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 : Madani Safia & Soumani Khawla

DOMAINE : Science et Technologie

FILIERE : Télécommunication

OPTION : Systèmes de télécommunications

Thème

Analyse et évaluation des mécanismes de renouvellement de clés dans le protocole SKWN

Jury de soutenance :

Nom et Prénom	Grade	Qualité
MESMOUDI Samira	MCB	Encadrante
MERAH Lahcane	MCA	Président
CHAKER Mohsen Nacer Saleh	MCB	Examinateur

Promotion : 2022/2023

REMERCIEMENTS

En préambule à ce mémoire, nous tenons tout d'abord à remercier ***ALLAH*** *le tout puissant et miséricordieux, qui nous aide et qui nous a donné la force, le courage et la patience d'accomplir ce Modeste travail.*

Nos vifs remerciements vont aux membres du jury ; monsieur le président Dr. BIRANE Mouhoub pour l'intérêt qu'il est porté à notre recherche en acceptant de scruter notre travail Et de l'enrichir par leur propositions.

Nos sincères remerciements vont également s'adressent à monsieur l'examinateur Dr. CHAKER Mohsen Naser Saleh pour son aide, sa disponibilité, ses compétences scientifiques, son soutien et sa gentillesse.

Nos remerciements s'étendent également à tous nos enseignants durant les années des études.

En second lieu, nous tenons à remercier notre encadrante Dr. MESMOUDI Samira, pour son précieux conseil et son aide durant toute la période du travail.

Nous remercions nos très chers parents qui ont toujours été là pour nous.

Enfin, nous tenons également à remercier toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

Merci à tous et à toutes.

Dédicace

A mes très chers parents (Mon Père Belgacem, Ma Mère Nakhla.k) qui m'ont guidé durant les moments les plus difficiles de ce long chemin, pour leur sacrifice durant toute leur vie afin de me voir devenir ce que je suis.

A ma sœur Hanane et mes frères
Fares,naceur ,Abdelkader,haouari et Hamza

A ma chere Aissa , je te remercie du fond du cœur.

A mes amis Anfal , Yassmine et Assma .

Et bien sur sans oublier toutes les personnes qui m'ont soutenu durant mon cursus de formation

Madani Safia

Dédicace

Je dédie ce modeste travail a :
A mes parents, grâce à leurs tendres encouragements et leurs grands sacrifices, ils ont pu créer le climat affectueux et propice à la poursuite de mes études.
A mes sœurs et mon frère.
A toute mes amies et mes collègues.

Soumani Khaoula

Résumé

Les applications militaires de traçage, la surveillance des habitats, la surveillance et l'agriculture de précision ne sont que quelques exemples d'une vaste gamme d'applications possibles de la surveillance continue offerte par les RCSF. Malheureusement, les RCSF ne sont pas parfaits ! En raison de leurs ressources limitées et de leur déploiement dans des zones parfois hostiles, ces réseaux sont vulnérables à différents types d'attaques. Par conséquent, la sécurisation des communications représente l'un des défis les plus importants pour les réseaux de capteurs sans fil. Cette sécurité est généralement assurée par le chiffrement des données transmises. En effet, il serait inutile d'intégrer des algorithmes cryptographiques dans un système si la gestion des clés correspondantes n'est pas satisfaisante.

Dans le cadre de ce projet de fin d'études et après avoir examiné plusieurs protocoles et solutions de gestion de clés proposés pour les RCSF, nous avons choisi d'implémenter et de vérifier les métriques de performance du protocole SKWN pour le renouvellement des clés. Les résultats présentés dans ce mémoire sont issus de plusieurs simulations, qui démontrent que le renouvellement des clés du SKWN répond bien aux critères de performance souhaités par les réseaux RCSF, tout en réduisant les risques de compromission de la sécurité.

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

Abstract:

Military tracking applications, habitat monitoring, surveillance, and precision agriculture are just a few examples of the wide and varied range of possible applications of continuous monitoring offered by RCSFs (Wireless Sensor Networks). Unfortunately, RCSFs are not perfect! Due to their limited resources and deployment in sometimes hostile areas, these networks are vulnerable to different types of attacks. Therefore, the need to secure communications represents one of the most important challenges in wireless sensor networks. This security is generally ensured by encrypting the transmitted data. Indeed, it would be pointless to integrate cryptographic algorithms into a system if the corresponding key management is not satisfactory.

As part of this end-of-studies project, after discussing some key management protocols and solutions proposed for RCSFs, we have chosen to implement and verify the performance metrics of the key renewal protocol, SKWN. The results presented in this thesis are derived from several simulations, which demonstrate that the key renewal of SKWN meets the desired performance criteria for RCSF networks, while reducing the risk of compromising security.

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

ملخص

التطبيقات العسكرية للتعقب ومراقبة الموائل والمراقبة والزراعة الدقيقة هي مجرد أمثلة قليلة لمجموعة واسعة من التطبيقات الممكنة للمراقبة المستمرة التي تقدمها شبكة RCSF لسوء الحظ، RCSF ليست مثالية! نظرًا لمواردها المحدودة وانتشارها في مناطق معادية في بعض الأحيان، لذلك هذه الشبكات عرضة لأنواع مختلفة من الهجمات. لذلك ، يمثل تأمين الاتصالات أحد أهم التحديات التي تواجه شبكات الاستشعار اللاسلكية. يتم ضمان هذا الأمان بشكل عام عن طريق تشفير البيانات المرسلة. في الواقع ، سيكون من غير المجدي دمج خوارزميات التشفير في نظام إذا كانت إدارة المفاتيح المقابلة غير مرضية.

كجزء من مشروع نهاية الدراسات هذا وبعد مراجعة العديد من بروتوكولات وحلول الإدارة الرئيسية المقترحة لـ RCSF ، اخترنا تنفيذ والتحقق من مقاييس الأداء لبروتوكول SKWN لتجديد المفتاح. تأتي النتائج المقدمة في هذه الأطروحة من عدة عمليات محاكاة، والتي توضح أن تجديد المفاتيح SKWN يفي بمعايير الأداء التي تريدها شبكات RCSF ، مع تقليل مخاطر اختراق الأمان

الكلمات المفتاحية: شبكات الاستشعار اللاسلكية ، الأمن ، إدارة المفاتيح ، التشفير، تجديد المفتاح

Table des matières

Liste des figures

Liste des tableaux

Introduction générale

L'essor des nouvelles technologies ainsi que les progrès effectués dans les domaines des micro-électroniques, des télécommunications, des réseaux et du traitement de l'information ont permis de produire à coût raisonnable des capteurs de quelques millimètres cubes de volume, susceptibles de fonctionner en réseau appelé communément réseau de capteur sans fil (RCSF).

Dans un scénario d'application classique, les capteurs sont déployés dans un champ d'intérêt afin de mesurer certains phénomènes physiques et de faire remonter les informations collectées à une station de base, nommée le nœud puits. Ce dernier a plus de ressources que les autres nœuds et peut traiter les informations reçues localement. Le nœud puits est administré par un utilisateur via un réseau externe (internet, satellite, etc.).

Durant les deux dernières décennies, une attention particulière a été accordée aux réseaux de capteurs sans fil. En effet, ils ont été largement utilisés dans différents domaines d'application : militaire, contrôle industriel, surveillance environnementale, santé, la surveillance domestique et des maisons.

La sécurité est une nécessité pour la majorité des applications qui utilisent les RCSFs, notamment si les nœuds capteurs sont déployés dans des endroits peu sûrs, tels que les champs de bataille, les lieux stratégiques (aéroports, bâtiments critiques, etc.). Ces nœuds capteurs qui opèrent dans des lieux difficiles d'accès, sans protection et sans possibilité de rechargement de batterie, peuvent être soumis à des actions perturbatrices. De plus, l'environnement de communication sans fil permet d'écouter et d'espionner le trafic échangé dans le réseau, ce qui ouvre l'horizon pour lancer plusieurs types d'attaques. Par conséquent, assurer la sécurité des échanges des données au sein des RCSFs est une tâche importante et en même temps difficile.

En effet, les nœuds de capteurs sont généralement dotés de ressources très limitées en termes d'énergie, de capacité du calcul, d'espace du stockage de données et de débit de transmission, ces limitations 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 symétrique. 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.

La gestion des clés est le processus par lequel des clés cryptographiques sont produites, enregistrées, protégées, transférées, chargées, employées, et détruites.

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 [2] 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 garantir la sécurité et le renouvellement de clés dans les RCSFs, ce qui réduit les risques de compromission de la sécurité.

Nous avons choisi le mécanisme de renouvellement de clés de cette approche pour l'implémenter et vérifier leurs métriques de performances telles que 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 est une introduction et généralités sur les réseaux de capteurs sans fil : leurs définitions, leurs caractéristiques ainsi que leurs architectures et leurs domaines d'application sont présentés.
- Le deuxième chapitre sera dédié à la sécurité dans les RCSFs : les objectifs de la sécurité, les attaques et contremesures, les principaux concepts cryptographiques. Il décrit aussi quelques méthodes et protocoles concernant la gestion de clés proposés pour les RCSFs.
- 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

Généralités sur les réseaux de capteurs sans fil

1.1. Introduction

Les réseaux de capteurs sans-fil sont des systèmes distribués spécialement, composés de plusieurs dizaines de milliers de micro-capteurs. Ces entités sont généralement reliées par des réseaux de communication sans-fil. Dans tels réseaux les liens sont asymétriques, la topologie est dynamique, la bande passante limitée et aucun organe dédié au routage n'est présent. Il est donc rendu plus difficile que dans les réseaux filaires traditionnels.

Dans ce qui suit, on étudiera ce type de réseaux sans-fil et nœud de capteur sans fil. En outre, l'architecture de communication dans les réseaux de capteurs sera détaillée ainsi que l'ensemble de facteurs influant sur sa conception. On présentera à la fin le domaine d'application qu'utilise ce type de réseau.

1.2. Un nœud capteur sans fil

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

Un capteur est un système embarqué capable de récolter une valeur physique environnementale (température, pression,…) selon l'application pour laquelle il est conçu. Un capteur est composé de quatre unités qui lui permettent l'accomplissement de tâches de sensation, de calcul et de communication. Un capteur collecte des grandeurs physiques qu'il convertit en données numériques. Ces dernières seront par la suite envoyées directement à la SB dans leur état brut ou après avoir subi un traitement donné, et ce, pour les utiliser à des fins de commande [2].

Un nœud capteur (dit "mote" en anglais) est composé principalement d'un processeur, une mémoire, un émetteur/récepteur radio, un ensemble de capteurs, et une pile (voir figure 1.1). Il existe plusieurs modèles commercialisés dans le marché. Parmi les plus célèbres, les "mote" MICAx et TelosBe de Crossbow [1].

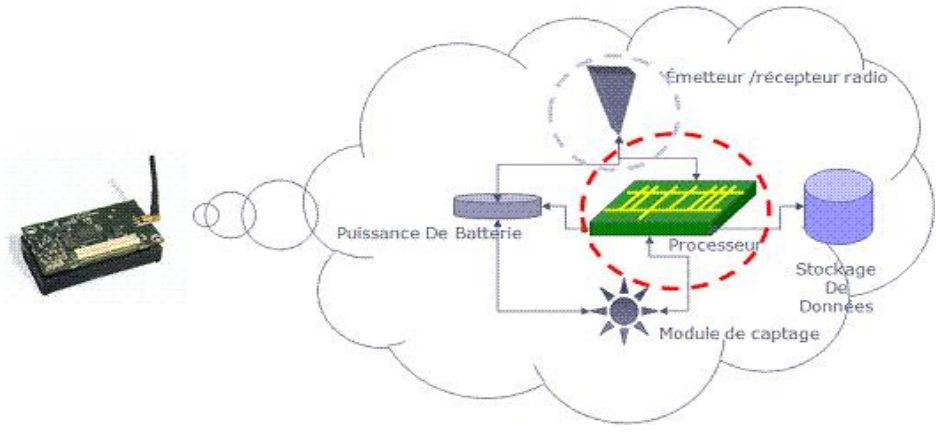

Figure1.1: Anatomie d'un nœud capteur

Les figures suivantes illustrent les composants d'un nœud capteur TelosB de CrossBow :

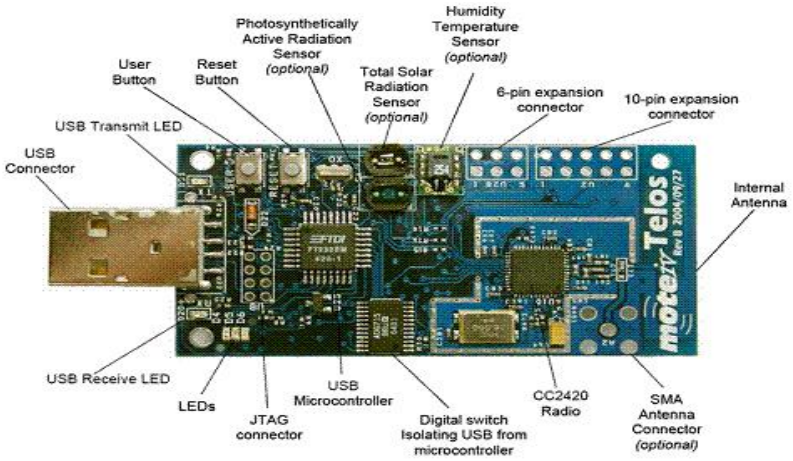

Figure1.2 : TelosB Recto [1]

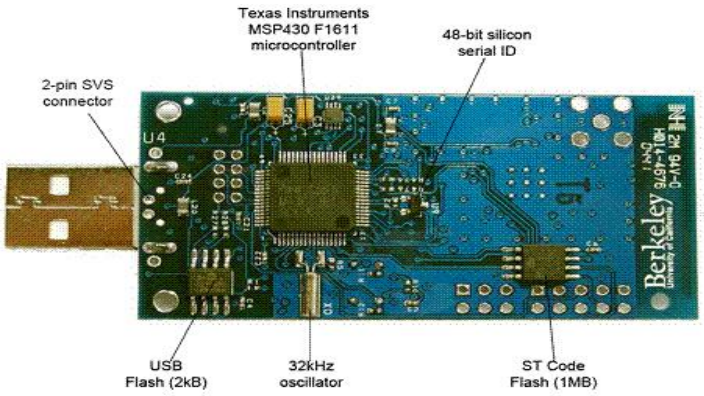

Figure1.2: TelosB Verso [1]

1.2.2. Architecture interne d'un capteur sans fil

L'architecture matérielle d'un nœud capteur est constituée de différents blocs, qui sont représentés sur la figure 1.4

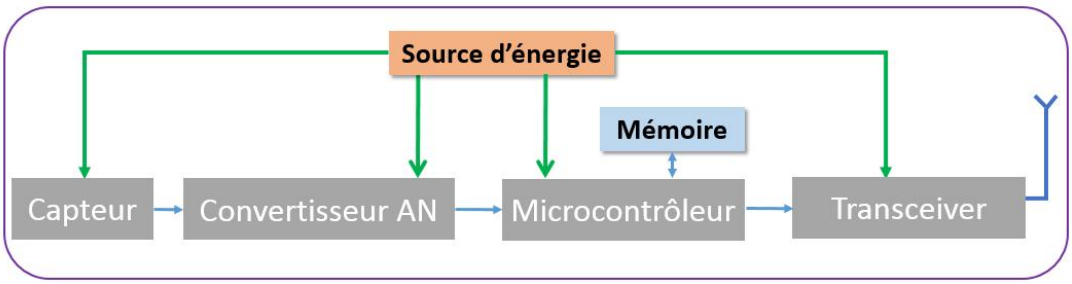

Figure 1.3: Architecture interne d'un capteur sans fil

La base de cette architecture repose sur l'alimentation du capteur à travers l'utilisation de piles ou de batteries. Cette alimentation assure le fonctionnement des autres blocs. Le rôle du convertisseur analogique numérique (AN) est de convertir les données mesurées par le capteur en données numériques. Ces dernières sont exploitables par la partie logicielle du nœud, qui est constituée d'un microcontrôleur et d'une partie mémoire pour le stockage de données. En, l'interface radio ou le transceiver permet de communiquer les informations acquises par le capteur commun a un autre nœud ou à une station de base. Un capteur est composé de 3 unités [3]:

1.2.2.1. l'unité d'acquisition

L'unité d'acquisition est composée d'un capteur qui va obtenir des mesures numériques sur les paramètres environnementaux et d'un convertisseur Analogique/Numérique qui va convertir l'information relevée et la transmettre à l'unité de traitement.

1.2.2.2. l'unité de traitement :

L'unité de traitement est composée de deux interfaces, une interface pour l'unité d'acquisition et une interface pour l'unité de transmission. Cette unité est également composée du processeur et d'un système d'exploitation spécifique. Elle acquiert les informations en provenance de l'unité d'acquisition et les envoie à l'unité de radiocommunication.

1.2.2.3. l'unité de transmission :

L'unité de transmission est responsable de toutes les émissions et réceptions de données via un support de communication radio.

1.2.3. Plates -formes existantes

Comme un certain nombre de technologies connues à ce jour, les nœuds de capteurs sans fil doivent être nés d'un projet militaire, ce qui entrave la mise en place d'un chrono graphie précise de leur développement. Cependant, le titre du premier prototype de nœuds de capteurs sans fil identifiable dans la bibliographie correspond sans aucun doute au module LWIM (Low-power Wireless Integrated Micro sensors) développé dans le milieu des années 90 par l'Agence pour les Projets de Recherche Avancée de Défense (DARPA) des Etats-Unis et l'UCLA. Il s'agissait d'un géophone équipé d'un capteur de transmission radio fréquences et d'un contrôleur PIC. Depuis un peu plus de 10 ans, la technologie des capteurs sans fil a beaucoup évolué. Les modules deviennent de plus en plus petits et les durées de vie prévues augmentent. Aujourd'hui, le marché de nœuds a été ouvert à l'industrie. Le fournisseur le plus connu est Cross Bow Inc., avec son offre de capteurs Mica2 et MicaZ

Plate-forme	Unité de traitement	Unité de transmission	Unité d'alimentation
Imote2	Intel PXA271 SRAM 256KB SDRAM 32MB Mémoire flash 32MB	CC2420	3.2-4.5 V
IRIS	Atmel ATMega1281 RAM 8 Ko Mémoire flash 512 Ko EEPROM 4Ko	IEEE 802.15.4	2.7-3.3 V
MICAz	Atmel ATMega128L Mémoire flash 128KB EEPROM 4KB	IEEE 802.15.4	2.7-3.3 V
TELOSB	Texas Instruments MSP430 Mémoire flash 48 KB EEPROM 16 KB RAM 10 KB	CC2420	2.1-3.6 V
Arduino Uno	ATmega328 Mémoire flash 32 KB EEPROM 1 KB SRAM 2 KB	Xbee shield 802.15.4	5 V

Tableau 1. 1 : Caractéristiques de quelques capteurs sans fil [7]

1.3. Réseaux de capteurs Sans-Fil (RCSF)

Les réseaux de capteurs sans-fil sont considérés comme un type spécial des réseaux Ad hoc où l'infrastructure fixe de communication et l'administration centralisée sont absentes et les nœuds jouent, à la fois, le rôle des hôtes et des routeurs. Ce type de réseaux consiste en un ensemble de micro-capteurs éparpillés aléatoirement à travers une zone géographique qui définit le terrain d'intérêt pour le phénomène capté.

Les micro-capteurs déployés sont capables de surveiller, d'une manière continue, une grande variété de conditions ambiantes telles que la température, l'humidité, et de détecter également l'occurrence des événements tel que les séismes,…etc. Malgré leur capacité limitées de captage et de traitement de donnée, qui n'est qu'une conséquence de leur taille miniaturisé, les composants de communication sans-fil intégrés à ces capteurs leur permettent de collaborer et de coordonner entre eux afin d'accomplir des tâches de captage complexes [4].

1.3.1. Architecture des réseaux de capteurs sans fil

Un RCSF (Réseaux de Capteur Sans Fil) est composé d'un ensemble de nœuds capteurs. Ces nœuds capteurs sont organisés en champs « sensor fields » (voir figure 1.5). 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. Puisque les RCSF se caractérisent par l'absence d'une infrastructure déterminée au préalable, les nœuds capteurs la construisent tout en permettant l'interaction avec l'environnement où ils appartiennent et en répondant aux différentes requêtes venant des utilisateurs ou des réseaux externes [5].

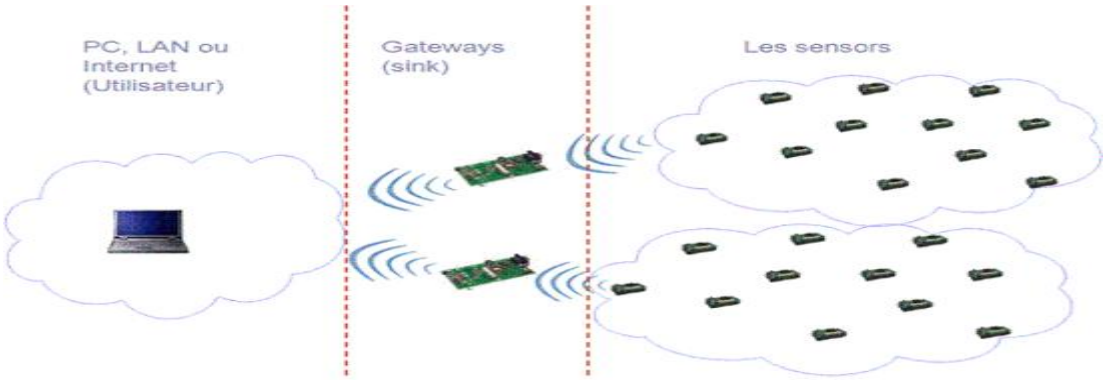

Figure1.4 : Architecture d'un RCSF.

1.3.2. Model de collecte d'information

Il y a deux méthodes pour collecter les informations d'un réseau de capteurs, à la demande et suite à un évènement :

1.3.2.1. À la demande:

Lorsque l'on souhaite avoir l'état de la zone de couverture à un moment T, le puits émet des brodcasts vers toute la zone pour que les capteurs remontent leur dernier relevé vers le puits. Les informations sont alors acheminées par le biais d'une communication multi-sauts.

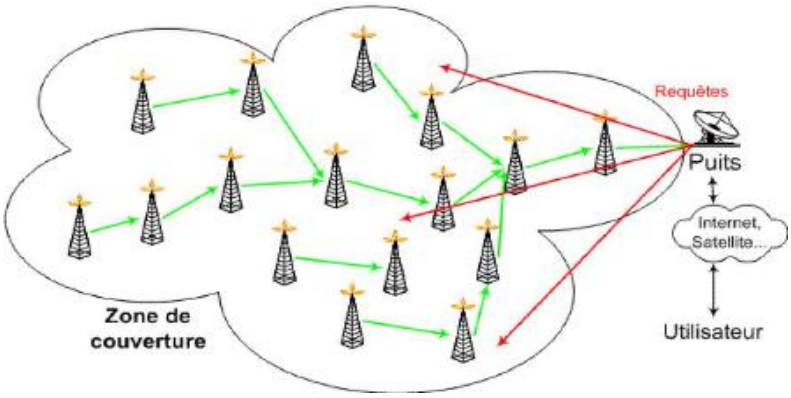

Figure1. 5: Collecter les informations à la demande.

1.3.2.2. Suite à un évènement :

Un événement se produit en un point de la zone de couverture (changement brusque de température, mouvement...), les capteurs situés à proximité remontent alors les informations relevées et les acheminent jusqu'au puits.

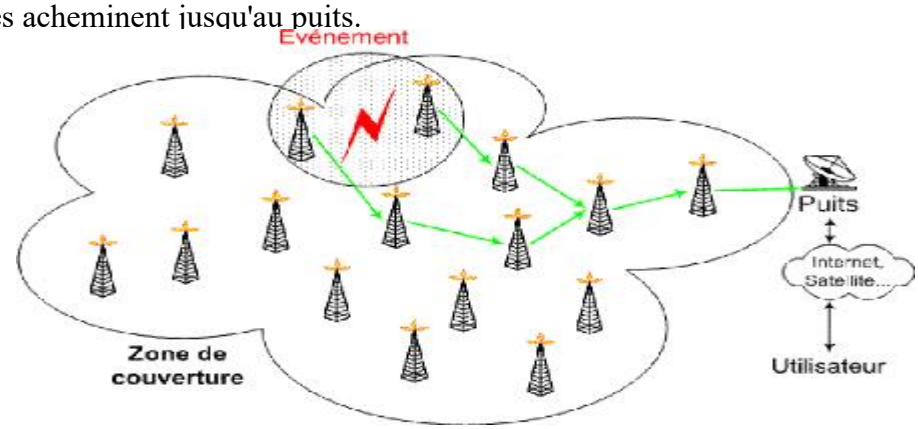

Figure1.6: Collecter les informations Suite à un événement.

1.3.3. Topologie et organisation

Les topologies des réseaux de capteurs sont déterminées à partir des protocoles de routage utilisés pour l'acheminement des données entre les nœuds et le sink. Ces protocoles peuvent être hiérarchiques, plat (Flat) ou basé localisation (location-based) [6]

1.3.3.1. Topologie Hiérarchique

Les protocoles à topologie hiérarchique forment des réseaux dans lesquels un nœud central sink est relié à un ou plusieurs autres nœuds qui appartiennent à un niveau plus bas dans la hiérarchie avec une liaison point à point. Aussi, chacun des nœuds du deuxième niveau aura également un ou plusieurs autres nœuds de niveau plus bas dans la hiérarchie reliés à lui avec une liaison point à point. Les nœuds du deuxième niveau jouent le rôle des passerelles entre ceux du troisième niveau et le sink. Un réseau basé sur une topologie hiérarchique doit avoir au moins trois niveaux dans sa hiérarchie, puisqu'un réseau avec un nœud central sink et seulement un niveau hiérarchique au-dessous. Si les nœuds dans un réseau basé sur la topologie hiérarchique doivent effectuer un tel traitement sur les données transmises entre les nœuds dans le réseau, alors les nœuds qui sont à des niveaux plus élevés dans la hiérarchie doivent effectuer plus de traitement que les nœuds de niveau inférieur. Protocol).

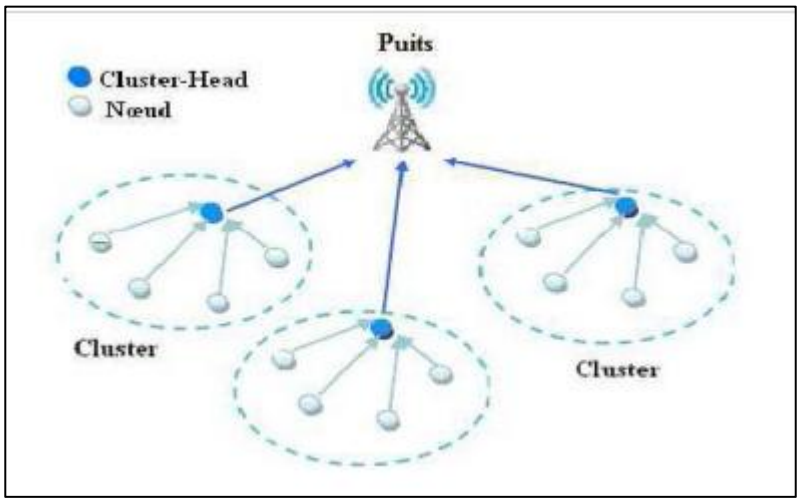

Figure1.7: Topologie hiérarchique par clustring d'un RCSF

1.3.3.2. Topologie plate :

Les protocoles à topologie plate (flat) considèrent que tous les nœuds sont égaux, ont elles-mêmes fonctions, et peuvent communiquer entre eux sans devoir passer par un nœud particulier ou une passerelle. Seul un nœud particulier, le Sink, est chargé de la collecte des données issues des différents nœuds capteurs afin de les transmettre vers les centres de traitement. En cas où la destination ne fait pas partie du voisinage de la source, les données seront transmises en utilisant les sauts multiples à travers les nœuds intermédiaires .Ce type de réseau présente l'avantage de l'existence de différents chemins d'une source vers une destination et c'est pour remédier au problème de changement brusque de topologie ou la défaillance d'un nœud intermédiaire.

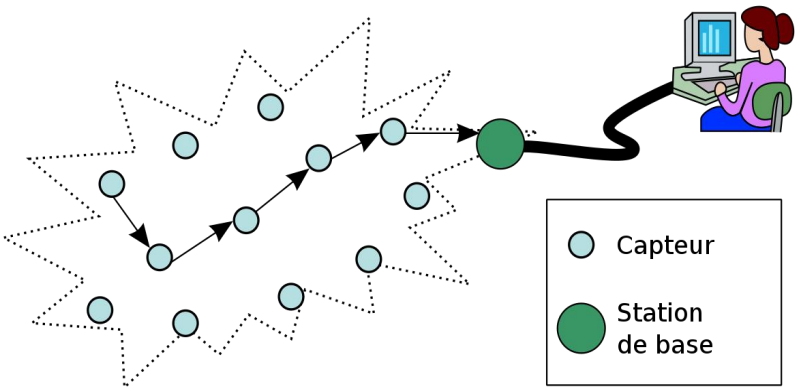

Figure1.8: Exemple d'une topologie plate d'un RCSF

1.3.4. Architecture protocolaire

Dans le but d'un établissement efficace d'un RCSF, une architecture en couches est adoptée afin d'améliorer la robustesse du réseau. Une pile protocolaire de cinq couches est donc utilisée par les nœuds du réseau. Citons la couche application, la couche transport, la couche

réseau, la couche liaison de données et la couche physique. De plus, cette pile possède trois plans (niveaux) de gestion [7].

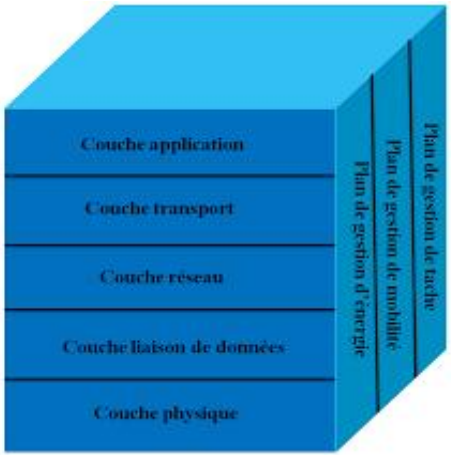

Figure1.9: La pile protocolaire dans les réseaux de capteur [7]

1.3.4.1. Couches de la pile protocolaire

- **La couche physique** : Spécifications des caractéristiques matérielles, des fréquences porteuses, etc.
- **La couche liaison :** Spécifie comment les données sont expédiées entre deux nœuds/routeurs dans une distance d'un saut. Elle est responsable du multiplexage des données, du contrôle d'erreurs, de l'accès au média,... Elle assure la liaison point à point et multipoint dans un réseau de communication.
- **La couche réseau :** Dans la couche réseau le but principal est de trouver une route et une transmission fiable des données, captées, des nœuds capteurs vers le puits "sink" en optimisant l'utilisation de l'énergie des capteurs.
- **La couche transport** : 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 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

1.3.4.2. Plans de gestion

Les différents plans de gestion intégrés dans la pile protocolaire sont :

- **Plan de gestion d'énergie:** sert à contrôler la consommation d'énergie d'un nœud. Par exemple, si le niveau d'énergie d'un nœud devient bas, et afin de prolonger la durée de vie du réseau, ce nœud diffuse à ses voisins une alerte les informant qu'il ne peut pas participer au routage et il réserve son énergie résiduelle pour le captage. [28]
- **Plan de gestion de mobilité :** capable de détecter et enregistrer le mouvement du nœud capteur afin de l'aider à se localiser. Ainsi, ce plan de gestion permet au nœud capteur de maintenir toujours une route vers l'utilisateur, et garder la trace de ses nœuds voisins. En déterminant leurs voisins, les nœuds capteurs peuvent équilibrer l'exécution des tâches et la consommation d'énergie. [6]
- **Plan de gestion de taches :** Il équilibre et ordonnance des taches sur les différents nœuds du réseau. En effet, effectuer la tâche du captage avec le même rythme par tous les nœuds déployés dans la même région spécifique n'est pas obligatoire, il est plus efficace si certain nœud exécutent cette tâche plus que d'autres selon leurs niveaux de batteries, de sorte que la durée de vie du réseau peut être prolongée. [26]

1.4. Caractéristiques d'un RCSF

Un réseau de capteurs présente des caractéristiques particulières comparativement aux autres réseaux sans fil. Dans cette section, nous présentons les principales caractéristiques de ces réseaux :

1.4.1. L'environnement d'exploitation

Le système d'exploitation est un gestionnaire de ressources pour les systèmes complexes. Dans un système typique, ces ressources comprennent un ou plusieurs processeurs de la mémoire vive, de la mémoire morte, un ordonnanceur) , des disques de stockage, des interfaces utilisateur tels que souris, clavier, imprimantes et écrans, et une ou plusieurs interfaces réseau. Le rôle du système d'exploitation est de gérer l'allocation de ressource processeur pour l'exécution des processus, en maximisant l'utilisation globale du processeur tout en optimisant l'interactivité de ces ressources aux utilisateurs d'une manière ordonnée et contrôlée. Un réseau de capteur consiste en un grand nombre de nœuds de petite taille alimentés par une batterie. Ils sont limités par la capacité de la batterie, la puissance du processeur et la capacité de communication. Le rôle du système d'exploitation pour capteur en réseau est d'être l'interface entre des ressources matérielles limitées et des applications distribuées. Il doit fournir une variété de services systèmes basiques comme gérer l'allocation

de ressource sur les périphériques de matériels divers, interrompre la gestion et la planification de tâches, gérer le réseau support. Le but est de faciliter la programmation des applications, mais aussi d'optimiser les utilisations de ressources.

1.4.2. La taille du réseau

Un grand nombre de nœuds dispersés aléatoirement (des réseaux de 10000 nœuds peuvent être envisagés).

1.4.3. La gestion d'énergie

Un capteur 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 envoie/transmet des valeurs. Le dysfonctionnement de quelques nœuds nécessite un changement de la topologie du réseau et un 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 [9].

1.4.4. La portée de communication

Les réseaux de capteurs peuvent contenir des centaines voire des milliers de nœuds capteurs. Un nombre aussi important engendre beaucoup de transmissions inter nodales et nécessite que le nœud sink (puits) soit équipé d'une mémoire importante pour stocker les formations reçues.

1.4.5. Le coût

Les réseaux de capteurs sont généralement composés d'un très grand nombre de nœuds. Le prix d'un nœud est critique afin de pouvoir concurrencer un réseau de surveillance traditionnel. Actuellement un nœud ne coûte souvent pas beaucoup plus que 1$. A titre de comparaison, un nœud Bluetooth, pourtant déjà connu pour être un système low-cost, revient environ à 10$ [10].

1.5. Domaines d'applications des RCSF

La miniaturisation, l'adaptabilité, le faible coût et la communication sans-fil permettent aux réseaux de capteurs d'envahir plusieurs domaines d'applications. Ils permettent aussi d'étendre le domaine des applications existantes.

Les réseaux de capteurs peuvent être composés, suivant leur utilisation, de différents types de nœuds capteurs, tels que les capteurs séismiques, thermiques, visuels, infrarouges, acoustiques et radar, ils sont capables de surveiller une grande variété de phénomènes ambiants. Parmi les domaines où ces réseaux se révèlent très utiles et peuvent offrir de meilleures contributions, on peut citer le militaire, la santé, l'environnemental, domotique**,** …etc [16].

1.5.1. Applications militaires

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

Figure 1.11 : Un service militaire utilisant les RCSF

1.5.2. Applications environnementales

Le contrôle des paramètres environnementaux par les réseaux de capteurs peut donner naissance à plusieurs applications. Par exemple, le déploiement des thermos -capteurs dans une forêt peut aider à détecter un éventuel début de feu et par la suite faciliter la lutte contre les feux de forêt avant leur propagation. Le déploiement des capteurs chimiques dans les milieux urbains peut aider à détecter la pollution et analyser la qualité d'air. De même leur déploiement dans les sites industriels empêche les risques industriels tels que la fuite de produits toxiques (gaz, produits chimiques, éléments radioactifs, pétrole,…etc.). Dans le domaine de l'agriculture, les capteurs peuvent être utilisés pour réagir convenablement aux changements climatiques par exemple le processus d'irrigation lors de la détection de zones sèches dans un champ agricole [51].

Figure 1.12 : Utilisation des RCSF dans l'agriculture.

1.5.3. 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 (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) [33].

Figure 1.13: le capteur CGM (continuous glucose monitor)

1.5.4. Applications 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 se met en état d'arrêt quand la chambre est vide, la climatisation et le chauffage s'ajustent selon les points multiples de mesure, le déclenchement d'une alarme par le capteur quand un intrus veut accéder à la maison [33].

Figure 1.14: les domaines d'application de la domotique

1.5.5. Application industrielle :

Placer des capteurs dans des sites industriels comme les centrales nucléaires, les raffineries de pétrole afin de détecter les fuites de produits toxiques (gaz, produits chimiques, pétrole, radiations). Les nœuds senseurs sont aussi utilisés dans ce domaine pour le contrôle et l'automatisation des chaînes de montage [33].

1.6. Défis des réseaux de capteurs sans fil

1.6.1. Consommation énergétique

Les nœuds intégrés dans l'habitat sont souvent alimentés par des petites batteries ou traditionnellement par des piles. L'économie d'énergie est l'un des facteurs cruciaux de conception. Pour accomplir leurs missions, les nœuds capteurs(en particulier les capteurs médicaux instruits dans le corps de la personne) doivent économiser leurs énergies pour opérer quelques mois, voire quelques années. Le remplacement/rechargement des batteries par les personnes âgées/patients peut être coûteux (rechargement oublié), difficile (nombre important de capteurs, etc.) et parfois impossible notamment pour les capteurs incorporels. Suivant l'architecture du réseau, la durée de vie d'un nœud a une influence plus ou moins grande sur la durée de vie de tout le réseau. Pour atteindre sa destination, le paquet envoyé par un capteur peut passer par d'autres nœuds qui jouent alors le rôle de relais/routeurs. Ce critère de performance n'a certainement pas le même impact que dans le cas d'un réseau très dense. Cependant, moins les nœuds consommeront, plus la durée de vie du réseau satisfera les exigences de l'application [18].

1.6.2. La qualité de service (Qos)

Comme dans de nombreux types de réseaux, la QoS (Quality of service) est un facteur important qui entre en jeu dans la conception du réseau. La QoS doit être considérée non seulement pour la transmission des données médicales récupérées par le WPAN, mais également pour le transfert des contenus multimédia, tels que les flux vidéo et les images fixes (afin de détecter la position d'une personne, détecter une chute, etc.). La QoS est liée à quatre paramètres principaux : le débit de transfert, le délai, la gigue et le taux de perte. Le délai de transfert de bout en bout par exemple a une importance capitale dans cette application. Parmi les paramètres qui influencent le délai, on peut citer : le temps de captage, le temps de traitement, le temps d'attente des paquets dans la file d'attente, le délai d'écoute du canal et le délai d'attente « *Backoff* » (qui dépend du type de la méthode d'accès), le délai de transmission, le délai de propagation et la latence de transition entre les modes de fonctionnement. [18].

1.6.3. Le passage à l'échelle

Généralement, un réseau de capteurs est constitué de nombreux nœuds répartis dans des endroits précis de l'habitat. Avoir un grand nombre de capteurs proches de la personne surveillée permet d'assurer et d'améliorer la qualité et la fiabilité des mesures. Le passage à l'échelle est l'un des critères utilisé pour tester l'évolutivité (surcharge du réseau) des protocoles télécommunication, en particulier les protocoles d'accès au médium MAC et les protocoles de routage [18].

1.6.4. Auto configuration

Le réseau de capteurs comporte un grand nombre de nœuds, qui sont principalement placés dans des endroits hostiles où la configuration manuelle n'est pas réalisable, ce qui nécessite une configuration automatique. Par conséquent, le réseau doit pouvoir se reconfigurer pour continuer sa fonction en cas d'insertion ou de suppression d'un nœud.

1.6.5. Mobilité

De très peu installations qui utilisent des capteurs mobiles, la plupart des architectures de réseau supposent que les nœuds capteurs sont stationnaires et d'autre part supporte la mobilité du sink ou du cluster-head. L'événement à capturer peut, aussi, être dynamique ou statique. Pour une application à événements statiques, le réseau travaille en mode réactif. Par contre, une application à événements dynamiques nécessite des signalisations périodiques [47]

1.6.6. Tolérance aux pannes

Certain nœuds peuvent générer des erreurs ou ne plus fonctionner à cause d'un manque d'énergie, un problème physique ou une interférence. La tolérance aux fautes est la capacité de maintenir les fonctionnalités du réseau sans interruptions dues à une erreur intervenue sur un ou plusieurs capteurs. Les réseaux de capteurs étant très denses, ils entraînent une redondance de données. Cette redondance garantit le fait que la mort de certains nœuds n'affecte pas le fonctionnement du réseau et que le système peut continuer à fournir des informations d'une qualité acceptable.

1.6.7. Sécurité

Certaines applications des réseaux de capteurs demandent une haute confidentialité et fiabilité des données telles les applications militaires et médicales. Pour garantir l'intégrité et la confidentialité de ces données, il est nécessaire de développer des méthodes de cryptographie qui soulève le problème de l'élaboration de protocoles de gestion de clés et qui doivent prendre en considération les limites des réseaux de capteurs [48]. Il est recommandé de protéger un réseau de capteurs des attaques externes telles le déni de service (DoS) qui peut être fatale pour les nœuds capteurs vues leurs batteries limitées [21].

1.6.8. Hétérogénéité

Plusieurs études ont supposé qu'un réseau de capteurs est constitué de nœuds homogènes ayant les mêmes capacités en termes de calcul, de transmission et d'énergie disponible. Cependant, selon l'application, un nœud capteur peut avoir des rôles déférents. L'existence d'un ensemble de capteurs hétérogènes soulève beaucoup de questions techniques liées au routage de données. Par exemple, quelques applications pourraient exiger divers types de capteurs pour surveiller la température, la pression et l'humidité de l'environnement et capturer l'image ou le cheminement visuel des objets mobiles. Ces capteurs spéciaux peuvent être déployés comme ils peuvent inclure les différentes fonctionnalités (un nœud peut être équipé de plusieurs unités de sensation différentes). Même le captage et la délivrance des données peuvent être produits par ces capteurs à différents taux. Par exemple, les protocoles hiérarchiques indiquent des nœuds cluster Heads qui sont différents des nœuds capteurs normaux. Ces cluster Heads peuvent être plus puissants que les autres nœuds capteurs en termes d'énergie, de bande passante et de mémoire. Par conséquence, ils sont chargés de la transmission des données à la station de base.

1.6.9. Routage

Le routage dans les réseaux de capteurs constitue un défi majeur. Ceci est dû aux caractéristiques distinguant ce type de réseaux par rapport aux autres. D'abord, le déploiement

d'un grand nombre de nœuds rend impossible l'établissement d'un schéma d'adressage global pour le réseau. Il n'est pas possible d'utiliser les protocoles de routage IP utilisé dans les réseaux classiques. En outre, les nœuds senseurs sont contraints en termes de capacité de traitement, de stockage et de ressources énergétiques ce qui nécessite une gestion attentive de ces ressources. Pour cette raison, il est recommandé de concevoir des protocoles de routage qui répondent aux exigences des réseaux de capteurs. Le déploiement aléatoire des nœuds dans le champ de captage engendre des zones denses et d'autres moins denses. Les nœuds dans les zones denses peuvent générer des données redondantes dont le routage épuise l'énergie des capteurs inutilement, d'où la nécessité de filtrer ces données en utilisant des mécanismes d'agrégation lors du processus de routage qui optimise la consommation d'énergie et l'utilisation de la bande passante.

1.7. Conclusion

Les caractéristiques attrayantes des réseaux de capteurs telles la, rapidité de déploiement et coût réduit créent, incessamment, de nouveaux domaines d'application. Ce large éventail d'applications fera des réseaux de capteurs une partie intégrante de notre vie. Toutefois, leur déploiement dans des environnements souvent hostiles rend l'intervention humaine difficile voire impensable ce qui pose le problème de disfonctionnement des nœuds dû à des dommages physiques ou à l'épuisement de leurs batteries. L'épuisement rapide des ressources énergétiques des nœuds est l'un des handicaps dont souffrent les réseaux de capteurs. Pour cela, les chercheurs consacrent une grande partie de leurs travaux aux mécanismes qui permettent de prolonger la durée de vie du réseau. Ceci peut être réalisé en minimisant l'énergie dissipée lors de la communication entre les nœuds puisque cette dernière est considérée comme étant la phase la plus gourmande en termes de consommation d'énergie.

Dans le chapitre suivant, nous allons présenter une vue détaillée sur la sécurité dans les réseaux de capteurs sans fil, en faisant le point sur les objectifs de la sécurité, les vulnérabilités, attaques, et solutions adaptées à ce type de réseau.

Chapitre 2

La sécurité dans les réseaux de capteurs sans fil

2.1. Introduction

Les RCSFs sont devenus très courants ces dernières années et leurs applications se multiplient considérablement. Ces réseaux sont composés de dispositifs sans fil miniatures qui ont une puissance de calcul et une capacité de stockage limitées. Aussi, souvent, ils embarquent une batterie comme seule source d'énergie. De plus, ces réseaux peuvent être déployés en masse dans des endroits hostiles et sans aucune surveillance ni intervention humaine. Cette situation rend ce type de réseaux vulnérables à des nombreuses attaques malveillantes. Par conséquent, il est nécessaire d'intégrer un mécanisme de sécurité qui non seulement gère les intrusions, mais garantit également un échange de données sécurisé.

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

2.2. Les objectifs de sécurité :

Un réseau de capteurs est un type particulier de réseau. Il partage certaines similitudes avec un réseau informatique typique, mais pose également des exigences uniques.

2.2.1. L'authentification :

En raison de la nature sans fil des médias et de la nature non surveillée des réseaux de capteurs, l'authenticité de la communication est extrêmement indispensable dans ces conditions. Un service d'authentification fiable doit garantir l'authentification à deux niveaux [1], [2] :

▪ *Authentification d'entité :* avant de permettre à n'importe quelles entités ou participant d'accéder aux services ou à des informations dans le réseau, une vérification d'entité doit être effectuée pour assurer que le demandeur soit une entité légitime et autorisée à récupérer ce service ou information. L'authentification peut être effectuée entre deux nœuds communiquant ou un nœud (par exemple, une tête de grappe) et plusieurs autres nœuds autour de ce nœud (c'est-à-dire une authentification de diffusion). [25]

▪ *Authentification de l'origine des données:* Les capteurs doivent s'assurer que les données reçues proviennent d'une source identifiée. Un adversaire n'est pas limité simplement à modifier le paquet de données. Il peut aussi changer complètement le trafic en injectant de

faux paquets supplémentaires. Ainsi, le récepteur doit s'assurer que les données utilisées dans n'importe quel processus décisionnel proviennent d'une source correcte. [25]

2.2.2. La confidentialité :

La confidentialité est essentielle pour assurer la sécurité du réseau en garantissant que seuls les destinataires désignés peuvent accéder aux informations d'un nœud. Dans les réseaux de capteurs, il est important d'empêcher la divulgation de données sensibles à l'adversaire, y compris les données stockées dans les nœuds et la distribution de clés. Les informations publiques sur les capteurs doivent également être cryptées pour se protéger contre les attaques d'analyse de trafic. La méthode standard pour assurer la confidentialité est le cryptage avec une clé partagée entre l'émetteur et le récepteur. [25]

2.2.3. L'intégrité :

L'intégrité des données est un service qui assure que les données n'ont pas été altérées pendant la transmission. Les altérations peuvent être accidentelles ou volontaires d'un attaquant. Dans les réseaux de capteurs, l'intégrité des données est cruciale pour garantir la fiabilité des données. Un service d'intégrité doit fournir des mécanismes pour détecter les altérations, même si la confidentialité est mise en place. Les nœuds malveillants peuvent altérer les données dans un paquet, mais la perte ou les dommages de données peuvent également se produire sans leur présence en raison des conditions instables du canal de communication sans fil. [24][43][44].

2.2.4. La disponibilité :

La disponibilité donne une assurance sur la réactivité et le temps de réponse d'un système pour transmettre une information d'une source à la bonne destination. Cela signifie aussi que les services du réseau sont disponibles aux parties autorisées si nécessaire et assure les services de réseau en dépit des attaques de déni de service (DoS) pouvant affecter n'importe couche du réseau. [27]

2.2.5. La fraicheur :

Elle concerne la fraîcheur de données et la fraîcheur des clés. Puisque tous les réseaux de capteurs fournissent quelques formes de mesures variables dans le temps, nous devons assurer que chaque message est frais. La fraîcheur de données implique que les données sont récentes, et elle assure qu'aucun adversaire n'a rejoué les vieux messages. [27]

2.3. Les vulnérabilités de la sécurité dans les RCSF :

Des contraintes parfois strictes et intrinsèques aux RCSFs imposent de penser à une sécurité mieux adaptée que son équivalent traditionnel des réseaux filaire. Certains contraintes sont inhérentes aux RCSF et d'autres liées à la technologie retenue. Nous distinguons deux catégories : la vulnérabilité physique et la vulnérabilité technologique.

2.3.1. La vulnérabilité technologique :

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

Limitation en énergie : L'énergie est l'une des principales raisons pour lesquelles les nœuds de capteurs échouent en raison de l'épuisement de la batterie. Une fois que les nœuds de capteurs sont déployés dans un réseau de capteurs, ils ne peuvent pas être facilement remplacés ou rechargés, ce qui entraîne des coûts opérationnels élevés. Par conséquent, la consommation d'énergie doit être minimisée pour prolonger la durée de vie des capteurs, ce qui nécessite à la fois un matériel économe en énergie et des mécanismes de sécurité à faible consommation énergétique.

Capacité de calcul limitée : En raison de la petite taille des nœuds et le faible coût, les nœuds capteurs disposent d'un microcontrôleur à faible capacité de calcul. Ainsi, ceci empêche l'utilisation de mécanismes de protection cryptographiques qui exigeant plus de puissance de calcul. [25].

Mémoire limitée : Un capteur est un petit dispositif avec une capacité limitée de mémoire et d'espace de stockage pour le code. Par exemple un capteur de type Mica mote, possède un processeur Atmel ATMEGA103 4 MHz avec 128 Ko de mémoire d'instructions, 512 Ko de mémoire flash, et seulement 4 Ko de RAM pour les données. Donc avec une telle limitation, il est indispensable de limiter la taille du code de l'algorithme de sécurité afin de construire un mécanisme de sécurité efficace [36], [37].

Transmission/réception : D'un point de vu énergétique, la transmission est l'opération la plus coûteuse dans les réseaux de capteurs sans fils. Il a été démontré que un bit transmis est équivalent à environ un millier d'opérations CPU [22]. Par conséquent, Dans la conception de mécanisme de sécurité, le nombre de messages échangé entre les nœuds capteurs doivent être pris en considération.

2.3.2. Vulnérabilités physique :

La vulnérabilité physique est le fait qu'un capteur est fréquemment déployé dans un environnement non-protégé et laissé sans surveillance pendant de longues périodes, tels que les lieux publics ou les environnements naturels (forêt, région montagneuse, désert, etc.), c.-à-

d. dont l'accès n'est nullement restreint. Ainsi, elle expose les liens de communication à des attaques. En plus, les nœuds capteurs sont vulnérables au vandalisme et à la capture physique. Généralement, ce moyen d'attaque permet à l'attaquant de changer en partie un capteur, en modifiant par exemple son code de programmation, ou en copiant les clés de protection afin de les réutiliser dans une nouvelle attaque. [26]

2.4. Classification des attaques dans les RCSF :

Dans les réseaux de capteurs, un attaquant peut effectuer une variété d'attaques n'ayant pas forcément le même objectif ou motivations. Ainsi le choix d'une stratégie de sécurité doit se baser sur une modélisation de l'attaque, ceci afin d'éviter un déploiement excessif de moyens de protection conduisant à des solutions irréalistes. Selon (Yong, et al, 2006), les attaques sur les réseaux de capteurs peuvent être classifiées dans les catégories suivantes: [49]

2.4.1. Attaques passives/attaques actives :

Les attaques passives se limitent à l'écoute et l'analyse du trafic échangé. Ce type d'attaque est plus facile à réaliser (il suffit de posséder un récepteur adéquat) et il est difficile de le détecter puisque l'attaquant n'apporte aucune modification sur les informations échangées. L'intention de l'attaquant peut être la connaissance des informations confidentielles ou bien la connaissance des nœuds importants dans le réseau, l'attaquant va se préparer à mener ultérieurement une action précise. [49]

Dans les attaques actives, un attaquant tente de supprimer ou modifier les messages transmis sur le réseau. Il peut aussi injecter son propre trafic ou rejouer d'anciens messages pour perturber le fonctionnement du réseau ou provoquer un déni de service. [49]

2.4.2. Attaques externes/Attaques internes :

Dans le cas de l'attaque externe, le nœud attaquant n'est pas autorisé à participer dans le réseau de capteurs. Des techniques de cryptographie et d'authentification protègent l'accès au réseau à ce type d'attaquant. Cependant ce dernier peut uniquement déclencher des attaques passives tels que l'écoute clandestine, le brouillage radio, ou l'attaque par rejeu. [49]

L'attaque interne est considérée comme la plus dangereuse du point de vue sécurité. Puisque l'attaquant qui capture un nœud, peut lire sa mémoire et avoir accès à son matériel cryptographique et par conséquent peut s'authentifier comme un nœud légitime et émettre des messages aléatoires erronés sans qu'il soit identifié comme intrus, puisqu'il utilise des clés valides. Les méthodes cryptographiques s'avèrent donc inefficace pour ce genre d'attaque. Il

est donc nécessaire d'utiliser d'autres méthodes complémentaires telles que les systèmes de de détection d'intrusion [28].

2.5. Description de quelques attaques :

Les différentes caractéristiques des réseaux de capteurs sans fil (énergie limitée, faible puissance de calcul, et l'utilisation des ondes radio, etc. ...) les exposent à de nombreuses attaques de sécurité. Dans cette section, nous présentons les attaques les plus connues dans les RCSFs.

2.5.1. Brouillage radio (Jamming)

C'est une attaque de type Déni de Service (DoS) dont le but est de perturber la communication. En effet, elle est dangereuse car elle peut isoler une région entière en ciblant des nœuds importants tels que la station de base ou le chef de cluster. L'attaquant utilise un puissant dispositif de brouillage pour interférer le canal de communication entre deux interlocuteurs. [55][25]

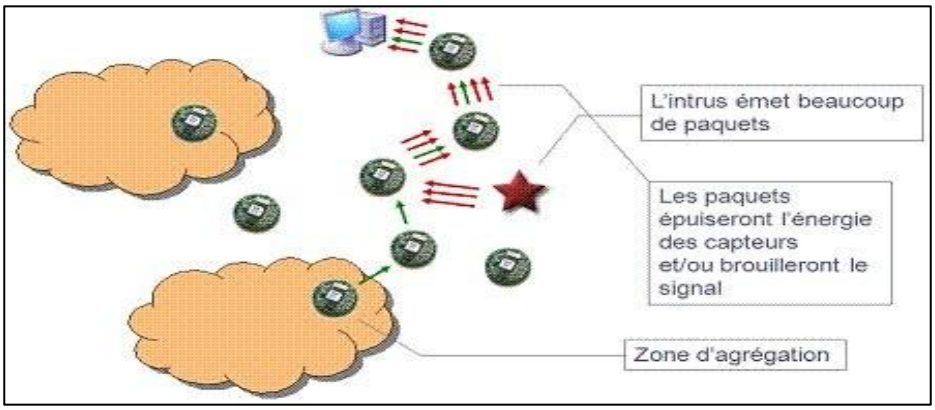

Figure 2.1: Attaque de "Jamming" [36]

2.5.2. Relais sélectif de paquets (Selective Forwarding)

Les réseaux de capteurs sans fil (RCSF) ont tendance à utiliser une communication à plusieurs étapes pour collecter les données, en supposant que tous les nœuds participant à la communication sont légitimes. Cependant, un nœud malveillant sur le chemin de transmission des données peut bloquer certains paquets pour empêcher leur livraison. Cette attaque peut être plus critique si le nœud malveillant cible des nœuds importants dans le réseau. L'attaquant peut réduire les chances de détection en rejetant uniquement les paquets ciblés et en transférant le reste. Des techniques comme l'utilisation de multiples chemins ou l'ajout de numéros de séquence sur les paquets peuvent être utilisées pour se défendre contre ce type d'attaques. [31][32]

2.5.3. L'attaque de trou de puits (Sinkhole)

Un nœud malveillant essaie de paraître le plus attrayant possible dans une zone donnée afin de tromper ses voisins et d'être choisi comme nœud relais sur leur route. Par conséquent, les nœuds compromis peuvent attirer la plupart des flux de données vers des zones spécifiques, souvent les plus proches de la station de base, ce qui empêche les paquets de parvenir à leur destination légitime. Ces attaques peuvent être combinées avec d'autres attaques telles que le routage sélectif, qui permet au nœud compromis de transmettre uniquement les paquets sélectionnés provenant de la zone importante. L'attaque du trou de puits est particulièrement difficile à défendre, en particulier dans les protocoles de routage qui se basent sur des informations de l'énergie ou d'estimation de fiabilité de bout en bout pour construire la topologie de routage dans le réseau, en raison de leurs contraintes limitées en termes de ressources. [49][50]

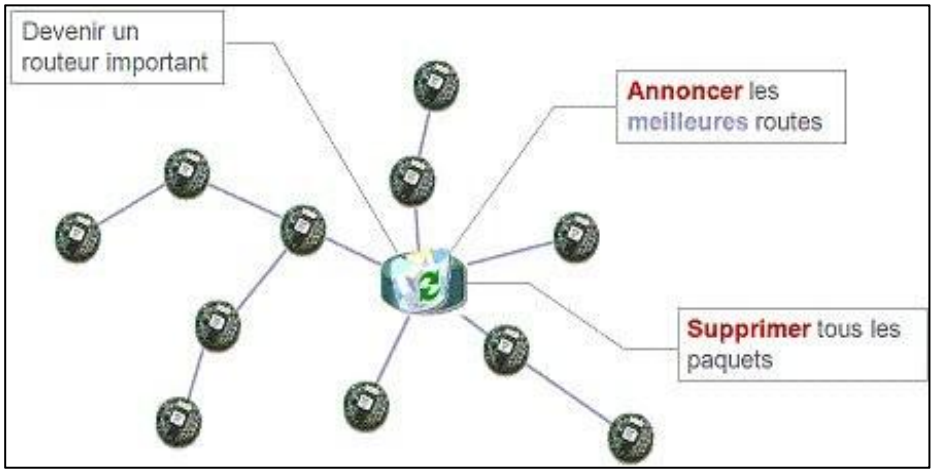

Figure 2.2: Attaque Sinkhole [54]

2.5.4. Attaque d'altération (Tampering) :

Les RCSFs sont généralement déployés dans des environnements non protégés et souvent sans surveillance. Par conséquent, les nœuds capteurs sont vulnérables aux attaques d'altération physique pour extraire toutes les informations importantes comme les clés cryptographiques. Dans ces conditions, un attaquant peut altérer les circuits électroniques, modifier les codes de programme ou même remplacer le nœud capteur par un capteur malveillant. [66]

2.5.5. Attaque du trou de ver (Wormhole)

Lorsqu'un Wormhole est utilisé pour connecter deux nœuds malveillants, ceux-ci peuvent capturer, répéter et manipuler les transmissions de données provenant de nœuds légitimes

voisins. Ce type d'attaque peut rapidement épuiser les ressources énergétiques des nœuds éloignés qui sont trompés en pensant qu'ils sont voisins [31] [32]. La figure suivante illustre un exemple de Wormhole

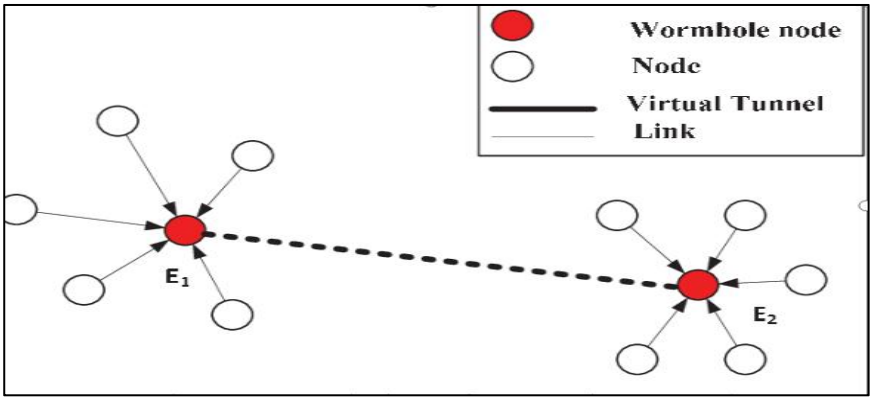

Figure 2.3 : Attaque Wormhole [36]

2.5.6. Attaque d'inondation par paquet de Hello (Hello flood attack)

Plusieurs protocoles de communication exigent que des nœuds capteurs échangent des paquets HELLO périodiques pour découvrir leurs voisins. Ainsi, chaque nœud recevant un tel paquet peut supposer qu'il se trouve dans la couverture radio de l'expéditeur. Un nœud malveillant doté d'un émetteur puissant peut exploiter cette exigence pour tromper un grand nombre de nœuds en leur faisant croire qu'ils sont dans son voisinage. Par conséquence, les nœuds capteurs peuvent tenter d'envoyer leurs données à des nœuds attaquants qui se trouvent en dehors de leur portée radio, ce qui peut entraîner une perte d'énergie et de données, perturbant ainsi le bon fonctionnement du système réseau. [31][32]

2.5.7. Attaque par rejeu (replay)

Dans cette situation, l'attaquant enregistre et redirige les paquets de communication entre les nœuds capteurs pour épuiser l'énergie des nœuds récepteurs. Les paquets transportent des informations de routage, de perception ou de configuration qu'il peut altérer pour créer des faux messages et détourner le réseau de sa fonction initiale. [38]

2.5.8. Réplication de nœuds

Lorsqu'un attaquant utilise une méthode de réplication de nœuds, il essaye de voler l'identité d'un nœud légitime existant en reproduisant son identifiant. Cela permet à l'attaquant d'insérer

un nœud malveillant dans le réseau, ce qui lui donne la possibilité de récupérer les clés cryptographiques et de perturber le fonctionnement du réseau. [31][32]

2.6. Mécanismes de sécurité :

Pour les RCSFs, les mécanismes de sécurité existants tentent de protéger le matériel des nœuds capteurs, le canal de communication et les protocoles et services. Nous citons dans ce qui suit quelques mécanismes de sécurité proposés contre les attaques ou les comportements malicieux.

2.6.1. Primitives cryptographiques :

Les différentes problématiques de sécurité nécessitent des solutions basées sur l'utilisation des primitives cryptographiques, qui sont les briques servants à construire les protocoles de sécurité. Pour cela nous allons aborder dans ce qui suit les diverses primitives cryptographiques destinées aux réseaux de capteurs sans fil.

2.6.1.1. La cryptographie

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. Dans les réseaux de capteurs sans fil, des systèmes cryptographiques basés sur des clés sécurisées sont nécessaires pour chiffrer et authentifier les messages entre les nœuds capteurs. Cependant, les méthodes cryptographiques traditionnelles doivent être adaptées aux contraintes des nœuds capteurs en termes de capacité de calcul et de mémoire, ainsi que de consommation d'énergie. Les techniques cryptographiques symétriques, asymétriques sont généralement utilisées dans les réseaux de capteurs sans fil.

- **La cryptographie symétrique:**

Utilise une clé partagée entre deux nœuds pour chiffrer et déchiffrer les messages échangés à l'aide d'un algorithme de chiffrement. Les algorithmes de chiffrement symétriques sont décomposés en deux catégories :

- ***Les algorithmes de chiffrement par blocs*** *:* sont les plus couramment utilisés et décomposent les données en blocs de taille égale. Ils peuvent également être utilisés dans d'autres outils de cryptographie tels que les fonctions de hachage et les codes MAC. Les algorithmes les plus utilisés sont : DES (Data Encryption Standard), AES (Advanced Encryption Standard) [42].

- ***Les algorithmes de chiffrement par flots :*** transforment les données en clair en un texte chiffré bit par bit en combinant les flux de bits en clair avec un flux de bits aléatoires. Un exemple de chiffrement en chaîne est l'algorithme RC5 (RivestCipher 4) [42]

La difficulté du chiffrement symétrique est la distribution des clés, nécessitant une clé partagée entre chaque paire de nœuds dans le réseau. Cependant, les algorithmes de chiffrement symétriques ne nécessitent pas de calculs complexes et énergivores pendant les phases de chiffrement et de déchiffrement.

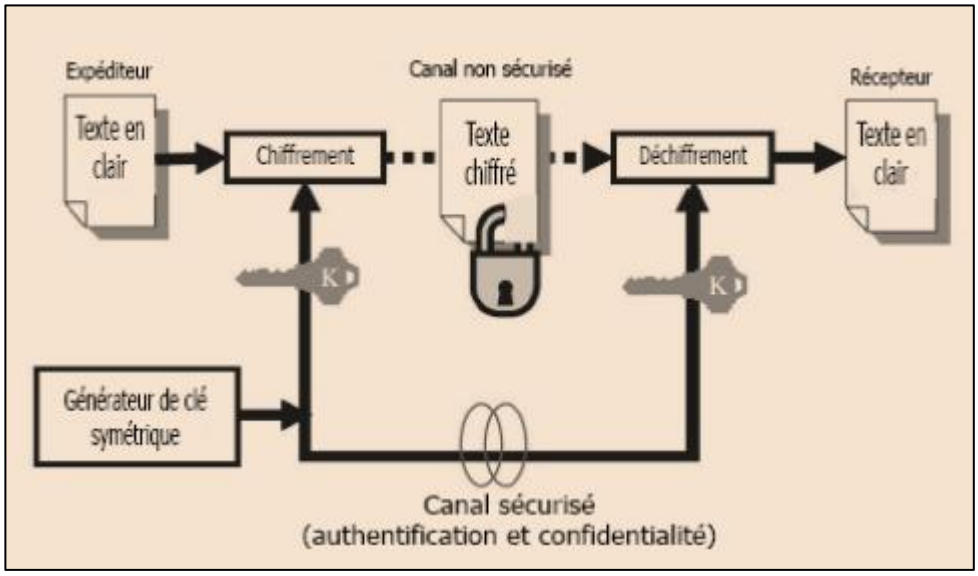

Figure 2.4 : La cryptographie symétrique [41]

- **La cryptographie asymétrique:**

Utilise deux clés générées par le destinataire du message: une clé privée conservée par le destinataire et une clé publique diffusée à tous les émetteurs du réseau. La clé publique sert à chiffrer le message et la clé privée sert à le déchiffrer. Cette méthode repose sur le fait qu'il est impossible de déduire la clé privée à partir de la clé publique. Cette approche facilite la distribution des clés car chaque nœud ne nécessite qu'une paire de clés, mais elle induit une complexité mathématique et de stockages importants, entraînant une consommation élevée d'énergie. Parmi les algorithmes de chiffrement asymétrique les plus connus nous citons : le RSA (Rivest Shamir Adleman) et l'ECC (elliptic curve cryptography) [65]

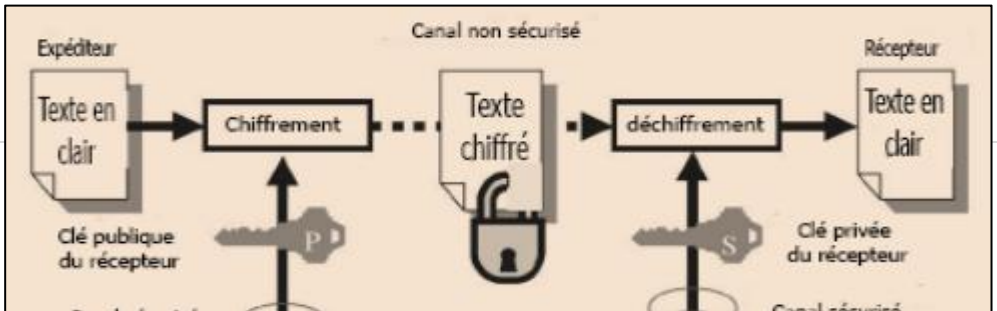

Figure 2.5 : La cryptographie asymétrique [53]

2.6.1.2. Fonction de hachage

Cette fonction permet de générer une empreinte (digest) de taille réduite à partir d'une chaîne de longueur variable. Elle est utilisée pour vérifier l'intégrité des messages transmis. Cette fonction est à sens unique, ce qui signifie qu'il est facile de générer une empreinte à partir d'une chaîne, mais impossible de déduire la chaîne à partir de l'empreinte. L'émetteur utilise la fonction de hachage pour créer l'empreinte du message transmis et envoie le message et l'empreinte au récepteur. Ce dernier calcule ensuite l'empreinte du message reçu et la compare à l'empreinte initiale pour vérifier l'intégrité du message. Si les deux empreintes correspondent, c'est que le message n'a pas été altéré. [41]

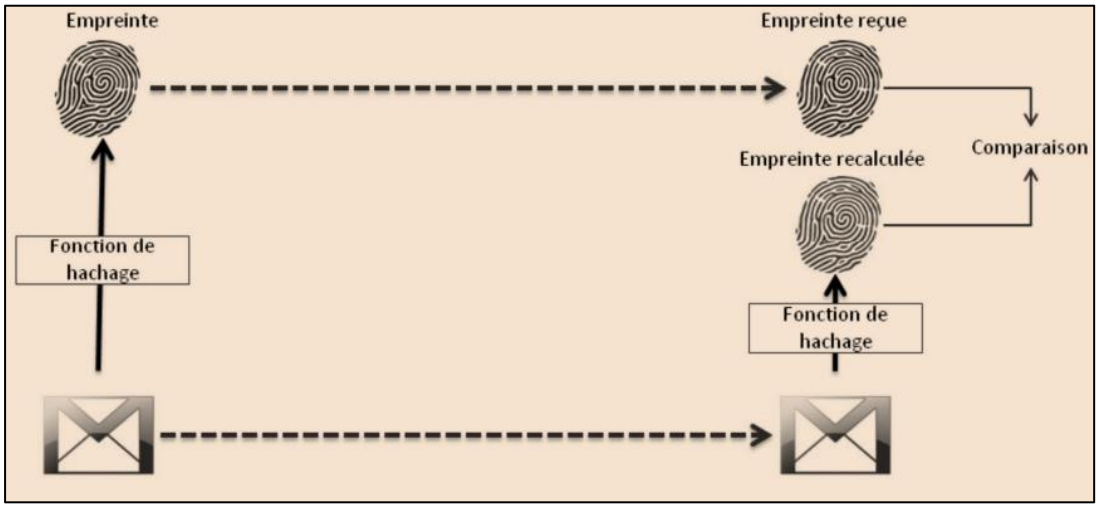

Figure 2.6: La fonction de hachage [41]

2.6.1.3. Le code d'authentification de message

Le code d'authentification de message (CAM), ou MAC (pour Message Authentification Code en anglais) fait partie des fonctions de hachage à clé symétrique assurant l'intégrité des données et l'authenticité de la source de données. Un MAC consiste à utiliser une fonction cryptographique de hachage combinée à une clé secrète (symétrique) connue uniquement par les deux entités communicantes (échangeant le message). Autrement dit, le MAC est un algorithme qui prend en entrée un message à transmettre et une clé secrète et qui produit un condensé. En effet, ce condensé est par la suite transmis avec les données. Le destinataire calcule à son coté le condensé MAC avec la même clé partagée avec l'expéditeur et le compare au condensé qu'il a reçu. S'ils sont identiques, alors l'expéditeur du message est authentique et les données n'ont pas été modifiées. [41]

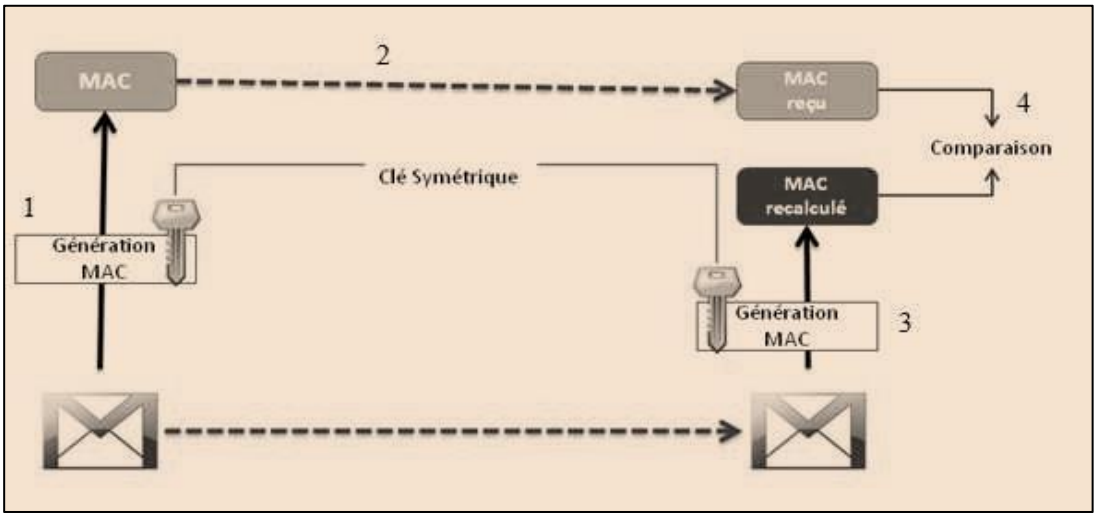

Figure 2.7 : le code d'authentification de message [41]

2.6.2. La gestion de clés

La gestion de clés est un service primordial pour la sécurité de n'importe quel système basé sur la communication. Elle permet de gérer de manière efficace, sécurisée et stable les clés utilisées dans les opérations cryptographiques. En effet, elle permet d'établir les clés cryptographiques utilisées entre les nœuds de manière sécurisée et fiable après le déploiement, 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. 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.

Généralement, la gestion de clés repose sur quatre fonctions pour assurer des services de sécurité tels que l'authentification, la sécurisation du routage et l'agrégation. Ces fonctions sont illustrées dans la figure ci-dessous :

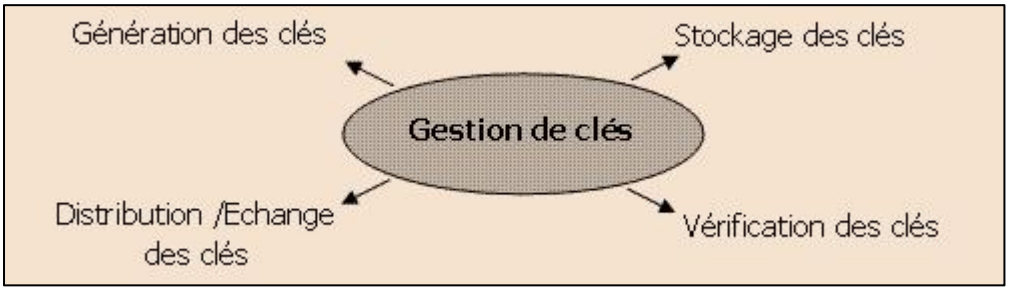

Figure 2.8: Fonctions de gestion de clés [55]

2.7. La gestion de clés dans les réseaux de capteurs sans fil

L'établissement d'une clé secrète entre les paires ou les groupes de nœuds est l'un des services de sécurité le plus important qui assure avec les primitives cryptographiques 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 cette section, nous présentons un aperçu sur les composants d'un système de gestion de clés dans les réseaux de capteurs sans fil. Il existe dans la littérature beaucoup de solutions, 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 métriques importantes pour l'évaluation de leurs performances.

2.7.1. Composants de la gestion des 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. Afin d'atteindre ce but d'une façon sécurisée, nous avons besoin d'un mécanisme de gestion de clés qui permet de: (i) la pré-distribution de clés cryptographiques avant le déploiement, (ii) l'établissement de clés après le déploiement d'une manière sécurisée, et (iii) le renouvellement et la révocation de clés pendant toute le cycle de vie du réseau. De ce fait, un système de gestion de clés inclut les trois composants suivants [25] :

2.7.1.1. L'établissement de clés:

L'établissement de clé est un processus par lequel une clé secrète partagée devient disponible pour deux ou plusieurs entités, pour une utilisation cryptographique ultérieure. 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. Dans les réseaux de capteurs sans fil, l'établissement de clés nécessite deux étapes de base. Le premier consiste à établir la confiance entre les entités participantes. Le second est le calcul de la clé cryptographique. Les deux étapes ont des exigences uniques pour maintenir la confidentialité des clés, fournir la disponibilité, fournir une protection de l'intégrité et une authentification suffisante, etc. [48]

2.7.1.2. Le renouvellement de clés:

Pour éviter une telle situation ou la rendre plus difficile pour l'adversaire, le système de gestion des clés doit permettre de régénérer les clés. Cela pose un défi majeur au système de gestion des clés car des nouvelles clés doivent être générées de manière efficace et compatible avec la consommation et la conservation de l'énergie. Plusieurs raisons justifient le renouvellement de clés du réseau RCSF [30].

- Renouvellement périodique
- Renouvellement à cause d'une compromission de nœud
- Renouvellement en cas de changement de la fonction du nœud.

2.7.1.3. La révocation de clés

La révocation de clé est un élément important dans un système de gestion de clé parce qu'elle permet d'éliminer les nœuds compromis du réseau et garantir que ces nœuds ne puissent plus déchiffrer les messages sensibles transmis sur le réseau. En effet, une fois la capture d'un nœud détectée, un message de révocation est ensuite envoyé, ce qui amène les nœuds à vérifier s'ils sont en communication avec le nœud compromis. Si c'est le cas, les clés de session partagées avec ce nœud sont révoquées. Ainsi, Seuls les liens entre le nœud capturé et ses voisins sont logiquement coupés. En outre, Les mécanismes de révocation sont importants pour empêcher les nœuds compromis d'injecter de fausses données ou de modifier des données des nœuds sécurisés. [30]

2.7.2. Les phases d'établissement de clés

Les protocoles de gestion de clés dans les réseaux de capteurs sans fil utilisent généralement la cryptographie asymétrique pour l'établissement de clés, car elle offre des mécanismes

fiables pour l'authentification et la distribution de clés. Cependant, la cryptographie asymétrique nécessite un espace de stockage important et une capacité de calcul élevée, ce qui la rend inappropriée pour les RCSFs. En revanche, l'utilisation de clés symétriques réduit considérablement la consommation d'énergie et l'espace de stockage réservé pour les clés. Cependant, l'implémentation de ces schémas doit prendre en compte les limites en termes d'énergie, de bande passante et de mémoire de stockage des nœuds capteurs. Bien que la cryptographie asymétrique ait ses avantages, la cryptographie symétrique est généralement préférée pour les RCSFs en raison de ses qualités uniques, ce qui explique pourquoi la plupart des approches de gestion de clés proposées pour les RCSF sont basées sur la cryptographie symétrique.[30]

Le problème majeur avec la cryptographie symétrique est de pouvoir trouver une méthode qui facilite l'établissement de clés entre les nœuds capteurs. La solution commune est d'utiliser une méthode de pré-distribution, dans laquelle les clés sont enregistrées dans les nœuds avant le déploiement. Les RCSFs utilisent un mécanisme à clé symétrique pour l'établissement de clés basée sur la pré-distribution de clés, qui comprend les trois étapes suivantes [30]:

2.7.2.1. Pré-distribution de clé (Key Predistribution) :

La pré-distribution de clés est nécessaire pour assurer une communication sécurisée. Cette étape implique de charger les clés dans chaque capteur avant leur déploiement, créant ainsi un jeu de clés. Une clé partagée entre deux capteurs leur permettra d'établir un lien sécurisé, mais il est peu pratique et peu flexible de pré-charger tous les capteurs avec une seule clé. La distribution de paires de clés distinctes pour chaque paire de capteurs est une solution plus efficace, mais elle soulève des problèmes de stockage et de sauvegarde d'identifiants de clés. Pourtant, la pré-distribution de clés est la méthode la plus sûre et la plus efficace pour garantir la sécurité des communications dans la phase de construction de RCSF, malgré les problèmes de stockage de clés dans les capteurs.

2.7.2.2. Découverte de clés partagée :

Après le déploiement, le protocole de communication est responsable de la découverte de la clé commune entre deux nœuds voisins. Selon la portée de l'antenne radio, un nœud doit découvrir ses voisins parmi lesquelles il partage une clé. Ainsi, si deux nœuds partagent la même clé donc un lien peut être établé entre les deux nœuds. Un système efficace de découverte ne doit pas permettre à un adversaire de connaitre les clés partagées entre les nœuds [25]

2.7.2.3. Établissement de clés de chemin:

Après la phase de découverte de clés partagées, le réseau devient un graphe connecté formé de quelques liens sécurisés. Les nœuds peuvent alors utiliser les liens existants pour mettre en place des clés partagées avec leurs voisins qui ne partageaient pas de clé en commun avec eux. Ainsi, toute paire de nœuds qui ne partagent pas une clé commune mais sont connecté par plusieurs sauts et souhaitent communiquer peuvent chercher un chemin sécurisé entre eux. Ce chemin passe par un ensemble de nœuds qui présente déjà des liens sécurisés. Une fois le chemin établi, la clé de chemin (pathkey) est générée et les deux nœuds peuvent l'exploiter pour commencer une communication sécurisée de bout en bout. [42] [43]

2.8. Classification des schémas de gestion de clés dans les RCSF

La gestion de clés est un mécanisme important dans le processus de configuration d'un système cryptographique. La conception d'un système de gestion de clés dans un RCSFs est un grand défi vue les contraintes liées à ce domaine, ainsi le choix d'une solution cryptographique revient à un autre défi. 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. [30]

Nous trouvons plusieurs classifications de gestion de clés dans la littérature comme celle de [29] – [30]. La figure 2.9 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.

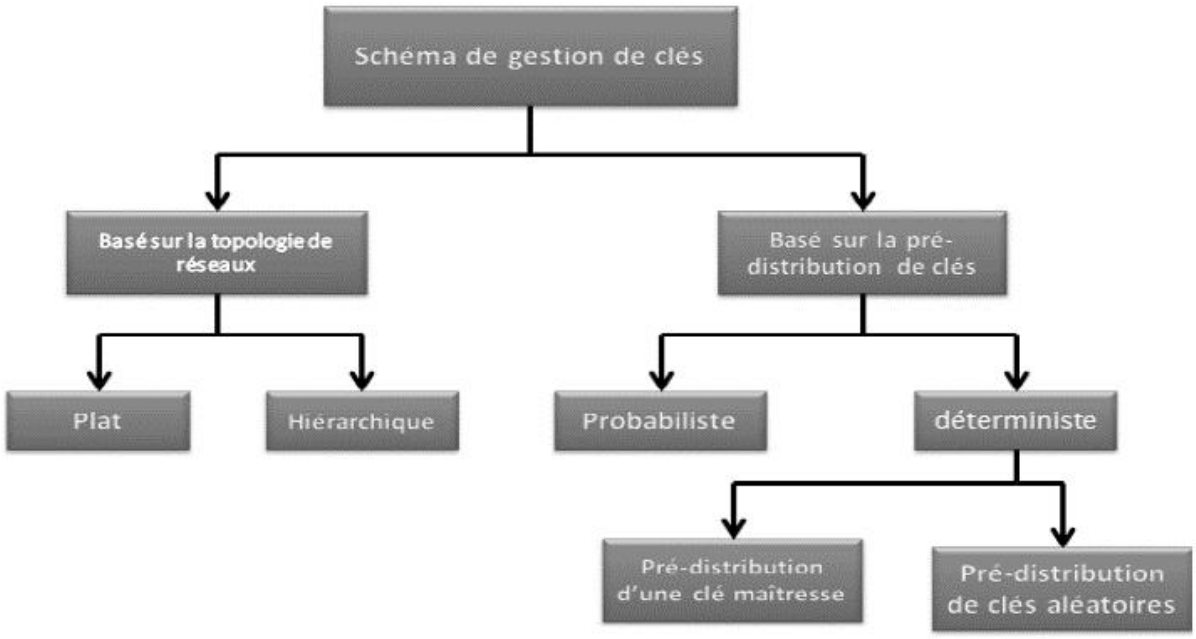

Figure 2.9 : Classification des schémas de gestion de clés pour les réseaux de capteurs sans fil

2.8.1. Schémas basés sur la pré-distribution de clés:

Les schémas basés sur la pré-distribution reposent sur le principe de distribution de clés statiques, où les nœuds sont pré-chargés par des clés dans leurs mémoires avant le déploiement dans la nature, d'une manière que chaque nœud a une clé commune qu'il partagera avec son voisin afin d'établir des communications secrètes. La plupart des schémas proposés pour les RCSFs sont basés sur la pré-distribution. Nous pouvons classer les schémas de cette catégorie en deux sous catégories :

2.8.1.1. Schémas probabilistes :

Le principe du protocole probabiliste est qu'avant le déploiement, un ensemble de clés est choisi aléatoirement à partir d'un nombre important de clés, avec condition pour que chaque deux nœuds voisins puissent avoir au moins une clé commune entre eux avec une certaine probabilité après le déploiement. La pré-distribution de clé est réalisée en plusieurs étapes : Commençant par la génération d'un Pool de clés avec leurs identifiants. Puis, un choix aléatoirement d'un ensemble de clé K dans le Pool P servant de porte-clés (Key ring) pour chaque nœud. Ces porte-clés sont stockés dans la mémoire des nœuds, par contre, l'association entre la liste des identifiants de porte-clés et identifiant de nœuds sont stockés dans la mémoire du nœud puits. Les méthodes probabilistes sont faciles et simples à mettre en œuvre dans la phase de distribution de clés après le déploiement, mais possèdent un

inconvénient qui réside dans le fait que la taille de l'ensemble des clés pré-distribuées va augmenter considérablement avec l'augmentation de la taille du réseau, ce qui influence la capacité mémoire des nœuds capteurs. Ainsi, ces méthodes ne sont pas sécurisées contre les attaques de capture physique des nœuds [41]. Dans cette section, nous détaillerons les principales solutions.

Eschenauer et Gligor ont proposé un schéma de gestion de clé basé sur la probabilité de partager une clé entre les nœuds d'un graphe aléatoire. L'idée maîtresse de ce schéma, est de distribuer aléatoirement un certain nombre de clés, issues d'un ensemble fini à chaque nœud du réseau avant son déploiement. Deux nœuds quelconque seront en mesure de s'échanger des messages sécurisés s'ils possèdent une clé commune. Dans ce schéma, trois phases sont nécessaires pour installer les clés secrètes entre les nœuds capteurs. [44]

(i) Phase de pré-distribution de clés

Un grand ensemble P de clés est généré. Pour chaque nœud, m clés sont choisies au hasard à partir de l'ensemble P. Ces m clés sont stockées dans la mémoire du nœud et forment le trousseau de clés du nœud. Le nombre de clés |P| de l'ensemble P est choisi de telle manière que deux sous-ensembles aléatoires de P de taille m auront une certaine probabilité p d'avoir au moins une clé en commun, par exemple pour une probabilité p = 0.5 on a besoin d'un sous ensemble de taille m = 75 clés de l'ensemble P de taille |S| = 10, 000 clés. [44]

(ii) Phase de découverte de clés partagées

Les nœuds découvrent leurs voisins et plus particulièrement ceux avec qui ils sont en mesure de communiquer de façon sécurisée, car ils possèdent une clé identique dans leur trousseau de clés respectifs. Le protocole est de diffuser la liste des identités des clés possédées, la clé partagée devient la clé de session de lien entre les deux nœuds. [44]

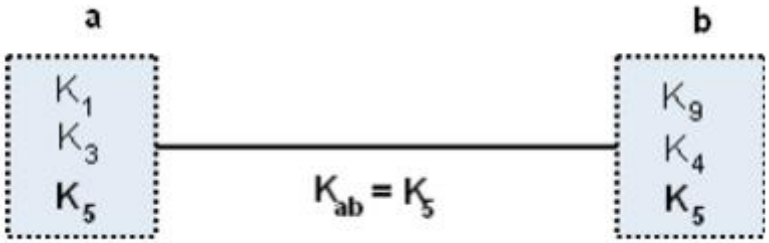

Figure 2.10 : Un exemple du schéma d'Eschenauer et Gligor [48]

(iii) Phase d'établissement de chemin de clé

Après la phase de découverte des clés partagées, le réseau devient un graphe connecté formé de quelques liens sécurisés. Les nœuds peuvent alors utiliser les liens existants pour mettre en place des clés partagées avec leurs voisins qui ne partageaient pas de clé en commun avec eux. [68]

(iv) Révocation de clés

La révocation d'un nœud compromis se fait par l'élimination de son porte-clés. Pour cela, un nœud contrôleur (qui est mobile et possède une grande connectivité) annonce un message simple de révocation contenant une liste signée des porte-clés pour que ces clés soient retirées des porte-clés des autres nœuds révoqués. 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 produite à cause de la suppression de clés du nœud compromis ce qui nécessite une reconfiguration de ces liens. [48]

Chan et al. [] 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 q clés avec avec $q > 1$ pour établir un lien sécurisé. La nouvelle clé utilisée pour la communication entre ces deux nœuds capteurs 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. 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 q clés et le nombre de clés qu'un nœud peut contenir [43].

2.8.1.2. Schémas déterministes :

Dans les RCSFs, il existe plusieurs façons de classer les protocoles de gestion de clés déterministes. En effet, l'une des classifications consiste à classer les protocoles de gestion des clés selon les catégories suivantes : méthodes de pré-distribution de clés aléatoires et méthodes de pré-distribution d'une clé maîtresse. Nous avons limité la synthèse bibliographique de cette partie à quelques méthodes pour ces deux catégories.

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

Dans cette catégorie les porte-clés sont générés d'une façon déterministe afin d'assurer l'établissement de certains liens entre les nœuds capteurs.

Blom [44] a proposé une méthode pour générer une clé symétrique distincte entre chaque paire de nœuds du réseau au moyen de calculs matriciels. Au début, la station de base crée une matrice symétrique D de la taille (λ + 1) (λ + 1) une matrice publique G de la taille (λ +1) × N sur un corps fini GF(q), où N est la taille du réseau et λ est le seuil prévu pour menacer la sécurité 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 $A=(D.G)^T$. Chaque élément de la matrice K est la clé du nœud i pour sécuriser la liaison avec le nœud j. Après, chaque nœud est pré-chargé avec la i-ème rangée de la matrice secrète et la i-ème colonne de la mat rice publique [44]. Cette méthode est illustrée à la figure 2.11.

Après déploiement, chaque paire de nœuds i et j peuvent individuellement calculer la clé partagée entre eux $K_{ij} = K_{ji}$ 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. [48]

Le schéma de Blom peut attribuer à chaque paire de nœuds capteurs une clé symétrique, et il tolère la compromission de λ nœuds. Par conséquent, il exige λ +1 d'espace mémoire et une diffusion d'un message de taille λ +1, et une multiplication coûteuse de deux vecteurs de λ +1 éléments. [48]

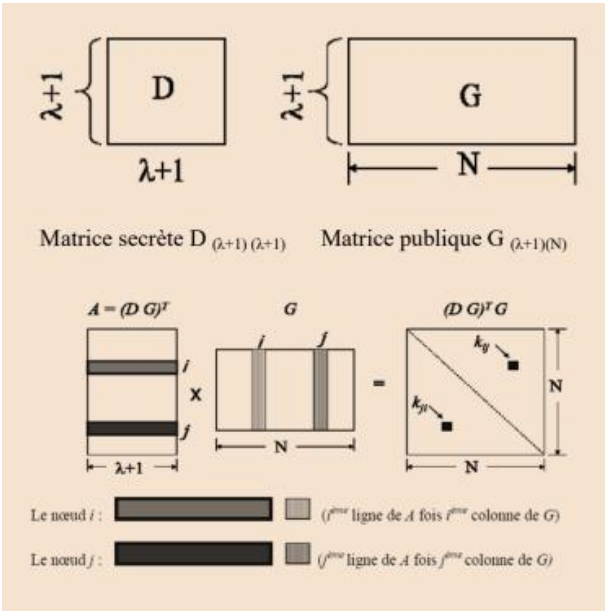

Figure2.11 : Méthode de Blom [45]

Chan et Perrig [89] ont présenté un schéma déterministe appelé PIKE (Peer Intermediaries for Key Establishment), dans lequel les clés secrète pour les communications dans le réseau sont pré-chargées pour que n'importe quel couple de nœuds A et B puisse toujours avoir la possibilité de trouver un nœud C du réseau qui ayant une clé commune avec A et B. Alors A pourra utiliser C comme nœud intermédiaire de confiance afin de transmettre son message d'établissement de clé à B. [45]

Les identifiants (ID) des N nœuds sont organisés dans une structure en grille à deux dimensions ($\sqrt{N}\times\sqrt{N}$). Chaque ID du nœud a une coordonnée unique (x,y), où x,y $\in\{0,1,2,\ldots,\sqrt{N}-1\}$. Chaque nœud partage des clés secrète uniques avec $2(\sqrt{N}-1)$ nœuds qui ont la même coordonnée x ou y. Si deux nœuds ne possèdent pas de coordonnées x ou y communes, ils doivent choisir un nœud intermédiaire possédant une coordonnée x ou y commune avec les deux pour les aider à établir une clé par paire en toute sécurité. [45]

La figure 2.12 illustre l'idée de base du schéma PIKE. Des lignes sombres connectent les nœuds qui partagent une clé unique avec le nœud A, et Les lignes lumineuses connectent les nœuds qui partagent une clé unique avec le nœud B. Il existe 2 nœuds qui partagent une clé unique avec les nœuds A et B. Ainsi, ils peuvent jouer le rôle d'intermédiaires de confiance dans l'établissement de clés entre A et B. Une fois le nœud intermédiaire C élu, A lancé le processus d'établissement de clés. Cependant, Chaque message échangé est accompagné d'un message d'authentification MAC (code) afin de garantir l'intégrité. [45]

00	01	02	03	04	...	09
10	11	12	13	14	...	19
20	21	22	23	24	...	29
30	31	32	33	34	...	39
.	.	.	.	.		.
.	.	.	.	.		.
.	.	.	.	.		.
90	91	92	93	94	...	99

Figure 2.12 : Un exemple d'Espace virtuel d'identifiants de nœudsd'un réseau de 100 nœuds pour le schéma PIKE [53].

- **Schémas basés sur la pré-distribution d'une clé maîtresse**

Afin d'assurer le déterminisme, Une clé commune est pré-chargée sur tous les nœuds capteurs avant leurs déploiements. Cette dernière est utilisée pour sécuriser les communications dans la phase d'établissement de clés afin de générer des clés par-paires entre chacun des deux nœuds, et qui sera effacée après l'établissement de clés.

Lai et autres [58] ont proposé BROSK (Broadcast Session Key). Dans ce schéma, une seule clé est chargée dans les nœuds avant le déploiement. Une paire de nœuds capteurs peut être établie une clé de session à l'aide de cette clé principale et d'un nombre aléatoire échangé entre chaque nœud 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. Ainsi, ce schéma n'a aucune résilience. En dehors de cela, il n'y a pas d'authentification car tous les nœuds capteurs ont la même clé principale [58].

2.8.2. Schémas basés sur la topologie de réseau :

Selon la topologie de réseau, les protocoles de gestion de clés dans un RCSF peuvent être hiérarchiques ou plats.. Dans un réseau hiérarchique, des clés par paire, par groupe et par réseau sont nécessaires pour sécuriser le flux de données, qui peuvent divisée en trois types :(i) par paire (unicast) entre des paires des nœuds capteurs et des nœuds capteurs à la station de base, (ii) par groupe (multidiffusion) au sein d'un groupe des nœuds capteurs, (iii) par réseau (diffusion) des stations de base aux nœuds capteurs. [49]

Dans un RCSF plat, il n'y a pas de membre riche en ressources et les nœuds de capteur ont des capacités équivalentes. Pour le flux de données, il est similaire au flux de données dans un réseau RCSF hiérarchique, à la différence que des messages réseau (diffusion) peuvent être envoyés par tous les nœuds capteurs. Les nœuds capteurs utilisent directement des clés pré-distribuées ou utilisent des clés matériaux pour générer de manière dynamique des clés par paires et par groupes.

Dans l'intention d'économie d'énergie, l'utilisation d'une topologie hiérarchique peut simplifier et améliorer l'évolutivité et l'efficacité de la procédure de gestion de clés. Dans la section suivante, nous présentons des protocoles de gestion de clés hiérarchiques.

2.8.2.1. Schémas hiérarchiques :

Zhu et autres proposent le protocole déterministe LEAP (Localized Encryption and Authentication Protocol) [42]. Ce protocole conçu pour les réseaux de capteurs hiérarchiques

afin de limiter l'impact du nœud compromis sur le voisinage immédiat. Pour réduire et minimiser l'implication de la station de base dans le processus de gestion de clés, LEAP 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, ce qui réduit en conséquence la consommation d'énergie et le trafic dans le réseau. LEAP se base sur l'exploitation du temps minimal Tmin (temps nécessaire pour qu'un adversaire puisse compromettre un nœud et récupérer la clé de ce dernier) pour permettre à deux nœuds voisins d'établir une clé symétrique, à partir de la clé pré-chargée sur chaque capteur avant le déploiement, ainsi que de supprimer cette dernière de la mémoire du nœud compromis en un temps T <Tmin. [58]

Mamun et autres [] présentent KMP, un système de gestion de clé sécurisé adopté pour les RCSFs hiérarchique. Ce système utilise la pré-distribution de clés partielles dans les nœuds capteurs avant le déploiement. Dans un premier temps, un pool des clés partielles est généré par la SB, puis chaque nœud de capteur est pré-distribué avec une clé de réseau N_K (partagée par tous les nœuds), un pool des clés partielles P, une liste d'index L (des clés partielles) et un identifiant unique ID. Dans un deuxième temps, pour chaque cluster i, la station de base envoie à chaque CH_i une liste d'index des clés partielles identifiée par LPK_i afin d'utiliser dans son cluster. Le cluster Head (CH) diffuse ensuite le LPK_i à tous les nœuds membres du cluster i. Une fois qu'un nœud de capteur a enseigné quelles clés partielles il utilisera avec son CH, il supprime le reste des clés partielles de P qui a été inséré. [67]

À ce point, les nœuds de capteurs sont prêts à établir les clés de communication. Pour chaque membre du cluster i, le CH_i envoie une liste d'ordres unique O_{CH_i} contenant la liste ordonnée des numéros d'index de q clés partielles sélectionnées à partir de LPK_i. En réponse, chaque nœud membre A_i crée également une liste d'ordres O_{A_i} avec un ordre différent des index et envoie l' O_{A_i} à CH_i. Les nœuds capteurs A_i et le cluster Head CH_i peuvent construire maintenant leurs clés de communication secrètes pour chaque cycle. Pour plus de simplicité, les auteurs ont utilisé une simple fonction de concaténation pour créer une clé de communication à partir des deux clés partielles ($K^t_{A_iCH_i} = L(O_{A_i}[t]) \parallel L(O_{CH_i}[t])$, où O_{Ai} $[t]$ renvoie le $t^{ème}$ index de A_i). Après chaque cycle, le CH et les membres peuvent régénérer des nouvelles listes d'ordres pour créer des nouvelles clés de communication. [67]

D'autres travaux [43] de gestion de clés sont récemment proposés dans les RCSFs hiérarchiques, mais considèrent des réseaux hétérogènes où les nœuds ont des capacités différentes avec des rôles différents.

2.9. La gestion de clés dynamique

Dans les schémas de gestion de clés statique, toutes les clés sont pré-distribuées aux nœuds avant le déploiement et aucun processus de renouvellement de clés n'est appliqué. Par conséquent, la probabilité que les clés soient compromises est augmentée considérablement. Un schéma de gestion dynamique des clés est un processus de régénération des clés. En effet, Il existe plusieurs raisons justifient le renouvellement de clés du réseau RCSF:

- Renouvellement périodique : Cela se fait volontairement après une période de temps spécifiée. La clé ne doit pas être utilisée pendant longtemps car elle offre des possibilités de compromis. Selon Abdullah et M. Bellare **[39]**, si la clé utilisée est longueur de k bits, elle doit être changée après $2^{2k/3}$ nombre de chiffrement. [39]
- Renouvellement à cause d'une compromission de nœud: Cette phase est déclenchée par la station de base lorsqu'elle détecte une anomalie du réseau, et s'effectue soit : de manière préventive : lors d'une tentative d'accès illégale par un attaquant ou bien obligatoirement : après la compromission d'un ou de plusieurs nœuds capteurs du réseau. [64]
- Renouvellement en cas de changement de la fonction du nœud : Cette phase ne concerne que les clusters d'une structure hiérarchique. Pour prolonger la durée de vie de l'ensemble du réseau, il est nécessaire de changer le chef de groupe. Ainsi, l'un de ses nœuds membres devient un chef de groupe. Par conséquent, certaines clés doivent être renouvelées pour assurer la sécurité. [64]

La gestion dynamique de clé possède plusieurs avantages, parmi lesquels on peut citer les suivants : [25]

- ✓ La durée de vie du réseau accrue, puisque toutes les clés capturées sont remplacées en temps opportun grâce à un processus connu sous le nom de rekeying ;
- ✓ Offre une plus grande probabilité de connectivité ;
- ✓ Fournit un meilleur support pour l'extension du réseau; lors de l'ajout de nouveaux nœuds ;

- ✓ Une taille de pool de clés plus petite, un minimum de stockage pour maintenir les clés dans les nœuds ;
- ✓ Moins de temps de communication pour générer des clés dynamiquement.

L'inconvénient majeur de ce type de gestion de clé est qu'il nécessite un nombre important de messages à échanger pour générer dynamiquement des clés, ce qui n'est pas toléré dans les RCSF. [25]

2.10. Quelques schémas de gestion de clés dynamique

Dans les réseaux de capteurs sans fil, plusieurs systèmes de gestion de clés statique, ont été proposés pour établir des communications sécurisées entre les nœuds capteurs. Cependant, peu de travaux envisagent un schéma de gestion de clés dynamique. Dans cette section, nous présentons des protocoles de gestion de clés dynamique.

Eltoweissy et autres [60] proposent un schéma appelé "exclusion-based system"(EBS). EBS est une formulation combinatoire du problème de gestion de clé par groupe qui permet de produire des résultats optimaux par rapport aux paramètres n, k et m, où n est la taille du groupe, k est le nombre de clés stockées par chaque membre, et m est le nombre de messages de renouvellement. EBS utilise une technique pour déterminer les valeurs optimales de k et m en fonction n, et décrire le compromis entre k et m. Dans les schémas basés sur EBS, chaque nœud n est assigné à k clés d'un pool de taille P = k + m (1 <k; m <n, où n est le nombre de nœuds capteurs dans le réseau). Le processus de renouvellement est déclenché sur l'ensemble du réseau pour renouveler les clés du réseau si une capture d'un nœud est détectée. Les m clés, non connues par le nœud capturé dans le réseau, sont utilisés pour remplacer les clés des nœuds non compromis. Dans le processus de renouvellement, les clés de remplacement sont générées, cryptées avec toutes les m clés inconnues aux nœuds capturés et distribuées seulement aux autres nœuds qui connaissent collectivement les m clés. [60]
L'inconvénient majeur de ce système est le coût du processus de renouvellement dans le cas où un petit nombre de nœuds dans le réseau est compromis (le renouvellement est déclenché sur l'ensemble du réseau), ainsi que des informations sur l'ensemble du réseau pourraient être découvertes par un adversaire après une attaque réussie. [60]

Zhang et autres [61] a proposé un schéma de gestion des clés déterministes distribuées à efficacité énergétique réduite s'appelle EDDK (energy-efficient distributed deterministic key management scheme), qui visait à résoudre les attaques d'épuisement des ressources et les

attaques par déni de service. Dans le schéma EDDK, chaque nœud est pré-chargé avec une fonction pseudo-aléatoire f et une clé initiale K_I qui peut utiliser pour calculer sa clé individuelle. De plus, chaque nœud de capteur stocke une table qui maintient les informations des nœuds voisins tels que ID de voisin, clé par paire, numéro de séquence. Il partage également une clé de cluster locale avec ses nœuds voisins et stocke également cette clé dans la table. Ce schéma comprend trois phases: l'établissement de clés, transfert des données et maintenance de clés. [61]

Dans la phase d'établissement de la clé par paire, un nœud A calcule d'abord sa clé individuelle K_A par $K_A = f_{K_I}(ID_A)$, puis génère une séquence numérique aléatoire SN_A et diffuse le message $JOIN$ aux nœuds voisins. Le message $JOIN$ contient $ID_A \parallel E_{K_A}(SN_A \parallel K_G) \parallel MAC_{K_A}(ID_A \parallel E_{K_A}(SN_A \parallel K_G))$. Lorsque les deux nœuds A et B reçoivent le message $JOIN$ l'un de l'autre, ils vérifient l'exactitude du message $JOIN$. Après vérification, les clés par paires sont générées: $K_{AB} = f_{K_I}(K_A \oplus K_B, SN_A \oplus SN_B)$. Comme LEAP, une fois que le temporisateur d'établissement de clé a atteint sa valeur de seuil prédéfinie, un nœud supprime toutes les clés individuelles de ses voisins, les nombres aléatoires, la fonction pseudo-aléatoire et la clé initiale pour améliorer la sécurité et économiser l'espace de stockage dans le nœud.[61]

Le principal avantage du schéma EDDK réside dans le fait que les clés par paire sont décentralisées et que la compromission d'un nœud de capteur n'affecte pas les autres liaisons de communication. Il est également résistant aux attaques par rejeu, à identité multiple (Sybil) et à la réplication de nœud. Le principal inconvénient d'EDDK est qu'il n'est pas applicable dans les réseaux denses, car chaque nœud capteur doit stocker une table, qui inclut les informations de tous ses voisins. [61]

2.11. Métriques d'évaluation:

Selon la fonctionnalité et l'environnement d'application de la gestion des clés, 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.

2.11.1. Efficacité des ressources:

Dans les réseaux de capteurs, l'efficacité des ressources représente une métrique de performance significative. Pour cela, un bon schéma de gestion des clés ne devrait pas consommer une grande quantité de ressources. Les ressources peuvent être ici :

Puissance de calcul : est mesurée en termes de quantité de cycles de processeur nécessaires pour l'établissement de clés.

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.

Espace de stockage : est la quantité de mémoire nécessaire pour enregistrer les informations de sécurité, tel que les clés. En effet, l'espace mémoire des nœuds capteurs n'est que de quelques dizaines de kilo-octets, ce qui signifie que le système de gestion de clés ne peut pas stocker trop de clés dans les nœuds capteurs**.**

2.11.2. Résilience contre la capture de nœud

Résilience contre la capture de nœud ou résistance contre la capture de nœud, cette métrique mesure comment le RCSF est compromis quand un nœud est compromis, et l'influence de ce nœud sur la sécurité du réseau. En effet, quand un nœud est capturé par un adversaire, son secret entier ainsi que les liens établis avec ses voisins sont compromis. Les effets d'une telle attaque peuvent affecter d'autres nœuds capteurs 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. Ainsi, 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. [25]

2.11.3. La connectivité:

La connectivité se définie comme la probabilité qu'un nœud puisse partage une clé avec l'ensemble de ses voisins (c.à.d. établir un lien sécurisé). 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. Par conséquent, pour garantir la continuité de la sécurité, la méthode de gestion de clés (déterministe ou probabiliste) doit être capable de garantir une bonne connectivité du réseau. [57]

2.11.4. Passage à l'échelle (scalability):

Le nombre de nœuds déployés dans un réseau de capteur sans fil peut être à l'ordre de centaines, voire plusieurs milliers. Pour certaines applications, il peut atteindre quelques millions. De plus, pendant toute la durée de vie du réseau de capteurs, des nœuds peuvent rejoindre ou quitter. Afin d'assurer le bon fonctionnement du réseau, les schémas de gestion de clés doivent pouvoir s'adapter à différentes tailles de réseau. Par ailleurs, les fonctionnalités de sécurité et d'efficacité des petits réseaux doivent être conservées lorsqu'elles sont appliquées aux réseaux plus grands. [56]

2.12. Conclusion

Nous avons abordé dans ce chapitre le problème de sécurité dans les RCSFs, à savoir les différentes vulnérabilités qui peuvent être rencontrées, les attaques qui menacent les RCSFs, ainsi que les différents mécanismes de sécurité adaptées tel que les primitives cryptographiques et la gestion de clés dans les RCSFs.

Nous avons déduit que la gestion de clés dans un RCSF est un processus très important et nécessaire pour garantir un haut niveau de sécurité dans un réseau assez vulnérable. Pour cela, Nous avons aussi présenté un état de l'art qui détaille les composants d'un protocole de gestion de clés destiné aux RCSFs en particulier. Ensuite, quelques solutions existantes sont classées et décrites.

Nous avons vu que les protocoles basés sur la méthode de pré-distribution sont les plus appropries aux RCSF, pour leur faible coût. L'inadaptation de la cryptographie asymétrique a conduit les recherches dans la gestion de clés vers la cryptographie symétrique. Malgré que plusieurs solutions de ces schémas paraissent prometteuses, il existe encore certains défis à relever qui nécessitent une prise en considération par les solutions de sécurité.

Chapitre 3

Implémentation et évaluation d'un mécanisme de renouvellement de clés

3.1. Introduction

Pour la majorité des applications qui utilisent les RCSFs, il est crucial de mettre en place un mécanisme de sécurité. Ce dernier est d'autant plus nécessaire lorsque les nœuds capteurs sont présents dans un environnement peu sûr. La gestion de clés joue un rôle central pour assurer la sécurité, car pratiquement tous les mécanismes de sécurité sont basés sur le cryptage où sont liés à celui-ci. Dans les RCSFs, cette gestion est cruciale pour pouvoir offrir aux communications inter nœuds un niveau de sécurisation appréciable. Les schémas existants de gestion de clés se focalisent sur l'efficacité d'établissement de clés après le déploiement du réseau, et ignorent le renouvellement de clés qui rend la gestion de clés dynamique et ajoute une difficulté supplémentaire à la tâche de l'attaquant.

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 mecanisme de renouvellement de clés du travail [1] 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 et la consommation d'énergie.

Dans ce chapitre, nous présentons trois stratégies de renouvellement de clés qui ont été développées par les auteurs du travail [1] et dédiées pour une gestion de clés associée aux RCSFs ayant une topologie hiérarchique. Nous commencerons d'abord par présenter la motivation derrière ce choix, ensuite nous présenterons les détails fonctionnels de ce processus. Nous évaluerons par la suite leurs performances.

3.2. Motivation du choix du protocole

Dans les RCSFs, quand on étudie une méthode de gestion des clés, il est nécessaire de prendre en compte la notion de robustesse de la méthode, de la consommation d'énergie et de la taille de la mémoire utilisée.

- La robustesse est liée à la nature des clés de cryptage et la façon de distribution des clés.
- La consommation d'énergie est liée au nombre de messages échangés durant l'installation des clés, et le coût des opérations de calcul des clés secrètes partagées.
- La taille de mémoire utilisée est liée à la taille de la clé et le nombre de clés stockées.

La gestion des clés dans ce cas est non seulement une question critique mais doit tenir compte des faibles ressources des nœuds. Plusieurs schémas de gestion de clés ont été proposés pour

établir des communications sécurisées entre les nœuds capteurs. Cependant, peu de travaux envisagent un schéma de gestion de clés dynamique. Après l'étude de certains protocoles existants dans la littérature, nous avons constaté que le protocole SKWN est un choix efficace pour garantir la sécurité et le renouvellement de clés dans les réseaux capteurs sans fil, ce qui réduit les risques de compromission de la sécurité. Plusieurs avantages sont attribués au protocole SKWN [1]

- 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 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.
- SKWN est modifiable et évolutif;
- SKWN est déterministe et repose sur la cryptographie symétrique.
- Robuste contre les attaques de capture de nœuds;

3.3. Modèle du réseau :

Notre travail se concentre sur les réseaux RCSFs hiérarchiques en clusters pour leur capacité à optimiser la consommation d'énergie. Cette capacité est obtenue grâce aux rôles de nœuds distincts : la station de base (BS: Base station), le cluster-head (CH : Cluster Head), et le membre du cluster (CM : Cluster member).

Le principe est de partitionner le réseau en plusieurs groupes (ou clusters) dont chacun est vu comme un sous réseau ayant la topologie en étoile. Chaque groupe possède un chef qui relie les membres de son groupe à la station de base. La communication entre les nœuds capteurs et le chef du cluster peut être directe ou indirecte (en multi-sauts) pour les nœuds distants. Ainsi, il peut y avoir plusieurs niveaux dans la hiérarchie, où les chefs des clusters forment entre eux des chaînes menant vers la station de base (voir figure 3.1)

Les cluster-heads sont répartis uniformément dans le réseau en fonction de critères tels que la portée de communication et les capacités en ressources et en énergie. La rotation des cluster-head doit également être considérée pour prolonger la durée de vie du réseau

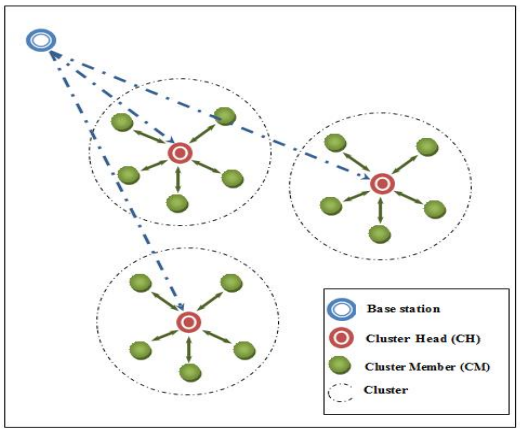

Figure 3.1 : Modèle d'architectures hiérarchique pour un RCSF

3.4. Description détaillée sur le fonctionnement

SKWN est un nouveau schéma de gestion de clés intelligent et dynamique pour les réseaux de capteurs sans fil hiérarchiques. Il comprend trois sous-schémas dédiés à (i) a l'Établissement de clés, (ii) Au renouvellement de clés, et (iii) à l'Intégration d'un nouveau nœud. Dans le cadre de notre étude, nous nous sommes intéressés au sous schéma lié au renouvellement de clés. Dans ce dernier, un renouvellement de clés est effectué à la demande. Il y a trois raisons pour changer une clé cryptographique:

- Détection d'un adversaire qui a compromis un CH.
- Détection d'un adversaire qui a compromis un CM.
- Élection d'un nouveau CH.

Trois niveaux de sécurité différents sont utilisés en fonction des trois cas de renouvellement. En effet, le niveau de sécurité change par rapport à la raison du renouvellement de clés. Dans ce qui suit, nous présentons des processus de renouvellement pour chaque cas. Le tableau 3.1 résume des notations que nous avons utilisées pour détailler chaque processus.

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
n	le nombre de membres de cluster
C	le nombre de clusters.

Tableau 3.1 : Acronymes définition

3.4.1. Processus de renouvellement de clés pour le cluster-head compromis (Comp_CH)

Tout d'abord, il est important de comprendre que le cluster-head est le nœud principal dans un réseau de capteurs sans fil. Il est responsable de la gestion et de la coordination des autres nœuds du réseau. Lorsqu'un cluster-head est compromis, cela signifie qu'un attaquant a réussi à prendre le contrôle de ce nœud. Cela peut avoir des conséquences graves pour la sécurité du réseau, car un attaquant peut maintenant accéder à toutes les données transmises entre les nœuds, ainsi qu'à tous les dispositifs connectés au RCSF. Le renouvellement de clés est donc une mesure indispensable pour rétablir la sécurité du réseau et empêcher l'attaquant d'avoir accès à des données sensibles.

Après avoir compromis un nœud CH, la station de base commence par élire un nouveau CH individuellement. Ensuite, il envoie un message contenant le type de message pour en déterminer le but. [56]

$$BS \rightarrow CH_{New}: id_{BS} \parallel E_{K_{in}}\{REFRESH\_CHcomp, CPT, N_{BS}\}$$

$$\parallel MAC_{K_{in}}\{id_{BS} \parallel E_{K_{in}}\{REFRESH\_CHcomp, CPT, N_{BS}\}\}$$

Après avoir reçu le message de rafraîchissement, le nouveau nœud CH diffuse le message $REFRESH\_CHcomp$ avec le niveau de sécurité requis. [38]

$$CH_{New} \rightarrow * : id_{CH_{New}} \parallel Lev \parallel E_{K_r}\left\{id_{CH_{compromise}}, REFRESH\_CHcomp, CPT, N_{CH_{New}}\right\}$$

$$\parallel MAC_{K_r}\left\{id_{CH_{New}} \parallel Lev \parallel E_{K_r}\{id_{CH\_compromise}, REFRESH\_CHcomp, CPT, N_{CH_{New}}\}\right\}$$

Après avoir reçu le message $REFRESH\_CHcomp$, chaque nœud CH efface la clé partagée avec le CH compromis et calcule une nouvelle clé par paire partagée avec le nouveau nœud CH. [56]

$$K_{CH_\alpha - CH_{New}} = H_{K_r}^{CPT}(\max(id_{CH_\alpha}, id_{CH_{New}}) \parallel \min(id_{CH_\alpha}, id_{CH_{New}}) \parallel CPT) \quad (3.1)$$

Le message $REFRESH\_CHcomp\_REP$ est ensuite envoyé au nouveau CH. Ce message contient la liste d'identification L_id_{CM} de l'ensemble des nœuds membres. [68]

$$CH_\alpha \rightarrow CH_{New}: id_{CH_\alpha} \parallel Lev \parallel E_{K_r}\{REFRESH\_CHcomp\_REP, CPT, N_{CH_\alpha}, L\_id_{CM}\}$$

$$\parallel MAC_{K_r}\left\{id_{CH_\alpha} \parallel Lev \parallel E_{K_r}\{REFRESH\_CHcomp\_REP, CPT, N_{CH_\alpha}, L\_id_{CM}\}\right\}$$

Chaque nœud CM (membre du groupe du nouveau CH), recevant le message $REFRESH\_CHcomp$, efface la clé partagée avec le nœud CH compromis et calcule une nouvelle clé où

$$K_{CM_j - CH_{New}} = H_{K_r}^{CPT}(K_{CM_j - CM_l} \parallel id_{CH_{compromise}}) \quad (3.2)$$

$K_{CM_j - CM_l}$ dans la formule est la clé précédente partagée entre le nœud CM_j et le noeud $CM_l = CH_{New}$

En réponse, le nœud CM diffuse un message $REFRESH\_CHcomp\_REP$.

$$CM_j \rightarrow * : id_{CM_j} \parallel id_{CH_{New}} \parallel E_{K_r}\left\{REFRESH\_CHcomp\_REP, CPT, N_{CM_j}\right\}$$

$$\parallel MAC_{K_r}\left\{id_{CM_j} \parallel id_{CH_{New}} \parallel E_{K_r}\left\{REFRESH\_CHcomp\_REP, CPT, N_{CM_j}\right\}\right\}$$

Le nouveau CH reçoit deux types de messages $REFRESH\_CHcomp\_REP$. Le premier est diffusé par tous les membres de leur cluster pour vérifier son authenticité et rafraîchir la clé partagée entre eux comme la formule (3.2). Le second est envoyé par les autres nœuds CH afin de rafraîchir la clé à l'aide de la formule (3.1). [56]

Après avoir reçu le message $REFRESH\_CHcomp\_REP$ diffusé par les autres nœuds CM du même cluster, le nœud CM vérifie l'authenticité et rafraîchit les clés précédentes avec:

$$K_{CM_i-CM_j} = H_{K_r}^{CPT}(K_{CM_i-CM_j}) \tag{3.3}$$

Selon les étapes décrites ci-dessus, le nœud CH compromis sera isolé, chaque clé partagée avec ce nœud sera effacée et toutes les clés nécessaires seront actualisées. La figure 3.2 résume le processus de renouvellement de clés.

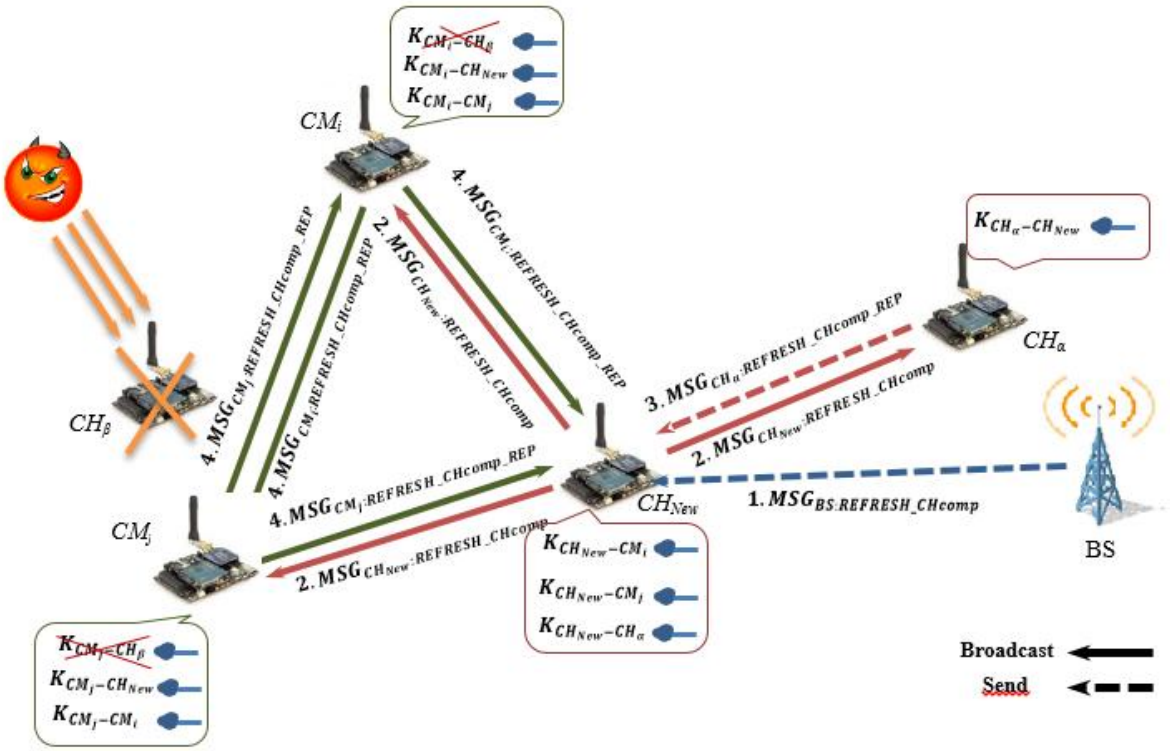

Figure 3.2. Le processus de renouvellement de clés pour un cluster-head compromis (Comp_CH)

3.4.2. Processus de renouvellement de clés pour un membre de cluster compromis (Comp_CM)

Ce processus consiste à isoler le nœud CM compromis, afin de limiter son accès aux autres membres de cluster et protéger le système. En effet, un nœud CH est plus important qu'un nœud CM. Par conséquent, il est évident de réduit dans ce cas le niveau de sécurité requis. Le processus de renouvellement de clés est décrit comme suit:

Lorsqu'un nœud CH détecte un adversaire, qui compromet un membre du cluster, il diffuse un message $REFRESH\_CMcomp$ pour notifier les autres nœuds et rafraîchir les clés. Le message de rafraîchissement doit contenir l'ID de nœud compromis et le niveau de sécurité requis. [68]

$$CH_\alpha \rightarrow * : id_{CH_\alpha} \parallel Lev \parallel E_{K_r}\{id_{CM\_compromise}, REFRESH\_CMcomp, CPT, N_{CH_\alpha}\}$$

$$\parallel MAC_{K_r}\left\{id_{CH_\alpha} \parallel Lev \parallel E_{K_r}\{id_{CM\_compromise}, REFRESH\_CMcomp, CPT, N_{CH_\alpha}\}\right\}$$

Chaque nœud CH recevant le message $REFRESH\_CMcomp$ efface l'identification du nœud CM compromis de la liste appropriée L_id_{CM} et rafraîchit la clé par paire avec le CH notifié avec:

$$K_{CH_\beta - CH_\alpha} = H_{K_r}^{CPT}(K_{CH_\beta - CH_\alpha}) \tag{3.4}$$

Chaque nœud CM (membre de CH émetteur), qui reçoit le message $REFRESH\_CMcomp$, efface l'identification et la clé du nœud CM compromet et rafraîchit les clés avec:

$$K_{CM_j - CH_\alpha} = H_{K_r}^{CPT}(K_{CM_j - CH_\alpha} \parallel id_{CM_{compromise}}) \tag{3.5}$$

Le message de réponse de rafraîchissement est diffusé par le nœud CM:

$$CM_j \rightarrow * : id_{CM_j} \parallel id_{CH_\alpha} \parallel E_{K_r}\left\{REFRESH\_CMcomp\_REP, CPT, N_{CM_j}\right\}$$

$$\parallel MAC_{K_r}\left\{id_{CM_j} \parallel id_{CH_\alpha} \parallel E_{K_r}\left\{REFRESH\_CMcomp\_REP, CPT, N_{CM_j}\right\}\right\}$$

Le message $REFRESH\_CMcomp\_REP$ reçu est utilisé pour vérifier l'authentification des autres nœuds CM de leur cluster et rafraîchit les clés avec la formule (3.3). [56]

Après avoir reçu le message $REFRESH\_CMcomp\_REP$ diffusé par les autres nœuds CM de leur cluster, le nœud CH vérifie l'authenticité et rafraîchit les clés précédentes avec la formule (3.5). Ensuite, les clés précédentes partagées avec les nœuds CH sont actualisées avec la for

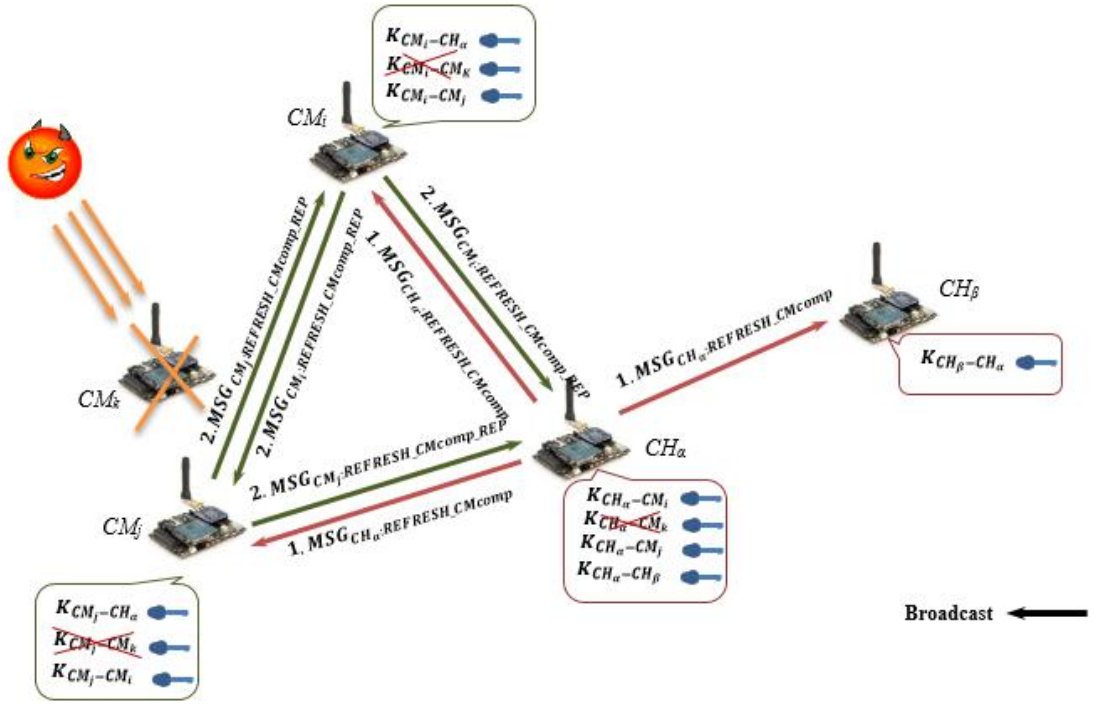

Figure 3.3 : Le processus de renouvellement de clés pour un membre de cluster compromis (Comp_CM)

À la fin de ces étapes, le nœud CM compromis sera isolé, chaque clé partagée avec ce nœud sera effacée et toutes les clés nécessaires seront rafraîchies. Le processus de renouvellement de clés dans ce cas est illustré à la figure 3.3.

3.4.3. Processus de renouvellement de clés pour l'élection d'un nouveau cluster-head (ELEC)

Afin de prolonger la durée de vie de réseau, il est nécessaire de remplacer le nœud CH. Ainsi, certaines clés doivent être renouvelées pour garantir la sécurité. Dans ce cas, l'absence d'un nœud compromis CH ou CM réduit le niveau de sécurité requis. La procédure détaillée pour le processus de renouvellement de clés est décrite comme suit:

Lorsque le nouveau CH est élu, il lance le processus de renouvellement de clés en diffusant le message de rafraîchissement. Ce message contient l'ID du nœud CH précédent

$$CH_{New} \rightarrow *: id_{CH_{New}} \parallel Lev \parallel E_{K_r}\{id_{CH\_previous}, REFRESH\_ELEC, CPT, N_{CH_{New}}\}$$
$$\parallel MAC_{K_r}\left\{id_{CH_{New}} \parallel Lev \parallel E_{K_r}\left\{id_{CH_{previous}}, REFRESH\_ELEC, CPT, N_{CH_{New}}\right\}\right\}$$

Chaque nœud CH, après avoir vérifié l'authenticité du message de demande de renouvellement de clés du nouveau cluster-head, remplace l'identification du nouveau nœud CH par l'identification du nœud CH précédent dans la liste L_id_{CM}. Il calcule ensuite la nouvelle clé partagée entre eux en utilisant la formule (3.1). Il envoie ensuite le message $REFRESH\_ELEC\_REP$ au nouveau CH, qui contient l'identification de l'ensemble de ses membres L_id_{CM}.

$$CH_{\alpha} \rightarrow CH_{New}: id_{CH_{\alpha}} \parallel Lev \parallel E_{K_r}\{REFRESH\_ELEC\_REP, CPT, N_{CH_{\alpha}}, L\_id_{CM}\}$$
$$\parallel MAC_{K_r}\left\{id_{CH_{\alpha}} \parallel Lev \parallel E_{K_r}\{REFRESH\_ELEC\_REP, CPT, N_{CH_{\alpha}}, L\_id_{CM}\}\right\}$$

Chaque nœud CM (membre de CH émetteur), qui reçoit le message $REFRESH\_ELEC$, remplace la clé partagée avec le nœud CH précédent par la clé suivante:

$$K_{CM_j - CH_{New}} = H_{K_r}^{CPT}\left(K_{CM_j - CM_l} \parallel id_{CH_{New}}\right) \quad (3.6)$$

Tels que $K_{CM_j-CM_l}$dans la formule est la clé précédente partagée entre le nœud CM_j et le nœud $CM_l = CH_{New}$

Un rafraîchissement de toutes les clés partagées est effectuée avec les autres nœuds CM de leur cluster et la clé partagée avec le CH précédent (revenu membre) avec la formule (3.3).

Après avoir reçu le message $REFRESH\_ELEC$, le CH précédent calcule la clé partagée avec le nouveau nœud CH avec la formule (3.6) et rafraîchit les clés précédentes partagées avec les nœuds CM avec la formule (3.3).

Après avoir reçu le message $REFRESH\_ELEC\_REP$ diffusé par les autres nœuds CH, le nouveau nœud CH calcule la clé avec chaque CH émetteur suivant la formule (3.1) et rafraîchit les clés précédentes partagées avec les nœuds CM avec la formule (3.6).

Le nouveau CH rafraîchit non seulement la clé partagée avec ses membres de cluster, mais calcule également la clé partagée avec chaque nœud CH et enregistre la liste de ses membres.

Le processus de renouvellement de clés dans le cas de l'élection d'un nouveau CH est illustré à la figure 3.4

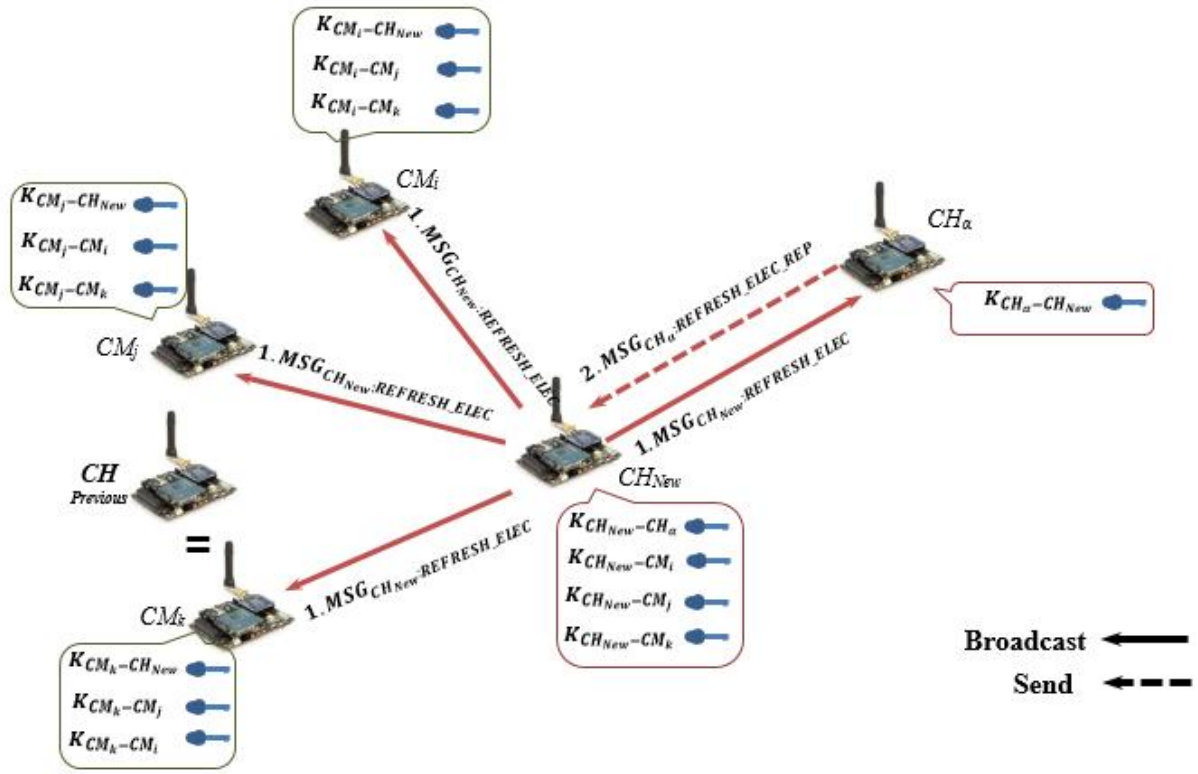

Figure 3.4. Le processus de renouvellement de clés pour une élection d'un nouveau cluster-head (ELEC)

3.5. Simulation

La simulation des RCSFs consiste principalement en la reproduction du comportement des nœuds capteurs et des interactions entre eux. C'est une étape incontournable pour l'évaluation des modèles d'application ou des protocoles de communication.

3.5.1. Présentation de l'environnement Tinyos

On a choisi le système Tinyos pour réaliser notre simulation. Tinyos est un système d'exploitation adapté aux capteurs. Il supporte de nombreuses plates-formes et il fournit des concepts très importants pour réaliser les simulations. Par ailleurs, TinyOS indique l'environnement de simulation d'applications de RCSF qui tournent sous le système d'exploitation TinyOS. Cet environnement est formé par le système d'exploitation TinyOS, l'émulateur Cygwin, le simulateur TOSSIM et tout un ensemble d'outils de simulation. Dans ce contexte, nous présentons dans cette partie l'environnement TinyOS sur lequel fonctionne le simulateur TOSSIM.

- **TinyOS**

TinyOS est un système d'exploitation open source spécialement conçu pour les réseaux de capteurs sans fil. Il est développé en C et est conçu pour être exécuté sur des dispositifs à ressources limitées tels que les nœuds de capteur. TinyOS fournit une interface de programmation simple et une infrastructure de communication pour développer facilement des applications de surveillance et de collecte de données. Les principaux avantages de TinyOS sont sa taille compacte, son faible coût de fonctionnement et sa flexibilité. Il prend en charge une variété de protocoles de communication, y compris IEEE 802.15.4, ZigBee et 6LoWPAN, ainsi que des interfaces pour les capteurs de température, de lumière et de mouvement. TinyOS est un système d'exploitation léger et flexible qui offre une solution de connectivité simple et abordable pour les réseaux de capteurs sans fil. [48]

- **Cygwin**

Cygwin est une collection de logiciels libres à l'origine développés par Cygnus Solutions permettant à différentes versions de Windows d'émuler un système Unix. Cygwin tente de créer un environnement Unix sous Windows, rendant possible l'exécution de ces logiciels après une simple compilation. [49]

- **Le simulateur TOSSIM**

Pour arriver à simuler le comportement des capteurs au sein d'un RCSF, un outil très puissant a été développé et proposé pour TinyOS sous le nom de TOSSIM. TOSSIM simule le comportement des nœuds de capteurs et permet aux développeurs de contrôler l'environnement de simulation, y compris le nombre de nœuds, la disposition physique des nœuds et la topologie du réseau. TOSSIM possède une interface graphique appelée TinyViz qui permet de visualiser de manière intuitive le comportement de chaque capteur au sein du réseau. En plus, il a une extension PowerTOSSIM, qui permet de modéliser la consommation énergétique des différents nœuds du réseau.

3.5.2. Déroulement de mecanisme de renouvellement de clés

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

- **Renouvellement de clés pour le cluster-head compromis**

La figure 3.5 montre quelques transmissions unicast qui se passent à l'algorithme Comp_CH. La transmission unicast est signalée par une flèche rose. Les nœuds CH envoient un message de rafraîchissement ($REFRESH\_CHcomp\_REP$) au nouveau CH.

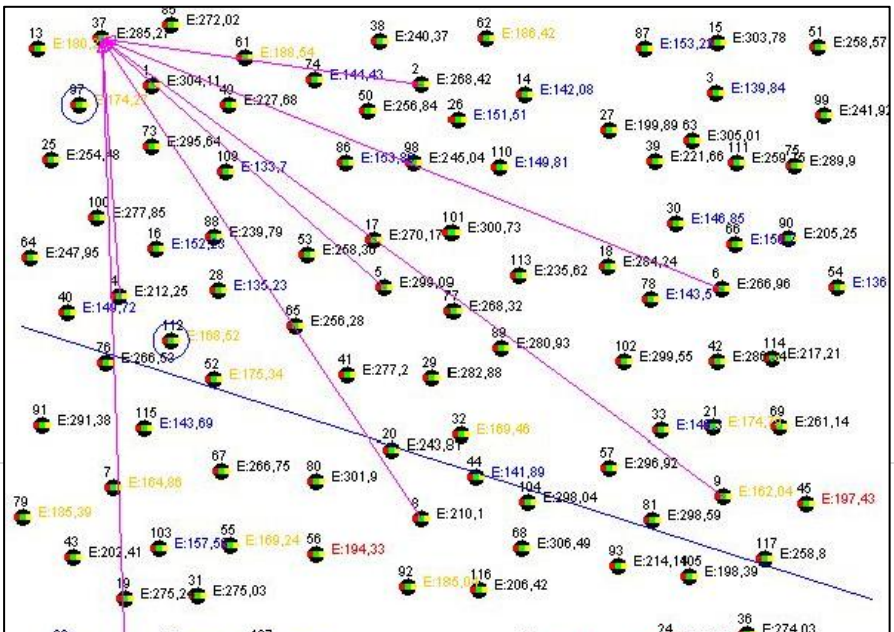

Figure 3.5 : L'envoie de message *REFRESH_CHcomp_REP*

❖ **Renouvellement de clés pour un membre de cluster compromis**

La figure 3.5 montre les transmissions de diffusion qui se passent durant l'algorithme Comp_CM. Une transmission de diffusion est marquée par des cercles bleus. Chaque nœud CM diffuse un message de réponse de rafraîchissement.

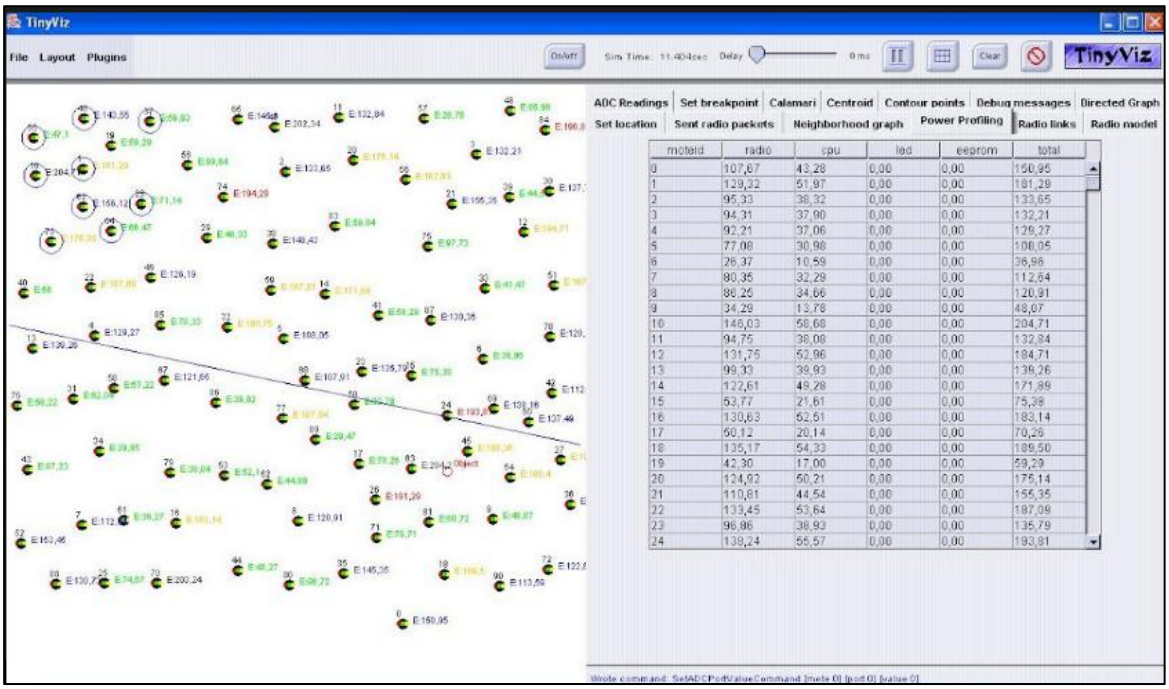

Figure 3.6 : La diffusion de message *REFRESH_CMcomp_REP*

❖ **Renouvellement de clés pour l'élection d'un nouveau cluster-head**

Chaque nœud CH, après la réception du message de demande de renouvellement de clés du nouveau cluster-head, il envoie le message *REFRESH_ELEC_REP* au nouveau CH. La figure 3.6 montre quelques transmissions unicast qui se passent à cette étape de l'algorithme ELEC.

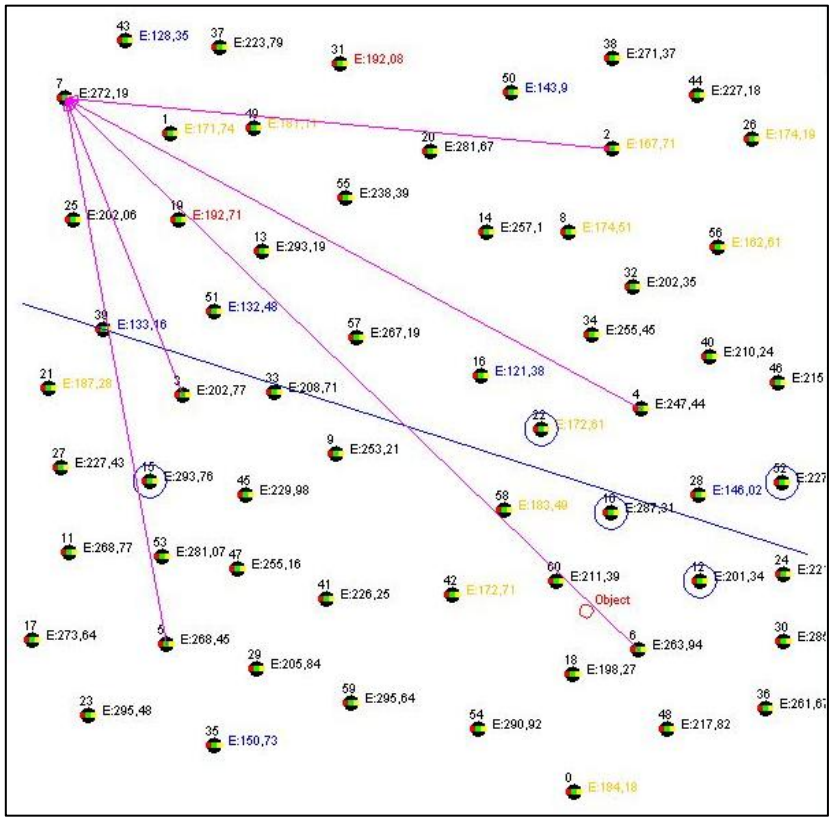

Figure 3.7 : L'envoie de message *REFRESH_ELEC_REP*

3.5.3. Environnement de simulation et résultats

Pour évaluer les performances de différents mécanismes de renouvellement de clés du protocole SKWN, nous les avons implémentés en utilisant le langage de programmation

NesC afin de les intégrer à TinyOS. Un ensemble de simulations sont effectuées en utilisant l'environnement TOSSIM.

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

Nombre de nœuds du réseau	**30, 60, 90, 120, 150**
La taille du réseau	(150 x 150) m^2
Le nombre de CH	10%
Nombre d'itération (simulations)	25: les résultats que nous allons présenter sont une moyenne de 25 simulations pour un même scénario
Taille de paquet de données	31 octets : c'est le paquet de transmission de TinyOS
Le taux d'erreur de transmission	0
La portée radio	22 m

Tableau 3.2 : Les paramètres de simulation

3.5.3.1. La complexité de communication :

Elle consiste à calculer pour chaque nœud du réseau ; le nombre de messages envoyés et reçus. Et ceci dans le but d'avoir une idée sur la complexité de communication dans le réseau. Pour les trois approches, nous avons considéré trois entités (c.-à-d. nœud CH dominant, nœud CH et nœud CM) dans le réseau avec des rôles différents.

- Pour un nœud CM, le nombre de paquets échangés sont les mêmes pour les deux approches Comp_CH et Comp_CM. De plus, ce nombre ne dépend pas de la taille du réseau (Tableau 3.3). En ce qui concerne l'approche ELEC, le nœud CM génère moins de paquets.
- Pour un nœud CH, comme le montre le tableau 3.4, les deux approches ELEC et Comp_CH ont le même nombre de paquets échangés. Alors que dans Comp_CM a un faible coût de communication et cela vient du nombre réduit de paquets échangés
- Pour le nœud CH dans Comp_CM et le nouveau CH élu pour Comp_CH et ELEC, le nœud dominant joue le rôle d'un agent. Pour ce nœud, chaque méthode a un nombre différent de paquets échangés (Tableau 3.5).

	La complexité de calcul	Le coût total de communication
Comp_CH	$1\ Enc + (n-1)Dec + ((n-1) * CPT)\ Hash\ function$	n
Comp_CM	$1\ Enc + (n-1)Dec + ((n-1) * CPT)\ Hash\ function$	n
ELEC	$1\ Dec + (n * CPT)\ Hash\ function$	1

Tableau 3.3 : Comparaison entre les différents mécanismes de renouvellement de clés en termes de complexité de calcul et de communication pour les nœuds CM

	La complexité de calcul	Le coût total de communication
Comp_CH	$1\ Enc\ + 1\ Dec + CPT\ Hash\ function$	2
Comp_CM	$1\ Dec + CPT\ \ Hash\ function$	1
ELEC	$1\ Enc + 1\ Dec + CPT\ Hash\ function$	2

Tableau 3.4: Comparaison entre les différents mécanismes de renouvellement de clés en termes de complexité de calcul et de communication pour les nœuds CH

	La complexité de calcul	Le coût total de communication
Comp_CH	$1\ Enc\ + (n + C - 1)Dec + ((n + C - 2) * CPT)\ Hash\ function$	$n + C$
Comp_CM	$1\ Enc\ + (n - 1)Dec + ((n + C - 2) * CPT)\ Hash\ function$	n
ELEC	$1\ Enc\ + (C - 1)Dec + ((n + C - 1) * CPT)\ Hash\ function$	C

Tableau 3.5: Comparaison entre les différents mécanismes de renouvellement de clés en termes de complexité de calcul et de communication pour le nœuds CH dominant

La figure 3.7 illustre la complexité de communication de chaque méthode pour différentes tailles de réseau. Par conséquent, les résultats sont compatibles avec la comparaison faite dans les tableaux 3.2, 3.3et 3.4.

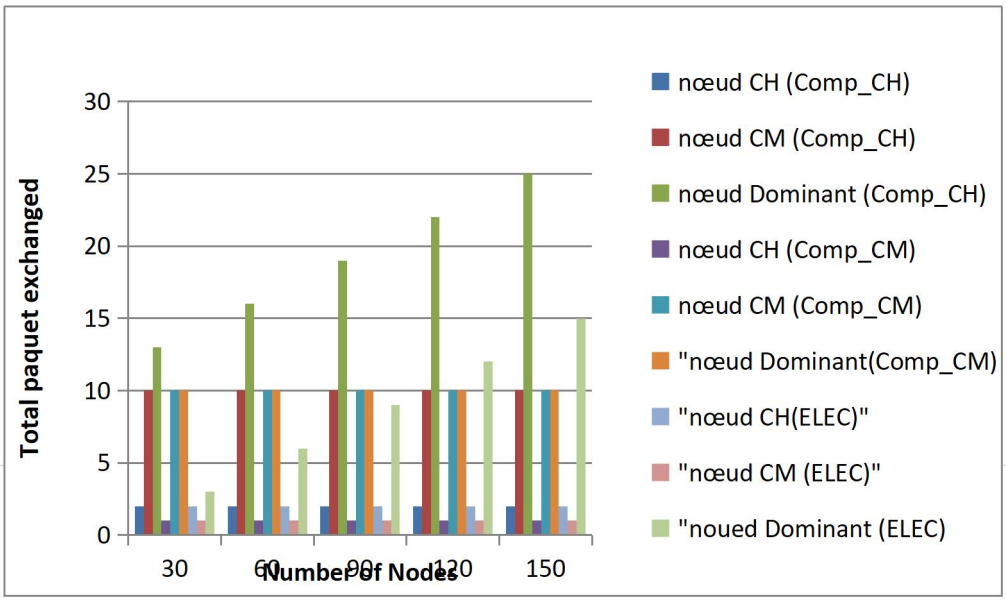

Figure 3.8 Comparaison du nombre de paquets échangés.

3.5.3.2. La consommation d'énergie

La consommation d'énergie est un paramètre important pour tout schéma de renouvellement de clés. Par conséquent, nous avons utilisé le plugin PowerTOSSIM dans TinyViz pour analyser l'énergie. En effet, chaque méthode a un nombre différent de paquets échangés et un nombre différent d'utilisation de la fonction de cryptage RC5 (Voir tableau 3.3, tableau 3.4 et tableau 3.5). La figure 3.8 illustre la consommation d'énergie de chaque méthode pour différentes tailles de réseau. Ainsi, les résultats sont compatibles avec la comparaison faite dans les tableaux ci-dessus. Il est évident que l'approche ELEC nécessite moins de consommation d'énergie par rapport à l'approche Comp_CH. De l'autre côté, l'approche Comp_CM nécessite moins d'énergie par rapport au Comp_CH. En effet, le nœud CM (ou le nœud CH) échange moins de paquets dans le processus de renouvellement de clés.

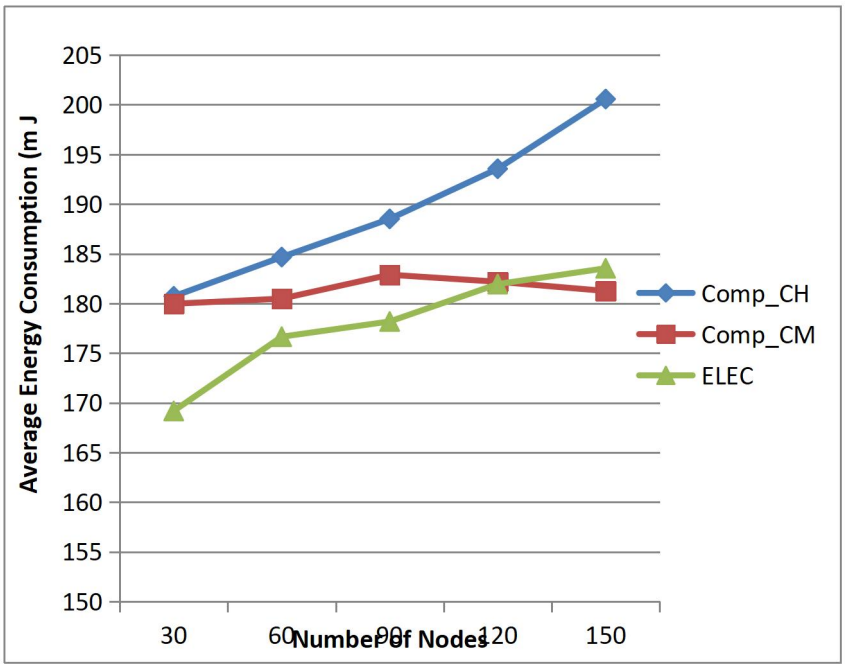

Figure 3.9 : La consommation d'énergie par un nœud capteur

3.6. Conclusion

Dans ce chapitre, nous avons présenté le processus d'implémentation ainsi que l'évaluation d'un mécanisme de renouvellement de clés destinée aux RCSFs 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 implémentée permet de produire des nouvelles clés d'une manière efficace et conforme à une consommation et conservation d'énergie.

Après des études expérimentales effectuées sur la consommation d'énergie et le coût de communication, nous avons constaté qu'une consommation d'énergie efficace pouvait être atteinte en utilisant un niveau de sécurité variable pour chaque scénario de renouvellement de clés.

Conclusion générale

Les RCSFs, malgré la diversité de leurs applications telles que dans les situations critiques et militaires, leurs succès dépend de leur propre sécurité. La vulnérabilité des nœuds de capteurs et celle du canal de communication face aux attaques malicieuses constitue un obstacle majeur freinant leur prolifération. De ce fait, la protection de ce type de réseau, en utilisant des solutions de sécurité adaptées aux capteurs, constitue un défi en suscitant un effort considérable contrairement aux mécanismes traditionnels utilisés dans les réseaux filaires.

En effet, les chercheurs travaillent sur cette problématique proposent des mécanismes de sécurité adaptés aux nœuds de capteurs. Cependant, nous avons pu voir que la gestion de clés constitue la pierre angulaire des autres mécanismes de sécurité, car il serait inutile d'intégrer des algorithmes cryptographiques dans un système de sécurité si la gestion de clés correspondante n'est pas satisfaisante.

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 protocole 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 et le renouvellement de ces clés, ce qui réduit les risques de compromission de la sécurité.

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

Nous avons évalué les performances de renouvellement de clés du protocole SKWN en fonction de coût de communication et de la consommation d'énergie. Pour de meilleurs résultats d'évaluation, les performances de protocole 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 et le coût de communication, nous avons constaté que le mécanisme de renouvellement répond bien aux critères de performances souhaités du réseau.

BLIOGRAPHIE

[1] (https://moodle.utc.fr/file.php/498/SupportWeb/co/Module_RCSF_35.html)

[2] Sadia INGRACHEN,Sarah OUBABAS, « Elaboration d'un protocole de routage efficace en énergie pour les réseaux de capteurs sans fil »,UNIVERSITE MOULOUD MAMMERI DE TIZI OUZOU,2013

[3] http://www-igm.univ-mlv.fr/~dr/XPOSE2006/AurelieBunel/Presentation.html

[4] Lynda TLILI, «MODELE DE CONFIANCE POUR SECURISER LE ROUTAGE DANS LES RESEAUX DE CAPTEURS SANS -FIL»,UNIVERSITÉ MOULOUD MAMMERI DE TIZI-OUZOU

[5] https://www.rapport-gratuit.com/topologies-des-reseaux-de-capteurs-sans-fils/

[6] FERRAT HANANE,CHERDIOUI SABRINA,« LE ROUTAGE DANS LES RESEAUX DE CAPTEURS SANS FILS»,UNIVERSITE MOULOUD MAMMERI DE TIZI OUZOU

[7] Salheddine Kabou, «état de l'art sur les réseaux de capteurs sans fil»,Université de Bechar,2010

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

[9] Rahim KACIMI,«Techniques de conservation d'´energie pour les r´eseaux de capteurs sans fil»,l'Institut National Polytechnique de Toulouse ,2009

[10] G. Terrasson, R. Brianda, S. Basrourb and O. Arrijuriaa. Energy Model for the Design of Ultra-Low Power Nodes forWireless Sensor Networks. Procedia Chem. 2009, 1, 1195-1198.

[11] V. Dupe, G. Terrasson, I. Estevez and R. Briand. Autonomy constraint in microsensor design: From decision making to energy optimization. In Proceedings of the IEEEInternational Conference on Green Computing and Communications, Besancon, France,20-23 November 2012 ; pp. 647-650.

[12] G. Terrasson, A. Liaria and R. Briand. System Level Dimensioning of Low Power Biomedical Body Sensor Networks. In Proceedings of the Faible Tension Faible ConsommationConference (FTFC), Monaco, France, 4-6 May 2014.

[13] G. Terrasson, R. Briand, S. Basrourb and V. Dupea. A Top-Down Approach for the Design of Low-Power Microsensor Nodes for Wireless Sensor Network. In Proceedings of the 2009 Forum on Speci_cation, Design Languages (FDL), Sophia Antipolis, France,22-24 September 2009.

[14] M.M. DIOURI, *Réseaux de capteurs sans-fil: routage et sécurité*, mémoire, INSA de Lyon, 2009/2010.

[15] Alessandra Flammini, Paolo Ferrari, Daniele Marioli, Emiliano Sisinni, Andrea Taroni ,"*Wired and wireless sensor networks for industrial applications*", Microelectronics Journal 40 (2009) 1322–1336.

[24] A. S. Uluagac, C. P. Lee, R. A. Beyah, et J. A. Copeland, « Designing Secure Protocols for Wireless Sensor Networks », in *Wireless Algorithms, Systems, and Applications*, vol. 5258, Y. Li, D. T. Huynh, S. K. Das, et D.-Z. Du, Éd. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, p. 503- 514.

[25] Athmani samir,« Protocoles pour la Sécurité des Réseaux de Capteurs Sans Fil »,2018

[26] TWAGIRAYEZU Jean Bosco,«Proposition d'un nouveau protocole de routage avec agrégation des données pour contrôler la congestion dans un réseau de capteurs sans fil», UNIVERSITE MOULOUD MAMMERI DE TIZI OUZOU,2011

[27] Messai Mohamed Lamine, « securité dans les reseaux de capeurs sans fil», Université Abderrahmane Mira de Bejaia ,2008

[28] KHALILI Zeyneb,BOUCHRAM,«Une technique d'optimisation de la consommation d'énergie dans les réseaux de capteurs sans fil»,Université Ahmed Draia - Adrar,2019

[29] A. Boukerche, Éd., *Algorithms and protocols for wireless sensor networks*. Hoboken, N.J: Wiley, 2009.

[30] Ben Zerrouk Amel ,Yaici Sara,«Gestion de clés dans les Réseaux de Capteurs Sans Fil »,Université Abderrahmane Mira de Béjaïa,2016

[31] W. Wang, S. Zhang, G. Duan, et H. Song, « Security in Wireless Sensor Networks », in *Wireless Network Security*, Higher Education Press, Beijing and Springer-Verlag Berlin Heidelberg, 2013, p. 129- 177.

[32] A. R. Dhakne et P. N. Chatur, « Detailed Survey on Attacks in Wireless Sensor Network », in *Proceedings of the International Conference on Data Engineering and Communication Technology*, vol. 469, S. C. Satapathy, V. Bhateja, et A. Joshi, Éd. Singapore: Springer Singapore, 2017, p. 319- 331.

[33] Mohamed BENAZZOUZ, « Surveillance de tout point d'une zone d'intérêt à l'aide d'un réseau de capteur multimédia sans fil »,Ecole nationale supérieure d'informatique Oued- Smar Alger Algérie - magistère IRM 2013

[34] D. G. Padmavathi et M. D. Shanmugapriya, « A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks », vol. 4, no 1, p. 9, 2009.

[35] J. P. Walters, Z. Liang, W. Shi, et V. Chaudhary, « Wireless Sensor Network Security: A Survey », in *Security in Distributed, Grid, and Pervasive Computing*, 2006 Auerbach Publications, CRC Press, p. 50.

[36] Y Challal, « Réseaux de Capteurs Sans Fils », Cours, Systèmes Intelligents pour le Transport, Université de Technologie de Compiègne, France, 17 Novembre 2008.

[37] M. Shaon, K. Ferens, «Wireless Sensor Network Wormhole Detection using an Artificial Neural Network »,2015

[38] MESMOUDI Samira,«Vers une nouvelle approche intelligente pour la gestion de clés dans les réseaux de capteurs sans fils »,2019

[39] M. Panda, « Security in Wireless Sensor Networks using Cryptographic Techniques », *Am. J. Eng. Res.*, p. 7, 2014.

[40] J. Ibriq, I. Mahgoub, et M. Ilyas, « Secure Routing in Wireless Sensor Networks », in *Handbook of Information and Communication Security*, P. Stavroulakis et M. Stamp, Éd. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, p. 553- 78.

[41] Doumi Abdelmoumain,«La Sécurité des Communications dans les Réseaux de Capteurs sans Fils»,

[42] RAMDANI MOHAMED,«PROBLÈMES DE SÉCURITÉ DANS LES RÉSEAUX DE CAPTEURS AVEC PRISE EN CHARGE DE L'ÉNERGIE», UNIVERSITÉ DE SAAD DAHLAB DE BLIDA ,2013

[43]A. Abduvaliyev, A.-S. K. Pathan, J. Zhou, R. Roman, et W.-C. Wong, « On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks », *IEEE Commun. Surv. Tutor.*, vol. 15, no 3, p. 1223- 1237, 2013.

[44]A. A. Strikos, « A full approach for Intrusion Detection in Wireless Sensor Networks », School of Information and Communication Technology Stockholm, Sweden 16453, 2007.

[45] Eichenauer et V. lustre. Schéma de gestion des clés réseau capteur distribué. Actes de la 9ème conférence ACM sur la sécurité Informatique et communications, ACM, PP. 41-47, novembre 2002.

[46] t. Blom. Distribution de clé non publique. Les progrès de la cryptographie, Springer,PP. 231-236, 1983.Protocil

[47] H. Chan, A. Bereg et D. Song. Schémas de randomisation pour interrupteurs pour réseaux de capteurs. Dans un séminaire sur la sécurité et la confidentialité. dans les actes,IEEE, PP. 197-213, 11-14 mai 2003.

[48] BELKIS Dihia ,FERDJI Lydia «Proposition d'un protocole de routage hiérarchique Sécurisé pour les réseaux de capteurs sans fil »,UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU,2016

[49] https://www.scribd.com/document/202541784/Cygwin#

[50] DJAMA Lynda.Mebarki Soraya, «Protocole de gestion de clés dans les réseaux de capteurs sans fil»,UniversitéA/ Mira de Béjaïa,2016

[51] WASSILA HOCEINI , «Un nouveau système de confiance pour les Réseaux de Capteurs sans fils»,l'université MOULOUD MAMMERI de TIZI-OUZOU

[52] J. Sen, « A survey on wireless sensor network security », *Int. J. Commun. Netw. Inf. Secur.*, vol. 1, no 2, p. 55- 78, août 2009.

[53] W. Znaidi, « Modélisation formelle de réseaux de capteurs à partir de TinyOS », Projet de fin d'études, Ecole Polytechnique de Tunisie, 2006.

[54] Y Challal, « Réseaux de Capteurs Sans Fils », Cours, Systèmes Intelligents pour le Transport, Université de Technologie de Compiègne, France, 17 Novembre 2008.

[55] D.Baker, H.X.Mel, *La Cryptographie Décryptée*, Campus Press edition, Référence Collection, pp. 414, Juillet 2001.

[56] Ali OUBAZIZ, « Prise en charge d'un grand nombre de capteurs sans fil dans 6LoWPAN»,UNIVERSITÉ MOULOUD MAMMERI DE TIZI-OUZOU

[57]Jamil Ibriq, Imad Mahgoub, « *Cluster-based Routing in Wireless Sensor Networks: issues and challenges* », Departement of computer science and engineering, Florida Atlantic University, 2004.

[60] S. Zhu, S. Setia, and S. Jajodia. "LEAP: Efficient security mechanisms for large-scale distributed sensor networks". In ACM CCS, pp. 62–72, October 2003.

[61] B. Lai, S. Kim, and I. Verbauwhede. "Scalable session key construction protocol for wireless sensor networks". In IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES), 2002.

[62] M. Eltoweissy, M. Moharrum, et R. Mukkamala, « Dynamic key management in sensor networks », *IEEE Commun. Mag.*, vol. 44, no 4, p. 122- 130, avr. 2006.

[63] J. Zhang et V. Varadharajan, « Wireless sensor network key management survey and taxonomy », *J. Netw. Comput. Appl.*, vol. 33, no 2, p. 63- 75, mars 2010.

[64] M. Abdalla and M. Bellare, "Increasing the Lifetime of a Key: A Comparative Analysis of the Security of re-Keying Techniques", In Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security:Advances in Cryptology (ASIACRYPT '00), pp. 546-559, December 2000.

[65] https://fr.m.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique?fbclid=Iw

[66] IDRISS MAKHLOUF, « Gestion de clés basée identité pour les réseaux AD hoc»,UNIVERSITÉ LARBI BEN M'HIDI -OUM EL BOUAGHI,2019

[67] SEBBAH ABDERREZAK,CHERRAK SOUFIANE,« GESTION DE CLES DANS LES RESEAUX DE CAPTEURS CORPORELS SANS FIL (WBAN)»,Université Abou Bakr Belkaid– Tlemcen,2016

[68] HAMOUID Khaled,«sécurité dans les Réseaux Ad Hoc»,Université Abderahmane Mira de Béjaia ,2006

Résumé

Les applications militaires de traçage, la surveillance des habitats, la surveillance et l'agriculture de précision ne sont que quelques exemples d'une vaste gamme d'applications possibles de la surveillance continue offerte par les RCSF. Malheureusement, les RCSF ne sont pas parfaits ! En raison de leurs ressources limitées et de leur déploiement dans des zones parfois hostiles, ces réseaux sont vulnérables à différents types d'attaques. Par conséquent, la sécurisation des communications représente l'un des défis les plus importants pour les réseaux de capteurs sans fil. Cette sécurité est généralement assurée par le chiffrement des données transmises. En effet, il serait inutile d'intégrer des algorithmes cryptographiques dans un système si la gestion des clés correspondantes n'est pas satisfaisante.

Dans le cadre de ce projet de fin d'études et après avoir examiné plusieurs protocoles et solutions de gestion de clés proposés pour les RCSF, nous avons choisi d'implémenter et de vérifier les métriques de performance du protocole SKWN pour le renouvellement des clés. Les résultats présentés dans ce mémoire sont issus de plusieurs simulations, qui démontrent que le renouvellement des clés du SKWN répond bien aux critères de performance souhaités par les réseaux RCSF, tout en réduisant les risques de compromission de la sécurité.

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

Abstract:

Military tracking applications, habitat monitoring, surveillance, and precision agriculture are just a few examples of the wide and varied range of possible applications of continuous monitoring offered by RCSFs (Wireless Sensor Networks). Unfortunately, RCSFs are not perfect! Due to their limited resources and deployment in sometimes hostile areas, these networks are vulnerable to different types of attacks. Therefore, the need to secure communications represents one of the most important challenges in wireless sensor networks. This security is generally ensured by encrypting the transmitted data. Indeed, it would be pointless to integrate cryptographic algorithms into a system if the corresponding key management is not satisfactory.

As part of this end-of-studies project, after discussing some key management protocols and solutions proposed for RCSFs, we have chosen to implement and verify the performance metrics of the key renewal protocol, SKWN. The results presented in this thesis are derived from several simulations, which demonstrate that the key renewal of SKWN meets the desired performance criteria for RCSF networks, while reducing the risk of compromising security.

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

ملخص

التطبيقات العسكرية للتعقب ومراقبة الموائل والمراقبة والزراعة الدقيقة هي مجرد أمثلة قليلة لمجموعة واسعة من التطبيقات الممكنة للمراقبة المستمرة التي تقدمها شبكة RCSF لسوء الحظ، RCSF ليست مثالية! نظرًا لمواردها المحدودة وانتشارها في مناطق معادية في بعض الأحيان، لدلك هذه الشبكات عرضة لأنواع مختلفة من الهجمات. لذلك ، يمثل تأمين الاتصالات أحد أهم التحديات التي تواجه شبكات الاستشعار اللاسلكية. يتم ضمان هذا الأمان بشكل عام عن طريق تشفير البيانات المرسلة. في الواقع ، سيكون من غير المجدي دمج خوارزميات التشفير في نظام إذا كانت إدارة المفاتيح المقابلة غير مرضية.

كجزء من مشروع نهاية الدراسات هذا وبعد مراجعة العديد من بروتوكولات وحلول الإدارة الرئيسية المقترحة لـ RCSF ، اخترنا تنفيذ والتحقق من مقاييس الأداء لبروتوكول SKWN لتجديد المفتاح. تأتي النتائج المقدمة في هذه الأطروحة من عدة عمليات محاكاة، والتي توضح أن تجديد المفاتيح SKWN يفي بمعايير الأداء التي تريدها شبكات RCSF ، مع تقليل مخاطر اختراق الأمان

الكلمات المفتاحية: شبكات الاستشعار اللاسلكية ، الأمن ، إدارة المفاتيح ، التشفير، تجديد المفتاح