

الجمهورية الجزائرية الديمقراطية الشعبية
République algérienne démocratique et populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique
جامعة عين تموشنت بلحاج بوشعيب
Université -Ain Temouchent- Belhadj Bouchaib
Faculté des Sciences et de Technologie
Département des Mathématiques et Informatique



Projet de Fin d'Etudes
Pour l'obtention du diplôme de Master en : Informatique
Domaine : Mathématiques et Informatique
Filière : Informatique
Spécialité : Réseaux et Ingénierie des Données (RID)

Thème

**Les indicateurs locaux de position pour la tolérance
aux pannes dans les réseaux de capteurs sans fil**

Présenté par :

Melle ZAIMI Rania Dounia Zed

Devant le jury composé de :

Mlle BOUHALOUAN Djamila	MCB	UAT.B.B (Ain Temouchent)	Président
Mme ABDERRAHIM Nazih	MCB	UAT.B.B (Ain Temouchent)	Examinateur
Mr MESSAOUDI Mohamed Amine	MCB	UAT.B.B (Ain Temouchent)	Encadreur

Année Universitaire 2022/2023

REMERCIEMENTS

Je tiens premièrement à me prosterner remerciant mon Dieu ALLAH le tout puissant de m'avoir donné la force morale et physique pour achever mon mémoire de fin d'étude.

Tout d'abord, je remercie le Docteur MESSAOUDI Amine, pour m'avoir honoré par son encadrement, sa disponibilité indéfectible, ses conseils précieux, ses nobles valeurs humaines pendant les moments difficiles ainsi que pour la confiance qu'il m'a témoignée jusqu'à l'aboutissement de ce travail.

Mes remerciements vont également aux membres de jury qui me fait le grand honneur de juger mon travail : Je remercie Docteur BOUHALOUAN Djamila qui a bien voulu présider le jury. Je remercie également l'examinatrice Dr ABDERRAHIM, pour l'intérêt qu'elle a porté à mon travail.

Un grand merci va également à l'ensemble des membres du CNAS, avec lesquelles j'avais pu avoir de nombreux échanges scientifiques. Je tiens aussi à exprimer toute ma gratitude à tous les enseignants du département d'informatique qui ont contribué à ma formation et pour leur soutien moral et leurs encouragements.

DEDICACE

À ma très chère grand-mère.

À ma chère mère, à mon cher père.

À ma meilleure professeure Dr. BOUHALOUAN Djamila.

À mes amis, ma chère amie Fatima BEN AHMED DAHO qui m'avait soutenue avec amour et tendresse pendant ce travail,

À ma famille.

À mon petit frère Chiheb.

Rania

RESUME

En théorie des graphes, les indicateurs locaux de position permettent de mesurer le degré de centralité ou d'accessibilité des différents sommets à l'intérieur d'un graphe. Les avantages relatifs des différents sommets peuvent varier selon le critère retenu. L'objectif principal de ce projet de fin d'études est de proposer une solution tolérante aux pannes qui consiste à exploiter les indicateurs locaux de position dans le but de garantir un bon fonctionnement du réseau de capteurs sans fil même après la faille de certains de ses composants.

Mots clés :

Théorie des graphes, indicateurs locaux de position, Réseaux de capteurs sans fil, défaillances, tolérance aux pannes, simulation.

ABSTRACT

In graph theory, local position indicators are used to measure the degree of centrality or accessibility of the various vertices inside a graph. The relative advantages of the various vertices may vary depending on the criterion used. The main objective of this end-of-studies project is to propose a fault-tolerant solution which consists in exploiting the local position indicators with the aim of guaranteeing the correct operation of the wireless sensor network even after the failure of some of its components.

Key words:

Graph theory, local position indicators, wireless sensor networks, failures, fault tolerance, simulation.

ملخص

في نظرية الرسم البياني ، تُستخدم مؤشرات الموضع المحلية لقياس درجة المركزية أو إمكانية الوصول للرؤوس المختلفة داخل الرسم البياني. قد تختلف المزايا النسبية للرؤوس المختلفة اعتمادًا على المعيار المستخدم. الهدف الرئيسي لمشروع نهاية الدراسات هذا هو اقتراح حل يتسامح مع الأخطاء والذي يتمثل في استغلال مؤشرات الموقع المحلية بهدف ضمان التشغيل الصحيح لشبكة أجهزة الاستشعار اللاسلكية حتى بعد فشل بعض مكوناتها.

الكلمات الدالة :

نظرية الرسم البياني، مؤشرات الموقع المحلية، شبكات الاستشعار اللاسلكية، الأعطال، تحمل الخطأ، المحاكاة.

TABLE DES MATIERES

REMERCIEMENT	II
DEDICACE	III
RESUME	IV
ABSTRACT	V
ملخص	VI
LISTE DES FIGURES	XI
LISTE DES TABLEAUX	XII
LISTE DES ABREVIATIONS ET SIGLES	XIV
INTRODUCTION GENERALE	2
CHAPITRE I : LES RESEAUX DE CAPTEURS SANS FIL	4
I.1. Introduction	5
I.2. Les Réseaux sans fil	5
I.2.1. Définitions	5
I.2.2. Classification des Réseaux Sans Fil	6
I.2.2.1. Classification selon la zone de couverture	6
I.2.2.2. Classification selon l'infrastructure	8
I.3. Les Réseaux de capteurs sans fil	10
I.3.1. Définitions	10
I.3.2. Historique	11
I.3.3. Architecture d'un RCSF	12
I.3.4. Caractéristique réseaux de capteurs sans fil	12
I.3.5. Types de réseaux de capteurs sans fil	13
I.3.5.1. Réseaux de poursuite	13
I.3.5.2. Réseaux de collection des données d'environnement	13
I.3.5.3. Réseaux de surveillance et sécurité	13
I.3.6. Les protocoles de routage dans les RCSF	14
I.3.6.1. Selon leur Topologie du Réseau	15
I.3.6.2. Selon leur Type de protocoles	15
I.3.6.3. Protocoles Ad Hoc adaptés pour RCSF	16
I.3.7. Applications des RCSF	17
I.3.8. Comparaison entre les réseaux Ad hoc classiques et les réseaux de capteurs	18
I.3.9. Différentes problématiques présentes dans les RCSF	19

I.4. Conclusion	21
CHAPITRE II : LA TOLERANCE AUX PANNES DANS LES RCSF	23
II.1. Introduction	23
II.2. Les pannes	23
II.3. Origines des pannes dans les RCSFs	23
II.3.1. Pannes de point de vue composant	24
II.3.2. Pannes de point de vue système	25
II.4. Classification des pannes	25
II.4.1. Panne selon la durée	26
II.4.2. Panne selon la cause	27
II.4.3. Panne selon le comportement résultat	27
II.5. Causes des pannes	27
II.6. Définition de la tolérance pannes	28
II.7. Fonctionnement	28
II.8. Procédure générale de tolérance aux pannes	29
II.8.1. Détection de la panne	29
II.8.2. Détention de la panne	29
II.8.3. Recouvrement de la panne	29
II.8.4. Traitement de la panne	29
II.9. Exemple d'un RCSF tolérant aux pannes	30
II.10. Classification des solutions de tolérance aux pannes dans les RCSF	31
II.10.1. Classification selon la nature de l'algorithme / protocole	31
II.10.2. Classification architecturale	31
II.11. Conclusion	33
CHAPITRE III : LES INDICATEURS LOCAUX DE POSITION	35
III.1. Introduction	35
III.2. Les modèles de graphes théoriques	35
III.2.1. Réseaux aléatoires	35
III.2.2. Réseaux petits mondes (small world network)	35
III.2.3. Réseau invariant d'échelle (Scale-free network)	35
III.3. La Théorie des graphes	36
III.3.1. Définition et notations	36
III.3.2. Les types des graphes	37

III.3.2.1. Graphes connexes/complémentaires	37
III.3.2.2. Graphes planaires	37
III.3.2.3. Composantes connexes	38
III.3.2.4. Cycles	38
III.3.3. Valuation et orientation	39
III.3.3.1. Graphes Valués	39
III.3.3.2. Graphes Orientés	39
III.4. OUTILS GENERAUX DE DESCRIPTION DES GRAPHES	40
III.4.1. Indicateurs globaux	40
III.4.1.1. Indicateurs de connexité.....	40
III.4.1.2. Indicateurs de connectivité	41
III.4.2. Indicateurs locaux.....	43
III.4.2.1. Centralité de degré (C_D)	43
III.4.2.2. Centralité d'éloignement moyen (C_E)	44
III.4.2.3. Centralité d'éloignement maximal (C_M)	45
III.4.2.4. Centralité d'intermédiarité (C_I)	45
III.5. Influence du type de graphe sur les indicateurs de centralités	46
III.6. Conclusion	47
CHAPITRE IV : SIMULATION	49
IV.1. Introduction	49
IV.2. Environnement de simulation	49
IV.2.1. Système d'exploitation CONTIKI	49
IV.2.1.1 Présentation	49
IV.2.1.2. Caractéristiques de Contiki	49
IV.2.1.3. Architecture de CONTIKI	50
IV.2.2. Le simulateur Cooja pour les applications Contiki	51
IV.3. Implémentations et déroulements de simulation	52
IV.3.1. Les scénario de la simulation	55
IV.3.1.1. Scénario 1 (Centralité de degré (C_D)	55
IV.3.1.2. Scénario 2 (Centralité d'éloignement moyen (C_E)	59
IV.3.1.3. Scénario 3 (Centralité d'éloignement maximal (C_M)	60
IV.3.1.4. Scénario 4 (Centralité d'intermédiarité (C_i)	61
IV.4. Résultats des simulations	62

IV.5. L'analyse des résultats des simulations	63
IV.6. Conclusion	65
CONCLUSION GENERALE	66
REFERENCE BIBLIOGRAPHIQUE	69

LISTE DES FIGURES

FIGURE I.1 : Classification des réseaux sans fil.....	6
FIGURE I.2 : Classification des réseaux sans fil selon leur taille	6
FIGURE I.3 : Les technologies et la classification des RSF selon leur taille	8
FIGURE I.4 : Un Réseau Cellulaire	9
FIGURE I.5 : Un Réseau Ad Hoc	10
FIGURE I.6 : un réseau de capteur sans fil	11
FIGURE I.7 : les réseaux de capteurs sans fil	11
FIGURE I.8 : L'architecture d'un RCSF	12
FIGURE I.9 : Classification des protocoles de routage dans les RCSF	14
FIGURE I.10 : Les applications des RCSF	18
FIGURE II.1 : Classification des panes	26
FIGURE II.2 : Procédure générale de tolérance aux pannes	29
FIGURE II.3 : Réseau de capteur multimodal	30
FIGURE III.1 : Les différents types de réseaux.....	36
FIGURE III.2 : Un graphe G avec 4 sommets et 3 arêtes	37
FIGURE III.3 : Un graphe connexe.....	37
FIGURE III.4 : Le graphe de Petersen, à gauche et son complémentaire, à droite	37
FIGURE III.5 : Un graphe Planaire	38
FIGURE III.6 : graphe 4 composantes connexes.....	38
FIGURE III.7 : Un Cycle	39
FIGURE III.8 : Graphe Valué	39
FIGURE III.9 : Arc (x,y).....	39
FIGURE III.10 : Graphe non orienté	40
FIGURE III.11 : Exemple d'application (indicateur connexité).....	41
FIGURE III.12 : Exemple d'application (indicateur connectivité)	42
FIGURE III.13 : Exemple d'application (les indicateur locaux)	43
FIGURE IV.1 : Système d'exploitation CONTIKI	50
FIGURE IV.2 : Interface graphique de Cooja	51
FIGURE IV.3: Compilation et lancement des simulations sur Cooja.	52
FIGURE IV.4: Les différentes topologies de simulation avant le déclenchement d'action correctif.....	53

FIGURE IV.5.1: DODAG Simulation1 avant le déclenchement d'action correctif	54
FIGURE IV.5.2: DODAG Simulation2 avant le déclenchement d'action correctif	54
FIGURE IV.5.3: DODAG Simulation3 avant le déclenchement d'action correctif	54
FIGURE IV.6: le fichier Mobility.	55
FIGURE IV.7: les étapes de Mobilité.	56
FIGURE IV.8.1: Mobilité des nœuds scénario 1 Simulation 1	57
FIGURE IV.8.2: Mobilité des nœuds scénario 1 Simulation 2	57
FIGURE IV.8.3: Mobilité des nœuds scénario 1 Simulation 3	57
FIGURE IV.9.1: DODAG scénario 1 S1 après le déclenchement d'action correctif	58
FIGURE IV.9.2: DODAG scénario 1 S2 après le déclenchement d'action correctif	58
FIGURE IV.9.3: DODAG scénario 1 S3 après le déclenchement d'action correctif	58
FIGURE IV.10.1: DODAG scénario 2 S1 après le déclenchement d'action correctif	59
FIGURE IV.10.2: DODAG scénario 2 S2 après le déclenchement d'action correctif	59
FIGURE IV.10.3: DODAG scénario 2 S3 après le déclenchement d'action correctif	59
FIGURE IV.11.1: DODAG scénario 3 S1 après le déclenchement d'action correctif	60
FIGURE IV.11.2: DODAG scénario 3 S2 après le déclenchement d'action correctif	60
FIGURE IV.11.3: DODAG scénario 3 S3 après le déclenchement d'action correctif	60
FIGURE IV.12.1: DODAG scénario 4 S1 après le déclenchement d'action correctif	61
FIGURE IV.12.2: DODAG scénario 4 S2 après le déclenchement d'action correctif	61
FIGURE IV.12.3: DODAG scénario 4 S3 après le déclenchement d'action correctif	61
FIGURE IV.13: Résultats de simulation.	62

LISTE DES TABLEAUX

TABLE I.1 : Comparaison entre les réseaux Ad hoc classiques et les réseaux de capteurs	20
TABLE III.1 : Les Calcul des indices de connexité	42
TABLE III.2 : Les Calcul des indices de connectivité.....	43
TABLE III.3 : La centralité de degré	44
TABLE III.4 : La centralité de d'éloignement moyen	46
TABLE III.5 : La centralité de d'éloignement maximal	46
TABLE III.6 : La centralité de d'intermédiarité	46
TABLE IV.1 : Les paramètres de simulation	53

LISTE DES ABREVIATION ET SIGLE

RCSF	Réseaux de capteurs sans fil
WSN	Wireless sensor Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network
WWAN	Wireless Wide Area Network
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ADCs	Analog-to-Digital Convertors
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
RSSI	Received Signal Strength Indication
MAC	Medium Access Control
COOJA	Contiki OS Java Simulator
OS	Operating System

INTRODUCTION GENERALE

INTRODUCTION GENERALE

Aujourd'hui, les réseaux sans fil sont de plus en plus populaires du fait de leur facilité de déploiement. Ces réseaux jouent un rôle primordial au sein des réseaux informatiques. Ils offrent des solutions ouvertes pour fournir la mobilité ainsi que des services essentiels là où l'installation d'infrastructures n'est pas possible.

Les réseaux sans fil sont généralement classés selon deux catégories : les réseaux sans fil avec infrastructure fixe qui utilisent généralement le modèle de la communication cellulaire et les réseaux sans fil et sans infrastructure fixe ou les réseaux ad-hoc. Un réseau ad-hoc consiste donc en un grand nombre d'unités mobiles se déplaçant dans un environnement quelconque en utilisant, comme moyen de communication, des interfaces sans fil.

Durant ces deux dernières décennies, une nouvelle architecture appelée Réseau de Capteur Sans Fil (RCSF) a vu le jour. Ce type de réseau est né de la fusion entre les systèmes embarqués et les communications sans fil. Un RCSF ("WSN : Wireless Sensor Network" en Anglais) est un réseau Ad hoc composé d'un grand nombre de nœuds qui sont des micro-capteurs communiquant via des liaisons sans fil par des ondes radioélectriques de façon autonome. Ces nœuds encore appelés capteurs sont capables de récolter plusieurs paramètres sur l'environnement qui les entoure, appelé généralement zone de captage (ou zone de surveillance). Ensuite, ils doivent si nécessaire traiter les données capturées et les transmettre à un ou plusieurs nœuds de collecte appelés station de base, collecteurs, centres de traitements (ou "sink" en Anglais). Dans la suite, j'utilise les termes station de base afin de désigner les nœuds collecteurs.

Le RCSFs représentent un nouveau paradigme pour extraire les données de différents environnements, ce qui a permis le développement d'une vaste gamme d'applications comme le contrôle de l'environnement, la recherche biomédicale, l'e-Health, l'agriculture de précision, les activités militaires, *etc.* Pour de telles applications, les RCSFs permettent d'assurer diverses tâches telles que la surveillance, la détection d'événements et la collecte d'informations.

Ces tâches ne peuvent être assurées correctement que si les RCSFs font preuve de robustesse, de tolérance aux pannes, d'autonomie d'énergie,

La ressource énergétique limitée d'un nœud capteur, ainsi que les environnements hostiles et dangereux dans lesquels les RCSFs sont déployés, augmentent la probabilité de pannes et rendent la mission de maintien du bon fonctionnement du réseau plus difficile.

En plus, pour certains environnements, le remplacement d'un nœud défaillant ou de sa batterie est rarement envisageable voire impossible. Par ailleurs, le déploiement dense des nœuds capteurs fait surgir d'autres problèmes tels que les

interférences produites par les transmissions simultanées des nœuds voisins. Tous les problèmes cités précédemment représentent de vrais challenges que les RCSFs doivent relever.

Pour pallier ces manquements, plusieurs techniques et mécanismes ont été proposés pour tenir compte des limites des RCSFs et améliorer leur autonomie, leur fiabilité et leur degré de tolérance aux pannes.

L'objectif de ce mémoire est de réaliser une étude pour atteindre et avoir l'indicateur local de position le plus efficace avec la tolérance aux pannes dans les réseaux de capteurs sans fil.

Pour ce faire, J'ai organisé mon travail autour de quatre chapitres encadrés par une introduction et une conclusion :

Le chapitre 1: est une introduction aux réseaux de capteurs sans fil, une présentation de leur architecture et principales caractéristiques, les applications potentielles et les différentes problématiques présentes dans les RCSF.

Le chapitre 2 : Est une présentation des différentes catégories de pannes qui peuvent survenir durant le cycle de vie d'un réseau de capteurs sans fil, leurs caractéristiques, causes et les solutions proposées pour cette tolérance.

Le chapitre 3 : Est une notion de base de la théorie des graphes et des différents outils généraux de description des graphes qui sont des indicateurs globaux et je détaille les différents indicateurs locaux de position pour la tolérance des pannes dans les réseaux de capteurs sans fil ainsi que l'influence du type de graphe sur les indicateurs de centralité.

Le chapitre 4 : constitue le cœur de mon travail. Ce chapitre concerne la simulation et les résultats obtenus par l'expérimentation. Je vais présenter d'abord l'environnement de travail, puis la simulation et les résultats obtenus et enfin l'analyse et la comparaison des résultats.

Enfin, je vais conclure ce mémoire par une conclusion générale et on présente quelques perspectives.

CHAPITRE I: LES RESEAUX DE CAPTEURS SANS FIL.

I.1. Introduction :

Les capteurs existent depuis plusieurs années dans les domaines de l'industrie tels que l'aéronautique, l'automobile. On observe actuellement une forte recrudescence de ce type d'équipements qui sont interconnectés pour former des réseaux de capteurs. Avant, ils étaient reliés directement à leur base de traitement par une liaison filaire, ces capteurs sont maintenant de plus en plus interconnectés par ondes radios (ZigBee par exemple). En 2003, selon le magazine Technology Review du MIT, le réseau de capteurs sans fil est l'une des dix nouvelles technologies qui bouleverseront le monde et notre manière de travailler et de vivre.

Chaque capteur collabore avec ses voisins via des liens sans fil, et si nécessaire doit retransmettre les informations venant de capteurs trop éloignés pour communiquer directement avec la station de base qui à son tour retransmet ces données, après les avoir traité, au utilisateur final du réseau. La conception des capteurs à petite taille et à faible coût qui ont la capacité de traiter, détecter, stocker et communiquer des données, et de les intégrer dans ce qu'on appelle réseaux de capteurs sans fil ouvre la possibilité de les intégrer dans différents domaines d'applications allant de la surveillance militaire à la surveillance médicale en passant par la domotique, l'écologie, la télématique et la logistique. Vu leur conception, les réseaux de capteurs se diffèrent des réseaux ad Hoc traditionnels en un ensemble de points qui sont :

- Les réseaux de capteurs ont plus de nœuds avec une plus haute densité.
- Les nœuds dans les réseaux de capteurs sont assez fragiles et vulnérables à diverses formes de défaillances : faible capacité d'énergie, faible débit, cassure, etc.

Dans ce présent chapitre, je retrace la classification des réseaux sans fil et ensuite les principales notions de base des réseaux de capteurs sans fil. [1]

I.2. Les Réseaux sans fil :

I.2.1. Définitions :

Un **réseau sans fil** est un réseau informatique numérique qui connecte différents postes ou systèmes entre eux par ondes radio. Il peut être associé à un réseau de télécommunications pour réaliser des interconnexions à distance entre nœuds. [2]

I.2.2. 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 figure suivante [3]:

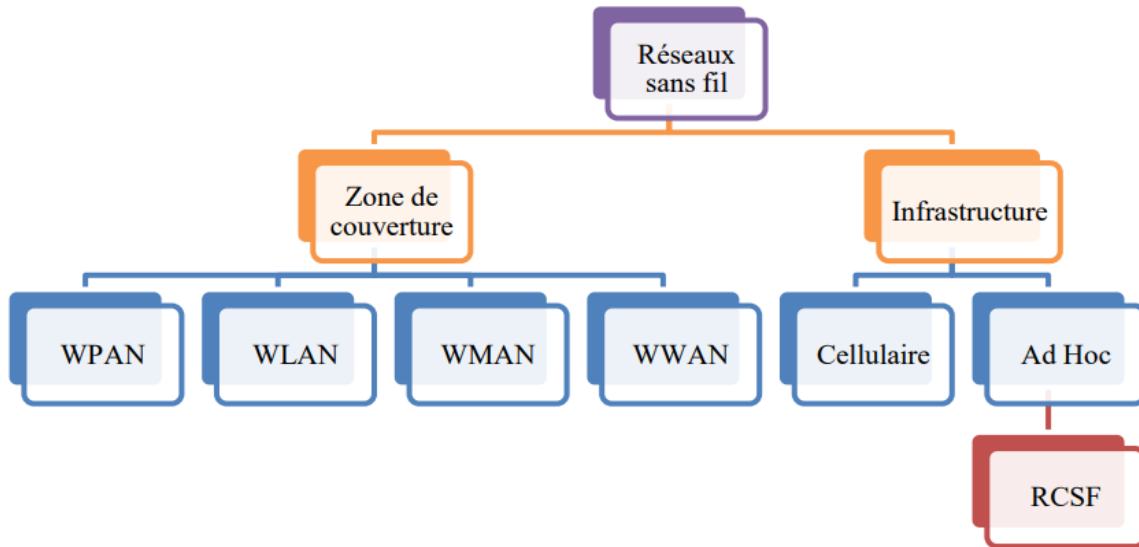


Figure I.1 : Classification des réseaux sans fil.

I.2.2.1. 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.

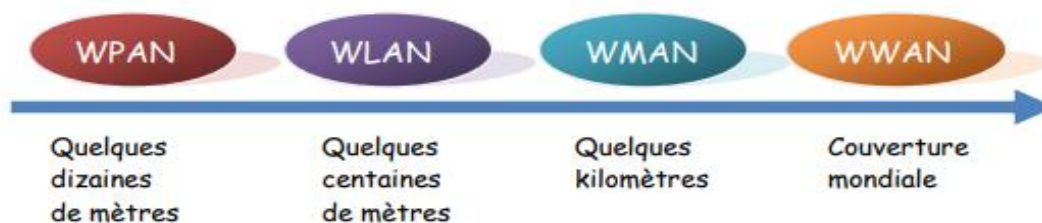


Figure I.2 : Classification des réseaux sans fil selon leur taille.

A. WPAN (Wireless Personal Area Network) :

Le *réseau personnel sans fil* concerne les réseaux sans fil d'une faible portée : de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes.

On va donc retrouver dans les WPAN pas mal de normes domotiques, en plus des liaisons courtes portées :

- Le Bluetooth
- Le ZigBee
- ANT
- Le KNX sans fil
- Z-wave
- Le WiFi, bien que ce soit plutôt un WLAN, mais comme souvent c'est personnel...
- Tous les protocoles utilisant le 433 MHz, courte portée et largement utilisés en domotique
- Tous les protocoles utilisant le 868 MHz, aussi utilisés en domotique.

B. WLAN (Wireless Local Area Network) :

Le *réseau local sans fil* est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre eux les terminaux présents dans la zone de couverture, Il existe plusieurs technologies concurrentes :

- Le **Wifi (ou IEEE 802.11)**, soutenu par l'alliance **WECA** (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres.
- **hiperLAN2 (High Performance Radio LAN 2.0)**, norme européenne élaborée par l'**ETSI** (European Telecommunications Standards Institute). HiperLAN 2 permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 MHz.

C. WMAN (Wireless Metropolitan Area Network) :

Le *réseau métropolitain sans fil* est connu sous le nom de **Boucle Locale Radio (BLR)**. Ils sont basés sur la norme **IEEE 802.16**. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication.

La norme de WMAN la plus connue est le **WiMAX**, permettant d'obtenir des débits de l'ordre de 70 Mbit/s sur un rayon de plusieurs kilomètres.

D. **WWAN (Wireless Wide Area Network) :**

Le *réseau étendu sans fil* est également connu sous le nom de *réseau cellulaire mobile*. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil.

Les principales technologies sont les suivantes :

- **GSM** (*Global System for Mobile Communication* ou en français *Groupe Spécial Mobile*)
- **GPRS** (*General Packet Radio Service*)
- **UMTS** (*Universal Mobile Telecommunication System*)

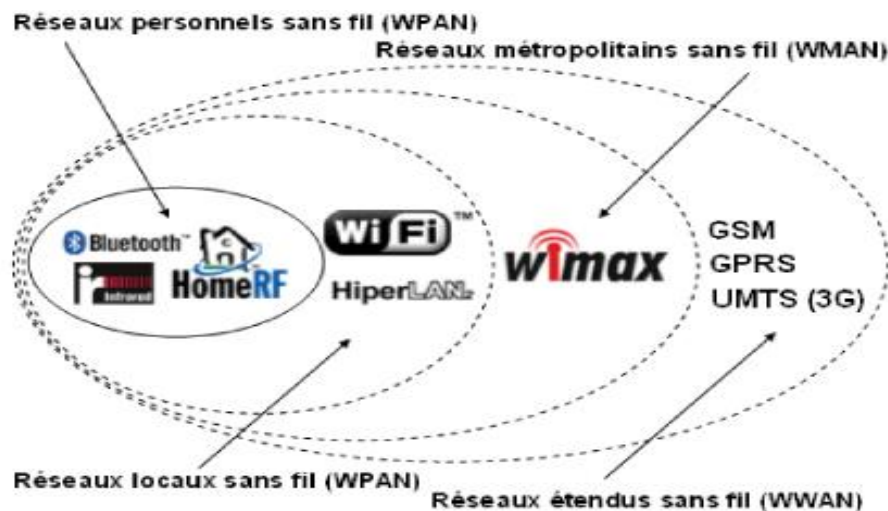


Figure I.3 : Les technologies et la classification des RSF selon leur taille. [4]

I.2.2.2. **Classification selon l'infrastructure :**

Les environnements mobiles sont des systèmes composés de sites mobiles et qui permettent à leurs utilisateurs d'accéder à l'information indépendamment de leurs positions géographiques. Les réseaux mobiles ou sans fil, peuvent être classés en deux classes: les réseaux avec infrastructure et les réseaux sans infrastructure.

A. **Les réseaux Cellulaire (avec infrastructure) :**

Un réseau cellulaire est un réseau radio distribué sur terre à travers des cellules où chaque cellule comprend un émetteur-récepteur à emplacement fixe appelé station de base. Ensemble, ces cellules assurent une couverture radio sur de plus grandes zones géographiques. L'équipement utilisateur (UE), tel que les téléphones mobiles, est donc en mesure de communiquer même si l'équipement se déplace à travers les cellules pendant la transmission.

Les réseaux cellulaires offrent aux abonnés des fonctionnalités avancées par rapport aux solutions alternatives, notamment une capacité accrue, une faible consommation d'énergie de la batterie, une zone de couverture géographique plus large et une interférence réduite avec d'autres signaux. Les technologies cellulaires populaires comprennent le Système mondial de communication mobile, le service général de radio par paquets, le 3GSM et l'accès multiple par division de code.

Dans cette catégorie, on trouve les réseaux **WLAN** (Wi-Fi), **WMAN** (WiMAX) et **WWAN** (GSM). [4]

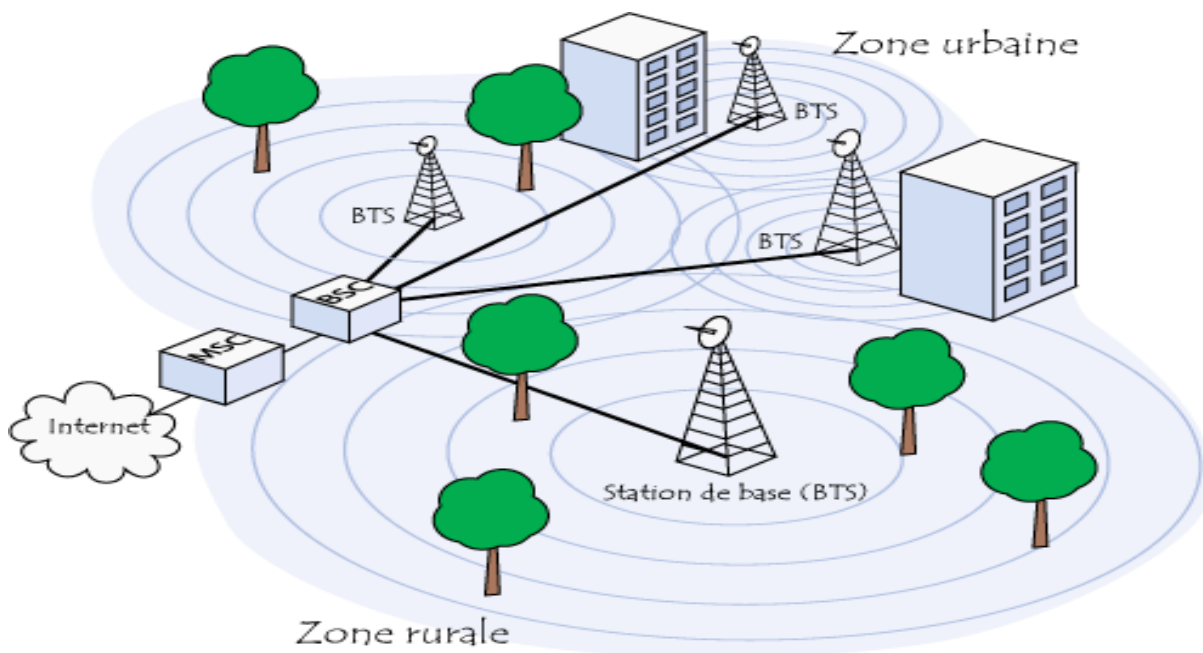


Figure I.4: Un Réseau Cellulaire. [4]

B. Les Réseaux Ad Hoc (sans infrastructure) :

Un **réseau sans fil ad hoc** ou **WANET** (Wireless Ad Hoc Network) ou **MANET** (Mobile Ad Hoc Network) est un type de réseau sans fil décentralisé.

Il ne s'appuie pas sur une infrastructure préexistante, comme des routeurs dans les réseaux filaires ou des points d'accès dans les réseaux sans fil administrés. Au lieu de cela, chaque nœud participe au routage en retransmettant les données aux autres nœuds, de façon que le choix du nœud qui va transmettre les données est opéré dynamiquement sur la base de la connectivité du réseau et de l'algorithme de routage utilisé.

Dans le système d'exploitation Windows, le ad-hoc est un mode de communication (paramètre) qui permet aux ordinateurs de communiquer directement entre eux sans routeur. [5]

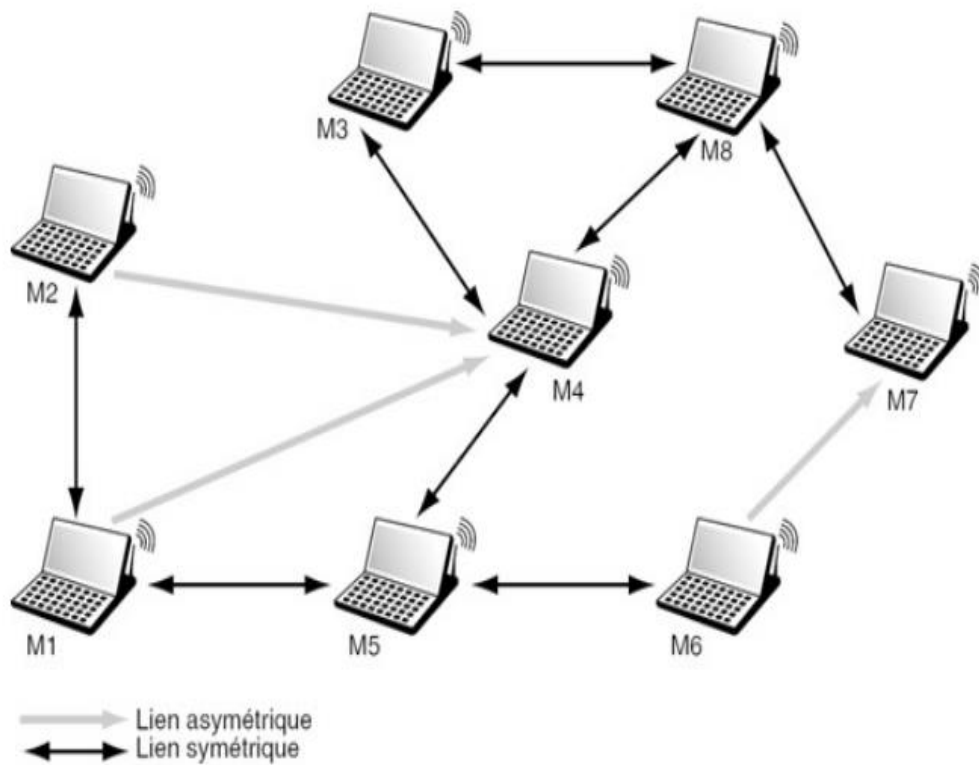


Figure I.5 : Un Réseau Ad Hoc.

I.3. Les Réseaux de capteurs sans fil :

I.3.1. Définitions :

Un **capteur** réalise l'acquisition d'une grandeur physique (température, luminosité, présence, distance, ...) qu'il transforme en un signal électrique. L'interface reçoit les informations des capteurs, les traite et envoie des ordres aux actionneurs. [6]

Un **réseau de capteurs sans fil** est un réseau *ad hoc* avec un grand nombre de **nœuds** qui sont des micro-capteurs capables de récolter et de transmettre des **données** environnementales d'une manière autonome. La position de ces nœuds n'est pas obligatoirement prédéterminée. Ils peuvent être aléatoirement dispersés dans une zone géographique, appelée « *champ de captage* » correspondant au terrain d'intérêt pour le phénomène capté. En plus d'applications civiles, il existe des applications militaires aux réseaux de capteurs (détection d'intrusions, localisation de combattants, véhicules, armes, etc. sur un **champ** de bataille, sous l'**eau**, dans l'espace, dans le sol...). [7]

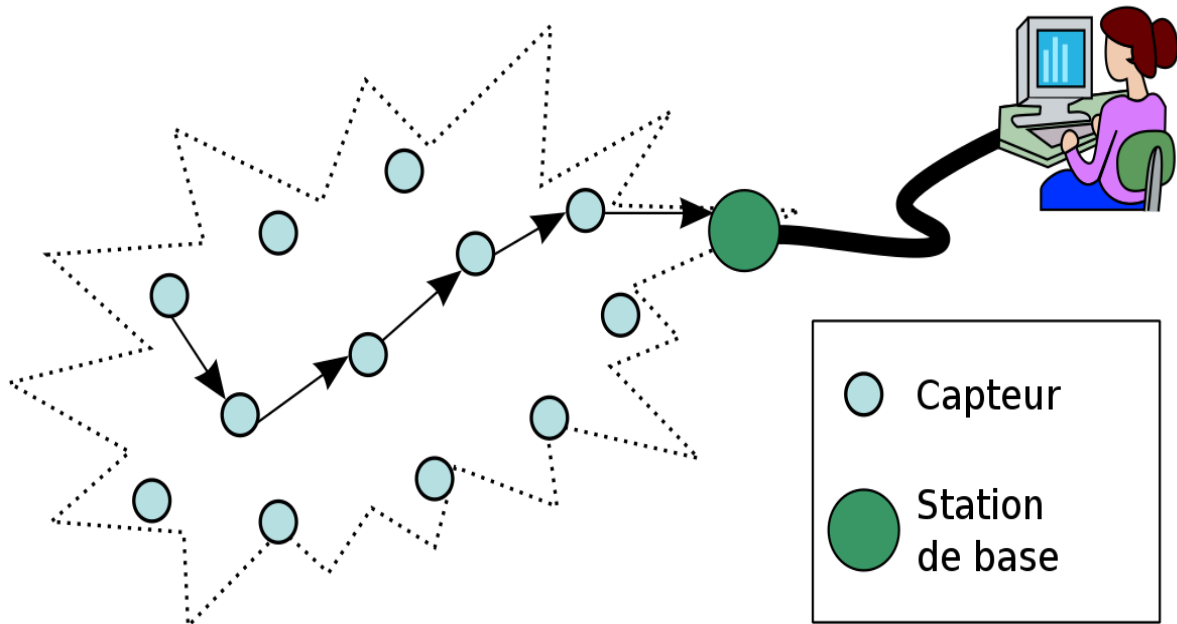


Figure I.6: un RCSF

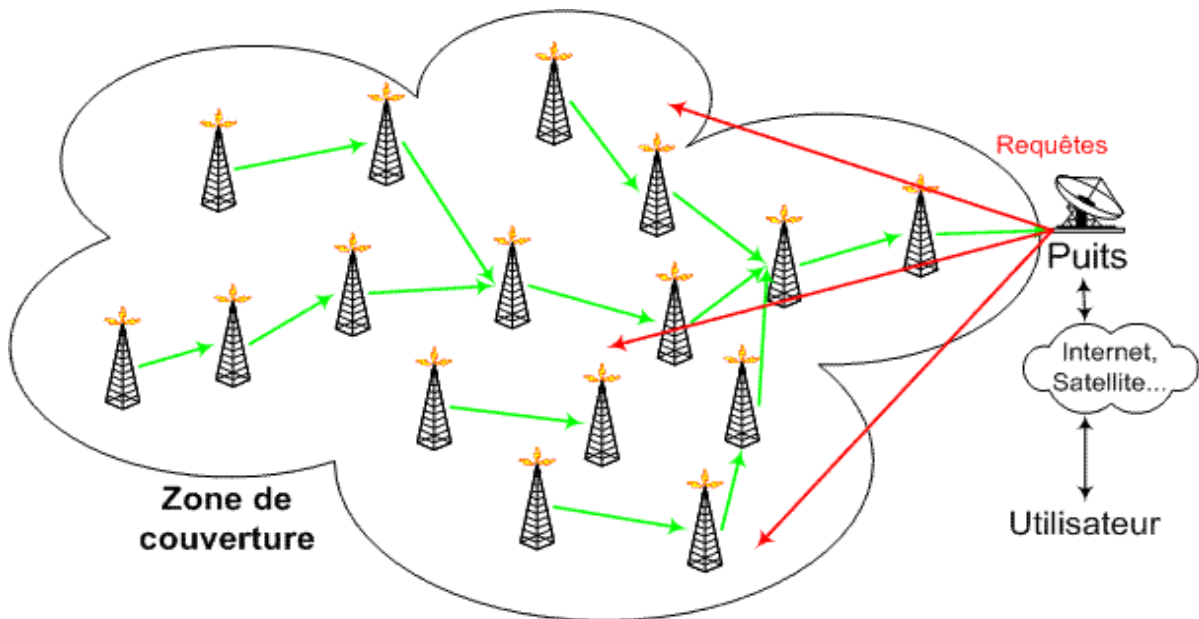


Figure I.7: les réseaux de capteurs sans fil

I.3.2. Historique :

Jusque dans les années 1990, hormis pour quelques balises radio, pour acheminer les données d'un capteur au *contrôleur central* il fallait un câblage coûteux et encombrant.

De nouveaux réseaux de capteurs sont apparus dans les années 1990, notamment dans les domaines de l'environnement et de l'industrie, permis par les récents progrès du domaine des techniques sans-fils (wireless). Aujourd'hui, grâce aux récents progrès des techniques sans-fils, de nouveaux produits exploitant des réseaux de capteurs sans-fil sont employés pour récupérer ces données environnementales. [8]

I.3.3. Architecture d'un RCSF :

Un RCSF est composé d'un ensemble de noeuds capteurs. Ces noeuds capteurs sont organisés en champs « sensor fields » (voir figure suivante). Chacun de ces noeuds a la capacité de collecter des données et de les transférer au noeuds passerelle (dit "sink" en anglais ou puits) par l'intermédiaire d'une architecture multi-sauts. Le puits transmet ensuite ces données par Internet ou par satellite à l'ordinateur central «Gestionnaire de taches» pour analyser ces données et prendre des décisions. [9]

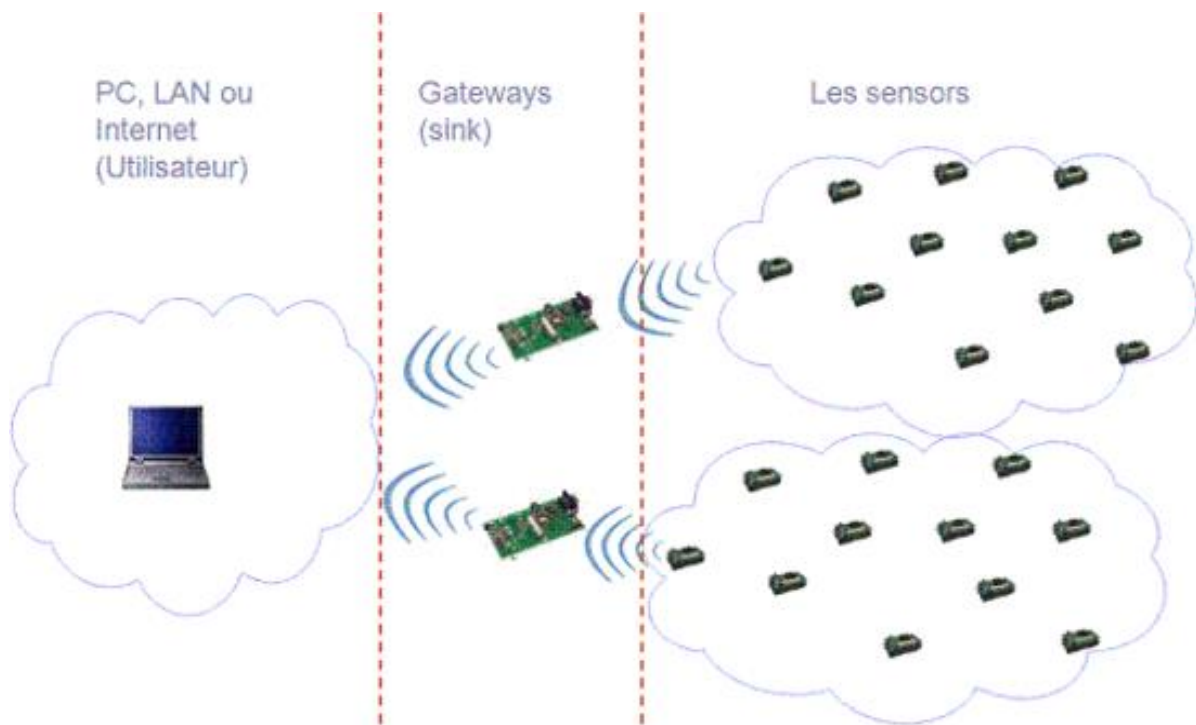


Figure I.8: L'architecture d'un RCSF

I.3.4. Caractéristique réseaux de capteurs sans fil :

Par ailleurs les caractéristiques essentielles des RCSF s'établissent comme suit :

Scalabilité et adaptabilité: Importance des nombres de nœuds qui peut parfois atteindre des millions en vue d'une meilleure granularité de surveillance, avec une polyvalence de remplacement en cas de défaillance.

Caractéristiques du trafic interrompu: L'accès sans fil est perturbé pas les interférences inévitables au sein d'un RCSF (Exp : perturbation des liens radio dans un hôpital).

Réseaux multi-sauts: Les RCSF adoptent des communications multi saut en raison des limitations des ressources physique s dues à la miniaturisation des composants électroniques

Réduction de la consommation de l'énergie : La gestion de l'énergie au sein d'un RCSF est limitée du fait que les capteurs sont alimentés par des batteries qui ne peuvent être changées par suite des milieux hexogènes défavorables (sachant que le rechargement des batteries est très onéreux et donc très peu rentable d'un point de vue économique).

Différents types de déploiements : Engendrent des conséquences qui diffèrent d'un déploiement à un autre :

- Le déploiement dans la nature mène à une absence de sécurité physique causée par la présence d'intrus ou de capture de nœuds.
 - Le déploiement dans un lieu précis exige une topologie préconfiguré.
 - Le déploiement aléatoire demande des algorithmes d'auto organisation.
- [10]

I.3.5. Types de réseaux de capteurs sans fil :

I.3.5.1. Réseaux de poursuite :

Ces réseaux sont généralement développés par l'armée, ils peuvent servir à surveiller toutes les activités d'une zone stratégique ou d'accès difficile, ainsi on pourra détecter des agents chimiques, biologiques ou des radiations avant des troupes. On peut aussi penser à des capteurs embarqués sur les soldats pour faciliter leur guidage et le contrôle de leur position depuis la base.

I.3.5.2. Réseaux de collection des données d'environnement :

Les nœuds de ce type de réseau peuvent avoir plusieurs fonctionnalités et différents types de capteurs. Ce type de réseau nécessite généralement un flux de données faible, une durée de vie importante ; il sert à la collecte périodique des données environnementales puis leur transmission vers la station de base.

I.3.5.3. Réseaux de surveillance et sécurité :

La différence entre ce réseau et le réseau de collection des données d'environnement est que les nœuds ne transmettent pas l'ensemble des données collectées mais seulement les rapports concernant une violation de la sécurité. Ce sont en général des nœuds fixes qui contrôlent d'une façon continue la détection d'une anomalie dans le fonctionnement d'un système.

Ainsi les altérations dans la structure d'un bâtiment, suite à un séisme, pourraient être détectées par des capteurs intégrés dans les murs ou dans le béton, sans alimentation électrique ou autres connexions filaires. [11]

I.3.6. Les protocoles de routage dans les RCSF :

Les protocoles de routage pour les RCSF 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 :

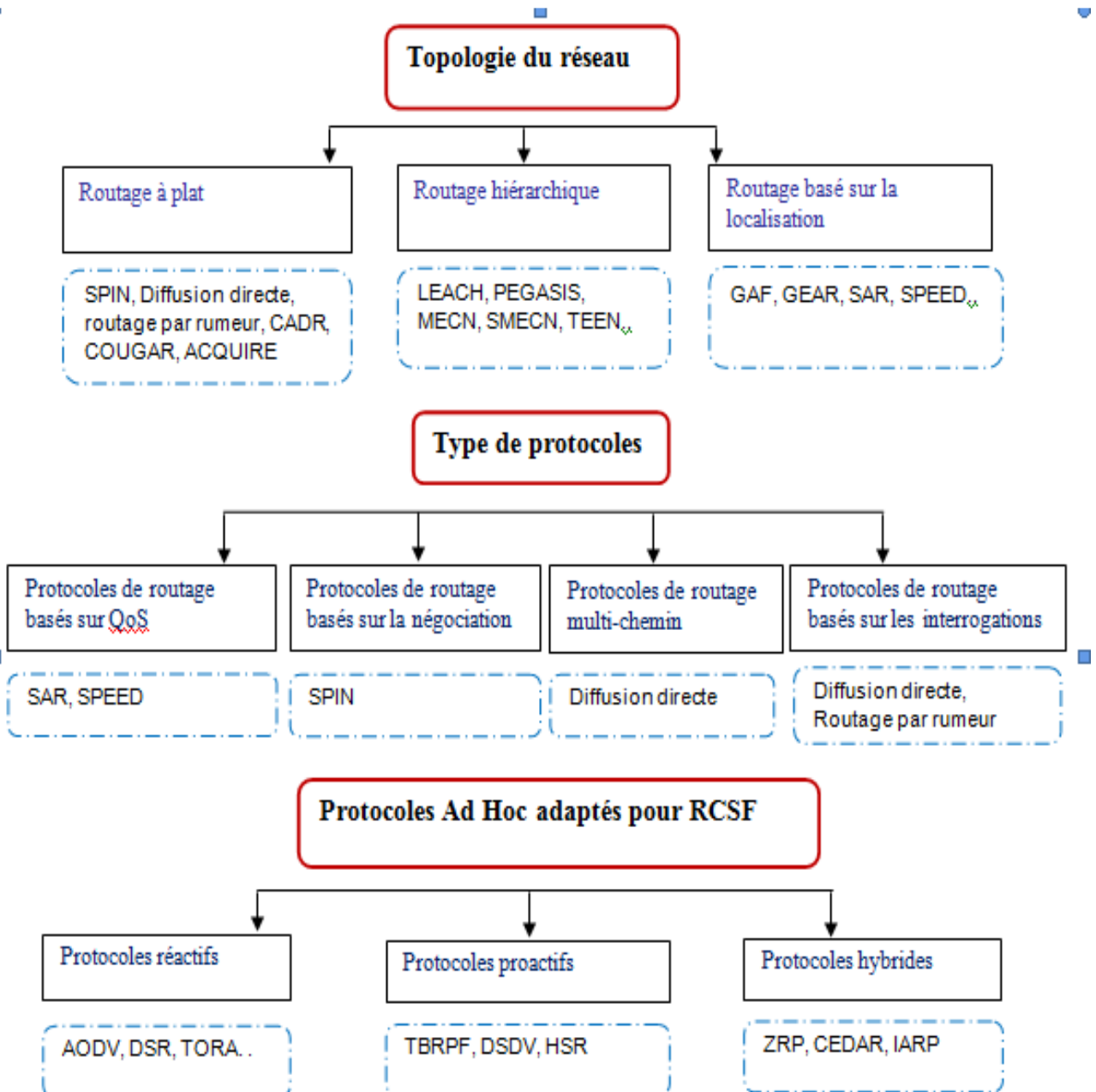


Figure I.9: Classification des protocoles de routage dans les RCSF

I.3.6.1. Selon leur Topologie du Réseau :

A. Routage plat :

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.

B. Routage 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.

C. Routage basé 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.

I.3.6.2. Selon leur Type de protocoles :

A. Protocoles de routage basés sur la qualité de service :

Dans ce type de protocole de routage, la qualité de service et l'énergie consommée doivent être maintenues dans le réseau. Chaque fois que le puits demande des données des nœuds dans le réseau, la transmission des données doit satisfaire certains paramètres de qualité de service, tels que, la latence (les données doivent être envoyées dès qu'elles sont détectées) et la bande passante consommée. Le protocole SAR (Sequential Assignment Routing) est l'un des premiers protocoles qui assure la qualité de service dans les réseaux de capteurs.

B. Protocoles de routage basés sur la négociation :

Ces protocoles utilisent des descripteurs de haut niveau codés en haut niveau afin d'éliminer la transmission des données redondantes. Chaque nœud effectue un suivi de la consommation de ses ressources ce qui influence ses décisions lors des

négociations. Les négociations se font à travers des paquets d'avertissement, de requête et de données.

C. Protocoles de routage multi-chemins :

Ces protocoles sont efficaces pour la gestion de plusieurs chemins. Les nœuds envoient les données collectées sur plusieurs liens au lieu d'un seul. Cela permet une bonne fiabilité et une bonne tolérance aux pannes dans le réseau car il existe un chemin alternatif lorsque le chemin primaire échoue.

D. Protocoles de routage basés sur les interrogations :

Le routage basé sur les interrogations propage les requêtes émises par la station de base. La station de base envoie des requêtes demandant certaines informations des nœuds du réseau, le nœud, qui est responsable de la détection et de la collecte des données, lit ces requêtes et s'il y a égalité avec les données demandées dans la requête commencent à envoyer les données à la station de base.

I.3.6.3. Protocoles Ad Hoc adaptés pour RCSF :

A. Protocoles réactifs :

Ce sont des protocoles qui calculent la route sur demande avant d'effectuer le routage et n'ont pas besoin de connaître la topologie du réseau ou d'échanger périodiquement des informations sur le routage. L'aspect « sur demande » du routage élimine la nécessité de mettre à jour la route, mais augmente le délai de démarrage du routage à cause du temps de découverte de la route. Plusieurs protocoles ont été développés dans cette catégorie, on peut citer l'AODV, le DSR, TORA ...

B. Protocoles proactifs :

Les protocoles proactifs effectuent un calcul de toutes les routes possibles avant d'effectuer le routage. Les nœuds maintiennent une information sur la topologie du réseau sous forme de tables de routage, et ce, de façon périodique ou suite à un événement. Ce genre de protocoles consomme beaucoup de ressources du réseau, du fait de la connaissance préalable de la topologie. Il existe plusieurs protocoles proactifs, tels que, le TBRPF , DSDV et le HSR.

C. Protocoles hybrides :

À chaque fois qu'un nœud a besoin de router une information, d'abords, calcule toutes les routes possibles avec la méthode proactive ensuite s'adapte pendant le routage avec la méthode réactive. [12]

I.3.7. Applications des RCSF :

Les RCSF peuvent avoir beaucoup d'applications (voir figure suivantes). Parmi elles, je cite :

Découvertes de catastrophes naturelles : On peut créer un réseau autonome en dispersant les nœuds dans la nature. Des capteurs peuvent ainsi signaler des événements tel que feux de forêts, tempêtes ou inondations. Ceci permet une intervention beaucoup plus rapide et efficace des secours.

Détection d'intrusions : En plaçant, à différents points stratégiques, des capteurs, on peut ainsi prévenir des cambriolages ou des passages de gibier sur une voie de chemin de fer (par exemple) sans avoir à recourir à de coûteux dispositifs de surveillance vidéo.

Applications métier : On pourrait imaginer devoir stocker des denrées nécessitant un certain taux d'humidité et une certaine température (min ou max). Dans ces applications, le réseau doit pouvoir collecter ces différentes informations et alerter en temps réel si les seuils critiques sont dépassés.

Contrôle de la pollution : On pourrait disperser des capteurs au-dessus d'un emplacement industriel pour détecter et contrôler des fuites de gaz ou de produits chimiques. Ces applications permettraient de donner l'alerte en un temps record et de pouvoir suivre l'évolution de la catastrophe.

Agriculture : Des nœuds peuvent être incorporés dans la terre. On peut ensuite questionner le réseau de capteurs sur l'état du champ (déterminer par exemple les secteurs les plus secs afin de les arroser en priorité). 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.

Surveillance médicale : En implantant sous la peau de mini capteurs vidéo, on peut recevoir des images en temps réel d'une partie du corps sans aucune chirurgie pendant environ 24h. On peut ainsi surveiller la progression d'une maladie ou la reconstruction d'un muscle.

Contrôle d'édifices : On peut inclure sur les parois des barrages des capteurs qui permettent de calculer en temps réel la pression exercée. Il est donc possible de réguler le niveau d'eau si les limites sont atteintes. On peut aussi imaginer inclure des capteurs entre les sacs de sables formant une digue de fortune. La détection rapide d'infiltration d'eau peut servir à renforcer le barrage en conséquence. Cette technique peut aussi être utilisée pour d'autres constructions tels que ponts, voies de chemins de fer, routes de montagnes, bâtiments et autres ouvrages d'art. [13]

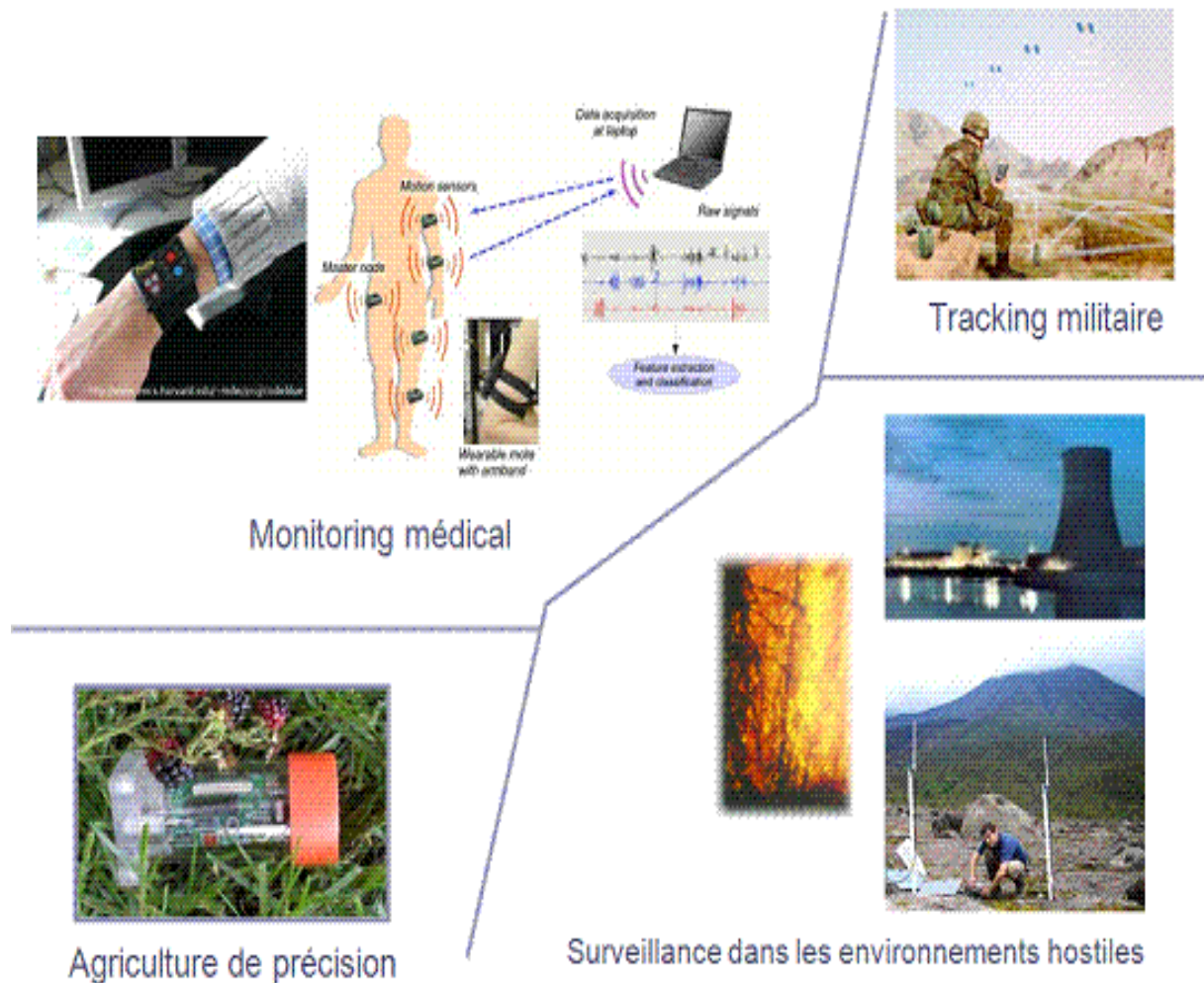


Figure I.10 : Les applications des RCSF.

I.3.8. Comparaison entre les réseaux Ad hoc classiques et les réseaux de capteurs :

Les réseaux de capteurs sans fil sont apparentés aux réseaux ad hoc. En effet, ces deux types de réseaux ont de nombreux points communs. La ressemblance que nous pouvons remarquer immédiatement est que les deux sont des réseaux sans fil distribués avec une infrastructure pas toujours bien définie. Des chercheurs dans le domaine des MANET se sont consacrés à cette ressemblance, mais aussi à d'autres similarités comme la limitation d'énergie, de mémoire et de capacité de calcul. Ils essaient d'apporter leur savoir-faire et d'adapter aux RCSF (Réseaux de Capteurs Sans Fil) les algorithmes, protocoles et techniques dédiés initialement aux MANET.

Cependant, Ces deux classes de réseaux sans fil se différencient sur plusieurs aspects, nous résumons les principales différences dans le tableau suivant : [14]

Réseaux Ad-Hoc Classiques	Réseaux de capteurs
<ul style="list-style-type: none"> ➤ Mobile, portable... ➤ Génériques ➤ Chaque nœud à son propre objectif ➤ Flot de données any- to- any ➤ Communication point à point ➤ La qualité de service est majeure ➤ Mobilité ➤ Aucun nœud central 	<ul style="list-style-type: none"> ➤ Petits capteurs ➤ Objectifs ciblés ➤ Nœuds collaborent pour atteindre un objectif Commun ➤ Flot de données Many –to- one ➤ Utilisation du broadcast ➤ Energie est un facteur déterminant ➤ Mobilité faible ➤ Station de base (coordination)

TAB I.1 : Comparaison entre les réseaux Ad hoc classiques et les réseaux de capteurs.

I.3.9. Différentes problématiques présentes dans les RCSF :

Les axes de recherche dans les réseaux de capteurs sans-fil sont de caractère pluridisciplinaire, ils touchent les domaines de l'informatique, de l'automatique, du traitement du signal, de l'électronique, des nanotechnologies et des mathématiques. Les recherches dans le domaine des réseaux de capteurs ont révélé plusieurs problématiques, parmi ces problématiques on peut citer :

Routage : Le routage dans les réseaux de capteurs est une problématique importante. Les protocoles de routage des réseaux filaires ne sont pas adaptés aux réseaux de capteurs. On peut facilement imaginer le nombre de mises à jour nécessaires lors du déploiement de 50 nouveaux capteurs dans une topologie de plusieurs milliers d'autres. L'un des principaux avantages du routage sur un ensemble dominant est qu'il est supporté par seulement une partie des nœuds du réseau. Seuls ces nœuds maintiennent des informations de routage et eux seuls auront à les mettre à jour en cas de modification de la topologie.

Consommation d'énergie : L'énergie est considérée comme une ressource rare dans les applications de réseaux de capteurs sans-fil. En effet, les nœuds généralement utilisent des batteries, souvent non rechargeables, et généralement n'ont pas de mécanismes de production d'électricité. Il est communément dit que les applications pour lesquelles les réseaux de capteurs sont focalisés suggèrent que le changement des batteries est difficile ou impossible. Selon l'application, les nœuds pourraient être dans des endroits difficiles d'accès, sur un champ de bataille, et ainsi de suite. Il en résulte que l'efficacité de la gestion de l'emploi de l'énergie disponible est une question souvent vitale pour le réseau.

Ressources limitées : La demande exige une tendance vers la miniaturisation des nœuds, ainsi que vers l'élargissement de la durée de vie et la baisse du prix des unités. Les nœuds ont donc des ressources extrêmement limitées, en comparaison avec l'équipement informatique que on a de nos jours (tels que les ordinateurs portatifs et les PDAs (Personal Digital Assistant), etc.), en termes de mémoire disponible, de capacité et de vitesse de traitement, de débit, etc. En effet, des caractéristiques comme la haute vitesse de traitement et de transmission de données, ou une grande capacité de mémoire, sont des facultés qui amènent à une consommation énergétique très importante. Si on veut avoir de capteurs de taille microscopique, de faible consommation d'énergie et de faible coût de fabrication, on ne peut pas utiliser de microcontrôleurs ou transmetteurs radio de haute vitesse.

Dimension et densité du réseau : Les réseaux de capteurs sont considérés comme des réseaux de très grande dimension, de l'ordre de plusieurs centaines à plusieurs milliers de nœuds, déployés de manière dense (chaque nœud peut avoir plusieurs dizaines de voisins). La forte densité du réseau peut entraîner des problèmes de congestion, si les nœuds essaient de communiquer au même moment, donc des retards dans la diffusion de messages et des pertes de paquets. La densité du réseau est généralement mise à profit pour partager le temps de travail entre les capteurs proches, et ainsi augmenter la durée de vie du réseau. Le facteur d'échelle est également important pour la conception des protocoles de communication et des traitements de données. Le routage de paquets doit être effectué d'une manière économique en énergie, sans pour autant que les nœuds soient obligés de minoriser toutes les routes possibles. Pour maîtriser la quantité d'information à faire remonter au puits, des algorithmes de fusion de données sont aussi à envisager.

Environnement de communication non contrôlable : Il est habituel dans la littérature de prendre l'exemple d'un réseau de nœuds de capteurs déployé en larguant les capteurs depuis un avion. Pour ce type de déploiement, le positionnement des capteurs n'est pas contrôlé, de sorte que le réseau doit faire face à des problèmes de connectivité d'un certain nombre de nœuds qui se retrouvent en dehors de la zone de couverture des autres nœuds, soit parce qu'ils sont trop éloignés, soit parce qu'ils sont tombés dans des lieux qui entravent la propagation des ondes radio ou tout simplement parce qu'ils ont été détruits. Les réseaux de capteurs héritent de tous les problèmes de l'usage d'une communication sans-fil, tels que des problèmes d'interférences et des problèmes de sécurité (attaques). Les signaux radio émis par les nœuds peuvent être sérieusement endommagés par les interférences présentes dans le milieu. Les basses fréquences peuvent être perturbées par le bruit des machines ou d'autres agents que ne sont pas nécessairement communicants, tandis que les hautes fréquences sont perturbées par d'autres équipements communicants que utilisent les mêmes bandes de fréquences [15].

Topologie dynamique : Les réseaux de capteurs sont des réseaux dont la topologie peut changer très fréquemment. Ces changements topologiques peuvent être dus à la mobilité des nœuds. Mais même pour les applications où les nœuds sont fixes, des changements peuvent se produire lorsque des nœuds sont ajoutés ou enlevés, soit par action directe de l'utilisateur, soit par le basculement de l'état des nœuds (actif/endormi), soit par l'épuisement de l'énergie, ou la panne des nœuds. Ce changement aléatoire de la disposition des nœuds exige que les nœuds puissent s'auto-organiser et cela passe par des méthodes efficaces en énergie et robustes au facteur d'échelle.

Qualité de service : Des protocoles au niveau de la couche MAC devraient être capables d'établir des priorités entre les flux, limiter les pertes de paquets vitaux pour la gestion du réseau, ou du moins en restreindre l'impact.

Diffusion de l'information : Les protocoles de diffusion conçus pour les réseaux de capteurs doivent tenir compte de leurs spécificités ainsi que de leurs contraintes intrinsèques imposées. Ainsi, pour concevoir un protocole efficace, il faudrait assurer une couverture maximale des capteurs composant le réseau (taux d'accessibilité supérieur 90%), minimiser le nombre des réémetteurs et des réceptions redondantes ainsi que la consommation d'énergie.

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 de leur communauté. Les algorithmes de cryptographie conçus pour les réseaux de capteurs doivent tenir compte des ressources limitées que présentent ces réseaux. [16]

I.4. Conclusion :

Les réseaux de capteurs sans fil sont une technologie récente. Les progrès de miniaturisation et d'allongement de la durée de vie des batteries, annoncent un futur prometteur à cette technologie. De plus, le développement de nouveaux capteurs permettra d'étendre les domaines d'applications déjà nombreux.

CHAPITRE II:

La tolérance des pannes dans les réseaux de capteurs sans fil.

II.1. Introduction :

L'expansion des réseaux de capteurs sans fil n'a cessé de s'accroître ces dernières décennies. Ceci a permis de généraliser leur utilisation dans différents domaines applicatifs (médicales, environnementales, militaires, etc.). Malgré la diversité de ces applications et leurs exigences (nature de trafic, contraintes de débit, de délai,...), elles requièrent toutes que le réseau sous-jacent soit suffisamment robuste et fiable pour assurer les fonctions de base d'un RCSF à savoir la couverture et la connectivité. Il en résulte que quelle que soit l'application choisie, le RCSF en question est tenu d'assurer un degré de tolérance aux pannes selon la criticité de l'application afin de garantir son bon fonctionnement. Ainsi, plusieurs solutions et mécanismes ont été proposés dans la littérature pour assurer le recouvrement de pannes dans les RCSFs que je propose d'étudier dans le présent chapitre.

J'entame mon étude par l'identification de différentes catégories de pannes qui peuvent survenir au niveau d'un RCSF. Ensuite, je présente les classifications des techniques de tolérance aux pannes dans les RCSFs selon différents critères. J'ai veillé tout au long du chapitre à différencier les procédures et les classifications des solutions de la tolérance aux pannes dans les réseaux de capteurs sans fil.

II.2. Les panne :

Une panne du système se produit lorsque son comportement devient inconsistant et ne fournit pas le résultat voulu. La panne est une conséquence d'une ou plusieurs erreurs où une erreur représente un état invalide du système dû à une faute (défaut). La faute est donc la première cause de l'erreur, cette dernière provoque la faille du système. [17]

II.3. Origines des pannes dans les RCSFs :

En général, un RCSF est déployé soit pour collecter d'informations d'une zone d'intérêt, soit pour détecter un événement.

Selon l'application, une perturbation de l'une des tâches du réseau peut affecter la qualité du service livré. Ainsi, nous considérons toute faute ou erreur qui empêche un nœud du RCSF de capturer et/ou transmettre comme étant une panne.

Dans cette partie, nous allons classier les différentes pannes qui peuvent se produire au niveau d'un RCSF, en précisant leurs origines ainsi que l'impact que cela peut avoir sur le réseau. Deux classifications peuvent être appliquées sur les pannes des RCSFs : une première classification de point de vue composant du réseau et une deuxième classification de point de vue système. D'un point de vue composant du réseau, une panne peut se produire en raison des problèmes au niveau du nœud capteur, du nœud puits ou du réseau ; alors que d'un point de vue système, la panne

est classée selon la couche où elle a eu lieu : couche matérielle, couche logicielle, couche de communication du réseau ou couche application. [18]

II.3.1. Pannes de point de vue composant :

Pannes du nœud capteur : La panne d'un nœud survient en raison de la défaillance du matériel (unité de capture, CPU, mémoire, interface réseau, batterie, etc.) ou du logiciel (routage, MAC et application).

De plus, une panne du matériel peut mener à une défaillance logicielle. Par exemple, si l'énergie d'un nœud tombe en-dessous d'un certain seuil, l'unité de capture peut fournir des lectures incorrectes. Cependant, certains services du nœud peuvent toujours continuer à fonctionner correctement. À titre d'exemple, un nœud peut être toujours utilisé pour acheminer des données même si son unité de capture est défaillante. Comme l'épuisement de la ressource énergétique est une panne très fréquente dans les RCSFs, tout mécanisme qui minimise la consommation d'énergie et qui prolonge la durée de vie des nœuds est considéré comme une solution de tolérance aux pannes préventive dans les RCSFs.

Pannes du réseau : Les applications, qui utilisent de RCSFs, exigent la collecte d'informations des nœuds capteurs et la transmission des données vers un ou plusieurs nœuds puits. Cette tâche peut être perturbée par l'occurrence de certaines pannes au niveau des liens entre les nœuds du réseau. Dans les RCSFs, la nature des liens sans fil les rend propices aux erreurs en raison de beaucoup de facteurs comme les interférences entre les nœuds du même réseau ou avec des nœuds de réseaux différents ainsi que les collisions entre les paquets, ce qui mène à la perte des données transmises. Comme une deuxième source d'erreurs, un mauvais choix des routes par le protocole de routage peut considérablement altérer le bon fonctionnement du réseau. Par exemple, si le trafic passe essentiellement par des routes où les liens sont de très mauvaise qualité alors le taux de perte des paquets sera très important et les performances du réseau seront dégradées. Par ailleurs, le protocole de routage doit respecter les exigences de l'application pendant la sélection des routes. Par exemple, une application de collecte périodique de données tolère le retard généré par la sélection d'une nouvelle route, tandis qu'une application d'alerte exige que les données atteignent le nœud puits dans un temps très court même en présence des pannes. De plus, le fait que les données doivent être toujours envoyées au nœud puits soulève l'importance de la connectivité dans les RCSFs.

Pannes du nœud puits : Le nœud puits est un composant essentiel dans un RCSF. Sa panne mène à la panne du réseau en entier si aucun mécanisme de tolérance aux pannes n'est mis en œuvre. Comme pour un nœud capteur, les erreurs au niveau du puits peuvent survenir aussi bien au niveau du matériel que du logiciel. Cependant, contrairement aux nœuds capteurs, le nœud puits n'a aucune contrainte énergétique.

II.3.2. Pannes de point de vue système :

Pannes de la couche matérielle : Dans cette couche, les erreurs sont le résultat de la défaillance d'un ou de plusieurs composants du capteur, à savoir la mémoire, la batterie, l'unité de capture et la radio sans fil. Il y a trois raisons de base qui causent la panne : la qualité des composants, l'énergie limitée qui peut aboutir à des lectures incorrectes quand elle chute en-dessous d'un certain seuil ; et finalement, l'environnement hostile dans lequel le réseau est déployé.

Pannes de la couche logicielle : Cette couche est représentée par deux composants : le logiciel du système (le système d'exploitation) et le middleware (incluant communication, routage et agrégation des données). Les bogues sont la source d'erreurs principale dans cette couche. Une solution à envisager est d'implémenter des versions différentes de chaque programme. Par exemple, au niveau middleware, un grand nombre de protocoles sont conçus pour assurer la tolérance aux pannes.

Pannes de la couche communication du réseau : Cette couche est l'une des couches les plus critiques du RCSF en raison des liens de communication sans fil qui peuvent être enclins à la panne. Les fautes peuvent être causées par les environnements dangereux et par les interférences entre les nœuds capteurs eux-mêmes ou les réseaux coexistants. Une méthode pour surmonter ces problèmes et améliorer la performance de la communication est d'utiliser des méthodes de correction d'erreur, des mécanismes de retransmission et de la communication multi-canal.

Pannes de la couche application : Nous ne pouvons pas appliquer les mêmes techniques pour toutes les applications. En effet, chaque application spécifie son propre degré de tolérance aux pannes en se basant sur ses exigences qui peuvent être différentes des exigences des autres applications. La couverture et la connectivité représentent les deux exigences les plus importantes pour les applications. Leur importance diffère d'une application à une autre. [18]

II.4. Classification des pannes :

Il est utile de classer les pannes selon différents critères. Le schéma suivant montre une classification générale selon la durée, la cause ou le comportement d'une panne :

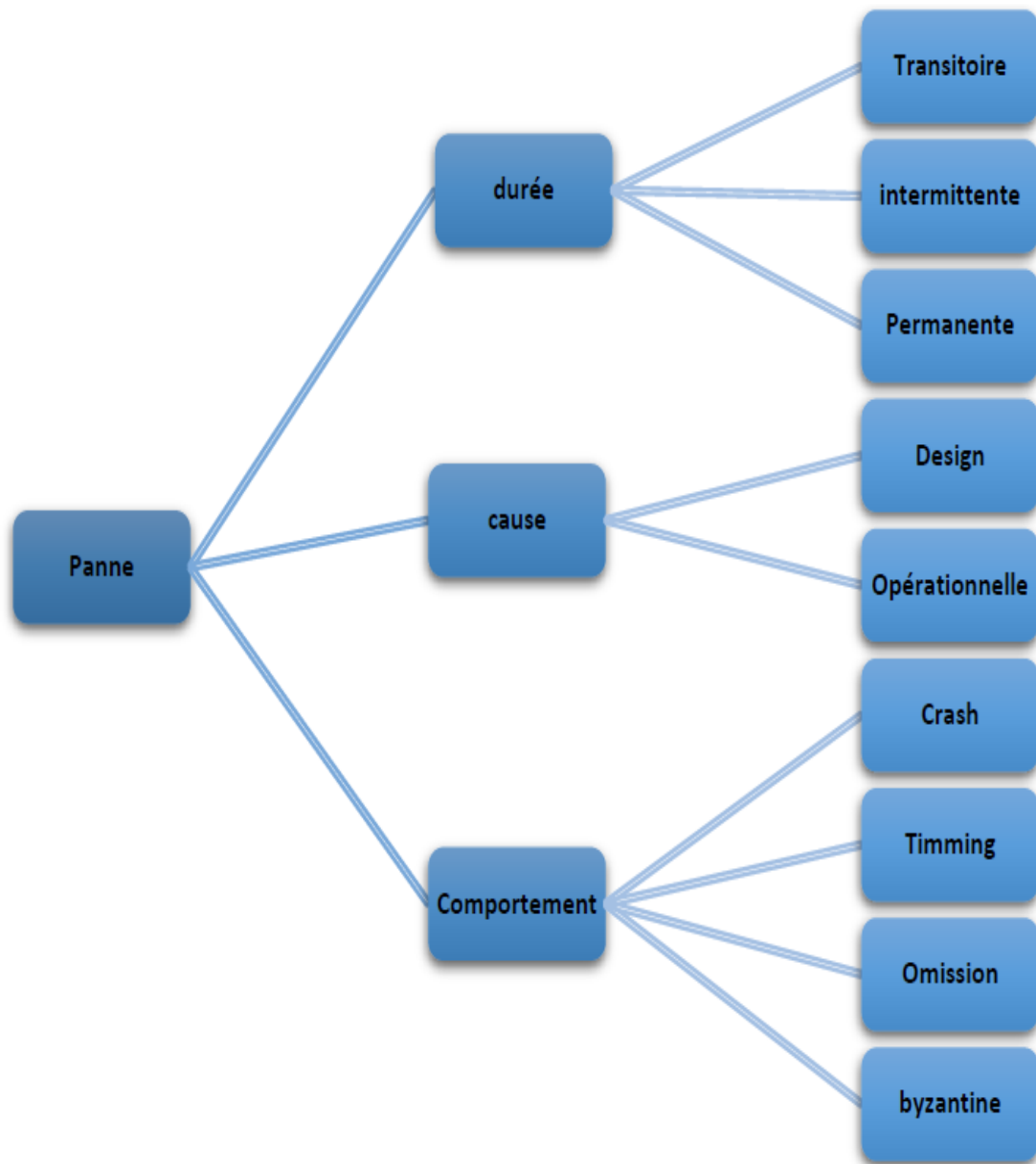


Figure II.1 : Classification des pannes .

II.4.1. Panne selon la durée :

Basée sur sa durée, la panne peut être classifiée en :

- **Transitoire** : conséquence d'un impact environnemental temporaire, elle peut éventuellement disparaître sans aucune intervention.
- **Intermittente** : variante de la panne transitoire, elle se produit occasionnellement et de façon imprévisible. Elle est généralement due à l'instabilité de certaines caractéristiques matérielles ou à l'exécution du programme dans un espace particulier de l'environnement.

- **Permanente** : continue et stable dans le temps, la panne permanente persiste tant qu'il n'y a pas d'intervention externe pour l'éliminer. Un changement physique dans un composant provoque une panne matérielle permanente.

II.4.2. Panne selon la cause :

On distingue deux types de pannes selon leur cause :

- **Panne de design** : due à une mauvaise structuration du réseau ou du composant en particulier. En pratique, ce genre de panne ne devrait pas exister grâce aux tests et simulations avant la réalisation finale du réseau.
- **Panne opérationnelle** : qui se produit durant le fonctionnement du système. Elle est généralement due aux causes physiques. En outre, on peut distinguer, spécialement pour les réseaux de capteurs, trois principales causes :

- **Energie** : l'épuisement de la batterie cause l'arrêt du capteur. La consommation d'énergie est très importante pour déterminer la durée de vie d'un noeud capteur, et donc de tout le réseau ;

- **Sécurité** : la destruction physique accidentelle ou intentionnelle par un ennemi peut être une cause de panne. L'absence de sécurité dans les réseaux de capteurs augmente le risque des pannes de ce type ;

- **Transmission** : la nature vulnérable de transmission radio, la présence d'obstacles dans les environnements hostiles ainsi que les interférences électriques peuvent être la source d'une faute lors du transfert de données.

II.4.3. Panne selon le comportement résultat :

Après l'occurrence d'une panne, on distingue quatre différents comportements possibles du composant concerné :

- **Panne accidentelle (Crash)** : le composant soit, s'arrête complètement de fonctionner ou bien continue mais sans retourner à un état stable (valide).
- **Panne d'omission** : le composant n'est plus capable d'améliorer son service (échec total).
- **Panne de synchronisation (Timing)** : le composant effectue son traitement mais fournit le résultat en retard.
- **Panne Byzantine** : cette panne est de nature arbitraire ; le comportement du composant est donc imprévisible. Due à des attaques très malicieuses, ce type de pannes est considéré le plus difficile à gérer. [19]

II.5. Causes des pannes :

Les capteurs peuvent subir des pannes et des défaillances dues à de différentes causes et phénomènes qui peuvent être internes ou externes selon leurs origines. Ces pannes que peut subir un réseau de capteurs peuvent être dues à :

- L'épuisement d'énergie des capteurs.
- Perte de connexion sans fil due à l'épuisement de la batterie d'un capteur.
- Destruction physique (accidentelle ou volontaire).
- Interférences environnementales. [20]

II.6. Définition de la tolérance pannes :

Dans les RCSF, un ou plusieurs capteurs peuvent ne pas fonctionner correctement, la propriété de tolérance aux pannes est définie par l'aptitude du réseau à maintenir ses fonctionnalités, en cas de panne de certains de ses nœuds. Elle vise donc à minimiser l'influence de ces pannes sur la tâche globale du réseau. [21]

II.7. Fonctionnement :

La propriété de tolérance aux pannes est définie par l'habilité du réseau à maintenir ses fonctionnalités sans interruptions provoquées par la panne des capteurs. Elle vise donc à minimiser l'influence de ces pannes sur la tâche globale du réseau. Cette propriété $R(t)$ est modélisée dans par une distribution de poisson où $R(t)$ donne la probabilité de ne pas avoir une panne pour un noeud capteur pendant l'intervalle de temps $[0,t]$.

$$R(t) = \exp(-\lambda k t)$$

Où λ est le taux de pannes du noeud capteur k , et t est la période de temps.

Les protocoles conçus pour les réseaux de capteurs doivent atteindre le niveau de tolérance aux pannes requis par le réseau, cela dépend essentiellement de l'environnement de déploiement du réseau, des caractéristiques des micro-capteurs, etc. En effet, si le réseau de capteurs est destiné aux environnements avec un faible degré d'interférences, tel que ceux utilisés dans les bâtiments pour surveiller le taux d'humidité et le degré de température, les protocoles utilisés ne doivent pas cibler une grande tolérances aux pannes, car dans ce type de réseaux, il n'existe pas une grande interférence avec l'environnement, et ses noeuds ne sont pas exposés au risque d'endommagement. Par contre, si le réseau est destiné aux applications militaires telle que la surveillance et le contrôle d'un champ de bataille, le niveau de tolérance aux pannes visé par les protocoles employés doit être très élevé, car les noeuds sont exposés à un grand risque d'endommagement par des actions hostiles, et les informations captées sont très critiques. Par conséquent, le niveau de tolérance aux pannes requis dépend de l'application du réseau de capteurs conçu, et les schémas de conception doivent prendre en charge ce paramètre. [22]

II.8. Procédure générale de tolérance aux pannes :

La conception d'une procédure pour la tolérance aux pannes dépend de l'architecture et des fonctionnalités du système. Cependant, certaines étapes générales sont exécutées dans la plupart des systèmes comme c'est illustré dans la figure :



Figure II.2 : Procédure générale de tolérance aux pannes.

II.8.1. Détection de la panne :

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.

II.8.2. Détection 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.

II.8.3. Recouvrement de la panne :

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 » qui utilise l'information redondante correcte pour éliminer l'impact de l'information erronée, et « répétition » qui effectue, après la détection d'une panne, un nouvel essai pour exécuter une partie du programme, dans l'espoir que la panne soit transitoire.

II.8.4. Traitement de la panne :

Dans cette phase, la réparation du composant en panne 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. [23]

II.9. Exemple d'un RCSF tolérant aux pannes :

Le problème de fusion dans un réseau de capteurs multimodal tolérant aux pannes utilisant des capteurs numériques binaires peut être modélisé par l'exemple illustré dans la Figure suivante. On considère un réseau de capteurs pour la reconnaissance de personnes déployé dans une société pour identifier ses employés. Six personnes nommées A, B, C, D, E et F travaillent dans cette société.

Le système de reconnaissance utilise deux types différents de capteurs :

- capteur de taille (grandeur) ;
- capteur pour la reconnaissance vocale qui demande à chaque entrant d'introduire une phrase secrète donnée à l'aide d'un microphone.

La figure ci-dessous montre les six personnes ainsi que leurs caractéristiques (taille et voix) représentées dans le graphe.

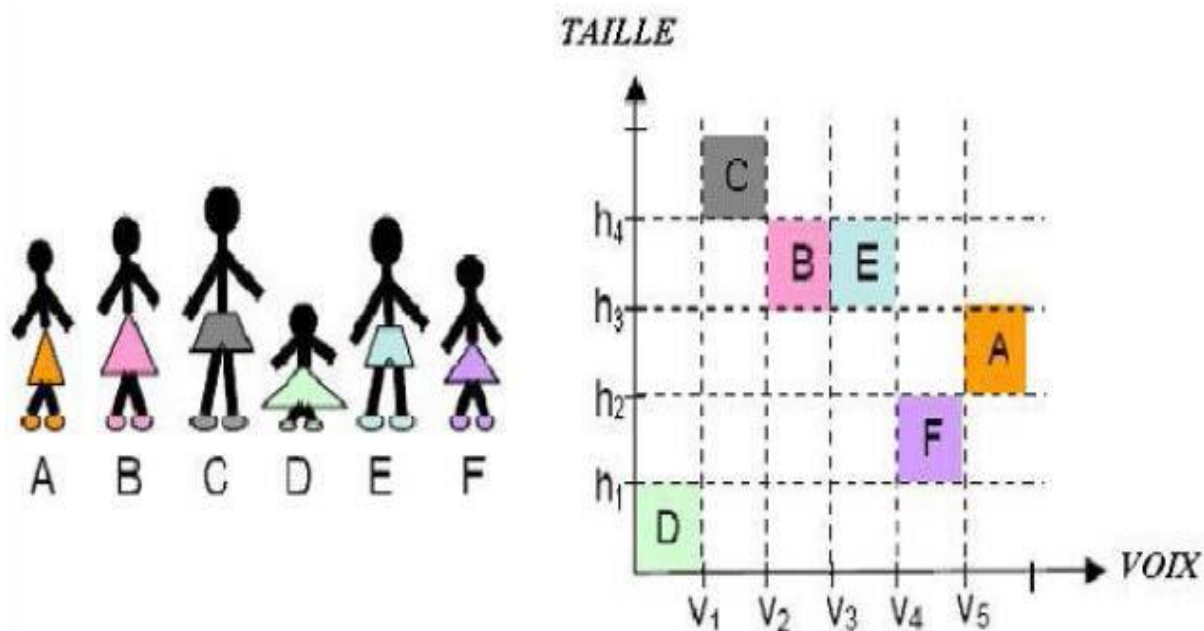


Figure II.3 : Réseau de capteur multimodal

Il est évident de constater que le système peut distinguer entre deux personnes P1 et P2 si elles sont représentées dans deux surfaces différentes sur le graphe. Selon l'exemple, si tous les capteurs fonctionnent correctement, chaque personne va occuper une surface différente.

En outre, dans la plupart des cas, et malgré la défaillance de l'un des capteurs de taille ou de voix, la reconnaissance de toutes les personnes est encore possible. Ceci grâce à la tolérance aux pannes hétérogène où le capteur en panne d'un certain type peut être remplacé par la fonctionnalité d'un capteur de l'autre type. Cependant,

pour le cas des personnes B et E, qui ont la même taille, la voix est le seul critère pour les distinguer ; d'où, le système ne devrait avoir aucune tolérance aux pannes pour le capteur V3 qui distingue entre B et E. Si on exclut l'un de B ou E du personnel de la société, alors le système sera complètement tolérant aux pannes. [24]

II.10. Classification des solutions de tolérance aux pannes dans les RCSF :

Les protocoles tolérants aux pannes peuvent être vus de plusieurs angles différents. De ce fait, un ensemble de critères est défini pour les classifier. Deux catégories de classification sont exposées :

II.10.1. Classification selon la nature de l'algorithme / protocole :

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 [YC08].

- **Algorithme préventif** : 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 permet de consommer moins d'énergie et évite donc une extinction prématurée de la batterie ce qui augmente la durée de vie des noeuds
- **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 nouveau noeud agrégation...etc.

II.10.2. 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 noeuds 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 noeuds 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 noeud 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 noeuds voisins et éviter les collisions durant le transfert;
- **Mobilité** : certains protocoles proposent comme solution tolérante aux pannes : la sélection d'un ensemble de noeuds 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 noeud mobile est généralement doté d'une batterie plus importante que celle d'un noeud capteur.

Gestion des données : les protocoles classés dans cette catégorie offrent une meilleure gestion des 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 noeud d'agrégation combine les données provenant de plusieurs noeuds 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 approches importantes 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). [25]

II.11. Conclusion :

Dans ce chapitre, j'ai présenté les concepts fondamentaux du pannes et de tolérance aux pannes dans les réseaux de capteurs sans fil. Ainsi, j'ai énuméré les origines des pannes dans les RCSFs et j'ai classifié les mécanismes de tolérance aux pannes dans les RCSFs selon plusieurs critères.

Dans le chapitre suivant j'ai détaillé les indicateurs locaux de position pour la tolérance aux pannes dans les RCSF.

CHAPITRE III:

Les indicateurs locaux de position.

III.1. Introduction :

La théorie des graphes est une branche un peu à part des mathématiques. Son efficacité dans la résolution des problèmes de recherche opérationnelle et son aspect synthétique pour la représentation des problèmes les plus complexes via les relations topologiques entre les entités d'un graphe sont les deux facteurs essentiels qui ont fait son succès. Ceci explique son développement croissant dans les sciences sociales, physique et biologique d'où l'apparition de modèles de graphes théoriques tel que les « réseaux petits mondes » et les « réseaux invariants d'échelle ».

III.2. Les modèles de graphes théoriques :

III.2.1. Réseaux aléatoires :

Un graphe aléatoire est un graphe qui est généré par un processus aléatoire. Un graphe aléatoire de taille N est un graphe à N sommets dont on a choisi aléatoirement les arrêtes. Le modèle d'Erdős-Rényi suppose que l'existence de chaque arête est indépendante de celle des autres et que chaque arête a une probabilité p d'exister. La distribution des degrés des sommets du graphe suit une loi de Poisson. Ce modèle de graphe théorique repose donc sur un modèle de construction qui se caractérise par une loi statistique. En cela, il constitue le premier modèle de graphe théorique. Les graphes aléatoires s'opposent aux graphes réguliers peu présents dans la nature (un graphe est dit régulier quand tous les sommets ont le même nombre de voisins, c'est à dire le même degré).

III.2.2. Réseaux petits mondes (small world network) :

Les réseaux de type « petit monde » (small-world) décrits par [Watts-Strogatz 98] sont des graphes où chaque noeud est connecté avec son voisin le plus proche avec des connexions réciproques aléatoires, et une distance topologique moyenne faible, ce qui traduit une forte connexité. Ce modèle de réseau a connu un succès rapide, principalement dû à son lien direct avec les travaux de Stanley Milgram concernant les fameux « six degrés de séparation » : seules six personnes nous séparent de n'importe quelle autre personne dans le monde. Ce genre de graphe possède alors un coefficient d'agglomération supérieur (en fait très supérieur) et un diamètre inférieur à un graphe aléatoire de même ordre et de même taille.

III.2.3. Réseau invariant d'échelle (Scale-free network) :

Introduit par Barabasi et Albert, ces graphes sont caractérisés par une distribution de degré qui suit une loi de puissance, c'est-à-dire à des graphes où il existe une large distribution de degrés différents, décroissant très lentement, ce qui traduit une hiérarchisation des noeuds selon leur degré. Pour expliquer cette distribution inégalitaire des degrés on peut prendre l'exemple d'Internet. La création d'un site Internet sur un sujet précis implique la création de rubrique de liens vers les sites de référence de ce sujet qui envoie de façon préférentielle vers les sites de référence

concernant ce sujet, et la centralité de ces sites de référence tend à augmenter au cours du temps. Les noeuds « hub » de ce genre de réseau sont connectés directement à ceux de plus petites tailles et ceci permet une tolérance aux pannes même en cas de faillite d'un noeud central en terme de degré. La distribution du coefficient d'agglomération dans ce modèle de réseau suit une loi de puissance : ce coefficient est inversement proportionnelle à l'augmentation du degré d'un noeud, ce qui implique que les noeuds de faible degré appartiennent à des « small world networks ». Plusieurs réseaux du monde réel sont modélisés par ce modèle de graphe tel que les réseaux sociaux, les réseaux de paiement interbancaires, ... [26]

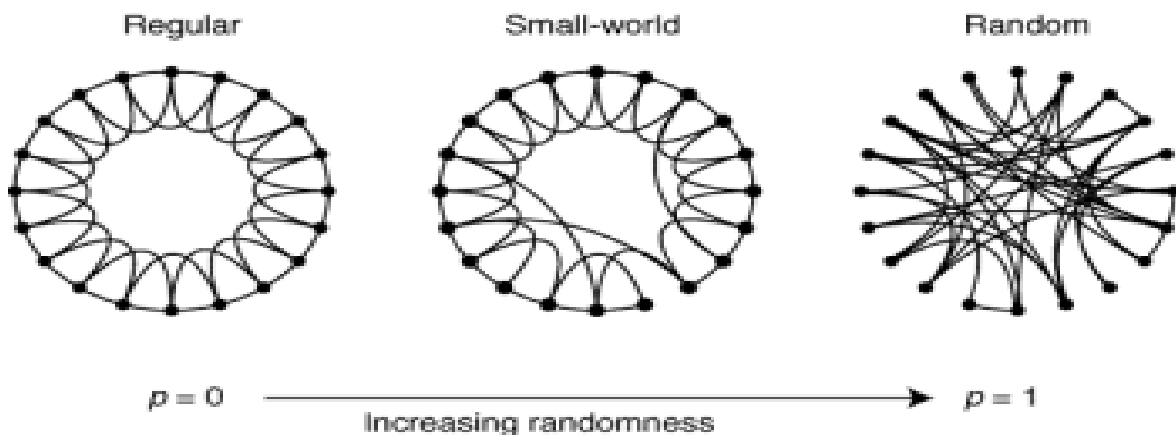


Figure III.1: Les différents types de réseaux.

III.3. La Théorie des graphes :

III.3.1. Définition et notations:

Un graphe G est défini par un couple $(V(G), E(G))$, où $V(G)$ est un ensemble de sommets et $E(G)$ est un ensemble de paires de sommets appelées arêtes. Lorsqu'il n'y a pas d'ambiguïté, nous notons simplement V et E . Le nombre de sommets dans le graphe G est appelé ordre de G , est noté par $n = |V(G)|$, et le nombre d'arêtes est appelé la taille de G , et est noté par $|E(G)|$. Un graphe est dit fin ou infini suivant son ordre.

Soit G un graphe et soient u, v deux sommets de G . Une arête reliant deux sommets u, v est notée uv au lieu de $\{u, v\}$. Si $uv \in E$, alors u et v sont dits adjacents ou voisins.

Par contre, si $uv \notin E$, alors u et v sont dits non-adjacents ou non-voisins. Si $e = uv$ est une arête de G , alors u et v sont les extrémités de e , et e est dite incidente à u et v . Deux arêtes sont dites adjacentes si elles ont une extrémité en commun. Une boucle est une arête dont les extrémités sont confondues.

Un graphe simple est un graphe sans boucles ni arête multiple (i.e tout couple de sommets est relié par au plus une arête). Dans tout ce qui suit on s'intéresse qu'à des graphes simples et finis.

A titre d'exemple d'un graphe, on considère le graphe G de la Figure suivante, dont l'ensemble des sommets est $\{v_1, v_2, v_3, v_4\}$ et l'ensemble des arêtes est $\{v_1v_2, v_2v_3, v_3v_4\}$.

Les Sommets v_1 et v_2 sont adjacents dans G, alors que v_1 et v_3 ne le sont pas. [27]

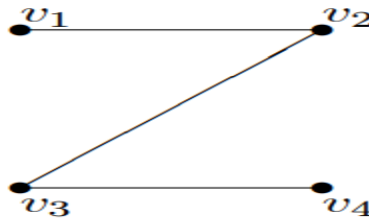


FIGURE III.2: Un graphe G avec 4 sommets et 3 arêtes.

III.3.2. Les types des graphes :

III.3.2.1. Graphes connexes/complémentaires :

Un graphe G est connexe si pour tout couple de points différents x et y, il existe une chaîne entre x et y.

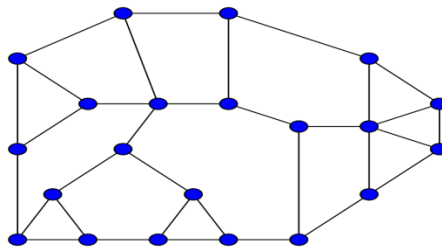


FIGURE III.3: Un graphe connexe.

G' est le graphe complémentaire de G, si $G = (V, U)$ et $G' = (V, U')$. $(x_i, x_j) \in U \Leftrightarrow (x_i, x_j) \notin U'$.

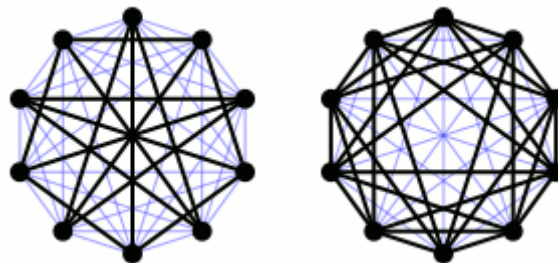


FIGURE III.4: Le graphe de Petersen, à gauche et son complémentaire, à droite.

III.3.2.2. Graphes planaires:

Un graphe planaire est un graphe qui peut être dessiné dans un plan de telle manière que ses arêtes ne se coupent pas en dehors de leurs extrémités. Lorsqu'un graphe planaire est dessiné de telle manière que ses arêtes ne se

coupent pas en dehors de leurs extrémités, on dit qu'il est représenté sans croisement. [28]

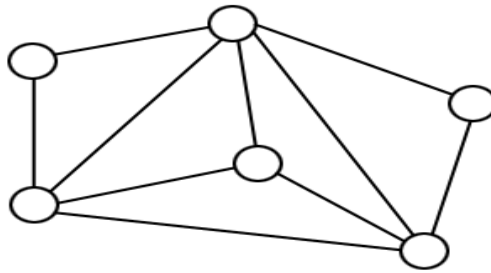


FIGURE III.5: Un graphe Planaire.

III.3.2.3. Composantes connexes :

Dans Une composante connexe d'un graphe G est un ensemble exhaustif de sommets deux à deux connectables. Deux sommets reliés par une arête font forcément partie de la même composante connexe. Dans le cas d'un graphe orienté G où l'orientation des arcs importe, on parle de composante fortement connexe. [29]

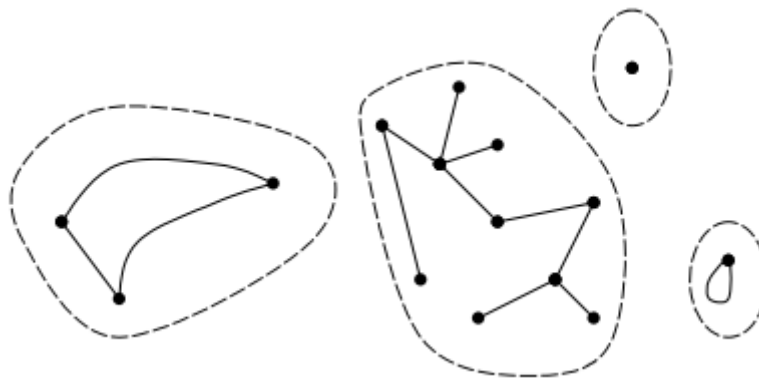


FIGURE III.6: graphe 4 composantes connexes.

III.3.2.4. Cycles :

Dans un graphe non orienté, un cycle est une suite d'arêtes consécutives distinctes (chaîne simple) dont les deux sommets extrémités sont identiques. Dans les graphes orientés, la notion équivalente est celle de circuit, même si on parle parfois aussi de cycle (par exemple dans l'expression graphe acyclique orienté).

Le terme de cycle désigne parfois aussi le graphe cycle C_n constitué d'un cycle élémentaire de longueur n .

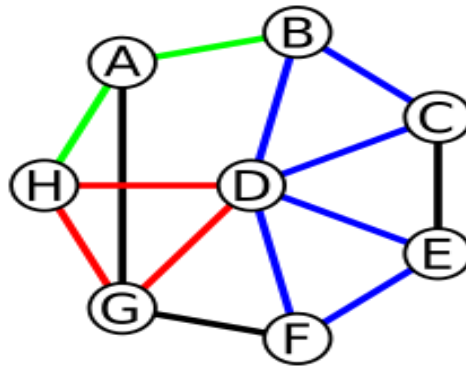


FIGURE III.7: Un Cycle.

Dans ce graphe, le cycle rouge est élémentaire. Le cycle bleu ne l'est pas. La chaîne verte n'est pas fermée et ne forme donc pas un cycle [30]

III.3.3. Valuation et orientation :

III.3.3.1. Graphes Valués :

Un **graphe valué** est un graphe dans lequel chacune des arêtes présente une valeur. Le graphe valué peut être orienté ou non.

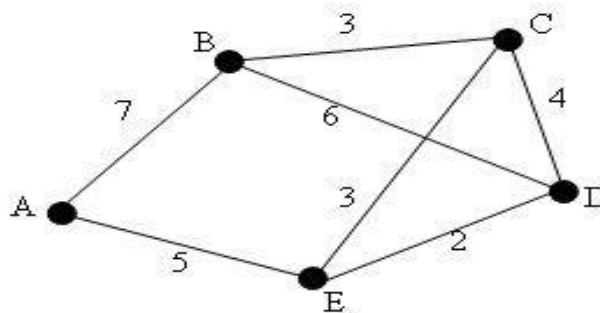


FIGURE III.8: Graphe Valué.

III.3.3.2. Graphes Orientés :

Un graphe orienté est un couple (V, U) où V est l'ensemble des sommets, et U est l'ensemble des arcs de G . Chaque arc est un couple de sommets, on notera (x, y) , l'arc (x, y) .

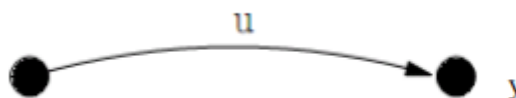


FIGURE III.9: Arc (x,y) .

Un graphe non orienté est un couple (V, E) où V est l'ensemble des sommets, et E est l'ensemble d'arêtes de G . Chaque arête est une paire de sommets, on notera xy l'arête $\{x, y\}$. [31]

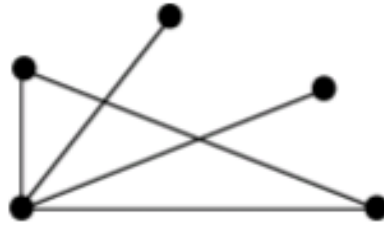


FIGURE III.10: Graphe non orienté.

III.4. OUTILS GENERAUX DE DESCRIPTION DES GRAPHES :

III.4.1. Indicateurs globaux:

III.4.1.1. Indicateurs de connexité:

La connexité désigne la possibilité de relier des sommets ou des groupes de sommets les uns aux autres, elle est utilisée pour décrire l'état d'un réseau dont une des arêtes est coupée. Par exemple, si une inondation vient rompre un pont qui constitue l'unique lien entre deux portions d'un «territoire», le réseau résultant perd sa propriété de connexité, ce qui peut avoir des conséquences négatives en particulier sur l'acheminement des secours. [32]

La connexité est un indicateur de la cohésion d'un réseau et donc de la cohésion de l'espace qu'il dessert. Sur un territoire la connexité du réseau de transport constitue une condition nécessaire à l'accessibilité des lieux [33].

Les indicateurs globaux de connexité mesurent le degré de fragmentation d'un graphe en composantes connexes séparées les unes des autres. Soit S le nombre de sommets d'un graphe, C son nombre de composantes connexes et $S_1..S_k$ le nombre de sommets de chacune des composantes connexes ($S_1+S_2+...S_k = S$), on peut définir deux indices de connexité dont les valeurs sont comprises entre 0 (graphe vide) et 1 (graphe connexe).

- **Indice de connexité simple** : $IC1 = (S-C)/(S-1)$
- **Indice de connexité pondéré** : $IC2 = [(S_1)^2 +(S_2)^2 + ... (S_k)^2] / S^2$

Exemple d'application :

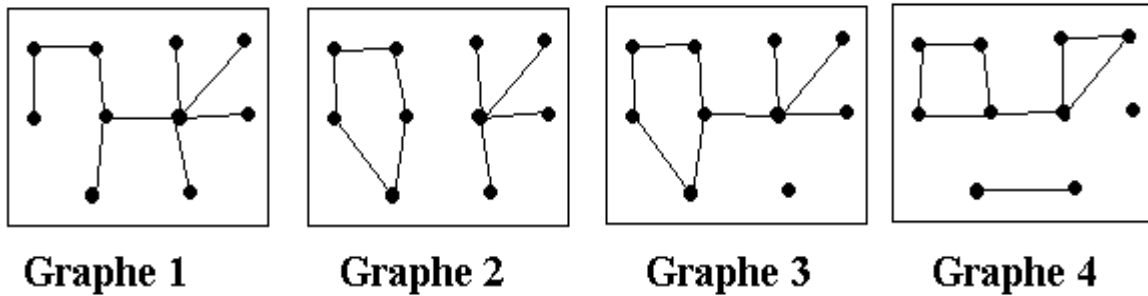


FIGURE III.11: Exemple d'application (indicateur connexité).

Calcul des indices de connexité :

Situation	Indice de connexité simple	Indice de connexité pondéré
Graphe 1	$9/9 = 100\%$	$100/100 = 100\%$
Graphe 2	$8/9 = 89\%$	$(25+25)/100 = 50\%$
Graphe 3	$8/9 = 89\%$	$(81+1)/100 = 81\%$
Graphe 4	$7/9 = 78\%$	$(49+4+1)/100 = 54\%$

TAB III.1: Les Calcul des indices de connexité.

Commentaire :

- **L'indice de connexité simple** est relativement imprécis et peu fiable, car il ne tient pas compte que du nombre de composantes connexes et pas de leurs tailles respectives. Il est évident que les situations présentées sur les graphes 2 et 3 ne sont pas équivalentes, or elles correspondent à un même indice de connexité simple (89%).
- **L'indice de connexité pondéré**, beaucoup plus précis, exprime la probabilité que deux sommets tirés au hasard puissent être reliés par un chemin (i.e. appartiennent à la même composante connexe). Il montre que le graphe 3 est beaucoup plus connexe que le graphe 2. On remarque d'ailleurs que le graphe 4 (pourtant découpé en trois composantes connexes) a une connexité pondérée supérieure au graphe 2 (pourtant découpé simplement en 2).

III.4.1.2. Indicateurs de connectivité:

Les indicateurs globaux de connectivité mesurent la densité et la variété des relations possibles, directes ou indirectes entre les sommets d'un graphe. Ils permettent de préciser les différences entre des graphes connexes (qui ont tous des indices de connexités égaux à 100%). Leur calcul repose sur le nombre de sommets (S), le nombre de liens (L) et le nombre de composantes connexes (C) d'un graphe.

Les indicateurs de connectivité basé sur la fréquence des liens :

- **L'indice de connectivité β** exprime le rapport entre le nombre de liens et le nombre de sommets. Cet indice est simple à calculer. Une valeur supérieure ou égale à 1 indique la présence de circuits à l'intérieur du graphe.

$$\beta = L/S$$

- **L'indice de connectivité γ** est une version standardisée de l'indice précédent, avec une valeur comprise entre 0 et 1. Il exprime le rapport entre le nombre de liens observé et le nombre maximal de liens possibles. ce qui donne la formule suivante : $\gamma = L/L_{max}$

Les indicateurs de connectivité basé sur le nombre de circuits indépendants :

- **Le nombre cyclomatique μ** exprime le nombre maximal de circuits indépendants que l'on peut construire simultanément à l'intérieur d'un graphe.

$$\mu = L-S+C$$

- **L'indice de connectivité α** est une version standardisée de l'indice précédent, avec une valeur comprise entre 0 et 1. Cet indice exprime le rapport entre le nombre observé de circuits indépendants et sa valeur maximale. Dans le cas d'un graphe planaire, le nombre maximal de circuits est égal à $(2N-5)$, ce qui donne la formule suivante:

$$\alpha = \mu/\mu_{max}$$

Exemple d'application :

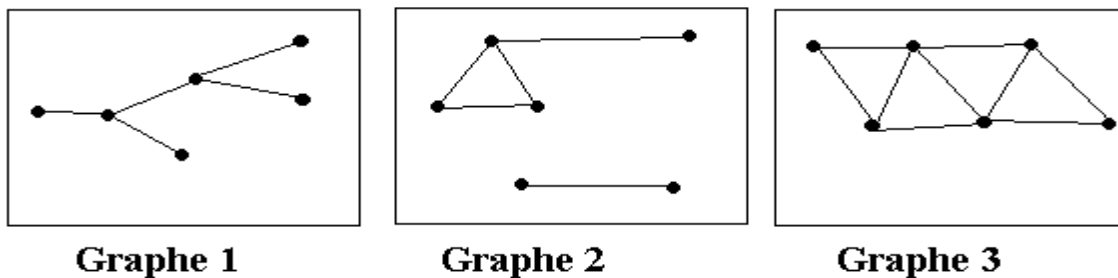


FIGURE III.12: Exemple d'application (indicateur connectivité).

Calcul des indices de connectivité :

	L	S	C	β	γ	μ	α
Graphe 1	5	6	1	0.83	42%	0	0%
Graphe 2	5	6	2	0.83	42%	1	14%
Graphe 3	9	6	1	1.50	75%	4	57%

TAB III.2: Les Calcul des indices de connectivité.

III.4.2. Indicateurs locaux:

Les indicateurs locaux de position permettent de mesurer le degré de centralité ou d'accessibilité des différents sommets à l'intérieur d'un graphe. Les avantages relatifs des différents sommets peuvent varier selon le critère retenu.

Exemple d'application :

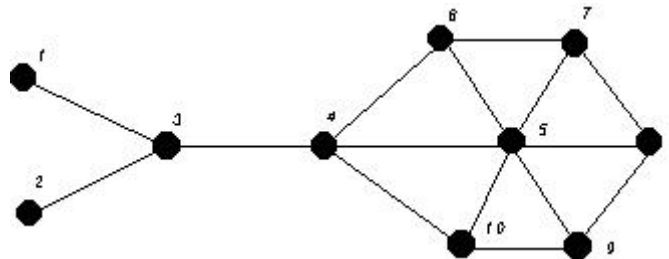


FIGURE III.13: Exemple d'application (Les indicateurs locaux).

III.4.2.1. Centralité de degré (C_D) :

La centralité de degré correspond au nombre de liaisons directes qui partent d'un sommet. Elle correspond en géographie à la notion de carrefour.

Sommet	1	2	3	4	5	6	7	8	9	10
C _D	1	1	3	4	6	3	3	3	3	3

TAB III.3: La centralité de degré .

Elle est influencée par la nature du graphe : pondéré ou non. Dans le cas d'un graphe orienté, la centralité de degré peut être divisée en trois sous-mesures: la centralité de degré, celle en rapport aux liens entrants et celles des liens sortants.

A. Degré binaire : La centralité de degré [34] est la forme la plus intuitive de toutes les mesures de centralité. Elle définit le nombre d'acteurs avec lesquels un nœud est lié directement et donc elle mesure l'importance d'un acteur qui est ici directement proportionnelle à sa valeur de centralité de degré. Cette mesure, exprime le nombre d'alternatives disponibles pour un acteur de la structure. Augmenter le nombre d'alternatives augmente le pouvoir d'un acteur. La centralité de degré est aussi appelée mesure de centralité locale [35] car elle ne prend pas en compte la structure globale du graphe vu qu'elle est déterminée directement par le voisinage immédiat du nœud pris en considération. L'apport d'information de cette mesure peut être limité dans certains cas.

Soit G = (V, E) un graphe d'ordre N et [a_{ij}] sa matrice d'adjacence binaire. Dans le cas ou le graphe G est non-orienté, la centralité de degré d'un nœud est défini par :

$$C^{deg}(v_i) = \frac{1}{N-1} \sum_{j=1}^N a_{ij}$$

Dans le cas où le graphe G est orienté, chaque nœud $v_i \in V$ possède alors deux mesures de centralité de degré : une par rapport aux liens entrants et une par rapport aux liens sortants.

B. Degré de Pondération : La notion de centralité de degré a ensuite été étendue à la somme des poids, si le graphe est pondéré [36] [37]. Cette mesure exprime un effet de « résistance » du nœud dans le graphe. Bien que préféré pour analyser les réseaux pondérés, le degré pondéré et le degré simple expriment deux notions différentes, car le degré pondéré mesure l'engagement d'un acteur dans un réseau indépendamment du nombre de voisins auxquels il est connecté. Cette mesure est formulée comme suit:

$$S_i = C_D^W(i) = \sum_j^N a_{ij}$$

Où A est maintenant la matrice d'adjacence dans laquelle a_{ij} une valeur supérieure à zéro si le nœud i est connectée au nœud j.

C. Centralité Combinée : D'après [37] la combinaison des deux mesures précédentes (degré binaire et degré pondéré) sera plus utile en vue d'extraire une information pertinente : car elle combine la topologie et le poids. En effet, le degré binaire considère tous les liens de la même façon (0 absence du lien et 1 présence du lien), alors que le degré pondéré ne fait pas de distinction entre un seul lien de valeur 2 et deux liens de valeur 1. Cette combinaison est faite en définissant un paramètre alpha, dont la valeur est positive et ne dépend que de la nature du réseau et de son contexte d'étude : un coefficient positif inférieur à 1 donnera plus d'importance au degré binaire, tandis qu'un coefficient supérieur à 1 favorisera le rôle du poids des liens. Cette mesure est défini comme suit :

$$C_D^{W\alpha}(i) = K_i \times \left(\frac{S_i}{K_i}\right)^\alpha \quad \text{ou} \quad K_i = C_D(i) = \sum_j^N a_{ij} : \text{degré du noeud } i.$$

Pour les graphes orientés, les auteurs ont défini les mesures suivantes pour qualifier l'activité d'un noeud :

$$C_{D-out}^{W\alpha}(i) = K_{i-out} \times \left(\frac{S_{i-out}}{K_{i-out}}\right)^\alpha \quad C_{D-in}^{W\alpha}(i) = K_{i-in} \times \left(\frac{S_{i-in}}{K_{i-in}}\right)^\alpha$$

La valeur d'alpha, dans ces deux équations, est similaire à celle pour un graphe non orienté.

III.4.2.2. Centralité d'éloignement moyen (CE):

La centralité d'éloignement moyen correspond à la distance moyenne entre un sommet et l'ensemble des autres sommets. Le calcul de cette mesure de centralité implique la construction d'une matrice de distances de plus court chemin à l'intérieur du graphe. [38]

<i>D_{ij}</i>	1	2	3	4	5	6	7	8	9	10	tot
1	-	2	1	2	3	3	4	4	4	3	26
2	2	-	1	2	3	3	4	4	4	3	26
3	1	1	-	1	2	2	3	3	3	2	18
4	2	2	1	-	1	1	2	2	2	1	14
5	3	3	2	1	-	1	1	1	1	1	14
6	3	3	2	1	1	-	1	2	2	2	17
7	4	4	3	2	1	1	-	1	2	2	20
8	4	4	3	2	1	2	1	-	1	2	20
9	4	4	3	2	1	2	2	1	-	1	20
10	3	3	2	1	1	2	2	2	1	-	17
C_E	2.9	2.9	2.0	1.6	1.6	1.9	2.2	2.2	2.2	1.9	2.1

TAB III.4: La centralité d'éloignement moyen.

A titre indicatif, cet indice équivaut également à l'indice de centralité de Bavelas, dont la normalisation est effectuée par rapport à la somme des plus courts chemins pour toute paire ordonnée de sommets du graphe [39]:

$$C_{\text{Bavelas}} = \frac{\sum_j \sum_k d_{jk}}{\sum_k d_{ik}}$$

III.4.2.3. Centralité d'éloignement maximal (C_M) :

Elle correspond à la distance maximale entre un sommet et l'ensemble des autres sommets. [5]

<i>Sommet</i>	1	2	3	4	5	6	7	8	9	10
C_M	4	4	3	2	3	3	4	4	4	3

TAB III.5: La centralité d'éloignement maximal.

III.4.2.4. Centralité d'intermédiarité (C_I) :

La centralité d'intermédiarité correspond **au nombre de liaisons transitant obligatoirement par un sommet**, c'est-à-dire au nombre de liaisons entre les autres sommets qui peuvent être contrôlés depuis un sommet donné.

<i>Sommet</i>	1	2	3	4	5	6	7	8	9	10
C_I	0	0	15	18	0	0	0	0	0	0

TAB III.6: La centralité d'intermédiarité.

La centralité d'intermédiation [34] mesure le nombre de fois où un agent est l'intermédiaire sur le plus court chemin entre deux autres, il s'agit donc du degré de médiation d'un agent sur les transferts d'information entre deux autres agents. Cette mesure paraît particulièrement appropriée dans l'étude du pouvoir dans les réseaux de communication parce que l'intermédiation permet la manipulation de l'information transmise. Finalement, la centralité de proximité mesure la manière dont on peut éviter le contrôle d'autres membres de l'organisation là où l'intermédiation représente au contraire la manière dont on peut accroître la dépendance des autres. La centralité peut être définie comme la probabilité qu'une information transmise entre deux nœuds passe par un nœud donné. [40].

Soit $G = (V, E)$ un graphe (orienté ou non) d'ordre N . La centralité d'intermédiation d'un nœud est $v_i \in V$ définie par :

$$C^{int}(v_i) = \sum_{j=1}^N \sum_{k=1}^N \frac{g_{jk}(v_i)}{g_{jk}}$$

Où $G_{jk}(v_i)$ est le nombre total de chemins géodésiques entre les nœuds v_j et v_k qui passent par le nœud v_i et G_{jk} est le nombre total des plus courts chemins entre les nœuds v_j et v_k . La centralité d'intermédiation est basée sur l'idée que les nœuds ne communiquent entre eux qu'à travers les chemins les plus courts mais suivant le contexte d'étude on peut avoir intérêt à prendre en compte le fait que les nœuds peuvent interagir en utilisant des chemins autres que les chemins géodésiques.

La notion de centralité d'intermédiation de nœud proposé par Freeman a été généralisée à la centralité d'intermédiation de lien ou intermédiation de lien par [Girvan & Newman 02], [Newman & Girvan 04]. Cette mesure est définie comme suit:

$$C^{int}(a_{kl}) = \sum_{i=1}^N \sum_{j=1}^N \frac{g_{ij}(a_{kl})}{g_{ij}}$$

III.5. Influence du type de graphe sur les indicateurs de centralités :

L'analyse d'un réseau complexe de données réelles doit commencer par s'interroger sur la nature de la centralité qu'il faut prendre en compte, à savoir la centralité locale, ou la centralité globale. Savoir quelle est la combinaison de nœuds et de liens qu'il faut prendre en compte pour analyser un réseau dans un contexte donné est primordial, mais avant de poser la question de choix de mesures de centralités, l'évaluation des corrélations qui peuvent exister entre les mesures à utiliser est nécessaire. En effet, l'existence d'une forte corrélation implique une redondance de l'information et donc l'analyse est peu informative quant aux particularités qui peuvent rester indétectable par cette famille liée de mesures. Cependant, si les mesures sont peu corrélées, l'analyse du réseau, via ces mesures, sera meilleure en quantité et en qualité. Plusieurs recherches faites dans ce sens ont prouvé qu'une étude de la topologie du réseau en lui-même peut favoriser le choix

de certaines mesures. Les études expérimentales sur des données réelles ou expérimentales ont été menées par des chercheurs comme [Bolland 88] pour déterminer les corrélations qui peuvent exister entre les différentes mesures de centralités. Une corrélation forte implique que peu d'informations peuvent être utiles et que les mesures utilisées forment une famille liée. En effet, plusieurs facteurs peuvent influencer le degré de corrélation entre les mesures tels que le type de la matrice : symétrique ou asymétrique, le contexte étudié et les propriétés du réseau comme sa densité. [41]

III.6. Conclusion :

Dans ce chapitre, j'ai présenté les notions de base de la théorie des graphes et des différents outils généraux de description des graphes qui sont des indicateurs globaux et j'ai détaillé les différents indicateurs locaux de position pour la tolérance des pannes dans les réseaux de capteurs sans fil ainsi que l'influence du type de graphe sur les indicateurs de centralité.

CHAPITRE IV: SIMULATION

IV.1. Introduction :

La dernière étape dans mon étude a consisté à passer de la théorie à la pratique afin de faire des plusieurs simulations par système d'exploitation CONTIKI-COOJA. Cette étape est très importante, et me permet de savoir les résultats et de faire une comparaison entres les indicateurs locaux de position que j'ai déjà présenté dans le chapitre précédent.

IV.2. Environnement de simulation :

Les RCSFs sont considérés parmi les systèmes à ressources limitées à cause des caractéristiques des noeuds capteurs telles qu'une mémoire réduite, une ressource d'énergie très limitée, un processeur de faible fréquence de calcul, etc. De ce fait, les outils logiciels traditionnels conçus aux ordinateurs comme Linux ou Windows ne sont plus adaptables à ce type de systèmes. Pour cela, plusieurs systèmes d'exploitation légers ont été développés [42] pour répondre aux attentes des systèmes embarqués et qui sont dédiés spécialement aux RCSFs. [43]

Dans cette section, je vais présenté le système d'exploitation Contiki qui est un système *open-source* embarqué, le simulateur Cooja.

IV.2.1. Système d'exploitation CONTIKI :

IV.2.1.1 Présentation :

Contiki [44] est un système d'exploitation *open-source*, intégré, modulaire, flexible, générique qui s'appuie sur un modèle de fonctionnement hybride, destiné aux réseaux de capteurs. Ce système a été développé par un groupe de développeurs de l'industrie et du monde universitaire par Adam Dunkels de l'institut suédois d'informatique en 2004. Il fonctionne sur les microcontrôleurs de faible puissance et permet de développer des applications qui font une utilisation efficace du matériel tout en fournissant une communication standardisée sans fil de faible puissance pour une gamme de plateformes des microcontrôleurs tels que le Atmel AVR et TI MSP430, [45] qui sont utilisés dans les familles Telos, Tmote et MICA.

IV.2.1.2. Caractéristiques de Contiki :

L'évolution de Contiki a été déterminée essentiellement par les caractéristiques suivantes:

Normes Internet: Contiki a présenté l'idée d'utiliser la communication IP dans des réseaux de capteurs basse consommation. En plus il supporte les protocoles IPV6 et 6LOWPAN. Cela s'avère particulièrement utile dans la mesure où les noeuds communiquent en IPV6 et utilisent le standard 802.15.4 définie par l'IEEE.

Développement rapide: Les applications à base de Contiki sont écrites en C standard. Ces applications peuvent être émulées avec le simulateur Cooja avant d'être injectées sur des capteurs réels.

Une sélection du matériel: Il fonctionne sur une gamme de différentes plateformes matérielles de faible puissance tels que la famille de MICA et la famille de Telos et est conçu pour être facile à porter sur les nouveaux matériels.

Logiciel Open Source: Contiki est un système open source dont le code est toujours disponible. Et il peut être exploité librement dans les deux systèmes commerciaux et non commerciaux sans restrictions.

Couche de protocole Rime: Rime est une légère couche de communication [46] conçue pour des radios basse puissance et supporte des opérations simples. Elle fournit à la couche applicative un jeu d'instructions de communication, permettant les inondations de réseau, de collecte de données, et les différentes connexions avec les capteurs voisins, pour établir des schémas de routage.

Allocation de mémoire: Contiki est conçu pour les systèmes légers. Il a une empreinte mémoire limitée ayant seulement quelques kilo-octets de mémoire disponible (2 kilo-octets de RAM et 40 kilo-octets de ROM). De plus, il fournit un ensemble de mécanismes d'allocation dynamique de mémoire.

Consommation d'énergie: Contiki a été conçu pour réduire au maximum la consommation en énergie du capteur. Ainsi, lorsqu'aucune tâche n'est active, il se met automatiquement en veille.

IV.2.1.3. Architecture de CONTIKI :

Contiki OS est basé sur une architecture modulaire. Il est constitué d'un noyau, de bibliothèques, d'un ordonnanceur et d'un gestionnaire de processus. Le rôle de Contiki, est de gérer les ressources physiques telles que le processeur, la mémoire, les périphériques (d'entrée/sortie). Le noyau se compose d'un planificateur pour la gestion des événements synchrones et asynchrones. Il utilise un mécanisme qui lui permet de fonctionner comme un système multitâche.

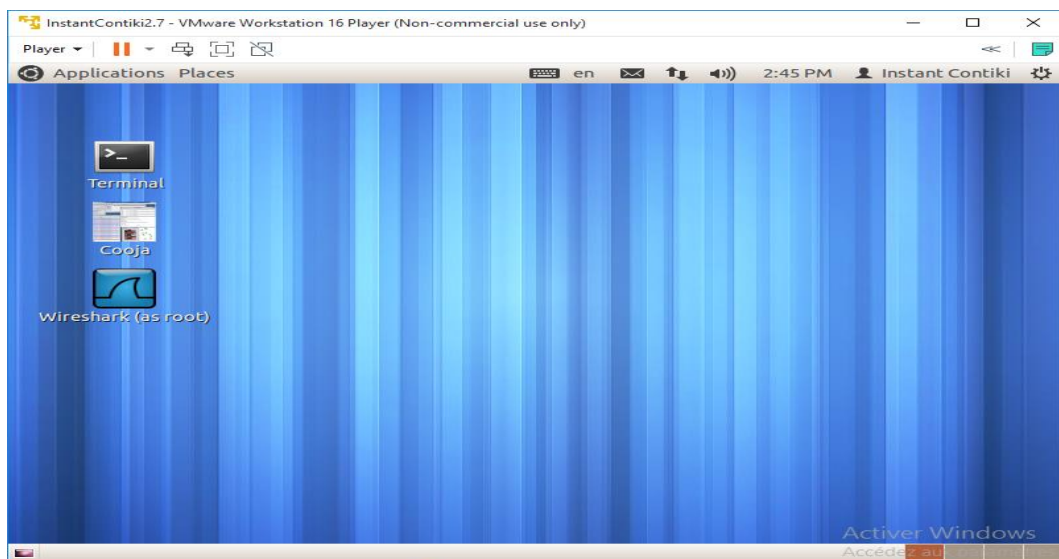


FIGURE IV.1: Système d'exploitation CONTIKI.

IV.2.2. Le simulateur Cooja pour les applications Contiki :

Contiki propose un simulateur de réseau appelé Cooja. Ce simulateur permet l'émulation de différents capteurs sur lesquels seront chargés un système d'exploitation et des applications. COOJA permet ensuite de simuler les connexions réseaux et d'interagir avec les capteurs. Cet outil permet aux développeurs tester les applications à moindre coût. Il offre une variété des capteurs supportés comme : exp5438, z1, wismote, micaz, sky, jcreate, esb.

Pour dérouler les tests de simulations j'ai utilisé le simulateur inclus dans le système contiki appelé COOJA, qui a les caractéristiques suivantes:

- COOJA combine des simulations de capteurs matériels de nœuds et simulations du comportement de haut niveau en une seule simulation
- COOJA est flexible et extensible de manière à ce que tous les niveaux du système peuvent être modifiés ou remplacés
- COOJA est une application Java, toutes les interactions avec le Code Contiki se fait à travers Java Native Interface (JNI). L'interface de simulateur COOJA est composée de plusieurs fenêtres (plugins) [47] , comme illustré dans la Figure suivante.

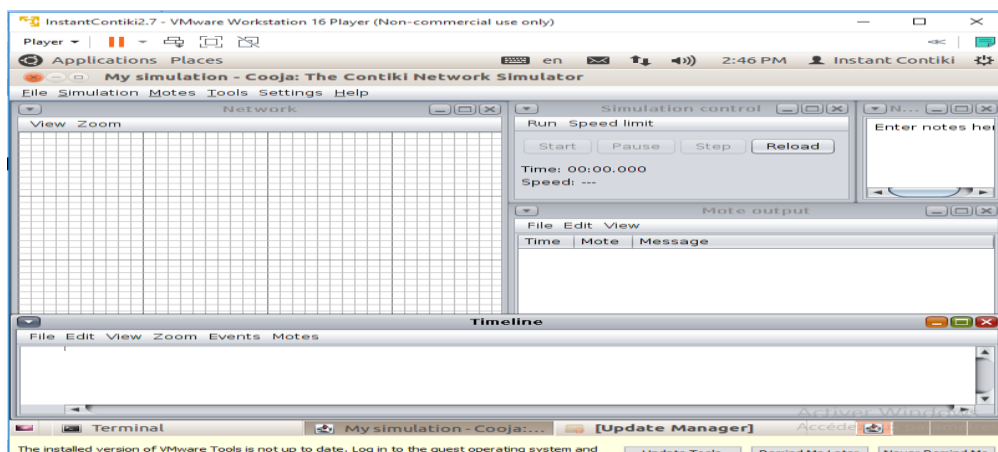


FIGURE IV.2: Interface graphique de Cooja.

- **Mote output** : présente ce que les capteurs génèrent comme sortie via leurs ports séries.
- **Network** : présente le réseau simulé et le flux de communication durant la simulation.
- **simulation control** : cette fenêtre contient quatre boutons
 - 1) Start : pour démarrer une simulation
 - 2) Pause : pour arreter la simulation
 - 3) Reload : pour recharger une simulation
 - 4) Step : pour régler la vitesse de la simulation
- **Power tracker** : pour voir la consommation d'énergie par les capteurs durant la simulation.

IV.3. Implémentations et déroulements de simulation :

Les paramètres de simulation sont exprimés dans le tableau suivant :

Paramètres	Valeurs
Système d'exploitation	Contiki-2.7
Simulateur	Cooja
Type de nœud	Sky mote
Nombre de nœud	1 Sink + 30 nœud sender
Topologie	Aléatoire
MAC/adaptation layer	ContikiMac / 6LowPAN
Protocole de routage	RPL
Radio environment	UDGM
Range de transmission	50m
Duré de la simulation	variable

Tab IV.1: Les paramètres de simulation

Après le lancement l'interface du simulateur cooja et la fenêtre de simulation et le choix du firmware à charger sur les capteurs, on pourra observer les logs et le trafic des messages entre les capteurs comme le montre la figure suivante :

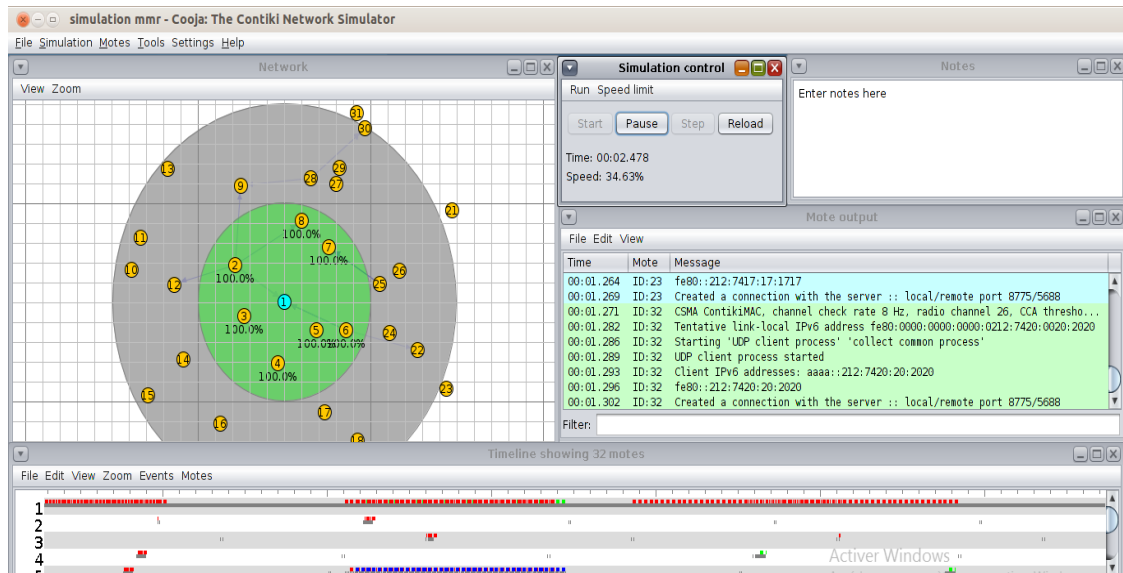


FIGURE IV.3: Compilation et lancement des simulations sur Cooja.

Etape 1: Création d'un réseau de capteurs sans fil composé de (31 nœuds (1 nœud Sink et 30 nœud Sender) avec des positions aléatoires). Figure IV.4 montre les différentes topologies de simulation avant le déclenchement d'action correctif.

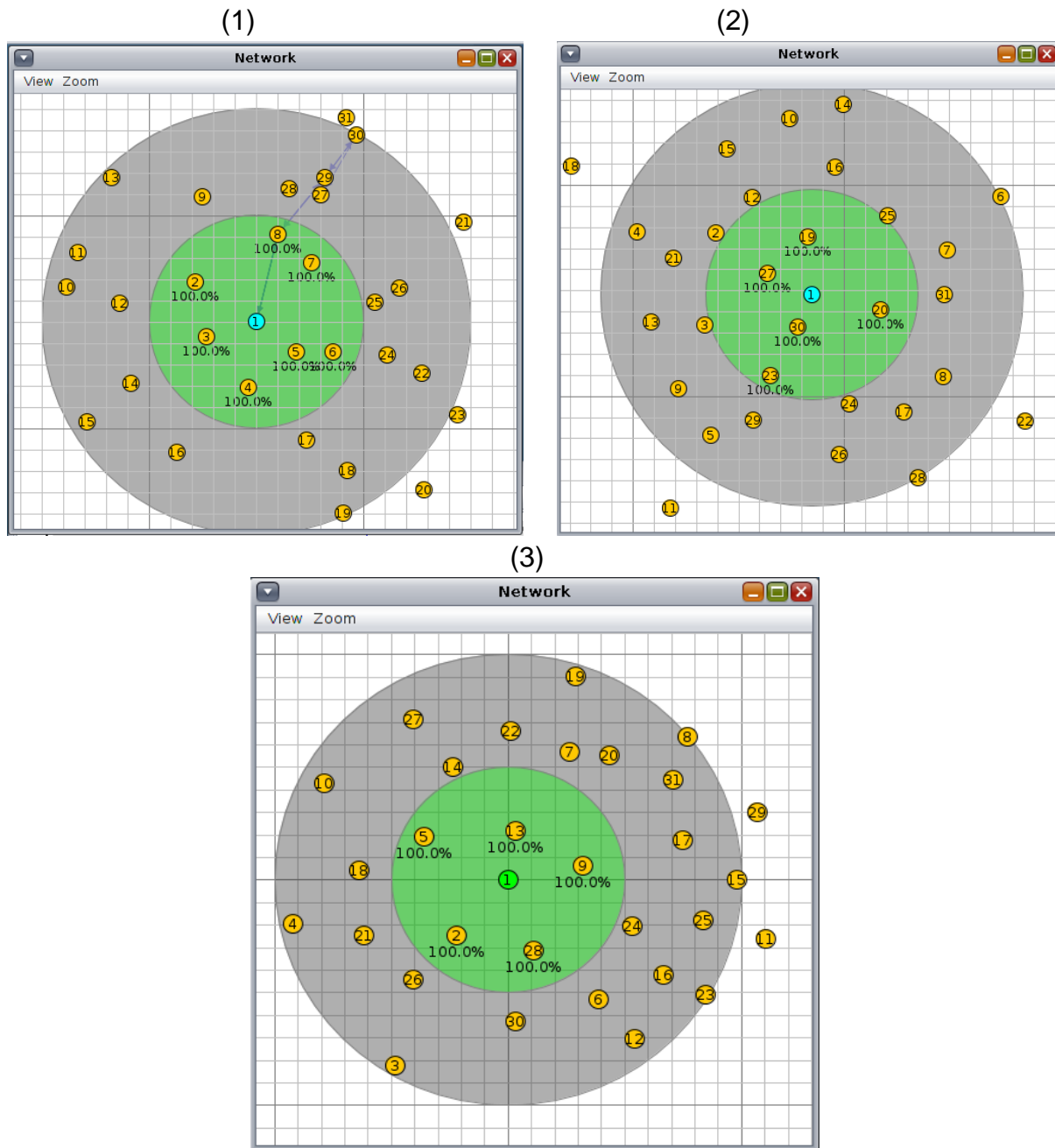


FIGURE IV.4: Les différentes topologies de simulation avant déclenchement d'action correctif.

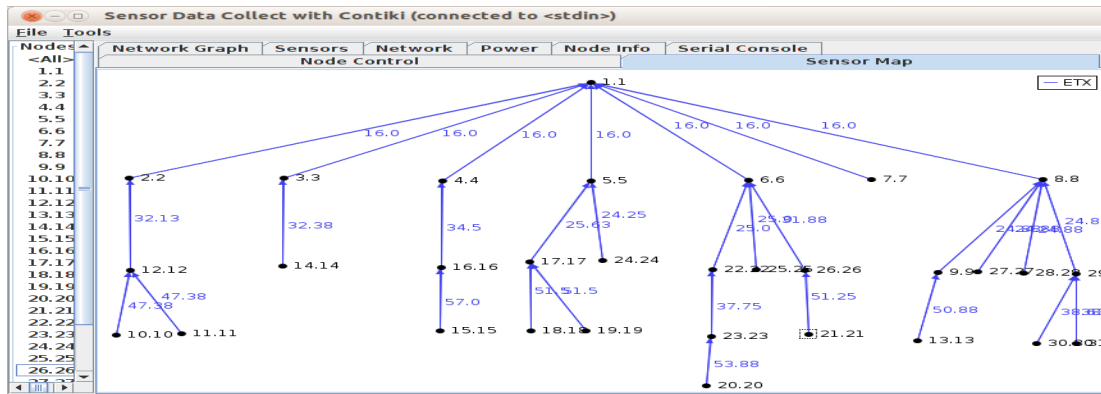


FIGURE IV.5.1: DODAG Simulation1 avant déclenchement d'action correctif.

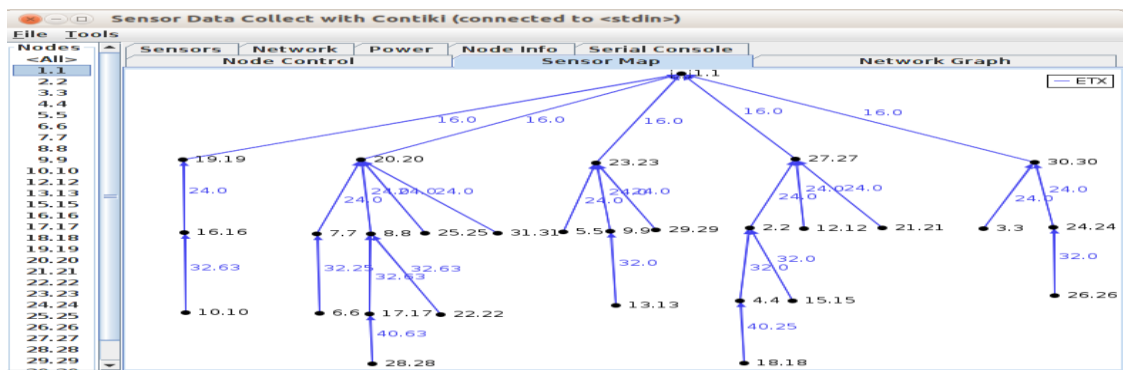


FIGURE IV.5.2: DODAG Simulation2 avant déclenchement d'action correctif.

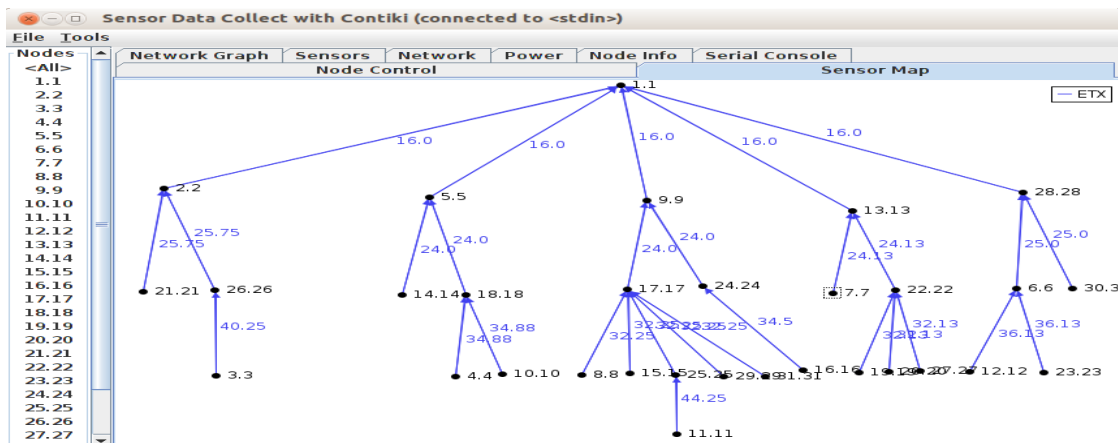


FIGURE IV.5.3: DODAG Simulation3 avant déclenchement d'action correctif.

À travers le DODAG, j'identifiais les nœuds défaillants, par exemple pour la simulation 1 j'identifiais le nœud 8 et pour la simulation 2 le nœud 20 et pour la simulation 3 le nœud 9. Cela permet de fournir des informations précieuses pour l'analyse de résultat.

Etape 2: le déclenchement d'action correctif. Je supprime le nœud 8 pour la simulation (1), le nœud 20 pour la simulation (2) et le nœud 9 pour la simulation (3),

Par la suite je calcule les indicateurs locaux pour tous les autres nœuds.les scénarios suivante montre les étapes pour les calcules :

IV.3.1. Les scénario de la simulation :

IV.3.1.1. Scénario 1 (Centralité de degré (C_D)) :

D'après les calcules des centralités de degré, le nœud 21 a la valeur de degré minimal par rapport aux autres nœuds.

Donc le nœud 21 remplace le nœud 8 dans la simulation (1), le nœud 6 remplace le nœud 20 dans la simulation (2) et le nœud 3 remplace le nœud 9 dans la simulation (3)

Pour le remplacement et la mobilité des nœuds je dois passer par l'outil "Mobility" Comme illustre les figures suivante :

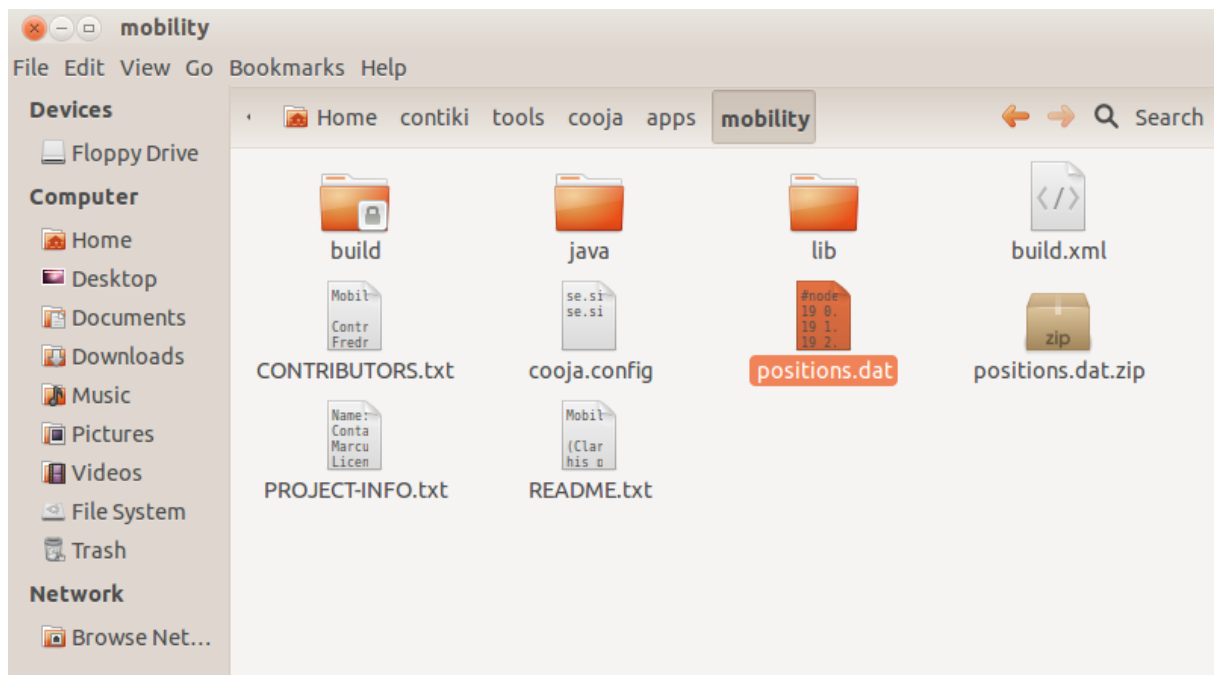


FIGURE IV.6: le fichier Mobility.

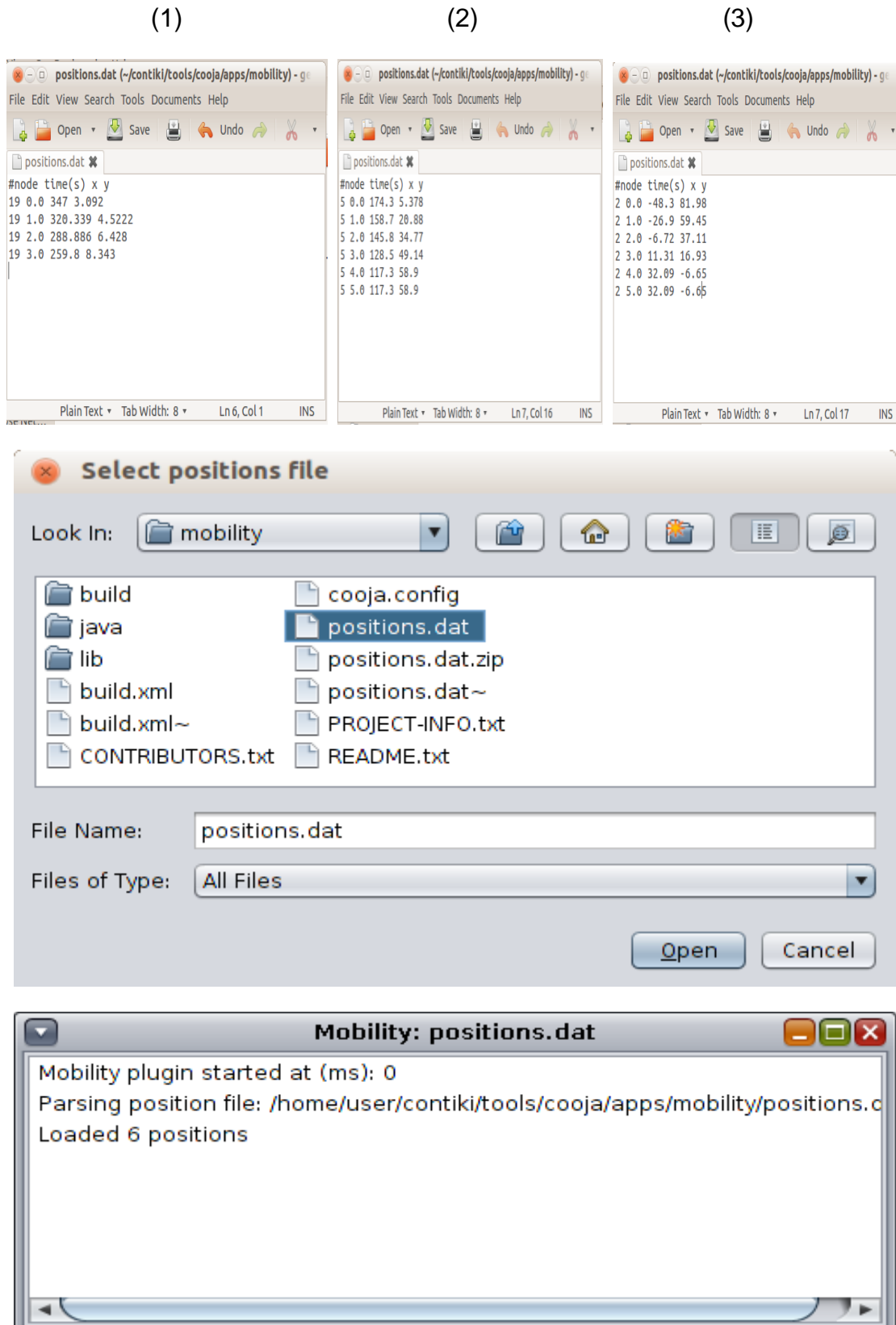


FIGURE IV.7: les étapes de la mobilité.

Les figures suivantes montrent le remplacement (la mobilité) des nœuds défaillants par des nœuds choisis en fonction de leur centralité de degré pour les trois simulations.

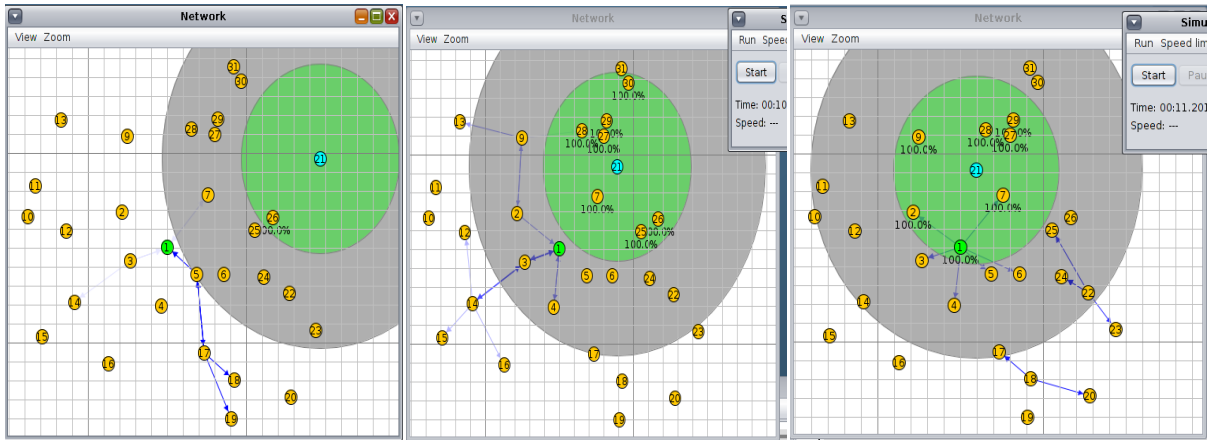


FIGURE IV.8.1: Mobilité des nœuds scénario 1 simulation 1.

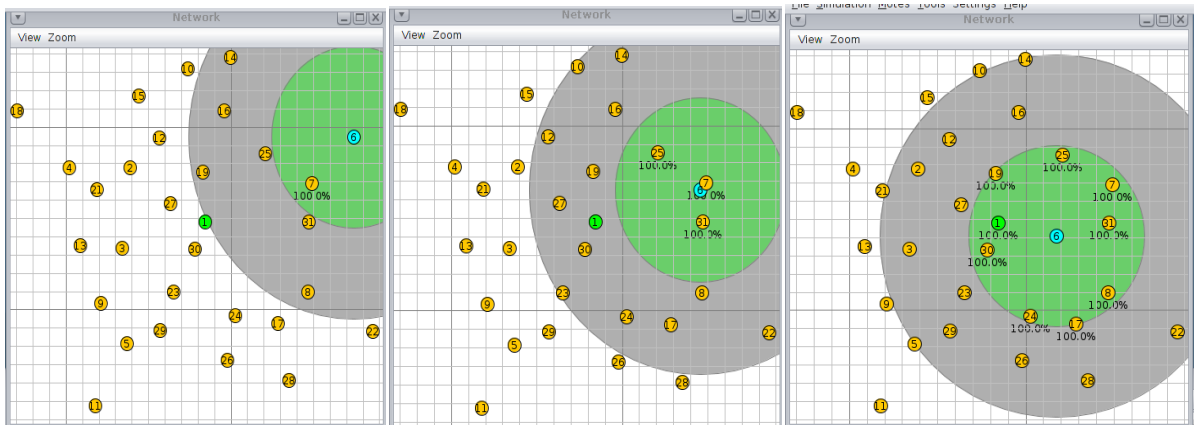


FIGURE IV.8.2: Mobilité des nœuds scénario 1 simulation 2.

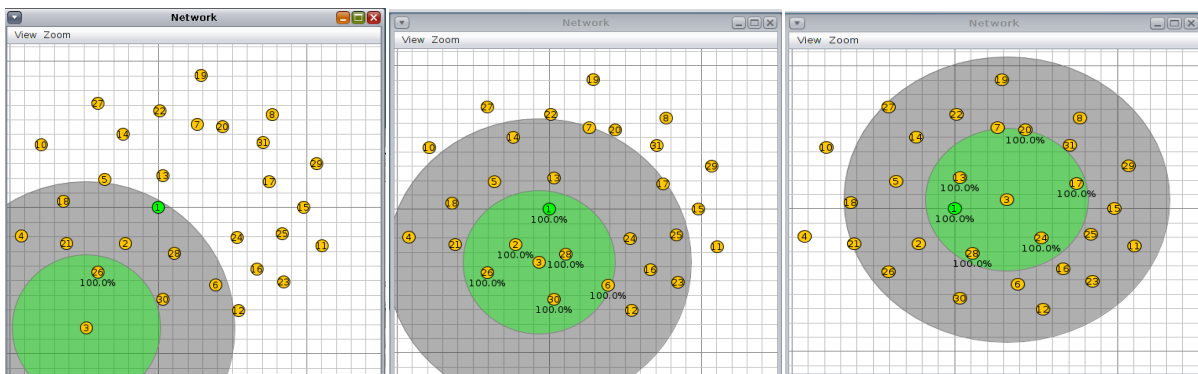


FIGURE IV.8.3: Mobilité des nœuds scénario 1 simulation 3.

Les figures [IV.9, IV.10, IV.11 et IV.12] montrent la modification du DODAG après le déclenchement d'action correctif. Car lorsqu'un nœud défaillant est remplacé par un nouveau nœud, cela peut entraîner des ajustements dans la structure hiérarchique du DODAG. Les nœuds voisins du nœud défaillant doivent mettre à jour leurs informations de routage pour prendre en compte un nouveau nœud voisin.

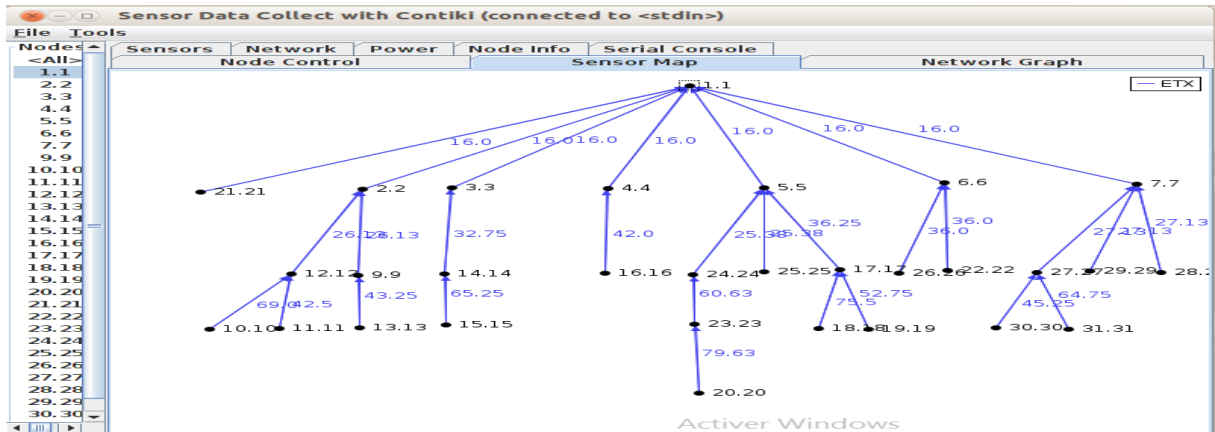


FIGURE IV.9.1: DODAG scénario 1S1 après le déclenchement d'action correctif.

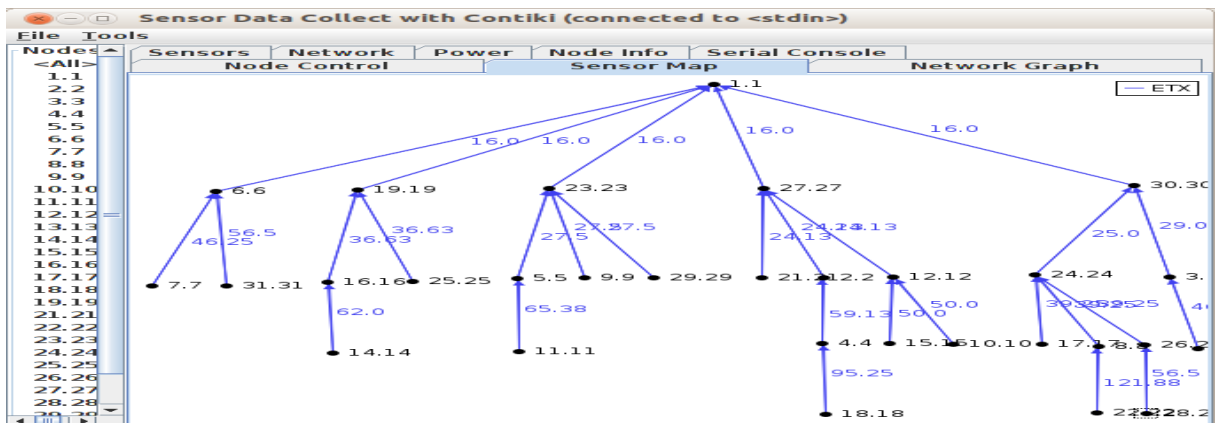


FIGURE IV.9.2: DODAG scénario 1S2 après le déclenchement d'action correctif.

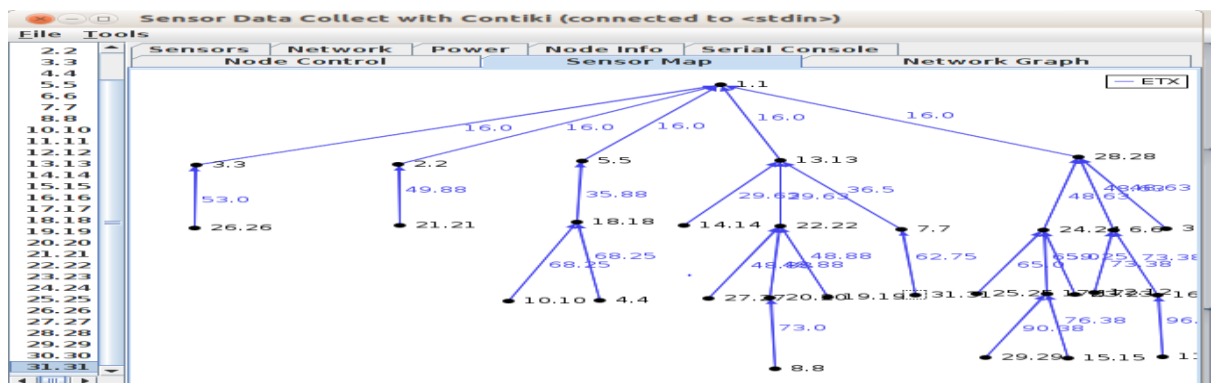


FIGURE IV.9.3: DODAG scénario 1S3 après le déclenchement d'action correctif.

IV.3.1.2. Scénario 2 (Centralité d'éloignement moyen (C_E) :

Après les calculs des centralités d'éloignement moyen j'ai constaté que le nœud 20 avait la distance moyenne avec l'ensemble des autres sommets, alors il remplace le nœud 8 dans la simulation (1), le nœud 18 remplace le nœud 20 dans la simulation (2) et le nœud 4 remplace le nœud 9 dans la simulation (3)

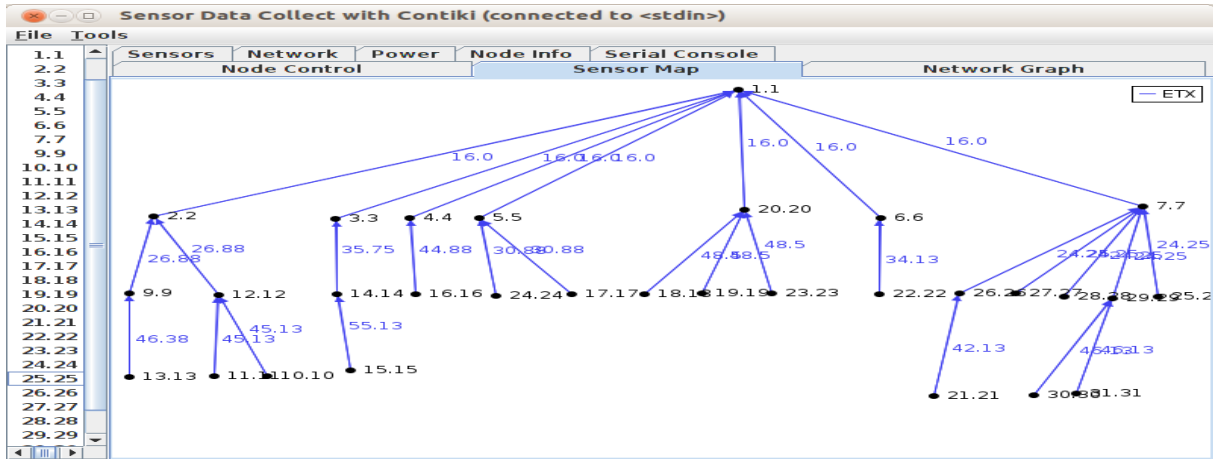


FIGURE IV.10.1: DODAG scénario2S1 après le déclenchement d'action correctif.

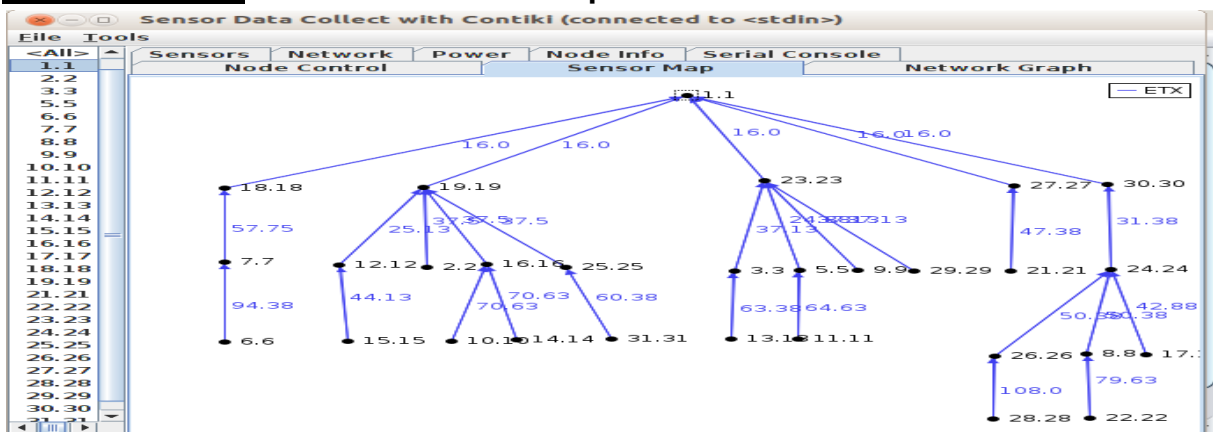


FIGURE IV.10.2: DODAG scénario2S2 après le déclenchement d'action correctif.

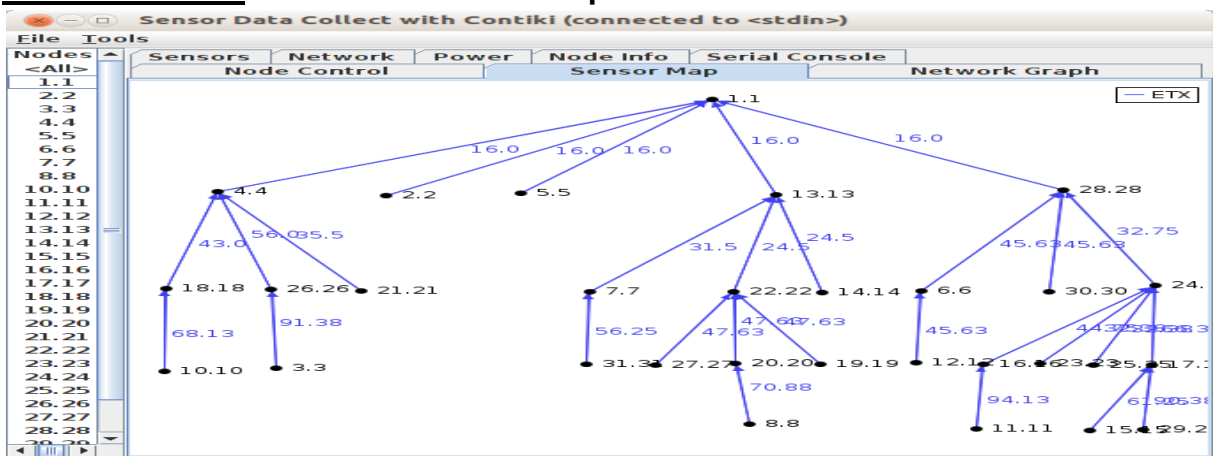


FIGURE IV.10.3: DODAG scénario2S3 après le déclenchement d'action correctif.

IV.3.1.4. Scénario 4 (Centralité d'intermédiarité (C_i) :

Après les calculs des centralités d'intermédiarité, j'ai constaté que le nœud 26 a 29 liaisons avec les autres nœuds qui peuvent être contrôlées, alors il remplace le nœud 8 dans la simulation (1), le nœud 7 remplace le nœud 20 dans la simulation (2) et le nœud 26 remplace le nœud 9 dans la simulation (3)

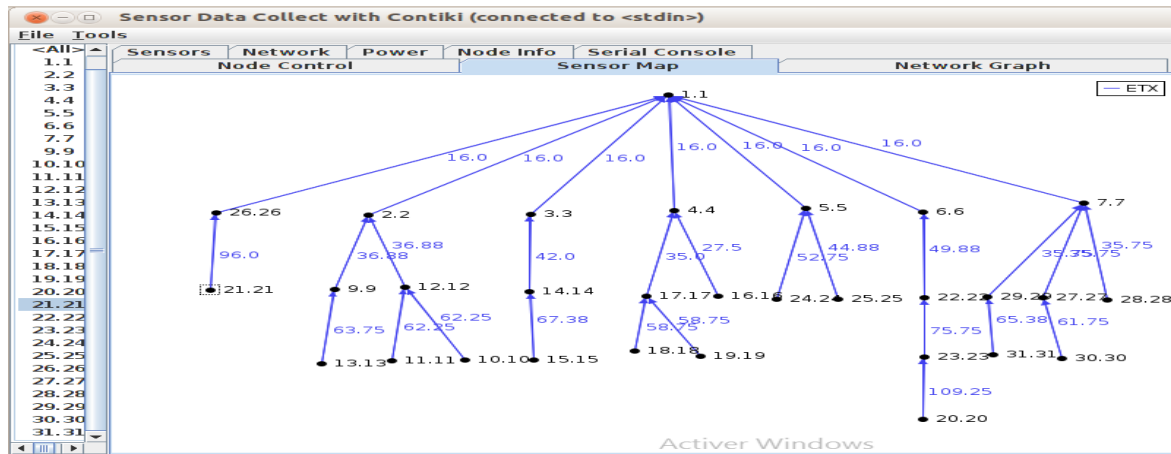


FIGURE IV.12.1:DODAG scénario4S1 après le déclenchement d'action correctif.

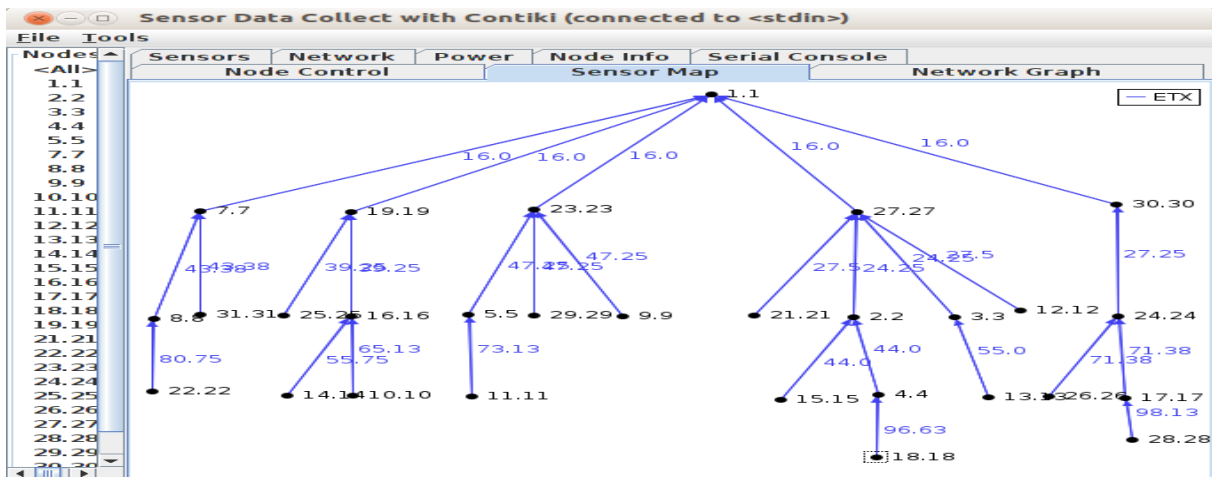


FIGURE IV.12.2:DODAG scénario4S2 après le déclenchement d'action correctif.

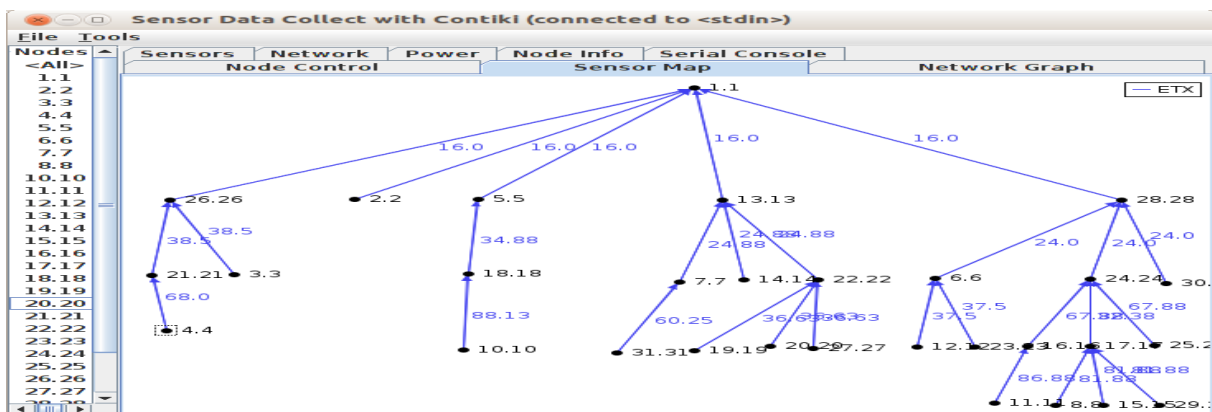


FIGURE IV.12.3:DODAG scénario4S3 après le déclenchement d'action correctif.

IV.4. Résultats des simulations :

J'ai effectué plusieurs simulations. Par la suite, j'ai simulé le déclenchement d'action correctif et après j'ai calculé le temps requis pour la construction du DODAG avec ces indicateurs. cela permet d'approfondir l'analyse des résultats et de comparer les performances des différents indicateurs pour mieux comprendre les implications et les limitations spécifiques de chaque indicateur dans mon étude pour avoir l'indicateur local de position le plus efficace pour la tolérance aux pannes dans les RCSF.

La figure suivante illustre le temps requis pour la construction du DODAG en fonction des indicateurs locaux de position dans les trois simulations.

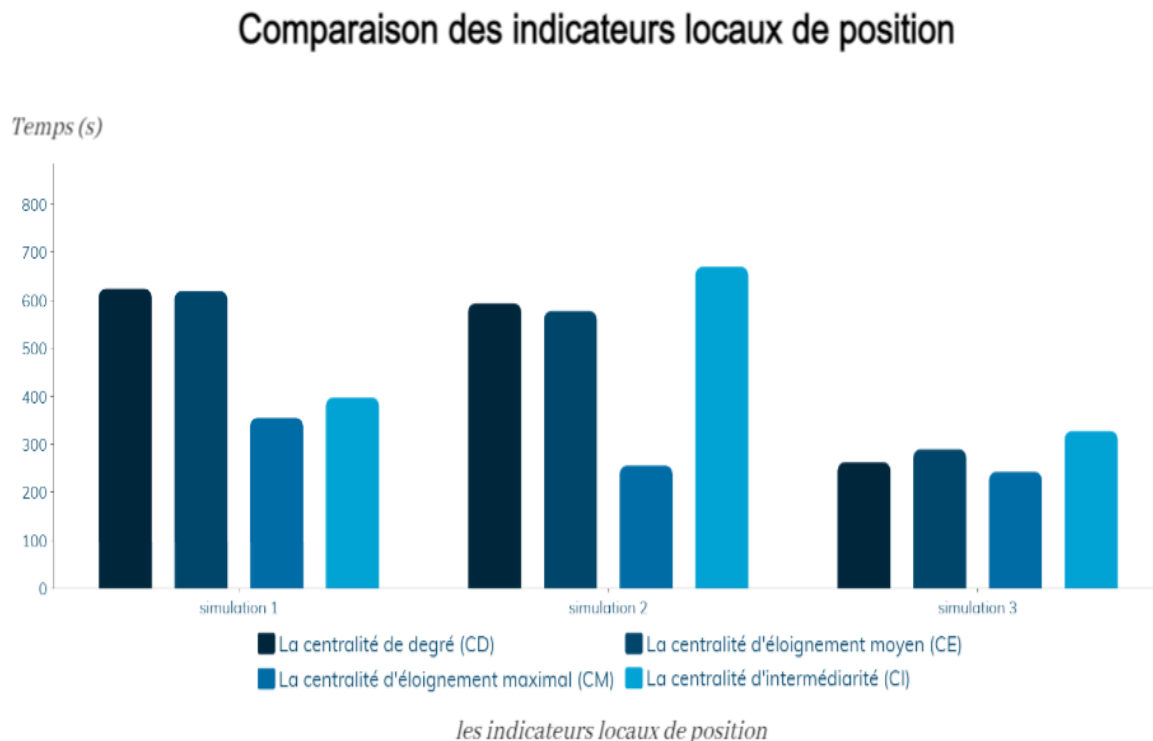


FIGURE IV.13: Résultats de simulation.

1. Les temps requis pour la construction du DODAG dans les simulations 1 et 2 sont élevés par rapport aux temps dans la simulation 3.
2. Le temps requis pour la construction du DODAG dans les simulations 2 et 3 utilisant la centralité d'intermédiarité est le plus élevé par rapport à la simulation 1.
3. Le temps requis pour la construction du DODAG dans les trois simulations utilisant la centralité de degré et la centralité d'éloignement moyen est toujours élevé.
4. Le temps requis pour la construction du DODAG dans les trois simulations utilisant la centralité d'éloignement maximal est le plus diminué.

IV.5. L'analyse des résultats des simulations :

Pour analyser le temps requis pour la construction du DODAG en fonction des indicateurs locaux de position dans les trois simulations, j'ai effectué une comparaison des temps de construction pour chaque indicateur. Cela me permettra de déterminer lequel des indicateurs offre les meilleures performances en termes de temps.

1. Les différents temps requis pour la construction du DODAG dans les trois simulations peuvent être attribués à des topologies de réseau différentes.

La topologie du réseau, c'est-à-dire la configuration des nœuds et des liens entre eux, peut avoir un impact significatif sur le temps requis pour la construction du DODAG.

Dans chaque simulation, la topologie spécifique du réseau peut influencer la manière dont les nœuds sont connectés les uns aux autres et comment le DODAG est construit. Certaines topologies peuvent être plus complexes que d'autres, ce qui peut nécessiter plus de temps pour établir les relations hiérarchiques dans le DODAG.

Les facteurs suivants peuvent contribuer à des topologies de réseau différentes :

Densité du réseau : Un réseau avec une plus grande densité, c'est-à-dire un grand nombre de nœuds dans une zone donnée, peut nécessiter plus de temps pour établir les liens entre les nœuds et construire le DODAG.

Répartition spatiale des nœuds : Si les nœuds sont répartis de manière uniforme dans l'espace, la construction du DODAG peut être relativement rapide. Cependant, si les nœuds sont regroupés dans certaines zones ou s'ils suivent une distribution spatiale particulière, cela peut compliquer la construction du DODAG et augmenter le temps requis.

Connectivité du réseau : Un réseau avec une connectivité élevée, c'est-à-dire avec de nombreux liens entre les nœuds, peut nécessiter plus de temps pour établir la structure hiérarchique du DODAG.

2. Le temps requis pour la construction du DODAG dans les simulations 2 et 3 utilisant la centralité d'intermédiation est le plus élevé par rapport à la simulation 1.
3. Le temps requis pour la construction du DODAG dans les trois simulations utilisant la centralité de degré et la centralité d'éloignement moyen est toujours élevé.

Cela suggère que cet indicateur peut prendre plus de temps pour établir les relations hiérarchiques dans le DODAG par rapport aux autres indicateurs évalués.

La complexité du calcul de la centralité d'intermédiarité peut expliquer pourquoi le temps requis pour la construction du DODAG est plus élevé dans les simulations utilisant cet indicateur. Le processus de recherche nombre de liaisons entre les autres sommets qui peuvent être contrôlées depuis un sommet donné peut nécessiter des calculs supplémentaires et des opérations de recherche complexes, ce qui peut augmenter le temps requis. Peut également être influencé par d'autres facteurs tels que la taille du réseau, la méthode de construction du DODAG. Ces facteurs peuvent tous jouer un rôle dans les variations des temps de construction observés.

Les temps de construction du DODAG peuvent varier en fonction de la taille du réseau, de la densité des nœuds, de la méthode de construction utilisée.

4. Le temps requis pour la construction du DODAG dans les trois simulations utilisant la centralité d'éloignement moyen est le plus diminué.

Cela suggère que cet indicateur local de position présente des avantages en termes de temps de calcul par rapport aux autres indicateurs tels que la centralité de degré ou la centralité d'éloignement moyen.

La réduction du temps requis pour la construction du DODAG peut être bénéfique dans les réseaux de capteurs sans fil, où les ressources computationnelles peuvent être limitées. Une réduction du temps de calcul signifie une utilisation plus efficace des ressources et une construction plus rapide du DODAG, ce qui peut être important pour assurer des performances optimales du réseau.

si le temps requis pour la construction du DODAG dans les trois simulations après l'utilisation et le calcul de la centralité d'éloignement maximal est le plus diminué, cela peut indiquer que cet indicateur offre une meilleure efficacité de calcul par rapport aux autres indicateurs.

Les résultats de simulation ont prouvé l'importance du choix de la centralité d'éloignement maximal (CM). Et prouve être un bon indicateur local de position pour la tolérance aux pannes dans les réseaux de capteurs sans fil

La centralité d'éloignement maximal peut donc être un outil précieux dans la planification de la tolérance aux pannes dans les réseaux de capteurs sans fil, en identifiant les nœuds les plus critiques et en prenant des mesures pour les protéger contre les pannes ou les défaillances.

IV.6. Conclusion :

Dans ce chapitre, j'ai présenté mon environnement de travail le système d'exploitation open-source Contiki, le simulateur Cooja.

Ensuite, j'ai décrit les étapes de la simulation et le fonctionnement de la mobilité des nœuds. Et enfin, j'ai fait une comparaison des temps requis pour la construction du DODAG en fonction des indicateurs locaux de position dans les trois simulations dans le but de mon étude et j'ai évalué et conclure que la centralité d'éloignement maximal est un indicateur locaux de position efficace pour la tolérance aux pannes dans un réseau de capteurs sans fil,

CONCLUSION GENERALE

CONCLUSION GENERALE

Les réseaux de capteurs sont composés d'un très grand nombre de dispositifs de communication ultra petits, autonomes avec des ressources de calcul et d'énergie limitées. Ils sont actuellement considérés comme l'une des technologies qui bouleverse notre façon de vivre, grâce à leur utilisation dans différents domaines d'application. Cependant, les réseaux de capteurs sans fil rencontrent plusieurs problèmes qui affectent leur bon fonctionnement dû à leurs caractéristiques ; tels que les limitations de batterie, le type de communication, les environnements hostiles où sont déployés les capteurs, etc... La tolérance aux pannes est donc la capacité de maintenir les fonctionnalités du réseau sans interruption due à une panne d'un nœud capteur. Par ailleurs, l'assurance de la tolérance aux pannes dans le domaine des réseaux de capteurs sans fil représente un défi de recherche très important, plus particulièrement dans ce type de réseaux qui sont caractérisés par les contraintes des nœuds capteurs.

Pour cela ce mémoire est structuré autour de quatre (04) chapitres. Le premier chapitre présente les notions générales sur les réseaux de capteurs sans fil, j'ai commencé par la définition des réseaux sans fil et les classifications passant à la définition d'un RCSF ainsi que les différentes caractéristiques, types possibles de ces derniers. Ce chapitre permet également de faire une présentation des différents protocoles de routage et les applications conçus pour les RCS. Il est terminé par une présentation de différentes problématiques présentes dans les RCSF.

Ensuite le second chapitre où j'ai détaillé le problème de tolérance aux pannes. J'ai présenté une classification des différents types de pannes ainsi qu'une définition de la tolérance aux pannes. Ce chapitre me permet aussi de discuter la procédure générale de tolérance aux pannes, ainsi que les différentes techniques de gestion et solutions de pannes.

De plus dans le troisième chapitre une présentation de la théorie des graphes, ainsi qu'une présentation des différents outils de description des graphes, les indicateurs locaux et globaux et j'ai détaillé les différents indicateurs locaux de position pour la tolérance aux pannes dans les RCSF.

Dans le quatrième chapitre, j'ai présenté d'abord mon environnement de simulation, le système d'exploitation CONTIKI et le simulateur COOJA. Ensuite, les étapes et les scénarios de la simulation. La dernière partie de ce chapitre sera consacrée à l'analyse l'évaluation des résultats.

Je me suis intéressé à la problématique de la tolérance aux pannes dans les réseaux de capteurs sans fil. En particulier, je me suis focalisé sur Le problème du remplacement des nœuds défaillants et la restauration de la connectivité après l'occurrence d'une panne. Pour cela j'ai effectué plusieurs simulations ou j'ai créé un réseau de capteurs sans fil composé de (31 nœuds avec des positions aléatoires).

Par la suite, j'ai simulé la panne et calculé les quatre centralités (la centralité de degré (C_D), la centralité d'éloignement moyen (C_E), la centralité d'éloignement maximal (C_M) et la centralité d'intermédiarité (C_i)). Après j'ai remplacé les nœuds de défaillance par des nœuds correspondant aux résultats des calculs dans le but d'évaluer les métriques déjà citées et les comparer pour avoir l'indicateur locaux de position le plus efficace pour la tolérance aux pannes dans les RCSF.

Dans mon étude, j'ai mené une analyse approfondie des indicateurs locaux de position pour le remplacement des nœuds défaillants dans les réseaux de capteurs sans fil. Et les résultats obtenus ont confirmé que la centralité d'éloignement maximal (C_M) est un indicateur local de position extrêmement efficace. Cette approche améliore la connectivité, réduit les perturbations, optimise l'utilisation des ressources et augmente la durée de vie du réseau sans fil. Ces résultats soulignent l'importance de la centralité d'éloignement maximal dans la gestion et la maintenance des réseaux de capteurs.

J'ai remplacé les nœuds défaillants par des nœuds ayant une centralité d'éloignement maximal élevée, j'ai constaté une réduction notable des délais de transmission. Les nœuds avec une centralité d'éloignement maximal élevée sont généralement plus proches des autres nœuds du réseau, ce qui permet une transmission plus rapide des données.

Bien que Contiki soit largement utilisé dans les études sur les réseaux de capteurs sans fil (RCSF), il présente certaines limitations, notamment en termes de temps de simulation. Contiki peut être limité en termes de temps de simulation pour les grands réseaux de capteurs ou pour des scénarios complexes. En raison de la complexité des simulations et des contraintes de ressources des nœuds de capteurs, les simulations avec Contiki peuvent prendre beaucoup de temps pour être exécutées, ce qui peut être un inconvénient lors de l'exploration de scénarios de grande envergure ou de longues périodes de temps. Ainsi que mon étude ait démontré l'efficacité de la centralité d'éloignement maximal en tant qu'indicateur dans les réseaux de capteurs, mais il reste des opportunités pour des études futures afin d'améliorer ma compréhension de son utilisation. Ces domaines d'amélioration potentiels peuvent contribuer à renforcer la pertinence et l'applicabilité de la centralité d'éloignement maximal dans les réseaux de capteurs sans fil.

Malgré les limites rencontrées, ma recherche a apporté une contribution significative en approfondissant la compréhension des réseaux de capteurs sans fil (RCSF) et de la tolérance aux pannes. En mettant l'accent sur l'amélioration de cette tolérance grâce aux indicateurs locaux de position, j'ai exploré une approche novatrice qui peut avoir un impact important sur la fiabilité et la résilience des RCSF.

Enfin, j'espère que mon travail sera une source d'inspiration pour d'autres personnes qui s'intéressent à ce domaine passionnant.

REFERENCES BIBLIOGRAPHIQUE

REFERENCES BIBLIOGRAPHIQUE

- [1] Auteur. Date_maj. Chapitre 1 Les réseaux de capteurs : concepts de base. Récupéré le 02 février 2023 de https://elearning-facsci.univ-annaba.dz/pluginfile.php/3070/mod_resource/content/1/chapitre%2001-RCSF.pdf
- [2] Wikipédia. (2023, mise à jour 25 janvier). Réseau sans fil - Wikipédia. Récupéré le 02 février 2023 de https://fr.wikipedia.org/wiki/Réseau_sans_fil
- [3] document intitulé « Réseaux sans fil - Introduction » issu de l'encyclopédie informatique Comment Ça Marche (www.commentcamarche.net) est mis à disposition sous les termes de la licence Creative Commons. Récupéré le 02 février 2023 de <https://web.maths.unsw.edu.au/~lafaye/CCM>
- [4] Theastrologypage. 2023(mise à jour Février). Qu'est-ce qu'un réseau cellulaire? - définition de techopedia. Récupéré le 02 février 2023 de <https://fr.theastrologypage.com/cellular-network>
- [5] Wikipédia. 2023(mise à jour 13 janvier). Réseau ad hoc - Wikipédia. Récupéré le 03 février 2023 de https://fr.wikipedia.org/wiki/Réseau_ad_hoc
- [6] S. Mnasri, N. Nasri et T. Val, "Contribution au déploiement optimisé des réseaux de capteurs sans fil", dans *Journées Nationales des Communications Terrestres (JNCT)*, 2014, pp. 2-13.
- [7] M. Le berre, "Optimisation de déploiement et localisation de cible dans les réseaux de capteurs", *thèse de doctorat de l'Université de technologie de Troyes*, juin 2014, pp. 1-30.
- [8] Techno Science. Date. Réseau de capteurs sans fil - Définition et Explications. Récupéré le 31 janvier 2023 de <https://www.techno-science.net/glossaire-definition/Reseau-de-capteurs-sans-fil.html>
- [9] B. Sahraoui, "La géolocalisation dans les réseaux de capteurs sans fil", *Mémoire de fin d'études cycle ingénieur d'état en Informatique*, 2011, pp. 10-15.
- [10] M.A.Sari, "Etude du RSSI pour l'estimation de la distance dans les réseaux de capteurs sans fil", mémoire pour l'obtention du diplôme de Master en Informatique, Département d'Informatique, Université Abou Bakr Belkaid– Tlemcen, 2017.
- [11] K.Beydoun . « Conception d'un protocole de routage hiérarchique pour les réseaux de capteurs »Thèse de doctorat, Spécialité :Informatique, l'u.f.r des sciences et techniques de l'université de Franche-Comté,2009.

- [12] A. Boulis, "Castalia: A simulator for Wireless Sensor Networks and Body Area Networks, Version 3.2 User's Manual", *NICTA, March 2011*, pp. 2-120.
- [13] Yacine Challal. (2008, Version1; 18 décembre) .Cours Réseaux de Capteurs Sans Fils - Architecture d'un RSCF. Récupéré le 01 février 2023 de https://moodle.utc.fr/file.php/498/SupportWeb/co/Module_RSCF_33.html
- [14] Auteur. Date. Chapitre 4 Les protocoles de routage dans les réseaux de Récupéré le 04 février 2023 de https://elearning-facsci.univ-annaba.dz/pluginfile.php/3073/mod_resource/content/1/Chapitre%204.pdf
- [15] L. SAMPER, Modélisations et analyses de réseaux de capteurs, thèse, Institut National Polytechnique de Grenoble, 2008.
- [16] Etienne Duris et Dominique Revuz tous deux Maître de Conférences à l'Université de Marne-la-Vallée et enseignants dans la filière Informatique Réseaux (IR). Mars 2006. Conclusion - Les Réseaux de capteurs sans fil. Récupéré le 04 février 2023 de <http://igm.univ-mlv.fr/~dr/XPOSE2006/Bunel/Conclusion.html>
- [17] Ali MAHMOUD, Annette BOHM and Magnus JONSON. "Wireless sensor networks for surveillance applications - A comparative survey of MAC protocols". In Proceedings of the 4th International Conference on Wireless and Mobile Communications (ICWMC'08), pp399-403, Washington, DC, USA, 2008.
- [18] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. "wireless sensor networks : a survey". Elsevier Science, 38(4), 2002.
- [19] John Paul WALTERS et al., "Wireless Sensor Network Security: A Survey", Department of Computer Science Wayne State University, 2006.
- [20] Boucif Amar BENSABAR, « Introduction à la sécurité des réseaux de capteurs sans fil » ; Cours, laboratoire de Mathématiques et Informatique Appliquées LAMIA, Université du Québec à Trois-Rivières.
- [21] <http://dSPACE.univ-tlemcen.dz/bitstream/112/5928/1/Reseaux-de-capteurs-tolerance-aux-pannes-agregateurs-NesC-TinyOs.pdf>
- [22] HOBLOS G., STAROSWIECKI M., AITOUCHA A. « Sur la Tolérance aux Fautes de Capteurs et d'Actionneurs », Journal Européen des Systèmes Automatisés, vol. 35, n°3, 331-352, 2001.
- [23] Taleb, A. A., Pradhan, D. K., & Kocak, T. (2009, June). A technique to identify and substitute faulty nodes in wireless sensor networks. Third International Conference on Sensor Technologies and Applications, SENSORCOMM'09. (pp. 346-351). IEEE.

- [24] Farinaz Koushanfar, Miodrag Potkonjak , Alberto Sangiovanni-Vincentelli. « fault tolerance in wireless sensor networks » Handbook of Sensor Networks e-book, Compact Wireless and Wired Sensing Systems, chapter 36, 2005.
- [25] B. Selic. "fault tolerance techniques for distributed systems". <http://www.ibm.com/developerworks/rational/library/114.html>, 2004.
- [26] **[Watts D. J. & Strogatz S. 98]** *Collective dynamics of 'small-world' networks*. Nature, 393:440–442.
- [27] Tonica, I., Décompositions arborescentes de graphes : Calcul, approximations heuristique, HDR, Université d'Orléans, 2006.
- [28] Broersma, H., T. Kloks, D. Kratsh et H. Müller, Independent sets in asteroidal triplefree graphs, Mémoire No. 1359, Université de Twente, Enschede, la Hollande, 1996.
- [29] BOLLOBAS B : Modern Graph Theory. Springer Verlag, New York, 1998, 394pp.
- [30] Wikipédia. (2023, Mise à jour 10 avril 2023 à 08:58). Concept en théorie des graphes- Wikipédia. de https://fr.wikipedia.org/wiki/Cycle_%28théorie_des_graphes%29
- [31] Trotignon, N., Graphes parfaits : Structure et algorithmes, thèse de Doctorat, Université Grenoble I, 2004.
- [32] Claude Grasland, GO303 : Organisation de l'espace (1) Analyse spatiale et modélisation des phénomènes géographiques, GRAPHES ET RESEAUX (Documents de cours), Université Paris VII / UFR GHSS , 2000-2001..
- [33] LAURENT CHAPELON (9 août 2007). CONNEXITÉ-hypergeo.eu. de <https://hypergeo.eu/connexite/>
- [34] **Freeman L. C. 79]**, *Centrality in social networks conceptual clarification*. Social Networks, 1(3):215-239, 1979.
- [35] **[Scott J. P. 00]** *Social Network Analysis: A Handbook*. Sage Publications Ltd, 2000.
- [36] **[Opsahl 08]** *Prominence and control: The weighted rich-club effect*. Physical Review Letters 101 (168702).
- [37] **[Newman M. E. J. 04]** *Fast algorithm for detecting community structure in networks*. Physical Review E, 69(6):066133, 2004
- [38] GRASLAND C: Cours de licence de géographie: Organisation de l'espace - Analyse spatiale et modélisation des phénomènes graphiques. Université Paris VII. <http://ibm2.cicrp.jussieu.fr/grasland/go303/ch1/ch1.html>

- [39] HURIOT J.-M., PERREUR J.: La centralité/ L'accessibilité. In AURAY J.-P. et al: Lacyclopédie d'économie spatiale, 1994, pp. 47-58
- [40] **[Borgatti S. P. & Everett M. G. 06]** *A graph theoretic perspective on centrality.* Social Networks 28(4):466–484
- [41] **[Bolland J. M. 88]** *Sorting out centrality: An analysis of the performance of four centrality models in real and simulated networks.* Social Networks 10(3):233–253
- [42] Muhammad Omer Farooq and Thomas Kunz. Operating systems for wireless sensor networks: A survey. *Sensors*, 11(6):5900–5930, 2011.
- [43] Philip Levis, Sam Madden, Joseph Polastre, Robert Szewczyk, Kamin Whitehouse, Alec Woo, David Gay, Jason Hill, Matt Welsh, Eric Brewer, et al. Tinyos: An operating system for sensor networks. *Ambient intelligence*, 35:115–148, 2005.
- [44] Adam Dunkels, Bjorn Gronvall, and Thiemo Voigt. Contiki-a lightweight and flexible operatin system for tiny networked sensors. In *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*, pages 455–462. IEEE, 2004.
- [45] Alok Ranjan, HB Sahu, and Prasant Misra. A survey report on operating systems for tiny networked sensors. *arXiv preprint arXiv:1505.05269*, 2015. RÉFÉRENCES 57
- [46] Adam Dunkels. Rime-a lightweight layered communication stack for sensor networks. In *Proceedings of the European Conference on Wireless Sensor Networks (EWSN), Poster/Demo session, Delft, The Netherlands.* Citeseer, 2007.
- [47] Tinyos. [http :/www.tinyos.net/](http://www.tinyos.net/), 2010