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

Université Amar Thelidji- Laghouat

FACULTE: DE TECHNOLOGIE

DEPARTEMENT : D'ELECTRONIQUE

MEMOIRE DE MASTER

Réalisé par : Regue Soumia & Souici Wahiba

DOMAINE : Science et Technologie

FILIERE : Télécommunication

OPTION : Systèmes de télécommunications

Thème

Sécurité du routage hiérarchique dans les réseaux de capteurs sans fil

Jury de soutenance :

Nom et Prénom	Grade	Qualité
MESMOUDI Samira	MCB	Encadrant
	MCA	Président
	MCB	Examinateur

Promotion : 2021/2022

Remerciement

Avant tout nous remercions ALLAH de nous avoir donné la volonté pour préparer ce travail.

Notre gratitude et notre reconnaissance que nous saurions Suffisamment exprimer vont d'abord à notre encadreur madame **MESMOUDI Samira** *qui nous a proposé suivi, dirigé et encouragé pour finir ce travail avec une très grande générosité, qu'elle trouve ici l'expression de nos meilleures salutations.*

Nos remerciements vont aussi :

Les nombres du jury qui nous ont fait l'honneur d'évaluer et juger notre travail.

Nous voudrons aussi exprimer notre vive reconnaissance envers tous les enseignants de département d'électronique ainsi que tous ceux qui ont participé à notre formation

Dédicaces

J'ai l'honneur de dédier ce modeste travail réalisé grâce à l'aide De Dieu Tout puissant

*A mes chers **parents**, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,*

*A ma chère sœur **Bent lhadj** et mes chérs fréres **Hamza** & **Youcef** & **Bachir** pour leurs encouragements permanents, et leur soutien moral*

A toute ma famille pour leur soutien tout au long de mon parcours universitaire,

*A mon fiancé **Walid** et mes chères cousines **Djihane** & **Ihssane***

*A mes chères amies **Aicha** & **Souad** & **Meriem** & **Leila & Wahiba***

Sans oublié ma chére tante Fatima et mon camarade Ahmed Chaib silàa Allah yarhmhom

Soumia regue

Dédicaces

J'ai J'ai l'honneur de dédier ce modeste travail réalisé grâce à l'aide De Dieu Tout puissant
A mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,
A mon mari chère Ibrahim nebair
A mes chères sœurs amina aya anfal israa marwa tasnim pour leurs encouragements permanents, et leur soutien moral
A mes chères frères Ibrahim salem Ahmed anas
A toute ma famille pour leur soutien tout au long de mon parcours universitaire

Sans oublié mon camarade Ahmed Chaib silàa Allah yarhmo

Wahiba Souici

Résumé

Les Réseaux Les réseaux de capteurs sans fil (WSN) sont souvent déployés dans des environnements difficiles, Cela les rend très vulnérables. Par conséquent, il est nécessaire d'assurer la sécurité des communication est l'un des défis les plus importants de RCSF. en raison des ressources mémoire Limité et limité en énergie, incapacité à utiliser des algorithmes de sécurité complexe dans les réseaux de capteurs. Notre objectif dans ce projet de fin de recherche est de trouver une solution Il intègre le mécanisme de sécurité du protocole de routage en couches LPWS (A New protocole de regroupement de capteurs sans fil basé sur la localisation). Utiliser MAC (message Code d'authentification) et des clés préchargées au niveau du nœud pour la sécurité communication, ce qui nous aidera à obtenir un algorithme efficace pour faire face aux intrusion un taux de détection très élevé.

Mots clés : Réseaux de capteurs sans fil, sécurité, routage hiérarchique, LPWS.

Abstract:

Wireless Wireless Sensor Networks (WSNs) are often deployed in harsh environments, making them highly resilient vulnerable. Therefore, ensuring communication security is one of the most important requirements a major challenge for RCSF. Complicated due to limited memory resources and performance constraints Security algorithms cannot be used in sensor networks. Our goals in this final project are this paper proposes a combination of hierarchical routing protocol LPWS (a new location-based protocol for wireless sensor clusters). Use MAC (message verification code) and the pre-shared key on the node to ensure the security and This will help us get an efficient algorithm to deal with intruders with a very high detection rateValuation

Keywords: Wireless sensor network, Security, Hierarchical routing protocol, LPWS.

ملخص

غالبًا ما يتم نشر شبكات االستشعار الالسلكية (RCSFs) في بيئات قاسية ، مما يجعلها عرضة للهجمات. لذلك ، من الضروري التأكد يعد االتصال أحد أهم التحديات في RCSF ، وادام خوارزميات أألمان بسبب موارد الذاكرة المحدودة وقيود الطاقة. شبكات االستشعار
المعقدة. هدفنا في مشروع نهاية البحث هذا هو اقتراح حل يدمج آليات أألمان لبروتوكوالت التوجيه الهرمي يضمن LPWS (بروتوكول
تجميع المستشعر الالسلكي الجديد المستند إلى الموقع(استخدام MAC(رمز مصادقة الرسالة(أمن مستوى العقدة ومفاتيح أمان االتصال مسبقة
التحميل ، والتي ستساعدنا في الحصول على خوارزمية فعالة للتكيف عمليات االقتحام لها معدل اكتشاف مرتفع جدًا.

الكلمات المفتاحية :

شبكات االستشعار الالسلكية المن بروتوكول التوجيه ذي التسلسل الهرمي LPWS

Table des matières

Liste des figures

Liste des tableaux

Introduction générale

La D'énormes développements dans les domaines de la microélectronique, de la micromécanique et des technologies de communication sans fil ont permis de produire de petits dispositifs de détection et de communication à des coûts raisonnables. Ces dispositifs sont appelés nœuds capteurs. Ils sont capables de collecter des données environnementales et de les transmettre à des points centralisés appelés stations de base ou récepteurs. Tous les nœuds de capteurs forment un réseau de capteurs sans fil (RCSF). Ce type de mise en réseau est largement utilisé et fait l'objet de plusieurs études scientifiques. C'est une solution efficace dans diverses applications telles que militaire, environnementale, domotique, industrielle, etc.

Dans RCSF, le routage des données vers les stations de base est une opération fondamentale. Cependant, le schéma de routage conçu doit prendre en compte les modifications de la topologie du réseau, ainsi que d'autres caractéristiques telles que la bande passante, la qualité de la liaison et les contraintes de puissance. Ces facteurs affectent négativement les performances des protocoles de routage. Dans ce cadre, plusieurs études ont été menées, notamment pour garantir un acheminement fiable des données et optimiser les économies d'énergie.

Dans cet mémoire, nous nous concentrerons sur les problèmes liés au routage des données sur RCSF et sur le routage hiérarchique plus précis des données. Ce dernier est considéré comme un outil qui permet des performances plus élevées en termes de consommation d'énergie par rapport aux autres types de routage (c'est-à-dire le routage à topologie plate). Bien que ces protocoles puissent augmenter la durée de vie du réseau en manipulant ses ressources tout en respectant plusieurs contraintes telles que la consommation d'énergie, ils présentent également certaines limites. En effet, aucun mécanisme de sécurité n'est intégré à ces protocoles. Par conséquent, ils sont vulnérables même aux attaques simples. Par conséquent, un attaquant peut facilement monopoliser le réseau et le faire mal fonctionner. Notre projet comprend la sécurisation du protocole de routage en couches LPWS. En effet, notre solution doit garantir un compromis entre performance, simplicité et efficacité.

Organisation de mémoire

Ce manuscrit est organisé en trois chapitres suivis d’une conclusion générale :

- Le premier chapitre est une introduction et généralités sur les réseaux de capteurs sans fil : leurs définitions, leurs caractéristiques ainsi que leurs architectures et leurs domaines d'application sont présentés. Puis, nous avons présenté quelques protocoles de routage.
- Dans le deuxième chapitre, nous présentons un aperçu sur les concepts de sécurité dans les RCSFs qui diffèrent des autres réseaux. Nous commençons d'abord par les limites des réseaux de capteurs qui rendent la sécurité pour ce type de réseaux un véritable défi. Enfin, nous identifions une taxonomie des attaques et nous discutons les besoins des différents mécanismes de sécurité destinés aux RCSFs
- Le troisième chapitre concerne une solution de sécurisation pour le protocole LPWS. Il présente le schéma de sécurisation, le déroulement de notre protocole SEC-LPWS et les résultats de simulation seront alors donnés pour confirmer notre proposition.

Enfin, une conclusion générale sera donnée pour résumer les grands points qui ont été abordés.

Chapitre 1

Généralités sur les réseaux de capteurs sans fil

Introduction

Un réseau de capteurs sans fil (plus connus sous le nom de Wireless Sensor Network (WSN) en anglais) est composé d'un ensemble de terminaux ou ce qu'on appelle des nœuds capteurs qui peuvent communiquer via des liaisons radio, sans infrastructure fixe préalable. Le réseau devra fonctionner de façon autonome, sans intervention humaine. Les nœuds sont généralement matériellement petits, construits à partir des composants pas chers. Ce type de réseau est composé de centaines ou de milliers d'éléments (capteurs), a pour but la collecte de données de l'environnement, leur traitement et leur transmission vers le monde extérieur.
Nous allons retracer dans ce chapitre le fonctionnement général des réseaux de capteurs sans fil. Nous abordons d'abord les composants d'un capteur sans fil et ses fonctionnalités, leurs architectures protocolaire, les différentes topologies et organisation utilisées dans ce genre de réseau, leurs domaines d'applications, par la suite nous définissons également les principaux facteurs et contraintes qui influencent la conception des réseaux de capteurs sans fil. Et finalement, nous avons affecté la conception des protocoles de routage au sein des RCSF.

Les nœuds de réseau de capteur sans fil

Un nœud de capteur sans fil est un petit dispositif électronique capable d'interagir avec l'environnement où il est déployé, de mesurer une valeur physique (température, lumière, pression, etc.), et de la communiquer à un centre de contrôle via une station de base. Dans Les deux prochaines sous-sections. Nous écrivons d'abord les différents modules matériels du nœud capteur. Puis, nous consacrons la suite au système d'exploitation qui commande les modules matériels.

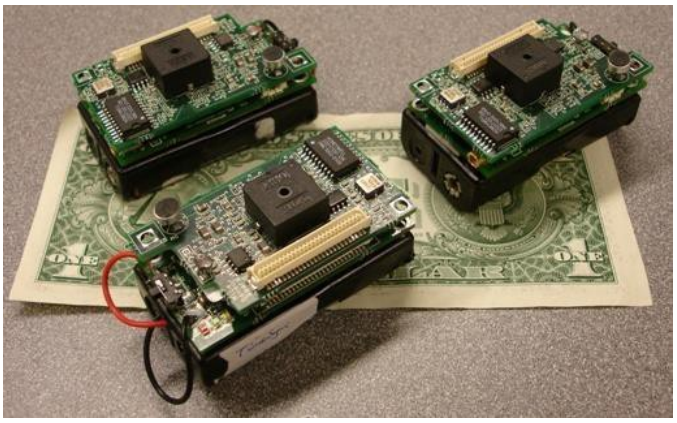


Figure 1.1. : Capteur sans fil

Aspect matériel

Le nœud de capteur est composé principalement de quatre unités : l'unité d'acquisition, l'unité de traitement, l'unité de communication et l'unité d'énergie (voir figure 1.2).

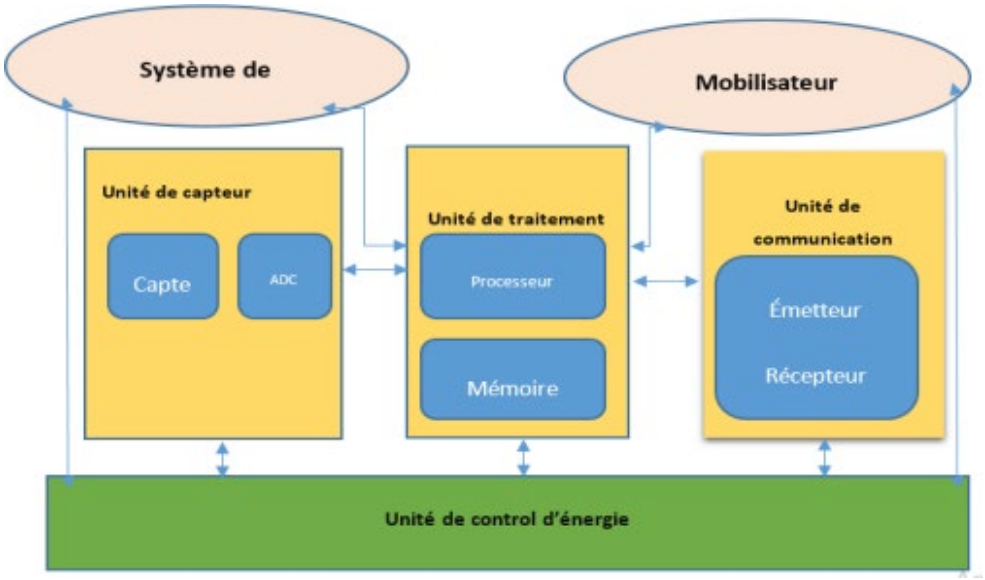


Figure 1.2 : les composants de base d'un nœud capteur sans fil [2]

Unité d'acquisition :

Elle se compose de deux sous unités, unité de captage et un convertisseur analogique numérique (CAN) [3].

- Les capteurs obtiennent des mesures sur les paramètres environnementaux sous forme analogique,
- Le CAN convertit ces données analogiques en données numériques compréhensibles par l'unité de traitement [4].

Unité de traitement :

Cette unité est également composée d'un processeur qui supporte un système d'exploitation spécifique tel que Contiki et Tinyos [4]. Elle comprend de deux interfaces : une interface pour l'unité d'acquisition et une autre pour l'unité de transmission. Elle est chargée de gérer des procédures qui permettent à un nœud capteur de collaborer avec les autres nœuds du réseau. Elle peut aussi analyser les données captées pour alléger la tâche du nœud puits [3].

Unité de communication :

Cette unité est responsable de toutes les émissions et les réceptions de données via un support de communication sans fil et une antenne [4]. Ce dernier peut être de type optique (comme dans les capteurs Smart Dust) ou de type radio fréquence (MICA2).

Unité d'énergie :

Cette unité est responsable de la gestion de l'énergie et de l'alimentation de tous les composants du capteur, généralement se trouve sous la forme de batterie de basse tension ou des piles. Les batteries utilisées peuvent être rechargeables par l'énergie solaire. [2].
De plus, un nœud capteur peut être équipé par d'autres composants supplémentaires tels que :

- Système de localisation géographique GPS (Global Position System).
- Un dispositif mobilisateur chargé de déplacer le capteur pour accomplir la requête assignée

Le système d'exploitation

Les systèmes d'exploitation pour les RCSFs sont des systèmes temps réel configurables pour une tâche donnée et pour optimiser l'utilisation des ressources. Tinyos [5] est le système d'exploitation le plus répondu dans la littérature. Tinyos est un système d'exploitation open-source conçu pour les réseaux de capteurs sans fil. Il respecte une architecture basée sur une association de composants, réduisant la taille du code nécessaire à sa mise en place. Cela s'inscrit dans le respect des contraintes de mémoire qu'observent les réseaux de capteurs sans fil. La conception de Tinyos a été écrite entièrement en NesC (Network Embedded System C) [6] , une extension de C. Sa bibliothèque de composants comprend les protocoles réseaux, les services de distribution, des pilotes de capteurs et les outils d'acquisition de données. Il existe aussi d'autres systèmes d'exploitation pour les RCSFs tel que Contiki, MANTIS (The MultimodAl system for NeTworks of In-situ wireless Sensors), Nano- RK, LiteOS.

Réseau de capteur sans fil (RCSF)

Architecture des réseaux de capteurs sans fil

Un réseau de capteur sans fil(RCSF), consiste en un ensemble de nœuds capteurs variantes de quelques dizaines d'éléments à plusieurs milliers, placés de manière, plus ou moins aléatoire, dans une zone géographique appelée zone de captage, ou zone d'intérêt, afin de surveiller un phénomène physique et de récolter leurs données d'une manière autonome. Les nœuds

capteurs utilisent une communication sans fil pour acheminer les données captées vers un nœud collecteurs appelé nœud puits (sink en anglais), ou par satellite à l'ordinateur central (Gestionnaire de taches) pour analyser ces données et prendre des décisions. Ainsi, l'utilisateur peut adresser des requêtes aux autres nœuds du réseau, précisant le type de données requises, puis récolter les données environnementales captées par le biais du nœud puits. En plus des nœuds capteurs, le modèle peut introduire les super-nœuds, appelés des passerelles (Gatways) [7]. Ces derniers possèdent une source d'énergie importante, la capacité de traitement et de stockage plus élevées comparativement aux nœuds capteurs. Ils peuvent ainsi être utilisés pour exécuter les taches plus complexes comme la fusion des données issues des capteurs d'une même zone. Dans le cas le plus simple, les nœuds capteurs seront dans le voisinage direct du puits (communication à un a un saut). Cependant, dans le cas d'un réseau à grande échelle, ils ne sont pas tous dans le voisinage du puits et les données seront acheminées du nœud source vers le puits en transitant par plusieurs nœuds, selon un mode de communication multi-sauts comme l'illustre la figure 1.3 ci-après.

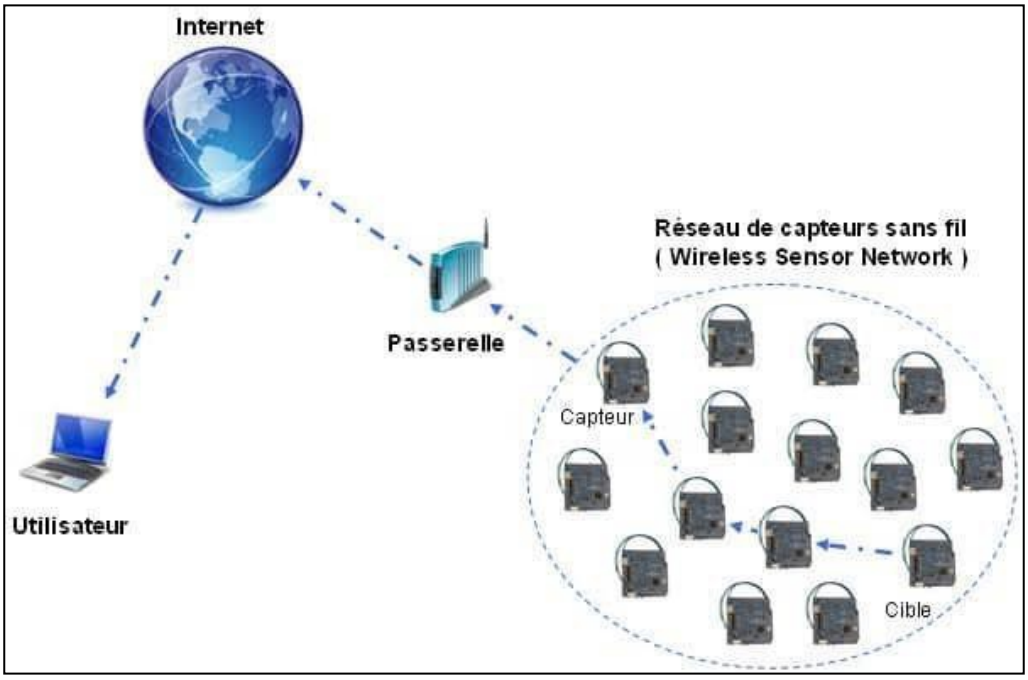


Figure1.3 : Architecture d'un réseau de capteurs sans fil

Model de Collecte d'informations

Il y a deux méthodes pour collecter les informations dans un réseau de capteurs.

- **Collecte d'informations à la demande :**

Lorsque l'on souhaite connaitre l'état de la zone d'intérêt à l'instant t, le nœud puits émet une requête en broadcasté vers tous les nœuds déployés dans la zone d'intérêt pour que ces derniers remontent leur dernier relevé vers le nœud puits. Les informations sont alors acheminées vers le nœud puits par le biais d'une communication multi-sauts.

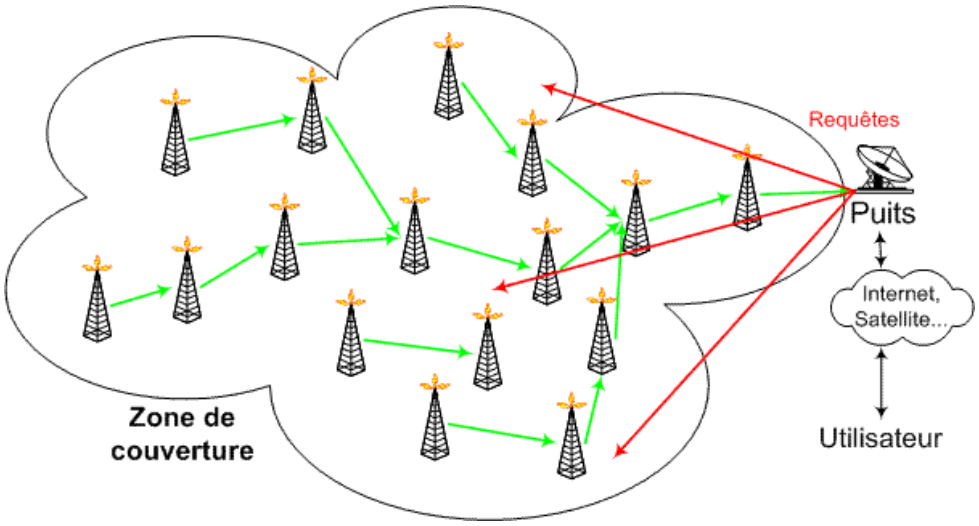


Figure 1.4 : Collecte d'informations à la demande [8]

- **Suite à un événement**

Suite à un événement se produit en un point de la zone d'intérêt (changement brusque de température, détection d'un mouvement...), les capteurs situés à proximité de ce point cible remontent alors les informations relevées et les acheminent jusqu'au nœud puits. [2]

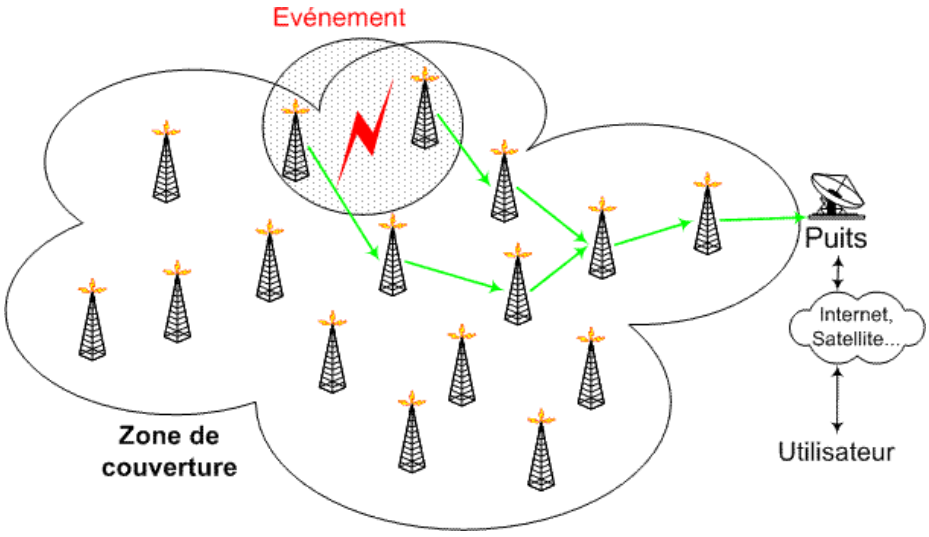


Figure 1.5 : application orientée événement [8]

Topologie et organisation de RCSF

La topologie détermine l'organisation des capteurs dans le réseau, une fois les nœuds capteurs déployés, ils s'auto-organisent et s'auto-configurent pour constituer un réseau. Les topologies dans les réseaux de capteurs dépendent des applications et des techniques utilisées pour faire acheminer l'information des capteurs à la station de base [9] . Il existe deux principales topologies dans les RCSFs.

Topologie plate

Dans une topologie plate, le réseau est homogène, où tous les nœuds ayant les mêmes caractéristiques matérielles (même capacité de calcul, capacité énergétique, capacité de stockage, portée de communication, etc.). Cette architecture est utilisée pour une densité de capteurs élevée (plusieurs nœuds capteurs / m^2). Les capteurs peuvent communiquer directement avec la station de base (Figure 1.6) en utilisant une forte puissance, ou via un mode multi-sauts avec des puissances très faibles (c'est-à-dire que l'information envoyée par un nœud récolteur doit transiter par plusieurs nœuds intermédiaires avant d'atteindre sa destination finale sur le réseau et sans aucun traitement supplémentaire sur la donnée transportée). [9]

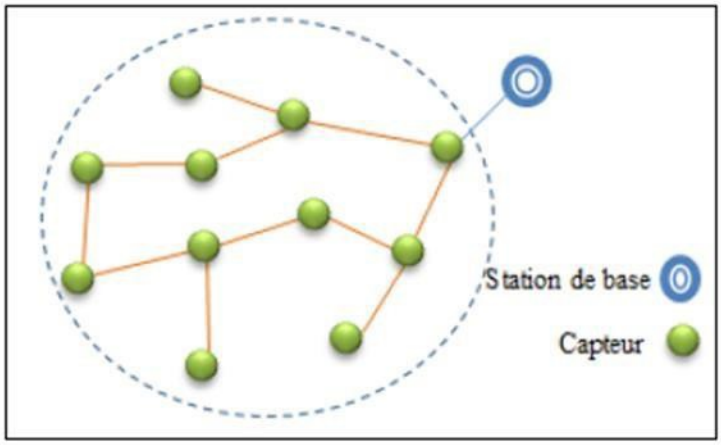


Figure 1.6 : Topologie Plate [9]

Topologie Hiérarchique

Le principe de cette topologie est de partitionner le réseau en plusieurs groupes (ou clusters) dont chacun est vu comme un sous réseau ayant la topologie en étoile. Chaque groupe possède un chef qui relie les membres de son groupe à la station de base. La communication entre les nœuds capteurs et le chef du cluster peut être directe ou indirecte (en multi-sauts) pour les nœuds distants. Ainsi, il peut y avoir plusieurs niveaux dans la hiérarchie, où les chefs des clusters forment entre eux des chaînes menant vers la station de base [10]

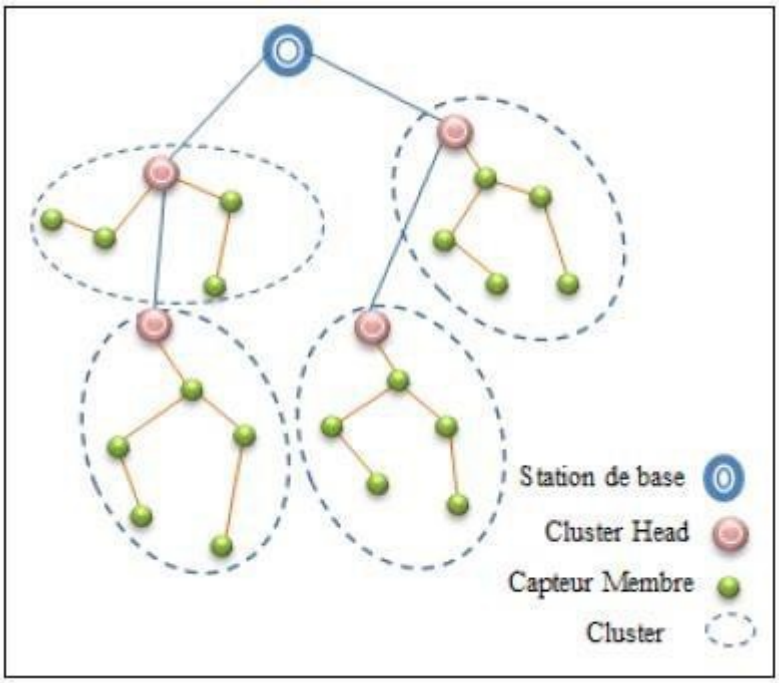


Figure 1.7 : Topologie hiérarchique [9]

Architecture protocolaire dans les RCSF

Les réseaux de capteurs sans fil imposent des contraintes supplémentaires aux protocoles de communication. Par conséquent, le modèle traditionnel en couches (modèle OSI), ne répond pas aux exigences de ce type particulier de réseaux. En effet, dans le but d'un établissement efficace d'un RCSF, une architecture en couches est adoptée afin d'améliorer la robustesse du réseau. Une pile protocolaire de cinq couches similaires à celles du modèle OSI (physique, liaison, réseau, transport et application) et de trois plans de gestion : un plan de gestion d'énergie, un plan de gestion de mobilité et un plan de gestion de taches est donc utilisée par les nœuds du réseau (Figure 1.5).

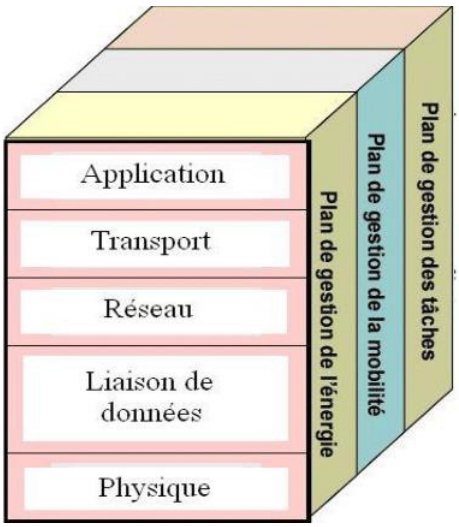


Figure 1.8 : Pile protocolaire dans les réseaux de capteurs

Couches de la pile protocolaire

Suivant la fonctionnalité des capteurs, différentes applications peuvent être utilisées et bâties sur la couche application. La couche transport aide à gérer le flux de données si le réseau de capteurs l'exige. Elle permet de diviser les données issues de la couche application en segments pour les délivrer, ainsi elle réordonne et rassemble les segments venus de la couche réseau avant de les envoyer à la couche application. La couche réseau prend soin de router les données fournies par la couche transport. Le protocole MAC (Media Access Control) de la couche liaison assure la gestion de l'accès au support physique. La couche physique assure la transmission et la réception des données au niveau bit.

Plans de gestions

Les plans de gestion d'énergie, de mobilité et de tâche contrôlent l'énergie, le mouvement et la distribution de tâche au sein d'un nœud capteur. Ces plans aident les nœuds capteurs à coordonner la tâche de captage et minimiser la consommation d'énergie. Ils sont donc nécessaires pour que les nœuds capteurs puissent collaborer ensemble, acheminer les données dans un réseau mobile et partager les ressources entre eux en utilisant efficacement l'énergie disponible. Ainsi, le réseau peut prolonger sa durée de vie.

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

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

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

Consommation et conservation d'énergie d'un nœud capteur

Un nœud capteur sans fil étant un dispositif micro-électronique, il ne peut être équipé que par une source limitée d'énergie. La batterie est considérée comme l'unique alimentation en ressources énergétiques des capteurs, dont la capacité est limitée étant donné sa petite dimension et son remplacement ou rechargement est souvent impossible. Au-delà de l'endroit hostile ou difficile d'accès avec moins de contrôle et d'existence humaine.

Le modèle de consommation d'énergie

Un nœud capteur utilise son énergie pour réaliser trois actions principales comme le montre la figure 1.9 :

- L'acquisition des données,
- La communication,
- Le traitement des données.

L'énergie totale consommée par un nœud capteur est donnée par la formule suivante **:**

$$E_{total} = E_{capture} + E_{transmission} + E_{réception} + E_{traitement} \quad (1.1)$$

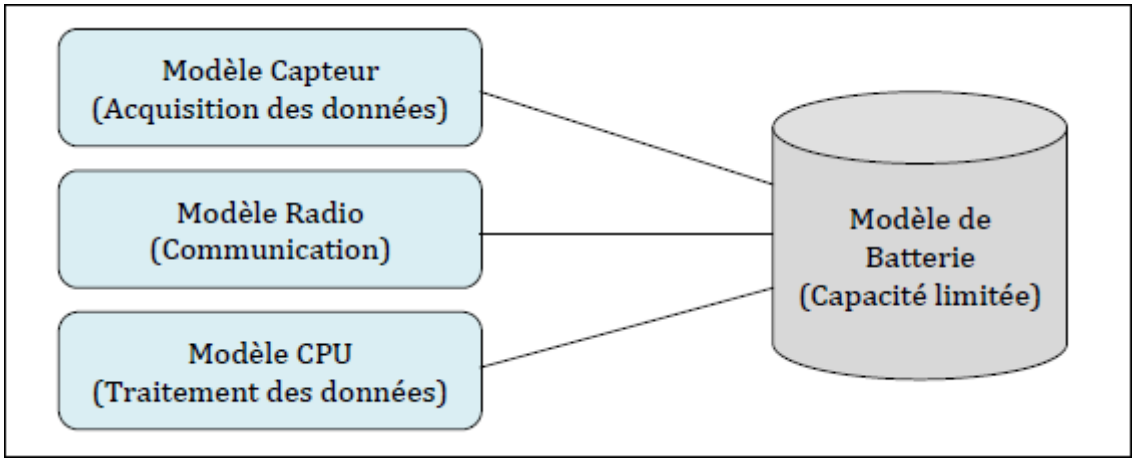


Figure 1.9 : modèle de consommation d'énergie

- **Acquisition :** L'énergie consommée pour effectuer l'acquisition n'est pas très importante. Néanmoins, elle varie en fonction du phénomène observé et du type des données collectées (scalaire ou multimédia).

- **Communication :** L'énergie totale pour la communication est la somme de l'énergie consommée par le circuit de transmission, l'amplificateur (dont le but est d'amplifier le signal selon la distance entre l'émetteur et le récepteur), et le circuit de réception.
- **Traitement des données** : L'énergie consommée pour les opérations de calcul est beaucoup plus faible que l'énergie de communication car les données traitées en général sont de types scalaires (température, humidité, vitesse du vent, etc).

Le graphique de la figure 1.10 montre l'énergie consommée pour chaque état et pour chaque action réalisée par un nœud capteur. On voit clairement que la tâche de transmission est la plus gourmande en énergie suivie de celle de la réception, alors que la tâche de capture et celle du traitement sont négligeables.

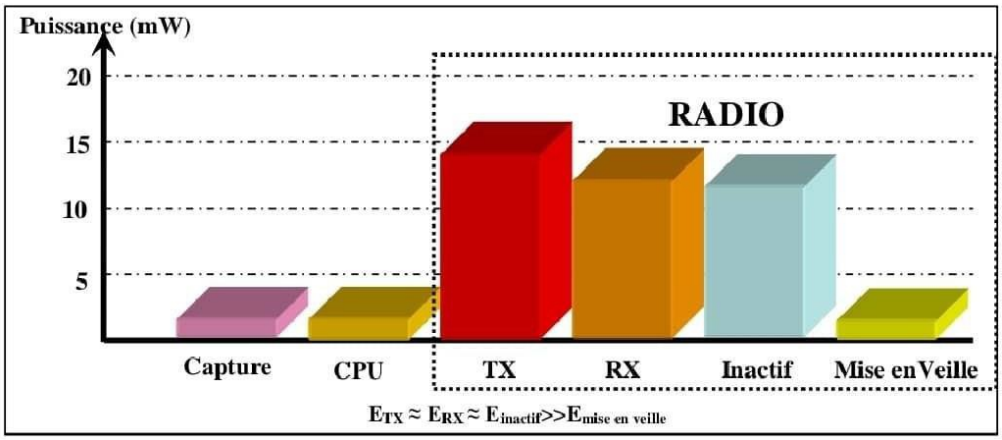


Figure 1.10 : consommation de l'énergie électrique par un nœud capteur

L'importance de l'efficacité énergétique

L'efficacité en consommation d'énergie représente une métrique de performance spécifique, qui influence directement sur la durée de vie du réseau. Malgré les progrès qui ont été faits, la durée de vie du réseau continue d'être un défi majeur et un facteur clé, exigeant plus de recherches sur l'efficacité énergétique des plates-formes et des protocoles de communication [11]. L'optimisation de la consommation d'énergie exigeant la conservation de l'énergie à tous les niveaux de la pile de protocole le plus possible. Pour cela, les concepteurs au moment du développement des protocoles, négliger les autres métriques de performances au profit du facteur de consommation d'énergie. Les protocoles efficaces en énergie visent à minimiser la consommation d'énergie pendant l'activité du réseau. Dans la littérature, il existe de nombreux mécanismes de conservation d'énergie et qui s'imposent comme les plus économes en énergie

telles les techniques de routage efficace en énergie et ordonnancement de l'interface radio, agrégation de données spatio-temporelle. Il existe bien évidemment beaucoup d'autres méthodes de conservation d'énergie. Par exemple, les mécanismes cross-layer et les paradigmes émanant de l'auto-organisation des systèmes [11].

Domaines d'applications des réseaux de capteurs

Au début de l'apparition des RCSFs, leurs domaines d'application étaient limités tout comme les types de capteurs qui existaient à cette époque. Aujourd'hui, une variété de capteurs est commercialisée. Des capteurs de température, des capteurs chimiques, séismiques, capteurs de pression, d'humidité et autre ont permis l'extension de la plage d'application utilisant les réseaux de capteurs pour atteindre tous les domaines.

Applications médicales

Dans le domaine de la médecine, les réseaux de capteurs peuvent être utilisés pour assurer une surveillance permanente des organes vitaux de l'être humain grâce à des micro-capteurs qui pourront être avalés ou implantés sous la peau (surveillance de la glycémie, détection de cancers, etc.). Ils peuvent aussi faciliter le diagnostic de quelques maladies en effectuant des mesures physiologiques telles que : la tension artérielle, battements du cœur, à l'aide des capteurs ayant chacun une tâche bien particulière. Les données physiologiques collectées par les capteurs peuvent être stockées pendant une longue durée pour le suivi d'un patient pour une ultérieure décision médicale. Donc on peut ainsi surveiller la progression d'une maladie. [12]

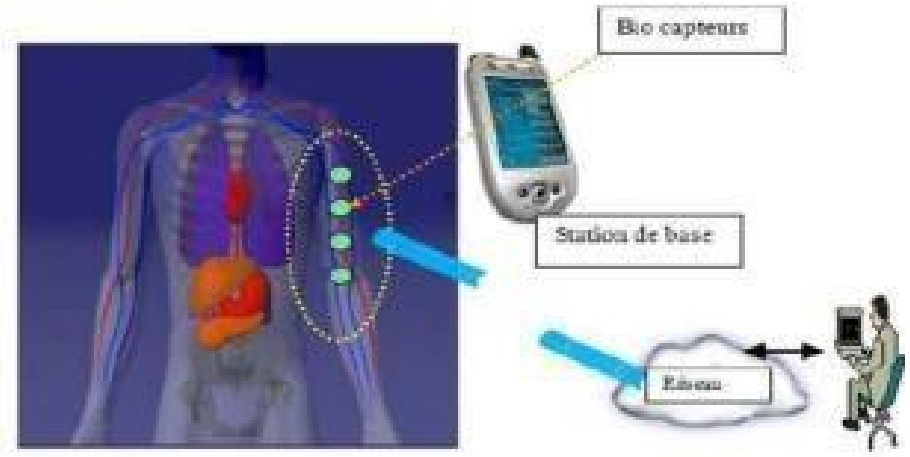


Figure 1.11 : application des RCSF en médecine.

Applications militaires

Le domaine militaire a été comme dans le cas de plusieurs technologies, un précurseur pour le développement d'applications des réseaux de capteurs. Le déploiement rapide, le cout réduit, l'auto-organisation et la tolérance aux pannes des réseaux de capteurs sont des caractéristiques qui rendent ce type de réseaux un outil appréciable dans un tel domaine. Un réseau de capteurs déployé sur un secteur stratégique ou difficile d'accès, permet par exemple d'y surveiller tous les mouvements (amis ou ennemis), ou d'analyser le terrain avant d'envoyer des troupes (détection d'agents chimiques, biologiques ou de radiations, par exemple). [12]

Figure 1.12 : Un service militaire utilisant les RCSF

Applications domotiques

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. [12]

Figure 1.13 : le contrôle d'une maison grâce à un téléphone intelligent ou une tablette

Applications environnementales

Les réseaux de capteurs peuvent être utilisés pour surveiller les changements environnementaux. Ils servent à déterminer les valeurs de certains paramètres à un endroit donné, par exemple : la température, la pression atmosphérique, etc. En dispersant des nœuds capteurs dans la nature, on peut détecter des événements tels que des feux de forêt, des tempêtes ou des inondations. Ceci permet une intervention beaucoup plus rapide et efficace des secours. Dans le domaine de l'agriculture, les capteurs peuvent être utilisés pour réagir convenablement aux changements climatiques, par exemple en déclenchant le processus d'arrosage lors de la détection de zones sèches dans un champ agricole. On peut aussi imaginer équiper des troupeaux de bétail de capteurs pour connaître en tout temps, leur position ce qui éviterait aux éleveurs d'avoir recours à des chiens de berger. [12]

Figure 1.14 : utilisation des capteurs météo dans l'agriculture avec RCSF

Défis des applications RCSF

Les RCSF 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 RCSF.

Consommation énergétique

Le capteur est limité en énergie en raison de sa taille. Dans la plupart des cas, il est impossible de remplacer la batterie. Cela signifie que la durée de vie du capteur dépend en grande partie de la durée de vie de la batterie. Dans un réseau de capteur (multi-sauts), chaque nœud collecte des données et envoie des valeurs. La défaillance de certains nœuds nécessite de modifier la topologie du réseau et de réacheminer les paquets de données. Toutes ces opérations son énergivores, c'est pourquoi les recherches actuelles se concentrent principalement sur les moyens de réduire cette consommation [13]

Le passage à l'échelle

Le nombre de nœuds déployés sur une zone de captage pour certaines applications peut atteindre des milliers. Dans ce cas, le réseau doit fonctionner avec des densités de capteurs très grandes. Ceci peut engendrer des problèmes de communication et de contrôle qui nécessite des protocoles capables de les gérer, ces protocoles doivent être capables de traiter un grand nombre d'évènements sans être saturés [13]

Qualité de service

Pour les réseaux de capteur sans fil, la qualité de service est la quantité des informations, qui est extraite des données collectées dans l'environnement où les capteurs ont été déployés. Le niveau de qualité de services peut être défini par un ensemble de normes et d'attributs, tels que le délai, la bande passante et le nombre de paquets perdus [13]

L'auto-configuration

Vu que les réseaux de capteurs sont déployés aléatoirement dans des environnements souvent hostiles, l'intervention de l'être humain n'est pas permise pour assurer leurs organisations. De ce fait, ces réseaux doivent pouvoir s'auto-configurer pour assurer un bon fonctionnement sans interruption.

Tolérance aux pannes

Ce facteur est défini par la capacité d'un réseau de capteur de maintenir son bon fonctionnement malgré la présence de quelques défaillances. Ces derniers peuvent survenir par manque d'énergie ou en raison de dommages physiques ou d'interférences environnementales. En effet, la panne de quelques nœuds entraine la perte des liens de communication et ainsi un changement significatif dans la topologie du réseau. Le degré de tolérance dépend du degré de criticité de l'application et des données échangées. Afin de maintenir le bon fonctionnement du réseau, les protocoles conçus doivent alors s'adapter à la nouvelle topologie du réseau en formant de nouvelles routes entre les nœuds [14]

Hétérogénéité

Dans de nombreuses études, tous les capteurs d'une application sont considérés comme homogènes (c'est-à-dire même capacité de calcul, de communication et d'énergie). Toutefois, selon l'application, certains capteurs peuvent avoir des rôles différents, générer une architecture hétérogène.

Routage

Les protocoles de routage doivent être adaptatifs à la flexibilité des RCSFs (auto-configurant). L'information devrait être persistante malgré les changements des nœuds du réseau. En outre, les algorithmes de routage devraient être intelligents pour choisir les sauts et les pas de distance miniums pour le transfert des données avec un faible coût d'énergie.

La sécurité

Pour les applications qui exigent un niveau de sécurité assez élevé telles que les applications militaires, des mécanismes d'authentification, de confidentialité, et d'intégrité doivent être mis en place au sein du réseau. Les algorithmes de cryptographie conçus pour les réseaux de capteurs doivent tenir compte des ressources limitées de ces derniers. De plus, l'absence d'une protection physique des nœuds capteurs ainsi que la nature des liens sans fil, rend le réseau vulnérable aux attaques malveillantes.

Le routage dans les réseaux de capteurs sans fil

D'une manière générale, le routage est un mécanisme de transmission d'information qui assure l'acheminement des données à la bonne destination via un réseau de connexion donné.

Le but de routage consiste à déterminer un chemin idéal des paquets à travers le réseau en prenant compte de certains critères de performances. Le problème consiste à trouver l'investissement de moindre coût en capacités nominales et de réserves qui assure le routage du trafic nominal et garantit sa vie en cas de n'importe quelle panne d'arc ou de nœud. Si on suppose que les coûts des liens sont identiques, le chemin indiqué dans la figure suivante est le chemin optimal reliant la station source et la station destination. Une bonne stratégie de routage utilise ce chemin dans le transfert des données entre les deux stations.

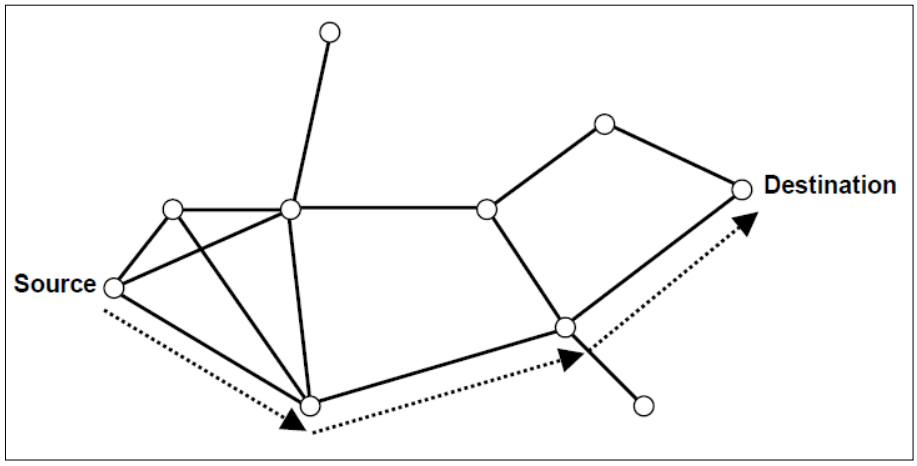


Figure 1.15 : Exemple d'un chemin utilisé dans le routage entre la source et la destination

En ce qui concerne les RCSFs, un grand nombre de capteurs sont mis en œuvre pour surveiller les phénomènes et rapporter les informations au centre de contrôle à distance. Pour atteindre cet objectif, les capteurs ont la capacité de communiquer et de coopérer entre eux, d'acheminer les informations collectées vers la station de base, tout en assurant sa fiabilité et d'utiliser le chemin le plus court entre le nœud qui détecte ce phénomène et la station de surveillance. Cette opération permet d'acheminer les informations entre le nœud détecteur et le nœud récepteur, et elle comprend la recherche du chemin le plus court. Dans cette optique, plusieurs protocoles de routage ont été proposés dans la littérature. Le problème qui se pose dans l'environnement réseau ad hoc est l'adaptation au mode de routage d'un grand nombre d'unités existant dans un environnement caractérisé par des capacités de calcul et de sauvegarde modérées et des changements topologiques rapides. Par conséquent, il semble important que toute conception de protocole de routage prenne compte des problèmes suivants. [15]

- Offrir un support pour effectuer des communications multipoints fiables.
- Assurer un routage optimal.

- La minimisation de la charge du réseau.
- Offrir une bonne qualité concernant le temps de latence.

Contraintes de routage dans les réseaux de capteurs sans fil

Le routage dans les réseaux de capteurs diffère de celui des réseaux Ad Hoc dans les points suivants :

- il n'est pas possible d'établir un système d'adressage global pour le grand nombre de nœuds.
- les applications des réseaux de capteurs exigent l'écoulement de données mesurées depuis des sources multiples vers la destination finale « Sink ».
- les différents capteurs peuvent générer les mêmes données à proximité d'un phénomène (problème de la redondance des données).
- les nœuds capteurs exigent ainsi une gestion soigneuse des ressources.

En raison de ces différences, de nouveaux protocoles de routage ont été proposés dans les réseaux de capteurs.

Les critères de performance des protocoles de routage en RCSF

La performance des réseaux de capteurs sans fil est fondée sur les facteurs suivants :

● **Evolutivité :** l'évolutivité est un facteur important dans les réseaux de capteurs sans fil. Une zone de réseau n'est pas toujours statique, elle change selon les besoins des utilisateurs. Tous les nœuds dans le domaine du réseau doivent être évolutifs ou être en mesure de s'adapter aux changements dans la structure du réseau en fonction de l'utilisateur.

● **L'énergie :** chaque nœud utilise peu d'énergie pour des activités telles que la détection, le traitement, le stockage et la transmission. Un nœud dans le réseau doit savoir combien d'énergie sera utilisée pour effectuer une nouvelle tâche à laquelle il est soumis. L'énergie consommée peut varier selon le type de fonctionnalité ou l'activité qu'il a à accomplir.

● **Le temps de traitement :** il se réfère au temps pris par le nœud dans le réseau pour assurer l'ensemble de l'opération commençant par la détection, le traitement des données ou le stockage de données, la transmission ou la réception sur le réseau.

● **Le schéma de transmission :** la transmission de données par les nœuds de capteurs vers la destination ou la station de base se fait par un schéma de routage à un seul saut ou à multi-saut.

● **Synchronisation :** dans les communications radio entre les nœuds d'un RCSF, les capteurs écoutent en permanence les transmissions et consomment de l'énergie s'ils ne sont pas

synchronisés les uns et les autres. Pour cela, un nœud doit avoir la même notion de temps pour se mettre en veille et se réveiller que ses voisins.

● **Contrôle de paquets :** un paquet envoyé avant la transmission entre deux nœuds est appelé le paquet de contrôle. Le paquet de contrôle contient le nombre de bits de données envoyés, l'adresse du nœud de destination et certaines informations qui contribuent à éviter les collisions pendant la transmission.

Classification des protocoles de routage

Les protocoles de routage pour les RCSFs ont été largement étudiés, et différentes études ont été publiées. Les méthodes employées peuvent être classifiées suivant plusieurs critères comme illustré sur la figure suivante :

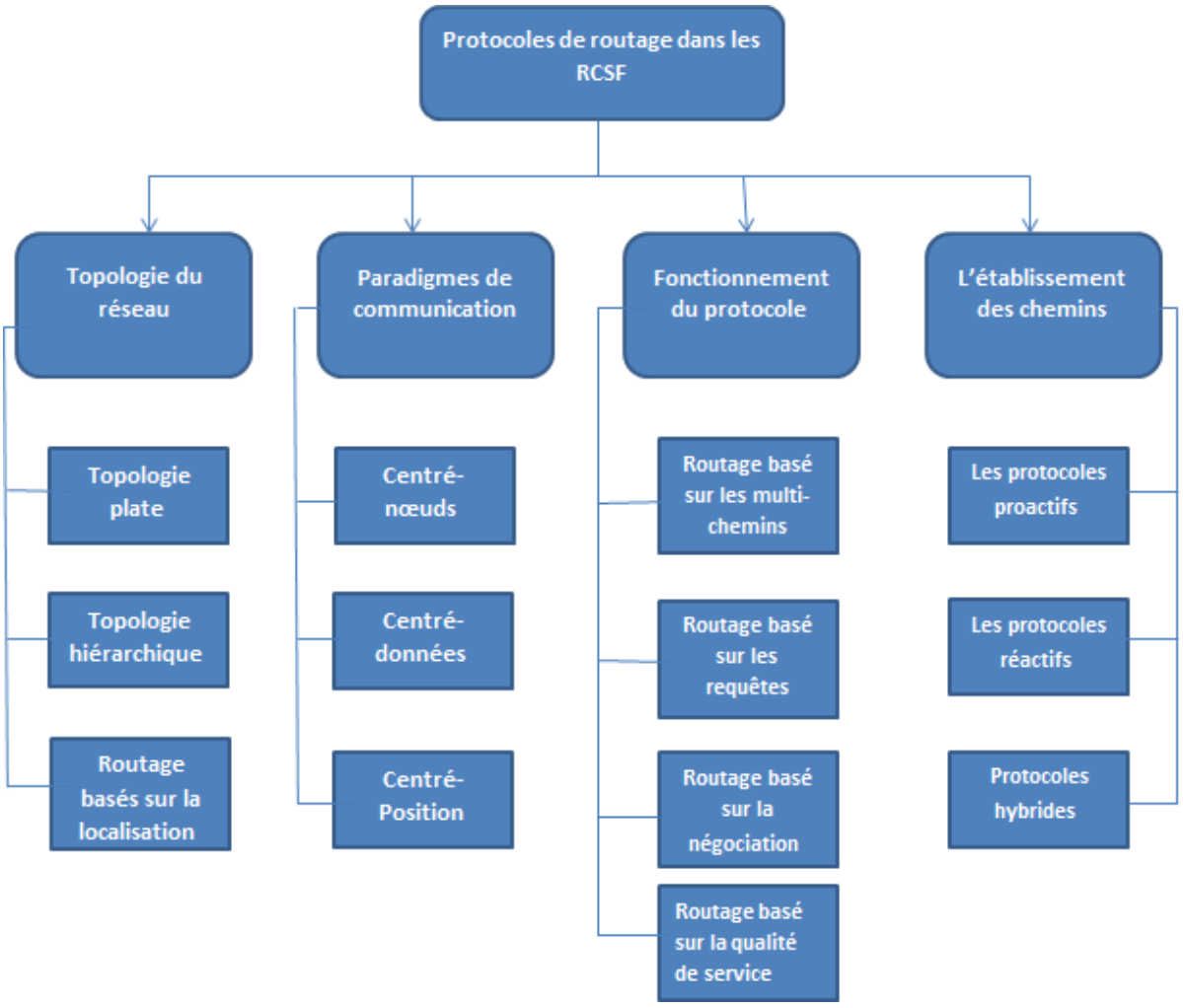


Figure 1.16 : Classification des protocoles de routage dans les RCSF

Classification selon la topologie du réseau

La topologie détermine l'organisation logique adaptée par les protocoles de routage afin d'exécuter les différentes opérations de découverte de routes et de transmission de données. Elle joue un rôle significatif dans le fonctionnement d'un protocole.

- **Topologie plate :**

Dans les protocoles de routage plats, tous les nœuds jouent le même rôle. Chaque nœud distribue des données à d'autres nœuds qui se trouvent dans leurs rayons de transmission. L'utilisation du lien de transmission diffère d'un protocole à un autre.

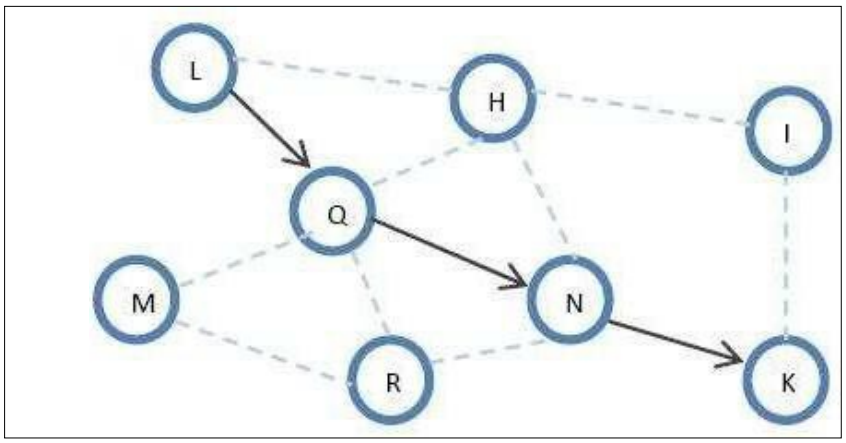


Figure 1.17 : Topologie plate

- **Topologie hiérarchique :**

Dans le routage hiérarchique, le réseau est partitionné en groupes appelés "clusters". Un cluster est constitué d'un chef (cluster-head) et de ses membres. Le cluster-head collecte et agrège les données et vérifie si les données collectées ne sont pas redondante avant de les envoyer au sink. Cela permet d'économiser l'énergie en minimisant le nombre de messages transmis à la destination. LEACH (Low Energy Adaptive Clustering Hierarchical) est l'un des premiers protocoles de routage pour les réseaux de capteurs.

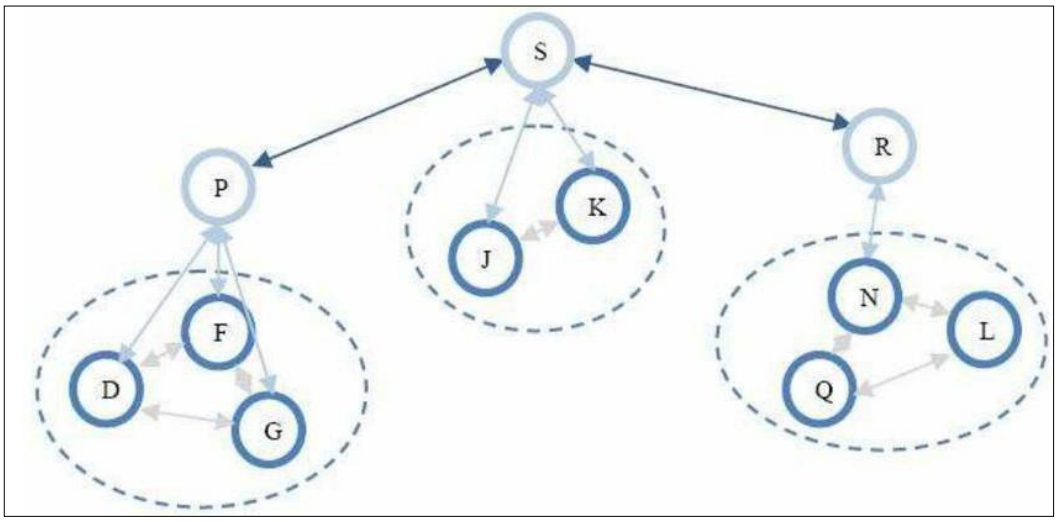


Figure 1.18 : Topologie hiérarchique

- **Topologie basée sur la localisation**

Dans le routage basé sur la localisation, le routage est effectué en utilisant l'emplacement des nœuds. Selon la force des signaux entrants, il est possible de calculer la distance du nœud voisin le plus proche. Ils permettent la transmission directionnelle de l'information en évitant l'inondation d'information dans l'ensemble du réseau. Par conséquent, le coût de contrôle de l'algorithme est réduit et le routage est optimisé. De plus, avec la topologie réseau basée sur des informations de localisation de nœuds, la gestion du réseau devient simple.

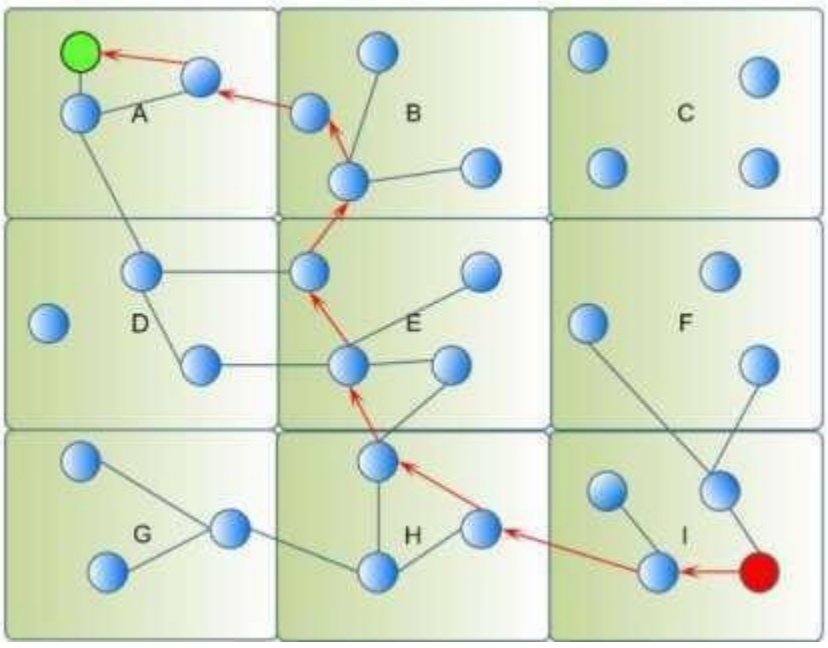


Figure 1.19 : Topologie basés sur la localisation [15]

Classification selon les paradigmes de communication

Le paradigme de communication détermine la manière dont les nœuds sont interrogés. Dans les RCSF, il existe trois paradigmes de communication : centré nœuds, centré données et basé sur la localisation. [16]

- **Centré-nœuds :**

Ce paradigme est celui employé dans les réseaux conventionnels, où il est nécessaire de connaître et d'identifier les nœuds communicants (comme l'adresse IP). Les réseaux ad hoc utilisent ce genre de paradigme, qui s'intègre bien avec l'utilisation de ce type d'environnement. Cependant, pour les réseaux de capteurs, un routage basé sur une Identification individuelle des nœuds ne reflète pas l'usage réel du réseau. Pour cela, un autre paradigme a été introduit : data centric. Néanmoins, le paradigme node centric n'est pas à écarter totalement, car certaines applications nécessitent une Interrogation individuelle des capteurs. [17]

- **Centré-données :**

Paradigme suppose qu'il est difficile d'avoir des identifiants comme les adresses MAC ou IP pour pouvoir communiquer entre les nœuds capteurs. Ainsi, le routage ne serait pas en fonction d'une adresse de destination, mais suivant les données disponibles au niveau des capteurs. Ces données seront propagées de proche en proche pour arriver au nœud puits. [18]

- **Centré-Position:**

Dans cette approche, les décisions de routage sont établies selon la position des nœuds. La distance entre les nœuds voisins peut être estimée sur la base de la puissance du signal arrivé. Un tel type de routage nécessite que les nœuds aient connaissance de leurs positions géographiques. Par conséquent, ce type de mécanismes nécessite un déploiement d'une solution de positionnement, dont le degré de précision requis dépend de l'application ciblée. L'utilisation du GPS reste trop coûteuse pour un RCSF. Néanmoins, d'autres méthodes de localisation et de positionnement des capteurs ont été développées comme par exemple la triangulation. [19]

Classification selon le mode de fonctionnement du protocole

Le mode de fonctionnement définit la manière avec laquelle les données sont propagées dans le réseau. Selon ce critère, les protocoles de routage peuvent être classifiés en quatre catégories : routage basé sur la Qualité de Service, routage basé sur les requêtes, routage multi-chemins, et routage basé sur la négociation. [20]

- **Routage basé sur les multi-chemins :**

Dans cette catégorie, les protocoles de routage utilisent des chemins multiples plutôt qu'un chemin simple afin d'augmenter la performance du réseau. La fiabilité d'un protocole peut être mesurée par sa capacité à trouver des chemins alternatifs entre la source et la destination en cas de défaillance du chemin primaire. Pour cette raison, certains protocoles construisent plusieurs chemins indépendants, c.-à-d. : ils ne partagent qu'un nombre réduit (voir nul) de nœuds. Malgré leur grande tolérance aux pannes, ces protocoles requièrent plus de ressources énergétiques et plus de messages de contrôle. [21]

- **Routage basé sur les requêtes :**

Dans ce type de routage, le puits génère des requêtes afin d'interroger les capteurs. Ces requêtes sont exprimées soit par un schéma valeur-attribut ou bien en utilisant un langage spécifique (par exemple SQL : Structured Query Language). Les nœuds qui détiennent les données requises doivent les envoyer au nœud demandeur à travers le chemin inverse de la requête. Les requêtes émises par le puits peuvent aussi être ciblées sur des régions spécifiques du réseau. [22]

- **Routage basé sur la négociation :**

En détectant le même phénomène, les nœuds capteurs inondent le réseau par les mêmes paquets de données. Ce problème de redondance peut être résolu en employant des protocoles de routage basés sur la négociation. En effet, avant de transmettre, les nœuds capteurs négocient entre eux leurs données en échangeant des paquets de signalisation spéciales, appelés métadonnées. Ces paquets permettent de vérifier si les nœuds voisins disposent déjà de la donnée à transmettre. Cette procédure garantit que seules les informations utiles seront transmises et élimine la redondance des données. [23]

- **Routage basé sur la qualité de service :**

Dans les protocoles de routage basés sur QoS, le réseau doit équilibrer entre la consommation d'énergie et la qualité de données. En particulier, le réseau doit satisfaire certaines métriques de QoS, par exemple, retard, énergie, largeur de bande passante, …etc. Les protocoles de cette approche sont très recommandés pour les applications de surveillance (centrales nucléaires, applications militaires, etc.). [24]

Classification selon le mode d'établissement des chemins

Suivant la manière de création et de maintien des chemins pendant le routage, nous distinguons trois catégories de protocoles de routage : les protocoles proactifs, les protocoles réactifs et les protocoles hybrides [25].

- **Les protocoles proactifs :**

Ces protocoles utilisent l'échange régulier de messages de contrôle pour maintenir au niveau de chaque nœud des tables de routage vers toute destination atteignable depuis celui-ci. Ces tables sont maintenues mêmes quand les routes ne sont pas utilisées. Cette approche permet de disposer d'une route vers chaque destination immédiatement au moment où un paquet doit être envoyé. Les protocoles proactifs sont adaptés aux applications qui nécessitent un prélèvement périodique des données. Par conséquent, les capteurs peuvent se mettre en veille pendant les périodes d'inactivité, et n'enclencher leur dispositif de capture qu'aux instants lorsqu'ils basculent en mode actif.

- **Les protocoles réactifs :**

Ces protocoles créent les routes à la demande. Lorsqu'un nœud a besoin d'une route, une procédure de découverte globale est déclenchée. Cette procédure s'achève par la découverte de la route ou lorsque toutes les permutations de routes possibles ont été examinées. La route trouvée est maintenue par une procédure de maintenance de routes jusqu'a ce que la destination soit inaccessible à partir du nœud source ou que le nœud source n'aura plus besoin de cette route.

- **Protocoles hybrides :**

Ces protocoles combinent les deux idées des protocoles proactifs et réactifs. Ils utilisent un protocole proactif pour apprendre le proche voisinage (par exemple le voisinage à deux ou à trois sauts), ainsi, ils disposent de routes immédiatement dans le voisinage. Au-delà de la zone du voisinage, le protocole hybride fait appel à un protocole réactif pour chercher des routes

Les protocoles de routage hiérarchiques

Le routage hiérarchique est considéré comme étant l'approche la plus favorable en terme d'efficacité énergétique. Il se base sur le concept (nœud standard - nœud maître) où les nœuds standard acheminent leurs messages à leur maître, lequel les achemine ensuite dans le réseau tout entier via d'autres nœuds maîtres jusqu'à la station de base (sink). Le point fort de ce type de protocoles est l'agrégation et la fusion des données afin de diminuer le nombre de messages transmis au sink, ce qui implique une meilleure économie d'énergie [26, 27, 28]. En fait, deux grandes approches sont dérivées de ce type de protocoles à savoir : chaine-based approach (approche chaînée) comme PEGASIS et cluster-based approach (approche à grappe) comme LEACH [26]

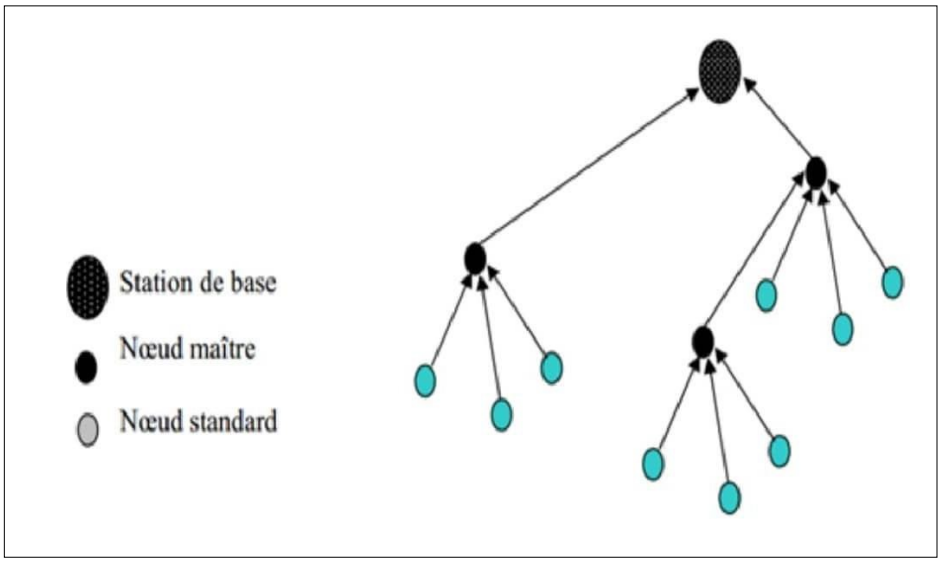


Figure 1.20 : le routage hiérarchique

Le protocole de routage «LEACH »

LEACH (Low Energy Adaptive Clustering Hierarchy) est un protocole de routage hiérarchique introduit par Hienzelman et all. Ce protocole se base sur la clustérisassions dynamique. Au départ, LEACH sélectionne au hasard quelques nœuds capteurs au tant que chefs de cluster et tourne ce rôle d'une manière uniforme pour répartir la charge entre les capteurs et prolonger la durée de vie du réseau. Dans [28], le pourcentage des nœuds capteurs qui doivent agir au tant que chefs de groupe est égale à 5%, ces clusters agrègent les données transmises par ses membres et envoient ces données à la station de base, Pour cette raison, les clusters head ont besoin plus d'énergie que les autres nœuds. L'opération de LEACH est divisée en tours, où chaque tour commence avec une phase d'installation suivies d'une phase de communication :

- **La phase d'installation :**

Chaque capteur choisit lui-même d'être un chef de groupe avec une probabilité P qui est choisie en fonction du nombre de Clusters k et du nombre de nœud capteurs N dans le réseau. De même pour les prochaines chois des itérations suivantes, ce protocole vérifie si le nœud n'été pas une tête de groupe dans les plus récents tours. Puis chaque capteur choisit un nombre aléatoire, r, entre 0 et 1. Si ce nombre aléatoire est inférieur à une valeur de seuil T(n), le nœud devient un CH pour le cycle actuel. Le seuil est défini comme suit :

$$(n) = \begin{cases} \frac{P}{1-P(r \bmod \frac{1}{P})} & Si \quad (n \in G) \\ 0 & sinon \end{cases}$$

Où

P est le pourcentage désiré des CHs, r est l'itération actuelle et G représente l'ensemble des nœuds qui n'ont pas été cluster-heads dans les dernières $(1/P)$ itérations.

Une fois que les CHs sont choisies, ils envoient un message d'annonce au reste des nœuds dans le réseau qu'ils sont les nouveaux chefs de cluster. Après avoir reçu cette annonce(ADV) contenant l'ID du nœud et un en-tête qui distingue ce message d'annonce. Chaque nœuds non tête décident du groupe auquel ils veulent appartenir. Cette décision est basé sur l'intensité du signal d'annonce, puis il informe le CH qu'il appartient à son groupe, et cela se fait par un message Join-REQ contenant l'ID du nœud et l'ID du CH. A la réception de tous les messages à partir des nœuds qui serait certainement inclus dans le cluster, le CH crée une planification TDMA afin d'attribuer pour chaque nœud une tranche de temps où il peut transmettre. Ce calendrier sera diffusé à tous les nœuds du cluster.

- **La phase de communication** :

Selon le calendrier designer par le CH, les nœuds capteurs peuvent commencer la détection et la transmission de données à leur chef, et ce dernier agrège ces données avant de les envoyer à la station de base.

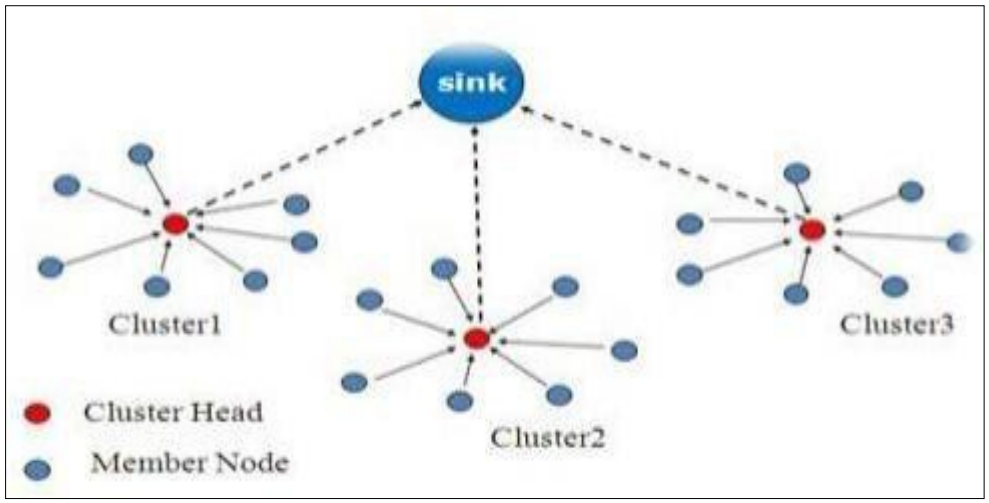


Figure 1.21 : Algorithme de routage LEACH [31]

Le protocole de routage «LPWS»

Le protocole LPWS (A New Location Based Protocol for Wireless Sensor Clustering) est basé sur la subdivision de réseau en plusieurs cellules sous forme de grille, et le

positionnement des nœuds capteurs dans chaque cellule. Chaque grille possède un ensemble de nœuds qui communiquent entre eux en envoyant des messages d'identification. Chaque nœud de la cellule est doté à reconnaître son chef (CH), cette opération se fait avec la comparaison des distances entre sa position et la position du centre de la cellule, les résultats sont sauvegardées dans un tableau pour y accéder dans les prochains rounds sans répéter l'opération et gaspiller l'énergie. Une fois les nœuds sont organisés et savent leur CH, les étapes suivantes s'attribuent tel que le protocole LEACH (les nœuds captent la température et l'envoie au CH, ces données sont ensuite agrégées par le CH qui les fusionne et les compresse, puis le résultat final est envoyé à la station de base). [29]

LPWS fonctionne en deux phases. Dans la première phase, l'élection des CHs et la formation des clusters sont effectuées, tant dis que dans la deuxième phase, le processus de transmission de données est lancé. Dans ce qui suit, nous présentons le déroulement du protocole proposé.

- **La phase d'installation**

Etape 1 : Planification

Dans cette étape, le réseau entier est représenté par une grille de taille Z/k dans laquelle chaque cellule représente une région bien précise de ce réseau. Chacune des cellules de la grille se verra affecter un ensemble des nœuds capteurs formant un cluster.

Une fois les nœuds déployés, ils effectuent la planification du réseau afin de déterminer l'identification de la cellule (ID cellule) à laquelle il appartient et les coordonnées (x, y) du centre de gravité (COG: Center Of Gravity) de leur cellule. En effet, ce processus se déroule durant le round 0. [1]

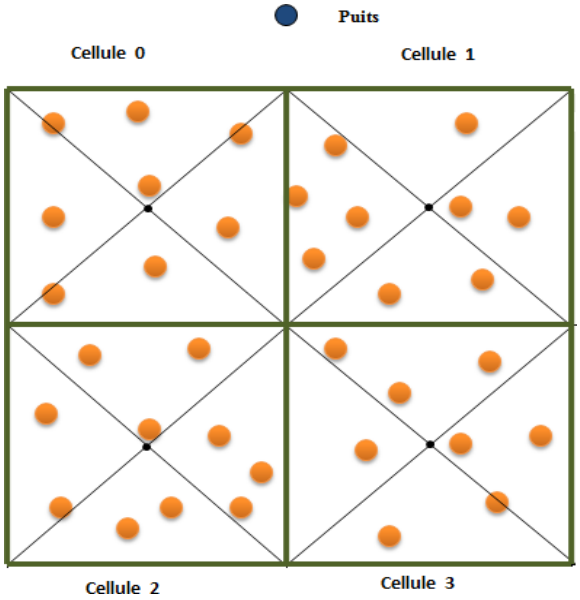


Figure 1.22 : Etape de Planification [1]

Etape 2: Initialisation

La phase d'initialisation commence par l'envoi d'un message d'initialisation de la part de la station de base à tous les nœuds capteurs du réseau. En fait, cela se déroule aussi durant le round 0. [21]

Etape 3: Annonce

A la fin de la phase d'initialisation et durant le round 0, chaque nœud qui a reçu le message d'initialisation diffuse un message d'annonce aux autres nœuds. Ce message contient son identifiant, sa position (en coordonnées (x, y)) et l'identification de sa cellule. [1]

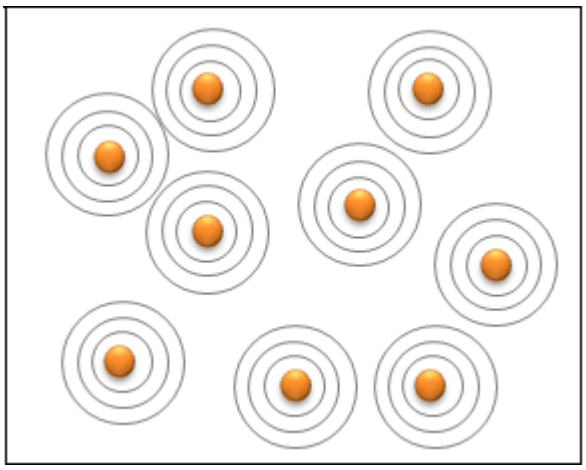


Figure 1.23 : Phase d'Annonce [1]

Etape 4: Election

Les nœuds qui ont reçu ces messages, doivent vérifier si l'ID de la cellule reçu dans le message correspond à l'ID de cellule enregistrée (sa cellule). Ainsi, chaque nœud capteur identifie l'ensemble des nœuds capteurs qui se trouvent dans la même cellule. Il calcule ensuite la distance qui sépare sa position du centre de la cellule, ainsi que la distance qui sépare chaque nœud et le centre de cette même cellule. [29]

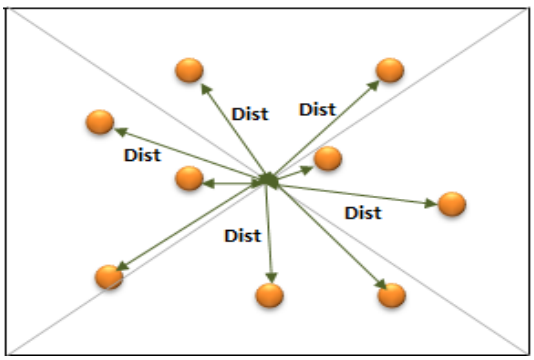


Figure 1.24 : Etape d'Élection (calcul des distances) [1]

Après l'accomplissement de cette tâche, tous les nœuds non-CHs arrivent à identifier leurs CHs. En effet, le CH va être choisi en se basant sur le tri des distances calculées.

Chaque nœud CH ou non-CH dans la même cellule construit un tableau contenant l'identificateur de nœud membre, et un index, qui est construit selon l'ordre des distances calculées. [1]

D'ailleurs, un slot est attribué à chaque nœud membre pour communiquer avec le nœud CH, ce slot est égal à index+1. [1]

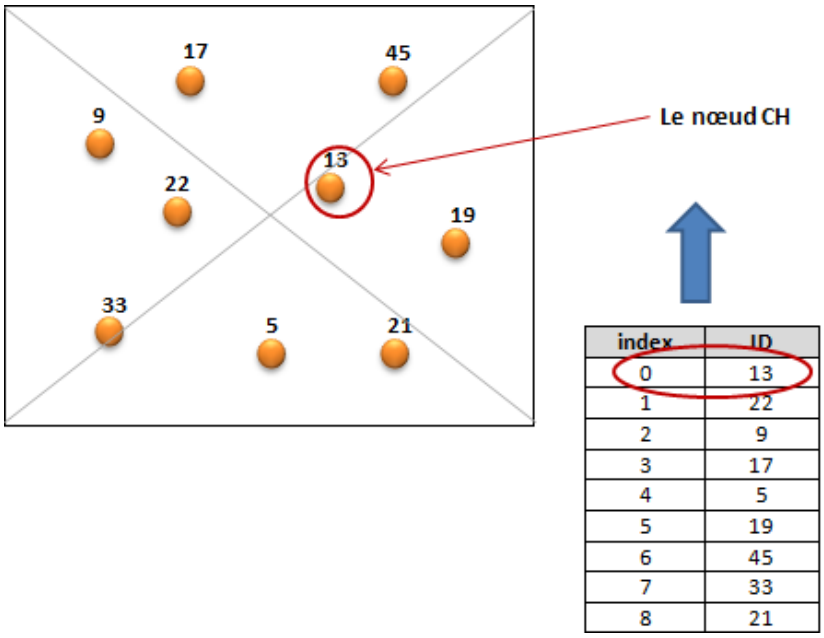


Figure 1.25 : Etape d'Élection (le choix de CH) [1]

- **La phase transmission**

Dans cette phase, le transfert de données vers le puits aura lieu. En utilisant l'ordonnanceur TDMA, les nœuds membres émettent leurs données captées pendant leurs propres slots. Ces données sont ensuite agrégées par les CH selon la fonction d'agrégation (moyenne, somme, suppression des redondances…etc.) et envoient le résultat final au puits. [1]

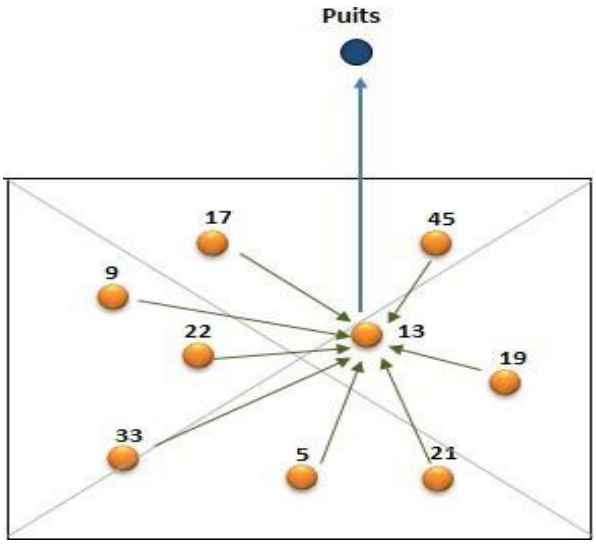


Figure 1.26 : La phase transmission [1]

A la fin de la phase de transmission, le nœud puits reçoit les données agrégées (envoyées par d'autres nœuds) et initie un nouveau round.

Quand le round est différent de 0 ($r \neq 0$), ce processus est modifié, cette fois on ignora la phase d'initialisation. Ceci est dû au fait que l'élection des nœuds CHs va être automatique. Les CH élus sont les nœuds correspondant au ID approprié au index du tableau (tel que index=r) et comme les tableaux des nœuds de chaque cluster sont les mêmes, les autres nœuds connaissent directement son CH pour ce round.

Ainsi, après la réception de message d'initialisation de nouveau round r, les nœuds passent directement à la phase transmission. [1]

Conclusion

Dans ce premier chapitre, nous avons présenté les réseaux de capteurs sans fil, leurs architectures, leurs contraintes ainsi que leurs domaines d'applications. Nous avons vue qu'ils présentent un intérêt considérable et réalisent une nouvelle étape dans l'évolution des technologies de l'information et de la communication. La conception de réseaux de capteurs autonomes, reliés par des liens sans fil, est un domaine de recherche très actif qui suscite un intérêt croissant vu la diversité de ces applications : santé, environnement, industrie et même dans le domaine sportif.

Le routage de données est considéré comme le domaine le plus exploré parmi les domaines de recherche sur les réseaux de capteur. Il représente aussi 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. Les protocoles de routage pour les RCSFs sont nombreux avec un unique objectif : Assurer la délivrance des paquets collectés par les nœuds capteurs tout en parvenant à étendre la durée de vie du réseau.

Dans ce chapitre, nous avons présenté les différentes classifications des protocoles de routage dans les réseaux de capteurs sans fil. Parmi les protocoles existants on s'intéresse particulièrement à la classe des protocoles hiérarchiques. Ainsi, nous avons effectué une étude exhaustive du protocole LEACH et LPWS. Bien que ces deux protocoles puissent augmenter la durée de vie du réseau en manipulant ses ressources tout en respectant plusieurs contraintes telle que la consommation d'énergie, ils exposent certaines limitations. En effet, aucun mécanisme de sécurité n'est intégré dans ces protocoles. Ainsi, ils sont très vulnérables même aux simples attaques. Donc, un attaquant peut facilement monopoliser le réseau et induit à son disfonctionnement. Par conséquent, Dans le chapitre suivant, nous allons aborder le concept de sécurité dans les réseaux de capteurs.

Chapitre 2

La sécurité dans les RCSFs : Taxonomie des menaces et des solutions

Introduction

Les RCSFs connaissent actuellement une grande extension et une large utilisation dans différents types d'applications, les nœuds capteurs de ces réseaux sont dispersés dans des environnements qui peuvent être propices à des hostilités d'un adversaire, le bon fonctionnement du réseau peut être compromis. C'est la raison pour laquelle assurer la sécurité dans ce type de réseaux devient un enjeu très important et ce notamment en ce qui concerne le bon acheminement des données. Assurer la sécurité des échanges au sein des RCSFs est une tâche difficile, les capteurs qui les constituent comme mentionné précédemment, sont limités en termes de puissance, d'énergie, de capacité de communication et de calcul. Par conséquent, la mise en place des mécanismes de sécurité traditionnels sont inadaptables à ce type de réseau.

Dans ce chapitre, nous allons donner un aperçu sur les problèmes de sécurité dans les RCSFs qui différent des autres réseaux. Par la suite, nous étudierons les services de base de la sécurité à respecter pour éviter ces menaces. Puis, on va décrire les différents mécanismes de sécurité destinés aux RCSFs.

Les vulnérabilités de la sécurité dans les RCSF

La vulnérabilité physique

La vulnérabilité physique est le fait qu'un capteur est fréquemment installé dans un lieu peu sûr, c.-à-d. dont l'accès n'est nullement restreint. Nous pouvons citer les lieux publics, les environnements naturels (forêts, régions montagneuses) ainsi que les bâtiments, maisons intelligentes et musées ("smart environnement"). En effet, elle expose les liens de communication à des attaques. Ainsi que, les capteurs sont vulnérables à la capture physique et au vandalisme.

La vulnérabilité technologique

Est liée à plusieurs contraintes qui retour à la technologie des capteurs.

- **Limitation en énergie:**

L'énergie est un facteur critique à considérer en concevant des mécanismes de sécurité], L'énergie des nœuds de capteur est limitée, et généralement irremplaçable. Alors, cette limitation impose la conception des mécanismes de sécurité à faible consommation énergétique.

- **Capacité de calcul limitée:**

Le capteur est doté d'un processeur d'une capacité de calcul très réduite ce qui empêche l'utilisation de mécanismes de protection cryptographiques qui exigeant plus de puissance de calcul.

- **Mémoire limitée:**

Dans les réseaux de capteurs sans fils, la limitation des ressources restreint les mécanismes de sécurité. En effet, les nœuds n'ont pas la capacité de mémoriser des clés de taille importante ou d'exécuter des protocoles cryptographique complexes

- **Transmission/réception:**

D'un point de vu énergétique, la transmission est l'opération la plus coûteuse dans les réseaux de capteurs sans fils. Il a été démontré que un bit transmis est équivalent à environ un millier d'opérations CPU [32]. Par conséquent, Dans la conception de mécanisme de sécurité, le nombre de messages échangé entre les nœuds capteurs doivent être pris en considération.

Les Exigences de sécurité

Sécuriser un système informatique implique directement l'atteinte des objectifs suivants :

Authentification

En raison de la nature sans fil des médias et de la nature non surveillée des réseaux de capteurs, l'authenticité de la communication est extrêmement indispensable dans ces conditions. Un service d'authentification fiable doit garantir l'authentification à deux niveaux [29] [30] :

- Authentification d'entité : avant de permettre à n'importe quelles entités ou participant d'accéder aux services ou à des informations dans le réseau, une vérification d'entité doit être effectuée pour assurer que le demandeur soit une entité légitime et autorisée à récupérer ce service ou information. L'authentification peut être effectuée entre deux nœuds communiquant ou un nœud (par exemple, une tête de grappe) et plusieurs autres nœuds autour de ce nœud (c'est-à-dire une authentification de diffusion).
- Authentification de l'origine des données: Les capteurs doivent s'assurer que les données reçues proviennent d'une source identifiée. Un adversaire n'est pas limité simplement à modifier le paquet de données. Il peut aussi changer complètement le trafic en injectant de faux paquets supplémentaires. Ainsi, le récepteur doit s'assurer que les données utilisées dans n'importe quel processus décisionnel proviennent d'une source correcte.

Confidentialité

La confidentialité des données est une des pierres angulaires de la sécurité du réseau. La confidentialité est le fait de s'assurer que le contenu échangé (par exemple, des données collectées, des rapports, des commandes) entre les nœuds capteurs n'est accessible et compréhensible qu'à ceux dont l'accès est autorisé. Donc, même si un adversaire possède le privilège d'accéder au contenu, il ne devrait pas pouvoir décoder les messages échangés dans le réseau [29] . Dans les réseaux de capteurs, la confidentialité devrait répondre aux exigences suivantes [31] [32] :

- Un nœud capteur ne doit pas divulguer ses données aux nœuds voisins. En particulier dans une application militaire, les données stockées dans les nœuds capteurs peuvent être très sensibles. Dans de nombreuses applications, les nœuds communiquent des données hautement sensibles, par exemple la distribution de clés, il est donc extrêmement important de construire un canal sécurisé dans un réseau de capteurs sans fil.
- Les informations publiques sur les capteurs, telles que les identités des capteurs et les clés publiques, doivent également être cryptées dans une certaine mesure pour les protéger contre les attaques d'analyse de trafic.

Intégrité

L'intégrité des données dans les réseaux de capteurs est nécessaire pour assurer la fiabilité des données. Un service d'intégrité de données doit fournir des mécanismes aux nœuds communicants pour que ces derniers puissent détecter qu'un paquet n'a pas été falsifié, altéré ou modifié pendant la transmission. Même avec la mise en œuvre de la confidentialité, cela ne signifie pas que les données sont sécurisées. Un nœud malveillant peut ajouter quelques fragments ou manœuvrer les données dans un paquet. Ce nouveau paquet peut alors être envoyé au récepteur original. La perte ou les dommages de données peut même se produire sans présence d'un nœud malveillant mais aux conditions instables dues au canal de communication sans fil [29] [30] [31].

Fraîcheur de données

Même si la confidentialité et l'intégrité des données sont assurées, un adversaire peut facilement envoyer des paquets périmés dans le réseau. A la réception de ce genre de paquets, ces derniers peuvent être authentifiés et décryptés par un nœud sans détecter leur nature, ce qui implique des perturbations au niveau de plusieurs tâches dans les RCSF, parmi lesquelles on note : le résultat d'une fonction d'agrégation, quand il y a des stratégies de partage de clés

utilisées dans la conception ou lorsque des tâches administratives et décisives se basent sur des anciens paquets. Pour résoudre ce problème, un compteur relatif au temps différent peut-être ajouté dans le paquet pour assurer la fraîcheur des données [33]. Ainsi, la fraicheur des données consiste à s'assurer que les paquets soient récents et qu'aucun vieux paquet n'a été rejoué dans le réseau.

Disponibilité

La disponibilité est la capacité permanente d'avoir accès à tous les services ou les fonctionnalités fournis par le réseau pour chaque membre du réseau. En effet, la disponibilité peut être menacée à cause des deux raisons suivantes :

- La présence d'attaques internes ou externes telles qu'une attaque par déni de service (DoS) [30].
- Les approches utilisées pour satisfaire les autres objectifs de sécurité telles que la confidentialité ou l'intégrité des données.

Classification des attaques dans les RCSF

Selon des critères bien spécifiques, comme la puissance de l'attaquant, l'appartenance ou non de ce dernier au réseau. Les attaques contre les réseaux de capteurs peuvent être classées selon les catégories suivantes :

Attaques passives/actives

Les attaques passives ne sont intéressées que par la collecte des informations sensibles sans aucune modification ou influence sur la communication. Ces informations collectées comme la détection des nœuds importants dans le réseau (Cluster-Head) peuvent ensuite aider l'attaquant à de réaliser des attaques malveillantes. Les attaques actives ont comme objet, la perturbation de la fonction du réseau et de la dégradation de ses performances. L'attaquant tente d'exploiter les failles de sécurité du réseau pour lancer des attaques diverses dans le but de modifier les données.

Attaques internes/externes

Un attaque externe se produit de l'extérieur du réseau de capteurs c.-à-d. elles se produisent par des nœuds qui ne sont pas déployées à l'intérieur du réseau et que ne sont pas autorisées à participer dans le réseau. Alors que les attaques internes se produisent par des nœuds internes malveillants.

Attaques orientées selon les couches protocolaires

Pour cette méthode de classification, on peut classer les attaques selon la couche ciblée.

Les attaques ciblant la couche physique

La couche physique correspond au médium physique utilisé afin de transmettre des données entre deux nœuds. Une attaque qui cible cette couche vise généralement à créer des interférences pour occuper les canaux et empêcher les nœuds capteurs de communiquer normalement. Un attaquant peut transmettre en continu des signaux radio sur un canal sans fil. Il peut aussi envoyer des signaux à haute énergie afin de bloquer efficacement le support sans fil et d'empêcher les capteurs de communiquer. [9]

Les attaques ciblant la couche de liaison de données

Les attaquants peuvent exploiter les comportements de protocole prédéfinis au niveau de la couche liaison pour lancer des attaques contre cette couche. Donc, ils peuvent provoquer des collisions afin de causer une interférence, provoquer un épuisement des ressources énergétiques des capteurs par des retransmissions répétées des paquets, ou intercepter des messages afin d'acquérir des informations. [9]

Les attaques ciblant la couche réseau

La couche réseau des RCSFs est vulnérable aux différents types d'attaques, telles que les attaques DoS [34] qui visent à perturber complètement les informations de routage, et donc l'ensemble du fonctionnement du réseau. Une attaque de Sinkhole tente d'achemine presque tout le trafic vers le capteur malveillant. L'attaquant va convaincre ses voisins comme étant la station de base ou du cluster-head. Par conséquent tous les paquets reçus seront modifiés et envoyer à la station de base. Les informations de routage falsifiées, altérées ou rejoué sont les attaques les plus directes lancées contre un protocole de routage afin de perturber le trafic sur le réseau.

Les attaques ciblant la couche transport

Des attaques peuvent profiter les spécifications de la couche transport : par exemple, un attaquant peut émettre un nombre considérables d'informations, telle qu'une demande d'une nouvelle connexion. Ainsi les ressources d'un capteur, qui atteignent rapidement la limite maximale (saturation). L'attaque de désynchronisation est un autre exemple d'attaque dans cette couche [34].

Les attaques ciblant la couche application Erreur ! Signet non défini.

La couche application des RCSFs est vulnérable aux différents types d'attaques, telles que Overwhelm, la répudiation, et la corruption de données. En cas d'attaque Overwhelm, un intrus amène le réseau à acheminer de gros volumes de trafic vers la station de base. Ce type d'attaque consomme de la bande passante de réseau et épuiser l'énergie des nœuds capteurs.

Les attaques visant les réseaux de capteurs

La sécurité est un enjeu majeur dans les réseaux de capteurs sans fil qui sont vulnérables à des nombreuses attaques et menaces de sécurité. La nécessité de connaitre l'attaque pour comprendre comment l'attaquant agit et donc savoir comment le protéger. Nous décrivons dans cette partie les principales attaques contre les RCSFs.

Jamming

C'est une attaque de type Déni de Service (DoS) dont le but est de perturber la communication. L'attaquant bloque la réception du canal radio d'un nœud en transmettant sur sa bande de fréquence afin de provoquer des interférences radio. Il existe différentes stratégies pour l'attaque jamming :

- En émettant un signal radio sans interruption (constant jamming). Cette stratégie nécessitant beaucoup d'énergie.
- En émettant régulièrement à intervalle fixe ou d'une façon aléatoire sur un canal afin de préserver son énergie
- En émettant un signal si le canal est actif (réactive jamming).

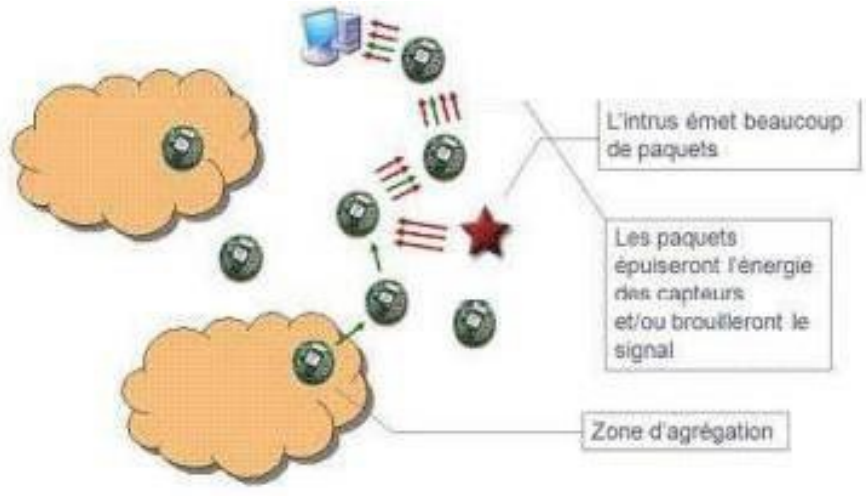


Figure 2.1 : Attaque de jamming

Selective Forwarding

Dans cette attaque, l'intrus empêche la transmission de certains paquets. Ces derniers seront par la suite supprimés par ce nœud malveillant. Il est à noter que le choix des paquets est basé sur certains critères tel que : le contenu des paquets, adresse source de l'émetteur, ou d'une façon aléatoire.

Sinkhole

Un nœud malveillant va convaincre ses voisins que c'est le nœud le plus proche de la station de base en utilisant une puissance de transmission élevée afin d'attirer vers lui tout le trafic permettant de contrôler la plus part des données circulant dans le réseau. Par conséquent tous les paquets reçus seront modifiés et transmis à la station de base dans le but d'empêcher cette dernière d'obtenir des données complètes et correctes.

Attaque physique (Tampering)

Elle consiste à la capture et à l'accès physique au nœud afin d'extraire toutes les informations importantes comme les clés utilisées pour le chiffrement.

L'attaque Sybil

Dans cette attaque, un nœud malicieux peut prendre l'identité d'autres nœuds légitimes dans le réseau (par le vol ou bien par la fabrication), cette attaque peut dégrader l'efficacité de plusieurs fonctionnalités comme la distribution de données, l'agrégation des données, ou remplir la liste de voisinage des nœuds voisins avec des nœuds inexistants. Cette attaque visant à changer l'intégrité des données et les mécanismes de routage.

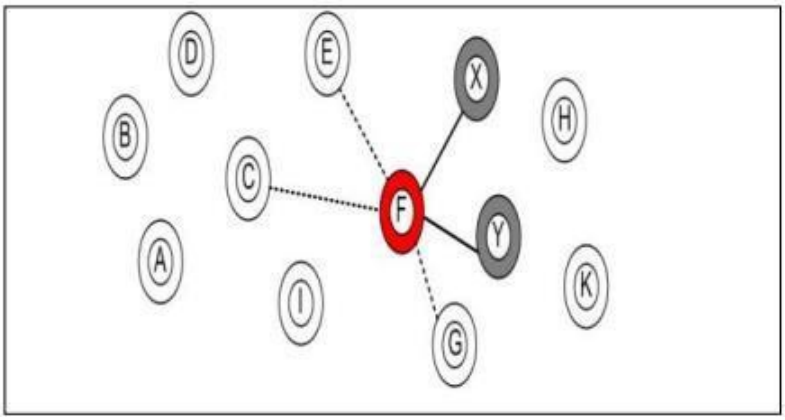
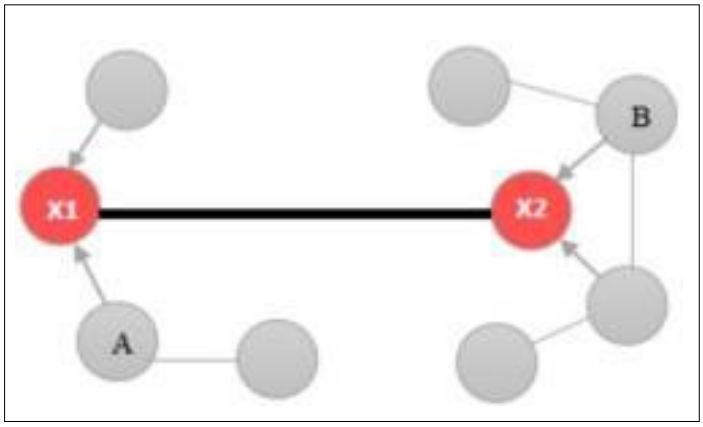


Figure 2.2 : L'attaque sybil

Wormhole

Dans cette attaque, un nœud malicieux enregistre les paquets et les envoie via un lien ou tunnel de faible latence vers un autre nœud malicieux dans le réseau. A l'aide d'un canal filaire ou sans fil à longue portée.



Figue2.3 : L'attaque Wormhole

L'attaque Hello flood

Le nœud malicieux diffuse un message Hello dans le réseau en utilisant une grande énergie d'émission. Par conséquent, tous les nœuds qui réceptionnent le message essayeront de transmettre leurs paquets à travers le nœud malveillant. Le but de cette attaque consiste à consommer l'énergie des nœuds et empêcher leurs messages d'être échangés.

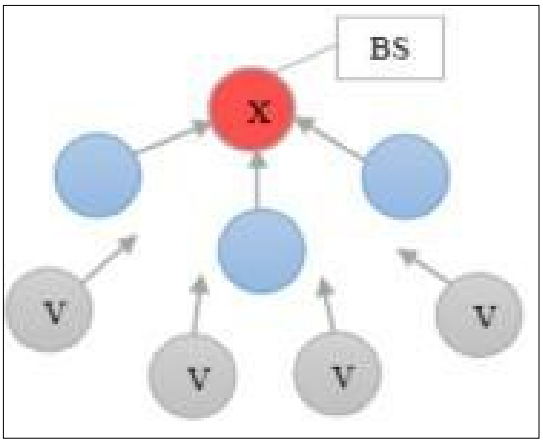


Figure2.4 : L'attaque Hello flood

Attaque par rejeu(replay)

Est une forme d'attaque réseau dans laquelle l'intrus peut injecter des précédents échanges interceptés par celui-ci. Cette attaque vise la fraicheur de données.

Réplication de nœuds

Elle consiste à capturer un nœud, construire des copies légitimes de ce dernier et les ajouter partout au réseau créant ainsi des identités multiples utilisant la même cryptographie que le nœud légitime original.

Mécanismes de sécurité

Plusieurs mécanismes, sont mis en place afin de répondre aux problèmes de sécurités dans les RCSFs. En effet, dans le cadre du développement d'un mécanisme de sécurité, il faut toujours assurer un compromis entre la sécurité garantie et le surcoût imposé par le mécanisme appliqué. Nous citons dans ce qui suit quelques mécanismes de sécurité proposés contre les attaques ou les comportements malicieux.

Primitives cryptographiques utilisées dans les RCSF

Plusieurs mécanismes basés généralement sur l'utilisation des primitives cryptographiques sont mis en place afin de répondre à la question de la sécurité dans les RCSFs.

La cryptographie

L'établissement d'un système cryptographique basé sur des clés sécurisées est l'une des premières contre-mesures de sécurité dans les RCSFs, ce qui permet aux nœuds capteurs de chiffrer et d'authentifier les messages communiqués entre eux. Les méthodes cryptographiques utilisées dans les réseaux RCSFs doivent répondre aux contraintes des nœuds capteurs et la nature des communications sans fil, ainsi que d'être évaluées en fonction de la taille du code, de la taille des données, du temps de traitement et de la consommation d'énergie. Mais comme les nœuds capteurs sont limités dans leurs capacités de calcul et de mémoire, les techniques cryptographiques traditionnelles bien connues ne peuvent pas être simplement appliqués aux RCSFs sans les adapter. Par conséquent, pour satisfaire les contraintes de sécurité mentionnées ci-dessus, soit les techniques existantes doivent être adaptées, soit des techniques nouvelles doivent être développées. Sur la base des techniques cryptographiques existantes, Les systèmes cryptographiques sont généralement classés selon les trois aspects suivants: les techniques cryptographiques symétriques, les techniques cryptographiques asymétriques.

En raison des contraintes des nœuds capteurs, la sélection de la technique cryptographique appropriée est une tâche essentielle et vitale dans les RCSFs [35] [36].

Cryptographie symétrique :

La cryptographie à clé symétrique est également connue sous le nom de cryptographie à clé partagée, à clé unique et à clé secrète. Deux primitives sont utilisées dans le cryptage symétrique la substitution et la transposition (permutation). En raison de sa facilité d'implémentation sur un matériel qui dispose de ressources (mémoire, calcul, énergie) limitées, La plupart des schémas de sécurités destinées aux RCSFs utilisent uniquement la cryptographie à clé symétrique. Dans ce type de cryptage, une phase de pré-distribution de clés secrètes est obligatoire avant le déploiement des nœuds capteurs, donc l'expéditeur et le destinataire doivent partager la même clé secrète pour commencer à crypter et décrypter les messages entre eux en utilisant cette clé. Deux types de chiffrements symétriques sont utilisés [37]

- Le chiffrement en chaîne est fait bit à bit sans attendre la réception entière des données. L'algorithme le plus connu est : RC4/RC5 (Rivest Cipher 5).
- Le chiffrement par bloc consiste à fractionner les données en blocs de taille fixe (64 bits, 128 bits). Chaque bloc sera ensuite chiffré une fois qu'il atteint une taille envisagée. Les algorithmes les plus utilisés sont : DES (Data Encryption Standard), AES (Advanced Encryption Standard) [38].

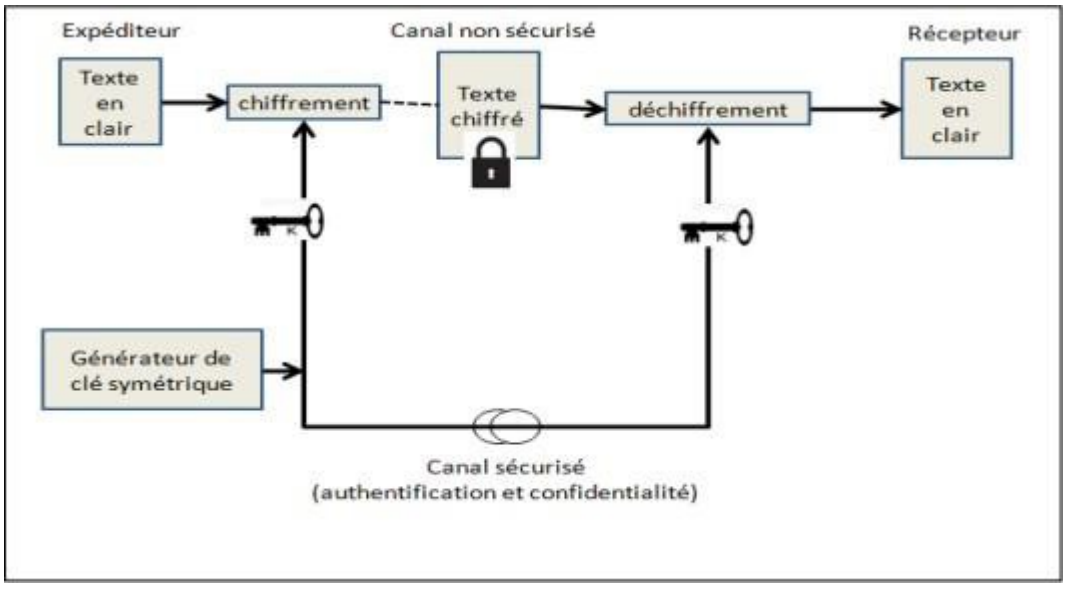


Figure 2.5 : la cryptographie symétrique.

Cryptographie asymétrique :

ou à clé publique se repose sur l'utilisation de deux clés différentes, qui sont générées par le récepteur: une clé publique diffusée à tous les nœuds servant au chiffrement de données qu'ils vont émettre au récepteur et une clé privée maintenue secrète chez le récepteur servant pour le déchiffrement de ces

données lorsque ce dernier les reçoit. Ainsi, l'expéditeur peut utiliser la clé publique du destinataire pour chiffrer un message que seul le destinataire (en possession de la clé privée) peut déchiffrer, garantissant la confidentialité du contenu. D'un autre côté, l'expéditeur peut utiliser sa propre clé privée pour signer un message et le destinataire peut vérifier la signature du message à l'aide de la clé publique correspondante. Dans ce cas, ce mécanisme permet aussi de garantie l'authentification des auteurs des messages en utilisant la signature numérique. La figure 2.5 illustre un mécanisme de chiffrement basé sur la cryptographie asymétrique. Bien que le chiffrement asymétrique comporte des avantages, mais la complexité de ce type de cryptographie n'exige que le nœud capteur à une capacité de traitement et de stockage plus élevée et une consommation d'énergie plus haute. Parmi les algorithmes de chiffrement asymétrique les plus connus nous citons : l'ECC (elliptic curve cryptography) et le RSA (Rivest Shamir Adleman) [38].

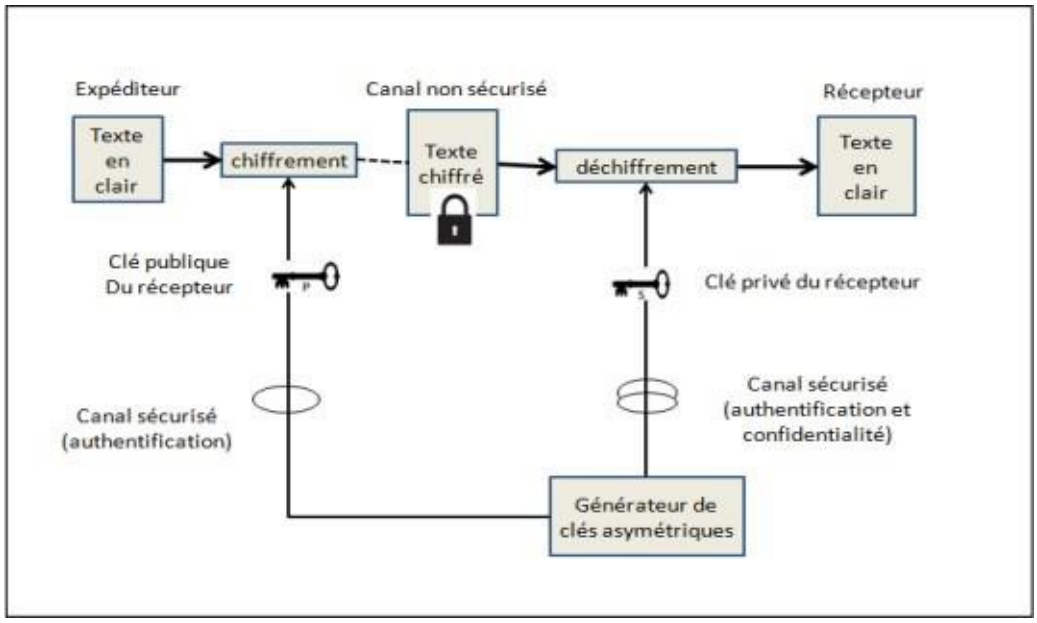


Figure2.6 : La cryptographie asymétrique.

La fonction de hachage

Une fonction de hachage cryptographique consiste à calculer une courte empreinte de taille fixe à partir d'un bloc de données de taille arbitraire. En général, Il est facile de calculer l'empreinte à partir du contenu du message à transmettre, tandis qu'il est difficile de trouver le contenu du message à partir de l'empreinte (c.à.d. très difficile à inverser). Cette empreinte est recalculée par le destinataire afin qu'il la compare à celle calculée par l'expéditeur. Si elles sont différentes, alors les données ont été modifiées pendant leur transmission. Les fonctions de hachage sont souvent utilisées comme un mécanisme qui vérifie l'intégrité d'un message ou bien pour générer des signatures numériques.

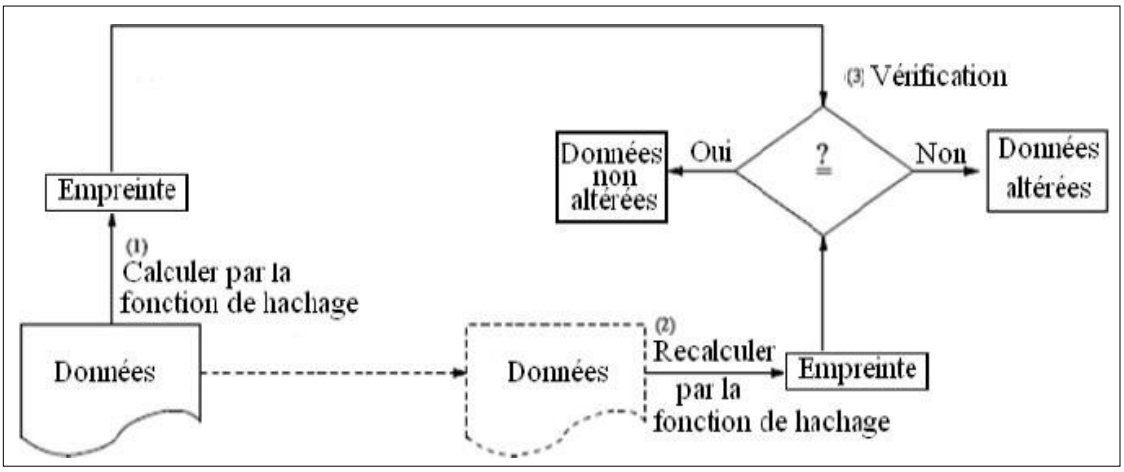


Figure 2.7 : La fonction de hachage

Code d'authentification de message

Le code d'authentification de message MAC (Message Authentiquassions Code) fait partie des fonctions de hachage à clé symétrique assurant l'intégrité des données comme toute autre fonction de hachage, en plus, l'authenticité de la source de données. Comme illustré dans la figure (cette clé est utilisée pour calculer le code MAC par l'émetteur (1). Ce code est par la suite envoyé avec les données (2). Le récepteur calcule à son tour le code MAC avec cette même clé et le compare au code qu'il a reçu (3). S'ils sont bien identiques (4), alors la source est authentique et les données n'ont pas été altérées.

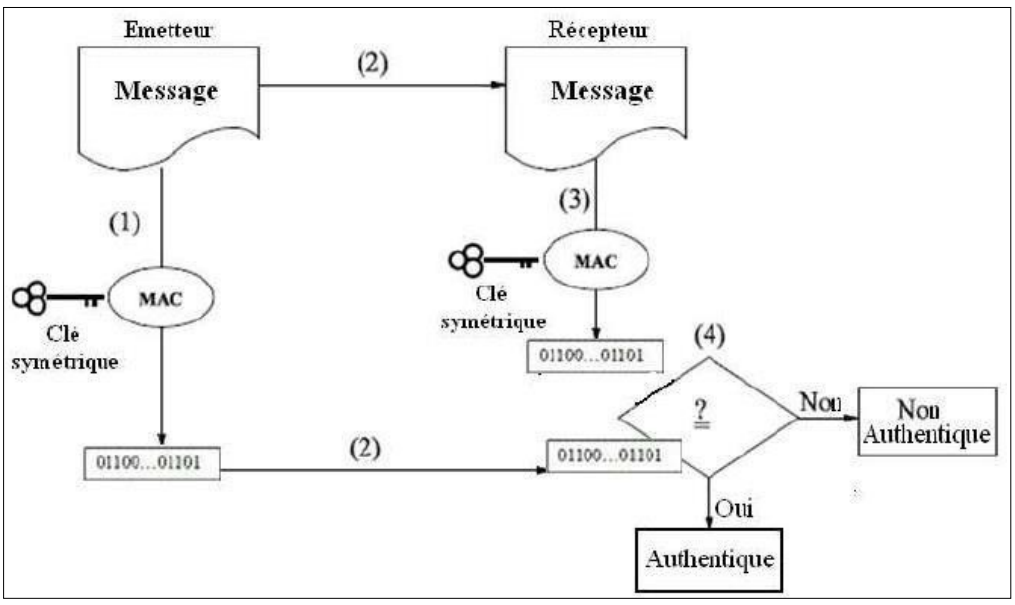


Figure 2.8 : Le code d'authentification de message MAC.

Protocoles et services: protocoles de base

Bien que la protection du canal de communication protège les RCSFs contre certaines attaques, elle ne garantit pas entièrement que d'autres attaques ne les affectent pas. En effet, il existe d'autres attaques spécifiques aux protocoles élaborées qui peuvent perturber, détruire ou corrompre un réseau. Ainsi, la capacité du réseau d'exécuter ses fonctions est diminuée ou élimine. Par conséquent, il est nécessaire de créer des protocoles et services spécialisés capables de soutenir adéquatement la protection des données.

Pour rappel, l'objectif de ce mémoire est la sécurité du routage dans les réseaux de capteurs sans fil, qui constitue l'une des défis majeurs et qui confrontent le bon fonctionnement de ces derniers. Nous concentrons dans ce qui suit sur les principaux mécanismes permettant de sécuriser les protocoles de routage.

Protocoles et services: protocoles de base

Bien que la protection du canal de communication protège les RCSFs contre certaines attaques, elle ne garantit pas entièrement que d'autres attaques ne les affectent pas. En effet, il existe d'autres attaques spécifiques aux protocoles élaborées qui peuvent perturber, détruire ou corrompre un réseau. Ainsi, la capacité du réseau d'exécuter ses fonctions est diminuée ou élimine. Par conséquent, il est nécessaire de créer des protocoles et services spécialisés capables de soutenir adéquatement la protection des données.

Pour rappel, l'objectif de ce mémoire est la sécurité du routage dans les réseaux de capteurs sans fil, qui constitue l'une des défis majeurs et qui confrontent le bon fonctionnement de ces derniers. Nous concentrons dans ce qui suit sur la sécurité de routage.

Sécurité de routage dans les RCSFs

Le problème du routage consiste à déterminer un acheminement optimal des paquets à travers le réseau au sens d'un certain critère de performance comme la consommation énergétique. Une attaque simple de déni de service sur un protocole de routage consiste pour un nœud à refuser arbitrairement de transférer certains messages ou de supprimer un paquet en transit de façon aléatoire. L'attaque du trou de ver peut également faire croire à deux nœuds distants qu'ils sont très proches alors qu'en réalité ils sont éloignés de plusieurs sauts. En présence de telles attaques, les nœuds du réseau seront alors contraints de mettre à jour leur table de routage pour continuer d'assurer la fiabilité de leur service. Il est donc nécessaire de sécuriser les protocoles de routage conçus initialement pour un environnement sans risque ou même de concevoir de nouveaux algorithmes robustes afin de mener à bien l'opération de

l'acheminement des données même en présence des nœuds malicieux. Cette problématique a été très largement étudiée par les chercheurs ces dernières années.

Conclusion

Nous avons abordé dans ce chapitre le problème de sécurité dans les RCSFs, à savoir les différentes vulnérabilités qui peuvent être rencontrées, les mécanismes de sécurité dans ce réseau, les attaques qui menacent les RCSFs, ainsi que les différents mécanismes de sécurité existants qui tentent de protéger le canal de communication et les protocoles et services. Plusieurs travaux de recherches ont été menés pour résoudre les problèmes de sécurité liés aux RCSFs, tels que la sécurité de l'agrégation de données, la sécurité de routage et la sécurité de la localisation.

Dans le chapitre précédent, nous avons présenté le protocole de routage hiérarchique LPWS dont l'objectif principal est le prolongement du temps de la vie du réseau ainsi que la gestion efficace de la consommation énergétique. Cependant, la sécurité présente un grand challenge vu les caractéristiques du protocole LPWS. Par exemple, des attaques peuvent provoquer des menaces dangereuses contre le réseau.

Dans nos travaux, nous avons investigué ce problématique et nous avons proposé dans le prochain chapitre une alternative sécurisée du protocole LPWS qui permet de pallier aux problèmes de sécurité les plus importants.

Chapitre 3

Sécurisation du protocole de routage LPWS

Introduction

Malgré les avancées technologiques, il est actuellement évident de constater que les nœuds capteurs possèdent une faible capacité en termes de calcul, de stockage et d'énergie, ce qui les rend vulnérables et faciles à corrompre afin de récupérer les informations qu'ils possèdent.

C'est la raison pour laquelle assurer la sécurité dans ce type de réseaux devient un enjeu très important et ce notamment en ce qui concerne le bon acheminement des données.

Et comme il a déjà été cité dans le chapitre précédent, LPWS est un protocole de routage non sécurisé. Nous allons dans ce chapitre proposer une solution de sécurisation pour ce protocole. Notre premier but est d'atteindre un niveau de sécurité acceptable sans dégrader les performances du réseau. De ce fait, nous avons établi un nouveau protocole SEC-LPWS (Secured - A New Location Based Protocol for Wireless Sensor Clustering), qui est en mesure de pallier aux importantes attaques visant le protocole de routage LPWS.

Pour cela, nous commençons par introduire les principes de base de cette proposition, ensuite nous présenterons les détails de notre algorithme. Également, nous présentons une analyse des performances de notre protocole par rapport au protocole LPWS.

Objectifs de la sécurité pour LPWS

Lorsque nous abordons le problème de sécurité, nous visons à atteindre certains objectifs telles que : l'authentification de sources de données, et l'intégrité de données, etc. Notre travail consiste à déterminer l'ensemble de mesures à prendre, et cela dans le but d'atteindre les objectifs visés.

Afin de faire face aux attaques décrites dans le chapitre précédent, le protocole LPWS a besoin d'assurer l'authentification, la confidentialité et l'intégrité. Ainsi, nous obtenons un nouveau protocole sécurisé que nous appelons « SEC-LPWS » (Secured - A New Location Based Protocol for Wireless Sensor Clustering).

Authentification de sources de messages

C'est le service le plus important car on ne pourra pas assurer une confidentialité ou une intégrité de messages échangés si, dès le départ, nous ne sommes pas sûrs de communiquer avec le bon nœud. Cette solution assure que les sources de données ne parviennent pas d'un nœud malveillant. L'authentification des données est assurée grâce au Code d'Authentification de Message (CAM), ou MAC en anglais (Message Authentication Code). [40]

Différents types de transmissions à sécuriser

Le service d'authentification de la source de messages doit être assuré dans tous les paquets émis sur tous les liens de communication reliant les différentes entités du réseau (station de base – CH, CH– CM). A travers ces liens, deux types de transmissions sont employés, dont chacun nécessite un mécanisme de sécurité particulier [41] :

- **Unicast** : L'authentification de sources de données dans les transmissions unicast est facilement réalisée grâce aux fonctions MAC.
- **Broadcast** : Les techniques implémentant la transmission unicast ne peuvent pas être appliquées telles quelles aux transmissions de groupes. En effet les mécanismes basés sur une clé secrète ne peuvent pas être appliquée directement à l'authentification en broadcast, car un nœud compromis récepteur peut facilement deviner le message de l'expéditeur. Par conséquent, d'autres mécanismes doivent être utilisés pour garantir l'authentification de sources de messages dans de telles transmissions

Différents liens de communication à sécuriser

Dans la partie suivante, nous allons recenser d'une manière exacte les liens à sécuriser afin de se prémunir contre les attaques visant le protocole LPWS:

- **Station de base-voisins :** Ce lien est utilisé au moment du déclenchement du round par la station de base. Des conséquences fatales pourront découler si un nœud malicieux parvient à se faire passer pour ce dernier en provoquant ainsi l'attaque « Forged Base Station ». L'attaquant peut annoncer le déclenchement d'un round toutes les t périodes très proches. Ainsi, les processus qui suivent cette étape vont se répéter d'une façon périodique et contiguë. Cela mène, d'une part, à ne pas laisser les nœuds se charger de la phase de captage, et d'autre part, à épuiser rapidement leur énergie dû à un travail effectué d'une façon répétée.
- **Nœuds -voisins :** Ce lien est utilisé pendant l'étape de planification à partir des nœuds vers leurs voisins. Si ces nœuds ne sont pas authentiques, l'attaque « Ghost Nodes » pourra facilement se provoquer.
- **Membres-CH :** ce lien est utilisé lors de l'envoi de la température du nœud membre au nœud CH. Un CH doit être sûr de la source de messages venant des membres de son groupe. Si ce lien n'est pas sécurisé, un nœud malicieux pourra injecter de fausses données au CH. Il pourra aussi transmettre plusieurs données afin qu'elles soient traitées par le CH pour falsifier son résultat d'agrégation et pour le saturer ou l'épuiser.

- **CH-station de base :** ce lien est utilisé lors de l'envoi des résultats d'agrégation du CH à la station de base. Un nœud malicieux peut alors attaquer ce schéma en injectant de fausses données dans le réseau ou en falsifiant le résultat d'une opération d'agrégation. Dans ce cas, la station de base doit authentifier les CH afin de ne pas recevoir des données d'un nœud malicieux

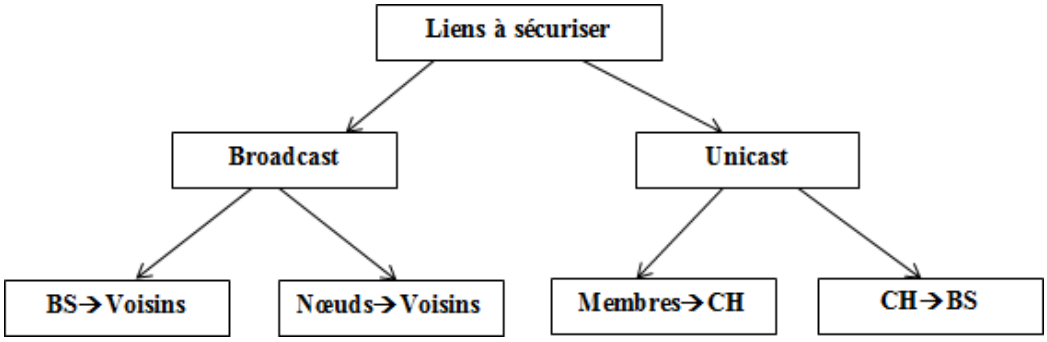


Figure.3.1: Liens de communication à sécuriser dans LPWS.

Confidentialité

Dans les RCSFs, les données captées sont sensibles et peuvent être menacées par des évènements extérieurs ou intérieurs, d'où le besoin d'assurer leur confidentialité. En ce qui concerne LPWS, il manipule des données secrètes. Par conséquent, on a besoin d'assurer ce service au niveau du routage.

Intégrité de messages échangés

Il est primordial d'assurer que les informations de routage transmises n'ont pas été altérées comme l'annonce d'un nouveau round, l'envoie des coordonnées (x, y) des nœuds. En effet, un attaquant peut modifier les paquets de données qu'il a interceptés. Par conséquent, une garantie d'intégrité de données permet de faire face à l'injection ou la modification des paquets.

Fonctionnement du protocole proposé

Le processus de fonctionnement de SEC-LPWS est divisé en trois phases qui sont : (i) la pré-distribution de clés, (ii) la formation du cluster et l'établissement de clés, et (iii) la transmission de données. Dans la première phase les nœuds sont pré-chargés avec certain matériel cryptographique tel que la clé de réseau. SEC-LPWS utilise un crypto-système symétrique et prend en charge dans la deuxième phase la formation de clusters et l'établissement de deux clés : $K_{CH_\alpha - BS}$ (la clé partagée entre le cluster head CH_α et la station de base) et la clé $K_{CM_j - CH_\alpha}$(la clé partagée entre un nœud membre CM_j et son cluster head

CH_α. Ces deux clés seront utilisées dans la dernière phase afin d'établir des communications sécurisées. Enfin, chaque nœud membre envoie les données captées à son CH correspondant qui va les agréger et les envoyer directement à la station de base.

Dans SEC-LPWS, deux fonctions sont appliquées aux messages afin d'assurer les objectifs de sécurité des communications. La première est la fonction $MAC\{\ \}$ (code d'authentification du message), utilisée pour authentifier les données envoyées. La deuxième est la fonction $E\{\ \}$, utilisée pour chiffrer les données envoyées. Tandis que, RC5 est utilisé comme algorithme de chiffrement dans ces deux fonctions. Nous utilisons également le nonce (N_S), utilisé pour calculer les clés partagées. De plus, le type du message est envoyé dans le paquet afin de déterminer son objectif.

Nous exposons au tableau 3.1 un résumé des notations que nous avons utilisées afin de détailler chaque phase de ce système. Dans ce qui suit, nous avons détaillé chaque phase liée au protocole proposé.

Notation	Explication
id_{CM_j}	Identificateur de membre de cluster j
id_{CH_α}	Identificateur de cluster-head α
id_P	Identificateur de nœud puits
$E_K(M)$	Chiffrement du message M avec la clé K
$MAC_K(M)$	Code d'authentification de message du message M avec la clé symétrique K
N_S	Nonce généré par le nœud de capteur S
$H_K^{i}(\ )$	$i^{ème}$ fonction de hachage avec la clé symétrique K
r	Compteur reflète le nombre de round
$S \rightarrow *: M$	Le nœud S diffuse le message M
$A \parallel B$	Concaténation de l'information A avec l'information B
$\oplus$	opération XOR au niveau du bit
$cellu\_ID$	Identificateur de la cellule
Val_Temp	La valeur de la température captée
$Temp\_Moy$	La valeur de la température moyenne calculée

Tableau 3.1 : Acronymes définition

La phase de pré-distribution de clés

Plusieurs nœuds capteurs sont pré-chargés avec plusieurs informations avant d'être livrés dans la zone de détection. La SB doit pré-charger certain matériel cryptographique dans chaque nœud pour générer des autres clés. Ces matériaux incluent:

- Une clé K_{in} partagée avec la station de base pour chiffrer / déchiffrer les messages de la station de base vers les nœuds.
- Une clé de réseau K_N partagée par tous les nœuds du réseau, utilisée pour chiffrer / déchiffrer les messages juste après le déploiement.
- Un numéro d'identification unique ID

La phase de formation de cluster et l'établissement de clés

Une fois les nœuds déployés, ils effectuent la planification du réseau afin de déterminer l'identification de la cellule (ID cellule) à laquelle il appartient et les coordonnées (x, y) du centre de gravité (COG: Center Of Gravity) de leur cellule. En effet, ce processus se déroule durant le round 0.

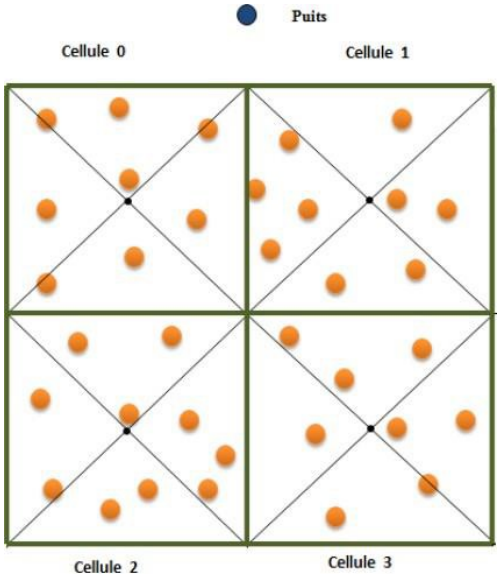


Figure 3.2 : Etape de Planification [9]

La station de base initie la construction des clusters en diffusant un message « $HELLO$ » chiffré par la clé de réseau K_{in} comme suit :

$$BS \rightarrow *: id_{BS} \parallel cellu\_ID \parallel E_{K_{in}}\{\text{HELLO}, N_{BS}\} \parallel MAC_{K_{in}}\{id_{BS} \parallel cellu\_ID \parallel E_{K_{in}}\{\text{HELLO}, N_{BS}\}\}$$

Chaque nœud qui a reçu le message « $HELLO$ » diffuse un message d'annonce « $ELECTION$ » aux autres nœuds. Ce message contient son identifiant, sa position (en coordonnées (x, y)) et l'identification de sa cellule.

$$N \rightarrow *: id_N \parallel cellu\_ID \parallel E_{K_N}\{ELECTION, x, y, N_N\} \parallel MAC_{K_N}\{id_N \parallel cellu\_ID \parallel E_{K_N}\{ELECTION, x, y, N_N\}\}$$

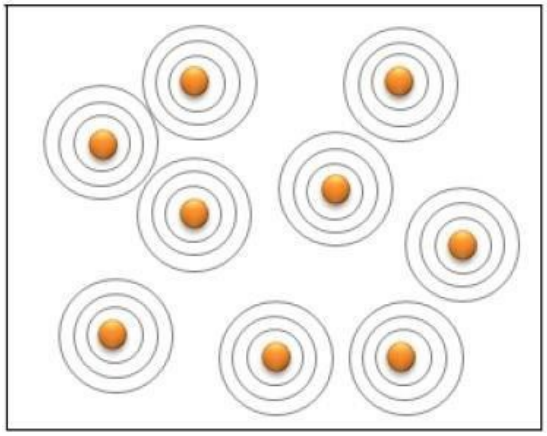


Figure 3.3 : Phase d'Annonce [9]

Les nœuds qui ont reçu ces messages, doivent vérifier si l'ID de la cellule reçu dans le message correspond à l'ID de cellule enregistrée (sa cellule) et authentifie le message « $ELECTION$ » (en vérifiant le MAC). Ainsi, chaque nœud capteur identifie l'ensemble des nœuds capteurs qui se trouvent dans la même cellule. Il calcule ensuite la distance qui sépare sa position du centre de la cellule, ainsi que la distance qui sépare chaque nœud et le centre de cette même cellule.

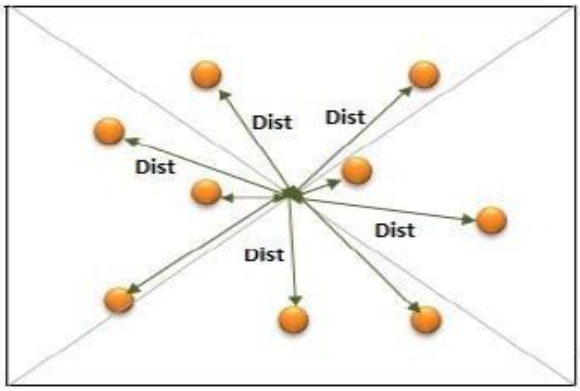


Figure 3.4 : Etape d'Élection (calcul des distances)

Après l'accomplissement de cette tâche, tous les nœuds non-CHs arrivent à identifier leurs CHs. En effet, le CH va être choisi en se basant sur le tri des distances calculées.

Chaque nœud CH ou non-CH dans la même cellule construit un tableau contenant l'identificateur de nœud membre, et un index, qui est construit selon l'ordre des distances calculées.

D'ailleurs, un slot est attribué à chaque nœud membre pour communiquer avec le nœud CH, ce slot est égal à index+1.

Après cette étape, les nœuds capteurs sont prêts à établir les clés de communications. En

effet, dans la topologie hiérarchique en cluster, un nœud membre CM_i du cluster C_α ne communique qu'avec son cluster-head CH_α. Pour cela, afin d'établir une clé de cryptage pour sécuriser la communication entre un membre de cluster CM_i et leur cluster-head CH_α, les nœuds (membre ou cluster-head) calcule la clé par paire à l'aide de l'équation suivante:

$$K_{CM_j-CH_\alpha} = H_{K_N}\ (ma\ x\ (id\ _{CM}, id_{CH_\alpha})\ \|\ N_{CM_j} \oplus N_{CH_\alpha}) \tag{3.1}$$

À la fin de la phase de formation de cluster et l'établissement de clés, les clés K_N et K_{in} seraient supprimées de la mémoire du nœud. Dans ce cas, des nouvelles clés seront calculées avant d'effacer les clés précédentes:

$$K_{in} = H_{K_i}\ (K_{in}) \tag{3.2}$$

$$K_N = H_{K_N}\ (K_N) \tag{3.3}$$

r : est un compteur, initialisé à zéro, qui reflète le numéro du round. Le r dans ce cas est égal à 1.

La phase transmission

Dans cette phase, le transfert de données vers la station de base aura lieu. En utilisant l'ordonnanceur TDMA, les nœuds membres émettent leurs données captées pendant leurs propres slots.

$$CM_j \rightarrow CH_\alpha : id_{CM_j}$$

$$\| E_{K_{CM_j-CH_\alpha}}\{DATA\_Send, Temp\_Val\} \| MAC_{K_{CM_j-CH_\alpha}}\{ id_{CM_j}$$

$$\| E_{K_{CM_j-CH_\alpha}}\{DATA\_Send, Temp\_Val\}\}$$

Après la réception du message « $DATA\_Send$ », chaque nœud CH commence par vérifier l'authenticité du message (en vérifiant le MAC) et ensuite agréger les données selon la fonction d'agrégation (moyenne, somme, suppression des redondances…etc.). Ils envoient ensuite le résultat final à la station de base.

$$CH_\alpha \rightarrow BS : id_{CH_\alpha}$$

$$\| E_{K_{CH_\alpha-BS}}\{DATA\_Agreg, Temp\_Moy\} \| MAC_{K_{CH_\alpha-BS}}\{ id_{CH_\alpha}$$

$$\| E_{K_{CH_\alpha-BS}}\{DATA\_Agreg, Temp\_Moy\}\}$$

Tel que $K_{CH_\alpha - BS}$ est la clé par paire partagées entre le cluster head CH_α et la station de base. Elle est calculée à l'aide de l'équation suivante:

$$K_{CH_\alpha - BS} = H_{K_i}(id_{BS} \parallel id_{CH_\alpha} \parallel r) \quad (3.4)$$

A la fin de la phase de transmission, la station de base reçoit les données agrégées (envoyées par d'autres nœuds) et initie un nouveau round.

Quand le round est différent de 0 (r≠0), ce processus est modifié, cette fois on ignora la phase d'initialisation. Ceci est dû au fait que l'élection des nœuds CH va être automatique. Les CH élus sont les nœuds correspondant au ID approprié au index du tableau (tel que index=r) et comme les tableaux des nœuds de chaque cluster sont les mêmes, les autres nœuds connaissent directement son CH pour ce round.

Ainsi, après la réception de message d'initialisation de nouveau round r, des nouvelles clés sont calculées et les nœuds passent directement à la phase transmission.

Simulation

La simulation des réseaux de capteurs consiste principalement en la reproduction du comportement des nœuds capteurs et des interactions entre eux. C'est une étape incontournable pour l'évaluation des modèles d'application ou des protocoles de communication. De plus, la simulation offre un gain considérable en temps, une flexibilité en permettant la variation des paramètres et une meilleure visualisation des résultats [42].

Dans cette section, nous présentons les outils utilisés pour la mise en œuvre des protocoles LPWS et SEC- LPWS. D'ailleurs, Nous donnons un aperçu sur le déroulement des deux approches.

Présentation de l'environnement Tinyos

On a choisi le système Tinyos pour réaliser notre simulation. Il est adapté aux capteurs. Il supporte de nombreuses plates-formes et il fournit des concepts très importants pour réaliser les simulations. La nomination TinyOS indique d'une part un système d'exploitation conçu particulièrement pour les RCSFs et qui doit être installé sur chaque nœud capteur du réseau. D'une autre part, TinyOS indique l'environnement de simulation d'applications de RCSF qui tournent sous le système d'exploitation TinyOS. Cet environnement est formé par le simulateur TOSSIM, le système d'exploitation TinyOS, l'émulateur Cygwin et tout un ensemble d'outils de simulation. Dans ce contexte, nous présentons dans cette partie l'environnement TinyOS sur lequel fonctionne le simulateur TOSSIM.

TinyOS

Suite aux différents défis des RCSF qu'on a vus dans les chapitres précédents, l'université de Berkeley, en plus de nombreux contributeurs ont développé un système d'exploitation destiné au RCSF afin de faciliter l'implémentation et l'exécution de protocoles dédiés à ce type de réseaux. L'objectif consiste à minimiser la taille du code afin de respecter les contraintes de ressources énergétiques et physiques des nœuds capteurs. Ce système est intitulé TinyOS [40]. Il a l'avantage de permettre une programmation simple et puissante tout en gardant la portabilité du code pour les nombreuses plateformes supportées. Il est utilisé par plus de 500 universités et centres de recherche dans le monde vu la caractéristique open source qu"il détient [41]. Il respecte une architecture basée sur une association de composants. Il utilise une programmation entièrement réalisée en langage NesC.

Cygwin

Cygwin est une collection de logiciels libres à l'origine développés par Cygnus Solutions permettant à différentes versions de Windows d'émuler un système Unix. Cygwin tente de créer un environnement Unix sous Windows, rendant possible l'exécution de ces logiciels après une simple compilation. [42].

Le simulateur TOSSIM

Avant sa mise en place, le déploiement d'un RCSF nécessite une phase de simulation afin de s'assurer du bon fonctionnement de tous les protocoles de communication qu'il utilise. En effet, pour de grands réseaux, le nombre de capteurs peut atteindre plusieurs milliers et entraine donc un coût financier relativement important. Ainsi, il faut réduire au maximum les erreurs de la conception. Malgré cela, il reste des facteurs réels qui ne peuvent être pris en compte par la simulation, tels que les contraintes physiques (perturbations électromagnétiques, inondations, etc.) ou les aléas (détériorations dues à un animal, etc.). Pour arriver à simuler le comportement des capteurs au sein d'un RCSF, un outil très puissant a été développé et proposé pour TinyOS sous le nom de TOSSIM. Le principal but de TOSSIM est de créer une simulation très proche de ce qui se passe dans les RCSFs dans le monde réel. Une économie d'effort et une préservation du matériel sont possibles grâce à cet outil. Pour une compréhension moins complexe de l'activité du réseau, TOSSIM peut être utilisé avec une interface graphique TinyViz. Cette dernière est équipée par plusieurs API plugins qui permettent d'ajouter plusieurs fonctions à notre simulateur comme par exemple suivre la dépense d'énergie en utilisant un autre simulateur qui s'appelle PowerTOSSIM .

Déroulement de LPWS et SEC-LPWS

Dans cette partie, nous utiliserons TinyViz pour expliquer les différentes étapes des deux algorithmes LPWS et SEC-LPWS. Un fichier de configuration est créé et permet à TinyViz de se démarrer avec les paramètres spécifiés. Ceux-ci représentent : le nombre et l'emplacement des nœuds capteurs, la durée de simulation, et les plugins que l'on souhaite activer dès le début de la simulation comme Debug Messages et power profiling.

- **Déclenchement du round et la diffusion des messages d'annonces :**

La figure 3.5 montre les transmissions de diffusion qui se passent durant les différentes étapes du protocole. Une transmission de diffusion de l'algorithme LPWS ou SEC-LPWS est marquée par des cercles bleus. La station de base envoie une diffusion aux nœuds voisins pour notifier le round, ses voisins envoient à leur tour selon une transmission broadcast un message d'annonce.

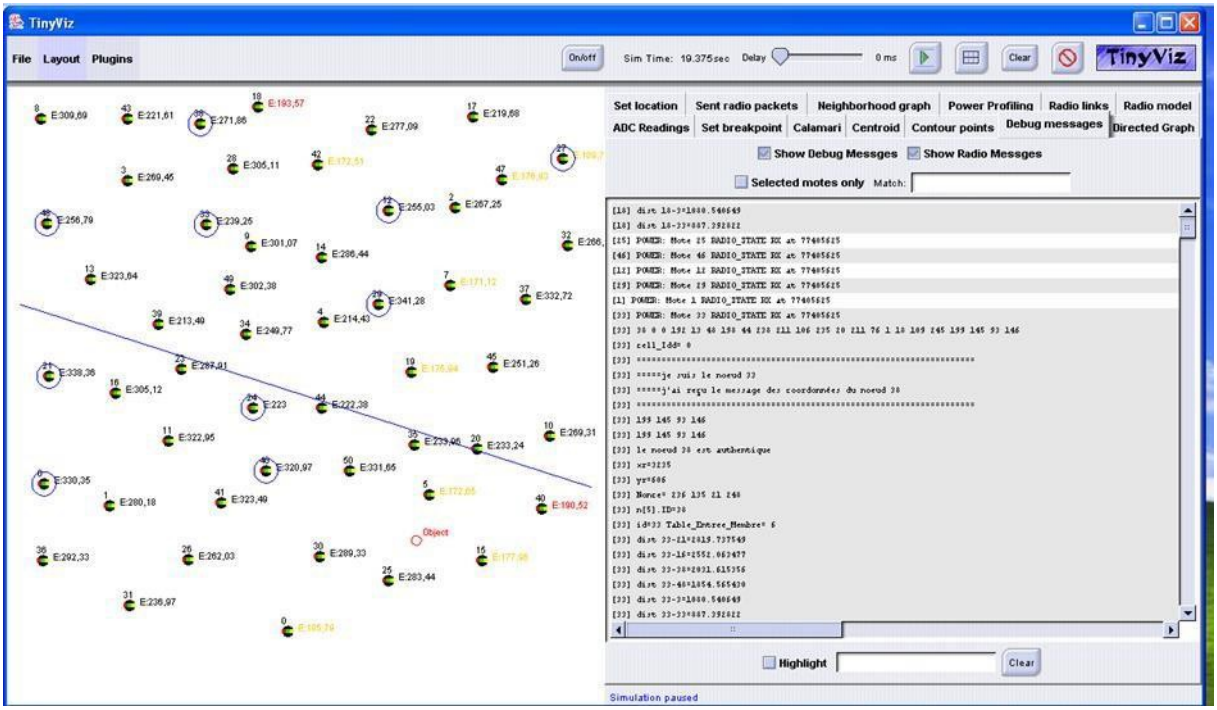


Figure 3.5 : Déclenchement du round et la diffusion des messages d'annonces

- **Formation des groupes et l'envoie des températures :**

Une fois le CH est élu, les nœuds membres émettent leurs données captées de la température pendant leurs propres slots. La figure 3.6 montre quelques transmissions unicast qui se

passent à cette étape de l'algorithme LPWS et SEC-LPWS. La transmission unicast est signalée par une flèche rose.

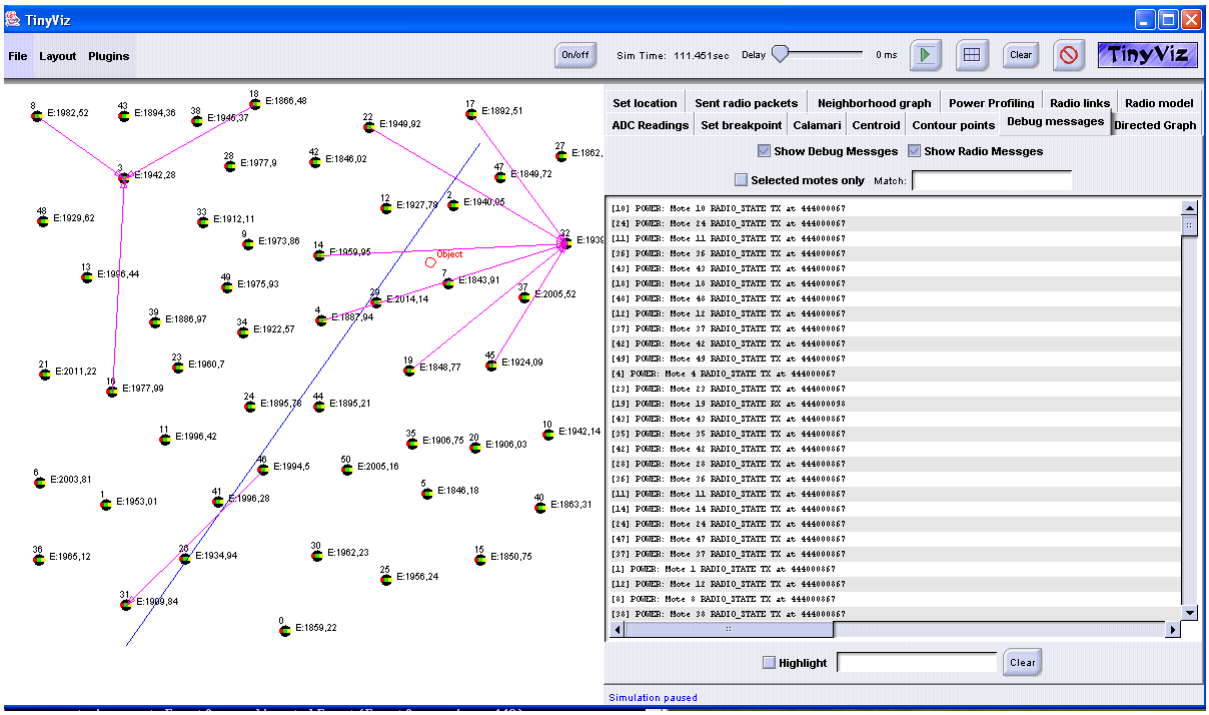


Figure 3.6: Formation des groupes et l'envoie des températures

❖ **L'agrégation des données et la transmission à la station de base :**

Après un certain temps, le CH agrège les températures reçues et envoie son résultat d'agrégation à la station de base (Puits).

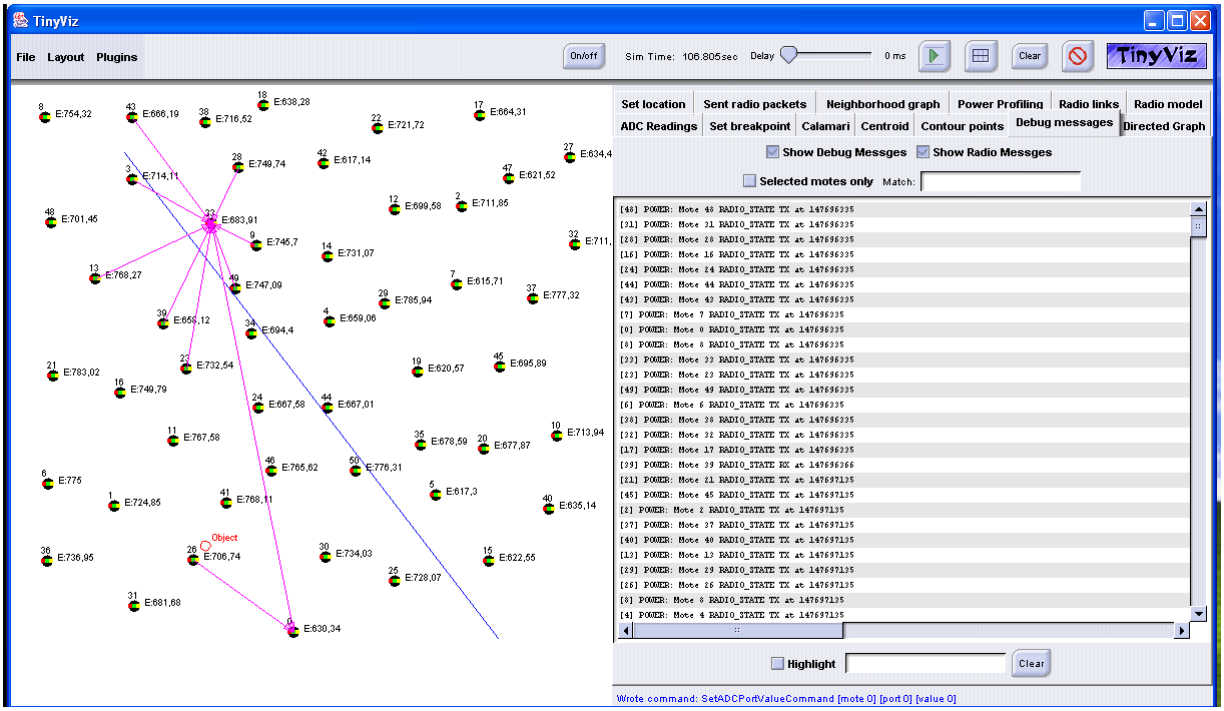


Figure 3.7 : L'agrégation des données et la transmission à la station de base

Environnement de simulation et résultats

Pour évaluer les performances de protocole de routage SEC-LPWS par rapport au protocole LPWS, nous l'avons implémenté en utilisant le langage de programmation NesC afin d'être en mesure de l'intégrer à TinyOS. Les simulations sont effectuées à l'aide de l'environnement TOSSIM. Nous nous sommes intéressés essentiellement à la consommation d'énergie des nœuds capteurs puisqu'elle constitue un paramètre primordial pour la détermination de la durée de vie d'un RCSF.

Avant de lancer les simulations, nous devons ajuster certains paramètres qui sont présentés par le tableau suivant :

Nombre de nœuds du réseau	**20, 50, 100, 150**
La taille du réseau	(100 x 100) m^2
Délai de la simulation	500 secondes : les résultats de la simulation adéquats durant l'état transitoire
Nombre d'itération (simulations)	10: les résultats que nous allons présenter sont une moyenne de 10 simulations pour un même scénario
Taille de paquet de données	29 octets : c'est le paquet de transmission de TinyOS
Modèle de propagation	Modèle Lossy.

Tableau 3.2 : Les paramètres de simulation

Afin d'évaluer les performances de protocole SEC-LPWS, nous nous intéressons aux métriques suivantes :

❖ **Consommation d'énergie des CH et des CM sur un échantillon de 50 nœuds :**

La figure 3.8 représente les résultats de calculs de la consommation d'énergie des nœuds CH et des nœuds CM. Nous pouvons vérifier, en analysant le résultat de la figure, que les sommets représentent l'énergie consommée par des nœuds qui ont été élus CH durant la simulation. Nous pouvons bien constater que les nœuds dans le protocole SEC-LPWS consomment plus d'énergie que ceux du protocole LPWS, d'un taux approximativement égal à 0.2 % et cela est due aux mécanismes de sécurité introduit.

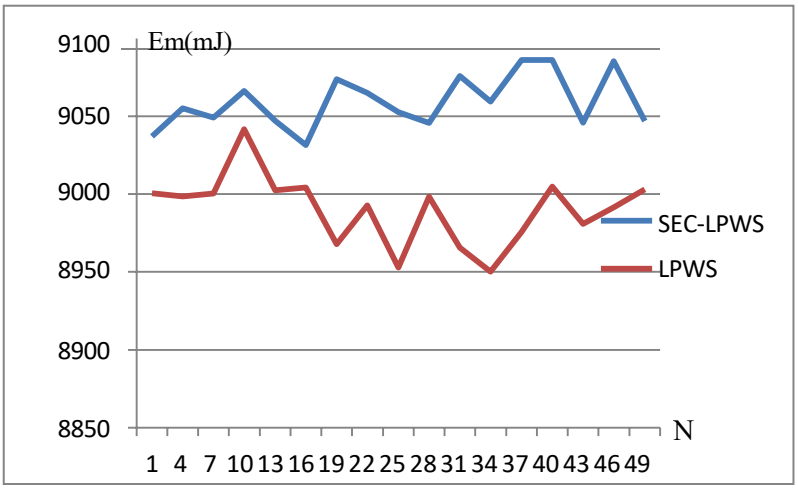


Figure 3.8 : Energie consommée par nœud (N=50)

❖ **Moyenne de consommation d'énergie :**

La consommation d'énergie est un paramètre important pour tous les protocoles de routage dans les RCSFs. Par conséquent, nous avons utilisé le plugin PowerTOSSIM dans TinyViz pour analyser l'énergie. Cette énergie est calculée sur la base des instructions exécutées pour les opérations cryptographiques et pour les opérations radio (émission et réception des messages). La figure 3.9 illustre la variation de l'énergie moyenne consommée en fonction de la taille de réseau, la courbe nous permet de remarquer que la taille du réseau est indépendante de la consommation d'énergie, à cause de la topologie hiérarchique du protocole LPWS qui le rend très scalable, sinon il y'a une légère différence entre les deux protocoles d'environ 0.2% sachant que la sécurité est couteuse en énergie.

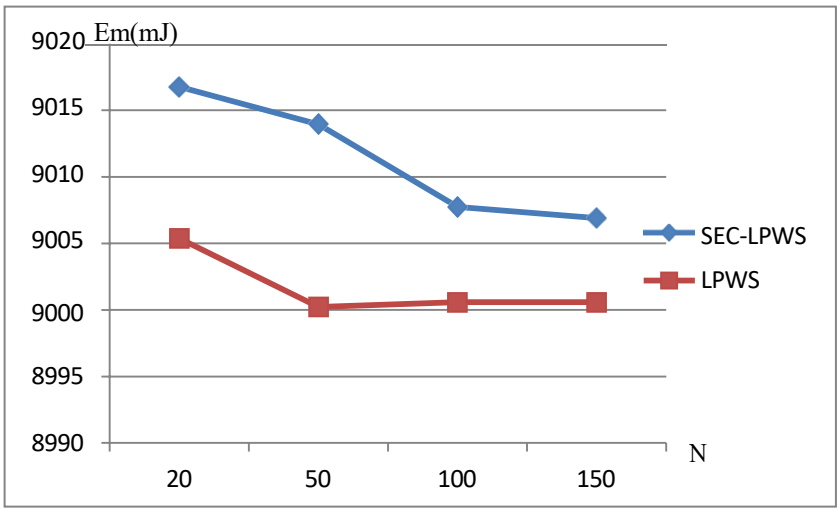


Figure 3.9: Moyenne de consommation d'énergie

Conclusion

Dans ce chapitre, nous avons présenté une solution pour la sécurisation du protocole de routage LPWS. Le système d'exploitation TinyOS est utilisé. Nous avons proposé une programmation entière en langage NesC et une simulation avec TOSSIM. L'approche proposé appelée SEC-LPWS **(S**ecured - A New Location Based Protocol for Wireless Sensor Clustering) permet de sécuriser le processus de transfert de données dans chaque phase du protocole LPWS. Ainsi, nous avons pu assurer l'intégrité, l'authentification et la confidentialité des données transmises.

Après des études expérimentales effectuées sur la consommation d'énergie nous avons constaté que le protocole SEC-LPWS répond bien aux critères de performances souhaités du réseau et donc une longévité du réseau plus grande.

Conclusion générale

Les Les réseaux de capteurs sans fil sont le prochain grand Avancées technologiques dans le développement de capteurs, processeurs puissants et les protocoles de communication sans fil. Ce type de réseau se compose de certains ou Des milliers d'éléments destinés à collecter des données environnementales, leur traitement et Ils se sont propagés au monde extérieur. En effet, l'application du réseau Des capteurs de plus en plus diversifiés, notamment pour la gestion du trafic Environnement urbain, surveillance des sites sensibles et recherche sur le milieu naturel.

Si l'acheminement correct n'est pas garanti pour accommoder Les contraintes physiques et applicatives du RCSF, associées à une cybersécurité stricte, garantissent que Confidentialité, authentification et intégrité des communications.

Dans ce travail, nous nous intéressons à la sécurisation des services de routage, qui Permet de fournir des solutions de sécurité pour le protocole LPWS (A New protocole de regroupement de capteurs sans fil basé sur la localisation) utilisant des mécanismes de sécurité Le plus approprié compte tenu de la spécificité du RCSF et des autres outils La sécurité telle que le code MAC pour l'authentification de la source du message doit être garantie et l'intégrité des données. Nos recherches nous ont conduit au protocole de sécurité SEC-LPWS (Sécurité - un nouveau protocole de clustering de capteurs sans fil basé sur la localisation).

La performance de ce protocole est évaluée en fournissant des études expérimentales, qui Cela permet une analyse approfondie du protocole. Les résultats de la simulation montrent Les performances du réseau ne se dégradent pas après la protection de la sécurité pertinente Consommation d'énergie.

BLIOGRAPHIE

[1] T.Boudries, F.Feroudj, ‟Développement d'un protocole de routage pour les réseaux de capteurs sans fil(RCSF)‟, MEMOIRE MASTER En Télécommunications, Université Amar Telidji- Laghouat, 14 / 07 /2021

[2] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci A Survey on Sensor Networks.Georgia Institute of Technology. Pages 102-114,IEEE Communications Magazine. August 2002

[3] A.Chouha, „‟ Traitement Et Transfert D'images Par Réseau De Capteurs Sans Fil,‟, Mémoire De Magistère En Informatique, Université Hadj Lakhder – Batna, 16/ 03/2011

[4] A.Saidi, W.Mamem,‟‟‟ Développement D'une Application Orientée Surveillance Pour Les Réseaux De Capteurs Sous Contiki‟‟‟, Mémoire De Licence En Informatique, Université Abou Bakr Belkaid– Tlemcen, 27 Mai 2015

[5] tinyos. [Online]. http://www.tinyos.net/

[6] D. Gay, P. Levis, R.V. Behren, M. Melsh, E. Brewer, and D. Culler, "The nesC Language: A Holistic Approach to Networked Embedded Systems", In Proceedings of the ACM SIGPLAN conference on Programming language design and implementation (PLDI '03), pp. 1-11, San Diego, California, USA, June 2003.

[7] Gauray Jolly, Mustafa C. Kusçu, Pallavi Kokate et Mohamed Younis, "A Low-Energy Key Management Protocol for Wireless Sensor Network", Proceedinge of the Eighth IEEE International Symposium on Computers and Communication, (ISCC'03), IEEE COMPUTER SOCIETY . 2003.

[8] A.Benayad,‟‟‟Implémentation Et Sécurisation du Protocole De Routage AODV optimisé pour les RCSF (OAODV)‟‟‟, MEMOIRE MASTER En Télécommunications, Université Aboubakr Belkaïd– Tlemcen, 26 / 09 /2017

[9] S.Mesmoudi, „‟Vers Une Nouvelle Approche Intelligente Pour La Gestion De Clés Dans Les Réseaux De Capteurs Sans Fils‟‟‟, Thèse De Docteur En Télécommunication, Université Aboubakr Belkaïd – Tlemcen, 09 /07 /2019

[10]N. LASLA, „‟ La gestion de clés dans les réseaux de capteurs sans-fil‟‟‟, Mémoire Magistère En Informatique Industrielle, Institut National de formation en Informatique (I.N.I) Oued-Smar, Alger 2006 – 2007.

[11] R. Kacimi, "Techniques de conservation d'énergie pour les réseaux de capteurs sans fil ", thèse de doctorat en réseaux et télécommunications, université de Toulouse, France, 2009

[12] S´everine Sentilles Architecture logicielle pour capteurs sans-fil en réseau Rapport de recherche, Universit´e de Pau et des Pays de l'Adour, juin 2006.

[13] A.Hanneche, ‟ Conception d'un nouveau protocole pour les réseaux de capteurs sans fils‟, MEMOIRE MASTER En informatique, Université L'arbi Ben M'hidi -Oum El Boua.

[14] K. Akkaya and M. Younis. "A survey on routing protocoles for wirless Sensor networks". Department of computer Science and Electrical Engineering University of Maryland, Baltimore Conty, MD 21250, 2003.

[15] M. Yasser ROMDHANE, « Evaluation des performances des protocoles S-MAC et Directed Diffusion dans les réseaux de capteurs », Projet De Fin d'Etudes, école supérieur de communication de Tunis,2007

[16] R. Marin Perianu. , Wireless Sensor Networks in Motion : Clustering Algorithms for Service Discovery and Provisioning, thèse de doctorat. University of Twente,, 2008.

[17] V. Rodoplu and T. H. Ming, "Minimum energy mobile wireless networks". IEEE Journal of Selected Areas in Communications, Vol. 17, No. 8, pp. 1333-1344, 199

.[18] C. Chong and S. Kumar, “Sensor networks: Evolution, opportunities, and challenges” Proceedings of IEEE, August 2003.
[19] H. Qi, P. T. Kuruganti and Y. Xu, “The Development of Localized Algorithmsin Wireless Sensor Networks”. Published on 202 SENSORS ISSN, pp. 1424- 8220, July 2010.
[20] Y. Yu, D. Estrin, and R. Govindan, “Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks,” UCLA Computer Science Department Technical Report, UCLA-CSD TR-01-0023, May 2001.
[21] C. B. Abbas, R. González, N. Cardenas and L. J. G. Villalba, “A proposal of a wireless sensor network routing protocol”.Springer Science and Business Media .Telecommunication Systems. pp. 61–68, March 2008..
[22] L. Doherty, K. S. J. Pister, and L. El Ghaoui, “Convex position estimation in wireless sensor networks”. In Proceedings of the IEEE INFOCOM, vol.3, Alaska, pp.1655-1663, 2001.
[23] C. Intanagonwiwat, R. Govindan and D. Estrin, “Directed diffusion: A scalable and robust communication paradigm for sensor networks”. In the Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'00), Boston, MA, August 2000.
[24] D. Estrin, R. Govindan, J. Heidemann, and Satish Kumar, “Next century challenges: Scalable Coordination in Sensor Networks”. In the Proceedings of the 5th annual ACM/IEEE international conference on Mobile Computing and Networking (MobiCom’99), Seattle, WA, August 1999.
[25] R. Jurdak, “Wireless Ad Hoc and Sensor Networks:A Cross-Layer Design perspective”, University College Dublin, 2007.
[26] F. Akyildiz, Weilian Su, Sankarasubramaniam, E. Cayirci, "A survey on sensor networks", IEEE Communications, Aug 2002.
[27] C. Schurgers and M.B. Srivastava, "Energy efficient routing in wireless sensor networks", MILCOM Proceedings on Communications for Network-Centric Operations, 2001.
[28] Callaway, Edgar H., ’Wireless Sensor Networks : Architectures and Protocols’, Auerbach Publications (2003).
[29] A. S. Uluagac, C. P. Lee, R. A. Beyah, et J. A. Copeland, « Designing Secure Protocols for Wireless Sensor Networks », in Wireless Algorithms, Systems, and Applications, vol. 5258, Y. Li, D. T. Huynh, S. K. Das, et D.-Z. Du, Éd. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, p. 503-514.
[30] D. G. Padmavathi et M. D. Shanmugapriya, « A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks », vol. 4, no 1, p. 9, 2009.
[31] J. Sen, « A survey on wireless sensor network security », Int. J. Commun. Netw. Inf. Secur., vol. 1, n o 2, p. 55-78, août 2009.
[32] J. P. Walters, Z. Liang, W. Shi, et V. Chaudhary, « Wireless Sensor Network Security: A Survey », in Security in Distributed, Grid, and Pervasive Computing, 2006 Auerbach Publications, CRC Press, p. 50.
[33] S. Athmani, « Protocole de sécurité Pour les Réseaux de capteurs Sans Fil. » Mémoire de Magistère. Université de Batna 2., 2010.
[34]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. "Wireless sensor networks: a survey". Computer Networks 38, Elsevier Science, pp. 393–422, 2002.
[35]G. Sharma, S. Bala, et A. K. Verma, « Security Frameworks for Wireless Sensor Networks- Review », Procedia Technol., vol. 6, p. 978-987, 2012.
[36]M. Panda, « Security in Wireless Sensor Networks using Cryptographic Techniques », Am. J. Eng. Res., p. 7, 2014.

[37]D. E. BOUBICHE, « Une approche Inter-Couches (cross-layer) pour la Sécurité dans les RCSF. », Thèse de doctorat. Université de Batna 2., 2013.
[38]M. Panda, « Security in Wireless Sensor Networks usi
Entrer
[39] Messai Mohamed Lamine, « Sécurité dans les Réseaux de Capteurs Sans-Fil », Université de Bejaia, 2008.
[40] Adam Dunkels, Björn Grönvall, Thiemo Voigt, « Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors », 29th Annual IEEE International Conference on Local Computer Networks, Swedish Institute of Computer Science, 2004.
[41] Cormac Duffy, Cormac J. Sreenan, John Herbert, Utz Roedig, « A Performance Analysis of MANTIS and TinyOS », Technical Report CS-2006-27-11, University College Cork, Ireland, November 2006.
[42] S. Zhu, S. Setia, and S. Jajodia. "LEAP: Efficient security mechanisms for largescaledistributed sensor networks". In ACM CCS, pp. 62–72, October 2003.

Résumé

Les Réseaux Les réseaux de capteurs sans fil (WSN) sont souvent déployés dans des environnements difficiles, Cela les rend très vulnérables. Par conséquent, il est nécessaire d'assurer la sécurité des communication est l'un des défis les plus importants de RCSF. en raison des ressources mémoire Limité et limité en énergie, incapacité à utiliser des algorithmes de sécurité complexe dans les réseaux de capteurs. Notre objectif dans ce projet de fin de recherche est de trouver une solution Il intègre le mécanisme de sécurité du protocole de routage en couches LPWS (A New protocole de regroupement de capteurs sans fil basé sur la localisation). Utiliser MAC (message Code d'authentification) et des clés préchargées au niveau du nœud pour la sécurité communication, ce qui nous aidera à obtenir un algorithme efficace pour faire face aux intrusion un taux de détection très élevé.

Mots clés : Réseaux de capteurs sans fil, sécurité, routage hiérarchique, LPWS.

Abstract:

Wireless Wireless Sensor Networks (WSNs) are often deployed in harsh environments, making them highly resilient vulnerable. Therefore, ensuring communication security is one of the most important requirements a major challenge for RCSF. Complicated due to limited memory resources and performance constraints Security algorithms cannot be used in sensor networks. Our goals in this final project are this paper proposes a combination of hierarchical routing protocol LPWS (a new location-based protocol for wireless sensor clusters). Use MAC (message verification code) and the pre-shared key on the node to ensure the security and This will help us get an efficient algorithm to deal with intruders with a very high detection rateValuation

Keywords: Wireless sensor network, Security, Hierarchical routing protocol, LPWS.

ملخص

غالبًا ما يتم نشر شبكات االستشعار الالسلكية (RCSFs) في بيئات قاسية ، مما يجعلها عرضة للهجمات. لذلك ، من الضروري التأكد يعد االتصال أحد أهم التحديات في RCSF ، وال يمكن استخدام خوارزميات ألمان بسبب موارد الذاكرة المحدودة وقيود الطاقة. شبكات االستشعار المعقدة. هدفنا في مشروع نهاية البحث هذا هو اقتراح حل يدمج آليات ألمان لبروتوكوالت التوجيه الهرمي يضمن LPWS (بروتوكول تجميع المستشعر الالسلكي الجديد المستند إلى الموقع(استخدام MAC(رمز مصادقة الرسالة(أمن مستوى العقدة ومفاتيح أمان االتصال مسبقة التحميل ، والتي ستساعدنا في الحصول على خوارزمية فعالة للتكيف عمليات االقتحام لها معدل اكتشاف مرتفع جدًا.

الكلمات المفتاحية :

شبكات االستشعار الالسلكية االمن بروتوكول التوجيه ذي التسلسل الهرمي LPWS