REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR

ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE SAAD DAHLAB DE BLIDA 1

FACULTE DES SCIENCES

**PROJET DE FIN D'ETUDE**

**POUR L'OBTENTION DU DIPLOME DE MASTER EN INFORMATIQUE**

**SPECIALITE : SECURITE DES SYSTEMES D'INFORMATION**

**THEME**

# Création d'un système de détection d'intrusion dans un réseau de capteurs sans fils

**Mémoire présenté par :**

**AIT Nadir**

**Promotrice: Professeur BOUSTIA Narhimene**
**Co-promotrice: SAIDIA Siham**

**Année Universitaire : 2019- 2020**

# REMERCIEMENT

*Je remercie tout d'abord ALLAH le tout puissant qui m'a donné la force de mener à bon terme ce modeste travail.*

*Je tiens à remercier sincèrement toutes les personnes qui ont apporté leur contribution à l'aboutissement de ce projet.*

*Je remercie ma promotrice M^lle^ BOUSTIA pour son soutien et ses précieux conseils.*

*Je remercie ma co-promotrice M^me^ SAIDIA pour son soutien et ses précieux conseils.*

*Je remercie aussi tous les enseignants de département d'informatique pour les efforts consacrés pour nous transmettre le savoir.*

*En fin, je tiens à remercier les membres de jury qui vont faire l'honneur d'apprécier ce travail.*

# *Dédicace :*

*Je dédie ce modeste travail à :*

** Mes parents qui m'encouragent toujours.*

**Mes frères et sœurs.*

** Tous mes amis.*

.

*Ainsi qu'à toutes les personnes qui m'ont encouragé.*

*Nadir*

# SOMMAIRE

# LISTE DES FIGURES

# LISTE DES TABLEAUX

# INTRODUCTION GÉNÉRALE

Au cours de ces dernières années, la convergence de la micro-électronique et des technologies de communication sans-fil a permis la création d'une combinaison entre les systèmes embarqués et les systèmes distribués ayant engendré les Réseaux de Capteurs Sans-Fil ou RCSFs (Wireless Sensor Networks). Les capteurs apparaissent comme des systèmes autonomes miniaturisés, équipés d'une unité de traitement et de stockage de données, d'une unité de transmission sans-fil et d'une batterie [1].

Organisés sous forme de réseau, les capteurs (ou nœuds) d'un RCSF, malgré la limitation de leurs ressources de calcul, de stockage et d'énergie, ont pour mission de récolter des données et les faire parvenir à une station de base.

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

**Contexte et problématique**

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

Des mécanismes de protection existent mais il est souvent nécessaire d'ajouter à ces systèmes des mécanismes de détection d'intrusion afin de compléter les fonctions de sécurité.

Un système de détection d'intrusions (IDS, de l'anglais Intrusion Detection System) est un périphérique ou processus actif qui analyse l'activité du réseau pour détecter toute entrée non autorisée et / ou toute activité malveillante. La manière dont un IDS détecte des anomalies peut beaucoup varier ; cependant, l'objectif principal de tout IDS est de prendre sur le fait les auteurs avant qu'ils ne puissent vraiment endommager vos ressources.

Les IDS protègent le réseau contre les attaques, les mauvaises utilisations et les compromis. Ils peuvent également surveiller l'activité du réseau, analyser les configurations du réseau contre toute vulnérabilité, analyser l'intégrité de données et bien plus.

**Objectif**

Le but de ce projet est la création d'un Système de détection d'intrusion (à base de signatures dans un réseau de capteurs sans fils (WSN)).

Ce présent mémoire est divisé en trois (03) chapitres.

Nous allons présenter dans le premier chapitre des généralités sur les réseaux de capteurs sans fil ainsi on va décrire 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 second chapitre traite les aspects fondamentaux de la sécurité des réseaux de capteurs sans fil. Je présente également les solutions de base, qui sont proposées dans la littérature pour répondre aux besoins en termes de sécurité.

Le chapitre 3 présente la conception et la mise en œuvre d'un système de détection d'intrusion pour les réseaux de capteurs sans fil avec une simulation dans l'environnement CONTIKI COOJA. Nous clôturerons notre travail par une conclusion générale et des perspectives.

# CHAPITRE 1. CONCEPTS GENERAUX SUR LES RESEAUX DE CAPTEURS SANS FIL (RCSF)

## 1.1 Introduction

Depuis les premières inventions des systèmes informatiques jusqu'à nos jours, on constate que chaque époque marque une évolution technologique. Actuellement, la technologie des réseaux et les domaines qu'elle inclut prennent de plus en plus d'ampleur dans les systèmes informatiques. Parmi les technologies, en vogue, répondant à ces domaines, on cite entre autres les réseaux de capteurs sans fil. Un réseau de capteurs sans fil peut être défini comme un ensemble de composants miniatures (capteurs) capable de capter des grandeurs physiques à partir d'un environnement donné et de transformer ces données en grandeurs numériques dans le but d'établir une communication avec les autres capteurs du réseau et d'acheminer la somme des données collectées vers une station de base.

Dans ce chapitre, je parle sur les réseaux en général et les réseaux de Capteurs Sans Fil (RCSFs) ou Wireless Sensor Network (WSN) en partant de leur cellule élémentaire, le capteur sans fil.

## 1.2. Le nœud capteur

Le nœud capteur est un petit dispositif électronique qui est caractérisé par sa limitation en ressources énergétiques, de stockage, et en capacité de calcul (voir la Figure 1.1). 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 2.1 : Quelques types de nœud capteur

## 1.3. Architecture matérielle d'un capteur sans fil

Le nœud de capteur est composé principalement de quatre unités : l'unité d'acquisition (de captage), l'unité de traitement (calcul), l'unité de communication (transmission) et une source d'énergie (voir la Figure 1.2) [3].

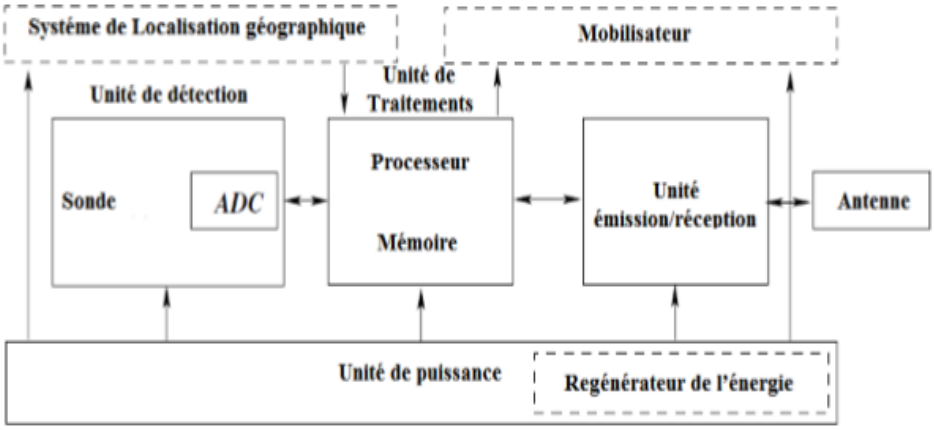


Figure 1.2 : Architecture d'un nœud capteur

**Unité de capture (Sensing unit) :** composée d'un dispositif de capture physique qui prélève l'information de l'environnement local et un convertisseur analogique/numérique appelé ADC (Analog to Digital Converter) qui va convertir l'information relevée et la transmettre à l'unité de traitement [3].

**Unité de traitement (Processing unit) :** est composée de deux interfaces : une interface pour l'unité d'acquisition et une autre pour l'unité de transmission. Cette unité est également composée d'un processeur et d'une mémoire, elle acquiert les informations en provenance de l'unité d'acquisition et les stocke en mémoire ou les envoie à l'unité de transmission [4].

**Unité de transmission (Transceiver unit) :** responsable de la transmission et de la réception des données via un support de communication radio. Ce dernier peut être de type optique (comme dans les capteurs Smart Dust) ou de type radio fréquence (MICA2) [3].

**Unité d'énergie (Power unit) :** Elle exécute des opérations de contrôle de l'énergie restante et de mesure de la durée de vie du capteur. Un micro-capteur est muni d'une ressource énergétique généralement une batterie, pour alimenter tous ses composants. Cependant, cette ressource énergétique est limitée et dans la plupart des cas irremplaçable. L'unité de contrôle d'énergie constitue donc l'un des systèmes les plus importants, elle est responsable de répartir l'énergie sur les autres modules et de réduire les dépenses énergétiques (par la mise en veille des composants inutiles, par exemple). Cette unité peut aussi gérer des systèmes de rechargement d'énergie à partir de l'environnement observé, telles que les cellules solaires [4].

## 1.4. Le réseau de capteurs sans fil

Un réseau de capteurs sans fil (RCSF) est composé d'un ensemble de nœuds capteurs, limités en capacité mémoire et de calcul, devant être économes en énergie, ce qui les contraint à exploiter une faible puissance de transmission et des portées et des débits modestes. Ces nœuds capteurs sont organisés en champs. Chacun de ces nœuds est autonome et a la capacité de collecter des données et de les transférer au nœud puits (station de base) par l'intermédiaire d'une architecture multi-sauts. Le puits transmet ensuite ces données par Internet ou par satellite à un ordinateur central "Gestionnaire de tâches" pour analyser et évaluer ces données et prendre des décisions.

## 1.5. Topologies des réseaux de capteurs sans fils

Il existe deux catégories pour les réseaux de capteurs : les réseaux de capteurs plats et les réseaux de capteurs hiérarchiques.

### 1.5.1. Les réseaux de capteurs plats

Un réseau de capteurs est composé d'un nombre souvent très important de nœuds qui sont soit posés à un endroit précis, soit dispersés aléatoirement. Ce dispersement aléatoire des capteurs nécessite que le protocole utilisé pour les réseaux de capteurs possède des algorithmes d'auto organisation. Afin de résister aux déploiements, ces capteurs doivent être très solides et de plus, ils doivent aussi pouvoir survivre dans les conditions les plus extrêmes dictées par leur environnement d'utilisation (feu ou eau par exemple). Ces nœuds capteurs sont organisés en champs " sensor fields ". Chacun de ces nœuds a la capacité de collecter des données et de les transférer au nœud passerelle (dit " sink " en anglais ou puits) par l'intermédiaire d'une architecture multi-sauts. Le puits transmet ensuite ces données par internet ou par satellite à l'ordinateur central " Gestionnaire de tâches " pour analyser ces données et prendre des décisions [5].

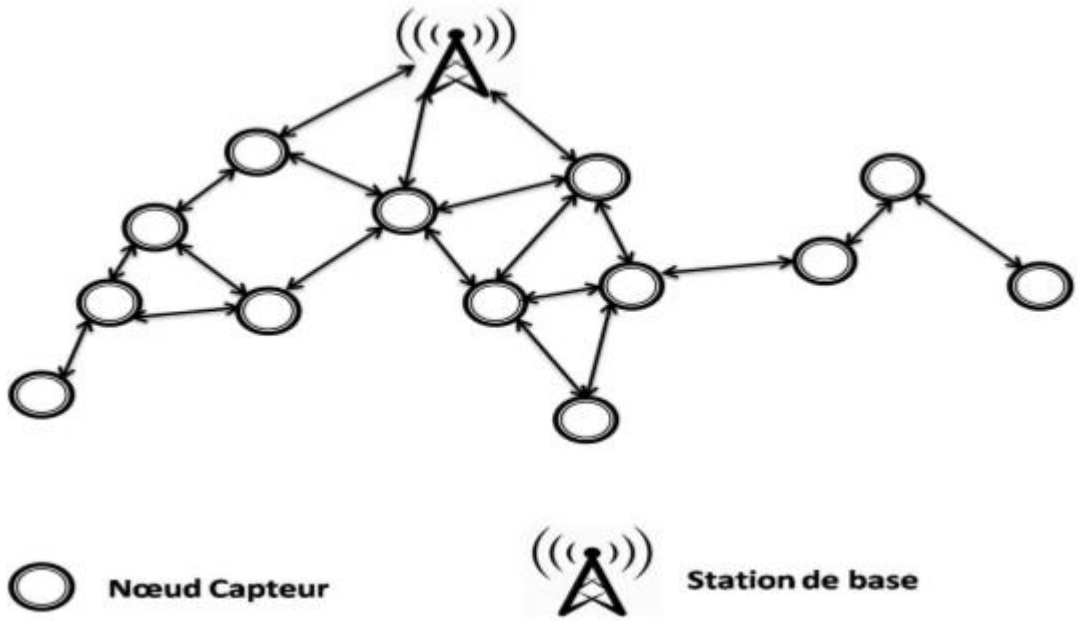


Figure 1.3 : Modèle de la topologie Plate

### 1.5.2. Les réseaux de capteurs hiérarchiques

Le point clé dans un réseau de capteurs hiérarchique est la distinction entre les nœuds du réseau. Cette distinction peut se faire au niveau physique ou au niveau logique :

- Au niveau physique : lorsqu'il y a une différentiation au niveau matériel, les nœuds sont hétérogènes et différents de par leurs capacités et fonctionnalités. De ce fait, certains nœuds disposent de caractéristiques supplémentaires et peuvent réaliser des tâches plus complexes que d'autres nœuds. Cependant, il existe un coût supplémentaire, au niveau du prix et de la consommation énergétique, pour les dispositifs ayant plus de fonctionnalités [5].

- Au niveau logique : dans un réseau homogène les nœuds peuvent également être hiérarchisés selon leurs fonctionnalités. Dans un découpage en clusters, par exemple, permettant de partitionner le réseau et donc de le structurer, certains nœuds appelés cluster-Head ou encore têtes de clusters ont pour rôle d'organiser leurs clusters respectifs. Les cluster-Head qui sont des nœuds de niveau supérieur dans la hiérarchisation peuvent communiquer exclusivement entre eux [5].

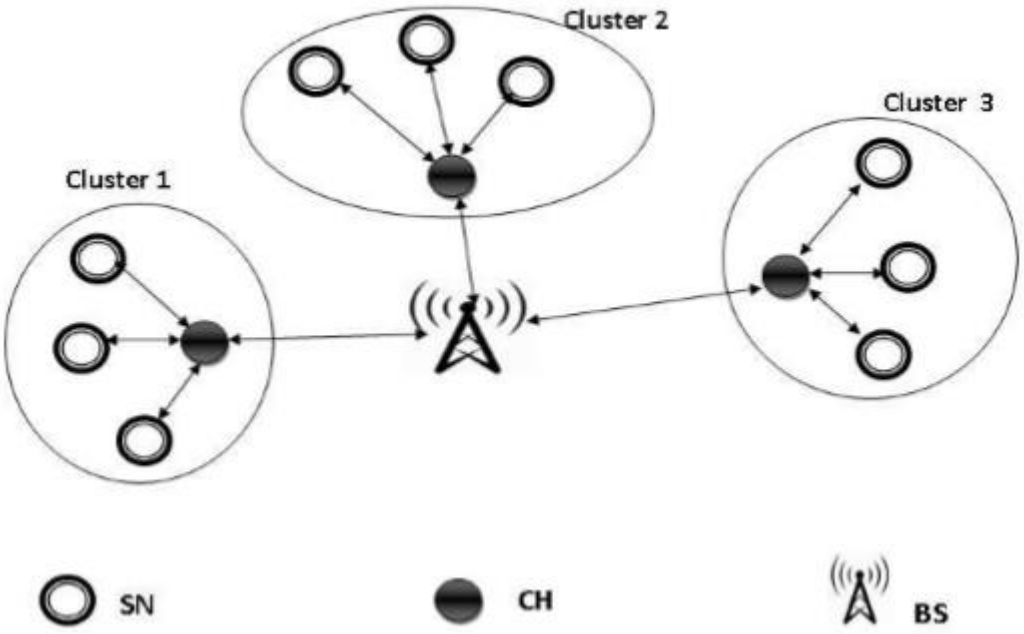


Figure 1.4 Modèle de la topologie Hiérarchique

## 1.6. Domaines d'applications des RCSF

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

### 1.6.1. 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.

### 1.6.2. La 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 à 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.

### 1.6.3. 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.

### 1.6.4. Les applications commerciales

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.

### 1.6.5. Les applications transportées

Il est possible d'intégrer des nœuds capteurs au processus de stockage et de livraison. Le réseau ainsi formé, pourra être utilisé pour connaître la position, l'état et la direction d'un paquet ou d'une cargaison.

### 1.6.6. Les applications agricoles

Dans les champs agricoles, les capteurs peuvent être semés avec les graines. Ainsi, les zones sèches seront facilement identifiées et l'irrigation sera donc plus efficace.

## 1.7. Systèmes 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. Voici quelques exemples des systèmes d'exploitation pour les réseaux de capteurs les plus répandus :

### 1.7.1. 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 d'un 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 exigée, par exemple lorsque le logiciel du nœud doit être mis à jour souvent pour une grande quantité de nœuds.

### 1.7.2. TinyOs

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 de programmation NesC (Network Embedded System C), une extension du langage de programmation C., l'utilisation du langage NesC permet l'optimisation du code et par conséquence réduit l'usage de la mémoire à accès aléatoire (RAM).

### 1.7.3. 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 tâches actives sont terminées, MANTIS est un système dynamique où les modifications applicatives peuvent être réalisées pendant le fonctionnement.

## 1.8. Contraintes et facteurs de conception des réseaux de capteurs sans fil

La conception et la réalisation des réseaux de capteurs sans fil sont influencées par plusieurs paramètres. Ces facteurs servent comme directives pour le développement des algorithmes et protocoles utilisés dans les RCSF [6].

**Durée de vie du réseau :** c'est l'intervalle de temps qui sépare l'instant de déploiement du réseau de l'instant ou l'énergie du premier nœud s'épuise. Selon l'application, la durée de vie exigée pour un réseau peut varier entre quelques heures et plusieurs années.

**La tolérance aux fautes :** certains nœuds peuvent générer des erreurs ou ne plus fonctionner à cause d'un manque d'énergie, un problème physique ou une interférence. Ces problèmes ne doivent pas affecter le reste du réseau, c'est le principe de la tolérance aux fautes.

**Ressources limitées :** en plus de l'énergie, les nœuds capteurs ont aussi une capacité de traitement et de mémoire limitée. En effet, les industriels veulent mettre en œuvre des capteurs simples petits et peu coûteux qui peuvent être achetés en masse.

**Bande passante limitée :** Afin de minimiser l'énergie consommée lors du transfert de données entre les nœuds, les capteurs opèrent à bas débit. Un débit de transmission réduit n'est pas handicapant pour un réseau de capteurs où les fréquences de transmission ne sont pas importantes [6].

**Le facteur d'échelle :** Le nombre de nœuds déployés pour une application peut atteindre des milliers. Dans ce cas, le réseau doit fonctionner avec des densités de capteurs très grandes. Un nombre aussi important de nœuds engendre beaucoup de transmissions inter-nodales et nécessite que la station de base soit équipée de mémoire suffisante pour stocker les informations reçues [6].

**Topologie dynamique :** La topologie des réseaux de capteurs peut changer au cours du temps pour les raisons suivantes [6] :

- Les nœuds capteurs peuvent être déployés dans des environnements hostiles (champ de bataille par exemple), la défaillance d'un nœud capteur est, donc très probable.

- Un nœud capteur peut devenir non opérationnel à cause de l'expiration de son énergie.

- Dans certaines applications, les nœuds capteurs et les stations de base sont mobiles.

**Agrégation de données :** Dans les RCSFs, les données produites par les nœuds capteurs voisins sont très corrélées spatialement et temporellement. Ceci peut engendrer la réception par la station de base d'informations redondantes. Réduire la quantité d'informations redondantes transmises par les capteurs permet de réduire la consommation d'énergie dans le réseau et ainsi d'améliorer sa durée de vie. L'une des techniques utilisée pour réduire la transmission d'informations redondantes est l'agrégation des données. Avec cette technique, les nœuds intermédiaires agrègent l'information reçue de plusieurs sources. Cette technique est connue aussi sous le nom de fusion de données [6].

## 1.9. Pile protocolaire

Le rôle de la pile protocolaire consiste à standardiser la communication entre les composants du réseau, afin que les différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles. Ce modèle comprend cinq couches, ainsi que trois couches pour la gestion de la puissance d'énergie, la gestion de la mobilité et la gestion des tâches (interrogation du réseau de capteurs). Le but d'un système en couche est de séparer le problème en déférentes parties selon leur niveau d'abstraction. Chaque couche du modèle communique avec une couche adjacente. Chaque couche utilise ainsi les services des couches inférieures, et en fournit à celle de niveau supérieur [7].

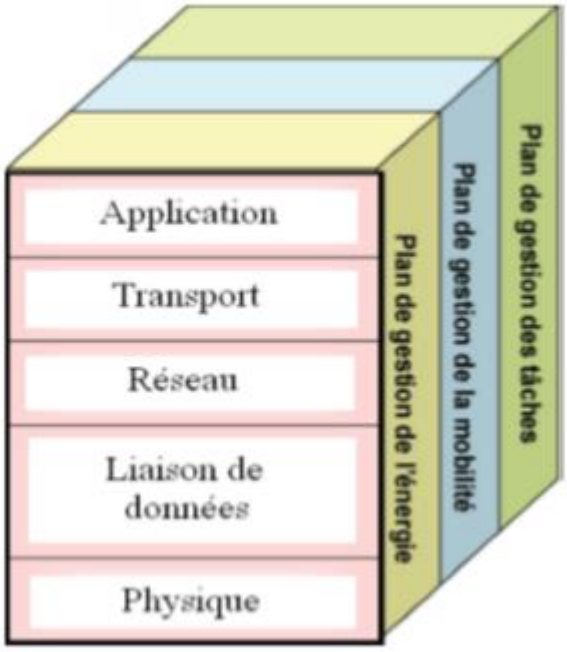


Figure 1.5. Pile protocolaire dans les réseaux de capteurs sans fil

**La couche liaison :** spécifie comment les données sont expédiées entre deux nœuds dans une distance d'un saut. Elle est responsable du multiplexage des données, du contrôle d'erreur de l'accès au media. Elle assure la liaison point à point et multipoint dans un réseau de communication [7].

**La couche réseau :** dans la couche réseau, le but principal est de trouver une route et une transmission fiable des données captées des nœuds capteurs vers le puits, en optimisant l'utilisation de l'énergie des capteurs. Ce routage diffère de celui des réseaux de transmission ad hoc sans fils par les caractéristiques suivantes :

- Il n'est pas possible d'établir un système d'adressage global pour le grand nombre de nœuds.

- Les applications des réseaux de capteurs exigent l'écoulement des données mesurées de sources multiples à un puits particulier.

- Les multiples capteurs peuvent produire de mêmes données à proximité d'un phénomène (redondance).

- Les nœuds capteurs exigent ainsi une gestion soigneuse des ressources.

En raison de ces différences, plusieurs nouveaux algorithmes ont été proposés pour le problème de routage dans les réseaux de capteurs.

**Couche physique :** cette couche se charge de l'adaptation du signal au support de transmission, elle gère aussi le type de transmission du signal (mode synchrone ou asynchrone).

**La couche transport :** cette couche est chargée du transport des données, de leur découpage en paquets, du contrôle de flux, de la conservation de l'ordre des paquets et de la gestion des éventuelles erreurs de transmission [7].

**La couche application :** cette couche assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, géré directement par les logiciels. En plus de ces cinq couches, la pile protocolaire des réseaux de capteurs comporte trois niveaux : le niveau de gestion d'énergie, le niveau de gestion de mobilité et le niveau de gestion des tâches [7].

**Le niveau de gestion d'énergie :** le niveau de gestion d'énergie adopte quelques mécanismes pour contrôler et essayer d'optimiser l'énergie consommée par les capteurs. Ainsi, lorsqu'un capteur atteint un niveau critique d'énergie, il informe son voisin de son incapacité à participer au routage [7].

**Le niveau de gestion de la mobilité :** le niveau de gestion de mobilité détecte et enregistre les mouvements des nœuds capteurs afin de leur permettre de garder continuellement un chemin vers le nœud puits et de maintenir une image récente de la carte du réseau [7].

**Le niveau de gestion des tâches :** lors d'une opération de capture dans une région donnée, les nœuds composant le réseau ne travaillent pas obligatoirement au même rythme, cela dépend essentiellement de la nature du capteur, de son niveau d'énergie et de la région dans laquelle il a été déployé. Le niveau de gestion des tâches doit donc assurer l'équilibrage et la distribution des tâches sur les différents nœuds concernés afin d'optimiser la consommation d'énergie [7].

## 1.10. Conclusion

Dans ce chapitre, nous avons essayé de donner quelques généralités sur les réseaux de capteurs sans fils que nous avons considérés 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'application, les topologies, les systèmes d'exploitations dédiés à 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 RESEAUX DE CAPTEURS SANS FIL

## 2.1. Introduction

Parmi les caractéristiques majeures des nœuds de capteurs, nous distinguons la limitation de leurs ressources en termes de capacité de calcul, d'espace de stockage des données et la faible portée radio. Les ressources limitées de ces nœuds et les environnements hostiles dans lesquels ils pourraient être déployés, rendent ce type de réseaux très vulnérables aux attaques. Dans ce contexte, une grande communauté de chercheurs tente de proposer des mécanismes de sécurité pour la prévention et la détection de tout type d'attaque, en tenant compte des contraintes de ce type de réseaux [4].

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 la confidentialité des communications.

Tandis que d'autres domaines comme les applications environnementales, exigent l'intégrité et la fiabilité des communications.

La sécurité dans les réseaux de communication est par définition tout mécanisme permettant de couvrir les vulnérabilités du réseau et de protéger ses entités, ses utilisateurs ainsi que les informations échangées. En effet, différents types d'attaques existent déjà et plein de nouvelles catégories de menaces ne cessent d'émerger. De ce fait, la sécurité des réseaux informatiques constitue une discipline indépendante et un domaine très intéressant de la recherche scientifique.

Dans ce chapitre, je présente les aspects fondamentaux de la sécurité des réseaux de capteurs sans fil. Je présente également les solutions de base, qui sont proposées dans la littérature pour répondre aux besoins en termes de sécurité.

## 2.2. Les contraintes de la sécurité dans les RCSF

Le déploiement des nœuds capteurs dans des endroits ouverts, inaccessibles et hostiles, rend 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 :

### 2.2.1. La Contrainte d'énergie

C'est très important de savoir que l'énergie est la ressource qui doit être gérée avec une grande attention dans les réseaux de capteurs sans fil.

Le remplacement de la batterie est difficile ou parfois impossible (exemple : applications dans des terrains hostiles) ce qui cause que la durée de vie du réseau dépende radicalement de la durée de vie des batteries des capteurs sans fil.

Le besoin en l'énergie est résumé dans la puissance supplémentaire consommée par les nœuds capteurs en raison du traitement requis par les exigences de sécurité et la transmission des données. En plus, l'impact énergétique du code de sécurité ajouté dans les nœuds capteurs doit être pris en compte par les chercheurs.

### 2.2.2. 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.

| | 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 de ressources pour quelques nœuds capteurs

Le ci-dessus présente des limitations physiques pour quelques nœuds capteurs.

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.

### 2.2.3. 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.

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

### 2.2.4. Gestion à distance

Etant donné 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.

### 2.2.5. Exposition aux attaques

Comme tous les systèmes d'information, les réseaux de capteurs sans fil sont susceptibles d'être l'objet d'une attaque, de plus, les nœuds sont exposés aux attaques physiques, donc l'attaquant peut avoir le contrôle total sur des nœuds du réseau ou supprimer le nœud capteur, cela se fait par le vol ou la destruction du nœud.

## 2.3. Les exigences de sécurité dans les réseaux de capteurs sans fil

Un réseau de capteurs est un type spécial de réseaux. Il partage quelques vulnérabilités avec un réseau informatique typique, mais pose également des conditions uniques de ses propres caractéristiques [8]. Par conséquent, un protocole de sécurité pour un réseau de capteurs sans fil, doit satisfaire une ou plusieurs conditions de sécurité, à savoir :

### 2.3.1. Intégrité

Les données circulant dans le réseau ne doivent pas pouvoir être altérées ou changées au cours de la communication. Il faut donc s'assurer que personne ne puisse capturer et modifier les données du réseau. De la même manière il faut vérifier que les données n'ont pas subi d'altération due à un disfonctionnement du matériel, qui est un risque important sur des capteurs sensibles aux changements d'états [10]. L'intégrité peut être assurée par l'utilisation des fonctions de hachage cryptographiques qui permettent d'obtenir pour chaque message une empreinte numérique [2].

### 2.3.2. Confidentialité

La confidentialité est un point important dans la communication dans les réseaux de capteurs sans fil. Elle consiste à préserver le secret des messages échangés et ne pas les révéler aux adversaires. Elle assure que les données transmises ne sont divulguées que par le destinataire souhaité. Elle peut être assurée soit par l'utilisation du chiffrement symétrique ou asymétrique des données.

### 2.3.3. Authentification

Un attaquant n'est pas limité simplement à modifier le paquet de données. Il peut changer le jeu entier de paquets en injectant les paquets additionnels. Ainsi, le récepteur doit s'assurer que les données utilisées dans n'importe quel processus décisionnel proviennent de la source correcte.

D'autre part, en construisant le réseau de capteurs, l'authentification est nécessaire pour beaucoup de tâches administratives (coefficient de reprogrammation ou de contrôle). D'après ce qui précède, nous pouvons voir que l'authentification de message est importante pour beaucoup d'applications dans les réseaux de capteurs. Officieusement, l'authentification de données permet à un récepteur de vérifier que les données sont vraiment envoyées par l'expéditeur réclamé.

Dans le cas de communication bipartite [9], l'authentification de données peut être réalisée par un mécanisme purement symétrique : l'expéditeur et le récepteur partagent une clef secrète pour calculer le code d'authentification de message de toutes les données communiquées.

L'authentification des capteurs est nécessaire pour s'assurer que l'identité déclarée par un capteur est bien celle du capteur déclarant. En l'absence d'un mécanisme permettant d'authentifier clairement un nœud du réseau, de nombreuses attaques peuvent se mettre en place comme l'attaque Sybil [10].

### 2.3.4. Fraîcheur de données

La fraîcheur des données permet de savoir si la donnée est récente ou non. Cela signifie que la fraîcheur de données suggère que les données soient récentes, et elles s'assurent qu'aucun vieux message n'a été rejoué. Cette condition est particulièrement importante quand il y a des stratégies de partager les clefs utilisées dans la conception. Des clefs typiquement partagées doivent être changées avec le temps. [10].

Cependant, cela prend du temps pour que de nouvelles clefs partagées soient propagées au réseau entier. Dans ce cas-ci, il est facile pour l'adversaire d'employer une attaque par rejeu (*Replay Attack*- en anglais). Pour résoudre ce problème un compteur relatif au temps différent, peut être ajouté dans le paquet pour assurer la fraîcheur de données.

### 2.3.5. La localisation

Le besoin de se localiser et de connaître la position des autres nœuds dans le réseau peut aider pour lutter contre d'éventuelles attaques jouant sur les distances. L'utilité d'un réseau de capteurs se fondera sur ses capacités de localiser automatiquement chaque capteur dans le réseau. Un réseau de capteurs conçu pour détecter des anomalies aura besoin de l'information précise de la position afin d'indiquer exactement l'endroit d'un défaut. [10]

### 2.3.6. Auto-Organisation

Un réseau de capteurs sans fil est un réseau qui exige que chaque nœud capteur soit indépendant et assez flexible à l’auto organisation. Il n'y a aucune infrastructure fixe disponible pour la gestion de réseau dans un réseau de capteurs. L’auto organisation apporte un grand défi à la sécurité du réseau de capteurs sans fil.

## 2.4. Classification des attaques dans les réseaux de capteurs sans fil

Les attaques contre les réseaux de capteurs peuvent être classées selon plusieurs critères bien définies, comme la puissance de l'origine de l'attaque, l'appartenance ou non de ce dernier au réseau. Ces attaques peuvent être divisées aux catégories suivantes [11]:

### 2.4.1. Attaques passives vs Attaques actives

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

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 capteurs importants dans le réseau (Cluster-Head) peuvent ensuite être utilisées pour aider l'attaquant à réaliser d'autres attaques malveillantes.

### 2.4.2. Attaques externes vs attaques internes

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

### 2.4.3. Attaques physiques vs Attaques à distance

Une attaque à distance est mise en œuvre à partir d'une place distante du réseau, par exemple, en émettant un signal à haute énergie pour interrompre la communication. Cependant dans l'attaque physique, un adversaire accède physiquement au nœud de capteurs pour falsifier les données ou pour la destruction matérielle des nœuds.

### 2.4.4. Les attaques impuissantes et les attaques puissantes

Dans les attaques impuissantes (mote-class), l'attaquant utilise un certain nombre de nœuds ayant des capacités équivalentes à celles des nœuds capteurs du réseau pour l'attaquer, alors que dans les attaques puissantes (laptop-class) qui sont les plus dangereuses, l'attaquant fait appel à des dispositifs relativement puissants (exemple : les ordinateurs portables) qui peuvent perturber le réseau en entier.

### 2.4.5. Attaques accidentelles vs attaques intentionnelles

Les attaques accidentelles sont représentées par le disfonctionnement du nœud capteur causé par son environnement (par exemple, les cassures qui peuvent être causées par les animaux dans un réseau agricole). Cependant, les attaques intentionnelles et qui sont les plus fréquentes et les plus nuisibles aux réseaux de capteurs sans fil, sont gérées par des personnes malveillantes ayant un objectif malicieux.

## 2.5. Exemples d'attaques dans les réseaux de capteurs sans fil

### 2.5.1. L'attaque Sinkhole

Dans cette attaque, l'intrus semble très attractif aux autres nœuds, il diffuse des messages falsifiés annonçant qu'il est la meilleure prochaine destination des flux de données des autres nœuds. Selon les métriques adoptées par le protocole de routage suivant lesquelles se porte la décision du routage, les messages falsifiés peuvent annoncer un niveau d'énergie très élevé, un délai minime ou un nombre de sauts optimal vers la station de base [12].

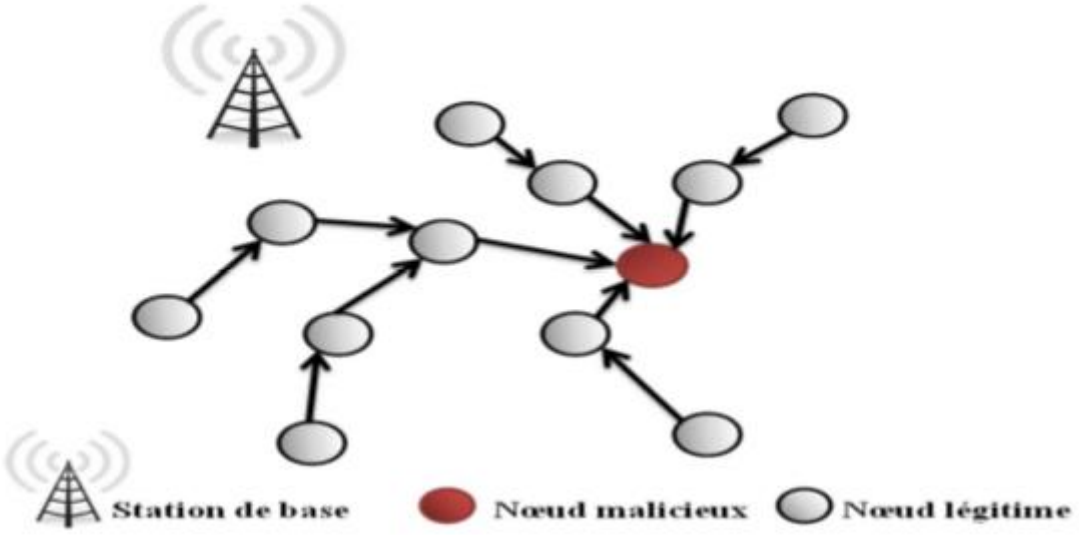


Figure 2-1 : Exemple d'attaque Sinkhole

Le 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 conséquence, 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. [13]

### 2.5.2. L’attaque d’acheminement sélectif (Selective Forwarding)

Dans ce type d’attaque, l’attaquant empêche la transmission de quelques paquets qui seront par la suite supprimés par le nœud malveillant. Le choix des paquets peut être aléatoire ou basé sur quelques critères tel que : le contenu des paquets, adresse source de l’émetteur. Dans la Figure 2-2, le nœud malicieux 5 transmet tous les paquets sauf ceux qu'il reçoit du nœud 4.

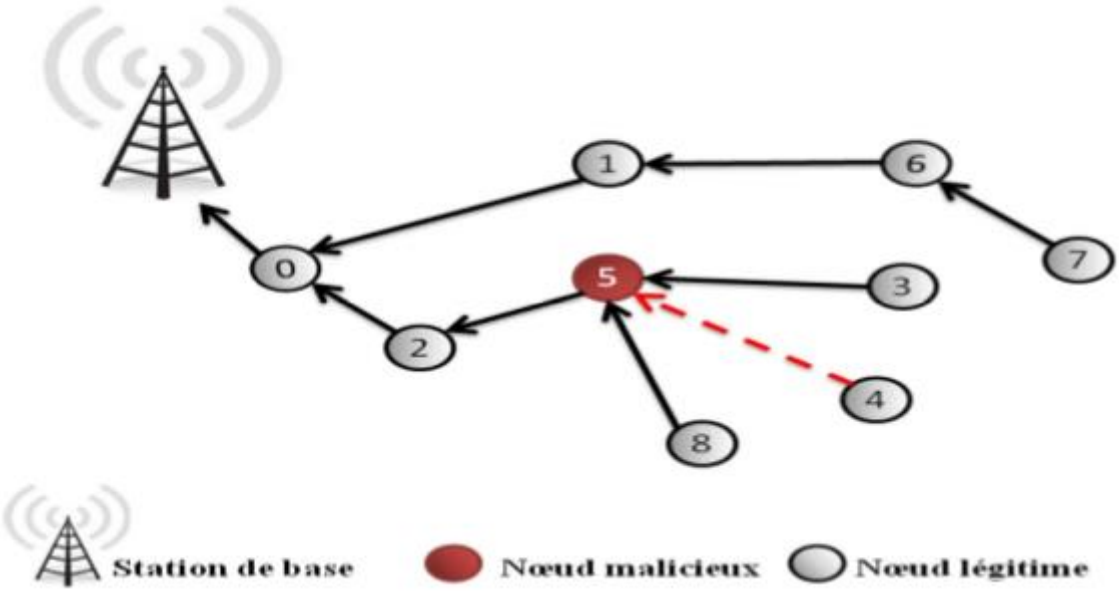


Figure 2-2 : Exemple d’attaque Selectif Forwarding

### 2.5.3. L’attaque Sybil

Dans ce type d’attaque le nœud malicieux fabrique et diffuse plusieurs identités ou des positions géographiques différentes pour maximiser sa chance d’être un point d’intersection entre plusieurs chemins du routage. Notons que les identités annoncées peuvent correspondre à des nœuds réels qui existent dans le réseau, comme elles peuvent être des fausses identités. Cette attaque affecte sensiblement les protocoles de routage multi-chemins. Cette attaque vise à changer l'intégrité des données et les mécanismes de routage.

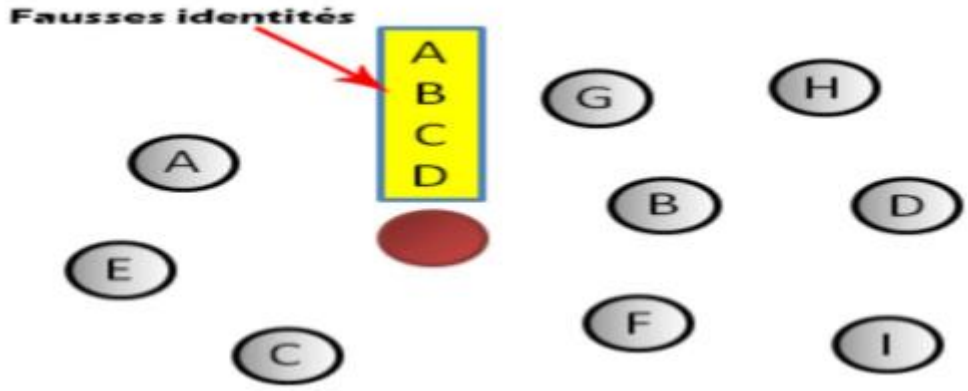


Figure 2-3 : Exemple d'une attaque Sybil

### 2.5.4. L'attaque Hello flood

Dans cette attaque, le nœud malicieux utilise le message 'Hello' pour découvrir les nœuds voisins. Un attaquant utilise ce mécanisme pour consommer l'énergie des capteurs et empêcher leurs messages d'être routés, comme l'illustre la figure 2.4. [14]

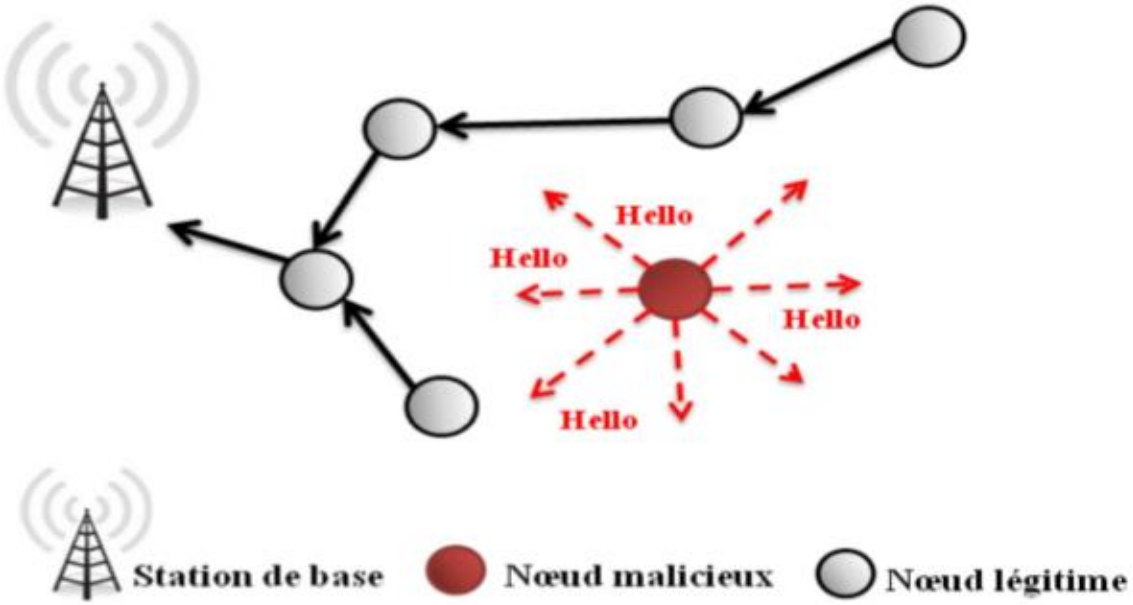


Figure 2-4 : Exemple d'une attaque Hello Flood

### 2.5.5. L'attaque Worm Hole

Dans cette attaque, un nœud malveillant reçoit les paquets de données à un point dans le réseau et les retransmet à un autre nœud malveillant en utilisant un lien «Worm Hole» à haut débit (tunnel) et par conséquence, la communication de la source vers la destination passe par ces nœuds malveillants. L'impact de cette attaque est qu'elle empêche la découverte de routes valides et menace la sécurité de la transmission de paquets de données. [15]

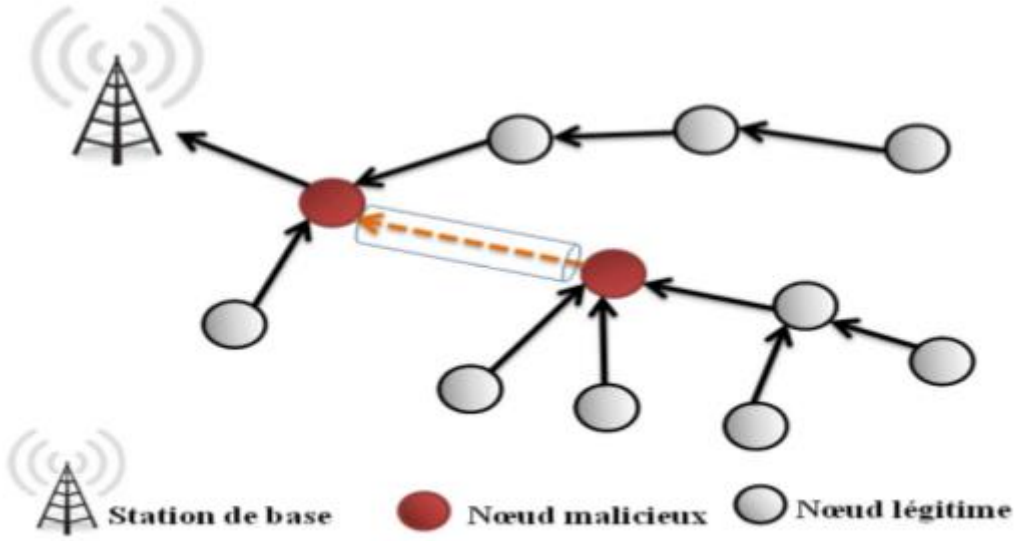


Figure 2-5 : Exemple d'une attaque wormhole

### 2.5.6. L'attaque de Jamming

C'est une attaque de type Déni de Service (DoS) dont le but est de perturber le réseau. 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 plusieurs stratégies pour exécuter l'attaque jamming :

- En émettant un signal radio sans interruption (constant jamming). Cette stratégie nécessite beaucoup d'énergie.
- En émettant régulièrement à intervalle fixe ou d'une façon aléatoire sur un canal. Cette stratégie nécessite moins d'énergie.
- En émettant un signal si le canal est actif (réactive jamming).

### 2.5.7. L’attaque par rejeu de données

Dans ce type d’attaques, l’attaquant rejoue un ancien message plusieurs fois dans le réseau. Cela peut entraîner de fausses alertes ou empêcher le signalement d’une urgence, l’impact pourrait être assez négatif. L’attaque est moins détectable si elle est effectuée par un attaquant interne (un nœud compromis) car elle sera difficile à détecter [12].

## 2.6. Mécanismes de sécurité dans les réseaux de capteurs sans fil

Plusieurs mécanismes sont mis en place afin de répondre à la question de la sécurité dans les réseaux de capteurs sans fil.

Ces mécanismes de sécurité contre les attaques ou les comportements malveillants proposés dans la littérature sont classés en trois catégories [3] :

### 2.6.1. Cryptographie

La cryptographie est utilisée pour assurer l’'authentification, l'intégrité et la confidentialité des données transmises. Les opérations cryptographiques sont basées sur des primitives telles que les fonctions de hachage, le chiffrement symétrique et la cryptographie à clé publique [16].

Les techniques cryptographiques protègent le réseau uniquement contre les attaques externes. Par contre, ce type de mécanisme ne peut pas détecter les attaques internes lorsque l'attaquant connaît les clés de chiffrement et les utilise pour crypter et décrypter les messages.

### 2.6.2. Stéganographie

La stéganographie vise à cacher ou intégrer un message, soit dans un autre message ou dans un ensemble de données multimédia (image, vidéo, etc.). La stéganographie requiert plus de ressources de traitement que les techniques de cryptographie, ce qui nécessite beaucoup d’efforts pour l’intégrer dans les réseaux de capteurs sans fil en raison de leurs ressources limitées.

### 2.6.3. Système de détection d'intrusion (IDS : Intrusion Detection System)

Un système de détection d'intrusion a la capacité de détecter avec une grande précision les attaques internes. Ce mécanisme permet de détecter les activités suspectes et les anomalies sur le réseau analysé et déclenchera une alarme lorsqu'un comportement suspect se produit.

## 2.7. Les systèmes de détection d'intrusion dans les réseaux de capteurs sans fil

Un IDS (Intrusion Detection System), est un outil qui permet de détecter des attaques ou des événements suspects, pouvant poser problèmes, de tenter de les supprimer en suggérant des actions, de déclencher des alertes. Il est capable de détecter avec une grande précision les attaques internes. Ce mécanisme permet de détecter les activités anormales ou suspectes sur le réseau analysé et déclenchera une alarme lorsqu'un comportement suspect se produit.

### 2.7.1. Les principaux composants d'un agent IDS

L'agent IDS est installé dans la couche application [3], il comporte 3 modules. Ces modules sont présentés dans la Figure 2.6.

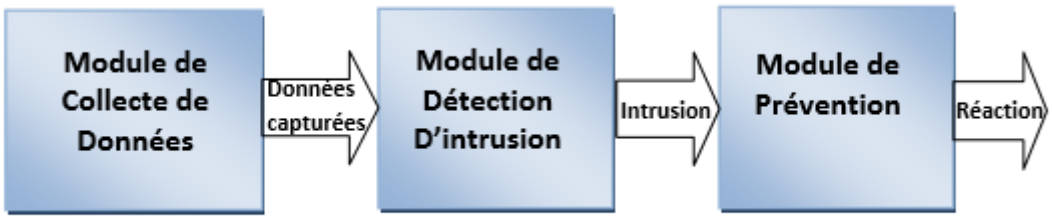


Figure 2.6 Les modules d'un agent IDS

**Module de collecte de données.** Ce module est responsable de la capture des paquets au sein du réseau en filtrant et en formatant les données brutes provenant d'une source de données.

**Module de détection d'intrusion.** C'est un outil matériel ou logiciel qui met en œuvre l'approche choisie pour la détection. Parmi ces approches, il y a la détection à base de signature d'attaquant et la détection d'anomalie.

**Module de prévention.** La prévention d'intrusion est un ensemble d'actions pour anticiper et stopper les attaques. Ces actions peuvent être prédéfinies par exemple comme l'envoi d'une alarme à la station de base.

### 2.7.2. Les différentes technologies des IDSs

### Les systèmes de détection d'intrusion réseau (Network Based IDS)

Ces systèmes visent à intercepter et analyser les paquets qui circulent dans le réseau. Toutes les communications dans le réseau sans fil sont vérifiées. Par conséquent, les nœuds peuvent mutuellement vérifier le trafic réseau. Il est composé de sondes (capteurs) qui capturent le trafic sur le réseau et d'un moteur pour analyser ce trafic.

**Les avantages**

- Contrôler un grand nombre d'hôte avec un petit coût de déploiement.

- Identifier les attaques à plusieurs nœuds.

- Fonctionner dans des environnements cryptés.

**Les inconvénients**

- Ne peut pas fonctionner dans des environnements cryptés.

- Ne permet pas de vérifier si une attaque est couronnée de succès.

### Systèmes de détection d'intrusion basés sur l'hôte (Host Based IDS)

Host Based IDS est un agent logiciel installé sur le nœud à protéger il analyse en temps réel les flux de trafic de cette machine ainsi que les fichiers journaux. Contrairement à un NIDS, un HIDS ne protège donc que le système local.

### Les avantages

- Contrôler avec précision les activités locales des utilisateurs.

- Déterminer si une attaque est couronnée de succès, et déterminer l'impact de cette attaque.

- Assurer une grande sécurité contre les attaques parce qu'il est invisible aux attaquants.

### Les inconvénients

- Difficile à déployer et gérer pour un grand nombre d'hôtes.

## 2.7.3. Les approches d'IDS

## L'approche basée connaissance (A base de 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 de signatures, ce type de système détecte facilement et rapidement les attaques et menaces présentes dans un flux réseau ou sur une machine. [17]

**Les avantages**

- Très efficace pour la détection d'attaques connues avec un taux très bas des alarmes de type faux positif.

- Les alarmes générées sont significatives.

**Les inconvénients**

- Détecte seulement les attaques qui sont déjà enregistrées. Donc, la base de données des signatures doit être toujours mise à jour avec de nouvelles signatures d'attaques .

## L'approche comportementale (La détection d'anomalie)

L'idée principale de la détection d'anomalie est de modéliser durant une période d'apprentissage le comportement "normal" d'un réseau de capteurs sans fil en définissant une ligne de conduite qui comporte les statistiques du réseau durant le comportement normal.

Un profil est donné par une métrique et un modèle statistique. Une métrique est une variable qui modélise le comportement quantitatif du réseau sur une période de temps.

Un modèle est utilisé pour détecter si les nouvelles valeurs du réseau concordent avec les valeurs déjà observées durant l'apprentissage (et supposées normales), et de considérer ensuite (en phase de détection) comme suspect tout comportement inhabituel (les déviations significatives par rapport au modèle de comportement "normal"). [17]

Plusieurs techniques sont utilisées dans l'approche comportementale à savoir :

- Technique de machines à vecteurs de support (SVM).

- Détection basée sur une classification binaire.
- Détection Basée sur les spécifications.
- Utilisation des réseaux de neurones.

**Les avantages**

- Elle n’exige pas des connaissances préalables de toutes les attaques.

- Elle permet la détection de la mauvaise utilisation des privilèges.

**Les inconvénients**

- Génère un nombre élevé d’alarmes de type faux positif en raison des comportements imprévisibles d'utilisateurs et des réseaux.

- Ces approches nécessitent des phases d’apprentissage pour caractériser les profils de comportements normaux et anormaux.

## 2.8. Conclusion

Les réseaux de capteurs sans fil sont souvent déployés dans des environnements insécurisés. Ces capteurs sont vulnérables aux menaces internes ou externes. Les systèmes de détection d'intrusion (IDS) étant très efficaces dans la protection du réseau contre les attaques.

Dans ce chapitre, j’ai présenté les contraintes et les exigences de sécurité, la classification des attaques, ainsi que quelques types d’attaques connues.

Il est clair que les mécanismes de sécurité utilisées dans les réseaux traditionnels ne peuvent pas être directement appliquées aux réseaux de capteurs sans fil, vu les contraintes de sécurité qui caractérisent ce type de réseau. En conséquence, les réseaux de capteurs sans fil exigent l’adaptation des mécanismes de sécurité aux caractéristiques et aux vulnérabilités des réseaux de capteurs sans fil.

# CHAPITRE 3. SIMULATION ET PROPOSITION

## 3.1. Introduction

Dans le développement d'un réseau de capteurs sans fil pour une application réelle, la simulation par un logiciel de son comportement et de ses performances est essentielle.

Plusieurs facteurs changent le comportement d'un RCSF dont la partie physique (antenne et radio), la topologie, le canal de propagation, la consommation d'énergie, et le protocole de communication.

L'objectif de cette partie est d'interpréter les résultats de différentes simulations faites sur un RSCF sous certaines conditions, pour chaque simulation nous récupérons les résultats des messages reçus et la consommation d'énergie, afin de concevoir une application qui détecte automatiquement la présence des attaques en se basant sur les signatures d'attaques observées dans la phase de simulations.

Ainsi, dans ce chapitre nous allons présenter l'environnement de simulation de réseau CONTIKI COOJA et l'application proposée écrite en C++ sous la plateforme Qt.

## 3.2. Présentation de l'environnement de simulation

### 3.2.1. Intérêt de la simulation

Une expérimentation directe exécutée sur les réseaux de capteurs sans fils réels peut être très couteuse ou impossible.

Plusieurs environnements de simulation ont été créés afin de simplifier les études sur les RSCFs en termes de temps et de coût financier.

La simulation permet ainsi de tester à moindre coût les nouveaux protocoles et d'anticiper les problèmes qui pourront se poser dans le futur afin d'implémenter une meilleure technologie.

### 3.2.2. Les principaux critères de choix d'un simulateur

Le choix d'un simulateur approprié à notre étude est fait parmi plusieurs simulateurs existants : OMNET++, TinyOS, MANTISOS, CONTIKI-OS..., il est important de fixer les

critères de choix de simulateur convenable pour notre étude. Voici les principaux critères de choix de simulateur :

- La gratuité ou non du simulateur.
- La plateforme sur laquelle le simulateur fonctionne.
- L'existence de la notion des RCSFs.
- Le langage de développement utilisé.
- La disponibilité sur le web.
- La visualisation des paramètres et indication des résultats ex. consommation d'énergie.

### 3.2.3. CONTIKI

Contiki est un système d'exploitation léger et flexible pour les capteurs sans fils, il est créé par une équipe du centre suédois de recherche scientifique SICS.

Destiné à être embarqué dans des capteurs miniatures ne disposant généralement que de ressources limitées, Contiki propose les principales caractéristiques et fonctionnalités d'un système d'exploitation tout en favorisant une consommation énergétique et une empreinte mémoire minimales. Ses principales caractéristiques sont le support des protocoles IPv6 et 6LoWPAN, sa flexibilité et sa portabilité. Disponible gratuitement sous licence BSD, Contiki peut être utilisé et modifié, même à des fins commerciales.

#### Fonctionnement et théorie

Écrit en langage C, 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 d'entrées/sorties.

Il fournit ensuite aux applications informatiques des interfaces permettant d'utiliser ces ressources. Contiki occupe peu d'espace en mémoire et permet une consommation d'énergie très faible.

Contiki offre deux types de connectivité :

La couche Rime, elle permet un dialogue vers les capteurs voisins ainsi que le routage.

La couche uIP, orientée Internet, elle offre les services essentiels du protocole IP mais nécessite plus de ressources que Rime.

Pour économiser la mémoire, tout en fournissant un bon contrôle de flux dans le code, Contiki utilise un mécanisme appelé Protothreads qui englobe la programmation événementielle et la programmation multithreads. Contiki gère les standards 6LoWPAN, RPL13, CoAP14. Contiki offre également des services comme un serveur Telnet fournissant un accès similaire à un Shell Unix, un serveur web, une interface graphique fournie par un serveur VNC et d'autres fonctionnalités comme un navigateur web.

### 3.2.4. Le simulateur COOJA

Contiki propose un simulateur de réseau appelé Cooja. Ce simulateur permet l'émulation de différents capteurs sur lesquels seront chargés un système d'exploitation et des applications. COOJA permet ensuite de simuler les connexions réseaux et d'interagir avec les capteurs. Cet outil permet aux développeurs de tester les applications à moindre coût. Il offre une variété des capteurs supportés comme : exp5438, z1, wismote, micaz, sky, jcreate, esb.

Pour dérouler les tests de simulations nous avons utilisé le simulateur inclus dans le système contiki appelé COOJA, qui a les caractéristiques suivantes [3] :

– COOJA combine des simulations de capteurs matériels de nœuds et simulations du comportement de haut niveau en une seule simulation.

– COOJA est flexible et extensible de manière à ce que tous les niveaux du système peuvent être modifiés ou remplacés.

–COOJA est une application Java, toutes les interactions avec le Code Contiki se fait à travers Java Native Interface (JNI). L’interface de simulateur COOJA est composée de plusieurs fenêtres (plugins), comme illustré dans la Figure 3.1.

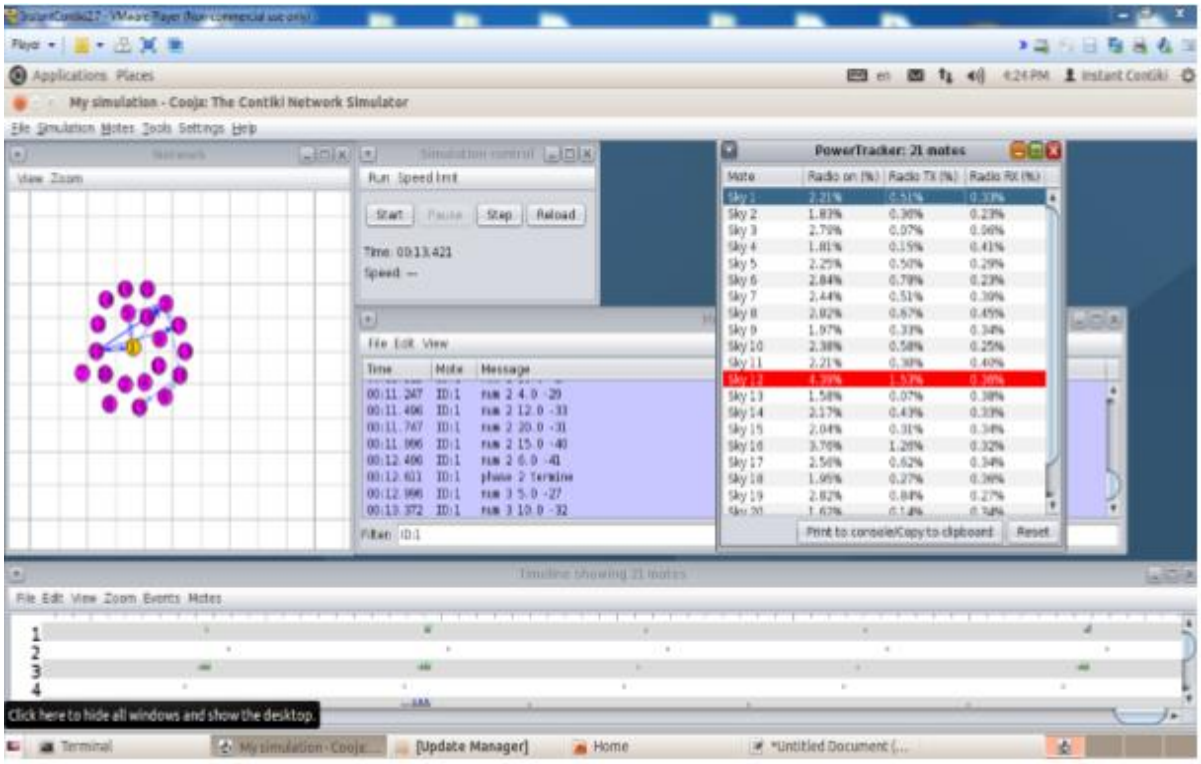


Figure 3.1. Interface de simulateur COOJA

- Mote output : présente ce que les capteurs génèrent comme sortie via leurs ports séries.

- Network : présente le réseau simulé et le flux de communication durant la simulation.

- 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.

– Power tracker : pour voir la consommation d'énergie par les capteurs durant la simulation.

## 3.2.5. Installation

Pour l'installation de Contiki et le simulateur COOJA :

• Il faut télécharger instant Contiki depuis Sourceforge par exemple. Il s'agit d'un fichier de grande taille (presque 2GB) ; une fois le téléchargement fini il faut décompresser le fichier instant contiki.zip et placer le nouveau répertoire sur le bureau.

• Dans une deuxième étape, il faut télécharger et installer la machine virtuelle VMwarePlayer et lancer le fichier instant Contiki2.7.vmx dans VMware Player, et attendre le démarrage d'Ubuntu linux.

• Dans la dernière étape il faut se connecter à Contiki Cooja et faire les configurations nécessaires.

## 3.3. Déroulement des simulations

Nous avons effectué les tests sur les réseaux qui ont la topologie en étoile et à chaque fois on introduit un nœud malicieux. Grâce à un programme écrit en langage C, que nous avons réalisé, nous récupérons les résultats, qui nous intéressent, à savoir :

– Moyenne de messages reçus à temps : Si les capteurs envoient un message chaque 1s par exemple, en 1 minute (le temps de la simulation) chaque capteur va envoyer environ 60 messages. Ce qui fait que le capteur mobile peut recevoir jusqu'à 60 groupes de massages, les messages de chaque groupe ont le même identifiant qui sera incrémenté lors de la transmission du prochain groupe.

– Moyenne de messages arrivés en retard : Un message dit qu'il est en retard, il n'est pas arrivé avec son groupe.

– Consommation d'énergie : Grâce au plugin Powertracker de Cooja, nous pouvons récupérer le pourcentage de consommation d'énergie de chaque capteur durant la simulation.

On a utilisé les trois scénarios suivants :

1. Le scénario sans attaque.
2. Le scénario avec l'attaque de trou noir.
3. Le scénario avec l'attaque Hello Flood.

### Les métriques utilisées dans la simulation

A-Taux de paquets reçus ou Packet Delivery Ratio (PDR) : Le PDR est le rapport entre le nombre des paquets qui sont délivrés avec succès à une destination sur le nombre de paquets qui ont été envoyés par l'expéditeur [18].

B- Taux de perte de paquets ou Packet Loss Rate (PLR) : Le PLR est le rapport entre le nombre de paquets qui ne sont pas arrivés à la destination souhaitée et le nombre total de paquets transmis [18].

C- Le taux de consommation d'énergie : est récupéré par le plugin Powertracker de Cooja, ce paramètre indique la présence ou non d'une attaque sur le RCSF.

## 3.4. Résultats et interprétations

### 3.4.1 Scénario 1 : Un réseau de capteurs sans fil sans attaque

Dans le premier scénario on utilise un réseau de capteurs sans fil composé de dix (10) nœuds avec une topologie en étoile avec des positions aléatoires et sans utiliser un nœud malicieux.

Les paramètres de ce scénario sont exprimés dans le tableau suivant

| Paramètres | Valeurs |
|---|---|
| Simulateur | Contiki Cooja 2.7 |
| Attaque | Pas d'attaque |
| Temps de simulation | 3600s (1h) |
| Nombre de nœud | 10 |
| Nombre de nœud malicieux | 0 |
| Topology | etoile |
| La norme | 802.11 |

Tableau 3.1. Les paramètres du scénario 1

Et la topologie du réseau est schématisée dans la figure suivante

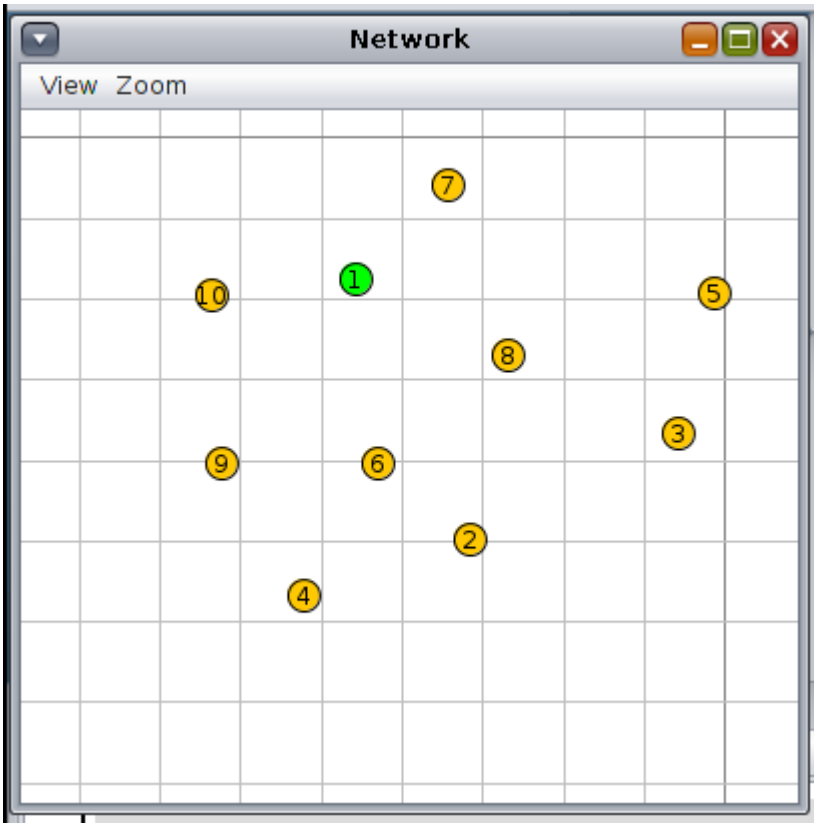


Figure 3.2. Scénario 1 : Un réseau de capteurs sans fil sans attaque

- Le taux de paquets livrés avec succès (PDR)

| Data sent | Data received |
|---|---|
| 531 | 531 |

PDR = 531 / 531 = 100 %

- Le taux de paquets perdus (PLR)

PLR = (531-531) / 531 = 0 %

- La consommation d'énergie : on a observé le comportement énergétique du réseau dans les cas idéaux

| nœud | CPU power | LPM power | Listen power | Transmit power | Power |
|---|---|---|---|---|---|
| **1** | 0,354 | 0,153 | 0,389 | 0,034 | 0,93 |
| **2** | 0,338 | 0,156 | 0,391 | 0,038 | 0,923 |
| **3** | 0,402 | 0,151 | 0,421 | 0,039 | 1,013 |
| **4** | 0,311 | 0,154 | 0,379 | 0,042 | 0,886 |
| **5** | 0,351 | 0,153 | 0,403 | 0,028 | 0,935 |
| **6** | 0,36 | 0,153 | 0,402 | 0,031 | 0,946 |
| **7** | 0,369 | 0,152 | 0,383 | 0,029 | 0,933 |
| **8** | 0,356 | 0,153 | 0,383 | 0,031 | 0,923 |
| **9** | 0,354 | 0,153 | 0,401 | 0,035 | 0,943 |
| **10** | 0,356 | 0,152 | 0,399 | 0,037 | 0,944 |

Tableau 3.2. La consommation d'énergie dans le scénario 1

### 3.4.2. Scénario 2 : Un réseau de capteurs sans fil avec l'attaque black hole

Dans ce scénario, on a changé le nœud numéro 10 par un nœud malicieux qui effectue l'attaque de trou noir, ce nœud fait discrètement disparaitre le trafic sans informer la source du trafic. Lors de l'examen d'un réseau informatique, les trous noirs ne peuvent pas être détectés.

Les paramètres et la topologie de ce scénario sont décrits dans le tableau et la figure suivantes

| Paramètres | Valeurs |
|---|---|
| Simulateur | Contiki Cooja 2.7 |
| Attaque | black hole |
| Temps de simulation | 3600s (1h) |
| Nombre de nœud | 10 |
| Nombre de nœud malicieux | 1 |
| Topology | etoile |
| La norme | 802.11 |

Tableau 3.3. Les paramètres du scénario 2

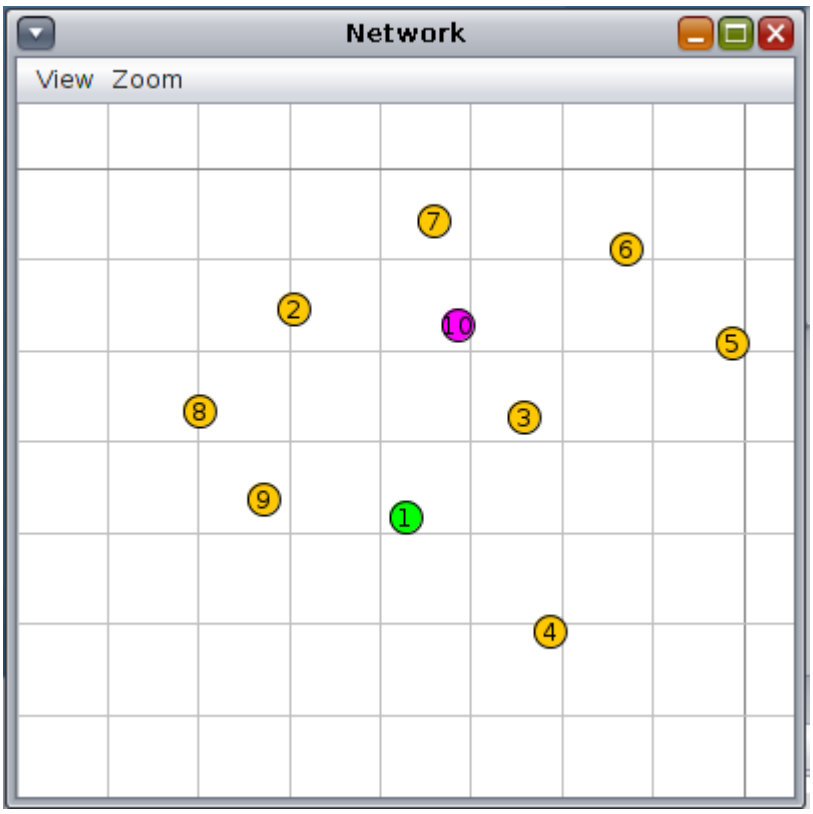


Figure 3.3. Scénario 2 : Un réseau de capteurs sans fil avec l'attaque black hole

- Le taux de paquets livrés avec succès (PDR)

| Data sent | Data received |
|---|---|
| 548 | 497 |

PDR = 497 / 548 = 90.69 %

- Le taux de paquets perdus (PLR)

PLR = (548-497) / 548 = 9.31 %

- La consommation d'énergie : on a observé le comportement énergétique du réseau dans les cas idéaux

| nœud | CPU power | LPM power | Listen power | Transmit power | Power |
|---|---|---|---|---|---|
| 1 | 0,354 | 0,157 | 0,407 | 0,028 | 0,946 |
| 2 | 0,389 | 0,153 | 0,389 | 0,03 | 0,961 |
| 3 | 0,384 | 0,151 | 0,389 | 0,032 | 0,956 |
| 4 | 0,356 | 0,154 | 0,402 | 0,029 | 0,941 |
| 5 | 0,351 | 0,151 | 0,392 | 0,035 | 0,929 |
| 6 | 0,378 | 0,153 | 0,372 | 0,032 | 0,935 |
| 7 | 0,379 | 0,151 | 0,38 | 0,03 | 0,94 |
| 8 | 0,377 | 0,157 | 0,371 | 0,032 | 0,937 |
| 9 | 0,359 | 0,153 | 0,393 | 0,034 | 0,939 |

Tableau 3.4. La consommation d'énergie dans le scénario 2

On constate un comportement non idéal par le réseau de capteurs sans fil où il y a une perte de message équivalente à 9% causé par l'attaque effectué par le nœud malicieux, mais le comportement énergétique des nœuds est semblable au scénario sans attaque.

### 3.4.3. Scénario 3 : Un réseau de capteurs sans fil avec l'attaque Hello Flood

Dans ce scénario on a changé le nœud numéro 10 par un nœud malicieux qui effectue l'attaque de Hello Flood, ce nœud émet des messages de type « hello » en permanence pour consommer l'énergie des capteurs voisins et empêcher leurs messages d'être routés.

Les paramètres et la topologie de ce scénario sont décrits dans le tableau et la figure suivants.

| Paramètres | Valeurs |
|---|---|
| Simulateur | Contiki Cooja 2.7 |
| Attaque | Hello Flood |
| Temps de simulation | 3600s (1h) |
| Nombre de nœuds | 10 |
| Nombre de nœuds malicieux | 1 |
| Topology | etoile |
| La norme | 802.11 |

Tableau 3.5. Les paramètres du scénario 3

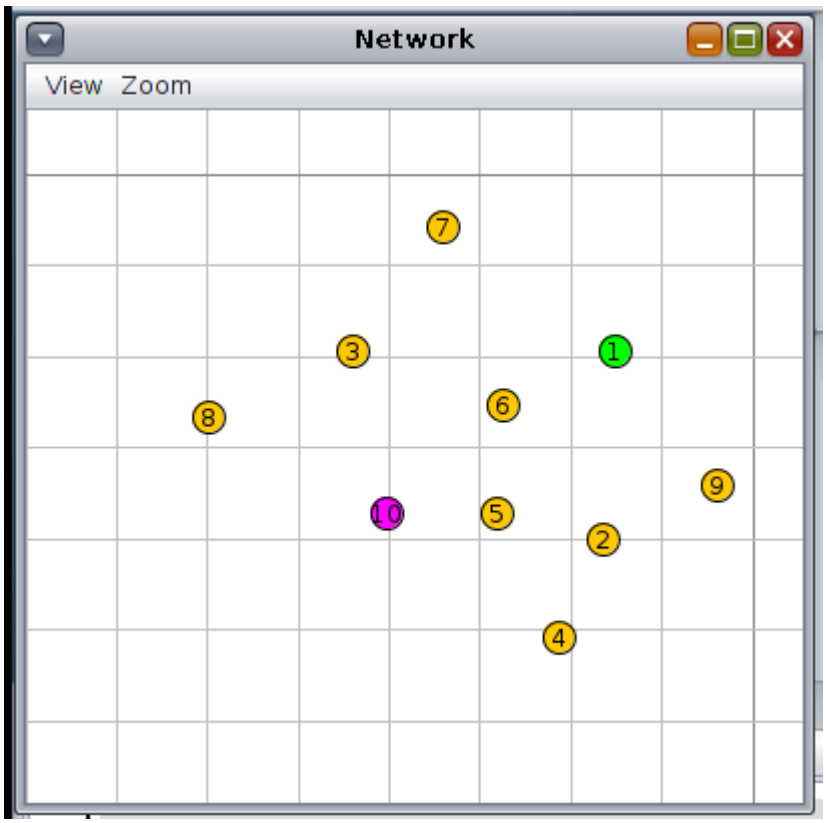


Figure 3.4. Scénario 3 : Un réseau de capteurs sans fil avec l'attaque Hello Flood

- Le taux de paquets livrés avec succès (PDR)

| Data sent | Data received |
|---|---|
| 539 | 538 |

PDR = 538 / 539 = 99.81 % (Presque 100 %)

- Le taux de paquets perdus (PLR)

PLR = (539-538) / 539 = 0.19 %

- La consommation d'énergie : on a observé une consommation excessive d'énergie dans le capteur 5.

| nœud | CPU power | LPM power | Listen power | Transmit power | Power |
|---|---|---|---|---|---|
| 1 | 0,353 | 0,154 | 0,388 | 0,034 | 0,929 |
| 2 | 0,339 | 0,154 | 0,339 | 0,037 | 0,869 |
| 3 | 0,401 | 0,15 | 0,461 | 0,041 | 1,053 |
| 4 | 0,35 | 0,158 | 0,377 | 0,029 | 0,914 |
| 5 | 1,861 | 0,772 | 1,997 | 0,252 | 4,882 |
| 6 | 0,379 | 0,15 | 0,4 | 0,03 | 0,959 |
| 7 | 0,357 | 0,151 | 0,408 | 0,011 | 0,927 |
| 8 | 0,351 | 0,151 | 0,387 | 0,016 | 0,905 |
| 9 | 0,35 | 0,157 | 0,405 | 0,022 | 0,934 |

Tableau 3.6. La consommation d'énergie dans le scénario 3

On constate dans ce scénario que le taux de messages délivrés est presque parfait, pas de perte de message or le nœud capteur numéro 5 consomme trop d'énergie., son comportement énergétique est causé par le nœud malicieux qui émet constamment des message de type « hello ».

## 3.5. Proposition

Dans les chapitres précédents, j'ai parlé sur les réseaux en général et les réseaux de Capteurs Sans Fil (RCSFs) ou Wireless Sensor Network (WSN) en partant de leur cellule élémentaire, le capteur sans fil, ensuite j'ai présenté les aspects fondamentaux de la sécurité des réseaux de capteurs sans fil. Je présente également les solutions de base, qui sont proposées dans la littérature pour répondre aux besoins en termes de sécurité et j'ai réalisé des simulations des scénarios sur le simulateur Contiki Cooja.

Notre proposition est un IDS basé sur les scénarios qui sont des IDS avec base de connaissance des signatures d'attaques connues, dans notre cas on a opté pour l'attaque « hello flood » et « black hole », cette application est écrite en C++ sous la plateforme Qt et pend en entrée les métriques du réseau et les compare avec celle d'un réseau idéal et un réseau sous les attaques précédentes.

### 3.5.1 L'environnement de l'application

Qt est une bibliothèque multiplateforme pour créer des GUI (programme sous forme de fenêtre). Qt est écrite en C++ et est faite pour être utilisée à la base en C++, mais il est aujourd'hui possible de l'utiliser dans d'autres langages comme Java, Python, etc.

Qt est constituée d'un ensemble de modules. On peut y trouver entre autres ces fonctionnalités :

- ✓ Module GUI: c'est toute la partie création de fenêtres. Nous nous concentrerons surtout sur le module GUI dans ce projet.
- ✓ Module OpenGL: Qt peut ouvrir une fenêtre contenant de la 3D gérée par OpenGL.
- ✓ Module de dessin: pour dessiner dans des fenêtres (en 2D).
- ✓ Module réseau: Qt fournit une batterie d'outils pour accéder au réseau, que ce soit pour créer un logiciel de Chat, un client FTP, un lecteur de flux RSS, etc.
- ✓ Module SVG: possibilité de créer des images et animations vectorielles, à la manière de Flash.

- ✓ Module de script: Qt supporte le Javascript (ou ECMAScript), que l'on peut réutiliser dans des applications pour ajouter des fonctionnalités, sous forme de plugins par exemple.
- ✓ Module XML: c'est un moyen très pratique d'échanger des données avec des fichiers formés à l'aide de balises, un peu comme le XHTML.
- ✓ Module SQL: permet un accès aux bases de données (MySQL, Oracle, PostgreSQL...).

### 3.5.2. Présentation de l'interface

L'interface de notre application est composée de cinq zones principales :

**Zone 1 :** Où les réseaux enregistrés sont listés, elle comporte plus de 10 réseaux.

**Zone 2 :** Elle comporte un bouton pour charger le réseau, puis l'analyser, et les résultats seront affichés dans les autre zones.

**Zone 3 :** Elle donne les informations et des remarque sur le comportement du réseau.

**Zone 4 :** Elle affiche la nature de l'attaque si elle existe.

**Zone 5 :** Elle donne les informations sur la structuration du réseau choisi.

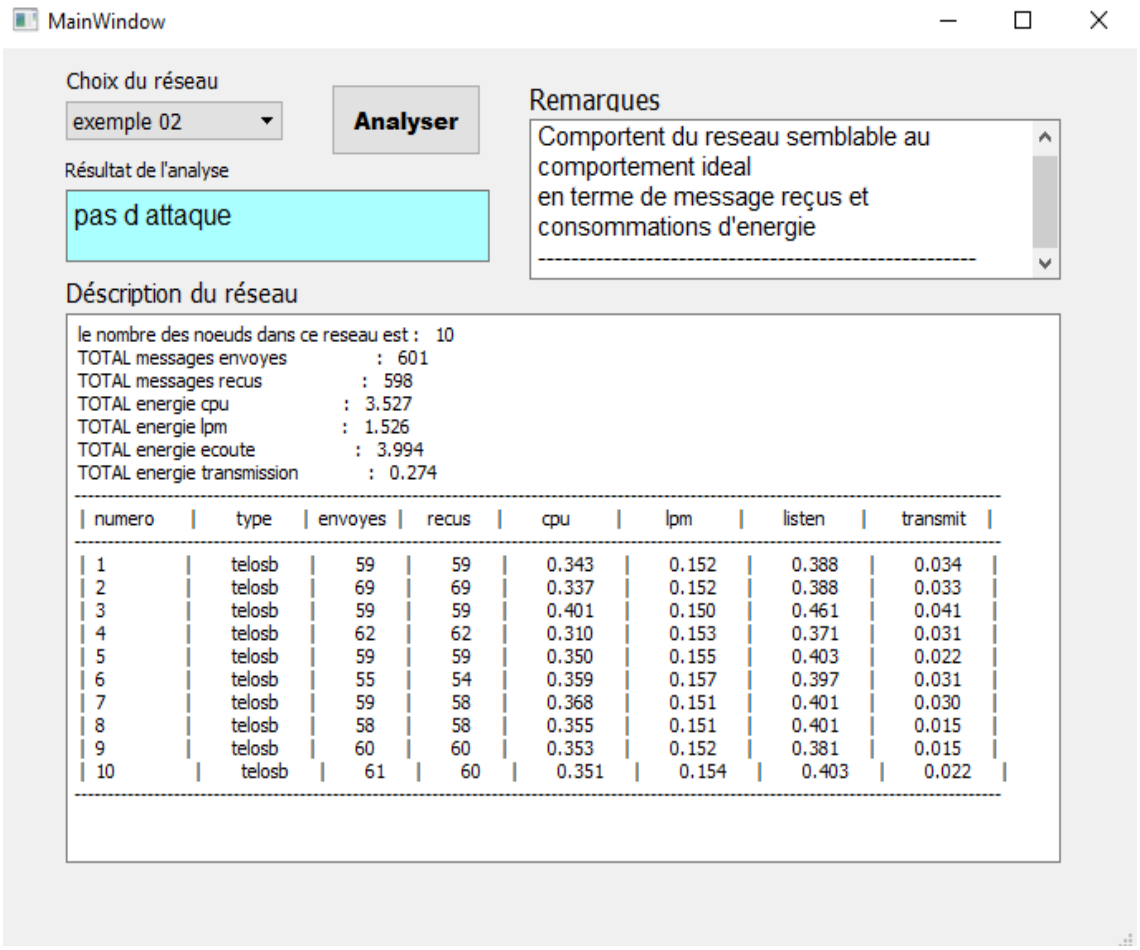


Figure 3.5. Interface de l'application

### 3.5.3. Fonctionnement de l'application

L'application a comme entrée, des données numériques capturées après la simulation d'un réseau sous le simulateur Cooja en utilisant le module PowerTracker pour mesurer l'énergie dépensée par chaque capteur, ensuite, ces données seront comparées à celles de la liste des signatures d'attaques enregistrées, s'il y a une correspondance, l'application va afficher les remarques observées sur le comportement du réseau et afficher l'attaque suspecte correspondante, sinon l'application va indiquer l'absence d'attaques.

Voici quelques exemples du fonctionnement de l'application :

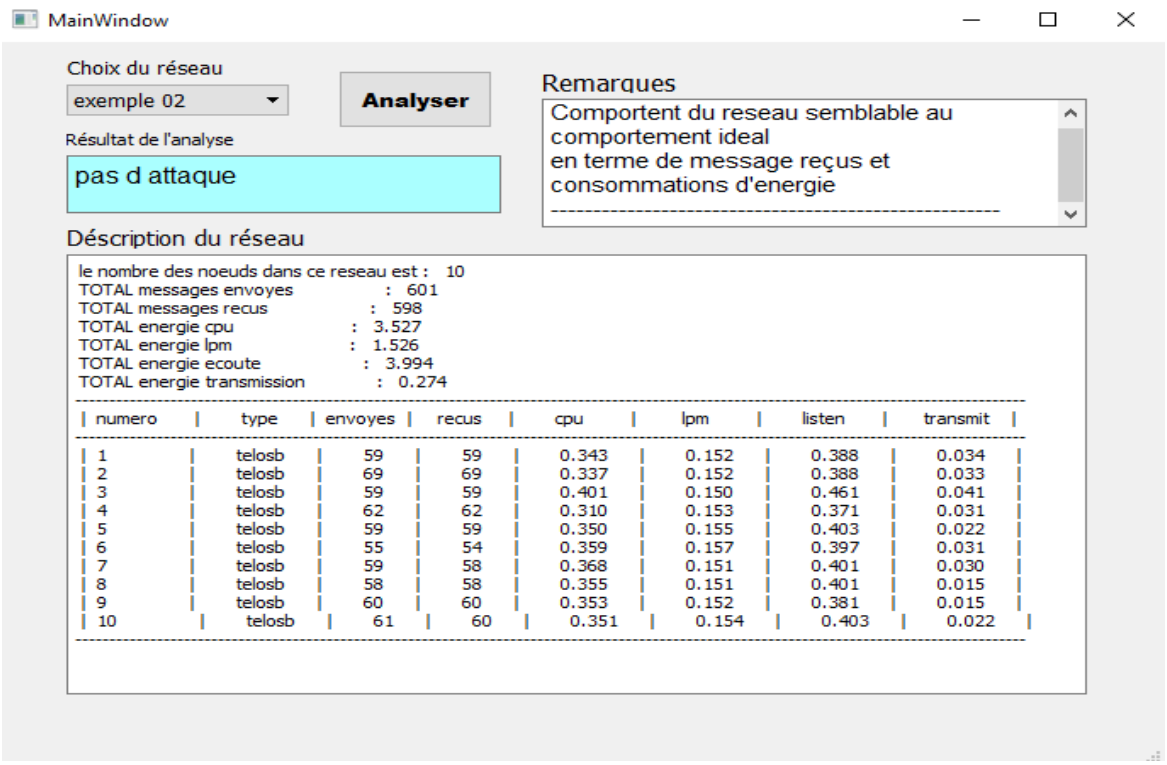


Figure 3.6. Exemple 1 du fonctionnement d'application

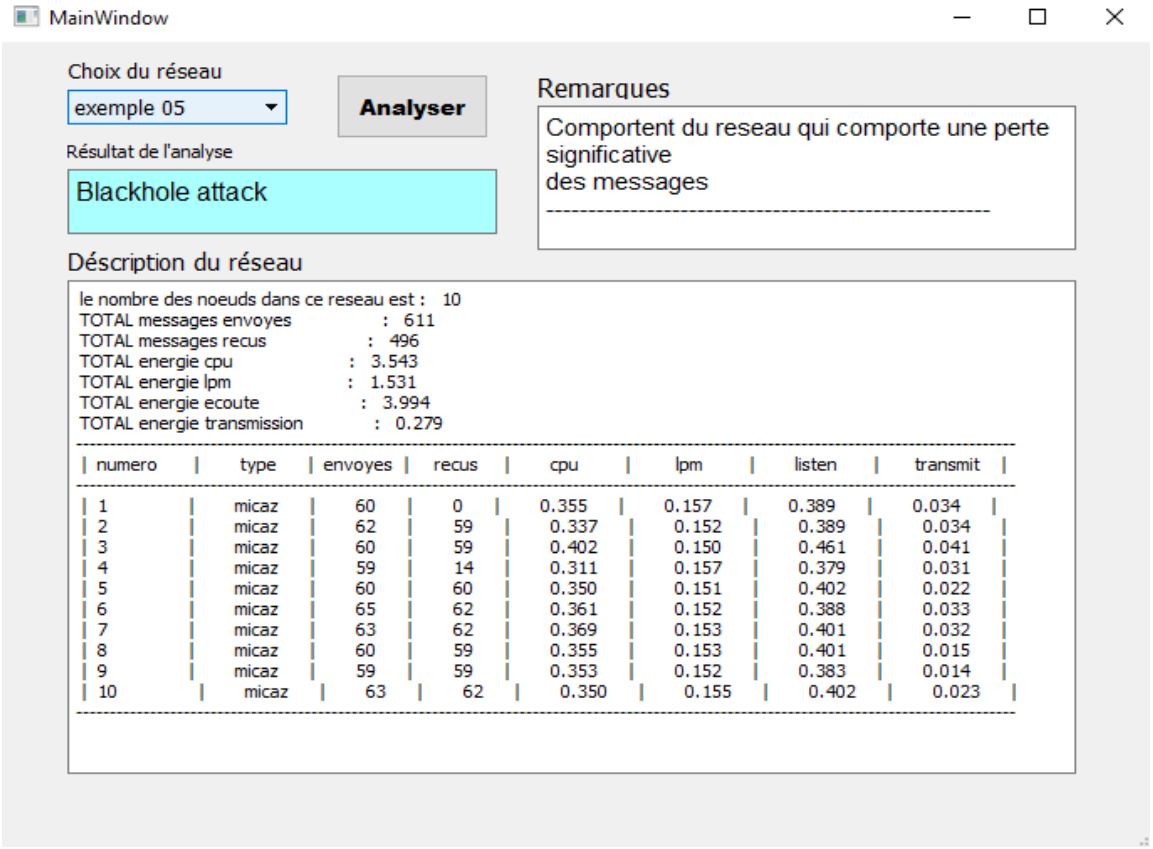


Figure 3.7. Exemple 2 du fonctionnement d'application

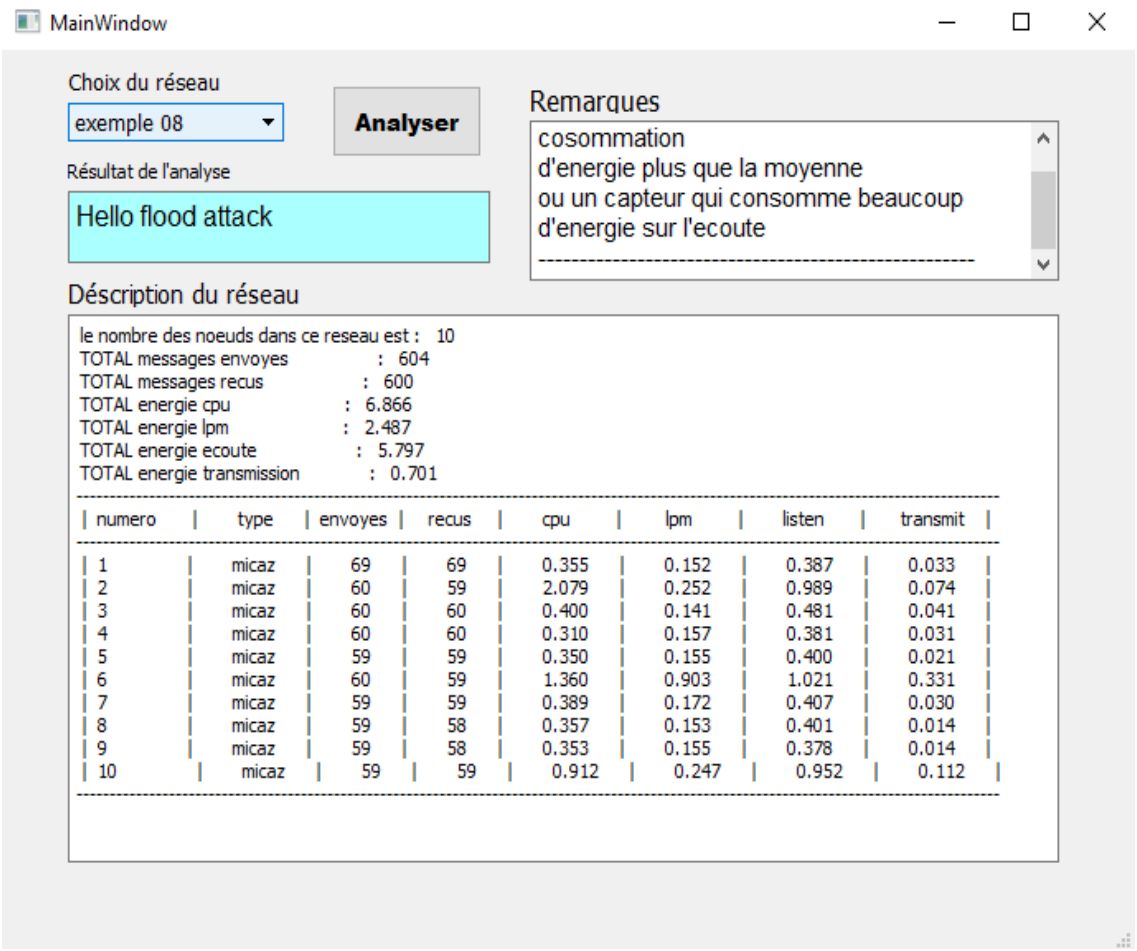


Figure 3.8. Exemple 3 du fonctionnement d'application

### 3.5.4. Diagramme de séquence

Le diagramme de séquence fait parties des diagrammes comportementaux (dynamique) et plus précisément des diagrammes d'interactions. Il permet de représenter des échanges entre les différents objets et acteurs du système en fonction du temps. Il montre la séquence des échanges de messages entre les objets participant à un scénario.

Le diagramme de notre application est représenté sur la figure 3.9. Sur ce diagramme, nous nous apercevons qu'il existe essentiellement quatre objets principaux dans notre système à savoir :

L'utilisateur : c'est la personne qui veut utiliser l'application, il est chargé de choisir le réseau à analyser, ensuite il va voir l'affichage des résultats d'analyse.

L'interface : c'est l'interface de l'application, elle est chargée de l'interaction avec l'utilisateur, et de transmettre ces choix aux autre composantes de l'application.

La fonction de comparaison : est la partie du code chargée de comparer les données du réseau à analyser avec celle des réseaux enregistrés dans la bases de signatures d'attaques, la fonction de comparaison génère des remarques sur le comportement du réseau aussi indique s'il y a une attaque.

Les signatures : est un ensemble de données numériques capturées après la simulation d'un réseau dans le cas sans attaques ou avec attaques, cet ensemble est la liste des signatures d'attaques.

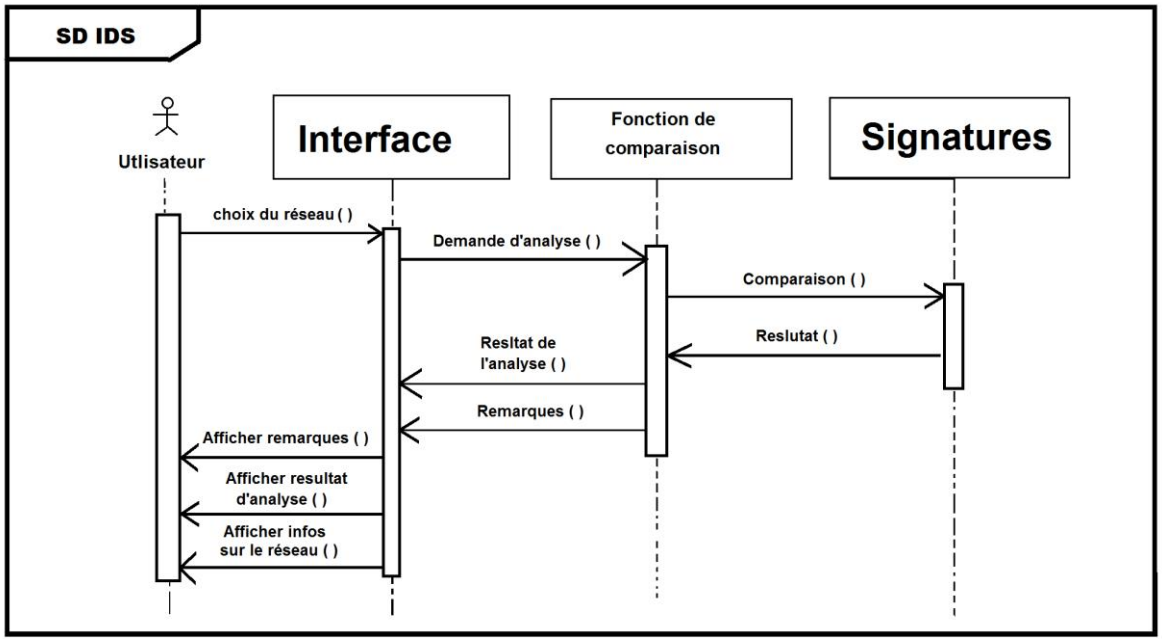


Figure 3.9. Diagramme de séquence

## 3.6. Conclusion

Dans ce chapitre, nous avons effectué des simulations faites sur un RSCF dans plusieurs scénarios, pour chaque simulation nous récupérons les résultats des messages reçus et la consommation d'énergie, ainsi nous avons interprété les résultats de ces différentes simulations.

Ensuite nous avons présenté l'application que nous avions proposée et donné des explications sur toutes les fonctionnalités qu'elle assure. Après, nous avons donné quelques exemples de fonctionnement de cette application.

# CONCLUSION GENERALE

Les réseaux de capteurs constituent un axe de recherche très fertile ainsi qu'un outil qui peut être appliqué dans plusieurs domaines différents. Cependant, il reste encore de nombreux problèmes de sécurité à résoudre dans ce domaine pour un fonctionnement efficace de ces réseaux et afin de pouvoir les utiliser dans les conditions réelles.

Parmi ces problèmes, on a le problème de la détection des attaques et l'une des solutions proposées est le système de détection d'intrusion

Un IDS (Intrusion Detection System), est un outil qui a pour vocation la surveillance d'un ou plusieurs réseaux de machines. Il y a deux approches importantes des IDS : L'approche basée connaissance (La détection d'abus (misuse detection), et l'approche comportementale (La détection d'anomalie (anomaly detection).

Cependant, il reste encore de nombreux problèmes à résoudre dans ce domaine afin de pouvoir les utiliser dans les conditions réelles Parmi les problèmes qu'on peut rencontrer dans ce genre de réseaux, nous citons la problématique de la sécurité, et pour cela le réseau sera exposé à plusieurs types d'attaques interne et externe.

Dans ce mémoire on a étudié la nature des réseaux de capteurs sans fil et la sécurité de ce type de réseau, et on a aussi étudié les systèmes de détection d'intrusion applicables pour les RCSFs, ensuite nous avons effectué des simulations dans plusieurs scénarios, ainsi nous avons interprété les résultats de ces différentes simulations.

A la fin, nous avons présenté l'application que nous avions proposée et donné des explications sur toutes les fonctionnalités qu'elle assure. Après, nous avons donné quelques exemples de fonctionnement de cette application.

Néanmoins, notre travail reste perfectible et des extensions et améliorations doivent être menées. Pour cela, nous recommandons, comme perspectives à ce travail :

- Son extension au cas des différentes attaques pour enrichir la base de signatures.
- L'adaptation du système de détection d'intrusion au temps réel.
- L'étude de faisabilité d'un système de détection d'intrusion basé sur la détection d'anomalie, ou même d'un système de détection d'intrusion hybride qui utilise les deux approches en même temps pour une meilleure détection.

# BIBLIOGRAPHIE

[1] MEZRAG Fares " Sécurité du Routage Hiérarchique Basée sur les Clusters dans les Réseaux de Capteurs sans Fil " - Thèse de Magister – Université 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] S.A.H. SEDJELMACI, Mise en œuvre de mécanismes de sécurité basés sur les IDS pour les réseaux de capteurs sans fil, Thèse de doctorat, Février 2013.

[4] K. BADER, Détection d'intrusions dans les réseaux de capteurs sans fil, Rapport de Stage 2009-2010.

[5] F.Z BEVHAMIDA.Tolerance aux pannes dans les reseaux de capteur sans fil.memoire de magistere en ingenierie des systemes informatique,Ecole Nationale superieure en informatique, Alger,Algerie,2009.

[6] :I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. " Wireless sensor Networks : a survey ", article .BWNL, SECE, GIT, Atlenta, USA, 20 December 2001.

[7] S. Abbes,"Implémentation d'une application orientée surveillance pour les réseaux de capteurs", Université Abou Bakr Belkaid- Tlemcen Faculté des Sciences Département d'Informatique, 2011 /2012.

[8] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless Sensor Network Security: A Survey ", Department of Computer Science Wayne State University.

[9] Guy Pujolle. "Les Reseaux". 5eme edition, 2006, ISBN : 2-212-11987-9.

[10] Y.CHALLAL, Réseaux de capteurs sans fils, Support de cours, 2008.

[11] C. Karlof, D. Wagner, Secure routing in wireless sensor networks: attacks and Countermeasures Ad Hoc Networks 1 (2) (2003) 293–315.

[12] S. Sahraoui, S. Bouam, Secure routing optimization in hierarchical cluster-based wireless sensor networks, International Journal of Communication Networks and Information Security (IJCNIS) 5 (3) (2013) 178-185.

[13] Y. Shen, S. Liu, Z. Zhang, Detection of Hello Flood Attack Caused by Malicious Cluster Heads on LEACH Protocol, International Journal of Advancements in computing Technology 7 (2) (2015) 40-47.

[14] W.ZNAIDI, Quelques propositions de solutions pour la sécurité des réseaux de capteurs sans fil, Thèse de doctorat, 2010.

[15] Al-kahtani, M.S, "Survey on security attacks in Vehicular Ad hoc Networks(VANETs)", in Signal Processing and Communication Systems (ICSPCS), 2012 6thInternational Conference on, pp. 1-9, December 2012, Gold Coast, Australia. PrintISBN: 978-1-46732392-5.

[16] R. Roman, C. Alcaraz, and J. Lopez, "A Survey of Cryptographic Primitives and Implementations for Hardware-Constrained Sensor Network Nodes", Mobile Networks and Applications, 12 ( 4): 231244, 2007.

[17] Mme LABED Ines, « Proposition d'un système immunitaire artificiel pour la détection d'intrusions», UNIVERSITE MENTOURI DE CONSTANTINE FACULTE DES SCIENCES DE L'INGENIEUR, 2005-2006.

[18] Yahyaoui, A., Abdellatif, T., Attia, R.: READ: reliable event and anomaly detection system in wireless sensor networks. In: 2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pp. 193–198. IEEE (2018).

## RESUME

Les réseaux de capteurs sans fil (RCSF) sont des réseaux constitués d'entités autonomes miniaturisées appelées nœuds capteurs pouvant communiquer entre eux via des liaisons radio. La sécurité est l'un des problèmes majeurs de ce type de réseaux. Pour cela, plusieurs travaux ont été proposés afin de résoudre ce genre de problème.

Dans ce projet, nous avons conçu et réalisé un système de détection d'intrusion dans les réseaux de capteurs sans fil à base de signatures. Nos résultats expérimentaux sont basés sur l'utilisation du système d'exploitation Contiki et le simulateur Cooja.
**Mots-clés** : Réseaux de capteurs sans fil, système de détection d'intrusion, Contiki, Cooja.

## ABSTRACT

Wireless sensor networks (WSN) are composed of autonomous miniaturized entities called sensor nodes, which can communicate with each other via radio links. The security is one of the major problems of this type of networks. Therefore, several studies have been proposed to solve this problem.

In this project, we designed and implemented a signature based intrusion detection system for wireless sensor networks. Our experimental results are based on the use of Contiki operating system and the Cooja simulator.
**Key-words:** Wireless sensor networks, intrusion detection system, Contiki, Cooja.

**ملخص**

شبكات الاستشعار اللاسلكية هي عبارة عن شبكات مكونة من وحدات مصغرة مستقلة تدعى المستشعرات، والتي تتواصل فيما بينها عن طريق الراديو. التأمين يعتبر مشكلا حساسا بالنسبة لهذا النوع من الشبكات. لذلك عدة دراسات اقترحت لحل هذا المشكل.

في هذا المشروع، قمنا بتصميم وانجاز نظام كشف الاختراقات يعتمد على الاشارات. استخدمنا نظام التشغيل Contiki وبرنامج المحاكاة Cooja من اجل الحصول على النتائج التجريبية لعملنا هذا.
**مفاتيح**

شبكات الاستشعار اللاسلكية، نظام كشف الاختراقات، Contiki، Cooja.