République algérienne démocratique et populaire Ministère del'enseignement supérieur et de la recherche scientifique

Université Abbes Laghrour de Khenchela

MÉMOIRE DE FIND'ÉTUDES

Faculté des sciences et de la technologieDépartement : mathématiques et informatique

Maîtrise en informatique option génie logiciel et systèmes distribués

Thème

Election un leader pour la gestion dynamique et distribué des réseaux

Présenté par :

M^me^. Trad Rabia

M^me^. Moussaoui Amira

Devant le Jury composé de :

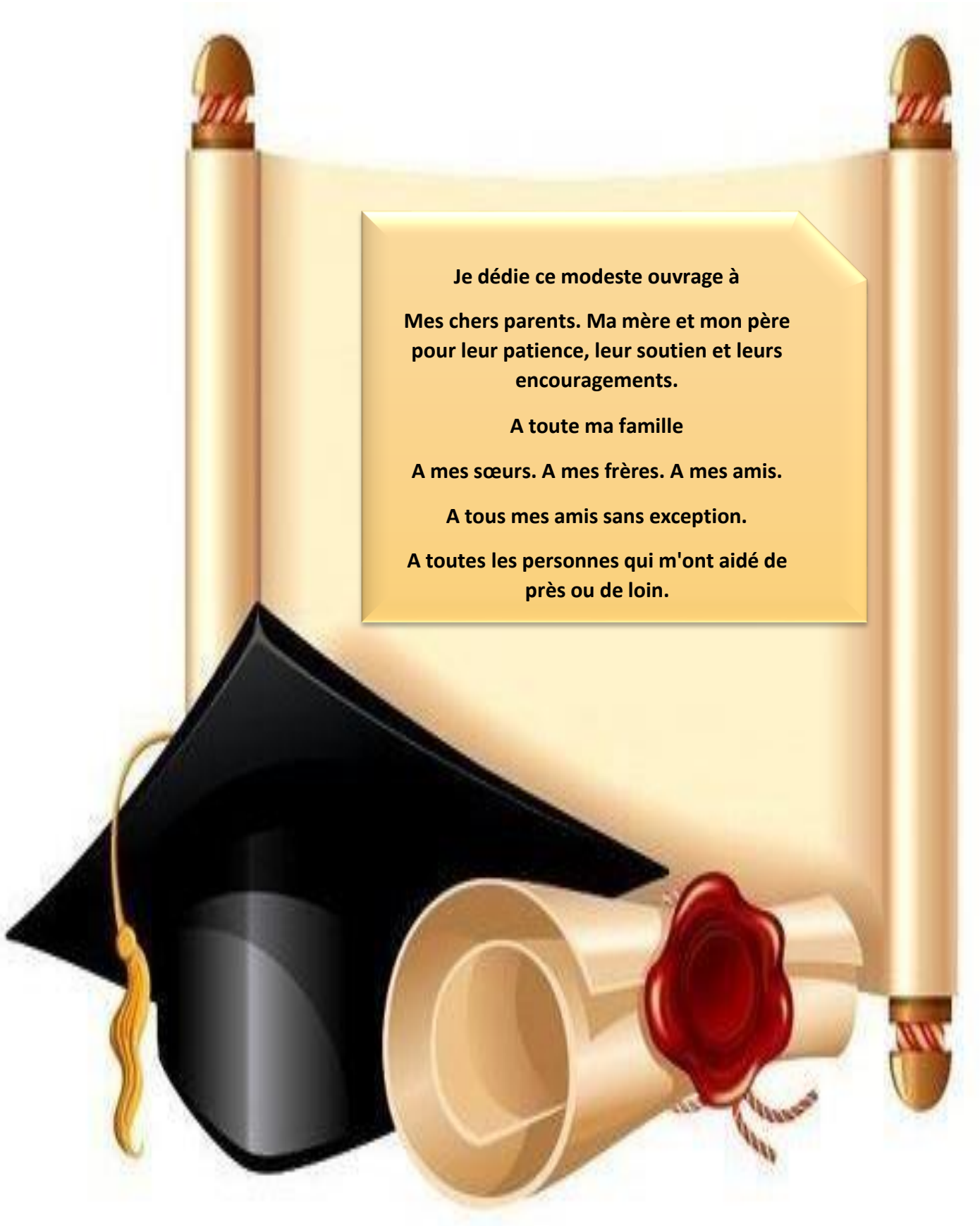
M^r^. Tioura Abdelhamid	**Président**
M^r^	**Promotrice**
M^r^	**Examinatrice**

Promotion : 2022/2023

En préambule à ce travail, nous remercions Dieu qui nous aide et nous donne patience et courage durant ces années d'études. Nous tenons à remercier l'ens. Tioura Abdelhamid pour nous avoir suivi durant le travail sur cette thèse, pour ses précieux conseils, et la compétence de son encadrement.

Nous tenons à exprimer nos sincères remerciements à tous les professeurs qui nous ont enseigné et qui par leur compétence nous ont soutenu dans la poursuite de nos études.

Dédicaces



Je dédie ce modeste ouvrage à

Mes chers parents. Ma mère et mon père pour leur patience, leur soutien et leurs encouragements.

A toute ma famille

A mes sœurs. A mes frères. A mes amis.

A tous mes amis sans exception.

A toutes les personnes qui m'ont aidé de près ou de loin.

Table des matières

Tableau des matières

Tableau des figures

CERT	**C**omputer **E**mergency **R**esponse **T**eam
CIDR	**C**lassless **I**nter-**D**omain **R**outing
CPU	**C**entral **P**rocessing **U**nit
DAQ	**D**ata **A**cquisition
DDoS	**D**istributed **D**enial **o**f **S**ervice
DMZ	**D**e **M**ilitarized **Z**one
DNS	**D**omain **N**ame **S**ervice
DVD	**D**igital **V**ersatile **D**isc
FTP	**F**ile **T**ransfer **P**rotocol
H-IDS	**H**ost **B**ased **I**ntrusions **D**etection **S**ystem
HTTP	**H**yper **T**ext **T**ransfer **P**rotocol
HTTPS	**H**yper **T**ext **T**ransfer **P**rotocol**S**ecure
ICMP	**I**nternet **C**ontrol Message **P**rotocol
IDS	**I**ntrusions **D**etection **S**ystem
IDWG	**I**ntrusions **D**etection exchange format **W**orking **G**roup
IETF	**I**nternet **E**ngineering **T**ask **F**orce
IGRP	**I**nterior **G**ateway **R**outing **P**rotocol
IP	**I**nternet **P**rotocol
IPS	**I**ntrusions **P**revention **S**ystem
IPSec	**I**nternet **P**rotocol **S**ecurity
IPX	**I**nternetwork **P**acket **E**xchange
ISS	**I**nternet **S**ecure **S**ystem
LAN	**L**ocal **A**rea **N**etwork
NFS	**N**etwork **F**ile **S**ystem

N-IDS	**N**etwork **B**ased **I**ntrusions **D**etection **S**ystem
NMAP	**N**etwork **M**ap per
NTP	**N**etwork **T**ime **P**rotocol
OSPF	**O**pen **S**hortest **P**ath First
OSI	**O**pen **S**ystems **I**nterconnection
PHP	**H**ypertext **P**reprocessor
POP3	**P**ost **O**ffice **P**rotocol **V**ersion 3
PSSI	Information Systems Security Policy
RIP	**R**outing **I**nformation **P**rotocol
RPC	**R**emote **P**rocedure **C**all
SI	Information System
SGBD	Database Management System
SSH	**S**ecure **S**hell
SSI	Information Systems Security
SSL	**S**ecure **S**ocket **L**ayer
TCP	**T**ransmission **C**ontrol **P**rotocol
TLS	**T**ransport **L**ayer **S**ecurity
UDP	**U**ser **D**atagram **P**rotocol
URI	**U**niform **R**esource **I**dentifier
URL	**U**niform **R**esource **L**ocator
USB	**U**niversal **S**erial **B**us
VPN	**V**irtual **P**rivate **N**etwork
IOT	**I**nternet **o**f **T**hings
IdO	**I**nternet **D**es **O**bjets
IoT-GS	**I**nternet **o**f **T**hings **G**lobal **S**tandards **I**nitiative

Introduction générale

A. Introduction générale

Au cours de ces dernières années, la technologie des réseaux sans-fil n'a cessé de croître grâce aux développements technologiques dans divers domaines liés à la micro-électronique et aux communications sans-fil.

Après les réseaux pour téléphones mobiles et les réseaux Ad-hoc, la recherche aujourd'hui s'oriente vers les réseaux de capteurs sans-fil.

Les réseaux de capteurs sont un nouveau paradigme des réseaux mobiles.

Ils forment un type particulier des réseaux Ad-Hoc constitués de différentes entités mobiles inconnus et ne reposant sur aucune infrastructure fixe ou un contrôle centralisé, dans lesquels les nœuds sont des capteurs. Dans ce type de réseaux, les capteurs échangent l'information sur l'environnement afin d'établir une vue globale de la région surveillée. Cette information sera, ensuite, délivrée à l'utilisateur externe à travers le nœud passerelle « Sink ».

La propagation et l'acheminement de données dans un réseau de capteurs représentent une fonctionnalité très importante. En effet, la principale fonctionnalité de tels réseaux est l'opération de routage qui doit prendre en considération toutes les caractéristiques du réseau afin d'assurer les meilleures performances du système. Le routage dans les réseaux de capteurs est très différent de celui des réseaux traditionnels.

Dans les réseaux traditionnels, comme l'Internet ou les réseaux cellulaires, ce sont les routeurs dédiés qui prennent en charge de sauvegarder et de transférer les données pour les nœuds terminaux. Tandis que dans les réseaux de capteurs, puisqu'il n'existe pas de routeur dédié, le routage doit être effectué par chacun des nœuds du réseau pour assurer une disponibilité maximale de service de routage.

Ainsi tout nœud est à la fois terminal et routeur, et il doit échanger avec d'autres nœuds non seulement du trafic d'applications, mais aussi des mésanges pour le contrôle du réseau et le routage des données.

A.1 L'objectif de notre travail est:

Étudier les informations générales sur Election d'un leader pour la gestion dynamique et distribué des réseaux de capteurs sans fil et Étudier L'économie d'énergie et tolérance aux pannes dans les RCSF.

Case study:

Le dernier chapitre concerne notre travail.

Chapitre1 : Election d'un leader pour la gestion dynamique et distribué des réseaux de capteurs sans fil

I.1 Introduction :

Les progrès réalisés ces dernières décennies dans les domaines de la microélectronique, de la micromécanique, et des technologies de communication sans fil, ont permis de produire avec un coût raisonnable des composants de quelques millimètres cubes de volume,

Ces derniers, sont appelés nœuds capteurs, intégrant : une unité d'acquisition chargée de collecter des grandeurs physiques (chaleur, humidité, vibrations, etc…) et de les transformer en grandeurs numériques, une unité de traitement informatique et de stockage de données et un module de transmission sans fil. De ce fait, les nœuds capteurs sont de véritables systèmes embarqués.[1]

Le déploiement de plusieurs d' entre eux, en vue de collecter et transmettre des données environnementales vers un ou plusieurs points de collecte, d'une manière autonome, forme un réseau de capteurs sans fil.[1]

I.2 Réseaux de capteurs sans fil

I.2.1 Définition d'un capteur sans fil

Un capteur sans fil est petit dispositif électronique autonome, mis dans un environnement afin de détecter un événement réel (température, humidité, mouvement. . .), puis les transformer en données binaires exploitable par un système informatique.[1]

I.2.2 Architecture d'un capteur sans fil Un capteur sans fil

Les RCSFs sont composés d'objets communicants (Nœuds) intégrés dans une zone d'intérêt, chaque objet communicant comporte 3 :

- Unité d'acquisition
- Unité de traitement
- Unité de contrôle d'énergie
- Unité de transmission

Il peut contenir également, suivant son domaine d'application, des modules supplémentaires tels qu'un système de localisation (GPS), ou bien un système générateur d'énergie (cellule solaire,…). On peut même trouver des capteurs, un peu plus volumineux, dotés d'un système mobilisateur chargé de déplacer le capteur en cas de nécessité. [2]

I.2.3 Caractéristiques de capteurs sans fil

Les capteurs sans fil peuvent varier considérablement, en ce qui concerne la taille, leur coût, la puissance de traitement, les protocoles et les systèmes d'exploitation. Les capteurs sont équipés d'émetteurs-récepteurs de radiofréquence de courte portée pour faciliter la recherche et la récupération des données dans le réseau. Les processeurs utilisés dans ces capteurs peuvent varier d'ultra faible puissance à des processeurs 32bits, de même pour l'espace mémoire qui peut varier de quelques kilooctets à l'ordre de mégaoctets.
[2]

I.3 Réseau de capteur sans fil

Les réseaux de capteur sans fil (RCSF) ou en anglais Wireless Sensor Network (WSN), sont considérés comme un type spécial des réseaux Ad Hoc, ils sont constitués d'un grand nombre de petits nœuds de détection (capteurs) qui jouent à la fois le rôle d'hôte et de routeur. Les nœuds capteurs sont déployés de façon aléatoire sur une zone géographique afin de collecter les données sur leur environnement puis les transmettre à un ou plusieurs puits. La communication sans fil, la topologie dynamique ainsi que l'absence de contrôle centralisé rend les RCSF plus vulnérables et fragile par rapport aux réseaux filaires ou sans fil traditionnel.[3]

I.3.1 Architecture d'un réseau de capteur sans fils

Un RCSF est composé d'un grand nombre de capteur dispersés en densité dans un terrain d'intérêt appelé zone de captage, le nombre de capteurs déployés est déterminé selon la taille de cette zone, la distance entre deux nœuds est en fonction de la puissance de communication. Les capteurs collectent les données puis les transmettent via un routage multi-sauts a un point de collecte appelé puits (en anglais sink) ou station de base, ce dernier transmet ces données à l'utilisateur final. [3]

I.4 Classification des Réseaux Sans Fil

Les réseaux sans fil peuvent avoir une classification selon deux critères. Le premier est la zone de couverture du réseau. Au vu de ce critère il existe quatre catégories : les réseaux personnels, les réseaux locaux, les réseaux métropolitains et les réseaux étendus. Le second critère est celui de l'infrastructure ainsi que le modèle adopté. Par rapport à ce critère on peut diviser les réseaux sans fils en : réseaux avec infrastructures et réseaux sans infrastructure, comme on le voit dans l'illustration de la figure1.1.[3]

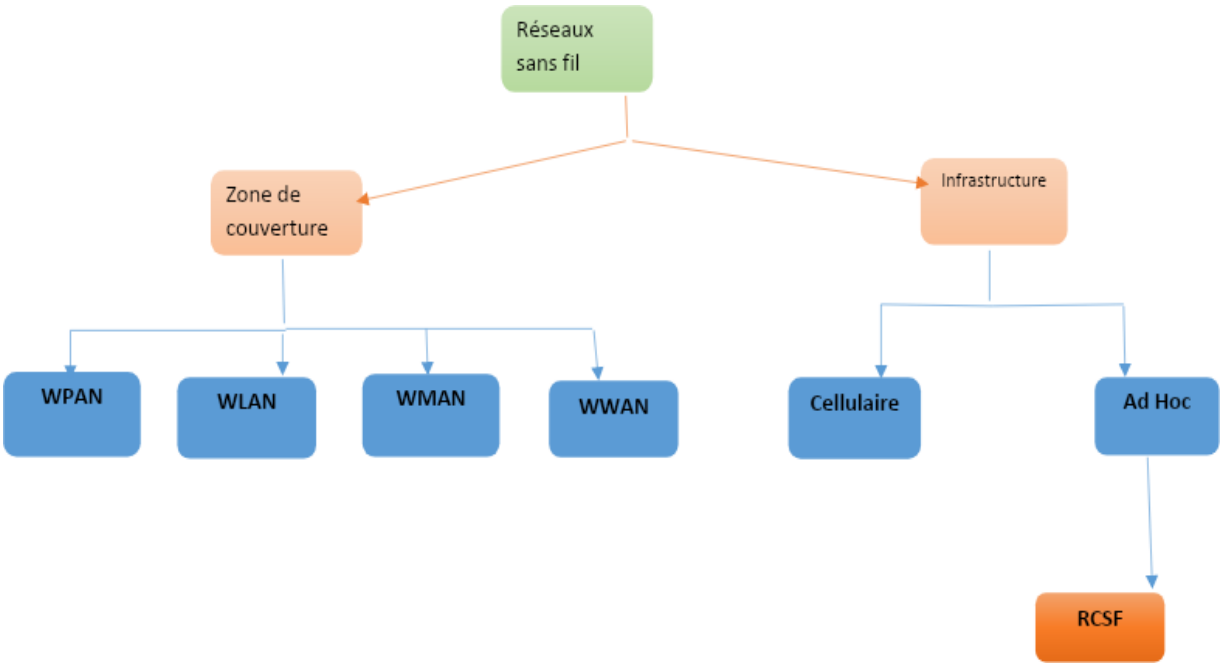


Figure1.1- Classification des Réseaux Sans Fil [4]

1) Classification selon la zone de couverture

La classification des réseaux en fonction de la taille de la zone qu'ils couvrent, donne quatre classes des réseaux qui sont les suivants : WPAN, WLAN, WMAN, WWAN :

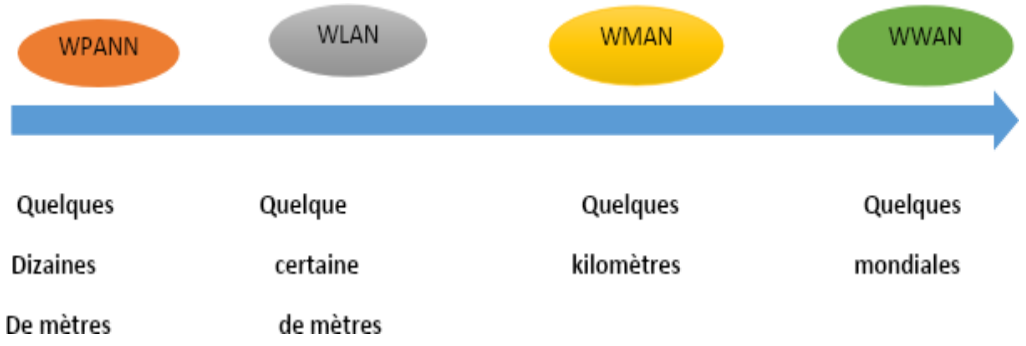


Figure1.2- Classification des réseaux sans fil suivant leur taille.[5]

A. Les WPAN (Wireless Personale Area Networks). Dans cette catégorie, on retrouve les réseaux sans fil à échelle humaine dont la portée maximale est limitée à quelques dizaines de mètres autour de (bureaux, salles de conférence...). Ils sont le plus souvent utilisés à faire communiquer entre eux des matériels présents sur une personne .Ils sont également utilisés pour relier des équipements informatiques entre eux sans liaison filaire.

B. Les WLAN (Wireless Local Area Networks). est la catégorie des réseaux locaux sans fil dont la portée va jusqu à 500 m, pour les applications couvrant un campus, un bâtiment, un aéroport, un hôpital, etc. On y trouve les standards tels que le Wi-Fi (Wireless Fidélité) et les HIPERLAN.

C. Les WMAN (Wireless Métropolitain Area Networks). Plus connus sous le nom de Boucle Locale Radio (BLR), ce type de réseau utilise le même matériel que celui qui est nécessaire pour constituer un WLAN mais peut couvrir une plus grande zone de la taille d'une ville avec une portée pouvant aller jusqu à 50 Km. est dans cette catégorie que on classe le Wi MAX et les HIPERMAN.

D. Les WWAN (Wireless Wide Area Networks).est la catégorie de réseaux cellulaires mobiles dont la zone de couverture est très large, à échelle mondiale. Dans cette catégorie, on peut citer le GSM et ses évolutions (GPRS, EDGE), le CDMA et l'UMTS.

I.5 Domaines d'application des réseaux de capteurs sans fil

Les RCSF peuvent avoir beaucoup d'applications. Parmi elles, nous citons :

1. Applications militaires

Le déploiement rapide, l'auto-configuration et la tolérance aux pannes des de capteurs sont des caractéristiques qui font de ce type de réseaux un outil appréciable dans un tel domaine. Déploiement sur un endroit stratégique ou difficile d'accès, afin de surveiller toutes les activités des forces ennemies ou d'analyser le terrain avant d'envoyer des troupes (par la détection d'agents chimiques, biologiques ou de radiations.

[6]

2. Applications liées à la sécurité

Les altérations dans la structure d'un bâtiment, suite à un séisme ou au vieillissement, pourraient être détectées par des capteurs intégrés dans les murs ou dans le béton, sans alimentation électrique ou autres connexions filaires. Les capteurs doivent s'activer périodiquement et peuvent ainsi fonctionner durant des années, voire des décennies. Un réseau de capteurs de mouvements peut constituer un système d'alarme distribué qui servira à détecter les intrusions sur un large secteur.

3. Applications environnementales

Des thermo-capteurs dispersés à partir d'un avion sur une forêt peuvent signaler un éventuel début d'incendie dans le champ de captage ; ce qui permettra une meilleure efficacité pour la lutte contre les feux de forêt. Dans les champs agricoles, les capteurs peuvent être semés avec les graines. Ainsi, les zones sèches seront facilement identifiées et l'irrigation sera donc plus efficace. Sur les sites industriels, les centrales nucléaires ou dans les pétroliers, des capteurs peuvent être déployés pour détecter des fuites de produits toxiques (gaz, produits chimiques, éléments radioactifs, pétrole,…etc.) et alerter les utilisateurs dans un délai suffisamment court pour permettre une intervention efficace.
Une grande quantité de capteurs peut être déployée en forêt ou dans un environnement de conservation la faune afin de recueillir des informations diverses sur l'état du milieu naturel et sur les comportements de déplacement.

4. Applications médicales

Surveillance permanente des patients et une possibilité de collecter des informations physiologiques de meilleure qualité facilitant ainsi le diagnostic de maladies grâce à des micro-capteurs qui pourront être intègres ou implantes sous la peau.

- Les micros-cameras qui peuvent être ingérées et sont capables, sans avoir recours à la chirurgie, de transmettre des images de l'intérieur d'un corps humain,
- La création d'une rétine2 artificielle composée d'une centaine de micro capteurs pour améliorer la vision de l'œil.
-

5. Applications écologiques

L'intégration de plusieurs micro-capteurs dans le système de climatisation et de chauffage des immeubles. Ainsi, la climatisation ou le chauffage ne sont déclenches qu'aux endroits où il y a des personnes présentes et seulement si c'est nécessaire. Le système distribué peut aussi maintenir une température homogène dans les pièces. Utilisée à grande échelle, une telle application permettrait probablement de réduire la demande mondiale en énergie.

6. Applications de traçabilité et de localisation

Suite à une avalanche il est nécessaire de localiser les victimes enterrées sous la neige en équipant les personnes susceptibles de se trouver dans des zones à risque par des capteurs. Ainsi, les équipes de sauvetage peuvent localiser plus facilement les victimes.
Contrairement aux solutions de traçabilité et de localisation basées sur le système de GPS (Global Positionning System), les réseaux de capteurs peuvent être très utiles dans des endroits clos comme les mines par exemple 2 Organe sensible de la vision.

7. Applications commerciales

Il est possible d'intégrer des nœuds capteurs au processus de stockage et de livraison. Le réseau ainsi formé, pourra être utilisé pour connaître la position, l'état et la direction d'un paquet ou d'une cargaison. Il devient alors possible pour un client qui attend la réception
D'un paquet, d'avoir un avis de livraison en temps réel et de connaître la position actuelle du

paquet. Pour les entreprises manufacturières, les réseaux de capteurs permettront de suivre le procédé de production à partir des matières premières jusqu'au produit final livré.

I.6 Limite des RCSF

Malgré les avantages des RCSF (faible cout, flexibilité, emplacement facile…), les RCSF souffre de plusieurs inconvénients comme la durée de vie limitée à cause des ressources d'énergies restreintes qui l'alimentent comme les piles ou les batteries. Les capteurs sans fil disposent d'une mémoire très petite et ne peuvent stocker qu'une partie des informations collectées. D'autre part le processeur doté ne peut pas effectuer des calculs très grandes communications au sein du réseau peuvent être influencées par les différents obstacles dans le terrain d'intérêt. [7]

I.7 Conclusion

Les réseaux de capteurs sans fil se propagent dans plusieurs domaines d'application. Ils sont devenus indispensables pour les mesures de certaines grandeurs physiques telles que la température, l'humidité, la vibration, etc. ou physiologiques.
Les caractéristiques de flexibilité, de tolérance aux fautes, de fidélité élevée de capture, les coûts bas et la rapidité de déploiement des réseaux de capteurs, créent beaucoup de nouveaux domaines d'application pour la télédétection. Actuellement, cette large étendue d'applications fait que le réseaux de capteurs sont une partie intégrante de notre vie.

Cependant, la réalisation des réseaux de capteurs doit effectivement satisfaire des contraintes telles que la tolérance aux fautes, la SCA labilité, le coût, le matériel, le changement de topologie, l'environnement et la consommation efficace d'énergie.

Chapitre2 : L'économie d'énergie et tolérance aux pannes dans les RCSF

II.1 Introduction

La limitation d'énergie dans les capteurs sans fil, et les environnements hostiles dans lesquels ils pourraient être déployés, sont des facteurs qui rendent ce type de réseaux très vulnérables. Ainsi, la perte de connexions sans fils peut être due à une extinction d'un capteur suite à un épuisement de sa batterie, ou tout simplement à une destruction physique accidentelle ou intentionnelle par un ennemi. Par ailleurs, l'absence de sécurité physique pour ce type de capteurs, et la nature vulnérable des communications radios sont des caractéristiques qui augmentent les risques de pannes sur ce type de réseau. [8]

II.2 Définition

Certains nSuds capteurs peuvent être bloqués ou tomber en panne à cause d'un manque d'énergie, d'un dégât matériel ou d'une interférence environnementale. La panne d'un nSud capteur ne doit pas affecter le fonctionnement global de son réseau. C'est le problème de fiabilité ou de tolérance aux pannes. La tolérance aux pannes est donc la capacité de maintenir les fonctionnalités du réseau sans interruption due à une panne d'un nSud capteur.[9]

- **Détection d'erreur**

C'est la première phase dans chaque schéma de tolérance aux pannes, dans laquelle on reconnaît qu'un événement inattendu s'est produit. Les techniques de détection de pannes sont généralement classifiées en deux catégories : en ligne et autonome (offline). La détection offline est souvent réalisée à l'aide de programmes de diagnostic qui s'exécutent quand le système est inactif. La détection en ligne vise l'identification de pannes en temps réel et est effectuée simultanément avec l'activité du système.

- **Détention de la panne**

Cette phase établit des limites des effets de la panne sur une zone particulière afin d'empêcher la contamination des autres régions. En cas de détection d'intrusion, par exemple, l'isolation des composants compromis minimise le risque d'attaque des composants encore fonctionnels.

- **Recouvrement d'erreur**

C'est la phase dans laquelle on effectue des opérations d'élimination des effets de pannes. Les deux techniques les plus utilisées sont « masquage de panne » et « répétition »

- Masquage de panne : utilise l'information redondante correcte pour éliminer l'impact de l'information erronée ;
- Répétition : après que la panne soit détectée, on effectue un nouvel essai pour exécuter une partie du programme, dans l'espoir que la panne soit transitoire.

- **Traitement de panne**

Dans cette phase, la réparation du composant en panne isolé est effectuée. La procédure de réparation dépend du type de la panne. Les pannes permanentes exigent une substitution du composant avec un autre composant fonctionnel. Le système doit contenir un ensemble d'éléments redondants (ou en état standby) qui servent à remplacer les nSuds en panne.

II.3 Classification des solutions

Les protocoles tolérants aux pannes peuvent être vus de plusieurs angles différents. De ce fait, un ensemble de critères est défini pour les classifier. Nous citons, entre autre, des catégories de trois classifications distinctes. [10]

II.3.1 Classification selon la phase de traitement

Dans cette classification, nous divisons l'ensemble des algorithmes en deux principales catégories. Si le traitement est effectué avant la panne ; on parle donc d'algorithmes préventifs sinon, les algorithmes sont dits curatifs.

- **Algorithme préventif** : implémente des techniques tolérantes aux pannes qui tentent de retarder ou éviter tout type d'erreur afin de garder le réseau fonctionnel le plus longtemps possible. La conservation d'énergie à titre d'exemple, permet de consommer moins d'énergie et évite donc une extinction prématurée de la batterie ce qui augmente la durée de vie des nSuds ;
- **Algorithme curatif** : utilise une approche optimiste, où le mécanisme de tolérance aux pannes implémenté n'est exécuté qu'après la détection de pannes. Pour cela, plusieurs algorithmes de recouvrement après pannes sont proposés dans la littérature, par exemple : le recouvrement du chemin de routage, l'élection d'un nouvel agrégateur...etc.

II.3.2 Classification architecturale

Cette classification traite les différents types de gestion des composants, soit au niveau du capteur individuellement ou bien sur tout le réseau. Nous distinguons trois catégories principales :

- **Gestion de la batterie** : cette catégorie est considérée comme une approche préventive, où les protocoles définissent une distribution uniforme pour la dissipation d'énergie entre les différents nSuds capteurs ; afin de mieux gérer la consommation d'énergie et augmenter ainsi la durée de vie de tout le réseau. En outre, le mécanisme de mise en veille est une technique de gestion de batterie. En effet, les protocoles déterminent des délais de mise en veille des nSuds capteurs inactifs pour une meilleure conservation d'énergie ;
- **Gestion de flux** : cette catégorie regroupe les techniques qui définissent des protocoles de gestion de transfert des données (routage, sélection de canal de transmission...etc.). nous pouvons trouver des approches préventives ou curatives sur les différentes couches (réseau, liaison de données...etc.) telles que :
  - **Routage multi-chemin** : utilise un algorithme préventif pour déterminer plusieurs chemins depuis chaque capteur vers le nSud collecteur. Ceci garantit la présence de plus d'un chemin fiable pour la transmission et offre une reprise rapide du transfert en cas de panne sur le premier chemin sélectionné (choisir un des chemins qui restent);
  - **Recouvrement de route** : après détection de panne, une technique curative permet de créer un nouveau chemin qui soit le plus fiable pour retransmettre les données ;
  - **Allocation de canal** : cette solution, implémentée au niveau MAC, effectue une allocation du canal de transmission d'une manière à diminuer les interférences entre les nSuds voisins et éviter les collisions durant le transfert ;
  - **Mobilité** : certains protocoles proposent comme solution tolérante aux pannes la sélection d'un ensemble de nSuds mobiles chargés de se déplacer entre les capteurs et

collecter les données captées. Ceci réduira l'énergie consommée au niveau de chaque capteur en éliminant sa tâche de transmission. Un nSud mobile est généralement doté d'une batterie plus importante que celle d'un nSud capteur.

- **Gestion des données** : les protocoles classés dans cette catégorie offrent une meilleure gestion de données et de leur traitement. Deux principales sous-catégories sont déterminées :
  - **Agrégation** : considérée comme approche préventive, l'opération d'agrégation effectue un traitement supplémentaire sur les données brutes captées depuis l'environnement. Un nSud agrégateur combine les données provenant de plusieurs nSuds en une information significative ; ce qui réduit considérablement la quantité de données transmises, demande moins d'énergie et augmente ainsi la durée de vie du réseau ;
  - **Clustering** : une des importantes approches pour traiter la structure d'un réseau de capteurs est le clustering. Il permet la formation d'un backbone virtuel qui améliore l'utilisation des ressources rares telles que la bande passante et l'énergie. Par ailleurs, le clustering aide à réaliser du multiplexage entre différents clusters. En outre, il améliore les performances des algorithmes de routage. Plusieurs protocoles utilisent cette approche préventive (parfois considérée comme approche curative) qui sera détaillée plus tard.

II.3.3 Classification selon le niveau d'implémentation

Cette classification permet de répartir les protocoles sur les différentes couches de l'architecture des réseaux de capteurs. Ainsi, les algorithmes de routage sont au niveau réseau, les techniques de sélection de canal sur la couche MAC...etc.

II.4 Solutions de routage tolérantes aux pannes

Les protocoles de routage permettent de choisir les meilleurs chemins pour acheminer la donnée depuis la source vers l'utilisateur final. Par ailleurs, ils permettent de sélectionner un chemin de remplacement en cas d'échec d'envoi sur la route initiale ; à cause d'une panne au niveau d'un ou plusieurs nSuds de cette route**. [10]**

- **Aperçus**

La motivation de cet algorithme vient du besoin de fournir un support pour toutes les contraintes : faible latence, fiabilité, recouvrement rapide en cas de panne et conservation d'énergie. PEQ combine la conservation d'énergie avec le routage multi-chemins en sélectionnant parmi toutes les routes disponibles, celles qui consomment moins d'énergie. En plus de ce mécanisme préventif qui permet un routage fiable, un mécanisme de recouvrement de pannes est implémenté. Ce dernier remplace le chemin en panne par une autre route qui soit de liens fiables et consomme moins d'énergie. Ainsi, le protocole PEQ couvre la procédure de tolérance aux pannes par la gestion de la consommation d'énergie, la sélection des meilleures routes puis leur recouvrement en cas de panne**. [11]**

II.5 PEQ : Periodic, Event-driven, Query-based

II.5.1 Publish/subscribe

PEQ introduit le paradigme Publish/Subscribe (voir figure suivante) pour l'interaction entre le collecteur et les nSuds capteurs. En effet, les capteurs envoient des notifications d'événements au

collecteur, qui va souscrire son intérêt pour certaines de ces informations. Les capteurs concernés publient par la suite l'information désirée.

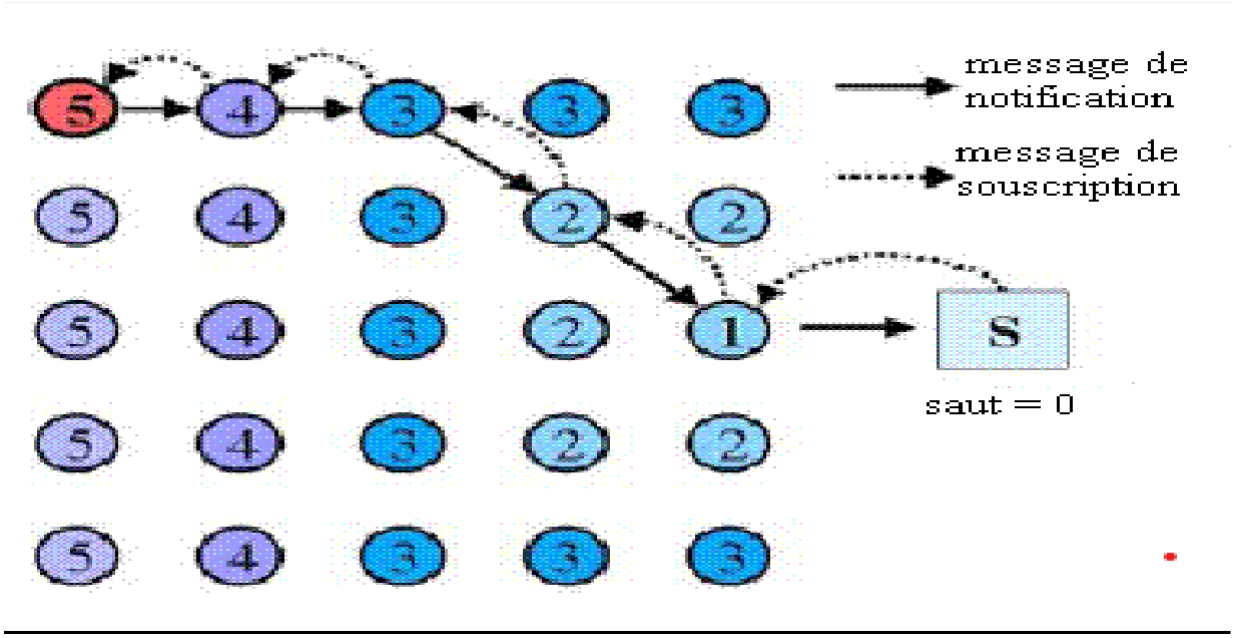


Figure2.1- Le paradigme Publish/Subscribe[

Les quatre principales phases du protocole sont : [12]

1. **Construction de l'arbre de routage** : cet arbre permet de définir les différents chemins multi-sauts possibles pour acheminer les données. Le collecteur commence le processus en initialisant la variable « saut » à 0 ; par la suite, chaque nSud capteur prend la valeur du saut actuelle, l'incrémente puis l'envoie à tous ses voisins. Ainsi la valeur au niveau de chaque capteur désigne le nombre nécessaire de sauts pour communiquer avec le collecteur. A la fin de cette phase seulement les meilleurs chemins sont enregistrés ;
2. **Transmission de paquets de notification** : chaque nSud capteur envoie selon sa table de routage et l'événement capté, une notification de l'information qu'il a. Pour cela, il utilise le chemin le plus rapide et le moins coûteux en terme d'énergie ;
3. **Propagation des paquets de souscription** : dans cette étape, après une souscription, par le collecteur, des données à transmettre, chaque nSud achemine cette dernière jusqu'au nSud capteur concerné ;
4. **Mécanisme de recouvrement de route** : le recouvrement est effectué après détection de pannes (voir figure suivante). Un nSud envoie son paquet puis attend un acquittement ACK. S'il est reçu, le message a été bien transmis ; sinon une panne est détectée au niveau du chemin de routage. On effectue donc une recherche "SEARCH" pour la sélection d'un autre nSud destination tout en minimisant le coût du nouveau chemin. Si aucun nSud n'est trouvé (tous les voisins sont détruits) le nSud devient isolé et doit donc augmenter son rayon de transmission radio pour atteindre les nSuds voisins lointains.

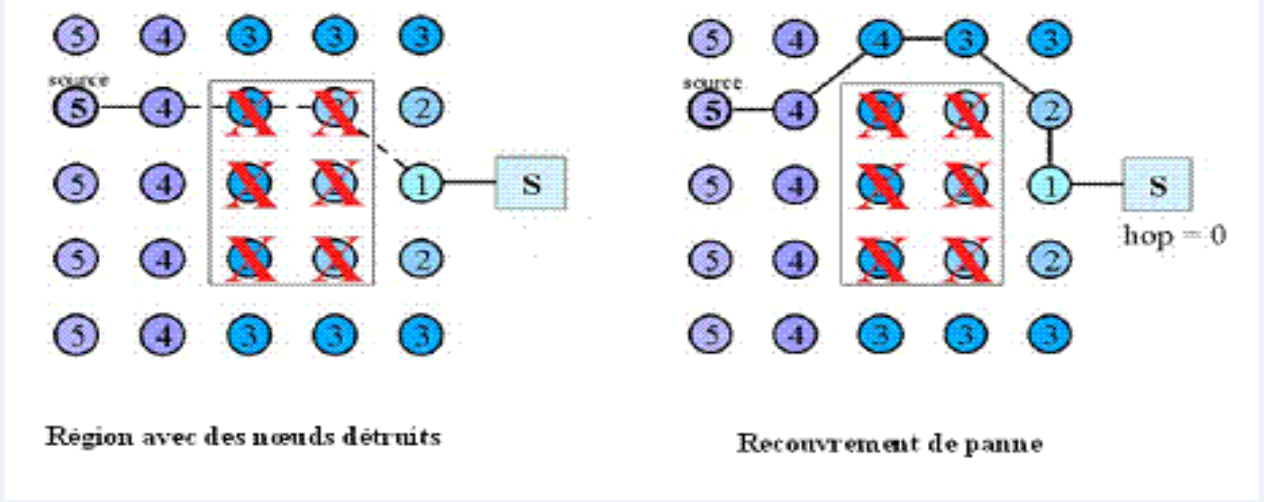


Figure2.2- Mécanisme de recouvrement de route [13]

II.5.3 Protocole EAR [13]

Une solution hybride pour la tolérance aux pannes est proposée dans le protocole EAR. Pour son concept préventif, EAR offre une meilleure conservation d'énergie et définit plusieurs chemins de routage afin de garantir une fiabilité du transport et d'augmenter la durée de vie du réseau. En outre, un mécanisme de recouvrement de pannes est implémenté. Le protocole EAR supporte des réseaux de capteurs à collecteurs multiples (plusieurs nSuds puits). Chaque nSud capteur génère un paquet RPT (Report) contenant des informations pour les intérêts et préférences de l'utilisateur. Les paquets RPT peuvent être envoyés vers n'importe quel collecteur. Cependant, pour chaque nSud intermédiaire le protocole de routage choisit le meilleur chemin qui réduit la consommation d'énergie et la latence.

II.5.3 Phase d'initialisation

Cette phase permet la construction de l'arbre de routage contenant tous les chemins possibles pour la dissémination des données. Chaque collecteur diffuse un message ADV (Advertisement) demandant des paquets RPT. Seuls les nSuds voisins du collecteur reçoivent le message ADV puis enregistrent le chemin dans leur table de routage ; sans propager le message ADV vers les autres nSuds, comme le montrent les étapes a) et b) de la figure suivante. Les autres nSuds capteurs envoient une demande RREQ (Route Request) cherchant un chemin vers le collecteur (d'étape c). Si un nSud, ayant déjà une route stockée dans sa table, reçoit RREQ, il envoie un paquet RREP (Route Reply) à son nSud voisin concerné par la demande (d'étapes). Le processus d'initialisation se termine quand chaque nSud reçoit une réponse RREP suite à sa requête RREQ ; puis enregistre le chemin dans sa table de routage ;

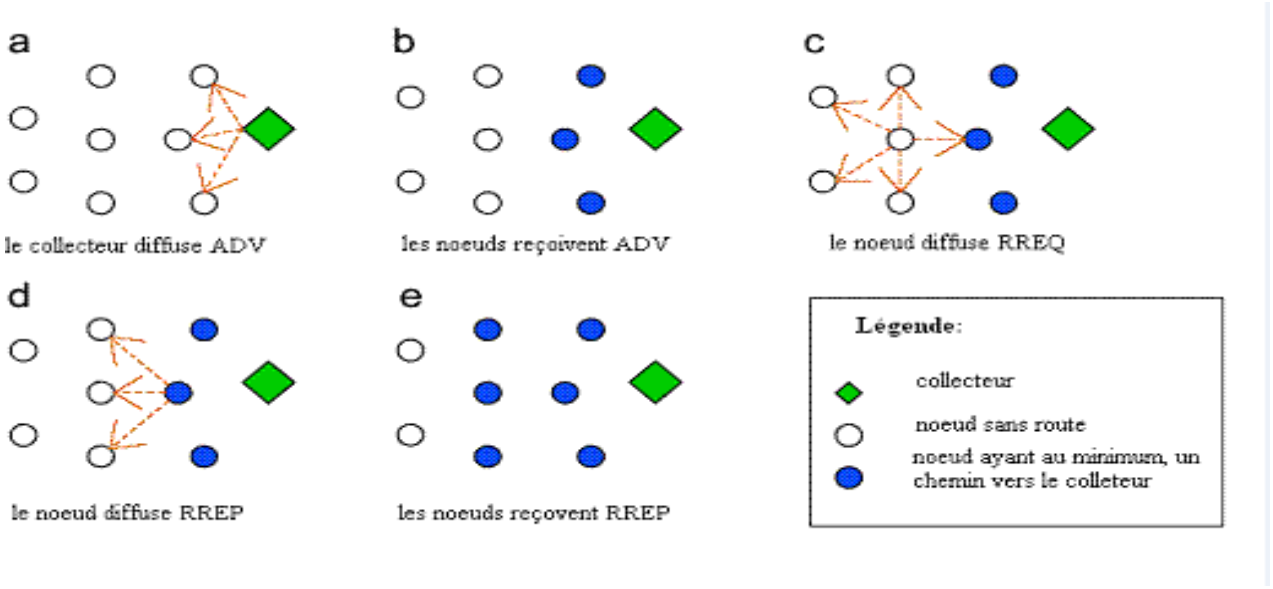


Figure2.3- Phase d'initialisation

II.5.4 VTRP (Variable Transmission Range Protocol)

VTRP est une solution de variation du rayon de transmission pour une meilleure propagation de données. Il permet de remédier au problème d'obstacles en les évitant par l'augmentation du rayon de transmission. Ce dernier augmente la probabilité d'atteindre des nSuds actifs quand le rayon actuel utilisé ne couvre aucun nSud à cause de pannes ou d'inactivité des nSuds voisins ou encore dans le cas des réseaux à faible densité. En outre, VTRP offre une meilleure longévité du réseau en évitant l'utilisation fréquente des nSuds critiques (les voisins proches du collecteur) ceci permet d'alléger leur fonction de routage ; conserve leur batterie et augmente ainsi la durée de vie de tout le réseau.

VTRP utilise des rayons de transmissions variés pour la propagation de données ; i.e. il permet d'augmenter les rayons de transmissions de différentes manières. Soit k nSuds avec k informations. Le problème posé dans cette étude est donc « comment acheminer toutes les k informations au collecteur d'une manière fiable et efficace ».

- **Phase de recherche**

Soit p' un nSud qui a reçu une information E de p. dans la phase de recherche, p' utilise une diffusion périodique de message afin de découvrir le noeud p le plus proche du collecteur (meilleur chemin de p' vers le collecteur en passant par p). Cependant, Une détection de panne est possible si aucun noeud p n'est trouvé. Trois différentes raisons sont possibles pour un tel échec : soit le noeud p est mis en veille et ne peut donc répondre à p'; soit il est en panne (détruit, batterie épuisée...etc.) ou bien à cause d'un obstacle qui empêche la communication entre les deux nSuds ;

- **Phase de transmission directe**

En cas où la phase de recherche réussit, p' envoie l'information à p et envoie un message « succès » à p ;

- **Phase de variation du rayon de transmission**

Si la phase de recherche échoue (aucun noeud p n'est détecté) p' passe à la phase de variation de son rayon de transmission qui représente le cas de recouvrement après pannes. En effet, chaque nSud

maintient un compteur local ³ initialisé à 0. A chaque échec de l'étape de recherche, le compteur est incrémenté, et le rayon de transmission R est modifié selon la valeur de ³. Quatre différentes fonctions sont définies selon la vitesse de variation du rayon de transmission : linéaire, multiplicative, exponentielle et aléatoire ;

1. **Progrès constant :** VTRP est convenable dans ce cas aux réseaux où un large nombre de nSuds est compromis ;
2. **Progrès multiplicatif :** VTRPm définit un rayon de transmission qui est augmenté d'une manière radicale. Ce changement offre une meilleure probabilité pour trouver des nSuds actifs. En revanche, il requiert une consommation d'énergie plus importante ;
3. **Progrès exponentiel :** VTRPp est une variante qui augmente le rayon d'une vitesse encore plus rapide ;
4. **Progrès aléatoire :** quand la densité du réseau n'est pas connue au préalable, on utilise l'approche aléatoire VTRPr pour éviter un mauvais comportement du réseau suite à un mauvais choix.

Chapitre3 : Protocole par la gestion dynamique de RCSF Leach vs Pegasis

III. Introduction

Dans ce chapitre, on présente deux protocoles les plus importants dans la littérature des réseaux de capteurs sans fils (RCSF) qui permettent la gestion dynamique de la communication entre les nouds du réseau ; Le premier est le protocole LEACH, qui permet d'établir une hiérarchie entre les nouds du réseau.

Le deuxième est le protocole Pegsise, basé sur les chaînes ; son idée de base est de prolonger la durée de vie du réseau où les nœuds seront organisés de telle sorte ils forment une chaîne.

Une comparaison des deux protocoles est site à travers l'illustration des avantages et des inconvignieants des deux protocoles.

III.1 Protocoles d'agrégation dans les réseaux de capteurs sans fils

Les différentes techniques d'agrégation de données dans les réseaux de capteurs sont classées en deux approches, comme illustré à la figue suivante (Fig 3.1): [14]

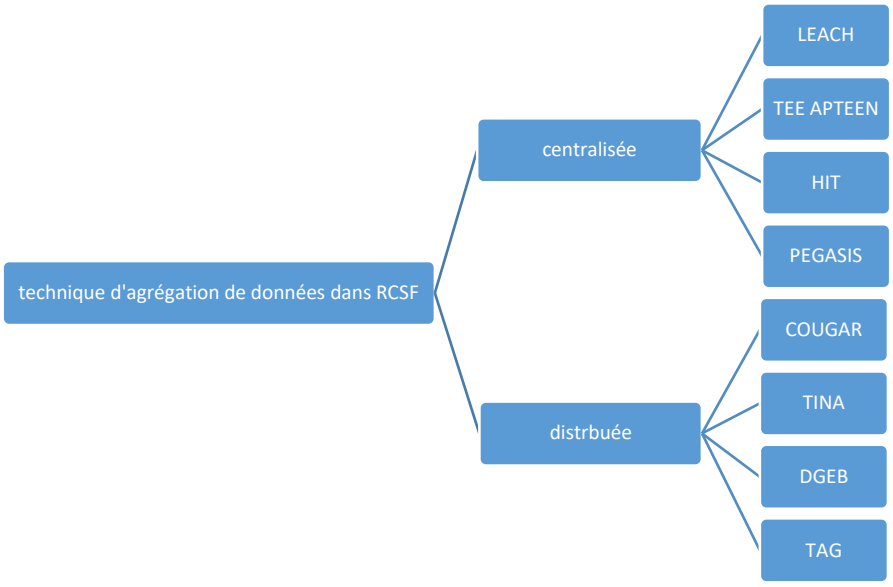


Figure3.1- Protocoles d'agrégation dans les réseaux de capteurs sans fils

La performance des différents protocoles de routage et de gestion des Rcsfs est mesurée selon plusieurs critères qui sont

III.2 Critères de performance des protocoles de routage dans les RCSF

La spécificité des RCSF a permis d'instaurer des critères de performances bien particuliers pour les protocoles de routage conçus à ce type de réseaux. Parmi ces critères, nous citons :

- **Évolutivité:** l'évolutivité est un facteur important dans les RCSF. Une zone de réseau n'est pas toujours statique, elle change selon les besoins des utilisateurs ou à cause de l'occurrence des pannes. A cet effet, tous les nœuds dans le domaine du réseau doivent être en mesure de s'adapter aux changements de la topologie.
- **L'énergie:** Les capteurs présentent une autonomie d'énergie et les batteries dont ils disposent sont rarement rechargeables et remplaçables.

- **Le temps de traitement : il** se réfère au temps pris par le nœud dans le réseau pour assurer l'ensemble des opérations commençant par la détection, le traitement des données, leur stockage, leur transmission ou leur réception sur le réseau. En outre, l'information devrait y arriver au poste de contrôle dans une durée raisonnable en particulier pour les applications orientées événement.
- **Le schéma de transmission**
- **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 entre eux. Pour cela, un nœud doit savoir gérer son temps de veille en tenant compte des périodes de veille de ses voisins.
  – Overhead: Avant l'établissement des routes, les capteurs échangent des paquets de contrôle.De ce fait, un protocole de routage performant doit minimiser son overhead. En outre, lors de l'échange de données, on assiste à éviter les collisions pour minimiser les envois multiples.
  – Fiabilité de livraison : la plupart des protocoles de routage ont été conçus dans un environnement idéal. Néanmoins, la présence des obstacles pour y avoir un impact négatif sur la qualité des messages reçus. De ce fait, il est recommandé de prendre en considération la qualité des liens avant toute communication et le type d'environnement dans lequel ces capteurs sont déployés.

III.2.1 Données centrées :

a. Protocoles hiérarchiques : [15]

1. **LEACH** : LEACH est l'une des premières approches de routage hiérarchique pour les RCSF. L'idée proposée dans LEACH a été une source d'inspiration pour de nombreux protocoles de routage hiérarchiques, bien que certains protocoles ont été développés indépendamment. Dans ce qui suit, nous explorons les principaux protocoles de routage hiérarchiques dédiés aux RCSF.

1.1.Présentation du protocole LEACH : [16]

Un nœud est mis en cluster pour la session réelle si le nombre créé est inférieur au seuil suivant :

Où p est le pourcentage de sommets groupés, c'est la période de temps, et il n'y a pas de nœuds sans sommets groupés dans la dernière période 1/p.

Le protocole se déroule en rondes. Chaque tour se compose de deux phases : construction et connexion.

1.1.1 Phase de construction : Le but de cette phase est la construction des clusters en choisissant les chefs et en établissant la politique d'accès au média au sein de chaque groupe. Cette phase commence par la prise de décision locale pour devenir cluster-head. Chaque noeud n choisit un nombre aléatoire, si ce nombre est inférieur à une valeur T (n), le noeud devient cluster-head. T (n) est définie comme suit :

$$T(n)=\begin{cases}\frac{p}{1-p\times(r mod)} & \text{si } n\epsilon G \\ 0 & \text{sinon}\end{cases}$$

Avec :

- **P :** pourcentage désiré de cluster-heads pendant un round.
- **r :** numéro du round.
- **G :** l'ensemble des noeuds qui n'ont pas été élu cluster-heads pendant les 1/P rounds précédents. Par la suite, chaque noeud qui s'est élu cluster-head émet un message de notification. Les noeuds membres récoltent les messages de notification, et décident leur appartenance à un cluster. La décision est basée sur l'amplitude du signal reçu : le cluster-head ayant le signal le plus fort est choisi (i.e. le plus proche). En cas d'égalité, un chef aléatoire est choisi. Chaque membre informe son chef de sa décision. Toutes les communications précédentes étant faite dans une topologie plate, la méthode CSMA doit être employée. Par la suite, les communications au sein d'un cluster peuvent être faites avec la méthode TDMA. Pour cela, chaque chef établie un schedule TDMA pour ses membres, en indiquant pour chaque noeud son slot d'émission. Ce schedule est envoyé aux membres.

1.1.2 Phase de communication

En utilisant le Schedule TDMA, les membres émettent leurs données captées pendant leurs propres slots. Cela leur permet d'éteindre leur interface de communication en dehors de leurs slots réservés, afin d'économiser leur énergie. Ces informations sont ensuite agrégées, pour être transmises au collecteur (sink). Cette communication, entre un cluster-head et le collecteur, se fait d'une manière directe, i.e. : le cluster-head adapte son émetteur radio afin d'atteindre directement le collecteur. [17]

1.2.Avantages et inconvénients de LEACH

Bien que LEACH puisse augmenter la durée de vie du réseau en manipulant ses

Ressources tout en respectant plusieurs contraintes telle que la consommation d'énergie, il

Présente certaines limitations. Dans ce qui suit, nous citons quelques avantages et

Inconvénients du protocole LEACH.

1.2.1. <u>Avantages</u>

Le protocole LEACH présente les avantages suivants :

- Algorithme distribué : l'auto-configuration des clusters se fait indépendamment dela BS.
- Rotation des rôles de chefs de groupes : les CHs sont choisis de façon aléatoire et périodique parmi les nœuds formant le cluster ce qui empêche la forte consommation d'énergie pour la transmission des données.

- Faible énergie pour l'accès au média : Le mécanisme de groupes permet aux nœuds d'effectuer des communications sur des petites distances avec leurs CHs afin d'optimiser l'utilisation du média de communication en la faisant gérer localement par un CH pour minimiser les interférences et les collisions.
- Agrégations des données : Les CHs compressent les données arrivant de leurs membres, et envoient un paquet d'agrégation au nœud puits afin de réduire la quantité d'informations qui doit lui être transmise. Cela permet de réduire la complexité des algorithmes de routage, de simplifier la gestion du réseau, d'optimiser les dépenses d'énergie et enfin de rendre le réseau plus évolutif

1.2.2. Inconvénients

- Absence des CHs: On pourra ne pas avoir des CHs durant un round si les nombres Aléatoires générés par tous les nœuds du réseau sont supérieurs à la probabilité Pi(t).
- La distance entre le CH et les autres nœuds : Les nœuds les plus éloignés du CH meurent rapidement par rapport aux plus proches.
- Diminution de l'énergie des nœuds : cette diminution est due à l'utilisation d'une communication à un seul saut au lieu d'une communication multi-sauts.
- La rotation des CHs : c'est une méthode qui n'est pas efficace pour de grandes structures de réseaux à cause de la surcharge d'annonces engendrées par le changement des CHs, et qui réduit le gain d'énergie initial.
- La sécurisation : le protocole LEACH n'est pas sécurisé. Aucun mécanisme de sécurité n'est intégré dans ce protocole. Ainsi, il est très vulnérable même aux simples attaques. Donc, un attaquant peut facilement monopoliser le réseau et induit à son disfonctionnement

III.2.2 Le protocole de routage PEGASIS

Le protocole PEGASIS, proposé par Lindsey et Raghavendra en 2002, est un protocole basé sur les chaînes. L'idée de base du protocole est que, dans le but de prolonger la durée de vie du réseau, les nœuds vont être organisés de telle sorte à ce qu'ils forment une chaîne, n'auront ainsi besoin de communiquer qu'avec seulement leurs voisins les plus proches. Pour localiser le voisin le plus proche, chaque nœud utilise la force du signal pour mesurer la distance vers tous les nœuds voisins, et ajuster par la suite la force du signal de telle sorte que seul un nœud peut être entendu. La forme agréée des données sera envoyée à la BS par n'importe quel nœud dans la chaîne et les nœuds dans cette dernière vont se prendre en relais dans la transmission à la BS. [18]

1. La construction des chaînes

Les nœuds vont être organisés de sorte qu'ils forment une chaîne, qui peut être soit calculée d'une façon centralisée par la BS et émise à tous les nœuds, ou accomplie par les nœuds capteurs eux-mêmes en employant un algorithme avide (greedy algorithme). Si la chaîne est calculée par les nœuds capteurs, ils peuvent d'abord obtenir toutes les données sur l'emplacement des nœuds capteurs et calculent localement la chaîne en utilisant le même algorithme avide. Puisque tous les nœuds ont les mêmes données d'emplacement et

exécutent le même algorithme, ils vont tous produire le même résultat. Pour construire la chaîne, PEGASIS commence avec le nœud le plus éloigné de la BS. Le voisin le plus proche de ce nœud sera le nœud suivant dans la chaîne. [19]

Les voisins successifs sont sélectionnés de cette manière parmi les nœuds non visités afin de former la chaîne de nœuds. L'algorithme commence par le nœud le plus lointain pour s'assurer que les nœuds les plus loin de la BS ont des voisins proches à mesure que, dans l'algorithme avide, les distances voisines augmenteront graduellement puisque des nœuds déjà présents sur la chaîne ne peuvent pas être revisités. La figure III.4 montre la construction de chaîne en utilisant l'algorithme avide où le nœud n0 se joint au nœud n1 qui se joint à son tour au nœud n2, et le nœud n2 se joint au nœud n3. Quand un nœud meurt, la chaîne est reconstruite de la même manière pour dévier le nœud Mort

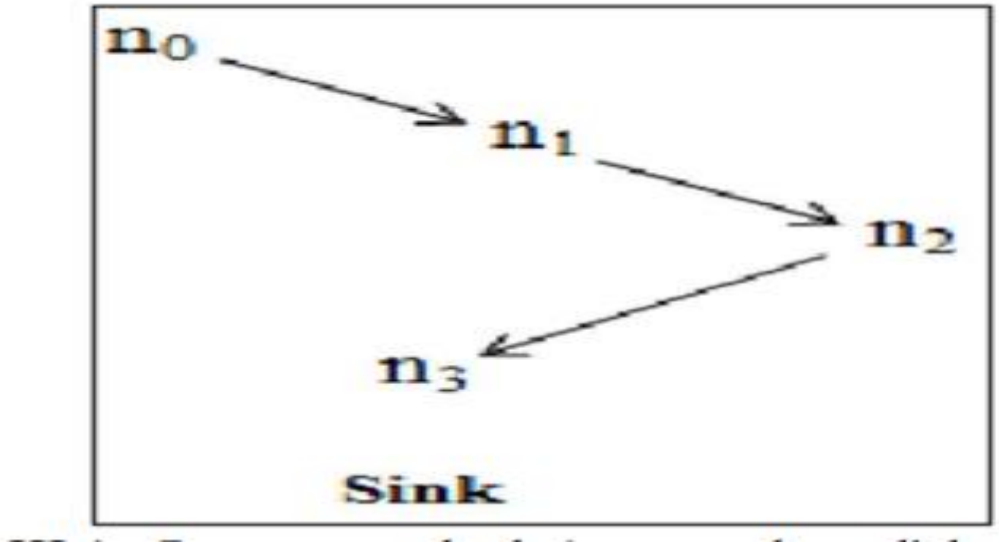


Figure3.3- La construction des chaînes

2. Déroulement de l'algorithme

Pour collecter les données des nœuds capteurs dans chaque cycle, chaque nœud reçoit les données d'un voisin, les fusionne avec les siennes, et transmet à un autre voisin dans la chaîne. À noter que ce nœud, noté i, serait à une position aléatoire sur la chaîne que nous l'appelons j. Les nœuds se relient dans la transmission à la BS et PEGASIS va utiliser le nombre i mode N sachant que N représente le nombre de nœuds afin de transmettre à la BS dans le cycle i. Ainsi, le leader dans chaque cycle de communication sera à une position aléatoire sur la chaîne.[20]

Chaque cycle de collecte de données peut être lancé par la BS avec un signal de balise qui synchronisera tous les nœuds capteurs. Puisque tous les nœuds connaissent leurs positions sur la chaîne, PEGASIS peut employer une approche de slot de temps, TDMA, pour la transmission des données. Dans le ième cycle de collecte de données, le nœud (i-1) sera leader.

Le nœud n0 transmettra ses données au nœud n1 dans le premier slot, n1 fusionne et transmet les données dans le deuxième slot, et ainsi de suite jusqu'à ce que le nœud leader soit atteint. Dans les slots suivants, les transmissions de données ont lieu depuis le nœud nn-

1 et se déplacent vers le nœud leader de l'extrémité de la chaîne. Finalement, dans le nième slot, le leader transmet les données à la BS

Alternativement, dans un cycle donné, PEGASIS peut utiliser une approche de déplacement de jeton à contrôle simple lancée par le leader pour commencer la transmission des données des extrémités de la chaîne. Le coût est très petit du fait que la taille du jeton est très petite. Montre un exemple de déplacement de jeton. Le nœud n2 est le leader et va passer le jeton le long de la chaîne commençant au nœud n0. Le nœud n0 passera ses données au nœud n2. Après que le nœud n2 ait reçu les données du nœud n1, il passera le jeton au nœud n4, et le nœud n4 passera ses données au nœud n2 avec fusion des données le long de la chaîne

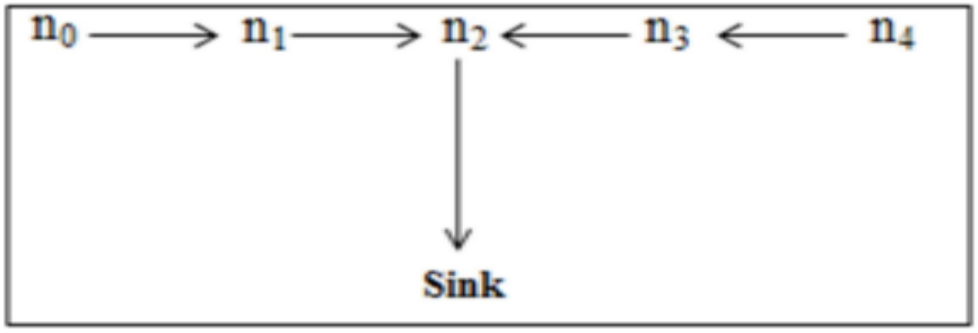


Figure3.4-Déroulement de l'algorithme

PEGASIS exécute la fusion de données à chaque nœud excepté les nœuds de fin de chaîne. Chaque nœud va fusionner les données de ses voisins avec les siennes afin de générer un paquet simple et les transmet par la suite à son autre voisin (s'il en a deux). Dans l'exemple précédent, Le nœud n0 transfère ses données au nœud n1, qui agrège ses propres données avec celles du nœud n0, puis les communique au nœud leader n2. Le nœud n2 passe le jeton au nœud n4 qui transmet ses données au nœud n3. Ce dernier agrège éventuellement ses données avec celles du nœud n4 et les transmet à son tour au nœud n2, qui attend pour recevoir des données de ses voisins et puis les agrège avec ses propres données et transmet un message unique à la BS. Ainsi, dans PEGASIS, chaque nœud va recevoir et transmettre un paquet de données dans chaque cycle et sera le leader une fois chaque N cycles. En addition, les nœuds reçoivent et transmettent des paquets de contrôle de jeton très petits. [20]

3. Avantages et inconvénients du protocole PEGASIS

Bien que le protocole PEGASIS engendre beaucoup d'avantages en ce qu'il offre comme bonne manipulation de ressources du réseau en respectant plusieurs contraintes telle que la consommation d'énergie, un nombre d'inconvénients restent plus ou moins apparents. Dans la suite, nous mentionnons quelques avantages et inconvénients de ce protocole. [21]

3.1. Avantages

- Utilisation d'agrégation des données qui minimise le nombre des transmissions et qui conserve l'énergie.
- Elimination de la phase de la construction des clusters pour chaque round qui génère une surconsommation d'énergie importante.

3.2. Inconvénients

- Bien que l'overhead du clustering soit évité, PEGASIS exige toujours un ajustement dynamique de la topologie puisqu'un nœud devrait connaître le niveau d'énergie de ses voisins avant de relayer ses données.
- Ce protocole atteint rapidement ses limites de fonctionnement dans le cadre des réseaux fortement denses.
- Le délai de livraison des données est très important lorsque la chaine formée est très longue. Et, le nœud qui transmet les données vers le puits peut devenir un point de congestion du réseau

Conclusion

Dans ce chapitre, nous avons parlé du routage hiérarchique qui vise à rendre les protocoles plus favorables au passage à l'échelle tout en restant plus économique en consommation d'énergie. Et cela, afin de couvrir une zone de captage plus large.

Ainsi, nous avons identifié le protocole LEACH et sa variante, LEACH-C qui suivent une approche basée sur les groupes et le protocole PEGASIS qui est un protocole basé sur les chaînes. Cela, nous permet de passer au dernier chapitre qui est le cœur de notre recherche, la simulation de deux catégories des protocoles, l'un basé sur les groupes qui est LEACH ,VLEACH, LEACH-C, ModLEACH et l'autre basé sur les chaînes qui est PEGASIS en essayant de comparer les résultats en termes de consommation d'énergie et de durée de vie du réseau.

Chapitre4 : L'algorithme du protocole Leach

IV. Introduction

Dans ce chapitre, nous proposons un protocole hiérarchique adaptatif qui permet une Consommation fiable d'énergie pour les réseaux de capteurs sans fil, et nous avons appelé (Leach Leader). Nous introduisons algorithme du protocole qui adopte approche Centralisée, Le protocole est inspiré du protocole célèbre Leach, ce qui donne des Performances meilleurs dans les réseaux de capteurs sans fil.

Pour une implémentation correcte et fiable du protocole, en prenant en considération les Es détails spécifiques d'algorithme et des fonctions requises pour l'application, nous avons Ajouté des méthodes et des fonctions supplémentaires, Tels que la transmission de Données, le calcul de distance, optimisation de la sélection du chef de groupe. Nous Fournissons également une explication détaillée de l'implémentation.

Afin de teste la performance de notre solution une simulation est faite dans un Environnement adéquat ce qui nous a permet de présenter las résultat à la fin du chapitre.

IV.1 Le principe de fonctionnement de l'algorithme

Est l'un des algorithmes de routage hiérarchiques les plus populaires pour les RCSF. L'idée est de former des clusters basés sur la puissance du signal reçu et utiliser les clusterheads comme des routeurs à la station de base. Ceci permettra d'économiser l'énergie puisque les transmissions ne seront effectuées que par ces clusterheads plutôt que par tous les nœuds. Tous les traitements de données tels que la fusion ou l'agrégation de données sont assurés par les clusterheads. Ces clusterheads changent de rôle au hasard au fil du temps afin d'équilibrer la dissipation d'énergie des nœuds. Cette décision est prise par le nœud en choisissant un nombre aléatoire entre 0 et 1

IV.1.1 Expliquer le fonctionnement du programme

Le protocole LEACH (Low Energy Adaptive Clustering Hierarchy) est un algorithme utilisé dans les réseaux de capteurs sans fil pour économiser l'énergie et prolonger la durée de vie du réseau. Voici les principes de fonctionnement de l'algorithme LEACH :

1. **Formation des clusters :** Dans le protocole LEACH, les nœuds de capteurs sont regroupés en clusters pour faciliter la communication. Au début de chaque cycle, les nœuds décident de manière probabiliste s'ils seront les cluster heads (nœuds chefs de cluster) pour ce cycle. Chaque nœud calcule une probabilité en fonction de son niveau d'énergie actuel, et s'il génère un nombre aléatoire inférieur à cette probabilité, il devient un cluster head pour ce cycle. [21]
2. **Attribution des nœuds aux clusters :** Une fois que les cluster heads sont sélectionnés, les autres nœuds de capteurs du réseau choisissent le cluster auquel ils vont se joindre. Ils le font en sélectionnant le cluster head le plus proche sur la base d'un critère tel que la distance ou la force du signal.

3. **Transmission des données :** Les cluster heads collectent les données des nœuds qui leur sont affiliés et agrègent ces données pour réduire la quantité de trafic à transmettre. Les cluster heads utilisent ensuite des techniques de communication efficaces pour envoyer les données agrégées à un nœud central ou à une station de base.

4. **Rotation des cluster heads :** Étant donné que les cluster heads ont un rôle de communication plus intensif, ils consomment plus d'énergie que les autres nœuds. Pour équilibrer la consommation d'énergie dans le réseau, les cluster heads sont sélectionnés de manière probabiliste à chaque cycle, ce qui permet à tous les nœuds d'avoir la possibilité d'agir en tant que cluster head au fil du temps.

5. **Répétition des cycles** : Le protocole LEACH fonctionne par cycles, où chaque cycle se compose des étapes de formation des clusters, d'attribution des nœuds aux clusters, de transmission des données et de rotation des cluster heads. Cette répétition permet de répartir équitablement la charge de communication et d'économiser l'énergie globale du réseau.

IV.2 L'objectif :

L'objectif principal du protocole LEACH est de réduire la consommation d'énergie globale du réseau en optimisant l'utilisation des ressources et en évitant la mort prématurée des nœuds de capteurs. Cela permet d'améliorer l'efficacité énergétique et de prolonger la durée de vie du réseau de capteurs sans fil.

IV.3 Conception (l'algorithme) :

- **La première étape :**

Compris ! Si j'ai bien saisi, vous souhaitez générer une simulation plus réaliste en donnant des dimensions de surface, le nombre de capteurs, ainsi que des coordonnées et des niveaux d'énergie aléatoires pour chaque capteur. Voici comment vous pourriez aborder cela :

Dimensions de la surface : Déterminez la longueur et la largeur de la zone dans laquelle les capteurs sont placés. Ces dimensions peuvent être spécifiées en unités appropriées (par exemple, mètres ou kilomètres).

Nombre de capteurs : Choisissez le nombre de capteurs que vous souhaitez placer dans la zone. Ce nombre peut varier en fonction de vos besoins de simulation.

Génération de coordonnées : Générez des coordonnées aléatoires pour chaque capteur dans la zone définie par les dimensions. Vous pouvez utiliser des fonctions ou des bibliothèques aléatoires pour obtenir des coordonnées x et y dans la plage définie par les dimensions.

Attribution d'énergie : Pour chaque capteur, attribuez un niveau d'énergie aléatoire. Vous pouvez spécifier des bornes supérieure et inférieure pour les niveaux d'énergie afin de contrôler leur variation. Par exemple, vous pouvez définir une valeur maximale d'énergie pour un capteur et générer aléatoirement les niveaux d'énergie en fonction de cette valeur maximale.

Autres caractéristiques : Si vous souhaitez ajouter d'autres caractéristiques aléatoires aux capteurs, comme des états de repos, vous pouvez également les générer aléatoirement en spécifiant des probabilités ou des intervalles pour chaque état.

Une fois que vous avez généré les coordonnées et les niveaux d'énergie aléatoires pour chaque capteur, vous pouvez utiliser ces informations dans votre simulation de l'algorithme LEACH. Chaque capteur sera représenté par ses coordonnées et son niveau d'énergie, ce qui permettra de simuler une situation réaliste avec des capteurs placés dans une zone donnée, et où chaque capteur a ses propres caractéristiques uniques. N'oubliez pas d'adapter ces étapes à votre environnement de programmation ou à l'outil que vous utilisez pour réaliser la simulation.

```
from Leach import Network



wsn = Network(sensorsNumber=50, width=20, height=20,
              maxEnergy=18, num_clusters=4)
wsn.start()
```

- **La deuxième étape :**

Dans de nombreux groupes ou organisations, il existe une structure hiérarchique où différents leaders sont responsables de différentes équipes, départements ou domaines d'expertise. Le leader senior, ou le chef de groupe, est généralement considéré comme le chef d'orchestre du groupe et joue un rôle clé dans la coordination et la gestion de l'ensemble de l'organisation.

La position centrale du leader senior, comme vous l'avez mentionné, peut symboliser sa position de liaison entre les autres leaders. En étant au cœur du groupe, le leader senior peut faciliter la communication, la collaboration et la résolution des problèmes entre les différentes parties prenantes. Cette proximité permet également au leader senior de comprendre les besoins et les préoccupations de chaque leader et de prendre des décisions informées qui bénéficient à l'ensemble du groupe.

Le rôle du leader senior en tant que nœud puits peut également impliquer la prise en charge des responsabilités globales de leadership, telles que la définition de la vision stratégique, la prise de décisions importantes, la gestion des conflits et la représentation du groupe auprès d'autres entités externes.

Cependant, il est important de noter que le succès d'un groupe ne repose pas uniquement sur le leader senior, mais sur la collaboration et l'engagement de tous les leaders et membres du groupe. Une dynamique de leadership efficace et une communication ouverte à tous les niveaux sont essentielles pour maintenir un fonctionnement harmonieux de l'organisation.

```
def start(self):
    # Générer des positions de capteurs aléatoires
    self.generateSensors()
    self.cluster_sensors()
    self.showNodes()

def generateSensors(self, ):
    self.sensors = []
    for i in range(self.sensorsNumber):
        x = randint(1, self.width)
        y = randint(1, self.width)
        energy = randint(1, self.maxEnergy - 2)
        self.sensors.append(SensorNode(i, x, y, energy))

def generateSink(self):
    # Generer le sink node de toute le network au center de toutes les tete
    cluster_head_coordinates = np.array(
        [(node.x, node.y) for node in self.sensors if node.is_cluster_head])
    center_x = int(np.mean(cluster_head_coordinates[:, 0]))
    center_y = int(np.mean(cluster_head_coordinates[:, 1]))
    x_sink = center_x
    y_sink = center_y
    energy_sink = self.maxEnergy

    self.sinkNode = SensorNode(
        self.sensorsNumber, x_sink, y_sink, energy_sink)
```

- **La troisième étape :**

consiste à essayer de diviser en clusters. En utilisant k-means, nous associons chaque capteur au groupe auquel il appartient. Ensuite, dans chaque groupe, nous choisissons celui qui a plus d'énergie que les autres. Il sera le leader de le groupe sélectionné. Nous l'appelons le chef de groupe(clustersleader).

```
    def cluster_sensors(self):
        # Collecter toute les positions et energy de chaques sensor
        positions = np.array([(node.x, node.y) for node in self.sensors])
        energies = np.array([node.energy for node in self.sensors])

        # Classify toute les sensors par apport leur position (x,y) en utilisant method K-Moyens
        kmeans = KMeans(n_clusters=self.num_clusters, random_state=0)
        kmeans.fit(positions)

        # Lie chaque sensor avec sa cluster IDs
        cluster_ids = kmeans.labels_
        for i, node in enumerate(self.sensors):
            node.cluster_id = cluster_ids[i]

        # trouver le sensor qui a un valeur maximum de energy pour chaque classe et marque comme tete de chaque cluster
        cluster_energy_max = {}
        for node in self.sensors:
            if node.energy > cluster_energy_max.get(node.cluster_id, -float('inf')):
                cluster_energy_max[node.cluster_id] = node.energy
```

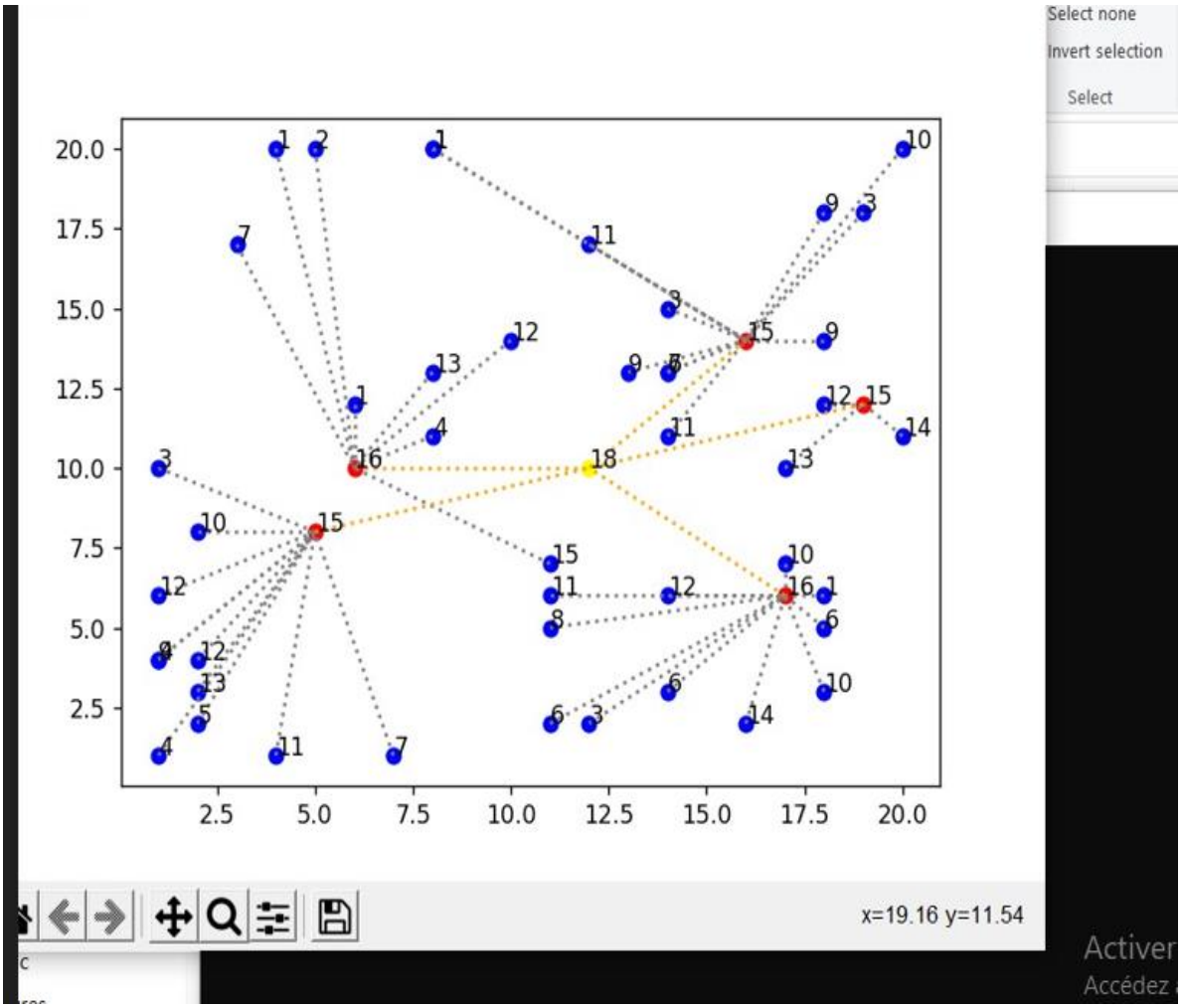
```
        return sensor_nodes

    def cluster_sensors(self):
        # Collecter toute les positions et energy de chaques sensor
        positions = np.array([(node.x, node.y) for node in self.sensors])
        energies = np.array([node.energy for node in self.sensors])

        # Classify toute les sensors par apport leur position (x,y) en utilisant method K-Moyens
        kmeans = KMeans(n_clusters=self.num_clusters, random_state=0)
        kmeans.fit(positions)

        # Lie chaque sensor avec sa cluster IDs
        cluster_ids = kmeans.labels_
        for i, node in enumerate(self.sensors):
            node.cluster_id = cluster_ids[i]

        # trouver le sensor qui a un valeur maximum de energy pour chaque classe et marque comme tete de chaque cluster
        cluster_energy_max = {}
        for node in self.sensors:
            if node.energy > cluster_energy_max.get(node.cluster_id, -float('inf')):
                cluster_energy_max[node.cluster_id] = node.energy

        for node in self.sensors:
            if node.energy == cluster_energy_max.get(node.cluster_id):
                node.is_cluster_head = True

        # Liee chaque sensor to chaque cluster a son cluster Tete sensor
        for node in self.sensors:
```

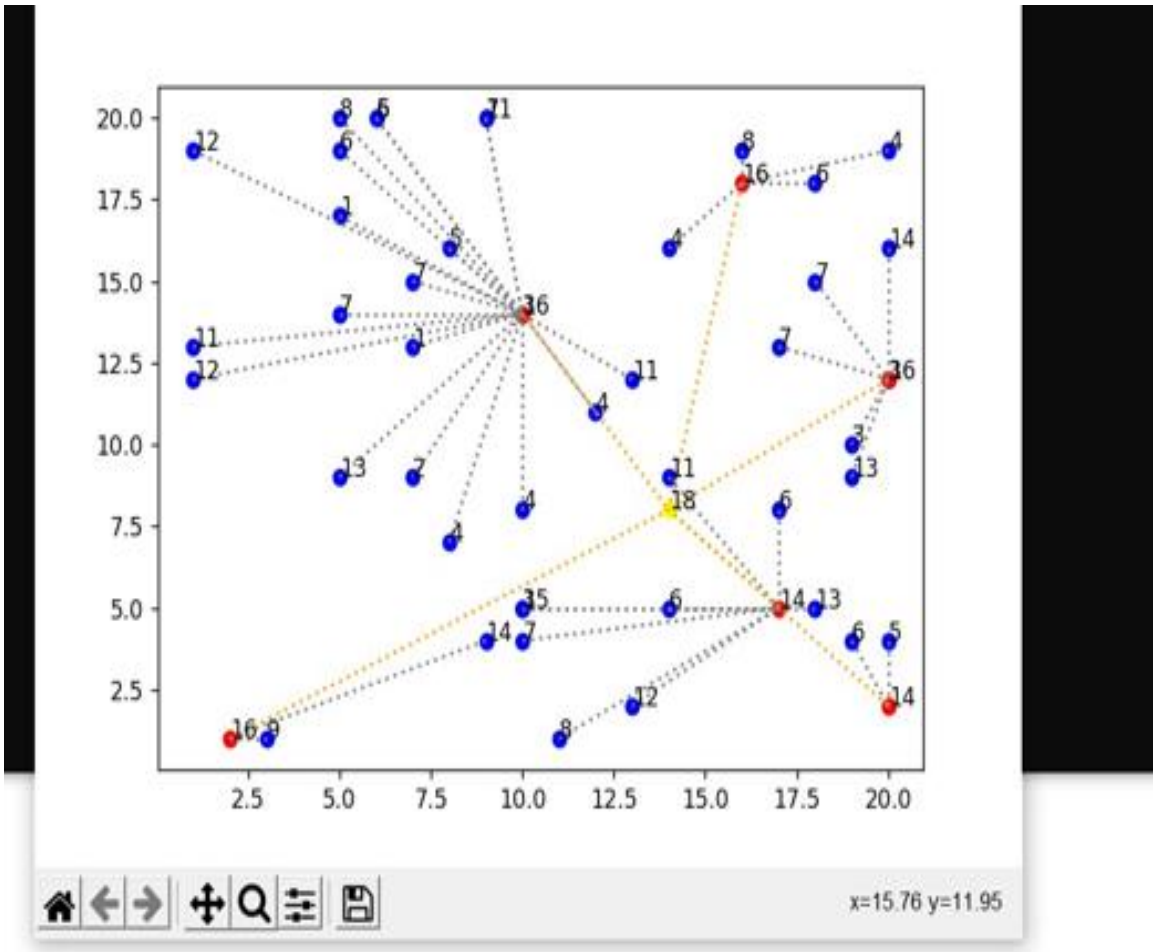
IV.4 Des explication sur l'implémentation langage utilise simulation importer matplotlib.pyplot

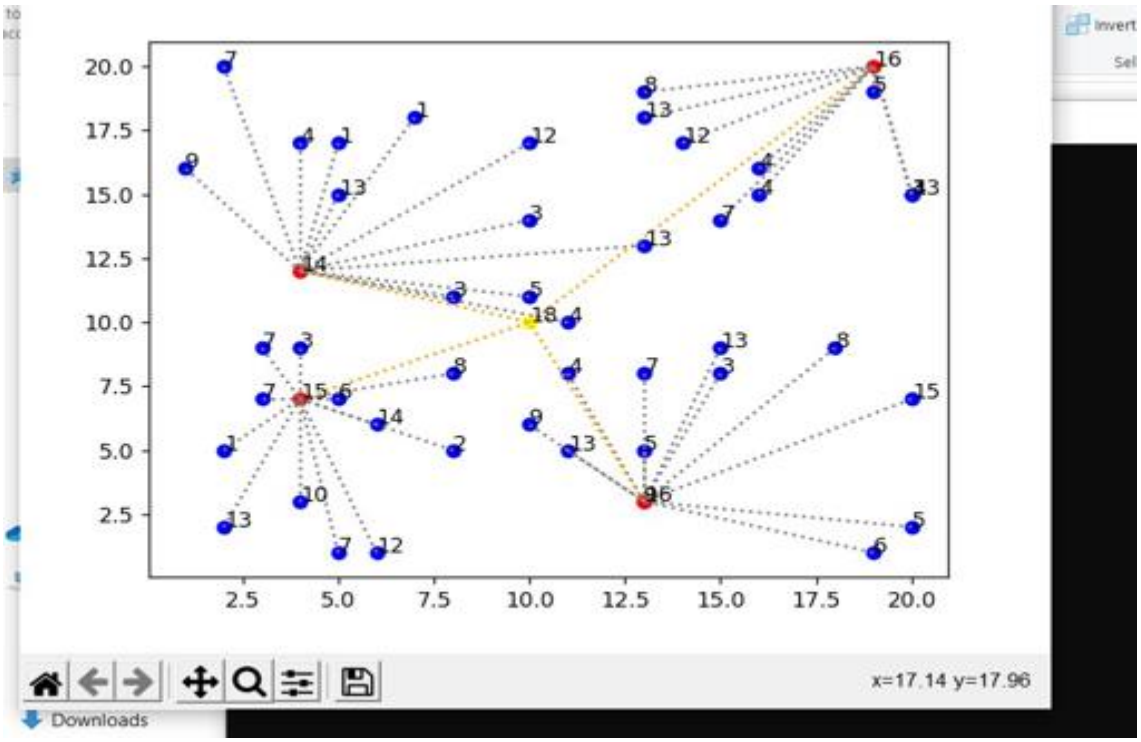
Cette ligne de code importe la bibliothèque Matplotlib et la renomme plt, ce qui est une pratique courante pour rendre ses fonctions plus faciles à utiliser.

Une fois que vous avez importé Matplotlib, vous pouvez commencer à utiliser ses fonctionnalités pour créer des tracés, des graphiques et des visualisations de données. N'hésitez pas à me demander si vous avez besoin d'aide pour une tâche spécifique avec Matplotlib.

Le programme et le résultat de la recherche sont un petit exemple :


Select none
Invert selection
Select
x=19.16 y=11.54


x=15.76 y=11.95


x=17.14 y=17.96
Downloads

CONCLUSION

En conclusion, le Low Power Adaptive Hierarchy Protocol (LEACH) est un algorithme de clustering largement utilisé dans les réseaux de capteurs sans fil (RCSF) pour économiser l'énergie des nœuds. Il permet d'organiser les nœuds en groupes, en sélectionnant au hasard le nœud leader du cluster (CH) pour chaque tour.Ainsi, notre recherche a stipulé un protocole cloné à partir de lixiviation et l'a légèrement modifié et renommé leachleader.

Référence

[1] htmlChristophe Baland, Damien Cauquil, Thomas Gayet, Julia Juvigny, Renaud Lifchitz, NhaKhanh Nguyen , la sécurité de l‟Internet des Objets, livre blanc.

[2] https://www.researchgate.net/figure/Open-Systems-Interconnection-OSI-reference- Dos attaqurs. https://www.ionos.fr/digitalguide/serveur/know-how/

[3] https://www.tutorialsmate.com/2020/05/types-of-computer-networks.html

[4] https://www.guru99.com/tcp-ip-model.html

[5] /https://www.camerecole.org/classes/1441-configuration-d-un-reseau-informatique.html

[6] https://fr.wikipedia.org/wiki/Mod%C3%A8le_OSI

[7] Laurent Poinsot «Introduction à la sécurité informatique», support de cours,UniversitéParis 13.

[8] Les virus informatique clusif 2005, page 10

[9] Les virus informatique clusif 2005, page 10

[10] Philippe Biondi, Architecture expérimentale pour la détection d'intrusions dans unsystème informatique, Article de recherche, Avril-Sptembre 2001

[11] Le grand livre de la sécurité informatique. SecuriteInfo, Editions du 6 nouvembre2006

[12] Laurent Bloch-Christophe Wolfhugel. Sécurité informatique .EYROLLES, 2emeedition. 2005.

[13] M.Tran Van Tay, le système de détection des intrusions et le système d'empêchement des intrusions (ZERO DAY), Rapport de stage de fin d'étude, institut de la francophonie pour l'informatique, université de Québec à Montréal, Féverier 2005.

[14] M.Tran Van Tay, le système de détection des intrusions et le système d'empêchement des intrusions (ZERO DAY), Rapport de stage de fin d'étude, institut de la francophonie pour l'informatique, université de Québec à Montréal, Féverier 2005.

[15] https://fr.wikibooks.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_informatiques/S%C3%A9curit%C3%A9_informatique/D%C3%A9tection_d%27intrusion4

[16] https://www.memoireonline.com/02/22/12729/m_Etude-conception-et-mise-en-uvre-dun-systeme-de-surveillance-par-detection-dintrusion-dans-un-re9.html

Référence

[17] Hervé Debar, Benjamin Morin, Frédéric Cuppens, Fabien Autrel, Ludovic Mé, Bernard Vivinis Salem Benferhat, Mireille Ducassé, Rodolphe Ortalo, Détection d'intrusions : corrélationd'alertes. Article de synthèse, Caen, France, 2004.

[18] Yann Berthier, Jean-Baptiste Marchand, Détection d'intrusions et analyse forensique.

[19] http://dspace.univ-tlemcen.dz/bitstream/112/6320/1/Etude-et-mise-en-place%20.pdf

[20] Thierry Evangilista, Les IDS Les systèmes de détection d'intrusions informatiques édition DUNOD, Paris 2004.

[21] https://dspace.univ-guelma.dz/jspui/bitstream/123456789/10125/1/HAMOUDA_DJALLEL1603195191.pdf

[22] Article, Team redac février 15, 2023, datascientest.com/machine-learning-tout-savoir

Conclusion générale

B. Conclusion générale

Les réseaux de capteurs sans-fils sont des systèmes distribués spécialement, composés de plusieurs dizaines de milliers de micro-capteurs.

Ils mettent en jeu de nombreuses entités, souvent autonomes d'un point de vue énergétique. Ces entités remplissent essentiellement deux tâches: la collecte de mesures et la communication de mesures en direction d'une station de collecte. Ces entités sont généralement reliées par des réseaux de communication sans-fil. Dans de tels réseaux les liens sont asymétriques, la topologie est dynamique, la bande passante limitée et aucun organe dédié au routage n'est présent. L'ensemble des éléments du réseau participe activement au routage de l'information.

Il est donc rendu plus difficile que dans les réseaux filaires traditionnels. En effet, le processus de routage dans ce type de réseau est en saut par saut (multi-hop). La recherche de route repose nécessairement sur de l'inondation qui consiste à envoyer un message (par exemple la construction d'une route) à ses voisins pour qu'ils fassent de même etc.

Le bon fonctionnement du routage dépend ainsi du comportement de l'ensemble des nœuds du réseau qui doivent respecter le protocole en usage.

Il est très fréquemment supposé que ces nœuds sont de confiance.

B.1<u>Nous avons structuré notre mémoire en quatre chapitres :</u>

Dans le premier chapitre, nous présentons une étude générale d'election d'un leader pour la gestion dynamique et distribué des réseaux de capteurs sans fil.

Le deuxième chapitre est consacré à l'étude de L'économie d'énergie et tolérance aux pannes dans les RCSF.

Le troisième chapitre est consacré aux.

Le quatrième chapitre consacré à l'étude de.

Le dernier chapitre concerne notre travail.

Mots-clés : réseaux de capteurs, routage, sécurité du routage, confiance, modèle de confiance.
Réseaux de capteurs sans fil, agrégation de données dans un réseau, LEACH, TinyOS

Résume

Dans ce travail, nous avons principalement étudié le problème qui faisait fonctionner la capture sans fil avec une certaine puissance et une durée plus longue. Nous avons étudié les protocoles proposés par Leach et Pegsis
L'accent a été mis sur le protocole Leach et sa mise en œuvre. Dans ce travail, nous avons créé un code tel que :
Le chef choisit au milieu du groupe et ne le laisse pas voter comme d'habitude.

Abstract

In this work, we mainly studied the problem which made the wireless capture work with certain power and longer time. We studied the protocols proposed by leach and pegsis
The focus was on the Lash protocol and its implementation. In this work, we created code such as:
The leader chooses in the middle of the group and does not let them vote as usual.

تلخيص

في هذا العمل، درسنا بشكل أساسي المشكل الذي جعل الالتقاط اللاسلكي يعمل بطاقة معينة و مدة أطول. درسنا بروتوكولات تم اقتراحهم متمثلين في بروتوكول leach و pegsis
تم التركيز على بروتوكول لاش و العمل به. في هذا العمل قمنا بعمل رمز بحيث يختار الشاف في منتصف المجموعة و لا يتركه للانتخاب مثل المعتاد.