REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE IBN KHALDOUN - TIARET

MEMOIRE

Présenté à :

FACULTÉ MATHEMATIQUES ET INFORMATIQUE
DÉPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

MASTER

Spécialité :Réseaux et Télécommunication

Par :

- BOUDAA Noureddine
- GHELLAL Abdellah

Sur le thème

La détection des attaques DoS par la régression logistique dans les réseaux de capteurs sans fil

---

Soutenu publiquement le 28/10/2018 à Tiaret devant le jury composé de :

Mr. BENGHENI ABDELMALEK	Grade	Université MCA	Président
Mr. BEKKAR KHALED	Grade	Université MAA	Encadreur
Mr. BOUALEM ADDA	Grade	Université MAA	Examinateur

Remerciement

Nous remercions en premier lieu ALLAH qui nous a éclairé le chemin du savoiret qui nous a donné la volonté et la patience d'achever ce modeste travail demémoire, notre grand salut sur le premier éducateur notre prophète Mohamed(satisfaction et salut de dieu soit sur lui).
Nous tenons à adresser nos remerciements à nos parents qui ont consenti dessacrifices et prodigué des encouragements tout au long de nos études.
Nous adressons nos vifs remerciements et nos sincères gratitudes à notre Encadreur BEKKAR KHALEDqui nous a fait l'honneur d'avoir la charge d'encadrer notretravail de mémoire avec grande patience pour la confiance qu'il a eue en notreprojet et surtout pour ses orientations ainsi que son aide précieuse et ses conseilspour réaliser cette mémoire.
Nous remercions également notre jury d'avoir accepté de juger notre travail.

En fin, nous tenons à remercier également nos collègues pour leur aide àla réalisation de cette Modeste Mémoire.

Nous tenons à remercier nos professeurs de département d'informatique de nousavoir incités à travailler en mettant à notre disposition leurs expériences et leurcompétence.On n'oublie surtout pas nos parents et nos proches pour leurs contributions, leurs soutiens et leur patience.
Merci à toutes et à tous

Dédicaces

On dédie ce modeste travail :

À nos très chers parents.

À nos frères et sœurs.

Tous nos amis.

Et on remercie tous ceux et celles qui ont contribué à réaliser ce travail.

Résumé.

Les réseaux RCSF sont omniprésents dans divers domaines tels que la sante et le secteur Militaire. Ces réseaux ont plusieurs avantages comme la facilité de déploiement massif de leurs capteurs, la protection et la supervision des applications critiques, et le fonctionnement en continu du réseau à temps réel.

Cependant, les attaques de dénis de service, peuvent avoir des impacts négatifs sur les applications critiques des réseaux RCSF, minimisant ainsi la sécurité au sein de ces réseaux. Donc, il est important de sécuriser ces réseaux afin de maintenir leur efficacité. Et, comme les nœuds capteurs sont incapables de traiter leur sécurité d'une manière autonome, une approche globale de la sécurité contre les attaques devient indispensable.

Les attaques dans les réseaux RCSF, dont les dénis de service font partie, ciblent les informations en circulation. Ces dénis de service se caractérisent par un type d'utilisateur, par un type de service partagé, et par un temps d'attente raisonnable. Plusieurs mécanismes de sécurité de réseaux RCSF sont utilisés afin de contrer les effets des dénis de service.

Notre étude s'intéresse spécifiquement sur la détection d'attaque DoS. Parmi les solutions proposées, nous trouvons les (IDS) basés sur la technique d'apprentissage automatique qui ont prouvés leur efficacité.

Dans notre travail, nous avons utilisé cette solution avec le classificateur de **la régression logistique.** Nombreux scénarios de simulation contenant plusieurs cibles de comportements (Normal, Blackhole, Hello-Flood, et DoS) ont été testés, et les résultats obtenus sont intéressants et nous permettent de tirer diverses conclusions.

Mots clés: Réseaux de capteurs sans fil (RCSF), Sécurité de RCSF, Système de détection d'intrusion (IDS), Denis de service (Dos), la régression logistique.

Sommaire

Table des matières

Chapitre 2 : Sécurité et détection d'intrusion

Chapitre 3 : IDS basé sur l'apprentissage pour RCSF par logistique regression

Liste des figures

Liste des tableaux

Liste des abreviations

ABIDS : Détection d'Intrusion basée sur une application .

AODV : pour Ad hoc On Demand Distance Vector.

DOS :Deni de Service.

DSN :DistributedSensor Network.

DSR :Dynamic Source Routing.

FIFO :premier entré, premier sorti.

HIDS : Les systèmes de détection d'intrusion basés sur l'hôte.

IDS : système de détection d'intrusions.

IP : protocole internet.

NIDS : La Détection d'Intrusion Réseau.

RC : Rayon de Communication.

RS : Rayon de Sensation.

RREP : Le message de réponse à la demande de route.

RREQ : message de demande de route.

RTP : protocole de communication informatique permettant le transport de données.

TCP : protocole de contrôle de transmissions.

UDP : protocole de datagramme utilisateur.

RCSF : réseau de capteurs sans fil.

WSN : Wireless Sensor Network.

Introduction Générale

Introduction Générale

Le besoin effréné d'informations et l'évolution rapide de la micro-électronique et des technologies sans fil ont permis la création de petits appareils électroniques avec un coût très réduit (ressources limitées), capables de collecter et de traiter l'information de manière autonome et flexible. Ces appareils peuvent être interconnectés et déployés à grande échelle, donnant naissance à un nouveau type de réseaux nommé réseau de capteurs sans fil (RCSF). Le développement des RCSFs était originalement motivé par les applications militaires (surveillance des champs de bataille, localisation de l'ennemie…). Néanmoins, leurs performances remarquables en termes de fiabilité et de faible coût ont permis de proliférer leur utilisation dans le domaine d'application civil (surveillance d'environnement, l'industrie, la domotique, la santé…).

Les réseaux de capteurs sans fil sont conçus pour fonctionner en groupe et coopérer afin de transmettre les données collectées à un point central appelé station de base ou sink. Chaque noeud capteur est équipé d'un microprocesseur à faible puissance de calcul, d'une petite batterie, d'une antenne radio et d'un ou plusieurs capteurs. Ainsi, les RCSFs doivent opérer en prenant toujours en compte leur limitation de ressources. Ces derniers sont le plus souvent déployés aléatoirement dans des zones hostiles et inexplorées, et doivent s'auto-organiser à l'aide des communications sans fil. La station de base est le seul lien avec le monde extérieur et dispose de plus de ressources par rapport aux nœuds capteurs. Le réseau de capteurs joue le rôle d'un pont entre le monde physique et le système informatique, en fournissant des mesures et des propriétés physiques du monde réel.

La sécurité représente un défi majeur très important pour les RCSFs, étant donné que des décisions stratégiques peuvent être prises en se basant sur les informations reçues par les nœuds capteurs. Comme la plupart des réseaux distribués, les RCSFs sont exposés aux menaces de sécurité. En outre, leurs caractéristiques spéciales les rendent très vulnérables aux attaques malicieuses. En effet, les RCSFs sont généralement déployés dans des zones inconnues sans aucune protection physique, ce qui facilite leur capture et compromission. De plus, l'environnement de communication sans fil permet d'écouter et d'espionner le trafic échangé dans le réseau, ce qui ouvre l'horizon pour lancer plusieurs types d'attaques. De l'autre côté, la limitation des ressources des nœuds capteurs rend inappropriée l'application des solutions de sécurité classiques. Ainsi, en plus d'offrir un bon niveau de sécurité, les protocoles de sécurité dédiés aux RCSFs doivent respecter les contraintes de ressources de ces derniers. Par conséquent, il est nécessaire d'utiliser des mécanismes efficaces pour protéger ce type de réseau.

Toutefois il est bien connu, que les systèmes de détection d'intrusion (IDSs) sont des mécanismes de sécurité très efficaces pour protéger le réseau contre les attaques malveillantes ou l'accès non autorisé, contrairement à d'autres mécanismes telle que la cryptographie qui reste inefficace lorsque l'attaquant se trouve à l'intérieur du réseau. Par ailleurs, les techniques de

détection d'intrusion doivent être conçues pour détecter et prévenir l'exécution des attaques les plus dangereuses.

Les IDS sont classés en trois catégories en fonction de leur méthodologie de détection: méthode basée sur l'abus, basée sur la spécification et basée sur l'anomalie [1]. Ce dernier a plusieurs techniques de détection : basée sur la connaissance, basée sur l'apprentissage automatique, et la détection basée sur la statistique. Ce système de détection présente un avantage par rapport au précèdent il détecte les nouveaux types d'attaques. Cependant il faudra faire parfois des ajustements afin que le fonctionnement de référence corresponde au mieux à l'activité normale des utilisateurs et ainsi réduire les fausses alertes qui en découleraient.

Notre problématique et de détecter des attaques dénis de service à travers un IDS basé sur techniques d'apprentissage automatique qui a prouvé son efficacité et en utilisant l'algorithme de classificateur de la régression logistique. Notre objectif est de construire un système d'apprentissage automatique pour détecter les attaques DoS tout en variant plusieurs fonctionnalités pour obtenir le moyen de protection le plus efficace. Notre étude repose sur des simulations en utilisant différents scenarios en comportement normal et malveillant afin de tirer profit des résultats obtenus.

Ce mémoire est organisé en trois chapitres en plus d'une introduction et d'une conclusion générales :

✓ **Dans le premier chapitre** : sur les concepts généraux des réseaux de capteurs sans fil (RCSF), nous essayons de donner une vue générale sur la notion de capteurs, de réseaux de capteurs sans fil, des contraintes dans la conception d'un réseau de capteurs ainsi que des divers domaines qui les utilisent.

✓ **Dans le deuxième chapitre**, nous présentons les techniques de détection d'intrusion et leurs approches et les différentes sortes d'IDS. Aussi, nous décrivons les attaques les plus communs dans les RCSF.

✓ **Dans le troisième chapitre**, nous expliquons notre approche et les outils sur lesquels nous avons basés pour construire notre système IDS. Des expériences et les commentaires associés aux résultats obtenus ont été aussi présentés dans ce chapitre.

Chapitre I

Présentation des réseaux de captures sans fil

Chapitre1 : Présentation des réseaux de captures sans fil

1.1. Introduction

Les avancées récentes en technologie des systèmes micro-électromécanique, des communications sans fil, et de l'électronique numérique ont permis le développement de nœuds capteurs peu coûteux, multifonctionnels et de basse puissance. Ces capteurs sont petits par la taille et communiquent sur des courtes distances. Ces nœuds capteurs minuscules, sont constitués de composants de capture, de traitement de données et de communications. Ils ont influencé l'idée des réseaux de capteurs basés sur la collaboration d'un grand nombre de nœuds. Chaque nœud est un dispositif électronique qui possède une capacité de calcul, de stockage, de communication et d'énergie. Chaque capteur est doté d'un module d'acquisition qui lui permet de mesurer des informations environnementales : température, pression, accélération, sons, image, vidéo etc... **[2]**

L'étendue des applications des réseaux de capteurs est vaste, on les retrouve dans le domaine de la santé, de la sécurité et dans le secteur militaire. Les réseaux de capteurs permettent à l'utilisateur une meilleure compréhension de l'environnement. De nos jours, les réseaux de capteurs sans fils font partie intégrante de notre vie.

1.2. Les réseaux de capteurs sans fil ($RCSF_S$)

Les réseaux de capteurs sans fil sont considérés comme un type spécial des réseaux ad-hoc où l'infrastructure fixe de communication et l'administration centralisée sont absentes et les nœuds jouent, à la fois, le rôle des hôtes et des routeurs (**figure 1.1**). Les nœuds capteurs sont des capteurs intelligents "smart sensors", capables d'accomplir trois taches complémentaires : le relevé d'une grandeur physique, le traitement éventuel de cette information et la communication avec d'autres capteurs. L'ensemble de ces capteurs, déployés pour une application, forme un réseau de capteurs. Le but de celui-ci est de surveiller une zone géographique, et parfois d'agir sur celle-ci (il s'agit alors de réseaux de capteurs actionneurs) **[3]**.

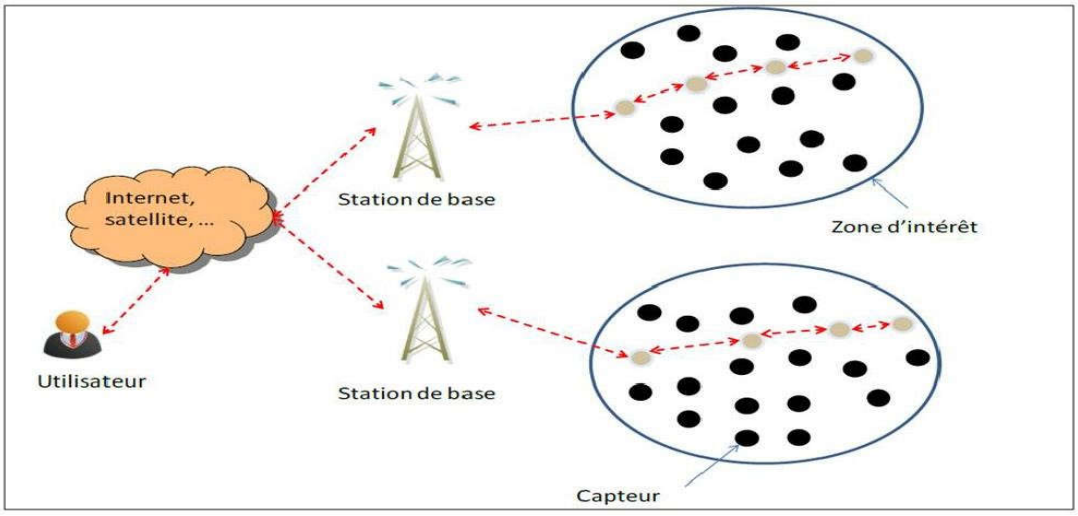


Figure 1.1 - Schéma général d'un réseau de capteurs.

1.2.1. Les capteurs

Un capteur est un petit appareil autonome capable d'effectuer des mesures simples sur son environnement immédiat. La tendance actuelle en termes d'utilisation de ces capteurs, c'est leur possibilité à communiquer de manière radio (réseaux sans-fil de type Wifi) avec d'autres capteurs proches (quelques mètres). On peut ainsi constituer un réseau de capteurs qui collaborent sur une étendue assez vaste.

Comme les ressources d'un capteur sont très limitées, on peut même envisager que la réalisation d'un service complexe puisse être effectuée grâce à une composition de services plus simples et donc à une forme de collaboration « intelligente » des capteurs **[4]**.

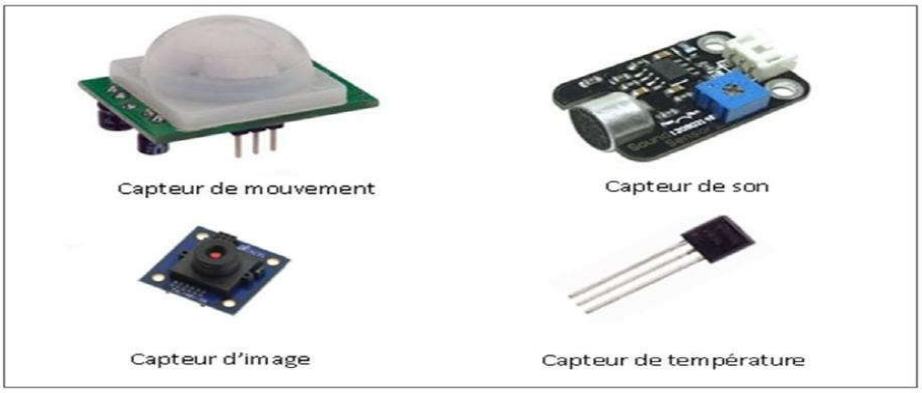


Figure 1.2 - Exemple des modèles de capteurs.

1.2.2. Classification des capteurs

1.2.2.1 Capteurs passifs

Ils n'ont pas besoin d'apport d'énergie extérieure pour fonctionner (exemple : thermistance, potentiomètre, thermomètre à mercure...). Ce sont des capteurs modélisables par une impédance. Une variation du phénomène physique étudié (mesuré) engendre une variation de l'impédance.

1.3.2.1 Capteurs actifs

Ils sont constitués d'un ensemble de transducteurs (chronomètre mécanique, jauge d'extensomètre et gyromètre...). Ce sont des capteurs que l'on pourrait modéliser par des générateurs comme les systèmes photovoltaïques et électromagnétiques. Ainsi ils génèrent soit un courant, soit une tension en fonction de l'intensité du phénomène physique mesuré [5].

1.2.3. Les nœuds capteur

C'est l'acteur principal d'un **WSN (Wireless Sensor Network)**, il se caractérise par une taille réduite et un coût faible avec des ressources limitées en termes d'énergie. Leur type, leur architecture et leur disposition géographique dépendent de l'exigence de l'application en question. Il permet de capter les informations par l'unité d'acquisition, de les traiter au niveau de

l'unité de traitement puis de les envoyer vers le puits (sink), via l'interface de communication sans fil Radio.

Un nœud capteur est caractérisé par une zone de captage qui est une zone de couverture des phénomènes et une zone de communication.

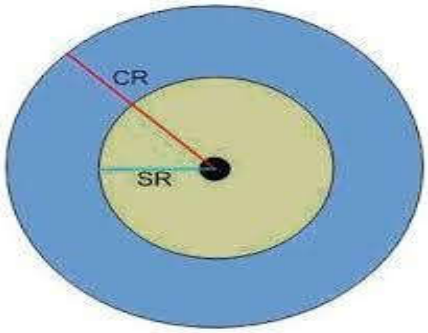


Figure 1.3 - Zone de Captage pour un nœud capteur.

1.2.4. Le collecteur (puits ou sink)

C'est un capteur particulier qui permet la collecte d'information depuis les nœuds capteurs et l'envoyer vers des utilisateurs, qui sont connectés avec le sink via un réseau internet ou satellite. Il y a essentiellement trois types de sink :

A Un nœud appartenant au réseau comme n'importe quel autre nœud.

B Le sink peut être un dispositif extérieur au réseau, par exemple, un ordinateur portatif .

C Une passerelle vers un autre réseau tel qu'internet, ou la demande de l'information vient d'un certain centre de traitement lointain.

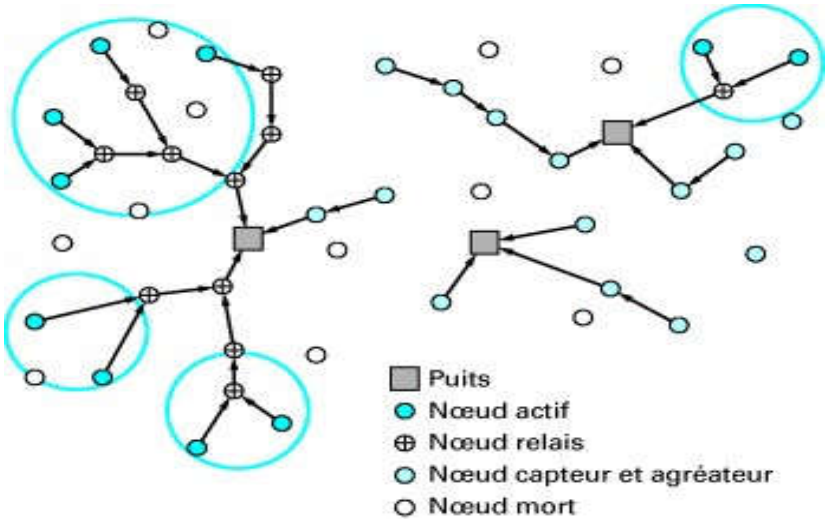


Figure 1.4 -Exemple de réseau de capteurs.

1.3. Les domaines d'application des réseaux de capteurs sans fil

Les réseaux de capteurs sans fil sont utilisés dans une variété d'applications telles que la surveillance militaire, le domaine médical, des applications commerciales et des applications environnementales, ...

- **Surveillance militaire**. L'utilisation des capteurs dans le domaine militaire est en pleine expansion, ces dispositifs peuvent être utilisés dans les opérations de surveillance des champs de bataille, la détection d'intrusion et reconnaissances des forces amies et ennemies. Parmi les travaux concrétisés dans ce domaine, nous pouvons citer les projets phares suivants: le projet DSN (DistributedSensorNetwork)**[6]** développé par la DARPA (Défence Advanced ResearchProjects Agency), le projet WATS (Wide Area Tracking System) pour la détection des dispositifs nucléaires développés par le laboratoire Lawrence Livermore National **[7]**.
- **Applications médicales**. Dans le domaine médical; les capteurs sont utilisés pour la surveillance des données physiologiques d'un patient. A titre d'exemple, la référence [8] propose une nouvelle plateforme pour la surveillance des personnes cardiaques en utilisant les capteurs pour la collecte des données ECG (la durée QRS, la durée entre deux piques R, l'amplitude du pique R) et le téléphone mobile pour la détection des pathologies cardiaques.

- **Applications environnementales**. Les capteurs sont récemment utilisés dans le domaine de l'agriculture. La fonction des capteurs dans ce domaine consiste à surveiller les taux de pesticides dans l'eau potable, le degré d'érosion, et le niveau de pollution de l'air en temps réel **[9]**.
- **Applications commerciales**. Dans les entreprises, les réseaux de capteurs permettent de suivre le procédé de production à partir des matières premières jusqu'au produit final livré **[10]**. Grâce aux réseaux de capteurs, les entreprises peuvent offrir une meilleure qualité de service tout en réduisant les coûts **[11][12]**.

1.4. L'architecture d'un nœud capteur

1.4.1. Architecture matérielle

La principale tâche d'un nœud capteur dans un **RCSF** est de détecter, traiter et transmettre des données. Un nœud capteur est un ensemble de quatre composants essentiels qui sont:

➢ **Unité de captage « d'acquisition »** : elle est composée d'un dispositif de capteur physique qui mesure l'information de l'environnement : température, pression, image…etc. et un convertisseur analogique/numérique (CAN) qui convertisse les signaux produits lors de capteur afin de les transmettre à l'unité de traitement.

➢ **Unité de traitement** : elle est composée d'un processeur avec une petite unité de stockage **RAM** pour les données et une **ROM** pour les programmes et souvent une mémoire flash. Elle acquiert les informations en provenance de l'unité d'acquisition et les stocke en mémoire ou les envoie à l'unité de transmission.

➢ **Unité de communication** : Elle est responsable de toutes les transmissions et les émissions des données, elle est munie d'un module radio émetteur / récepteur qui permet d'échanger l'information.

➢ **Unité d'énergie** : les capteurs sont équipés d'une batterie de taille minuscule (des fois, une pile). Cette batterie est responsable de l'alimentation de tous les composants du capteur. Le problème est que cette unité n'est ni rechargeable et souvent irremplaçable ce qui limite la durée de vie du capteur.

Il existe des applications dont les besoins nécessitent d'autres composants qui s'ajoutent à ceux décrits précédemment, comme:

- Le système de localisation pour déterminer la position des nœuds.
- Le mobilisateur pour déplacer un nœud d'un lieu à un autre.

Le schéma suivant illustre l'architecture matérielle d'un nœud capteur

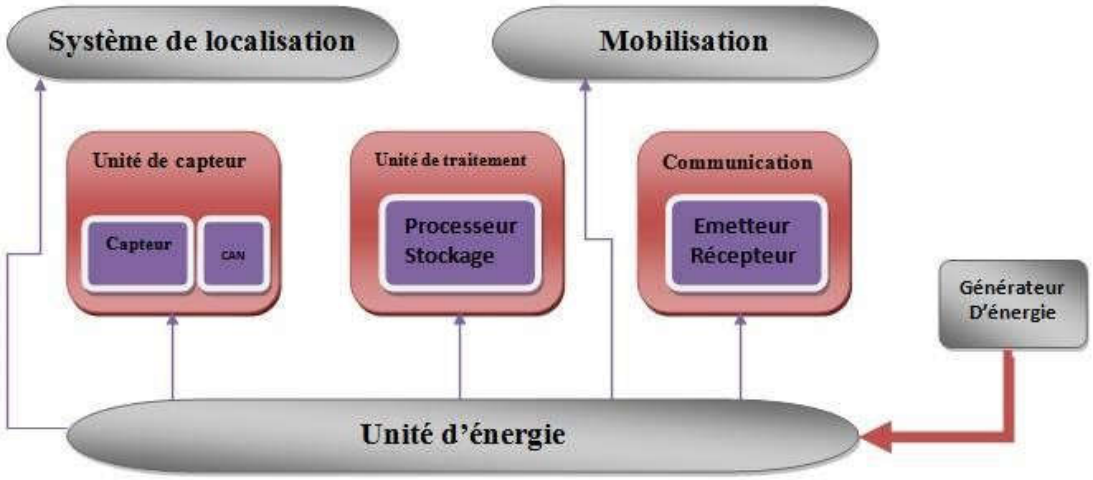


Figure 1.5 - L'architecture matérielle d'un nœud capteur.

1.4.2. Architecture logicielle

L'un des systèmes d'exploitation les plus connus dans le domaine des RCSF est « **TinyOS** ». Il est libre et est utilisé par une large communauté de scientifiques dans des simulations pour le développement et le test des algorithmes et protocoles réseau **[13]**.

1.4.3. Architecture d'un réseau de capteurs

Les principales topologies de réseau qui s'appliquent aux réseaux de capteurs sans fil sont décrites dans cette section.

- **Réseau étoile (Point-à-Multipoint)**

Un réseau en étoile, comme illustré dans **la figure 1.6** est une topologie de communications où une station de base peut envoyer et/ou recevoir un message à un certain nombre de nœuds distants. Les nœuds distants peuvent seulement envoyer ou recevoir un message de la station de base, ils ne sont pas autorisés à envoyer des messages entre eux. L'avantage de ce type de réseau pour les réseaux de capteurs sans fil est sa simplicité ainsi que la capacité des nœuds capteurs de maintenir une consommation minimale d'énergie. Cette topologie assure également une basse latence de communication entre le nœud capteur et la station de base. L'inconvénient d'un tel réseau est que la station de base doit être dans la portée de transmission par radio de tous les différents nœuds. Ce qui, malheureusement, diminue la robustesse en raison de la dépendance du réseau à un nœud simple pour contrôler l'ensemble.

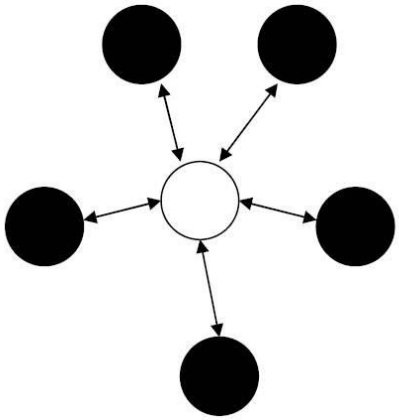


Figure 1.6 -la topologie étoile des réseaux.

- **Le réseau maillé :**

Un réseau maillé comme il est montré dans **la figure 1.7** est un réseau ou n'importe quel nœud peut transmettre à n'importe quel autre à condition qu'il se situe dans sa portée de transmission par radio. Ceci nous conduit aux communications multi sauts, c'est-à-dire, que si un nœud veut envoyer un message à un autre hors de sa portée de communication par radio, il peut utiliser des nœuds intermédiaires pour expédier ce message au nœud désiré. Cette topologie de réseau a l'avantage de la redondance et de la sociabilité. Si un nœud est détruit, un nœud peut encore communiquer à n'importe quel autre nœud dans sa portée, ce dernier qui peut expédier le message à l'endroit désiré.

L'inconvénient de ce type de réseau réside dans sa grande consommation d'énergie essentiellement par les nœuds qui implémentent la communication multi sauts par apport aux nœuds qui n'ont pas cette possibilité et qui limite souvent la durée de vie des batteries. Un autre inconvénient est l'augmentation du temps de réponse.

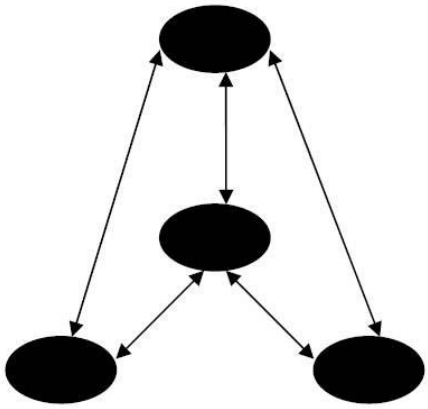


Figure 1.7-la topologie maillée des réseaux.

1.4.4. Architecture de communication d'un RCSF

Les nœuds capteurs sont habituellement dispersés dans une zone de capture. Chacun de ces nœuds a la possibilité de collectées les données et de les router vers une ou plusieurs stations de base (sinknodes). Ce dernier est un point de collecte de données capturées. Il peut communiquer les données collectées à l'utilisateur final à travers un réseau de communication, éventuellement l'Internet. L'utilisateur peut à son tour utiliser la station de base comme passerelle, afin de transmettre ses requêtes au réseau (**figure 1.8**).

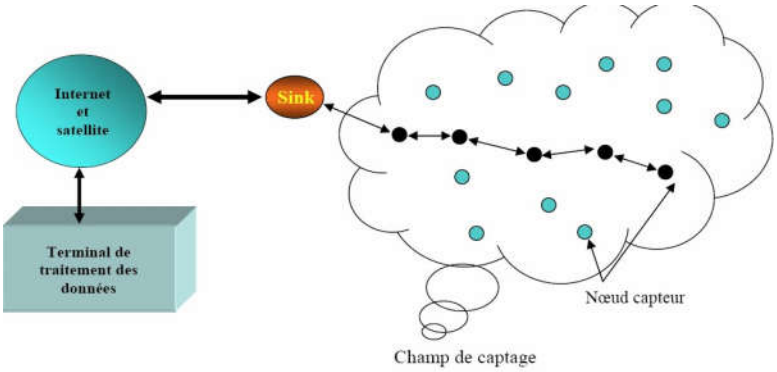


Figure 1.8-Architecture de communication d'un RCSF.

1.4.5. Architecture protocolaire

Un RCSF est une série de connexions entre les capteurs leur permettant de communiquer. Le contenu, la portée, la taille, la vitesse et la fiabilité du réseau dépend d'un ensemble de protocoles et de leur implémentation. Les protocoles sont un moyen de communication prédéterminé. Conceptuellement, il est utile de représenter l'ensemble de ces protocoles sous forme d'une pile, c'est ce qu'on appelle la pile protocolaire. La pile protocolaire **[14]** utilisée par la station de base, ainsi que tous les autres capteurs du réseau, est illustrée dans **la figure 1.9.**Elle comprend la couche application, la couche transport, la couche réseau, la couche liaison de données, la couche physique, le plan de gestion de l'énergie, le plan de gestion de la mobilité et le plan de gestion des taches.

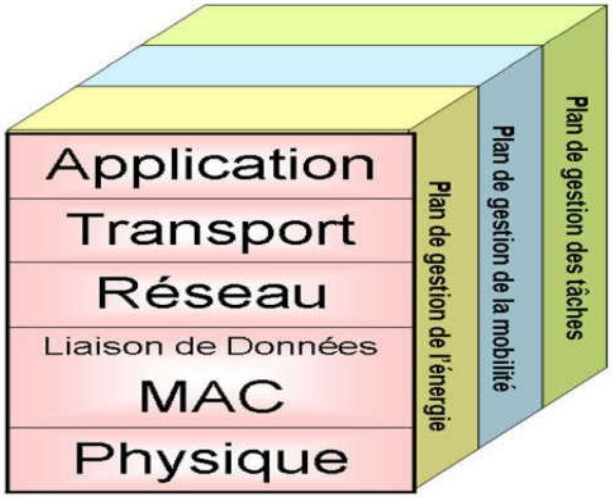


Figure 1.9-La pile protocolaire des réseaux de capteurs.

- **La couche physique** : La couche physique est responsable de :
  - ❖ La sélection des fréquences porteuses.
  - ❖ La détection du signal.
  - ❖ La modulation.
- **La couche liaison de données**

En générale, cette couche est responsable du multiplexage du flux de données, de la détection et le verrouillage des trames de données, du contrôle d'accès aux média (MAC: Media

Access Control), et du control des erreurs. Elle assure une connexion fiable (point-à-point ou point-à-multipoints) selon la topologie du réseau de capteurs.

- **La couche réseau**

Le but principal de la couche réseau est de trouver une route et une transmission fiable des données, captées, des nœuds capteurs vers le puits en optimisant l'utilisation de l'énergie des capteurs. Les caractéristiques spécifiques aux RCSFs exigent que leurs protocoles de routage diffèrent de ceux des réseaux ad hoc traditionnels.

- **La couche transport**

Cette couche est chargée du transport des données, de leur découpage en paquets, du contrôle de flux, de la conservation de l'ordre des paquets et de la gestion des éventuelles erreurs de transmission.

- **La couche application**

Elle constitue l'ensemble des applications implémentées sur un réseau de capteurs. Ces applications doivent fournir des mécanismes permettant à l'utilisateur d'interagir avec le réseau de capteurs à travers différentes interfaces, et éventuellement, l'intermédiaire d'un réseau étendu (par exemple ; Internet). Il s'agit donc du niveau le plus proche des utilisateurs, géré directement par les logiciels.

Quant aux niveaux (plans) intégrés dans la pile protocolaire, ils ont les fonctions suivantes :

- **Le plan de gestion d'énergie**

Un nœud de capteur sans fil, nécessite seulement une source d'énergie limitée (< 0.5Ah, 1.2 V). La vie du nœud montre, une dépendance forte à l'égard de la vie de la batterie. Le plan de gestion d'énergie doit gérer la manière dont les nœuds utilisent leurs énergies. Par exemple, le nœud doit se mettre en sommeil après la réception d'un message à partir d'un voisin afin d'éviter la duplication des messages déjà reçus.

- **Le plan de gestion de mobilité**

Puisque les nœuds peuvent être mobiles, un système de gestion de mobilité doit exister. Un tel système doit être capable d'enregistrer les mouvements du nœud afin de l'aider à se localiser.

- **Plan de gestion de tâche**

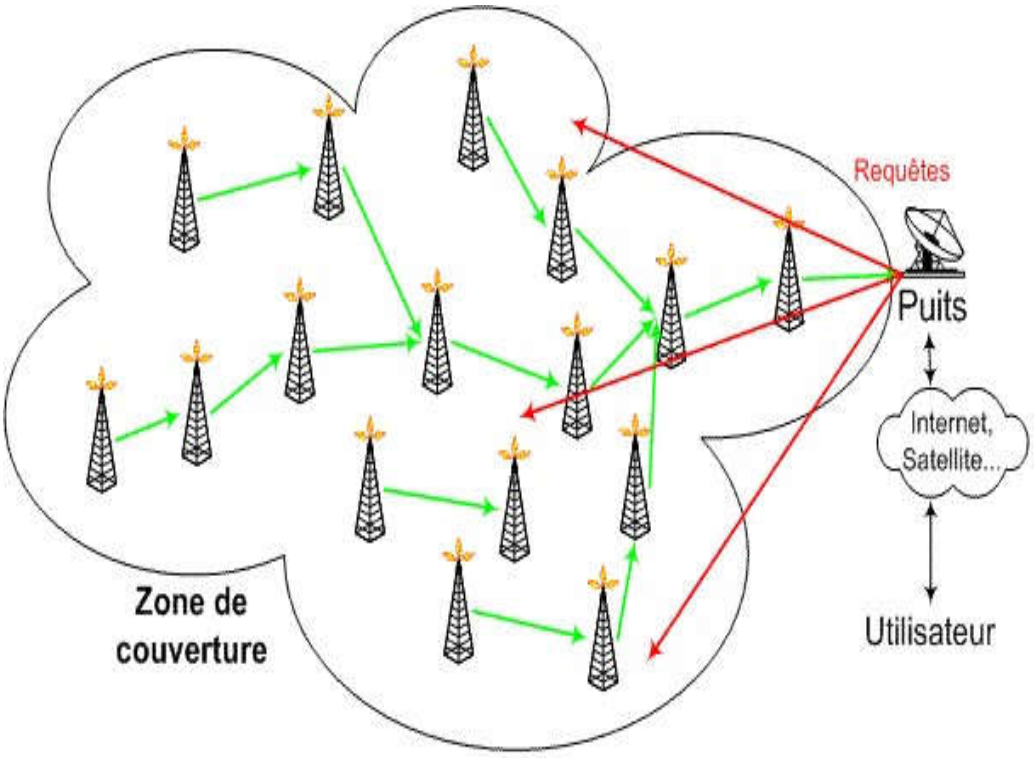
Lors d'une opération de captage dans une région donnée, les nœuds composant le réseau ne doivent pas obligatoirement travailler avec le même rythme, cela dépend essentiellement de la nature du capteur, son niveau d'énergie et la région dans laquelle il a été déployé. Pour cela, le niveau de gestion des tâches assure l'équilibrage et la distribution des tâches sur les différents nœuds du réseau, afin d'assurer un travail coopératif et efficace en matière de consommation d'énergie, et par conséquent, prolonger la durée de vie du réseau.

1.5. Collection des informations

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

A) A la demande

Lorsque l'on souhaite avoir l'état de la zone de couverture à un moment t, le puits émet des broadcasts vers toute la zone pour que les capteurs remontent leur dernier relevé vers le puits. Les informations sont alors acheminées par le biais d'une communication multi-sauts **(figure 1.10).**



b) Suite à un événement

Un événement se produit en un point de la zone de couverture (changement brusque de température, mouvement...), les capteurs situés à proximité remontent alors les informations relevées et les acheminent jusqu'au puits comme ils sont indiqués sur **la figure 1.11**.

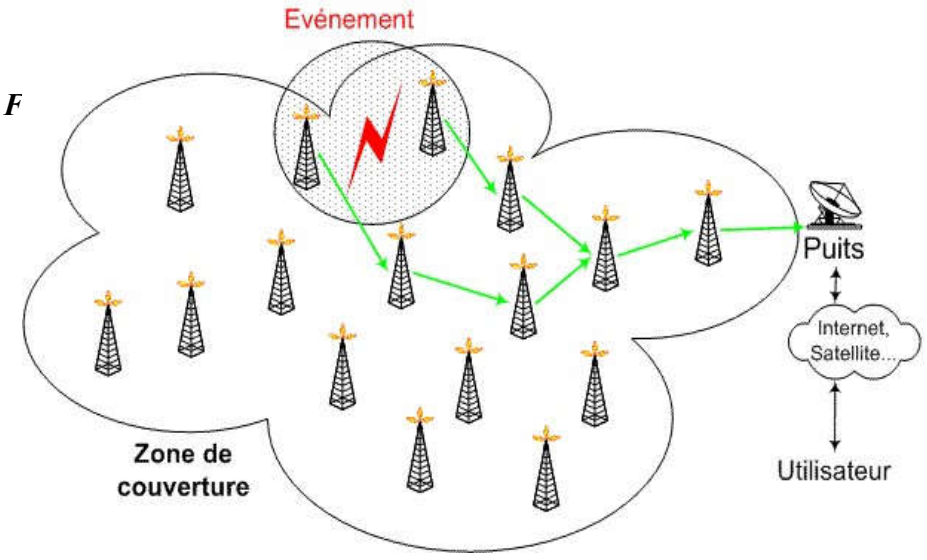


Figure 1.10-Collection des informations à la demande.

1.6. Contraintes dans la conception d'un réseau de capteurs

Les réseaux de capteurs diffèrent des réseaux classiques où l'on peut être relativement générique et définir seulement un certain nombre de classes de service pour satisfaire le maximum de besoins. Ici, les contraintes sont plus nombreuses et empêchent la création d'un type spécifique du réseau de capteurs. Sans être exhaustif, voici une liste de contraintes possibles lors de la conception d'un réseau de capteurs.

1.6.1. Contraintes liées à l'application

Il est impossible aujourd'hui de créer un réseau de capteurs capable de répondre aux besoins de toutes les applications potentielles. On peut relever des mesures pour une infinité de situations et dans des environnements très variables tout en ayant une concentration faible ou forte des capteurs. Dans certains cas, il existe des applications qui nécessitent un grand nombre de capteurs pour être mises en place. La difficulté réside alors dans la recherche d'un dénominateur commun à toutes ces applications ce qui est pour l'instant très complexe et relève de l'impossible. C'est pourquoi, l'application devient le principal paramètre lors de la conception de protocoles très spécifiques pour que le fonctionnement des capteurs produise le résultat attendu par l'application en question.

1.6.2. Contraintes énergétique

L'énergie est considérée comme la contrainte principale dans un réseau de capteurs. Déjà comme pour tout réseau sans fil, il est important de tenir compte de cette contrainte car la plupart des machines fonctionnent sur batterie. Après la décharge de la batterie, l'utilisateur est obligé de trouver une source électrique pour la recharger.

Cependant, dans les réseaux de capteurs, il est pratiquement impossible de recharger de par le nombre élevé de capteurs déployés et de par la difficulté de l'environnement dans lesquels ils peuvent se trouver. On parle alors pour la pile ou la batterie d'âme du capteur. Une fois vide, le capteur est considéré comme mort ou hors service. L'objectif à atteindre devient l'augmentation de la durée de vie du réseau de capteurs. Ce paramètre peut être défini sous différentes formes telles que la consommation globale de tous les capteurs ou l'évitement qu'un capteur important perde son énergie ou la perte de la connectivité du réseau.

1.6.3. Contraintes liées aux déterminismes

La plupart des réseaux de capteurs sont destinés à être déployés dans des environnements hostiles sur des sites industriels importants ou à opérer pendant des scénarios de crises. L'information que le capteur mesure doit parfois atteindre le collecteur d'informations en un temps borné bien défini. Au-delà de ce temps, l'information est considérée comme périmée ou non existante. Atteindre le déterminisme sur un réseau de capteurs sans fil n'est pas une tâche évidente. La raison vient du fait que pratiquement tous les standards de communication sans fil aujourd'hui utilisent des méthodes probabilistes pour accéder à cette interface radio.

1.6.4. Contraintes de passage à l'échelle

Le passage à l'échelle (scalability) indique que le réseau est suffisamment large et peut croître de manière illimitée. En d'autres termes, quand on passe à l'échelle, il est trop tard pour effectuer des mises à jour radicales au réseau. À chaque nouvel ajout, on doit prendre en considération les services existants et assurer leur pérennité. De plus, gérer un grand réseau par des humains devient une tâche difficile voire impossible à réaliser. Pour pouvoir opérer quand on passe à l'échelle, il faut que les capteurs soient capables de s'auto-configurer seuls. L'auto-configuration peut aller de la simple attribution d'un identifiant jusqu'à l'application du protocole pour le bon fonctionnement du nœud dans son environnement. L'algorithmique distribué est la science la plus adaptée pour résoudre les problèmes du passage à l'échelle.

1.6.5. Contraintes liées à la qualité de service

La notion de qualité de service est légèrement différente ici de celle déployée dans les réseaux classiques. Souvent on parle de haut débit ou de faible débit, etc. Ici, avec des petits débits on peut parfois atteindre la qualité exigée. La qualité se définit par la capacité d'interpréter l'information collectée par le puits. Il n'existe donc pas de définition objective de la qualité. En fonction du réseau et du type de mesure, la qualité est alors précisée.

1.6.6. Contraintes liées à la protection de l'information

Comme pour tout réseau sans fil, l'information circule sur une interface partagée et non dédiée. N'importe quel intrus peut alors soit récupérer l'information, soit la modifier ou la rendre

inexploitable. C'est pourquoi des mesures de sécurité doivent être mise en place pour protéger l'information. Cependant, tous les mécanismes de sécurité sont créés pour des réseaux où les nœuds disposent d'une forte capacité de traitement, ce qui n'est pas le cas des capteurs. À ce jour, très peu de solutions sont adaptées aux capteurs en termes de sécurité.

1.6.7. Contraintes liées à l'environnement

Les capteurs interagissent avec l'environnement où ils mesurent leurs grandeurs physiques. De façon générale, ces mesures sont relevées à des instants relativement espacés dans le temps puis soudainement, soit pour des raisons de catastrophe ou d'événement exceptionnel, ils se mettent en mode de forte fréquence de mesures et envoient de l'information en rafale. Il faut alors préparer le réseau à supporter ce type d'événement rare mais largement consommateur de ressources et sujet à des situations de congestions et de difficultés majeures.

1.6.8. Contraintes de simplicité

Enfin proposer des protocoles et des mécanismes simples et légers doit être la marque de fabrique du réseau de capteurs. Ces derniers sont de machines largement plus faibles qu'une machine de bureau ou même que des téléphones portables.

1.7. Conclusion

Actuellement, les applications basées sur les réseaux de capteurs sont une partie intégrante de notre vie. Dans ce chapitre, nous avons présenté les réseaux de capteurs sans fil (RCSF), leurs différentes architectures ainsi que certains de leurs domaines d'application. Cependant, la réalisation des réseaux de capteurs doit effectivement satisfaire de contraintes telles que la tolérance aux fautes, la scalabilité, le coût, le matériel, le changement de topologie, l'environnement et la consommation efficace d'énergie. Puisque ces contraintes sont impérieuses pour les réseaux de capteur, de nouvelles techniques adhoc de gestion de réseaux sans fil sont exigées. Beaucoup de chercheurs s'occupent actuellement à développer les technologies requises pour les différentes couches de la pile de protocoles comme nous allons le constater dans les chapitres suivants.

Chapitre II

Sécurité et détection d’intrusion

2.1. Introduction

Les réseaux de capteurs sans fil sont constitués de nœuds déployés en grand nombre en vue de collecter et transmettre des données environnementales vers un ou plusieurs points de collecte d'une manière autonome. Ces réseaux ont un intérêt particulier pour les applications militaires, environnementales, domotiques, médicales, et bien sûr les applications liées à la surveillance des infrastructures critiques. Ces applications ont souvent besoin d'un niveau de sécurité élevé. Or, de part de leurs caractéristiques (absence d'infrastructure, contrainte d'énergie, topologie dynamique, nombre important de capteurs, sécurité physique limitée, capacité réduite des nœuds), la sécurisation des réseaux de capteurs est à la source, aujourd'hui, de beaucoup de défis scientifiques et techniques.

Toutes ces applications ont des contraintes de sécurité très différentes. Cependant, dans la plupart d'entre elles, l'intégrité et l'authenticité des données doivent être fournies pour s'assurer que des nœuds non-autorisés ne puissent pas injecter des données dans le réseau. Le chiffrement des données est souvent requis pour des applications sensibles telles que les applications militaires ou les applications médicales.

Le présent chapitre à pour objectif de traiter la problématique de la sécurité dans les réseaux de capteurs sans fil.

2.2. Système de détection d'intrusion (IDS)

Un système de détection d'intrusions (IDS, de l'anglais Intrusion Détection System) est un périphérique ou processus actif qui analyse l'activité du système et du réseau pour détecter toute entrée non autorisée et/ou toute activité malveillante. La manière dont un IDS détecte les anomalies peut beaucoup varier.

Les IDS protègent un système contre les attaques, les mauvaises utilisations et les compromis. Ils peuvent également surveiller l'activité du réseau, analyser les configurations du système et du réseau contre toute vulnérabilité, analyser l'intégrité des données **[15]**.

Les figures 2.1 et 2.2 illustrent les systèmes vulnérable et non vulnérable aux attaques.

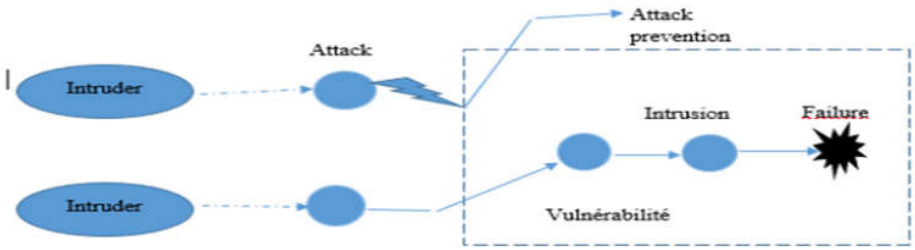


Figure 2.1 -Système vulnérable aux attaques

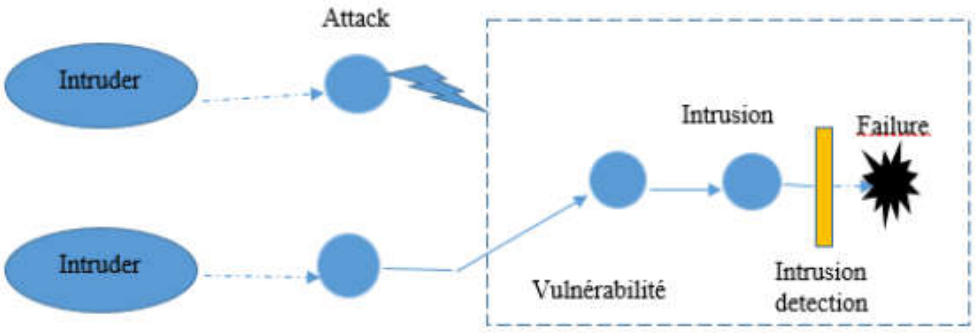


Figure 2.2 -Système non vulnérable aux attaques.

2.3. Approches de détection d'intrusions

La détection d'intrusion peut être définie comme la détection automatique et la génération d'une alarme pour rapporter qu'une intrusion a eu lieu ou est en cours. Parmi les approches de détection d'intrusion utilisées on peut citer :

2.3.1 Approche comportementale (Anomaly Détection)

Le comportement observé du système cible est comparé aux comportements normaux et espérés. Si le comportement du système est significativement différent du comportement normal ou attendu, on dit que le système cible présente des anomalies et fait l'objet d'une intrusion [16]. L'avantage principal de cette approche est de pouvoir détecter de nouvelles attaques. Cependant, elle génère souvent de nombreux faux positifs car une déviation du comportement normal ne correspond pas toujours d'une attaque.

2.3.2 Approche par scenarios (Misuse Détection)

Consiste à modéliser non plus des comportements normaux, mais des comportements interdits. Dans cette approche on analyse les données d'audits à la recherche de scénarios d'attaques prédéfinis dans une base de signatures d'attaque [17]. Le principal avantage d'une approche par scénario est la précision des diagnostics qu'elle fournit par rapport à ceux avancés par l'approche comportementale. Par contre son inconvénient majeur est de ne pouvoir détecter que les attaques enregistrées dans la base de signatures.

2.4. Les différentes sortes d'IDS

Les différents IDS se caractérisent par leur domaine de surveillance. Celui-ci peut se situer au niveau d'un réseau d'entreprise, d'une machine hôte ou d'une application.

2.4.1.La détection d'intrusion basé sur l'hôte

Les systèmes de détection d'intrusion basés sur l'hôte ou HIDS (Host IDS) analysent exclusivement l'information concernant cet hôte. Comme ils n'ont pas à contrôler le trafic du réseau mais "seulement" les activités d'un hôte ils se montrent habituellement plus précis sur les types d'attaques subies.

Ces IDS utilisent deux types de sources pour fournir une information sur l'activité de la machine : les logs et les traces d'audit du système d'exploitation. Chacune des sources a ses avantages : les traces d'audit sont plus précises et détaillées et fournissent une meilleure information ; alors que les logs fournissent l'information essentielle et sont plus petits, mais

certaines attaques peuvent passer inaperçues, alors qu'elles sont détectables par une analyse des traces d'audit.

Les HIDS sont en général placés sur des machines sensibles, susceptibles de subir des attaques et possédant des données sensibles pour l'entreprise. Les serveurs, web et applicatifs, peuvent notamment être protégés par un HIDS. Quelques HIDS connus : Tripwire, WATCH, DragonSquire, Tiger, Security Manager. . .

2.4.2.Détection d'Intrusion basée sur une application

Les IDS basés sur les applications sont un sous-groupe des IDS hôtes. Ils contrôlent l'interaction entre un utilisateur et un programme en ajoutant des fichiers logs afin de fournir de plus amples informations sur les activités d'une application particulière. Un ABIDS (Application Based IDS) se situe au niveau de la communication entre un utilisateur et l'application surveillée.

L'avantage de cet IDS est qu'il lui est possible de détecter et d'empêcher des commandes particulières dont l'utilisateur pourrait se servir avec le programme et de surveiller chaque transaction entre l'utilisateur et l'application. De plus, les données sont décodées dans un contexte connu, leur analyse est donc plus fine et précise.

Par contre, du fait que cet IDS n'agit pas au niveau du noyau, la sécurité assurée est plus faible, notamment en ce qui concerne les attaques de type "Cheval de Troie".

De plus, les fichiers de log générés par ce type d'IDS sont des cibles faciles pour les attaquants et ne sont pas aussi sûrs.

2.4.3. La Détection d'Intrusion Réseau (NIDS)

Le rôle essentiel d'un IDS réseau est l'analyse et l'interprétation des paquets circulant sur ce réseau. L'implantation d'un NIDS (Network IDS) sur un réseau se fait de la façon suivante : des capteurs sont placés aux endroits stratégiques du réseau et génèrent des alertes s'ils détectent une attaque. Ces alertes sont envoyées à une console sécurisée, qui les analyse et les traite éventuellement. Cette console est généralement située sur un réseau isolé, qui relie uniquement les capteurs et la console.

- **Les capteurs**placés sur le réseau en mode furtif (ou stealth mode), de façon à être invisibles aux autres machines. Pour cela, leur carte réseau est configurée en mode "promiscuous", c'est à dire le mode dans lequel la carte réseau lit l'ensemble du trafic, de plus aucune adresse IP n'est configurée. Du fait de leur invisibilité sur le réseau, il est beaucoup plus difficile de les attaquer et de savoir qu'un IDS est utilisé sur ce réseau

- **Emplacement** Il est possible de placer les capteurs à différents endroits, en fonction de ce que l'on souhaite observer. Les capteurs peuvent être placés avant ou après le pare-feu, ou encore dans une zone sensible que l'on veut protéger spécialement. Si les capteurs se trouvent après un pare-feu, il leur est plus facile de dire si le pare-feu a été mal configuré ou de savoir si une attaque est venue par ce pare-feu. Les capteurs placés derrière un pare-feu ont pour mission de détecter les intrusions qui n'ont pas été arrêtées par ce dernier. Il est également possible de placer un capteur à l'extérieur du pare-feu (avant le firewall). L'intérêt de cette position est que le capteur peut ainsi recevoir et analyser l'ensemble du trafic d'Internet. Les capteurs IDSs sont parfois situés à l'entrée des zones du réseau particulièrement sensibles (parcs de serveurs, données confidentielles. . .), de façon à surveiller tout trafic en direction de cette zone.

  Les avantages des NIDSs sont les suivants : les capteurs peuvent être bien sécurisés puisqu'ils se contentent d'observer le trafic et permettent donc une surveillance discrète du réseau. Les NIDSs sont très utilisés et remplissent un rôle indispensable, mais ils présentent néanmoins de nombreuses faiblesses. En effet, la probabilité de faux négatifs (attaques non détectées) est élevée et il est difficile de contrôler le réseau entier. De plus, ils doivent fonctionner de manière cryptée d'où une complication de l'analyse des paquets. Quelques exemples des NIDSs : NetRanger, Dragon, NFR, Snort, ISSReal-Secure. Même si on distingue HIDS et NIDS, la différence devient de plus en plus réduite puisque les HIDS possèdent maintenant les fonctionnalités de base des NIDSs. Des IDSs bien connus comme ISS RealSecure se Nomment aujourd'hui "IDS hôte et réseau".

2.5. Détection d'Intrusion dans les WSN

2.5.1 Architectures des IDS dans les réseaux de capteurs

Les architectures des IDS dans les réseaux ad hoc et les réseaux de capteurs sans fils peuvent être classées en trois catégories [18]:

- ✓ Architecture Autonome (Stand-alone)
- ✓ Architecture Distribué et coopératif (Distributed and Cooperative)
- ✓ Architecture Hiérarchique (Hierarchical).

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

B **Architecture Distribuée et coopérative (Distributed and Cooperative)** : Dans cette architecture chaque nœud exécute son propre IDS mais les IDS's coopèrent afin de créer un mécanisme de détection d'intrusion global.

C **Architecture Hiérarchique (Hierarchical)** : 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-Head du réseau.

2.5.2 Propriétés d'un IDS dans les réseaux de capteurs

Dans les réseaux de capteurs sans fil un système de détection d'intrusion doit satisfaire les propriétés suivantes [19], [20]:

A Audit local (Localizeauditing) Un IDS 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.

B Ressources minimales (Minimizeresources) Un IDS 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 nœuds telles que la bande passante et la puissance sont limitées. La déconnexion peut survenir à tout moment. La communication entre les nœuds pour la détection d'intrusion ne doit donc pas prendre toute la bande passante disponible.

C **Pas de nœud de confiance (Trust no node**) Un IDS dans les réseaux de capteur ne doit faire confiance à aucun nœud car, contrairement aux réseaux filaires, les nœuds capteurs peuvent être compromis facilement.

D **Distribué (Be trulydistributed)** 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.

E **Sécurisé (Be sécure)** un IDS doit être capable de résister aux attaques.

2.6. Vulnérabilités dans un RCSF

Les mécanismes de défense dans un réseau de capteurs ne doivent pas juste tenir en compte de la nature de l'attaque, mais doivent également tenir compte de la nature de l'attaquant et de ses caractéristiques.

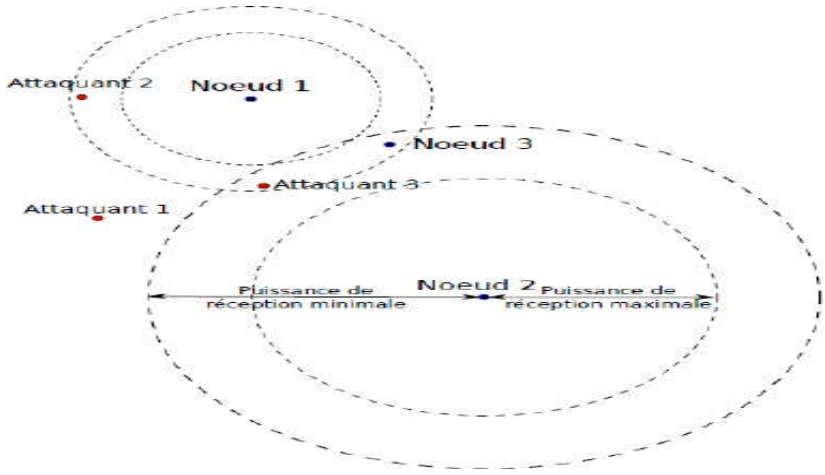
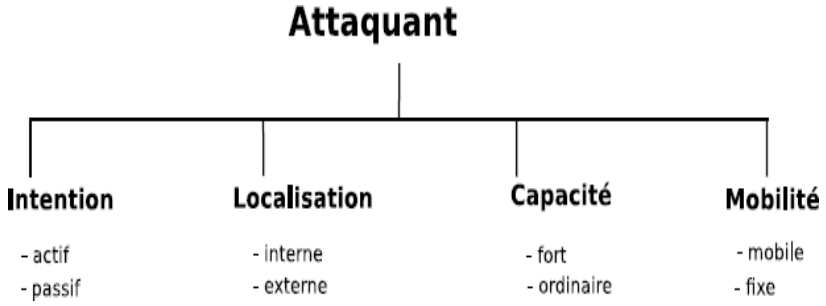


Figure 2.3 -Attaques dans un RCSF

Ainsi, un attaquant peut-être classifié selon son intention, localisation, capacité et sa mobilité **[21].**

Figure 2.4 -Classification des attaquants



Selon son intention :

Attaquant passif *:* ici l'attaquant essaye de collecter des données sur le réseau sans affecter son fonctionnement. Par exemple, une écoute passive des messages sur le canal sans fil.

Attaquant actif *:* ici l'attaquant essaye de détruire le fonctionnement du réseau d'une manière partielle ou bien totale. Plusieurs attaques, qui seront détaillées dans la section.

Selon sa position par rapport au réseau:

Attaquant externe *:* ici l'attaquant est considéré comme un "étranger" par rapport au réseau, il s'agit d'un utilisateur non autorisé qui s'introduit depuis l'extérieur du périmètre de sécurité du réseau.

Attaquant interne *:* ici l'attaquant se manifeste comme une entité légitime du réseau autorisée à accéder aux ressources fournies par le système. L'attaquant est ainsi authentifié et reconnu par l'ensemble des éléments du réseau.

Selon sa capacité :

Attaquant fort *:* ici l'attaquant est équipé d'extra-ressources par rapport à l'ensemble des nœuds présents dans le réseau. Par exemple, un attaquant utilise un PC portable avec un médium radio sophistiqué.

Attaquant ordinaire *:* ici l'attaquant possède les mêmes caractéristiques que les autres nœuds.

Selon sa mobilité *:*

L'attaquant peut être fixe ou mobile: Un attaquant mobile dans un réseau est plus difficile à détecter par rapport à un attaquant fixe.

2.7. Exigences en sécurité

Les applications n'ont pas les mêmes besoins de sécurité, mais en général, les besoins primaires à considérer lors de l'étude de la sécurité dans les RCSFs sont **[22]:**

Authentification : Un nœud doit savoir et vérifier la légitimité du nœud qui essaye d'établir une connexion avec lui. Par conséquent, l'authentification est un mécanisme fondamental pour assurer le contrôle d'accès dans le réseau.

Contrôle d'accès : Il représente est la capacité des nœuds du réseau (ou bien d'une unité centrale comme la station de base) à accorder l'accès approprié aux ressources (connectivité, données,) en fonction d'informations sûres.

Confidentialité : Le canal radio est particulièrement vulnérable à l'écoute clandestine. Par conséquent, la confidentialité des informations échangées est également une condition importante pour assurer la sécurité du réseau.

Intégrité : Comme le canal radio est également fortement vulnérable aux attaques actives, l'intégrité des données doit être convenablement protégée. Le nœud doit s'assurer que le message n'a pas été modifié en cours de route.

Vie privé : Dans un réseau la protection de la vie privée (en anglais privacy) est exigée. Le réseau ne devrait pas indiquer l'endroit des nœuds dans le réseau, ni l'identité des autres nœuds avec lesquels ils communiquent.

Non-répudiation (garantie par la signature numérique) : elle permet d'assurer la source d'un paquet. Ainsi un nœud ne peut pas nier l'envoi d'un paquet dans le passé.

2.8. Défis de la sécurisation des réseaux de capteurs

La sécurisation des réseaux de capteurs reste un problème difficile pour les raisons suivantes [21]:

Capacités limitées : Les ressources de calcul et de mémoire des nœuds sont relativement faibles. L'énergie limitée des capteurs est probablement la caractéristique la plus pénalisante. Le plus grand des défis dans le domaine des réseaux de capteurs reste de concevoir des protocoles, entre autre de sécurité, qui minimisent l'énergie afin de maximiser la durée de vie du réseau. En d'autres mots, l'énergie est sans aucun doute la ressource qui convient de gérer avec la plus grande attention.

2.9. Les attaques dans RCSFs

Les attaques se font sur toutes les couches de communication : sur la couche physique, sur la couche MAC (liaison), sur la couche réseau (routage) et sur la couche application [23].

La figure suivante résume les plus importantes attaques:

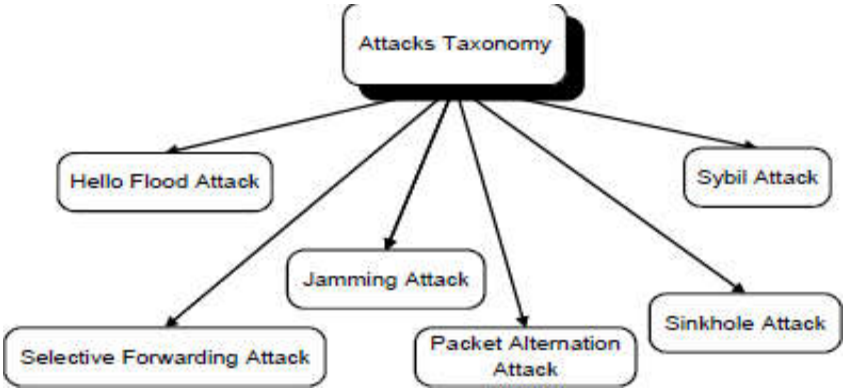


Figure 2.5 -Classification des attaques

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

Tampering : Elle consiste à la capture et à l'accès physique au nœud à fin d'extraire toutes les informations présentes comme les clés de cryptage.

Collision : Elle est comparable au jamming, l'adversaire envoie son signal quand il entend un nœud légitime entrain de transmettre à fin de provoquer des interférences (attaque DoSs).

Expédition sélective : Dans cette attaque, un nœud malveillant agira comme un nœud normal en transférant des messages mais va sélectivement jeter certains.

Sinkhole/ Blackhole : Un nœud peut devenir un trou noir en informant qu'il a le plus court chemin (meilleurs métriques de routage) vers la station de base et ainsi toute l'information lui sera acheminée. Les nœuds victimes le choisiront comme un transitaire pour les paquets et lui peut faire ce qu'il veut avec toutes les informations reçues.

Boucle de routage : La coopération de plusieurs nœuds peut créer une boucle dans le mécanisme de routage entre une source et un nœud destinataire.

Sybille : Dans cette attaque, un nœud malveillant peut prétendre être plusieurs nœuds (identités multiples) légitimes (contrecarrant le processus de collaboration d'une tâche distribuée comme l'agrégation des données ou le vote) ou inexistants (remplir la liste de voisinage des nœuds voisins avec des nœuds inexistants).

Réplication de nœuds : C'est une variante de l'attaque sybille. 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.

Hello flood : Dans cette attaque de type DoS, les paquets sont envoyés pour la découverte d'un voisin. Un dispositif sophistiqué qui utilise un signal radio puissant à longue portée pourrait envoyer des paquets de ce genre et ainsi inonder une partie du réseau tout en provoquant de fausses listes de voisins.

Worm Hole : Dans l'attaque de trou de ver, un nœud compromis enregistre les paquets et les envoie via un lien ou tunnel de faible latence vers un autre nœud malicieux dans le réseau.

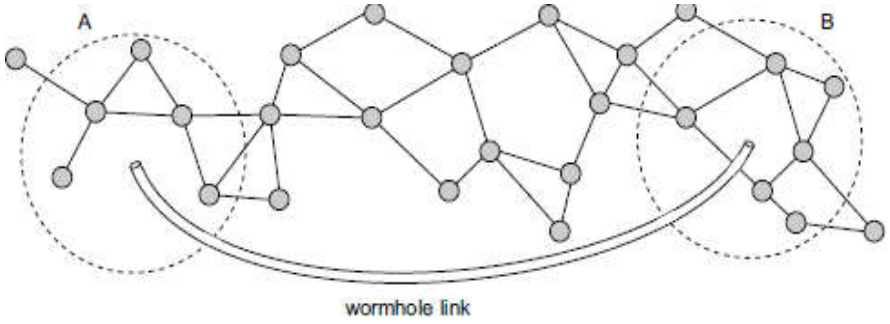


Figure 2.6 - Attaque Worm Hole

ou plusieurs nœuds ou un ordinateur portable. Elle vise à épuiser les ressources limitées (mémoire et énergie) d'un nœud légitime. L'attaquant envoie successivement des demandes de connexions à un nœud légitime jusqu'à ce que ce dernier meure.

Forceddelay : Un nœud malveillant retarde délibérément les paquets à l'intérieur de son élément de transmission à fin de retarder la transmission des événements importants.

Désynchronisation : L'attaque consiste à perturber la communication déjà établie entre deux nœuds en les poussant à rompre leur synchronisation.

2.9.1 Protocoles de routage sécurisés

Le problème du routage consiste à déterminer un acheminement optimal des paquets à travers le réseau au sens d'un certain critère de performance comme la consommation énergétique. Une attaque simple de déni de service sur un protocole de routage consiste pour un nœud à refuser arbitrairement de transférer certains messages ou de supprimer un paquet en transit de façon aléatoire.

Plusieurs propositions ont été faites pour sécuriser différents algorithmes de routage, essentiellement les algorithmes de routage à la demande dans les réseaux ad-hoc ou les réseaux de capteurs. Il est donc nécessaire de sécuriser les protocoles de routage conçus initialement pour

un environnement sans risque ou même de concevoir de nouveaux algorithmes robustes afin de mener à bien l'opération de l'acheminement des données même en présence des nœuds malicieux.

2.10. Conclusion

Les applications basées sur les réseaux sans fil ont besoin d'un niveau de sécurité élevé car ils fournissent des services essentiels, voire vitaux. La sécurité est un domaine très vaste et représente un défi scientifique à cause des caractéristiques spécifiques des réseaux de capteurs.

Dans ce chapitre nous avons présenté les différentes problématiques de la sécurité dans les réseaux de capteurs sans fils. Les IDS comme étant des solutions à certains problèmes de sécurité ont était traité.

Chapitre III

Notre approche : IDS basé sur la régression logistique dans les RCSF

3.1. Introduction

La sécurité est devenue un aspect important à relever dans l'exploitation des réseaux de capteurs sans fil. Cela est particulièrement vrai pour les environnements hostiles et insécurisés.

Dans ce chapitre, nous allons proposer une approche d'un IDS pour RCSF basée sur la régression logistique. Au début, nous créons notre propre jeu de données ; ceci va nous servir à l'étape d'expérimentation. Nous allons justifier tous les choix faits sur le niveau de caractérisation des attaques et les attributs ciblés en utilisent le classificateur de la régression logistique. Ensuite, nous décrivons notre étude expérimentale et ses résultats obtenus.

3.2. Schéma de détection proposé

La méthode de détection est basée sur la classification de la régression logistique, avant la détailler, nous allons expliquer le fonctionnement de ce genre de classificateur.

3.3. La régression logistique

La régression logistique ou modèle logit est un modèle de régression binomiale. Comme pour tous les modèles de régression binomiale, il s'agit de modéliser au mieux un modèle mathématique simple à des observations réelles nombreuses. En d'autres termes d'associer à un vecteur de variables aléatoires {x1,….., x_k } une variable aléatoire binomiale génériquement notée y. La régression logistique constitue un cas particulier de modèle linéaire généralisé. Elle est largement utilisée en apprentissage automatique.

3.2.1 Application

La régression logistique est largement répandue dans de nombreux domaines. On peut citer de façon non exhaustive :

- En médecine, elle permet par exemple de trouver les facteurs qui caractérisent un groupe de sujets malades par rapport à des sujets sains.
- Dans le domaine des assurances, elle permet de cibler une fraction de la clientèle qui sera sensible à une police d'assurance sur tel ou tel risque particulier.
- Dans le domaine bancaire, pour détecter les groupes à risque lors de la souscription d'un crédit.

- En économétrie, pour expliquer une variable discrète. Par exemple, les intentions de vote aux élections.

Par exemple, Vincent Loonis[24] utilise un modèle de régression logistique pour étudier les déterminants de la réélection des députés français depuis les débuts de la IIIe République.

3.2.2 Le modèle

3.3.2.1 Notations

Soit Y la variable à prédire (variable expliquée) et $X=(X_1,X_2,...,X_J)$ les variables prédictives (variables explicatives).

Dans le cadre de la régression logistique binaire, la variable Y prend deux modalités possibles {1,0}. Les variables X_j sont exclusivement continues ou binaires.

- Soit Ω un ensemble de n échantillons, comportant n_1 (resp. n_0) observations correspondant à la modalité 1 (resp. 0) de Y.
- $P(Y=1)$ *(resp.* $P(Y=0)$*)* est la probabilité a priori pour que Y=1 (resp. Y=0). Pour simplifier, cela sera par suite noté $p(1)$ *(resp.* $p(0)$*).*
- $P(X|1)$ *(resp.* $P(X|0)$*)* est la distribution conditionnelle des X sachant la valeur prise Y
- La probabilité a posteriori d'obtenir la modalité 1 de Y *(resp. 0)* sachant la valeur prise par X est notée $p(1|X)$ *(resp.* $p(0|X)$*)*.

3.3.2.1 Hypothèse fondamentale

La régression logistique repose sur l'hypothèse fondamentale suivante, où l'on reconnaît la mesure nommée « évidence » $\mathbf{Ev(p)} = \ln\frac{p}{1-p}$ popularisée par I.J. Good[25], E.T Jaynes[26] et Myron Tribus [27] pour les besoins de l'inférence bayésienne en évitant des renormalisations continuelles sur [0,1] :

$$\ln\frac{p(X|1)}{P(X|0)} = a_0 + a_1x_1 + \ldots + a_jx_j \quad (3.1)$$

Une vaste classe de distributions répondent à cette spécification, la distribution multinormale décrite en analyse discriminante linéaire par exemple, mais également d'autres distributions, notamment celles où les variables explicatives sont booléennes (0/1).

Par rapport à l'analyse discriminante toujours, ce ne sont plus les densités conditionnelles *P(X|1) et P(X|0)* qui sont modélisées mais le rapport de ces densités. La restriction introduite par l'hypothèse est moins forte.

3.3.2.1 Le modèle LOGIT

La spécification ci-dessus peut être écrite de manière différente. On désigne par le terme ***LOGIT*** de *P(1|X)* l'expression suivante

$$\ln\frac{p(1|X)}{1-P(1|X)} = b_0 + b_1x_1b_j+\ldots+x_j \quad (3.2)$$

- Il s'agit bien d'une « régression » car on veut montrer une relation de dépendance entre une variable à expliquer et une série de variables explicatives.
- Il s'agit d'une régression « logistique » car la loi de probabilité est modélisée à partir d'une loi logistique En effet, après transformation de l'équation ci-dessus, nous obtenons.

$$P(1|X) = \frac{e^{b_0+b_1x_1+\ldots+b_jx_j}}{1+e^{b_0+b_1x_1+\ldots+b_jx_j}} \quad (3.3)$$

Remarque : Équivalence des expressions

Nous sommes partis de deux expressions différentes pour aboutir au modèle logistique. Nous observons ici la concordance entre les coefficients a_j et b_j. Reprenons le ***LOGIT***

$$\ln\frac{p(1|X)}{1-P(1|X)} = \ln\frac{p(1|X)}{P(0|X)} = \ln\frac{p(1)p(X|1)}{P(0)P(X|0)} = \ln\frac{p(1)}{P(0)} + \ln\frac{p(X|1)}{P(X|0)} \quad (3.4)$$

$$\ln\frac{p(1|X)}{1-P(1|X)} = b_0 + b_1x_1+\ldots+b_jx_j \quad (3.5)$$

Nous constatons que $\begin{cases} b_0 = \ln\frac{p}{p} + a_0 \\ b_0 = a_j, j \geq 1 \end{cases}$ (3.6)

3.4. Vue globale du système

Nous avons suivi plusieurs étapes afin de construire un système IDS, notre étude repose sur des simulations. **La figure 3.1** illustre le système proposé. D'abord, nous lançons une simulation de comportements normal et malveillant dans de nombreux scénarios (Blackhole/Normal, Dos/Normal, Flood/Normal) ; les sorties sont un lot de fichiers de trace qui capturent nos simulations. A partir de ces fichiers, nous extrairons diverses caractéristiques qui définissent ces comportements (normal et malveillant) en utilisant la régression logistique binomial et générant des modèles « Normal et malveillant ». Dans ce qui suit, nous détaillons chacune de ces étapes.

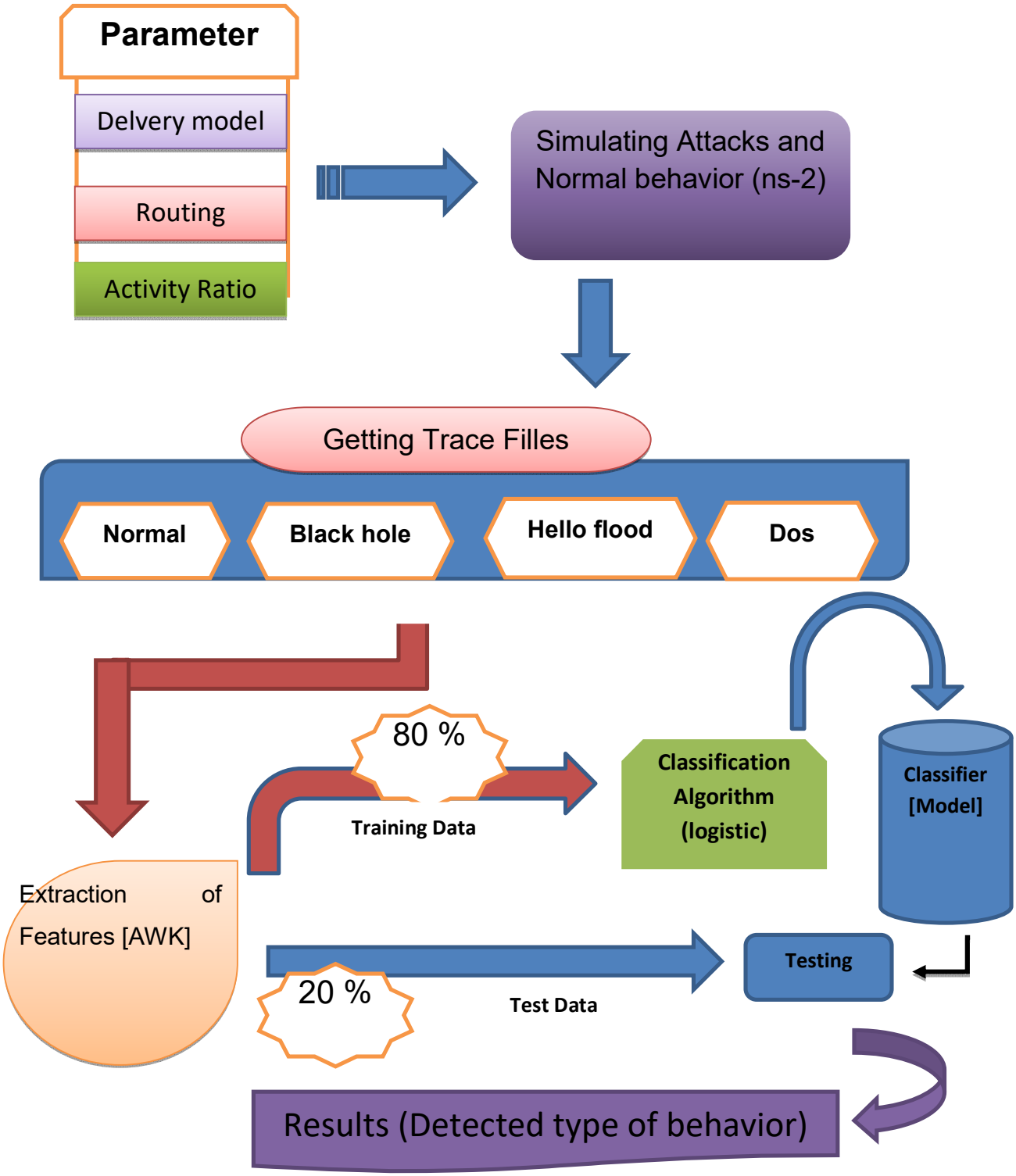


Figure 3.1 - Vue globale du système

3.4.1 Simulation

En ce qui concerne le modèle de fourniture de données, plusieurs éléments doivent être pris en compte en fonction de la nature de l'application. En fait, le modèle de transmission de données au sinkpeut être continu ou périodique, événementiel, diriger par une requête Query-driven et Hybrid[28]. Dans le modèle de livraison continue, chaque nœud capteur envoie des données périodiquement, tandis que les événements et les modèles pilotés par les requêtes (Query-driven), la transmission des données débute lorsqu'un événement se produit ou lorsque le récepteur génère une requête. Dans notre expérience, et pour être plus général, nous avons choisi de baser sur les événements du modèle de livraison de données dans lequel un nœud envoie des données au Sink. En fait, nous modélisons le moment des événements qui se produisent au hasard. En plus de comportement normal, nous adoptons trois types d'attaques qui tombent principalement dans la catégorie Déni de service : Blackhole, Hello Flood et DoS.

En outre, pour avoir de nombreux scénarios, nous avons considéré un autre paramètre qui fixe le nombre de nœuds de travail (Paramètre Ratio d'activité). Ce paramètre est ajouté pour mesurer la performance d'un IDS dans de nombreux scénarios de charge de travail. Par souci de simplicité, nous avons opté pour le protocole AODV.

3.4.1.1 Les attributs collectés

De nombreux attributs peuvent être considérés pour caractériser un comportement au niveau de la connexion. Dans notre étude, nous avons examiné certains d'entre eux comme indiqué dans le tableau 3.1. Nous avons classé ces caractéristiques en fonction de leur type: Données, Routage et Temps.

Feature	Type	Description
Duration	Time	The amount of time between sending the first packet and receiving the last packet.
All Received Packets	Data, Routing	All the packets (regardless of who sent them and their type) that the sink received during the duration of this connection
AODV Route Request	Routing	The number of AODV RREQ packets that the sending node has sent.
AODV Route Reply	Routing	The number of AODV RREP packets that the sending node has sent.
TCP packet sent	Data	The number of TCP packets which the sending node has sent.
TCP packet received	Data	The number of TCP packets that the sink has received.
TCP packet dropped	Data	The number of TCP packets that got dropped.
TCP packet forward	Data	The sum of the number of times that each TCP packet in this connection got forwarded.
Energy consumed	-	The amount of energy consumed by all the nodes inherent to the connection.
Packet delivery ratio	Data	the ratio of received TCP packets to sent TCP packets.
Average delay	Time	The average delay of the received TCP packets during the connection.
Max hop	Routing	Maximum number of hops during the connection.
Average hop	Routing	Average number of hops during the connection.
Throughput	Data	the amount of received data in the connection duration (kbps).

Tableau3.1 - Descriptions des attribues ciblées

3.5. Expériences et résultats

Rappelons que l'objectif principal de ce travail est de construire un système d'apprentissage automatique base sur la régression logistique pour détecter les attaques, tout en variant plusieurs attributs pour obtenir le plus efficace entre elles.

D'abord, nous spécifions le modèle d'application de notre RCSF. Ensuite, nous décrivons les outils utilisés dans cette expérience. Après, nous détaillons le processus de simulation des comportements normaux et malveillants sous ns-2. Enfin, nous présentons les résultats et leur interprétation.

3.5.1 Modèle d'application

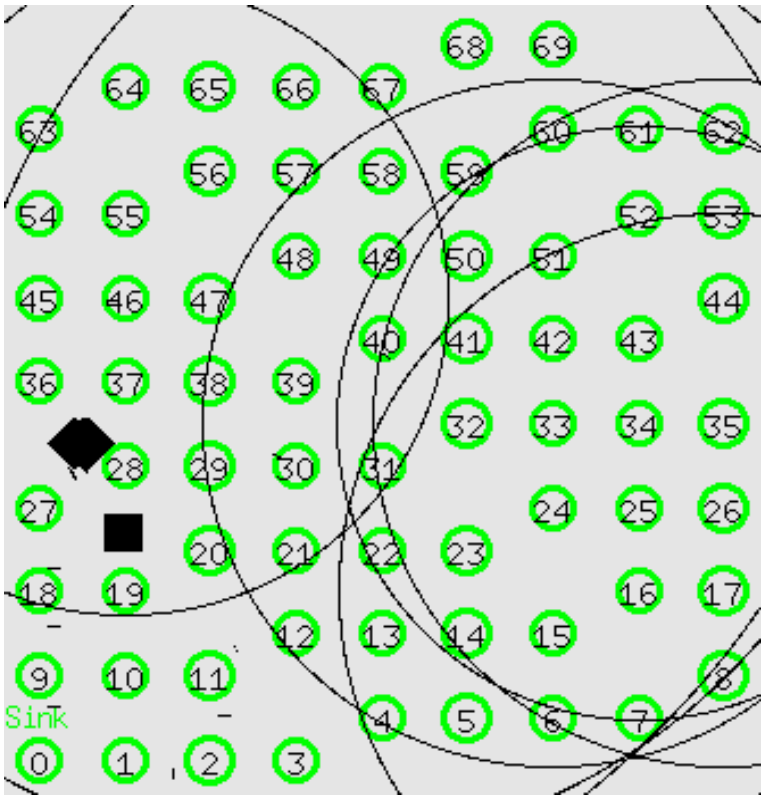


Figure 3.2- Modèle d'application (en cours de simulation)

Nous avons considéré un environnement simple, où les nœuds de capteurs sont statiques et placés dans une topologie maillée comme le montre la **Figure 3.2.** Le nœud avec l'identification "0" est considéré comme le Sink. Nous avons utilisé 70 nœuds dans nos simulations. Ce choix est fait pour faciliter la visualisation.

Rappelons que le modèle de diffusion de données est piloté par les événements. Les nœuds détectent des valeurs telles que la température, la pression, le son, etc. Lorsque ces valeurs atteignent un certain seuil, elles sont transmises au Sink.

Concernant le routage, nous avons effectué notre analyse en utilisant AODV. Notre choix est justifié par son adéquation avec RCSF. En plus de la capacité à soutenir la mobilité.

3.6. Outils utilisés

Afin de rendre nos résultats reproductibles, nous sommes appuyés sur un ensemble des outils et des langues Open Source.

3.6.1 Ns-2

Ns-2 est un outil de simulation Open-Source, qui fonctionne sous Linux. C'est un simulateur à événements discrets ciblé sur la recherche en réseau et accorde un support solide pour la simulation de routage, protocoles multicast et protocoles IP, tels que UDP, TCP, RTP et SRM à travers les réseaux filaires et sans fil. Il a également un soutien pour plusieurs protocoles et la capacité de détailler graphiquement le trafic réseau. En outre, ns-2 porte peu d'algorithmes dans le routage et la mise en file d'attente. Les algorithmes de routage tels que AODV, DSR et DSDV. Les algorithmes de mise en file d'attente incluent un déficit de mise en file d'attente équilibré, round-robin et FIFO [29].

3.6.2 GAWK

GNU AWK est une implémentation Open Source de l'AWK langage de programmation, et il est disponible pour tous les systèmes UNIX R. Le langage AWK est un langage de script basé sur les données, puissant outil de manipulation de texte, et le langage de correspondance de modèle qui est particulièrement utile pour l'extraction de données [30]. Comme le montre la

figure 3.3 AWK suit un flux de travail simple, d'abord, l'exécution du Begin {} bloquer, puis, lire l'entrée une ligne à la fois, lors de l'exécution le bloc Action {} sur ces lignes, après avoir terminé l'entrée, il exécute le bloc End {}.

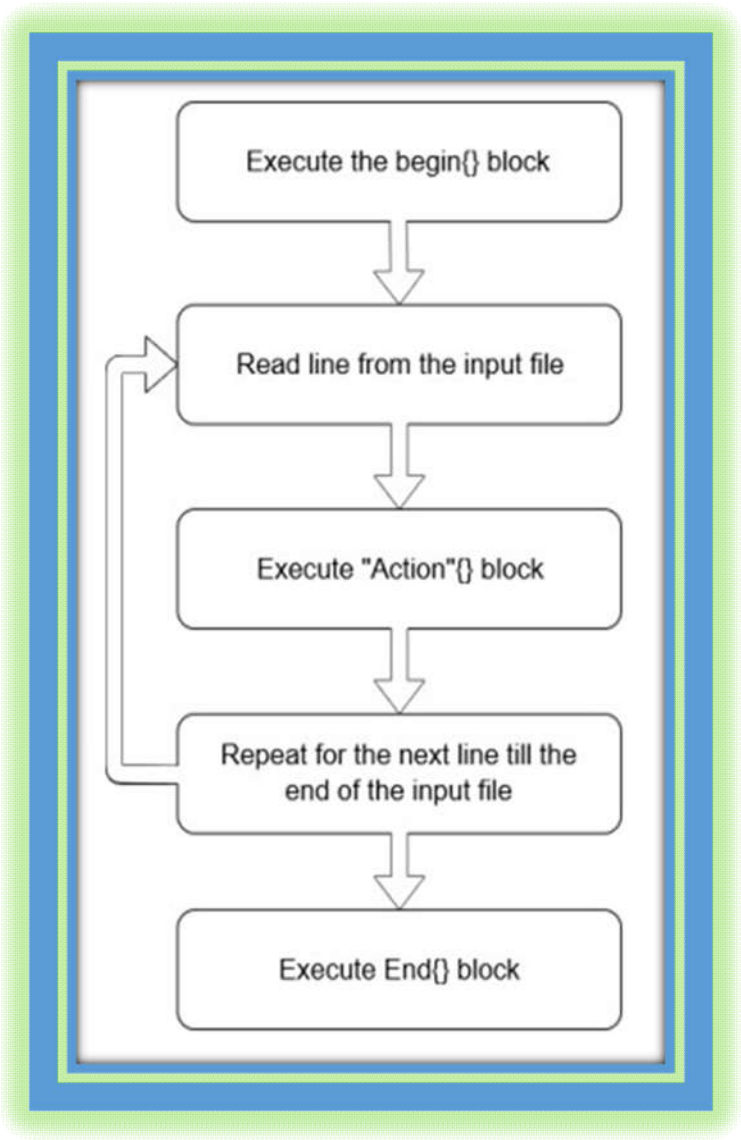


Figure 3.3- Flux de travail de script AWK

3.6.3 WEKA

L'environnement Waikato pour l'analyse des connaissances est un logiciel, avec des interfaces utilisateur graphiques qui facilitent d'accéder à un ensemble d'outils de visualisation, d'algorithmes d'analyse de données et techniques d'avant-garde en apprentissage automatique [31].

3.7. Simulation des comportements et paramètres

Nous avons simulé les comportements Normal et trois différents malveillants : Blackhole, Hello Flood et DoS. Concernant le comportement Normal, nous avons choisi le protocole AODV pour le routage et TCP pour la transmission. Il y a 70 nœuds dans notre topologie, alors que le plan de livraison est à un temps, un nœud d'envoie des données au récepteur (nœud 0). Dans le but de diversifier les scénarios, nous avons varié le nombre nœuds de travail dans un scénario. Ceci est réalisé en considérant quatre différents ratios d'activité (10%, 25%, 50%, 75%) dans chaque scénario. Pour simuler le modèle de la diffusion événementielle, le nœud commence à envoyer des données à des moments aléatoires comme dans des applications réelles. Pour reproduire le même scénario Normal lors de la simulation des attaques, nous avons capturé le scénario (Sauvegarde de l'identité de travail nœuds et leur temps de début de transmission de données).
. En ce qui concerne les comportements malveillants, nous avons généré la même topologie comme comportement normal avec les mêmes paramètres, alors nous avons chargé le fichier contenant les identités des nœuds et temps de début des données d'envoi. Ensuite, nous avons choisi au hasard un seul nœud pour qu'il agisse de manière malveillante. Nous avons choisi trois comportements malveillants différents :

- **Blackhole** Le nœud malveillant supprime tous les paquets qui passent à travers. Pour ce faire, il attire son nœud voisin en forgeant l'itinéraire de la réponse avec moins de nombre de sauts et plus numéro de séquence.
- **Hello Flood :** Le nœud inondé continue d'envoyer des messages RREQ malgré la réception de messages RREP, dans le but de gaspiller la bande passante du réseau et d'épuiser ses ressources.
- **DoS :** Le nœud attaquant continue d'envoyer des paquets au récepteur, dans le but de le rendre inactif.

En suivant les scénarios décrits précédemment, nous avons lancé les simulations. Cela a conduit à un ensemble de fichiers de trace à partir de laquelle nous extrayons les attributs ciblés. Nous avons déployé des scripts AWK pour effectuer cette extraction. Chaque connexion est caractérisée par toutes les fonctionnalités.

3.8. Résultats et interprétations

3.8.1 Mesures d'évaluation

L'évaluation de la qualité de notre système IDS est faite avec les quatre éléments de base qui sont : les vrais positifs (VP), i.e. les anomalies effectivement détectées, les faux négatifs (FN), i.e. les anomalies non-détectées, les faux positifs (FP), i.e. les fausses alarmes et les vrais négatifs (VN). On peut les résumer sous la forme d'une matrice de confusion (Table 3.2).

		Observation	
		normal	attaque
Prediction	normal	**VP**	**FP**
	attaque	**FN**	**VN**

Tableau 3.2 - Matrice de confusion pour un problème de classification à 2 classes.

Pour mesurer le pourcentage d'échantillons correctement classés, on utilise l'incertitude (1) (i.e. le ratio de vrais positifs et vrais négatifs sur le nombre total d'échantillons). Cependant, il peut fausser l'évaluation lorsque le nombre de vrais négatifs est considérablement supérieur au nombre de vrais positifs. C'est pourquoi l'on utilise d'autres métriques en complément.

$$\textbf{Incertitude : I} = \frac{VP+FN}{VP+VN+FP+FN} \quad (1)$$

Le premier critère est la précision (2), i.e. le ratio entre le nombre de varies anomalies et le nombre d'échantillons classés par l'algorithme comme des anomalies. Plus la valeur est petite et plus il y a de faux positifs. Le second critère est le rappel (3), qui est le pourcentage

d'anomalies correctement classées en tant que telles parmi toutes les vraies anomalies. Ainsi, plus le rappel est petit et plus il y a d'anomalies non détectées.

$$\textbf{Précision : P} = \frac{\textbf{VP}}{\textbf{VP} + \textbf{FP}} \textbf{(2)Rappel : R} = \frac{\textbf{VP}}{\textbf{VP} + \textbf{FN}} \qquad \textbf{(3)}$$

$$\textbf{F-mesure : F} = 2.\frac{\textbf{(précision.rappel)}}{\textbf{(précision+rappel)}} \qquad \textbf{(4)}$$

Résultats obtenus

Dans le but de mesurer l'efficacité du notre approche, les figures et les tableaux suivants présentent les performances comparatives de la classification adoptée en termes de précision et rappel, F-Measure, et les matrices de confusions en fonction du taux d'activité (10% ,25%,50%,75%) et cela,pour tous les comportements de la simulation.

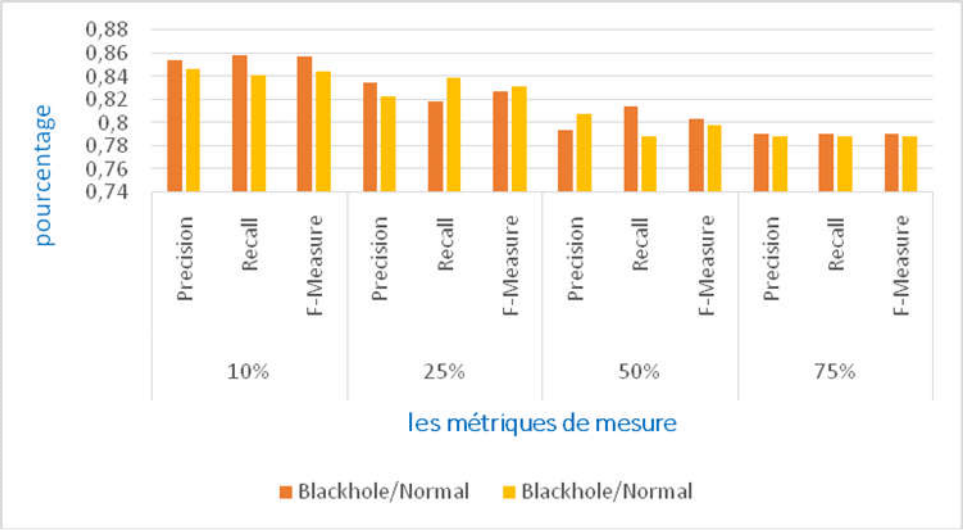


Figure 3.4 -Classement des performances en fonction de taux de l'activité (Blakhole/Normal)

ans la figure 3.4, nous observons que :

✓ ladétection d'attaque (Blakhole) est diminuée sur tous les scénarios de taux d'activité RCSF. Plus nous augmentons le taux d'activité, la détection de l'attaque (Blakhole) sera diminué.

✓ L'écart entre les performances comparatives de classification (précision, rappel, f-measure) est diminué et variant aussi selon le d'activité. Exemple : nous observons un écart de plus de 5.5% pour F-measure entre le rapport d'activité 10% et 75%.

Tauxd'activité	Matrice de confusion			
10%		a	b	a b <-- classified a = Normal b = ATTACK
	a	2232	366	
	b	381	2021	
25%		a	B	
	a	976	216	
	b	193	1004	
50%		a	B	
	a	1007	230	
	b	262	971	
75%		a	b	
	a	1008	266	
	b	266	988	

Tableau 3.3 – Matrice de confusion (Blakhole / Normale)

Dans le tableau 3.3, on observe selon l'activité du trafic sur le comportement de la simulation (Blakhole / Normale) qu'à chaque fois on a une diminution continue de la proportion des échantillons ou des paquets et qui sont correctement classés (vrai positif ou Faux positif).

Exemple : nous observons un écart de plus de 6% sur le classement correct (TP et TF) de la proportion des paquets entre le rapport d'activité 10% et 75%.

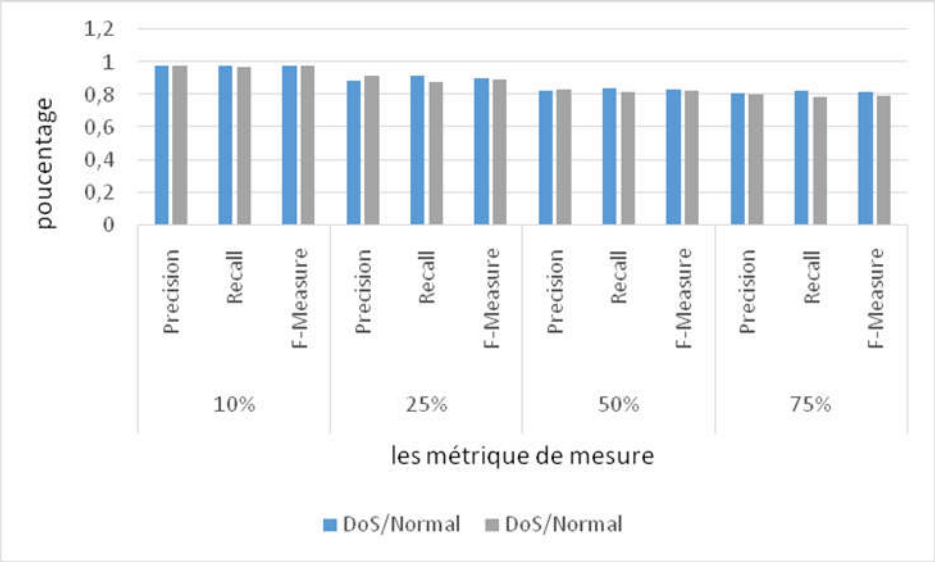


Figure 3.5 - Classement des performances en fonction de taux de l'activité (Dos/Normal)

Dans **la figure3.5,** nous observons que :

✓ la détection d'attaque (Dos) est diminuée sur tous les scénarios de taux d'activité RCSF. Plus nous augmentons le taux d'activité, la détection de l'attaque (Dos) sera diminué.

✓ L'écart entre les performances comparatives de classification (précision, rappel, f-measure) est diminué et variant aussi selon le d'activité. Exemple : nous observons un écart de plus de 18% pour F-measure entre le rapport d'activité 10% et 75%.

Tauxd'activité	Matrix de confusion			
10%		a	b	a b <-- classified
	a	2521	47	a = Normal
	b	60	2279	b = ATTACK
25%		a	B	
	a	1111	99	
	b	144	1053	
50%		a	B	
	a	1044	201	
	b	215	978	
75%		a	B	
	a	1092	230	
	b	**253**	**927**	

Tableau 3.4 – Matrice de confusion (Dos / Normale)

Dans le tableau 3.4. On observe selon l'activité du trafic sur le comportement de la simulation (Dos/Normale) qu'à chaque fois on a une assez forte diminution continue de la proportion des échantillons ou des paquets et qui sont correctement classés (vrai positif ou Faux positif)

Exemple : nous observons un écart de plus de 17% sur le classement correct (TP et TF) de la proportion des paquets entre le rapport d'activité 10% et 75%.

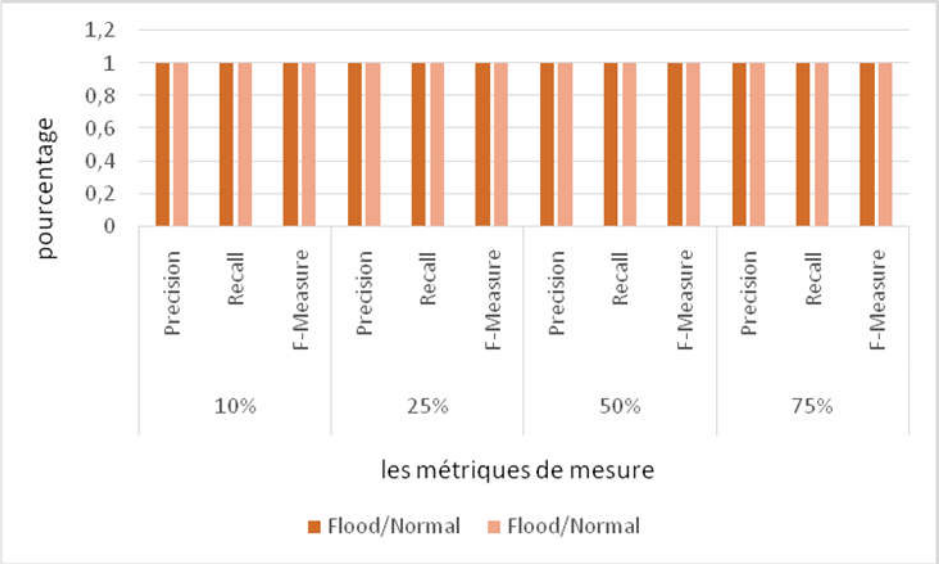


Figure 3.6 - Classement des performances en fonction de taux de l'activité (Flood / Normal)

Dans la figure 3.6, nous observons que :

✓ la détection d'attaque (Flood) est la plus facile sur tous les scénarios de taux d'activité RCSF.

✓ L'écart entre les performances comparatives de classification (précision, rappel, f-measure) est égal à « 0 » et n'est pas affecté par le taux d'activité. Exemple : nous observons un écart égal à 0% pour F-measure entre le rapport d'activité 10% et 75%.

Tauxd'activité	Matrix de confusion			a b <-- classified a = Normal b = ATTACK
10%		a	B	
	a	2537	0	
	b	0	2503	
25%		a	B	
	a	1181	0	
	b	0	1208	
50%		a	B	
	a	1221	0	
	b	0	1264	
75%		a	B	
	a	1268	0	
	b	0	1281	

Tableau 3.5 – Matrice de confusion (Flood / Normale)

Dans le tableau 3.5, nous observons que quel que soit l'activité du trafic sur le comportement de la simulation (Dos / Normale), la proportion des échantillons ou des paquets qui sont correctement classés (vrai positif ou Faux positif) et toujours égal 100%, et cela veut dire que la classification des paquets incorrecte et nulle.

Exemple : nous observons un écart de plus de 0% sur le classement correct (TP et TF) de la proportion des paquets entre le rapport d'activité 10% et 75%.

3.9. Conclusion

Les réseaux de capteurs sans fil (RCSFs) se retrouvent malheureusement très exposés aux attaques telles que le déni de service.Au cours de ce chapitre, nous avons présenté notre système

de détection (IDS) pour les RCSFs en utilisant la régression logistique. Nous avons commencé par le prétraitement d'un ensemble de données pour effectuer, par la suite, la simulation.

Avant simuler le comportement de notre IDS, nous avons justifié tout fait sur les choix de niveau de caractérisation de l'attaque, des caractéristiques ciblées, et du classificateur utilisé. Ensuite, nous avons décrit notre expérimentation en commentant les résultats obtenus. Ces dernières nous ont permis de tirer plusieurs conclusions dans ce domaine.

Conclusion Générale

Les réseaux de capteurs sans fil (RCSF$_S$) sont en plein développement, et deviennent de plus en plus répandus. Actuellement, ils constituent un thème de recherche très dynamique, tiré vers le haut, par leurs utilisations dans divers domaines. En effet, leurs applications sont de plus en plus nombreuses et diversifiées.

Une problématique majeure dans les réseaux de capteurs, est leur sécurité. En effet ces derniers sont très vulnérables à de multiples attaques vu leur contraintes critiques (énergie, mémoire, etc.). Par exemple les attaques DOS$_S$.

Dans ce travail, nous sommes intéressés à la problématique de sécurité dans les réseaux de capteurs sans fil. Plus précisément à la system détection d'intrusion (IDS).

La solution proposée consiste à détecter les attaques par l'étude de l'impact des attaques DoS sur l'ensemble des attributs d'un RCSF. Pour ce faire, nous avons expérimenté de nombreux scénarios de simulation contenant plusieurs comportements ciblés. Ces comportements sont (Normal, Blackboule), (normal, Hello-Flood) et (normal, Dos). Plus tard nous avons appliqué notre méthode de détection d'intrusion (IDS) qui est basée sur l'apprentissage a travers du classificateur de la régression logistique.

À l'avenir, Ce travail peut être enrichi en essayant d'autres configurations et protocoles de simulation et un autre classificateur.

Bibliographie

Et

Références

Bibliographie Et Références

[1] Butun, I., Morgera, S. D., and Sankar, R. A surveyof intrusion detection systems in wireless sensor networks. IEEE Communications Surveys & Tutorials 16, 1 (20I.6), 266{282. 2, 16, 22.

[2] Boudjaadar Amina ; « Plateforme basée Agents pour l'aide à la conception et simulation , 2010 .

[3] http://licencerk.wikeo.fr/chapitre1.html.

[4] BENHABIB Imane et ABOURA Wissam , Etude et caractérisation de la couche physique du standard IEEE802.16/WIMAX, 2012.

[5] Hung-Cuong LE, Optimisation d'accès au médium et stockage de données distribuées dans les réseaux de capteurs.

[6] C.Y. Chong and S.P. Kumar, « Sensor network: evolution, opportunities, and challenges », Inproceedings of the IEEE, 91(8), pp. 1247-156, 2003.

[7] T.B. Gosnell, J.M. Hall, C.L. Hall, C.L. Ham, D.A. Knapp, Z.M. Koening, S.J. Luke, B.A. Pohl,A.Schan von Wittenau, and J.K. Wolford, «Gamma-ray identification of nuclear weapon materials»,Technical Report DE97053424, Lawrence Livermore National Lab, CA, USA, 1997.

[8] R. Merzougui, M. Feham and H. Sedjelmaci, « Design and implementation of an algorithm for cardiac pathologies detection on mobile phone », International Journal of Wireless InformationNetworks, 18 (1):11-23, 2011.

[9] M. Mana, « Adaptation et intégration de la sécurité biométrique aux réseaux de capteurs corporelssans fil », Thèse de Doctorat en télécommunication, Université de Tlemcen, Algérie, Janvier 2011.

[10] K. Beydoun, « Conception d'un protocole de routage hiérarchique pour les réseaux de capteurs »,Thèse de Doctorat en informatique, Université de Franche-Comté, France, Décembre 2009.

[11] M. Fitzgerald. Technnology Review: Tracking a Shopper's Habits, August 2008.http://www.technologyreview.com/computing/21161/ .

[12] V. Tsetsos, G. Alyfantis, T. Hasiotis, O. Sekkas, and S. Hadjiefthymiades, «Commercial wirelesssensor networks: technical and business issues», Second Annual Conference on Wireless On-demandNetwork Systems and Services, St. Moritz, Switzerland, pp.166-173, 2005.

[13] David Martins, "Sécurité dans les réseaux de capteurs sans fil stéganographie et réseauxde confiance ", Thèse de doctorat, Université de FRANCHE-COMTÉ, 2010.

[14] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, In journal of Computer Networks, vol.38, pp. 393-422, 2002.

[15] J. Newsome, E. Shi, D. Song and A. Perrig, 'The Sybil Attack in Sensor Networks Analysis and Defenses', In Proceedings of the Third International Symposium on Information Processing in Sensor Networks (IPSN 2004),April 2004.

[16] Messai Mohamed Lamine. Securite dans les Reseaux de Capteurs Sans-Fil.Memoire de Magistere en Informatique Ecole Doctorale d'Informatique de bejaia 2007/2008.

[17] Peng Ning ,Yun Cui,and Douglas S .Reeves. Constructing attacks scenarios through correlation of intrusion alerts. In ACM Conference on Computer and Comminication Security.pages 245-254,2002.

[18] Oliver Poblete , 'An Overview of the Wireless Intrusion Detection System',SANS Institute InfoSec Reading Room , January 2005.

[19] LABRAOUI Nabila , 'La sécurité dans les réseaux de capteurs sans fil AdHoc', Thèse de doctorat, Université de Tlemcen, 2012.

[20] S.Ahmed SEDJELMACI, 'Mise en oeuvre de mécanisme de sécurité basés sur les IDS pour les réseaux de capteurs sans fil', Thèse de doctorat, Université de Tlemcen, 2013.

[21] A.Perrig, J. Stankovic and D. Wagner, 'Security in Wireless Sensor Networks', In Communications of the ACM, Vol. 47, No. 6, June 2004, pp. 53-57.

[22]LABRAOUI Nabila , 'La sécurité dans les réseaux de capteurs sans fil Ad Hoc',Thèse de doctorat, Université de Tlemcen, 2012.

[23] Yongguang Zhang , Yi-An Huang , 'Intrusion Detection Techniques for Mobile Wireless Networks', Mobile Networks and Applications, (2003) 1–16.

[24] Vincent Loonis, « Les déterminants de la réélection des députés français de 1871 à 2002 », Histoire & Mesure, vol. 21, no 1, 2006.

[25] Good, I. J. (1965), Franz L. Alt and Morris Rubinoff, eds., "Speculations Concerning the First Ultraintelligent Machine", Advances in Computers, Advances in Computers.

[26] E. T. Jaynes et G. Larry Bretthorst (dir.), Probability theory : the logic of science, Cambridge, UK New York, NY, Cambridge University Press, 2003, 758 p.

[27] Stutz, M. Get started with gawk: Awk language fundamentals, September 2006.

[28] Stojmenovic, I. Handbook of sensor networks: algorithms and architectures, vol. 49. John Wiley & Sons, 2005.

[29] Kabir, M. H., Islam, S., Hossain, M. J., and Hossain, S. Detail comparison of network simulators. International Journal of Scienti_c & Engineering Research 5 (2014), 203{218.

[30] Stutz, M. Get started with gawk: Awk language fundamentals, September 2006.

[31] Witten, I. H., Frank, E., Hall, M. A., and Pal, C. J. Data Mining: Practical machine learning tools and techniques. Morgan Kaufmann, 2016.