technique cryptographiques. Ces techniques permettent aux nœuds de vérifier d'une manière sécurisée l'identité des autres nœuds, et peuvent donc essayer de prévenir tout dommage causé par les nœuds malicieux. Nous considérons également des attaques à partir des nœuds qui sont autorisés pour faire partie du réseau, on les appelle nœuds internes. Des nœuds internes peuvent lancer des attaques parce qu'ils ont été compromis par des nœuds malicieux.

Le succès d'une attaque dépend de la vulnérabilité du système et l'efficacité des contre-mesures. Les attaques peuvent être divisées en deux catégories principales :

2.4.1 Attaques passives

Faire une attaque passive est le fait de tenter d'espionner l'information qui circule dans le réseau dans le but d'en prendre connaissance uniquement, sans l'altérer. L'attaquant écoute le trafic dans le réseau pour déterminer, par exemple, quels nœuds veulent établir une route ou quel nœud est privilégié de faire des opérations particulières pour qu'ensuite l'usurper et lancer des attaques.

2.4.2 Attaques actives

Dans une attaque active, l'attaquant participe activement dans la perturbation du réseau. Il détruit les paquets, modifie les paquets, répond aux paquets, fabrique des messages ou usurpe d'autres nœuds. La figure 2.5 illustre une classification des attaques actives. Dans ce qui suit, nous décriverons brièvement un certain nombre de ces attaques.

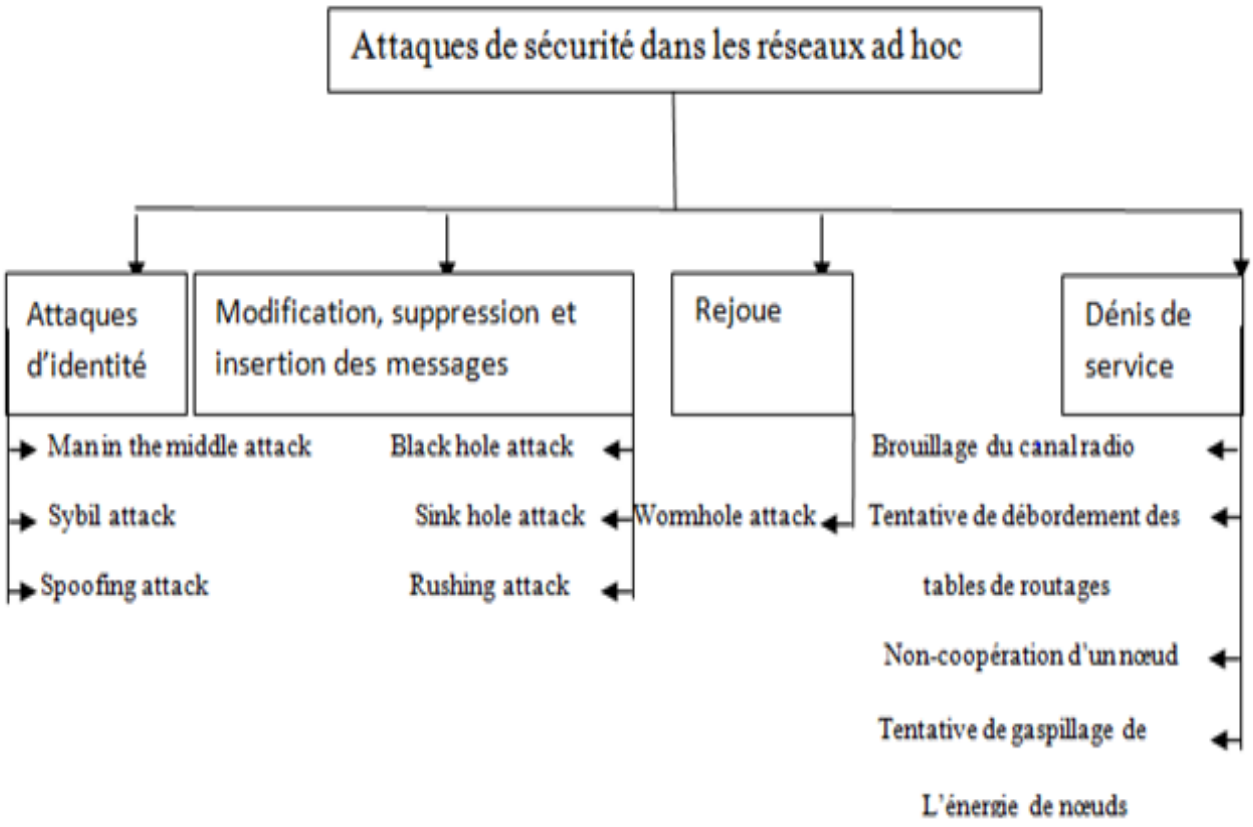

FIGURE 2.5 – Classification des attaques

2.4.2.1 Attaques d'identité

Dans cette classe d'attaque, un intrus usurpe l'identité d'un autre nœud, afin de l'utiliser pour mener des attaques contre les autres nœuds du réseau. Un nœud peut usurper facilement l'identité d'un autre nœud, ceci peut être fait-en changeant sa propre adresse IP, MAC ou toutes autres identités définies dans la couche application avec celle d'un autre nœud légitime. Certaines procédures fortes d'authentification peuvent être employées pour

empêcher cette attaque. Cette classe d'attaque inclut :

- ***Attaque Sybil :*** Dans cette attaque, le nœud présente des identités multiples aux autres nœuds du réseau, créant ainsi des inconsistances dans les tables de routage des nœuds voisins. Ce qui permet de créer plusieurs routes, passant par le nœud malicieux, qui ne sont en réalité qu'un seul chemin. [17]
- ***Usurpation d'identité (Spoofing) :*** Un nœud malicieux change son adresse IP ou son adresse MAC afin de se faire passer pour un autre nœud légitime du réseau. L'intrus ensuite, peut lancer ses attaques avec l'identité de ce nœud. [18]
- ***Man in the middle attack :*** L'attaquant peut personnifier le récepteur pour l'expéditeur, et vice versa, sans que l'un ou l'autre se rendent compte qu'ils ont été attaqués. De cette façon, l'attaquant se positionne entre le récepteur et l'émetteur et en conséquence, il peut mener facilement son attaque dans le réseau.

2.4.2.2 Modification, suppression et injection des messages

Dans un réseau ad hoc, un nœud malicieux peut modifier ou supprimer les messages passant par lui, comme il peut injecter de nouveaux messages dans le but de perturber le bon fonctionnement du réseau. Cette classe d'attaque inclut :

- ***Attaque Black hole :*** Un nœud falsifie les informations de routage pour forcer le passage des données par lui-même. Sa seule mission est ensuite de ne rien transférer, créant ainsi une sorte de puits ou " trou noir " dans le réseau. [19]
- ***Attaque Gray hole :*** C'est une variante de l'attaque Blackhole qui consiste à éliminer seulement les paquets de données de certaines applications qui sont vulnérables à la perte de paquets [20].
- ***Attaque Rushing :*** Concerne les protocoles de routages réactifs dans lesquels l'attaquant ne respecte pas les règles d'accès au canal, imposées par la couche MAC pour précipiter les paquets de RREQ passant par lui. Par conséquent, ces paquets se propagent plus rapidement vers la destination et donc il est fort possible que tous les autres paquets seront éliminés. Car dans la plupart des protocoles de routages réactifs, les auteurs proposent des mécanismes de contrôle pour minimiser le coût de découverte de route, selon lesquels les nœuds intermédiaires rediffusent seulement les paquets de contrôle (les paquets RREQ) arrivant en premier, et éliminent tous les autres exemplaires de ce paquet arrivant ultérieurement [21].

2.4.2.3 Replay ou rejeu des messages

Un nœud malicieux réinjecte des messages dans le réseau. Des anciens messages continuent à circuler ce qui occupe de la bande passante et peut même affecter la justesse de la topologie. Le wormhole est un exemple typique de cette catégorie d'attaque.

- ***Attaque Wormhole :*** Dans une attaque wormhole ou trou ver, un attaquant reçoit des paquets dans un point du réseau, puis les encapsule vers un autre attaquant, pour les réintroduire dans le réseau. Dans ce genre d'attaque, les adversaires coopèrent pour fournir un canal à basse latence, pour la communication, en utilisant une radio pour communiquer avec une puissance plus élevée et des liens à longue portée. Ceci favorise les nœuds voisins à acheminer leurs données à travers l'attaquant [19].

2.4.2.4 Dénis de services(DoS)

Cette classe d'attaque inclut toute attaque touchante à la disponibilité du réseau. On cite à titre d'exemple :

- **Consommation des ressources :** L'attaquant consomme les ressources du réseau (bande passante, mémoire, énergie) de sorte que le réseau devienne indisponible aux utilisateurs.
- **Destruction ou changement d'information :** Dans cette attaque de DoS, un attaquant essaye de changer ou détruire l'information de configuration, de ce fait empêchant les utilisateurs légitimes d'employer le réseau. Un réseau incorrectement configuré ne peut pas bien travailler ou ne pas fonctionner du tout.

Les modèles de dénis de services suivants, s'appliquent plus particulièrement dans le cas de réseau ad hoc [22].

- Brouillage du canal radio pour empêcher toute communication.
- Tentative de débordement des tables de routage des nœuds servant de relais.
- La non coopération des nœuds au bon fonctionnement du réseau pour préserver de l'énergie. Cette attaque est connue sous le nom de "SELFISHNESS" et peut être détectée grâce à des mécanismes de réputation et de détection des comportements égoïstes.
- Tentative de gaspillage de l'énergie des nœuds ayant une autonomie de batterie faible. Cette attaque est connue sous le nom de "SLEEP DEPRIVATION" et

consiste à faire en sorte que le nœud soit obligé de rester en état d'activité et ainsi de lui faire consommer toute son énergie.

– Attaques sur les mécanismes de sécurité eux même.

2.5 Solution de sécurité dans les réseaux ad hoc

Les besoin d'utilisation des réseaux ad hoc et leurs vulnérabilités aux attaques ont conduit au développement de plusieurs solutions pour sécuriser leurs routages. Dans ce qui suit nous présenterons les solutions de sécurité trouvées dans la littérature qui sont classifiées comme illustré dans la figure 2.6.

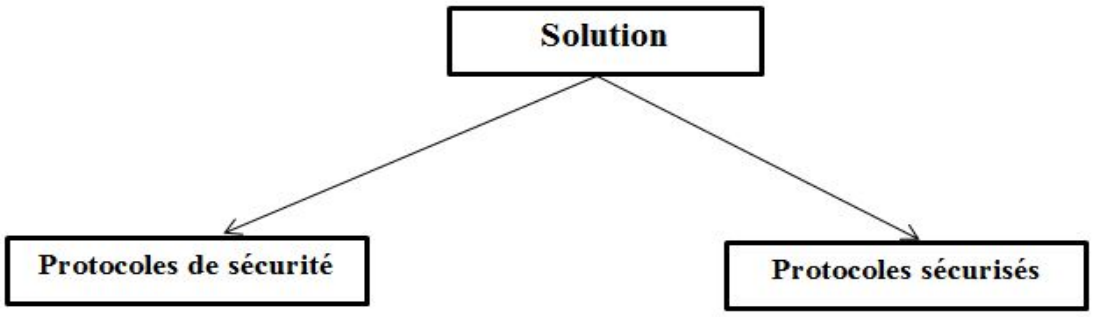

FIGURE 2.6 – Classification des solutions de sécurité dans les réseaux ad hoc

2.5.1 Protocoles de sécurité dans les réseaux ad hoc

Quand on parle de la sécurisation du routage, on désire assurer l'intégrité, la non répudiation, et la disponibilité de service. La protection des messages de routage est garantie par une signature ; ce n'est pas important de chiffrer les messages, car les informations topologiques ne sont pas secrètes.

Un certain ensemble de protocoles visants la sécurité ont été développés, parmi eux on trouve :

- **ARAN**

  Sanzgiri et al. ont proposé le protocole sécurisé ARAN[23] qui prévoit l'utilisation de la cryptographie à clé publique pour sécuriser la construction des chemins des protocoles réactifs tels que AODV.

Il suppose l'existence d'un serveur d'authentification, dont le rôle est de gérer la distribution des certificats pour les nœuds autorisés dans le réseau.

ARAN s'appuie sur deux mécanismes d'authentification. Le premier consiste en une authentification de bout en bout afin qu'un nœud destinataire puisse d'une part authentifier l'origine d'un message de contrôle, et d'autre part vérifier la non modification des données statiques (i.e. l'adresse du nœud source et destinataire) pendant le transit. Le second est une authentification de saut en saut dans lequel chaque nœud sollicité dans un processus de recherche ou de maintenance de chemin utilise sa signature et son certificat pour s'authentifier auprès d'autres nœuds voisins.

Une étude comparative entre ARAN et chacun des protocoles AODV et DSR a montré une grande résistance de ce protocole envers les attaques de modification et d'usurpation d'identité. mais ARAN s'avère extrêmement coûteux en consommation de ressources à cause du rand nombre des opérations de signature et de vérifications de signature utilisées pour assurer la sécurité.

- **SLSP**

  Papadimitratos et Haas proposent SLSP[24], un protocole à état de lien dont ils ont modifié les messages de contrôle afin d'en sécuriser le contenu. Ce protocole utilise les signatures numériques ainsi que les chaînes de hachage à sens unique pour garantir l'intégrité des mises à jour de l'état des liens.

  L'authentification du message se fait par vérification de la signature avec la clé publique de l'émetteur. Alors que les chaînes de hachage permettent juste de limiter le diamètre de diffusion des messages de mise à jour topologique. En revanche, rien n'empêche un nœud de rejouer la valeur de hachage reçue et/ou d'augmenter le compteur de sauts plus que nécessaire.

  Par ailleurs, tout comme pour le protocole SEAD, les paquets de données ne sont pas protégés contre la falsification, le rejeu, la modification ou la destruction. Enfin, SLSP ne permet pas de prendre en compte d'éventuels attaquants complices qui pourraient forger des métriques erronées ou même de créer des tunnels.

- **TESLA**

  Le protocole TESLA [25], a été proposé comme solution contre les comportements malveillants dont l'objectif est la découverte des informations de la topologie ou l'injection de fausses informations du routage. TESLA permet d'authentifier les

messages avec un MAC (Message Authentication Code) dépendant d'une clé secrète qui n'est divulguée par l'émetteur du message qu'après un délai d'attente δ. La valeur δ est calculée de manière à ce qu'on soit sûr que le destinataire a reçu le message avant la divulgation de la clé. Le temps δ ne doit pas être trop important pour limiter les latences dans le réseau. En effet, un destinataire doit attendre la divulgation de la clé secrète avant de pouvoir effectivement traiter un message. La clé secrète utilisèe pour le MAC est issue d'une chaine de clés.Un élément de la chaine k_i est calculé de la manière suivante : k_i-1 = h(k_i+1) où h est une fonction de hachage. L'élément initial k_n est choisi par l'émetteur, celui-ci va utiliser ces clés par ordre croissant, c'est à dire en commençant par k_1. En réception, le destinataire pourra vérifier la relation suivante : k_i-1 = h(k_i) où k_i est la clé dernièrement reçue et k_i-1 correspond à la clé précédente. Cette condition assure que la clé k_i fasse bien partie de la chaine de clé de l'émetteur, ce qui assure, en plus de l'intégrité, la propriété de l'authenticité du paquet.

- **TIK**

  Est un protocole dérivé de TESLA qui est une solution pour l'attaque de type wormhole. Il utilise un packet leash, c'est-à-dire une trame d'information qui restreint la distance de transmission maximale d'un message ou sa durée de vie. Tous les nœuds du réseau doivent avoir des horloges fortement synchronisées. L'authentification des clés est accomplie grâce à des arbres de hachage qui sont une optimisation de des chaînes de hachage. Le nœud émetteur génère un MAC de la forme H (M, k_i) à l'aide d'un packet M et une clé k_i. La clé k_i a un temps de vie t_i et peut être authentifiée par la valeur h dans l'arbre de hachage. Le MAC est inclus dans l'entête du message. Avant d'envoyer le paquet, le nœuds estime une limite au temps d'arrivée du paquet et rajoute la clé k_i. Le nœud qui reçoit le paquet vérifie que la clé n'a pas été divulguée en se basant sur le temps t_i. Si la vérification à vérifier l'intégrité du message en comparant le MAC reçu avec celui calculé.[26]

- **MAE**

  Met en place un service de certification auto-organisé qui soit configurable suivant la politique de sécurité et adapté aux réseaux ad hoc. Dans ce modèle, l'autorité de certification(CA) est distribuée à l'aide de la cryptographie a seuil, qui permet de distribuer la clé privé de CA. MAE présente les dispositifs habituels permettant

de certifier les clés publiques et aussi la gestion de la révocation des certificats. Son principal avantage et qu'il s'adapte à tous les protocoles du routage qu'ils soient proactifs ou réactifs.[27]

2.5.2 Protocoles sécurisés dans les réseaux ad hoc

Divers protocoles sont développés pour sécuriser les protocoles de routages existants. Parmi eux on cite :

- **SAODV**

  Zapata et Asokan ont proposé une extension de sécurité pour le protocole AODV nommée Secure AODV [28].

  SAODV consiste à faire usage d'une signature numérique (créée par cryptographie à clé publique) pour protéger les données statiques des messages de contrôle et cela à l'aide d'un algorithme de chiffrement asymétrique (RSA), puis de recourir à des chaînes de hachage pour protéger l'intégrité de la partie non statique qu'est le compteur de sauts. Comme pour ARAN, des services d'authentification, d'intégrité et de non-répudiation de bout en bout, entre le nœud source et destination, sont ainsi obtenues. Cependant, l'utilisation des chaînes de hachage pour contrer les manipulations illégales sur le compteur de sauts reste limitée. En outre, dans le cas où plusieurs attaquants sont en collusion, une attaque de type wormhole peut être menée. A travers cette attaque, l'attaquant parvient à manipuler le compteur de sauts et à raccourcir la longueur d'un chemin, ceci de manière transparente pour les autres nœuds.

- **SEAD**

  SEAD est un protocole proactif de routage ad hoc sécurisé, basé sur DSDV et permet d'authentifier l'émetteur d'une information de routage. En utilisant les chaînes de hachage à sens unique, SEAD permet d'empêcher l'altération des champs mutables, à savoir le champ métrique nombre de saut et le champ numéro de séquence. En appliquant d'une manière répétitive une fonction de hachage à sens unique, on obtient une chaîne. Les éléments de cette chaîne seront utilisés par les nœuds dans la procédure d'authentification et cela sans utiliser le cryptage à clé publique. Ainsi, il évite les opérations coûteuses dues aux signatures.[29]

Bien que SEAD soit une solution intéressante pour sécuriser le protocole DSDV, il n'est pas suffisant pour empêcher les nœuds malveillants d'agir sur les paquets de données. En effet, la retransmission de ces paquets n'est pas assurée par le protocole de routage et un nœud peut facilement les falsifier, les rejouer, les modifier ou simplement les détruire.

- **SRP**

  Proposé par Papadimitratos et Haas, est un protocole de routage sécurisé conçu comme une extension qui peut être appliqué à une multitude de protocoles réactifs existants en particulier DSR. Il nécessite une SA entre chaque paire de nœuds communiquant, dans laquelle une clé secrète est partagée. Lors de l'nitialisation de la découverte de route, une RREQ est envoyée dont l'entête SRP contient : le numéro de séquence, un nonce, et MAC (hachage calculé sur l'entête IP, le numéro de séquence et la clé secrète) [24]. Le MAC permet au destinataire de vérifier l'intégrité et l'authentification de la requête en calculant un hachage sur les champs de l'entête et le comparant avec le MAC contenu dans la requête. SAODV est la version sécurisée du protocole AODV proposé par Zapata et al [28], les messages RREQ et RREP sont signés par le nœud expéditeur, et la signature est vérifiée par les nœuds intermédiaires avant l'acheminement du message. Ce protocole nécessite un serveur CA pour gérer une PKI, avec laquelle les messages de routage sont signés par leurs créateurs. Il garantit l'intégrité et l'authentification des messages de contrôle du protocole AODV.

2.6 Conclusion

Un réseau ad hoc est vulnérable par plusieurs types d'attaques à cause de ses caractéristiques inhérentes qui sont : l'ouverture du support de communication, la mobilité éventuelle des nœuds et l'absence d'infrastructure. Les solutions proposées pour garantir les différents services de sécurité sont multiples, mais ne sont ni suffisamment efficaces, ni performantes à cause de la sévérité des attaques. Dans ce chapitre, un état de l'art a été établi, en particulier, les différentes attaques, ainsi que les solutions de sécurité ont été présentées. Le chapitre suivant, nous allons le consacré à l'attaque wormhole que nous avons choisi comme sujet d'étude de notre travail.

CHAPITRE 3

ATTAQUE WORMHOLE DANS LES RÉSEAUX AD HOC

3.1 Introduction

Par nature, un réseau ad hoc est vulnérable par plusieurs types d'attaques. Le wormhole est l'une des attaques les plus sévères qui ont attiré l'attention de plusieurs chercheurs. Il s'agit d'une attaque qui consiste à capter les paquets dans une zone et les rejouer dans une autre zone. Cela a un impact négatif sur le fonctionnement du réseau en particulier le routage. En effet, une telle action malicieuse conduit à la falsification de l'information du voisinage utilisée dans le routage et à la dégradation de la performance du réseau en conséquence.

Dans ce chapitre, nous présenterons la spécification de l'attaque wormhole et décriverons la façon dont elle est menée. Ensuite, nous résumerons les différentes approches de sécurité proposées dans la littérature pour se protéger contre cette attaque.

3.2 Spécification de l'attaque wormhole

Le Wormhole est une attaque qui se produit généralement par deux nœud malveillants, dans lequel l'attaquant reçoit ou intercepte des paquets à un point dans le réseau, puis les transmet via un tunnel au prochain attaquant qui se trouve dans un autre point de réseau par le biais d'une liaison directe [32]. Une telle attaque n'exige aucune connaissance

préalable du réseau pour être menée et elle est jouable même lorsque les services de sécurité sont implémentés, ce qui rend difficile sa détection et prévention [33].

L'exemple de la figure 3.1 illustre comment une attaque wormhole est menée. Le nœud source S envoie normalement des paquets à la destination D via le chemin (S-abc-D). Les deux nœuds malicieux M1 et M2 établissent un tunnel entre eux de sorte que M1 capte les paquet dans sa zone, les achemine à M2 via le tunnel, ensuite M2 les rejoue dans sa zone.

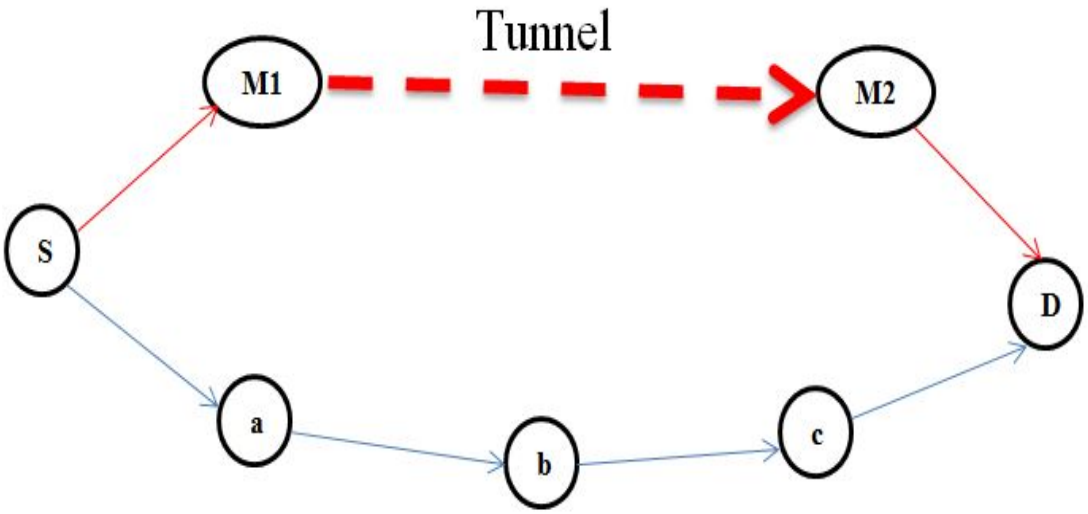

FIGURE 3.1 – Description de l'attaque wormhole

Une attaque wormhole peut être menée soit en mode caché ou en mode participation. En mode caché, les nœuds légitimes ne peuvent pas apercevoir les nœuds malicieux car ces derniers ne s'impliquent pas dans les opérations du réseau tel que la routage. Tandis que, en mode participation, les nœuds malicieux se considèrent des nœuds à part entière et participent activement dans les opérations du réseau [31].

3.3 Classification des attaques Wormhole

Les attaquants de Wormhole peuvent employer deux techniques différentes de communication pour mener leur attaque : un canal d'encapsulation et un canal hors bande.

3.3.1 Wormhole utilisant l'encapsulation

Dans ce type d'attaque de Wormhole, deux nœuds malveillants cherchent à perturber l'opération normale du protocole de cheminement dans le réseau. Pour cela, les nœuds malveillants doivent s'impliquer dans le procédé de découverte de route. Pour atteindre ce but, les nœuds malveillants doivent donner l'impression que la route passant par eux est la plus courte que les autres route.

Sur la Figure 3.2, si un protocole réactif de cheminement (AODV, DSR, etc.) est employé, quand le nœud S cherche à établir un chemin vers le nœud D en annonçant un message de RREQ, dès que le nœud malveillant M1 entendra le paquet de RREQ, il encapsule le paquet et il l'envoie, au cours de son transit, le paquet ne peut être décapsulé que par M2, de cette façon, M1 et M2 créent un tunnel qui servira à mener l'attaque Wormhole [36].

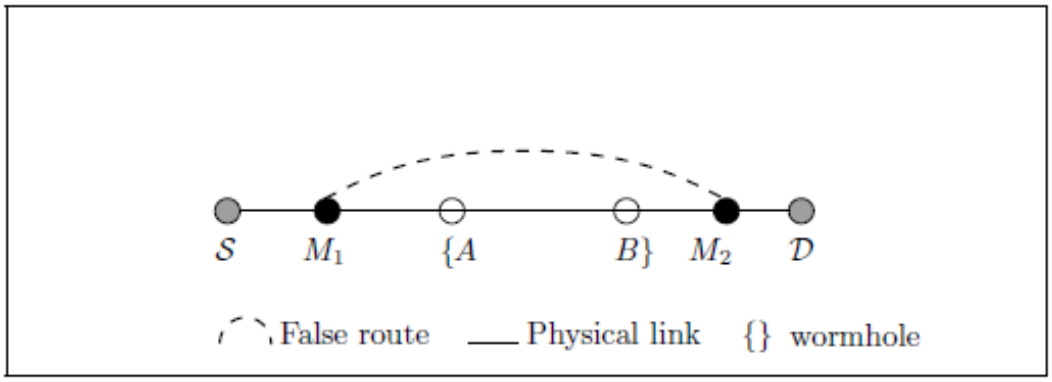

FIGURE 3.2 – Wormhole utilisant l'encapsulation

Une fois que le nœud M2 reçoit le message du nœud M1, il décapsule le paquet récupérant le message original RREQ il, cherche à atteindre le nœud D. Quand le RREQ arrive à D, le nombre de sauts présents dans le paquet sera moins que le vrai nombre de sauts traversé.

Dans le cas où un protocole proactif de cheminement comme OLSR est utilisé, les nœuds malveillants M1 et M2(la figure 3.2) vont encapsuler le message "HELLO" du nœud S vers le nœud D, et vice versa par le chemin (M1-A-B-M2). Par conséquent, la procédure de découverte du voisinage est manœuvrée, donnant à S et D des informations

fausses sur leurs nœuds voisins, et les nœuds malveillants M1 et M2 contrôlent le trafic partagé entre les nœuds S et D.

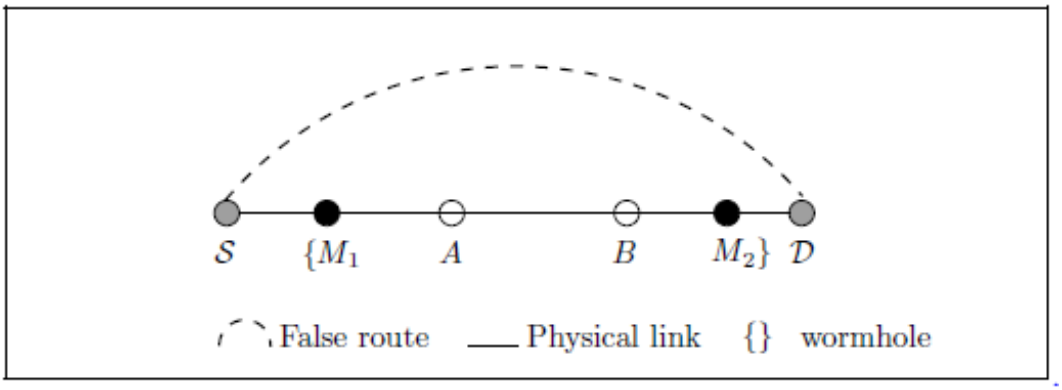

FIGURE 3.3 – Encapsulation de message HELLO

3.3.2 Wormhole utilisant un canal hors bande

Ce type d'attaque de Wormhole est lancé par deux nœuds malveillants stratégiquement situés dans un réseau partageant un canal hors bande de haut-largeur de bande (filaire ou radio). Sur la figure 3.4, quand le nœud S diffuse un paquet de contrôle (RREQ, HELLO, etc.) dirigé vers le nœud D, le nœud malveillant M1 reçoit le paquet et il l'envoie à M2 en utilisant le canal hors bande. Le nœud M2 reçoit le paquet de contrôle et il le rediffuse pour atteindre le nœud D. Le chemin via le tunnel est plus court en termes de nombre de sauts que le chemin passant les nœuds légitimes, donc, c'est le chemin du wormhole qui sera choisi pour transiter les paquets entre S et D.

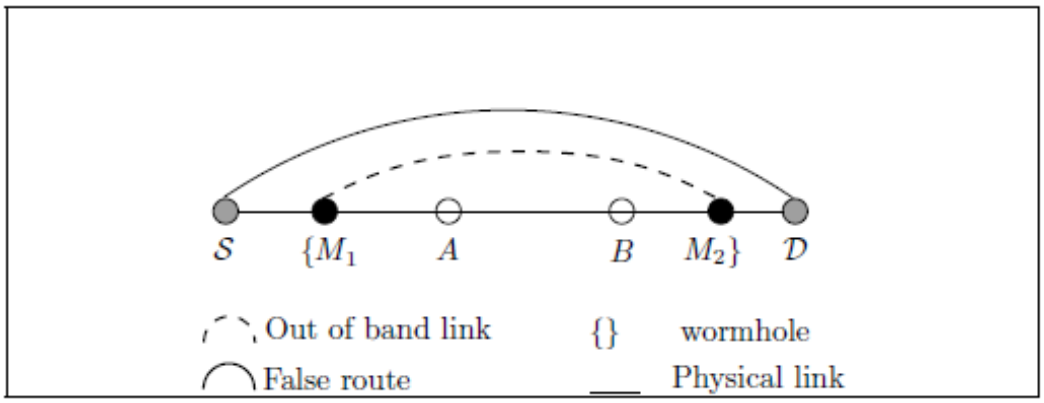

FIGURE 3.4 – Wormhole utilisant un lien hors bande

Les attaques wormhole peuvent être aussi classées selon la visibilité des nœuds malveillants en trois types : closed, half-open, and open(fermé,semi-ouvert,ouvert).

3.3.3 Attaque Wormhole fermée

Dans des attaques fermées de Wormhole, deux nœuds malveillants percent un tunnel et envoient les paquets d'une extrémité à l'autre et les rediffusent sans les modifier ou ajouter n'importe quelle information, même lorsque le paquet fait partie de la procédure de découverte de route. De cette façon, les nœuds malveillants sont invisibles au reste du réseau. Sur la figure 3.5(a), les nœuds malveillants M1 et M2 développent une attaque fermée dans laquelle les nœuds S et D croient qu'ils sont directement reliés.

3.3.4 Attaque Wormhole semi-ouverte

Dans une attaque semi-ouverte de Wormhole, sur la figure 3.5 (b), seulement un des nœuds malveillants ajoute son information à l'en-tête de paquet selon le protocole normal de cheminement, alors que l'autre nœud malveillant perce un tunnel et rediffuse les paquets sans ajouter n'importe quelles informations sur lui-même.

3.3.5 Attaque Wormhole ouverte

Dans ce type d'attaque de Wormhole, les nœuds malveillants M1 et M2 se composent de nœuds internes qui participent activement au protocole de cheminement. Les attaquants incluent leur propre information dans l'en-tête de paquet selon la procédure nor-

mal. Ils ne cachent pas leur présence dans le réseau, mais se trouvent au sujet de la distance qui les sépare, faisant des nœuds honnêtes croient que les deux nœuds malveillants sont les voisins directs.

Sur la figure 3.5(c), les deux attaquants (M1 et M2) sont évidents aux nœuds S et D, mais les informations sur la distance entre eux sont falsifiées.[36]

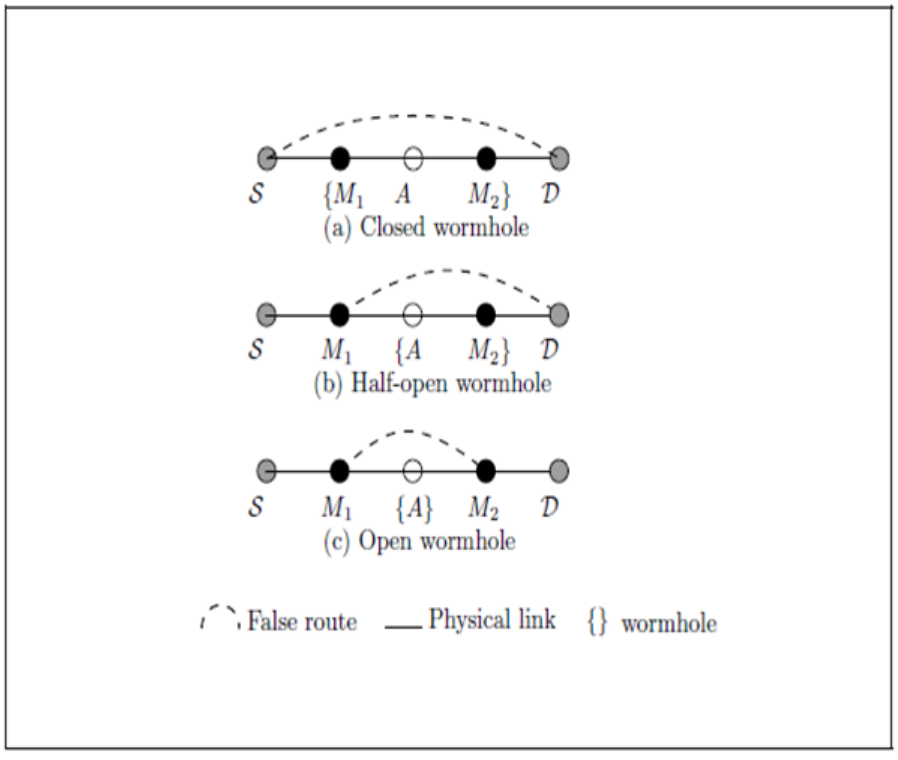

FIGURE 3.5 – Classification du wormhole selon la visibilité

3.4 Spécification du Wormhole dans AODV et OLSR

3.4.1 Wormhole dans AODV

Dans les protocoles réactifs, la route n'est construite qu'à la demande d'une application. L'attaque Wormhole dans AODV est un type d'attaque de relecture qui est particulièrement difficile à détecter. Le processus de lancement de cette attaque est illustré dans la figure 3.6, dans laquelle :

1. Le nœud A diffuse une requête de découverte de la route RREQ.

2. Le nœud X capte et retransmet directement cette requête au nœud Y, via le tunnel préétabli, le nœud Y de son tour, rediffuse le message RREQ.
3. Le nœud B, quand il reçoit la requête, répond à la source avec RREP (Route REPlay) via le même chemin qui a reçu la requête RREQ.
4. Le nœud A, après sa réception de la réponse RREP, va déduire le plus court chemin menant à B (dans l'exemple un seul saut).
5. Notons que le but des attaquants est de construire ce tunnel, après cela ils peuvent lancer n'importe quel type d'attaque avec ce tunnel,(suppression sélective ou totale des paquets de données, etc).

Une attaque wormhole n'est pas difficile à mettre en place et il peut être extrêmement dangereuse. En outre, trouver de meilleures techniques pour la détection des attaques Wormhole et la sécurisation d'AODV contre eux, reste un grand défi dans les réseaux mobiles ad hoc.

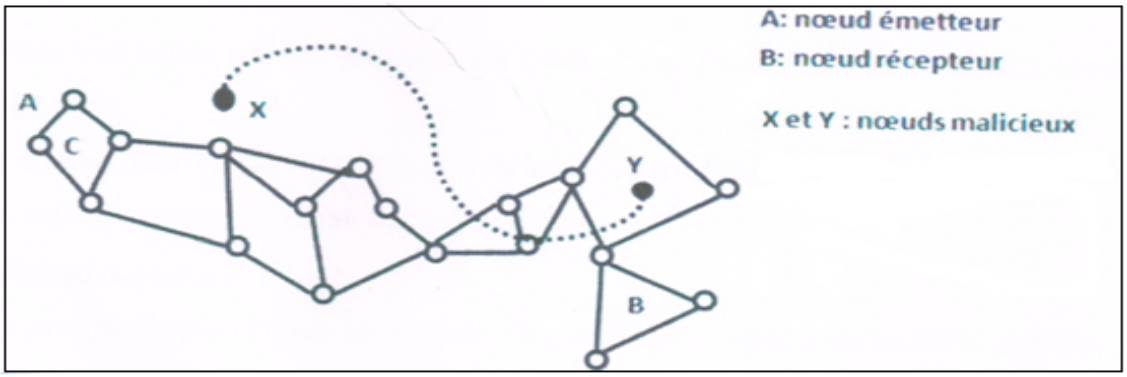

FIGURE 3.6 – Wormhole dans AODV et OLSR

3.4.2 Wormhole dans OLSR

Dans les protocoles proactifs, les nœuds entretiennent toutes les routes du réseau avec l'échange périodique des paquets de contrôle. Ci après, les étapes de lancement de cette attaque illustrées dans la figure 3.6 :

1. Le nœud A diffuse un message HELLO qui contient la liste de ses voisins.
2. Le nœud X capte et retransmet directement le message HELLO au nœud Y, le nœud Y à son tour, diffuse ce message.

3. Le nœud B quand il reçoit le message HELLO, va conclure que le nœud A est un voisin asymétrique. Ainsi, à l'arrivée du message HELLO, le nœud B met dans son message HELLO l'information qu'entre lui et le nœud A il y'a un lien asymétrique.
4. Aussi le nœud Y va capter ce message et le transmet directement à travers le tunnel au nœud X, puis ce dernier le diffuse.
5. Le nœud A, après sa réception de message HELLO, va conclure que le nœud B est un voisin symétrique. Ainsi à l'arrivé de l'instant l'émission du message HELLO, le nœud A met dans son message HELLO l'information que le nœud B est un voisin symétrique, les deux attaquants doivent procéder de la même façon que l'étape 2. Ainsi le nœud B va déduire que le nœud A est un voisin symétrique.

D'après ceci on remarque bien que le wormhole a falsifié la relation de voisinage entre les deux nœuds A et B, c'est-à-dire, il a fait croire que les deux nœuds A et B sont actuellement des voisins.

3.5 Solutions de sécurité contre le Wormhole

Dans cette partie, nous allons présenter la majorité des solutions proposées dans la littérature contre l'attaque wormhole.

3.5.1 Packet Leash technique

Un leach est une information (de temps ou de positionnement géographique) qui est incluse dans chacun des paquets émis sur le réseau et qui sert à restreindre leur distance maximale de transmission autorisée.

Deux méthodes d'utilisation des leaches sont proposées, dont la première est basée sur le support d'un service de positionnement géographique et la seconde est basée sur une synchronisation d'horloge précise entre les nœuds.

– **Leash géographiques :** Est une méthode qui est mise en place en 2003 par Hu pour protéger le réseau contre l'attaque wormhole, où les leash géographique permettent d'assurer la distance entre le récepteur et l'émetteur d'un message. Afin de mettre en œuvre un leach géographique dans les réseaux ad hoc, certaines exigences doivent être fournies, comme chaque nœud doit connaitre sa propre localisation (par

GPS), tous les nœuds doivent avoir les horloges synchronisés lâchement et la signature numérique(RSA) afin de vérifier l'authentification et la localisation et l'heure d'expéditeur.

Quand un paquet est envoyé par un nœud, il insère sa propre emplacement (ps) et le moment où le paquet est transmis (ts) dans l'entête de paquet. Quand le paquet arrive au nœud suivant, L'emplacement du récepteur(pr) et le temps de réception de paquet(tr) est comparée avec les valeurs de l'expéditeur. Quand l'émetteur et le récepteur ont utilisés des horloges synchronisées, si les horloges d'entre eux sont synchronisées à ±,donc, une borne supérieure de la distance entre l'émetteur et le récepteur (DSR) est calculable par le récepteur.

$$dsr < \| \text{ps - pr} \| + 2V * (\text{tr- ts+ } \alpha) + \beta$$

Où V est la vitesse lumière, et β est l'erreur maximale que peut être survenu dans la recherche de l'information de localisation.

– **Leach temporelle :** Dans cette méthode, tous les nœuds calculent l'expiration temps de chaque paquet en utilisant la vitesse de la lumière et ajouter cette date d'expiration dans le paquet pour détecter l'attaque de trou de ver. Les Leach géographiques sont plus avantageux que les leach temporelles, car ils ne nécessitent pas une horloge bien synchronisée. Il a les limites de la technologie GPS.

3.5.2 Méthode utilisant des antennes directionnelles

Hu et Evans proposent une méthode de vérification du voisinage au moyen d'antennes directionnelle. Ces antennes sont utilisées pour la restriction d'accès et la découverte des voisins. Des nœuds voisins sont identifiés par des zones où chaque zone est définie par les antennes directionnelles. Les zones sont numérotées de 1 à N. Quand un nœud reçoit un signal d'un autre nœud pour la première fois, ce dernier peut obtenir la direction approximative du signal et identifier le nœud inconnu par sa zone. Ensuite, le nœud coopère avec ses nœuds voisins pour vérifier la légitimité du nœud inconnu, par exemple, en vérifiant si le nœud inconnu est connu par les nœuds voisins. Des antennes directionnelles peuvent être considérées en tant que solutions basées par l'endroit.

3.5.3 Méthode utilisant un graphe theoretique

Lazos et al. propose une méthode basée sur un graphe théorique pour caractériser l'attaque de trou de ver et dérive les conditions nécessaires et suffisantes pour que n'importe quelle solution candidate puisse empêcher des trous de ver. Cette approche n'exige pas la synchronisation, ou des horloges fortement précises, et seulement une petite fraction de nœuds ont besoin de connaître leur endroit [30].

3.5.4 SECTOR

Srdjan Capkun et al. ont proposé SECTOR qui compose d'un ensemble de mécanismes pour la vérification des périodes de rencontres entre les nœuds dans les réseaux sans fils multi sauts. Ce qui nous intéresse ici, c'est de présenter le mécanisme proposé contre l'attaque wormhole.

L'idée est très simple, puisque l'attaque wormhole va faire croire que deux nœuds qui sont loin de se voir comme des voisins (la distance qui sépare ces nœuds est plus grande que leur portée de transmission). Ainsi si un nœud peut calculer la distance qui le sépare avec l'autre, il peut déduire s'il est réellement son voisin. Les autres proposent le protocole MAD, qui permet aux deux nœuds de mesurer simultanément la distance qui sépare l'un de l'autre. Chaque nœud doit avoir un dispositif qui lui permet l'envoie des bits séparés. Prenons deux nœuds u et v :

- Le nœud commence l'envoie des bits, au même moment il mesure le temps entre l'envoie de bit a_i et la réception de bit b_i
- Le nœud v mesure le temps calculés entre l'émission de b_i et la réception de a_{i+1}.
- A partir des temps calculés, les nœuds peuvent estimer une borne sur leur distance.

3.5.5 LITEWORP

LITEWORP est un protocole léger simple, pour détecter et atténuer des attaques de wormhole dans les réseaux sans fil ad hoc. LITEWORP fixe la découverte voisine de deux-sauts et la surveillance locale du trafic de commande pour détecter les nœuds impliqués dans l'attaque de wormhole. Ce protocole n'exige pas un matériel spécialisé, tel que les antennes directrices ou les horloges pour la synchronisation entre les nœuds dans le réseau. Dans LITEWORP, la détection et l'isolement sont faits judicieusement pour réduire au

minimum la possibilité de prendre pour victime des nœuds innocents dus à de fausses alertes provoquées par des collisions normales [37].

3.5.6 MOBIWORP

MOBIWORP a été proposé pour détecter et diagnostiquer des attaques de trou de ver dans les réseaux mobiles ad hoc. Le MOBIWORP utilise la surveillance locale de communication de voisinage par chaque nœud comme primitif. Il n'exige pas du matériel spécialisé aux nœuds de réseau, mais il se base sur une autorité centrale CA pour le cheminement de position des nœuds mobiles et maintenir leur comportement.

La détection dans MOBIWORP peut être locale ou globale. Dans la détection locale, le nœud malveillant est détecté par son voisinage. Tandis que dans la détection globale, le nœud malveillant est détecté sur l'échelle du réseau par le CA. La détection et le procédé d'isolement sont faits judicieusement pour réduire au minimum la possibilité de prendre pour victime des nœuds innocents dus à de fausses alertes provoquées par des collisions [35].

3.5.7 LDAC

Localized-Decentralized Algorithm for Countering ou LDAC est un algorithme contre des attaques de wormhole qui permet de vérifier la contiguïté d'un voisin potentiel, en utilisant seulement l'information de connectivité. L'idée de LDAC est de rechercher les sous-structures simples, dans le graphe de connectivité, qui indiquent qu'aucune attaque n'a eu lieu. L'avantage principal de cette approche est qu'il n'exige aucun matériel spécial tel que des antennes ou GPS [38].

3.6 Conclusion

Dans ce chapitre, nous avons présenté un état de l'art sur l'attaque wormhole. Il s'agit d'une attaque particulière, sévère et difficile à détecter. En effet, elle peut être menée même en présence des mécanismes assurant les différents service de sécurité. Son principe est l'utilisation d'un tunnel, reliant deux nœuds malicieux, pour acheminer des paquets captés dans une zone par l'un des nœud malicieux, afin de les rejouer par l'autre nœud malicieux dans une autre zone. L'objectif est la falsification des relations de voisinage et la dégradation de la performance du réseau en conséquence. Les solutions détectives et/ou préventives proposées dans la littérature restent toujours inefficaces et non suffisamment performantes pour faire face à cette attaque. Dans le chapitre suivant, nous allons proposer un schéma de prévention contre une telle attaque qui vient renforcer les solutions existantes en matière de détection et de prévention de l'attaque wormhole.

L'attaque de wormhole est l'une des attaques les plus actives contre les réseaux ad hoc sans fil, elle est très sévère du fais qu'elle peut être exécutée même si la communication du réseau fournit la confidentialité, l'authentification et l'intégrité, elle peut être aussi lancée avec ou sans compromettre des nœuds et il est difficile de la détecter. Dans le chapitre suivant, nous allons proposer notre solution pour se protéger contre ce genre d'attaque.

CHAPITRE 4

APPROCHE DE SÉCURITÉ POUR L'ATTAQUE WORMHOLE

4.1 Introduction

Un réseau ad hoc présente l'avantage d'être facile moins chère et rapide à déployer, cela à cause de ses caractéristiques inhérentes qui sont principalement l'ouverture de médium de communication, la mobilité et l'absence d'infrastructure. On contre partie ces mêmes caractéristiques ont rendu ce type de réseau facilement vulnérable. Le wormhole, sujet de notre étude, est l'une des attaques les plus sévères et qui a un impact négatif sur la performance du réseau. En effet, en falsifiant les informations de voisinage, cette attaque peut causer un séreux problème qui provoque la mise hors fonction le réseau tout entier. Les solutions proposées dans la littérature, bien qu'elles soient multiples et diversifiés, elles n'arrivent pas à étouffer complètement l'effet de l'attaque wormhole. Ceci nous a motivé de proposer une solution de sécurité à la fois efficace et performante.

Pour lutter contre l'attaque wormhole, nous proposerons une solution qui se base sur le découpage en zones de la région considéré ces zones possèdent chacune un identifiant différent. Pour envoyer un paquet, un nœud donné doit indiquer dans le paquet l'identifiant de la zone dans laquelle il se trouve au moment de l'envoi de ce paquet. De cette façon le wormhole qui capte des paquets dans une zone et les rejoues dans une zone lointaine, peut être facilement détecté grâce à la vérification de l'identifiant de la zone. A noter

que la solution proposée est légère, performante et scalable. Ceci dans le sens où aucun matérielle n'est nécessaire pour sa mise en œuvre. Par simulation, nous mesurerons son efficacité et évaluer sa performance en termes d'overhead de communication.

Le reste de ce chapitre est structuré autour de quatre sections. Dans la deuxième section nous décriverons le modèle de réseau utilisé suivi par la section trois où les détailles de notre schéma de sécurité sont présentées. Les résultats de simulations sont interprétés et analysée dans la section quatre et le chapitre s'achèvera par une conclusion qui récapitulera notre solution de sécurité et énumèrera les perspectives.

4.2 Modéle de réseau

Le réseau considéré dans notre travail est composé d'un certain nombre de nœuds dispersés d'une manière aléatoire dans une région. Le réseau est découpé en plusieurs zones, chacune possède un identifiant utilisé par les nœuds lors de l'envoie des paquets. Pour lancer l'attaque de wormhole, deux malicieux localisés dans des zones différentes, établissent un tunnel (un lien physique en fibre optique).

L'attaque consiste à capter les messages par le premier nœud malicieux et les envoyer via le tunnel au deuxième malicieux. Ce dernier rejoue les messages reçus dans le réseau, suite à une attaque wormhole les nœuds dans une région Z1 vont Coire qu'il y'a des liens de voisinages entre eux et les nœuds qui se trouvent dans une région Z2 et ceci malgré que les nœuds de la région Z1 sont en réalité hors porté de transmission des nœuds de la région Z2. Le résultat d'un tel comportement peut être la falsification des relations de voisinages entre les nœuds. Ceci affectera les différentes fonctionnalités du réseau en particulier la fonction de routage. A noter qu'au niveau de notre réseau aucune restriction n'est faite sur la topologie du réseau (statique ou dynamique), et nous ne exigeons pas que les nœuds soient équipés d'un matériels spéciale ou se référons à une horloge de synchronisation comme c'est le cas dans certains schéma de sécurité proposés dans la littérature.

4.3 Solution de sécurité proposée

Dans cette section, nous présenterons dans un premier lieu les hypothèses sous lesquelles notre solution est fonctionnelle. Ensuite la solution proposée sera décrite en détailles, ses avantages et inconvénients seront aussi signalés.

4.3.1 Hypothèse

Dans le réseau considéré dans notre travail, nous supposons que le réseau est découpé en zones et chaque zone est identifiée par un identifiant unique. Il est évident que la mobilité entraine la mise à jour des identifiants des zones au niveau des nœuds quand ces derniers se déplacent d'une zone à une autre.

Nous supposons aussi que les nœuds du réseau sont homogènes particulièrement en termes de puissance de transmission, ceci pour éviter le cas où la portée de communication d'un nœud très puisant dépassera même les zones voisines.

4.3.2 Détail de la solution

Pour lutter contre l'attaque wormhole nous avons proposé une solution qui repose sur le découpage du réseau en zones. Chaque zone est désignée par un identifiant unique utilisé par les nœuds lors de la communication. L'idée consiste à envoyer l'identifiant de la zone avec chaque paquet transmit de cette façon les paquets captés dans une zone et rejoués dans une autre zone lointaine sont facilement détectées grâce à l'identifiant réseau qui accompagne les paquets envoyés. Comme il est illustré sur la figure 4.1, Les paquets générés par le nœud A qui se trouve dans la zone 3, captés par le nœud malicieux M1 et acheminés via le tunnel vers le nœud malicieux M2 pour être rejoués par M2 et reçu par le nœud B qui se trouve dans la zone 22. Ce scénario d'attaque est facilement détectable par le nœud B au moment de la réception des paquets par un nœud qui se trouve dans une zone non voisine à la zone de B. en d'autre termes, le nœud A ne considère légitime que les paquets reçus des nœuds se retrouvant dans une zone voisine, par contre, un paquet reçu de la part d'un nœud qui se retrouve dans une zone non voisine indique la présence

d'une attaque wormhole.

Le pseudo algorithme suivant résume notre schéma de sécurité contre l'attaque wormhole.

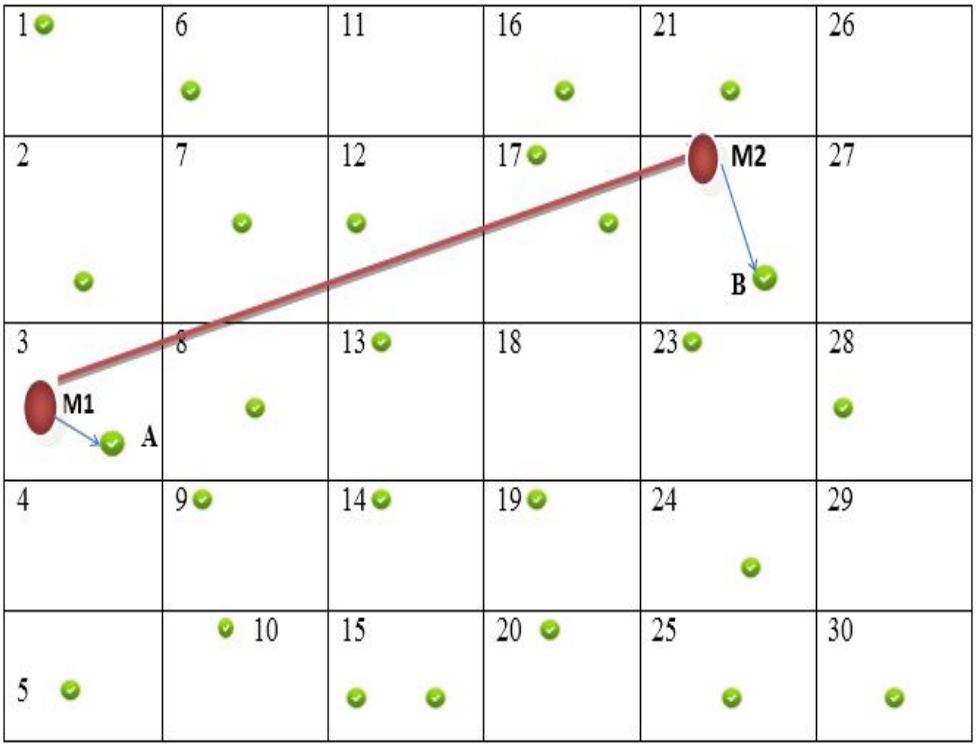

FIGURE 4.1 – schéma de la solution.

1. Le réseau est découpé en zones, dont chaque nœud appartient à une et une seul zone.
2. Un nœud source S peut communiquer seulement avec un nœud D qui appartient à la même zone que sa zone (la zone de S) ou à une zone voisine (d'un seul saut).
3. Un nœud source S envoie l'identifiant de sa zone avec chaque paquet transmit, de cette façon les paquets captés dans une zone et rejoués dans une autre zone lointaine sont facilement détectées grâce à l'identifiant réseau qui accompagne les paquets envoyés.

L'avantage de notre schéma de sécurité est qu'il n'a pas besoin de matériels supplémentaires pour sa mise en œuvre, et il n'exige aucune coopération entre nœuds pour sécuriser le réseau contre l'attaque wormhole. Il est aussi facilement intégrable dans n'importe quel protocole de routage existant. La seule modification consiste à rajouter un champ dans les

paquets pour stocker l'identifiant de la zone. Nous remarquons aussi que notre solution n'exige aucune connaissance préalable du voisinage à k-sauts (k>1). En plus, la solution proposée ne fait référence à aucune horloge de synchronisation comme c'est le cas dans certaines approches de sécurité proposées dans la littérature. Ces avantages, bien évidemment, rendent la solution proposée plus scalable et performante en terme d'overhead de communication. La contrainte que peut présenter notre solution est le découpage en zones du réseau. En effet, dans un réseau découpé en plusieurs petites zones la détection de wormhole sera plus précise, mais en contre partie, la mise à jour de l'identifiant de la zone au niveau des nœuds qui bougent est très fréquente. Dans le cas où le nombre de zones est petit, cela rendra la détection de wormhole moins précise.

4.4 Paramètres de simulation

Pour mesurer l'efficacité de notre solution en termes de taux de détection et évaluer sa performance, nous avons effectué une série de simulation utilisant les paramètres listés dans le tableau suivant :

Paramètre	**Valeur**
Nombre de nœuds	20
Taille de réseau	100*100 m
Nombre de zones	5*5
Temps de simulation	500s
Portée de communication	25m
Taille des paquets	1024 bits
Protocole de routage	AODV

TABLE 4.1 – les paramètres de simulation.

L'ensemble des nœuds sont déployés d'une manière aléatoire. Dans une surface de 100*100m, parmi ces nœuds, on a choisit deux nœuds malicieux localisés dans des zones différentes. Ces derniers vont jouer l'attaque en établissant un tunnel entre eux. Chaque nœud dans le réseau génère périodiquement des messages HELLO pour découvrir le voi-

sinage à un seul saut. Ces paquets HELLO vont être captés par le premier malicieux dans sa zone et acheminer via le tunnel vers le deuxième malicieux qui les rejoues dans sa zone.

4.5 Métriques de simulation

Pour prouver l'efficacité de notre solution et évaluer sa performance, Nous avons mesuré les métriques suivantes :

1. **PDR(Packet Delevery Ratio) :** indique le pourcentage des paquets reçus avec succès par le destinataire par apports aux nombre total des paquets envoyés.
2. **PSR (Packet Sent Ratio) :** représente le taux des paquets envoyés avec succès par le nœud source.

   Ces deux métriques ont été choisies pour justement monter l'effet négatif du wormhole sur la communication entre les nœuds sources et destination d'une part, et la neutralisation de cet effet par notre solution d'autre part.
3. **Taux de prévention :** représente tout simplement la valeur de PDR étant donné que le nombre de zones est tel. Cette métrique a été choisie pour montrer que la prévention du wormhole est plus au moins précise selon que le nombre de zones est grand ou petit.
4. **Faux négatif :** : représente le nombre de cas où le wormhole est mené sans être prévenu et ceci en fonction du nombre des zones. Cette métrique a été choisie parce qu'il est facilement remarquable que si le nombre de zones diminue alors des cas où le wormhole est réussi sans être prévenu peuvent se produire.

4.6 Résultats de simulation

4.6.1 Interprétation et analyse

- **Effet du wormhole**

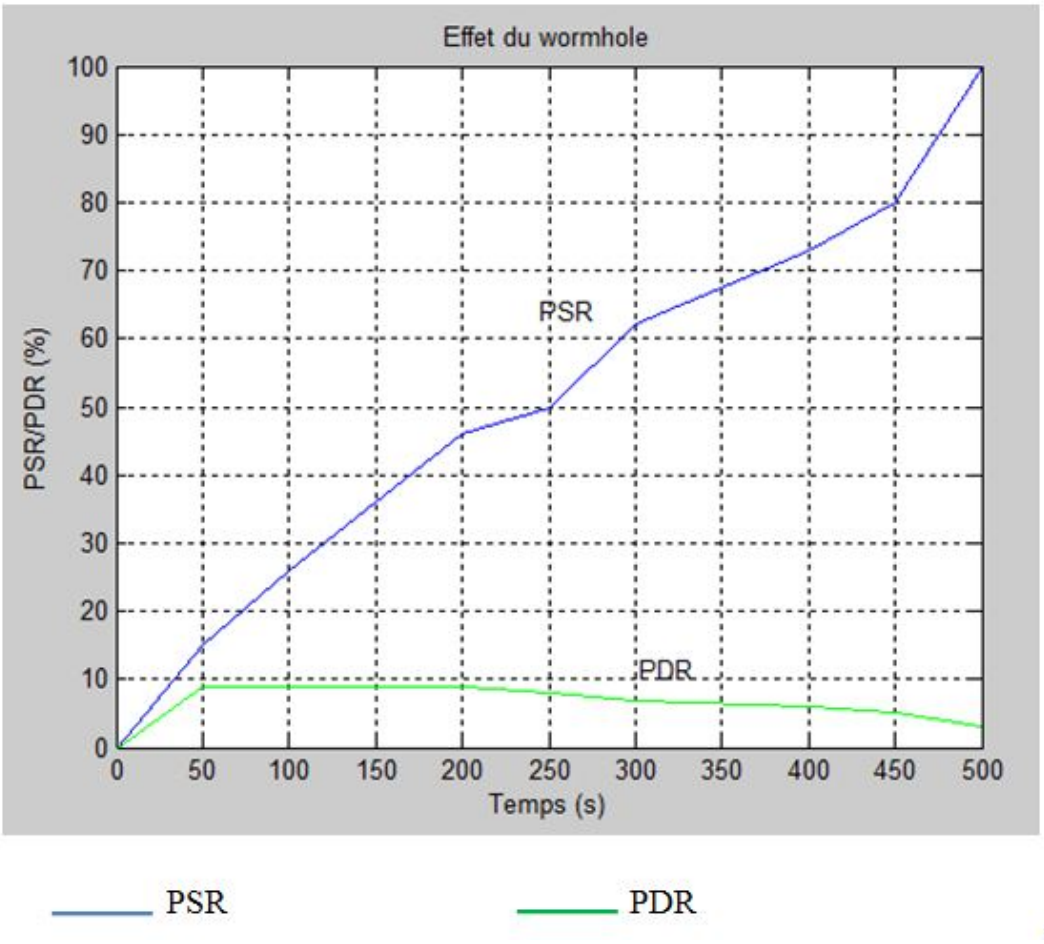

FIGURE 4.2 – Effet du wormhole.

La figure 4.2 illustre la mesure du PDR et du PSR en fonction du temps dans le cas d'attaque. On constate que Le pourcentage des paquets envoyés avec succès par les nœuds sources est en augmentation, en contre partie le nombre de paquet reçus avec succès commence à chuter en menant l'attaque de wormhole à l'instant 50s. Le PSR s'augmente car l'attaque wormhole n'influence pas sur les paquets lors de l'émission, ce qui signifie la baisse de PDR juste après avoir mené l'attaque wormhole.

- **Effet de la solution**

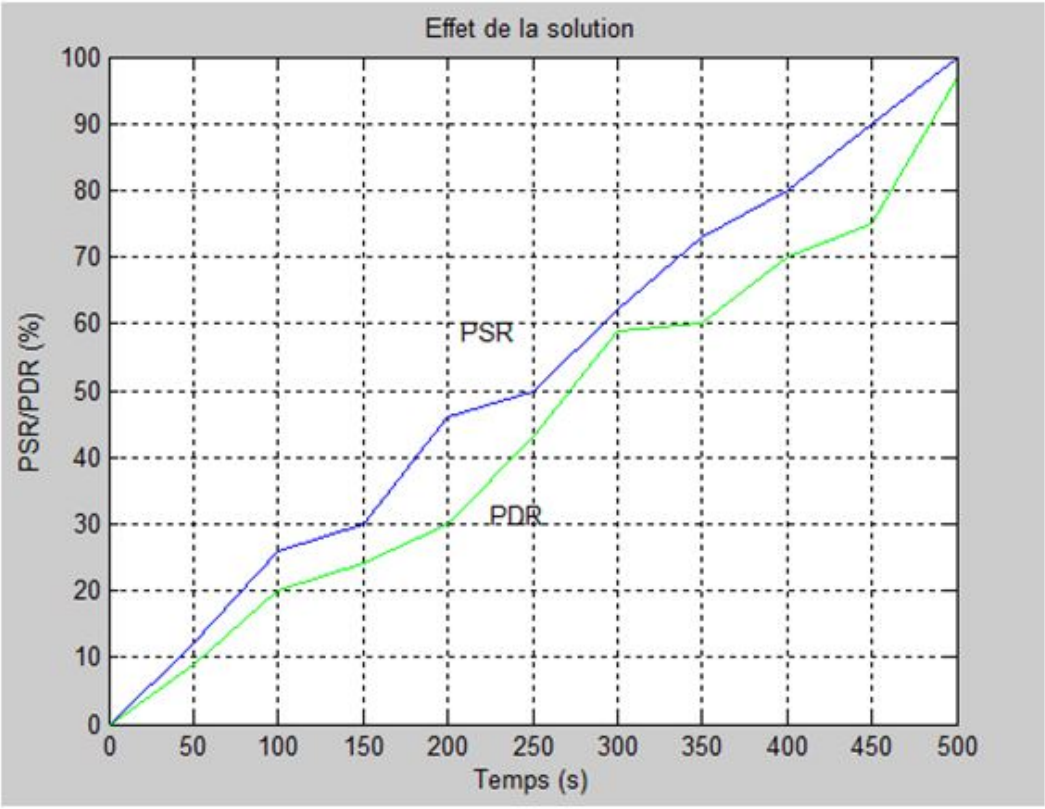

FIGURE 4.3 – Effet de la solution.

La figure 4.3 illustre le PDR et du PSR en fonction du temps dans le cas de la solution. Le pourcentage de paquets envoyés avec succès par les nœuds sources et même le pourcentage des paquets reçus avec succès sont en augmentation, Le PSR et le PDR sont en augmentation cela est dû à l'effet de la solution proposée qui a empêché le wormhole cela a causé la non perte de paquets.

- **Taux de prévention**

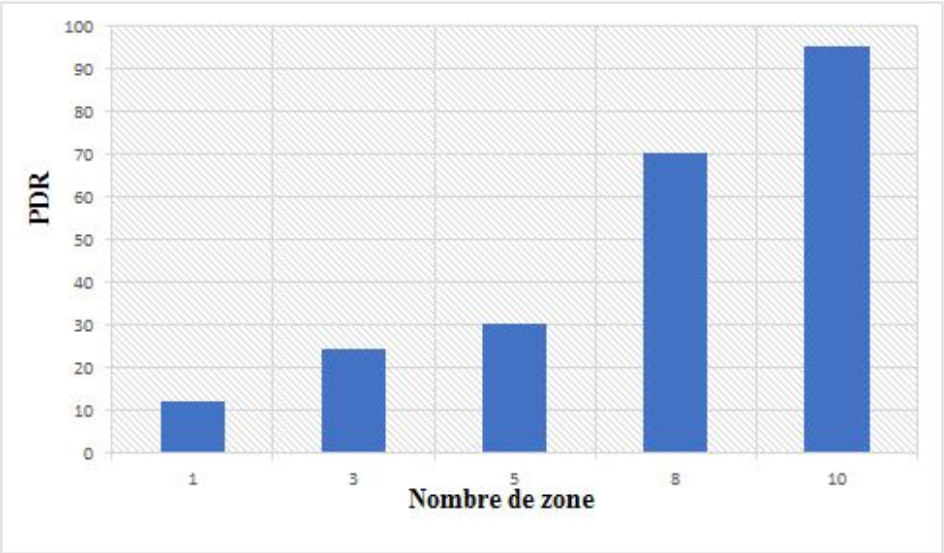

FIGURE 4.4 – Taux de prévention.

Dans figure 4.4 on remarque que le PDR s'augment avec l'augmentation du nombre de zones. L'augmentation de nombre de zone a conduit à l'augmentation de nombre de paquets reçus avec succès. La prévention du wormhole est plus au moins précise selon que le nombre de zones est grand ou petit.

- **Faux négative**

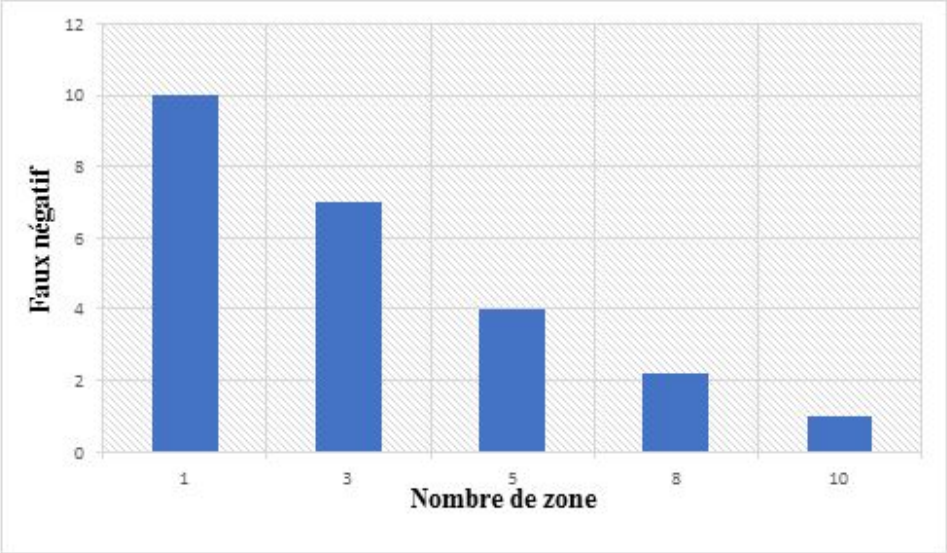

FIGURE 4.5 – Faux négatif.

La Figure 4.5 Illustre le nombre de faux négatifs. On remarque que Le faux négatif se deminue en diminuant le nombre de zones. La diminution du faux négatif est dû para port aux nombre de zone car il est facilement remarquable que si le nombre de zones diminue alors des cas où le wormhole est réussi sans être prévenu peuvent se produire.

4.7 Conclusion

Dans ce chapitre nous nous sommes focalisés sur l'attaque wormhole dans laquelle les paquets captés dans une zone sont rejoués sur autre zone par l'utilisation d'un tunnel établi entre deux noeuds malicieux. La conséquence d'une telle attaque est la dégradation de la performance du réseau à cause de la falsification des relations de voisinage. Pour remédier à ce problème de sécurité, un schéma de prévention a été proposé.

L'idée est que le réseau est découpé en zone est chaque zone est identifié par un identifiant unique. Pour transmettre son paquet, un nœud est dans l'obligation d'envoyer aussi l'identifiant de la zone dans laquelle il se trouve, de cette façon le récepteur peut découvrir d'où provient le paquet reçu. Le scénario où le paquet est reçu à partir d'une zone voisine est considéré comme étant un comportement normal tandis que la réception des paquets venant de zone lointaine est susceptible d'être une attaque wormhole. Les résultats de simulation montrent que notre schéma de prévention est efficace, néanmoins le nombre de faux positif reste toujours non négligeable.

En perspectives nous envisageons d'améliorer notre schéma de prévention en minimisant le nombre de faux négatif. En plus des mesures de sécurité doivent être envisagées pour protéger les identifiants des zones contre la modification.

CONCLUSION GÉNÉRALE

Les solutions de sécurité proposées dans la littérature reposent principalement sur des outils cryptographiques ou non cryptographiques et sur la réputation des nœuds pour s'assurer de l'authenticité de ces derniers, préserver l'intégrité et la confidentialité des données, contrôler l'accès au médium des données, et garantir l'anonymat des nœuds. Vue la multitude des vulnérabilités des réseaux ad hoc, ces solutions n'arrivent pas à faire face d'une manière efficace est performante aux différentes attaques possibles. En conséquence, la sécurité reste toujours un problème de recherche ouvert et il le remède loin d'être évident.

Dans notre travail, nous nous sommes focalisés sur l'attaque wormhole dans les réseaux ad hoc. Il s'agit d'une attaque très sévère qui consiste à établir un tunnel entre deux nœuds malicieux, afin de relayer les paquets entre deux zones différentes. L'objectif est de falsifier les relations de voisinage et perturber en conséquence l'opération de routage, en dégradant ainsi la performance du réseau. Pour se prévenir de cette attaque, nous avons proposé une solution qui consiste à découper le réseau en zones et exige l'envoi de l'identifiant du réseau à chaque communication entre nœuds. Notre solution présente l'avantage d'être légère et scalable dans le sens où aucun matériel tel que le GPS est exigé et aucune horloge n'est nécessaire comme c'est le cas dans certaines solutions existantes. Les résultats de simulation montrent que notre solution est efficace pour se prévenir de cette attaque.

D'après les résultats de simulation, il est à noter que notre schéma de prévention présente un nombre de faux négatif non négligeable. Dans un travail futur, nous allons

améliorer notre solution pour minimiser le nombre de faux négatif afin de rendre la prévention plus efficace et performante. En plus, nous allons mettre en œuvre des mécanismes de sécurité pour protéger l'identifiant de la zone contre une éventuelle modification possible. Nous envisageons aussi de comparer notre solution avec des solutions de référence en termes d'efficacité et robustesse.

BIBLIOGRAPHIE

[1] N. BOUKHECHEM. Routage dans les réseaux mobiles ad hoc par une approche a base d'agents. Mémoire magister, Université de Constantine, 2008.

[2] Barry Leiner James A. Freebersyser. A dod perspective on mobile ad hoc networks. *Ad Hoc Networking*, pages 29–51, 2001.

[3] J. Macker S. Corson. Mobile ad hoc networking (`MANET`) : Routing protocol performance issues and evaluation considerations. *Request for Comments*, January 1999.

[4] Abdelmajid HAJAMI. Sécurité du routage dans les réseaux sans fil spontanés. ThÈse doctort, Ecole Natonale Supérieure d'Informatique, Rabat.

[5] Abderrezak RACHEDI. Contributions à la sécurité dans les réseaux mobiles ad hoc. ThÈse doctort, Université d'Avignon, 29 mars 2012.

[6] M. Tahar Abbes. Proposition d'un protocole à économie d'énergie dans un réseau hybride gsm et ad hoc. Thèse de doctorat, Université d'Oran,Département d'Informatique, 2012.

[7] S. Boukli Hacene. Qualité de service. Thèse de doctorat, Université Djillali Liabes, 2012.

[8] P.Bhagwat C.Perkins. Highly dynamic destination-sequences distance-vector routing-(dsdv) for mobile computers. *ACM SIGCOMM*, pages 234–244, september 1994.

[9] E.M. Royer and C.K. Toh. A review of currentroutingprotocols for ad hoc mobile wireless networks. Technical report, University of California and Georgia Institute of Technology, USA, 1999.

[10] B. Ait Salem. Sécurisation des réseaux ad hoc : Systèmes de confiance et de détection de répliques. Thèse de doctorat, 2011.

[11] E.M. Royer and Charles E. Perkins. Multicast operation of the ad-hoc on-demand distance vector routing algorithm. Technical report, University of California.

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

[13] Riahla Med Amine. Conception et mise en oeuvre d'un nouveau protocole de routage multi chemins sécurisé pour les réseaux ad hoc basé sur les colonies defourmis. mémoire de magister, Université de Boumerdes, 2008.

[14] H. W. da Silva A. L. dos Santos M. N. Lima and G. Pujolle. A security management architecture for supporting routing services on wanets. Technical report, Federal University of Parana.

[15] Pietro Michiardi. *Coopération dans les réseaux ad hoc : Application de la théorie des jeux et de l'évolution dans le cadre d'observabilité imparfaite*. 2006.

[16] Étude technique réalisée par CGI. Étude technique cryptographie à clé publique et signature numérique principes de fonctionnement. Technical report, Septembre 2002.

[17] David Wagner Chris Karlof. Secure routing in wireless sensor networks : attacks and countermeasures. *Ad Hoc Networks*, pages 293–315, 2003.

[18] Alexandre Poquet. Les attaques sur le routage dans les réseaux ad hoc. 09 février 2007.

[19] Ross Anderson Frank Stajano. The resurrecting duckling :security issues for ad- hoc wireless networks. volume 1796, 1999.

[20] A. L. dos Santos M. N. Lima, H. W. da Silva and G. Pujolle. A security management architecture for supporting routing services on wanets. Technical report, Federal University of Parana, Brazil, 2010.

[21] A. Perrig Y.C. Hu and D. B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In *Proceedings of the 2nd ACM workshop on Wireless securitys*, pages 30–40, San Diego,USA, 2003.

[22] L. Nauymi. F. Dupont S. Gombault et B. Tharon V. Gayraud. Cryptography and network security, principal and practice. technical report. Technical report, In Sympo-

sium sur la sécurité des technologies de l'information et de la communication SSTIC, Rennes France, june 2013.

[23] Céline Burgod. Contribution à la sécurisation du routage dans les réseaux ad hoc. Thèse de doctorat, Université de LIMOGES, Octobre 2009.

[24] PanagiotisPapadimitratos and Zygmunt J. Haas. Secure link state routing for mobile ad hoc networks. *SAINT Workshops*, pages 379–383, 2003.

[25] Shekhar M. Arora, Z. Zafrulla and K. Ramanatha. Secure dynamic source routing protocol (sdsr) for mobile ad hoc networks. technical report, 2004.

[26] A.Perrig Y.Hu and P.Leashes. A defense against wormhole attacks in wereless. Master's thesis, Rice University, 2001.

[27] L. Me R. S. Puttini and R. T. Sousa. Certication and authentication services for securing manet routing protocols. 2003.

[28] Manel Guerrero Zapata and N. Asokan. Securing ad hoc routing protocols. pages 1–10, ACM, 2002. Workshop on Wireless Security.

[29] Adrian Perrig Yih-chun Hu, David B. Johnson. Sead : Secure efficient distance vector routing for mobile wireless ad hoc networks. *Mobile ComputingSystems and Applications*, pages 3–13, 2002.

[30] Ahmad Heidari and Islamic Azad. A survey of wormhole attack and countermeasures against that in wireless ad-hoc networks. Iran, 12-14 May 2011. Khavaran Higher-education Institute.

[31] Moutushi Singh and Rupayan Das. A survey of different techniques for detectionof wormhole attack in wireless sensor network. *International Journal of Scientific and Engineering Research*, 3, October 2012.

[32] Hamid Sarbazi-Azad Sina Meraji. Adaptive routing in wormhole-switched necklace-cubes : Analytical modelling and performance comparison. 2009.

[33] James Ford Yurong Xu, Guanling Chen and Fillia Makedon. *Critical Infrastructure Protection*, volume 253, chapter Detecting Wormhole attacks in wireless sensor Networks, pages 267–279. 2008.

[34] Baltej Kaur Saluja. A survey of different approaches to detect wormhole attack. *International Journal of Computer Science and Information Technologies*, 5(3) :4369–4372, 2014.

[35] Ness B. Shroff Issa Khalil, Saurabh Bagchi. *MOBIWORP : Mitigation of the wormhole attack in mobile multihop wireless networks*. 2008.

[36] Luis Fernando GARCIA. Preventing layer-3 wormhole attacks with multipath dsr montrial. Thèse de doctorat, September 2009.

[37] Saurabh Bagchin Issa Khalil and Ness B. Shroff. Liteworp : Detection and isolation of the wormhole attack in static multihop wireless networks. *Computer Networks*, pages 3750–3772, 2007.

[38] Tassos Dimitriou Thanassis Giannetsosa. Ldac :a localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks. *Journal of Computer and System Sciences*, 2014.

Résumé

Un réseau ad hoc est vulnérable par plusieurs types d'attaques. Le wormhole est l'une des attaques les plus sévères, dans laquelle un nœud malicieux capte les paquets dans une zone, les achemine via un tunnel préétabli vers un autre nœud malicieux qui les rejoue dans une autre zone. L'objectif est la falsification des relations de voisinage et la dégradation de la performance du réseau en conséquence. Pour lutter contre une telle attaque, nous avons proposé une solution qui découpe le réseau en zones désignées par des identificateurs, ensuite, l'identificateur de la zone est toujours envoyé avec les paquets lors de la transmission. De cette façon, le wormhole est détecté car la communication entre zones non voisines n'est pas permise. Par simulation, nous avons prouvé l'efficacité de notre solution et évaluer sa performance. En perspective, nous allons comparer notre solution avec des travaux de référence.

Mots-clés : réseaux ad hoc, vulnérabilités des réseaux ad hoc, sécurité des réseaux ad hoc, wormhole.

Abstract

An ad hoc network is vulnerable to several types of attacks. The wormhole is one of the powerful attacks, in which a malicious node collects the packets in a zone, conveys them via a tunnel towards another malicious node which remove them in another zone. The objective is the falsification of the neighbor relations, and the degradation of the performance of the network consequently. To fight against such attack, we proposed a solution which cuts out the network in zones indicated by identifiers, then, the identifier of the zone east always sent with the packages during the transmission. In this way, the wormhole is detected because the communication between non close zones is not allowed. By simulation, we proved the effectiveness of our solution and evaluated its performance. In prospect, we will compare our solution with work of reference.

Keywords : ad hoc networks, vulnerabilities of the ad hoc networks, safety of the ad hoc networks, wormhole