République Algérienne Démocratique & Populaire

Ministère de l'Enseignement Supérieur & de la Recherche Scientifique

Université Dr Moulay Tahar de Saida. Faculté de Technologie Département d'informatique

N° Attribué par la bibliothèque

Année Universitaire : 2019/2020

Implémentation d'un Système de détection d'intrusion dans un Réseau de Capteurs Sans Fil.

Mémoire présenté en vue de l'obtention du diplôme de Master Académique en Informatique : Sécurité d'information & cryptographie

***Présenté par** :*

Messatfa Salah Eddine
&
Ferketou Ahmed Zakaria

Encadré par :

Dr. Abdelkader Khobzaoui

Dédicaces

Ce modeste travail est dédié à tous mes enseignants, que Dieu les récompense, pour tous ce qu'ils ont fait pour moi. Merci mes enseignants. Vous m'avez accueillis au primaire, éveillé au collège, instruits au lycée et formé à la Fac. Je ne vous remercierai jamais assez. A présent, je comprends ce je vous dois. Vous avez donné de votre temps. Pour moi vos visages, resteront gravés dans ma mémoire pour toujours

Messatfa Salah Eddine

Dédicaces

Je dédie ce modeste travail

A mes parents, mes estimes pour eux sont immenses, je vous remercie pour tout ce que vous avez fait pour moi. Que dieu vous préserve une longue vie heureuse.

A tous mes amis. Je vous dédie ce travail et vous souhaite un avenir à la hauteur de vos ambitions. Que notre amitié dure

A Toute ma famille, Tous ceux que j'aime, qui m'aiment et me comblez de conseils

A tous ceux qui, un jour, ont pensé à moi

Les plus beaux mots ne sauraient exprimer ma redevance.

Ferketou Ahmed Zakaria

Remercîment

Nous remercions Dieu tout puissant de nous avoir permis de mener à terme ce projet qui est un point de départ d'une merveilleuse aventure, celle de la recherche, source de remise en cause permanente et de perfectionnement perpétuelle.

Nous tenons à exprimer toute notre reconnaissance et toute notre considération à Monsieur, AEK KHOBZAOUI pour avoir bien voulu nous encadrer, pour tout le temps qu'il nous a octroyé et pour tous les conseils qu'il nous a prodigués. Qu'il trouve ici l'expression de notre profonde gratitude.

Nous désirons, aussi, remercier les enseignants du département d'informatique de l'université Dr moulayTahar de Saïda. Qui nous ont fourni les outils nécessaires de réussite dans nos études universitaires.

Nous adressons nos honorables respects au président de jury, aux membres de jury et à tous ceux qui ont bien voulu accepter d'examiner et d'évaluer ce travail.

Messatfa Salah Eddine

Ferketou Ahmed Zakaria

Introduction

Les réseaux de capteurs sans fil (RCSF) ont suscité beaucoup d'intérêt depuis leur apparition en raison de leurs vastes applications dans plusieurs domaines militaires et civils. En effet cette technologie a connu un essor spectaculaire et s'est, largement, développé. Aujourd'hui, les RCSF sont utilisées dans la domotique, la surveillance, l'agriculture, la santé, et dans bien d'autres domaines.

Cette technologie a ouvert des perspectives pour l'amélioration de la qualité de vie de l'Homme. Elle représente beaucoup d'avantages, car elle permet de rester en interaction, permanente, avec l'environnement qui l'entoure.

Néanmoins, les RCSF sont soumis à plusieurs contraintes liées à leur limitation de ressources énergétiques, de stockage et de capacité calculatoire. A cela s'ajoute-les contraintes de la communication sans fils et leur déploiement dans des environnements hostiles. A côté des contraintes fortes en ressources se pose la question de la sécurité, dont la mise en place est une nécessité absolue. En effet, les RCSF sont vulnérables à différents types d'attaques visant la confidentialité et l'intégrité des données aussi bien que leur disponibilité. L'attaque peut consister, par exemple, à injecter, saturer ou endommager les équipements du réseau. Dans des applications critiques, de telles attaques peuvent être néfastes et peuvent engendrer des dégâts économiques et sécuritaires majeurs.

Le problème de la sécurité est un problème fondamental surtout pour les applications critiques tel que la surveillance militaire et nucléaire. Les ressources limitées des capteurs rend difficile l'implémentation des solutions classiques de sécurité. En général les techniques de sécurité appliquées aux RCSF sont catégorisées en deux classes. La première regroupe les techniques basées sur la prévention tel que la cryptographie et l'authentification et restent difficiles à implémenter dans les RCSF à cause de leur exigence en matière de ressources (Mémoire, stockage et puissance de calcul). La deuxième classe, quant à elle, regroupe les techniques de détection basées sur le comportement des capteurs formant le réseau pour détecter les attaques.

Plusieurs travaux de recherches ont été menés pour résoudre les problèmes de sécurité liés aux réseaux de capteurs sans fil, tels que : l'établissement de clés de paires entre capteurs, la sécurité de l'agrégation de données, l'authentification d'une source de diffusion, la sécurité du routage et de la localisation, ainsi que le contrôle d'accès au réseau de capteur sans fil. Dans le cadre de ce projet de fin d'études, nous nous intéressant aux systèmes de détection d'intrusion (IDS) pouvant être utilisés à fin de détecter les comportements malveillant dans les RCSF. Ces derniers analysent les paquets entrants et sortants dans le réseau afin d'identifier une signature malveillante.

Dans le premier chapitre de ce document, nous introduisant la notion de capteur sans fil. Nous tacherons de le définir, présenter ses caractéristiques et spécificités comme nous définissons qu'est qu'un réseau de capteurs sans fil et nous citerons quelques-unes de leurs domaines d'utilisation. Le deuxième chapitre quant à lui sera consacré à la problématique de la sécurité des RCSF où nous détaillons les différentes techniques de détection d'intrusion en se basant sur le cas des réseaux de capteurs sans fil.

Table des matières

Liste de figures

Liste des tables

Chapitre 1: Les réseaux de capteurs sans fil

I-*Introduction :*

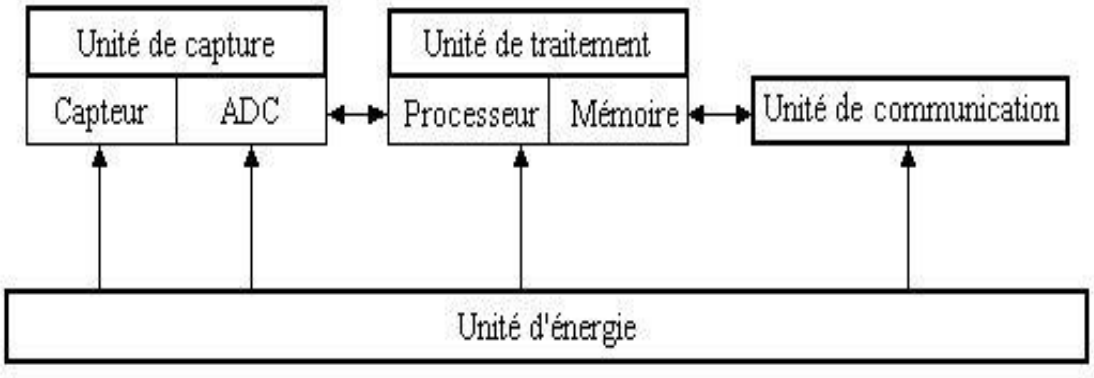
Les réseaux de capteurs sans fil constituent un cas particulier des réseaux sans infrastructure [1](réseaux ad hoc) comportant un très grand nombre de petits appareils, ou capteurs, déployés dans ou autour d'une zone géographique appelée champ de captage. La spécificité marquante de ses composants réside dans le fait qu'il possédant des ressources particulièrement limitées mais sont dotés d'une capacité d'auto-organisation, de coopération, de tolérance au panne et aux erreurs et un faible coût de déploiement. Les réseaux de capteurs sans fil représente une technologie embarquée et omniprésente qui trouve des applications dans divers secteurs. Parmi ces domaines d'application, on cite la surveillance et la préservation de l'environnement, la fabrication industrielle, la médecine, l'agriculture, la télématique et la logistique ainsi que l'exploration spatiale et bien d'autres secteurs. Initialement ses capteurs avaient un simple rôle de détecteurs de températures, fumée, d'intrusion. Aujourd'hui ils sont appelés à relever, d'analyser et de communiquer plusieurs données.

Le présent chapitre, sera consacré à présenter le fonctionnement d'un réseau de capteur sans fil.

I .1- *Capteur sans fil :*

Un capteur sans fil est défini comme étant un mini-composant qui permet l'acquisition des données, de les traiter et de les communiquer. Il est composé de plusieurs éléments ou modules correspondant chacun à une tâche particulière d'acquisition, de traitement et de transmission des données plus une source d'énergie comme le montre la figure 1-1.

.



- ***Figure 1. 1- Composants d'un nœud capteur***

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

- ***Unité de traitement*** *: l'unité de traitement est composée de deux interfaces, une interface pour l'unité d'acquisition et une interface pour l'unité de transmission. Cette unité est également composée d'un processeur et d'un système d'exploitation spécifique. Elle acquiert les informations en provenance de l'unité d'acquisition et les envoie à l'unité de transmission.*
- ***Unité de transmission*** *: l'unité de transmission est responsable de toutes les émissions et réceptions de données via un support de communication radio.*

Ces trois unités sont alimentées par une source d'énergie qui est responsable de répartir l'énergie disponible aux autres modules et de réduire les dépenses en mettant en veille les composants inactifs par exemple. Cette unité se trouve généralement sous la forme de batteries standards de basse tension. Souvent, une pile AA normale d'environ 2.2-2.5 Ah fonctionnant à 1.5 V.

D'autres composants peuvent être utilisé dans certains capteurs selon les applications dans lesquelles ils sont utilisés comme « des mobilisateur »pour qu'ils puissent se déplacer ou bien de GPS (Global Position System) pour permettre de déterminer leur position géographique [1]. Les Figure 1.2 présente quelques exemples de capteurs sans fil. Globalement, les capteurs sont conçus selon l'application pour laquelle ils sont utilisés cela nous donne une grande variété de capteurs.

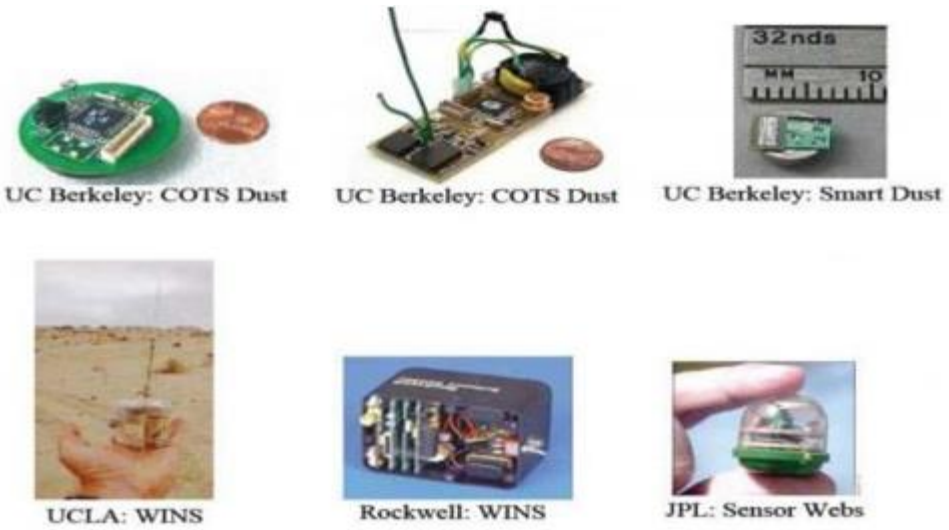


Figure 1.2: Exemples de capteurs

I .2- Technologies des capteurs :

Il est à noter que le fait que les capteurs sans fil sont issus des projets militaires entrave une mise en place d'une chronologie précise de leur développement. Néanmoins, la littérature spécialisée indique que le premier prototype de capteurs sans fil identifiable correspond sans aucun doute au module LWIM (low-power Wireless IntegratedMicrosensors)[2] développé par l'agence pour les projets de recherche avancée de défense des états unis communément connue sous l'acronyme DARPA. Ce premier protocole était, géophone doté d'un capteur de transmission radio fréquences et d'un contrôleur PIC. Depuis la technologie des capteurs sans fil ont beaucoup évoluée et les capteurs sont devenus de plus en plus miniatures et leurs durées de vie ne cessent d'augmenter. Crossbow est le fournisseur le plus connu avec son Mica2 et MicaZ présentés dans la figure 1.3.

Figure 1.3 – Modèles de capteurs sans file

Les capteurs MICA développés par l'université de Berkeley et commercialisés par CrossBow et les capteurs TinYOde développés pour des applications liées à l'industie par la compagnie Shockfish se comptent, eux aussi, parmi les plus connus. Bien que différents, ces modèles on,t en commun, les mêmes composant de base. Ils se présentent sous forme de cartes intégrées regroupant l'unité de communication et l'unité de traitement, tandis que l'unité de captage est conçue comme une carte distincte qui peut être attachée sur l'unité principale cela permet leurs la réutilisation pour différents applications. On distingue, globalement quatre principaux types de plateformes :

- *Plateforme de capteurs miniaturisés : cette plateforme est dédiée aux capteurs de tailles très réduite (quelques mm^3) et faible bande passante (<50Knps). Spec, conçue par l'université de berkely, dont la taille est d'environs 2mm sur 2.5 mm est la plateforme la plus connue de ce genre.*
- *Plateforme des capteurs généraux : développée à fin de capter et router des informations de monde anbiant. Quelques plateformes de cette famille ont été développées à la base de MiCAZ.*
- *Plateforme de capteurs à haute bande passante : ayant pour but de transporter de gros volumes de données (vidéo, son de vibration). Imote en est un exemple typique de cette famille.*

- *Plateforme de passerelles : les dispositifs de cette famille servent à transporter les informations envoyées par le réseau de capteurs vers un réseau traditionnel dont le Stargate et un exemple typique.*

Le tableau 1.1 résume les caractéristiques de quelque capteur.

Fabricant	Modèle	Processeur/ Microcontrôleur	Radio	RAM	Flash	Batterie
Crossbow	MICA2	Atmega 128L MPR400 (8-bit), 16 Mhz	433/915 Mhz	4 KB	128 KB	2xAA
	MICAz	Atmega 128L MPR2400 (8-bit), 16 Mhz	2.4 GHz, 802.15.4 Couche base de ZigBee	4 KB	128 KB	2xAA
	TelosB	TI MSP 430 (16-bit), 8/16 Mhz	2.4 GHz, 802.15.4	10 KB	48 KB	2xAA
	Imote2	Intel PXA271 (32-bit) , 13 Mhz	2.4 GHz IEEE 802.15.4/ ZigBee Compliant	32 MB	32 MB	3xAA
Shockfish S A	TinyNode	TI MSP430 (16-bit), 16Mhz	868 / 915MHz	10 KB	512 KB	2/3xAA
Berkeley	Dot-mote	Atmel AVR 8535 (8-bit), 4MHz	868-916 Mhz	0.5KB	8KB	3v, 10-20 mA
Sun	Sun Spot	ARM920T core (32 bit), 180 MHz	2.4 GHz IEEE 802.15.4	512KB	4MB	3.7V, 750 mAh

***Tableau 1.1** Caractéristiques de capteurs existants actuellement*

I.3 - Les réseaux de capteurs sans fil :

Un réseau de capteur sans fil est constitué d'un nombre plus ou moins grand de nœuds capteurs(figure 1.4)

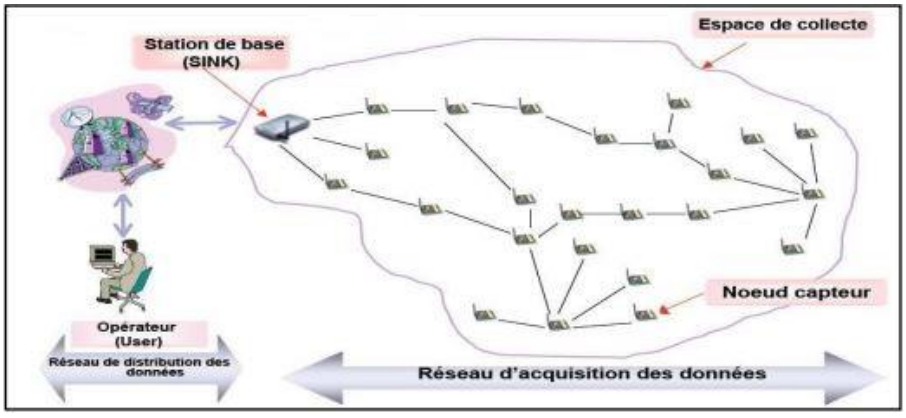


Figure 1.4- Réseau de capteur sans fil

Ces nœuds sont autonomes, distribués dans l'espace qui coopèrent pour surveiller des conditions environnementales ou physiques, tels que la température, le bruit, la vibration, la

pression, le mouvement, etc. A l'origine, le développement des réseaux de capteur sans fil a été motivé par des applications militaires telles que la surveillance de champ de bataille. Cependant, ce type de réseau est maintenant employé dans plusieurs domaines d'applications civiles, comme la surveillance d'environnement, d'habitat, la surveillance médicale, l'automatisation des maisons, le contrôle du trafic [5]. L'architecture des réseaux de capteurs sans fil utilise beaucoup de sources. Historiquement, beaucoup de travaux ont été effectués dans le contexte des réseaux à auto-organisation, mobiles et Ad Hoc. Un réseau de capteurs est constitué essentiellement de plusieurs nœuds capteurs, un nœud sink (ou station de base) et un centre de traitement des données.

- ***Les nœuds*** *sont des capteurs dont le type, l'architecture et leur disposition géographique dépendent de l'exigence de l'application en question. Leur énergie est souvent limitée puisqu'ils sont alimentés par des piles.*

- ***Le sink*** *est un nœud particulier du réseau: Il est chargé de la collecte des données issues des différents nœuds du réseau. Il doit être toujours actif puisque l'arrivée des informations est aléatoire. C'est pourquoi son énergie doit être illimitée. Dans un réseau de capteur sans fil plus ou moins large et à charge un peu élevée, on peut trouver deux sinks ou plus pour alléger la charge.*

- ***Centre de traitement des données:*** *c'est le centre vers lequel les données collectées par le sink sont envoyées. Ce centre a le rôle de regrouper les données issues des nœuds et les traiter de façon à en extraire l'information utile exploitable. Le centre de traitement peut être éloigné du sink [1], alors les données doivent être transférées à travers un autre réseau, c'est pourquoi on introduit une passerelle entre le sink et le réseau de transfert pour adapter le type de données au type du canae.*

A un niveau plus élevé un RCSF peut être vu comme étant une combinaison de deux entités de réseau :

- ***Le réseau d'acquisition des données:*** *c'est l'union des nœuds capteurs et du sink. Son rôle consiste à collecter les données à partir de l'environnement et de les rassembler au sink.*

- ***Le réseau de distribution des données:*** *son rôle est de connecter le réseau d'acquisition des données à un utilisateur.*

I .4 -Topologies d'un réseau de capteurs sans fil :

De façon générale, les architectures des réseaux de capteurs se présentent sous forme de deux topologies comme le montre la figure 1.5.:

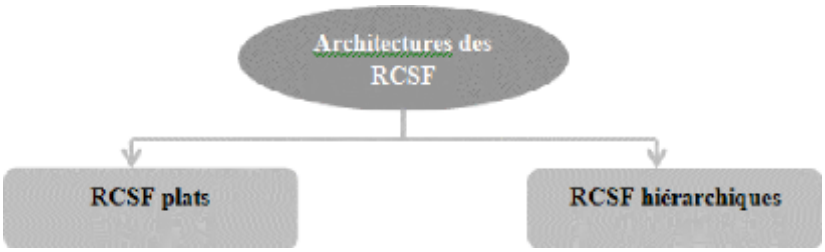


Figure 1.5 Les types d'architecture des RCSF

I .4.1- Les réseaux de capteurs sans fil plats :

Un réseau de capteurs sans fil plat[1](figure 1.6) est un réseau homogène, où tous les nœud sont le même niveau de responsabilité et disposent des mêmes capacités et fonctionnalités concernant le captage, la communication et la complexité du matériel, seul le sink échappe à cette règle puisqu'il joue le rôle d'une passerelle chargée de la collecte des données issues des différents nœuds capteurs pour les transmettre à l'utilisateur.

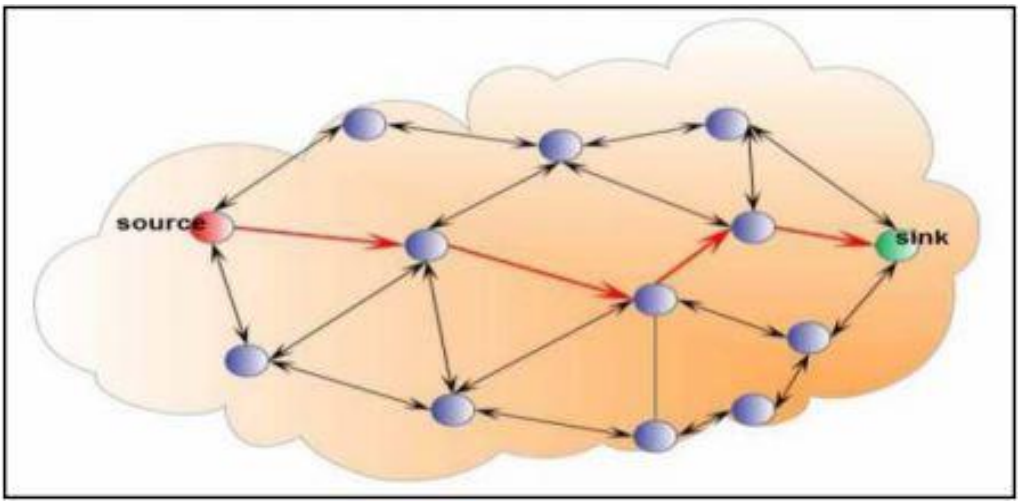


Figure 1.6- Topologie Plate

I .4.2 - Les réseaux de capteurs sans fil hiérarchiques :

Un réseau de capteurs hiérarchique (Figure 1.7) est un réseau hétérogène où les nœuds ont des capacités différentes, par exemple certains nœuds peuvent disposer d'une source d'énergie plus importante, une plus longue portée de communication et/ou une plus grande puissance de calcul. Ceci permet de décharger la majorité des nœuds simples à faible coût de plusieurs fonctions du réseau.

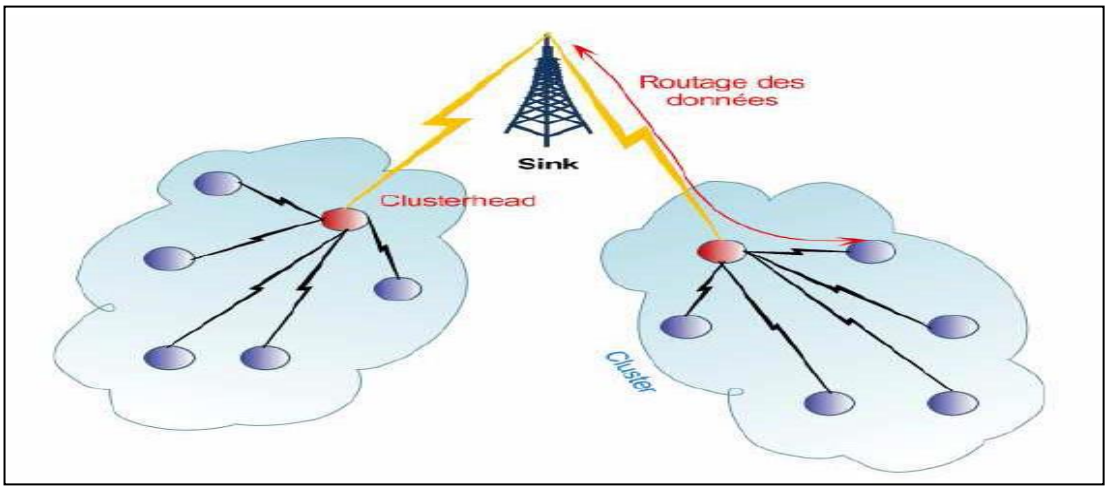


Figure 1.7 -Topologie hiérarchique

I .5 -Architecture protocolaire

Une pile protocolaire de cinq couches est utilisée par les nœuds du réseau : la couche application, la couche transport, la couche réseau, la couche liaison de données et la couche physique.De plus, cette pile possède trois plans (niveaux) de gestion : le plan de gestion des tâches, le plan de gestion de la mobilité et le plan de gestion de l'énergie.

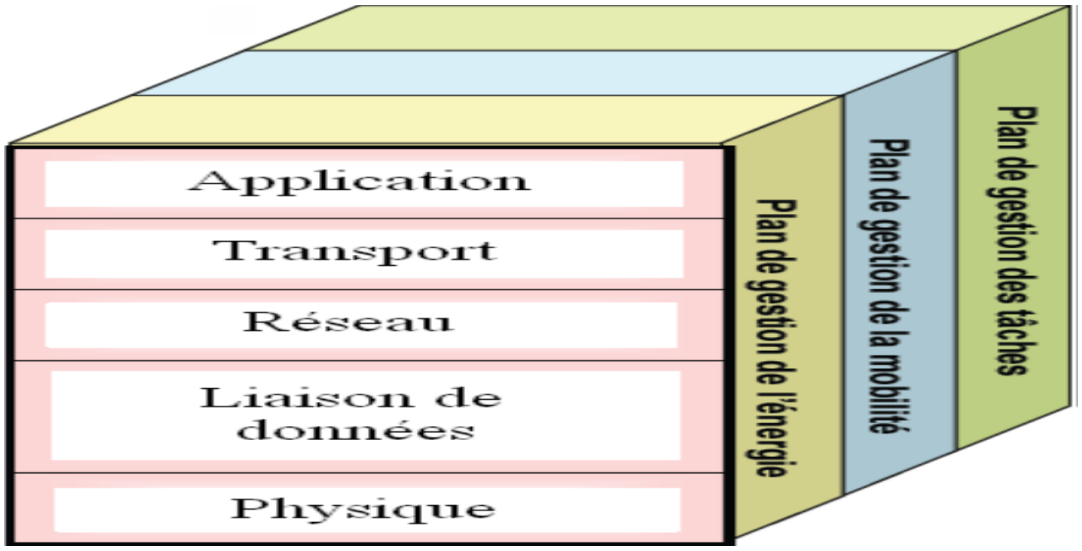


Figure 1.8 La pile protocolaire dans les réseaux des capteurs sans fil.

La couche application

La couche application constitue l'ensemble des applications implémentées sur un RCSF, ces applications devraient fournir des mécanismes permettant à l'utilisateur d'interagir avec le réseau de capteur à travers les différentes interfaces, et éventuellement par intermédiaire d'un réseau étendu (exemple internet).

Cette couche est responsable par exemple sur la collecte, le codage, l'agrégation et la compression des données collectées.

La couche transport :

Dans les réseaux de capture, cette couche est essentiellement présente pour constitue une interface entre la couche application et la couche réseau. Ses principaux objectifs sont :

- *Multiplexer et démultiplexer les messages entre les applications et la couche réseau.*
- *Contrôler les donnes a haut niveau.*
- *Réguler la quantité des donnes injectées dans le réseau.*

La couche réseau :

Elle s'occupe du routage de données fournies par la couche transport. Elle établit les routes entre les nœuds capteurs et le nœud puits et sélectionne le meilleur chemin en termes d'énergie, délai de transmission, débit, etc.

Les protocoles de routage conçus pour les RCSF sont différents de ceux conçus pour

Les réseaux Ad Hoc puisque les RCSF sont différents selon plusieurs critères comme :

- *l'absence d'adressage fixe des nœuds tout en utilisant un adressage basé-attribut.*
- *l'établissement des communications multi-sauts.*
- *l'établissement des routes liant plusieurs sources en une seule destination pour agréger des données similaires, etc.*

Parmi ces protocoles, nous citons : LEACH (Low-Energy Adaptive Clustering Hierarchy)

Et SAR (Sequential Assignement Routing).

La couche liaison de données :

Elle est responsable de l'accès au media physique et la détection et la correction d'erreurs intervenues sur la couche physique. De plus, elle établitune communication saut-par-saut entre les nœuds. C'est-à-dire, elle détermine les liens de communication entre eux dans une distance d'un seul saut.

La couche physique

Elle permet de moduler les données et les acheminer dans le media physique tout en choisissant les bonnes fréquences.

- ***Plan de gestion d'énergie*** *:Contrôle l'utilisation de la batterie. Par exemple, après la réception d'un message, le capteur éteint son récepteur afin d'éviter la duplication des messages déjà reçus. En outre, si le niveau d'énergie devient bas, le nœud diffuse à ses voisins une alerte les informant qu'il ne peut pas participer au routage. L'énergie restante est réservée au captage*
- ***Plan de gestion de mobilité :****Détecte et enregistre le mouvement du nœud capteur. Ainsi, un retour arrière vers l'utilisateur est toujours maintenu et le nœud peut garder trace de ses nœuds voisins. En déterminant leurs voisins, les nœuds capteurs peuvent balancer l'utilisation de leur énergie et la réalisation de tâche.*
- ***Plan de gestion de tâche****:Balance et ordonnance les différentes tâches de captage de données dans une région spécifique. Il n'est pas nécessaire que tous les nœuds de cette région effectuent la tâche de captage au même temps ; certains nœuds exécutent cette tâche plus que d'autres selon leur niveau de batterie.*

I .6- *Contraintes influençant les* réseaux de capteurs sans fil :

La création des protocoles adaptés aux réseaux de capteurs sans fil ou bien contribuant à leur développement reste une problématique difficile pour les raisons suivantes [7]:

- ***Capacité limitée :*** *Non seulement les ressources de calcul et de mémoire des nœuds sont relativement faibles, mais en plus, ils opèrent avec des piles ce qui rend leur durée de vie limitée, un protocole efficace et réaliste doit minimiser au maximum l'overhead de communication et de stockage pour ne pas pénaliser le réseau.*

- ***Agrégation de données :*** *Il a été démontré dans plusieurs publications scientifiques que le fait d'agréger les données avant de les envoyées à une station de base va permettre de diminuer le nombre de messages envoyés, de réduire les puissances d'émission et ainsi économiser de l'énergie.*

- ***Echelle de dynamicité :*** *Les réseaux de capteurs contiennent souvent un nombre de nœuds très important. Ces réseaux sont souvent peu stables et très dynamiques: les capteurs, qui ont épuisés leur pile, disparaissent et de nouveaux nœuds doivent être déployés pour assurer une certaine connectivité.*

- ***Protection physique faible :*** *Les capteurs sont souvent déployés dans des environnements non-protégés (montagnes, forets, champs de bataille,...). Par conséquent, ils peuvent facilement être interceptés et corrompus. De plus, à cause de leur faible cout, ils utilisent rarement des composants électroniques anti-corruption (tamper-resistantdevices).*

I.7- Principaux facteurs de conception :

La conception et la réalisation des réseaux de capteurs sans fil sont influencées par plusieurs paramètres, les plus importants sont présentés comme suit :

- ***Durée de vie*** *: C'est la caractéristique la plus fondamentale d'un réseau de capteurs. Elle dépend du type d'application et donc de la durée et de l'échantillonnage des mesures. Les contraintes liées au changement (ou rechargement) des batteries sont dépendantes des déploiements et du coût de maintenance des nœuds. Il est donc essentiel d'avoir une durée de vie du réseau la plus longue possible.*

- ***Etendu du réseau*** *: La plupart des réseaux de capteurs sont composés de quelques dizaines de nœuds, mais certaines applications peuvent exiger l'utilisation de réseaux de capteurs composés de centaines ou de milliers de nœuds. La zone que doit couvrir le réseau est également important dans son dimensionnement.*

- ***Faible coût*** *: Les réseaux de capteurs peuvent contenir un nombre important de nœuds. Il est donc nécessaire d'avoir un coût unitaire par nœud le plus faible possible, pour obtenir un coût raisonnable du réseau global.*

- ***Scalabilité*** *: Dans le cas d'un nœud endommagé, le réseau doit être capable de prendre en considération cette modification tout en assurant une qualité de service égale. La redondance des capteurs peut être un moyen d'assurer cette fonction. La notion de scalabilité est alors utilisée pour dire que l'architecture et les protocoles de communications du réseau doivent s'adapter et prendre en compte l'ajout ou la perte de nœuds dans le réseau. Les exigences énumérées ci-dessus conduisent à ce qu'un réseau de capteurs doit présenter les caractéristiques suivantes :*

- ***Faible consommation*** *: La durée de vie la plus longue possible traduit l'exigence la plus importante de la plupart des applications. Par conséquent, pour atteindre cette autonomie, il est crucial de minimiser la consommation moyenne des capteurs. Une des alternatives explorées aujourd'hui par les chercheurs consiste à extraire l'énergie de l'environnement (énergie solaire, vibrations mécaniques, bruit acoustique…). Ces techniques peuvent grandement améliorer la durée de vie, mais comme la production d'énergie est très faible, une consommation d'énergie réduite des capteurs reste de la plus haute importance.*

- ***Faible complexité matérielle et logicielle*** *: Les fonctionnalités mises en œuvre par la partie matérielle se doivent d'être aussi simples que possible, car l'augmentation de la complexité de cette dernière peut conduire à une augmentation de la consommation d'énergie. La complexité de la partie logicielle doit également être faible sous peine d'augmenter les consommations liées aux accès mémoire.*

- ***Auto-configuration*** *: Un réseau de capteurs doit pouvoir configurer tous ses paramètres indépendamment de son environnement d'installation. Selon le nombre de nœuds, et selon leur déploiement, une configuration manuelle n'est pas du tout envisageable. Le réseau doit par exemple être capable d'identifier les positions des nœuds, ce qui lui permettra d'identifier et de tolérer d'éventuelles pannes (problème de batterie) ou bien encore d'intégrer de nouveaux nœuds.*

I.8- *Système d'exploitation :*

Les systèmes d'exploitation représentent un socle sur lequel s'appuient les programmes d'application. Ils servent de lien ou d'interface entre l'architecture matérielle et la partie logicielle. Dans les réseaux de capteurs sans fil, les systèmes d'exploitation conservent ce rôle. Mais, au regard des contraintes des RCSF, ils possèdent différentes fonctionnalités et en nombre plus restreint en comparaison d'un système d'exploitation classique. La gestion des utilisateurs fait partie des fonctionnalités mises de côté.

Pour répondre aux contraintes de ressources des RCSF, certaines parties voire l'ensemble du système d'exploitation peuvent être organisées différemment d'une structure classique en couches superposées comme illustrer dans la figure 1.9.

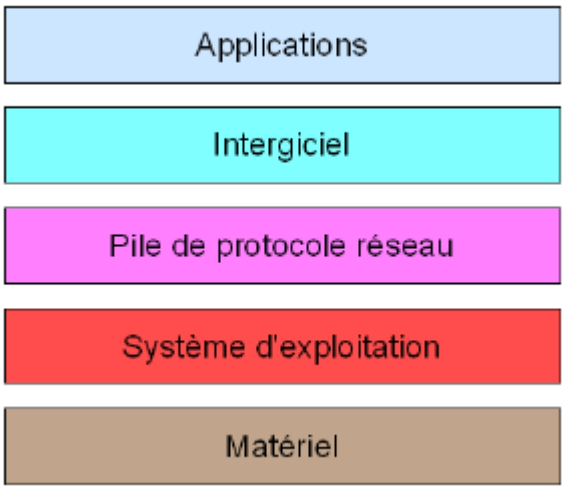


Figure 1.9- Architecture par couches superposées d'un système d'exploitation pour RCSF

Les systèmes d'exploitation des réseaux de capteurs sans fil sont caractérisés, principalement, par leur petite taille à cause des limitations en ressources physique, mais avec plus de performances en temps d'exécution, en occupation de mémoire et en gestion d'énergie. Parmi les systèmes d'exploitation destinés aux réseaux de capteurs sans fil on cite :

- ***TinyOs*** *qui est un système open source conçu par l'université de Berkeley. Il est entièrement réalisé en NesC, langage orienté composant syntaxiquement proche du C et se caractérise par :*
  - ***1-*** *Une architecture basée composant.*
  - ***2-*** *Un modèle de programmation basé événement*
  - ***3-*** *Un modèle de concurrence basé sur des événements et des tâches.*
  - ***4-*** *Sa bibliothèque de composants est particulièrement complète puisqu'elle contient des protocoles réseaux, des pilotes de capteurs et des outils d'acquisition de données. Un programme s'exécutant sur TinyOs est constitué d'une sélection de composants systèmes et de composants développés spécifiquement pour l'application à laquelle il sera destiné (mesure de température, du taux d'humidité…)*

- ***Contiki*** *qui est un système configurable modulaire organisé en modules, une architecture plate. Un cœur non-reconfigurable permet de télécharger les modules applications ou sous-systèmes, qui constituent alors l'unité de reconfiguration dans Contiki. Un modèle d'exécution événementiel permet une implémentation efficace d'un état stable pour les modules. Il conçu pour prendre le moins de place possible, avec une faible empreinte mémoire. Pour cela, le code est écrit en C. Ainsi, le système complet est supposé pouvoir tourner sans problèmes avec 2 ko de RAM et 40 ko de ROM. Comme il possède une gestion de la programmation parallèle sous forme de « proto-threads », qui sont des processus légers développés spécialement pour l'occasion de même que µIPv6 permet d'être compatible IPV652,55.*

- ***Mantis*** *est un système d'exploitation multithreads développé en C et dispose d'un environnement de développement Linux et Windows. Il peut être déployé sur de nombreuses plateformes, tels que MICA2, MICAz, et TELOS. Son empreinte mémoire est faible : 500 octets en RAM et 14 ko en flash59. Il a été conçu par l'université du Colorado, en 2005, avec comme objectif d'offrir un système d'exploitation multi threading. C'est un système modulaire dont le noyau supporte également les entrées/sorties synchrones, et un ensemble de primitives de concurrence. L'économie d'énergie est réalisée par Mantis par une fonction de veille (sleepfunction) qui inactive le capteur lorsque tous les threads actifs sont terminés. Mantis est un système dynamique, les modifications applicatives peuvent être réalisées en fonctionnement. Mantis apporte une compatibilité avec le modèle événementiel TinyOS à travers TinyMOS (MOS est la contraction de MantisOS), dont son noyau est équipé. Comme la plupart des systèmes d'exploitation pour capteurs, Mantis dispose d'une pile réseau, regroupée dans la couche COMM*[6]*. La communication est basée sur le principe de messages pondérés Active Message (AM).*

Le tableau 1.2 résume les défis qu'on rencontre dans la conception et le déploiement d'un système de réseau de capteurs et les solutions proposées.

Défis d'un système de réseau de capteur	Solutions envisageables
Énergie du capteur constitue une ressource limitée pour la transmission des données	-Utiliser un réseau de capteurs qui se déploie, de faible puissance, à court transmissions. -utilisation des réseaux de capteur multi hop. -Filtrer les données sur place et de transmettre uniquement des données filtrées
La distribution des événements Spatio-temporel dynamique et non déterministe. Peut ne pas être en mesure avant de déterminer comment déployer de façon optimale les capteurs individuels.	-Utiliser un réseau de capteurs pour augmenter la densité de capteur autour des positions estimées de la source du signal quand déterministe; Distributions de capteur de conception pour être reconfigurable, auto-organisation, d'être mobile Soutenez échantillonnage variable et charge les données en rafales collection
Défaillance du capteur est commune en raison d'un manque de puissance, dommage physique, actif (blocage) ou passive environnemental interférence de l'émetteur-récepteur,	Utiliser les réseaux de capteurs denses de faible puissance avec des chemins redondants pour acheminer les données à travers le réseau
Réseaux de capteurs multi-hop peuvent avoir une dynamique topologie. Aucune connaissance globale sur la structure de réseau.	Utiliser des protocoles de routage spécialisé pour travailler sur topologies dynamiques
Les capteurs peuvent être trop coûteux de mettre à jour une fois déployé	conception des capteurs et le nœud de capteur d'accès avec faible maintenance. soutien des capteurs de redondance
Les capteurs peuvent générer d'énormes quantités de données	Utilisation du traitement de données à la fois dans le capteur et le nœud de capteur d'accès

Tableau 1.2 - Les défis d' un système réseaux de capteur.

I.9- *Applications des réseaux de capteurs :*

L'utilisation des capteurs est depuis longtemps une réalité au sein de multiples domaines tel le contrôle d'intrusion, le calcul de température, le calcul de changement climatique, la surveillance des déplacements d'animaux (avec récepteurs GPS), surveillance de malades,…

Les militaires ont été les précurseurs dans le domaine de la recherche sur les réseaux de capteurs. Dans un contexte militaire, un réseau de capteurs offre des avantages très précieux, a s'avoir le contrôle des équipements et munitions, la communication à bas coût entre les unités avec une logistique peu compliquée, reconnaissance et surveillance d'un champ de bataille ainsi qu'une estimation très rapide et évolutive des dégâts encourus en temps de crise.

Une très forte utilisation des capteurs sans fil a été, aussi, enregistrée dans le domaine médical où les capteurs sans fil ont été déployés dans le cadre de vie de la personne surveillée dans le but de surveiller à distance et de manière permanente ses constantes vitales.

Dans le domaine industriel, les réseaux de capteurs sans fil offrent une grande flexibilité d'emploi puisqu'ils permettent de s'affranchir des contraintes liées aux câblages. Il est alors possible de satisfaire des contraintes de poids, de mobilité, de facilité de déploiement,… etc Parmi les applications des réseaux de capteurs sans fil dans le milieu industriel, nous citons la surveillance de l'état de santé d'un ouvrier ou du risque de le voir exposé à des conditions de travail dangereuses (exposition à la radioactivité), la gestion des stocks, contrôle des machines à distances,… etc. Dans le domaine commercial, les capteurs sans fil servent à améliorer les processus de stockage, de livraison, pour connaitre la position, l'état et la direction d'un produit.

Dans le cadre de la protection environnementale, les capteurs sans fil sont utilisés, par exemple, pour la détection d'incendies dans des grandes zones forestières, la détection de la pollution, l'analyse de la qualité de l'air, surveiller d'éventuels tsunami, inondations, volcan,… Comme ils sont utilisés dans le cadre de suivi d'écosystèmes comme la surveillance d'oiseaux, croissance des plantes, …

I.10- *Conclusion :*

Les réseaux de capteurs sans fil constituent une considérable avancé dans l'évolution des technologies de l'information et de la communication et ont suscité un grand intérêt vu leur facilité déploiement et de leur faible coût.

Dans ce chapitre, nous avons défini et décrit, bien que brièvement, ce qu'est un capteur sans fil, sons architecture et ses caractéristiques. Comme nous avons introduit la notion de réseau de capteurs sans fil qui est un type particulier de réseau Ad-hoc. Et en fin, nous avons jeté un bref aperçu sur quelques domaines d'application de ses réseaux. Le chapitre suivant sera consacré à la problématique de la sécurité des réseaux de capteur sans fil.

Chapitre 2 : La sécurité dans les réseaux de capteurs sans fil

II–*Introduction :*

Comme pour les réseaux d'ordinateurs classique, les aspects liés à la sécurité avaient été peu ou pas abordés dans les premiers travaux de recherche portant sur les réseaux de capteurs sans fil. La faute n'était pas à la motivation des chercheurs mais aux ressources disponibles au sein des capteurs. Pour mettre en place une application de réseau de capteurs, il faut résoudre essentiellement les problématiques de routage, de gestion de données. La sécurité vient ensuite et s'appuie sur les ressources restantes. La conception de ces applications suppose que tous les nœuds engagés sont coopératifs et dignes de confiance. Cependant, ceci n'est pas le cas dans le monde réel, où les nœuds sont exposés à différentes types d'attaques qui peuvent carrément endommagé le bon fonctionnement du réseau. Ces attaques exploitent essentiellement l'incertitude du canal de communication et le déploiement aléatoire des nœuds capteurs dans des zones difficiles à surveiller. Comme les autres réseaux sans fil, les réseaux de capteurs sont susceptibles d'attaques passives et actives. Les attaques passives se contentent de voler les données tandis que les actives provoquent la répétition, la modification et la suppression des données comme elles peuvent causer la congestion et la distribution d'information de routage incorrecte.

Garantir la sécurité de ce type de réseau est une tâche difficile vu que les nœuds ont des ressources très limitées. En général, les solutions pour sécuriser les RCSF se catégorisent en deux catégories. La première englobe les techniques basées sur la prévention telle que la cryptographie et l'authentification. Cette catégorie de solutions est difficile à implémenter à cause les limitations en ressources des capteurs. La deuxième catégorie, quant à elle, regroupe les techniques de détection d'attaques basées sur le comportement des nœuds du réseau. Dans ce contexte, on compte quelques techniques et protocoles de détection d'intrusion. La plus part de ces techniques sont étroitement liées aux protocoles de routage.

Dans ce chapitre, nous présenterons les contraintes et les exigences de sécurité dans les RCSF[3], ensuite nous abordons la détection d'intrusion dans ce type de réseaux.

II.1-Les Exigences de sécurité :

Sous sa forme la plus simple, la sécurité consiste à s'assurer que des fouineurs ne peuvent ni lire ou dans le pire des cas, ni modifier des informations ou messages destinés à d'autres et à interdire à des personnes non autorisées d'accéder à des services : ou plus clairement, elle peut être définie comme étant l'ensemble de méthodes techniques et outils chargés de protéger les ressources d'un système informatique afin d'assurer, principalement les services suivant :

- ***La confidentialité*** *est première préoccupation des militaires, semble être la qualité la plus importante d'un système sûr. Elle consiste à s'assurer que l'information privée ou confidentielle ne soit pas interceptée, visualisée ou copié par des utilisateurs non autorisés. Un autre aspect de la confidentialité est la protection du flot de trafic contre l'analyse. Cela requiert qu'un attaquant ne puisse observer ou relever, sur un équipement de communication, les caractéristiques d'un trafic, tel que: les sources et destinations, les fréquences, longueurs ou autres.*

- ***L'authentification*** *est le mécanisme permettant de certifier qu'un sujet (utilisateur ou un programme s'exécutant pour le compte d'un utilisateur) est bien ce qu'il prétend être. Ce mécanisme est essentiel pour permettre la définition des droits d'accès des différents sujets et leur mise en œuvre. Typiquement, l'authentification des utilisateurs est effectuée au cours du processus d'ouverture de session quand un utilisateur envoie les informations sur son identité (généralement un nom d'utilisateur et un mot de passe).*

- ***L'intégrité****, dite aussi l'authentification de données, évite la corruption, l'altération et la destruction des données dans le réseau de manière non autorisée. La corruption de l'intégrité des données peut avoir plusieurs sources :*
  - *Les bogues logiciels ou actions malveillantes de la part des utilisateurs.*
  - *L'infection virale du système informatique, les chevaux de Troie.*
  - *Les panes matérielles causées par l'usure, des accidents ou catastrophes naturelles*
  - *Les erreurs de saisie, de stockage ou de transmission réseau.*

Afin de minimiser ces menaces d'intégrité, les procédures suivantes doivent être Implémentées :

- *La sauvegarde régulière des données importantes dans des endroits sûrs.*
- *L'utilisation des listes d'accès pour contrôler les autorisations d'accès aux données.*
- *Maintenance curative et préventive du matériel.*
- *L'utilisation des signatures numériques pour s'assurer que les données n'ont pas étaient altérées pendant leur transmission et stockage.*
- *L'ajout de code dans les applications pour valider leurs entrées.*

- ***La disponibilité*** *des systèmes et des données dans le cadre de l'usage prévu est une exigence destinée à assurer que le système fonctionne correctement et que le service n'est pas refusé aux utilisateurs autorisés. Elle consiste à protéger le*

Réseau contre les attaques intentionnelles ou accidentelles, tel que l'effacement non autorisé de données ou tout autre déni de service ou d'accès aux données d'une part et d'empêcher l'utilisation du système ou des données à des fins non autorisées.

- ***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*

II.2- *Contraintes de sécurité dans les réseaux sans fil :*

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 :

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

- **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.*

- **Fonctionnement sans surveillance :** *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.*

II.3-Attaques contre les réseaux de capteurs sans fil *:*

Une attaque peut être définie comme une tentative d'accès non autorisé à un service ou une ressource ou une information ou bien la tentative de compromettre l'intégrité, la disponibilité ou la confidentialité du réseau. On trouve plusieurs catégorisations des attaques visant les réseaux de capteurs sans fil selon des critères spécifiques. Par exemple selon l'appartenance de l'attaquant ou non au réseau, les attaques contre les réseaux de capteurs peuvent être soit externes ou internes. Une attaque externe se produit de l'extérieur du réseau de capteurs .C.-à-d. elles lancées 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. Mais si on considère la puissance de l'attaquant et l'effet causé par l'intrusion on peut les classé en attaques passives et actives. 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)[3] peuvent ensuite aider l'attaquant à de réaliser des attaques malveillantes.

Les réseaux de capteurs sans fil sont vulnérables à de nombreuses attaques et menaces qu'on doit nécessairement connaître pour comprendre comment l'attaquant agit et donc savoir comment lui faire face protéger. Les principales attaques contre les RCSF sont :

- II.3.1**Déni de Service (DoS) :** *Le but de ce type d'attaque est de rendre le réseau dysfonctionnel. L'attaque Déni de Service (DoS) consiste à rendre les différentes ressources indisponibles. Dans ce type d'attaques, l'entité malveillante peut bloquer le canal après la transmission des messages falsifiés et donc, interrompre la connexion réseau. L'attaque Déni de service peut être générée en diffusant à plusieurs reprises des faux messages avec des signatures non valides pour consommer la bande passante ou d'autres ressources du nœud* ciblé.

- II.3.2 **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 noeud 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 nécessite 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).

- II.3.3 **Selective Forwarding :** *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.*

- II.3.4 **Black Hole (Trou noir) :** *cette attaque est due à un nœud malveillant qui prétend avoir une route optimale pour la destination et qui indique que le paquet devrait être acheminé par lui en transmettant de fausses informations de routage. L'impact de cette attaque est que le nœud malveillant peut soit détruire ou utiliser improprement les paquets* interceptés sans les transmettre.

- II.3.5 **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*

- II.3.6 **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.*

- II.3.7 **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*.

- II.3.8 **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.*

- II.3.9 **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.*

- II.3.10 **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.

- II.3.11 **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.*

II.4- *Détection d'intrusion dans les réseaux sans fil :*

Nous appelons ***intrusion*** *toute violation de la sécurité logique d'un système informatique. Ces tentatives de subversion s'appuient sur divers types de faiblesses(Fig.2.1) pouvant être classifiées en quatre* ***catégories*** *:*

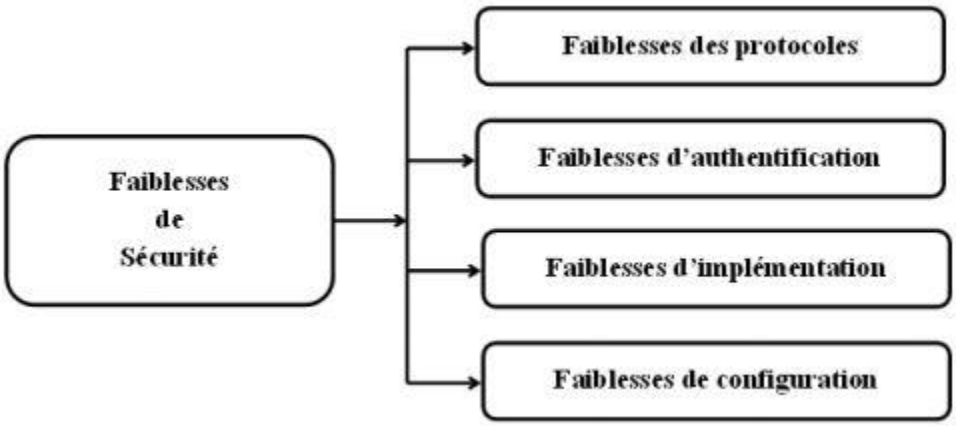


Figure 2.1 : Typologie des faiblesses de sécurité

- ***Faiblesses des protocoles*** *: Les protocoles réseau n'ont pas été, initialement, conçus pour tenir compte des problèmes de sécurité. Ni le protocole IP ni SNMP, par exemples, ne comportent de couche sécurité et s'expose à diverses attaques, tel que les attaques par fragmentation, déni de service,... D'autres formes d'attaques exploitent des bogues ou de mauvaises implémentations des piles TCP/IP dans les systèmes réseau.*
- ***Faiblesses d'authentification*** *: Les protocoles réseau n'ont prévu aucun mécanisme d'authentification véritable et subissent des attaques qui s'appuient sur ces faiblesses d'authentification comme les attaques de type spoofing. Généralement, les pirates tentent de s'infiltrer dans un réseau informatique d'une itératives en utilisant des comptes génériques, standardisés tel que admin, toor, sybase, solaris, linux, etc., associés à des mots de passe identiques au nom du compte. Quant aux mots de passe des constructeurs, il suffit de se rendre sur le site http : // www.google.fr et de rechercher « default password » pour se faire une idée du laxisme ambiant.*
- ***Faiblesses d'implémentation ou bogues****: Les faiblesses d'implémentation ou des bogues des programmes (systèmes d'exploitation, application de routage,...) exposent les réseaux à de nombreux types d'attaques très sophistiquées tel que les attaques de type SYN flooding et ping-of-death.*
- ***Mauvaises configuration*** *: Une mauvaise configuration des équipements et logiciels de gestion ou d'administration réseau est à l'origine de plusieurs attaques. Par exemple un firewall mal configuré laisse passer du trafic non autorisé par la politique de sécurité. La configuration des équipements réseau est critique et doit suivre des règles strictes d'implémentation afin d'éviter que le réseau ne soit compromis.*

II.5 -*Approches de détection d'intrusion :*

Les méthodes de détection définissent la philosophie sur laquelle l'analyseur est construit. Depuis le rapport séminal de J.P. Anderson[5], plusieurs approches de détection d'intrusion ont été suggérées. Plusieurs schémas de classification de ces approches ont été proposés dans la littérature spécialisée. La plus populaire de ces classifications consiste à classer les approches de détection en deux grandes classes : la détection d'anomalie et la détection d'abus d'utilisation. Une classification, qui est considérée ici, également aussi connue que la première, les classe en deux catégories d'approches à savoir : Détection d'abus d'utilisation, détection d'anomalie. La performance de ces approches est mesurée en terme de : Faux négatif et de faux positif. Le faux positif désigne la situation dans laquelle le système de détection d'intrusion signale une activité normale comme étant une intrusion. Alors que la fausse négative décrit le fait qu'une intrusion est reportée comme étant une activité normale.

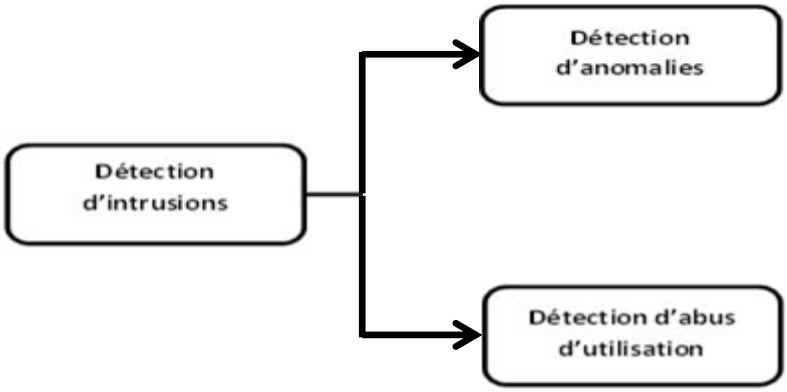


Figure 2.2 : – Approches de détection d'intrusion

La détection d'abus d'utilisation tente de coder les connaissances sur les intrusions connues sous forme de signatures spécifiques. La détection d'anomalie et la détection par spécification établissent un modèle à partir de flux de données observés sous les conditions normales sans la présence d'aucune intrusion. Dans la détection par spécification, les experts en matière de sécurité informatique prédéfinissent les différents comportements autorisés du système. Tout événement ne coïncidant pas avec les spécifications est reporté comme intrusion.

II.5.1- *Détection d'abus d'utilisation :*

Est l'approche la plus basique et la plus ancienne. Elle repose sur le concept de bibliothèque de signatures d'attaques et consiste à surveiller (monitoring) le trafic réseau à la recherche des empreintes (signatures) d'attaques connues et répertoriées dans une base de connaissances (signatures) sous forme de règles. Les données d'audit collectées par le système de détection d'intrusion sont comparées avec le contenu de la base de signatures. Si une correspondance est trouvée, une alerte est générée (Figure 2.3). Dans le cas échéant, toute intrusion sera considérée comme une action légitime.

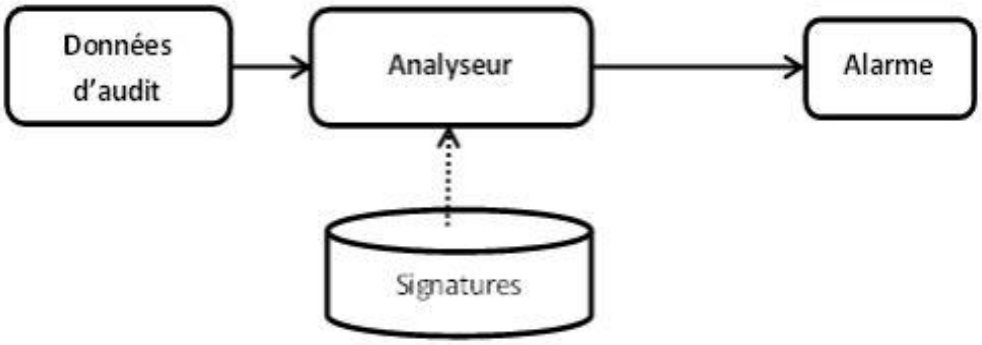


Figure 2.3 : Diagramme d'un système de détection d'abus d'utilisation.

Les signatures d'attaques sont établies par des experts de sécurité familiarisés avec les vulnérabilités des systèmes et les attaques ou menaces connues. Les systèmes de détection, basés sur cette approche, se caractérisent les uns des autres par la façon de représenter les signatures d'attaques et les mécanismes utilisés pour vérifier les occurrences de ces signatures dans les données d'audit. Ils utilisent, généralement, des systèmes experts pour analyser les données d'audit. Les systèmes de détection d'abus produisent un faible taux de faux positifs. Cela est dû au fait que les langages de description d'attaques permettent, habituellement, de modéliser les attaques, à un niveau très fin, de tel façon que seulement quelques activités légales coïncident avec une entrée de la base de signatures. Par contre, ils sont incapables de détecter de nouvelles attaques (non décrites dans la base de signatures) ou même des variantes d'attaques connues. MIDASWisdom and Sense (W & S), NADIR, NIDES,furent les premiers systèmes de détection utilisant cette approches.

II.5.2- ***Détection d'anomalie*** *:*

Ces modèles "comportementaux" sont apparus bien plus tard que les systèmes à base de signatures. Initialement proposés par JP. ANDERSON puis repris et étendus par D.E. DENNING [3], ces modèles se basent sur l'hypothèse selon laquelle l'exploitation d'une vulnérabilité du système implique un usage anormal de celui-ci. Une intrusion est donc identifiable en tant que déviation par rapport au comportement habituel d'un utilisateur.

La détection d'anomalie suppose que tout comportement inattendu est l'évidence d'une intrusion. Elle analyse un ensemble de caractéristiques du système et compare leur comportement à un ensemble de valeurs prévues. Dans le cas où les statistiques calculées ne concordent pas avec les mesures prévues une tentative d'intrusion est signalée (Fig. 2.4).

Implicite est la croyance qu'un certain ensemble de métrique peut caractériser le comportement prévu d'un utilisateur ou d'un processus. Il est à noter qu'il existe plusieurs approches et techniques pour construire ou décrire un comportement normal de l'utilisateur :

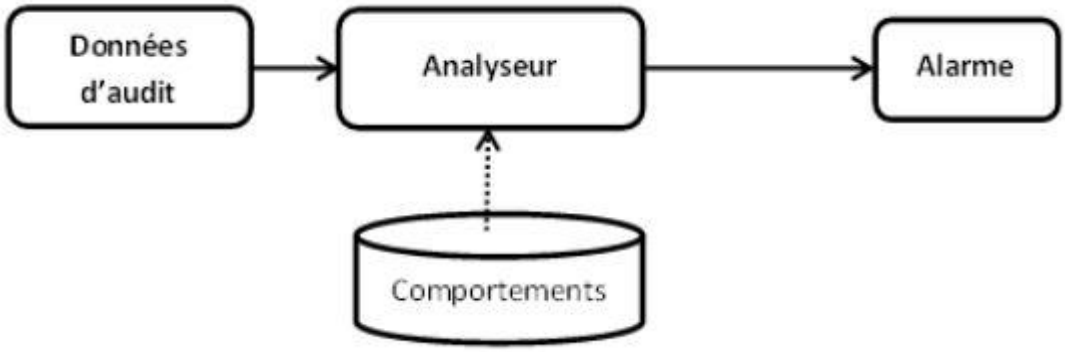


Figure 2.4 : Diagramme d'un système de détection d'anomalie.

– ***Observation de seuils*** *: Il s'agit de fixer le comportement normal d'un utilisateur par la donnée de seuils à certaines mesures (par exemple, le nombre maximum de mots de passe erronés). Comme il est difficile de caractériser un comportement intrusif en termes de seuil, cette méthode peut entraîner beaucoup de fausses alarmes et d'événements malveillants non détectés.*

– ***Approche bayésienne*** *: les réseaux Bayésiens mettent l'accent sur les relations de causalité existantes. Dans les situations où la connaissance de l'ensemble des relations entre les phénomènes est incomplète, il devient nécessaire de les décrire de manière probabiliste. Les indications obtenues progressivement sur l'état du système modélisé influent sur la confiance que l'on accorde à une hypothèse donnée.*

– ***Profilage d'utilisateurs****: On établit des profils individuels du travail des usagers, auxquels ils sont censés adhérer ensuite. Au fur et à mesure que l'utilisateur change ses activités, son profil de travail attendu se met à jour. Il reste cependant difficile de déterminer un profil pour un utilisateur irrégulier ou très dynamique.*

– Profilage de groupes *: Pour réduire le nombre de profil à gérer, on classe les utilisateurs par groupe. Chaque groupe est caractérisé par genre de travail commun. Un profil de groupe est calculé en fonction de l'historique des activités du groupe entier. On vérifie que les individus du groupe travaillent en conformité et ne dévient pas par rapport à ce qu'a été défini comme profil de groupe. Mais il est parfois pas évident de trouver le groupe le plus approprié à une personne. D'ailleurs, il est parfois nécessaire de créer un groupe pour un seul individu.*

– ***Profilage d'utilisation de ressources*** *: Il s'agit d'observer l'utilisation de certaines ressources comme les processeurs, les ports de communication, les comptes, les applications, les mémoires de masse, la mémoire vive sur de longues périodes, on vérifie et on compare par rapport à ce qui a été observé par le passé. On peut aussi observer les changements dans l'utilisation des protocoles réseau, rechercher les ports qui voient leur trafic augmenter anormalement. L'expérience a montré qu'il est difficile d'interpréter les écarts par rapport au profil normal.*

– ***Profilage de programmes exécutables*** *: Les virus, les chevaux de Troie et autres programmes malveillant peuvent être démasqués profilant la façon dont les objets du système comme les fichiers ou les imprimantes sont utilisés. Donc, le profilage de programmes exécutables stipule qu'on observe l'utilisation des ressources du système par les programmes exécutables. Ce profilage peut se faire par type d'exécutable. On peut par exemple détecter le fait qu'un serveur d'impression se mette à attendre des connexions sur des ports autres que ceux qu'il utilise d'habitude.*

–***Profilage statistique*** *: DENNING a défini un modèle statistique de comportement utilisateur dans. Ce modèle statistique permet de déterminer, au vue de n observations* x_1, ..., x_n *faites sur une variable x, si la valeur xn+1 de l'observation (n + 1) est normale ou non. Explicitement, un profil est constitué d'un ensemble de variables représentant une quantité accumulée d'événements (nombre de fois qu'une commande système particulière à été exécutée par un utilisateur, nombre de quantum de temps CPU occupé par un programme, etc.) pendant une certaine période de temps.*

– ***Graphes*** *: Certaines approches comportementales utilisent des modèles à base de graphes pour mettre en évidence des propriétés et des relations entre ces propriétés. L'intérêt de cette approche est qu'elle permet de traiter plus facilement des événements rares. On parle d'apprentissage des comportements normaux dans le cas d'un système informatique ouvert et de spécification des comportements normaux dans le cas d'un système informatique fermé.*

II.5.3- *Comparaison des approches de détection :*

Considérons dans un premier temps la différence entre la détection d'abus et la détection d'anomalie sur le plan de connaissance, configuration, données générées, exactitude.

1. Connaissance *: Un système de détection d'intrusion utilisant l'approche de détection des malveillances doit " connaître " toutes les signatures possibles. Il doit identifier les détails d'une attaque aussi bien que son modèle à un niveau d'abstraction élevé qui caractérise la classe de l'attaque. De son côté un système se basant sur les modèles comportementaux doit disposer d'une complète connaissance sur les différents comportements probables du système pour être en mesure de détecter toutes les attaques. En réalité cela n'est pas possible et représente une situation idéale.*

2. Configuration *: En général, un système de détection utilisant une base de signatures exige un effort de configuration moins que celui exigé par un système de détection basé sur les modèles comportementaux. Cependant il nécessité plus de données, d'analyse et de mise à jour. Par contre, les systèmes de détection basés sur les modèles comportementaux sont plus difficiles à configurer par ce qu'il demande une définition compréhensive des comportements connus et probables du système. En général, un support automatique est*

fourni mais nécessite beaucoup de temps dans son développement et les données qu'il utilise doivent être claires.

3. Données Générées (*reported data****)*** *: Les systèmes de détection d'intrusion utilisant une base de signatures produisent des conclusions basées sur " pattern matching ". Alors que les conclusions des systèmes de détection basés sur les models comportementaux sont basées sur des corrélations statistiques entre les profils actuels et probables.*

4. L'exactitude des signatures *: Les profils, décrivant les comportements, non correctement spécifiés produisent, potentiellement, un nombre élevé de "faux positifs" et de "faux négatifs".*

Afin de contourner les inconvénients et de tirer profits des avantages de chacune des approches, certaines systèmes de détection hybrides utilisent une combinaison des modèles comportementaux (détections des anomalies) et de la détections de malveillance.

II.6- *Règles pour la détection des attaques dans les réseaux de capteurs :*

Un ensemble de règles a été proposé, dans la littérature, afin de détecter des attaques du type: Hello flood, Black hole, Selective for warding, Jamming, Wormhole, et Déni de service (DOS) lancées contre un réseau de capteurs sans fil. Ces règles sont illustrées dans le Tableau 2.1.

Nom de la règle	Description de la règle	Attaques détecté
Règle de l'intervalle	Le temps de réception entre deux paquets successifs ne doit pas être supérieur ou inferieur à un certain seuil	*Hello flood*
Règle de retransmission	L'agent IDS surveille si le nœud retransmit le paquet reçu à son voisin	*Black hole et Selective Forwarding*
règle de la répétition	Nombre de retransmissions du même message par le nœud	Déni de service (DOS)
Portée de transmission radio	Le message reçu par L'agent IDS doit être de provenance de l'un des ses nœuds voisin	*Wormhole, Hello flood*
Règle de brouillage	Le nombre de collisions associées à un message doit être inférieur au nombre prévu de collisions	*Jamming*
Règle de delay	Une anomalie est détectée si le message n'est pas transmis en temps demandée.	*Jamming et* DOS

Tableau 2.1: Règles pour la détection des attaques dans les réseaux de capteurs

Une mise à jour continue de ces règles doit être appliquée pour une détection efficace de ces attaques.

II.7- *Système de détection d'intrusion :*

On appelle Systèmes de Détection d'intrusion un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion. Un système de détection d'intrusion n'est en aucun cas une mesure de sécurité autonome mais un complément indispensable aux mécanismes de sécurité préventifs.

*Il y a trois principaux composants dans un IDS : le module de collection des données, le module de détection, et le module de réponse. Le module de collection des données assure les tâches de collecte et du prétraitement des données comme : le stockage et le transfert des données au module de détection. Un IDS peut utiliser différentes sources de données telles que: les logs du système, les paquets du réseau, etc. Un IDS qui surveille uniquement les activités de l'hôte et détecte les intrusions uniquement au niveau hôte, est appelé host-based IDS[3] (abrégé HIDS, traduction de système de détection d'intrusion basé sur l'hôte). Si l'IDS surveille les activités et détecte les intrusions au niveau réseau, alors il est appelé network-based IDS (abrégé NIDS, traduction de système de détection d'intrusion basé sur le réseau). Dans les réseaux sans fil multi-sauts les NIDS utilisent généralement le mode promiscuité pour écouter et collecter des données dans un segment du réseau, et ainsi détecter les attaques distribuées. Il existe aussi les systèmes de détection d'intrusion hybrides qui surveille les activités au niveau réseau aussi bien qu'au niveau hôte pour assurer une meilleure détection *76+. En fonction de l'architecture du système on peut distinguer deux types d'IDS : centralisés et distribués. Il a été montré que les IDSs distribués sont hiérarchiquement organisés autour d'un nœud central et que peu d'entre eux sont complètement distribués. Généralement, seule la collecte de données est distribuée dans un IDS distribué.*

II.8- *Critères de choix d'un système de détection d'intrusion :*

*Aujourd'hui les systèmes de détection d'intrusion (***SDI)** *sont réellement devenus indispensables lors de la mise en place d'une infrastructure de sécurité opérationnelle. Ils s'intègrent donc toujours dans un contexte et une architecture qui imposent des contraintes pouvant être très diverses. C'est pourquoi il n'existe pas de grille d'évaluation unique pour ce type d'outil. Pourtant un certain nombre de critères peuvent être dégagés ; ceux-ci devront nécessairement être pondérés en fonction du contexte de l'étude.*

- ***Fiabilité** : Un détecteur d'intrusion doit être fiable ; les alertes qu'il génère doivent être justifiées et aucune intrusion ne doit pouvoir lui échapper. Un système de détection d'intrusion générant trop de fausses alertes sera à coup sûr désactivé par l'administrateur et un autre ne détectant rien ne sera rapidement considéré comme inutile.*

- ***Réactivité** : Un système de détection d'intrusion doit être capable de détecter les nouveaux types d'attaques le plus rapidement possible. Pour cela il doit rester constamment à jour. Des capacités de mise à jour automatique sont pour ainsi dire indispensables.*

- ***Facilité*** *de mise en œuvre et adaptabilité : Un système de détection d'intrusion doit être facile à mettre en œuvre et doit pouvoir surtout s'adapter au contexte dans lequel il doit opérer ; il est inutile d'avoir un système de détection d'intrusion émettant des alertes tous les 10 secondes si les ressources nécessaires à une réaction ne sont pas disponible pour agir dans les mêmes contraintes de temps.*

- ***Performance*** *: la mise en place d'un système de détection d'intrusion ne doit en aucun cas affecter les performances des systèmes surveillés. De plus, il faut toujours avoir la certitude que le système de détection d'intrusion a la capacité de traiter toute l'information à sa disposition (par exemple un système de détection d'intrusion réseau doit être capable de traiter l'ensemble du flux pouvant se présenter à un instant donné sans jamais dropper de paquets) car dans le cas contraire il devient trivial de masquer les attaques en augmentant la quantité d'information.*

- ***Multi canal*** *: Un bon système de détection d'intrusion doit pouvoir utiliser plusieurs canaux d'alerte (email, téléphone, fax...) afin de pouvoir garantir que les alertes seront effectivement émises. 6. Information : Le système de détection d'intrusion doit donner un maximum d'information sur l'attaque détectée afin de préparer la réaction.*

- ***Classification*** *: il doit être aisé de hiérarchiser la gravité des attaques détectées afin d'adapter le mode d'alerte.*

Dans les réseaux de capteurs sans fil un SDI doit satisfaire les propriétés suivantes [3] :

- ***Audit local*** *: un SDI pour les réseaux de capteurs sans fil doit fonctionner avec des données d'audits locales et partielles car dans les réseaux de capteurs sans fil, il n'y a pas de points centralisés (à part la station de base) qui peut collecter les données d'audit globales.*

- ***Ressources minimales:*** *un SDI pour les réseaux de capteurs doit utiliser un nombre minimum de ressources car les réseaux sans fils n'ont pas de connexions stables. De plus les ressources physiques du réseau et des noeuds telles que la bande passante et la puissance sont limitées. La déconnexion peut survenir à* tout moment. La communication entre les noeuds pour la détection d'intrusion ne doit donc pas prendre toute la bande passante disponible.

- ***Pas de nœud de confiance:*** *un SDI dans les réseaux de capteur ne doit faire confiance à aucun noeud car, contrairement aux réseaux filaires, les noeuds capteurs peuvent être compromis facilement.*

- ***Destribué:*** *veut dire que la collection et l'analyse de données doit se faire dans plusieurs endroits (locations). De plus l'approche distribuée s'applique aussi pour l'exécution de l'algorithme de détection et la corrélation d'alertes.*

- ***Sécurisé****: un SDI doit être capable de résister aux attaques.*

II.9- Architecture des SDIs dans les RCSF :

Les architectures des SDI dans les réseaux ad hoc et les réseaux de capteurs sans fils peuvent être classées en trois catégories [3] :

- ***Autonome** : Dans cette catégorie, chaque noeud opère comme un SDI indépendant et il est responsable de la détection des attaques contre lui. Par conséquent, dans cette catégorie, les SDI ne coopèrent pas et ne partagent aucune information entre eux. Cette architecture exige que chaque noeud soit capable d'exécuter un SDI.*

- ***Distribuée et coopérative:** Dans cette architecture chaque nœud exécute son propre SDI mais les SDIs coopèrent afin de créer un mécanisme de détection d'intrusion global.*

- ***Hiérarchique**: Dans ce cas le réseau de capteur est divisé en groupes (clusters). Dans chaque groupe, un leader joue le rôle de cluster-head. Ce nœud est responsable du routage dans le groupe et doit accepter les messages des membres du groupe indiquant quelque chose de malveillant. De même le cluster-head doit détecter les attaques contre les autres cluster-heads du réseau.*

II.10 - *Métriques d'évaluation des systèmes de détection d'intrusion dans le RCSF :*

Afin d'évaluer l'efficacité des systèmes de détection, un ensemble de métriques doit être adopté pour quantifier le niveau de sécurité et utiliser au mieux les ressources telles que la consommation d'énergie et l'espace de stockage. Ces indicateurs de performance nous permettront de choisir le meilleur système de détection. En conséquence, les métriques suivantes sont considérées comme des caractéristiques importantes pour la conception efficaces des systèmes de détection d'intrusion.

- ***Taux de détection :** Représente le pourcentage de détection d'attaques sur le nombre total d'attaques.*
- ***Taux de faux positifs** (les fausses alarmes) : C'est le rapport entre le nombre des connexions normales classées comme étant une anomalie sur le nombre total des connexions normales.*
- ***Taux de faux négatifs** : Elle est l'inverse du taux de détection, cette métrique est définie par le rapport des fausses détections d'attaques sur le nombre total d'attaques.*
- ***Consommation d'énergie :**.Mesure de l'énergie consommée par un système de détection d'intrusion. l'énergie totale du réseau est définie comme étant la somme de l'énergie consommée par chaque nœud.*
- ***L'efficacité** : Détermine le temps nécessaire pour un système de détection d'intrusion puisse détecter l'apparition du premier nœud attaquant.*

II.11- Conclusion :

Dans ce chapitre, nous avons essayé de jeter un bref aperçu sur la problématique de la sécurité dans les réseaux de capteurs sans fil. Nous avons présenté les exigences et les défis imposés pour sécuriser de tels réseaux ainsi que les principales attaques les menaçant. Aussi nous avons introduit la notion de détection d'intrusion dans les réseaux de capteurs sans fil. Nous avons définis les différentes approches de détection, les systèmes de détection leur architecture et les critères de leur choix.

A l'issu de ce chapitre, nous concluions que les mécanismes de sécurité utilisées dans les réseaux traditionnels ne peuvent pas être directement appliquées aux RCSF, vu les contraintes de sécurité qui caractérisent ce type de réseaux. En conséquence, les RCSF exigent donc le développement des mécanismes de sécurité qui tiennent compte de leurs caractéristiques et de leurs vulnérabilités.

Implémentation

III-*Introduction :*

L'objectif de ce chapitre consiste à implémenter et interpréter les résultats des différentes simulations faites sur un réseau de capteurs sans fil sous l'attaque Blackhole. Cette étude consiste à simuler un réseau de capteurs sans fil, à comparer et à souligner les diverses notifications apportées par le système de détection d'intrusions. Comme une expérimentation directe effectuée sur le terrain peut se révéler coûteuse, irrationnelle et même impossible. Nous nous sommes contentés d'une simple simulation. Cette simulation va nous permettre d'examiner facilement et rapidement les variantes du système étudié.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 la technologie la mieux adaptée aux besoins. Beaucoup de simulateurs réseaux ont été développés pour répondre. Parmi ces simulateurs, nous pouvons citer : OPNET, GloMosim, QualNet, INSANE, NetSim, OMNeT++, NS2. Dans le cadre de ce projet de fin d'étude, nous avons choisi d'utiliser NS-2 (Network simulator) qui est un simulateur de réseaux appartenant au domaine.

III.1-*L'attaque BlokHole :*

L'attaque Blackhole est une sorte d'attaque de type DOS (Denial Of Service), passive qui se produit dans le réseau lorsque le nœud malveillant saisit des données complètes et ne les transmet pas. Empêchant ainsi la source de communiquer avec la destination. L'attaque par trou noir est similaire au trou noir universel qui attaque toutes les choses qui s'en approchent.

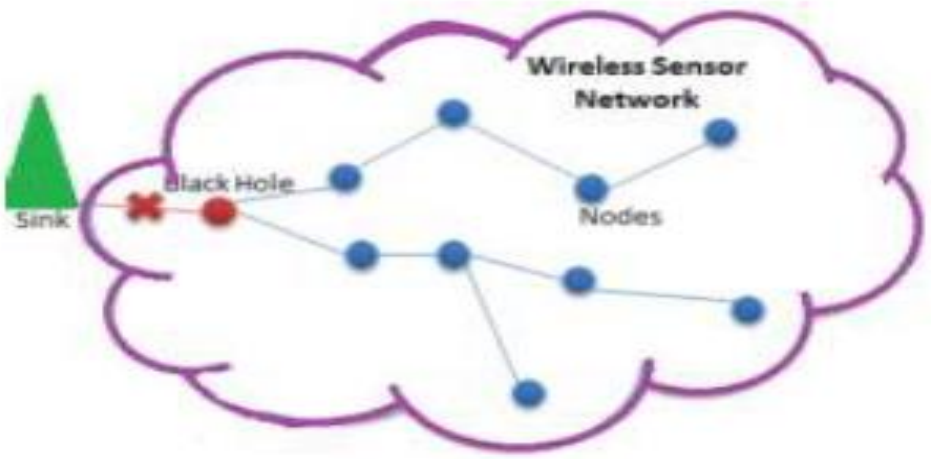


Figure 3.1 :Blackhole dans un réseau de capteurs sans fil

Le nœud malveillant prétend avoir une route optimale pour la destination et indique que le paquet devrait être acheminé par lui en transmettant de fausses informations de routage.

Ceci peut être réalisé, par exemple, par injection de faux paquets de contrôle dans le réseau. Si de tels paquets sont traités, un chemin passant par un trou noir sera mis en service. Une autre variante de cette attaque appelée greyhole existe. Elle consiste à ne pas supprimer tous les paquets, mais à en sélectionner quelques-uns uniquement. L'impact de cette attaque est que le nœud malveillant peut soit détruire ou utiliser improprement les paquets interceptés sans les transmettre.

Les attaques de trous noirs peuvent être classées en deux types:

- *Trou noir à nœud unique Dans ce cas, un seul nœud agit comme un trou noir entre la source et la destination.*
- *Collaboration du Trou noir Dans ce cas, deux ou plusieurs nœuds malveillants se combinent pour former un trou noir sur la route.*

L'attaque Trou Noir est l'un des problèmes les plus importants dans les réseaux ad-hoc , en général, cependant, elle peut être évitée, détectée et supprimée à l'aide de protocoles de sécurité.

III.2-Solution proposée :

Lors de notre recherche bibliographique, nous avons constatés l'existence de plusieurs travaux visant à proposer des solutions faisant face à cette attaque. Par exemple, certains travaux ont proposé une solution contre l'attaque le BLackhole en modifiant le protocole AODV[7]. Dans cette méthode chaque nœud intermédiaire doit inclure l'information «next hop» quand il envoie un paquet RREP. Une fois la source a reçu le paquet RREP et avant d'envoyer les paquets de données, il extrait l'adresse du «next hop» et lui envoie une nouvelle demande de route (FurtherRequest) afin de vérifier qu'il possède une route vers le nœud intermédiaire qui a envoyé le message de réponse, et qu'il a aussi une route vers le nœud destination. Le «next hop» répond avec un paquet de réponse de route (FurtherReply) qui comprend le résultat de contrôle. La source vérifie les informations des paquets FRREP et agit selon les règles suivantes:

- *Si le «next hop» possède une route vers le nœud intermédiaire et la destination, la source établit la route reçue du nœud intermédiaire et commence l'envoi des données.*
- *Si le «next hop» a une route vers la destination, mais n'a pas de route vers le nœud intermédiaire, la source suppose que le nœud intermédiaire est un nœud malicieux. Ensuite, elle initie l'envoi des données via la nouvelle route à travers le next hop et diffuse un message d'alarme dans le réseau afin d'isoler le nœud malveillant.*
- *Si le «next hop» n'a pas de routes vers le nœud intermédiaire et la destination, la source lancera un nouveau processus de découverte de route, et envoie également un message d'alarme afin d'isoler le nœud malveillant.*

Ce mécanisme est efficace, cependant, l'envoi d'un paquet FRREQ à partir du nœud source vers le «next hop» et l'attente du paquet FRREP du« next-hop » augmente la charge du routage «overhead» entre la source et le «next hop», surtout quand ce mécanisme est appliqué sur un réseau à grande échelle et la distance entre la source et le nœud malicieux est longue.

Une autre solution consiste à trouver plus d'une route vers la destination (au moins trois routes différentes). La source envoie un paquet RREQ au nœud destination en utilisant ces trois routes. La destination, le nœud malicieux et les nœuds intermédiaires vont répondre à ce

paquet. Le nœud expéditeur met ses paquets de données dans un tampon jusqu'à ce qu'il reçoit plus d'une réponse RREP; lorsque la source reçoit des RREP, si les routes à destination ont des nœuds partagés, la source peut reconnaître une voie sûre vers la destination, et les paquets vont être transmis. Si aucuns nœuds partagés ne semblent être dans ces routes redondantes, l'expéditeur attendra une autre RREP jusqu'à ce qu'un chemin avec des nœuds partagés identifié ou le temps d'attente soit expiré. Cette solution peut garantir à trouver une route sécurisé vers la destination, mais le principal inconvénient est le délai d'attente. Plusieurs paquets RREP doivent être reçues et traitées par la source. En outre, s'il n'y a pas de nœuds partagés entre les routes, les paquets ne seront jamais envoyés.

D'autres chercheurs ont proposé comme solution l'utilisation de deux protocoles de routage proactif : comme OLSR et réactif comme AODV[7], ensuite ils ont comparé les résultats des deux protocoles. Ils se sont basés sur le fait " les réseaux Ad hoc fonctionnent sans un administrateur central, cette caractéristique vulnérable peut être exploitée par un attaquant au sein de réseaux". Les chercheures ont utilisé le simulateur OPNET comme l'outil de mesure de performance du réseau Ad hoc. Le résultat de cette étude est la simulation de l'attaque de trou noir par l'AODV et OLSR et prendre les critères Delay, Throughput, Network Load, comme des critères de mesure de l'effet de l'attaque de trou noir.

Dans le cadre de ce mémoire, nous proposons l'implémentation, sous le simulateur NS-2[4], du Prior_ReceiveReply un mécanisme qui fait la détection de l'attaque blackhole proposé dans [4] et qui consiste, essentiellement à modifier uniquement le fonctionnement du nœud source sans altérer les nœuds intermédiaires et de destination.

DSN – Destination Sequence Number, NID – Node ID,
MN-ID – Malicious Node ID.

Step 1: (Initialization Process)
Retrieve the current time
Add the current time with waiting time
Step 2: (Storing Process)
Store all the Route Replies DSN and NID in RR-Table
Repeat the above process until the time exceeds
Step 3: (Identify and Remove Malicious Node)
Retrieve the first entry from RR-Table
If DSN is much greater than SSN then
discard entry from RR-Table
and store its NID in MN-ID
Step 4: (Node Selection Process)
Sort the contents of RR-Table entries according to the DSN
Select the NID having highest DSN among RR-table entries
Step 6: (Continue default process)
Call ReceiveReply method of default AODV Protocol

Algorithme 1- Prior-ReceiveReply

Dans ce mécanisme, quand le nœud source faitune demande de route avec un message RREQ, on définit d'abord le temps d'attente pour que le nœud source reçoivele RREQ provenant d'autres nœuds puis ajoute le temps actuel au temps d'attente. Puis dans le processus de stockage, on stock toutes les numéros des séquences RREQ et leurs nœuds dans la table RR-table jusqu'ç ce que le temps calculé soit dépassé. Généralement la première réponse d'itinéraireproviendra du nœud malveillant avec un numéro de séquence élevé, qui est stocké comme première entrée dans leRR-Table. Le numéro de séquence de la première destination et, ensuite, comparé à celui de la source. Si on constate une importante déférence, alors, surement, le nœud en question est malicieux et on doit, immédiatement, supprimer cette entrée de la RR-table. Une fois le nœud malicieux supprimé, le nœud ayant le numéro de séquence le plus élevé sera sélectionné comme nœud suivant.

III.3-Simulateur NS-2 :

NS (Network simulator) est un logiciel de simulation de réseaux informatiques développé lors d'un projet de la « DARPA », agence pour les projets de recherche avancée de défense aux États-Unis. Le simulateur NS, grâce à sa popularité, est devenu un standard et une référence pour tout objet de simulation. Ce simulateur est bien adapté aux réseaux à commutation de paquets. NS permet de modéliser tout composant du réseau en des objets réutilisables et modifiables. Il est possible de développer des parties, les publier et éventuellement les intégrer dans des modules de NS. Ce logiciel peut fonctionner sous les deux plateformes Windows et Linux, la différence est que sous linux, il est plus facile à l'installer. Sous Windows, on doit faire appel au chargeur « cygwin » qui permet d'émuler le serveur X de linux pour que plusieurs logiciels fonctionnant sous linux puissent fonctionner sous Windows.

Au départ, la version 1.0 de NS a été développée au Laboratoire National de Lawrence Berkeley (LBNL) par le groupe de recherche réseau. Son développement fait maintenant Partie du projet VINT (Virtual InterNetworkTestbed) qui a pour but la construction d'un Simulateur réseau offrant des outils et des méthodes novatrices, dans un environnement proche de la réalité. Ce simulateur essaie de répondre aux questions de mise à l'échelle (simulation de grandes topologies) et d'interaction entre divers protocoles.

- *NS-2 offre plusieurs avantages qui sont :*
- *NS2 est open source.*
- *Il est extensible, donc n'importe qui peut ajouter son propre protocole, ou faire une modification pour tester son algorithme.*
- *NS2 est orienté objet basé sur C++.*

À la simulation, NS utilise OTcl (orienté objet Tool Command Langage) qui est un langage pour interpréter des scripts de simulation de l'utilisateur. Le langage OTcl est en fait une extension orientée objet du langage Tcl.

Les outils NS2 et l'extension Mannasim permettent de créer un cadre de simulation détaillé pour un réseau de capteurs sans fil. En effet, NS2 nous permet de configurer les liens radio entre les nœuds de capteurs et ajuster le modèle de propagation qui convient. Le tableau 3-1 résume les paramètres de simulation.

Paramètre	Valeur
Type de canal	Channel/Wireless channel
Le modèle de propagation	Shadowing visibility
Le type d'interface réseau	Phy/WirelessPhy
Le type de MAC	Mac/802.11, 802.15.4
Antenne	Omni directionnelle
Modèle d'énergie	Batterie
La file d'attente	Queue/Drop Tail
Niveau d'énergie initial (J)	10
surface (m*m)	100*100

Tableau 3.1- Les paramètres de l'environnement de simulation

Le résultat d'une simulation est un fichier trace de l'extension «.tr » contenant tous les événements de la simulation. Un traitement ultérieur de ce fichier permet d'en soustraire l'information souhaitée. Par ailleurs, le simulateur permet la création d'un fichier d'animation (dont l'extension .nam), permettant de visualiser la simulation sur une interface graphique NAM (Network Animator). La figure 3.1 représente de façon simplifiée le point de vue d'un utilisateur de NS.

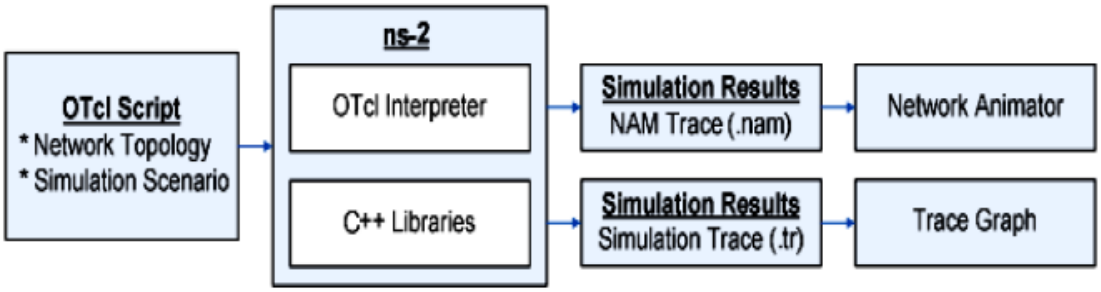


Figure 3. 2 : schéma de NS2

L'OTcl sert à décrire la topologie du réseau (nœuds, liaisons) et du trafic réseau (cheminement des paquets). NS2 interprète les scripts TCL et utilise la base de données de C++ sur les réseaux (C++Realm), il s'occupe ainsi des protocoles, des couches réseau et de leur simulation.

Le fonctionnement général de ce système se présente comme suit :

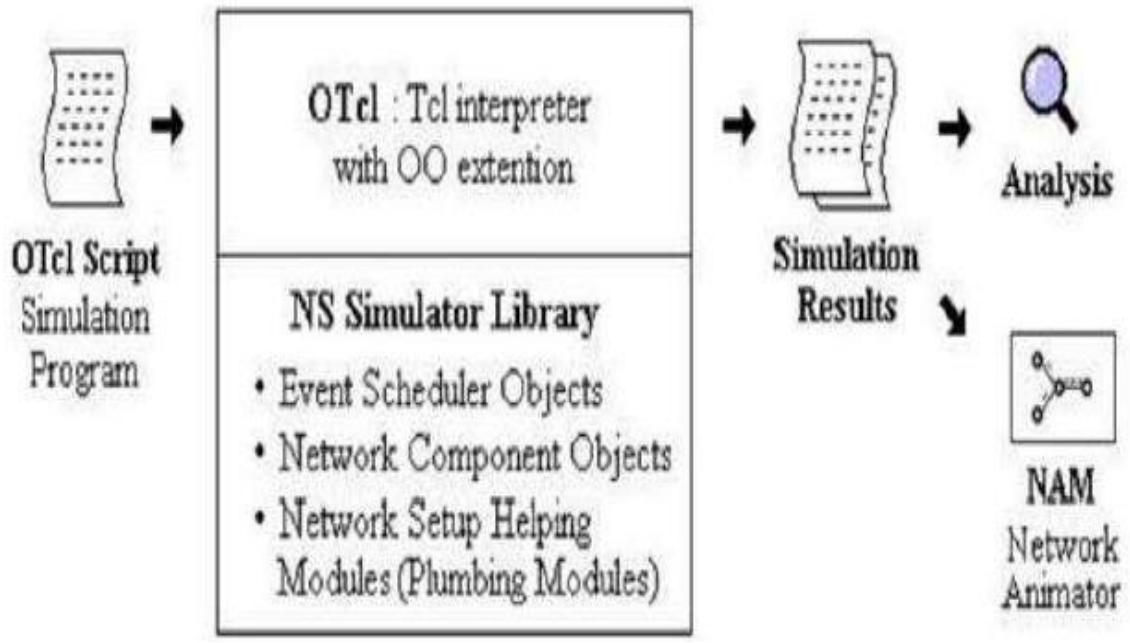


Figure 3.3 : Détail de fonctionnement du système OTcl – NS2.

III.4-Simulation d'un réseau de capteurs sans fil :

Le script OTcl est un fichier. TCL généré par un quelconque éditeur de texte et interprété par l'OTcl, il comprend en général les parties suivantes :

III.4.1- Les options de simulation : *sont le canal de transmission, le modèle de propagation, le type d'antenne, le type de couche liaison, type de file d'interface, le nombre maximum de paquets dans la file, le type d'interface réseau, le type MAC, le protocole de routage et le nombre de nœuds mobiles. La définition de chaque option se fait par la commande set val () pour affecter une valeur à la variable qui lui correspond. Cette partie est obligatoire au début de chaque simulation car tout nœud mobile se compose des éléments réseau détaillés en la figure suivante :*

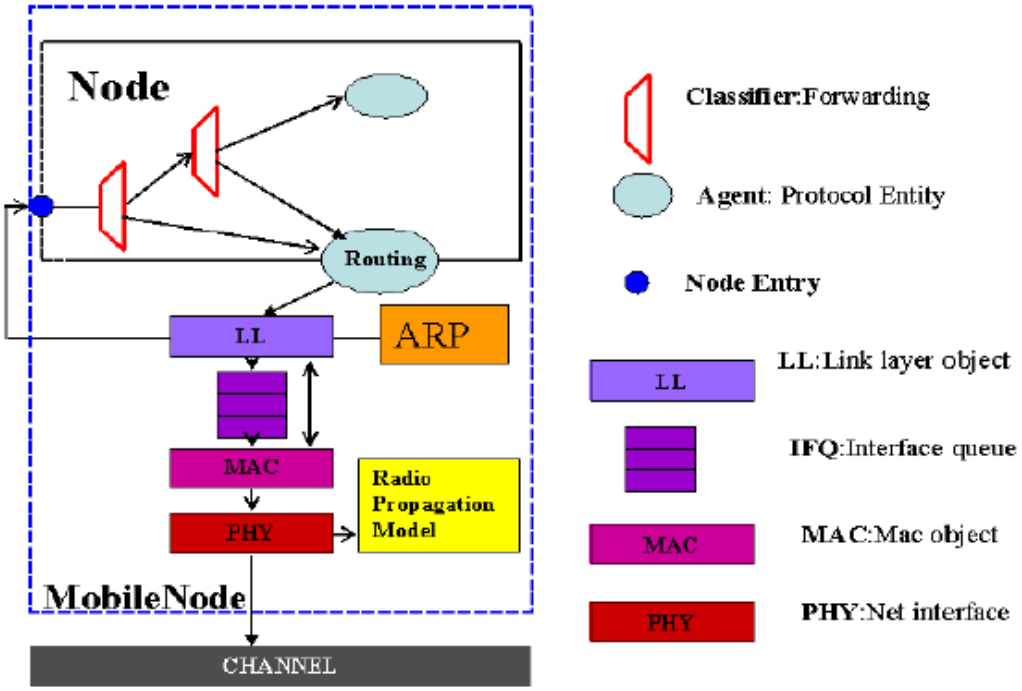


Figure3.4: Composants réseau ad_hoc

III.4.2-L'initialisation des variables globales :

Une nouvelle instance du simulateur : set ns_ [new simulator]

-l'option de traçage : $ns_ use-newtrace , nouvelle trace des événements

-créer le fichier trace : set tracefd [open fichiertrace.tr w]

-comment écrire dans le fichier trace : $ns_ trace-all &tracefd

-comment créer la trace d'une animation : set namtrace [open nomfichier.nam w]

-comment écrire dans le fichier animation : $ns_ namtrace-all-wireless $namtrace $val(x) $val(y)]

-préciser la topographie et l'initialiser : set topo [new Topography]

$topo load_flat_grid 500 500

créer un gestionnaire des opérations : create-god $val(nn), nn=nombre de noeud ;
Cette commande est essentielle car elle attache les noeuds au canal décrit plus haut.

III.4.3-La configuration des nœuds : *La configuration des nœuds utilise les options de simulation comme suit :*

```
set chan_1_ [new $val(chan)]
$ns_ node-config -adhocRouting $val(rp) \
-llType $val(ll) \
-macType $val(mac) \
-ifqType $val(ifq) \
-ifqLen $val(ifqlen) \
-antType $val(ant) \
-propType $val(prop) \
-phyType $val(netif) \
-channel $chan_1_ \
-topoInstance $topo \
-agentTrace ON \
-routerTrace ON \
-macTrace OFF \
-movementTrace ON
```

Pour créer les nœuds avec les paramètres spécifiés

```
for {set i 0} {$i < $val(nn) } {incr i}
{
set node_($i) [$ns_ node]
  $node_($i) random-motion 1;# enablerandom motion
}
```

III.4.4-Autres déclarations et initialisations : *Les positions initiales des nœuds doivent être déclarées, au moyen de leurs coordonnées, X, Y et Z (si nécessaire), par la commande $node_(n) set X_ 50.0 par exemple :*

Déclarer les couleurs des noeuds, si nécessaire, par :

```
$ns_ at .01 "$node_(1) colorblue" ;
```

Décrire la mobilité des noeuds : #Set destination format is

```
"setdest<x><y><speed>"
$ns_ at 0.01 "$node_(0) setdest 50.0 50.0 0.0"
$ns_ at 5.0 "$node_(0) setdest 350.0 350.0 0.0"
$ns_ at 6.0 "$node_(0) setdest 1.0 350.0 0.0"
$ns_ at 7.0 "$node_(0) setdest 50.0 50.0 0.0"
```

III.5-*L'implémentation d'un nœud malicieux :*

L'implémentation d'un nœud malicieux nécessite la mise-à-jour des fichiers dépendants (dependencies) du protocole AODV, qui sont montrés dans les figures suivantes :

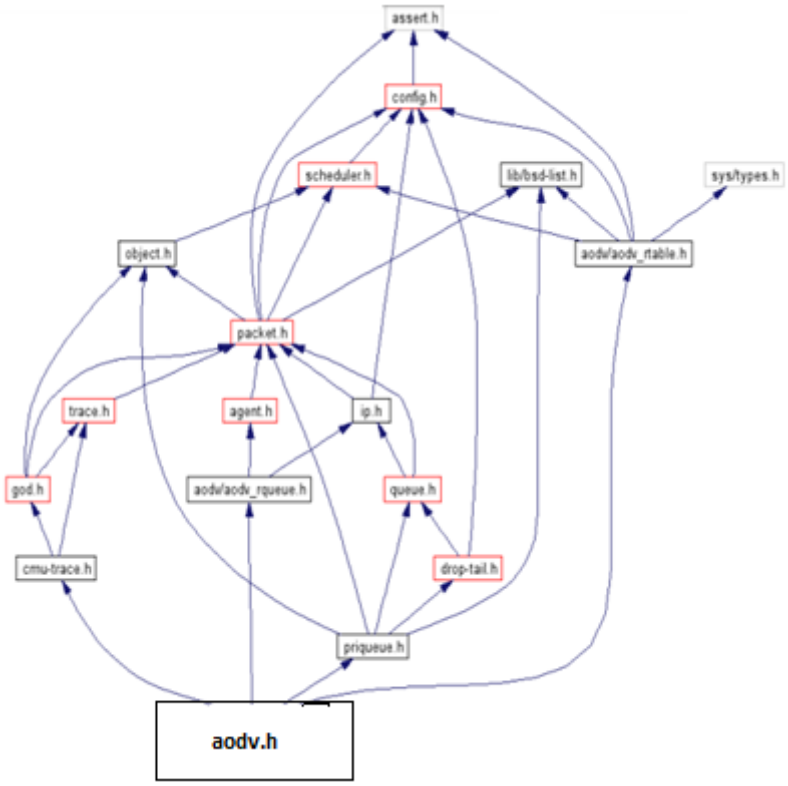


Figure 3.5 : Fichiers dépendants d'aodv.h

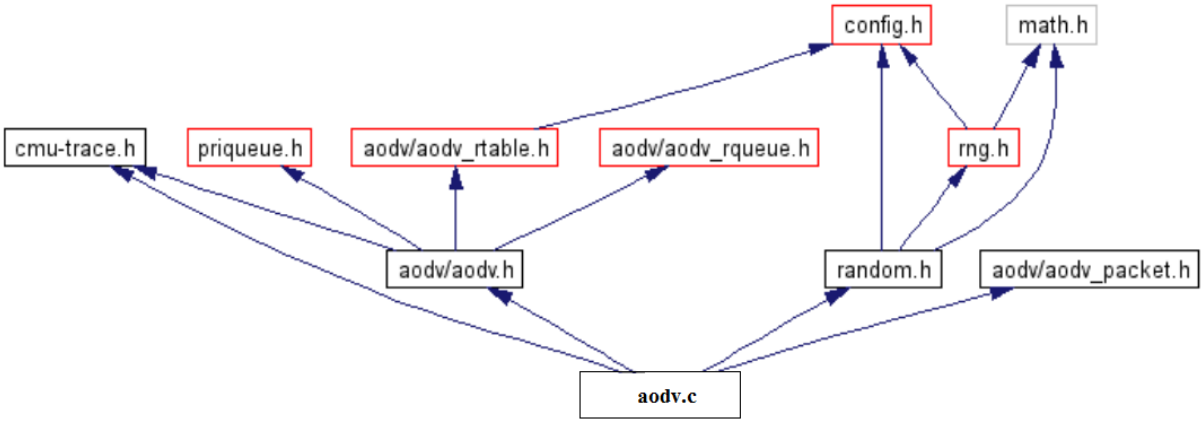


Figure 3.6 : Fichiers dépendants d'aodv.c

Dans le fichieraodv.h (header), déclarer le nœud malicieux : bool malicieux ;
Dans le fichier aodv.cc (source c++) :
Fonction AODV : malicieux = false ;

Fonction command effectuer le test :

```
If (strcmp(argv[1], ‘malicieux’ )==0)
{
   Malicieux = true ;
   Return TCL_OK ;
}
```

Fonction resolve, effectuer le test :

```
If (malicieux==true)
{
   Drop (p,DROP_MAL) ;
}
```

Dans le fichier cmu-trace.h, définir : #define DROP_MAL ‘MAL’

Dans le fichier TCL, caractériser le nœud malicieux :

```
$ns_ at 0 0 ‘$node_(3) colorred’
$node_(3) color ‘red’
$ns_ at 0 0 ‘[$node_(3) set ragent_] malicieux’
```

III.6-Simulation et Interprétation des résultats de simulation :

Dans le cadre d'une simulation sous NS-2, nous avons « construit » un réseau se composant de 50 nœuds 1 nœud malveillant (blackhole), La taille d'un paquet transmis est de 512 octets, La Vitesse de transmission d'un nœud est de 4 paquet/seconde, et la taille de topographie et de [500 x 500] m ,et le temps de simulation a duré 200 sec. Ces paramètres résumés dans le tableau suivant :

Paramètres	***Valeurs***
Simulator	*NS-2.35*
Canal	*Channel/Wireless channel*
Modèle de Propagation radio	*Propagation TwoRaymodel*
Network Interface	*Physical/Wirelessphy*
MAC	*MAC802_11*
Antenna	*Antenna/Omniantenna*
Interface QueueType	*Drop Tailpriority*
Protocols de routage	*AODV, AOMDV, DSDV*
Type de trafic	*CBR*
Nombre de noeuds	*10, 20, 30, 40, 50, 60,70*
Temps de pause	*10 s*
Taille de la zone géographique	*1000 m × 1000 m*
Temps de simulation	*200 s*

Table 3.2 – Paramètres de simulation

Dans notre étude, nous avons pris en compte les métriques suivantes :

- *Le taux de délivrance des paquets de données (delivery ratio) : Ce paramètre représente le pourcentage des paquets livrés à leurs destinations par rapport aux paquets émis dans le réseau. Il se calcule de la façon suivante :*

$$PDR=100\ x\ \frac{\sum (paquetsrecu)}{\sum (paquetemis)}\ \ (en\ \%)$$

- ***Taux d'overhead de routage (NormalizedRoutingLoad):*** *L'Overhead du réseau permet de mesurer le taux de paquets de contrôle de routage dans le réseau par rapport au nombre total de paquets reçus. Nous avons donc la formule suivante :*

Overhead= nombre de paquets de contrôle de routage / le nombre total des paquets reçus

Ce taux est recalcule à chaque émission ou réception d'un paquet au niveau de la couche Internet. Le calcul de l'overhead de routage est important pour déterminer la nature des paquets qui occupe le réseau.

- ***Le taux moyen de livraison réussie*** *des messages sur un canal de communication. Ces données peuvent être transmises via une liaison physique ou logique. Il est mesuré en bits par seconde*

Nous avons réalisé deux scénarii lors de la simulation :

Le scénario 1 : c'est le scénario dans lequel est injecté un nœud blackhole parmi les nœuds du réseau pour voir son comportement de par ses effets.

Le scénario 2 : c'est le scénario qui teste la solution (AODV modifié) pour montrer qu'il neutralise les effets du blackhole.

Nous allons varier le pause time pour chaque nombre de connexions par trafic et en fonction de ce dernier, nous allons évaluer des métriques mesurant notre protocole « normal » et sous l'attaque blackhole. Nous avons obtenu les résultats suivants :

1- *La figure 3.8 montre que dans le cas d'AODV normal, le taux de délivrance est supérieur à celui d'un AODV sous Blackhole. Cette dégradation de performances est due aux paquets supprimés par les nœuds malveillants dans le réseau.*

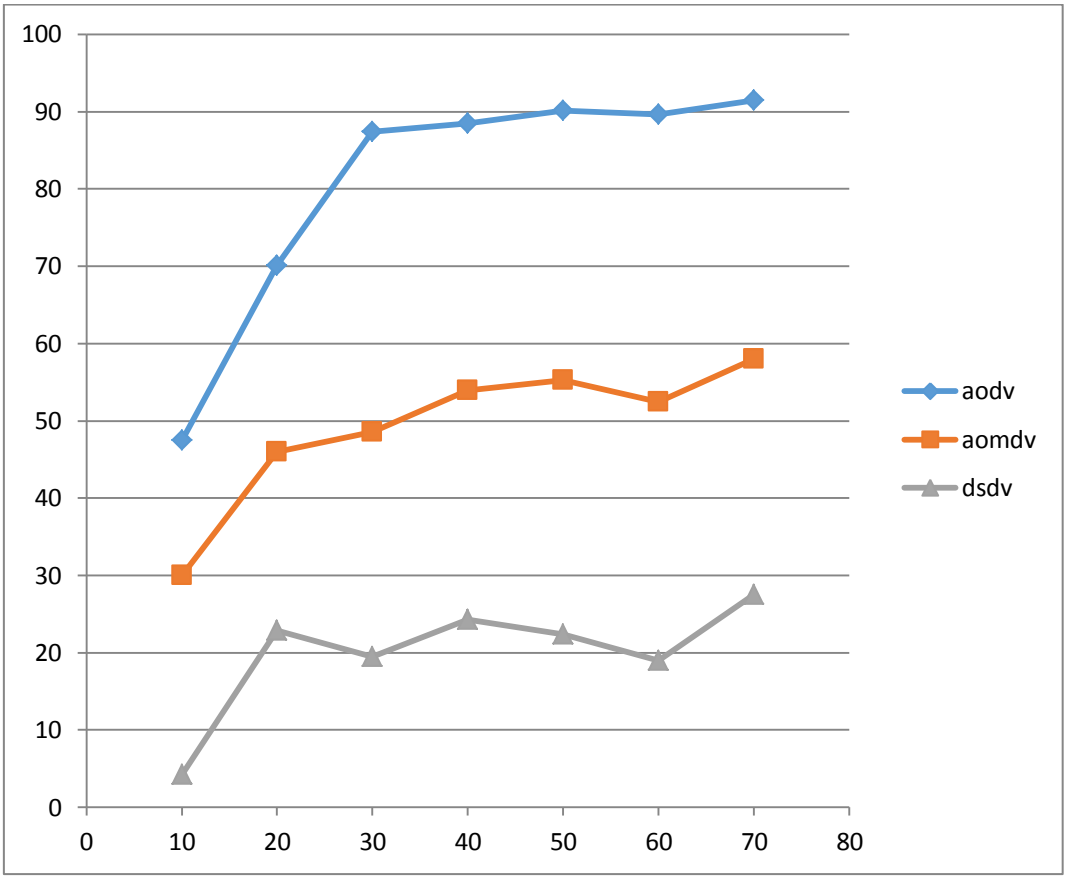


Figure 3.7 : Influence de la pause time sur PDR

2- *La figure 3.9 nous montre que dans AODV normal le taux des paquets émis sont très élevé par rapport à AODV sous Blackhole à cause de la file d'attente et la possibilité de long chemin. Pour l'AODV sous Blackhole la majorité des paquets n'arrive pas à destination ce qui cause une importante perte des paquets envoyés.*

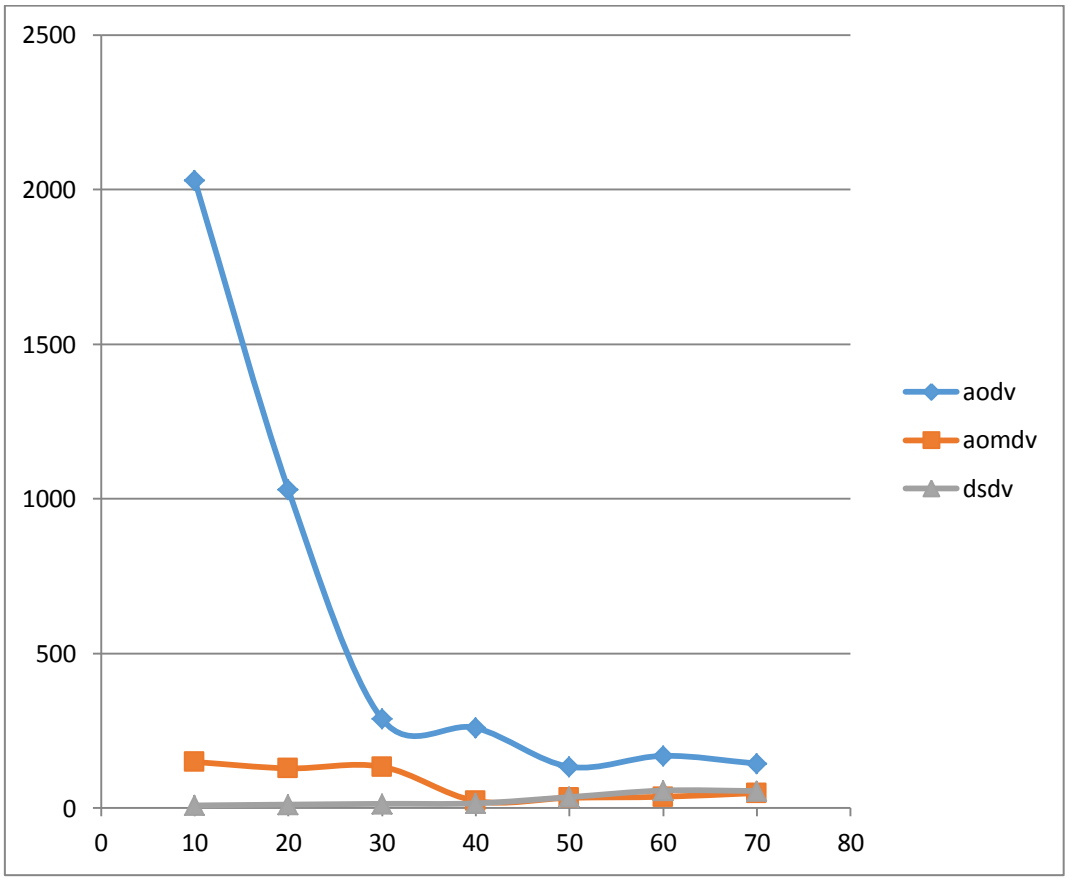


Figure 3.8 : Influence de la pause time sur délai

3- *La figure 3.10 montre que dans AODV normal l'Overhead est inférieur par rapport à l'AODV sous attaque.*

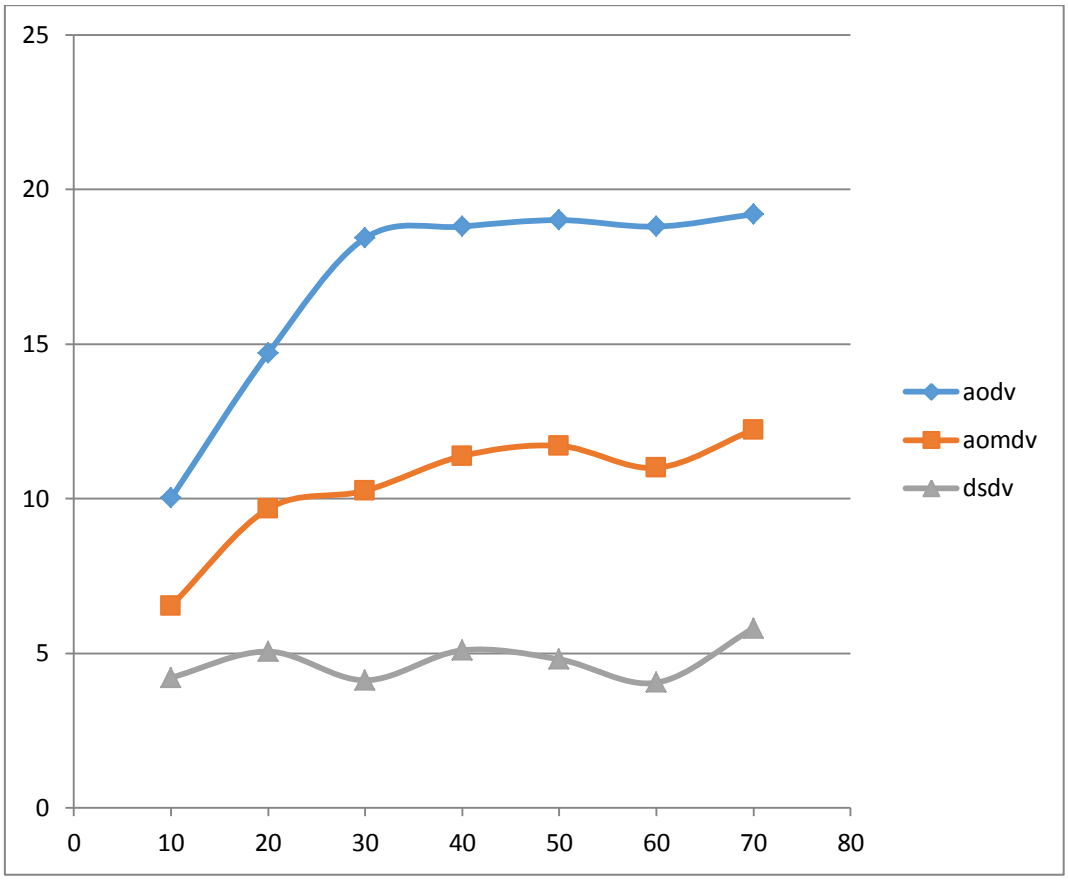


Figure 3.9 : Influence de la pause time sur taux moyen de livraison réussie des messages

La surcharge du réseau est représentée par le nombre de paquets de contrôle par rapport aux paquets donnés dans l'ensemble du réseau, le fait que l'ensemble des nœuds du réseau génère des paquets de contrôle périodiquement et que les nœuds malicieux suppriment tous les paquets de données affectent considérablement la surcharge du réseau.

Dans le premier scénario, le blackhole a supprimé les paquets envoyés vers le nœud destinataire. Alors que dans le deuxième scénario, les paquets arrivent à leur destinataire, l'AODV modifié a contourné l'attaque blackhole.

Conclusion Générale

Les problèmes inhérents aux réseaux sans fils sont assez sérieux et les touchent sur plusieurs plans laissant comprendre qu'ils resteront un domaine de recherche ouvert allant de leur conception jusqu'à leur exploitation. Ces réseaux sont exposés à plusieurs attaques, parmi lesquelles nous retrouvons l'attaque blackhole qui est lancée fréquemment dans le protocole AODV qui est le principal protocole utilisé dans ad-hoc.

Dans le cadre de ce mémoire, nous avons procédés à des simulations sur le protocole AODV normal, AODV sous attaque et ainsi que AODV modifié en utilisant le simulateur de réseau NS2.

Ce projet nous a permis de découvrir l'outil de simulation des réseaux NS2, découvrir et enrichir nos connaissances sur des domaines des réseaux sans fil et notamment ceux des capteurs sans fil ainsi que la problématique de sécurité de ce type de réseaux et plus précisément la tache de détection d'intrusion. A l'issue de cette étude, nous concluant qu'il ne peut y avoir une sécurité absolue vu le nombre important des facteurs qui conditionnent les performances des mécanismes de la sécurité informatique et celle des protocoles de routage des réseaux ad-hoc en particulier.

Bibliographie

[1] Abdelbari BEN YAGOUTA,Wireless Sensors Networks:Architectures, Applications & Limitations, Communication System Laboratory Sys'Com, National Engineering School of Tunis.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. "Wireless sensor networks: asurvey". Computer Networks 38, Elsevier Science, pp. 393–422, 2002.

[3] Abdelkader khobzaoui, Contribution des techniques dedatamining dans l'amélioration dessystèmes de détection d'intrusion dans lesréseaux informatiques. Thèse de doctorat en Informatique, Université DjillaliLiabesalgérie, 2017.

[4] DoumiAbdelmoumain, La Sécurité des Communications dans lesRéseaux de Capteurs sans Fils, Mémoire de Master, UNIVERSITE MOHAMED BOUDIAF - M'SILA, 2018

[5] FEHAM Mohammed, Mise En Place D'un Réseau De Capteurs Sans Fil PourLa Détection Des Feux De Forêt, Programme national de Recherche (2011-2013), Université de Tlemcen, 2013.

[6] Cuppens (Frédéric) ET Miège (Alexandre), Alert correlation in a cooperative intrusion detection framework. In: Proceedings of the IEEE Symposium on Security and Privacy, 2002

[7] NitalMistry, Devesh C Jinwala, and MukeshZaveri. Improving AODV Protocol against Blackhole Attacks.Proceedings of the International Multi Conference of Engineers and Computer Scientists - IMECS 2010, 2, 2010.