REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED BOUDIAF - M'SILA

FACULTE : MATHEMATIQUES ET DE L'INFORMATIQUE

DEPARTEMENT : INFORMATIQUE

N° :……..

DOMAINE : MATHEMATIQUES ET DE L'INFORMATIQUE

FILIERE : INFORMATIQUE

OPTION : RTIC

Mémoire présenté pour l'obtention
Du diplôme de Master Académique

Par: Doumi Abdelmoumain

Intitulé

La Sécurité des Communications dans les Réseaux de Capteurs sans Fils

Soutenu le: 24 /06 /2018 devant le jury composé de :

Saoudi Lalia	**Université de M'sila**	**Président**
Mezreg Fares	**Université de M'sila**	**Rapporteur**
Attir Azzedine	**Université de M'sila**	**Examinateur**

Année universitaire : 2017 /2018

TABLE DES MATIERES

LISTE DES TABLEAUX

LISTE DES FIGURES

INTRODUCTION GENERALE

La grande évolution dans les domaines de la micro-électronique, de la micromécanique, et des technologies de communication sans fil, ont permis de produire avec un coût raisonnable des petits dispositifs de détection et de communication. Ces dispositifs sont connus comme des nœuds capteurs. Ils ont la capacité de collecter et transmettre des données environnementales vers un point centralisé appelé la Station de Base (SB) ou le puit. L'ensemble des nœuds capteurs forme un Réseau de Capteurs Sans Fil (RCSF). Ce type de réseau est largement utilisé, et fait l'objet de plusieurs recherches scientifiques. Il constitue une solution efficace dans une grande variété d'applications comme les applications militaires, environnementales, domotiques, industrielles, etc. Parmi les caractéristiques de RCSF, (1) le déploiement de ses nœuds dans des zones ouvertes d'une manière aléatoire ou déterministe. (2) le fonctionnement autonome de ses nœuds capteurs. (3) l'échange des données entre des nœuds capteurs se fait sans utiliser une infrastructure réseau préexistante et fixe ou une administration centralisée. (4) Chaque nœud de réseau communique directement avec les autres nœuds qui se trouvent dans sa protée radio. La communication avec les nœuds distants ou hors portée radio se fait par l'intermédiaire des autres nœuds (communication multi-sauts).

Les architectures de communications dans RCSF sont généralement classées selon deux catégories : communication plate et communication basée sur les clusters. La communication basée sur les clusters est une manière efficace de réduire la consommation d'énergie totale du réseau fil. L'idée consiste à former des groupes (clusters) de nœuds capteurs et d'utiliser les CHs (Cluster-Heads) élus comme routeurs. Chaque CH collecte les données à partir de tous les nœuds capteurs qui appartenant à leur cluster, agrège les données rassemblées et les transmet directement vers station de base (SB).

Problématique

Les nœuds capteurs sont généralement déployés dans des zones non surveillées, la plupart des applications des RCSFs nécessitent un haut niveau de sécurité pour fournir les exigences de sécurité de base et rendre ces applications invulnérables aux différentes

attaques, empêchant un intrus de perturber le bien fonctionnement du réseau en prenant le contrôle des nœuds de capteurs. En plus, il est connu que les RCSF sont faciles à attaquer en raison de la nature du médium qui permet relativement facilement intrus d'espionner, d'altérer ou d'injecter des données dans le réseau.

Dans ce travail, nous nous intéressons aux problèmes de sécurité des communications dans les réseaux de capteurs, en particulier aux communications basées sur les clusters. Pour cela, nous proposons une solution de sécuriser des communications dans RCSF, qui offre une bonne protection en tenant compte des caractéristiques limitées des capteurs. L'objectif est donc, d'assurer les services de sécurité les plus importants. Ainsi la proposition peut être robuste face aux attaques comme DOS / Sybil. Notre proposition est basée sur la cryptographie symétrique pour faire du chiffrement/déchiffrement des données et pour calculer des MACs.

Organisation du mémoire

Ce mémoire est organisé de la manière suivante :

Introduction générale : présente le contexte et la problématique visée.

Chapitre 1 : est une introduction aux réseaux de capteurs sans fil qui sont considérés comme un type particulier de réseaux Ad-hoc.

Chapitre 2 : Dans ce chapitre, nous abordons la problématique de la sécurité dans les réseaux de capteurs, en expliquant les différentes vulnérabilités d'un réseau de capteur, les différents types d'attaques qui visent ce réseau ainsi que les exigences de sécurité existants et proposés pour faire face à ces menaces. Ensuite, nous présentons les différentes primitives cryptographiques utilisées dans les RCSFs.

Chapitre 3 : Dans ce chapitre nous exposons l'implémentation et l'évaluation de notre proposition. Le système d'exploitation Contiki est utilisé. Il consiste une programmation entière en langage C et une simulation avec Cooja.

Conclusion générale : Elle résume notre proposition et nos perspectives de recherches.

Chapitre 1

LES RESEAUX DE CAPTEURS SANS FIL

1. Introduction

Les progrès technologiques réalisés dans les communications sans fil et dans la micro-électronique ont conduit à la naissance d'un nouveau genre de réseaux Ad-Hoc appelé Réseau de Capteurs Sans Fil (RCSF). Ce type de réseau consiste généralement en un grand nombre de nœuds (nœuds capteurs). Ces nœuds peuvent être déployés dans des endroits géographiques en vue de collecter et transmettre des données vers un point de collecte appelé Sink ou Station de Base (SB). Le déploiement des nœuds capteurs se fait par manière aléatoire (avion) ou déterministe (manuelle). [1]

Généralement, les RCSF peuvent être utilisés dans différent domaines tel que : le militaire, l'environnementale, le médicale et la surveillance et le contrôle industriel.

2. Le Nœud capteur

Le nœud capteur est un petit dispositif électronique qui est caractérisé par sa limitation en ressources énergétique, de stockage, et en capacité de calcul. Il est déployé d'une manière aléatoire ou déterministe dans une zone géographique appelée champ de captage en vue de faire l'acquisition des données (par exemple : l'humidité, l'intensité de la luminosité, la température) à partir de l'environnement surveillé, les traiter et les communiquer. [2]

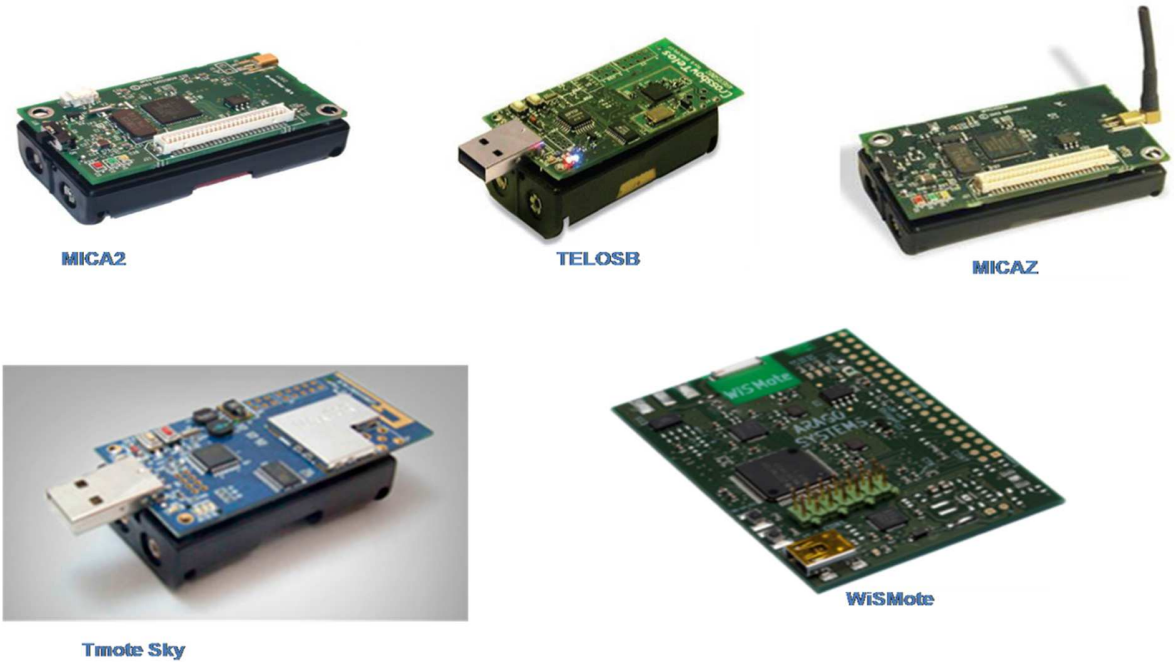

Figure 1-1 : Quelques types de noeud capteur

2.1. Composants matériels d'un nœud capteur sans fil [3]

2.1.1. **Unité d'acquisition** :

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

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

2.1.2. Unité de traitement :

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

2.1.3. Unité de communication (Transceiver)

Responsable de toutes les émissions /réceptions des données via un support de communication sans fil.

Cette unité comporte deux modules : un module radiofréquence d'émission / réception permettant la communication sans fil entre les différents nœuds du réseau, et un module série permettant l'interaction entre l'utilisateur et le nœud capteur pour faciliter la reprogrammation de l'unité de traitement.

2.1.4. Unité d'énergie (batterie)

Alimente les unités d'acquisition, de traitement et de communication. Dans certains RCSF applications (domaine militaire), il est impossible de recharger ou changer une batterie, donc avoir une meilleure gestion de la consommation d'énergie est primordial pour augmenter la durée de vie du réseau. Les nouveaux capteurs peuvent posséder des générateurs d'énergie renouvelable (par exemple: l'énergie solaire).De plus, un nœud capteur peut être équipé d'autres composants supplémentaires tels que :

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

La figure 1-2 résume Un exemple de consommation d'énergie d'un capteur de MicaZ. Nous notons que, parmi ces trois unités, l'unité de communication est celle qui consomme le plus d'énergie.

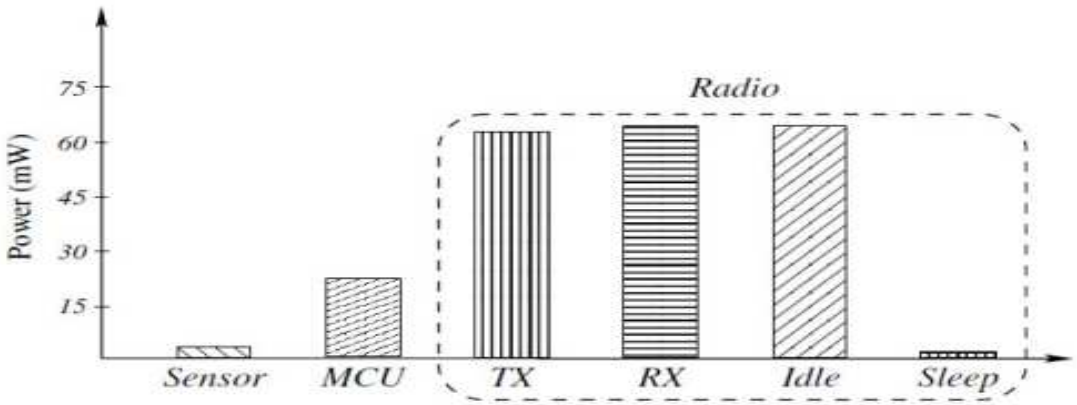

Figure 1-2: Consommation d´énergie d'un capteur Micaz[4]

3- Les réseaux de capteur sans fils.[5]

Un réseau de capteurs sans fil (RCSF), "Wireless Sensor Network (WSN)" est considéré comme un type particulier des réseaux Ad-hoc. RCSF compose d'un grand nombre de nœuds capteurs distribues sur une zone donnée soit d'une manière aléatoire (avion, missile) ou déterministe (manuelle, robot), Les nœuds capteurs communiquent entre eux par des liens radio pour le partage d'information et le traitement coopératif.

Chaque nœud communique directement avec les autres nœuds situés dans sa portée de transmission. La communication avec le nœud distant ou hors de portée de transmission se fait par l'intermédiaire d'autres nœuds qui acheminent les données vers la destination, ce processus est assuré par un protocole de routage.

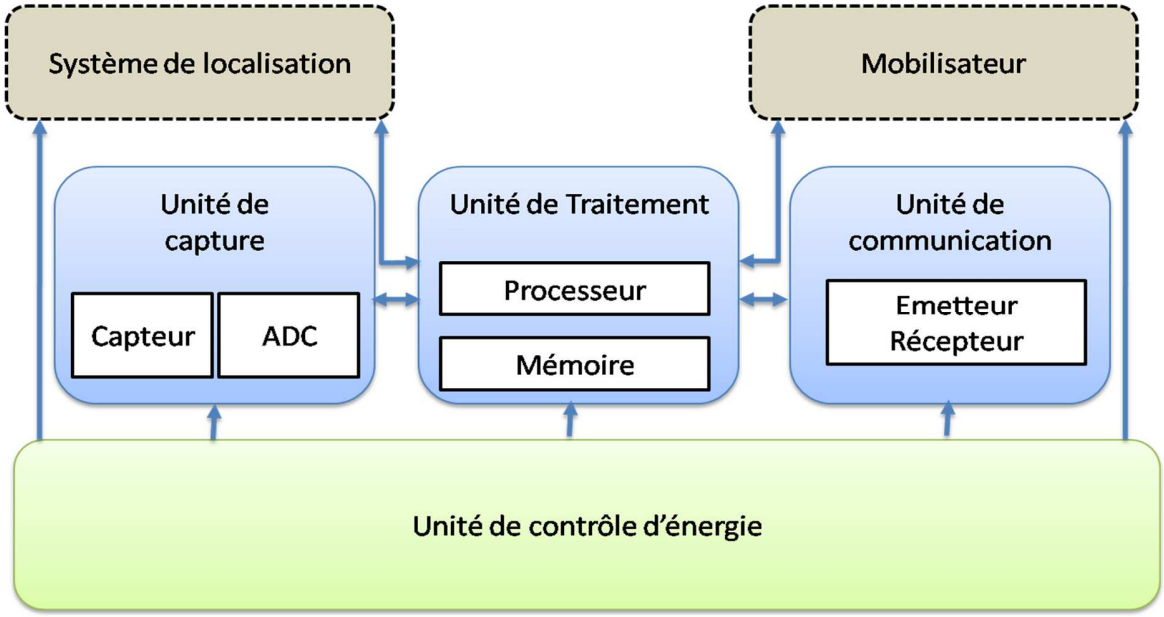

Figure 1-3 : Composants d'un capteur sans fil

Il existe plusieurs modèles commercialisés des capteurs sans fil, nous citons : TmoteSky et WiSMote, MICAZ, TINYNODE, TELOSB, Le tableau 1-1 illustré les principales caractéristiques techniques de quelques capteurs.

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

Tableau 1-1 : Caractéristiques techniques des capteurs [6]. [7]

3-1 Domaines d'applications des RCSF

Les RCSF peuvent avoir nombreux domaines d'applications, Dans ce qui suit, nous présentons de quelques exemples :

3-1.1 Les applications Militaires :

Dans ce domaine, l'utilisation des réseaux de capteurs sans fil s'avère très utile et appréciable. Ces dispositifs peuvent être utilisés dans la surveillance des champs de bataille, ou des frontières. En plus, les nœuds capteurs sont capables de détecter une variété d'évènements tels que la présence ou l'absence de certains types d'objets (agents chimiques, biologiques, ou radiations), sa position, sa vitesse, sa taille, ou encore sa direction.

3-1.2 Surveillance médicale :

Les RCSFs sont largement répandus et utilisés aujourd'hui dans le domaine médical, dans le but de garantir une surveillance permanente des organes vitaux de l'être humain et cela grâce `a des micro-capteurs qui pourront être avalés ou implantés sous la peau

(surveillance de la glycémie, détection de cancers,...etc.).En plus, les nœuds capteurs peuvent être utilisés pour recevoir des images en temps réel d'une partie du corps sans aucune chirurgie

3-1.3 Les applications environnementales :

Les réseaux de capteurs sans fil sont largement utilisés dans les applications environnementales en raison de leur capacité de prévenir les catastrophes naturelles (tempête, inondation, feu de forêt …), le déploiement de capteurs dans les sites industriels peut empêcher et prévenir certains risques industriels tels que la fuite de produits toxiques (gaz, produits chimiques radioactifs, etc.), cela permet une intervention rapide et efficace des secours.

3-1.4 Applications commerciale

Il est possible d'intégrer des capteurs au processus de stockage et de livraison dans le domaine commercial. Le réseau ainsi formé pourra être utilisé pour connaître la position, l'état et la direction d'un paquet. Il devient alors possible pour un client qui attend la réception d'un paquet, d'avoir un avis de livraison en temps réel et de connaître la localisation actuelle du paquet.

Pour les entreprises manufacturières, les réseaux de capteurs permettront de suivre le procédé de production à partir des matières premières jusqu'au produit final livré. Grâce aux réseaux de capteurs, les entreprises pourraient offrir une meilleure qualité de service tout en réduisant leurs coûts [18]

3-2 Topologies d'un RCSF

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

3-2.1 Topologie hiérarchique (à base de cluster)

Dans cette architecture, le réseau est constitué d'un ensemble de groupe de capteurs (cluster), dans chaque cluster un chef de groupe appelé *Cluster-Head* a la responsabilité de collecter et gérer les informations à partir de ces nœuds membres, par la suite agréger ces données et les envoyer à la station de base.

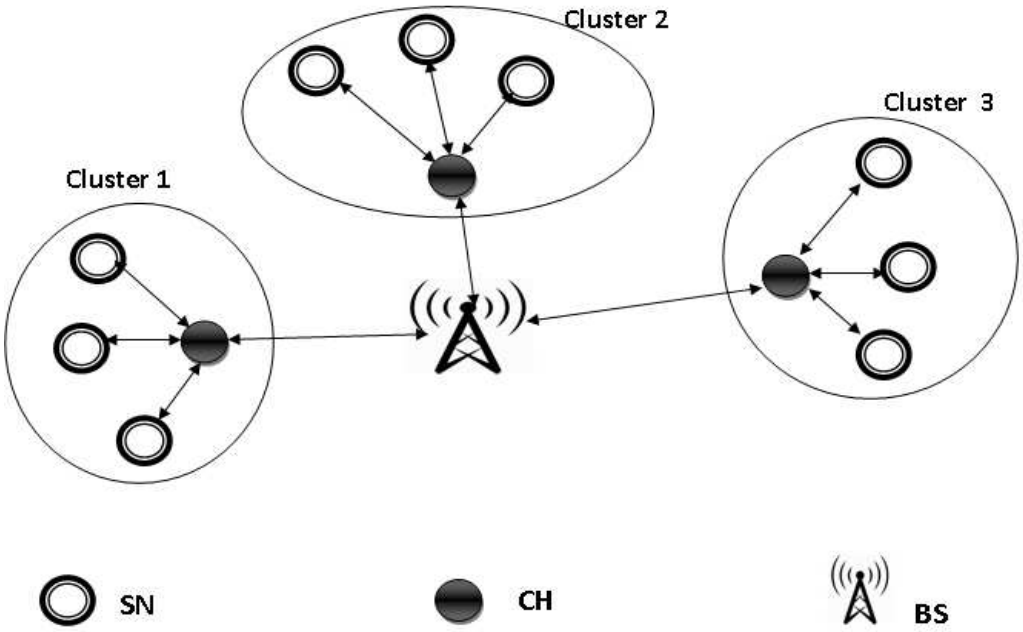

Figure 1-4 : Modèle de la topologie hiérarchique.

3-2.2 La topologie plate

Tous les nœuds dans le réseau ont le même niveau de responsabilité. Les capteurs communiquent entre eux afin d'acheminer l'information au nœud centralisé (station de base) via un mode multi-sauts. C'est-à-dire que si un nœud veut envoyer un message vers la station de base et que celle-ci est en dehors de sa portée radio, il envoie son message à un nœud intermédiaire (dans sa portée radio) pour passer le message et la même procédure se répète récursivement, jusqu'à ce que le message arrive à la station de base.

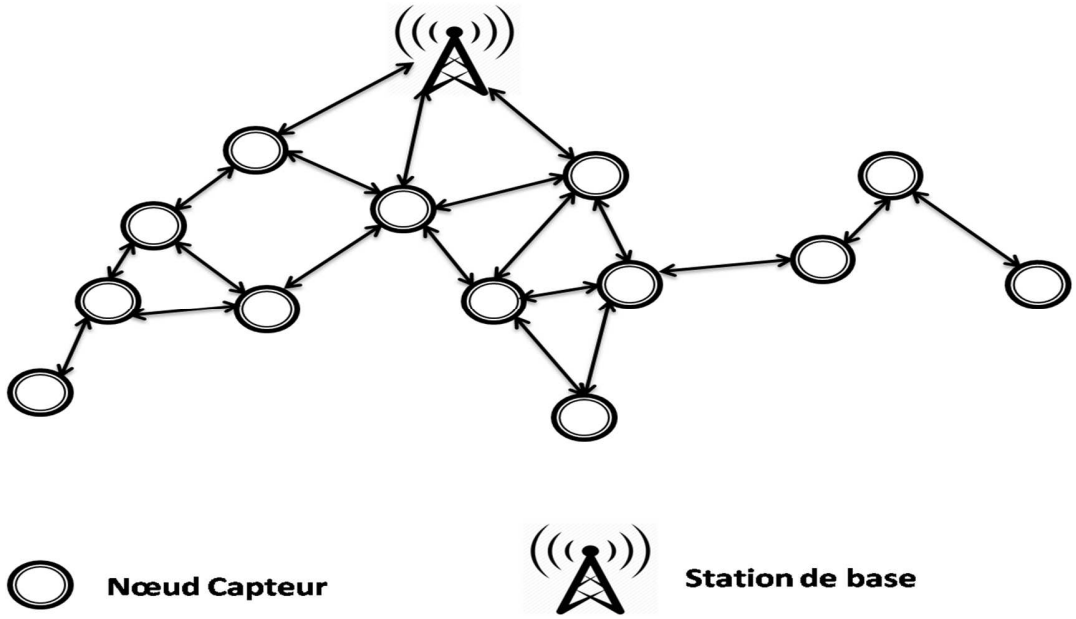

Figure 1-5 : Modèle de la topologie Plate

3-3 Système d'exploitation conçus pour les RCSF

Les systèmes d'exploitation destinés aux réseaux de capteurs doivent être de petite taille à cause des limitations en ressources physiques, mais avec plus de performances en temps d'exécution, en occupation de mémoire et en gestion d'énergie. Comme exemple d'OS pour les réseaux de capteurs nous pouvons citer :

3-3.1 Contiki

Est un système d'exploitation léger et flexible écrit en langage C, portable et open source pour capteurs miniatures. Contiki est spécialement conçu pour respecter les contraintes des RCSFs, en particulier, celles qui sont liées aux limitations de l'espace mémoire (il en occupe environ 32 kilooctets de ROM et 4 kilooctets de RAM).

Contiki est constitué d'un noyau, de bibliothèques, d'un ordonnanceur et d'un jeu de processus. Comme tout système d'exploitation, son rôle est de gérer les ressources physiques telles que le processeur, la mémoire, les périphériques informatiques (d'entrées/sorties). Il fournit ensuite aux applications informatiques des interfaces permettant d'utiliser ces ressources. Conçu pour les modules de capteurs sans-fil

Pour la communication, Contiki implémente deux mécanismes : Rime et uIP. Le premier mécanisme consiste en une couche située juste au-dessous des applications, le deuxième mécanisme (uIP : micro IP) est une implémentation adaptée d'une pile protocolaire basée IP (les protocoles : TCP (Transmission Control Protocol), UDP (User Datagram Protocol), IP (Internet Protocol), ICMP (Internet Control Message Protocol)). L'adoption de tel mécanisme de communication rend possible la communication directe entre un capteur et n'importe quel hôte IP.Contiki pourrait être le meilleur choix lorsque la flexibilité est le plus important, par exemple lorsque le logiciel du nœud doit être mis à jour souvent pour une grande quantité de nœuds.

3-3.2 Tinyos OS

TinyOS est un système d'exploitation open source pour les réseaux de capteurs sans fil qui trouve sa genèse au sein du laboratoire d'informatique de l'université de Berkeley et qui a été l'un des premiers systèmes d'exploitation conçus pour les réseaux de capteurs miniatures. En effet, TinyOS est le plus répandu des OS pour les réseaux de capteurs sans fil. Il est capable d'intégrer très rapidement les innovations en relation avec l'avancement des applications et des réseaux eux-mêmes tout en minimisant la taille du code source en raison des problèmes inhérents de mémoire dans les réseaux de capteurs.

Les applications de TinyOS sont écrites en langage déprogrammation NesC (Network Embedded System C), une extension du langage programmation C., l'utilisation du langage NesC permet l'optimisation du code et par suite réduit l'usage de la mémoire à accès aléatoire (RAM).

3-3.3 MantisOS

MANTIS (MultimodAlNeTworks of In-situ micro Sensor) OS apparu en 2005, a été conçu par l'université du Colorado. C'est un système d'exploitation léger et multitâche pour les capteurs, adapté aux applications où plusieurs traitements, chacun associé à un ou plusieurs processus, sont en concurrence pour accéder aux ressources du capteur sans fil. Il dispose d'un environnement de développement Linux et Windows.

La programmation d'application sur MANTIS OS se fait en langage C, son empreinte mémoire est faible : 500 octets en mémoire RAM et 14kilo-octets en mémoire flash. C'est un système modulaire dont le noyau supporte également des entrées/sorties synchrones et un ensemble de primitives de concurrence, l'économie d'énergie est réalisée par MANTIS à l'aide

d'une fonction de veille appelée sleep function qui désactive le capteur lorsque toutes les taches actives sont terminées, MANTIS est un système dynamique ou les modifications applicatives peuvent être réalisées pendant le fonctionnement

.

4 Conclusion

Dans ce chapitre, nous avons essayé de donner quelques généralités sur les réseaux de capteurs sans fils que nous avons considéré comme un cas particulier de réseaux Ad-hoc. Pour cela, nous avons décrit les principaux concepts liés aux réseaux de capteurs sans fil tels que : l'architecture, les domaines d'applications, les topologies, les systèmes d'exploitations dédies au ce type de réseau. Le chapitre suivant sera consacré à l'étude de la sécurité dans les réseaux de capteurs sans fil.

Chapitre 2

LA SECURITE DANS LES RCSF

1. Introduction

Ces dernières années, Les besoins de sécuriser des communications dans RCSF sont en croissance. Ils varient d'un domaine d'application à un autre, par exemple, les sites industriels et militaires exigent un niveau élevé d'authentification et de confidentialité des communications. Tandis que d'autres domaines comme les applications environnementales, exigent l'intégrité et la fiabilité des communications.

Dans ce chapitre, nous commençons par présenter les contraintes et les exigences de sécurité dans les RCSF, ensuite nous abordons la cryptographie et ses primitives utilisés pour protéger les communications sans fil. Nous concluons ce chapitre en présentant les définitions et la classification des attaques dans les RCSF.

2. Les contraintes de la sécurité dans les RCSF

Le déploiement des nœuds capteurs dans des endroits ouverts, inaccessibles et hostiles, rendent les réseaux de capteurs exposés à de nombreuses attaques. La sécurisation de ce type de réseau reste un problème difficile due à des contraintes suivantes :

2.1. La contrainte des ressources

L'énergie, la mémoire de données, l'espace du code sont des ressources clés pour la mise en œuvre d'un mécanisme de sécurité efficace, Toutefois, ces ressources sont très limitées dans les nœuds capteurs sans fils.

Le tableau 2-1 Présente des limitations physiques pour quelques nœuds capteurs.

	Tmote SKY	MicaZ	Sun-SPOT	Intel® Mote 2	TelosB
CPU	8 MHz	16 MHz	180 MHz	13-416 MHz	8 MHz
Mémoire Flash	48 Ko	128 Ko	4 Mega	32 Mega	48 Ko
RAM	10 Ko	4 Ko	512 Ko	256 Ko	10 Ko

Tableau 2-1 : Limitations physiques pour quelques nœuds capteurs

2.1.1. Limitation en énergie :

Il est à noter que l'énergie est la ressource qui doit être gérer avec une grande attention. Le remplacement de la batterie est difficile (exemple : applications militaires) ce qui fait que la durée de vie du réseau dépende grandement de la durée de vie des batteries des nœuds capteurs. Le besoin à l'énergie est résumé dans la puissance supplémentaire consommée par les nœuds capteurs en raison du traitement requis par les exigences de sécurité. En plus, l'impact énergétique du code de sécurité ajouté dans les nœuds capteurs doit être pris en compte des chercheurs.

2.1.2. Limitation de la mémoire et de l'espace de stockage

Le nœud capteur contient une mémoire très limitée. Ceci signifie qu'un mécanisme complexe de sécurité pourrait avoir un nombre d'instructions trop grand et donc réserver trop de mémoire, et ne laisser que très peu de mémoire pour d'autres opérations pour le nœud capteur. Ainsi, la taille du code de sécurité doit être la plus petite possible et le nombre de clés stockées doit être également petit.

2.2. Manque de fiabilité de communication

Un canal sans fil est un moyen de communication ouvert accessible par toute personne qui se trouve dans la portée du signal.

Cependant, ce moyen est à son tour un obstacle pour la sécurité, rendant facile la production des attaques sur le réseau de capteurs.

2.3. Fonctionnement sans surveillance

Chapitre 2 : La sécurité dans les RCSF

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

2.4. Exposition aux attaques physiques

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

2.5. Gestion à distance

Etant donnée l'environnement ouvert de déploiement des nœuds et le manque de la surveillance humaine, il est important de gérer à distance les nœuds capteurs après leur déploiement. Par exemple, dans un scenario militaire, dans lequel les nœuds de capteurs sont placés derrière les lignes des ennemies pour des missions de reconnaissance, aucun accès direct ne sera possible après le déploiement.

3. Les Exigences de sécurité

Les principales exigences de la sécurité sont :

3.1. Authentification

C'est le mécanisme de vérifier l'identité d'un noud qui veut communiquer avec d'autres nœuds. Il arrive qu'un attaquant puisse forger et injecter des paquets falsifiés dans le réseau, dans ce cas, le noud capteur doit être capable de vérifier la validité d'identité de nœud source.

3.2. Confidentialité

La confidentialité est une point très important dans la communication sans fils des RCSF, elle fait référence à la limitation d'accès à l'information, seules les nœuds et les personnes autorisées peuvent accéder les données échangées dans le réseau et empêcher de ceux qui sont non autorisé. Les données doivent donc être chiffrées.

3.3. Intégrité

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

3.4. Fraîcheur de données :

Ce qui implique que les données doivent être récentes et garantit qu'aucun attaquant ne peut réinjecter les anciens messages. En conséquence, les nœuds capteurs et la station de base doivent établir des mécanismes appropriés pour assurer la fraîcheur des données communiquées.

3.5. Disponibilité :

Cette exigence sert à garantir que les services réseau requis sont disponibles même si le réseau de capteur est ciblé par des attaques comme de déni de service.

4. Classification des attaques

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

4.1. Attaques externes vs attaques internes:

Un attaque externe se produit de l'extérieur du réseau de capteurs .C.-à-d. elles se produisent par des nœuds qui ne sont pas déployées à l'intérieur du réseau et que ne sont pas autorisées à participer dans le réseau. Alors que les attaques internes se produisent par des nœuds internes malveillants.

4.2. Attaque passive vs Attaque active

Les attaques passives ne sont intéressées que par la collecte des informations sensibles sans aucune modification ou influence sur la communication. Ces informations collectées comme la détection des nœuds importants dans le réseau (Cluster-Head) peuvent ensuite aider l'attaquant à de réaliser des attaques malveillantes.

Les attaques actives ont comme objet, la perturbation de la fonction du réseau et de la dégradation de ses performances. L'attaquant tente d'exploiter les failles de sécurité du réseau pour lancer des attaques diverses dans le but de modifier les données.

4.3. Attaque Mote-class vs AttaqueLaptop-class:

Une Attaque Mote-class se produit par un nœud de capteur. C.-à-d. l'équipement d'attaque possède le même type matériel de nœud capteurs ciblé.

Cependant, une attaque Laptop-class utilise des périphériques plus puissants, tel que un ordinateurs portables.

4.4. Attaques physiques vs Attaque à distance

Dans l'attaque physique, un adversaire accède physiquement au nœud de capteur qui est lésé par la falsification ou par la destruction matériel de nœud. En revanche, une attaque à distance est mise en œuvre à partir d'une distance, par exemple, en émettant un signal à haute énergie pour interrompre la communication.

5. Les attaques visant les réseaux de capteurs

La sécurité est un enjeu majeur dans les réseaux de capteurs sans fil qui sont vulnérables à des nombreuses attaques et menaces de sécurité. La nécessité de connaitre l'attaque pour comprendre comment l'attaquant agit et donc savoir comment le protéger.

Nous décrivons dans cette partie les principales attaques contre RCSF.

5.1. Jamming

C'est une attaque de type Déni de Service (DoS) dont le but est de perturber la communication. L'attaquant bloque la réception du canal radio d'un nœud en transmettant sur sa bande de fréquence afin de provoquer des interférences radio.

Il existe différentes stratégies pour l'attaque jamming :

- En émettant un signal radio sans interruption (constant jamming). Cette stratégie nécessitant beaucoup d'énergie.
- En émettant régulièrement à intervalle fixe ou d'une façon aléatoire sur un canal afin de préserver son énergie

- En émettant un signal si le canal est actif (réactive jamming).

5.2. SelectiveForwarding

Dans cette attaque, l'intrus empêche la transmission de certains paquets. Ces derniers seront par la suite supprimés par ce nœud malveillant. Il est à noter que le choix des paquets est basé sur certains critères tel que : le contenu des paquets, adresse source de l'émetteur, ou d'une façon aléatoire. Dans la **Figure 2-1** le nœud malicieux 5 transmet tous les paquets sauf ceux qu'il reçoit du nœud 4, fondée sur l'adresse d'origine.

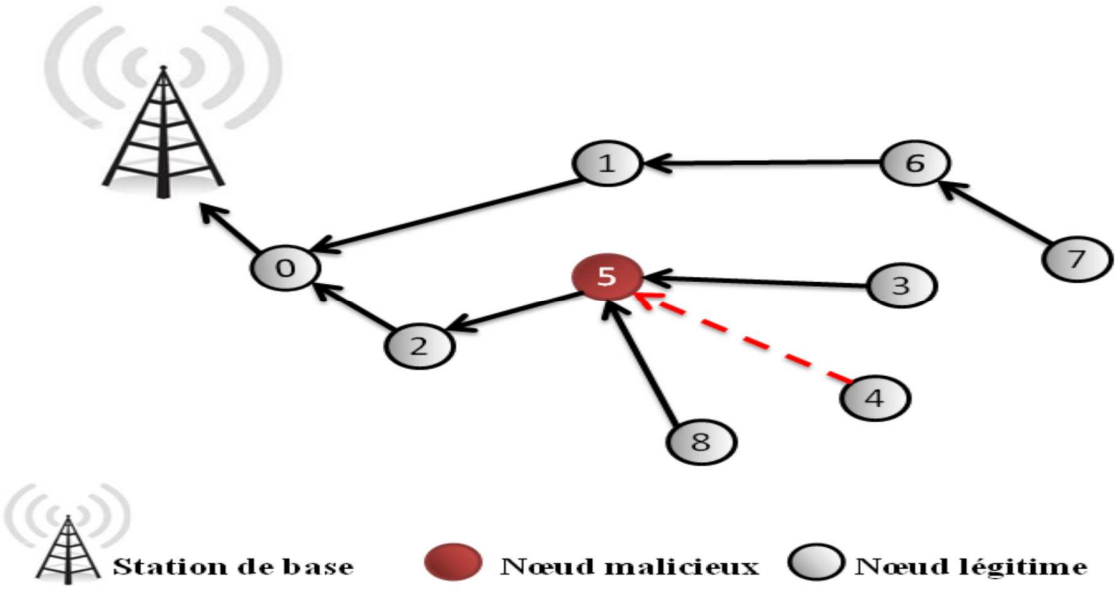

Figure 2-1 : Exemple d'attaque Sélective Forwarding

5.3. Sinkhole

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

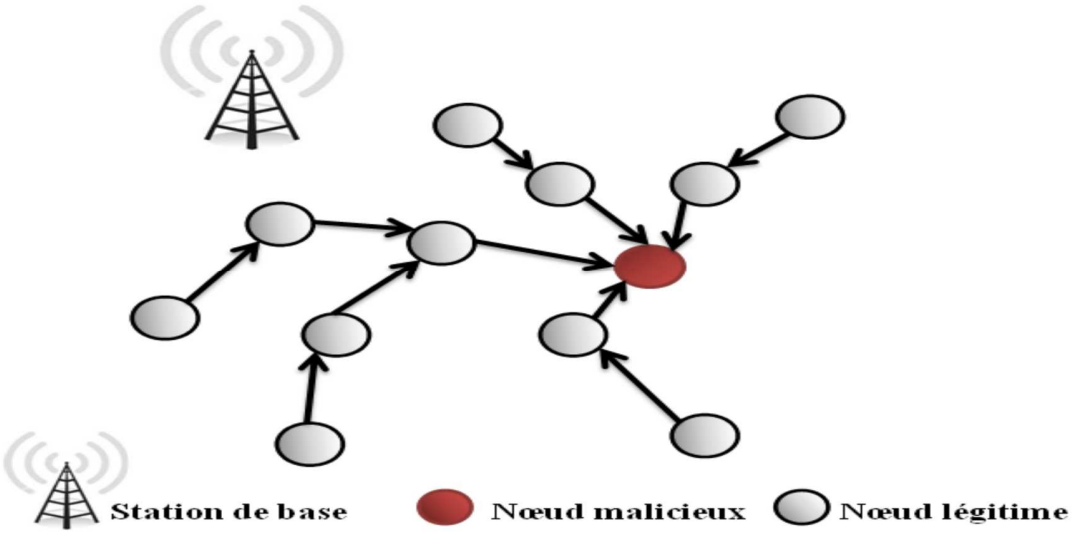

Figure 2-2 : Exemple d'attaque Sinkhole

5.4. Attaque physique (Tampering)

Elle consiste à la capture et à l'accès physique au nœud afin d'extraire toutes les informations importantes comme les clés utilisées pour le chiffrement.

5.5. L'attaque Sybil

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

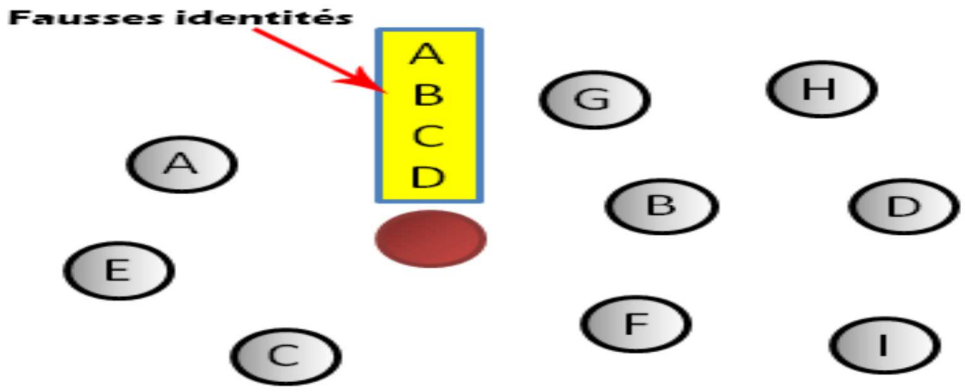

Figure 2-3 : Exemple d'une attaque sybil

5.6. Wormhole

Dans cette attaque, un nœud malicieux enregistre les paquets et les envoie via un lien ou tunnel de faible latence vers un autre nœud malicieux dans le réseau. A l'aide d'un canal filaire ou sans fil à longue portée.

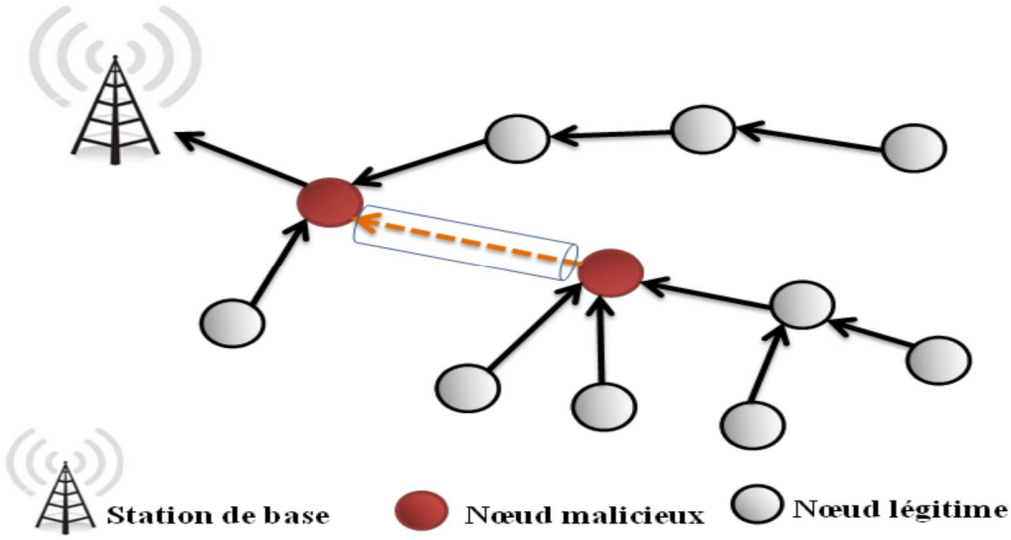

Figure 2-4 : Exemple d'une attaque wormhole

5.7. L'attaque Hello flood

Le nœud malicieux diffuse un message Hello dans le réseau en utilisant une grande énergie d'émission. Par conséquent, tous les nœuds qui réceptionnent le message essayeront de transmettre leurs paquets à travers le nœud malveillant. Le but de cette attaque consiste à consommer l'énergie des nœuds et empêcher leurs messages d'être échangés.

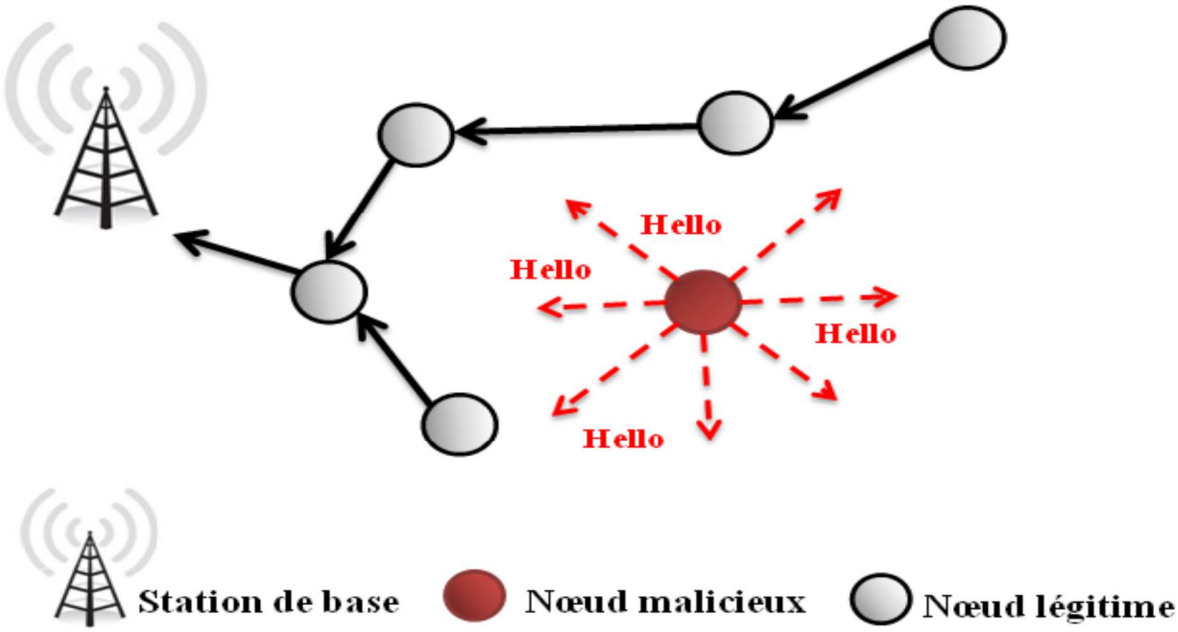

Figure 2-5 : Exemple d'une attaque Hello Flood

5.8. Attaque par rejeu(replay)

Est une forme d'attaque réseau dans laquelle l'intrus peut injecter des précédents échanges interceptés par celui-ci. Cette attaque vise la fraicheur de données.

5.9. Réplication de nœuds

Elle consiste à capturer un nœud, construire des copies légitimes de ce dernier et les ajouter partout au réseau créant ainsi des identités multiples utilisant la même cryptographie que le nœud légitime original.

Chapitre 2 : La sécurité dans les RCSF

6. Primitives cryptographiques utilisées dans les RCSF

Plusieurs mécanismes basés généralement sur la notion de cryptographie, sont mis en place afin de répondre à la question de la sécurité dans les RCSF. Le chiffrement et le déchiffrement des messages sont effectuées par des algorithmes cryptographiques.
Ces algorithmes reposent généralement sur des problèmes mathématiques complexes et difficiles à résoudre.

Nous présentons par la suite, les différentes primitives cryptographiques qui sont utilisées dans les réseaux de capteurs sans fil.

6.1. La cryptographie

Le mot « cryptographie » est composé des mots grecs: « crypto » signifie caché et «graphy» qui signifie écrire. La cryptographie est définie comme étant une science permettant de protéger une communication et d'assurer que l'information contenue dans un message n'est révélée qu'au destinataire de ce message. On distingue deux familles de cryptographie : La cryptographie symétrique et la cryptographie asymétrique

6.1.1. Cryptographie symétrique

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

Avantages :

- L'avantage principal de ce mode de chiffrement est sa rapidité.
- Pas d'opérations mathématiques complexes pour crypter ou décrypter les données.
- Pas de grandes dissipations énergétiques durant les phases de chiffrement et de déchiffrement.
- Plus adapté pour les RCSF.

Inconvénients :

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

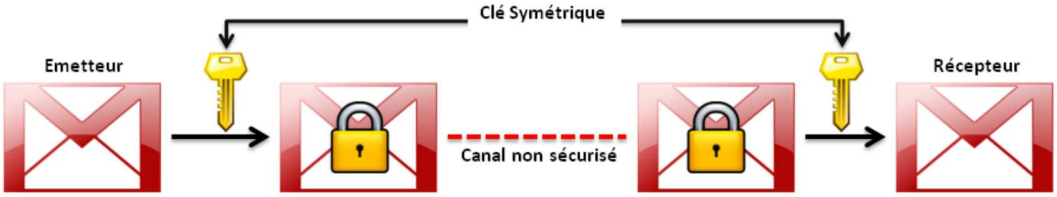

Figure 2-6 : Le chiffrement symétrique

6.1.2. Cryptographie asymétrique

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

Figure 2-7 : Le chiffrement asymétrique

6.2. La fonction de hachage

Elle permet de générer une chaîne de taille inférieure et généralement fixe à partir d'une chaîne de longueur quelconque. Par conséquent, la chaîne résultante est appelée empreinte (digest en anglais). D'un autre cotée, une fonction de hachage est une fonction à sens unique,

autrement dit qu'il est facile à calculer l'empreinte d'une chaîne donnée, mais il est impossible de déduire à la chaîne initiale à partir d'une empreinte donnée.

Cette fonction est utilisée pour la vérification de l'intégrité des messages transmis

L'émetteur utilise la fonction de hachage pour créer une empreinte du message transmettre, puis il transmet le message et l'empreinte vers le récepteur. A la réception du message, le récepteur calcule l'empreinte du message reçu et il la compare à l'empreinte initiale. Si les deux empreintes correspondent, c'est que le message n'a pu être altéré.

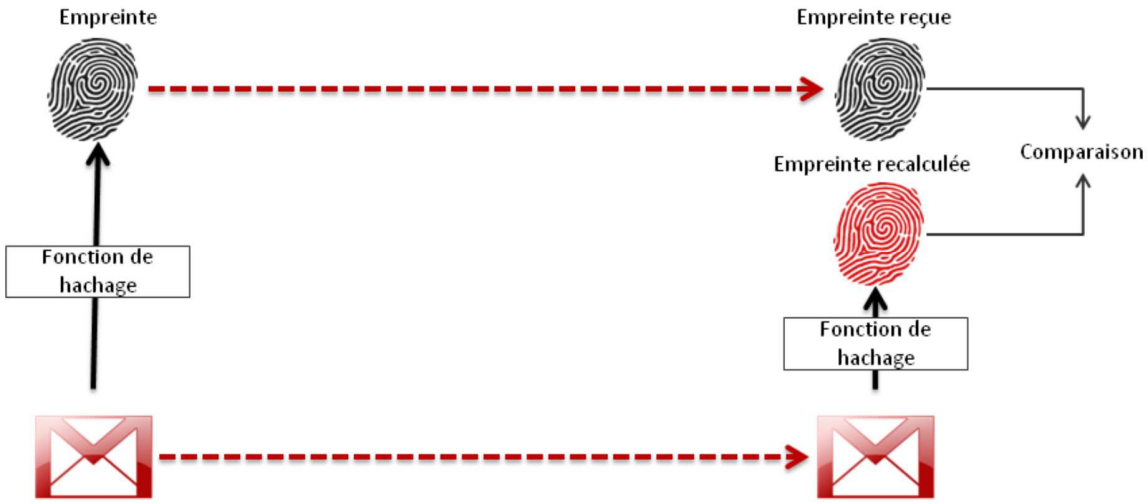

Figure 2-8 : La fonction de hachage

6.3. Code d'authentification de message

Le code d'authentification de message MAC (Message Authentication Code) fait partie des fonctions de hachage (C'est le mécanisme qui assure l'intégrité de données. Cette fonction calcule une courte empreinte de taille fixe à partir d'une donnée de taille arbitraire) à clé symétrique assurant l'intégrité des données comme toute autre fonction de hachage, en plus, l'authenticité de la source de données.

Comme illustré dans la figure 2-9, cette clé est utilisée pour calculer le code MAC par l'émetteur (1). Ce code est par la suite envoyé avec les données (2).

Le récepteur calcule à son tour le code MAC avec cette même clé et le compare au code qu'il a reçu (3). S'ils sont bien identiques (4), alors la source est authentique et les données n'ont pas été altérées.

6.4.Le système de détection d'intrusion

Le système de détection d'intrusion (IDS : *Intrusion Detection System*)est capable de détecter avec une grande précision les attaques internes. Ce mécanisme permet de détecter les

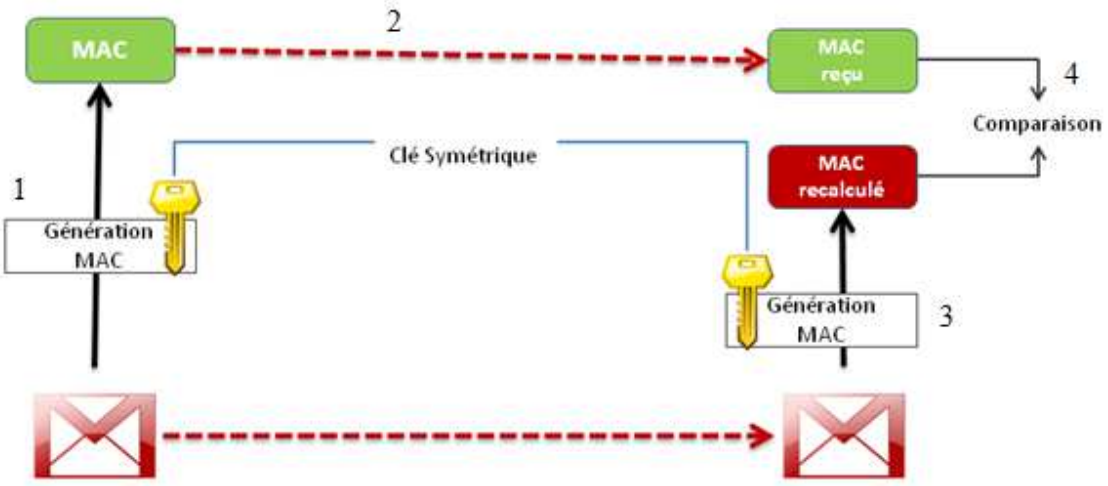

Figure 2-9 : Code d'authentification de messages MAC

activités anormales ou suspectes sur la cible analysée et déclenchera une alarme lorsqu'un comportement malveillant se produit. Les IDS utilisent différents mécanismes pour déceler les attaques:

- les signatures.
- la recherche de motif(détection d'anomalie).

6.4.1. IDS basé scénarios (signatures)

Les IDS basés sur les scénarios sont des IDS avec base de connaissance des signatures d'attaques connues, grâce à sa base de données, ce type de système détecte facilement et rapidement les attaques et menaces présentes dans un flux réseau ou sur une machine. Il présente

néanmoins des limites : si l'attaque n'est pas connue, le système ne détecte rien, donc des mises à jour fréquentes doivent être faites sur ces bases pour qu'ils restent performants.

6.4.2. IDS basé sur l'approche comportementale

Il nécessite un entrainement fait à partir du comportement normal d'un trafic réseau.
Ce type IDS utilise des méthodes de calcul probabiliste, qui associé à des méthodes de classifications de données, permettent de déterminer qu'une attaque a lieu ou non à partir d'un flux réseau. Ce système ne nécessite aucune mise à jour et est capable de détecter de nouvelles attaques.

7. Conclusion

A travers ce chapitre, nous avons présenté les exigences de sécurité, la classification des attaques, les contraintes de la sécurité, les différents types d'attaques.
Il est clair que les mécanismes de sécurité utilisées dans les réseaux traditionnels ne peuvent pas être directement appliquées aux RCSF, vu les contrainte de sécurité qui caractérise ce type de réseau. En conséquence, les RCSF exigent donc le développement des mécanismes de sécurité tiennent compte de leurs caractéristiques et de leurs vulnérabilités

Chapitre 3

PROPOSITION POUR SECURISER LA COMMUNICATION DANS RCSF

1. Introduction

Les nœuds capteurs sont généralement déployés dans des zones non surveillées, la plupart des applications des RCSFs nécessitent un haut niveau de sécurité pour fournir les exigences de sécurité de base et rendre ces applications invulnérables aux différentes attaques, empêchant un intrus de perturber le bien fonctionnement du réseau en prenant le contrôle des nœuds de capteurs. Un autre problème important qui affecte l'utilisation des RCSFs est la sécurité des communications sans fil. Par nature, les communications sur les canaux sans fil ne sont pas sécurisées et permettent aux intrus d'espionner, d'altérer ou d'injecter des données dans le réseau.

Dans ce Chapitre nous présenterons notre proposition pour sécuriser la communication et la transmission des données dans les réseaux de capteurs à architecture hiérarchique (Cluster-Based). Cette proposition répond aux exigences de sécurité comme : l'authentification, la confidentialité, l'intégrité et la fraicheur des données. En plus, elle prend en considération les contraintes de limitation des ressources énergétiques et physiques d'un nœud capteur.

2. Modèles et hypothèses

Avant de présenter le détail du notre proposition, nous présenterons dans ce qui suit les notations utilisées, le modèle de l'attaquant ainsi que les hypothèses liées au RCSF.

2.1. Notation

Les notations utilisées dans le reste de ce chapitre sont :

SB	*Station de Base*
CH	*Cluster-Head qui joue le rôle de chef du cluster*
SN	*Nœud capteur*
Idi	*Identité de nœud i de taille 1 Byte*
A || B	*Concaténation de l'information A avec l'information B*
M	*Message en claire de taille 16 Byte*
K	*Clé symétrique de taille 16 Byte*
C	*Message Crypté de taille 16 Byte*
Temp	*La valeur de température captée par SN*
DATA	*Le paquet envoyé par les SN et les CH*
N	*Un nonce généré contient le Numéro message à envoyer*
MAC	*Code d'authentification du message M de taille 4 Byte*
H (K, M)	*Fonction de hachage du message M utilisant la clé K*
Enc(K , M)	*Fonction symétrique de chiffrement du message M utilisant la clé K*
Dec(K , C)	*Fonction symétrique de Déchiffrement du message C utilisant la clé K*

Tableau 3-1 : Notation

2.2. Modèle de l'attaquant

Nous considérons qu'un attaquant peut être passif ou actif durant le fonctionnement du réseau.

2.3. Modèle du réseau

Nous considérons un réseau de capteurs à architecture clustérisée, le réseau est composé d'une station de base, plusieurs clusters où chaque cluster est constitué de plusieurs nœuds capteurs (SensorNode : SN) statiques, et un Chef de cluster (Cluster Head : CH**)** qui jouera le rôle de l'agrégateur.

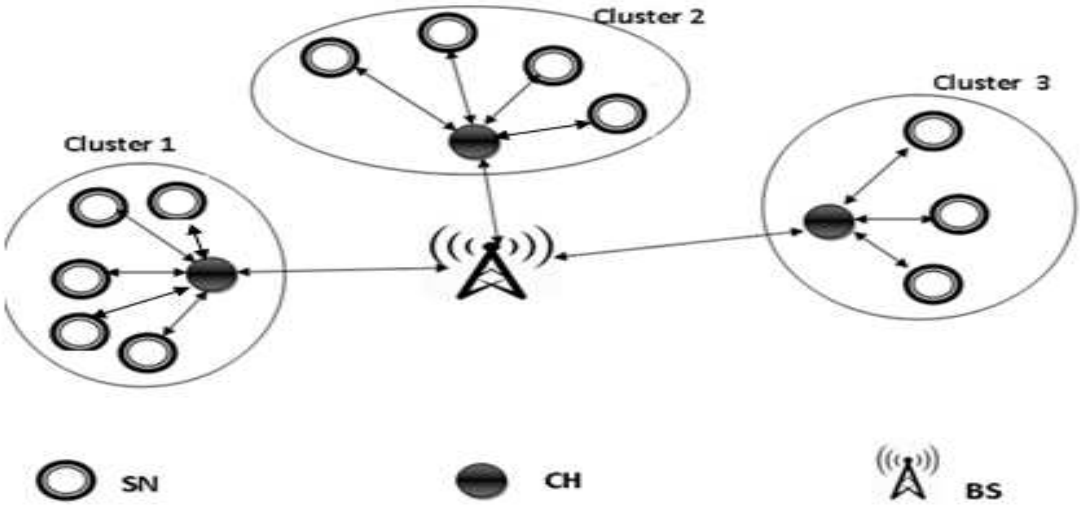

Figure 3-1 : Model du réseau

Les nœuds de réseau servent à récolter des données comme un relevé de température. Les nœuds membres (SN), sont chargés de capter et envoyer la température chaque 30 seconde vers le CH. Tandis que le rôle de Chef de cluster CH est de recevoir tous les données viennent de ses SN, calculer le moyenne de température et l'envoyer vers la station de base SB. Il est à noter que aucune communication direct entre les SN ou entre Les SN et la SB**,** toutes communication doit passer par les CH**.**

Les nœuds capteurs sont homogènes en termes de capacité de traitement, de communication, d'énergie et de stockage. Cependant la station de base possède des ressources illimitées, elle est digne de confiance et responsable de la configuration des nœuds avant le déploiement.

Nous supposons que les clés symétrique utilisées pour les nœuds membres, les CH et la SB sont générées par la station de base et avant le déploiement. La SB et les nœuds de capteurs ne sont pas mobiles.

3. Objectifs de notre proposition

En prenant en considération les contraintes de limitation des ressources énergétiques et physiques, nous avons proposé un mécanisme de sécurité léger qui puisse atteindre les objectifs suivants :

- Sécuriser la communication entre la SB, CH, et les SN en assurant les exigences de sécurité : l'authentification, la confidentialité, l'intégrité et la fraicheur des messages.
- Faire face aux différents d'attaques passives et actives tel que l'attaque de déni de service (DoS) et l'attaque par rejeu.

4. Solution proposée

Notre proposition consiste de 03 phases :

4.1. Phase d'initialisation (avant la distribution des nœuds) :

Dans cette phase la SB utilise le protocole de routage *Routing Protocol for Low Power and Lossy network* (RPL) qui commence par la création d'un *Destination OrientedDirectedAcyclic Graph* (DODAG) orienté vers la SB puis la SB et les CH diffuse ses identités pour être connu par les SN.

Chaque SN est pré-chargé par une clé symétrique $K_{SN\text{-}CH,}$ partagée avec son CH afin de sécuriser la communication SN-CH.

4.2. Phase de transmission de données par SN :

Nous pouvons deviser cette phase en quatre étapes :

Etape 1 :

Chaque SN calcule un MAC (Code d'authentification du message**)**à partir de message claire M qui contient la valeur de température captée et l'ID de SN : **(M = Temp || ID)** et

MAC = H (M,$K_{SN\text{-}CH}$). Il à noter que la taille de MAC est 4 Bytes [21]

Etape 2 :

Chaque SN Chiffre son message M en utilisant l'algorithme symétrique AES-128 bits avec uneclé symétrique $K_{SN\text{-}CH}$

C = Enc(M, $K_{SN\text{-}CH}$).

Etape 3 :

Chaque SN génère un nonce N qui contient un numéro de séquence de message à envoyer.

Etape 4 :

Chaque SN génère un paquet **DATA** de taille de 22 Byte, à envoyer vers son CH en concaténant le message crypté C, un MAC, un numéro de séquence N et ID de SN.

Le format finale de DATA est**: DATA = C || MAC || N || ID**

4.3. Phase de réception par le CH :

Nous pouvons aussi deviser cette phase en trois étapes :

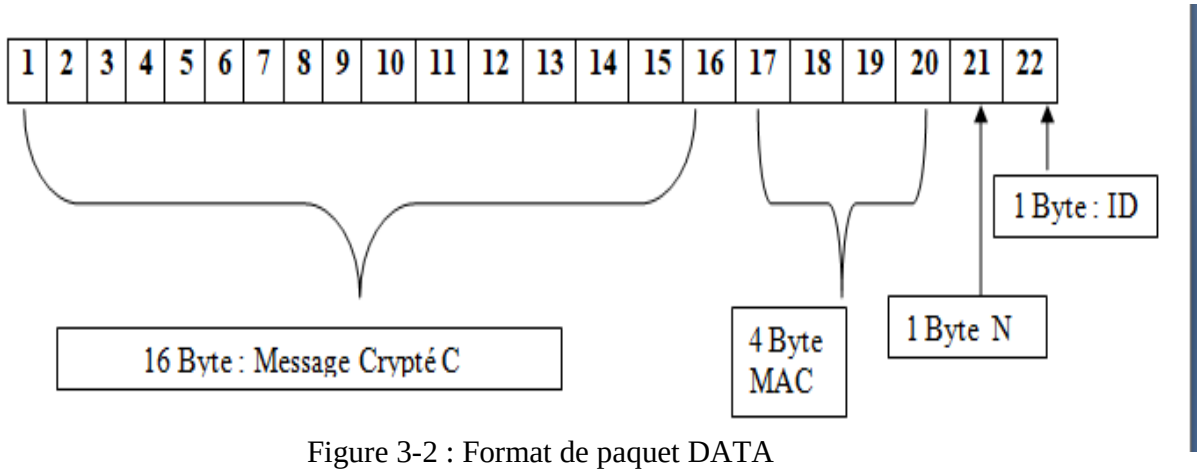

Figure 3-2 : Format de paquet DATA

Etape 1 : Une fois le CH reçu le paquet DATA provenant de son SN, il déchiffre de 16 premiers Bytes de paquet qui contient le message C en utilisant l'algorithme symétrique AES-128 bits et sa clé symétrique K_{SN-CH}

$M = Dec (K_{SN-CH}, C)$

Etape 2 : Apres le déchiffrement, le CH calcule le MAC2 à partir de message déchiffrée M en utilisant la même fonction de hachage H utilisé par le SN

$MAC2 = H (M,K_{SN-CH})$

Ensuite Le CH vérifie MAC2 avec le MAC reçu dans le paquet (Les 4 Bytes après le message C).

- Si MAC2 ≠ MAC : le message est modifié donc le paquet sera rejeté par le CH.
- Si MAC2 = MAC : Le paquet est accepté, donc l'intégrité de données est assurée.

Etape 3 : Apres la vérification de MAC, le CH vérifiera le numéro de séquence de message (le Byte N° 21 dans le paquet DATA) et le comparée avec le dernier numéro de message N1 arrivé par le même SN

- Si N <= N1 donc un attaque rejeu est détecté, et ensuite le paquet sera rejeté.
- Si N > N1 donc la fraicheur de message est assurée.
- La figure 3-3 représente le fonctionnement de notre proposition

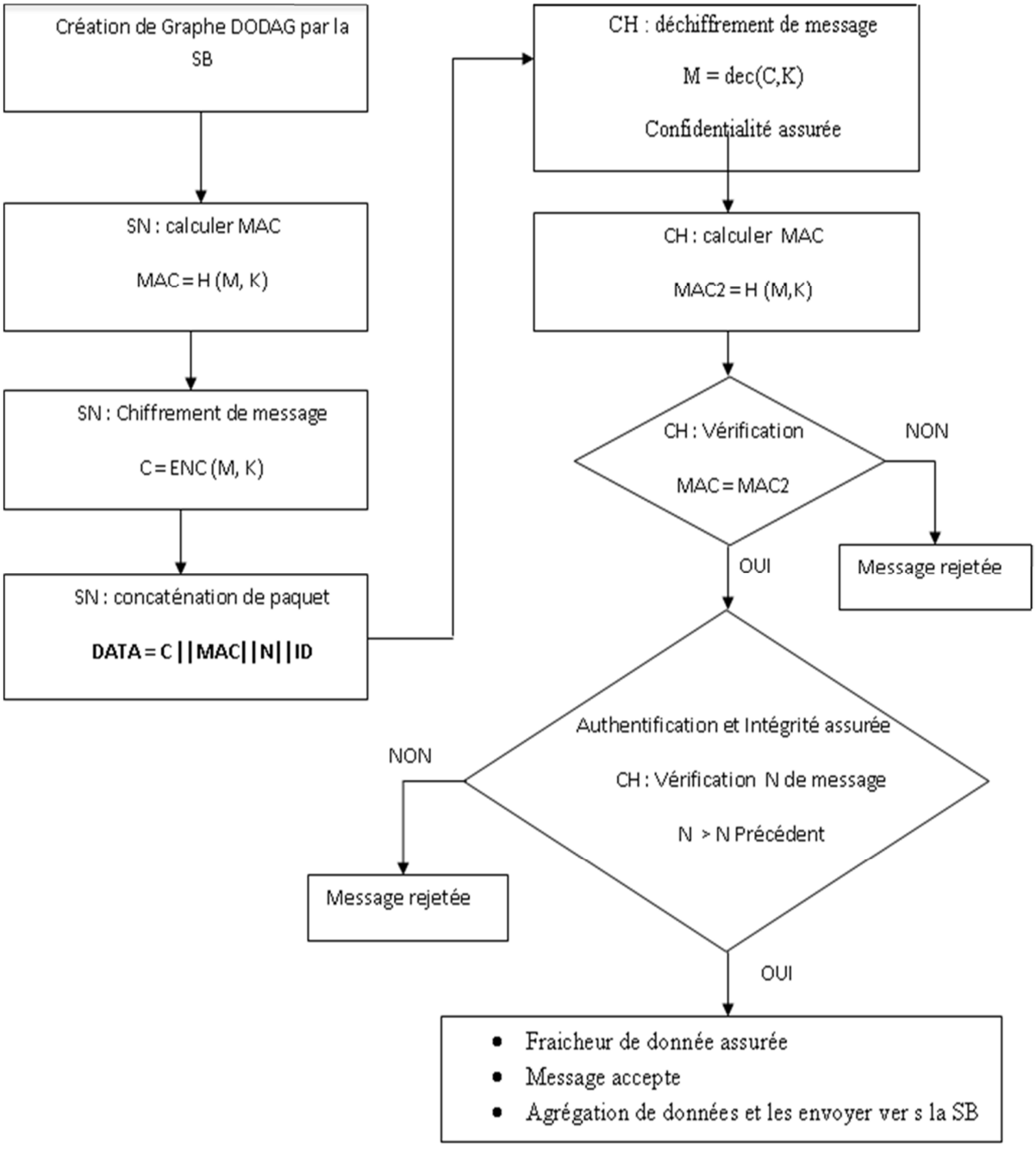

Figure 3-3: Fonctionnement de notre proposition

5. Analyse théorique de la sécurité

Notre proposition assure la confidentialité, car tous les messages échangés dans le réseau, sont chiffrés. Ainsi il peut garantir la fraîcheur, l'intégrité et l'authentification du nœud originaire du message transmis en ajoutant un nonce N et un MAC au message envoyé. Notre proposition permet également de faire face aux attaques qui sont fréquemment menées dans RCSF, parmi ces attaques:

Attaque d'écoute (eavesdropping)

Ce type d'attaque vise la confidentialité des messages. Elle permet à l'adversaire d'écouter facilement les transmissions pour récupérer par la suite le contenu des messages circulant dans le réseau. Notre proposition évite cette attaque par l'utilisation du chiffrement à clé symétrique.

Modification/insertion des données

Cette attaque vise l'intégrité des données. L'adversaire peut altérer les messages transmis par le nœud membre dans le but de falsifier le résultat d'agrégation, par conséquent, le CH accepte les données altérées par l'adversaire et les agrège. Ainsi, le résultat final est forcément erroné. La solution proposée permet de lutter contre cette attaque car le message est protégé par un MAC.

L'attaque par rejeu

Ce type d'attaque vise la fraicheur des messages. Dans notre proposition, les messages précédents interceptés par un intrus, ne peuvent être réinjectés puisque chaque message transmis contient un numéro de séquence de message.

6. Simulation et évaluation des performances

Dans cette section nous allons d'abord présenter l'environnement de simulation par la suite, nous exposons un aperçu sur l'implémentation de notre proposition pour sécuriser la communication. Nous allons présenter les résultats de simulation, puis nous présentons les métriques de performances mesurées, les paramètres de simulation, ainsi que l'interprétation des résultats obtenus à l'issue de simulation.

6.1. L'environnement de simulation

Dans cette section, nous faisons une brève présentation du système d'exploitation ContikiOS et de son simulateur réseau Cooja utilisé pour effectuer nos simulations.

6.1.1. Le système d'exploitationContiki [19]

Est un système d'exploitation léger et flexible écrit en langage C, portable et open source pour capteurs miniatures. Contiki est spécialement conçu pour respecter les contraintes des RCSFs, en particulier, celles qui sont liées aux limitations de l'espace mémoire (il en occupe environ 32 kilooctets de ROM et 4 KO de RAM), son rôle est de gérer les ressources physiques telles que le processeur, la mémoire, les périphériques informatiques (d'entrées/sorties).

Il fournit également une version implémentée du protocole de routage RPL (Routing over Low power and LossyNetworks) utilisé dans notre proposition. Contiki OS intègre un simulateur de réseau appelé Cooja qui permet d'évaluer différents paramètres d'un réseau de capteurs

6.1.2. Le simulateur Cooja : [20]

Est un simulateur de réseau développé en Java permet l'émulation de différents nœuds capteurs sur lesquels seront chargés un système d'exploitation et des applications. Cooja permet aussi de simuler des connexions réseaux, et d'interagir avec des nœuds capteurs. Cet outil permet aux développeurs de tester les applications à moindre coût. Parmi les nœuds capteurs qui sont supportés à ce jour par Cooja: EXP5438, Z1, WISMOTE, MICAZ, TMOTESKY, ESB.
L'interface de simulateur Cooja est composée de plusieurs fenêtres (plugins) ce qui est illustré dans la Figure 3-4

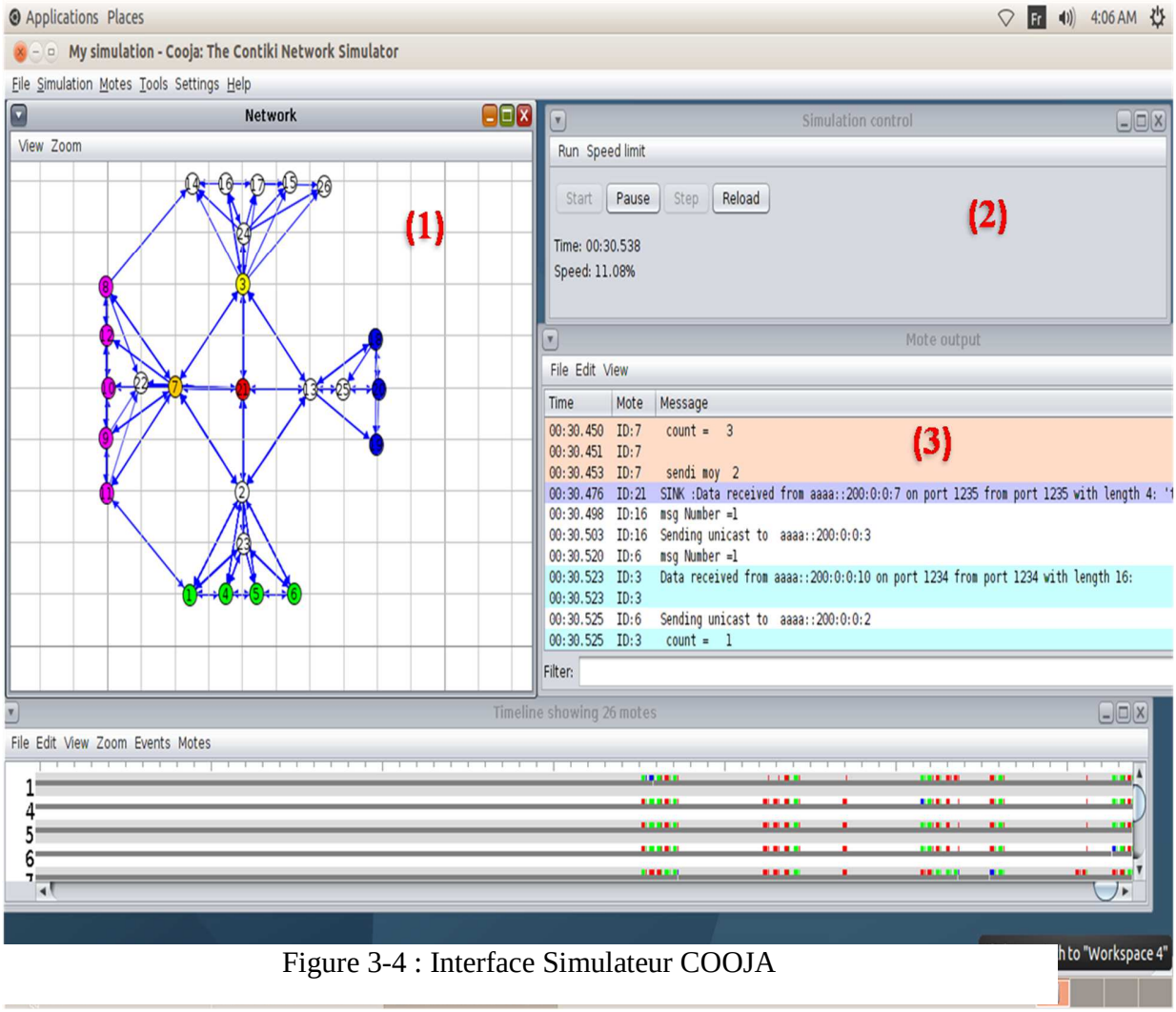

Figure 3-4 : Interface Simulateur COOJA

- **Section 1 :** Network : présente le réseau simulé et le flux de communication durant la simulation.
- **Section 2 :** Simulation control : cette fenêtre contient quatre boutons :

  1) Start : pour démarrer une simulation.

  2) Pause : pour arrêter la simulation.

  3) Reload : pour recharger une simulation.

  4) Step : pour régler la vitesse de la simulation.
- **Section 3 :**Mote output : présente ce que les capteurs génèrent comme sortie via leurs ports séries.

6.2. Implémentations, simulation et évaluation de performances

Afin d'évaluer les performances de notre proposition, nous avons procédé à la comparer avec une autre simulation simple sans chiffrement de données avec les mêmes paramètres et métriques.

6.2.1. paramètres de la simulation utilises

Mobilité	**Statique**
Type de capteur	Wismote
Chip radio	CC2520
Nombre totale des nœuds	21
Nombre de nœud capteur SN	17
Nombre de Cluster Head CH	4
Topologie	Clustérisée
Portée radio d'un capteur	50 Mètres
Taille d'un paquet de données	22 Byte
Durée de la simulation (virtuelle)	05 Minutes
Adressage Réseau	IP V6
Terrain size	1000 X 1000 Mètre
Neouds malicieux	8 nœuds (type d'attaqueDoS / Sybil)

Tableau 3-2 : Paramètres de la simulation

6.2.2. La partie du code

Le code de notre mécanisme comprend trois parties, une partie concerne la station de base BS, une partie concerne le nœud capteur SN et l'autre partie concerne le cluster head.

Partie Station de base :

```
ipaddr = set_global_address();  ……..1

create_rpl_dag(ipaddr);  ……..2

servreg_hack_register(SERVICE_ID, ipaddr);……..3

simple_udp_register(&unicast_connection, 1235,
                    NULL, 1235, receiver);……..4
```

1- Obtention de l'adresse IP V6.
2- Création de graphe DODAG par la SB utilisant le protocole de routage RPL.
3- Déclaration de l'identité de la SB pour être connue par les CH.
4- Création d'un unicast connexion avec le port 1235 et l'adresse IP de la SB pour la transmission et la réception de données.

Chapitre 3 -Proposition pour sécuriser la communication dans RCSF

Partie Nœud Capteur SN :

```
powertrace_start(CLOCK_SECOND * 20);……..1
set_global_address(); ……..2
simple_udp_register(&unicast_connection, UDP_PORT,
                      NULL, UDP_PORT, receiver);……..3

etimer_set(&send_timer, 30);

SENSORS_ACTIVATE(sht11_sensor);……..4
PROCESS_WAIT_EVENT_UNTIL(etimer_expired(&send_timer));…5
addr = servreg_hack_lookup(SERVICE_ID);……..6

val = (sht11_sensor.value(SHT11_SENSOR_TEMP)/100);……..7
sprintf(data, "%d",val); ……..8
h=hash(data, key,4); ……..9
AES_encrypt(key, data); ……..10
memcpy(buf,data,16);……..11
strcat(buf, h); ……12
buf[20]= msg; ……..13
buf[21]= node_id; ……14
simple_udp_sendto(&unicast_connection, buf, sizeof(buf),
addr);……15
```

1- calcul la consommation d'énergie chaque 20 seconde
2- Obtention de l'adresse IP V6.
3- Création d'un unicast connexion pour la transmission de données.
4- Activation de capteur de température.
5- Chaque évènement se déclenche après chaque 30 seconde.
6- Chercher l'adresse IP de CH.
7- capturer la température
8- Copier la valeur de température dans la variable DATA(16 Byte).
9- Calculer le MAC
10- Chiffrer la variable DATA
11- Copier DATA chiffrée dans le Buffer BUF.
12- Ajouter le MAC au Buffer.

13- Copier le numéro de séquence de massage dans le 21eme byte de Buffer.

14- Copier l'ID de SN dans le 22eme byte de Buffer.

15- Envoyer le Buffer vers le CH.

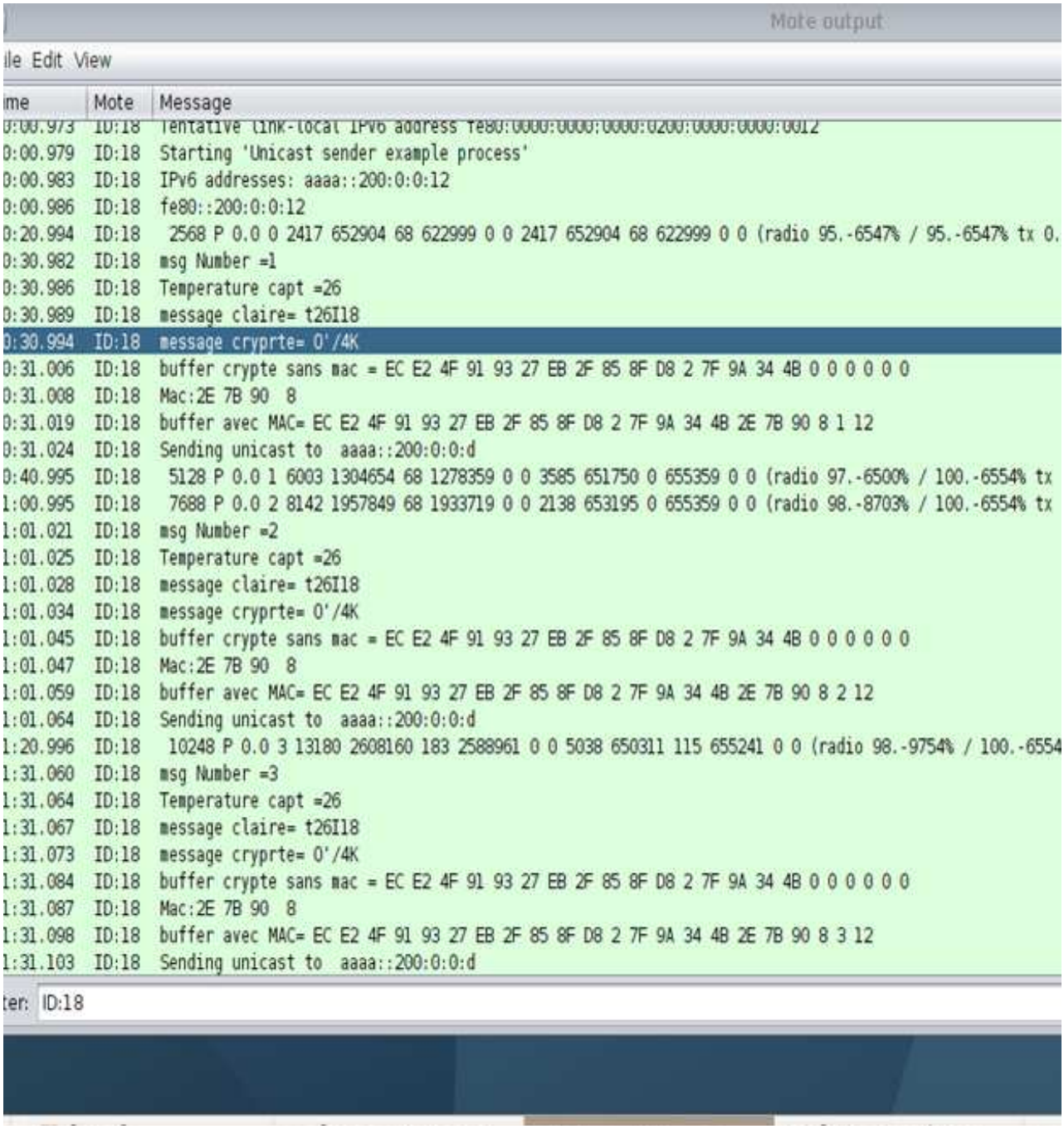

Figure 3-5 : Neuod capteur output

Chapitre 3 -Proposition pour sécuriser la communication dans RCSF

Partie Cluster Head CH:

```
if (msg>msgg[id11]) {printf(" Msg Vérifié avec succès \n");…… 1

AES_decrypt(key,data); ……..……..……..2

h= hash(data, key,4); ……..……..3

int ret = memcmp(h,mac,4);……..4

if (ret==0) {printf("Mac verifier avec succ¡©e \n");}

else {printf("Mac incorrect \n");};……..5

count++; ……..6
if (count == 3 ) {count = 0;moy = (sum/3)
printf(" \n sending  moy %d \n",moy); ……..7

} else

{ sum = sum+ tmp;}
```

1- Vérification de numéro de message arrivée avec le dernier message reçu.
2- Déchiffrement de 16 premiers Bytes Reçus qui contient la valeur de température.
3- Calculer le MAC de DATA déchiffrée.
4- Comparaison le MAC reçu avec le MAC Calculé(h).
5- Si MAC = h, le message est accepté sinon le message est rejeté.
6- Incrémenter le conteur de message reçu.
7- Si le CH reçoit les messages de tous ses SN, il calcule et envoie la moyenne vers la SB

Chapitre 3 -Proposition pour sécuriser la communication dans RCSF

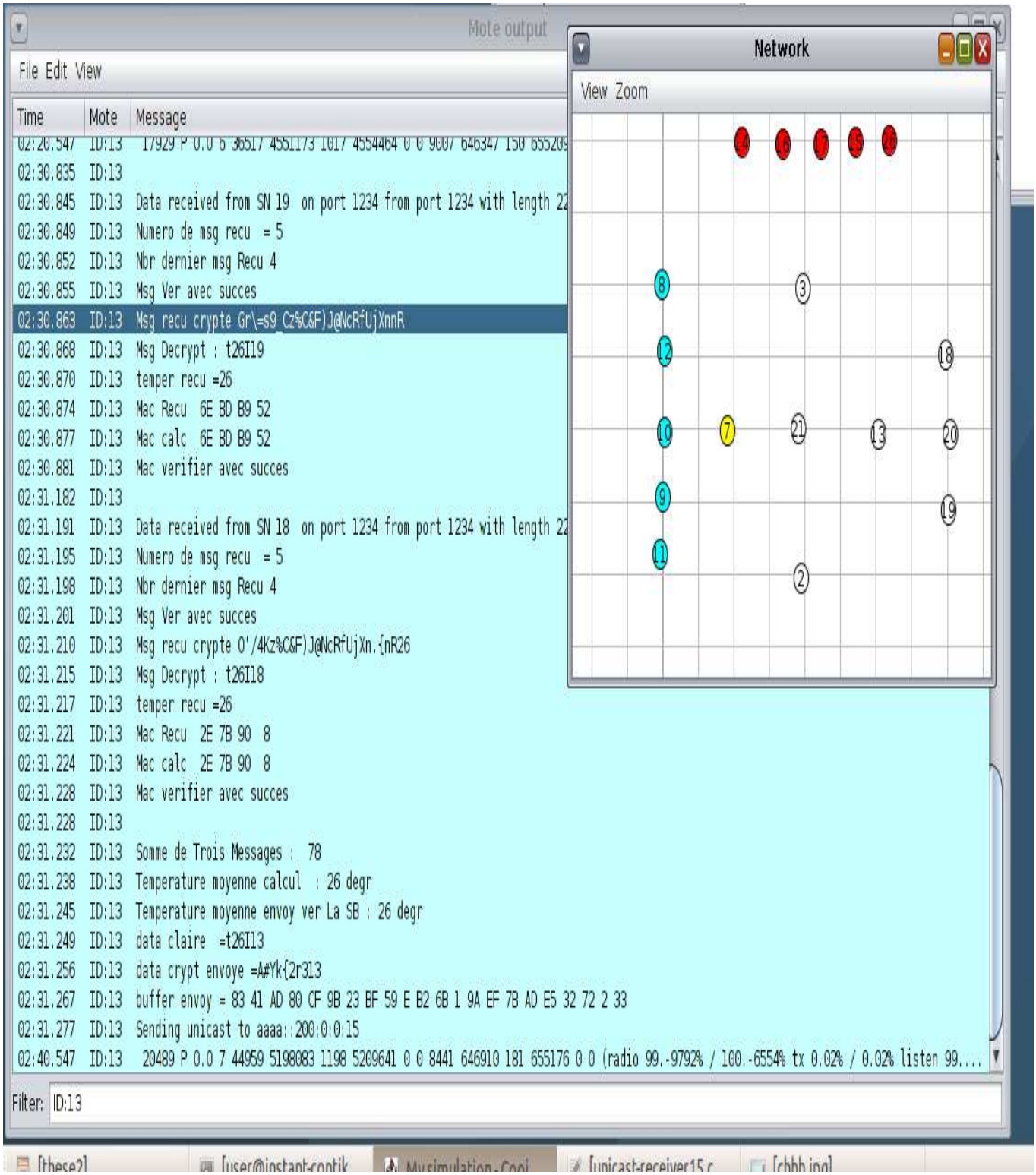

Figure 3-6 : Cluster Head Output

6.3. Résultats et interprétations

Dans cette section, nous allons présenter et analyser les résultats en termes d'énergie consommée, nous allons comparer l'énergie consommé par notre proposition (modèle réseau sécurisé) avec l'énergie consommée par un autre exemple (même modèle de réseau mais sans aucune sécurisation) dans les deux cas : sans attaque et avec un attaque de type DoS /Sybil

Nous avons utilisé l'extension PowerTrace afin de calculer l'énergie consommée. Nous avons suivi les étapes suivant pour utiliser cette extension dans notre simulateur Cooja.

- Inclusion de la fonctionnalité de Power trace : **#include "powertrace.h"**
- Dans notre code après **" PROCESS_BEGIN ( ) "** nous ajoutons cette line pour imprimer les valeurs de consommation énergétique toutes les 20 secondes **powertrace_start(CLOCK_SECOND* 20).**
- Nous ajoutons dans le fichier Makefile : **APPS+=powertrace .**

6.3.1. Consommation moyenne d'énergie sans la présence d'attaque

Après l'implémentation de 21 nœuds (17 nœuds capteurs SN, 4 Cluster Head CH) dans les deux codes (code de notre solution et code de l'exemple). La durée de simulation est estimée par une période de 5 minutes.

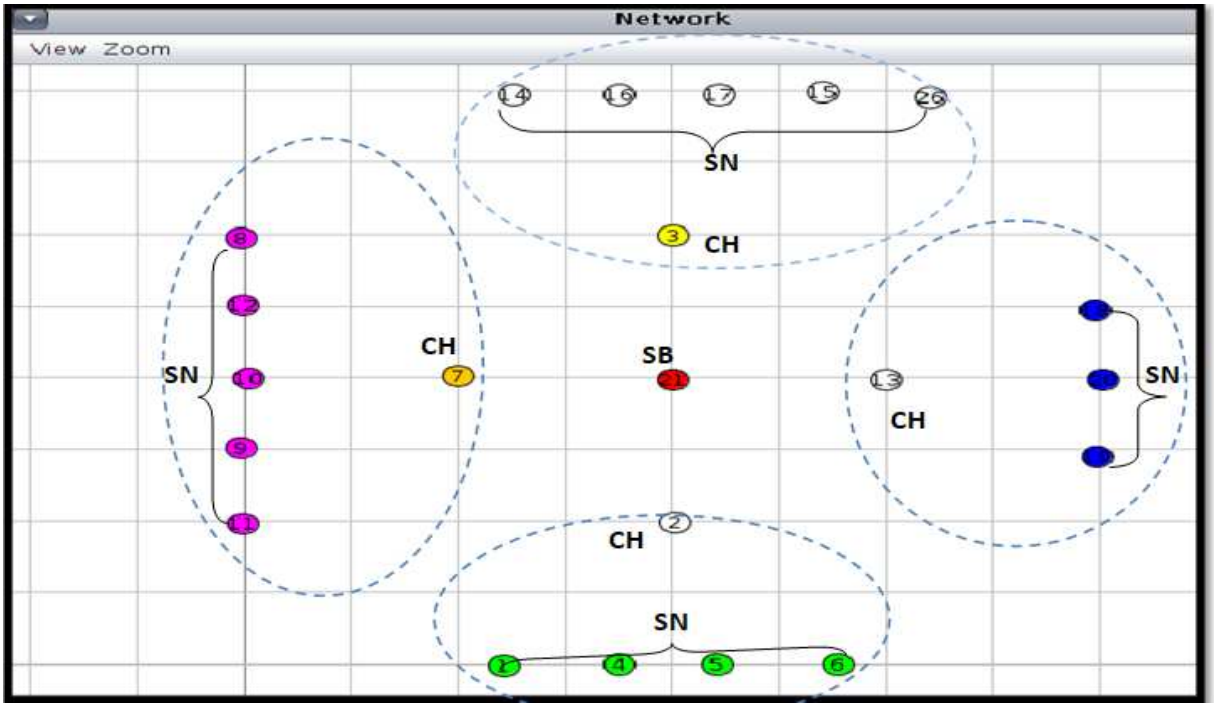

Figure 3-7 : Simulation sans attaque

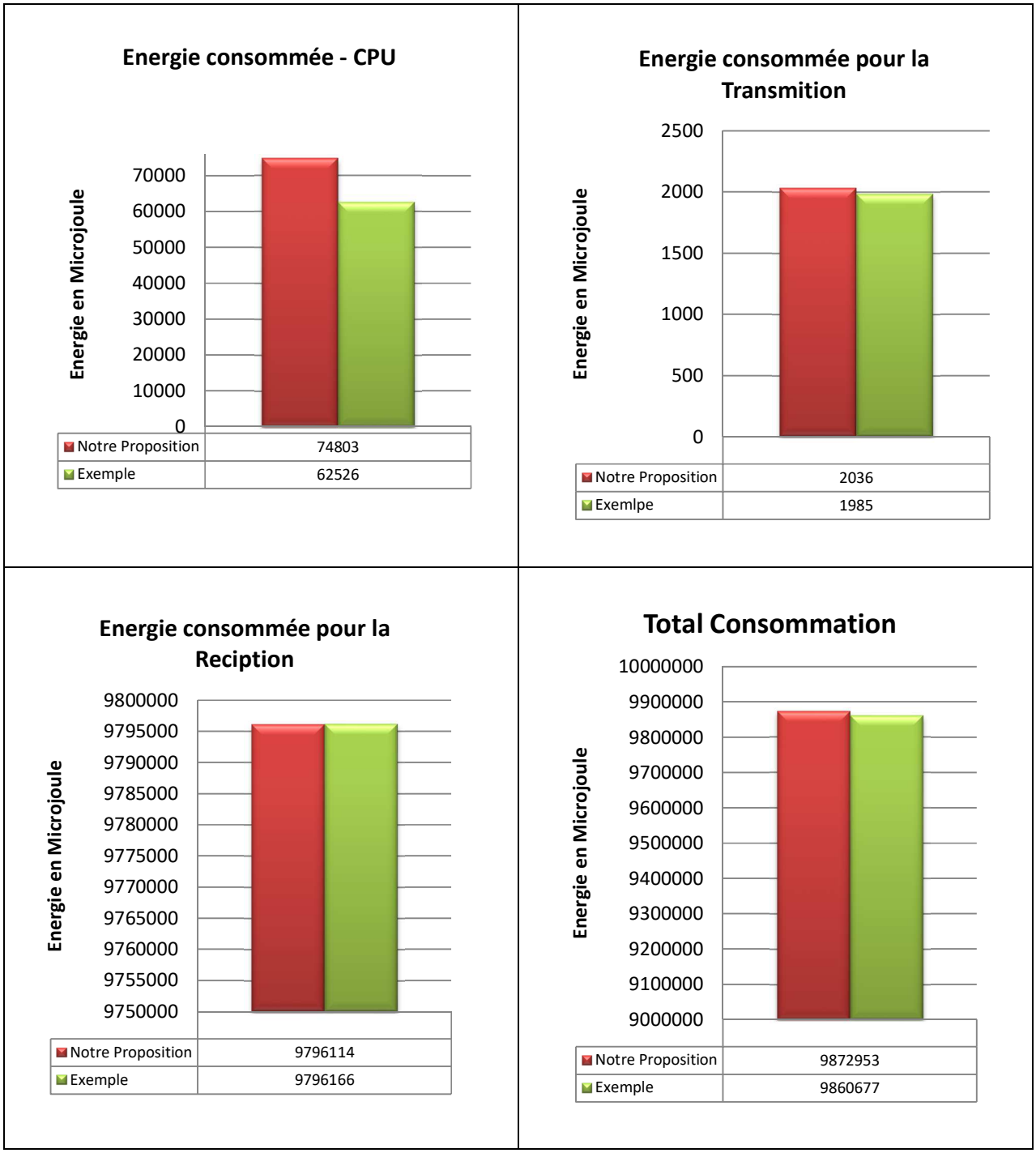

Figure 3-8 : Consommation moyenne d'énergie - Sans Attaque -

La Figure 3-8 illustre l'énergie moyenne consommée par tous les nœuds dans le réseau (SN+CH).D'après cette figure, nous pouvons remarquer que la différence en termes de consommation d'énergie, entre notre proposition et le modèle de communication non sécurisé est presque faible, avec un taux 0.0012 % de consommation totale d'énergie. Ceci explique que dans

notre proposition les nœuds de capteur font un calcul supplémentaire pour la sécurité (chiffrement / déchiffrement – calcul MAC).

Désignation	Taux d'augmentation %
Consommation de CPU	16.4%
Consommation de transmission de messages	0.025%
Consommation de Réception de messages	0.00001%
Consommation Totale	**0.0012%**

Tableau 3-3 : Taux d'augmentation de consommation

6.3.2. **Consommation moyenne d'énergie avec la présence d'attaques (DOS** /SYBIL)

Dans la simulation, nous avons ajouté dans chaque cluster des nœuds malicieux (Voir la figure 3-9). Ces nœuds malicieux lancent des attaques de type Dos /Sybil . Ceci est dans le but de dégrader l'efficacité de plusieurs fonctionnalités comme la distribution de données, l'agrégation des données, et l'épuisement des batteries des CHs par le biais de l'envoi massif des messages (chaque 10 secondes).

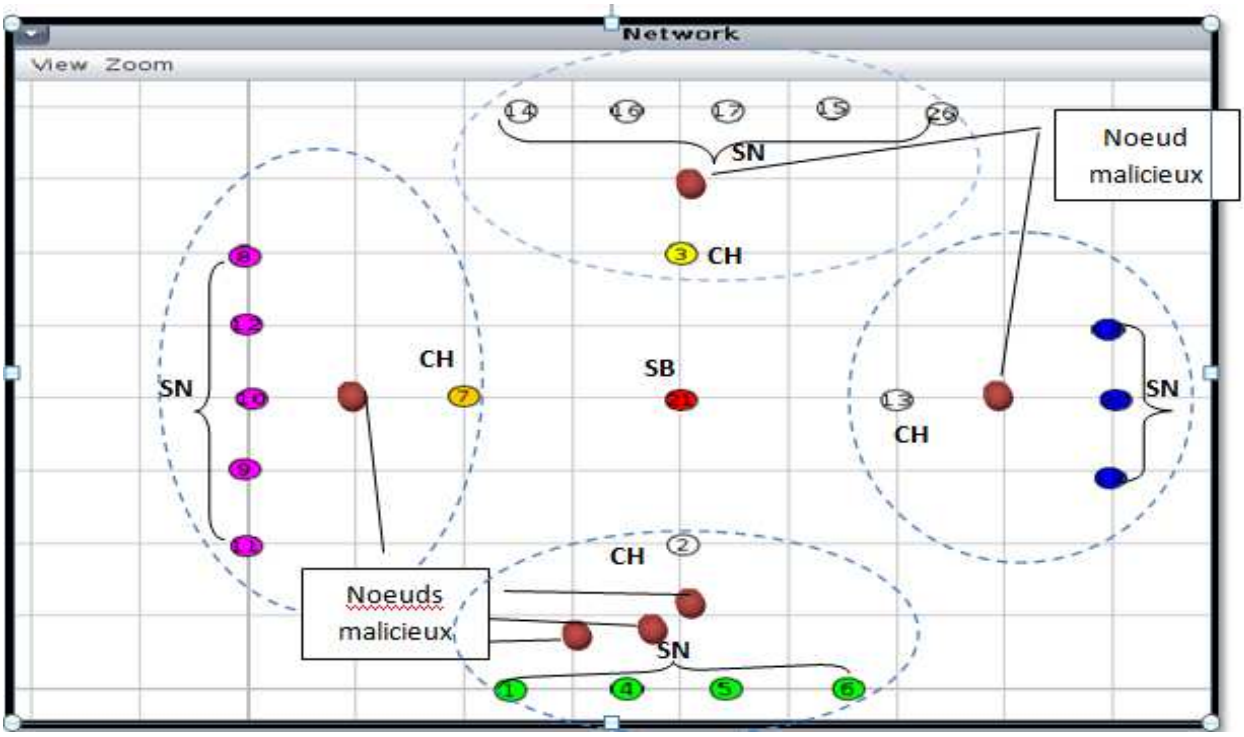

Figure 3-9 : Simulation Avec Attaque

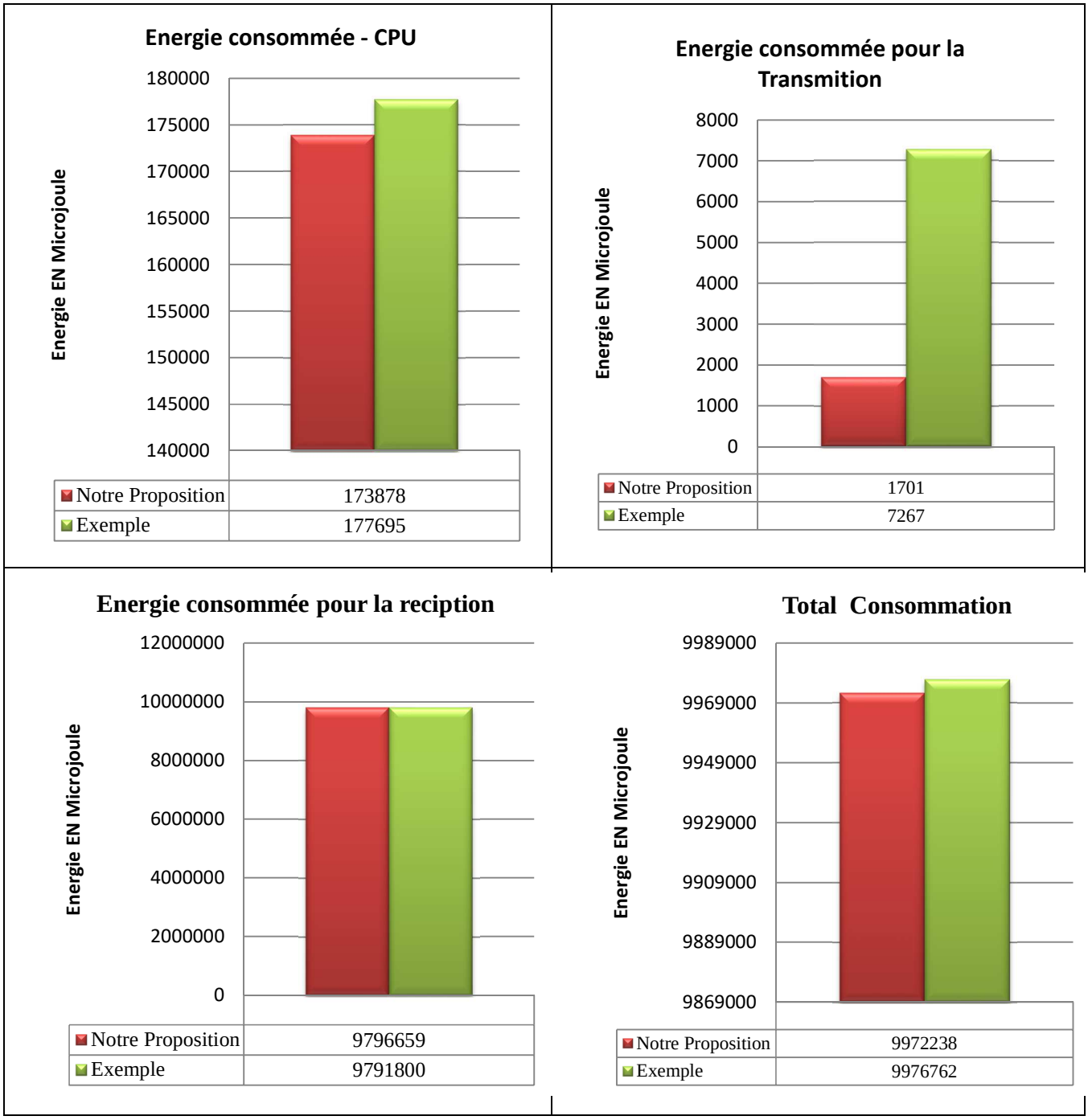

Figure 3-10 : Consommation moyenne d'énergie - Avec Attaque -

D'après la figure 3-10, nous pouvons remarquer que notre proposition offre de meilleures performances en termes de consommation d'énergie pour la communication et le CPU, avec un

taux global 0.045% de diminution de consommation énergétique (voir le tableau 3-3). Ceci explique que grâce aux services de sécurité introduits, ces attaques n'ont aucun effet sur notre solution de sécurité.

Désignation	Taux de diminution %
Consommation de CPU	2.15%
Consommation de Transmission	76 %
Consommation de Réception	0.04 %
Consommation Totale	**0.045%**

Tableau 3-4 : Taux de diminution de consommation

7. Conclusion

Dans ce chapitre, nous avons présenté l'implémentation ainsi que l'évaluation de notre proposition et un modèle de réseau non sécurisé. Le système d'exploitation Contiki est utilisé. Il consiste une programmation entière en langage C et une simulation avec Cooja.

Par la suite, nous avons implémenté des attaques DoS /Sybil qui visent la communication dans un modèle de réseau non sécurisé, afin de voir les effets néfastes que l'absence de sécurité peut donner. Cependant, ces attaques sont détectées par notre solution grâce aux services de sécurité qu'il offre.

Par ailleurs, nous avons constaté que les tests de performances effectués sur la consommation d'énergie ont montré que notre proposition permet de stabiliser la consommation d'énergie même en présence des nœuds malicieux.

CONCLUSION GENERALE

Les réseaux de capteurs constituent un axe de recherche très fertile et peuvent être utilisés dans plusieurs domaines différents. Cependant, il reste encore de nombreux problèmes à résoudre dans ce domaine afin de pouvoir optimiser leur utilisation dans le monde réel. L'un des problèmes qu'on peut rencontrer dans ce genre de réseau est la sécurité de communication à cause que les RCSF sont faciles à attaquer en raison de la nature du médium qui permet relativement facilement aux adversaires d'écouter, de falsifier ou d'injecter des données dans le réseau.

Le première chapitre de ce mémoire a été comme une introduction aux réseaux de capteurs sans fil qui sont considérées comme un type particulier de réseaux Ad-hoc en suite dans le deuxième chapitre nous avons abordé la problématique de la sécurité en expliquant les déférentes vulnérabilités et les différents types d'attaques qui peuvent viser ce type de réseau et nous avons terminé par la présentation de déférentes primitives cryptographiques utilisées dans les réseaux de capteurs.

Dans le troisième chapitre, nous avons proposé et simulé une solution de sécurité afin de résoudre le problème de sécurité de communication dans le RCSF en utilisant la cryptographie basée sur la clé symétrique afin d'assurer la confidentialité de donnée. La fonction de hachage est utilisée aussi pour générer le MAC (code d'authentification de message), ceci pour assurer l'intégrité et l'authentification des données. La fraicheur des données est assurée par l'utilisation un nonce qui représente le numéro de séquence de message envoyé. La solution proposée permet aussi de résister contre les attaques qui sont menées contre les RCSF.

Cette proposition a été implémentée par le langage C et simulée dans Cooja (le simulateur de Contiki). Nos résultats ont montré que la charge générée par notre proposition est presque faible par rapport à communication non sécurisée dans RCSF. En plus, notre proposition permet de stabiliser la consommation d'énergie en présence des attaques.

Comme perspective de notre travail, nous allons continuer à améliorer ce travail, en implémentant un mécanisme pour la gestion et l'échange des clés dans RCSF en prenant en

compte d’autres métriques comme la mémoire, le perte de paquets pour obtenir de meilleurs résultats possible.

BLIOGRAPHIE

[1] MEZRAG Fares " Sécurité du Routage Hiérarchique Basée sur les Clusters dans les Réseaux de Capteurs sans Fil " - Thèse de Magister – Universite Amar Telidji – Laghouat – 2016

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E.l. Cayirci, "A survey on sensor networks". IEEE Communications Magazine, pp. 102-114, August 2002.

[3] Vernon S. Somerset, "Intelligent and Biosensors, Edited by Vernon S. Somerset", Intech, January 2010.

[4] Ian F. Akyildiz, Mehmet Can Vuran. "Wireless Sensor Networks". John Wiley & Sons Ltd, 2010.

[5] Abdellatif Chafik - Architecture de réseau de capteurs pour la surveillance de grands systèmes physiques à mobilité cyclique - Thèse de doctorat – Université de lorraine –Metz 2014

[6] C. Duran-Faundez, "Transmission d'images sur les réseaux de capteurs sans fil sous la contrainte de l'énergie". Thèse de doctorat, Université Henri Poincaré, Centre de recherche en automatique de Nancy, Juin 2009.

[7] Z. Wassim, "Quelques propositions de solutions pour la sécurité des réseaux de capteurs sans fil". Thèse de doctorat, Institut national des sciences appliquées de Lyon, Octobre 2010.

[8] http://www.technologyreview.com/computing/21161/ -Michael Fitzgerald. TechnnologyReview: Tracking a Shopper's Habits. Technology Review. [En ligne] 04 August 2008. Consulter le 09-06-2018

[9] Wang, Yong; Attebury, Garhan; and Ramamurthy, Byrav, "A Survey of Security Issues In Wireless Sensor Networks" - Published in IEEE Communications Surveys & Tutorials • 2nd Quarter 2006.

[10] WassimDrira, Chakib Bekara, Maryline Laurent-Maknavicius, «Securite dans les reseaux de capteurs sans fil : Conception et implementation », TELECOM & Management Paris-Sud, 2008

[11] B. Veeramulllu, S. Sathiya, Ch. LavanyaSusanna, "Confidentiality in Wireless Sensor Network," International Journal of Soft Computing and Engineering (IJSCE), vol. 2, issue 6, January 2013.

[12] M. M. Patel, A. Aggarwal, "Security attacks in wireless sensor networks: A survey," International Conference on Intelligent Systems and Signal Processing (ISSP), pp. 329-333, March 2013.

[13] D. Djenouri, L. Khelladi and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks", IEEE Communications Surveys and Tutorials ,Vol. 7 , pp. 2-28, 2005.

[14]SarmadUllah khan, " Key management in wireless sensor networks, IP-Based sensor networks, content centric networks", Thèse de doctorat - POLITECNICO DI TORINO- March 14, 2013

[15] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks :attacks and countermeasures".in IEEE SNPA,pp. 113-127, May 2003.
[16] S. ATHMANI, Protocole de sécurité Pour les Réseaux de capteurs Sans Fil, thèse de magister, Université Hadj Lakhder - Batna- 2010

[17] E. Yoneki and J. Bacon. A Survey of Wireless Sensor Network Technologies: Research Trends and Middleware's Role. Technical Report UCAM-CL-TR646, 2005.

[18] BenyettoLahouari - Détection d'intrusions dans les réseaux Ad Hoc - thèse de magister – Université des sciences et technologies d'Oran - 2011 –

[19] A. Dunkels, B. Grönwall, T. Voigt « Contiki – a Lightweight and Flexible Operating System for Tiny Networked Sensors » 1st IEEE Workshop on Embedded Networked Sensors (IEEE EmNetS-I), Tampa, Florida, USA, November 2004.

[20] http://www.contiki-os.org/start.html#start-cooja – Site Web Consulter le 07-05-2018

[21] M. Bellare, R. Canetti, and H. Krawczyk. "Keying hash functions for message authentication", Crypto '96, LNCS No. 1109. pages 1–15, 1996

ملخص

ركزنا اهتمامنا في هذا العمل حول مشاكل الأمن الخاصة بشبكات الاستشعار اللاسلكية. هدفنا الرئيسي هو تأمين الاتصال بين أجهزة الاستشعار في الشبكة وذلك من خلال ضمان المتطلبات الأمنية الهامة ومواجهة الهجمات التي يتم تنفيذها بشكل متكرر ضد هذا النوع من الشبكات من جهة، ومراعاة عائق محدودية الموارد التي تتميز بها أجهزة الاستشعار من جهة أخرى. استخدمنا نظام التشغيل Contiki وبرنامج المحاكاة Cooja من اجل الحصول على النتائج التجريبية لعملنا هذا

كلمات البحث: شبكات الاستشعار اللاسلكية، تأمين الاتصال، التعتيم، كونتيكي، كوجا.

Abstract

In this work, we are interested in studying the problems of security in wireless sensor networks. Our main objective is to secure the communication between the sensor nodes in the network by ensuring the important security requirements and to face the attacks that are frequently carried out against this type of network. The constraints of limitation of the energy and physical resources of the sensor node, are taken into account. Our experimental results are based on the use of Contiki operating system and the Cooja simulator.

Keywords: Wireless sensor networks, secure the communication, Cryptography, Contiki, Cooja.

Résumé

Dans ce travail, nous intéressons à l'étude des problèmes de la sécurité dans les réseaux de capteur sans fil. Notre objectif principales de sécuriser la communication entre les nœuds capteurs dans le réseau en assurant les importantes exigences de sécurité et faire face aux attaques qui sont fréquemment menées contre ce type de réseau en prenant en considération les contraintes de limitation des ressources énergétiques et physiques d'un nœud capteur. Nos résultats expérimentaux sont basés sur l'utilisation de système d'exploitation Contiki et le simulateur Cooja.

Mots clés : Réseaux de capteurs sans fil, sécurité de communication, cryptographie, Contiki, Cooja.