République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane MIRA-Béjaïa

Faculté des Sciences Exactes

Département d'Informatique

Mémoire de fin de cycle

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

Option : Administration et Sécurité des Réseaux

Thème

Sécurité contre l'Attaque d'Interférence dans les Réseaux Ad hoc

Pésenté par :

M^elle^ BENIDIR Dalida.

M^elle^ KENANI Hayat.

Soutenu devant le jury composé de :

Présidente	**Mme. ABASSI Nacira**	**Univ. A. Mira de Béjaïa.**
Examinatrice	**Mme. SABRI Salima**	**Univ. A. Mira de Béjaïa.**
Examinateur	**M. BOUDRIES Abdelmalek**	**Univ. A. Mira de Béjaïa.**
Rapporteur	**M. BAADACHE Abderrahmane**	**Univ. A. Mira de Béjaïa.**

Promotion : 2013/2014

Remerciements

Nos vifs remerciements vont d'emblée à Dieu tout puissant qui nous a dotées d'une grande volonté et d'un savoir adéquat pour mener à bien ce modeste travail.

Nos remerciements sont adressés également à nos chers parents pour tous les sacrifices consentis à notre égard et leur énorme

soutien.

À tous nos proches.

À notre encadreur, ***M. BAADACHE Abderrahmane*** *qui nous a inculquées une grande confiance et nous a orientées dans le bon sens quant à l'élaboration de ce projet.*

Aux membres de la commission pour avoir accepté de juger notre modeste travail.

À tous nos enseignants et les membres du département informatique de l'université ABDERAHMENE MIRA.

Et enfin, à tous ceux qui ont participé de près ou de loin à l'accomplissement de ce projet.

Dédicaces

Je dédie ce modeste travail :

À mes très chèrs parents

À mes chèrs frères Nadir, Abd L'aziz ,Dahmane et Rafik

À mes trés chère sœur Hadjila,Ghania et Saida

À ma chère grande mère Ourida,

À toute ma famille sans exception,

À tous mes amis,

À ma binôme DALIDA

Et à tout mes amis.

HAYAT

Dédicaces

Je dédie ce modeste travail :

À la mémoire de ma chère grand-mère ZAHRA que je n'oublierai jamais,

À mon père que j'aime tellement, l'homme qui a tout donné pour mon bonheur, c'est l'homme le plus cher au monde,

À ma très chère mère que j'aime plus que n'importe qui et j'espère qu'elle va être fière de moi,

À mon cher unique et petit frère KARIM,

À ma tante HAKIMA, son mari MAHMOUD, son fils MASSINISSA et ses filles : DYHIA et TINHINANE.

À ma binôme HAYAT

Et à tout mes amis(es).

DALIDA

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AODV : Ad hoc On demand Distance Vector

ARAN : Authenticated Routing for Ad hoc Network

AP : Access Point

CC : Correlation Coefficient

DoS : Denial of Service

DSDV : Destination Sequenced Distance Vector

DSR : Dynamic Source Routing

ETSI : European Telecommunication Standards Institute

IP : Internet Protocol

IEEE : Institute of Electrical and Electronics Engineers

LMAC : Lightweight Medium Access Control

MAC : Message Authentication Code

MAC : Medium Access Control

MAE : Manet Authentication Extension

MANET : Mobile Ad Hoc Network

NS : Number Sequence

OLSR : Optimized Link State Routing protocol

OSI : Open Systems Interconnection

PDA : Personal Digital Assistant

PDR : Packet Delivred Ratio

PSR : Packet Sent Ratio

PHY : Physique

EP : Error Probability

RREP : Route REPly

RREQ : Route REQuest

SAODV : Secure Ad hoc On demand Distance Vector routing

SAR : Security Aware ad hoc Routing protocol

SEAD : SEcure Ad hoc Distance vector routing

SS : Signal Strength

SRP : Secure Routing Protocol

SIFS : Short Inter Frame Spacing

TESLA : Time Efficient Stream Loss tolerant Authentication

TIK : TESLA with Instant Key disclosure

TDMA : Time Division Multiple Access

ZRP : Zone Routing Protocol

Introduction générale

Un réseau sans fil est un ensemble d'équipements (ordinateurs portables, PDA, tablette, etc.) qui utilisent un médium de communication sans fil pour communiquer. Ce type de réseaux ne vient pas remplacer les réseaux filaires, mais plutôt les étendre. Il peut fonctionner selon deux modes : infrastructure ou ad hoc. Dans le mode infrastructure, la communication s'effectue via des points d'accès auxquels plusieurs nœuds mobiles sont associés ; tandis que dans le mode ad hoc, les nœuds sans fil n'ont pas besoin du point d'accès pour communiquer, ils peuvent s'auto-organiser pour assurer la connectivité. Dans notre travail, on s'est focalisé sur les réseaux ad hoc. Ce genre de réseaux est simple, rapide et moins cher à déployer, ce qui justifie son utilisation par plusieurs applications militaires et civiles. Il est caractérisé essentiellement par l'ouverture du médium de communication, la mobilité, l'absence d'infrastructure et l'administration centralisée. Bien que les caractéristiques de ces réseaux offrent plus de convivialité et de commodité aux utilisateurs, ces derniers sont vulnérables par plusieurs attaques possibles. En effet, sans mécanisme de sécurité, le trafic envoyé dans l'air peut être facilement intercepté, modifié ou même supprimé. Généralement, garantir la sécurité dans un réseau ad hoc revient à assurer les services suivants : authentification des participants, intégrité et confidentialité des données, disponibilité du réseau, le contrôle d'accès et l'anonymat. Les solutions de sécurité proposées dans la littérature se basent essentiellement sur des outils cryptographiques et non cryptographiques ou encore utilisent les IDS pour détecter les intrusions. Bien que multiples, ces mécanismes de sécurité ne garantissent pas une sécurité absolue, mais il existe toujours des failles de sécurité exploitées pour mener d'autres attaques de sécurité.

Dans ce mémoire, on s'est intéressé à l'attaque jamming (interférence ou brouillage). Il s'agit d'une attaque sévère dans laquelle l'attaquant monopolise le canal de communication, empêchant ainsi les nœuds légitimes de communiquer ; elle peut être lancée soit

au niveau MAC ou physique. Au niveau MAC, l'attaquant viole le protocole MAC utilisé pour ordonnancer l'accès au canal, en insérant des paquets inutiles pour faire croire aux autres nœuds que le canal est occupé ; elle peut aussi être lancée au niveau PHY par l'envoi d'un signal bruit pour perturber le signal légitime. Pour se protéger contre cette attaque, la littérature propose plusieurs solutions qui se basent principalement sur le saut de fréquences et l'étalement du spectre. Ces solutions restent dans la majorité des cas non suffisamment efficaces et robustes, ce qui nous a motivées à chercher une autre solution contre cette attaque. Notre solution consiste à établir un chemin entre deux nœuds source et destinataire de sorte que chaque paire de nœuds intermédiaires qui se succèdent dans le chemin utilisent un canal différent ; de cette façon, en cas d'attaque d'un canal, uniquement les deux nœuds reliés par ce canal seront affectés. À la détection de l'attaque, les deux nœuds négocient un autre canal de communication pour rétablir la communication entre eux. Notre solution est avantageuse dans le sens où la synchronisation sur le nouveau canal n'implique que les deux nœuds intermédiaires concernés. Par simulation, nous avons évalué la performance de notre solution et nous l'avons comparée avec la technique du saut de fréquences en termes d'overhead et du temps de latence.

Notre mémoire est structuré au tour de quatre chapitres. Le premier chapitre introduit les réseaux sans fil ad hoc, en particulier les caractéristiques, les domaines d'application, les normes de ces réseaux ainsi que les protocoles du routage. Le second chapitre aborde la sécurité des réseaux ad hoc, il présente les vulnérabilités de ces derniers, les services de sécurité ainsi que les différentes solutions proposées dans la littérature. Le troisième chapitre se focalise sur l'attaque d'interférence dans les réseaux ad hoc qui est le sujet de notre travail. Le dernier chapitre est consacré à la description de notre proposition et à l'analyse et l'interprétation des résultats de la simulation. Enfin le mémoire s'achève par une conclusion et perspectives.

1

Généralités sur les réseaux ad hoc

1.1 Introduction

Un réseau sans fil est un système composé de nœuds (ordinateur portable, PDA, NetBook, etc.) éventuellement mobiles, qui permet à ses utilisateurs de communiquer via des ondes radio. Ce type de réseaux offre une grande flexibilité d'emploi. En particulier, il permet la mise en réseau des nœuds dont le câblage serait trop onéreux à réaliser dans leur totalité, voire même impossible. Deux types de réseaux sans fil peuvent être distingués. Le réseau avec infrastructure qui est constitué de plusieurs stations de base, reliées entre elles par une architecture filaire jouant le rôle d'un routeur pour faire communiquer des nœuds assignés à des stations de bases différentes. Le réseau sans infrastructure ou ad hoc est un réseau dans lequel chaque nœuds peut jouer le rôle d'un routeur ou d'un client, i.e. il n'y a pas de stations de bases comme dans le réseau avec infrastructure.

Dans ce chapitre, nous allons présenter les principaux concepts liés aux réseaux sans fil. Nous commençons par la définition de ce type de réseaux et les deux classes qui le constituent (mode infrastructure et mode sans infrastructure). Nous introduisons ensuite le concept des réseaux ad hoc et leurs caractéristiques. Enfin, nous allons citer quelques domaines d'application ainsi que les différentes classes des protocoles du routage utilisés dans les réseaux ad hoc.

1.2 Réseaux sans fil

En raison de leur facilité de déploiement et de leur coût relativement faible, les réseaux sans fil sont de plus en plus utilisés.

1.2.1 Définition

Un réseau sans fil (en anglais wireless network) est un réseau dans lequel les différents éléments participants (ordinateur portable, PDA, téléphone portable, etc.) ne sont pas raccordés entre eux par un média physique. La transmission des données se fait via des ondes hertziennes. Ceci permet aux utilisateurs de se déplacer dans un périmètre de couverture pouvant aller d'une dizaine de mètres à quelques kilomètres [1].

1.2.2 Architectures

Les architectures des réseaux sans fil peuvent fonctionner selon deux modes : le mode avec infrastructure et le mode ad hoc.

1.2.2.1 Mode avec infrastructure

Dans ce mode, le réseau sans fil est composé de deux ensembles d'entités distinctes : les "composantes fixes" d'un réseau de communication filaire et les "composantes mobiles". Certaines composantes fixes, appelées stations de bases (nœuds contenants le point d'accès) sont munies d'une interface de communication sans fil pour la communication directe avec les composantes ou les nœuds mobiles localisés dans une zone géographique limitée appelée cellule (FIGURE 1.1).

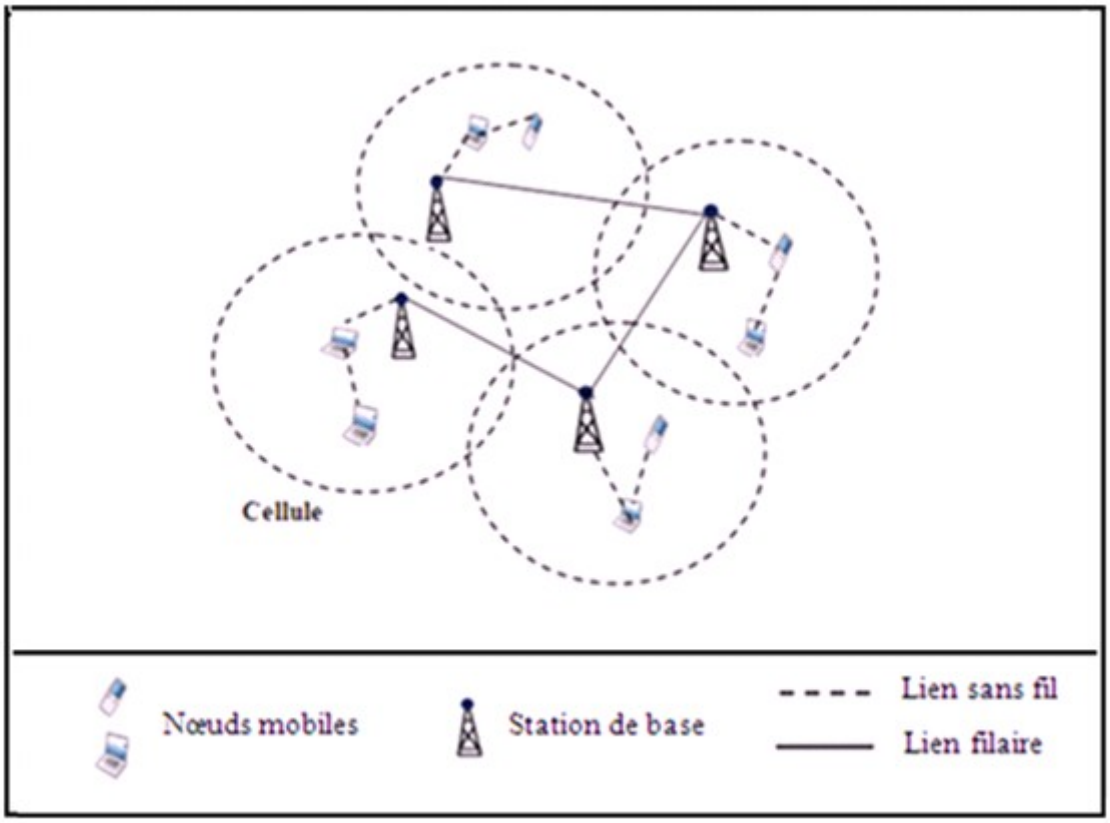

FIGURE 1.1 – Mode avec infrastructure

1.2.2.2 Mode sans infrastructure ou ad hoc

Un réseau sans infrastructure ou ad hoc ne comporte pas l'entité " site fixe ", tous les sites du réseau sont mobiles et se communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil. L'absence de l'infrastructure ou du réseau filaire oblige les unités mobiles à se comporter comme des routeurs qui participent à la découverte et la maintenance des routes pour les autres nœuds du réseau (FIGURE 1.2).

La différence entre le mode sans infrastructure et le mode avec infrastructure est que dans le second, toutes les communications passent par l'AP, alors que dans le premier

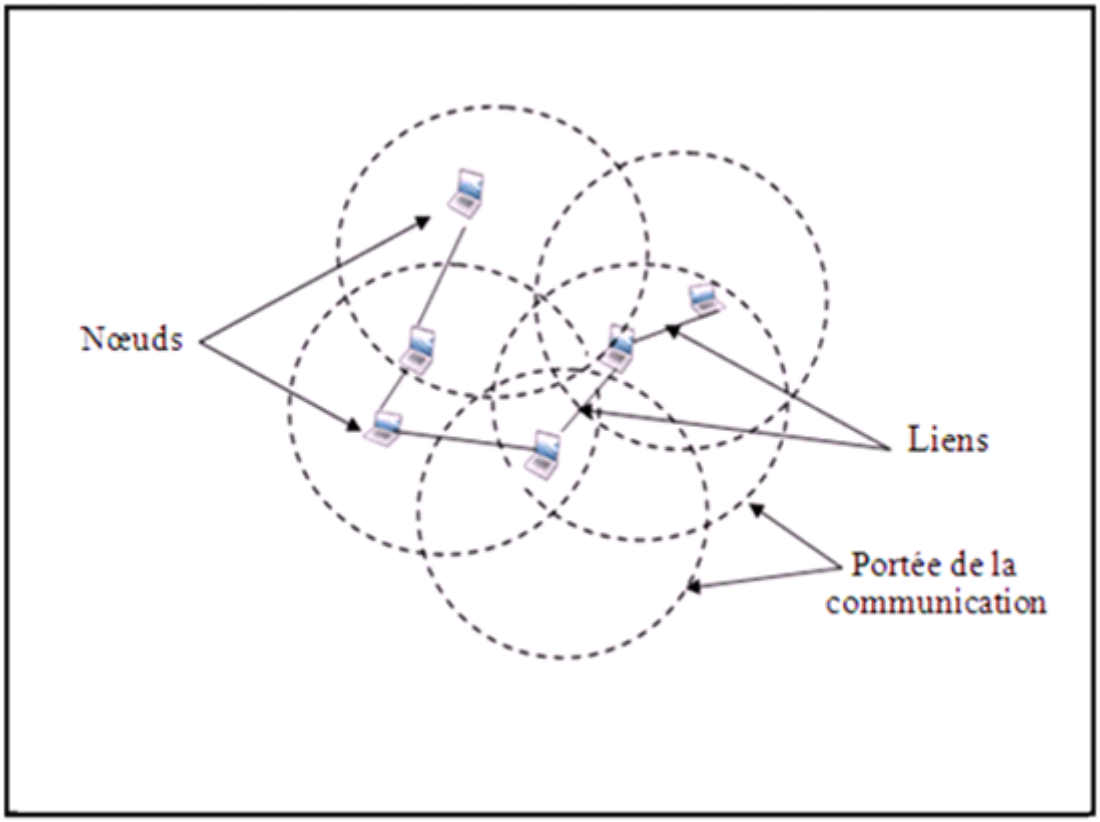

FIGURE 1.2 – Mode sans infrastructure

mode, la communication entre deux machines, qui sont à la portée radio l'une de l'autre, se fait directement.

1.3 Réseaux mobiles ad hoc

1.3.1 Définition

Les réseaux ad hoc, appelés aussi MANET (Mobile Ad hoc NETwork) sont formés dynamiquement par un grand nombre de stations mobiles (nœuds) qui se connectent sans utiliser d'infrastructure existante en utilisant comme moyen de communication des interfaces sans fils . Les nœuds interagissent et peuvent coopérer pour s'échanger des services. Ces nœuds sont donc libres de se déplacer et de s'organiser arbitrairement. Chaque nœud est capable de communiquer directement avec ses voisins par l'intermédiaire desquels il communique avec des nœuds plus éloignés, donc peut servir comme relais aux autres nœuds du réseau [2].

1.3.2 Caractéristiques

Les caractéristiques principales qui différencient un réseau ad hoc d'un réseau filaire sont :

- **Absence d'infrastructure :** Les réseaux mobiles ad hoc se distinguent des autres réseaux mobiles par l'absence d'infrastructure préexistante et de tout genre d'administration centralisée. Les nœuds mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue [3].
- **Mobilité des nœuds :** Dans un réseau ad hoc, les nœuds peuvent être mobiles, ceci conduit à une topologie dynamique qui peut changer rapidement, de façon aléatoire et non prédictible.
- **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 nœud soit modeste [4].
- **Coût du déploiement réduit :** Le déploiement d'un réseau sans fil est moins coûteux que celui d'un réseau filaire.
- **Sécurité physique limitée :** Les réseaux mobiles ad hoc sont plus touchés par le paramètre de sécurité physique que les réseaux filaires. Cela est dû au fait que les nœuds mobiles peuvent être déployés dans des endroits quelconques, et en conséquence, ils se retrouvent moins protégés physiquement.
- **Interférences :** Les liens radios ne sont pas isolés. Deux transmissions simultanées sur une même fréquence ou utilisant des fréquences proches peuvent s'interférer [5].
- **Vulnérabilité :** Les réseaux ad hoc présentent plusieurs failles de sécurité. La liaison sans fil peut permettre à des nœuds non autorisés d'écouter et d'accéder facilement au réseau.
- **Énergie limitée :** Les nœuds sont alimentés par des sources d'énergie autonomes comme des batteries qui s'épuisent avec le temps.
- **Nœud caché :** Supposons que le nœud B est à la portée de communication des nœuds A et C, et que A est sur le point de communiquer avec le nœud B. Si le nœud C décide d'envoyer des données au nœud B et étant donné que C n'est pas à la portée de communication du nœud A, alors les paquets envoyés par C à B s'interfèrent avec ceux envoyés par A à B (FIGURE 1.3)[6]. Dans ce cas, le

nœud C est un nœud caché au nœud A. Ainsi, les nœuds cachés peuvent causer les collisions dans la transmission des données, donc un nœud caché est celui qui est dans la portée de transmission du destinataire mais en dehors de la portée de transmission de l'émetteur [7].

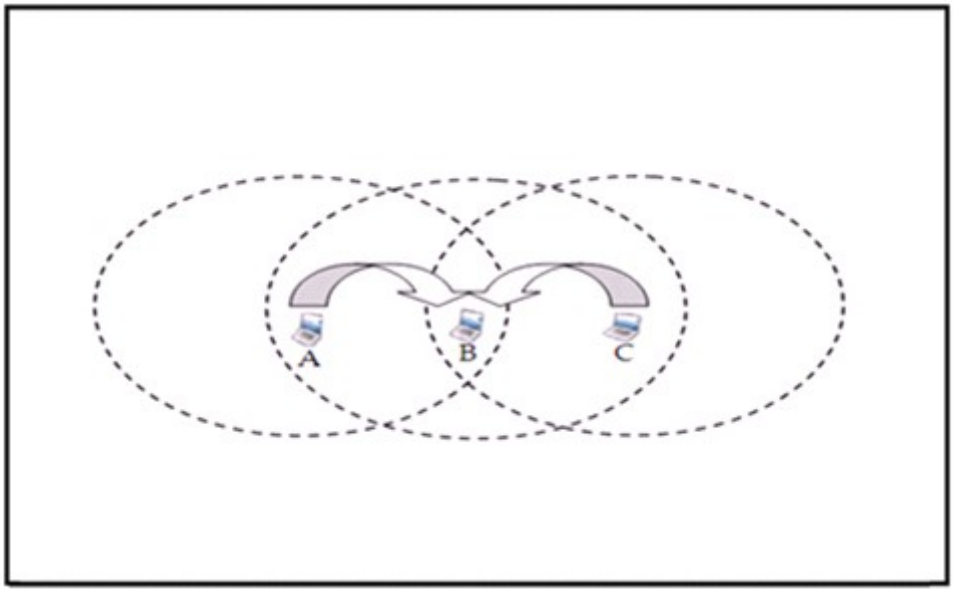

FIGURE 1.3 – Problème du nœud caché

- **Nœud exposé :** Le nœud C est à la portée radio à la fois des nœuds B et D. Supposons que B transmette actuellement des données au nœud A. Le nœud C, en écoutant le canal radio, le considèrera comme occupé et différera sa transmission vers le nœud D. Cependant cette transmission n'aurait pas gêné la réception du nœud A qui est hors de la portée de C, ce qui réduit les performances de l'ensemble du système. Théoriquement, C peut avoir une conversation parallèle avec un autre terminal hors de la portée de transmission de B et dans la portée de transmission de C. Dans ce cas, le nœud C est un nœud exposé à B. Un nœud exposé est celui qui est dans la portée de transmission de l'émetteur mais en dehors de la portée de transmission du destinataire, donc est le complément du nœud caché [7].

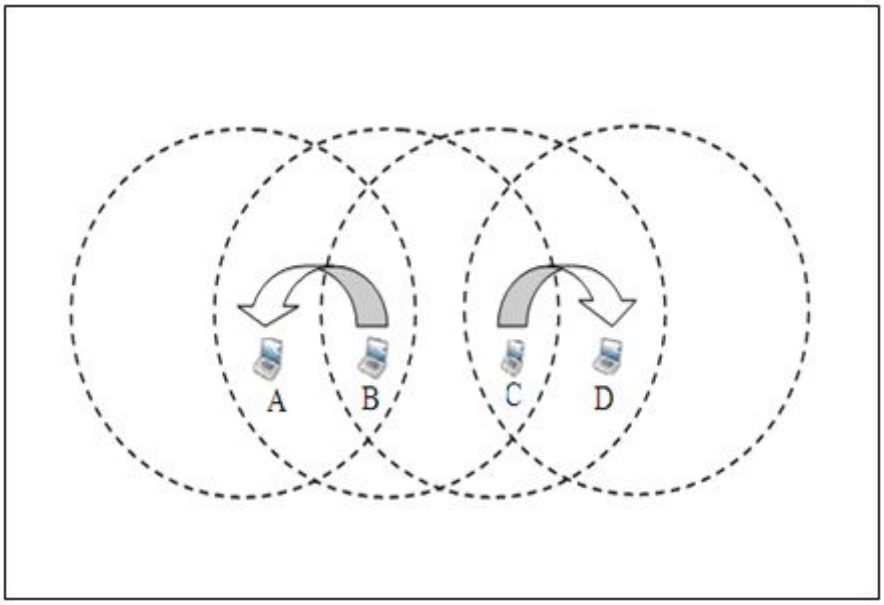

FIGURE 1.4 – Problème du nœud exposé

1.3.3 Normes

Plusieurs technologies sans fil sont déjà utilisées pour la mise en œuvre des réseaux ad hoc. Parmi ces technologies, nous citons :

- **Bluetooth :** Bluetooth ou IEEE 802.15, est une technologie de communication sans fil largement utilisée par des appareils tels que PDA, téléphones mobiles, tablette, etc. Le Bluetooth est une technologie de transmission qui utilise des ondes radio dont la bande de fréquences est de 2,4 à 2,4835 GHz. Un appareil équipé du Bluetooth peut fonctionner en mode commutation de paquets ou commutation de circuits [8].
- **IEEE 802.11 :** La norme IEEE 802.11 est un standard international décrivant les caractéristiques d'un réseau local sans fil. Elle s'attache à définir les couches basses du modèle OSI (la couche physique et la couche liaison de données). La couche physique définit la modulation des ondes radio et les caractéristiques de la signalisation pour la transmission des données, tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physiques) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité [9].

- **HiperLAN :** HiperLAN est une norme européenne standardisée par l'ETSI (European Telecommunication Standards Institute) qui a proposé deux versions d'HiperLAN :
  - **HiperLAN1 :** Fut proposée en 1996 ; elle permet un transfert autour de 20 Mbit/s dans la gamme de fréquence de 5 GHz.
  - **HiperLAN2 :** Fut proposée en 1999 ; elle permet d'obtenir un débit théorique de 54 Mbit/s sur une zone d'une centaine de mètres, dans une gamme de fréquences comprises entre 5150 et 5300 MHz [9].
- **HomeRF :** Cette technologie a été lancée en 1988 par le Home RF Working Group. Il s'agit d'une norme qui propose un débit théorique de 10 Mbit/s avec une portée d'environ 50 à 100 mètres [8].

1.3.4 Modélisation d'un réseau ad hoc

Un réseau ad hoc peut être modélisé par un graphe non orienté $G_t=(V_t, E_t)$ (FIGURE 1.4) où V_t représente l'ensemble des nœuds, et E_t représente l'ensemble des liens qui existent entre ces nœuds à l'instant t.

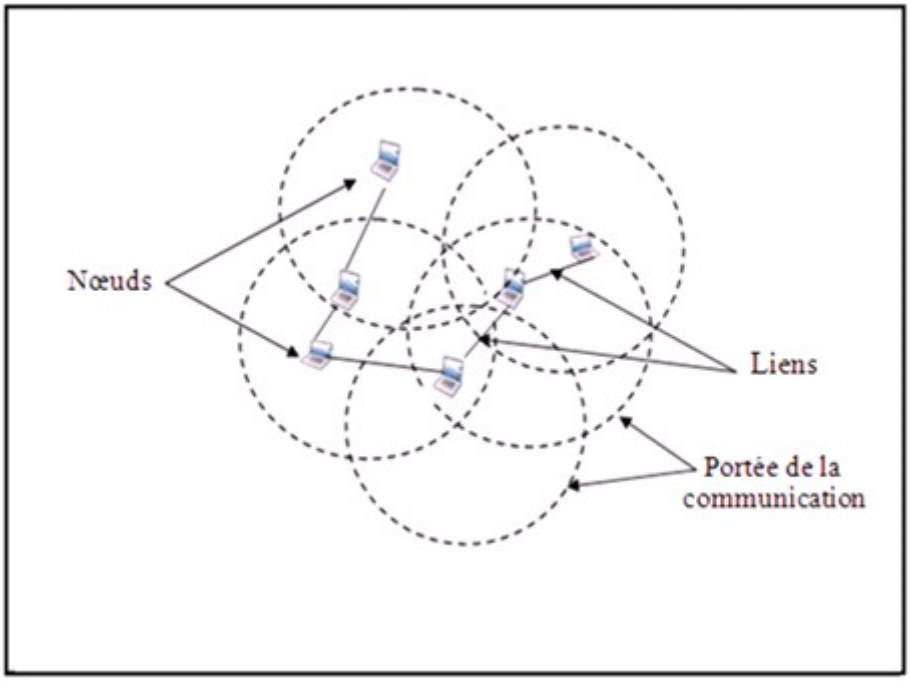

FIGURE 1.5 – Modélisation d'un réseau ad hoc

1.3.5 Domaines d'applications

Les réseaux mobiles ad hoc ont une très large palette d'utilisation. En effet, ils sont robustes, peu coûteux et s'adaptent aussi bien aux milieux urbains, qu'aux milieux ruraux. Parmi les applications de ces réseaux, nous citons [10] :

- **Applications militaires :** Les réseaux mobiles ad hoc ont été utilisés la première fois par l'armée. En effet, ce type de réseaux est la solution idéale pour maintenir une communication sur un champ de bataille entre les différentes unités de l'armée.
- **Opérations de secoures :** 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 secoures de communiquer.
- **Applications éducatives :** Le déploiement d'un réseau ad hoc lors d'une conférence ou d'une séance de cours est très judicieux car cela permet aux chercheurs et aux étudiants de partager des ressources (fichiers, accès à internet, etc.) et de communiquer sans avoir besoin d'une quelconque infrastructure.
- **Applications industrielles :** Les réseaux ad hoc sont largement utilisés dans le domaine industriel, un exemple d'une telle application est 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 leurs environnements afin de partager des informations dans le but de gérer et réguler le trafic routier. Les réseaux ad hoc sont alors la solution idéale.

1.4 Routage dans les réseaux mobiles ad hoc

Le routage est une méthode d'acheminement des information vers la bonne destination à travers un réseau de connexion donné, il consiste à assurer une stratégie qui garantit à n'importe quel moment un établissement de routes qui soient correctes et efficaces entre n'importe quelle paire de nœuds appartenants au réseau, ce qui assure l'échange des messages d'une manière continue. Vu les limitations des réseaux ad hoc, la construction des routes doit être faite avec un minimum de contrôle et de consommation de la bande passante [11].

1.4.1 Modes de communication

Comme illustré dans FIGURE 1.5, la communication dans les réseaux sans fil s'effectue selon trois modes :

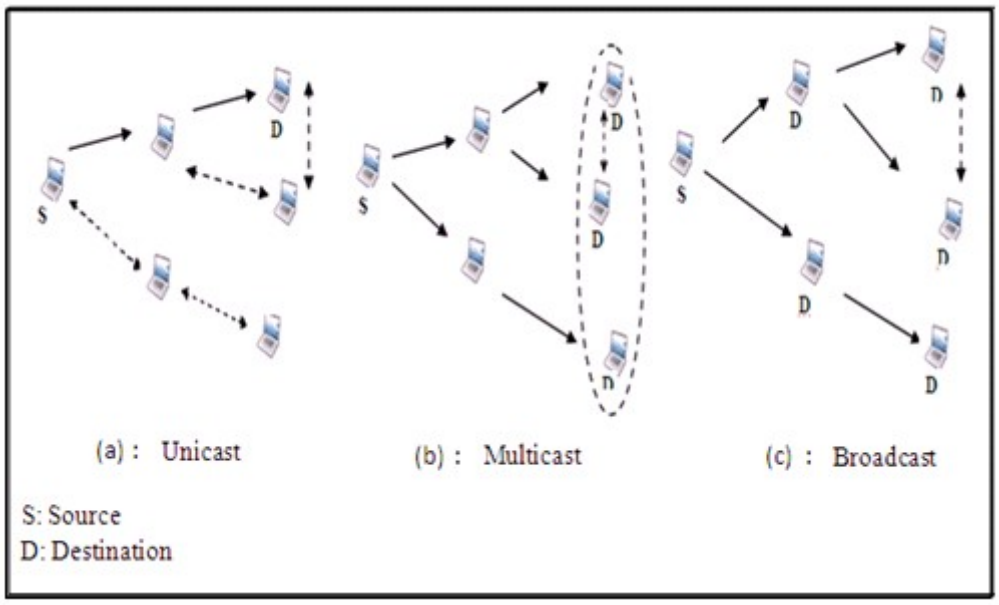

FIGURE 1.6 – Différents modes de communication

- **Communication unicast :** Dans ce mode, la communication se fait point à point, c'est-à-dire un seul nœud source communique avec un seul nœud destinataire (FIGURE 1.5 (a)).
- **Communication multicast :** Ou multipoints, dans laquelle un seul nœud source communique avec plusieurs nœuds destinataires.
- **Communication broadcast :** Ou diffusion, dans laquelle le message envoyé atteindra tous les nœuds du réseau.

1.4.2 Classification des protocoles du routage

D'une manière générale, toute stratégie du routage repose sur des méthodes et des mécanismes que nous pouvons regrouper en trois grandes classes (FIGURE 1.6) :

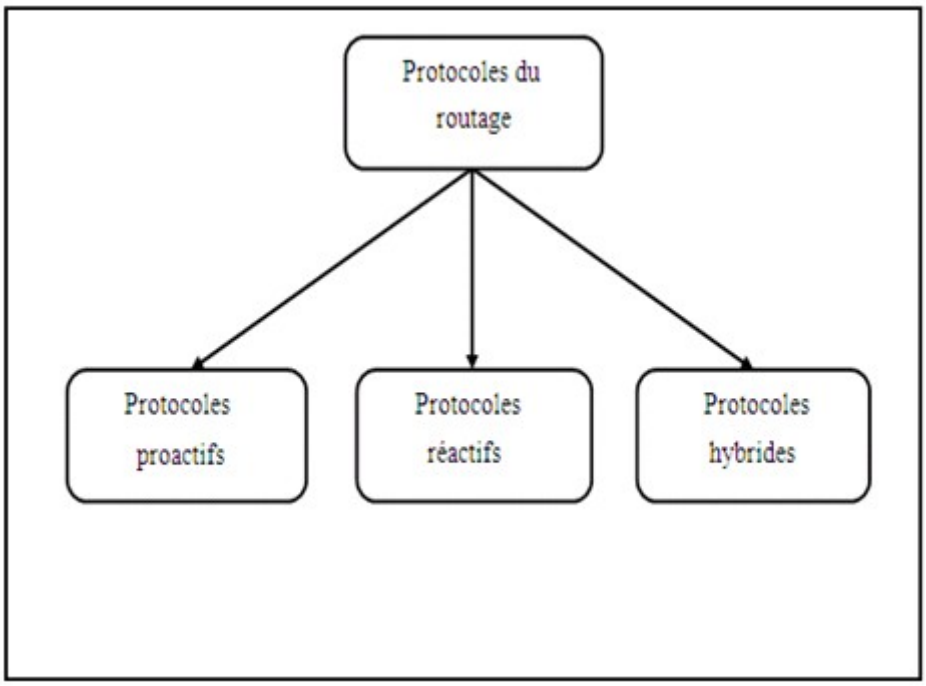

FIGURE 1.7 – Classification des protocoles du routage

Dans ce qui suit, nous allons décrire les différentes classes des protocoles du routage et souligner les avantages et les inconvénients de chacune de ces classes :

1.4.2.1 Protocoles du routage proactifs

Les protocoles du routage proactifs reprennent le principe du routage des réseaux filaires. Ils sont basés sur l'existence des tables de routage au niveau de chacun des nœuds. Lorsqu'un nœud du réseau souhaite envoyer un message, il consulte sa table de routage pour connaître la route à suivre jusqu'au destinataire du message.

Avec un protocole proactif, les routes sont disponibles immédiatement lors du besoin. Ainsi l'avantage d'un tel protocole est le gain du temps lors d'une demande de route. Le problème est que, les changements de routes peuvent être plus fréquents. Dans ce cas-là, le trafic induit par les messages de contrôles et de mise à jour des tables de routage peut être important. Le protocole le plus représentatif de cette catégorie est : OLSR (Optimized Link State Routing) [12].

1.4.2.2 Protocoles du routage réactifs

Les protocoles du routage réactifs ne maintiennent pas en permanence des tables du routage de l'ensemble du réseau. Lorsqu'un nœud a besoin d'envoyer un message vers un autre élément, il commence par déterminer une route lui permettant d'atteindre le

destinataire du message. Cette route sert à envoyer les informations et reste dans une table au niveau du nœud. Les nœuds du réseau n'ont donc qu'une vision partielle du réseau et ne connaissent que les autres éléments du réseau avec lesquels ils ont l'habitude de communiquer.

À l'opposé des protocoles proactifs, dans le cas d'un protocole réactif, aucun message de contrôle ne charge le réseau pour des routes inutilisées ; ce qui permet d'économiser la bande passante et l'énergie des nœuds. En contrepartie, la mise en place d'une route par inondation peut être coûteuse et engendrer des délais importants avant la découverte de la route. Le protocole AODV (Ad hoc On demand Distance Vector) est un exemple représentatif de cette catégorie [13].

1.4.2.3 Protocoles du routage hybrides

Les protocoles hybrides combinent les deux idées des protocoles proactifs et réactifs. Ils utilisent un protocole proactif, pour connaître les voisins les plus proches (par exemple voisinage à deux ou à trois sauts) et disposent des routes immédiatement dans le voisinage. Au-delà de cette zone prédéfinie, ils utilisent un protocole réactif pour chercher les routes vers des nœuds plus lointains.

Le protocole hybride est un protocole qui se veut comme une solution mettant en commun les avantages des deux approches précédentes en utilisant une notion de découpage du réseau. Cependant, il rassemble aussi les inconvénients des deux approches proactives et réactives. ZRP (Zone Routing Protocol) est un protocole représentatif de cette classe [1].

1.5 Conclusion

Dans ce chapitre, nous avons présenté les caractéristiques des réseaux sans fil ad hoc, ainsi que le routage dans de tels réseaux. À causes des caractéristiques inhérentes de ces réseaux, un vrai problème de sécurité se pose. Dans le chapitre suivant, nous allons mettre l'accent sur ce problème par la présentation des différentes attaques possibles ainsi que les solutions proposées dans la littérature pour se protéger contre ces attaques.

2

Sécurité dans les réseaux ad hoc

2.1 Introduction

Un réseau ad hoc est une collection de nœuds qui utilisent le médium de communication sans fil pour communiquer. Les caractéristiques d'un réseau ad hoc citées dans le chapitre précédent, rendent ce genre de réseaux vulnérable par plusieurs attaques. Malgré la diversité des solutions de sécurité proposées dans la littérature, le problème de sécurité reste toujours posé. Dans ce chapitre, nous allons mettre l'accent sur les différentes attaques possibles sur les réseaux ad hoc ainsi que les solutions proposées dans la littérature.

2.2 Vulnérabilités des réseaux ad hoc

Un réseau ad hoc est susceptible d'être attaqué par plusieurs attaques et ceci à cause des vulnérabilités suivantes [14] :

- **Absence d'infrastructure :** Les équipements de sécurité utilisés dans les réseaux traditionnels tels que les pare-feux ou les serveurs d'authentification ne peuvent pas être utilisés pour sécuriser un réseau ad hoc à cause de l'absence d'infrastructure.
- **Bande passante limitée :** À cause de la bande passante limitée, les communications peuvent facilement être perturbées. En effet, un attaquant peut occuper inutilement le support de communication pour empêcher la communication des nœuds légitimes. Il peut encore perturber la communication avec le bruit.
- **Liaison sans fil :** Quiconque possédant le récepteur adéquat peut potentiellement écouter ou perturber les messages échangés, à la différence dans les réseaux filaires où un attaquant doit gagner l'accès physique au câble pour mener son attaque.
- **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 des équipements fonctionnant avec une alimentation autonome.

2.3 Services de la sécurité

La sécurité d'un réseau sans fil ad hoc repose sur les services suivants [15] :

- **Authentification :** L'authentification consiste à s'assurer de l'identité d'un nœud.

Les nœuds, dans un réseau ad hoc, ont besoin de s'authentifier les uns des autres. L'authentification peut être assurée par les différents outils cryptographiques.

- **Confidentialité :** La confidentialité assure que les entités non autorisées ne peuvent jamais avoir accès à l'information en transit. La confidentialité peut être réalisée en utilisant la cryptographie.
- **Intégrité :** L'intégrité garantit que les informations communiquées entre les nœuds ne peuvent pas être modifiées ou altérés durant la transmission. L'intégrité peut être assurée par l'utilisation des fonctions de hachage.
- **Disponibilité :** La disponibilité consiste à assurer un accès et une utilisation effective et fiable du réseau pour toute entité autorisée. Elle est difficile à assurer dans les réseaux sans fil ad hoc étant données les contraintes qui pèsent sur ces réseaux (topologie dynamique, ressources limitées, etc.).
- **Non-répudiation :** La non-répudiation est le service qui assure qu'un nœud expéditeur ne peut pas nier l'envoi du message et le nœud récepteur ne peut pas nier la réception du message.
- **Contrôle d'accès :** Consiste à empêcher les nœuds non autorisés d'utiliser les ressources du réseau tels que les canaux de communication.
- **Anonymat :** Il est important dans certains cas, que l'identité des nœuds du réseau reste discrète. Pour assurer l'anonymat, l'identité d'un nœud est associée à un code, ceci implique la présence d'une autorité centrale pour stocker de manière sécurisée la correspondance identité/code.
- **Fraîcheur de données :** Même si l'authentification, l'intégrité et la confidentialité des données sont assurées, la fraîcheur de chaque message doit être également assurée. La fraîcheur des données permet de garantir que les données sont récentes et qu'aucun vieux message n'a été rejoué.

2.4 Attaques de sécurité

Plusieurs attaques peuvent être menées sur les différentes fonctionnalités des réseaux ad hoc. Dans ce qui suit nous allons mettre l'accent sur ces attaques.

2.4.1 Classification des attaques

La classification des attaques illustrée dans la FIGURE 2.1 est celle fréquemment trouvée dans la littérature et dans laquelle les attaques sont classées selon leurs sources en : externe ou interne, ou bien selon leurs effets en : passive ou active.

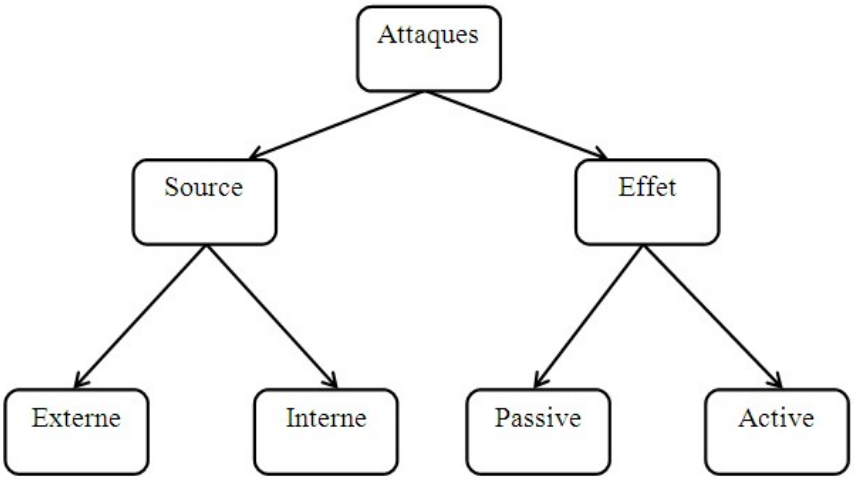

FIGURE 2.1 – Première classification des attaques

- **Attaques externes :** Une attaque externe est une attaque menée par un nœud malicieux qui ne fait pas partie du réseau. Par exemple, un groupe de nœuds qui partagent une clé pour chiffrer ou déchiffrer des messages échangés entre les membres du groupe. Une attaque externe consiste à prendre connaissance de la clé partagée afin de l'utiliser pour mener des attaques contre les membres du groupe.
- **Attaques internes :** Une attaque interne est celle menée par un nœud malicieux qui fait partie du réseau. Par exemple, un membre de ceux qui partagent une clé commune, lance des attaques pour perturber le bon fonctionnement du réseau.
- **Attaques passives :** Le but de cette attaque est limité à l'écoute et l'analyse du trafic échangé. L'attaquant tente d'espionner l'information qui circule dans le réseau et prive le réseau de la confidentialité du contenu des messages échangés.
- **Attaques actives :** Dans ce type d'attaques, l'attaquant se donnera les moyens pour altérer les messages qui circulent dans le réseau par suppression ou modification.

  Dans ce qui suit, nous allons décrire quelques-unes des attaques dans un réseau ad hoc.

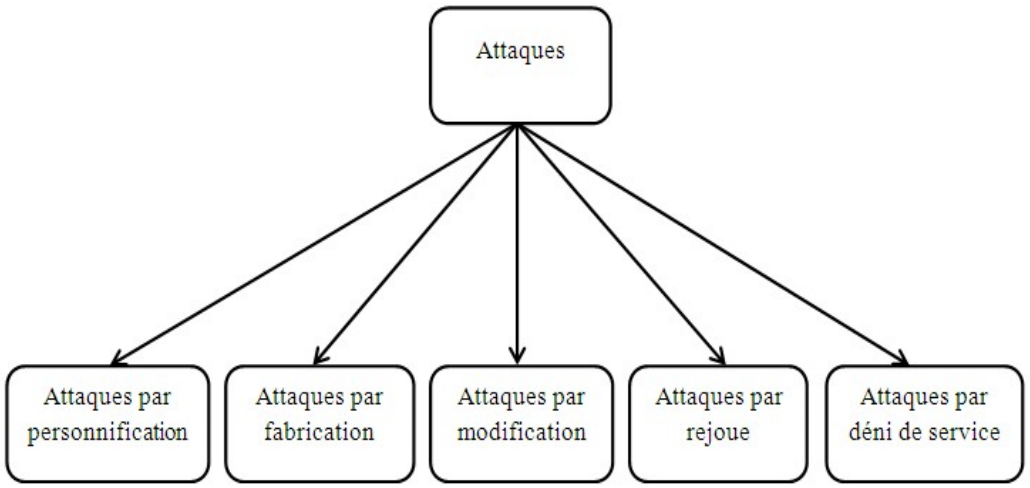

FIGURE 2.2 – Deuxième classification des attaques

2.4.1.1 Attaques par personnification

Dans ce genre d'attaques, l'intrus usurpe l'identité (adresse IP ou MAC par exemple) et les privilèges d'un autre nœud afin de mener son attaque dans le réseau. Ce type d'attaques peut être évité par l'utilisation de l'authentification. Cette catégorie d'attaques inclut :

- **Man in the Middle attack :** L'attaquant peut personnifier le récepteur et l'émetteur en se mettant entre les deux et de cette façon, il peut mener son attaque sans qu'aucun des deux ne puisse se rendre compte qu'ils ont été attaqués.
- **Spoofing attack :** Cette attaque consiste à usurper l'identité d'un autre nœud et l'utiliser pour envoyer des messages au nom du nœud victime.
- **Sybil attack :** L'attaquant usurpe des identités multiples existantes ou par la fabrication de nouvelles identités. Elle peut être simultanée ou non simultanée. Une attaque Sybil simultanée consiste à utiliser les fausses identités en même temps, tandis qu'une attaque Sybil non simultanée utilise les fausses identités à des instants différents.

2.4.1.2 Attaques par modification

Ces attaques consistent à modifier le contenu des paquets. Cette classe d'attaques inclut :

- **Misrouting attack :** Dans ce genre d'attaques, le nœud malicieux envoie des paquets à une fausse destination. Ce type d'attaques est effectué en modifiant

l'adresse finale de la destination des paquets.

- **Black mail attack :** L'attaque de Black mail cause une fausse identification en rendant malicieux des nœuds légitimes par l'insertion de ces derniers dans des listes noires utilisées pour garder la trace des nœuds malicieux. En conséquence, un nœud légitime sera vu par les autres nœuds du réseau comme étant un nœud malicieux et il sera évité dans une future communication.

2.4.1.3 Attaques par fabrication

Le nœud malicieux fabrique des messages et les insère dans le réseau afin de perturber les opérations de ce dernier ou pour consommer les ressources des nœuds. Cette classe peut inclure :

- **Routing table poisoning :** Le nœud malicieux envoie de fausses mises à jour du routage, il peut causer des congestions dans le réseau ou un partitionnement de ce dernier.
- **Black hole :** Le nœud malicieux supprime tous les paquets passant par lui. La conséquence d'une telle attaque peut être l'isolation de la destination des données.
- **Gray hole :** Cette attaque est presque similaire à la précédente, à la différence que les paquets sont supprimés sélectivement.

2.4.1.4 Attaques par rejoue

Dans cette classe d'attaques, l'attaquant a la possibilité de garder à sa possession des messages un certain temps et les rejouer plus tard, ou prendre des messages déjà diffusés dans une zone donnée et les rejouer dans une autre zone dans le réseau. Cette classe inclut :

- **Wormhole attack :** Le wormhole [15] est une attaque sophistiquée qui implique la coopération de deux nœuds malicieux pour capter le trafic dans un point donné dans le réseau et le rejouer dans un autre point du réseau.

2.4.1.5 Attaques par déni de service (DoS)

Cette classe d'attaques inclut toutes les attaques touchant à la disponibilité du réseau. Nous citons à titre d'exemple :

- **Consommation des ressources :** L'attaquant consomme les ressources du réseau (bande passante, mémoire, énergie, etc.) 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.

2.5 Contre-mesures de sécurité dans les réseaux ad hoc

Comme illustré dans la FIGURE 2.3, les contre-mesures de sécurité peuvent être classées en : contre-mesures sécurisées pour sécuriser des protocoles existants non sécurisés, ou des contre-mesures de sécurité conçues au départ en visant la sécurité comme premier objectif.

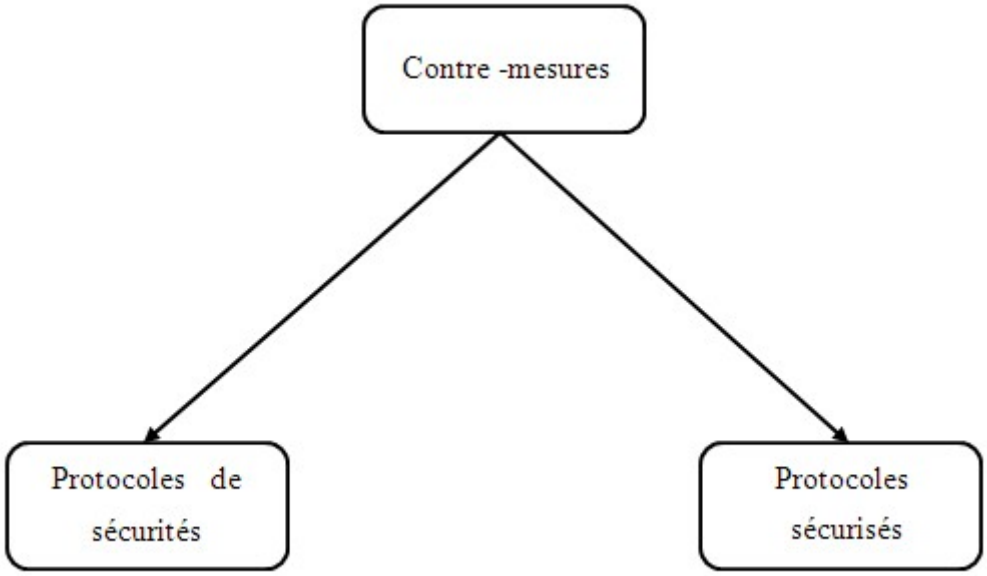

FIGURE 2.3 – Contre-mesures de sécurité

Dans ce qui suit, nous allons présenter quelques protocoles de sécurité.

2.5.1 Protocoles de sécurité

Dans cette classe, nous pouvons citer les protocoles suivants :

2.5.1.1 TESLA (Time Efficient Stream Loss tolerant Authentication)

Le protocole TESLA [16], 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 utilisée 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.

2.5.1.2 ARAN (Authenticated Routing protocol for Ad hoc Network)

Ce protocole, proposé par Sanzgiri et al.[17], se contente de l'authentification des nœuds de bout en bout par l'utilisation des certificats préétablis distribués par un serveur de confiance. Chaque nœud transmettant un message de demande de route, doit le signer. Le paquet de demande de route (RREQ, D, CertS, NS, t) kpriv(S) envoyé par le nœud source S à destination de D contient le certificat de l'émetteur CertS, une valeur aléatoire NS et un estampillage t. Ce paquet est signé à l'aide de la clé privée de la source kpriv(S). Le premier voisin recevant le paquet vérifie la validité de la signature et la validité du certificat de S avant de rajouter son certificat et signer le message avec sa signature.
Chaque nœud intermédiaire vérifie la signature et le certificat du nœud duquel il a reçu le message et les remplacent par sa signature et son certificat et ainsi de suite jusqu'à ce que le message atteigne la destination. L'inconvénient de cette méthode est qu'elle utilise

l'authentification saut par saut en vérifiant à chaque fois le certificat, ce qui augmente considérablement le calcul au niveau de chaque nœud ainsi que la taille des messages.

2.5.1.3 SAR (Security aware Ad hoc Routing protocol)

Le protocole SAR [18], se base sur la cryptographie symétrique. Il a été élaboré à l'origine pour prévenir les attaques du type " trou noir " qui consiste à supprimer l'intégralité des paquets au niveau d'un nœud malicieux. À l'instar des protocoles précédents, SAR est conçu pour être employé conjointement avec des protocoles réactifs tels qu'AODV ou DSR. Il utilise la notion de " niveaux de confiance " pour établir la sécurité d'un chemin. Ainsi, lorsqu'un nœud désire établir une route avec un certain niveau de sécurité, il génère un nouveau paquet RREQ indiquant le niveau de confiance requis. Par la suite, le mécanisme de découverte de routes diffère légèrement du schéma classique des protocoles réactifs dans le sens où seuls les nœuds satisfaisants le niveau de sécurité requis peuvent rediffuser la requête à leurs voisins ; dans le cas contraire, la requête est rejetée par le nœud. Une fois la route établie jusqu'à la destination, celle-ci génère en retour un paquet RREP avec le même niveau de sécurité. Dans l'éventualité, où aucune route en retour ne garantit le niveau de sécurité requis, celui-ci peut être ajusté par le nœud source. Cette approche implique de lier l'identité d'un nœud à un certain niveau de confiance. Pour se faire, il existe une clé secrète pour chaque niveau de sécurité défini et celle-ci doit être distribuée à tous les nœuds du réseau satisfaisants ce niveau de sécurité. Le contenu des paquets est ensuite chiffré par la clé de sorte que les nœuds du niveau inférieur ne puissent pas les lire. Cette capacité de partitionner le réseau en fonction des différents niveaux de sécurité fait de SAR un protocole original.

En contrepartie, il souffre de plusieurs défauts importants, le principal réside dans la distribution des clés. Celle-ci doit être éffectuée préalablement à la mise en place du réseau, par le biais d'un canal sûr. Ensuite, on peut imaginer que les nœuds de plus hauts niveaux de confiance sont utilisés pour distribuer les clés correspondantes à des niveaux inférieurs. Mais ceci ouvre la voie à des attaques sévères du type usurpation d'identité.

2.5.1.4 TIK (TESLA with Instant Key disclosure)

TIK [19], est un protocole dérivé de TESLA, spécialement conçu pour contrer les attaques du 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 (geographic leash) ou

sa durée de vie (temporal leash). 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 des chaines de hachage. Le nœud émetteur génère un MAC de la forme H(M, Ki) à l'aide d'un paquet 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_i dans l'arbre de hachage. Le MAC est inclus dans l'entête du message. Avant d'envoyer le paquet, le nœud estime une limite au temps d'arrivée du paquet et ajoute la clé K_i. Voici la composition du paquet : H(M, K_i), M, h_i, K_i. À l'arrivée, le nœud qui reçoit le paquet vérifie que la clé n'a pas été encore divulguée en se basant sur le temps t_i. Si tout est bon, le nœud destinataire authentifie la clé K_i en utilisant h_i et peut vérifier l'intégrité du message en comparant le MAC reçu avec celui calculé.

2.5.1.5 MAE (Manet Authentication Extension)

MAE [20], 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 à seuil, qui permet de distribuer la clé privée de CA. MAE présente les dispositifs habituels permettants 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.

2.5.2 Protocoles sécurisés

Ce sont des protocoles de sécurité conçus pour sécuriser des protocoles non sécurisés. Nous citons à titre d'exemple les protocoles suivants :

2.5.2.1 SAODV (Secure Ad hoc On demand Distance Vector)

Ce protocole a été proposé par Zapata et Asokan [21], pour sécuriser le protocole AODV. Son idée principale consiste à utiliser des signatures afin d'authentifier la plupart des champs des paquets " RREQ (Route Request) "et " RREP (Route Reply)" et d'utiliser des chaines de hachage pour protéger l'intégrité du compteur de sauts. Ainsi, SAODV constitue une extension d'AODV avec des signatures, afin de contrer les attaques du type " usurpation d'identité ". SAODV nécessite la présence d'une autorité de certification afin de vérifier les paquets signés, assurant ainsi leur authenticité. Dans SAODV, chaque paquet RREQ inclut une extension de signature simple. L'initiateur du paquet choisit

un nombre de sauts maximal en se basant sur une estimation du diamètre du réseau et génère ensuite une fonction de hachage à sens unique d'une longueur égale au nombre de sauts, plus un. Ce protocole assure une bonne authentification des messages de contrôle ainsi qu'une bonne intégrité.

Cependant, l'utilisation des chaines de hachage ne permet pas d'empêcher à 100% les attaques sur le compteur de sauts. Ainsi, bien que le hachage du nombre de sauts empêche un éventuel nœud malicieux d'annoncer des routes plus courtes qu'en réalité, rien n'empêche un attaquant d'augmenter arbitrairement la longueur de ces routes. En effet, un tel nœud peut appliquer la fonction de hachage plusieurs fois consécutives avant de relayer un paquet, la route apparaît ensuite plus longue qu'elle est en réalité.

2.5.2.2 SRP (Secure Routing Protocol)

Panagiotis et Haas ont proposé un protocole de routage sécurisé SRP [22], spécialement adapté aux caractéristiques du protocole DSR [23] et du protocole du routage ZRP [24]. Ainsi, ils ont conçu SRP comme une extension de l'en-tête des paquets RREQ et RREP. SRP utilise des numéros de séquence à l'intérieur des requêtes, de manière à garantir leurs fraîcheur. Cependant, ce numéro de séquence ne peut être vérifié qu'au niveau de la destination, il établit en outre des associations de sécurité, entre les nœuds communicants uniquement. Cette association est ensuite utilisée pour authentifier les paquets RREQ et RREP par le biais du MAC. Au niveau de la destination, SRP permet de détecter des modifications des paquets du type RREQ tandis qu'au niveau de la source, c'est l'intégrité des RREP qui sera vérifiée.

Puisque SRP ne nécessite des associations de sécurité qu'entre les nœuds communicants, il est relativement léger. En contrepartie, certains défauts ont assez pénalisé et limité son intérêt. Tout d'abord, SRP ne sécurise pas le mécanisme de maintenance des routes et délègue cette tâche à un autre protocole. De plus, SRP ne permet pas de détecter les modifications portant sur les informations du routage habituellement soumises à des modifications lors du routage. Par exemple, un nœud peut aisément corrompre, voire supprimer le contenu de la liste des nœuds comprise à l'intérieur d'un paquet du type RREQ. Enfin, l'intégrité des messages n'étant vérifiée qu'au niveau des nœuds source et destination.

2.5.2.3 SEAD (SEcure Ad hoc Distance vector routing)

SEAD [25], est un protocole sécurisé basé sur DSDV. Afin de trouver le chemin le plus court entre deux nœuds, les protocoles de routages du vecteur de distance utilisent une version distribuée de l'algorithme de Ballman-ford. Le protocole du routage SEAD utilise des chaines de hachage pour authentifier les compteurs de sauts et les numéros de séquences. Le protocole SEAD propose deux méthodes différentes afin d'authentifier la source de chaque mise à jour du routage. La première méthodes exige la synchronisation d'horloge entre les nœuds qui participent au réseau ad hoc, et utilise des mécanismes d'authentification d'émission tels que TELSA. La deuxième méthode exige l'existence d'un secret partagé entre chaque paire de nœuds. Ce secret peut être utilisé afin d'employer un MAC entre les nœuds qui doivent authentifier un message de la mise à jour du routage.

2.5.2.4 CONFIDANT

CONFIDANT est un protocole proposé par Buchegger et Boudec, qui a pour objectif de détecter et d'exclure les nœuds malicieux dans un réseau ad hoc. Il est composé de plusieurs modules :

- **Contrôleur :** Son rôle est de collecter des informations sur le comportement des nœuds dans le réseau. En écoutant le canal radio, ce module vérifie autant que possible que ses voisins se comportent bien en termes de participation au protocole du routage et de retransmission des paquets. Les observations servent à classifier directement un nœud comme bienveillant ou malveillant.
- **Système de réputation :** Il se charge de combiner les informations en une réputation locale sur chacun des nœuds, qui sert à son tour de décider si un nœud doit être considéré comme malicieux.
- **Gestionnaire de confiance :** C'est le module qui décide à quel moment un message d'alarme doit être envoyé aux autres nœuds de confiance afin de les avertir du comportement malicieux d'un nœud. C'est aussi lui qui décide si le contenu d'un message d'alarme doit être considéré ou ignoré.
- **Gestionnaire des chemins :** Il manipule la topologie vue par le nœud en fonction des degrés de confiance des autres nœuds afin d'exclure les nœuds malicieux du réseau.
- **Protocole du routage :** Il exploite l'information de la topologie pour trouver des chemins valides et fiables. Il se base sur le système de réputation pour refuser

des paquets en provenance des nœuds malicieux.

Le tableau suivant récapitule les solutions citées auparavant.

Protocoles	**Mécanismes de sécurité**	**Commentaires**
ARAN	Autorité de certification, cryptographie asymétrique et estampillage temporel.	Assure l'authentification, la non répudiation, l'intégrité et contre le rejoue de bons messages.
TESLA	Les MACs et les chaines de hachage.	Assure l'authentification et l'intégrité.
SAR	Utilise le niveau de confiance pour définir le meilleur chemin.	Contre l'attaque du trou noir, n'utilise pas le court chemin mais le chemin le plus sûr.
SRP	Les MACs.	Assure une sécurité de bout en bout.
SEAD	Chaines de hachage.	Détecter l'attaquant qui modifie le numéro de séquence ou le compteur de sauts.
CONFIDANT	Le contrôleur,le système de réputation,le gestionnaire de confiance,le gestionnaire des chemins et le protocole du routage.	Détecter et éliminer les nœuds malicieux.

SAODV	La signature numérique et les chaines de hachage.	Assure l'authentification des paquet RREQ et RREP, assure l'intégrité du compteur de sauts et contre les attaques du type usurpation d'identité.
TIK	L'arbre de hachage	Contre l'attaque du trou de ver.
MAE	La certification des clés publiques et la gestion de la révocation des certificats.	Distribuer la clé privée de l'autorité de certification (CA).

TABLE 2.1 – Tableau récapitulatif des différentes contre-mesures proposées

2.6 Conclusion

Dans ce chapitre, nous avons présenté un état de l'art sur la sécurité dans les réseaux ad hoc, dans lequel nous avons énuméré les différentes attaques possibles ainsi que les solutions rapportées dans la littérature. Dans le chapitre suivant, nous allons présenter l'attaque d'interférence (Jamming attack) qui est notre sujet d'étude.

3

Attaque d'interférence dans les réseaux ad hoc

3.1 Introduction

De nombreuses menaces de sécurité dans les réseaux sans fil ne sont pas en mesure d'être correctement traitées par des méthodes de sécurité classiques. Une classe de telles menaces constitue des attaques d'interférence ou du brouillage dans lesquelles le médium de communication partagé est occupé par des paquets injectés par un nœud malicieux, dans le but de monopoliser la communication. Ces attaques sont faciles à mener à cause de l'ouverture du médium de communication. En effet, les nœuds malicieux peuvent facilement observer les communications, et peuvent aussi facilement lancer des attaques de déni de service par l'injection de faux messages. La conséquence d'une telle attaque peut être la surcharge du support sans fil et l'empêchement d'autres nœuds de communiquer entre eux. Dans ce qui suit, nous allons présenter les différents types de l'attaque d'interférence, ainsi que les techniques proposées dans la littérature pour détecter et prévenir une telle attaque.

3.2 Définition de l'attaque d'interférence

Bien que plusieurs études aient focalisé sur l'attaque d'interférence, la définition de ce type d'attaques reste encore ambiguë. Une hypothèse courante est que le brouilleur de signaux RF (Radio Frequency) émet en permanence du bruit pour remplir un canal sans fil, de sorte que la circulation des paquets légitimes sera complètement bloquée. Cependant, un large éventail de comportements peut être adopté par un brouilleur pour mener son attaque. Par exemple, un brouilleur peut rester silencieux quand il n'y a aucune activité sur le canal, et de commencer les interférences dès qu'il détecte une activité de transmission sur le canal [26]. La caractéristique commune à toutes les attaques du brouillage est que leurs communications ne sont pas conformes avec les protocoles MAC sous-jacents. Par conséquent, un brouilleur peut être défini comme une entité qui essaie d'interférer avec la transmission et la réception dans une communication sans fil. Un brouilleur peut atteindre cet objectif, soit en prévenant la source du trafic de l'envoi des paquets, ou en empêchant la réception des paquets légitimes par le destinataire.

Selon la couche sur laquelle le brouillage est effectué, la littérature distingue :

- **Brouillage physique :** L'interférence physique, appelée aussi par radio, dans un milieu sans fil est une forme simple d'attaque DoS au niveau physique, dans laquelle l'attaquant émet en continu des signaux radios ou il envoie des bits aléatoires sur le canal de communication. Son objectif est de monopoliser le canal est d'empêcher les nœuds légitimes d'y accéder [26].
- **Brouillage virtuel :** Dans un réseau sans fil, les protocoles MAC écoutent le canal de communication pour déterminer la disponibilité de ce dernier et accorder la possibilité de transmission au nœud émetteur en conséquence. Le brouillage au niveau MAC peut être lancé en violant les protocoles MAC sous-jacents pour occuper constamment le canal de communication. L'avantage du brouillage au niveau MAC est que le brouilleur consomme moins d'énergie comparativement avec le brouillage au niveau physique [26].

3.3 Caractéristiques et critères d'efficacité d'un brouilleur

La finalité du brouillage est de monopoliser le canal afin d'empêcher les nœuds légitimes d'y accéder. Il peut être accompli soit par l'empêchement du nœud émetteur de transmettre correctement ses paquets et ceci par l'occupation continue du canal de communication. Il peut aussi entraver le récepteur de recevoir correctement les paquets qui lui sont destinés, et ceci par l'injection du bruit dans les paquets transmis. Dans le but de mesurer le degré d'efficacité d'un brouilleur, deux métriques de grande importance sont considérées :

- **Taux de paquets envoyés :** Appelé aussi PSR (Packet Sent Ratio), est défini comme étant le rapport entre le nombre de paquets envoyés avec succès par une source du trafic et le nombre de paquets que cette source a l'intention d'envoyer. Plus ce ratio est petit, plus le brouillage est efficace. Le PSR peut être facilement mesuré par un appareil sans fil en gardant la trace du nombre de paquets qu'il a l'intention d'envoyer et le nombre de paquets qui sont envoyés avec succès.

  PSR =Nombre de paquets envoyés avec succès/Nombre total de paquets à envoyer

  .
- **Taux de paquets délivrés :** Appelé aussi PDR (Packet Delivered Ratio), est

défini comme étant le rapport entre le nombre de paquets délivrés au destinataire et le nombre de paquets envoyés par l'expéditeur.

PDR =Nombre de paquets reçus /Nombre de paquets envoyés.

3.4 Modèles d'attaque d'interférence

Comme illustré dans la FIGURE 3.1, il existe de nombreuses stratégies d'attaques qui peuvent être employées par le brouilleur dans le but d'interférer avec d'autres communications sans fil. Ces différentes stratégies d'attaques auront différents niveaux d'efficacité. Dans ce qui suit, nous allons les décrire brièvement :

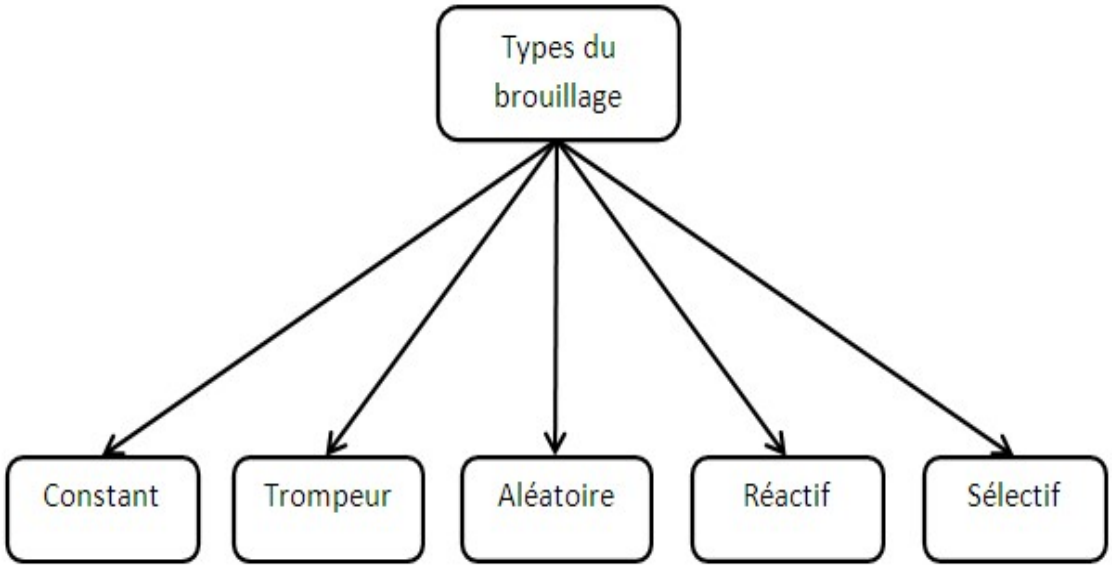

FIGURE 3.1 – Types du brouillage

- **Brouillage constant :** Le brouillage constant consiste à envoyer continuellement un signal radio sur le canal de communication. Il peut être implémenté soit par l'utilisation d'un générateur d'ondes qui envoie continuellement un signal radio, ou par l'utilisation d'un appareil sans fil qui envoie des bits aléatoires sans respecter le protocole MAC sous-jacent. Ce dernier, dans le cas normal, permet l'envoi des paquets si le canal de communication est libre. Ainsi, un brouilleur constant peut effectivement empêcher le trafic légitime d'être envoyé sur le canal de communication.
- **Brouillage trompeur :** Au lieu d'envoyer continuellement des bits aléatoires sur le canal de communication, le brouillage trompeur consiste à injecter des paquets réguliers dans le canal de communication sans interruption. Ce comportement fait

croire à un nœud légitime que le canal de communication est occupé par un trafic légitime. En conséquence, le nœud légitime se met en attente jusqu'à ce que le canal soit libre.

- **Brouillage aléatoire :** Au lieu d'envoyer continuellement un signal radio, le brouilleur aléatoire alterne entre le brouillage et le sommeil, i.e., après le brouillage pendant un certain temps, le brouilleur éteint son module radio et entre en sommeil, puis il reprend le brouillage après un certain temps du sommeil aléatoire. Durant la phase du brouillage, le brouilleur peut se comporter comme un brouilleur constant ou trompeur. Ce type de brouillages prend en considération l'énergie, i.e., il alterne entre le mode sommeil et le brouillage pour conserver son énergie le plus longtemps possible afin que son brouillage dure plus de temps.
- **Brouillage réactif :** Dans les trois types cités auparavant, le brouillage est dit actif. Il est actif dans le sens où le brouilleur essaie de bloquer le canal de communication. Une méthode alternative pour interférer avec des communications sans fil est d'utiliser une stratégie réactive, i.e., le brouilleur reste inactif s'il détecte un canal libre et à la détection d'une activité sur le canal, il commence son brouillage. Ce type de brouillages est plus difficile à détecter que les autres types [27].
- **Brouillage sélectif :** Dans ce type d'attaques, le brouilleur cible des paquets spécifiques de grande importance par l'exploitation de ses connaissances des détails d'implémentation des protocoles de communication au niveau des différentes couches de la pile protocolaire. Un exemple typique peut être l'attaque jamming des paquets d'acquittement utilisés pour acquitter la bonne réception des paquets de données [28].

3.5 Techniques de détection de l'attaque d'interférence

Les techniques de détection de l'attaque d'interférence proposées dans la littérature sont multiples. Ces techniques se focalisent sur l'attaque d'interférence menée soit au niveau de la couche MAC ou la couche physique. Dans ce qui suit, nous allons décrire les différentes techniques proposées dans la littérature et schématisées dans la FIGURE 3.2.

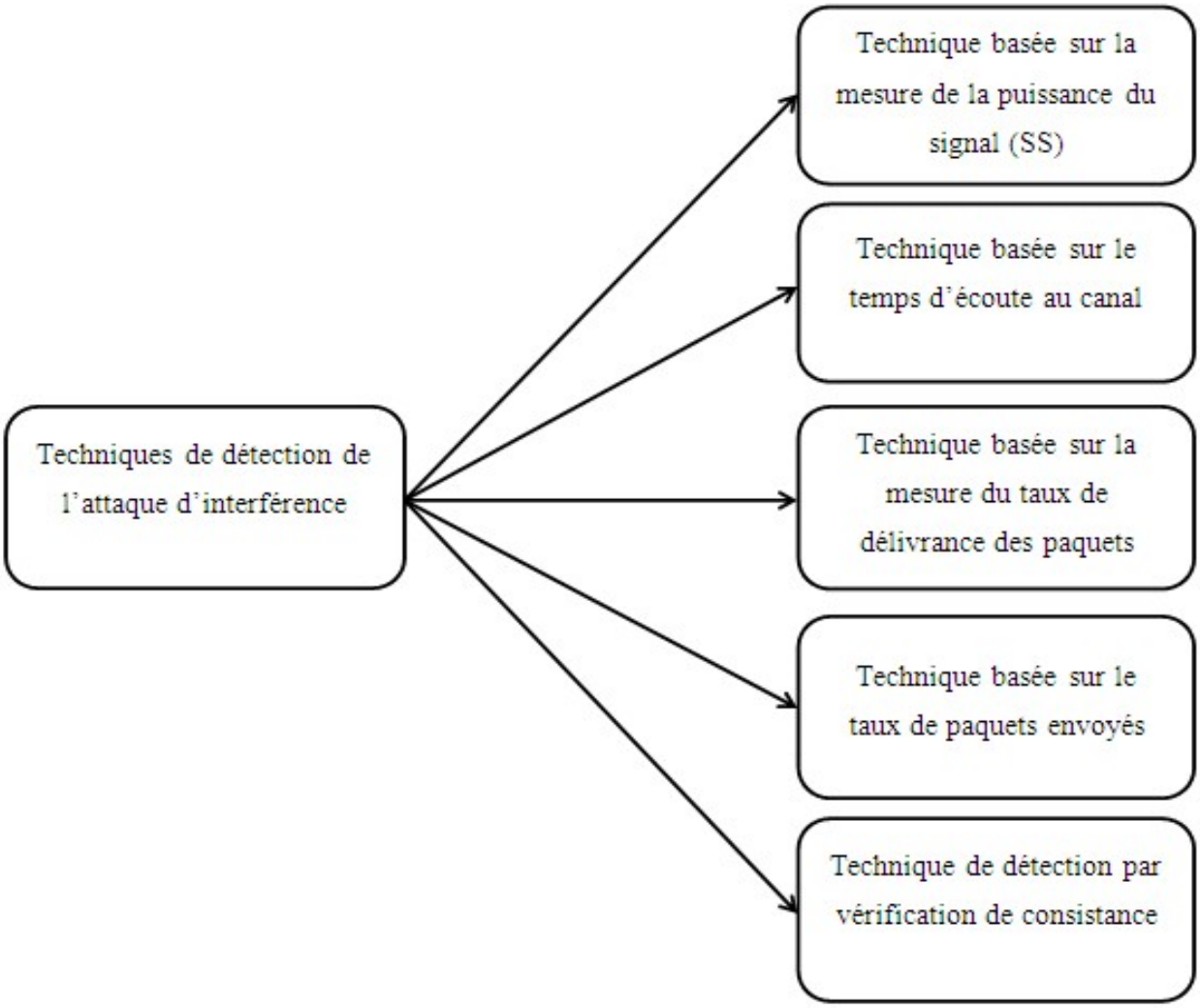

FIGURE 3.2 – Techniques de détection de l'attaque d'interférence

3.5.1 Technique basée sur la mesure de la puissance du signal

L'une des techniques utilisées pour détecter l'interférence est la mesure de la puissance du signal utilisé pour véhiculer l'information sur le support de communication. Cette technique est basée sur la constatation que la distribution du signal peut être affectée par le brouillage. Elle consiste donc à comparer la moyenne de la magnitude du signal avec un seuil calculé à partir du niveau du bruit ambiant. Une valeur moyenne de la magnitude du signal supérieure au seuil calculé signifie qu'un brouilleur est présent sur le canal de communication. Cette technique simple peut détecter le brouillage causé par l'envoi en continu d'un signal dont la puissance est différente à celle du signal utilisé pour véhiculer les paquets, mais elle ne peut pas détecter le brouillage trompeur ; par exemple, dans lequel un brouilleur occupe continuellement le canal par l'injection des paquets réguliers sans interruption, i.e., le brouilleur utilise le même signal utilisé pour transmettre un trafic

légitime [27].

3.5.2 Technique basée sur le temps d'écoute au canal

Un brouilleur garde le canal de communication continuellement occupé rien que pour empêcher la transmission ou la réception du trafic légitime. Un nœud légitime écoute d'abord le canal de communication et il ne commence la transmission que si le canal est libre. Cette constatation peut être utilisée pour détecter la présence d'un brouilleur sur le canal. Donc un nœud légitime se met en écoute au canal de communication et s'il constate que le temps d'écoute est trop important, il conclura que le canal est attaqué. Bien que simple et logique, cette technique peut conduire à une fausse détection. En effet, un temps d'écoute important peut être le résultat d'une congestion sur le canal de communication, ceci mène un nœud légitime à conclure que le canal est attaqué, mais en réalité le canal est congestionné. En outre, cette technique ne pourra pas détecter le brouillage aléatoire dans lequel un brouilleur alterne entre l'action du brouillage et le sommeil avec des durées aléatoires.

3.5.3 Technique basée sur la mesure du taux de délivrance des paquets

Le taux de délivrance des paquets est le rapport entre le nombre de paquets reçus avec succès et le nombre total de paquets envoyés. Cette mesure peut être utilisée pour détecter le brouillage sur le canal de communication. En effet, en mesurant le taux de délivrance des paquets, un nœud légitime peut déduire que le canal est attaqué s'il constate que ce taux est trop faible. Cette technique est bien limitée dans la mesure où un taux de délivrance des paquets faible peut être le résultat d'un canal congestionné à cause d'un trafic intense dans le réseau. Donc cette technique peut conduire à une fausse détection, plus particulièrement, dans un réseau fortement chargé [27].

3.5.4 Technique basée sur le taux de paquets envoyés

Le taux de paquets envoyés dénote le rapport entre le nombre de paquets envoyés avec succès et le nombre de paquets à envoyer. Cette mesure peut être utilisée pour détecter la présence d'un brouilleur sur le canal de communication. En effet, le nœud émetteur peut détecter le brouillage suite à la constatation d'un taux faible de paquets

envoyés. Aussi, cette technique peut conduire à une confusion parce qu'un taux de paquets envoyés faibles peut être le résultat de la congestion du réseau.

À noter que ces techniques peuvent être combinées pour avoir une technique plus efficace et précise pour détecter l'attaque d'interférence [27].

3.5.5 Technique de détection par vérification de consistance

Dans les techniques de détection précédentes, nous constatons que nous sommes incapables de détecter le type de l'attaque jamming , en plus, une valeur faible du PDR ne nous permet pas de différencier entre les scénarios du jamming et de congestion du réseau. Pour remédier à cette incapacité et améliorer la précision de la détection basée sur PDR, deux stratégies de détection sont envisageables. La première stratégie consiste à considérer la mesure du SS (puissance du signal) conjointement avec la mesure du PDR pour vérifier la consistance entre les deux mesures. À noter que cette technique s'applique entre un nœud et ses voisins, par laquelle le nœud détecte s'il est interféré et il n'est pas responsable des autres voisins [27]. L'objectif de cette technique est de vérifier si une valeur faible du PDR est consistante avec la valeur SS mesurée. Dans un scénario normal sans interférence, une forte valeur (respectivement faible) du SS correspond à une forte valeur (respectivement faible) du PDR. Par contre, une faible valeur du PDR n'implique pas une faible valeur du SS. Dans le cas du jamming, la valeur consistante à une valeur faible du PDR est bien une valeur forte du SS. La deuxième stratégie de détection consiste à augmenter la mesure du PDR par l'utilisation de la mesure de la position. En se basant sur l'information de la position, cette stratégie exploite le fait que les nœuds voisins proches à un nœud particulier ont un PDR fort et si le nœud constate que le PDR des nœuds voisins est faible alors il conclut que le canal est interféré [29].

3.6 Techniques de prévention de l'attaque d'interférence

Dans cette section nous allons présenter les différentes méthodes proposées dans la littérature pour éviter les attaques de jamming, ces méthodes incluent celle pour éviter le jamming au niveau physique et celle au niveau MAC comme illustré dans la FIGURE 3.3.

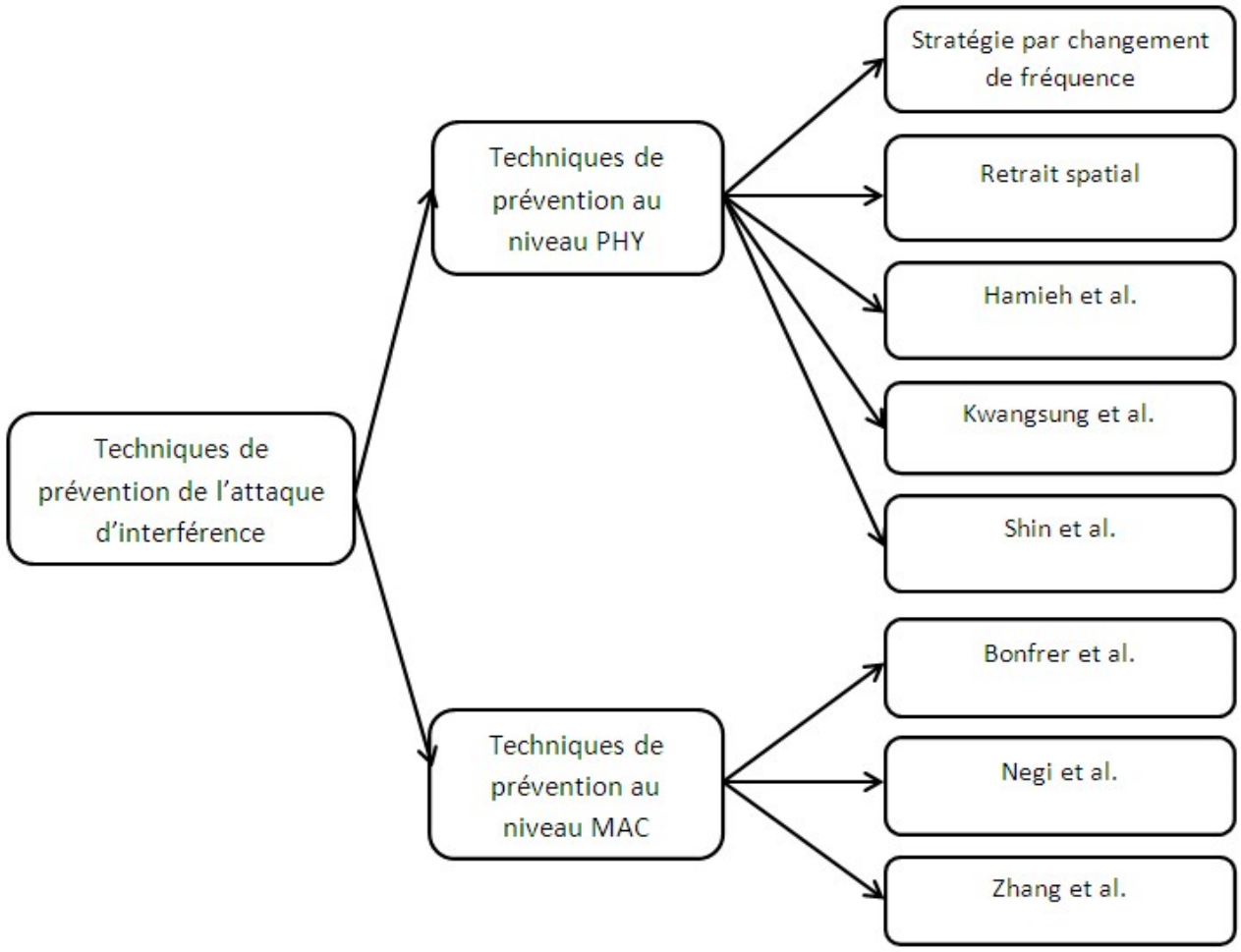

FIGURE 3.3 – Techniques de prévention de l'attaque d'interférence

3.6.1 Stratégie par changement de fréquence

Quand un nœud détecte qu'il est interféré, il change le canal et envoi un massage pour annoncer sa présence dans un nouveau canal, les nœuds frontières qui ne sont pas interférés mais qui sont voisins des nœuds interférés vont découvrir l'absence de leurs voisins dans le canal originale et explorer le prochain canal s'ils sont encore proches. Si le nœud détecte un message au niveau du canal récent, il revient au canal original et transmet un message pour informer le réseau entier de son changement.

L'inconvénient de cette stratégie pour les réseaux ad hoc est qu'elle exige l'utilisation des messages de flooding pour annoncer le changement du canal à travers le réseau ad hoc entier [27].

3.6.2 Retrait spatial

La deuxième stratégie est le retrait spatial dans laquelle les nœuds jammés essayent de se déplacer pour s'éloigner de la zone jammée ; cette solution s'applique pour des nœuds mobiles. Suite au déplacement des nœuds jammés, une restructuration du réseau est nécessaire pour reconstruire la topologie du réseau. À noter que la manière dont se déplacent les nœuds pour éviter le jamming peut causer la déconnexion de certains nœuds et le partitionnement du réseau en conséquence.

3.6.3 Hamieh et al.

Dans [30], les auteurs s'intéressent au jamming réactif, dont lequel le jammer est actif seulement quand il détecte une activité sur le canal. De cette manière le jammer sauvegarde d'avantage son énergie et diminue la probabilité d'être détecté. Pour différencier ce scénario d'attaque par rapport au scénario légitime, la solution mesure la dépendance entre les périodes de la réception correcte ou erronée. En effet, l'accès au canal par le jammer est dépendant de l'accès à ce même canal par les nœuds actifs, ainsi cette mesure de dépendance est plus grande dans le cas de l'attaque jamming que dans le cas normal. Pour mesurer cette dépendance, la solution utilise le coefficient de corrélation qui est une mesure statistique de la relation entre deux variables aléatoires définie comme suit : CC=(cov(X,Y))/(&X,&Y). La valeur du CC est comprise entre -1 et 1, une valeur proche de -1 ou 1 signifie une forte corrélation entre les deux variables, i.e., les deux variables sont reliées par une équation linéaire de la forme Y=a*X+b. Une valeur proche de 0 indique l'absence d'une relation entre les deux variables. Ce coefficient de corrélation est exploité dans la solution proposée en mesurant la probabilité d'erreurs(PE) et le coefficient de corrélation(CC). Ainsi, si CC est plus grand que PE alors une attaque jamming réactive s'est produite

3.6.4 Kwangsung et al.

Dans [31], les auteurs s'intéressent au jamming aléatoire et proposent une solution à la fois détective et préventive. La détection se fait en mesurant le PDR (taux de délivrance des paquets) et le SS (puissance du signal). Dans un scénario normal sans interférence, une valeur grande du SS correspond à une valeur grande du PDR, en plus, si la valeur du SS est petite alors la valeur du PDR le sera aussi. Par contre, une petite valeur du PDR n'implique pas nécessairement une petite valeur du SS. L'observation clé ici, est que

dans le cas d'interférence, la valeur du SS doit être grande et la valeur du PDR petite. En utilisant cette observation, chaque nœud compare les valeurs (PDR, SS) avec les valeurs seuils du PDR et SS. Si la valeur SS mesurée est plus grande que le SS seuil et la valeur PDR mesurée est plus petites que le PDR seuil alors le canal est interféré. Les valeurs SS et PDR seuils sont déterminées par simulation.

Pour éviter l'attaque jamming, les auteurs proposent un schéma qui assure un taux de transmission adaptatif pour assurer une utilisation plus efficace des liens de communication, en se basant sur la probabilité de transmission avec succès.

3.6.5 Shin et al.

Dans [32], les auteurs s'intéressent au jamming réactife et proposent une solution de sécurité basée sur l'identification des nœuds déclencheurs (ceux qui activent l'attaque jamming). Ce qui leur permet de concevoir un protocole du routage qui offre la possibilité de basculer ces nœuds déclencheurs en des nœuds récepteurs, en évitant ainsi l'activation des jammers et l'attaque de jamming en conséquence.

3.6.6 Bonfrer et al.

Les auteurs dans [33], développent un schéma de sécurité contre l'attaque jamming dans un réseau utilisant le protocole LMAC (Lightweight Medium Access Control). Ce dernier se base sur TDMA (Time Division Multiple Access) où le temps est divisé en cycles et chaque cycle est divisé en slots. Chaque slot est occupé par un nœud pour transmettre soit des messages de contrôles ou de données. Pour mener son attaque, un jammer écoute le canal pour déterminer le début du slot et sa taille, ensuite il se synchronise pour envoyer ses paquets en même temps que les paquets des autres nœuds, créant ainsi une interférence avec le trafic légitime. Pour remédier à cette attaque, les auteurs proposent un protocole LMAC modifié pour empêcher le jammer de déterminer avec exactitude le début et la taille du slot. Pour cela, ils translatent le début du slot avec une durée aléatoire, de cette façon, le jammer peut déterminer le début du slot mais pas la taille de ce dernier.

3.6.7 Negi et al.

Dans [34], les auteurs se focalisent sur l'attaque jamming qui exploite le paquet RTC pour réserver le canal de communication durant une période de M slots de temps. Durant cette période réservée par le jammer, le canal de communication est réellement libre mais

les nœuds légitimes ne peuvent y accéder car supposé occupé pour eux. Pour remédier à ce comportement malicieux, les auteurs proposent d'utiliser un nouveau message de contrôle envoyé périodiquement (chaque K slots) par le point d'accès dès qu'il détecte l'absence d'une activité sur le canal de communication.

3.6.8 Zhang et al.

Dans cette solution [28], les auteurs s'intéressent à l'attaque jamming contre les paquets d'acquittements. Le fonctionnement normal des protocoles MAC exige que les paquets de données doivent être acquittés par le récepteur avant d'être supprimés de la file d'attente de l'émetteur. Une attaque jamming travaillant pour s'interférer avec les paquets d'acquittement peut causer de sérieux dégâts dans le réseau. En effet, la perte des paquets d'acquittement à cause de l'interférence, provoque la retransmission des paquets. Ces derniers seront supprimés de la file d'attente de l'émetteur une fois le nombre de retransmission limite est atteint ; en plus, ces retransmissions bloquent le canal pour véhiculer d'autres paquets de données. Dans cette attaque, le jammer essaye d'écouter le canal de communication partagé et dès qu'il détecte une activité sur le canal (i.e. un paquet qui vient d'être déposé sur le canal en vue de le transmettre), il attend un certain temps (SIFS : Short Inter Frame Spacing), ensuite il envoie un petit paquet. Ce dernier va s'interférer avec le paquet d'acquittement qui vient d'être envoyé par l'émetteur. Pour éviter cette situation, les auteurs envisagent d'élargir la fenêtre de transmission de l'acquittement, en augmentant ainsi la probabilité de réception de l'acquittement par l'émetteur.

Techniques	**Niveaux**	**Limites**
Stratégie par changement de fréquence	PHY	Une fois l'attaque se produit, les nœuds doivent se synchroniser sur un autre canal, ce qui cause une innodation (flooding) du réseau.
Retrait spatial	PHY	Possibilité du partitionnement du réseau suite au déplacement des nœuds.
Hamieth et al.	PHY	Il s'agit d'une solution détective et non pas préventive.
Kwangsung et al.	PHY	C'est une solution pour éviter le jamming aléatoire, non utilisable pour détecter les autres types d'attaques jamming.

Shin et al.	PHY	Un overhead de communication et de calcul important.
Bonfrer et al.	MAC	Temps de latence important et une synchronisation entre les nœuds exigée.
Negi et al.	MAC	L'attaque ne peut pas être prévenue si le jammer réserve le canal durant M slots de temps avec M < K.
Zhang et al.	MAC	L'augmentation de la fenêtre de transmission d'ACK conduit à l'augmentation du temps de latence.

TABLE 3.1 – Tableau récapitulatif des techniques de prévention de l'attaque d'interférence

3.7 Conclusion

Dans ce chapitre, nous avons présenté un état de l'art sur l'attaque d'interférence, dans laquelle un nœud envoie un signal ou injecte des paquets dans le médium de communication partagé pour s'interférer avec les communications légitimes ; cette attaque peut

être menée soit au niveau PHY ou MAC. Différents types d'attaques jamming peuvent avoir lieu : constant, aléatoire, trompeur, réactif ou sélectif. Les techniques de détection se basent généralement sur des mesures telles que : PDR, PSR et SS. Les contre-mesures de sécurité pour se protéger contre cette attaque sont multiples, elles ciblent l'attaque jamming menée soit au niveau PHY ou MAC. Bien que multiples, ces contre-mesures ne protègent pas d'une manière efficace et robuste contre l'attaque de jamming, ce qui motive notre solution de sécurité qui sera présentée dans le chapitre suivant.

4

Solution de sécurité basée sur le changement du canal

4.1 Introduction

L'interférence, le brouillage ou le jamming est une attaque de déni de service qui peut être lancée soit au niveau PHY ou MAC de la pile protocolaire. Dans le premier cas, le brouilleur diffuse des signaux bruits pour s'interférer avec les signaux représentant le trafic légitime. Dans le deuxième cas, le brouilleur ne respecte pas le protocole MAC utilisé pour ordonnancer l'accès au support de transmission. Ceci par l'envoi des paquets sur le canal de communication pour faire croire aux autres nœuds que le canal est occupé. La conséquence d'une telle attaque est l'empêchement des autres nœuds de communiquer. À signaler que cette attaque peut être lancée avec un minimum de ressources en termes d'énergie et de capacité de calcul. La littérature propose plusieurs mécanismes de détection et/ou prévention de cette attaque en se basant essentiellement sur des mesures telles que PDR, PSR et SS. Bien que multiples, ces mécanismes restent insuffisamment efficaces et robustes, ce qui motive notre solution de sécurité contre l'attaque d'interférence qui fait l'objet de ce chapitre.

Dans ce qui suit, nous allons d'abord introduire le modèle du réseau sur lequel notre solution est implémentée, nous présentons ensuite un certain nombre d'hypothèses relatives à la faisabilité de notre solution et enfin nous détaillons notre solution et discutons les résultats de la simulation.

4.2 Modèle du réseau

Le réseau, dans lequel notre solution est implémentée, est une collection de nœuds qui partagent un médium de communication sans fil pour communiquer entre eux (FIGURE 4.1). Ce support de communication est composé de plusieurs canaux de communication. Un nœud source et destinataire doivent se mettre d'accord sur un canal de communication pour communiquer l'un avec l'autre. Pour mener son attaque, un brouilleur doit d'abord détecter le canal utilisé par les deux nœuds source et destination, ensuite il essaie d'occuper constamment le canal par l'insertion des messages inutiles sur ce même canal pour empêcher les deux nœuds source et destination de communiquer l'un avec l'autre.

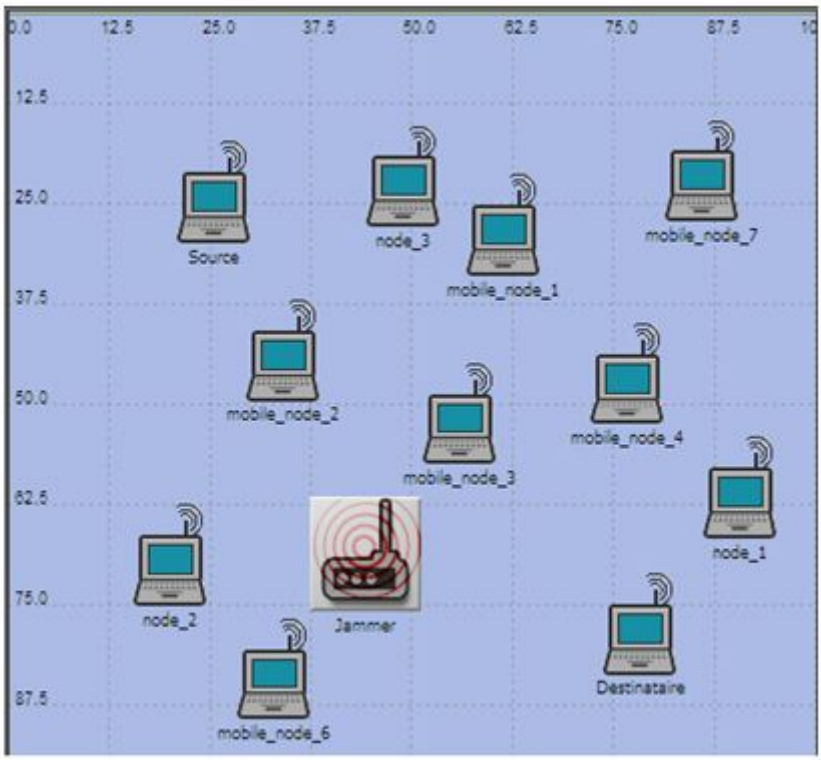

FIGURE 4.1 – Modèle du réseau

4.3 Solution de sécurité proposée

Dans cette section, nous allons présenter les hypothèses sous lesquelles notre solution est fonctionnelle et les détails de notre schéma de prévention contre l'attaque d'interférence.

4.3.1 Hypothèses

Dans notre contexte, les nœuds utilisent un support de communication sans fil partagé et multicanaux, i.e., plusieurs canaux peuvent être utilisés pour véhiculer les paquets entre deux nœuds source et destinataire. Nous supposons qu'à un moment donné, un attaquant ne cible qu'un seul canal de communication à la fois. Nous supposons aussi que le réseau utilise le protocole AODV pour le routage, bien évidemment que d'autres protocoles de routage peuvent aussi être utilisés. En plus on exclut toute possibilité de congestion dans le réseau.

4.3.2 Détail de la solution

Comme illustré dans la FIGURE 4.2, notre solution peut être décomposée en trois phases qui sont : la phase de négociation, la phase de détection et la phase de prévention.

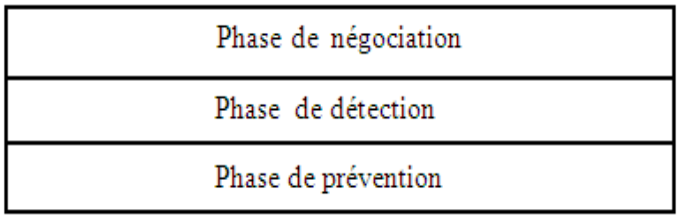

FIGURE 4.2 – Phases de notre solution

4.3.2.1 Phase de négociation

Cette phase peut être déroulée en parallèle avec la phase de découverte de routes, dans laquelle AODV essaye d'établir un chemin reliant deux nœuds source et destination. L'objectif de cette phase est la négociation du canal de communication à utiliser entre deux voisins dans un chemin de bout en bout. Autrement dit, deux nœuds qui se succèdent dans un chemin doivent se mettre d'accord sur le canal de communication à utiliser. Comme il est illustré dans la FIGURE 4.3, les nœuds composants le chemin reliant une source et une destination peuvent utiliser plusieurs canaux de communication différents. La seule contrainte exigée lors de la négociation est qu'un nœud doit utiliser deux canaux différents pour communiquer avec son prédécesseur et son successeur ; par exemple le nœud N_2 utilise le canal C_2 pour communiquer avec N_1 et le canal C_3 pour communiquer avec N_3, ceci pour éviter la situation où les deux liaisons N_1-N_2 (canal C_1) et N_2-N_3 (canal C_2) soient attaqués les deux à la fois.

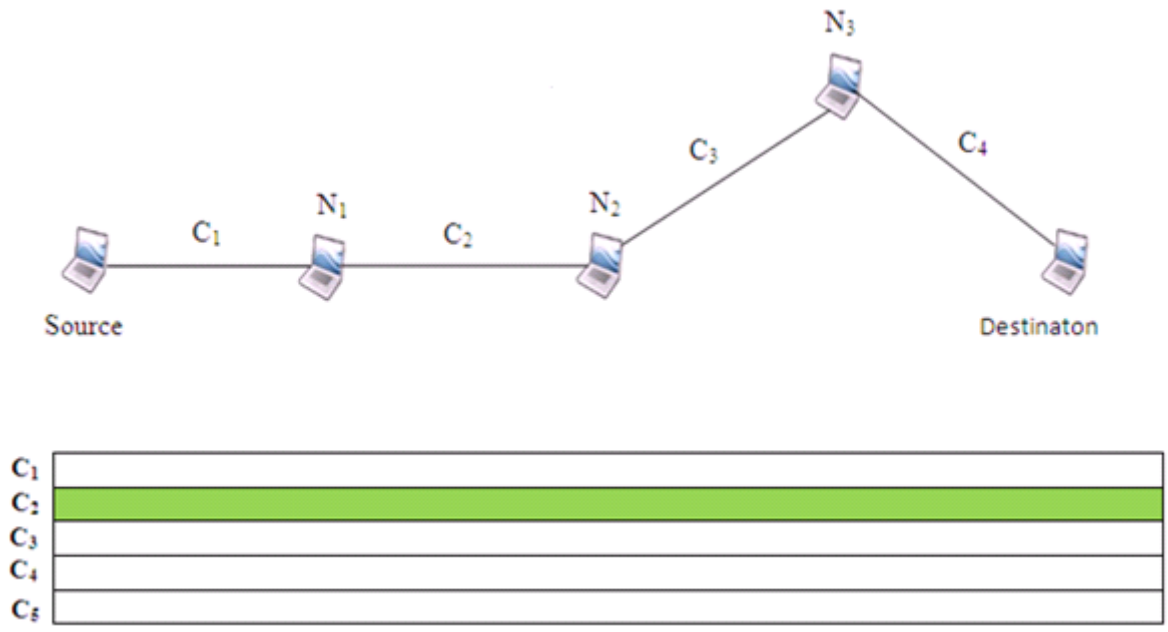

FIGURE 4.3 – Avant l'attaque

4.3.2.2 Phase de détection

Pour détecter l'attaque jamming, notre solution utilise les méthodes classiques de détection qui sont les mesures PDR, PSR et SS. Nous rappelons que le PDR est une mesure utilisée pour détecter l'attaque au niveau de la réception ; à ce niveau, si on constate que le PDR est faible alors on conclut qu'une attaque de jamming s'est produite. Idem pour PSR qui est une mesure utilisée pour détecter l'attaque au niveau de l'émission, si le PSR est faible alors on conclut que le canal est interféré. Le SS est généralement utilisé conjointement avec PDR pour que la détection soit plus précise. Dans notre phase de détection, on utilise la métrique PDR qui peut être une bonne mesure pour détecter l'attaque de jamming car le réseau ne peut plus en aucun cas être congestionné. Donc une valeur faible du PDR signifie pour nous que l'attaque jamming s'est produite dans le réseau.

4.3.2.3 Phase de prévention

L'idée clé de notre schéma de prévention est l'utilisation d'un autre canal de communication dès que le canal courant est interféré. Comme illustré dans la FIGURE 4.4(a), l'attaquant cible le canal C_2 reliant les nœuds N_1 et N_2. Lorsque ce dernier constate un PDR faible, il conclut que le canal C_2 est attaqué par une attaque jamming. Pour se prévenir de cette attaque, il procède à la négociation d'un autre canal de communication avec son prédécesseur N_1, donc il se présente sur un autre canal de communication. De son côté N_1, lorsqu'il constate l'absence de N_2 sur le canal courant C_2, il essaye de découvrir sa présence sur un autre canal et ceci en parcourant les autres canaux disponibles. La communication entre les deux nœuds s'établit sur un autre canal différent à ceux utilisés par N_1 et son prédécesseur et N_2 et son successeur. Comme illustré dans la FIGURE 4.4(b), les nœuds N_1 et N_2 vont utiliser le canal C_5 à la place du canal C_2. Nous signalons que dans notre solution, la négociation s'effectue entre les nœuds voisins et qu'il n'est plus nécessaire d'informer les autres nœuds du réseau du changement du canal entre les nœuds voisins. À la différence des autres techniques proposées dans la littérature, où une synchronisation totale sur le nouveau canal entre tous les nœuds du réseau est exigée, l'effet de l'attaque dans notre schéma est locale ce qui diminue considérablement l'overhead de communication et le temps de latence.

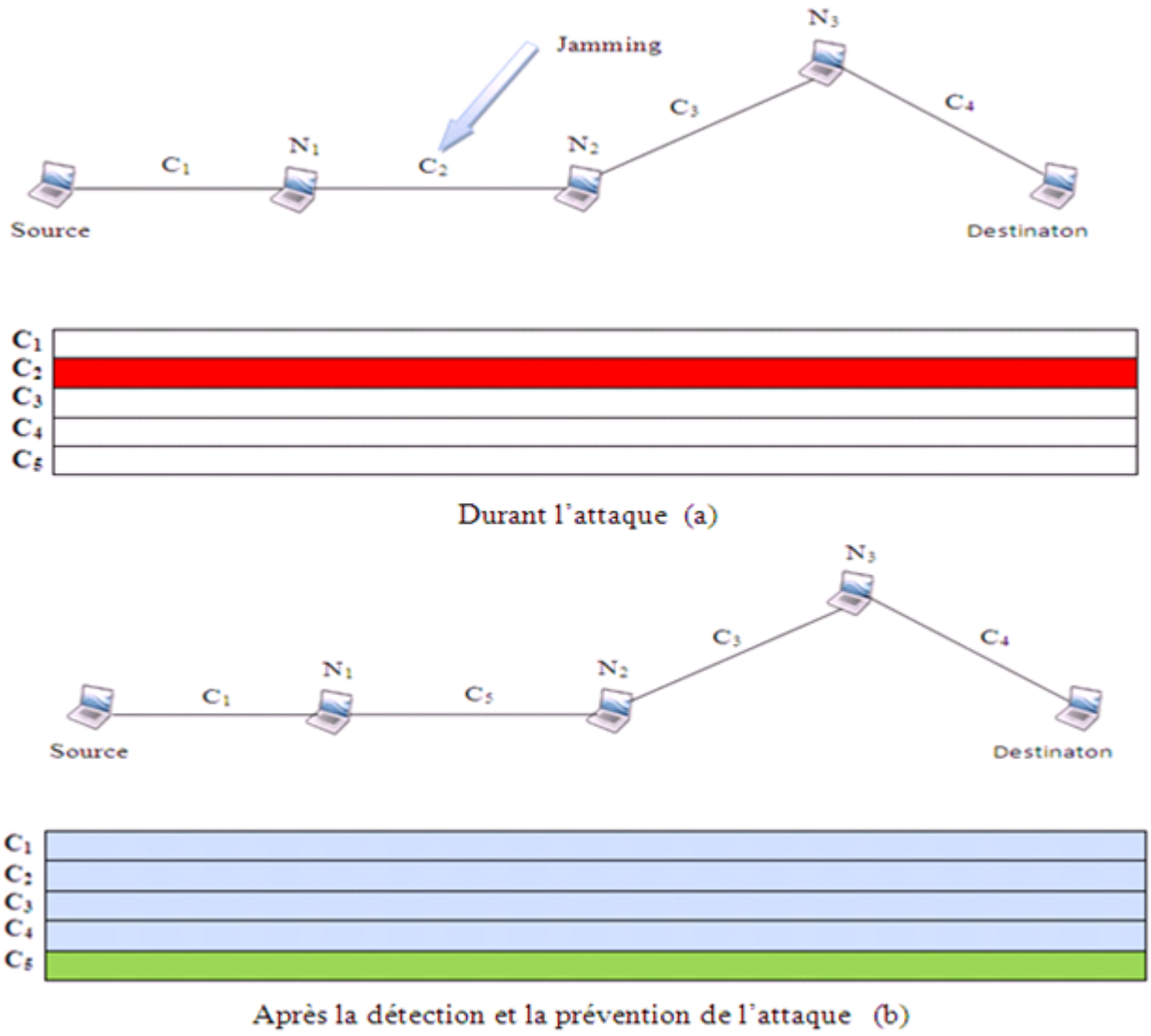

FIGURE 4.4 – Solution proposée

4.4 Résultats de simulation

Pour montrer l'efficacité de notre solution dans la prévention de l'attaque jamming, nous avons effectué une série de simulation en utilisant le langage Java. Les paramètres de simulation sont énumérés dans le tableau (TABLE 4.1).

Paramètres de simulation	Valeurs
Taille du réseau	1 km *1 km
Portée	20 m
Taille du paquet	1024 bits
Nombre de nœuds	20
Temps de simulation	100 secondes

TABLE 4.1 – Paramètres de simulation

Les nœuds sont déployés aléatoirement et parmi ces nœuds, on sélectionne deux nœuds source et destinataire, ainsi qu'un nœud jammer. Une route doit être établie entre les nœuds source et destinataire en utilisant un protocole du routage tel qu'AODV. Le nœud source génère un trafic qui va être acheminé vers le nœud destinataire par les nœuds intermédiaires composants la route établie. L'action malicieuse du jammer consiste à perturber le trafic par la génération d'un signal bruit, empêchant ainsi la communication entre les deux nœuds source et destination.

4.4.1 Métriques de simulation

Afin de mesurer la performance de notre solution, nous allons considérer les métriques suivantes :

- **PDR** : Dénote le taux de paquets délivrés.
- **PSR** : Dénote le taux de paquets délivrés avec succès.
- **Overhead** : Dénote les messages en plus pour la mise en œuvre de notre solution.
- **Temps de latence** : Dénote le temps écoulé entre l'envoi et la réception du paquet.

Les deux métriques PDR et PSR sont mesurées pour montrer l'efficacité de notre solution, tandis que l'overhead et le temps de latence sont mesurés pour comparer notre solution avec la technique du saut de fréquence proposée dans la littérature.

4.4.2 Analyse et discussion des résultats de simulation

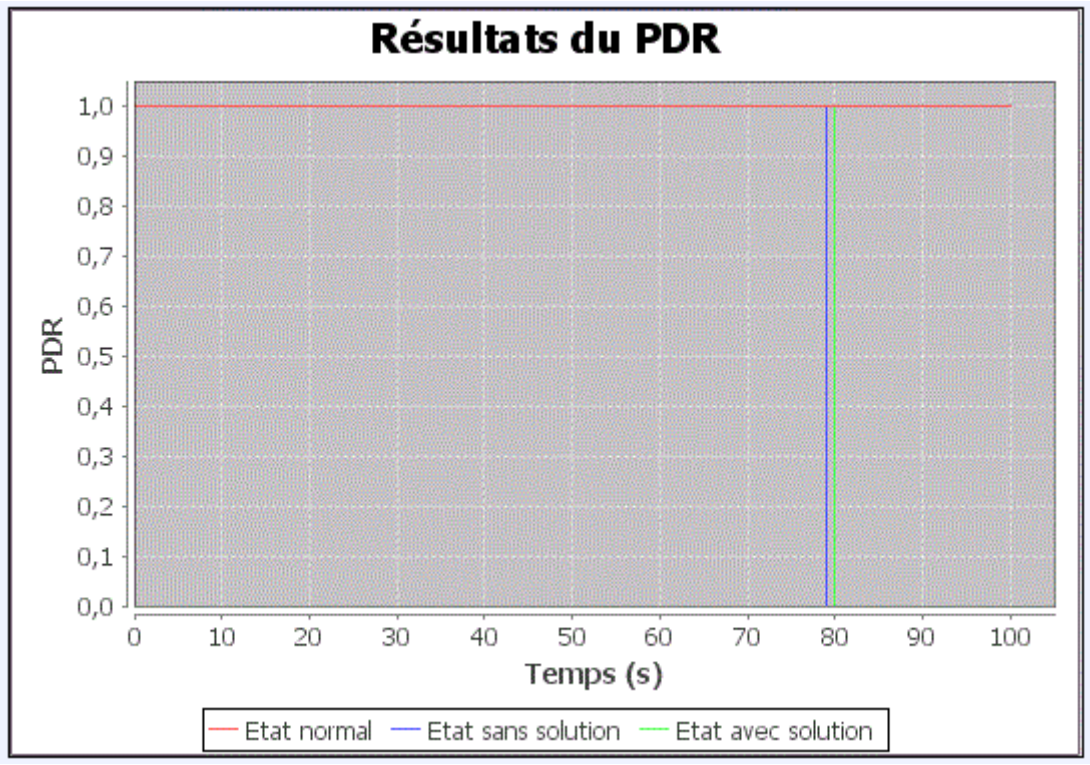

FIGURE 4.5 – Résultats du PDR

Dans le but de montrer que notre solution protège éfficacement contre l'attaque jamming, la FIGURE 4.5 illustre le taux du PDR tel qu'il est mesuré dans les trois cas : sans attaque, avec attaque et avec solution. Dans le cas sans attaque, le PDR est égale à 1, i.e., tous les paquets envoyés ont été bien délivrés. Dans le cas où le jammer est présent, nous constatons que le PDR est nul à partir d'un certain temps, ceci est dû à l'effet de l'attaque qui a empêché les nœuds source et destination de communiquer. En utilisant notre solution, nous remarquons une augmentation du PDR suite à la détection de l'attaque. En conséquence, notre solution est efficace pour se protéger contre une telle attaque.

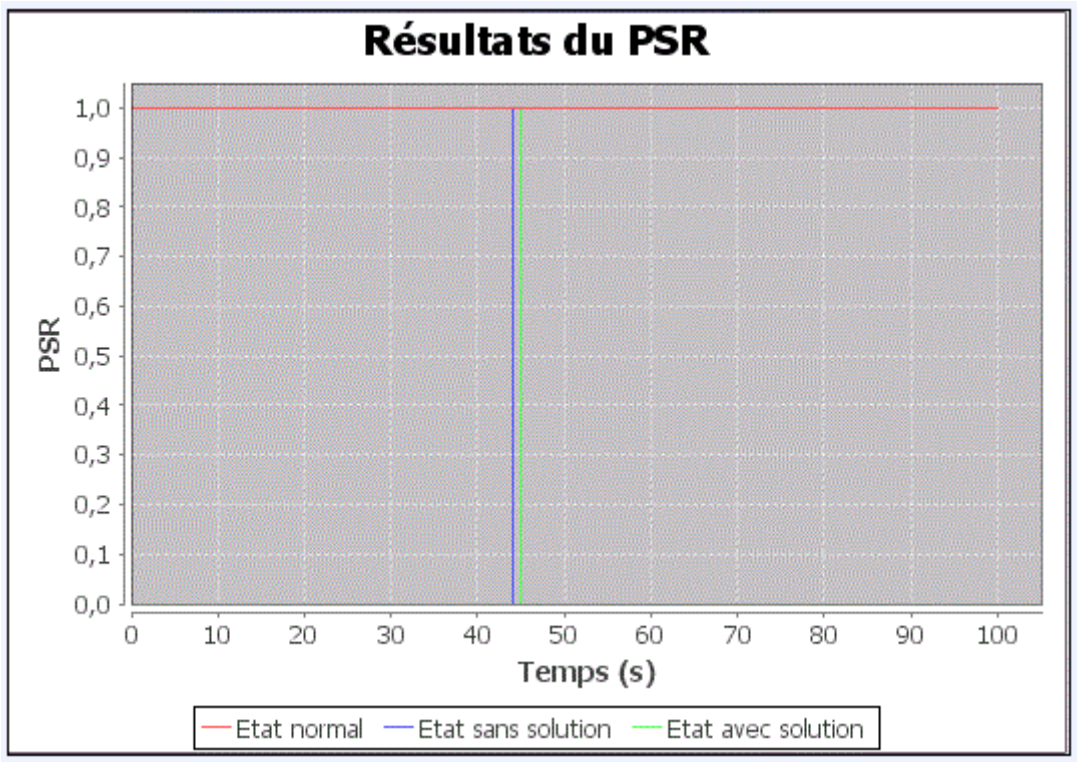

FIGURE 4.6 – Résultats du PSR

La FIGURE 4.6 montre le taux du PSR tel qu'il est mesuré dans les cas : sans attaque, aves attaque et avec solution. Dans le premier cas, le PSR est constant, ce qui explique que tous les paquets à envoyer ont été envoyés avec succès. En présence de l'attaque, le PSR chute suite à l'effet de l'attaque. Dans le dernier cas, le PSR remonte pour atteindre la valeur 1, d'où l'efficacité de notre solution dans la prévention de cette attaque.

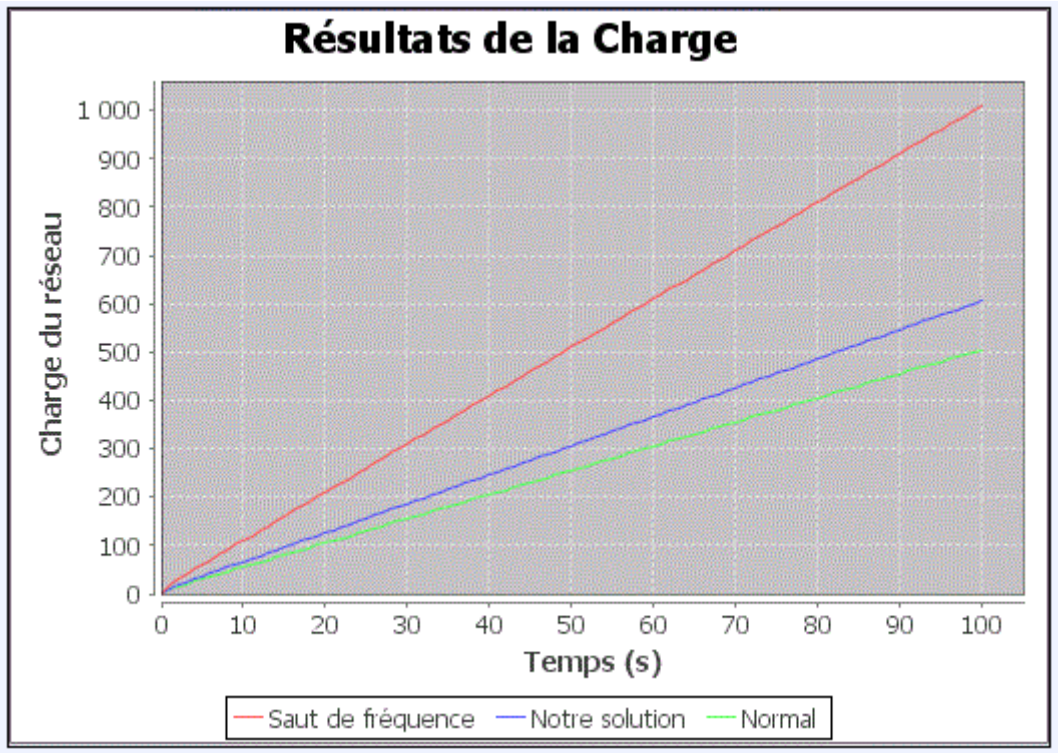

FIGURE 4.7 – Résultats de la charge

Dans la FIGURE 4.7, nous avons mesuré l'overhead généré par notre solution et celui généré par la technique du saut de fréquence proposée dans la littérature. Nous constatons que l'overhead généré par notre solution est moins important que celui généré dans la technique du saut de fréquence. En effet, dans la technique du saut de fréquence, suite au changement du canal, tous les nœuds du réseau doivent être synchronisés sur le nouveau canal, ce qui nécessite un échange de messages pour informer les autres nœuds du réseau du nouveau canal. Par contre, l'effet de l'attaque dans notre proposition est local, i.e., l'attaque n'affecte que le canal utilisé entre deux voisins, donc la synchronisation sur le nouveau canal n'est nécessaire qu'entre les deux voisins. C'est pour cela que notre solution génère peu d'overhead comparativement avec la technique du saut de fréquence.

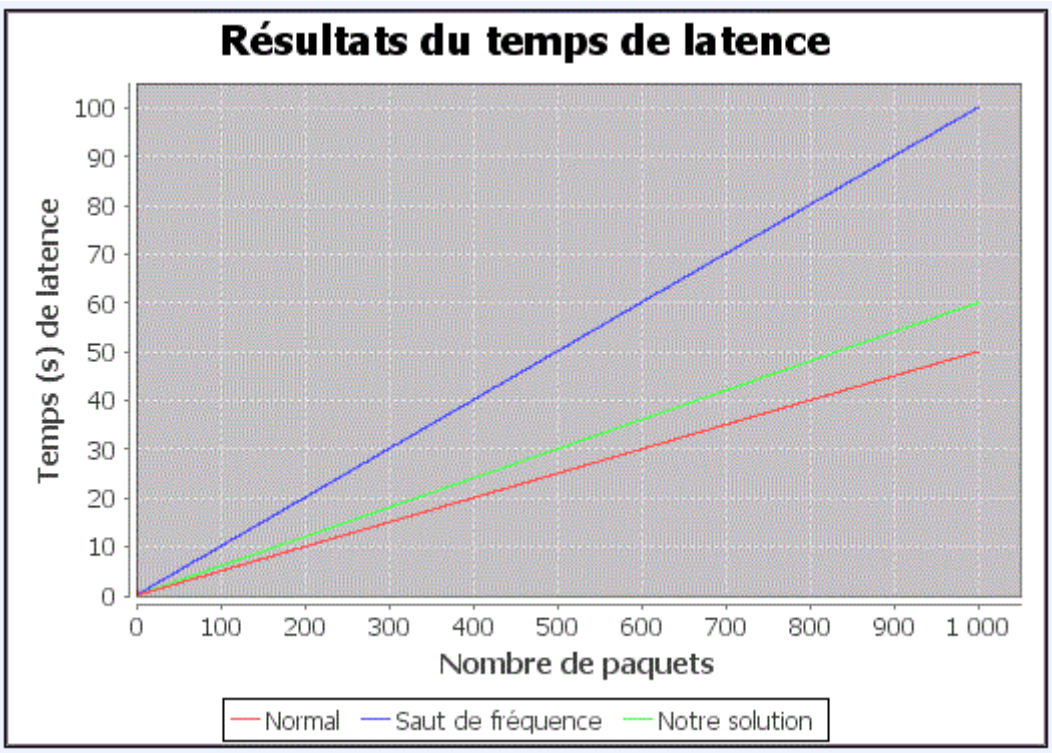

FIGURE 4.8 – Résultats du temps de latence

La FIGURE 4.8 illustre le temps de latence tel qu'il est mesuré dans notre solution et dans la technique du saut de fréquence. Le temps de latence important dans la technique du saut de fréquence est justifié par le fait que dans cette technique, tous les nœuds du réseau doivent être synchronisés sur le nouveau canal pour rétablir la communication. Contrairement à notre solution, où le temps de latence est négligeable car la synchronisation sur le nouveau canal est bien locale.

4.5 Conclusion

Dans notre travail, nous nous sommes intéressées à l'attaque d'interférence qui consiste à perturber la communication entre les nœuds légitimes dans un réseau. Pour se protéger contre cette attaque, nous avons proposé une solution qui se base sur la technique du saut de fréquence. Son idée clé est que les voisins utilisent des canaux différents pour communiquer. L'objectif est de réduire l'effet de l'attaque de telle sorte qu'il soit local. En effet, en attaquant un canal, uniquement les deux voisins reliés par ce canal seront affectés. La solution consiste à changer le canal attaqué par un nouveau canal non utilisé. L'avantage de notre solution est que les nœuds concernés par la synchronisation sont seulement les deux nœuds reliés par le canal attaqué, ce qui diminue considérablement l'overhead et le temps de latence. Les résultats de la simulation montrent que la solution proposée est efficace pour prévenir ce type d'attaques, et elle est plus performante en termes d'overhead et du temps de latence comparativement avec la technique du saut de fréquence.

Conclusion générale et perspectives

Un réseau ad hoc est une collection de nœuds éventuellement mobiles, utilisants un support sans fil pour communiquer. L'ouverture de ce médium de communication est une vulnérabilité largement exploitée par les attaquants pour mener des attaques DoS visant la disponibilité du réseau.

Dans ce mémoire, on s'est intéressées à l'une de ces attaques DoS qui est l'attaque jamming. Il s'agit d'une attaque qui peut être menée avec peu de ressources soit au niveau MAC, soit au niveau PHY. Son objectif au niveau MAC est de ne pas respecter les spécifications du protocole MAC sous-jacent et occuper constamment le canal de communication. Au niveau PHY, l'attaque consiste à envoyer un signal bruit qui s'interfère avec le signal légitime. Les solutions de la littérature peuvent être détectives et/ou préventives. La détection se fait en mesurant le PDR, le PSR ou une combinaison de ces deux mesures. La prévention se base grossièrement sur le saut de fréquence ou l'étalement du spectre. Notre solution, motivée par l'insuffisance des solutions de la littérature, consiste à établir un chemin dans lequel chaque paire de nœuds intermédiaires successifs partagent un canal différent. La détection de l'attaque dans notre solution utilise les mêmes techniques utilisées dans la littérature. À noter qu'en cas d'attaque d'un canal donné, uniquement les deux nœuds reliés par ce canal sont affectés ; pour rétablir la communication entre eux, il leurs suffit de négocier un nouveau canal de communication. L'avantage de notre solution est que la synchronisation n'est nécessaire que pour les deux nœuds reliés par le canal attaqué. Contrairement à la technique du saut de fréquence, où une synchronisation entre tous les nœuds est exigée. Les résultats de la simulation montrent que notre solution est efficace dans la détection et la prévention de cette attaque, et performante en termes d'overhead et du temps de latence comparativement avec la technique du saut de fréquence.

En perspectives, nous envisageons d'améliorer notre solution et tenir en compte

le cas où le réseau est congestionné. La solution future devra donc distinguer entre la situation de congestion du réseau et la situation où le canal est attaqué et prendre des mesures adéquates pour empêcher l'attaque d'interférence.

Bibliographie

[1] P. Mühlethaler . *Réseau Sans fil*,Eyrolles, 2002.

[2] J. Van der Meerschen . *Hybridation entre les modes ad-hoc et infrastructure dans les réseaux de type Wi-Fi* . Mémoire d'ingénieur en sciences appliquées, Université Libre de Bruxelles, 2005-2006.

[3] S. Oubbati,A. Oubbati et B. Oubbati. *La tolérance aux pannes des algorithmes de partage de ressources dans les systémes repartis et les reseaux ad hoc* .Mémoire d'ingéniorat, Université de Laghouat, 2010.

[4]M. Boulkamh Chouaib. *Prise en Compte de la QoS par les Protocoles de Routage dans les Réseaux Mobiles Ad Hoc*, Mémoire de magister, 2008.

[5] A. Laouiti. *Unicast et multicast dans les réseaux ad hoc*, 2002.

[6] H. Amir, L. Cherrat. *Routage avec Qualité de Service (QdS) dans les Réseaux Ad hoc.*Mémoire d'ingéniorat,université de bejaia, 2009.

[7] X. Xue. *Mécanisme de sécurité pour des protocoles de routage des réseaux ad hoc*, Thèse de doctorat, 2006.

[8] M. Frikha. Réseau ad hoc, Lavoisier, 2010.

[9] D. Dhoutaut. *Etude du standard IEEE 802.11 dans le cadre des réseaux : de la simulation à l'expérimentation* . Technical report, In Institut National des sciences Appliquées de lyon, 2003.

[10] K. AYAD. *Sécurité du routage dans les réseaux mobiles ad hoc*, Mémoire de magistére, Ecole nationale Supérieure en Informatique (ESI) Oued-Smar Alger, 2012.

[11] N. Badache. *La mobilité dans les systèmes répartis*, Janvier 1998.

[12] Ph. Jacquet, P. Muhlethaler, and A. Quayyum. *Optimized Link State Routing Protocol* . RFC n° 3626, IETF MANET Working Group, November 1998.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker. *Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*. ACM MOBIC, Boston MA, USA, pages 255-265, 2000.

[14] W. Stalling. *Cryptography and network security, principal and practice*. end edition prentice hall, 1999.

[15] A. Perrig, and D. Johnson. *Wormhole attacks in wireless networks* . IEEE Journal on Selected Areas in Communications, 24(2) :370-380, Feb 2006.

[16] G. Labouret . *Introduction à la cryptographie. cabine herve schauer consultants-hsc* . In Supports de cours, 09 février 2001.

[17] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields and E. M. Belding-Royer. *A Secure Routing Protocol for Ad Hoc Networks*. 10th IEEE International Conference on Network Protocols (ICNP'02), pages 78-89, (2002).

[18] M. Arora, Z. Zafrulla, Shekhar and Dr. K S Ramanatha. *Secure dynamic source routing protocol (SDSR) for mobile ad hoc networks*. technical report, 2004.

[19] A. Perrig, R. Canetti, J. Tygar, and D. Song. *The tesla broadcast authentication protocol*. RSA CryptoBytes, 2002.

[20] R. S. Puttini, L. Me, and R. T. Sousa. *Certification and authentication services for securing manet routing protocols*. In Proceedings of the Fifth IFIP TC6 International Conference on Mobile and Wireless Communications Networks, 2003.

[21]F. Dupont , S. Gombault, V. Gayraud, L. Nuaymi and B. T. Thomson. *La sécurité dans les réseaux sans fil ad hoc*. security lab, ENST Bretagne, 2002.

[22] I. R. J. M. McQuillan and E. C. Rosen. Student member, IEEE, and z.j. hass, senior member, IEEE. *In the new routing algorithm for the ARPANET* , May 1980.

[23] P. Misra, *Routing protocols for ad hoc mobile wireless networks* , Novembre 1999.

[24] M. E. Ermel. *Routage géographique dans les réseaux sans fil hétérogène.* SUPINFO,2004.

[25] G. Perkins , S. Das and belding Royer. *Ad hoc on-dernand distance vector (AODV) routing.* In IETF RFC 3561, 2003.

[26] P. Chaturvedi and K. Gupta .*Detection and Prevention of various types of Jamming Attacks in Wireless Networks.* International Journal of Computer Networks and Wireless Communications, 3(2) :pages 75, 79, 2013.

[27]Y. Zhang, Rutgers University. *Jamming Sensor Networks : Attack and Defense Strategies.* IEEE Network, pp. 41-47, 2006.

[28] Z. Zhang and J. Deng. *Jamming ACK Attack to Wireless Networks and a Mitigation Approach* . IEEE GlobecomL, page 4966-4970, 2008.

[29] W. Xu, W. Trappe, Y. Zhang and T. Wood. *The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks.* In proceedings of the international conerance on werelessInformation Net work(mobi hoc, 2005

[30] A. Hamieh and J. Ben-Othman. *Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution.* in the IEEE ICC 2009 proceedings, Pages=1-6, 2009.

[31] K. Chung. *Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks.* International Journal of Security and Its Applications Vol, 6, No. 2, April, 2012, pp. 149-154.

[32] I. Shin, Y. Shen, Y. Xuan and T. Znati. *Reactive jamming attacks in multi-radio wireless sensor networks : an efficient mitigating measure by identifying trigger nodes.* Proceedings of the 2nd ACM international workshop on Foundations of wireless ad hoc and sensor networking and computing FOWANC '09, Pages 87-96, 2009.

[33] D. Bonfrer, B. Schapendonk. *Link-Layer Jamming Attack against the Wireless Sensor Network LMAC Protocol and Countermeasure* . Pm2Hw2n 2008 : 67-71 // 2007.

[34] R. Negi and A. Rajeswaran. *DoS analysis of reservation based MAC protocols.* in ICC 2005.

Résumé

Un réseau ad hoc mobile est une collection de nœuds formants un réseau dynamique sans infrastructure préexistante ou une administration centralisée. Dans ce type de réseaux, chaque nœud fonctionne comme un routeur et utilise un protocole du routage pour acheminer les paquets des autres nœuds. Malgré facile et moins coûteux à déployer, ce type de réseaux reste vulnérable par plusieurs attaques à cause de ses caractéristiques comme la mobilité et l'ouverture du médium de communication. Dans notre travail, on s'est focalisé sur l'attaque d'interférence, dans laquelle un nœud malicieux occupe constamment le canal de communication utilisé par les nœuds communiquants, pour les empêcher de communiquer. Pour lutter contre une telle attaque, nous avons proposé une solution qui se base sur le changement du canal et se décompose en trois phases : négociation, détection et prévention. Les résultats de la simulation montrent que notre solution est efficace dans la détection et la prévention de l'attaque d'interférence.

Mots clés : réseau ad hoc, sécurité du routage, attaque DoS, interférence, brouillage.

Abstract

Ad hoc network is a collection of mobile nodes communicating with each other by wireless links. In this kind of networks, each node behaves as a router and uses a routing protocol to forward packets of other nodes. The deployment of such network is easier and less expensive, but it is vulnerable to several attacks because of the opening of the medium of communication and mobility. Therefore, the security in such a network is a real challenge for designers of protocols, particularly those relating to routing. In our work, we have focused on the jamming attack where the communication channel is occupied constantly by a malicious node. To cope with this attack, we have proposed a challenge based approach that is decomposed into three phases : negotiation, detection and prevention. Simulation results show that our solution detect and mitigate efficiently the jamming attack.

Key words : ad hoc network, routing security, DoS attack,jamming.