République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université Ahmed Draia - Adrar

Faculté des Sciences et de la Technologie

Département des Mathématiques et Informatique

Mémoire de fin d'étude, en vue de l'obtention du diplôme de Master en informatique

Option : Réseaux et Systèmes Intelligents

Thème

Une approche bio-inspiré pour un routage adaptatif efficace en énergie dans les réseaux de capteurs sans fil

Préparé par :

BAHOU Djelloul

Membre de jury composé de :

✍ Mr. KADDI Mohammed	Université d'Adrar	Président.
✍ Mr. DEMRI Mohammed	Université d'Adrar	Encadreur.
✍ Mr. OMARI Mohammed	Université d'Adrar	Examinateur.
✍ Mr. MAMOUNI El mamoun	Université d'Adrar	Examinateur.

Année Universitaire 2014/2015

Résumé

Concevoir et développer des protocoles de routage efficace en énergie pour les Réseaux de Capteurs Sans Fil (RCSF) présente un apport considérable pour améliorer les performances des réseaux et d'accroitre leur durée de vie. L'objectif de ce travail est d'adapter un protocole de routage hiérarchique bio-inspiré basé sur le principe de fonctionnement des cellules B dans système immunitaire Naturel (SIN) et que nous avons nommé **AISBCP** (Artificiel Immune System Based Clustering Protocol). La sélection clonale est l'un des théories du système immunitaire artificiel (SIA) et la plus utiliser pour résoudre des problèmes de façon intelligente basant sur la l'heuristique, la sélection naturel et la mutation. Cette nouvelle approche de classification évolutive permettra d'améliorer l'efficacité du routage dans les réseaux de capteurs. En effet, le nouvel algorithme de routage que nous proposons donne des bons résultats.

Mots Clés : RCSF, Protocole de routage, Energie, AISBCP et SIN, Sélection clonale, Clustering.

Abstract

Design and develop energy-efficient routing protocols for Wireless Sensor Networks (WSN) has an important contribution to improve network performances and increase their lifetime. The objective of this work is to adapt a bio-inspired hierarchical routing protocol based on the principle of the B cells in Natural Immune System (SIN) and that we named **AISBCP** (Artificial Immune System Based Clustering Protocol). Clonal sélections is one of the theories of artificial immune system (AIS) and mostly used to solve problems intelligently based on heuristics, the natural selection and mutation. This new evolutionary classification approach improves the efficiency of routing in sensor networks. In fact, the routing algorithm that we propose gives better results.

Keywords : WSN, Routing protocols, Energy, AISBCP and NIA, clonal selection, Clustering.

Dédicace

A mon père ;

A ma mère ;

A mes frères et mes sœurs ;

Aux les petits enfants :

Yasser, Fidaa et Iness ;

A toute ma famille ;

A mon encadreur Demri Mohamed ;

A mes amies et tous ceux que me sont cher.

Remerciements

Je dois tout d'abord à remercier dieu le tout puissant qui me donne le courage et la force de bien mener mon travail.

Je dois aussi remercie vivement et exprimer mon gratitude :

- *Tout d'abord à mon encadreuse Mr. DEMRI Mohammed pour ses conseils, et sa grande contribution dans la réalisation de mon travail et surtout pour sa grande patience et gentillesse à mon égard.*
- *A Mr. MAMOUNI El Mamoun à sa contribution dans la réalisation de mon travail.*
- *Aux touts les membres du département d'informatique pour leur amabilité et leur soutien.*
- *A tout le corps des enseignants de l'Université d'Adrar pour leur formation.*

SOMMAIRE

CHAPITRE II: ***Protocoles de routage dans les RCSFs : Etat de l'art***

CHAPITRE III: ***Système Immunitaire***

CHAPITRE IV: ***Implémentation et discussion***

LISTE DES TABLEAUX

LISTE DES FIGURES

Introduction générale

Introduction générale

Les avancées récentes dans le domaine de communication sans fil et les systèmes micro-électro-mécaniques ont permis le développement des micro-composants qui intègrent des dispositifs de captages et de communication sans fil dans un seul circuit pour capter des grandeurs physiques (chaleur, humidité, vibrations) et de les transformer en grandeurs numériques, une unité de traitement informatique et de stockage de données et un module de transmission sans fil, à dimension réduite, et avec un coût raisonnable. Ces composants, communément appelés micro-capteurs, ont favorisé l'idée de développer les réseaux de capteurs basés sur l'effort collaboratif d'un grand nombre de nœuds opérant d'une façon autonome et communiquant entre eux via des transmissions à courte portée.

Ce nouveau type de réseaux présente une grande amélioration comparé aux capteurs classiques qui sont généralement positionnés loin du phénomène surveillé. La position des nœuds utilisés n'est pas obligatoirement conçue au préalable, ce qui permet leur déploiement aléatoire dans les terrains inaccessibles ou pendant les opérations de secours aux cas de désastres. La réalisation des différentes applications liées aux réseaux de capteurs requièrent l'utilisation des techniques employées dans les réseaux ad hoc sans fil, cependant, la multitudes des protocoles doivent alors posséder des capacités de localisation et d'auto-organisation. Ces capteurs transmettent régulièrement les données au nœud central où les traitements sont accomplis et les données sont fusionnées. On distingue plusieurs critères faisant la différence entre les réseaux de capteurs et les réseaux ad hoc que nous mentionnons dont :

- Le nombre de nœuds est nettement plus grand dans les réseaux de capteurs que dans les réseaux ad hoc.
- Les nœuds capteurs sont plus exposés aux pannes.
- Les réseaux de capteurs utilisent principalement les communications broadcaste.
- Les nœuds capteurs sont caractérisés par des ressources plus limités (ressource d'énergie, puissance de calcul et mémoire).

Un capteur est muni d'une ressource énergétique (généralement une batterie) pour alimenter tous ses composants. Cependant, en raison de sa taille réduite, la ressource énergétique dont il dispose est limitée et généralement irremplaçable. Plusieurs travaux de recherche on était effectuée afin de proposer des stratégies de routages. Dans ce travail, nous

présentons tout d'abord un état de l'art sur des protocoles et les algorithmes de routage qui existe dans la litérature, afin de donner une vue globale sur les travaux de recherche existants et de décrire certaines techniques utilisées pour répondre aux objectifs de conceptions des réseaux de capteurs sans fil.

L'objectif principal de notre travail est d'adapter un nouveau protocole de routage basé sur l'approche dites System immunitaire artificiel (AIS) qui'l trouve ça place dans ce domaine de recherche. Nous inspérons à partir du métaphore du système immunitaire à reconnaître les antigènes, à mémoriser les cellules, et à sélectionnez les clones.

Ce mémoire est organisé en quatre chapitres:

Dans le premier chapitre, nous présenterons les réseaux de capteurs sans fil : leurs architectures de communication et leurs applications. Nous discuterons également les principaux facteurs et contraintes qui influencent la conception des réseaux de capteurs sans fil. Nous terminerons le chapitre par une description de la problématique de la consommation d'énergie dans les réseaux de capteurs sans fil.

Dans le deuxième chapitre, nous présenterons quelques solutions proposées pour conserver la consommation d'énergie, un état de l'art sur un enssemble des protocole des routage héiarchique et non héiarchique . Et en fin un petit Etude comparative entre quelques protocole héirachiques.

Dans le troisième chapitre, nous présenterons le système immunitaire naturel (NIS) et sont principe de fonctionnement. Nous présenterons aussi le système immunitaire Artificiel (AIS), leur principe algorithme plus utiliser, ces domaines d'application et petit étude comparative entre différents systèmes inspirés de la biologie.

Dans le dernier chapitre, nous détaillerons tout d'abord notre algorithme de routage basé sur l'agorithm de la selection cloanle pour réaliser un routage économe en terme d'énergie. Nous détaillerons le simulateur que nous avons conçu et nous discuterons les résultats de simulation obtenus.

CHAPITRE I

Introduction aux réseaux de capteurs sans fil

-RCSF-

I.1. Introduction

L'évolution de l'informatique a été marquée par différentes étapes dans la miniaturisation. Dernièrement, sont apparus d'infimes systèmes micro-électromécaniques, des dispositifs à bas coûts intégrant les fonctionnalités de captage, de traitement et de communication. Un grand nombre de ces dispositifs est déployé dans la nature afin de créer un réseau de capteurs à des fins aussi bien de contrôle que de motorisation. Ces dispositifs formant les nœuds, détectent les changements environnementaux et les signalent aux autres nœuds sur la base d'une architecture flexible du réseau. Les nœuds capteurs donnent la possibilité d'être déployés dans des environnements hostiles et sur de larges zones géographiques.

Dans ce chapitre nous présenterons les réseaux de capteur sans fil, ses applications et son architecture. Ensuite nous expliquerons les différentes contraintes dans un réseau de capteur et particulièrement la consommation d'énergie.

I.2. Définition d'un capteur

Un capteur est un dispositif qui transforme l'état d'une grandeur physique observée en une grandeur utilisable, exemple : une tension électrique, une hauteur de mercure, une intensité, la déviation d'une aiguille….etc.

Le capteur se distingue de l'instrument de mesure par le fait qu'il ne s'agit que d'une simple interface entre un processus physique et une information manipulable. Par opposition, l'instrument de mesure est un appareil autonome se suffisant à lui-même. Il dispose donc d'un affichage ou d'un système de stockage des données. Ce qui n'est pas forcément le cas du capteur.

Les capteurs sont les éléments de base des systèmes d'acquisition de données. Leur mise en œuvre est du domaine de l'instrumentation [1].

I.3. Classification des capteurs

Les capteurs ont plusieurs modes de classification :

- *Capteurs passifs:* Ils n'ont pas besoin d'apport d'énergie extérieure pour fonctionner (exemple : thermistance, potentiomètre, thermomètre à mercure…). Ce sont des capteurs modélisables par une impédance. Une variation du phénomène physique étudié (mesuré) engendre une variation de

l'impédance.

- *Capteurs actifs :* Ils sont constitués d'un ensemble de transducteurs alimentés (exemple: chronomètre mécanique, jauge d'extensomètre appelée aussi jauge de contrainte, gyromètre…). Ce sont des capteurs que l'on pourrait modéliser par des générateurs comme les systèmes photovoltaïques et électromagnétiques. Ainsi ils génèrent soit un courant, soit une tension en fonction de l'intensité du phénomène physique mesuré.

Les capteurs peuvent aussi faire l'objet d'une classification par type de sortie:

- *Capteurs analogiques :* Le signal des capteurs numériques peut être du type : sortie tension, sortie courant, règle graduée ... etc.

Quelques capteurs analogiques typiques : Capteur à jauge de contrainte, LVDT…etc.

- *Capteurs numériques:* Le signal des capteurs numériques peuvent être du type : Train d'impulsions avec un nombre précis d'impulsions ou avec une fréquence précise, Code numérique binaire, Bus de terrain … etc.

Quelques capteurs numériques typiques : Les capteurs incrémentaux, Les codeurs absolus.

I.4. Architecteur d'un nœud capteur

Un nœud capteur est composé de quatre composants de base [2] comme représentée dans la *figure I.1*: une *unité d'acquisition*, une *unité de traitement*, une *unité de transmission* (communication) et une source d'énergie. Ils peuvent également avoir d'autres composants dépendants de l'application tels qu'un *système de localisation* et *un mobilisateur.*

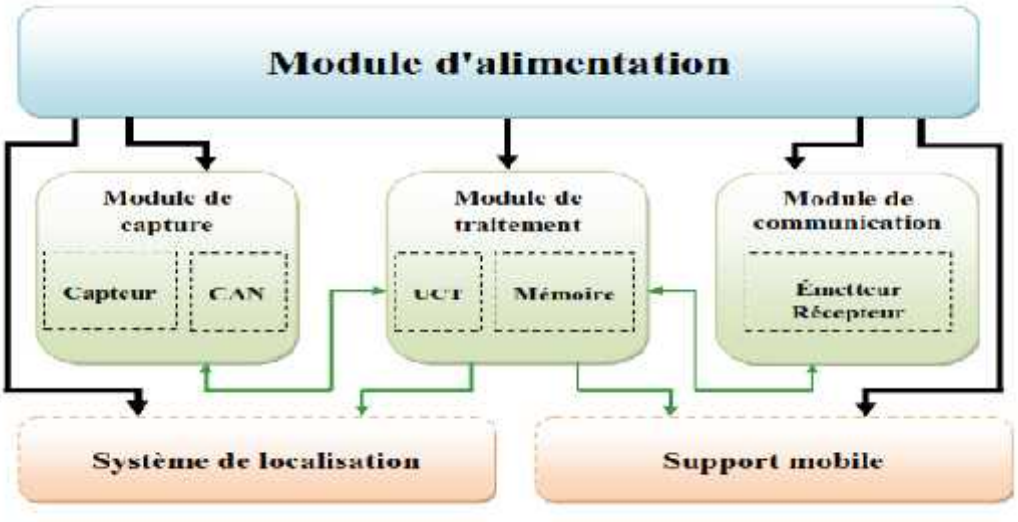

Figure I.1 : Les composants d'un nœud capteur

- *L'unité d'acquisition:* Elle se compose de deux sous unités, unité de captage et un convertisseur analogique – numérique (CAN). Le capteur permet de mesurer des informations environnementales : température, humidité, pression, accélération, sons, image, vidéo etc., puis produit des signaux analogiques qui sont convertis par un convertisseur analogique – numérique pour pouvoir être traitées par l'unité de traitement
- *L'unité de traitement:* l'unité de traitement est composée de deux interfaces, une interface pour l'unité d'acquisition et une interface pour l'unité de transmission. Cette unité comprend un processeur avec une petite unité de stockage, une RAM pour les données et une ROM pour les programmes et souvent une mémoire flash. Cette unité fonctionne à l'aide d'un système d'exploitation spécialement conçu pour les micro-capteurs (TinyOS par exemple). Elle est chargée de gérer des procédures qui permettent à un nœud capteur de collaborer avec les autres nœuds du réseau. Elle peut aussi analyser les données captées pour alléger la tâche du nœud puits.
- *L'unité de transmission (communication):* Cette unité est responsable d'effectuer toutes les émissions et réceptions des données sur un medium sans fil. Les composants utilisés pour réaliser la transmission sont des composants classiques, les unités de transmission de type Radio Fréquence (RF) sont préférables pour les RCSF parce que les paquets transportés sont de petites tailles avec un bas débit. Ainsi on retrouve les mêmes problèmes que dans tous les réseaux sans fil : la quantité d'énergie nécessaire à la transmission augmente avec la distance. Pour les réseaux sans fil classiques (LAN, GSM) la consommation d'énergie est de l'ordre de plusieurs centaines de milliwatts alors que pour les réseaux de capteurs, le système de transmission possède une portée de quelques dizaines de mètres. Pour augmenter ces distances tout en préservant l'énergie, le réseau utilise un routage multi sauts.
- *La source d'énergie :* Les capteurs sont de petits composants alimentés avec une batterie ou avec des piles. Pour qu'un réseau de capteurs reste autonome pendant une durée de quelques mois à quelques années sans intervention humaine, la consommation d'énergie devient le problème fondamental. Celle-ci n'est pas un grand problème pour les réseaux sans fil traditionnel, car on peut toujours recharger les batteries des dispositifs sans fil comme les téléphones portables ou les ordinateurs portables. Mais, dans un RCSF, il est difficile (parfois impossible

dans certaines applications) de changer la batterie. Cette unité peut aussi contenir des systèmes de rechargement d'énergie à partir de l'environnement observé telles que les cellules solaires, afin d'étendre la durée de vie totale du réseau.

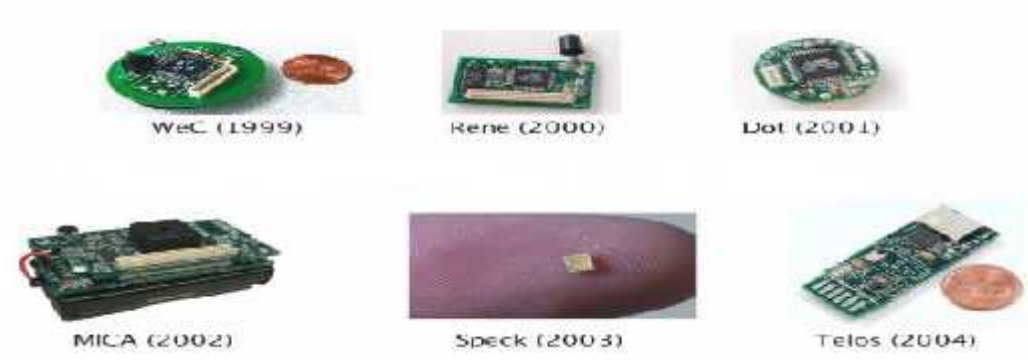

Figure I.2 : Quelque exemple des capteurs

I.5. Qu'est-ce un réseau Ad-hoc ?

Les réseaux mobiles sans fil, peuvent être classés en deux classes : les réseaux avec infrastructure qui utilisent généralement le modèle de la communication cellulaire, et les réseaux sans infrastructure ou les réseaux ad-hoc.

Plusieurs systèmes utilisent déjà le modèle cellulaire et connaissent une très forte expansion à l'heure actuelle (les réseaux GSM par exemple) mais requièrent une importante infrastructure logistique et matérielle fixe.

La contrepartie des réseaux cellulaires sont les réseaux mobiles ad-hoc. Un réseau ad-hoc peut être défini comme une collection d'entités mobiles interconnectées par une technologie sans fil formant un réseau temporaire sans l'aide de toute administration ou de tout support fixe. Aucune supposition ou limitation n'est faite sur la taille du réseau cela veut dire qu'il est possible que le réseau ait une taille très énorme.

Dans un réseau ad-hoc les hôtes mobiles doivent former, d'une manière ad-hoc, une sorte d'architecture globale qui peut être utilisées comme infrastructure du système. Les applications des réseaux ad-hoc sont nombreuses, on cite l'exemple classique de leur application dans le domaine militaire et les autres applications de tactique comme les opérations de secours et les missions d'exploration.

Du fait que le rayon de propagation des transmissions des hôtes soit limité, et afin que le réseau ad-hoc reste connecté, (c'est à dire tout unité mobile peut atteindre toutes autre), il se peut qu'un hôte mobile se trouve dans l'obligation de demander de l'aide à un autre

hôte pour pouvoir communiquer avec son correspondant. Il se peut donc que l'hôte destination soit hors de la portée de communication de l'hôte source, ce qui nécessite l'emploi d'un routage interne par des nœuds intermédiaires afin de faire acheminer les paquets de messages à la bonne destination.

La gestion de l'acheminement de données ou le routage, consiste à assurer une stratégie qui garantit, à n'importe quel moment, la connexion entre n'importe quelle paire de nœuds appartenant au réseau. La stratégie de routage doit prendre en considération les changements de la topologie ainsi que les autres caractéristiques du réseau ad-hoc (bande passante, nombre de liens, ressources du réseau…etc.). En outre, la méthode adoptée dans le routage, doit offrir le meilleur acheminement des données en respect des différentes métriques de coûts utilisées.

I.6. Qu'est-ce un réseau de capture sans fil ?

Un réseau de capteur sans fil (Wireless Sensor Network: WSN) est un type particulier de réseau ad-hoc défini par un ensemble coopérant de nœuds capteurs dispersés dans une zone géographique appelée zone de captage afin de surveiller un phénomène et récolter ses données d'une manière autonome.

Un réseau de capteurs se compose de deux types de nœuds : des simples capteurs et des collecteurs d'informations appelés puits (sink en anglais)

Le capteur est composé d'un microcontrôleur et d'un circuit radio:

- *Le microcontrôleur :* est simple et peut être embarqué aisément. Cet appareil doit répondre à l'exigence d'une faible consommation d'énergie tout en ayant la possibilité d'exécuter de simples opérations et de posséder une mémoire permettant d'emmagasiner de l'information. L'appareil doit aussi présenter la possibilité d'avoir un état oisif durant lequel il consomme une quantité d'énergie infinitésimale. Ces états oisifs peuvent parfois durer très longtemps. Le capteur peut se réveiller seulement pour capter la grandeur physique à mesurer et aussi pour effectuer des opérations de réseaux comme dialoguer avec des capteurs voisins ou relayer l'information provenant d'autres capteurs.

- *Le circuit radio :* assure la communication du capteur avec d'autres appareils via

des liens radios. Ces derniers ont facilité l'implantation massive de capteurs et ont offert une indépendance précieuse car il a réduit les coûts du câblage et de l'ingénierie nécessaire pour les installations passées. Grâce à la communication sans fil, un installateur peut déposer facilement des capteurs sans se soucier de la complexité des opérations pour les atteindre afin de relever les mesures. Il suffit d'être dans le champ de couverture radio pour transmettre ou recevoir l'information requise.

Avec ses capacités de traitement et de mémorisation, le capteur peut devenir un nœud actif dans un réseau relativement large. Lorsque le nombre de capteurs devient conséquent, la communication en réseau devient indispensable. Il n'est en effet alors plus possible d'atteindre un capteur directement par un câble ou même par une connexion radio. C'est là alors qu'on peut parler de véritables réseaux de capteurs capables de s'auto-configurer et de s'auto-organiser de manière dynamique. Ces propriétés offrent un très large spectre d'applications, notamment dans les domaines militaires, de l'environnement, de l'écologie, etc.

I.7. Architecture d'un réseau de capteurs sans fil

Un réseau de capteurs sans fil est composé d'un grand nombre de nœuds. Chaque capteur est doté d'un module d'acquisition qui lui permet de mesurer des informations environnementales : température, humidité, pression, accélération … etc.

Les données collectées par ces nœuds capteurs sont routées vers une ou plusieurs stations de base ou nœud puis (sink en anglais). Ce dernier est un point de collecte de données capturées. Il peut communiquer les données collectées à l'utilisateur final à travers un réseau de communication, éventuellement l'Internet ou un satellite. L'utilisateur peut à son tour utiliser la station de base comme passerelle, afin de transmettre ses requêtes au réseau (*Voir la figure I.3*).

En général, un RCSF est composé de quatre éléments montrés par *la figure I.3* : les nœuds capteurs, une station de base, phénomène à mesurer et l'utilisateur. [3]

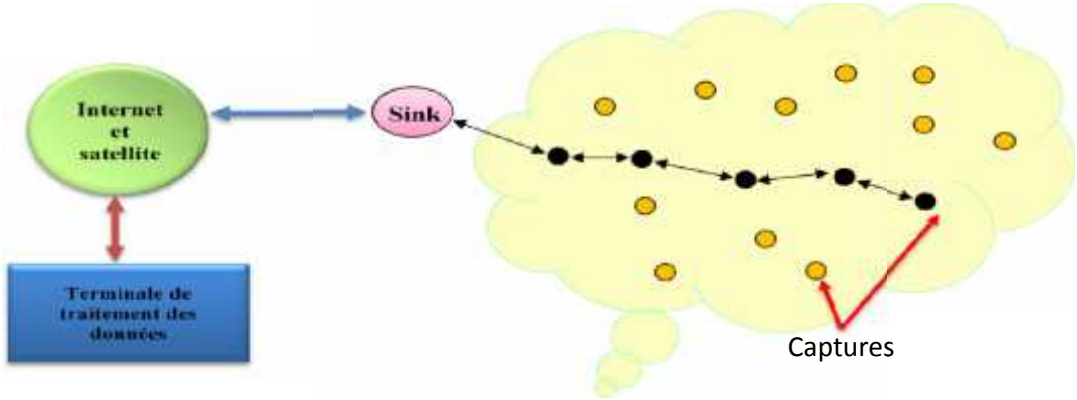

Figure I.3: Architecture d'un Réseau de Capteur Sans Fil.

I.8. Caractéristiques d'un réseau de capteurs sans fil

L'intégration des réseaux de capteurs avec le monde physique a rendu leur mode de fonctionnement différent de celui des réseaux informatiques traditionnels. Ils possèdent des caractéristiques particulières qui rendent le développement d'applications non-trivial.

Les réseaux de capteurs sans fil sont apparentés aux réseaux ad-hoc. En effet, ces deux types de réseaux ont de nombreux points communs :

- Réseaux sans infrastructure,
- Architecture décentralisée,
- Autonomie,
- Utilisation d'ondes radio pour communiquer.

Bien que de nombreux protocoles et algorithmes aient été proposés pour les réseaux ad-hoc traditionnels, ils ne sont pas bien adaptés aux caractéristiques et exigences des applications. Les points de différence entre les deux réseaux [6] sont :

- la densité des nœuds déployés est beaucoup plus importante dans les réseaux de capteurs.
- les nœuds capteurs ont des capacités limitées en énergie et mémoire.
- la topologie dans les réseaux de capteurs est souvent dynamique,
- dans un réseau de capteurs, la communication entre les nœuds se fait par diffusion et non pas point à point,
- les capteurs peuvent ne pas avoir un identifiant global à cause du grand nombre de nœuds.

Les nœuds capteurs ayant un petit volume qui approchera les quelques millimètres

cube dans un proche avenir, sont limités dans la quantité d'énergie qu'ils peuvent stocker. En outre, ces nœuds sont sensibles à l'échec, suite à l'épuisement des batteries ou bien aux influences de l'environnement. Dans cette section, nous allons montrer les différentes caractéristiques liées aux réseaux de capteurs telles que le *déploiement, la couverture, la connectivité, l'énergie, la mobilité*, etc.

I.8.1. Déploiement

Le déploiement des capteurs est la première opération (phase) dans le cycle de vie d'un réseau de capteurs. On peut envisager plusieurs formes de déploiements selon les besoins des applications. Les nœuds peuvent être déployés aléatoirement d'un avion ou d'une roquette par exemple, ou bien ils peuvent être placés un par un d'une manière déterministe par un humain ou un robot. Le déploiement peut être fait d'un seul coup ou bien peut être un processus continu en redéployant d'autres capteurs dans une même zone. Dans un grand nombre d'applications, le déploiement manuel est impossible. De plus, même lorsque l'application permet un dé- ploiement déterministe, le déploiement aléatoire est adopté dans la majorité des scénarios à cause de raisons pratiques tels que le coût et le temps. Cependant, le déploiement aléatoire ne peut pas fournir une distribution uniforme sur la région d'intérêt, ce qui déclenche de nouveaux problèmes dans les réseaux de capteurs. Les principaux problèmes engendrés sont la localisation, la couverture de la zone, la connexité et la sécurité.

I.8.2. Énergie et durée de vie

La durée de vie est un élément essentiel pour tout réseau de capteurs sans fil, C'est l'intervalle de temps qui sépare l'instant de déploiement du réseau de l'instant où l'énergie du premier nœud s'épuise. Selon l'application, la durée de vie exigée pour un réseau peut varier entre quelques heures et plusieurs années.

Un nœud capteur peut se trouver dans l'un des quatre états suivants [6] : actif en mode d'écoute, actif en mode de traitement de données, actif en mode de transmission ou non actif en mode veille. Un capteur est en veille lorsque sa radio est éteinte, dans ce cas sa consommation d'énergie est presque nulle. En effet, la principale source de consommation d'énergie d'un capteur est l'utilisation du réseau sans fil via son module de radiocommunications. Cette consommation d'énergie peut être réduite par la diminution de la transmission des données, d'où la nécessité du traitement local.

I.8.3. Connectivité

La plupart des réseaux de capteurs possèdent initialement une densité importante de capteurs, excluant ainsi l'isolement de nœuds. Pourtant, le redéploiement, la mobilité et les défaillances font varier la topologie du réseau, dont la connexité n'est pas toujours assurée.

I.8.4. Groupement « *clustering* »

Un réseau de capteur est souvent constitué de plusieurs milliers de nœuds capteurs. Pour réduire la complexité des algorithmes de routage, faciliter l'agrégation de données, simplifier la gestion du réseau comme l'affectation des adresses, et optimiser la consommation d'énergie, les nœuds sont regroupés dans des clusters. Les nœuds qui sont regroupés ensemble dans un cluster seront capables de communiquer facilement les uns avec les autres. On trouve plu- sieurs stratégies de groupement parmi lesquelles, les nœuds sont organisés en une hiérarchie en fonction de leur puissance et de leur proximité. Un chef de cluster est élu pour effectuer plusieurs tâches, comme le filtrage, la fusion et l'agrégation, avec la possibilité d'être changé s'il tombe en panne ou s'il arrive à sa limite d'énergie. Toutes les communications de tous les nœuds seront effectuées par l'intermédiaire du chef du cluster auquel ils appartiennent. Les algorithmes de formation de clusters peuvent être centralisés ou distribués.

I.8.5. Communication multi-saut

Contrairement aux réseaux traditionnels, un réseau de capteurs est constitué d'un grand nombre de nœuds déployés dans une zone locale, ayant une courte portée (rayon de communication), un faible débit et aucune existence d'infrastructure. Un nœud capteur peut communiquer directement avec ses voisins, c'est-à-dire ceux qui sont à sa portée de communication, et fait office de routeur pour les autres nœuds. Par exemple dans *la figure I.4*, le nœud B pourra relayer les messages du capteur D vers le capteur A. Dans ce cas, les nœuds capteurs communiquent en acheminant les messages par routage « multi-saut ».

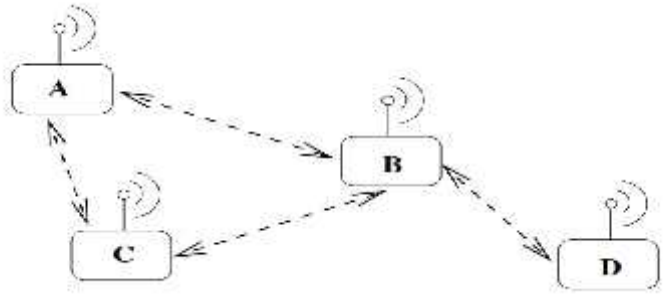

Figure I.4: Exemple de communication multi-saut dans un réseau de capteurs.

I.8.6. Synchronisation

La synchronisation du temps est un challenge important et coûteux dans les réseaux de capteurs à communication multi-saut. De nombreuses applications de réseaux de capteurs demandent une synchronisation des horloges locales des nœuds. Il y a plusieurs raisons pour étudier la synchronisation dans des réseaux de capteurs, les nœuds capteurs collaborent entre eux pour parvenir à une tâche de détection plus complexe. La fusion de don- née est un exemple d'une telle collaboration où les données collectées par différents nœuds sont regroupées en un seul résultat significatif. Par exemple dans le cas où nous voulons tracer le chemin d'un véhicule, les nœuds captent la position et le temps de détection du véhicule et les envoient à une station de base qui à son tour combine toutes les informations pour tracer le chemin complet. Il est évident que si les nœuds ne sont pas synchronisés, le chemin sera inexact. Cependant, la synchronisation peut être utilisée dans la gestion d'économie d'énergie pour augmenter la durée de vie du réseau. Par exemple, les capteurs peuvent être mis en veille à des instants déterminés, et se réveiller en cas de besoin.

I.9. Pile protocolaire

La pile protocolaire [3], [4] utilisée par la station de base ainsi que tous les autres capteurs du réseau est illustrée par la *figure I.5*. La pile protocolaire comprend la couche application, la couche transport, la couche réseau, la couche liaison de données, la couche physique, le plan de gestion de l'énergie, le plan de gestion de la mobilité et le plan de gestion des tâches.

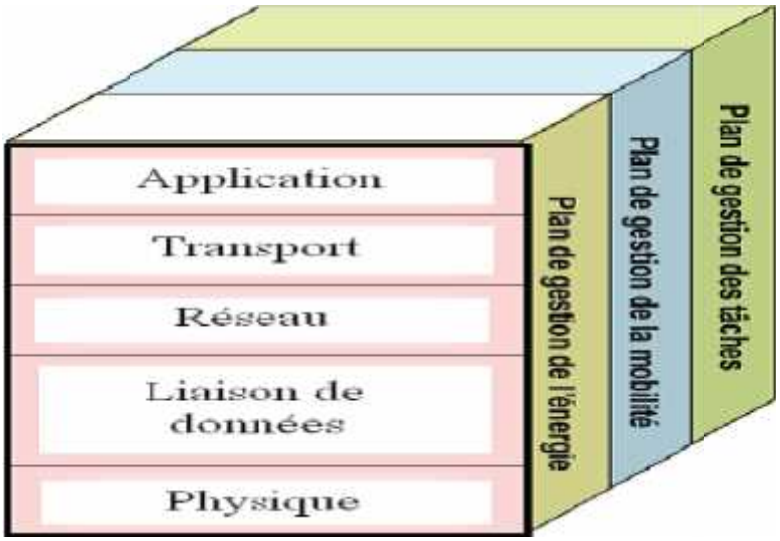

Figure I.5: Pile protocolaire.

Suivant la fonctionnalité des capteurs, différentes applications peuvent être utilisées et bâties sur la *couche application*.

I.9.1. Rôle des couches [5]

- **La couche physique :** Spécifications des caractéristiques matérielles, et assure la transmission et la réception des données au niveau bit.
- **La couche liaison:** Le protocole MAC (Media Access Control) de la couche liaison assure la gestion de l'accès au support physique, cette couche spécifie comment les données sont expédiées entre deux nœuds ou deux routeurs dans une distance d'un saut. Elle est responsable du multiplexage des données, du contrôle d'erreurs, de l'accès au media,... Elle assure la liaison point à point et multi-point dans un réseau de communication.
- **La couche réseau :** Dans la couche réseau le but principal est de trouver une route et une transmission fiable des données, captées, des nœuds capteurs vers le puits "sink" en optimisant l'utilisation de l'énergie des capteurs. Ce routage diffère de celui des réseaux de transmission ad hoc sans fils par les caractéristiques suivantes:
  - Il n'est pas possible d'établir un système d'adressage global pour le grand nombre de nœuds.
  - Les applications des réseaux de capteurs exigent l'écoulement des données mesurées de sources multiples à un puits particulier.
  - Les multiples capteurs peuvent produire de mêmes données à proximité d'un phénomène (redondance).

- Les nœuds capteur exigent ainsi une gestion soigneuse des ressources. En raison de ces différences, plusieurs nouveaux algorithmes ont été proposés pour le problème de routage dans les réseaux de capteurs.

✍ **La couche transport :** Cette couche est chargée du transport des données, de leur découpage en paquets, du contrôle de flux, de la conservation de l'ordre des paquets et de la gestion des éventuelles erreurs de transmission.

✍ **La couche application :** Cette couche assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, géré directement par les logiciels.

I.9.2. Plans de gestion

En outre, les plans de gestion de l'énergie, de la mobilité et des tâches surveillent la puissance, le mouvement et la distribution des tâches, respectivement, entre les nœuds capteurs. Ces plans de gestion sont nécessaires, de sorte que les nœuds capteurs puissent fonctionner ensemble d'une manière efficace pour préserver l'énergie, router des données dans un réseau de capteurs mobile et partager les ressources entre les nœuds capteurs. Du point de vue global, il est plus efficace d'utiliser des nœuds capteurs pouvant collaborer entre eux. La durée de vie du réseau peut être ainsi prolongée.

✍ **Plan de gestion d'énergie :** contrôle l'utilisation de la batterie. Par exemple, après la réception d'un message, le capteur éteint son récepteur afin d'éviter la duplication des messages déjà reçus. En outre, si le niveau d'énergie devient bas, le nœud diffuse à ses voisins une alerte les informant qu'il ne peut pas participer au routage. L'énergie restante est réservée au captage.

✍ **Plan de gestion de mobilité :** détecte et enregistre le mouvement du nœud capteur. Ainsi, un retour arrière vers l'utilisateur est toujours maintenu et le nœud peut garder trace de ses nœuds voisins. En déterminant leurs voisins, les nœuds capteurs peuvent balancer l'utilisation de leur énergie et la réalisation de tâche.

✍ **Plan de gestion des tâches:** balance et ordonnance les différentes tâches de captage de données dans une région spécifique. Il n'est pas nécessaire que tous les nœuds de cette région effectuent la tâche de captage au même temps, certains nœuds exécutent cette tâche plus que d'autres selon leur niveau de batterie.

I.10. Collection des informations

Il y a deux méthodes pour collecter les informations d'un réseau de capteurs:

I.10.1. A la demande

Lorsque l'on souhaite avoir l'état de la zone de couverture à un moment, le puits émet des broadcastes vers toute la zone pour que les capteurs remontent leur dernier relevé vers le puits. Les informations sont alors acheminées par le biais d'une communication multi-sauts comme ils sont indiqués sur la *figure I.6*.

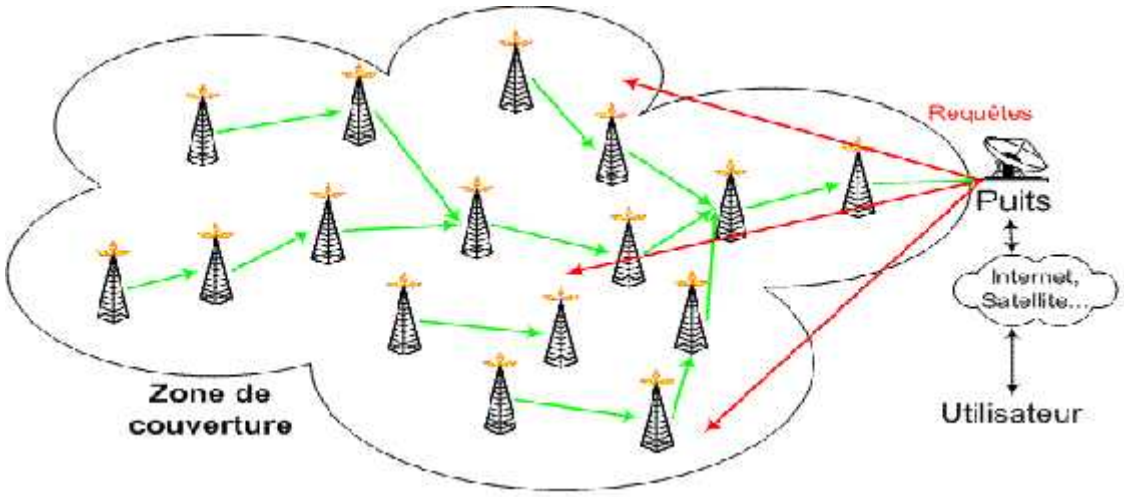

Figure I.6: Collection des informations à la demande.

I.10.2. Suite à un événement

Un événement se produit en un point de la zone de couverture (changement brusque de température, mouvement...), les capteurs situés à proximité remontent alors les informations relevées et les acheminent jusqu'au puits comme ils sont indiqués sur la *figure I.7*.

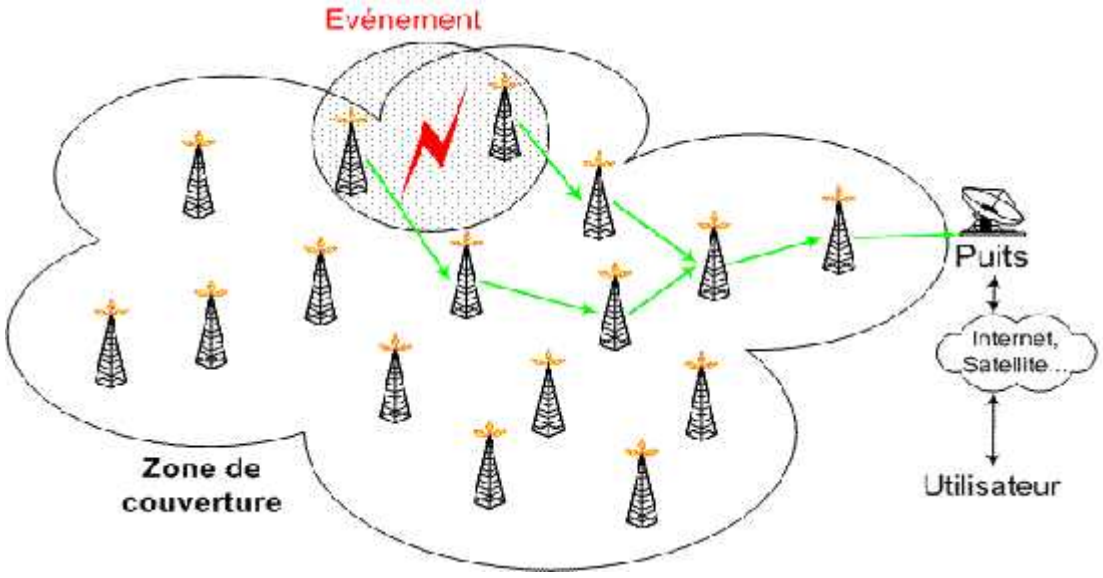

Figure I.7 : Collection des informations suite à un événement.

I.11. Contraintes de conception des RCSFs

Les réseaux de capteurs diffèrent des réseaux classiques où l'on peut être relativement générique et définir seulement un certain nombre de classes de service pour satisfaire le maximum de besoins. La conception et la réalisation des réseaux de capteurs sans fil sont influencées par plusieurs paramètres. Ces facteurs servent comme directives pour le développement des algorithmes et protocoles utilisés dans les RCSF. Les contraintes sont nombreuses et empêchent la création d'un type spécifique du réseau de capteurs. Sans être exhaustif, voici une liste de contraintes possibles lors de la conception d'un réseau de capteurs :

I.11.1. Contraintes liées à l'application

Il est impossible aujourd'hui de créer un réseau de capteurs capable de répondre aux besoins de toutes les applications potentielles. On peut relever des mesures pour une infinité de situations et dans des environnements très variables tout en ayant une concentration faible ou forte des capteurs. Dans certains cas, il existe des applications qui nécessitent un grand nombre de capteurs pour être mises en place. La difficulté réside alors dans la recherche d'un dénominateur commun à toutes ces applications ce qui est pour l'instant très complexe et relève de l'impossible. C'est pourquoi, l'application devient le principal paramètre lors de la conception de protocoles très spécifiques pour que le fonctionnement des capteurs produise le résultat attendu par l'application.

I.11.2. Contrainte énergétique

L'énergie est considérée comme la contrainte principale dans un réseau de capteurs. Déjà, comme pour tout réseau sans fil, il est important de tenir compte de cette contrainte car la plupart des machines fonctionnent sur batterie. Après la décharge de la batterie, l'utilisateur est obligé de trouver une source électrique pour la recharger.

Cependant, dans les réseaux de capteurs, il est pratiquement impossible de recharger de par le nombre élevé de capteurs déployés et de par la difficulté de l'environnement dans lesquels ils peuvent se trouver. On parle alors pour la pile ou la batterie d'âme du capteur. Une fois vide, le capteur est considéré comme mort ou hors service. L'objectif à atteindre devient l'augmentation de la durée de vie du réseau de capteurs. Ce paramètre peut être défini sous différentes formes telles que la consommation

globale de tous les capteurs ou l'évitement qu'un capteur important perde son énergie ou la perte de la connectivité du réseau, etc.

I.11.3. Ressources limitées

En plus de l'énergie, les nœuds capteurs ont aussi une capacité de traitement et de mémoire limitée. En effet, les industriels veulent mettre en œuvre des capteurs simples, petits et peu coûteux.

I.11.4. Bande passante limitée

Afin de minimiser l'énergie consommée lors de transfert de données entre les nœuds, les capteurs opèrent à bas débit. Typiquement, le débit utilisé est de quelques dizaines de Kb/s. Un débit de transmission réduit n'est pas handicapant pour un réseau de capteurs où les fréquences de transmission ne sont pas importantes.

I.11.5. Topologie dynamique

La topologie des réseaux de capteurs peut changer au cours du temps pour les raisons suivantes [4]:

- Les nœuds capteurs peuvent être déployés dans des environnements hostiles (champ de batail par exemple), la défaillance d'un nœud capteur est, donc très probable.
- Un nœud capteur peut devenir non opérationnel à cause de l'expiration de son énergie. Dans certaines applications, les nœuds capteurs et les stations de base sont mobiles.

I.11.6. Contraintes liées aux déterminismes

La plupart des réseaux de capteurs sont destinés à être déployés dans des environnements hostiles sur des sites industriels importants ou à opérer pendant des scénarios de crises. L'information que le capteur mesure doit parfois atteindre le collecteur d'informations en un temps borné bien défini. Au-delà de ce temps, l'information est considérée comme périmée ou non existante. Atteindre le déterminisme sur un réseau de capteurs sans fil n'est pas une tâche évidente. La raison vient du fait que pratiquement tous les standards de communication sans fil aujourd'hui utilisent des méthodes probabilistes pour accéder à cette interface radio.

I.11.7. Contraintes de passage à l'échelle

Le passage à l'échelle (scalability) indique que le réseau est suffisamment large et peut croître de manière illimitée. En d'autres termes, quand on passe à l'échelle, il est trop tard pour effectuer des mises à jour radicales au réseau. À chaque nouvel ajout, on doit prendre en considération les services existants et assurer leur pérennité. De plus, gérer un grand réseau par des humains devient une tâche difficile voire impossible à réaliser. Pour pouvoir opérer quand on passe à l'échelle, il faut que les capteurs soient capables de s'auto-configurer seuls. L'auto-configuration peut aller de la simple attribution d'un identifiant jusqu'à l'application du protocole pour le bon fonctionnement du nœud dans son environnement. L'algorithmique distribué est la science la plus adaptée pour résoudre les problèmes du passage à l'échelle.

I.11.8. Contraintes liées à la qualité de service

La notion de qualité de service est légèrement différente ici de celle déployée dans les réseaux classiques. Souvent on parle de haut débit ou de faible débit, etc. Ici, avec des petits débits on peut parfois atteindre la qualité exigée. La qualité se définit par la capacité d'interpréter l'information collectée par le puits. Il n'existe donc pas de définition objective de la qualité. En fonction du réseau et du type de mesure, la qualité est alors précisée.

I.11.9. Agrégation de donnée

Dans les réseaux de capteurs, les données produites par les nœuds capteurs voisins sont très corrélées spatialement et temporellement. Ceci peut engendrer la réception par la station de base d'informations redondantes. Réduire la quantité d'informations redondantes transmises par les capteurs permet de réduire la consommation d'énergie dans le réseau et ainsi d'améliorer sa durée de vie. L'une des techniques utilisée pour réduire la transmission d'informations redondantes est l'agrégation des données [5]. Avec cette technique, les nœuds intermédiaires agrègent l'information reçue de plusieurs sources. Cette technique est connue aussi sous le nom de fusion de données.

La plupart des approches de la gestion de données dans les réseaux de capteurs ont largement suivi des thèmes similaires, bien que leurs approches spécifiques varient grandement. Leur architecture repose sur les deux principes suivants :

- Utiliser un langage déclaratif pour décrire les requêtes sur les données : un langage déclaratif peut être particulièrement utile pour décrire l'interaction entre l'utilisateur et le réseau sachant que les détails de l'interaction entre les nœuds capteurs tel que, le routage et le placement du traitement des données (dans le réseau) ne sont pas connus par les utilisateurs.
- Supporter des traitements de données locaux : comme le traitement de données local (se fait par les nœuds du réseau) est beaucoup moins coûteux en énergie que la communication radio.

I.11.10. Contraintes liées à la protection de l'information

Comme pour tout réseau sans fil, l'information circule sur une interface partagée et non dédiée. N'importe quel intrus peut alors soit récupérer l'information, soit la modifier ou la rendre inexploitable. C'est pourquoi des mesures de sécurité doivent être mise en place pour protéger l'information. Cependant, tous les mécanismes de sécurité sont créés pour des réseaux où les nœuds disposent d'une forte capacité de traitement, ce qui n'est pas le cas des capteurs. À ce jour, très peu de solutions sont adaptées aux capteurs en termes de sécurité.

I.11.11. Contraintes liées à l'environnement

Les capteurs interagissent avec l'environnement où ils mesurent leurs grandeurs physiques. De façon générale, ces mesures sont relevées à des instants relativement espacés dans le temps puis soudainement, soit pour des raisons de catastrophe ou d'événement exceptionnel, ils se mettent en mode de forte fréquence de mesures et envoient de l'information en rafale. Il faut alors préparer le réseau à supporter ce type d'événement rare mais largement consommateur de ressources et sujet à des situations de congestions et de difficultés majeures.

I.11.12. Contraintes de simplicité

Enfin proposer des protocoles et des mécanismes simples et légers doit être la marque de fabrique du réseau de capteurs. Ces derniers sont de machines largement plus faibles qu'une machine de bureau ou même que des téléphones portables.

I.12. Domaines d'applications des réseaux de capteurs son fil

Le concept de réseaux de capteurs sans fil est basé sur une simple équation [12] :

« Capteurs + Processeur + Radio = Une centaine d'applications potentielles »

Les réseaux de capteurs peuvent être programmés à un grand nombre de fins dans des domaines différents, tels que le domaine militaire, scientifique, commercial, industriel, médical, environnement, sécurité, domotique etc, qui sont détaillées dans cette section.

Figure I.8 : domaine d'application de RCSFs.

I.12.1. Applications militaires

Comme dans le cas de plusieurs technologies, le domaine militaire a été un moteur initial pour le développement des réseaux de capteurs. Le déploiement rapide, le coût réduit, l'auto-organisation et la tolérance aux pannes des réseaux de capteurs sont des caractéristiques qui rendent ce type de réseaux un outil appréciable dans un tel domaine. Comme exemple d'application dans ce domaine, on peut penser à un réseau de capteurs déployé sur un endroit stratégique ou difficile d'accès, afin de surveiller toutes les activités des forces ennemies, ou d'analyser le terrain avant d'y envoyer des troupes (détection d'agents chimiques, biologiques ou de radiations). Des tests concluants ont déjà été réalisés dans ce domaine par l'armée américaine dans le désert de Californie [7].

Figure I.9 Tracé du chemin d'un véhicule militaire.

I.12.2. Applications liées à la sécurité

Les altérations dans la structure d'un bâtiment, suite à un séisme ou au vieillissement, pourraient être détectées par des capteurs intégrés dans les murs ou dans le béton, sans alimentation électrique ou autres connexions filaires. Les capteurs doivent s'activer périodiquement et peuvent ainsi fonctionner durant des années, voire des décennies.

Un réseau de capteurs de mouvements peut constituer un système d'alarme distribué qui servira à détecter les intrusions sur un large secteur. La surveillance de voies ferrées pour prévenir des accidents avec des animaux et des êtres humains peut être une application intéressante des réseaux de capteurs. La protection des barrages pourrait être accomplie en y introduisant des capteurs. La détection prompte de fuites d'eau, Permettrait d'éviter des dégâts. Les êtres humains sont conscients des risques et attaques qui les menacent. Pour cela, ils mettent à disposition toutes les ressources humaines et financières nécessaires pour leur sécurité. Cependant, des failles sont toujours présentes dans les mécanismes de sécurisation appliqués aujourd'hui, sans oublier leur coût très élevé. L'application des réseaux de capteurs dans le domaine de la sécurité pourrait diminuer considérablement les dépenses financières consacrées à la sécurisation des lieux et à la protection des êtres humains tout en garantissant de meilleurs résultats.

I.12.3. Applications environnementales

Des capteurs dispersés à partir d'un avion dans une forêt peuvent signaler un éventuel début d'incendie dans le champ de captage; ce qui permettra une meilleure efficacité pour la lutte contre les feux de forêt. Dans les champs agricoles, les capteurs peuvent être semés avec les graines. Ainsi, les zones sèches seront facilement identifiées et l'irrigation sera donc plus efficace. Sur les sites industriels, les centrales nucléaires ou dans les pétroliers, des capteurs peuvent être déployés pour détecter des fuites de produits toxiques (gaz, produits chimiques, éléments radioactifs, pétrole, etc.) et alerter les utilisateurs dans un délai suffisamment court pour permettre une intervention efficace. Une grande quantité de capteurs peut être déployée dans une forêt ou dans un environnement de conservation de la faune afin de recueillir des informations diverses sur l'état du milieu naturel et sur les comportements de déplacement. Par exemple, l'université de Pise en Italie a réalisé des réseaux de capteurs pour le contrôle des parcs naturels (feux, animaux,..). Il est ainsi possible "d'observer", sans déranger, des espèces animales difficiles à étudier dans leur environnement naturel et de proposer des solutions plus

efficaces pour la conservation de la faune. Les éventuelles conséquences de la dispersion en masse des micro-capteurs dans l'environnement ont soulevé plusieurs inquiétudes. En effet, chaque micro-capteur est doté d'une batterie qui contient des métaux nocifs. Néanmoins, le déploiement d'un million de capteurs de 1 mm3 chacun ne représente qu'un volume total d'un litre. Même si tout ce volume était constitué de batteries, cela n'aurait pas des répercussions désastreuses sur l'environnement.

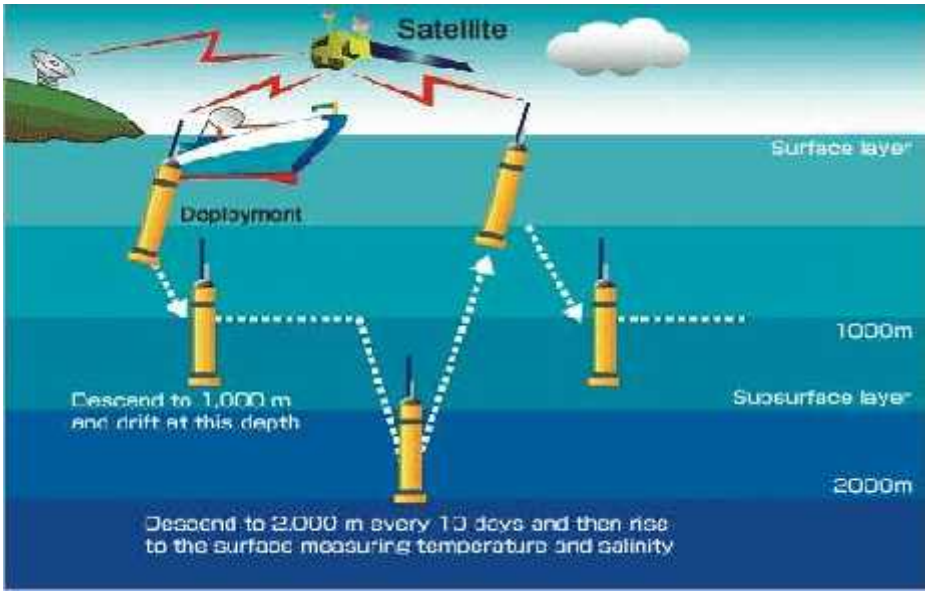

Figure I.10 : Application sur le contrôle de la qualité de l'eau.

I.12.4. Applications commerciales

Des nœuds capteurs pourraient améliorer le processus de stockage et de livraison. Le réseau ainsi formé, pourra être utilisé pour connaître la position, l'état et la direction d'un paquet ou d'une cargaison. Un client attendant un paquet peut alors avoir un avis de livraison en temps réel et connaître la position du paquet. Des entreprises manufacturières, via des réseaux de capteurs pourraient suivre le procédé de production à partir des matières premières jusqu'au produit final livré. Grâce aux réseaux de capteurs, les entreprises pourraient offrir une meilleure qualité de service tout en réduisant leurs coûts. Les produits en fin de vie pourraient être mieux démontés et recyclés ou réutilisés si les micro-capteurs en garantissent le bon état. Dans les immeubles, le système de climatisation peut être conçu en intégrant plusieurs micro-capteurs dans les tuiles du plancher et les meubles. Ainsi, La climatisation pourra être déclenchée seulement aux endroits où il y a des personnes présentes et seulement si c'est nécessaire [4].

I.12.5. Applications médicales

Les capteurs peuvent être implantés dans le corps humain pour contrôler les problèmes médicaux comme le cancer et pour aider les patients à maintenir leur santé. Ils peuvent être utilisés aussi pour surveiller les patients et l'avancement de leurs états dans un hôpital. En outre, en implantant sous la peau des mini capteurs vidéo, on peut recevoir des images en temps réel d'une partie du corps sans aucune chirurgie. On peut ainsi surveiller la progression d'une maladie ou la reconstruction d'un muscle. Un projet actuel consiste à créer une rétine artificielle composée de 100 micro-capteurs pour corriger la vue.

Dans [9], les auteurs ont réalisé un réseau de capteurs pour la surveillance des « signes vitaux ». Le système comprend quatre composantes : un identifiant formé d'un nœud capteur attaché au patient qui contient toutes les données qui le concernent (par exemple son nom), un capteur (par exemple un électrocardiogramme), un dispositif d'affichage qui examine les données du patient et ses signes vitaux, et enfin un stylo conservé par le personnel responsable (médecin), qui permet d'établir l'association entre les différents dispositifs ; ce stylo émet par infrarouge, un identifiant unique pour chaque patient, et peut recevoir les informations et les identificateurs du réseau humain.

Un autre exemple d'application médicale présenté dans [8], est illustré dans la *Figure I.11* Les auteurs présentent un système en temps réel pour suivre les patients. Ce système intègre des capteurs de signes vitaux, la position des capteurs, et un réseau ad-hoc pour permettre la surveillance à distance du patient. Cela facilitera la communication entre les pompiers sur scène (en cas de catastrophe), et les spécialistes dans les hôpitaux locaux qui seront disponibles pour la consultation à distance.

Figure I.11 : Le flux d'information d'un patient

I.12.6. Applications domestiques

Les réseaux de capteurs peuvent également être utilisés dans la domotique et l'environnement intelligent. Ils jouent un rôle essentiel dans les grandes usines et les entrepôts en surveillant les changements climatiques. Par exemple, des capteurs peuvent être utilisés pour contrôler les vibrations susceptibles d'endommager la structure d'un bâtiment. Dans [11], les auteurs décrivent une application qui surveille l'état de grandes structures comme des immeubles administratifs. Ils exploitent les avantages d'un réseau de capteurs tels que le déploiement rapide (environ une demi-heure face à plusieurs jours pour l'installation des réseaux filaires). Un réseau de capteurs a été déployé dans un campus universitaire [10], permettant aux différentes machines (serveurs, imprimantes, etc.) de tous les départements de communiquer ensemble.

I.12.7. Autres applications

Les réseaux de capteurs peuvent également être utilisés pour : surveiller 'infrastructure, lutter contre le terrorisme, contrôler du trafic, détecter des intrusions (en plaçant, à différents points stratégiques, des capteurs, on peut ainsi prévenir des cambriolages), contrôler les stocks (savoir le lieu, la quantité, la forme de tous les produits, contrôler leur flux, etc.), l'urbanisme, l'ingénierie civile (surveillance des structures, les capteurs peuvent être placés dans les ponts afin de détecter et de signaler les faiblesses structurelles, dans les réservoirs d'eau pour détecter les matières dangereuses), le recouvrement des catastrophes (par exemple chercher des signes de vie après un tremblement de terre), et beaucoup d'autres applications qui rendent notre entourage plus intelligent.

I.13. Conclusion

Les réseaux de capteurs sans fil présentent un intérêt considérable et une nouvelle étape dans l'évolution des technologies de l'information et de la communication. Cette nouvelle technologie suscite un intérêt croissant vu la diversité de ces applications : santé, environnement et industrie.

Dans ce premier chapitre, on a présenté les réseaux de capteurs sans fil, leurs architectures de communication, la pile protocolaire des capteurs, leurs diverses applications et les différents types de routage de données utilisés dans ce de réseau, et j'ai remarqué que plusieurs facteurs et contraintes compliquent la gestion de ce type de

réseaux. En effet, les réseaux de capteurs se caractérisent par une capacité énergétique limitée rendant l'optimisation de la consommation d'énergie dans des réseaux une tâche critique pour prolonger la durée de vie du réseau.

Cela fait des années que les réseaux de captures sans fil suscitent un engouement important dans la recherche. J'ai remarqué à travers mes lectures que « minimiser la consommation d'énergie d'un nœud de capture » est « le cheval de bataille » de toutes les solutions et les protocoles. C'est pour cette raison oni présenté des notions de base sur le routage non hiérarchique, le routage hiérarchique de données et quelques techniques de conservation d'énergie.

CHAPITRE II

Protocoles de routage dans les RCSFs

- Etat de l'art-

II.1. Introduction

Le routage est une méthode d'acheminement des informations vers une destination donnée dans un réseau de connexion. Comme nous l'avons déjà vu, l'architecture des réseaux Ad-hoc est caractérisée par l'absence d'infrastructure fixe préexistante, à l'inverse des réseaux de télécommunication classiques. Un réseau Ad-hoc doit s'organiser automatiquement de façon à être déployé rapidement et pouvoir s'adapter aux conditions du trafic et aux différents mouvements pouvant intervenir au sein des nœuds mobiles.

Dans le but d'assurer la connectivité du réseau, malgré l'absence d'infrastructure fixe, chaque nœud est susceptible d'être mis à contribution pour participer au routage et pour retransmettre les paquets d'un nœud qui n'est pas en mesure d'atteindre sa destination directement ; tout nœud joue ainsi le rôle de poste de travail et de routeur. C'est le cas du réseau de capteurs qui est un réseau Ad-hoc avec des contraintes plus fortes d'énergie, de capacité, de calcul et de stockage.

Chaque nœud participe donc au routage ce que lui permet de découvrir les chemins existants afin d'atteindre les autres nœuds du réseau. Le fait que la taille d'un réseau puisse être importante, surtout dans le cas des réseaux de capteurs, souligne que les techniques de routage dans les réseaux classiques nécessitent des modifications. Le problème qui se pose dans le contexte de ces réseaux est l'adaptation de la méthode d'acheminement utilisée à un grand nombre de nœuds possédant de modestes capacités de calculs et de sauvegarde et parfois présentant des changements de topologie.

Il est impossible qu'un nœud puisse garder les informations de routage concernant tous les autres nœuds, car le réseau peut être volumineux. Ce problème ne se pose pas dans le cas des réseaux de petites tailles, car l'inondation (la diffusion pure qui fait propager un paquet dans le réseau entier) faite pour ce but dans ces réseaux n'est pas coûteuse ; par contre dans un réseau volumineux, le manque de données de routage concernant les destinations peut impliquer une large diffusion dans le réseau. Cela si on considère seulement la phase de découverte des routes peut dégrader considérablement les performances du système caractérisé principalement par une faible bande passante et une capacité énergétique limitée.

Dans le cas où le nœud destination se trouve dans la portée de communication du nœud source, le routage devient évident et aucun protocole de routage n'est initié, ce qu'on appelle envoi direct ou à un seul saut. Mais ce cas est généralement rare dans les réseaux Ad-hoc et

les réseaux de capteurs. Un nœud source peut avoir besoin de transférer des données à un autre nœud qui ne se trouve pas dans sa portée de communication. La *Figure II.1* montre un exemple d'un réseau constitué de quatre nœuds. Le nœud A envoie directement un paquet à B sans besoin de routage puisque B est dans la portée de communication de A (envoi direct). D'ailleurs, si le nœud A veut envoyer un paquet au nœud D, il doit utiliser les « services » des nœuds intermédiaires B et C puisque le nœud D n'est pas dans la portée de A. A envoie le paquet à B ; B transmet le paquet à C ; C, à son tour, transmet le paquet au nœud D. Cette technique est appelée routage multi-sauts (multi-hops).

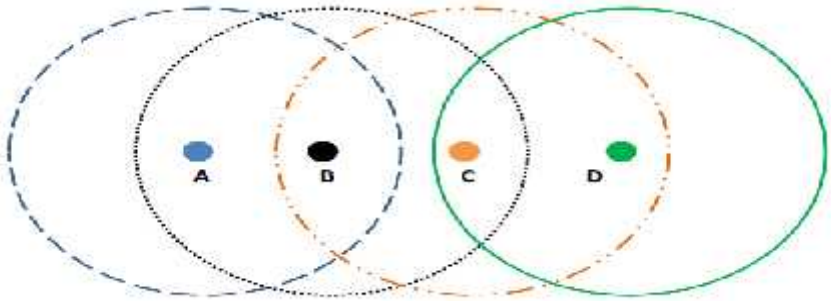

Figure II.1 : Communication multi-sauts entre A et D

II.2. Protocoles de routage non hiérarchiques

II.2.1. Introduction

L'objectif principal d'un protocole de routage pour un réseau Ad-hoc est l'établissement correct et efficace d'itinéraires entre une paire de nœuds afin que des messages puissent être acheminés. Le protocole de routage permet aux nœuds de se connecter directement les uns aux autres pour envoyer les messages par des sauts multiples. Par la suite, nous présentant un état de l'art des principaux protocoles de routage à plat (non hiérarchique) dans les réseaux Ad-hoc car la présentation de ces protocoles nous permettra de mieux analyser l'avantage de l'approche hiérarchique surtout dans les grands réseaux. Malgré que notre intérêt se focalise sur les protocoles hiérarchiques, nous avons rédigé cet état de l'art parce qu'un réseau de capteurs partage forcément des caractéristiques et des contraintes des réseaux Ad-hoc qu'il faut prendre en compte lors d'une proposition d'un protocole de routage.

II.2.2. DSDV (Destination Sequenced Distance Vector)

DSDV [15] est un protocole proactif de routage à vecteur de distance. Chaque nœud du réseau maintient une table de routage contenant le saut suivant et le nombre de sauts pour

toutes les destinations possibles. Des diffusions de mises à jour périodiques tendent à maintenir la table de routage complètement actualisée à tout moment.

Afin d'éviter le bouclage (loop-freedom), DSDV utilise les numéros de séquence (Sequence Number) pour indiquer la « nouveauté » d'une route. Une route R est considérée plus favorable qu'une autre R', si R a un numéro de séquence plus grand ; si ces deux routes ont le même numéro de séquence, alors R est plus favorable s'il possède un nombre inférieur de sauts. Le numéro de séquence pour une route est initialisé par le nœud émetteur et incrémenté pour chaque nouvel avertissement de route. Quand un nœud détecte un lien brisé vers une destination D, il met à jour le nombre de sauts pour l'entrée de la destination D dans sa table avec la valeur infini et incrémente son numéro de séquence.

Les boucles de routes peuvent survenir lorsque des informations incorrectes de routage sont présentes dans le réseau après un changement dans la topologie du réseau (lien brisé par exemple). Dans ce contexte, l'utilisation des numéros de séquence adapte DSDV à une topologie dynamique de réseau comme dans un réseau Ad-hoc.

DSDV utilise des mises à jour étiquetées lorsque la topologie change. La transmission des mises à jour est retardée afin d'introduire un effet d'amortissement quand la topologie change rapidement.

II.2.3. GSR (Global State Routing)

Le protocole GSR [15] est un protocole similaire au protocole DSDV décrit précédemment. Ce protocole utilise les idées du routage basé sur l'état des liens (Link State, LS), et les améliore en évitant le mécanisme inefficace d'inondation des messages de routage. GSR utilise une vue globale de la topologie du réseau, comme c'est le cas dans les protocoles basés sur LS. Le protocole utilise aussi une méthode, appelée la méthode de dissémination, utilisée dans le DBF (Distributed Bellman-Ford [14]).

Dans ce protocole, chaque nœud ni maintient : une liste de voisins Vi, une table de topologie TTi, une table des nœuds suivants NEXTi (Next Hop), et une table de distance Table_Di. La table de la topologie TTi, contient pour chaque destination, l'information de l'état des liens telle qu'elle a été envoyée par la destination, et une estampille de l'information. Pour chaque nœud destination j, la table NEXTi contient le nœud vers lequel les paquets destinés à j seront envoyés. La table de distance contient la plus courte distance pour chaque nœud destination.

De la même manière que les protocoles LS, les messages de routage sont générés suivant les changements d'états des liens. Lors de la réception d'un message de routage, le nœud met à jour sa table de topologie (représentée par un graphe dans LS) et cela dans le cas où le numéro de séquence du message reçu est supérieur à la valeur du numéro de séquence sauvegardé dans la table (exactement comme le fait le protocole DSDV). Par la suite, le nœud reconstruit sa table de routage et diffuse les mises à jour à ses voisins. Le calcul des chemins peut se faire avec n'importe quel algorithme de recherche des plus courts chemins. Par exemple, dans [15], l'algorithme du GSR utilise l'algorithme de Dijkstra modifié de telle façon qu'il puisse construire la table des nœuds suivants (NEXT HOP) et la table de distance Table_D, en parallèle avec la construction de l'arbre des plus courts chemins (l'arbre dont la racine est le nœud source).

La principale modification de GSR sur l'algorithme LS traditionnel, est la façon de diffusion des informations de routage qui circulent dans le réseau. Dans LS, si on détecte des changements de topologie, les paquets d'états de liens sont générés et diffusés par inondation dans tout le réseau. Par contre, GSR maintient la table - la plus récente - d'état des liens reçus à travers les voisins, et l'échange uniquement avec ses voisins locaux, d'une façon périodique.

II.2.4. FSR (Fisheye State Routing)

Le protocole FSR [17] peut être vu comme une amélioration du protocole GSR présenté précédemment. Le nombre élevé de messages de mise à jour échangés implique une grande consommation de la bande passante, ce qui a un effet négatif dans les réseaux Ad-hoc caractérisés par une bande passante limitée. Le protocole FSR est basé sur l'utilisation de la technique "œil de poisson" (fisheye), proposée par Kleinrock et Stevens [17] qui l'ont utilisée dans le but de réduire le volume d'information nécessaire pour représenter les données graphiques. L'œil de 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 [17]. 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 la précision, quand la distance augmente.

Le protocole FSR est similaire à LS, dans sa sauvegarde de la topologie au niveau de chaque nœud. La modification principale réside dans la manière avec laquelle les informations de routage circulent. Dans FSR, la diffusion par inondation de messages n'existe

pas. L'échange se fait uniquement avec les voisins directs.

Les données de mise à jour, échangées périodiquement dans FSR, ressemblent au vecteur échangé dans le protocole DSDV, où les distances sont modifiées suivant l'estampille du temps ou le numéro de séquence associé au nœud qui a été à l'origine de la mise à jour. Dans FSR (comme dans LS) les états de liens sont échangés, l'image complète de la topologie du réseau est gardée au niveau de chaque nœud, et les meilleurs chemins sont échangés en utilisant cette image.

Comme nous l'avons déjà dit, l'état des liens change fréquemment dans les réseaux Ad-hoc. FSR effectue la mise à jour de ces changements de la même manière que le protocole GSR; ce qui résout les problèmes de LS concernant le volume de paquets de contrôle. Avec GSR, et quand la taille du réseau devient très grande, les messages de mise à jour peuvent consommer une bande passante considérable. Afin de réduire le volume de messages échangés sans toucher à la consistance et à la précision des données de routage, FSR utilise la technique « œil de poisson » vue précédemment. La *Figure II.2* illustre cette technique. Dans cette figure, on définit la portée, ou le champ de vision de l'œil de poisson, avec un nœud du centre d'identificateur égal à 1. La portée est définie en termes de nœuds qui peuvent être atteints en passant par un certain nombre de sauts. Dans la *Figure II.2*, trois portées sont montrées pour 1, 2 et supérieures à 2 respectivement. En conséquence, les nœuds sont colorés en noir, gris et blanc. Le nombre de niveaux et le rayon de chaque portée va dépendre de la taille du réseau. Le nœud de centre (le nœud 1) maintient les données les plus précises des nœuds appartenant au cercle le plus proche ; la précision diminue progressivement, pour les cercles moins proches du centre.

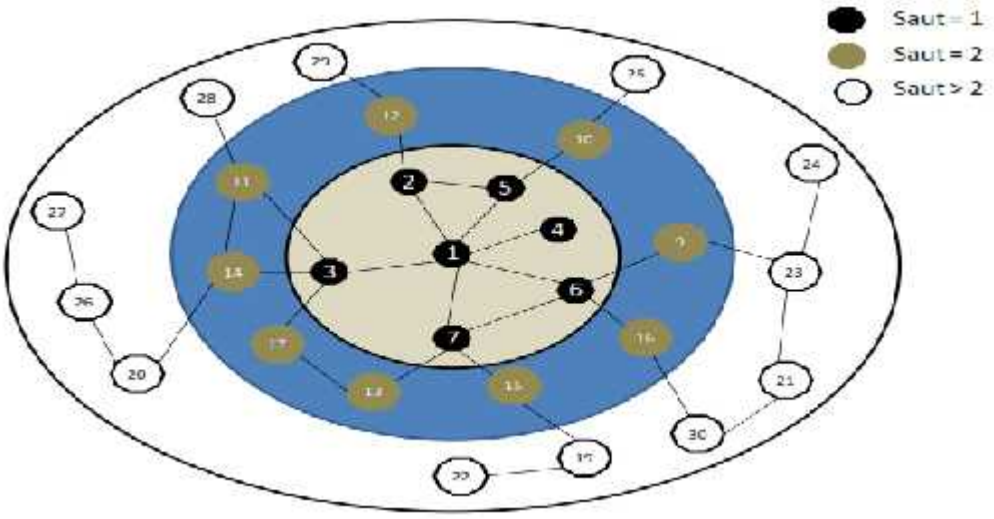

Figure II. 2 : Technique "œil de poisson" dans le protocole FSR

La réduction du volume des données de mise à jour est obtenue en utilisant des périodes d'échanges différentes pour les différentes entrées de la table. Les entrées qui correspondent aux nœuds les plus proches sont envoyées aux voisins avec une fréquence élevée (donc avec une période d'échange relativement petite). Par exemple, les entrées des nœuds en gras (voir la *Figure II.2*) sont échangées fréquemment. Le reste des entrées est échangé avec une fréquence moins élevée. De cette manière, un grand nombre d'échanges de données de routage est évité, ce qui réduit le volume des messages qui circulent dans le réseau.

Cette stratégie fournit périodiquement des mises à jour pour les nœuds proches mais elle crée de grandes latences pour celles des nœuds éloignés. Cependant, l'imprécision sur le meilleur chemin vers une destination lointaine est minimisée par le fait que la route devient plus précise lorsque le paquet s'approche de la destination.

Le protocole FSR peut être utilisé dans les réseaux Ad-hoc dont le nombre de nœuds est grand. Le protocole utilise un volume raisonnable de messages de contrôle. En outre, il évite le travail énorme de recherche de chemins, effectué dans les protocoles réactifs ; ceci accélère la transmission. De plus, FSR maintient des calculs précis concernant les destinations proches. Malgré ses avantages, FSR ne répond pas aux contraintes des réseaux de capteurs (surtout la contrainte d'énergies).

II.2.5. AODV (Ad-hoc On Demand Distance Vector)

AODV [19] est un protocole à vecteur de distance, comme DSDV, mais il est réactif plutôt que proactif comme DSDV. En effet, AODV ne demande une route que lorsqu' il en a besoin. AODV utilise les numéros de séquence d'une façon similaire à DSDV pour éviter les boucles de routage et pour indiquer la « nouveauté » des routes. Une entrée de la table de routage contient essentiellement l'adresse de la destination, l'adresse du nœud suivant, la distance en nombre de sauts (i.e. le nombre de nœuds nécessaires pour atteindre la destination), le numéro de séquence destination, le temps d'expiration de chaque entrée dans la table.

Lorsqu'un nœud a besoin de trouver une route vers une destination dont l'entrée dans la table de routage n'existe pas ou est expirée, il diffuse un message de demande de route (Route Requête message, RREQ) à tous ses voisins. Le message RREQ est diffusé à travers le réseau jusqu'à atteindre la destination. Durant son parcours à travers le réseau, le message RREQ réalise la création des entrées temporaires des tables de routage pour la route inverse des nœuds à travers lesquels il passe. Si la destination, ou une route vers elle, est

trouvée, une route est rendue disponible en envoyant un message réponse de route (Route Reply, RREP) au nœud source. Cette réponse de route traverse le long du chemin temporaire inversé du message RREQ. Dans son chemin de retour vers la source, RREP introduit la création des entrées pour la destination dans les tables de routage des nœuds intermédiaires. Les entrées de routage expirent après une certaine période (time-out). Précisons que le protocole AODV ne supporte que les liens symétriques dans la construction des chemins inverses.

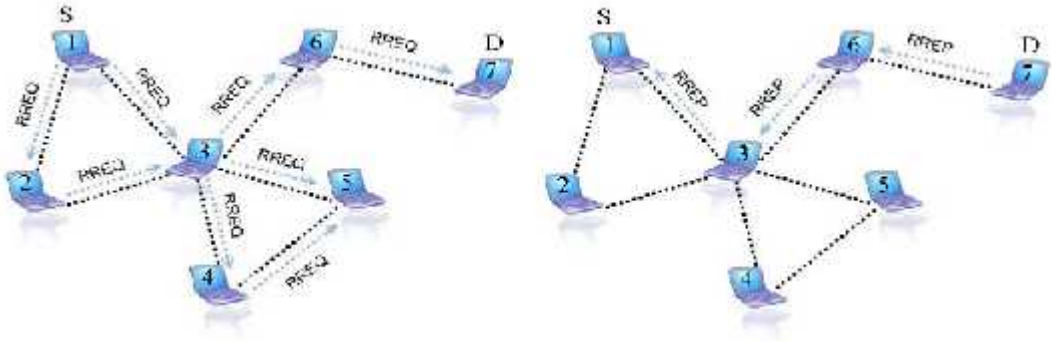

Figure II.3 : Fonctionnement de la procédure de demande de route dans AODV

La *Figure II.3* illustre le mécanisme de création des routes d'AODV. Il y a d'abord diffusion de la demande de route. Ensuite, la destination envoie une réponse, qui, grâce aux informations recueillies par les nœuds lors de la diffusion de la demande de route, crée une route de la destination vers la source. A noter que le protocole de routage AODV n'assure pas la détection du meilleur chemin existant entre la source et la destination.

Les nœuds voisins sont détectés par des messages périodiques HELLO (un message particulier de RREP). Si un nœud x ne reçoit pas un message HELLO d'un voisin y par lequel il envoie des données, ce lien est considéré brisé et une indication de défaillance de lien est envoyée à ses voisins actifs. Ces derniers propagent l'indication à leurs voisins qui utilisaient le lien entre x et y. Lorsque le message du lien brisé atteint finalement les sources affectées, celles-ci peuvent choisir d'arrêter l'envoi des données ou de demander une nouvelle route en envoyant un nouveau message RREQ.

II.2.6. DSR (Dynamic Source Routing)

DSR [20] est un protocole de routage réactif qui utilise le routage de source afin d'envoyer des paquets de données. Dans ce type de routage, les entêtes des paquets de données portent la séquence des nœuds à travers lesquels le paquet doit passer. Ceci signifie que les nœuds intermédiaires ont juste besoin de garder des traces de leurs voisins

intermédiaires afin de transférer les paquets de données. Le nœud source a besoin de savoir l'ordre complet des nœuds jusqu'à la destination.

Comme dans AODV, la demande d'une route dans DSR exige une inondation avec des paquets Route Request. Un nœud recevant ce paquet cherche dans sa « cachette de route » (similaire à la table de routage dans AODV), où toutes ses routes connues sont stockées, une route contenant la destination demandée. S'il n'y a pas de route trouvée, le nœud transfère le paquet Route Request plus loin après avoir ajouté sa propre adresse à la séquence de nœuds stockée dans le paquet Route Request. Le paquet se propage dans le réseau jusqu'à l'arrivée à destination ou à un nœud possédant une route vers cette destination. Si une route est trouvée, un paquet Route Reply contenant la séquence de nœuds appropriée pour atteindre la destination est renvoyé en unicast au nœud source. DSR ne prend pas en compte la bidirectionnalité des liens puisque le paquet Route Reply est envoyé au nœud source selon une route déjà stockée dans la « cachette de routes » d'un nœud intermédiaire ou à l'aide d'une réponse du nœud destinataire.

Afin d'éviter des inondations inutiles du réseau avec des messages Route Request, la procédure de demande de route commence d'abord à questionner les nœuds voisins s'ils ont une route disponible dans le voisinage direct. Ceci est fait en envoyant le premier paquet Route Request avec une limite de sauts égale à zéro, afin que celui-ci ne soit pas transféré ensuite aux voisins. S'il n'y a pas de réponses obtenues lors de cette demande initiale, un nouveau paquet Route Request est diffusé dans le réseau entier.

Un nœud DSR est capable de connaître des routes en lisant des paquets qui ne lui sont pas adressés. Cependant, cette technique exigeant un récepteur actif dans le nœud, peut être plutôt consommatrice d'énergie. Dans les réseaux où les nœuds ont une capacité énergétique limitée, le but est de mettre en veille l'émetteur-récepteur afin de conserver l'énergie le plus possible.

II.2.7. OLSR (Optimized Link State Routing)

Comme son nom l'indique, OLSR est un protocole proactif à état des liens optimisé ; il permet d'obtenir aussi des routes de plus court chemin. Alors que dans un protocole à état des liens, chaque nœud déclare ses liens directs avec ses voisins à tout le réseau, dans le cas d'OLSR, les nœuds ne déclarent qu'une sous-partie de leur voisinage grâce à la technique des relais multipoints (MultPoint Relaying, MPR) [21] décrite par la suite.

a. Relais multipoints

Cette technique consiste essentiellement, pour un nœud donné, à ignorer un ensemble de liens et de voisins directs, qui sont redondants pour le calcul des routes de plus court chemin. Plus précisément, dans l'ensemble des voisins d'un nœud, seul un sous-ensemble de ses voisins est considéré comme pertinent. Il est choisi de façon à pouvoir atteindre tout le voisinage à deux sauts (tous les voisins des voisins) ; cet ensemble est appelé l'ensemble des relais multipoints. L'algorithme de calcul de relais multipoints est donné dans [21].

Ces relais multipoints sont utilisés de deux façons : pour diminuer le trafic dû à la diffusion des messages de contrôle dans le réseau, et aussi pour diminuer la taille du sous-ensemble des liens diffusés à tout le réseau puisque les routes sont construites à base des relais multipoints [21].

L'idée de MPR est de minimiser l'inondation du trafic de contrôle dans un réseau en réduisant les retransmissions dupliquées dans la même région. Chaque nœud dans le réseau sélectionne un ensemble de nœuds de son voisinage auxquels ses messages seront transmis. Un nœud sélectionne ses MPRs parmi ses voisins à un saut avec un lien symétrique. Cet ensemble est choisi de manière à couvrir tous les nœuds qui sont à deux sauts. Les nœuds sélectionnés comme MPRs annoncent régulièrement leur condition de MPR dans les messages de contrôle envoyés à son voisinage. De cette façon, un nœud annonce au réseau qu'il est capable d'atteindre les nœuds qui l'ont élu comme MPR. Dans le calcul de la route, les MPRs sont utilisés pour la mise en place des routes vers toutes les destinations du réseau. Ainsi, en sélectionnant la route par l'intermédiaire des MPRs, on évite les problèmes liés à la transmission de paquets sur des liens unidirectionnels. Chaque nœud maintient l'information sur ses voisins qui ont été sélectionnés comme MPR. Un nœud obtient cette information par les messages de contrôle reçus périodiquement de ses voisins [21].

La *Figure II.4* montre la différence entre une diffusion pure et la diffusion en utilisant les MPRs. Par exemple, afin d'atteindre tous les nœuds à 3 sauts, la diffusion pure a besoin de 24 retransmissions du paquet envoyé par la source (voir la *Figure II.3*, côté gauche). En utilisant les MPRs ou les relais multipoints (nœuds en gras dans le côté droit de la *Figure II.4*), il suffit de retransmettre le paquet de la source 11 fois pour atteindre les nœuds à 3 sauts.

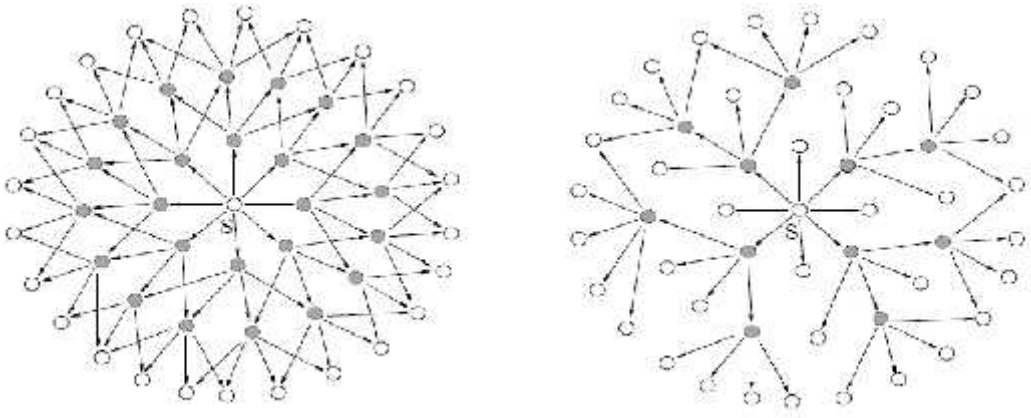

Figure II.4 : Diffusion pure et diffusion en utilisant les MPRs dans OLSR

b. Fonctionnement du protocole

OLSR est un protocole proactif et très bien adapté aux réseaux larges et denses. Tous les nœuds du réseau serviront de routeur et OLSR maintient sur chaque nœud une table de routage complète. Le protocole est complètement distribué, il n'y a pas d'entité centrale. Chaque nœud choisit la route la plus adaptée en fonction des informations qu'il a reçues.

Pour maintenir à jour toutes les informations nécessaires au choix des relais multipoints (MPRs) et au calcul de la table de routage, les nœuds OLSR ont besoin de s'échanger des informations périodiquement. Pour s'informer du proche voisinage, les nœuds OLSR envoient périodiquement des messages dits HELLO contenant la liste de leurs voisins. Ces messages permettent à chacun de choisir son ensemble de relais multipoints.

Le deuxième type de message d'OLSR est le message TC (Topology Control). Par ce message les sous-ensembles de voisinage que constituent les relais multipoints sont déclarés périodiquement dans le réseau. Ils sont diffusés en utilisant une diffusion optimisée par relais multipoints. Ces informations offrent une carte du réseau contenant tous les nœuds et un ensemble partiel de liens, mais suffisant pour la construction de la table de routage.

La table de routage est calculée par chacun des nœuds et le routage des données s'effectue saut par saut sans l'intervention d'OLSR dont le rôle s'arrête à la mise à jour de la table de routage [21].

II.2.8. SPIN (Sensor Protocol for Information via Negotiation)

Le protocole SPIN [21] permet de disséminer des informations sur le réseau de manière ciblée. Le fonctionnement du protocole SPIN permet de réduire la charge du réseau par

rapport aux méthodes de diffusion traditionnelles telles que l'inondation ou l'algorithme de Gossiping.

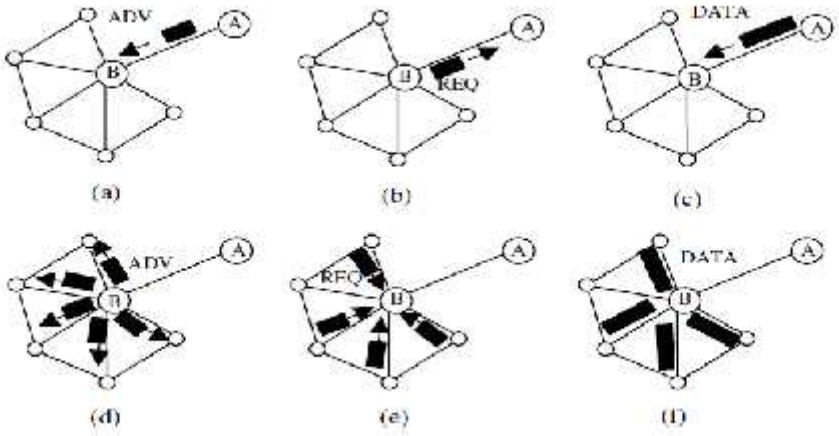

Figure II.5 : Fonctionnement du protocole SPIN [21]

Le protocole SPIN utilise essentiellement trois types de paquets ADV/REQ/DATA. Un nœud voulant émettre une donnée commence par envoyer un paquet ADV. Ce paquet ADV consiste d'une méta-donnée sur les données à émettre. Les méta-données peuvent décrire plusieurs aspects comme le type des données et la localisation de son origine. Les nœuds qui reçoivent ce paquet vérifient si les données les intéressent. Si oui, ils répondent par un paquet REQ. Le nœud qui a initié la communication envoie alors un paquet DATA pour chaque réponse REQ reçue (voir la *Figure II.5*). Un nœud peut parfaitement ne pas répondre aux messages ADV, par exemple dans le but d'économiser son énergie. Ensuite chaque nœud qui fait office de relais peut très bien agréger ses propres donnés aux données qui sont déjà contenues dans le paquet [21].

II.3. Protocoles de routage hiérarchiques

II.3.1. Introduction

Lorsque la taille du réseau devient de plus en plus importante, sa gestion devient plus difficile. Les protocoles de routage à plat fonctionnent bien quand le réseau ne comprend pas un grand nombre de nœuds. La structuration d'un réseau est un des outils principaux pour sauvegarder l'énergie dans chaque nœud du réseau, ce qui aboutit à prolonger la vie du système. Une des structures les plus connues est la hiérarchie. La technique de hiérarchisation sert à partitionner le réseau en sous ensembles afin de faciliter la gestion du réseau surtout le routage, qui se réalise à plusieurs niveaux. Dans ce type de protocoles, la vue du réseau devient locale ; des nœuds spéciaux peuvent avoir des rôles supplémentaires. La littérature

comprend plusieurs contributions dans les techniques de hiérarchisation du réseau, Ce que nous avons classifié à l'état de l'art suivant, dans l'intérêt de faciliter leur comparaison.

Un cluster est défini par un ensemble de nœuds et possède un nœud nommé nœud-chef ou Cluster Head (CH). Le rôle du CH est de faire le relais entre les nœuds du cluster et la station de base directement ou via d'autres CHs. Le CH possède généralement des ressources énergétiques supérieures aux autres nœuds du réseau. Cette technique est appelée cautérisation (voir la *Figure II.6*). Le CH est élu suivant différents critères et informations sur le réseau : le niveau de l'énergie d'un capteur, la connexion avec les autres capteurs, la position géographique, etc. Une zone est définie par un ensemble de nœuds mais ne possède pas un nœud-chef (ou CH). Ainsi, un cluster est une sous-classe d'une zone.

La construction des groupes (zones ou clusters) s'appuie sur des informations sur le réseau, exigeant donc son instrumentation. Cette prise de mesures peut être, dans certaines circonstances, statique (comme la position des capteurs dans un système immobile) ou dynamique (comme le niveau énergétique des capteurs).

Une autre structure utilisée est la chaîne [22]. Le principe d'une chaîne est qu'un nœud ne peut communiquer qu'avec deux voisins. On a trouve aussi des structures qui combinent les groupes et les chaînes. En se basant sur une architecture hiérarchique, plusieurs protocoles de routage pour les réseaux Ad-hoc de grande taille ont été proposés. Dans la suite nous en détaillerons quelques uns.

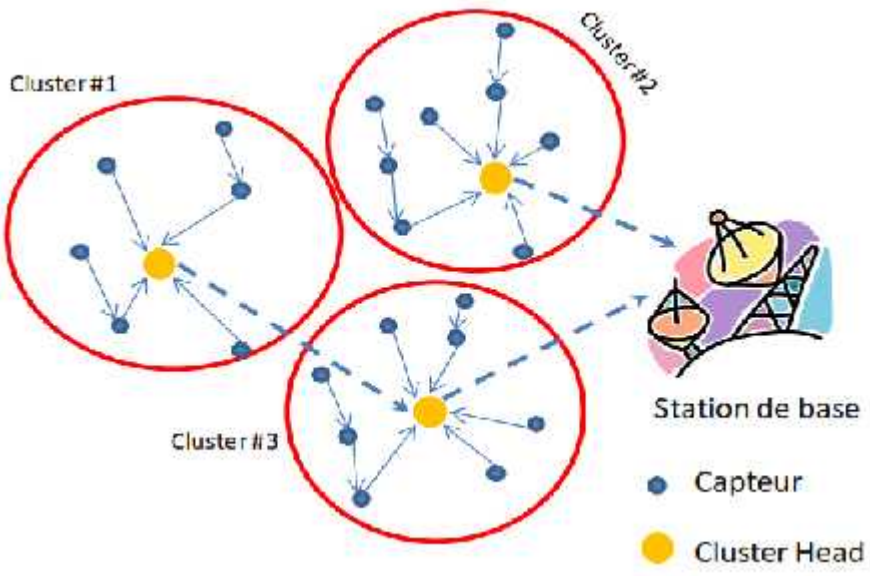

Figure II.6 : Architecture en cluster

II.3.2. ZHLS (Zone-based Hierarchical Link State Protocol)

Le protocole ZHLS [13] est basé sur la décomposition du réseau en un ensemble de zones disjointes. Dans ce protocole, les membres d'une zone n'élisent pas de représentants contrairement à d'autres protocoles hiérarchiques. ZHLS utilise la technique GPS5 afin que chaque nœud sache sa position et la zone dans laquelle il se trouve. Avec cette décomposition, on a deux niveaux de topologies : le niveau nœud, et le niveau zone. La topologie basée sur le premier niveau renseigne sur la manière dans laquelle les nœuds d'une zone donnée sont connectés physiquement. Un lien virtuel peut exister entre deux zones, s'il existe au moins un nœud de la première zone, qui soit physiquement connecté à un nœud de l'autre zone (voir la *Figure II.7*). La topologie basée sur le niveau zone, donne le schéma de la connexion des différentes zones. La taille de la zone dépend de la mobilité des nœuds, la densité du réseau, la puissance de transmission et les caractéristiques de propagation. Le protocole est proactif quand le nœud destinataire est dans la même zone que le nœud émetteur. D'autre part, il est réactif si le nœud destinataire n'appartient pas à la même zone que le nœud émetteur.

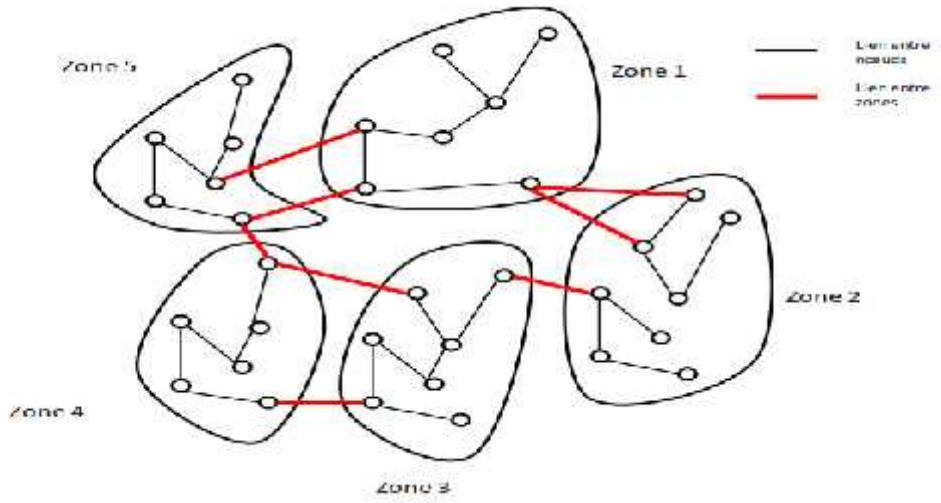

Figure II.7 : Décomposition du réseau en zones dans ZHLS

Dans ce protocole, les paquets qui contiennent les états des liens ou les LSPs (Link State Packet) peuvent être divisés en deux classes : les LSPs orientés nœuds (NodeLSP) et les LSPs orientés zones (ZoneLSP). Pour un nœud donné, un paquet NodeLSP contient l'information d'un nœud voisin tandis qu'un paquet ZoneLSP contient l'information de la zone et il est échangé d'une manière globale. De cette façon, chaque nœud du réseau possède une connaissance complète concernant les nœuds de sa propre zone, et seulement une connaissance partielle du reste du réseau. Cette connaissance partielle est matérialisée par l'état de la connexion des différentes zones du réseau.

a. Construction des tables de routage intra-zone

Chaque nœud diffuse une demande de vérification de liens (Link Request). Les nœuds appartenant à sa portée de communication répondent par un paquet contenant l'ID du nœud et sa zone. Après avoir reçu toutes les réponses, le nœud génère son paquet NodeLSP. Ce paquet NodeLSP contiendra les IDs des nœuds voisins dans sa zone et l'ID de la zone de ses voisins dans les différentes zones. Le paquet NodeLSP d'un nœud est transféré à tous les nœuds de la même zone. Les informations de l'ensemble de ces paquets NodeLSP seront stockées chez chaque nœud de la zone. Les informations des paquets venant des autres zones ne sont pas stockées puisqu'elles ne sont propagées que dans leurs propres zones. De cette façon, un nœud connaît la topologie basée sur le niveau nœud de sa zone (graphe LS). L'algorithme de Dijkstra (ou SPF, Shortest Path Algorithm) est utilisé pour construire la table de routage intra-zone.

b. Construction des tables de routage inter-zone

Certains nœuds peuvent recevoir des réponses sur leurs demandes de vérification de liens (Link Request) des nœuds qui ne sont pas dans sa zone. Ces nœuds sont appelés des nœuds « Gateway ». Après l'échange des paquets NodeLSP dans la phase intra-zone, chaque nœud connaît les zones connectées à sa zone. A ce moment, chaque nœud de la même zone génère le même paquet ZoneLSP. Les nœuds « Gateway » envoient le paquet ZoneLSP à tous les nœuds du réseau. Chaque zone exécute la même procédure. Une liste de paquets ZoneLSP est stockée par chaque nœud du réseau. Par la suite, chaque nœud du réseau connaîtra la topologie du réseau (niveau zone). Une table de routage inter-zone est construite et SPF est utilisé pour trouver le plus court chemin.

Les tables sont mises à jour périodiquement. Les nœuds « Gateway » ne diffuseront pas les paquets ZoneLSP si les nouvelles valeurs sont les mêmes que les anciennes. Le ZoneLSP n'est mis à jour qu'à la création ou lors de la césure d'un lien virtuel entre les zones. Ainsi, si un nœud « Gateway » reçoit deux copies du même ZoneLSP, il ne transfère qu'une seule, ce qui réduit le surcoût dans le réseau.

Par conséquent, l'acheminement des données se fait de deux façons : le routage inter-zones, et le routage intra-zone. Pour une destination donnée, les données sont envoyées entres les zones en utilisant les identificateurs de zones jusqu'à ce que les données atteignent la zone finale de destination. Par la suite, les paquets de données circulent à l'intérieur de la zone finale, en utilisant l'identificateur du nœud destination. L'adresse < ID zone, ID nœud >, est

suffisante pour atteindre n'importe quelle destination même si le réseau change de topologie.

II.3.3. Le protocole LEACH (Low-Energy Adaptive Clustering Hierarchy)

Le protocole LEACH est le plus populaire des protocoles de routage hiérarchique, proposé par Heinzelman et al. (2000) [14] pour former des clusters en se basant sur l'intensité du signal radio reçu. En effet, LEACH utilise un algorithme distribué où chaque nœud décide d'une manière autonome s'il sera ClusterHead ou non en calculant aléatoirement une probabilité pu et en la comparant à un seuil T(u); puis, il informe son voisinage de sa décision. Chaque nœud non ClusterHead décide du cluster à joindre en utilisant un minimum d'énergie de transmission (i.e. le plus proche). L'algorithme se déroule en plusieurs rounds et pour chaque round, une rotation du rôle du ClusterHead est initie selon la probabilité « pu » choisie et comparé à la formule suivante du seuil:

$$T(u) = \begin{cases} \dfrac{p}{1 - p \times (r \times mod(\frac{1}{p}))} & si\ u \in G \\ 0 & sinon \end{cases}$$

Où ***p***: le pourcentage des CHs sur le réseau (généralement 5%);

r: numéro du round en cours;

G: l'ensemble des nœuds qui n'était pas CH dans les (1/***p***) rounds précédentes.

LEACH suppose que chaque nœud du réseau peut communiquer directement avec le puits; alors que, les nœuds non-ClusterHead ne peuvent communiquer qu'avec leurs ClusterHead choisi, en utilisant la technique TDMA instaurée par ce dernier. Cette technique permet de minimiser les collisions en allouant à chaque nœud un temps privé pour transmettre ses données vers son CH.

LEACH est exécuté en deux phases : la phase « set-up » et la phase « steady-state » suivant la *Figure II.8*. Dans la première phase, les clusters heads sont sélectionnés et les clusters sont formés, et dans la seconde phase, le transfert de données vers la station de base aura lieu. Durant la première phase, le processus d'élection des clusters heads est déclenché pour choisir les futurs clusters heads. Ainsi, une fraction prédéterminée de nœuds s'élisent comme cluster heads selon le schéma d'exécution suivant : durant une période T, un nœud n choisit un nombre aléatoire nb dont la valeur est comprise entre 0 et 1 ($0 < nb < 1$). Si nb est inférieure à une valeur seuil alors le nœud n deviendra cluster head durant la période courante, sinon le nœud n devrait rejoindre le cluster head le plus proche dans son voisinage.

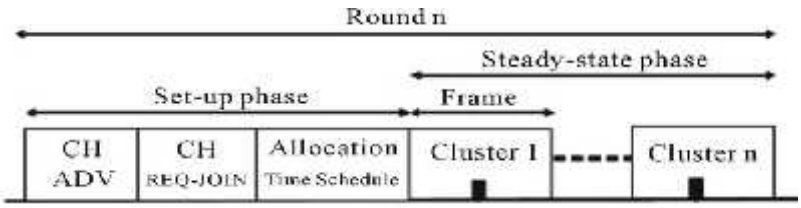

Figure II.8: Formation des clusters dans LEACH [16]

LEACH préconise, également, une agrégation de données au niveau des CHs pour plus de conservation d'énergie. Cependant, plusieurs critiques sont apportées au protocole LEACH relatives à ses hypothèses contraignantes de départ, à savoir:

- La possibilité de communiquer avec le puits à travers n'importe quel nœud du réseau exige une consommation d'énergie importante des nœuds lointains. Ce qui rend le protocole moins apte au passage à l'échelle,
- L'agrégation des données est centrée au niveau des CHs, ce qui les rend les maillons faibles du réseau;
- La rotation du rôle du CH sur l'ensemble des nœuds du cluster, permet d'une part d'équilibrer la consommation de l'énergie du cluster. Mais, elle génère une surconsommation d'énergie, car chaque rotation de CH nécessite une phase de diffusion pour faire connaitre le nouveau CH;
- LEACH ne garantie pas une distribution homogène des CHs sur le réseau, car le seul critère d'élection du CH est une probabilité aléatoire. Cela n'empêche pas une concentration des CHs dans une région limitée au détriment de l'ensemble du réseau.

Plusieurs variantes de LEACH ont été proposées pour palier aux problèmes de la version originale, à savoir, LEACH-C qui est une version centralisée [15], où l'algorithme s'exécute au niveau du puits pour permettre une meilleure distribution des CHs sur réseau.

II.3.4. Le protocole PEGASIS (Power-Efficient GAthering in Sensor Information Systems)

Il est considéré comme une optimisation de LEACH [17], proposé par Lindsey et autres en 2002 [18]; PEGASIS regroupe les nœuds du réseau sous forme d'une longue chaine en se basant sur le principe qui stipule qu'un nœud ne peut communiquer qu'avec le nœud le plus proche de lui. Ainsi, il ajuste sa radio pour une communication très courte pour conserver son énergie. Pour communiquer avec le puits, le processus est organisé en rounds; au cours de chaque round un seul nœud est autorisé à communiquer avec le puits directement. Ce

privilège est accordé à l'ensemble des nœuds du réseau à tour de rôle. Une meilleure conservation d'énergie est obtenue, également, en agrégeant les données sur chaque nœud du réseau.

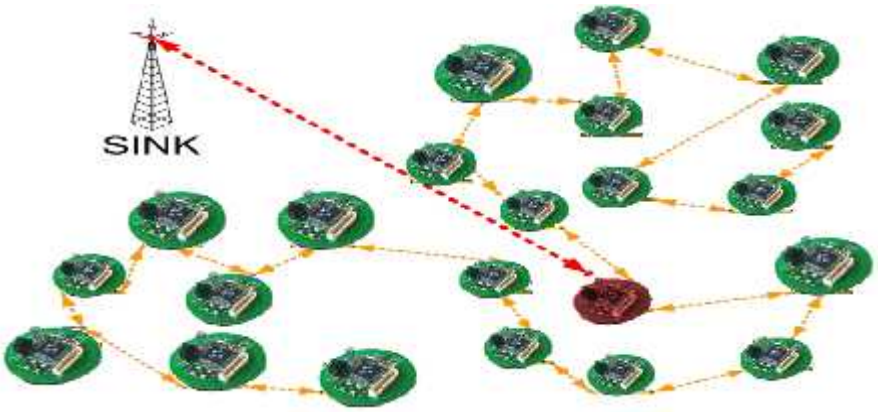

Figure II.9: Formation des chaîne*s gourmandes dans PEGASIS*

Algorithme de la chaîne Greedy:

- Commencez avec nœud le plus éloigné de BS
- Ajouter à chaîne voisin le plus proche de ce noeud qui n'a pas été visitée
- Répétez jusqu'à ce que tous les nœuds ont été ajoutés à la chaîne
- Construits avant le 1er tour de la communication, puis reconstruite lorsque les nœuds meurent

La fusion de données à chaque nœud (sauf nœuds d'extrémité):

- Un seul message est transmis à chaque nœud

Calcul Delay: N unités pour un nœud réseau N

- Transmission séquentielle est supposée

Nœud i (mode N) est le chef de file dans i ronde

La simulation montre que PEGASIS garantit une durée de vie de réseau deux fois plus importante que LEACH [19]. Cette performance est obtenue en utilisant l'agrégation des données qui minimise le nombre des transmissions, et en éliminant la phase de la construction des clusters pour chaque round qui génère une surconsommation d'énergie importante.

Cependant, dans PEGASIS chaque nœud nécessite une connaissance actualisée de la topologie pour s'informer de l'état énergétique de ses voisins afin de router ses données efficacement. Cela génère une surconsommation d'énergie importante surtout pour les réseaux à grande échelle. En plus, PEGASIS stipule que tous les nœuds du réseau peuvent atteindre le puits ce que nécessite une transmission réglable avec un surcoût énergétique non négligeable.

En plus, le délai de livraison des données est très important lorsque la chaine formée est très longue. Et, le nœud qui transmet les données vers le puits peut devenir un point de congestion du réseau.

Une amélioration de PEGASIS dite H-PEGASIS [19] a tenté de résoudre le problème de délai de livraison de données en adoptant des communications parallèles avec le puits pour les nœuds géographiquement distants entre eux

II.3.5. TEEN (Threshold-sensitive Energy Efficient sensor Network protocol)

Manjeshwar et *Agrawal* [20] ont proposé une technique de clustering appelée TEEN pour les applications critiques où le changement de certains paramètres peut être brusque. L'architecture du réseau est basée sur un groupement hiérarchique à plusieurs niveaux où les nœuds les plus proches forment des clusters. Puis ce processus de clustering passe au deuxième niveau jusqu'à ce que la station de base soit atteinte. Après la formation des clusters, chaque cluster-head transmet à ses membres deux seuils : un seuil Hard HT (hard threshold), qui est la valeur seuil du paramètre contrôlé (surveillé) et un seuil Soft ST (soft threshold) représentant une petite variation de la valeur du paramètre contrôlé. L'occurrence de cette petite variation ST permet au nœud qui la détecte de la signaler à la station de base en transmettant un message d'alerte. Par conséquent, le seuil Soft réduira le nombre de transmissions puisqu'il ne permet pas la transmission s'il y a peu ou pas de variation de la valeur du paramètre contrôlé.

Au début, les nœuds écoutent le médium continuellement et lorsque la valeur captée du paramètre contrôlé dépasse le seuil Hard, le nœud transmet l'information. La valeur captée est stockée dans une variable interne appelée SV. Les nœuds ne transmettront des données que si la valeur courante du paramètre contrôlé est supérieure au seuil hard HT ou diffère du SV d'une quantité égale ou plus grande que la valeur du seuil Soft ST. Puisque la transmission d'un message consomme plus d'énergie que la détection des données, alors la consommation d'énergie dans TEEN est moins importante que dans les protocoles proactifs ou ceux qui transmettent des données périodiquement tels que LEACH.

Cependant, l'inconvénient principal de ce protocole est que, si les seuils HT et ST ne sont pas reçus, les nœuds ne communiqueront jamais, et aucune donnée ne sera transmise à l'utilisateur, ainsi la station de base ne connaît pas les nœuds qui ont épuisé leur énergie. TEEN ne convient pas aux applications qui nécessitent des envois périodiques de données.

II.3.6. APTEEN (Adaptive Threshold-sensitive Energy Efficient sensor Network protocol)

Pour remédier aux limitations du protocole TEEN, les auteurs ont proposé une extension de TEEN appelée APTEEN (61). APTEEN est un protocole hybride qui change la périodicité et les valeurs seuils utilisées dans TEEN selon les besoins de l'utilisateur et le type d'application. Dans APTEEN, les cluster-heads transmettent à leurs membres les paramètres suivants :

- l'ensemble de paramètres physiques auxquels l'utilisateur est intéressé pour obtenir des informations (A),
- les seuils : seuil Hard HT et seuil Soft ST,
- un Schedule TDMA permettant d'assigner à chaque nœud un intervalle fini de temps appelé slot,
- un compteur de temps (CT) : c'est la période de temps maximum entre deux transmissions successives d'un nœud.

Dans APTEEN, les nœuds surveillent en continu l'environnement. Ainsi, les nœuds qui détectent une valeur d'un paramètre qui dépasse le seuil HT, transmettent leurs données. Une fois qu'un nœud détecte une valeur qui dépasse HT, il ne transmet les données au cluster head que si la valeur de ce paramètre change d'une quantité égale ou supérieure à ST. Si un nœud ne transmet par de données pendant une période de temps CT, il devrait faire une capture de données et les retransmettre. APTEEN offre une grande flexibilité qui permet à l'utilisateur de choisir l'intervalle de temps CT, et les valeurs seuils HT et ST pour que la consommation d'énergie soit contrôlée par la variation de ces paramètres. Cependant, APTEEN nécessite une complexité supplémentaire pour implémenter les fonctions de seuils et de périodes de temps CT. Ainsi, le surcoût et la complexité associés à la formation des clusters à plusieurs niveaux par TEEN et APTEEN sont assez élevés.

II.3.7. CTLMN (Clustering Technique for Large multihop Mobile wireless Networks)

Lin et Chu [23] proposent une technique pour un large réseau Ad hoc. La structure de cluster est contrôlée par la distance égale au nombre de sauts. Cette technique repose sur la manière dont les nœuds sont regroupés dans un cluster en utilisant le nombre maximum de sauts R qui indique le rayon du cluster.

Chaque nœud contient les informations (i, C_i, d_i, n_i) dites informations de cluster qui sont respectivement : l'ID de nœud, l'ID de son cluster, le nombre de sauts à partir de CH, l'ID du prochain nœud sur le chemin de cluster.

Le maintien du cluster se fait comme suit : lorsqu'un nœud se déplace au-delà de R, il quitte son cluster et peut rejoindre un autre cluster s'il se retrouve à une distance égale à R sauts du CH (du nouveau cluster). Si la distance entre deux CHs est inférieure ou égale à un nombre prédéterminé de sauts D (Distance de cluster écartant), le CH qui a le plus grand ID est écarté, et les nœuds dans le cluster écarté cherchent un autre cluster pour le rejoindre.

II.3.8. HEED (Hybrid, Eenergy-Efficient, Distributed approach)

Younes et *Fahmy* [24] ont proposé un algorithme de clustering distribué appelé HEED pour les réseaux de capteurs. Contrairement aux techniques précédentes, HEED ne fait aucune restriction sur la distribution et la densité des nœuds. Il ne dépend pas de la topologie du réseau ni de sa taille mais il suppose que les capteurs ont la possibilité de modifier leur puissance de transmission. HEED sélectionne les cluster-heads selon un critère hybride regroupant l'énergie restante des nœuds et un second paramètre tel que le degré des nœuds. Il vise à réaliser une distribution uniforme des cluster heads dans le réseau et à générer des clusters équilibrés en taille. Un nœud u est élu comme cluster head avec une probabilité Pch égale à :

$$Pch = Cprob\ (En/Etotal)$$

Où En est l'énergie restante du nœud n, Etotal est l'énergie initial dans le réseau et Cprob est le le nombre optimal de clusters. Cependant, l'évaluation de Etotal présente une certaine difficulté, à cause de l'absence de toute commande centrale. Un autre problème réside dans la détermination du nombre optimal de clusters. De plus, HEED ne précise pas de protocole particulier à utiliser pour la communication entre les clusters heads et le sink. A l'intérieur du cluster, le problème ne se pose pas car la communication entre les membres du cluster et le cluster head est directe (à un saut). D'autre part, avec HEED, la topologie en clusters ne réalise pas de consommation minimale d'énergie dans les communications intra-cluster et les clusters générés ne sont pas équilibrés en taille.

II.4. Conclusion

On a décrit dans les sections précédentes quelques protocoles de routage non hiérarchique dans les réseaux Ad-hoc et de capteurs. Lorsque le réseau visé est plus étendu, la gestion devient plus difficile lorsqu'un protocole non hiérarchique est utilisé pour la gestion des

communications. Chaque nœud doit stocker plus d'informations concernant le réseau et ses voisins. Les exigences en taille des réseaux de capteurs, dues aux déploiements généralement étendus, rendent le stockage des informations de topologie très coûteux par rapport aux ressources disponibles dans ces dispositifs. De même, le surcoût de communications entre les nœuds devient plus important dû aux échanges additionnels de paquets. Toute communication se traduit en consommation énergétique, qui constitue un objectif de minimisation dans les réseaux de capteurs. La bande passante limitée est ainsi influée par l'étendue du réseau.

On a aussi décrit des protocoles de routage hiérarchique dans les réseaux Ad-hoc et de capteurs. Les travaux actuels concernant le routage hiérarchique nous ont permis l'identification de trois structures principales d'organisation : les zones, les clusters et les chaînes (voir la *Figure II.10*). Celles-ci sont à la base de la classification proposée à la fin de cette conclusion, qui résume également les caractéristiques des algorithmes de routage hiérarchique.

Les zones définissent généralement un sous-ensemble de nœuds capteurs sans contrôleur central. Une forme particulière présente dans la littérature est la grille, zone bien identifiée par des surfaces carrées de taille donnée. La structure du cluster est la plus répandue : elle identifie, en plus du périmètre de la zone, un nœud particulier, le cluster head, ayant la fonction de gestionnaire de la construction et de l'appartenance. Le choix des clusters heads est souvent dépendant de facteurs divers comme le niveau énergétique, les positions géographiques ou la connectivité. Les approches cluster présentent les inconvénients classiques similaires aux systèmes centralisés, car le cluster heads sont source de concentration d'information et sont donc susceptibles de défaillance rapide pour des raisons de consommation énergétique.

La caractéristique « point-à-point » des partitionnements en zones, dans lesquels les nœuds ont tous le même rôle, permet d'éviter le goulot d'étranglement dans le trafic, les points de défaillance et simplifie la gestion de la mobilité. Les chaînes, structure dans laquelle un nœud ne peut pas communiquer qu'avec deux nœuds voisins, sont le résultat de la recherche des schémas

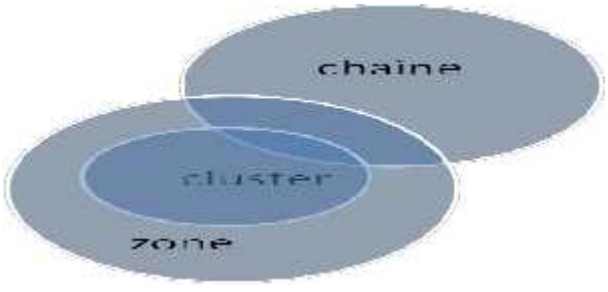

Figure II.10 : Classification des principales structures hiérarchiques d'un réseau

La hiérarchisation répond aux besoins d'un réseau étendu, notamment un réseau de capteurs. Pour ce faire, certains protocoles exigent des informations concernant le réseau. Nous citerons la position géographique des nœuds, l'énergie résiduelle des nœuds, l'état des liens, etc. La position géographique peut être obtenue en utilisant des techniques de localisation ou le GPS. L'information concernant l'énergie des nœuds et des états des liens ne peut pas être obtenue qu'à travers la communication entre les nœuds. D'autres protocoles exigent des contraintes matérielles comme la possibilité de varier la puissance de transmission du nœud, une capacité de traitement adéquate, une capacité énergétique importante, une vaste mémoire, etc. Certains protocoles se basent sur la structure en cluster, d'autres sur la structure en zone, et d'autres sur la structure en chaîne. Un bon état de l'art sur ces protocoles est décrit dans [25]. Le *Tableau II.1* résume les caractéristiques principales de chaque protocole.

Protocoles		**Type de hiérarchie**	**Information exigée sur le réseau**	**Variation de puissance de transmission**	**Nombre prédéfini de clusters/zones /chaînes**
	ZHLS	Zone	Position des nœuds	NON	NON
	LEACH	Cluster	Energie des nœuds	OUI	NON
	PEGASIS	Chaîne	Energie des nœuds	OUI	NON
	TEEN	Cluster	Position des nœuds	NON	NON
	APTEEN	Cluster	Position des nœuds	NON	NON
	CTMN	Cluster	Position des nœuds	NON	NON
	HEED	Cluster	Energie des nœuds	OUI	NON

Tableau II. 1 : Bilan des protocoles de routage hiérarchique dans le réseau de capteurs

Dans les approches de routage pour les réseaux de capteurs, les efforts ont été concentrés sur la définition d'une topologie hiérarchique à deux ou plusieurs niveaux basée sur les clusters. Ces nœuds exigent une capacité de calcul et de communication plus importante, leur choix nécessite l'instrumentation du réseau, permettant d'appliquer des critères de sélection. Un autre point critique est le besoin de décentralisation des décisions, surtout dans les réseaux de grande taille.

A propos de ces besoins. Notre objectif est de proposer un protocole de routage hiérarchique, basé sur une topologie des clusters, s'appuyant sur des décisions et calculs distribués. Les algorithmes bio-inspirés, spécifiquement le système immunitaire, trouvent leur place dans ce domaine de recherche. Pour bien comprendre ce système, nous allons décrire au chapitre suivant le principe du système immunitaire naturel et artificiel, et comment peut-on modéliser et implémenter des problèmes avec ce système.

CHAPITRE III

Système Immunitaire

III.1. Introduction

Il existe de nombreux problèmes complexes qui ne peuvent pas être résolu par un algorithme dans un temps polynomial. A partir de 1980, des méthodes nommées métaheuristiques ont commencé à apparaitre pour résoudre au mieux les problèmes complexes.

L'étude du corps humain à toujours suscité une grande attention du fait de sa grande complexité. Notre domaine de recherche se base principalement sur l'extraction des métaphores utiles, à partir des systèmes biologiques, afin de créer des solutions informatiques efficaces aux problèmes complexes. Les développements les plus appréciables tirés du modèle humain, ont été les « réseaux de neurones » inspirés par le fonctionnement du cerveau, et les « algorithmes évolutionnaires »inspirés par la théorie de l'évolution darwinienne.

Cependant, plus récemment, on assiste à un intérêt croissant accordé à l'utilisation d'un autre système biologique qui est « le système immunitaire » comme source d'inspiration pour résoudre des problèmes complexes. Les systèmes immunitaires artificiels essaient de reproduire des caractéristiques intéressantes du système immunitaire naturel te l que la capacité d'adaptation, la mémorisation, la reconnaissance de formes, l'apprentissage et le traitement parallèle distribué. Pour tout cela et pour d'autres raisons, le système immunitaire a suscité un intérêt significatif en vue de son emploi comme métaphore d'inspiration dans le calcul. Ce domaine de recherche est connu sous l'appellation des ***systèmes immunitaires artificiels***.

Ce chapitre est composé de deux sections principales une première section est consacrée à la présentation du système immunitaire biologique (les différents composants immunitaires et les différents mécanismes utilisés par ce système). Alors nous allons récapituler les propriétés intéressantes du système immunitaire, qui constituent d'un point de vue informatique une source d'inspiration très riche, et dans la deuxième section, On a essaie présente le système immunitaire artificiel (AIS) et le processus de conception d'un AIS. Et à la fin On a essaie présente également les différents algorithmes immunitaires.

III.2. Système immunitaire naturel (NIS)

Le système immunitaire naturel (NIS : Naturel Immun System) est un système complexe qui peut être vu sous différents angles : molécules, cellules et organes. Le système doit protéger le corps des entités dangereuses appelées antigènes. Les éléments de base du NIS sont les globules blancs ou lymphocytes. Pour pouvoir identifier les autres molécules, des lymphocytes particuliers (cellules B) produisent des récepteurs, appelés anticorps 'paratope', responsables de la reconnaissance des antigènes. Le paratope se lie à une partie spécifique de l'antigène appelée épitope. Le degré de cette liaison ou affinité est très fort si seulement les deux formes sont complémentaires.

Ainsi, la reconnaissance d'un antigène par une cellule B est en fonction de l'affinité entre les anticorps de la cellule B et cet antigène (voir la Figure 3.1).

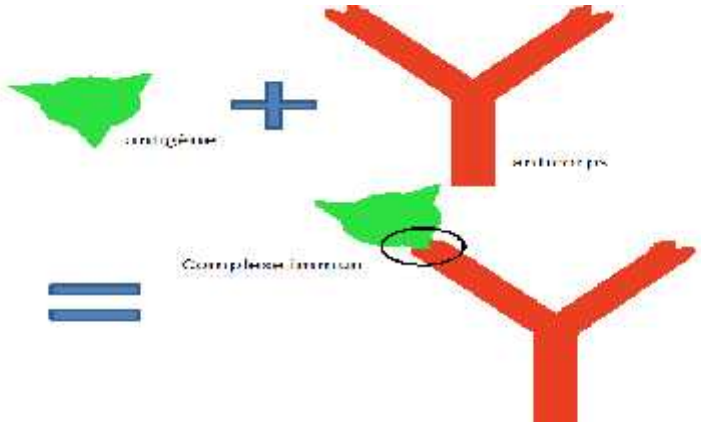

Figure III.1 : Schéma représentant la formation du complexe immune

Les cellules B qui reconnaissent mieux l'antigène vont être proliférées en se clonant, selon le principe de la sélection clonale. Les clones subissent alors des mutations somatiques qui vont promouvoir leur variation génétique.

Lorsque la population atteint la maturité, les clones se différencient en cellules mémoires et cellules plasma. Cette expansion clonale confère au système immunitaire sa mémoire. D'un autre coté, les cellules B avec une faible affinité seront mutées, ou détruites par sélection négative.

III.2.1. Historique

- L'immunologie est une science relativement nouvelle. Son origine est attribuée à *Edward Jenner* qui a découvert en 1796, que la vaccine ou *cow-pox*, induit une protection contre la variole humaine, une maladie souvent mortelle

(*Janeway Jr. & Travers*, 1997). Ce chercheur la baptise« vaccination hisprocess », expression qui décrit l'inoculation des individus en bonne santé par des échantillons affaiblis ou atténués d'agents qui provoquent des maladies, en vue d'obtenir une protection contre ces maladies.

- Lorsqu'*Edward Jenner* introduisit la vaccination, on ne savait encore rien sur l'agent ethnologique de l'immunologie. Au XIXe siècle, *Robert Koch* confirma que les maladies infectieuses sont causées par des microorganismes pathogènes, dont chacun est responsable d'une pathologie donnée.
- Au début des années 1900, *Jules Bordet* et *Karl Landsteiner* portent la discussion sur la notion de « spécificité immunologique ». Il montre que le système immunitaire est capable de produire des anticorps spécifiques contre les produits chimiques synthétisés artificiellement, et qui donc n'ont jamais existé à l'état naturel.
- Les années soixante sont en général considérées comme le début de l'époque moderne de l'immunologie. *Rodney Porter* et *Gerald Edelman* réussirent à élucider la structure des anticorps entre 1959 et 1961, et furent lauréats du prix Nobel de médecine en 1972.
- Vers 1960, la communauté scientifique découvrait, grâce aux travaux de *Jacques Miller*, d'autres caractéristiques fondamentales des cellules immunitaires.
- En 1989, *Charles Janeway* propose un modèle selon lequel, ce serait l'immunité innée qui serait la véritable gardienne des clefs du déclenchement d'une réponse immunitaire.

III.2.2. Concepts immunologiques

Le système immunitaire étant très complexe, il doit être vu sous différents angles. On peut le considérer en tant qu'un ensemble d'organes, molécules ou cellules.

III.2.2.1. Les organes immunitaires

Le système immunitaire est constitué principalement des organes suivants:

- *Moelle osseuse* : c'est le lieu de maturation des lymphocytes B.
- *Thymus* dans le bas du cou, il constitue le site de maturation des lymphocytes T.
- *des Vaisseaux lymphatiques* : ils transportent la lymphe ; les vaisseaux lymphatiques sont situés dans tout le corps.

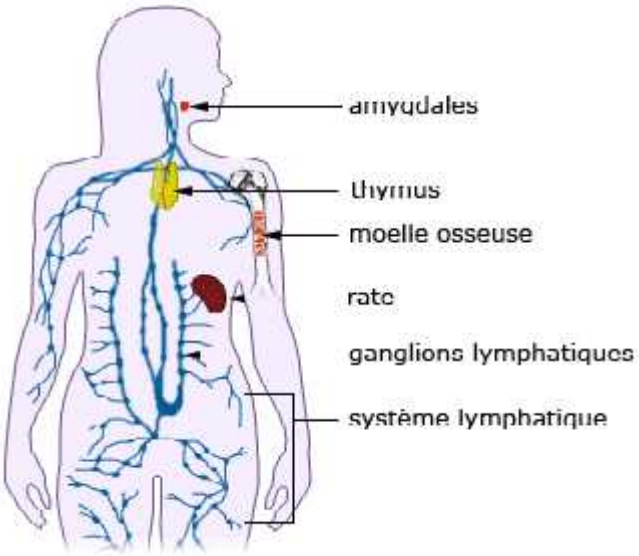

Figure III.2 : Les organes du système immunitaire

III.2.2.2. Les cellules immunitaires

Les globules blancs appelées leucocytes sont impliquées dans la défense. Elles se trouvent dans le sang et la lymphe. Il existe différents types de globules blancs, les plus importantes étant les lymphocytes. Chez l'homme les lymphocytes représentent 5 à 15% des lymphocytes sanguin [26] et se composent de :

- ***Lymphocytes B***, ou cellules B, appelés également bursocytes. Ces lymphocytes ont pour rôle de fabriquer des immunoglobulines appelées anticorps : ils sont responsables de l'immunité humorale. Ils possèdent deux fonctions essentielles :
  - Leur activation par un corps étranger induit leur transformation en cellules sécrétrices d'immunoglobulines.
  - Les lymphocytes B ont également la capacité de se comporter en cellule présentant le corps étranger.
- ***Lymphocytes T:*** C'est une catégorie de lymphocytes qui joue un grand rôle dans la réponse immunitaire primaire mais également secondaire. « T » est l'abréviation de Thymus. Il existe différentes variantes des lymphocytes T. Leur rôle est d'attaquer les cellules infectées. Les cellules T aidants sont essentiellement chargées de l'activation des cellules B; Les cellules T tueuses quant à elles s'attachent aux anticorps et leurs injectent des produits toxiques pour les tuer ; Une autre variante de cellules T, les suppresseurs, servent à éviter les réactions immunitaires non appropriées (maladies auto-immune).

- ***Anticorps:*** Un anticorps est une protéine complexe utilisée par le système immunitaire pour détecter et neutraliser les agents pathogènes de manière spécifique. Les anticorps constituent l'immunoglobuline principale du sang. Ils sont sécrétés par des cellules dérivées des lymphocytes B : les plasmocytes. Ils sont capables de détecter et de neutraliser des substances étrangères. Il est important de signaler qu'il y a plus de dix millions d'anticorps différents dans un organisme, ce qui explique leur spécificité. Les immunoglobulines ou anticorps sont formés de deux chaînes polypeptidiques lourdes et de deux autres chaînes légères, assemblées sous forme d'un Y par des ponts disulfures [26] .

III.2.2.3. Les antigènes

Un antigène est une macromolécule naturelle ou synthétique, reconnue par des anticorps ou des cellules du système immunitaire et capable d'engendrer une réponse immunitaire. Les antigènes sont généralement des protéines, des polysaccharides et leurs dérivés lipidiques. On distingue deux classes d'antigènes :

- *Les antigènes de classe 1*, présents dans toutes les cellules;
- *Les antigènes de classe 2*, présents uniquement dans les cellules immunitaires.

Les antigènes, en tant que marqueurs des agents étrangers à l'organisme, sont à la base de la réponse immunitaire adaptative. C'est la reconnaissance de l'antigène par les cellules immunocompétentes, directement ou via les cellules présentatrices d'antigène (CPA), qui active l'immunité spécifique.

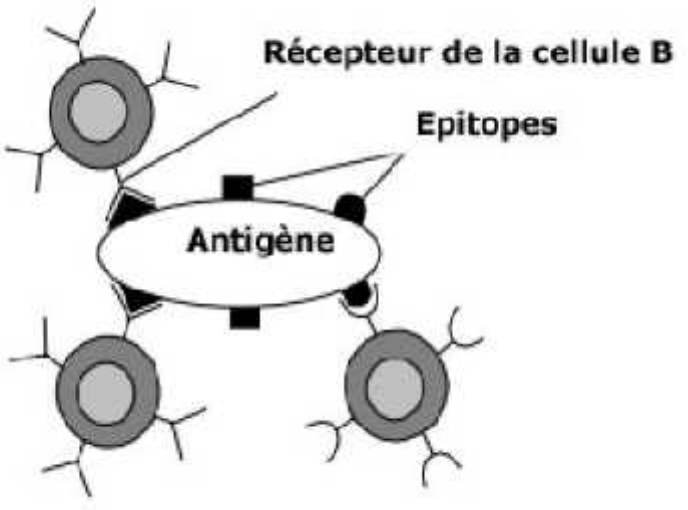

Figure III.3: Structure d'un antigène avec ses *épitopes*.

III.2.3. Architecture du système immunitaire

La défense de l'organisme contre le milieu extérieur comporte une immunité dite *innée ou naturelle*, c'est-à-dire existante en absence de tout contact avec un antigène, et une immunité dite *adaptative ou acquise*, c'est-à-dire apparaissant après contact de l'organisme avec des molécules étrangères qui sont des antigènes.

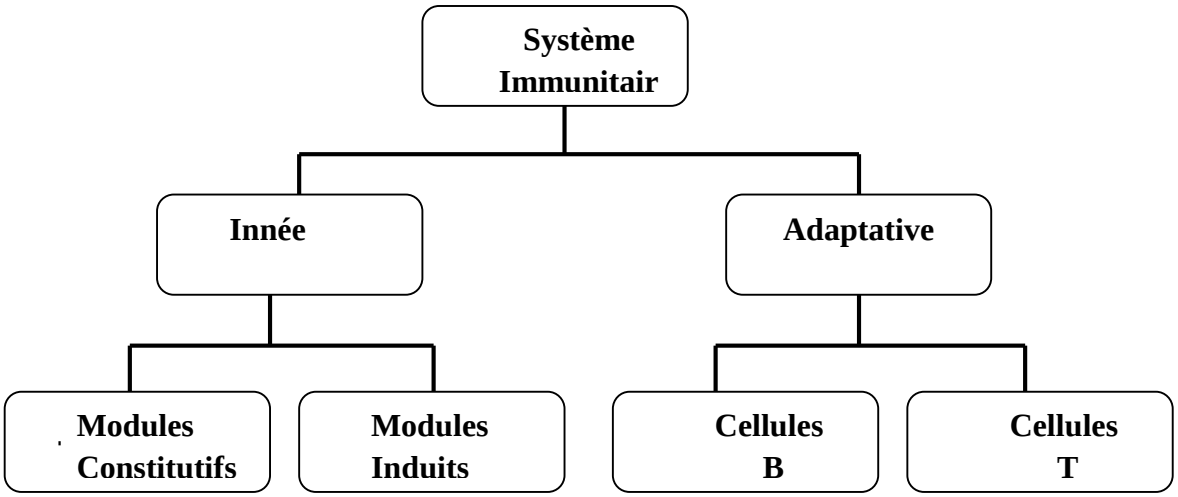

Figure III.4 : Architecture du système immunitaire

III.2.3.1. Immunité innée

L'immunité innée est la première ligne de défense vis-à-vis des agents infectieux et pathogènes qui nous entourent. Elle est mise en jeu immédiatement et est fonctionnelle 4 jours (96 heures).Elle met en jeu différents modules de défense :

- Des modules constitutifs comme la barrière peau-muqueuse.
- Des modules induits comme la phagocytose et la réponse inflammatoire, qui nécessite les cellules phagocytaires et les cytokines.

La réponse immunitaire innée est induite par un signal danger émis suite à l'interaction spécifique entre des récepteurs du soi appelés PRR (Pattern Recognition Receptors) et des molécules du non-soi appelées PAMP (Pathogen Associated Molecular Patterns) présentes au niveau des microorganismes qu'ils soient pathogène ou non.

La réponse du système immunitaire inné est non spécifique à un type particulier d'intrus mais elle est identique contre tous les pathogènes qui envahissent le corps. Il joue un rôle vital pour l'initialisation et la régularisation de la réponse immunitaire adaptative.

III.2.3.2. Immunité adaptative

L'immunité adaptative est constituée de types différents de cellules dont chacune joue un rôle important. Elle résulte du contact du système immunitaire avec les antigènes grâce à la caractéristique d'apprentissage et mémorisation du système immunitaire.

La première intrusion d'un antigène entraine une réponse lente et une réaction difficile du système immunitaire, cependant elle permet de mémoriser l'antigène grâce à ses marqueurs. Si le même antigène pénètre une seconde fois le corps, la réponse sera plus rapide et bien spécifique avec production d'anticorps particuliers pour cet antigène. Les lymphocytes T, les lymphocytes B et les immunoglobulines constituent les principaux acteurs de l'immunité adaptative. L'immunité adaptative est dite immunité à mémoire La réponse de l'immunité adaptative est lancée après la réponse de l'immunité innée, les deux types d'immunités sont liées et se complètent. [27]

III.2.4. Propriétés du système immunitaire

Avec des propriétés très importantes, il devient une référence précieuse et une source d'inspiration pour les nouvelles branches de l'informatique. Beaucoup de travaux de recherche ont vu le jour en s'inspirant du fonctionnement de ce dernier. Voici quelques unes des propriétés les plus importantes du système immunitaire :

- *Multicouche :* Le système immunitaire possède une architecture multicouche qui consiste en deux sous-systèmes inter-liés qui sont : le système immunitaire inné et le système immunitaire adaptatif. Ces deux systèmes combinent leurs tâches et responsabilités pour assurer la protection et la sécurité globale.

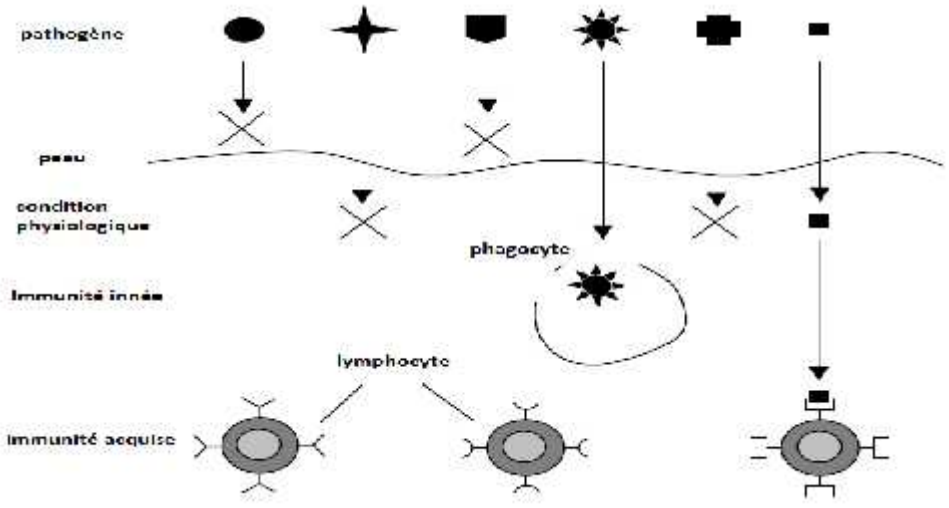

Figure III.5: La structure multicouche du système immunitaire.

- *Unicité:* Chaque élément dans le système immunitaire assume des responsabilités particulières.
- *Autonomie :* Le système immunitaire humain ne possède aucun contrôle central ou un gestionnaire particulier. Il possède une autonomie globale dans la détection et l'élimination des intrus.
- *Distribution :* Les cellules immunitaires et les molécules sont distribuées dans le corps humain pour assurer sa protection. Il n'existe pas un point de contrôle centralisé.
- *Parallélisme:* Le système immunitaire est capable de produire plusieurs réponses immunitaires en même temps à des endroits dispersés.
- *Tolérance au soi* : Le système immunitaire humain peut différencier entre les cellules de soi et les cellules de non soi.
- Apprentissage: Le système immunitaire augmente la capacité d'identification des anticorps à un antigène sélectif (les réponses primaire et secondaire). Il apprend continuellement les structures des pathogènes.
- *Adaptabilité :* Le système immunitaire humain permet la production des cellules de plus en plus spécialisées pour l'identification des antigènes. Cela est garanti par la théorie de la sélection clonale suivie par le mécanisme de l'hyper mutation somatique.
- *Dynamique :* Le système immunitaire change continuellement par la création de nouvelles cellules et molécules, l'élimination des cellules vieilles ou endommagées. Un bon exemple de la dynamique du système immunitaire est la théorie du réseau idiotypique.
- *Mémorisation :* Après une réponse immunitaire à un antigène donné, un ensemble de cellules constituent l'ensemble des cellules mémoires qui seront dotées pour une durée de vie longue afin de fournir des réponses immunitaires plus rapides et plus puissantes aux rencontres suivantes d'un même antigène.
- *Coopération:* Les cellules immunitaires coopèrent leurs capacités pour assurer une meilleure détection et également une protection puissante par exemple les cellules T d'aide, les molécules MHC, etc.
- *Détection:* Le système immunitaire est capable d'identifier et de détecter les intrus dans le corps sans aucune connaissance antérieure de la structure de ces intrus.

III.2.5. Théories immunitaires

Le comportement et les réactions du système immunitaire sont principalement régis par des théories immunitaires :

III.2.5.1. La sélection Négative/Positive

Cette théorie gère le processus de création au niveau de la discrimination entre soi et non soi. Les lymphocytes ont sur leurs surfaces des récepteurs (paratopes). Les lymphocytes, issus de la moelle osseuse, migrent vers le thymus ; à ce stade ils sont appelés cellules T naïves ou immatures. Leurs paratopes subissent un processus de réarrangement génétique pseudo aléatoire, puis un test très important est mis en place [28].Le test en question consiste à vérifier si les nouveaux récepteurs s'attaquent aux cellules du soi ; dans ce cas ces lymphocytes sont détruits et purgés de la population des nouveaux lymphocytes : on parle de sélection négative. Le reste de la population est autorisé à quitter le thymus pour circuler dans le sang et effectuer leurs taches de surveillance [27].

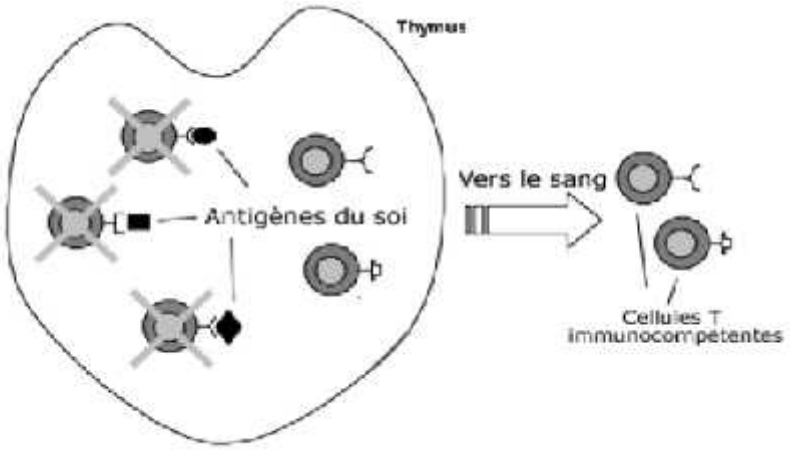

Figure III.6: Sélection négative dans le thymus

III.2.5.2. La sélection clonale

La théorie de la sélection clonale décrit les conséquences de la réponse immunitaire suite à un stimulus antigénique en assurant que seules les cellules qui reconnaissent l'antigène subissent des proliférations et différentiations.

Quand un antigène envahit le corps, des cellules immunitaires reconnaissent cet antigène avec des degrés d'affinité différents. La réponse des cellules B est la production des anticorps dont chaque cellule sécrète un seul type d'anticorps qui est

relativement spécifique à l'antigène. L'appariement fort entre les récepteurs des anticorps et l'antigène, produit la stimulation des cellules B, c'est-à-dire la prolifération (clone) et la maturation des cellules de plasma.

Le taux de prolifération d'une cellule est directement proportionnel à son affinité. Avec l'antigène les cellules qui ont les plus grandes affinités seront les plus proliférées et réciproquement. En plus, les lymphocytes qui ont une forte affinité peuvent se différencier en des cellules mémoires. [28]

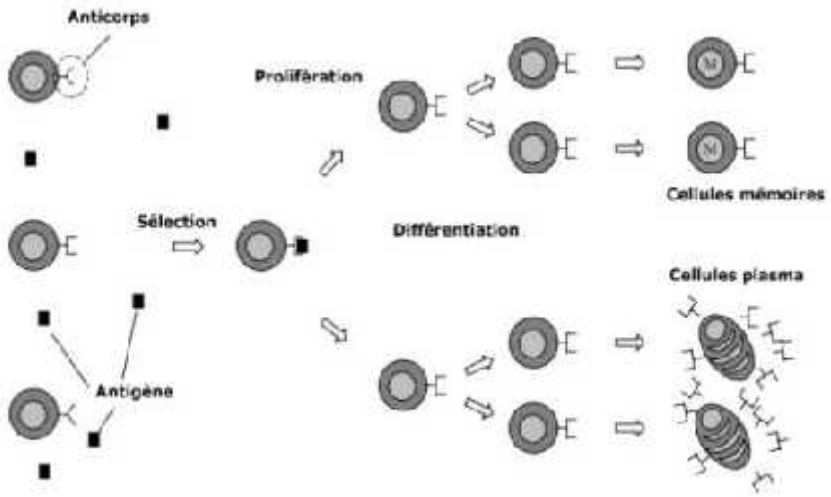

Figure III.7: Théorie de la sélection clonale

III.2.5.3. Théorie des réseaux immunitaires (ou idiotypiques)

La théorie des réseaux immunitaires a été proposée dans le milieu des années soixante-dix par *Jerne* 1974 [29]. L'hypothèse était que le système immunitaire disposait d'un réseau idiotypique de cellules B interconnectées pour la reconnaissance de l'antigène. Ces cellules se stimulent et se suppriment les unes aux autres de manière à conduire à la stabilisation du réseau. Deux cellules B sont reliées si les affinités qu'ils partagent dépassent un certain seuil, et la force de la connexion est directement proportionnelle à l'affinité qu'ils partagent. [29]

Ce réseau de cellules B est dû à la capacité des paratopes, situé sur les cellules B, de se lier aux idiotypes d'autres B-cellules. La liaison entre idiotypes et paratopes a pour effet de stimuler les cellules B. Ceci est due au fait que les paratopes sur les cellules B réagissent aux idiotypes des cellules B similaires, car il serait pris pour un antigène. Cependant, pour contrer la réaction, il y a une certaine quantité de suppression entre les cellules B qui agit comme un mécanisme de régulation. [29]

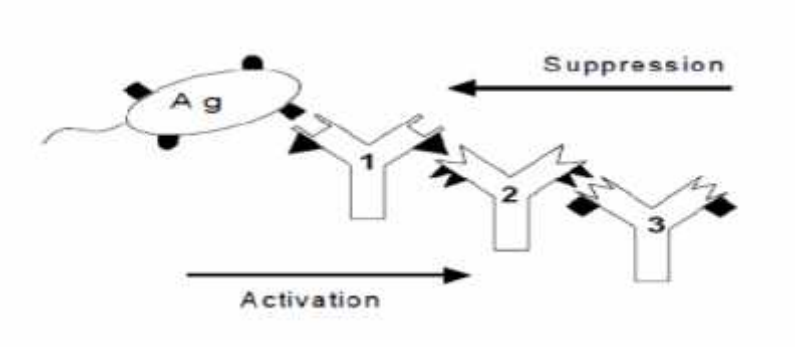

Figure III.8 : Représentations du réseau idiotypique.

Un antigène (A) stimule la production d'anticorps de la classe 1, qui stimulent la production d'anticorps de la classe 2, et ainsi de suite.

III.2.6. Fonctionnement du système immunitaire

Le corps est protégé par un ensemble de cellules et molécules qui coopèrent et dont la cible est l'antigène, une molécule étrangère provenant d'une bactérie, un virus ou tout autre envahisseur. On peut voir dans la *Figure III.9* simplifié de la réponse immunitaire :

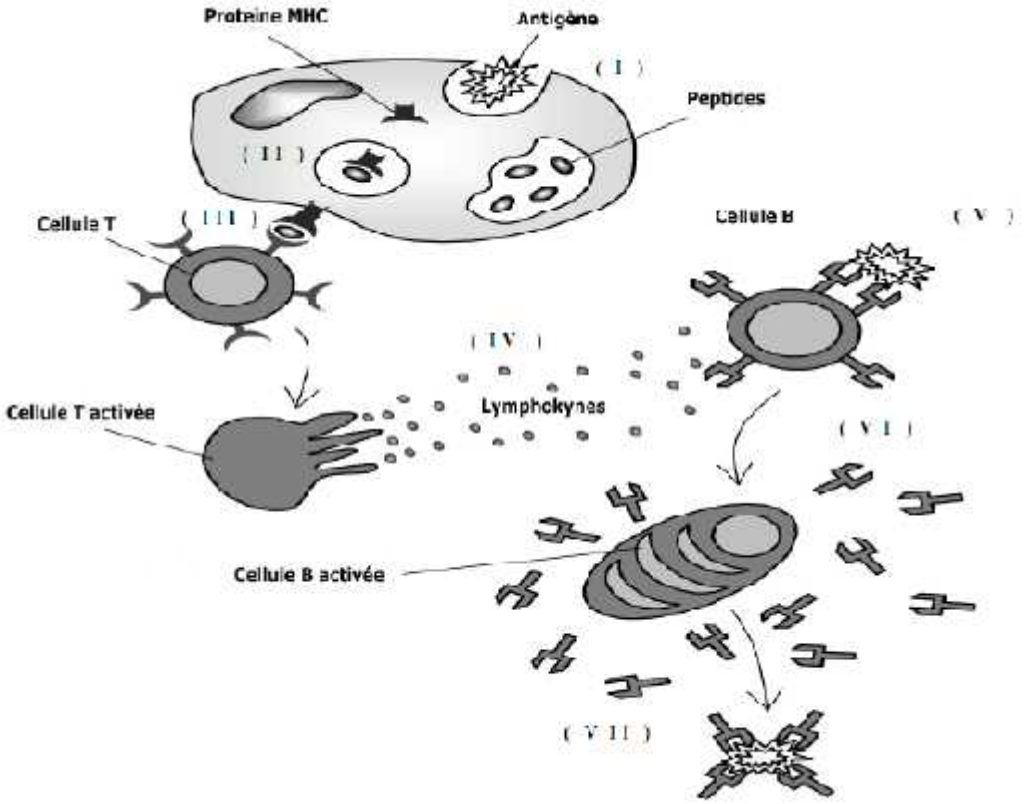

Figure III.9: Déroulement de la réponse immunitaire.

I. Des cellules spécialisées appelées cellules présentatrices d'antigène (APC), tel que les macrophages, parcourent le corps, en ingérant et digérant des antigènes qu'ils trouvent et les fragmentant en peptides antigéniques.
II. Des fragments de ces peptides sont joints au CMH (Complexe Majeur d'Histocompatibilité) et sont affichées sur la surface de la cellule.
III. Les cellules T, possèdent des récepteurs qui permettent à chacun d'entre eux de reconnaître une combinais on différente de peptide-CMH.
IV. Les cellules T activés par la reconnaissance, se divisent et sécrètent des lymphokines (Protéine produite par les lymphocytes qui déclenche leur multiplication, activant ainsi le répons e immunitaire) ou des signaux chimiques, qui mobilisent d'autres composantes du système immunitaire.
V. Les lymphocytes B, qui ont également des récepteurs d'une seule spécificité sur leur surface, répondent à ces signaux. Contrairement aux récepteurs des cellules T, toutefois, celles des cellules B peuvent reconnaître les pièces d'antigènes libres, sans les molécules CMH.
VI. Lorsqu'elles sont activées, les cellules B se divisent et se différencient en cellules plasma qui sécrètent des anticorps, qui sont la forme soluble de leurs récepteurs.
VII. En se liant à des antigènes qu'ils trouvent, les anticorps peuvent les neutraliser ou précipiter leur destruction.
VIII. Certains lymphocytes T et B deviennent des cellules mémoires qui persistent dans la circulation, elles permettent une réponse immunitaire plus rapide du même antigène dans de prochaine exposition. Parce que les gènes d'anticorps dans les cellules B sont souvent victimes de mutation, la réponse immunitaire s'améliore après immunisations répétées, ce phénomène est appelé *la maturation d'affinité*.

III.3. Système immunitaire artificiel (AIS)

III.3.1. Historique

- L'intérêt pour les AISs (Artificiels Immunitaires Systems) est apparu au milieu des années 80 avec la publication de l'article de *Farmer, Packard* et *Perelson* "*The immune system, adaptation and machine learning*" et celui de *Bersini* et de *Varela* sur les réseaux immunitaire en 1990.
- Cependant, c'est seulement au milieu des années 90 que les AISs sont devenus un domaine de recherche.
- En 1994, *Dasgupta* a entrepris des études étendues sur des algorithmes de sélection négatives. *Hunt* et *Cooke* ont commencé des travaux sur les modèles de réseau immunitaire en 1995, *Timmis* et *Neal* ont continué ce travail et ont apporté quelques améliorations.
- Le premier livre sur les systèmes immunitaires artificiels a été édité par *Dasgupta* en 1999.
- Le travail de *De Castro, Von Zuben*, *Nicosia* et de *Cutello* sur la sélection clonal « CLONALG » est devenu notable en 2002.

III.3.2. Définitions

Les AISs constituent un domaine de recherche assez récent comparés aux autres métaheuristiques qui se sont inspiré de la biologie. Les AISs ont plusieurs définitions, voici quelques unes: [30]

- *Définition 1 :* Les AISs sont des méthodes de manipulation de données, de classification, de représentation et de raisonnement qui s'inspirent d'un modèle biologique plausible 'le système immunitaire humain' (*Star lab*).
- *Définition 2:* Les AISs sont des systèmes informatiques basés sur des métaphores du système immunitaire naturel (*Timmis 2000*).
- *Définition 3:* Les AISs sont des systèmes adaptatifs, s'inspirant des théories de l'immunologie , ainsi que des fonctions, des principes et des modèles immunitaires, afin d'être appliqués à la résolution de problèmes (*Castro et Timmis 2002*).
- *Définition 3:* Le système immunitaire artificiel est la composition de méthodologies intelligentes inspirées par le système immunitaire naturel afin de résoudre des problèmes du monde réel. (*Dasgupta*) [31].

III.3.3. Modélisation des systèmes immunitaires artificiels

Le modèle commun connu sous le nom du Framework des systèmes immunitaires artificiels, définit les règles que doit respecter un AIS ainsi que les processus à suivre pour l'élaboration de nouvelles approches. Les conditions nécessaires sont :

- La représentation des composants systèmes (modèles abstraits des cellules immunitaires).
- L'utilisation des mesures d'affinité pour évaluer l'affinité entre les composants systèmes.
- Un ensemble d'algorithmes pour contrôler l'évolution et la dynamique d'AIS.

Les trois conditions citées ci-dessus sont indispensables pour l'élaboration d'un Framework pour définir un système immunitaire artificiel. Ce schéma (voir *Figure III.10*) représente le processus de modélisation d'un AIS :

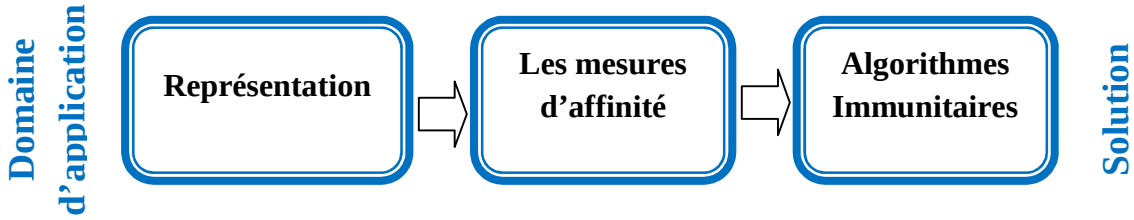

Figure III.10 : Structure de conception d'un AIS

III.3.3.1. La représentation

Les cellules B et T sont les cellules les plus importantes dans le système immunitaire. Elles présentent des récepteurs superficiels utiles pour la reconnaissance des intrus, récepteurs dont les formes sont complémentaires à la forme d'antigène. Les cellules et les molécules immunitaires sont alors les éléments qui doivent être *modélisés* et *employés* dans les modèles proposés par le système immunitaire artificiel.

Il est assumé que chaque antigènes agit spécifiquement avec tous les anticorps dont les compléments existent dans une petite région d'encerclement. Cette région est caractérisée par un paramètre «S » appelé le seuil d'affinité.

Le résultat de la définition du seuil d'affinité est le volume Vs qui est appelé la région d'identification.

III.3.3.2. Les mesures d'affinités

L'affinité entre un anticorps et un antigène est relative à leur distance, Un antigène est représenté par un vecteur Ag = {Ag1, Ag2,…, AgL}, un anticorps est à son tour représenté par un vecteur Ab = {Ab1, Ab2,…, AbL}.

Pour mesurer le degré de complétude entre l'antigène et l'anticorps, plusieurs techniques peuvent être utilisées. Le plus souvent on recourt à l'utilisation des distances. Différentes distances existent dont voici les plus utilisées : La distance euclidienne, La distance de Manhattan et La distance de Hamming. Plus la distance antigène-anticorps est petite, plus l'affinité entre ces derniers, est grande.

Il ne reste plus qu'à implémenter les théories immunitaires que nous allons voir dans la suite. Les principales théories immunitaires sont la théorie de la sélection clonale, la théorie de la sélection négative/positive et la théorie du danger.

III.3.3.3. Les algorithmes immunitaires

Il existe **différents** algorithmes des théories immunitaires selon le contexte et le problème à résoudre.

III.3.3.3.1. La sélection négative

Les algorithmes de la sélection négative sont inspirés par le principal mécanisme dans le thymus qui produit un ensemble de cellules T matures capables de se lier seulement aux antigènes du non-soi.

Le premier algorithme de la sélection négative a été proposé par *Forrest* en 1994 pour détecter la manipulation de données causée par un virus dans un système informatique (Le système nommé LYSIS). Le point de départ de cet algorithme est de produire un ensemble de chaînes de soi 'S', qui définissent l'état normal du système. La tâche est alors de générer un ensemble de détecteurs 'D', qui ne se lient (reconnaissent) que le complément de S. Ces détecteurs peuvent ensuite être appliqués à de nouvelles données afin de les classer comme étant soi ou non-soi, ou dans le cas de l'œuvre originale de *Forrest*, détecter si les données ont été manipulées.

L'algorithme de *Forrest* produit l'ensemble de détecteurs via le processus suivant:

*Entrée : **S** = ensemble d'éléments du soi.*

*Sortie : **D** = ensemble de détecteurs généré.*

Début

Répéter jus qu'à ce que les critères d'arrêt aient été atteints :

*1. Générer aléatoirement des détecteurs potentiels et les placer dans un ensemble **P**.*

*2. Déterminer l'affinité de chaque membre de **P** avec chaque membre de l'ensemble **S**.*

*3. Si un élément de **S** est reconnu par un détecteur de **P** selon un seuil de reconnaissance **r**:*

- *Alors le détecteur est rejeté,*
- *Sinon il est ajouté à l'ensemble de détecteurs disponibles **D**.*

Fin

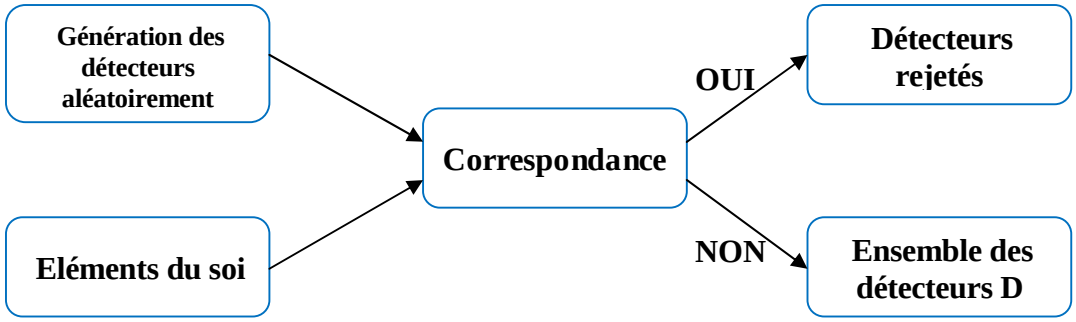

Figure III.11: Génération de l'ensemble de détecteurs.

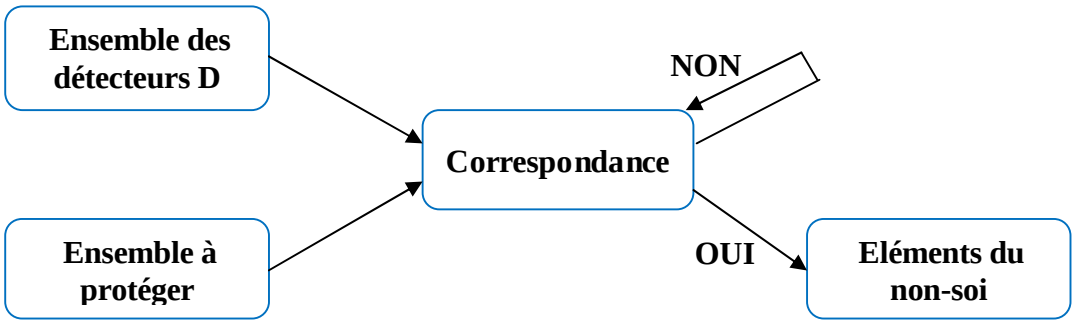

Figure III.12: Surveillance d'éléments du non-soi.

III.3.3.3.2. La sélection clonale

La théorie de la sélection clonale a été utilisée comme source d'inspiration pour le développement des AISs qui effectuent des tâches d'optimisation et de reconnaissance de formes. En particulier, l'inspiration a été prise du processus de maturation d'affinité des cellules B et de son mécanisme d'hyper-mutation. Ces AIS font souvent appel à l'idée de cellules mémoires afin de conserver les bonnes solutions du problème à résoudre. Dans leur livre, *Castro* et *Timmis* mettent en évidence deux aspects importants de la maturation d'affinité dans les cellules B qui peuvent être exploitées à partir du point de vue informatique:

- Le premier est que la prolifération (clonage) des cellules B est proportionnelle à l'affinité de l'antigène auquel elles se sont liées, donc les cellules avec le plus grand taux d'affinité, sont celles qui produisent le plus de clones.
- En second lieu, les mutations subies par les anticorps d'une cellule B sont inversement proportionnelles à l'affinité de l'antigène auquel ils se sont liés, donc plus l'affinité est grande, plus le taux de mutation est petit.

Utilisant ces deux caractéristiques, *De Castro* et *Von Zuben* ont développé l'un des algorithmes d'AIS inspiré de la sélection clonale les plus populaires et largement utilisés appelé CLONALG, qui a été utilisé pour effectuer les tâches de filtrage et d'optimisation multimodale. [32]

*Entrée : **S** = ensemble d'antigènes.*

*Sortie : **M** = ensemble de détecteurs de mémoire capable de classer de nouveaux modèles.*

Début:

Crée r un ensemble aléatoire d'anticorps, A.

*Pour chaque élément de **S** faire :*

1. *Déterminer l'affinité avec chaque anticorps de l'ensemble **A**.*
2. *Créer un sous-ensemble **K** des anticorps avec le plus grand taux d'affinité.*
3. *Générer des clones des anticorps du sous-ensemble **K**. Le nombre de clones pour un anticorps est proportionnel à son affinité*
4. *Appliquer le processus de mutation sur les clones pour augmenter leur degré de correspondance avec l'antigène.*
5. *Exposer les clones de nouveau à l'antigène et recalculer leurs affinités.*
6. *Les meilleurs clones seront placés dans l'ensemble **M**.*
7. *Remplacer les **n** anticorps de plus faible affinité dans **A** par de nouveaux anticorps générés aléatoirement.*

Fin

Bien que performant le CLONALG présente certains inconvénients, par exemple il ne permet pas de capitaliser les informations générées par chaque population de clone, car dès qu'une cellule mémoire est sélectionnée le reste des cellules mutées seront éliminées, alors que cette population pourrait contenir un certain nombre de cellules de haute affinité. En préservant une grande partie de la population de cellules mature, l'algorithme pourrait construire à partir d'une base solide de liens de haute affinité et devrait théoriquement aboutir à une solution optimale en moins de générations. Toutefois, ceci introduit le risque de convergence vers un minimum local. Ceci pourrait être évité en générant de façon aléatoire de nouveaux anticorps et les ajouter à la population.

En 2003, *White* et *Garrett* dans leur article " *Improved Pattern Recognition with Artificial Clonal Selection*" utilisent l'algorithme CLONALG pour le problème de reconnaissance de formes et après avoir examiné la performance de la technique sur la classification des caractères non vue, ils ont proposé une version enrichie du CLONALG appelé CLONCLAS (CLONal selection algorithm for CLASsification). Le principe est d'allouer une classe à chaque anticorps de la population, ce qui lui permet d'effectuer une

classification en attribuant sa classe à un antigène. Quand un nouvel antigène est exposé à la population, il est alloué à la classe de l'anticorps avec la plus grande affinité pour cet antigène.

*Entrée : **S** = ensemble d'antigènes.*

*Sortie : **M** = ensemble de détecteurs de mémoire capable de classer de nouveaux modèles.*

Début

1. *Générer aléatoirement une population initiale d'anticorps **Ab**. Il est compos é de deux sous-ensembles $\boldsymbol{Ab_m}$ (population de mémoire) et $\boldsymbol{Ab_r}$ (population réservoir).*
2. *Sélectionnez un antigène $\boldsymbol{Ag_i}$ de la population **S**.*
3. *Pour **G** générations faire*
   - *Effectuer les étapes **1-6** de **CLONA LG***
   - *Remplacez les anticorps dans $\boldsymbol{Ab_r}$ avec le même nombre d'anticorps de la population triés des clones qui ont subit une mutation.*
   - *Supprimer les anticorps avec une faible affinité dans la population $\boldsymbol{Ab_r}$ et les remplacer avec de nouveaux membres générés de façon aléatoire.*

   Fin
4. *Revenir à l'étape **2** jus qu'à ce que tous les antigènes aient été présentés.*

Fin.

La théorie du réseau immunitaire a suggéré un système immunitaire avec un comportement dynamique même en absence d'un antigène de non-soi. Il existe plusieurs modèles du réseau immunitaire dans cette section on a pencherons sur le modèle nommé aiNet (**a**rtificial **i**mmune **Net**work) qui a été proposé par *De Castro* et *Von Zuben*. [32]

Le modèle aiNet sera composé d'un ensemble d'anticorps, reliés entre eux par des liens avec leurs forces de connexion associé. Les anticorps aiNet sont censés représenter les images du réseau interne des agents pathogènes contenues dans l'environnement auquel ils sont exposés. Les connexions entre les anticorps déterminera leurs interrelations, fournissant un degré de similitude entre eux: plus les anticorps sont proche, plus ils sont similaires.

*Entrée : **S** = ensemble d'antigène à reconnaitre, **nt** seuil d'affinité réseau, **ct** seuil piscine clonale, **h** le nombre de clones avec la plus grande affinité, **a** le nombre de nouveaux anticorps à introduire.*

*Sortie : **N** = ensemble de détecteurs mémoire capable de classer les modèles non vue.*

Début

1. *Créer un premier ensemble aléatoire d'anticorps **N**.*
2. *Répéter jus qu'à ce qu'un des critères d'arrêt soit atteint*

   *Pour chaque individu de **S** faire*

   - *Déterminer l'affinité avec chaque anticorps en **N**.*
   - *Générer des clones des anticorps avec la plus haute affinité.*
   - *Muter les attributs de ces clones, Sélectionner quelques clones de plus haute affinité pour constituer l'ensemble mémoire **C** ;*
   - *Éliminez tous les éléments de **C** dont l'affinité avec l'antigène est inférieur à un seuil prédéfini **ct** ;*
   - *Déterminer l'affinité entre tous les anticorps en **C** et éliminer les anticorps dont l'affinité avec les autres est inférieur au seuil **ct** ;*
   - *Incorporer les clones restants de **C** dans **N** ;*

   Fin
3. *Déterminer l'affinité entre chaque paire d'anticorps dans **N** et éliminer tous les anticorps dont l'affinité est inférieur au seuil **nt** ;*
4. *Introduire un nombre **a** d'anticorps générés aléatoirement et les placer dans **N** ;*

   Fin

Fin

III.3.3.4. Implémentation d'un AIS

Afin d'implémenter un système immunitaire artificiel, il faut suivre les étapes suivantes:

- Identifier les éléments qui feront partie de l'AIS.
- Choisir la meilleure représentation (encoding) pour ces éléments.
- Déterminer la mesure d'affinité appropriée (la fonction objective du problème).
- Choisir l'algorithme immunitaire qui convient le mieux au type du problème à résoudre.

III.3.3.5. Domaines d'application des AISs

Le système immunitaire artificiel s'inspire du système immunitaire naturel et chaque processus du ce système sert de base pour un modèle différent. Cette diversité de modèle permet que les AISs soient utilisés pour résoudre plusieurs problèmes différents tel que : [33]

- *Robotique :* L'une des tâches les plus difficiles de la robotique est le problème de navigation autonome, où un robot (un ensemble de robots) doit pouvoir accomplir certaines tâches sans aucune indication extérieure.
- *Optimisation :* Les problèmes d'optimisation sont présents dans plusieurs domaines d'applications. Le but dans ce type de problème est de trouver l'ensemble des meilleures conditions admissibles pour atteindre un certain objectif. En 2000, *De Castro* et *Von Zuben* ont présenté un algorithme de sélection clonale, qui prend en compte la maturation de l'affinité de la réponse immunitaire, afin de résoudre des problèmes complexes, comme l'apprentissage et l'optimisation multimodal. Leur algorithme constitue une mise en œuvre des processus biologiques et ne tient pas compte de toute sophistication mathématique pour améliorer ses performances dans des tâches particulières.
- *Sécurité des ordinateurs :* La protection des ordinateurs contre les virus, les utilisateurs non autorisés, etc., constitue un champ riche de la recherche pour les systèmes de détection d'anomalie. En 1994, *Forrest* et *al*. dans leur article "*Self Non-self Discrimination in a Computer*" comparent le problème de la protection des systèmes informatiques à celui de l'apprentissage de la distinction entre soi et le non-soi des systèmes immunitaires. Ils ont décrit une stratégie de détection basée sur la sélection négative intrinsèque à notre système immunitaire.
- *La détection et l'élimination des virus informatiques :* Dans le système développé par *Kephart* en 1994 dans son [43], un ensemble d'anticorps de virus informatiques ou des vers qui n'ont pas été rencontrés ont été générés de façon à favoriser une réponse plus rapide et plus forte contre des futures infections. Il était également préoccupé par la réduction du risque d'une réaction auto-immune, dans laquelle le système immunitaire informatique aurait à tort identifié les logiciels légitimes comme étant indésirables. En 1999, *Okamoto* et *Ishida* dans leur article ont proposé un système multi-agent basé sur les AISs, plus précisément l'algorithme de la sélection négative. La détection des virus est réalisée en

effectuant une correspondance entre les informations propres d'un fichier (tel que les premiers bits de l'entête du fichier, sa taille, le chemin d'accès) et le fichier de l'hôte. La neutralisation des virus est faite par la réécriture des informations initia les sur le fichier infecté.

- *Reconnaissance de formes :* La reconnaissance de formes est le domaine de recherche qui étudie le fonctionnement et la conception de systèmes capables de reconnaître des tendances dans les données. Il renferme des sous-disciplines comme l'analyse discriminante, l'extraction de caractéristiques, estimation de l'erreur, inférence grammaticale et syntaxique (appelé reconnaissance des formes syntaxiques). Quelques domaines d'application : l'analyse d'image, la reconnaissance de caractères, l'analyse de la parole, le diagnostic, l'identification des personnes et l'inspection industrielle. *Forrest* et *al* dans [42] utilisent un modèle binaire du système immunitaire, afin d'étudier la reconnaissance de formes et l'apprentissage dans le système immunitaire. Ils utilisent aussi un algorithme génétique pour étudier le maintien des capacités de diversité et généralisation du modèle de chaîne de bits du système immunitaire, lors de la généralisation des moyens de détection de schémas communs qui sont partagés entre de nombreux antigènes.
- *Diagnostic médical :* L'utilisation des systèmes de classification pour le diagnostic médical augmente graduellement. Il n'y a aucun doute que le facteur le plus important lors du diagnostic est la décision de l'expert mais les systèmes intelligents de diagnostic apportent une aide non négligeable puisqu' ils réduisent les erreurs dues à la fatigue. Ces systèmes peuvent aussi réduire le temps nécessaire au diagnostic.
- *Segmentation d'images.* [37]
- *Apprentissage.* [38]
- *Ordonnancement.* [39]
- *Data mining.* [40]
- *Système de classification.* [41]

III.3.3.6. Etude comparative entre différents systèmes inspirés de la biologie

Ce tableau récapitule la comparaison entre les différents systèmes inspirés de la biologie qui sont : *les systèmes immunitaires artificiels* inspirés du système immunitaire humain, *les réseaux de neurones* inspirés du fonctionnement du cerveau et *les algorithmes évolutionnaires* inspirés par la théorie de l'évolution darwinienne.

Caractéristique de système	AIS	RN	GA
Composants	Chaîne d'attribut	Neurones artificiels	Chaînes de chromosomes
Structure	Ensemble d'éléments discrets/gérés en réseau	Neurones gérés en réseau	Elément discret
Stockage de la Connaissance	Chaînes d'attributs / connexion réseau	Poids de connexion	Chaînes chromosomiques
Dynamique	Apprentissage/Evolution	Apprentissage	Evolution
Interactions avec d'autres composants	Par l'identification des chaînes d'attribut ou des connexions réseau	Par des connexions du réseau	Par des opérateurs de recombinaison et/ou la fonction d'évaluation
Seuil	Influence l'affinité des éléments	Influence l'activation de neurone	Influence les variations génétiques
Etat	Concentration et affinité	Niveau d'activation des neurones de sortie	L'information génétique dans les chromosomes

Tableau III.1 : Comparaison entre les différents systèmes inspirés de la biologie.

III.4. Conclusion

Dans ce chapitre on a décrit que les systèmes immunitaires artificiels sont des algorithmes qui s'inspirent du domaine de la biologie plus précisément les systèmes immunitaires des vertébrés. Ce chapitre était destiné à présenter les différentes théories et concepts nécessaires au développement d'un AIS. Il faut noter que les SIAs sont particulièrement intéressantes pour résoudre les problèmes dans des environnements distribués et dynamiques.

Comme dans d'autres techniques bio-inspirés, les AISs visent à développer des modèles différents en s'inspirant des différents processus du NIS. Par exemple : l'algorithme de la sélection clonale proposé par *De Castro* et *Von Zuben* en 2000, l'algorithme de la sélection négative présenté par *Forrest* en 1994, et les réseaux immunitaires artificiels proposés par *Farmer* en 1986. Ces différents mécanismes sont généralement utilisés pour résoudre différents types de problèmes: les modèles de réseau immunitaire sont adaptés pour faire face à des environnements dynamiques, tandis que les algorithmes basés sur le principe de la sélection clonale sont adéquats pour résoudre les problèmes d'optimisation, et les stratégies de sélection négative sont appliquées avec succès à des tâches de détection d'anomalies ou intrusion. [33]

CHAPITRE IV

Implémentation et discussion

IV.1. Introduction

Comme nous l'avons mentionné dans les chapitres précédents, l'une des contraintes majeures de conception des RCSF est l'énergie. Certes, les capteurs sont dotés d'une batterie, et sont généralement déployés dans des zones où c'est impossible de remplacer ses batteries ou de les recharger. La durée de vie d'un RCSF est donc étroitement liée à la consommation d'énergie pour chaque nœud capteur. Le module qui consomme plus d'énergie est le module radio. L'unité de transmission (communication) est responsable d'effectuer toutes les émissions et réceptions des données via un medium sans fil. Les unités de transmission de type radio fréquence sont préférables pour les RCSF parce que les paquets transportés sont de petites tailles avec un très bas débit. Ainsi on retrouve les mêmes problèmes rencontrés dans tous les réseaux sans fil : *la quantité d'énergie nécessaire à la transmission est proportionnelle à la distance.*

Il est donc nécessaire de minimiser la distance totale de transmissions dans un RCSF. Pour ce faire, nous avons proposé une version modifié de l'algorithme CLOLALG développé par *De Castro* et *Von Zuben en 2002* (l'un des célèbres algorithmes des AIS) pour bien minimiser la distance total de transmission dans le réseau à l'aide de clustering (regroupement) , ce qui réduirait aussi le nombre de transmission, et avec l'agrégation des données dans le RCSF on peut réduire aussi la quantité de données à transmettre sur le réseau, le nombre de transmission et les distance de transmission et par conséquent moins d'énergie consommé.

Alors et pour mettre en œuvre notre algorithme de routage adapté (AISCBP), et tester ses efficacités dans la prolongation de la durée de vie du réseau, nous l'avons implémenté sur un simulateur des RCSF qui a était développé sous l'environnement C ++ Builder XE.

IV.2. Description générale de l'algorithme proposé

Comme nous l'avons mentionné précédemment, notre algorithme proposé est une version modifiée de l'algorithme proposé dans [34], il s'agit de la sélection clonale.

Dans leur livre, *Castro* et *Timmis* mettent en évidence deux aspects importants de la maturation d'affinité dans les cellules B qui peuvent être exploitées à partir du point de vue informatique:

- Le premier est que la prolifération (clonage) des cellules B est proportionnelle à l'affinité de l'antigène auquel elles se sont liées, donc les cellules avec le plus grand taux d'affinité, sont celles qui produisent le plus de clones.
- En second lieu, les mutations subies par les anticorps d'une cellule B sont inversement proportionnelles à l'affinité de l'antigène auquel ils se sont liés, donc plus l'affinité est grande, plus le taux de mutation est petit.

Utilisant ces deux caractéristiques, *De Castro* et *Von Zuben* ont développé l'un des algorithmes d'AIS inspiré de la sélection clonale les plus populaires et largement utilisés appelé CLONALG, qui a été utilisé pour effectuer les tâches de filtrage et d'optimisation multimodale. [32]

Bien qu'il est performant, le CLONALG présente certains inconvénients, par exemple il ne permet pas de capitaliser les informations générées par chaque population de clone, car dès qu'une cellule mémoire est sélectionnée le reste des cellules mutées seront éliminées, alors que cette population pourrait contenir un certain nombre de cellules de haute affinité. En préservant une grande partie de la population de cellules mature, l'algorithme pourrait construire à partir d'une base solide de liens de haute affinité et devrait théoriquement aboutir à une solution optimale en moins de générations. Toutefois, ceci introduit le risque de convergence vers un minimum local. Ceci pourrait être évité en générant de façon aléatoire de nouveaux anticorps et les ajouter à la population.

En 2003, *White* et *Garrett* dans leur article " *Improved Pattern Recognition with Artificial Clonal Selection*" utilisent l'algorithme CLONALG pour le problème de reconnaissance de formes et après avoir examiné la performance de la technique sur la classification des caractères non vue, ils ont proposé une version enrichie du CLONALG appelé CLONCLAS (CLONal selection algorithm for CLASsification). Le principe est d'allouer une classe à chaque anticorps de la population, ce qui lui permet d'effectuer une classification en attribuant sa classe à un antigène. Quand un nouvel antigène est exposé à la population, il est alloué à la classe de l'anticorps avec la plus grande affinité pour cet antigène.

IV.3. Description détaillée de l'algorithme proposé

La figure suivante représente l'organigramme résumant les déférentes phases d'exécution de l'algorithme proposé :

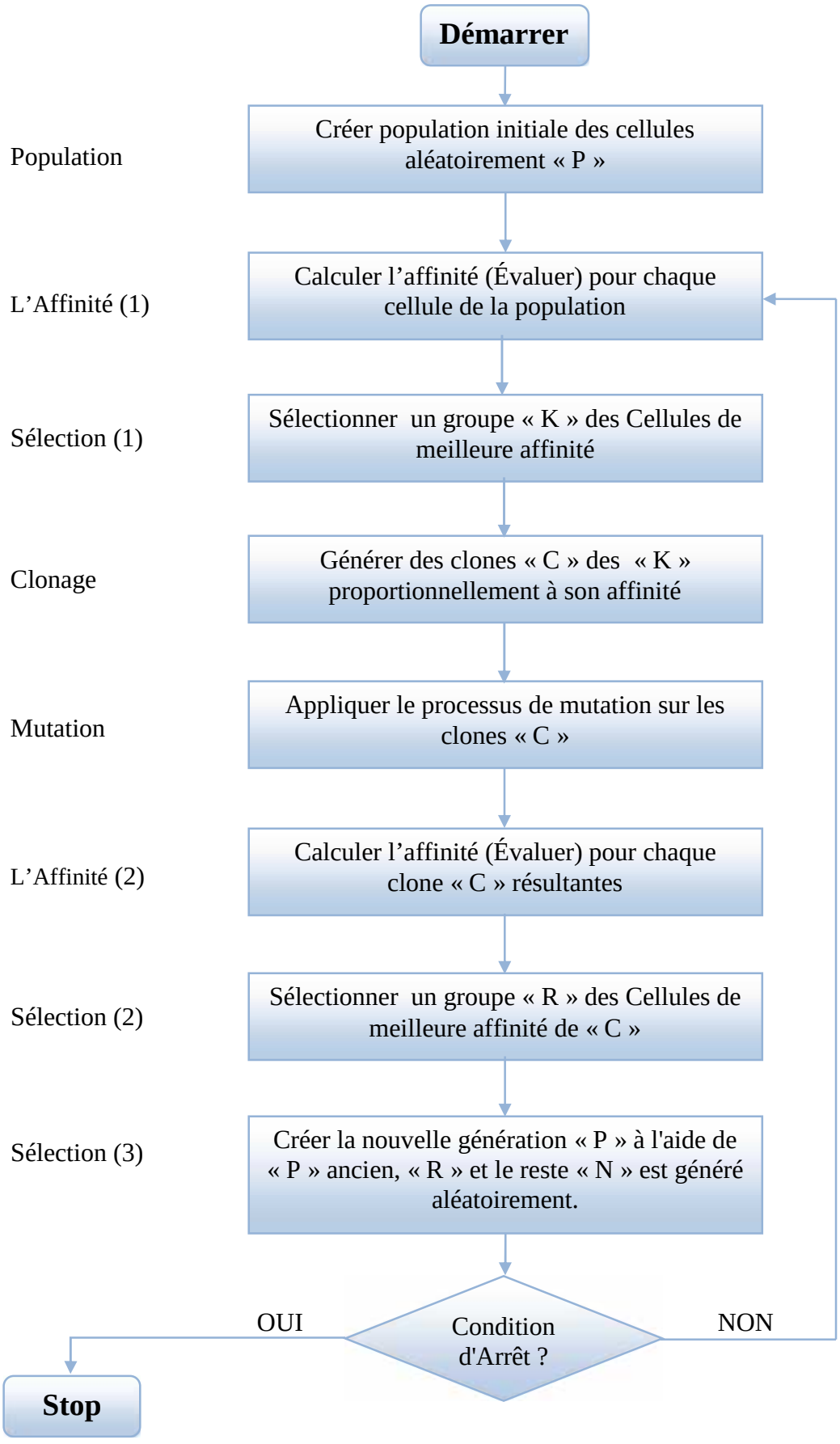

Figure IV.1 : L'organigramme de l'algorithme proposé.

- ***La population initiale* P**

Dans un premier temps, dans notre espace de recherche, après le déploiement des captures dans la zone du captage, les cellules de la population initiale sont codées en binaire (0 ou 1). Les grappes (clusters) sont formées d'une manière aléatoire, un nombre soit 0 ou 1 est affecté à chaque nœud capteur aléatoirement, le 0 pour un nœud régulier et 1 pour un nœud chef de cluster.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	0	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0

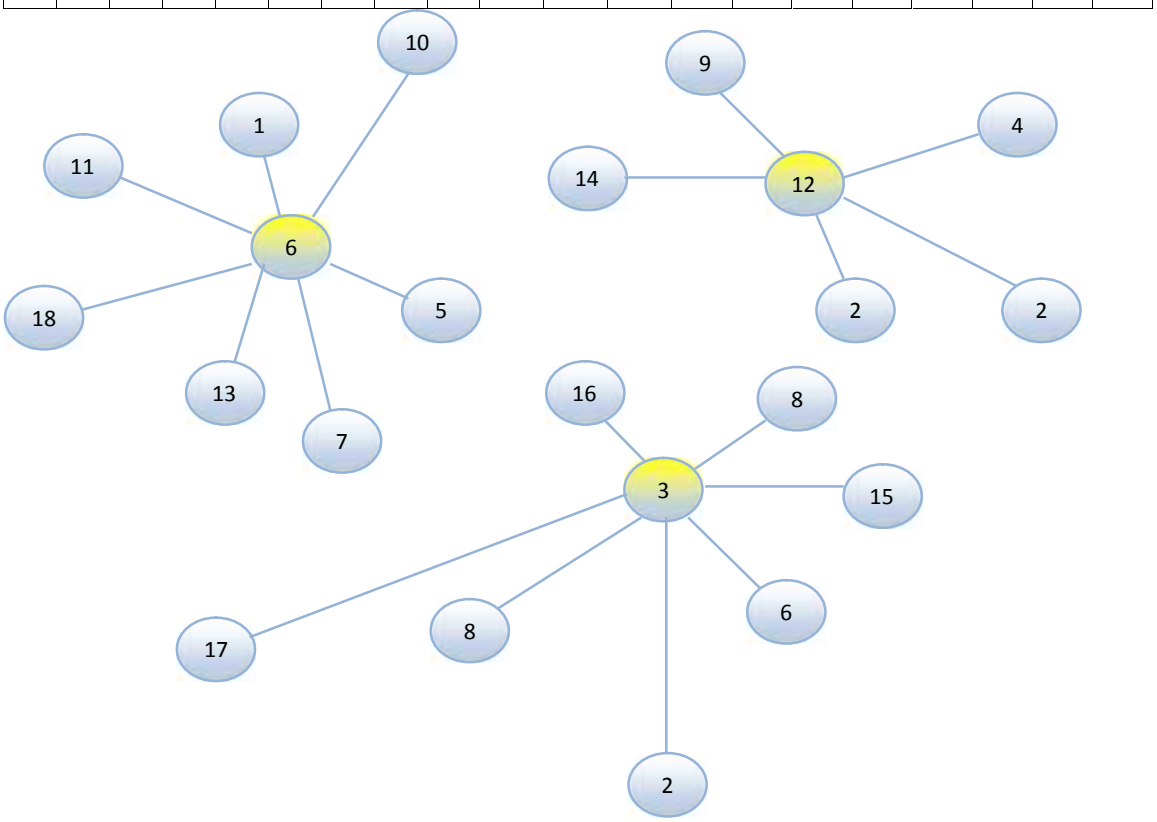

Figure IV.2 : Exemple d'ne cellule codée en binaire.

- ***L'Affinité (1)***

L'affinité (pour chaque cellule anticorps) est la fonction d'évaluation pour mesurer le degré de similarité entre l'antigène et l'anticorps.

L'énergie utilisée pour l'agrégation des données ainsi que la distance totale de transmission, sont les principaux facteurs qu'on cherche à minimiser. En plus, la diminution du nombre de grappes est un autre facteur qui peut être visé par notre fonction d'affinité.

Notre fonction d'affinité est la suivante :

$$Affinité = Min\left(\sum_{i=1}^{m-1}\left(\frac{E}{Er_i} d_{noeud}\ \text{à}\ CH\right) + \sum_{i=1}^{nch}\left(\frac{E}{Er_i} + d_{CH}\ \text{à}\ BS\right)\right)$$

- *m:* le nombre des membres de chaque cluster (m-*1*: le nombre des membres sans chef).
- *nch :* le nombre des clusters dans le réseau (le nombre des chefs des clusters).
- Er : L'énergie restante dans le i^{eme} capteur.
- E : l'énergie initiale de chaque capteur.
- d_{noeud} à CH : la distance d'un nœud simple à sont chef (CH) qu'il regroupé.
- d_{CH} à BS : la distance entre un chef de cluster (CH) et la station de base (BS).

En effet, la fonction d'affinité pour chaque cellule est composée de deux parties, la première cherche à sélectionner les nœuds qui ont plus d'énergie et minimiser la distance totale de transmission à l'intérieur d'un même cluster (intra-cluster), la deuxième partie cherche à choisir les cluster-heads qui ont plus d'énergie et minimiser la distance totale de transmission entre les différentes cluster-head et la station de base (inter-cluster).

Les cellules immunitaires qui ont une faible affinité, ont plus de chance d'être élu pour subir des operateurs de reproduction et mutations.

- ***Sélection (1):***

La sélection naturelle est le mécanisme qui concerne l'efficacité de l'anticorps de l'entité qu'ils représentent, permettant ainsi à cet organisme efficace qui est bien adapté à l'environnement de reproduire (cloner) plus souvent que ceux qui ne le sont pas. Notre algorithme Sélectionner les **K** premier meilleurs Affinité.

- ***Clonage :***

Le clonage désigne principalement un processus de la multiplication artificielle à l'identique d'un anticorps, c'est-à-dire avec conservation exacte du même génome pour tous les descendants (les clones). Le clonage des anticorps est proportionnel à l'affinité de l'antigène auquel elles se sont liées, donc les cellules avec le plus grand taux d'affinité, sont celles qui produisent le plus de clones. Notre algorithme cloner les K meilleurs de population et le mettre dans un groupe **C**.

- ***Mutation :***

La mutation (un type impopulaire) est une forme de reproduction utilisée dans notre algorithme, ce qui provoque les anticorps d'une progéniture d'être différentes de celles de ses parents, notre algorithme appliqué le processus de mutation sur les clone **C**.

- ***L'Affinité (2) :***

L'affinité pour chaque clone de **C**, la fonction d'évaluation mesurer le degré de similarité entre l'antigène et l'anticorps. (Exposer les clones à l'antigène et recalculer leurs nouvelles affinités).

- ***Sélection (2):***

Est le même processus que nous avons mentionné dans *Sélection (1)*, Seulement être appliqué sur les clones. L'objectif de cette opération est pour s'assurer les meilleurs clones **R** sont remplace les cellules (les anticorps) faible affinité aves l'antigène dans la prochaine tour (round).

- ***Sélection (3) :***

Il est le dernier processus. Est déterminée de façon que les cellules qui participent à la session suivante de l'algorithme, Où nous avons sélectionné trois groupes des cellules (anticorps) pour Trier les cellules qui composent la nouvelle population pour le prochain round. Notre algorithme Sélection les K Meilleurs de P, R Meilleurs de C et reste est généré aléatoirement Selon le taux de la sélection.

- ***L'Algorithme :***

*Entrée : **A** = est l'antigène (représente le déploiement des capture).*

Début:

*Créer un ensemble aléatoire d'anticorps, **P**.*

*Pour cet antigène **A** faire :*

1. *Déterminer l'affinité avec chaque anticorps de l'ensemble **P**.*
2. *Créer un sous-ensemble **K** des anticorps avec le plus grand taux d'affinité.*
3. *Générer des clones **C** des anticorps du sous-ensemble **K**. Le nombre de clones pour un anticorps est proportionnel à son affinité*
4. *Appliquer le processus de mutation sur les clones **C** pour augmenter leur degré de correspondance avec l'antigène.*
5. *Exposer les clones **C** de nouveau à l'antigène et recalculer leurs affinités.*
6. *Les meilleurs clones seront placés dans l'ensemble **R**.*
7. *Remplacer les **n** anticorps de plus faible affinité dans **P** par de nouveaux anticorps générés aléatoirement (**P = K + R + n**).*

Fin

IV.4. A propos de l'environnement C ++ Builder

Comme environnement de programmation, nous avons choisi C ++ Builder XE3 d'Embarcadero, qui est l'un des principaux environnements de développement RAD à base de C / C ++, qui est dédié au développement rapide d'applications (Rapid Application Développent) sous Windows.

C++ Builder permet de réaliser de façon très simple l'interface des applications et de relier aisément le code utilisateur aux événements Windows, quelle que soit leur origine (souris, clavier, événement système, etc.)

C++ Builder repose sur un ensemble très complet de composants visuels prêts à l'emploi. La quasi totalité des contrôles de Windows (boutons, boîtes de saisies, listes déroulantes, menus et autres barres d'outils) y sont représentés, regroupés par catégorie. Leurs propriétés sont éditables directement dans une fenêtre spéciale intitulée éditeur d'objets. L'autre volet de cette même fenêtre permet d'associer du code au contrôle sélectionné.

La *figure IV.3* représente un exemple typique de l'interface de C++ Builder au cours d'une session de travail.

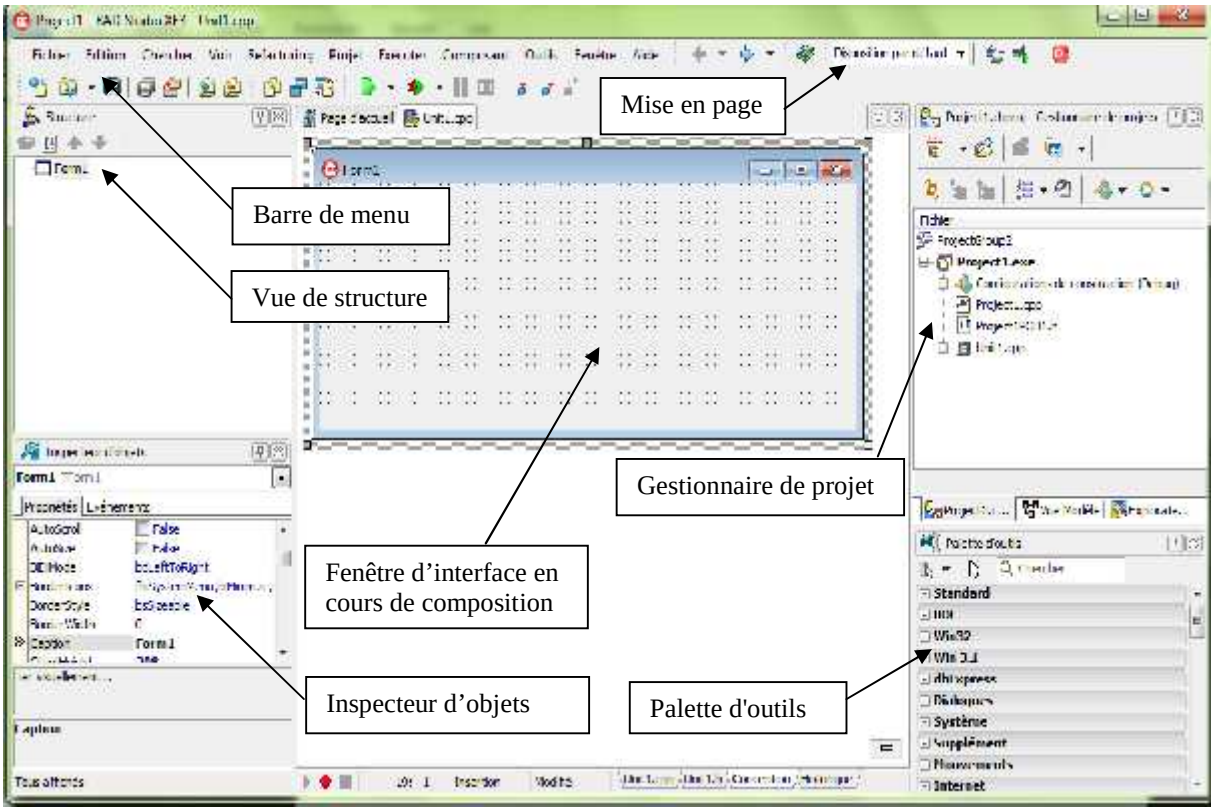

Figure IV.3 : L'interface de C++ Builder

Il est possible d'ajouter à l'environnement de base des composants fournis par des sociétés tierces et même d'en créer soit même.

Un outil RAD c'est également un ensemble de squelettes de projets qui permettent de créer plus facilement une application SDI ou MDI, une DLL, des objets OLE, etc. A chacun de ces squelettes est habituellement associé un expert qui par une série de boîtes de dialogues permet de fixer une partie des options essentielles à la réalisation du projet associé.

Les différences par rapport à Borland C++ sont assez nombreuses. La première réside dans la nature du code produit. Si OWL, la bibliothèque de gestion de la programmation sous Windows et Borland C++ était très compatible C++ ANSI, la gestion de la VCL ne l'est pas pour les raisons exprimées au paragraphe précédent.

En outre, C++ Builder pose les problèmes communément liés aux outils de haut niveau. Par exemple, il est très difficile d'accéder directement aux messages Windows. En effet, s'il est toujours possible d'utiliser les primitives de l'API Windows, ces dernières ont elles - même été encapsulées dans une API de plus haut niveau, fournissant certaines valeurs par défaut à des paramètres clef.

En outre, certains messages Windows se révèlent totalement inaccessibles. Donnons un exemple lié aux boîtes d'édition de texte. Dans OWL, rappelons-le, il était possible de passer la taille du tampon de saisie au constructeur de l'objet associé à une boîte d'édition. Il était alors possible d'associer un événement au remplissage du tampon de saisie. Avec C++ Builder, cette facilité a disparu.

IV.5. Description et paramètres de simulation

Afin et régler les différents paramètres nécessaires pour la mise en ouvre de notre algorithme proposé, nous avons conçu un simulateur d'un RCSF avec une interface conviviale. Il ya plusieurs paramètres dont nous avons besoin et qui conduisent a bien adapter la configuration le réseau et le l'algorithme proposé par rapport au l'objectif de notre travail. Et la *figure IV.4* suivant présente l'ensemble des paramètres à régler au démarrage de notre application.

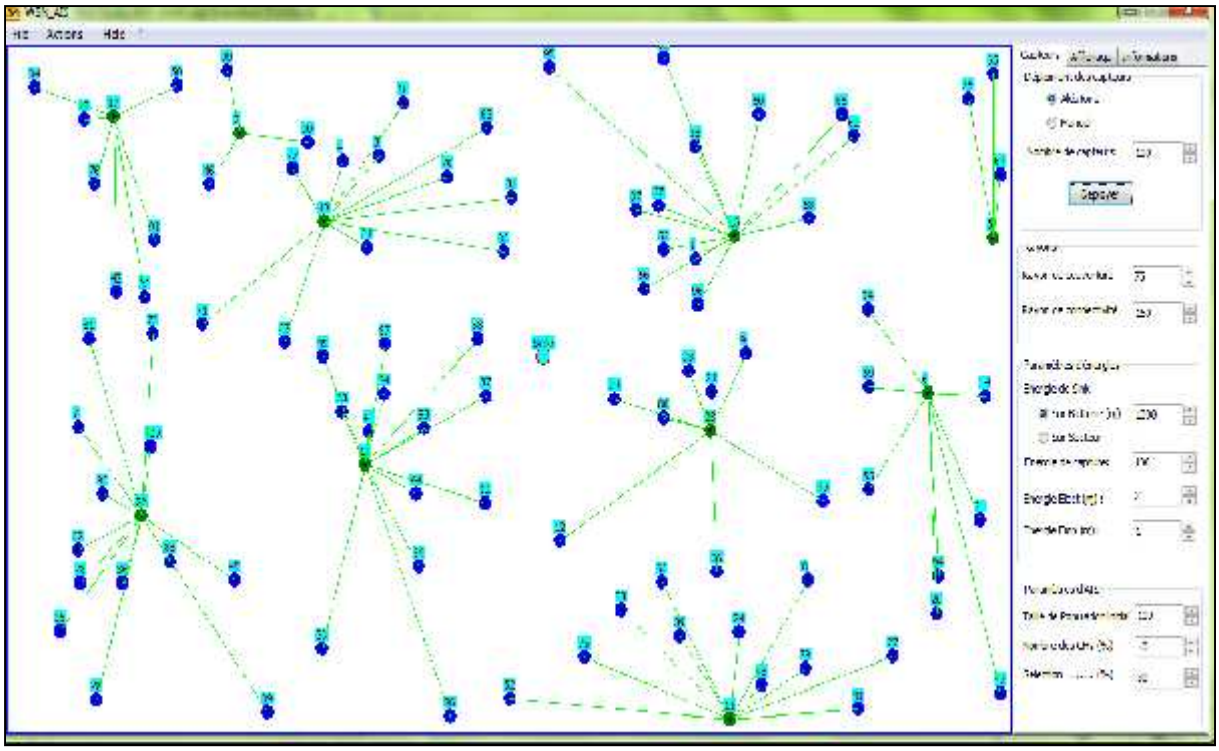

Figure IV.4: Réglage des paramètres de simulation.

IV.5.1. Déploiement des captures

Ces dispositifs (captures) formant les nœuds, détectent les changements environnementaux et les signalent aux autres nœuds sur la base d'une architecture flexible du réseau. Les nœuds capteurs donnent la possibilité d'être déployés dans des environnements hostiles et sur de larges zones géographiques, ces dispositif est déployé soit manuel ou de manière aléatoire selon le cas avec un nombre prédéterminé des captures.

IV.5.2. Les rayons

Il existe deux types, rayon de couverture et de connectivité. Le premier est un porté de capture, est le rayon de la région à surveiller par une capture qu'il soit limité et qui peut varier d'une à l'autre. Et la seconde est un porté de transmission, qui représenter la portée maximale de la communication entre les capteurs pour acheminiez les données à la station de base.

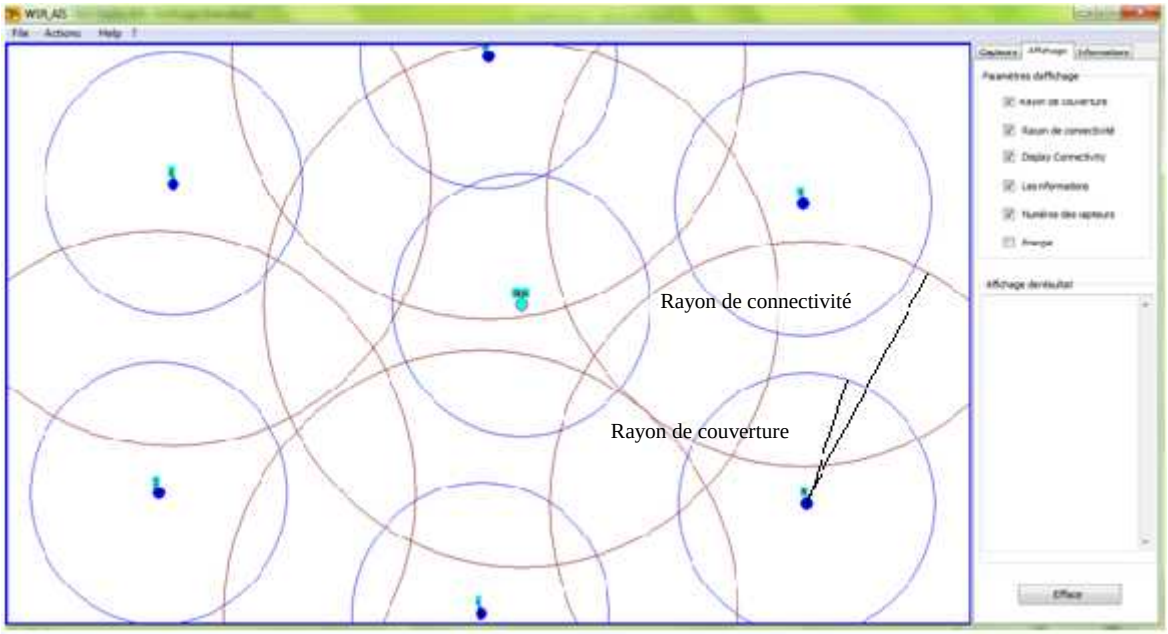

Figure IV.5: Rayon de couverture et de connectivité d'un nœud de capture

IV.5.3. Paramètres d'énergies

Les approches fondées sur les grappes sont adaptés aux applications de surveillance continue. Par exemple, Heinzelman et al décrivent le protocole LEACH, qui est une approche basée sur le cluster hiérarchique auto-organisé pour les applications de surveillance. La zone de collecte de données est divisée au hasard en plusieurs groupes, où le nombre de grappes est prédéterminé selon le nombre des CHs.

Réseaux de capteurs sans fil hiérarchiques à base de cluster peuvent distribuer les ressources d'une manière équilibrée et sont des avantages spéciaux liés à l'évolutivité, la consommation efficace de l'énergie, et l'agrégation de données simple. Le modèle du système utilisé dans ce travail est basé sur le modèle présenté dans [34], où la dissipation d'énergie est essentiellement de transmettre et recevoir des données. Le module radio dissipation d'énergie *E*.

$$E = \begin{cases} lE_{elect} + lE_{mp} & Transmission \\ lE_{elect} & Récéption \end{cases}$$

Où *Eelect (nj/b)* est l'énergie dissipée à chaque émission ou de réception électronique et Emp *(pj/b/m^2)* est l'énergie dissipée par l'amplificateur de puissance d'émission pour atteindre un niveau acceptable au niveau du récepteur. *L* est la longueur du paquet.

Le principal objectif du protocole de routage basé cluster hiérarchique est de générer des grappes avec une efficacité énergétique pour les nœuds de capteurs déployés au hasard.

En utilisant un technique round, chaque membre associé agit comme une tête de cluster. CH reçoit des messages des membres de la grappe et transmet les messages agrégés à une station de base distante (BS). Comme toutes les transmissions sont mono-hop, les membres du cluster transmettent à courte portée des messages de diffusion et CH transmettent à longue portée des messages de diffusion.

L'approche de la tête du cluster peut être une bonne solution pour les clusters où le CH meurt pendant un certains rounds. Depuis le rôle d'un CH consomme de l'énergie, après un certain nombre de transmissions, un nouvel ensemble de grappes est formé.

En d'autres termes, les grappes sont maintenues pendant une courte durée appelé un tour. Un tour se compose d'une phase d'élection et une phase de transfert de données. Dans une phase de l'élection, le capteur nœuds auto-organiser en un nouvel ensemble de grappes, où chaque cluster contient tête de cluster. Dans la phase de transfert de données, les éléments de tête de cluster transmettent un nombre spécifié de transmissions à longue portée à BS.

IV.5.4. Paramètres d'AIS

La population initiale présente l'ensemble aléatoire d'anticorps, Ils représentent la seule entrée de l'algorithme proposé. Le nombre des grappes (clusters) dans le réseau est prédéterminé dans tous les anticorps, par exemple dans le protocole LEACH est 5%. Et on à le Taus de sélection utiliser chaque sélection dans l'algorithme (les meilleurs anticorps dans chaque population, les meilleurs clones par rapport la fonction d'affinité dans laquelle cette algorithme s'exécute en un nombre prédéterminé des rounds (ou itérations).

IV.5.5. Paramètres d'affichage

Leur le déroulement de l'algorithme, Nous pouvons contrôler les paramètres liés ou l'affichage de réseau comme le rayon de couverture, le rayon de connectivité, le numéro de capture et le rapport d'énergie de capture dans chaque round. On à aussi afficher résultat de la simulation concernant le nombre d'itération, la valeur d'affinité dans chaque round, le meilleurs anticorps dans chaque round et le nombre des captures active dans chaque round comme dans la *figure IV.7* suivant qui présente le mode d'exécution de notre simulation après l'initialisation des paramètres réseau et l'AIS et Donne l'ordre de d'exécution en cliquant sur *Run* existe dans la barre de menu de notre application.

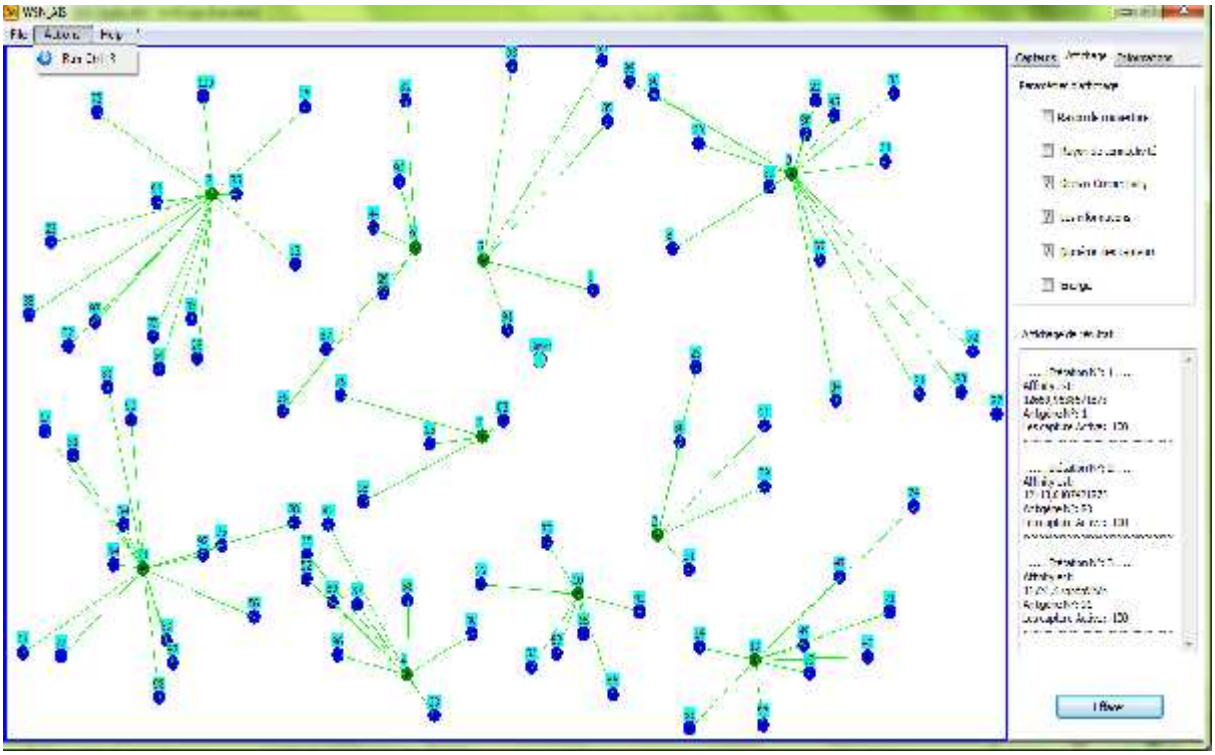

Figure IV.6: Affichage des résultats de la simulation.

IV.6. Simulation et résultats

Dans cette section, nous allons présenter les résultats de simulation que nous avons obtenus. Ces résultats valides les performances de notre modèle de simulation que nous avons conçu, et pour cela, ces résultats seront comparés avec celles des autres travaux de la littérature [35].

Il existe trois techniques d'évaluation de performances d'un système. Le premier c'est la méthode analytique qu'il s'agit de réduire le système en un modèle mathématique et de l'analyser numériquement. L'approche analytique est parfois rapide à réaliser, mais présente le souci de la représentation fidèle du système. Il est parfois très complexe, voire impossible, de modéliser le comportement réel du système mathématiquement. La deuxième technique est par mesure qu'il s'agit de faire des mesures et de les analyser directement sur un système réel. Cette technique permet de comprendre le vrai comportement du système. Faire des mesures sur des systèmes réels n'est pas toujours possible, car ça pourrait gêner le fonctionnement du système ou aussi pour des problèmes de coûts (système non encore existant, instruments de mesure complexes, etc.). La troisième technique la seul disponible est la simulation qu'il s'agit d'implanter un modèle simplifié du système à l'aide d'un programme de simulation adéquat. C'est une technique largement utilisée pour l'évaluation

des performances. Elle présente l'avantage par rapport aux méthodes analytiques de traduire d'une manière plus réaliste le comportement du système à évaluer. On procède généralement à la simulation pour évaluer un nouveau système ou bien pour des raisons de coûts d'évaluation par des mesures réelles. En plus, la simulation permet de visualiser les résultats sous forme de graphes faciles à analyser et à interpréter.

La simulation de notre algorithme constitue la plus importante étape de notre travail puisque on peut prouver les améliorations effectuées en termes d'économie d'énergie et de prolongement de la durée de vie global du réseau en analysant les résultats fournis.

Dans cette simulation, et pour comparer les performances de notre algorithme, en termes de l'économie d'énergie et la durée de vie du réseau par rapport aux deux autres algorithmes de la littérature, à savoir LEACH et GA [35][36]. Tout au long de la simulation et après chaque itération, nous avons mesuré l'énergie résiduelle de chaque nœud capteurs, afin de calculer le nombre total des nœuds vivants. Pour qu'on puisse cette comparaison, nos paramètres de simulation sont les mêmes que dans [35]. Et nous assumons que tous les nœuds ont une position fixe durant toute la période de simulation et la station de base est positionnée an centre de la zone du captage.

Taille de réseau	100 m
Nombre des nœuds	200
Energie Initiale	2 J
E_{elect}	50 nJ/bit
$\boldsymbol{\varepsilon_l}$	0.0013 pJ/bit/m^2
$\boldsymbol{\varepsilon_s}$	10 pJ/bit/m^2
Zone de couverture	100*100 m^2
Distance de SB	200 m
Langur de paquet	200 bits
$d_{co}=d_{crossover}$	85 m

Tableau IV.1: Les paramètres de simulation

Taille de la population initiale	100
Langur de chromosome	20
Taux de croisement	5
Taux de mutation	2
Itération	100

Tableau IV.2 : Les paramètres de GA

Nombre de population des anticorps	100
Nombre des CHs	10%
Taux de mutation	30 %
Itération	100

Tableau IV.3 : Les paramètres d'AISBCP

La *Figure IV.7* suivant représente la formation des grappes (clusters) durant la simulation de notre algorithme proposé.

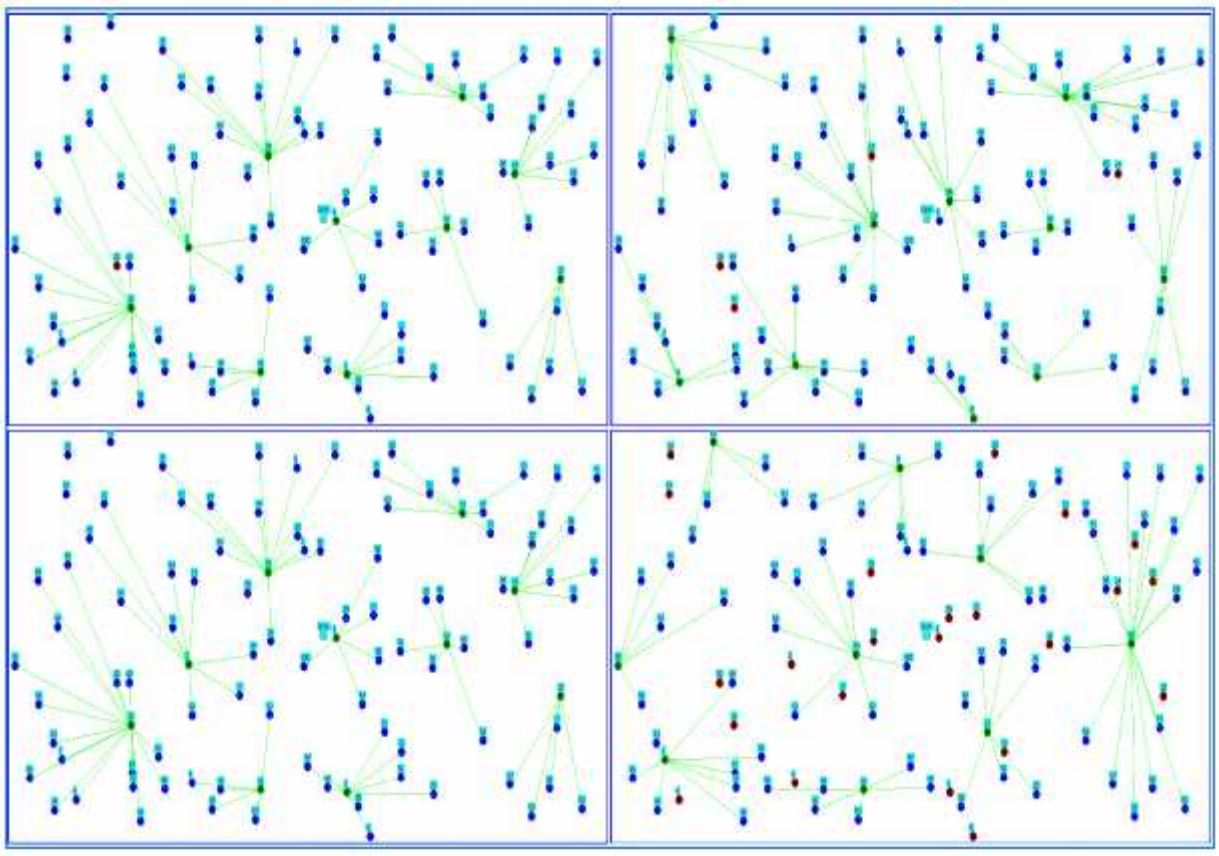

Figure IV.7: La formation des grappes en 4 itérations différentes.

La *Figure IV.8,* montre un résultat de notre algorithme de l'échantillon :

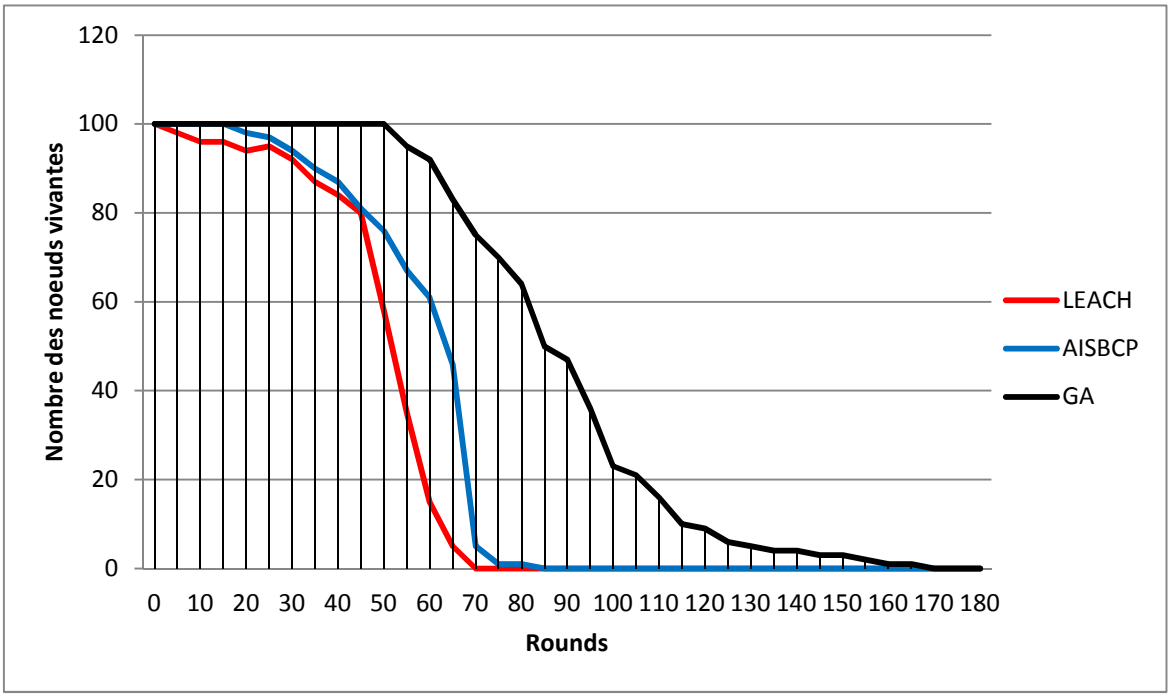

Figure IV.8: La duré de vie du réseau.

On remarque que pour les trois protocoles (LEACH, GA et AISBCP) le nombre des nœuds vivant diminue avec l'augmentation des nombre des rounds du réseau mais Le LEACH juste après le 5 premiers rounds, mais AISBCP rèste à un régime stable jusqua la 20ème rounds (15 rounds après LEACH), contrairement au GA qui rèste toujours stable jusqua la 50eme round.

Pour chacun de ces 3 protocles, la dimuniation se contunuie jusqu'au la mort de tous les nœuds (fin de duré de vie). Le LEACH est en premier lieu (au 70eme round), mais avec AIS le réseau reste fonctionnel environs 10 rounds après le LEACH, et dérnièrement c'est le GA en 170eme rounds. d' ou, nous pouvons constater que en terme d'optimisation de la durée de vie du réseau, notre protocole AISBCP est toujours plus performant par rapport au LEACH. le *Tableau IV.4* suivant représente le nombre des nœuds vivants correspont au chaque protocoles dans chaque 20 rounds.

ROUNDS	Protocoles		
	LEACH	AISBCP	GA
0	100	100	100
20	94	98	100
40	84	87	100
60	15	61	92
80	0	1	64
100	0	0	23
120	0	0	9
140	0	0	4
160	0	0	1
180	0	0	0

Tableau IV.4 Tableau comparative des résultats de simulation.

Alors et pour bien interpreter cette comparaison, la *Figure IV.9* represente une visualisation graphique des résultats obtenus.

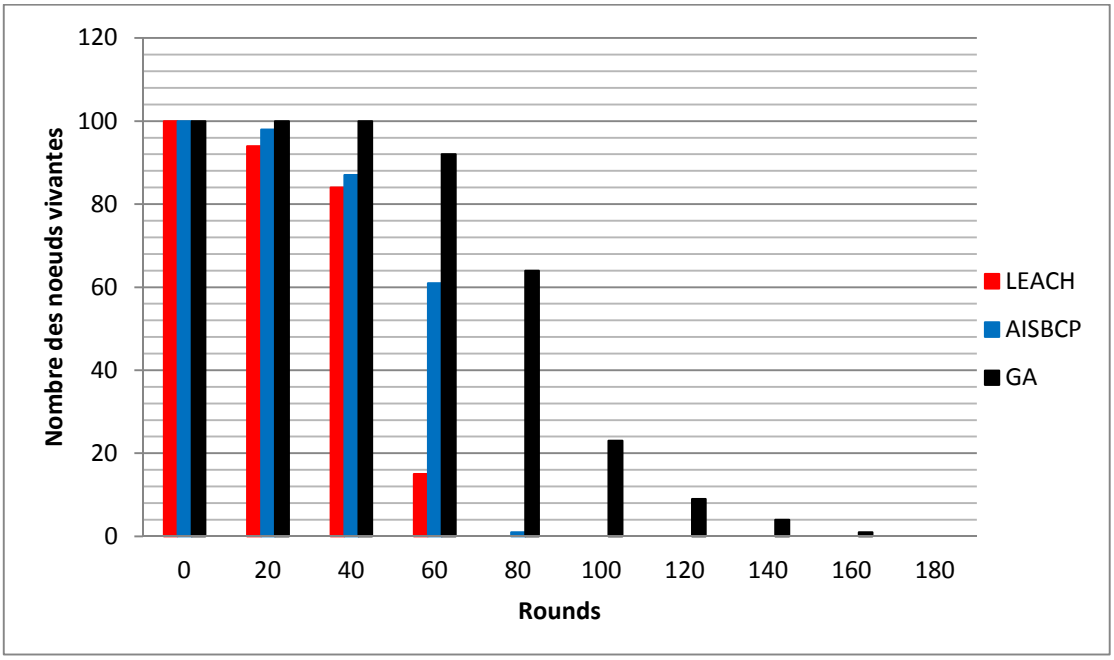

Figure IV.9 : Histogramme des performances de LEACH, GA et AISBCP.

La *Figure IV.10* représente les valeurs de notre fonction d'affinité ou moment de fonctionnement de réseau.

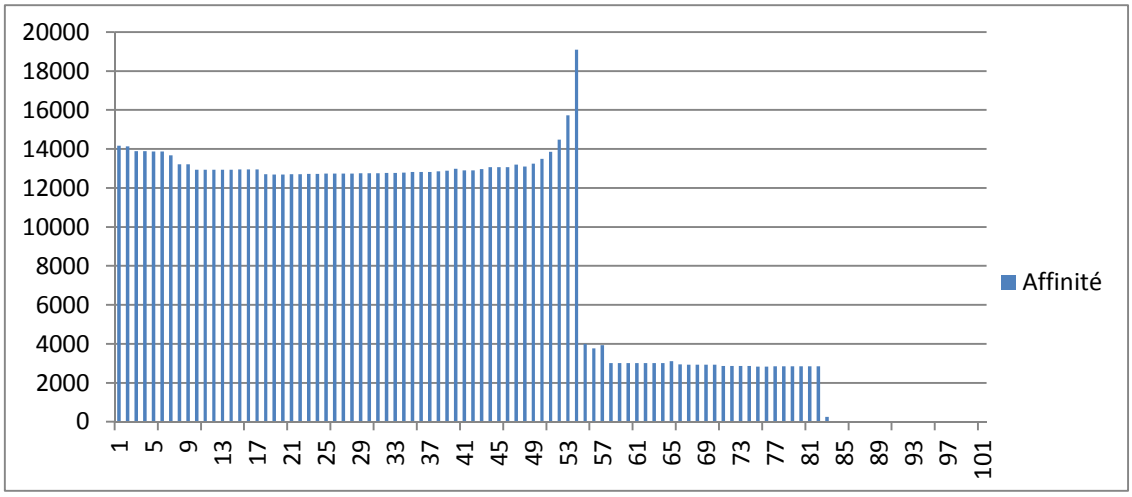

Figure IV.10: Les changements de la valeur d'affinité.

IV.7. Conclusion

En se basant sur les résultats de la stimulation, nous avons démontré que notre protocole améliore la dissipation d'énergie à l'intérieur des clusters, augmente le gain d'énergie, et par conséquent, prolonge considérablement la durée de vie du réseau de 10% à 30% comparé au protocole LEACH.

Conclusion générale

Conclusion générale

Dans ce travail, nous avons pu adapter un algorithme de routage pour l'optimisation de clustering pour un routage efficace en énergie dans les réseaux de capteurs sans fil, il s'agit d'AISBCP. Ce protocole est inspiré à travers d'observations de fonctionnement du système immunitaire. Plusieurs éléments clés du système immunitaire ont été employés pour le développement de ce modèle. L'un de ces éléments est l'abstraction des cellules B en tant que moyen de représentation des données. La réaction entre un antigène et un anticorps des cellules B a été simulées grâce à l'utilisation de la distance euclidienne.

La notion d'affinité entre les cellules est très importante. L'affinité intercellulaire joue un rôle clé dans la réduction des données et des critères de conservation l'énergie de réseau; par conséquent, elle favorise les possibilités de généralisation qui sont importantes pour un meilleur Affinité à l'antigène qui représente le déploiement (les positions) des captures dans la zone de couverture et le rapport d'énergie ou moment de fonctionnement de réseau.

Afin de montrer le bon comportement du protocole proposé, nous avons utilisé un simulateur implémenté sous l'environnement Embarcadero C++ Builder XE3 dans laquelle chaque capteur est défini par son ID et son position dans le champ de captage.

Les simulations ont montré des bons résultats dans la plupart des cas, une consommation énergétique très réduite, et par conséquence une prolongation de la duré de vie des réseaux. Afin de montrer sa performance en termes de conservation d'énergie, notre protocole a été comparé avec deux autres protocoles de la littérature à savoir LEACH et GA.

Pour améliorer les résultats obtenus, nous envisageons, par la suite, les adaptations suivantes:

- Une hybridation entre notre algorithme et une autre méthode (ACO, PSO…) pour un routage multi-saut des données entre les chefs des clusters et la station de base.
- Une technique de mettre en état veille des nœuds redondants, afin de conserver leur énergie et par suite prolonger la duré vie du système.
- Implémenter et tester d'autres techniques intelligentes (Termite Algorithm, Wolf Search Algorithm ⋯etc.

Références

LES REFERENCES

[1]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. "Wireless sensor networks : a survey. Computer Networks (Elsevier) ", vol.38, no.4, March 2000, pp.393-422.

[2]. CAYIRCI, E. (2004). "Wireless sensor networks". In : D. Katsaros et al. (éd), Wireless information highways (pp. 273-301). Hershey : Idea group inc.

[3]. Yazeed Al-Obaisat, Robin Braun "On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management" Institute of Information and Communication Technologies University of Technology, Sydney, Australia.

[4]. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, A survey on sensor networks. IEEE Communications Magazine, vol 40, pp. 102-114, August, 2002.

[5]. Yacine CHALLAL « réseau de capteur sans fil », support de cours, 17/11/2008

[6]. [1] AKYILDIZ (I. F.), SU (W.), SANKARASUBRAMANIAM (Y.) et CAYIRCI. (E.), « Wireless sensor networks : a survey. », IEEE Communications Magazine, vol. 40, n°8, August 2002, p. 102–114.

[7]. Brown, M. J. Users Guide Developed for the JBREWS Project. Los Alamos National Laboratory of California University. 1999. Technical repport LA-UR-99-4676.

[8]. Andrews, P. Johnson and D.C. Remote continuous monitoring in the home.

Telemedicine and Telecare. June 1996, Vol 2, pp. 107-113.

[9]. BALDUS (H.), KLABUNDE (K.) et MUESCH (G.), « Reliable setup of medical body sensor networks », In proc of the European conference on Wireless Sensor Networks (EWSN), Germany, 2004, p. 353–363

[10]. CHINTALAPUDI (K.), FUN.), PARK (J.) et al., « Monitoring civil structures with a wireless sensor network », IEEE Internet Computing, vol. 10, n°2, 2006, p. 26–34.

[11]. HERRING (C.) et KAPLAN (S.), « Component based software systems for smart environments », IEEE Personal Communications, Octobre 2000, p. 60–61.

[12]. HILL (J.-L.), « l'architecture système pour les réseaux de capteurs sans fil », thèse à l'Université de Californie à Berkeley, 2003.

[13]. Hamma, T. Katoh, T. Bista, B.B. Takata, T. « An Efficient ZHLS Routing Protocol for Mobile Ad-Hoc Networks ». 17th International Conference on Database and Expert Systems Applications. 2006, pp.66-70.

[14]. W. HEINZELMAN, A. CHANDRAKASAN, H. BALAKRISHNAN, «Energy-Efficient Communication Protocol for Wireless Microsensor networks», in Proc. 33rd

Hawaii International Conference on System Sciences (HICS '00), Janvier 2000.

[15]. Charles E. Perkins, Pravin Bhagwat. « Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers ». ACM SIGCOMM Computer Communication Review. October 1994, Vol. 24, 4.

[16]. Michael Fitzgerald. Technnology Review: « Tracking a Shopper's Habits. Technology Review ». [En ligne] 04 August 2008, Consulté en Mars 2015. http://www.technologyreview.com/computing/21161/.

[17]. Pei, Guangyu, Gerla, M. and Chen, Tsu-Wei. Fisheye state routing: « a routing scheme for ad hoc wireless networks ». IEEE International Conference on Communication. 2000, Vol. 1, pp. 70-74.

[18]. Stevens, L. Kleinrock and K. Fisheye: « A Lenslike Computer Display Transformation ». s.l.: UCLA, Computer Science Department, 1971. Technical report.

[19]. E. Perkins, E. M. Royer, S. R. Das. «Ad-hoc on demand distance vector (aodv) routing. In IETF, Internet Draft, draft-ietf-manet-aodv-05.txt. [En ligne] 2000.

[20]. David B. Johnson, David A. Maltz, and Josh Broch. DSR: « The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks ». [éd.] Tomasz Imielinski and Hank Korth. Kluwer Academic Publishers . 1996. pp. 153-181.

[21]. Anis Laouiti, Cédric Adjih. « Mesures de performances du protocole OLSR. Projet Hipercom ». 2003. Rapport technique.

[22]. Lindsey, S. Raghavendra, C.S. PEGASIS: « Power-efficient gathering in sensor information systems. IEEE Aerospace Conference Proceedings. 2002, Vol. 3, pp.31-130.

[23]. Lin H., Chu Y. « A clustering technique for large multihop mobile wireless networks ». Vehicular Technology Conference Proceedings. 2000, Vol. 7, pp. 1545-1549.

[24]. O. Younis, S. Fahmy. Heed: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Transactions on Mobile Computing 03 (4). 2004, pp. 366–379.

[25]. Hui Chen, Jannong Cao. A Design Framework and Taxonomy for Hybrid Routing Protocols in Mobile Ad Hoc Networks. IEEE Communications Surveys & Tutorials, 3rd quater 2008. 2008, Vol. 10,3

[26]. P. Allain, Les médicaments 3ème édition. 2006, Magazine pharmacorama.

[27] Leandro Nunes De Castro, Fernando J. Von Zuben, The Construction of a Boolean

Competitive Neural Network Using Ideas from Immunology. S.l.: Neurocomputing, 2003. P.51-85.

[28]. Mehdi Dastani, Amal El Fallah Sghrouchni. Programming Multi Agents Systems. S.l. : First International Workshop, ProMAS, 2003.

[29]. U.Aickelin and D.Dasgupta, "Artificial immune systems" in Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques. 2005, pp. 375-399.

[30]. Hiba Khelil, Abdelkader Benyettou. "Application du système immunitaire artificiel ordinaire et amélioré pour la reconnaissance des caractères artificiels". Université des sciences et de la technologie d'Oran : Laboratoire Signal Image Parole SIMPA, 2006.

[31]. Medical News Today. [En ligne].http://www.medicalnewstoday.com/info/diabetes/ Consulté en Avril 2015.

[32]. Timmis, T. Knight, L.N. de De Castro, and E. Hart., "An O verview of Artificial Immune Systems," in Computation in Cells and Tissues: Perspectives and Tools for Thought, Natural Computation Series., 2004, pp. 51-86.

[33]. A. Watkins, L. Boggess, and J. Timmis, "Artificial Immune Recognition System (AIRS): An Immune-Inspired Supervised Learning Algorithm," Genetic Programming and Evolvable Machines, pp. 291–317, 2004.

[34]. W. R. Heinzelman, A.P. Chandrakasan. An Application-Specific Protocol Architecture for Wireless Micro-sensor Network. IEEE Transactions on Wireless Communications, Vol. 1, N°4, 2002.

[35]. W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan,"Energy-Efficient Communication Protocol for Wireless Microsensor Networks," Proceedings of the Hawaii International Conference on System Sciences, Hawaii, 4-7 January 2000, pp.3005-3014.

[36]. Ali Norouzi, Faezeh Sadat Babamir, Abdul Halim Zaim "A New Clustering Protocol for Wireless Sensor Networks Using Genetic Algorithm Approach" Wireless Sensor Network, october 2011.

[37]. McCoy & Devarajan. "Artificial Immune Systems and Aerial Image Segmentation", en 1997.

[38]. Potter et De Jong. "The Coevolution of Antibodies for Concept Learning", en 1998.

[39]. Hart et al. "Producing Robust Schedules Via An Artificial Immune System", en 1998.

[40]. Hunt & Fellows "Introducing an Immune Response into a CBR system for data Mining", en 1996.

[41]. Forrest & Hofmeyr. "John Holland's Invisible Hand: an Artificial Immune System " , en 1999.

[42]. Forrest et al dans "Using Genetic Algorithms to Explore Pattern Recognition in the Immune System" en 1993.

[43]. Kephart. "A Biologically Inspired Immune System for Computers", en 1994.