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 : NOUACER Hadjira & RAISSI Souhila

DOMAINE : Technologie

FILIERE : Télécommunications

OPTION : Système des télécommunications

Thème

Implémentation et évaluation d'un protocole de gestion de clé dédié aux réseaux capteurs sans fils (RCSF)

Jury de soutenance :

Nom et Prénom	Grade	Qualité
MESMOUDI Samira	MCB	Encadreur
ROUGAB Mourad	MAA	Président
REGUIGUE Mourad	MCB	Examinateur

Promotion : 2020/2021

Remerciement

Si la destination est importante, le parcours ne l'est pas moins. Ces cinq années d'études, nous ont permis de bien comprendre la signification de cette phrase. En effet, le trajet parcouru ne s'est pas réalisé sans défis et sans labeur.

Avant tout, nous remercions Dieu le tout puissant d'avoir été à nos côtés, et de nous avoir donné la force et la patience pour accomplir ce travail.

Au terme de ce travail, nous tenons à remercier, très particulièrement Mme Mesmoudi samira d'avoir accepté la lourde tâche d'être la directrice de ce mémoire. Patiente, compréhensive et toujours disponible pour nous aider. Ses conseils et interventions nous ont été d'une grande importance.

Nos remerciements vont aussi aux membres du jury pour l'honneur d'avoir voulu examiner et évaluer ce mémoire

Dédicace

Je dédie ce travail :

A ma chère mère,

A mon cher père,

Qui n'ont jamais cessé, de formuler des prières à mon égard, de me soutenir et de m'épauler pour que je puisse atteindre mes objectifs.

A mon petit frère

A mes sœurs

Pour ses soutiens moral et leurs conseils précieux tout au long de mes études.

A mon cher grand -mére,

Qui je souhaite une bonne santé.

A ma chère binôme, HADJIRA NOUACER

Pour sa entente et sa sympathie.

A mon cher, SADDAM

Qui m'a aidé et supporté dans les moments difficiles.

Dédicace

Je remercie Allah de m'avoir donné la santé et la volonté ainsi que la conscience d'accomplir mes études pour l'obtention de diplôme. Je dédie ce modeste travail et ma profonde gratitude:

A mon défunt très ma mère compatissante qui m'a tellement soutenue durant ma vie et ses sacrifices elle est l'espoir de mon existence. A mes chères sœurs et mes chers frères et leurs enfants joviaux. Toutes les familles :

Qui je souhaite une bonne santé.

A ma chère binôme, raissi souhila

Résumé :

Les réseaux de capteurs sans fil (RCSFs) ont attiré un grand intérêt dans la dernière décennie. Ils représentent une technologie émergente qui vise à offrir des capacités innovantes. Leurs utilisations ne cessent pas d'augmenter et ceci dans de nombreux domaines qu'ils soient scientifiques, logistiques, militaires ou encore sanitaires. Cependant, les contraintes liées aux ressources (énergie, mémoire et traitement) et l'environnement hostile dans lequel ils peuvent être déployés, rendent ce type de capteurs vulnérables aux attaques. De ce fait, le besoin de sécuriser les communications représente l'un des défis les plus importants dans les réseaux de capteurs sans fil. Cette sécurité est généralement assurée par le cryptage des données transmises, ce qui nécessite l'établissement de nombreuses clés cryptographiques. La gestion de clés est la première fonction fondamentale puisque les nœuds ont besoin d'une clé commune valide pour exploiter les mécanismes de cryptographie. Dans le cadre de ce mémoire et après avoir abordé quelques protocoles et solutions de gestion de clés proposés pour les RCSFs, nous avons choisi l'une des approches liées au travail de Q. Mamun et autres [1] pour l'implémenter et vérifier leurs métriques de performances. L'approche implémentée est appelée SC-SPK **(S**ecured **C**ommunication **K**ey **E**stablishment for Cluster based Wireless Sensor Networks - *Shared Partial Keys*). Cette dernière surpasse les protocoles de pré-distribution de clés aléatoires dans le sens où elle optimise le coût de communication et l'espace de stockage. Ainsi que deux nœuds communicants utilisent toujours une nouvelle clé secrète pour le cryptage/décryptage des données à chaque cycle. Les résultats présentés dans ce mémoire sont issus de plusieurs simulations, qui démontrent que le protocole SC-SPK répond bien aux critères de performances souhaités par les réseaux RCSFs, tout en maintenant un niveau de sécurité très élevé.

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

Abstract:

Wireless Sensor Networks (WSN) have attracted great interest in the past decade. They represent an emerging technology that aims to offer innovative capabilities. Their uses continue to increase and this in many fields: scientific, logistical, military or even health. However, resource constraints (energy, memory and processing) and the hostile environment in which they can be deployed, make this type of sensor vulnerable to attack. Therefore, the need to secure communications is one of the most important challenges in wireless sensor networks. This security is generally provided by encryption of the transmitted data, which requires the establishment of many cryptographic keys. Key management is the first fundamental function since the nodes need a valid common key to exploit the cryptographic mechanisms. Within the framework of this work and after having reviewed some protocols and key management solutions proposed for WSNs, we chose the approach proposed by Q. Mamun and others [1] to implement it and verify their performance metrics. The implemented approach is called SC-SPK (Secured Communication Key Establishment for Cluster based Wireless Sensor Networks - Shared Partial Keys). This approach outperforms random key pre-distribution protocols by optimizing communication cost and storage space. As well as two communicating nodes always use a new secret key for the encryption / decryption of the data at each cycle. The results presented in this work come from several simulations, which demonstrate that the SC-SPK protocol responds well to the performance criteria desired by WSNs, while maintaining a very high level of security.

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

ملخص:

جذبت شبكات الاستشعار اللاسلكية (RCSFs) اهتمامًا كبيرًا في العقد الماضي. لإنها تمثل تقنية ناشئة تهدف إلى تقديم قدرات مبتكرة. و لازالت استخداماتها في تزايد ، وهذا في العديد من المجالات سواء كانت علمية أو لوجستية أو عسكرية أو حتى صحية. ومع ذلك، فإن قيود الموارد (الطاقة، الذاكرة والمعالجة) والبيئة المعادية التي يمكن نشرها فيها، تجعل هذا النوع من أجهزة الاستشعار عرضة للهجوم. لذلك ، تعد الحاجة إلى تأمين الاتصالات من أهم التحديات في شبكات الاستشعار اللاسلكية. يتم توفير هذا الأمان بشكل عام عن طريق تشفير البيانات المرسلة ، الأمر الذي يتطلب إنشاء العديد من مفاتيح التشفير. إدارة المفاتيح هي الوظيفة الأساسية الأولى لأن العقد تحتاج إلى مفتاح مشترك صالح لاستغلال آليات التشفير. في إطار هذه الأطروحة وبعد الاقتراب من بعض البروتوكولات وحلول الإدارة الرئيسية المقترحة لمرافقRCSF، اخترنا أحد الأساليب المتعلقة بعمل Q. Mamun وآخرون [1] لتنفيذه والتحقق من مقاييس أدائهم. يُطلق على النهج الذي تم تنفيذه اسم SC-SPK (الإتصال الآمن لإنشاء المفاتيح لشبكات الاستشعار اللاسلكية - المفاتيح الجزئية المشتركة). يتفوق الأخير على بروتوكولات التوزيع المسبق للمفاتيح العشوائية من حيث أنه يحسن تكلفة الاتصال ومساحة التخزين، بالإضافة إلى أن عقدتين متصلتين تستخدمان دائمًا مفتاحًا سريًا جديدًا لتشفير / فك تشفير البيانات في كل دورة. تأتي النتائج المقدمة في هذه الأطروحة من عدة عمليات محاكاة، والتي توضح أن بروتوكول SC-SPK يستجيب جيدًا لمعايير الأداء التي تريدها شبكات RCSF، مع الحفاظ على مستوى عالٍ جدًا من الأمان.

الكلمات الرئيسية :شبكة الاستشعار اللاسلكية، الأمن، إدارة المفاتيح ،التشفيرة

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

ACK: Acknowledge

CCA: Clear Channel Assessment

CAN : convertisseur analogique-numérique

CODA: Congestion Détection and Avoidance

CTS Clear To Send

EBS : le système de base d'exclusion

GPS : Global Position System

MAC: Media Access control

PDU: Protocol Data Unit

PPP : le protocole point point

RCSF : Réseaux de capteur sans fil

RTS: Request To Sen

SMP: Sensor Management Protocol

SQDDP: Sensor Query and Data Dissemination Protocol

SC-SPK: **S**ecured **C**ommunication Key Establishment for Cluster based Wireless Sensor Networks -P*rivate* P*artial* K*eys*

TADAP: Task Assignment and Data Advertisement Protocol

TCP: Transmission control Protocol

UDP: User Datagramme Protocol

Introduction générale

Les récentes avancées dans les domaines des technologies de communication sans-fil et microélectroniques ont permis le développement de minuscules capteurs (de quelque millimètre cube de volume) capable de répondre à un ou plusieurs stimuli engendré par un changement dans un état physique ou chimique, comme la chaleur, la lumière, la pression ou la vibration et génère un signal qui peut être mesuré. Cette technologie rend possible ces nœuds de s'organisent en réseaux de mesure, appelés réseaux de capteurs sans fil (RCSFs) ou Wireless Sensor Networks (WSN) en anglais.

Les réseaux de capteurs ont de nombreuses perspectives d'applications dans des domaines très variés : applications militaires, domotique, surveillance industrielle ou de phénomènes naturels. Le rôle critique, la variété d'applications et la popularité des RCSFs ont apporté une grande importance à ce type de réseaux. Cette importance émergente des réseaux de capteurs pourrait être entravée par leurs problèmes de sécurité inhérents. La nécessité d'intégrer des services de sécurité devient l'une des principales préoccupations pour la pérennité du succès des RCSFs dans un certain nombre de domaines. En effet, les RCSFs sont généralement déployés dans des zones inconnues sans aucune protection physique, ce qui facilite leur capture et compromission. 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. Il est nécessaire donc d'intégrer un mécanisme de sécurité qui non seulement gère les intrusions, mais garantit également un échange de données sécurisé. Cependant, assurer la sécurité des échanges des données au sein des RCSFs est une tâche importante et en même temps difficile. En effet, Les nœuds capteurs sont limités en termes de calcul, de mémoire et des capacités énergétiques, ces contraintes influencent négativement le bon fonctionnement des techniques spéciales qui fournissent la sécurité requise.

Les mécanismes de sécurité sont construits autour des algorithmes de cryptage et d'authentification puissants. Pour atteindre les objectifs de sécurité, la gestion de clés est la première fonction fondamentale puisque les nœuds capteurs ont besoin d'une clé commune valide pour exploiter les primitives cryptographiques.

Généralement, la gestion de clés définit par le procédé de pré-distribution de clés qui exige un chargement d'information secrète dans les nœuds avant leur déploiement dans le réseau, permet aussi d'assigner des nouvelles clés aux nœuds joignant le réseau, retirer les clés quand les nœuds quittent le réseau et renouvellement des clés expirées.

Dans le cadre de notre étude et après avoir abordé certains protocoles et solutions de gestion de clés proposés pour les RCSFs, nous nous sommes intéressés par le travail [1] intitulé "Secured Communication Key Establishment for Cluster based Wireless Sensor Networks ". Dans ce travail les auteurs ont développé deux approches différentes pour la gestion de clés. Nous avons choisi l'une de ces approches pour l'implémenter et vérifier leurs métriques de performances telles que le coût de stockage, le coût de communication, et la consommation d'énergie.

Organisation de mémoire

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

- Le premier chapitre présente un survol biographique sur les réseaux de capteurs sans fil.
- 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 méthode 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 I
Généralités sur les réseaux de capteurs sans fil

1.1. Introduction

Les Réseaux de Capteurs Sans Fil (RCSF) se composent généralement d'un grand nombre de petits dispositifs, qui communiquent entre eux via des liens radio de faible portée pour le partage d'information et le traitement coopératif. Ces dispositifs appelés nœuds capteurs, les nœuds sont généralement matériellement petits, construits à partir des composants pas chers. Ce type de réseau est composé de centaines ou de milliers d'éléments (capteurs), a pour but la collecte de données de l'environnement, leur traitement et leur transmission vers le monde extérieur. L'affranchissement de la communication par ondes radio a permis à ces réseaux d'être présents dans plusieurs domaines tels que : le secteur industriel mais aussi pour les organisations civiles où la surveillance et la reconnaissance de phénomènes physiques est une priorité. En effet, un réseau de capteurs peut être mis en place dans le but de surveiller une zone géographique plus ou moins étendue pour détecter un évènement. Dans ce chapitre, nous nous attachons à décrire les bases nécessaires à la compréhension des réseaux de capteurs sans fil. L'architecture, les applications, les caractéristiques ce type de réseaux sont les points abordés.

1.2. Le Nœud capteur

Depuis un peu plus de 15 ans, la technologie des capteurs sans fil à beaucoup évolué (voir figure 1.1). Un capteur sans fil est un petit dispositif électronique capable d'interagir avec l'environnement où il est déployé, de mesurer une valeur physique (température, lumière, pression, etc.), et de la communiquer à un centre de contrôle via une station de base. Généralement, Un nœud est constitué d'unités essentielles et d'unités supplémentaires.

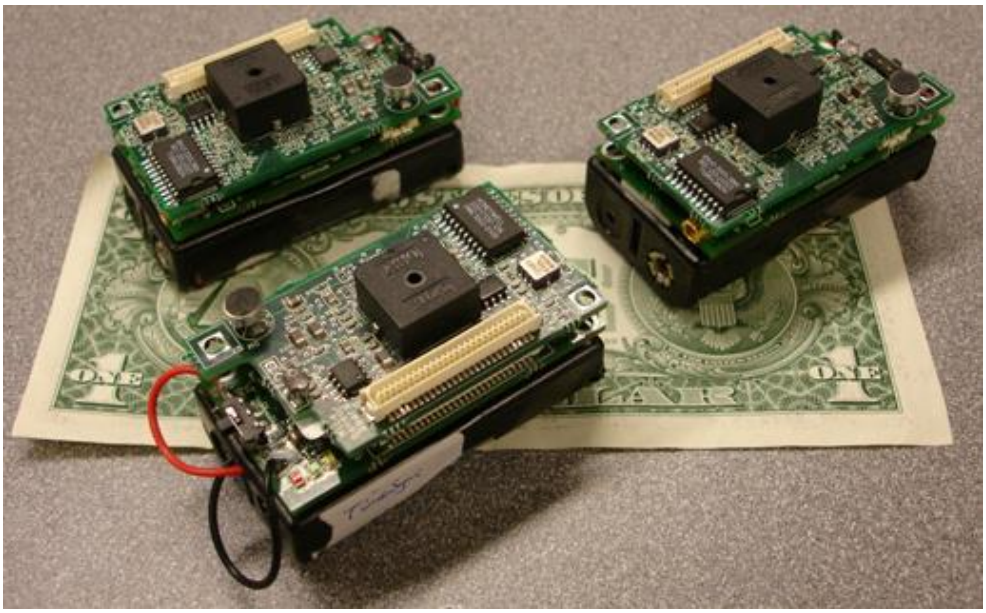

Figure 1 -1 capteur sans fil [2]

1.2.1. Composants matériels d'un nœud capteur sans fil

Le nœud de capteur est composé principalement de quatre unités : l'unité d'acquisition, l'unité de traitement, l'unité de communication et une source d'énergie (voir figure 1.2).

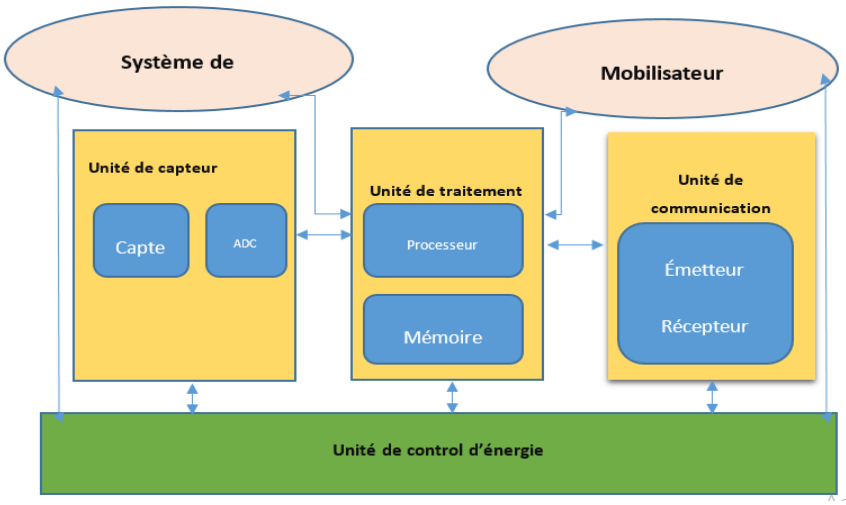

Figure 1 -2 les composants de base d'un nœud capteur sans fil [3]

1.2.1.1. Unité d'acquisition

Elle se compose de deux sous unités, unité de captage et un convertisseur analogique-numérique (CAN) [4].

- Les capteurs obtiennent des mesures sur les paramètres environnementaux sous forme analogique
- CAN convertit ces données analogiques en données numériques compréhensibles par l'unité de traitement [5].

1.2.1.2. Unité de traitement

Cette unité est également composée d'un processeur qui supporte un système d'exploitation spécifique tel que Contiki et Tinyos [5]. Elle comprend de deux interfaces : une interface pour l'unité d'acquisition et une autre pour l'unité de transmission. [3]. Elle est chargée de gérer des procédures qui permettent à un noud capteur de collaborer avec les autres nœuds du réseau. Elle peut aussi analyser les données captées pour alléger la tâche du nœud puits [4].

1.2.1.3. Unité de communication

Cette unité est responsable de toutes les émissions et les réceptions de données via un support de communication sans fil et une antenne [5]. Ce dernier peut être de type optique (comme dans les capteurs Smart Dust) ou de type radio fréquence (MICA2) [3].

1.2.1.4. Unité d'énergie

Cette unité est responsable de la gestion de l'énergie et de l'alimentation de tous les composants du capteur, généralement une batterie ou des piles. Les batteries utilisées peuvent être rechargeables par l'énergie solaire. Notant que la transmission consomme beaucoup d'énergie par rapport à l'unité de calcul [3]. De plus, un nœud capteur peut être équipé par d'autres composants supplémentaires tels que :

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

1.3. Réseaux de Capteurs Sans Fil (RCSF)

1.3.1. Architecture des réseaux de capteurs sans fil

Un réseau de capteur sans fil est un type particulier de réseau Ad hoc Mobile. Il est composé d'un ensemble de dispositifs très petits, nommés nœuds capteurs, distribués sur une zone donnée afin de mesurer une grandeur physique ou surveiller un évènement et de réagir en cas de besoin en envoyant l'information collectée à un ou plusieurs points de collecte, à l'aide d'une connexion sans fil.

Dans un tel réseau, chaque nœud est un dispositif électronique qui possède une capacité de calcul, de stockage, de communication et d'énergie [4]. Selon les capteurs qui le composent sont capables de faire trois taches :

- Le prélèvement d'une grandeur physique,
- e traitement éventuel de cette information,
- La communication avec d'autres capteurs . . . etc [2].

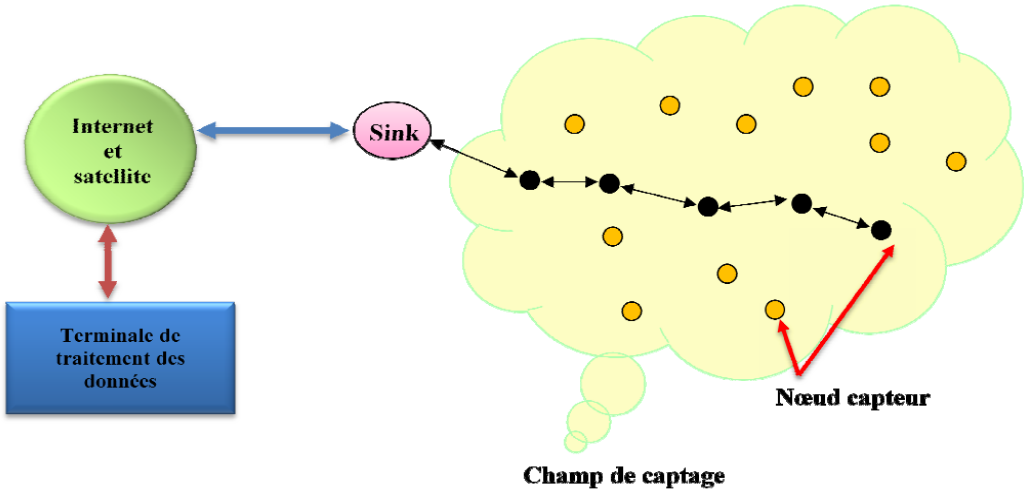

Figure 1-3 Architecture d'un Réseau de Capteur Sans Fil [4]

1.3.2. Model de Collecte d'informations

Il y a deux méthodes pour collecter les informations d'un réseau de capteurs :

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 diffusions (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 comme s'est illustré par la figure 1.4.

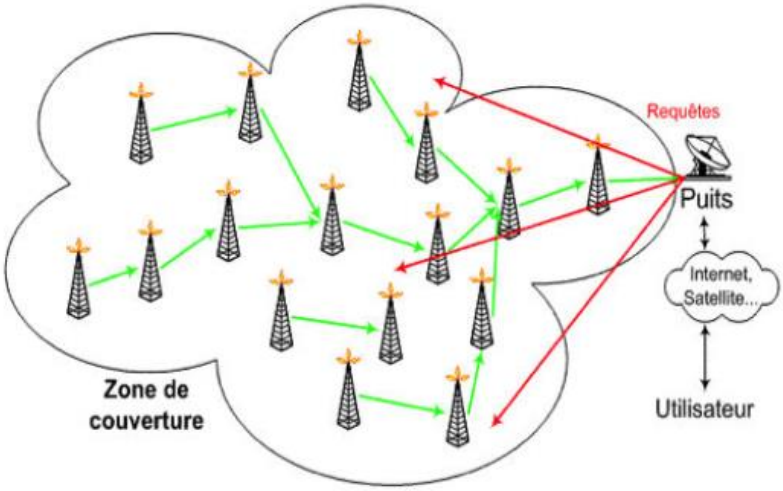

Figure 1-4 Collection des informations à la demande du puits [6]

1.3.2.2. Suite à un événement

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

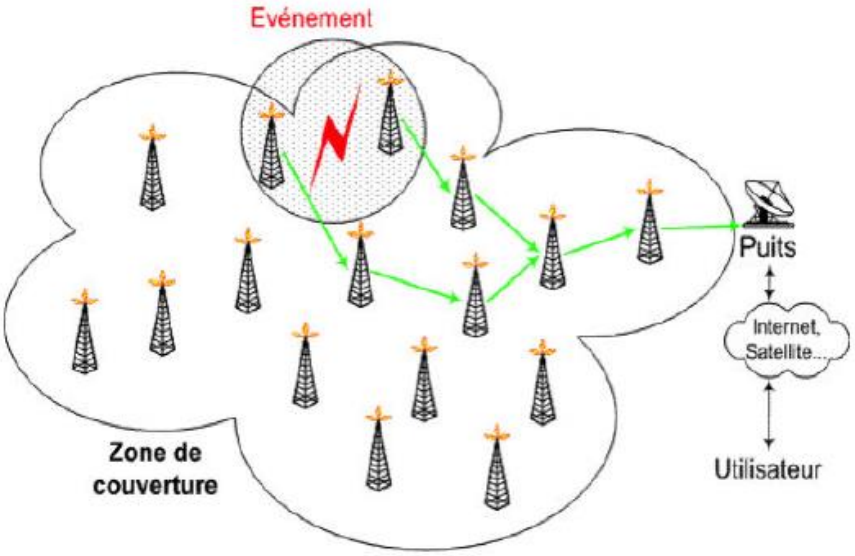

Figure 1-5 collection des informations suite à un événement [6]

1.3.3. Architecture protocolaire

L'architecture d'un nœud capteur peut être représentée par deux piles protocolaires : pile capteur et pile réseau. La première pile est liée au canal de capture et la seconde au canal sans fil de communication. La pile protocolaire utilisée par le nœud puits ainsi que tous les autres capteurs du réseau illustrée, prend en charge le problème de consommation d'énergie, intègre le traitement des données transmises dans les protocoles de routage, et facilite le travail coopératif entre les capteurs. Comme le montre la figure 1.6, la pile protocolaire est constituée de cinq couches : une couche d'application, une couche de transport, une couche réseau, une couche de liaison de données et une couche physique, et de trois plans de gestion : un plan de gestion d'énergie, un plan de gestion de mobilité et un plan de gestion de taches.

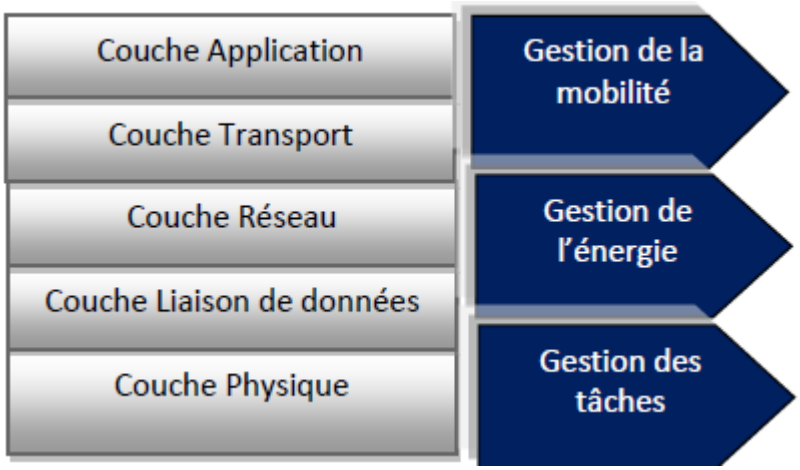

Figure 1-6 Modèle en couches pour la communication dans les RCSFs [7].

1.4.2.1 Couche application

Cette couche assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, gère directement par les logiciels. La couche d'application représente des données pour l'utilisateur ainsi que du codage et un contrôle du dialogue : des mécanismes de communication offerts aux applications de l'utilisateur [3]. Parmi les Trois protocoles d'application, nous citons : Sensor Management Protocol (SMP), Task Assignment and Data Advertisement Protocol (TADAP) et Sensor Query and Data Dissémination Protocol (SQDDP).

1.4.2.2. 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. Les deux principaux protocoles utilisés sont les protocoles TCP et UDP. En fonction des protocoles, le PDU est appelé « segment » (TCP), « datagramme » (UDP), ou encore « paquet » [3].Le développement d'un protocole pour la couche transport doit être générique et indépendant de l'application. Il doit offrir une fiabilité variable des paquets pour différentes applications [7]

1.4.2.3. Couche réseau

Cette couche permet de gérer l'adressage et le routage des données, le routage détermination d'un chemin permettant de relier les deux machines distantes; le relayage retransmission d'un PDU (Protocol Data Unit ou Unité de données de protocole) dont la destination n'est pas locale pour le rapprocher de sa destination finale. Ces protocoles doivent aisément gérer les

communications entre plusieurs nœuds capteurs et faire aboutir les données captées vers le Sink. En plus, ces protocoles doivent prendre en considération les contraintes de ressources telles que l'énergie, la bande passante, la mémoire et les capacités de calcul.

1.4.2.4. La couche de liaison de données

Dans le domaine des réseaux informatiques, la couche de liaison de données est la seconde couche des sept couches du modèle OSI, Elle 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 sur le media, les moyens de détecter et potentiellement corriger les erreurs qui peuvent survenir au niveau de la couche physique. Ethernet pour les réseaux locaux (multi-nœuds), le protocole point point (PPP), HDLC et ADCCP pour des connexions point à points (double nœud) sont des exemples de protocoles de liaison de données. Les codes de contrôle d'erreurs simples avec un codage et décodage de moindre complexité pourraient présenter les meilleures solutions pour les RCSF. Dans la conception d'un tel protocole, il est important d'avoir de bonnes connaissances des caractéristiques du canal et des techniques d'implémentation [7].

1.4.2.5. Couche physique

Cette couche doit assurer des techniques d'émission, de réception et de modulation de données d'une manière robuste. Les fonctions principales de cette couche incluent la détection du signal (CCA : Clear Channel Assessment), la synchronisation des trames de données et le chiffrement. Les plateformes radio comme le standard IEEE 802.15.4 pour les RCSF offrent de nouvelles fonctionnalités à la couche physique telle que le chiffrement et les messages d'auto-acquittement.

1.4. Topologies d'un RCSF

De façon générale, les architectures des réseaux de capteurs se présentent sous forme de deux topologies :

1.4.1. Topologie hiérarchique (à base de cluster)

L'architecture hiérarchique est composée de plusieurs couches : une couche de capteurs, une couche de transmission et une couche de point d'accès [8].

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 1.7) [7].

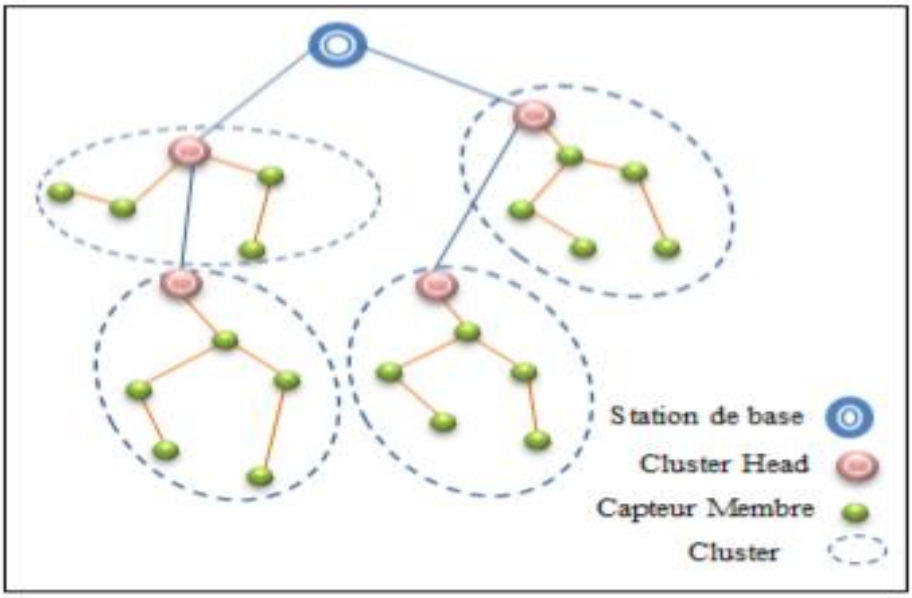

Figure 1-7 Topologie hiérarchique [8]

1.4.2. La topologie plate

Dans la topologie plate, à l'exception du nœud puits qui joue le rôle d'une passerelle et qui est responsable de la transmission de l'information collectée à l'utilisateur final [8]. Selon le service et le type de capteurs, une densité de capteurs élevée (plusieurs nœuds capteurs/m2) ainsi qu'une communication multi-sauts peut être nécessaire pour l'architecture plate. Tous les autres nœuds sont identiques, ils ont la même capacité en termes d'énergie et du calcul (Voir figure 1.8).

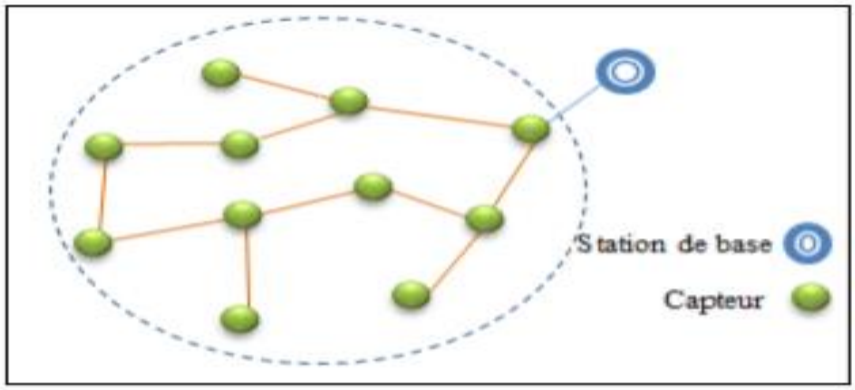

Figure 1-8 La topologie plate [8]

1.5. Les principales caractéristiques des RCSFs

Les réseaux de capteurs sans fil présentent de nombreuses caractéristiques, parmi ces dernières, nous citons [8] :

1.5.1. La consommation réduite d'énergie

L'économie d'énergie est une des problématiques majeures dans les réseaux de capteurs. En effet, la recharge des sources d'énergie est souvent trop coûteuse et parfois impossible. Il faut donc que les capteurs économisent au maximum l'énergie afin de pouvoir fonctionner. Le nœud capteur est limité en énergie. Dans la plupart des cas, le remplacement de la batterie est quasi impossible ce qui fait que la durée de vie du réseau dépende grandement de la durée de vie des batteries des nœuds capteurs. D'autre part, la nature de réseau peut parfois entraîner une dissipation supplémentaire de l'énergie. Ceci pourrait être le cas par exemple lors de dysfonctionnement de quelques nœuds capteurs, ce qui nécessite un changement de la topologie du réseau et un ré-routage des messages. Toutes ces opérations sont bien évidemment gourmandes en énergie. C'est pour cette raison que les recherches dans le domaine des RCSFs se concentrent principalement sur l'économie d'énergie [7].

1.5.2. L'auto-configuration des nœuds capteurs

Il y a deux manières de procéder pour transmettre des données d'un nœud source à un nœud destinataire (puit ou point de collecte).Pour assurer la détection d'un paramètre au niveau des capteurs, il faut intégrer une application qui s'exécute sur le système TinyOS pour effectuer la tâche voulue. Un nœud de capteur assure plusieurs taches telles que la détection de changement de température, le traitement et de génération et la transmission de données.

Alors un capteur doit avoir la capacité de s'auto-configurer dans un réseau de capteur mais également de pouvoir collaborer avec les autres nœuds du réseau. Chaque capteur du réseau possède un module possédant une antenne émettrice/réceptrice qui permet de communiquer avec les nœuds qui sont proches [9]

1.5.3. La scalabilité

La particularité du réseau de capteur sans fil est qu'il soit capable de prendre en compte et gérer un très grand nombre de nœuds qui coopère pour un même objectif. Contrairement aux réseaux sans fils traditionnels (personnel, local, étendu, E). De plus, La collaboration des nœuds est très importante dans les RCSFs. Par exemple, éviter le traitement et la transmission des données redondantes sur tout le réseau. Ce genre de traitement est nécessaire afin d'éviter une perte d'énergie et de temps importantes dans le cadre d'une optimisation de la consommation de l'énergie à travers tout le réseau.

1.5.4. La tolérance aux panaux

La tolérance aux pannes c'est la capacité de maintenir les fonctionnalités du réseau sans interruption en cas de défaillance d'un nœud capteur. Afin d'assurer la communication entre la station de base et les autres nœuds d'un réseau de capteur, la limitation d'énergie dans les RCSFs, et les environnements hostiles dans lesquels ils pourraient être déployés, sont des facteurs qui rendent ce type de réseaux très vulnérables [10].

1.5.6. La capacité de communication

Il y a deux manières pour transmettre les données. La première est d'utiliser une transmission de longue portéeavec un seul saut afin de transmettre des données vers le point de collecte. La deuxième est d'utiliser le multi-saut qui permet de transmettre les données à des nœuds voisins et ainsi de suite vers le point de collecte [11].

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

Le domaine d'applications des RCSF est très varié. La miniaturisation, l'adaptabilité, la taille de plus en plus réduite des micro-capteurs, leur coût de plus en plus faible, la large gamme des types de capteurs disponibles (thermique, optique, ect) [**5**] ainsi que le support de communication sans fil utilisé, permettent l'utilisation des réseaux de capteurs dans plusieurs domaines parmi lesquels, nous citons [**3**] :

Figure 1-9 Les domaines d'applications des réseaux de capteurs sans fil [12]

1.6.1. Applications militaires

Les premières applications potentielles des réseaux de capteurs ont concerné le domaine militaire [**4**]. Les RCSF permettent la détection des mouvements ennemis sur un champ de bataille ou bien de tracer leurs mouvements. Dans le domaine militaire, cette technologie peut impulser de nouvelles stratégies de communication ou encore servir à détecter des dispositifs nucléaires et les dépister. Actuellement, les RCSF peuvent être une partie intégrante dans le commandement, le contrôle, la communication, la surveillance, la reconnaissance, etc [**3**].

1.6.2. Applications liées à la sécurité

L'application des réseaux de capteurs dans le domaine de la sécurité pourrait diminuer considérablement les dépenses financières consacrées à la sécurisation des lieux et à la protection des êtres humains [1**3**]. L'intégration des capteurs dans de grandes structures telles que les ponts ou les bâtiments aidera à détecter les fissures et les altérations dans la structure suite à un séisme ou au vieillissement de la structure. Un réseau de capteurs de mouvements peut constituer un système d'alarme distribué qui servira à détecter les intrusions sur un large secteur [9].

1.6.3. Applications environnementales

Dans ce domaine, les capteurs peuvent être exploités pour détecter les catastrophes naturelles (feux de forêts, tremblements de terre, etc.), de même leur déploiement dans les sites industriels empêche les risque industriels tels que la fuite de produits toxiques (gaz, produits chimiques, éléments radioactifs, pétrole, ect). En outre, ce domaine d'application inclut les prévisions de la météo [**14**].

1.6.4. 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, ..). Ils peuvent aussi faciliter le diagnostic de quelques maladies en effectuant des mesures physiologiques telle que la tension artérielle, le rythme cardiaque, … [**5**]. 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, ...) chez les personnes dépendantes (handicapées ou âgées) [**4**].

1.6.5. Applications écologiques

L'intégration de plusieurs micro-capteurs dans le système de climatisation et de chauffage des immeubles. La climatisation ou le chauffage ne sont déclenches qu'aux endroits où il y a des personnes présentes et seulement si c'est nécessaire. Le système distribué peut aussi maintenir une température homogène dans les pièces [**9**].

1.6.6. Applications de traçabilité et de localisation

La traçabilité, la localisation et ciblage dans le RCSF sont généralement utilisés pour suivre un événement, une personne, un animal ou même un objet [**15**]. En équipant les personnes susceptibles de se trouver dans des zones à risque par des capteurs. Ainsi, les équipes de sauvetage peuvent localiser plus facilement les victimes. Contrairement aux solutions de traçabilité et de localisation basées sur le système de GPS (Global Positionning System), les réseaux de capteurs peuvent être très utiles dans des endroits clos comme les mines par exemple.

1.6.7. Applications commerciales

Des nœuds capteurs pourraient améliorer le processus de stockage et de livraison. Le réseau ainsi formé, pourra être utilisé pour connaître la position, l'état et la direction d'un paquet ou d'une cargaison [**4**]. Il devient alors possible pour un client qui attend la réception d'un paquet, d'avoir un avis de livraison en temps réel et de connaître la position actuelle du paquet. Pour les entreprises manufacturières, les réseaux de capteurs permettront de suivre le procédé de production à partir des matières premières jusqu'au produit final livré [9].

1.7. Les contraintes des réseaux de capteurs sans fil

La conception et la réalisation des réseaux de capteurs sans fil sont influencées par plusieurs facteurs [**16**] :

1.7.1. Limitation d'énergie et de ressources

Stocker de l'énergie dans une batterie du nœud, distribuer la puissance au nœud via un fil ou récolter l'énergie ambiante sont les principales méthodes pour fournir de l'énergie aux nœuds sans fil [**14**]. En plus de l'énergie, les nœuds capteurs ont aussi une capacité de traitement et de mémoire limitée. En effet, les industriels veulent mettre en œuvre des capteurs simples, petits et peu coûteux [**4**].

1.7.2. Topologies dynamiques et conditions environnementales difficiles

Le déploiement d'un grand nombre de nœuds nécessite une maintenance de la topologie [**5**]. Le changement de la topologie de réseau est l'un des aspects les plus importants dans les réseaux de capteurs sans fil, un environnement fortement caustique ou corrosif, niveau d'humidité élevé, vibrations, saleté et poussière, ou autres conditions qui remettent en question les performances. Ces dures conditions peuvent provoquer un dysfonctionnement pour une partie des nœuds de capteurs [**9**]. Ce changement topologique du réseau résulte à la défection d'un ou de plusieurs nœuds capteurs, la mobilité des nœuds capteurs, ainsi que l'ajout de nouveaux nœuds capteurs, ces raisons peut engendrer des difficultés de connectivité, on outre rend la topologie du réseau fréquemment instable. Dans ces cas il faut que les nœuds capteurs soient capables d'adapter leur fonctionnement dans le but de maintenir la topologie souhaitée [**8**].

1.7.3. Localisation

Dans bon nombre d'applications des réseaux de capteurs, les nœuds capteurs sont souvent déployés aléatoirement. La majorité de ces applications exigent la connaissance de la position physique des capteurs pour pouvoir localiser les évènements détectés. Sans connaitre leurs positions, ces applications n'auraient aucun sens. Pour ces raisons, la localisation des capteurs est un parmi les principaux problèmes dans ce type de réseaux et de nombreuses solutions ont été proposées pour le résoudre. Ces solutions sont soit imprécises, soit couteuses en énergie.

1.7.4. La sécurité

En fonction de l'application, la sécurité peut être critique. Les réseaux de capteurs sans-fils ont plus touché par le paramètre de sécurité que les réseaux filaires classiques RCSF sont très vulnérables aux attaques en raison de leur déploiement sans surveillance et les nœuds capteur ne sont pas protégés contre la mauvaise manipulation ou attaques. L'écoute, le brouillage, et les attaques de retransmission peuvent entraver ou empêcher l'opération et par conséquent, le contrôle d'accès, l'intégrité des messages, et la confidentialité doit être garanti [**17**]

1.8. Conclusion

Les réseaux de capteur sans fil sont des réseaux sans fil décentralisés basés sur la notion d'un grand nombre des nœuds. Dans ce chapitre, nous avons présenté en premier lieu quelques généralités sur les réseaux de capteur sans fil, à savoir quelques définitions de base sur les RCSF ainsi que leurs domaines d'applications, la description d'un RCSF, leurs spécificités et les concepts nécessaires à la compréhension des réseaux de capteurs, les différentes architectures d'un nœud capteur, la consommation d'énergie réduite, qui s'adapteront aux caractéristiques des RCSF.

Dans le chapitre suivant, nous allons aborder le problème de la sécurité en mentionnant quelques attaques dans les RCSF.

Chapitre II
Sécurité des communications dans les réseaux de Capteurs sans fil.

2.1. Introduction

Les réseaux de capteurs sans fil sont déployés sans infrastructure prédéfinie et laissés généralement sans surveillance. Les caractéristiques inhérentes des réseaux de capteurs sans fil les rendent particulièrement vulnérables aux attaques. Comme les données sont transmises par voie hertzienne, il est extrêmement facile pour un adversaire d'espionner le trafic. Dans ce contexte, une grande communauté de chercheurs tente de proposer des mécanismes afin de renforcer la sécurité des données communiquées pour diminuer le risque d'interception et d'altération. Généralement, afin de protéger les communications et de permettre une consommation d'énergie minime tout en assurant une sécurité fiable, il est nécessaire d'utiliser des primitives cryptographiques comme les algorithmes de chiffrement. Il est également essentiel d'établir des clés secrètes entre les paires ou les groupes de nœuds capteurs, ce qui est nécessaire aux primitives cryptographiques qui permettent d'assurer les services de sécurité dans un RCSF. Ainsi, Il est primordial d'utiliser un mécanisme de gestion de clés Afin d'assurer l'efficacité de ces fonctionnalités.

Dans ce chapitre, nous allons donner un aperçu sur les problèmes de sécurité dans les RCSFs qui différent des autres réseaux. Puis, on va décrire les différents mécanismes de sécurité destinés aux RCSFs, notamment en termes d'établissement et de gestion des clés. Ensuite, nous détaillons le mécanisme de la gestion de clés et on a classé leurs méthodes et protocoles. Enfin, nous représentons les métriques d'évaluation et une conclusion.

2.2. Objectif de la sécurité dans les RCSFs

Sécuriser un système informatique implique directement l'atteinte des objectifs suivants :

2.2.1. Authentification

Un adversaire n'est pas limité simplement à modifier le paquet de données. Il peut changer le jet entier de paquets en injectant les paquets additionnels. Ainsi, avec l'authentification le récepteur doit s'assurer que les données utilisées dans n'importe quel processus décisionnel proviennent de la source correcte [**9**].C'est-à-dire qu'un nœud malveillant ne peut pas prétendre être un nœud de réseau de confiance [**18**]. L'authentification des données est assurée grâce au Code d'Authentification de Message (CAM), ou MAC en anglais (Message Authentification Code) [**19**].

2.2.2. La confidentialité

La confidentialité est la garantie que l'information d'un nœud n'est rendue accessible ou révélée qu'à son destinataire. Dans notre cadre, il est important qu'aucun capteur étranger au système ne puisse être mis à proximité dans l'intention de surveiller les informations échangées. Le chiffrement offre une certaine confidentialité qui protège les paquets de données d'être révélée à des attaquants passifs par le biais d'écoutes clandestines [**20**].

2.2.3. L'intégrité

Permet de vérifier qu'une donnée n'a pas été modifiée par une entité tierce (nœuds intermédiaires malveillants). C'est un service qui garantit que les données n'ont pas été altérées pendant la transmission. Garantir l'intégrité des données dans le réseau signifie bloquer toute essai d'injection de fausses données. Généralement, afin de vérifier l'intégrité le MAC (Message Authentiquassions Code) et les signatures numériques sont utilisés [**8**].

2.2.4. La disponibilité

Elle signifie que le réseau est disponible pour assurer ses services et autoriser les parties communicantes lorsque ceci est nécessaire. Cette propriété reste difficile à assurer dans les RCSF étant donnée les contraintes qui pèsent sur ces réseaux [gdc2] tel que : la topologie dynamique, la communication sans fil qui peut être facilement brouillée ou perturbée par un attaquant, et les ressources limitées des capteurs de transit [**8**].

2.2.5. La Fraîcheur

Elle permet de garantir que les données échangées sur le réseau sont actuelles et ne sont pas une réinjection de précédents échanges interceptés par un attaquant [gdc2]. Pour résoudre ce problème, un compteur ou bien un nombre pseudo-aléatoire peut être intégré aux paquets de données pour filtrer les vieux messages [**8**].

2.3. Les vulnérabilités de la sécurité dans les RCSF

Les réseaux de capteurs sans fils possèdent quelques faiblesses sont inhérentes à la nature des réseaux de capteurs sans fils et d'autres à la technologie retenue pour leur mise en œuvre et leur déploiement. Nous distinguons deux catégories de précarité : les vulnérabilités physiques et les vulnérabilités technologiques.

2.3.1. La vulnérabilité physique

La vulnérabilité physique est le fait qu'un capteur est fréquemment installé dans un lieu peu sûr, 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 [**21**]. Ainsi que, les capteurs sont vulnérables à la capture physique et au vandalisme.

2.3.2. La vulnérabilité technologique

Les vulnérabilités technologiques sont liées à plusieurs facteurs tel que :

- **L'énergie** :

L'énergie est un facteur critique à considérer en concevant des mécanismes de sécurité [doc], L'énergie des nœuds de capteur est limitée, et généralement irremplaçable. Alors, cette limitation impose la conception des mécanismes de sécurité à faible consommation énergétique

- **La mémoire** :

Dans les réseaux de capteurs sans fils, la limitation des ressources restreint les mécanismes de sécurité. En effet, les nœuds n'ont pas la capacité de mémoriser des clés de taille importante ou d'exécuter des protocoles cryptographique complexes **[22]**

- **Transmission/réception** :

Les capacités de transmission/réception du capteur sont limitées pour des besoins de conservation d'énergie. En effet, la transmission est particulièrement l'opération la plus couteuse d'un point de vu énergétique dans les RCSFs (la transmission d'un bit est équivalent à environ 800 à 1000 opérations CPU).Par conséquent, Dans la conception de mécanisme de sécurité, le nombre de messages échangé entre les nœuds capteurs doivent être pris en considération.

2.4. Attaques et contremesures

Une variété d'attaques contre les RCSFs est rapportée dans la littérature spécialisée. Pour faire face à ces attaques, diverses contre-mesures ont été proposées. La plupart des attaques détaillées dans cette partie concernent les réseaux sans fil comme WLAN, MANET et WSN. Les différentes caractéristiques des réseaux de capteurs sans fil (faible puissance de calcul, énergie limitée, et l'utilisation des ondes radio, etc. ...) les exposent à de nombreuses attaques

de sécurité. Nous détaillons dans la suite quelques types d'attaques et les contremesures pour se défendre de leurs effets. Nous avons choisi de répartir les attaques selon l'intention de l'attaquant **[23].**

2.4.1. Collection d'informations

L'attaquant commence à collecter et analyser les données grâce à des attaques de type «collection d'informations». Il peut par la suite utiliser ces données pour déclencher d'autres types d'attaques selon les failles découvres par ses analyses **[23].**

Eavesdropping ou Passive Monitoring

L'attaque *Eavesdropping* fait partie des attaques passives pour lesquelles les adversaires cherchent à surveiller ou à collecter les informations circulant dans le réseau **[23].** Le but de cette attaque est d'écouter le trafic sur les canaux de communication et d'intercepter les paquets. En effet, ce type d'attaques est plus facile à réaliser (il suffit de posséder un récepteur adéquat) et il est difficile de le découvrir puisque l'attaquant n'apporte aucune modification sur les données échangées. Ainsi, l'intrus peut espionner et capter des données stratégiques qui peuvent aider au lancement d'attaques plus dangereuses ou bien la connaissance des nœuds importants dans le réseau (chef de groupe "cluster head").

Divulgation d'information

Cette attaque est utilisée pour connaître un maximum d'informations sur le RCSF comme la topologie, le protocole MAC, le protocole de routage et les mécanismes de sécurité comme l'authentification et les algorithmes de chiffrement, etc. L'analyse des paquets reçus ou envoyés d'un nœud pourra donner des précisions sur son rôle. Pour lutter cette attaque, il faut user des clés suffisamment grandes ou renouvelées périodiquement **[21].**

2.4.2. Perturbation des communications

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

liaison de données, réseau et transport de la pile protocolaire **[23].** Nous détaillons dans ce qui suit quelques attaques qui perturber les communications dans les réseaux de capteurs sans fils **[21].**

2.4.2.1. Jamming

Une attaque bien connue sur la communication sans fil, vu la sensibilité du média sans fil au bruit, le nœud malveillant essaye d'interférer avec la fréquence radio utilisée par les nœuds capteurs dans le réseau **[24].** Il s'agit d'émettre des signaux sur les mêmes fréquences de manière à empêcher les transmissions et/ou les réceptions de données sur ces fréquences, et provoque ainsi l'indisponibilité des canaux de transmission. Dans ce cas-là, l'intention est de provoquer un déni de service.

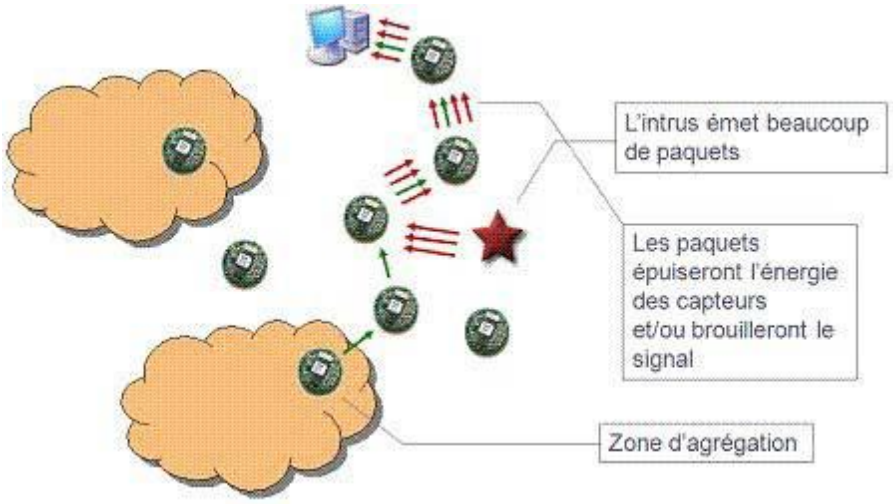

Figure 2-1 Attaque de jamming [9]

2.4.2.2. Collision

L'attaque de collision peut être facilement lancée par un nœud légitime, qui ne respecte pas les conditions d'accès au média de transmission. L'objectif est de provoquer des collisions avec des transmissions voisines. En effet, l'attaquant vérifie le canal de communication afin d'assurer que le support est occupé (réception des paquets RTS et CTS). Si c'est le cas, il envoi des paquets corrompus afin d'entrer en collision avec les paquets échangés dans le réseau.

2.4.3. Agrégation de données et épuisement de ressources

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

2.4.3.1. Sybil

L'attaque par identité multiple ou Sybil est l'une des attaques les plus difficiles à détecter. Le nœud malicieux dans ce type d'attaque peut prétendre un nombre important d'identités afin d'altérer le fonctionnement des autres nœuds du réseau. Cette attaque peut être utilisée pour lancer d'autres types d'attaques tels que le trou noir. Chaque identité (ID) peut être générée aléatoirement ou être dupliquée (recopiée) d'une identité légitime qui existe déjà. Ainsi, un nœud malveillant bien placé peut facilement intercepter les clés cryptographiques, ce qui provoque de graves perturbations à l'ensemble du réseau **[24].**

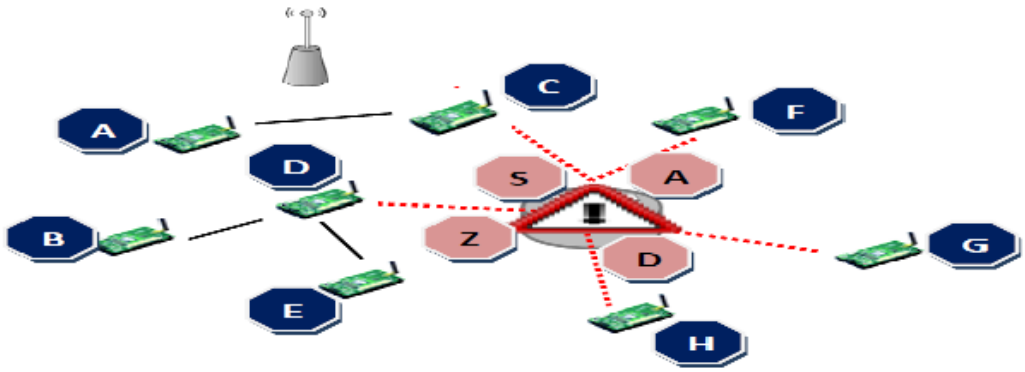

Figure 2-2 L'attaque Sybil [25]

2.4.3.2. De-Synchronisation

L'objectif de cette attaque est l'interruption des connexions existantes. Un attaquant peut par exemple intercepter à plusieurs reprises des messages destinés à un autre nœud dans le réseau, incitant ainsi le nœud récepteur à demander la retransmission des trames manquées. Si l'attaque est lancée au bon moment, l'attaquant peut dégrader ou même empêcher le nœud récepteur de bien échanger les données avec les nœuds émetteurs. Par conséquent, le nœud attaquant pousse sa victime à gaspiller son énergie en tentant de réparer les erreurs de transmission qui n'ont jamais vraiment existé **[24].**

2.4.4. Capture physique de nœuds

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

2.4.4.1. Tampering (Attaque d'altération)

Les RCSFs sont généralement déployés dans des zones hostiles et non surveillées. Par conséquent, les nœuds capteurs sont vulnérables aux attaques d'altération physique pour extraire toutes les informations importantes comme les clés cryptographiques **[24].** 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

2.5. Solutions adaptées aux communications des RCSF

Les RCSFs sont menacés facilement à cause de l'utilisation de l'air comme médium de transmission et ont besoin d'être protégés par des méthodes adaptées à leurs applications **[23].** Pour cela, il est nécessaire de protéger les communications entre les nœuds capteurs, où aucun adversaire ne peut altérer l'échange des paquets de données. Pour créer ce canal, il est nécessaire d'utiliser des primitives cryptographiques, et il est également nécessaire d'établir les informations de sécurité (clés secrètes) essentiels à ces primitives.

2.5.1. Primitives cryptographique

Plusieurs mécanismes basés généralement sur l'utilisation des primitives cryptographiques sont mis en place afin de répondre à la question de la sécurité dans les RCSFs. Une primitive cryptographique est un algorithme cryptographique de bas niveau, bien documenté, et sur la base duquel est bâti tout système de sécurité informatique. Ces algorithmes fournissent notamment des fonctions de hachage cryptographique et de chiffrement. Ces primitives reposent généralement sur des problèmes mathématiques complexes et difficiles à résoudre. Nous allons aborder dans ce qui suit les différentes primitives cryptographiques destinées aux réseaux de capteurs sans fil.

2.5.1.1. 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 [26]. Les objectifs de la cryptographie sont la confidentialité, l'authentification, l'intégrité des données et la non-répudiation. L'établissement d'un système cryptographique basé sur des clés sécurisées est l'une des premières contre-mesures de sécurité dans les RCSFs. On distingue deux types de cryptographies permettant d'assurer chacune un certain nombre de propriétés :

La cryptographie symétrique :

La cryptographie à clé symétrique est également connue sous le nom de cryptographie à clé partagée, à clé unique et à clé secrète. Pour fonctionner, elle nécessite que la même clé soit utilisée entre deux nœuds communicants pour chiffrer et déchiffrer les données en utilisant un algorithme de chiffrement symétrique .Il existe deux types d'algorithmes de chiffrement symétrique :

- **Le chiffrement en chaîne**

Le chiffrement en chaîne consiste à chiffrer le texte clair au fur et à mesure de sa création ou de sa réception par le module de chiffrement. Il est fait bit à bit sans attendre la réception entière des données. L'algorithme le plus connu est : RC4 (*Rivest Cipher 4*) [27].

- **Chiffrement par bloc**

Le chiffrement par bloc scinde les données à chiffrer en blocs de taille fixe (souvent 64 ou 128 bits). Chaque bloc sera ensuite chiffré une fois qu'il atteint la taille envisagée. Les algorithmes les plus utilisés sont [28] : DES (*Data Encryption Standard*), AES (*Advanced Encryption Standard*).

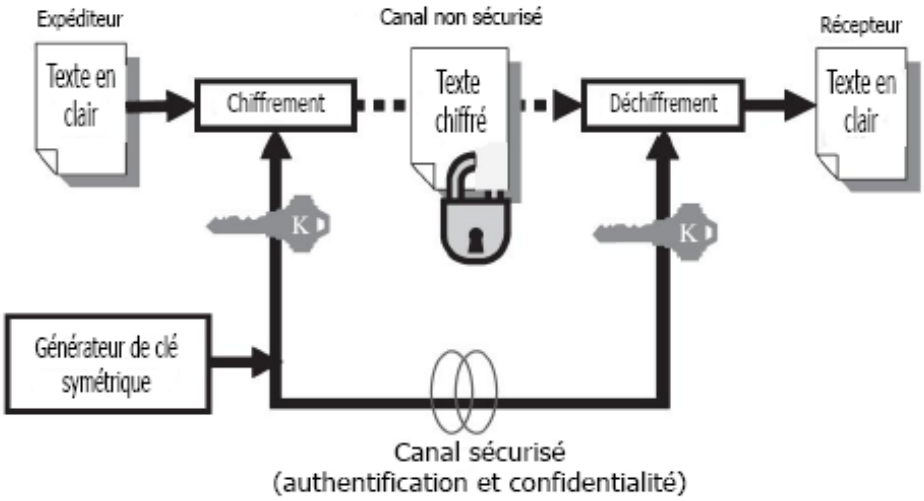

Figure 2-3 la cryptographie symétrique [27]

La cryptographie asymétrique

Elle se repose sur l'utilisation de deux clés différentes, qui sont générées par le récepteur : une clé publique diffusée à tous les nœuds servant au chiffrement de données qu'ils vont émettre au récepteur et une clé privée maintenue secrète chez le récepteur servant pour le déchiffrement de ces données lorsque ce dernier les reçoit. Ainsi, l'émetteur peut utiliser la clé publique du récepteur pour chiffrer un message que seul le récepteur (en possession de la clé privée) peut déchiffrer, garantissant la confidentialité du contenu. D'un autre côté, l'émetteur peut utiliser sa propre clé privée pour signer un message et le récepteur peut vérifier la signature du message à l'aide de la clé publique correspondante. Dans ce cas, ce mécanisme permet aussi de garantie l'authentification des auteurs des messages en utilisant la signature numérique. La figure 2.3 illustre un mécanisme de chiffrement basé sur la cryptographie asymétrique. Bien que le chiffrement asymétrique comporte des avantages, mais la complexité de ce type de cryptographie n'exige que le nœud capteur à une capacité de traitement et de stockage plus élevée et une consommation d'énergie plus haute. Parmi les algorithmes de chiffrement asymétrique les plus connus nous citons : l'ECC (elliptic curve cryptography) [20] et le RSA (Rivest Shamir Adleman) [29].

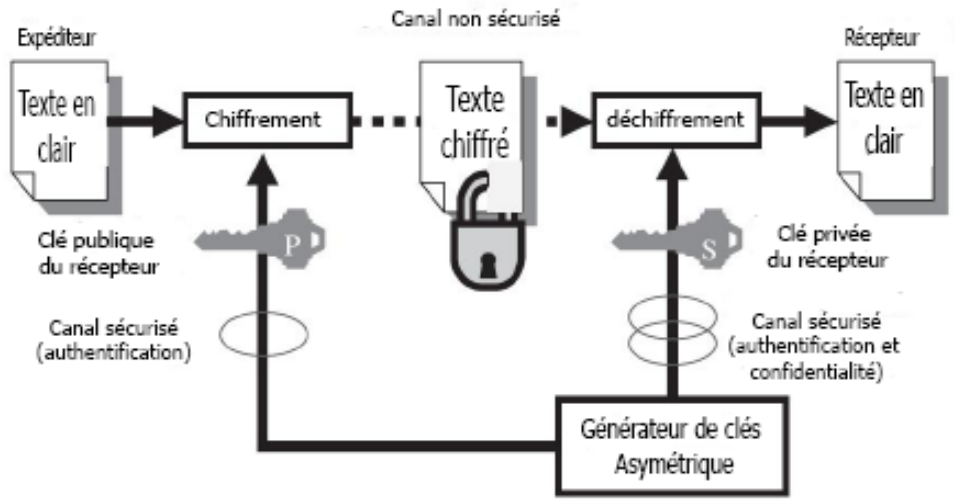

Figure 2-4 la cryptographie asymétrique [27]

2.5.1.2. La fonction de hachage

Il s'agit de la troisième grande famille d'algorithmes utilisés en cryptographie. Le principe est qu'un message clair de longueur quelconque doit être transformé en un message de longueur fixe inférieure à celle de départ. Le message réduit portera le nom de "haché" ou de "condensé". L'intérêt est d'utiliser ce condensé comme empreinte digitale du message original afin que ce dernier soit identifié de manière univoque. Deux caractéristiques (théoriques) importantes sont les suivantes [1] :

- Ce sont des fonctions unidirectionnelles : À partir d'H (M), il est impossible de retrouver M.

- Ce sont des fonctions sans collisions : À partir de H(M) et M il est impossible de trouver M′ ≠ M tel que H(M′) = H(M).

Les algorithmes de hachage les plus utilisés actuellement sont : MD5 (MD signifiant Message Digest) créant une empreinte digitale de 128 bits et SHA (Secure Hach Algorithme) créant des empreintes d'une longueur de 160 bits.

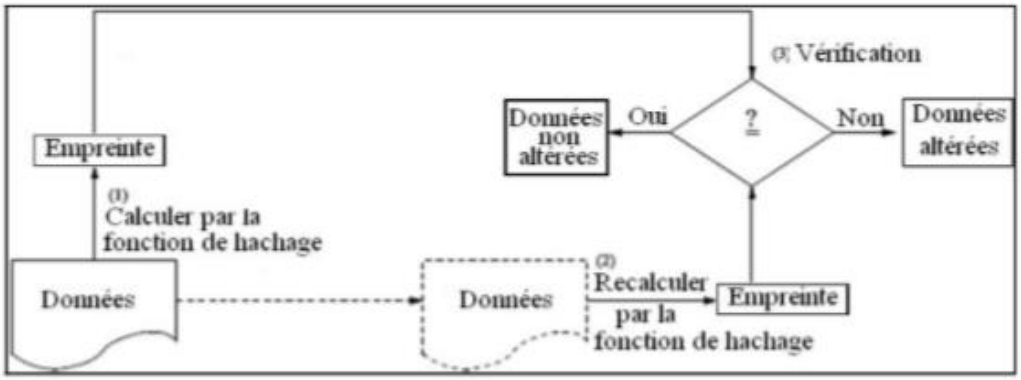

Figure 2-5 La fonction de hachage [29]

2.5.1.3. Le code d'authentification de message

Le code d'authentification de message (MAC) est un système qui permet l'authentification du message lui-même, et quelquefois l'expéditeur. Il permet donc au destinataire de vérifier que le message que lui a envoyé un expéditeur avec qu'il est en relation n'est pas corrompu (il s'agit ici de modification frauduleuse et volontaire du message et non pas d'erreurs de transmissions qui elles sont traitées par d'autres mécanismes. En effet, un MAC est un algorithme qui prend en entrée un message M à envoyer et une clé secrète K et qui produit un condensé. Ce dernier est par la suite envoyé avec les données. Le destinataire calcule à son tour le condensé MAC avec cette même clé et le compare au condensé qu'il a reçu. Ainsi, Un MAC doit être difficile à forger c-à-dire qu'un attaquant ne doit pas pouvoir calculer de MAC sans connaître la clé.

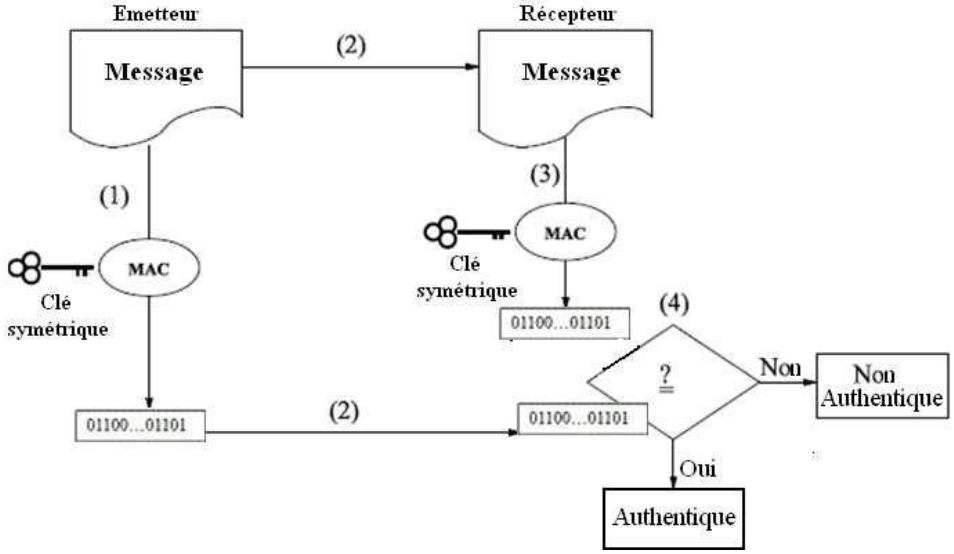

Figure 2-6 Le code d'authentification de message MAC [29]

2.5.2 La gestion des clés

La gestion des clés est définie comme étant l'ensemble des techniques et procédures qui ont pour but la distribution et l'établissement de clés secrètes entre deux ou plusieurs entités communicantes afin de réaliser les techniques cryptographiques. En effet, elle fournit des mécanismes efficaces, sécurisés et fiables de gestion de matériels utilisées dans les opérations cryptographiques. Elle clés 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. Par conséquence, la gestion de clés revêt un caractère primordial pour l'établissement d'une communication sécurisée.

2.6. La gestion de clés : méthodes et protocoles

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

2.6.1. Composants de la gestion de clés

La gestion de clés est un mécanisme essentiel pour assurer la sécurité des applications et des services réseau dans les RCSF. L'objectif de la gestion de clés consiste à définir les clés utilisées entre les nœuds de manière sécurisée et fiable après le déploiement. En outre, ce système doit prendre en charge le renouvellement et la révocation des clés pendant tout le cycle de vie du réseau. De ce fait, un système de gestion de clés inclut les trois composants suivants (voir figure 2.7) [16].

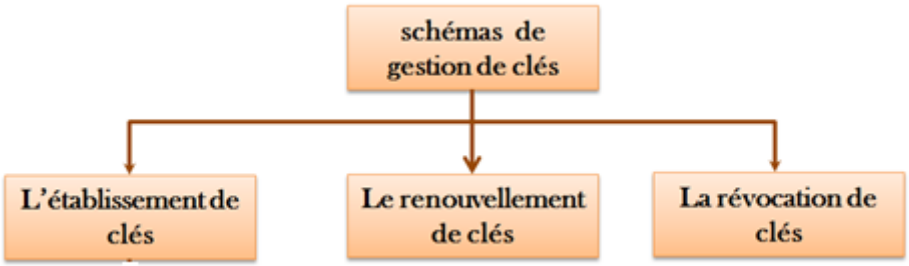

Figure 2-7 Schéma global montrant les composants d'un protocole dédié à la gestion de clés au sein d'un réseau de capteurs [8]

2.6.1.1. L'établissement de clés

L'établissement de clé est un processus ou protocole par lequel une clé secrète partagée devient disponible pour deux ou plusieurs entités, pour une utilisation cryptographique ultérieure. Ainsi, l'établissement de clé consiste à créer une clé de session entre les entités qui ont besoin de communiquer en toute sécurité les unes avec les autres. L'établissement de clés dans les réseaux de capteurs 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 fournir la disponibilité, maintenir la confidentialité des clés, fournir une protection de l'intégrité et une authentification suffisante, etc.

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

Pour éviter ou rendre une telle situation plus difficile pour l'adversaire, le système de gestion de clés doit permettre le renouvellement de clés. Il constitue un défi majeur pour le système de gestion de clés puisque des nouvelles clés doivent être créées d'une manière efficace et conforme à une consommation et conservation d'énergie. Plusieurs raisons justifient le renouvellement de clés du réseau RCSF [30].

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

2.6.1.3. La révocation de clés

La révocation d'un nœud compromis se fait par l'élimination de leur trousseau de clés. Pour cela, lorsqu'un nœud contrôleur (qui a une grande connectivité et peut être mobile) détecte un nœud compromis dans le réseau il diffuse un message de révocation à tous les nœuds du réseau pour que les clés du nœud compromis soient retirées des listes de clés des autres nœuds. La révocation assure qu'un nœud capteur évincé n'est plus en mesure de déchiffrer les messages sensibles transmis sur le réseau. Ainsi, ce processus consiste à empêcher tous intrus de modifier le comportement du réseau en injectant de fausses données ou en modifiant des données des nœuds sécurisés.

2.6.2. Les phases d'établissement de clé

Traditionnellement, l'établissement de clés s'effectue en se basant sur un système qui basé sur les technique de cryptage asymétrique (clé publique) se prêtent à l'établissement de clés, car elles permettent la construction sécurisée de clé secrètes partagées. Par contre, les RCSFs ne peuvent pas palier toutes les exigences de la cryptographie asymétrique (*capacité de calcul et mémoire de stockage)*, ce qui rend son utilisation non appropriée, ainsi une approche symétrique particulière est déployée dans les RCSFs, ce qui réduit le coût d'établissement de clés. Le problème majeur avec la cryptographie symétrique est de pouvoir trouver une méthode qui achevé l'établissement de clé entre les nœuds. Pour résolvent ce problème en passant par le procédé de pré-distribution de clés qui demande un chargement d'information secrète dans les nœuds capteurs avant leur déploiement dans le réseau. Cette information secrète aide des nœuds capteurs à dériver la clé secrète réelle. Les réseaux de capteurs sans fils usent un mécanisme à clé symétrique pour l'établissement de clés reposée sur la pré-distribution de clés, cela est réalisé en trois étapes suivantes [27] :

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

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

de clés, un gros problème est de savoir comment charger un ensemble de clés (appelé porte-clés) dans la mémoire limitée de chaque capteur.

2.6.2.2. Découverte de clé partagée

Après le déploiement, selon la portée de communication, un nœud doit découvrir ses voisins parmi lesquelles il partage une clé. Ainsi, si un nœud partage une clé commune avec un nœud particulier, il peut utiliser cette clé pour une communication sécurisée. Le bon schéma de découverte de voisin ne donnera pas à un adversaire l'opportunité de découvrir les clés partagées et ne peut donc faire que l'analyse du trafic.

2.6.2.3. Établissement de clés de chemin

Après la phase de découverte de clés partagées, le réseau devient un graphe connecté formé de quelques liens sécurisés. 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 [33] [34].

2.6.3. Classification de méthodes et protocoles

La plupart des protocoles de gestion de clés existants pour les réseaux de capteurs sans fils sont basées sur la cryptographie symétrique. En général, la majorité des techniques basées sur les systèmes symétriques résolvent le problème d'établissement de clés en passant par une phase de pré-distribution. La pré-distribution de clés de chiffrement dans un RCSF est le fait de stocker ces clés dans la mémoire des nœuds avant le déploiement. Nous trouvons plusieurs classifications de gestion et distribution de clés dans la littérature comme celle de [35] – [36]. La figure 2.8. illustre une taxonomie des solutions de gestion de clés basées sur la pré-distribution. Dans cette taxonomie, les protocoles sont classés dans plusieurs catégories selon la topologie du réseau (hiérarchique ou plate) et la manière avec laquelle les nœuds voisins partagent des clés communes (probabiliste ou déterministe). Dans cette section, nous détaillerons les principales solutions de cette figure.

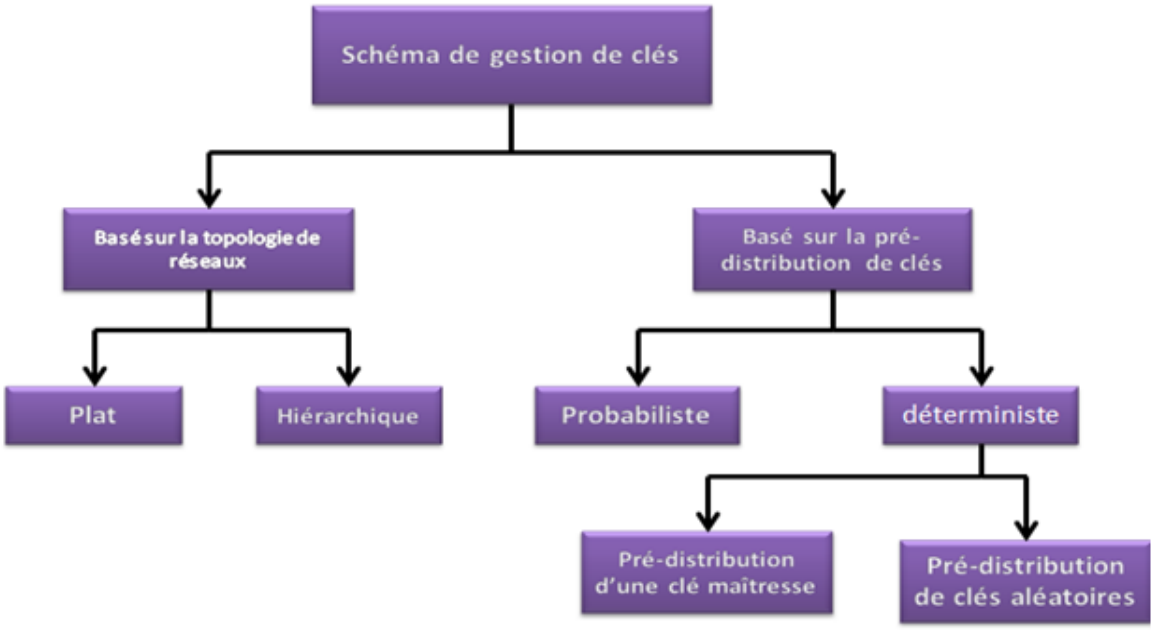

Figure 2-8 Classification des schémas de gestion de clés dans le réseau de capteur sans fil [34]

2.6.3.1. Schémas probabilistes

Pour les approches probabilistes, il est important qu'un sous ensemble de clés choisies au hasard à partir d'un grand ensemble de clés et placés dans les nœuds capteurs avant le déploiement. Donc, l'idée de base de ces approches est que deux nœuds capteurs communiquent entre eux ont une certaine probabilité d'avoir partagé une clé commune qui appartient aux deux sous-ensembles de ces communicants.

Eschenauer et Gligor ont proposé un schéma de gestion de clés basé sur la probabilité de partager une clé entre les nœuds d'un graphe aléatoire. Il fournit des techniques pour la pré-distribution de clés, la découverte de la clé partagée, l'établissement de clé de chemin ainsi que la révocation de clés. L'idée maîtresse de ce schéma est de distribuer aléatoirement un certain nombre de clés, issues d'un ensemble fini à chaque nœud du réseau avant son déploiement. Deux nœuds quelconques seront en mesure de s'échanger des messages sécurisés s'ils possèdent une clé commune. Dans ce schéma, trois phases sont nécessaires pour installer les clés secrètes entre les nœuds capteurs [30].

(i) Phase de pré-distribution de clés

Un grand ensemble de clés P (Pool) est générée. Ensuite, pour chaque nœud, m clés sont choisies au hasard de l'ensemble P. Ces m clés sont stockés dans la mémoire du nœud et forment le porte-clés (Key ring) du nœud. Le nombre de $|P|$ de l'ensemble est choisi de telle maniéré que deux sous-ensemble aléatoire 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 $|P|$=10000 clés [14].

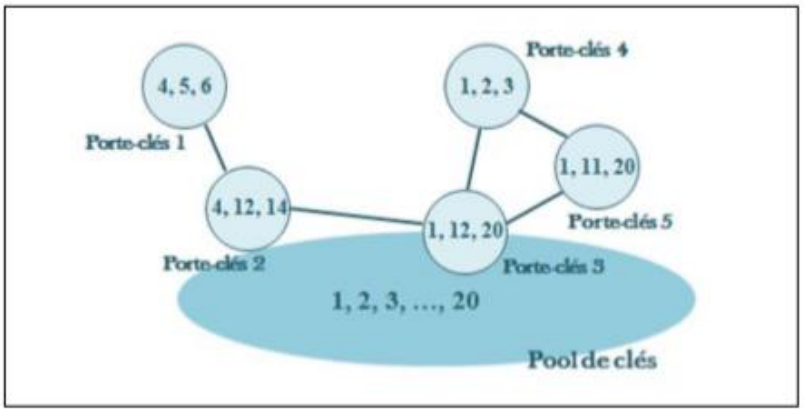

Figure 2-9 un exemple du schéma d'Eschenauer et Gligor [36]

(ii) Phase de découverte de clés partagées

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

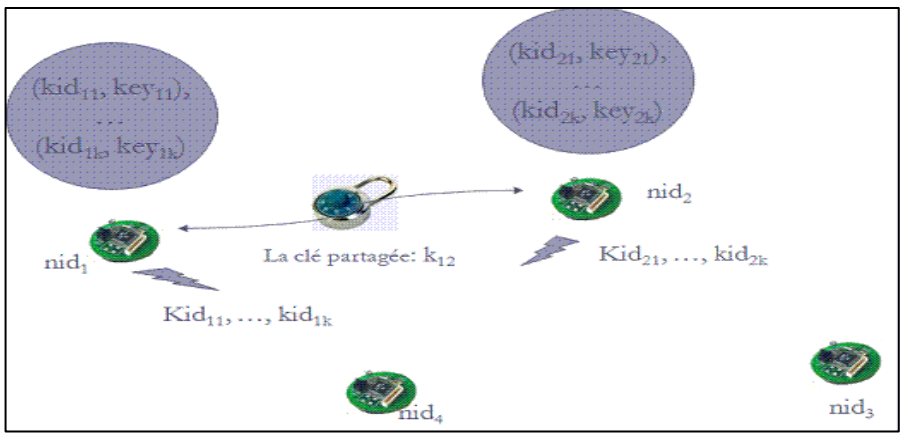

Figure 2-10 découvertes des clés partagées [8]

(iii)Phase d'établissement de chemin de clé

Après la phase de découverte de clés partagées, le réseau devient un graphe connecté formé de quelques liens sécurisés. Les nœuds capteurs 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 [38]. La figure suivante illustre cette phase :

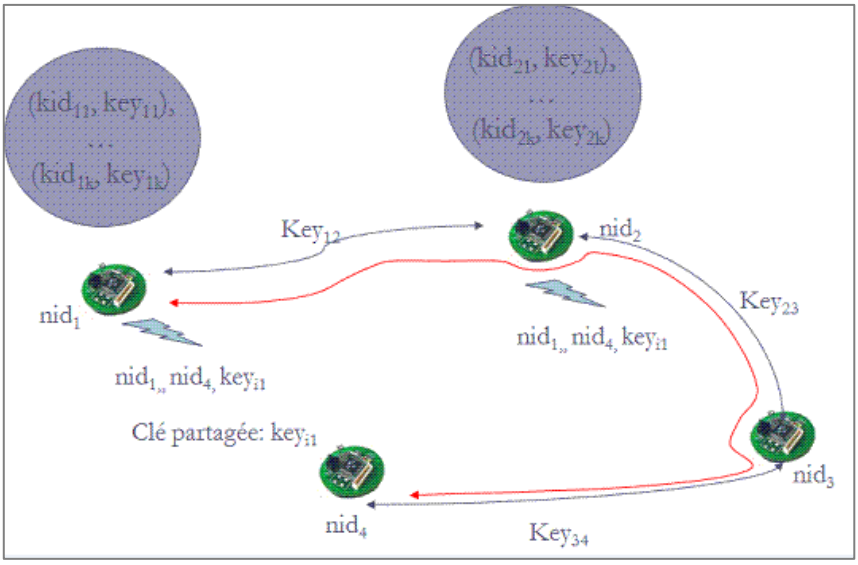

Figure 2-11 Etablissement de chemins sécurisés [8]

(iv)Révocation de clés

La révocation d'un nœud compromis se fait par l'élimination de leur trousseau de clés. Pour cela, un nœud contrôleur (qui a une grande connectivité et peut être mobile) annonce un message simple de révocation contenant une liste signée de k identificateurs des clés (k_{idi}) pour que ces clés soient retirées des trousseaux de clés des autres nœuds [38]. La liste des identités est signée par une clé de signature générée par le nœud contrôleur et envoyée en unicast à chaque nœud en la chiffrant avec la clé partagée entre tous les nœuds et le nœud de contrôle pendant la phase de pré-distribution de clés. Une disparition des liens sera produit à cause de la suppression de clés du nœud compromis ce qui nécessite une reconfiguration de ces liens. (par la découverte de clés partagées ou l'établissement de chemin de clé). La figure suivante illustre cette phase :

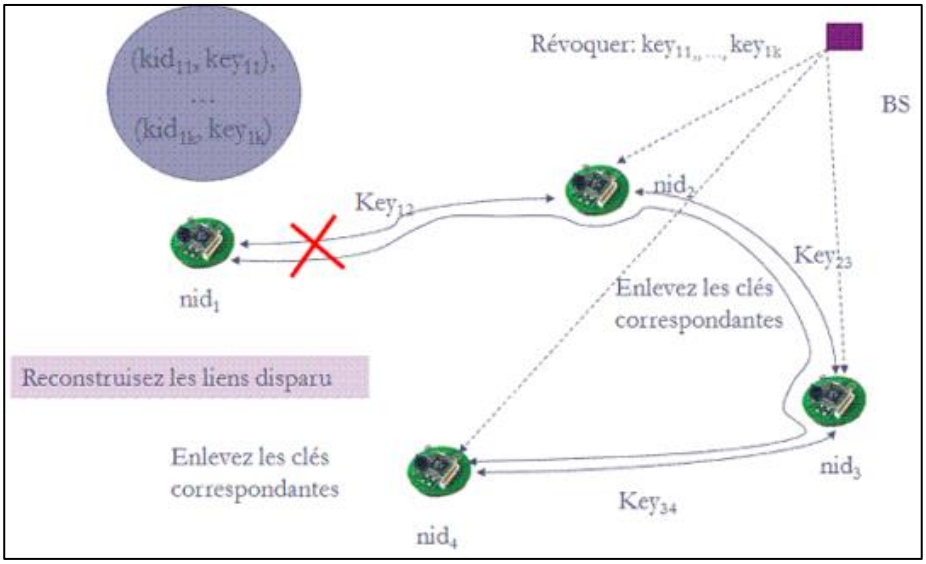

Figure 2-12 révocations de clés [38]

Chan et al. Ce schéma est identique à celui d'Eschenaur et Gligor sauf qu'au lieu d'exiger le partage d'une clé commune pour sécuriser un lien, une paire de nœud doit partager q clés avec q > 1 pour établir un lien sécurisé. La nouvelle clé utilisée pour la communication entre ces deux nœuds est le hash de toutes les clés partagées. Un exemple de schéma de pré-distribution de clé Q-composite est illustré à la figure 2-13. La taille du pool de clés $|P|$ est le paramètre critique à calculer pour que le schéma Q-Composite soit efficace. Ainsi, $|P|$ est calculée en fonction de la contrainte de la probabilité que deux nœuds partagent au moins q clés et le nombre de clés qu'un nœud peut contenir m. [27].

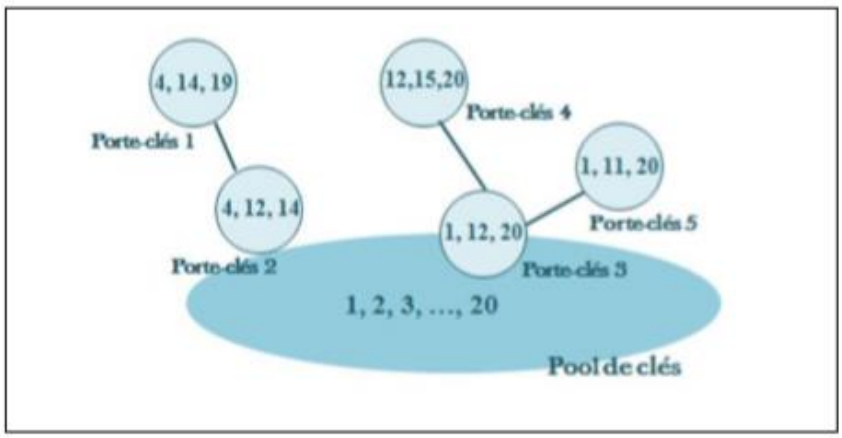

Figure 2-13 schéma Q-composit (36]

2.6.3.2. Schémas déterministes

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

Blom utilise une matrice publique G de taille (λ+1) N et une matrice D symétrique de taille (λ+1)(λ+1) qui est générée sur GF (q) et où N est la taille du réseau. L'ensemble des clés par-paires de ces N nœuds sont stockées dans une matrice symétrique appelée matrice secrète $K = AG$, sachant que $= (DG)^T$. K_{ij} de la matrice K est la clé du nœud i pour sécuriser la liaison avec le nœud j. Après, chaque nœud i est pré-chargé avec la i-ème rangée de la matrice secrète et la i-ème colonne de la matrice publique [9]. Cette méthode est illustrée à la figure 2.14. Après déploiement, chaque paire de nœuds i et j peuvent individuellement calculer la clé partagée entre eux $K_{ij} = k_{ji}$ 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. Le schéma de Blom nécessite une multiplication coûteuse de deux vecteurs de taille λ +1 où les éléments sont aussi grands que la taille de clé cryptographique correspondante. Chaque nœud capteur diffuse un message et reçoit un message de chaque nœud dans sa couverture radio, où les messages portent un vecteur de taille λ +1 [2].

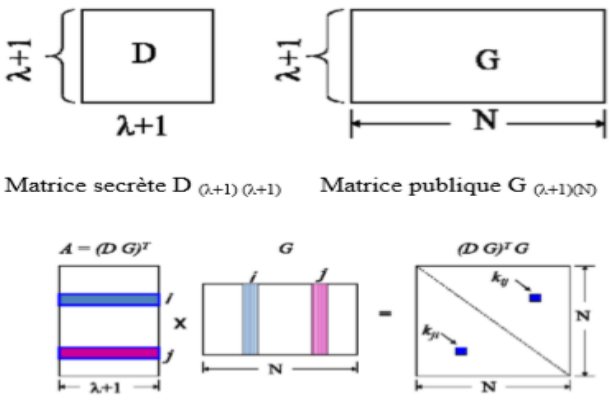

Figure 2-14 méthode de Blom [8]

Blundo et autres [38] ont proposé une approche conforme également à la propriété de λ du fait qu'elle utilise un polynôme symétrique bivariant de degré λ, $P(x,y) = \sum_{i=0}^{\lambda}\sum_{j=0}^{\lambda} a_{ij}x^i y^j$, qui est généré sur un corps fini $GF(q)$, où nous avons $P(x,y) = P(y,x)$ en choisissant $a_{ij} = a_{ji}$. Chaque nœud i est pré-distribué avec un polynôme $P(i,y)$. Après le déploiement, Pour établir une clé par paire, chaque nœud évalue le polynôme à l'ID de l'autre nœud de capteur. Dans le cas de deux nœuds quelconques i et j, la clé commune entre eux est $K_{ij} = P(i,j) = P(j,i)$. Ce mécanisme polynômial assure que la sécurité est parfaite quand pas plus de λ nœuds sont compromis, la communication est réduite et le coût de stockage du polynôme est relatif au degré λ.

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

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

Lai et al. ont proposé le protocole BROSK (Broadcast Session Key). Dans ce schéma, une seul clé chargée dans les nœuds avant le déploiement. Une paire de nœuds peut être établie une clé de session à l'aide de cette clé principale et d'un nombre aléatoire échangé entre chaque capteur. Ce schéma présente une évolutivité infinie et chaque capteur n'a besoin que de très peu de mémoire. Cependant, l'inconvénient est évident. Lorsque la clé principale est compromise, toutes les clés paires sont exposées. Par conséquent, ce schéma n'a aucune résilience. En dehors de cela, il n'y a pas d'authentification car tous les capteurs ont la même clé principale [39].

Zhu et autres proposent le protocole déterministe LEAP (Localized Encryption and Authentication Protocol). LEAP est un protocole de gestion de clés conçu pour les réseaux de capteurs hiérarchiques afin de limiter l'impact du nœud compromis sur le voisinage immédiat. Il prend en charge l'établissement de quatre types de clés pour chaque nœud capteur : une clé individuelle partagée avec la station de base, une clé par paire partagée avec un autre nœud capteur, une clé de cluster partagée avec plusieurs nœuds voisins et une clé de groupe partagée entre tous les nœuds du réseau. Avant le déploiement, la BS génère une clé maîtresse initiale et la stocke dans la mémoire de chaque nœud capteur. Lorsque la phase de déploiement est terminée, chaque nœud capteur u dérive de cette clé sa propre clé individuelle $K_u = f_{K_I}(ID_u)$ .Puis il diffuse un message « HELLO » contenant son identifiant ID à ses

voisins. Lorsqu'il reçoit un « ACK » d'un voisin v, il pourra vérifier son identité en calculant au début K_v ($K_v = f_{K_I}(ID_v)$) et par suite le MAC. Une fois l'identité de v vérifiée, u calcule sa clé unique partagée avec lui $K_{uv} = f_{K_v}(ID_u)$. Le noeud v pourra calculer cette clé de la même façon. Après que le temporisateur d'établissement de clé atteint sa valeur de seuil T_{min}, le nœud supprime la clé maîtresse initiale et les clés individuelles de ses nœuds voisins. Il garde seulement sa clé individuelle et les clés uniques partagées avec ses voisins. Supposons que soit maintenant un chef de cluster qui souhaite envoyer une clé de cluster à ses nœuds voisins. Il génère au début une clé aléatoire ; puis il la chiffre à l'aide de la clé par paire partagée avec chaque nœud voisin avant de l'envoyer en unicast à ses voisin (membre de cluster). . Cependant, la clé de groupe est pré-chargée à chaque nœud capteur avant le déploiement. [40] [41].

2.6.4. Métriques d'évaluation

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

2.6.4.1 .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 capteur est compromis, et l'influence de ce nœud sur la sécurité du réseau [38]. En effet, quand un nœud est capture par un intrus, son secret entier ainsi que les liens établis avec ses voisins sont compromis. Les effets d'une telle attaque peuvent affecter d'autres nœuds dans le réseau. Dans ce cas il peut utiliser les informations stockées dans les nœuds capteurs compromis pour lancer des nouvelles attaques. Dans le contexte d'établissement de clés, l'adversaire peut essayer de déduire la clé partagée entre les nœuds capteurs non compromis. Les schémas probabilistes sont vulnérables aux compromissions des nœuds, du moment où les clés pré-charges dans les nœuds capteurs sont prélevées à partir du même pool. En outre, la résilience à la capture du nœud capteur change d'un schéma à un autre selon le nombre de clés requis pour l'´établissement d'un lien sécurise.

2.6.4.2 Connectivité

La connectivité se définie comme la probabilité qu'un nœud puisse partage une clé (c.à.d établir un lien sécurisé) avec l'ensemble de ses voisins. Comme nous avons étudié dans la partie 2.6.3.2, dans un grand nombre des schémas déterministes, tous les nœuds sont pré-chargés avec une clé initiale. Cette clé est utilisée après le déploiement et lors de phase d'établissement de clés pour dériver des clés par-paires avec tous les nœuds voisins. Par contre, pour les schémas de gestion de clés probabiliste des paires des nœuds capteurs ne peuvent pas avoir une clé partagée, cela permet de limiter la connectivité du réseau. Par conséquent, pour garantir la continuité de la sécurité, la méthode de gestion de clés (déterministe ou probabiliste) doit être capable d'assurer une bonne connectivité du réseau.

2.6.4.3. Passage à l'échelle (scalability)

Le nombre de nœuds capteurs déployés dans un réseau peut être à l'ordre de centaines, voire plusieurs milliers. Pour certaines applications, il peut atteindre quelques millions. Afin de garantir le bon fonctionnement du réseau, les nouveaux 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.

2.6.4.4. Efficacité des ressources

Dans les réseaux de capteurs, l'efficacité des ressources représente une métrique de performance significative. Pour cela, les concepteurs au moment du développement des protocoles de gestion de clés, ne doit pas consommer une grande quantité de ressources. Les ressources ici pourraient être :

La capacité de stockage : est la quantité de mémoire nécessaire pour enregistrer les informations de sécurité, tel que les clés.

La capacité de communication : est mesuré par le nombre de messages échangés nécessaire pour la gestion de clés.

La puissance de traitement : est mesurée en termes de quantité de cycles de processeur nécessaires pour l'établissement de clés.

2.7. Conclusion

La gestion de clés est le mécanisme de sécurité fondamental dans les réseaux de capteurs sans fil. Il s'agit des technologies de base pour établir des communications sécurisées entre les RCSFs et les contraintes de ces derniers qui rendent impossible l'application des méthodes classiques de sécurité dans de tels réseaux. 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, 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. Nous avons présenté néanmoins quelques schémas de gestion de clés utilisant les méthodes de pré-distribution de clés. 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 III
Implémentation et évaluation d'un protocole de gestion de clés

3.1. Introduction

Malgré les prouesses et avancés technologiques, il est actuellement évident de constater que les nœuds capteurs possèdent une faible capacité en termes de calcul, de stockage et d'énergie, ce qui les rend vulnérables et faciles à corrompre afin de récupérer les informations qu'ils possèdent. Dans ce contexte, un mécanisme de sécurité est en effet nécessaire pour la majorité des applications basées sur le RCSF, en particulier lors de l'utilisation des nœuds capteurs dans un lieu peu sûr. La gestion de clés constitue la pierre angulaire des autres mécanismes de sécurité, car presque tous les mécanismes de sécurité reposent sur le cryptage ou sont liés à celui-ci., toutes les méthodes de gestion de clés que nous avons étudiées ont été proposés dans le but d'avoir un schéma fiable, qui garantit un niveau élevé de sécurité, et optimise les métriques des performances.

Dans le cadre de notre étude et après avoir abordé quelques protocoles et solutions de gestion de clés proposés pour les RCSFs, nous nous sommes intéressés par le travail [1] intitulé "Secured Communication Key Establishment for Cluster based Wireless Sensor Networks ". Dans ce travail les auteurs ont développé deux approches différentes pour la gestion de clés. Nous avons choisi l'une de ces approches pour l'implémenter et vérifier leurs métriques de performances telles que le coût de stockage, le coût de communication, et la consommation d'énergie.

Dans ce chapitre, nous présentons cette version de protocole de gestion de clés qui a été associée aux RCSFs ayant une topologie hiérarchique. Nous commencerons d'abord par présenter la motivation derrière ce choix. Nous présentons ensuite les détails de cette version de protocole de gestion de clés, suivie d'une évaluation de leurs performances.

3.2. Motivation du choix du protocole

La gestion des clés dans les réseaux de capteurs sans fil est l'un des aspects assurant la sécurité de la communication des messages transitant dans le réseau. Cependant, les travaux portant sur le problème d'énergie dans ce domaine ont essentiellement pris le dessus. Toutefois, trois critères sont principalement pris en considération : le coût de la communication, le coût de calcul ainsi que l'espace mémoire nécessaire pour le stockage d'informations au niveau de chaque nœud capteur. Après l'étude de certains protocoles existants dans la littérature, nous avons décidé d'implémenter et d'évaluer l'une des approches de gestion de clés qui a été les fruits de travail de Q.Mamun et autres [1] intitulé "

Secured **C**ommunication **K**ey **E**stablishment for Cluster based Wireless Sensor Networks - *Shared Partial Keys* " que nous avons baptisé SC-SPK. Les raisons pour ce choix sont [1] :

- SC-SPK dédiée à une topologie hiérarchique en clusters des RCSFs, qui peut simplifier et améliorer la scalabilité et même améliorer l'efficacité de la procédure de gestion de clés ;
- SC-SPK est modifiable et évolutif ;
- SC-SPK est déterministe et basé sur la cryptographie symétrique.
- présente des avantages importants en termes de coût de stockage grâce à l'emploi des clés partielles au lieu des clés complètes ;
- 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.
- robuste contre les attaques de capture des nœuds ;
- Une caractéristique importante du SC-SPK est que deux nœuds communicants utilisent toujours une nouvelle clé secrète pour le cryptage/décryptage des données à chaque cycle. Cette fonctionnalité permet aux RCSFs d'obtenir une résilience aux attaques.

3.3. Spéciations générales sur le modèle du réseau

Dans notre étude, nous nous intéressons aux réseaux RCSF hiérarchiques à base en clusters en raison de leurs avantages dans la prolongation de la durée de vie du réseau de capteurs. En effet, dans cette architecture, le réseau est constitué d'un ensemble de groupe de capteurs (cluster), tel qu'il est illustré dans la Figure 3.1. Dans chaque cluster un chef de groupe appelé *cluster-head* a la responsabilité de collecter et gérer les informations à partir de ces nœuds membres, par la suite agréger ces données et les envoyer à la station de base [8].

Tous les nœuds du réseau, à l'exception de la station de base, ont les mêmes ressources. Les cluster-heads sont uniformément distribuées dans le réseau et sont choisies en fonction de la fonction de regroupement, dont la valeur dépend de divers critères tels que la localisation, la portée de communication, les capacités en ressources et en énergie. L'énergie résiduelle de cluster-head est réduite lors des calculs et des communications. Il est donc nécessaire de disposer des mécanismes de rotation du CH qui permettent de prolonger la durée de vie du CH et par conséquent du réseau

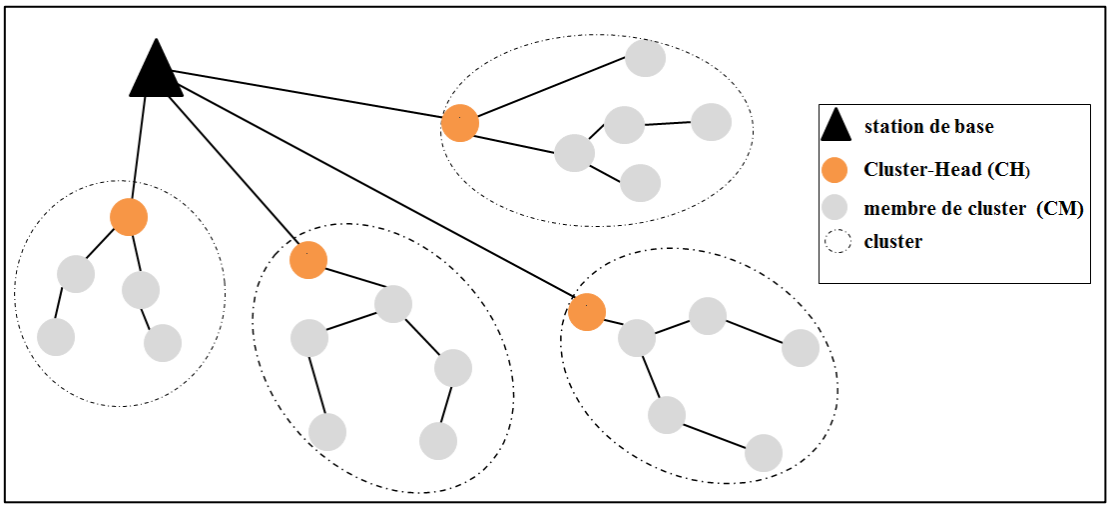

Figure 3-1 Modèle d'architectures hiérarchique pour un RCSF [8]

3.4. Fonctionnement du protocole

SC-SPK (**S**ecured **C**ommunication Key Establishment for Cluster based Wireless Sensor Networks -***P**rivate **P**artial **K**eys*) est un système de gestion de clés déterministe destiné aux RCSFs hiérarchique en clusters. Ce système reposé sur la pré-distribution de clés partielles et la cryptographie symétrique. Le processus de déroulement de SC-SPK est divisé en trois phases qui sont : la pré-distribution de clés, la formation du cluster et l'état stable. Dans la première phase les nœuds sont pré-chargés avec certain matériel cryptographique tel que le pool de clés partielles et la liste d'index de clés partielles. Dans la deuxième, après la formation des clusters et une vérification d'authentification par la station de base, tous les nœuds capteurs d'un cluster partagent la même liste de clés partielles. Enfin, chaque cluster aura un ensemble distinct de clés partielles qui seront utilisées dans cette dernière phase pour établir les clés secrètes de communication. Nous exposons au tableau 3.1 un résumé des notations que nous avons usées afin de détailler chaque phase de ce système. Dans ce qui suit, nous avons détaillé chaque phase liée au schéma de gestion de clés**.**

Tableau 1 Acronymes définition

Notation	Explication
N	nombre total de nœuds de capteurs déployés.
m	nombre total des clusters.
k	nombre total des clés partielles dans le pool de clés.
η	le nombre d'index de clés sélectionné.
Ci	i^{ème} cluster.
P	pool de clés partielles.
PK_i	i^{ème} clé partielle.
L	Liste d'index de clés partielles
L_i	Liste d'index de clés partielles dédie au i^{ème} cluster
ind_n	index de la n^{ème} clé partielle
$ID(x)$	identification unique du nœud x
A_i	un nœud capteur qui est dans le cluster c_i
CH_i	cluster-head de cluster c_i
L_id_{CM}	Liste contenant les identifiants des nœuds membres du cluster
$E_K(M)$	Chiffrement du message M avec la clé K
N_k	La clé de réseau.
$R^q_{A_j}(L_i)$	la fonction adoptée par le nœud A_i pour sélectionner q nombre d'indices de Li dans un ordre aléatoire.
O_{A_i}	l'ensemble d'index de clés partielles sélectionnées par le nœud A_i
$K^t_{A\_B}$	La clé sécrète établie entre les nœuds de capter A et B pour le t^{ème} cycle.
$A \rightarrow B : M$	Le nœud A envoyer le message M au nœud B
$\|\|$	La fonction de concaténation

3.4.1. La pré-distribution de clés

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

- Un pool de clés partielles P, tel que $P = \{PK_1, PK_2, \dots, PK_k\}$
- Une liste d'index de clés partielles, tel que $L = \{ind_1, ind_2, \dots, ind_k\}$
- Une clé de réseau N_k.
- Un numéro d'identification unique ID

3.4.2. La formation du cluster

Après le déploiement des nœuds capteurs, ils signalent d'abord leur emplacement physique à la station de base, puis le réseau commence à sélectionner les cluster-heads à l'aide des algorithmes de sélection des cluster-heads [43] [44].
Une fois le cluster C_i (i=1, 2, …, m) formé et chaque nœud reçoit l'identifiant de leur CH, tous les nœuds membres du cluster envoient leurs ID au cluster-head CH_i.

$$A_i \rightarrow CH_i : E_{K_N}\{ID(A_i)\} \quad \text{tel que } A_i \in C_i$$

Après avoir rassemblé tous les ID, le cluster-head envoie tous les ID avec son propre ID à la station de base pour l'authentification.

$$CH_i \rightarrow SB : E_{K_N}\{\text{L\_ID}, ID(CH_i)\}$$

Où $\text{L\_ID} = \{ID(A_1), ID(A_2), ID(A_3), \dots, ID(A_m)\}$

Ici, m est le nombre de nœuds A dans chaque cluster.

Notez que toutes les communications dans les phases d'établissement de clés sont cryptées par la clé de réseau N_k

Si l'authentification réussit, la station de base (SB) sélectionne une liste de clés partielles dans le pool de clés P pour chaque cluster et envoie la liste d'index identifiées comme $L_i (L_i \subset L)$ au cluster-head du cluster C_i.

$$SB \rightarrow CH_i : E_{K_N}\{L_i\}$$

Où $L_i = \{ind_1, ind_2, \dots, ind_\eta\}$

Ici, η est le nombre d'index de clés sélectionné.

Ensuite, chaque cluster-head CH_i diffuse la liste L_i à tous les nœuds membres du cluster C_i.

$$CH_i \rightarrow A_i : E_{K_N}\{L_i\}$$

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

Une fois qu'un nœud membre a informai quelles clés partielles il emploiera avec son CH, il retire le reste de clés partielles de P qui a été inséré dans la phase de pré-distribution. La figure 3.2 résume le processus de cette phase.

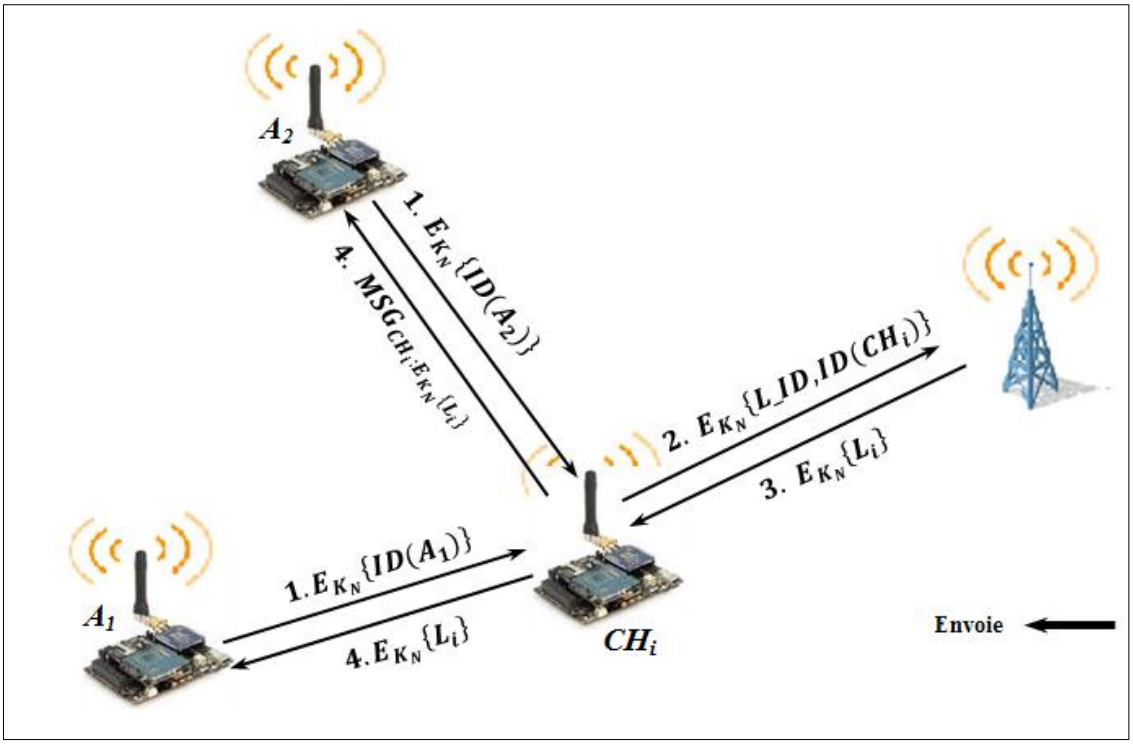

Figure 3-2 le processus de la phase de formation du cluster

L'état stable :

Dans cette phase, les nœuds capteurs sont prêts à établir les clés de communication. En effet, dans la topologie hiérarchique en cluster, un nœud membre A_i du cluster C_i ne communique qu'avec son cluster-head CH_i. Pour cela, afin d'établir une clé de cryptage pour sécuriser la communication entre un membre de cluster A_i et leur cluster-head CH_i, les nœuds (membre ou cluster-head) agissent comme suit :

Le cluster-head CH_i envoie une liste d'ordre unique O_{CH_i} à chaque membre du cluster A_i, contenant la liste ordonnée des numéros d'index de q clés partielles sélectionnées à partir de L_i.

$$CH_i \rightarrow A_i : E_{K_N}\{O_{CH_i}\}$$

Où $O_{CH_i} = R^q_{CH_i}(L_i)$

En réponse, chaque nœud membre A_i crée également une liste d'ordres O_{A_i} avec un ordre différent des index et l'envoyer à CH_i.

$$A_i \rightarrow CH_i : E_{K_N}\{O_{A_i}\}$$

Où $O_{A_i} = R^q_{A_i}(L_i)$

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

Où

$$K^t_{A_i CH_i} = L_i(O_{A_i}[t]) \parallel L_i(O_{CH_i}[t])$$

Où $O_{A_i}[t]$ renvoie le $t^{ème}$ index de A_i

Pour le prochain cycle, A_i et CH_i calculent la clé secrète comme

$$K^{t+1}_{A_i CH_i} = L_i(O_{A_i}[t+1]) \parallel L_i(O_{CH_i}[t+1])$$

Notons qu'après chaque cycle, le cluster-head et les membres peuvent créer des nouvelles listes d'ordres pour générer des nouvelles clés de communication.

Après cette phase, tous les nœuds capteurs (membre ou cluster-head) établissent des clés de communication. Un aperçu du processus de cette phase est présenté à la figure 3.3.

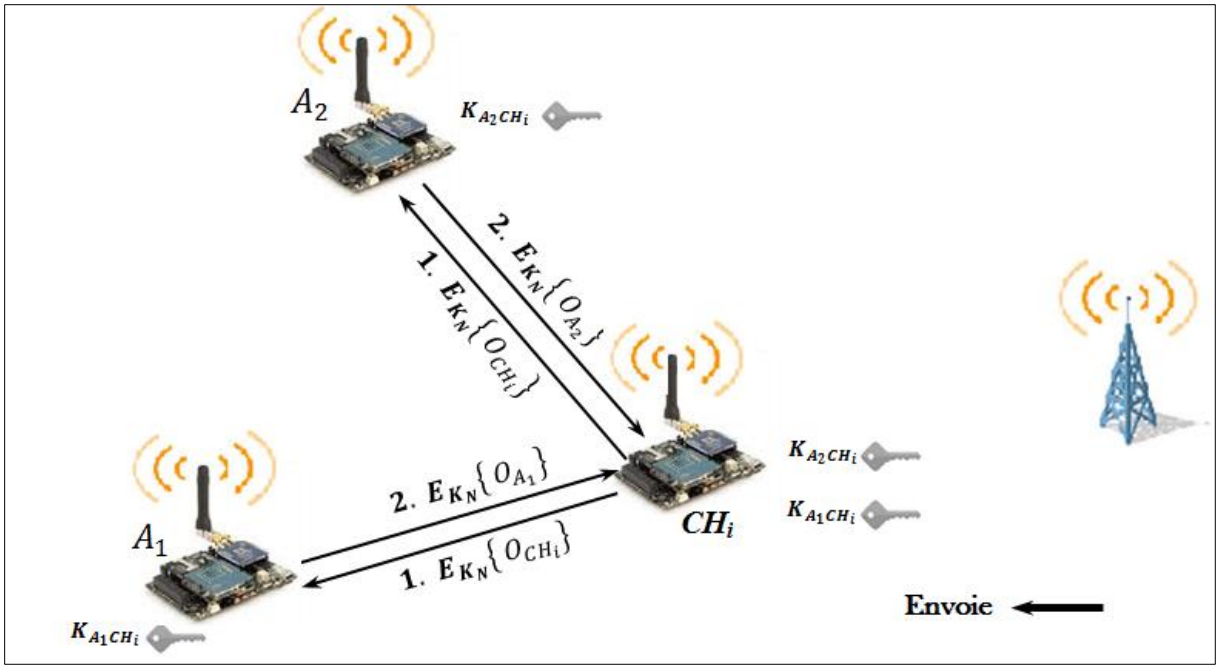

Figure3-3 le processus de la phase d'état stable

3.5. Simulation

La simulation des réseaux de capteurs 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. De plus, la simulation offre un gain considérable en temps, une flexibilité en permettant la variation des paramètres et une meilleure visualisation des résultats [44].

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 [46]. Par ailleurs, TinyOS indique l'environnement de simulation d'applications de RCSFs 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 cadre, nous exposons dans ce qui suit l'environnement TinyOS sur lequel fonctionne le simulateur TOSSIM.

3.5.1.1. TinyOS

TinyOS est un système d'exploitation open-source spécialement conçu pour les réseaux de capteurs sans fil, développé par l'université américaine de BERKELEY. Sa conception a été entièrement réalisée en NesC, langage oriente composant proche du C, et la bibliothèque de composants de TinyOS est particulièrement complète puisque on' y retrouve des protocoles réseaux, des pilotes de capteurs et des outils d'acquisition de donnés. Un programme s'exécutant sur TinyOS est constitué d'une sélection de composants systèmes et de composants développes spécifiquement pour l'application à laquelle il sera destine (mesure de température, du taux d'humidité...). TinyOS s'appuie sur un fonctionnement événementiel, c'est- à -dire qu'il ne devient actif qu'à l'apparition de certains événements, par exemple l'arrivée d'un message radio. Le reste du temps, le capteur se trouve en état de veille, garantissant une durée de vie maximale connaissant les faibles ressources énergétiques des capteurs. Ce type de fonctionnement permet une meilleure adaptation à la nature aléatoire de la communication sans fil entre capteurs [16].

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. [40].

Le simulateur TOSSIM

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

3.5.2. Environnement de simulation et résultats

Pour évaluer les performances de SC-SPK, nous l'avons implémenté en utilisant le langage de programmation NesC [45] afin d'être en mesure de l'intégrer à TinyOS. Les simulations sont effectuées à l'aide de l'environnement TOSSIM [46]. Notre modèle d'expérimentation considère plusieurs réseaux d'une taille variant de 30 à 150 nœuds de type MICA2, Les nœuds sont répartis uniformément et de manière aléatoire. Dispersés sur une surface de 150 × 150 m. La portée de transmission d'un capteur est de 22 m, la taille d'un paquet est de 104 octets et le taux d

‟erreur de transmission est de zéro.

Il faut noter que dans nos simulations, le nombre d'index des clés partielles (5) et le nombre d'index dans la liste ordonnée (q) est de 500 et 25 index respectivement.

Afin d'évaluer les performances de protocole SC-SPK, nous nous intéressons aux métriques suivantes :

3.5.2.1. Le coût 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. La figure 3.4 présente le nombre de paquets de données échangés durant l'établissement de clés des réseaux de taille variant de 30 à 150 nœuds capteurs. Comme la montre cette figure, le coût de communication pour SC-SPK n'est pas affecté par l'évolution du nombre des nœuds. Comparé au CH, le nœud membre nécessite moins de coût de communication. Une évaluation du nombre de paquets transmis et reçus dans le réseau, est présentée dans le tableau 2 :

Tableau 2 : le nombre de paquets échangés

Type de nœud	**Message**	**Number de paquets**	**Le coût total de communication**
Membre	Envoyé	$1 + q.x$	$1 + 2.q.x + 5.x$
	Reçu	$5.x + q.x$	
Cluster-head	Envoyé	$1 + n.5.x + n.q.x$	$1 + (n+1).5.x + 2.n.q.x$
	Reçu	$5.x + n.q.x$	

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

Ainsi, le coût de communication dans SC-SPK dépend linéairement du nombre d'index de clés partielles (η) et du nombre d'index dans la liste ordonnée (q) crée par le cluster-head (CH) ou par le nœud membre (A).

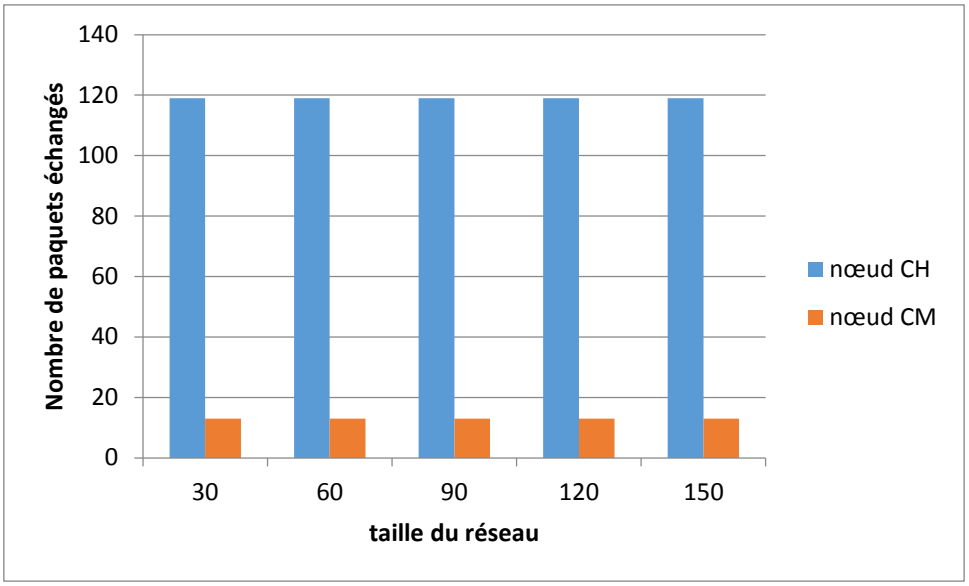

Figure 3-4 le nombre de paquets échangés lors d'établissement de clés

3.5.2.2. Le coût de stockage

Nous nous intéressons au nombre de clés stockées dans chaque type de nœud, car la taille d'espace mémoire exploité est fortement reliée au nombre de clés stockées. La figure 3.5 montre la taille de la mémoire exploitée pour stocker les clés par un nœud membre et un cluster-head en fonction de la taille de réseau. Il est bien clair que dans SC-SPK, pour stocker les clés, un leader utilise un espace mémoire très grand. En effet, la mémoire exploité est liée principalement aux besoins du nœud de capteur pour stocker la clé de réseau (doit être de 128 bits), les m clés partielles (de 64 bits chacune), la liste d'index de clés partielles, les deux listes des index ordonnés (la première est créé par le nœud membre et la seconde est envoyé par leur CH). Dans le cas où le nœud est un cluster-head, $2.n$ listes ordonnée est stockée.

Notons que, pour un pool de clés contenant k clés partielles, $log_2 k$ bits sont requis pour chaque index utilisé.

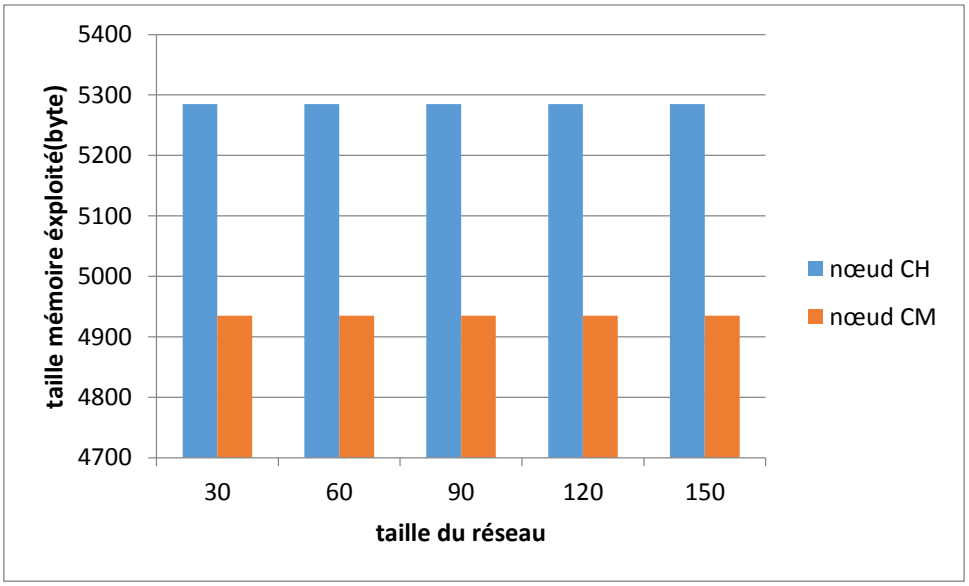

Figure 3-5 l'utilisation de la mémoire par un nœud capteur

3.5.2.3. La consommation d'énergie

La consommation d'énergie est un paramètre important pour toutes les approches de gestion de clés dans les RCSFs. Par conséquent, nous avons utilisé le plugin PowerTOSSIM dans TinyViz pour analyser l'énergie. Cette énergie est calculée sur la base des instructions exécutées pour les opérations cryptographiques et pour les opérations radio (émission et réception des messages). La figure 3.6 montre la variation de l'énergie consommée par SC-SPK en fonction de la taille de réseau.

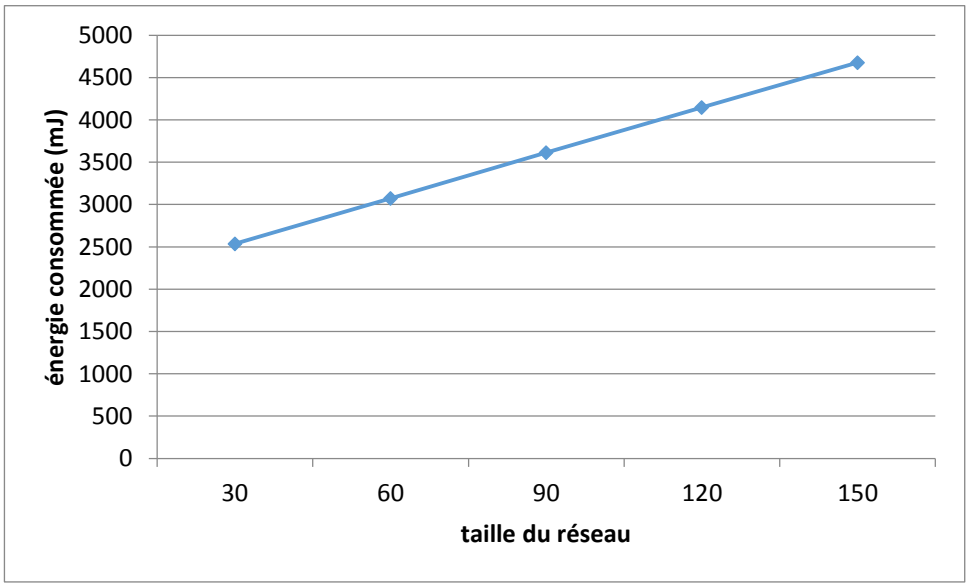

Figure 3-6 la consommation d'énergie par un nœud capteur

3.6. Conclusion

Dans ce chapitre, nous avons présenté l'implémentation le processus d'implémentation ainsi que l'évaluation d'une approche de gestion de clés destinée aux réseaux de capteurs sans fil hiérarchiques. Le système d'exploitation TinyOS a été d'ailleurs utilisé. Nous avons proposé une programmation entière en langage NesC et une simulation avec TOSSIM. L'approche implémenté appelée SC-SPK **(S**ecured **C**ommunication **K**ey **E**stablishment for Cluster based Wireless Sensor Networks - *Shared Partial Key*s) permet à chaque nœud capteur d'établir une clé par paire symétrique secrète pour l'échange de données avec son cluster-head. Le protocole SC-SPK est déterministe et basé sur la cryptographie symétrique. Il surpasse d'autres protocoles de la pré-distribution de clés aléatoires dans le sens où il nécessite moins de coût de communication, car la phase d'établissement de clés de chemin est absente. Il présente des avantages importants en termes de coût de stockage grâce à l'emploi des clés partielles au lieu des clés complètes. C'est dans ce sens que, deux nœuds capteurs communicants utilisent à chaque cycle une nouvelle clé secrète pour le cryptage/décryptage des données. Cette fonctionnalité permet aux RCSFs d'obtenir une résilience aux attaques.
Après des études expérimentales effectuées sur la consommation d'énergie, le coût de communication et le coût de stockage, nous avons constaté que le protocole SC-SPK répond bien aux critères de performances souhaités du réseau, tout en maintenant un niveau de sécurité très élevé.

Conclusion générale

L'élargissement du domaine d'application des réseaux de capteurs sans fils (RCSFs) nécessite plus de sécurité pour garantir l'authenticité, l'intégrité et la confidentialité des données qui circulent dans le réseau. En effet, La sécurité des RCSFs présente des défis liés aux contraintes énergétiques des nœuds et leurs capacités physiques. Par conséquent, les chercheurs travaillent sur cette problématique et proposent des protocoles de sécurité adaptés aux nœuds de capteurs. Cependant, nous avons pu voir que la gestion de clés est la première fonction fondamentale puisque tous les mécanismes de sécurité s'appuient en général sur le cryptage ou sont liés à celui-ci.

Dans le cadre de notre étude et après avoir abordé quelques protocoles et solutions de gestion de clés proposés pour les RCSFs, nous nous sommes intéressés par le travail de Q.Mamun et autres [1] intitulé " **S**ecured **C**ommunication **K**ey **E**stablishment for Cluster based Wireless Sensor Networks ". Dans ce travail les auteurs ont développé deux approches différentes pour la gestion de clés. Nous avons choisi l'une de ces approches pour l'implémenter et vérifier leurs métriques de performances.

L'approche implémenté appelée SC-SPK **(S**ecured **C**ommunication **K**ey **E**stablishment for Cluster based Wireless Sensor Networks - *Shared Partial Keys*) dédiée à une topologie hiérarchique en clusters. Il permet à chaque nœud capteur d'établir une clé par paire symétrique secrète pour l'échange de données avec son cluster-head. Le protocole SC-SPK est déterministe et basé sur la cryptographie symétrique.

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

En ce qui concerne les résultats de simulation obtenus sur la consommation d'énergie, le coût de communication et le coût de stockage, nous avons constaté que le protocole SC-SPK répond bien aux critères de performances souhaités du réseau, tout en maintenant un niveau de sécurité très élevé.

Ainsi, SC-SPK surpasse les protocoles de pré-distribution de clés aléatoires dans le sens où il nécessite moins de coût de communication (car la phase d'établissement de clés de chemin est absente dans ce protocole) et aussi moins d'espace de stockage (en raison de clés partielles

plutôt que complets stockées dans chaque nœud capteur), et ce à cause du fait que deux nœuds communicants utilisent toujours une nouvelle clé secrète pour le cryptage/décryptage des données à chaque cycle.

BIBLIOGRAPHIE

[1] Q. Mamun, R. Islam, and M. Kaosar, "Secured Communication Key Establishment for Cluster based Wireless Sensor Networks", International Journal of Wireless Network and Broadband Technologies (IJWNBT), vol. 4(1), pp. 29-44, 2015.

[2] M.Hamid, R.Rouam, „"Optimisation De Déploiement Et De Localisation De Cible Dans Les Réseaux De Capteurs Sans Fil"", Mémoire De Master En Informatique, Universite Akli Mohand Oulhadj –Bouira, 2018

[3] Ch. Kazi Tani, W.Benhaddouche**, ''** Implémentation Et Test D"un Protocole De Prévention De L"attaque Clone Dans Un Réseau De Capteurs Sans Fil **'',** Mémoire De Master En Informatique**,** Université Abou Bakr Belkaid– Tlemcen, 23 Juin 2014

[4] A.Chouha, „" Traitement Et Transfert D"images Par Réseau De Capteurs Sans Fil „", Mémoire De Magistère En Informatique, Université Hadj Lakhder – Batna, 16/ 03/2011

[5] A.Saidi, W.Mamem,"" Développement D"une Application Orientée Surveillance Pour Les Réseaux De Capteurs Sous Contiki""**,** Mémoire De Licence En Informatique, Université AbouBakr Belkaid– Tlemcen**,** 27 Mai 2015

[6] A.Benayad,""Implémentation Et Sécurisation du Protocole De Routage AODV optimisé pour les RCSF (OAODV)"", MEMOIRE MASTER En Télécommunications, Université Aboubakr Belkaïd– Tlemcen, 26 / 09 /2017

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

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

[9] S.Athmani, „" Protocole De Sécurité Pour Les Réseaux De Capteurs Sans Fil"", Mémoire Magistère En Informatique, Université Hadj Lakhder - Batna, 15/07/2010

[10] La tolérance aux pannes dans les réseaux de capteurs sans fil

[11] O.DRISSI, Implémentation d'une strategie de routage multi-niveau de données d'un réseau de capteurs sans fil dans le domaine ferroviaire, Mémoire de fin d'étude en Génie Electrique, Université du Québec à Trois-Riviéres, Canada, juin 2014.

[12] K. BENBADALLAH',Optimisation d'un protocol de routage AODV dans les réseau de capteurs sans fils'',Mémoire de fin d'étude En T2lécommunications , Univertsité Aboubaker Belkaid-Tlemcen,14 juin 2016.

[13] M.Bouallegue, „"Protocoles De Communication Et Optimisation De L"énergie Dans Les Réseaux De Capteurs Sans Fil"" Mémoire Doctorat En Télécommunications, Université Du Maine, 31/03/2016

[14] A.Hentati, „" Sélection Des Noeuds Dans Les Réseaux De Capteurs Sans Fil Avec Récolte D"énergie"", Mémoire Maîtrise En Sciences Appliquées (Génie Éléctrique), Université De Montréal, Juin 2016

[15] K.Barka,"" Une Plateforme Middleware Pour L"auto-Adaptation Des Réseaux De Capteurs Sans Fil Hétérogènes"", Thèse Doctorat En Informatique, Université De Batna 2, 08/06/2019

[16] Ch.Kazi Tani, W.Benhaddouche**, ''**Implémentation Et Test D"un Protocole De Prévention De L"attaque Clone Dans Un Réseau De Capteurs Sans Fil"" Mémoire Master En Informatique, Université Abou Bakr Belkaid– Tlemcen, 23 Juin 2014

[17] S.Maarouf, S.Ouadah, ‘’Implémentation Et Evaluation Des Schémas De Routage Sur Une Plateforme Réelle De Réseaux De Capteurs Sans Fil’’, Mémoire Master En Informatique, Université Abou Bakr Belkaid– Tlemcen, 25 Juin 2014
[18] I.F. AKYILDIZ, W. Su, Y. SANKARASUBRAMANIAM, E. CAYIRCI. "Wireless sensor networks: a survey". Computer Networks 38, Elsevier Science, pp. 393–422, 2002.
[19] B.A. BENSABER, ‘’Réseaux de Capteurs : Impacts et défis pour la société ‘’, École d’été Internationale, Université de Bejaïa, Du 30 juin au 03 juillet.
[20] Y. MALEH, A. EZZATI, « Etude Et Développement D’un Protocole Symétrique Pour Sécuriser Les Communications Des RCSF », Thèse De Doctorat, Faculté Des Sciences Et Technique De Settat, 2015
[21] Z.BELKHEDIM, S. DEKKICHE, ‘’Implémentation d’un protocole de sécurité dans les réseaux de capteurs sans fil’’, Mémoire De Master en Télécommunications, Université Hassiba Benbouali De Chlef, octobre 2020
[22] F. HU, N.K.SHARMA,’’ Security Considerations In Ad Hoc Sensor Networks’’, Ad Hoc Networks 3, Elsevier Science, pp. 69–89, 2005.
[23] I.MANSOUR, ‘'Contribution A La Sécurité Des Communications Des Réseaux De Capteurs Sans Fil”, Thèse De Doctorat En Informatique, Université Blaise Pascal – Clerment Ii, France, 5 Juillet 2013.
[24] D.E.BOUBICHE,’’ Une approche Inter-Couches (cross-layer) pour la Sécurité dans les R.C.S.F ’’, Thèse Doctorat en Informatique, Université de Batna
[25] Z.BELKHEDIM, S. DEKKICHE, ‘’Implémentation d’un protocole de sécurité dans les réseaux de capteurs sans fil’’, Mémoire De Master en Télécommunications, Université Hassiba Benbouali De Chlef, octobre 2020
[26] A. Berrachedi, et A. Diarbakirli, “ Sécurisation du protocole de routage hiérarchique LEACH dans les réseaux de capteurs sans fil”, mémoire de fin d'étude pour l'obtention du diplôme d'ingénieur d'état en informatique, Ecole nationale Supérieure d’Informatique (E.S.I), Algérie, Juin 2009
[28] S.jacob, ‘’protection cryptographique des bases de donnéses conception et cryptanalyse’’ soutenance,3 oct 2012
[27] W. ZNAIDI, “ Quelques propositions de solutions pour la sécurité des réseaux de capteurs sans fil”, thèse de doctorat en informatique, L'Institut National des Sciences Appliquées de Lyon, France, 2010
[29] A.Benayad,’’Implémentation Et Sécurisation du Protocole De Routage AODV optimisé pour les RCSF (OAODV)’’, MEMOIRE MASTER En Télécommunications, Université Aboubakr Belkaïd– Tlemcen, 26 / 09 /2017

[30]M.Bouallegue, ‘’Protocoles De Communication Et Optimisation De L’énergie Dans Les Réseaux De Capteurs Sans Fil’’ Mémoire Doctorat En Télécommunications, Université Du Maine, 31/03/2016
[31] Ch.Kazi Tani, W.Benhaddouche**, ‘’**Implémentation Et Test D’un Protocole De Prévention De L’attaque Clone Dans Un Réseau De Capteurs Sans Fil’’ Mémoire Master En Info
rmatique, Université Abou Bakr Belkaid– Tlemcen, 23 Juin 2014
[32] F. Hu, J. Ziobro, J. Tillett, et N. K. Sharma, « Secure Wireless Sensor Networks: Problems and Solutions », *Rochester Inst. Technol. Rochester N. Y. USA*, vol. 1, no 4, p. 11, 2004.
[**33]**Y. Maleh et A. Ezzati, « Etude et développement d’un protocole symétrique pour sécuriser les communications des RCSF », Thèse de doctorat, Faculté des Sciences et Technique de Settat, 2015.

[34] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, et P. Spilling, « A survey ofkey management in ad hoc networks », *IEEE Communications Surveys & Tutorials*, vol. 8, no 3, p. 48–66, 2006.
[35] S. Ruj, A. Nayak, I. Stojmenovic, « Key Predistribution in Wireless Sensor Networks When Sensors Are Within Communication Range », in *Theoretical Aspects of Distributed Computing in Sensor Networks*, S. Nikoletseas, J. D. P. Rolim, Éd. Berlin, Heidelberg, 2011, p. 787‑832.
[36] S. A. Camtepe, B. Yener, « Key Distribution Mechanisms for Wireless Sensor Networks: a Survey », 2005.
[37]Y.Challal, Réseaux de capteurs sans fil, Système intelligents pour de transfert, Université de Technologie de Compiègne, Heudiasuc, France.17/11/2008.
[38]H. Chan, A. Perrig, and D. Song. "Random key pre-distribution schemes for sensor networks". In Proceedings of the IEEE Symposium on Security and Privacy, pp. 197–213, May 11–14, 2003.
[39] C. Blundo, A. D. Santix, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. "Perfectlysecurekey distribution for dynamic conferences". In: Proceedings of the 12th AnnualInternational Cryptology Conference on Advances in Cryptology, Berlin: Spring-Verlag,pp. 471-486, 1992.
[40]S. Zhu, S. Setia, and S. Jajodia. "LEAP: Efficient security mechanisms for largescaledistributed sensor networks". In ACM CCS, pp. 62–72, October 2003.
[41] X. Zhang, J. He, and Q. Wei, "EDDK: energy-efficient distributed deterministic key management for wireless sensor networks", EURASIP Journal on Wireless Communications and Networking, vol. 2011(12), pp. 1-11, 2011.
[42] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks", IEEE Transactions on Mobile Computing, vol. 3(4), pp. 366–379, 2004.
[43] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless micro sensor networks", In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, January 2000.
[44]M.NAIDJA, '' Auto-adaptation dans les RCSF hétérogènes pour des e-applications'', Thèse Doctorat en Informatique, Université de Batna 2, 24 /05/2018
[45] D. Gay, P. Levis, R.V. Behren, M. Melsh, E. Brewer, and D. Culler, "The nesC Language: A Holistic Approach to Networked Embedded Systems", In Proceedings of the ACM SIGPLAN conference on Programming language design and implementation (PLDI '03), pp. 1-11, San Diego, California, USA, June 2003.
[46] N. Lee, M. Welsh, and D. Culler, " TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications", In Proceedings of 1st International Conference on Embedded networked sensor systems (SenSys '03), ACM, pp. 126-137, Los Angeles, California, USA, November 2003.