République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohamed Khider – BISKRA

N d'ordre :
RTIC02/M2/2022

Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département d'Informatique

Mémoire

Présenté pour obtenir le diplôme de master académique en

INFORMATIQUE

Parcours : Réseaux et Technologies de l'Information et de la Communication

Titre : Conception d'un système de gestion de clés pour les réseaux de capteur sans fil .

Réalisé par :
Chaima Hachouf

Sous la direction de :
Dr.Aloui Imene

Abstract

Currently, the integration of key management systems for wireless sensor networks (RCSF) has a positive impact on the level of security on this type of network.

In the majority of studies proposed to solve safety problems in RCSFs, energy is the essential factor taken into account. Achieving a secure protocol without too much affecting the lifetime of the network is a great challenge !

The context of our study is devoted to increasing the security of sensor networks taking into account the energy constraint. This work focuses more particularly on solving a key management system for RCSFs.

In this work, we propose a new secure protocol RA-LEACH as a secure version of the LEACH protocol ; where we apply two encryption algorithm to the LEACH routing protocol. The first step is the application of asymmetric encryption by RSA to ensure the identity of the sensor nodes. And the second step is applying symmetric encryption by AES to encrypt the data. Our new method helps improve security solutions without significantly affecting network lifetime.

Key words :

Sensor network, routing protocols, security, energy, key management.

Résumé

Actuellement, l'intégration des systèmes de gestion de clés pour les réseaux de capteurs sans fil (RCSF) a un impact positif au niveau de sécurité sur ce type de réseaux.

Dans la majorité des études proposées pour résoudre les problèmes de sécurité dans les RCSFs, l'énergie est le facteur essentiel qui prit en compte. Réaliser un protocole sécurisé sans trop affecter la durée de vie du réseau c'est un grand défi !

Le contexte de notre étude est consacrée à augmenter la sécurité des réseaux de capteurs on prenant en considération la contrainte d'énergie. Le présent travail se concentre plus particulièrement sur la résolution d'un système de gestion de clés pour les RCSFs.

Dans ce travail, nous proposons un nouveau protocole sécurisé RA-LEACH comme une comme une version sécurisée du protocole LEACH ; où on applique deux l'algorithme du cryptage au protocole de routage LEACH. La première étape est l'application du cryptage asymétrique par RSA pour assurer l'identité des nœuds capteurs. Et la deuxième étape est l'application du cryptage symétrique par AES pour chiffrer les données. Notre nouvelle méthode permet d'améliorer les solutions de sécurité sans trop affecter la durée de vie du réseau.

Mots-clés :

Réseau de capteur, les protocoles de routage, sécurité, énergie, gestion de clés.

Remerciement

Au nom de Dieu, le Très Miséricordieux, le Plus Miséricordieux, et que les prières et la paix soient sur le plus honorable des messagers, Muhammad Amin, sur lui la paix et les bénédictions. . Tout d'abord, je veux remercier Dieu pour tout ce qu'il m'a donné et pour toute la force qu'il m'a donnée.

Je tiens également à remercier du fond du cœur mon superviseur, le **Dr Imene Aloui** , pour m'avoir guidé dans cette bataille que vous m'avez donnée et m'avoir montré la bonne direction pour devenir une meilleure personne et faire mon travail.

Je voudrais également dire un merci spécial à ma famille, merci à **ma mère** ,**mon père** et mes frères : **Aymen, Ikram, Ghoufran** et mon cousin : **Sara** , pour leur soutien tout au long de mes journées universitaires et de projet, ils sont une grande partie de mon succès aujourd'hui.

Et mes amis :**Narimen** , **Ikhlasse** , **Wafa** et Tout le monde vous remercie pour tout

Liste des sigles et acronymes

RCSF :*Réseaux de capteurs sans fil*

WSN :*Wireless Sensor Network en anglais*

RSA :*Rivest–Shamir–Adleman*

AES :*Advanced Encryption Standard*

LEACH :*Low-Energy Adaptive Clustering Hierarchy*

CH :*Cluster-Head*

TDMA :*Time Division Multiple Acces*

CSMA :*Carrier Sense Multiple Access*

MATLAB :*MATrix LABoratory*

Table des matières

Table des figures

Liste des tableaux

Introduction Générale

Aujourd'hui, Les communications sans fil jouent un rôle important dans nos vies, et l'avancement de ces technologies nous a permis de voir une nouvelle vision et d'acquérir de nouvelles perspectives dans les industries des communications. Contrairement à un environnement câblé, un environnement sans fil offre une plus grande flexibilité dans l'accès et le traitement des informations via des dispositifs informatiques tels que des ordinateurs portables, des ordinateurs et des capteurs [9].

La technologie des Réseaux de Capteurs Sans Fil (RCSF) joue un rôle important dans le domaine de la télécommunication sans fil. Elle permet d'apercevoir une nouvelle façon de recueillir les données avec une la bonne qualité de service [1].

Cependant, un RCSF est principalement limité en termes de ressources (capacités insuffisante de stockage, de traitement et d'autonomie) et par conséquence ils sont limités en termes de sécurité [1].

En raison de leur déploiement dans des environnements sans surveillance, les différents nœuds capteurs d'un RCSF sont vulnérables à la compromission et susceptibles d'une violation physique. De plus, l'utilisation des transmissions sans-fil rend les RCSFs perméables à des malveillances de toutes sortes, et constitue un véritable challenge de sécurité à relever [13].

La nature décentralisée des réseaux et le manque d'infrastructure, les méthodes de sécurité mises en œuvre dans les RCSF doivent inclure la collaboration entre les nœuds, ainsi que les défis de sécurité typiques tels que le routage sécurisé et l'agrégation sécurisée des données [13].

Afin de résoudre ces limites, l'un des solutions proposées par les chercheurs est la conception des systèmes de gestion de clés pour les réseaux de capteur sans fil.

L'objectif principal de ce travail est de réaliser un système de gestion de clés pour les réseaux de capteur sans fil. Où nous proposons un nouveau protocole sécurisé RA-LEACH (RSA- AES-Low-Energy Adaptive Clustering Hierarchy) comme une version sécurisée du protocole LEACH.

Nous avons choisi le protocole LEACH en raison de ses performances en termes d'énergie par rapport à d'autres protocoles de routage.

Notre proposition ajouter au LEACH l'aspect de sécurité où elle combine à la fois l'utilisation des deux algorithmes de cryptage RSA et AES. Notre nouvelle méthode permet

d'améliorer les solutions de sécurité sans trop affecter la durée de vie du réseau.

1. La structure de notre travail est la suivante :

   (a) Le chapitre 1 présente la littérature qui couvre le concept du réseau de capteurs sans fils.

   (b) Le chapitre 2 introduit l'aspect de la sécurité et de la gestion de clés dans les réseaux de capteurs.

   (c) Le chapitre 3 est dédié à la conception de notre architecture proposée RA-LEACH. Où en donnant une description sur le travail et en présente les différentes étapes pour atteindre notre objectif.

   (d) Le chapitre 4 présente, les résultats de simulations qui ont été menées pour évaluer la fonctionnalité du notre système de sécurité.

Chapitre 1

Réseau de capteurs sans fil

1.1 Introduction

Les réseaux de capteurs sans fil ont gagné en popularité ces dernières années, en particulier depuis l'introduction des systèmes microélectromécaniques, c'est une technologie qui a contribué au développement rapide des capteurs intelligents. Les réseaux de capteurs sans fil consistent en un ensemble de nœuds de capteurs à petite échelle et à faible coût avec une portée de communication, une puissance, un traitement et un stockage limités. Les réseaux structurés et non structurés sont deux formes de RCSF. Dans le premier cas, les nœuds sont affichés avec soin, tandis que dans le second cas, les nœuds sont affichés rapidement. L'infrastructure du réseau RCSF est très limitée. Il s'agit simplement d'un ensemble d'un grand nombre de nœuds de capteurs qui fonctionnent ensemble pour surveiller une zone ou collecter des données environnementales. Un RCSF non structuré est celui qui contient un ensemble dense de nœuds de capteurs entre les deux types de RCSF. Ces nœuds capteurs peuvent être positionnés en déplacement et, une fois déployés sur le terrain, peuvent fonctionner quelle que soit la météo [1].

1.2 Réseaux de capteurs sans fil

Un Réseau de Capteurs Sans Fil (RCSF ou WSN : Wireless Sensor Network en anglais) C'est un système distribué qui connecte un grand nombre d'entités indépendantes appelées "capteurs sans fil" ou "capteurs". Nous saurons de quoi il s'agit et en quoi il consiste.

1.2.1 Définition de capteur

Un capteur est un appareil électronique à faible coût qui convertit l'état d'une grandeur physique perçue (température, lumière, pression, etc.) en une grandeur utilisable. Ces minuscules entités électroniques forment les éléments centraux des réseaux de capteurs [2].

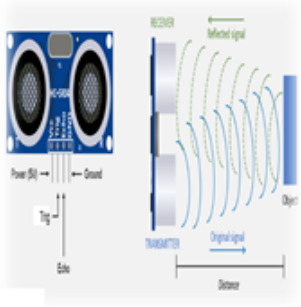
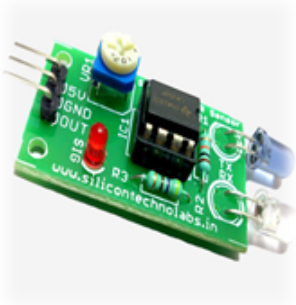
module multi-capteurs	Capteur à ultrasons	Capteur infrarouge	Capteurs de proximité
			

FIGURE 1.1 – Exemples de capteurs [2].

1.2.2 Définition Réseaux de capteurs sans fil

Un réseau de capteurs sans fil est un groupe de différents nœuds de capteurs connectés ensemble dans un ou plusieurs bassins dans une zone appelée zone de capteurs, et peut être déployé dans n'importe quelle partie du monde pour collecter et analyser des informations telles que la température, la pression, les vibrations, le son ...etc.Cette architecture se base sur l'interaction entre les trois éléments suivant [1] :

1. **nœud de capteur**
2. **Zone d'intérêt** : également appelée « terrain de bassin versant », une zone géographique dans laquelle nous somme il place des capteurs réseau à surveiller [1].
3. **Stations de base (Sink)** : également appelées nœuds de connexion où les données circulent Je finis. Il dispose de plus de ressources matérielles et permet la collecte et le stockage des informations issues des capteurs [1].

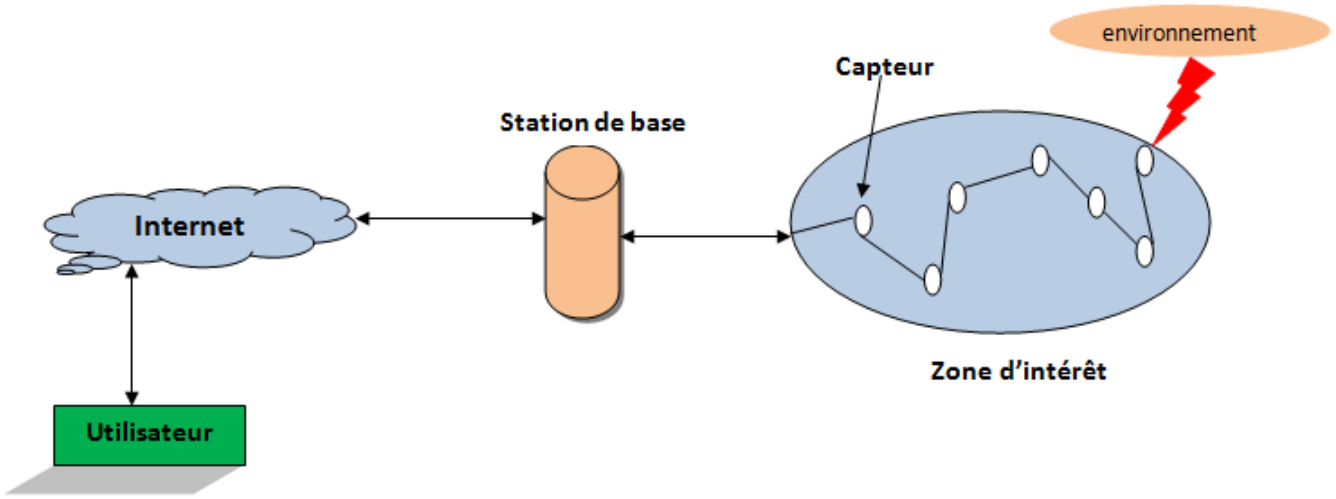


FIGURE 1.2 – Réseaux de capteurs sans fil[9].

1.2.3 Types de nœuds dans un RCSF

Les capteurs et les nœuds sans fil sont un appareil qui vous permet de surveiller et de diagnostiquer les systèmes, ils sont faciles à installer et à configurer, RCSF peut contenir différents types de nœuds [4].

1. **Un nœud régulier** : est un nœud avec une unité d'envoi et une unité de traitement de données. L'unité de transmission de données est responsable de toutes les transmissions et réceptions de données sur un support de communication sans fil qui peut être de type optique ou de type radiofréquence [4].
2. **Un nœud capteur** : est un nœud régulier équipé d'une unité d'acquisition ou de détection [4].
3. **Un nœud actionneur ou robot** : est un nœud doté d'une unité lui permettant d'exécuter certaines tâches spécifiques comme des tâches mécaniques (se déplacer, combattre un incendie, piloter un automate, etc.)[4].
4. **Un nœud puits** : est un nœud doté d'un convertisseur série connecté à une seconde unité de communication (GPRS, Wi-Fi, WiMax, etc.)[4].
5. **Un nœud passerelle** : est un nœud permettant de relayer le trafic dans le réseau sur le même canal de communication [4].

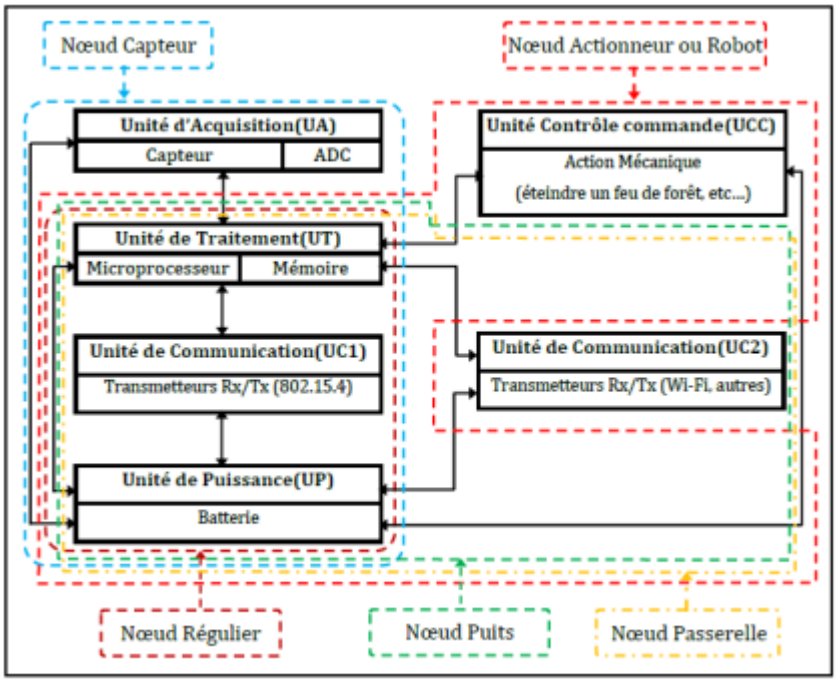


FIGURE 1.3 – Architecture des différents types de nœuds [4].

1.2.4 Structure d'un nœud de capteur sans fil

Le nœud de capteur sans fil est équipé de capteurs,d'émetteurs-récepteurs sans fil et de composants d'alimentation, comme le montre la (figure 4). Les nœuds uniques dans un réseau de capteurs sans fil sont de nature ressource, avec une vitesse de traitement, une capacité de stockage et une bande passante de communication limitées [3].

1. **Architecture matérielle**

   Nous avons 4 unité dans le nœud capteur composé de :

   (a) **L'unité d'acquisition (sensing unit)** : est généralement composée de deux sous-unités : les capteurs et les convertisseurs analogique-numérique ADCs1

   . Les capteurs obtiennent des mesures numériques sur les paramètres environnementaux et les transforment en signaux analogiques.

   . Les ADCs convertissent ces signaux analogiques en signaux numériques [3].

   (b) **L'unité de traitement (Processing unit)** : est une unité qui a le travail le plus important dans le nœud de détection qui traite les données capturées et les stocke dans la mémoire [3].

   (c) **L'unité de transmission (Transceiver unit)** : est responsable de toutes les émissions et réceptions des données via un support de communication radio. qui relie le nœud au réseau [3].

(d) **L'unité d'alimentation ou batterie (power unit)** : c'est une unité importante qui alimentait le nœud en énergie [3].

De plus, un nœud capteur peut être équipé d'autres composants supplémentaires tels qu'un système de localisation et mobilisateur .

2. **Architecture logicielle** :

La contrainte énergétique des capteurs exige l'utilisation de systèmes d'exploitation légers tels que TinyOS ou Contiki. Cependant, TinyOS reste toujours le plus utilisé et le plus populaire dans le domaine des RCSFs. Il est libre et est utilisé par une large communauté scientifique dans des simulations pour le développement et le test des algorithmes et des protocoles [4].

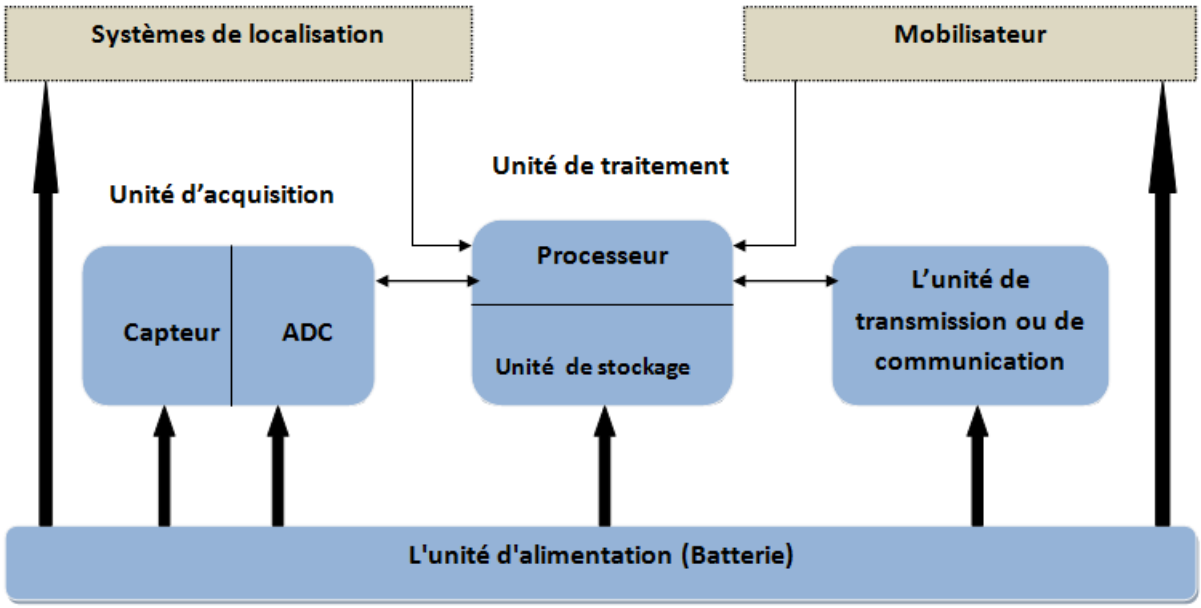


FIGURE 1.4 – composant des nœuds capteurs [3].

1.3 Caractéristiques du RCSF

il présente de nombreuses caractéristiques telles que la mobilité, la commutation de caractères et la capacité limitée de la batterie. Il a également quelques caractéristiques distinctives [5].

-Durée de vie du réseau : C'est l'intervalle de temps qui sépare l'instant de déploiement du réseau de l'instant où l'énergie du premier nœud s'épuise ou le dernier nœud ou un pourcentage de nœuds.Selon l'application, la durée de vie exigée pour un réseau peut varier entre quelques heures et plusieurs années [2][5].

-Bande passante limitée : Afin de minimiser l'énergie consommée lors de transfert de données entre les nœuds, les capteurs opèrent à bas débit. Typiquement, le débit utilisé est de quelques dizaines de Kb/s. Un débit de transmission réduit n'est pas handicapant pour un réseau de capteurs où les fréquences de transmission ne sont pas importantes [2][5].

-Média du transport : Dans un réseau de capteurs, la communication multi-sauts entre les nœuds est réalisée avec des liens sans fil à l'aide de media optique, infrarouge ou radio. La plus part des réseaux de capteurs utilisent des circuits de communication à radio fréquence grâce à leur faible coût ainsi que leur facilité d'installation [6].

-Topologie du réseau : Elle est en constante évolution à cause du changement de l'état d'activité des capteurs (actif, mise en veille et passif). Il faut que les capteurs soient capables d'adapter leur fonctionnement afin de maintenir la topologie souhaitée et assurer la couverture totale de la zone de déploiement [2][5].

-Déploiement : Les capteurs sont soit déployés manuellement quand leur nombre est petit soit de manière aléatoire lancés en masse depuis un avion, par exemple [5].

-Passage à l'échelle : La plupart des protocoles sont conçus pour des réseaux de capteurs de taille moyenne. Cependant, ces protocoles sont dits efficaces si les performances des réseaux ne doivent pas chuter d'une manière drastique quand le nombre de capteurs augmente dans le réseau [2][5].

-Consommation d'énergie : L'économie d'énergie est l'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 pour une durée maximale [2][5].

-Auto-configuration : Les capteurs sont généralement déployés aléatoirement dans des zones d'intérêt hostiles et en grand nombre. Par conséquent, aucune intervention humaine ne peut être requise pour assurer leur organisation.L'auto-configuration de ces réseaux s'avère nécessaire pour leur bon fonctionnement [2][5].

-Qualité de service : cette caractéristique est visée dans les réseaux de capteurs afin d'assurer la fiabilité de livraison des paquets entre les nœuds sources et réduire le délai de réception de ces paquets. Les protocoles doivent vérifier la stabilité du réseau ainsique les données redondantes transmises dans le réseau selon la répartition dutrafic [6].

-Mode de transmission : Il joue un rôle important dans les réseaux de capteurs. Les nœuds peuvent transmettre des données vers d'autres nœuds dans le réseau en utilisant uneseule fréquence ou bien plusieurs fréquences [2][5].

-Mobilité :la nœuds de détection peuvent être mobiles ou statiques, selon l'application [2][5].

-Scalabilité : Contrairement aux réseaux sans fil traditionnels (personnel, local ouétendu), un RCSF peut contenir un très grand nombre de nœuds capteurs (des centaines.desmilliers. . .). Un réseau de capteur est scalable parce qu'il a la faculté d'accepter un très grand nombre de nœuds qui collaborent ensemble afin d'atteindre un objectif commun [2][5].

-Tolérance aux pannes : Dans le cas de dysfonctionnement d'un nœud à cause de l'épuisement de son énergie par exemple, ou aussi en cas d'ajout denouveaux nœuds capteurs dans le réseau, ce nœud doit continuer à fonctionner normalementsans interruption. Ceci explique le fait qu'un RCSF n'adopte pas de topologie fixe mais plutôt dynamique [2][5].

-Densité importante des nœuds : Les RCSFs sont caractérisés par leur fortedensité. Cette densité peut atteindre, selon le type d'application, 20 nœuds/m3 surtout lorsqu'il s'agit de capteurs associés à des petits objets connectés [10].

-Collaboration entre les nœuds : Les contraintes strictes de consommationd'énergie mènent les nœuds capteurs à détecter et traiter les données d'une manièrecoopérative afin d'éviter le traitement redondant d'une même donnée observée, et qui aura un impact négatif sur la perte d'énergie [10].

1.4 Pile protocolaire dans les RCSF

Dans le but de créer un RCSF efficace, une architecture multicouche est adoptée afin d'améliorer la robustesse du réseau, un paquet de protocole à cinq couches est utilisé par les nœuds du réseau et trois plan de gestion [1].

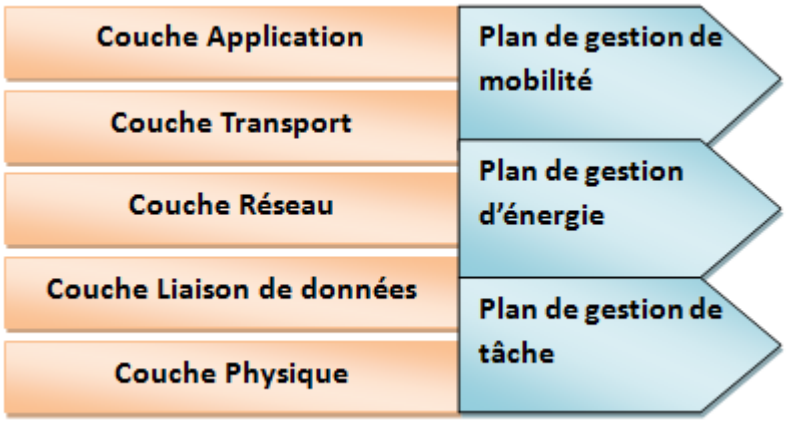


FIGURE 1.5 – Pile protocolaire dans les RCSF [26].

- Les rôles des couches :

- Couche physique : Matériels pour envoyer et recevoir les données.

• Couche liaison de données : Gestion des liaisons entre les nœuds et les stations de base, contrôle d'erreurs.

• Couche réseau : Routage et transmission des données.

• Couche transport : Transport des données, contrôle de flux.

• Couche application : Interface pour les applications au haut niveau.

• Plan de gestion d'énergie : Contrôle l'utilisation d'énergie.

• Plan de gestion de mobilité : Gestion des mouvements des nœuds.

• Plan de gestion de tâche : Balance les tâches entre les nœuds afin d'économiser de l'énergie.

1.5 Classification des applications des RCSF

Les applications des réseaux de capteurs sans fil peuvent être classées en quatre types d'applications :

1.5.1 Applications orientées temps

Cette catégorie représente les applications dans lesquelles l'acquisition et la transmission des données capturées sont temporelles : instant précis, période d'acquisition. Cette période d'acquisition peut être plus ou moins longue selon l'application. Ainsi, la quantité de données échangées dans le réseau dépend de la périodicité des mesures à effectuer sur l'environnement [8].

1.5.2 Applications orientées événements

Dans ce type d'application, les capteurs envoient des données à la station de base uniquement si un événement spécial se produit. On peut citer l'exemple de la surveillance des feux de forêt où le capteur envoie des alarmes à la station de base dès que la température dépasse une certaine limite [12].

1.5.3 Applications orientées requêtes

Dans ce cas, un capteur envoie de l'information uniquement suite à une demande explicite de la station de base. Cette classe d'applications est destinée aux applications adaptées à l'utilisateur. Ce dernier peut requérir des informations à partir de certaines régions dans le réseau ou interroger les capteurs pour acquérir des mesures bien particulières. Dans ce cas,

des connaissances sur la topologie du réseau et l'emplacement des capteurs sont nécessaires [24].

1.5.4 Applications hybrides

Ce type d'application met en œuvre tous les modes de fonctionnement. Dans un réseau conçu pour suivre des objets, le réseau peut se combiner entre un réseau de surveillance (pilotée par le temps) et un réseau de collecte de données piloté par les événements [24].

1.6 Domaines d'applications des RCSFs

Le RCSF est appliqué dans de nombreux domaines, qui sont actuellement soit au stade d'utilisation mature, soit encore aux premiers stades de développement. Ils sont classés selon la nature de leur utilisation en six catégories générales, comme le montre la figure [7].

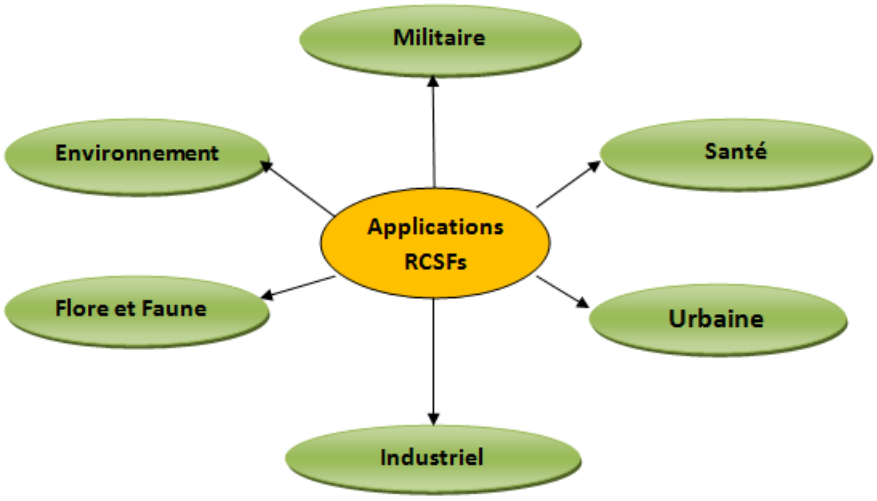


FIGURE 1.6 – Applications RCSF [7].

1.6.1 Applications militaires

Dans ce domaine, il stimule et améliore la recherche dans le WSN, par conséquent, dans le WSN militaire, le contrôle et la communication d'utilisation, la détection de l'état du soldat et autres [7].

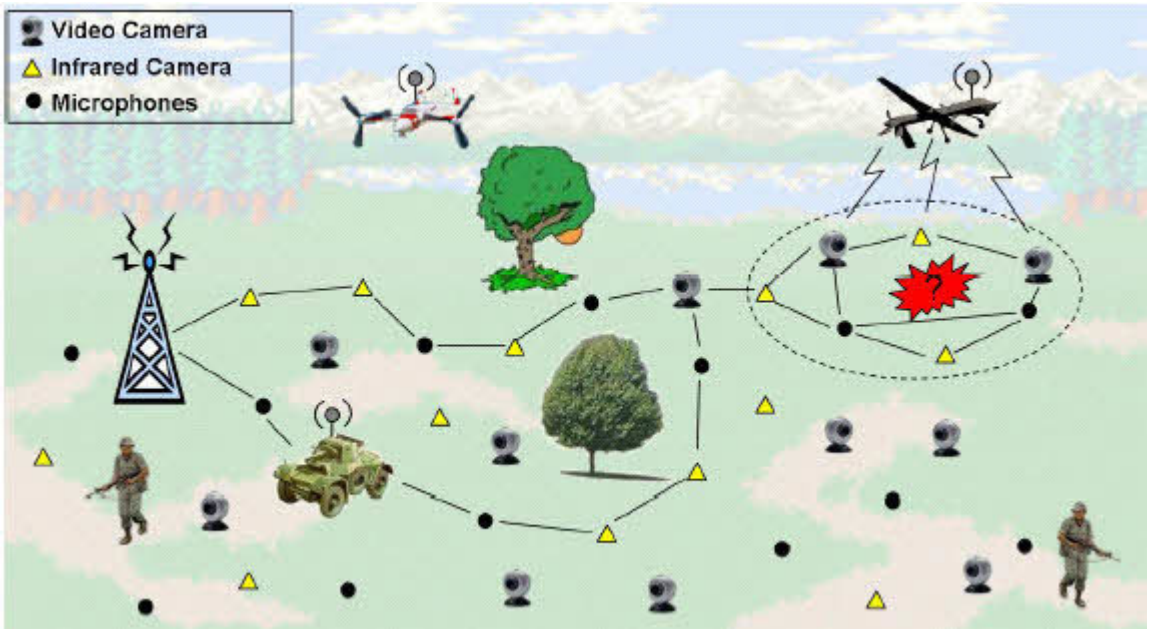


FIGURE 1.7 – Exemple d'application militaire dans RCSF .

1.6.2 Applications industrielles

Le RCSF peut être appliqué dans de nombreuses applications industrielles différentes pour aider à résoudre des problèmes connexes tels que les problèmes technologiques, les problèmes robotiques, la logistique et la santé des machines [7].

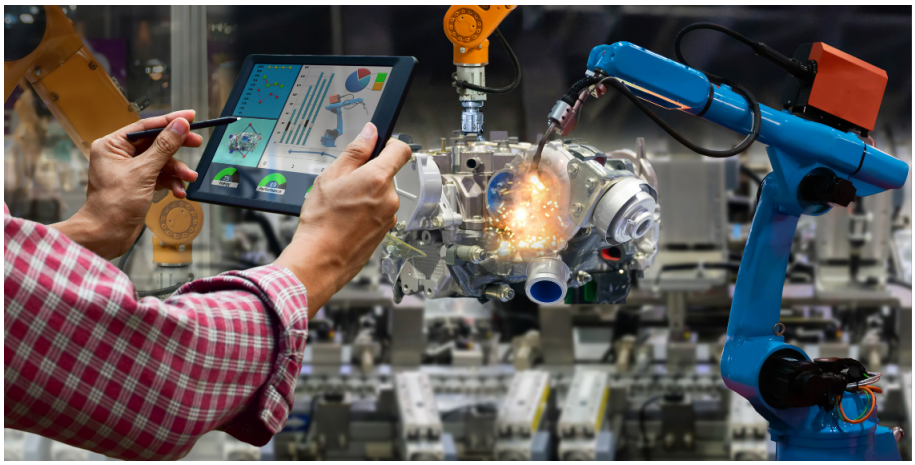


FIGURE 1.8 – Exemple d'application industrielles dans RCSF .

1.6.3 Demandes de santé

De nos jours, le système de santé est très complexe. Le système proposé est conçu pour fournir des solutions de soins de santé de bout en bout à l'aide de réseaux de capteurs sans fil [7].

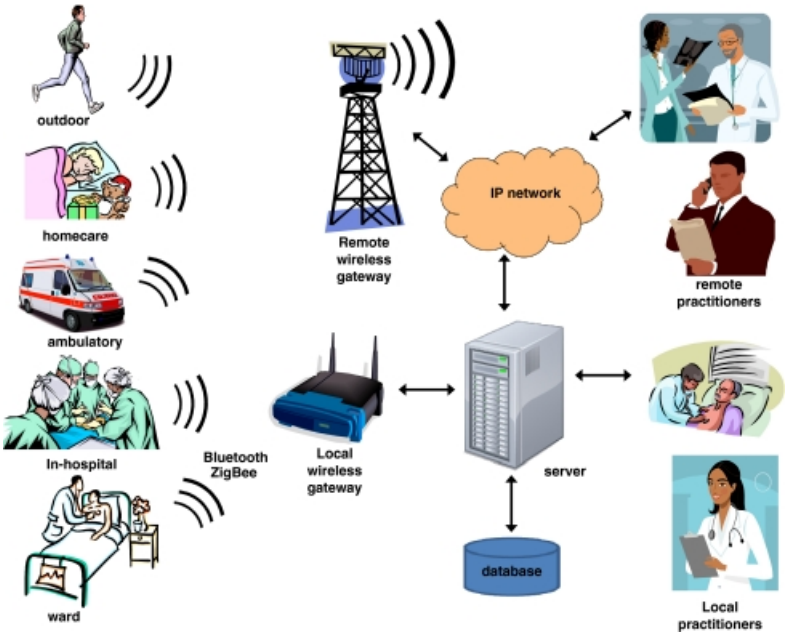


FIGURE 1.9 – Exemple Demandes de santé dans RCSF.

1.6.4 Applications au secteur agricole

La surveillance de l'humidité et de la température du sol est l'une des applications les plus importantes du RCSF en agriculture. Lors de la surveillance de l'environnement [7].

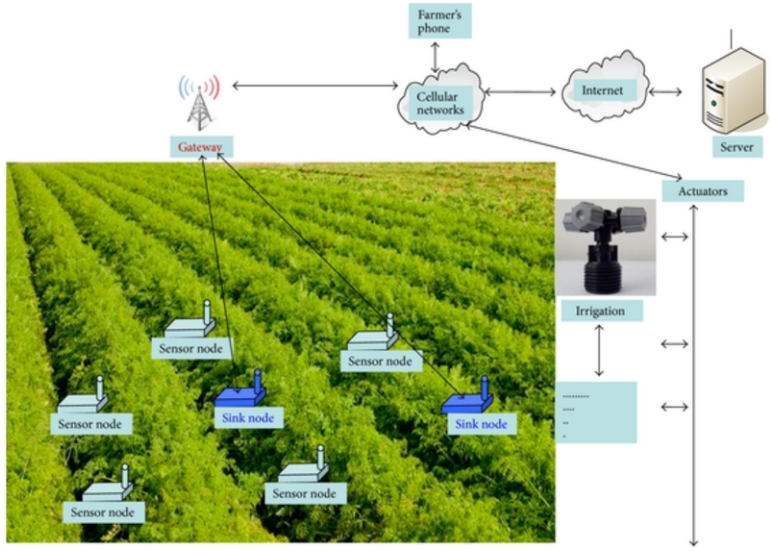


FIGURE 1.10 – Exemple Applications au secteur agricole dans RCSF.

1.6.5 Applications à domicile

Les capteurs peuvent être trouvés dans les appareils ménagers tels que les réfrigérateurs, les fours à micro-ondes, les aspirateurs, les systèmes de sécurité et également dans les systèmes de surveillance de l'eau [7].

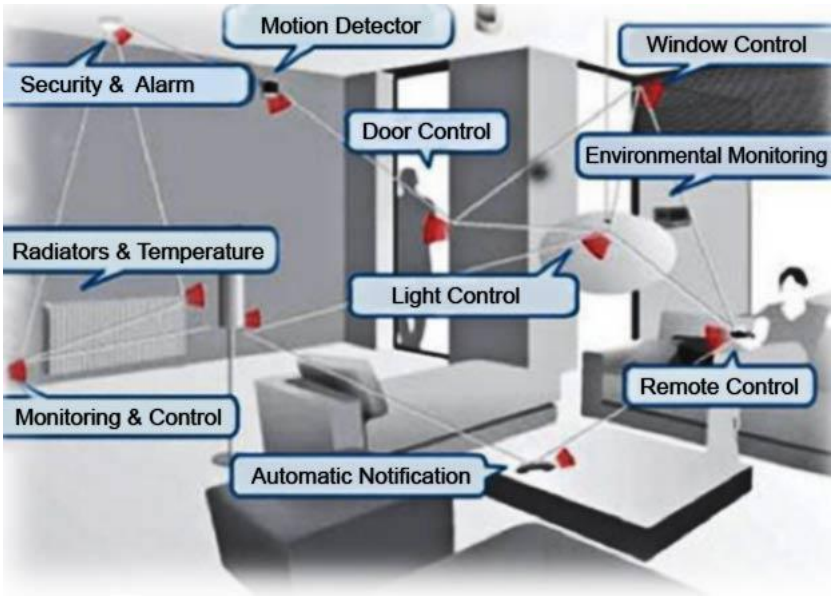


FIGURE 1.11 – Exemple Applications à domicile dans RCSF.

1.6.6 Applications environnementales

Application environnementale qui nécessite principalement une surveillance continue des conditions ambiantes dans des zones hostiles, difficiles et éloignées qui peuvent être améliorées par RCSF [7].

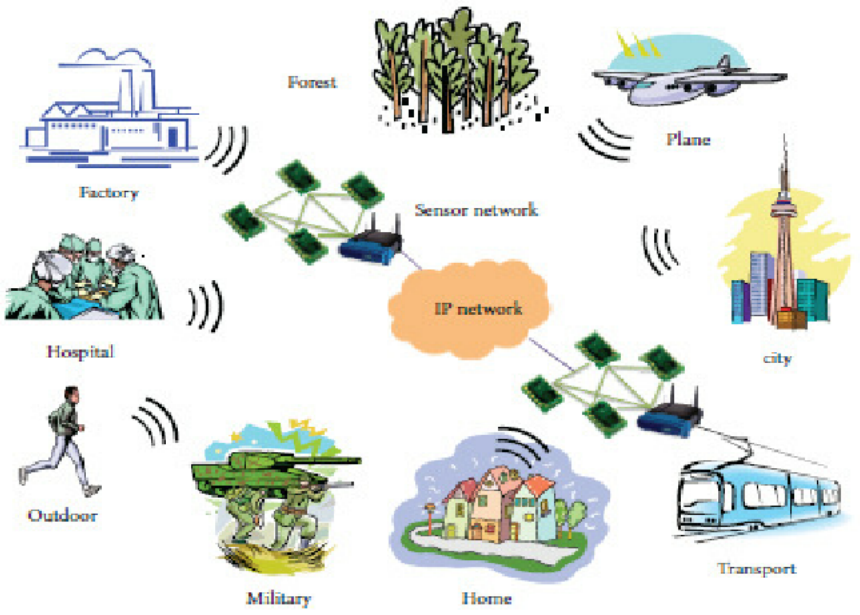


FIGURE 1.12 – Exemple Applications environnementales dans RCSF.

1.7 Modèles de communication dans RCSF

Nous avons deux modèles de communication dans RCSF qui sont :

1. **Modèle à un houblon** :

   C'est l'un des moyens les plus simples de déployer et de représenter une connexion directe, chaque nœud de notre réseau transmet des données directement à la station de base, ce type de connexion permet non seulement d'économiser de l'énergie, mais est également bon sur la côte, l'inconvénient est que les nœuds avoir une gamme limitée de connexions[8].

2. **Modèle multi-sauts** :

   Dans ce modèle, un nœud transmet des données, les données se déplacent par sauts d'un nœud à un autre [8].

1.8 Avantage / inconvénient du RCSF

RCSF a de nombreux avantages, et en même temps il a aussi des inconvénients, dans le tableau suivant, nous expliquons cela [7] :

Les avantage	Les inconvénient
1- Facilité de déploiement	1- Un risque de sécurité
2- Portée étendue du capteur	2- Fiabilité
3- Efficace dans les situations extrémes et les environnements hostiles	3- Vitesse inférieure
4- Tolérer l'erreur	4- Moins de controle
5- Précision améliorée et moins de frais	5- Détermination de la durée de vie de la batterie et des capacités de transmmission

TABLE 1.1 – Avantage / inconvénient du RCSF

1.9 Défis des RCSFs

Les principaux défis lancés par la communauté des chercheurs sont principalement liés aux problèmes le conception physique [28] :

- Conception des capteurs : Trouver de nouvelles conceptions adéquates et spécifiques pour des environnements donnés (détecteur de chute, capteurs multimédias ...).

- Protocoles de communication : Trouver de nouvelles paradigmes et protocoles de communication qui prennent en compte l'évitement de collisions, les vides,le routage des données.

- Passage à l'échelle :Afin d'assurer le bon fonctionnement du réseau, les nouveaux systèmes de déploiement doivent pouvoir fonctionner avec un grand nombre de nœuds.

- Sécurité : Dans les applications sensibles la sécurisation des données est nécessaire. D'où, il faudrait tenir compte des ressources limitées des capteurs pour proposer des solutions légères en termes de calcul et de stockage.

- Préservation de l'énergie et optimisation : Trouver de nouvelles visions d'optimisations.

- Conception du middleware : Dans la couche physique, la fiabilité de l'acquisition doit être augmentée. Au niveau de la direction, de nouveaux aspects de la direction sont développés avec un équilibrage de charge pour augmenter la durée de vie.

1.10 Consommation d'énergie en RCSFs

En ce moment, nous assistons au développement de technologies telles que la technologie RCSFs et, en même temps, nous avons un gros problème de limitations de puissance en termes de durée de vie limitée de la batterie. En effet, chaque nœud dépend de l'énergie pour faire son travail, et pour cette raison, cela devient une conséquence majeure dans RCSFs

que si un nœud tombe en panne, il peut interrompre le système dans son ensemble.L'énergie consommée par un nœud capteur est principalement due aux opérations suivantes : capture, traitement et communication des données [9].

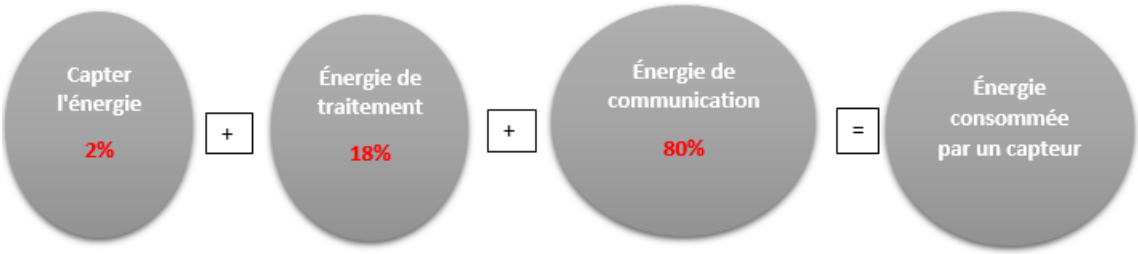


FIGURE 1.13 – Énergie consommée par un capteur dans RCSF [9].

1.11 Protocoles de routage dans RCSFs

Les données de tout réseau sont acheminées d'un nœud à un autre pour voyager de la source à la destination. Le chemin de routage doit être le plus court pour le haut débit du réseau . En général, le routage est divisé en un routage à plat, un routage hiérarchique et un routage basé sur l'emplacement sur la structure du réseau[11].routage hiérarchique et un routage basé sur l'emplacement sur la structure du réseau[11].

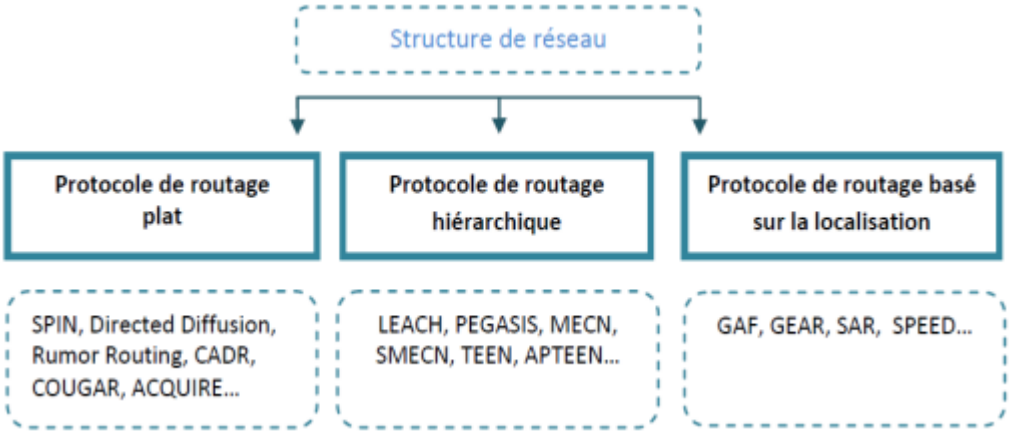


FIGURE 1.14 – Protocoles de routage dans la structure de réseau basée sur RCSF[29].

1.11.1 Routage à plat

Est un routage multi-sauts où tous les nœuds s'exécutent en même temps et au même moment. Et surtout, notre réseau est généralement assez grand et les nœuds sont affectés à la même tâche de détection. Alors. Étant donné que tous les nœuds transmettent des données,

la redondance entraînera certainement une consommation d'énergie élevée et importante. La station de base ou le récepteur peut demander des données dans la région afin que tous les nœuds de la région envoient des données après un événement. Et voici quelques schémas routage à plat[11] :

-SPIN

-GBR

-CADR

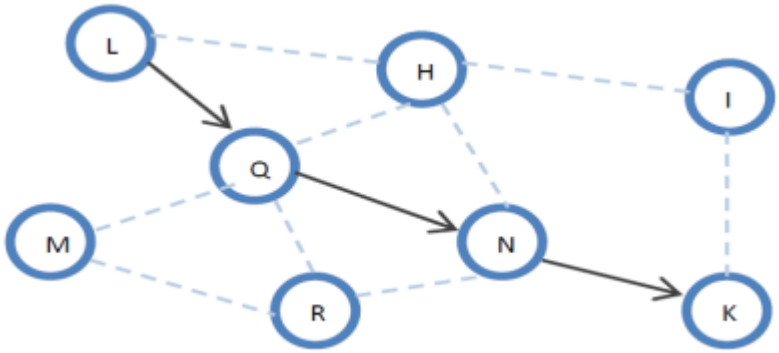


FIGURE 1.15 – Routage à plat [29].

1.11.2 Routage basé sur la localisation

l'emplacement des nœuds est connu grâce à un GPS de faible puissance sur chaque nœud. Ainsi, les nœuds sont des adresses par leur propre emplacement, mais tous les nœuds ne sont pas tenus de travailler ensemble. Ainsi, ils peuvent économiser de l'énergie et dormir pendant que d'autres sont sentir les événements. La distance entre les nœuds du capteur peut être détectée la force du signal reçu de ces nœuds[11] :

-SAR

-APS

-LAR

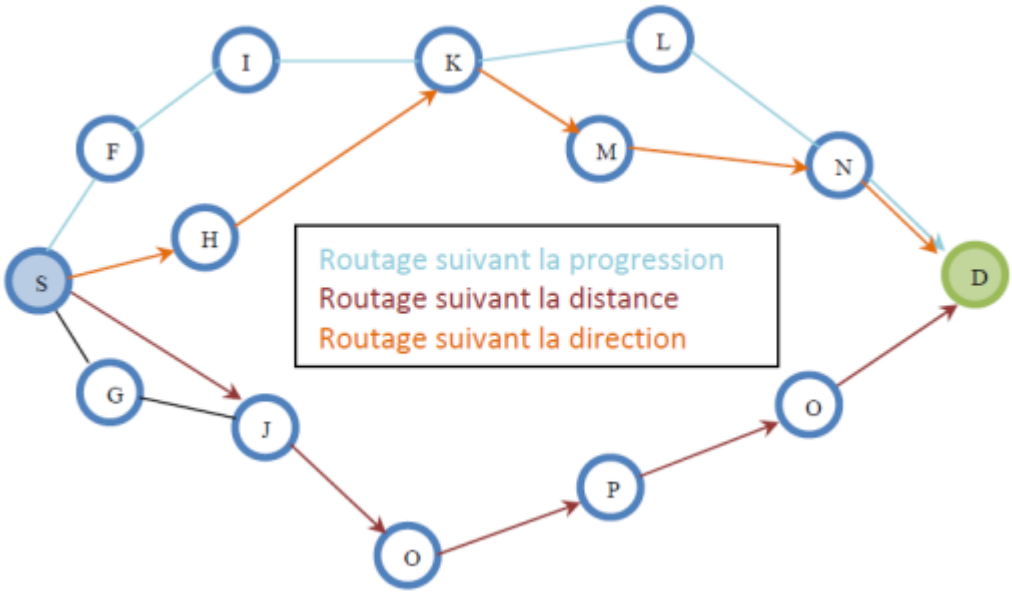


FIGURE 1.16 – Routage basé sur la localisation [29].

1.11.3 Routage de base hiérarchique

Dans le routage hiérarchique, les nœuds ne sont pas capables de communiquer à une très grande distance. Par conséquent, le routage hiérarchique basé sur des clusters devient une très bonne solution, l'importation de ce protocole est mis en œuvre par l'agrégation de données provoquant une diminution de l'énergie consommation, où les paquets sont envoyés au puits Et voici quelques-uns des routages hiérarchiques[11] :

-LEACH

-MECN

-PEGASIS

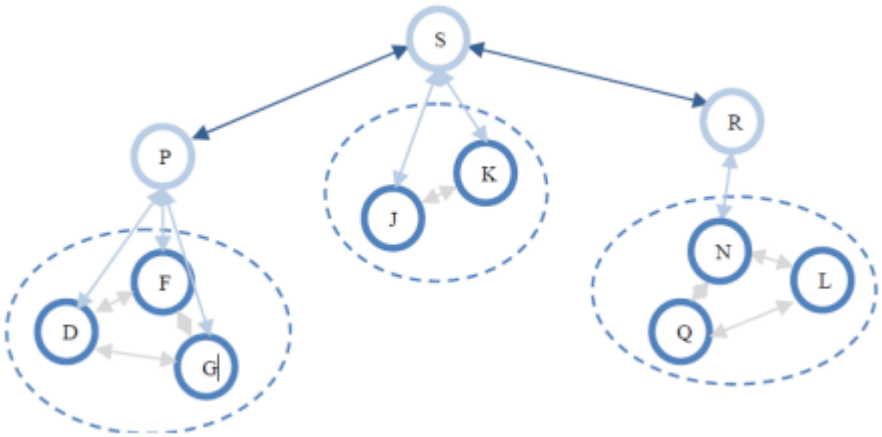


FIGURE 1.17 – Routage de base hiérarchique [29].

1.12 Conclusion

Dans ce chapitre, nous avons présenté en termes généraux les réseaux de capteurs sans fil, leur architecture, leurs principales limites de conception et leurs domaines d'application. Pour pouvoir mettre en œuvre ce réseaux de capteurs sans fil, la sécurité joue un rôle important, et l'un des aspects de cette dernière dans ce domaine est la gestion des clés. Dans le chapitre suivant, nous examinerons certains des protocoles proposés, affectant la gestion des clés dans RCSF, trouvés dans la littérature.

Chapitre 2

Etat de l'art sur la sécurité d'un système de gestion de clés pour RCSF

2.1 Introduction

De nos jours, la recherche est témoin de perturbations au niveau de la sécurité dans les RCSFs en raison des contraintes physiques des capteurs. Les RCSFs ont une capacité de traitement, mémoire, bande passante et batterie limitée. Par conséquent, il est nécessaire de personnaliser des mécanismes de sécurité qui prennent en considération les limitations de ressources dans ce genre de réseaux. De ce fait, les algorithmes de chiffrement sont un choix évident dans les réseaux de capteurs[12].

Ce chapitre présente une généralité sur les protocoles de routage sécurisé. Il se concentre particulièrement sur les travaux qui se basent sur la gestion des clés pour augmenter le niveau de la sécurité dans les RCSF avec une analyse comparative de ces travaux.

2.2 Aspect général de sécurité

La sécurité des ordinateurs est la protection des éléments auxquels vous accordez de la valeur [12].

La pertinence de la sécurité dans les réseaux de capteurs est étayée par de nombreuses menaces . En raison des canaux sans fil et les capacités limitées des noeuds capteurs, il peut être relativement facil pour l'adversaire de contrôler ou même prendre le contrôle du comportement d'un RCSF non protégé. Un réseau de capteurs doit être prêt pour prévenir ou minimiser l'effet de ces attaques en utilisant divers mécanismes possibles, tels que la communication sécurisée (canaux sécurisés, protocoles sécurisés : par exemple le routage, l'agrégation, synchronisation de l'heure) etc[13].

Les primitives de sécurité, telles que la cryptographie à clé symétrique et la cryptographie à clé publique, permet le construction d'une communication sécurisée entre deux ou plusieurs dispositifs, assurer la confidentialité, l'intergritét l'authentification.

2.2.1 Les Mesures de sécurité

Menaces Il s'agit d'ennemis capables de lancer une attaque exploitant une vulnérabilité. RCSF est utilisé dans un grand nombre d'applications avec des exigences de sécurité différentes. Ainsi, le protocole de sécurité de RCSF doit répondre à une ou plusieurs exigences de sécurité[15] :

L'authentification :

En gérant et en identifiant les participants, il permet une coopération sans risque au sein du RCSF. Il semble être un composant essentiel d'un réseau RCSF sécurisé. En effet, nous

ne pouvons pas garantir le secret et l'intégrité des communications que nous envoyons si nous ne sommes pas sûrs de communiquer avec le bon nœud dès le départ. Un attaquant peut rejoindre le réseau et insérer des messages erronés s'il est mal géré. L'utilisation d'un Message Authentication Code (CAM), ou MAC en anglais, assure à la fois l'authentification de l'origine du message et son intégrité. HMAC est un exemple de MAC. [25]

L'intégrité :

Il garantit que les données reçues n'ont été en aucune façon altérées lors de leur parcours sur le réseau, que ce soit intentionnellement ou non. Elle peut être assurée par l'utilisation de fonctions de hachage cryptographique, qui permettent d'attribuer à chaque message une empreinte numérique [25].

La confidentialité :

Compte tenu de la communication sans fil du RCSF, la confidentialité reste une priorité une fois les parties vérifiées. Il s'agit de garder secrets les messages échangés et de ne pas les révéler aux adversaires. L'utilisation de la cryptographie à clé symétrique ou asymétrique peut assurer la confidentialité [25].

La disponibilité : Il indique que le réseau est prêt à fournir des services et que les parties peuvent communiquer en cas de besoin. Compte tenu des limites des RCSF, cette caractéristique reste difficile à atteindre [25].

considérez les réseaux suivants :

- Topologie dynamique.
- Les ressources du nœud de transit sont limitées.
- Il est assez facile de brouiller ou d'altérer les communications sans fil.

Fraîcheur de données :

Ce dernier service assure que les données échangées sur le réseau sont à jour et non une réintroduction d'échanges passés interceptés par un attaquant [25].

2.2.2 Les mécanismes de sécurité

Plusieurs mécanismes ont été développés, qui reposent généralement sur le concept de cryptographie, c'est-à-dire l'étude de techniques mathématiques permettant de garantir certains services de sécurité. Il permet de convertir explicitement les informations en informations cryptées, puis à partir de ces informations cryptées, de restituer les informations d'origine [17].

1. **Les outils cryptographiques**

Il existe de nombreux outils de chiffrement, notamment :

(a) **Le chiffrement** : est le système de cryptage qui assure la confidentialité. Pour cela, il utilise des clés. Il est de deux types [17].

i. **Le chiffrement symétrique :**

La même clé est utilisée entre deux nœuds connectés pour chiffrer et Déchiffrement des données à l'aide d'un algorithme de chiffrement symétrique [17].

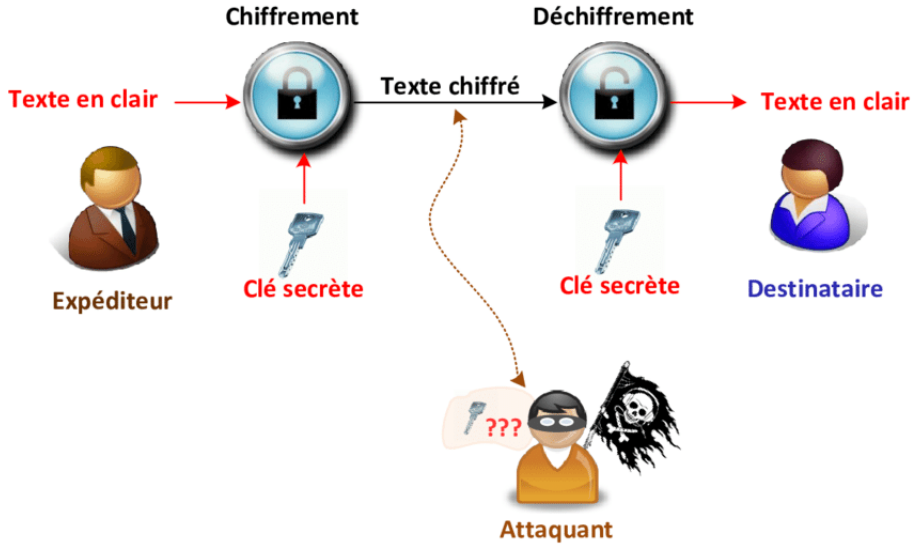


FIGURE 2.1 – Le chiffrement symétrique [14].

ii. **Le chiffrement asymétrique :**

Deux clés différentes sont générées par le récepteur : une clé publique qui est distribuée à tous les nœuds et qui sert à chiffrer les données qu'ils enverront au récepteur, et une clé privée qui est gardée secrète dans le récepteur et qui sert à déchiffrer ces données lorsque ce dernier les envoie. au récepteur.recevoir[17].

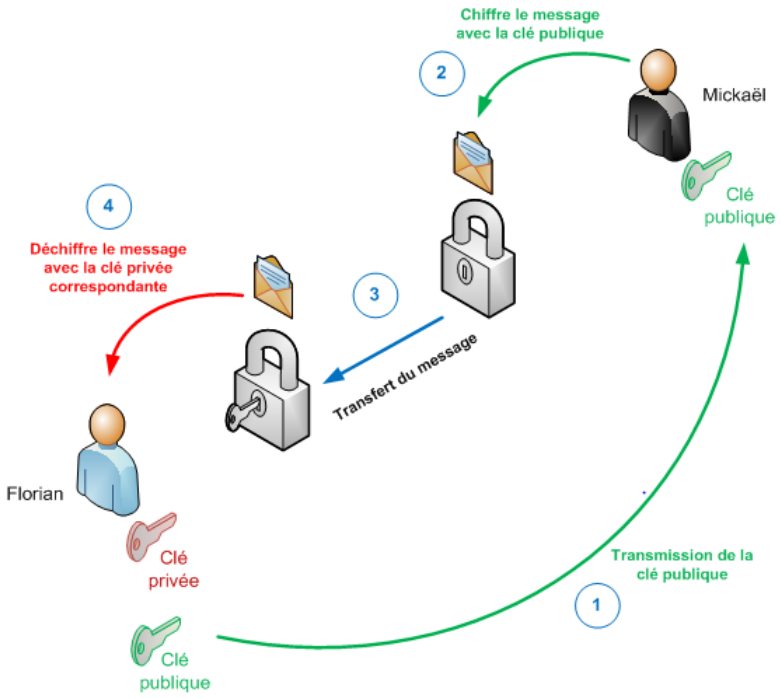


FIGURE 2.2 – Le chiffrement asymétrique[14].

(b) **La signature digitale**

La signature digitale est un système cryptographique assurant la non-répudiation de la source. Elle repose sur les clés asymétriques. L'émetteur (A) signe les données à transmettre avec sa clé privée (A) en produisant une signature digitale (1). Ce dernier est par la suite envoyé avec les données (2). Si elle peut être déchiffrée avec la clé publique (A) par le récepteur (B) et si son résultat est identique aux données reçues alors la signature est valide(4), c'est-à-dire, les données proviennent bien de leur émetteur légitime qui ne pourra pas nier l'émission de ces données dans le futur[17].

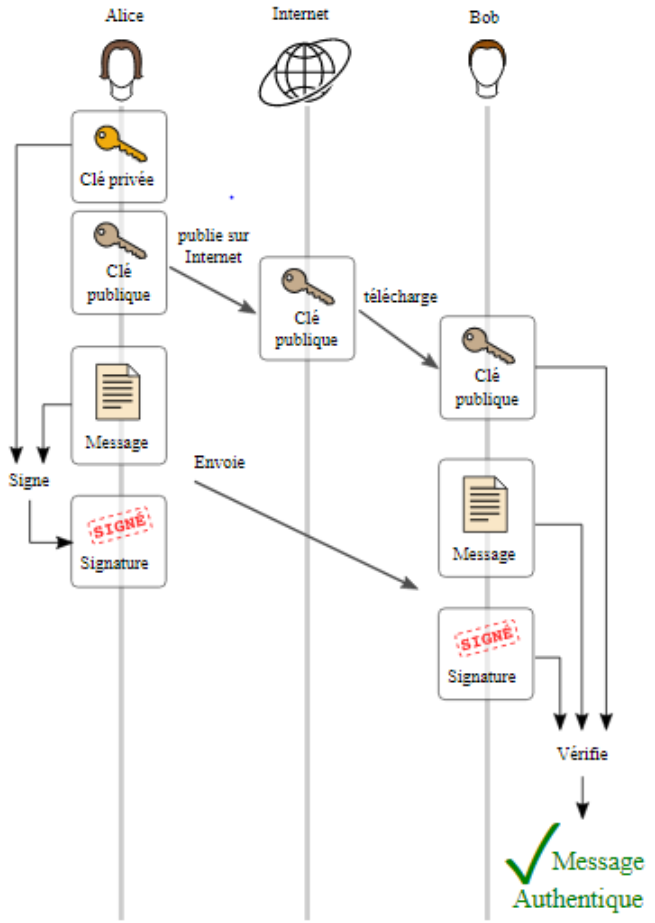


FIGURE 2.3 – La signature digitale.

(c) **La fonction de hachage**

La fonction de hachage consiste à pousser l'entrée d'une chaîne aléatoire dans une chaîne de longueur fixe. C'est l'un des outils de cryptage les plus importants, il fournit l'authenticité, les signatures numériques, la stéganographie numérique, etc[17].

FIGURE 2.4 – La fonction de hachage[14].

2.3 Sécurité dans le réseaux de capteurs sans fil

2.3.1 les contraintes

La conception du RCSF est affectée par plusieurs contraintes. Ces facteurs importants servent de lignes directrices pour le développement d'algorithmes et de protocoles utilisés dans les réseaux de capteurs [18].

Au niveau de la communication

- Perte de données à cause de la transmission radio
- La bande passante est limitée et partagée par tous les noeuds du réseau de capteurs.
- Interférences : ce réseau travaille sur une bande de fréquences non propriétaire .

Au niveau du matériel

- Puissance de calcul limitée : il fonctionne avec des registres 8 ou 16 bits, et les processeurs du réseau de capteurs diffèrent de ceux de la machine classique.
- Consommation d'énergie : les noeuds sont typiquement gérés par la durée de vie de leurs batteries , minimiser la consommation d'énergie est d'une importance primordiale afin de maximiser la durée de vie du RCSF [19].
- Mémoire limitée : 2 à 250 Ko de RAM et 1 à 32 Mo de mémoire flash.
- Environnement : les nœuds de capteur doivent être conçus pour répondre à des conditions environnementales difficiles (telles que chaleur élevée, pluie, humidité, etc.).

2.3.2 les vulnérabilités et attaques

Les vulnérabilités consistent en de nombreuses attaques, et la plupart des attaques sont similaires à celles qui sont appliquées dans les réseaux traditionnels.Le type d'attaque est de faire la distinction entre les attaques actives et les attaques passives [18] :

1. **Les attaques passives :**

   Les attaques passives reposent sur l'écoute et le partage d'analyse du trafic de données, ce qui a facilité l'investigation et difficile à détecter, composé de deux phases [20].

   (a) **Écoute clandestine :**

   c'est en interférant avec les données personnelles de quelqu'un, que l'attaquant apprend facilement la vulnérabilité de notre système [21].

(b) **Analyse du trafic :**

Il y a une forte probabilité que quelqu'un puisse analyser les schémas de communication dus à la transmission de messages dans des réseaux faibles [21].

(c) **Adversaires camouflés :**

C'est l'introduction de son nœud pour se cacher dans le réseau de capteurs. Ces nœuds peuvent ensuite être copiés comme un nœud normal pour attirer les paquets, puis détourner les paquets et effectuer une analyse de confidentialité [21].

2. **Les attaques actives :**

Les tentatives de modification ou de suppression d'un fichier dans le cadre du message entier peuvent introduire son trafic dans le réseau ou renvoyer d'anciens messages pour perturber le fonctionnement du réseau ou provoquer un déni de service. [22]

(a) **Node capture Attack :**

l'attaque s'appuie sur le contrôle total du capteur et extrait les informations de l'existant [18].

(b) **Attaque DOS :**

Le serveur est détruit en mettant du trafic sur la capacité du serveur afin de ré-exécuter des attaques DoS [21].

(c) **Attaque de chantage :**

Un nœud malveillant annonce qu'un autre nœud légitime a été infecté pour éliminer cette dernière forme dans le réseau. Un nœud attaquant permet de traiter un grand nombre de nœuds ; Cela peut perturber tout le processus [20].

(d) **Rejouer l'attaque :**

ce type d'attaque implique généralement le verrouillage passif d'une unité de données et sa retransmission ultérieure pour générer une attaque [21].

(e) **Transfert sélectif :**

Un nœud agit comme un routeur et affecte ses rôles, il peut refuser de transférer des messages et simplement les supprimer.

(f) **Attaque de trou de ver :**

C'est très dangereux pour notre réseau, dans lequel l'intrus enregistre le flux de paquets à un endroit très spécifique du réseau sans fil et l'envoie à un autre endroit [21].

(g) **Sybille Attaques :**

un dispositif malveillant qui prend illégalement plusieurs identités et utilise d'autres nœuds pour participer à des algorithmes distribués[21][20].

2.4 les protocoles sécurisé dans RCSF par la gestion des clés

L'utilisation de systèmes de gestion de clés économes en énergie qui garantissent la sécurité des RCSF est un défi pour les chercheurs en raison des contraintes de ressources auxquelles sont confrontés les nœuds de capteurs dans les RCSF. Dans cette partie, nous passerons en revue certains des principaux protocoles de gestion.

2.4.1 An Efficient and Hybrid Key Management for Heterogeneous Wireless sensor Networks

Ce protocole se compose de nœuds avec différentes capacités de puissance et est équipé de différents détecteurs qui collectent et transmettent différents modèles. La méthode choisit un modèle de réseau hiérarchique et hétérogène qui distingue [31] :

Station de base : les différentes informations collectées sont traitées à son niveau car elles sont suffisantes d'énergie.

Capteurs avancés : Équipés d'une puissance élevée, affichage Large bande passante, espace de stockage et capacité de calcul.

Capteurs basse fréquence : ils ont une capacité de puissance inférieure à celle des capteurs spéciaux Capteurs H.

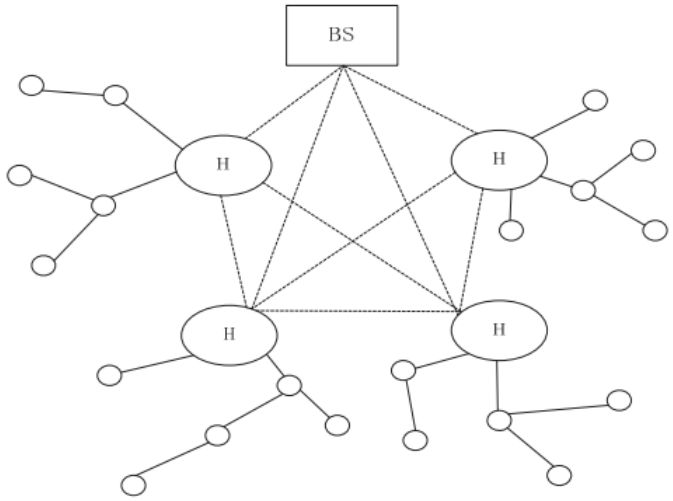


FIGURE 2.5 – Modèle d'architecture de gestion efficace et hybride des clés pour RCSF hétérogènes[31].

1. **Type de clés utilisées :**

   L'utilisation de clés symétriques pour créer des liens sécurisés est due à leur faible puissance. En effet, l'utilisation de commutateurs symétriques consomme moins d'énergie que celle de commutateurs asymétriques.

2. **Mise à jour des clés :**

   Après écoulement du temps T, les capteurs H génèrent un nouveau nombre aléatoire r', qui est alors supprimé.

   Si aucun nœud n'est capturé pendant la période T, le capteur calculera l'utilisation de la clé de bloc H avant de la diffuser aux autres nœuds du cluster.

   Si un nœud est capturé pendant la période T, alors K0 n'est plus fiable dans ce cas, le capteur H va générer r´ et l'encoder à l'aide des clés KHL avant de l'envoyer aux nœuds du groupe. Une fois sur place, les capteurs L fonctionnent.

2.4.2 Energy Efficient key Management Scheme for Wireless Sensor Networks

Ce système proposé se concentre sur la création et la maintenance de paires de clés entre des nœuds adjacents et le commutateur de réseau. Chaque nœud de capteur crée une clé de réseau et une paire de clés à l'aide de fonctions polynomiales. La fonction polynomiale est identifiée par l'identifiant. Pour augmenter la sécurité des messages dans le réseau lors de la phase d'initialisation, les nœuds utilisent leur clé unique. La station de base calcule les clés

individuelles de tous les nœuds à l'aide des clés et des identifiants uniques qu'elle a stockés [30].

1. **Type de clés utilisées :**

   Il existe trois clés partagés, un avec la station de base, un avec chaque nœud adjacent et un avec tous les nœuds du réseau. Où nous créons les clés, une clé unique, puis une paire de clés entre les nœuds adjacents et la clé de groupe.

2. **Mise à jour des clés :**

   En plus de la clé réseau, un délai est configuré pour recréer les paires de clés. Les clés ont été mises à jour à ce moment. Seul le paramètre de la fonction polynomiale est modifié dans cette procédure.

2.4.3 Large Scale Wireless Sensor Networks with Multi-Level Dynamic Key Management Scheme

Ce protocole prend en charge deux modèles de réseau bien connus pour les WSN : le modèle hiérarchique et modèle distribué. Son autorité de certification est la Mobile Authentication Authority (MCA)[32].

1. **Type de clés utilisées :**

   Il utilise deux clés asymétriques, chaque nœud stockant sa propre clé privée et la clé publique du MCA. Afin d'échanger des messages en toute sécurité entre les deux nœuds, ils doivent d'abord échanger leurs identités. Un nœud peut créer une clé partagée avec un nœud voisin selon le protocole

2. **Mise à jour des clé :**

   La mise à jour de la clé démarre lorsque le flux de messages atteint un certain seuil. Le processus de mise à jour peut également être effectué par les chefs de groupe. Lorsqu'un chef de cluster trouve un nœud non autorisé dans le réseau, il envoie un message de mise à jour à tous les nœuds du cluster, leur demandant de changer leurs clés partagées.Lorsqu'un nœud décide de mettre à jour une clé partagée, il redémarre la phase de découverte du voisin comme mentionné précédemment.

2.4.4 A Low Energy Key Management Protocol for Wireless Sensor Networks

LEKM est un modèle hiérarchique, le nombre de capteurs regroupés par un point d'intérêt. Il existe un nœud de commande responsable de la tâche du réseau qui est censé être sécurisé et

approuvé par tous les nœuds. Le concept comprend des portails, qui sont des super nœuds. Il a plus de mémoire et est équipé de processeurs hautes performances. Les capteurs sont divisés en différentes classes par des portes (clusters). La méthode de pré-distribution est utilisée dans le protocole de gestion de clé déterministe. Définit la manière dont les clés sont distribuées, ajoutées, révoquées et renouvelées pendant la durée de vie du réseau de capteurs[37].

1. **Types de clés utilisées :**

   Chaque nœud de capteur stocke deux clés secrètes. L'un est partagé avec la porte et l'autre est partagé avec le nœud pilote. Chaque porte stocke les clés qu'elle partage avec les capteurs de son groupe, et la clé est partagée avec le nœud de contrôle.

2. **Mise à jour des clé :**

   Comme dans le cas de la révocation, le nœud de contrôle produit de nouvelles clés et les pousse vers les portes pour terminer le renouvellement des clés du nœud capteur. Le temps entre les mises à jour ultérieures peut être affecté par le volume de trafic, la force des cœurs de chiffrement et la charge de traitement supplémentaire aux portes.

2.4.5 Light Weight Extensible Authentication Protocol

Le protocole LEAP pour les réseaux de capteurs sans fil est un mécanisme de gestion de clé déterministe. La technique de gestion des clés de LEAP permet un traitement en réseau tout en minimisant l'impact sur la sécurité d'un nœud compromis sur l'environnement immédiat du réseau. Les clés individuelles, les clés de paire, les clés de groupe et les clés qlobal font partie des quatre types de clés que LEAP fournit pour chaque nœud de capteur[31].

1. **Types de clés utilisées :**

   Il utilise quatre clés, une seule clé Chaque nœud possède une clé unique qu'il partage avec SB. Une clé paire est que chaque nœud partage une clé principale avec chacun de ses voisins immédiats. La clé de groupe est une clé partagée à l'échelle mondiale, utilisée par SB pour chiffrer les messages et les envoyer aux membres du groupe. La clé publique est partagée par un nœud avec tous ses voisins et est principalement utilisée pour sécuriser les messages diffusés.

2.4.6 Light Weight Polynomial-Based Key Management Protocol for Distributed Wireless Sensor Networks

LPKM est un système distribué de gestion de clés RCSF. Les nœuds capteurs peuvent créer un groupe et établir une clé partagée à l'aide de LPKM. Chaque nœud de capteur

peut avoir trois types de clés différents. Un mécanisme d'authentification de diffusion locale probabiliste est également inclus dans LPKM, qui fournit une authentification de source via la collaboration entre les nœuds environnants[40].

1. **Types de clés utilisées :**

   Trois types de commutateurs peuvent être générés pour chaque nœud de capteur. Partage d'une clé pour chaque paire avec un nœud adjacent à un saut. Une clé pour chaque paire est partagée avec un nœud multi-sauts non contigu. Une clé de groupe est partagée avec tous les nœuds du même groupe. Une clé de groupe partagée par l'ensemble du réseau.

2.4.7 Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks

VEBEK est un protocole de communication sécurisé qui crypte les informations à l'aide d'un mécanisme basé sur une clé RC4. La clé de l'encodeur du RC4 change dynamiquement en fonction de la quantité d'énergie restant dans le capteur. VEBEC se compose de trois parties : Module de génération de clé primaire L'encodeur et l'émetteur sont alimentés par défaut. Il peut également identifier et filtrer la désinformation que les opposants poussent dans le réseau [27].

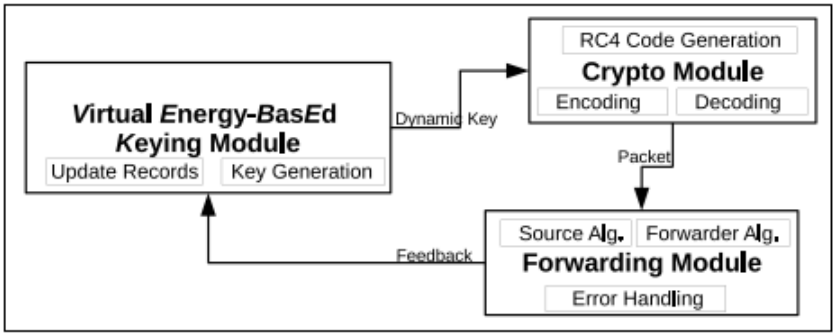


FIGURE 2.6 – Structure modulaire de VEBEK [27].

1. **Types de clés utilisées :**

   Ce protocole implique la génération de clés dynamiques, contrairement à d'autres systèmes de génération de clés, peu de messages sont échangés pour générer les clés. En fait, le nœud capteur calcule ses clés en utilisant La puissance virtuelle résiduelle, qui est la puissance dont dispose chaque nœud lorsqu'il se propage dans le réseau. Chaque action du nœud capteur vaut un certain coût énergétique, et donc sa diminution.

2. **Mise à jour des clés :**

   Dans VEBEK, une seule clé est utilisée à la fois pour un seul paquet, les prochains paquets seront codés et décodés par d'autres clés. En effet dans ce protocole les clés sont calculées à partir de l'énérgie virtuelle de laquelle disposent les noeuds capteurs. Après chaque action (envoi ou reception d'informations), cette énérgie est décrémentée, et c'est à partir de cette nouvelle valeur qu'une nouvelle clé est produite et calculée.

2.4.8 An Efficient Identity-Based Key Management Scheme for Wireless Sensors Networks using the Bloom Filter

IBKM est un modèle de réseau hiérarchique, et il a trois différents types d'appareils sans fil : Station de base , masse de tête et nœud de capteur, IBKM se compose de trois étapes : initialisation des paramètres, enregistrement du fichier de nœud et génération et partage de la clé secrète entre deux nœuds [36].

1. **Types de clés utilisées :**

   IBKM se compose de trois phases : initialisation des paramètres, enregistrement du nœud et partage de la clé secrète génération entre deux nœuds.

2.4.9 Schéma aléatoire de pré-distribution de clés de L.Eschenauer et D.Gligor

Eschenauer et Gligor ont présenté une technique de gestion de clés basée sur la probabilité que les nœuds d'un graphe aléatoire partagent une clé. La prédistribution des clés, la découverte des clés partagées, l'établissement du chemin des clés et la révocation des clés sont toutes couvertes. L'idée essentielle derrière cette technique est de distribuer un nombre fini de clés à chaque nœud du réseau au hasard avant qu'il ne soit déployé. Si deux nœuds partagent une clé partagée, ils pourront s'envoyer des communications sécurisées[39].

1. **Types de clés utilisées :**

   Un grand ensemble de clés est généré pour chaque nœud. Les clés sont choisies au hasard dans l'ensemble et ces clés sont stockées dans la mémoire du nœud et forment le jeu de clés du nœud.

2. **Mise à jour des clés :**

   C'est la même chose que le nœud effectuant lui-même une révocation de clé. Le nœud impacté effectue une phase de découverte de clé partagée et éventuellement une phase

d'établissement de chemin de clé pour restaurer le lien rompu après la suppression de la clé révoquée.

2.4.10 Virtual Location-Based Key Management Scheme for Wireless Sensor Networks

VLKM est un protocole de gestion de clés basé sur la localisation virtuelle, qui sera utilisée pour la génération de clés pour chaque tour [29].

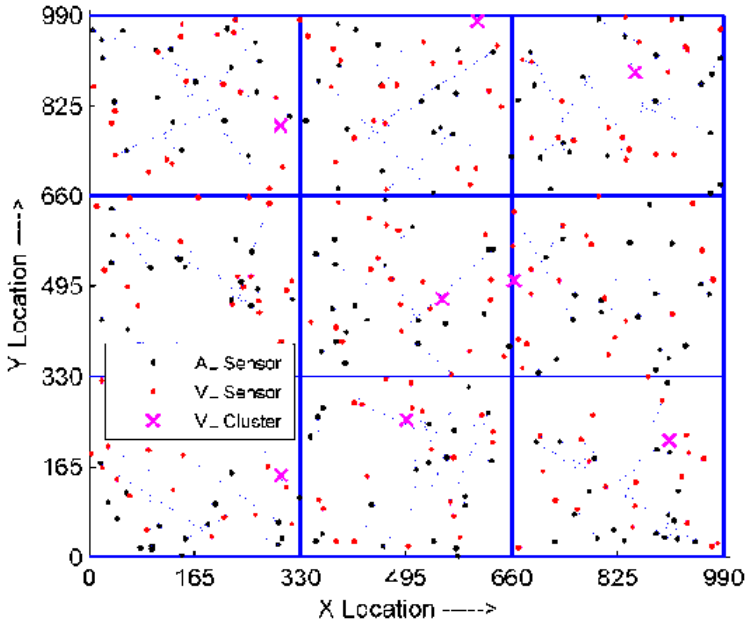


FIGURE 2.7 – Déploiement aléatoire des noeuds et localisation virtuelle [29]

1. **Types de clés utilisées :**

   Il utilise deux clés : clé de cluster Il s'agit d'une clé partagée par tous les nœuds d'un même cluster, également connue de la station de base. Cette touche est utilisée lors de l'appel Nœuds avec le cluster head du même groupe Le commutateur du capteur Cette clé est partagée entre le nœud du capteur et la station de base. Le chef de cluster utilise cette clé pour communiquer avec la station de base.

2. **Mise à jour des clés :**

   Les clés sont mises à jour en fonction du changement de l'emplacement virtuel, que ce soit pour les clusters ou les nœuds. Autrement dit, si un nœud veut changer sa clé, il effectue un mouvement virtuel, modifiant son emplacement actuel et produisant une nouvelle clé.

2.5 Etude comparative entre les traveaux

Protocoles	Cout de communication	Espace mémoire	Cout de calcul	Prédistribution de clés
Energy Efficient Key Management Scheme	Moyen	Faible	Faible	Oui
LPKM	Moyen	Moyen	Elevé	Non
LEAP	Moyen	Moyen	Moyen	Oui
LEKM	Moyen	Moyen	Moyen	Oui
Large Scale WSN with Mlti-level Dynamic KMS	Elevé	Elevé	Moyen	Non
EHKM	Moyen	Elevé	Moyen	Oui
IBKM	Elevé	Moyen	Elevé	Non
VEBEK	Faible	Faible	Elevé	Non
L.E et D.G	Moyen	Elevé	Faible	Non
VLKM	Faible	Faible	Elevé	Non

TABLE 2.1 – Etude comparative entre les traveaux

Selon les résultats de l'étude, qui sont présentés dans le tableau ci-dessus, les principales procédures de gestion basées sur une approche de pré-distribution sont les plus adaptées au RCSF en raison de leur faible coût. A l'exception des protocoles avec un grand nombre de commutateurs, tels que EHKM et LE/DG, leur coût de connexion est moyen et le moins coûteux en espace mémoire. A l'exception de VEBEK, qui calcule des clés à partir de propriétés virtuelles telles que la puissance résiduelle ou la localisation, les protocoles sans pré-allocation ont un coût de transfert élevé et sont très coûteux en termes d'espace mémoire.

2.6 Conclusion

La sécurité dans les réseaux de capteurs reste toujours un problème persistant. Afin de résoudre ce problème, plusieurs chercheurs ont adoptés l'intégration des algorithmes de cryptage pour augmenter le niveau de la sécurité dans les RCSF. Dans ce chapitre, nous avons passé en revue les principaux travaux dans ce contexte avec une comparaison entre

eux.

Dans le chapitre suivant, nous entamons le développement de notre solution de gestion de clé pour les RCSFS.

Chapitre 3

Conception d'un modèle sécurisé pour les réseaux de capteurs

3.1 Introduction

Le contexte de notre étude est consacrée à augmenter la sécurité des réseaux de capteurs on prenant en considération la contrainte d'énergie. Le présent travail se concentre plus particulièrement sur la résolution d'un système de gestion de clés pour les RCSFs.

Dans la majorité des études proposées pour résoudre les problèmes de sécurité dans les RCSFs, l'énergie est le facteur essentiel qui prit en compte. Réaliser un protocole sécurisé sans trop affecter la durée de vie du réseau c'est un grand défi !

Pour cette raison, nous proposons un nouveau protocole sécurisé RA-LEACH (RSA-AES -Low-Energy Adaptive Clustering Hierarchy) comme une version sécurisée du protocole LEACH. Nous avons choisi le protocole LEACH en raison de ses performances en termes d'énergie par rapport à d'autres protocolesde routage.

Notre proposition ajouter au LEACH l'aspect de sécurité où elle combine à la fois l'utilisation des deux algorithmes de cryptage RSA et AES. On commence, par l'application du cryptage asymétrique par RSA pour assurer l'identité des nœuds capteurs. On suite, par l'application du cryptage symétrique par AES pour chiffrer les données.

Notre nouvelle méthode permet d'améliorer les solutions de sécurité sans trop affecter la durée de vie du réseau.

3.2 Description globale de RA-LEACH

La structure de notre modèle est représentée par la figure 3.1, qui comprend les cinq étapes suivantes :

- Étape 0 : Génération de clés et l'implémentation du protocole LEACH

Dans cette étape, la station de base, génère et distribuer les clés AES et RSA au niveau des nœuds capteurs avant leur déploiement. ET on génère aussi l'implémentation du protocole de routage LEACH ; où en déterminent les clusters avec ses chefs.

- Étape 1 : Assurer l'identité

Dans cette étape, lorsque les nœuds détectent des informations, les identités des nœuds sont chiffrées par l'algorithme RSA et les envoyer à leur chef correspond.

- Étape 2 : Validation de l'identité du nœud

Après la réception des identifiants, les chefs des groupes doit vérifier les identifiants chiffrés reçu s'il existe dans sa base de données ou bien non.

- Étape 3 : Transmission des données

Après la validation d'identité des nœuds par leur chef, les donner son envoyées par les nœuds aux chefs correspond.

- Étape 4 :Cryptage et l'envoi des données avec AES

A ce stade, le chef de groupe est crypté les données à l'aide de l'algorithme AES et les envoyer à la station de base.

- Étape 5 : Réception des données

Une fois que la station de base reçoit les données chiffrées, il les déchiffrera et les enregistrera.

Chacune de ces étapes est répétée pour chaque région.

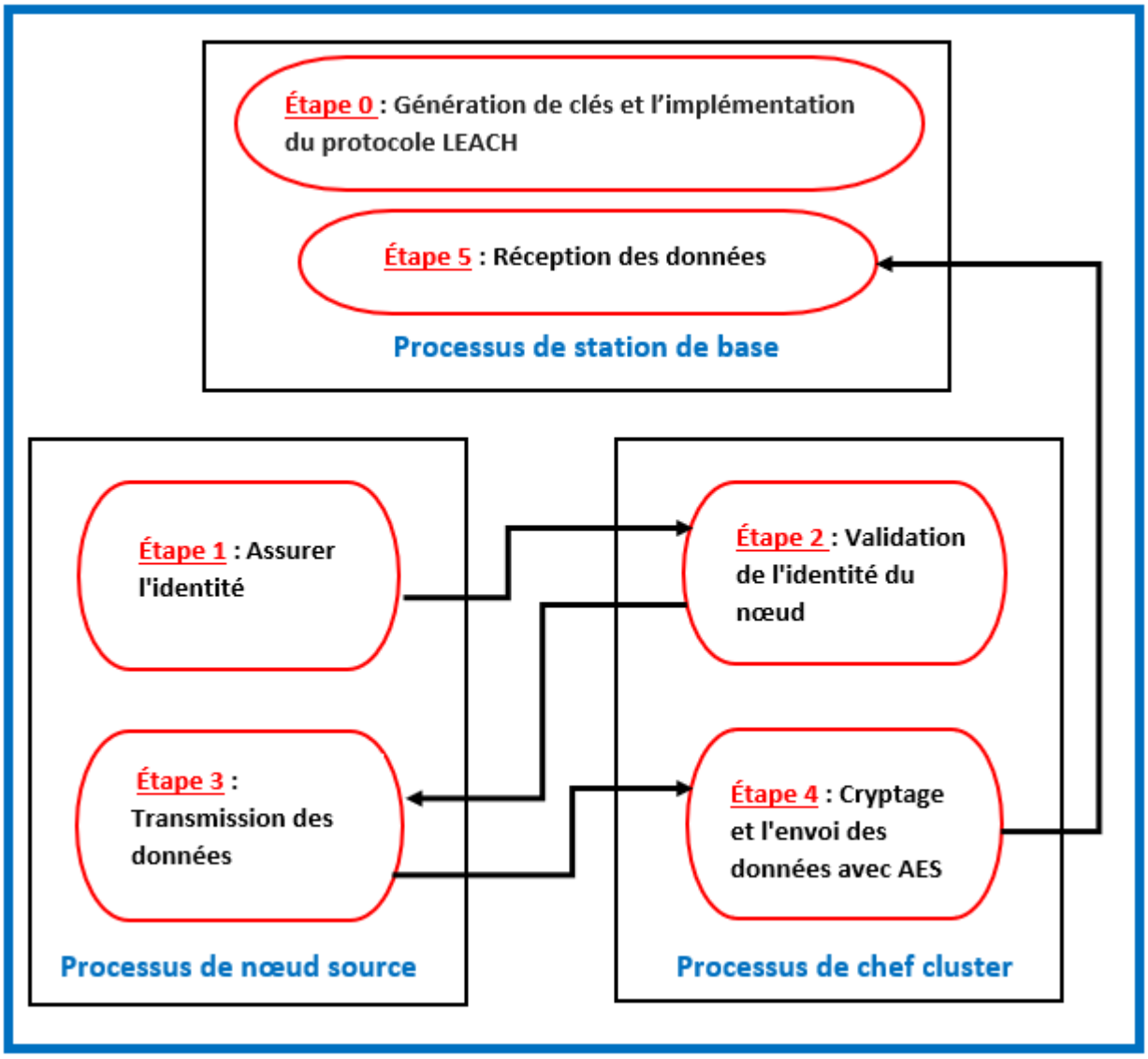


FIGURE 3.1 – Description globale de RA-LEACH.

3.3 Description détaillée de RA-LEACH

Dans cette section, nous allons approfondir les étapes mentionner ci-dessus de la stratégie proposée.

3.3.1 Génération de clés et l'implémentation du protocole LEACH

3.3.1.1 Génération des clés

Dans cette étape, les clés de pré-distribution sont générées, c'est-à-dire avant le déploiement des nœuds.

Nous utilisons un cryptage symétrique et asymétrique Nous avons d'abord AES est un algorithme de chiffrement par bloc, pour le chiffrement symétrique, nous installons la clé symétrique tout au long de la simulation, une clé est générée de sorte que la longueur de la clé soit de 4 et les données sont placées au niveau du bloc du niveau du bloc 4 * 4 et les données sont cryptées au niveau du bloc de 128 bits.

En ce qui concerne la génération de clés RSA dans le chiffrement asymétrique, les étapes suivantes sont suivies

- générer les clés RSA :

cette étape est très simple et consiste en une méthode simple qui générera la clé privée pour la méthode de chiffrement RSA. Pour créer ces clés, nous devons suivre ces cinq étapes :

1. Sélectionnez deux grands nombres premiers p et q. Les nombres premiers doivent être grands pour qu'ils soient difficiles à comprendre pour quelqu'un
2. La deuxième étape consiste à calculer n, et $n = p \times q$
3. La troisième étape consiste à calculer la fonction totient : Q(n)=$(p-1)(q-1)$.
4. On sélectionne maintenant un entier a, tel que e est premier avec Q(n) et $1 < e < Q(n)$. le couple de nombres (n, e) constitue la clé publique
5. Dans la dernière étape on calcule d tel que e.d = 1 mod Q(n). d peut être trouvé en utilisant l'algorithme d'Euclide étendu. Le couple (n, d) constitue la clé privée.

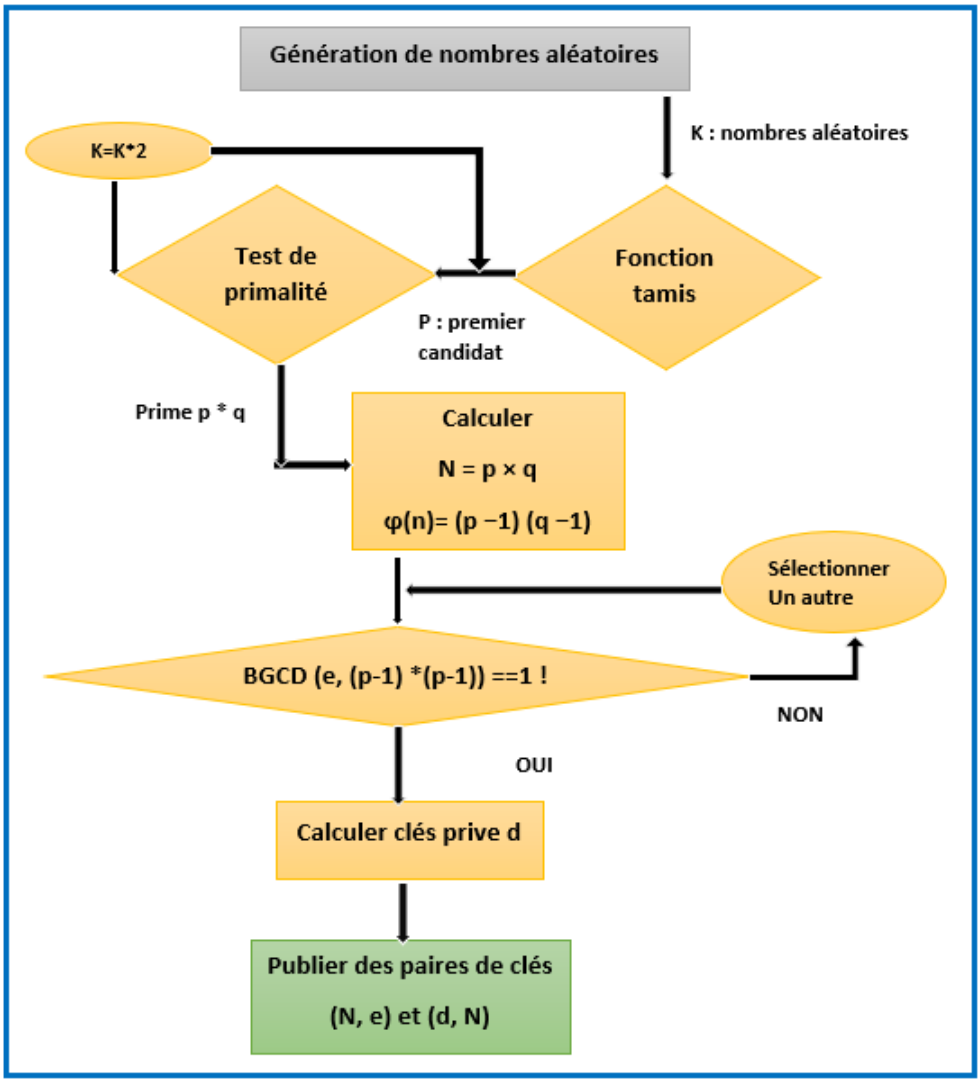


FIGURE 3.2 – Génération de paire de clés RSA.

3.3.1.2 Implémentation du protocole LEACH :

LEACH (Low-Energy Adaptive Clustering Hierarchy) est un protocole de routage hiérarchique, utilisant un processus de clustering qui divise le réseau en deux niveaux : les têtes de cluster et les nœuds membres. Le protocole se déroule en rondes. Chaque manche se compose de deux phases : la construction et la communication [40].

1. **Phase de construction :**

   Le but de cette phase est de construire les clusters en choisissant les leaders et en établissant la politique d'accès aux médias au sein de chaque groupe. Cette phase commence par la prise de décision locale pour devenir cluster-head. Chaque nœud n choisit un nombre aléatoire, si ce nombre est inférieur à une valeur T(n), le nœud devient cluster-head. T (n) est défini comme suit [40] :

$$T(n)=\begin{cases}\dfrac{P}{1-P*(r \bmod \frac{1}{P})} & \text{Si } n \in G \\ 0 & \text{Sinon}\end{cases}$$

avec :

P : pourcentage désiré de cluster-heads pendant un round.

r : numéro du round.

G : Nœuds de groupe pour lesquels aucun chef de groupe n'a été élu lors des tours 1/P précédents. L'en-tête du bloc avec le signal le plus fort (c'est-à-dire le plus proche) est choisi. En cas d'égalité, un chef au hasard est choisi. La méthode CSMA doit être utilisée pour toutes les connexions antérieures réalisées dans une structure plate. Ensuite, les communications à l'intérieur du bloc peuvent être effectuées en utilisant la méthode TDMA [40].

2. **Phase de communication :**

   Avec la méthode TDMA, les membres envoient leurs données capturées sur leurs propres créneaux horaires. Cela leur permet d'éteindre leur interface de communication en dehors des créneaux réservés, afin d'économiser de l'énergie. Ces informations sont ensuite collectées, pour être envoyées au collecteur (aquarium). Cette communication, entre le cluster header et le collecteur, se fait de manière directe, c'est-à-dire que le cluster head adapte son émetteur radio afin d'atteindre directement le collecteur.

3.3.2 Assurer l'identité

Dans cette étape, le nœud source chiffre l'identifiant avec RSA, l'identifiant chiffré C est calculé comme suit :C = P^emod n. Nous chiffrons l'identifiant une seule fois.

Après avoir crypté l'identifiant, nous l'envoyons a chef de cluster pour confirmer son identité.

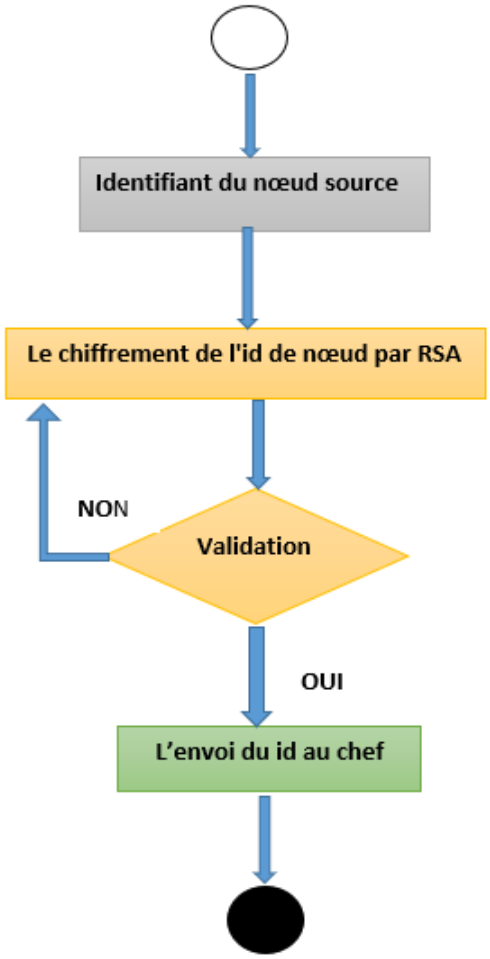


FIGURE 3.3 – Assurer l'identité

3.3.3 Validation de l'identité du nœud

Cette étape est réalisée après avoir reçu l'identifiant chiffré des nœuds sources, le chef de cluster déchiffre l'identifiant par RSA, Comme suit : P $=C^e$mod n. Ensuite, le chef de cluster vérifie si l'identifiant existe dans la base de données ou non. S'il est présent, le chef de groupe répond avec approbation, sinon annule.

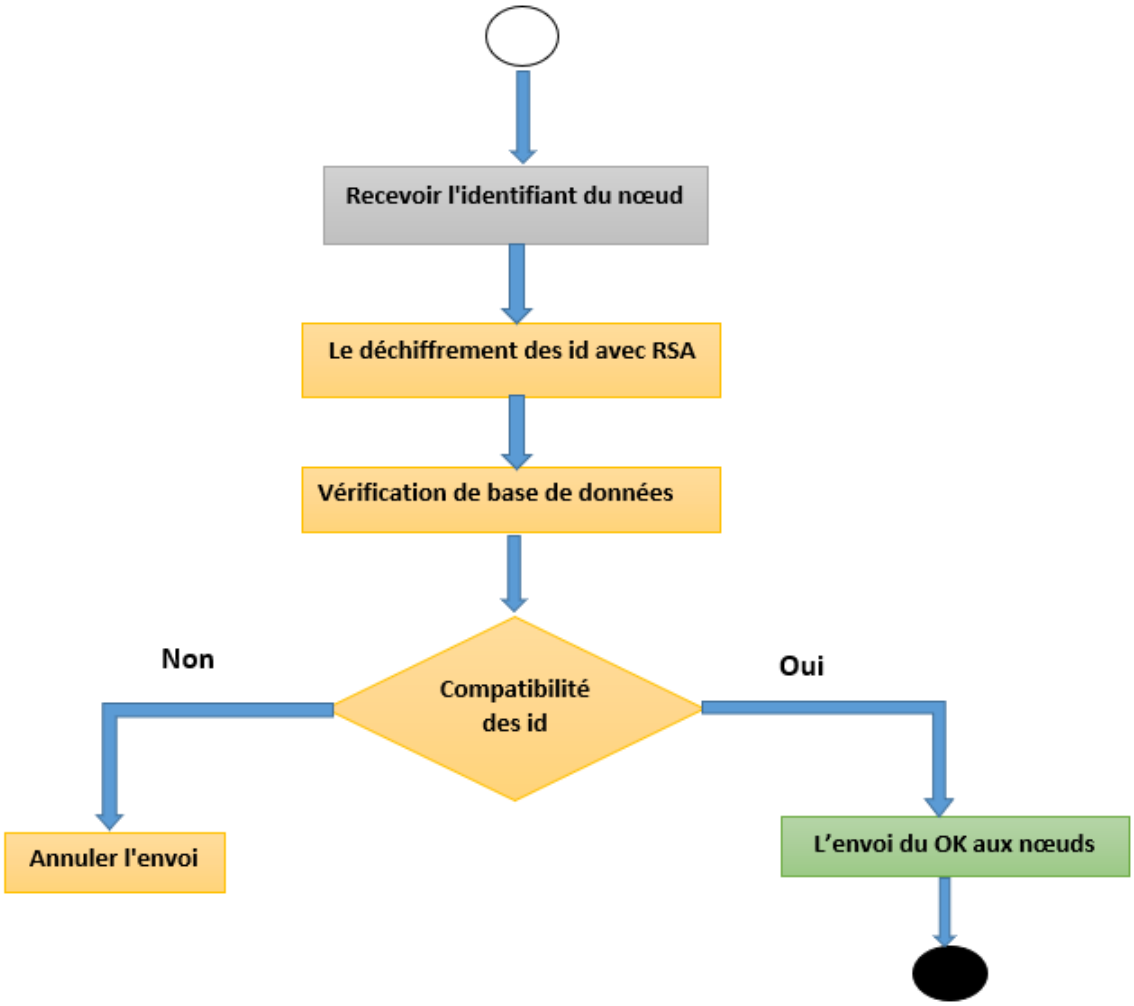


FIGURE 3.4 – Validation de l'identité du nœud.

3.3.4 Transmission des données

À ce stade, l'acceptation est reçue du chef de groupe. Ensuite, le nœud source valide le consentement et envoie les données au chef de groupe.

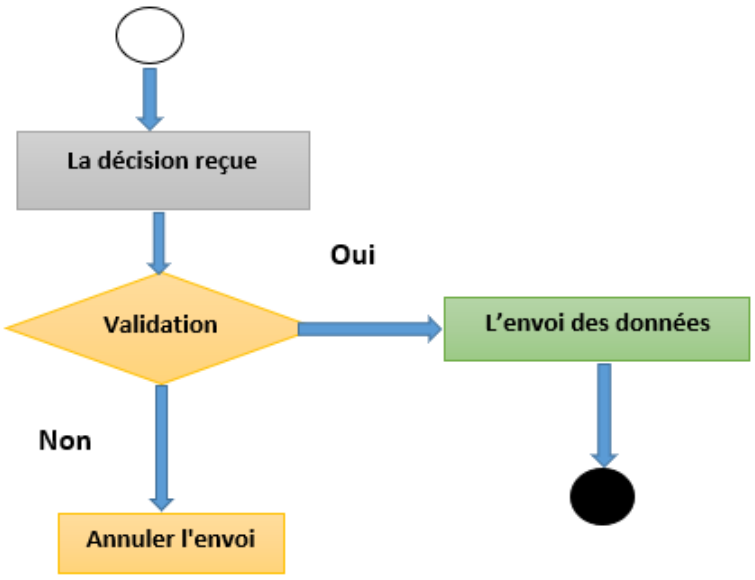


FIGURE 3.5 – Transmission des données.

3.3.5 Cryptage et l'envoi des données avec AES

À ce stade, après avoir reçu les données des nœuds sources, le chef de groupe collecte et organise les informations. Le chef de groupe crypte les données avec l'algorithme AES, qui utilise une seule clé symétrique, après quoi le chef envoie les données cryptées à la base. station.

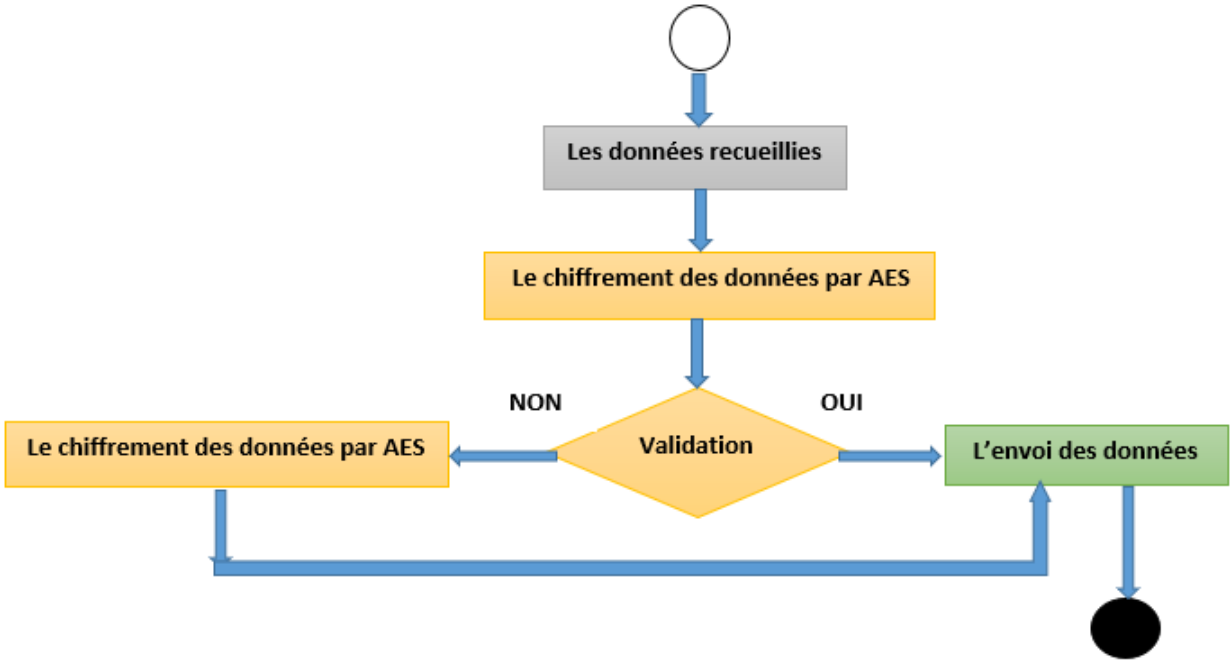


FIGURE 3.6 – Cryptage et l'envoi des données avec AES.

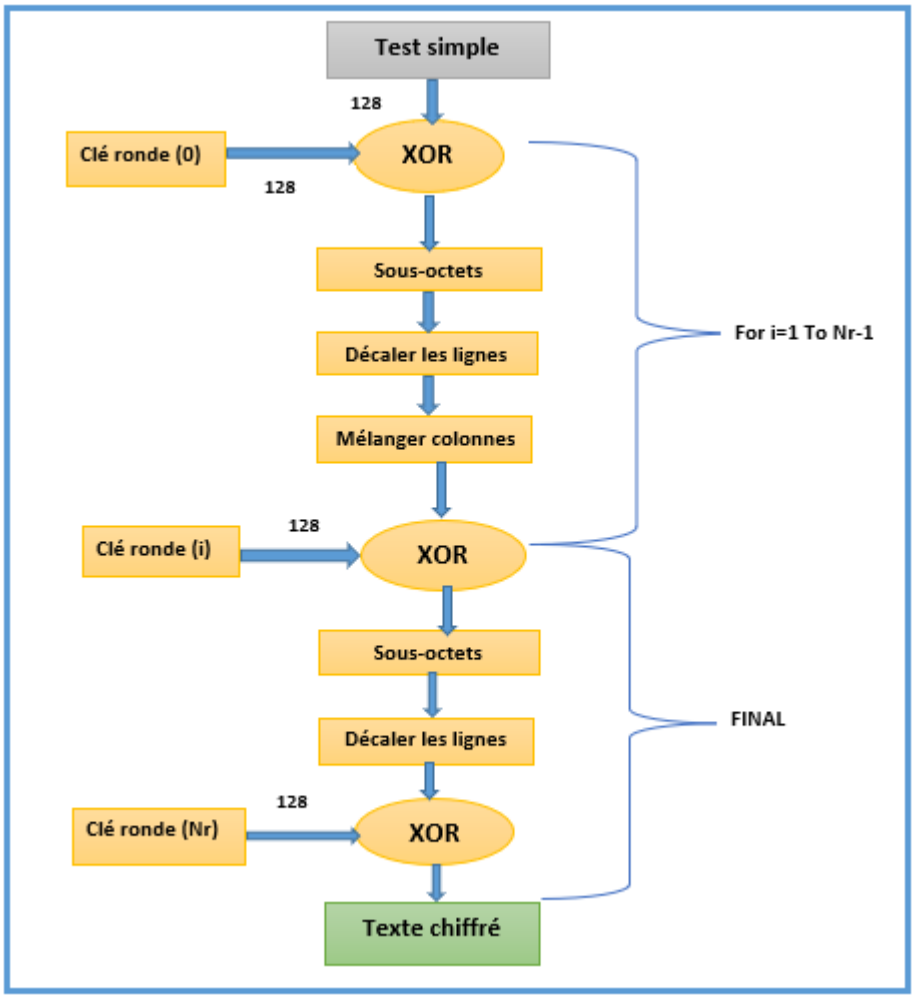


FIGURE 3.7 – chiffrement AES.

3.3.6 Réception des données

Une fois que la station de base reçoit les données chiffrées par le chef de bloc, la station de base déchiffre ces données par AES et affiche ces données, comme illustré dans la figure suivante Déchiffrée par AES :

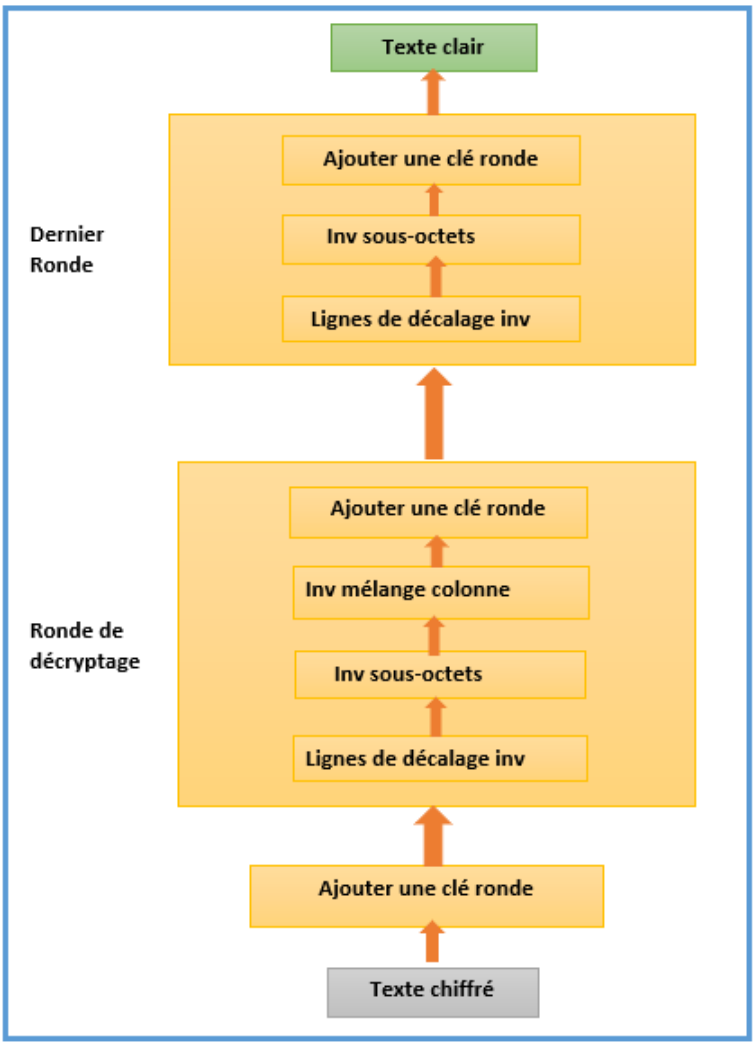


FIGURE 3.8 – déchiffrement AES.

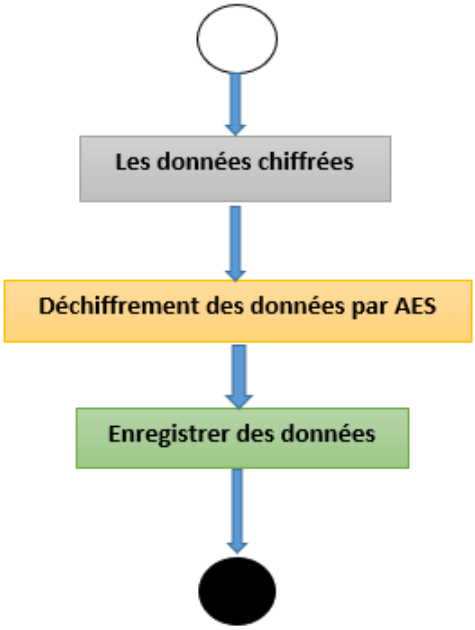


FIGURE 3.9 – Réception des données.

3.4 Fonctionnement générale

Le processus général de notre solution sera illustré dans la figure ci-dessous :

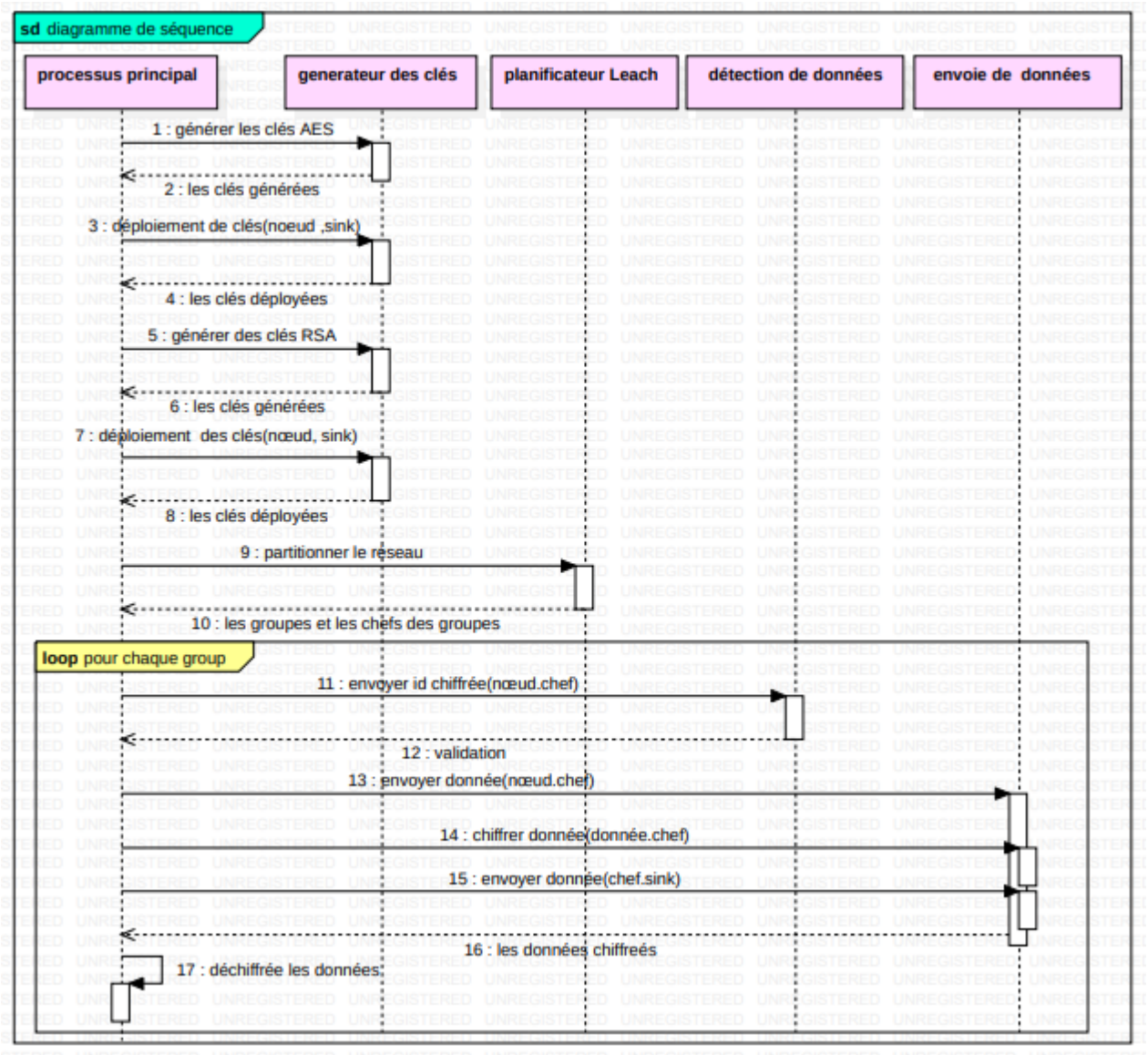


FIGURE 3.10 – diagramme de séquence de la solution proposée.

Explication du diagramme de séquence de la solution proposée :

• Tout d'abord, la station de base, génère et distribuer les clés AES et RSA au niveau des nœuds capteurs avant leur déploiement.

• Après le déploiement des nœuds, on lance l'implémentation du protocole de routage LEACH ; où en déterminent les clusters avec ses chefs.

• Lorsque les nœuds détectent des informations, dans chaque groupe, les identités des nœuds sont chiffrées par l'algorithme RSA et les envoyer à leur chef correspond.

• Après la validation d'identité des nœuds par leur chef, les donner son envoyé par les nœuds aux chefs correspond ; ce dernier est crypté les données à l'aide de l'algorithme AES et les envoyées à la station de base.

- Finalement, la station de base reçoit les données cryptées et les déchiffrées.

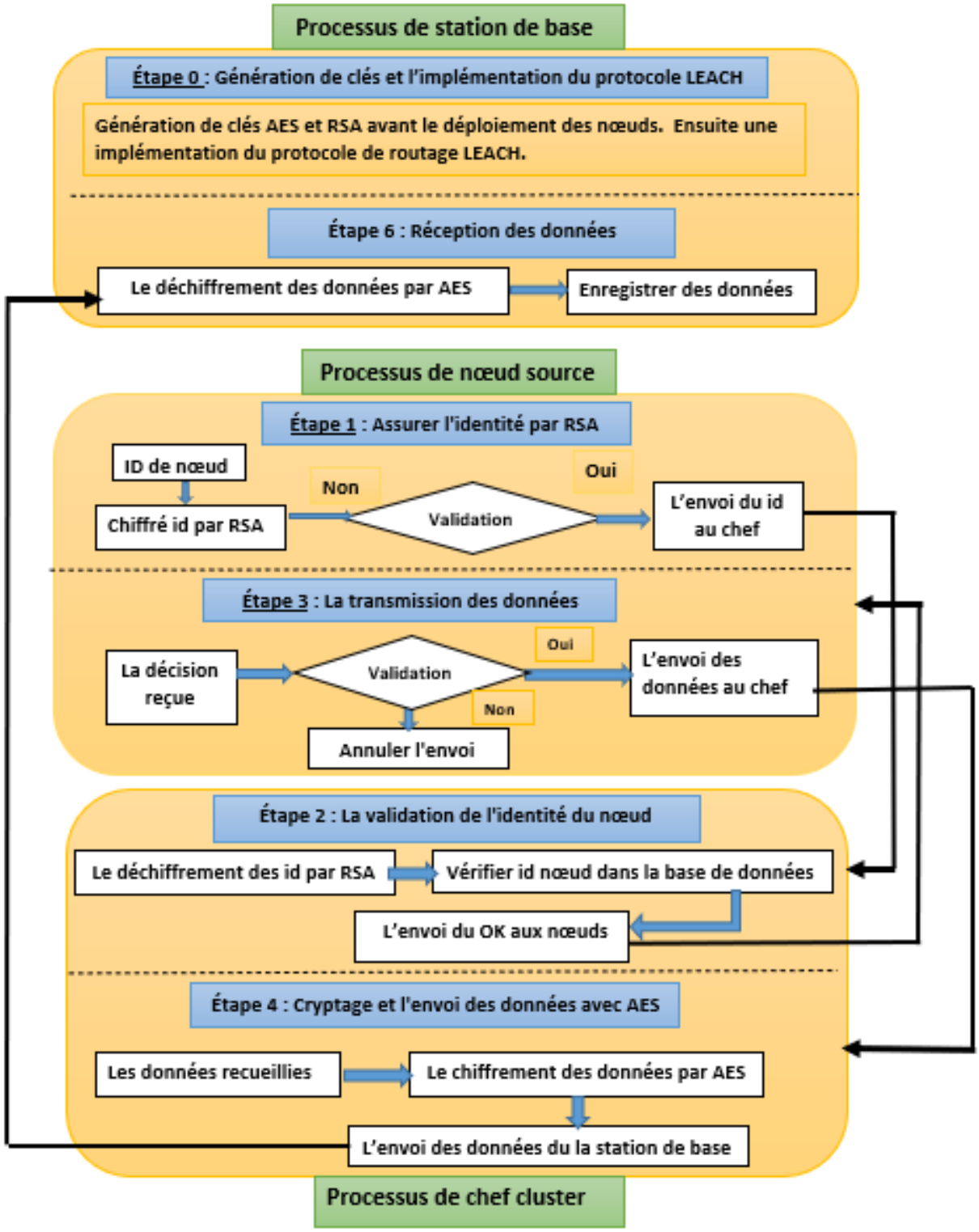


FIGURE 3.11 – Fonctionnement générale.

3.5 Conclusion

Dans ce chapitre, nous avons fait une analyse de la description et de la modélisation de notre solution proposée RA-LEACH. Ce dernier consiste à développer un protocole de routage sécurisé pour les réseaux de capteurs sans fils. Elle se base sur l'ajout du concept de la cryptographie au protocole LEACH.

Notre solution aide à protéger le RCSF contre les menaces où on offre deux niveaux de cryptage ; l'un symétrique par l'utilisation de l'algorithme AES, et autre asymétrique par l'utilisation de l'algorithme RSA. Celle-ci sans trop affecter la consommation d'énergie qui est le facteur de base qui influence dans les Récifs.

Le chapitre suivant sera consacré essentiellement à l'implémentation du notre système

Chapitre 4

Implémentation

4.1 Introduction

Comme nous avons vu dans le chapitre précèdent, nous avons parlé de la visualisation et de la modélisation de notre technique RA-LEACH ; où on applique deux l'algorithme du cryptage au protocole de routage LEACH. La première étape est l'application du cryptage asymétrique par RSA pour assurer l'identité des nœuds capteurs. Et la deuxième étape est l'application du cryptage symétrique par AES pour chiffrer les données.

Ce chapitre présente les résultats de simulations obtenus à partir de l'exécution du RA-LEACH que nous avons mis en œuvre pour résoudre le problème de la sécurité dans les RCSFs, ainsi que son analyse et validation.

De même, nous présentons les outils et les plateformes de développement utilisés à l'implémentation des différents composants du système.

L'impact de différents paramètres des modèles LEACH et RA-LEACH est examiné. Par conséquent, les résultats généraux de chaque algorithme sont présentés. Les discussions sur les valeurs des résultats sont alors fournies.

4.2 Outils de développement

Pour réaliser notre approche RA-LEACH, nous avons utilisé les outils suivants :

4.2.1 Outils logiciel

MATLAB :

MATLAB est un environnement de bureau qui combine un langage de programmation exprimant directement la matrice et les mathématiques matricielles avec un environnement de bureau conçu pour l'analyse et la conception itératives. Il est livré avec Live Editor, qui vous permet d'écrire des scripts qui mélangent du code, de la sortie et du texte formaté dans un bloc-notes exécutable. Nous avons utilisé MATLAB pour encoder et programmer notre langage [39].

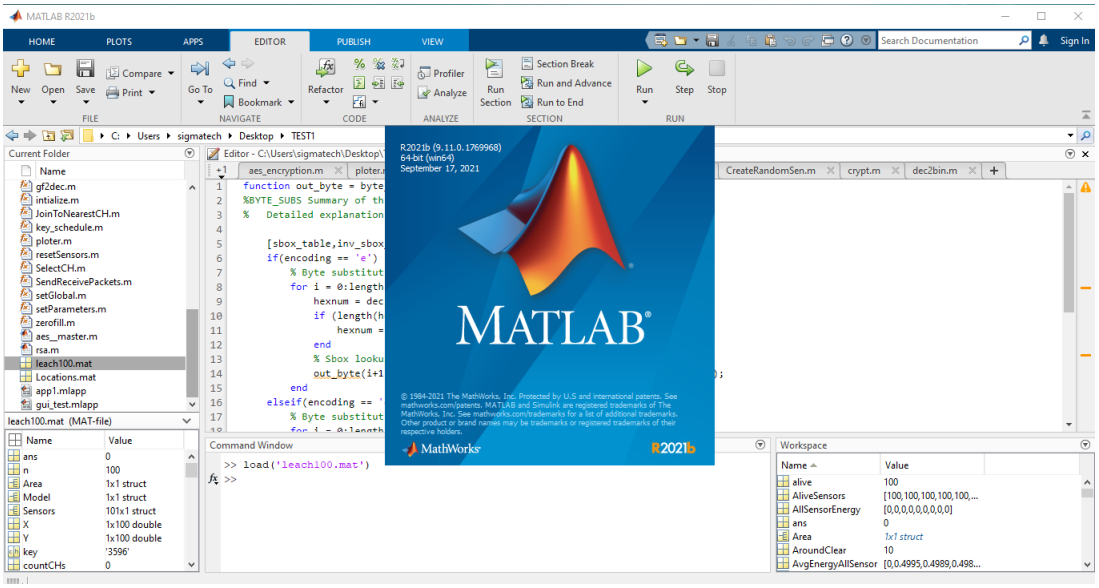


FIGURE 4.1 – MATLAB R2021a.

4.2.2 Outils matériel

Pour nos appareils, nous utilisons un ordinateur portable de Hp 3168ngw,Avec ces spécifications DESKTOP-NP3D6PF.

FIGURE 4.2 – Hp 3168ngw.

Processeur : Intel(R) Core(TM) i3-6006U CPU @ 2.00GHz 2.00 GHz

RAM : 8 Go.

Windows 10 : Système d'exploitation de Microsoft pour PC, tablettes, appareils intégrés et appareils Internet des objets.

Type du systéme : Système d'exploitation 64 bits, processeur x64.

4.3 Modèle énergétique

L'énergie consommée par un noeud capteur est due essentiellement aux opérations suivantes : la capture, le traitement et la communication de données.

la consommation d'énergie est appelée Ec est définie comme suit :[38][9]

Ec = Es/détection(sensing)+Es/traitement(processing)+Es/communication où :

- Es/sensing : la consommation d'énergie de l'unité de détection
- Es/processing : la consommation énergétique de l'unité de traitement
- Es/communication : la consommation énergétique de l'unité de communication.

elle est égale à la somme de deux valeurs :

ETX qui est la transmission d'énergie et ERX qui est la réception d'énergie

Es/communication = ETX + ERX(2) où :

ETX (k, d) = (Eelec * k)+(Eamp *k * d^2)

ERX (k) = Eelec * k(4)

Es/traitement(processing)= P*T

P : Puissance = TDP x (OC MHz /Stock MHz) x $(OCVcore/StockVcore)^2$

T : durée = durée algorithme RSA + durée algorithme AES

K : la taille du paquet (bits)

d : la distance entre l'émetteur et le récepteur

Eelec : énergie pour faire fonctionner les circuits de l'émetteur ou du récepteur

Eamp : amplificateur de transmission

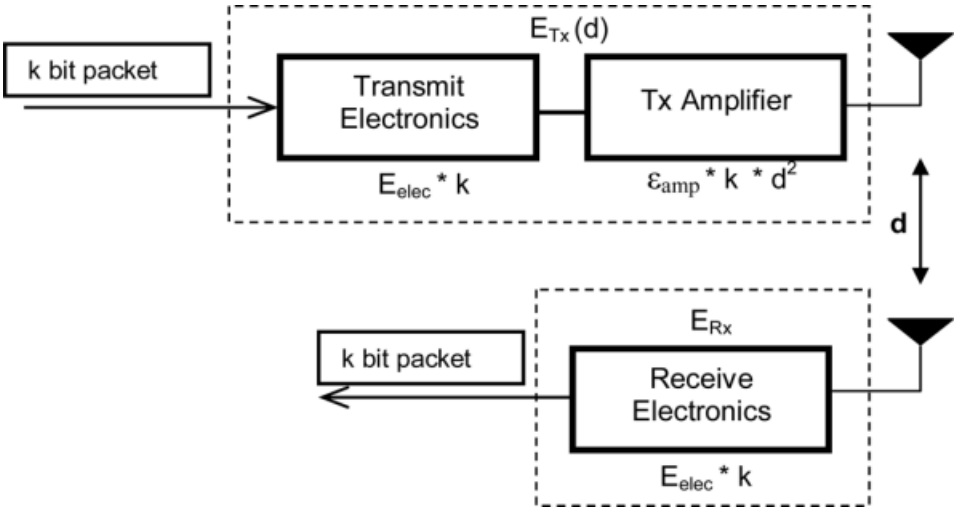


FIGURE 4.3 – Modèle de consommation d'énergie [9][38] .

4.4 Modèle de réseau

Pour commencer, nous avons implémenté un réseau de dimensions 200 × 200 et avec une station de base (puits) au milieu, la propagation s'est produite de manière aléatoire dans chaque région, tous les nœuds du réseau simulé commencent avec une puissance initiale égale à E0 = 0,5 J et un nombre illimité quantité de données à envoyer à la station de base. De plus, la puissance de la station de base est illimitée. Comme le montre la figure ci-dessous :

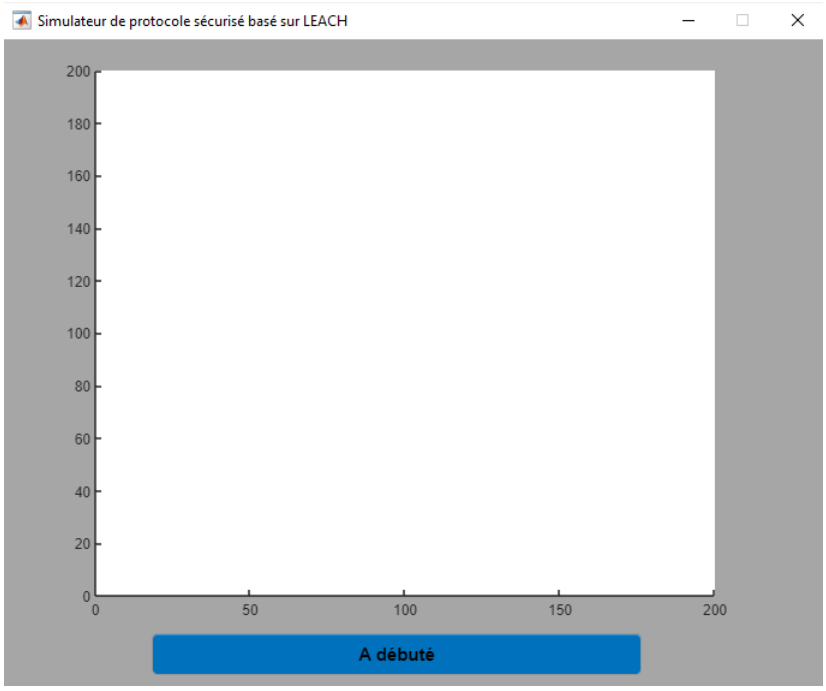


FIGURE 4.4 – la dimension de réseau.

4.5 Structure du programme

La simulation de routage sécurisé que nous avons implémentée se compose de plusieurs structures et niveaux comme indiqué ci-dessous :

4.5.1 Fonctions du programme

Afin d'implémenter nos protocoles de routage sécurisé, nous devons implémenter plusieurs fonctions dans notre projet comme indiqué :

1. **Les fonctions de Cryptage :**

   Afin de concevoir une simulation de protocole de sécurité, les fonctions RSA et AES qui incluent la génération de clé, le chiffrement et le déchiffrement doivent être programmées.

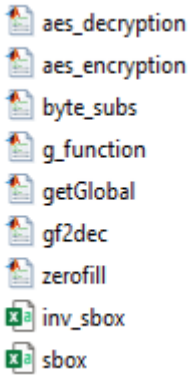


FIGURE 4.5 – Les fonctions AES .

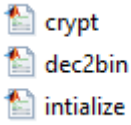


FIGURE 4.6 – Les fonctions RSA .

2. **Les fonctions de LEACH :**

   Afin de programmer le protocole LEACH, plusieurs fonctions doivent être conçues à partir de celui-ci.

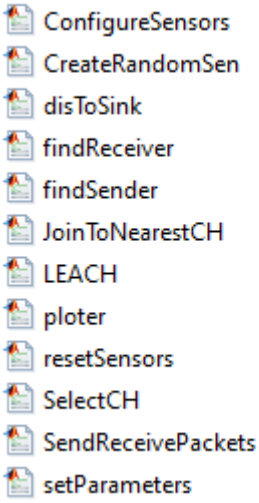


FIGURE 4.7 – Les fonctions de LEACH .

3. **Les données matricielles :**

   Lorsque la simulation est exécutée, le résultat est enregistré sous forme de valeurs dans les tables matricielles.

Sensors

101x1 struct with 14 fields

Fields	xd	yd	G	df	type	E	id	dis2sink	dis2ch	MCH	E_s
77	181.0269	106.7544	0	0	'N'	0.4898	77	81.3080	10.3588	11	0.5107
78	21.8308	165.1618	0	0	'N'	0.4890	78	101.7668	33.8322	81	0.5117
79	67.6195	58.7946	9	0	'C'	0.4856	79	52.4059	0	79	0.5151
80	149.2627	2.0673	0	0	'N'	0.4884	80	109.6249	97.6087	13	0.5125
81	9.6895	133.5832	9	0	'C'	0.4855	81	96.3526	0	81	0.5156
82	120.6936	105.2205	0	0	'N'	0.4867	82	21.3419	18.8327	85	0.5144
83	145.9419	141.4507	0	0	'N'	0.4858	83	61.8774	31.0210	85	0.5153
84	156.2754	57.5954	0	0	'N'	0.4865	84	70.4633	42.5001	13	0.5144
85	138.5064	111.3340	9	0	'C'	0.4846	85	40.1398	0	85	0.5163
86	79.3042	12.3181	0	0	'N'	0.4877	86	90.0912	47.9228	79	0.5130
87	156.0351	67.5168	0	0	'N'	0.4876	87	64.7695	33.6670	13	0.5133
88	121.5732	148.2508	0	0	'N'	0.4870	88	52.8540	40.6151	85	0.5139
89	20.9626	25.5777	0	0	'N'	0.4892	89	108.5614	35.9686	69	0.5117
90	109.9080	97.0459	0	0	'N'	0.4874	90	10.3390	10.3390	101	0.5136
91	178.0951	159.7921	9	0	'C'	0.4897	91	98.3562	0	91	0.5109
92	146.8682	10.2664	0	0	'N'	0.4876	92	101.2361	90.3188	13	0.5134
93	14.5771	17.7055	0	0	'N'	0.4902	93	118.6148	43.9592	69	0.5104
94	159.6702	188.6016	0	0	'N'	0.4921	94	106.8212	34.1975	91	0.5083

FIGURE 4.8 – Les données matricielles et résultats .

4.5.2 Interface du programme

L'interface utilisateur génère des clés, le déploiement des noeuds , le cryptage de l'identité, la transmission des données, le cryptage et le décryptage des données.

1- génère des clés :

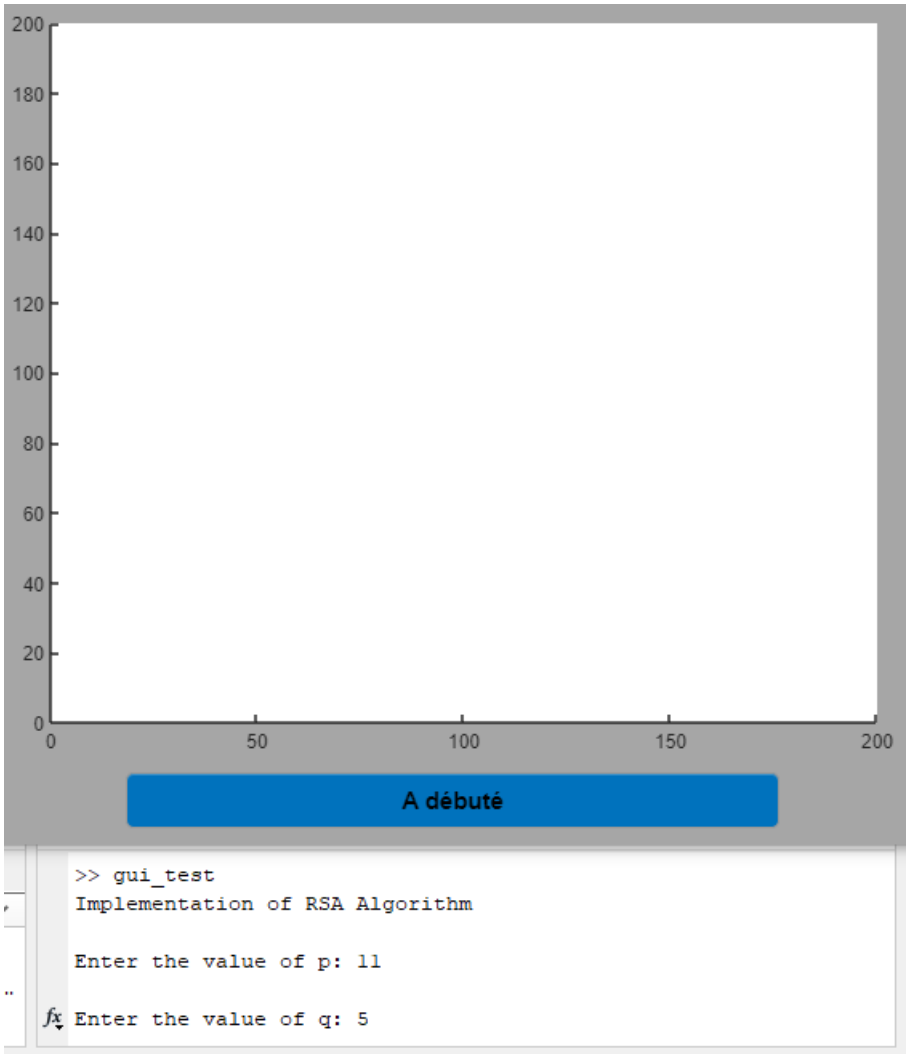


FIGURE 4.9 – entrée les clés .

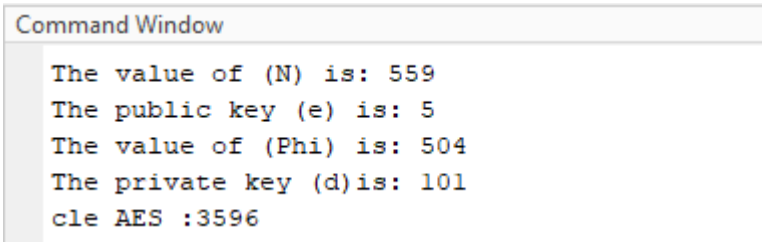


FIGURE 4.10 – gèneration des clés .

2-déploiement des noeuds :

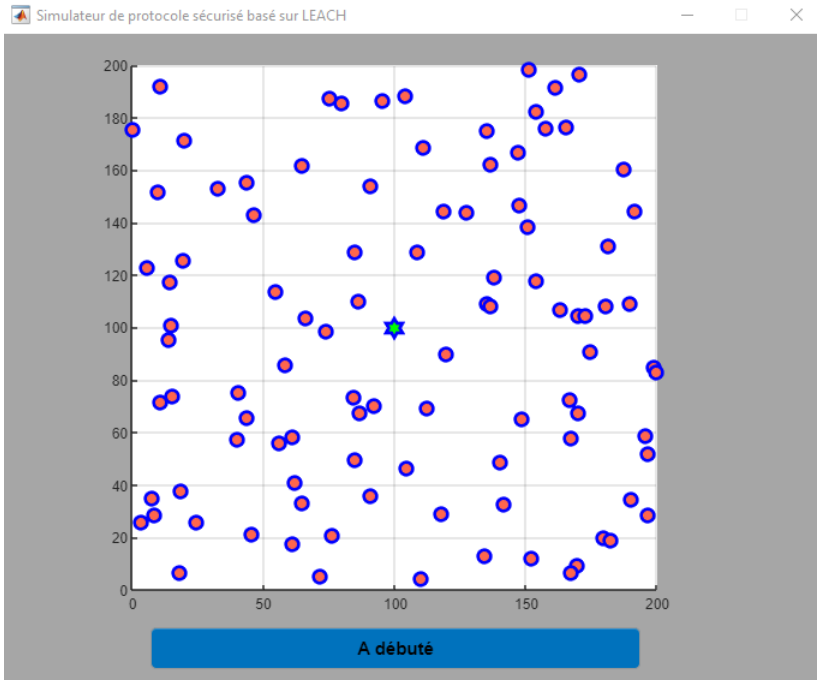


FIGURE 4.11 – le déploiement des 100 nœuds .

CreateRandomSen.m

```
function CreateRandomSen(Model,Area)
    n=Model.n;
    x=Area.x;
    y=Area.y;
    X=zeros(1,n);
    Y=X;
    for i=1:1:n
        X(i)=rand()*x;
        Y(i)=rand()*y;
    end
    save ('Locations','X','Y');

end
```

FIGURE 4.12 – Fonction Créer un capteur aléatoire .

3- cryptage de l'identité :

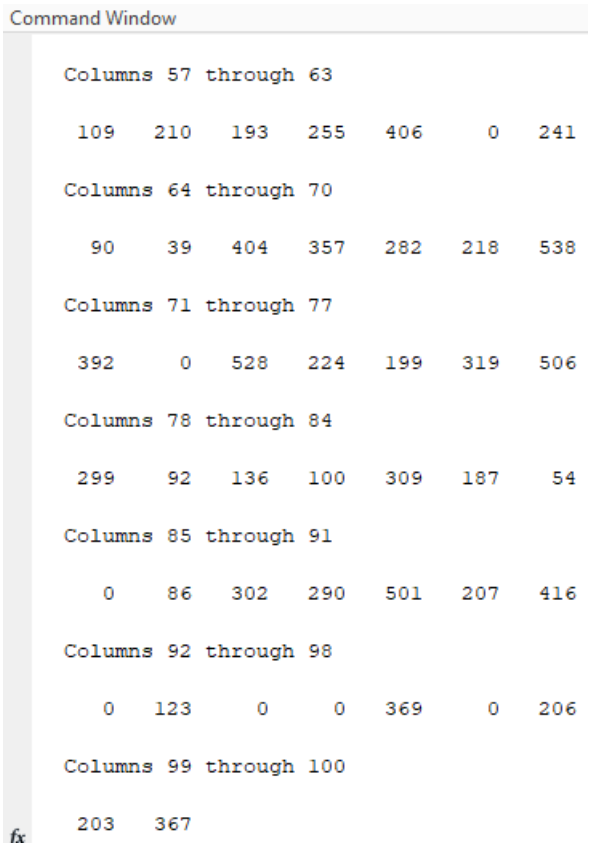


FIGURE 4.13 – Les identifiants de nœud sont chiffrés par RSA après le déploiement.

4- transmission des données :

Après le processus de déploiement du contrat, le chef de cluster est directement sélectionné et l'identifiant crypté lui est envoyé du chef de cluster avec transmission de données.Il collecte les informations, crypte les données et les envoie à la station de base.

```
SelectCH.m
function [CH,Sensors]=SelectCH(Sensors,Model,r)
global delta;
    CH=[];
    countCHs=0;
    n=Model.n;
 for i=1:1:n
        if(Sensors(i).E>0)
            temp_rand=rand;
            if (Sensors(i).G<=0)
                %Election of Cluster Heads
        if(temp_rand<= (Model.p/(1-Model.p*mod(r,round(1/Model.p)))))
                    countCHs=countCHs+1;
                    plot(Sensors(i).xd,Sensors(i).yd,'o','LineWidth',
                     grid on;
                     hold on;
                    CH(countCHs).id=i;
                    Sensors(i).type='C';
                    Sensors(i).G=round(1/Model.p)-1;
      Sensors(i).donnee=Model.DpacketLen;
      disp('Decrypted ASCII of Message:');
      message(i)= crypt((Sensors(i).id),Pk,d);
      disp(message);
end
      Sensors(i).DpacketLen=Model.DpacketLen;
```

FIGURE 4.14 – fonction sélection chef de cluster .

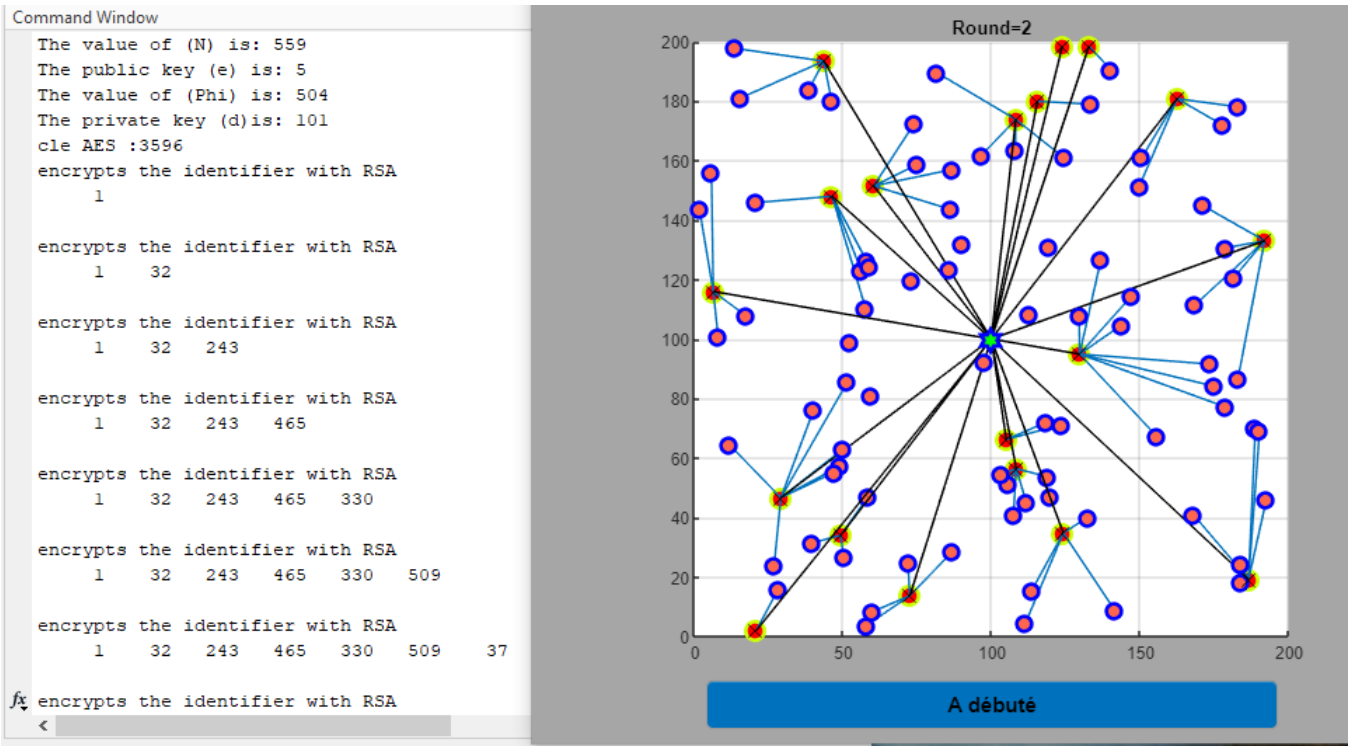


FIGURE 4.15 – transmission de données.

```
for i=1:n
if (Sensors(i).type=='N' && Sensors(i).dis2ch<Sensors(i).dis2sink &&
            Sensors(i).E>0)

        XL=[Sensors(i).xd ,Sensors(Sensors(i).MCH).xd];
        YL=[Sensors(i).yd ,Sensors(Sensors(i).MCH).yd];
        hold on
        line(XL,YL)
    end
end
```

FIGURE 4.16 – tracer l'état du réseau à la fin de la phase de configuration .

```
for i=1:length(TotalCH)

    Receiver=n+1;                %Sink
    Sender=TotalCH(i).id;        %CH
    Sensors=SendReceivePackets(Sensors,Model,Sender,'Data',Receiver);
    disp('send Data packet from CH to Sink after Data aggregation :Send

end
```

FIGURE 4.17 – envoyer le paquet de données du CH au récepteur après l'agrégation des données.

5- cryptage et le décryptage des données :

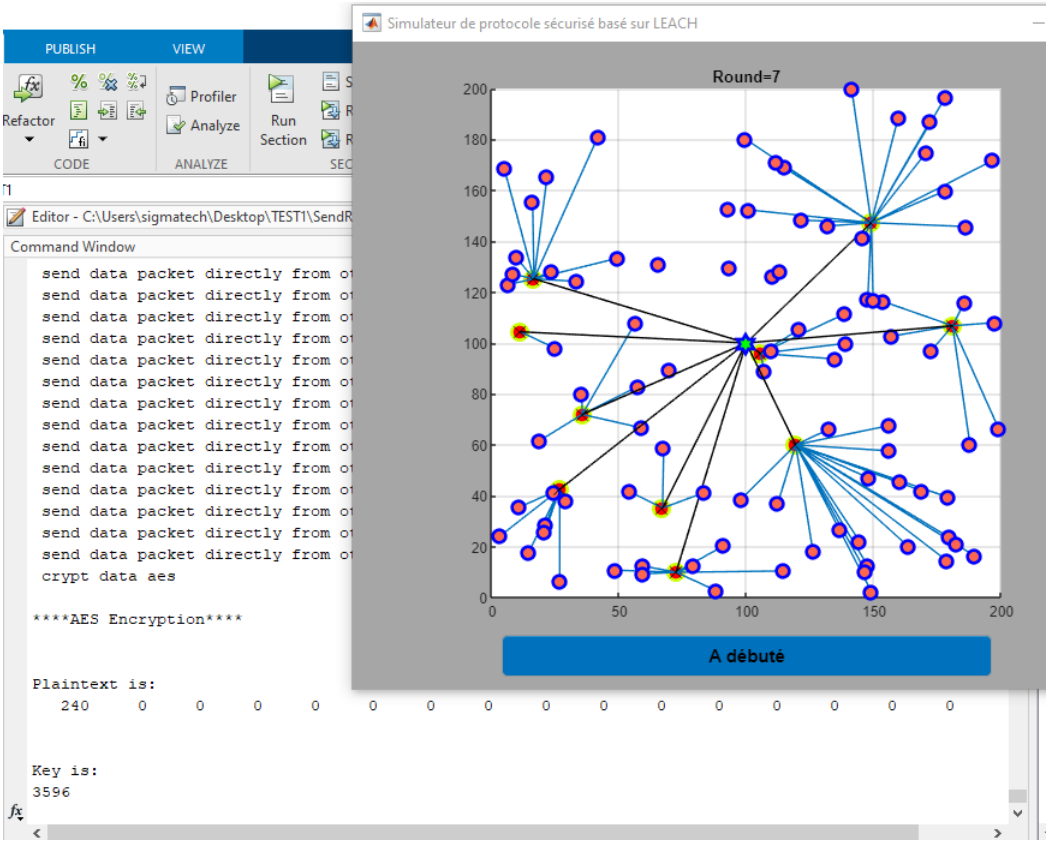


FIGURE 4.18 – Les données sont cryptées par AES .

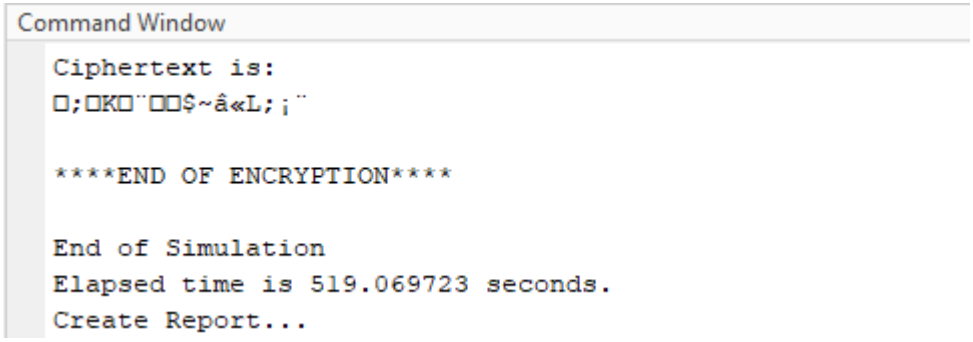


FIGURE 4.19 – Déchiffrer les données.

```
alive=0;
SensorEnergy=0;
for i=1:n
    if Sensors(i).E>0
        alive=alive+1;
        SensorEnergy=SensorEnergy+Sensors(i).E;
    end
end
AliveSensors(r)=alive; %#ok

SumEnergyAllSensor(r+1)=SensorEnergy; %#ok

AvgEnergyAllSensor(r+1)=SensorEnergy/alive; %#ok

ConsumEnergy(r+1)=(initEnergy-SumEnergyAllSensor(r+1))/n; %#ok

En=0;
for i=1:n
    if Sensors(i).E>0
        En=En+(Sensors(i).E-AvgEnergyAllSensor(r+1))^2;
    end
end

Enheraf(r+1)=En/alive; %#ok
```

FIGURE 4.20 – Calcul d'énergie

4.6 Simulation

La simulation que nous avons appliquée comprend les paramètres suivants, comme indiqué dans les tableaux moins :

4.6.1 Paramètres de simulation

Nous résumons tous les paramètres utilisés dans les simulations dans le tableau suivant :

1- Paramètres réseau :

Paramètres	Valeur
Taille	200×200 m
Type de déploiement	Aléatoire
Taille du paquet	120 bits
Portée radio	20 m
Technologie sans fil	zigbee IEEE802.15.4

TABLE 4.1 – Paramètres de simulation

2- Paramètres de nœud :

Paramètres	Valeur
Nombre de noeuds	100
Nombre maximum de round	50
ID de la station de base	101
ID des nœuds	[1-100]
Processeur	ATmega128

TABLE 4.2 – Paramètres de nœud

3- Paramètres d'énergie :

Paramètres	Valeur
Probabilité d'élection optimale d'un nœud pour devenir chef de cluster	0.1
Energie initiale de chaque noeud	0.5 Joul
Energie initiale du réseau	50 Joul
Nombre de paquets envoyés en phase d'état stable	10
énergie d'agrégation	5*0.000000001
énergie d'amplification	0.0013*0.00000000001
énergie de transmission	50*0.000000001
énergie de reception	50*0.000000001
énergie d' filtrage des données	10*0.000000000001

TABLE 4.3 – Paramètres de énergie

4.6.2 Résultats et discussion

Dans cette section, nous présentons les résultats obtenus à partir de l'exécuter le protocole de routage LEACH et notre proposition RA-LEACH. Où nous discutons et analysons ces résultats acquis par la comparaison des mesures de performance au-dessus.

1- consommation d'énergie :

Figure 4.21 et 4.22 détermine l'efficacité de l'algorithme RA-LEACH sur le niveau Consommation d'énergie. Où nous présentons les résultats de l'impact du nombre de nœuds sources sur le coût de l'énergie. La consommation d'énergie pour notre solution RA-LEACH est plus proche du protocole LEACH. cela est dû à sa pré-distribution des clés. Et aussi, il dirige la grande complexité de traitement vers la station de base.

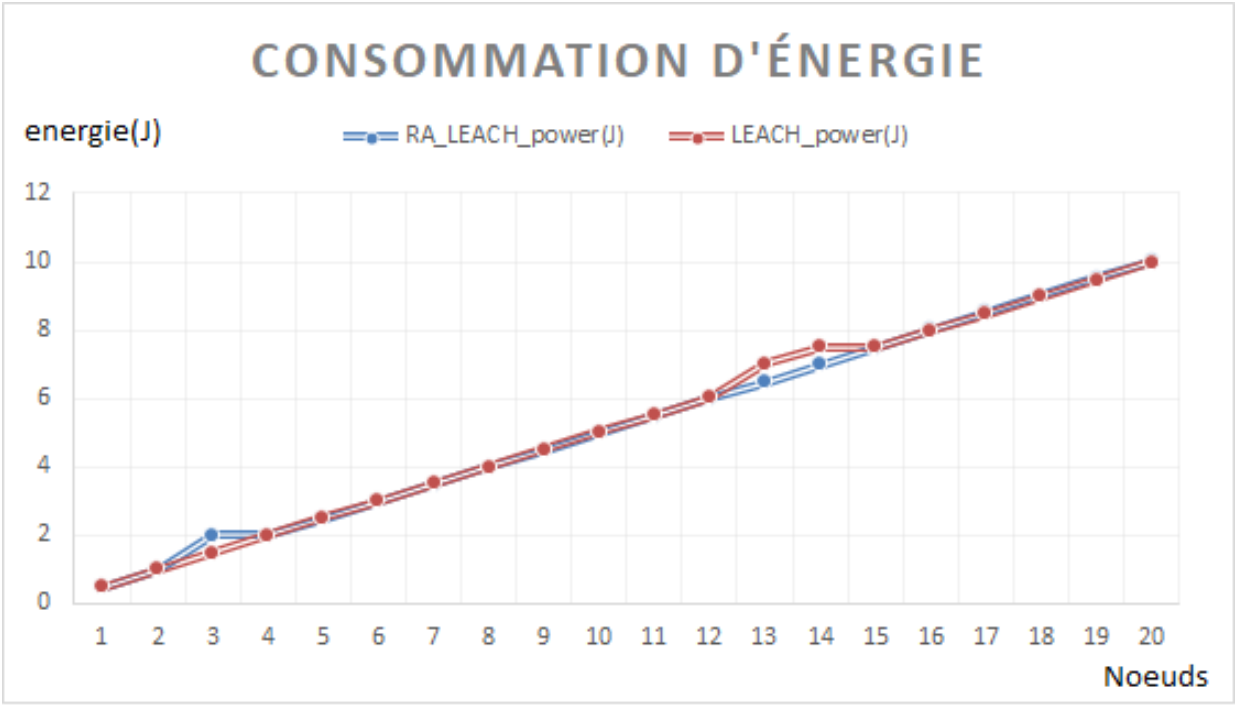


FIGURE 4.21 – courbe graphique représentant consommation d'énergie .

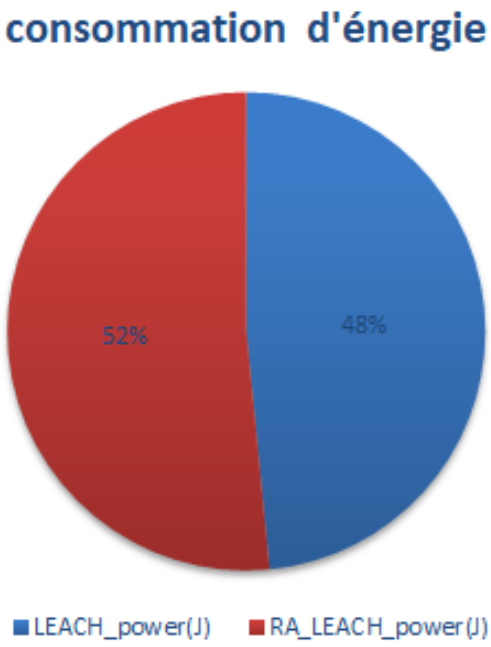


FIGURE 4.22 – pourcentage de consommation d'énergie .

2- temps de traitement :

Concernant la durée de la tâche, les figures 4.23 et 4.24 montrent les résultats de l'impact

du nombre de nœuds sources sur la durée de la tâche. Les résultats obtenus en utilisant l'algorithme RA-LEACH ne sont pas très satisfaisant en termes de durée de la tâche à cause du traitement du cryptage ajouté. Ils sont distants du protocole LEACH qui prend beaucoup moins de temps pour exécuter une tâche.

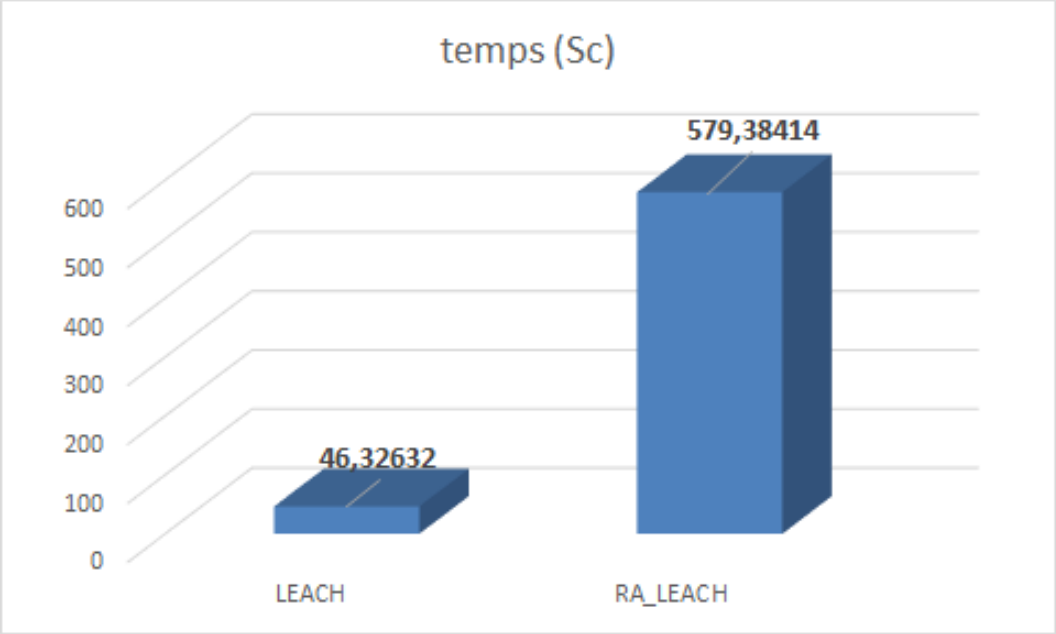


FIGURE 4.23 – Graphiques à barres du temps écoulé .

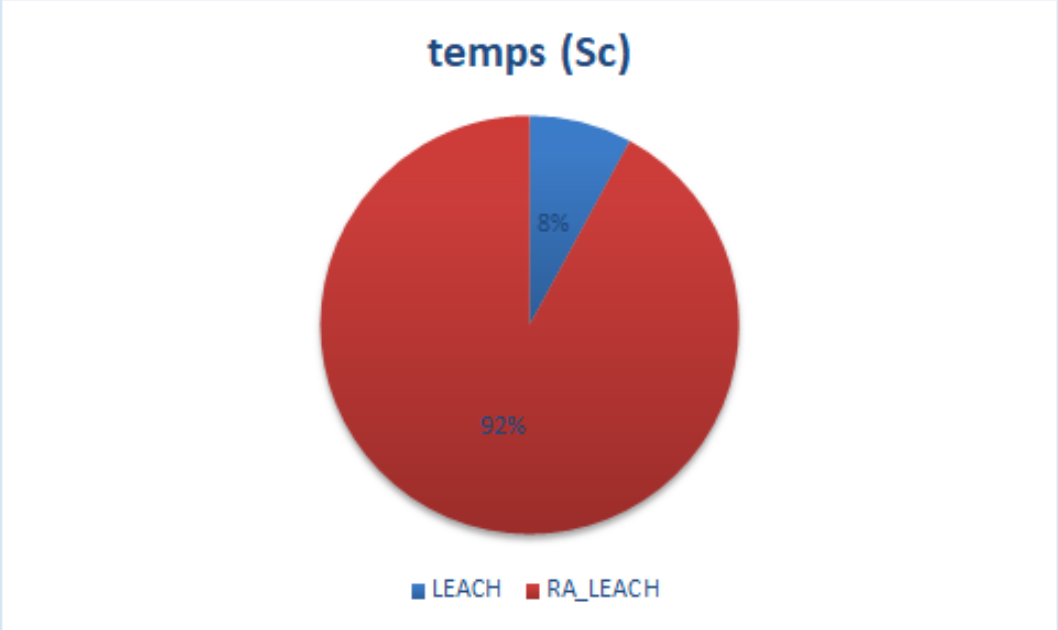


FIGURE 4.24 – cercle du pourcentage du temps écoulé .

4.7 Conclusion

Dans ce chapitre, nous avons exposé les outils que nous avons utilisés, les modèles de réseau ainsi que les paramètres de simulation avec les résultats obtenus.

Par conséquent, les résultats de RA-LEACH montre que le niveau de la sécurité du réseau est augmenté sans trop affecter la consommation d'énergie, cependant le temps de traitement à augmenté de manière significative par rapport au protocole LEACH.

Conclusion Générale

Les nœuds dans un RCSF fonctionnent généralement sans surveillance, donc ils sont vulnérables aux manipulations. Par conséquent, la capture d'un nœud par un adversaire est relativement facile et ses données recueillies peuvent alors être facilement récupéré. La recherche doit donc être dirigée vers des schémas avec un mécanisme de sécurité efficace et de faible complexité sans affecter la consommation d'énergie.

Dans notre étude, nous avons abordé le problème de sécurité dans les réseaux de capteurs sans fil en utilisant les algorithmes de cryptage AES et RSA. L'intérêt principal de cette recherche porte sur l'augmentation du niveau de sécurité, on prenant en considération la contrainte d'énergie. Nous proposons un nouveau protocole sécurisé RA-LEACH comme une version sécurisée du protocole LEACH ; où on applique deux l'algorithme du cryptage au protocole de routage LEACH. La première étape est l'application du cryptage asymétrique par RSA pour assurer l'identité des nœuds capteurs. Et la deuxième étape est l'application du cryptage symétrique par AES pour chiffrer les données.

Les résultats de la simulation prouvent l'efficacité du protocole RA-LEACH proposé en ce qui concerne la quantité d'énergie consommée, pour résoudre le problème de sécurité dans les réseaux de capteurs sans fil.

Les travaux proposés dans ce projet ouvrent des nouveaux défis dans le futur pour améliorer la performance du protocole RA-LEACH.

Dans la section suivante, nous mentionnons brièvement les limites de ce travail qui nous doit prendre comme des perspectives :

· Analyser RA-LEACH sur des nœuds mobiles ;

· Tester RA-LEACH sur un RCSF de grand échelle ;

· Mise à jour des clés RSA et AES ;

· Appliquer RA-LEACH sur d'autres protocoles hiérarchiques.

Bibliographie

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, Wireless sensor networks : a survey , Computer networks,March 2002.

[2] L.Khelladi, N.Badache, Les Réseaux de Capteurs : Etat de l'Art, Rapport de recherche. Laboratoire des Systèmes Informatiques, Faculté d'Informatique et Eléctronique, Bab Ezzouar, Alger, Février 2004.

[3] Matin, M. A., Islam, M. M. –Overview of Wireless Sensor Network. Wireless Sensor Networks - Technology and Protocols,2018.

[4] Cheick-Tidjane Kone. Conception de l'architecture d'un réseau de capteurs sans fil de grande dimension. Réseaux et télécommunications. Université Henri Poincaré-Nancy I, 2011.

[5] LIU Yong-Min 1, 2, WU Shu-Ci 1, NIAN Xiao-Hong 2,The Architecture and Characteristics of Wireless Sensor network ,March 2021.

[6] Muhammad r ahamed ,xu huang,dharmandra sharma, and hongya cui, Wireless Sensor Network : Characteristics and Architectures,International Scholarly and Scientific Research Innovation ,2012.

[7] Dionisis Kandris , Christos Nakas , Dimitrios Vomva and Grigorios Koulouras,Applications of Wireless Sensor Networks : An Up-to-Date Survey, microSENSES Research Laboratory, Department of Electrical and Electronic Engineering, Faculty of Engineering, University of West Attica,February 2020.

[8] Luis M. Borges, Student Member, IEEE, Fernando J. Velez, Senior Member, IEEE, Antonio S. Lebres "Survey on the Characterization and Classification of Wireless Sensor Network Applications ",24 April 2014.

[9] Imene ALOUI, Une Approche Agent Mobile Pour Les Réseaux De Capteurs, thesis of doctorat, biskra university 2016.

[10] A. Mehiaoui, "Etude comparative entre les deux protocoles de routage LEACH et PEGASIS dans les réseaux de capteurs sans fil",24/05/2015.

[11] endi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan, Energy Efficient Communication Protocol for Wireless Microsensor Networks , Massachusetts Institute of Technology Cambridge,2019.

[12] Charles P. Pfleeger ,Shari Lawrence Pfleeger ,Jonathan Margulies "security-in-computing-5-e".January 2015.

[13] Archana Choudary," What is Network Security : An introduction to Network Security" Octobe 2009.

[14] Telecom Saint-Etienne – Laboratoire Hubert Curien,"Approche didactique pour l'enseignement de l'attaque DPA ciblant l'algorithme de chiffrement AES" ,March 2012.

[15] Jaydip Sen. Security in Wireless Sensor Networks. Department of Computer Science Engineering, National Institute of Science Technology, INDIA 04/2016.

[16] Dr. G. Padmavathi, Mrs. D. Shanmugapriya ,A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,3 Sep 2009.

[17] D.Baker, H.X.Mel, La Cryptographie Décryptée, Campus Press edition, Référence Collection, pp. 414, Juillet 2021.

[18] Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim :A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks. (Journal of Security Engineering), 9 3 2012 6,2018.

[19] W.Heinzelman, A.Chandrakasan, H.Balakrishnan, Energy-Efficient Communication Protocol for Wireless Microsensor Networks, International Conference on Systems Science, January 2010.

[20] Mohamed-Lamine Messai. Classification of Attacks in Wireless Sensor Networks.nternational Congress on Telecommunication and Application'14 University of A.MIRA Bejaia, Algeria, 23-24 APRIL 2014.

[21] Furrakh Shahzad1 , Maruf Pasha2 , Arslan Ahmad2. A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. nternational Journal of Computer Science and Information Security (IJCSIS), December 2016.

[22] Mohamed-Lamine Messai. Classification of Attacks in Wireless Sensor Networks.nternational Congress on Telecommunication and Application'14 University of A.MIRA Bejaia, Algeria, 23-24 APRIL 2014.

[24] S. MOAD, "Optimisation de la consommation d'énergie dans les réseaux de capteurs sans fil " Master recherche en 2éme année informatique, vol. Université : FSICRennes 1, Laboratoire de recherche : DYONISOS-IRISA, 2018.

[25] B. Kaliski, "The MD2 Message-Digest Algorithm", RFC 1319, April 2002.

[26] Somia SAHRAOUI,Mécanismes de sécurité pour l'intégration des RCSFs à l'IoT (Internet of Things),Doctorat thesis, Université de Batna 2,2016.

[27] A-S.Uluagac, R-A.Beyah, Y.Li, J-A.Copeland, VEBEK : Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks, IEEE Transactuions on Mobile

Computing, Version accepted for publication by IEEE,2013.

[28] T. Allik, H. Makhlouf, and N. Koulalene, "Mise en place d'un réseau de capteurs sans fil pour la surveillance des paramètres de production de l'unité de conditionnement d'huile au sein de Cévital," Université abderrahmane mira béjaia, 2017.

[29] SAHRAOUI belkheyr,"Etude d'un protocole de routage basé sur les colonies de Fourmis dans les réseaux de capteurs sans fil ",Doctorat thesis,2014.

[30] N.Sughanthi, V.Sumathy, Energy Efficient Key Management Scheme for Wireless Sensor Networks, Int J Compute Commun, February, 2014.

[31] Y.Zhang, J.Pengfei, An Efficient and Hybrid Key Management Scheme for Heterogeneous Wireless Sensor Networks, The 26th Chinese Control and Decision Conference, May 31 2014.

[32] O-K.Sahingoz, Large Scale Wireless Sensor Networks with Multi-Level Dynamic Key Management Scheme, Journal of Systems Architecture,2013.

[36] Z.Qin, X.Zhang, K.Feng, Q.Zhang,et J.Huang, IBKM : An Efficient IdentityBased Key Management Scheme for Wireless Sensor Networks Using the Bloom Filter, October 2014.

[37] G.Jolly, M.C.Kuscu, P.Kokate, et M.Younis, LEKM : A Low-Energy Key Management Protocol for Wireless Sensor Networks, IEEE Symposium on Computers and Communications, Juillet 2013.

[38] Akyildiz, I.F., W. Su, Y. Sankarasubramaniam, E. Cayirci, « A Survey on Sensor Networks ». IEEE Communication Magazine, Aout 2016.

[39] Site Officiel de Matlab ,MATLAB Simulink - MathWorks ,https : //www.mathworks.com/products /matlab.html (visité par 15-06-2022).

[40] Yaye M. Sarr, Université de Thiès, Bamba Guèye, Université Cheikh Anta Diop et Cheikh Sarr, Université de Thiès , Réduction des clusters singletons dans le protocole LEACH pour les réseaux de capteurs sans fil, 2018.