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

Université Amar Thelidji- Laghouat

FACULTE: DE TECHNOLOGIE

DEPARTEMENT : D'ELECTRONIQUE

MEMOIRE DE MASTER

Réalisé par : MIHOUBI Bouchra

DOMAINE : Science et Technologie

FILIERE : Télécommunication

OPTION : Systèmes de télécommunications

Thème

Proposition d'un nouveau schéma de gestion de clés pour sécuriser la formation des clusters dans les RCSFs

Jury de soutenance :

Nom et Prénom	Grade	Qualité
BIRANE Mouhoub	MCA	Président
BOUZIDI Mohammed Redha	MCB	Examinateur
MESMOUDI Samira	MCB	Encadrante

Promotion : 2022/2023

Remerciements

قَالَ رَسُولُ اللَّهِ ﷺ: «مَن لا يشكرُ النَّاسَ لا يشكرُ الله»

*Je souhaite en premier lieu á remercier **Dieu**qui m'aaide á accomplir ce modeste travail et qui m'a donné toute la patience et la volonté pour surpasser tous les moments difficiles durant la réalisationde ce projet.*

*En second lieu, je tiens à exprimer ma profonde gratitude et mes sincères remerciements á ma promotrice **Mme. MESMOUDI Samira**pour avoir dirigé ce travail, pour son aide et ses précieux conseils ainsi que pour les nombreuses discussions que nous avons effectué.*

Je tiens également à adresser mes remerciements aux membres du jury pour avoir accepté d'examiner mon travail et de l'enrichir par leurs propositions.

Je voudrai aussi exprimer ma vive reconnaissance envers tous les enseignants de département d'électronique ainsi que tous ceux qui ont participé à ma formation.

Enfin, merci á toutes les personnes qui m'ont soutenu tout au long de cette aventure académique.

Dédicaces

Je dédie cet événement marquant de ma vie à la mémoire demon père ***El haj TAHER*** *(que Dieu bénisse son âme), qui m'a toujours poussé, motivé et encouragé dans mes études. J'espère que,du monde qui est sien maintenant, il apprécie cet humblegeste comme preuve de reconnaissance de la part d'une fillequi a toujours priée pour le salut de son âme. Puisse Dieu, le tout puissant, l'avoir en sa sainte miséricorde.*

À ma ***chèremère****qui était toujours avec moi, qui m'a soutenue et encourage durant mes études.*

À mes sœurs et mon frère, pour leur amour,leur soutien et leur encouragement.

À mes chères amies ***Lina*** *et* ***Meriem****.*

À mes proches et ceux qui me donne de l'amour et la vivacité.

À tous ceux que j'aime.

ملخص

شهدت" شبكات الاستشعار اللاسلكية (RCSF) "جذبًا كبيرًا بسبب تطبيقاتها الواسعة في المجالات العسكرية والمدنية. ومع ذلك، تجعل القيود الكبيرة على الطاقة والذاكرة والبيئة القاسية التي يمكن نشرها فيها هذا النوع من الاستشعار عرضة للهجمات. وبالتالي، حماية هذا النوع من الشبكات باستخدام حلاً آمنًا مخصصًا للأجهزة المستشعرة هو تحدي يجب معالجته. يتم ضمان هذه الأمان عادةً عبر تشفير البيانات المرسلة، مما يتطلب إنشاء العديد من المفاتيح التشفيرية. إدارة المفاتيح هي الوظيفة الأساسية الأولى حيث يحتاج العقد إلى مفتاح مشترك صالح لاستخدام آليات التشفير.

في هذا مشروع التخرج، نقترح بروتوكول إدارة المفاتيح CFKM لشبكات الاستشعار اللاسلكية الهرمية. اقتراحنا يضمن تكوين العناقيد وإنشاء المفاتيح في الشبكة. بالتالي، لا يقدم CFKM ميزات أمان موثوقة فحسب، بل يحسن أيضًا استهلاك الطاقة والتكاليف الزائدة المتعلقة بالاتصال واستخدام الذاكرة. النتائج المقدمة في هذا البحث مأخوذة من محاكاة متعددة تظهر جدوى وفعالية اقتراحنا.

الكلمات المفتاحية: شبكة الاستشعار اللاسلكية، الأمان، إدارة المفاتيح، التشفير، التجميع.

Résumé

Les réseaux de capteurs sans fil (RCSF) ont attiré beaucoup d'attention en raison de leurs vastes applications dans les domaines militaires et civils. Cependant, les contraintes énergétiques et de mémoire et l'environnement hostile dont lesquels ils peuvent être déployés, rendent ce type de capteurs vulnérables aux attaques. De ce fait, la protection de ce type de réseau en utilisant des solutions de sécurité adaptées aux capteurs est un chalenge qui va être traité. Cette sécurité est généralement garantie par le cryptage des données transmises, ce qui nécessite l'établissement de nombreuses clés cryptographiques. La gestion de clés est la première fonction fondamentale puisque les nœuds ont besoin d'une clé commune valide pour exploiter les mécanismes de cryptographie.
Dans ce projet de fin d'étude, nous proposons CFKM, un protocole de gestion de clés pour les réseaux de capteurs sans fil hiérarchiques. Notre proposition permet d'assurer la formation des clusters et l'établissement des clés dans le réseau. Ainsi, CFKM ne fournit pas seulement des mécanismes de sécurité fiables, il optimise également la consommation d'énergie et les surcoûts liés à la communication et à l'utilisation de la mémoire. Les résultats présentés dans ce mémoire sont issus de plusieurs simulations, qui démontrer la faisabilité et l'efficacité de notre proposition.

Mots clés : Réseau de capteurs sans fil, la sécurité, la gestion de clés, la cryptographie, le clustering.

Abstract:

The wireless sensor networks (WSNs) have attracted significant attention due to their wide-ranging applications in both military and civilian domains. However, the energy and memory constraints and the hostile environments in which they may be deployed make these sensors susceptible to attacks. Therefore, safeguarding this network type using security solutions tailored to sensors is a challenge that will be addressed. Typically, data encryption ensures this security, necessitating the establishment of numerous cryptographic keys. Key management is the primary and essential function, as nodes require a valid common key to operate cryptographic mechanisms.
In this end-of-study project, we propose CFKM, a key management protocol for hierarchical wireless sensor networks. Our proposal ensures the formation of clusters and the establishment of keys within the network. As a result, CFKM not only provides reliable security mechanisms but also optimizes energy consumption and minimizes communication and memory usage costs. The results presented in this paper stem from multiple simulations, demonstrating the feasibility and effectiveness of our proposal.

Keywords: Wireless Sensor Network, Security, Key Management, Cryptography, Clustering.

Table des matières

CHAPITRE3: APPROCHE DE GESTIONDE CLES PROPOSEE

Liste des figures

Liste des tableaux

Liste des abréviations

CFKM: Cluster formation and Key management scheme for Wireless sensor Networks.

SC-SPK: Secured Communication Key Establishment for Cluster based Wireless Sensor Networks –*Private Partial Keys.*

RCSF: Réseaux de Capteurs Sans Fil.

CH: Cluster-Head.

CM: Nœuds capteurs membres.

SB (BS): Station de Base.

COG: Centre de Gravité.

MEMS: Micro-Electro-Mechanical-Systems.

ADC: Analog-to-Digital Convertor.

GPS: Global Position System.

TinyOS: Tiny Operating System.

NesC: Network Embedded System C.

MAC: Message Code.

QOS: Quality Of Service.

LEACH: Low Energy Adaptive Clustering Hierarchy.

HEED: Hybrid Energy Efficient Distributed clustering.

TEEN: Threshold-sensitive Energy Efficient Sensor Network Protocol.

APTEEN: Adaptive Threshold-sensitive Energy Efficient Sensor Network Protocol.

PEGASIS: Power-Efficient Gathering in Sensor Informations Systems.

VGA: Virtual Grid Architecture Routing.

Introduction générale

La grande évolution dans les domaines de la micro-électronique, de la micromécanique, et des technologies de communication sans fil, ont permis de produire avec un coût raisonnable des petits dispositifs de détection et de communication. Ces dispositifs sont connus comme des nœuds capteurs. Ils ont la capacité de collecter et transmettre des données environnementales vers un point centralisé appelé la Station de Base ou le puit. L'ensemble des nœuds capteurs forme un Réseau de Capteurs Sans Fil (RCSF). De nos jours, les RCSFs couvrent des domaines d'applications très variés. Ils ont été initialement développés pour des besoins militaires tels que la surveillance des frontières. Par la suite, leur utilisation s'est répandue pour couvrir d'autres secteurs d'activités tels que l'environnement, la médecine, l'industrie et l'agriculture. Dans le domaine médical, ils permettent par exemple le suivi permanent et à distance du rythme cardiaque et de la tension artérielle des malades. Dans le domaine environnemental, leur importance est particulièrement avérée dans le cas où les nœuds sont déployés en grand nombre et largués par un hélicoptère dans des zones hostiles et dangereuses par exemple pour la détection des feux de forêts et la gestion des catastrophes naturelles.

En effet, malgré les avancées remarquables dans ce domaine, il reste encore beaucoup des problèmes à résoudre, parmi les plus fondamentales on à la sécurité d'échange des données.

Généralement, les capteurs sont déployés dans des zones non surveillées, la majorité des applications des RCSFs nécessitent un haut niveau de sécurité afin de fournir les exigences de sécurité de base et rendre ces applications invulnérables aux différentes attaques, empêchant un intrus de perturber le bon fonctionnement du réseau en prenant le contrôle des nœuds de capteurs. En plus, il est connu que les RCSF sont faciles à attaquer en raison de la nature du médium qui permet facilement qu'un intrus d'espionner, d'altérer ou d'injecter des données dans le réseau. Il est nécessaire donc d'intégrer un mécanisme de sécurité qui garantit un échange de données sécurisé.

Les nœuds capteurs sont limités en termes de calcul, de mémoire et des capacités énergétiques, ces contraintes influencent négativement le bon fonctionnement des techniques spéciales qui fournissent la sécurité requise. L'emploi des primitives cryptographiques notamment la cryptographie symétrique est l'une des solutions proposée pour faire face au problème de sécurité. En effet, afin d'atteindre les objectifs de sécurité, La gestion de clés constitue la pierre angulaire des autres mécanismes de sécurité, car presque tous les mécanismes de sécurité reposent sur le cryptage ou sont liés à celui-ci.

Nous proposons dans ce mémoire un nouveau protocole nommé CFKM (Cluster formation and Key management scheme for Wireless sensor Networks) dont l'objectif est de surpasser les limites des protocoles de gestion de clés existants. Notre approche est destinée aux réseaux de capteurs sans fils hiérarchiques. CFKM est déterministe et repose sur la cryptographie symétrique.

Afin d'offrir une performance globale optimisée, nous nous intéressons notamment à la contrainte énergétique du fait que les batteries des capteurs ne peuvent généralement être rechargées. Afin de surmonter ces contraintes, un nouveau algorithme de clustering ont été proposé pour découper le réseau en sous-réseaux appelés les clusters, pour chaque cluster le nœud qui a la meilleure position dans le cluster est élu comme chef de cluster, ce CH est chargé de collecter les données détectées par ses membres et de les envoyer à la station de base, ceci est dans le but de minimiser la consommation d'énergie et par conséquent augmente la durée de vie du réseau

Organisation de mémoire

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

- Le premier chapitre est une introduction et généralités sur les réseaux de capteurs sans fil : leurs définitions, leurs caractéristiques ainsi que leurs architectures et leurs domaines d'application sont présentés. En outre, nous avons présenté la notion de cluster et de clustering, propriétés, avantages et objectifs du clustering. Puis, nous donnons une classification des approches de clustering proposées dans la littérature. Ensuite, nous avons présenté quelques algorithmes de clustering.
- Dans le deuxième chapitre, nous présentons un aperçu sur les concepts de sécurité dans les RCSFs qui diffèrent des autres réseaux. Nous commençons d'abord par les limites des réseaux de capteurs qui rendent la sécurité pour ce type de réseaux un véritable défi. Enfin, nous identifions une taxonomie des attaques et nous discutons les besoins des différents mécanismes de sécurité destinés aux RCSFs
- Le troisième chapitre présente notre proposition liée au protocole de gestion de clés nommée CFKM (Cluster formation and Key management scheme for Wireless sensor Networks). Nous commençons d'abord par donner les détails de notre protocole, et nous effectuons par la suite une évaluation de ses performances par rapport au protocole SC-SPK.

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

Chapitre 1

Généralités sur les réseaux de capteurs sans fil

1.1. Introduction

Les réseaux de capteurs sont le fruit des dernières avancées technologiques dans le domaine des réseaux sans fil, la technologie « MEMS » (Micro-Electro-MechanicalSystems) et les systèmes embarqués [23]. Pour un prix modique et avec des moyens abordables, il est désormais possible de concevoir des composants, de petite taille, comprend un dispositif de capture et peut être utilisé dans courte portée via une connexion sans fil. La mise en réseau de ces composants, connus sous le nom de micro capteurs, réagissent aux événements et analysent les données capturées de grande surface.

Dans ce qui suit, on étudiera ce type de réseaux de capteurs sans-fil, ses principales caractéristiques, les différents domaines d'applications de ce type de réseau ainsi que les techniques de conservation énergétique. En outre, l'architecture, la topologie et la communication dans les réseaux de capteurs sera détaillée ainsi que les contraintes influençant les réseaux de capteurs sans fil.

1.2. Les nœuds de réseau de capteursans fil

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

Figure 1.1: Exemple d'un capteur.

1.2.1. Aspect matériel

Le nœud de capteur est composé principalement de quatre unités : l'unité d'acquisition, l'unité de traitement, l'unité de communication et l'unité d'énergie

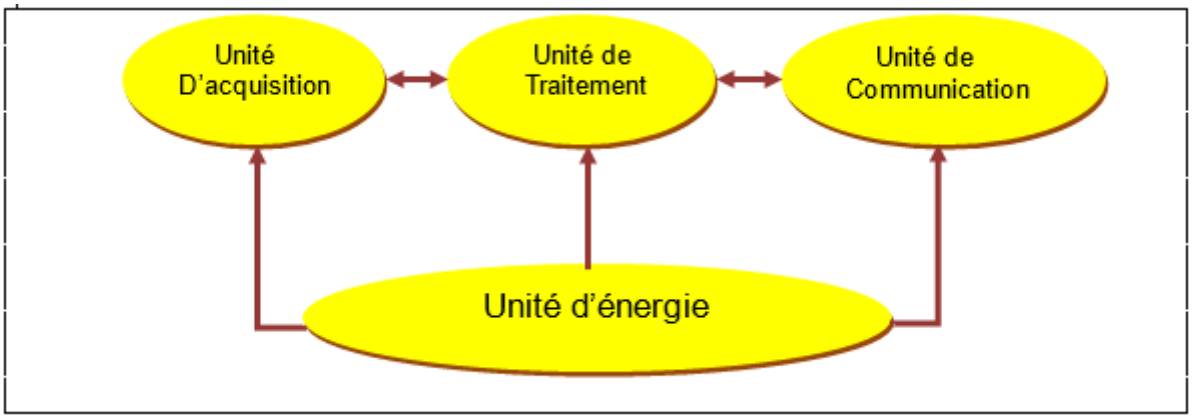


Figure 1.2: Architecture d'un nœud de capteur.

- **Unité d'acquisition :**

Généralement composée de deux sous-unités : les capteurs et les convertisseurs analogique-numérique (ADC: Analog-to-Digital Convertor).

- Le capteur obtient des mesures sur les paramètres environnementaux et les transformes en signaux analogiques.
- ADC convertit ces signaux analogiques en des signaux numériques

- **Unité de traitement :**

Composée d'un microcontrôleur et d'une mémoire intégrant un système d'exploitation spécifique, cette unité est responsable de tous les traitements effectués par un nœud capteur. Elle comprend deux interfaces : une interface avec l'unité d'acquisition et une autre avec l'unité de communication, L'unité de traitement contrôle les procédures permettant au nœud capteur de réaliser les tâches d'acquisition et de stockage de données collectées.

- **Unité de communication :**

Cette unité est chargée d'assurer la communication entres les nœuds capteurs composants le réseau en se basant sur le principe émetteur/récepteur, elle intègre un dispositif radio qui permet de garantir l'émission et la réception des données entres les nœuds via une communication sans fil.

- **Unité d'énergie (batterie)**

Alimente les unités d'acquisition, de traitement et de communication. Dans certaines applications (domaine militaire), il est impossible de recharger ou changer une batterie, donc avoir une meilleure gestion de la consommation d'énergie est primordial pour augmenter la durée de vie du réseau. Les nouveaux capteurs peuvent posséder des générateurs d'énergie renouvelable (par exemple: l'énergie solaire).

De plus, un nœud capteur peut être équipé d'autres composants supplémentaires tels que :

- Système de localisation géographique GPS (Global Position System).
- Un dispositif mobilisateur chargé de les déplacer en cas d'obligation.

1.2.2. Le système d'exploitation

Par conséquent, le domaine des capteurs sans fil est en plein essor, et de nombreux nouveaux produits sont susceptibles d'inonder le marché dans les prochaines années. Notamment parce que des technologies « open source » sont associées à ce succès avéré, comme **TinyOS**, développé à Berkeley.

TinyOS est un système d'exploitation open source conçu pour les capteurs embarqués sans fil et est actuellement utilisé par plus de 500 universités et centres de recherche à travers le monde.

La programmation sur cette plateforme se fait uniquement en **NesC** (langage C). La principale caractéristique de ce système d'exploitation est sa très petite mémoire (quelques kilo-octets). [5][6]

1.2.3. Vue d'ensemble des plates formes existantes

Actuellement, une large gamme de plateforme de micro¯capteurs est disponible. Leurs architectures et leurs tailles différentes selon les types d'applications auxquelles elles sont destinées. La (figure 1.3) indique l'évolution des capteurs à travers le temps.

Figure 1. 3: Progression des technologies de capteurs à travers le temps.

1.3. Réseaux de capteurs sans fil (RCSF)

Le déploiement des entités capteurs qui permet de collecter et de transmettre les données mesurées vers un ou plusieurs points de collecte, forme un réseau de capteurs sans fil. Ces réseaux sont composés de centaines, voire de milliers de capteurs avec une infrastructure décentralisée: tous les nœuds participent au fonctionnement du réseau.

1.3.1. Architecture des réseaux de capteurs sans fil

Un réseau de capteur sans fil est constitué d'un nombre plus ou moins grand de nœuds capteurs. Ces nœuds sont autonomes, distribués dans l'espace qui coopèrent pour surveiller des conditions environnementales ou physiques, tels que la température, le bruit, la vibration, la pression, le mouvement, etc. A l'origine, le développement des réseaux de capteur sans fil a été motivé par des applications militaires telles que la surveillance de champ de bataille. Cependant, ce type de réseau est maintenant employé dans plusieurs domaines d'applications civiles, comme la surveillance d'environnement, d'habitat, la surveillance médicale, l'automatisation des maisons et le contrôle du trafic [1].

L'architecture des réseaux de capteurs sans fil utilise beaucoup de sources. Historiquement, beaucoup de travaux relatifs ont été effectué dans le contexte des réseaux à auto-organisation, mobiles et Ad Hoc. Un réseau de capteurs est constitué essentiellement de plusieurs nœuds capteurs, un nœud sink (ou station de base) et un centre de traitement des données.

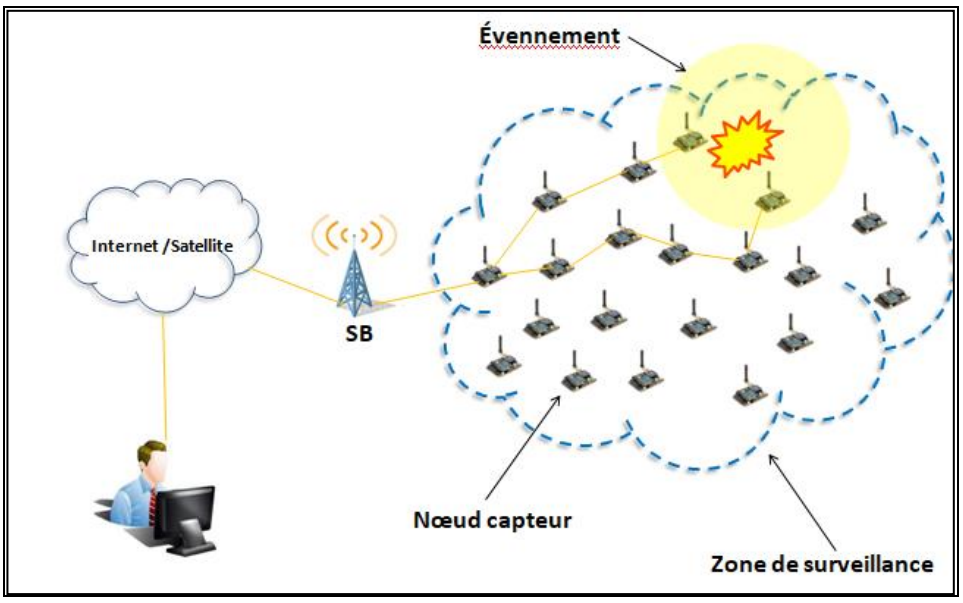


Figure 1.4: Architecture d'un réseau de capteur sans fil.

Les nœuds : sont des capteurs, leur type, leur architecture et leur disposition géographique dépendent de l'exigence de l'application en question. Leur énergie est souvent limitée puisqu'ils sont alimentés par des piles.

Le sink : est un nœud particulier du réseau: Il est chargé de la collecte des données issues des différents nœuds du réseau. Il doit être toujours actif puisque l'arrivée des informations est aléatoire. C'est pourquoi son énergie doit être illimitée.

Centre de traitement des données: c'est le centre vers lequel les données collectées par le sink sont envoyées. Ce centre a le rôle de regrouper les données issues des nœuds et les traiter de façon à en extraire l'information utile exploitable. Le centre de traitement peut être éloigné du sink, alors les données doivent être transférées à travers un autre réseau, c'est pourquoi on introduit une passerelle entre le sink et le réseau de transfert pour adapter le type de données au type du canal.

1.3.2. La communication dans un RCSF

La communication entre les nœuds capteurs dans le RCSF est représentée par une série de connexions contrôlées par plusieurs protocoles, ces derniers sont organisés sous forme ce qu'on appelle pile protocolaire utilisée par la station de base ainsi que par les autres nœuds capteurs composant le réseau, la figure ci-dessous illustre la pile protocolaire d'un RCSF.

Cette pile comporte cinq couches qui ont les mêmes fonctions que celles du modèle OSI ainsi que trois couches pour la gestion d'énergie, la gestion de la mobilité et la gestion des tâches.

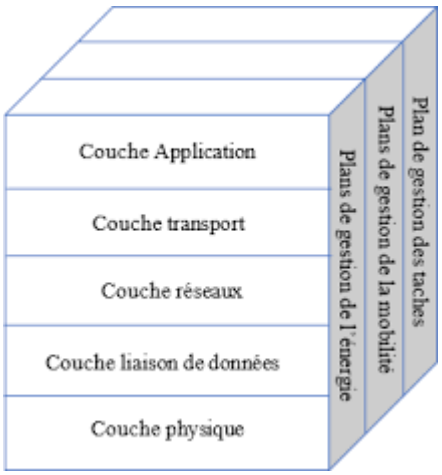


Figure 1.5: Pile protocolaire d'un RCSF.

Rôles des couches:

- ✓ Couche physique : Matériels pour envoyer et recevoir les données.
- ✓ Couche liaison de données : Gestion des liaisons entre les nœuds et les stations de base, contrôle d'erreurs.
- ✓ Couche réseau : Routage et transmission des données.
- ✓ Couche transport : Transport des données, contrôle de flux.
- ✓ Couche application : Interface pour les applications au haut niveau.
- ✓ Plan de gestion d'énergie : Contrôle l'utilisation d'énergie.
- ✓ Plan de gestion de mobilité : Gestion des mouvements des nœuds.
- ✓ Plan de gestion de tâche : Balance les tâches entre les nœuds afin d'économiser de l'énergie.

1.3.3. Topologie et organisation de RCSF

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

1.3.3.1. Topologie plate

Dans une topologie plate, le réseau est homogène, où tous les nœuds ayant les mêmes caractéristiques matérielles (même capacité de calcul, capacité énergétique, capacité de stockage, portée de communication, etc.). Cette architecture est utilisée pour une densité de capteurs élevée (plusieurs nœuds capteurs /m ^{2}). Les capteurs peuvent communiquer directement avec la station de base (Figure 1.6) en utilisant une forte puissance, ou via un mode multi-sauts avec des puissances très faibles (c'est-à-dire que l'information envoyée par un nœud récolteur doit transiter par plusieurs nœuds intermédiaires avant d'atteindre sa destination finale sur le réseau et sans aucun traitement supplémentaire sur la donnée transportée). [23]

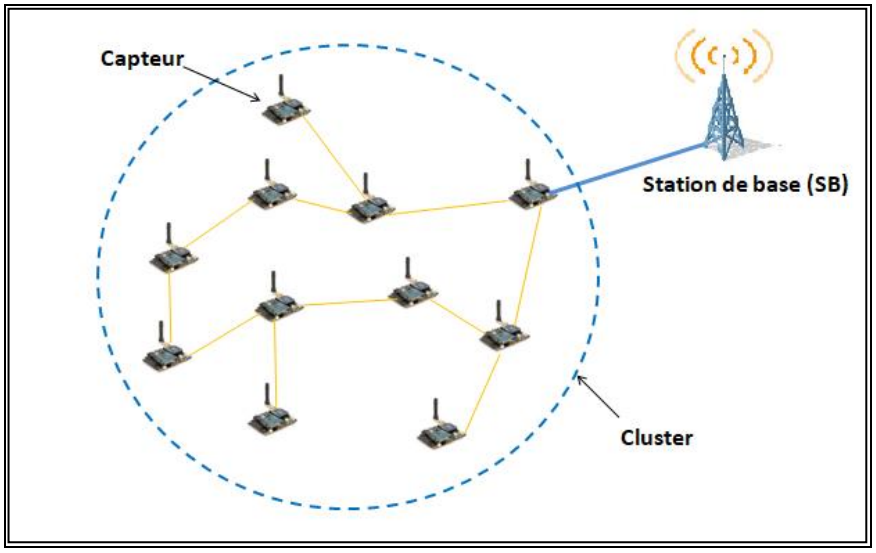


Figure 1.6: Topologie plate.

1.3.3.2. Topologie hiérarchique

Le principe de cette topologie est de partitionner le réseau en plusieurs groupes (ou clusters) dont chacun est vu comme un sous réseau ayant la topologie en étoile. Chaque groupe possède un chef qui relie les membres de son groupe à la station de base. La communication entre les nœuds capteurs et le chef du cluster peut être directe ou indirecte (en multi-sauts) pour les nœuds distants. Ainsi, il peut y avoir plusieurs niveaux dans la hiérarchie, où les chefs des clusters forment entre eux des chaînes menant vers la station de base.[23]

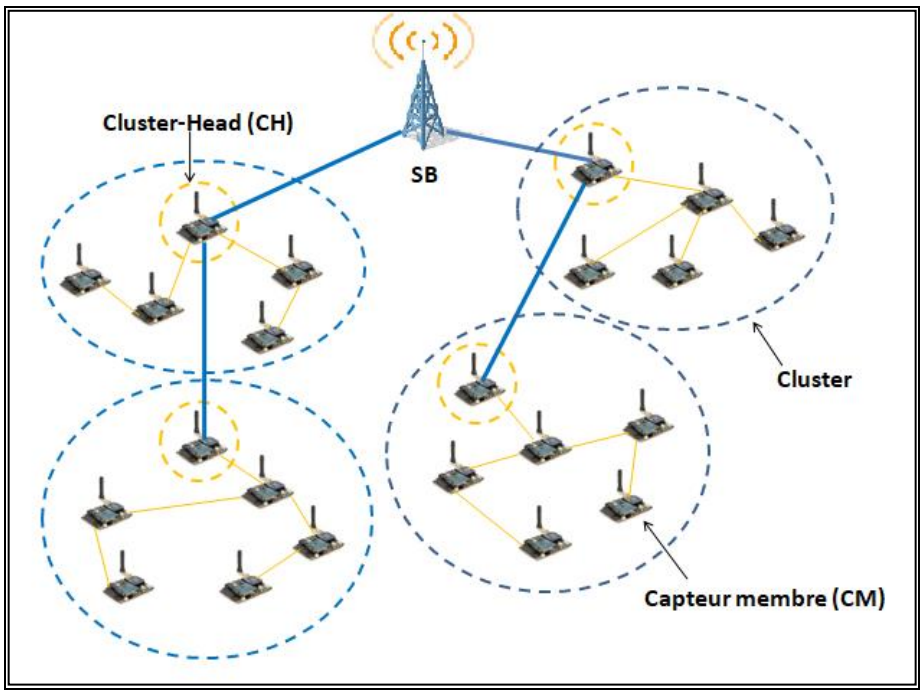


Figure 1.7: Topologie hiérarchique.

1.4. Caractéristiques des RCSF

Pour assurer le bon fonctionnement d'un réseau de capteur, il faut tenir compte d'un certain nombre de caractéristiques tel que :

- ✓ Les RCSFs présentent une architecture décentralisés et arbitraire.
- ✓ Les nœuds capteurs sont des dispositifs de petite taille.
- ✓ Les capteurs sont susceptibles de tomber en panne.
- ✓ La topologie du réseau change à cause de la mobilité et la défaillance des nœuds, les obstacles environnementaux.
- ✓ Adaptabilité : D'où l'intérêt d'avoir un très grand nombre de nœuds, on cherche toujours à avoir une meilleur surveillance en cas de défaillance.
- ✓ Réseau multi-saut : Les RCSFs utilisent des communications multi-saut à cause de la limitation des ressources physiques.
- ✓ Réduction de la consommation d'énergie : l'énergie au sein d'un RCSF est limitée car les capteurs sont alimentés par des batteries qui ne peuvent pas être rechargées ou remplacées
- ✓ Différents types de déploiement : génère des conséquences qui sont différents d'un déploiement à un autre tel que l'absence de sécurité. [8]

1.5. Techniques de conservation énergétique dans les RCSF

La première étape dans la conception de système énergétique de capteurs consiste à analyser les caractéristiques de consommation d'énergie d'un nœud de capteur sans fil. Cette analyse systématique de l'énergie d'un nœud capteur est extrêmement importante pour identifier les problèmes dans le système énergétique pour permettre une optimisation efficace. L'énergie consommée par un capteur est principalement dû aux opérations suivantes : la détection, le traitement et la communication. [9]

- ✓ **Energie de capture :** Un capteur peut être équipé par multiples senseurs (humidité, la chaleur, les mouvements, la position, …). De ce fait les sources de consommation d'énergie pour les opérations de détection ou de capture sont : l'échantillonnage, la conversion analogique-numérique, le traitement de signal et l'activation de la sonde de capture.
- ✓ **Energie de traitement :** L'énergie de traitement est composée de deux sortes d'énergie: l'énergie de commutation et l'énergie de fuite. L'énergie de commutation est déterminée par la tension d'alimentation et la capacité totale commutée au niveau logiciel (en exécutant un logiciel). Par contre, l'énergie de fuite correspond à l'énergie consommée lorsque l'unité de calcul n'effectue aucun traitement. En général, l'énergie de traitement est faible par rapport à celle nécessaire pour la communication.
- ✓ **Energie de communication :** L'énergie de communication se décline en trois parties : l'énergie de réception, l'énergie de l'émission et l'énergie en état de veille. Cette énergie est déterminée par la quantité des données à communiquer et la distance de transmission, ainsi que par les propriétés physiques du module radio. L'émission d'un signal est caractérisée par sa puissance ; quand la puissance d'émission est élevée, le signal aura une grande portée et l'énergie consommée sera plus élevée. Notons que l'énergie de communication représente la portion la plus grande de l'énergie consommée par un nœud capteur (voir figure 1.8).

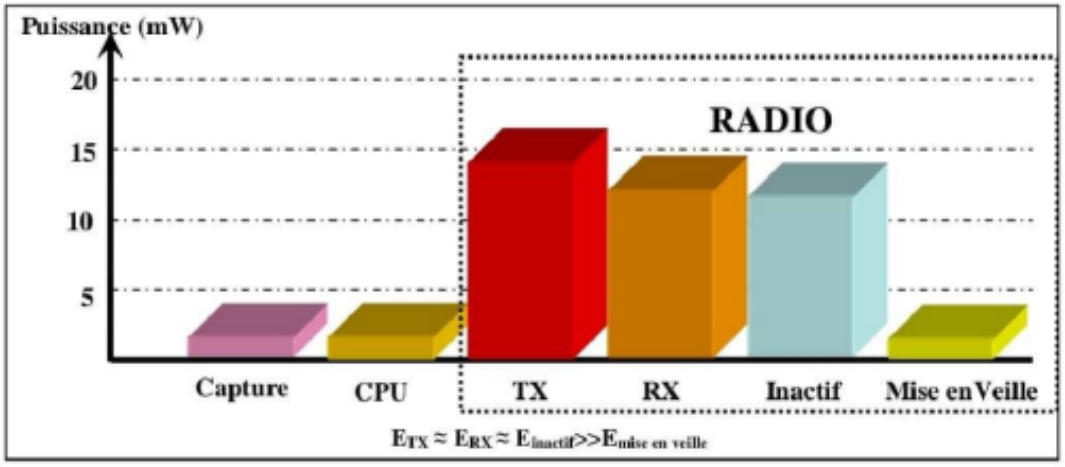


Figure 1.8 : consommation de l'énergie électrique par un nœud capteur

1.6. Domaines d'applications des réseaux de capteurs sans fil

Les réseaux de capteurs sans fil peuvent avoir beaucoup d'applications. Parmi elles, nous citons:

1.6.1. Applications environnementales

Les réseaux de capteurs peuvent être utilisés pour surveiller les changements environnementaux. Ils servent à déterminer les valeurs de certains paramètres à un endroit donné, comme par exemple : la température, la pression atmosphérique, etc. En dispersant des nœuds capteurs dans la nature, on peut détecter des événements tels que des feux de forêts, des tempêtes ou des inondations. Ceci permet une intervention beaucoup plus rapide et efficace des secours. Dans le domaine de l'agriculture, les capteurs peuvent être utilisés pour réagir convenablement aux changements climatiques, par exemple en déclenchant le processus d'arrosage lors de la détection de zones sèches dans un champ agricole. [02]

1.6.2. Applications médicales

Dans le domaine de la médecine, les réseaux de capteurs peuvent être utilisés pour assurer une surveillance permanente des organes vitaux de l'être humain grâce à des micro-capteurs qui pourront être avalés ou implantés sous la peau (surveillance de la glycémie, détection de cancers, etc.). Ils peuvent aussi faciliter le diagnostic de quelques maladies en effectuant des mesures physiologiques telles que : la tension artérielle, battements du cœur, à l'aide des capteurs ayant chacun une tâche bien particulière. Les données physiologiques collectées par

les capteurs peuvent être stockées pendant une longue durée pour le suivi d'un patient pour une ultérieure décision médicale.

1.6.3. Applications militaires

Le faible coût, le déploiement rapide, l'auto-organisation et la tolérance aux pannes sont des caractéristiques qui ont rendu les réseaux de capteurs efficaces pour les applications militaires.

En effet, comme beaucoup d'autres technologies de l'information, ces réseaux sans-fil proviennent principalement de la recherche militaire. Des réseaux de capteurs autonomes sont envisagés comme l'ingrédient essentiel dans cette lancée vers des systèmes de guerre centrés sur les réseaux. Ils peuvent être rapidement déployés et utilisés pour la surveillance des champs de bataille afin de fournir des renseignements concernant l'emplacement, le nombre, le mouvement, et l'identité des soldats et des véhicules, ou bien encore pour la détection des agents chimiques, biologiques et nucléaires.

1.6.4. Domaine domotique

Le déploiement des capteurs de mouvement et de température dans les futures maisons dites intelligentes permet d'automatiser plusieurs opérations domestiques telles que : la lumière qui s'éteint et la musique qui se met en état d'arrêt quand la chambre est vide, la climatisation et le chauffage s'ajustent selon les points multiples de mesure, le déclenchement d'une alarme par le capteur anti-intrusion quand un intrus veut accéder à la maison. [02]

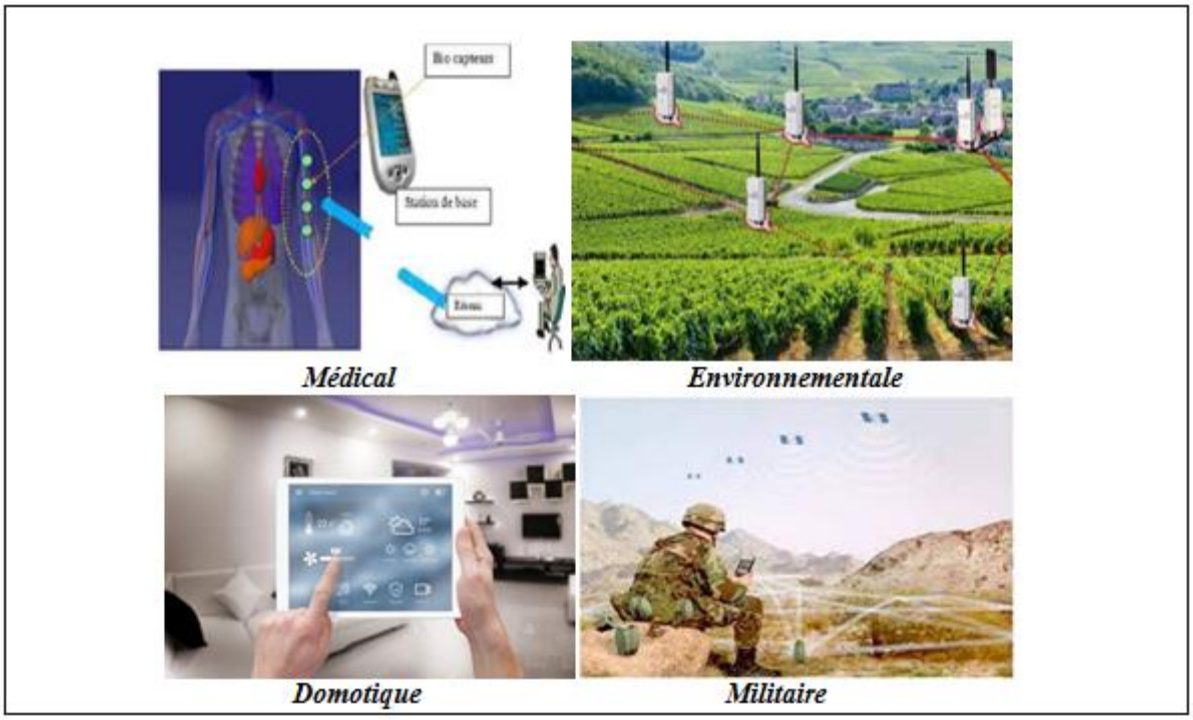


Figure 1.9: Applications des RCSF.

1.7. Contraintes influençant les réseaux de capteurs sans fil

La conception des RCSF, leurs protocoles et algorithmes sont guidés par plusieurs facteurs :

1.7.1. Consommation énergétique

Un capteur, de par sa taille, est limité en énergie (< 1.2 V). Dans la plupart des cas le remplacement de la batterie est impossible. Ce qui veut dire que la durée de vie d'un capteur dépend grandement de la durée de vie de la batterie. Dans un réseau de capteurs (multi-sauts) chaque nœuds collecte des données et transmet des valeurs. Le dysfonctionnement de quelques nœuds nécessite un changement de la topologie du réseau et un re-routage des paquets. Toutes ces opérations sont gourmandes en énergie, c'est pour cette raison que les recherches actuelles se concentrent principalement sur les moyens de réduire cette consommation. [10]

1.7.2. Le passage à l'échelle

L'une des caractéristiques des RCSF est qu'ils peuvent contenir des centaines voire des milliers de nœuds capteurs. Suivant l'application, ce nombre peut encore augmenter jusqu'à des millions de capteurs. Les nouveaux schémas doivent pouvoir garantir un bon

fonctionnement avec ce nombre élevé de capteurs. Ils doivent aussi exploiter la nature fortement dense des réseaux de capteurs. [11]

1.7.3. Qualité de service (QoS)

Dans les réseaux informatiques classiques, la Qualité de Service (QoS) signifie la capacité du système de communication à garantir les performances exigées par l'application, c'est à dire en termes de délai de transmission de bout-en-bout, de taux de perte et de débit. Cependant, les métriques de QoS sont dépendantes de l'application adoptée en raison de différentes caractéristiques spécifiques de chaque type de données utilisées. En ce qui concerne les réseaux de capteurs sans fils, la QoS est la quantité et la qualité des informations qui sont extraites par les données récoltées sur l'environnement où les capteurs ont été déployés. Le niveau de qualité de service peut être défini par un ensemble de critère et des attributs tel que le temps de latence, la bande passante, et le nombre de paquets perdus.

1.7.4. L'auto-configuration

Un réseau de capteur sans fil peut être déployé de deux façons différentes, soit de manière aléatoire à l'aide d'un avion ou de drones, soit de manière bien définie par un humain. Alors un capteur doit avoir la capacité de s'auto-configurer dans un réseau de capteur mais également de pouvoir collaborer avec les autres nœuds du réseau. Chaque capteur du réseau possède un module possédant une antenne émettrice/réceptrice qui permet de communiquer avec les nœuds qui sont proches. Ainsi en échangeant des informations avec ces voisins, tout nœud dans le réseau aura la possibilité de découvrir les routes qu'il adoptera suivant les besoins de l'application.

1.7.5. Mobilité

La position des capteurs sur la zone de captage n'est pas toujours fixe. Un nœud capteur peut devenir mobile et changer sa position selon les besoins de l'utilisateur. Des traitements spécifiques pour la maintenance des liens et la mise à jour des informations de routage sont à prévoir lors de la conception d'un protocole de routage.

1.7.6. Tolérance aux pannes

La tolérance aux pannes c'est la capacité de maintenir les fonctionnalités du réseau sans interruption en cas de défaillance d'un nœud capteur. Afin d'assurer la communication entre

la station de base et les autres nœuds d'un réseau de capteur, les protocoles de routage sont basés sur la communication multi-sauts. Chaque nœud joue alors, en plus du rôle de source de données, le rôle d'un routeur. Toutefois, ces nœuds sont sujets à de nombreuses pannes, dues principalement à l'épuisement des batteries et aux destructions physiques. Ainsi, la panne de nœuds entraîne la perte des liens de communication et donc un changement significatif dans la topologie globale du réseau. Ceci peut affecter d'une façon considérable la connectivité du réseau et diminuer, en conséquence, sa durée de vie. [10]

1.7.7. Hétérogénéité

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

1.7.8. Routage

En réseaux ad hoc, les protocoles de routage sont censés appliquer trois fonctions principales:

- La détermination et la détection des changements de la topologie du réseau.
- Le maintien de la connectivité réseau.
- Le calcul et la détection des bons itinéraires.

Pour les réseaux de capteurs, moins d'effort a été donnée aux protocoles de routage, même si c'est clair que les protocoles de routage ad hoc tels que DSDV (destination sequenced distance vecteur), TORA (temporallyorderedroutingalgorithm), DSR (dynamic source routing), et AODV (ad hoc on demand distance vector) ne sont pas adaptées pour le réseaux de capteur pour la cause du type de trafic appelé « plusieurs à un » et que tous les nœuds typiquement transmettent à une seule station de base ou centre de fusion. Néanmoins, certains mérites de ces protocoles se rapportent aux caractéristiques des réseaux de capteurs, comme la communication multi-sauts et le routage. Le routage peut être associé à la compression des données pour améliorer l'évolutivité du réseau.

1.7.9. La sécurité

La pertinence de la sécurité dans les réseaux de capteurs est étayée par de nombreuses

menaces existantes qui peuvent entraver plusieurs fonctionnalités majeures des réseaux mondiaux. En raison des canaux sans fil et les capacités limitées des nœuds capteurs, il peut être relativement facile pour l'adversaire de contrôler ou même prendre le contrôle du comportement d'un RCSF non protégé. Un réseau de capteurs doit être prêt pour prévenir ou minimiser l'effet de ces attaques en utilisant divers mécanismes possibles, tels que la communication sécurisée (canaux sécurisés, protocoles sécurisés: par exemple le routage, l'agrégation, synchronisation de l'heure) etc. Les primitives de sécurité, telles que la cryptographie à clé symétrique et la cryptographie à clé publique, permet la construction d'une communication sécurisée entre deux ou plusieurs dispositifs, assurer la confidentialité, l'intégrité et l'authentification.

1.8. Service de clustering dans les réseaux de capteurs sans fil

1.8.1. Notions du clustering et cluster

1.8.1.1. Définition

Un cluster est un sous-ensemble de nœuds connexe, et la structuration ou clustering est le processus de regroupement des nœuds en clusters donnant ainsi au réseau une structure hiérarchique.

Généralement et comme la montre la figure 1.10, les clusters comportent trois types de nœuds:

- Un nœud particulier appelé chef de cluster ou "cluster-Head" (CH). Ce dernier permet de coordonner les membres de son cluster, d'agréger et /ou de traiter les données collectées et de les transmettre au collecteur de données. Le chef de cluster est choisi pour jouer ce rôle soit d'une manière déterministe (chef de cluster prédéfini) ou d'une manière aléatoire (chef de cluster élu parmi les nœuds du réseau selon une métrique bien particulière ou une combinaison de métriques).
- Un nœud passerelle ou "Gateway" qui possède des liens inter-clusters et peut donc accéder à des clusters voisins et acheminer les données entre eux.
- Enfin un nœud ordinaire ne possédant pas de liens avec les autres clusters et quand il s'attache à un chef de cluster il en devient membre. [13]

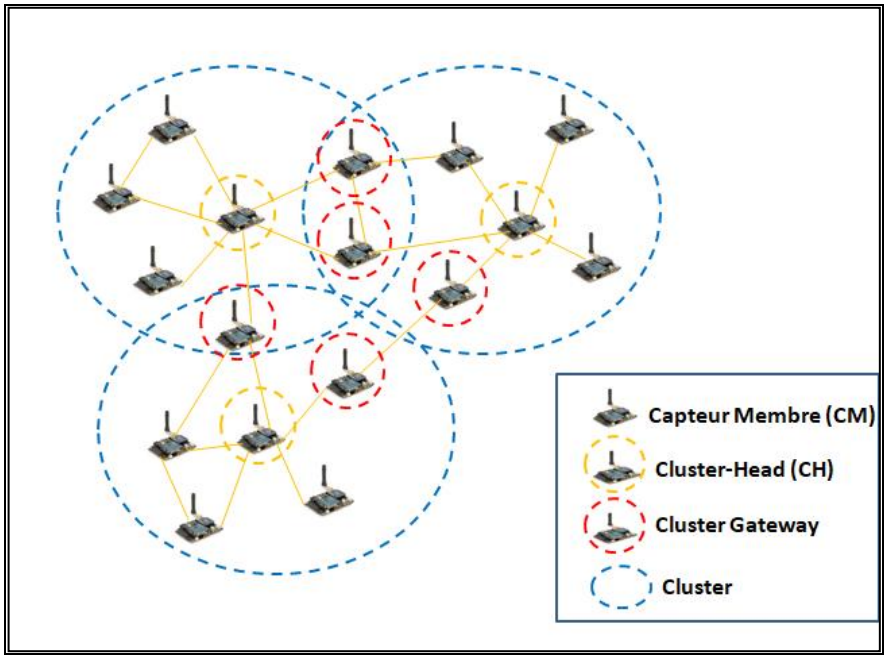


Figure 1.10: Exemple de structure de clusters.

1.8.1.2. Formation des clusters

Les Algorithmes du groupement (clustering) organisent le réseau en sous réseaux (clusters), plus homogènes selon une métrique ou une combinaison de métriques, formant ainsi une topologie virtuelle. Chaque cluster identifie un nœud particulier appelé cluster-head. Le cluster-head, permet de coordonner entre les nœuds membres de son cluster, d'agréger leurs données collectées et de les transmettre par la suite à la station de base. De ce fait, seulement les nœuds leader seront responsables de l'acheminement de l'information collectée vers la station de base. Minimisant ainsi l'énergie consommée par les nœuds capteurs. Il existe plusieurs méthodes de formation de clusters. La méthode la plus répandue. S'exécute comme suit :

- Chaque nœud découvre son voisinage en utilisant des messages Hello.
- Chaque nœud décide, en se basant sur des informations locales sur la topologie, s'il va devenir cluster-head ou pas.
- Le nœud élu comme cluster-head diffuse un message dans son voisinage invitant ses voisins qui ne sont pas encore affiliés à un autre cluster de le rejoindre. [14]

1.8.1.3. Election de cluster-head

La phase d'élection du cluster-head appelée aussi la phase Setup, utilise une métrique (le degré de connectivité, l'énergie restante, mobilité…) ou une combinaison de métriques pour

choisir un nœud leader qui est le cluster-head. [14]

1.8.1.4. Communication intra-cluster et inter-cluster

Chaque cluster-head est chargé d'assurer une bonne communication au sein de son cluster. Par ailleurs, il doit assurer le routage entre les différents cluster-heads en maintenant les informations liées au routage. De plus, étant donné que les cluster-heads ne sont pas directement reliés, des nœuds passerelles doivent être choisis pour assurer la communication entre les cluster-heads.

1.8.1.5. Maintenances des clusters

Une mise à jour des clusters est réalisée soit dans le but de s'adapter aux changements de la topologie (dans le cas où un cluster-head ou un membre du cluster migre d'un cluster à un autre) soit pour équilibrer la consommation d'énergie dans le réseau (si le cluster-head garde son statut le plus longtemps possible, sa batterie sera épuisée, et ainsi il perdra son rôle). Parmi les protocoles proposés dans cette catégorie : LEACH [14]

1.8.2. Les objectifs du clustering

L'objectif principal de la structuration du réseau en clusters est de réduire les communications. Cet objectif général inclus plusieurs sous objectifs. Nous allons lister les plus importants [9] :

- ✓ Augmenter la durée de vie du réseau : par la réduction des communications, le clustering cherche à minimiser la consommation des ressources énergétiques des nœuds. Par conséquence Cela permet d'augmenter la durée de vie du nœud et du réseau.
- ✓ Equilibrer la charge : le clustering vise une répartition équitable des taches les plus couteuses dans le réseau pour éviter des points de congestion ou une consommation déséquilibrée de ressources entre les nœuds du réseau.
- ✓ Optimiser la bande passante : on cherche à travers la structuration du réseau en clusters d'optimiser l'utilisation de la bande passante, par la minimisation des communications et d'éviter la duplication des messages et les retransmissions inutiles.
- ✓ Assurer une qualité de service (QoS) : Le clustering permet d'assurer une certaine qualité de service, même en présence de coupures de liens de communication qui provoquent un arrêt temporaire du service fourni par l'applicatif du réseau en raison de la mobilité des nœuds ou d'autres fautes transitoires.

- ✓ Assurer la réduction de délai : le clustering cherche d'assurer une communication entre n'importe quel couple de nœuds se trouvant dans le même cluster ou dans des clusters différents, cette communication doit être assurée avec un délai acceptable selon les besoins requis.

1.8.3. Propriétés du clustering

- ✓ Nombre de cluster : Dans quelques approches éditées l'ensemble de CHs sont prédéterminés et le nombre de clusters est ainsi déterminé à l'avance. La sélection aléatoire de CHs parmi les nœuds déployés produit habituellement un nombre variable de clusters.
- ✓ La stabilité : Quand le nombre de clusters varie et les nœuds membres d'un cluster évolue dans le temps, le schéma de clustering est dit adaptatif. Autrement, il est considéré fixe puisque les nœuds ne s'échangent pas parmi les clusters et le nombre de clusters reste invariant tout au long de la durée de vie du réseau.
- ✓ Topologie intra-cluster : Certaines approches de clustering sont basées sur les communications directes entre un nœud et son CH. Cependant, la connectivité multi-saut de nœud à CH est parfois exigés, particulièrement quand la portée de communication est limitée et/ou le nombre de CHs est borné.
- ✓ Connectivité inter-CH : Quand un CH n'a pas de possibilités de communication à longue portée, sa connectivité à la station de base doit être assurée. Dans ce cas, l'approche de clustering doit assurer la praticabilité d'établir un itinéraire inter-CH et de chaque CH à la station de base. Certains travaux supposent que les CHs pourraient atteindre directement la station de base. [14]

1.8.4. Cas d'utilisations possible de clustering

Le clustering est devenu largement utilisé ces dernières années pour résoudre différents problèmes, voici quelques cas d'utilisation :

- ✓ Routage hiérarchique: il est possible d'utiliser le clustering pour réduire la complexité du routage en gérant localement la communication intra-cluster par les Cluster Head. Cela permet d'avoir un minimum d'informations à stocker dans les tables de routage. Du fait de cette hiérarchie dans le réseau, le routage peut être beaucoup plus efficace et plus rapide.

- ✓ Coordination des communications: permet de mieux coordonner les communications dans le réseau grâce à la structure hiérarchique offerte par le clustering, En effet, il est possible, par exemple, d'organiser les communications au sein de clusters par le Cluster-Head mais aussi d'établir des politiques de communication entre clusters adjacents.
- ✓ Agrégation de données : la hiérarchisation du réseau engendrée par la structuration en clusters permet une agrégation de donnée par niveau de hiérarchie. Associée au routage hiérarchique, cette agrégation peut permettre de réduire le nombre de messages envoyés depuis les clusters, diminuant ainsi le trafic dans le réseau.
- ✓ Passage à l'échelle : le routage hiérarchique basé sur le clustering s'impose comme une approche très puissance pour résoudre le problème de Scalabilité. En effet, la technique de clustering permet de réduire la complexité du routage à grande échelle par le biais de la division du réseau en clusters.

1.8.5. Classifications des solutions des clustering

Plusieurs solutions de clustering qui ont été proposée dans la littérature. Mandicou BA classifié ces solutions d'abord suivant la famille à laquelle elles appartiennent, puis selon le diamètre des clusters et enfin selon la métrique utilisée pour élire le Cluster-Head.

1.8.5.1. Classification selon la famille d'algorithmes

Il existe deux grandes familles de solutions de clustering :

- Les algorithmes non auto-stabilisants.
- Les algorithmes auto-stabilisants.

Les solutions de structuration non auto-stabilisantes sont caractérisées par une initialisation bien déterminée. En effet, un algorithme doit démarrer avec des états bien définis et corrects. De plus, ces solutions considèrent les aspects les plus fondamentaux tels que la consommation énergétique, la mobilité des nœuds ou la densité du réseau, etc. Elles visent à améliorer la stabilité du réseau, de réduire la surcharge du réseau, etc. Cependant, les solutions de structuration non auto-stabilisantes sont souvent vulnérables aux pannes transitoires.

Les solutions auto-stabilisantes ne nécessitent aucune initialisation des contenus des variables des nœuds et des canaux de communication ni aucune intervention extérieure. Les nœuds sont en mesure de gérer leurs états de façon autonome et distribuée, de détecter et de corriger les pannes transitoires en un nombre fini de transitions. Pour ces raisons, de nombreuses

recherches ont été focalisées sur l'élaboration de solutions de clustering auto stabilisantes. [15]

1.8.5.1.1. Classification selon le diamètre de cluster

Dans chacune des deux familles de clustering que nous avons présentes ci-dessus (auto stabilisante confirme non auto-stabilisante), nous pouvons classer les solutions existantes en deux groupes : les solutions à 1 saut et celles à k sauts.

Les solutions à 1 saut:dans ces solutions chaque nœud du cluster se trouve à une distance de 1 saut du cluster-Head et le diamètre maximal des clusters et donc égal à 2. Les solutions à 1 saut, du fait du faible diamètre maximal qui est égal à 2, construisent un nombre important de cluster de petite taille. La conséquence qui en découle est que les clusters sont sensibles aux pannes transitoires favorisant ainsi de fréquentes reconstructions.

Les solutions à k sauts : sont proposés pour pallier le problème posé par les solutions à 1 saut. Dans les solutions k sauts un nœud peut se situer jusqu'à une distance de k sauts du Cluster-Head. Ainsi, le diamètre des clusters est au plus égal à 2 k. Notons que quel que soit le diamètre du cluster, il est possible de construire un arbre couvrant de cluster donnant ainsi un niveau de hiérarchisation supplémentaire.

1.8.5.1.2. Classification selon la métrique d'élection de cluster-head

De même, dans les deux familles de clustering, pour élire les Cluster-Heads, trois types de métriques différentes peuvent être utilisées : (1) les métriques fixes, (2) les métriques variables et (3) une combinaison de métriques fixe(s) et/ou variable(s).

Dans la première catégorie, une métrique fixe, c'est-à-dire constante dans le temps, est utilisée pour élire les Cluster-Heads. Parmi ces métriques fixes, nous pouvons citer l'identifiant des nœuds, le degré des nœuds, etc.

Avec la deuxième catégorie, pour choisir les Cluster-Heads, une métrique variable. C'est-à-dire pouvant évoluer au cours du temps, est utilisée. Comme métriques variables, nous pouvons donner l'exemple de la mobilité, de l'énergie, de densité, etc.

Pour la troisième catégorie, une combinaison d'une ou de plusieurs métriques fixe(s) et/ou variable(s) est utilisée comme critère discriminatoire pour la formation des clusters. Par exemple, nous pouvons citer une combinaison de " identifiant + degré + énergie", " identifiant + densité + énergie", " identifiant + énergie" etc. Notons aussi que des coefficients de normalisation sont généralement associés aux différentes métriques dans une combinaison.

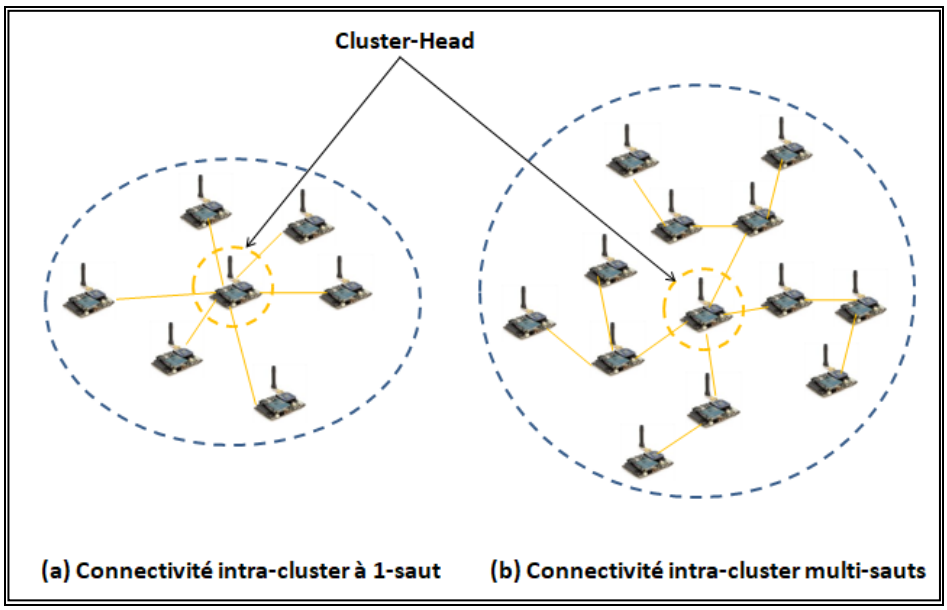


Figure 1.10: Clusters à 1-saut ou à k-sauts.

1.8.6. Les principaux algorithmes de clustering conçus pour les réseaux de capteurs sans fil

Le clustering dans les réseaux de capteurs est une approche efficace de réduire la consommation d'énergie dans un cluster en exécutant les fonctions d'agrégation et de fusion de données dans le but de minimisé le nombre de messages transmis à la station de base et prolonger la durée de vie du réseau.

Dans cette section, nous présentons les principales techniques du clustering proposées pour les réseaux de capteurs.

- **LEACH (Low Energy Adaptive Clustering Hierarchy)**

LEACH [16] est un protocole basé sur les groupes, dans lequel les chefs de groupes élus collectent les données à partir de tous les nœuds capteurs appartenant à leur groupe, agrègent les données rassemblées par des procédures de fusion, et transmettent ces données directement à la station de base. Les chefs de groupes élus demeurent ainsi pour une période de temps appelée « round ». Au début de chaque round, chaque nœud détermine la possibilité d'être un chef de groupe pendant la période en cour, s'il décide de l'être, il annonce sa décision à tous ses nœuds voisins. Les autres nœuds qui décident de ne pas être un chef de groupe, se joignent à l'un des chefs élus après recevoir leurs décisions, la sélection du chef de groupe adéquat se base sur plusieurs paramètres prédéterminés tel que le rapport signal/bruit (SNR).

- **HEED (Hybrid Energy Efficient Distribured Clustering)**

HEED [17] est un protocole de clustering dans lequel l'élection du chef de cluster est basée principalement sur l'énergie résiduelle et d'autres paramètres tels que la distance des voisins ou le nombre de voisins. Dans HEED, la fonction de formation de cluster est déclenchée à des intervalles donnés pour l'élection du chef de cluster et les nœuds non couverts, ceux sans chef de cluster, qui peuvent s'élire eux-mêmes. En outre, les paramètres HEED tels que la probabilité de sélection minimale, qui est une probabilité pour qu'un nœud soit élu en tant que chef de cluster et l'intervalle de fonctionnement du réseau, qui informe l'utilisateur de la fréquence du processus d'élection du chef de cluster, peuvent être facilement réglés pour une meilleure optimisation en cas des exigences d'une application telle que la densité du réseau. Le faible coût de communication et la bonne évolutivité sont les principaux avantages de HEED. En revanche, les différents niveaux d'énergie ne sont pas pris en compte.

- **TEEN (Threshold-sensitive Energy Efficient Sensor Network protocol)**

TEEN [16] est un protocole de routage basé sur les groupes et proposé par Manjeshwar et al. Ce protocole est similaire à LEACH décrit dans la section précédente, sauf que les nœuds ne sont pas supposés avoir un taux fixe de données à transmettre. TEEN utilise la même stratégie que LEACH pour l'étape de formation des groupes, mais adopte une approche différente pour la phase de transmission des données. Durant cette étape, TEEN utilise deux paramètres définis par l'utilisateur appelé hard threshold (ht) et soft threshold (st) et ceci, pour pouvoir déterminer le besoin de transmission de la donnée captée vers la station de base. Si la valeur captée excède ht pour la première fois, elle est stockée dans une variable et transmise durant le temps alloué par le chef du groupe au nœud concerné. Si la valeur captée dépasse, par la suite, la valeur stockée par une magnitude st, le nœud décide de la transmettre et stocke cette nouvelle valeur dans son cache pour les comparaisons ultérieures.

- **APTEEN (Adaptive Threshold Senstive Energy Efficient sensor Network protocol)**

APTEEN est une extension de TEEN qui fait à la fois la collection des captures périodique de données et qui réagit aux événements critiques. Quand la SB forme des clusters, les clusters head diffusent les attributs, les valeurs des seuils, ainsi que le calendrier de transmission à tous les nœuds. Le CH effectue également l'agrégation de données afin d'économiser l'énergie. [16]

- **PEGASIS (Power-Efficient Gathering in sensor information systems)**

PEGASIS [16] est une version améliorée du protocole LEACH. PEGASIS forme des chaînes plutôt que des clusters de nœuds de capteurs afin que chaque nœud transmette et reçoive uniquement des données d'un voisin. Un seul nœud est sélectionné à partir de cette chaîne pour transmettre à la station de base. L'idée de PEGASIS est qu'il utilise tous les nœuds pour transmettre ou recevoir des données avec ses plus proches voisins. Il déplace les données reçues de nœud à nœud, puis les données seront agrégées jusqu'à ce qu'elles atteignent tous la station de base. Donc, chaque nœud du réseau est tour à tour un chef de file de la chaîne, ainsi que responsable pour transmettre l'ensemble des données recueillies et fusionnées par la chaîne de nœuds au niveau de la station de base.

1.9. Conclusion

En conclusion, cette étude approfondie sur les réseaux de capteurs sans fil (RCSF) et le service de clustering a mis en évidence leur importance cruciale dans de nombreux domaines, allant de la surveillance environnementale à la santé en passant par la sécurité. Les RCSF offrent une solution efficace et économique pour la collecte de données en temps réel, ce qui permet de prendre des décisions éclairées et d'améliorer la gestion de systèmes complexes.

Le service de clustering se révèle être une approche stratégique dans les RCSF, permettant de regrouper les capteurs en clusters pour faciliter la gestion du réseau, économiser l'énergie et prolonger la durée de vie des capteurs.

Cependant, il est essentiel de prendre en compte divers facteurs lors de la conception et de l'implémentation du service de clustering, tels que l'hétérogénéité des capteurs, la mobilté, la topologie du réseau et la sécurité des données.

Dans ce chapitre, nous avons présenté les différentes classifications des algorithmes de clustering dans les réseaux de capteurs sans fil. Bien que ces algorithmes puissent augmenter la durée de vie du réseau tout en respectant plusieurs contraintes telle que la consommation d'énergie, ils exposent certaines limitations. En effet, aucun mécanisme de sécurité n'est intégré dans ces algorithmes. Ainsi, ils sont très vulnérables même aux simples attaques. Donc, un attaquant peut facilement monopoliser le réseau et induit à son disfonctionnement. Par conséquent, Dans le chapitre suivant, nous allons aborder le concept de sécurité dans les réseaux de capteurs.

Chapitre 2

La sécurité dans les RCSFs: Menaces et Solutions

2.1. Introduction

La sécurité est un domaine très important pour les RCSF, particulièrement pour des applications sensibles du domaine militaire, médicale, et autre. La sécurité intervient pour certaines fonctions sensibles telles que la transmission des paquets, le routage et la gestion d'un réseau, fonctions effectuées par certains ou tous les nœuds disponibles dans les RCSF.

Les données circulant doivent être garanties correctes et valides. Il est primordial de pouvoir s'assurer que l'information n'a pas été altérée et émane effectivement de la source considérée.

Les points abordés dans ce chapitre, traitent l'aspect sécurité dans les RCSF, les défis à relever, les problèmes de sécurité et on terminera par l'introduction d'un axe très important dans la construction de n'importe qu'elle application basée sur la communication, et qui est la gestion de clés cryptographiques.

2.2. Objectif de la sécurité dans les RCSF

La sécurité dans RCSF est un ensemble cohérent de mécanismes, d'algorithmes, de procédures et de schémas permettant d'atteindre et de maintenir un certain niveau de sécurité. Lorsque nous parlons sur le problème de sécurité, Cela signifie que nous voulons atteindre un ensemble d'objectifs, dont le plus important :

2.2.1. Authentification

L'authentification est le processus effectué par une entité pour vérifier l'identité d'un nœud souhaitez communiquer avec d'autres nœuds. Comme les mots de passe, les signatures numériques ou code Authentification des messages.

2.2.2. La confidentialité

La confidentialité est un point très important dans la communication des RCSF, elle assure la limitation d'accès à l'information, seules les nœuds autorisés peuvent accéder les données dans le réseau et empêcher de ceux qui sont non autorisé. Les données doivent donc être chiffrées.

2.2.3. L'intégrité

Le mécanisme de sécurité doit garantir qu'un message envoyé par un noud capteur à l'autre n'est pas modifié ou altérées par un nœud non autorisé.

2.2.4. La disponibilité

Cette propriété sert à garantir que les services réseau sont disponibles même si le réseau de capteur est ciblé par des attaques comme de déni de service et le système inexploitable ou inutilisable.

2.2.5. La Fraîcheur

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

Pour résoudre ce problème, un compteur relatif au temps différent peut-être ajouté dans le paquet pour assurer la fraîcheur des données. Ainsi, la fraicheur des données consiste à s'assurer que les paquets soient récents et qu'aucun vieux paquet n'a été rejoué dans le réseau[18].

2.3. Sources de vulnérabilités dans les RCSF

Quelques faiblesses sont inhérentes aux RCSF, d'autres liées à la technologie retenue. Nous distinguons deux catégories : les vulnérabilités du nœud capteur et les vulnérabilités technologiques :

2.3.1. Vulnérabilité du nœud capteur

2.3.1.1. Protection physique faible

A cause de leurs faibles coûts, Les capteurs peuvent être déployés dans des environnements non-protégés (montagnes, forêts, champs de bataille, etc.).Ainsi, ils utilisent rarement des composants électroniques anti-corruption (tamper-résistant devices).

Par conséquent, ces réseaux sont vulnérables aux catastrophes naturelles (tremblements de terre, les tornades ou les inondations) et peuvent facilement être interceptés et corrompus ou encore subir des attaques physiques (destruction définitive des capteurs de telle sorte que les pertes soient irrécupérables) dans un tel environnement. Il est bien clair qu'aucun protocole de sécurité ne peut résister à ce type d'attaques physiques, mais des techniques de sécurité peuvent être conçues afin de fournir des capacités d'auto-réparation au réseau.

2.3.1.2. Ressources extrêmement limitées de nœuds capteurs

La mise en œuvre de toute approche de sécurité nécessite une certaine capacité de ressources, y compris la mémoire des données, l'espace de code, puissance de calcul et l'énergie pour alimenter le capteur. Cependant, en raison du faible coût et de miniaturisation, ces ressources sont très limitées dans ce type de nœuds capteurs sans fil. Les principales limitations dues aux caractéristiques des nœuds capteurs sont :

- **Limitation de mémoire et d'espace de stockage**

Un capteur est un petit dispositif avec une capacité limitée de mémoire et d'espace de stockage pour le code. Par exemple un capteur de type Mica mote, possède un processeur Atmel ATMEGA103 4 MHz avec 128 Ko de mémoire d'instructions, 512 Ko de mémoire flash, et seulement 4 Ko de RAM pour les données. Donc avec une telle limitation, il est indispensable de limiter la taille du code de l'algorithme de sécurité afin de construire un mécanisme de sécurité efficace.

- **Limitation de la puissance énergétique**

L'énergie est un autre défi dans les RCSF; elle est considérée comme la contrainte la plus sévère aux capacités des capteurs sans fil. C'est l'une des principales raisons pour lesquelles les nœuds sont sujets à des défaillances en raison de l'épuisement des batteries. Une fois les nœuds capteurs déployés dans un réseau de capteurs, ils ne peuvent pas être facilement remplacés (coût d'exploitation élevé) ou rechargés. Pour transmettre des données, un nœud capteur doit allumer son antenne radio ce qui consomme beaucoup d'énergie (la transmission est particulièrement coûteuse en termes de puissance énergétique). Si des nœuds stratégiques et importants subissent une attaque de privation de sommeil, ou l'attaquant transfère généralement des paquets inutiles vers le nœud cible afin de garder sa radio allumée, ce qui consomme leur batterie afin de l'épuiser complètement. Par conséquent, le nœud capteur devient incapable de prendre part au processus de communication, ce qui dégrade

sérieusement les performances du réseau. Ainsi, la consommation d'énergie doit être minimisée pour prolonger la durée de vie des capteurs; cela nécessite à la fois l'efficacité énergétique du matériel ainsi que l'efficacité de la sécurité.

- **Limitation de puissance de calcul**

En raison de la petite taille des nœuds et le faible coût, les nœuds capteurs disposent d'un microcontrôleur à faible capacité de calcul. Par exemple, les capteurs de type Telos B contiennent un processeur RISC 16 bits avec 8 MHz. De telle contrainte sur la puissance de calcul exige des algorithmes de sécurité extrêmement compétents en termes de complexité de calcul. Ainsi, ceci réduit également la faisabilité de certaines techniques de cryptage efficace.

2.3.2. Vulnérabilités technologiques du réseau

Malgré les améliorations matérielles et logicielles apportées aux RCSF ces dernières décennies, les principaux obstacles de sécurité dans les RCSF émergent à partir des caractéristiques du réseau qui les rendent efficaces et attirants:

2.3.2.1. Communication non fiable

Une communication non fiable est une autre source de vulnérabilité pour la sécurité des RCSF. La sécurité du réseau dépend fortement d'un protocole bien défini, qui à son tour dépend de la communication.

- *Support sans fil:* La nature elle-même du support de communication sans fil est l'une des principales menaces de sécurité des RCSF, Contrairement aux réseaux filaires où un périphérique doit être physiquement connecté au support, le support de communication sans fil est ouvert et accessible à tout le monde. Cela conduit à plus de soucis de sécurité dans les RCSF, ce qui constitue l'une des primordiales menaces à la sécurité des capteurs. Avec le moindre effort, un adversaire qui pénètre dans la zone de couverture peut commodément capturer, Falsifier ou rejouer tous les messages échangés. Un intrus ayant un émetteur puissant peut rendre les nœuds capteurs incapables de transmettre des paquets par la production d'un bruit sur le canal. Donc, le média peut apparaître comme occupé en permanence. Les médias sans fil permettent facilement aux intrus d'interceptés de détruire des paquets valides, et injecter des malveillants ou encore corrompus.
- *Transfert non fiable:* Dans les RCSF, le routage des paquets est sans connexion, ce qui est intrinsèquement peu fiable. Dans le cas d'une erreur de canal ou l'abondant des

nœuds hautement congestionnés, des paquets peuvent être corrompus et par conséquent, des paquets critiques de sécurité peuvent être endommagés ou perdus. []

- *Latence:* Une valide synchronisation entre les nœuds est indispensable pour tout mécanisme de sécurité qui se base sur la distribution de clés cryptographiques et les rapports d'événements. Une synchronisation correcte entre les nœuds capteurs dans les RCSF est presque impossible en raison d'encombrement du réseau, le routage multi-sauts et le traitement des nœuds, ce qui introduit une latence importante dans le réseau.
- *Conflits:* Une communication fiable ne peut être assurée à cause de la propriété de diffusion dans les RCSF. Au milieu du transfert des paquets, des conflits peuvent se produire en raison des collisions des paquets, ce qui provoque l'échec du transfert. Un intrus puissant peut facilement exploiter cette faiblesse, afin de perturber le réseau par la production d'interférences dans la zone de couverture.
- *Environnement multi-sauts:* Afin de réduire le coût de déploiement, et pour un déploiement facile et rapide, une architecture multi-sauts est indispensable pour les réseaux de capteurs sans fil, dans laquelle les nœuds ont la possibilité d'auto-guérison, d'auto-configuration et d'auto-ajustement. Ce type d'architectures permet aux adversaires de menacer la sécurité par l'exploitation de quelques attaques comme : l'attaque de trou noir, l'attaque de routage sélectif, l'attaque sybil, ainsi que les attaques qui permettent la création de chemins erronés ou inexistants entre la source et la destination.

2.3.2.2. Déploiement à grand échelle

Afin de couvrir des zones immenses et de fournir une redondance, le nombre de nœuds capteurs dans un RCSF peut être très important (de dizaines à des centaines de milliers de nœuds). Ainsi, les capteurs peuvent être largués par voie aérienne et leur emplacement géographique exact peut donc être imprédictible. Ces deux facteurs offrent des avantages aux attaquants qui incitent le réseau à les accepter comme des nœuds légitimes, ou plus encore d'utiliser leur propre formule pour capturer ou reprogrammer les nœuds légitimes dans le réseau. L'échelle étendue dans les RCSF pose des problèmes de recherche sérieux et complexes pour le développement d'un mécanisme de sécurité qui prend en charge un grand nombre de nœuds répartis sur une grande surface, en maintenant l'énergie , l'espace mémoire et la puissance de calcul du nœuds capteurs.

2.3.2.3. Topologie de réseau dynamique

De nombreux facteurs rendent la topologie des RCSF dynamique et non déterministe. Donc, aucune topologie fixe ne peut être définie à l'avance en raison de quelques facteurs, tels que le réapprovisionnement périodique du réseau (la révocation de nœud épuisé ou défaillant et l'ajout de nouveaux nœuds), les mouvements de nœud, etc. cette topologie instable qui aura une grande incidence sur les performances des protocoles de sécurité, rend les mécanismes de sécurité traditionnels, basés sur des configurations statiques, impossibles à appliquer.

Il est donc nécessaire que tout mécanisme de sécurité conçu pour ces réseaux puisse fonctionner dans cet environnement dynamique et évolutif. Des techniques de sécurité plus robustes doivent être élaborées, et qui peuvent s'adapter dynamiquement en fonction de la modification de la topologie du réseau. Pour cela, une transparence en ce qui concerne l'ajout et la révocation des nœuds sur le réseau, ainsi que des informations concernant la reconfiguration de la topologie du réseau est nécessaire.

2.4. Menaces et solutions

2.4.1. Principes d'attaques et d'attaquants

Une attaque peut être définie comme une tentative d'accès non autorisé à un service, une ressource ou une information, ou la tentative de compromettre l'intégrité, la disponibilité ou la confidentialité d'un système. Les attaquants, les intrus ou les adversaires sont à l'origine d'une attaque. La faiblesse d'une conception, d'une implémentation, d'une configuration ou d'une limitation de la sécurité du système qui pourrait être exploitée par des attaquants est connue sous le nom de vulnérabilité ou faille. Toute circonstance ou tout événement (tel que l'existence d'un attaquant et les vulnérabilités) susceptibles d'avoir un impact négatif sur un système à travers une faille de sécurité est appelé menace et la probabilité qu'un attaquant exploite une vulnérabilité particulière, causant des dommages à un actif du système est connue sous le nom de risque. [17]

Les attaquants peuvent également être catégorisés selon de nombreux critères. La figure 2.1 illustre les différentes caractéristiques utilisées pour présenter une classification détaillée des attaquants.

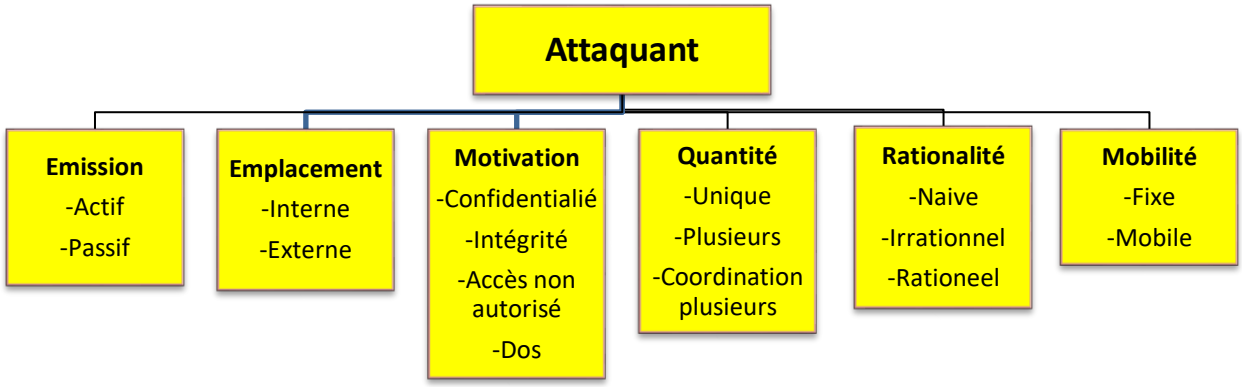


Figure 2.1: Taxonomie des Attaquants.

Un attaquant peut être un nœud interne ou externe du réseau. Un attaquant interne est un nœud qui a été compromis et fait partie du réseau attaqué. Par conséquent, l'attaquant peut connaître toutes les informations cryptographiques appartenant au nœud compromis. Donc les attaques actives peuvent être organisées par des attaquants internes. En d'autres termes, un attaquant interne peut être vu comme un nœud qui a été enregistré légalement ou un nœud autorisé à accéder au réseau. Les attaques externes peuvent être passives ou actives. Un attaquant externe est généralement un nœud ou plusieurs qui ne sont pas les bienvenus sur le réseau. Lorsqu'il y a plusieurs attaquants, ils peuvent collaborer les uns avec les autres, ce qui peut être considéré comme un cas plus difficile à défendre.

2.4.2. Taxonomie des attaques

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

2.4.2.1. Attaques passives/Actives

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

2.4.2.2. Attaques internes/externes

- *Les attaques internes :* se produisent par des nœuds internes malveillants.

- *Les attaques externes :* se produisent de l'extérieur du réseau de capteurs c'est-à-dire, elles se produisent par des nœuds qui ne sont pas déployées à l'intérieur du réseau et que ne sont pas autorisées à participer dans le réseau.

2.4.2.3. Attaques orientées selon les couches protocolaires

Dans cette section nous étudions les problèmes de sécurité du point de vue pile protocolaire, les attaques possibles dans chaque couche et les défenses appropriées :

- **Couche physique**

Les attaques associées à la première couche physique sont peu nombreuses mais, en même temps, peuvent être les plus difficiles à prévenir. On peut citer le brouillage radio sur la même fréquence que le réseau utilise et l'attaque physique d'un nœud. Les défenses envisageables contre le brouillage sont les suivantes :

- L'utilisation de la technique de l'émission par saut de fréquence.
- L'isolement de la région brouillée (changer les informations de routage pour contourner la zone attaquée).
- L'utilisation d'un matériel résistant à l'attaque physique de capteur ("tamperproofnode").

L'attaque physique d'un nœud est le problème le plus contrariant dans la sécurité des RCSF.

- **Couche liaison**

Cette couche géré l'accès au canal (couche MAC). Les attaques courantes utilisent le mécanisme d'accès au réseau pour bloquer le système, l'adversaire peut par exemple induire une collision dans un octet d'une transmission pour perturber tous les paquets.

La prévention de ces attaques peut se limiter à imposer l'usage de petits paquets et utiliser des techniques de correction plutôt que de demander la retransmission de paquet.

- **Couche réseau**

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

- **Couche transport**

Si les couches liaison de données et réseau sont sécurisées, la couche transport peut être sure que les paquets qu'elle reçoit de la couche réseau sont confidentiels et authentifies.

- **Couche application**

Différents types d'attaques peuvent être effectuées dans cette couche, telles que Overwhelm, la répudiation, la corruption de données. En cas d'attaque Overwhelm, un attaquant amène le réseau à acheminer de gros volumes de trafic vers la station de base. Ce type d'attaque consomme de la bande passante de réseau et épuiser l'énergie des capteurs.

2.4.3. Description de quelques attaques

le RCSF à une probabilité plus élevée d'être attaqué que tous les autres types de réseaux, en raison de leurs ressources et de leurs environnements limités déployer. Les attaques sont généralement faites en insérant des éléments hostiles dans le réseau. Il existe également des attaques hors réseau, qui Interférer avec ou modifier un signal à transmettre. Dans cette section, nous vous présentons les attaques les plus célèbresde RCSF :

- ***Analyse du trafic :***est une attaque qui met en jeu des mécanismes d'écoute passive et de surveillance du réseau. L'attaque en analysant uniquement les chemins empruntés par les paquets sur le réseau pourra récupérer des informations précieuses sur les vulnérabilités de ce réseau.
  Analyser le trafic peut permettre à un attaquant de connaitre la position des nœuds d'agrégation de donnée ou des bases du réseau en repérant les lieux ou le plus grand nombre de paquets transitent.
- ***Brouillage radio :***Le médium de transmission des informations est un point vulnérable dans un réseau. En l'occurrence, il est quasiment impossible de restreindre l'accès à un médium utilisant des ondes radio. Un attaquent peut donc envoyer des ondes sur la même fréquence que le RCSF pour brouiller les ondes radio. Les nœuds du réseau n'ont alors plus accès au médium et ne peuvent plus communiquer du fait de ce brouillage radio. Or un réseau sans accès au médium est un réseau hors service.
- ***Hello Flooding :*** Les protocoles de découverte utilisent des messages de type « HELLO » pour découvrir ses nœuds voisins et pour s'insérer dans un réseau. Dans une attaque dite de HELLO Flooding, un attaquent utilise ce mécanisme pour consommer l'énergie des capteurs et empêcher leurs messages d'être routés.

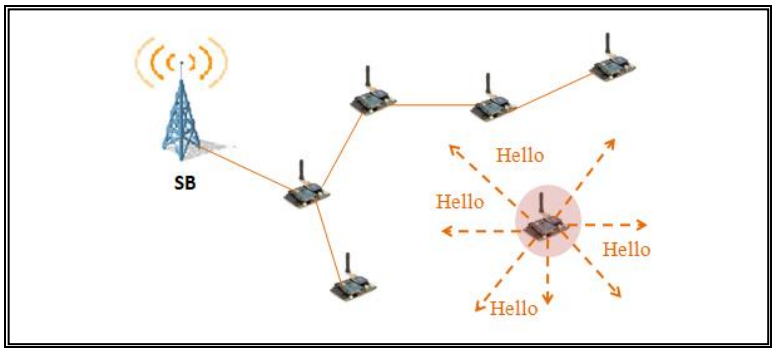


Figure 2.2: Attaque Hello Flooding.

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

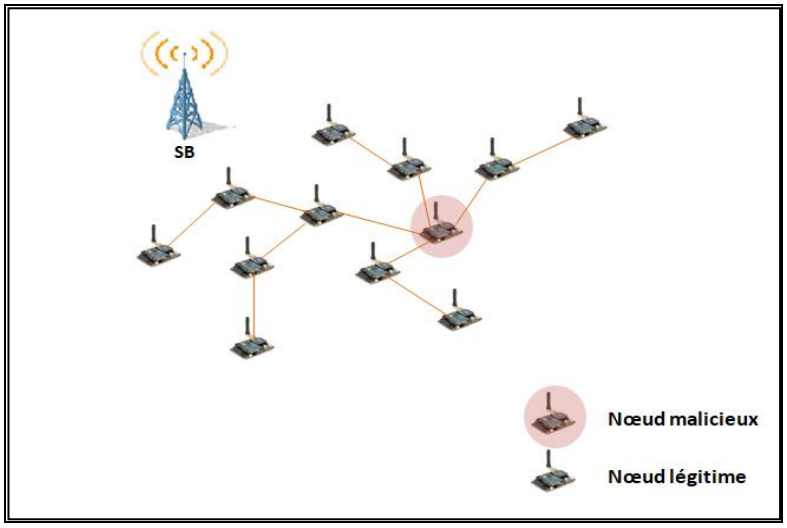


Figure 2.3: Attaque Sinkhole.

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

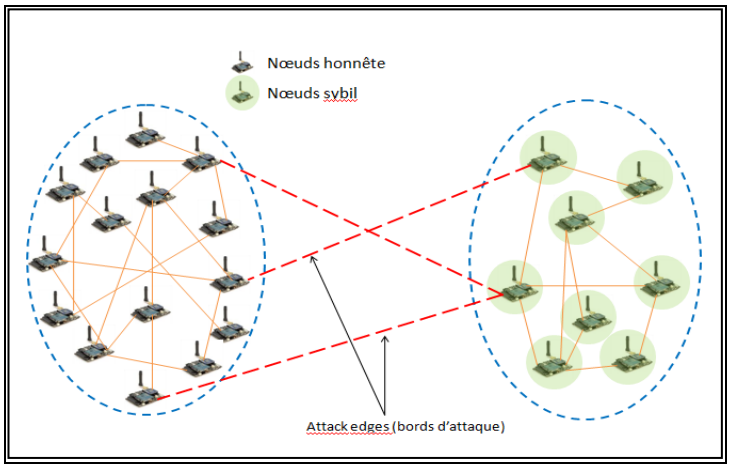


Figure 2.4: Attaque Sybil.

- ***Wormholes* :** Connu aussi sous le vocable de tunneling, dans cette attaque, un adversaire peut recevoir des messages et les rejouer dans déférentes parties à l'aide d'un tunnel entre les nœuds malicieux.

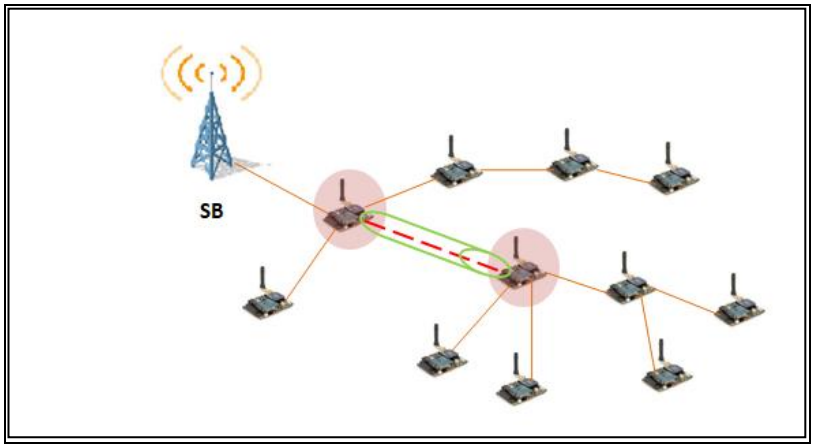


Figure 2.5: Attaque Wormholes.

2.4.4. Mécanismes de sécurité

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

2.4.4.1. Solutions adaptées aux communications des RCSF

La caractéristique la plus évidente d'un RCSF est que la communication se passe sur un canal sans fil, le milieu sans fil est habituellement un canal radio. Ainsi, il est ouvert et accessible à tout le monde. Pour Cela, il est nécessaire d'établir un canal de communication sécurisé entre

les nœuds capteurs, où aucun attaquant ne peut endommager l'échange des messages. Pour créer ce canal, il est nécessaire d'utiliser des primitives cryptographiques, et il est également essentiel d'établir les informations de sécurité (clés secrètes) nécessaires à ces primitives.

2.4.4.1.1. Primitives cryptographiques

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

La cryptographie

La cryptographie est l'étude des techniques mathématiques qui permettent d'assurer certains services de sécurité. Elle est définie comme étant une science permettant de convertir des informations "en clair" en informations cryptées (codées), c'est à dire non compréhensibles, et puis, à partir de ces informations cryptées, de restituer les informations originales.

La cryptographie est réalisée selon certains outils. Avant de les aborder, il est commode de définir la notion de clé qui sera utilisée tout au long de cette partie.

Une clé : Dans la cryptographie moderne, l'habilité de maintenir un message crypté secret, repose non pas sur les algorithmes, mais sur une information secrète dite clé qui est un paramètre utilisé en entrée d'une opération cryptographique et qui doit être utilisée avec les algorithmes pour produire le message crypté. [21]

- ***Cryptographie symétrique :***Une même clé est utilisée entre deux nœuds communicants pour chiffrer et déchiffrer les données en utilisant un algorithme de chiffrement symétrique.

  - *Avantage :*

  - L'avantage principal de ce mode de chiffrement est sa rapidité.

  - Pas d'opérations mathématiques complexes pour crypter ou décrypter les données.

  - Pas de grandes dissipations énergétiques durant les phases de chiffrement et de déchiffrement.

  - Plus adapté pour les RCSF.

  - *Inconvénients :*

La distribution de clés est difficile car dans un système symétrique, chaque nœud a besoin d'une clé partagée avec chaque autre nœud du réseau. Donc on aura à gérer $\frac{n(n-1)}{2}$clés où n est le nombre des nœuds dans le réseau.

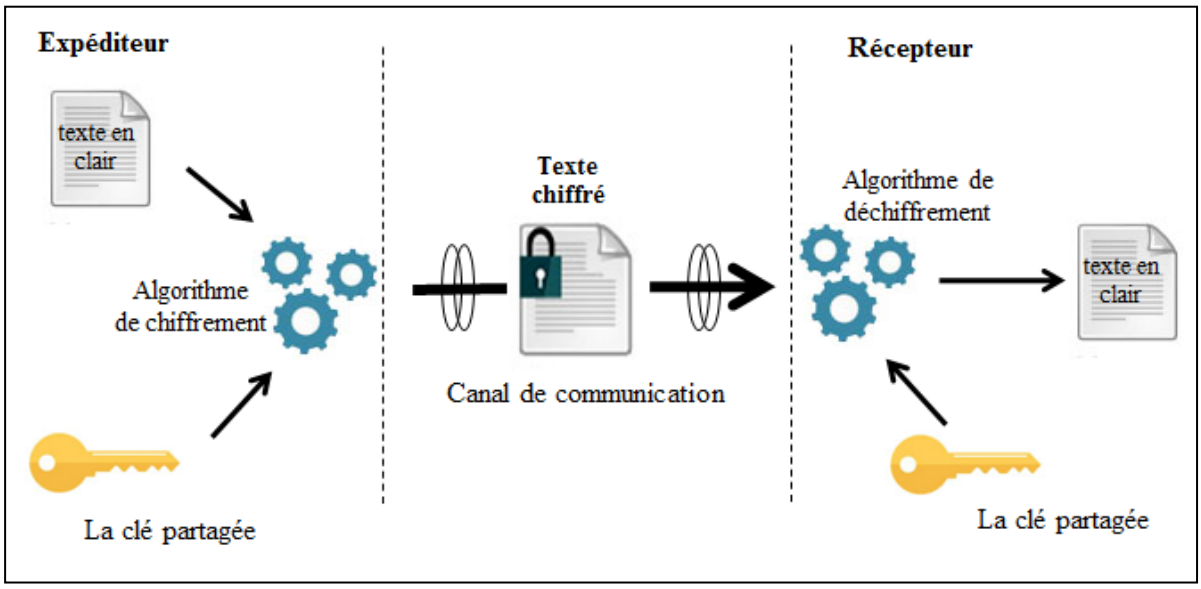


Figure 2.6: Cryptographie symétrique.

- ***Cryptographie asymétrique :***Dans la cryptographique asymétrique (ou la cryptographie à clé publique), la clé de chiffrement et la clé de déchiffrement sont différentes. Une des clés appelée clé publique (qui est diffusée) utilisée généralement pour chiffrer le message. Tandis que l'autre clé appelée clé privée (gardée secrète), permet de déchiffrer le message cryptée.

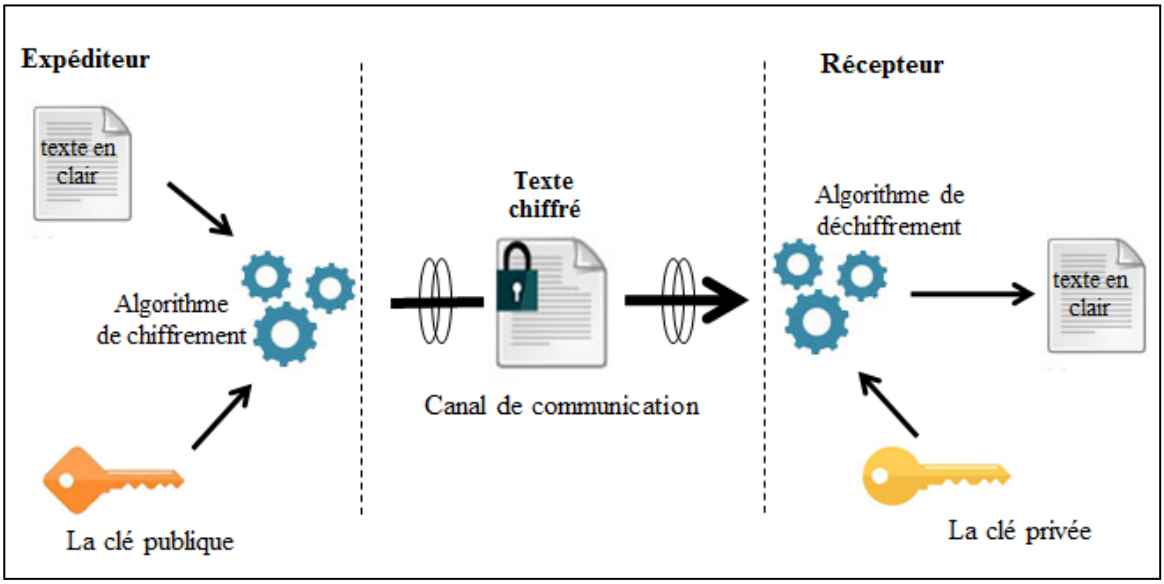


Figure 2.7: Cryptographie asymétrique.

- ***La fonction de hachage :***

'la fonction de hachage est le mécanisme qui assure l'intégrité de donnes. Cette fonction calcule une courte empreinte de taille fixe à partir d'une donnée de taille arbitraire. Etant donnée une fonction de hachage***f,*** et un message à transmettre***m.*** La fonction ***f*** doit remplir ces conditions [19] :

- Il est facile de calculer $f(m)$ · c'est-à-dire, de calculer l'empreinte à partir du contenu du message.
- Il est difficile de calculer m tel que$(m) = f$, c'est-à-dire de trouver le contenu du message à partir de l'empreinte. C'est pourquoi la fonction f est dire à sens unique.
- Il est difficile de trouver un autre message $m2$ tel que $f(m) = f(m2)$, c'est-à-dire il est difficile de trouver deux messages aléatoires qui donnent la même empreinte et cela mène à la résistance aux collisions, Cette empreinte est recalculée par le récepteur afin qu'il la compare à celle calculée par l'émetteur. Si elles sont différentes, alors les données ont été altérées pendant leur transmission.

Les fonctions de hachage les plus courantes sont : MD5, SHA-1.

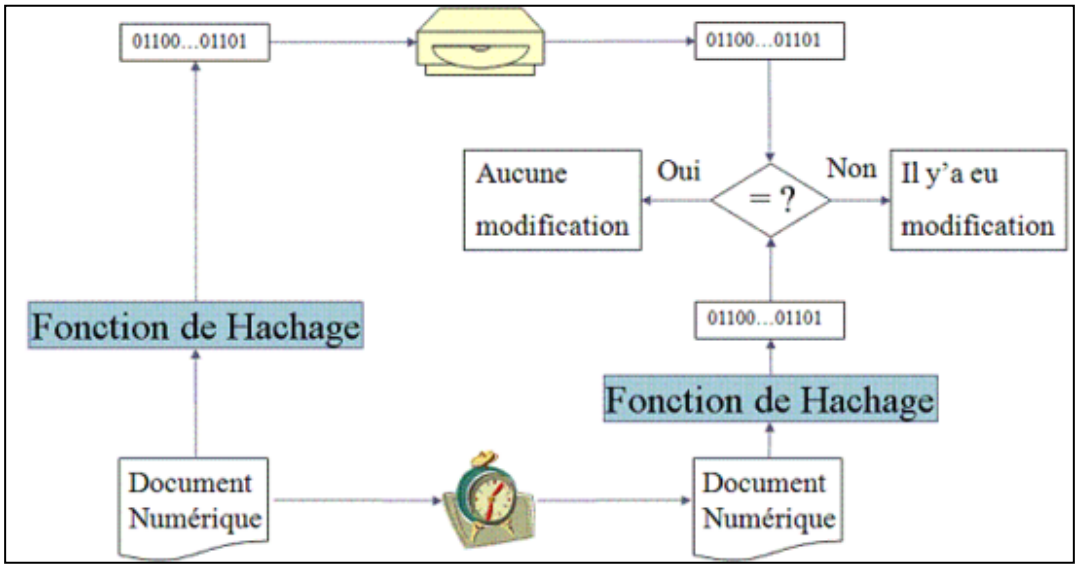


Figure 2.8: Fonction de hachage.

- ***Le code d'authentification de message***

Le code d'authentification de message MAC (Message Authentification Code) fait partie des fonctions de hachage à clé symétrique assurant l'intégrité de données comme toute autre fonction de hachage , en plus, l'authenticité de la source de données . Cette clé est utilisée pour calculer le code MAC par l'émetteur. Ce code est par la suite envoyé avec les données.

[19]. Le récepteur calcule à son tour le code MAC avec cette même clé et le compare au code qu'il a reçu. S'ils sont bien identiques, alors la source est authentique et les données n'ont pas été altérées.

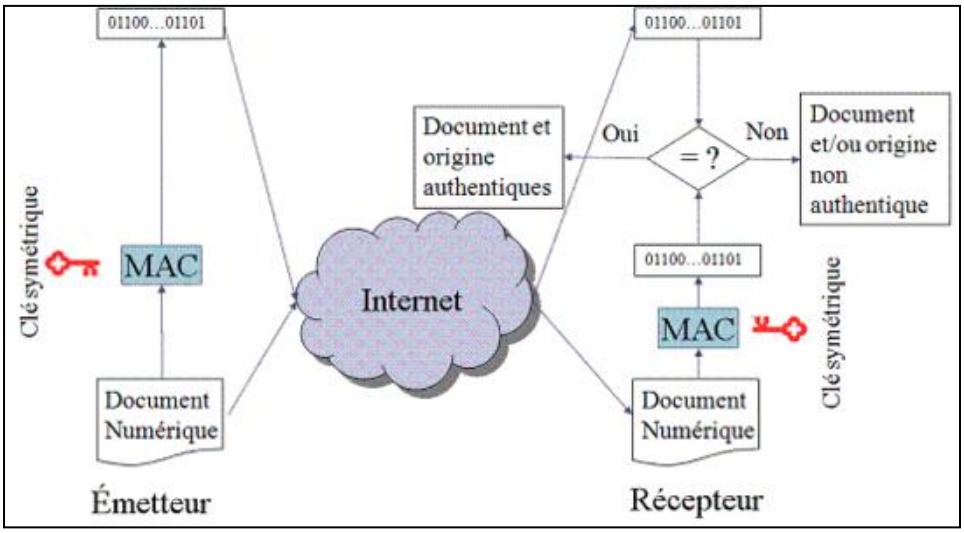


Figure 2.9: Le code d'authentification de message MAC.

La gestion des clés

La gestion des clés est un des aspects les plus difficiles de la configuration d'un système cryptographique de sécurité. Pour qu'un tel système fonctionne est soit sécurisé, chacun des utilisateurs doit disposer d'un ensemble de clés secrètes (dans un système à clés secrètes) ou de paire de clés publiques/privés (dans un système à clés publiques). Cela implique de générer les clés et de les distribuer de manière sécurisée aux nœuds capteurs. Il doit aussi pouvoir enregistrer et gérer ses clés publiques et privées de manière sure. Dans les systèmes à clés publiques, la gestion des clés comprend la capacité à vérifier et à gérer les clés publiques des autres nœuds. []

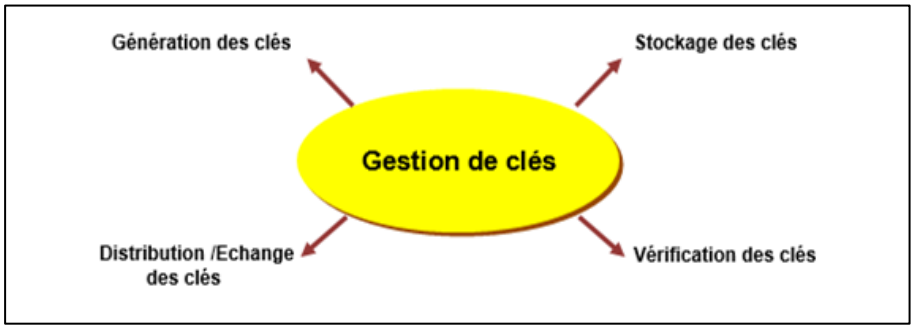


Figure 2.10: Fonctions de la gestion de clés.

2.4.4.2. Protocoles et services

Bien que la protection du canal de communication protège les RCSF contre certaines attaques, elle ne garantit pas entièrement que d'autres attaques ne les affectent pas. Par exemple, une attaque DoS peut conduire à une dégradation d'un ou plusieurs services réseau et cela compromettre la disponibilité du réseau, et d'autres attaques spécifiques aux protocoles élaborées peuvent perturber, détruire ou corrompre un réseau. Cependant, elles peuvent être n'importe quel événement qui diminue ou élimine la capacité du réseau d'exécuter ses fonctions attendues. Par conséquent, il est nécessaire de créer des protocoles et services spécialisés capables de soutenir adéquatement la protection des données.

Nous concentrons dans ce qui suit sur les principaux mécanismes qui sont utilisés pour sécuriser les protocoles de base du réseau RCSF à savoir : les mécanismes permettant de sécuriser le routage, l'agrégation de données, la localisation et la synchronisation temporelle.

2.4.4.2.1. La sécurité de routage

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

2.4.4.2.2. La sécurité d'agrégation de données

Il existe deux grandes catégories de solutions selon le mécanisme cryptographique utilisé :

- Solutions basées sur le cryptage de bout en bout : dans cette catégorie on utilise des mécanismes cryptographiques qui sécurisent l'information captée de bout en bout tout en permettant aux nœuds intermédiaires de réaliser les opérations d'agrégation.

Dans cette catégorie, la vérification de l'information ne se fait généralement qu'au niveau du collecteur, ce qui engendre une forte contamination de la fausse information.

- Solutions basées sur le cryptage de proche en proche : dans ce cas, la véracité de l'information est vérifiée de proche en proche et son rejet peut se faire à n'importe quel niveau de l'arbre couvrant le RCSF.

2.4.4.2.3. La sécurité de la localisation

Dans les RCSF, la localisation est un facteur très important pour assurer la fiabilité de leur fonctionnement. Dans un nombre important d'applications des réseaux de capteurs, les nœuds sont généralement déployés aléatoirement. La plupart de ces applications (militaires, suivis des animaux) exigent la connaissance de la position physique des nœuds capteurs afin de pouvoir localiser l'origine des événements détectés. En effet, l'utilité d'un RCSF se fondera sur ses capacités de localiser automatiquement chaque capteur dans le réseau. Ainsi, un réseau de capteurs conçu afin de détecter des événements aura besoin d'informations précises sur l'endroit pour repérer exactement la position de ces derniers. En outre, la localisation peut être utilisée aussi pour d'autres aspects tels que dans l'identification des données, et dans les protocoles de routage géographique dans les réseaux à grande échelle. Par conséquent la sécurisation des mécanismes de localisation est nécessaire pour protéger le réseau des adversaires malicieux qui tentent de compromettre les informations de localisation afin de perturber le fonctionnement du réseau.

2.4.4.2.4. Les systèmes de détection d'intrusions

Le système de détection d'intrusion (IDS : Intrusion Détection System) est capable de détecter avec une grande précision les attaques internes. Ce mécanisme permet de détecter les activités anormales ou suspectes sur la cible analysée et déclenchera une alarme lorsqu'un comportement malveillant se produit. Les IDS utilisent différents mécanismes pour déceler les attaques:

- *Technique de détection à base de signature:* Cette approche consiste à comparer l'action observée d'un nœud avec un ensemble de signatures (actions habituellement effectuées par des adversaires) d'adversaires répertoriés par le système de détection. On détecte que le nœud analysé est défini comme étant un adversaire quand on parvient à trouver une signature parmi les actions analysées.

- *Technique de détection à base d'anomalies:* Cette approche est focalisée d'abord sur la modélisation d'activité normale d'un nœud et puis identifier tout ce qui s'éloigne de ce modèle de référence comme étant une anomalie. L'avantage principal de cette technique est de pouvoir détecter les attaques inconnues. Le système de détection d'intrusion (IDS) reste une tâche importante qui complété les fonctions de sécurité par leur détection et prévention de toutes les attaques malveillantes.

2.5. La gestion des clés dans les réseaux de capteurs sans fil

Après leur déploiement, les capteurs ont besoin d'établir des clés cryptographiques avec leurs voisins pour assurer des services de sécurité:

- ✓ Sécuriser le routage.
- ✓ Sécuriser l'agrégation.
- ✓ Coopération (authentification).

La gestion des clés fournit des mécanismes fiables, sécurisés et efficaces par lesquels les clés cryptographiques sont générées, stockées, protégées, transférées, chargées, utilisées et détruites. Par conséquence, la gestion de clés est un service primordial pour la sécurité de n'importe quel système basé sur la communication.

2.5.1. Composants de la gestion de clés

Sous les contraintes strictes et sévères posés par les RCSF, la conception d'un système de gestion de clés est un grand défi. De ce fait, un système de gestion de clés inclut les trois composants suivants :

2.5.1.1. L'établissement de clés

L'établissement d'une clé secrète entre deux nœuds ou plusieurs est l'un des services de sécurité le plus important qui assure la confidentialité et l'intégrité des échanges dans un RCSF. Afin d'atteindre ce but d'une façon sécurisée, nous avons besoin d'un protocole qui permet de gérer : la pré-distribution de clés avant le déploiement et l'établissement de clés d'une façon sécurisée après le déploiement.

2.5.1.2. Le renouvellement de clés ("re-keying")

Il est possible que dans certains cas la vie des clés expirent et de nouvelles clés doivent être mises en service. Le renouvellement des clés "re-keying" est un défi puisque de nouvelles clés

doivent être produites d'une manière efficace et conforme à une consommation et conservation d'énergie. [20]

2.5.1.3. La révocation de clés

La révocation de clé est un élément important dans un système de gestion de clé parce qu'elle permet de limiter le danger causé par une capture de nœuds du réseau. Elle consiste à supprimer des clés avant leur expiration prévue à l'origine. Une fois la capture d'un nœud détectée, le système de gestion de clés devrait fournir des mécanismes permettant de révoquer les clés compromises des nœuds identifiés de manière dynamique et lancer ensuite un mécanisme de renouvellement de clés. Seuls les liens entre le nœud capturé et ses voisins sont logiquement coupés. La révocation assure qu'un nœud capteur évincé n'est plus en mesure de déchiffrer les messages sensibles transmis sur le réseau. Ainsi, ce processus consiste à empêcher tous intrus de modifier le comportement du réseau en injectant de fausses données ou en modifiant des données des nœuds sécurisés.

2.5.2. Les phases d'établissement de clés

Dans les RCSFs, les protocoles de gestion de clés sont basés sur des fonctions cryptographiques symétriques ou asymétriques. Bien que la cryptographie asymétrique comporte des avantages certains par rapport à la cryptographie à clé symétrique et malgré qu'elle offre une meilleure résistance aux attaques de compromission de nœud ainsi que les recherches qui visent à les appliquer aux RCSFs, la cryptographie à clé symétrique possède ses propres qualités qui la rend toujours la plus préférée pour les RCSF. Pour cela et principalement en raison de sa consommation d'énergie raisonnable la plupart des solutions de gestion de clés existantes sont basées sur la cryptographie symétrique.

Le problème majeur avec la cryptographie symétrique est de pouvoir trouver une méthode qui achevé l'établissement de clé entre les nœuds. Afin de résolvent ce problème d'établissement de clés en passant par le procédé de pré-distribution de clés qui exige un chargement d'information secrète dans les nœuds capteurs avant leur déploiement dans le réseau. Cette information secrète, déployée dans le réseau, peut être une clé secrète, ou de l'information auxiliaire qui aide des nœuds à dériver la clé secrète réelle.

Les RCSF utilisent un mécanisme à clé symétrique pour l'établissement de clé basée sur la pré-distribution de clés, cela est réalisé en trois étapes suivantes :

2.5.2.1. Pré-distribution de clés (Key pre-distribution)

La seule méthode pratiques pour la distribution des clés aux nœuds de RCSF dont la topologie est inconnue avant le déploiement devra compter sur la pré-distribution des clés, des clés doivent être installées dans des nœuds à fin de sécuriser la transmission de paquets. [20]

2.5.2.2. Découverte de clé partagée

Chaque nœud doit découvrir ses voisins dans son porté sans-fil de communication avec lesquelles il partage des clés. Un lien de communication existe entre deux nœuds de capteur seulement s'ils partagent une clé. Le bon schéma de découverte des voisins ne donnera à un attaquant aucune occasion de découvrir les clés partagées et l'attaquant peuvent seulement faire l'analyse de trafic. [20]

2.5.2.3. Établissement de clés de chemin

Pour n'importe quelle paire de nœuds qui ne partagent pas une clé mais sont reliés par un chemin multi saut doivent fixer une clé de chemin "path key" pour sécuriser la communication bout à bout, cette clé de chemin ne peut pas être celle déjà employée entre les nœuds voisins. [20]

2.5.3. Classification des méthodes de gestion de clés

Bien que la cryptographie à clé publique comporte des avantages certains par rapport à la cryptographie à clé symétrique et malgré les recherches qui visent à les appliquer aux RCSF, la cryptographie à clé symétrique possède ses propres qualités qui la rend toujours la plus préférée pour les RCSF. Pour cette raison la plupart des schémas de gestion de clés proposés pour les RCSF sont basés sur la cryptographie symétrique. Le problème majeur avec la cryptographie symétrique est de pouvoir trouver une méthode qui facilite l'établissement des clés entre les nœuds. La solution commune est d'utiliser une méthode de pré-distribution, dans laquelle les clés sont chargées dans les nœuds capteurs avant le déploiement. La figure suivante illustre une taxonomie des solutions de gestion de clés basée sur la pré-distribution. Dans cette taxonomie, les protocoles sont classés selon la façon avec laquelle les nœuds voisins partagent des clés communes (probabiliste ou déterministe), et selon la topologie du réseau (hiérarchique ou plate).

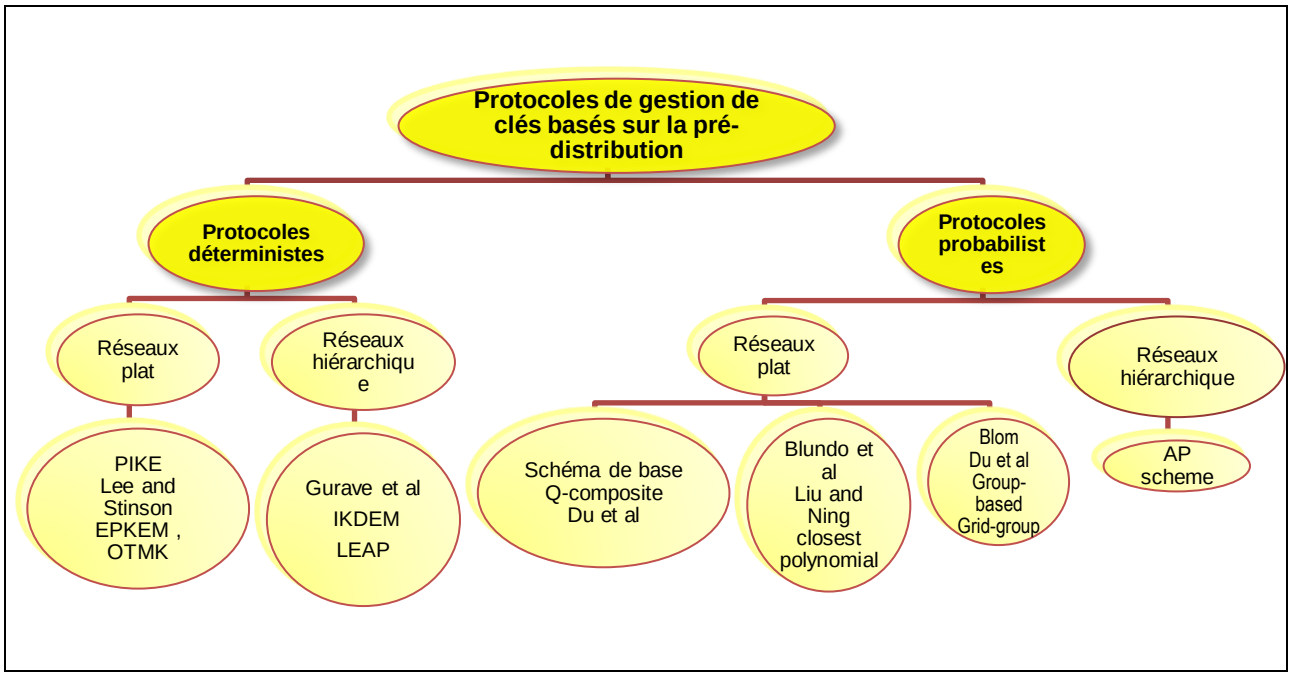


Figure 2.11: Taxonomie des protocoles de gestion de clés basés sur la pré-distribution dans les RCSF.

2.5.3.1. Schémas probabilistes

Pour les protocoles de gestion de clés probabilistes, un sous ensemble de clés prélevées à partir d'un grand ensemble de clés et placés dans les nœuds capteurs. L'idée de cette méthode est que deux nœuds communiquent entre eux ont une certaine probabilité d'avoir partagé une clé commune qui appartient aux deux sous-ensembles de ces communicants.

EschenaueretGligor ont proposé un schéma de gestion de clé basé sur la probabilité de partager une clé entre les nœuds d'un graphe aléatoire. Il fournit des techniques pour la pré-distribution de clé, la découverte de la clé partagée, l'établissement de chemin de clé, et la révocation de clé. [22]

L'idée maîtresse de ce schéma, est de distribuer aléatoirement un certain nombre de clés, issues d'un ensemble fini à chaque nœud du réseau avant son déploiement. Deux nœuds quelconques seront en mesure de s'échanger des messages sécurisés s'ils possèdent une clé commune.

- *Phase de pré-distribution de clés :* un grand ensemble S de clés est générée$(2^{17} - 2^{20} Clés)$. Pour chaque nœud, m clés sont choisisses au hasard de l'ensemble $S(S = \{(K_{id1}, Key_1)\}, (K_{id2}, Key_2), \dots\})$. Ces m clés sont stockées dans la mémoire du nœud et forment le trousseau de clés du nœud. Le nombre de clés $|S|$de l'ensemble est choisi de telle manière que deux sous-ensembles aléatoires de S de taille m auront une certaine probabilité p d'avoir au moins une clé en commun, par exemple pour une probabilité $p = 0.5$ on a besoin d'un sous ensemble de taille $m = 75$ clés de l'ensemble S de taille $|S| = 10.000$ clés.

- *Phase de découverte de clés partagées :* Les nœuds découvrent leurs voisins et plus particulièrement ceux avec qui ils sont en mesure de communiquer de façon sécurisée car ils possèdent une clé identique dans leur trousseau de clés respectif. Le protocole peut être de diffuser la liste des identités K_{idi} des clés possédées. La clé partagée devient la clé de session du lien entre les deux nœuds. La figure 2.8 illustre cette phase :

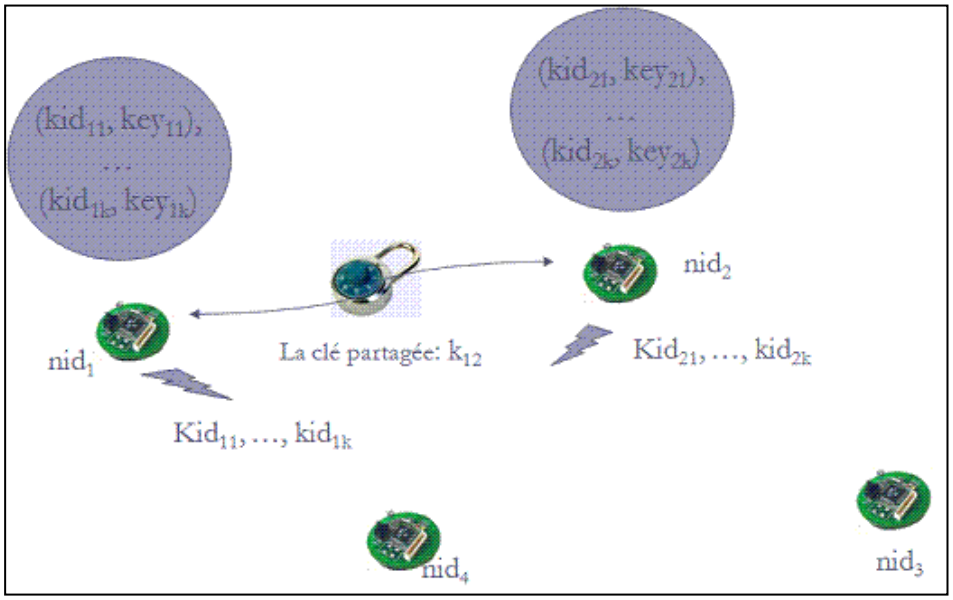


Figure 2.12: Découverte des clés partagées.

- *Phase d'établissement de chemin de clés :* Après la phase de découverte de clés partagées, le réseau devient un graphe connecté formé de quelques liens sécurisés. Les nœuds peuvent alors utiliser les liens existants pour mettre en place des clés partagées avec leurs voisins qui ne partageaient pas de clé en commun avec eux. La figure suivante illustre cette phase :

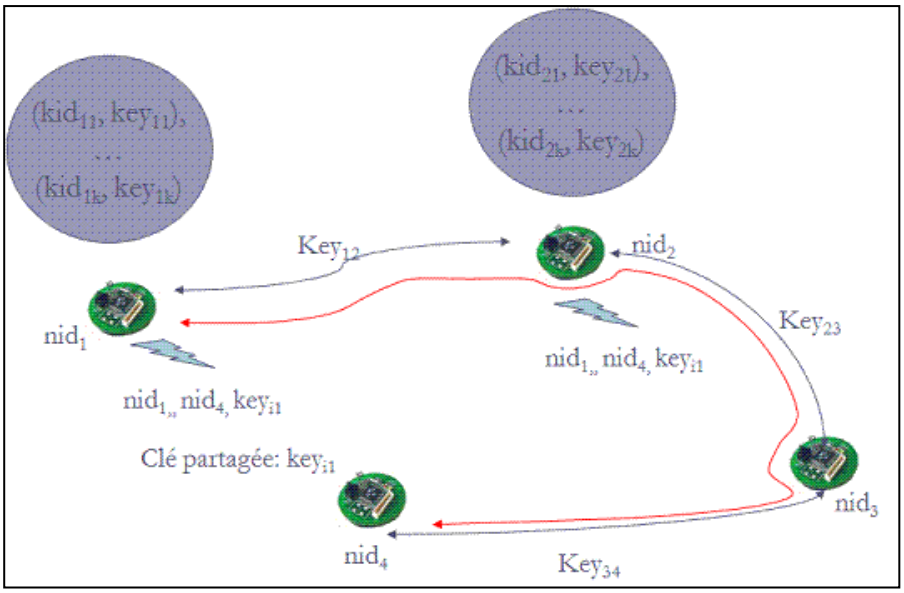


Figure 2.13: Etablissement de chemins sécurisés.

- *La révocation de clés :* La révocation d'un nœud compromis se fait par l'élimination de leur trousseau de clés. Pour cela, un nœud contrôleur (qui a une grande connectivité et peut être mobile) annonce un message simple de révocation contenant une liste signée de K identificateurs des clés (K_{idi}) pour que ces clés soient retirées des trousseaux de clés des autres nœuds. La liste des identités est signée par une clé de signature K_e générée par le nœud contrôleur et envoyée en unicast à chaque nœud $\boldsymbol{i}$en la chiffrant avec la clé K_{ci}(la clé K_{ci} est partagée entre le contrôleur et le i ème nœud pendant la phase de pré-distribution de clés). Quelques liens seront disparus à cause de la suppression de clés du nœud compromis ce qui nécessite une reconfiguration de ces liens (par la découverte de clés partagées ou l'établissement de chemin de clé).

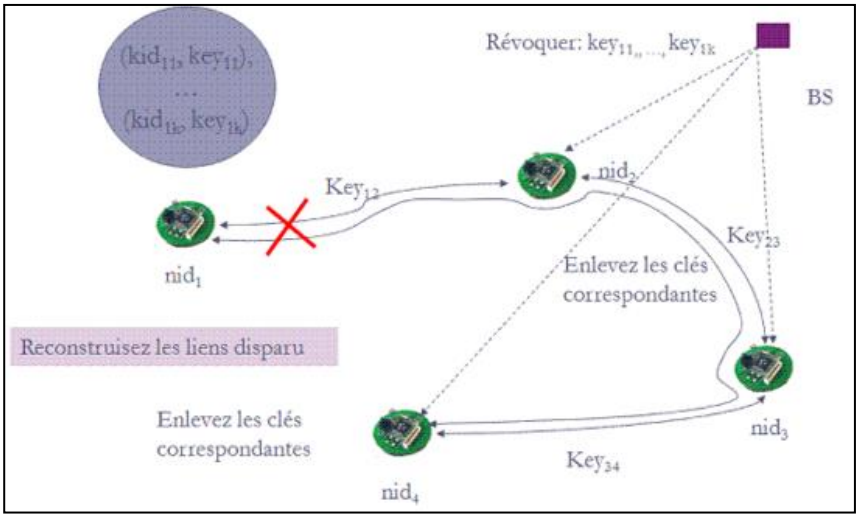


Figure 2.14: Révocation de clés.

Schéma q-composite de H.CHAN, A.PERRIG et D.SONG : Ce schéma est identique à celui de Eschenaur et Gligor sauf qu'au lieu d'exiger le partage d'une clé commune pour sécuriser un lien, une paire de nœud doit partager q clés avec $q > 1$ pour établir un lien sécurisé. La nouvelle clé utilisée pour la communication entre ces deux nœuds est le hash de toutes les clés partagées, par exemple pour deux nœuds quelconque qui partage q' clés $(q' \geq q)$ la clé utilisée pour la communication est $K = hash\,(k_1 \,||\, k_2 \,||\, \ldots \,||\, k_{q'})$.Plus le nombre de clé partagées augmente plus la résilience contre la capture du nœud augmente. Autrement, lorsque le nombre exigé de clés partagées augmente, il devient plus difficile à un attaquant avec un ensemble donné de clés de casser un lien. Cependant, pour préserver une probabilité donnée p que deux nœuds partageant des clés suffisantes pour établir un lien sécurisé, il est nécessaire de réduire la taille de l'ensemble de clés S. Ceci permet à un attaquant de gagner un plus grand échantillon de S en cassant peu de nœuds. La figure suivante illustre un exemple de partage de clés avec $q = 2$:

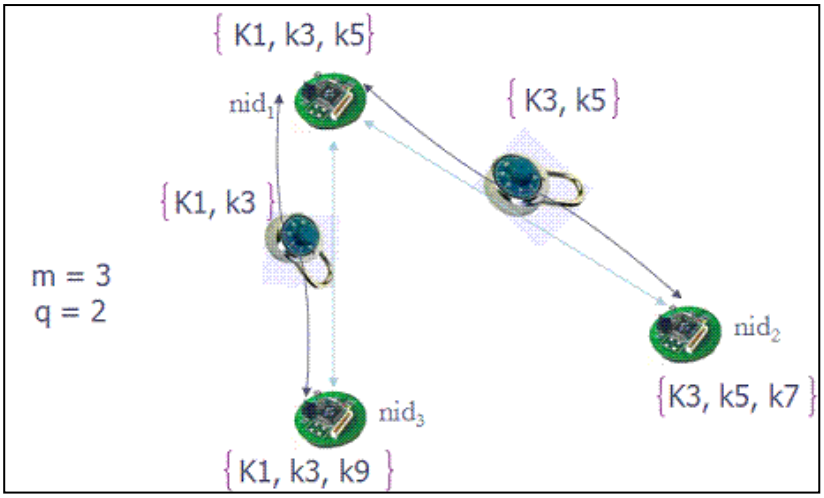


Figure 2.15: Schéma q-composite.

2.5.3.2. Schémas déterministes

Contrairement aux schémas de gestion de clés probabilistes, les protocoles de gestion de clés déterministes assurent que chaque nœud est capable d'établir une clé par-paire avec ses voisins. Pour garantir le déterminisme, les protocoles, tels que LEAP et OTMK, utilisent une clé commune, transitoire et pré-chargée dans tous les nœuds avant leurs déploiements. Cette clé est utilisée en vue de générer des clés par-paires entre chacun des deux nœuds voisins. Pour sécuriser les nœuds contre les attaques de captures, la clé transitoire est effacée du nœud après la génération des clés par-paires. Dans les réseaux ayant une organisation hiérarchique, les schémas de gestion de clés déterministes centralisent la responsabilité d'établissement des

liens sécurisés entre les membres du cluster au niveau du chef de cluster. Malgré que ces schémas offrent l'avantage de consommer moins d'énergie, ils sont vulnérables par rapport aux attaques de captures, et particulièrement quand le chef de cluster est compromis. [21]

Zhu et autres proposent le protocole déterministe LEAP (LocalizedEncryption and Authentication Protocol). LEAP est basé sur une clé initiale K_{in} chargée dans chacun des nœuds du réseau. Les auteurs de LEAP supposent que pour compromettre un nœud, l'adversaire nécessite un temps minimal T_{min} : c'est le temps de brancher un câble série et le temps de copier le contenu de la mémoire du nœud compromis. LEAP exploite ce temps (de confiance) pour permettre à deux nœuds voisins d'établir d'une manière sécurisée une clé symétrique de session à partir de la clé initiale transitoireK_{in}. AprèsT_{min}, la cléK_{in} est supprimée de la mémoire du nœud. Il prend en charge :

- *Chargement de la clé initiale :* Le contrôleur (SB) génère une clé initiale K_{in} et charge chaque nœud avec cette clé. Chaque nœud u dérive une clé principale (Maser Key) $K_u = F_{K_{in}}(u)$, F_k étant une fonction pseudo-aléatoire.
- *Découverte des voisins :* Immédiatement après son déploiement, le nœud u essaye de découvrir ses voisins en diffusant un message HELLO qui contient son ID. aussi, il initie un timer qui sera déclenché après le tempsT_{min}. Le nœud u attend un ACK de chacun de ses voisins V qui contient l'identificateur de v. l'ACK est authentifié en utilisant la clé principaleK_v, qui est dérivée comme suit : $K_v = F_{K_{in}}(v)$. Comme le nœud u a la clé K_{in}, il pourra aussi vérifier l'authenticité du ACK reçus :

  $u \rightarrow *, u$

  $v \rightarrow u, v/\mathrm{MAC}\ (K_v, u/v)$

- *Etablissement de la clé par-paire :* le nœud u calcule sa clé par paire K_{uv} avec v, comme suit :

  $$K_{uv} = F_{K_v}(u).$$

  Le nœud v peut de même calculer K_{uv} de la même manière.
  K_{uv}sert comme clé entre u et v.

- *Effacement des clés :* lorsque le timer expire aprèsT_{min}, le nœud u efface K_{in}et toutes les clés principales K_v de ses voisins. Il est à noter que le nœud u n'efface pas sa clé principaleK_u.

- *Sécurité de LEAP :* A la fin de ces quatre étapes, le nœud u aura établi une clé par-paire partagée avec chacun de ses voisins. Cette clé sera utilisée pour sécuriser les données échangées entre eux. De plus, aucun nœud dans le réseau ne possède la clé K_{in}. Un adversaire peut écouter clandestinement tout le trafic dans cette phase, mais sans la clé K_{in}il ne peut injecter des informations incorrectes ou déchiffrer les messages. Un adversaire compromettant un nœud après T_{min}, obtient seulement les clés du nœud compromis. Quand un nœud compromis est détecté, ses voisins suppriment simplement les clés qui ont été partagée avec lui.

2.5.4. Métriques d'évaluation

Des métriques sont employées pour comparer les différents protocoles de gestion des clés, ces métriques sont [20] :

2.5.4.1. Efficacité des ressources

Comme les nœuds de capteur sont limités en ressources, un bon schéma de gestion de clés ne doit pas consommer une grande quantité de ressources. Les ressources ici pourraient être :

- L'espace de stockage : est la quantité de mémoire nécessaire pour enregistrer les clés.
- La capacité de communication : détermine le nombre de messages échangés pour la gestion des clés.
- La puissance de calcul : est mesuré en termes de quantité de cycles de processeur nécessaires pour établir une clé.

2.5.4.2. Résilience contre la capture de nœud

Ou résistance contre la capture de nœud, cette métrique mesure comment le RCSF est compromis quand un nœud est compromis, et l'influence de ce nœud sur la sécurité du réseau.

2.5.4.3. La connectivité

La connectivité de clé est définie comme la probabilité qu'une paire de nœuds puissent établir une clé commune entre eux. En effet, dans un grand nombre des schémas de gestion de clés probabiliste des paires des nœuds capteurs ne peuvent pas avoir une clé partagée, cela permet de limiter la connectivité du réseau. Pour assurer la continuité de la sécurité, La méthode de gestion de clés doit être capable d'assurer une bonne connectivité du réseau.

2.5.4.4. Passage à l'échelle (scalability)

Le nombre de nœuds de capteurs déployés dans la zone de détection peut atteindre plusieurs centaines, voire plusieurs milliers. De plus, pendant toute la durée de vie du réseau de capteurs, des nœuds peuvent rejoindre ou quitter. Par conséquent, les solutions de gestion de clés doivent pouvoir s'adapter à différentes tailles de réseau. Dans le même temps, les fonctionnalités de sécurité et d'efficacité des petits réseaux doivent être conservées lorsqu'elles sont appliquées aux réseaux plus grands.

2.6. Conclusion

Ce chapitre a mis en évidence l'importance cruciale de la sécurité dans les réseaux de capteurs sans fil. L'étude a souligné les principales menaces auxquelles les RCSF sont confrontés, telles que l'interception de données, les attaques par déni de service et la compromission des capteurs. Ces menaces peuvent avoir des conséquences graves, allant de la perte de données sensibles à la perturbation des opérations du réseau.

Pour faire face à ces défis, différentes techniques de sécurité ont été examinées, telles que le chiffrement des données, les mécanismes d'authentification, la détection d'intrusion et la gestion des clés. Ces techniques contribuent à la confidentialité, l'intégrité et la disponibilité des données dans les RCSF.

Nous avons déduit que la gestion de clés dans un RCSF représente un point très important pour de nombreux services de sécurité, beaucoup de travaux ont été effectués afin d'avoir un schéma performant qui assure un niveau élevé de sécurité et optimise les métriques de performances et conserve l'énergie. Pour conclure, Toutes les méthodes que nous avons étudiées dans ce chapitre possèdent de grands avantages. Cependant, il est difficile d'assurer un niveau de sécurité élevé avec une consommation d'énergie minimale. Par conséquent, un protocole de sécurité doit être fourni un meilleur compromis entre la fiabilité et la consommation d'énergie.

Chapitre 3

Approche de gestion de clés proposée

3.1. Introduction

Les nœuds de capteurs sont généralement déployés dans des zones non surveillées, et la plupart des applications RCSF nécessitent un niveau de sécurité élevé pour fournir les exigences de sécurité de base et mettre ces applications à l'abri de différentes attaques, empêchant les intrus de détruire le système en contrôlant le fonctionnement normal des nœuds capteurs. La sécurité des communications sans fil est un autre problème important affectant l'utilisation de RCSF. La communication sur les canaux sans fil est intrinsèquement non sécurisée et permet aux intrus d'espionner, de falsifier ou d'injecter des données dans le réseau.

Dans ce contexte, un mécanisme de sécurité est en effet nécessaire pour la majorité des applications basées sur le RCSF, en particulier lors de l'utilisation des nœuds capteurs dans un lieu peu sûr. La gestion de clés constitue la pierre angulaire des autres mécanismes de sécurité, car presque tous les mécanismes de sécurité reposent sur le cryptage ou sont liés à celui-ci.

Dans ce chapitre, nous exposons notre système développé baptisé CFKM (Cluster formation and Key management scheme for Wireless sensor Networks), dédié pour une gestion de clés innovante associée aux réseaux de capteurs ayant une topologie hiérarchique. Nous commencerons d'abord par présenter la motivation derrière cette conception, ensuite nous présenterons les détails de cette dernière. Nous évaluons par la suite les performances par rapport au protocole SC-SPK.

3.2. Spécifications générales sur le modèle du réseau

Dans notre approche, nous envisageons l'utilisation d'une architecture de réseau hiérarchique basée sur le concept de clustering. Selon cette architecture, les nœuds capteurs sont déployés de manière aléatoire et uniforme. Pour organiser le réseau, les nœuds capteurs sont regroupés en clusters. Chaque cluster est supervisé par un cluster-Head (CH) qui est responsable de la collecte de la gestion des informations provenant des nœuds capteurs membres (CM) du cluster. Les données collectées sont agrégées par les CH et transmises à une station de base (SB) qui se charge de la gestion globale du réseau et de la communication avec l'extérieur. Les nœuds capteurs sont tous similaires en termes de capacités de traitement, de communication, d'énergie et de stockage. En revanche, la station de base dispose de

ressources illimitées. Les CH sont répartis uniformément dans le réseau et leur élection repose sur des critères tels que la portée de communication, la localisation et les ressources disponibles. Il est important de gérer l'énergie des CH, qui diminue lors des calculs et des communications. Ainsi, des mécanismes de rotation des CH sont nécessaires pour prolonger la durée de vie du réseau en remplaçant régulièrement les CH et en équilibrant la consommation d'énergie.

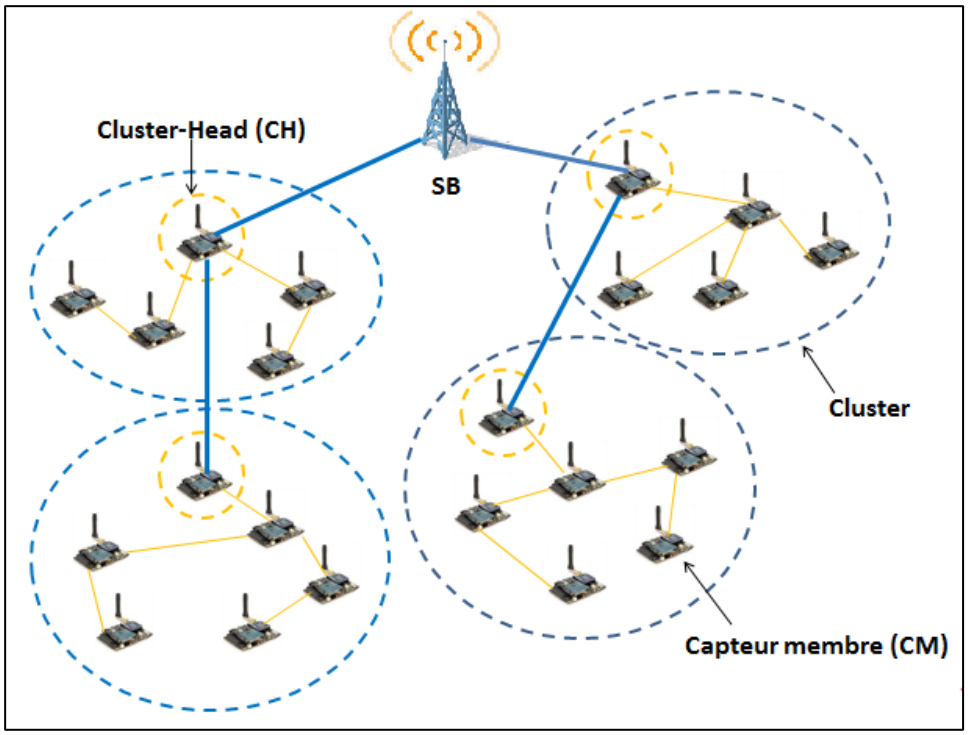


Figure 3.1 : Modèle d'architectures hiérarchique pour un RCSF

3.3. Le système de gestion de clés proposé

Notre proposition repose sur l'établissement de clés. Elle permet de gérer les clés cryptographiques avant et pendant le déploiement du réseau. En s'appuyant sur des clés pré-chargées, notre schéma est entièrement distribué. En effet, aucune clé secrète ne sera échangée via le réseau.

Avant le déploiement du réseau de capteurs, deux clés sont pré-distribuées à chaque capteur. Ces clés permettent de sécuriser la phase de déploiement. L'une de ces clés est utilisée pour sécuriser les communications pendant la phase de formation du cluster et l'établissement de clés et sera effacée après le déploiement de clés.

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

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

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

Tableau 3.1 : Acronymes définition

3.3.1. La phase de pré-distribution de clés

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

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

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

CFKM utilise un crypto-système symétrique et prend en charge dans cette phase la formation de clusters et l'établissement deux types de clés : la clé $K_{CM_j-CH_\alpha}$ (la clé partagée entre un nœud membre CM_j et son cluster head CH_α) et $K_{CH_\alpha-CH_\beta}$(la clé partagée entre deux cluster head CH_αet CH_β). Ces clés seront utilisées afin d'établir des communications sécurisées.
La phase deformation de cluster et l'établissement de clésdu protocole CFKM se déroule en plusieurs étapes :

Etape 1 : Planification

Dans cette étape, le réseau global est représenté par une grille de taille Z / K, ou chaque cellule correspond à une région spécifique du réseau. Chaque cellule de la grille est attribuée à un ensemble de nœuds capteurs formant un cluster. Une fois les nœuds déployés, ils procèdent à la planification du réseau pour déterminer l'identification de leur cellule (ID cellule) ainsi que les coordonnées (x, y) du centre de gravité (COG :Center Of Gravity) de leur cellule. Cette planification se déroule au round 0.

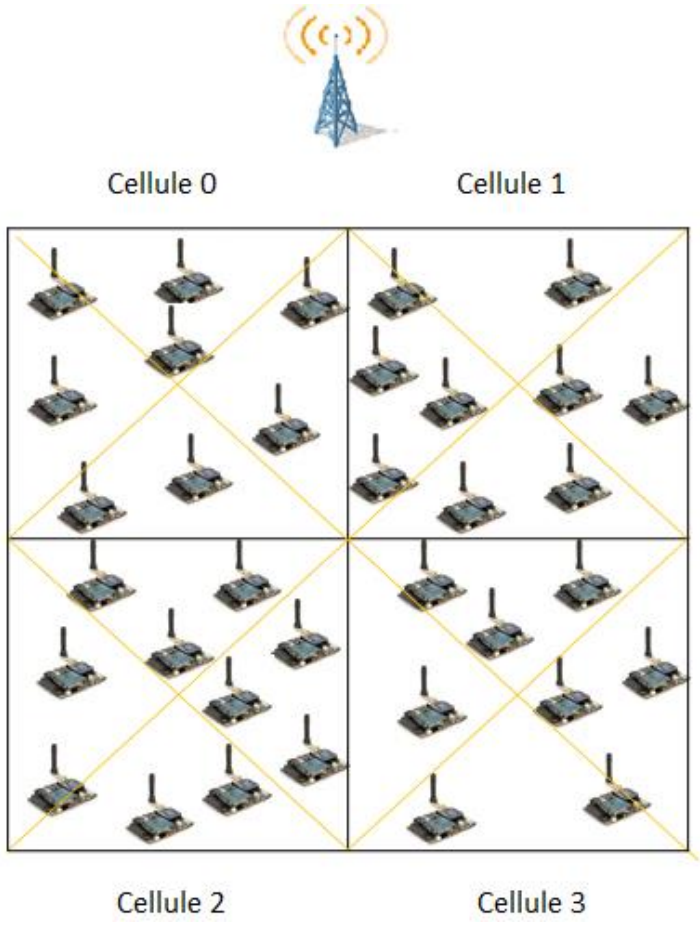


Figure 3.2 : Etape de Planification

Etape 2 : Initialisation

La phase d'initialisation débute par l'envoi d'un message d'initialisation « $HELLO$ »par la station de base à tous les nœuds capteurs du réseau. Le message envoyé est chiffré par la clé de réseau K_{in} comme suit :

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

Etape 3 : Annonce

A la fin de la phase d'initialisation, chaque nœud de capteur ayant reçu le message « $HELLO$ » diffuse un message d'annonce « $ELECTION$ » aux autres nœuds. Ce message contient l'identifiant du nœud, sa position (coordonnées (x, y)) et l'identification de sa cellule. Cette étape se déroule également au round 0.

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

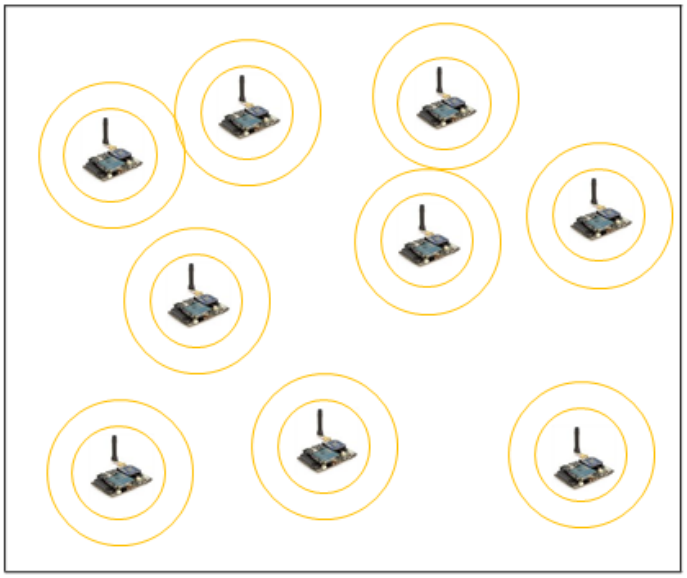


Figure 3.3 : Phase d'Annonce

Etape 4 : Election des CH et calcul des clés

Les nœuds qui ont reçu les messages « $ELECTION$ », doivent vérifier si l'ID de la cellule reçu dans le message correspond à l'ID de cellule enregistrée (sa cellule) et authentifie le message « $ELECTION$ » (en vérifiant le MAC). Chaque nœud capteur identifie ainsi les autres nœuds capteurs se trouvant dans la même cellule. Il calcule ensuite la distance entre sa position et le centre de la cellule, ainsi que la distance qui sépare chaque nœud et le centre de cette même cellule. Une fois cette étape effectuée, tous les nœuds non-CH deviennent à identifier leur CH respectif. En effet, le CH est sélectionné en fonction du classement des distances calculées. Chaque nœud, qu'il soit CH ou non-CH dans la même cellule, intègre un tableau contenant l'identifiant du nœud membre et un indice qui est déterminé selon l'ordre des distances calculées. De plus, un slot est attribué à chaque nœud membre pour communiquer avec le CH, ce slot est égal à index+1.

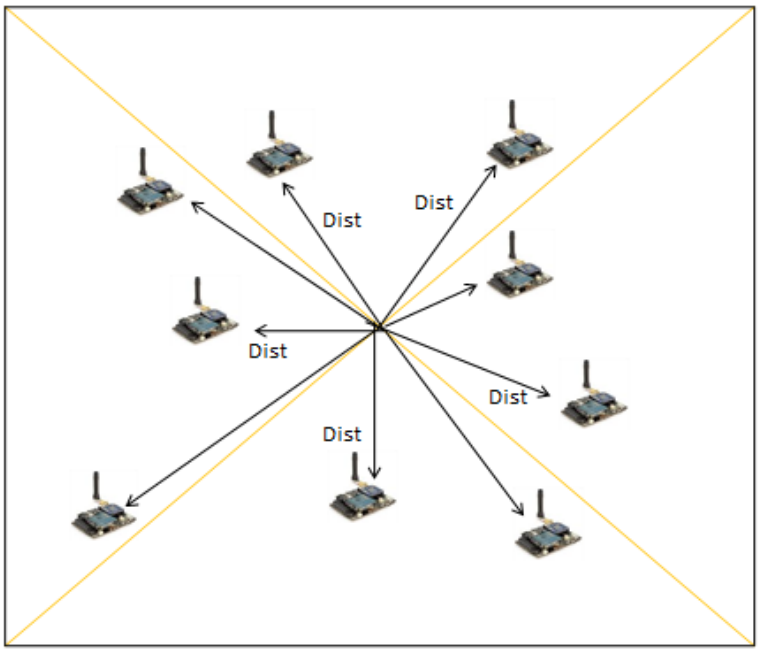
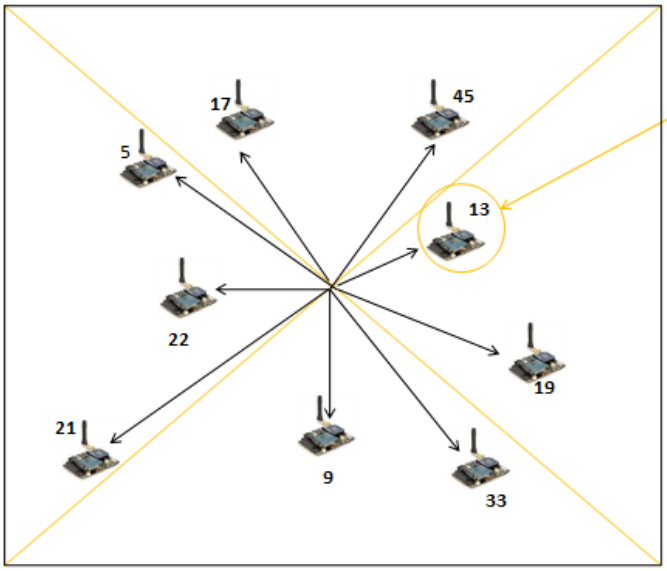


Figure 3.4 : Etape d'Élection (calcul des distances)



Le nœud CH

index	ID
0	13
1	22
2	9
3	17
4	5
5	19
6	45
7	33
8	21

Figure 3.5 : Etape d'Élection (le choix de CH)

Afin d'établir une clé de cryptage pour sécuriser la communication entre un membre de cluster CM_i et leur cluster-head CH_α, les nœuds (membre ou cluster-head) calculent la clé par paire à l'aide de l'équation suivante:

$$K_{CM_j-CH_\alpha} = H_{K_N}\left(max\left(id_{CM_j}, id_{CH_\alpha}\right) \| N_{CM_j} \oplus N_{CH_\alpha}\right) \quad (3.1)$$

Étape 5 :Etablissement de clés entre les nœuds CH

A ce point, les nœuds CH sont prêts à établir les clés pour sécuriser les communications entre eux.Pour cela, chaque nœud CH diffuse un message de requête contenant la liste L_id_{CM} aux autres CH.

$$CH_\alpha \rightarrow *: id_{CH_\alpha} \| cellu\_ID \| E_{K_r}\{HELLO\_REQ, N_{CH_\alpha}, L\_id_{CM}\}$$

$$\| MAC_{K_r}\left\{id_{CH_\alpha} \| cellu\_ID \| E_{K_r}\{HELLO\_REQ, N_{CH_\alpha}, L\_id_{CM}\}\right\}$$

Où$L_id_{CM} = \{id_{CM_1}, id_{CM_2}, id_{CM_3}, \dots, id_{CM_n}\}$

Ici, n est le nombre de nœuds CM dans chaque cluster.

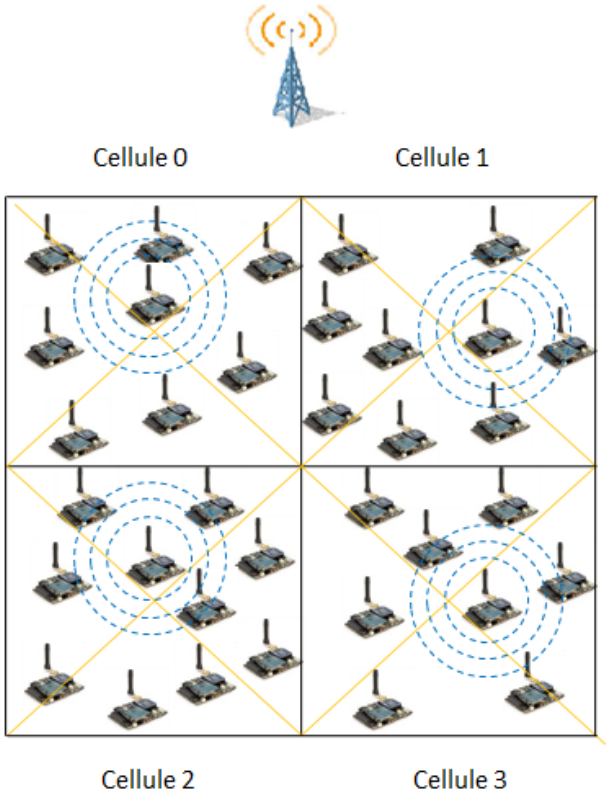


Figure 3.6 : Etape d'établissement de clés entre les nœuds CH
(Les nœuds CH diffusent le message$HELLO_REQ$)

Chaque cluster-head, après avoir reçu les messages $HELLO\_REQ$ des autres nœuds CH, vérifie l'authenticité (en vérifiant le MAC) et calcule les clés par paires partagées entre eux.

$$K_{CH_\alpha - CH_\beta} = H_{K_r}(max(id_{CH_\alpha}, id_{CH_\beta}) \parallel min(id_{CH_\alpha}, id_{CH_\beta}) \parallel N_{CH_\alpha} \oplus N_{CH_\beta}) \quad (3.2)$$

3.3.3. Effacement de clés

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

$$K_{in} = {H_{K_{in}}}^r(K_{in}) \quad (3.3)$$

$$K_N = {H_{K_N}}^r(K_N) \quad (3.4)$$

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

3.4. Description d'une approche utilisée pour l'évaluation

SC-SPK (**S**ecured**C**ommunication Key Establishment for Cluster based Wireless Sensor Networks -***P****rivate****P****artial* ***K****eys*) est un système de gestion de clés déterministe destiné aux RCSFs hiérarchiqueen clusters. Ce système reposé sur la pré-distribution de clés partielleset la cryptographie symétrique. Le processus de déroulement de SC-SPK est divisé en trois phases qui sont : la pré-distributionde clés, la formation du cluster et l'état stable. Dans la première phase les nœuds sont pré-chargés avec certain matériel cryptographique tel que le pool de clés partielles et la liste d'index de clés partielles. Dans la deuxième, après la formation des clusters et une vérification d'authentification par la station de base, tous les nœuds capteurs d'un cluster partagent la même liste de clés partielles. Enfin, chaque cluster aura un ensemble distinct de clés partielles qui seront utilisées dans cette dernière phase pour établir les clés secrètes de communication. Dans ce qui suit, nous avons détaillé chaque phase liée au schéma de gestion de clés**.**

- **La pré-distribution de clés**

Avant le déploiement, la station de base doit pré-charger certain matériel cryptographique dans chaque nœud capteur afin de générer des autres clés. Ces matériaux incluent:

- Un pool de clés partielles P,
- Une liste d'index de clés partielles,
- Une clé de réseau N_k.
- Un numéro d'identification unique ID

❖ **La formation du cluster**

Une fois le cluster C_i (i=1, 2, …, m) formé et chaque nœud reçoit l'identifiant de leur CH, tous les nœuds membres du cluster envoient leurs IDau cluster-headCH_i.

Après avoir rassemblé tous les ID, le cluster-head envoie tous les ID avec son propre ID à la station de base pour l'authentification. Si l'authentification réussit, la station de base (SB) sélectionne une liste de clés partielles dans le pool de clés P pour chaque cluster et envoie la liste d'index identifiées comme $L_i (L_i \subset L)$ au cluster-head du clusterC_i. Ensuite, chaque cluster-headCH_idiffuse la liste L_ià tous les nœuds membres du clusterC_i.

Ainsi, chaque cluster aura un ensemble différent de clés partielles et ces clés seront utilisées pour établir les clés secrètes de communication dans la phase suivante.

Une fois qu'un nœud membre a informai quelles clés partielles il emploiera avec son CH, il retire le reste de clés partielles de P qui a été inséré dans la phase de pré-distribution. La figure 3.3 résume le processusde cette phase.

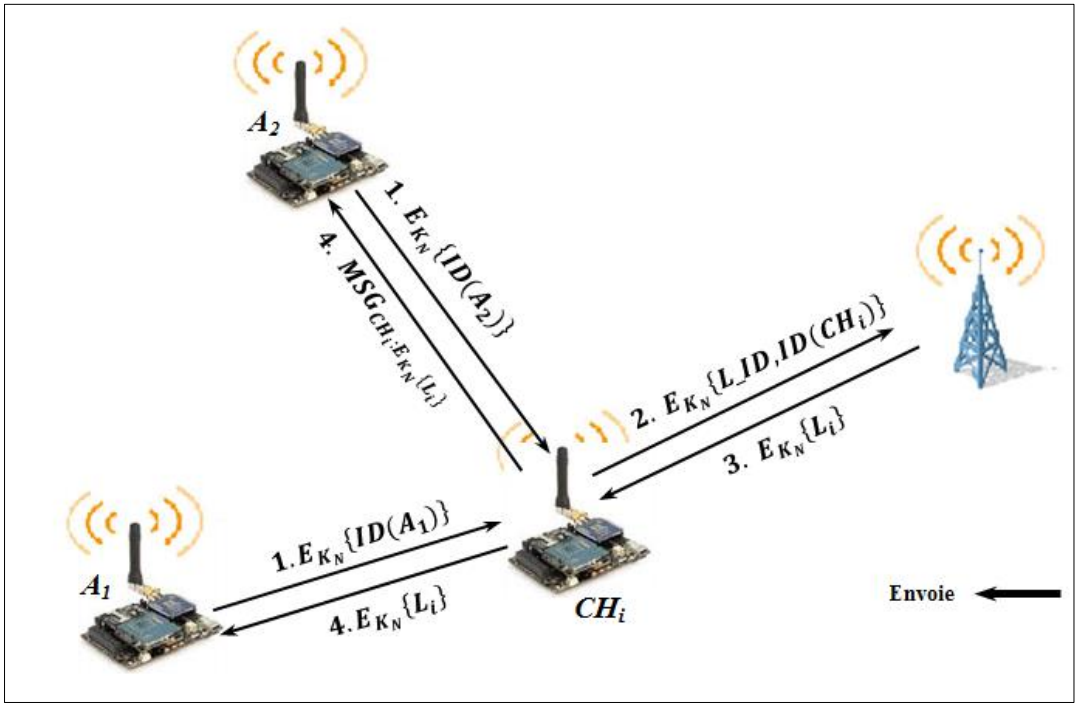


Figure 3.7 : Le processus de la phase de formation du cluster

❖ **L'état stable :**

Dans cette phase, les nœuds capteurs sont prêts à établir les clés de communication. Pour cela, afin d'établir une clé de cryptage pour sécuriser la communication entre un membre de cluster A_i et leur cluster-head CH_i, les nœuds (membre ou cluster-head) agissent comme suit:

- Le cluster-head CH_i envoie une liste d'ordre unique O_{CH_i} à chaque membre du cluster A_i, contenant la liste ordonnée des numéros d'index de q clés partielles sélectionnées à partir de L_i.
- En réponse, chaque nœud membre A_i crée également une liste d'ordres O_{A_i} avec un ordre différent des index et l'envoyer à CH_i.

À ce point, les nœuds capteur A_i et le cluster-head CH_i sont prêts à établir les clés de communication secrètes pour chaque cycle.

Après cette phase, tous les nœuds capteurs (membre ou cluster-head) établissent des clés de communication. Un aperçu du processus de cette phase est présenté à la figure 3.4.

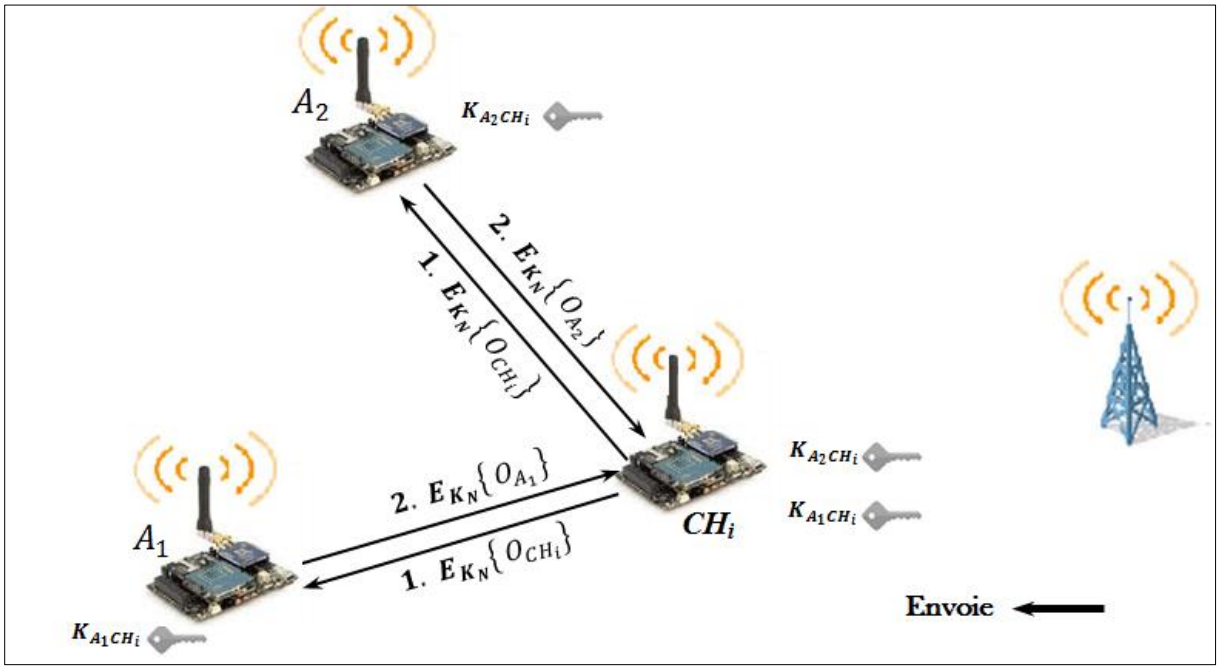


Figure 3.8 : Le processus de la phase d'état stable

3.5. Simulation

Comme beaucoup de technologies, le fonctionnement d'un réseau de capteurs sans fil peut être reproduit de façon virtuelle via un simulateur numérique. Ainsi, on peut prévoir le résultat de fonctionnement de notre système.

3.5.1. Présentation de l'environnement TinyOS

L'environnement TinyOS est conçu pour prendre en charge le développement et la simulation d'applications de RCSF. Il comprend le système d'exploitation TinyOS, le simulateur TOSSIM, l'émulateur Cygwin et d'autres outils de simulation.

3.5.1.1. Tinyos

TinyOS est basé sur des propriétés qui font que ce système d'exploitation, s'adapte particulièrement bien aux systèmes à faible ressources [25]:

- **Disponibilité et sources:** TinyOS est un système principalement développé et soutenu par l'université américaine de Berkeley, qui le propose en téléchargement sous la licence BSD et en assure le suivi. Ainsi, l'ensemble des sources sont disponibles pour de nombreuses cibles matérielles.
- **Event-driven :** Le fonctionnement d'un système basé sur TinyOS s'appuie sur la gestion des évènements se produisant. Ainsi, l'activation de tâches, leur interruption ou encore la mise en veille du capteur s'effectue à l'apparition d'évènements, ceux-ci ayant la plus forte priorité.Ce fonctionnement évènementiel (event-driven) s'oppose au fonctionnement dit temporel (time-driven) où les actions du système sont gérées par une horloge donnée.

- **Non préemptif:** Le caractère préemptif d'un système d'exploitation précise si celui-ci permet l'interruption d'une tâche en cours. TinyOS ne gère pas ce mécanisme de préemption entre les tâches, mais donne la priorité aux interruptions matérielles. Ainsi, les tâches entre elles ne s'interrompent pas mais une interruption peut stopper l'exécution d'une tâche.
- **Pas de temps réel:** Lorsqu'un système est dit « temps réel » celui ci gère des niveaux de priorité dans ses tâches, permettant de respecter des échéances données par son environnement. Dans le cas d'un système strict, aucune échéance ne tolère de

dépassement contrairement à un système temps réel. TinyOS se situe au-delà de ce second type, car il n'est pas prévu pour avoir un fonctionnement temps réel.

- **Consommation d'énergie :** TinyOS a été conçu pour réduire au maximum la consommation en énergie du capteur. Ainsi, lorsqu'aucune tâche n'est pas active, il se met automatiquement en veille.
- **Langage:** TinyOS a été programmé en langage NesC qui est un langage conçus pour incarner les concepts structurant et le modèled'exécution de TinyOS. C'est une extension du langage C orientée composant, ilsupport alors la syntaxe du langage C et il est compilé vers le langage C avant sacompilation en binaire.

3.5.1.2. Le simulateur TOSSIM

TOSSIM permet de simuler le comportement d'un capteur au sein d'un réseau de capteurs, il est un simulateur discret basé sur la programmation par événement, de même qu'il est conçu et désigné pour simuler les réseaux de capteurs qui utilisent la plateforme TinyOS. Le principal but de TOSSIM est de créer une simulation très proche de ce qui ce passe dans ces réseaux dans le monde réel. TOSSIM simule le comportement des applications de TinyOS à un niveau très bas. Le réseau est simulé au niveau des bits et chaque interruption dans le système est capturée. TOSSIM fourni deux modèles de radios pour la communication : Le modèle par défaut « simple » où les paquets sont transmis dans le réseau sans aucune erreur et ils sont reçus par chaque nœud. Avec ce modèle il est ainsi possible que deux nœuds différents peuvent envoyer un paquet en même temps avec la conséquence que ces deux paquets seront alors détruit à cause du chevauchement des signaux. Le deuxième modèle est le modèle « lossy », dans ce modèle les nœuds sont placés dans un graphe direct formé d'un couple (a, b) ce qui signifie qu'un paquet envoyé par le nœud a peut-être été reçu par le nœud b. TOSSIM est équipé aussi d'un simulateur graphique TinyViz. Cette application est équipée par plusieurs API plugins qui permet d'ajouter plusieurs fonctions à notre simulateur comme par exemple contrôler les entrées de notre radio ou bien suivre la dépense d'énergie en utilisant un autre simulateur qui s'appelle PowerTOSSIM[26].

3.5.1.3. Emulateur Cygwin

L'émulateur Cygwin est utilisé pour exécuter TinyOS et TOSSIM sur des systèmes d'exploitation Windows. Il fournit une couche de compatibilité UNIX pour exécuter des outils basés sur Linux sur des machines Windows.

3.5.2. Environnement de simulateur et résultats

Afin d'évaluer les performances de CFKM, nous avons implémenté en utilisant le langage de programmation NesC pour l'intégrer à TinyOS. Une série de simulations sont effectuées en utilisant l'environnement TOSSIM. En effet, l'ensemble de simulations est consacré à la comparaison de CFKM avec SC-SPK.

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

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

Tableau 3.2 : Les paramètres de simulation

3.5.2.1. Le coût de communication

En ce qui concerne SC-SPK, le coût de communication dépend linéairement du nombre d'index des clés partielles (m) et du nombre d'index dans la liste ordonnée (q) crée par le CH ou le CM. Chaque nœud membre envoie un message à son CH, reçoit $m \times x$ messages permettant d'échanger la liste d'index de clés du CH et reçoit $q \times x$ messages permettant d'échanger la liste d'ordres crée par son CH pour déterminer les clés communes entre eux. En réponse, chaque nœud membre envoie une liste d'ordres unique, qui doit envoyer $q \times x$ messages. Après chaque CH nœud reçoit la liste d'index des clés de la SB, il envoie environ $m \times x$ messages et environ $q \times x$ messages pour transmettre une liste d'ordres unique à chaque nœud membre. Il reçoit également les listes d'ordres de leurs nœuds membres. Ainsi, pour un cluster comprenant n nœuds membres, $n \times q \times x$ messages au total sont reçus.

Noter que le variable x est le rapport$taille_index/taille_paquet$(tel que,$taille_index$et $taille\_paquet$ representent le nombre de bits requis pour identifier chaque clé partielle et la taille(en bits) de données échangées dans le paquet respectivement).

De l'autre côté, dans CFKM, pour un réseau de N nœuds comportant C clusters de n membres, chaque CH après la réception de message d'initialisation, diffuse un message d'élection contient sa position (coordonnées (x, y)) et l'identification de sa cellule, reçoit $(n-1)$ messages des autres membres de la même cellule et $(C-1)$ messages des autres nœuds CH, puis diffuse un message contenant la liste d'identification de l'ensemble des nœuds membres. Chaque nœud CM reçoit également un message d'initialisation de la station de base, diffuse un message d'élection, puis reçoit $(n-1)$ messages des autres membres de la même cellule.

Comme la montre la figure 3.9, le coût de communication pour SC-SPK n'est pas affectée par l'évolution du nombre des nœuds et ceci pour CH et CM. Alors que dans CFKM, les nœuds CH nécessitent moins de coût de communication. Comparé au CH, le nœud CM nécessite moins de coût de communication et a une valeur fixe par rapport à N.

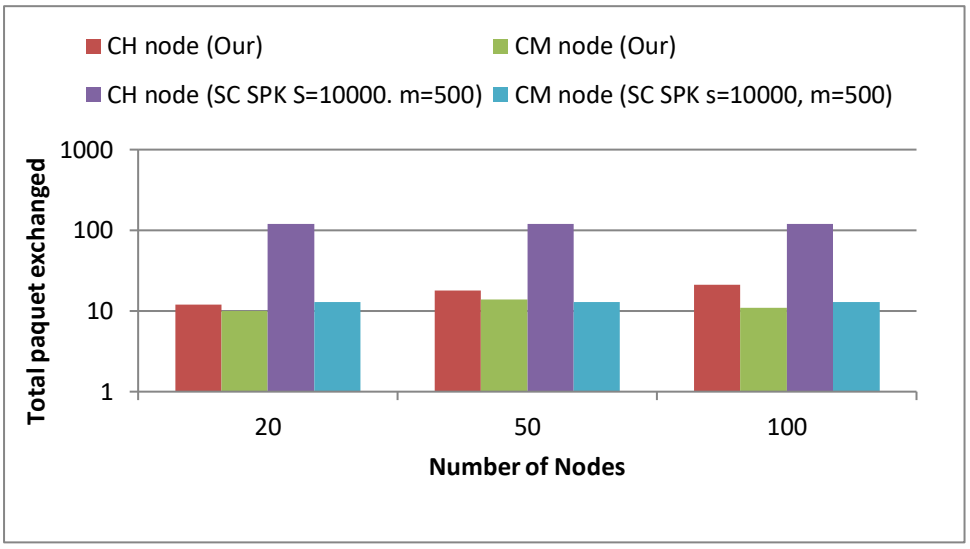


Figure 3.9. Comparaison du nombre de paquets échangés.

3.5.2.2. Le coût de stockage

La figure 3.10 illustre le totale de stockage requise par rapport à la taille du réseau. À partir de cette figure, on peut constater que SC-SPK utilisent plus de mémoire que CFKM. En effet, la mémoire de stockage requise par SC-SPK est principalement liée aux besoins du nœud capteur afin de stocker les m clés partielles (de 64 bits chacune), la liste d'index (de clés partielles), la clé de réseau (doit être de 128 bits de longueur), les deux listes index ordonnés de q clés partielles (la première est créé par le nœud membre et la seconde est envoyé par leur CH). En cas de CH, $2n$ listes ordonnée est stockée. Pour un pool de clés contenant S clés partielles, $log_2 S$ bits sont requis pour chaque index utilisé.

Pour CFKM, chaque nœud de capteur ne doit stocker que deux clés dans sa mémoire avant le déploiement. Après le déploiement, chaque nœud CH est pré-chargé avec $(C-1)$ clés partagées avec les autres nœuds CH et n clés partagées avec ses nœuds CM. Lorsque la taille du réseau augmente, l'espace mémoire total augmente linéairement pour le nœud CH. En effet, le nœud CM utilise moins de mémoire pour stocker les clés. Il suffit de stocker une seule clé (c à d la clé partagée avec le nœud CH).

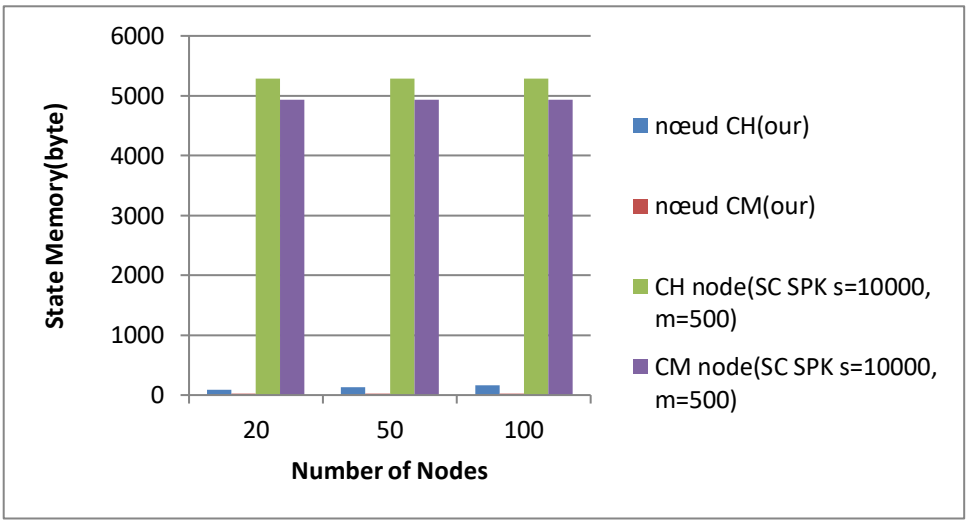


Figure 3.10 : L'utilisation de la mémoire par un nœud capteur

3.5.2.3. La consommation d'énergie

La consommation d'énergie est un paramètre important pour toutes les approches de gestion de clés dans les RCSFs. Par conséquent, nous avons utilisé le plugin PowerTOSSIM dans TinyViz pour analyser l'énergie. Cette énergie est calculée sur la base des instructions exécutées pour les opérations cryptographiques et pour les opérations radio (émission et réception des messages). La figure 3.11 montre la variation de l'énergie consommée par CFKM et SC-SPK en fonction de la taille de réseau.

Il est évident que l'énergie consommée par CFKM est négligeable par rapport à celle liée au SC-SPK. En effet, dans CFKM, le nœud CM (et le nœud CH) échange moins de paquets, et la taille des messages échangés pour la construction des clés par paires est plus petite que celle SC-SPK.

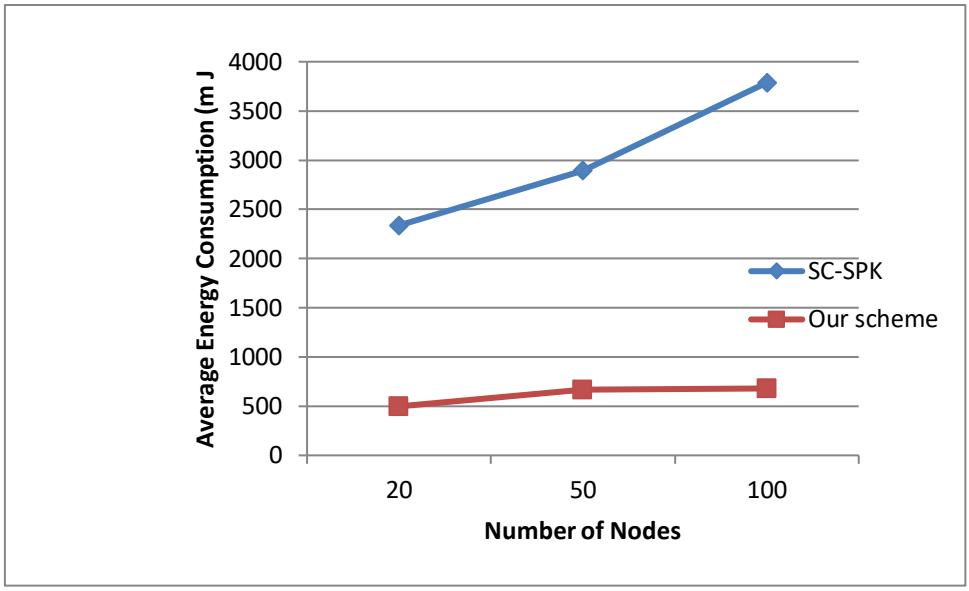


Figure 3.11 : La consommation d'énergie par un nœud capteur

3.6. Conclusion

Dans ce chapitre, nous avons proposé un schéma de gestion de clés pour les réseaux de capteurs sans fil hiérarchiques. Notre schéma proposée appelée CFKM (Cluster formation and Key management scheme for Wireless sensor Networks) permet d'assurer la formation des clusters et l'établissement des clés dans le réseau. Par comparaison avec le protocole SC-SPK, CFKM fournit non seulement un mécanisme de sécurité fiable, mais optimise également la consommation d'énergie et les coûts liés à la communication et à l'utilisation de la mémoire. Nous avons validé notre proposition en fournissant une étude expérimentale, ce qui permet une analyse approfondie de notre schéma.

Conclusion générale

Les réseaux de capteurs sans fil sont une nouvelle technologie qui a surgi après les grands progrès technologiques concernant le développement des capteurs, des processeurs puissants et des protocoles de communication sans fil. Ce type de réseau composé de certains ou de milliers d'éléments a pour but la collecte de données de l'environnement, leurs traitements et leurs disséminations vers le monde extérieur. En effet, les applications des réseaux de capteurs sont de plus en plus nombreuses et diversifiées, notamment la gestion du trafic urbain, la surveillance des sites sensibles et l'étude de l'environnement naturel.

Cependant, ces applications sont souvent déployées dans des environnements hostiles, où les nœuds et la communication sont des cibles attrayantes pour les attaquants. De plus, vu les contraintes de miniaturisation, les nœuds de capteurs sont dotés de ressources limitées en terme de calcul, d'espace de stockage et d'énergie. Par conséquent, les ressources limitées de ces nœuds et les environnements hostiles dans lesquels ils pourraient être déployés, rendent ce type de réseaux très vulnérables à plusieurs types d'attaques.

Par conséquent, il est nécessaire d'utiliser des mécanismes efficaces pour protéger ce type de réseau. Toutefois il est bien connu, que la gestion de clés constitue la pierre angulaire des autres mécanismes de sécurité, qui s'appuient en général sur le cryptage.

Dans ce travail, notre objectif a été de proposer une solution efficace au problème de la gestion de clés dans les réseaux de capteurs sans fil. Pour cela, après avoir étudié profondément les schémas existants et montré leurs limites, nous avons constaté que le défi dans la conception des schémas de gestion de clés est de trouver un compromis entre un système efficace et les contraintes caractérisant les RCSFs.

Dans le cadre de ce mémoire, nous avons proposé un protocole de gestion de clés nommé CFKM (Cluster formation and Key management scheme for Wireless sensor Networks). Notre proposition permet d'assurer la formation des clusters et l'établissement des clés dans le réseau. Par rapport aux schémas existants, CFKMoptimise la consommation d'énergie et les coûts liés à la communication et à l'utilisation de la mémoire.

Les performances de ce protocole ont été évaluées en fournissant une étude expérimentale, ce qui permet une analyse approfondie de ce protocole. En ce qui concerne les résultats de simulation obtenus sur la consommation d'énergie, le coût de communication et le coût de stockage,

nous avons constaté que le protocole CFKM répond bien aux critères de performances souhaités du réseau, tout en maintenant un niveau de sécurité très élevé.

- **Perspectives**

Concevoir un protocole efficace de gestion de clés demeure encore un domaine de recherche ouvert. Il serait donc plausible, comme perspective de notre travail, d'adapter notre proposition à une mobilité des nœuds, et le comparé à d'autres protocoles proposés dans la littérature pour montrer son efficacité.

Bibliographies

[01] L. KHELLADI & N. BADACHE, Les réseaux de capteurs : état de l'art, rapport de recherche, Université de Bab Ezzouar, 2004.

[02] Mohamed BENAZZOUZ , Magistère IRM 2013, Ecole nationale supérieure d'informatique Oued-Smar Alger Algérie.

[03] DOUMI Abdelmoumin, La Sécurité des Communications dans les Réseaux de Capteurs sans Fils, Université MOHAMED BOUDIAF - M'SILA.

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

[05] Techno-Science.net, 29/05/2023.

[06] Iottechtrends.com

[07] HAMED KHODJA Nesrine & TEKFA Kenza, Magistère, Mise en place d'une solution pour la détection des frontières dans les RCSF, Université de Bejaia, 2020.

[08] Mekki nabil & Mohammedi kada, Magistère, Techniques de conservation d'énergie pour les réseaux de capteur sans fil, Université de Saida, 2018.

[09] KHALILI Zeyneb & BOUCHRA Meryem, Magistère, Une technique d'optimisation de la consommation d'énergie dans les réseaux de capteurs sans fil, Université de Adrar, 2019.

[10] BOUCHENEB Sonia & NAFI Mohammed, Magistère, Gestion de clés basée sur des clusters dans les réseaux de capteurs sans fil, Université de Begaia, 2016.

[11] BOUKHIAR Amine, Magistère, La tolérance aux pannes dans les réseaux de capteurs sans fil, Université de Bejaia, 2016.

[12] http://www.univbejaia.dz/xmlui/bitstream/handle/123456789/1571/Gestion%20de%20cl%C3%A9s%20bas%C3%A9e%20sur%20des%20clusters.pdf?sequence=1&isAllowed=y visite le 02/05/2023.

[13] GHERBI Chirihane, Doctorat, Algorithme de routage pour les réseaux de capteurs

avec prise en charge de la consommation d'énergie, Université de OUM EL BOUAGHI, 2017.

[14] BOUNAR Seyyid-Ali & KRIKET Farhat, Magistère, Etude du clustering dans les réseaux de capteurs sans fil, Université de Jijle, 2016.

[15] http://www.univ-bejaia.dz/xmlui/bitstream/handle/123456789/1571/Gestion%20de%20cl%C3%A9s%20bas%C3%A9e%20sur%20des%20clusters.pdf?sequence=1&isAllowed=y visite le 13/04/2023.

[16] Nakas, C., Kandris, D. & Visvardis, G. (2020) *Energy Efficient Routing in wireless sensor networks: A comprehensive survey*, *MDPI*.

[17] THMANI Samir, Doctorat, Protocoles pour la Sécurité des Réseaux de Capteurs Sans Fil, Université de Batna2, 2018.

[18] BENSAFI Zineb, Magistère, Contrôle d'accés basé sur les courbes elliptiques pour la sécurité dans les réseaux de capteurs, Université de Tlemcen, 2012.

[19] MESSAI Mohamed Lamine, Magistère, Sécurité dans les Réseaux de Capteurs Sans fil, Université de Bejaia, 2008.

[20] ATHMANI Samir, Magistère, Protocole de sécurité Pour les Réseaux de capteurs Sans Fil, Université de Batna, 2010.

[21] LASLA Noureddine, La gestion de clés dans les réseaux de capteur sans fil, Université d'Alger, 2007.

[22] Challal, Y. (no date a) Le routage dans les RCSF : Menaces et solutions, Réseaux de Capteurs Sans Fils - Le routage dans les RCSF : menaces et solutions.

[23] TLILI Lynda, Magistère, Modelle de confiance pour sécuriser le routage dans les réseaux de capteurs sans fil, Université de Tizi-Ouzou, 2011.

[24] ANGE Anastasie & KEUMBOUK Donfack, Magistère, Une approche de protocole de géocasting sécurisé sans un réseau de capteurs sans fil déployés dans l'espace, Université de DACHANG.

[25] Mohammed & MEKIDICHE Hichem, Magistère, La géolocalisation de réseaux capteurs (algorithme DVHOP).

[26] BOUZIDI Zineb & BENAMEUR Amina, Magistère, Mise en place d'un réseau de capteurs sans fil pour l'irrigation intelligente, Université de Tlemcen, 2012.

Résumé

Les réseaux de capteurs sans fil (RCSF) ont attiré beaucoup d'attention en raison de leurs vastes applications dans les domaines militaires et civils. Cependant, les contraintes énergétiques et de mémoire et l'environnement hostile dont lesquels ils peuvent être déployés, rendent ce type de capteurs vulnérables aux attaques. De ce fait, la protection de ce type de réseau en utilisant des solutions de sécurité adaptées aux capteurs est un chalenge qui va être traité. Cette sécurité est généralement garantie par le cryptage des données transmises, ce qui nécessite l'établissement de nombreuses clés cryptographiques. La gestion de clés est la première fonction fondamentale puisque les nœuds ont besoin d'une clé commune valide pour exploiter les mécanismes de cryptographie.
Dans ce projet de fin d'étude, nous proposons CFKM, un protocole de gestion de clés pour les réseaux de capteurs sans fil hiérarchiques. Notre proposition permet d'assurer la formation des clusters et l'établissement des clés dans le réseau. Ainsi, CFKM ne fournit pas seulement des mécanismes de sécurité fiables, il optimise également la consommation d'énergie et les surcoûts liés à la communication et à l'utilisation de la mémoire. Les résultats présentés dans ce mémoire sont issus de plusieurs simulations, qui démontrer la faisabilité et l'efficacité de notre proposition.

Mots clés : Réseau de capteurs sans fil, la sécurité, la gestion de clés, la cryptographie, le clustering.

Abstract:

Wireless sensor networks (WSNs) have attracted much attention due to their wide applications in military and civil fields. However, the energy and memory constraints and the hostile environment in which they can be deployed make this type of sensor vulnerable to attacks. Therefore, protecting this type of network using security solutions adapted to sensors is a challenge that will be addressed. This security is generally guaranteed by the encryption of the transmitted data, which requires the establishment of numerous cryptographic keys. Key management is the first fundamental function since nodes need a valid common key to operate cryptographic mechanisms.
In this final project, we propose CFKM, a key management protocol for hierarchical wireless sensor networks. Our proposal ensures the formation of clusters and the establishment of keys in the network. Thus, CFKM not only provides reliable security mechanisms, it also optimizes energy consumption and overheads related to communication and memory usage. The results presented in this dissertation come from several simulations, which demonstrate the feasibility and effectiveness of our proposal.

Keywords: Wireless sensor network, security, key management, cryptography, clustering.

ملخص

جذبتشبكاتالاستشعاراللاسلكية(WSN) الكثيرمنالاهتمامبسببتطبيقاتهاالواسعةفيالمجالاتالعسكريةوالمدنية.
ومعذلك،فإنالقيودالمفروضةعلىالطاقةوالذاكرةوالبيئةالمعاديةالتييمكننشرهافيهاتجعلهذاالنوعمنأجهزةالاستشعارعرضةللهجمات.
ولذلك،فإنحمايةهذاالنوعمنالشبكاتباستخداماتالحلولالأمنيةالمتكيفةمعأجهزةالاستشعاريمثلتحديًاسيتمالتصديله.
يتمضمانهذاالأمانبشكلعاممنخلالتشفيرالبياناتالمرسلة،الأمرالذييتطلبإنشاءالعديدمنمفاتيحالتشفير.
تعدإدارةالمفاتيحأولوظيفةأساسيةنظرًالأنالعقدتحتاجإلىمفتاحمشتركصالحلتشغيلآلياتالتشفير.
فيهذاالمشروعالنهائي،نقترحCFKM،وهوبروتوكولإدارةالمفاتيح لشبكاتالاستشعارالاسلكيةالهرمية.
يضمناقتراحناتكوينمجموعاتوإنشاءمفاتيحفيالشبكة.
وبالتالي،لايوفرCFKMآلياتأمنيةموثوقةفحسب،بليعملأيضًاعلىتحسيناستهلاكالطاقةوالنفقاتالعامةالمتعلقةبالاتصالاتواستخداماتالذاكرة.
النتائجالمقدمةفيهذهالأطروحةتأتيمنعدةعملياتمحاكاة،والتيتوضحجدوىوفعاليةاقتراحنا.

الكلماتالمفتاحية: شبكةالاستشعارالاسلكية،الأمن،إدارةالمفاتيح،التشفير،التجميع