Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa

Faculté des Scineces Exactes

Département informatique

Thème

Sécurité dans les réseaux Ad Hoc

Wormhole

MÉMOIRE DE FIN D'ÉTUDES

En vue de l'obtention du diplôme de Master

Option :

Administration et sécurité des réseaux

Soutenu devant le jury composé de :

Président	M^r	KHANOUS
Examinateur	M^r	MOUMEN
Examinateur	M^r	DEMOUCHE
Promoteur	M^r	BAADACHE

Présenté par :

M^r *TIGHIDET* Abdelghani

M^r *IMLOUL* Fatah

Promotion 2012/2013

Dédicaces

A mes parents

Je vous dois ce que je suis aujourd'hui grâce à votre amour, à votre patience et vos innombrables sacrifices. Que ce modeste travail, soit pour vous une petite compensation et reconnaissance envers ce que vous avez fait d'incroyable pour moi. Que Dieu, le tout puissant, vous préserve et vous procure santé et longue vie afin que je puisse à mon tour vous combler.

A mes très chères sœur et frère : **Hanane** et **Lamine**.

A toute ma famille.

A Tous ceux qui me sont chers.

A tous mes amis et, plus particulièrement, à ceux qui ont contribué de près ou de loin à la réalisation de ce modeste travail.

Abdelghani

Dédicaces

A ma très chère mère :

Ta prière et ta bénédiction m'ont été d'un grand secours Pour mener à bien mes études.

Je te dédie ce travail en témoignage de mon profond amour.

Puisse Dieu, le Tout Puissant, te préserver et t'accorder santé, longue vie et bonheur inchallah .

A mon Père :

Aucune dédicace ne saurait exprimer l'amour,L'estime, le dévouement et le respect que j'ai toujours eu Pour toi. Rien au monde ne vaut les efforts fournis jour et nuit pour mon éducation et mon bien être. Ce travail est le fruit de tes sacrifices que tu as consentis pour mon éducation et ma formation

A mes chères ami(e)s qui ont contibués à la réalisation de ce projet (Hakim,Lamine...etc).

Fatah

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.

Table des matières

Table des figures

Liste des tableaux

Résumé

Un réseau Ad Hoc est un système de communication autonome d'un ensemble d'appareils mobiles (PDA, ordinateurs portables, téléphone, etc.) reliés par des liens sans fils.

Ces derniers peuvent jouer le rôle de routeur ou de passerelle afin de permettre une communication d'un mobile à un autre. Cette technologie constitue donc une solution très attractive pour construire des réseaux dynamique de terminaux mobiles qui allient les avantages de la simplicité de construction à un coût construction relativement modeste. L'utilisation des réseaux ad hoc est de plus en plus répandue et les applications sont multiples : déploiement d'un réseau en cas de sinistre majeur rendant inopérable l'infrastructure réseautique existante, déploiement d'un réseau militaire dans une zone d'opération, déploiement d'un réseau de capteurs, etc. Toutefois, ces réseaux posent encore de nos jours des défis majeurs en termes de sécurité.

Un mécanisme de gestion de clés constitue une partie primordiale de toute architecture de sécurité pour garantir la confidentialité, l'intégrité et l'authentification des communications. Cependant, le déploiement de tel mécanisme dans les MANETs est une tache critique à cause des caractéristiques de ces réseaux notamment l'absence d'infrastructure et d'une autorité centrale. Le but de ce mémoire est d'étudier les défis de sécurité posés dans les MANETs et de proposer une solution adéquate adaptée à la nature de ces réseaux.

Mots clés : reseaux Ad Hoc, sécurité de routage.

Abstract

An network ad hoc is a self-hoc communication system of a set of mobile devices (PDA, notebook, phone, etc..), Connected by links without son. These can act as a router or gateway to enable mobile communication from one to another. This technology is a very attractive solution for building dynamic networks of mobile devices that combine the advantages of simple construction to build a relatively modest cost.

The use of ad networks hoc is becoming more widespread and multiple applications including network deployment in the event of a major disaster rendering inoperable existing networking infrastructure, deployment of a military network in the area of operation, deployment of a network of sensors, etc.. However, these systems still pose major challenges today in terms of safety.

A mechanism for key management is a critical part of any security architecture to ensure the confidentiality, integrity and authentication of communications. However, the deployment of such a mechanism in MANETs is a critical task due to the characteristics of these networks includes the lack of infrastructure and a central authority. The purpose of this memory is to study the security challenges in MANETs and propose appropriate to the nature of these networks solution.

Key words : ADd Hoc network, routing security.

Liste des Acronymes

MANET : Mobile Ad hoc Network.

PAN : Personal Area Network.

ZRP :Zone Routing Protocol.

SEAD : Secure Efficient Ah Doc Distance vectore routing protocol.

OLSR : Optimized Link State Routing.

QoS : Quality of Service.

CA :Certification Authority.

PKI :Public Key Infrastructure.

MAC : Medium Access Control.

TDMA :Time Division Multiple Access.

GPS : Global Positionning System.

SLSP :Secure Link State routing Protocol

AODV :Ad hoc On-Demand Distance Vector.

RERR :Route ERRor.

RREP :Route REPlay.

RTT :Round Trip Travel Time.

MAD : Mutual Authenticated Distance-bounding.

MDS :Multi-Dimensional Scaling.

ARAN :Authenticated Routing for Ad hoc Network.

Introduction générale

Un réseau ad hoc mobile (MANET) est un système autonome de nœuds mobiles, reliés par des liens sans fils, dont l'union forme un graphe arbitraire. Les nœuds du réseau jouent le rôle de routeurs ils sont libres de se déplacer aléatoirement et de s'organiser arbitrairement. En conséquence, la topologie du réseau peut changer rapidement et de manière imprévisible.Les réseaux sans fil ad hoc sont composés de systèmes informatiques divers, plus oumoins complexes, appelés nœuds, par la suite en ayant la possibilité de communiquer de manièreautonome par ondes radio. Les nœuds interagissent et peuvent coopérer pour s'échanger des services. Un nœud peut, à la fois communiquer directement avec d'autres nœuds, ou servir de relais. Un relais permet à des nœuds, se trouvant hors de portée radio les uns des autres decommuniquer. Ces réseaux sont dits ad hoc dans la mesure où ils ne nécessitent pas d'infrastructure fixe. Ils peuvent exister temporairement pour répondre à un besoin ponctuelde communication.

Un tel réseau ne nécessite pas d'infrastructure fixe et représente une option attractive, pour connecter spontanément des terminaux mobiles. Les champs d'application sont divers : déploiement d'un réseau durant une opération militaire sur un champ de bataille ou durant une opération de sauvetage, dans un lieu difficilement accessible... etc. Quelle que soitl'application visée, un réseau MANET possède des exigences spécifiques, en terme de sécurité ;du fait de ses particularités : liens sans fils, contraintes d'énergie, limitation éventuelle de la bande passante et de la puissance de calcul, non connectivité permanente d'un nœud avec(tous) les autres nœuds .... Jusqu'à présent, les nombreux travaux traitant de la sécurité des MANET, s'articulent principalement selon les trois problématiques suivantes : la définition des modèles de confiance, la mise au point de mécanismes d'authentification et de gestion de clefs adaptés et la sécurisation des protocoles de routage ad hoc.

Chapitre 1

Généralité sur les réseaux Ad Hoc

1.1 Introduction

Aujourd'hui, les environnements mobiles offrent une grande flexibilité d'emploi, 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 connus sous le nom de réseaux ad hoc qui se focalisent à notre thème(voire la figure).

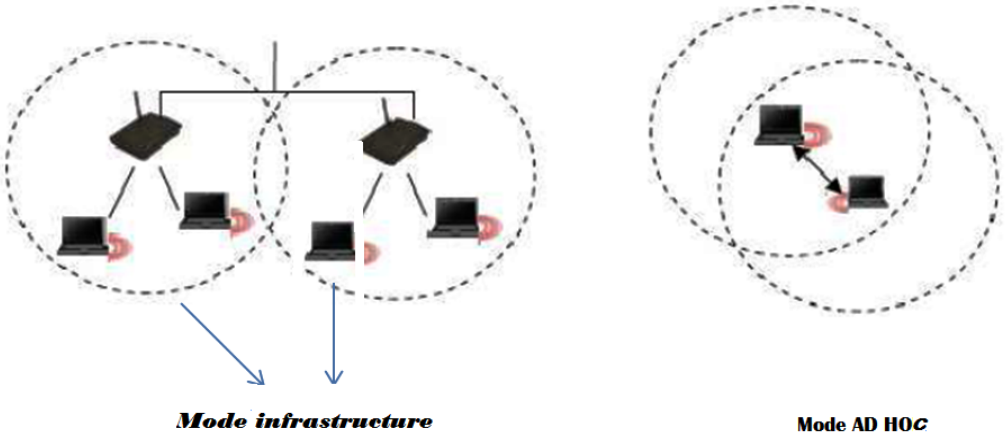

FIGURE 1.1 – les réseau en mode AD HOC et infrastructure

1.2 Les réseaux Mobiles

Un réseau est dit mobile, s'il permet à ses utilisateurs d'accéder à l'information, indépendamment de leurs positions géographiques. Pour communiquer entre eux, les nœuds du réseau mobile, utilisent une

interface de communication sans fil (médium radio ou infrarouge), qui permet de propager les signaux sur une certaine distance. Les réseaux mobiles offrent une plus grande flexibilité d'emplois et un plus grand confort par rapport aux réseaux statiques.

1.3 Les Réseaux AD HOC

1.3.1 Définition

Le terme **" ad hoc "** est une locution d'origine latine, qui signifie " qui convient au sujet, à la Situation. " On parle donc de réseaux auto-adaptatifs (capables de s'organiser par eux-mêmes [1]. Une Autre lecture de la définition peut signifier une propriété d'universalité de ce moyen de communication, comme si ce procédé pouvait satisfaire tous les besoins en termes de communication entre objets mobiles.

Un réseau ad hoc mobile (MANET : Mobile Ad hoc NETwork), est considéré comme un système autonome dynamique ,composé des nœuds mobiles interconnectés par des liens sans fil, sans l'utilisation d'une infrastructure fixe et sans administration centralisée [2]. Les nœuds sont libres de se déplacer aléatoirement et s'organisent arbitrairement. Par conséquent, la topologie du réseau peut varier de façon rapide et surtout imprévisible.

Modélisation : Un réseau mobile ad hoc peut être modélisé par un graphe $Gt = (Vt, Et)$ où :
Vt : représente l'ensemble des nœuds (les unités ou les hôtes mobiles) du réseau.
Et : modélise l'ensemble des connexions qui existent entre ces nœuds. (Figure 1.2).
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].

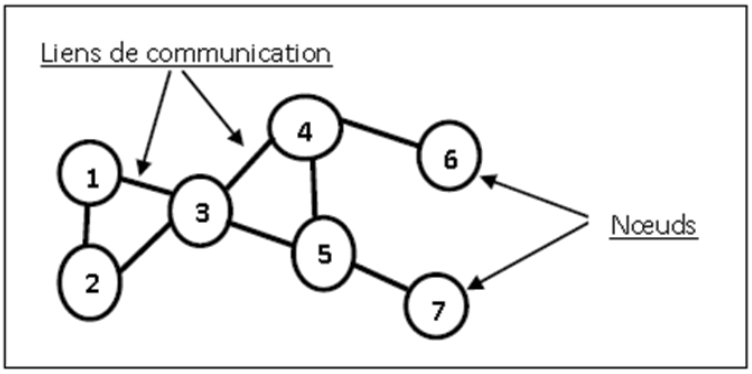

FIGURE 1.2 – Modélisation d'un réseau ad hoc

1.3.2 Caractéristiques des réseaux Ad hoc

Les réseaux mobiles Ad hoc possèdent non seulement les mêmes caractéristiques que les réseaux mobiles, mais aussi un certain nombre de caractéristiques qui leur sont propres et qui les différencient des autres. Nous pouvons citer quelques caractéristiques principales :

• **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[4]. Un nœud joue le rôle aussi bien d'un acteur actif dans le réseau émetteur et récepteur ,mais aussi ,de routeur pour relayer la communication des autres nœuds du réseau.

• **Topologie du réseau dynamique** les nœuds du réseau sont autonomes et capables de se déplacer de manière arbitraire voir la figure(1.3). Cette mobilité [5] ne fait que la topologie réseau est dynamique, car elle peut changer à tout instant de façon rapide et aléatoire .
Ce changement de topologie a un impact sur les connexions ou les liens unidirectionnels et bidirectionnels des nœuds. Comme exemple, un nœud (routeur) peut à chaque moment quitter ou rejoindre le réseau.

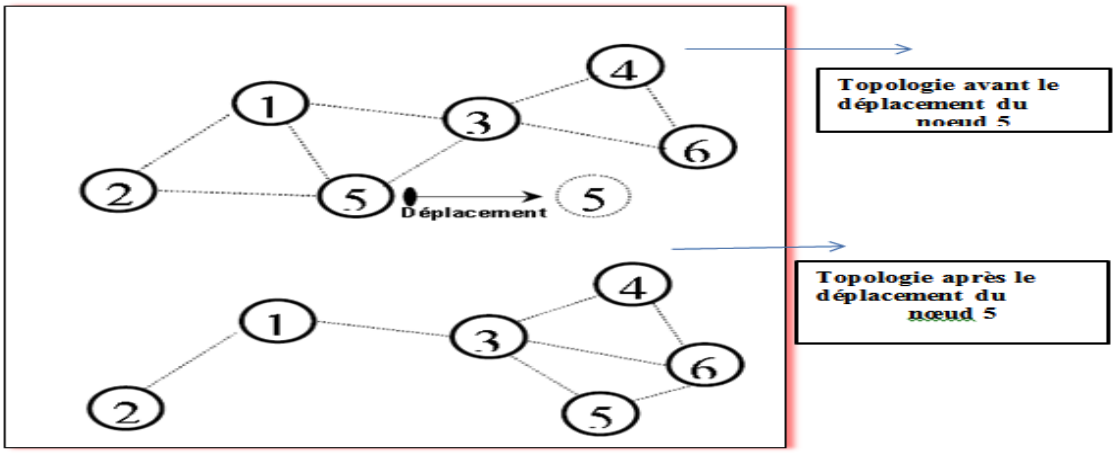

FIGURE 1.3 – Changement de la topologie d'un réseau ad hoc

• **Canal de communication sans fil :** nous savons que les liaisons sans fil auront toujours une capacité inférieure à des liaisons filaires. La bande passante est moins importante, et en plus ,le débit est confronté aux effets multiples d'interférences, du bruit ...etc

• **Ressources limitées :** les sources d'énergie telles, que les batteries sont nécessaires pour la

communication des nœuds mobiles. Malheureusement, ces sources d'énergie ont une durée de vie limitée et leur épuisement dépend des traitement effectués au niveau du nœud ,telles que les opérations de transmission, réception et les calculs complexes,etc...Par conséquent, la consommation d'énergie constitue unvéritable problème.
Les mécanismes de gestion d'énergie sont nécessaires pour les nœuds ,dans le but de conserver l'énergie et d'augmenter leur durée de vie. Donc, n'importe quelle solution destinée aux réseaux mobiles Ad hoc doit prendre en compte la contrainte de l'énergie.

• **Taille du réseau :** Dans le réseau mobile Ad hoc, la portée de transmission des nœuds est petite ou moyenne (environ 250 mètres). Cela a un impact sur la couverture du réseau (la taille du réseau est de quelques centaines de nœuds) [6].
C'est pourquoi le réseau est utilisé dans certains cas pour étendre temporairement un réseau filaire dans un environnement où le déploiement du réseau filaire n'est pas possible.

• **Nœuds cachés :** Ce phénomène est très particulier à l'environnement sans fil. Un exemple est illustré par la figure(1.4). Dans cet exemple, les nœuds **B** et **C** ne s'entendent pas, à cause d'un obstacle qui empêche la propagation des ondes. Les mécanismes d'accès au canal, vont permettre, alors à ces nœuds, de commencer leurs émissions simultanément. Ce qui provoque des collisions au niveau du nœud **A**.

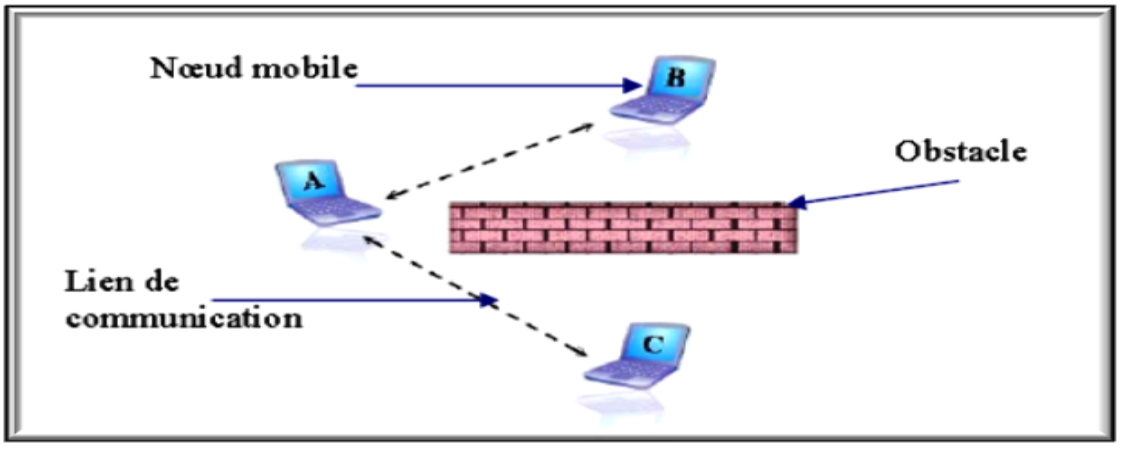

FIGURE 1.4 – Station caché

• **Vulnérabilité aux différentes attaques :** les réseaux mobiles Ad hoc sont des réseaux qui héritent des mêmes vulnérabilités que les réseaux sans fil classiques, et sont en plus, sensibles à d'autres menaces liées à leurs propres caractéristiques.

1.3.3 Types de réseau AD hoc

Les réseaux Ad hoc sont divers, nous pouvons en citer quelques uns [7] :

• **Les réseaux personnels :**

PAN (Personal Area Network) désigne un réseau restreint d'équipements informatiques habituellement utilisés dans le cadre d'une utilisation personnelle. Parmi les technologies sans fil utilisées par les réseaux PAN, nous pouvons citer le Bluetooth, l'infrarouge (IR), ou le zigbee (la technologie802.15.4).

• **Les réseaux de capteurs :**

Ce sont des réseaux composés de nœuds ,intégrant une unité de mesure chargée de capter des grandeurs physiques (chaleur, humidité, vibrations)et de les transformer en grandeurs numériques, une unité de traitement informatique de stockage de données et un module de transmission sans fil (Wireless).

• **Les réseaux de voitures :**

Les voitures de nos jours embarquent de plus en plus de technologie, et ont de plus en plus, besoin de communiquer avec l'extérieur. Les voitures équipées par des capteurs sur les toits et/ou, les parechocs sont capables de créer des plateformes des réseaux mobiles Ad hoc et de relier en réseau, les automobiles passant à proximité les unes des autres [8]. Des prototypes ont déjà été développés pour les véhicules d'urgence (les ambulances, les voitures des pompiers,... etc).

1.4 Applications des réseaux Ad hoc

Les réseaux ad hoc sont utilisés dans toutes les applications où le déploiement d'une architecture centralisée est contraignant, voire impossible. En effet, la robustesse, le coût réduit et le déploiement rapide qu'ils présentent, leur confèrent un accès à une large palette d'applications dont :

- **Applications militaires :**

Les réseaux ad hoc ont été utilisés 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 unités d'une armée [9].

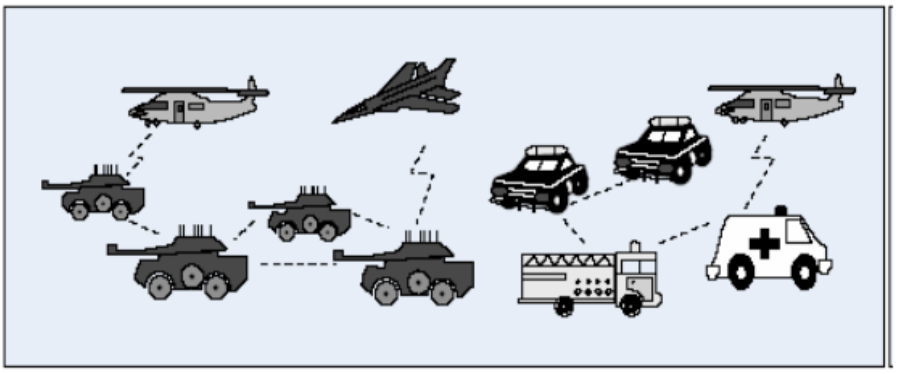

FIGURE 1.5 – Champs de bataille

- **Les opérations de secours :**

Dans les zones touchées par les catastrophes naturelles cyclones, séismes, etc.., le déploiement d'un réseau ad hoc figure(1.6) est indispensable, pour permettre aux unités de secours de communiquer.

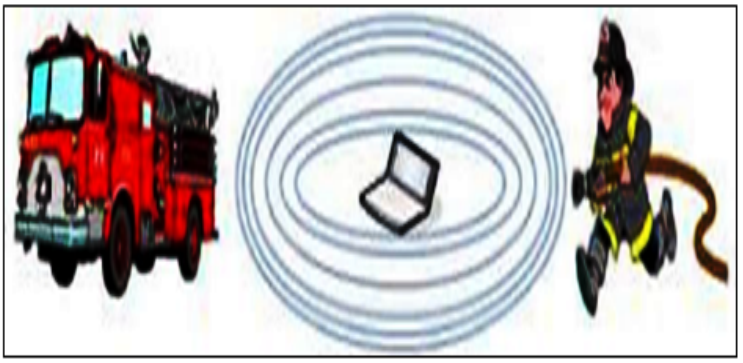

FIGURE 1.6 – Les opération de secours

- **L'utilisation à des fins éducatives**

Le déploiement d'un réseau ad hoc lors d'une conférence, ou d'une séance en cours, est très judicieux, car cela permet aux chercheurs et étudiants, de partager des ressources (fichiers, accès à internet. . .etc.) et de communiquer sans avoir besoin d'une quelconque infrastructure.

- **Applications industrielles :**

Des scénarios plus complexes dans le domaine industriel appelés réseaux de capteurs (Sensor Networks), peuvent former un MANET pour s'adapter à différents environnements. Un exemple, d'une telle Application, est la formation d'un MANET pour la surveillance médicale, la détection des Feux de forêt, la surveillance des volcans. . .etc.

- **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 de réguler le trafic routier. Les réseaux ad hoc sont alors, la solution idéale.

- **Applications commerciales :**

pour un paiement électronique distant (taxi) ou pour l'accès mobile à Internet.(voir la figure 1.7)

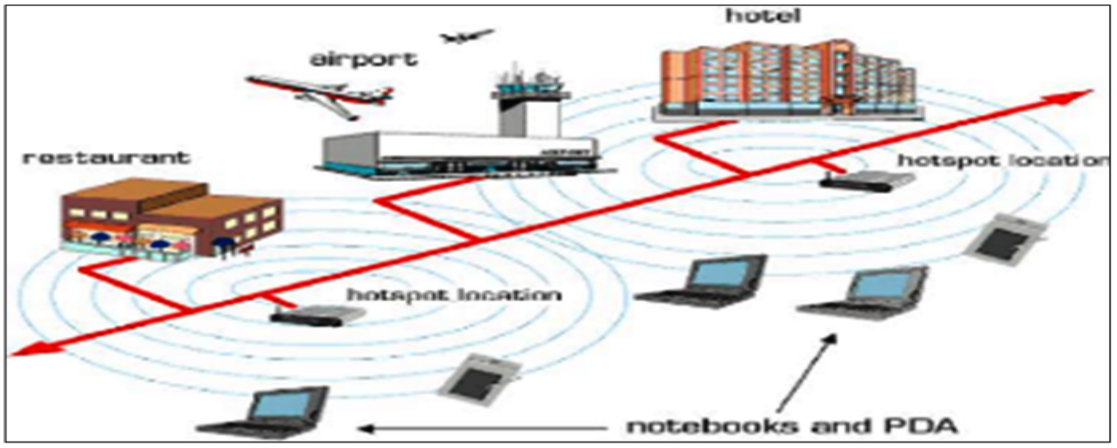

FIGURE 1.7 – Applications commerciales mode Ad Hoc

1.5 Avantages et inconvénients des réseaux Ad Hoc

1.5.1 Avantages des réseaux Ad Hoc

- **Faciles à déployer :** il suffit de mettre en place plusieurs machines ,pour que le réseau existe. Ceci rend la construction d'un réseau Ad Hoc, plus rapide.
- **Les nœuds sont mobiles :** l'absence de câblages autorise les nœuds à se déplacer l'un par rapport aux autres, au cours du temps.
- **Évolutifs :** pour ajouter un nœud à un réseau AD HOC préexistant, il suffit d'approcher le nouveau venu ,d'au moins l'un des membres du réseau. De même ,il suffit de l'en éloigner pour le retirer du réseau.

1.5.2 Inconvénients des réseaux Ad Hoc

- **Une bande passante limitée :** une des caractéristiques primordiales des réseaux basés sur la communication sans fil , est l'utilisation d'un médium de communication partagé. Ce partage fait que la bande passante réservée à un hôte soit modeste [10].
- **Des contraintes d'énergie :** les hôtes mobiles ,sont alimentés par des sources d'énergie autonomes ,donc restreintes, comme les batteries ; par conséquent la durée de traitement est réduite ;Donc le paramètre d'énergie doit être pris en considération dans tout contrôle fait par le système.
- **Une sécurité physique limitée :** les réseaux mobiles AD HOC sont plus touchés par le paramètre de sécurité, que les réseaux filaires classiques. Cela se justifie ,entre autres, par les vulnérabilités des liens radio aux attaques, ainsi que les contraintes et limitations physiques ,qui font que ,le contrôle des données transférées doit être minimisé.

Modes de communications dans les réseaux Ad Hoc : Avant de parler des protocoles de routage propremententss dit, nous allons rappeler quels sont les principaux modes de communications dans les réseaux ,et particulièrement dans les réseaux Ad hoc :

◇**la communication ,point à point ou unicast :** pour laquelle il y a une source et une seule destination.

◇**la communication multipoints ou multicasts :** permet d'envoyer un message à plusieurs destinataires.

◇**la diffusion ou broadcast :** envoie un message à tous les nœuds du réseau.

Ces trois modes de communication sont schématisés par la figure suivante :

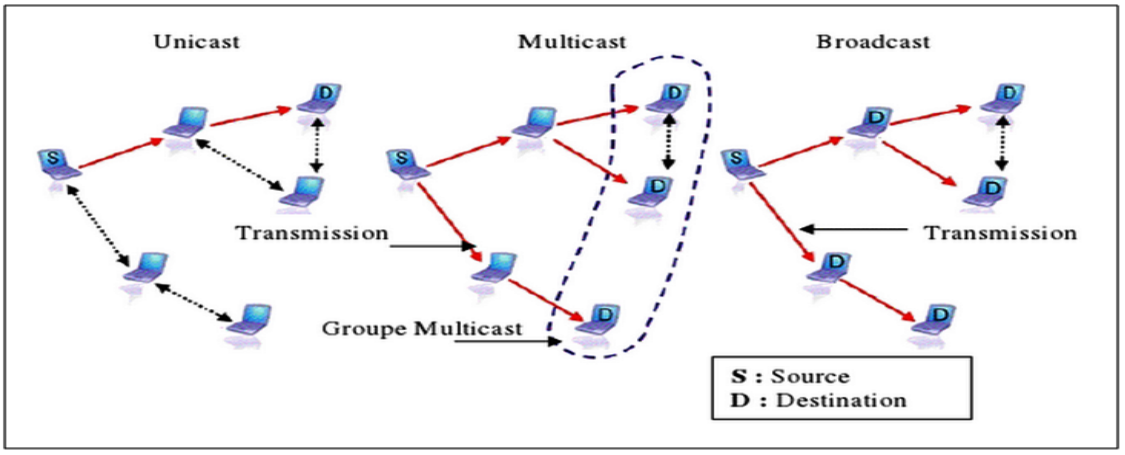

FIGURE 1.8 – communication des réseaux ad hoc

1.6 Routage dans les réseaux ad hoc

Le routage est une méthode d'acheminement des informations vers la bonne Destination, à travers un réseau de connexion donnée. Il consiste, à assurer une stratégie qui garantit, à n'importe quel moment, un établissement de routes qui soient correctes et optimales ,entre n'importe quelle paire de nœuds appartenant au réseau ;Ce qui assure l'échange des messages d'une manière continue.
Le routage est donc, la brique technologique de base des réseaux sans fil Ad Hoc.
Il constitue un sérieux problème à résoudre, pour que ces réseaux puissent fonctionner dans des bonnes conditions.

1.6.1 Classification des protocoles de routage :

Suivant la manière de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent être séparés en :

- Proactifs.
- Réactifs.
- Hybrides.

De nombreux protocoles et algorithmes ont été proposés pour rendre la communication dans les réseaux ad hoc plus efficace. leurs performances, ont été analysées dans différentes situations.

1.6.2 Les protocoles de routage proactifs :

Un protocole proactif est un protocole qui construit les tables de routage avant que la demande en soit effectuée. Il identifie en fait à chaque instant la topologie du réseau.
Parmi ces protocoles, on présente les deux exemplaires :**DSDV+** et **QOSLR**.

Le protocole DSDV+ : C'est un protocole de routage avec La Qualité de Service (QoS) et réservation de ressources, fondé sur DSDV [11] ;Il est basé sur la méthode d'accès au niveau MAC TDMA (Time Division Multiple Access) qui permet le calcul de la Bande Passante.

Le protocole QOSLR : QOLSR est un protocole de routage , proactif basé sur le protocole OLSR [12]. Ce dernier propose d'avoir des messages de contrôle réduit et de minimiser l'inondation du trafic de contrôle. Pour réduire cette inondation, on utilise le concept des Relais Multipoints.

1.6.3 Les protocoles réactifs :

Un protocole réactif est un protocole qui construit une table de routage lorsqu'un nœud en effectue la demande. Il ne connaît pas la topologie du réseau, il détermine le chemin à prendre pour accéder à un nœud du réseau lorsqu'on lui demande. on présente comme un exemple les protocoles réactifs **CEDAR** et **BRuiT**.

Le protocole CEDAR : CEDAR [13] Il repose sur l'élection dynamique par les nœuds d'un cœur de réseau stable approxime un ensemble dominant minimum. Le processus distribue d'élection de ces nœuds est local et dynamique [14].

Le protocole BRuiT : Les routes sont construites à la demande, et les tables de routage ne contiennent que des routes actives, et non des routes vers tous les mobiles du réseau, comme c'est le cas avec les protocoles proactifs. Cependant, comme nous l'avons signalé, BRuIT[15] intégré également de la qualité de service, garantissant, sur demande des applications, une communication à un débit donné entre deux nœuds.

1.6.4 Les protocoles hybrides :

Dans ce type de protocole, on peut garder la connaissance locale de la topologie jusqu'à une certaine distance (nombre prédéfini de sauts) par un échange périodique de trame de contrôle, autrement dit par une technique proactive. Les routes vers des nœuds plus lointains sont obtenues par schéma réactif, c'est-à-dire par l'utilisation de paquets de requête en diffusion [16]. Avec ce système, on dispose immédiatement des routes dans notre voisinage proche, et lorsque la recherche doit être étendue plus loin, elle en est optimisée.

Le protocole ZRP « Zone Routing Protocol »

ZRP [16] est un protocole de routage dit hybride. Il met en place, simultanément, un routage proactif et un routage réactif, afin de combiner les avantages des deux approches. Pour ce faire, il passe par un concept de découpage du réseau en différentes zones, appelées "zones de routage". Une zone de routage pour un nœud S, est définie par son "rayon de zone". Ce rayon correspond au nombre de sauts maximum qu'il peut y avoir entre un nœud D et le nœud S.

1.7 Conclusion

Ce chapitre a été consacré à la description générale des réseaux ad :hoc ,qui représentent le grand avantage d'avoir une extrême souplesse grâce, à l'absence du câblage et d'une infrastructure fixe, et par sa facilité de déploiement ,son coût réduit. Cependant, les caractéristiques des réseaux ad hoc soulèvent des nouvelles problématiques qui sont spécifiques à ce type de réseau. Afin de satisfaire les besoins de toutes ces applications, de nouvelles fonctionnalités doivent être réalisées, plus particulièrement, au niveau du routage de données et de la sécurité du routage. En effet, l'absence d'une infrastructure centralisée, fait du routage dans les réseaux ad hoc un problème très compliqué.

Chapitre 2

Sécurité dans les Réseaux Ad hoc

2.1 Introduction

Aujourd'hui, les réseaux filaires peuvent assurer, un niveau de sécurité très élevé. Mais dans les réseaux sans fil, en particulier les réseaux ad hoc, les défauts 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 MANETs. Dans ce chapitre, nous énumérons ces vulnérabilités induites, ainsi que les attaques possibles et leurs solutions.

2.2 Définition de la sécurité

La sécurité est la situation dans laquelle un système informatique, connecté ou non à un réseau externe de télécommunications, est protégé des dangers internes ou externes, en d'autres termes la sécurité informatique [17] est un ensemble de techniques assurant que les ressources (matérielles ou logicielles) d'un système d'information d'une organisation donnée, sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient.

2.3 Vulnérabilité des réseaux Ad Hoc

• Les réseaux Ad Hoc présentent quelques faiblesses. Certaines faiblesses sont liées à la technologie sans fil, d'autres aux caractéristiques de ces réseaux.

• La première vulnérabilité de ces réseaux est liée à la technologie sans fil sous. En effet, l'utilisation d'un canal radio favorise l'écoute et la perturbation des messages échangés par tout nœud possédant le

récepteur adéquat même s'il se trouve dans un lieu public, à l'extérieur du bâtiment où se déroulent les échanges.

• Les nœuds sont aussi des points de vulnérabilité du réseau. En effet, un attaquant peut compromettre un terminal laissé sans surveillance.

•L'absence d'infrastructure fixe est une autre faiblesse des réseaux Ad Hoc, car elle rend impossible l'utilisation d'une entité centrale pour la gestion des accès aux ressources du réseau.

• De même, la capacité limitée des nœuds en puissance de calcul et énergie consommée, empêche l'utilisation des mécanismes cryptographiques résistants, comme la cryptographie à clef publique.

2.4 Objectif de la sécurité

Les principaux objectifs ou services de la sécurité sont :

◇**Confidentialité :** La confidentialité empêche les données d'être consultées par des entités nonautorisées. Des contrôles d'accès strict, doivent être mis en place, pour garantir la confidentialité des données dans les réseaux ad hoc. Étant donné que lescommunications sans fil transitent via les airs, 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. [18]

◇**Authentification de l'origine des données :**Dans un réseau, un adversaire peut facilement injecter des paquets additionnels, ainsi le récepteur doit s'assurer que les données reçues proviennent effectivement de la source supposée.

◇**Disponibilité :**Le principe de la disponibilité [19], permet de s'assurer que les services réseau désirés sont toujours disponibles même à la présence des attaques.

◇**Non répudiation de l'origine :**C'est un mécanisme destiné à prévenir, que la source ou la

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

2.5 Mécanisme de la sécurité

2.5.1 La Cryptographie

La cryptographie est la science d'écriture et de lecture de messages codés. En effet, elle joue un rôle essentiel dans toutes les communications sécurisée en chiffrant un message dit **" texte clair "** en un deuxième dit**" texte crypté "**, à l'aide d'une clé en utilisant des moyens matériels ou logiciels conçus à cet effet. Les informations originales sont restituées à partir de celles codées. Cette opération inverse est nommée décryptage voir la figure (2.1). En d'autres termes, la cryptographie est un traitement fait sur une donnée qui sera transmise à un destinataire, à travers un canal peu sur en présence d'adversaire , 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.

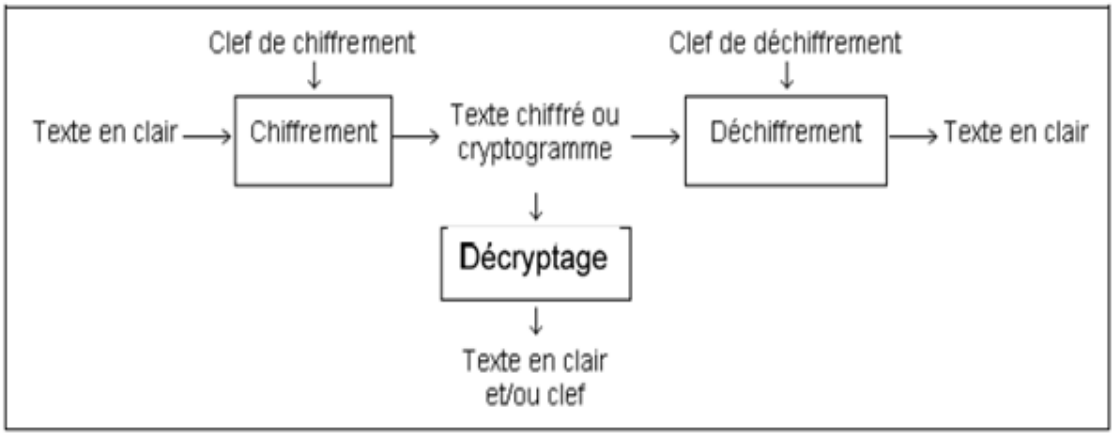

FIGURE 2.1 – Cryptographie

– **Chiffrement symétrique**

Dans la cryptographie conventionnelle figure (2.2), 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.

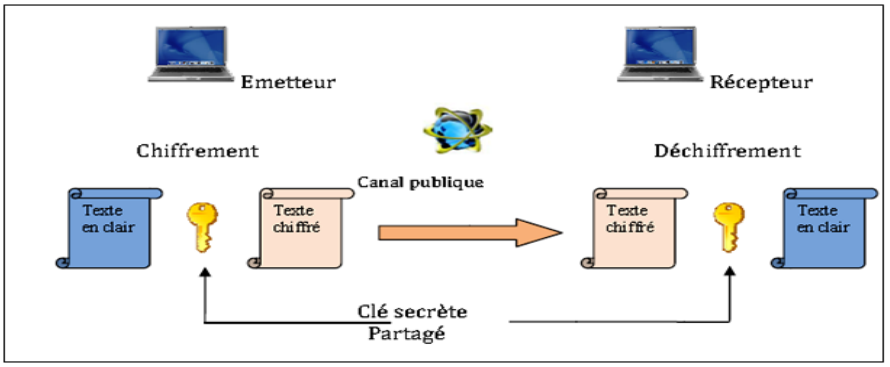

FIGURE 2.2 – Cryptographie symétrique

– **Chiffrement asymétrique**

Le concept de cryptographie à clef publique figure, [19] fut inventé par Whitfield Diffie et Martin Hellman en 1976, afin de résoudre le problème de distribution des clefs, posé par la cryptographie à clef secrète.

La cryptographie asymétrique(ou cryptographie à clé publique) : elle repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le message et l'autre de le décoder.

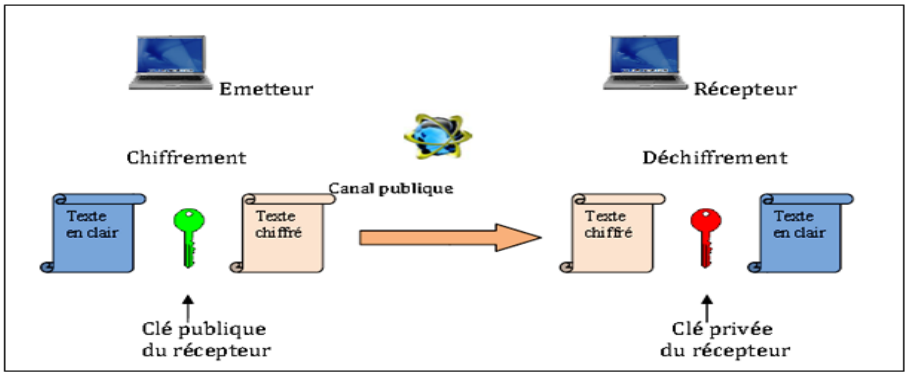

FIGURE 2.3 – Cryptographie asymétrique

2.5.2 Fonction de hachage

Une fonction de hachage est une fonction qui convertit un grand ensemble en un ensemble plus petit. Cette propriété fait que ce type de fonction est très utilisé en informatique, en particulier pour accéder rapidement à des données grâce aux tables de hachage. En effet, une fonction de hachage, permet d'associer à une chaîne de caractères un entier particulier. Ainsi, si nous connaissons l'empreinte des chaînes de caractères stockées, nous pouvons rapidement vérifier si une chaîne se trouve ou non dans cette table. Le résultat de cette fonction est par ailleurs aussi appelé somme de contrôle, empreinte, résumé de message, condensé, etc.

◇**Les fonctions de hachage à sens unique :**

une fonction de hachage à sens unique, est une fonction irréversible, qui fournit l'empreinte à partir d'une chaine fournie en entrée. La particularité de cette fonction est qu'il, est aisé de calculer l'empreinte d'une chaîne donnée, mais il est difficile de retrouver ou déduire la chaîne initiale à partir de l'empreinte [20].

2.5.3 La signature numérique

La signature numérique est définie comme des " données ajoutées à un message ", ou transformation cryptographique d'un message, permettant à un destinataire 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), assuré alors la non répudiation.

La signature électronique est basée sur l'utilisation conjointe d'une fonction dehachage, et de la cryptographie asymétrique.

◇**Étapes de signature d'un message :** 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 électronique qu'il appose au message original, avant d'émettre l'ensemble, message et signature, sur le réseau.

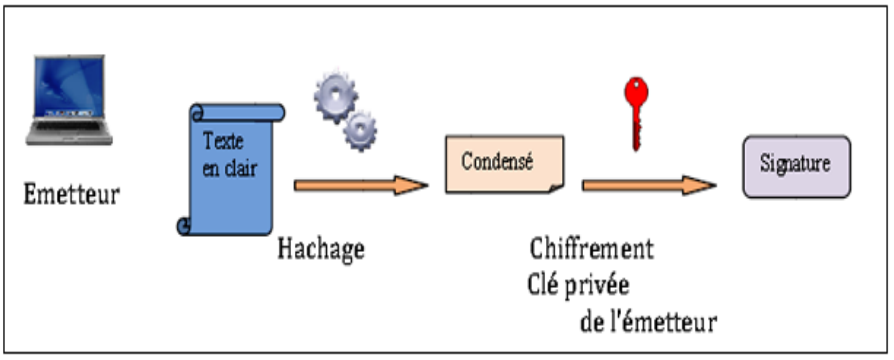

FIGURE 2.4 – Signature d'un message

◇**Etapes de vérification :** Pour vérifier la signature on passe par trois étapes :

1. Déchiffrement du condensé de message : le condensé est déchiffré avec la clé publique de l'émetteur.

2. Evaluation des condensés : le hachage est un processus unidirectionnel, il est impossible de trouver le message d'origine à partir de condensé, le destinataire doit réévaluer le condensé en utilisant le même algorithme de hachage que 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 de 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.[21]

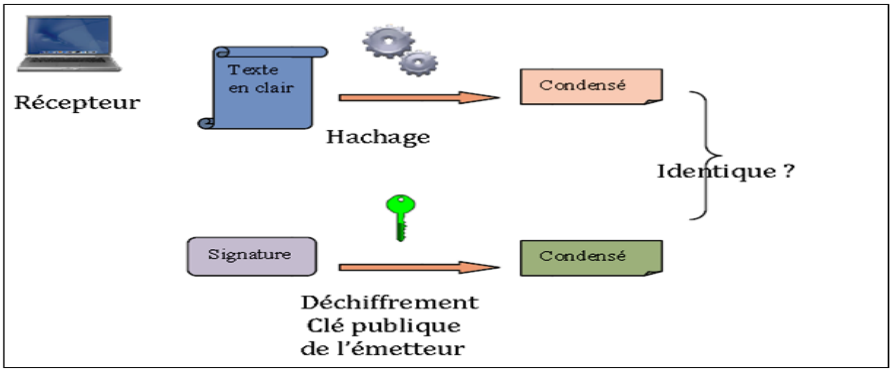

FIGURE 2.5 – vérification de la signature d'un message

2.5.4 Certificats électroniques

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 sécuritaire par un tiers de confiance appelé autorité de certification (Certificate Authority, ou 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 (ou du propriétaire).
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.
◇Le nom du propriétaire du certificat.
◇Le propriétaire du certificat.
◇La clé publique du propriétaire.

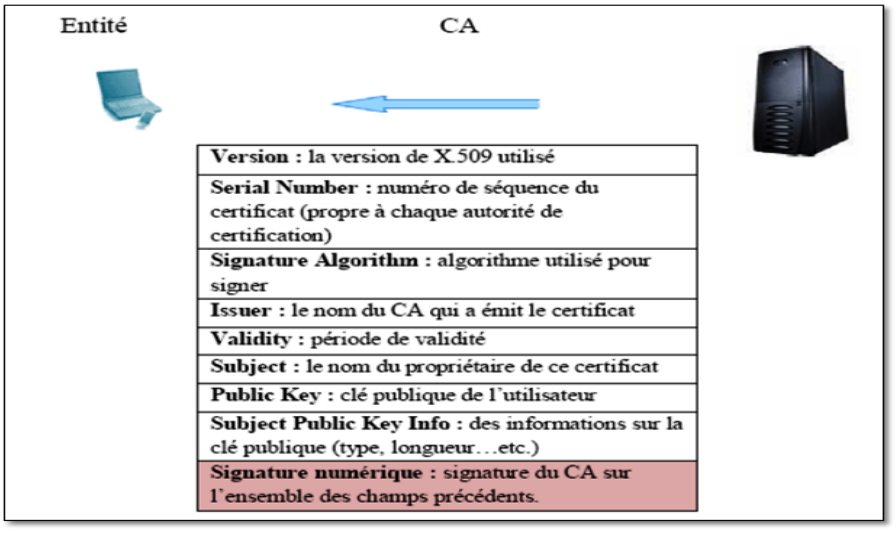

FIGURE 2.6 – Contenu d'un certificat

◇**Vérification du certificat :**

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. [21]

2.6 Classification des attaques dans les réseaux ad hoc

les attaques sont classifiées selon plusieurs critères :

◇**Attaque interne ou externe :**

Si l'attaquant ou le nœud malicieux, se trouve dans le réseau, on parle d'une attaque interne, dans le cas ou le nœud malicieux se connecte depuis l'extérieur, on dira que l'attaque est externe.

◇**Attaque passive ou active :**

Dans le cas d'une attaque active, le nœud essaie d'altérer le message envoyé, d'un nœud à un autre dans le but, de modifier le protocole ; ici l'intégrité du message n'est pas protégée. Par contre, une attaque passive prive le réseau de la confidentialité des messages échangés.

◇**Attaque individuelle ou attaque distribuée :**

Dans l'attaque individuelle, une seule entité est utilisée, par contre il existe des attaques qui utilisent plusieurs nœuds c'est ce qu'on appelle attaque distribuée, ce genre d'attaques est plus dangereux et difficile à détecter.

2.7 Types d'attaques dans les réseaux ad hoc

2.7.1 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 :[22]

◇**Sybil attack :** 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. [22]

◇**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 [23]

◇**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.

2.7.2 Modification, suppression et insertion des messages

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

◇**Black hole attack :** 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.[23][24].

◇**Attaque Grayhole :** 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 [25].

◇**Attaque Rushing :** L'attaque Rushing [26] concerne les protocoles de routage 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 routage réactifs, les auteurs proposent des mécanismes de contrôle pour minimiser le coût de découverte de route, selon lesquels les noeuds intermédiaires rediffusent seulement les paquets de contrôle (les paquets RREQ)arrivant en premier, et éliminent tous les autres exemplaires de ce paquet arrivant ultérieurement.

2.7.3 Replay ou rejeu

Un nœud malicieux réinjecte des messages dans le réseau. Desanciens messages continuent à circuler ce qui occupe de la bande passante et peutmême affecter la justesse de la topologie.

◇**Wormhole attack :** Dans une attaque 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. [26].

2.7.4 Dénis de services (DoS) :

Cette classe d'attaque inclut toutes attaques touchant 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 devient 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 peut ne pas bien travailler ou ne pas fonctionner du tout.

2.8 Protection du protocole de routage 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.

Dans la littérature, il existe plusieurs protocoles de routage, sécurisés par l'ajout d'une signature dans les paquets de contrôle :
pour exemple SRP, SLSP, SAODV, ARAN, SEAD.

◇**ARAN (Authenticated Routing for Ad hoc Networks) :** Sanzgiri et al. ont proposé le protocole sécurisé ARAN [27] 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 grand nombre des opérations de signature et de vérifications de signature utilisées pour assurer la sécurité.

◇**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, DSA), 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 " Secure Efficient Ad hoc Distance vector routing protocol "** [29] est un protocole proactif de routage ad hoc sécurisé, basé sur DSDV qui 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 en nombre de sauts 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. 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 noeud peut facilement les falsifier, les rejouer, les modifier ou simplement les détruire.

◇**SLSP "Secure Link State Protocol " :** Papadimitratos et Haas proposent SLSP [30], 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 lecompteur 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 pourraientforger des métriques erronées ou même de créer des tunnels.

2.9 Conclusion

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

Dans un réseau ad hoc, tous les nœuds doivent participer aux opérations de routage. Ils gèrent entre autre l'établissement des chemins, la dissémination de notifications deruptures de chemins et la retransmission des données. Etant donné cette caractéristique, il devient relativement facile, pour un nœud malveillant, de mener divers types d'attaques, rendant ainsi le réseau inopérant.

Qu'il s'agisse de nœuds malveillants internes ou bien de nœuds normaux compromis par un attaquant au cours de l'exploitation du réseau. Ces nœuds déviants sont particulièrement difficiles à contenir.

Chapitre 3

Attaque worhole dans les reseux Ad Hoc

3.1 Introduction

Des attaques de vers dans les réseaux ad hoc , ont attiré beaucoup d'attention au cours de ces années. Ce sont des événements graves, impliquant deux nœuds malveillants a transitant à traves un tunnel , d'un bout d'un réseau à l'autre. Plusieurs approches ont été proposées pour détecter ces attaques, mais seulement quelques solutions : exploiter les informations fournies par les systèmes de routage multi-trajets.

Dans ce chapitre, nous présentons quelque type attaque de trou de ver dans les protocoles de routage, et des solutions les plus importantes proposées pour contrer des attaques de vers, comme ainsi ,que d'une nouvelle approche pour les détecter.

3.2 Description de wormhole

Le trou de ver est une attaque qui se produit généralement par deux nœuds malveillants par l'intermédiaire d'une connexion hors bande, dans lequel le premier adversaire ,reçoit ou intercepte des paquets puis les transmèttrent via un tunnel au prochain adversaire qui se trouve dans un autre point de réseau par le biais d'un directionnel à grande distance liaison sans fil ou même en utilisant liaison filaire directe [31]. Ainsi, il peut simplement convaincre ces deux nœuds séparés qu'ils sont voisins en envoyant des paquets entre les deux entre eux.

D'autre part, un adversaire à l'aide de cette attaque pourrait convaincre les nœuds qui sont situés à plusieurs sauts, à partir d'une station de base qui sont seulement un ou deux sauts de là. Si un attaquant est situé près de la station de base, il peut interrompre le routage en faisant un bien placé trou de ver

complètement [32].

Exemple suivant dans la figure 3.1 illustre le fonctionnement, le nœud de source (S) envoie des paquets à destination ,par la voie normale (SBCE-D), mais également ces paquets sont écoutés par le premier nœud malveillant (W1), puis un tunnel à la seconde malveillant nœud (W2). Enfin, W2 les transmet au nœud de destination (D) avant qu'ils ne soient arrivés à D de la voie normale.

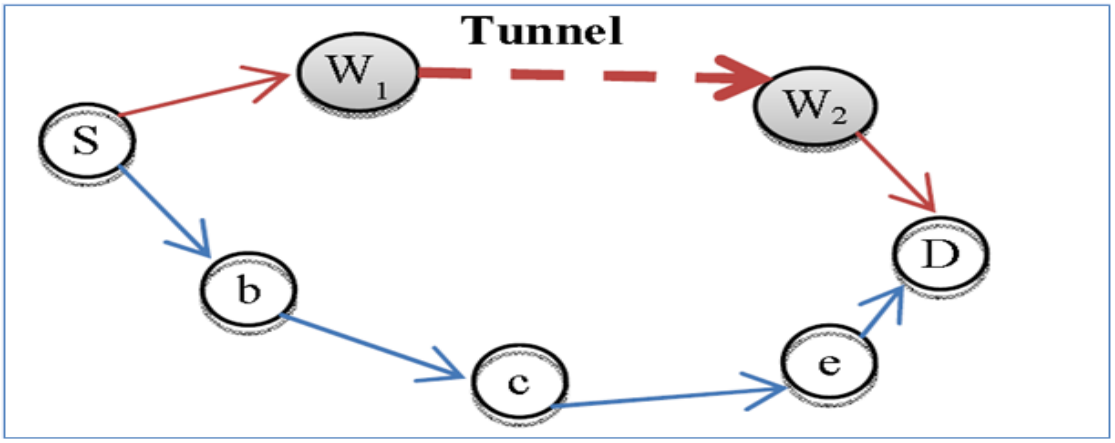

FIGURE 3.1 – Attaque Wormhole

Les attaques de trou vers sont capables d'être créés dans les réseaux sans fil ad hoc, en utilisant au moins l'une des méthodes suivantes :

Le premier type de trou de ver se produit ,lorsque les nœuds malicieux sont statiques. Dans cette situation, au moins un nœud malveillant est situé à l'intérieur de l'itinéraire de la source à la destination. Ce type d'attaque est nommé wormhole statique.

Un autre type de cette attaque est wormhole mobile.les nœuds malveillants ne sont pas déployés dans la voie de la destination. Ainsi, un de ces nœuds seront situées dans le chemin de déplacement et entendant les paquets de données et leur traitement pour des informations de routage [33]. L'identification de trou ver dynamique, est si difficile et, il n'est pas facile de concevoir un procédé pour empêcher les deux en même temps.

Ce type d'attaque peut-être apparu dans l'autre type, dans lequel ,un attaquant d'experts peut créer son propre réseau virtuel jusqu'à ce que la nouvelle voie créée par l'attaquant ,contient le même nombre de sauts que de l'itinéraire initial.

3.3 Types d'attaques trou de ver

Wormhole attaquants peuvent utiliser deux différentes techniques de communication pour effectuer leur attaque [34] : Un canal d'encapsulation et un canal out-of-band.

◇Wormhole par un canal encapsulation

Dans ce mode d'attaque, le tunnel est réalisé par encapsulation de sorte que les champs du paquet encapsulé ne seront pas modifiés au cours de son acheminement.

Considérons la figure 3.2, dans laquelle la source S veut découvrir le chemin le plus court vers le nœud D. S diffuse alors un paquet RREQ. le nœud malicieux M2 reçoit le paquet RREQ, première extrémité du tunnel, l'encapsule dans un nouveau paquet destiné à M1 et l'envoie à travers le tunnel.

Le nœud M1, deuxième extrémité du tunnel, décapsule le paquet reçu, extrait le paquet RREQ et diffuse ce dernier à ses voisins en particulier D. Simultanément le paquet RREQ va traverser A-B-C pour atteindre D. Le destinataire D reçoit donc deux paquets RREQ.

Le premier venant de M1 avec saut count égal à trois comme s'il avait traversé uniquement M2 et M1, alors qu'en réalité il a traversé sept sauts S-M2-E-F-G-H-M1-D. Le deuxième venant de C avec un saut count égal à quatre. D choisit alors le chemin le plus court soit celui à travers M1. De cette façon, l'intrus peut contrôler tout le trafic.

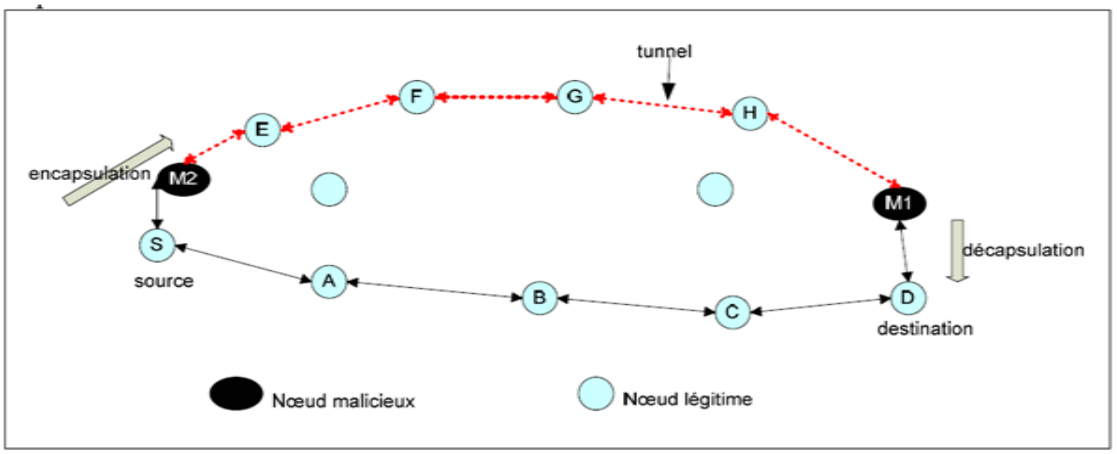

FIGURE 3.2 – Wormhole par encapsulation

◇Wormhole utilisant Out-of-Band Canal

Ce mode d'attaque est lancée par trou de ver ayant un canal à bande passante élevée out-of-band entre les nœuds malveillants. Ce canal peut être réalisé, par exemple, en utilisant une liaison sans fil directionnel longue portée, ou une liaison filaire directe. Ce mode d'attaque est plus difficile de lancer que la précédente, car elle a besoin de se spécialisée dans la capacité du matériel. Considérez le scénario décrit dans la figure (3.3).

Le Nœud A envoie une requête de route vers le nœud B, et les nœuds X et Y sont des nœuds malveillants ayant un canal hors bande entre eux. Nœud X exploite le tunnel de la demande d'itinéraire à Y, qui est un voisin légitime de B. Nœud Y diffuse le paquet pour ses voisins, Y compris B. B obtient deux parcours demande-A - X - Y - B et A - C - D - E - F - B. Le premier est à la fois plus court et plus rapide que le second, et est donc choisi par B.

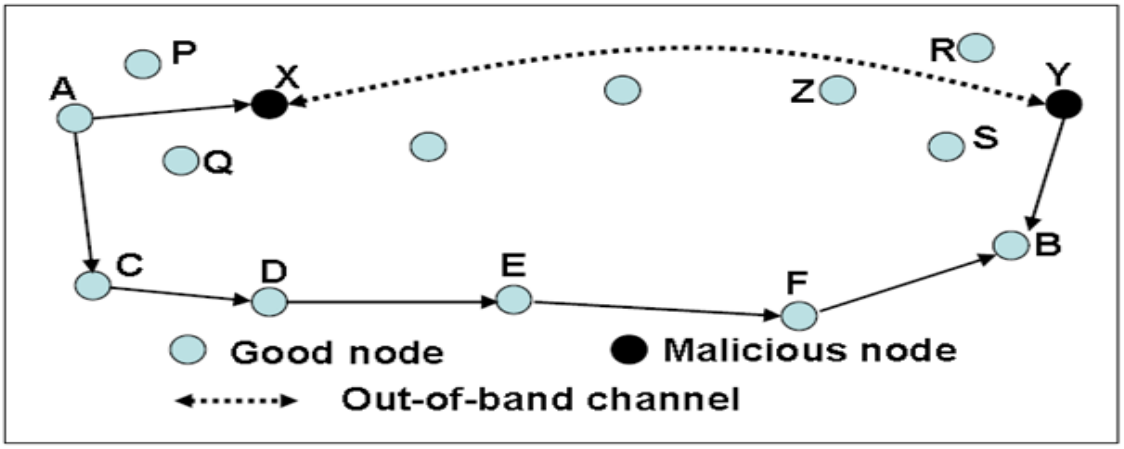

FIGURE 3.3 – WORMHOLE DANS canal à bande passante élevée

◇Wormhole utilisant respect du protocole

Certains protocoles de routage, tels que ARAN [35], choisir l'itinéraire du plus court délai, de préférence à l'une, avec la plus courte nombre de sauts. Pendant la transmission de demande de route.

Ceci est motivé par le fait, que la transmission de la demande est effectuée par radiodiffusion et, par conséquent, de réduire les collisions couche MAC est important. Un nœud malveillant peut créer un trou de ver par ce qu'il n'est simplement pas conforme au protocole et à la diffusion sans reculer.

Le but de l'adversaire, est de laisser la demande paquet qu'elle arrive à l'avant-première à la destination, augmentant ainsi les chances d'être inclus dans le chemin. C'est une forme particulière de l'attaque au sol décrit dans [36].

◇**Wormhole utilisant Packet Relay**

Dans ce mode d'attaque trou de ver, un nœud malicieux, relaie les paquets entre deux nœuds distants pour convaincre qu'ils sont voisins. Il peut être lancé par un seul nœud malveillant. Coopération par un plus grand nombre de nœuds malveillants sert à élargir la liste de voisins d'un nœud de victime à plusieurs sauts.

Par exemple, supposons que le nœud A et le nœud B soient deux nœuds non voisins avec un nœud voisin malveillant X. Nœud X peut relayer les paquets entre nœuds A et B, afin de leur donner l'illusion qu'ils sont voisins.

3.4 Wormhole dans le protocole OLSR

L'attaque trou de ver peut fortement influencer la construction topologie ; elle peut être fatale pour les protocoles de routage, particulièrement proactives OLSR, que les paquets de contrôle des échanges pour Neighbor Discovery et la construction de la topologie.

La figure 3.4 représente un réseau Ad Hoc, y compris un tunnel trou de ver.

Lorsque le nœud A diffuse son message HELLO le nœud X (l'attaquant) copier ce message "HELLO" et l'envoie au nœud Y à travers le wormhole construit. Y reçoit l'HELLO message et replays dans son discours.

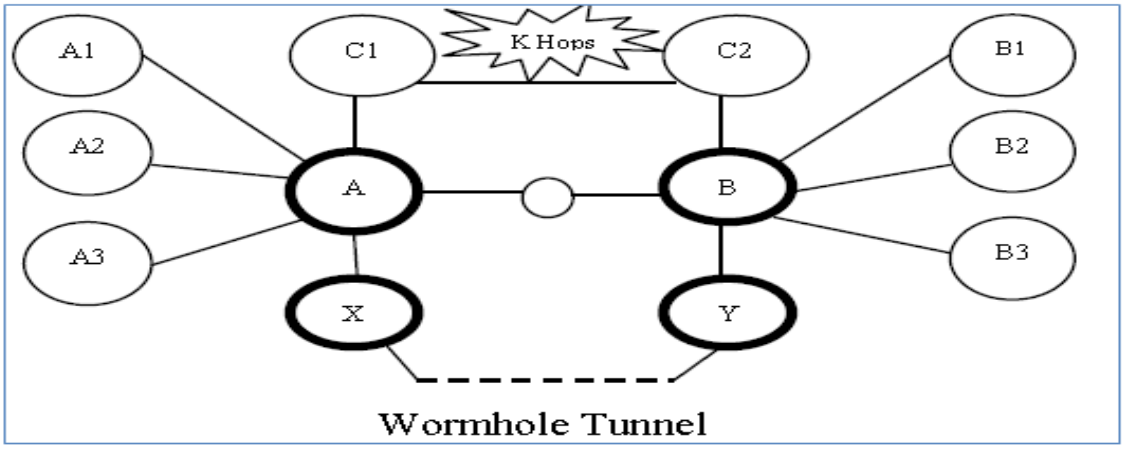

FIGURE 3.4 – Attaques de vers dans OLSR

Lorsque le nœud B reçoit le message rejoué, le nœud B considère le nœud A comme voisin 1 saut. Après un certain temps, une relation de symétrie peut être établie entre A et B dans le mécanisme du protocole OLSR. Une fois que ce lien est établi symétrique, A et B sont très susceptibles de choisir l'autre en tant que relais multipoints (MPR), ce qui conduit alors à un échange de messages de certaine topologies commande (TC) et des paquets de données à travers le tunnel vortex.

Dans notre exemple, de figure 3.4 B peuvent s'attendre les voisins à 1-saut de A, qui sont voisins de B à un 2-saut que la partie A. Par conséquent, B doit choisir A en tant que voisins MPR , attendre 1-saut de A, alors la transmission d'informations erronées, ce qui conduit à perturbation du routage et de la perte de connectivité.

3.5 Wormhole dans le protocole AODV

Attaque Wormhole dans AODV est un type d'attaque de relecture qui est particulièrement difficile dans MANET pour se défendre contre. Même si les informations de routage sont confidentielles, les cryptées ou authentifiées, il peut être très efficace et dommageable.

Dans les protocoles réactifs en particulier AODV, la route n'est construite, qu'à à la demande d'une application. Ainsi pour bien comprendre l'attaque dans ce cadre, il est nécessaire de voir réellement ces conséquences.

Voici le processus de lancement de cette attaque, illustré dans cette figure (3.5) :

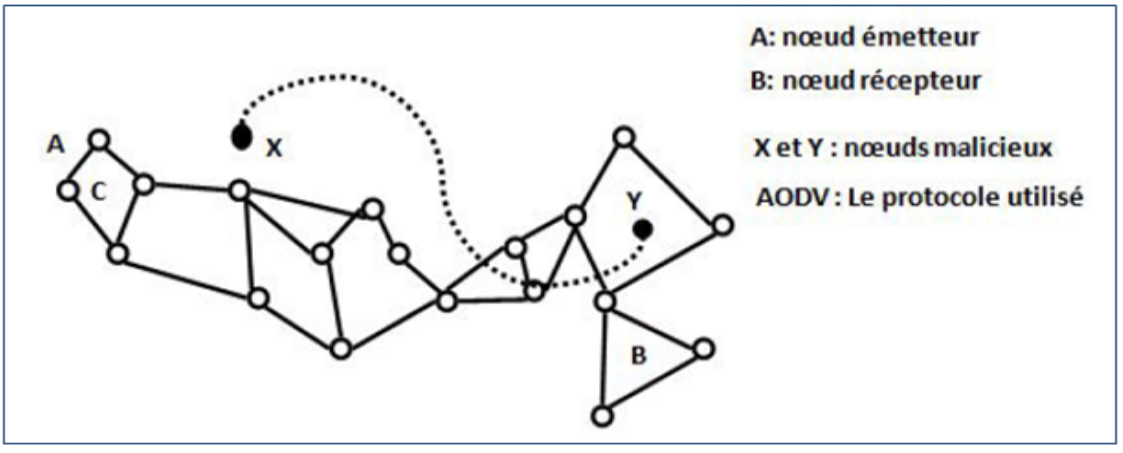

FIGURE 3.5 – Attaque wormhole dans AODV

1. Le nœud A diffuse une requête de découverte de la route RREQ (Route REQuest).

2. Le nœud X capte et retransmet directement cette requête au nœud Y, via le tunnel préétabli, le nœud

Y de son tour, diffuse le message RREQ.
3. Le nœud B, quand il reçoit la requête, répond à la source avec une 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 (Wormhole), après cela, ils peuvent lancer n'importe quel type d'attaque avec ce tunnel, (suppression sélective ou totale des paquets de données, l'attaque BlackHole, DoS,... etc.).

Une attaque trou de ver n'est pas si difficile à mettre en place, mais peut être extrêmement dangereuse pour un MANET. En outre, trouver de meilleures techniques pour la détection des attaques de vers et la sécurisation AODV contre eux, reste un grand défi dans les réseaux mobiles ad-hoc.

3.6 Solutions aux attaques de Wormhole

Nous allons présenter dans cette section, la majorité des solutions proposées dans la littérature pour contrer, l'attaque wormhole. Nous montrerons que la plupart de ces propositions sont inefficaces ou inadéquates, à cause de l'utilisation soit, d'un matériel dédié, soit parce qu'elles utilisent des informations coûteuses ou difficiles à obtenir.

3.6.1 Packet Leash Technique

De nombreuses méthodes ont été proposées à l'aide d'une Packet Leash Technique pour la détection de l'attaque wormhole.

Le **Packet Leash** [36] est la méthode qui défend contre l'attaque de trou ver . Les leash peuvent être regroupées soit géographiquement ou temporellement.

– **Geographical Leashes**

Une laisse géographique [37], est une méthode qui est mise en œuvre dans2003 par Hu pour protéger le réseau contre les attaques de trou ver .

Il est basé sur cette caractéristique que le récepteur du paquet ,est situé à une certaine distance de l'émetteur. Afin de mettre en œuvre laisse géographique dans les réseaux ad hoc, d'une part certaines exigences doivent être fournies, comme chaque nœud doit connaître sa propre localisation (par GPS), tous les nœuds doivent avoir les horloges synchronisées lâchement et la signature

numérique (RSA) dans Afin de vérifier l'authentification de la localisation et l'heure de 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 le en-tête 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 sont utilisés horloges synchronisées, si les horloges d'entre eux sont synchronisés à $\pm\alpha$, donc, une borne supérieure distance entre l'émetteur et le récepteur (DSR) est calculable par le récepteur .

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

en ce qui est la vitesse lumière, Ts est l'horodatage dans le paquet et ? est l'erreur maximale que peut-être survenu dans la recherche informations de localisation.

– **leash tomporelle** Dans cette méthode, tous les nœuds calculent l'expiration temps de chaque paquet en utilisant la vitesse de la lumière et ajoutez cette date d'expiration dans l'en-tête du paquet. La Destination compare son propre temps d'arrivée et l'heure d'expiration dans le paquet pour détecter l'attaque vortex (le trou de ver). Laisses géographiques sont plus avantageux que laisses temporelles, car ils ne nécessitent pas une bien horloge synchronisée. Il a les limites de la technologie GPS.

3.6.2 Temps-de-vol (Time-of-flight)

La technique de temps de vol est proposée pour se protéger contre l'attaque de wormhole. Cette dernière est semblable aux laisses temporelles [38]. Le principe de ces techniques est le suivant :

• Mesurer le temps de déplacement aller-retour (RTT : (Round Trip Travel Time) d'un message.

• Estimer la distance entre les nœuds, en se basant sur le temps de déplacement &.

• déterminer si la distance calculée d, est dans la marge de communication maximum possible.

Supposant que le signal sans fil voyage avec une vitesse égale à la vitesse de la lumière c :

$$d = (c * \&)/2 \text{.....(1)}$$

$$\& = 2d/c \text{.....(2)}$$

Un nœud n est un voisin d'un nœud m si la distance entre n et m ne dépasse pas la marge de transmission radio R, i.e $R > d$.

$$R > (c * \&)/2 \text{.....(3)}$$

$$\& = 2R/c \text{.....(4)}$$

On note que l'utilisation du RTT élimine le besoin d'horloge synchronisé, un nœud exige seulement l'information temporelle fournie par sa propre horloge.

3.6.3 Nœuds avec des antennes directionnelles

Les antennes directionnelles ont été largement étudiées dans la littérature générale [39]. Quand antennes directionnelles sont utilisées, les nœuds utilisent "secteurs" spécifiques de leur antennes pour communiquer avec l'autre, comme représenté sur la figure 3.6.

Par conséquent, un nœud reçoit un message de son voisin à quelques informations sur la localisation de ce voisin, il connaît l'orientation relative du prochain, par rapport à elle-même, comme le montre la figure. Ce petit supplément d'information rend découverte vortex beaucoup plus facile que dans les réseaux avec exclusivement antennes omni-directionnelles.

Dans [39], Hu et Evans proposer une solution à des attaques de vers pour les réseaux ad hoc dans lesquels tous les nœuds sont équipés avec des antennes directionnelles.

Wormhole des incohérences importantes dans le réseau qui peut être facilement détectés. En SERLOC [40], Lazos et al utilisent une approche légèrement différente.

En SERLOC, à seulement quelques nœuds doivent être équipés d' antennes directionnelle, mais ces nœuds doivent également être géo-localisés. Ces nœuds peuvent envoyer des balises de localisation, sur la base desquelles les nœuds de réseau régulières déterminent leur propre position relative.

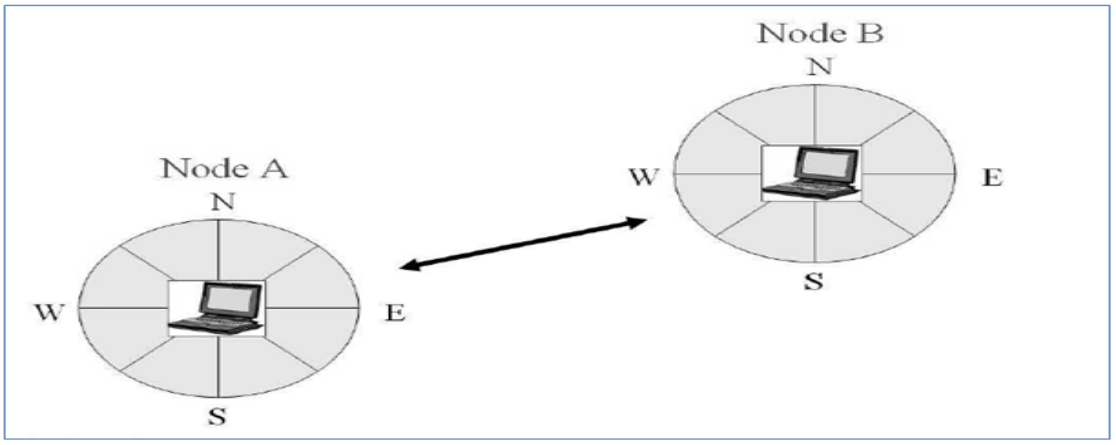

FIGURE 3.6 – Noeuds utilisant des antennes directionnelles. Lorsque les nœuds A et B communiquent

3.6.4 Le protocole MAD

Dans [41], les auteurs proposent le protocole MAD (Mutual Authenticated Distance-bounding).

Cette approche combine à la fois une mesure de la distance et une authentification. La mesure de la distance est effectuée en mesurant le temps de vol (RTT Round Trip Time) d'une requête (challenge) avec sa réponse.

Pour pouvoir s'authentifier deux nœuds doivent partager une clef. Apres avoir échanger des nonces, les deux nœuds calculent un état commun qui sera utilisé lors de la phase d'authentification. La phase suivante requiert une bonne synchronisation entre les nœuds.

Les deux nœuds échangent des bits sous la forme de challenge et de réponse. Le temps est mesuré entre l'émission d'un challenge et de la réception de la réponse. Finalement, les deux nœuds échangent les signatures de ce qu'ils ont reçus. Si les signatures sont correctes et si les contraintes de temps de vol sont satisfaites, le protocole réussit.

Le protocole MAD exige l'utilisation d'une interface radio capable de basculer rapidement d'un mode receveur vers un mode transmetteur (et vice versa). De plus, tout délais lors de l'échange des bits influence la précision de la mesure de temps et donc la sécurité.

3.6.5 Sécuriser les liens

Dans [42], les auteurs proposent un mécanisme de détection de l'attaque wormhole en sécurisant chaque lien dans le réseau. Dans cet algorithme, chaque nœud essaye d'estimer la distance qui le sépare de chacun de ses voisins directs. Cette estimation est effectuée à l'aide d'un échange de message simultané en utilisant une radio générant des ondes ultrasons.

Ensuite, chaque nœud échange les informations de ces valeurs de distances calculées (i.e. chaque nœud diffuse sa table de voisins ainsi que leurs distances estimées respectives). Une fois ces données échangées, chaque nœud exécute un ensemble de tests géométriques sur les données locales ainsi obtenues, afin de détecter les faux liens présents à cause de l'attaque wormhole.

En utilisant ce mécanisme de sécurisation des liens entre les nœuds voisins, les auteurs affirment qu'une attaque wormhole ne peut être exécutée. L'inconvénient de cette approche ,est que, chaque nœud doit être équipé d'une seconde radio à ultrasons, permettant l'estimation des distances entre les nœuds voisins.

3.6.6 Algorithme MDS

Dans [43], Wang et al. propose l'algorithme MDS (i.e. multi-dimensional scaling) qui consiste à virtualiser le réseau à l'aide d'une station de base, et à chercher des inconsistances dans les liens (i.e. l'idée est ici de reconstruire une topologie virtuelle du réseau à partir des informations reçues, afin de détecter des liens de voisinages illégaux).

Chaque nœud rapporte à la station de base sa liste de voisins ainsi que les estimations de distances de chacun (ici on n'a pas besoin d'une estimation précise contrairement aux propositions précédentes). MDS essaye ensuite de déterminer les positions virtuelles possibles pour chaque nœud de telle manière que les contraintes induites par la connectivité des nœuds et les distances estimées soient respectées. Une déformation dans la topologie virtuelle apparaîtra si une attaque de wormhole existe.

L'inconvénient de cette approche centralisée est que la perte des données reportée à la station de base pourra fausser les résultats (ceci est le cas pour toutes approches centralisées).

Voici le tableau recapulatif sur les solutions existantes ;

Proposition	Condition	Commentaires
Leashes temporelles	Horloge précisément synchronisée	tous les nœuds doivent avoir une forte synchronisation
Leashes géographiques	Avoir un GPS,Avoir une horloge synchronisée	La technologie GPS est limitée dans certeinnes zones d'où la limitation de cette méthode.
Temps-de-vol (Time-of-flight)	Utilisation du RTT (Round Trip Travel Time)	L'utilisation du RTT élimine le besoin d'horloge synchronise.
Les nœuds avec des antennes s directionnelle	Tous les nœud sont équipés des antennes directionnelles	les antennes devoile les voisins entre les noueds
Le protocole MAD	Chaque nœud doit avoir un matériel spécial lui permettent d'envoyer des bits séparés et de répondre immédiatement	deux nœuds s'authentifient, doivent échanger 2.n bits. Cette technique gourmande en terme de bande passante.
Algorithme MDS	Avoir une station de base	La perte des données reportée à la station de base pourra fausser les résultats.

TABLE 3.1 – Tableau récapitulatif des solutions

3.7 Conclusion

L'attaque womrhole l'une des attaque les plus sévere dans les reseaux mobile Ad Hoc dans laquelle un nœud malicieux intercepte les paquets en les passant par un tunnel, au lieu de les acheminer vers les successeurs cad dans un chemin reliant une source et une destination données.

Notre solution consiste à vérifier le bon acheminement des messages par des nœuds intermédiaire en utilisant La cryptographie asymétrique pour s'authentifier entre chaque nœud pour avoir un chemin source destination sans le trou vers.

Le chapitre suivant présente les résultats de simulation de notre solution en considérant un réseau qui utilise AODV ou OLSR comme protocole de routage.

Chapitre 4

Approche de sécurité pour l'attaque wormhole

4.1 Introduction

Plusieurs solutions ont été proposées, pour sécuriser les réseaux ad hoc. Ces solutions diffèrent selon le besoin en sécurité et les moyens possibles (autorité de certification, centre de distribution de clefs, algorithmes cryptographiques, ...). Actuellement, les principaux axes de recherche, portent sur l'authentification, la génération de clefs et la sécurité des protocoles de routage.

4.2 Modèle de réseaux

Comme nous avons déjà vu dans le premier chapitre, les réseaux mobiles ad hoc, sont dépourvus d'infrastructures (sans station de base), i.e, l'interconnexion entre les nœuds se fait sans point d'accès, chaque nœud joue le rôle d'un routeur avec des liens bidirectionnels, dans notre travail nous avons un ensemble de nœuds légitimes et au moins, deux nœuds malicieux qui placent un tunnel pour effectuer l'attaque wormhole.

4.3 Mécanisme de sécurité contre l'attaque wormhole

Hypothèses

Soit un réseau ad hoc qui contient un ensemble des nœuds avec des liens bidirectionnels, et un annuaire de clés qui partage des clés secrètes entre l'annuaire et chaque nœud de réseau pour assurer l'authentification (gestionnaire de clé qui contient toutes les clés des nœuds de notre réseau).

Méthode proposée

Comme on a vu dans le chapitre précédent les nœuds malicieux mettent en place un tunnel pour un échange des informations entre les attaquants et pour contrer cette attaque, on a proposé une solution qui contienne les étapes suivante :

- L'échange des clés secrètes entre chaque nœud et l'annuaire.
- Chaque nœud doit détecter ses vrais voisins à deux sauts.
- Détection de l'attaque wormhole.

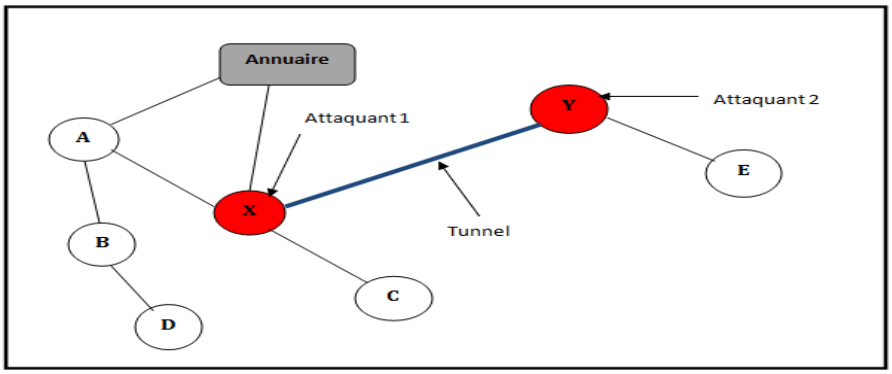

FIGURE 4.1 – schéma de la solution

1. **Etape de partage des clés**

   Chaque nœud qui veut se connecter aux réseaux, doit passer par l'annuaire pour obtenir sa clé secrète voir la figure 4.2

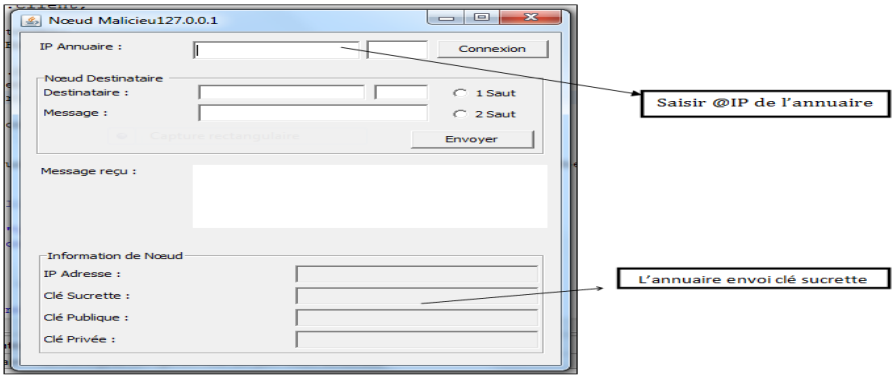

FIGURE 4.2 – Authentification au prés de l'annuaire

L'annuaire échange une clé secrète Ksi ($I := 1..N$) différente entre tous les nœuds $Ni(I := 1..N)$ passant par lui.En suite chaque nœud envoi ses informations (adresse ip, clé publique) chiffrer par sa clé secrète, et pour la communication entre les nœuds, l'émetteur doit récupérer la clé publique du destinataire au prés de l'annuaire pour chiffrer son message. Et dans le cas où l'annuaire ne possède pas la clé publique de destinataire, il va demander à ce dernier d'échanger ses informations avec lui.

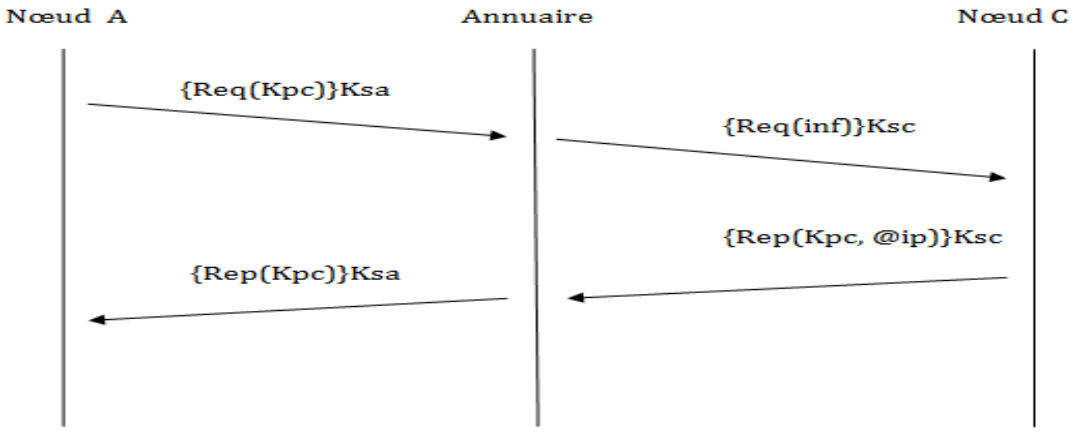

FIGURE 4.3 – Nœud A demande la clé publique de C au prés de l'annuaire

En suite les nœuds de réseau Utilisent l'algorithme de chiffrement RSA pour l'échange des messages suivant ses étapes :

Création des clés : le nœud crée 4 nombres p,q, e et d :

◇ p et q sont deux grands nombres premiers distincts. Leur génération se fait au hasard, en utilisant un algorithme de test de primalité probabiliste.

◇ e est un entier premier avec le produit $(p-1)*(q-1)$.

◇ d est tel que $e*d = 1$ modulo $(p-1)*(q-1)$. Autrement dit, ed-1 est un multiple de $(p-1)*(q-1)$.

◇ On peut fabriquer d à partir de e, p et q, en utilisant l'algorithme d'Euclide.

1.Distribution des clés

Le couple (e, n) constitue la clé publique d'un nœud. Il la rend disponible en la mettant dans un annuaire. Le couple (d, n) constitue sa clé privée. Il la garde secrète.

2.Envoi du message codé

le nœud A veut envoyer un message codé à B. Il le représente sous la forme d'un ou plusieurs entiers M compris entre 0 et $n-1$. Le nœud A possède la clé publique (n, e) de B. il calcule $C = Memodn$. C'est ce dernier nombre qu'elle envoie à B.

3.Réception du message codé

B reçoit le message chiffré C et il calcule grâce à sa clé privée $D = Cd(modn)$. D'après un théorème du mathématicien Euler,$D = Mde = M(modn)$. Il a donc reconstitué le message initial.

2. **Etape de détection des voisins**

   Avant que les nœuds ne communiquent entre eux, et partagent des paquets, ces derniers découverent ses voisins, via les protocoles de routage (OLSR, AODV) en créant des listes de voisinage à un saut et, à deux sauts, mais dans cette procédure o réside le problème, dont les attaquants peuvent modifier les listes de voisinage à deux sauts en coopérant avec un tunnel, en provoquant un disfonctionnement de la topologie des réseaux et un isolement de quelques nœuds.

   Dans notre solution, on a proposé un échange de message entre les nœuds à deux sauts qui contient l'identificateur de l'émetteur, un nombre aléatoire et un temps de vie de message chiffré avec la clé publique.

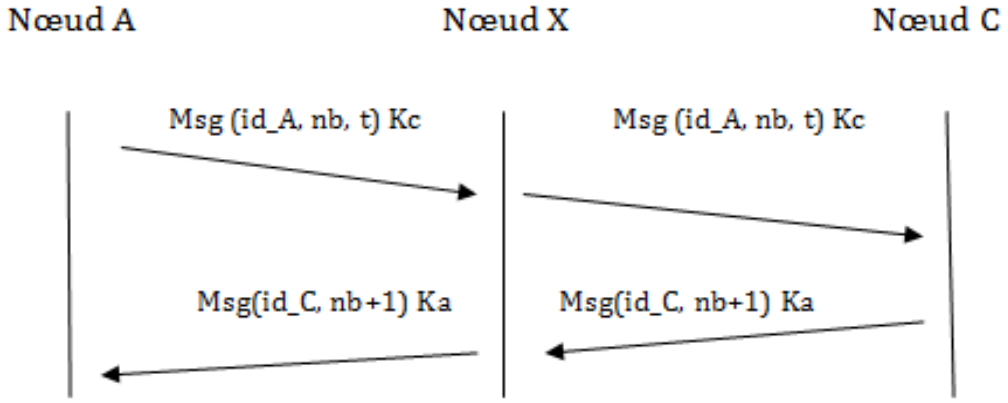

FIGURE 4.4 – Autentification des noeuds à deux sauts

Après avoir échangé les messages, chaque nœud avait assuré ses voisins à deux sauts, dans notre exemple le nœud C doit envoyer un acquittement pour le nœud A.

3. **Etape de détection de l'attaque wormhole**

   Dans l'étape de détection de voisinage, l'échange des messages entre les nœuds à deux sauts peut nous donner des possibilités pour détecter l'attaque de trou de ver, dans notre exemple, le nœud A envoi le message à C chiffré avec la clé kc (clé publique de C obtenue dans l'annuaire par A) et si le nœud A ne reçoit pas d'acquittement de C, nous allons conclure qui ya possibilité d'une attaque wormhole.

4.4 Simulation et analyse de Performance

4.4.1 Environnement de simulation

Pour tester les performances d'une solution apportée à un problème de communication dans un réseau, il n'est pas toujours possible d'accéder aux infrastructures nécessaires en raison de leurs coûts élevés. De plus, les expérimentations réelles n'offre souvent pas une grande souplesse.
Rappelons que les réseaux ad hoc sont des réseaux qui englobent plusieurs unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces radio. En effet, il serait très coûteux, et même impossible de mettre en place un réseau à des fins de tests de certains critères. Nous avons effectué une série de simulations en utilisant une application réalisée avec le langage java. Tout d'abord, nous définissons les paramètres de nos scénarios, ensuite nous présenterons nos résultats de simulation.

4.4.2 Paramètres de simulation

Dans nos simulations, l'environnement est un réseau de taille 1000 x 1000 m, dans lequel se trouvent généralement 10 à 100 nœuds, mais ce nombre est varié pour tester l'effet de la densité de nœuds sur les différents facteurs de performance à étudier le long de ce chapitre.
Nous effectuons des simulations d'une durée de 300 secondes, et un nœud source qui génère des paquets de taille 1024 bits.
Le tableau suivant résume les paramètres utilisés dans nos simulations :

Paramètres	**Valeurs**
Taille de réseau	$1000M$
Taille des paquets (bits)	1024bits
Nombre de nœuds	5
Temps de simulation (sec)	900s

TABLE 4.1 – Paramètres de simulation

La simulation a été effectuée dans un réseau qui utilise AODV (protocole réactif) ou OLSR (protocole proactif) comme protocole du routage.

4.4.3 Métriques de simulation

Nous avons choisi quelque métriques les plus souvent abordées dans le domaine de la sécurité pour évaluer les performances pour les protocoles AODV et OLSR :

PDR Packet Delevery Ratio

C'est le taux de paquets livrés avec succès. Cette métrique représente le pourcentage des paquets livrés à leurs destinations avec succès par rapport à la somme des paquets des donnés émis dans le réseau.

$$\textbf{PDR = Nombre de paquets reçus / Nombre de paquets émis}$$

EED Average End to End Delay

c'est le délai moyen de bout en bout. Ce paramètre concrétise la durée moyenne de transmission d'un paquet de données depuis la source vers la destination. Il introduit tous les délais d'établissement d'une route. Il est intéressant d'évaluer cette métrique car certaines applications exigent un certain délai de transfert qu'il ne faut pas dépasser.

$$EED = \sum \ Temps \ \ de \ \ livraison \ \ d'un \ \ paquet \ \ / \ \ Nombre \ \ de \ \ paquets \ \ reus.$$

La simulation consiste à mesurer ces métriques dans un réseau qui utilise AODV ou OLSR dans les deux cas suivants :

1. Avec attaque et sans utiliser la solution.

2. Avec attaque et utiliser la solution.

4.5 Analyse des résultats

Après une simulation de notre application réalisée par le langage JAVA, qui est connecté au wamp serveur, ce dernier sauvegarde les valeurs de simulation dans sa base de données.

1. Simulation réalisée **sans** notre solution :

cas sans solution			
temps	msg reçus	msg envoyé	pdr
1	2	11	0,18
3	6	34	0,18
5	20	82	0,24
7	37	130	0,28
9	48	178	0,27
10	66	227	0,29
12	83	275	0,30
14	97	323	0,30
15	102	371	0,27
17	116	420	0,28
19	122	431	0,28
21	159	436	0,36
23	170	441	0,39
25	207	447	0,46
26	221	455	0,49
29	237	464	0,51
30	250	471	0,53
31	257	474	0,54
32	267	476	0,56

2. Simulation réalisée **avec** notre solution

cas avec solution			
Temps	msg reçus	msg envoyé	pdr
1	2	12	0,17
3	45	80	0,56
5	79	128	0,62
7	114	176	0,65
8	152	224	0,68
10	178	272	0,65
12	216	320	0,68
14	250	368	0,68
15	278	416	0,67
17	306	464	0,66
19	346	512	0,68
21	378	560	0,68
22	410	609	0,67
24	442	658	0,67
26	473	706	0,67
28	508	754	0,67
29	537	802	0,67
31	575	850	0,68
32	623	899	0,69

Nous allons voir les résultats dans la figure suivante :

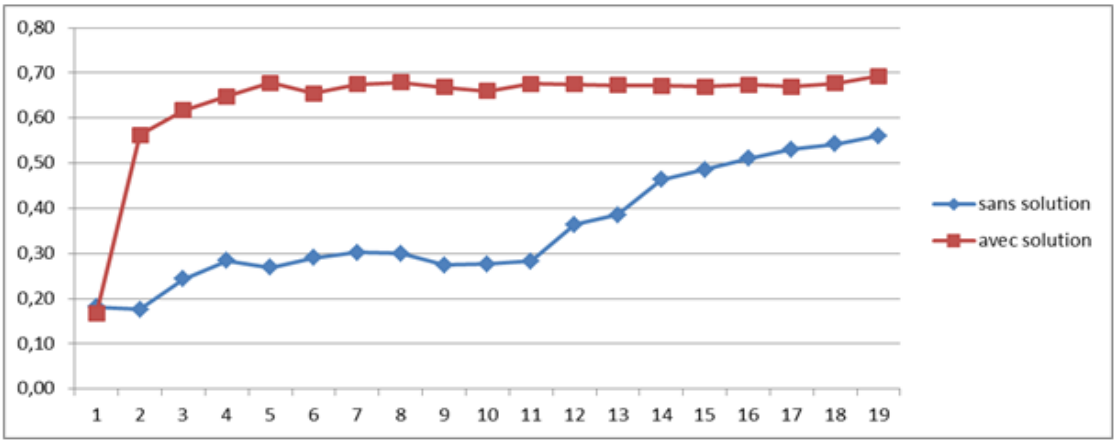

FIGURE 4.5 – Résultats de la simulation

Le trafic envoyé par le nœud émetteur dans le cas d'une attaque de wormhole et sans solution, nous avons remarqué que les messages reçus sont très diminués par apport aux messages émis, et cela reviens à la perte des messages envoyé, qui ont une durée de vie, qui sont perdu dans le tunnel établi entre les deux attaquants. Et dans le cas de notre approche, nous avons remarqué qu'il ya pas beaucoup de perte après la détection des vrais voisins à deux sauts.

4.6 Conclusion

Dans cette partie nous avons évalué les performances de notre approche dans la détection de l'attaque wormhole, à travers les graphes obtenus nous remarquons l'efficacité de notre solution qui empêche la modification, le rejoue des messages et la falsification des relations de voisinage pour avoir le bon fonctionnement du réseau.

Conclusion Générale

Un réseau ad hoc est un ensemble de nœuds interconnectés par des liens sans fil. Il présente l'avantage d'être facile et moins couteux à déployer, mais en contrepartie, il est vulnérable par plusieurs attaques, à cause de l'ouverture de medium de communication et la possibilité de mobilité des nœuds. Les messages diffusés dans le réseau peuvent être intercepté es et modifiés ou supprimés par les nœuds malicieux, ceci a fait de la sécurité des échanges dans un réseau ad hoc, un défi pour les concepteurs des protocoles, en particulier ceux concernant le routage. Plusieurs solutions ont été proposées pour sécuriser les différentes fonctions d'un réseau ad hoc, mais à cause de la diversité des attaques qui exploitent les vulnérabilités multiples d'un réseau ad hoc, la sécurité reste toujours un problème et de nouvelles solutions de sécurité sont plus que nécessaires pour rendre le réseau ad hoc plus résistant contre les différentes attaques possibles.

L'attaque Wormhole, l'une parmi les attaques les plus sévères qui peut être lancée même si le support de communication est sécurisé et authentique. Les conséquences de cette attaque contre les protocoles de routage dans les réseaux mobiles ad hoc ont été bien étudiées. Aussi une étude assez exhaustive a été faite sur les travaux proposes dans la littérature pour sécuriser les réseaux ad hoc contre l'attaque Wormhole, dans notre travail on s'est intéressé par cette attaque, et après la spécification de la manière avec laquelle une telle attaque peut être menée, nous avons proposé une solution qui se base sur la sécurisation du voisinage a deux sauts et les acquittements.

References bibliographiques

[1] <Contribution a la sécurisation du routage dans les réseaux ad hoc Celine> BURGOD These doctorat de L'UNIVERSITE DE LIMOGES.

[2] S. Corson, J. Macker, 'Mobile Ad hoc Networking (MANET) : Routing Protocol Performance Issues and Evaluation Considerations', Request for Comments 2501, IETF, January 1999 .

[3] «Sécurité du routage dans les réseaux sans fil spontanés » Abdelmajid HAJAMI THÈSE de doctorat a Ecole Natonale Supérieure d'Informatique (ENSIAS) : Rabat ".

[4] , " Hybridation entre les modes ad hoc et infrastructure dans les réseaux de type Wi :Fi ". Mémoire d'Ingénieur Civil Informaticien en Sciences Appliquées.Université Libre de Bruxelles 2005 :2006.

[5] < Etude du standard IEEE802.11 dans le cadre des Réseaux ad hoc > Dominique D houtaut These doctorat L'institut National des Science Appliquées de lyon .

[6] James A. Freebersyser, Barry Leiner, "A DoD perspective on mobile ad hoc networks ?, Ad Hoc Networking, Addison Wesley, pp. 29 :51, 2001.

[7] Contributions à la sécurité dans les réseaux mobiles ad Hoc THÈSE doctort Abderrezak RACHEDI l'Université d'Avignon le 29 mars 2012.

[8] Authentification dans les Réseaux Véhiculaires Opérés > Christian TCHEPNDA,Thèse docrtat de l'Ecole Nationale Supérieure des Télécommunications et électronique paris.

[9] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. l. Cayirci ; "A survey on sensor networks" ; IEEE Communications Magazine, Vol. 40, No. 8, pp. 102 :116, Août2002

[10] La tolérance aux pannes des algorithmes de partage de ressources dans les systèmes repartis et les réseaux Ad Hoc Sami Abdelmadjid Oubbati et Benarfa Université Amar Telidji Laghouat - Ingénieur d'état en informatique 2010.

[11] Charles E. Perkins and Pravin Bhagwat. Highly dynamic destination sequenced distance :vector routing (dsdv) for mobile computers. In SIG : COMM, pages 234 :244, 1994.

[12] T. Clausen, P. Jacquet, 'Optimized Link State Routing Protocol (OLSR)', Request for Comments : 3626 ,October 2003.

[13] <'CEDAR : a Core :Extraction Distributed Ad hoc Routing algorithm'> Prasun Sinha Raghupathy Sivakumar Vaduvur Bharghavan University of Illinois at Urbana Champaign.

[14] Etude comparative entre les protocoles de routage de la QoS dans les réseaux Adhoc SEDDIKI Noureddine d & 1 FEHAM Mohammed Laboratoire STIC, Faculté des sciences de l'Ingénieur.

[15] BRuIT :Bandwidth Reservation under InTerferencesin ?uence Claude CHAUDET, Isabelle GUERIN ´ LASSOUS Laboratoire de l'Informatique du Parallelisme - ENS Lyon - 46 allée d'Italie - 69007 Lyon.

[16] Paul Mahlethan, " 802.11 et les réseaux sans fil ", livre Edition Eyrolles, 2002, ISNB : 2-212-11154-1.

[17.1]Z. J. Haas. A new routing protocol for the reconfigurable wireless networks, 1997, In Proc. of the IEEE Int. Conf. on Universal Personal Communications.

[17.2] Michel Hoffmann. Du "dictionnaire dicodunet http ://www.dicodunet.com/definitions/internet/secur informatique.html

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

[19] 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 ", Thèse de magister, université de Boumerdes, 2008.

[20] A. Yger and J.-A. Weil, Mathématiques appliquées L3, P. Education, Ed. 2009.

[21] Étude technique réalisée par CGI, " Étude technique Cryptographie à clé publique et signature numérique Principes de fonctionnement ". Septembre 2002.

[22] Chris Karlof, David Wagner, "Secure routing in wireless sensor networks : attacks and countermeasures", Ad Hoc Networks 1(2003) 293-315, 2003.

[23] Alexandre Poquet. "Les attaques sur le routage dans les réseaux ad hoc ". Présentation lors de la Journée scientifique de l'équipe ARMOR 2. IRISA,Rennes, le vendredi 09 février 2007.

[24] Frank Stajano, Ross Anderson. "The Resurrecting Duckling :Security Issues for Ad- hoc Wireless Networks". Dans 7th International Workshop on Security Protocols, volume 1796 des Lecture Notes in Computer Science, pages 172- 194. Springer-Verlag, 1999.

[25] M. N. Lima, H. W. da Silva, A. L. dos Santos, and G. Pujolle, "A Security Management Architecture for Supporting Routing Services on WANETs," Federal University of Parana, Curitiba, Parana, Brazil, Technical Report, 2010.

[26] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad Hoc network routing protocols," in Proceedings of the 2nd ACM workshop on Wireless security, San Diego, CA, USA, 2003, pp. 30-40.

[27] Céline Burgod, " Contribution à la sécurisation du routage dans les réseaux ad hoc ". Thèse de

doctorat, Spécialité informatique, Université de LIMOGES, le 12 octobre 2009.

[28] Manel Guerrero Zapata and N. Asokan. Securing ad hoc routing protocols. InW. Douglas Maughan and Nitin H. Vaidya, editors,Workshop on Wireless Security, Pages 1-10. ACM, 2002.

[29] Yih-chun Hu ,David B. Johnson, Adrian Perrig "SEAD : Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks". Article de recherche publié dans Mobile Computing Systems and Applications, 2002. Proceedings Fourth IEEE Workshop 2002. PAGES 3-13.

[30] Panagiotis Papadimitratos and Zygmunt J. Haas. Secure link state routing for mobile ad hoc networks. In SAINT Workshops, pages 379-383. IEEE Computer Society, 2003.

[31] Çayirci, E., & Rong, C. (2009). Security in Wireless Ad Hoc and Sensor Networks. London : Wiley.

[32] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks : attacks and countermeasures. Ad Hoc Networks , 293-315.

[33] Poornima, E., & Bindhu, C. (2011). Prevention of WormholeAttacks in Geographic Routing Protocol. International Journal of Computer Network and Security (IJCNS), 42-50.

[34] Wang et al , (2006) Prevention of WormholeAttacks.

[35] Hu, Y.-C., Perrig, A., & Johnson , D. (2006). Wormhole attacks in wireless networks. IEEE Journal on Selected Areas in Communications , 370-380.

[36] Laisses paquet : une défense contre les attaques de vers dans les réseaux sans fil, Y.-C. Hu, A. Perrig, DB Johnson, INFOCOM 2003 Vingt-deuxième annuelle conjointe Conférence de l'IEEE Computer et sociétés de communication, vol. 3, 30 Mars- Avril 3rd 2003, pp 1976-198.

[37] Wormhole Attack Detection in Mobile Ad Hoc NetworksAjay Prakash Rai, VineetSrivastava, Rinkoo Bhatia Institute Of Technology and Management, Gwalior (M.P), India.

[38] D. B. Johnson Y.C.Hu, A.Perrig. Packet leashes : a defense against wormhole attacks in wireless net works. infocom 2003, twenty-secondannual joint conferenceof the IEEE computer and communication societies, vol.3. March 30 -April 3rd 2003 1976-1986.

[39] The use of directional antennas to prevent wormhole attacks, L. Hu, D. Evans, Proceedings of the 11th Symposium Network and Distributed System Security, pp. 131-141 2003 17.

[40] Serloc : Secure Range-Independent Localization for Wireless Sensor Networks, L. Lazos, R. Poovendran, Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, October 2004.

[41] Srdjan .apkun, Levente Buttyán, and Jean-Pierre Hubaux. Sector : secure tracking of node encounters in multi-hop wireless networks. In SASN '03 : Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pages 21-32, New York, NY, USA, 2003. ACM.

[42] Reza Shokri, Marcin Poturalski, Gael Ravot, Panos Papadimitratos, and Jean-Pierre Hubaux. A practical secure neighbor veri-cation protocol for wireless sensor networks. In WiSec '09 : Proceedings of the second ACM conference on Wireless network security, pages 193-200, New York, NY, USA, 2009. ACM.

[43] Weichao Wang and Bharat K. Bhargava. Visualization of wormholes in sensor networks. In Markus Jakobsson and Adrian Perrig, editors, Proceedings of the 2004 ACM Workshop on Wireless Security, Philadelphia, PA, USA, October 1, 2004, pages 51-60. ACM, 2004.