
République Algérienne Démocratique et Populaire
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
CENTRE UNIVERSITAIRE BELHADJ BOUCHAIB D'AÏN-TÉMOUCHENT



Institut des Sciences
Département de Mathématiques et Informatique

Mémoire

Pour l'obtention du Diplôme de Master en Informatique

Option : Réseaux et Ingénierie des Données (RID)

Présenté par :

Mlle. Amina Wafaa SAADALLAH
M. Mohammed Seddik BELBACHIR

OPTIMISATION DES PERFORMANCES PAR LA GESTION DE LA MOBILITÉ DANS LES RÉSEAUX DE CAPTEURS SANS FIL

Encadrant :

M. Mohamed Amine MESSAOUDI
Maitre Assistant "A" à C.U.B.B.A.T.

Soutenu en 2018

Devant le jury composé de :

Président :	M. Ali BENZERBADJ (M.A.A)	C.U.B.B.A.T.
Examineur :	Mlle. Djamila BOUHALOUANE (M.A.A)	C.U.B.B.A.T.
Encadrant :	M. Mohamed Amine MESSAOUDI (M.A.A)	C.U.B.B.A.T.

Dédicaces

Je dédie ce modeste travail

*A mon cher père, à ma chère mère, pour leur extrême amour, et leurs incessants
encouragements.*

*Depuis de nombreuses années, ils ont toujours eu foi en moi et n'ont jamais cessé de croire en
moi, que DIEU les préserve et leur prête bonne santé et une longue vie prospère.*

A mes chères sœurs, Imene et Asmaa ainsi qu'à mon frère Azzedine

*A mon binôme BELBACHIR Seddik Mohamed qui a su me soutenir tout au long de la
réalisation de notre travail.*

A mes amis qui m'ont toujours soutenu, et encouragé

Un grand merci à Nadir, Hind, Fadia, Ismail et la liste est encore bien longue A toute

A la famille « SAADALLAH et BENAOUDA ».

*A mon encadrant, aux membres du jury, à tout le cadre professoral du département
des Mathématiques et Informatique, à tous mes professeurs qui m'ont fait confiance tout au
long de mon cursus universitaire, et qui m'ont fait acquérir des compétences
et un savoir dont je serai éternellement reconnaissante.*

SAADALLAH Amina Wafaa

Dédicaces

Je dédie ce modeste mémoire aux personnes les plus chères à mon cœur

*A mes chers parents, qui n'ont jamais cessé de m'épauler, que dieu les préserve et leur
accorde une longue vie,*

A mes frères Sidahmed, Ben Ali ainsi qu'à mes chères sœurs Ikram et Douaa

A mon binôme SAADALLAH Amina Wafaa qui m'a soutenu

durant la réalisation de notre mémoire

A mes très chers amis Hind, Ibtissem, Madjid, Rayene, Othmane

Adel, Mohamed et bien d'autres

A toute ma famille, à tous mes amis

*Et un grand merci à mon encadrant, aux membres du jury et à tous les enseignants du
département des Mathématiques et Informatique, qui m'ont accompagné durant tout
mon parcours universitaire.*

BELBACHIR MOHAMED SEDDIK

Remerciements

*D'abord nous remercions le bon DIEU tout puissant de nous avoir
donné le courage, la volonté et la patience de réaliser et
d'accomplir ce mémoire.*

*Nous tenons à exprimer nos plus sincères remerciements à M. MESSAOUDI M.A
pour son encadrement, ses conseils avisés
qui nous ont beaucoup servi à l'élaboration de ce travail.*

*Nous adressons également notre sincère reconnaissance à M. BENZERBADJ pour avoir
accepté de présider le jury de notre soutenance. Nos remerciements vont aussi
à Mlle BOUHALOUANE pour avoir accepté d'évaluer notre modeste travail.*

*Sans oublier toute personne ayant
contribué de près ou de loin à accomplir et mener à bien notre projet de fin d'études.*

Résumé

Un réseau Ad-hoc est une collection d'entités mobiles interconnectées par une technologie sans fil, formant un réseau temporaire à la topologie variable et dynamique. A peine initialisées, ces entités sont capables en un temps relativement court de communiquer indépendamment de leur localisation géographique. Fonctionnant sans infrastructure et sans l'aide de toute administration centralisée, les communications multi-sauts y sont possibles grâce à des protocoles de routage spécifiques.

Dans le cadre de ce mémoire le comportement du protocole de routage géographique GPSR est abordé suivi d'un algorithme qui a fait ses preuves par le passé, inspiré du comportement collectif des colonies de fourmis dans la nature, il a été conçu pour répondre aux besoins de l'optimisation combinatoire et la résolution de problèmes complexes tels que celui du Problème du Voyageur de Commerce.

Mots clés :

Abstract

An Ad-hoc network is a collection of a mobile entities interconnected by wireless technology, forming a temporary network with a variable and dynamic topology. Barely initialized, these entities are able in a relatively short time to communicate independently of their geographical location. Operating without infrastructure and Without the help of any centralized administration, multi-hops communications are possible through specific routing protocols.

As part of our work, the behavior of the geographic routing protocol GPSR is approached followed by an algorithm that has been proven in the past, inspired by the collective behavior of ants colony in nature, It was designed to meet the needs of combinatorial optimization and complex problems solving such as the Travelling Salesman Problem.

Keywords : mots clé en anglais

Table des matières

Table des Figures	iii
1 Les réseaux Ad-hoc	3
1.1 Introduction	4
1.2 Les réseaux sans fil émergents	4
1.3 Les environnements mobiles	4
1.3.1 Réseaux mobiles avec infrastructure	5
1.3.2 Réseaux sans fil sans infrastructure (Ad-hoc)	5
1.4 Les réseaux Ad-hoc	6
1.4.1 Concept	6
1.4.2 Modélisation d'un réseau Ad-hoc	6
1.4.3 Modes de communication dans un réseau Ad-hoc	7
1.4.4 Caractéristiques des réseaux Ad-hoc	7
1.5 Le routage dans les réseaux Ad-hoc	9
1.5.1 Les protocoles de routage basés sur la topologie	9
1.5.1.1 Les protocoles de routage proactifs	9
1.5.1.2 Les protocoles de routage réactifs	12
1.5.1.3 Les protocoles hybrides	16
1.5.2 Les protocoles de routage basés sur la localisation (géographiques)	17
1.6 La gestion de mobilité dans les réseaux Ad-hoc	19
1.6.1 Les modèles individuels	19
1.6.1.1 Les modèles sans mémoire	19
1.6.1.2 Les modèles avec mémoire	21
1.6.2 Les modèles de groupes	22
1.7 Conclusion	24
2 La sûreté de fonctionnement	25
2.1 Introduction	26
2.2 La sûreté de fonctionnement	26
2.2.1 Principe	26
2.2.2 Méthodes d'analyse de sûreté de fonctionnement	27
2.3 Défaillances d'un réseau informatique sans fil	27
2.3.1 La consommation d'énergie	27
2.3.1.1 Facteurs de dissipation d'énergie	28
2.3.1.2 Sources de surconsommation d'énergie	28
2.3.2 L'interception de données	29
2.3.2.1 L'intrusion réseau	29
2.3.2.2 Le brouillage radio	30
2.3.2.3 Les dénis de service	30
2.3.3 Les interférences	30

2.3.3.1	Obstacles physiques	30
2.3.3.2	Achalandage du réseau	31
2.3.3.3	Interférences fréquentielles	31
2.3.4	Congestion dans un réseau	31
2.3.4.1	Scénario de la congestion du réseau	32
2.3.4.2	Symptômes de la congestion	32
2.4	Les problèmes de mobilité	32
2.5	Conclusion	33
3	Approche et algorithmes	34
3.1	Introduction	35
3.2	Principe de fonctionnement du protocole GPSR	35
3.2.1	Mode Greedy	35
3.2.2	Mode Perimeter	37
3.2.2.1	Planarisation avec le graphe RNG (Relative Neighbourhood Graph)	38
3.2.2.2	Planarisation avec le graphe GG (Gabriel Graph)	39
3.2.3	Diagramme de cas d'utilisation	41
3.3	La rencontre des réseaux informatiques et de l'intelligence artificielle	42
3.3.1	Pourquoi le choix des fourmis	42
3.3.2	Relation avec l'informatique	42
3.4	L'algorithme de colonie de fourmis	42
3.4.1	Le Problème du Voyageur de Commerce	43
3.4.2	Principe de l'algorithme de colonie de fourmis "Ant System"	44
3.4.2.1	Définition informelle	44
3.4.2.2	Définition formelle	45
3.5	Conclusion	46
4	Implémentation et résultats	47
4.1	Introduction:	48
4.2	Environnement de travail : machine utilisée	48
4.3	Langage de programmation	48
4.4	Environnement de développement : Logiciel utilisé	48
4.5	Simulation et discussion des résultats	49
4.6	Conclusion:	54
	Bibliographie	57

Table des figures

1.1	Réseaux mobiles avec infrastructure	5
1.2	Réseaux sans fil sans infrastructure (Ad-hoc)	6
1.3	Modélisation d'un réseau Ad-hoc	7
1.4	La technique œil de poisson	11
1.5	Le partitionnement du réseau en groupes.	12
1.6	Construction de l'enregistrement de route.	13
1.7	Le renvoi du chemin.	13
1.8	La propagation du paquet de requête.	15
1.9	(x,y) : (le niveau de référence, la taille du noeud).	16
1.10	La réaction du protocole TORA de la défaillance du lien (5,7).	16
3.1	Exemple du mode Greedy	36
3.2	Echec du mode Greedy	37
3.3	Planarisation d'un graphe	37
3.4	Graphe RNG	38
3.5	Graphe GG	39
3.6	Exemple du mode Perimeter	40
3.7	La règle de la main droite (intérieur du triangle).	40
3.8	Diagramme de cas d'utilisation.	41
3.9	Contournement d'un obstacle par une colonie de fourmis.	44
4.1	Initialisation des paramètres de simulation	49
4.2	Initialisation des paramètres de l'algorithme de colonie de fourmis	50
4.3	Test de simulation	51
4.4	Parcours des nœuds mobiles	52
4.5	Solution optimale : Matrice de probabilités	52
4.6	Établissement des liens	53
4.7	Historique	54

Introduction

Le développement technologique que perçoit le monde actuellement a touché tous les secteurs, particulièrement le domaine de la télécommunication qui connaît une évolution considérable avec l'apparition de la technologie sans fil. Avec le succès de cette dernière, il devient simple et aisé d'accéder à un réseau de n'importe où et à tout moment sans avoir à connecter les appareils communicants, physiquement à une infrastructure.

Dans les réseaux Ad-hoc, la connectivité doit être maintenue et préservée autant que possible automatiquement lorsque la topologie du réseau change (suite à l'apparition, la disparition ou aux mouvements de certains nœuds).

Dans un contexte critique, notre démarche consiste à rendre chaque nœud capable de joindre directement ses voisins en utilisant des nœuds intermédiaires mobiles. Ces derniers se chargent de relayer les paquets et ainsi offrir une continuité de service. Cependant, la mobilité est une tâche contraignante et pénible à gérer car elle doit être abordée à différentes couches pour être transparente aux utilisateurs.

L'objectif de notre travail est d'étudier, analyser et expérimenter l'algorithme de colonie de fourmis (nœuds mobiles) sur un réseau de capteurs sans fil, afin d'assurer la continuité de service (transmission des paquets) jusqu'à destination grâce à la mise en œuvre du protocole géographique GPSR (Greedy Perimeter Stateless Routing).

Ce mémoire comporte quatre chapitres :

Dans le premier chapitre, nous présentons les concepts de base des réseaux sans fil en mettant l'accent sur les réseaux Ad-hoc, leur principe et modes de fonctionnement ainsi que le processus et les protocoles de routage utilisés. Nous finirons ce chapitre par la présentation des différents modèles de la gestion de mobilité dans les réseaux Ad-hoc.

Plusieurs rappels théoriques sont présentés dans le second chapitre consacré à la sûreté de fonctionnement, cette discipline qui cherche à mesurer la qualité de service délivrée par un système, de manière à ce que l'utilisateur ait en lui une confiance justifiée. Nous présentons aussi dans ce chapitre une simple identification des défaillances qui peuvent se poser et porter atteinte au bon fonctionnement de notre réseau.

Le troisième chapitre est consacré à la présentation détaillée du protocole de routage utilisé ainsi que les algorithmes de base qui ont servi à l'implémentation du protocole GPSR plus l'algorithme de colonie de fourmis qui servira à résoudre un problème d'optimisation combinatoire qui est celui du voyageur de commerce.

Nous présentons dans le dernier chapitre notre simulation informatique, en appliquant les algorithmes et les concepts vus dans le chapitre précédent. Et nous analyserons en dernier lieu les résultats des tests menés sur notre application.

Nous terminons ce mémoire par une conclusion générale dans laquelle nous précisons les apports de notre démarche et les perspectives à cette dernière.

Chapitre 1

Les réseaux Ad-hoc

Sommaire

1.1	Introduction	4
1.2	Les réseaux sans fil émergents	4
1.3	Les environnements mobiles	4
1.3.1	Réseaux mobiles avec infrastructure	5
1.3.2	Réseaux sans fil sans infrastructure (Ad-hoc)	5
1.4	Les réseaux Ad-hoc	6
1.4.1	Concept	6
1.4.2	Modélisation d'un réseau Ad-hoc	6
1.4.3	Modes de communication dans un réseau Ad-hoc	7
1.4.4	Caractéristiques des réseaux Ad-hoc	7
1.5	Le routage dans les réseaux Ad-hoc	9
1.5.1	Les protocoles de routage basés sur la topologie	9
1.5.2	Les protocoles de routage basés sur la localisation (géographiques)	17
1.6	La gestion de mobilité dans les réseaux Ad-hoc	19
1.6.1	Les modèles individuels	19
1.6.2	Les modèles de groupes	22
1.7	Conclusion	24

1.1 Introduction

De nos jours l'interconnexion des ordinateurs donne lieu à de nombreux types de réseaux différents, plus ou moins étendus et bien connus, chacun d'eux se distingue par l'objectif qu'il sert, par sa taille et par les technologies qu'il sert.

Avec l'avènement d'Internet, ces technologies des réseaux et des télécommunications ont connu une progression phénoménale dans le domaine des infrastructures. Dans cette vision, bon nombre d'applications ont pu migrer des environnements traditionnels câblés vers des environnements profitant de la technologie sans fil offrant ainsi de meilleurs avantages tel que la facilité de déploiement et des coûts raisonnables.

Dans ce chapitre nous présentons le principe de fonctionnement des réseaux mobiles Ad-hoc, ainsi qu'une classification des protocoles de routage du groupe MANET (Mobile Adhoc Network) qui ont été proposés pour assurer le service de routage dans ce type de réseaux suivi des différents modèles de mobilité.

1.2 Les réseaux sans fil émergents

Un réseau sans fil est par définition un réseau, où deux ou plusieurs terminaux peuvent communiquer sans liaison filaire en ayant recours à des ondes radioélectriques (radio ou infrarouge) ceci pour but d'assurer la connectivité entre les périphériques sur une zone géographique qui peut être étendue et ce même en cas de mobilité.

Les systèmes sans fil opèrent sur des bandes non soumises à licence, comme les bandes ISM (industriel, scientifique et médical) sous réserve de respect des conditions de puissance et de fréquence définies pour chaque pays par l'agence nationale des fréquences, où tous les équipements sont autorisés à utiliser le spectre électromagnétique, pourvu qu'ils limitent leur puissance d'émission afin de laisser les autres coexister.

Parmi la famille des réseaux sans fil, on compte les réseaux Ad-hoc qui suscitent un grand intérêt dans le domaine scientifique et de la recherche, plusieurs groupes de recherche se sont formés suite à cela dont le groupe IETF (Internet Engineering Task Force) qui a son tour a créé le groupe MANET qui est chargé de standardiser des protocoles de routage basés sur la technologie IP pour les réseaux Ad-hoc sans fil.

1.3 Les environnements mobiles

Les environnements mobiles permettent une grande flexibilité d'emploi. Plus précisément la mise en réseau de sites dont le câblage serait coûteux à mettre en œuvre permettant ainsi à l'utilisateur d'accéder à des informations indépendamment de leurs positions géographiques autrement dit l'utilisateur peut se déplacer dans le réseau tout en gardant la même adresse, il a la possibilité d'accéder aux services offerts par le réseau de n'importe où et à n'importe quel moment. Cela nécessite d'une part des mécanismes de localisation de l'utilisateur, et d'autre part une assurance de la continuité des communications en cours de déplacement (le mécanisme handover).

L'environnement mobile offre beaucoup d'avantages par rapport aux environnements traditionnels. Toutefois, le problème de la mobilité dans les réseaux sans fil n'est pas négligeable, de nouveaux problèmes peuvent apparaître tels que les problème de routage

Les réseaux mobiles peuvent être classés comme suit : avec infrastructure et sans infrastructure.

1.3.1 Réseaux mobiles avec infrastructure

Le réseau est obligatoirement composé d'un point d'accès ou d'un site fixe appelé station de base (SB), munis d'une interface de communication sans fil pour la communication directe avec les sites ou unités mobiles (UM), une station de base couvre une zone géographique limitée appelée cellule, une unité mobile est rattachée à un moment donné qu'à une station de base lui offrant tous les services tant que l'UM est à l'intérieur de la zone de couverture de la SB.

La SB fait office de pont entre un réseau filaire et un réseau sans fil, permettant de relier une UM à une unité connectée à un site fixe. La SB est aussi le point de passage de la transmission d'une UM à une autre UM. Si les deux UM dépendent de la même SB, la trame est simplement relayée par la SB. Si les deux UM sont à deux SB différentes, une trame échangée entre les deux UM doit être relayée par le réseau filaire qui relie les deux points d'accès. Les points d'accès peuvent être répartis sur tout le réseau filaire, agrandissant d'autant la couverture du réseau sans fil.

Dans le cas où un nœud mobile se déplace en dehors de la portée radio d'une station de base, un mécanisme de Handover se produit, ce dernier consiste à faire le passage du contrôle d'une station de base au contrôle d'une autre station de base adjacente.[7].

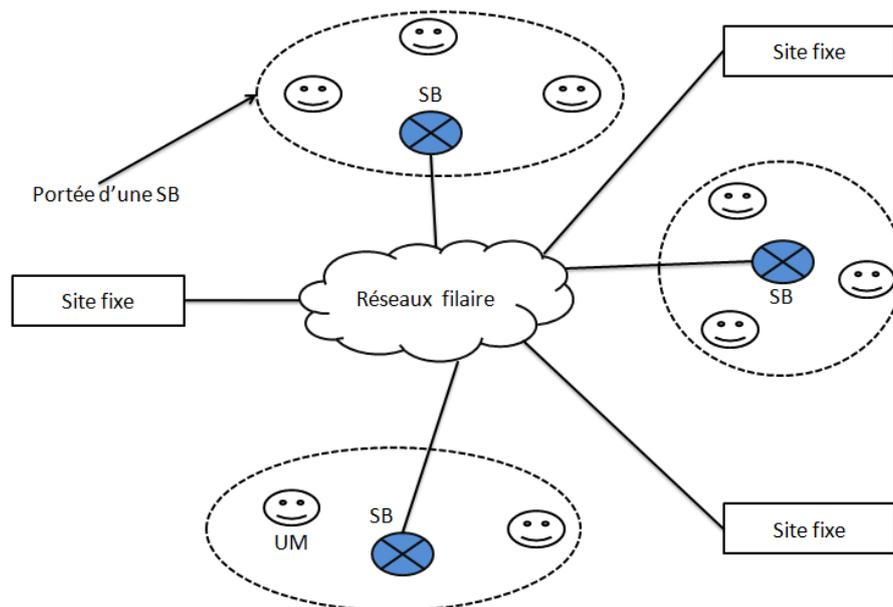


FIGURE 1.1 – Réseaux mobiles avec infrastructure [10]

1.3.2 Réseaux sans fil sans infrastructure (Ad-hoc)

Il s'agit d'un mode Point à Point, dans ce modèle de mobilité l'entité de site fixe n'existe pas et donc ne nécessitant pas de points d'accès. Il permet de connecter les stations quand

aucun point d'accès n'est disponible. L'absence d'infrastructure oblige les UM à jouer le rôle de routeurs[7].

La figure 1.2 montre l'exemple de l'UM A qui peut envoyer à l'UM C malgré que cette dernière n'est pas dans la portée de l'UM A, pour faire elle envoie les messages à l'UM B qui va les envoyer à l'UM C [7].

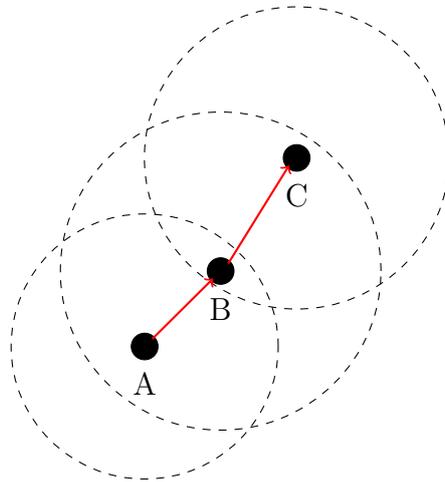


FIGURE 1.2 – Réseaux sans fil sans infrastructure (Ad-hoc) [10]

1.4 Les réseaux Ad-hoc

1.4.1 Concept

Les réseaux sans fil multi-sauts (Multi-Hop Wireless Ad hoc Networks) communément appelés réseaux Ad-hoc sont une classe de réseaux sans fil qui se caractérisent par l'absence d'infrastructure, ce qui nécessite forcément des capacités d'auto-organisation et d'auto-configuration.

Dans leur configuration mobile appelée MANET, ils sont définis comme étant un ensemble d'unités mobiles communiquant via un médium radio sur une zone géographique quelconque de manière autonome et coopérative avec pour seul moyen de communication, les ondes radio qui se propagent entre les nœuds. Une des particularités des réseaux Ad-hoc, est que chaque nœud communicant fait office d'hôte et de routeur.

1.4.2 Modélisation d'un réseau Ad-hoc

Un réseau Ad-hoc peut être modélisé par un graphe $G_t = (V_t, E_t)$ où V_t représente l'ensemble des nœuds (i.e. les unités ou les hôtes mobiles) du réseau et E_t modélise l'ensemble des connections qui existent entre ces nœuds. Si $e = (u, v)$ appartient à E_t , cela veut dire que les nœuds u et v sont en mesure de communiquer directement à l'instant t [29].

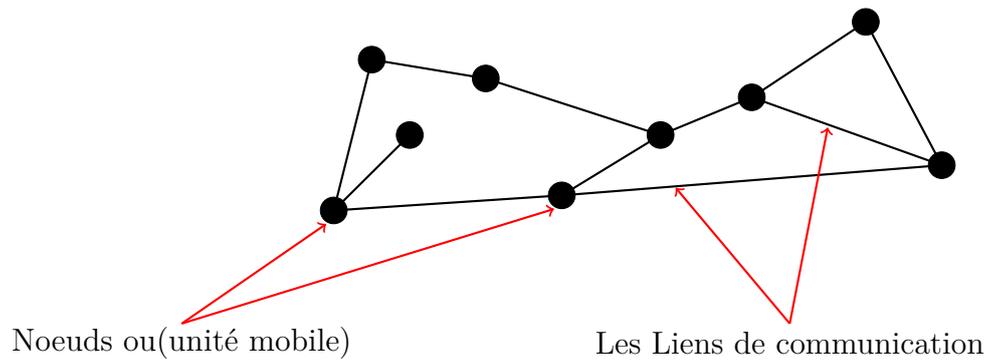


FIGURE 1.3 – Modélisation d'un réseau Ad-hoc

1.4.3 Modes de communication dans un réseau Ad-hoc

Il existe deux modes de communication, dans le premier cas il est question de deux nœuds se trouvant dans une même portée radio, ils peuvent donc communiquer directement, ce mode est appelé Transmission mono-saut, cependant dans le deuxième mode, où les nœuds source et destination peuvent ne pas être dans une même portée radio, des chemins de routage multi-sauts sont alors nécessaires voire inévitables pour l'acheminement de paquets en utilisant d'autres nœuds comme relais pour assurer la communication, ce mode est appelé Transmission multi-sauts.

La mobilité des nœuds présente l'avantage de pouvoir changer la topologie de manière dynamique et fluide mais surtout aléatoire, mais par moments cette caractéristique peut s'avérer problématique quand les changements sont fréquents, au risque d'engendrer une rupture de liens ; un autre inconvénient est considérable, celui des contraintes d'interférences quand deux transmissions simultanées utilisent une même fréquence ou des fréquences proches qui peuvent interférer.

1.4.4 Caractéristiques des réseaux Ad-hoc

Les réseaux Ad-hoc sont caractérisés par ce qui suit [21] :

- **Absence d'infrastructure centralisée :**

Les réseaux Ad-hoc travaillent dans un environnement distribué indépendamment d'une administration centralisée contrairement aux réseaux mobiles ce qui leur prodigue une autonomie et la capacité de se déplacer librement, les hôtes mobiles dans un tel réseau jouent également le rôle de routeurs ce qui permet de relayer et maintenir les communications du réseau d'une manière continue.

- **Routage par relais**

Le routage par relais signifie que si un nœud souhaite communiquer avec un autre nœud qui se trouve dans sa portée, il peut le faire directement par contre s'il se trouve hors de sa portée, il doit avoir recours à d'autres nœuds actifs pour relayer l'information jusqu'au nœud destinataire.

- **Une topologie dynamique**

Les nœuds dans ce type de réseau pouvant se déplacer librement et de façon arbitraire, des routes peuvent se créer et disparaître instantanément et très souvent, ce qui provoque des changements fréquents dans la topologie du réseau à des instants imprévisibles, d'une manière rapide et aléatoire. Ces modifications doivent être prises en compte par le protocole de routage utilisé pour assurer l'acheminement des paquets.

- **Contrainte d'énergie**

Disposant de batteries limitées, les nœuds ont par conséquent une durée de traitement relative à cela. Sachant qu'une partie de l'énergie est déjà consommée par la fonctionnalité de routage, les services et les applications supportées par chaque nœud deviennent eux aussi réduits.

- **Une bande passante limitée**

Du au fait de l'utilisation d'un médium de communication partagé dans les réseaux Ad-hoc, la bande passante réservée à un hôte reste modeste.

- **L'hétérogénéité des nœuds**

Un nœud mobile peut être équipé d'une ou plusieurs interfaces radio ayant des capacités de transmission variées et opérant dans des plages de fréquences différentes. Cette hétérogénéité de capacité peut engendrer des liens asymétriques dans le réseau. De plus, les nœuds peuvent avoir des différences en terme 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.

- **Sécurité et vulnérabilités**

Dans les réseaux Ad-hoc, le principal problème ne se situe pas tant au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau. Les possibilités de s'insérer dans le réseau sont plus grandes, la détection d'une intrusion ou d'un déni de service plus délicate et l'absence de centralisation pose un problème de remontée de l'information de détection d'intrusions.

- **Multi-sauts**

Un réseau Ad-hoc est qualifié par "Multi-sauts" car plusieurs nœuds mobiles peuvent participer au routage et servent comme routeurs intermédiaires, il utilise souvent des sauts multiples pour éviter les obstacles, minimiser la consommation d'énergie ou pour joindre un nœud qui n'est pas dans la portée de communication de l'émetteur.

- **Taille des réseaux Ad-hoc**

Elle est souvent de petite ou de taille moyenne (une centaine de nœuds), le réseau est utilisé pour étendre temporairement un réseau filaire, comme pour une conférence ou des situations où le déploiement du réseau fixe n'est pas approprié. Cependant, certaines applications des réseaux Ad-hoc peuvent nécessiter une utilisation allant jusqu'à des dizaines de milliers de nœuds

1.5 Le routage dans les réseaux Ad-hoc

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

Le routage dans les réseaux Ad-hoc est beaucoup plus complexe que le routage traditionnel à cause de l'instabilité de la topologie, suite à cela bon nombre d'algorithmes de routage ont été proposés pour la découverte et le maintien des routes.

Les réseaux MANET ont comme caractéristique une forte mobilité, ce qui entraîne des changements fréquents et une topologie très dynamique. Différentes solutions ont alors vu le jour. Traditionnellement, les protocoles de routage dans les réseaux Ad-hoc se divisent en deux grandes classes : la première étant celle des protocoles de routage basés sur la topologie qui compte deux sous classes : les proactifs et les réactifs. A l'heure actuelle, il est un peu plus difficile de conserver ce découpage manichéen, une troisième sous classe est alors apparue, celle des protocoles hybrides. Et il y a également la deuxième classe de protocoles de routage qui sont basés sur la localisation géographique utilisant la position physique des nœuds pour acheminer les paquets de données.

1.5.1 Les protocoles de routage basés sur la topologie

1.5.1.1 Les protocoles de routage proactifs

Les protocoles de routage proactifs diffusent des messages de contrôle périodiques pour la création, la maintenance et la mise à jour des routes, et ce en parallèle de la transmission des données. Même s'il n'y a pas de trafic, cette maintenance reste toujours active. Cette classe de protocole est basée sur les mêmes méthodes utilisées pour les protocoles de routage dans les réseaux filaires. Les deux principales méthodes sont : la méthode à État de Liens (Link State) et la méthode du Vecteur de Distances (Distance Vector).

Ces deux méthodes reposent sur la technique du plus court chemin ce qui permet à une source de trouver le chemin le plus court vers une destination.

1. La méthode à État de Liens (Link State)

Dans cette méthode, chaque nœud maintient sa propre vision de toute la topologie du réseau. La mise à jour de cette vision se fait par diffusion périodique des requêtes par chaque nœud déclarant l'état des liens de ses voisins à tous les nœuds du réseau. L'opération de mise à jour peut se faire aussi dans le cas de changement d'un état des liens. Une fois que la mise à jour est effectuée, chaque nœud change sa vision de la topologie en se basant sur l'image complète du réseau formé des liens les plus récents. Ensuite, il applique un algorithme de calcul de route optimale pour calculer la distance qui le sépare d'une destination donnée. L'algorithme Dijkstra est un exemple des algorithmes les plus couramment appliqués dans le calcul du plus court chemin.

2. La méthode du Vecteur de Distances (Distance Vector)

Par contre dans cette méthode, chaque nœud diffuse à ses voisins sa vision des distances qui le séparent de tous les hôtes du réseau. Chaque nœud calcule le chemin le plus court vers n'importe quelle destination en se basant sur les informations reçues par tous ses voisins.

Cette approche est basée sur l'algorithme distribué de Bellman Ford (BF). Le processus de calcul de plus court chemin se répète jusqu'à ce que le réseau atteigne un état stable. Les protocoles de routage proactifs réunissent les idées des deux méthodes. Ils essayent de réduire leurs limitations, et de prendre en compte les caractéristiques des environnements mobiles afin de les adapter à ce nouvel environnement.

Dans cette catégorie, les protocoles de routage proactifs maintiennent une vision de la table de routage dans chaque nœud, grâce aux messages de mise à jour communiqués aux nœuds à chaque changement de la topologie. Les protocoles basés sur ce principe, dits aussi à diffusion de table, sont entre autres : DSDV, WRP, GSR, FSR, HSR, ZHLS, CGSR, DREAM, OLSR, etc.

Nous allons décrire dans ce qui suit, les protocoles les plus importants de cette classe :

■ LE PROTOCOLE DE ROUTAGE « DSDV » [31]

- Basé sur l'idée classique de l'algorithme distribué de Bellman-Ford en rajoutant quelques améliorations.
- Chaque station mobile maintient une table de routage qui contient :
 1. Toutes les destinations possibles.
 2. Le nombre de nœud (ou de sauts) nécessaire pour atteindre la destination.
 3. Le numéro de séquences (SN : sequence number) qui correspond à un nœud destination.
- Le SN est utilisé pour faire la distinction entre les anciennes et les nouvelles routes, ce qui évite la formation des boucles de routage.
- La mise à jour dépend donc de deux paramètres : Le temps, c'est à dire la période de transmission, et Les événements.
- Un paquet de mise à jour contient :
 1. Le nouveau numéro de séquence incrémenté, du nœud émetteur. Et pour chaque nouvelle route
 2. L'adresse de la destination
 3. Le nombre de nœuds (ou de sauts) séparant le nœud de la destination.
 4. Le numéro de séquence (des données reçues de la destination) tel qu'il a été estampillé par la destination.

■ LE PROTOCOLE DE ROUTAGE « FSR » [28]

- Le protocole FSR est basé sur l'utilisation de la technique "œil de poisson" (fisheye), proposée par Kleinrock et Stevens, qui l'ont utilisé dans le but de réduire le volume d'information nécessaire pour représenter les données graphiques.
- Dans la pratique, l'œil d'un poisson capture avec précision, les points proches du point focal. La précision diminue quand la distance, séparant le point vu et le point focal, augmente. La figure suivante illustre la technique FE utilisée par le protocole :

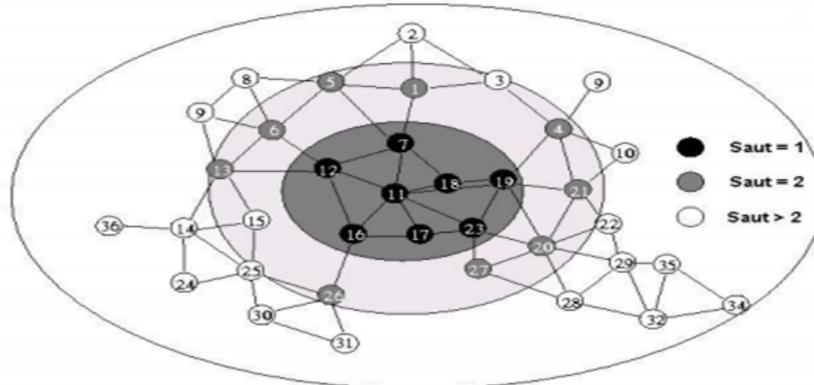


FIGURE 1.4 – La technique œil de poisson [19]

- Dans le contexte du routage, l'approche du "fisheye" matérialise, pour un nœud, le maintien des données concernant la précision de la distance et la qualité du chemin d'un voisin direct, avec une diminution progressive, du détail et de précision, quand la distance augmente.
- La diminution de fréquence est assurée en changeant les fréquences de mise à jour, et cela en utilisant des périodes d'échanges différentes pour les différentes entrées de la table de routage. Les entrées qui correspondent aux nœuds les plus proches, sont envoyés aux voisins avec une fréquence élevée (donc avec une période d'échange relativement petite).

■ LE PROTOCOLE DE ROUTAGE « HSR » [16]

- Le protocole HSR combine les notions de groupes dynamiques, niveaux hiérarchiques avec une gestion efficace de localisation.
- Dans le HSR, l'image de la topologie du réseau, est sauvegardée sous forme hiérarchique. Le réseau est partitionné en un ensemble de groupes.
- Dans un groupe, un nœud doit être élu pour représenter le reste des membres. Les représentants des groupes dans un niveau l , deviennent des membres dans le niveau $l + 1$. Ces nouveaux membres, s'organisent en un ensemble de groupes de la même manière du niveau bas, et ainsi de suite pour le reste des niveaux. La figure suivante illustre l'application du mécanisme de partitionnement hiérarchique :

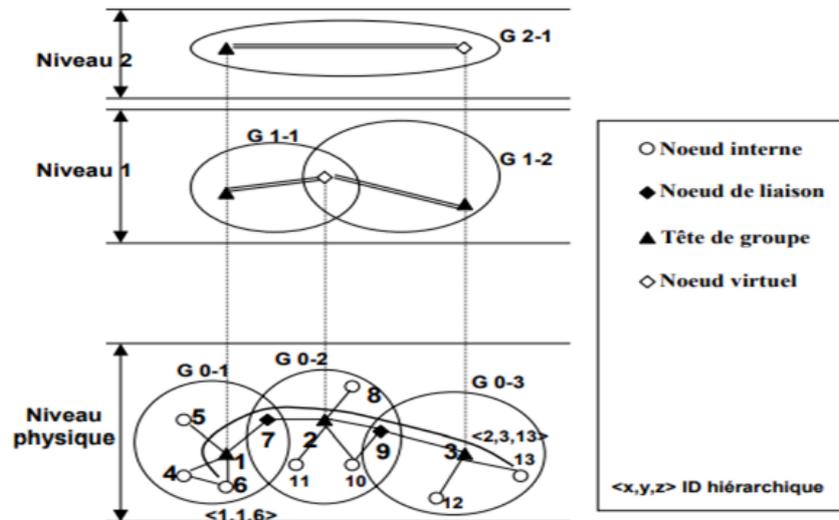


FIGURE 1.5 – Le partitionnement du réseau en groupes. [19]

- L'adresse hiérarchique, suffit pour délivrer les paquets de données à une destination, indépendamment de la localisation de la source, et cela en utilisant la table HSR. Exemple : l'acheminement des données entre le nœud 6 et le nœud 3 (figure précédente).

1.5.1.2 Les protocoles de routage réactifs

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 spécifiée, inconnue au préalable. Dans ce qui suit nous allons décrire les protocoles les plus importants de cette classe [1]

■ LE PROTOCOLE DE ROUTAGE « DSR » [5]

- Le protocole "Routage à Source Dynamique" (DSR), est basé sur l'utilisation de la technique "routage source". Dans cette technique : la source des données détermine la séquence complète des nœuds à travers lesquelles, les paquets de données seront envoyés.
- Un site initiateur de l'opération de "découverte de routes", diffuse un paquet requête de route. Si l'opération de découverte est réussite, l'initiateur reçoit un paquet réponse de route qui liste la séquence de nœuds à travers lesquels la destination peut être atteinte. Le paquet requête de route contient donc un champ enregistrement de route, dans lequel sera accumulée la séquence des nœuds visités durant la propagation de la requête dans le réseau, comme le montre la figure suivante :

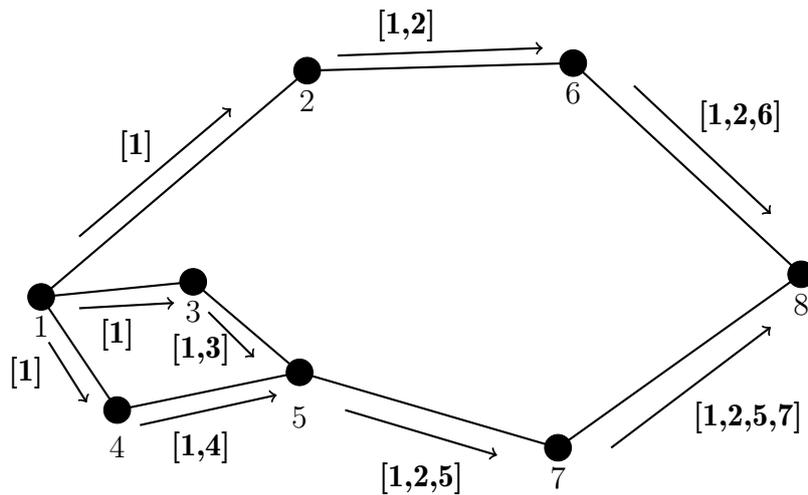


FIGURE 1.6 – Construction de l’enregistrement de route. [5]

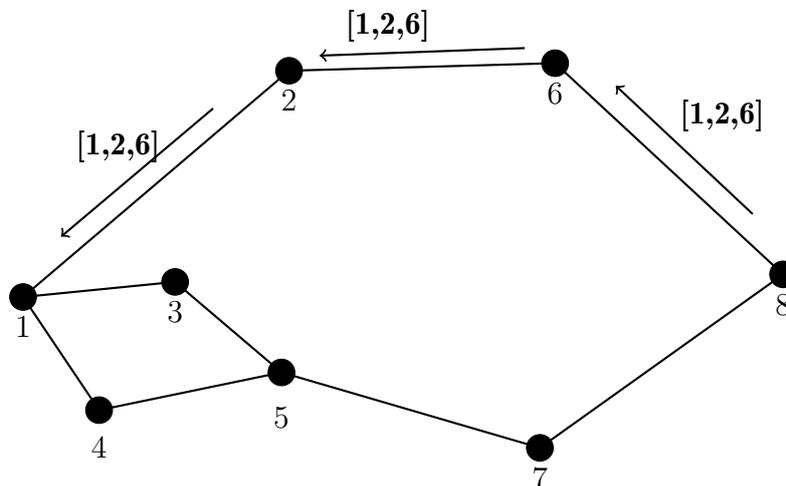


FIGURE 1.7 – Le renvoi du chemin. [5]

▷ La découverte de chemins dans le DSR.

- Afin d’assurer la validité des chemins utilisés, le DSR exécute une procédure de maintenance de routes.
- Quand un nœud détecte un problème fatal de transmission, à l’aide de sa couche de liaison, un message erreur de route (route error) est envoyé à l’émetteur original du paquet.
- Le message d’erreur contient l’adresse du nœud qui a détecté l’erreur et celle du nœud qui le suit dans le chemin.
- Lors de la réception du paquet erreur de route par l’hôte source, le nœud concerné par l’erreur est supprimé du chemin sauvegardé, et tous les chemins qui contiennent ce nœud sont tronqués à ce point là. Par la suite, une nouvelle opération de découverte de routes vers la destination, est initiée par l’émetteur.

- L'utilisation de la technique "routage source", fait que les nœuds de transit n'aient pas besoin de maintenir les informations de mise à jour pour envoyer les paquets de données, puisque ces derniers contiennent toutes les décisions de routage.
- Dans ce protocole, il y a une absence totale de boucle de routage, car le chemin source- destination fait partie des paquets de données envoyés.

■ LE PROTOCOLE DE ROUTAGE « AODV » [9]

- Le protocole AODV représente essentiellement une amélioration de l'algorithme DSDV discuté déjà, dans le contexte réactif. Le protocole AODV, réduit le nombre de diffusions de messages, et cela en créant les routes lors du besoin, contrairement au DSDV, qui maintient la totalité des routes.
- L'AODV utilise les principes des numéros de séquence à fin de maintenir la consistance des informations de routage.
- A cause de la mobilité des nœuds dans les réseaux ad hoc, les routes changent fréquemment ce qui fait que les routes maintenues par certains nœuds, deviennent invalides. Les numéros de séquence permettent d'utiliser les routes les plus nouvelles (fresh routes).
- De la même manière que dans le DSR, l'AODV utilise une requête de route dans le but de créer un chemin vers une certaine destination. Cependant, l'AODV maintient les chemins d'une façon distribuée en gardant une table de routage, au niveau de chaque nœud de transit appartenant au chemin cherché.
- Un nœud diffuse une requête de route dans le cas où il aurait besoin de connaître une route vers une certaine destination et qu'une telle route n'est pas disponible. Cela peut arriver :
 1. Si la destination n'est pas connue au préalable ;
 2. Si le chemin existant vers la destination a expiré sa durée de vie ou il est devenu défaillant.
- Le champ numéro de séquence destination du paquet RREQ, contient la dernière valeur connue du numéro de séquence, associé au nœud destination. Cette valeur est recopiée de la table de routage. Si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut. Le numéro de séquence source du paquet RREQ contient la valeur du numéro de séquence du nœud source.
- Afin de maintenir des routes consistantes, une transmission périodique du message "HELLO" est effectuée. Si trois messages "HELLO" ne sont pas reçus consécutivement à partir d'un nœud voisin, le lien en question est considéré défaillant.
- Le protocole AODV ne présente pas de boucle de routage, en outre il évite le problème "counting to infinity" de Bellman-Ford, ce qui offre une convergence rapide quand la topologie du réseau ad hoc change.

■ LE PROTOCOLE DE ROUTAGE « TORA » [13]

- Ce protocole a été conçu principalement pour minimiser l'effet des changements de la topologie qui sont fréquents dans les réseaux ad hoc.
- Afin de s'adapter à la mobilité des réseaux ad hoc, le protocole stocke plusieurs chemins vers une même destination, ce qui fait que beaucoup de changements de topologie n'auront pas d'effets sur le routage des données, à moins que tous les chemins qui mènent vers la destination seront perdus (rompus).
- TORA est caractérisé essentiellement par le fait que les messages de contrôle sont limités à l'ensemble des nœuds proches du lieu de l'occurrence du changement de la topologie.
 - Dans ce protocole, l'utilisation des meilleurs chemins a une importance secondaire, les longs chemins peuvent être utilisés afin d'éviter le contrôle induit par le processus de découverte de nouveaux chemins.
- TORA est basé sur l'utilisation de la propriété appelée "orientation destination" des graphes acycliques orientés. Un graphe acyclique orienté (DAG) est orienté destination s'il y a toujours un chemin possible vers une destination spécifiée.
- Le graphe devient non orienté destination, si un lien (ou plus) devient défaillant. Dans ce cas, les algorithmes utilisent le concept d'inversement de liens. Ce concept assure la transformation du graphe précédent, en un graphe orienté destination durant un temps fini.
- Afin de maintenir le DAG orienté destination, l'algorithme TORA utilise la notion de taille de nœud. Chaque nœud possède une taille qui l'échange avec l'ensemble de ses voisins directs. Un lien est toujours orienté du nœud qui a la plus grande taille, vers le nœud qui la plus petite taille.

La figure suivante montre la création du DAG dans le protocole TORA :

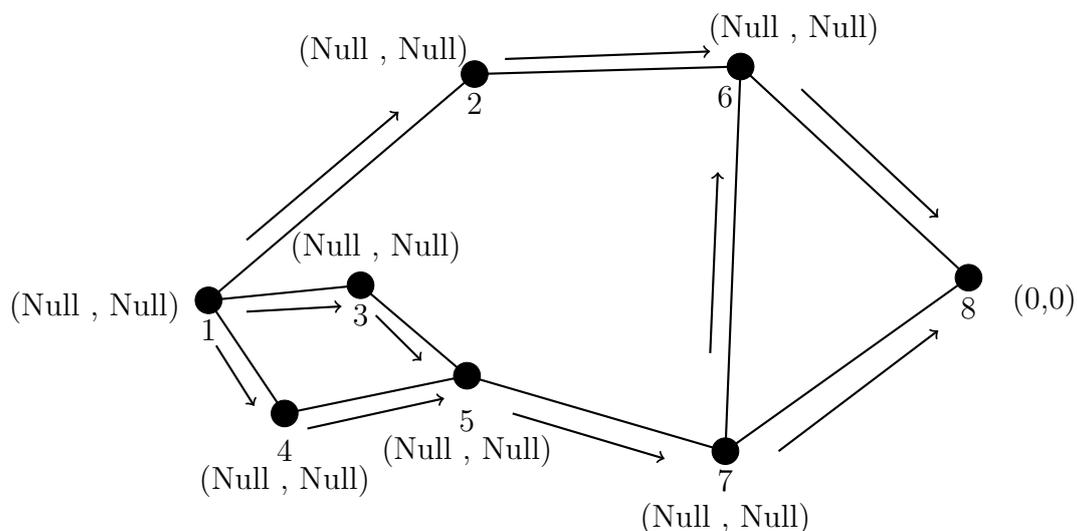


FIGURE 1.8 – La propagation du paquet de requête. [27]

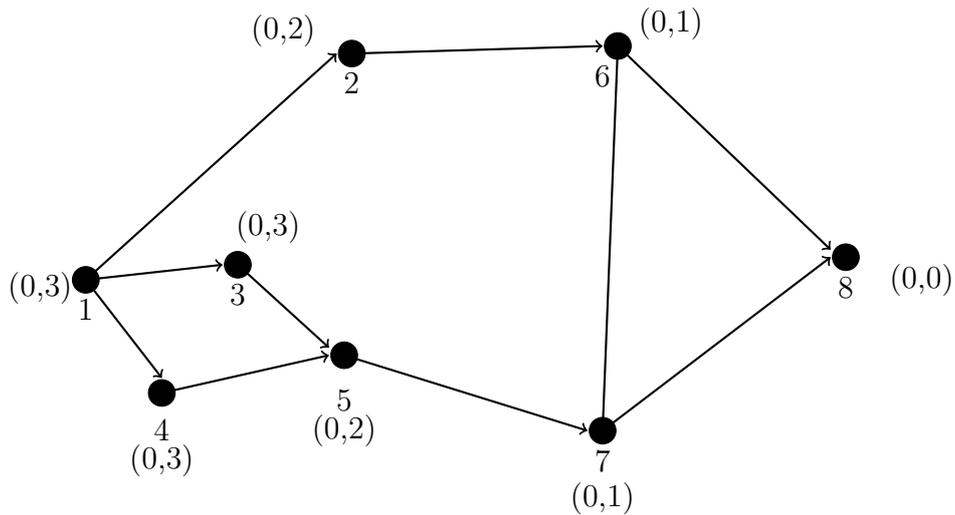


FIGURE 1.9 – (x,y) : (le niveau de référence, la taille du noeud) [27]

▷ La création des routes dans le protocole TORA en se basant sur l'inversement des liens.

- Quand un nœud i détecte une défaillance, i.e. invalidité d'un lien (sachant qu'il ne possède pas de suivants valides vers la destination), il lance un nouveau niveau de référence. L'objectif du nouveau niveau de référence est d'indiquer à la source l'invalidité des chemins rompus.

La figure suivante donne un exemple de ce processus :

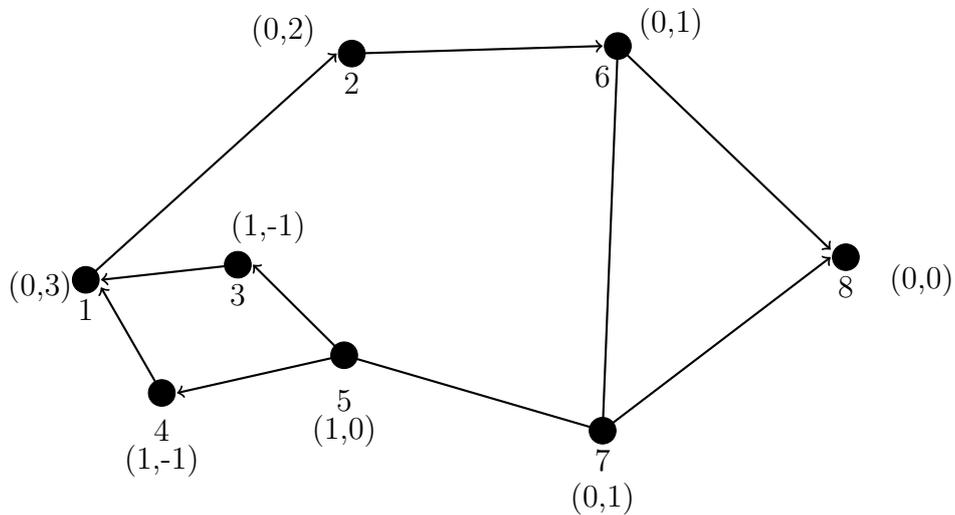


FIGURE 1.10 – La réaction du protocole TORA de la défaillance du lien $(5,7)$ [27]

1.5.1.3 Les protocoles hybrides

Le protocole de routage ZRP (Zone Routing Protocol) est un protocole hybride qui combine les deux approches proactive et réactive. Le protocole ZRP divise le réseau en différentes zones. Pour chaque nœud, il définit une zone de routage exprimée en nombre de sauts maximal σ . Ainsi, la zone de routage d'un nœud inclut tous les nœuds qui sont à une distance au maximum de σ sauts.

Les nœuds qui sont exactement à σ sauts sont appelés nœuds périphériques. À l'intérieur de cette zone, ZRP utilise un protocole proactif et à l'extérieur de cette zone de routage, il fait appel à un protocole réactif. Le protocole proactif est IARP (IntraZone Routing Protocol) et le réactif est celui de l'IERP (IntErzone Routing Protocol).

Chaque nœud doit tout d'abord connaître ses voisins. Pour cela, ZRP utilise soit le protocole de contrôle d'accès au support (MAC) pour connaître les voisins immédiats ou le protocole NDP (NeighbourDiscovery Protocol) pour la transmission et la gestion des échanges de messages HELLO. Par la suite, chaque nœud invoque le protocole IARP pour découvrir les routes vers tous les autres nœuds qui se trouvent dans sa zone de routage. Cependant, le protocole IERP est utilisé à la demande pour chercher les routes entre un nœud et une destination qui se trouvent à l'extérieur de sa zone de routage.

Un troisième protocole BRP (Bordercast Resolution Protocol) est inclus avec IERP pour guider la propagation des requêtes de recherche de route dans le réseau. BRP utilise les données de la topologie fournies par le protocole IARP afin de construire sa liste des nœuds de périphérie et la façon de les atteindre [14].

Routage Proactif		Routage Réactif	
Avantages	Inconvénients	Avantages	Inconvénients
La topologie du réseau est connue de tous les mobiles. Les routes sont disponibles immédiatement.	Il faut diffuser régulièrement des informations sur les changements de topologie du réseau.	Les nœuds mobiles ne conservent pratiquement aucune information sur la topologie globale du réseau, seules les informations sur les routes actives sont stockées	
Les protocoles proactifs disposent en permanence d'une route pour chaque destination dans le réseau	Un volume de signalisation important	Les protocoles réactifs génèrent à priori un volume très faible de signalisations	Les protocoles réactifs engendrent un délai lors de la construction (ou la reconstruction) des routes et produisent plus difficilement des routes optimales

TABLE 1.1 – Comparaison entre protocoles proactifs et protocoles réactifs

1.5.2 Les protocoles de routage basés sur la localisation (géographiques)

Les protocoles de routage géographiques sont les plus adaptés pour les réseaux Ad-hoc mobiles, puisque le mécanisme de routage se base sur les données géographiques des nœuds.

Les nœuds découvrent les informations (totales ou partielles) sur la topologie en échangeant des messages d'état. Ces informations guident ensuite les décisions de routage.

Le routage basé sur la localisation (ou routage géographique) est très efficace pour les réseaux de grande taille et avec un rythme important de changement de topologie.

Chaque nœud connaît sa position en utilisant un service de localisation et connaît celles des autres par échange de messages.

On peut citer dans ce qui suit, quelques-uns des protocoles géographiques les plus célèbres et utilisés :

■ Le Protocole LAR (Location-Aided Routing) [34]

- Optimisation de protocole réactif pour minimiser le surcoût de l'inondation.
- LAR réduit le nombre de messages en limitant la zone de diffusion de requêtes.
- Les informations de localisation obtenues grâce à une requête antérieure sont utilisées pour estimer la localisation du destinataire.
- Le service de localisation ne fait pas partie du protocole LAR (point faible).
- La source diffuse sa requête à ses voisins, requête incluant son estimation de la location du destinataire et sa distance estimée par rapport au destinataire.
- Chaque nœud X qui reçoit la requête calcule sa distance par rapport au destinataire. S'il est plus proche de la destination que la source, il relaie la requête à ses voisins en remplaçant la distance source-destination par X-destination dans la requête.
- Le destinataire D qui reçoit une requête renvoie une réponse au nœud qui a relayé la requête. La réponse contient la position actuelle de D et son temps courant, il peut aussi envoyer des informations sur sa vitesse et direction.
- Connaissance de localisation → Meilleure redirection des requêtes

■ Le protocole GyTAR

Le protocole de routage GyTAR (improved Greedy Traffic-Aware Routing protocol) est un protocole de routage géographique basé sur la localisation (position) et adapté aux réseaux mobiles capable de trouver des chemins robustes. L'objectif de ce protocole est de router les données de proche en proche en considérant les différents facteurs spécifiques à ce genre d'environnements/réseaux. Ce protocole suppose que chaque véhicule connaît sa position courante et ceci grâce au GPS. De plus un nœud source est sensé connaître la position du destinataire pour pouvoir prendre des décisions de routage, cette information est donnée par un service de localisation tel que GLS (Grid Location Service) et peut déterminer la position des intersections voisines à travers des cartes numériques [25].

■ Le protocole GPSR

Le protocole de routage GPSR (Greedy Perimeter Stateless Routing)[20] est donc un protocole de routage basé sur la position, qui contient deux parties. La première correspond à une méthode de choix du prochain nœud transmetteur qui aura le rôle de retransmettre les paquets, et cela tout en se basant sur les informations de position des voisins (nœuds candidats) et de la destination des paquets. Cette méthode consiste à choisir le candidat qui est à une distance la plus proche à vol d'oiseau de la destination. La deuxième partie de GPSR est en fait une méthode pour contourner les obstacles et les zones géographiques vides, qui ne présentent aucun candidat transmetteur dans le voisinage [20].

1.6 La gestion de mobilité dans les réseaux Ad-hoc

Au cours de ces dernières années, de nombreux modèles de mobilité ont été proposés dans la littérature scientifique afin de simuler le comportement des nœuds en essayant de reproduire le plus fidèlement possible les conditions du fonctionnement réel du protocole de routage pour que les résultats et performances soient pertinents.

On distingue deux grandes familles de modèles de mobilité, la classe des modèles individuels qui est composée à son tour des modèles avec mémoire et des modèles sans mémoire et il y a la deuxième classe qui est celle des modèles de groupe.

1.6.1 Les modèles individuels

Dans ces modèles, chaque nœud se déplace indépendamment des autres. Ces modèles peuvent être classés selon l'aspect aléatoire de leur mouvement, soit un mouvement absolument aléatoire sans aucune mémoire du passé, soit un mouvement souple où les variations de la vitesse, direction et position à chaque instant sont fonction de l'état précédent [10].

1.6.1.1 Les modèles sans mémoire

Dans ces modèles, un nœud choisit une position et une vitesse d'une façon absolument aléatoire et sans aucune mémoire du passé. Dans ces modèles, on peut avoir fréquemment des comportements extrêmes des nœuds comme un arrêt soudain, une accélération soudaine et des tours brutaux. Les modèles existants dans cette catégorie sont [10] :

1. Le Random Walk (RW)

il a été introduit pour la première fois par Einstein en 1926 en tant qu'approximation du mouvement aléatoire des particules. Dans ce modèle, le vecteur vitesse de chaque nœud mobile est défini par sa norme et sa direction. Ce vecteur est modifié périodiquement et la nouvelle valeur de ses paramètres est choisie uniformément sur $[V_{\min}, V_{\max}]$ pour la vitesse et $]0, 2\pi]$ pour la direction. V_{\min} et V_{\max} sont deux constantes représentant respectivement la vitesse minimale et maximale à laquelle un mobile peut se déplacer. Bien qu'à l'origine, ce modèle n'était pas prévu pour décrire le déplacement de nœuds mobiles dans un réseau Ad-hoc, de nombreux travaux l'utilisent et étudient son influence sur les protocoles de communication [15].

2. Le modèle Random WayPoint (RWP)

Dans ce modèle, la mobilité des nœuds est typiquement aléatoire et tous les nœuds mobiles sont distribués uniformément dans l'espace de simulation. Afin de modéliser la trajectoire d'un nœud mobile, RWP prévoit trois paramètres : sa destination, sa vitesse et son temps de pause. Le changement de vecteur vitesse est événementiel : il survient à chaque fois qu'un mobile atteint sa destination, avec un temps de pause entre chaque déplacement. L'algorithme RWP consiste à :

- Placer un certain nombre de nœuds mobiles dans un espace de simulation (une zone carrée).
- Affecter une position de coordonnées (x,y) , une vitesse de déplacement, et une destination initiale à atteindre pour chaque mobile.
- Faire repartir vers chaque mobile une autre destination choisie aléatoirement avec une nouvelle vitesse après un éventuel temps de pause et à chaque fois que les mobiles atteignent leur destination dans le carré.
- Répéter le même processus.

Il existe des points de ressemblances et de différences entre les deux modèles de mobilité RW et RWP. La principale différence entre ces deux modèles est la fréquence des changements des vecteurs vitesse qui est périodique avec RW et événementielle avec RWP. Par contre, la norme du vecteur vitesse est identique pour les deux modèles, et choisie uniformément sur $[V_{min}, V_{max}]$. La direction est choisie sur l'intervalle $]0, 2\pi[$ pour les deux modèles, mais dans RW, elle est définie uniformément, en revanche dans RWP, elle est déterminée par sa destination [3].

3. Le modèle Random Direction(RD)

Le Random Direction a été créé pour éviter l'effet de concentration des nœuds au centre produit par le Random Waypoint. Dans ce modèle, chaque nœud choisit aléatoirement, comme dans le Random Walk, une direction qui est un angle entre 0 et 2π et une vitesse entre V_{min} et V_{max} . La différence entre ce modèle et le Random Walk est qu'ici le nœud ne voyage pas pendant un certain temps ou d'une certaine distance mais se déplace suivant la direction choisie jusqu'à atteindre le bord de la surface de simulation où il prend un temps de repos. Une fois le temps de pause terminé, le nœud choisit de nouveau et aléatoirement une nouvelle direction et une nouvelle vitesse et répète le même processus [15].

4. Le modèle Restricted Random Waypoint

L'idée de ce modèle de mobilité est extraite du fait que la plupart des gens se déplacent pour un certain temps dans une même localité avant d'aller vers une autre localité. Donc dans ce modèle, la surface de simulation contient des rectangles qui représentent des villes liées par des autoroutes. Chaque nœud utilise le Random Waypoint pour se déplacer dans l'une des villes un certain nombre de fois spécifiées par un paramètre, avant de voyager vers une autre ville où il va se déplacer pour un certain moment et ainsi de suite [23].

1.6.1.2 Les modèles avec mémoire

Dans ces modèles, appelés aussi corrélés, la vitesse et la direction à chaque instant, dépendent de l'instant précédent. Les modèles corrélés existants sont [10] :

1. Le modèle de Boundless

Dans ce modèle la position et la vitesse d'un nœud à tout instant $(t+At)$, dépendent de la position et de la vitesse à l'instant t . La position (x,y) du mobile et sa vitesse i sont mises à jour chaque At unité de temps comme suit [6]

$$v(t + At) = \min[\max(v(t) + Av, 0), Vmax]$$

$$\theta(t + At) = \theta(t) + A\theta$$

$Vmax$: La vitesse maximale.

Av : Le changement de vitesse distribuée uniformément entre $[-Amax*At, Amax*At]$

$Amax$: Accélération maximale qu'un nœud peut avoir.

$A\theta$: La variation de la distribution, distribuée uniformément entre $[-a* At, a* At]$ a : Valeur maximale du changement d'angle qu'un nœud peut avoir.

Le Boundless a un effet de bord différent des modèles déjà cités. Un nœud qui atteint le bord, continue pour sortir et rentrer de l'autre coté de la surface de simulation.

A cause de cet effet de bord, les nœuds dans ce modèle, se déplacent comme si les bords de la simulation n'existaient pas. L'action d'un nœud qui sort et rentre de l'autre côté, est semblable à celle d'un nœud qui sort définitivement de la simulation avec un nouveau qui arrive en même temps pour le remplacer.

2. Le modèle de Gauss Markov

Dans ce modèle, le temps est discrétisé en intervalles de durée constante. A chaque instant t , un nouveau vecteur vitesse, noté v_t , est choisi. Le nom de ce modèle fait référence aux deux propriétés que possède le processus à l'origine du vecteur vitesse des mobiles. Ce processus est en effet markovien car son état futur ne dépend pas des états passés mais uniquement de son état présent. Il contient également une composante gaussienne car pour pouvoir introduire une modification entre deux valeurs consécutives, ce processus fait intervenir une distribution normale. L'expression du vecteur vitesse dans un espace à deux dimensions est définie par :

$$v_x^{t+1} = \alpha v_x^t + (1 - \alpha)\mu_x + \sigma_x \sqrt{1 - \alpha^2} w_x^t$$

$$v_y^{t+1} = \alpha v_y^t + (1 - \alpha)\mu_y + \sigma_y \sqrt{1 - \alpha^2} w_y^t$$

où $\mu = [\mu_x, \mu_y]$ représente le vecteur vitesse moyen et $\sigma = [\sigma_x, \sigma_y]$ son écart type. $w = [w_x, w_y]$ représente le vecteur d'un processus gaussien normalisé $N(0,1)$.

Le vecteur vitesse à un instant $t + 1$, v^{t+1} , dépend donc à la fois de sa vitesse à l'instant t , v^t , mais également d'une composante totalement indépendante : w^t .

La constante $\alpha \in [0, 1]$ permet d'établir le niveau de dépendance temporelle du vecteur vitesse. Plus ce facteur est élevé, plus le vecteur vitesse à l'instant $t + 1$ est proche de celui à l'instant t . Lorsque $\alpha = 1$, le modèle Gauss-Markov devient un modèle fluid-flow caractérisé par un vecteur vitesse constant.

Au contraire plus ce facteur est faible et plus les fluctuations du vecteur vitesse sont importantes. Lorsque $\alpha = 0$, il n'existe plus aucune dépendance avec le mouvement précédent. La trajectoire des mobiles est alors la même que pour le modèle Random-Walk.

3. Le modèle de Markovian Random Path

Le Markovian Random Path, appelé aussi A Probabilistic Version of Random Walk, utilise une chaîne de Markov pour modéliser le mouvement d'un nœud. La chaîne de Markov est une suite de variables aléatoires (X_n) telle que, pour chaque n , X_{n+1} soit indépendante de X_k , pour $k = n-1$, et dépend uniquement de X_n . Dans ce modèle, les mouvements des nœuds sont séparés en directions horizontales et verticales, chaque direction représentant une variable aléatoire.

1.6.2 Les modèles de groupes

Dans les modèles préalablement cités, un nœud se déplace indépendamment des autres nœuds. Sa vitesse, position et direction de mouvement ne sont pas affectées par d'autres nœuds. Ces modèles individuels ne sont capables de capturer que certains scénarios. Dans quelques applications comme les secours en cas de désastre ou les champs de bataille, la collaboration d'équipe existe, les membres d'une équipe suivent leur chef et les mouvements d'un membre peuvent être influencés par les membres du voisinage. Nous avons donc besoin des modèles de groupe pour simuler certains scénarios.

Dans un modèle de groupe, les nœuds se déplacent ensemble comme un groupe de soldats par exemple qui a une certaine mission à accomplir. Les modèles de groupe qui existent sont les suivants :

1. Le modèle exponentiel aléatoire corrélé

Dans ce modèle, le mouvement de chaque groupe est contrôlé indépendamment des autres groupes. A chaque étape de temps, un groupe se déplace d'une distance aléatoire dans une direction aléatoire. Chaque nœud change ses coordonnées polaires, qui sont une distance et un angle.

2. Le modèle de mobilité de colonne :

Dans ce modèle, chaque groupe de nœuds, peut avoir une ou plusieurs références. Une référence est un nœud du groupe qui a pour rôle de guider les autres nœuds pendant leur déplacement. Au début de la simulation, les références de chaque groupe sont placées d'une façon formant une colonne et chaque nœud est placé en relation avec sa référence, autour de laquelle, il a le droit de se déplacer en utilisant l'un des modèles de mobilité par entité. Une référence peut avoir un seul nœud autour d'elle.

La position de l'axe des références change de la manière suivante.

Nouvelle position = ancienne position + vecteur anticipé.

Le vecteur anticipé est calculé suivant un angle aléatoire entre 0 et π radian (puisque le déplacement est seulement en avant) et une distance aléatoire [32].

3. Le modèle de mobilité de communauté nomade (NCMM)

Dans ce modèle, chaque groupe de noeuds possède un seul point référence en commun. Les noeuds de chaque groupe se déplacent autour de leur point référence en utilisant un modèle de mobilité par entité (Random Walk) et ne peuvent pas la dépasser d'une certaine distance, précisée dans les paramètres, et qui est la distance maximum entre un noeud et sa référence. Le déplacement d'une référence se fait aussi suivant un modèle singulier.

Quand le point de référence change, tous les noeuds mobiles dans le groupe se déplacent vers le nouveau secteur défini par le point de référence et commencent à errer autour du nouveau point de référence [32].

4. Le modèle de mobilité de poursuite [15]

Le modèle de mobilité de poursuite contient, comme Nomadic Community, un seul point de référence. La différence est que la référence joue ici le rôle d'une cible qui est poursuivie par les autres noeuds, comme le mouvement d'un groupe de policiers essayant d'attraper un voleur. La position de chaque noeud dans le groupe varie de la manière suivante :

Nouvelle position = position ancienne + accélération (cible) + vecteur aléatoire. Accélération (cible) est une information sur le déplacement de la cible et le vecteur aléatoire est le mouvement d'un noeud selon un modèle de mobilité singulier (Random Walk par exemple). Ce mouvement est limité puisqu'il s'agit de poursuivre la cible sans la dépasser.

5. Le modèle de mobilité d'un groupe avec point de référence(RPGM) [32]

Le modèle de mobilité d'un groupe avec point de référence noté RPGM (Referenced Point Group Mobility Model) représente le mouvement aléatoire d'un groupe de noeuds aussi bien que le mouvement aléatoire de chaque noeud individuellement dans le groupe. Les mouvements du groupe sont basés sur le chemin parcouru par un centre du groupe qui est utilisé pour calculer le mouvement du groupe par l'intermédiaire d'un vecteur de mouvement GM qui peut être choisi aléatoirement ou être prédéfini.

Le mouvement du centre du groupe caractérise complètement le mouvement de son groupe (la direction et la vitesse). Les noeuds individuels se déplacent aléatoirement par rapport à leurs propres points de référence prédéfinis, dont les mouvements dépendent du mouvement du groupe.

Le modèle RPGM utilise le vecteur GM pour calculer les nouveaux points de référence, RP ($t + 1$), à l'instant $t + 1$. La nouvelle position de chaque noeud est alors calculée par la somme vectorielle du vecteur GM avec un vecteur aléatoire de mouvement, RM.

La longueur de RM est uniformément distribuée dans un disque qui a pour centre RP ($t + 1$), tandis que sa direction est uniformément distribuée dans $[0.. 2]$.

Le modèle RPGM a été conçu pour faire face à des scénarios tels qu'une avalanche après laquelle une équipe de secours se composant d'humains et de chiens, travaillent en coopération.

Les guides humains (centre des groupes) tendent à définir un chemin général puisqu'ils connaissent habituellement l'endroit approximatif des victimes. Chacun des chiens crée son propre chemin aléatoire autour du secteur général choisi par leurs guides humains.

1.7 Conclusion

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'urgences ou de travaux temporaires dont les autres réseaux qui peuvent engendrer des frais importants. Cependant de nouveaux problèmes apparaissent.

Dans ce contexte, une identification des défaillances appliquée aux réseaux Ad-hoc s'impose afin de rechercher et d'exploiter les informations relatives aux évènements non souhaités, les prendre en considération, afin de proposer des solutions pour obtenir un système plus fiable.

Chapitre 2

La sûreté de fonctionnement

Sommaire

2.1	Introduction	26
2.2	La sûreté de fonctionnement	26
2.2.1	Principe	26
2.2.2	Méthodes d'analyse de sûreté de fonctionnement	27
2.3	Défaillances d'un réseau informatique sans fil	27
2.3.1	La consommation d'énergie	27
2.3.2	L'interception de données	29
2.3.3	Les interférences	30
2.3.4	Congestion dans un réseau	31
2.4	Les problèmes de mobilité	32
2.5	Conclusion	33

2.1 Introduction

Le domaine des réseaux et ses applications impliquent des exigences de fonctionnement sûres et l'identification des défaillances s'avère fondamentale pour garantir un système fiable.

Dans ce contexte, une analyse entrant dans le cadre de la sûreté de fonctionnement s'impose, afin d'identifier les causes et les conséquences des défaillances, le principal objectif est d'atteindre "le Graal" du système : zéro accident, zéro arrêt, zéro défaut, zéro maintenance, pour y arriver, des mesures et diverses méthodes d'analyse des défaillances ont été mises en place.

Nous présentons dans ce chapitre une brève définition du concept de sûreté de fonctionnement ainsi que les principales méthodes de résolution pour finir avec un recensement des différents types de défaillances qui peuvent toucher un réseau Ad-hoc et porter préjudice à son bon fonctionnement.

2.2 La sûreté de fonctionnement

Elle est apparue comme une étant une nécessité au cours XXème siècle, notamment avec la révolution industrielle et technologique.

2.2.1 Principe

Elle est par définition considérée comme étant la science des défaillances et des pannes, c'est une notion générique qui mesure la qualité de service délivrée par un système, de manière à ce que l'utilisateur ait en lui une confiance justifiée. Cette confiance justifiée s'obtient à travers une analyse qualitative et quantitative des différentes propriétés du service délivré par le système. Elle a pour but d'aider à la décision en [18] :

- Comprenant et identifiant les risques.
- Optimisant l'architecture et comparant des solutions différentes.
- Optimisant les moyens de soutien en comparant des solutions.
- Justifiant les choix de façon rationnelle et démontrée.

La sûreté de fonctionnement est mesurée par les grandeurs probabilistes associées **FDMS** pour Fiabilité, Disponibilité, Maintenabilité et Sécurité [18].

- **La Fiabilité** : caractérise l'aptitude d'un système ou d'un matériel à accomplir une fonction requise dans des conditions données pendant un intervalle de temps donné.
- **La Maintenabilité** : est l'aptitude d'un bien, dans des conditions données à être maintenu ou rétabli dans un état où il peut accomplir une fonction requise en utilisant des procédures et des moyens prescrits.
- **La Disponibilité** : C'est l'aptitude d'un dispositif à remplir ou à être en état de remplir une fonction à un instant donné, en alliant les notions de Fiabilité et de Maintenabilité et de la logistique de maintenance.
- **La Sécurité** : c'est l'aptitude d'un système à ne pas générer, dans des conditions données, des événements critiques ou catastrophiques.

2.2.2 Méthodes d'analyse de sûreté de fonctionnement

Une analyse prévisionnelle de sûreté de fonctionnement est un processus d'étude d'un système réel de façon à produire un modèle abstrait du système relatif à une caractéristique de sûreté de fonctionnement (Fiabilité, Disponibilité, Maintenabilité, Sécurité). Les éléments de ce modèle seront des événements susceptibles de se produire dans le système et son environnement [26], tels par exemple :

- Des défaillances et des pannes des composants du système.
- Des événements liés à l'environnement.
- Des erreurs humaines en phase d'exploitation. Le modèle permet ainsi de représenter toutes les défaillances et les pannes des composants du système qui compromettent une des caractéristiques de SdF.

Afin d'aider l'analyste, plusieurs méthodes d'analyse ont été mises au point. Les principales étant :

- **APD/APR** : Analyse Préliminaire des Dangers/Défaillances/Risque,
- **AMDE** : Analyse des Modes de Défaillances et de leurs Effets.
- **HAZOP** : HAZard and OPerabilitystudy.
- **MDS** : Méthode du Diagramme de Succès.
- **MTV** : Méthode de la Table de Vérité.
- **MAC** : Méthode de l'Arbre des Causes.
- **MCPR** : Méthode des Combinaisons de Pannes Résumées.
- **MACQ** : Méthode de l'Arbre des Conséquences.
- **MDCC** : Méthode du Diagramme Causes-Conséquences.
- **MEE** : Méthode de l'Espace des Etats.

Nous avons décidé d'opter pour une simple identification des défaillances pour recenser les types de pannes qui peuvent affecter un réseau informatique Ad-hoc. Mais avant de procéder, il faut savoir qu'est-ce qu'une défaillance : C'est une cessation de l'aptitude d'une entité à accomplir une fonction requise ou à fonctionner comme prévu dans un temps donné et dans des conditions données.

2.3 Défaillances d'un réseau informatique sans fil

2.3.1 La consommation d'énergie

Les nœuds-capteurs sont alimentés principalement par des batteries. En outre, ils doivent le plus souvent avoir une durée de vie de l'ordre de plusieurs mois, voire de quelques années, puisque le remplacement des batteries n'est pas envisageable pour des réseaux de taille importante, avec des milliers de nœuds [30].

2.3.1.1 Facteurs de dissipation d'énergie

Différents facteurs peuvent provoquer la dissipation de l'énergie d'un nœud-capteur. Cette dissipation d'énergie se fait de manière générale selon plusieurs modes [30] :

- **Le MCU** : Généralement les MCUs possèdent divers modes de fonctionnement : actif, "idle", et sommeil, à des fins de gestion d'énergie. Chaque mode est caractérisé par une quantité différente de consommation d'énergie. Toutefois, la transition entre les modes de fonctionnement implique un surplus d'énergie et de latence. Ainsi, les niveaux de consommation d'énergie des différents modes, les coûts de transition entre les modes mais encore le temps passé par le MCU dans chaque mode ont une incidence importante sur la consommation totale d'énergie d'un nœud-capteur.
- **La radio** : la radio opère dans quatre modes de fonctionnement : émission, réception, "idle", et sommeil. Une observation importante dans le cas de la plupart des radios est que le mode "idle" induit une consommation d'énergie significative, presque égale à la consommation en mode réception. Ainsi, il est plus judicieux d'éteindre complètement la radio plutôt que de passer en mode "idle" quand l'on a ni à émettre ni à recevoir de données. Un autre facteur déterminant est que, le passage de la radio d'un mode à un autre engendre une dissipation d'énergie importante due à l'activité des circuits électroniques. Par exemple, quand la radio passe du mode sommeil au mode émission pour envoyer un paquet, une importante quantité d'énergie est consommée pour le démarrage de l'émetteur lui-même.
- **Le détecteur ou le capteur proprement dit** : il y a plusieurs sources de consommation d'énergie par le module de détection, notamment l'échantillonnage et la conversion des signaux physiques en signaux électriques, le conditionnement des signaux et la conversion analogique-numérique. Étant donné la diversité des capteurs, il n'y a pas de valeurs typiques de l'énergie consommée. En revanche, les capteurs passifs (température, sismiques, ...) consomment le plus souvent peu d'énergie par rapport aux autres composants du nœud-capteur. A noter, que les capteurs actifs tels que les sonars, les capteurs d'images, etc. peuvent consommer beaucoup d'énergie.

En outre, il existe d'autres formes de dissipation d'énergie telles que les lectures et les écritures mémoire.

Un autre aspect non négligeable est le phénomène d'auto-décharge de la batterie. En effet, cette dernière se décharge d'elle-même et perd de sa capacité au fil du temps en ou encore suite aux effets de la mobilité.

2.3.1.2 Sources de surconsommation d'énergie

Nous appelons surconsommation d'énergie [30] toute consommation inutile que l'on peut éviter afin de conserver l'énergie d'un nœud-capteur. Les sources de cette surconsommation sont nombreuses. Certains de ces phénomènes sont les causes majeures de la perte d'énergie et on peut brièvement les recenser comme suit :

- **Les collisions** : elles sont la première source de perte d'énergie. Quand deux trames sont émises en même temps et se heurtent, elles deviennent inexploitables et doivent être abandonnées. Les retransmettre par la suite, consomme de l'énergie. Tous les protocoles MAC

essayent à leur manière d'éviter les collisions. Les collisions concernent plutôt les protocoles MAC avec contention.

- **L'écoute à vide (idle-listening)** : un nœud dans l'état "idle" est prêt à recevoir un paquet, mais il n'est pas actuellement en train de recevoir quoi que ce soit. Ceci est coûteux et inutile dans le cas des réseaux à faible charge de trafic. Plusieurs types de radios présentent un coût en énergie significatif pour le mode "idle". Éteindre la radio est une solution, mais le coût de la transition entre les modes consomme également de l'énergie, la fréquence de cette transition doit alors rester "raisonnable".
- **L'écoute abusive (overhearing)** : cette situation se présente quand un nœud reçoit des paquets qui ne lui sont pas destinés. Le coût de l'écoute abusive peut être un facteur dominant de la perte d'énergie quand la charge de trafic est élevée et la densité des nœuds grande.
- **L'overhead des paquets de contrôle** : l'envoi, la réception, et l'écoute des paquets de contrôle consomment de l'énergie. Comme les paquets de contrôle ne transportent pas directement des données, ils réduisent également le débit utile effectif.

2.3.2 L'interception de données

Par défaut un réseau sans fil est non sécurisé, c'est-à-dire qu'il est ouvert à tous et que toute personne se trouvant dans le rayon de portée d'un point d'accès peut potentiellement écouter toutes les communications circulant sur le réseau. Pour un particulier, la menace est faible car les données sont rarement confidentielles, si ce n'est les données à caractère personnel. Pour une entreprise en revanche l'enjeu stratégique peut être très important. Dans ce qui suit [12], nous allons citer les différents types de failles qui peuvent permettre à un intrus de dérober et intercepter les données circulant au sein d'un réseau :

2.3.2.1 L'intrusion réseau

Lorsqu'un point d'accès est installé sur le réseau local, il permet aux stations d'accéder au réseau filaire et éventuellement à internet si le réseau local y est relié. Un réseau sans fil non sécurisé représente de cette façon un point d'entrée royal pour le pirate au réseau interne d'une entreprise ou une organisation.

Outre le vol ou la destruction d'informations présentes sur le réseau et l'accès à internet gratuit pour le pirate, le réseau sans fil peut également représenter une aubaine pour ce dernier dans le but de mener des attaques sur Internet. En effet étant donné qu'il n'y a aucun moyen d'identifier le pirate sur le réseau, l'entreprise ayant installé le réseau sans fil risque d'être tenue responsable de l'attaque.

2.3.2.2 Le brouillage radio

Les ondes radio sont très sensibles aux interférences, c'est la raison pour laquelle un signal peut facilement être brouillé par une émission radio ayant une fréquence proche de celle utilisée dans le réseau sans fil. Un simple four à micro-ondes peut ainsi rendre totalement inopérable un réseau sans fil lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.

2.3.2.3 Les dénis de service

La méthode d'accès au réseau de la norme 802.11 est basée sur le protocole CSMA/CA, consistant à attendre que le réseau soit libre avant d'émettre. Une fois la connexion établie, une station doit s'associer à un point d'accès afin de pouvoir lui envoyer des paquets. Ainsi, les méthodes d'accès au réseau et d'association étant connues, il est simple pour un pirate d'envoyer des paquets demandant la désassociation de la station. Il s'agit d'un déni de service, c'est-à-dire d'envoyer des informations de telle manière à perturber volontairement le fonctionnement du réseau sans fil.

D'autre part, la connexion à des réseaux sans fils est consommatrice d'énergie. Même si les périphériques sans fils sont dotés de fonctionnalités leur permettant d'économiser le maximum d'énergie, un pirate peut éventuellement envoyer un grand nombre de données (chiffrées) à une machine de telle manière à la surcharger. En effet, un grand nombre de périphériques portables (assistant digital personnel, ordinateur portable, ...) possèdent une autonomie limitée, c'est pourquoi un pirate peut vouloir provoquer une surconsommation d'énergie de telle manière à rendre l'appareil temporairement inutilisable, c'est ce que l'on appelle un déni de service sur batterie.

2.3.3 Les interférences

Les interférences sur le réseau sans fil peuvent se manifester de différentes manières pouvant toutes être résolues si la source des interférences est identifiée. Certains périphériques pouvant causer des interférences sur le réseau sans fil, ainsi que des matériaux structurels, tels que des plans de travail et des murs, pouvant avoir un impact sur le signal sans fil [17].

2.3.3.1 Obstacles physiques

Les sources les plus connues d'interférence sont les obstacles physiques : mur de béton, de briques, de bois, peinture au plomb etc. Mais il n'y a pas que les murs qui nuisent à un bon signal sans fil, le métal, le verre et l'eau sont également nuisibles.

Voici une liste qui indique le niveau potentiel d'interférence en fonction du type d'obstacle.

Type d'obstacle	Potentiel d'interférence
Bois	Faible
Matériaux synthétique	Faible
Verre	Faible
Eau	Moyen
Brique	Moyen
Marbre	Moyen
Enduit	Elevé
Béton	Elevé
Verre blindé	Elevé
Métale	Très Elevé

TABLE 2.1 – Liste des matériaux et leur niveau d'interférence

2.3.3.2 Achalandage du réseau

Le partage du réseau entre différents appareils est aussi source d'interférence. Quand 6 appareils utilisent une même connexion, certains appareils auront une meilleure performance, au détriment des autres appareils connectés.

2.3.3.3 Interférences fréquentielles

Un autre problème qui peut se poser, est quand deux transmissions simultanées utilisent une même fréquence ou des fréquences proches pouvant ainsi interférer l'une avec l'autre. En fait, tous les appareils utilisant une bande de fréquence de 2,4 GHz ou de 5 GHz sont susceptibles d'interférer : téléphone sans fil domestique, haut-parleur sans fil, moniteurs externes et écrans ACL, micro-ondes etc.

2.3.4 Congestion dans un réseau

Les réseaux informatiques sont conçus pour transmettre les données à la vitesse la plus élevée possible. Les protocoles modernes comme TCP savent adapter leur utilisation au gabarit du réseau. En règle générale, ces mécanismes suffisent à garantir la bonne gestion des flux. Il arrive malgré tout qu'une mauvaise conception du réseau ou un évènement imprévu entraînent la surcharge momentanée d'un point précis.

En effet, les problèmes de congestion arrivent lorsque les nœuds d'un réseau saturent leurs files d'attente et donc perdent des paquets. Si ces paquets sont réexpédiés ou si des messages de gestion de réseau se mettent à circuler en grand nombre, les performances du réseau vont s'écrouler très vite [2].

2.3.4.1 Scénario de la congestion du réseau

Une liaison réseau saturée est une liaison qui doit transmettre plus de trames que ne le permet son support physique. Il s'agit par exemple du port d'un routeur qui devrait émettre 110 Mbits/s (mégabits par seconde) quand la norme utilisée est le 100BaseTX (100 Mbps).

A ce stade le routeur commence par placer les paquets surnuméraires dans un tampon local "buffer". Ce tampon est vidé lorsque la saturation se termine et que la liaison permet l'écoulement.

Si la saturation se maintient suffisamment longtemps pour remplir le tampon, le routeur doit se résoudre à ne pas traiter les paquets ("drop"). Il peut éventuellement en informer l'émetteur par divers mécanismes ("TCP ECN" ou "ICMP Congestion detected").

Les routeurs peuvent utiliser des politiques de "Quality of Service" (QOS) pour déterminer quels paquets supprimés en priorité ("best effort"). Les autres paquets sont prioritaires et sont moins concernés par la congestion.

Si la congestion se produit sur un équipement moins performant qu'un routeur (commutateur, hub, firewall ou borne wifi), les résultats sont catastrophiques.

2.3.4.2 Symptômes de la congestion

La congestion se traduit avant tout par un ressenti utilisateur classique : la lenteur. Cet état reflète la variation du débit effectif du réseau, c'est à dire le temps nécessaire pour transmettre l'intégralité d'une donnée d'un point à un autre. Le débit efficace n'existe pas en tant que tel, il se compose dans la réalité de 3 indicateurs distincts :

- la latence.
- la gigue¹.
- le taux de perte.

Il existe de nombreuses études sur l'influence de ces paramètres. En synthèse on peut retenir quelques faits. En premier lieu le débit efficace est inversement proportionnel à la latence. Multiplier la latence par deux revient à diviser le débit par deux. Ensuite la gigue, qui est la variation de la latence dans le temps, impacte le débit en influençant la latence. Enfin le débit théorique est inversement proportionnel à la racine carrée du taux de perte. En résumé lorsqu'une congestion se produit, la latence augmente du fait de l'utilisation des tampons, la gigue augmente pour la même raison et le taux de perte n'est plus nul. Le débit efficace est impacté directement par cet état.

2.4 Les problèmes de mobilité

Une caractéristique particulière aux réseaux Ad-hoc est la variation de leur topologie. Au-delà de la qualité de liaison qui peut être à l'origine de variation (la qualité de transmission est telle que la liaison est considérée comme inexistante) la mobilité des éléments génère des changements de connectivité. Un nœud d'un réseau Ad-hoc se déplace, il peut joindre ou quitter un réseau Ad-hoc à tout moment, c'est-à-dire se retrouver hors de portée d'émission d'un nœud

1. la gigue est la variation de la latence au fil du temps plus précisément, la différence de délai de transmission de bout en bout entre des paquets choisis dans un même flux de paquets, sans prendre en compte les paquets éventuellement perdus

du réseau.

Le protocole de routage, via une procédure de maintenance de routes, est en charge de la gestion de ces changements de topologie. De par sa conception il s'adapte naturellement à ceux-ci

Une adaptation de routage, plus élaborée est requise pour prendre en compte le niveau de mobilité d'un élément de façon à choisir des routes stables, la stabilité de la route pouvant amener un gain de performance. En effet, si une route se rompt, le protocole de routage est à même (si cela est possible) d'en trouver une autre, mais il y aura eu des pertes de données générant une baisse de performances, et donc, en évitant de passer par des routes qui sont peut-être rapides mais de courte durée, le protocole de routage peut alors espérer augmenter son taux de délivrance d'informations. Le problème pour la mise en place de cette adaptation est d'évaluer la stabilité d'un lien, la mobilité d'un élément [22].

2.5 Conclusion

Dans ce chapitre, nous avons mis l'accent sur la sûreté de fonctionnement, cette discipline qui cherche à mesurer la qualité de service délivrée par un système, de manière à ce que l'utilisateur ait en lui une confiance justifiée qui s'obtient à travers une analyse des différentes propriétés du service délivré par le système.

Ensuite, nous avons cité les différentes méthodes et approches d'analyse de défaillances en sûreté de fonctionnement où nous avons appliqué une simple identification des défaillances pour mieux analyser les réseaux Ad-hoc..

Cette analyse nous dysfonctionnelle a permis d'identifier pour notre système les défaillances potentielles, leurs causes, leurs conséquences et les barrières existantes.

Nous présentons dans le chapitre suivant les concepts de base ainsi que les principaux algorithmes utilisés dans notre démarche qui vise à garantir la continuité des communications dans un réseau de capteurs sans fil.

Chapitre 3

Approche et algorithmes

Sommaire

3.1	Introduction	35
3.2	Principe de fonctionnement du protocole GPSR	35
3.2.1	Mode Greedy	35
3.2.2	Mode Perimeter	37
3.2.3	Diagramme de cas d'utilisation	41
3.3	La rencontre des réseaux informatiques et de l'intelligence artificielle	42
3.3.1	Pourquoi le choix des fourmis	42
3.3.2	Relation avec l'informatique	42
3.4	L'algorithme de colonie de fourmis	42
3.4.1	Le Problème du Voyageur de Commerce	43
3.4.2	Principe de l'algorithme de colonie de fourmis "Ant System"	44
3.5	Conclusion	46

3.1 Introduction

Après avoir présenté l'environnement mobile Ad-hoc dans le premier chapitre ainsi que les différents modèles de mobilité nous avons pu effectuer par la suite une identification des défaillances et citer les différents problèmes qui peuvent porter atteinte au bon fonctionnement du réseau et à l'acheminement des paquets.

Le contenu de ce chapitre est consacré à la présentation détaillée du protocole de routage utilisé GPSR ainsi que les algorithmes de base qui ont servi à son implémentation, en plus de l'algorithme de colonie de fourmis qui servira à résoudre un problème d'optimisation combinatoire qui est celui du voyageur de commerce. Ceci a pour but de renforcer le chemin du passage des paquets et d'assurer la continuité de service .

3.2 Principe de fonctionnement du protocole GPSR

Le protocole de routage GPSR (Greedy Forwarding Stateless Routing)[20] est un protocole géographique réactif conçu à l'origine pour les réseaux mobiles Ad-hoc (MANET), il a été adapté par la suite aux réseaux de capteurs sans fils (Wireless Sensor Networks)[20].

Le protocole GPSR utilise les coordonnées des nœuds pour le routage en supposant qu'ils se trouvent sur un même plan.

Les nœuds mobiles au sein d'un tel environnement étant susceptibles de se déplacer ne permettent pas l'adaptation de certains algorithmes de routage qui se basent sur la topologie du réseau ou le processus de découverte des routes pour l'acheminement des paquets. L'acheminement des paquets par GPSR se fait alors selon deux modes : le "**Greedy Forwarding**" et le "**Perimeter Forwarding**".

3.2.1 Mode Greedy

Le principe dans le mode Greedy ou de transmission gloutonne, est que quand un nœud reçoit un paquet, il choisit le voisin le plus proche de la destination pour le lui transmettre en parcourant les nœuds de la source à la destination où chaque nœud qui reçoit un paquet l'achemine en faisant un saut vers le nœud intermédiaire le plus proche de la destination dans sa zone de couverture. Cette technique est répétée de manière récursive jusqu'à ce que le nœud de destination soit atteint.

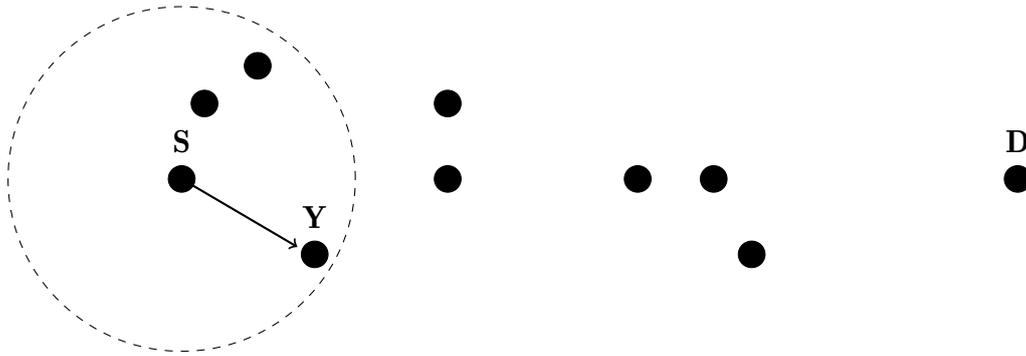


FIGURE 3.1 – Exemple du mode Greedy[20]

Le nœud source **S** reçoit ou génère un paquet destiné au nœud de destination **D**. Le nœud **S** relaye le paquet à **Y**, ce dernier étant le plus proche de la destination que des autres nœuds se trouvant dans la portée de **S** et ainsi de suite. Ce processus de transfert du paquet se répète jusqu'à l'atteinte de la destination **D**.

Algorithme 1 Algorithme Greedy

Algorithme :**Pour** tout $j \in \text{voisin}(i)$ **faire** $Min = \infty$ **Si** $\text{calcul_distance}(j, \text{destination}) < Min$ **alors** $Min = \text{calcul_distance}(j, \text{destination})$ $\text{Meilleur_voisin} = j$ **Fin Si****Fin Pour**

Cet algorithme d'acheminement offre un taux de réussite assez proche des réseaux filaires dans le cas où la mobilité de la destination n'est pas très dynamique.

Cependant, lorsqu'un nœud se trouvant le plus proche de la destination que tous ses voisins mais qu'elle reste inaccessible en un seul saut à cause du déploiement aléatoire, de la présence d'obstacles radio, ou de la défaillance des nœuds, alors le mode Greedy Forwarding échoue, et le mode Perimeter Forwarding est à ce moment là utilisé. La Figure 3.2 montre un exemple de ce problème d'acheminement.

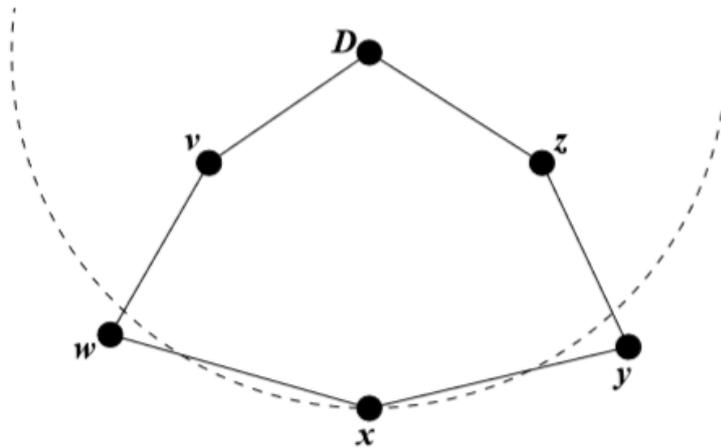


FIGURE 3.2 – Echec du mode Greedy (x est plus proche de D que ses voisins y, w) [20]

3.2.2 Mode Perimeter

L'algorithme du Perimeter Forwarding consiste à transformer la topologie du réseau en un graphe planaire (dont les arêtes ne s'intersectent pas) pour éviter que le périmètre soit parcouru avec une boucle infinie. Ce graphe peut être de type RNG (Relative Neighborhood Graph) ou GG (Gabriel Graph).

Le graphe représentant le réseau Ad-hoc n'est pas généralement planaire. Il est nécessaire donc de construire des sous-graphes planaires, connectés au graphe formé par les nœuds du réseau.

Pour convertir le graphe du réseau en un graphe planaire, il suffit d'enlever les arêtes d'intersection tout en s'assurant que le graphe initial ne présente aucune discontinuité.

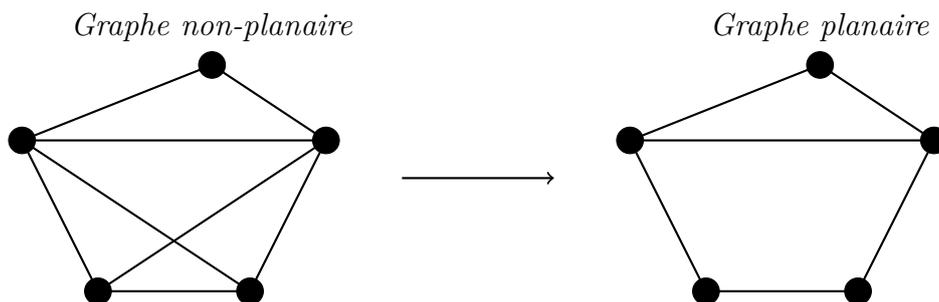


FIGURE 3.3 – Planarisation d'un graphe

Pour cela, deux mécanismes ont été mis en place :

3.2.2.1 Planarisation avec le graphe RNG (Relative Neighbourhood Graph)

Une connection uv existe si :

$$\forall w \neq u, v : d(u, v) \leq \max[d(u, w), d(v, w)]$$

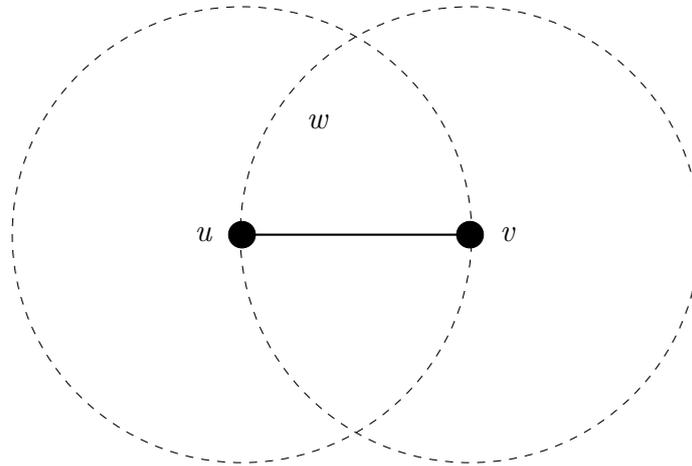


FIGURE 3.4 – Graphe RNG [20]

Algorithme 2 Algorithme RNG

Algorithme :

```

Pour tout  $v \in \text{voisin}(u)$  faire
  Pour tout  $w \in \text{voisin}(u)$  faire
    Si  $\text{distance}(u, v) > \max[\text{distance}(u, w), \text{distance}(v, w)]$  alors
       $\text{Eliminer\_voisin}(v)$ 
    Fin Si
  Fin Pour
Fin Pour

```

3.2.2.2 Planarisation avec le graphe GG (Gabriel Graph)

Une connection **uv** existe entre les sommets u et v si aucun autre sommet w n'est présent dans le cercle dont le diamètre est **uv**.

$$\forall w \neq u, v : d^2(u, v) < [d^2(u, w) + d^2(v, w)] \quad (3.1)$$

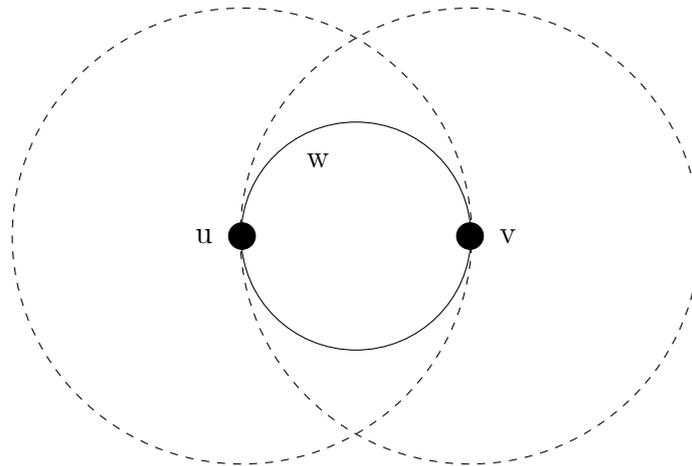


FIGURE 3.5 – Graphe GG [20]

Algorithme 3 Algorithme GG Planaire

Algorithme :

Pour tout $v \in \text{voisin}(u)$ **faire**
 Pour tout $w \in \text{voisin}(u)$ **faire**
 $m = \text{midpoint entre } \vec{uv}$
 Si $\text{distance}(m, w) < \text{distance}(m, u)$ **alors**
 Eliminer_voisin(v)
 Fin Si
 Fin Pour
Fin Pour

Juste après le processus de planarisation, le paquet traverse le graphe jusqu'à atteindre la destination en utilisant "la règle de la main droite". Ce mécanisme implique que lorsqu'un paquet arrive à un nœud X du nœud Y , le chemin à suivre est le prochain qui se trouve dans le sens inverse des aiguilles d'une montre en partant de X et par rapport au segment $[XY]$ tout en évitant les « crossing links »¹ (route déjà parcourue). La figure 3.6 montre un exemple plus précis de ce mode.

1. crossing links = intersection des liens

3.2.3 Diagramme de cas d'utilisation

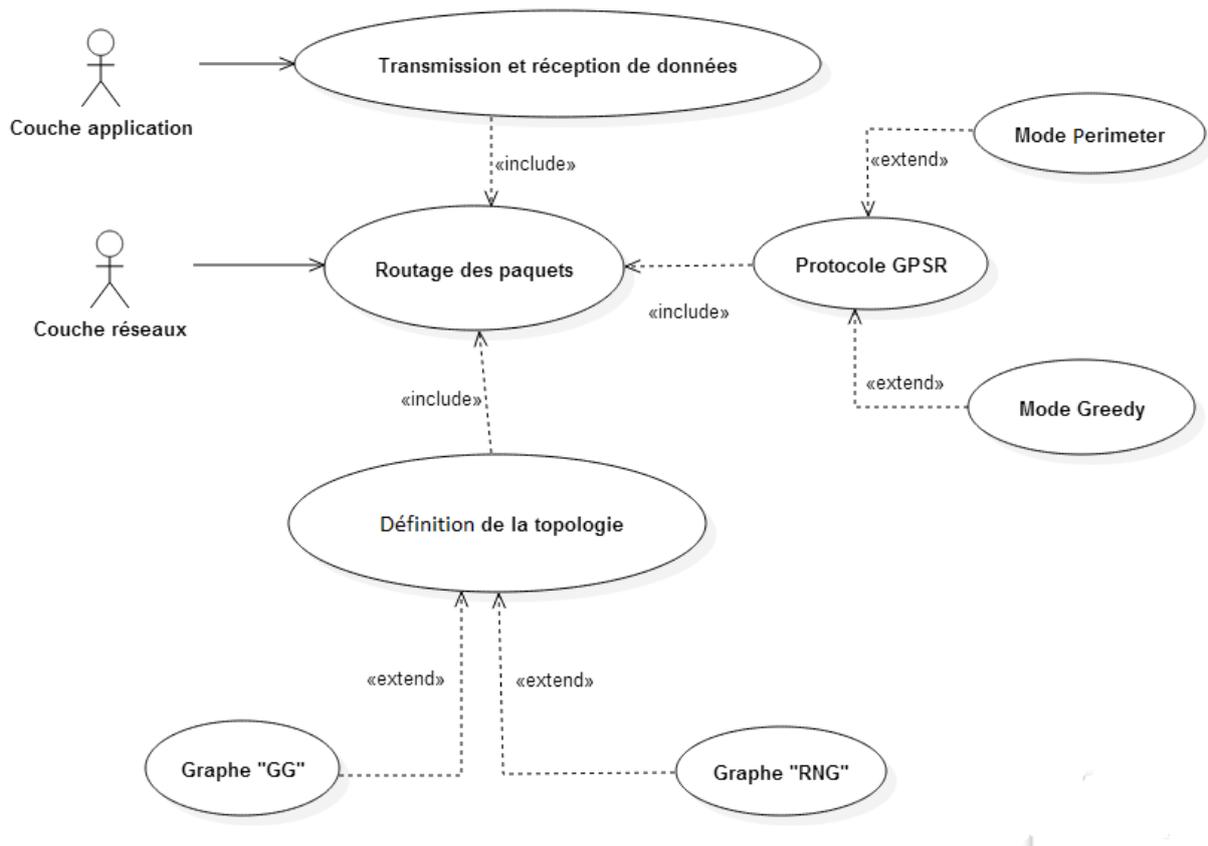


FIGURE 3.8 – Diagramme de cas d'utilisation.

Nous avons vu que le routage avec le protocole GPSR permet à un nœud de choisir le prochain relai en fonction des informations de position de ses voisins et de la destination de façon périodique.

Nous avons choisi de mener notre approche sur cet environnement de routage parce qu'il présente l'avantage et la caractéristique principale à un nœud de récupérer les informations des nœuds voisins par un équipement de positionnement GPS, plutôt que d'obtenir un grand nombre d'informations de routage, mais également de maintenir une table de voisinage ainsi qu'une table de routage.

Toutefois, dans un environnement mobile comme c'est le cas pour les réseaux Ad-hoc la transmission du paquet n'est pas chose aisée à cause du changement dynamique et fréquent de la topologie. Nous avons alors décidé d'avoir recours à une méthode méta-heuristique inspirée de la nature et relevant du domaine de la bio-informatique et de l'intelligence artificielle pour assurer la continuité de service et la transmission des paquets jusqu'à destination.

3.3 La rencontre des réseaux informatiques et de l'intelligence artificielle

Dès la conception des premiers réseaux informatiques, les scientifiques se sont intéressés à emprunter des comportements observés dans la nature. Initialement, cette coopération avait pour but d'aider les biologistes dans leur travail quotidien, mais elle s'est renforcée par la suite pour transmettre une partie des découvertes fondamentales en produits informatiques concrets comme la reconnaissance digitale, mais également de s'inspirer du comportement social de certaines espèces pour améliorer les recherches et les techniques informatiques.

De cette collaboration entre les deux sciences sont nés de nouveaux domaines comme la bio-informatique et les bio-technologies, où les méthodes algorithmiques de l'informatique et le savoir des biologistes se sont entremêlés, pour donner naissance à un mélange des vocabulaires et d'approches entre les deux domaines bien que complètement opposés en apparence.

3.3.1 Pourquoi le choix des fourmis

Le comportement des fourmis est un comportement collectif. Chaque fourmi a pour priorité le bien être de la communauté. Chaque individu de la colonie est à priori indépendant et n'est pas supervisé d'une manière ou d'une autre. Ce concept est appelé Hétéarchie (s'opposant à la Hiérarchie), chaque individu est aidé par la communauté dans son évolution et en retour il aide au bon fonctionnement de celle-ci. La colonie est donc autocontrôlée grâce à de mécanismes relativement simples à étudier. En se basant sur les travaux existants, nous contribuons à l'étude des fourmis du point de vue de la découverte de connaissances, avec comme objectif de résoudre des problèmes réels qui se sont posés lors de l'implémentation du protocole GPSR dans un environnement mobile.

3.3.2 Relation avec l'informatique

Les études préalables ont permis d'observer une colonie de fourmis à la recherche de nourriture, Il en a été déduit qu'elles arrivaient à résoudre des problèmes tels que celui de la recherche du plus court chemin. Des problèmes assez complexes en soi, par des mécanismes simples à comprendre et à modéliser. La simulation de leur comportement par des algorithmes devient alors chose aisée [8].

3.4 L'algorithme de colonie de fourmis

Un algorithme de colonies de fourmis est un algorithme itératif à population où tous les individus partagent un savoir commun qui leur permet de guider leurs futurs choix et d'indiquer aux autres individus des directions à suivre ou au contraire à éviter.

Cette méthode a pour but de construire les meilleures solutions à partir des éléments qui ont été explorés par d'autres individus. Chaque fois qu'un individu découvre une solution au problème, bonne ou mauvaise, il enrichit la connaissance collective de la colonie. Ainsi, chaque fois qu'un nouvel individu aura à faire des choix, il pourra s'appuyer sur la connaissance collective pour pondérer ses choix [24].

Un risque apparaît lorsqu'un chemin non optimal est marqué. En effet, les fourmis qui s'en trouveront à proximité seront tentées d'y passer augmentant encore le niveau de phéromone de ce chemin. Pour diminuer le risque d'enfoncer la colonie dans un minimum local du problème, on pourra prendre soin de diminuer automatiquement le niveau de phéromone de tout le système, pour rehausser l'intérêt des autres chemins qui pourraient faire partie de la solution optimale. Ce paramètre, correspondant au taux d'évaporation des phéromones, est l'un des paramètres principaux de l'algorithme [33].

De la même manière, aucun chemin ne devra être inondé de phéromones et aucun chemin ne devra être totalement invisible, on pourra donc aussi contrôler le niveau de phéromone de chaque chemin pour le maintenir entre des bornes minimum et maximum. Un chemin inondé de phéromones masquerait tous les autres à proximité et un chemin pas du tout phéromonné ne serait jamais choisi par une fourmi, en conséquence nous devons conserver ces chemins avec des valeurs raisonnables. Ces bornes min et max sont aussi des paramètres de l'algorithme.

Les fourmis peuvent rencontrer certains types de problèmes dans le cas où elles se déplacent entre une source de nourriture et leur nid en essayant de trouver le chemin le plus court vers la destination. Des problèmes d'optimisation combinatoire ont alors été transposés à cette façon qu'ils ont d'organiser leur travail collectif tel que le problème de voyageur de commerce qui consiste à minimiser un effort en terme de distance à parcourir.

3.4.1 Le Problème du Voyageur de Commerce

Le Problème du Voyageur de Commerce (PVC), ou Traveling Salesman Problem (TSP), est un classique du genre dans le domaine de l'optimisation combinatoire. Il consiste à trouver le chemin le plus court reliant n villes données, chaque ville ne devant être visitée qu'une seule fois.

Le problème est plus généralement défini comme un graphe complètement connecté (N, A) , où les villes sont les nœuds N et les trajets entre ces villes, les arêtes A .

Un voyageur de commerce doit visiter un ensemble v_1, \dots, v_n de n villes dont on connaît les distances respectives $d(v_i, v_j), \forall (i, j) \in \{1, \dots, n\}$. Le problème consiste à trouver la permutation σ telle que la séquence $s = (v_{\sigma(1)}, \dots, v_{\sigma(n)})$ minimise la distance totale $D(\sigma)$ parcourue par le voyageur :

$$D(\sigma) = \sum_{k=i}^{n-1} d(v_{\sigma(i)}, v_{\sigma(i+1)}) + d(v_{\sigma(n)}, v_{\sigma(1)})$$

L'espace de recherche est l'ensemble des combinaisons possibles des n villes, soit au total $n!$ combinaisons. Ce problème, peut être aussi considéré comme la recherche d'un circuit hamiltonien² de longueur minimale dans un graphe complet pouvant être antisymétrique dans le cas général ($\exists (i, j)$ tel que $d(v_i, v_j) \neq d(v_j, v_i)$).

Pour résoudre ce genre de problèmes complexes en optimisation combinatoire tel que le PVC, il ont dû faire appel à la nature, les fourmis étant les premières à avoir suscité leur intérêt par leur comportement social collaboratif. Ce qui a donné naissance à une série d'algorithmes mettant en œuvre le "Ant System" (AS par la suite) [11], qui peut être présenté, d'une manière générale, comme un algorithme d'optimisation stochastique distribué. Plus exactement, il est défini comme une combinaison de calcul distribué, de récompense retardée [4].

2. Un circuit hamiltonien est un circuit possédant au moins un cycle passant par tous les sommets d'un graphe orienté une fois et une seule.

3.4.2 Principe de l'algorithme de colonie de fourmis "Ant System"

3.4.2.1 Définition informelle

La recherche du plus court chemin par une colonie de fourmis est illustrée par l'apparition d'un obstacle sur un chemin entre la source de nourriture et le nid.

La présence d'un obstacle sur le chemin contraint les fourmis à en faire le tour par l'un des deux chemins (A ou B).

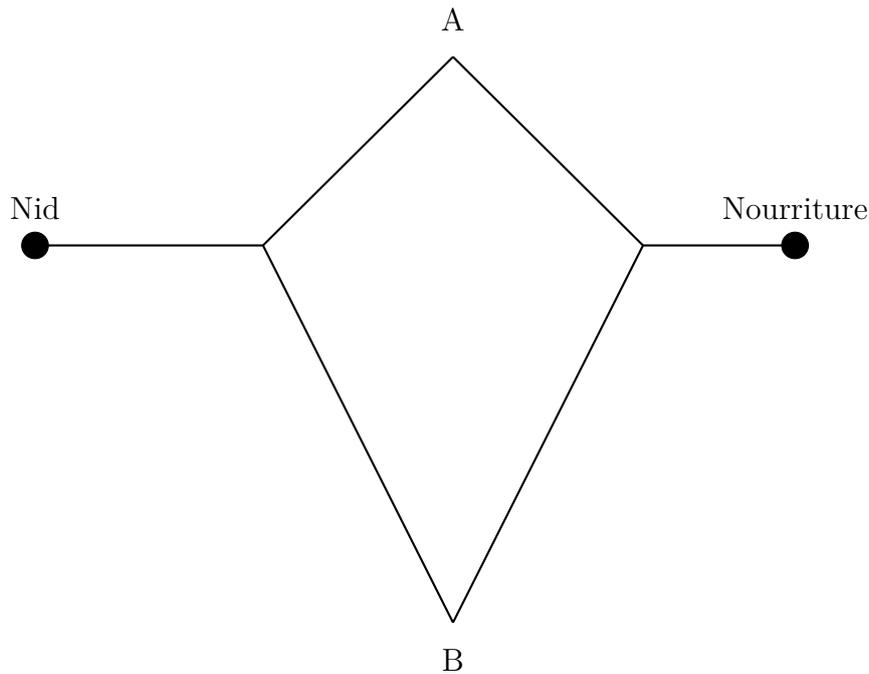


FIGURE 3.9 – Contournement d'un obstacle par une colonie de fourmis.

Quand les fourmis commencent à arriver par la gauche du dessin, en moyenne, la moitié des fourmis choisissent le plus long chemin (A) et l'autre moitié le plus court (B).

Les fourmis déposant toutes des phéromones, le chemin B sera plus marqué que A pour un temps donné. Comme les fourmis suivent en probabilité le chemin le plus marqué, le phénomène s'amplifie et le chemin B devient majoritairement suivi par les ouvrières.

Enfin, l'aspect probabiliste du déplacement des fourmis assure qu'elles seront toujours à la recherche d'une meilleure solution puisque que même quand les fourmis choisissent majoritairement le chemin B, la probabilité de choisir A ne devient pas nulle. De plus, les phéromones étant des substances chimiques volatiles, elles s'évaporent avec le temps, ce qui permet aux fourmis de continuer l'exploration de leur environnement.

3.4.2.2 Définition formelle

A chaque itération t ($1 \leq t \leq tmax$), chaque fourmi k ($k = 1, \dots, m$) parcourt le graphe et construit un trajet complet de $n = |N|$ étapes (on note $|N|$ le cardinal de l'ensemble N).

Pour chaque fourmi, le trajet entre une ville i et une ville j dépend de :

1. la liste des villes déjà visitées, qui définit les mouvements possibles à chaque pas, quand la fourmi k est sur la ville i : J_i^k
2. l'inverse de la distance entre les villes : $n_{ij} = 1/d_{ij}$, appelée visibilité. Cette information "statique" est utilisée pour diriger le choix des fourmis vers des villes proches, et éviter les villes trop lointaines.
3. la quantité de phéromone déposée sur l'arête reliant les deux villes, appelée l'intensité de la piste. Ce paramètre définit l'attractivité d'une partie du trajet global et change à chaque passage d'une fourmi. C'est, en quelque sorte, une mémoire globale du système, qui évolue par apprentissage. La règle de déplacement (appelée "règle aléatoire de transition proportionnelle" est la suivante :

$$P_{i,j}^k(t) = \begin{cases} \frac{(\tau_{ij}(t)^\alpha) \times (n_{ij}^\beta)}{\sum_{l \in J_i^k} (\tau_{il}(t)^\alpha) \times (n_{il}^\beta)} & \text{si } j \in J_i^k \\ 0 & \text{si } j \notin J_i^k \end{cases}$$

où α et β sont deux paramètres contrôlant l'importance relative de l'intensité de la piste, $\tau_{ij}(t)$, et de la visibilité, $n_{ij}(t)$

Avec $\alpha = 0$, seule la visibilité de la ville est prise en compte, la ville la plus proche est donc choisie à chaque pas. Au contraire, avec $\beta = 0$, seules les pistes de phéromone jouent.

Pour éviter une sélection trop rapide d'un trajet, un compromis entre ces deux paramètres, jouant sur les comportements de diversification et d'intensification, est nécessaire. Après un tour complet, chaque fourmi laisse une certaine quantité de phéromone $\Delta\tau_{ij}^k(t)$

$$\Delta\tau_{ij}^k(t) = \begin{cases} \frac{Q}{L^k(t)} & \text{si } (i, j) \in T^k(t) \\ 0 & \text{si } (i, j) \notin T^k(t) \end{cases}$$

Où $T^k(t)$ est le trajet effectué par la fourmi k à l'itération t , $L^k(t)$ la longueur de la tournée et Q un paramètre fixé.

L'algorithme ne serait pas complet sans le processus d'évaporation des pistes de phéromone. En effet, pour éviter d'être piégé dans des solutions sous-optimales, il est nécessaire de permettre au système "d'oublier" les mauvaises solutions. On contrebalance donc l'additivité des pistes par une décroissance constante des valeurs des arêtes à chaque itération. La règle de mise à jour des pistes est donc :

$$\tau_{ij}(t+1) = (1 - \rho) + \sum_{k=1}^m \Delta\tau_{ij}^k(t)$$

Où m est le nombre de fourmis et ρ le taux d'évaporation. La quantité initiale de phéromone sur les arêtes est une distribution uniforme d'une petite quantité $\tau_0 \geq 0$.

Algorithme 5 Algorithme de colonie de fourmis

Algorithme :

Pour $t = 1, \dots, t_{max}$ **faire**
 Pour chaque fourmis $k = 1, \dots, m$ **faire**
 Choisir une ville aléatoire
 Pour chaque ville non visitée i **faire**
 Choisir une ville j , dans la liste J_i^k des villes restantes.
 Fin Pour
 Déposé une piste $\Delta\tau_{ij}^k(t)$.
 Fin Pour
 Evaporer la piste.
Fin Pour

3.5 Conclusion

Dans ce chapitre, nous avons détaillé le protocole de routage géographique utilisé (GPSR) à travers ses deux algorithmes : le Greedy Forwarding et le Perimeter Forwarding. Par la suite, nous avons présenté l'algorithme de colonie de fourmis pour lequel nous avons opté pour assurer le renforcement du chemin et la continuité de service.

Le chapitre suivant sera consacré à l'implémentation de notre application de simulation, ainsi qu'à la présentation de l'environnement de travail, pour finir sur les résultats des tests menés sur cette dernière.

Chapitre 4

Implémentation et résultats

Sommaire

4.1	Introduction :	48
4.2	Environnement de travail : machine utilisée	48
4.3	Langage de programmation	48
4.4	Environnement de développement : Logiciel utilisé	48
4.5	Simulation et discussion des résultats	49
4.6	Conclusion :	54

4.1 Introduction :

Dans cette partie, nous donnons les détails de l'implémentation et de l'expérimentation des différents aspects théoriques présentés dans les chapitres précédents. Nous commençons par la présentation de l'environnement de programmation ainsi que le langage utilisé ; puis nous mettons en exergue les résultats des tests de simulation avec les commentaires.

4.2 Environnement de travail : machine utilisée

Nous avons expérimenté les algorithmes sur une machine ACER ayant un processeur Intel(R) Core(TM) i3-5005U M CPU, 2GHz, doté d'une mémoire vive de 4,00 GO. Le système d'exploitation utilisé est Microsoft Windows 10 avec l'EDI NetBeans IDE 8.2

4.3 Langage de programmation

Java : C'est un langage de programmation à usage général, évolué et à objet dont la syntaxe est proche des langages C et C++. Ses caractéristiques ainsi que la richesse de son écosystème et de sa communauté lui ont permis d'être très largement utilisé pour le développement d'applications de types très disparates. Java est notamment largement utilisé pour le développement des services web. Il est installé dans plus de 3 milliards de machine [Sun].

4.4 Environnement de développement : Logiciel utilisé

NetBeans : C'est un environnement de développement intégré (EDI), placé en open source par Sun en juin 2000 sous licence CDDL et GPLv2 (Common Development and Distribution License). En plus de Java, NetBeans permet également de supporter différents autres langages, comme Python, C, C++, JavaScript, XML, Ruby, PHP et HTML. Il comprend toutes les caractéristiques d'un IDE moderne (éditeur en couleur, projets multi-langage, refactoring, éditeur graphique d'interfaces et de pages Web). Conçu en Java, NetBeans est disponible sous Windows, Linux, Solaris (sur x86 et SPARC), Mac OS X ou sous une version indépendante des systèmes d'exploitation (requérant une machine virtuelle Java).

4.5 Simulation et discussion des résultats

Dans cette interface, nous initialisons les paramètres nécessaires à la simulation tels que les caractéristiques des nœuds (fixes et mobiles) ainsi que la loi de distribution choisie (Aléatoire, Poisson, Bernoulli) sans oublier le choix de l'algorithme de planarisation.



FIGURE 4.1 – Initialisation des paramètres de simulation

Dans l'interface ci-dessous, on définit les paramètres de l'algorithme de colonie de fourmis suivants : le taux d'évaporation de phéromone, la quantité initiale de phéromone, le coefficient de visibilité alpha et le coefficient du taux de phéromone beta. Sachant que le phéromone dans notre application est calculé grâce à "la règle aléatoire de transition proportionnelle" donnant comme résultat la matrice de probabilité qui va déterminer le chemin optimal.

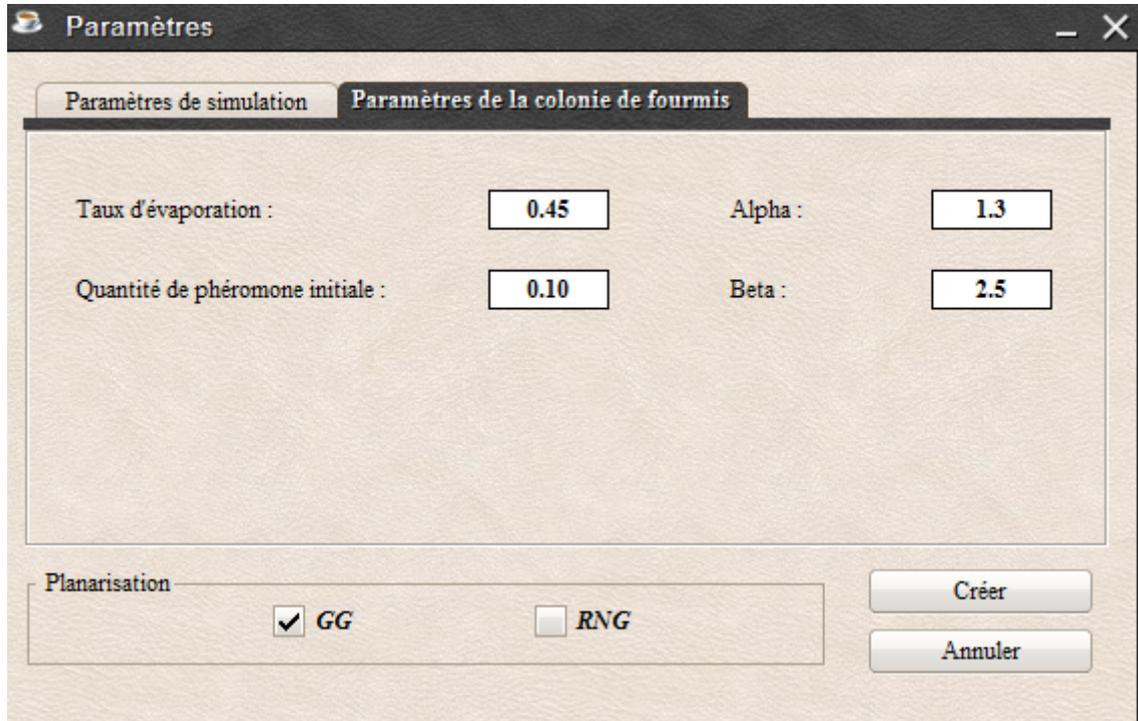


FIGURE 4.2 – Initialisation des paramètres de l'algorithme de colonie de fourmis

Dans la figure 4.3 on effectue le test de simulation après avoir initialisé quelques options comme la vitesse de mobilité, la portée des nœuds ainsi que la possibilité d'afficher les liens entre les nœuds. La fenêtre présente une surface dans laquelle est affichée la simulation en temps réel avec un déploiement des nœuds (fixes et mobiles) suivant la loi de distribution choisie au préalable. L'interface présente également trois tableaux d'affichage définissant, en partant du tableau du haut vers le bas : Les caractéristiques de chaque nœud (Identifiant, État du nœud, Position, etc.), ensuite un tableau des scénarios de communications effectuées (générés aléatoirement) et enfin un troisième tableau représentant la matrice de probabilité qui déterminera la solution optimale résultante de l'algorithme des fourmis.

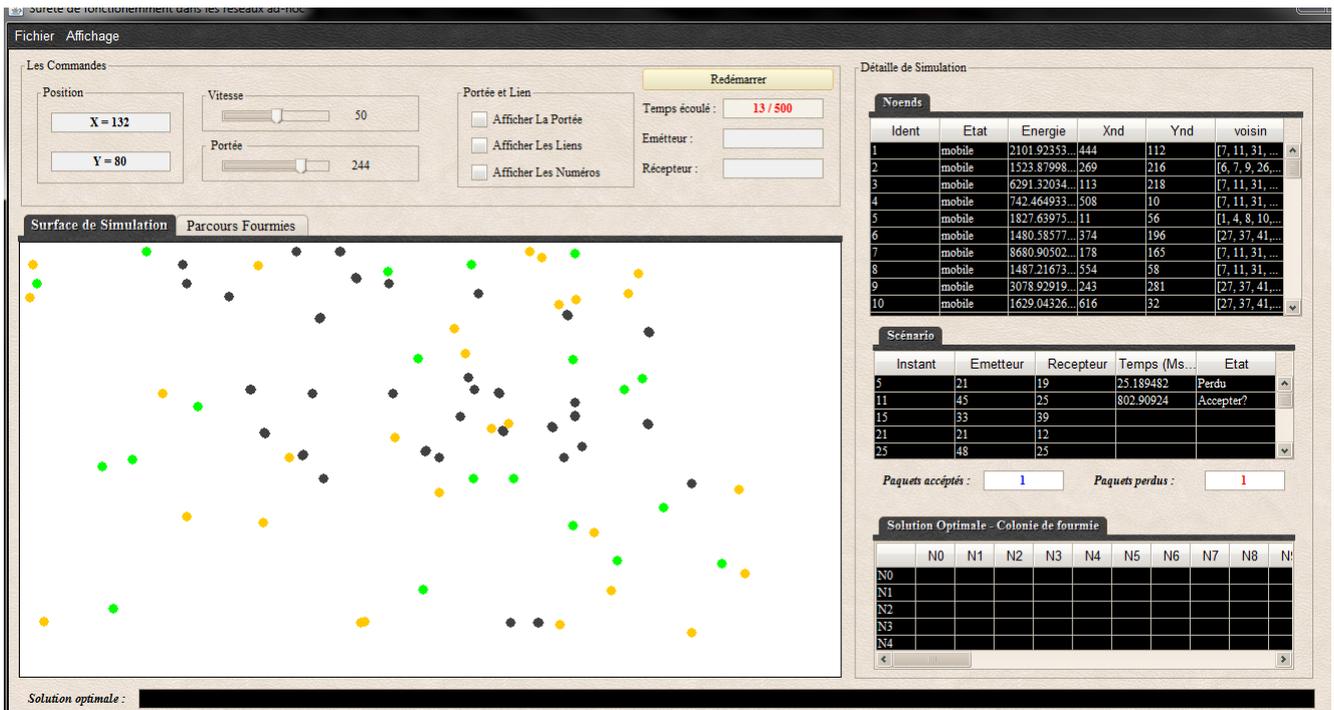


FIGURE 4.3 – Test de simulation

Dans l'onglet "Parcours fournis", nous affichons le parcours détaillé de chaque nœud mobile, chacun d'eux devra accomplir un cycle hamiltonien en passant par tous les nœuds fixes du graphe une seule fois et une seule.

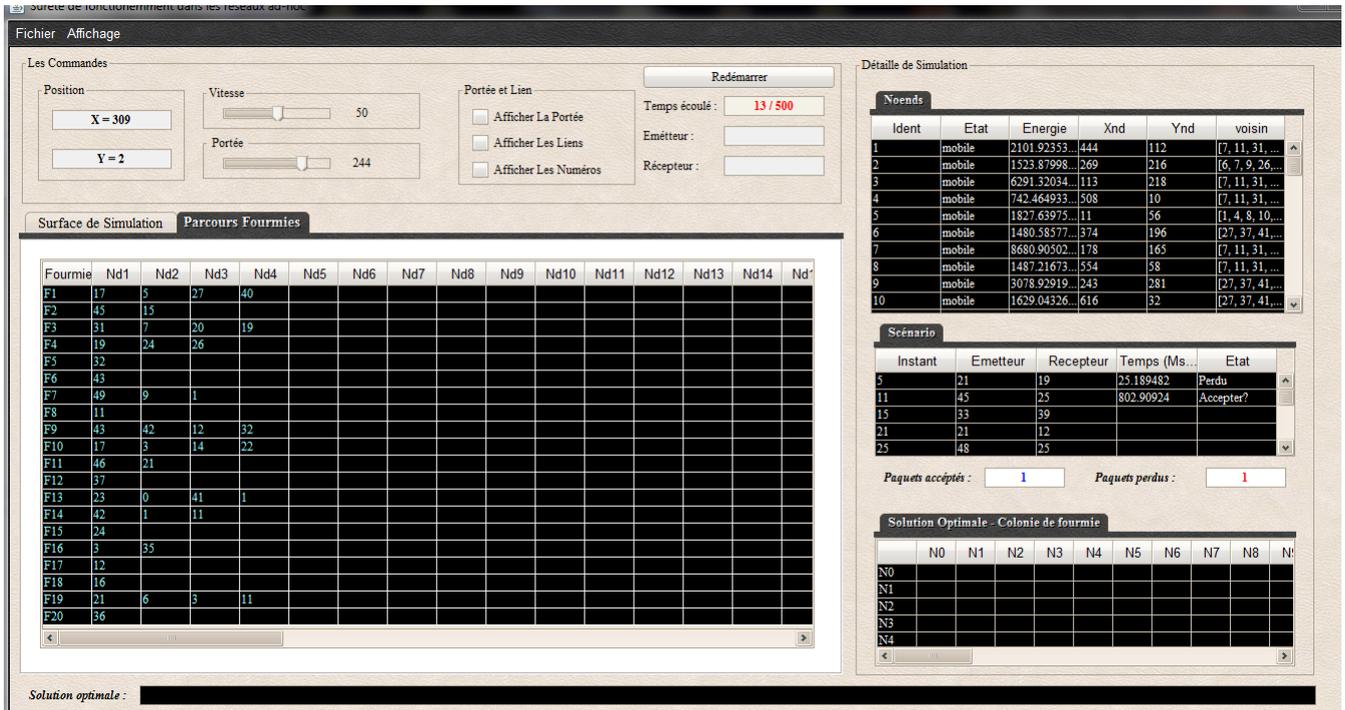


FIGURE 4.4 – Parcours des nœuds mobiles

Dès que tous les nœuds mobiles aient fini de parcourir tous les sommets fixes formant ainsi un cycle hamiltonien, on aura comme résultat une matrice qui indique la probabilité du choix du nœud suivant ce qui permettra de déterminer le chemin optimal ; lequel par la suite, les autres nœuds mobiles devront forcément suivre.

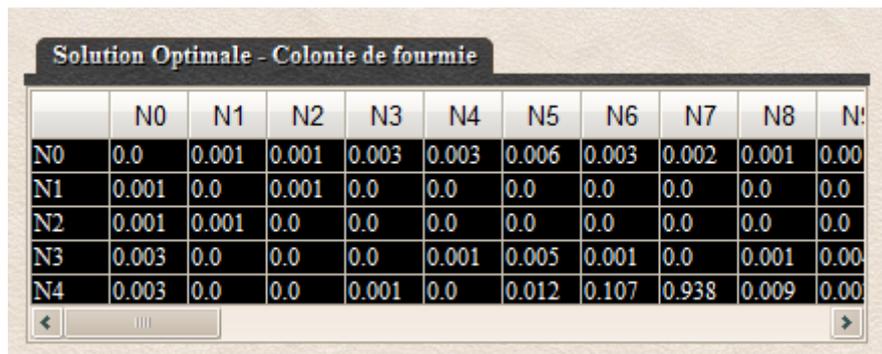


FIGURE 4.5 – Solution optimale : Matrice de probabilités

La figure suivante représente le graphe avec l'établissement des liens entre les nœuds. Entre les sommets immobiles, les liens sont fixes tandis que pour les nœuds en mouvement, les liens établis que se soit avec des sommets fixes ou mobiles, apparaissent et disparaissent en fonction du mouvement et du changement de la topologie et suivant la portée des nœuds voisins.

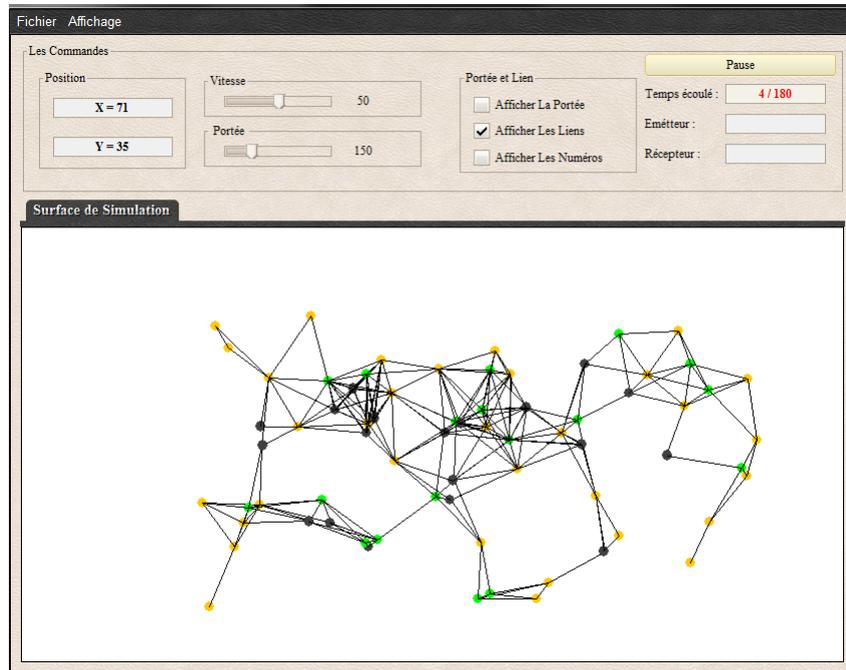


FIGURE 4.6 – Établissement des liens

Cette dernière fenêtre affiche l'historique des nœuds, où y sont présentés les événements de communications enregistrés ainsi que les différents chemins générés.

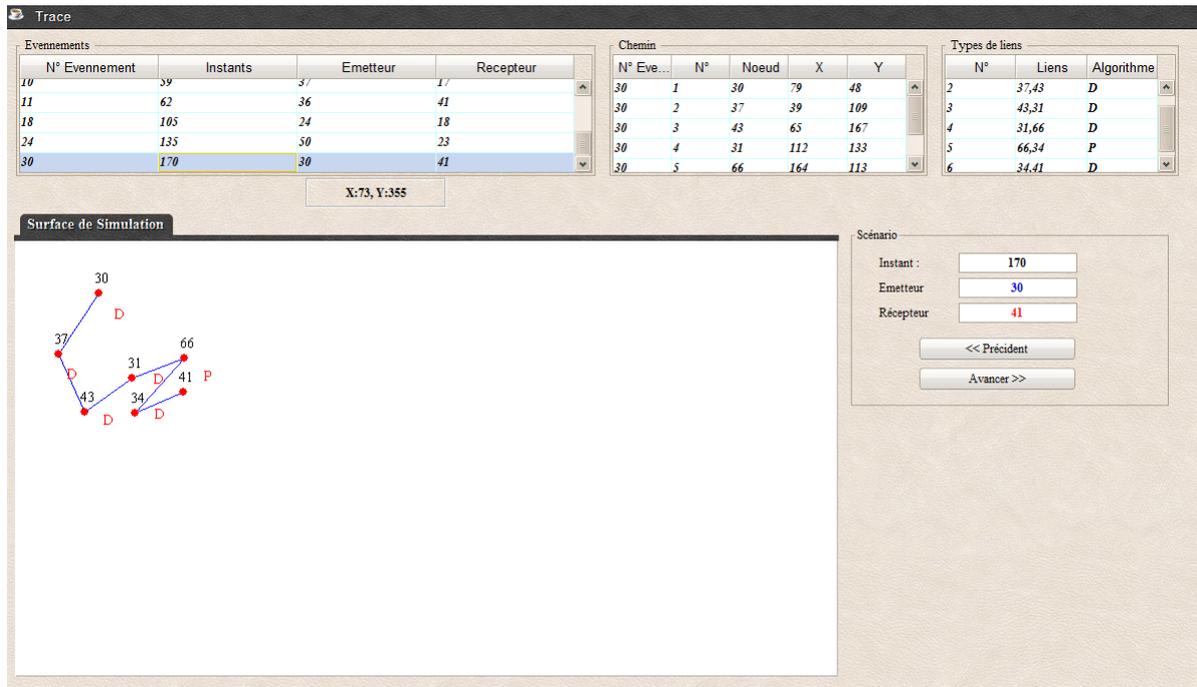


FIGURE 4.7 – Historique

4.6 Conclusion :

Ce chapitre a conclu tous les efforts fournis à la réalisation de notre démarche, par un aboutissement et une validation de notre travail grâce à la mise en œuvre d'une application de simulation, basée sur le développement du protocole géographique GPSR associé à l'algorithme de colonie de fourmis afin d'assurer la continuité du bon fonctionnement du réseau.

Pour cela, nous avons effectué divers tests de simulation en modifiant à chaque fois les paramètres de simulation, ce qui nous a permis de constater que les méthodes choisies, conçues initialement pour résoudre des systèmes complexes d'optimisation combinatoire, peuvent être appliquées aux protocoles de routage des réseaux Ad-hoc afin de corriger les éventuelles défaillances.

Conclusion

Dans ce mémoire, nous avons adapté un concept inspiré de la nature plus particulièrement du comportement collectif des fourmis pour optimiser la connectivité de notre réseau de capteurs sans fil. Afin de parvenir à cet objectif, notre travail s'est effectué en plusieurs étapes présentées tout au long de ce document et que nous résumons dans ce qui suit :

Nous nous sommes intéressés au départ, à la description des concepts de base des réseaux sans fil en mettant l'accent sur les réseaux Ad-hoc, leur principe et modes de fonctionnement ainsi que le processus et les protocoles de routage utilisés. Ce qui nous a permis de poser notre problématique : Est-il possible d'assurer une continuité de service face aux changements permanents de la topologie de notre réseau (apparition, disparition ou mouvement de certains nœuds) ?

Pour répondre à cette question nous avons fait appel aux techniques de la sûreté de fonctionnement, En effet la seconde étape a permis de présenter plusieurs rappels théoriques sur cette discipline, qui cherche à mesurer la qualité de service délivrée par un système, de manière à ce que l'utilisateur ait en lui une confiance justifiée. Nous avons conclu cette étape par une simple identification des défaillances qui peuvent se poser et porter atteinte au bon fonctionnement de notre réseau.

Dans la troisième étape, nous avons détaillé le protocole de routage utilisé ainsi que les algorithmes de base qui ont servi à l'implémentation du protocole GPSR, Nous avons expliqué par la suite l'algorithme de colonie de fourmis qui a servi à résoudre un problème d'optimisation combinatoire étant celui du voyageur de commerce.

Dans la dernière étape, nous avons validé notre démarche par le développement d'une application de simulation. Tout en appliquant les algorithmes et les concepts vus dans l'étape précédente. Nous avons effectué plusieurs tests de simulation en modifiant à chaque fois les paramètres de simulation tels que le nombre des nœuds (fixes et mobiles), les scénarios des communications, la vitesse de déplacement, la portée d'émission et de réception, et le déploiement des nœuds (aléatoire, Bernoulli, Poisson).

A l'issue de cette simulation, nous avons pu constater que les méthodes bio-inspirées en l'occurrence les algorithmes de colonie de fourmis peuvent s'appliquer aux protocoles de routage dans les réseaux Ad-hoc. Nous avons montré que l'association des nœuds mobiles (fourmis) aux réseaux de capteurs sans fil (nœuds fixes) donne un système capable d'agir et de corriger les défaillances, et par conséquent assure un service fiable et de bonne qualité.

Nous proposons donc comme perspective à notre travail d'utiliser d'autres variantes d'algorithmes de colonie de fourmis, et essayer d'éviter la convergence rapide vers la solution optimale (problème non résolu dans notre démarche). Une autre perspective de notre travail consiste à

perfectionner les résultats obtenus en terme de temps d'exécution et d'économie d'énergie en faisant appel à un simulateur tels que Cooja, Castalia ou Ns3 avec des scripts prédéfinis dont l'efficacité a été prouvée au préalable dans une variété de travaux dans le domaine des réseaux informatiques.

Bibliographie

- [1] Kahina Ait Ali. *Modélisation et étude de performances dans les réseaux VANET*. PhD thesis, Université de Technologie de Belfort-Montbéliard, 2012.
- [2] Jean-Luc Archimbaud. Cours interconnexion et conception de réseaux (informatiques). 2002.
- [3] Christian Bettstetter, Giovanni Resta, and Paolo Santi. The node distribution of the random waypoint mobility model for wireless ad hoc networks. *IEEE Transactions on mobile computing*, 2(3) :257–269, 2003.
- [4] Sihem Bouri. *Optimisation de la production et de la structure d'énergie électrique par les colonies de fourmis*. PhD thesis, Thèse, Université JilaliLiabès, 2007.
- [5] Josh Broch, David A Maltz, David B Johnson, Yih-Chun Hu, and Jorjeta Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, pages 85–97. ACM, 1998.
- [6] Tracy Camp, Jeff Boleng, and Vanessa Davies. A survey of mobility models for ad hoc network research. *Wireless communications and mobile computing*, 2(5) :483–502, 2002.
- [7] J Carsique, N Daujeard, A Lallemand, and R Ladjadj. Le routage dans les réseaux mobiles ad hoc, 2003.
- [8] MARILL Guillaume COSTANZO Andrea, LUONG Thé Van. *Optimisation par colonies de fourmis*. Université de Nice - Sophia Antipolis, 2006.
- [9] Mariam Dawoud. Analyse du protocole aodv. *Université Paul Sabatier*, 2006.
- [10] Bécaye DIOUM. Effets de la mobilité sur les protocoles de routage dans les réseaux ad hoc. *Université MOULOUD MAMMERI de TIZI OUZOU (Algerie)-Ingenieur d'état en Systeme d'information avancé*, 2007.
- [11] Johann Dréo. *Adaptation de la méthode des colonies de fourmis pour l'optimisation en variables continues. Application en génie biomédical*. PhD thesis, PhD thesis, Paris 12, 2004.
- [12] RIDENE Feten and RAISSI Adel. *Authentification dans les Réseaux Wifi par le protocole radius*. Université Virtuelle de Tunis, 2010/2011.
- [13] Anuj K Gupta, Harsh Sadawarti, and Anil K Verma. Performance analysis of aodv, dsr and tora routing protocols. *International Journal of Engineering and Technology*, 2(2) :226, 2010.
- [14] Zygmunt J Haas, Marc R Pearlman, and Prince Samar. The zone routing protocol (zrp) for ad hoc networks. 2002.
- [15] Xiaoyan Hong, Mario Gerla, Guangyu Pei, and Ching-Chuan Chiang. A group mobility model for ad hoc wireless networks. In *Proceedings of the 2nd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems*, pages 53–60. ACM, 1999.

-
- [16] Xiaoyan Hong, Kaixin Xu, and Mario Gerla. Scalable routing protocols for mobile ad hoc networks. *IEEE network*, 16(4) :11–21, 2002.
- [17] Chiraz Houaidia, Adrien Van den Bossche, Hanen Idoudi, Thierry Val, and Leila Azzouz Saidane. Impact des interférences dans un réseau sans fil multi-sauts. In *Journées Nationales des Communications Terrestres-JNCT 2014*, number ISBN 978-3, pages pp–87, 2014.
- [18] Tayeb Houasnia. *Pondération des taux de défaillances des équipements qui opèrent dans des milieux hostiles*. PhD thesis, Université du Québec à Trois-Rivières, 1999.
- [19] Atsushi Iwata, Ching-Chuan Chiang, Guangyu Pei, Mario Gerla, and Tsu-Wei Chen. Scalable routing strategies for ad hoc wireless networks. *IEEE journal on selected areas in communications*, 17(8) :1369–1379, 1999.
- [20] Brad Karp and Hsiang-Tsung Kung. Gpsr : Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 243–254. ACM, 2000.
- [21] TAHAR Abbes Mounir. *Protocole de routage à économie et énergie pour les transports des données dans un réseau cellulaire hybride*. PhD thesis, Université Mohamed Boudiaf des sciences et de la technologie d’Oran.
- [22] Sabrine Naimi. *Gestion de la mobilité dans les réseaux Ad Hoc par anticipation des métriques de routage*. PhD thesis, Université Paris Sud-Paris XI, 2015.
- [23] William Navidi and Tracy Camp. Stationary distributions for the random waypoint mobility model. *IEEE transactions on Mobile Computing*, 3(1) :99–108, 2004.
- [24] Baudouin TSOFAK NGUIMEYA, Mathurin SOH, and Laure Pauline. Algorithmes hybrides pour la résolution du problème du voyageur de commerce. *Article universitaire. Université de Dshang, Cameroun et Université de Yaoundé I, Cameroun*.
- [25] Zeyun Niu, Wenbing Yao, Qiang Ni, and Yonghua Song. Dreq : a qos routing algorithm for multimedia communications in vehicular ad hoc networks. In *Proceedings of the 2007 international conference on Wireless communications and mobile computing*, pages 393–398. ACM, 2007.
- [26] Daniel Noyes and François Pérès. Analyse des systèmes-sûreté de fonctionnement. *Techniques de l’ingénieur*, 2007.
- [27] Vincent Douglas Park and M Scott Corson. A highly adaptive distributed routing algorithm for mobile wireless networks. In *INFOCOM 97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution, Proceedings IEEE*, volume 3, pages 1405–1413. IEEE, 1997.
- [28] Guangyu Pei, Mario Gerla, and Tsu-Wei Chen. Fisheye state routing : A routing scheme for ad hoc wireless networks. In *Communications, 2000. ICC 2000. 2000 IEEE International Conference on*, volume 1, pages 70–74. IEEE, 2000.
- [29] Mathias Péron. *Etude de l’équité dans les réseaux ad hoc*. PhD thesis, Master’s thesis, Ecole Normale Supérieure de Lyon, 2003.
- [30] Vijay Raghunathan, Curt Schurgers, Sung Park, and Mani B Srivastava. Energy-aware wireless microsensor networks. *IEEE Signal processing magazine*, 19(2) :40–50, 2002.
- [31] Abdul Hadi Abd Rahman and Zuriati Ahmad Zukarnain. Performance comparison of aodv, dsdv and i-dsdv routing protocols in mobile ad hoc networks. *European Journal of Scientific Research*, 31(4) :566–576, 2009.
- [32] Miguel Sánchez and Pietro Manzoni. Anejos : a java based simulator for ad hoc networks. *Future generation computer systems*, 17(5) :573–583, 2001.

- [33] Pierre Schwartz. *Application d'un algorithme de colonie de fourmis au problème du voyageur de commerce*. Developpez.com, 2008.
- [34] Yuan Xue and Baochun Li. A location-aided power-aware routing protocol in mobile ad hoc networks. In *Global Telecommunications Conference, 2001. GLOBECOM'01. IEEE*, volume 5, pages 2837–2841. IEEE, 2001.