République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Larbi Tébessi - Tébessa
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département : Mathématiques et Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique
Filière : Informatique
Option : Réseaux et Sécurité informatique

Thème

Développement d'une nouvelle stratégie de sécurité ANTI-BRUIT pour les réseaux Mobile ad hoc

Présenté Par :

BOUACHMA Baraà

Devant le jury :

Mr AMROUNE Mohamed MCA UnivérsitéLarbi Tébessi Président
Mme BOUAKKAZ Fatima MAA UnivérsitéLarbi Tébessi Examinatrice
Mr MERZOUG Soltane MCB UnivérsitéLarbi Tébessi Encadreur

Date de soutenance : 28/06/2020

Résumé

Un réseau mobile ad hoc (MANET) est un système autonome de plates-formes mobiles appelées nœuds qui sont libres de se déplacer aléatoirement et sans contrainte. La communication dans ce type de réseau est soumise à de nombreux problèmes de sécurité tels que les attaques de brouillage, donc la sécurité est désormais devenue une exigence fondamentale. Plusieurs travaux pour la sécurité anti-brouillage dans les réseaux MANET ont été proposés. Dans ce mémoire, nous avons proposé un technique anti-brouillage qui se combine deux techniques (FHSS et DSSS). Afin de confirmer les améliorations apportées par notre technique nous avons conduit une simulation à laide du simulateur réseau NS3.

ملخص

شبكة الجوال المخصصة (*MANET*) هي نظام مستقل لمنصات الجوال تسمى العقد التي تتمتع بحرية التنقل بشكل عشوائي ودون قيود. يخضع الاتصال في هذا النوع من الشبكات للعديد من المشاكل الأمنية مثل هجمات التشويش، لذا أصبح الأمان الآن متطلبًا أساسيًا. تم اقتراح العديد من الأعمال لأمان مكافحة التشويش في شبكات *MANET*. في هذه المذكرة، اقترحنا تقنية مضادة للتشويش تجمع بين تقنيتين (*FHSS* و*DSSS*). من أجل تأكيد التحسينات التي أدخلتها تقنيتنا ، أجرينا محاكاة باستخدام محاكي شبكة *NS3*.

Remerciements

Au nom d'Allah, le tout – miséricordieux, le très miséricordieux.

La louange est à ***Allah*** *l'unique et la paix et le salut sur celui qui n'a point de messager après lui et sur sa famille, ses compagnons et tous ceux qui souvient son chemin jusqu'au jour de la résurrection.*

Mes remerciements vont tout premièrement à dieu tout-puissant pour la volonté, la santé et la patience, qu'il m'a donnée durant toutes ces langues années.

Je tiens à exprimer mes respects et mes vives gratitudes au Mr. MERZOUG Soltane qui m'a fait l'honneur d'assurer mon encadrement et qui n'a pas hésité à participé à la réalisation de ce modeste travail avec ses précieux conseils et ses bonnes orientations et je lui exprime ma gratitude pour sa patience et sa bonne humeur.

Mes vifs remerciements s'adressent aussi à Dr. AMROUNE Mohammed et Mme. BOUAKKAZ Fatima d'avoir accepté d'examiner et d'évaluer ce travail.

Mes remerciements aussi à tous qui m'ont aidé de près ou de loin pour finir ce travail.

MERCI BEAUCOUP

Dédicace

Tous les mots ne sauraient exprimer la gratitude, l'amour, le respect, la reconnaissance, c'est tous simplement que je dédie cette mémoire à :

A Mon très cher Père Abed :

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

A Ma tendre Mère :

Tu représente pour moi la source de tendresse et l'exemple de dévouement qui n'a pas cessé de m'encourager. Tu as fait plus qu'une mère puisse faire pour que ses enfants suivent le bon chemin dans leur vie et leurs études.

A Mes chers frères :

Je leur souhaite du succès dans leur vie personnelle et académique.

A Mes chers amis :

Pour tous les souvenirs éternels dans nos cœurs, je les remercie pour leur soutien et pour m'accompagner, merci.

A tous ma famille :

Je les remercie de m'avoir soutenu et d'être à mes côtés tout au long de ma carrière scolaire, en particulier pour ma deuxième mère, Ahlam.

A tous ceux dont l'oubli du nom n'est guère celui du cœur…

Table des matières

Liste des abréviations

RCSF	Réseau de Capteurs Sans Fils
IETF	Internet Engineering Task Force
RFC	Requests For Comments
MPR	Multi Point Relay
LSR	Link State Routing
RREQ	Route REQuest
RREP	Route REPly
IARP	IntrAzone Routing Protocol
IERP	IntErzone Routing Protocol
BRP	Border Resolution Protocol
GPS	Global Positioning System
SNR	Signal-to-Noise Ratio
BS	Base Station
PDPT	Packet Dropped Per Terminal
CDMA	Code Division Multiple Access
DoS	Denial of Service
BW	BandWidth
LPI	Low Probability of Intercept
AJ	Anti Jamming
PN	Pseudo Noise
RF	Radio Frequency
RTS	Request to Send
CTS	Clear to Send
DCF	Distributed Coordination Function
PCF	Point Coordination Function
EP	Error Probability
CC	Correlation Coefficient

Liste des tableaux

Liste des figures

INTRODUCTION GÉNÉRALE

Introduction générale

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

Les réseaux mobiles sans fil, peuvent être classés en deux catégories : les réseaux avec infrastructure qui utilisent généralement le modèle de la communication cellulaire, et les réseaux sans infrastructure ou les réseaux ad hoc. Plusieurs systèmes utilisent déjà le modèle cellulaire et connaissent une très forte expansion à l'heure actuelle mais requièrent une importante infrastructure.

Un réseau ad hoc mobile est un ensemble autonome et coopératif de nœuds mobiles qui se déplacent et communiquent par une transmission sans fil qui ne suppose pas d'infrastructure préexistante. Le réseau ad hoc mobile se forme de manière spontanée et provisoire dès que plusieurs nœuds mobiles se trouvent à portée radio les uns des autres. Les nœuds communiquent, selon la distance qui les sépare, par deux modes de communication : soit les nœuds mobiles peuvent directement communiquer (en transmission ad hoc) car ils sont à portée de transmission, soit ils doivent utiliser d'autres nœuds mobiles comme des relais pour acheminer les paquets à destination (la transmission est multi-sauts) donc chaque nœud est à la fois utilisateur final et routeur afin de relayer les paquets vers leur destinations Et cela à cause de la couverture limitée du champ radio disponible à chaque nœud. Les nœuds capteurs collectent l'information environnementale parfois les traitent et les envoient à d'autres nœuds en utilisant une commination multi saut sans fil jusqu' à atteindre la station de base appelé également le nœud puits (Sink).

Les réseaux mobiles Ad hoc ont été initialement développés pour des applications militaires, mais leurs propriétés en font des solutions pratiques dans de nombreux domaines de la vie courante. Grâce à cette technologie mobile Ad hoc, les utilisateurs n'ont pas besoin d'une infrastructure préexistante pour communiquer et ils peuvent aussi se déplacer tout en restant connectés à leurs services [1].

L'élargissement du domaine d'application des réseaux mobiles Ad hoc nécessite plus de sécurité pour assurer l'intégrité et la confidentialité des données qui circulent dans le réseau. En effet, les réseaux mobiles Ad hoc sont confrontés à des nombreuses caractéristiques qui rendent les solutions de sécurité développées pour les réseaux filaires ou sans fil avec infrastructure inapplicables dans le contexte des réseaux mobiles Ad hoc. Ce dernier est vulnérable à divers types d'attaques qui peuvent être lancées de façon relativement simple [1].

Parmi ces attaques les attaques de brouillages, qui sont toute perturbation ou interférence avec la transmission physique et la réception de signaux sans fil. Cela peut être intentionnel, sous forme d'interférences radioélectriques, involontaire en cas de collision et de parasites sur le récepteur, ou dans le cadre d'une attaque. Lors d'une attaque de brouillage, le but des brouilleurs est de perturber la communication entre l'émetteur et le récepteur en utilisant une puissance minimale. Cette attaque est catastrophique car le brouilleur exploite la nature ouverte et partagée du support sans fil pour perturber les communications en réduisant le rapport signal / bruit (SNR). Un attaquant disposant d'énormes ressources peut continuellement brouiller la bande du spectre pour perturber la communication dans la bande. De plus, un attaquant peut décider de brouiller la bande par intermittence, forçant ainsi le nœud récepteur à abandonner les paquets en raison d'une altération. Le dispositif de brouillage souvent utilisé pour perpétrer cette attaque sélectionne un canal commun qui est actuellement occupé par les nœuds pour empêcher la transmission réussie des données. L'objectif principal du dispositif de brouillage est d'occuper le canal et de s'assurer que le réseau n'est pas disponible pour les nœuds légitimes, tandis que ces nœuds, d'autre part, tentent de maximiser l'utilisation du réseau [2].

Objectifs

Dans le réseau de capteurs sans fil, il est difficile d'identifier les attaques par brouillage, ce qui peut augmenter les menaces à la sécurité. Cette menace est la raison pour laquelle cette étude vise à proposer une nouvelle stratégie anti-brouillage pour les réseaux MANET. Les objectifs sont les suivants :

1. Proposer une approche de détection d'attaque par brouillage basée sur une nouvelle stratégie de sécurité qui soit efficace.
2. Reconnaître les attaques par brouillage dans les réseaux MANET.
3. Estimer l'efficacité et l'efficience des brouilleurs.
4. Valider les métriques de sécurité de MANET.

Structure du mémoire

Cette mémoire est composée de quatre chapitres : dans le premier chapitre nous présentons les environnements mobiles et les principaux concepts liés aux réseaux mobiles ad hoc.

Dans le deuxième chapitre, nous présentons quelques protocoles de routage dans les réseaux ad hoc mobiles et nous présentons le problème des attaques de brouillage avec quelques techniques de détection, en plus quelques techniques anti-brouillages.

Dans le troisième chapitre, nous présentons une proposition d'une technique hybride pour la sécurité anti-brouillage et une étude de cas pour démontrer le principe de fonctionnement de cette technique hybride.

Dans le dernier chapitre, nous faire une simulation pour démontrer l'efficacité de notre technique.

Plan des chapitres

1. Chapitre 01 : Réseaux de capteurs sans fil et réseaux MANET

Dans le premier chapitre, nous présentons, avec explication les deux concepts suivant (les réseaux de capteurs sans fils et les réseaux MANET) en présentant les notions clés liées à ces concepts. On présente ce qu'est les réseaux de capteurs sans fils avec leurs domaines d'application, leurs catégories et ces caractéristiques avec quelques problèmes existant dans ce type de réseau. On présente aussi ce qu'est les réseaux MANET et leur différente caractéristique, leur avantages et inconvénients, domaines d'application et explication de leur modélisation.

2. Chapitre 02 : Le routage dans les réseaux mobiles Ad Hoc et les Techniques Anti-brouillages.

Le deuxième chapitre, présente les protocoles de routage dans les réseaux MANET et les techniques anti-brouillages. Il est composé de deux parties : la première partie présente les types des protocoles de routage dans les réseaux MANET avec quelques protocoles. Dans la deuxième partie nous présentons les attaques de brouillage avec les types de brouillage et les brouilleurs dans une figure, ensuite on présente les techniques de détection de brouillage et les techniques de contre-mesure (anti-brouillage).

3. Chapitre 03 : Contribution

Le troisième chapitre expliquera en détail une proposition hybride (combine les deux techniques FHSS et DSSS) qui est un technique anti-brouillage pour améliorer les performances de sécurité de transmission des données dans les réseaux MANET, ensuite nous avons fait un cas d'études détaillés pour mieux expliquer les étapes de fonctionnement de cette proposition.

4. Chapitre 04 : Implémentation et Résultats d'Expérimentation

Le dernier chapitre présente une simulation pour notre technique proposée. Nous avons présenté dans ce chapitre les outils qui nous ont aidés pour faire cette simulation tels que NS3 (Network Simulator 3), ensuite nous avons mentionné quelques étapes essentielles pour l'installation de ce simulateur, enfin on a présenté les résultats de la simulation avec une petite discussion pour quelques facteurs de fiabilité.

CHAPITRE 1

RÉSEAUX DE CAPTEURS SANS FIL ET RÉSEAUX MANET

Chapitre 1

Réseaux de capteurs sans fil et réseaux MANET

1.1 Introduction

Les réseaux de capteurs sans fil (RCSFs ou WSNs : Wireless Sensor Networks) sont composés d'un grand nombre de nœuds qui sont des capteurs intelligents (smart sensors) déployés densément à proximité immédiats du phénomène à surveiller. Le but de chaque capteur est recueille les données et les acheminer à un puits (Sink ou station de base) Chaque capteur est capable d'effectuer d'une manière autonome trois tâches complémentaires : mesure d'une valeur physique, traitement des mesures, et communication par voie hertzienne. Un capteur est limité en matière de bande passante, de puissance de calcul, de mémoire disponible et d'énergie. Les RCSFs sont devenus de plus en plus omniprésents. En raison de ses diverses applications telles que: applications médicales, commerciales et militaires, il reçoit une attention particulière de la communauté scientifique. Selon MIT's Technology Review, il s'agit de l'une des dix nouvelles technologies qui vont influer sur notre manière de vivre et de travailler. Les RCSFs sont considérés comme un type particulier des réseaux ad hoc [3].

L'évolution récente de la technologie dans le domaine de la communication sans fil et l'apparition des unités de calcul portables poussent aujourd'hui les chercheurs à faire plus d'efforts afin de parvenir au but des réseaux : « L'accès à l'information n'importe où et n'importe quand ».

Le concept des réseaux mobiles ad hoc essaie d'étendre les notions de la mobilité à toutes les composantes de l'environnement. Ici, contrairement aux réseaux basés sur la

communication avec infrastructure (cellulaire), aucune administration centralisée n'est disponible, ce sont les hôtes mobiles eux-mêmes qui forment une infrastructure du réseau. Aucune supposition ou limitation n'est faite sur la taille du réseau ad hoc, le réseau peut par conséquent contenir des centaines ou même des milliers d'unités mobiles [4].

Dans ce chapitre, nous allons présenter les réseaux de capteurs sans fils et les réseaux MANET et les principaux concepts qui y sont liés.

1.2 Réseau sans fil

Un réseau sans fil est un réseau informatique ou numérisé dont leur équipements (postes / systèmes) sont connectés entre eux par des ondes radios.

Le réseau sans fil peut associer à un réseau de télécommunication pour réaliser des interconnexions entre nœuds. La norme la plus utilisée actuellement pour les réseaux sans fil est la norme IEEE802.11 [5].

1.2.1 Les catégories des réseaux sans fil

Les réseaux sans fil peuvent avoir une classification selon deux critères. Le premier est la zone de couverture du réseau. Concernant ce critère il existe quatre catégories : les réseaux personnels, les réseaux locaux, le réseau métropolitain et les réseaux étendus [6]. Le deuxième critère est l'infrastructure, et c'est ce qui nous importe. Par rapport à ce critère on peut diviser les réseaux sans fils en deux catégories : réseaux avec infrastructures et réseaux sans infrastructure.

1.2.1.1 Réseau avec infrastructure (cellulaires)

Ce mode désigne un réseau composé d'une infrastructure permettant l'échange d'information entre les différentes stations du réseau. Cette infrastructure est basée sur un matériel spécifique qui fournit un ensemble de services. Ce matériel est appelé un point d'accès (AP). Dans cette topologie, une cellule d'un réseau IEEE 802.11 composée d'un AP et d'un ensemble de stations est appelée Basic Server Set (BSS). Les éléments distingués dans les réseaux d'infrastructures sont les points d'accès, ils sont utilisés pour toutes les communications entre les équipements du réseau, si une station mobile dans une infrastructure BSS doit communiquer avec une seconde station mobile, la communication doit prendre deux sauts. Premièrement, la station mobile d'origine transmet la trame au point d'accès. Et deuxièmement, le point d'accès transmet la trame à la station de destination.

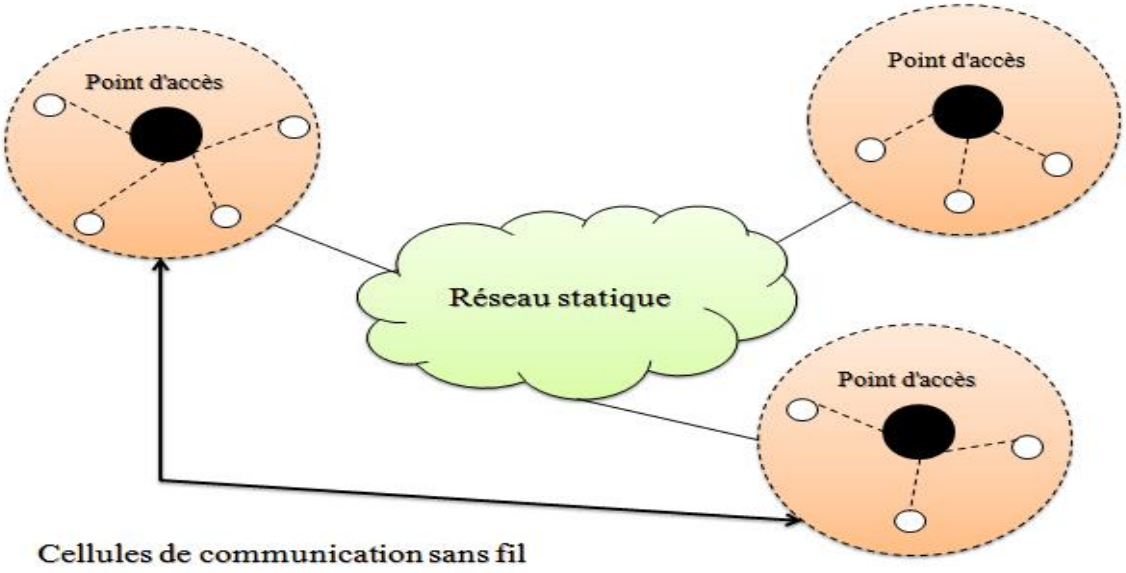

Figure 1: Réseau sans fil avec infrastructure.

1.2.1.2 Réseau sans infrastructure (Ad Hoc)

Un réseau sans fil ad hoc (ou MANET, pour Mobile Ad hoc NET work) est formé par un ensemble d'hôtes qui s'organisent seuls et de manière totalement décentralisée, formant ainsi un réseau autonome et dynamique ne reposant sur aucune infrastructure filaire. Ces hôtes peuvent être fixes ou mobiles. Selon ces hypothèses, tout ensemble d'objets munis d'une Interface de communication adéquate est susceptible spontanément de former un tel réseau. Aucune infrastructure n'étant disponible, ces objets ont donc à découvrir dynamiquement leur environnement. Un réseau ad hoc étant avant tout un réseau sans fil, les objets communiquent entre eux par le biais d'une interface radio. Ces communications sont donc soumises aux phénomènes physiques qui régissent les ondes radio, telles qu'une forte atténuation du signal avec la distance. Ainsi, seuls les hôtes suffisamment proches les uns des autres sont capables de communiquer directement ensemble, et les communications de longue distance doivent s'effectuer par le biais d'un mécanisme nommé multi-sauts : cela signifie simplement que certains objets doivent relayer les messages de proche en proche jusqu'à ce que leur acheminement soit effectue. L'utilisation d'une antenne radio omnidirectionnelle implique

également qu'un message envoyé par un émetteur quelconque est reçu par tous les récepteurs suffisamment proches de lui [7].

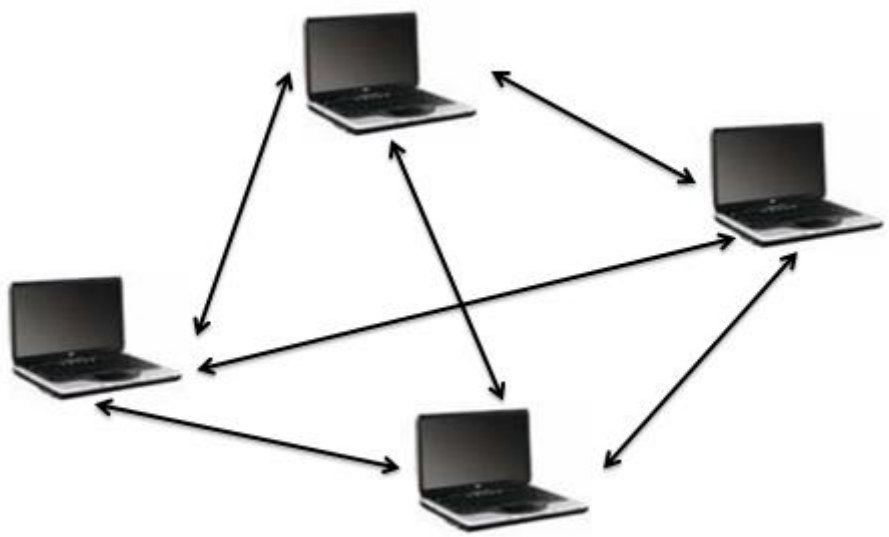

Figure 2: Réseau sans fil sans infrastructure.

1.3 Réseau de capteurs sans fils

Un réseau sans fil de capteurs est une collection de nœuds. Chaque nœud se compose d'une unité de traitement (un ou plusieurs microcontrôleurs, CPU), peut contenir plusieurs types de mémoire (RAM, disque durs et mémoires Flash), doter d'un émetteur/récepteur et une source d'énergie (par exemple, des batteries et des piles solaires). Les nœuds de ces réseaux consistent en un grand nombre de capteurs capables de récolter et de transmettre des données environnementales d'une manière autonome, dispersés aléatoirement à travers une zone géographique (champ de captage) et mettant en œuvre un routage multi saut jusqu'au nœud considéré comme un « point de collecte ». Les réseaux sans fil de capteurs se composent de nœuds de capteurs qui doivent coopérer à l'exécution d'une fonction spécifique. En particulier, avec la capacité des nœuds de sentir, traiter et communiquer les

données, elles sont bien convenues pour exécuter la détection d'événement, qui est clairement une application en avant des réseaux sans fil de capteurs [8].

1.3.1 Un capteur

Un capteur est un petit appareil autonome capable d'effectuer des mesures simples sur son environnement immédiat, comme la température, la vibration, la pression, etc. Chaque capteur assure trois fonctions principales : la collecte, le traitement et la communication de l'information vers un ou plusieurs points de collecte appelés station de base (SB) [9].

1.3.2 Architecture d'un capteur

Un capteur se compose des éléments suivants :

- Unité de traitement
- Unité de capture
- Unité de communication
- Unité d'alimentation

- **Unité de traitement** : L'unité principale du capteur, est un processeur ajouté à une mémoire vive RAM. Il gère le mouvement des autres unités pour établir un bon fonctionnement. Sur certains capteurs elle peut embarquer un système d'exploitation pour faire fonctionner le capteur. Elle peut aussi être couplée à une unité de stockage, qui servira par exemple à y enregistrer les informations transmises par l'unité de capture.
- **Unité de capture** : L'unité d'acquisition est composée d'un capteur qui va des mesures numériques sur les paramètres environnementaux et d'un convertisseur analogique/numérique qui va convertir l'information relevée et la transmettre à l'unité de traitement.
- **Unité de communication** : L'unité de transmission est responsable de toutes les émissions et réceptions de données via un support de communication radio.

- **Unité d'alimentation** : Elle considérée comme une batterie pour alimenter les trois autres unités.

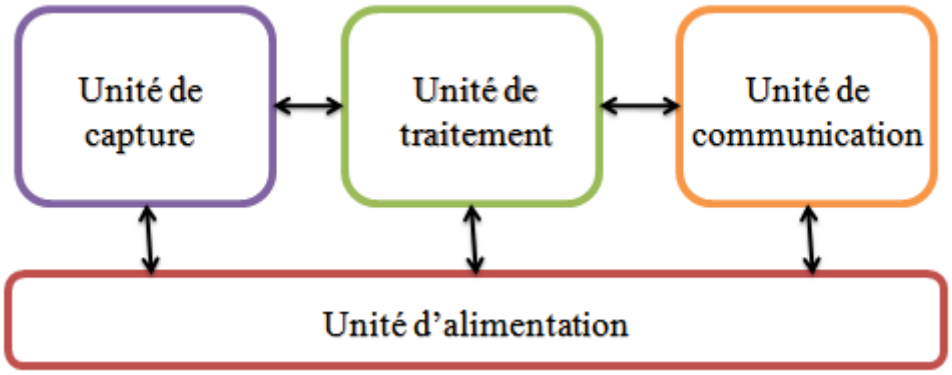

Figure 3: Architecture d'un capteur.

1.3.3 Caractéristiques des réseaux de capteurs sans fil

Un ensemble de caractéristiques sont importantes pour l'accomplissement des tâches assignées aux applications. Les plus importants sont :

- **Le type de service :** on s'attend à ce que le RCSF (réseaux de capteurs sans fil) offre à l'utilisateur, des informations significatives sur l'objet d'intérêt [10].

- **La Qualité de service QoS :** C'est une métrique de la qualité de service qui va être offerte par un RCSF à ses utilisateurs/applications. Le niveau de QoS est défini par un ensemble d'attributs comme le temps d'attente, la largeur de bande, et la perte de paquets qu'on relie directement avec le type de service du réseau. Dans QoS pour les RCSFs, la quantité et la qualité d'information extraites à partir des puits deviennent appropriées [10].

- **Tolérance aux fautes :** il est important que le RCSF soit capable de traiter l'échec des nœuds capteurs. Une manière reconnue de satisfaire cette contrainte est de réaliser un déploiement redondant des nœuds capteurs [10].

- **La durée de la vie :** C'est la durée pendant laquelle le réseau reste opérationnel. On s'attend à ce que le RCSF puisse fonctionner au moins pendant le temps requis pour accomplir la tâche donnée. Néanmoins, la définition de la durée de vie dépend de l'application du RCSF et elle est en relation directe avec le fonctionnement efficace du réseau [10].

- **Scalabilité :** Cette caractéristique traduit la capacité de maintenir la performance indépendamment de la taille du réseau. Comme un grand nombre de nœuds de capteur peuvent être employés dans les applications de RCSF, les architectures et les protocoles doivent fournir le support approprié pour maintenir efficacement les services fournis par le réseau [10].

- **Maintenance :** les changements dans l'environnement du réseau, par exemple, l'apparition de nœuds de capteurs avec des batteries épuisées, exigent une solution permettant l'adaptation et le maintien des services du RCSF [10].

- **Programmation flexible :** C'est la capacité des nœuds de capteur à modifier les options de traitement des données acquises et à effectuer des changements et des ajustements de leurs tâches [10].

1.3.4 Applications des réseaux de capteurs sans fil

La diminution de taille et de coût des capteurs augmente l'utilisation du WSN chaque jour, l'élargissement de la gamme des types de capteurs disponibles (thermique, optique, vibrations, MultiMedia …) et l'évolution des supports de communication sans fil ont élargi le champ d'application des réseaux de capteurs. Alors que ces petits appareils pourraient être en mesure de collecter et de traiter des informations complexes provenant de l'environnement (météorologie, étude des courants, de l'acidification des océans, de la dispersion de polluants, de propagules, etc.). Cette partie expose quelque exemple d'applications potentielles.

❖ **Applications militaires**

Comme pour de nombreuses autres technologies, le domaine militaire a été le moteur initial pour le développement des réseaux de capteurs. Le déploiement rapide, le coût réduit, l'auto-organisation et la tolérance aux pannes des réseaux de capteurs sont des caractéristiques qui font de ce type de réseaux un outil appréciable dans un tel domaine. Actuellement, les RCSFs peuvent être une partie intégrante dans le commandement, le contrôle, la communication, la surveillance, la reconnaissance, etc [11].

❖ **Applications environnementales**

Dans ce domaine, les capteurs peuvent êtres exploités pour détecter les catastrophes naturelles (feux de forêts, tremblements de terre, etc.), détecter des fruits des produits toxiques (gaz, produits chimiques, pétrole, etc.) dans des sites industriels tels que les centrales nucléaires et les pétrolières [11].

❖ **Applications à la sécurité**

L'application des réseaux de capteurs dans le domaine de la sécurité peut diminuer considérablement les dépenses financières consacrées à la sécurisation des lieux et des êtres humains. Ainsi, l'intégration des capteurs dans de grandes structures telles que les ponts ou les bâtiments aidera à détecter les fissures et les altérations dans la structure suite à un séisme ou au vieillissement de la structure [11].

❖ **Applications médicales**

Les réseaux de capteurs sont également largement répandus dans le domaine médical. Cette classe inclut des applications comme : fournir une interface d'aide pour les handicapés, collecter des informations physiologiques humaines de meilleure qualité, facilitant ainsi le diagnostic de certaines maladies, surveiller en permanence les malades et les médecins à l'intérieur de l'hôpital [11].

❖ **Applications commerciales**

Parmi les domaines dans lesquels les réseaux de capteurs ont aussi prouvé leur utilité, on trouve le domaine commercial. Dans ce secteur on peut énumérer plusieurs applications comme : la surveillance de l'état du matériel, le contrôle et l'automatisation des processus d'usinage, etc. [11].

❖ **Applications agricoles**

Dans le domaine de l'agriculture, les capteurs peuvent être utilisés pour réagir convenablement aux changements climatiques par exemple le processus d'irrigation lors de la détection de zones sèches dans un champ agricole [12].

Figure 4 : domaines d'applications des réseaux de capteurs sans fil.

1.3.5 Problèmes des réseaux de capteurs sans fil

➢ **Consommation d'énergie** : L'économie d'énergie est une des problématiques majeures dans les réseaux de capteurs. En effet, la recharge des sources d'énergie est souvent trop coûteuse et parfois impossible. Il faut donc que les capteurs économisent au maximum l'énergie afin de pouvoir fonctionner. En effet, un réseau de capteurs ne peut pas survivre si la perte de nœuds est très importante car ceci engendre des pertes de communications dues à une très grande distance entre les nœuds restants. Les

réseaux de capteurs fonctionnant selon un mode de routage par saut, chaque nœud du réseau joue un rôle important dans la transmission de données. Le mauvais fonctionnement d'un nœud implique un changement dans la topologie et impose une réorganisation du réseau [13].

- **Routage** : les protocoles de routage dans les réseaux ad hoc (DSDV, TORA, DSR.....) ne sont pas adaptés pour les réseaux de capteurs sans fils a cause que ces protocoles sont censés appliquer trois fonctions principales : la détermination et la détection des changements de la topologie du réseau, le maintien de la connectivité réseau et le calcul et la sélection des bon itinéraires. Par contre dans les réseaux de capteurs sans fils, moins d'effort donnée aux protocoles de routages. et malgré ça, certains avantages de ces protocoles se rapportent aux caractéristiques des réseaux de capteurs sans fils, comme la communication multi-sauts et le routage QoS [14].

- **Localisation** : Un système de localisation existe déjà, qui est disponible sur toute la surface du globe le GPS. Pourtant, il n'est pas satisfaisant pour l'usage nécessaire, car il cumule les handicaps. Il est disponible seulement en extérieur, et encore si aucun obstacle ne vient obstruer le champ de vue des récepteurs : le fonctionnement sous un feuillage dense, ou dans des villes aux rues étroites, n'est pas possible, où seulement dans de très mauvaises conditions. De plus il est particulièrement coûteux, et la réception du signal est très gourmande en énergie [14].

- **Sécurité** : En fonction de l'application, la sécurité peut être critique. Le réseau devrait permettre la détection des intrusions et la tolérance, ainsi qu'un fonctionnement robuste dans le cas de défaillance parce que, souvent, les nœuds capteur ne sont pas protégés contre les mauvaises manipulations ou attaques. L'écoute, le brouillage, et les attaques de retransmission peuvent entraver ou empêcher l'opération ; par conséquent, le contrôle d'accès, l'intégrité des messages, et la confidentialité doit être garanti [14].

- **Tolérances aux pannes** : Les nœuds peuvent être exposés aux pannes et aux manques d'énergie a cause de leurs fabrication (ce sont des produits de série bon marché, il peut donc y avoir des capteurs défectueux). Quand un nœud se panne il ne doit pas affecter le fonctionnement global de son réseau. La tolérance aux pannes est donc la capacité de maintenir les fonctionnalités du réseau sans interruption due à une panne d'un nœud capteur [13].

- **Agrégation des données** : Les données produites par les nœuds dans les réseaux de capteurs sans fil sont très reliées, ce qui implique l'existence de redondances de données. Une approche répandue consiste à agréger les données au niveau des nœuds intermédiaires afin de réduire la consommation d'énergie lors de la transmission de ces données [13].

- **Environnement** : les capteurs doivent pouvoir fonctionner sans surveillance dans des régions géographiquement éloignées ou inaccessibles. Parce que ces capteurs peuvent fonctionner sous haute pression au fond de l'océan, dans un environnement dur tel que les champs de bataille, dans des champs biologiquement ou chimiquement souillés ou même dans des milieux extrêmement froids [13].

1.4 Les réseaux ad hoc mobiles MANET

1.4.1 Définition

Les réseaux ad-hoc mobiles, appelés MANET (Mobile Ad-hoc Network) aussi, sont formés dynamiquement par un grand nombre de stations mobiles (nœuds) qui se connectent sans utiliser d'infrastructure existante mais en se servant des interfaces sans fils (onde radio) comme moyen de communication. Les nœuds interagissent et peuvent coopérer pour s'échanger des services. Ces nœuds sont donc libres de se déplacer et de s'organiser arbitrairement, impliquant une grande variabilité de la topologie du réseau. Généralement, les routes entre les nœuds d'un tel réseau sont constituées de plusieurs sauts (hops). Chaque nœud est capable de communiquer directement avec ses voisins (se trouvant dans la zone de

portée de leur antenne), voisins par lesquels ils passent pour communiquer avec des nœuds plus éloignés donc peut servir comme relais aux autres nœuds du réseau [15].

Figure 5: Réseau ad hoc mobile MANET. [15]

1.4.2 Caractéristiques des réseaux ad hoc

- **L'absence d'infrastructure** : les réseaux ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructures préexistante et de tout genre d'administration centralisée. Les équipements des unités mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue [15].

- **Une topologie dynamique** : les unités mobiles du réseau, se déplacent d'une façon libre et arbitraire. Par conséquent la topologie du réseau peut changer, à des instants

imprévisibles, d'une manière rapide et aléatoire. Les liens de la topologie peuvent être unis ou bidirectionnels [15].

- **Les contraintes d'énergie** : les unités mobiles sont alimentées par des sources d'énergie autonomes comme les batteries ou les autres sources consommables et par conséquent d'une durée de traitement réduite. Sachant qu'une partie de l'énergie est déjà consommée par la fonctionnalité du routage, cela limite les services et les applications supportées par chaque nœud. Le paramètre d'énergie doit être pris en considération dans tout contrôle fait par le système [15].

- **Une bande passante limitée** : un des caractéristiques primordiales des réseaux basés sur la communication sans fil est l'utilisation d'un médium de communication partagé. Ce partage fait que la bande passante réservée à un hôte soit faible. La limitation de la bande passante influe considérablement sur le volume des informations échangées [15].

- **Une sécurité physique limitée** : les réseaux mobiles ad hoc sont plus touchés par le paramètre de sécurité, que les réseaux filaires. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé due les grandes possibilités d'insérer des nœuds (unités mobiles) dans le réseau et donc la détection d'une intrusion est plus délicate, et l'absence de centralisation pose un problème de remontée de l'information et de détection d'intrusions [15].

- **Equivalence des nœuds du réseau** : dans un réseau classique, il existe une distinction nette entre les nœuds terminaux (stations, hôtes) qui supportent les applications, et les nœuds internes (routeurs par exemple) du réseau, en charge de l'acheminement des données. Cette différence n'existe pas dans les réseaux ad hoc car tous les nœuds peuvent être amenés à assurer des fonctions de routage. Donc, les nœuds combinent les rôles de routeur et de station hôte, permettant ainsi d'acheminer de façon autonome, les paquets d'un usager à un autre [15].

- **L'hétérogénéité des nœuds** : un nœud mobile peut être équipé d'une ou plusieurs interfaces radio ayant des capacités de transmission variées et opérant dans des plages de fréquence différentes. Cette hétérogénéité de capacité peut engendrer des liens asymétriques dans le réseau. De plus, les nœuds peuvent avoir des différences en termes de capacité de traitement (CPU, mémoire) de logiciel et de mobilité (lent, rapide). Dans ce cas, une adaptation dynamique des protocoles s'avère nécessaire pour supporter de telles situations [15].

- **L'auto configuration** : les réseaux ad hoc sont capables de se configurer sans intervention d'administrateur. Cette configuration consiste au choix d'une adresse IP, la détermination des serveurs DNS du réseau, la détermination du protocole de routage et d'accès au médium... Cette configuration se fait alors grâce à une coopération entre les nœuds du réseau [15].

- **Communication par lien radio** : les communications entre les nœuds se font par l'utilisation d'une interface radio. Il est alors important d'adopter un protocole d'accès au médium qui permet de bien distribuer les ressources radio et ceci en évitant le plus possible les collisions et en réduisant les interférences. Les technologies de communication sans fil sont alors indispensables à la mise en place d'un réseau ad hoc. Malgré des progrès très importants, leurs performances restent et resteront en deçà de celles des technologies des réseaux filaires [15].

- **Le multihops** : les nœuds mobiles peuvent participer au routage et servent comme routeurs intermédiaires [15].

1.4.3 Modélisation des réseaux ad hoc mobiles

Un réseau ad hoc peut être modélisé par un graphe Gt = (Vt, Et), où : Vt représente l'ensemble des nœuds (i.e. les unités ou les hôtes mobiles) du réseau et Et modélise l'ensemble des connections qui existent entre ces nœuds. Si e = (u, v) appartient à Et, cela veut dire que les nœuds u et v sont en mesure de communiquer directement à l'instant t. La figure suivante représente un réseau ad hoc de 9 unités mobiles sous forme d'un graphe [15]:

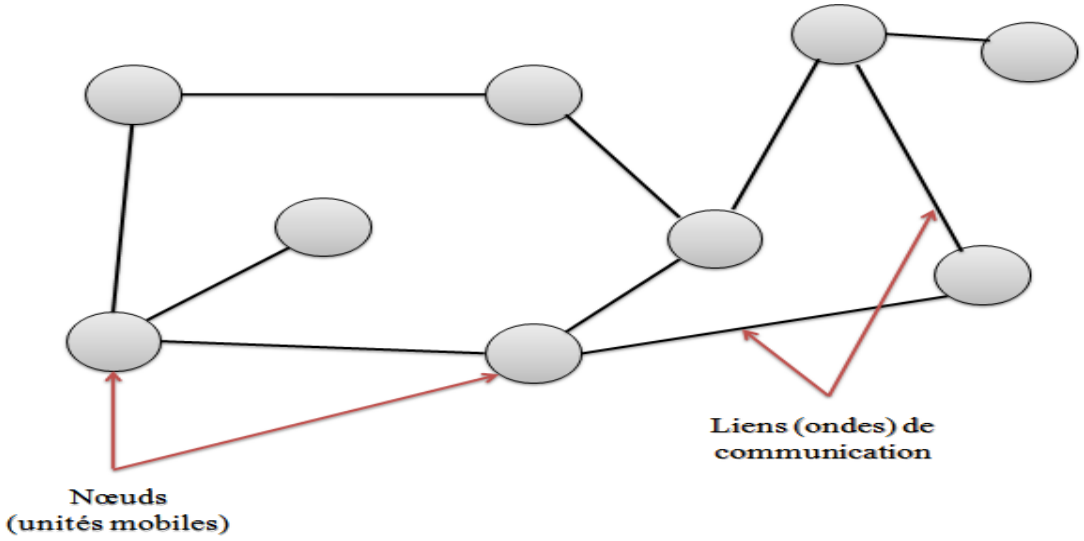

Figure 6: Modélisation d'un réseau ad hoc mobile.

1.4.4 Les avantages et les inconvénients des réseaux ad hoc mobiles

A) Les avantages

Les réseaux mobiles Ad Hoc sont utiles quand aucune connexion filaire n'est disponible, par exemple lors d'une opération militaire, et plus généralement quand le déploiement rapide d'un réseau est nécessaire. Dans ce cas, les nœuds communiquent en acheminant les messages par routage « multi-saut ». Indépendamment du fait de disposer ou non d'une infrastructure, le mode Ad Hoc multi-saut a de nombreux avantages en comparaison avec le mode de communication avec stations de base :

- **Pas de câblage** : l'une des caractéristiques des réseaux Ad Hoc est l'absence d'un câblage, et ce en éliminant toutes les connexions filaires qui sont remplacées par des connexions radio [15].

- **Déploiement facile, rapide et peu onéreux** : l'absence du câblage donne plus de souplesse, et permet de déployer un réseau Ad Hoc facilement et rapidement. Cette facilité peut être justifiée par l'absence d'une infrastructure préexistante permettant, ainsi, d'économiser tout le temps de déploiement et d'installation du

matériel nécessaire. Donc dans les situations d'urgence comme en cas de catastrophes, il sera facile de former un réseau ad hoc rapidement pour organiser une opération de secours [15].

- **Adaptation en milieu urbain** : les réseaux ad hoc s'adaptent bien en milieu urbain à cause des obstacles physiques. En effet, contrairement à un réseau sans fil avec infrastructure sans lequel une connexion est perdue entre le point d'accès et le récepteur si un mur les sépare, dans un réseau ad hoc, l'émetteur va établir une connexion en passant par un ou plusieurs nœuds intermédiaires pour le contourner [15].

- **Permet la mobilité** : comme l'indique leur nom, et à l'image des réseaux sans fil avec infrastructure, les réseaux mobiles Ad Hoc permettent une certaine mobilité à leurs nœuds. De ce fait, ces derniers peuvent se déplacer librement à condition de ne pas s'éloigner trop les uns des autres pour garder leur connectivité [15].

- **Extensible** : l'une des propriétés les plus importantes d'un réseau Ad Hoc est la possibilité de l'étendre, et d'augmenter sa taille très facilement et sans nécessiter trop de moyens. Pour expliquer cet aspect, il suffit uniquement d'imaginer l'arrivée d'un nouveau nœud mobile à un réseau Ad Hoc déjà installé et mis en place. Pour que ce nœud fonctionne au sein du réseau, il suffit de procéder à quelques configurations au niveau du nœud lui-même [15].

- **Coût** : le déploiement d'un réseau Ad Hoc ne nécessite pas d'installer des stations de base, les mobiles sont les seules entités physiques nécessaires pour déployer un tel réseau. Ce qui conduit à la réduction de son coût d'une manière significative [15].

B) Les inconvénients

Cependant, les réseaux ad hoc ont aussi des inconvénients que nous pouvant résumer comme suit :

- **Topologie non prédictible** : l'activité permanente et les déplacements fréquents des nœuds d'un réseau Ad Hoc rendent son étude très difficile. La raison est bien connue, le changement rapide de sa topologie dû aux déplacements des nœuds [15].

- **Capacités limitées (puissance de calcul, mémoire, énergie)** : dans un tel réseau, la configuration de la portée de communication des nœuds (ce qui revient à paramétrer la puissance d'émission) est importante. En effet, il faut qu'elle soit suffisante pour assurer la connectivité du réseau. Mais plus on accroît la portée des mobiles, plus les communications demandent de l'énergie. Il faut donc trouver un compromis entre la connectivité du réseau et la consommation énergétique [6].

- **Délai important** : les réseaux ad hoc ont dans la plupart des cas une latence plus importante que celle des réseaux sans fil avec infrastructure. En effet afin de joindre une destination, les données doivent parfois traverser de nombreuses machines. Chaque relais ajoutera un délai supplémentaire au temps d'acheminement [15].

- **Taux d'erreur important** : les risques de collisions augmentent avec le nombre de nœuds qui partagent le même médium. Par conséquent, plus la portée augmente, plus le risque de collisions n'est important. Le protocole de routage doit disposer d'une gestion d'erreur appropriée sinon il serait possible de perdre des paquets critiques de sécurité [15].

- **Sécurité** : un autre dilemme des réseaux Ad Hoc, et qui attire la curiosité des chercheurs et des spécialistes de ce domaine est la notion de sécurité. Un réseau Ad Hoc tel que définit précédemment ne permet pas d'assurer la confidentialité de l'information échangée entre les nœuds. Contrairement aux réseaux filaires, les réseaux sans fil sans infrastructure ne peuvent utiliser un matériel spécifique (firewall par exemple) pour empêcher les accès non autorisés au réseau [15].

- **La bande passante limitée** : un des effets de ces débits relativement faibles est que la congestion sera généralement la norme plus que l'exception. La demande sur les applications distribuées dépasse souvent la capacité du réseau. Comme le réseau mobile est souvent une simple extension d'un réseau fixe, les utilisateurs mobiles Ad Hoc demandent les mêmes services. Cette demande ne cessera de croître avec l'augmentation des traitements multimédias et des applications basées sur les réseaux [15].

- **Le problème de qualité de service (QoS)** : De ce fait les protocoles de qualité de service habituels ne sont pas utilisable directement dans le monde ad hoc et des solutions spécifiques doivent être proposés, Il est difficile d'établir une QoS sur un réseau ad hoc car les éléments composant une route d'acheminement sont susceptibles de disparaître à tout moment [15].

- **Sécurité physique limitée** : de leur nature, les réseaux sans fil sont très sensibles aux attaques extérieures. La topologie de ces réseaux favorise ce genre de menaces, donc on ne peut appliquer les techniques de sécurité traditionnelles conçues pour les réseaux filaires [15].

1.4.5 Les domaines d'applications des réseaux ad hoc mobiles

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

- **Les applications militaires** : les réseaux 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 troupes unités d'une armée [15].

- **Les opérations de secours** : dans les zones touchées par les catastrophes naturelles (cyclone, séisme, etc.), le déploiement d'une infrastructure de communication fixe n'est pas envisageable, mais la communication entre équipes de secours est nécessaire au bon déroulement des opérations de sauvetage. La rapidité de déploiement des réseaux ad hoc fait d'eux une solution idéale pour ce genre de situation [15].

- **L'utilisation privée** : un réseau ad hoc peut être très bien utilisé à l'intérieur d'une maison (Home Network) où un ensemble de robots ou d'équipements peuvent s'échanger des informations pour mieux organiser les tâches ménagères par exemple [15].

- **L'utilisation à des objectifs éducatifs** : 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 étudiants de partager des ressources (fichiers, accès à internet…etc.) et de communiquer sans avoir besoin d'une quelconque infrastructure [15].

- **Applications industrielles** : des scénarios plus complexes dans le domaine industriel appelés réseaux de capteurs (Sensor Networks) peuvent former un MANET pour s'adapter à différents environnements. Un exemple d'une telle application est la formation d'un MANET pour la surveillance médicale, la détection des Feux de forêt, la surveillance des volcans…etc [15].

- **Mise en œuvre des réseaux véhiculaires** : sur un réseau routier les véhicules peuvent avoir besoin de communiquer entre eux ou avec leur environnement afin de partager des informations dans le but de gérer et réguler le trafic routier. Le déplacement à grande vitesse des véhicules rend impossible l'établissement de réseaux avec infrastructure entre eux, les réseaux ah hoc sont alors la solution idéale [15].

1.5 Conclusion

Dans ce chapitre, nous avons présenté les réseaux de capteurs sans fil ainsi que leurs applications dans les différents domaines de la vie. Et nous avons présenté aussi les réseaux ad hoc mobiles MANET. Le réseau Ad hoc manifeste beaucoup de simplicité et assez d'avantages par rapport aux autres réseaux (filaires et cellulaires) par sa facilité de déploiement en cas d'urgence ou de travaux temporaires dont les autres réseaux engendrent des frais importants. Cependant de nouveaux problèmes apparaissent, en effet l'absence d'une infrastructure centralisée fait du routage dans les réseaux ad hoc un problème très compliqué. Dans la plupart des cas, le nœud destination ne se trouve pas obligatoirement dans la portée du nœud source ce qui implique que l'échange des données entre les deux nœuds, doit être effectué par des stations intermédiaires. Par ailleurs, la topologie de ces réseaux qui peuvent être continuellement mobile oblige les protocoles de routage à réagir rapidement.

Après avoir présenté l'environnement mobile ad hoc, une étude sur le routage et les techniques anti-brouillages dans cet environnement sera faite dans le chapitre prochain.

CHAPITRE 2

LE ROUTAGE DANS LES RÉSEAUX MOBILES AD HOC ET LES TECHNIQUES ANTI-BROUILLAGES (ETAT DE L'ART)

Chapitre 2

Le routage dans les réseaux mobiles Ad Hoc et les Techniques Anti-brouillages (Etat de l'art)

2.1 Introduction

Aujourd'hui, les réseaux sans fil deviennent populaires à cause de progrès de la technologie sans fil et la popularité croissante des périphériques sans fil. Le réseau MANET est un réseau indépendant de l'infrastructure avec des nœuds mobiles sans fil dont ces nœuds sont libres de rejoindre et de quitter le réseau, ce qui implique des défis de sécurité dans le réseau tels que les attaques de brouillage, pour cela plusieurs techniques ont été créés et développés pour éviter les problèmes de sécurité dans les réseaux MANET.

Le chapitre est organisé comme suit : la première section présente quelques protocoles de routage dans les réseaux MANET. La deuxième section, présente un bref aperçu sur le principe de brouillage et quelques techniques de détection et contre-mesure de brouillage.

2.2 Les protocoles de routage dans les réseaux MANET

2.2.1 Les protocoles de routage proactifs

Les protocoles de routage utilisés dans les réseaux filaires conventionnels, tels que le protocole Etat de Lien (Link State) et le protocole du Vecteur du Distance (Distance Vector), exigent une mise à jour périodique des données de routage qui doit être diffusée par les différents nœuds de routage du réseau. Cette philosophie est utilisée dans les protocoles de routage proactifs. Pour cela, nous allons examiner ces deux principales méthodes avant de présenter quelques protocoles de cette classe.

Dans le protocole "Link State", chaque nœud de routage maintient sa propre vision de la topologie du réseau et qui inclut l'état de ses canaux de sortie. Pour que cette vision soit à jour, chaque nœud diffuse (par inondation) périodiquement l'état des liens de ses voisins à tous les nœuds du réseau. Cela est fait aussi quand il y a un changement d'état de liens.

Dans le protocole de routage "Distance Vector", chaque nœud de routage diffuse à ses nœuds de routage voisins, sa vision des distances qui le séparent de tous les hôtes du réseau. En se basant sur les informations reçues depuis tous ses voisins, chaque nœud de routage fait un certain calcul pour trouver le chemin le plus court vers n'importe quelle destination. Le processus de calcul se répète, s'il y a un changement de la distance minimale séparant deux nœuds, et cela jusqu'à ce que le réseau atteigne un état stable.

Les protocoles de routage proactifs essaient d'adopter les idées des deux protocoles précédents pour les environnements mobiles en essayant de réduire ou d'éliminer leurs limitations tout en prenant en considération, les caractéristiques du nouvel environnement [16].

1. ***Le protocole DSDV (Dynamic Destination Sequenced Distance Vector)***

Le protocole de routage de vecteur de distance ordonnancé par distance DSDV a été conçu spécialement pour les réseaux mobiles. Il est basé sur l'idée classique de l'algorithme distribué de Bellman-Ford en ajoutant quelques améliorations.

Des perfectionnements sont faits afin d'éviter le problème des boucles présentes dans DBF (Distributed Bellman-Ford). Ceci est évité en étiquetant chaque entrée de table de routage avec un numéro de séquence pour commander l'information de routage.

Chaque nœud du réseau maintient dans sa table de routage un ensemble d'informations pour chaque destination contenant [16]:

- L'adresse du destinataire : l'identifiant du prochain nœud vers cette destination.
- Le nombre de sauts (nœuds) nécessaire pour l'atteindre.
- Le plus grand numéro de séquence reçu pour cette destination. Il est utilisé pour permettre au nœud mobile de faire la distinction entre les anciennes routes et les nouvelles routes découvertes vers cette destination pour éviter la formation des boucles de routage.

La mise à jour de la table de routage peut se faire de deux façons [17] :

- **Une mise à jour complète** : dans ce cas l'unité mobile transmet la totalité de la table de routage aux voisins, ce qui nécessite l'envoie de plusieurs paquets de données.
- **Une mise à jour incrémentale** : dans ce cas seuls les nouvelles entrées ou celles qui ont subi un changement par rapport à la dernière mise à jour, sont envoyées, ce qui réduit le nombre de paquets transmis.

2. Le protocole OLSR (Optimized Link State Routing)

Le protocole OLSR (Optimized Link State Routing) est une version adaptée au cas des réseaux sans fi l du protocole LSR (Link State Routing) utilisé pour les réseaux filaires ; en introduisant la notion de MPR. Les MPR sont des nœuds élus qui assurent le relais de l'information dans le réseau. Chaque nœud émet la liste de ses voisins mais seuls les nœuds MPR la rediffusent (la Figure 7). Ce sont les nœuds MPR qui assurent le routage dans le réseau [18].

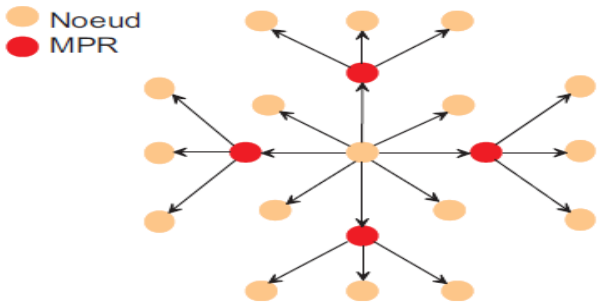

Figure 7: Le principe des nœuds MPR. [18]

Le protocole OLSR est performant dans les réseaux denses car les MPR permettent de limiter l'inondation du réseau. De plus il est très réactif, chaque nœud sait à tout moment comment atteindre les autres. Par contre, en termes de consommation énergétique, il sollicite beaucoup les nœuds car ils doivent émettre en permanence des messages et c'est en émission que les supports radio consomment le plus : OLSR est difficilement applicable pour des réseaux de capteurs [18].

Il existe d'autre protocoles de routage proactifs tels que :

- WRP : Wireless Routing Protocol
- GSR : Global State Routing
- FSR : Fisheye State Routing
- CGSR: Cluster-Getway Switching Routing
- HSR : Hierarchical State Routing
- ZHLS: Zone Based Hierarchical Link State

Mais les deux protocoles (DSDV et OLSR) sont les plus utilisés.

3. Les avantages et les inconvénients des protocoles proactifs

A) Avantages

Avec un protocole proactif, les routes sont disponibles immédiatement, ainsi l'avantage d'un tel protocole est le gain de temps lors d'une demande de route.

B) Inconvénients

Le problème est que, les changements de routes peuvent être plus fréquents que la demande de la route et le trafic induit par les messages de contrôle et de mise à jour des tables de routage peut être important et partiellement inutile, ce qui gaspille la capacité du réseau sans fil. De plus, la taille des tables de routage croit linéairement en fonction du nombre de nœud.

De ce fait, un nouvel type de protocole a apparu, il s'agit des protocoles de routage réactifs.

2.2.2 Les protocoles de routage réactifs

Les protocoles de routage réactifs (dits aussi : protocoles de routage à la demande), représentent les protocoles les plus récents proposés dans le but d'assurer le service du routage dans les réseaux sans fils. La majorité des solutions proposée pour résoudre le problème de routage dans les réseaux ad hoc, et qui sont évaluées actuellement par le groupe de travail MANET appartiennent à cette classe de protocoles de routage. Les protocoles de routage appartenant à cette catégorie, créent et maintiennent les routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et cela dans le but d'obtenir une information [16].

Actuellement, le plus connu de ces protocoles est AODV.

1. Le protocole DSR (Dynamic Source Routing)

Le protocole DSR est un protocole réactif qui s'appuie sur deux sortes de paquets. Lorsqu'un nœud veut émettre un message, il fait une demande de route au moyen d'un paquet RREQ envoyé au destinataire. Ce paquet est propagé dans le réseau jusqu'à atteindre le destinataire, chaque station retransmettant le paquet modifié en inscrivant son adresse dans le

champ actualisant ainsi la route prise par le paquet. Lorsque le destinataire reçoit le paquet RREQ, il répond à la source avec un paquet RREP lui indiquant la route pour l'atteindre. La Figure 8 illustre le principe de découverte d'une route entre le nœud A et le nœud G. Il peut malgré tout y avoir des problèmes en cas de lien asymétrique et des problèmes d'irrégularités au niveau des ondes électromagnétiques, la route de retour n'étant pas forcement possible [18].

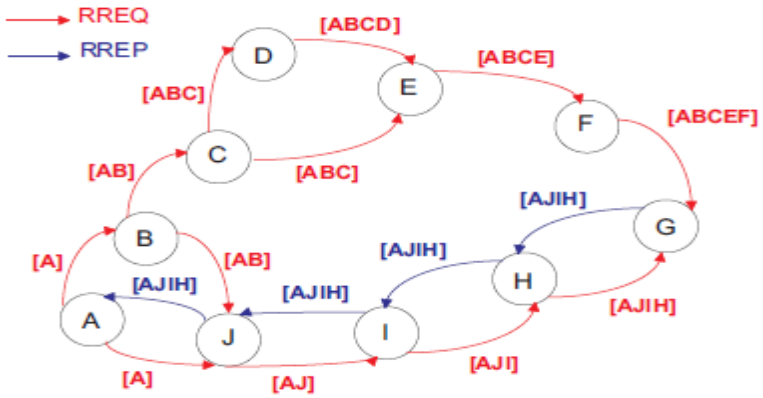

Figure 8: Le principe de découverte de route dans le protocole DSR. [18]

2. *Le protocole AODV (Ad hoc On demand Distance Vector)*

Le protocole AODV reprend les principes du protocole DSR pour la recherche des routes, mais afin de limiter le trafic, il diminue la taille des paquets en n'incluant pas toute la route au niveau de ceux-ci. Ce sont les nœuds intermédiaires qui stockent les routes au niveau de la table de routage. Lors de la réponse à une demande de route, le paquet utilise ces tables pour revenir à la source de la demande. Ces tables sont en cache et peuvent accélérer ainsi la découverte d'une route. Des messages "Hello" sont également utilisés afin de connaître la validité des liens [18].

Il existe d'autre protocoles de routage réactifs tels que :

- LMR : Lightweight Mobile Routing
- ABR : Associativity Based Routing

- SSR : Signal Stability Routing
- RDMAR: Relative Distance Micro-discovrey Ad hoc Routing

3. Les avantages et les inconvénients des protocoles réactifs

A) Avantages

A 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 de ne pas gaspiller les ressources du réseau.

B) Inconvénients

La mise en place d'une route par inondation peut être coûteuse et provoquer des délais importants avant l'ouverture de la route et les retards dépassent bien souvent les délais moyens admis par les logiciels, aboutissant à une impossibilité de se connecter alors que le destinataire est bien là.

De ce fait, un nouvel type de protocole a apparu, il s'agit des protocoles de routage hybrides.

2.2.3 Les protocoles de routage hybrides

Les protocoles dits hybrides ont un fonctionnement moins caractéristique que les deux précédents types. Ils peuvent voir leur comportement varier suivant les liens entre les nœuds du réseau, la position des nœuds dans le réseau ou l'état de fonctionnement du nœud en termes de capacité énergétique par exemple.

1. Le protocole ZRP (Zone Routing Protocol)

Le protocole ZRP utilise en fait deux protocoles de routage, un proactif et un réactif. Une taille de zone en nombre de sauts est définie, par exemple, comme sur la Figure 9. Les nœuds présents dans la zone A à 2 sauts sont gérés suivant un protocole proactif : le protocole IARP [18].

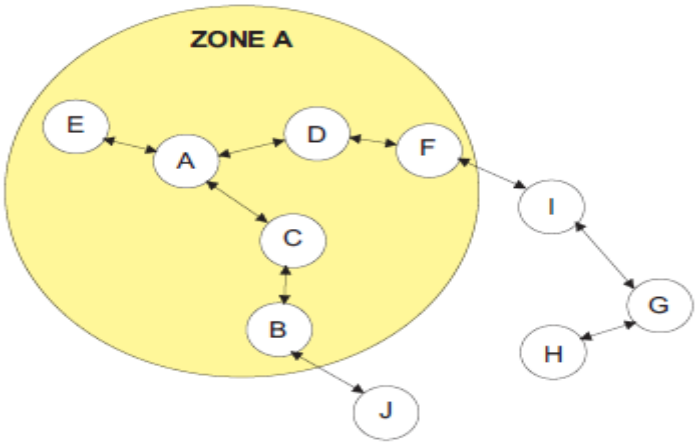

Figure 9: Le principe des zones dans le protocole ZRP. [18]

Les paquets de contrôle possèdent une durée de vie en nombre de sauts ; lorsqu'un nœud reçoit un paquet de contrôle, il actualise sa table de routage et il retransmet le paquet en décrémentant la durée de vie du paquet. Lorsque la durée de vie du paquet de contrôle est nulle, la bordure de zone est atteinte et le paquet n'est plus retransmis. Les nœuds hors de la zone A sont atteints grâce à un protocole réactif : le protocole IERP. Un troisième protocole gère les transitions entre les deux précédents : le protocole BRP [18].

Il existe d'autre protocoles de routage réactifs tels que :

- Cluster Based Routing Protocol (CBRP)
- Energy Aware Dynamic Source Routing (EADSR)
- …

2. Les avantages et les inconvénients de routage hybrides

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 découpe du réseau.

Cependant, il rassemble toujours quelques inconvénients des deux approches proactives et réactives.

2.2.4 Les protocoles de routage géographiques

Les protocoles de routage géographiques se différencient de ceux précédemment présentés par l'utilisation d'une donnée supplémentaire dans la recherche des routes : la position géographique des nœuds du réseau. Cette position peut être obtenue de différentes façons [18]:

- Par l'utilisation d'un récepteur GPS au niveau de chaque nœud du réseau
- Par l'utilisation d'un récepteur GPS pour seulement quelques nœuds du réseau afin d'optimiser la recherche des routes dans les protocoles classiques
- Par l'utilisation du signal radio pour localiser les nœuds par triangulation par rapport à des points de référence

Il existe plusieurs protocoles de routage géographiques tels que :

- DREAM : Distance Routing Effect Algorithm for Mobility
- LAR : Location Aided Routing
- GPSR: Greedy Perimeter Stateless Routing

2.3 Les techniques Anti-brouillages

2.3.1 Attaque de brouillage

Le brouillage dans les réseaux sans fil est défini comme la perturbation des communications sans fil existantes en diminuant le rapport signal / bruit aux côtés du récepteur par la transmission de signaux sans fil interférents. Le brouillage est différent des interférences régulières du réseau car il décrit l'utilisation délibérée de signaux sans fil dans le but de perturber les communications, tandis que les interférences se réfèrent à des formes involontaires de perturbations. Des interférences involontaires peuvent être causées par les communications sans fil entre les nœuds au sein des mêmes réseaux ou d'autres appareils.

D'autre part, les interférences intentionnelles sont généralement menées par un attaquant qui a l'intention d'interrompre ou d'empêcher les communications dans les réseaux. Le brouillage peut se faire à différents niveaux, de l'entrave à la transmission à la distorsion des paquets dans les communications légitimes [19].

2.3.2 Techniques de brouillage

Le point clé d'une attaque de brouillage réussie est le rapport signal / bruit (SNR), SNR = P_signal / P_bruit, où *P* est la puissance moyenne.

1. ***Brouillage ponctuel :*** la méthode de brouillage la plus populaire est le brouillage ponctuel dans lequel l'attaquant dirige toutes ses transmettre la puissance sur une seule fréquence que la cible utilise avec la même modulation et suffisamment de puissance pour remplacer le signal d'origine. Le brouillage ponctuel est généralement très puissant, mais il peut être facilement évité en passant à un autre la fréquence a cause qu'il brouille une seule fréquence chacun fois [20].

2. ***Brouillage de balayage :*** Lors du brouillage par balayage, le brouilleur est plein la puissance passe rapidement d'une fréquence à l'autre. Bien que cette méthode de brouillage présente l'avantage capable de brouiller plusieurs fréquences en succession rapide, elle ne les affecte pas tous en même temps, et c'est l'efficacité de ce type de brouillage. Cependant, dans un environnement RCSF, il est susceptible de causer des pertes de paquets et retransmissions et, par conséquent, consommer de précieuses ressources énergétiques [20].

3. ***Barrage de brouillage :*** en barrage de brouillage une gamme de fréquences est bloquée en même temps. Son principal avantage c'est qu'il est capable de brouiller plusieurs fréquences à la fois avec suffisamment de puissance pour diminuer le SNR de l'ennemi récepteur. Cependant, comme la plage de fréquences brouillées augmente la puissance de sortie du brouillage est réduite proportionnellement [20].

4. ***Brouillage trompeur*** *:* un brouillage trompeur peut être appliqué dans une seule fréquence ou dans un ensemble de fréquences, il est utilisé lorsque l'adversaire souhaite ne pas la révéler existence. En inondant le RCSF de fausses données, elle peut tromper les mécanismes défensifs du réseau (le cas échéant) et terminer sa tâche sans laisser de traces [20].

2.3.3 Types de brouillage / brouilleur

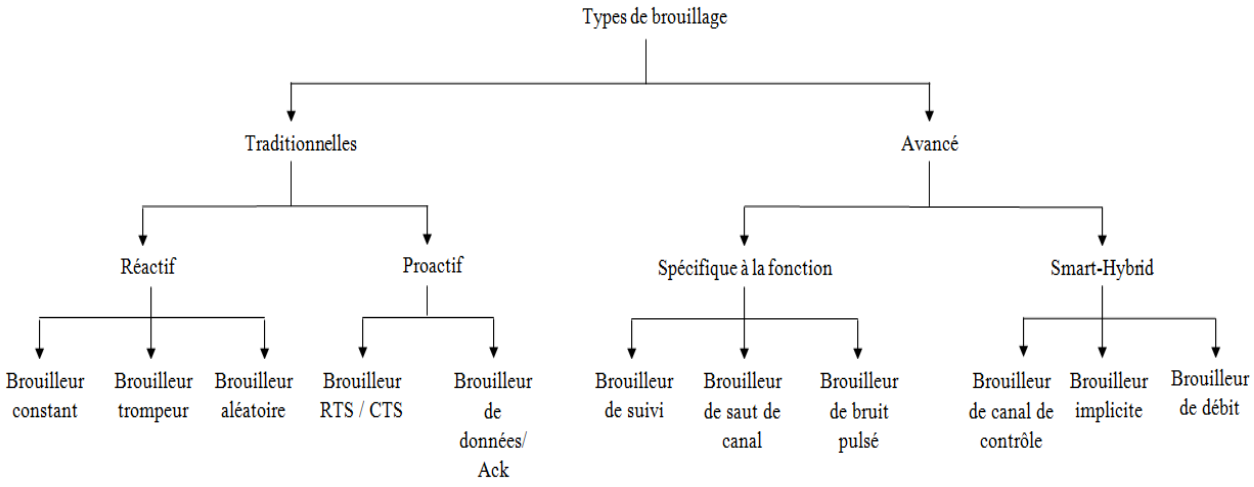

Figure 10: Types de brouillage / brouilleur. [19]

2.3.4 Détection et contre-mesure de brouillage

I. Techniques de détection :

A. Brouillage traditionnelle :

- ***JAM (Jammed-Area Mapping)*** : une méthode de détection et d'atténuation qui cartographie la zone bloquée dans les réseaux de capteurs sans fil et achemine les paquets dans la région affectée. JAM peut cartographier une région bloquée en 1 à 5 secondes. Si l'utilité d'un canal pour un nœud tombe en dessous d'un certain seuil, par exemple le nombre de tentatives infructueuses de capture du canal sans fil est supérieur à 10, la présence d'un brouilleur est détectée. Ensuite, le système de

détection du nœud donne un message JAMMED ou UNJAMMED qui est diffusé à son voisin [19].

- ***Système de fourmis*** : un algorithme évolutif pour détecter le brouillage au niveau de la couche physique et redirige les messages vers un nœud de destination approprié. Il formule une hypothèse pour tester si une attaque DoS est authentique ou non. En obligeant un agent à parcourir le réseau de manière itérative, le système fourmis collecte les informations pour divers itinéraires vers une destination. Ces informations sont ensuite enregistrées dans une liste «tabu» et seront utilisées pour la redirection. Les informations sur l'énergie et la distance sont utilisées pour décider si un brouillage est détecté ou non [19].

- ***Système hybride*** : un système anti-brouillage hybride en combinant 3 techniques de défense: réplication de la station de base (BS), évasion de la station de base et routage par trajets multiples entre les stations de base. Le schéma de réplication implique que plusieurs stations de base répliquées sont présentes dans le réseau. Le schéma d'évasion fait référence au retrait spatial d'une station de base lorsqu'un brouillage est détecté. Le routage à chemins multiples a lieu lorsqu'il existe plusieurs routes de données entre un nœud et une station de base [19].

- ***Système d'inférence floue*** : un mécanisme de détection de brouillage centralisé en calculant l'indice de brouillage en utilisant le rapport signal / bruit (SNR) et les valeurs de paquets abandonnés par terminal (PDPT). Ceci est suivi d'une vérification de confirmation et d'un regroupement à 2 voies des nœuds de voisinage. Une station de base exécute l'algorithme de détection pour obtenir le nombre de paquets reçus par un nœud pendant une période de temps particulière, les paquets abandonnés par le nœud et la force du signal. La station de base calcule ensuite le PDPT et le SNR à partir des données reçues pour percevoir la présence d'un brouilleur [19].

B. Brouillage avancé

- ***Détection et atténuation du brouillage multicouche*** : La détection de brouillage peut être effectuée au niveau de la couche physique ou MAC; cela se fait très rarement sur les couches supérieures. Dans certains cas, la détection de brouillage se fait à l'aide d'approches multicouches. Le protocole est basé sur la couche physique mais utilise les mécanismes de sécurité de la couche supérieure. La détection de brouillage se fait lorsque l'émetteur utilise des motifs de test supplémentaires lors de sa transmission [10].

- ***FIJI (Fighting implicit jamming)*** : une méthode de détection de brouillage inter-couche contre les brouilleurs intelligents en implémentant une partie du système dans le pilote et une partie dans le module réseau. Un point d'accès (AP) exécutant le système FIJI maintient que les clients bloqués reçoivent le débit maximal, tandis que les clients non bloqués ne sont pas affectés. L'algorithme de détection fonctionne en calculant le retard de transmission de données pour chacun des clients connectés à l'AP. Le brouillage est perçu lorsqu'il y a une augmentation brusque du trafic sur la liaison descendante en raison de l'augmentation du temps de retard de transmission du client [19].

II. Techniques de contre-mesure (anti-brouillage) :

A. Brouillage traditionnelle :

- ***Saut de canal*** : Le saut de canal ou le passage d'un canal à un autre est la contre-mesure la plus populaire au brouillage. Récemment, un mécanisme de saut de fréquence piloté par message et contrôlé par code a été proposé. Il génère un motif de saut dynamique à chaque changement de canal. En utilisant la technique de codage de séquence de pseudo-bruit (PN) qui contribue également partiellement à la détection de canaux bloqués à l'aide de capacités de détection de spectre. La conception est proposée pour l'émetteur et le récepteur. C'est une technique de saut efficace lorsque les nœuds ont une capacité de détection de spectre et que le brouilleur n'est pas trop compliqué [19].

B. Brouillage avancé :

- ***Spectre étalé :*** Le spectre étalé (Spread Spectrum) est une technologie de modulation numérique et une technique basée sur les principes de l'étalement d'un signal sur de nombreuses fréquences pour éviter les interférences et la détection du signal. Comme son nom l'indique, c'est une technique pour étaler le spectre transmis sur une large gamme de fréquences. Il a commencé à être utilisé par des applications militaires en raison de sa faible probabilité d'interception (LPI) ou de sa démodulation, de ses interférences et de son anti-brouillage (AJ) du côté ennemi. L'idée d'étalement du spectre est d'étaler un signal sur une large bande de fréquences pour utiliser une bande passante plus grande que la bande passante de données tandis que la puissance reste la même. Et dans la mesure où le signal d'étalement ressemble au signal de bruit dans la même bande de fréquences, il sera difficile de reconnaître le signal que cette caractéristique d'étalement assure la sécurité de la transmission [21]. Il existe quelque technique basée sur le spectre étalé, tels que FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum) et Nœud Hermès (FHSS & DSSS).

1. ***FHSS (Frequency Hopping Spread Spectrum)*** : Le spectre étalé à saut de fréquence FHSS est une technologie de transmission utilisée dans les réseaux sans fil et une technique pour générer un spectre étalé en sautant la fréquence porteuse. Le FHSS utilise un signal à bande étroite qui est inférieur à 1 MHz. Dans cette méthode, le signal de données est modulé avec un signal de porteuse à bande étroite qui "saute" de façon aléatoire et le saut se produit dans une séquence "prévisible" pseudo-aléatoire PN dans un temps régulier de fréquence en fréquence qui est synchronisé aux deux extrémités. Pour le saut de fréquence, un mécanisme doit être défini pour transmettre les données dans un canal clair et pour éviter les canaux encombrés. Le saut de fréquence est le changement périodique de la fréquence de transmission et le saut se produit sur une largeur de bande de fréquence qui se compose d'un nombre de canaux. Le canal qui est utilisé comme canal sauté est une bande passante instantanée tandis que le spectre de saut est appelé bande passante de saut totale. Saut de fréquence

catégorisé en saut lent et saut rapide qui, en sautant lentement, plus d'un symbole de données est transmis dans le même canal et par fréquence de saut rapide change plusieurs fois pendant un symbole. La séquence de saut signifie le canal suivant à sauter; il existe deux types de séquence de saut: la séquence de saut aléatoire et la séquence de saut déterministe [21].

La séquence de saut est codé sur *n* bit, et le nombre de fréquences est calculé à partir de *n* comme suit : *Nf = 2 ^ n.* Ce nombre de fréquences forme un cycle dans lequel *Nf = Nt.*

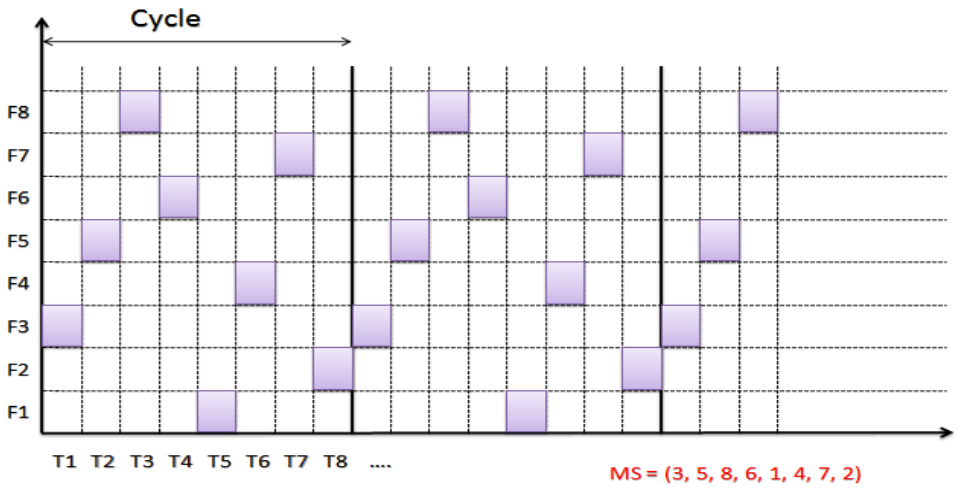

Figure 11: Une transmission basée sur Frequency Hopping Spread Spectrum.

2. ***DSSS (Direct Sequence Spread Spectrum) :*** Dans le système DSSS, chaque utilisateur se voit attribuer une séquence de codes unique qui permet à l'utilisateur d'étaler le signal d'information sur la bande de fréquences attribuée. Les signaux des différents utilisateurs sont séparés au niveau du récepteur par corrélation croisée du signal reçu avec chacune des séquences de codes utilisateur possibles. Les interférences éventuelles à bande étroite sont également supprimées dans ce processus. Afin de classer un système comme système modulé à spectre étalé (SS), la bande passante de transmission doit être beaucoup plus grande que la bande passante de l'information et la bande passante radiofréquence (RF) résultante doit être

déterminée par une fonction autre que l'information envoyée. La modulation SS transforme un signal porteur d'informations en un signal de transmission avec une bande passante beaucoup plus grande. Cette transformation est obtenue en codant le signal d'information avec un signal de code qui est indépendant des données et a une largeur spectrale beaucoup plus grande que le signal de données. Les données sont réparties en multipliant avec un code de bruit pseudo-aléatoire (PN). Une séquence PN (code) est une séquence binaire qui présente des propriétés de caractère aléatoire mais qui a une longueur finie et est donc déterministe [22]. La codification des données par rapport à la séquence PN se faire à partir de la table de la vérité XOR.

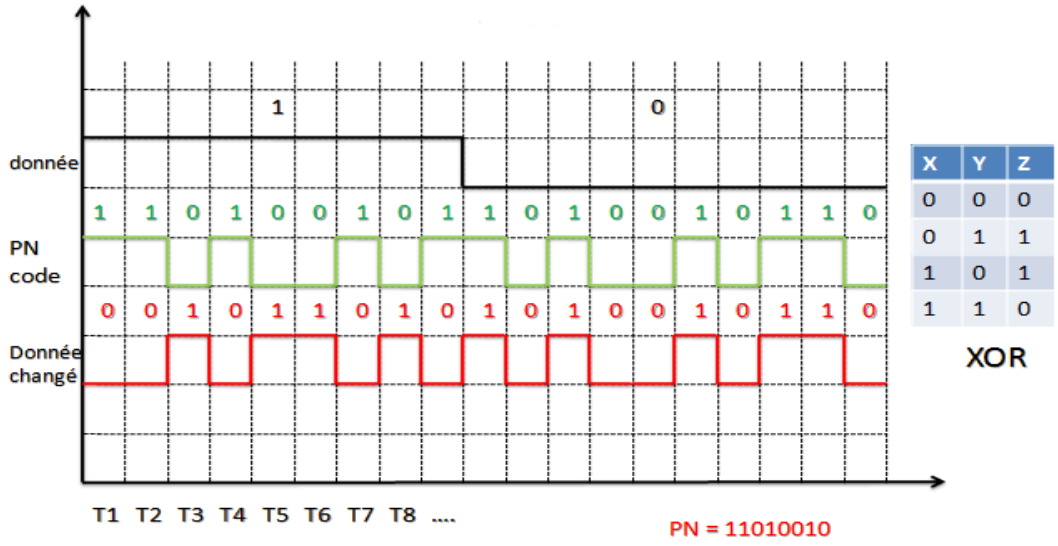

Figure 12: Une transmission basée sur Direct Sequence Spread Spectrum.

3. ***Nœud Hermès (FHSS & DSSS) :*** Le DSSS utilise une bande passante plus large pour la transmission du signal tandis que le FHSS permet d'éviter les interférences. Un schéma hybride DSSS et FHSS, appelé Nœud Hermès, est proposé pour faire face aux attaques de brouillage dans les réseaux de capteurs. Le Nœud Hermès effectue 1000000 de sauts par seconde (FHSS) pour éviter les brouilleurs à suivi rapide. Le DSSS est utilisé pour faire en sorte que l'attaquant détecte les signaux de données comme un bruit blanc, ce qui l'empêche de détecter la bande radio de communication.

Le Nœud Hermès utilise 55 canaux de fréquence pour le FHSS et 275 MHz de bande passante pour le spectre étalé dans le DSSS. La séquence de fréquences du FHSS et le code de pseudo-bruit (PN) du DSSS doivent être connus afin que le signal d'origine puisse être récupéré. Un mot secret est utilisé comme graine pour les générations de séquence de canaux et le code PN. Le mot secret est généralement codé en dur pour un réseau particulier afin qu'un nouveau nœud entrant dans le réseau puisse être identifié avec les nœuds existants. La synchronisation entre les nœuds est importante pour que le Nœud Hermès fonctionne correctement, ce qui est réalisé par le récepteur [19].

4. *FHSS vs DSSS vs Nœuds Hermès :*

Tableau 1: Comparaison entre FHSS / DSSS et Nœuds Hermès.

Technologie	Avantages	Inconvénients	Applications
FHSS	- Portée relativement élevée. - Technologie avantageuse en termes de sécurité et de fiabilité. - Consommation d'énergie faible. - Augmente la capacité du signal.	- Débit faible. - Sensible au nombre d'émetteurs émettant dans la même bande. - Efficacité spectrale peu élevée. - Nécessite une synchronisation fine entre l'émetteur et le récepteur.	- Convient à la transmission de signaux courts, y compris en environnement perturbé. - Solution retenue notamment par Bluetooth.
DSSS	- Bonne efficacité spectrale. - Systèmes de redondance	- Technologie relati-vement sophistiquée.	- Convient à la transmission de

	par étalement peu sensibles aux interférences et aux erreurs de transmission. - Possibilité d'obtenir des débits élevés. - Possibilité d'améliorer les performances.	- Nécessite des composants rapides. - Consommation d'énergie élevée.	signaux longs. - Solution retenue notamment par Zig Bee et Wi-Fi 802.11b.
Nœuds Hermès	- Bonne efficacité spectrale - Technologie très avantageuse en termes de sécurité et de fiabilité. - Débit élevés. - Garantissent un taux de livraison de succès de paquets satisfaisant même dans des environnements fortement bloqués.	- Un algorithme plus sécurisé pour la génération de changement de fréquence est également nécessaire. - Consommation d'énergie élevée. - La mise en œuvre du Nœud Hermès n'est pas une tâche simple en raison des technologies qui sont incorporées.	- Solution retenue notamment par Zig Bee et Bluetooth. - Convient à la transmission de signaux longs.

Les techniques FHSS et DSSS sont les techniques anti-brouillages les plus utilisés dans les réseaux MANET.

2.3.5 Travaux connexes

1. ***Mise en œuvre au niveau de la couche MAC :***

Cette technique a été proposée par [23]. Le débit du réseau peut être réduit en raison de la difficulté de collision RTS (Request to Send), pour cette raison, les seuils de fragmentation RTS / CTS sont également inclus dans cette technique. Les protocoles de contrôle d'accès au support sans fil (MAC) doivent organiser les transmissions des nœuds sur le canal de transmission commun. Le groupe de travail IEEE 802.11 a suggéré deux algorithmes différents pour la résolution de conflits. La première est la fonction de coordination distribuée (DCF), totalement distribuée, et la seconde, la fonction de coordination ponctuelle (PCF), qui dispose d'un protocole d'accès centralisé. Le mécanisme RTS / CTS (Request to Send / Clear to Send) est un processus d'établissement de liaison qui réduit le nombre de collisions lorsque des nœuds masqués s'exécutent sur le réseau.

2. ***Détection par corrélation :***

Cette architecture de détection du brouillage dans les réseaux ad hoc a été proposée par [24]. La corrélation est une mesure de l'association entre deux variables aléatoires. Un nœud de transmission mesure la probabilité d'erreur (EP) et le coefficient de corrélation (CC), si le CC est plus grand que l'EP relatif produit, le réseau est considéré comme bloqué. Cela signifie qu'il y a un brouillage avec un faible pourcentage, et il n'affecte pas le réseau et il n'a pas besoin d'être découvert ou défendu. La relation entre CC et EP peut être mesurée par simulation ou par mesure de la régression dans une dynamique de réseau normale. Le système de détection est composé de deux phases : *Phase d'initialisation* et *Phase de détection.* La solution est facile à implémenter dans les périphériques existants à cause de :

- Simple et efficace pour détecter les attaques par brouillage.
- Il n'ya pas de surcharge de communication.
- Les frais de stockage et de calcul nécessaires sont très faibles.

3. Estimation des défis de sécurité dans les MANET :

Cette technique a été proposée par [25]. En général, il existe deux facteurs les plus importants dans les mesures de sécurité: les attaques et les services de sécurité. Les services indiquent quelques stratégies de protection pour créer un réseau protégé, tandis que les attaques utilisent des vulnérabilités de réseau pour surmonter un service de sécurité. Les services de sécurité incluent: disponibilité, autorisation, intégrité, confidentialité des données et non-réputation. De même, les attaques incluent: l'attaque de trou de ver, l'attaque de trou noir, l'attaque de routage, l'attaque d'espionnage, la consommation de ressources, le DoS, l'attaque de brouillage, la fabrication, l'attaque de modification, etc.

4. Identification de voisin sécurisé résilient au brouillage JR-SNI:

JR-SNI (Jamming-Resilient Secure Neighbour Identification) est une technique a été proposé par [26]. Elle est basée sur la pré-distribution de code d'étalement et le DSSS (Direct Sequence Spread Spectrum) pour détecter les attaques de brouillage dans les MANET. Cette technique proposée a permis à deux nœuds voisins de se découvrir efficacement avec possibilité de dépassement malgré les brouilleurs omniprésents. L'efficacité et l'efficience de ces approches proposées ont été vérifiées par des estimations théoriques détaillées et des résultats de simulation.

5. Jeu de coalition basé sur la réputation RBCG :

RBCG (Reputation Based Coalition Game) est un algorithme a été développé par [27]. Il est pour identifier et atténuer les hits de brouillage d'initiés bien conçus dans les MANET. Les nœuds vont créer une grande coalition constante pour créer une décision de défense stratégique de manière sécurisée, maintenir la coalition impressionnante s'appuyer sur la réputation du nœud et interdire à tout nœud attaquant de s'appuyer sur la valeur de réputation. Les résultats ont révélé que la technique proposée a fourni un cadre afin de quantifier les informations requises par les adversaires pour établir des attaques de brouillage d'initiés.

2.3.6 Synthèse

Les attaques de brouillage sont un grand problème de sécurité dans les réseaux MANET, et ce concept est considéré comme un axe de recherche très important, pour cela il existe plusieurs travaux de recherche comme [23], [24], [25], [26], et [27]. Tous les chercheurs proposent des modèles ou des techniques ou des algorithmes pour faire une contre-mesure de brouillage. La table (2) donne une comparaison entre ces travaux.

Tableau 2: Comparaison entre les travaux connexes.

Approche	Type de l'approche	Approche définit au		Type d'attaque			Codification du signal
		Niveau Architectural	Niveau Application	Attaque de brouillage	Autre attaque	Au niveau de la couche MAC	
[23]	Algorithme		✓			✓	
[24]	Architecture	✓		✓			
[25]	Technique		✓	✓	✓		
[26]	Technique		✓	✓			✓
[27]	Algorithme		✓	✓			
Notre processus de contre-mesure	Technique		✓	✓			✓

Le tableau ci-dessus présente les métriques de chaque recherche, et comme on peut le voir il existe des recherches (des techniques, des algorithmes, ou des architectures) qui sont définit au niveau d'application et d'autre au niveau architectural, donc les recherches [23], [25], [26], [27] sont définit au niveau d'application par contre la recherche [24] est définit au niveau architectural. En plus il existe plusieurs types d'attaques que la recherche les détecter comme les recherches [24], [26], [27] sont proposées pour les attaques de brouillage dans les réseaux MANET, la recherche [23] est proposée pour les attaques au niveau de la couche MAC et la dernière recherche [25] est proposée pour d'autre attaques par exemple : le DoS, l'attaque de trou noir, l'attaque de routage, etc. Finalement il y a la codification du signal qui se fait seulement par la recherche qui est proposée par [26].

Pour dépasser ces limites, nous abordons dans la suite de cette mémoire le problème de brouillage sous ces aspects :

- Proposition d'un technique anti-brouillage basé sur la combinaison des deux méthodes FHSS et DSSS.
- Implémenter un programme pour faire une simulation.

2.4 Conclusion

Dans ce chapitre nous avons présenté un état de l'art sur les protocoles de routage dans les réseaux MANET. Le routage est réalisé par des types de protocoles, parmi ces types on a présenté quelques protocoles proactifs qu'établissent les routes à l'avance en se basant sur l'échange périodique des tables de routage, et quelques protocoles réactifs qui cherchent les routes à la demande, en plus les protocoles hybrides et les protocoles géographiques.

Ensuite, nous avons présenté les techniques anti-brouillages et quelques travaux de recherche dans le même but, malgré ça la sécurité n'est pas réalisée d'une manière complète.

Dans le chapitre suivant, nous allons proposer une nouvelle technique afin d'assurer une meilleure protection contre les attaques de brouillage.

CHAPITRE 3

CONTRIBUTION

Chapitre 3

Contribution

3.1 Introduction

L'utilisation des réseaux ad hoc mobile exige une sécurité anti-brouillage très élevés pour obtenir une transmission des données complète. Malgré qu'il existe des nombreux techniques et algorithmes de sécurité anti-brouillage, les défis de sécurité ne sont pas encore terminés. Pour cela on va proposer une technique hybride pour la sécurité anti-brouillage dans les reseaux MANET.

Dans ce chapitre, nous allons présenter notre technique hybride, son principe de fonctionnement ainsi que ses concepts de base afin de mieux expliquer la manière par laquelle on combine la technique FHSS avec la technique DSSS.

3.2 Principes de base

Après avoir étudié quelques techniques anti-brouillages existants dans les réseaux MANET, nous avons vu que les techniques FHSS et DSSS sont les techniques anti-brouillages les plus utilisés dans les réseaux MANET à cause de son fiabilité en termes de sécurité et ils sont utilisé pour différents domaines.

1. ***FHSS (Frequency Hopping Spread Spectrum) :***

Une technique de transmission des données, elle divise le message en 79 sous canaux de débit 1 Mb/s et de largeur de 1MHz. Le paquet ne transmis pas dans un seul canal de transmission, elle se transmise dans différents canaux. Les sauts sont connus sous le nom du modèle de sauts, et seulement le récepteur et l'émetteur qui connue ce modèle, ce modèle contient les fréquences de chaque saut, ces fréquences sont codées. Si le code est de n bit alors le nombre des fréquences est 2^n. La transmission du donnée se divise on des cycles, chaque cycle est de 2^n de fréquences et de 2^n d'unités de temps.

2. ***DSSS (Direct Sequence Spread Spectrum) :***

Une technique de transmission de données, son principe est que le signal se change par rapport à un autre signal donné s'appelle PN code. Le changement du signal se base sur la table de vérité XOR.

3.3 Présentation de notre contribution : Technique Hybride

Notre proposition est une technique hybride qui combine les techniques FHSS et DSSS, ces deux principaux techniques sont considérés dans cette proposition, de FHSS, on utilise le principe de saut de canal et l'idée de division de canaux et de modèle de saut, et de DSSS, on utilise la codification du signal selon un code PN.

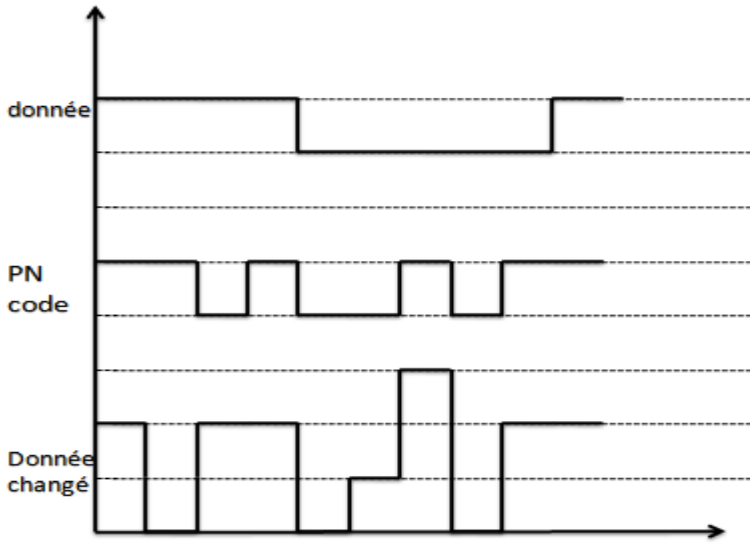

Figure 13: Idée de base de fonctionnement de la proposition.

Comme nous voir dans la figure ci-dessus, le signal changé est codé et il sera envoyé avec le principe de saut de canal en même temps.

3.3.1 Principe de fonctionnement

Dans une unité de temps, le signal est codé par rapport au code PN correspondant dans cette unité selon la table de vérité XOR, si le bit est '1' dans le canal *x* alors le signal est entre le canal *x* et le canal *x*+1, sinon le signal est entre le canal *x* et le canal *x*-1, après cela il y a un test pour voir si la donnée est terminée ou non, s'elle termine la codification se termine, sinon on passe au canal suivant selon le modèle de saut et on répète l'opération.

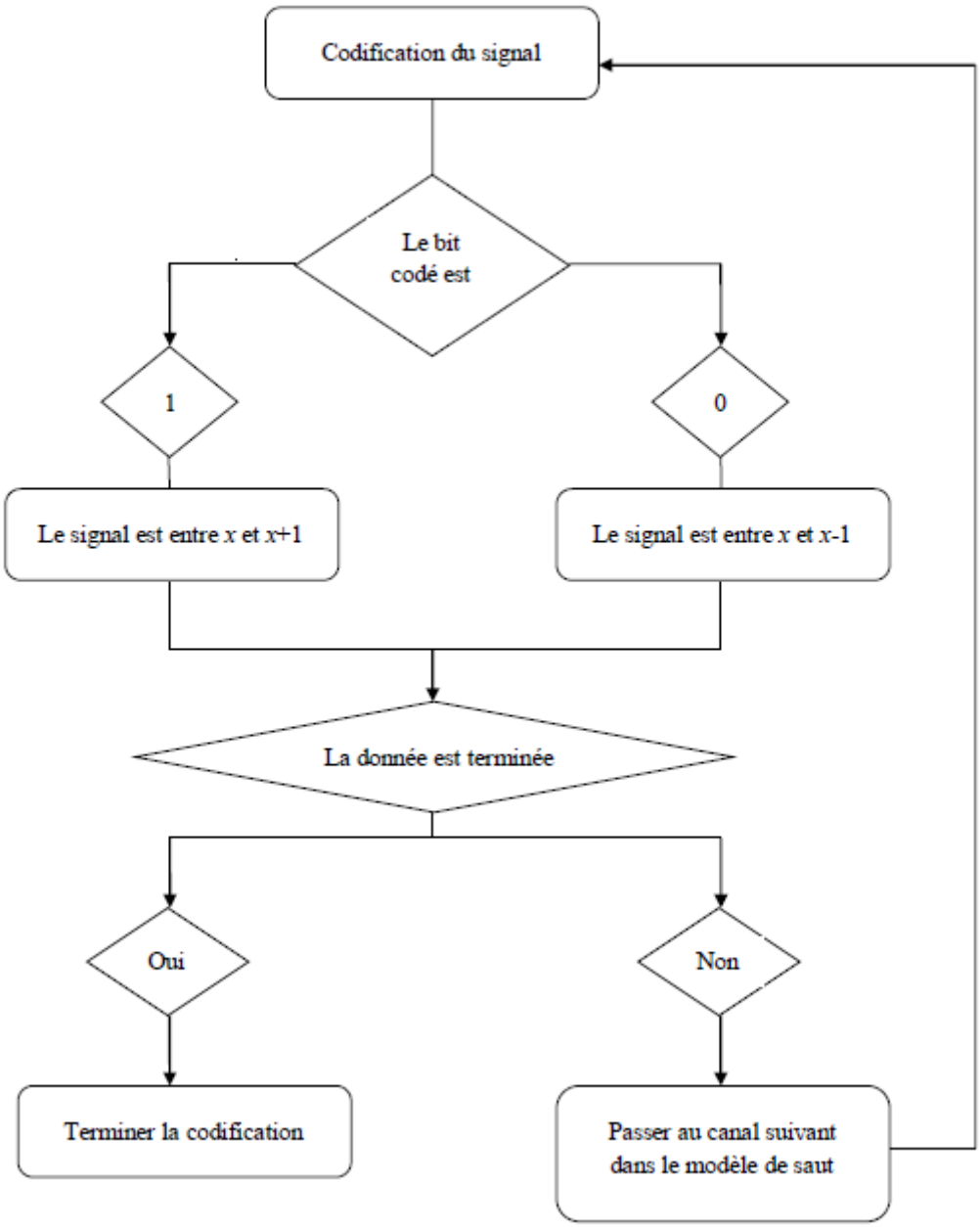

Figure 14: Organigramme pour présenter le principe de fonctionnement de notre proposition.

3.3.2 Cas d'étude

On suppose qu'on a : une fréquence codée sur 3 bits, le modèle de sauts est (5, 8, 4, 1, 6, 3, 2, 7), comme le montre le tableau 3. Le PN code est : 10010111.

Tableau 3: Les codes des fréquences.

Le code	L'ordre
000	**4**
001	**7**
010	**6**
011	**3**
100	**1**
101	**5**
110	**8**
111	**2**

Le signal de la donnée est comme suit :

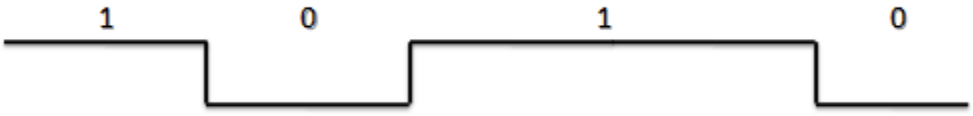

Figure 15: Données suggérées.

Le PN code est comme suit :

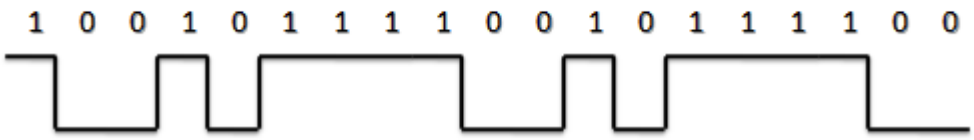

Figure 16: PN code suggéré.

Voici comment le signal sera transmis :

1. Codification du signal par rapport au PN code selon la table de vérité XOR.

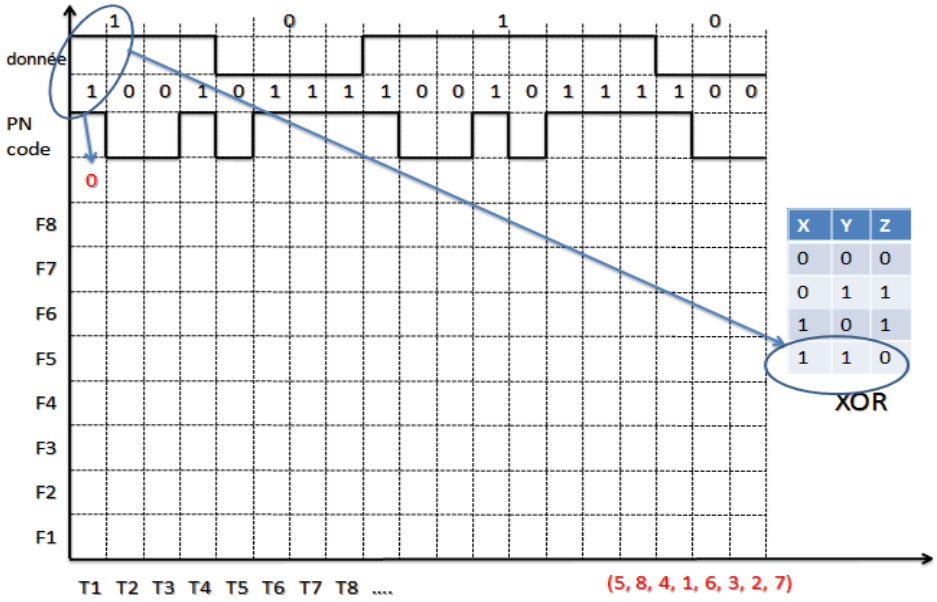

Figure 17: Codification du signal par rapport au PN code selon la table XOR.

2. Comme on le voit le bit codé est 0 et le canal dans lequel le signal sera transmis est 5, donc le signal codé sera entre les canaux 5 et 4, comme le montre la figure 18 ci-dessous.

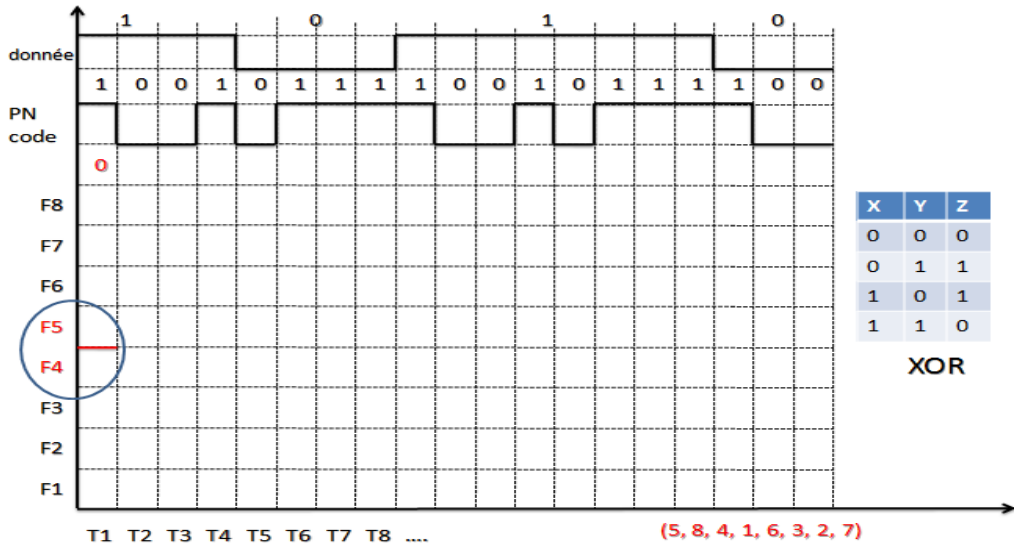

Figure 18: La position du signal dans la première unité de temps.

3. Comme on le voit dans la figure ci-dessus la donnée n'est pas terminée, donc on va passer au canal suivant qui est 8 et on va coder le signal.

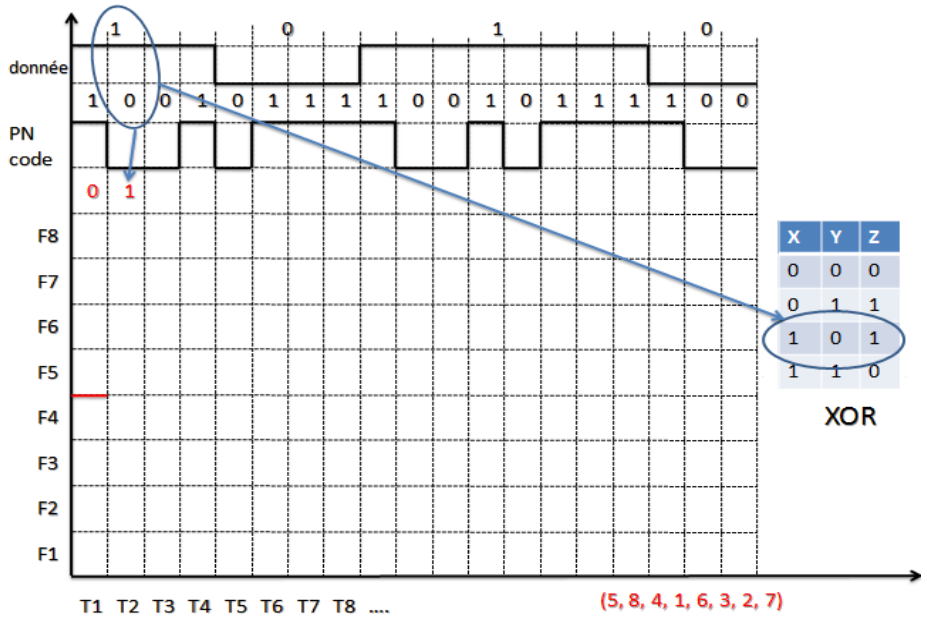

Figure 19: Deuxième codification du signal.

4. Dans ce cas, le bit codé est 1 donc le signal codé sera entre les canaux 8 et 9.

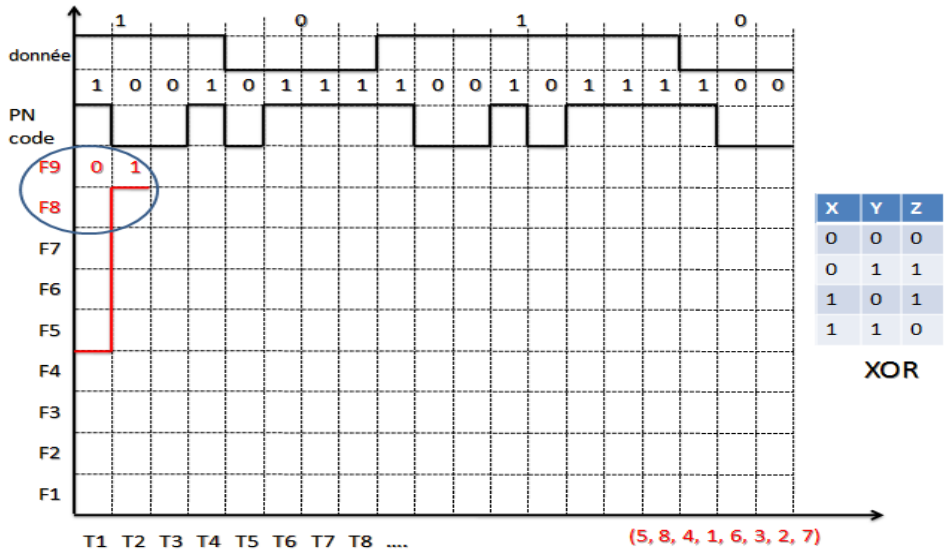

Figure 20: La position du signal dans la deuxième unité de temps.

5. On complète de cette façon jusqu'à la fin de la donnée. La figure 21 donne le signal final à envoyer.

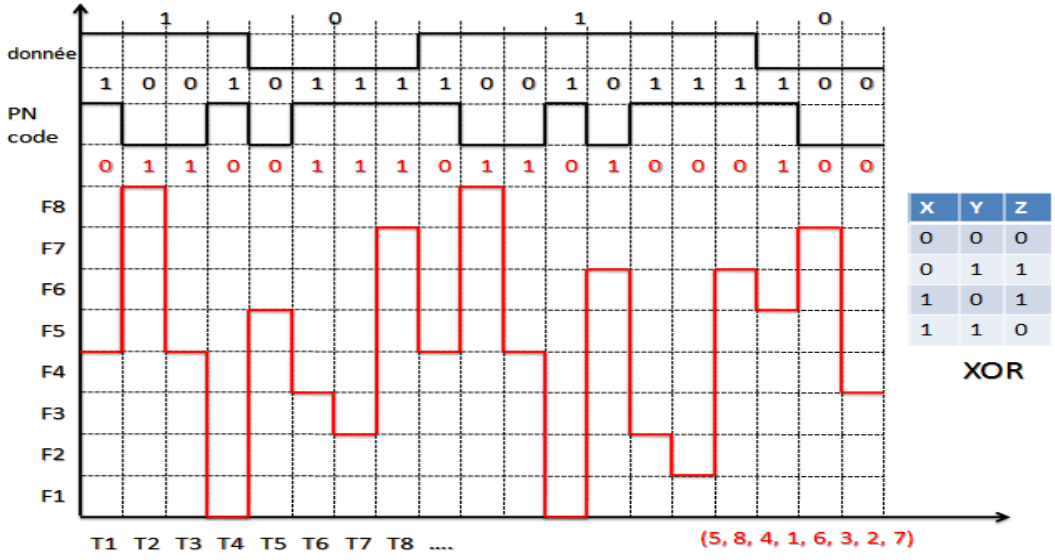

Figure 21: Donnée envoyée par notre proposition hybride.

3.4 Discussion

La technique hybride proposée est basée sur la codification du signal de DSSS et le saut de canal de FHSS pour améliorer des points qui définie la sécurité anti-brouillage dans les réseaux ad hoc mobile.

La technique FHSS est avantageuse en termes de sécurité et fiable en termes de consommation d'énergie, un nombre d'inconvénients plus au moins apparents. Nous citons parmi eux :

- Le débit de transmission est faible.
- L'idée de cycle pose un problème de sécurité, lorsqu'un brouilleur connaitre le contenu d'un seul cycle, il peut connaitre le contenu de toute la donnée.

La technique DSSS a complété certains inconvénients de FHSS, dans laquelle elle augmente le débit de transmission, et est une technique avec une bonne efficacité spectrale.

Après avoir analysé les deux techniques (FHSS et DSSS), on a constaté qu'on peut améliorer le principe de codification du signal et ajoutant l'idée de saut de canal et la division des canaux, ce qui nous amène à proposer une nouvelle technique hybride combinant les avantages des deux grandes techniques (Frequency Hopping Spread Spectrum) et (Direct Sequence Spread Spectrum). Les points importants permettant de développer cette proposition sont :

- ✓ Adopter une technique pour une meilleure sécurité anti-brouillage.
- ✓ Réduire la consommation d'énergie résultant de l'utilisation de la technique DSSS.

3.5 Conclusion

Dans ce chapitre, on a présenté une technique hybride pour la sécurité anti-brouillage dans les réseaux MANET qui combine les deux techniques FHSS (Frequency Hopping Spread Spectrum) et DSSS (Direct Sequence Spread Spectrum) et leur principe de fonctionnement, ensuite on a fait une étude de cas pour démontrer les étapes de cette technique.

Dans le chapitre suivant, on va passer à l'étape d'implémentation qui constitue un point important dans le processus d'analyse des performances de la proposition.

CHAPITRE 4

IMPLÉMENTATION ET RÉSULTATS D'EXPÉRIMENTATION

Chapitre 4

Implémentation et Résultats d'Expérimentation

4.1 Introduction

Afin d'implémenter notre technique anti-brouillage, une simulation a été effectuée pour réaliser un prototype de notre proposition par la création d'un réseau de capteurs sans fil avec des nœuds mobiles et en essayant d'envoyer des paquets de données. Avant de détailler nos simulations, nous allons d'abord parler des outils utilisés dans ce travail, et l'outil de simulation fournis et la motivation pour NS3, nous allons présenter l'environnement de simulation. Ensuite, on va donner les résultats de la simulation. Enfin, nous allons faire une discussion sur ces résultats.

4.2 Présentation des terminologies

4.2.1 Machine Virtuelle (VMware Workstation PRO 15.0)

Une machine virtuelle ou (Virtual Machine) est un fichier informatique, généralement appelé image, qui se comporte comme un véritable ordinateur. En d'autres termes, créer un ordinateur dans un ordinateur. Il s'exécute dans une fenêtre, un peu comme n'importe quel autre programme, offrant à l'utilisateur final la même expérience sur une machine virtuelle que celle qu'il aurait sur le système d'exploitation hôte lui-même.

4.2.2 Ubuntu 16.04

Ubuntu 16.04 est une version labélisée LTS, est un système d'exploitation GNU/Linux basé sur la distribution Linux Debian. Il est développé, commercialisé et maintenu pour les ordinateurs individuels par la société Canonical.

4.2.3 NS3 (Network Simulator 3)

Est un logiciel libre de simulation à événements discrets très largement utilisé dans la recherche académique et dans l'industrie. Il est considéré par beaucoup de spécialistes des télécommunications comme le meilleur logiciel de simulation à événements discrets, en raison de son modèle libre, permettant l'ajout très rapide de modèles correspondant à des technologies émergentes.

4.3 Résultats de simulation et Discussion

4.3.1 Installation du NS3

Installer les conditions préalables pour mettre NS3 bien fonctionne, tels que python,

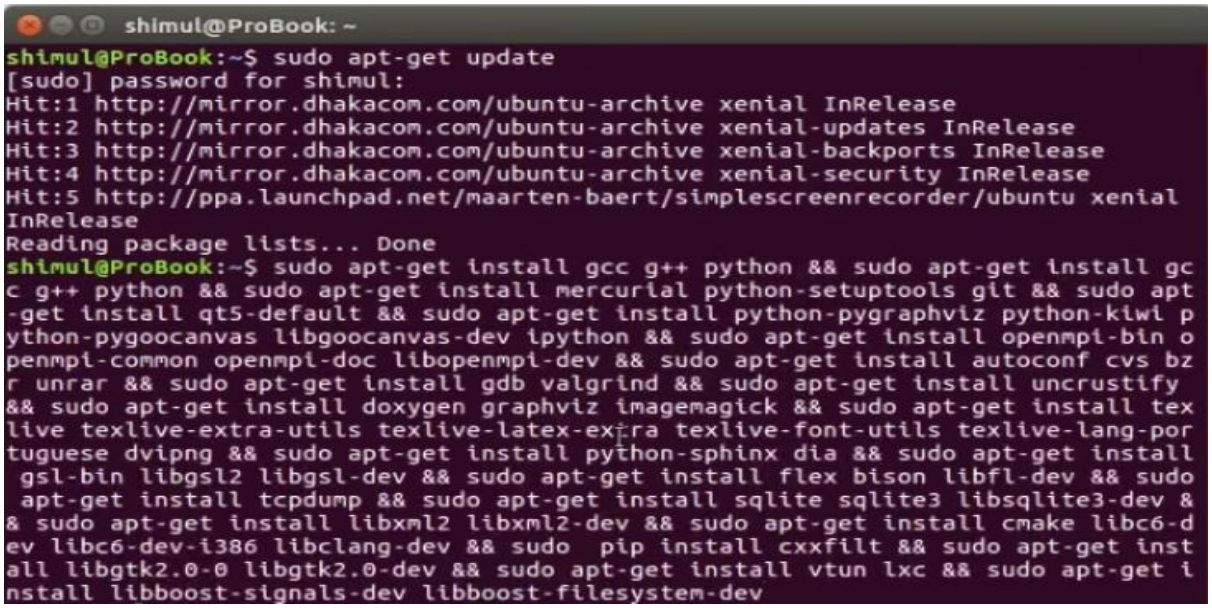

Figure 22: L'installation des conditions préalables.

On continue l'installation en cliquant sur *Y*. Lorsque l'installation d'un tel outil termine, il affiche une question si vous voulez continuer l'installation ou non comme il est illustré dans l'image ci-dessous.

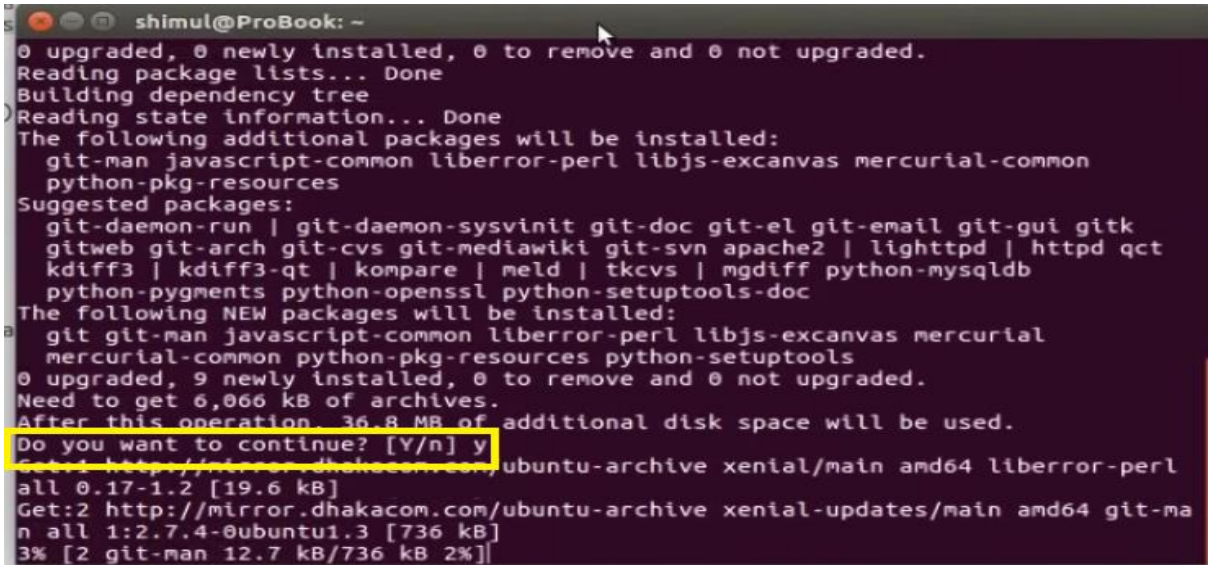

Figure 23: Continuer l'installation.

On va créer un dossier sous le nom ns3 et télécharger ns3 et le placer dans ce dossier, ensuite nous allons télécharger un dossier complémentaire sous le nom de *ns-allinone-3.27*, comme il est illustré dans les trois captures ci-dessous.

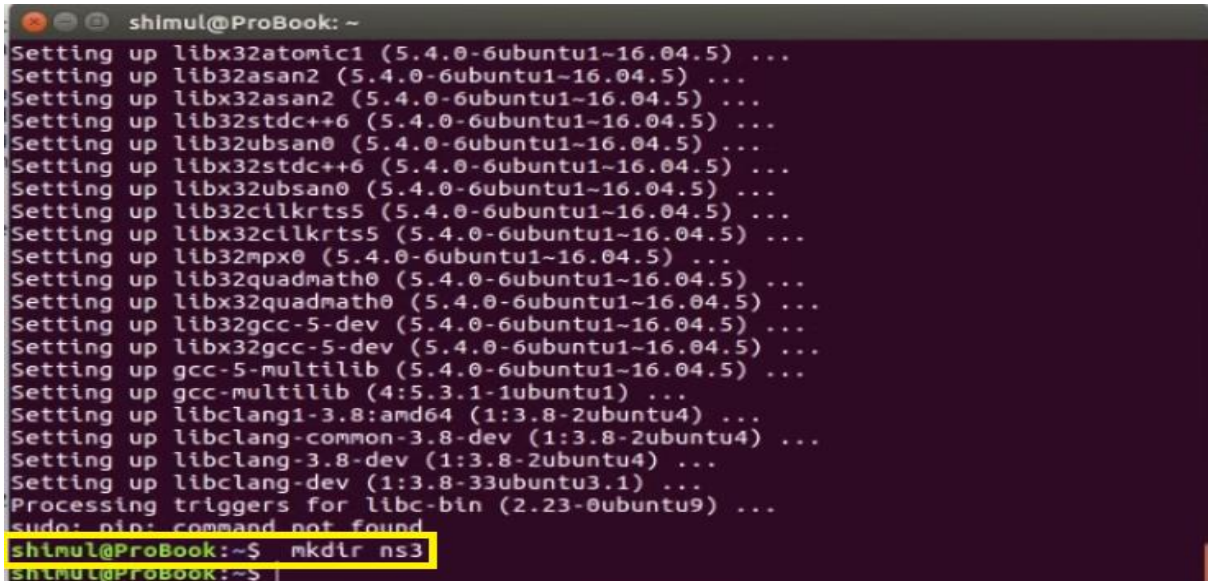

Figure 24: Création d'un fichier (ns3).

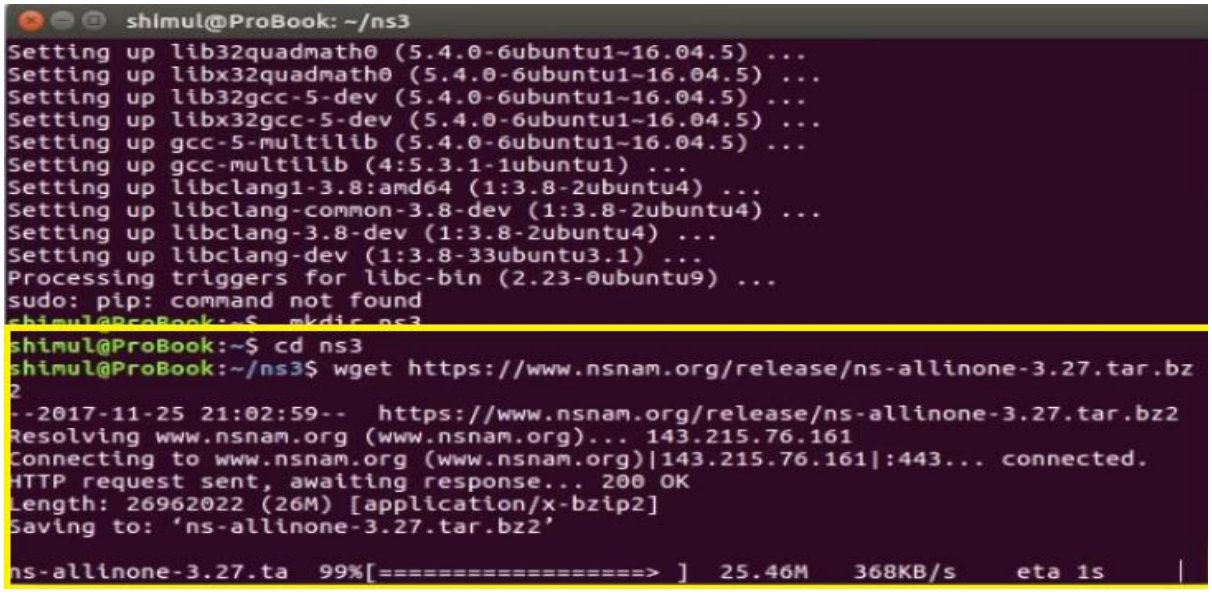

Figure 25: Placement de ns3 dans le dossier.

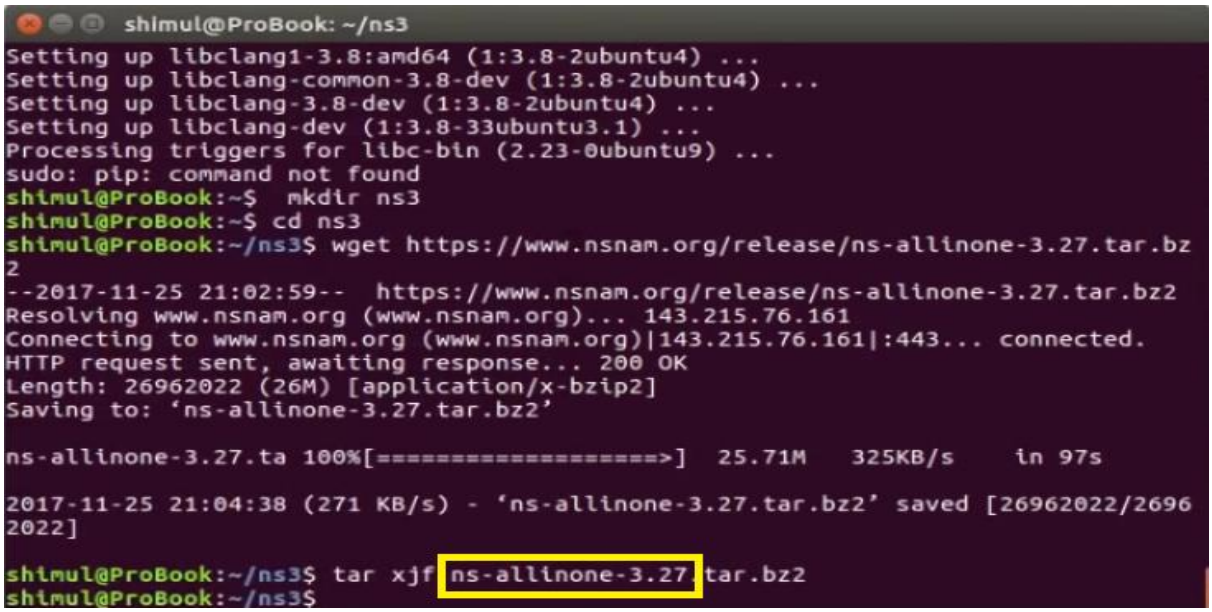

Figure 26: Création du fichier complémentaire.

Quand on termine toute l'installation et les configurations, nous allons faire un test pour voir si l'installation est bien terminée.

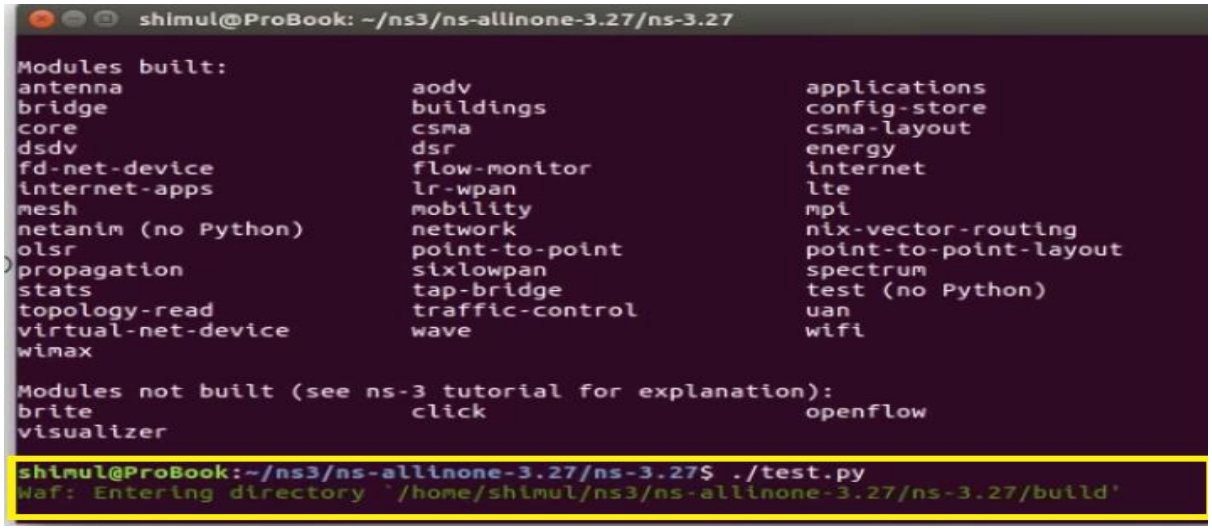

Figure 27: Vérification de l'installation.

4.3.2 Paramètres de simulation

Tableau 4: les paramétres de simulation.

Paramètres	Nombre
Taille du paquet à envoyer	200 Octets
Nombre de paquets à envoyer	10000
Temps de début de la simulation	0.0 Secondes
Distance entre les nœuds	10.0 Secondes

4.3.3 Résultats de simulation

La simulation de ns3 est réalisée pour cette proposition. La capture d'écran ci-dessous est utilisée pour afficher le code ns3 sur Ubuntu 16.04.

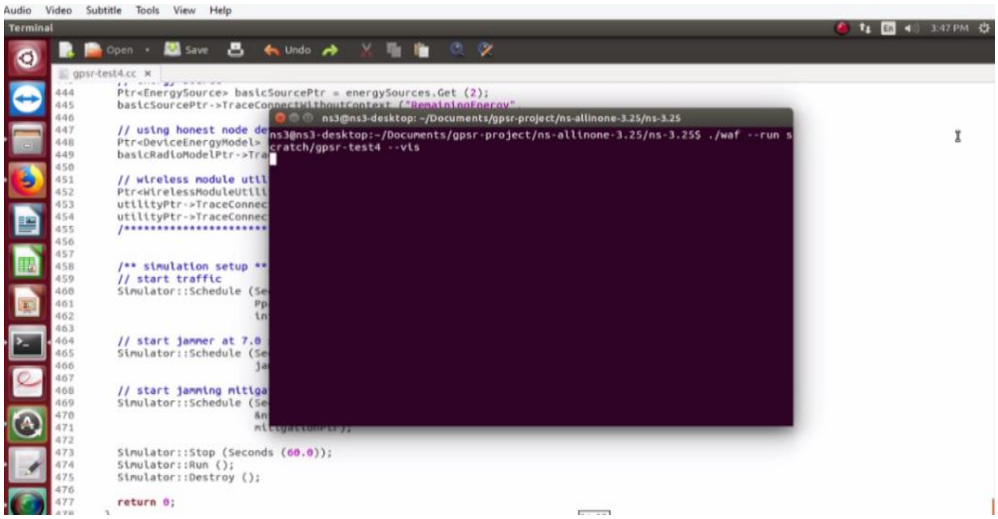

Figure 28: Le code avec NS3.

Une fois le code exécuté, il affiche l'animation du nœud de sortie. Il est illustré dans les deux captures ci-dessous.

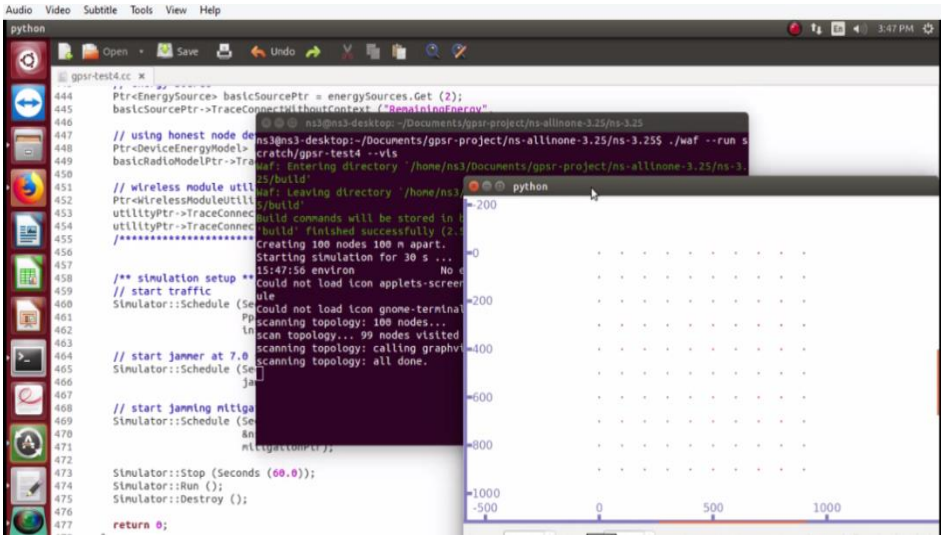

Figure 29: Les nœuds de sortie.

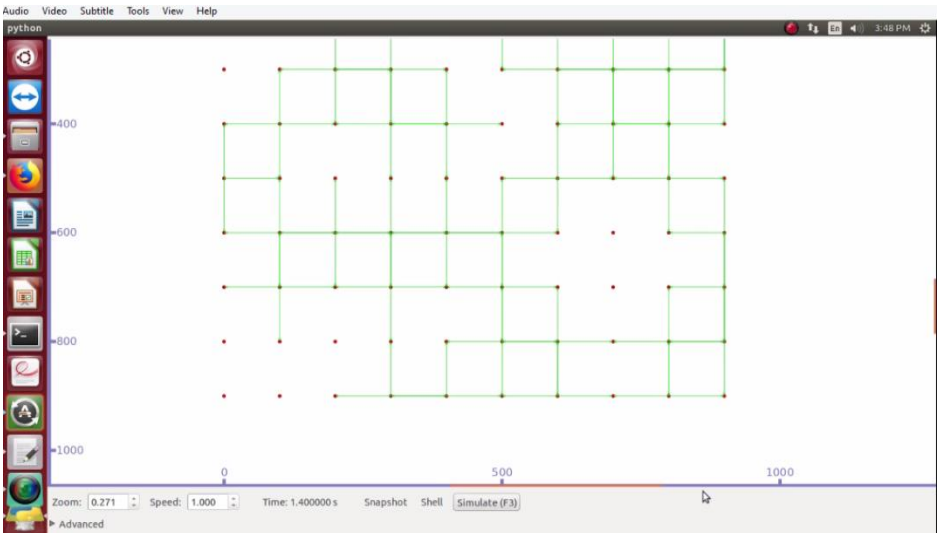

Figure 30: Le passage de données.

4.3.4 Discussion

1. ***Retard Vs Temps de simulation :***

Ici, calculez l'anti brouillage proposé et de base en fonction du retard et de la simulation. Le délai de bout en bout du paquet est le temps de génération du paquet par la source jusqu'à la réception de destination qui est proposée et l'attaque de brouillage de base. Le retard et le temps de simulation sont exprimés en sec. Par conséquent, tous les retards dans les réseaux sont appelés comme des retards de bout en bout comme le temps de transmission et les files d'attente de tampon. Les retards sont également appelés latence. Le retard est une mesure de la manière dont un protocole de routage s'adapte aux nombreuses contraintes du réseau et il est utilisé pour fournir la fiabilité du réseau. Il est illustré dans l'image ci-dessous.

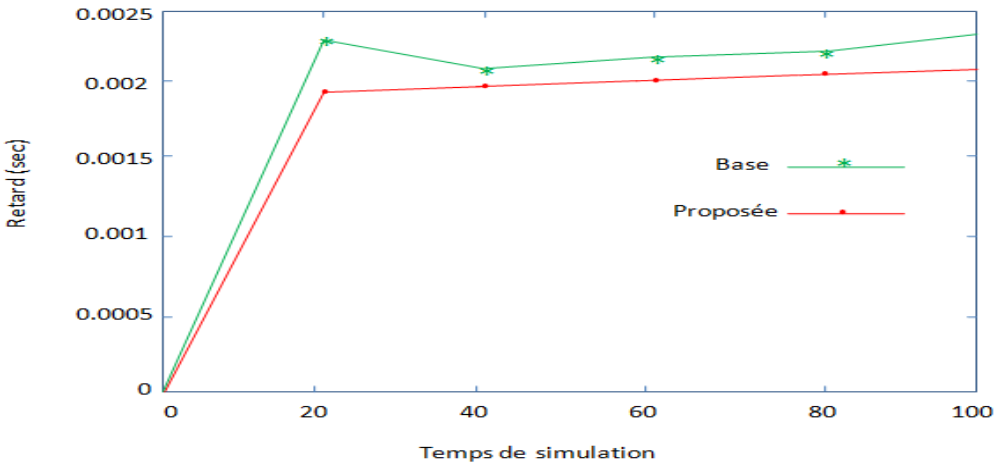

Figure 31: Retard Vs Temps de simulation.

2. ***Consommation d'énergie Vs Temps de simulation :***

Ici, calculez l'anti brouillage proposé et de base en fonction de la consommation d'énergie et du temps de simulation. La consommation d'énergie est utilisée pour représenter le niveau d'énergie des nœuds du réseau à tout moment spécifié. Il est utilisé pour augmenter la consommation d'énergie des équipements utilisés pour accéder à Internet. Il est illustré dans l'image ci-dessous.

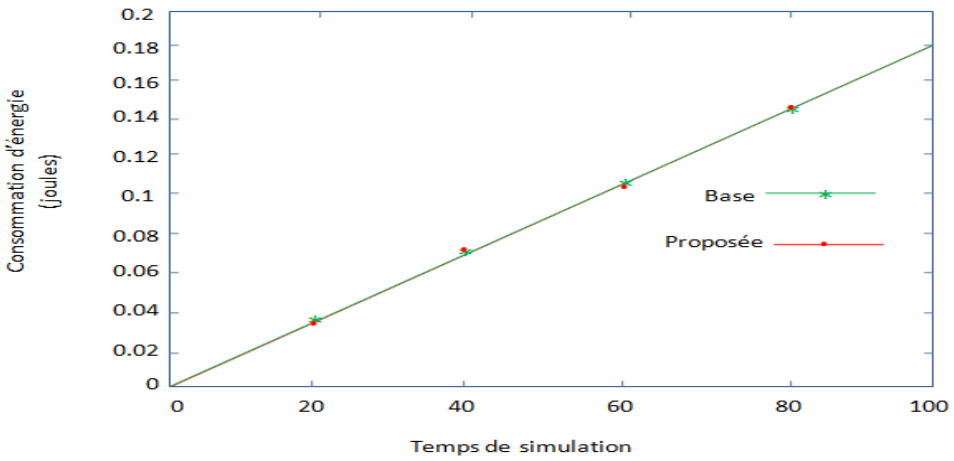

Figure 32: Consommation d'énergie Vs Temps de simulation.

4.4 Conclusion

Dans ce chapitre on a expliqué l'opération de l'installation du simulateur NS3 qui nous a aidés à réaliser notre simulation. Ce travail peut encore être développé pour couvrir toutes les étapes du chapitre 3 et de créer un technique anti-brouillage complet.

L'évaluation que nous avons effectuée (simulation sous NS3), nous a permis de voir l'impact de la mobilité et le nombre de nœuds sur le débit utile, le taux de retard et la consommation d'énergie que ce soit pour le technique hybride.

Notre technique hybride est plus performante en termes de consommation d'énergie et le taux de retard, ainsi il fourni le meilleur rapport, puisqu'il garantit plus de sécurité anti-brouillage dans le réseau.

CONCLUSION GÉNÉRALE

Conclusion générale

L'émergence de nouvelles technologies de communication sans fil et la prolifération des équipements mobiles évolués tels que les assistants personnels, les téléphones ou les ordinateurs portables, font que nous assistons depuis quelques années à des modifications importantes et des évolutions révolutionnaires dans le domaine de l'information et de la communication. En effet, le déploiement croissant de réseaux sans fil ad hoc offre la perspective d'un réseau omniprésent, permettant aux utilisateurs en déplacement d'être rapidement connectés et d'avoir de plus accès à tout instant et en tous lieux à des réseaux et à leurs services associés.

Les réseaux ad hoc mobiles MANET constituent des sujets de recherche innovants pour diverses disciplines des sciences et techniques de l'information et de la communication mais avec toutefois des contraintes spécifiques s'érigeant en défis certains à relever. Parmi les problèmes posés à l'heure actuelle dans ce type de réseaux, la sécurité en est un véritable et auquel une solution adéquate doit être apportée. Il existe de nombreux types d'attaques qui perturbent et menacent le bon transfert de données entre les nœuds mobiles, tels que les attaques de brouillage qu'il s'agit de l'un des types d'attaques les plus courants dans ce type de réseau.

Le travail consigné dans ce mémoire a été le fruit d'une étude menée dans le contexte des RCSFs en général et des réseaux ad hoc mobiles en particulier et ce, relativement au problème de sécurité contre les attaques de brouillage.

Plusieurs travaux de sécurité anti-brouillage ont été proposés récemment pour les réseaux MANET qui peuvent être des techniques, des architectures et des algorithmes. Nous avons présenté certains techniques anti-brouillages.

Puis, nous avons introduit la notion de spectre étale et quelques techniques basés sur ce principe, tels que FHSS (Frequency Hopping Spread Specrtrum) et DSSS (Direct Sequence Spread Spectrum) qui sont deux techniques anti-brouillages. La transmission des données dans la première technique est basée sur le saut de canal, et dans le deuxième est basé sur la codification du signal.

En conclusion, nous avons pensé de profiter les avantages des deux techniques anti-brouillages et nous avons concevoir une solution hybride dans cette mémoire. La transmission des données dans cette technique est basée sur la codification du signal et le saut de canal en même temps ; le signal transféré est codé selon un autre signal qui s'appelle PN code et chaque unité de temps il change le canal de transmission.

A l'avenir, nous pensons de profiter la technique basée sur la théorie de jeux, à cause de son utilité et son efficacité de sécurité anti-brouillage pour améliorer les performances de notre travail.

Bibliographie

[1] Abderrezak Rachedi. Contributions à la sécurité dans les réseaux mobiles ad Hoc. Réseaux et télécommunications [cs.NI]. Université d'Avignon, 2008. Français.

[2] O.Osanaiye, A.S.Alfa, G.P.Hancke, "A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks".

[3] Internet Engineering Task Force (IETF). Groupe de travail MANET (mobile ad hoc network).

[4] F.Ameza, "Les technologies de routage sans fil: Le routage dans les réseaux ad hoc (OLSR et AODV), Memoire Online.

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

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

[7] A.Zianni, "Etude de la sécurité des données dans les réseaux de capteurs sans fil", ZigBee

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

[9] I.F. AKYILDIZ, W. S. SANKARASUBRAMANIAM, E. CAYIRCI: Wireless Sensor Networks: A Survey. Computer networks, 2002, 38, pp.393-422.

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

[11] K.BADER, "Détection d'intrusion dans les réseaux de capteurs sans fils, Master recherche 2 en Informatique, IFSIC-Rennes 1, 2009/2010.

[12] K.BEYDOUN, Conception d'un protocole de routage hiérarchique pour les réseaux de capteurs, Grade de Docteur,L'université de FRANCHE-COMTE,16 décembre 2009.

[13] Mme LABRAOUI Nabila, La sécurité dans les réseaux sans fil Ad hoc.

[14] I.F.Akyildiz, W. Su, Y. Sankarasu bramaniam, E. Cayirci, (2002). Wireless sensor networks: a survey. Elsevier Science.

[15] Van der Meerschen Jérôme, « Hybridation entre les modes ad-hoc et infrastructure dans les réseaux de type Wi-Fi ». Mémoire de fin en vue de l'obtention du grade d'Ingénieur Civil Informaticien en Sciences Appliquées. Université Libre de Bruxelles, Faculté des Sciences Appliquées Année académique 2005-2006.

[16] N. Badache, D. Djenouri, A. Derhab, T. Lemlouma, "Les protocoles de routage dans les réseaux mobiles Ad Hoc", Laboratoire des logiciels de base CERIST, vol. 12, no. 02, 2002

[17] N.DAUJEARD, J.CARSIQUE, R.LADJADJ, A.LALLEMAND, «le routage dans les réseaux mobiles Ad hoc». 2003.

[18] J.P. Chanet. Algorithme de routage coopératif à qualité de service pour des réseaux ad hoc agrienvironnementaux. Réseaux et télécommunications [cs.NI]. Université Blaise Pascal -Clermont - Ferrand II, 2007. Français. tel-00343131.

[19] "Jamming and Anti-jamming Techniques in Wireless Networks: A Survey", Int. J. Ad Hoc and Ubiquitous Computing.

[20] A.Mpitziopouls, D.Gavalas, C.Konstantopoulos, G.Pantziou, " A Survey On Jamming Attacks and Countermeasures in WSNs", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 4, FOURTH QUARTER 2009

[21] N.H.Motlagh, Frequency Hopping Spread Spectrum An Effective Way to Improve Wireless Communication Performance Department of Information Technology, Vaasa University of Applied Sciences Finland, September 2014

[22] Aydin, N. and Arslan, T. and Cumming, D.R.S. (2005), "A direct-sequence spreadspectrum communication system for integrated sensor microsystems", IEEE Transactions on Information Technology in Biomedicine 9(1):pp. 4-12.

[23] A. Mangla, "Prevention of Jamming Attack in MANET", International Journal of Science, Engineering and Technology Research (IJSETR), vol. 4, no. 7, 2015.

[24] A. Hamieh and J. Ben-Othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution", IEEE ICC 2009 proceedings, 2009.

[25] A. Dorri and S. Kamel, "Security Challenges in Mobile Ad Hoc Networks: A Survey", International Journal of Computer Science & Engineering Survey, vol. 6, no. 1, pp. 15-29, 2015.

[26] R. Zhang, J. Sun, Y. Zhang and X. Huang, "Jamming-Resilient Secure Neighbor Discovery in Mobile Ad Hoc Networks", IEEE Transactions on Wireless Communications, vol. 14, no. 10, pp. 5588-5601, 2015.

[27] A. Al Sharah, T. Oyedare and S. Shetty, "Detecting and Mitigating Smart Insider Jamming Attacks in MANETs Using Reputation-Based Coalition Game", Journal of Computer Networks and Communications, vol. 2016, pp. 1-13, 2016.

Annexe A

Publication du mémoire

Notre proposition a été acceptée pour être publier à l'ACM - 8ème Conférence Internationale sur le Génie Logiciel et les Nouvelles Technologies (ICSENT'2019 " 8th International Conference on Software Engineering and New Technologies").

Voici la lettre d'acceptation :

Acceptance Letter

Paper ID: 62

Author(s): Baraa Bouachma

Title: Development and implementation of a new ANTI-JAMMING security strategy for ad hoc mobile networks MANET.

Dear Baraa Bouachma

It is our pleasure to inform you that the paper referenced above has been accepted for oral presentation at the ACM - 8th International Conference on Software Engineering and New Technologies (ICSENT'2019), to be held in Hammamet, Tunisia 28 - 30 December 2019.

Acceptance of your paper and publication in the proceedings of ICSENT'2019 are made with the understanding that at least one author will attend the conference to present the paper. The conference policy requires that at least one author of a paper registers the conference.

Annexe B

Code de la technique

```
NS_LOG_COMPONENT_DEFINE ("JammingMitigationExample");
using namespace ns3;
Void ReceivePacket (Ptr<Socket> socket)
{
        Ptr<Packet> packet;
        Address from;
        while (packet = socket->RecvFrom (from))
        {
                if (packet->GetSize () > 0)
                {
                        InetSocketAdress iaddr = InetSocketAdress::ConvertFrom (from);
                        NS_LOG_UNCOND ("--\nReceived one packet! Socket: "<<
iaddr.GetIpv4 ()
                                << " port: " << iaddr.GetPort () << " at time = " <<
                                        Simulator::Now ().GetSeconds () << "\n--");
                }
        }
}
static void GenerateTraffic (ptr<Socket> socket, uint32_t pktSize, Ptr<Node> n, uint32_t
pktCount, Time pktInterval);
{
        if (pktCount > 0)
        {
                socket->Send (Create<Packet> (pktSize));
                Simulator::Schedule (pktInterval, &GenerateTraffic, socket, pktSize, n,
pktCount - 1, pktInterval);
        }
        else
        {
                socket->Close ();
        }
}
```

```
Void NodeRss (double oldValue, double rss)
 {
        NS_LOG_UNCOND (Simulator::Now ().GetSeconds () << "s Node RSS = " << rss
<< "W");
 }
 Void NodePdr (double oldValue, double pdr)
 {
        NS_LOG_UNCOND (Simulator::Now ().GetSeconds () << "s Node PDR = " <<
pdr);
Void NodeThroughputRx ( double oldValue, double rxThroughput)
 {
        NS_LOG_UNCOND (Simulator::Now ().GetSeconds () << "s Node RX throughput
= " << rxThroughput);
 }
 int main (int argc, char *argv[])
 {
        LogComponentEnable ("NslWifiPhy", LOG_LEVEL_DEBUG);
        LogComponentEnable ("WirelessModuleUtility", LOG_LEVEL_DEBUG);
        LogComponentEnable ("JammerHelper", LOG_LEVEL_DEBUG);
        LogComponentEnable ("Jammer", LOG_LEVEL_DEBUG);
        LogComponentEnable ("ReactiveJammer", LOG_LEVEL_DEBUG);
        LogComponentEnable ("JammingMitigationHelper", LOG_LEVEL_DEBUG);
        LogComponentEnable ("JammingMitigation", LOG_LEVEL_DEBUG);
        LogComponentEnable ("MitigateByChannelHop", LOG_LEVEL_DEBUG);
        LogComponentEnable ("MitigateByChannelHop", LOG_LEVEL_DEBUG);
        std::string phyMode ("DSSSRate1Mbps");
        double Prss = -80;       //dBm
        uint32_t PpacketSize = 200;    // Octets
        bool verbose = false;
        // Paramètres de simulation
        uint32_t numPackets = 10000;   // Nombre de paquets à envoyer
        double interval = 1;   // Secondes
        double startTime = 0.0;   // Secondes
        double distanceToRx = 10.0;   // Mètres
        double offset = 81;
        CommandLine cmd;
        cmd.AddValue ("phyMode", "Wifi Phy mode", phyMode);
        cmd.AddValue ("Prss", "Intended primary RSS (dBm)", Prss);
        cmd.AddValue ("PpacketSize", "size of application packet sent", PpacketSize);
        cmd.AddValue ("numPackets", "Total number of packets to send", numPackets);
        cmd.AddValue ("numPackets", "Simulation start time", startTime);
        cmd.AddValue ("distanceToRx", "X-Axis distance between nodes", distanceToRx);
        cmd.AddValue ("verbose", "Turn on all device log components", verbose);
        cmd.Parse (argc, argv);
```

```
        Time interPacketInterval = Seconds (interval);
                Config::SetDefault
("ns3::WifiRemoteStationManager::FragmentationThreshold", StringValue ("2200"));
        // Désactiver RTS / CTS pour les trames inférieures à 2200 octets
        Config::SetDefault                ("ns3::WifiRemoteStationManager::RtsCtsthreshold",
StringValue ("2200"));
                Config::SetDefault      ("ns3::WifiRemoteStationManager::NonUnicastMode",
StringValue ("phyMode"));
        NodeContainer c;
        c.Create (100);
        NodeContainer honestNodes;
        honestNodes.Add (c.Get (0));
          ……….
          ……….
        honestNodes.Add (c.Get (99));
        NodeContainer jammerNode (c.Get (99));
        wifiHelper wifi;
        if (verbose)
        {
                wifi.EnableLogComponents ();
        }
        wifi.SetStandard (WIFI_PHY_STANDARD_80211b);
        /** Wifi PHY **/
         /***************************************************************************/
         NslWifiPhyHelper wifiPhy = NslWifiPhyHelper::Default ();
         wifiPhy.Set ("NslRxGain", DoubleValue (-10));
         wifiPhy.Set ("NslRxGain", DoubleValue (offset + Prss));
         wifiPhy.Set ("NslCcaMode1Threshold", DoubleValue (0.0));7
         /***************************************************************************/
         /** Canal wifi **/
         NslWifiChannelHelper wifiChannel;
         wifiChannel.SetPropagationDelay ("ns3::ConstantSpeedPropagationDelayModel");
         wifiChannel.AddPropagationLoss ("ns3::FriisPropagationLossModel");
         // Créer un canal wifi **/
         Ptr<NslWifiChannel> wifiChannelPtr = wifChannel.Create ();
         wifiPhy.SetChannel (wifiChannelPtr);
         /** Couche MAC **/
         // Ajouter un MAC supérieur non QoS et désactiver le contrôle du débit
         NqosWifiMacHelper wifiMac = NqosWifiMacHelper::Default ();
         wifi.SetRemoteStationManager    ("ns3::ConstantRateWifiManager",    "DataMode",
StringValue (phyMode), "ControlMode", StringValue (phyMode));
         // Réglez-le en mode ad-hoc
         wifiMac.SetType ("ns3::AdhocWifiMac");
```

```
        /** Installer PHY + MAC **/
        NetDeviceContainer devices = wifi.Install (wifiphy, wifiMac, honestNodes);
        // Installer MAC & PHY sur le brouilleur
        NetDeviceContainer jammerNetdevice = wifi.Install (wifiphy, wifiMac, jammerNodes);
// Emplacement du brouilleur
        mobility.SetPositionAllocator (positionAlloc);
        mobility.SetMobilityModel ("ns3::ConstantPositionMobilityModel");
        mobility.Install (c);
/**************************************************************************************************/
        /** Utilitaire de module sans fil **/
/**************************************************************************************************/
        WirelessModuleUtilityHelper utilityHelper;
        // Définir la liste d'inclusion / exclusion pour tous les nœuds
        std::vector<std::string> AllInclusionList;
        AllInclusionList::push_back ("ns3::UdpHeader");      // Enregistrer uniquement l'en-tête Udp
        std::vector<std::string> AllExclusionList;
        AllExclusionList.push_back ("ns3::olsr::PacketHeader");  // Ignorer tous les en-têtes / remorques alsr
        // Attribuer des listes à l'aide
        utilityHelper.SetInclusionList (AllInclusionList);
        utilityHelper.SetExclusionList (AllExclusionList);
        // Installer sur tous les nœuds
        WirelessModuleUtilityContainer utilities = utilityHelper.InstallAll ();
/**************************************************************************************************/
        /** Brouilleur **/
       /**************************************************************************************************/
        JammerHelper jammerHelper;
        // Configurer le type de brouilleur
        jammerHelper.SetJammerType ("ns3::ReactiveJammer");
        // Définir les paramètres du brouilleur
        jammerHelper.Set ("ReactiveJammerRxTimeout", TimeValue (Seconds (2.0)));
        jammerHelper.Set ("ReactiveJammerReactionStrategy", UintegerValue(ReactiveJammer::FIXED_PROBABILITY));
        // Activer la réaction du brouilleur à l'atténuation du brouillage
        JammerHelper.Set ("ReactiveJammerReactToMitigation", UintegerValue(true));
        // Installer un brouilleur
        JammerContainer jammers = jammerHelper.Install (jammerNodes);
        // Obtenez le pointeur sur le brouilleur
```

```
        Ptr<Jammer> jammerPtr = jammers.Get (0);
        // Permettre à tous les brouilleurs de déboguer les instructions
        if (verbose)
        {
                jammerHelper.EnableLogComponents ();
        }

/**********************************************************************
**********/
        /** Atténuation des brouillages **/
/**********************************************************************
**********/
        JammingMitigationHelper mitigationHelper;
        // Configurer le type d'atténuation
        mitigationHelper.SetJammingMitigationTYpe ("ns3::MitigateByChannelHop");
        // Configurer les paramètres d'atténuation
        mitigationHelper.Set ("MitigateByChannelHopDelay", TimeValue (Seconds (0.0)));
        mitigationHelper.Set ("MitigateByChannelHopDetecttionMethod", UintegerValue
(MitigateByChannelHop::PDR_AND_RSS));
        // Installer l'atténuation sur des nœuds honnêtes
        JammingMitigationContainer mitigators = mitigationHelper.Install (honestNodes);
        // Obtenir le pointeur sur l'objet d'atténuation
        Ptr<JammingMitigation> mitigationPtr = mitigators.Get (0);

/**********************************************************************
****/
/**********************************************************************
*/
        /** Configuration de la simulation **/
        // Démarrer le trafic
        Simulator::Schedule (Seconds (startTime), &GenerateTraffic, source, PpacketSize,
honestNodes.Get (0), numPackets, interPacketInterval);
        // Démarrer le brouilleur à 7.0 secondes
        Simulator::Schedule (Seconds (startTime + 7.0), &ns3::Jammer::StartJammer,
jammerPtr);
        // Commencer l'atténuation du brouillage à 28.0 secondes
        Simulator::Schedule (Seconds (startTime + 28.0),
&ns3::JammingMitigation::StartMitigation, mitigationPtr);
        Simulator::Stop (Seconds (60.0));
        Simulator::Run ();
        Simulator::Destroy ();
                return 0;
 }
```

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Larbi Tébessi -Tébessa-

Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie

Déclaration sur l'honneur de non-plagiat

(À joindre obligatoirement au mémoire, remplie et signée)

Je soussigné(e).

Nom, prénom : Bouachma Barae

Régulièrement inscrit (e) 12/11/2018

N° de carte d'étudiant : M2015340211696

Année universitaire : 2019/2020

Domaine : Mathématiques et informatique

Filière : Information

Spécialité : Réseaux et sécurité informatique

Intitulé du mémoire : Développement et implémentation d'une nouvelle stratégie de sécurité ANTI-BRUIT pour les réseaux Mobile ad hoc Network (MANET)

Atteste que mon mémoire est un travail original et que toutes les sources utilisées ont été indiquées dans leur totalité .je certifie également que je n'ai ni recopié ni utilisé des idées ou des formulations tirées d'un ouvrage, article ou mémoire ,en version imprimée ou électronique, sans mentionner précisément leur origine et que les citations intégrales sont signalées entre guillemets.

Sanctions en cas de plagiat prouvé :

L'étudiant sera convoqué de vent le conseille de discipline, les sanctions prévues selon la gravité de plagiat sont :

- L'annulation du mémoire avec possibilité de la refaire sur un sujet différent.
- L'exclusion d'une année du master.
- L'exclusion définitive.

Fait Tébessa, le 15/06/2020

Signature de l'étudiant(e).