Table des matières

Table des figures

Liste des tableaux

Liste des algorithmes

Introduction Générale

Contexte

Les Réseaux de Capteurs Sans Fil (RCSFs) sont considérés comme un outil très puissant pour connecter les mondes physique et numérique. Cette classe particulière des réseaux Ad hoc [14] [15] [16] a fait l'objet d'une attention particulière au cours des dernières années parce qu'elle est considérée comme étant une technologie verte d'avenir permettant des applications dans différents domaines, incluant la surveillance des zones sensibles clôturées (p. ex., un site pétrolier ou nucléaire) et les frontières internationales, la surveillance de l'environnement, la surveillance des structures de bâtiments, la santé, l'industrie, l'agriculture, etc [11,17,18]. En outre, l'intégration graduelle des RCSFs à internet, dans le cadre du concept de l'internet des objets (en Anglais, Internet of Things (IoT)) [19–21], a permis d'accroître l'utilité de ces réseaux et par conséquent leur importance dans la vie de tous les jours. Cette intégration qui est décrite comme étant l'une des tâches de conception les plus importante de l'IoT, permet en effet aux flux de données générés par un RCSF d'être accessibles à tout utilisateur autorisé, partout dans le monde, en utilisant des mécanismes standards.

Les RCSFs sont la conséquence des avancées impressionnantes dans les technologies telles que l'intégration à très grande échelle (VLSI), les Systèmes Micro-Electro-Mécaniques (SMEM) et les communications sans fil. Un RCSF est constitué de plusieurs nœuds capteurs, dits aussi *motes*, peu coûteux et à faible consommation d'énergie (en Anglais low cost, low power), miniaturisés et multi-fonctionnels (scalaires et multimédias), allant de quelques dizaines à plusieurs centaines ou même des milliers, où chaque nœud est connecté à un ou plusieurs autres nœuds via des liaisons sans fil de type Radio-Fréquences (RF), acoustique, optique ou InfraRouge (IR). Les nœuds capteurs sont dotés de ressources limitées en termes d'énergie, de portée de capture et de communication, de bande passante, de vitesse de traitement et de capacité de stockage. Ils sont déployés, d'une manière aléatoire ou déterministe, dans une zone d'intérêt (indoor ou outdoor) pour collecter des informations du monde physique, éventuellement les traiter et les transmettre à un ou plusieurs nœuds collecteurs appelés puits (en anglais sinks). Un nœud puits peut soit utiliser localement les données provenant des nœuds capteurs, soit les relayer à un centre de décision distant, via une liaison haut débit (internet ou satellite).

Il existe de nombreux défis à surmonter dans ce type de réseaux, tous liés à la principale préoccupation qui est la *consommation d'énergie*. Parmi ces défis, nous citerons la couverture, la connectivité, le *routage*, la tolérance aux pannes et la sécurité.

La surveillance des zones sensibles clôturées (p. ex., un site pétrolier ou nucléaire) et des frontières internationales [22–29], est un domaine attrayant dans lequel les RCSFs sont de plus en plus utilisés. Etant donné que ce genre d'applications, comme d'ailleurs la plupart des applications à base des RCSFs, nécessitent un grand nombre de nœuds capteurs qui couvrent de grandes zones, il en résulte que le nœud sink pourrait être hors de la portée de communication du ou des nœud(s) source(s). Dans ce cas de figure une approche de communication multi-sauts est nécessaire. Ce mode de communication est aussi employé :

1. En raison de la rareté de la ressource énergétique au niveau des nœuds capteurs et de la limite de la puissance de transmission de ces derniers.
2. En raison de la nature des missions de surveillance à charge des applications dédiées à la surveillance des zones sensibles où les niveaux de puissance d'émission des nœuds capteurs sont maintenus à bas niveau afin d'éviter l'interception des signaux radio-fréquence. Ce type de missions de surveillance exige le plus souvent de la discrétion et même de la furtivité.
3. Pour surmonter l'atténuation du signal (surtout pour les liens de longue distance) dans les RCSFs déployés dans un environnement *réaliste* caractérisé par la présence du phénomène de l'*irrégularité* de la radio [30,31] dû à de multiples facteurs, tels que le type d'antenne et le type du médium, les obstacles (p. ex., les bâtiments, les collines, les montagnes) et les conditions météorologiques.

Le processus d'établissement de chemins d'un nœud source vers le sink à travers un ou plusieurs relais est appelé *routage* et est assuré par la couche réseau de la pile protocolaire des RCSFs. Le routage géographique, dit aussi routage basé sur la position, est un paradigme de routage approprié pour les RCSFs [32–34]. Il permet en effet la conception de protocoles efficaces et évolutifs, basés uniquement sur des décisions locales et nécessitant des capacités de stockage minimales. Ce type de routage s'appuie principalement sur deux techniques pour acheminer les paquets de données dans un RCSF, depuis les nœuds sources vers le(s) nœuds puits, à savoir les stratégies de routage en mode *glouton* (en Anglais, *Greedy* routing) et en mode *périmètre*.

En outre, additivement à un protocole de routage permettant le passage à l'échelle, efficace en énergie et fiable, les applications de surveillance des zones sensibles clôturées et des frontières internationales font appel à d'autres solutions pour rationaliser davantage la consommation de l'énergie dans le RCSF, telles que la mise en veille, la plupart du temps, de l'émetteur-récepteur sans fil et le contrôle de la puissance d'émission de ce dernier. Le but de cette rationalisation est d'étendre la durée de vie du RCSF et par conséquent celle de la mission de surveillance.

Motivation

1. La sécurisation des sites stratégiques ainsi que les frontières internationales d'un pays est cruciale pour la sécurité de celui-ci. Dans le contexte financier mondial actuel, les gouvernements s'efforcent à garantir le risque zéro au niveau de leurs sites stratégiques, et ce à moindre coût. Les RCSFs sont un sérieux candidat pour ce genre de mission, en raison entre autres de :

— Leur aspect économique

— leur aspect miniature qui permet la discrétion et la furtivité

— Leur fonctionnement sans intervention humaine

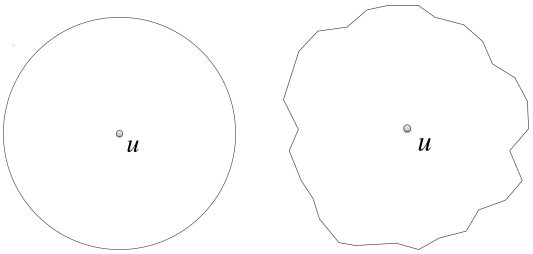
— Leur déploiement dans des zones inaccessibles ou hostiles à la présence humaine

— leur intégration à Internet grâce au concept de l'IoT.

Notons que des réseaux de centaines de nœuds de capteurs sont déjà utilisés dans le cadre des missions sensibles de surveillance.

2. L'économie d'énergie, qui constitue une préoccupation majeure dans les RCSFs, fait partie d'une démarche globalisante visant la diminution du CO2 dans l'atmosphère et encourage les technologies vertes.
3. Les RCSFs dédiés à la surveillance des zones clôturées et des frontières internationales sont généralement déployés en grand nombre et avec une forte densité sur une assez large zone. Il convient de noter que cette densité de déploiement permet d'obtenir une redondance qui est exploitée à différentes fins [35,36] (p. ex., couverture, économie d'énergie, tolérance aux pannes). Le grand nombre de nœuds empêche les nœuds de connaître la topologie de l'ensemble du RCSF. Par conséquent, des protocoles qui fonctionnent avec une connaissance limitée de la topologie, doivent être développés pour permettre le passage à l'échelle. Le routage basé sur la position ou géographique ne nécessite pas l'établissement ou la maintenance de routes et par conséquent il permet le passage à l'échelle, et ce même dans le cas où le réseau est très dynamique [33]. Ce type de routage peut être considéré comme une rupture par rapport aux paradigmes de routage dépendant de la topologie, grâce à l'utilisation de l'emplacement physique dans le processus de routage [34]. Un autre avantage du routage géographique est qu'il prend en charge la livraison des paquets à tous les nœuds situés dans une région géographique donnée en utilisant le géocasting [37]. De nos jours, les protocoles de routage géographiques s'imposent de plus en plus en raison du développement rapide de solutions logicielles et matérielles permettant de déterminer les positions absolues ou relatives des nœuds dans les réseaux Ad hoc déployés en indoor/outdoor [38].
4. Le modèle largement utilisé pour l'étude des RCSFs est ce qui est appelé le modèle à base de disques unitaires (en Anglais, Unit Disk Graph (UDG) [39, 40]. Ce modèle est fondé sur les principes de la théorie des graphes. Il représente la portée d'un nœud capteur sous forme d'un disque centré autour du nœud avec un rayon égal à 1 (voir Figure 1(a)). Comme nous pouvons le constater, un UDG est une simplification de la réalité dans la mesure où il ne reflète pas la nature variante, à travers le temps et l'espace, du canal sans fil. En effet, un UDG ne tient pas compte du phénomène de l'irrégularité de la radio [30, 31] du au type d'antenne et du médium, à la présence d'obstacles (p. ex., les bâtiments, les collines, les montagnes) et aux conditions météorologiques. Ce phénomène est à l'origine de l'irrégularité des portées de transmission, tel que le montre la Figure 1(b). Pour représenter les caractéristiques aléatoires du canal sans fil et par conséquent produire de solides résultats théoriques, la communauté scientifique a eu recours au modèle réaliste basé sur des disques non unitaires (en Anglais, Non-Unit Disk Graph (N-UDG)) (voir Figure 1(b)). Notons

que ce modèle reste peu exploré dans la littérature. Le fait de se rapprocher de la réalité pour proposer des solutions novatrices complètes et viables est une tendance de recherche aujourd'hui prometteuse.



(a) UDG. (b) N-UDG.

FIGURE 1 – UDG vs. N-UDG

Problématique

En bref, dans cette thèse il s'agit d'apporter des réponses aux questions suivantes :

1. Comment peût-on assurer une détection efficace d'intrus dans un site sensible clôturé, en s'appuyant sur la technologies des RCSF et en considérant un modèle d'étude radio réaliste ?
2. Comment peût-on garantir une remontée d'alarmes la plus sûre et la plus efficace possible à l'aide d'un RCSF, en cas de détection d'intrus ?
3. Comment peût-on optimiser la consommation de l'énergie dans un RCSF dédié à la surveillance des zones sensibles clôtures, en se basant sur une approche inter-couches ?

L'économie d'énergie et la fiabilité du routage des alertes, depuis le(s) nœuds source(s) où il y a eu intrusion, vers le nœud puits, constituent des défis majeurs lors de la conception des systèmes de surveillance basés sur les RCSFs, utilisés pour sécuriser les zones sensibles clôturées et les frontières internationales.

Les nœuds capteurs disposent en effet d'un budget énergétique très limité puisqu'ils sont alimentés par des batteries qui de surcroît ne sont pas facilement rechargeables ni remplaçables à cause de :

1. La nature de la mission de surveillance, qui le plus souvent nécessite de la discrétion et même de la furtivité,
2. L'environnement hostile dans lequel le réseau est déployé,
3. L'ampleur du déploiement (facteur d'échelle).

Par conséquent, la conception d'un protocole de surveillance à efficacité énergétique permet de prolonger la durée de vie du RCSF et par conséquent la durée de vie de la mission de surveillance.

D'autre part le canal radio peut être à l'origine de liaisons sans fil non fiables à cause du phénomène de l'irrégularité des portées de transmission. Ce phénomène est la conséquence de

plusieurs facteurs (p. ex., le type d'antenne et du médium, les obstacles, les conditions météorologiques) [30, 31]. Il est à l'origine de l'asymétrie des liens dans les RCSFs. Plusieurs études récentes ont montré qu'il a un impact négatif sur les protocoles de routage, notamment géographiques [39,41–47]. Par conséquent, la revisite des deux techniques de routage les plus employées par les protocoles géographiques, à savoir le routage en mode *glouton* (en Anglais, *greedy* routing) et le routage en mode *périmètre*, doit être faite à lumière du phénomène de l'irrégularité de la radio. C'est ce qui a été fait dans cette thèse, en considérant le modèle d'étude réaliste dit N-UDG.
La conception d'un protocole de surveillance garantissant un routage fiable des paquets d'alertes, à partir des nœuds capteurs sources où l'intrusion a été détectée, vers le nœud puits, s'avère donc d'une importance capitale afin d'assurer une protection élevée de la zone surveillée.

La conception des protocoles selon l'architecture en couches du modèle OSI, largement utilisée dans les réseaux de communication filaires, pourrait ne pas convenir aux réseaux sans fil tels que les réseaux cellulaires, les réseaux mobiles Ad hoc (MANET) et les RCSFs. En effet, les réseaux sans fil ont des particularités qui les distinguent des réseaux filaires conventionnels [48] (nature de diffusion du canal sans fil ainsi que sa nature variante à travers le temps et l'espace), et qui doivent être prises en compte lors de la conception de protocoles au niveau des différentes couches de la pile protocolaire. De surcroît, les RCSFs ont également des caractéristiques différentes des réseaux sans fil traditionnels, notamment la rareté de la ressource énergétique. Par conséquent, une approche émergente, dite Conception Inter-Couches (en Anglais, Cross-Layer Design) (CIC/CLD) [48–53], s'est imposés dans les réseaux sans fil et notamment dans les RCSFs. Cette nouvelle technique d'optimisation des performances par interaction ou fusion des couches, vise à améliorer les performances globales du réseau sans fil, telles que l'augmentation de la capacité du réseau, l'efficacité énergétique et la qualité de service (QoS). Cette approche a été adoptée pour la conception du protocole de surveillance proposé dans le cadre de cette thèse.

Objectifs

Notre travail consiste à proposer un protocole inter-couches pour la surveillance, à base des RCSFs avec un cycle d'activité (en Anglais, duty-cycled WSNs), des zones sensibles clôturées, en considérant un modèle radio réaliste (N-UDG). Le protocole doit :

1. Etre à efficacité énergétique afin de prolonger la durée de vie du réseau de surveillance et par conséquent celle de la mission de surveillance.
2. Assurer un routage géographique fiable des alertes vers le nœud puits afin de garantir une protection élevée de la zone surveillée. Etant donné que la couche PHY a un impact direct sur les performances des protocoles de routage géographique, comme nous l'avons mentionné précédemment, un protocole de routage tenant compte des conditions radio réalistes considérées, est nécessaire.

Le protocole de surveillance proposé utilise une approche inter-couches basée sur l'interaction des couches physique (PHY), contrôle d'accès au Médium (MAC) et réseau (NET).

Contributions

Cette thèse a fait l'objet de deux contributions que nous pouvons résumer comme suit :

— **Contribution 1→** : Proposition d'un algorithme de routage en mode *glouton* (en Anglais, *greedy*), inter-couches, appelé Cross-Layer Greedy Routing (CL-GR) [5], qui permet un routage géographique correct sur un N-UDG. Il fournit deux nouvelles stratégies de routage en mode *glouton*, appelées respectivement :

1. Progress towards the sink node through Symmetrical links that experience the lowest Path Loss (PSPL)
2. progress through symmetrical links, combining the Maximum Distance forwarding strategy and the PSPL (MDPSPL)

CL-GR a été comparé à :

1. Une version améliorée de l'algorithme de routage en mode *greedy* utilisé par le protocole Greedy Perimeter Stateless Routing (GPSR) [13], qui peut être exécutée sur un N-UDG, et que nous appelons E-GR (Enhanced Greedy Routing)
2. L'algorithme COP_GARE [54].

Les résultats de la simulation montrent que la PSPL et la MDPSPL permettent un meilleur ratio de livraison des paquets (en Anglais, Packet Delivery Ratio (PDR)) et une meilleure efficacité énergétique par rapport E-GR et à COP_GARE. En termes de délai de bout en bout, tandis que la stratégie PSPL augmente significativement cette métrique, la stratégie MDPSPL permet un délai de bout en bout satisfaisant, comparativement à E-GR et à COP_GARE.

— **Contribution 2→** : Proposition d'un protocole de surveillance des zones sensibles clôturées, en utilisant les RCSFs avec un cycle d'activité (en Anglais, duty-cycled WSNs). Le protocole en question [55] est basé sur une approche inter-couches et est conçu en utilisant le modèle d'étude réaliste, à savoir le modèle N-UDG. Il permet une efficacité énergétique et garantit un routage géographique fiable des alertes vers le nœud puits, en présence de liens asymétriques dus au phénomène de l'irrégularité de la radio.

Le protocole de surveillance proposé identifie d'abord les nœuds capteurs situés sur la clôture de la zone sensible à surveiller, qui seront utilisés comme des nœuds *sentinelles* (en Anglais Sentinel Nodes (SNs)), c.-à-d. des nœuds qui sont toujours dans un état actif. Les autres nœuds seront utilisés comme des nœuds relais avec un cycle d'activité (en Anglais, Duty-Cycled Relay Nodes (DC-RNs)), et ce pendant la phase de communication de données. Le processus d'identification des nœuds *sentinelles* et le routage des messages d'alerte (en Anglais, Alert Message (AM)) vers le nœud puits, sont tous deux effectués en utilisant une version améliorée du protocole GPSR (Greedy Perimeter Stateless Routing), qui s'appuie sur un (N-UDG), et est appelée GPSR over Symmetrical Links (GPSR-SL). Les deux stratégies de routage employées par GPSR-SL, en l'occurrence le mode *glouton* et le mode *périmètre*, acheminement les paquets d'alerte via les liens symétriques uniquement. En outre, afin de pallier à l'échec de routage du mode périmètre, résultant de l'échec

des algorithmes de planarisation [9, 41] lorsqu'ils sont exécutés sur un N-UDG, nous avons utilisé le correctif dit du témoin mutuel (en Anglais, Mutual Witness (MW) [9, 56]).

Les résultats de la simulation montrent que le protocole de surveillance proposé atteint un ratio de livraison de paquets (en Anglais, Packet Delivery Ratio (PDR)) plus élevé d'environ 3.63%, une efficacité énergétique et une latence satisfaisante par rapport au même protocole de surveillance basé sur le protocol GPSR.

Structure de la thèse

Ce manuscrit est structuré en deux parties :

— Une partie Etat de l'art (RCSFs et routage dans ces derniers), constituée de deux Chapitres, en l'occurrence Chapitre 1 et Chapitre 2.

— Une Partie Contributions constituée elle aussi de deux Chapitres, en l'occurrence Chapitre 3 et Chapitre 4. Etant donné que la thèse a fait l'objet de deux contributions, chacun des deux chapitre est dédié à une contribution.

Une Conclusion générale et les perspectives de nos travaux clôturent le manuscrit.

— **Chapitre 1 → Les Réseaux de Capteurs Sans Fil** : Ce chapitre est consacré à la présentation d'un état de l'art sur les RCSFs. Nous définissons tout d'abord ce nouveau concept des RCSFs, puis nous énumérons les caractéristiques intrinsèques de ce type de réseaux émergents, les défis auxquels ils font face, leurs types, leurs domaines d'application, leurs systèmes d'exploitation et les outils pour les évaluer. Ensuite, nous décrivons les aspects des couches de la pile protocolaire des RCSFs en insistant sur la nécessité de la conception de nouveaux protocoles, à tous les niveaux de cette pile protocolaire, qui tiennent compte des caractéristiques intrinsèques de ce type de réseaux. La conception inter-couches est décrite comme étant une solution prometteuse pour les RCSFs, dans la mesure elle vise à améliorer les performances globales du réseau sans fil, telles que l'augmentation de la capacité du réseau, l'efficacité énergétique et la qualité de service (QoS). A la fin du chapitre, nous abordons l'interconnection des RCSFs avec les réseaux externes, notamment l'internet, et l'environnement de déploiement des RCSFs. En ce qui concerne ce dernier point, nous décrivons trois modèles de propagation de signaux radio, tout en mettant l'accent sur l'importance de considérer un modèle de propagation radio réaliste lors de l'étude des RCSFs.

— **Chapitre 2 → Le routage dans les RCSFs** : Ce chapitre présente un état de l'art sur le routage dans les RCSFs avec une mise en évidence du routage géographique auquel nous nous intéressons dans cette thèse. Nous présentons tout d'abord les défis et les métriques du routage dans ce type de réseaux, puis nous donnons une classification des protocoles de routage dans les RCSFs, selon trois critères qui sont : la structure ou l'organisation du réseau, le processus de découverte des routes et la stratégie de routage employée. Au sein de la classe des protocoles géographiques, nous détaillons le fonctionnement des deux

approches d'acheminement de paquets les plus utilisées par ces protocoles, en l'occurrence l'approche en mode *glouton* et l'approche en mode *périmètre*. Le protocole géographique Greedy Perimeter Stateless Routing (GPSR) est aussi largement décrit. A la fin du chapitre nous expliquons les problèmes auxquels font face les techniques de routage en mode *glouton* et en mode *périmètre* quand elles sont exécutées sur un N-UDG qui reflète la présence du phénomène de l'irrégularité de la radio.

— **Chapitre 3 → Protocole de routage géographique inter-couches pour les RCSFs avec des portées radio irrégulières** : Dans ce chapitre, nous présentons tout d'abord une classification des stratégies de routage en mode *glouton* et ce sur la base d'une revue de littérature. Ensuite, nous détaillons notre première contribution qui consiste en un algorithme de routage géographique en mode *glouton*, inter-couches, appelé Cross-Layer Greedy Routing (CL-GR), permettant un routage correct sur un N-UDG. Nous commençons, en effet, par décrire le modèle réseau adopté ainsi que les hypothèses considérées, qui nous ont servis pour mener cette étude. Ensuite, les deux nouvelles stratégies de routage en mode *glouton* fournit par CL-GR, appelées respectivement Progress towards the sink node through Symmetrical links that experience the lowest Path Loss (PSPL), et progress through symmetrical links, combining the Maximum Distance forwarding strategy and the PSPL (MDPSPL), sont largement décrites. Enfin, nous discutons les résultats de simulation obtenus et nous présentons une analyse des coûts de caclcul et de communication des deux stratégies proposées. Nous tenons à noter que nous avons comparé notre CL-GR à une version améliorée de l'algorithme *greedy* utilisé par le protocole Greedy Perimeter Stateless Routing (GPSR) [13], qui peut être exécutée sur un N-UDG, et que nous appelons E-GR (Enhanced Greedy Routing), et à l'algorithme COP_GARE [54]. Les résultats de la simulation montrent que la PSPL et la MDPSPL permettent un meilleur ratio de livraison des paquets (en Anglais, Packet Delivery Ratio (PDR)) et une meilleure efficacité énergétique par rapport à E-GR et à COP_GARE. En termes de délai de bout en bout, tandis que la stratégie PSPL augmente significativement cette métrique, la stratégie MDPSPL permet un délai de bout en bout satisfaisant, comparativement à E-GR et à COP_GARE.

— **Chapitre 4 → Protocole de surveillance à efficacité énergétique et fiable dédié aux zones sensibles clôturées** : Ce chapitre aborde notre deuxième contribution qui consiste à proposer un protocole de surveillance des zones sensibles clôturées, tel qu'un site pétrolier ou nucléaire, à base des RCSFs avec un cycle d'activité (en Anglais, duty-cycled WSNs) et en présence de liens asymétriques. Cette asymétrie des liens est une des manifestation du phénomène de l'irrégularité de la radio. Le protocole de surveillance en question a été justement conçu pour tenir compte de ce phénomène. Il est en effet basé sur des algorithmes, en l'occurrence l'algorithme de détection des nœuds de bordure du RCSF et celui du routage géographique des alertes vers le sink, qui s'appuient sur un graphe de connectivité réseau modélisé en tant que N-UDG.

Nous commençons le chapitre par une revue de littératures à travers laquelle nous exa-

minons les mécanismes d'économie d'énergie ainsi que les protocoles de routage employés par les systèmes de surveillance des zones clôturées et des frontières internationales. Nous décrivons ensuite le modèle de surveillance à base des RCSFs avec cycle d'activité et les hypothèses utilisées pour mener cette étude, le protocole de routage fiable des alertes vers le sink, appelé GPSR [13] over Symmetrical Links (GPSR-SL), et le protocole de surveillance basé sur GPSR-SL. Enfin, nous discutons les résultats de simulation obtenus. Nous tenons à souligner que ces résultats montrent que le protocole de surveillance proposé, basé sur GPSR-SL, atteint un ratio de livraison de paquets (en Anglais, Packet Delivery Ratio (PDR)) plus élevé d'environ 3.63%, une efficacité énergétique et une latence satisfaisante par rapport au même protocole de surveillance basé sur le GPSR original.

Première partie

Etat de l'art

Chapitre 1

Les Réseaux de Capteurs Sans Fil

1.1 Introduction

Les progrès dans la mise en réseau et l'intégration ont permis l'émergence de petits nœuds, dit aussi *motes*, miniaturisés et peu coûteux, capables d'interagir avec leur environnement à travers des capteurs et des actionneurs, et de communiquer entre eux via des liaisons sans fil. Ces *motes* peuvent fonctionner de manière autonomes pour collecter, traiter et communiquer les informations sur leur environnement.

Un RCSF est un réseau auto-organisé qui comprend un grand nombre de nœuds allant de quelques dizaines à plusieurs centaines ou même des milliers de *motes*, déployés dans une zone d'intérêt (environnement intérieur ou extérieur). La mise en réseau des nœuds capteurs permet de mettre en œuvre de nombreuses applications, dans le domaine civile et militaire (par ex., l'armée, l'environnement, la santé, la maison, l'agriculture).

Les contraintes de miniaturisation et de faible coût de fabrication font que les nœuds capteurs sont dotés de ressources très limitées en termes de capacité de calcul, espace de stockage, débit de transmission et d'énergie embarquée. Ces limitations motivent une grande partie des problématiques de recherche dans le domaine des RCSFs, à savoir l'énergie, la couverture, la connectivité, le routage, la tolérance aux pannes et la sécurité. L'aspect économie d'énergie est l'une des préoccupation majeure de cette thèse.

Une autre contrainte à laquelle font face les RCSFs, est celle de l'irrégularité des portées de transmission radio qui est due à plusieurs facteurs (p. ex., le type d'antenne, les obstacles, les conditions météo) [30, 31]. Ce phénomène est à l'origine de la non fiabilité des liens radio dans les RCSFs. Plusieurs études récentes ont démontré qu'il a un impact négatif sur les protocoles de routage, notamment géographiques [39, 41–47, 57]. L'aspect fiabilité des liens entre les nœuds capteurs, lors du routage des paquets d'alerte dans une application de surveillance de zones sensibles clôturées, constitue la deuxième préoccupation de cette thèse.

l'architecture en couches du modèle OSI, largement utilisée dans les réseaux de communication filaires, pourrait ne pas convenir aux réseaux sans fil tels que les réseaux cellulaires, les réseaux mobiles Ad hoc (MANET) et les RCSFs. En effet, les réseaux sans fil ont des particularités qui les distinguent des réseaux filaires conventionnels [48] (nature de diffusion du canal

sans fil ainsi que sa nature variante à travers le temps et l'espace), et qui doivent être prises en compte lors de la conception de protocoles au niveau des différentes couches de la pile protocolaire. De surcroît, les RCSFs ont également des caractéristiques différentes des réseaux sans fil traditionnels. En effet, les nœuds capteurs sont dotés de ressources limitées, notamment en termes d'énergie. Par conséquent, une approche émergente, dite Conception Inter-Couches (en Anglais, Cross-Layer Design) (CIC/CLD) [48–53], qui remet en question la philosophie de conception du modèle mono-couches, s'est imposée dans les réseaux sans fil et notamment dans les RCSFs. Cette nouvelle technique d'optimisation des performances par interaction ou fusion des couches, vise à améliorer les performances globales du réseau sans fil, telles que l'augmentation de la capacité du réseau, l'efficacité énergétique et la qualité de service (QoS). Les deux protocoles proposés dans le cadre de cette thèse, sont basés sur une approche inter-couches par interaction de couches.

Ce chapitre est consacré à la présentation d'un état de l'art sur les RCSFs. Nous définissons tout d'abord ce nouveau concept des RCSFs, puis nous énumérons les caractéristiques intrinsèques de ce type de réseaux émergents, les défis auxquels ils font face, leurs types, leurs domaines d'application, leurs systèmes d'exploitation et les outils pour les évaluer. Ensuite, nous décrivons les aspects des couches de la pile protocolaire des RCSFs en insistant sur la nécessité de la conception de nouveaux protocoles, à tous les niveaux de cette pile protocolaire, qui tiennent compte des caractéristiques intrinsèques de ce type de réseaux. La conception inter-couches est décrite comme étant une solution prometteuse pour les RCSFs, dans la mesure elle vise à améliorer les performances globales du réseau sans fil, telles que l'augmentation de la capacité du réseau, l'efficacité énergétique et la qualité de service (QoS). A la fin du chapitre, nous abordons l'interconnection des RCSFs avec les réseaux externes, notamment l'internet, et l'environnement de déploiement des RCSFs. En ce qui concerne ce dernier point, nous décrivons trois modèles de propagation de signaux radio, tout en mettant l'accent sur l'importance de considérer un modèle de propagation radio réaliste lors de l'étude des RCSFs.

1.2 Définition d'un nœud capteur

Typiquement, un nœud capteur est un dispositif de taille réduite équipé principalement d'une unité de capture, une unité de traitement, une unité de communication et une unité d'alimentation en énergie, comme l'illustre la Figure 1.1. Pour minimiser la consommation d'énergie, la plupart des composants d'un nœud capteur, y compris l'émetteur-récepteur sans fil (unité de communication), seront probablement mis en état de veille la plupart du temps. Pour l'émetteur-récepteur sans fil, une autre solution est utilisée pour minimiser la consommation d'énergie, à savoir le contrôle de la puissance d'émission.

— *L'unité de capture :* est généralement composée de deux sous-unités, à savoir des capteur(s) et des Convertisseurs Analogique-Numérique (CANs), en Anglais, Analog-to-Digital Converters (ADCs).

  — *Le capteur :* convertit l'énergie dans le monde physique en énergie électrique qui peut être transmise à un système informatique. Il constitue l'interface entre le monde physique et le monde virtuel (numérique). Il existe une grande variété de capteurs qui

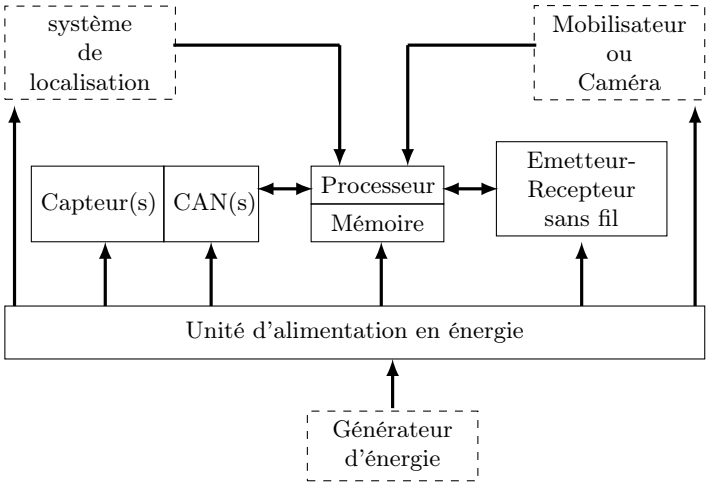


FIGURE 1.1 – Composants de base d'un nœud capteur.

FIGURE 1.2 – Nœud capteur MicaZ [1].

peuvent être attachés à un noeud capteur. Nous citerons entre autres, les capteurs de température, humidité, accélération, lumière, pression, gaz, détection de mouvement, acoustique et d'images. Les capteurs sont généralement classés en trois catégories [58] : capteurs passifs et omnidirectionnels (p. ex., capteurs de lumière, température, humidité, vibrations etc.), capteurs passifs directionnels (p. ex., capteurs vidéo [59]) et capteurs actifs (p. ex., sonar, radar, certains types de capteurs sismiques).

- *Le convertisseur analogique-numérique :* transforme les signaux analogiques, produits par les capteurs en fonction du phénomène observé, en signaux numériques, puis les transmis à l'unité de traitement.

— *L'unité de traitement :* est un micro-contrôleur (en anglais, Micro-Controller Unit (MCU)) qui intègre un processeur, une mémoire volatile (RAM) pour le stockage de données, une ROM, EPROM, EEPROM ou une mémoire FLASH pour le stockage du code (programme relativement simple), des compteurs (en Anglais, timers), des ports d'E/S configurables,

un CAN et d'autres périphériques. Elle permet le traitement des données et la gestion de la fonctionnalité d'un nœud capteur.
En raison du budget d'énergie limité dont dispose un nœud capteur, les micro-contrôleurs utilisés dans ce genre de dispositif ont tendance, en général, à être optimisés pour la consommation d'énergie et non pour les performances [60]. Dans de nombreuses conceptions de nœuds capteurs, on a des processeurs de 8 et 16 bits avec une faible vitesse d'horloge et quelques KOctets de RAM et quelques dizaines de KOctets de RAM FLASH pour le stockage de données et du code. Le Tableau 1.1 indique les caractéristiques de quelques MCUs de différents fabricants qui pourraient être utilisés dans les nœuds capteurs.

Fabricant	Modèle	FLASH (KB)	SRAM (KB)	EEPROM (KB)	SLEEP (mA)	1 MIPS[a] (mA)
Atmel	AT89C51RE2 (8051)	128	8	0	75	7.4
Atmel	ATmega1281 (AVR)	128	8	4	5	0.5
Atmel	AT91SAM7X (ARM)	128	32	0	26	1.1
Freescale	M68HC08	61	2	0	22	3.75
Microchip	PIC18LF8722	128	3.9	1	2.32	1.0
Microchip	PIC24FJ128	128	8	0	21	1.6
Semtech	XE8802 (CoolRisc)	22	1	0	1.9	0.3
TI	MSP430F1611	48	10	0	1.3	0.33

[a] À une tension d'alimentation de 3.0 V.

Tableau 1.1 – Caractéristiques de MCUs [10].

Cette contrainte énergétique impose qu'un MCU ne peut pas collecter continuellement des valeurs de capteurs. En pratique, les capteurs sont activés à des intervalles de plusieurs secondes, voire des minutes, ce qui serait suffisant pour les grandeurs qui changent lentement, telle que la température et l'humidité. Cependant la détection d'événements temporaires et en évolution rapide, tels que l'accélération, le mouvement et l'impulsion acoustique, devient très difficile. Le problème est résolu dans les capteurs numériques avancés par un état de surveillance à faible puissance où le capteur peut réveiller le MCU lorsqu'un événement prédéterminé se produit.

— *L'unité de communication :* Permet la communication sans fil.

— *L'unité d'alimentation en énergie :* La batterie est la principale source d'alimentation dans un nœud capteur. Une alimentation secondaire qui récupère l'énergie de l'environnement [61], comme p. ex., les panneaux solaires, peut être ajoutée au nœud et ce en fonction de la pertinence de l'environnement de déploiement.

Un nœud capteur peut également être dôté de composants supplémentaires dépendants de l'application tels qu'un système de localisation (utile dans le cas d'un routage géographique, p. ex.), un générateur d'énergie, un mobilisateur (pour déplacer le nœud capteur en vu de réaliser une tâche déterminée), ou une unité de capture vidéo telle qu'une caméra.

Fabricant	Modèle	Débit (Kbps)	Fréquence (MHz)	Tampon (Octets)	Veille (mA)	Inactif (mA)	RX (mA)	Sensibilité (dBm)	TX à 0 dBm (mA)
Microchip	MRF24J40	250	2400	128	2	-	18	-91	22
Nordic	nRF2401A	1000	2400	32	0.9	0.01	19	-85	13
Nordic	nRF24L01	2000	2400	32	0.9	0.03	12.3	-82	11.3
TI	CC2400	1000	2400	32	1.5	1.2	24	-87	19
TI	CC2420	250	2400	128	0.02	0.4	18.8	-95	17.4
TI	CC2500	500	2400	64	0.4	1.5	17	-82	21.2
Semtech	XE1201A	64	433	-	0.2	0.06	6.0	-102	11.0
Semtech	XE1203F	152.3	433/868/915	-	0.2	0.85	14.0	-101	33.0
TI	CC1000	76.8	433/868/915	-	0.2	0.1	9.3	-101	10.4
TI	CC1020	153.6	433/868/915	-	0.2	0.08	19.9	-81	16.2
TI	CC1100	500	433/868/915	64	0.4	1.6	16.5	-88	15.5
Nordic	nRF905	50	433/868/915	32	2.5	0.03	14.0	-100	12.5
RFM	TR1001	115.2	868	-	0.7	-	3.8	-91	12
RFM	TR3100	576	433	-	0.7	-	7.0	-85	10

Tableau 1.2 – Caractéristiques d'un émetteur-récepteur radio

1.3 Définition d'un RCSF

Le concept des RCSFs [17] [62] [63] [60] [64] [18] [65] [11] est le résultat de la convergence de la technologie des Systèmes Micro-Electro-Mécaniques (SMEM), des communications sans fil et de l'électronique numérique. Les RCSFs forment un nouveau type de réseau sans fil avec un nouvel ensemble de caractéristiques et de défis. Un RCSF est constitué de plusieurs nœuds capteurs appelés couramment capteurs, allant de quelques dizaines à plusieurs centaines ou même des milliers, où chaque nœud est connecté à un ou plusieurs autres nœuds via des liaisons sans fil de type Radio-Fréquences (RF), acoustique, optique ou InfraRouge (IR). Ce type de réseaux partage certaines caractéristiques importantes avec les réseaux Ad hoc [60].
Les nœuds capteurs sont dotés de ressources limitées en termes d'énergie, de portée de capture et de communication, de bande passante, de vitesse de traitement et de capacité de stockage. Ils sont déployés, d'une manière aléatoire ou déterministe, dans une zone d'intérêt pour collecter des informations du monde physique, éventuellement les traiter (traitement dans le réseau ou in-network processing [1]) et les transmettre, en utilisant un mode de communication multi-sauts, à un ou plusieurs nœuds collecteurs appelés puits (en anglais sinks). Les nœuds puits sont souvent plus puissants que les nœuds capteurs ordinaires. Ils pourraient être des PDA, des ordinateurs portables ou des ordinateurs de bureau. Ils peuvent être stationnaires ou mobiles [67]. Un nœud puits peut soit utiliser localement les données provenant des nœuds capteurs, soit les relayer à un centre de décision distant, via une liaison haut débit (internet ou satellite), tel qu'illustré par la Figure 1.3.

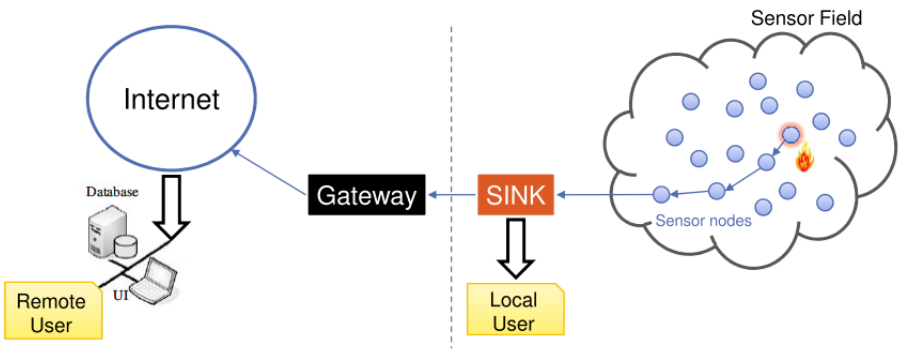


FIGURE 1.3 – Architecture typique d'un RSCF [2].

Les nœuds capteurs constituant un RCSF peuvent être homogènes ou hétérogènes (différents types de capteurs embarqués, différents rayons de capture, différents rayons de communication, différentes puissances de batteries ou différentes vitesses de calcul et capacités de stockage [68]). Ils peuvent être stationnaires ou mobiles. Ils peuvent être au courant de leurs positions à travers le système de positionnement global (GPS) ou une approche de localisation [69–72], ou non.

1. Le traitement dans le réseau consiste à effectuer l'agrégation des données (p. ex., calculer la moyenne de certaines valeurs) aux niveau des nœuds intermédiaires entre les sources et le sink. Ainsi, la quantité de données est réduite en traversant le réseau vers le sink [66].

1.4 Caractéristiques des RCSFs

Les RCSFs partagent certaines caractéristiques importantes avec les réseaux Ad hoc qui constituent leur classe mère, tel que le besoin de l'auto-organisation, la communication multi-sauts et la dynamicité temporelle de la topologie, de la connectivité et d'autres paramètres du réseau. Cependant, il existe des différences importantes entre ces deux types de réseaux, par exemple [18, 60, 73] :

— La tâche principale d'un nœud capteur n'est pas de servir un utilisateur humain comme c'est le cas dans les réseaux Ad hoc, mais de collaborer avec d'autres nœuds pour la collecte des données de l'environnement physique afin de satisfaire les besoins d'une application spécifique.

— Les nœuds dans les RCSFs sont peu mobiles (nœuds généralement stationnaires qui restent à leur place dans l'espace de déploiement). Les changements de topologie dans les RCSFs sont donc généralement causés par des nœuds qui ont basculé en mode veille pour économiser l'énergie ou qui ont cessé de fonctionner en raison d'une batterie déchargée, d'une défaillance du système ou d'un acte d'endommagement volontaire ou involontaire. Les nœuds dans les réseaux Ad hoc sont caractérisés par une forte mobilité. Ils se déplacent généralement en même temps que leurs utilisateurs. Nous citerons par exemple, les applications Ad hoc telles que les opérations commando militaires et les équipes de recherche dans des zones sinistrées. La conséquence directe de cette mobilité est la modification physique de la topologie du réseau.

— Etant donné que les données collectées par les capteurs sont basées sur des phénomènes communs, il est probable qu'il y ait une certaine redondance dans les données communiquées par les diverses sources à un puits particulier. Pour cette raison, l'agrégation de données a été présentée comme un paradigme essentiel pour le routage dans les RCSFs [74]. L'idée est de combiner en route les données provenant de différentes sources. Ce mode de routage est dit routage centré sur les données (en Anglais, data-centric routing). En effet, les nœuds relais examinent le contenu des données et effectuent une certaine forme de fonction d'agrégation/consolidation sur les données provenant de plusieurs sources. Ceci permet de minimiser le nombre de transmissions et par conséquent économiser de l'énergie qui constitue une contrainte majeure dans les RCSFs. Les réseaux Ad hoc, par contre, utilisent un routage de bout en bout basé sur l'adresse. Ce mode de routage dit routage centré sur l'adresse (en Anglais, address-centric routing) consiste à trouver des chemins courts entre des paires de nœuds (d'extrémité) adressables.

— Les RCSFs peuvent comporter des milliers à des dizaines de milliers de nœuds. Les réseaux Ad hoc sont par contre déployés en un nombre relativement faible, de l'ordre de dizaines à des centaines de nœuds.

— Bien que la consommation d'énergie constitue la principale préoccupation pour les deux types de réseaux, la durée de vie des applications basées sur les réseaux Ad hoc semble être beaucoup plus courte que celle des applications basées sur les RCSFs. Par exemple, un réseau Ad hoc, mis en place pour la communication d'urgence dans une zone sinistrée, peut

être opérationnel pendant plusieurs heures à plusieurs jours, tandis qu'un RCSF dédié à la surveillance environnementale peut durer plusieurs années. D'autre part, le réapprovisionnement en énergie des nœuds constituants les réseaux Ad hoc est plus facile que celui des nœuds des RCSFs, à cause de la proximité du premier type de nœuds avec les utilisateurs comme on l'a souligné plus haut.

— Le mode typique de communication dans les RCSFs est une sorte de reverse-multicast (plusieurs à un). En effet dans ce type de réseaux, il y a souvent un ou plusieurs nœuds récepteurs, dits collecteurs ou puits (en Anglais, sink), à qui (auxquels) le reste des nœuds du réseau, appelés nœuds sources, envoient leurs données. Dans les RCSFs, En plus de leur rôle de collecte de données, les nœuds puits peuvent configurer et contrôler le fonctionnement des nœuds sources, par l'envoi de messages de contrôle, en mode unicast (un à un), multicast (un à plusieurs) ou broadcast (diffusion). Dans les réseaux Ad hoc, il n'y a pas de nœuds distincts. La communication se fait entre n'importe quelle paire de nœuds.

1.5 Défis dans les RCSFs et mécanismes pour les résoudre

Le Tableau 1.2 recense les défis importants dans les RCSFs ainsi que les mécanismes requis correspondants pour les résoudre.

Défis	Mécanismes requis correspondants)
Les contraintes de ressources	Utilisation efficace des ressources **(Dans notre cas, on a utilisé le duty-cycling de la radio et la réduction des retransmissions à travers un routage géographique via des liens fiables, afin de rationaliser) la consommation de l'énergie**
Conditions d'environnement dynamique et extrêmes	Fonctionnement adaptatif du réseau
Redondance des données	Fusion de données et traitement localisé
La non fiabilité des liaisons sans fil	Fiabilité **(Dans notre cas, on a utilisé un routage géographique basé sur deux métriques : le nombre de sauts et la qualité des liens**)
Identification non globale (ID) pour les nœuds capteurs	Paradigme de communication centré sur les données
Défaillance des nœuds capteurs	Tolérance aux pannes
Déploiement à grande échelle	Capteurs de petite taille peu coûteux capables de s'auto-configurer et s'auto-organiser

Tableau 1.3 – Les RCSFs : Défis et solutions [11].

Comme il est mentionné dans le Tableau 1.3, les travaux de cette thèse se focalisent sur deux défis majeurs, à savoir la consommation d'énergie et la non fiabilité des liaisons dans un RCSF.

Le problème de l'efficacité énergétique peut être résolu de différentes manières [66]. Une approche consiste en l'optimisation de la conception du matériel et du logiciel embarqué, incluant les protocoles au niveau des différentes couches de la pile protocolaire (p. ex., dans notre cas nous avons agi au niveau de la couche MAC et la couche réseaux (NET)).
Pour rationaliser davantage la consommation de l'énergie, la conception inter-couches [48–53], dont il est question dans la Section 1.11, a émergé comme étant une technique très prometteuse. Elle fait référence à la conception de protocoles en exploitant la dépendance entre les couches de protocoles afin d'obtenir des gains de performance dans le réseau, tout en minimisant la dépense énergétique.

En ce qui concerne la problématique de la non fiabilité des liaisons sans fil, nous avons fait appel à cette même technique émergente (la conception inter-couches) pour prendre en compte l'état du canal (paramètre fourni par la couche physique (PHY)) au niveau de la couche réseau (NET), lors du routage des paquets de données vers le nœud puits.

1.6 Types de RCSFs

Les RCSFs actuels sont déployés sur terre, sous terre et sous l'eau. Ils doivent faire face à différents challenges et contraintes dépendant de leur environnement de déploiement. Il existe cinq types de RCSFs [11, 18], à savoir les RCSFs terrestres, RCSFs souterrains, RCSFs sous-marins, RCSFs multimédia et les RCSFs mobiles.

1.6.1 RCSFs terrestres

Les RCSFs terrestres [17] sont généralement constitués de centaines à des milliers de nœuds capteurs sans fil peu coûteux déployés, de manière aléatoire ou déterministe, dans une zone d'intérêt sur terre. Un RCSF terrestre doit faire face à plusieurs défis qui sont tous liés à la principale préoccupation d'un RCSF, à savoir l'énergie. Parmi ces défis, nous citerons la fiabilité de la communication dans un environnement dense, l'élimination de la redondance des données collectées, la maintenance de la connectivité du réseau et la minimisation du délai de bout en bout dans le réseau. La surveillance de l'environnement, la surveillance industrielle et la surveillance de zones sensibles à des fins sécuritaires, sont des exemples d'applications à base des RCSFs terrestres.

1.6.2 RCSFs souterrains

Les RCSFs souterrains se composent de nœuds capteurs sans fil déployés dans des grottes, des mines ou sous terre pour surveiller les conditions souterraines [75]. Des nœuds puits supplémentaires sont situés au dessus du sol pour relayer les informations des nœuds capteurs souterrains vers le(s) nœud(s) collecteur(s) final(aux). Un RCSF souterrain est plus cher qu'un RCSF terrestre en termes d'équipement, de déploiement et de maintenance. La communication sans fil constitue un défi majeur dans un environnement souterrain en raison de l'atténuation élevée et de la perte de signal. La conservation est aussi un objectif clé pour les RCSFs souterrains, d'autant plus qu'il est difficile de recharger ou de remplacer la batterie de nœuds de capteur

enfouis sous terre. Les RCSFs souterrains sont utilisés dans de nombreuses applications telles que la surveillance de l'agriculture, la surveillance souterraine du sol, de l'eau ou des minéraux et la surveillance des frontières entre les pays.

1.6.3 RCSFs sous-marins

Les RCSFs sous-marins [76, 77] sont constitués d'un certain nombre de nœuds capteurs sans fil et de véhicules déployés sous l'eau, par exemple dans l'environnement océanique. La cherté de ces nœuds fait que seuls quelques nœuds sont déployés et des véhicules sous-marins autonomes sont utilisés pour explorer ou collecter des données à partir de ceux-ci. La communication sans fil sous-marine utilise des ondes acoustiques qui présentent divers défis tels que la bande passante limitée, le long délai de propagation et le problème d'atténuation du signal. Comme pour les RCSFs terrestres et souterrains, le problème de la conservation d'énergie reste entièrement posé pour les RCSFs sous-marins. Parmi les applications des RCSFs sous-marins, nous citerons entre autres, la prévention des catastrophes naturelles (p. ex., séisme, tsunami), la surveillance de la pollution et la surveillance et l'exploration sous-marines.

1.6.4 RCSFs multimédia

Les RCSFs multimédia [78] sont constitués d'un ensemble de nœuds capteurs sans fil à faible coût équipés de caméras et de microphones, déployés de manière déterministe ou aléatoire. Les capteurs multimédia sont capables de stocker, traiter et récupérer des données de type vidéo, audio et image fixe. Les RCSFs multimédia doivent faire face à plusieurs défis tels que la forte demande de bande passante, la consommation d'énergie élevée, la garantie de la Qualité de Service (QdS) , traitement en réseau, filtrage et compression de contenu multimédia, et la conception inter-couches (en Anglais, cross-layer design). Des techniques de transmission à base d'un compromis entre l'utilisation d'une bande passante élevée et une faible consommation d'énergie doivent être développées, pour permettre la livraison d'un contenu multimédia tel qu'un flux vidéo. D'autre part, un certain niveau de QdS doit être assuré pour une livraison fiable du contenu. L'utilisation du traitement en réseau, filtrage, compression de contenu multimédia et l'approche inter-couches peuvent améliorer considérablement les performances du réseau en termes de traitement et de livraison du contenu multimédia. Les RCSFs multimédia améliorent sensiblement les applications de RCSFs existantes tels que le suivi et la surveillance.

1.6.5 RCSFs mobiles

Les RCSFs mobiles [18] consistent en une collection de nœuds capteurs sans fil mobiles qui peuvent se déplacer et interagir avec l'environnement physique. En plus de leur capacité de capture, calcul et communication, les nœuds mobiles peuvent se repositionner et s'organiser dans le réseau. Par conséquent, un routage dynamique doit être utilisé dans les RCSFs mobiles, au lieu du routage statique employé dans les RCSFs stationnaires. Les RCSFs mobiles sont confrontés à plusieurs défis tels que le déploiement, la gestion de la mobilité, la localisation avec mobilité, la navigation et le contrôle des nœuds mobiles, le maintien de la couverture et de la connectivité et

la minimisation de la consommation d'énergie en locomotion. Les applications des RCSFs mobiles incluent la surveillance de l'environnement, le suivi des cibles, la recherche et le sauvetage et la surveillance des frontières.

1.7 Domaines d'application des RCSFs

Le déploiement d'un grand nombre de nœuds capteurs sans fil de taille réduite, de faible coût de production, capables de s'auto-configurer, s'auto-organiser, capturer des grandeurs physiques (pression, température, humidité, gaz, mouvement, etc.) de leur environnement, éventuellement les traiter et les transmettre à un centre de décision distant, a permis l'émergence de nombreux domaines d'applications à base des RCSFs [11, 17, 18]. Parmi ces domaines, on citera le domaine militaire, de l'environnement, de la santé (les réseaux corporels, en Anglais, Body Area Networks -BAN-), de l'industrie et agriculture, et de l'urbanisation et infrastructure.

Les applications basées sur les RCSFs peuvent être classées en deux catégories : surveillance et suivi (en Anglais, monitoring and tracking). Par exemple, les capteurs peuvent être déployés dans une zone hostile dans le cadre d'une application de surveillance, dans une forêt pour la détection d'incendie, fixés aux taxis ou bus d'une grande ville pour étudier les conditions de circulation et planifier efficacement les itinéraires ou pour estimer le niveau de pollution par endroit dans la ville, ou fixés sur la chaussée pour l'aide au stationnement des véhicules en milieu urbain (parkings intelligents [79, 80]). Il est aussi envisagé qu'à l'avenir les capteurs intégreront tous les objets du quotidien pour les rendre intelligents [11]. Ces objets intelligents peuvent explorer leur environnement, communiquer avec d'autres objets intelligents et interagir avec les humains. C'est l'ère de l'Internet of Things (IoT) et l'Internet of Every things (IoE).

1.8 Systèmes d'exploitation pour les RCSFs

Plusieurs systèmes d'exploitation (OS) ont été développés pour les RCSFs [81–83]. Ces OS sont basés sur un modèle d'exécution piloté par les évènements, un modèle d'exécution piloté par les threads ou un modèle hybride. En général, les principales exigences pour un système d'exploitation pour les RCSFs sont [84, 85] :

— *Utilisation efficaces des ressources limitées* : Etant donné que les nœuds capteurs sont dotés de ressources très limitées, le système d'exploitation devrait les utiliser efficacement.

— *Concurrence* : Le système d'exploitation devrait être capable de gérer différentes tâches en même temps.

— *Flexibilité* : D'une part, la diversité du matériel ainsi que le rythme d'innovation dans celui-ci et d'autre part, l'énorme variation des exigences des différentes applications, exigent un système d'exploitation flexible.

— *Faible consommation d'énergie* : La conservation de l'énergie devrait être l'un des principaux objectifs du système d'exploitation.

Parmi ces OS, on citera TinyOS, SOS, MANTIS et Contiki.

— *TinyOS* [84] Ce système d'exploitation open source, développé à l'Université de Californie, Berkeley (UCB), Etats Unis d'Amérique, est de loin la plate-forme la plus utilisée dans les RCSFs. Il intègre une architecture basée sur les composants, qui minimise la taille du code et fournit une plate-forme flexible pour la mise en œuvre de nouveaux protocoles de communication. Il est dôté d'une bibliothèque de composants comprenant des protocoles réseau, des services distribués, des pilotes de capteurs et des outils d'acquisition de données, qui peuvent être adaptés aux exigences spécifiques de chaque application. TinyOS est basé sur un modèle d'exécution piloté par les événements qui permet des stratégies de gestion de l'énergie. Initialement écrit en langage C standard, le projet a depuis évolué vers un langage personnalisé, NesC [86] qui est une extension du langage C. Notons enfin que pour simplifier le développement de protocoles et d'applications pour les RCSFs, TinyOS fournit un support de simulation, à savoir le simulateur TOSSIM [87]. Le code de simulation est écrit en NesC et par conséquent peut être déployé sur des nœuds réels.
TinyOS peut fonctionner sur un large éventail de plates-formes matérielles, entre autres Imote2, Micaz, Mica2, TMote Sky (Telos Rev B), TinyNode, Zolertia Z1. Les micro-contrôleurs pris en charge incluent les séries Atmel AT90L, Atmel ATmega, Texas Instruments MSP et Intel XScale PXA271 [82].

— *SOS* [88] : Est un autre système d'exploitation basé sur les évènements, développé en langage C par l'Université de Californie, Los Angeles (UCLA), Etat Unis d'Amérique. SOS adopte le modèle de composants de TinyOS. Cependant, contrairement à TinyOS où les composants et leur communication sont définis statiquement au moment de la compilation, dans SOS les composants ou modules sont reconfigurables dynamiquement. Pour permettre une telle reconfiguration, SOS est constitué d'un noyau compilé statiquement et d'un ensemble de modules chargés dynamiquement. Il prend en charge les motes Mica2 et MicaZ, et le nœud XYZ de Yale [89].

— *MANTIS* [90] : MultimodAl system for NeTworks of In-situ wireless Sensors (MANTIS) est le premier système d'exploitation piloté par les threads ciblant le domaine des RCSFs. MANTIS est un OS léger et économe en énergie. Il a une empreinte (en Anglais, footprint. It is the amount of RAM, OS took to run) de 500 octets, qui inclut le noyau, le planificateur (en Anglais, scheduler) et la pile réseau. MOS est écrit en C et supporte le développement d'applications en C. MANTIS prend en charge la simulation des RCSFs via AVRORA [91]. Les plates-formes matérielles supportées par MANTIS sont Mica2, MicaZ et Telos.

— *Contiki* : Développé par l'Institut Suédois de l'Informatique, Contiki est un système d'exploitation pour les RCSFs, open source, léger et écrit en C. Il s'agit d'un système d'exploitation hybride. Par défaut, son noyau fonctionne comme un noyau piloté par les événements. Contiki implémente un support pour le multithreading préemptif à travers une bibliothèque au dessus du noyau. Il a été développé pour une utilisation sur une variété de plates-formes, y compris les micro-contrôleurs tels que le TI MSP430 et l'Atmel AVR, qui sont utilisés dans les familles Telos, Tmote et Mica. Contiki inclut en effet une très petite implémentation d'IP appelée uIP [92], ainsi qu'une implémentation d'IPv6 avec le support de 6LoWPAN [93] appelé uIPv6 . Contiki a récemment gagné en popularité grâce

justement à la pile TCP/IP intégrée et le support du multithreading préemptif. Il est en effet considéré comme un sérieux candidat pour l'IoT. Cooja [94, 95] est le simulateur de réseaux Contiki.

1.9 Les outils d'évaluation de performance pour les RCSFs

Les techniques les plus couramment utilisées pour l'analyse des performances des RCSFs sont [3, 96–99] : la modélisation analytique, la simulation, l'émulation, les bancs d'essai (en Anglais, testbeds) et les déploiements réels, tel qu'illustré dans la Figure 1.4.

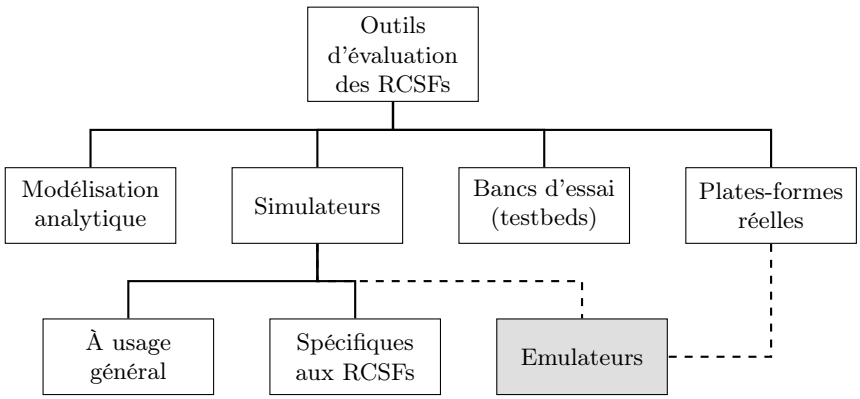


FIGURE 1.4 – Outils d'évaluation de performance pour les RCSFs [3].

Toutefois, il convient de noter que les simulateurs, les émulateurs et les bancs d'essai physiques sont des alternatives très utiles, par rapport au déploiement réel et à la modélisation analytique, pour l'évaluation des algorithmes et des protocoles dans un environnement contrôlé. En effet, le déploiement réel engendre un coût non négligeable en termes d'argent, de temps, d'efforts, et peut être rendu pratiquement irréalisable à cause de l'hostilité de l'environnement de déploiement. Quant à la modélisation analytique, elle peut aboutir à des modèles trop simplifiés conduisant à des résultats imprécis.

1.9.1 Modélisation analytique

les méthodes analytiques nécessitent certaines simplifications pour modéliser et prédire les performances des réseaux, ce qui les rend inappropriées pour les RCSFs, en raison des caractéristiques de ces derniers, par exemple, densité de nœuds, dynamicité de la topologie et les caractéristiques du support sans fil.

1.9.2 Déploiements réels

L'évaluation des performances par le biais d'un déploiement réel est pratiquement impossible ou peu pratique en raison du coût, du temps, des efforts et de l'environnement de déploiement qui est parfois hostile à la présence humaine.

1.9.3 Simulateurs pour les RCSFs

Etant donné que le déploiement réel et la création de bancs d'essai réels sont coûteux en termes de coût et de temps, et dans certains cas, impossibles (p. ex., à cause du facteur d'échelle, inaccessibilité du terrain), des simulations réseau fiables sont réalisées à l'aide de simulateurs, pour tester les fonctionnalités et les performances des protocoles RCSFs dans des conditions d'environnement changeantes et des exigences réseau spécifiques. Les simulateurs permettent en effet une réduction significative des coûts et la simulation de différents types de scénarios dans des intervalles de temps tolérables. Par conséquent la simulation est l'approche la plus utilisée pour concevoir, développer et tester les protocoles pour les RCSFs.

Les simulateurs utilisés dans le domaine des RCSFs peuvent être classés en deux catégories, à savoir les simulateurs à usage général et les simulateurs spécifiques aux RCSFs [3]. Parmi les simulateurs à usage général les plus importants, et qui sont utilisés pour les RCSFs, on citera : NS-2 [100], NS-3 [101], OMNeT++ [102], J-Sim [103], MATLAB [104] et Ptolemy II [105]. Quant aux simulateurs spécifiques aux RCSFs, on citera : SensorSim [106], Castalia [107], VisualSense [108], Mobility Framework [109], MiXiM [110], CupCarbon [111] et Prowler [112]/JProwler [113]. Il convient de noter que la plupart du temps, ces simulateurs spécifiques aux RCSFs sont basés sur les simulateurs à usage général (p. ex., SensorSim est basé sur NS-2, Castalia et MiXiM sont basés sur OMNeT++, VisualSense est basé sur Ptolemy et Prowler est basé sur MATLAB). En effet, des fonctionnalités et des bibliothèques supplémentaires sont développées et intégrées aux simulateurs à usage général, pour l'évaluation des performances des RCSFs.

Notons enfin que la plupart des simulateurs pour les RCSFs incorporent généralement les composants suivants [7] :

— modèles décrivant les caractéristiques des nœuds capteurs

— différents modèles de communication

— modèles pour l'environnement physique

— outils de collecte et d'analyse de statistiques et de visualisation des données collectées et du comportement du nœud capteur.

1.9.4 Emulateurs

Les émulateurs sont différents des simulateurs, dans la mesure où ils peuvent exécuter le même code sur les plates-formes réelles [3]. Par conséquent, ils réduisent l'effort d'implémentation et permettent d'obtenir des résultats plus précis que les simulateurs. Cependant, ils ont un inconvénient puisqu'ils simulent du code pour des plates-formes spécifiques. Ainsi, un émulateur aussi populaire que TOSSIM [87], est incapable d'émuler des RCSFs hétérogènes. ATEMU [114], Avrora [115], EmStar [116] et COOJA [94, 95] sont d'autres exemples d'émulateurs.

1.9.5 Bancs d'essai RCSFs (WSN testbeds)

Un banc d'essai RCSF est constitué de nœuds capteurs déployés dans un environnement contrôlé. Il est conçu pour soutenir la recherche expérimentale dans un environnement réel [11,18].

Il fournit en effet un environnement de test et d'évaluation de protocoles similaire au déploiement réel. Il fournit aussi l'opportunité de configurer, d'exécuter et de surveiller des expériences à distance.
Les auteurs de [11] ont classé les bancs d'essai en trois catégories selon leur déploiement :

1. externe (outdoor)
2. interne (indoor)
3. externe et interne (indoor and outdoor).

Parmi les plates-formes de test (bancs d'essai), nous citerons, entre autres, CitySense (outdoor) [117], MoteLab (indoor) [118], Emulab (indoor) [119], ORBIT (indoor) [120,121], SensLAB (indoor) [122] et Sensei-UU (indoor and outdoor) [123].

1.10 Pile protocolaire pour les RCSFs

Comme le montre la Figure 1.5, la pile protocolaire des RCSFs est généralement représentée par cinq couches seulement parmi les sept couches standards définies dans le modèle OSI. Il s'agit en effet des couches physique (PHY), liaison de données (DLL), réseau (NET), transport (TRAN) et application (APP).
Les protocoles de communication traditionnels implémentés au niveau des différentes couches de la pile protocolaire ne conviennent généralement pas aux RCSFs. En effet, ces protocoles n'ont pas été conçus pour tenir compte des contraintes de ressources de ce type de réseaux, à savoir l'énergie, la bande passante, la mémoire et la capacité de calcul. Par conséquent de nouveaux protocoles, à efficacité énergétique surtout, ont été proposés au niveau de chaque couche de la pile protocolaire. Certains de ces protocoles sont basés sur une approche inter-couches (en Anglais, Cross-Layer design) [4, 49, 124], au lieu de l'approche mono-couches traditionnelle. L'approche inter-couches permet une optimisation de métriques à travers l'interaction ou la fusion de couches. Nous rappelons qu'en ce qui nous concerne, les deux protocoles que nous proposons, à savoir le protocole de surveillance et le protocole de routage, sont basés sur une approche inter-couches par interaction de couches (PHY, MAC et NET).

1.10.1 Couche physique

La première couche de la pile de protocoles, la couche physique, est responsable de la définition et de la gestion des connexions entre les dispositifs individuels et leur support de communication. Les fonctions de la couche physique disponibles dans la plupart des émetteurs-récepteurs sont la sélection d'un canal de fréquence et d'une puissance d'émission, la modulation transmise et la démodulation des données reçues, la synchronisation des symboles et la génération d'horloge pour les données reçues.
La couche physique d'un émetteur-récepteur peut aussi inclure des fonctions supplémentaires, qui réduisent les besoins de traitement du MCU. Par exemple, une couche PHY conforme à la norme IEEE 802.15.4 [40](le standard IEEE 802.15.4 ou LR-WPAN pour Low-Rate WPAN, est la norme de communication la plus couramment utilisée pour l'implémentation des RCSFs tel que mentionné dans la Section 1.10) comprend :

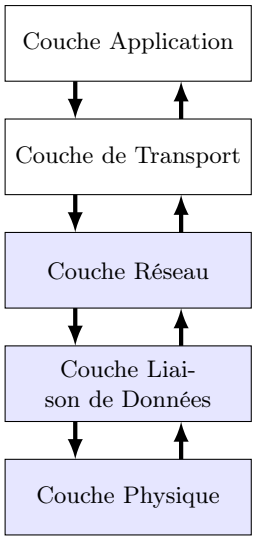


FIGURE 1.5 – Pile protocolaire des RCSFs.

— Une synchronisation de trames de données pour percevoir le début d'une trame entrante
— L'évaluation du canal pour détecter le trafic en cours dans un canal de fréquence (CCA -Clear Channel Assessment-)
— Un indicateur de la force du signal reçu (RSSI)
— Un indicateur de la qualité de liaison (LQI)
— Le calcul du contrôle de redondance cyclique (CRC) pour vérifier les erreurs sur les trames reçues
— cryptage / décryptage de données pour améliorer la sécurité du réseau
— Les accusés de réception automatiques après les trames reçues.

Les RCSFs sont soumis à des contraintes plus strictes que les réseaux sans fil traditionnels, comme nous l'avons décrit précédemment. Rappelons que les nœuds capteurs sont dotés de ressources très limitées en termes d'énergie, de puissance de traitement, de capacité de stockage et de portée de communication. Par conséquent, lors de la conception de la couche physique des RCSFs, ces contraintes doivent être prises en compte (p. ex., le standard 802.15.4 le fait).

1.10.2 Couche liaison de données

La couche de liaison de données s'interface avec les couches physique et réseau. Elle est chargée de fournir des services qui permettent à plusieurs nœuds d'accéder et de partager avec succès un support de communication. Ces services incluent le contrôle d'accès au médium, la livraison fiable, la détection et correction d'erreur. Elle se compose typiquement de deux sous-couches, à savoir la sous-couche de contrôle d'accès au médium (Medium Access Control - MAC) et la sous-couche de contrôle de liaison logique (Logical Link Control - LLC).
La sous-couche MAC est chargée de contrôler les accès concurrents au médium. La Figure 1.6

montre une classification des protocoles MAC existants, selon la méthode d'accès au support [7, 8, 125].

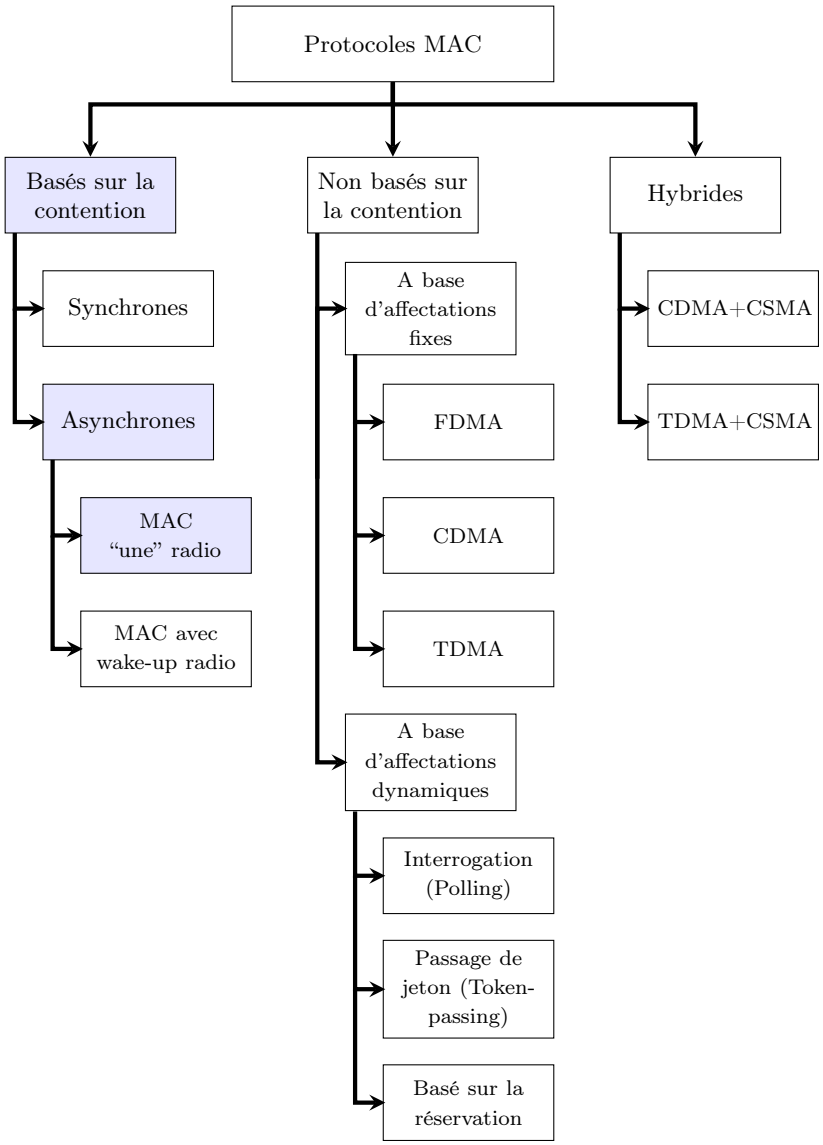


FIGURE 1.6 – Classification des protocoles MAC selon la méthode d'accès au support.

les protocoles *basés sur la contention*, dits *contention-based* ou *random access* protocols permettent aux nœuds d'accéder au média simultanément, mais fournissent des mécanismes pour réduire le nombre de collisions et la reprise en cas d'occurrence de celles-ci. Ce type de protocoles sont basés sur les concept de ALOHA [126, 127], CSMA [128], MACA [129] et MACAW [130]. Cette classe de protocoles peut être divisée en deux sous classes : la sous classe des protocoles synchrones [131,132] et celles des protocoles asynchrones. Les nœuds utilisant un protocole synchrone se réveillent périodiquement en même temps et communiquent entre eux durant des périodes actives communes. Les exigences de la synchronisation entre les nœuds peuvent être à l'origine de

la dégradation des performances du réseau et de l'augmentation de la consommation d'énergie. Pour y remédier, les protocoles asynchrones ont été proposés, et dans lesquels les nœuds se réveillent indépendamment les uns des autres. On distingue deux mécanismes de coordination qui permettent aux nœuds voisins de communiquer sans avoir besoin d'être synchronisés, à savoir :

1. L'envoi d'une série de courts préambules [133,134], d'une durée aussi longue que le période de veille du destinataire, avant de commencer l'envoi des données (cas des protocoles MAC utilisant "une" radio). Un exemple d'illustration est montré dans la Figure 4.3.
2. L'envoi d'un message de réveil [135] pour indiquer le point de départ de la transmission des données (cas des protocoles MAC utilisant une radio de réveil).

Les protocoles MAC non basés sur la contention [7, 8], dits *contention-free protocols* ou *schedule-based* protocols, fournissent une approche de partage de média qui garantit qu'un seul nœud accède au support sans fil à un moment donné. Cette catégorie peut en outre être divisée en deux sous classes, sous classes des assignations fixes et dynamiques. Elles indiquent respectivement si les réservations de slots sont fixes ou à la demande. Dans les protocoles à base des affectations fixes, les assignations de canal sont fixes, indépendamment du besoin des nœuds. Par contre, les protocoles à base des affectations dynamiques planifient l'accès au canal en fonction de la demande des nœuds ayant un trafic de messages à transmettre. Les nœuds n'ayant pas de trafic n'ont pas accès au canal. Il convient de noter que dans ces deux sous classes, l'absence de collision est garanti, ce qui n'est pas le cas dans la classe des protocoles à base de contention et ce à cause du problème du terminal caché (voir Figure 1.7).

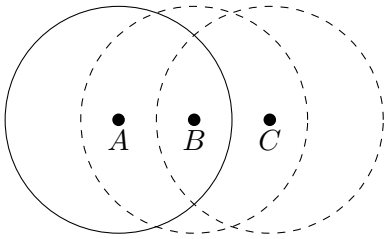


FIGURE 1.7 – Problème du terminal caché : Le noeud C transmet une information au noeud B. Si le noeud A écoute le canal radio, il ne détecte aucune transmission et par conséquent il croit qu'il peut communiquer avec le noeud B. A commence à transmettre à B. Une collision se produit au niveau de B. C est un terminal caché par rapport à A et vice versa.

Les protocoles hybrides, comme leur nom l'indique, combinent les caractéristiques des deux catégories de protocoles précédentes (avec et sans contention) pour atteindre des performances élevées. IEEE 802.15.4 [136,137], ZMAC (Zebra MAC) [138], sont des exemples de protocoles de cette classe.

Avec l'avènement des RCSFs, l'énergie est devenue l'un des principaux défis à relever lors de la conception des protocoles MAC [139,140]. Les sources de consommation d'énergie dans les RCSFs peuvent être attribuées aux trois principales fonctionnalités des nœuds capteurs, en l'occurrence la détection, le traitement et la communication. La capture et le traitement consomment une quantité d'énergie négligeable par rapport à la communication. Un nœud capteur dépense en effet le maximum d'énergie dans la transmission et la réception de données. Un moyen important

de conservation de l'énergie dans les RCSFs est d'éteindre la radio d'un nœud lorsque celui-ci n'a pas de paquets à transmettre ou à recevoir pendant une période spécifique. Le nœud est dit en mode "veille" lorsque sa radio est éteinte et en mode "actif" lorsqu'elle est allumée.

La couche MAC contrôle directement les activités de la radio, et son efficacité énergétique représente donc une métrique de performance très importante qui a un impact direct sur la durée de vie du réseau. Un protocole MAC à efficacité énergétique devrait en effet contrôler la radio pour éliminer ou au moins réduire les sources potentielles de gaspillage d'énergie lors d'une tentative de communication, à savoir :

— *Collisions* : Elles se produisent lorsque deux ou plusieurs nœuds capteurs tentent de transmettre simultanément. La nécessité de retransmettre un paquet qui a été corrompu par une collision augmente la consommation d'énergie.

— *Réceptions indésirables ou sur-écoute (overhearing)* : Est le fait qu'un nœud capteur reçoit des paquets envoyés en mode unicast (un à un) qui ne lui sont pas destinés. Ceci entraîne un gaspillage d'énergie, en particulier lorsque la densité du réseau est élevée et que le trafic de données est important. Notons que la sur-écoute ne constitue pas un problème pour les protocoles MAC basés sur TDMA, mais doit être considérée pour les protocoles MAC basés sur CSMA.

— *Paquets de contrôle (control packet ou overhead)* : Les paquets de contrôle sont nécessaires pour réguler l'accès au canal de transmission. Cependant un nombre élevé de paquets de contrôle transmis par rapport au nombre de paquets de données délivrés, indique une faible efficacité énergétique du protocole MAC.

— *Ecoute de la porteuse à vide (idle listening)* : Un nœud capteur est dit dans cet état, qui est aussi appelé *écoute inactive*, lorsqu'il écoute le support de communication pour les transmissions en cours, mais il n'y a pas de données qui lui sont destinées. Etant donné que les nœuds doivent écouter périodiquement le canal pour limiter la latence des données, il existe une consommation d'énergie due à l'écoute qui ne peut pas être évitée, même dans des scénarios où le trafic de données est faible. Sachant que l'énergie consommée durant cet état est souvent une fraction significative (50% et plus) de l'énergie consommée lors de la réception d'un paquet, un nœud capteur épuiserait donc le plus gros de son énergie en attendant des paquets entrants qu'il ne recevra pas. Nous rappelons que les radios ont généralement quatre niveaux de puissance correspondant aux états suivants : transmission, réception, écoute et sommeil.

— *Non disponibilité du récepteur (overemitting)* : Est causée par la transmission d'un paquet lorsque le nœud de destination n'est pas prêt (en mode veille).

— *Commutations fréquentes entre différents modes de fonctionnement de la radio* : Ceci peut entraîner une consommation importante d'énergie. Par conséquent, un protocole MAC doit veiller à la limitation du nombre de transitions entre les modes veille et actif pour économiser de l'énergie.

Le principal problème de la plupart des protocoles MAC conçus pour les réseaux sans fil traditionnels est que la radio du récepteur doit toujours être allumée (*idle listening*). Etant donné

que la puissance consommée lors de l'écoute d'un canal inactif est la même que la puissance consommée lors de la réception des données, la méthode en question est inefficace en termes d'énergie [141].

L'*idle listening* est un défi difficile à relever car les paquets entrants sont souvent imprévisibles. Les concepteurs des protocoles MAC pour les RCSFs doivent souvent recourir à un compromis entre une faible consommation d'énergie et une haute Qualité de Service (QoS), pour solutionner le problème de l'écoute inutile. Beaucoup d'efforts ont été faits pour réduire l'écoute inutile de la radio. Plusieurs solutions existent pour résoudre le problème de l'*écoute inactive* : protocole *contention-free* à base de TDMA, radio de réveil [142] et les protocoles à base de contention, utilisant un cycle d'activité.

Les protocoles MAC à base de contention, utilisant un cycle d'activité [2] (en Anglais, duty-cycle MAC protocols) [143] dans lesquels le temps de fonctionnement d'un nœud est divisé en cycles actif-sommeil, constituent la solution la plus couramment utilisée pour réduire l'*écoute inactive*. Chaque cycle consiste en une durée active pour les transmissions/réceptions et une durée de sommeil pendant laquelle l'interface radio est éteinte. Notons que plus le cycle d'activité est petit, plus la consommation d'énergie due à l'*écoute inactive* est faible. Idéalement, un nœud ne se réveille que lorsqu'il est sur le point de transmettre ou de recevoir des paquets.

Les protocoles MAC basés sur un cycle d'activité sont généralement classés en synchrones et asynchrones et ce selon le mécanisme employé pour coordonner la communication des nœuds (synchronisation, préambules, message de réveil) [10, 143]. S-MAC [131] et T-MAC [132] sont deux protocoles basés sur un cycle d'activité, synchrones, conçus pour les RCSFs. B-MAC [133] et X-MAC [134] sont quant à eux deux protocoles basés sur un cycle d'activité, asynchrones, conçus eux aussi pour les RCSFs. Notons que lors de la simulations de nos travaux, nous avons utilisé un protocole MAC à base de contention et asynchrone avec "1" radio, comme nous l'avons indiqué en couleur bleue dans la Figure 1.6. Il s'agit en effet du protocole TunableMAC (similaire au protocole B-MAC), fourni par le simulateur Castalia [107].

En plus de l'efficacité énergétique, d'autres facteurs importants [7, 83] doivent être pris en compte lors de la conception des protocoles MAC pour les RCSFs, entre autres, le passage à l'échelle, l'adaptabilité (incluant les changements de topologie, la taille du réseau, la densité et les caractéristiques du trafic), la latence et la fiabilité (p. ex., utilisation des acquittements et les retransmissions).

1.10.3 Couche réseau

La couche réseau (NET) est responsable de l'établissement de chemins de communication entre les nœuds d'un réseau et de la réussite du routage des paquets le long de ces chemins. Les protocoles de routage dans les RCSFs diffèrent des protocoles de routage traditionnels, dans la mesure où [18] :

— Etant donné que les nœuds capteurs n'ont pas d'adresses IP (Internet Protocol), donc les protocoles de routage IP ne peuvent pas être utilisés dans un RCSF.

2. Cycle d'activité = $\frac{actif}{(actif+sommeil)}$

— Les protocoles de routage pour les RCSFs doivent tenir compte du facteur d'échelle (scalabilité).

— Les protocoles de routage dans les RCSFs doivent tenir compte des contraintes de ressources auxquelles sont soumis ce type de réseaux, à savoir l'énergie, la bande passante et la capacité de stockage et de calcul.

— Les protocoles de routage dans les RCSFs devraient aussi aborder avec plus d'attention les problèmes de la tolérance aux pannes et de la sécurité.

1.10.4 Couche de transport

Les principaux objectifs d'un protocole de couche de transport pour les RCSFs, sont les suivants [40, 144] :

— *Contrôle de congestion* : C'est une tâche importante de la couche de transport qui permet d'atteindre la fiabilité requise. En outre, elle permet non seulement d'augmenter l'efficacité du réseau, mais aussi de conserver les ressources des nœuds capteurs.

— *Transport fiable* : Les données capturées doivent être acheminées de manière fiable vers le nœud puits. Il en est de même pour les commandes et les requêtes à destination des nœuds capteurs, et ce pour assurer le bon fonctionnement du RCSF.

— *Multiplexage et démultiplexage* : Etant donné que différentes applications peuvent fonctionner sur le même réseau, la couche de transport doit relier les couches application et réseau en utilisant le multiplexage et le démultiplexage.

Bien que les solutions développées pour les réseaux sans fil traditionnels [145] puissent être pertinentes, elles ne sont pas appropriées pour les RCSFs. des modifications importantes des protocoles de couche de transport existants sont nécessaires afin de satisfaire les objectifs cités ci-dessus et pour tenir compte des caractéristiques uniques des RCSFs [40]. Par exemple :

— TCP repose sur la retransmission de bout en bout pour fournir un transport de données fiable, qui consomme plus d'énergie et de bande passante que la retransmission à chaque saut [144]

— La corrélation inhérente dans les flux de données générés par les nœuds capteurs rend le mécanisme de fiabilité stricte de bout en bout significativement inefficace sur le plan énergétique.

— Tous ces protocoles nécessitent des besoins considérables en mémoire pour bufferiser les paquets transmis jusqu'à ce qu'ils soient reçus par le destinataire.

1.10.5 Couche application

La couche application fournit les interfaces nécessaires à l'utilisateur pour interagir avec le monde physique via le RCSF [40].

1.11 Conception Inter-Couches (CIC/CLD)

La conception inter-couches (en Anglais, Cross-Layer Design) [48–53] est une approche très importante dans le domaine des réseaux sans fil et notamment dans celui des RCSFs qui sont soumis à de fortes contraintes de ressources. La CIC/CLD permet l'interaction entre différentes couches non adjacentes, ce qui n'est pas possible dans les architectures en couches traditionnelles (les modèles OSI et TCP/IP). En effet, le modèle OSI à sept couches divise la tâche de mise en réseau globale en couches et définit une hiérarchie de services à fournir par les couches. Les services au niveau des couches sont réalisés en concevant des protocoles pour les différentes couches. L'architecture interdit la communication directe entre les couches non adjacentes. La communication entre les couches adjacentes est limitée aux appels de procédure et aux réponses [52].

En règle générale donc, la conception inter-couches fait référence à la conception de protocoles en exploitant la dépendance entre les couches de protocoles afin d'obtenir des gains de performance dans le réseau, tout en minimisant la dépense énergétique. Ceci est différent de la conception mono-couches, où les protocoles au niveau des différentes couches sont conçus indépendamment [52].

Les objectifs communs des optimisations inter-couches dans les RCSFs sont les suivants [124] :

— Réduction de la consommation d'énergie [146]

— Routage efficace [5, 54, 147–149]

— QoS [150]

— Ordonnancement optimal [151]

Différentes approches de conception inter-couches ont été proposées dans la littérature [51]. Parmi les plus utilisées, on retrouve celles basées sur :

— l'interaction de couches

— l'unification de couches adjacentes

1.11.1 CIC/CLD par interaction de couches

Dans cette catégorie, le modèle OSI traditionnel est maintenu et de nouvelles interfaces sont créées entre les couches. Les nouvelles interfaces sont utilisées pour permettre l'interaction des couches entre elles, et par conséquent le partage d'informations entre les couches lors de l'exécution. Les interactions peuvent être faites de bas en haut ou de haut en bas, comme le montre la Figure 1.8. Deux méthodes pour la mise en œuvre des interactions inter-couches sont généralement utilisées, à savoir :

1. la *communication directe entre les couches* : En pratique, la communication directe entre les couches signifie que les variables d'une couche sont visibles aux autres couches lors de l'exécution. Nous rappelons que dans une architecture mono-couches, chaque couche gère ses propres variables qui ne concernent pas les autres couches.

   La Figure 1.8 montre deux exemples d'interaction inter-couches [124] :

(a) des informations de routage au niveau de la couche réseau sont utilisées par la couche MAC afin de maximiser la durée de veille de chaque nœud, ce qui permet d'accroître l'efficacité énergétique dans le réseau [152].

(b) les informations sur l'état du canal peuvent être transmises à la couche réseau afin que le protocole de routage puisse éviter les liens de mauvaise qualité [5].

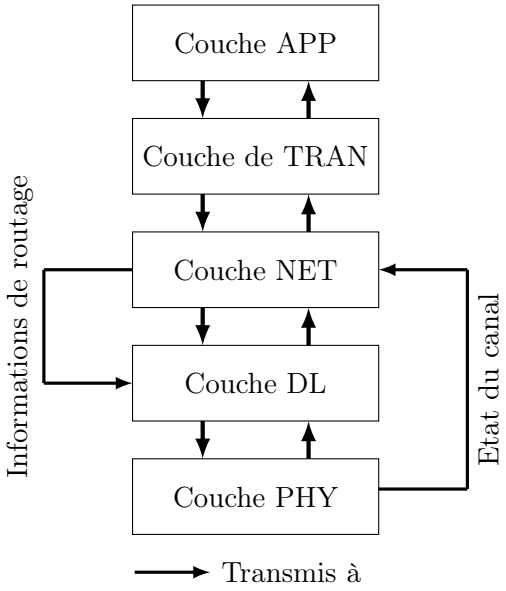


FIGURE 1.8 – Exemples d'interaction inter-couches.

2. *une base de données partagée entre les couches* : Consiste à utiliser une base de données commune accessible par toutes les couches, comme illustré dans la Figure 1.9. La base de données commune est comme une nouvelle couche, fournissant le service de stockage/récupération d'informations à toutes les couches.

   Su et al. [4] ont proposé un agent d'optimisation (En anglais, Optimization Agent (OA)) qui permet l'interaction entre différentes couches de la pile protocolaire (Figure 1.9). L'OA fonctionne comme un référentiel ou base de données qui contient les informations, tels que le numéro d'identification du nœud, le nombre de sauts, le niveau d'énergie du nœud, l'état de la liaison, etc., pour faciliter les interactions entre les différentes couches. Les interactions entre les couches peuvent être effectuées dans les deux directions et peuvent être intra-couches (entre couches adjacentes) ou inter-couches (à travers deux ou plusieurs couches adjacentes).

Benzerbadj et al. [5] et Kechar et al. [6] ont proposé une approche inter-couches basée sur l'interaction de la couche NET et la couche MAC, afin d'économiser de l'énergie. L'interaction entre ces deux couches adjacentes se fait en utilisant un simple mécanisme Stockage/Récupération sur un espace de stockage mémoire commun dédié à stocker les informations de routage actuelles, comme illustré dans la Figure 1.10.

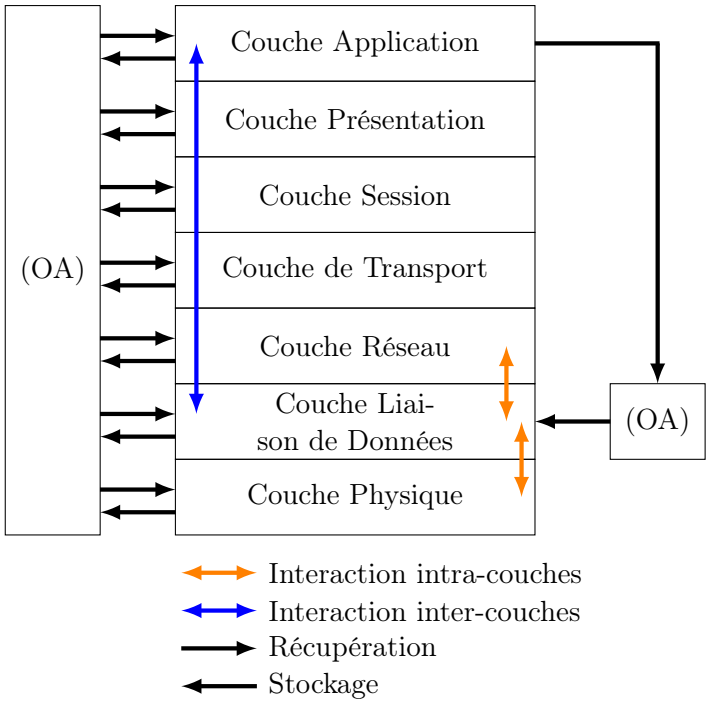


FIGURE 1.9 – Modèle de conception inter-couches proposé par [4].

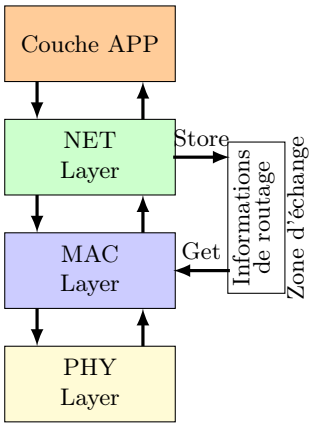


FIGURE 1.10 – Illustration de la conception inter-couches utilisée par les auteurs de [5, 6].

1.11.2 CIC/CLD par unification de couches adjacentes

Consiste à fusionner deux ou plusieurs couches adjacentes de telle sorte que le service fourni par la nouvelle super-couche soit l'union des services fournis par les couches constituantes. Cela ne nécessite aucune nouvelle interface à créer dans la pile protocolaire. Du point de vue architectural, la super-couche peut être interfacée avec le reste de la pile en utilisant les interfaces qui existent déjà dans l'architecture d'origine. Le protocole XLP proposé par Mehmet et al. [147] est le premier protocole qui intègre les fonctionnalités de toutes les couches, à partir de la couche PHY jusqu'à la couche TRAN dans un protocole inter-couches (voir Figure 1.11). Ce protocole assure

le contrôle de la congestion, le routage et le contrôle de l'accès au médium.

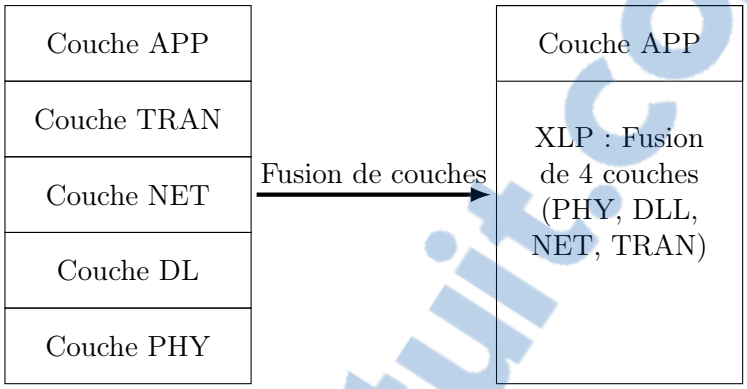


FIGURE 1.11 – XLP : Protocole inter-couches intégrant les fonctionnalités des quatre couches au dessous de la couche application.

1.12 Technologies de communication sans fil et les RCSFs

Les communications sans fil peuvent être classées en fonction de leurs applications typiques, débits et couverture. Le Tableau 1.4, émanant de l'IEEE (Institute of Electrical and Electronics Engineers), illustre cette classification [10] .

Classe	Débit	Couverture radio	Applications typiques	Standard de communication sans fil
WWAN	<10 Mbps	>10 km	Téléphonie, internet mobile	GSM, UMTS, satellite
WMAN	<100 Mbps	<10 km	Internet haut débit	IEEE 802.16, HIPERMAN
WLAN	<100 Mbps	<100 m	Remplacement du LAN filaire	IEEE 802.11, HIPERLAN/2
WPAN	<10 Mbps	<10 m	Transfert de données, personnelles	Bluetooth, IEEE 802.15.3
WSN	<1 Mbps	<1 km	Surveillance, contrôle	Propriétaire, IEEE 802.15.4, RFID

Tableau 1.4 – Une classification des technologies de communication sans fil [10].

Les réseaux étendus sans fil (WWANs) et les réseaux métropolitains sans fil (WMAN) offrent la couverture géographique la plus large, parmi les autres classes de réseaux énumérées dans le Tableau 1.4.

Les WWANs sont des réseaux sans fil qui peuvent être déployés sur de vastes zones tels que des villes ou des pays. Ils sont principalement constitués de réseaux téléphoniques cellulaires numériques tels que le système mondial de communications mobiles (GSM) et le Système de

télécommunications mobiles universelles (UMTS). Les satellites de communication appartiennent également à cette classe de réseaux.

Les WMANs (Wireless Metropolitan Networks) permettent la connexion de plusieurs réseaux dans une région métropolitaine, tels que différents bâtiments dans une ville ou dans un campus universitaire. Les WMANs sont basés sur les standards IEEE 802.16 HIPERMAN.

Les WLANs (Wireless Local Area Network) couvrent une petite zone (maison, bureau ou bâtiment). Ils ont été conçus pour étendre ou remplacer les LAN filaires, dans les cas où le câblage était coûteux ou impossible à réaliser en raison de la mobilité, de la courte durée de vie du réseau ou de la valeur historique des bâtiments. Le standard de base de ces réseaux est le IEEE 802.11 et ses nombreuses extensions pour des vitesses de communication plus élevées, le support de la qualité des services, la sécurité et la mise en réseau maillée. D'autres normes et spécifications industrielles, telles que le réseau local radioélectrique haute performance de type 2 (HIPERLAN/2), la arête d'un graphe domestique (HomeRF) et les télécommunications numériques sans fil améliorées (DECT), sont restées au stade de normalisation.

Les WPANs fournissent une interconnexion entre les appareils personnels, incluant les PDAs, les téléphones mobiles, les casques d'écoute et les ordinateurs portables. Bluetooth et IEEE 802.15.3 sont des exemples de WPANs.

Les RCSFs [153] constituent une classe émergente de technologies sans fil qui a récemment suscité beaucoup d'intérêt dans le domaine industriel et académique, et dont la prolifération massive est attendue dans les toutes prochaines années. Contrairement aux WLAN et aux WPAN, les RCSFs sont considérés comme étant à plus grande échelle, auto-organisés et strictement orientés application. Les RCSFs ont été mis en œuvre en tant que solutions propriétaires [10]. Si nous considérons uniquement les RCSFs sans fil à faible coût, faible consommation d'énergie, faible débit de données et courte portée de communication, le IEEE 802.15.4 LR-WPAN (Low-Rate WPAN) est la norme de communication la plus couramment utilisée pour l'implémentation de ce type de réseaux. Deux autres standards emergents, à savoir, ZigBee et 6LowPAN, basés sur le standard IEEE 802.15.4, sont largement adoptés dans la mise en œuvre des RCSFs.
La technologie d'identification par radio-fréquence (RFID) peut également être considérée comme appartenant à la classe des RCSFs avec une mise à l'échelle et des performances réseau limitées.

1.13 Interconnection des RCSFs avec les réseaux TCP/IP

« L'internet du futur, conçu comme un internet des objets (en Anglais, Internet of Things -IoT-, Internet of objects or Cyber-Physical Systems -CPS-), devrait être un réseau mondial d'objets interconnectés adressables uniquement, basé sur des protocoles de communication standards » [154]. Tout objet identifié par une adresse unique, y compris les ordinateurs, les capteurs, les étiquettes RFID ou les téléphones mobiles sera en mesure de rejoindre dynamiquement le réseau, de collaborer et coopérer efficacement pour accomplir différentes tâches.

L'une des tâches de conception les plus importantes de l'IoT est décrite comme étant l'intégration des RCSFs à internet [19, 20]. Cette intégration permet aux flux de données générés par un RCSF d'être accessibles à tout utilisateur autorisé, qu'il soit humain ou machine, partout

dans le monde, en utilisant des mécanismes standards. Trois approches de base permettent de connecter les RCSFs à internet [155–158], à savoir :

— Solution basée sur un proxy frontal (en Anglais Front-end Proxy solution)

— Solution basée sur une passerelle (en Anglais, Gateway solution)

— Solution basée sur une connectivité TCP/IP native (en Anglais, TCP/IP Overlay solution)

1.13.1 Solution basée sur un proxy frontal

Dans une solution proxy frontal, Il n'y a pas de connexion directe entre Internet et un nœud capteur. La communication entre les utilisateurs TCP/IP (Internet) et les nœuds capteurs se fait à travers le sink (station de base). Ce dernier sert d'interface entre le réseau d'acquisition de données (RCSF) et le réseau de diffusion de données (Internet). La station de base recueille et stocke toutes les informations provenant du RCSF, et envoie également des informations de contrôle aux nœuds capteurs. Etant donné que le RCSF est complètement indépendant d'Internet, il peut implémenter ses propres protocoles et algorithmes.

1.13.2 Solution basée sur une passerelle

Dans une solution à base de passerelle, le sink (ou station de base) agit comme une passerelle de couche d'application, chargée de traduire les protocoles des couches inférieures des deux réseaux (TCP/IP et propriétaire). Par conséquent, les nœuds capteurs et les hôtes TCP/IP peuvent directement échanger des informations.

Notons qu'il existe une autre solution similaire à celle que nous venons de décrire ci-dessus et est appelée solution à base de passerelle pour les réseaux tolérants au retard (en Anglais, Delay-Tolerant Networks gateway solution -DTN-). Elle se caractérise par le fait qu'elle implémente une nouvelle couche dans les deux réseaux (TCP/IP et RCSF), appelée *Bundle Layer*. La fonction principale de cette couche est de stocker et transférer (en Anglais, to forward) les paquets entre les deux réseaux. Cette solution offre la possibilité de différer la transmission d'un paquet dans le cas où le lien entre le sink et le nœud capteur est rompu.

1.13.3 Solution basée sur une connectivité TCP/IP native

Les nœuds capteurs communiquent avec d'autres nœuds en utilisant le protocole TCP/IP. Le sink va donc jouer le rôle d'un simple routeur uniquement, transférant les paquets depuis et vers les nœuds capteurs. Ces derniers doivent implémenter les protocoles et les normes utilisés sur internet, telles que la pile TCP/IP et les interfaces de services Web.

L'implémentation de la pile TCP/IP dans les RCSFs fait face à de nombreux problèmes, parmi lesquels [158] :

— Comment une adresse IP est assignée au nœud capteur

— Comment combiner efficacement, en fonction du trafic réseau, le routage basé sur l'adresse et celui basé sur les données

Une solution typique à base de connectivité TCP/IP native, est le standard émergent 6LowPAN. Ce dernier définit la méthode de transmission d'un paquet IPv6 sur une couche MAC IEEE 802.15.4. Les utilisateurs d'internet peuvent accéder à un nœud capteur directement en utilisant son adresse IPv6.

1.14 Environnement de déploiement des RCSFs

Les RCSFs sont déployés dans différents environnements internes et externes (en Anglais, indoor and outdoor environments), et ce en fonction des applications cibles.

La facilité de déploiement, la mise en réseau sans infrastructure, le déploiement dans des zones inaccessibles et parfois hostiles, la mobilité et la communication par diffusion, sont parmi les avantages des RCSFs [7, 40]. Ces avantages sont rendus possible grâce à la communication sans fil qui en même temps engendre des défis dus à la variabilité en temps et en espace du canal sans fil. Il convient de noter que la nature non déterministe du canal sans fil a un impact sur les protocoles des couches supérieures de la pile protocolaire, et qu'il convient d'en tenir compte. Nous rappelons qu'un des objectifs de cette thèse est justement la conception d'un protocole de routage géographique conscient de l'état du canal (en Anglais, channel-aware geographic protocol). Il permet un routage des paquets de données à travers des liens symétriques éprouvant la plus petite atténuation de parcours (en Anglais, symmetrical link experiencing the lowest path loss).

L'irrégularité de la radio [30, 31] est un phénomène commun dans les RCSFs. Ce phénomène est dû au type d'antenne et du médium, à la présence d'obstacles (par ex., les bâtiments, les collines, les montagnes, les murs dans un environnement indoor) et aux conditions météorologiques.

Le modèle largement utilisé pour l'étude des RCSF, à savoir le modèle à base de disques unitaires (en Anglais, Unit Disk Graph (UDG) [39, 40], ne permet pas de refléter le phénomène de l'irrégularité de la radio. Un UDG est en fait une simplification de la réalité. Il représente la portée d'un nœud capteur sous forme d'un disque centré autour du nœud avec un rayon égal à 1, comme illustré dans la Figure **??**(a)). Pour représenter les caractéristiques aléatoires du canal sans fil et par conséquent produire de solides résultats théoriques, la communauté scientifique a eu recours au modèle réaliste basé sur des disques non unitaires (en Anglais, Non-Unit Disk Graph (N-UDG)) (voir Figure 1(b)).

Plusieurs modèles de propagation des signaux radio ont été proposés dans la littérature [12]. Ils permettent de prédire l'influence de l'environnement sur la propagation du signal radio, en particulier, l'estimation de la puissance du signal à la réception à une certaine distance. Parmi ces modèles, nous citerons ceux proposés par le simulateur Castalia [107] que nous avons utilisé pour l'implémentation et la simulation des travaux de cette thèse.

1.14.1 Modèle de propagation en espace libre

Ce modèle suppose les conditions de propagation comme étant idéales, et que le rayon de propagation du signal radio est un disque, à l'intérieur duquel la réception est parfaite, et au-delà duquel il n'y a pas du tout de réception. Comme on peut le déduire, ce modèle de propagation

génère un graphe de connectivité réseau basé sur le modèle non réaliste dit modèle UDG.
La puissance reçue à une distance Transmetteur-Récepteur (T-R), notée d (en mètre) avec $d \geq d_0$, peut être calculée à partir de l'équation de Friis [58] suivante :

$$P_r(d) = \frac{P_t \times G_t \times G_r \times \lambda^2}{(4\pi)^2 \times d^2 \times L} \tag{1.1}$$

$$= \frac{P_t \times G_t \times G_r \times \lambda^2}{(4\pi)^2 \times d_0^2 \times L} \times \left(\frac{d_0}{d}\right)^2 \tag{1.2}$$

$$= P_r(d_0) \times \left(\frac{d_0}{d}\right)^2 \tag{1.3}$$

où :

— P_t est la puissance de transmission

— G_t et G_r sont les gains d'antenne de l'émetteur et du récepteur

— λ est la longueur d'onde

— d est la distance réelle entre l'émetteur et le récepteur

— d_0 est la distance de référence

— $L \geq 1$ résume les pertes dues aux circuits d'émission/réception

1.14.2 Modèle Log-distance path loss

Pour les environnements autres que l'espace libre, l'Equation (1.3) peut être généralisée comme suit :

$$P_r(d) = P_r(d_0) \times \left(\frac{d_0}{d}\right)^n \tag{1.4}$$

où :

— n est l'exposant de l'atténuation de parcours. Il indique à quelle vitesse l'atténuation de parcours augmente avec la distance T-R. Le Tableau 1.5 montre les valeurs de n pour différents environnements.

Environnement	n
Free space	2
Urban area cellular radio	2.7 to 3.5
Shadowed urban cellular radio	3 to 5
In building line-of-sight	1.6 to 1.8
Obstructed in building	4 to 6
Obstructed in factories	2 to 3

Tableau 1.5 – L'exposant de l'atténuation de parcours pour différents environnements [12].

L'*atténuation de parcours* (en Anglais, *path loss*) est définie comme le rapport de la puissance rayonnée à la puissance reçue $\frac{P_t}{P_r(d)}$ [58]. Elle peut être exprimée en decibel (dB), à partir de l'Equation (1.4) :

$$PL(d)[dB] = PL(d_0)[dB] + 10 \times n \times log_{10}(\frac{d}{d_0}) \tag{1.5}$$

où :

— $PL(d)$ est l'atténuation de parcours (en dB) à la distance T-R, notée d (en mètre),

— $PL(d_0)$ est l'atténuation de parcours (en dB) à la distance de référence d_0 (en mètre),

La puissance reçue $P_r(d)$ à la distance T-R notée d, est exprimée comme suit :

$$P_r(d)[dBm] = P_t[dBm] - PL(d)[dB] \tag{1.6}$$

1.14.3 Modèle log-normal shadowing

C'est une extension du modèle précédent qui prend en compte la présence d'obstacles. L'atténuation de parcours peut être exprimée comme suit :

$$PL(d)[dB] = PL(d_0)[dB] + 10 \times n \times log_{10}(\frac{d}{d_0}) + X_\sigma[dB] \tag{1.7}$$

où :

— X_σ est une variable aléatoire gaussienne (en dB), de moyenne nulle et d'écart-type σ (en dB). Elle représente l'effet shadowing.

Dans ce modèle, le rayon de communication n'est plus considéré comme un disque parfait. Par conséquent, le graphe de connectivité du réseau est un graphe basé sur le modèle réaliste d'étude des réseaux sans fil dit modèle N-UDG.

1.15 Conclusion

Dans ce chapitre, nous avons présenté un état de l'art sur les RCSFs. Nous avons montré l'importance de la conception inter-couches qui permet d'obtenir des gains de performance dans un RCSF, notamment en termes d'énergie, à travers l'exploitation de la dépendance entre les couches de la pile protocolaire. Nous avons aussi mis en évidence le rôle primordial de la technique du "duty cycling" dans la réduction de la consommation d'énergie des nœuds capteurs, et par conséquent dans l'extension de la durée de vie du RCSF. L'accent a été aussi mis sur l'intérêt de l'intégration des RCSFs à l'internet afin de permettre l'accessibilité, à travers la planète, aux flux de données générés par ces réseaux. En fin de chapitre, nous avons souligné l'extrême importance de s'appuyer sur un modèle radio réaliste lors de la conception des protocoles pour les RCSFs, ce qui constitue une méthode de recherche très prometteuse puisqu'elle tient compte de la nature variable du canal radio. Etant donné que cette variabilité aléatoire du canal radio a un impact certain sur les couches supérieures, la tendance de recherche dont nous parlons permet

de proposer des solutions, à tous les niveaux de la pile protocolaire, ayant un degré de confiance élevé par rapport aux solutions qui s'appuient sur un modèle radio idéaliste. Par conséquent ces solutions seront facilement reconnues par la communauté scientifique.

Dans le chapitre suivant, nous allons présenter un état de l'art sur les protocoles de routage dans les RCSFs, avec une attention particulière pour le routage géographique auquel nous nous intéressons dans cette thèse. Nous allons surtout mettre en évidence les problèmes auxquels font face les deux stratégies de routage les plus utilisées par les protocoles de routage géographique, à savoir l'approche *glouton* et l'approche *périmètre*, quand elles sont exécutées sur un N-UDG qui est la conséquence de la présence du phénomène de l'irrégularité de la radio.

Chapitre 2

Le routage dans les RCSFs

2.1 Introduction

Les données collectées par les nœuds capteurs dans un RCSF sont généralement propagées vers un sink (passerelle) connecté à un système de décision distant. Dans les RCSFs de petite taille où les nœuds et le sink sont à proximité, la propagation des données se fait généralement en mode mono-saut (communication directe entre les nœuds et le sink). Cependant, la plupart des applications à base des RCSFs nécessitent un grand nombre de nœuds capteurs qui couvrent de grandes zones. Il en résulte que le sink pourrait être hors de la portée de communication du ou des nœud(s) source(s). Dans ce cas de figure une approche de communication multi-sauts est nécessaire. Ce mode de communication est aussi employé en raison de la rareté de la ressource énergétique au niveau des nœuds capteurs et de la limite de la puissance de transmission de ces derniers. Dans une telle approche de communication, les nœuds capteurs doivent non seulement générer et diffuser leurs propres informations, mais aussi servir de relais pour d'autres nœuds. Le processus d'établissement de chemins d'un nœud source vers le sink, directement ou à travers un ou plusieurs relais est appelé routage et est assuré par la couche réseau de la pile protocolaire.

L'approche de communication multi-sauts devient également inévitable dans les deux cas suivants qui constituent l'objet de cette thèse :

1. les RCSFs dédiés aux applications de surveillance de zones sensibles, afin d'éviter l'interception des signaux Radio Fréquence (en Anglais, Radio-Frequency -RF-). En effet, dans ce mode de communication, les niveaux de puissance d'émission sont maintenus à bas niveau..
2. Les RCSFs déployés dans un environnement *réaliste* caractérisé par la présence du phénomène de l'irrégularité de la radio [30, 31]. Ce phénomène résulte de multiples facteurs, tels que le type d'antenne et le type du médium, et est accentué par les obstacles (par exemple, les bâtiments, les collines, les montagnes) et les conditions météorologiques. Le mode de communication multi-sauts va donc permettre de surmonter l'atténuation du signal, due à la présence de ce phénomène [40]. Notons que cette atténuation est beaucoup plus importante dans les liaisons sans fil de longue distance. En effet, la distance est aussi un facteur d'atténuation du signal, comme le montre l'Equation (1.7).

Le routage est l'un des principaux problèmes dans les RCSFs. En effet, la conception d'un

protocole de routage pour les RCSFs est très difficile en raison :

1. Des caractéristiques inhérentes qui distinguent ces réseaux des autres réseaux sans fil comme les réseaux Ad hoc mobiles (en Anglais, Mobile Ad hoc NETwork -MANET-) ou les réseaux cellulaires [159, 160] .
2. La non fiabilité des liaisons sans fil comme on l'a mentionné ci-dessus en mettant en évidence le phénomène de l'irrégularité des portées radio.

L'objectif des protocoles de routage dans les RCSFs est donc d'assurer une communication multi-sauts à faible coût énergétique, et fiable.

Ce chapitre présente un état de l'art sur le routage dans les RCSFs avec une mise en évidence du routage géographique auquel nous nous intéressons dans cette thèse. Nous présentons tout d'abord les défis et les métriques du routage dans ce type de réseaux, puis nous donnons une classification des protocoles de routage dans les RCSFs, selon trois critères qui sont : la structure ou l'organisation du réseau, le processus de découverte des routes et la stratégie de routage employée. Au sein de la classe des protocoles géographiques, nous détaillons le fonctionnement des deux approches d'acheminement de paquets les plus utilisées par ces protocoles, en l'occurrence l'approche en mode *glouton* et l'approche en mode *périmètre*. Le protocole géographique Greedy Perimeter Stateless Routing (GPSR) est aussi largement décrit. A la fin du chapitre nous expliquons les problèmes auxquels font face les techniques de routage en mode *glouton* et en mode *périmètre* quand elles sont exécutées sur un N-UDG qui reflète la présence du phénomène de l'irrégularité de la radio.

2.2 Défis du routage dans les RCSFs

La conception de protocoles de routage pour les RCSFs fait face à de nombreux défis dus aux particularités de ces réseaux et à la non fiabilité des liaisons sans fil. Dans ce qui suit, nous allons énumérer les principaux défis auxquels est confronté le routage dans les RCSFs [40].

2.2.1 Consommation d'énergie

En raison du budget énergétique limité alloué aux nœuds capteurs, la consommation d'énergie est la principale préoccupation dans les RCSFs. Par conséquent tous les protocoles de la pile protocolaire doivent obligatoirement tenir compte de la rareté de cette ressource. Ainsi, un protocole de routage doit acheminer les données, depuis les nœuds sources vers le(s) nœud(s) puits, à faible coût énergétique sans pour autant compromettre la précision du contenu de l'information (c.-à-d., d'une façon fiable). Pour y arriver, un tel protocole ne doit pas se contenter uniquement de la métrique conventionnelle qui consiste à minimiser le nombre de sauts entre la source et la destination. Cette métrique peut en effet ne pas convenir à cause de la non fiabilité des liaisons sans fil. De nouvelles métriques de routage à efficacité énergétique doivent être développées pour les RCSFs. Elles peuvent être développées en se basant sur une approche inter-couches tel que nous le verrons dans le prochain chapitre, quand nous présenterons notre première contribution qui consiste à router les paquets en utilisant un compromis entre le nombre de sauts parcourus et la qualité des liens constituants le chemin entre la source et la destination.

2.2.2 Passage à l'échelle

Les RCSFs sont généralement constitués d'un grand nombre de nœuds, de l'ordre de centaines ou de milliers ou plus, déployés le plus souvent avec une haute densité pour pouvoir observer en détail les phénomènes physiques. Le grand nombre de nœuds empêche les nœuds de connaître la topologie de l'ensemble du RCSF. Par conséquent, des protocoles entièrement distribués, fonctionnant avec une connaissance limitée de la topologie, doivent être développés pour permettre le passage à l'échelle. De plus, étant donné que la densité est élevée dans le réseau, l'échange d'informations locales devrait également être limité pour améliorer la performance du réseau en termes d'énergie. En outre, étant que les utilisateurs dans un RCSF sont intéressés par des informations collectives provenant de plusieurs capteurs concernant un phénomène physique donné au lieu d'informations provenant de capteurs individuels, le protocole de routage doit prendre en charge le traitement en réseau sans compromettre la consommation d'énergie.

2.2.3 Robustesse

La tolérance aux pannes est l'un des problèmes critiques dans les RCSFs [83]. En effet, les nœuds capteurs sont susceptibles d'être défaillants en raison de :

— L'épuisement de l'énergie

— Une défaillance matérielle

— Erreurs de liaison de communication (p. ex., à cause de l'irrégularité de la radio ou de l' interférence)

— Une attaque malveillante

— Etc.

Un protocole de routage pour les RCSFs doit donc être robuste contre ces défaillances.

2.2.4 Topologie

Dans plusieurs études, la topologie des RCSFs est supposée être statique. Cependant, dans de nombreuses applications, les nœuds puits, les nœuds capteurs ou l'évènement observé (la cible) peuvent être mobiles [58, 161]. En outre, en raison de la rareté de la ressource énergétique, les nœuds peuvent basculer entre deux états, actif et sommeil, pour économiser de l'énergie. Quand un nœud est dans un état de sommeil, il est retiré de la topologie du réseau. Il la rejoindra à nouveau quand il basculera en mode actif. Ces changements dynamiques peuvent affecter la structure de communication et par conséquent, les routes. Le protocole de routage doit donc s'adapter à ces changements de topologie du réseau.

2.2.5 Application

Le type d'application joue un rôle important dans la conception des protocoles de routage. En effet, dans les applications de surveillance de l'environnement (time-driven schemes) par exemple, les nœuds communiquent périodiquement leurs données collectées. Dans ce cas de figure,

des routes statiques peuvent être utilisées pour acheminer ces données, et ce tout au long de la durée de vie du RCSF. Cependant, dans les applications basées sur des événements (event-driven schemes telle que la détection de feux de forêt), les nœuds capteurs sont en état de veille la plupart du temps. Dès qu'un événement se produit, des routes doivent être générées, depuis le nœud qui a détecté l'évènement jusqu'au nœud puits, pour transmettre l'alerte à temps. Dans le cas de schémas basés sur des requêtes (query-event schemes), C'est au nœud sink de demander des données aux capteurs en cas de besoin. Il s'agit en effet du routage orienté-données qui fournit des itinéraires en fonction du contenu de la requête. Comme nous pouvons le constater, des techniques de routage différentes peuvent être nécessaires pour différents types d'applications.

2.2.6 Adressage

En raison du nombre relativement important de nœuds capteurs dans un réseau, les protocoles de routage basés sur les adresses ne peuvent pas être adoptés dans les RCSFs car ils nécessitent des adresses uniques pour chaque nœud du réseau. En outre, les utilisateurs sont intéressés par des informations collectives provenant de plusieurs capteurs concernant un phénomène physique donné au lieu d'informations provenant de capteurs individuels. Par conséquent, des protocoles de routage basés sur de nouveaux mécanismes d'adressage ou de nouvelles techniques de routage qui ne nécessitent pas d'identifiants uniques pour chaque nœud sont nécessaires (p. ex., routage centré sur les données).

2.3 Métriques de routage

Dans ce qui suit, nous allons présenter un bref aperçu sur les métriques de routage couramment utilisées dans les RCSFs [7].

2.3.1 Nombre de sauts minimal

C'est la métrique la plus utilisée dans les protocoles de routage. Elle consiste à trouver le chemin, du nœud source vers le nœud destination, nécessitant le plus petit nombre de sauts. L'utilisation de cette métrique devrait normalement générer de faibles délais de bout en bout et une faible consommation de ressources, puisqu'elle réduit le nombre de nœuds impliqués dans la communication. Cependant, étant donné que l'approche basée sur le nombre de sauts minimal ne tient pas compte de la disponibilité réelle des ressources au niveau de chaque nœud, la route générée est probablement non optimale en termes de délai, d'énergie et d'évitement de congestion. Notons que le fonctionnement de cette approche est revisité, à la lumière du phénomène de l'irrégularité de la radio, dans le prochain chapitre.

2.3.2 Energie

Etant donné que la consommation de l'énergie est une préoccupation majeure dans les RCSFs, l'efficacité énergétique est un aspect fondamental du routage dans ces réseaux. Cependant, il convient de noter qu'à la place d'une métrique d'énergie unique pouvant être appliquée au

problème de routage, il existe différentes interprétations de l'efficacité énergétique, dont nous énumérons quelques unes d'entre elles ci-dessous [162].

2.3.2.1 Energie minimale consommée par paquet

L'objectif est de minimiser la quantité totale d'énergie dépensée pour l'acheminement d'un seul paquet de la source à la destination. L'énergie totale est la somme de l'énergie consommée par chaque nœud constituant le chemin entre la source et la destination, pour recevoir et transmettre le paquet.

2.3.2.2 Temps maximum pour la partition d'un réseau

La partition d'un réseau peut intervenir suite à l'épuisement de la batterie d'un nœd qui relie deux parties de ce réseau, créant ainsi un sous-réseau qui n'est pas joignable. Pour éviter un tel scénario, il devient essentiel de réduire la consommation d'énergie de l'ensemble minimal de nœuds dont la suppression entraînera la partition du réseau. Par conséquent, on maintient un réseau où chaque nœud capteur peut être atteint via au moins une route.

2.3.2.3 Variance minimale des niveaux de puissance des nœuds

Il s'agit de répartir la consommation d'énergie sur tous les nœud du réseau qui sont considérés tous comme ayant une importance égale. Le but d'une telle approche pourrait être de maximiser la durée de vie du réseau,

2.3.2.4 Maximum (moyenne) de la capacité énergétique totale

Contrairement à la métrique "énergie minimale consommée par paquet" qui s'intéresse au coût énergétique de l'acheminement d'un paquet de la source à la destination, cette approche met l'accent sur l'énergie résiduelle (capacité énergétique) au niveau des nœuds capteurs. Un protocole de routage basé sur cette métrique privilégie les routes constituées de nœuds capteurs qui disposent de la plus grande énergie résiduelle, de la source à la destination. Ces routes sont dites routes à capacité énergétique totale maximale. Cependant, un tel protocole doit éviter de choisir des chemins inutilement longs afin de maximiser la capacité énergétique totale. Une variante de cette métrique est de maximiser la capacité énergétique moyenne ce qui permet d'éviter ce problème.

2.3.2.5 Maximum de la capacité énergétique minimale

L'objectif est de sélectionner la route ayant la plus grande capacité énergétique minimale. Cette technique favorise également les routes avec des réserves d'énergie plus importantes, mais protège également les nœuds de faible capacité contre l'expiration prématurée.

2.3.3 QoS

La QoS désigne des métriques de performance définies dans les réseaux, y compris la latence (ou délai) et le débit (en Anglais, throughput) de bout en bout, mais également la gigue (variation de délai) et la perte de paquets. Le choix d'une métrique QoS dépend du type d'application. Par exemple, les RCSFs dédiés à la détection et le suivi de cibles sont des réseaux non tolérants au délai (en Anglais, no delay tolerant networks). Par contre, les Réseaux de Capteurs Multimédia Sans Fil (RCMSF) qui sont concernés par le transit d'un volume élevé de données, peuvent nécessiter un débit élevé (en Anglais, high throughput).
En général, plusieurs métriques de qualité de service sont combinées, par exemple, le produit le produit de la bande passante d'un lien et son délai de bout en bout. Notons enfin que les RCSFs doivent chercher un compromis entre la satisfaction des exigences de qualité de service spécifiques à l'application et l'objectif primordial dans ce type de réseau qui est l'efficacité énergétique.

2.3.4 Robustesse

Il s'agit de choisir un chemin constitué de liens de bonne qualité (fiables) pour augmenter la probabilité de la transmission des paquets.

2.4 Classification des protocoles de routage dans les RCSFs

La Figure 2.1 présente trois classifications différentes des protocoles de routage dans les RCSFs [159], et ce sur la base de la structure ou l'organisation du réseau, le processus de découverte des routes et la stratégie de routage du protocole. Il convient de rappeler que certains protocoles de routage peuvent être classés dans plus d'une classe et sous-classe tel que illustré par le Tableau 2.2.

2.4.1 Classification selon la structure du réseau

En ce qui concerne la structure ou l'organisation du réseau, on recense trois classes auxquelles appartiennent la plupart des protocoles de routage.

2.4.1.1 Routage plat

Dans les réseaux organisés en topologie plate, tous les nœuds jouent le même rôle concernant le routage. En raison du grand nombre de nœuds, il n'est pas possible d'attribuer un identifiant global à chaque nœud. Cette considération conduit au routage centré sur les données (en Anglais, data-centric routing), où le nœud puits envoie des requêtes à certaines régions et attend des données provenant des nœuds capteurs situés dans les régions sollicitées. Etant donné que les données sont demandées via des requêtes, la désignation des attributs est nécessaire pour spécifier les propriétés de ces données.

Sensor Protocols for Information via Negotiation (SPIN) [17, 163] est le premier protocole centré sur les données, qui considère la négociation de données entre les nœuds capteurs afin d'éliminer la transmission de données redondantes à travers le réseau et économiser de l'énergie.

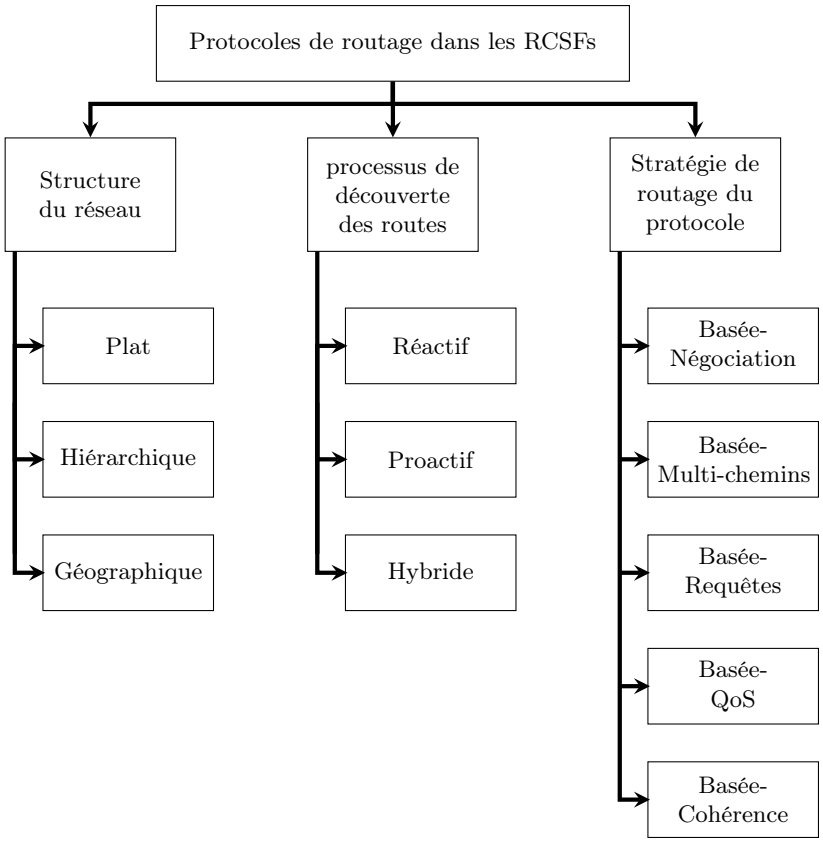


FIGURE 2.1 – Classification des protocoles de routage dans les RCSFs.

SPIN est rendu efficace par rapport aux techniques du *flooding* [17] et du *gossiping* [17] grâce à cette négociation entre les nœuds avant l'envoi des données réelles. En effet, au lieu d'envoyer toutes les données brutes collectées, les nœuds capteurs négocient entre eux par l'intermédiaire de paquets d'annonce contenant les méta-données décrivant les données. Les données collectées sont envoyées uniquement aux nœuds capteurs intéressés (qui répondent par un paquet de demande de données) à la suite de cette négociation. En outre, SPIN permet à chaque nœud de participer ou non à la négociation sur la base de son énergie résiduelle.

Plus tard, Directed Diffusion [164, 165], un autre protocole basé sur le routage centré sur les données et à efficacité énergétique, a été développé. Directed Diffusion diffère de SPIN dans la mesure où les requêtes sont émises à la demande par les nœuds puits et non annoncées par les nœuds capteurs comme dans SPIN.

2.4.1.2 Routage hiérarchique

Dans les protocoles de routage hiérarchiques, différents nœuds peuvent assumer différents rôles dans le processus de routage. Par exemple, certains nœuds peuvent être chargés de router des données pour le compte d'autres nœuds tandis qu'un autre ensemble de nœuds s'occupent uniquement de la génération et la propagation de leurs propres données. Dans une topologie

hiérarchique, les nœuds capteurs sont organisés en clusters. La création de clusters et l'attribution de tâches spéciales aux têtes des clusters peuvent considérablement renforcer le passage à l'échelle, accroître la durée de vie et l'efficacité énergétique du système global. Le routage hiérarchique est une manière efficace de réduire la consommation d'énergie dans un cluster en effectuant l'agrégation et la fusion de données afin de réduire le nombre de messages transmis au nœud puits. Low-Energy Adaptive Clustering Hierarchy (LEACH) [166] est l'une des premières approches de routage hiérarchique pour les RCSFs.

2.4.1.3 Routage géographique

Les protocoles de routage basés sur la position (en Anglais, position-based ou location-based protocols) reposent sur les positions des nœuds pour prendre des décisions de routage [32–34]. L'adresse de chaque nœud est déterminée en fonction de son emplacement physique qui peut être obtenu par satellite à l'aide de la technique GPS (Global Positioning System) ou d'autres techniques de positionnement [38, 69–72]. Chaque nœud n'a besoin de connaître que sa propre position, celle de ses voisins à un saut et celle de la destination finale, pour acheminer les paquets. Le routage basé sur la position ne nécessite donc pas l'établissement ou la maintenance de routes et par conséquent il permet le passage à l'échelle, et ce même dans le cas où le réseau est très dynamique [33]. Nous rappelons que La position de la destination finale est contenue dans l'entête du paquet à acheminer tandis que les position des voisins sont apprises à travers l'envoi à un saut de petits messages *hello*. Ces messages *hello* sont diffusés périodiquement par tous les nœuds, et contiennent l'IDentifiant (ID) et la position du nœud émetteur. Il convient de noter que la destination finale représente l'emplacement d'un nœud(nœud puits) ou d'une région géographique dans le cas de l'approche dite *geocasting*. Cette approche consiste à diffuser les données à tous les nœuds situés dans une certaine région géographique.

Les défis du routage géographique incluent la recherche d'un chemin efficace autour d'un vide qui s'est formé dans le réseau. Nous rappelons que la présence de vides dans un RCSF est due à l'irrégularité des portées de transmission des nœuds capteurs (à cause de l'irrégularité de la radio) [30, 31], au déploiement aléatoire initial des nœuds ou à un changement de topologie intervenant durant la durée de vie du réseau. Un protocole de routage géographique doit aussi être en mesure de gérer d'éventuelles inexactitudes dans les informations de localisation.

Les routages en mode *glouton* (en Anglais, *greedy* routing) et en mode *périmètre* ou *par face* (en Anglais, *perimeter* ou *face* routing) sont deux des premières stratégies de routage géographique et qui ont été ensemble à la base de nombreuses approches ultérieures. Le routage en mode *périmètre* est une stratégie de recouvrement en cas d'échec du routage en mode *glouton*, en présence de vides de routage (en Anglais, *routing voids* ou *routing holes*).

Plusieurs études ont montré que ces deux approches de routage, les plus utilisées par les protocoles de routage basés sur la position, ne fonctionnent pas bien quand elles sont exécutées sur un graphe de connectivité réseau modélisé avec des disques non unitaires (en Anglais, Non Unit Disk Graph (N-UDG)) [39, 41–47]. Un tel graphe de connectivité reflète la présence du phénomène de l'irrégularité de la radio qui est un phénomène commun dans les RCSFs. Les problèmes auxquels font face ces deux techniques de routage sont détaillés dans la Section 2.5.

2.4.1.3.1 Routage géographique en mode glouton

L'objectif de cette approche est de rapprocher, à chaque saut, le paquet de la destination finale. Pour répondre à cette exigence, plusieurs stratégies de routage, à base de distance, de progression et de direction, ont été proposées :

Mode glouton

L'objectif de cette approche est de minimiser le nombre de sauts requis pour atteindre la destination finale. Pour cela, la technique utilisée consiste à choisir, lors de chaque saut, un voisin qui minimise la distance à la destination. Par exemple, dans la Figure 2.2, le nœud source S choisira comme prochain saut le nœud E. Etant donné qu'elle tente, à chaque saut, de maximiser la progression vers la destination, l'approche *glouton* (en Anglais, *greedy)* est un bon choix quand la force du signal ne peut pas être ajustée.

Nearest with Forward Progress (NFP)

Cette stratégie choisit le plus proche voisin parmi tous les voisins qui permettent une progression positive, en termes de distance géographique, vers la destination finale [167]. Les nœuds capteurs qui peuvent adapter leurs puissances de transmission peuvent choisir la plus petite puissance de transmission nécessaire pour atteindre ce voisin. Ils contribuent ainsi à réduire les collisions de paquets dans leur voisinage. Dans l'exemple de la Figure 2.2, le prochain saut sera le nœud A.

Most Forwarding progress within Radius (MFR)

Sélectionne le voisin qui permet la plus grande progression positive vers la destination finale [168]. Le nœud avec le plus grand avancement sur la ligne reliant la source et la destination est choisi. La progression est définie comme étant la distance entre le nœud source et la projection de son voisin (voisin du nœud source) sur la ligne reliant ce même nœud source à la destination finale (nœud B dans l'exemple de la Figure 2.2). Cette technique tente de minimiser le nombre de sauts qu'un paquet doit parcourir.

Compass routing

Dans cette stratégie [169], le nœud source ou intermédiaire transmet le paquet au nœud voisin se trouvant dans la direction la plus proche par rapport à la ligne reliant l'émetteur et la destination. Par exemple dans la Figure 2.2, le nœud C est dans la direction la plus proche par rapport à la ligne reliant S et la destination D. Cette stratégie tente de minimiser la distance spatiale parcourue par un paquet.

En plus de ces stratégies de routage en mode *glouton* que nous venons de décrire et qui sont basées sur des métriques géométriques pour déterminer le prochain saut, d'autres stratégies peuvent être définies sur la base d'une combinaison de ces métriques géométriques avec d'autres

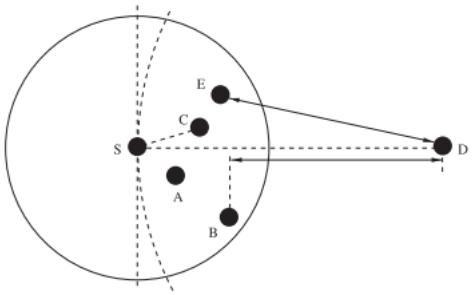


FIGURE 2.2 – Illustration des différentes stratégies de routage géographique en mode *glouton* [7].

critères. Nous citerons par exemple, l'énergie résiduelle des nœuds voisins afin d'étendre la durée de vie du réseau, ou la qualité des liens pour maximiser le taux de livraison de paquets (en Anglais, Packet Delivery Ratio (PDR)) et minimiser le nombre de retransmissions requises.

Cette forme de routage géographique conceptuellement simple, a cependant un inconvénient majeur. En effet, un paquet peut arriver au niveau d'un nœud qui n'a aucun voisin qui pourrait servir de prochain saut pour rapprocher le paquet de la destination. La Figure 2.5(a) montre un exemple où le nœud x est face à ce qu'on appelle un vide de routage, dans la mesure où il est plus proche de la destination *Destination* que ses uniques voisins w et y. Dans ce cas, le paquet est détruit ou une stratégie de recouvrement, tel que le mode *périmètre* décrit dans la section suivante, prend le relais. Une telle situation est appelée *minimum local*, et le nœud où l'acheminement en mode *glouton* s'est arrêté est appelé un nœud *concave*.
En outre, quand elle est exécutée sur un graphe de connectivité réseau modélisé comme un N-UDG, la technique de routage en mode *glouton* souffre des problèmes que nous décrivons dans la Section 2.5.1.

.

2.4.1.3.2 Routage géographique en mode périmètre

Comme on l'a souligné dans la section précédente, ce mode de routage est utilisé comme une stratégie de recouvrement en cas d'échec du mode *glouton*. Le routage en mode *périmètre* est appelé routage par face et il s'exécute sur un sous-graphe planaire [1] tel que le graphe de Gabriel (en Anglais, Gabriel Graph (GG)) [13, 170] ou le graphe Relative Neighborhood Graph (RNG) [13, 171]. Le sous-graphe planaire (GG) est construit à partir du graphe de connectivité réseau initial, comme le décrivent respectivement la Figure 2.3(a) et l'Algorithme 2.1, tandis que la construction du sous-graphe planaire RNG est décrite par la Figure 2.3(b) et l'Algorithme 2.2. Plus formellement, GG et RNG sont définis comme suit. Soit G un graphe noté $G(V, E)$, où V représente l'ensemble des sommets et E représente l'ensemble des arêtes.

1. Le graphe GG du graphe G est noté GG(V,E_g) où :

$$\forall u, v \in V : (u, v) \in E_g \Leftrightarrow \nexists w \in V : d^2(u, w) + d^2(v, w) < d^2(u, v) \tag{2.1}$$

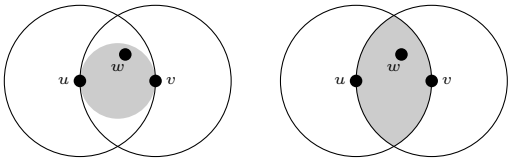
1. Un graphe planaire est un graphe dans lequel il n'y a pas deux arcs qui s'intersectent.

2. Le graphe RNG du graphe G est noté RNG(V,E_{rng}) où :

$$\forall u, v \in V : (u, v) \in E_{rng} \Leftrightarrow \nexists w \in V : max(d(u, w), d(v, w)) \leq d(u, v) \tag{2.2}$$

où : d représente la distance euclidienne entre deux nœuds.

Nous notons qu'il a été montré [171] que le RNG est un sous-ensemble du GG.



(a) L'arête $uv \notin$ GG s'il $\exists$ un témoin w dans le cercle ombré de diamètre uv.

(b) L'arête $uv \notin$ RNG s'il $\exists$ un témoin w dans la "lune" ombrée.

FIGURE 2.3 – Construction des graphes planaires GG et RNG à partir d'un graphe de connectivité réseau modélisé comme un UDG. [13].

Algorithme 2.1 Construction du GG.

Require: $\mathcal{N}(u)$ qui est l'ensemble des voisins du nœud u.
Ensure: Edge (u, v) belongs to GG or not. $\mathcal{N}_g(u)$ est l'ensemble des voisins de u appartenant à son GG.

```
1: while v ∈ N(u) do
2:   while w ∈ N(u) do
3:     if (w = v) then
4:       continue {go to next node}
5:     else
6:       {m is the middle of the segment uv}
7:       if (distance(m,w) < distance(u,m)) then
8:         N_g(u) ← N_g(u) − {v}
9:         break {leave the current loop}
10:      end if
11:    end if
12:  end while
13: end while
```

Le mode *périmètre* consiste à transmettre un paquet à sa destination finale en utilisant la bien connue règle de la main droite [2] [46,172] (voir Figure 2.5(b)). Un paquet est acheminé, dans le sens anti-horaire, le long des faces du sous-graphe planaire qui s'entrecroisent avec la ligne directe entre la source (le nœud où le paquet est entré en mode *périmètre* pour la première fois) et la destination finale (voir Figure 2.4)

2. La règle de la main droite (respectivement de la main gauche) indique que lorsqu'un paquet arrive au nœud x à partir du nœud y, la prochaine arête traversée est la suivante dans le sens contraire (respectivement dans le

Algorithme 2.2 Construction du RNG.

Require: $\mathcal{N}(u)$ qui est l'ensemble des voisins du nœud u.
Ensure: Edge (u, v) belongs to RNG or not. $\mathcal{N}_{rng}(u)$ est l'ensemble des voisins de u appartenant à son RNG.

```
1: while v ∈ N(u) do
2:   while w ∈ N(u) do
3:     if (w = v) then
4:       continue {go to next node}
5:     else
6:       if distance(u,v) > max(distance(u,w),distance(v,w)) then
7:         N_rng(u) ← N_rng(u) − {v}
8:         break {leave the current loop}
9:       end if
10:    end if
11:  end while
12: end while
```

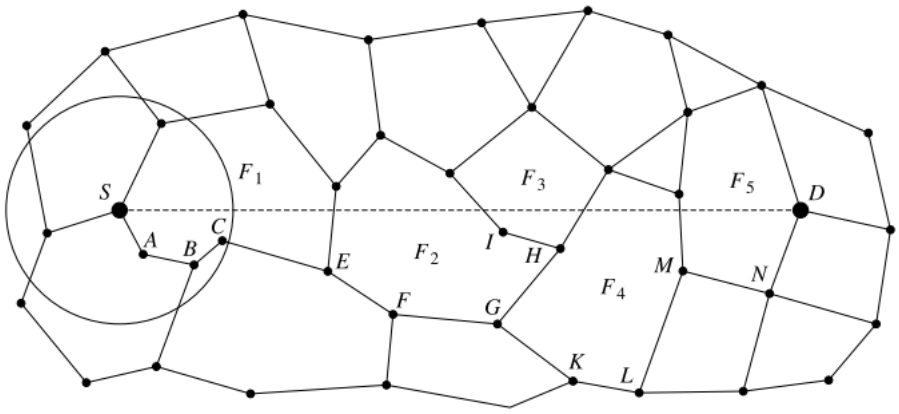


FIGURE 2.4 – Routage en mode *périmètre* (ou par face) d'un paquet depuis le nœud S vers le nœud D (le chemin emprunté est $SABCEFGHIHGKLMND$), en utilisant la règle de la main gauche [8].

Un graphe planaire possède deux types de face, internes et externes. Toutes les faces sont coupées par la ligne directe, (x,D), reliant le nœud où le paquet est entré en mode *périmètre* pour la première fois (appelons-le x) et la destination finale (appelons-la D). La règle de la main droite est appliquée sur chaque face afin d'atteindre un arc qui coupe (x,D). Une fois sur cet arc, l'acheminement se déplace vers la face adjacente coupée par (x,D).
A chaque fois qu'un nœud u doit transmettre un paquet, en utilisant le mode *périmètre*, à un nœud v il vérifie si l'arête (u, v) appartient à son GG (ou RNG) ou non. Si elle en fait partie, le nœud v devient candidat au prochain saut. Ensuite, parmi tous ces nœuds candidats, le prochain saut est choisi en utilisant la règle de la main droite. Si l'arête (u, v) choisie intersecte avec la

même sens) des aiguilles d'une montre, autour de x par rapport à l'arête (x,y)

ligne, entre le nœud où le paquet est entré en mode *périmètre* pour la première fois et le nœud destination, le mode *périmètre* passe à la face suivante du GG (ou RNG) et continue le routage du paquet sur cette face. Le mode *glouton* reprend lorsque le paquet atteint un nœud qui est plus proche de la destination finale que le nœud qui a initié le mode *périmètre*.
Nous notons que le mode *périmètre* souffre quant à lui de l'échec des algorithmes de planarisation, quand il est exécuté sur un graphe de connectivité réseau modélisé comme un N-UDG (voir Section 2.5.2).

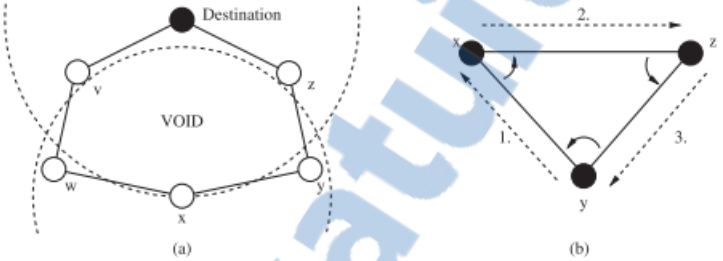


FIGURE 2.5 – Vide de routage et règle de la main droite [7].

2.4.1.3.3 Exemple d'illustration

Dans l'exemple représenté dans la Figure 2.6, on suppose que le nœud $n1$ veut envoyer un paquet au nœud destination finale $n7$. Le paquet est envoyé, en mode *greedy* au nœud $n3$ qui est le plus proche voisin de la destination $n7$. Arrivé au niveau du nœud $n3$, le paquet entre en mode *périmètre*, car ce nœud ($n3$) n'a pas de voisin plus proche que lui même de la destination $n7$. Le prochain saut, en utilisant la règle de la main droite (sens contraire des aiguilles d'une montre, autour de $n3$ par rapport à la ligne directe ($n3$,$n7$) représentée avec ligne discontinue sur la Figure 2.6), est le nœud $n4$. A la réception du paquet, le nœud $n4$ compare la distance euclidienne entre lui et le nœud $n7$, notée d(n_4,n_7), avec la distance entre le nœud où le paquet est entré en mode *périmètre* et le nœud $n7$, notée d($n3$,n_7). Etant donné que d(n_4,n_7) $>$ d($n3$,n_7), le mode *périmètre* continue. Autrement, le paquet aurait retourné en mode *greedy*. Le paquet est alors envoyé en mode *périmètre*, en utilisant la règle de la main droite, au nœud $n6$. Ce dernier compare d(n_6,n_7) et d(n_3,n_7). d(n_6,n_7) est supérieure à d(n_3,n_7), le paquet est envoyé au nœud destination $n7$ en utilisant la règle de la main droite.

2.4.1.3.4 Le protocole Greedy Perimeter Stateless Routing (GPSR)

Greedy Perimeter Stateless Routing (GPSR) est un protocole de routage basé sur la position pour les réseaux sans fil [13]. Il combine un routage en mode *glouton* (*greedy*) sur le graphe de connectivité initial, modélisé en utilisant un UDG, et un routage en mode *périmètre* sur un sous-graphe de connectivité planaire (obtenu à partir de l'UDG initial), pour la livraison de paquets dans un réseau sans fil. Il convient de noter les points suivants en ce qui concerne l'acheminement d'un paquet en utilisant le protocole GPSR :

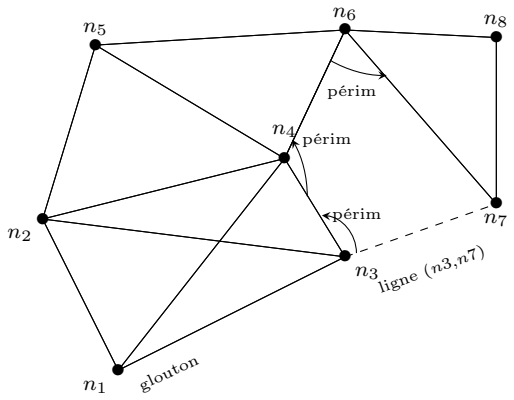


FIGURE 2.6 – Graphe de connectivité réseau

1. Uniquement le nœud source initial qui fixe la destination,
2. Le champ destination reste inchangé tout au long de l'acheminement du paquet,
3. Tous les paquets sont initialement marqués à l'origine comme étant en mode *glouton*.

Le Tableau 2.1 résume les champs d'entête d'un paquet GPSR.

Champ	Rôle
D	Position de la destination
d	Identifiant de la destination
h	Identifiant du saut précédent
L_p	Position du nœud où le paquet est entré en mode *périmètre*
L_f	Position du point partagé entre la face précédente et la nouvelle face, sur la ligne directe, (x_{L_p},D), reliant le nœud de coordonnées L_p au nœud destination d
e_0	Première arête traversée sur la face courante
M	Mode du paquet (*Greedy* ou *périmètre*)

Tableau 2.1 – Les champs d'entête d'un paquet GPSR [13].

Le protocole GPSR fonctionne de la manière suivante. A la réception d'un paquet en mode *glouton*, un nœud cherche dans sa table de voisins le nœud le plus proche de la destination. S'il ne trouve pas, il marque le paquet comme étant en mode *périmètre*. Le paquet sera alors acheminé sur un sous-graphe planaire (GG ou RNG) obtenu à partir du graphe de connectivité réseau initial, selon le mode *périmètre* décrit dans la Section 2.4.1.3.2 ci-dessus. Lors du routage en mode *périmètre*, les actions suivantes sont réalisées :

— Enregistre des coordonnées du nœud au niveau duquel le paquet est entré en mode *périmètre* pour la première fois, dans le champ L_p. cette sauvegarde permet de vérifier, en cours d'acheminement du paquet, si ce dernier peut retourner en mode *glouton*. En effet, quand un nœud reçoit un paquet dont le mode est marqué *périmètre*, il compare la distance entre lui et la destination finale D, notée d_1, et la distance entre le nœud de coordonnées L_p et d, notée d_2. Si $d_1 < d_2$, le paquet retourne en mode *glouton*.

— A chaque fois que GPSR achemine un paquet sur une nouvelle face, il enregistre dans L_f les coordonnées du point partagé sur (x_{L_p},D), entre la face précédente et la nouvelle face.

— GPSR enregistre dans e_0 la première arête (émetteur-récepteur) que le paquet traverse sur la face courante.

Notons enfin que lors de l'utilisation du routage en mode *périmètre* ou par face, deux cas de figures sont à considérer [13].

1. x et D sont connectés. Dans ce cas, GPSR permet d'atteindre la face contenant D et puis la règle de la main droite y mènera le long de cette face.
2. D est non atteignable (déconnectée du graphe). Deux cas sont possibles : le nœud déconnecté se trouve soit à l'intérieur d'une face intérieure, soit à l'extérieur d'une face extérieure. GPSR acheminera un paquet en mode périmètre jusqu'à la face correspondante. En atteignant cette face intérieure ou extérieure, le paquet tournera sans succès autour de la totalité de celle-ci, sans trouver pour autant trouver une arête qui croise (x,D) en un point plus proche de D que L_f. Le paquet va tourner sans succès autour de la face. En traversant e_0 pour le seconde fois, GPSR détecte la répétition et supprime le paquet.

2.4.2 Classification selon le processus de découverte des routes

Les protocoles de routage peuvent également être classés selon le processus de découverte des routes entre les nœuds sources et le nœud destination.

2.4.2.1 Protocoles réactifs

Les protocoles *réactifs* détectent les itinéraires à la demande, c'est-à-dire chaque fois qu'un nœud source souhaite envoyer des données à un nœud destination et qu'aucune route n'a déjà été établie. Il convient de noter que ce processus de découverte entraîne des retards avant que la transmission de données réelle puisse avoir lieu.

2.4.2.2 Protocoles proactifs

Contrairement aux protocoles réactifs, les protocoles de routage *proactifs* établissent des routes au préalable, c.-à-d., avant qu'elles ne soient réellement nécessaires. Ce type de protocole est décrit comme étant piloté par table (en Anglais, table-driven), car les décisions de transfert local sont basées sur le contenu d'une table de routage. Cette dernière contient une liste de destinations associées à un ou plusieurs voisins à 1 saut (du nœud courant) menant à ces destination ainsi que les coûts associés avec chaque prochain saut. Bien que les protocoles pilotés par table éliminent les retards dans la transmission des données dus à la découverte des routes, ils possèdent les désavantages suivants :

— Etablissement de routes qui ne seront jamais empruntées

— Expiration de la validité des routes découvertes. En effet, l'intervalle de temps entre la découverte de la route et son utilisation réelle peut être très important, ce qui peut conduire

à des routes obsolètes. Par exemple, un lien constituant la route peut avoir été rompu entretemps

— Le coût de construction et de maintien de tables de routage potentiellement très importantes

2.4.2.3 Protocoles hybrides

Certains protocoles présentent des caractéristiques de protocoles *réactifs* et *proactifs*. Il sont dits protocoles de routage *hybrides*. Ils utilisent une approche proactive pour connaître le proche voisinage, ce qui leur permet de disposer de chemins immédiats vers les nœuds de cette zone. Les routes vers les nœuds plus lointains sont obtenues en utilisant une approche réactive.

2.4.3 Classification selon la stratégie de routage du protocole

Les protocoles de routage diffèrent également dans leur fonctionnement, c.-à-d., la stratégie de routage du protocole.

2.4.3.1 Protocoles basés sur la négociation entre les nœuds capteurs

Ces protocoles intègrent la négociation entre nœuds capteurs avant de transmettre des données afin de s'assurer que seules des informations non redondantes seront transmises. Des décisions de communication sont également prises en fonction des ressources disponibles au niveau des nœuds capteurs. SPIN [163] est une famille de protocoles de routage conçus pour remédier aux insuffisances de l'inondation (en Anglais, flooding) par la négociation et l'adaptation des ressources. L'objectif de ces deux innovations clés (négociation et adaptation des ressources) intégrées par cette famille de protocoles est de venir à bout des déficiences des protocoles de routage basés sur l'inondation, à savoir l'implosion [17], le chevauchement (en Anglais, overlay) [17] et la non surveillance de l'utilisation des ressources [17]. Pour surmonter les problèmes d'implosion et de chevauchement, les nœuds SPIN négocient entre eux avant de transmettre des données. La négociation permet de s'assurer que seules les informations utiles seront transférées. En outre, dans SPIN, les nœuds interrogent leurs ressources avant la transmission des données. Chaque nœud possède son propre gestionnaire de ressources, qui est consulté par les applications avant de transmettre ou de traiter des données. Par conséquent, les nœuds capteurs peuvent réduire certaines activités lorsque l'énergie est faible, par exemple en étant plus prudent dans la transmission de données tierces.

2.4.3.2 Protocoles basés sur les chemins multiples

La stratégie de routage multi-chemins [173, 174] est une technique prometteuse dans les RCSFs. Le déploiement dense des nœuds dans un RCSF favorise la création de plusieurs chemins à partir des nœuds capteurs sources vers la destination. Les chemins multiples découverts peuvent être utilisés simultanément pour améliorer la fiabilité de transmission de données (p. ex., transmission de plusieurs copies d'un paquet de données original à travers des chemins différents pour assurer l'arrivée à destination d'au moins un paquet) ou pour fournir des ressources

réseau adéquates dans le cas d'un trafic intense, ou alternativement, à savoir le trafic prenant un chemin à la fois. Ce dernier cas, connu sous le nom de routage du chemin alternatif, est principalement utilisé à des fins de tolérance aux pannes (p. ex., en cas de défaillance de nœuds voisins ou de liaisons, un nœud capteur peut bénéficier de la disponibilité de chemins alternatifs pour transmettre ses paquets de données).

2.4.3.3 Protocoles basés sur les requêtes

Dans ce type de routage, les nœuds de destination propagent une requête à travers le réseau afin d'obtenir des données. Le nœud ayant en possession les données qui correspondent à la requête émise, les envoie au nœud initiateur de la requête. Ces requêtes sont décrites dans un langage naturel ou dans des langages de requêtes de haut niveau. Le protocole Directed diffusion [164,165] cité plus haut est un exemple de ce type de routage. Dans les protocoles de routage à diffusion dirigée, tout d'abord, un message d'intérêt est diffusé par le nœud puits, c'est-à-dire propagé par un algorithme d'inondation à travers le réseau. Ceci met en place des gradients qui déterminent le chemin vers l'origine de l'intérêt. Le nœud source, qui a les données demandées, les envoie le long du chemin du gradient de l'intérêt. Pour réduire la consommation d'énergie, les données envoyées par le nœud source peuvent être agrégées par les nœuds capteurs intermédiaires (par exemple, la suppression de doublons) avant d'être redirigées vers la destination.

2.4.3.4 Protocoles basés sur la QoS

L'objectif des protocoles de routage basés sur la QoS est de satisfaire certaines métriques de la QoS (ou une combinaison de plusieurs métriques), comme une faible latence, une faible consommation d'énergie, ou un faible taux de perte de paquets. le protocole Sequential Assignment Routing (SAR) est l'un des premiers protocoles de routage développé pour les RCSFs ayant introduit la notion de QoS dans ses décisions de routage. Il s'agit d'un protocole multi-chemins et piloté par table (en Anglais, table-driven), visant à atteindre l'efficacité énergétique et la tolérance aux pannes [175]. SAR crée plusieurs arbres provenant d'un nœud racine qui est l'un des voisins à un saut du nœud puits, pour établir plusieurs chemins entre chaque nœud et le nœud puits. Ces arbres poussent vers l'extérieur à partir du nœud puits, tout en évitant les nœuds ayant une faible QoS (par exemple, un retard élevé). SAR sélectionne une route pour un paquet sur la base de la métrique QoS, l'énergie (en termes de nombre de paquets qui peuvent être transmis sans épuisement d'énergie, si le nœud a une utilisation exclusive du chemin), et le niveau de priorité du paquet. La disponibilité de plusieurs chemins garantit une tolérance aux pannes et un recouvrement rapide suite à une rupture de chemin. Toutefois, la création et la maintenance des arbres sont des tâches coûteuses, notamment dans les RCSFs de taille assez grande.

SPEED [176] est un protocole géographique avec QoS. Il a été conçu pour gérer la congestion et fournir des services de communication en temps réel (des garanties temps-réel de bout en bout). Il est par conséquent particulièrement adapté à la diffusion de données en temps réel, mais n'inclut aucune autre mesure de QoS dans ses décisions de routage.

Protocole	Caractéristiques
SPIN	Topologie plate, centré-données, basé-requêtes, basé-négociation, basé-cohérence
Directed diffusion	Topologie plate, centré-données, basé-requêtes, basé-négociation, basé-cohérence
Rumour routing	Topologie plate, centré-données, basé-requêtes
DSDV	Topologie plate, proactif
OLSR	Topologie plate, proactif
AODV	Topologie plate, réactif
DSR	Topologie plate, réactif
LANMAR	Hiérarchique, proactif
LEACH	Hiérarchique avec support de la couche MAC
PEGASIS	Hiérarchique
SAFARI	Hiérarchique, hybride
GPSR	Géographique, unicast
GEAR	Géographique, geocast
SPBM	Géographique, multicast
SAR	Topologie plate avec QoS (temps réel, fiabilité), table-driven, multi-chemins
SPEED	Géographique avec QoS (temps-réel)
MMSPEED	Géographique avec QoS (temps-réel, fiabilité)

Tableau 2.2 – Caractéristiques de quelques protocoles de routage [7].

2.4.3.5 Protocoles basés sur la cohérence

Les techniques de routage utilisent différentes techniques de traitement des données [175]. En général, le traitement des différentes données circulant dans le réseau se fait sur la base de la coopération entre les nœuds capteurs. Les protocoles de routage cohérents effectuent seulement une quantité minimale de traitement, qui inclut l'élimination des doublons, avant que les données ne soient envoyées aux destinataires et aux agrégateurs de données. Ces derniers sont des nœuds qui effectuent un traitement ultérieur sur les données. Cependant, dans des protocoles non cohérents, les nœuds peuvent effectuer un traitement local significatif des données brutes avant de les envoyer à d'autres nœuds pour un traitement ultérieur. Pour effectuer un routage économe en énergie, un traitement cohérent est à sélectionner.

2.5 Problématique du routage géographique sur un N-UDG

Un défi de première importance dans les RCSFs est la conception de protocoles de routage basés sur la position, fiables et à efficacité énergétique, sous des conditions radio réalistes. En effet, sous de telles conditions, les portées de transmission radio des nœuds capteurs sont irrégulières (voir Figure 2.7), c.-à-d., la zone qu'un nœud capteur sans fil peut atteindre n'est pas nécessairement un disque. En effet, comme nous l'avons mentionné dans la Section 2.4.1.3 ci-dessus, plusieurs études ont montré que le routage en mode *glouton* et en mode *périmètre*,

les deux stratégies couramment utilisées par les protocoles de routage basés sur la position, ne fonctionnent pas bien sur un graphe de connectivité réseau modélisé comme un graphe de disques non-unitaires (N-UDG). Rappelons que ce dernier est le reflet du phénomène de l'irrégularité de la radio.
les problèmes auxquels font face ces deux stratégies, quand elles sont exécutées sur un N-UDG, sont détaillés ci-dessous.

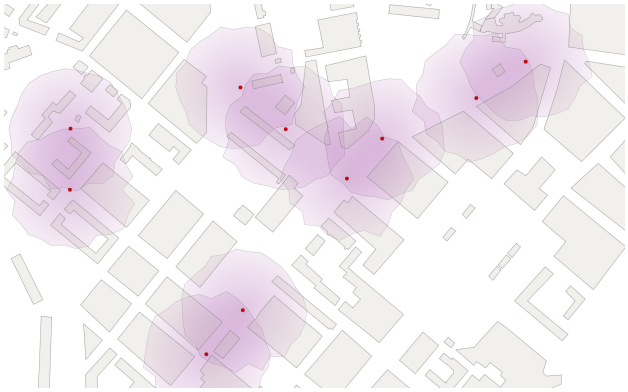


FIGURE 2.7 – Phénomène de l'irrégularité de la radio dans un déploiement réel de RCSFs.

2.5.1 Cas du routage en mode glouton basé sur le nombre de sauts minimal

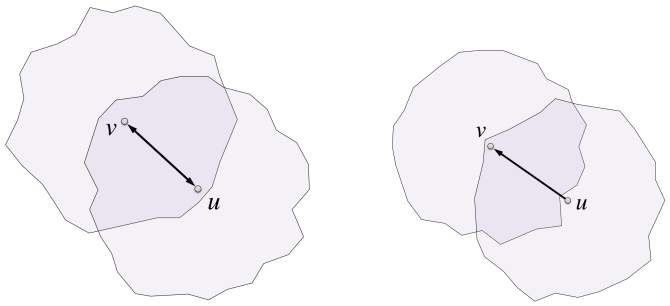
Dans cette section, nous allons revisiter la conception de cette stratégie, à la lumière du phénomène de l'irrégularité de la radio. Rappelons que la stratégie en question est également appelée stratégie d'acheminement à base de distance maximale puisqu'elle maximise la distance parcourue à chaque saut. Elle fonctionne bien dans des conditions de canal sans fil idéales et par conséquent sur un graphe de connectivité réseau sous-jacent modélisé comme un UDG : deux nœuds capteurs u et v dans le réseau sont dans la portée de transmission mutuelle si et seulement si leur distance euclidienne est inférieure à un certain seuil. Dans un tel graphe, tous les liens sont supposés être symétriques et tous les nœuds situés à la même distance de l'émetteur sont supposés recevoir le même signal (la perte de chemin est liée uniquement à la distance entre les nœuds capteurs). Cependant, lorsque les conditions réelles du canal sous-jacent sont prises en compte et que par conséquent le graphe de connectivité réseau résultant est un graphe de disque non-unité (N-UDG), la stratégie de routage en mode *glouton* basée sur la distance maximale souffre des problèmes suivants :

1. La stratégie à sauts minimal consiste à acheminer les paquets à travers de longs liens afin de maximiser la distance parcourue à chaque saut. Un long lien, entre le nœud transmetteur (en Anglais, the forwarding node) et son prochain plus proche voisin de la destination, peut être symétrique comme illustré par la Figure 2.8 (a) mais il peut manifester une atténuation de parcours (en Anglais, path loss) significative due à la distance et à l'irrégularité de la radio. De tels liens non fiables constituant le chemin emprunté par le paquet, depuis le nœud source jusqu'au nœud destination, entraînent une réduction du ratio de livraison des

paquets (PDR) et une perte d'énergie due aux retransmissions. De plus, le delai de bout en bout dans le réseau serait affecté négativement puisque les paquets pourraient atteindre la destination mais après un certain nombre de retransmissions.

2. Le lien entre le nœud transmetteur (en Anglais, the forwarding node) et son prochain plus proche voisin de la destination peut être asymétrique, en raison de l'irrégularité de la radio comme illustré par la Figure 2.8 (b). Par conséquent, le nœud transmetteur ne pourra pas recevoir un acquittement (en Anglais, ACKnowledgment (ACK)) de la part du voisin sélectionné, lui confirmant la bonne réception du paquet. Ne sachant pas si le paquet a été reçu ou pas, la couche MAC du nœud transmetteur retransmettra le paquet un nombre de fois égal au nombre de retransmissions initialement défini. Par conséquent, les liens asymétriques conduisent à une perte d'énergie due aux retransmissions. En outre, ils peuvent aussi entraîner une réduction du PDR et une augmentation du délai de bout en bout dans le cas où ils seraient également peu fiables, c.-à-d., éprouvant une atténuation de parcours importante.

Pour surmonter ces échecs de routage de la stratégie de routage en mode *glouton* à base de la distance maximale parcourue par un paquet à chaque saut, plusieurs propositions on été faites. Une revue de littérature de celles-ci est faite dans la Section 3.2.



(a) Lien symétrique (u peut entendre v et vice versa).

(b) Lien asymétrique dû à l'irrégularité de la radio (u peut entendre v mais pas vice versa).

FIGURE 2.8 – L'irrégularité de la radio donne lieu à des liens asymétriques.

2.5.2 Cas du routage en mode périmètre

Le mode *périmètre* souffre de l'échec des algorithmes de planarisation. Il a été montré qu'en présence du phénomène de l'irrégularité de la radio ou à cause de l'estimation incorrecte de la position des nœuds [9], ces algorithmes produisent un sous-graphe planaire partitionné, planaire avec des liaisons asymétriques ou non planaire, dans lequel des arcs croisés sont toujours présents [9, 41]. Ces trois pathologies conduisent à l'échec du routage en mode *périmètre*. Pour surmonter cet échec de routage sur un N-UDG, plusieurs correctifs ont été proposés tels que le correctif dit du témoin mutuel (en Anglais Mutual Witness (MW)) [9], le Cross-Link Detection

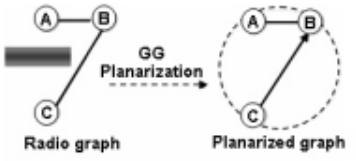
Protocol (CLDP) [56], le Lazy Cross-link Removal (LCR) [45] et Greedy Distributed Spanning Tree Routing (GDSTR) [177].

2.5.2.1 Exemples d'échec de routage en mode périmètre

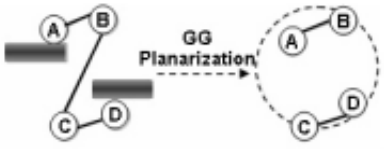
Dans la Figure 2.9(a), on considère que la distance entre C et A est inférieure à la distance entre C et B. Quand le nœud C construit son GG, il conserve l'arc (C,B) en dépit de l'existence du témoin A. Ceci est dû au fait que C et A ne communiquent pas à cause de l'obstacle existant entre eux. Le nœud B quant à lui élimine l'arc (B,C) de son GG, puisqu'il est au courant de l'existence de A (B et A communiquent entre eux). Le résultat est un sous-graphe planaire avec un lien unidirectionnel. Ces liens unidirectionnels peuvent produire une boucle infinie lors du routage en mode *périmètre*.

Dans la Figure 2.9(b), les obstacles empêchent B et D, ainsi que A et C, de communiquer entre eux. La construction du GG de C se traduit par la suppression de l'arc (C,B) à cause du témoin D. De même, la construction du GG de B se traduit par l'élimination de l'arc (B,C) du fait de l'existence du témoin A. Par conséquent, on aboutit à un sous graphe planaire déconnecté.

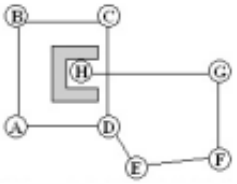
Enfin dans la Figure 2.9(c), nous constatons que les algorithmes de planarisation peuvent laisser des arcs qui se croisent, et ce en présence d'obstacles qui constituent une des causes de l'irrégularité de la radio. En effet, malgré que les liens (H,G) et (C,D) se croisent, ils ne sont pas éliminer lors de la planarisation. Ceci est dû au fait que C et D ne peuvent pas voir H, et H et G ne peuvent pas voir les nœuds C et D.



(a) Sous-graphe planaire avec des liaisons asymétriques.



(b) Sous-graphe planaire partitionné.



(c) Sous-graphe non planaire (présence d'arcs qui s'intersectent).

FIGURE 2.9 – Les trois types d'échec des algorithmes de planarisation en présence du phénomène de l'irrégularité de la radio [9].

2.5.2.2 Algorithme du GG avec le correctif du témoin mutuel

L'algorithme 2.3 illustre l'algorithme de planarisation dit du GG, auquel est appliqué le correctif MW. Le correctif en question indique qu'un nœud u élimine l'arc (u, v) du graphe initial, s'il existe au moins un témoin visible à la fois pour u et v, dans le cercle ombré de diamètre uv, représenté dans la Figure 2.3(a). Notons que le correctif du MW est appliqué de la même façon à l'algorithme de planarisation dit du RNG (le témoin mutuel est à chercher dans la "lune" représentée dans la Figure 2.3(b)).

Algorithme 2.3 Construction du GG en utilisant le correctif MW

Require: $\mathcal{N}(u)$, $\mathcal{N}(v)$ qui sont respectivement les ensembles des voisins des nœuds u et v.
Ensure: Edge (u, v) belongs to the Gabriel Graph of the node u or not. $\mathcal{N}_g(u)$ est l'ensemble des voisins de u appartenant à son GG.

```
1: while v ∈ N(u) do
2:   while w ∈ N(u) do
3:     if (w = v) then
4:       continue {go to next node}
5:     else
6:       {m is the middle of the segment uv}
7:       if ((w ∈ N(u)) ∧ (w ∈ N(v))) then
8:         if (distance(m,w) < distance(m,v)) then
9:           N_g(u) ← N_g(u) − {v}
10:          break {leave the current loop}
11:        end if
12:      end if
13:    end if
14:  end while
15: end while
```

Il convient de noter que l'application du correctif du MW à la planarisation GG n'est pas suffisante pour obtenir un sous-graphe planaire "sûr" [9].

2.6 Conclusion

Dans ce chapitre nous avons présenté un état de l'art sur le routage dans les RCSFs avec une attention particulière pour le routage géographique. Après avoir présenté les défis et les métriques du routage dans ce type de réseaux, nous avons présenté une classification des protocoles de routage. La classe des protocoles géographiques a été largement décrite. Nous avons en effet détaillé le fonctionnement des techniques de routage les plus utilisées par les protocoles de routage géographiques, à savoir l'approche *glouton* et l'approche *périmètre*. Ensuite, nous avons décrit le fonctionnement du protocole GPSR sur lequel est basée notre deuxième contribution. Enfin, nous avons expliqué l'influence de l'irrégularité de la radio sur les deux approches *glouton* et *périmètre* tout en évoquant les solutions permettant un routage correct à l'aide de ces deux approches quand elles sont exécutées sur un N-UDG.

Dans le prochain chapitre, nous abordons notre première contribution qui consiste justement à proposer un protocole de routage en mode *glouton*, inter-couches, appelé Cross-Layer Greedy Routing (CL-GR), permettant un routage correct sur un N-UDG. CL-GR fournit deux stratégies de routage en mode *glouton*, en l'occurrence Progress towards the sink node through Symmetrical links that experience the lowest Path Loss (PSPL), et progress through symmetrical links, combining the Maximum Distance forwarding strategy and the PSPL (MDPSPL). Les résultats de la simulation suggèrent que ce protocole est approprié pour les applications tolérantes et non tolérante au délai, et ce selon la stratégie de routage utilisée, à savoir la PSPL ou la MDPSPL.

Deuxième partie

Contributions

Chapitre 3

Protocole de routage géographique inter-couches pour les RCSFs avec des portées radio irrégulières

3.1 Introduction

Le routage géographique est un paradigme de routage approprié pour les RCSFs [32–34]. Il permet en effet la conception de protocoles efficaces et évolutifs, basés uniquement sur des décisions locales et nécessitant des capacités de stockage minimales. Le routage géographique comprend généralement deux phases :

— Le routage en mode *glouton* (*greedy*) dans lequel les paquets sont envoyés vers un nœud voisin qui les rapprochent de la destination,

— Le mode *périmètre*, invoqué lorsque le routage en mode *glouton* échoue, c.-à-d., le paquet arrive au niveau d'un nœud *concave* (un nœud qui n'a aucun voisin qui pourrait servir de prochain saut pour rapprocher le paquet de la destination). Ce mode de routage utilise la bien connue règle de la main droite [46, 172] et garantit de rapprocher les paquets de la destination si le graphe de connectivité réseau sous-jacent est planaire. Cependant, si le graphe n'est pas planaire, les paquets boucleront dans le réseau même si une route vers la destination existe.

Il a été montré que la stratégie de routage en mode *glouton*, basée sur la distance maximale, qui fonctionne correctement et efficacement sur un graphe de connectivité réseau modélisé comme un graphe de disques unitaires UDG [1](Unit Disk Graph), fonctionne mal lorsqu'elle est exécutée sur un graphe de connectivité réseau modélisé comme un graphe de disques non-unitaires N-UDG (Non Unit Disk Graph) [39,41–47,57]. Nous rappelons qu'un N-UDG reflète en effet le phénomène de l'irrégularité de la radio [30, 31] qui provient de multiples facteurs, tels que l'antenne et le

1. Un graphe de disques unitaires (UDG) reflète la connectivité dans un réseau sans fil, où chaque nœud a le même rayon de transmission R. Une arrête existe entre deux nœuds u et v si et seulement si la distance euclidienne entre eux n'est pas supérieure à une unité fixe R. Dans un tel graphe, un nœud est toujours connecté à tous les nœuds dans sa portée radio "nominale" fixe, et n'est jamais connecté à des nœuds en dehors de cette portée.

type de média, et est accentué par les obstacles (par exemple, les bâtiments, les collines, les montagnes) et les conditions météorologiques. la stratégie de routage en mode *glouton* souffre des problèmes que nous avons détaillés dans la Section 2.5.1 du Chapitre précédent.

Dans ce chapitre, nous présentons tout d'abord une classification des stratégies de routage en mode *glouton* et ce sur la base d'une revue de littérature. Ensuite, nous détaillons notre première contribution qui consiste en un algorithme de routage géographique en mode *glouton*, inter-couches, appelé Cross-Layer Greedy Routing (CL-GR), permettant un routage correct sur un N-UDG. Nous commençons, en effet, par décrire le modèle réseau adopté ainsi que les hypothèses considérées, qui nous ont servis pour mener cette étude. Ensuite, les deux nouvelles stratégies de routage en mode *glouton* fourni par CL-GR, appelées respectivement Progress towards the sink node through Symmetrical links that experience the lowest Path Loss (PSPL), et progress through symmetrical links, combining the Maximum Distance forwarding strategy and the PSPL (MDPSPL), sont largement décrites. Enfin, nous discutons les résultats de simulation obtenus et nous présentons une analyse des coûts de calcul et de communication des deux stratégies proposées.

Nous tenons à souligner que nous avons comparé notre CL-GR à une version améliorée de l'algorithme *greedy* utilisé par le protocole Greedy Perimeter Stateless Routing (GPSR) [13], qui peut être exécutée sur un N-UDG, et que nous appelons E-GR (Enhanced Greedy Routing), et à l'algorithme COP_GARE [54]. Les résultats de la simulation montrent que la PSPL et la MDPSPL permettent un meilleur ratio de livraison des paquets (en Anglais, Packet Delivery Ratio (PDR)) et une meilleure efficacité énergétique par rapport à E-GR et à COP_GARE. En termes de délai de bout en bout, tandis que la stratégie PSPL augmente significativement cette métrique, la stratégie MDPSPL permet un délai de bout en bout satisfaisant, comparativement à E-GR et à COP_GARE.

3.2 Travaux connexes

Les stratégies de routage en mode *glouton* peuvent être classées à priori en deux grandes classes, et ce selon le modèle de propagation radio employé et par conséquent selon le type de graphe de connectivité réseau sur lequel elles s'appuient. La première classe comprend les stratégies de routage en mode *glouton* qui reposent sur des modèles de propagation radio idéalistes tel que le modèle free space [12], et donc sur l'UDG qui en résulte. Une stratégie de routage en mode *glouton* couramment utilisée qui appartient à cette première classe est la technique d'acheminement *glouton* à base de distance maximale [13] où à chaque saut, un paquet est transmis au voisin le plus proche géographiquement de la destination. Cette stratégie tente de minimiser le nombre de sauts en transmettant un paquet à travers des liens longs qui risquent de subir une atténuation de parcours élevée, en raison de la distance et de l'irrégularité de la radio. Afin d'améliorer la performance de la stratégie de transmission de distance maximale, les auteurs de [178] proposent la métrique NADV (Normalized Advance) qui consiste à sélectionner le voisin suivant un compromis entre coût de liaison et proximité avec le nœud puits. Trois types de coûts de liaison sont pris en compte, à savoir le taux d'erreur sur les paquets (en Anglais, Packet Error Rate (PER)), le délai de liaison et la consommation d'énergie. La métrique NADV

repose sur un coût de liaison supposé être une fonction de la distance convexe croissante, ce qui n'est pas précis.

La deuxième classe comprend des stratégies de routage en mode *glouton* qui s'appuient sur des modèles de propagation radio réalistes tel que le modèle log-normal shadowing [12], et donc sur le N-UDG résultant. Dans [57], les auteurs utilisent la métrique ETX (en Anglais, Expected Transmission count metric) dans un vrai banc d'essai de 29 nœuds dotés de la technologie sans fil 802.11b. La métrique ETX, qui intègre les effets des taux de perte de liaison, de l'asymétrie et des interférences, trouve des chemins de haut débit dans les réseaux sans fil multi-sauts. L'ETX est basée sur les rapports de livraison, respectivement les rapports de livraison directe et inverse, d_f et d_r, qui sont prédits en utilisant des paquets *sonde* dédiés (en Anglais, dedicated probe packets) de 134 octets de charge utile. Étant donné que les tailles de paquet de données 802.11 peuvent varier, la métrique ETX peut ne pas prédire avec précision les débits. De plus, les paquets *sonde* génèrent du trafic supplémentaire.
Dans [30], les auteurs proposent un modèle d'irrégularité radio (en Anglais, radio irregularity Model (RIM)) qui améliore les modèles radio isotropes. Il se rapproche de trois propriétés principales des signaux radio, à savoir l'anisotropie, la variation continue et l'hétérogénéité. Les auteurs utilisent RIM pour montrer que l'irrégularité de la radio a un grand impact sur les protocoles de routage ainsi que sur les protocoles MAC. Ils montrent également que le routage basé sur la position est sévèrement affecté par l'irrégularité de la radio, puisqu'il repose sur une technique de découverte de voisins qui fonctionne bien seulement si les liens sont symétriques.
Dans [54], les auteurs proposent des algorithmes de routage en mode *glouton* basés sur une conception inter-couches et destinés à fonctionner dans un environnement réel : Greedy cross-layer position-based routing Algorithms in a REal environment (GARE). La décision de routage de GARE est prise en fonction de l'état du médium. GARE s'appuie sur la même métrique ETX utilisée dans [57], comme mesure de la qualité de la liaison entre deux nœuds capteurs. Les algorithmes GARE utilisent une fonction de pondération qui choisit des liens qui ont un rapport optimal entre la qualité du lien (estimé en utilisant la métrique ETX) et la longueur parcourue en un saut.
Dans [42, 43], les auteurs abordent ce qui est communément appelé le problème du lien le plus faible dans le routage en mode *glouton* à base de la distance maximale (en Anglais, the weakest link problem in maximum distance greedy forwarding), résultant de la présence de liens non fiables dans les déploiements réels des RCSFs. Ils étudient les compromis en matière d'énergie et de fiabilité relatifs au routage basé sur la position par rapport aux liens avec perte, dans les RCSFs. Les performances de plusieurs stratégies de routage sont comparées. Ils trouvent que le produit du taux de réception des paquets (en Anglais, Packet Reception Rate (PRR)) et de la distance parcourue vers la destination (PRR $\times$ d) est une métrique très appropriée pour le routage basé sur la position dans des environnements réalistes. En utilisant cette métrique, le nœud sélectionne le voisin avec le plus grand PRR $\times$ d, pour être le saut suivant. Les auteurs mentionnent que leur étude met l'accent sur des applications telles que la surveillance de l'habitat où l'interférence est presque absente.

D'après le revue de littérature qu'on vient de présenter ci-dessus, nous pouvons déduire que deux autres classifications des stratégies de routage en mode *glouton* peuvent être envisagées,

tel qu'illustré par La Figure 3.1. Il convient aussi de noter que certaines stratégies peuvent être classées dans plus d'une classe tel que le montre le Tableau 3.1.

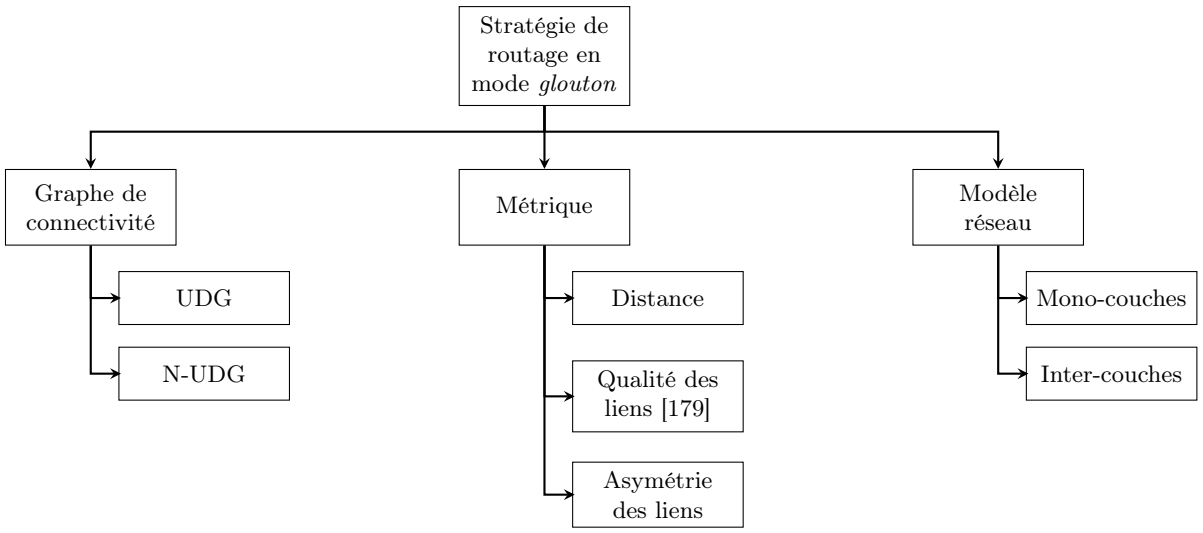


FIGURE 3.1 – Classification des stratégies de routage en mode *glouton*.

Dans ce chapitre, nous proposons un algorithme de routage en mode *glouton*, inter-couches, appelé Cross-Layer Greedy Routing (CL-GR), qui permet un routage géographique correct sur un N-UDG. CL-GR est conçu pour les RCSFs déployés de manière dense et avec un trafic de données assez élevé. Il permet le routage des paquets via des liens symétriques qui subissent la plus faible atténuation de parcours. L'atténuation de parcours qui est un paramètre de la couche PHY, est obtenu par la couche NET lors de la phase de découverte du voisinage et ce grâce à une conception inter-couches basée sur l'interaction de ces deux couches non adjacentes (PHY et NET). Par conséquent, aucun paquet *sonde* supplémentaire n'est utilisé (d'autres solutions proposées utilisent des paquets *sonde* pour prédire le PRR). Les résultats des simulations suggèrent que le CL-GR est à efficacité énergétique, fournit un PDR élevé et convient aux applications à base des RCSFs, tolérantes et non tolérantes au délai (en Anglais, delay and no delay tolerant WSN applications).

3.3 Description du modèle réseau utilisé et hypothèses

Nous considérons un RCSF statique, composé de N nœuds capteurs, et d'un nœud puits riche en ressources, déployés aléatoirement (voir Figure 3.2) pour surveiller une zone sensible clôturée externe (p. ex., champ pétrolier, site nucléaire, aéroport). Chaque nœud est au courant de sa propre position, obtenue par un système de positionnement global (GPS) ou une approche de localisation [38, 69–72]. De plus, la puissance d'émission de tous les nœuds est la même et est constante. Cependant, les portées de transmission des nœuds sont irrégulières en raison des propriétés des dispositifs (par ex., antenne non isotrope) et de la présence d'obstacles (p. ex., bâtiments, collines, montagnes). Par conséquent, les liens peuvent être peu fiables et asymétriques,

Stratégie	**Graphe**		**Métrique**			**Modèle réseau**	
	UDG	N-UDG	Distance	**Lien**		Mono[a]	Inter [b]
				Qualité	Asymétrie		
GPSR [13]	✓		✓			✓	
NADV [178]	✓		✓	✓		✓	
(PRR×d)-based [42, 43]		✓	✓	✓	✓	✓	
GARE [54]		✓	✓	✓	✓		✓
CL-GR [5]		✓	✓	✓	✓		✓

[a] mono-couches.
[b] Inter-couches.

Tableau 3.1 – Caractéristiques de quelques stratégies de routage en mode *glouton*.

et des vides peuvent être présents dans le réseau. Nous rappelons que des vides peuvent également exister en raison du déploiement initial. Dans ce travail, nous supposons qu'un paquet est transmis en utilisant seulement une stratégie de transfert *glouton*, c.-à-d., si un nœud n'a pas de voisin plus proche du nœud puits que lui-même (minimum local) en raison de la présence d'un vide dans le réseau, il détruit le paquet.

Dans cette étude, nous considérons que l'atténuation de parcours est due à la distance Transmetteur-Récepteur (T-R) et aux facteurs d'atténuation. L'atténuation de parcours entre deux nœuds est prédite en utilisant le modèle log-normal shadowing défini par l'Equation (1.7) (Section 1.14.3 du Chapitre 1).

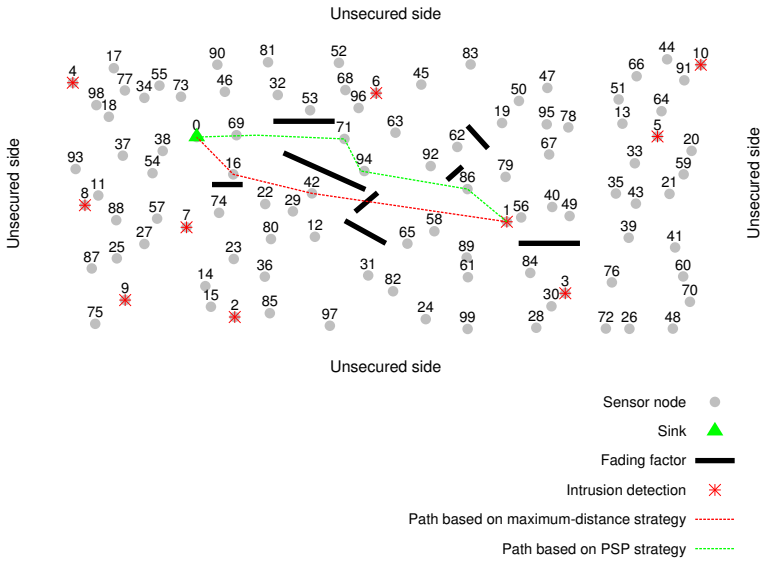


FIGURE 3.2 – Modèle de surveillance basé sur les RCSFs.

Il convient également de noter que nous ne considérons pas la variation temporelle de l'atténuation de parcours.

Champ	Nom
NI	Identifiant du nœud
NP	Position du nœud
NS	Ensemble des voisins=$\{(\text{NGI}_i,\text{PL2}_i(\text{NI} \rightarrow \text{NGI}_i))\}$, i=1..cardinal(N(NI)). NGI_i est l'identifiant du i^{me} voisin (voir Tableau 3.3)
PL	Atténuation de parcours du lien (NI → Récepteur) (C'est un champ partagé, rempli par la couche PHY)

Tableau 3.2 – Structure d'un paquet *hello* diffusé par un nœud NI.

Champ	Nom
NGI	Identifiant du voisin
NGP	Position du voisin
SYM	1 si le lien $(u \rightarrow NGI)$ est symétrique sinon 0
PL1	Atténuation de parcours subie par le lien $u \rightarrow NGI$ (rempli à partir de NS si SYM = 1)
PL2	Atténuation de parcours subie par le lien $NGI \rightarrow u$ (Fourni par la couche PHY via les paquets *hello*)

Tableau 3.3 – Table des voisins d'un nœud u.

Après le déploiement des nœuds capteurs, une étape de découverte de voisinage a lieu. Au cours de cette étape, chaque nœud diffuse périodiquement un paquet *hello* à un saut (3 séries de 3 *hello* par nœud, un nœud à la fois), incluant son identifiant, sa position et l'ensemble de ses voisins (NS) qui contient tous les nœuds que le nœud diffuseur peut entendre, comme le montre la structure d'un paquet *hello* dans le Tableau 3.2. A la réception d'un paquet *Hello*, un nœud remplit sa table de voisins dont la structure est montrée dans le Tableau 3.3, et vérifie si son identifiant appartient à l'ensemble des voisins (NS) inclus dans le paquet *hello* reçu. Si c'est le cas, il marque le lien, entre lui-même et le nœud à partir duquel il reçoit le paquet *hello*, comme étant symétrique (SYM = 1). Sinon, le lien est marqué comme étant asymétrique (SYM = 0). Nous notons que cette technique de détection des liens symétriques est la même que celle utilisée par la solution SGF (Symmetric Geographic Forwarding) [30].

Le graphe de connectivité réel du réseau obtenu à la fin de l'étape de découverte du voisinage est noté $G(V, E)$ où V représente l'ensemble des nœuds et E est l'ensemble des arcs représentant la connectivité entre les nœuds. Un arc (A, B), c.-à-d., $A \rightarrow B$, existe entre les nœuds A et B si et seulement si un paquet envoyé par A peut atteindre B. Nous indiquons l'ensemble des voisins

Champ	Nom
SI	Identifiant du nœud puits
SP	Position du nœud puits
AI	Information d'alerte

Tableau 3.4 – Structure d'un paquet d'alerte p.

d'un nœud u par $N(u)$.

Le processus de surveillance commence immédiatement après la fin de la phase de découverte du voisinage. Ainsi, lorsqu'une intrusion se produit, un paquet d'alerte est généré par le nœud (ou les nœuds) ayant détecté(s) l'intrusion, et transmis vers le nœud puits, à l'aide de CL-GR que nous décrirons dans la prochaine Section. A chaque saut, à la réception du paquet d'alerte, la couche MAC du récepteur, qui utilise un protocole MAC asynchrone basé sur la contention avec un mécanisme de retransmission, envoie un accusé de réception au nœud transmetteur (en Anglais, forwarding node), puis transmet le paquet d'alerte au prochain nœud capteur. Si le nœud transmetteur ne reçoit pas d'accusé de réception (ACK) après un délai d'expiration (temps pris par le paquet d'alerte pour atteindre le récepteur + le temps pris par le paquet ACK pour atteindre l'émetteur), il tente de retransmettre l'alerte. Après un nombre donné de retransmissions initialement défini au niveau de la couche MAC, l'envoi du paquet est abandonné.

3.4 Le protocole de routage géographique inter-couches (CL-GR)

Le protocole CL-GR peut être exécuté sur un UDG ou un N-UDG. Il fournit deux stratégies d'acheminement d'un paquet à sa destination finale, à savoir Progress towards the sink node through Symmetrical links that experience the lowest Path Loss (PSPL) et progress through symmetrical links, combining the Maximum Distance forwarding strategy and the PSPL (MDPSPL). Les deux stratégies en question utilisent une conception inter-couches basée sur une interaction de couches.

3.4.1 La stratégie de routage PSPL

La stratégie PSPL permet au nœud transmetteur d'acheminer un paquet en fonction de trois critères qui sont la progression vers le nœud puits, la symétrie et la fiabilité du lien (lien symétrique avec la plus faible atténuation de parcours), comme indiqué dans l'Algorithme 3.1. Le nœud transmetteur identifie ses voisins qui permettent une progression positive vers le nœud puits, parmi ceux avec lesquels il a un lien symétrique. Ceci est rendu possible grâce aux coordonnées de ses voisins stockées dans sa table de voisinage (voir Tableau 3.3), et les coordonnées de la destination finale incluses dans la structure du paquet d'alerte à transmettre, comme indiqué dans le Tableau 3.4. Ensuite, il sélectionne le voisin avec qui il a le lien qui subit la plus faible atténuation de parcours. Comme représenté dans la Figure 3.3, l'information sur l'atténuation de parcours est fournie par la couche PHY à la couche NET à travers une conception inter-couches basée sur l'interaction de ces deux couches non adjacentes. En effet, à la réception d'un paquet *hello*, la couche PHY met la valeur de l'atténuation de parcours (en dB), entre le nœud qui diffuse le paquet *hello* et le récepteur, dans le champ partagé PL du paquet *hello* reçu. Nous rappelons que l'atténuation de parcours entre deux nœuds est calculée par le module *canal* du simulateur Castalia [107], en utilisant l'Equation 1.7 (Section 1.14.3 du Chapitre 1). Lorsque le *hello* arrive au niveau de la couche NET, le nœud remplit sa table des voisins et vérifie ensuite s'il appartient ou non à l'ensemble des voisins (NS) inclus dans le paquet *hello* reçu. S'il appartient (c.-à-d., le lien entre lui-même et le nœud qui a diffusé le paquet *Hello* est symétrique) alors il remplit

le champ PL1 de sa table des voisins par la valeur contenue dans le champ PL correspondant à l'identifiant de ce voisin dans l'ensemble des voisins NS.

Algorithme 3.1 La stratégie PSPL de CL-GR.

Require: the alert packet p to forward, $N(u)$.
Ensure: next hop v if it exists, otherwise returns -1.

$d \leftarrow \text{distance}^1(u, p.\text{SP})$
$v \leftarrow -1$
$minPathloss \leftarrow$ arbitrary positive high value
while $w \in N(u)$ **do**
  if link(u,w) is symmetrical **then**
    if distance(w, p.SP) $< d$ **then**
      if Pathloss(u, w) $<$ minPathloss **then**
        minPathloss $\leftarrow$ Pathloss(u, w)
        $v \leftarrow w$
      end if
    end if
  end if
end while
return v

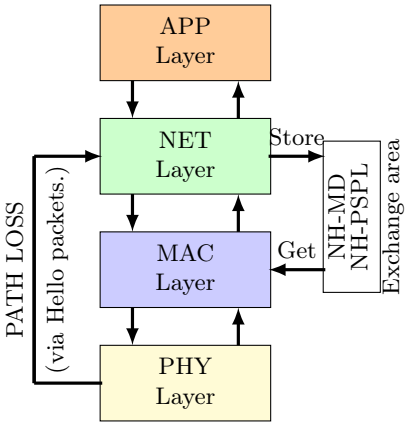


FIGURE 3.3 – Illustration de la conception inter-couches utilisée par le protocole CL-GR.

3.4.2 La stratégie de routage MDPSPL

La stratégie MDPSPL combine deux stratégies pour transmettre un paquet. Elle représente un compromis entre le nombre de sauts et la fiabilité des liens. Elle permet au nœud transmetteur de tenter d'envoyer le paquet à son voisin le plus proche géographiquement de la destination, via un lien symétrique comme indiqué dans l'Algorithme 3.3. Si le nœud transmetteur ne reçoit pas d'accusé de réception (ACK) après un délai d'expiration (temps pris par le paquet d'alerte pour atteindre le destinataire + le temps pris par le paquet ACK pour atteindre l'émetteur),

sa couche MAC retransmet le paquet en utilisant la stratégie PSPL. Ce processus est répété à chaque saut, jusqu'à ce que le paquet d'alerte atteigne sa destination finale. La MDPSPL utilise une conception inter-couches basée sur l'interaction de deux couches adjacentes, à savoir les couches NET et MAC. En effet, la couche MAC exploite les informations de routage sur le prochain saut, déterminées et stockées par la couche NET dans une mémoire d'échange commune, comme représenté sur la Figure 3.3. Le prochain saut NH-MD (Next Hop based on the Maximum Distance metric) est déterminé en utilisant la stratégie de routage en mode *glouton* basée sur la distance maximale, tandis que le prochain saut NH-PSPL (Next Hop based on the PSPL strategy) est déterminé en utilisant la stratégie PSPL, comme décrit dans l'Algorithme 3.2.

Algorithme 3.2 La stratégie MDPSPL de CL-GR.

Require: the alert packet p to forward, $N(u)$.
Ensure: next hops NH-MD and NH-PSPL if they exist, otherwise returns $-1, -1$.

```
d ← distance(u, p.SP)
v ← −1
minPathloss ← arbitrary positive high value
while w ∈ N(u) do
  if link(u,w) is symmetrical then
    if distance(w, p.SP) < d then
      d ← distance(w, p.SP))
      NH-MD ← w
    end if
    if distance(w, p.SP) < distance(u, p.SP) then
      if Pathloss(u, w) < minPathloss then
        minPathloss ← Pathloss(u, w)
        NH-PSPL ← w
      end if
    end if
  end if
end while
return NH-MD, NH-PSPL
```

Algorithme 3.3 Le processus de transmission au niveau de la couche MAC.

```
if Forwarding_strategy = MDPSPL then
  if (it is the first Transmission of the alert packet p) then
    Send p to next hop NH_MD
  else {(it is a retransmission of the alert packet p)}
    Send p to next hop NH_PSPL
  end if
else {(Forwarding_strategy = PSPL)}
  Send p to next hop NH_PSPL
end if
```

3.4.3 Exemple d'illustration

La Figure 3.2 montre deux chemins de routage, à travers des liens symétriques uniquement, d'un paquet d'alerte généré par le nœud source 1. La ligne rouge pointillée ($1 \rightarrow 42 \rightarrow 16 \rightarrow 0$) indique le chemin suivi par le paquet d'alerte, en utilisant la stratégie de routage en mode *glouton* à distance maximale, comme décrit par l'Algorithme 3.4. Le nœud 1 transmet le paquet au nœud 42 qui est son voisin le plus proche géographiquement de la destination. Cependant, le lien $1 \rightarrow 42$ subit une atténuation de parcours élevée due à la présence d'un facteur d'affaiblissement du signal (obstacle), comme indiqué dans la Figure 3.2. Ainsi, deux cas peuvent se produire comme indiqué précédemment dans la Section 2.5.1 (lien symétrique avec une atténuation de parcours significative). Le paquet sera perdu ou atteindra le nœud 42 après un certain nombre de retransmissions. Le premier cas conduit à une réduction du PDR et à un gaspillage d'énergie, tandis que le second cas augmente à la fois la consommation d'énergie et le délai de bout en bout.
D'autre part, la ligne verte pointillée ($1 \rightarrow 86 \rightarrow 94 \rightarrow 71 \rightarrow 69 \rightarrow 0$) indique le chemin suivi par le même paquet d'alerte, en utilisant la stratégie PSPL. Comme cela est illustré dans la Figure 3.2, le paquet d'alerte parcourt des liens qui permettent une progression positive vers le nœud puits et qui sont fiables. Par exemple, les liens tels que $86 \rightarrow 92$ et $71 \rightarrow 53$ ne sont pas utilisés dans le chemin emprunté, au profit des liens $86 \rightarrow 94$ et $71 \rightarrow 69$, respectivement. En effet, bien que les liens $86 \rightarrow 92$ et $71 \rightarrow 53$ soient respectivement plus courts que les liens $86 \rightarrow 94$ et $71 \rightarrow 69$, ils subissent une atténuation de parcours élevée due à la présence de facteurs d'affaiblissement du signal (obstacles), comme illustré dans la Figure 3.2.

3.5 Description de l'algorithme Enhanced Greedy Routing (E-GR)

Nous avons implémenté une version améliorée de l'algorithme de routage en mode *glouton* utilisé par GPSR, que nous appelons Enhanced Greedy routing (E-GR), afin de la comparer à notre algorithme CL-GR. Premièrement, nous avons ajouté un mécanisme permettant à chaque nœud d'identifier ses voisins avec lesquels il a des liens symétriques, comme expliqué dans la Section 3.3. Ensuite, nous avons modifié l'algorithme de routage en mode *glouton* original afin de permettre à un nœud de transmettre un paquet uniquement via des liens symétriques, comme décrit par l'Algorithme 3.4. L'E-GR peut alors être exécuté sur un N-UDG et par conséquent on peut comparer ses performances à celles du protocole CL-GR.

3.6 Evaluation des performances

Nous évaluons notre protocole CL-GR à travers des séries de simulations (50 simulations pour chaque scénario), sous le simulateur Castalia [107] basé sur la plate-forme OMNeT++ [102]. Nous employons cinq métriques, à savoir le PDR (Packet Delivery Ratio), délai moyen de bout en bout, nombre de sauts moyen, nombre total de retransmissions et l'énergie totale consommée dans le réseau, pour comparer les performances du CL-GR à celles de l'algorithme de routage en mode

Algorithme 3.4 E-GR.

Require: p, $N(u)$.
Ensure: next hop v if it exists, otherwise returns -1.

```
1: d ← distance(u, p.SP)
2: v ← −1
3: while w ∈ N(u) do
4:    if link(u,w) is symmetrical then
5:       if distance(w, p.SP) < d then
6:          d ← distance(w, p.SP))
7:          v ← w
8:       end if
9:    end if
10: end while
11: return v
```

glouton, appelé Enhanced Greedy Routing algorithm (E-GR) (voir Section 3.5), et à celles de l'algorithme COP_GARE [54].

Tous les résultats discutés ci-dessous représentent, pour chaque scénario, la moyenne des résultats des 50 simulations réalisées. L'interférence est gérée selon le modèle de gestion des interférences, implémenté dans le simulateur Castalia. Le modèle en question est basé sur la métrique SINR (Signal to Interférence plus Noise Ratio). En effet, lorsqu'un nœud reçoit plusieurs signaux émanant de plusieurs nœuds sources, il accepte celui avec le SINR le plus élevé. Le Tableau 3.5 résume les paramètres les plus importants de la simulation, le Tableau 3.6 détaille le modèle énergétique utilisé pour calculer la consommation d'énergie et le Tableau 3.7 montre la charge utile moyenne des paquets *hello* échangés lors de la simulation, en fonction de la taille du réseau (en nombre de nœuds). La charge utile du paquet *sonde* (en Anglais, probe packet) utilisée par l'algorithme COP_GARE pour déterminer la qualité de la liaison, est constante et est égale à 134 octets, comme il est mentionné dans le Tableau 3.5.

3.6.1 Définition des métriques de performance utilisées

1. PDR (Packet Delivery Ratio) : Représente le rapport entre le nombre d'alertes reçues par le nœud puits, et le nombre d'alertes envoyées par les sources d'alerte.
2. Nombre moyen de sauts : Représente le nombre total de sauts parcourus par les alertes reçues par le nœud puits sur le nombre total d'alertes reçues par celui-ci.
3. Nombre total de retransmissions : Représente le nombre total de retransmissions pendant la durée de la simulation.
4. Délai moyen de bout en bout : Représente le temps moyen écoulé entre l'envoi d'une alerte par une source d'alerte et le temps d'arrivée de cette alerte au niveau du nœud puits. Il est défini par le rapport entre le temps de transmission du nombre total d'alertes reçues par le nœud puits et ce même nombre total d'alertes reçues par celui-ci.

Paramètre	Valeur
Durée de la simulation	Selon le nombre de nœuds déployé et le nombre de séries de paquets *sonde*/*hello*
Nombre de simulations par scénario	50
Zone de déploiement	80 m × 80 m
Nombre de nœuds	Allant de 50 à 300, par pas de 50
Nombre de sources d'alerte	Allant de 5 à 35, par pas de 5
Déploiement	Aléatoire
Charge utile d'un paquet d'alerte	20 Octets
Charge utile d'un paquet *hello*	(12 + une taille variable) Octets
Charge utile d'un paquet *sonde* (COP_GARE)	134 Octets
Nombre Paquets *hello*	3 séries de 3 paquets,
envoyé par chaque nœud	Un nœud à la fois
Nombre de paquets *sonde*	8 séries de 10 paquets ,
envoyé par chaque nœud	Un nœud à la fois
Nombre de nœud puits	1
Radio	CC2420
Débit	250 kbps
Sensibilité radio	-95 dBm
Puissance d'émission	0 dBm
Modèle de propagation radio	Log-normal shadowing
n	2.4
σ	4.0 dB
Capacité de la batterie d'un nœud	18720 Joules
Consommation d'énergie	TX : 57.42 milliWatt RX : 62 milliWatt
Protocole Réseau	CL-GR, E-GR(GPSR), COP_GARE
Protocole MAC	Similaire au protocole X-MAC [134]
Nombre de retransmissions	1
Cycle d'activité	1
Gestion de l'interférence	Oui

Tableau 3.5 – Paramètres de simulation.

	TX(milliJoule)	RX(milliJoule)
Paquet *hello*	t_1(ms) × 57.42(mW)	t_1(ms) × 62(mW)
Paquet de donnée	t_2(ms) × 57.42(mW)	t_2(ms) × 62(mW)
Paquet ACK	t_3(ms) × 57.42(mW)	t_3(ms) × 62(mW)

Tableau 3.6 – Modèle énergétique utilisé.

5. Energie totale consommée dans le réseau : Représente l'énergie totale consommée dans le réseau, pendant la durée de la simulation, calculée selon le Tableau 3.6.

Nombre de nœuds	**Taille *hello*[a]**		
	Min.	Max.	Moyenne
50	36.1072	61.0952	52.4104
100	59.8256	108.0156	91.399733
150	83.17147	153.86	129.550725
200	106.1154	198.7648	166.967
250	127.70544	241.1856	202.278826
300	149.68693	284.0556	238.030281

[a] Octets.

Tableau 3.7 – Charge utile d'un paquet *hello* en fonction du nombre de nœuds dans le réseau.

3.6.2 Analyse des résultats

3.6.2.1 Effet de la variation du nombre de nœuds capteurs

La Figure 3.4 met en évidence le PDR en fonction de la variation du nombre de nœuds capteurs. Les résultats montrent que la MDPSPL obtient de meilleurs résultats que E-GR et COP_GARE. La PSPL améliore en moyenne, les scores réalisés par COP_GARE et E-GR, de 1.57% et 10.30%, respectivement. Ceci est dû au fait que la PSPL n'utilise que des liens fiables, c.-à-d., des liens avec la plus faible atténuation de parcours, tandis que E-GR et COP_GARE choisissent respectivement, des liens longue distance, et des liens avec un compromis entre la qualité de la liaison et la progression vers le nœud puits. Dans ce dernier cas, le nœud courant u, utilisant COP_GARE, sélectionne le voisin v qui minimise le rapport ETX (uv) sur la progression vers le nœud puits. Ainsi, dans les deux cas, des liens non fiables et moins fiables peuvent être utilisés pour transférer les paquets vers la destination finale. Il convient de noter que de tels liens peuvent parfois être le seul moyen d'atteindre certains nœuds et par conséquent la destination finale, comme nous pouvons le constater à travers les valeurs des PDR obtenues par respectivement la PSPL, E-GR et COP_GARE, quand le réseau est de faible densité (50 nœuds capteurs)

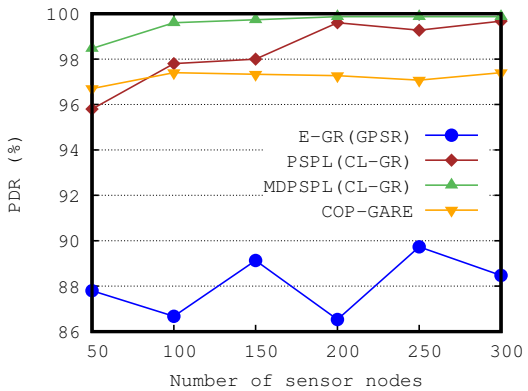


FIGURE 3.4 – PDR en fonction du nombre de nœuds capteurs (nombre de sources d'alerte = 30).

La MDPSPL surpasse la PSPL, et par conséquent les deux autres. Elle est en moyenne 1.30%, 2.50% et 11.6% plus efficace que la PSPL, COP_GARE et E-GR, respectivement. La raison est que la MDPSPL combine le routage en mode *glouton* basé sur la distance maximale et la PSPL, et par conséquent, les destinations qui ne sont pas accessibles en utilisant la première stratégie peuvent l'être en utilisant la seconde stratégie et vice versa.

Enfin, nous notons que le PDR obtenu par la PSPL et la MDPSPL croît lorsque le nombre de nœuds de capteurs croît. Cela peut être expliqué comme suit. Lorsque le réseau devient dense, les nœuds sont plus proches les uns des autres et par conséquent les liens sont plus fiables (la PSPL choisit des liens courts plus fiables). Quant à COP_GARE et E-GR, la variation est probablement due à l'augmentation du degré des nœuds, c.-à-d., que $\mathrm{N}(u)$ devient plus important et donc un nœud u a beaucoup plus de voisins candidats pour le prochain saut. Les nouveaux candidats pour le prochain saut peuvent être un facteur d'augmentation ou de diminution du PDR.

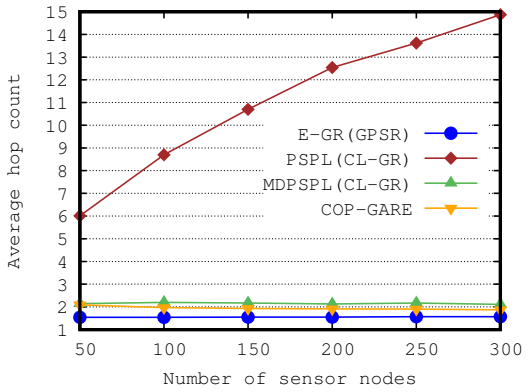


FIGURE 3.5 – Nombre moyen de sauts parcourus par un paquet d'alerte en fonction du nombre de nœuds capteurs (nombre de sources d'alerte = 30).

Comme nous pouvons le déduire de la Figure 3.5, étant donné qu'E-GR achemine les paquets par l'intermédiaire de liens longue distance, il minimise le nombre moyen de sauts parcourus par un paquet. Inversement, PSPL maximise cette même métrique (le nombre moyen de sauts parcourus), puisqu'elle achemine les paquets à travers des liens fiables qui sont généralement courts. Quant à MDPSPL et COP_GARE, ils génèrent presque le même nombre moyen de sauts, qui est significativement inférieur à celui généré par PSPL et légèrement supérieur à celui généré par E-GR. Cela peut être expliqué comme suit. MDPSPL essaie d'abord d'acheminer les paquets en utilisant la stratégie en mode *glouton* basée sur la distance maximale, puis, si le premier essai échoue, elle utilise la stratégie PSPL. COP_GARE favorise les voisins plus près de la destination, c.-à-d., qui permettent de réduire le nombre moyen de sauts parcourus, et avec la meilleure qualité de lien.

En outre, l'augmentation du nombre de nœuds capteurs entraîne une augmentation du nombre moyen de sauts (de 6 à 15) générés par la PSPL. Ceci peut s'expliquer par le fait que lorsque la densité du réseau augmente, les nœuds capteurs sont plus proches les uns des autres, et par conséquent les liens deviennent plus courts (donc plus fiables). D'autre part, l'augmentation

du nombre de nœuds capteurs n'a pas d'impact significatif sur le nombre moyen de sauts générés par les stratégies COP_GARE, E-GR et MDPSPL. En effet, le nombre moyen de sauts générés par ces trois stratégies reste quasi constant. La raison est que E-GR et MDPSPL continuent à sélectionner les liaisons longue distance, indépendamment de la densité de nœuds, respectivement à chaque transmission (E-GR) et au premier essai de chaque transmission (MDPSPL). COP_GARE continue de favoriser les voisins plus près de la destination, comme indiqué précédemment.

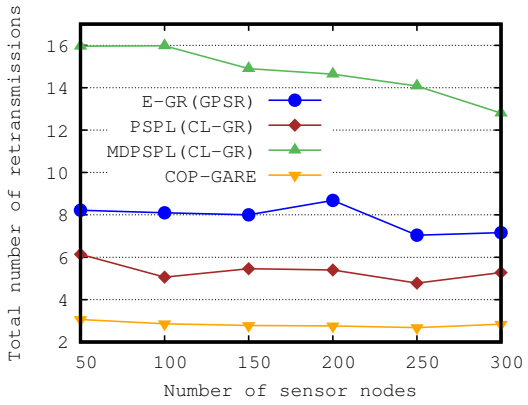


FIGURE 3.6 – Nombre total de retransmissions dans le réseau en fonction du nombre de nœuds capteurs (nombre de sources d'alerte = 30).

Comme le montre la Figure 3.6, le nombre total de retransmissions générées par COP_GARE est le plus bas, indépendamment de la densité de nœuds, et ce comparativement à PSPL, MDPSPL et E-GR. La raison est que COP_GARE est basé sur la métrique ETX qui minimise le nombre total attendu de transmissions de paquets (y compris les retransmissions).

En outre, la PSPL fonctionne mieux que E-GR et MDPSPL. Cela peut être expliqué comme suit. La PSPL achemine les paquets uniquement via les liens qui subissent la plus faible atténuation de parcours. Par conséquent, les signaux sont assez puissants pour atteindre leurs destinations sans retransmission. Ainsi, le mécanisme de retransmission, utilisé à chaque saut, sera beaucoup plus utilisé dans le cas de collisions, dues au phénomène du terminal caché ou du terminal exposé, que dans d'autres cas tels que l'affaiblissement du signal ou l'interférence. Ce raisonnement est confirmé par le nombre total de retransmissions générées par E-GR qui transmet les paquets via des liaisons longue distance, généralement non fiables, c.-à-d., des liaisons qui subissent une atténuation de parcours élevée due à divers facteurs d'affaiblissement du signal. Par conséquent, les paquets peuvent atteindre leur destination mais après des retransmissions, comme en témoigne la Figure 3.6.

En ce qui concerne le nombre total de retransmissions effectuées par la MDPSPL, il indique dans notre cas le nombre total d'échecs de la première tentative en utilisant la stratégie d'acheminement en mode *glouton* basée sur la distance maximale. En effet, nous n'avons considéré qu'une seule retransmission, comme mentionné dans le Tableau 3.5. Ainsi, étant donné que la MDPSPL permet un PDR plus élevé que l'E-GR, le nombre total de retransmissions générées par la MDPSPL est évidemment plus élevé que le nombre total de retransmissions générées par

E-GR.

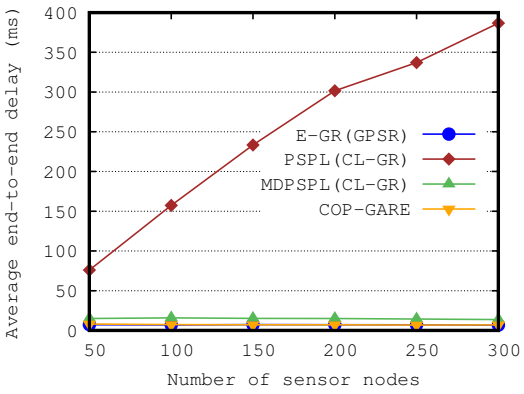


FIGURE 3.7 – Délai moyen de bout en bout en fonction du nombre de nœuds capteurs (nombre de sources d'alerte = 30).

La Figure 3.7 représente le délai moyen de bout en bout généré par les quatre stratégies. Comme nous pouvons le constater, la stratégie PSPL génère la latence la plus élevée puisqu'elle augmente le nombre de sauts parcourus par une alerte, comme nous l'avons indiqué précédemment. Inversement, COP_GARE et E-GR génèrent le délai de bout en bout le plus bas puisqu'ils minimisent, tous les deux, le nombre de sauts.

La MDPSPL génère un délai de bout en bout légèrement supérieur à COP_ GARE et E-GR, car elle combine la stratégie de routage basée sur la distance maximale et la PSPL. La MDPSPL qui est un compromis entre le nombre de sauts et la fiabilité des liaisons (sans favoriser les voisins plus proches de la destination), réduit significativement le délai de bout en bout par rapport à la stratégie PSPL. Elle génère un délai d'attente satisfaisant par rapport à celui généré par COP_GARE et E-GR. Par conséquent, contrairement à la PSPL, la stratégie MDPSPL peut être considérée comme un sérieux candidat pour le routage en mode *glouton* dans les applications non tolérantes au délai.

D'un autre côté, nous pouvons observer que le délai de bout en bout se comporte de la même manière que le nombre de sauts lorsque le nombre de nœuds déployés augmente.

On peut déduire de la Figure 3.8 que malgré le fait que les PDR obtenus par la PSPL et la MDPSPL soient supérieurs à celui obtenu par E-GR, il n'y a pas de différence significative en termes d'énergie totale consommée dans le réseau, entre ces trois stratégies. La principale raison est que la PSPL réduit le nombre total de retransmissions dans le réseau par rapport à E-GR, tandis que la MDPSPL diminue le nombre de sauts, comme indiqué précédemment. Une autre raison est que le routage, en utilisant E-GR, peut échouer au milieu du chemin ou peut être à un saut du nœud puits, ce qui conduit à un gaspillage d'énergie inutile.
E-GR a un meilleur rendement énergétique par rapport à la PSPL et la MDPSPL. Il économise en moyenne 210 et 16 Joules par rapport à ces deux stratégies, respectivement, comme le montre la Figure 3.9. La MDPSPL économise en moyenne 193 Joules par rapport à la PSPL.

COP_GARE induit la consommation d'énergie totale la plus élevée dans le réseau, car il utilise des paquets *sonde* pour déterminer les valeurs ETX des liens. Il consomme en moyenne

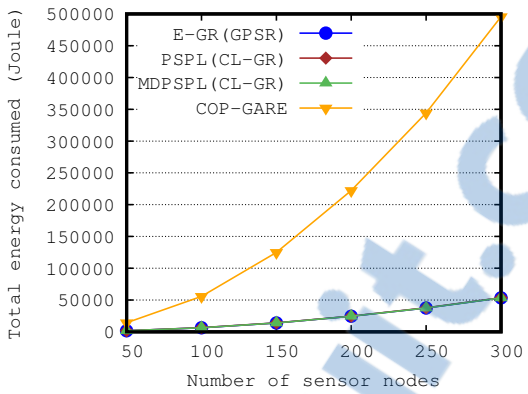


FIGURE 3.8 – Energie totale consommée dans le réseau en fonction du nombre de nœuds capteurs (nombre de sources d'alerte = 30).

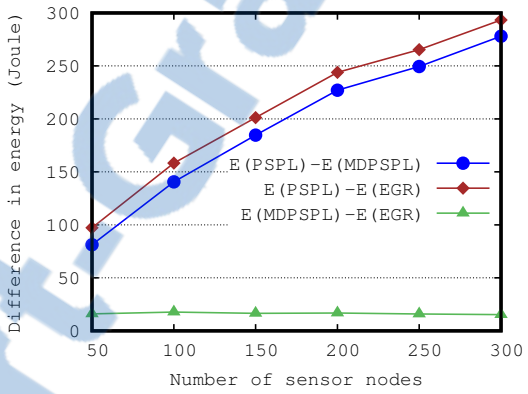


FIGURE 3.9 – Différence de consommation d'énergie dans le réseau en fonction du nombre de nœuds capteurs (nombre de sources d'alerte = 30).

186405 Joules de plus que la PSPL. Nous rappelons que nous avons défini les nœuds pour qu'ils transmettent 8 séries de 10 paquets *sonde*, pour déterminer l'ETX des liens, alors que nous les avons paramétrés pour qu'ils transmettent seulement 3 séries de 3 paquets *hello*, pendant la découverte de voisinage.

Enfin, nous notons que la consommation d'énergie augmente quand que le nombre de nœuds capteurs dans le réseau augmente.

Ces résultats concernant l'efficacité énergétique du protocole CL-GR sont très importants, car ils suggèrent qu'un paquet peut être acheminé de manière fiable avec un coût énergétique inférieur à celui permis par d'autres schémas de routage non fiables tel que E-GR, ou des schémas de routage fiables (par Ex., COP_GARE) mais consommant plus d'énergie. Par conséquent, le CL-GR convient aux applications de surveillance qui ont deux exigences principales : une faible consommation d'énergie pour prolonger la durée de vie du réseau et une livraison fiable des paquets. Ce sont les applications auxquelles nous nous intéressons dans cette thèse.

3.6.2.2 Effet de la variation du nombre de sources d'alerte

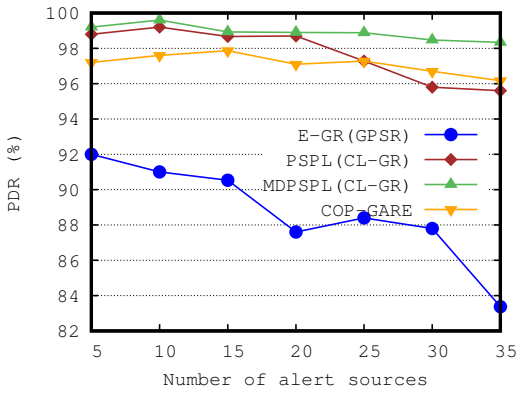


FIGURE 3.10 – PDR en fonction du nombre de sources d'alerte (nombre de nœuds capteurs = 50).

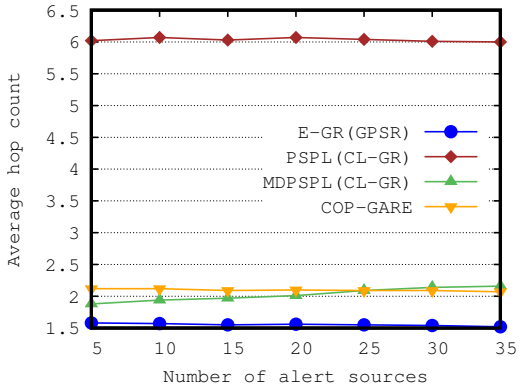


FIGURE 3.11 – Nombre moyen de sauts parcourus par un paquet d'alerte en fonction du nombre de sources d'alerte (nombre de nœuds capteurs = 50).

Comme représenté dans la Figure 3.10, le PDR obtenu par E-GR diminue rapidement (de 92% à 83.37 %), lorsque le nombre de sources d'alerte augmente. Ceci est dû au fait que l'E-GR achemine les paquets via des liaisons longue distance qui peuvent être très peu fiables, c.-à-d., des liaisons qui subissent une atténuation de parcours élevée. Par conséquent, les signaux ne résistent pas à l'interférence élevée due à l'augmentation des envois simultanés.

Inversement, le PDR obtenu par PSPL, MDPSPL et COP_GARE diminue lentement et ne descend pas en dessous de 95.8%, 98.34% et 96.17 %, respectivement. La raison est que les trois stratégies choisissent des liaisons fiables qui résistent mieux aux interférences. De plus, la métrique ETX utilisée par COP_GARE tient compte de l'interférence entre les sauts successifs des routes multi-sauts.

Le COP_GARE fonctionne mieux que la PSPL lorsque l'interférence augmente (à partir de 25 sources d'alerte, comme illustré par la Figure 3.10). Ceci peut s'expliquer par le fait que

COP_GARE tient compte de l'interférence entre sauts successifs, comme indiqué précédemment. D'autre part, la PSPL augmente le nombre de sauts et par conséquent, elle augmente le risque d'interférence.

La MDPSPL surclasse les trois autres stratégies, quelle que soit la densité de nœuds. MDPSPL obtient en moyenne 1.77% de meilleurs résultats que COP_GARE. C'est un résultat très intéressant car dans les applications de surveillance, il peut arriver que plusieurs intrus tentent en même temps de traverser la zone sécurisée (voir Figure 3.2), à partir de différents endroits. Ainsi, plusieurs alertes seront générées et envoyées simultanément vers le nœud puits. Dans ce cas, la MDPSPL, comme suggéré par les résultats de simulation, sera en mesure d'acheminer les alertes de manière fiable vers le nœud puits. Ceci est d'une importance primordiale dans le processus de surveillance d'une zone sensible car cela permet au système de décision à distance de réagir à presque toutes les alertes et à temps.

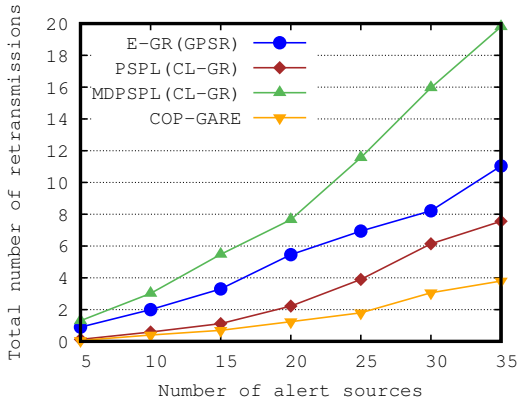


FIGURE 3.12 – Nombre total de retransmissions dans le réseau en fonction du nombre de sources d'alerte (nombre de nœuds capteurs = 50).

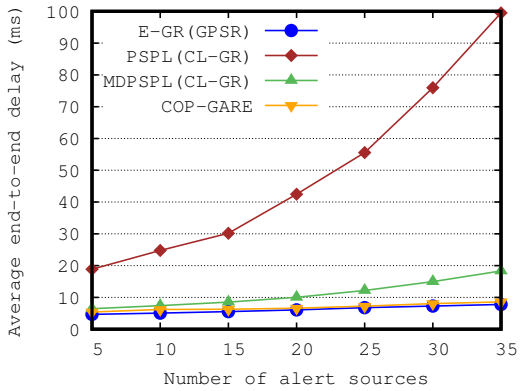


FIGURE 3.13 – Délai moyen de bout en bout en fonction du nombre de sources d'alerte (nombre de nœuds capteurs = 50).

Les Figures 3.11, 3.12, 3.13 et 3.14 représentent respectivement les résultats des quatre autres métriques considérées dans cette étude, à savoir le nombre moyen de sauts, le nombre total de re-

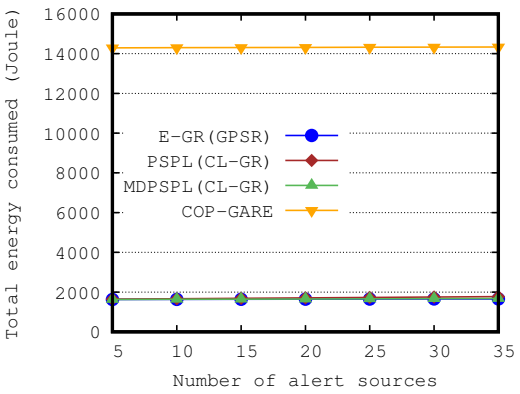


FIGURE 3.14 – Energie totale consommée dans le réseau en fonction du nombre de sources d'alerte (nombre de nœuds capteurs = 50).

transmissions, le délai de bout en bout et l'énergie totale consommée. Comme on peut le constater sur la Figure 3.12, le nombre total de retransmissions augmente en fonction de l'augmentation du nombre de sources d'alerte. Ceci est dû à la croissance de l'interférence résultant de l'augmentation des transmissions simultanées. Par conséquent, le délai de bout en bout (Figure 3.13) augmente quelle que soit la stratégie utilisée, conformément à ce qui a été dit précédemment sur cette métrique lorsque nous avons varié le nombre de nœuds capteurs.
D'autre part, le nombre moyen de sauts générés par chaque stratégie varie selon l'emplacement des sources d'alerte par rapport au nœud puits (voir Figure 3.11).
En ce qui concerne l'énergie totale consommée dans le réseau, les résultats de la simulation sont conforme à ce que nous avons dit sur le comportement de cette métrique, quand nous avons étudier l'effet de la variation du nombre de nœuds capteurs dans la Section 3.6.2.1.

Enfin, comme nous pouvons le déduire, les résultats de la simulation montrent clairement que la MDPSPL est adaptée à un environnement fortement interféré.

3.6.2.3 Effet de la variation de la taille du paquet d'alerte sur le PDR

La Figure 3.15 montre que MDPSPL et PSPL surpassent COP_GARE et E-GR. La raison est que l'une des sources d'erreur lors de l'estimation de l'ETX est la différence entre la taille des paquets *sonde* et les paquets de données. Nous rappelons que COP_ GARE utilise la métrique ETX pour déterminer la qualité des liens. D'autre part, les paquets sont transmis par des liens avec perte, lorsque E-GR est utilisé, ce qui justifie sa performance.

3.6.3 Analyse des coûts

3.6.3.1 Coûts de calcul

Le Tableau 3.8 résume les coûts de calcul des quatre stratégies de routages. En raison de la boucle *while* dans respectivement la ligne 4 de l'Algorithme 3.1, la ligne 4 de l'Algorithme 3.2 et la ligne 3 de l'Algorithme 3.4, la complexité temporelle de PSPL, MDPSPL et E-GR, est

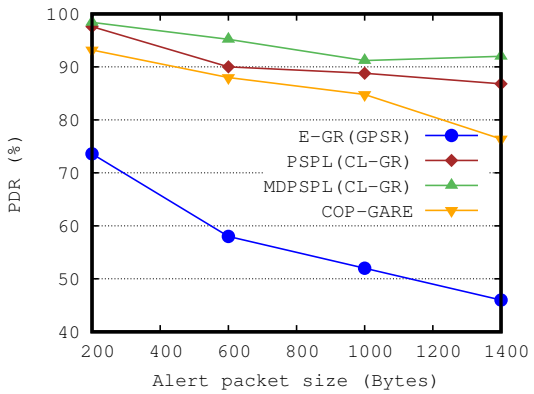


FIGURE 3.15 – PDR en fonction de la taille du paquet d'alerte (nombre de nœuds capteurs = 50, nombre de sources d'alerte = 5).

$O(deg)$, où deg est le nombre de voisins par nœud (c.-à-d., le degré du nœud dans le graphe de connectivité du RCSF). Le coût de calcul de la stratégie COP_GARE est également égal à $O(deg)$. En effet, l'algorithme COP_GARE utilise une boucle *while* pour trouver le prochain saut dans la table des voisins d'un nœud u.

Stratégie	Complexité temporelle
E-GR	$O(deg)$
PSPL	$O(deg)$
MDPSPL	$O(deg)$
COP_GARE	$O(deg)$

Tableau 3.8 – Coûts de calcul des différentes stratégies de routage étudiées.

3.6.3.2 Coûts de communication

Le Tableau 3.9 résume les coûts de communication des quatre stratégies de routage, où p est le nombre de retransmissions considérées et n est le nombre de nœuds capteurs dans le réseau.

Stratégie	**Complexité en nombre de messages**		
	Paquets *hello*	Routage mono-chemin	Total
E-GR	$O(n^2)$	$O(pn)$	$O(n^2)+O(pn)=O(n^2)$
PSPL	$O(n^2)$	$O(pn)$	$O(n^2)+O(pn)=O(n^2)$
MDPSPL	$O(n^2)$	$O(pn)$	$O(n^2)+O(pn)=O(n^2)$
COP_GARE	$O(n^2)$	$O(pn)$	$O(n^2)+O(pn)=O(n^2)$

Tableau 3.9 – Coûts de communication des différentes stratégies de routage étudiées.

3.7 Conclusion

Dans ce chapitre, nous avons présenté notre première contribution. Nous avons en effet, revisité la conception de la stratégie de routage en mode *glouton* à base de la distance maximale, et ce à la lumière du phénomène de l'irrégularité de la radio. Ensuite, nous avons présenté un algorithme de routage appelé Cross-Layer Greedy routing(CL-GR) pour les RCSFs avec des portées radio irrégulières. Le CL-GR est un algorithme de routage en mode *glouton* robuste, conçu pour être exécuté sur un N-UDG. Il fournit deux stratégies de routage géographiques, en l'occurrence la PSPL (Progress towards the sink node through Symmetrical links that experience the lowest Path Loss) et la MDPSL (progress through symmetrical links, combining the Maximum Distance forwarding strategy and the PSPL) qui sont toutes les deux basées sur une approche inter-couches par interaction de couches. Les résultats de la simulation suggèrent que ce protocole est approprié pour les applications tolérantes et non tolérante au délai, et ce selon la stratégie de routage utilisée, à savoir la PSPL ou la MDPSPL.

Dans le prochain chapitre, nous allons détailler notre deuxième contribution qui consiste en un protocole de surveillance de zone sensibles clôturées, tel qu'un site pétrolier ou nucléaire, à base des RCSFs ayant un cycle d'activité et utilisant un modèle de propagation radio réaliste. Le protocole en question est à efficacité énergétique afin de prolonger la durée de vie du réseau et par conséquent la longévité de la mission de surveillance, et utilise un protocole de routage géographique fiable, à savoir Greedy Perimeter Stateless Routing over Symmetrical Links (GPSR-SL), pour acheminer les alertes vers le nœud puits, en présence du phénomène de l'irrégularité de la radio.

Chapitre 4

Protocole de surveillance inter-couches à efficacité énergétique et fiable dédié aux zones sensibles clôturées

4.1 Introduction

La surveillance est un domaine attrayant dans lequel les RCSFs sont de plus en plus utilisés. Cependant, les applications de surveillance nécessitent une conception à efficacité énergétique et fiable, notamment quand on considère des hypothèses radio non idéales reflétant un environnement de déploiement réel (présence du phénomène de l'irrégularité de la radio [31]).

D'une part, le schéma de surveillance doit tenir compte de la rareté de la ressource énergétique dans ce type de réseau, afin de prolonger la durée de vie du réseau et par conséquent la longévité de la mission de surveillance. Nous rappelons que les nœuds capteurs sont alimentés par des batteries qui de surcroît ne sont pas facilement rechargeables ou remplaçables, en raison de :

1. La nature de la mission de surveillance, qui le plus souvent nécessite de la discrétion et même de la furtivité
2. L'environnement hostile dans lequel le réseau est déployé
3. L'ampleur du déploiement (facteur d'échelle)

D'autre part, le routage des paquets d'alerte, à partir des nœuds capteurs sources, où l'intrusion a été détectée, vers le nœud puits, doit être effectué de manière fiable pour assurer une protection élevée de la zone à surveiller. Etant donné que la couche PHY a un impact direct sur les performances des protocoles de routage, comme nous l'avons décrit à travers les trois précédents chapitres, un protocole de routage tenant compte des conditions radio réalistes considérées, doit être développé.

Ce chapitre aborde notre deuxième contribution qui consiste à proposer un protocole de surveillance des zones sensibles clôturées, tel qu'un site pétrolier ou nucléaire, à base des RCSFs avec un cycle d'activité (en Anglais, duty-cycled WSNs) et en présence de liens asymétriques. Cette asymétrie des liens est une des manifestation du phénomène de l'irrégularité de la radio. Le

protocole de surveillance en question a été justement conçu pour tenir compte de ce phénomène. Il est en effet basé sur des algorithmes, en l'occurrence l'algorithme de détection des nœuds de bordure du RCSF et celui du routage géographique des alertes vers le sink, qui s'appuient sur un graphe de connectivité réseau modélisé en tant que N-UDG.

Nous commençons le chapitre par une revue de littératures à travers laquelle nous examinons les mécanismes d'économie d'énergie ainsi que les protocoles de routage employés par les systèmes de surveillance des zones clôturées et des frontières internationales. Nous décrivons ensuite le modèle de surveillance à base des RCSFs avec cycle d'activité et les hypothèses utilisées pour mener cette étude, le protocole de routage fiable des alertes vers le sink, appelé GPSR [13] over Symmetrical Links (GPSR-SL), et le protocole de surveillance basé sur GPSR-SL. Enfin, nous discutons les résultats de simulation obtenus. Nous tenons à souligner ces résultats montrent que le protocole de surveillance proposé, basé sur GPSR-SL, atteint un ratio de livraison de paquets (en Anglais, Packet Delivery Ratio (PDR)) plus élevé d'environ 3.63%, une efficacité énergétique et une latence satisfaisante par rapport au même protocole de surveillance basé sur le GPSR original.

4.2 Travaux connexes

L'économie d'énergie et le routage des paquets d'alerte vers le nœud puits, sont deux questions clés dans la conception des systèmes de surveillance à base des RCSFs, utilisés pour sécuriser les zones sensibles clôturées (p. ex., site pétrolier ou nucléaire) et les frontières internationales. En effet, étant donné que les dispositifs de détection sont soumis à des contraintes énergétiques, la conservation de l'énergie assure l'extension de la durée de vie du réseau et, par conséquent, la longévité de la mission de surveillance. De plus, le signalement, au nœud puits, de la détection d'évènement doit être fait de manière fiable pour garantir une haute protection de la zone à surveiller. Dans cette Section, nous examinons les mécanismes d'économie d'énergie et les protocoles de routage utilisés dans de tels systèmes de surveillance.

Kim et al. [22] proposent un système de surveillance des clôtures, basé sur les RCSFs (en Anglais, WSN-based Fence surveillance System (WFS)). Ce système est élargi pour connecter et commander une caméras réseau, des véhicules terrestres sans pilote (UGV) et des véhicules aériens sans pilote (UAV), et ce afin d'améliorer la précision du système. Le WFS est organisé en trois parties : les capteurs de sol (terre) et de clôture, la station de base et les sous-systèmes (UAV et UGV). Pour économiser de l'énergie dans les RCSFs de type sol/clôture, les auteurs ont utilisé un mécanisme de veille/réveil pour les CPU, les modules RF et les capteurs. De plus, ils ont utilisé un protocole de routage hiérarchique pour rapporter le résultat de la détection collaborative effectuée par les capteurs de sol et de clôture à la station de base. WFS présente des caractéristiques intéressantes telles que l'adaptation aux changements dynamiques de la topologie du réseau et la faible consommation d'énergie. Cependant, aucune de ces caractéristiques n'a été vérifiée expérimentalement, en simulation ou en banc d'essai.

Dans [23], Sun et al. introduisent BorderSense pour les systèmes de patrouille frontalière (zone de surveillance longue bande). Il s'agit d'une architecture basée sur les RCSFs et organisée en 3 couches. BorderSense combine différents types de capteurs tels que les UGV/UAV, les capteurs

terrestres/souterrains, des capteurs multimédias (p. ex., radars, caméras), afin d'améliorer la précision de détection des systèmes de surveillance des frontières. La principale contribution de cet article est de décrire un cadre pour déployer et exploiter BorderSense. Les auteurs n'ont pas considéré les moyens d'économie d'énergie tels que le cycle veille/réveil ou le contrôle de la puissance de transmission pour économiser de l'énergie dans les RCSFs terrestres/souterrains. En ce qui concerne l'acheminement des données multimodales entre les capteurs des différentes couches lorsque des événements suspects sont détectés, les auteurs décrivent des protocoles de communication de la littérature sur la base desquels ils proposent des solutions de communication pour permettre une détection d'intrusion coopérative entre les trois couches de BorderSense. Ces solutions proposées n'ont pas été évaluées. L'évaluation des performances de BorderSense a été laissée pour des travaux futurs.

Rothenpieler et al. [24] présentent FlegSens qui est un système de surveillance pour les zones critiques, par exemple les frontières ou les propriétés privées. Le système utilise uniquement des capteurs infrarouge passifs simples pour la détection d'intrusion. L'objectif principal de FlegSens est d'assurer l'intégrité et l'authenticité des paquets d'alerte en présence d'un attaquant puissant qui peut même compromettre un certain nombre de nœuds capteurs dans le réseau. Pour prolonger la durée de vie du réseau, les auteurs utilisent un protocole, au niveau de la couche liaison de données (DLL), permettant de gérer les cycles d'activité des nœuds et minimiser les délais de communication de bout en bout. De plus, ils ont utilisé un mécanisme d'inondation (en Anglais, flooding) au niveau de la couche réseau pour communiquer la détection d'un intrus à une passerelle dédiée. Les algorithmes basés sur l'inondation ne sont pas évolutifs (ne permettent pas le passage à l'échelle), sont inefficaces sur le plan énergétique et ne garantissent pas une livraison fiable des paquets d'alerte.

Une approche pour atténuer le problème des vides (en Anglais, voids ou holes) dans les applications de surveillance basées sur les RCSFs, est proposée dans [25]. Les vides sont le résultat de la destruction intentionnelle des nœuds capteurs ou de l'extinction de ces derniers, en raison de l'épuisement de leurs batteries. Les résultats de la simulation montrent que cette approche d'atténuation basée sur le redéploiement des capteurs étend la durée de vie du réseau et maintient sa qualité de détection au-dessus d'un certain seuil. Les auteurs ont étudiés l'effet de trois facteurs principaux sur la qualité de détection et la durée de vie du réseau :

— densité de déploiement des nœuds capteurs
— inter-arrivée d'intrus
— redéploiement.

Les auteurs n'ont pas considéré l'effet des liens asymétriques sur la qualité de détection et la durée de vie du réseau.

Dans [26], les performances des protocoles, Ad hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR) et Optimized Link State Routing (OLSR), dans les applications de surveillance des frontières basées sur les RCSFs, sont comparées. La comparaison est effectuée sur la base des métriques suivantes :

— délai
— charge de trafic

— perte de paquets

— consommation d'énergie.

Les résultats de la simulation montrent que DSR fonctionne mieux que AODV et OLSR pour un réseau avec un nombre limité de nœuds. Cependant, l'un des inconvénients de DSR est qu'il repose sur un graphe de connectivité réseau avec des liens symétriques. En fait, quand un nœud connaît une route vers la destination, il envoie un paquet Route REPly (RREP), en mono-diffusion (en Anglais, unicast), au nœud source qui a sollicité la route, via le chemin inverse de celui qu'il a appris pendant la phase de diffusion des paquets Route REQuest (RREQ).

Bellazreg et al. [27] proposent un système de surveillance des frontières basé sur un RCSF hétérogène, déployé le long de la frontière sous la forme d'une ligne épaisse. Les auteurs ont décrit une stratégie de déploiement et une technique de routage pour assurer une bonne qualité de couverture et un échange de données efficace. Cependant, l'étude s'est concentrée sur la couverture et la connectivité sans prêter attention à la consommation d'énergie ou à la fiabilité des liens.

Dans [28], Hammoudeh et al. proposent un système de surveillance des frontières basé sur les RCSFs linéaires (en Anglais, Linear WSNs (LWSNs)). Leur système, basé sur une architecture plate et modulaire, comprend un ensemble de nœuds capteurs de base (en Anglais, Basic Sensor Nodes (BSN)) qui collaborent pour détecter et signaler des événements à une tour de surveillance (en Anglais, Monitoring Tower (MT)) qui est connectée à un centre de décision distant. Un protocole de communication inter-couches, appelé Levels Division Graph (LDG), est conçu pour répondre aux exigences des applications basées sur les LWSNs, en termes d'efficacité énergétique et de délai de bout en bout. Le protocole LDG ajuste dynamiquement la puissance de transmission des BSN en fonction de leur niveau réseau, qui est proportionnel à leur distance par rapport à la MT, pour économiser de l'énergie. De plus, les auteurs ont proposé un mécanisme de veille/réveil pour économiser plus d'énergie et réduire le délai de bout en bout. En outre, la sélection des liens dans l'algorithme LDG est basée sur une métrique de coût qui inclut l'énergie résiduelle du parent dans l'arbre de routage de données, la distance pour l'atteindre et la qualité du lien entre les deux nœuds. Cette dernière est fournie par la couche MAC sur la base de l'indicateur de force de signal reçu (RSSI). L'étude n'a pas précisé comment un BSN peut atteindre un MT en présence de liens asymétriques.

Il ressort clairement de l'étude de la littérature qu'il n'y a pas de réelles tentatives pour résoudre le problème de l'asymétrie des liens, qui a un impact négatif sur la performance des protocoles des couches supérieures. Le déploiement des RCSFs dans un environnement réel nécessite de nouveaux protocoles qui prennent en compte ce type de liens, qui est une des manifestations de l'irrégularité de la radio, et ce pour répondre aux exigences des applications de surveillance à base des RCSFs, notamment en termes de PDR, délai de bout en bout, consommation d'énergie et fiabilité.

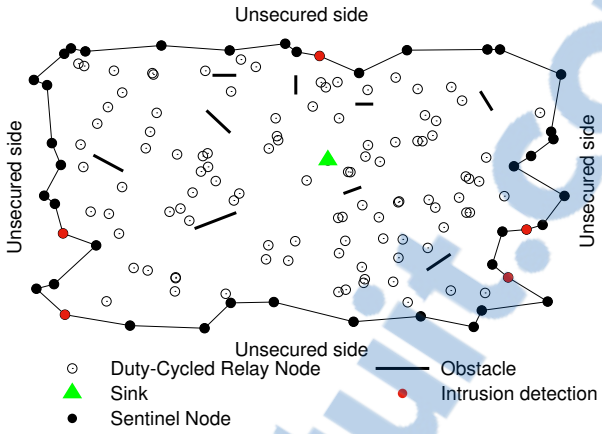


FIGURE 4.1 – Modèle de surveillance basé sur les RCSFs avec cycle d'activité.

4.3 Description du modèle réseau utilisé et hypothèses

Nous considérons un RCSF statique, composé de N nœuds capteurs, et d'un puits riche en ressources, comme représenté sur la Figure 4.1. Les nœuds sont déployés de manière aléatoire pour surveiller une zone sensible clôturée, tel qu'un site pétrolier ou nucléaire. Nous supposons que le terrain n'est pas libre d'obstacles. Chaque nœud est au courant de sa propre position, obtenue par un système de positionnement global (GPS) ou une approche de localisation [38, 69–72].

Les portées de transmission des nœuds sont irrégulières en raison de multiples facteurs, notamment le type d'antenne et de médium, les obstacles et les conditions météorologiques. Par conséquent, les liens entre les nœuds peuvent être asymétriques et des vides peuvent être présents dans le réseau. Nous rappelons que des vides peuvent également exister en raison du déploiement initial.

Dans cette étude, l'atténuation de parcours entre deux nœuds, due à la distance entre une paire transmetteur-récepteur (TR) et à la présence de facteurs d'atténuation du signal, est prédite à l'aide du modèle de propagation radio log-normal shadowing tel que défini dans [12], et qui est représenté par l'Equation (1.7) (Section 1.14.3 du Chapitre 1).

Le graphe de connectivité réel du réseau est noté $G(V, E)$, où V représente l'ensemble des nœuds et E est l'ensemble des arcs représentant la connectivité entre les nœuds. Un arc (A, B), c.-à-d., $A \rightarrow B$, existe entre les nœuds A et B si et seulement si un paquet envoyé par A peut atteindre B. Nous indiquons l'ensemble des voisins d'un nœud u par $\mathcal{N}(u)$ et son ensemble de voisins qui appartiennent à son Graphe de Gabriel (GG) par $\mathcal{N}_g(u)$. Nous rappelons qu'un GG est un graphe planaire, c.-à-d., un graphe dans lequel il n'y a pas deux arcs qui s'intersectent. Il est construit à partir du graphe de connectivité réseau initial, en utilisant l'Algorithme 2.1 ou l'Algorithme 2.3. Il convient de rappeler que le mode *périmètre* du protocole GPSR-SL (protocole sur le lequel s'appuie notre protocole de surveillance pour router les messages d'alerte vers le nœud puits), s'exécute sur un GG.

L'étape de découverte du voisinage a lieu une fois que les nœuds capteurs ont été initialement déployés. Cette phase est similaire à celle décrite dans la Section 3.3. Ensuite, la phase

Champ	Nom
NI	Identifiant du nœud
NP	Position du nœud
NS	Ensemble des voisins
	(tous les nœuds que NI peut entendre)

Tableau 4.1 – Structure d'un paquet *hello* diffusé par un nœud NI.

Champ	Nom
NGI	Identifiant du voisin
NGP	Position du voisin
SYM	1 si le lien $(u \rightarrow NGI)$ est symétrique sinon 0
STATUS	1 si SN, 0 sinon

Tableau 4.2 – Table des voisins d'un nœud u.

d'identification des nœuds *sentinelles* (SNs) commence. À la fin de cette phase, le cycle d'activité [1] des nœuds relais (DC-RNs) (nœuds qui n'ont pas été identifiés comme SNs) est initialisé à une valeur inférieure à 1, et le processus de surveillance démarre. Ainsi, lorsqu'un intrus tente de franchir la frontière du réseau, un message d'alerte (AM) est généré par le nœud SN ayant détecté l'intrusion, et envoyé vers le nœud puits, via des liaisons symétriques en utilisant le protocole GPSR-SL. Au niveau de la couche liaison de données, nous utilisons un protocole MAC asynchrone basé sur la contention (similaire au protocole B-MAC [133]), avec un mécanisme de retransmission.

4.4 Description du protocole GPSR-SL

Le protocole de routage Greedy Perimeter Stateless Routing over Symmetrical Links (GPSR-SL) est une variante du GPSR original que nous avons décrit dans la Section 2.4.1.3.4. Le GPSR original a été modifié comme suit.

1. nous avons ajouté un mécanisme de détection de la symétrie des liens, similaire à celui utilisé par la solution Symmetric Geographic Forwarding [30], qui permet à chaque nœud d'identifier ses voisins symétriques, et ce lors de la phase de découverte du voisinage qui est, rappelons-le, la même que celle décrite dans la Section 3.3. Les Tableaux 4.1 et 4.2 montrent respectivement, la structure d'un paquet *hello* et celle de la table des voisins d'un nœud, que nous avons utilisées. Notons qu'elles sont légèrement différentes par rapport à celles utilisées dans la Section 3.3.
2. Nous avons modifié les modes *glouton* et *périmètre* du GPSR original, comme décrit dans les Sections 4.4.1 et 4.4.2, respectivement.

1. Cycle d'activité = $\frac{actif}{actif+sommeil}$

4.4.1 Routage en mode *glouton*

Le mode *glouton* du GPSR-SL transmet un paquet en se basant sur deux critères, à savoir la distance et la symétrie des liens, comme indiqué dans l'Algorithme 4.1. Le nœud transmetteur choisit parmi ses voisins avec qui il a un lien symétrique, celui qui est le plus proche géographiquement du nœud puits. Etant donné que chaque nœud sauvegarde les coordonnées de tous ses voisins à 1 saut dans sa table de voisins (voir Tableau 4.2), et que les coordonnées du nœud puits sont incluses dans le paquet d'alerte à acheminer (voir Tableau 4.3), le nœud transmetteur est en effet capable d'identifier son voisin le plus proche géographiquement du nœud puits parmi ses voisins avec lesquels il a un lien symétrique. Nous rappelons que l'identification des voisins symétriques est effectuée pendant la phase de découverte du voisinage. Il convient de noter aussi que le routage en mode *glouton* de GPSR-SL est basé sur le même principe que la stratégie PSPL de CL-GR présenté dans le chapitre précédent (Section 3.4.1), à l'exception du fait qu'il se base sur deux critères au lieu de trois pour sélectionner le prochain saut.

Algorithme 4.1 Routage en mode glouton de GPSR-SL.

Require: a packet p, $\mathcal{N}(u)$.
Ensure: next hop v if it exists, otherwise returns -1.

```
1: d ← distance(u, p.SP)
2: v ← −1
3: while w ∈ N(u) do
4:    if link(u,w) is symmetrical then
5:       if distance(w, p.SP) < d then
6:          d ← distance(w, p.SP))
7:          v ← w
8:       end if
9:    end if
10: end while
11: return v
```

4.4.2 Routage en mode *périmètre*

Contrairement au routage *glouton* qui est exécuté sur le graphe de connectivité réseau sous-jacent initial, le routage en mode *périmètre* doit être exécuté sur un sous-graphe planaire construit à partir du graphe de connectivité réseau initial. La planarisation du graphe initial se fait à l'aide d'algorithmes de planarisation, tel que celui dit algorithme du GG (voir Algorithme 2.1).

Comme nous l'avons mentionné dans la Section 2.5.2, les algorithmes de planarisation ne parviennent pas à produire un sous-graphe planaire lorsque le graphe de connectivité réseau sous-jacent est un N-UDG. Cette défaillance entraîne par conséquent un échec de routage du mode *périmètre*. Parmi les correctifs proposés dans la littérature, nous avons choisi d'implémenter le correctif MW en raison de son haut niveau d'efficacité en termes de messages échangés [45] et de sa facilité d'implémentation. Il convient de noter que l'application de ce correctif à la planarisation GG n'est pas suffisante pour obtenir un sous-graphe planaire "sûr".

Champ	Nom complet
PK	Type de paquet (AM or BDP)
FM	Mode du paquet (*glouton* ou *périmètre*)
SI	Identifiant du sink
SP	Position du sink
PH	Identifiant du saut précédent
I-NPF	Identifiant du nœud où le paquet est entré pour la 1ère fois en mode *périmètre*
P-NPF	Position du nœud ayant pour identifiant I-NPF
LFP	Position du point partagé entre la face précédente et la nouvelle face, sur la ligne directe reliant le nœud I-NFP au nœud SI
FE	Première arête traversée sur la face courante

Tableau 4.3 – Les champs d'entête d'un paquet p (couche NET).

Le routage en mode *périmètre* de GPSR-SL s'exécute sur un sous-graphe planaire obtenu à l'aide de l'algorithme de planarisation GG auquel nous appliquons le correctif MW (voir Algorithme 2.3). Nous rappelons que le correctif en question indique qu'un nœud u élimine l'arc (u, v) du graphe initial, s'il existe au moins un témoin visible à la fois pour u et v, dans le cercle ombré de diamètre uv représenté dans la Figure 2.3. Dans notre cas, ceci est réalisé lorsque les nœuds diffusent leurs Neighbor Set (NS)afin d'identifier les liens symétriques, durant la phase de découverte du voisinage décrite dans la Section 3.3.

Chaque fois qu'un nœud u doit transmettre un paquet, en utilisant le mode *périmètre*, à un nœud v parmi ses voisins avec lesquels il a un lien symétrique, il vérifie si l'arc (u, v) appartient à son GG ou non. S'il en fait partie, le nœud v devient candidat au prochain saut. Ensuite, parmi tous ces nœuds candidats, le prochain saut est choisi en utilisant la règle de la main droite. Si l'arc (u, v) choisi intersecte avec la ligne, entre le nœud où l'AM est entré en mode *périmètre* pour la première fois et le nœud puits, le protocole GPSR-SL passe à la face suivante du GG et continue le routage de l'AM sur cette face. Le mode *glouton* reprend lorsque le paquet atteint un nœud qui est plus proche du nœud puits que le nœud qui a initié le mode *périmètre*.

4.5 Protocole de surveillance basé sur GPSR-SL

Dans cette section, nous allons présenter notre protocole de surveillance basé sur une approche inter-couches et dédié à la surveillance des zones sensibles clôturées, que nous avons appelé GPSR over Symmetrical Links (GPSR-SL). Initialement, GPSR-SL identifie les nœuds de bordure du réseau (en Anglais, Network Boundary Nodes (NBNs)) qui seront utilisés comme des nœuds *sentinelles* (en Anglais Sentinel Nodes (SNs)), lors du processus de surveillance. Comme leur nom l'indique, ces SNs sont maintenus tout le temps dans un état actif. Les nœuds restant seront utilisés comme des nœuds relais avec un cycle d'activité (en Anglais, Duty-Cycled Relay Nodes (DC-RNs)), et ce pendant la phase de communication de données durant laquelle, le

protocole de surveillance assure le routage des AMs, générés par les SNs, jusqu'au nœud puits.

4.5.1 Identification des nœuds de bordure du RCSF

Lorsque l'étape de découverte du voisinage se termine, le nœud puits commence la découverte des NBNs par la création et l'envoi d'un paquet de découverte de bordure (en Anglais, Border Discovery Packet (BDP)) vers une destination fictive (en Anglais, Fictitious Destination (FD)). Cette dernière est un nœud qui est déconnecté de tous les autres nœuds du RCSF. Il convient de noter que l'algorithme d'identification des NBNs est inspiré de l'algorithme décrit dans [180].

Algorithme 4.2 Protocole de surveillance proposé.

Require: a packet p, $\mathcal{N}(u)$, $\mathcal{N}_g(u)$.
Ensure: the forwarding of a packet p to a next hop v and the identification of NBNs.

if p.FM = "Greedy" **then**
  $v \leftarrow$ greedy(p)
  if $v = -1$ **then**
    $v \leftarrow$ perimeter(p)
  end if
else {FM = "Perimeter"}
  if dist(u, p.SP) < dist(p.P-NPF, p.SP) **then**
    p.FM $\leftarrow$ "Greedy"
    $v \leftarrow$ greedy(p)
    if $v = -1$ **then**
      $v \leftarrow$ perimeter(p)
    end if
  else
    $v \leftarrow$ perimeter(p)
  end if
end if
if $v \neq -1$ **then**
  forwarding p to v
  if (p.FM = "Perimeter" and p.PK = "BDP") **then**
    u identifies itself as SN and informs its neighbors.
  end if
else
  routing failure at node u
end if

Comme illustré dans la Figure 4.2, le nœud puits projette tout d'abord son emplacement 2D sur les quatre lignes délimitant le champ de déploiement, c.-à-d., les clôtures de la zone surveillée. Ensuite, il sélectionne le point le plus proche de lui-même parmi les quatre points obtenus, pour être la destination fictive (FD). Une fois celle-ci déterminée, Le nœud puits crée un BDP (voir Tableau 4.3), et l'envoie vers la FD, en utilisant le protocole GPSR-SL. Initialement, le champ mode du paquet (FM) de BDP est défini à *glouton*, comme nous l'avons mentionné dans la Section 2.4.1.3.4. Comme indiqué dans l'Algorithme 4.2, chaque fois que le BDP est transmis

en utilisant le mode *périmètre*, le nœud transmetteur s'identifie comme SN, et diffuse cette information à ses voisins. Quand le BDP revient au niveau du nœud où il est entré en mode *périmètre* pour la première fois (c.-à-d., le nœud NPF), l'étape de découverte des SNs s'arrête. En fait, lorsque le BDP revient à ce nœud (NPF), il est confirmé que tous les SNs ont été identifiés, parce que la FD est déconnectée de tous les autres nœuds et par conséquent le BDP ne l'atteindra jamais. A ce moment, on affecte un cycle d'activité (< 1) pour les nœuds DC-RNs, et le processus de surveillance est déclenché.

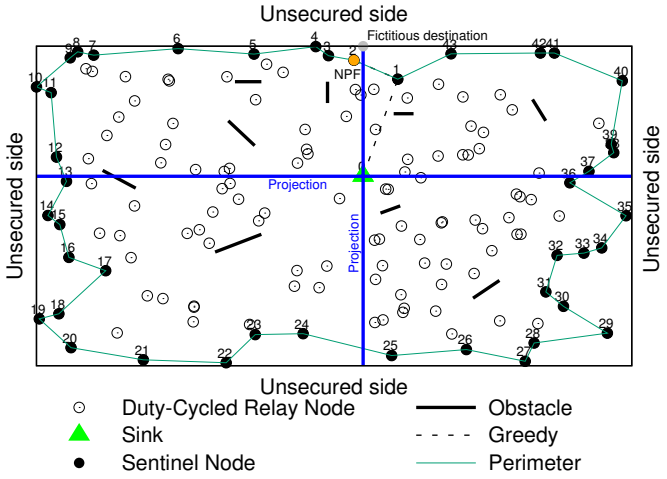


FIGURE 4.2 – Identification des nœuds de bordure du réseau.

Exemple d'illustration

La Figure 4.2 représente un exemple de découverte des nœuds de bordure d'un RCSF. Le nœud puits détermine la FD (représentée avec une couleur grise sur la Figure 4.2), puis envoie un BDP, en mode *glouton*, au nœud 1 qui est le nœud le plus proche géographiquement de la FD . Ensuite, le nœud 1 envoie le BDP à son voisin, le nœud 2, qui est le voisin le plus proche de la FD. Le nœud 2 n'a aucun voisin plus proche de la FD que lui-même, comme on peut le constater sur la Figure 4.2. Ce nœud est en effet un minimum local (ou nœud *concave*), au niveau duquel le BDP entre, pour la première fois, en mode *périmètre*.
Le nœud 2 qui est également appelé (NPF), change le FM de BDP en mode *périmètre* et le transmet au nœud 3, en utilisant la règle de la main droite. Le BDP va ainsi faire un tour complet dans le sens inverse des aiguilles d'une montre jusqu'à atteindre le nœud où il est entré pour la première fois en mode périmètre (NPF), soit le nœud 2. A ce moment, nous sommes sûrs que tous les NBNs ont été découverts.

4.5.2 Routage des messages d'alerte

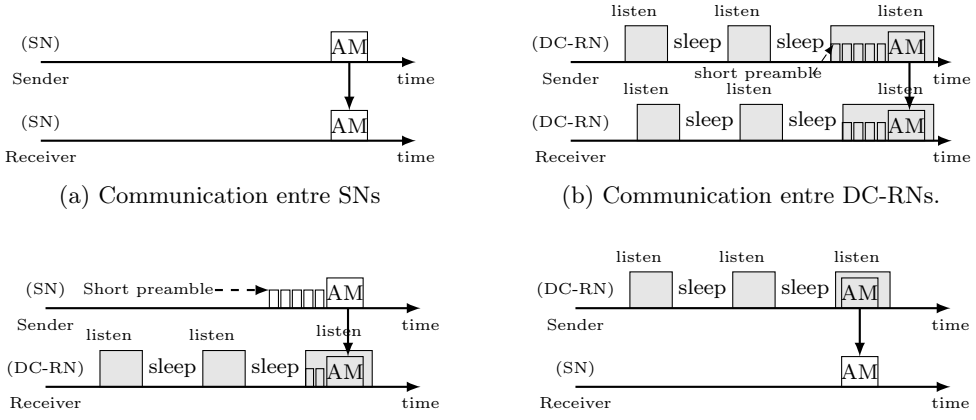
Lors de la détection d'une intrusion par un SN, celui-ci génère un AM et l'envoie vers le nœud puits, en utilisant un protocole de routage à sauts multiples, comme décrit par l'Algorithme 4.2.

Le prochain saut est donné par le protocole GPSR-SL en utilisant, soit le mode *glouton*, soit le mode *périmètre*. Nous rappelons que le mode *glouton* est exécuté sur le graphe de connectivité réseau initial. Il tente de transmettre l'AM, via des liens symétriques, au voisin le plus proche géographiquement du nœud puits.

Quant au mode *périmètre*, il faut un sous-graphe planaire pour acheminer l'AM jusqu'au nœud puits. Dans cette thèse, nous avons utilisé l'algorithme de planarisation GG auquel nous lui avons appliqué le correctif MW (voir Algorithme 2.3), pour construire un sous-graphe planaire à partir du graphe de connectivité réseau initial sous-jacent. Nous rappelons que le MW stipule qu'un nœud u élimine le lien (u, v) du graphe initial s'il existe au moins un témoin, visible à la fois pour u et v, dans le cercle ombré de diamètre uv représenté sur la Figure **??**. L'acheminement de l'AM est effectué sur le sous-graphe GG obtenu, en utilisant le mode *périmètre* de GPSR-SL, décrit dans la section 4.4.2.

Au niveau de la couche MAC, nous avons utilisé un protocole MAC asynchrone basé sur la contention, similaire au protocole B-MAC [133]. La communication entre deux nœuds se fait sur la base du statut du nœud destinataire (SN ou DC-RN), comme illustré dans la Figure 4.3. En effet, si le nœud destinataire est un DC-RN, l'émetteur transmet une série de courts préambules, d'une durée aussi longue que la période de sommeil du destinataire, avant d'envoyer l'AM comme le montrent les Figures 4.3 (b) et (c). Cependant, dans le cas où le nœud destinataire est un SN, l'émetteur va économiser de l'énergie en transmettant le AM directement sans le faire précéder de préambules, puisque SN est toujours dans un état actif. Ceci est illustré dans les Figures 4.3 (a) et (d).

L'information relative au statut du destinataire est obtenue par la couche MAC de l'émetteur au moyen d'une conception inter-couches par interaction entre les couches NET et MAC, comme le montre la Figure 4.4. Nous rappelons que lorsqu'un nœud s'identifie comme SN, lors de l'étape d'identification des NBNs, il diffuse son statut à ses voisins qui stockent cette information dans leur table de voisinage (couche NET).



(a) Communication entre SNs

(b) Communication entre DC-RNs.

(c) Communication entre SN et DC-RN

(d) Communication entre DC-RN et SN

FIGURE 4.3 – Communication entre deux nœuds au niveau de la couche MAC, en fonction du statut du nœud destinataire (SN ou DC-RN).

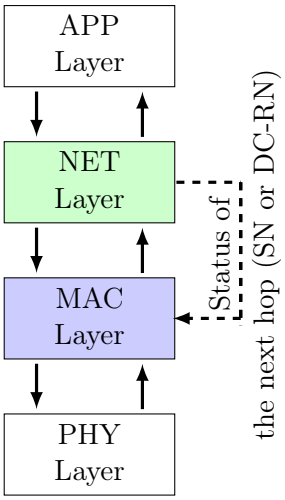


FIGURE 4.4 – Illustration de la conception inter-couches utilisée par le protocole GPSR-SL.

4.6 Evaluation des performances

La performance du protocole de surveillance présenté est évaluée par simulation sous le simulateur Castalia [107], basé sur la plate-forme OMNeT++ [102]. Nous utilisons trois métriques d'évaluation, à savoir la consommation d'énergie, le PDR (Packet Delivery Ratio) et le délai moyen de bout en bout, pour comparer les performances de notre protocole de surveillance GPSR-SL avec le protocole de surveillance GPSR. L'interférence est gérée selon le modèle de gestion des interférences, implémenté dans le simulateur Castalia. Le modèle en question est basé sur la métrique SINR (Signal to Interference plus Noise Ratio). En effet, lorsqu'un nœud reçoit plusieurs signaux émanant de plusieurs nœuds sources, il accepte celui avec le SINR le plus élevé. Tous les résultats discutés ci-dessous représentent, pour chaque scénario, la moyenne des résultats de 100 simulations réalisées. La durée de chaque simulation est de 120 secondes. Il convient de noter que la topologie du réseau est modifiée lors de chaque simulation, en faisant varier l'atténuation de parcours entre les nœuds (le nombre et les positions des nœuds restent inchangés). Nous rappelons que l'atténuation de parcours entre deux nœuds est prédite en utilisant l'Equation (1.7). La variation de l'atténuation de parcours est obtenue en variant l'effet shadowing représenté par la variable aléatoire distribuée gaussienne de moyenne nulle et d'écart type σ, X_σ. Le tableau 4.4 résume les paramètres les plus importants de la simulation.

4.6.1 Définition des métriques de performance utilisées

1. Energie totale consommée dans le réseau : Représente l'énergie totale consommée dans le réseau, pendant la durée de la simulation, calculée selon le modèle énergétique fourni par le simulateur Castalia.
2. PDR (Packet Delivery Ratio) : Représente le rapport entre le nombre d'alertes reçues par le nœud puits, et le nombre d'alertes envoyées par les nœuds sources d'alerte.

Paramètre	Valeur
Durée de la simulation	120 secondes
Terrain (avec obstacles)	90 m × 90 m
Nombre de nœuds	150
Topologie réseau par simulation	100 (Durant chaque simulation, le nombre et les positions des nœuds sont maintenus constant, tandis que l'atténuation de parcours entre les nœuds varie)
Nombre moyen de NBNs	44
Nombre moyen d'AMs envoyés	4.69, 9.19, 15.98
Déploiement	Aléatoire
Nombre de nœuds puits	1 (toujours en état actif)
Capacité de la batterie	18720 Joules
Modèle de propagation	Log-normal shadowing
n	2.4
σ	4.0 dB
Radio	CC2420
Débit	250 kbps
Sensibilité radio	-95 dBm
Puissance d'émission	0 dBm
Consommation d'énergie	TX : 57.42 milliWatt RX : 62 milliWatt
Protocole NET	GPSR-SL, GPSR
Protocole MAC	Tunable MAC (similaire à B-MAC)
Période d'écoute	10 millisecondes
Nombre de retransmissions	0
Cycle d'activité des SNs	1
Cycle d'activité des DC-RNs	Allant de 0.1 à 1.0 par pas de 0.1
Gestion de l'interférence	Oui

Tableau 4.4 – Paramètres de simulation.

3. Délai moyen de bout en bout : Représente le temps moyen écoulé entre l'envoi d'une alerte par un nœud source d'alerte et le temps d'arrivée de cette alerte au niveau du nœud puits. Il est défini par le rapport entre le temps de transmission du nombre total d'alertes reçues par le nœud puits et ce même nombre total d'alertes reçues par celui-ci.

4.6.2 Analyse des résultats

4.6.2.1 Effet de la variation de la durée du cycle d'activité

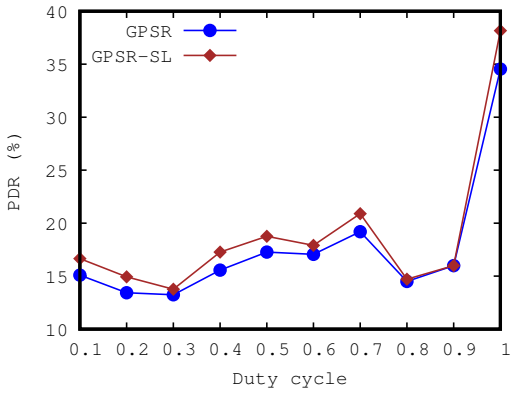
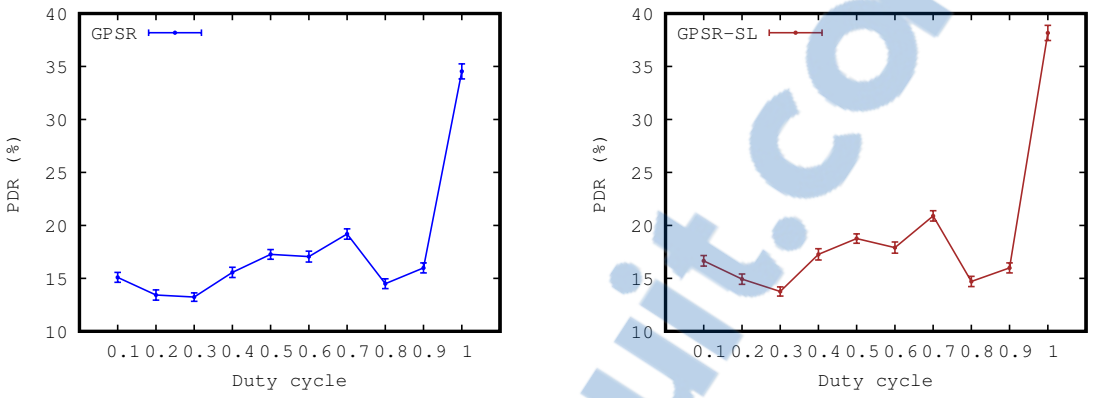


FIGURE 4.5 – PDR en fonction du cycle d'activité des DC-RNs (nombre total de nœuds = 150, nombre moyen de AMs envoyés sur les 100 simulations réalisées = 4.69).

La Figure 4.5 met en évidence le PDR en fonction de la variation de la longueur du cycle d'activité. Les résultats montrent que le protocole de surveillance proposé obtient un PDR plus élevé par rapport au GPSR original. Le PDR est amélioré en fonction des différentes longueurs du cycle d'activité considérées. L'amélioration est de 1.32% en moyenne. Elle atteint 3.63 % lorsque tous les nœuds du réseau sont maintenus à l'état actif. Le PDR élevé obtenu par le protocole proposé est la conséquence directe de l'utilisation de liens fiables, c.-à-d., des liens symétriques, pour transmettre les AMs. Cela est également dû à l'utilisation du correctif MW qui améliore les performances du routage en mode *périmètre* sur un N-UDG.

La Figure 4.6 montre les tracés PDR avec des barres d'erreur, correspondant respectivement à GPSR et GPSR-SL. Nous notons que nous avons utilisé un intervalle de confiance de 99.73%, c.-à-d., que 99.73% des valeurs de simulation se situent dans les trois écarts-types de la moyenne $(3 * \sigma)$.

La Figure 4.7 montre que le GPSR-SL permet d'économiser de l'énergie par rapport au GPSR. En effet, malgré le fait que le PDR atteint par GPSR-SL soit supérieur à celui du GPSR, la consommation totale d'énergie dans le réseau lors de l'utilisation du GPSR-SL est quasiment la même que celle résultant de l'utilisation du GPSR. La raison principale est que le GPSR-SL transmet les AMs via des liens symétriques, qui sont plus fiables que les liens asymétriques utilisés par le GPSR original. Le gaspillage d'énergie résultant de l'utilisation du GPSR est principalement dû au fait que les paquets sont perdus lorsqu'ils sont transmis par des liaisons asymétriques. Ce résultat montre que le GPSR-SL est capable d'atteindre le même PDR que le



(a) (b)

FIGURE 4.6 – PDR avec barres d'erreur, en fonction du cycle d'activité des DC-RNs (nombre total de nœuds = 150, nombre moyen de AMs envoyés sur les 100 simulations réalisées = 4.69).

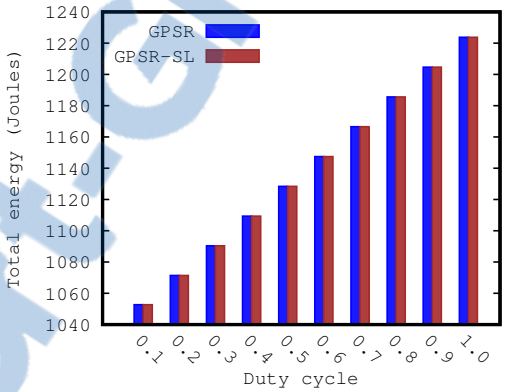


FIGURE 4.7 – Energie totale consommée dans le réseau en fonction du cycle d'activité des DC-RNs (nombre total de nœuds = 150, nombre moyen de AMs envoyés sur les 100 simulations réalisées = 4.69).

GPSR à une dépense énergétique plus faible. Cela rend le GPSR-SL plus adapté aux applications de surveillance à long terme, qui nécessitent une faible consommation d'énergie pour prolonger la durée de vie du réseau et fonctionner de manière fiable.

La Figure 4.8 montre le délai moyen de bout en bout généré par les deux protocoles. On peut observe que le GPSR-SL réalise un délai moyen de bout en bout raisonnable quelque soit le cycle de d'activité considéré, par rapport à GPSR. La légère différence ($\in$ [0.96 ms, 30.99 ms]) est due au fait que le lien entre le nœud transmetteur et le nœud le plus proche géographiquement du nœud puits n'est généralement pas symétrique. Par conséquent, le GPSR-SL ne choisira pas toujours le chemin le plus court, ce qui entraînera une augmentation du nombre de sauts parcourus par un AM pour atteindre le nœud puits.

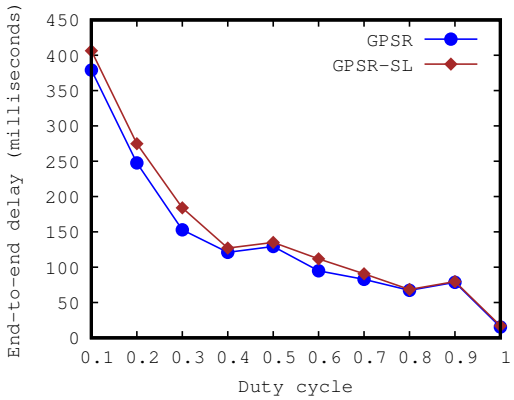


FIGURE 4.8 – Délai moyen de bout en bout en fonction du cycle d'activité des DC-RNs (nombre total de nœuds = 150, nombre moyen de AMs envoyés sur les 100 simulations réalisées = 4.69).

4.6.2.2 Effet de la variation du nombre d'alertes

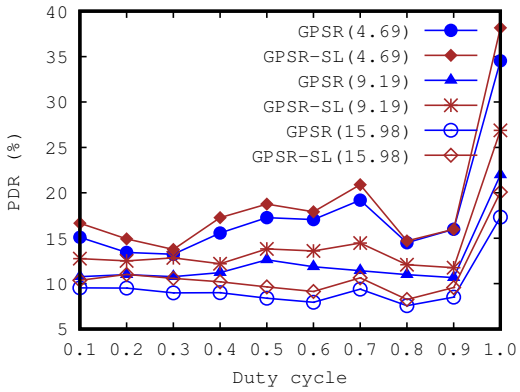


FIGURE 4.9 – PDR en fonction du nombre d'alertes (nombre total de nœuds = 150).

Comme représenté sur la Figure 4.9, le PDR atteint par GPSR et GPSR-SL diminue lorsque le nombre de AMs augmente, et ce pour les différentes durées de cycle d'activité considérées. Ceci est dû aux interférences qui sont la conséquence de l'augmentation des transmissions simultanées. Cependant, le GPSR-SL atteint un PDR plus élevé que le GPSR, puisque les AMs sont transmis via des liens symétriques plus résistants aux interférences. C'est un résultat très intéressant puisque dans les applications de surveillance, il est fréquent que plusieurs intrus tentent, en même temps, de traverser la zone sécurisée et ce depuis différents endroits (voir Figure 4.1). Ainsi, plusieurs AMs seront générés et envoyés simultanément vers le nœud puits. Dans ce cas, notre protocole de surveillance basé sur GPSR-SL sera en mesure de transmettre plus d'AMs au sink. Ceci est d'une importance capitale dans le processus de surveillance d'une zone sensible car il permet au système de décision distant de réagir à un nombre maximal d'AMs, ce qui assurera une protection élevée de cette zone.

Les Figures 4.10 et 4.11 représentent respectivement les résultats des deux autres métriques

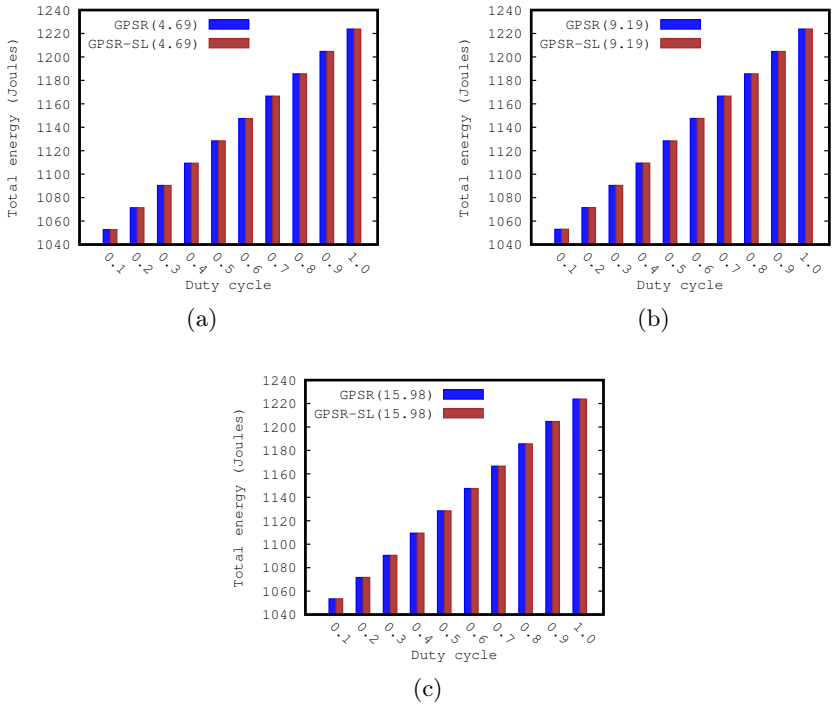


FIGURE 4.10 – Energie totale consommée dans le réseau en fonction du nombre d'alertes (nombre total de nœuds = 150).

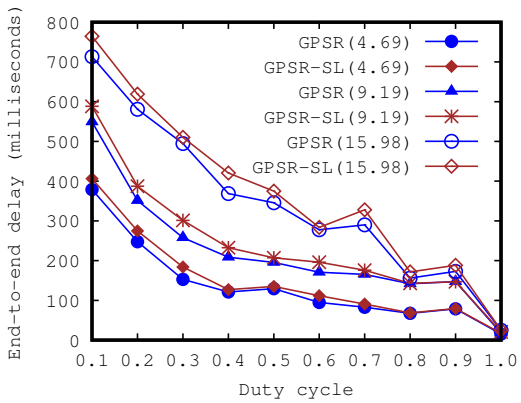
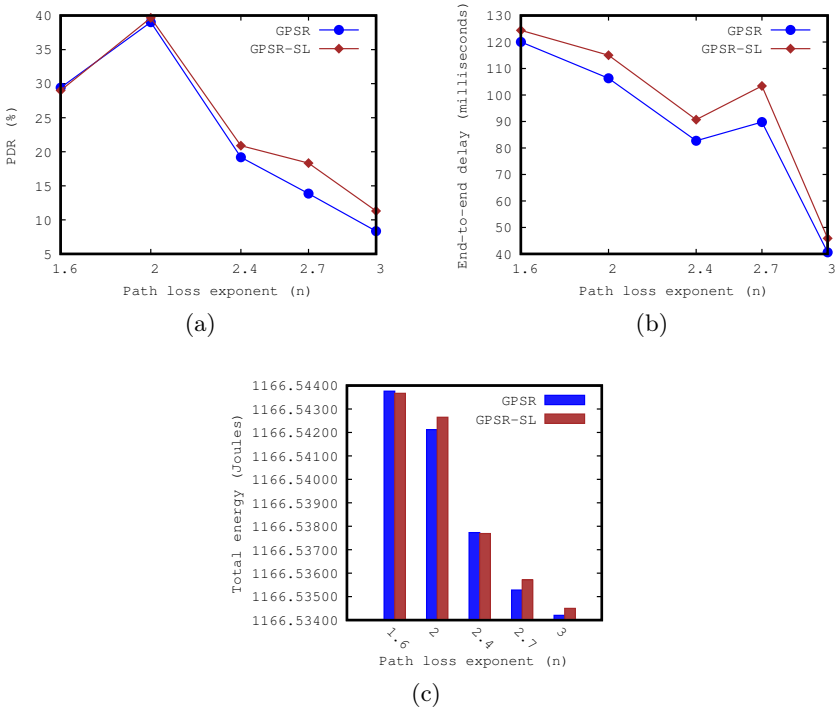


FIGURE 4.11 – Délai moyen de bout en bout en fonction du nombre d'alertes (nombre total de nœuds = 150).

considérées dans cette étude, à savoir l'énergie totale consommée et le délai moyen de bout en bout. Comme on peut le voir sur la Figure 4.10, l'énergie totale consommée dans le réseau, lors de l'utilisation de GPSR ou de GPSR-SL, est presque la même. Cela confirme notre analyse faite dans la Section 4.6.2.1, relativement à cette métrique. En outre, le délai moyen de bout en bout pour les deux protocoles, augmente puisque les nœuds vont, de plus en plus, retarder leurs transmissions en raison des interférences créées par les transmissions simultanées (voir

Figure 4.11). Nous notons enfin que le GPSR-SL obtient un délai raisonnable de bout en bout, comparé à son rival GPSR.

4.6.2.3 Effet de la variation de l'exposant de l'atténuation de parcours



(a) (b)

(c)

FIGURE 4.12 – Résultats de simulation des trois métriques considérées, en fonction de l'exposant de l'atténuation de parcours (nombre total de nœuds = 150, nombre moyen de AMs envoyés sur les 100 simulations réalisées = 4.69, cycle d'activité = 0.7 (70%)).

La Figure 4.12(a) met en évidence le PDR en fonction de la variation de l'exposant de l'atténuation de parcours (n). Les résultats montrent que GPSR-SL atteint un PDR plus élevé par rapport au GPSR original. Les Figures 4.12(b) et (c) montrent respectivement l'efficacité du GPSR-SL en termes de consommation d'énergie et de latence lorsqu'il est comparé à GPSR. En effet, notre protocole permet une efficacité énergétique et une latence satisfaisante. Par exemple, pour $n = 2.7$, le $\text{PDR}_{GPSR-SL} = 18.34\%$, l'énergie consommée est de 1166.53571 Joules et la latence est de 103.40 millisecondes, alors que le $\text{PDR}_{GPSR} = 13.86\%$, l'énergie consommée est de 1166.53528 Joules et la latence est de 89.8 millisecondes.

4.6.2.4 Effet de l'augmentation de la densité du réseau

Comme indiqué dans le Tableau 4.5, l'augmentation du nombre de nœuds capteurs conduit à la diminution du PDR obtenu par GPSR-SL, et ce pour les deux valeurs considérées du cycle d'activité (0.7(70%)) et (1.0(100%)). Cela peut être expliqué comme suit. Lorsque le réseau devient

Cycle d'activité	PDR(GPSR-SL$_{(150)}$)	PDR(GPSR-SL$_{(250)}$)
0.7 (70%)	20.90%	20.67%
1.0 (100%)	38.17%	36.81%

Tableau 4.5 – PDR réalisé par GPSR-SL en fonction du cycle d'activité et du nombre de nœuds capteurs.

dense, les nœuds sont plus proches les uns des autres et par conséquent des liens symétriques plus courts sont disponibles. Dans ce cas, GPSR-SL maximise le nombre de sauts moyen parcouru par un AM, augmentant ainsi le risque de collision (à cause du terminal caché) et d'interférence.

Cycle d'activité	PDR(GPSR$_{(150)}$)	PDR(GPSR$_{(250)}$)
0.7 (70%)	19.19%	18.29%
1.0 (100%)	34.54%	34.92%

Tableau 4.6 – PDR réalisé par GPSR en fonction du cycle d'activité et du nombre de nœuds capteurs.

En ce qui concerne GPSR (voir Tableau 4.6), la variation est probablement due à l'augmentation du degré [2] des nœuds, c.-à-d., $N(u)$ devient plus important et donc un nœud u a beaucoup plus de voisins candidats pour le prochain saut. Les nouveaux candidats pour le prochain saut peuvent être un facteur d'augmentation ou de diminution du PDR. Nous rappelons que l'augmentation du nombre de nœ]uds capteurs n'a pas d'impact significatif sur le nombre moyen de sauts générés par le GPSR puisque ce dernier continue à sélectionner les liaisons longue distance quelle que soit la densité du réseau (il favorise les voisins plus proches de la destination).

4.7 Conclusion

Dans ce dernier chapitre, nous avons présenté un protocole de surveillance inter-couches dédié aux zones sensibles clôturées sous des contraintes de terrain réalistes, tels que les obstacles et autres facteurs d'évanouissement de signal imprévisibles, par exemple les interférences, qui donnent naissance au phénomène de l'irrégularité de la radio. Le point clé du protocole de surveillance GPSR-SL proposé est qu'il est basé sur des algorithmes, qui prennent en compte le phénomène de l'irrégularité de la radio, en modélisant le graphe de connectivité réseau en tant que N-UDG. Les algorithmes en question sont l'algorithme d'identification des nœuds de bordure du RCSF et l'algorithme de routage des alertes vers le nœud puits. L'évaluation expérimentale démontre l'efficacité du GPSR-SL en termes de PDR, de consommation d'énergie et de délai de bout en bout lorsqu'il est comparé à son rival GPSR. En effet, les résultats montrent que le protocole proposé permet un PDR élevé sans augmenter la consommation d'énergie et en maintenant un délai de bout en bout acceptable pour l'application, et ce par rapport au GPSR original.

2. Ensemble des voisins d'un nœud

Conclusion et perspectives

Conclusion

Dans cette thèse, nous nous sommes intéressés aux problématiques de la consommation d'énergie et du routage réaliste dans les applications de surveillance des zones sensibles clôturées, à base des RCSFs avec cycle d'activité, et avec prise en compte des liens asymétriques dus au phénomène de l'irrégularité de la radio.

Après avoir introduit successivement le contexte, la problématique, la motivation et les objectifs de notre travail de recherche, nous avons présenté un état de l'art sur les RCSFs et un autre sur le routage dans ce type de réseaux, dans les Chapitres 1 et 2 respectivement. Dans le Chapitre 3, nous avons détaillé notre première contribution qui consiste en la proposition d'un protocole de routage géographique en mode *glouton*, inter-couches et basé sur un graphe de connectivité réseau modélisé comme un N-UDG. Le protocole en question, appelé CL-GR (Cross-Layer Greedy Routing), fournit deux stratégies d'acheminement d'un paquet à sa destination finale (sink), à savoir Progress towards the sink node through Symmetrical links that experience the lowest Path Loss (PSPL) et progress through symmetrical links, combining the Maximum Distance forwarding strategy and the PSPL (MDPSPL). Dans le Chapitre 4, nous avons abordé notre deuxième contribution consistant à proposer un protocole de surveillance pour les zones sensibles clôturées sous des contraintes de terrain réalistes, tels que les obstacles et autres facteurs d'évanouissement de signal imprévisibles, par exemple les interférences, qui donnent naissance au phénomène de l'irrégularité de la radio. Initialement, le protocole proposé identifie les nœuds de bordure du RCSF pour les utiliser comme nœuds sentinelles, c.-à-d., des nœuds qui sont toujours dans un état actif. Les nœuds restants sont utilisés en tant que nœuds relais avec un cycle d'activité, pendant la phase de routage des alertes vers le nœud puits. Les processus d'identification des nœuds de bordure et de routage des alertes sont assurés par le protocole Greedy Perimeter Stateless Routing through Symmetrical Links (GPSR-SL) qui est une version améliorée du protocole GPSR, reposant sur un graphe de connectivité représenté sous forme de disques non-unité (N-UDG).

Les résultats obtenus dans cette thèse sont très intéressants et ouvrent des perspectives très prometteuses de recherche dans le domaine du routage. Nous estimons avoir amélioré significativement l'état de l'art du routage géographique dédié aux RCSFs (les revues internationales de renommée dans lesquelles ont été publiées nos deux contributions en témoignent).

Cette thèse nous a permis d'enrichir nos connaissances scientifiques dans plusieurs domaines :

RCSFs/IoT, protocoles de communication (PHY, MAC, NET), simulation et évaluation des performances.

Nous tenons enfin à souligner le grand succès de déroulement de cette thèse, que ça soit en Algérie (Laboratoire RIIR) ou en France (LabSTICC), dans le cadre de la cotutelle entre l'Université Oran1 Ahmed Ben Bella et l'Université de Bretagne Occidentale (UBO). Cette expérience réussie incite sans doute à de futures collaborations scientifiques en matière de cotutelle et de co-encadrement entre les deux Universités.

Perspectives

Les perspectives immédiats de notre travail sont :

1. Validation expérimentale des résultats obtenus dans cette thèse à l'aide de bancs d'essai de capteurs réels.
2. Etude de l'impact de la mobilité (du sink par exemple) sur les contributions de cette thèse, c.à-d., comment les adapter à la mobilité.
3. Utilisation des UAVs pour améliorer la précision du système de surveillance des zones sensibles clôturées et les frontières internationales, en se basant sur le concept de coopération.

Publications internationales

[1] Ali Benzerbadj, Bouabdellah Kechar, Ahcène Bounceur, and Mohammad Hammoudeh. Surveillance of sensitive fenced areas using duty-cycled wireless sensor networks with asymmetrical links. *Journal of Network and Computer Applications*, 112 :41 – 52, 2018. 6

[2] Ali Benzerbadj, Bouabdellah Kechar, Ahcène Bounceur, and Bernard Pottier. Cross-layer greedy position-based routing for multihop wireless sensor networks in a real environment. *Ad Hoc Networks*, 71 :135 – 146, 2018. ix, 6, 34, 35, 36, 75

Communications internationales

[1] Ali Benzerbadj, Bouabdellah Kechar, Ahcène Bounceur, and Bernard Pottier. Energy efficient approach for surveillance applications based on self organized wireless sensor networks. *Procedia Computer Science*, 63 :165–170, 2015. The 6th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2015), Berlin, Germany, 27-30 Sep 2015. 3

[2] Ahcène Bounceur, Reinhardt Euler, Ali Benzerbadj, Farid Lalem, Massinissa Saoudi, Tahar Kechadi, and Marc Sevaux. Finding the polygon hull in wireless sensor networks. In *European Conference on Operational Research (EUROEURO conference), Invited talk*, University of Strathclyde, Glasgow, UK, 12-15 jul 2015.

[3] Ali Benzerbadj and Bouabdellah Kechar. Redundancy and criticality based scheduling in wireless video sensor networks for monitoring critical areas. *Procedia Computer Science*, 21 :234–241, 2013. The 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2013), Niagara Falls, Ontario, Canada, 21-24 Oct 2013. 3

[4] Ali Benzerbadj, Bouabdelah Kechar, and Mohamed Senouci. New approaches for calculating cover sets in wvsns for surveillance critical applications. In *Proceedings of the 1st International Conference on Distributed Systems and Decision (ICDSD'12)*, pages 94–99, Oran, Algeria, 21-22 Nov 2012.

Bibliographie

[1] MicaZ. The micaz is a 2.4 ghz mote module used for enabling low-power, wireless sensor networks. http://www.memsic.com/userfiles/files/Datasheets/WSN/micaz_datasheet-t.pdf, visité le 10.01.2018. ix, 15, vii, 13

[2] La Malfa S (2010). Wireless sensor networks. http://www.dees.unict.it/users/bando/files/wsn.pdf, visité le 23.03.2018. ix, 18, vii, 16

[3] Muhammad Imran, Abas Md Said, and Halabi Hasbullah. A survey of simulators, emulators and testbeds for wireless sensor networks. In *International Symposium on Information Technology (ITSim)*, volume 2, pages 897–902, Kuala Lumpur, Malaysia, 15-17 Jun 2010. IEEE. ix, 25, 26, vii, 23, 24

[4] Lim T Lee. Cross-layer design and optimization for wireless sensor networks. Technical report, Naval Postgraduate School Monterey CA, 2006. ix, 27, 35, 36, vii, 25, 32, 34

[5] Ali Benzerbadj, Bouabdellah Kechar, Ahcène Bounceur, and Bernard Pottier. Cross-layer greedy position-based routing for multihop wireless sensor networks in a real environment. *Ad Hoc Networks*, 71 :135–146, 2018. ix, 6, 34, 35, 36, 75, vii, 5, 32, 33, 67

[6] B Kechar, L Sekhri, and MK Rahmouni. CL-MAC : Energy efficient and low latency cross-layer mac protocol for delay sensitive wireless sensor network applications. *The Mediterranean Journal of Computers and Networks*, 6(1) :1–14, 2010. ix, 35, 36, vii, 33, 34

[7] Waltenegus Dargie and Christian Poellabauer. *Fundamentals of wireless sensor networks : theory and practice*. John Wiley & Sons, 2010. ISBN : 978-0-470-99765-9. ix, xi, 26, 29, 30, 32, 40, 48, 54, 57, 62, vii, 24, 27, 28, 37, 46, 52, 53

[8] Ivan Stojmenovic. *Handbook of sensor networks : algorithms and architectures*, volume 49. John Wiley & Sons, 2005. ISBN : 13 978-0-471-68472-5. ix, 29, 30, 56, 27, 28

[9] Young-Jin Kim, Ramesh Govindan, Brad Karp, and Scott Shenker. On the pitfalls of geographic face routing. In *Proceedings of the 2005 joint workshop on Foundations of mobile computing (DIALM-POMC '05)*, pages 34–43, Cologne, Germany, 02-02 Sep 2005. ACM. ix, 7, 64, 65, 66, 6, 54, 59

[10] Mauri Kuorilehto, Mikko Kohvakka, Jukka Suhonen, Panu Hämäläinen, Marko Hännikäinen, and Timo D Hamalainen. *Ultra-low energy wireless sensor networks in practice : Theory, realization and deployment*. John Wiley & Sons, 2008. ISBN : 978-0-470-05786-5. xi, 16, 32, 37, 38, 14, 30, 34, 35, 36

[11] Priyanka Rawat, Kamal Deep Singh, Hakima Chaouchi, and Jean Marie Bonnin. Wireless sensor networks : a survey on recent developments and potential synergies. *The Journal of Supercomputing*, 68(1) :1–48, 2014. xi, 1, 18, 20, 21, 23, 26, 27, 16, 19, 24, 25

[12] Theodore S Rappaport et al. *Wireless communications : principles and practice*, volume 2. prentice hall PTR New Jersey, 1996. ISBN : 9780133755367. xi, 40, 41, 72, 73, 97, 38, 39, 64, 65, 89

[13] Brad Karp and Hsiang-Tsung Kung. GPSR : Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 243–254, Boston, Massachusetts, USA, 06-11 Aug 2000. ACM. xi, 6, 8, 9, 54, 55, 57, 58, 59, 72, 75, 94, vii, viii, 52, 53, 64, 67, 86, 89, 93

[14] Mohammad Ilyas. *The handbook of ad hoc wireless networks*. CRC press, 2002. ISBN : 0-8493-1332-5. 1

[15] Stefano Basagni, Marco Conti, Silvia Giordano, and Ivan Stojmenovic. *Mobile ad hoc networking*. John Wiley & Sons, 2004. ISBN : 0-471-37313-3. 1

[16] Subir Kumar Sarkar, TG Basavaraju, and C Puttamadappa. *Ad hoc mobile wireless networks : principles, protocols and applications*. CRC Press, 2007. ISBN : 9781420062212. 1

[17] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. Wireless sensor networks : a survey. *Computer networks*, 38(4) :393–422, 2002. 1, 18, 21, 23, 50, 51, 60, 16, 19, 48, 49, 55

[18] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer networks*, 52(12) :2292–2330, 2008. 1, 18, 19, 21, 22, 23, 26, 32, 16, 17, 20, 24, 30

[19] Eleonora Borgia. The internet of things vision : Key features, applications and open issues. *Computer Communications*, 54 :1–31, 2014. 1, 38, 36

[20] Shuang-Hua Yang. Internet of things. In *Wireless Sensor Networks*, pages 247–261. Springer, 2014. 1, 38, 36

[21] Luca Mainetti, Luigi Patrono, and Antonio Vilei. Evolution of wireless sensor networks towards the internet of things : A survey. In *Proceedings of the 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2011)*, pages 1–6, Split, Croatia, 15-17 Sep 2011. IEEE. 1

[22] Youngsoo Kim, Jonggu Kang, Daeyoung Kim, Eunjo Kim, Poh Kit Chong, and Suckbin Seo. Design of a fence surveillance system based on wireless sensor networks. In *Proceedings of the 2nd International Conference on Autonomic Computing and Communication Systems (Autonomics '08)*, page 4, Turin, Italy, 23-25 Sep 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). 2, 94, 1, 86

[23] Zhi Sun, Pu Wang, Mehmet C Vuran, Mznah A Al-Rodhaan, Abdullah M Al-Dhelaan, and Ian F Akyildiz. Bordersense : Border patrol through advanced wireless sensor networks. *Ad Hoc Networks*, 9(3) :468–477, 2011. 2, 94, 1, 86

[24] Peter Rothenpieler, Daniela Krüger, Dennis Pfisterer, Stefan Fischer, Denise Dudek, Christian Haas, Andreas Kuntz, and Martina Zitterbart. Flegsens-secure area monitoring using wireless sensor networks. *Proceedings of the 4th Safety and Security Systems in Europe*, pages 136–139, 2009. 2, 95, 1, 87

[25] Rabun Kosar, Ilir Bojaxhiu, Ertan Onur, and Cem Ersoy. Lifetime extension for surveillance wireless sensor networks with intelligent redeployment. *Journal of network and computer applications*, 34(6) :1784–1793, 2011. 2, 95, 1, 87

[26] Hoda Sharei-Amarghan, Alireza Keshavarz-Haddad, and Gaëtan Garraux. Routing protocols for border surveillance using zigbee-based wireless sensor networks. In *International Conference on Computer Networks*, pages 114–123. Springer, 2013. 2, 95, 1, 87

[27] Ramzi Bellazreg, Noureddine Boudriga, and Sunshin An. Border surveillance using sensor based thick-lines. In *Proceedings of the International Conference on Information Networking 2013 (ICOIN)*, pages 221–226, Bangkok, Thailand, 28-30 Jan 2013. IEEE. 2, 96, 1, 88

[28] Mohammad Hammoudeh, Fayez Al-Fayez, Huw Lloyd, Robert Newman, Bamidele Adebisi, Ahcène Bounceur, and Abdelrahman Abuarqoub. A wireless sensor network border monitoring system : Deployment issues and routing protocols. *IEEE Sensors Journal*, 17(8) :2572–2582, 2017. 2, 96, 1, 88

[29] Tian He, Sudha Krishnamurthy, John A Stankovic, Tarek Abdelzaher, Liqian Luo, Radu Stoleru, Ting Yan, Lin Gu, Jonathan Hui, and Bruce Krogh. Energy-efficient surveillance system using wireless sensor networks. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services (MobiSys '04)*, pages 270–283, Boston, MA, USA, 06-09 Jun 2004. ACM. 2, 1

[30] Gang Zhou, Tian He, Sudha Krishnamurthy, and John A Stankovic. Impact of radio irregularity on wireless sensor networks. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services (MobiSys '04)*, pages 125–138, Boston, MA, USA, 06-09 Jun 2004. ACM. 2, 3, 5, 13, 40, 45, 52, 71, 73, 76, 98, 4, 11, 38, 43, 50, 63, 65, 68, 91

[31] Gang Zhou, Tian He, Sudha Krishnamurthy, and John A Stankovic. Models and solutions for radio irregularity in wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 2(2) :221–262, 2006. 2, 3, 5, 13, 40, 45, 52, 71, 93, 4, 11, 38, 43, 50, 63, 85

[32] Ivan Stojmenovic. Position-based routing in ad hoc networks. *Communications Magazine, IEEE*, 40(7) :128–134, 2002. 2, 52, 71, 50, 63

[33] Martin Mauve, Jorg Widmer, and Hannes Hartenstein. A survey on position-based routing in mobile ad hoc networks. *IEEE network*, 15(6) :30–39, 2001. 2, 3, 52, 71, 50, 63

[34] Fraser Cadger, Kevin Curran, Jose Santos, and Sandra Moffett. A survey of geographical routing in wireless ad-hoc networks. *IEEE Communications Surveys & Tutorials*, 15(2) :621–653, 2013. 2, 3, 52, 71, 50, 63

[35] Ali Benzerbadj and Bouabdellah Kechar. Redundancy and criticality based scheduling in wireless video sensor networks for monitoring critical areas. *Procedia Computer Science*, 21 :234–241, 2013. The 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2013), Niagara Falls, Ontario, Canada, 21-24 Oct 2013. 3

[36] Ali Benzerbadj, Bouabdellah Kechar, Ahcène Bounceur, and Bernard Pottier. Energy efficient approach for surveillance applications based on self organized wireless sensor networks. *Procedia Computer Science*, 63 :165–170, 2015. The 6th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2015), Berlin, Germany, 27-30 Sep 2013. 3

[37] Julio C Navas and Tomasz Imielinski. Geocast—geographic addressing and routing. In *Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking (MobiCom '97)*, pages 66–76, Budapest, Hungary, 26-30, Sept 1997. ACM. 3

[38] Jeffrey Hightower and Gaetano Borriello. Location systems for ubiquitous computing. *Computer*, 34(8) :57–66, 2001. 3, 52, 74, 97, 50, 66, 89

[39] Fabian Kuhn, Roger Wattenhofer, and Aaron Zollinger. Ad hoc networks beyond unit disk graphs. *Wireless Networks*, 14(5) :715–729, 2008. 3, 5, 13, 40, 52, 71, 4, 11, 38, 50, 63

[40] Ian F Akyildiz and Mehmet Can Vuran. *Wireless sensor networks*, volume 4. John Wiley & Sons, 2010. ISBN : 978-0-470-03601-3. 3, 27, 33, 40, 45, 46, 25, 30, 31, 37, 38, 43, 44

[41] Karim Seada, Ahmed Helmy, and Ramesh Govindan. Modeling and analyzing the correctness of geographic face routing under realistic conditions. *Ad Hoc Networks*, 5(6) :855–871, 2007. 5, 7, 13, 52, 64, 71, 4, 6, 11, 50, 54, 59, 63

[42] Marco Zúñiga Zamalloa, Karim Seada, Bhaskar Krishnamachari, and Ahmed Helmy. Efficient geographic routing over lossy links in wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 4(3) :12, 2008. 5, 13, 52, 71, 73, 75, 4, 11, 50, 63, 65, 67

[43] Karim Seada, Marco Zuniga, Ahmed Helmy, and Bhaskar Krishnamachari. Energy-efficient forwarding strategies for geographic routing in lossy wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems (SenSys '04)*, pages 108–121, Baltimore, MD, USA, 03-05 Nov 2004. ACM. 5, 13, 52, 71, 73, 75, 4, 11, 50, 63, 65, 67

[44] Christian Lochert, Martin Mauve, Holger Füßler, and Hannes Hartenstein. Geographic routing in city scenarios. *ACM SIGMOBILE mobile computing and communications review*, 9(1) :69–72, 2005. 5, 13, 52, 71, 4, 11, 50, 63

[45] Young-Jin Kim Ramesh Govindan, Brad Karp, and Scott Shenker. Lazy cross-link removal for geographic routing. In *Proceedings of the 4th international conference on Embedded networked sensor systems (SenSys '06)*, pages 112–124, Boulder, Colorado, USA, 31 Oct-03 Nov 2006. ACM. 5, 13, 52, 65, 71, 99, 4, 11, 50, 59, 63, 92

[46] Young-Jin Kim, Ramesh Govindan, Brad Karp, and Scott Shenker. Geographic routing made practical. In *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2 (NSDI'05)*, pages 217–230, USENIX Association Berkeley, CA, USA, 02-04 May 2005. USENIX Association. 5, 13, 52, 55, 71, 4, 11, 50, 53, 63

[47] Lali Barriere, Pierre Fraigniaud, Lata Narayanan, and Jaroslav Opatrny. Robust position-based routing in wireless ad hoc networks with irregular transmission ranges. *Wireless Communications and Mobile Computing*, 3(2) :141–153, 2003. 5, 13, 52, 71, 4, 11, 50, 63

[48] Sanjay Shakkottai, Theodore S Rappaport, and Peter C Karlsson. Cross-layer design for wireless networks. *IEEE Communications magazine*, 41(10) :74–80, 2003. 5, 13, 14, 21, 34, 4, 11, 12, 19, 31

[49] Tommaso Melodia, Mehmet C Vuran, and Dario Pompili. The state of the art in cross-layer design for wireless sensor networks. In *International workshop of the EuroNGI network of excellence*, pages 78–92. Springer, 2005. 5, 14, 21, 27, 34, 12, 19, 25, 31

[50] Rajeev Ranjan and Shirshu Varma. Challenges and implementation on cross layer design for wireless sensor networks. *Wireless personal communications*, 86(2) :1037–1060, 2016. 5, 14, 21, 34, 12, 19, 31

[51] Bo Fu, Yang Xiao, Hongmei Deng, and Hui Zeng. A survey of cross-layer designs in wireless networks. *IEEE Communications Surveys & Tutorials*, 16(1) :110–126, 2014. 5, 14, 21, 34, 12, 19, 31, 32

[52] Vineet Srivastava and Mehul Motani. Cross-layer design : a survey and the road ahead. *IEEE Communications Magazine*, 43(12) :112–119, 2005. 5, 14, 21, 34, 12, 19, 31, 32

[53] Vijay T Raisinghani and Sridhar Iyer. Cross-layer design optimizations in wireless protocol stacks. *Computer Communications*, 27(8) :720–724, 2004. 5, 14, 21, 34, 12, 19, 31

[54] Milan Lukic, Bogdan Pavkovic, Nathalie Mitton, and Ivan Stojmenovic. Greedy geographic routing algorithms in real environment. In *Proceedings of the Fifth International Conference on Mobile Ad-hoc and Sensor Networks (MSN' 09)*, pages 86–93, Fujian, China, 14-16 Dec 2009. IEEE. 6, 8, 34, 72, 73, 75, 81, 32, 64, 65, 67

[55] Ali Benzerbadj, Bouabdellah Kechar, Ahcène Bounceur, and Mohammad Hammoudeh. Surveillance of sensitive fenced areas using duty-cycled wireless sensor networks with asymmetrical links. *Journal of Network and Computer Applications*, 112 :41–52, 2018. 6

[56] Young-Jin Kim, Ramesh Govindan, Brad Karp, and Scott Shenker. Practical and robust geographic routing in wireless networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems (SenSys '04)*, pages 295–296, Baltimore, MD, USA, 03-05 Nov 2004. ACM. 7, 65, 6, 59

[57] Douglas SJ De Couto, Daniel Aguayo, John Bicket, and Robert Morris. A high-throughput path metric for multi-hop wireless routing. *Wireless Networks*, 11(4) :419–434, 2005. 13, 71, 73, 11, 63, 65

[58] Holger Karl and Andreas Willig. *Protocols and architectures for wireless sensor networks*. John Wiley & Sons, 2007. ISBN : 13 978-0-470-09510-2. 15, 41, 42, 47, 13, 39, 45

[59] Nawel Bendimerad. *Système de surveillance d'infrastructures publiques à l'aide des réseaux de capteurs vidéo sans fil*. Thèse de doctorat, Université d'Oran 1 Ahmed Ben Bella, 2015. 15, 13

[60] Andreas Willig. Wireless sensor networks : concept, challenges and approaches. *e & i Elektrotechnik und Informationstechnik*, 123(6) :224–231, 2006. 16, 18, 19, 14, 17

[61] Faisal Karim Shaikh and Sherali Zeadally. Energy harvesting in wireless sensor networks : A comprehensive review. *Renewable and Sustainable Energy Reviews*, 55 :1041–1054, 2016. 16, 14

[62] Chee-Yee Chong and Srikanta P Kumar. Sensor networks : evolution, opportunities, and challenges. *Proceedings of the IEEE*, 91(8) :1247–1256, 2003. 18, 16

[63] David Culler, Deborah Estrin, and Mani Srivastava. Guest editors' introduction : Overview of sensor networks. *Computer*, 37(8) :41–49, 2004. 18, 16

[64] Luca Benini, Elisabetta Farella, and Carlotta Guiducci. Wireless sensor networks : Enabling technology for ambient intelligence. *Microelectronics journal*, 37(12) :1639–1649, 2006. 18, 16

[65] Chiara Buratti, Andrea Conti, Davide Dardari, and Roberto Verdone. An overview on wireless sensor networks technology and evolution. *Sensors*, 9(9) :6869–6896, 2009. 18, 16

[66] Giuseppe Anastasi, Marco Conti, Mario Di Francesco, and Andrea Passarella. Energy conservation in wireless sensor networks : A survey. *Ad hoc networks*, 7(3) :537–568, 2009. 18, 21, 16

[67] Abdul Waheed Khan, Abdul Hanan Abdullah, Mohammad Hossein Anisi, and Javed Iqbal Bangash. A comprehensive study of data collection schemes using mobile sinks in wireless sensor networks. *Sensors*, 14(2) :2510–2548, 2014. 18, 16

[68] Isabel Dietrich and Falko Dressler. On the lifetime of wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 5(1) :5, 2009. 18, 16

[69] Nirupama Bulusu, John Heidemann, and Deborah Estrin. Gps-less low-cost outdoor localization for very small devices. *Personal Communications, IEEE*, 7(5) :28–34, 2000. 18, 52, 74, 97, 16, 50, 66, 89

[70] Andreas Savvides, Chih-Chieh Han, and Mani B Strivastava. Dynamic fine-grained localization in ad-hoc networks of sensors. In *Proceedings of the 7th annual international conference on Mobile computing and networking (MobiCom '01)*, pages 166–179, Rome, Italy, 2001. ACM. 18, 52, 74, 97, 16, 50, 66, 89

[71] Azzedine Boukerche, Horacio ABF Oliveira, Eduardo F Nakamura, and Antonio AF Loureiro. Localization systems for wireless sensor networks. *wireless Communications, IEEE*, 14(6) :6–12, 2007. 18, 52, 74, 97, 16, 50, 66, 89

[72] Guangjie Han, Huihui Xu, Trung Q Duong, Jinfang Jiang, and Takahiro Hara. Localization algorithms of wireless sensor networks : a survey. *Telecommunication Systems*, 52(4) :2419–2436, 2013. 18, 52, 74, 97, 16, 50, 66, 89

[73] Bouabdellah Kechar. *Problématique de la consommation d'énergie dans les réseaux de capteurs sans fil.* Thèse de doctorat, Université d'Oran 1 Ahmed Ben Bella, 2010. 19, 17

[74] L Krishnamachari, Deborah Estrin, and Stephen Wicker. The impact of data aggregation in wireless sensor networks. In *Proceedings of the 22nd International Conference on Distributed Computing Systems Workshops*, pages 575–578, Vienna, Austria, 2-5 Jul 2002. IEEE. 19, 17

[75] Ian F Akyildiz and Erich P Stuntebeck. Wireless underground sensor networks : Research challenges. *Ad Hoc Networks*, 4(6) :669–686, 2006. 21, 19

[76] John Heidemann, Yuan Li, Affan Syed, Jack Wills, and Wei Ye. Underwater sensor networking : Research challenges and potential applications. *Proceedings of the Technical Report ISI-TR-2005-603, USC/Information Sciences Institute*, 2005. 22, 20

[77] Ian F Akyildiz, Dario Pompili, and Tommaso Melodia. Challenges for efficient communication in underwater acoustic sensor networks. *ACM Sigbed Review*, 1(2) :3–8, 2004. 22, 20

[78] Ian F Akyildiz, Tommaso Melodia, and Kaushik R Chowdhury. A survey on wireless multimedia sensor networks. *Computer networks*, 51(4) :921–960, 2007. 22, 20

[79] Streetline – connecting the real world. http://www.streetline.com, visité le 04.01.2018. 23, 21

[80] J. Markoff. "can't find a parking spot ? check smartphone". http://www.nytimes.com/2008/07/12/business/12newpark.html, visité 04.01.2018. 23, 21

[81] Muhammad Omer Farooq and Thomas Kunz. Operating systems for wireless sensor networks : A survey. *Sensors*, 11(6) :5900–5930, 2011. 23, 21

[82] Habib M Ammari. *The art of wireless sensor networks.* Springer, 2014. ISBN : 978-3-642-40008-7. 23, 24, 21, 22

[83] Sudip Misra, Isaac Zhang, and Subhas Chandra Misra. *Guide to wireless sensor networks.* Springer Science & Business Media, 2009. ISBN :978-1-84882-217-7. 23, 32, 47, 21, 30, 45

[84] Philip Levis, Sam Madden, Joseph Polastre, Robert Szewczyk, Kamin Whitehouse, Alec Woo, David Gay, Jason Hill, Matt Welsh, Eric Brewer, et al. Tinyos : An operating system for sensor networks. *Ambient intelligence*, 35 :115–148, 2005. 23, 24, 21, 22

[85] Tobias Reusing. Comparison of operating systems tinyos and contiki. *Sens. Nodes-Operation, Netw. Appli.(SN)*, 7 :7–13, 2012. 23, 21

[86] David Gay, Philip Levis, Robert Von Behren, Matt Welsh, Eric Brewer, and David Culler. The nesc language : A holistic approach to networked embedded systems. *Acm Sigplan Notices*, 49(4) :41–51, 2014. 24

[87] Philip Levis, Nelson Lee, Matt Welsh, and David Culler. Tossim : Accurate and scalable simulation of entire tinyos applications. In *Proceedings of the 1st international conference on Embedded networked sensor systems (SenSys '03)*, pages 126–137, Los Angeles, California, USA, 05-07 Nov 2003. ACM. 24, 26, 22

[88] Chih-Chieh Han, Ram Kumar, Roy Shea, Eddie Kohler, and Mani Srivastava. A dynamic operating system for sensor nodes. In *Proceedings of the 3rd international conference on Mobile systems, applications, and services (MobiSys '05)*, pages 163–176, Seattle, Washington, USA, 06-08 Jun 2005. ACM. 24, 22

[89] Yale University. The xyz sensor node, an open source wireless sensing platform developed at enalab, yale university. http://www.cs.yale.edu/enalab/XYZ/, visité le 21.01.2018. 24, 22

[90] Shah Bhatti, James Carlson, Hui Dai, Jing Deng, Jeff Rose, Anmol Sheth, Brian Shucker, Charles Gruenwald, Adam Torgerson, and Richard Han. Mantis os : An embedded multithreaded operating system for wireless micro sensor platforms. *Mobile Networks and Applications*, 10(4) :563–579, 2005. 24, 22

[91] Avrora. The avr simulation and analysis framework. http://http://compilers.cs.ucla.edu/avrora/, visité le 19.01.2018. 24, 22

[92] Adam Dunkels. Full tcp/ip for 8-bit architectures. In *Proceedings of the 1st international conference on Mobile systems, applications and services (MobiSys '03)*, pages 85–98, San Francisco, California, USA, 05-08 May 2003. ACM. 24, 22

[93] Zach Shelby and Carsten Bormann. *6LoWPAN : The wireless embedded Internet*. John Wiley & Sons, 2011. ISBN : 9780470747995. 24, 22

[94] Cooja. Wsn simulator using the contiki operating system. http://www.contiki-os.org, visité le 20.01.2018. 25, 26, 23, 24

[95] Fredrik Osterlind, Adam Dunkels, Joakim Eriksson, Niclas Finne, and Thiemo Voigt. Cross-level sensor network simulation with cooja. In *Proceedings of the 31st IEEE Conference on Local Computer Networks*, pages 641–648, Tampa, FL, USA, 14-16 Nov 2006. IEEE. 25, 26, 23, 24

[96] Bartosz Musznicki and Piotr Zwierzykowski. Survey of simulators for wireless sensor networks. *International Journal of Grid and Distributed Computing*, 5(3) :23–50, 2012. 25, 23

[97] Jens Horneber and Anton Hergenröder. A survey on testbeds and experimentation environments for wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 16(4) :1820–1838, 2014. 25, 23

[98] Leon P Steyn and Gerhard P Hancke. A survey of wireless sensor network testbeds. In *AFRICON, 2011*, pages 1–6, Livingstone, Zambia, 13-15 Sep 2011. IEEE. 25, 23

[99] Wolfgang Kiess and Martin Mauve. A survey on real-world implementations of mobile ad-hoc networks. *Ad Hoc Networks*, 5(3) :324–339, 2007. 25, 23

[100] NS-2. The network Simulator ns-2. https://www.isi.edu/nsnam/ns/, visité le 01.03.2018. 26, 24

[101] NS-3. The network Simulator ns-3. https://www.nsnam.org/, visité le 01.03.2018. 26, 24

[102] OMNeT++. Discrete Event Simulator. http://www.omnetpp.org, visité le 04.01.2018. 26, 80, 104, 24, 72, 96

[103] J-Sim. Java-based simulation system. https://sites.google.com/site/jsimofficial/,https://sites.google.com/site/jsimofficial/, visité le 01.03.2018. 26, 24

[104] MATLAB. Language of technical computing. http://www.mathworks.com/products/matlab/, visité le 01.03.2018. 26, 24

[105] Ptolemy II. Heterogeneous modeling and design. http://ptolemy.eecs.berkeley.edu/ptolemyII/, visité le 01.03.2018. 26, 24

[106] SensorSim. Sensor simulator built on ns-2. https://github.com/openintents/sensorsimulator, visité le 01.03.2018. 26, 24

[107] Castalia. An OMNeT-based simulator for low-power wireless networks. https://github.com/boulis/Castalia, visité le 04.01.2018. 26, 32, 40, 77, 80, 104, 24, 30, 38, 69, 72, 96

[108] VisualSense. Component-based modeling and simulation framework built on ptolemy ii for wsns. https://ptolemy.eecs.berkeley.edu/visualsense/, visité le 01.03.2018. 26, 24

[109] Mobility Framework. A framework to support simulations of wireless and mobile networks within omnet++. http://mobility-fw.sourceforge.net/, visité le 01.03.2018. 26, 24

[110] MIXIM. Mixed simulator. http://mixim.sourceforge.net/, visité le 01.03.2018. 26, 24

[111] CupCarbon. A Smart City and IoT Wireless Sensor Network Simulator. http://www.cupcarbon.com, visité le 04.01.2018. 26, 24

[112] Prowler. Probabilistic wireless network simulator. http://www.isis.vanderbilt.edu/projects/nest/prowler/, visité le 04.03.2018. 26, 24

[113] JProwler. Java-based probabilistic wireless network simulator. http://w3.isis.vanderbilt.edu/projects/nest/jprowler/, visité le 04.03.2018. 26, 24

[114] Jonathan Polley, Dionysus Blazakis, Jonathan McGee, Daniel Rusk, and John S Baras. Atemu : a fine-grained sensor network simulator. In *Proceedings of the First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, SECON 2004*, pages 145–152, Santa Clara, CA, USA, 4-7 Oct 2004. IEEE. 26, 24

[115] Ben L Titzer, Daniel K Lee, and Jens Palsberg. Avrora : Scalable sensor network simulation with precise timing. In *Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005)*, pages 477–482, Boise, ID, USA, 15-15 Apr 2005. IEEE. 26, 24

[116] Lewis Girod, Jeremy Elson, Alberto Cerpa, Thanos Stathopoulos, Nithya Ramanathan, and Deborah Estrin. Emstar : A software environment for developing and deploying wireless sensor networks. In *USENIX Annual Technical Conference, General Track*, pages 283–296, 2004. 26, 24

[117] Rohan Narayana Murty, Geoffrey Mainland, Ian Rose, Atanu Roy Chowdhury, Abhimanyu Gosain, Josh Bers, and Matt Welsh. Citysense : An urban-scale wireless sensor network and testbed. In *Proceedings of IEEE Conference on Technologies for Homeland Security*, pages 583–588, Waltham, MA, USA, 12-13 May 2008. IEEE. 27, 25

[118] Geoffrey Werner-Allen, Patrick Swieskowski, and Matt Welsh. Motelab : A wireless sensor network testbed. In *Proceedings of the 4th international symposium on Information processing in sensor networks (IPSN '05)*, page 68, Los Angeles, California, USA, 24-27 Apr 2005. IEEE Press. 27, 25

[119] David Johnson, Tim Stack, Russ Fish, Daniel Montrallo Flickinger, Leigh Stoller, Robert Ricci, and Jay Lepreau. Mobile emulab : A robotic wireless and sensor network testbed. In *Proceedings of the 25th IEEE International Conference on Computer Communications*, pages 1–12. IEEE, 2006. 27, 25

[120] Dipankar Raychaudhuri, Ivan Seskar, Max Ott, Sachin Ganu, Kishore Ramachandran, Haris Kremo, Robert Siracusa, Hang Liu, and Manpreet Singh. Overview of the orbit radio grid testbed for evaluation of next-generation wireless network protocols. In *Proceedings of Wireless Communications and Networking Conference, 2005 IEEE*, volume 3, pages 1664–1669, New Orleans, LA, USA, 13-17 Mar 2005. IEEE. 27, 25

[121] ORBIT. Open-access Research Testbed for Next-Generation Wireless Networks. http://www.orbit-lab.org/, visité le 06.01.2018. 27, 25

[122] SensLAB. Senslab : very large scale open wireless sensor network testbed. http://www.senslab.info/, visité le 06.01.2018. 27, 25

[123] Olof Rensfelt, Frederik Hermans, Per Gunningberg, Lars-Åke Larzon, and Erik Björnemo. Repeatable experiments with mobile nodes in a relocatable wsn testbed. *The Computer Journal*, 54(12) :1973–1986, 2011. 27, 25

[124] Lucas DP Mendes and Joel JPC Rodrigues. A survey on cross-layer solutions for wireless sensor networks. *Journal of Network and Computer Applications*, 34(2) :523–534, 2011. 27, 34, 25, 32

[125] Fatima Zahra Djiroun and Djamel Djenouri. Mac protocols with wake-up radio for wireless sensor networks : A review. *IEEE Communications Surveys & Tutorials*, 19(1) :587–618, 2017. 29, 27

[126] Norman Abramson. The aloha system : another alternative for computer communications. In *Proceedings of the November 17-19, 1970, fall joint computer (AFIPS '70 (Fall))*, pages 281–285, Houston, Texas, USA, 17-19 Nov 1970. ACM. 29, 27

[127] Lawrence G Roberts. Aloha packet system with and without slots and capture. *ACM SIGCOMM Computer Communication Review*, 5(2) :28–42, 1975. 29, 27

[128] Leonard Kleinrock and Fouad Tobagi. Packet switching in radio channels : Part i–carrier sense multiple-access modes and their throughput-delay characteristics. *IEEE transactions on Communications*, 23(12) :1400–1416, 1975. 29, 27

[129] Phil Karn et al. Maca-a new channel access method for packet radio. In *ARRL/CRRL Amateur radio 9th computer networking conference*, volume 140, pages 134–140, 1990. 29, 27

[130] Vaduvur Bharghavan, Alan Demers, Scott Shenker, and Lixia Zhang. Macaw : a media access protocol for wireless lan's. *ACM SIGCOMM Computer Communication Review*, 24(4) :212–225, 1994. 29, 27

[131] Wei Ye, John Heidemann, and Deborah Estrin. An energy-efficient mac protocol for wireless sensor networks. In *Proceedings of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 3, pages 1567–1576, New York, NY, USA, 23-27 Jun 2002. IEEE. 29, 32, 27, 30

[132] Tijs Van Dam and Koen Langendoen. An adaptive energy-efficient mac protocol for wireless sensor networks. In *Proceedings of the 1st international conference on Embedded networked sensor systems (SenSys '03)*, pages 171–180, Los Angeles, California, USA, 05-07 Nov 2003. ACM. 29, 32, 27, 30

[133] Joseph Polastre, Jason Hill, and David Culler. Versatile low power media access for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems (SenSys '04)*, pages 95–107, Baltimore, MD, USA, 03-05 Nov 2004. ACM. 30, 32, 98, 103, 28, 91, 96

[134] Michael Buettner, Gary V Yee, Eric Anderson, and Richard Han. X-mac : a short preamble mac protocol for duty-cycled wireless sensor networks. In *Proceedings of the 4th international conference on Embedded networked sensor systems (SenSys '06)*, pages 307–320, Boulder, Colorado, USA, 31 Oct-03 Nov 2006. ACM. 30, 32, 82, 28, 74

[135] Curt Schurgers, Vlasios Tsiatsis, Saurabh Ganeriwal, and Mani Srivastava. Topology management for sensor networks : Exploiting latency and density. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing (MobiHoc '02)*, pages 135–145, Lausanne, Switzerland, 09-11 Jun 2002. ACM. 30, 28

[136] Gang Lu, Bhaskar Krishnamachari, and Cauligi S Raghavendra. Performance evaluation of the ieee 802.15. 4 mac for low-rate low-power wireless networks. In *Proceedings of IEEE International Conference on Performance, Computing, and Communications*, pages 701–706, Phoenix, AZ, USA, 15-17 Apr 2004. IEEE. 30, 28

[137] Ed Callaway, Paul Gorday, Lance Hester, Jose A Gutierrez, Marco Naeve, Bob Heile, and Venkat Bahl. Home networking with ieee 802.15. 4 : a developing standard for low-rate wireless personal area networks. *IEEE Communications magazine*, 40(8) :70–77, 2002. 30, 28

[138] Injong Rhee, Ajit Warrier, Mahesh Aia, Jeongki Min, and Mihail L Sichitiu. Z-mac : a hybrid mac for wireless sensor networks. *IEEE/ACM Transactions on Networking (TON)*, 16(3) :511–524, 2008. 30, 28

[139] Ilker Demirkol, Cem Ersoy, and Fatih Alagoz. Mac protocols for wireless sensor networks : a survey. *IEEE Communications Magazine*, 44(4) :115–121, 2006. 30, 28

[140] Pei Huang, Li Xiao, Soroor Soltani, Matt W Mutka, and Ning Xi. The evolution of mac protocols in wireless sensor networks : A survey. *IEEE communications surveys & tutorials*, 15(1) :101–120, 2013. 30, 28

[141] Amre El-Hoiydi. Aloha with preamble sampling for sporadic traffic in ad hoc wireless sensor networks. In *Proceedings of 2002 IEEE International Conference on Communications*, volume 5, pages 3418–3423, New York, NY, USA, 28 Apr-2 May 2002. IEEE. 32, 29

[142] Matthew J Miller and Nitin H Vaidya. A mac protocol to reduce sensor network energy consumption using a wakeup radio. *IEEE Transactions on mobile Computing*, 4(3) :228–242, 2005. 32, 29

[143] Ricardo C Carrano, Diego Passos, Luiz CS Magalhaes, and Celio VN Albuquerque. Survey and taxonomy of duty cycling mechanisms in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 16(1) :181–194, 2014. 32, 30

[144] Chonggang Wang, Kazem Sohraby, Bo Li, Mahmoud Daneshmand, and Yueming Hu. A survey of transport protocols for wireless sensor networks. *IEEE network*, 20(3) :34–40, 2006. 33, 30, 31

[145] Ahmad Al Hanbali, Eitan Altman, and Philippe Nain. A survey of tcp over ad hoc networks. *IEEE Communications Surveys & Tutorials*, 7(3) :22–36, 2005. 33, 31

[146] Sunil Kulkarni, Aravind Iyer, and Catherine Rosenberg. An address-light, integrated mac and routing protocol for wireless sensor networks. *IEEE/ACM Transactions on networking*, 14(4) :793–806, 2006. 34, 32

[147] Mehmet C Vuran and Ian F Akyildiz. Xlp : A cross-layer protocol for efficient communication in wireless sensor networks. *IEEE transactions on mobile computing*, 9(11) :1578–1591, 2010. 34, 36, 32, 33

[148] Laura Galluccio, Alessandro Leonardi, Giacomo Morabito, and Sergio Palazzo. A mac/-routing cross-layer approach to geographic forwarding in wireless sensor networks. *Ad hoc networks*, 5(6) :872–884, 2007. 34, 32

[149] Jae Young Choi, Hyung Seok Kim, Iljoo Baek, and Wook Hyun Kwon. Cell based energy density aware routing : a new protocol for improving the lifetime of wireless sensor networks. *Computer Communications*, 28(11) :1293–1302, 2005. 34, 32

[150] Yong Yuan, Zongkai Yang, Zhihai He, and Jianhua He. An integrated energy aware wireless transmission system for qos provisioning in wireless sensor network. *Computer Communications*, 29(2) :162–172, 2006. 34, 32

[151] Hang Su and Xi Zhang. Battery-dynamics driven tdma mac protocols for wireless body-area monitoring networks in healthcare applications. *IEEE Journal on selected areas in communications*, 27(4), 2009. 34, 32

[152] Changsu Suh, Young-Bae Ko, and Dong-Min Son. An energy efficient cross-layer mac protocol for wireless sensor networks. In *Proceedings of Asia-Pacific Web Conference*, pages 410–419. Springer, 2006. 35, 32

[153] John A Stankovic, TE Abdelzaher, Chenyang Lu, Lui Sha, and Jennifer C Hou. Real-time communication and coordination in embedded sensor networks. *Proceedings of the IEEE*, 91(7) :1002–1022, 2003. 38, 36

[154] Delphine Christin, Andreas Reinhardt, Parag S Mogre, Ralf Steinmetz, et al. Wireless sensor networks and the internet of things : selected challenges. *Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose sensornetze*, pages 31–34, 2009. 38, 36

[155] Rodrigo Roman and Javier Lopez. Integrating wireless sensor networks and the internet : a security analysis. *Internet Research*, 19(2) :246–259, 2009. 39, 36

[156] Adam Dunkels, Juan Alonso, Thiemo Voigt, Hartmut Ritter, and Jochen Schiller. Connecting wireless sensornets with tcp/ip networks. In *Proceedings of International Conference on Wired/Wireless Internet Communications (WWIC 2004)*, pages 143–152. Springer, 2004. 39, 36

[157] Cristina Alcaraz, Pablo Najera, Javier Lopez, and Rodrigo Roman. Wireless sensor networks and the internet of things : Do we need a complete integration ? In *1st International Workshop on the Security of the Internet of Things (SecIoT'10)*, Tokyo, Japan, 2010. 39, 36

[158] Kun Yang. *Wireless sensor networks*. Springer, 2014. ISBN : 978-1-4471-5504-1. 39, 36, 37

[159] Jamal N Al-Karaki and Ahmed E Kamal. Routing techniques in wireless sensor networks : a survey. *IEEE wireless communications*, 11(6) :6–28, 2004. 46, 50, 44, 48

[160] Kemal Akkaya and Mohamed Younis. A survey on routing protocols for wireless sensor networks. *Ad hoc networks*, 3(3) :325–349, 2005. 46, 44

[161] Eylem Ekici, Yaoyao Gu, and Doruk Bozdag. Mobility-based communication in wireless sensor networks. *IEEE Communications Magazine*, 44(7) :56–62, 2006. 47, 45

[162] Suresh Singh, Mike Woo, and Cauligi S Raghavendra. Power-aware routing in mobile ad hoc networks. In *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking (MobiCom '98)*, pages 181–190, Dallas, Texas, USA, 25-30 Oct 1998. ACM. 49, 47

[163] Wendi Rabiner Heinzelman, Joanna Kulik, and Hari Balakrishnan. Adaptive protocols for information dissemination in wireless sensor networks. In *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking (MobiCom '99)*, pages 174–185, Seattle, Washington, USA, 15-19 Aug 1999. ACM. 50, 60, 48, 55

[164] Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin. Directed diffusion : A scalable and robust communication paradigm for sensor networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom '00)*, pages 56–67, Boston, Massachusetts, USA, 06-11 Aug 2000. ACM. 51, 61, 49, 56

[165] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, John Heidemann, and Fabio Silva. Directed diffusion for wireless sensor networking. *IEEE/ACM Transactions on Networking (ToN)*, 11(1) :2–16, 2003. 51, 61, 49, 56

[166] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the 33rd annual Hawaii international conference on System Sciences*, pages 10–pp, Maui, HI, USA, 7-7 Jan 2000. IEEE. 52, 50

[167] Ting-Chao Hou and Victor Li. Transmission range control in multihop packet radio networks. *IEEE Transactions on Communications*, 34(1) :38–44, 1986. 53, 51

[168] Hideaki Takagi and Leonard Kleinrock. Optimal transmission ranges for randomly distributed packet radio terminals. *IEEE Transactions on communications*, 32(3) :246–257, 1984. 53, 51

[169] Evangelos Kranakis, Harvinder Singh, and Jorge Urrutia. Compass routing on geometric networks. In *Proceedings of 11th Canadian Conference on Computational Geometry*, pages 51–54, 1999. 53, 51

[170] K Ruben Gabriel and Robert R Sokal. A new statistical approach to geographic variation analysis. *Systematic zoology*, 18(3) :259–278, 1969. 54

[171] Godfried T Toussaint. The relative neighbourhood graph of a finite planar set. *Pattern recognition*, 12(4) :261–268, 1980. 54, 55

[172] Prosenjit Bose, Pat Morin, Ivan Stojmenović, and Jorge Urrutia. Routing with guaranteed delivery in ad hoc wireless networks. *Wireless networks*, 7(6) :609–616, 2001. 55, 71, 53, 63

[173] Marjan Radi, Behnam Dezfouli, Kamalrulnizam Abu Bakar, and Malrey Lee. Multipath routing in wireless sensor networks : survey and research challenges. *Sensors*, 12(1) :650–685, 2012. 60, 55

[174] Wenjing Lou, Wei Liu, and Yanchao Zhang. Performance optimization using multipath routing in mobile ad hoc and wireless sensor networks. In *Combinatorial optimization in communication networks*, pages 117–146. Springer, 2006. 60, 55

[175] Katayoun Sohrabi, Jay Gao, Vishal Ailawadhi, and Gregory J Pottie. Protocols for self-organization of a wireless sensor network. *IEEE personal communications*, 7(5) :16–27, 2000. 61, 62, 56

[176] Tian He, John A Stankovic, Chenyang Lu, and Tarek Abdelzaher. Speed : A real-time routing protocol for sensor networks. Technical report, Virginia Univ CharlottesVille Dept of Computer Science, 2002. 61, 56

[177] Ben Leong, Barbara Liskov, and Robert Morris. Geographic routing without planarization. In *NSDI*, volume 6, page 25, 2006. 65, 59

[178] Seungjoon Lee, Bobby Bhattacharjee, and Suman Banerjee. Efficient geographic routing in multihop wireless networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages 230–241, Urbana-Champaign, IL, USA, 25-27 May 2005. ACM. 72, 75, 64, 67

[179] Nouha Baccour, Anis Koubâa, Luca Mottola, Marco Antonio Zúñiga, Habib Youssef, Carlo Alberto Boano, and Mário Alves. Radio link quality estimation in wireless sensor networks : a survey. *ACM Transactions on Sensor Networks (TOSN)*, 8(4) :34, 2012. 74, 66

[180] Mohamed Aissani, Sofiane Bouznad, Abdelmalek Hariza, and Salah-Eddine Allia. An effective approach for handling both open and closed voids in wireless sensor networks. *Sensors & Transducers*, 14(2) :196, 2012. 101

ملخص

شبكات الحسّاسات اللاسلكية، المسمّاة باللغة الانجليزية (Wireless Sensor Networks -WSNs) هي فئة من شبكات ad hoc التي تخضع للبحث المكثف. يعتبر هذا النوع من الشبكات أداة قوية لتوصيل العالمين المادي و الرقمي، وهي تتكون من عدد كبير من الحسّاسات التي تتميّز بموارد محدودة من حيث الطاقة، نطاق الإحساس والاتصال، سرعة المعالجة وسعة التخزين. يتم نشرها في بيئة داخلية أو خارجية في العديد من مجالات التطبيق، مثل المجال العسكري، الصحي، البيئة، الزراعة و المنازل الذكية. تؤدي ندرة موارد الحسّاسات وعدم موثوقية الروابط اللاسلكية إلى دفع معظم القضايا البحثية في مجال WSNs، و هي الطاقة، التغطية، الاتصال (connectivité)، التوجيه، الاسترجاع عند العطب (tolérance aux pannes) و الأمن.

تهدف هذه الأطروحة إلى اقتراح برتوكول مراقبة يعتمد على تصميم cross-layer ، فعّال فيما يخص استهلاك الطاقة و موثوق به، مخصّص لحراسة المناطق الحساسة المسيّجة، مثل حقول النفط والمواقع النووية. وذلك باستعمال شبكات الحسّاسات ذات دورة نشاط، المسمّاة باللغة الانجليزية (duty-cycled WSNs) ، مع أخذ بعين الاعتبار الروابط الغير متناظرة (asymmetrical links) الناتجة عن ظاهرة عدم انتظام الراديو(radio irregularity). يبدأ البروتوكول المقترح بتحديد الحسّاسات الحدودية لشبكة الحسّاسات المنشورة، لاستخدامها كحسّاسات حارسة (Sentinel nodes)، بمعنى أنها تكون دائما في حالة نشاط. بينما يتم استخدام الحسّاسات المتبقية كحسّاسات ترحيل ذات دورة نشاط (duty-cycled relay nodes) أثناء مرحلة توجيه التنبيهات صوب جامع البيانات (sink). يتم تحديد الحسّاسات الحدودية وتوجيه البيانات باستخدام نسخة محسّنة من بروتوكول GPSR، و المسمّاة GPSR-SL، و التي تعتمد على الرسم البياني المعروف ب N-UDG. تم تنفيذ بروتوكول المراقبة المقترح المعتمد على نموذج cross-layer، و تم تقييم أداءه باستعمال بيئة المحاكاة OMNeT++/Castalia. تظهر نتائج الأداء أن هذا البروتوكول يحقق نسبة تسليم للتنبيهات أعلى بنسبة 3.63%، كفاءة استخدام الطاقة و وقت استجابة (délai de bout en bout) مرضي، و ذلك عبر مقارنته بنفس البروتوكول المعتمد على الGPSR الأصلي.

الكلمات المفتاحية:

شبكات الحسّاسات اللاسلكية، توفير الطاقة، عدم انتظام الراديو، عدم تناظرا لروابط، خسارة المسار، الرسم البياني المعتمد على الأقراص غير الوحدوية، الرسم البياني المستوي، حسّاسات حدودية، دورة نشاط، التصميم الجغرافي الموثوق، GPSR، تصميم cross-layer

Abstract

Wireless Sensor Networks (WSNs) are a special class of Ad hoc networks, which are under intensive research. They are considered as a very powerful tool to connect the physical and the digital worlds. They consist of a large number of sensor nodes that are characterised with limited resources in terms of energy, range of sensing and communication, processing speed and storage capacity. They are deployed in an indoor or outdoor environment in many application domains such as army, environment, health, home and agriculture. The scarcity of sensor node resources and the unreliability of wireless links drive most of the research issues in the field of WSNs, namely energy, coverage, connectivity, routing, fault tolerance and security.

The aim of this thesis is to propose an energy-efficient and reliable cross-layer surveillance protocol for sensitive fenced areas, such as oil or nuclear sites, using duty-cycled WSNs with asymmetrical links due to the radio irregularity phenomenon. Initially, the proposed protocol identifies the boundary nodes of the deployed WSN, to be used as sentinel nodes, i.e., nodes that are always in an active state. The remaining nodes are used as duty-cycled relay nodes during the routing phase to relay alerts towards the sink. The boundary nodes identification process and alert routing are both performed using an enhanced version of the Greedy Perimeter Stateless Routing (GPSR) protocol, referred to as GPSR over Symmetrical Links (GPSR-SL) and which relies on a Non Unit Disk Graph (N-UDG). The proposed cross-layer surveillance protocol has been implemented and its performance has been evaluated under the OMNeT++/ Castalia simulation environment. Performance results shows that this protocol achieves higher Packet Delivery Ratio by up to 3.63%, energy efficiency and satisfactory latency when compared to the same protocol based on the original GPSR.

Keywords: Wireless Sensor Networks, Energy efficiency, Radio irregularity, Link asymmetry, Path loss, Non unit disk graph, Planar graph, Network boundary nodes, Duty cycle, Reliable geographic routing, GPSR, Cross-layer design

Résumé

Les Réseaux de Capteurs Sans Fil (RCSFs) constituent une classe particulière des réseaux Ad hoc, faisant l'objet de recherches intensives. Ils sont considérés comme un outil très puissant pour connecter le monde physique et le monde numérique. Ils se composent d'un grand nombre de nœuds capteurs dotés de ressources limitées en termes d'énergie, de portée de capture et de communication, de vitesse de traitement et de capacité de stockage. Ils sont déployés dans un environnement intérieur ou extérieur, et ce dans de nombreux domaines d'application tels que l'armée, l'environnement, la santé, la maison et l'agriculture. La rareté des ressources des nœuds capteurs et la non fiabilité des liaisons sans fil motivent la plupart des problématiques dans le domaine des RCSFs, à savoir l'énergie, la couverture, la connectivité, le routage, la tolérance aux pannes et la sécurité.

L'objectif de cette thèse est de proposer un protocole de surveillance inter-couches, à efficacité énergétique et fiable, pour la surveillance des zones sensibles clôturées, tel qu'un site pétrolier ou nucléaire, utilisant les réseaux de capteurs sans fil avec un cycle d'activité, et avec prise en compte des liens asymétriques dus au phénomène de l'irrégularité de la radio. Initialement, le protocole proposé identifie les nœuds de bordure du RCSF pour les utiliser comme nœuds sentinelles, c.-à-d., des nœuds qui sont toujours dans un état actif. Les nœuds restants sont utilisés en tant que nœuds relais avec un cycle d'activité, pendant la phase de routage des alertes vers le nœud puits. Le processus d'identification des nœuds de bordure ainsi que le routage des alertes, sont assurés par le protocole Greedy Perimeter Stateless Routing through Symmetrical Links (GPSR-SL) qui est une version améliorée du protocole GPSR, reposant sur un graphe de connectivité représenté sous forme de disques non-unité (N-UDG). Le protocole de surveillance inter-couches proposé a été implémenté et ses performances ont été évaluées en utilisant l'environnement de simulation OMNeT++/Castalia. Les résultats de performance montrent que ce protocole permet d'obtenir un ratio de livraison de paquets plus élevé d'environ 3.63%, une efficacité énergétique et une latence satisfaisante par rapport au même protocole basé sur le GPSR original.

Mots clés : Réseaux de Capteurs Sans Fil, Economie d'énergie, Irrégularité de la radio, Asymétrie des liens, Affaiblissement de propagation, Graphe à base de disques non-unité, Graphe planaire, Nœuds de bordure, Cycle d'activité radio, Routage géographique fiable, GPSR, Conception inter-couches

Titre : Approche inter-couches pour l'économie d'énergie et la fiabilité dans les Réseaux de Capteurs Sans Fil dédiés aux Applications Critiques de Surveillance

Mots clés : Réseaux de Capteurs Sans Fil, Economie d'énergie, Irrégularité de la radio, Asymétrie des liens, Affaiblissement de propagation, Graphe à base de disques non-unité, Graphe planaire, Nœuds de bordure, Cycle d'activité radio, Routage géographique fiable, GPSR, Conception inter-couches

Les Réseaux de Capteurs Sans Fil (RCSFs) constituent une classe particulière des réseaux Ad hoc, faisant l'objet de recherches intensives. Ils sont considérés comme un outil très puissant pour connecter le monde physique et le monde numérique. Ils se composent d'un grand nombre de nœuds capteurs dotés de ressources limitées en termes d'énergie, de portée de capture et de communication, de vitesse de traitement et de capacité de stockage. Ils sont déployés dans un environnement intérieur ou extérieur, et ce dans de nombreux domaines d'application tels que l'armée, l'environnement, la santé, la maison et l'agriculture. La rareté des ressources des nœuds capteurs et la non fiabilité des liaisons sans fil motivent la plupart des problématiques dans le domaine des RCSFs, à savoir l'énergie, la couverture, la connectivité, le routage, la tolérance aux pannes et la sécurité. L'objectif de cette thèse est de proposer un protocole de surveillance inter-couches, à efficacité énergétique et fiable, pour la surveillance des zones sensibles clôturées, tel qu'un site pétrolier ou nucléaire, utilisant les réseaux de capteurs sans fil avec un cycle d'activité, et avec prise en compte des liens asymétriques dus au phénomène de l'irrégularité de la radio. Initialement, le protocole proposé identifie les nœuds de bordure du RCSF pour les utiliser comme nœuds sentinelles, c.-à-d., des nœuds qui sont toujours dans un état actif. Les nœuds restants sont utilisés en tant que nœuds relais avec un cycle d'activité, pendant la phase de routage des alertes vers le nœud puits. Le processus d'identification des nœuds de bordure ainsi que le routage des alertes, sont assurés par le protocole Greedy Perimeter Stateless Routing through Symmetrical Links (GPSR-SL) qui est une version améliorée du protocole GPSR, reposant sur un graphe de connectivité représenté sous forme de disques non-unité (N-UDG). Le protocole de surveillance inter-couches proposé a été implémenté et ses performances ont été évaluées en utilisant l'environnement de simulation OMNeT++/Castalia. Les résultats de performance montrent que ce protocole permet d'obtenir un ratio de livraison de paquets plus élevé d'environ 3.63%, une efficacité énergétique et une latence satisfaisante par rapport au même protocole basé sur le GPSR original.

Title : Cross-layer approach for energy efficiency and reliability in Wireless Sensor Networks dedicated to Critical Applications of Surveillance

Keywords : Wireless Sensor Networks, Energy efficiency, Radio irregularity, Link asymmetry, Path loss, Non unit disk graph, Planar graph, Network boundary nodes, Duty cycle, Reliable geographic routing, GPSR, Cross-layer design

Wireless Sensor Networks (WSNs) are a special class of Ad hoc networks, which are under intensive research. They are considered as a very powerful tool to connect the physical and the digital worlds. They consist of a large number of sensor nodes that are characterized with limited resources in terms of energy, range of sensing and communication, processing speed and storage capacity. They are deployed in an indoor or outdoor environment in many application domains such as army, environment, health, home and agriculture. The scarcity of sensor node resources and the unreliability of wireless links drive most of the research issues in the field of WSNs, namely energy, coverage, connectivity, routing, fault tolerance and security. The aim of this thesis is to propose an energy-efficient and reliable cross-layer surveillance protocol for sensitive fenced areas, such as oil or nuclear sites, using duty-cycled WSNs with asymmetrical links due to the radio irregularity phenomenon. Initially, the proposed protocol identifies the boundary nodes of the deployed WSN, to be used as sentinel nodes, i.e., nodes that are always in an active state. The remaining nodes are used as duty-cycled relay nodes during the routing phase to relay alerts towards the sink. The boundary nodes identification process and alert routing are both performed using an enhanced version of the Greedy Perimeter Stateless Routing (GPSR) protocol, referred to as GPSR over Symmetrical Links (GPSR-SL) and which relies on a Non Unit Disk Graph (N-UDG). The proposed cross-layer surveillance protocol has been implemented and its performance has been evaluated under the OMNeT++/ Castalia simulation environment. Performance results show that this protocol achieves higher Packet Delivery Ratio by up to 3.63%, energy .efficiency and satisfactory latency when compared to the same protocol based on the original GPSR.

Résumé

Les Réseaux de Capteurs Sans Fil (RCSFs) constituent une classe particulière des réseaux Ad hoc, faisant l'objet de recherches intensives. Ils sont considérés comme un outil très puissant pour connecter le monde physique et le monde numérique. Ils se composent d'un grand nombre de nœuds capteurs dotés de ressources limitées en termes d'énergie, de portée de capture et de communication, de vitesse de traitement et de capacité de stockage. Ils sont déployés dans un environnement intérieur ou extérieur, et ce dans de nombreux domaines d'application tels que l'armée, l'environnement, la santé, la maison et l'agriculture. La rareté des ressources des nœuds capteurs et la non fiabilité des liaisons sans fil motivent la plupart des problématiques dans le domaine des RCSFs, à savoir l'énergie, la couverture, la connectivité, le routage, la tolérance aux pannes et la sécurité.L'objectif de cette thèse est de proposer un protocole de surveillance inter-couches, à efficacité énergétique et fiable, pour la surveillance des zones sensibles clôturées, tel qu'un site pétrolier ou nucléaire, utilisant les réseaux de capteurs sans fil avec un cycle d'activité, et avec prise en compte des liens asymétriques dus au phénomène de l'irrégularité de la radio. Initialement, le protocole proposé identifie les nœuds de bordure du RCSF pour les utiliser comme nœuds sentinelles, C'est à dire, des nœuds qui sont toujours dans un état actif. Les nœuds restants sont utilisés en tant que nœuds relais avec un cycle d'activité, pendant la phase de routage des alertes vers le nœud puits. Le processus d'identification des nœuds de bordure ainsi que le routage des alertes, sont assurés par le protocole Greedy Perimeter Stateless Routing through Symmetrical Links (GPSR-SL) qui est une version améliorée du protocole GPSR, reposant sur un graphe de connectivité représenté sous forme de disques non-unité (N-UDG). Le protocole de surveillance inter-couches proposé a été implémenté et ses performances ont été évaluées en utilisant l'environnement de simulation OMNeT++/Castalia. Les résultats de performance montrent que ce protocole permet d'obtenir un ratio de livraison de paquets plus élevé d'environ 3.63%, une efficacité énergétique et une latence satisfaisante par rapport au même protocole basé sur le GPSR original.

Mots-clés:

Réseaux de Capteurs Sans Fil ; Economie d'énergie; Irrégularité de la radio; Asymétrie des liens; Graphe à base de disques non-unité; Graphe planaire; Nœuds de bordure; Cycle d'activité radio; GPSR; Conception inter-couches.