République Algérienne Démocratique et Populaire
Ministere de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

En vue d'obtention du Diplôme master en recherche

Spécialité

Informatique

Option

Intelligence artificielle

Thème

Les protocoles de routage opportunistes sécurisés

PRÉSENTÉ PAR : BOUAICHE Farah
CHALANE Amel

Soutenu en 2020

Encadreur	**Dr A.TIAB**	**PhD**	**U. A/Mira Béjaia.**
Co-encadreur	**Dr S.F.OUADA**	**PhD**	**U. A/Mira Béjaia.**

Béjaia, Septembre 2020.

⁕ LISTE DES ABREVIATIONS ⁕

ACK ACKnowledgement
ACO Ant Colony Optimization
AQRV Adaptive QoS-based Routing
COPE Cooperative Power and Energy-efficient
CH Cluster Head
CSMA Carrier Sense Multiple Access
CTS Clear To Send
CGF Contention based Geographic Forwarding
EAX Expected Any-path transmissions
EAOR Energy Aware Opportunistic Routing protocol
EARTOR Energy-Aware Real-Time Opportunistic Routing protocol
EFFORT Energy eFFicient Opportunistic Routing Technology
ETX Expected Transmission count
ETT Expected Transmission Time
EXOR EXtremely Opportunistic Routing
FEC Forward Error Correction
GCF Geographic Collaborative Forwarding
GPS Global Positioning System
GPRS General Packet Radio Service
HC Hop Count
IEEE Institute of Electrical and Electronics Engineers
MAC Medium Access Control
OEC Opportunistic End-to-end Cost
ORTR Opportunistic Real-time Routing
RCSF Réseau de capteur sans fil
RO Routage Opportuniste
RTS Ready To Send
RGR Robust Geographic Routing protocol
SOAR Simple Opportunistic Adaptive Routing Protocol
CSMA/CA Collision Avoidance
TORP TinyOS Opportunistic Routing Protocol
QEOR QoS aware and Energy efficient Opportunistic Routing protocol
QoS Quality of Service
WSN Wireless sensor network
XOR Exclusive Or

⁂ *Remerciements* ⁂

C'est avec un grand plaisir que nous réservons ces lignes en signe de gratitude et de reconnaissance à tous ceux qui ont contribué de près ou de loin à la concrétisation de ce projet.

Nous remercions en premier lieu le bon DIEU de nous avoir donné les moyens,l'énergie mais surtout la volonté nécessaire pour la réalisation de ce modeste mémoire. Nos vifs remerciements vont d'emblées à nos chers parents pour tous les sacrifices consentis à notre égard et leur énormes soutien.

Nous exprimons notre reconnaissance à Madame TIAB Amel et Madame OUADA Farah d'avoir joué pleinement leurs rôles de promoteurs en étant à nos côtés tout au long de l'étude de notre projet.Leurs conseils et orientations nous ont guidé jusqu'à l'aboutissement de ce travail.

⁂ *Dédicaces* ⁂

Á mes parents, à mes frères et soeurs, à toute ma famille, à mes amis de A a Z, et tout ceux qui m'ont aidé .
Á ma binôme Chalane Amel et sa famille.
Bouaiche Farah

Á mes parents, à mes frères et soeurs, à toute ma famille, à mes amis de A a Z, et tout ceux qui m'ont aidé .
Á ma binôme Bouaiche Farah et sa famille.
Chalane Amel

M. Farah et Amel

Table des matières

Table des figures

Liste des tableaux

Introduction générale

L'apparition des nouvelles technologies ainsi que les progrès effectués dans le domaine des réseaux et du traitement de l'information ont entraîné l'apparition de nouveaux outils et objets tels que les réseaux 18 de capteurs et leurs applications. Depuis quelques années, les réseaux de capteurs sans fil Réseau de capteur sans fil (RCSF) s'ouvrent à plusieurs domaines d'applications : militaire, sécurité civile (surveillance des risques d'incendie, des catastrophes naturelles, des centrales nucléaires, ...), transport (automobile, ferroviaire, aéronautique, spatial), industriel (contrôle de la qualité de production, surveillance des lieux, ...), environnement,etc. L'environnement intègre de plus en plus des capteurs pour le contrôle, la commande ou la surveillance des lieux ou des systèmes. Un RCSF est un ensemble de capteurs autonomes à faible coût, interconnectés par un réseau de communications sans fil, capables d'effectuer des mesures sur l'environnement pour construire une vue globale de la région contrôlée. Son but est la collecte d'un ensemble de grandeurs environnementales, physiques ou physiologiques entourant ces capteurs, telles que la température, l'humidité, glycémie, ou tension, etc.., afin de les acheminer vers des centres de contrôle, ils sont considérés comme un type spécial de réseaux ad hoc. Les nœuds de ce type de réseaux consistent en un grand nombre de micro-capteurs capables de récolter et de transmettre des données environnementales d'une manière autonome. Notre travail consiste à étudier les réseaux de capteurs sans fil, et plus exactement le concept de routage opportuniste sécurisé, ce dernier est un nouveau mécanisme de routage qui exploite le concept de diffusion dont les réseaux sans fil sont caractérisé pour acheminer convenablement des paquets.

Nous allons voir dans le premier chapitre qui est intitulé « Généralités sur les réseaux de capteurs sans fils » une présentation générale sur les réseaux de capteurs sans fil ,leurs composants ainsi que leur fonctionnement.

Dans le deuxième chapitre intitulé « Etat de l'art des protocoles de routage opportuniste sécurisé » nous traiterons le routage opportuniste ,plus précisément le routage opportuniste sécurisé ainsi ses avantages et ses inconvénients,au final une classification des protocoles sécurisés.

Ce travail s'achèvera pas une conclusion générale et les perspectives.

Chapitre 1

Généralités sur les réseaux de capteurs sans fils

1.1 Introduction

De nos jours les réseaux de capteurs sans fil sont devenus primordiale grâce à leurs grand succès dans plusieurs domaines. Ce chapitre est consacré à une vue générale sur ces réseaux, y compris les problèmes et vulnérabilités par rapport à la sécurité. Nous définissons tout d'abord les notions de bases, par la suite nous parlerons de l'architecture, les caractéristiques et contraintes de conception de ces réseaux. Ensuite nous présentons les domaines d'application en détails ainsi que le routage dans les RCSF's. Puis nous abordons la sécurité dans ces réseaux, ses limites et exigences, voir les objectifs de sécurité et les attaques.

1.2 Réseau de capteur sans fil :

1.2.1 Définition d'un capteur sans fil :

Un capteur est un petit dispositif électronique qui nous permet de mesurer une valeur physique environnementale (température, lumière, pression, humidité, vibration, etc.), et de la transférer vers une station de base [1]. Chaque capteur assure les trois principales fonctions de base qui sont l'acquisition de données, les traitements sur ces données et leurs communications aux stations de bases.

1.2.2 Définition d'un réseau de capteurs sans fil :

Un réseau de capteur sans fil (RCSF) en anglais Wireless sensor network (WSN) (Wireless Sensor Network), est un type spécial de réseau ad-hoc défini par un ensemble coopérant de capteurs déployés dans une zone géographique appelée zone de captage ou zone d'intérêt, afin de surveiller un phénomène quelconque et de récolter des données d'une manière autonome. Les capteurs utilisent une communication sans fil pour acheminer les données captées avec un routage multi-sauts vers un nœud considéré comme "point de collecte", appelé station de base ou nœud puits ou sink en anglais. Cette dernière peut-être connectée à une machine puissante via internet, réseaux GPRS ou par satellite [2].

1.2.3 Architecture d'un RCSF :

Un RCSF est composé d'un ensemble de nœuds capteurs, Chacun de ces nœuds a la capacité de collecter des données et de les transférer au nœud Sink par l'intermédiaire d'une architecture multi-sauts. Le sink transmet ensuite ces données par Internet ou par satellite à l'ordinateur central

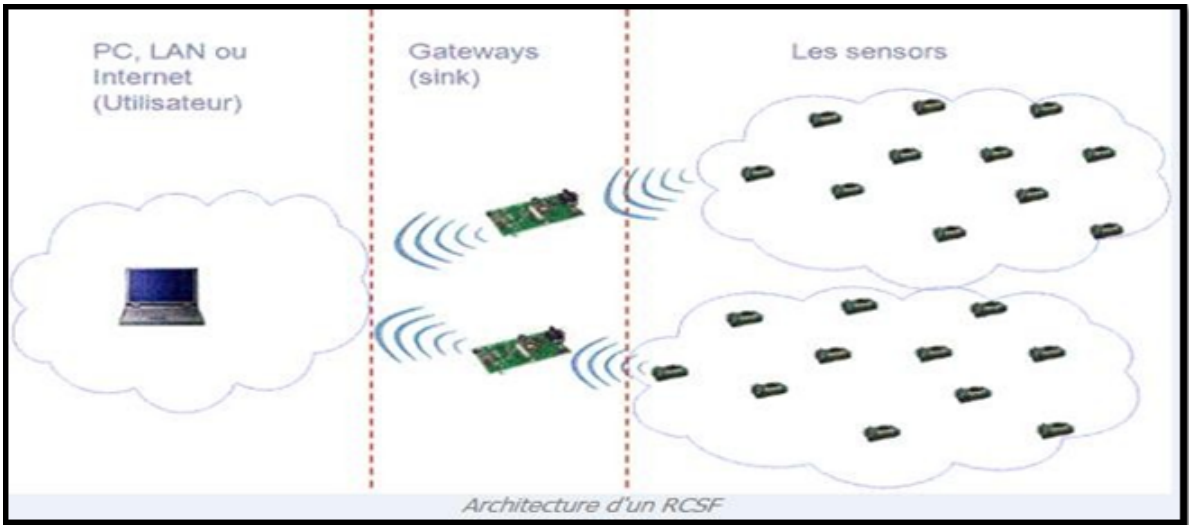

FIGURE 1.1: Architecture d'un RCSF [3].

Gestionnaire de taches pour analyser ces données et prendre des décisions [3]. La figure suivante illustre l'architecture d'un RCSFs :

1.2.4 Caractéristiques et contraintes de conception des RCSFs :

Les RCSFs font objet actuellement d'une grande attention en raison de leurs potentiels Illimitées. Toutefois, nous présentons ici les défis clés de la recherche pour les RCSFs :

- La tolérance aux fautes : Certain nœuds peuvent générer des erreurs ou ne plus fonctionner à cause D'un manque d'énergie,d'un problème physique ou d'une interférence. Ces problèmes n'affectent pas le reste du réseau. La tolérance aux fautes est la capacité de maintenir les fonctionnalités du réseau sans interruptions dues à une erreur intervenue sur un ou plusieurs capteurs [4].
- L'échelle : Le nombre de nœuds déployés pour un projet peut atteindre le million. Un nombre aussi important de nœuds engendre beaucoup de transmissions inter-nodales et nécessite que le sink soit équipé d'une capacité de mémoire importante pour stocker les informations reçues [4].

- La consommation d'énergie : la batterie d'un capteur est limitée en énergie en raison de sa petite taille, et le fait qu'elle n'est pas rechargeable ou remplaçable ceci diminue la durée de vie du capteur [5].

- Les contraintes matérielles : la taille du capteur est La principale contrainte matérielle. Par la suite viennent d'autres contraintes telle que la consommation d'énergie doit être moindre pour que le réseau survive le plus longtemps possible, qu'il s'adapte aux différents environnements (fortes chaleurs, eau,), qu'il soit autonome et très résistant vu qu'il est souvent déployé dans des environnements hostiles [4].

- Stockage : les nœuds capteurs sont limités en taille mémoire [4].

Agrégation de données : le fait que La distance entre les capteurs est très petite ceci engendre la redondance de données, C'est pour cela on opte vers la réduction des informations dans les capteurs afin de réduire la consommation de l'énergie [6].

FIGURE 1.2: Quelques domaines d'application des RCSFs [10].

1.2.5 Domaines d'application des RCSFs :

Les réseaux de capteurs peuvent être constitués de différents types de capteurs qui sont en mesure de contrôler ou de superviser plusieurs variétés de paramètres environnementaux. On trouve parmi ceux-là, la température, l'humidité, la pression, le niveau de bruit, le mouvement d'objets et la composition des sols [6]. Voici quelques applications des RCSFs dans certains domaines :

— Application de surveillance : L'application des réseaux de capteurs dans le domaine de sécurité peut diminuer considérablement les dépenses financières consacrées à la sécurisation des lieux et des êtres humains. Ainsi, l'intégration des capteurs dans de grandes structures telles que les ponts ou les bâtiments aidera à détecter les fissures et les altérations dans la structure suite à un séisme ou au vieillissement de la structure. Le déploiement d'un réseau de capteurs de mouvement peut constituer un système d'alarme qui servira à détecter les intrusions dans une zone de surveillance [7].

— La domotique : Le déploiement des capteurs de mouvement et de température dans les futures maisons dites intelligentes permet d'automatiser plusieurs opérations domestiques telles que : la lumière qui s'éteint et la musique qui se met en état d'arrêt quand la chambre est vide, la climatisation et le chauffage s'ajustent selon les points multiples de mesure, le déclenchement d'une alarme par le capteur anti-intrusion quand un intrus veut accéder à la maison.

— Applications commerciales : Des nœuds capteurs peuvent être utilisés pour améliorer les processus de stockage et de livraison. Le réseau peut aussi être utilisé pour connaitre la position, l'état et la direction de la marchandise.Donc durant l'attente du client ,il peut avoir l'état de la livraison en temps réel et connaitre la position des marchandises qu'il a commandées [8].

— Applications dans le domaine sportif : L'évolution des réseaux de capteurs est utilisée de plus en plus dans le domaine sportif, à savoir les systèmes de surveillance, les systèmes de calcul de trajectoires (comme dans le tennis), systèmes de détection d'erreurs d'arbitrage (comme dans le football indiquent si le balle a franchi la ligne de but) et d'autres applications des réseaux de capteurs sont illustrées dans la figure 1.3 qui suit [7] :

1.3 Routage dans RCSFs :

Dans les RCSFs, les capteurs sont déployés en grand nombre pour surveiller un tel phénomène et faire remontrer l'information à un centre de contrôle distant. Pour atteindre cette finalité, les capteurs ont la capacité de communiquer et collaborer entre eux pour acheminer l'information collectée à la station de base en garantissant sa fiabilité et en empruntant le plus court chemin entre le nœud qui a détecté ce phénomène et la station de base. Cette opération permet le routage de l'information entre le nœud détecteur et le nœud sink et elle consiste à trouver les plus courts chemins [14].

1.4 Classes de protocoles de routage dans les RCSFs :

Récemment, les protocoles de routage pour les RCSFs ont été largement étudiés. On peut classifier ces méthodes selon plusieurs critères comme illustré sur la figure suivante [9] :

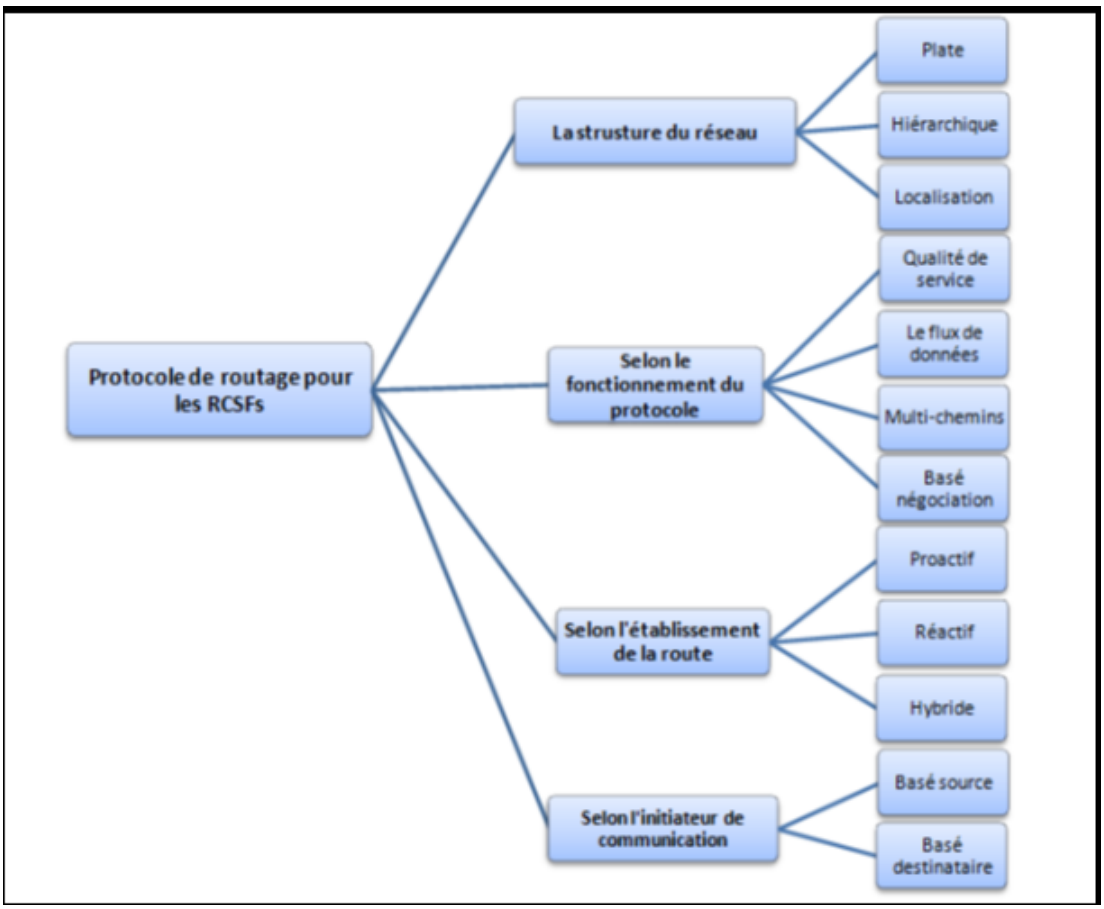

FIGURE 1.3: Classification des protocoles de routage pour RCSF[1].

1.4.1 Classification selon la structure du réseau :

La topologie représente l'emplacement des capteurs dans le réseau. On trouve deux topologies principales dans les protocoles de routage pour les RCSF's [9] :

— Topologie plate : tous les nœuds ont le même rôle. Les nœuds sont semblables en termes de ressources [9].

— Topologie hiérarchique : les topologies hiérarchiques consistent à diviser les nœuds en plusieurs niveaux de responsabilité, afin d'augmenter la scalabilité du système. Le clustering est la méthode la plus usée où le réseau est partitionné en groupes appelés "clusters". Un cluster est constitué d'un chef (cluster-Head) et de ses membres [9].

1.4.2 Classification selon l'initiateur de communication :

Il existe trois paradigmes de communication au niveau des RCSF's [9] :

— Nœud central : ce paradigme est employé dans les réseaux conventionnels, où les communications se basent sur l'identification des nœuds participants, qui se fait à l'aide d'adresses IP [9].

— Donnée centrale : dans un RCSF, la donnée est plus importante que le nœud lui-même, ce qui rend son identification inutile. Dans le paradigme donné centrale, les communicants sont identifiés par leurs données, et donc tout le système (routage, interrogation, . . . etc.) doit être régit par cette propriété. Ainsi, le système peut être vu comme une base de données distribuée, où les nœuds forment des tables virtuelles, alimentées par les données captées [9].

— Position centrale : dans cette approche, les positions des nœuds représentent le moyen principal d'adressage et de routage. Dans certaines applications, il est plus intéressant d'interroger le système en utilisant les positions des nœuds, que leurs adresses IP. Dans ce cas, le routage s'effectue grâce à des techniques géométriques afin d'acheminer l'information d'une zone géographique vers une autre [9].

1.4.3 Type d'application :

La méthode de captage des données dans un RCSF dépend de l'application et de l'importance de la donnée. De ce fait, les RCSFs peuvent être catégorisés comme celle déterminée par le temps ou par l'évènement[9].

— Application déterminée par le temps : un réseau déterminé par le temps est approprié pour des applications qui nécessitent un prélèvement périodique des données. Par exemple, cela est utile dans des applications de monitoring (feu, météo) afin d'établir des rapports périodiques [9].

— Application déterminée par l'événement : dans des applications temps réel, les capteurs doivent réagir immédiatement à des changements soudains des valeurs captées. Un prélèvement périodique des données est inadapté pour ce type de scénarios. Pour cela, le protocole doit être réactif et doit donner des réponses rapides à l'occurrence d'un certain nombre d'évènements [9].

1.4.4 Classification selon l'établissement de la route :

On peut classifier les protocoles selon trois catégories :

— les protocoles proactifs : Les protocoles de routage proactifs essaient de maintenir les meilleurs chemins existants vers toutes les destinations possibles au niveau de chaque nœud du réseau. Pour ce faire, les nœuds du réseau maintiennent des tables de routage pour toutes les destinations indépendamment de l'utilité des routes [18].

— les protocoles réactifs : Les protocoles de routage réactifs maintiennent des routes à la demande. Lorsque le réseau a besoin d'une route, une procédure de découverte est lancée. Une fois que la route n'est plus utilisée, elle sera immédiatement détruite ce qui permet une conservation d'énergie [18].

— les protocoles hybrides : Les protocoles hybrides combinent les deux idées des protocoles proactifs et réactifs. Ils utilisent un protocole proactif pour avoir connaissance du proche voisinage (par exemple le voisinage à deux ou trois sauts). Au-delà de la zone de voisinage, le protocole hybride fait appel à un protocole réactif pour chercher des routes [18].

Classification selon le fonctionnement du protocole :

Les protocoles de routage peuvent être classés selon leurs fonctionnalités en quatre catégories :

— Routage basé sur la Qualité de Service (QdS) : Dans les protocoles de routage basés sur la QdS, le réseau doit assurer un équilibrage, la consommation d'énergie et la qualité de données. En particulier, le réseau doit satisfaire une certaine métrique de QdS. Ce type de protocole est utilisé dans les applications qu'ont des exigences temps réel (monitoring médical, application militaire) [19].

— Protocole basé sur les multi-chemins : Les protocoles basé sur ce type de routage maintiennent plusieurs chemins afin d'augmenter les performances du réseau. Lorsque le chemin primaire est défaillant, les données vont être acheminées vers la destination via des chemins alternatifs.

— Routage basé sur la négociation : Ces protocoles utilisent des descriptions de données afin d'éliminer les transmissions de données redondantes, par une négociation préalable entre la source et la destination. Cette procédure garantit que seules les informations utiles qui seront transmises [19].

— Routage basé sur le flux de données dans le réseau : Dans ce type de protocole, la phase d'établissement de route est modélisée et résolue comme un problème de demande de flux de données ou le flot représente la route que les paquets empruntent, et la demande représente le taux auquel les paquets sont produits par les différents nœuds [19].

— Routage Opportuniste :Le routage opportuniste est un mécanisme récent de routage pour les RCSFs. Contrairement au routage traditionnel,il exploite son environnement, en utilisant le concept de diffusion qui caractérise les réseaux sans fil afin d'acheminer adéquatement les paquets[20].

1.5 Sécurité (exigences/limites) des RCSFs

Les RCSF ne sont pas parfaits à cause de leur faible coût et leur déploiement dans des zones parfois hostiles, les nœuds sont assez fragiles et vulnérables. Ainsi, la perte de connexions sans fils peut être due à une extinction d'un capteur suite à un épuisement de sa batterie, ou tout simplement à une destruction physique accidentelle ou intentionnelle par un ennemi ce qui touche à la sécurité de ces RCSFs, voici deux volets complémentaires de cette sécurité [9] :

— La sécurité opérationnelle : qui a comme objectif qu'un réseau devrait continuer à fonctionner même lorsque certains de ses composants sont attaqués (l'exigence de la disponibilité du service) [9].

— La sécurité des informations : qui assure la confidentialité, l'intégrité et l'authenticité des informations [9].

1.5.1 Objectifs de Sécurité :

— Authentification : Cette propriété consiste à vérifier l'identité d'un émetteur de données, afin permet d'éviter l'injection de paquet par un tiers non autorisé.Elle permet de même d'authentifier les données qui transitent sur le réseau [9].

— Intégrité : Cette propriété consiste à s'assurer que la donnée n'a pas été modifiée. Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière accidentelle ou intentionnelle) [9].

— Confidentialité : Apres l'authentification, le réseau assure la confidentialité des informations transmises et que les personnes intruses ne pourront y accéder au contenue de ces données mis a part les personnes qui possèdent ce droit. Les données doivent être cachées ou cryptées. Elle peut être assurée soit par la cryptographie à clé privée ou la cryptographie à clé publique [12].

— Non répudiation : S'assurer que l'émetteur ne peut pas nier l'émission et le récepteur ne peut nier la réception [13].

— Disponibilité : S'assurer que l'information est présente et utilisable au moment où l'on en a besoin. Ça Permet de s'assurer que l'on peut toujours communiquer avec toutes les parties du réseau et que leurs données soient accessibles [13].

1.5.2 Les attaques

On peut classifier les attaques dans un RCSF en deux groupes principaux : les attaques passives et les attaques actives, qui sont bien évidemment plus dangereuses [11] :

— a.Menaces de type passif : l'attaquant est limité à l'écoute et l'analyse du trafic échangé. Cette attaque prive le réseau de la confidentialité des messages échangés. Eventuellement, l'analyse du trafic représente un risque pour l'anonymat des participants et le respect de leurs vies privées [11].Cette figure représente d'une attaque passive :

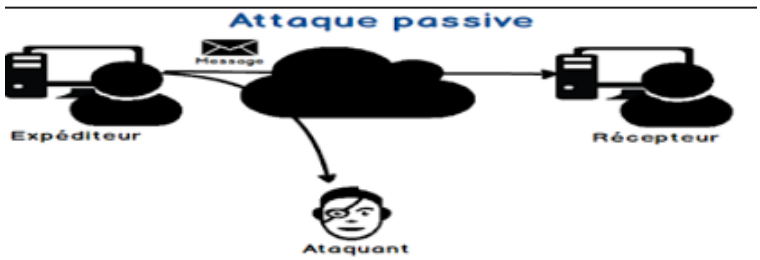

FIGURE 1.4: Illustration d'une attaque passive [15].

— b.Menaces de type actif : l'attaquant se donnera les moyens d'agir sur la gestion, la configuration et l'exploitation du réseau. Il peut injecter son propre trafic, modifier le fonctionnement d'un nœud, usurper l'identité d'un élément valide, rejouer des messages, modifier des messages transitant sur le réseau ou provoquer un déni de service [11].La figure suivante explique comment se fait une attaque passive :

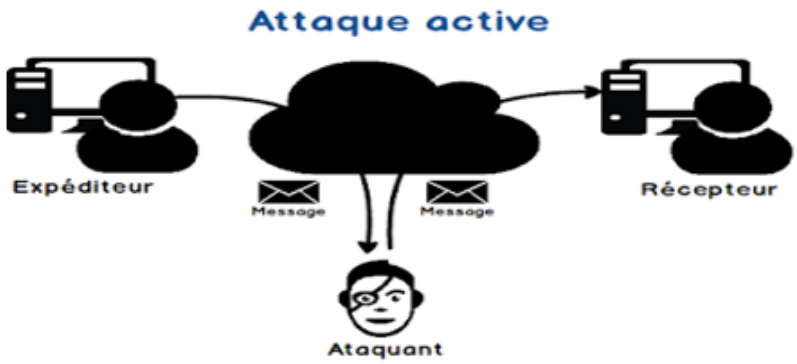

FIGURE 1.5: Illustration d'une attaque active [15].

1.6 Vulnérabilités des RCSFs :

Les propriétés des réseaux de capteurs sont à double tranchant. Certes ils permettent une grande facilité de production et de déploiement, mais rendent le système global de communication assez « fragile » à un certain nombre de défaillances. Les vulnérabilités des RCSFs émergent à partir des propriétés qui les rendent efficaces et attrayants [16].

— a)Coûts réduits et miniaturisation Un des objectifs de conception des réseaux de capteurs sans fil est la surveillance de territoires épars, difficiles d'accès, tout en facilitant le déploiement de ces réseaux. Pour atteindre cet objectif, la taille d'un RCSF doit être suffisamment grande pour assurer une large couverture. De ce fait, le coût unitaire d'un nœud du réseau doit être suffisamment réduit pour que l'usage d'un RCSF comportant des centaines, voire des milliers de nœuds soit économiquement viable [16].

— b)Déploiement au sein de l'environnement physique : La plupart des applications de RCSF exigent un déploiement étroit des nœuds à l'intérieur ou à proximité des phénomènes à surveiller. Cette proximité physique avec l'environnement conduit à de fréquentes compromissions intentionnelles ou accidentelles des nœuds. Pour des raisons économiques, les nœuds d'un RCSF ne peuvent être conçus pour garantir une protection physique inviolable. Par conséquent, un adversaire « bien équipé » peut extraire des informations cryptographiques des nœuds capteurs. Comme un RCSF est généralement sans surveillance humaine, le risque d'attaque des nœuds et de récupérer leur contenu est élevé [16].

1.7 Conclusion

Dans ce chapitre, nous avons introduit une vue générale des réseaux de capteurs sans fil, nous avons cité les concepts fondamentaux, les notions de bases de ces réseaux, par la suite nous avons présenté leurs architecture. Les RCSFs représentent un problème complexe car nous devons assurer la fiabilité de livraison de données, la performance du système et tout cela en consommant moins d'énergie, ce qui nous a aussi mené à faire une étude sur ces derniers. Dans le chapitre suivant, nous dressons un état de l'art des protocoles de routage opportuniste existants pour les RCSFs et nous discuterons la possibilité d'adaptation à la sécurité dans cet environnement.

Chapitre 2

Etat de l'art des protocoles de routage opportuniste sécurisé

2.1 Introduction :

Le routage opportuniste (RO) est une approche récemment développée utilisée dans un réseau multi-sauts sans fil. L'objectif du routage opportuniste est de franchir l'inconvénient et vulnérabilité de la transmission sans fil imprécise ,en tirant profit de la nature d'émission du milieu sans fil tels qu'une transmission surprise par des voisins multiples.Dans ce chapitre, nous illustrons d'abord l'idée fondamentale du RO, ,ainsi que le principe de fonctionnement, par la suite nous parlerons des avantages du RO et applications ,voir les métriques de routage opportuniste, la classification de quelques protocoles de RO. En conclusion, nous rédigeons un tableau de comparaison entre différents protocoles traités dans ce chapitre en se concentrant sur différents métriques.

2.2 Définition de routage opportuniste :

Le routage opportuniste est mécanisme récent de routage pour les RCSFs. Contrairement au routage traditionnel, où on sélectionne le prochain voisin avant la transmission ce qui peut accuser des problèmes de réception si les liaisons sont soumises à des erreurs. Le routage opportuniste tire profit de la diffusion existante au niveau des réseaux sans fil de sorte que chaque nœud qui arrive à surprendre un paquet et soit proche de la destination est capable de participer dans l'envoi des paquets reçus [20].

Le routage opportuniste exploite son environnement, en utilisant le concept de diffusion qui caractérise les réseaux sans fil afin d'acheminer adéquatement les paquets. À la place de choisir un nœud de relais distinct à chaque transmission, le routage opportuniste propage le paquet à un ensemble de nœuds candidats. Ensuite, les candidats, qui ont reçu correctement le paquet, exécutent un protocole de coordination pour choisir le meilleur chemin afin d'expédier le paquet[21].

Dans le routage traditionnel, les protocoles présélectionne un ou plusieurs nœuds prédéterminés avant le début de la transmission et emploie un voisin prédéterminé pour expédier un paquet. Le RO quant à lui, franchit l'inconvénient de la transmission sans fil imprécise en annonçant une transmission qui peut être surprise par des voisins divers [22].

2.3 Principe de fonctionnement :

L'objectif du routage opportuniste est d'employer la nature de radiodiffusion du réseau sans fil de sorte que la transmission d'un nœud peut être surprise par des nœuds multiples. Au lieu de choisir le prochain nœud d'expéditeur en avant, le RO choisit le prochain nœud dynamiquement à l'heure de la transmission. L'expédition est faite par le nœud le plus proche de la destination.

La tâche principale du RO est de choisir l'expéditeur, placer et donner la priorité aux nœuds dans l'ensemble [23]. Le routage opportuniste tire profit de la nature diffusante du support en utilisant les liens opportunistes.

Les candidats ayant bien reçu le paquet se coordonne pour déterminer celui qui va relayer le message [24]. La figure ci-dessous représente des liens opportunistes qui sont instables c'est à dire n'étant pas toujours présent, candidatset(S)=A,B,D qui est l'ensemble des candidats relayeurs .

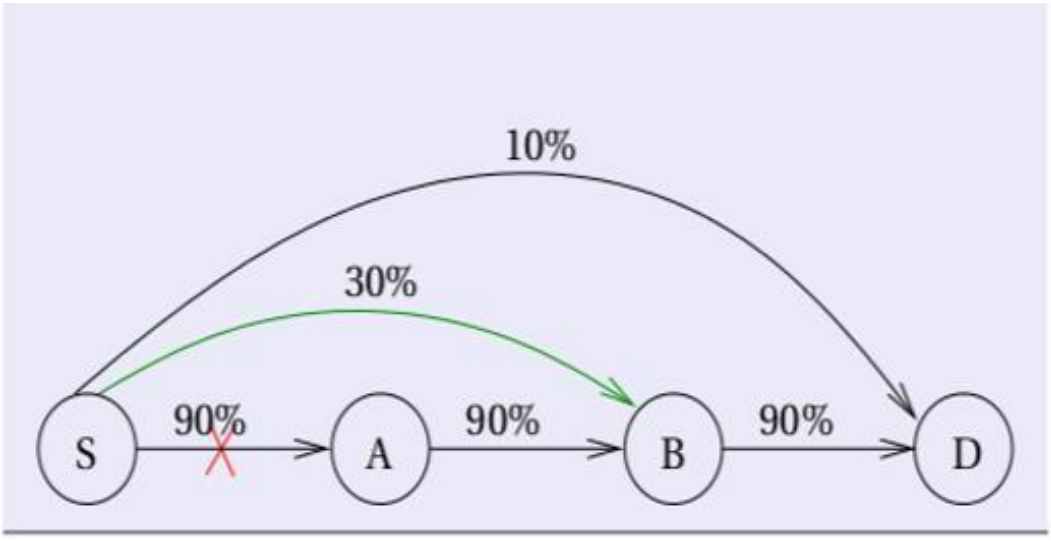

FIGURE 2.1: Illustration des liens opportunistes [25].

2.4 Avantages du routage opportuniste :

Le routage opportuniste est plus performant que le routage traditionnel. IL offre plusieurs avantages dont :

Réduction des pertes d'énergie et des délais

Le RO peut être appliqué aux RCSFs afin de réduire la consommation d'énergie provoqué par les retransmissions et le détour dynamique des nœuds qui ont moins d'énergie. Le RO établit le concept de sommeil qui incite les nœuds capteurs à s'endormir lorsque les transmissions des données n'ont pas eu lieu. De ce fait, le RO permet aux capteurs de conserver leur énergie[26].

Augmenter la fiabilité

Le RO transmet les paquets qu'à travers un seul lien distinct, autrement dit le RO a des liens de secours additionnels ce qui réduit la probabilité d'échec de transmission [27].

Augmente la qualité de la transmission :

Le RO prend en compte toutes les liaisons pour transmettre un paquet, cela inclus les liaisons courtes porté de bonne qualité et les liaisons longues porté de mauvaise qualité, ce qui signifie qu'avec une seule transmission, un paquet peut être délivré avec succès grâce à une transmission longue portée au lieux de passer par tous les nœuds intermédiaires. Par conséquent, la performance peut être améliorée [27]. De plus, les résultats d'analyse théorique et d'expérimentation ont montré que le RO a le potentiel d'exécuter le routage mieux que traditionnel[28].

Détermination efficace des nœuds d'expédition :

Une des avantage majeures du RO c'est que le prochain relais est choisi dynamiquement a travers plusieurs relais, de ce fait, le risque de perte des paquets diminue [27].

2.5 Applications du routage opportuniste :

Le routage opportuniste peut être utilisé dans plusieurs applications telle que :

Opérations de secours :

Lorsque les catastrophes naturelles ont eu lieu dans une zone précise,telle que le séisme par exemple, le déploiement d'un routage opportuniste est indispensable afin de permettre aux unités de secours de communiquer. En sélectionnant de façon opportuniste les meilleurs liens/nœuds (mobiles ou fixes) disponibles pour communiquer avec le personnel de secours et d'urgence, ce qui permet des opérations de recherche et de sauvetage plus résilientes [29].

Cette illustration représente des opérations de sauvetage basées sur le routage opportuniste dans les zones sinistrées :

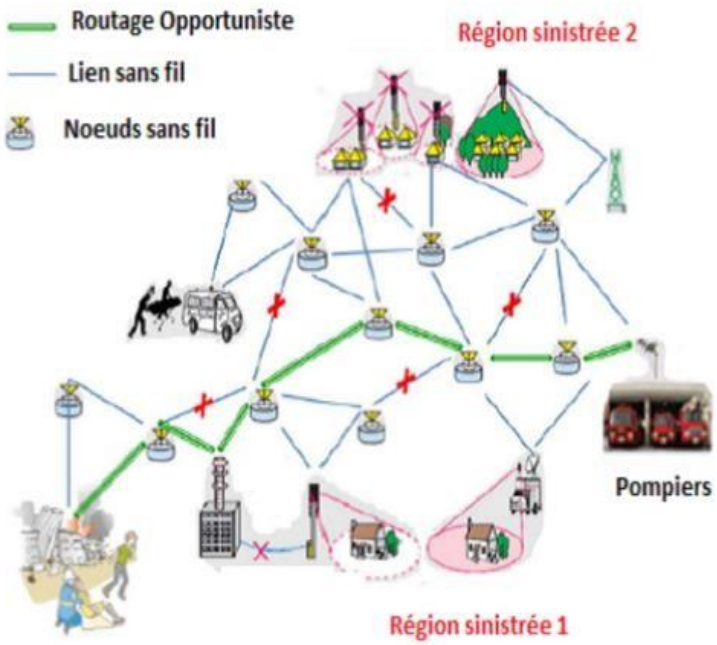

FIGURE 2.2: exemple d'opérations de sauvetage basées sur le routage opportuniste[29].

Organisation industrielle :

Le routage opportuniste sert à relier les opérations industrielles et les sites tels que les champs De pétrole et de gaz, l'exploitation minière et les zones de construction, qui sont difficiles à Mettre en réseau à cause de leur situation géographique et de leurs environnements de propagation. Le routage opportuniste correspond le mieux à ce type d'environnement grâce à sa nature adaptative. Prenant exemple, dans les sites de mines souterraines caractérisées par l'atténuation haute du signal et les

perturbations fréquentes du réseau, le RO permet aux travailleurs de terrain de rester connectés à la meilleure unité de communication dans leur environnement et de transférer leur appel de manière fiable à l'unité de sécurité centrale correspondante[29] .

Connexion dans les zones rurales :

Étant donné le manque d'infrastructures dans les zones rurales, le routage opportuniste offre une alternative abordable pour la fourniture d'internet. En effet, en utilisant les dispositifs sans Fil disponibles en tant que relais, le routage opportuniste offre une meilleure couverture D'internet, en contribuant ainsi à combler les lacunes numériques [29]. En raison de la nature intermittente des communications dans ce type d'applications, ainsi que Le manque d'infrastructures, le routage traditionnel ne peut pas être utilisé. En effet, il ne peut pas s'adapter aux changements fréquents de ces réseaux contrairement au routage Opportuniste qui offre plus de flexibilité et de robustesse [29].

2.6 Composants du routage opportuniste :

Le routage opportuniste diffère du routage traditionnel dans beaucoup d'aspects, les multiples relais candidats et la sélection dynamique des relais après la transmission de données. La sélection des relais candidats et la coordination entre eux sont deux composants primaires du routage opportuniste [30].

2.6.1 La sélection des candidats :

Un des principaux composants du routage opportuniste est la sélection des relais candidats, qui est semblable à la construction des tables de routage dans le routage traditionnel. La sélection de relais candidats doit maintenir tous les relais possibles et marquer la priorité de chaque relais candidat pour les méthodes de coordination. La tâche de la sélection des relais candidat est encore divisée en deux parties, à savoir l'ordre de priorité et filtrage des relais candidat [30] Tous les nœuds dans le réseau utilisent un algorithme de sélection pour choisir l'ensemble des nœuds voisins (candidats) qui peuvent aider de la meilleure façon qui soit dans le processus d'expédition vers une destination donné, et enmême tempsréduire auminimum le nombre prévu de transmissions [30]. Dans le but de sélectionner et de prioriser un ensemble de nœuds candidats, les algorithmes de routages opportunistes utilisent une ou plusieursmétriques [31]. Ces métriques dépendent principalement de l'application spécifique du protocole de routage. En ce sens, ces métriques peuvent être classées comme suit [32].

- **Métrique nombre de saut :** Peut être définie comme le nombre de périphérique réseaux entre le nœud source et le nœud destinataire ou le nombre de liaison point à point dans un chemin de transmission. Le nœud source génère des paquets qui incluent un champ réservé au compteur de nœuds définit par le nombre de sauts Hop Count (HC). A chaque fois qu'un dispositif est capable de recevoir ces paquets, ce dispositif modifie le paquet en incrémentant le champ HC. En outre, le dispositif compare le champ contre une limite prédéterminée et supprime le paquet si la valeur du champ est trop haute. Ceci empêche les paquets de rebondir sans fin dans le réseau dû aux erreurs de cheminement [33].
- **Métrique ETX :** peut être définie comme le nombre de périphérique réseaux entre le nœud source et le nœud destinataire ou le nombre de liaison point à point dans un chemin de transmission. Le nœud source génère des paquets qui incluent un champ réservé au compteur de nœuds définit par le nombre de sauts Hop Count (HC). A chaque fois qu'un dispositif est capable de recevoir ces paquets, ce dispositif modifie le paquet en incrémentant le champ HC. En outre, le dispositif compare le champ contre une limite prédéterminée et supprime le paquet si la valeur du champ est trop haute. Ceci empêche les paquets de rebondir sans fin dans le réseau dû aux erreurs de cheminement [33].

- **Métrique EAX :** Cette métrique est une extension d'ETX. Elle calcule le nombre moyen de transmissions prévues en tenant compte de tous les chemins qui peuvent être utilisés dans un routage opportuniste [34].
- **Métrique ETT :** : La métrique ETT estime le tempsrequis pour transmettre un paquet sur une liaison. ETT peut être calculé en ajustant la métrique ETX selon la taille du paquet etla capacité de transmission de la liaison [33].
- **Métrique d'avancement bits-mètres par seconde :** Cette métrique également géographique prend en compte les progrès de paquets pour les différents taux de transmission qui sont disponibles dans le réseau. Elle est spécialement indiquée lorsque le réseau supporte une variété de technologies radio [35].

2.6.2 Coordination des candidats :

La coordination est le mécanisme utilisé par les nœuds candidats pour définir lequel a la priorité la plus élevé pour recevoir et ainsi expédier le paquet. Une bonne coordination entre les nœuds candidats devrait choisir le meilleur dans un temps record et sans occasionner de redondance dans la transmission des paquets [36]. Les approches de coordination sont divisées en quatre catégories principales basées sur le mécanisme utilisé :

- **Coordination basé sur un acquittement :** Un nœud malveillant peut interférer dans une communication en transmettant un paquet « en sens inverse » pour causer une collision. En particulier, le nœud malveillant cible un paquet (ou trame) d'acquittement (ACK) afin de bloquer/retarder la communication ce qui, outre le débit, affecte la consommation d'énergie des nœuds. Pour mieux comprendre le déroulement de cette attaque, nous l'illustrons dans la Figure 2.3 Un adversaire place un nœud malveillant M entre deux nœuds N1 et N2 qui communiquent entre eux. Il désire à travers ce nœud perturber leurs communications. Au début, l'adversaire écoute les échanges. Il remarque que le paquet 1 envoyé par N1 est suivi d'un acquittement ACK envoyé de la part du destinataire N2. Ainsi, l'adversaire mesure approximativement le temps nécessaire entre la réception du paquet et l'envoi de l'ACK de la part de N2. Il attend l'envoi du paquet 2 puis il émet un paquet juste au bon moment pour provoquer une collision avec l'ACK. Après un certain temps d'attente, N1 va devoir renvoyer le paquet 2 car il n'a pas pu décoder l'acquittement et considère que le premier envoi du paquet 2 est infructueux. Cette attaque perturbe les échanges entre N1 et N2 et oblige ces nœuds à perdre leur énergie en renvoyant des paquets [37]. La détection d'une telle attaque est difficile car le temps d'attaque est court et les paquets envoyés par le nœud malveillant sont similaires à des paquets normaux [37].

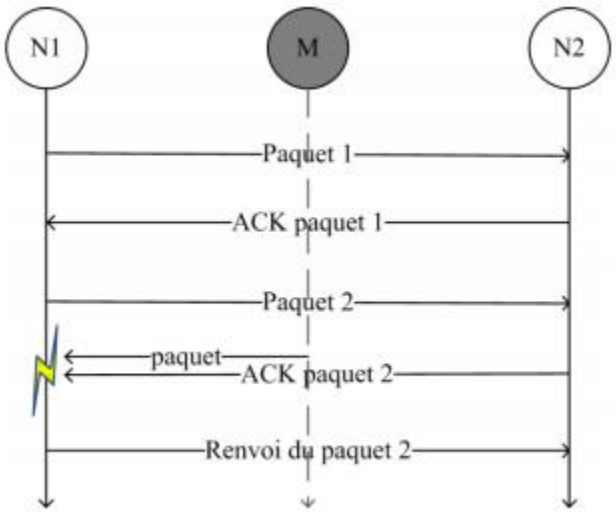

FIGURE 2.3: L'attaque par collision [37].

Un nœud malveillant M se place entre deux nœuds pour essayer de perturber leurs communications en envoyant des paquets en même temps que les ACK.

- **Coordination temporisée :** Pour sélectionner le meilleur relais d'une liste de relais candidats admissibles, les relais candidats dans la méthode de coordination temporisée, attendent avant de retransmettre un paquet pendant un délai basé sur un ordre prédéfini. Le premier à répondre est alors choisi comme prochain relais. Une méthode de coordination temporisée généralement se comporte comme suit : Tous les relais candidats sont d'abord ordonnés selon une métrique prédéfinie. L'ordre de priorité est produit par une source (ordre de priorité global) ou l'expéditeur (ordre de priorité local) et est inclus dans l'en-tête du paquet. Après qu'un paquet de données soit diffusé, les relais candidats répondront dans l'ordre, c'est à dire le i ème relais candidat prioritaire répondra au i ème slot de temps. Un relais candidat répond à son tour seulement quand il n'y a aucune réponse des autres. Par conséquent, avant qu'un relais candidat réponde, il peut confirmer que tous les relais candidats plus prioritaires n'ont pas réussi à recevoir les paquets de données. Une fois qu'un relais candidat répond, il est choisi en tant que prochain relais et empêchera les autres de répondre [38], [39], [40].
- **Coordination basé sur le codage réseau :** L'intégration du RO avec une stratégie appropriée de codage peut considérablement l'améliorer, par exemple : la correction d'erreurs appelé (forward error correction : FEC) peut réduire le rapport de perte de paquet des liens qui affecte par conséquent le classement des relais candidats par ordre de priorité. L'intégration du codage réseau et le Routage opportuniste peut réduire le nombre total de transmissions en guidant les paquets à de prochains nœuds avec plus de chances de codage [41]. La figure ci-dessous représente un réseau de travail et par des liaisons unidirectionnelles, de capacité Unitaire.

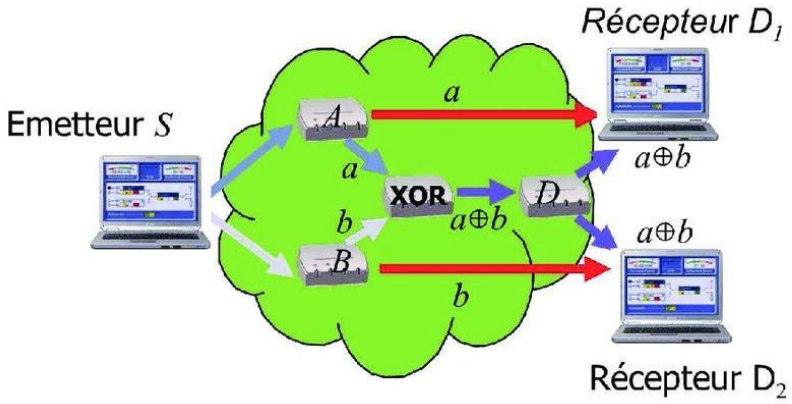

FIGURE 2.4: Exemple canonique du codage réseau par câble [42].

- **Basée sur les messages RTS/CTS :** Certains mécanismes peuvent employer des paquets de contrôle explicites échangés immédiatement avant ou après une transmission de données pour la coordination distributive. La station transmet un message appelé (RTS signifiant Demande pour émettre) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur (généralement un point d'accès) répond un (CTS signifiant Le champ est libre pour émettre), puis la station commence l'émission des données. A la réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (ACK). Toutes les stations avoisinantes patientent alors pendant un temps qu'elle considère être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée [43].
  La figure ci-dessous montre un protocole CSMA/CA qui utilise un mécanisme d'esquive de collision basé sur un principe d'accusé de réceptions réciproques entre l'émetteur et le récepteur :

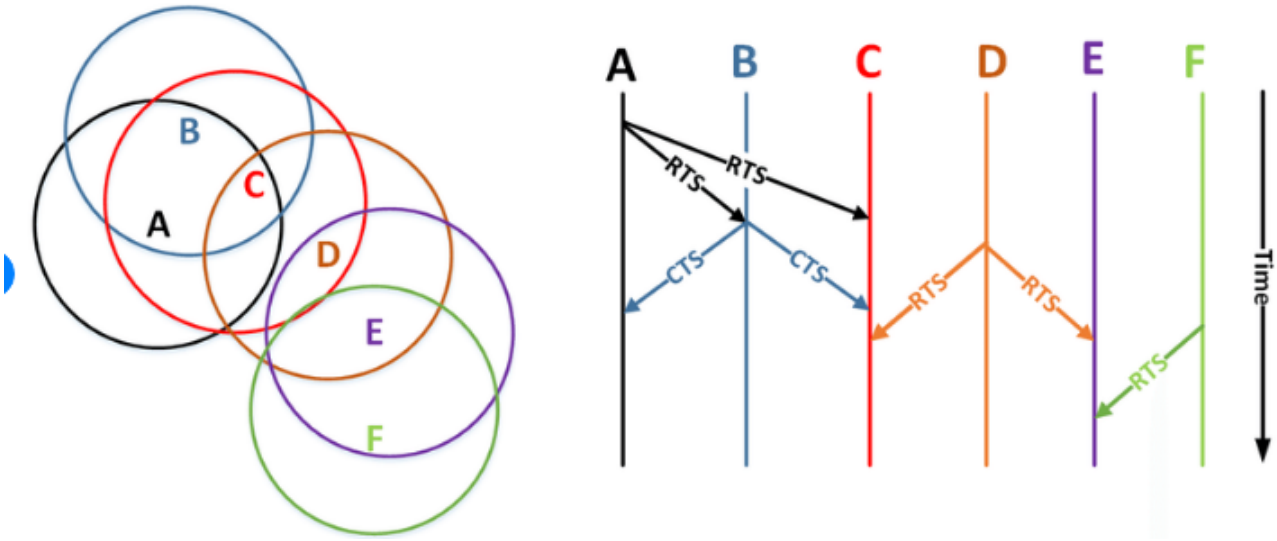

FIGURE 2.5: Un problème de blocage multi-sauts [44].

- **Coordination à base de jeton :** Cette approche permet de résoudre le problème de l'exclusion mutuelle répartie, elle se base sur la notion de privilège. Celui-ci est symbolisé par la possession d'un objet unique particulier que nous appelons un jeton. Il n'existe qu'un seul jeton dans tout le système. L'obtention de ce jeton garantit l'exclusivité de l'accès à la ressource. La propriété de vivacité est assurée en faisant en sorte que le jeton puisse se déplacer de processus en processus et parcourir tous les processus. En ce qui concerne la vivacité, deux possibilités existent : le jeton passe de lui-même de processus en processus en dessinant un anneau logique incluant tous les processus (le processus qui désire entrer en section critique garde le jeton, entre en section critique et fait suivre le jeton à sa sortie de section critique),le processus qui désire entrer en section critique demande le jeton et attend de le posséder avant d'entrer effectivement en section critique. Cet algorithme est efficace car il évite les famines et réalise l'exclusion mutuelle [44].

2.7 Classification des protocoles de routage opportunistes :

Nous présentons ci-dessous (figure 2.6)une classification des protocoles de routage opportuniste dans les RCSFs discutés dans la section précédente.

2.7.1 Protocoles basés sur le taux de livraison :

Les nœuds candidats sont sélectionnés selon les métriques ETX ou bien EAX.

- **Extreme Opportunistic Routing (ExOR)** Ce protocole intègre la couche réseau et MAC. Il suppose que tous les nœuds connaissent le taux de perte sur chaque lien sans fil et peuvent utiliser un routage à état des liens. C'est le premier protocole de routage opportuniste [45]. La liste des relais candidats se base sur la métrique ETX, et est ordonnée en fonction du nombre de sauts. Quand on trouve plusieurs voisins dont le chemin vers la destination possédant le même nombre de sauts, dans ce cas ils sont ordonnés selon le taux de livraison. La liste ordonnée est alors incluse dans l'en-tête du paquet de données. Quand un relais candidat reçoit le paquet, il doit répondre avec une trame d'acquittement ACK, Car la couche de liaison est modifiée pour intégrer cette fonctionnalité supplémentaire. L'émission de l'ACK est également ordonnée de sorte que le relais candidat de priorité plus Élevée répond le premier [45].

Avantages :

— Il assure le routage et l'ordonnancement des transmissions afin d'éviter les problèmes de collision.

— Il améliore le débit dans les RCSFs.

— Il augmente la fiabilité de transmission des paquets[47].

Inconvénients : Le protocole ExOR souffre du problème de duplication de paquets [47] :

— Plusieurs relais potentiels relayent le paquet, cela induit une consommation d'énergie inutile.

— La redondance des paquets de données.

- **Protocole SOAR :** SOAR a été présenté dans [46] afin de supporter des flots multiples. C'est un protocole de routage proactif où chaque nœud maintient une table de routage contenant la destination, la route sélectionnée par défaut et la liste des nœuds impliqués dans la participation. La sélection de la route peut être basée sur la métrique ETX ou n'importe quelle autre métrique tout en tenant compte de la priorité. A la différence de MORE, SOAR permet aux nœuds non sélectionnés et qui soient proches de la route établie par défaut de participer dans la transmission afin de minimiser des transmissions inutiles. Cependant, la source doit limiter le nombre de nœuds concernés. En ce qui concerne les transmissions, SOAR procède de la même manière que le protocole TCP et le compteur de temps est calculé pour estimer l'instant de la prochaine transmission.

Avantages :

— Il garantit un transfert opportuniste efficace en sélectionnant judicieusement les nœuds, en utilisant des minuteries basées sur les priorités [48].

— Il surpasse les autres protocoles en choisissant le plus court chemin [49].

Inconvénients : — Ne garantit pas la connexion des nœuds de transfert sélectionnés.

— la Coupure entre les nœuds de transfert peut entraîner de sérieuses performances dégradation car les paquets de données ne peuvent pas progresser à travers la partition.

2.7.2 Protocoles de routage opportuniste basé sur le codage réseau :

Les paquets sont codés à l'émission dans cette classe de protocoles :

- **COPE. XORs in The Air : Practical Wireless Network Coding** Un mécanisme de codage réseau pratique a été proposé dans [50], pour supporter une communication unicast efficace dans un réseau mesh sans fil. Ce protocole emploi une écoute opportuniste pour permettre à chaque nœud d'acquérir des informations d'état locales et la diffusion de paquets codés pour améliorer le débit du réseau. Dans COPE, Chaque nœud enregistre les paquets pour un temps petit et informe aussi ses voisins des paquets qu'il a écoutés en annotant les paquets envoyés. Lorsqu'un nœud transmet un paquet, il utilise sa connaissance de ce que ses voisins ont écouté afin d'effectuer un codage opportuniste et emploi l'opérateur XOR pour coder plusieurs paquets et les transmettre comme un seul paquet.

  Avantages :

  —Améliore simultanément le débit du réseau et le débit TCP.

  —Permet un codage robuste.

  —facilité la mise en œuvre et l'importance de la communication unicast.

  Inconvénients :

  —L'applicabilité du COPE est limitée.

- **BEND. Network Coding Via Opportunistic Forwarding** c'est un protocole qui combine les caractéristiques de codage réseau et la transmission opportuniste dans les réseaux mesh IEEE 802.11 pour créer davantage de possibilités de codage dans le réseau. Profitant de la redondance des paquets parmi les relais candidats, ce protocole change de routes localement et de façon dynamique pour atteindre de meilleures possibilités de codage. BEND est

surtout une solution de la couche MAC, elle est basée sur MAC IEEE 802.11 et fonctionne indépendamment de toute source ou protocole de routage à état des liens.

Avantages :

—Permet d' obtenir de meilleures opportunités de codage.

—Permet d'avoir un gain de codage plus élevé.

—Permet d'atténuer les pertes de paquets dues aux erreurs de canal.

Inconvénients :

—Il n'est pas globalement optimal.

2.7.3 Protocoles de routage opportuniste géographiques :

Cette classe de protocoles s'appuie sur l'hypothèse que chaque nœud a une certaine connaissance sur sa position et les positions des autres nœuds.

- **CGF. Contention-based Geographic Forwarding** Ce protocole [52], est une version préliminaire des protocoles de routage opportuniste géographiques. Il n'exige pas l'échange des messages des états des liens entre les nœuds, c'est à la source d'envoyer un paquet de contrôle quand il y a besoin d'envoyer un paquet de données. Les relais candidats décident en toute indépendance de leur aptitude à retransmettre le paquet de données en fonction de leur distance par rapport à la destination. En particulier, les relais candidats sont dans la zone de transmission, c'est à dire qu'ils sont plus près de la destination que la source. Ensuite, le relais candidat coordonne pour décider du nœud qui retransmettra le paquet de données.

  Avantages :

  —Evitement de collision.

  —Permet une optimisation des paramètres et est performant pour une densité des nœuds.

  —Réduit considérablement les exigences de stockage de topologie.

  —Permet de couvrir des modèles de réseau plus sophistiqués.

  Inconvénients :

  —N'étend pas efficacement la durée de vie du réseau par rapport à d'autres protocoles .

- **RGR. Robust Geographic Routing protocol** Ce protocole [53], sélectionne les relais candidats en fonction de leur distance par rapport à la destination, c'est à dire les nœuds qui sont plus près de la destination ont une priorité plus élevée. Le nombre maximum de relais candidats est limité à cinq nœuds qui peuvent être inclus dans les en-têtes des paquets de données, et la source est responsable de l'ordre des nœuds dans la liste de relais candidats.

— L'utilisation des GPS's permet d'améliorer la connaissance de la position au centimètre près. Des traitements du signal dans des récepteurs plus sophistiqués permettent d'améliorer la précision de positionnement (résolution de la distance) [47].

— Dans le routage basé sur la localisation géographique, la région de sensation est connue et la requête peut être donc dirigée uniquement vers cette région, ce qui éliminera le nombre de transmission de manière significative [47].

— Les nœuds doivent être équipés d'un système de localisation par satellite [47].

— Le routage basé sur la localisation géographique n'est pas un bon choix pour les applications qui exigent une livraison fiable à des intervalles réguliers des paquets de données [47].

Avantages :

— Le protocole RGR atteint d'excellentes performances même dans des conditions de mobilité de nœud élevée.

Inconvénients :

—Nombre de nœuds relais est limité.
—Rareté des ressources qui cause une operation couteuse lors de la surveillances des nœuds capteurs a leurs environnement.

2.7.4 Protocoles de routage opportuniste conscients de l'énergie :

Ces propositions se basent sur la métrique de l'énergie.

- **TORP. TinyOS opportuniste Routing Protocol** Un protocole de routage opportuniste efficace en énergie pour les RCSFs se comportant comme le protocole EXOR a été mis en oeuvre sur TinyOS par J. Carnley et al. appelé TinyOS opportuniste Routing Protocol (TORP) [54]. Le protocole TORP tente de rendre un nœud capteur plus efficace en réduisant le nombre de transmissions nécessaires pour livrer les données à la destination. Cependant, il nécessite une connaissance globale de la topologie du réseau, ce qui est trop coûteux ou irréaliste pour des RCSFs larges[54].

  Avantages :
  —Efficace en energie.
  Inconvénients :
  —Trop couteux pour les RCSFs larges car il necessite une connaissance globale de la topologie du réseau.

- **EAOR. Energy Aware Opportunistic Routing protocol** P. Spachos et al. Ont proposé Energy Aware Opportunistic Routing protocol (EAOR) [55], un protocole opportuniste conscient de l'énergie conçu pour les RCSFs. Ce protocole essaie de transmettre les paquets sur les relais qui sont proches de la destination et qui ont aussi un haut niveau d'énergie. De cette façon, il peut découvrir plus de chemins de routage par rapport aux autres protocoles de routage opportuniste et peut réduire la consommation d'énergie totale et prolonger la durée de vie du réseau.
  Avantages :
  —Reduire la consommation d'energie de 35Prolonger la durée de vie du réseau jusqu'à 25
  Inconvénients :
  —les demandes doivent arriver une par une.

2.7.5 Protocoles de routage opportuniste temps réel :

Cette classe de protocoles est conçue dans le but de satisfaire les exigences temporelles des applications temps réel.

- **ORTR. Opportunistic Real-time Routing** J. Kim et al. Ont proposé ORTR [56], une méthode heuristique qui intègre les fonctionnalités de la couche réseau et de la couche MAC pour la transmission des données temps réel dans les RCSFs. ORTR calcule une région optimale où les données doivent être envoyées pour garantir la livraison en temps réel, en utilisant une puissance de transmission efficace. Tout d'abord, il calcule la plus petite puissance de transmission exigée par les données temps réel et tous les nœuds dans la région optimale qui garantissent les exigences de temps. D'autre part, l'un des nœuds est sélectionné en utilisant le niveau de batterie restant afin d'équilibrer le niveau de puissance. Toutefois, dans le cas où un rapport cyclique bas est appliqué dans ORTR, la zone de transmission peut ne pas

contenir aucun nœud.

Avantages :

—Fournit un service en temps réel garanti avec une puissance de transmission optimale sans dégrader le bilan énergétique .

Inconvénients :

—ORTR n'est pas adapté pour prendre en charge des données périodiques en temps réel.

- **EARTOR. Energy-Aware Real-Time Opportunistic Routing protocol** W. Yang et al. Ont proposé EARTOR [57] afin de remédier aux problèmes du protocole ORTR. EARTOR est un protocole de routage opportuniste temps réel, efficace en énergie pour les applications avec des contraintes de latence de bout-en-bout spécifiées. Son but est d'équilibrer entre la consommation d'énergie et la latence de bout-en-bout et vise à maximiser le nombre de transmissions réalisées. Les techniques de base adoptée par EARTOR comprennent la conception inter-couches qui intègre le rapport cyclique (duty cycling), un mécanisme de sélection pour chaque relais candidat qui prend en considération son énergie résiduelle, les informations de localisation et l'ordre de priorité du relais candidat. Cependant EARTOR emploie le GPS et il se base plutôt sur les services de la couche MAC.

  Avantages :

  —Offrir une communication fiable et temps réel pour les RCSFs industriels.

  Inconvénients :

  —Il nécessite des informations précises de positionnement global pour effectuer les tâches de routage, ce qui ne peut être obtenu de manière fiable.

  —Ce protocole ne considère pas les propriétés inhérentes aux RCSFs comme la limite de la taille mémoire des nœuds capteurs

2.7.6 Protocoles de routage opportuniste avec QoS :

Cette classe de protocoles est conçue dans le but de satisfaire les exigences de la QoS dans les RCSFs.

- **EFFORT. Energye eFFicient Opportunistic Routing Technology in wireless sensor networks** C-C. Hung et al. Ont prpoposé EFFORT [58], un protocole de routage opportuniste distribué qui introduit une nouvelle métrique, permettant de calculer le coût opportuniste de bout-en-bout, appelée Opportunistic End to end Cost (OEC). Cette métrique considère conjointement le coût énergétique de transmission de bout-en-bout, l'énergie résiduelle de chaque capteur et la fiabilité de transmission au niveau de chaque relais, et peut être calculée efficacement à partir du noeud sink vers chaqu'un des noeuds de façon récursive. Effectivement, le protocole EFFORT étend efficacement la durée de vie du réseau par rapport aux autres protocoles de routage opportuniste comme GCF.

  Avantages :

  —Le protocole EFFORT étend efficacement la durée de vie du réseau.

  —Minimiser la consommation d'énergie de tous les nœuds.

  Inconvénients :

  —Il n'est pas totalement optimale par rapport à d'autres protocoles de routage opportunistes.

- **QEOR. Protocole de routage opportuniste avec QoS et efficacité énergétique pour les RCSFs** C'est un nouveau protocole de routage opportuniste avec QoS et efficacité énergétique intitulé QEOR, , c'est le premier protocole de routage opportuniste spécialement conçu pour les RCSFs industriels [59]. C'est un protocole avec QoS et efficacité énergétique, dont le principal objectif est de sélectionner intelligemment les relais candidats afin de profiter pleinement des

avantages du routage opportuniste, et de fournir les exigences des applications industrielles.
Avantages :
—Réduction de la consommation d'énergie et de la surcharge des paquets ainsi qu'une amélioration de la durée de vie du réseau.
—Maximiser la fiabilité sur les liaisons réseau.

Inconvénients :
—la possibilité de perte ou de mauvaise transmission de l'ACK.

- **AQRV .Adaptive QoS-based Routing using ACO** Ce protocole de routage appelé Routage adaptatif basé sur la QoS pour les réseaux véhiculaires utilisant ACO (AQRV). Basé sur le concept ACO, L'AQRV combine des composants réactifs et proactifs pour établir et maintenir le meilleur chemin de routage [61]. Des fourmis réactives avant et arrière sont envoyées entre la source et la destination pour explorer et configurer le meilleur itinéraire composé d'une liste d'intersections, respectivement. La fonctionnalité principale de la sélection d'itinéraire est de s'appuyer sur une estimation de la qualité de relais du segment de route qui est exprimée en termes de trois paramètres de qualité de service combinés, à savoir : le délai, la probabilité de connectivité et le taux de livraison des paquets AQRV met en œuvre une maintenance proactive des itinéraires à l'aide de fourmis proactives pour mettre à jour, étendre et améliorer les informations de routage. Dans la session de transfert de paquets de données, AQRV choisit dynamiquement la meilleure intersection suivante pour les paquets de données, et lorsqu'ils sont transmis entre deux intersections adjacentes, les paquets de données utilisent une méthode simple mais efficace mécanisme de retenue et d'avance [62], qui peut réduire les effets du véhicule individuel mouvement sur les chemins de routage [61].

  Avantages :
  —Etendre et améliorer les informations de routage.

  Inconvénients :
  —L'analyse est théoriquement assez difficile dans ACO,Les décisions ne sont pas séquentielles mais sont Aléatoire.

Cette méthode peut accélérer la convergence de la meilleure route et réduire les frais généraux du réseau[61]. De plus, l'utilisation de la QoS globale peut améliorer la stabilité de l'itinéraire et éviter un routage extrême conditions dans les prochaines sélections d'itinéraire[61].

La figure suivante représente une classification détaillée des protocoles de routage opportunistes :

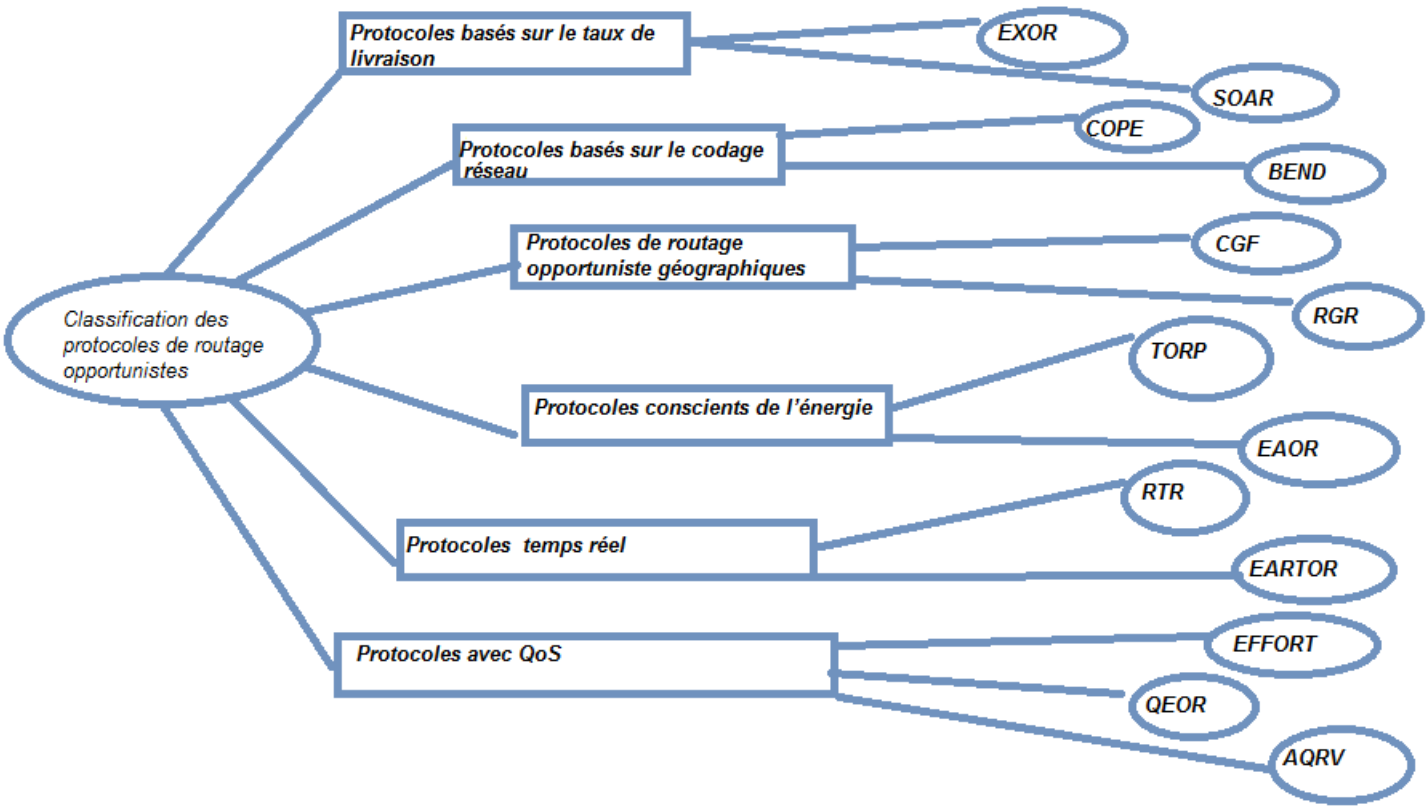

FIGURE 2.6: classification des protocoles de routage opportuniste [60].

2.8 Comparaison entre les différents protocoles de routage opportuniste :

Nous présentons ici la classification des protocoles de routage opportuniste dans les RCSFs discutés dans la section précédente. La table ci-dessous montre comment ces protocoles s'adaptent aux différentes catégories.

Protocole	Classe	selection	coordination	avantages	inconvénients
EXOR[45]	Basé sur le Taux de Livraison	Nombre de sauts et ETX	Temporisée/ Acquittement	— Il améliore le débit et augmente la fiabilité	redondance des paquets de données.
Soar[46]	Basé sur le taux de livraison	ETX	Temporisée/ Acquittement	transfert opportuniste efficace	Ne garantit pas la connexion des noeuds transférés
COPE[50]	Basé sur le Codage réseau	Basé sur le Codage réseau	Codage réseau	codage robuste	L'applicabilité du COPE est limitée
BEND[51]	Basé sur le codage réseau	Nombre de sauts	Codage réseau	un gain de codage plus élevé	Il n'est pas globalement optimal
CGF[52]	Géographique/ Conscient de l'énergie	EPA : avancement de paquet prévu	RTS-CTS	évitement de collision	n'etends pas la durée de vie du réseau
RGR[53]	Géographique	Avancement de paquet et nombre de voisins	RTS-CTS	mobilité de nœud élevée	Nombre de nœuds relais limité
TORP [54]	Conscient de l'énergie	ETX	Temporisée	Efficace en energie	Trop couteux pour les RCSFs larges
EAOR[55]	Conscient de l'énergie	Energie plus Distance	RTS-CTS	consommation d'energie réduite	les demandes doivent arriver une par une.
ORTR [56]	Temps réel	Puissance de la batterie et le temps de transmission	Acquittement	puissance de transmission optimale	pas adapté pour prise en charge des données périodiques
EARTOR [57]	Temps réel	Energie résiduelle et informations de localisation	Acquittement	communication fiable	—Il nécessite des informations précises.
EFFORT[58]	QoS et efficacité énergétique	Opportunistic End to end Cost (OEC)	Acquitement	Minimiser la consommation d'énergie de tous les nœuds	Il n'est pas totalement optimale.
QEOR [59]	QoS et efficacité énergétique	Energie	Acquitement	efficace en energie	mauvaise transmission de l'ACK.
AQRV[61]	QoS	Energie	acquittemement	améliorer les informations de routage	L'analyse est théoriquement assez difficile dans ACO.

TABLE 2.1: Classification des protocoles de routage opportuniste.

Le tableau ci-dessus montre la classification que nous avons pu établir dans la section précédente des différents protocoles que nous avons étudiés dans ce deuxième chapitre. Comme cité précédemment le routage opportuniste est un concept récent, de ce fait il est difficile de trouver une classification conforme et universelle pour les protocoles de routage opportuniste. Cependant leurs conceptions soulèvent certaine questions fondamentales comme le choix de l'ensemble des expéditeurs, la priorité, la duplication ou la suppression d'expéditeurs ...etc, les réponses à ces questions nécessite de prendre en compte des critères tel que l'efficacité, la compatibilité avec les mécanismes de control d'accès au support (MAC), l'utilisation d'information sur l'état du réseau, l'emplacement des nœuds, la méthode de codage ...etc.

2.9 Conclusion :

Ce chapitre a été axé sur le routage opportuniste dans les RCSFs. Ainsi, une définition de ce dernier et une présentation du principe de fonctionnement. Plusieurs métriques ont été employées, de ce fait, établi une classification des protocoles de routage opportuniste et une liste des protocoles de routage opportuniste a été énumérée. Enfin, un tableau montrant la classification des protocoles de routage a été dressé. Bien que le RO soit un nouveau concept dans les RCSFs. L'étude de ces protocoles nous a permis de mettre en relief les avantages et les inconvénients des stratégies de routage adoptées par chacun d'eux, bien que plusieurs de ces stratégies paraissent prometteuses, il existe toujours certains défis qui persistent et nécessitent leur prise en considération par les protocoles de routage dans les réseaux de capteurs. Le chapitre suivant sera consacré à la description de notre nouveau protocole de routage opportuniste sécurisé répondant aux besoins et les exigences des RCSFs.

Chapitre 3

Le Protocole ExOR muni d'un mécanisme de sécurité

3.1 Introduction :

Les RCSFs ont été largement recherché en raison de l'avantage significatif apporté par transmissions sans infrastructure et multi-sauts. Cela dit, beaucoup de problème de sécurité découlent de la nature de ces réseaux, De plus L'efficacité énergétique est aussi un problème critique pour les réseaux de capteurs, car de nombreux capteurs sont équipés de batteries dont la durée de vie est limitée. Pour cela, nous avons besoin d'une technique ou d'un protocole de routage qui augmentera la durée de vie du réseau et assurera la fiabilité.

Dans ce chapitre, nous allons proposons un protocole de routage opportuniste ExOR muni d'un mécanisme de sécurité. À notre connaissance, ExOR est le premier protocole de routage opportuniste d'autres voies de réflexions ont été conçues après sa mise en œuvre. ExOR est décrit comme une technique de routage opportuniste qui dispose de plusieurs avantages.

D'abord, nous présenterons le protocole son principe de fonctionnement et quelques avantages et inconvénients ensuite nous présentons les motivations de ce travail et nous fournissons un aperçu détaillé des problèmes de sécurité. Enfin, nous décrivons notre protocole ExOR avec sécurité ainsi quelque notions de base liées à la cryptographie et à l'infrastructure de gestion de clés..

3.2 Protocole ExOR :

ExOR est le premier protocole de routage opportuniste proposé en 2005,utilisé pour les réseaux sans fil à sauts multiples[63]. Il s'agit d'un Protocole de routage MAC qui augmente le débit du réseau. Le choix de chaque nœud de l'itinéraire sélectionné est reporté à la fin de la transmission. Comme avantage, ExOR utilise des liaisons longues avec un taux de perte important qui est évité par un protocole de routage classique[17].
Le principal défi d'ExOR est la coordination. C'est pourquoi les nœuds participants devraient coopérer et organiser leur expédition ; ils utilisent le paquet d'en-tête ExOR. Le schéma décrit le Paquet d'en-tête d'ExOR ajouté à chaque paquet avant son transfert. ExOR utilise un lot de paquets. Le nœud source contient la liste des candidats priorisés par la proximité de la destination :

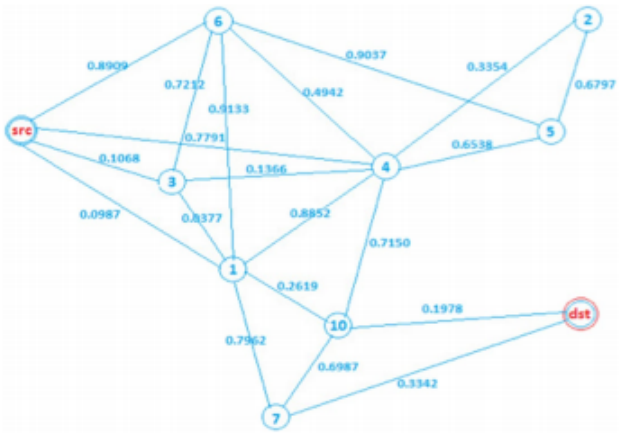

FIGURE 3.1: Evolution des valeurs ETX lors de la dixième itération de transmission[77].

3.3 Principe de fonctionnement du protocole EXOR :

ExOR dispose de différents composants comme tout autres protocoles de RO. Selon son fonctionnement : il utilise End to end comme méthode de sélection d'expéditeurs, l'ETX comme métrique pour assigner la priorité à l'ensemble des expéditeurs, il n'est pas basé sur le codage, utilise la topologie du réseau pour acheminer les paquets [64].

Plus précisément, Un nœud émetteur indique dans le paquet, une liste de relayeurs potentiels classés par ordre de priorité pour relayer le paquet et le transmet en broadcast. Sur réception du paquet, un nœud vérifie s'il est dans la liste. Si c'est le cas il déclenche une temporisation dont la durée dépend de la place du nœud (plus il est loin dans la liste, plus la temporisation est longue), calculée par une métrique ETX qui considère uniquement le taux de perte dans le sens de la transmission, car il n'y a pas d'acquittements. Après écoulement de la temporisation, le nœud émet le paquet s'il n'a pas déjà été émis. Si le nœud n'est pas dans la liste, il ne participe pas au relayage du paquet, Les transmissions sont effectuées jusqu'à ce que 95% des paquets aient atteint la destination finale. Ce type de routage permet de réduire le nombre de retransmissions, car il augmente la fiabilité des transmissions [65].

La figure, ci-dessous montre les valeurs ETX de chaque nœud dans le réseau par rapport au nœud E, La valeur ETX de chaque nœud est la somme des valeurs ETX de liaison le long du chemin ETX le plus bas vers E [66].

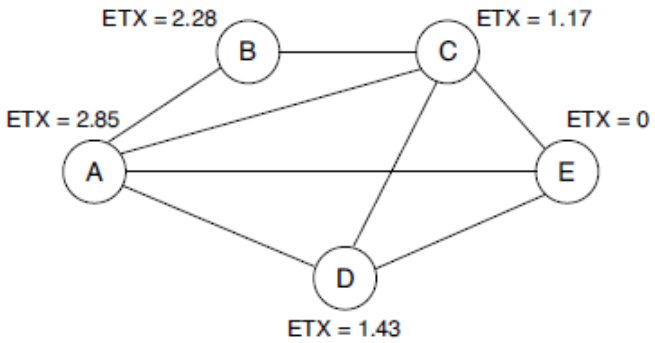

FIGURE 3.2: : Nombre de transmissions estimé (ETX) du nœud E de chaque nœud du réseau[66].

3.3.1 Avantages :

Le protocole EXOR comprend plusieurs avantages qui sont [66] :

-Il évite les problèmes de collision, en fortifiant l'ordonnancement des transmissions ainsi que le routage.
-Il améliore le débit dans les RCSFs.
-Il augmente la fiabilité de transmission des paquets.
-Fournit des données en masse plus rapidement que le routage traditionnel, pour itinéraires longs et courts.

3.3.2 Inconvénients :

La duplication de paquets représente un problème sensible pour l'EXOR [66] :

-Un gaspillage en consommation d'énergie causé par Les relais potentiels qui relayent le paquet.
-La redondance des paquets de données.
-Vulnérable contre diverses attaques.

3.4 Définition de la cryptographie :

La cryptographie est une science qui utilise des mathématiques pour chiffrer et déchiffrer des données. Elle permet de stocker des informations sensibles et de les transmettre à travers des réseaux non sûrs de telle sorte qu'elles ne puissent pas être lues par personne à l'exception du destinataire convenu. La cryptographie offre des services de sécurité tels que l'authentification, la confidentialité, l'intégrité et la non-répudiation [70].

3.5 Notions de base de la cryptographie :

3.5.1 Clés :

Une clé est une valeur numérique codé en bits utilisée avec un algorithme cryptographique pour produire une donnée chiffrée spécifique [71].

3.5.2 Chiffrement / Déchiffrement :

Le chiffrement est le processus cryptographique utilisant un algorithme avec une clé pour transformer une donnée en claire en une donnée chiffrée de manière à la rendre incompréhensible afin d'assurer le service de confidentialité [72]. Le déchiffrement est le processus inverse qui applique une transformation sur une donnée chiffrée de manière à le ramener dans sa forme original.

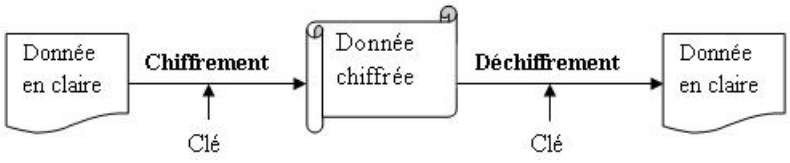

FIGURE 3.3: Chiffrement/ Déchiffrement[72].

3.5.3 Chiffrement symétrique :

La cryptographie symétrique (figure 3.4) utilise une même clé pour chiffrer et pour déchiffrer des données.

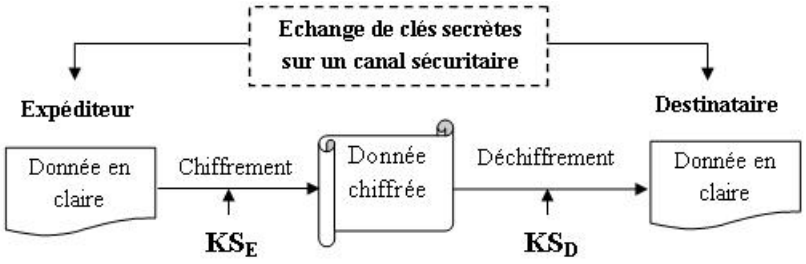

FIGURE 3.4: Chiffrement symétrique[73].

3.5.4 Chiffrement asymétrique (à clé publique) :

La cryptographie à clé publique repose sur un schéma asymétrique (cf.figure 1.3) utilisant une paire de clés : une clé publique, publiée dans des annuaires/serveurs de clés et accessible à tout le monde, et une clé privée, gardée secrètement et n'est connue que par son propriétaire [74].

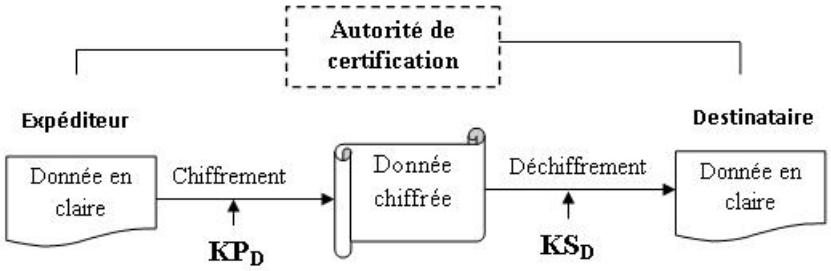

FIGURE 3.5: Le chiffrement asymétrique[74].

L'expéditeur chiffre la donnée avec la clé publique du destinataire KPD et l'envoie au destinataire. Ce dernier déchiffre la donnée avec sa clé secrète KSD.

3.5.5 Fonction de hachage :

Comme le processus de chiffrement/déchiffrement est long, la parade trouvée était d'uti-liser une fonction de hachage (figure 3.5)

FIGURE 3.6: Hachage[74].

La fonction de hachage calcule un haché de longueur fixe et petite, à partir d'une donnée de longueur variable et grande. Il est impossible de retrouver la donnée originale à partir du haché.

3.5.6 Signature numérique :

La signature d'une donnée est calculée à l'aide de la clé privée du signataire permettant à la personne qui reçoit cette donnée de contrôler l'authenticité de son origine et de vérifier que l'information en question n'a pas être modifiée [75]. Nous illustrons sur la figure 3.6 les étapes de passage pour la signature numérique :

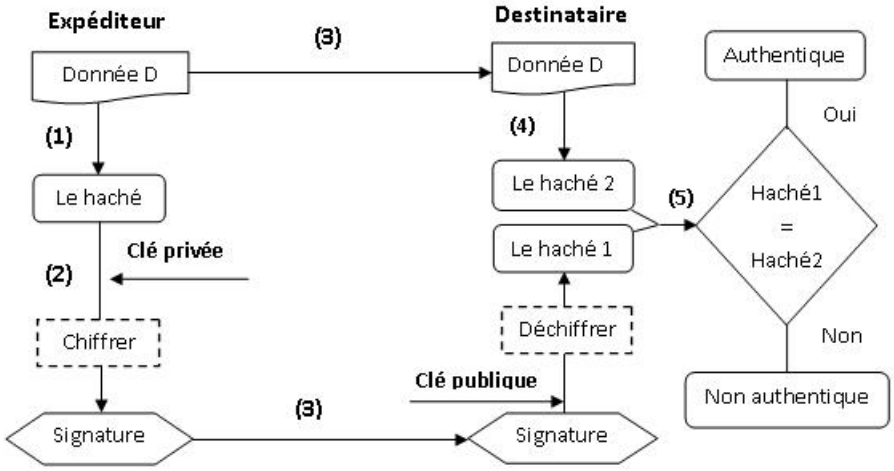

FIGURE 3.7: Signature numérique [75].

(1) L'expéditeur calcule le haché de la donnée D en utilisant une fonction de hachage.
(2) Il chiffre le haché avec sa clé privée.
(3) Le destinataire reçoit la donnée signée par l'expéditeur, il le déchiffre avec la clé pu-blique de ce dernier.
(4) Le destinataire calcule le haché de la donnée.
(5) Si les deux hachés sont égaux, alors l'expéditeur est authentifié.

3.5.7 Certificat à clé publique :

Un certificat est un document numérique liant une clé publique à une personne, une ap-plication ou un service. Il permet de valider des clés publiques. Un certificat numérique contient généralement les informations [76] suivantes :

— La version.
— Numéro de série.
— Algorithme de chiffrement utilisé pour signer le certificat.
— Nom de l'autorité de certification émettrice.
— Date de début de validité.
— Date de fin de validité.
— Clé publique du propriétaire.
— Signature numérique de l'autorité de certification.

3.6 Nouveau protocole ExOR proposé :

Il est nécessaire d'améliorer Le protocole ExOR pour répondre au problème de consommation d'énergie ainsi que la durée de vie des RCSFs, car il souffre de duplication de paquets et ceci cause un gaspillage en consommation d'énergie. Pour cela l'agrégation est l'une des techniques d'économie d'énergie considérée dans les RCSF. Le clustering est la méthode utilisée dans notre travail afin d'améliorer ExOR.

3.7 Le but du clustering :

Le clustering est un Processus qui partitionne un ensemble de données ou nœuds en sous-classes (clusters)[78],donc il nous permettra de regrouper les nœuds pour de former des clusters de N nœuds ayant des clusters Head (CH).

Sélection des candidats :

Afin de sélectionner un cluster, il est nécessaire de calculer l'ETX, ainsi que la distance entre le nœud i et le nœud j donc si la distance entre N(i) et N(j) est trop petite ou minimale, on dit qu'ils appartiennent au même cluster.

Nous avons élaboré un algorithme afin d'hiérarchiser ce réseau de nœuds ,l'algorithme 1 explique cette opération de sélection :

```
Pour i allant de 1 à N faire
|
|  pour j allant de i+1 faire
|
|   |        Si(Distance<Distance(i,j))alors
|   |       |
|   |       |  C[i]<-- i;
|   |       |
|   |       |  i ajouté à C[i];
|   |
|          fin si;
|
   fin pour;
fin pour;


   pour i allant de à N faire
   |
   |   Si(cluster(i)= vrai) alors
   |   |
   |   |  i<-- i+1;
   |   |sinon
   |   |
   |   |    C[i]<-- i;
   |   |
   |   |   i ajouté à C[i];
   |   |
   |    fin si;

       pour i<-- i+1 à N faire
       |   si (cluster(i)=Vrai) alors
       |   |
       |   |  j<-- j+1;
       |   |
       |   |sinon
       |   |
       |   |  si (ETX(i,j)< ETX) et (Distance<Distance(i,j)) alors
       |   |  |
       |   |  | j ajouté à C[i];
       |   |  fin si;
       |   ||
       |   fin si;
       fin pour;
```

Tel que : i est le noeud capteur i ; j est le noeud capteur j ; C est un cluster ; Cluster(i) est une procédure de type booléen qui vérifie si un nœud appartient à un cluster. Distance(i) est une procédure qui calcule la distance entre les différents nœuds du réseau.

3.7.1 Election des cluster Head (CH) :

Tout comme la selection des noeuds ,les clusters head (CH) sont choisi selon la métrique ETX, De sorte que le cluster ayant l'ETX minimum sera choisit comme cluster head (CH). L'algorithme 2 explique cette opération d'élection :

```
pour i allant de à N faire
|
|   Si(NBR(i)= 1) alors
|   |
|   |  le noeud est CH;
|   |sinon
|   |
|   |     Si(NBR(i)= 2) alors
|   |       |      si (ETX (N1)<ETX (N2))alors
|   |       |        |    N1 est CH;
|   |       |        | sinon  N2 est CH;
|   |       |    fin si;
|
|   |
|   |       |sinon
|   |       |        le noeud ayant l'ETX minimale sera CH;
|   |
|            fin si;
|
|    |fin si;
|fin pour;|
```

Tel que :
i est le nœud capteur i ; NBR() : une procédure qui calcule le nombre de nœuds dans le cluster. N1 :le nœud 1. N2 : le nœud 2. CH : le cluster head.

3.8 Fonctionnement du protocole :

Ce nouveau protocole d'ExOR amélioré fonctionne selon les points suivants :

— Selection des candidats : ExOR utilise une selection basé sur le nombre de sauts[45].

— Coordination des candidats : ExOR utilise une coordination, basée sur un acquittement[45].

— Acheminement des données : Determine les CH prioritaire lors de l'envoie des paquet,cette priorité est determiné selon la métrique ETX.

— Metrique utilisé : ETX est la métrique utilisée ,elle consiste a calculer le taux de transmissions des noeuds.

3.8.1 Différence entre ExOR et ExOR amélioré :

Voici un exemple du fonctionnement de l'ExOR :

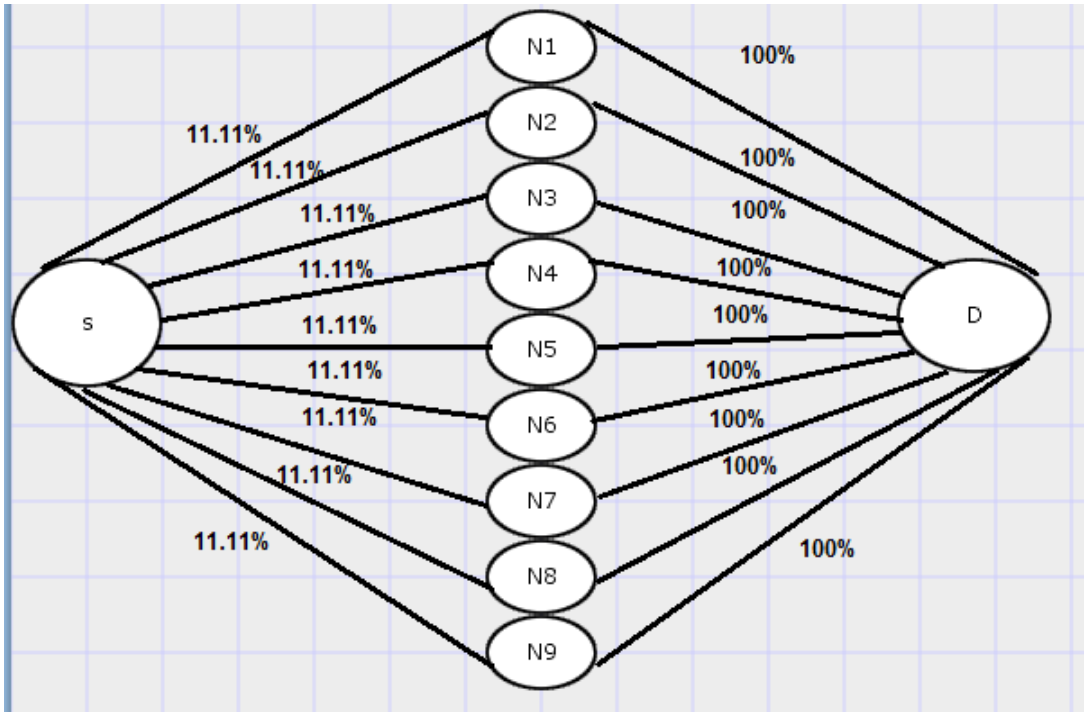

FIGURE 3.8: Probabilités qu'un paquet soit délivré à une destination utilisant ExOR.

S est le noeud source.

D est le noeud destination.
ETX est calculé ainsi :
ETX=1/(df*dr) tel (df*dr)=probabilité de transmission.
donc ETX= (1/Pr)
dans cet exemple on a :
Nbrtrans = 1/ETX
Nbrtrans =$[1/(1 \ \ (1 \ \ 0{,}1111)^9)] + 1 = 2.53 transmissions$

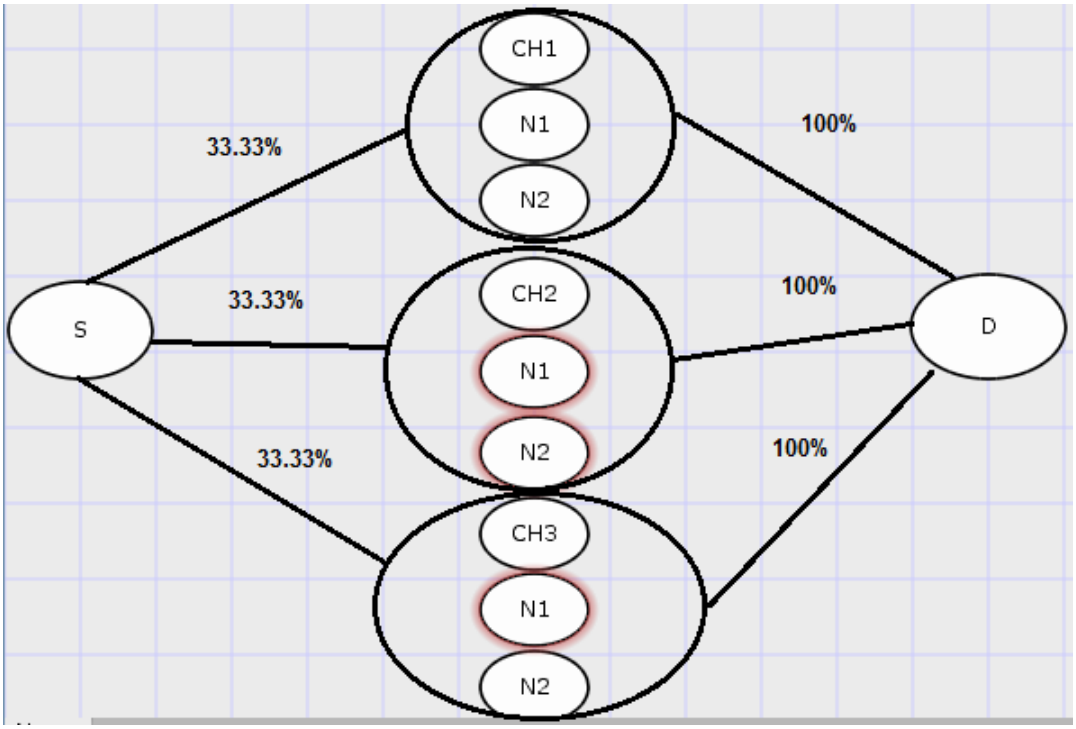

FIGURE 3.9: Probabilités qu'un paquet soit délivré à une destination utilisant le protocole proposé

Nbrtrans = $[1/(1–(1–0.3333)^3)] + 1 = 2.42 transmissions$

Nous constatons que le nombre de transmissions dans l'ExOR amélioré est inférieur à celui de l'ExOR ,ce qui explique une diminution en consommation d'énergie dans le deuxieme.Ceci est l'un des avantages de ce protocole.

3.9 Conclusion :

Dans ce chapitre, nous avons proposé une nouvelle stratégie de routage ExOR, qui est un routage opportuniste avec des mesures de sécurité ainsi l'agrégation qui est l'une des techniques d'économie d'énergie considérée dans les RCSF.

Dans le chapitre qui suit nous allons faire une abstraction de simulation de notre protocole qui représente un point très important dans l'analyse des performances afin d'expliquer les résultats de cette amélioration..

Chapitre 4

Abstraction de simulation

Ce dernier chapitre est sensé traiter l'implémentation et les resultats de simulation, du protocole ExOR ainsi que le protocole ExOR amélioré ,sous l'environnement de developpement Matlab. MATLAB est un langage de script émulé par un environnement de développement du même nom , il est utilisé à des fins de calcul numérique,MATLAB permet de manipuler des matrices, d'afficher des courbes et des données, de mettre en œuvre des algorithmes, de créer des interfaces utilisateurs, et peut s'interfacer avec d'autres langages comme le C, C++, Java, et Fortran[78].
Matlab est un simulateur très performant,contient un langage de programmation de haut niveau.

Cette partie devrait mesurer l'afficacité énergetique de l'ExOR et l'ExOR amélioré en tenant compte de certaines caractéristiques,tel que la durée de vie du réseau,taux de livraison et l'énergie consommée afin de prouver que l'ExOR amélioré est beaucoup plus performant que l'ExOR classique en terme de consommation d'énérgie... etc

Conclusion générale

Les réseaux de capteurs sont une nouvelle technologie qui a surgit après les grands progrès technologie concernant le développement des capteurs intelligents, des processeurs puissants et des protocoles de communications sans fil. Ils ont été classés parmi les 21 technologies les plus importantes du 21éme siècle. En effet, la recherche dans le domaine des capteurs est en train de vivre une révolution importante, ouvrant des perspectives d'impacts significatifs dans de nombreux domaines , pour que ces réseaux puissent mener à bien leurs missions ils doivent assurer un certain niveau de contrôle qui diffèrent selon l'application déployée.

Dans ce travail nous avons débuté par une étude approfondie sur les RCSFs dont le but est de mettre en évidence les services critiques du réseau, donc nous avons donné un aperçu sur les RCSF et certaines de leurs applications. D'un point de vue personnel, ce projet nous a apporté des bénéficies personnels, il a permis de découvrir un nouveau domaine, une nouvelle manière de programmer.

Bibliographie

[1] M. LEHSAINI, «Diffusion et couverture basées sur le clustering dans les réseaux de capteurs : application à la domotique. », thèse de doctorat en informatique, Université A.B Tlemcen Faculté des Sciences pour l'Ingénieur Université de Franche-Comté U.F.R Sciences et Techniques École Doctorale SPIM, 2009.

[2] Wikipédia,https ://fr.wikipedia.org/wiki/,réseaux de capteurs sans fil,Consulté de 11 Mars2020.

[3] M.Bagaa, N. Lasla, A. Ouadjaout and Y.Challal ; "SEDAN : Secure and Efficient protocol for Data Aggregation in wireless sensor Networks", 32nd IEEE Conference on Local Computer Networks (LCN 2007) pp. 1053-1060, Worksohop on Netwok Security.

[4] L. Paradis and Q. Han. A survey of fault management in wireless sensor networks.Plenum Press New York, USA, 2007.

[5] I. Teixeira, J.F. de Rezende, A. de Castro, and A.C.P. Pedroza. Wireless sensor network : Improving the network energy consumption. In XXI Symposium Brazilian Telecommunications, SBT'04, Belem, Brazil, 2004.

[6] I.F. Akyildiz, W. Su,et al. A survey on sensor networks. In IEEE Communications Magazine, volume 40, pages 102-116, 2002.

[7] M.BENAZZOUZ Surveillance de tout point d'une zone d'intert à l'aide d'un reseau de capteur multimedia ,memoire master,2013.

[8] V.Tsetsos,et all,Commercial wireless sensor networks : Technical and business issues. In 2nd International Conference on Wireless on Demand Network Systems and Service (WONS 2005), 19- 21 January 2005, St. Moritz, Switzerland, pages 166-173. IEEE Computer Society, 2005.

[9] Y.CHALLAL,réseau de capteur sans fil, support de cours, 17/11/2008.

[10] A.JORIO. « Le Clustering basé sur la Classification Spectrale pour l'Optimisation D'Energie dans les Réseaux de Capteurs Sans Fil Homogènes ». Thèse de Doctorat, 26/12/2015. .

[11] S. Chachulski, M. Jennings,et all, Trading structure for randomness in wireless opportunistic routing, Conference of the Special Interest Group on Data Communication, Kyoto, Japan, 2007, pp. 169-180.

[12] Règlement (CE) No 460/2004 du parlement européen et du conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information,2004.

[13] Wikipédia,https ://fr.wikipedia.org ,consulté le 01/07/2020.

[14] A.ABDESSELAM ,Conception d'un algorithme de routage basé sur l'heuristique du recuit simulé pour les réseaux de capteurs à grande échelle, mémoire master,2013.

[15] Waytolearnx, https ://waytolearnx.com différence entre attaque active et attaque passive, consultation 01/07/2020.

[16] techniquesingenieur,https ://www.techniques-ingenieur.fr, consulté le 01/07/2020.

[17] S.Biswas,R.Moris,ExOR : Opportunistic multi-hop routing for wireless networks. M.I.T, Computer Science and Artifcial Intelligence Laboratory,2005.

[18] S.Adel,"Performance Evaluation of AODV and DSDV Routing Protocol in wireless sensor network Environment", College of civil aviation and meteorology, Libya,2012.

[19] W.Heinzelman, A.Chandrakasan, H. Balakrishnan,"Energy-efficient communication protocol for wireless sensor networks", in : Proceeding of the Hawaii International Conference System Sciences, 2000.

[20] NS. CHELLOUG. Optimisation d'énergie dans les algorithmes de routage pour réseaux mobile. PhD thesis, Université Constantine 2, 2007.

[21] L. Loiseau. De l'exploitation des réceptions opportunistes dans les mécanismes de relayage pour les réseaux sans-fil. PhD thesis, l'Université de Rennes 1, 2013.

[22] S.Tuenkam, Opportunistic Routing June 22, 2016.

[23] L. babu and P. Balasubramanie. A survey on opportunistic routing protocols. International Journal of Innovative Research in Computer and Communication Engineering, 2014.

[24] A. MOURADIAN. Proposition et vérification formelle de protocoles de communications temps-réel pour les réseaux de capteurs sans fil. PhD thesis, Ecole doctorale Lyon, 2013

[25] S. OUARET and M. ATMANI. Amélioration du protocole de routage gossiping dans les réseaux de capteurs.Master's thesis, Université Abderahmane Mira de Béjaïa, 2008.

[26] N. Chakchouk, A Survey on Opportunistic Routing in Wireless Communication Networks, IEEE Communication Surveys Tutorials, Vol. 17, No. 4, 2015, pp. 2214- 2241.

[27] A. Darehshoorzadeh, L. Cerda-Alabern, and V. Pla, Opportunistic routing in wireless mesh networks,springer science and business media, 2013.

[28] A. Abins and N. Duraipandian. Survey on opportunistic routing protocols in wireless networks. American-Eurasian Journal of Scientific Research, 2015.

[29] A. Triviño-Cabrera and S. Cañadas-Hurtado, Survey on Opportunistic Routing in Multihop Wireless Networks, International Journal of Communication Networks and Information Security,

Vol. 3, No. 2, 2011, pp.170-177.

[30] Chee-Yee Chong,Srikanta P. Kumar Sensor Networks : Evolution, Opportunities, and Challenges,2008.

[31] C.-J. Hsu, H.-I. Liu and W. Seah, Economy : a duplicate free opportunistic routing, International Conference on Mobile Technology, Application and Systems, Nice,France, 2009, pp. 1-6.

[32] Z. Zhong, J. Wang, G-H. Lu and S. Nelakuditi, On Selection of Candidates for Opportunistic Any-Path Forwarding, SIGMOBILE Mobile Computing and Communications Review, Vol. 10, No. 4, 2006, pp. 1-2.

[33] A. Darehshoorzadeh, L. Cerda-Alabern, and V. Pla. Opportunistic routing in wireless mesh networks. springer science and business media, 2013.

[34] N. Ahmed, S. S. Kanhere, et S. Jha, « The holes problem in wireless sensor networks : a survey », SIGMOBILE Mob. Comput. Commun. Rev., vol. 9, no 2, p. 4–18, 2005.

[35] S. Biswas and R. Morris, ExOR : opportunistic multi-hop routing for wireless networks, Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Philadelphia, Pennsylvania, USA, 2005, pp. 133-144.

[36] E. Rozner,et al, SOAR : simple opportunistic adaptive routing protocol for wireless mesh networks, IEEE Transactions on Mobile Computing, Vol. 8, No. 12, 2009, pp. 1622- 1635.

[37] K. Zeng,et al, On throughput efficiency of geographic opportunistic routing in multihop wireless networks, Mobile Networks and Applica-tions, Vol. 12, No. 5, 2007, pp. 347- 357.

[38] H. Liu,et al, Opportunistic routing for wireless ad hoc and sensor networks. IEEE Communications Magazine, 2009.

[39] Denis Conan, Télécom sudPari,.Algorithme à base de jeton de Ricart et Agrawala , et de Suzuki et Kasami,consulté le 14 Avril 2020.

[40] Jean-François Pilou. La Couche Liaison WIFI, la Couche Liaison de Données. Comment ça marche, 2016.

[41] El.Ar-Reyouchi,Optimisation des performances des réseaux de communications sans fil : Performances des réseaux de communications sans fil pour la télégestion des stations de la Télédiffusion TV/FM,juin2017.

[42] S. Biswas and R. Morris, ExOR : opportunistic multi-hop routing for wireless networks, Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Philadelphia, Pennsylvania, USA, 2005, pp. 133-144.

[43] M.Akbar Hossain .A distributed multichannel MAC protocol for estabilishement in cognitive radio Ad Hoc networks,novembre 2017.

[44] K. MESSAD,L. RAHMANI, Le routage opportuniste dans les réseaux de capteurs sans fil, mémoire master,2016.

[45] E. Rozner, J. Seshadri, Y-A.Mehta, L.Qiu, 'SOAR : Simple Opportunistic Adaptive Routing Protocol for Wireless Mesh Networks' . IEEE Transactions on Mobile Computing 2009.

[46] X.Mao et al,Energy-Efficient Opportunistic Routing in Wireless Sensor Networks,IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22,2011.

[47] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard and J. Crowcroft, Xors in the air : practical wireless network coding, IEEE/ACM Transactions On Networking, Vol. 16, No. 3, 2008, pp. 497-510.

[48] J. Zhang, Y. P. Chen and I. Marsic, Network Coding Via Opportunistic Forwarding in Wireless Mesh Networks, IEEE Wireless Communications and Networking Conference, Las Vegas, Nevada, USA, 2008, pp. 1775-1780.

[49] D. Chen, J. Deng and P. K. Varshney, Selection of a Forwarding Area for ContentionBased Geographic Forwarding in Wireless Multi-Hop Networks, IEEE Transactions on Vehicular Technology, Vol. 56, No. 5, 2007, pp. 3111-3122.

[50] S. Yang, C. K. Yeo and B. S. Lee, Robust Geographic Routing with Virtual Destination based Void Handling for MANETs, IEEE Vehicular Technology Conference, Ottawa, Canada, 2010, pp. 1-5.

[51] P. Spachos, P. Chatzimisios and D. Hatzinakos, Energy Aware Opportunistic Routing in Wireless Sensor Networks, IEEE Globecom Workshops, Anaheim, California, USA, 2012, pp. 405-409.

[52] J. Kim and B. Ravindran, Opportunistic real-time routing in multihop wireless sensor networks, Symposium on Applied Computing, Honolulu, Hawaii, USA, 2009, pp. 2197-2201.

[53] W. Yang, W. Liang and W. Dou, Energy-Aware Real-Time Opportunistic Routing for Wireless Ad Hoc Networks, IEEE Global Telecommunications Conference, Miami, Florida, USA , 2010, pp. 1-6.

[54] C-Ch. Hung, K-. C-J. Lin, C-C. Hsu, C-F. Chou and C-J. Tu, On Enhancing Network-Lifetime Using Opportunistic Routing in Wireless Sensor Networks, IEEE Computer Communications and Networks, Zürich, Switzerland, 2010, pp. 1-6.

[55] A. Tiab, L. Bouallouche-Medjkoune and S. Boulfekhar, A new QoS aware and energy efficient opportunistic routing protocol for wireless sensor networks, International Journal of Parallel Emergent and Distributed Systems, 2016, pp. 1-17.

[56] A.tiab, ROUTAGE DANS LES RCSFS EN ENVIRONNEMENT INDUSTRIEL : ÉCONOMIE D'ÉNERGIE ET QUALITÉ DE SERVICE,thése de doctorat,2017.

[57] Y.Guang, Protocoles de routage opportunistes et avec qualité de service pour les réseaux véhiculaires VANETs, Réseaux et télécommunications [cs.NI]. Université Paris Sud - Paris XI, 2015.

[58] R. Santos, A. Edwards, R. Edwards, and N. Seed. Performance evaluation of routing protocols in vehicular adhoc networks. International Journal of Ad Hoc and Ubiquitous Computing, 1(2) :80–91, Nov. 2005.

[59] H. Liu, B. Zhang, H. T. Mouftah, X. Shen, and J. Ma. Opportunistic routing for wireless ad hoc and sensor networks. IEEE Communications Magazine, 2009.

[60] Yawen Barowski, Saad Biaz, and Prathima Agrawal. Towards the performance analysis of IEEE 802.11 in multi-hop ad-hoc networks. In IEEE Wireless Communications and Networking Conference, 2005, volume 1, pages 100–106. IEEE, 2005.

[61] M. Conti and M. Kumar. Opportunities in opportunistic computing. Computer, 43(1) :42–50, 2010.

[62] Sanjit Biswas et Robert Morris, «ExOR : Opportunistic MultiHop Routing for Wireless Networks». Dans ACM SIGCOMM'05, 21-26 août 2005.

[63] J.Mangues-Bafalluy,A Survey on Routing Protocols that really Exploit Wireless Mesh Network Features,Journal of Communications ,Mars 2010.

[64] D. De Couto, D. Aguayo, J. Bicket, and R. Morris. A high-throughput path metric for multi-hop wireless routing. In Proc. ACM/IEEE MobiCom, September 2003.

[65] B.Wu, J. Chen, J. Wu, and M. Cardei. "A survey on attacks and countermeasures in mobile ad hoc networks". Wireless Network Security, pages 103–135, 2007.

[66] J.Fuentesand, A. Gonzlez-Manzano, A. Gonzlez-Tablas, and J. Blasco, "Security Models in Vehicular Ad-hoc Networks : A Survey". IETE Technical Review, 31(1) :47–64, 2014.

[67] M. Riguidel G. Wang Y. Wu, Y. Zhao and P. Yi. Security and trust management in opportunistic networks : a survey. Security Comm. Networks, 8 :18121827, 2015.

[68] Babakhouya, A. and Challal, Y. and Bouabdallah, A. and Gharout, S. "Securing Distance Vector Routing Protocols for Hybrid Wireless Mesh Networks", SAR-SSI 2010

[69] Ouadjaout, A., M. Bagaa, A. Bachir, Y. Challal, N. Lasla, L. Khelladi, "Information Security in Wireless Sensor Networks" in Encyclopedia on Ad Hoc and Ubiquitous Computing, pp. 427-472, World Scientific, 2009

[70] M. Riguidel G. Wang Y. Wu, Y. Zhao and P. Yi. Security and trust management in opportunistic networks : a survey. Security Comm. Networks, 8 :18121827, 2015.

[71] M.Mehdi, A.Anou, S.Zair, M.Bensebti and M.Djebari « la Sécurité dans les Réseaux Ad Hoc », March 25-29, 2007.

[72] E-watching.net, sécurité informatique "Explications sur la cryptographie" Version 1.0, 22 fevrier 2008.

[73] Patra R, Surana S, Nedevschi S. Hierarchical identity based cryptography for end-to-end security in DTNs. In : 4th international conference on intelligent computer communication and processing (ICCP) ; August 2008.

[74] Paul C. Kocher , Cryptography Research, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems ".

[75] Zhongtian Jia, XiaodongLin, Seng-HuaTan, LixiangLi, YixianYang. Public key distribution scheme for delay tolerant networks based on two-channel cryptography, Journal of Network and Computer Applications, 9 March 2011.

[76] M. Ouwais Kabaou,H.Hamouda,Implementation and Evaluation of Opportunistic Routing Protocols for Wireless and New Generation Communication Networks,2020.

[77] M.Rifqi,Clustering,2001-2002.

[78] Wikipédia,https ://fr.wikipedia.org/wiki/MATLAB,consulté le 26/09/2020.

Mots clé : WSN,RO,ExOR.