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 : Saoual Hadia & Bedrane Kaouther

DOMAINE : Science et Technologie

FILIERE : Télécommunication

OPTION : Systèmes de télécommunications

Thème

Implémentation d'un protocole de sécurité dans les réseaux de capteurs sans fil (RCSF)

Jury de soutenance :

Nom et Prénom	Grade	Qualité
MESMOUDI Samira	MCB	Encadreur
BIRANE Mouhoub	MCA	Président
RAMDANI Saadi	MCB	Examinateur

Promotion : 2021/2022

Remerciement

Tout d'abord, je tiens à remercier dieu de m'avoir donné la santé, la volonté, le courage, et la patience pour réaliser ce travail.

Mes remerciements vont à Dr mesmoudi samira mon encadreur qui a guidé de ses précieux conseils et suggestions, et la confiance qu'il m'a témoigné et tout au long de ce travail.

Je tiens à gratifier aussi les membres de jury pour l'intérêt qu'ils ont porté à moi en acceptant d'examiner notre travail.

Nous adressons nos sincères sentiments de gratitude et de reconnaissance également à toutes nos professeurs, et les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

Dédicace

Je présente ce travail:

À mon adorable père et à ma chère maman,

Pour ce soutien moral et leurs conseils précieux tout au long de mes études.

A mes frères "Ali" et "Younes" et mes sœurs "Lamia" et "Zahra",

Pour leurs aides et supports dans les moments difficiles.

A ma chère binôme et sœur "Saoual Hadia",

Qui m'ont aidée et soutenue dans les moments difficiles et la préparation de ce travail.

Je remercie spécialement mon professeur "Adda Kritsa",

Qui m'a donné les bases des mathématiques.

Tous mes collègues et tous mes amis.

"Bedrane kaouther"

Dédicace

Un grand merci à l'ensembles de ma familles, mes collègues, mes amis pour leur amour, leur confiance, leurs conseils ainsi que leur soutien…

Je dédie ce travail A ma maman qui m'a soutenu et encouragé durant ces années d'études. Qu'elle trouve ici le témoignage de ma profonde reconnaissance. A mes frères "Med el amine", "Abdelatif" et ma chère soeur "Insaf" Ceux qui ont partagé avec moi tous les moments d'émotion lors de la réalisation de ce travail.

A ma adorable binome que je considère comme ma deuxième soeur "Kaouthar bedrane", qui m'a soutenu dans la préparation de ce travail.

Hadia saoual

Résumé

Les progrès technologique réalisées ces dernières années dans les réseaux sans fil ont conduit au développement d'une nouvelle génération de réseaux ad hoc, appelés réseaux de capteurs sans fil (RCSF), constitués de nœuds capteurs déployés en grand nombre dans une zone géographique en vue de collecter et transmettre des données environnementales. La spécificité de ce type de réseaux sans fil est sa limitation en ressources (énergie, mémoire et traitement), ajoutant à cela la communication sans fil et leur déploiement dans des environnements hostiles, ce qui rend ce type de réseau vulnérable à différent type d'attaques. De ce fait, le besoin de sécuriser les communications représente l'un des défis les plus importants dans les réseaux de capteurs sans fil. Cette sécurité est généralement assurée 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 le cadre de ce projet de fin d'études et après avoir abordé quelques protocoles et solutions de gestion de clés proposés pour les RCSFs, nous avons choisi l'approche SKWN pour l'implémenter et vérifier ses métriques de performances. Cette dernière surpasse les protocoles de gestion de clés dans le sens où elle optimise le coût de communication, l'espace de stockage et la consommation d'énergie.

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

Abstract:

The technological progress made in recent years in wireless networks has led to the development of a new generation of ad hoc networks, called wireless sensor networks (WSN), that consist of sensor nodes deployed in large numbers in a geographical area in view to collect and transmit environmental data. The specificity of this type of wireless networks is its limitation regarding resources (energy, memory and processing), adding to this the wireless communication and their deployment in hostile environments, which makes this type of network vulnerable to different types of attacks. Therefore, the need for secure communications represents one of the most important challenges in wireless sensor networks. This security is generally ensured by the encryption of the data transmitted, which requires the establishment of numerous cryptographic keys. Key management is the first fundamental function since the nodes need a valid common key to exploit the cryptography mechanisms. As part of this end-of-studies project and after having discussed some proposed key management protocols and solutions for RCSFs, we chose the SKWN approach to implement it and verify its performance metrics. The latter outperforms key management protocols in that it optimizes communication cost, storage space and power consumption.

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

ملخص

أدى التقدم التكنولوجي الذي تم إحرازه في السنوات الأخيرة في الشبكات اللاسلكية إلى تطوير جيل جديد من شبكات ad hoc ، تسمى شبكات الاستشعار اللاسلكية (RCSF) ، والتي تتكون من عقد استشعار منتشرة بأعداد كبيرة في منطقة جغرافية تقوم بنقل البيانات البيئية. خصوصية هذا النوع من الشبكات اللاسلكية هي محدودية الموارد (الطاقة والذاكرة والمعالجة) ، إضافة إلى ذلك الاتصال اللاسلكي ونشرها في بيئات معادية ، مما يجعل هذا النوع من الشبكات عرضة لأنواع مختلفة من الهجمات. لذلك ، تمثل الحاجة إلى الاتصالات الآمنة أحد أهم التحديات في شبكات الاستشعار اللاسلكية. يتم ضمان هذا الأمان بشكل عام عن طريق تشفير البيانات المرسلة ، الأمر الذي يتطلب إنشاء العديد من مفاتيح التشفير. إدارة المفاتيح هي الوظيفة الأساسية الأولى لأن العقد تحتاج إلى مفتاح مشترك صالحة لاستغلال آليات التشفير. كجزء من مشروع نهاية الدراسات هذا وبعد مناقشة بعض بروتوكولات وحلول الإدارة الرئيسية المقترحة لـ RCSF, اخترنا نهج SKWN لتنفيذه والتحقق من مقاييس أدائه. يتفوق الأخير على بروتوكولات الإدارة الرئيسية من حيث أنه يحسن تكلفة الاتصال ومساحة التخزين واستهلاك الطاقة.

الكلمات المفتاحية: شبكات الاستشعار اللاسلكية ، الأمن ، إدارة المفاتيح ، التشفير.

Table des matières

Chapitre2: Sécurité des communications dans les réseaux de Capteurs sans fil

Liste des figures

Liste des tableaux

Introduction générale

Les progrès réalisés ces dernières décennies dans les domaines de la microélectronique, de la micromécanique, et des technologies de communication sans fil, ont permis de produire avec un coût raisonnable des composants de quelques millimètres cubes de volume. Ces derniers, appelés micro-capteurs, intègrent : une unité de captage chargée de capter des grandeurs physiques (chaleur, humidité, vibrations) et de les transformer en grandeurs numériques, une unité de traitement informatique et de stockage de données et un module de transmission sans fil.

De ce fait, les micro-capteurs sont de véritables systèmes embarqués. Le déploiement de plusieurs d'entre eux, en vue de collecter et transmettre des données environnementales vers un ou plusieurs points de collecte, d'une manière autonome, forme un réseau de capteurs sans fil. Selon le magazine Technology Review du MIT, il s'agit de l'une des dix nouvelles technologies qui bouleverseront le monde et notre manière de vivre et de travailler.

Ce type de réseau est largement utilisé, et fait l'objet de plusieurs recherches scientifiques. Il constitue une solution efficace dans une grande variété d'applications comme les applications militaires, environnementales, domotiques, industrielles, etc.

Les nœuds capteurs sont généralement déployés dans des zones non surveillées, la plupart des applications des RCSFs nécessitent un haut niveau de sécurité pour fournir les exigences de sécurité de base et rendre ces applications invulnérables aux différentes attaques, empêchant un intrus de perturber le bien 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 relativement facilement intrus d'espionner, d'altérer ou d'injecter des données dans le réseau.

Il est nécessaire donc d'intégrer un mécanisme de sécurité qui non seulement gère les intrusions, mais garantit également un échange de données sécurisé. Cependant, assurer la sécurité des échanges des données au sein des RCSFs est une tâche importante et en même temps difficile. En effet, 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.

Parmi ces solutions adéquates l'emploi des primitives cryptographiques notamment la cryptographie à clé secrètes (symétrique). Le principe de la cryptographie symétrique repose sur le partage d'une clé commune entre chaque paire de nœuds désirant communiquer.

En effet, pour atteindre les objectifs de sécurité, la gestion de clés est la première fonction fondamentale puisque les nœuds capteurs ont besoin d'une clé commune valide pour exploiter les primitives cryptographiques.

Généralement, la gestion de clés permet de pré-distribuer des clés cryptographiques, de révoquer les clés si les nœuds quittent le réseau, de renouveler des clés expirées, et d'assigner des nouvelles clés en cas d'une nouvelle intégration de nœud.

Dans le cadre de notre étude et après avoir abordé certains protocoles et solutions de gestion de clés proposés pour les RCSFs, nous nous sommes intéressés par le travail [1] intitulé "SKWN : Smart and dynamic Key management scheme for hierarchical Wireless sensor Networks". Dans ce travail les auteurs ont développé une approche de gestion de clés dont l'objectif est de surpasser les limites des protocoles existants.

Nous avons choisi cette approche pour l'implémenter et vérifier leurs métriques de performances telles que le coût de stockage, le coût de communication, et la consommation d'énergie.

Organisation de mémoire

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

- Le premier chapitre présente une description générale sur le fonctionnement des réseaux de capteurs sans fil, leur application ainsi que les différentes topologies et organisations utilisées dans ce genre de réseau. Par la suite, nous avons décrit quelques défis et contraintes liés à la conception des RCSF.
- Le deuxième chapitre comprend l'aspect de sécurité : les objectifs de la sécurité, les principaux concepts cryptographiques, les attaques et contremesures. Il décrit aussi quelques méthode et protocoles concernant la gestion de clés existants dans la littérature.
- Dans le dernier chapitre; nous donnons une étude détaillée sur l'approche implémentée. Nous présentons par la suite les outils nécessaires pour faire la simulation à savoir le système d'exploitation TinyOs, le langage NesC et le simulateur TOSSIM, suivi de la présentation des résultats de simulation et l'évaluation des performances.

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

Chapitre 1

Concepts généraux sur les réseaux de capteurs sans fil

1.1. Introduction

Les récents progrès et les nombreuses avancées technologiques dans les domaines de la micro-électronique et les progrès atteints dans les domaines d'intégration et de la miniaturisation ont permis la fabrication d'entités miniaturisées, communément appelées capteurs, faibles en coût et de plus en plus performantes, capables de se disposer dans l'environnement de manière aisée sans altération du paysage ambiant. Également, les progrès des technologies de communication sans fil a permis aux capteurs d'être plus autonomes ce qui favorise un déploiement facile et rapide dans des endroits difficile d'accès ou complètement inaccessibles. Sur un champ de captage, les capteurs coopèrent entre eux sans aucune intervention externe (humaine, infrastructure de base…etc.) pour former une infrastructure de communication dite réseau de capteurs sans fil.

Un réseau de capteurs sans fil est composé de plusieurs milliers de capteurs communicants via des liaisons sans fil placés dans des endroits précis ou dispersés aléatoirement sur une zone à surveiller, capables de collecter, traiter et s'auto-organiser afin de transmettre des informations sur leur environnement.

Dans ce chapitre nous présenterons les réseaux de capteurs sans fil, leurs architectures, leurs caractéristiques, leurs domaines d'application ainsi que leurs propres contraintes imposées.

1.2. Nœud de capteur sans fil

1.2.1. Qu'est-ce qu'un capteur?

C'est un composant électronique autonome à faible coût, capable d'effectuer des mesures simples sur son environnement immédiat servant á la surveillance et au contrôle d'un phénomène donné. Ces petites entités électroniques, constituent les briques de base des réseaux de capteurs, dont l'objectif est de récolter des grandeurs physiques de leur environnement proche (luminosité, mouvement, température, pression barométrique, etc.), et éventuellement de les traiter et de les communiquer à leurs voisins ou vers un ou plusieurs points de collecte appelés station de base (SB). [2]

1.2.2. Architecture interne d'un capteur sans fil

Un nœud capteur est composé de quatre unités principales, qui sont présentées dans la (figure 1.2)

- **Unité d'acquisition :** Elle est généralement composée de deux sous-unités : les capteurs et les convertisseurs analogique numérique ("ADC : Analog Digital Converter" en Anglais). Les capteurs permettent d'obtenir des mesures numériques sur les paramètres environnementaux et les transforment en signaux analogiques que les ADC convertissent à leur tour en signaux numériques.
- **Unité de traitement (processeur) :** Cette unité est composée de deux interfaces qui sont l'interface avec l'unité d'acquisition et une autre avec l'unité de communication. Son rôle est de contrôler l'ensemble des procédures permettant à un nœud capteur de collaborer avec les autres nœuds dans le but de réaliser les tâches d'acquisition et de stockage des données collectées.
- **Unité de communication :** L'unité de communication ("Transceiver" en Anglais) est composée d'un émetteur/récepteur qui permet aux nœuds capteurs du réseau de pouvoir communiquer entre eux par l'intermédiaire de liaisons radio.
- **Batterie :** Elle permet d'alimenter les différentes unités énumérées du nœud capteur décrites ci-dessus.

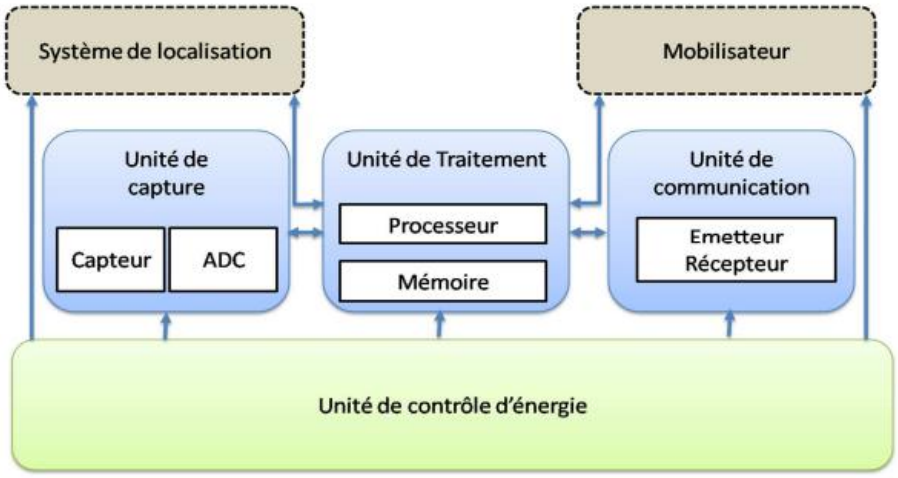

Figure 1.1 : Architecture interne d'un capteur sans fil. [3]

1.2.3. Caractéristiques principales d'un capteur:

En analysant la gamme des composants disponibles sur le marché et les prototypes présents dans la littérature, il est évident que la principale caractéristique d'un nœud capteur sans fil est sa petite taille. Une deuxième caractéristique, évidente mais essentielle est l'autonomie (pas seulement d'énergie élevée au point de vue de leur source évidente, mais aussi de leur fonctionnement).

Ces deux premières particularités induisent plusieurs autres caractéristiques à considérer, en particulier la vitesse de calcul et la vitesse de transmission. Des performances élevées en termes de vitesse de traitement et de transmission impliquent une consommation élevée.
De manière générale, il est souhaitable que la durée de vie de la batterie des nœuds soit la plus grande possible, donc les différentes unités qui composent un nœud sont généralement très limitées en termes de ressources et de performances pour que leur consommation d'énergie soit extrêmement faible [4].

1.2.4. Vue d'ensemble des plates-formes existantes

Il existe dans le monde plusieurs fabricants de capteurs. Nous citerons Cross Bow, Cisco, Data, Euro Therm, Shockfish SA, et Sens2B. Parmi ces capteurs, il existe quelques-uns qui sont capables de varier la puissance du signal émis afin d'élargir/réduire le rayon de communication et en conséquence la zone de communication.

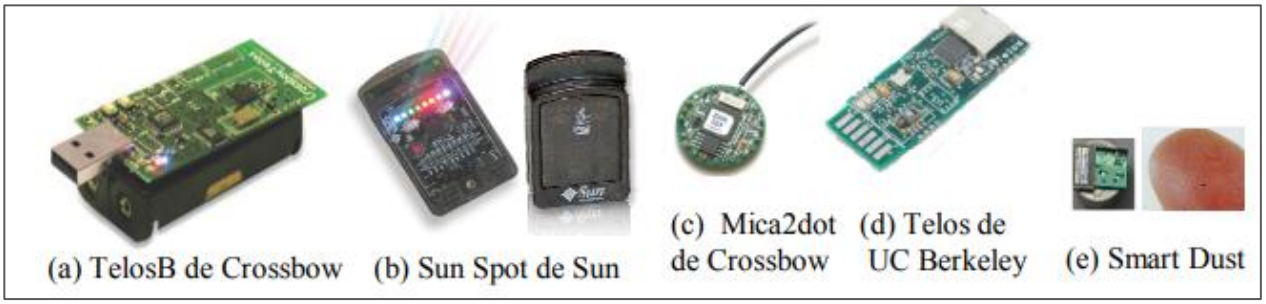

Figure 1.2 : Quelques modèles de capteurs sans fil.

Aujourd'hui, divers exemples de capteurs existent sur le marché (figure 1.3) dont les caractéristiques dépendent du type d'application. Nous citons : TmoteSky et WiSMote, MICAZ, TINYNODE, TELOSB, Le tableau 1-1 illustré les principales caractéristiques techniques de quelques capteurs.

Tableau 1-1 : Caractéristiques techniques des capteurs [6] [8]

Propriétés	TmoteSky	WiSMote	MICAZ	TelosB
Microcontrôleur	MSP430 F1611	TI MSP430F5437x	ATmega 128L	TI MSP430
Fréquence d'horloge	3.9 MHz	16 MHz	16 MHz	8 MHz
RAM (Ko)	10	16	4	10
ROM (Ko)	48	256	128	48
Radio	CC2420	CC2520	CC2420	CC2420
Batterie	2.1 - 3.6V	2.1 - 3.6V	2.7 - 3.3V	1.8 - 3.6 V

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 [5].

1.3.1. Architecture des réseaux de capteurs sans fil :

Un RCSF est composé d'un ensemble de nœuds capteurs. Ces nœuds capteurs sont organisés en champs « sensor fields ». Chacun de ces nœuds a la capacité de collecter des données et de les transférer au nœud passerelle (dit "sink" en anglais ou puits) par l'intermédiaire d'une architecture multi-sauts. Le puits transmet ensuite ces données par Internet ou par satellite à l'ordinateur central « Gestionnaire de taches » pour analyser ces donner et prendre des décisions. Cette architecture est illustrée dans la figure 1.3.

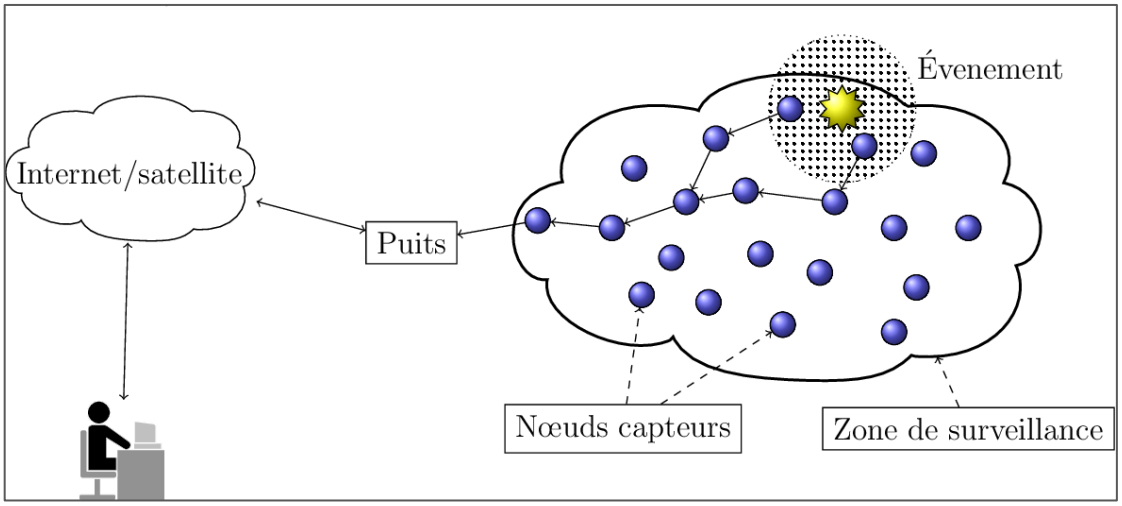

Figure 1.3 : Architecture de base d'un réseau de capteur sans fil [7]

Zone de surveillance (espace de collecte) : Il est considéré comme étant la zone d'intérêt pour le phénomène capté, là où les nœuds capteurs y sont placés.

Nœuds capteurs : Ce sont le cœur du réseau, leur rôle est de collecter les données et de les router vers la station de base. Leur énergie est souvent limitée puisqu'ils sont alimentés par une batterie.

Station de base (sink, puits) : C'est un nœud particulier chargé d'accueillir, stocker et traiter les données en provenance des autres nœuds et de diffuser les différentes requêtes sur le réseau. Sa source d'énergie est généralement illimitée puisqu'il faut qu'elle reste toujours active pour recevoir les données.

Utilisateur final (gestionnaire des tâches) : il reçoit les données collectées par la station de base. Son rôle consiste à les regrouper et les traiter pour en extraire les informations utiles[6].

1.3.2. La communication dans un RCSF :

Pour la communication dans un RCSF une pile protocolaire est utilisée. Le rôle de cette pile consiste à standardiser la communication entre les composants du réseau afin que différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles. Ce modèle comprend 5 couches qui ont les mêmes fonctions que celles du modèle OSI ainsi que 3 couches pour la gestion de la puissance d'énergie, la gestion de la mobilité ainsi que la gestion des tâches (interrogation du réseau de capteurs). Le but d'un système en couches est de séparer le problème en différentes parties (les couches) selon leur niveau d'abstraction. Chaque couche du modèle communique avec une couche adjacente (celle du dessus ou celle

du dessous). Chaque couche utilise ainsi les services des couches inférieures et en fournit à celle de niveau supérieur.

La pile protocolaire utilisée par la station de base ainsi que tous les autres capteurs du réseau est illustrée par la figure 1.4. Cette pile comprend :

- **La couche application:** Cette couche assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, géré directement par les logiciels.
- **La couche transport:** Elle est généralement présenter pour constituer une interface entre la couche application et la couche réseau. Cette couche est chargée du transport des données, de leur découpage en paquets, du contrôle de flux, de la conservation de l'ordre des paquets et de la gestion des éventuelles erreurs de transmission
- **La couche réseau:** Dans la couche réseau le but principal est de trouver une route et une transmission fiable des données. Elle est chargée de router les données fournis par la couche transport. Afin d'établir les routes entre les nœuds capteurs et le puits, différents protocoles de routage sont conçus pour sélectionner le meilleur chemin en terme d'énergie, de débit, de délai de transmission, etc. Parmi ces protocoles, nous citons: LEACH (Low-Energy Adaptive Clustering Hierarchy) et SAR (Sequential Assignement Routing).
- **La couche liaison:** Spécifie comment les données sont expédiées entre deux nœuds dans une distance d'un saut. Elle est responsable du multiplexage des données, du contrôle d'erreurs, de l'accès au media, … etc. Elle assure la liaison point à point et multi-point dans un réseau de communication. Cette couche assure la fiabilité de la communication en utilisant les techniques de contrôle d'erreur de transmission et aussi les méthodes de contrôle d'accès au médium (MAC).
- **La couche physique:** Elle est responsable de la sélection de la fréquence de modulation/démodulation, de la génération de la fréquence porteuse et du cryptage/ décryptage.

Due à la forte contrainte de limitation de ressource des RCSF, trois plans de gestion doivent être ajoutés afin de gérer la consommation d'énergie, la mobilité des nœuds et l'ordonnancement des tâches**.** Ces plans aident les nœuds capteurs à coordonner la tâche de captage et minimiser la consommation d'énergie. Ils sont donc nécessaires pour que les nœuds capteurs puissent collaborer ensemble, acheminer les données dans un réseau mobile et

partager les ressources entre eux en utilisant efficacement l'énergie disponible. Ainsi, le réseau peut prolonger sa durée de vie.

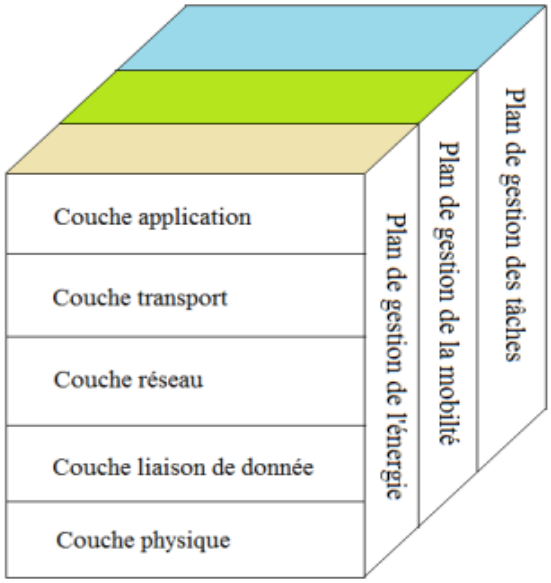

Figure 1.4 : Modèle en couches pour la communication dans les RCSF

1.3.3. Topologie et organisation de RCSF:

Les topologie dans les RCSF dépendent des applications et des techniques utilisées pour la transmission des données capturées par des différents nœuds capteurs vers la station de base. On distingue principalement deux types de topologies pour les RCSF qui sont les topologies plates et les topologies hiérarchiques.

- **Topologie plate:**

Dans les topologies plates, tout nœud capteur peut communiquer directement avec le centre de traitement en utilisant une forte puissance d'émission ou par l'intermédiaire d'un mode de communication multi-sauts en utilisant une puissance d'émission beaucoup plus faible. Dans le premier cas, la consommation énergétique du nœud pour l'envoi au centre de traitement est plus importante à cause de la puissance élevée utilisée; ainsi ces nœuds peuvent rapidement épuiser leur énergie avec ce mode de transmission. Dans le cas de la communication multi-sauts qui est le plus fréquent, un nœud capteur qui veut transmettre ses données à un autre nœud destinataire se trouvant hors de sa portée de transmission (par exemple la station de base), peut utiliser d'autres nœuds intermédiaires comme relais (routeurs). Ce mode offre comme principaux avantages la possibilité de passage à l'échelle, la gestion des redondances et des tolérances aux pannes. Cependant, on peut noter comme inconvénients une

consommation d'énergie plus importante dans l'ensemble du réseau. La figure 1.5 illustre un exemple de RCSF fonctionnant selon un mode d'architecture plate.[8]

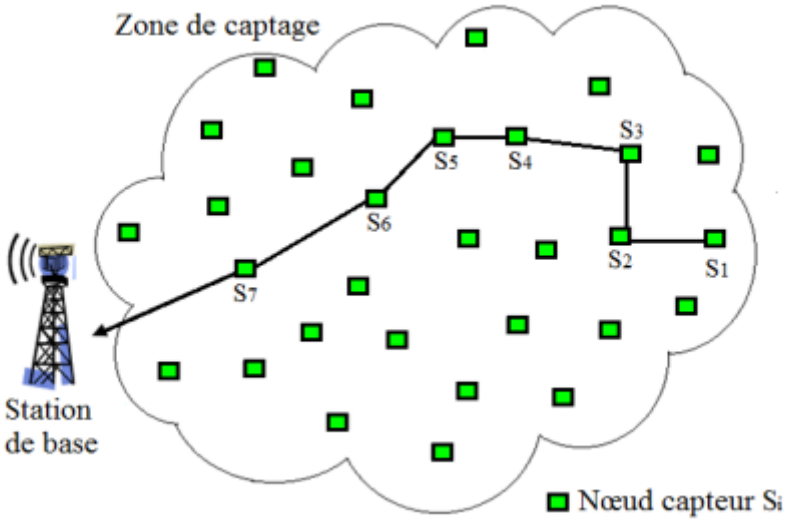

Figure 1.5: Exemple d'un RCSF fonctionnant selon un mode d'architecture à plat

- **Topologie hiérarchique:**

Dans les topologies hiérarchiques, le réseau est partitionné en clusters. Dans chaque cluster, un nœud appelé "CH: Cluster Head" est élu et ce dernier représente tous les nœuds membres de son cluster. Ainsi, tout nœud capteur doit être soit CH, soit membre d'un cluster. Un nœud qui n'est pas CH ne peut pas envoyer directement ses données capturées à la station de base. Il les envoie ainsi à son CH qui à son tour peut envoyer ces données à la station de base. Les CH peuvent également agréger des données reçues de plusieurs sources différentes avant de les envoyer à la station de base, allégeant ainsi cette dernière de certaines tâches de traitements, et diminuant aussi le trafic dans le réseau.

Les avantages de ce mode hiérarchique sont la simplicité, la faible consommation énergétique surtout pour les nœuds capteurs non CH et une latence plus faible entre les CH et la station de base, puisqu'ils envoient directement les données à cette dernière. L'inconvénient majeur est que chaque CH constitue un point de défaillance unique. En plus, ce mode nécessite beaucoup de messages de signalisations pour l'élection et la maintenance des CH. Nous pouvons également noter comme inconvénient, des problèmes de passage à l'échelle. La figure 1.6 illustre un RCSF fonctionnant selon l'architecture hiérarchique en clusters.

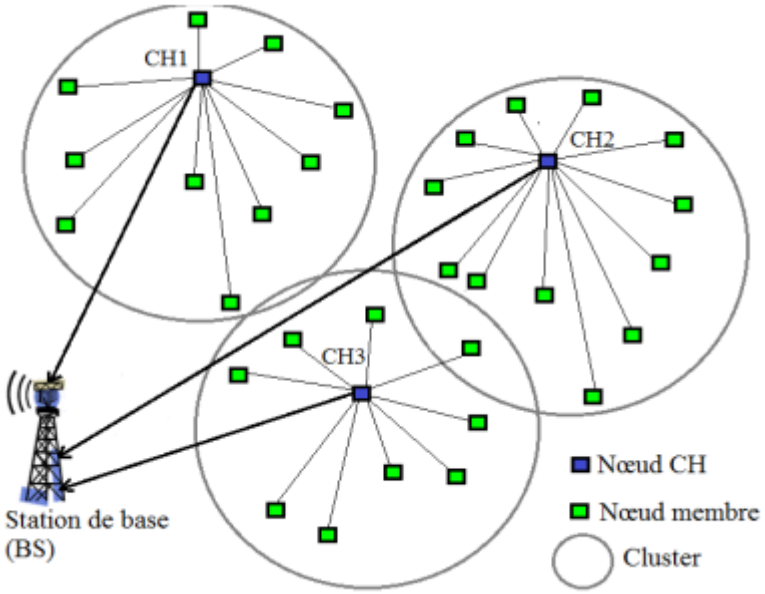

Figure 1.6: Exemple d'un RCSF fonctionnant selon une architecture hiérarchique en clusters.

1.4. Caractéristiques des RCSFs:

Les RCSFs présentent des caractéristiques propres au niveau des capteurs du réseau comme par exemple: l'énergie, la portée de transmission, ainsi que de la puissance de stockage et au niveau du réseau qui est formé par ces nœuds comme par exemple la bande passante, le déploiement sur une surface précise, et la topologie du réseau.

Parmi les caractéristiques les plus importantes d'un réseau de capteurs, nous citons

1.4.1. L'énergie:

L'énergie est considérée comme la principale et fondamentale contrainte dans les réseaux de capteurs sans fil. Chaque nœud fonctionne grâce à une batterie ayant une capacité limitée dû à sa petite taille mais également non rechargeable. L'utilisation de ces capteurs se fera dans la plupart des cas, dans des environnements hostiles ou difficiles d'accès, ce qui ne permettra pas la récupération de celles-ci. Nous pouvons donc dire que toute utilisation de la technologie du réseau de capteur sans fil doit prendre en compte principalement de la problématique « consommation énergétique ».

1.4.2. La portée de transmission:

La capacité de transmission des capteurs est liée au rayonnement des antennes utilisées. La transmission d'information ne peut avoir lieu que si la distance entre les nœuds ne dépasse pas un certain seuil. Bien évidemment la consommation d'énergie est proportionnelle à la distance qui sépare les nœuds. Plus celles-ci sont éloignés et plus la consommation sera importante. La topologie de la zone géographique peut également jouer un rôle car des obstacles peuvent s'ajouter aux contraintes de la transmission des données entre les capteurs. Une zone de perception et une zone de communication peuvent être définies pour un capteur. La zone de perception permet au capteur de détecter des données physiques sur l'environnement qui l'entoure. Dès lors, la zone de communication permet à chaque entité du réseau d'avoir un aperçu des nœuds voisins pour de futures communications et de transmission de données.

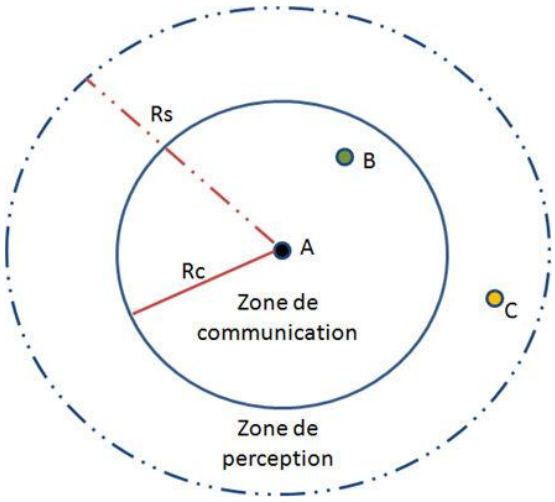

Figure 1. 7 : Illustration de la zone de communication et de perception d'un capteur.

La Figure 1.7 montre les zones définies par ces deux rayons pour le capteur A. La zone de communication est la zone où le capteur A peut communiquer avec les autres nœuds (le capteur B). D'autre part, la zone de perception est la zone où le capteur A peut capter l'événement qui s'y produit. En effet, pour qu'un capteur ait une portée de communication suffisamment grande, il est nécessaire d'utiliser un signal assez puissant. Cependant, l'énergie consommée serait importante. Comme les capteurs sont généralement disposés sur la zone à couvrir de façon aléatoire, il est nécessaire de disposer d'une densité importante de nœuds. Mais si la densité de capteurs est trop importante et que la zone que l'on veut surveiller est « trop » couverte, alors des capteurs vont fonctionner inutilement.

1.4.3. La puissance de stockage et de traitement :

Habituellement les nœuds capteurs ont une taille très petite, ce facteur de forme limite la quantité de ressources qui peuvent être mises dans nœuds, par conséquent, la capacité de traitement et de mémoire devient très limitée. Par exemple, les nœuds capteurs de type « Tmote Sky » sont composés d'un microcontrôleur cadencé à 8MHz, 48Ko de mémoire et d'une radio de débit environ 250 kbps avec une fréquence pouvant aller à 2,4 Ghz, la portée de transmission de ce type de capteur peut atteindre 50 mètres. [9]

1.5. Techniques de conservation énergétique dans les RCSFs:

Les techniques de conservation permettent généralement la mise en œuvre d'approches qui peuvent optimiser la consommation énergétique des capteurs selon leurs modes d'activités (actif, TX, RX ou sleep). L'énergie consommée par un nœud capteur est due essentiellement aux opérations suivantes de capture, de traitement et de communication.

a) ***L'énergie de capture:*** L'énergie de capture est la partie énergétique dépensée par un nœud capteur lorsque celui-ci effectue les opérations d'échantillonnage, de conversion analogique/numérique et d'activation de son module de capture. Le coût de cette énergie dépend du type spécifique du capteur (image, son, température, etc.) et des opérations précédentes. Cette énergie est en général très faible par rapport à la quantité énergétique totale consommée par un nœud capteur donné.

b) ***L'énergie de traitement:*** L'énergie de traitement d'un nœud capteur représente la quantité énergétique dépensée par celui-ci pendant les opérations de lecture et d'écriture en mémoire. Cette énergie est scindée en deux parties: 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. L'énergie de fuite représente l'énergie dissipée lorsque le processeur n'effectue aucun traitement. L'énergie de traitement est relativement faible par rapport à l'énergie dépensée durant la communication.

c) ***L'énergie de communication:*** L'énergie de communication d'un nœud capteur est divisée en deux parties : l'énergie dépensée durant la transmission de données (TX) et celle dépensée pendant la réception de données (RX). Cette énergie dépend non seulement de la quantité des données à transmettre (taille des paquets) mais également

de la distance entre l'émetteur et le récepteur et le type du module de communication utilisé. En effet, la portée d'un signal dépend non seulement de sa puissance d'émission (TX power) mais également des propriétés physiques du milieu de propagation. Cependant, la puissance d'émission influe grandement sur la portée du signal. Ainsi, lorsque la puissance d'émission est élevée, le signal aura une grande portée, et par conséquent l'énergie consommée sera plus importante. L'énergie de communication représente la plus grande partie de l'énergie consommée par un nœud capteur.

1.6. Domaines d'applications des réseaux de capteurs:

La miniaturisation des capteurs, le coût de plus en plus faible, la large gamme des types de capteurs disponibles ainsi que le support de communication sans fil utilisé, permettent aux réseaux de capteurs de se développer dans plusieurs domaines d'application. Ils permettent aussi d'étendre les applications existantes. Les réseaux de capteurs peuvent se révéler très utiles dans de nombreuses applications lorsqu'il s'agit de collecter et de traiter des informations provenant de l'environnement. Parmi les domaines où ces réseaux peuvent offrir les meilleures contributions, nous citons les domaines : militaire, surveillance, environnemental, médical, domotique, commercial,… etc.

1.6.1. Applications environnementales:

Le contrôle des paramètres environnementaux par des RCSF peut donner naissance à plusieurs applications. Par exemple, le déploiement des thermo-capteurs dans une forêt peut aider à détecter un éventuel début de feu, et par la suite peut faciliter les moyens de lutte en temps réel. Le déploiement des capteurs chimiques dans les milieux urbains peut aider à détecter la pollution et analyser la qualité d'air. De même, le déploiement de capteurs dans les sites industriels peut empêcher et prévenir certains risques industriels tels que la fuite de produits toxiques (gaz, produits chimiques radioactifs, etc.). Des nœuds capteurs peuvent également être déployés dans l'espace ou au fond des océans à partir d'avions, de ballons ou dans des navires afin de mesurer des paramètres environnementaux sur ces champs de captages, et signaler d'éventuels problèmes environnementaux (par exemple des pollutions, des aléas météorologiques, etc.). Ceci permettra ainsi d'améliorer la maîtrise de ces environnements et l'efficacité des moyens de lutte en cas de problèmes.

Figure 1.8 : Installation des capteurs Libelium en forêt pour détection des incendies (Le nord de l'Espagne)

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, etc. 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. D'autre part, ces réseaux peuvent détecter des comportements anormaux (chute d'un lit, choc, cri, etc.) chez les personnes dépendantes (handicapées ou âgées).

Figure 1.8 : Exemple d'un système de monitoring cardiaque d'AliveCore avec capteur biométrique et application pour iPhone.

1.6.3. Applications militaires:

Le domaine militaire a été un moteur initial pour le développement des réseaux de capteurs. En effet, les différents avantages qu'offrent ces réseaux qui sont entre autres le déploiement rapide, le coût réduit des équipements, l'auto-organisation et la tolérance aux pannes qui rendent ce type de réseaux très appréciable dans le domaine militaire. Un réseau de capteurs déployé dans un champ de bataille dans un secteur stratégique ou dans une zone difficile d'accès, ceci permet par exemple de surveiller tous les mouvements de l'ennemi ou d'analyser le terrain (détection de mines, d'agents chimiques, biologiques, des radiations, détection et tracé du chemin d'un véhicule militaire, etc.) avant de déployer des troupes. Ainsi, beaucoup de projets dans le domaine des RCSF ont été lancés dans le but d'aider des unités militaires et pour protéger des villes contre des attaques telles que les menaces terroristes, etc.

Figure 1.9 : Exemple d'une application militaire

1.6.4. Domaine domotique:

Avec le développement technologique, les capteurs peuvent être embarqués dans des appareils, tels que les aspirateurs, les fours à micro-ondes, les réfrigérateurs, les magnétoscopes, etc. Ces capteurs embarqués peuvent interagir entre eux et avec un réseau externe via Internet pour permettre à un utilisateur de contrôler les appareils domestiques localement ou à distance. 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 s'éteint et la musique s'arrête quand la chambre est vide, la climatisation

et le chauffage s'ajustent selon les points multiples de mesure, l'alarme est déclenchée par le capteur anti-intrusion quand un étranger veut pénétrer dans la maison.

Figure 1.10 : le contrôle d'une maison grâce à un téléphone intelligent ou une tablette

1.7. Contraintes influençant les réseaux de capteurs sans fil:

1.7.1. Consommation énergétique:

Un capteur, de par sa taille, est limité en énergie (< 1.2V). 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 nœud 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.

1.7.2. 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.

1.7.3. Passage à l'échelle:

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

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:

Le traitement des erreurs dans un réseau est un critère du bon fonctionnement d'un réseau ainsi que du protocole et des services mis en place. La tolérance aux pannes est la capacité d'assurer la continuité du fonctionnement du réseau sans interruption qui peut être due à un ou plusieurs capteurs pendant les transmissions.

Certains capteurs peuvent générer des erreurs ou ne peuvent plus transmettre à cause d'une énergie limité pour pouvoir continuer à jouer un rôle actif dans le réseau, ou d'une

interférence survenue par des champs électriques momentanées. Les protocoles de routage doivent s'adapter et gérer ce genre panne afin de permettre le bon fonctionnement du réseau, mais également au milieu hostile ou les nœuds vont être déployés.

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, 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 (temporallyordered routing algorithm), 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 QoS. 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 le construction d'une communication sécurisée entre deux ou plusieurs dispositifs, assurer la confidentialité, l'intégrité et l'authentification.

1.8. Conclusion :

Les réseaux de capteurs sans fil présentent un intérêt considérable et une nouvelle étape dans l'évolution des technologies de l'information et de la communication. Cette nouvelle technologie suscite un intérêt croissant vu la diversité de ces applications : santé, environnement, industrie, … etc.

Dans ce premier chapitre, nous avons présenté les réseaux de capteurs sans fil, leurs architectures de communication, la pile protocolaire des capteurs et leurs diverses applications. Cependant, nous avons remarqué que plusieurs facteurs et contraintes compliquent la gestion de ce type de réseaux, la sécurité de ces réseaux est l'un des défis les plus importants à considérer. Dans le chapitre suivant, nous introduirons en détail la sécurité dans les réseaux du capteur sans fil.

Chapitre 2

Sécurité des communications dans les réseaux de Capteurs sans fil

2.1. Introduction

Les nœuds capteurs sont conçus pour être déployés d'une manière dense dans des endroits hostiles et difficiles d'accès, d'où la nécessité de limiter au maximum leurs dimensions physiques qui s'obtiennent impérativement au détriment des capacités de calcul de traitement et de ressources énergétiques.

En raison de leur déploiement en environnements ouverts, de leurs ressources limitées, et la nature du medium de transmission ; les réseaux de capteurs doivent faire face à de nombreuses attaques. Sans mesures de sécurité un agent malveillant peut lancer plusieurs types d'attaques qui peuvent nuire au travail des réseaux de capteurs sans fil (RCSF) et empêcher leur bon objectif de déploiement. La sécurité est donc une dimension importante pour ces réseaux.

Dans ce contexte, une grande communauté de chercheurs tente de proposer des mécanismes afin de renforcer la sécurité des données communiquées pour diminuer le risque d'interception et d'altération. Généralement, afin de protéger les communications, il est nécessaire d'utiliser des primitives cryptographiques comme les algorithmes de chiffrement. Il est également essentiel d'établir des clés secrètes entre les paires ou les groupes de nœuds capteurs, ce qui est nécessaire aux primitives cryptographiques qui permettent d'assurer la confidentialité, l'authentification, la disponibilité, l'intégrité des échanges des données dans un RCSF. Afin d'assurer l'efficacité de ces fonctionnalités, nous avons besoin d'un mécanisme de gestion de clés.

Dans ce chapitre, nous présentons les différents objectifs de la sécurité puis nous citons des solutions adaptées concernant les attaques et contremesures. Ensuite, nous détaillons le mécanisme de la gestion de clés et on a classé leurs méthodes et protocoles. Enfin, nous représentons les métriques d'évaluation.

2.2. Objectif de la sécurité dans les RCSFs :

La sécurité des réseaux de capteurs sans fils doit assurer les objectifs suivants :

2.2.1. Authentification :

Elle permet de coopérer au sein des RCSFs sans risque, en contrôlant et en identifiant les participants. Elle apparaît comme la pierre angulaire d'un réseau de capteur sans fil sécurisé. En effet, on ne peut assurer une confidentialité et une intégrité des messages échangés si, dès

le départ, on n'est pas sûr de communiquer avec le bon nœud. Si l'authentification est mal gérée, un attaquant peut se joindre au réseau et injecter des messages erronés. [10]

L'utilisation de Code d'Authentification de Message (CAM), ou MAC en anglais (Message Authentication Code) [11], permet d'assurer à la fois l'authentification de l'origine et l'intégrité du message.

2.2.2. La confidentialité :

La confidentialité des données est la question la plus importante dans la sécurité de réseau. Ce service désigne la garantie que l'information soit inaccessible aux adversaires. Cela signifie que l'information émise par chaque capteur n'est lisible que par le capteur auquel cette information est destinée, l'approche standard pour sécuriser nos transfert de données et de crypter les données avec une clé secrète connais par l'émetteur et le récepteur. [11]

2.2.3. L'intégrité :

Cette propriété permet d'assurer que le contenu d'un message n'a pas été modifié durant sa transmission dans le réseau et bloquer tout essai d'injection de fausses données, que ce soit volontairement ou accidentellement. Ainsi un capteur intermédiaire compromis peut altérer un message entre l'émetteur et le récepteur. Généralement, afin de vérifier l'intégrité le MAC (Message Authentication Code) et les signatures numériques sont utilisés. [12]

2.2.4. La disponibilité :

Elle signifie que le réseau est disponible pour assurer ses services et autoriser les parties communicantes lorsque ceci est nécessaire. Cette propriété reste difficile à assurer dans les RCSFs étant donné les contraintes qui pèsent sur ces réseaux, à savoir : topologie dynamique, ressources limitées des nœuds de transit, communications sans fil pouvant être facilement brouillées ou perturbées. [13]

2.2.5. La Fraîcheur :

Elle permet de garantir la fraîcheur de données et la fraîcheur des clés. En effet, les données sont valides seulement dans un intervalle de temps limité. Par conséquent, lorsqu'un capteur reçoit un paquet de données, il doit être vérifié que les données transmises sont récentes ou non, et que l'adversaire n'a pas retransmis des vieux messages. Pour résoudre ce problème, un

compteur ou bien un nombre pseudo-aléatoire peut être intégré aux paquets de données pour filtrer les vieux messages. [12]

2.3. Les contraintes de la sécurité dans les RCSF :

Un réseau de capteurs sans fil est un réseau spécial qui a de nombreuses contraintes, comparés au réseau informatique traditionnel. En raison de ces contraintes, il est difficile de recourir directement à des approches de sécurité existantes pour le domaine des réseaux de capteurs sans fil. Par conséquent, élaborer des mécanismes de sécurité efficaces tout en empruntant des idées à partir des techniques de sécurité actuelles. Il est toutefois primordial de connaître et comprendre ces contraintes [14].

2.3.1. La contrainte des ressources :

Toutes les approches de sécurité nécessitent une certaine quantité de ressources pour leur implémentation, y compris la mémoire de données, l'espace du code, et l'énergie pour alimenter le capteur. Toutefois, actuellement, ces ressources sont très limitées dans un minuscule capteur sans fil.

- **Limitation en énergie :**

L'énergie est un facteur critique à considérer en concevant des mécanismes de sécurité, puisque les capteurs sont fréquemment déployés à des endroits hostiles, donc on ne peut pas changer les batteries ou les recharger. Alors, il est très important de minimiser la consommation d'énergie et de prolonger la durée de vie des batteries. Cette limitation impose la conception des mécanismes de sécurité à faible consommation énergétique.

- **Limitation de la mémoire et de l'espace de stockage**

Dans les RCSFs, la limitation des ressources restreint les mécanismes de sécurité. En effet, les nœuds capteurs n'ont pas la capacité de mémoriser le code de sécurité et les données relatives (tel que les clés de cryptage de taille importante) ou d'exécuter des protocoles cryptographique qui exigeant plus de puissance de calcul.

2.3.2. Manque de fiabilité de communication

Un canal sans fil est un moyen de communication ouvert accessible par toute personne qui se trouve dans la portée du signal. Cependant, ce moyen est à son tour un obstacle pour la sécurité, rendant facile la production des attaques sur le réseau de capteurs.

2.3.3. Fonctionnement sans surveillance

Les nœuds capteurs sont souvent distribués dans des endroits non accessibles tels que des champs de bataille au-delà des lignes ennemies, à l'intérieur de grandes machines, au fond d'un océan, dans des champs biologiquement ou chimiquement souillés, Par conséquent, ils doivent pouvoir fonctionner sans surveillance dans des régions géographiques éloignées. Ceci peut produire des faiblesses de sécurité pour le réseau.

2.3.4. Exposition aux attaques physiques

Les nœuds sont exposés aux attaques physiques. Donc l'attaquant peut avoir le contrôle total sur des nœuds du réseau ou supprimer le nœud capteur, cela se fait par le vol ou la destruction du nœud.

2.3.5. Gestion à distance

La gestion à distance d'un réseau de capteurs pour détecter toute altération physique et les problèmes d'entretien physique (par exemple, le remplacement des piles), est pratiquement impossible. L'exemple le plus concret, un nœud de capteur utilisé pour des missions de reconnaissance à distance derrière les lignes ennemies.

2.4. Attaques et contremesures :

Une variété d'attaques contre les RCSFs est rapportée dans la littérature spécialisée. Pour faire face à ces attaques, diverses contre-mesures ont été proposées. Les différentes caractéristiques des réseaux de capteurs sans fil (faible puissance de calcul, énergie limitée, et l'utilisation des ondes radio, etc. ...) les exposent à de nombreuses attaques de sécurité. Nous détaillons dans la suite quelques types d'attaques et les contremesures pour se défendre de leurs effets. Nous avons choisi de répartir les attaques selon l'intention de l'attaquant.

2.4.1. Collection d'informations :

L'attaquant commence à collecter et analyser les données grâce à des attaques de type «collection d'informations». Il peut par la suite utiliser ces données pour déclencher d'autres types d'attaques selon les failles découvres par ses analyses.

- **Eavesdropping ou Passive Monitoring :**

L'attaque Eavesdropping fait partie des attaques passives pour lesquelles les adversaires cherchent à surveiller ou à collecter les informations circulant dans le réseau. Le but de cette attaque est d'écouter le trafic sur les canaux de communication et d'intercepter les paquets. En effet, ce type d'attaques est plus facile à réaliser (il suffit de posséder un récepteur adéquat) et il est difficile de le découvrir puisque l'attaquant n'apporte aucune modification sur les données échangées. Ainsi, l'intrus peut espionner et capter des données stratégiques qui peuvent aider au lancement d'attaques plus dangereuses ou bien la connaissance des nœuds importants dans le réseau (chef de groupe "cluster Head"). [14]

- **Divulgation d'information :**

Cette attaque est utilisée pour connaître un maximum d'informations sur le RCSF comme la topologie, le protocole MAC, le protocole de routage et les mécanismes de sécurité comme l'authentification et les algorithmes de chiffrement, … etc. L'analyse des paquets reçus ou envoyés d'un nœud pourra donner des précisions sur son rôle. Pour lutter cette attaque, il faut utiliser des clés suffisamment grandes ou renouvelées périodiquement. [14]

2.4.2. Perturbation des communications :

Le média sans fil est un média ouvert, il est à son tour un obstacle à la sécurité. Par conséquent, un nœud attaquant peut endommager les paquets de données en provoquant des collisions et des interférences dans le canal de communication. De plus, toute transmission peut facilement retransmise, interceptée, ou altérée par un adversaire. Les attaques de cette catégorie sont considérées comme des attaques actives qui visent les couches : physique, liaison de données, réseau et transport de la pile protocolaire. Nous détaillons dans ce qui suit quelques attaques qui perturber les communications dans les réseaux de capteurs sans fils.

- **Jamming :**

Dans cette attaque, le nœud malveillant essaye d'interférer avec la fréquence radio utilisée par les nœuds capteurs dans le réseau. La source de brouillage peut être assez puissante pour perturber l'ensemble du réseau. Le nœud malveillant peut lancer des attaques de brouillage

stratégiques en ciblant des zones sensibles du réseau (station de base) sans attirer les attentions (signal de brouillage qui respecte les normes du réseau). [15]

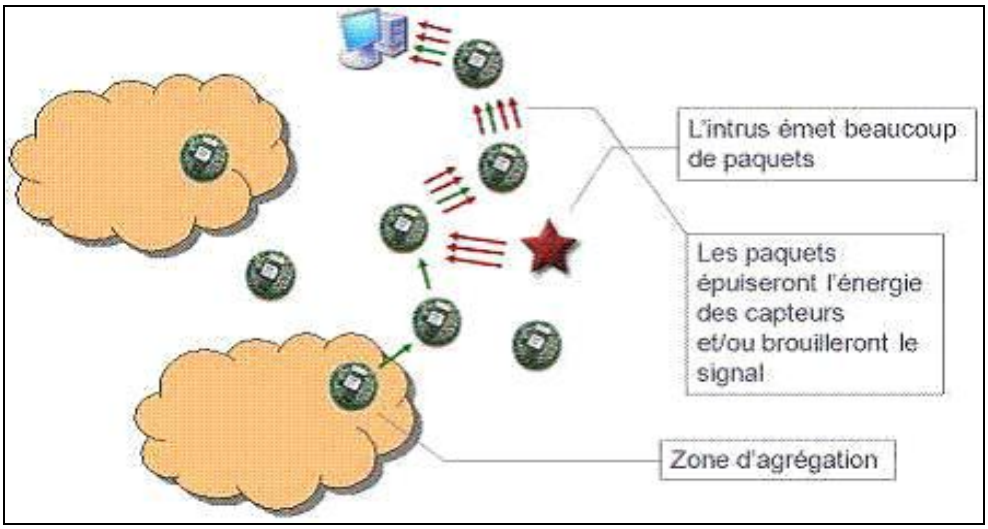

Figure 2.1 : attaque de Jamming [15]

- **Collision :**

L'attaque de collision peut être facilement lancée par un nœud compromis *(ou malveillant)*, qui ne respecte pas les conditions d'accès au média de transmission. L'objectif est de provoquer des collisions avec des transmissions voisines en envoyant périodiquement un simple paquet de bruit. Par exemple, dans le protocole SMAC, l'attaquant vérifie le canal de communication afin d'assurer que le support est occupé *(réception des paquets RTS et CTS)*. Si c'est le cas, il envoi des paquets corrompus afin d'entrer en collision avec les paquets échangés dans le réseau.

2.4.3. Agrégation de données et épuisement de ressources :

Les attaques de ces deux catégories sont considérées comme des attaques actives qui visent les couches : liaison de données, réseau et transport de la pile protocolaire.

- **Sybil**

Le principe de cette attaque est la déstabilisation du fonctionnement des protocoles de routage multi-sauts et les mécanismes de maintenance de topologie réseau. Le nœud malveillant peut créer un grand nombre d'identités afin de gagner de l'influence sur les autres nœuds du réseau.
Chaque identité (ID) peut être générée aléatoirement ou être dupliquée *(recopiée)* d'une identité légitime qui existe déjà. Ainsi, le nœud attaquant peut profiter de ces multiples identités pour être

sélectionné comme chef de groupe *(cluster Head)*, ou pour créer des chemins de routage pour son propre intérêt. [12]

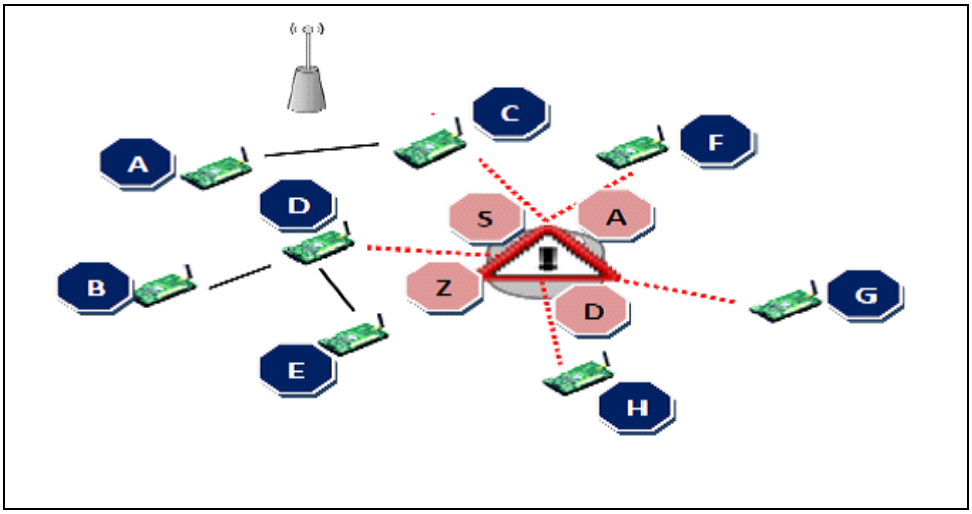

Figure 2.2 : attaque de Sybil [13]

- **De-Synchronisation**

L'attaquant fait croire à un nœud capteur (victime) qu'il n'a pas reçu un certain nombre de paquets en faussant la séquence des paquets intercepter qui est réellement destinée à un autre nœud capteur dans le réseau. L'attaquant réalise ce type d'attaque en augmentant le numéro de séquence des paquets passants par lui plus que prévu auprès du nœud victime. Ainsi, il incite le destinataire à demander la retransmission des paquets manquants auprès des expéditeurs. Par conséquent, l'attaquant pousse sa victime à dissiper son énergie en tentant de réparer les erreurs de transmission qui n'ont pas vraiment existées. [14]

2.4.4. Capture physique de nœuds :

La plupart des applications des réseaux de capteurs exigent un déploiement étroit des nœuds à l'intérieur ou à proximité des phénomènes à surveiller. Cela peut conduire à de fréquentes captures et compromissions des nœuds capteurs, car les nœuds capteurs ne peuvent pas tous intégrer des solutions de protection physique. L'attaque Tampering est classée dans cette catégorie car elle a besoin d'un accès physique aux nœuds capteurs.

- **Tampering (Attaque d'altération) :**

Les RCSFs sont généralement déployés dans des zones hostiles et non surveillées. Par conséquent, les nœuds capteurs sont vulnérables aux attaques d'altération physique pour

extraire toutes les informations importantes comme les clés cryptographiques. Ces informations peuvent être utilisées ultérieurement afin de déclencher d'autres types d'attaques. En effet, un attaquant peut aussi modifier les codes de programmes, altérer les circuits électroniques ou même remplacer le nœud capteur par un capteur malveillant.[15]

2.5. 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.

2.5.1. Primitives cryptographique

Plusieurs mécanismes basés généralement sur la notion de cryptographie, sont mis en place afin de répondre à la question de la sécurité dans les RCSFs. Le chiffrement et le déchiffrement des messages sont effectuées par des algorithmes cryptographiques. Ces algorithmes reposent généralement sur des problèmes mathématiques complexes et difficiles à résoudre. Nous présentons par la suite, les différentes primitives cryptographiques qui sont utilisées dans les réseaux de capteurs sans fil.

2.5.1.1. La cryptographie

La cryptographie est l'une des premières solutions de sécurité qui répond à l'ensemble des problèmes liés à la sécurité des informations. Elle permet 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. On distingue deux types de cryptographies :

- **La Cryptographie symétrique**

Une même clé est utilisée entre deux nœuds communicants pour chiffrer et déchiffrer les données en utilisant un algorithme de chiffrement symétrique. L'avantage principal de ce mode de chiffrement est sa rapidité. Ainsi que, elle n'a pas de grandes dissipations

énergétiques durant les phases de chiffrement et de déchiffrement. Par conséquent, elle est plus adaptée pour les RCSFs. Deux types de chiffrements symétriques sont utilisés]:

- Le chiffrement en chaîne est fait bit à bit sans attendre la réception entière des données. L'algorithme le plus connu est : RC4/RC5 (*Rivest Cipher 5*) [12].
- Le chiffrement par bloc consiste à fractionner les données en blocs de taille fixe (64 bits, 128 bits). Chaque bloc sera ensuite chiffré une fois qu'il atteint une taille envisagée. Les algorithmes les plus utilisés sont : DES (*Data Encryption Standard*), AES (*Advanced Encryption Standard*) [12].

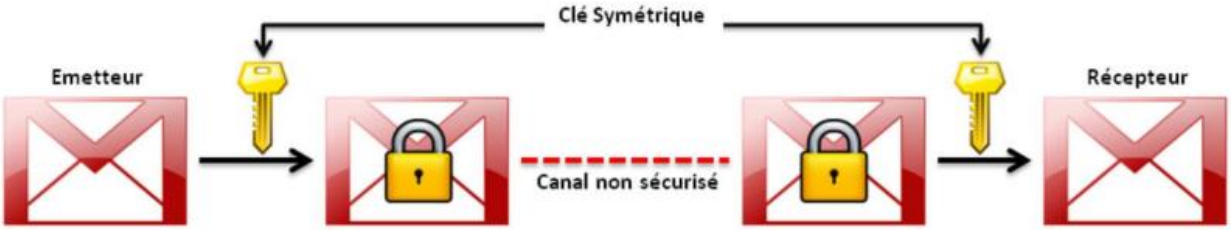

Figure 2.3 : Cryptographie symétrique

- **La cryptographie asymétrique**

Dans la cryptographique asymétrique (ou la cryptographie à clé publique), deux clés différentes sont générées par le récepteur : une clé publique diffusée à tous les nœuds servant au chiffrement de données qu'ils vont émettre au récepteur, et, une clé privée maintenue secrète chez le récepteur servant pour le déchiffrement de ces données lorsque ce dernier les reçoit. Le point fondamental sur lequel repose la sécurité du chiffrement asymétrique est l'impossibilité de déduire la clé privé à partir de la clé publique. La figure2.4 illustre un mécanisme de chiffrement basé sur la cryptographie asymétrique. Bien que le chiffrement asymétrique comporte des avantages, mais la complexité de ce type de cryptographie n'exige que le nœud capteur à une capacité de traitement et de stockage plus élevée et une consommation d'énergie plus haute. Parmi les algorithmes de chiffrement asymétrique les plus connus nous citons : le RSA (Rivest Shamir Adleman) [16] et l'ECC (elliptic curve cryptography) [12]

Figure 2.5 : Cryptographie symétrique

2.5.1.2. La fonction de hachage

Cette fonction permet de générer une chaîne de taille inférieure et généralement fixe à partir d'une chaîne de longueur quelconque. Par conséquent, la chaîne résultante est appelée empreinte (digest en anglais). D'un autre cotée, une fonction de hachage est une fonction à sens unique, autrement dit qu'il est facile à calculer l'empreinte d'une chaîne donnée, mais il est impossible de déduire à la chaîne initiale à partir d'une empreinte donnée. En général, les fonctions de hachage sont utilisées comme un mécanisme qui vérifier l'intégrité d'un message envoyé. L'émetteur utilise la fonction de hachage pour créer une empreinte du message transmettre, puis il transmet le message et l'empreinte vers le récepteur. A la réception du message, le récepteur calcule l'empreinte du message reçu et il la compare à l'empreinte initiale. Si les deux empreintes correspondent, c'est que le message n'a pu être altéré.

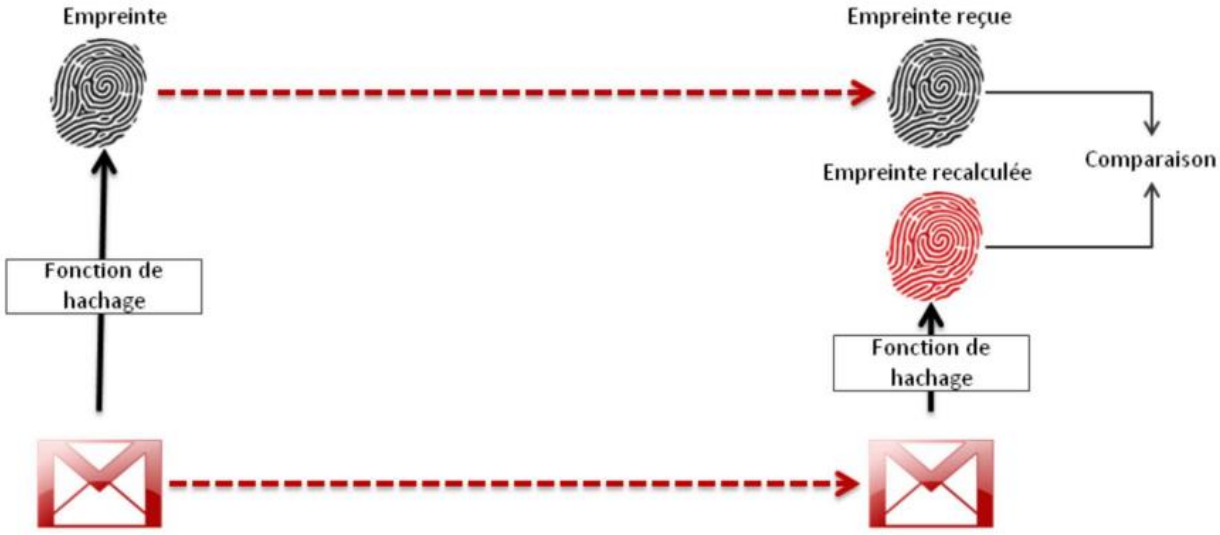

Figure 2.6 : la fonction de hachage

2.5.1.3. Le code d'authentification de message

Le code d'authentification de message (CAM), ou MAC (pour Message Authentication Code en anglais) permettant d'assurer d'une part l'intégrité du message transmis et d'autre part l'authenticité de l'expéditeur. Un MAC consiste à calculer une courte empreinte de taille fixe à partir d'une donnée de taille arbitraire combinée à une clé secrète (symétrique) connue uniquement par les deux entités communicantes (échangeant le message). Comme illustré dans la figure 2.7, cette clé est utilisée pour calculer le code MAC par l'émetteur (1). Ce code est par la suite envoyé avec les données (2). Le récepteur calcule à son tour le code MAC avec cette même clé et le compare au code qu'il a reçu (3). S'ils sont bien identiques (4), alors la source est authentique et les données n'ont pas été altérées. Un exemple de MAC utilisé dans la pratique est le HMAC (Hash Message Authentication Code) [16]. Ce dernier (c.à.d. le HMAC) peut utiliser n'importe quelle fonction de hachage, comme SHA-1[16] ou MD5 [17].

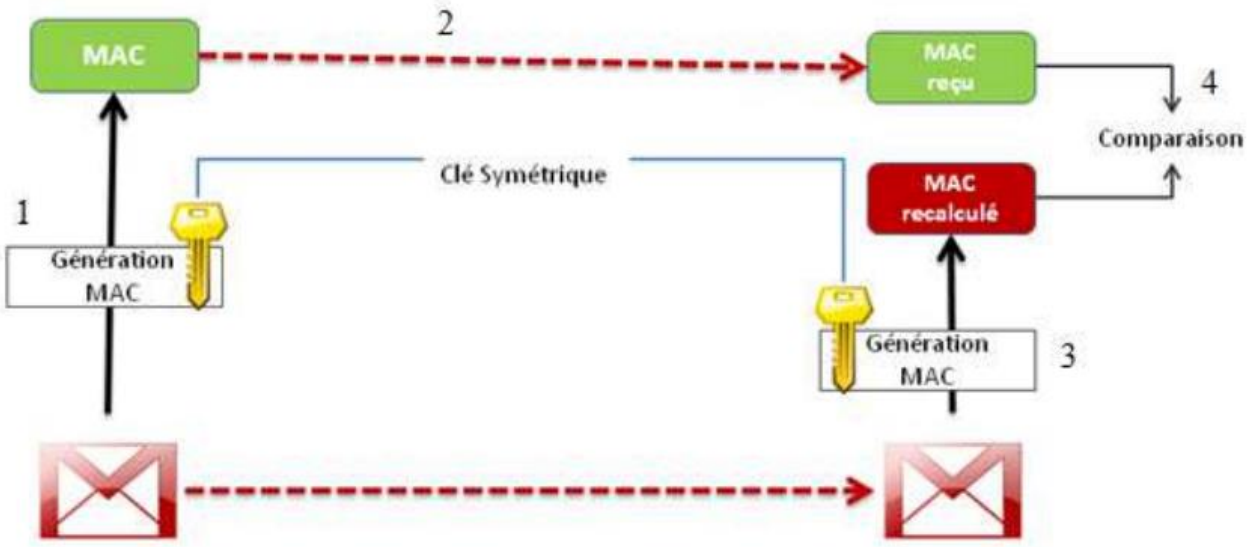

Figure 2.7 : le code d'authentification de message

2.5.2. La gestion des clés

La sécurité des communications dans un RCSF commence par la protection des liens entre chaque paire de nœuds de ce réseau. Elle pourra être assurée à l'aide de primitives cryptographiques (c.à.d. l'utilisation du chiffrement, déchiffrement, de la signature, etc.). La gestion de clés est l'un des aspects les plus difficiles lors de la configuration d'un système cryptographique de sécurité. Pour qu'un tel système fonctionne et soit sécurisé, chacun des utilisateurs doit disposer d'un ensemble de clés secrètes (dans un système à clés secrètes), ou de pair de clés privée/publique (dans un système à clés publiques). Cela implique de générer

les clés et de les distribuer de manière sécurisée aux utilisateurs ou d'offrir à l'utilisateur le moyen de les générer. Il doit aussi pouvoir enregistrer et gérer ses clés publiques et privées de manière sûre.

La gestion des clés dans ce cas est non seulement une question critique mais doit tenir compte des faibles ressources des nœuds capteurs. Pour cette raison, les caractéristiques spéciales aux réseaux de capteurs sans fil ne permettent pas d'utiliser des méthodes complexes. En effet, le temps de calcul et la consommation d'énergie dans les traitements doivent être raisonnables. Par conséquent, la gestion de clés doit garantir le couplage des caractéristiques propres aux RCSFs aux exigences de sécurité.

2.6. La gestion de clés : méthodes et protocoles

Nous présentons dans cette section un aperçu sur les composants d'un système de gestion de clés dans les RCSFs. Il existe dans la littérature beaucoup de solutions dédiées à des problèmes qui ont été étudiés durant cette mémoire. Nous souhaitons cependant ici introduire les principaux schémas de gestion de clés qui sont utilisés pour sécuriser les RCSFs suivis d'une discussion sur les critères importants pour l'évaluation de leurs performances.

2.6.1. Composants de la gestion de clés

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. 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 :

2.6.1.1. 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.

2.6.1.2. Le renouvellement de clés

Le renouvellement de clés asymétriques et symétriques est nécessaire afin de maintenir un niveau de sécurité élevé. Il constitue un défi majeur pour le système de gestion de clés puisque des nouvelles clés doivent être créées d'une manière efficace et conforme à une consommation et conservation d'énergie. Le renouvellement des clés se fait soit i) volontairement : après une période de temps, ii) préventivement : lors d'une tentative d'accès illégale par un attaquant ou bien iii) obligatoirement : après la compromission d'un ou de plusieurs nœuds capteurs du réseau.

2.6.1.3. 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. [14]

2.6.2. Les phases d'établissement de clé

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 RCSFs 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 [16]:

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

Dans le cas des RCSFs, où la topologie du réseau est inconnue qu'après le déploiement des nœuds, une phase de pré-distribution des clés qui consiste de chargées les clés dans les nœuds capteur avant le déploiement, est le seul moyen sûr et efficace qui permet aux nœuds communicants de partager les clés secrètes d'une manière sécurisée.

Les clés stockées dans la mémoire avant le déploiement constituent le porte-clés (Key ring). S'il existe une clé commune entre deux nœuds, ils peuvent créer une connexion sécurisée entre eux. La solution optimale en termes de ressources est de pré chargé tous les nœuds par une seule clé secrète. Ce qui provoque une très faible résilience, alors un adversaire puissant peut capturer un nœud et compromettre la clé très facilement. Pour surmonter ce problème, une autre solution consiste à utiliser une paire de clés distinctes pour toutes les paires de nœuds possibles dans le réseau. Cependant, deux problèmes qui se posent dans les schémas traditionnels de pré distribution de clés, dont le premier est de savoir comment charger un ensemble de clés dans la mémoire limité de chaque capteur. Le second problème inclue la sauvegarde de l'identifiant clé parmi un ensemble de clés et l'association de l'identifiant du nœud avec un nœud de contrôleur de confiance [18].

2.6.2.2. Découverte de clé partagée

Après le déploiement, Chaque nœud a besoin de découvrir ses voisins dans son porté sans-fil de communication avec laquelle il partage des clés. Donc, Si un nœud capteur découvre qu'il partage une clé commune avec un nœud particulier, il peut utiliser cette clé pour une communication sécurisée. Le bon schéma de découverte de voisin ne donnera pas à un adversaire l'opportunité de découvrir les clés partagées et ne peut donc faire que l'analyse du trafic.

2.6.2.3. Établissement de clés de chemin

S'il n'existe pas de clé commune entre deux nœuds capteurs voulant communiquer, et qui sont relies par un chemin multi saut, alors un chemin sécurisé doit être trouvé entre eux. Ce chemin passe par un ensemble de nœuds capteurs qui contient déjà des liens sécurisés. Une

fois ce chemin établi, la clé de chemin (pathkey) est générée et communiquée via ce chemin et les deux nœuds peuvent l'utiliser pour communiquer en toute sécurité.

2.6.3. Classification de méthodes et protocoles

Étant donné que les nœuds des réseaux RCSFs ont des contraintes de calcul et de puissance, les protocoles de gestion de clés pour ces réseaux doivent être extrêmement légers. La plupart des protocoles de gestion de clés existants pour les RCSFs sont basés sur la cryptographie à clé symétrique car les techniques de cryptographie à clé publique sont en général intensives en calcul. En général, La plupart des méthodes basées sur les systèmes symétriques résolvent le problème d'établissement de clés en passant par une phase de pré-distribution. Nous trouvons plusieurs classifications de gestion de clés dans la littérature. La figure 2.8 illustre une taxonomie des solutions de gestion de clés basées sur la pré-distribution. Dans cette taxonomie, les protocoles sont classés dans plusieurs catégories selon la topologie du réseau (hiérarchique ou plate) et la façon avec laquelle les nœuds voisins partagent des clés communes (probabiliste ou déterministe). Dans cette section, nous détaillerons les principales solutions de cette figure.

2.6.3.1. Schémas probabilistes

Dans ce cas 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.

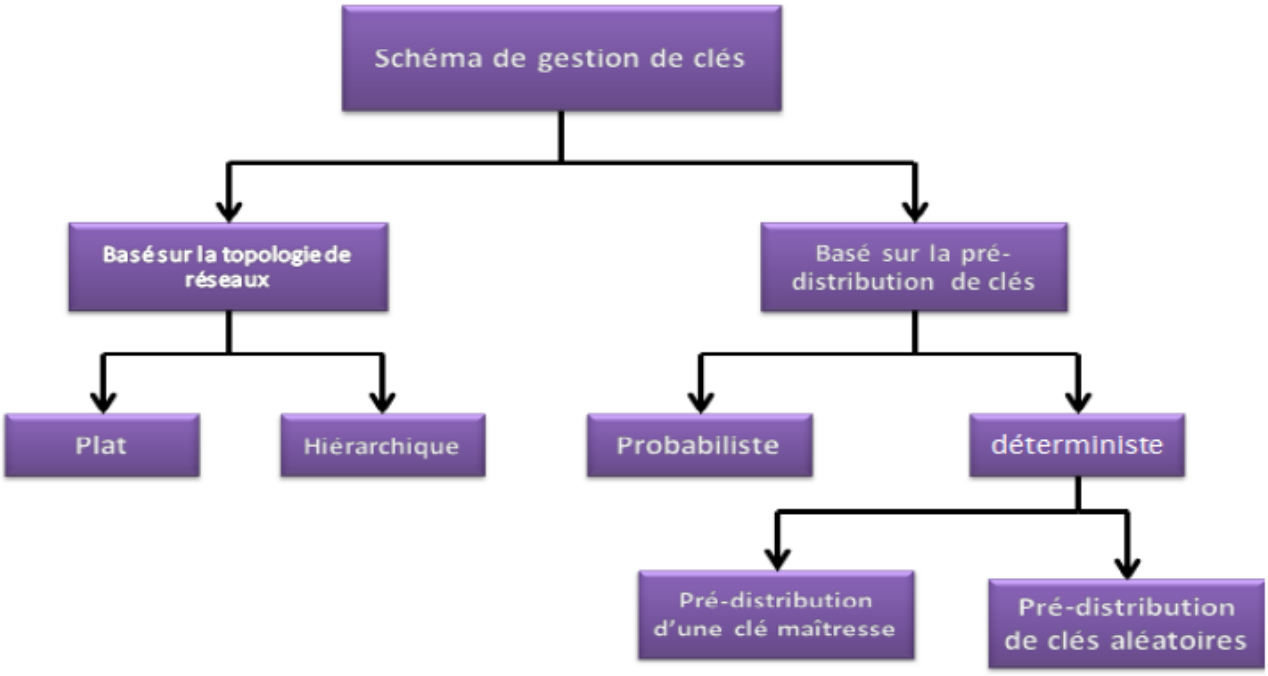

Figure 2.8 : Classification des schémas de gestion de clés dans le réseau de capteur sans fil [13]

Eschenauer et Gligor [13] ont été parmi les premiers à introduire le concept de pré-distribuer ou de stocker dans les nœuds capteurs. Cette méthode est considérée comme le schéma basique des méthodes probabilistes. Il adresse l'établissement de clés, leur renouvellement et leur révocation. Dans ce schéma, trois phases sont nécessaires pour installer les clés secrètes entre les nœuds capteurs.

(i) Phase de pré-distribution de clés :

Cette phase est effectuée avant le déploiement. Au début, un grand ensemble de clés P(Pool) est généré et chaque clé est associée à un identificateur.

Ensuite, pour chaque nœud, clés sont choisies au hasard à partir de l'ensemble. Ces clés sont stockées dans la mémoire du nœud et forment le porte-clés (Key ring) du nœud (voir figure 2.9). Le nombre de clés |P| de l'ensemble est choisi de telle manière que deux sous-ensembles aléatoires de de taille auront une certaine probabilité 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 P de taille $|S| = 10000$ clés.

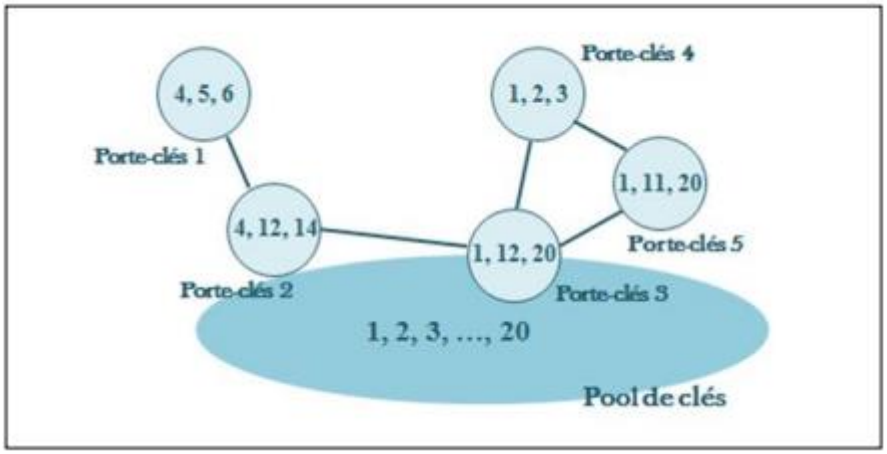

Figure 2.9 : Un exemple du schéma d'Eschenauer et Gligor [18].

(ii) Phase de découverte de clés partagées :

Après le déploiement, les nœuds découvrent leurs voisins et plus particulièrement ceux avec qu'ils sont en mesure de communiquer de façon sécurisée car ils possèdent une clé identique dans leur porte-clés respectif. Une simple méthode est que les nœuds diffusent leurs listes d'identifiants des clés stockées dans sa mémoire à d'autres nœuds. Si un nœud découvre qu'il partage une clé commune avec un nœud particulier, il peut utiliser cette clé pour une communication sécurisée.

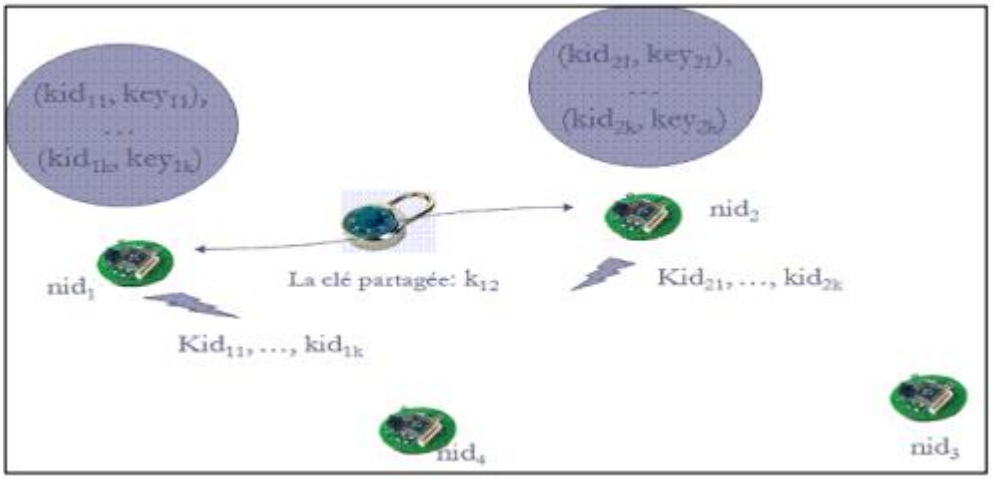

Figure2.10 : Découvertes des clés partagées [18]

(iii) Phase d'établissement de chemin de clé

Après la phase de découverte de clés partagées, le réseau est un graphe connecté formé de liens sécurisés. Les nœuds peuvent alors utiliser les liaisons existantes pour mettre en place des clés partagées avec leurs voisins qui ne partageaient pas de clé en commun avec eux, dans

laquelle il sélectionne un nœud intermédiaire agissant comme un médiateur entre les deux nœuds capteurs afin d'établir une clé de session commune. Ensuite, cette clé est utilisée comme clé de chemin pour les paires de nœud sélectionnées.

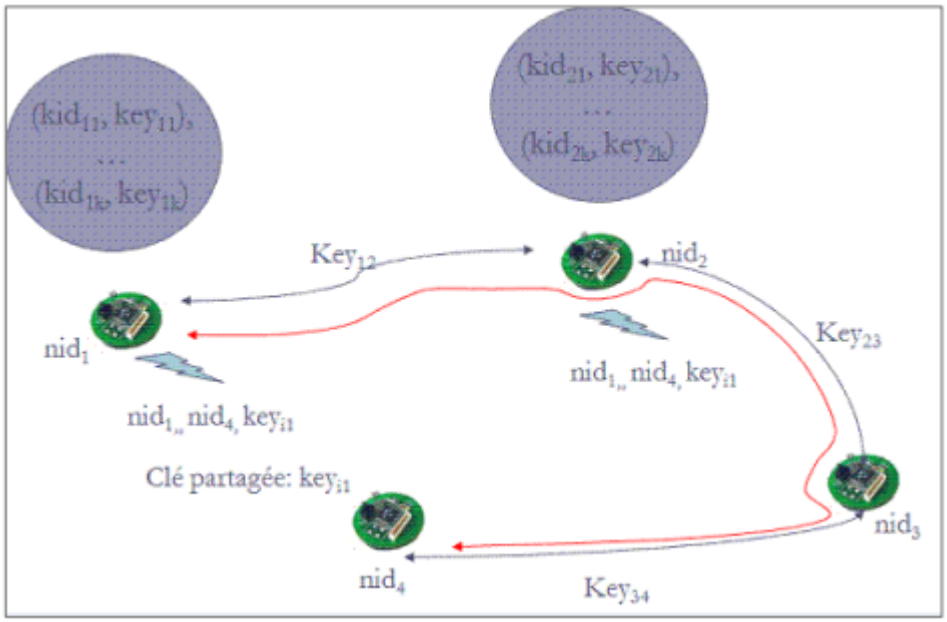

Figure2.11 : Etablissement de chemins sécurisés [18]

(iv)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 générée par le nœud contrôleur et envoyée en unicast à chaque nœud en la chiffrant avec la clé partagée entre tous les nœuds et le nœud de contrôle pendant la phase de pré-distribution de clés. Une disparition des liens sera produit 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). La figure suivante illustre cette phase :

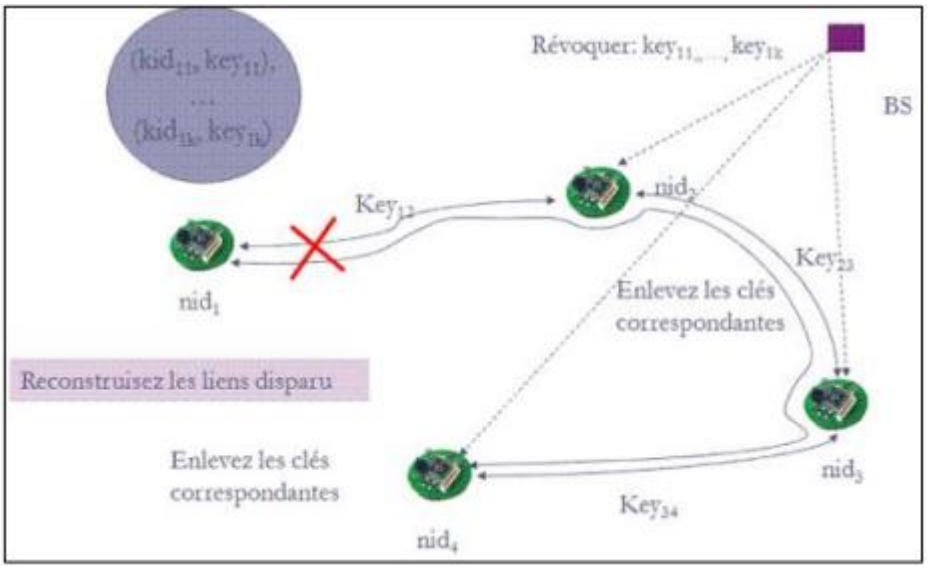

Figure 2.12 : révocations de clés [18]

Chan et al. [13] se sont basés sur la méthode de Eschenauer et al. Afin de proposer un nouveau schéma de pré-distribution Q-Composite, où deux nœuds voisins doit partager 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. Plus le nombre de clé partagées est augmenté plus la résilience contre la capture du nœud augmente. Un exemple de schéma de pré-distribution de clé Q-composite est illustré à la figure 2.13. La taille du pool de clés |P| est le paramètre critique à calculer pour que le schéma Q-Composite soit efficace. Ainsi, |P| est calculée en fonction de la contrainte de la probabilité que deux nœuds partagent au moins clés et le nombre de clés qu'un nœud peut contenir m.

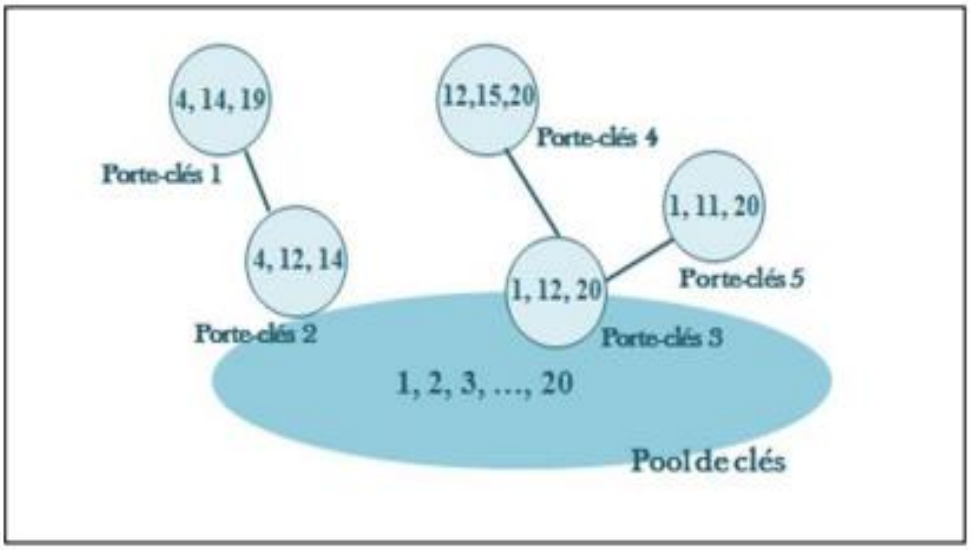

Figure 2.13 : Schéma q-composite [18]

2.6.3.2. Schémas déterministes

- **Schémas de pré-distribution de clés aléatoires :**

Dans ce type des méthodes déterministes, les porte-clés sont générés d'une manière déterministe pour s'assurer de l'établissement de certains liens entre les nœuds capteurs.

Blom [13] utilise une matrice publique G de taille (λ+1) N et une matrice D symétrique de taille (λ+1)(λ+1) qui est générée sur GF (q) et où N est la taille du réseau. L'ensemble des clés par-paires de ces N nœuds sont stockées dans une matrice symétrique appelée matrice secrète K=AG, sachant que $A=(DG)^T$. Kij de la matrice K est la clé du nœud i pour sécuriser la liaison avec le nœud j. Après, chaque nœud i est pré-chargé avec la i-ème rangée de la matrice secrète et la i-ème colonne de la matrice publique []. Cette méthode est illustrée à la figure 2.14. Après déploiement, chaque paire de nœuds i et j peuvent individuellement calculer la clé partagée entre eux Kij =Kji en échangeant seulement leurs colonnes en claire, car la clé est le produit scalaire de leur propre ligne et les colonnes reçues de l'autre. Le schéma de Blom nécessite une multiplication coûteuse de deux vecteurs de taille λ +1 où les éléments sont aussi grands que la taille de clé cryptographique correspondante. Chaque nœud capteur diffuse un message et reçoit un message de chaque nœud dans sa couverture radio, où les messages portent un vecteur de taille λ +1.

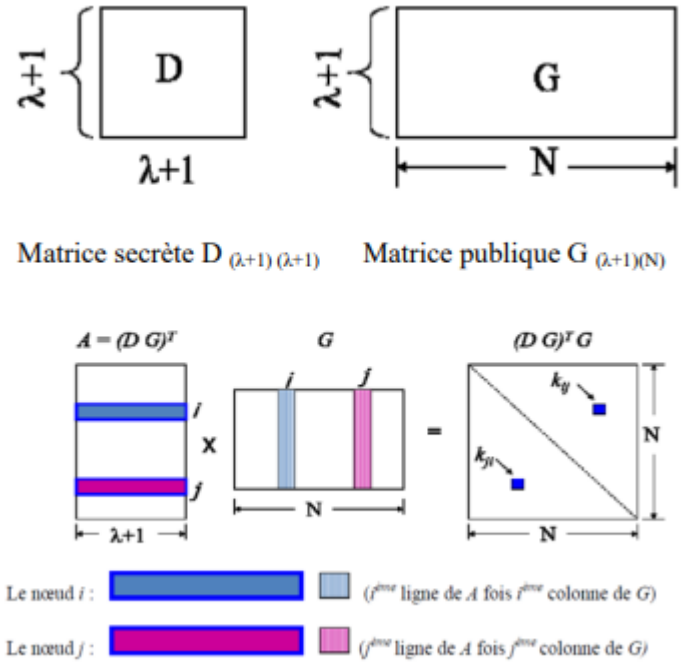

Figure2.14 : Méthode de Blom [13]

Blundo et autres [12] a présenté un schéma de gestion de clé basé sur un polynôme. Le composant de base de ce schéma est le polynôme symétrique bivariant de degré λ, $P(x,y)= \sum^{\lambda}_{i=0}\sum^{\lambda}_{j=0} a_{ij}x^iy^j$ qui est généré sur un corps fini GF(q), où nous avons P(x,y)=P(y,x) en choisissant $a_{ij}=a_{ji}$. Chaque nœud i est pré-chargé avec un polynôme P(i,y) Pour établir une clé par paire après le déploiement, chaque nœud évalue le polynôme à l'ID de l'autre nœud de capteur. Ainsi, deux nœuds i et j peuvent calculer la clé par paire entre eux en échangeant leur identification d'abord, puis peuvent tirer individuellement leur clé commune entre eux $K_{ij}=P(i,j) = P(j,i)$. Ce mécanisme polynômial assure que deux nœuds quelconques établissent une clé unique, la communication est réduite, la sécurité est parfaite quand pas plus de λ nœuds sont compromis où λ est le degré du polynôme. Le coût de stockage du polynôme est relatif au degré λ.

- **Schéma basé sur la pré-distribution d'une clé maîtresse**

Pour assurer le déterminisme, Une clé commune est pré-distribuée sur tous les nœuds avant leurs déploiements. Elle est employée afin de sécuriser les communications dans la phase d'établissement de clés, et qui sera effacée à la fin de cette phase.

Lai et al. [18] ont proposé le protocole BROSK (Broadcast Session Key). Dans ce schéma, une seul clé chargée dans les nœuds avant le déploiement. Une paire de nœuds peut être établie une clé de session à l'aide de cette clé principale et d'un nombre aléatoire échangé entre chaque capteur. Ce schéma présente une évolutivité infinie et chaque capteur n'a besoin que de très peu de mémoire. Cependant, l'inconvénient est évident. Lorsque la clé principale est compromise, toutes les clés paires sont exposées. Par conséquent, ce schéma n'a aucune résilience. En dehors de cela, il n'y a pas d'authentification car tous les capteurs ont la même clé principale.

Zhu et autres [13] proposent le protocole déterministe LEAP (Localized Encryption and Authentication Protocol). LEAP est un protocole de gestion de clés conçu pour les réseaux de capteurs hiérarchiques afin de limiter l'impact du nœud compromis sur le voisinage immédiat. Il prend en charge l'établissement de quatre types de clés pour chaque nœud capteur : une clé individuelle partagée avec la station de base, une clé par paire partagée avec un autre nœud capteur, une clé de cluster partagée avec plusieurs nœuds voisins et une clé de groupe partagée entre tous les nœuds du réseau. Avant le déploiement, la BS génère une clé maîtresse initiale et la stocke dans la mémoire de chaque nœud capteur. Lorsque la phase de déploiement est terminée, chaque nœud capteur dérive de cette clé sa propre clé individuelle

$K_u = f_{K1}(ID_u)$.Puis il diffuse un message « HELLO » contenant son identifiant ID à ses voisins. Lorsqu'il reçoit un « ACK » d'un voisin, il pourra vérifier son identité en calculant au début Kv ($Kv = f_{k1}(ID_u)$ et par suite le MAC. Une fois l'identité de vérifiée, calcule

sa clé unique partagée avec lui $Kuv = f_{kv}(ID_u)$. Le nœud pourra calculer cette clé de la même façon. Après que le temporisateur d'établissement de clé atteint sa valeur de seuil T min, le nœud supprime la clé maîtresse initiale et les clés individuelles de ses nœuds voisins. Il garde seulement sa clé individuelle et les clés uniques partagées avec ses voisins. Supposons que soit maintenant un chef de cluster qui souhaite envoyer une clé de cluster à ses nœuds voisins. Il génère au début une clé aléatoire ; puis il la chiffre à l'aide de la clé par paire partagée avec chaque nœud voisin avant de l'envoyer en unicast à ses voisin (membre de cluster). Cependant, la clé de groupe est pré-chargée à chaque nœud capteur avant le déploiement

2.7. Métriques d'évaluation

Plusieurs métriques peuvent affecter la gestion de clés en termes d'énergie, connectivité, scalabilité, etc. Par conséquent, cette section décrit les métriques les plus couramment employées pour évaluer les différents protocoles de gestion de clés proposés pour les réseaux de capteurs sans fils.

2.7.1. 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 :

- La puissance de calcul : est mesurée en termes de quantité de cycles de processeur nécessaires pour l'établissement de clés. Par exemple, la cryptographie à clé asymétrique n'est pas prise en compte en raison de la forte exigence de calcul.
- La capacité de communication : détermine le nombre de messages échangés requis pour la gestion de clés. Étant donné que la communication domine la consommation d'énergie des nœuds capteurs. Par conséquent, le nombre de messages doit être réduit que possible.
- L'espace de stockage : est la quantité de mémoire nécessaire pour stocker les informations de sécurité, telles que les clés (par exemple clés publique / privée, clés par paire) et le certificat d'utilisateur (par exemple, ID). La mémoire dans les nœuds

capteurs n'est que des dizaines de kilo-octets, ce qui implique que le schéma de gestion de clés ne peut pas stocker trop de clé dans les nœuds capteurs.

2.7.2. Résilience contre la capture de nœud

Une autre métrique qui doit être respecté est la résilience contre la capture de nœud. Quand un nœud est capture par un intrus, son secret entier ainsi que les liens établis avec ses voisins sont compromis. Les effets d'une telle attaque peuvent affecter d'autres nœuds dans le réseau. Dans ce cas il peut utiliser les informations stockées dans les nœuds capteurs compromis pour lancer des nouvelles attaques. Dans le contexte d'établissement de clés, l'adversaire peut essayer de déduire la clé partagée entre les nœuds capteurs non compromis. Les schémas probabilistes sont vulnérables aux compromissions des nœuds, du moment où les clés pré-charges dans les nœuds capteurs sont prélevées à partir du même pool. En outre, la résilience à la capture du nœud capteur change d'un schéma à un autre selon le nombre de clés requis pour l´établissement d'un lien sécurise. [18]

2.7.3. La connectivité

La connectivité de clé est définie comme la probabilité qu'une paire de nœuds puissent établir une clé commune entre eux. Elle produit lorsque le nombre important de nœuds dans un RCSF sont généralement dispersés de façon aléatoire, et ne sont pas uniformément répartis sur le champ de captage. Ce qui implique que certaines régions du champ de déploiement puissent bénéficier d'une meilleure connectivité. La connectivité locale prend en compte la connectivité entre toute paire de nœuds voisins, tandis que la connectivité globale fait référence à la connectivité de l'ensemble du réseau, 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. [18]

2.7.4. Passage à l'échelle (scalability)

Un réseau est dit 'scalable' si le réseau peut facilement être augmenté sans perdre ses propriétés essentielles ou sans réduire ses performances. En premier, 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. [17]

2.8. Conclusion

Nous avons abordé dans ce chapitre les objectifs de la sécurité, les attaques et les contremesures où nous présentons quelques solutions adaptées tel que les primitives cryptographiques et la gestion de clés dans les RCSF.

Nous avons déduit que la gestion des clés est l'un des secteurs les plus importants dans la sécurité des RCSFs, 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

Implémentation et évaluation d'un protocole de gestion de clés

3.1. Introduction

Les capteurs sans fil sont dotés de faible capacité en termes de calcul, d'énergie et d'espace de stockage. Les capteurs sont en effet faciles à corrompre afin de récupérer les informations qu'ils possèdent. 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. Dans le cadre de notre étude et après avoir abordé quelques protocoles et solutions de gestion de clés proposés pour les réseaux de capteurs sans fil, nous nous sommes intéressés par le travail [12] intitulé «SKWN : Smart and dynamic Key management scheme for hierarchical Wireless sensor Networks) " pour l'implémenter et vérifier leurs métriques de performances telles que le coût de communication, le coût de stockage et la consommation d'énergie.

Dans ce chapitre, nous présentons ce protocole qui a été développée par les auteurs du travail [13] et dédié pour une gestion de clés associée aux réseaux de capteurs ayant une topologie hiérarchique. Nous commencerons d'abord par présenter la motivation derrière ce choix, ensuite nous présenterons les détails fonctionnels de ce protocole. Nous évaluons par la suite leurs performances.

3.2. Motivation du choix du protocole

Plusieurs schémas de gestion de clés ont été proposés mais la conception d'un système de gestion de clés reste un problème difficile dans les réseaux de capteur sans fil en raison des contraintes liées aux ressources des nœuds capteurs, telles que la mémoire, la puissance de calcul et l'énergie. Après l'étude de certains protocoles existants dans la littérature, nous avons décidé d'implémenter et évaluer un protocole intitulé SKWN "Smart and dynamic Key management scheme for hierarchical Wireless sensors Networks"

 SKWN dédiée à une topologie hiérarchique en clusters des RCSF. Cependant, l'utilisation d'une topologie hiérarchique peut simplifier et améliorer la scalabilité et même améliorer l'efficacité de la procédure de gestion de clés;

 SKWN est déterministe et repose sur la cryptographie symétrique.

 SKWN est modifiable et évolutif;

 Robuste contre les attaques de capture de nœuds;

 Optimise la consommation d'énergie par l'utilisation des simples routines de calcul et un nombre réduit de messages afin d'établir les clés cryptographiques.

3.3. Spécifications générales sur le modèle du réseau

Dans notre travail, nous supposons une architecture de réseau hiérarchique basée sur le principe du clustering. Dans cette architecture, les nœuds capteurs sont déployés de manière aléatoire et uniforme. Pour organiser le réseau, les capteurs sont divisés en clusters comme montre la figure 3.1 où chaque cluster est géré par une tête de cluster (CH : Cluster Head), qui a la responsabilité de collecter et gérer les informations à partir de ces nœuds capteurs membres (CM : Cluster member), par la suite agréger ces données et les envoyer à la station de base (SB). La station de base gère le réseau et communique avec le monde extérieur.

Les nœuds capteurs sont homogènes en termes de capacité de traitement, de communication, d'énergie et de stockage. Cependant la station de base possède des ressources illimitées.

Les cluster-heads sont uniformément réparties dans le réseau et sont élues en fonction d'une métrique spécifique ou d'une combinaison de métriques, dont la valeur dépend de divers critères tels que la portée de communication, la localisation, les capacités en ressources et en énergie. L'énergie résiduelle de cluster-head est réduite lors des calculs et des communications. Il est donc essentiel de disposer des mécanismes de rotation du CH qui permettent de prolonger la durée de vie du CH et par conséquent du réseau.

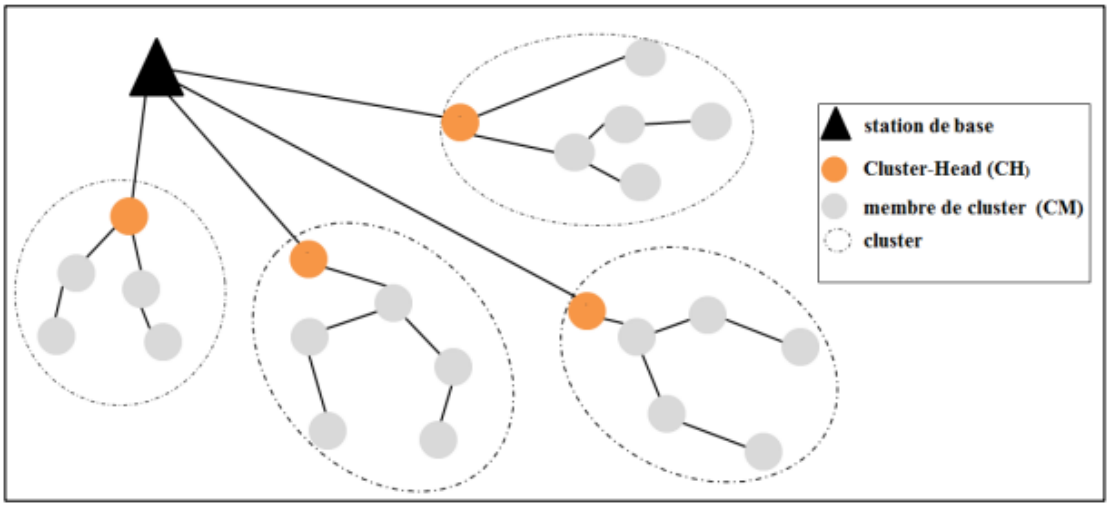

Figure 3.1 : Modèle d'architectures hiérarchique pour un RCSF

3.4. Description détaillée sur le fonctionnement du protocole

SKWN est un nouveau schéma de gestion de clés pour les réseaux de capteurs sans fil hiérarchiques. Il comprend trois sous-schémas dédiés à (1) a l'Établissement de clés, (2) Au Renouvellement de clés, et (3) à l'Intégration d nouveau nœud. Dans le cadre de notre étude, nous nous sommes intéressés au sous schéma lié à l'établissement de clés. Ce dernier permet

de gérer les clés cryptographiques avant et pendant le déploiement du réseau. Il s'appuie sur des clés pré-chargées. En effet, aucune clé secrète ne sera échangée via le réseau.
SKWN permet l'établissement sécurisé de clés sur la base d'un mécanisme cryptographique adaptatif prenant en compte l'environnement de déploiement et les menaces perçues.

3.4.1. L'établissement de clés

Avant le déploiement du RCSF, 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 d'installation de clés et sera effacée après le déploiement de clés. Nous avons détaillé dans ce qui suit chaque étape liée au sous-schéma d'établissement de clés:

3.4.1.1. La pré-distribution de clés

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

- Une clé K_{in} partagée avec la station de base pour chiffrer / déchiffrer les messages du nœud vers la station de base et les messages en sens inverse.
- Une clé K_r partagée par tous les nœuds du réseau, utilisée pour chiffrer / déchiffrer les messages juste après le déploiement.

Une fois les nœuds déployés, ils signalent d'abord leur emplacement physique à la station de base, puis le réseau commence à sélectionner les cluster-heads à l'aide des algorithmes de sélection des cluster-heads [18] [13]. Chaque nœud de capteur reçoit alors l'identifiant de leur CH.

3.4.1.2. L'étape d'installation de clés

Dans SKWN, deux fonctions sont appliquées aux messages afin d'assurer les objectifs de sécurité des communications. La première est la fonction $MAC_{K_r}\{\}$ (code d'authentification du message), utilisée pour authentifier les données envoyées. La deuxième est la fonction $E_{K_r}\{\}$, utilisée pour chiffrer les données envoyées. Tandis que, RC5 est utilisé comme algorithme de chiffrement dans ces deux fonctions. Egalement, un nonce (N_S) est utilisé, non seulement pour vérifier l'intégrité du paquet envoyé, mais également pour calculer les clés partagées. De plus, le paramètre Lev est utilisé pour déterminer le niveau de sécurité par rapport aux besoins

de sécurité. Le type du message est également envoyé dans le paquet afin de déterminer son objectif.

Dans cette approche, l'établissement de clés est considéré pendant une courte période, notée T_{min} . En effet, la probabilité de compromettre un nœud pendant cette période est négligeable. Les étapes suivantes sont effectuées par les nœuds capteur (nœud CH ou nœud CM) afin de s'assurer que des clés distinctes sont établies sur tous les nœuds.

Tableau 3.1 : Acronymes définition

Notation	Explication
id_{CM_j}	Identificateur de membre de cluster j
id_{CH_α}	Identificateur de cluster-head α
id_{BS}	Identificateur de la station de base
L_id_{CM}	Liste contenant les identifiants des nœuds membres du cluster
$E_K(M)$	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
Lev	Niveau de sécurité pour chaque application
CPT	Compteur reflète le nombre de renouvellement de clés
$S \rightarrow *: M$	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

Étape 1. Les cluster-heads lancent la phase d'établissement de clés en diffusant un message $HELLO$ contenant leur identifiant. Ils initient un Timer qui sera déclenché après le temps T_{min}.

$$CH_\alpha \rightarrow *: id_{CH_\alpha} \parallel Lev \parallel E_{K_r}\{HELLO, N_{CH_\alpha}\} \parallel MAC_{K_r}\left\{id_{CH_\alpha} \parallel Lev \parallel E_{K_r}\{HELLO, N_{CH_\alpha}\}\right\}$$

Étape 2. Après avoir reçu le message d'initiation de leur cluster-head, le nœud CM authentifie le message $HELLO$ (en vérifiant le MAC) et calcule la clé par paire à l'aide de l'équation suivante:

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

Ils répondent ensuite par le message $HELLO\_REP$ qui contient leur identifiant

$$CM_j \rightarrow *:$$

$$id_{CM_j} \| id_{CH_\alpha} \| E_{K_r}\{HELLO\_REP, N_{CM_j}\} \| MAC_{K_r}\left\{id_{CM_j} \| id_{CH_\alpha} \| E_{K_r}\{HELLO\_REP, N_{CM_j}\}\right\}$$

Étape 3. Après la réception du message $HELLO\_REP$, chaque nœud CH commence par vérifier l'authenticité du message (en vérifiant le MAC) et identifie ensuite l'ensemble des capteurs qui se trouvent dans le même cluster. Ils diffusent ensuite un message de requête contenant la liste L_id_{CM} aux autres CH.

$$CH_\alpha \rightarrow *: id_{CH_\alpha} \| Lev \| E_{K_r}\{HELLO\_REQ, N_{CH_\alpha}, L_{\_id_{CM}}\}$$

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

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.

Étape 4. Chaque nœud CM, après avoir vérifié l'authenticité du message $HELLO\_REP$ des autres nœuds CM, identifie les nœuds membres appartenant au même cluster. Il calcule ensuite la clé par paire partagée avec chaque nœud membre.

$$K_{CM_i - CM_j} = H_{K_r}\left(\min\left(id_{CM_i}, id_{CM_j}\right) \| N_{CM_i} \oplus N_{CM_j}\right) \quad (3.2)$$

Étape 5. 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.

$$K_{CH_\alpha - CH_\beta} = H_{K_r}(max\ (id_{CH_\alpha}, id\ _{CH_\beta}) \| min\ (id_{CH_\alpha}, id\ _{CH_\beta}) \| N_{CH_\alpha} \oplus N_{CH_\beta}) \quad (3.3)$$

Pour chaque interaction dans la phase d'installation, un MAC de message nécessite 4 octets, 2 octets pour les identifications de source et de destination et 1 octet pour le niveau de sécurité. Nous considérons également 8 octets pour les données cryptées. Lorsque les données cryptées correspondent au type de message et au nonce, nous avons respectivement besoin de 1 et 4 octets. Dans le cas où le message diffusé contient la liste d'identification L_id_{CM} de l'ensemble des nœuds membres, la taille des données cryptées dépend non seulement du type de message et du nonce, mais également du nombre de nœuds CM dans chaque cluster. Par conséquent, la taille du message pour $HELLO$ et $HELLO\_REP$ est respectivement de 15 et 16 octets.

Selon les étapes décrites ci-dessus, tous les nœuds CH et CM du réseau établissent des clés distinctes. Dans cette phase, chaque taille de clé est de 8 octets. La figure 3.2 résume le processus d'établissement de clés.

3.4.1.3. Effacement de clés

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

$$K_{in} = H_{K_{in}}{}^{CPT}(K_{in}) \tag{3.4}$$

$$K_r = H_{K_r}{}^{CPT}(K_r) \tag{3.5}$$

CPT est un compteur, initialisé à zéro, qui reflète le nombre de renouvellements de clés. Le CPT dans ce cas est égal à 1.

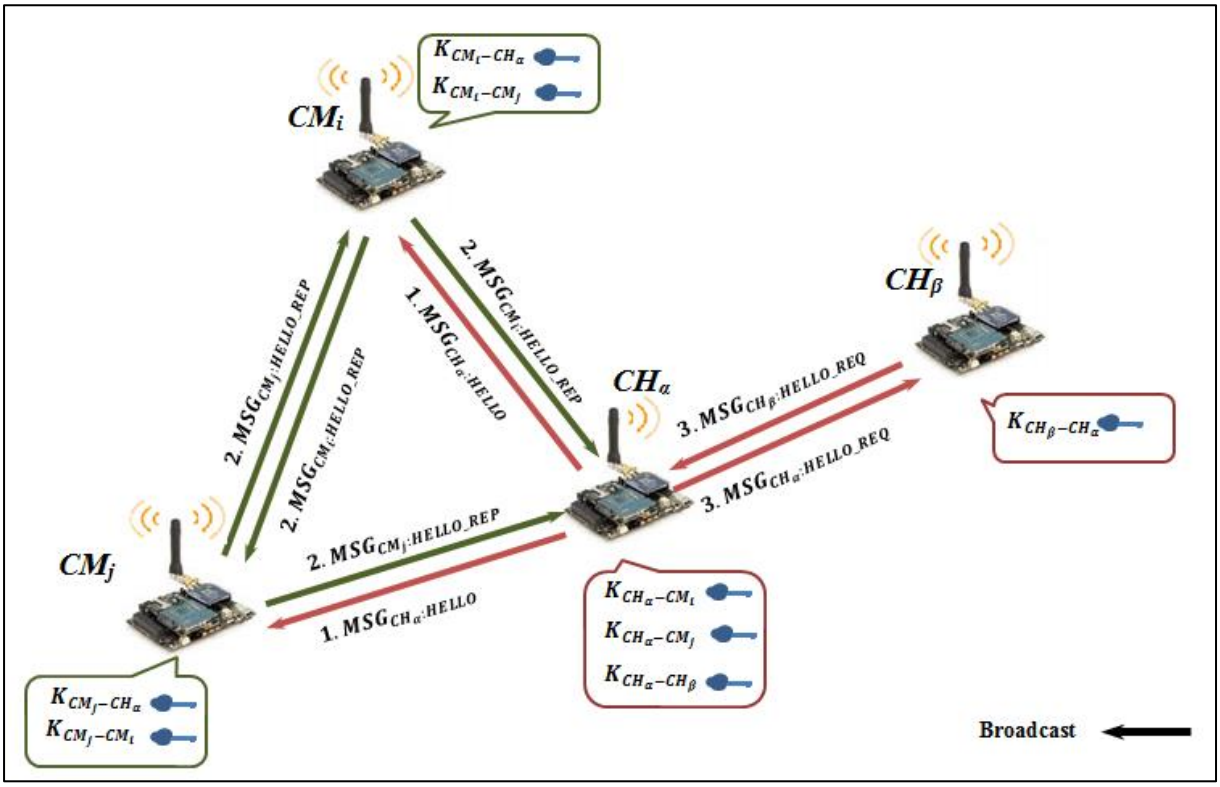

Figure 3.2. Le processus d'établissement de clés

3.5. Description de l'approche SC-SPK:

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 hiérarchique en clusters. Ce système reposé sur la pré-distribution de clés partielles et la cryptographie symétrique. Le processus de déroulement de SC-SPK est divisé en trois phases qui sont : la pré-distribution de 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 ID au cluster-head CH_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 cluster C_i. Ensuite, chaque cluster-head CH_i diffuse la liste L_i à tous les nœuds membres du cluster C_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 processus de cette phase.

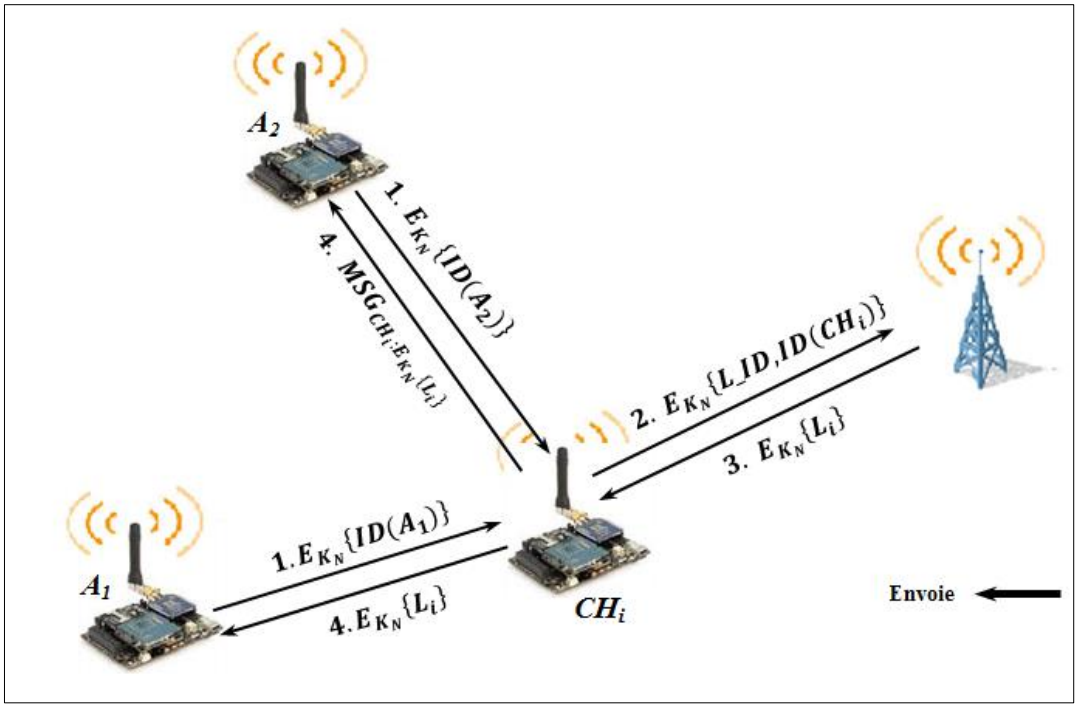

Figure 3.3 : Le processus de la phase de formation du cluster [12]

- **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.

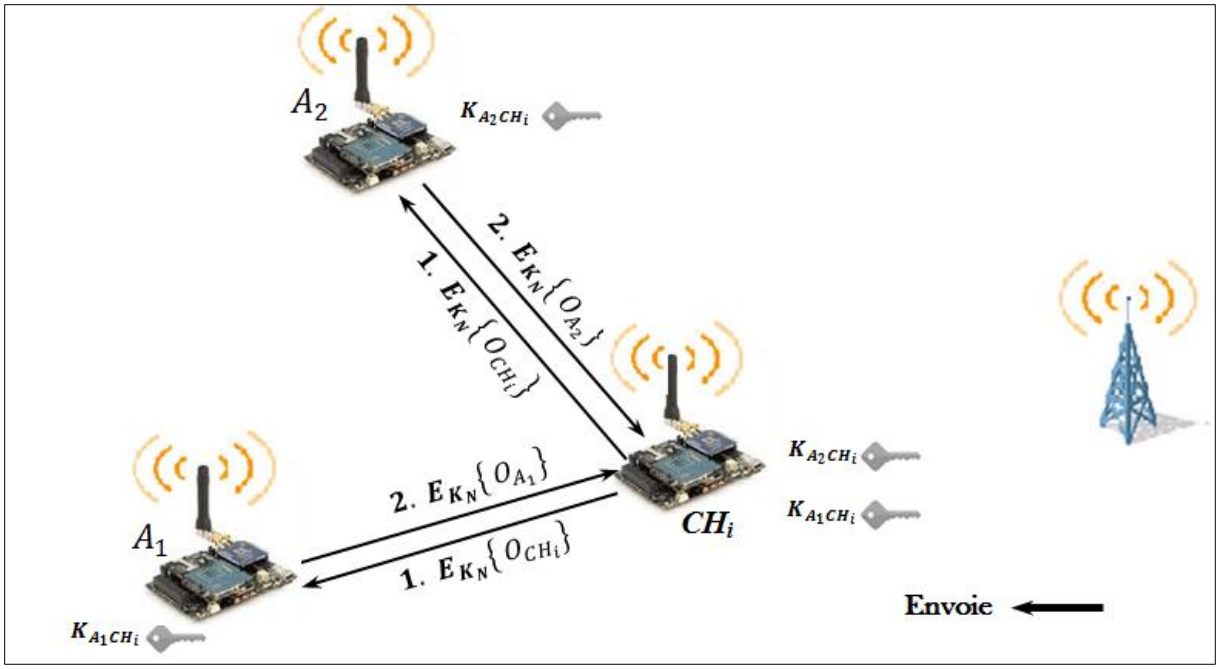

Figure 3.3 : Le processus de la phase d'état stable [12]

3.6. 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.

3.6.1. Présentation de l'environnement Tinyos

On a choisi le système Tinyos pour réaliser notre simulation. Il est adapté aux capteurs. Il supporte de nombreuses plates-formes et il fournit des concepts très importants pour réaliser les simulations.

La nomination TinyOS indique d'une part un système d'exploitation conçu particulièrement pour les RCSFs et qui doit être installé sur chaque nœud capteur du réseau. D'une autre part, TinyOS indique l'environnement de simulation d'applications de RCSFs qui tournent sous le système d'exploitation TinyOS. Cet environnement est formé par le simulateur TOSSIM, le système d'exploitation TinyOS, l'émulateur Cygwin et tout un ensemble d'outils de simulation. Dans ce contexte, nous présentons dans cette partie l'environnement TinyOS sur lequel fonctionne le simulateur TOSSIM [13]

- **TinyOS**

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

- **Cygwin**

La principale plate-forme de notre environnement est Cygwin. En effet, c'est à travers cette plateforme que nous pouvons communiquer avec TinyOS depuis Windows. Cygwin est une collection de logiciels libres, permettant à différentes versions de Windows de Microsoft d'émuler un système Unix. En fait, il tente de créer un environnement Unix sous Windows, rendant possible l'exécution de ces logiciels après une simple compilation.

- **Le simulateur TOSSIM**

TOSSIM est un outil très puissant a été développé et proposé pour TinyOS. Le but principal de TOSSIM est de créer une simulation très proche de ce qui se passe dans les RCSFs dans le monde réel. Une économie d'effort et une préservation du matériel sont possibles grâce à cet outil. TOSSIM est souvent utilisé en conjonction avec une interface graphique appelée TinyViz qui permet à l'utilisateur de visualiser le déroulement de la simulation. En outre, il a une extension Power TOSSIM, qui permet de simuler et évaluer la consommation d'énergie des différents nœuds capteurs du réseau.

3.6.2. Environnement de simulation et résultats

Afin d'évaluer les performances de SKWN, nous l'avons implémenté en utilisant le langage de programmation NesC et ce afin de 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 SKWN avec SC-SPK.

Pour le modèle de simulation, nous utilisons plusieurs réseaux d'une taille variant de 30 à 150 nœuds de type MICA2 dispersés aléatoirement sur une surface de 150 × 150 m. Environ 10% de ces nœuds sont des cluster-Head (CH). La portée radio d'un capteur est de 22 mètres, la taille d'un paquet de données est de 31 octets et le taux d'erreur de transmission est de 0.

3.6.2.1. 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 SKWN, pour un réseau de N nœuds comportant C clusters de n membres, chaque CH diffuse un message, reçoit n messages de ses membres 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 de leur CH, diffuse un message en réponse, puis reçoit $(n-1)$ messages des autres membres du même cluster.

Comme la montre la figure 3.4, comme le nombre des nœuds augmente, le coût de communication n'est pas affectée par l'évolution du nombre des nœuds et ceci pour CH et CM. Alors que dans SKWN, 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.

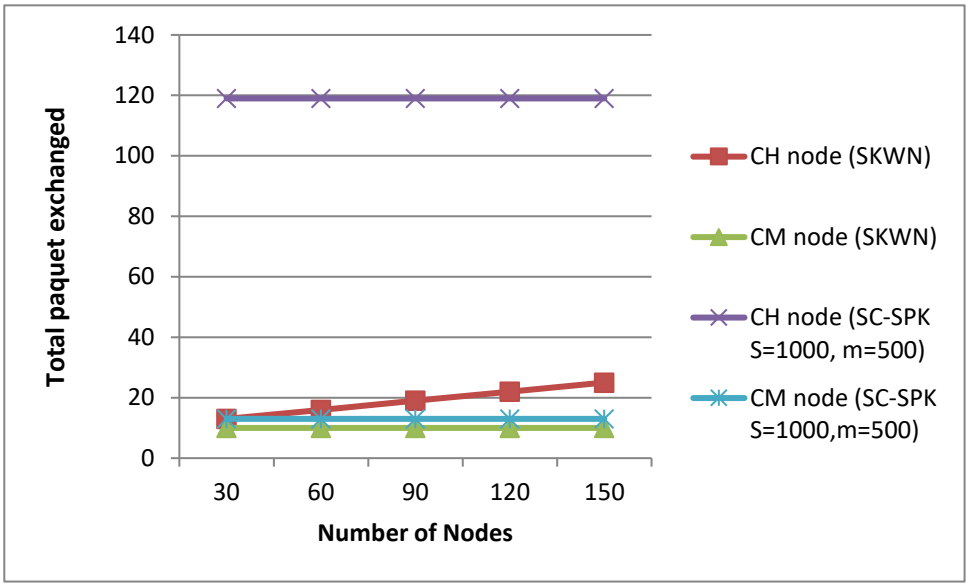

Figure 3.4. Comparaison du nombre de paquets échangés.

3.6.2.2. Le coût de stockage

Nous nous intéressons au nombre de clés stockées dans chaque type de nœud, car la taille d'espace mémoire exploité est fortement reliée au nombre de clés stockées. La figure 3.5 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 SKWN. 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 SKWN, 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 n clés.

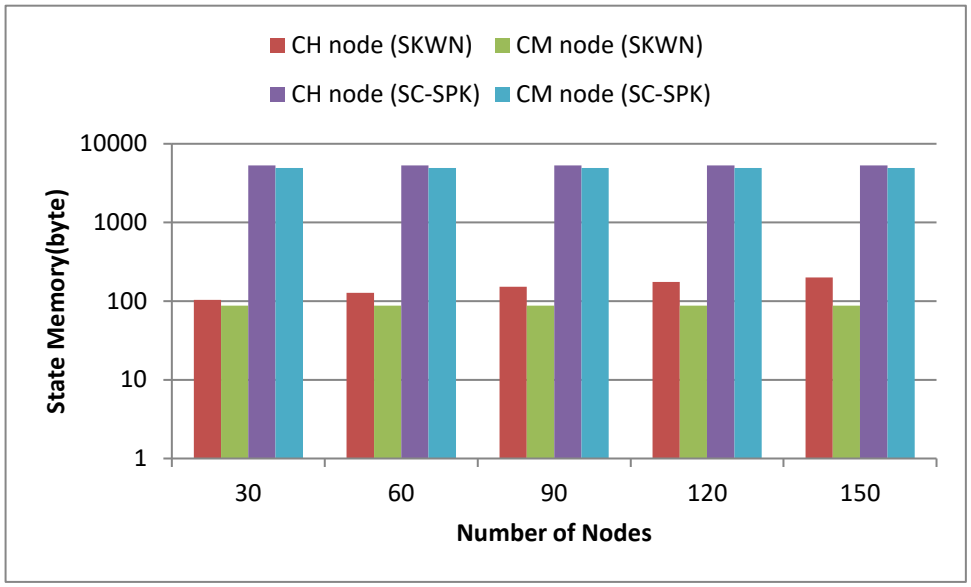

Figure 3.5 : L'utilisation de la mémoire par un nœud capteur

3.6.2.3. 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 3.6 montre la variation de l'énergie consommée par SKWN et SC-SPK en fonction de la taille de réseau.

Il est évident que l'énergie consommée par SKWN est négligeable par rapport à celle liée au SC-SPK. En effet, dans SKWN, 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.

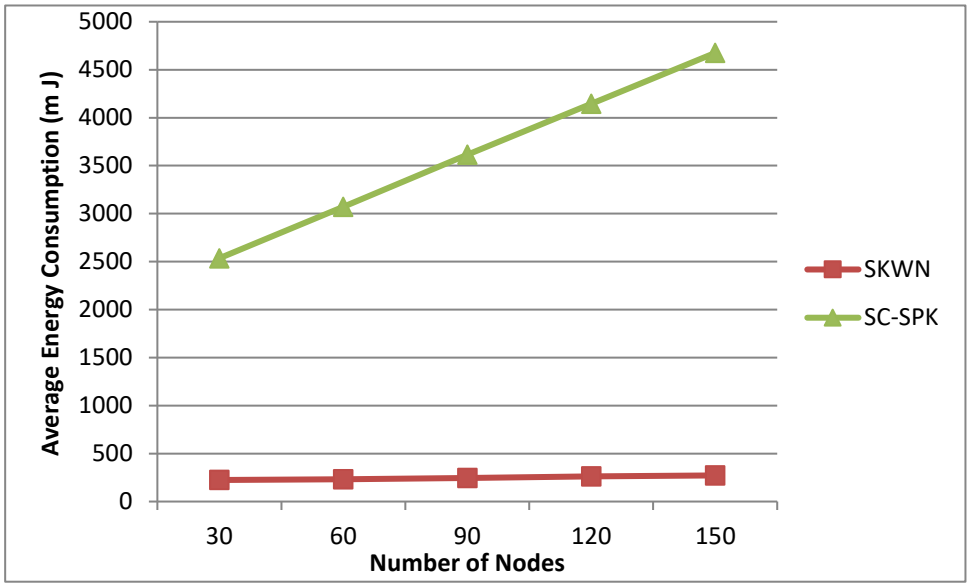

Figure 3.6 : La consommation d'énergie par un nœud capteur

3.7. Conclusion

Dans ce chapitre, nous avons présenté le processus d'implémentation ainsi que l'évaluation d'une approche de gestion de clés destinée aux réseaux de capteurs sans fil hiérarchiques. Le système d'exploitation TinyOS a été d'ailleurs utilisé. Nous avons proposé une programmation entière en langage NesC et une simulation avec TOSSIM. L'approche implémenté appelée SKWN (Smart and dynamic Key management scheme for hierarchical Wireless sensor Networks) permet à chaque nœud capteur d'établir une clé par paire symétrique secrète pour l'échange de données avec son cluster-head. SKWN est déterministe et basé sur la cryptographie symétrique.

Après des études expérimentales effectuées sur la consommation d'énergie, le coût de communication et le coût de stockage, nous avons constaté que le protocole SKWN répond bien aux critères de performances souhaités du réseau, tout en assurant un niveau de sécurité très élevé.

Conclusion générale

Les réseaux de capteurs sans fil ont émergé suite à des besoins militaires tels que la surveillance sur le terrain de combat. Puis, ils ont trouvé leur chemin pour des applications civiles. Aujourd'hui, les réseaux de capteurs sans fil sont devenus une technologie clé pour les différents types « d'environnements intelligents ». De nos jours, ils nous aident par exemple à avoir un bon système de sécurité à la maison.

De tels usages ne peuvent être mis en œuvre sans garantir une sécurité stricte de réseau, assurant la confidentialité, l'authentification, l'intégrité des communications.

La gestion de clés est un service primordial pour la sécurité de n'importe quel système basé sur la communication. Sous les contraintes des RCSFs, la conception d'un système de gestion de clés est un grand défi.

Dans le cadre de notre étude et après avoir abordé quelques protocoles et solutions de gestion de clés proposés pour les RCSFs, nous nous sommes intéressés par le travail [1] intitulé " SKWN : Smart and dynamic Key management scheme for hierarchical Wireless sensor Networks ". Dans ce travail les auteurs ont développé une approche pour la gestion de clés. Cette dernière est dédiée à une topologie hiérarchique en clusters. Il permet à chaque nœud capteur d'établir une clé par paire symétrique secrète pour l'échange de données avec son cluster-head. Le protocole SKWN est déterministe et basé sur la cryptographie symétrique.

Nous avons évalué les performances du protocole SKWN en fonction de trois métriques importantes: le coût de communication, le coût de stockage et la consommation d'énergie. Pour de meilleurs résultats d'évaluation, les performances de protocole SKWN sont expérimentées sur un environnement de test proche du réel (Tinyos).

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 SKWN répond bien aux critères de performances souhaités du réseau, tout en maintenant un niveau de sécurité très élevé.

BLIOGRAPHIE

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

[2] https://moodle.utc.fr/file.php/498/SupportWeb/co/Module_RCSF_10.html

[3] https://images.app.goo.gl/xgVy9QAi1DDnEwCE8

[4] https://moodle.utc.fr/file.php/498/SupportWeb/co/Module_RCSF_14.html

[5] https://moodle.utc.fr/file.php/498/SupportWeb/co/Module_RCSF_7.html

[6] http://www.snm.ethz.ch/ [En ligne; accédé Avril 2017].

[7] https://www.semanticscholar.org/paper/Compression-d%27images-dans-les-r%C3%A9seaux-de-capteurs-Makkaoui/162c059de89d7900412a4fb0fa894f386a2745a2

[8] https://tel.archives-ouvertes.fr/tel-01531464 Submitted on 1 Jun 2017

[9] https://www.iot-lab.info/hardware/wsn430/ [En ligne; accédé Avril 2017].

[10] https://elearning-facsci.univ-annaba.dz/pluginfile.php/29291/mod_resource/content/1/Ch%20II-Caract%C3%A9ristiques%20m%C3%A9trologiques%20des%20capteurs.pdf

[11] R. Verdone, D. Dardari, G. Mazzini, and A. Conti, "WirelessSensor and Actuator Networks Technologies, Analysis and Design", London,UK, Elsevier, 2008.

[12] https://www.ummto.dz/dspace/bitstream/handle/ummto/12747/OubazizAli.pdf?sequence=1

[13] N. Hadjira, R. Souhila, "Implémentation et évaluation d'un protocole de gestion de clé dédié aux réseaux capteurs sans fils (RCSF)", Système des télécommunications, Université Amar Thelidji-Laghouat, 2020/2021

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

[15] https://moodle.utc.fr/file.php/498/SupportWeb/co/Module_RCSF_67.html

[16] W. ZNAIDI, “ Quelques propositions de solutions pour la sécurité des réseaux de capteurs sans fil”, thèse de doctorat en informatique, L'Institut National des Sciences Appliquées de Lyon, France, 2010

[17] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, et P. Spilling, « A survey ofkey management in ad hoc networks », *IEEE Communications Surveys & Tutorials*, vol. 8, no 3, p. 48–66, 2006.

[18] Z. BELKHEDIM, S. DEKKICHE «*Implémentation d’un protocole de sécurité dans les réseaux de capteurs sans fil »*, SYSTEMES DE TELECOMMUNICATIONS, 2020