الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة غرداية

Université de Ghardaïa

كلية العلوم والتكنولوجيا

Faculté des Sciences et de la Technologie

قسم الرياضيات والإعلام الآلي

Département des Mathématiques et de l'Informatique

Mémoire pour l'obtention de diplôme Master en Informatique

Dans le cadre de l'Arrêté Ministériel 1275, Certificat de fin d'études - Startup / Brevet

THEME

Une approche d'apprentissage automatique pour la détection des mauvais comportement dans les réseaux de capteurs sans fil

Présenté par :

- *Rabia Eladaouia Bouhicha*
- *Fatima Zohra Koumyem*

Encadré par :

- *Mr. Ahmed Saidi*

Année Universitaire : 2022/2023

الجمهوريـــة الجزائريـــة الديمقراطيـــة الشعبيـــة
République Algérienne Démocratique et Populaire

وزارة التعليـــم العالـــي والبحـــث العلمـــي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعـــة غـــردايـــــــة
Université de Ghardaïa

كـــليـــة العـــلـــوم والتكنولـوجيـــا
Faculté des Sciences et de la Technologie

قســـم الرياضيـــات والاعـــلام الآلـــي
Département des Mathématiques et de l'Informatique

مخبـر الرياضيـــات و العـــلـــوم التطبيقيـــة
Laboratoire des Mathématiques et de Sciences Appliquées

Nd'enregistrement
/..../..../..../

Mémoire de fin d'étude, en vue de l'obtention du diplôme

Master

Spécialité : Systèmes Intelligents pour l'Extraction des Connaissances

Thème

Une approche d'apprentissage automatique pour la détection des mauvais comportement dans les réseaux de capteurs sans fil

Soutenu publiquement le 06/07/2023 par :

Rabia Eladaouia Bouhicha & Fatima Zohra Koumyem

Devant les membres du jury

Mr. Youcef MAHDJOUB	MAA	Univ. Ghardaia	Président
Mr. Abdelkader BOUHANI	MAA	Univ. Ghardaia	Examinateur
Mr. Houssem Eddine DEGHA	MCB	Univ. Ghardaia	Examinateur
Mr. Elcheikh BEN GAIED	MCA	Univ. Ghardaia	Examinateur
Mr. Ahmed SAIDI	MCB	Univ. Ghardaia	Encadreur
Mr. Moussa BABOUSMAIL	Aéroport de Ghardaia		Partenaire économique

Année Universitaire : 2022/2023

REMERCIEMENT

D'abord, nous remercions ALLAH Tout-Puissant de nous avoir donné la force et le courage afin que nous puissions accomplir cet humble travail, ainsi que la capacité de surmonter toutes les difficultés.

Nous tenons à remercier notre superviseur Mr.Ahmed Saidi pour son soutien, ses conseils et ses efforts pour mener à bien ce travail.

Sincères remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail et de l'enrichir du leurs propositions.

Enfin, nous tenons également à remercier toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

Dédicaces

Je dédie ce travail à mes adorables parents Djamila et El hachemi qui m'ont toujours encouragé durant mes années d'étude et ma grand-mère Zohra, et ma chère tante Amera.

À ma chère soeur Wafa et mon cher frère Merouane, qui m'ont soutenu et encouragé, ainsi qu'à la femme du mon frère Attora et ses fils Chiheb et Iheb, à qui je souhaite bonne chance dans leurs études.

À toute ma famille Bouhicha et Bahaz.

À tout mes professeurs qui ont contribué à notre formation.

À mes amies Dina , Aya, Rababe , Alla , Maria et à toutes les personnes qui ont une place spéciale dans mon cœur et ma vie.

À chère amie avant d'être mon binôme dans le mémoire Fatima et tous les étudiants de 2éme Master informatique.

Merci

Adaouia Bouhicha

Dédicaces

Je dédie ce travail à mes très chers parents pour leur encouragement et source de vie d'amour et d'affection merci d'avoir fait de moi la personne que je suis.

À mon cher frère et à hmida et à ma chère sœur et son fils source de joie et de bonheur.

À tout mes professeurs qui ont contribué à notre formation.

À toute ma famille à tous mes amis et à l'ensemble des étudiants de la promo.

À Adaouia chère amie avant d'être mon binôme.

À vous cher lecteurs.

Merci

Fatima Koumyem

Résumé

Les réseaux de capteurs sans fil est un domaine de recherche en évolution continue avec une multitude de contexte d'application. Malgré ses avantages, ce type de réseau présente plusieurs défis, tel que le problème de sécurité qui reste ouvert et non totalement résolu. Le facteur de confiance est une stratégie efficace qui sécurise le réseau contre les attaques interne et le mauvais comportement des noeuds. Plusieurs modèles on été proposés, mais la majorité de ces modèles considèrent une seule type de confiance communication, données ou bien énergie dans l'évaluation du comportement des noeuds. Cela rendre ces modèles vulnérables aux attaques ciblant d'autres types de confiance.

Dans notre projet de fin d'études, on a proposé une approche de sécurité basée sur le facteur de confiance qui prendre en considération tous les types de confiance. Premièrement, on a proposé plusieurs critères afin de modéliser le comportement du noeud. Les critères proposés permettent l'évolution de chaque type de confiance. Puis, on a utilisé l'algorithme SVM pour la classification des noeuds malicieux ou bien fiable selon leurs comportements dans le réseau.

D'après les résultats obtenus avec la simulation, notre approche peut détecter efficacement les noeuds malicieux dans le réseau.

Mots clés : Réseaux de capteurs sans fil, Sécurité , Confiance, Comportement, Noeuds malicieux

Abstract

Wireless sensor networks are a continuously developing area of research with numerous applications. Despite their benefits, these networks present several challenges, including unresolved security issues. The trust factor is an effective strategy for securing the network against internal attacks and bad node behavior. While several models have been proposed, most only consider one type of trust communication, data or energy, leaving them vulnerable to attacks targeting other types of trust.

In our graduation project, we proposed a security approach based on the trust factor that considers all types of trust. We first proposed several criteria to model node behavior, allowing for the evolution of each type of trust. We then used the SVM algorithm to classify nodes as malicious or reliable based on their behavior in the network.

Our simulation results demonstrate that our approach can effectively detect malicious nodes in the network.

Keywords: Wireless sensor networks, Security , Trust, Behaviour, Malicious nodes.

ملخص

شبكات الاستشعار اللاسلكية هي مجال بحث دائم التطور مع العديد من سياقات التطبيق. على الرغم من مزايا هذا النوع من الشبكات ، إلا أنه يطرح عدة تحديات ، مثل مشكلة الأمان التي تظل مفتوحة ولم يتم حلها بالكامل. عامل الثقة هو استراتيجية فعالة تؤمن الشبكة ضد الهجمات الداخلية وسلوك المستشعر السيئ. تم اقتراح العديد من النماذج ، لكن غالبية هذه النماذج تأخذ في الاعتبار نوعًا واحدًا فقط من ثقة الاتصالات أو البيانات أو الطاقة في تقييم سلوك العقد.مما يجعل هذه النماذج عرضة للهجمات التي تستهدف أنواعًا أخرى من الثقة.

في أطروحتنا ، اقترحنا نموذج أمني قائم على عامل الثقة الذي يأخذ في الاعتبار جميع أنواع الثقة. أولاً ، تم اقتراح عدة معايير لنمذجة سلوك العقدة. تسمح المعايير المقترحة بتطور كل نوع من أنواع الثقة. بعد ذلك ، استخدمنا خوارزمية SVM لتصنيف العقد الخبيثة أو الموثوقة وفقًا لسلوكها في الشبكة.

وفقًا للنتائج التي تم الحصول عليها من خلال المحاكاة ، يمكن لنهجنا ذلك الكشف الفعال عن العقد الخبيثة في الشبكة.

الكلمات المفتاحية: شبكات الاستشعار اللاسلكية ، الأمن ، الثقة ، السلوك ، العقد الخبيثة

TABLE DES MATIÈRES

Liste des tableaux **iii**

Liste des figures **iv**

Liste des abréviations **v**

Introduction générale **1**

1 Concepts de base **3**
1.1 Introduction . . . 3
1.2 Généralités sur les réseaux de capteurs sans fil . . . 3
1.2.1 Qu'est-ce qu'un noeud capteur ? . . . 3
1.2.2 Les composants d'un noeud capteur . . . 4
1.2.3 La pile protocolaire des RCSF . . . 5
1.2.4 Architectures de réseaux de capteurs sans fil . . . 6
1.2.5 Les caractéristiques des RCSF . . . 7
1.2.6 Domaines d'application dans les RCSF . . . 8
1.2.7 Les problèmes existant dans les RCSF . . . 9
1.3 La sécurité dans les réseaux de capteurs sans fil . . . 10
1.3.1 Terminologies . . . 10
1.3.2 Les objectifs de sécurité . . . 10
1.3.3 Vulnérabilités des réseaux de capteurs sans fil . . . 11
1.3.4 Les défis de sécurité dans RCSF . . . 11
1.3.5 Les attaques dans les réseaux de capteurs sans fil . . . 12
1.3.6 Les mécanismes de prévention . . . 14
1.3.7 Les travaux de détection . . . 15
1.3.8 Les approches de surveillance utilisés dans RCSF . . . 17
1.4 Apprentissage automatique (ML) . . . 17
1.5 Conclusion . . . 18

2 Etat de L'art **19**
2.1 Introduction . . . 19
2.2 Le système de confiance utilisé dans la littérature . . . 19
2.3 Travaux connexes pour la surveillance des RCSF . . . 21
2.4 Critères d'évaluation des approches proposées . . . 28
2.5 Synthèse . . . 31

2.6 Conclusion 32

3 Conception et réalisation **33**
3.1 Introduction 33
3.2 Présentation de modèle 33
3.2.1 Architecture de notre modèle 35
3.3 Les critères utilisés pour l'évaluation du comportement d'un noeud 36
3.3.1 Les critères liés à la communication 36
3.3.2 La métrique liée aux données 38
3.3.3 La métrique liée consommation d'énergie 38
3.3.4 La métrique liée à la mobilité 39
3.4 Algorithme proposée 39
3.5 Simulation et analyse 40
3.5.1 Évaluation de résultat 43
3.5.2 Classification SVM 45
3.6 Comparaison entre les algorithmes 46
3.6.1 Résultats expérimentaux de notre modèle 47
3.6.2 Discussion 48
3.7 Conclusion 48

Conclusion **49**

Bibliographie **50**

LISTE DES TABLEAUX

2.1 Critères d'évaluation d'approches classiques 29
2.2 Critères d'évaluation d'approches ML 30

3.1 Configuration de la simulation 40
3.2 Les caractéristiques utilisées 41
3.3 Résultats des performances 48

TABLE DES FIGURES

1.1 Capteur sans fil (Sahraoui, 2013) . . . 4
1.2 Les composants d'un noeud capteur (Nada, 2021) . . . 4
1.3 Un réseau de capteur sans fil (Ngom, 2016) . . . 5
1.4 La pile protocolaire . . . 6
1.5 Architecture plate (Ngom, 2016) . . . 7
1.6 Architecture hiérarchique (Ngom, 2016) . . . 7
1.7 Attaque Jamming (Khelifa Benahmed et Seddiki, 2018) . . . 13
1.8 Attaque Sybil (Khelifa Benahmed et Seddiki, 2018) . . . 13

2.1 Système de confiance (Saidi, 2022) . . . 20
2.2 Modèle de confiance STMWSN (Rathore, Badarla et George, 2016) . . . 21
2.3 La structure EDTM (Jiang et al., 2014) . . . 22
2.4 L'architecture de la méthode d'évaluation de la confiance (T. Zhang, Yan et Yang, 2018) . . . 23
2.5 La structure de TAAPML (Chinnaswamy et Annapurani, 2021) . . . 24
2.6 Les caractéristiques globales du WSN-DS (S. E. Quincozes, Kazienko et V. E. Quincozes, 2023) . . . 26
2.7 La sélection de caractéristiques basée sur IG, GR et OneR (S. E. Quincozes, Kazienko et V. E. Quincozes, 2023) . . . 26
2.8 Le système IDS proposé (Gulganwa et Jain, 2022) . . . 27

3.1 Conception de réseau . . . 34
3.2 Evaluation de confiance directe . . . 35
3.3 Achitecture de modèle . . . 35
3.4 Nombre des voisins . . . 43
3.5 Les paquets envoyés . . . 43
3.6 Les paquets reçus . . . 43
3.7 Le taux de données . . . 44
3.8 L'énergie . . . 44
3.9 La vitesse . . . 44
3.10 La valeur de confiance pour chaque noeud . . . 45
3.11 Classification SVM . . . 45
3.12 Matrice de confusion . . . 46
3.13 Matrice de confusion de classification . . . 47

LISTE DES ABRÉVIATIONS

BS **B**ase **S**tation

GPU **G**raphics **P**rocessing **U**nit

IDE **I**ntegrated **D**evelopment **E**nvironment

IDS **I**ntrusion **D**etecion **S**ystem

KNN **K** **N**earest **N**eighbors

MAC **M**essage **A**uthentication **C**ode

ML **M**achine **L**earning

RAM **R**andom **A**ccess **M**emory

RCSF **R**éseau **C**apteurs **S**ans **F**il

SE **S**pecification **E**dition

SVM **S**upport **V**ector **M**achine

WSN **W**ireless **S**ensor **N**etwork

INTRODUCTION GÉNÉRALE

Récemment, les réseaux de capteurs sans fil deviennent une technologie largement utilisée en raison de leurs caractéristiques. Un réseau de capteurs sans fil est un type de réseau ad-hoc composé d'un grand nombre de capteurs déployés dans une zone géographique avec des petites tailles. Ces capteurs peuvent communiquer entre eux, et partager des informations afin de captés différents évènements.

Aujourd'hui, on retrouve les RCSF dans plusieurs domaines d'applications y compris commerciales, militaires et environnementales. Toute cette expansion est due à la communication sans fil, à l'auto-organisation, au déploiement rapide et à la réduction des coûts.

Le problème le plus courant avec les réseaux de capteurs est qu'ils disposent de ressources limitées telles que l'énergie, la mémoire et la puissance de traitement, ce qui les rend vulnérables à de nombreux types d'attaques.

Et quand le sujet est la sécurité des réseaux, on parle de la sécurité des noeuds connectés contre les attaques internes et externes, une attaque interne est menée par un noeud de réseau malveillant qui menace d'autres noeuds de réseau, une attaque externe effectué par des noeuds qui sont à l'extérieur du réseau. Ils essaient de pirater le réseau de plusieurs manières. Le danger dans ces types d'attaque c'est qu'elles peuvent entendre le trafic des communications et modifier le contenu des informations.

Notre objectif est comment détecter les noeuds malicieux dans un réseau de capteurs et les classer avec un modèle d'apprentissage automatique.

Dans notre travail, on propose une technique de confiance comme une solution de sécurité pour détecter les noeuds égoïstes malicieux et qui constituent une menace interne pour le réseau. On effectue une simulation de ce modèle de confiance et comment les noeuds connaissent leurs voisins et comment la confiance est établie. Le modèle permet à chaque noeud d'évaluer ses voisins selon le degré de confiance, et sur la base de cette évaluation, on identifie si le voisin est dangereux ou non, on définit des métriques de performance qui nous permettent d'évaluer le comportement des noeuds à tout moment dans le réseau. Ainsi détecter les noeuds malicieux et classer ces noeuds avec un modèle d'apprentissage automatique.

Le présent mémoire comprend trois chapitres organisés comme suit :

- **Chapitre 1 :** Ce chapitre présente d'abord les généralités sur les réseaux de capteurs telles que les caractéristiques, les domaines d'application, l'architecture, ainsi que les problèmes des RCSFs. Il introduit ensuite les concepts de sécurité dans les réseaux de capteurs en passant par les vulnérabilités, les différents attaques, les travaux de détection et les approches de surveillance. Et enfin, une présentation sur l'apprentissage automatique.
- **Chaptitre 2 :** Pour ce chapitre, une présentation des travaux classiques et à base de l'apprentissage automatique sur la surveillance des réseaux de capteurs, suivi d'une évaluation de ces travaux.
- **Chaptitre 3 :** Le dernier chapitre fournit une description de notre modèle proposé et l'utilisation de l'apprentissage automatique pour classer les résultats et une discussion de ces résultats, avec une comparaison.

Chapitre1

CONCEPTS DE BASE

1.1 Introduction

Les réseaux de capteurs sont une catégorie de réseaux sans fil comportant un grand nombre de noeuds. Ils sont caractérisés par un déploiement très dense et à grande échelle dans des environnements souvent limités en terme de ressources. Les réseaux de capteurs sans fil (RCSF) sont aujourd'hui utilisés dans plusieurs domaines et résolvent de nombreux problèmes. Donc, ce chapitre est consacré aux notions élémentaires. Il est divisé en une section générale sur RCSFs, une section sur la sécurité des réseaux de capteurs et enfin une présentation sur l'apprentissage automatique.

1.2 Généralités sur les réseaux de capteurs sans fil

Cette section décrit les capteurs, l'architecture des réseaux de capteurs, leurs propriétés, les domaines d'application et les problèmes qui existent dans RCSF.

1.2.1 Qu'est-ce qu'un noeud capteur ?

Un capteur est un petit appareil qui détecte des événements ou phénomène physique dans un environnement, et communique avec d'autres capteurs via des liaisons sans fil (Maarouf et Ouadah, 2014).

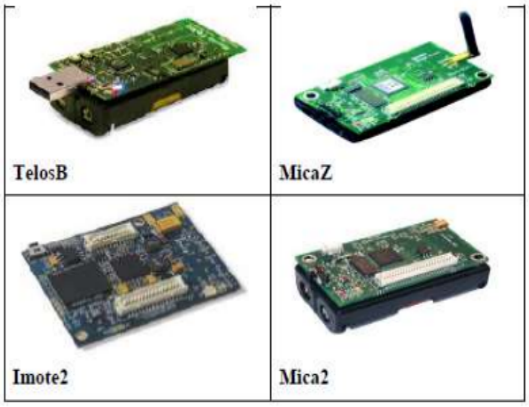

FIG. 1.1 : Capteur sans fil (SAHRAOUI, 2013)

1.2.2 Les composants d'un noeud capteur

Un capteur est composé de quatre composants de base : unité de captage, unité de traitement, unité de communication, et une unité d'énergie. Il existe d'autres composants additionnels dépendant de l'application (un générateur d'énergie, un système de localisation, et un mobilisateur).

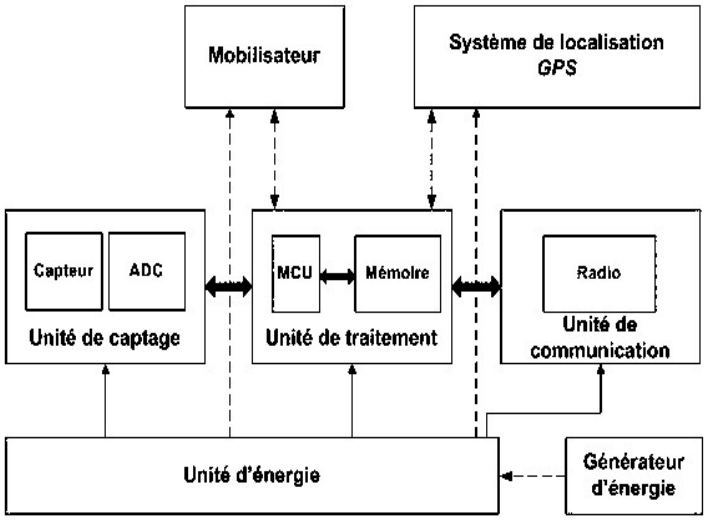

FIG. 1.2 : Les composants d'un noeud capteur (NADA, 2021)

1. **Unité de captage :** Composée d'un capteur qui capte ou mesure les données physiques et converti l'information en données numériques qui peuvent être utilisées par lunité de traitement (SAHRAOUI, 2013).

2. **Unité de traitement :** Elle a besoin de stocker les informations pendant le traitement local et l'agrégation des données. Cette unité a deux interfaces (unité de

captage, unité de communication), elle exécute les protocoles de communications et analyse les données captées (Sahraoui, 2013).

3. **Unité de communication :** Elle effectue toutes les émissions et réceptions des données via un support de communication radio. Elle peut être de type optique (comme dans les noeuds Smart Dust), ou de type radio-fréquence (Sahraoui, 2013).

4. **Unité d'énergie :** La consommation d'énergie est un point très important pour les réseaux de capteurs. Il est impossible de recharger ou changer une batterie, donc avoir une meilleure gestion de la consommation d'énergie est primordial pour augmenter la durée de vie du réseau (Sahraoui, 2013).

1.2.3 La pile protocolaire des RCSF

Un réseau de capteurs sans fil est un type de réseau ad-hoc avec un grand nombre de noeuds qui sont des micro-capteurs capables de récolter et de transmettre des données environnementaux d'une manière autonome (Sahraoui, 2013). La position de ces noeuds peut être aléatoirement dispersés dans une zone géographique "champ de captage " correspondant au terrain d'intérêt pour le phénomène capté.

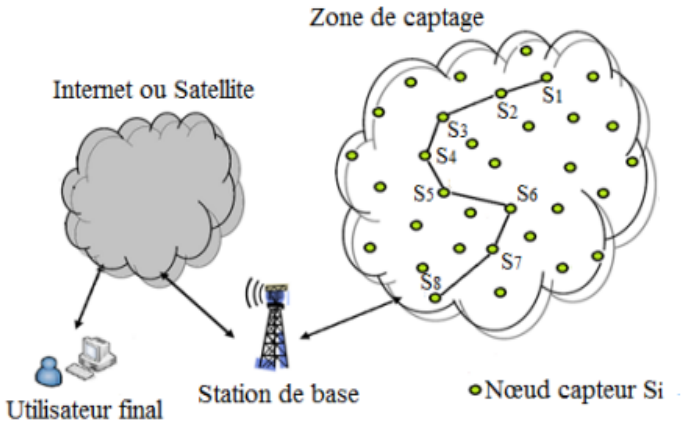

Fig. 1.3 : Un réseau de capteur sans fil (Ngom, 2016)

La pile protocolaire de RCSF est composée de 5 couches, la couche application, la couche transport, la couche réseau, la couche liaison de données et la couche physique. Ainsi que 3 couches pour la gestion de la puissance, la gestion de la mobilité et la gestion des tâches.

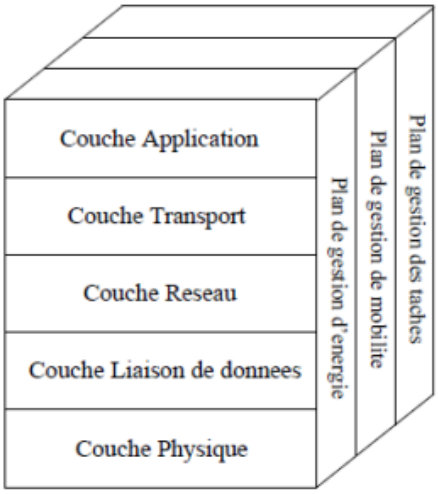

FIG. 1.4 : La pile protocolaire

1. **Couche application :** C'est une couche qui assure une interface avec les applications, elle affiche les données d'un capteur dans le format approprié acceptable pour l'utilisateur final (AMMAR, 2012).
2. **Couche transport :** Cette couche est responsable de la fiabilité de la transmission des données et du contrôle du flux réseau (AMMAR, 2012).
3. **Couche réseau :** Cette couche est responsable de sélectionner le meilleur chemin entre la source et les noeuds de destination en termes d'énergie, délai de transmission, débit...etc (ATHMANI, 2010).
4. **Couche liaison de données :** Elle est responsable de l'accès sur le média, la détection et la correction d'erreurs intervenues sur la couche physique (MONNET, 2015).
5. **Couche physique :** Cette couche permet de modifier et de transmettre des données dans le média physique en choisissant les fréquences appropriées (ATHMANI, 2010).

1.2.4 Architectures de réseaux de capteurs sans fil

Il y a deux types d'architectures pour les réseaux capteurs sans fil :

1.2.4.1 Les réseaux de capteurs sans fil plats

Les protocoles à topologie plate (flat) considèrent que tous les noeuds sont égaux, ont les mêmes fonctions, et peuvent communiquer entre eux sans devoir passer par un noeud particulier ou une passerelle (ALI, 2011).

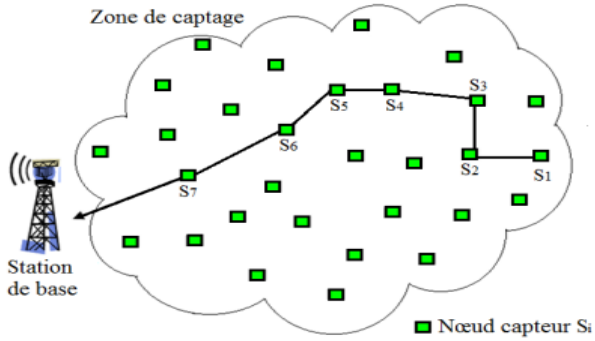

FIG. 1.5 : Architecture plate (NGOM, 2016)

1.2.4.2 Les réseaux de capteurs sans fil hiérarchiques

Les protocoles à topologie hiérarchique forment des réseaux dans lesquels un noeud central (le niveau supérieur de la hiérarchie) est relié à un ou plusieurs autres noeuds qui appartiennent à un niveau plus bas dans la hiérarchie (deuxième niveau) avec une liaison point à point (ALI, 2011).

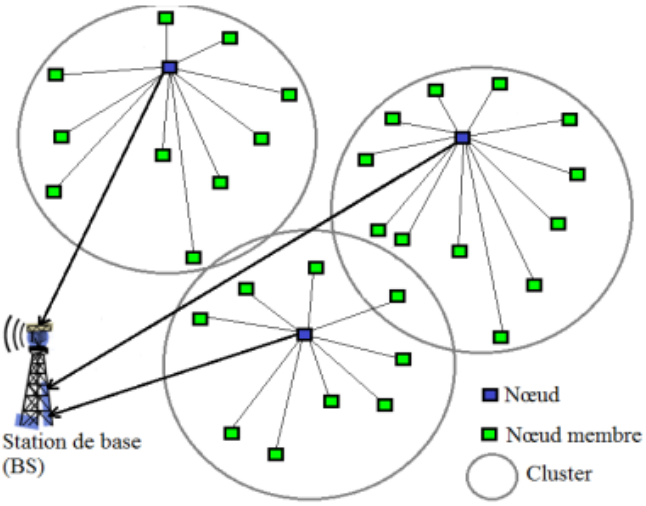

FIG. 1.6 : Architecture hiérarchique (NGOM, 2016)

1.2.5 Les caractéristiques des RCSF

Les réseaux de capteurs se caractérisent par :

- **Absence d'infrastructure :** Les réseaux de capteurs se caractérisent des autres réseaux mobiles par la propriété d'absence d'infrastructure préexistante et de tout genre d'administration centralisée (SAHRAOUI, 2013).

- **Scalabilité :** Le nombre de noeuds dispersés aléatoirement dans les réseaux de capteurs dépasse 1000 noeuds (Benahmed, 2011).
- **Interférences :** Deux transmissions simultanées peuvent interférer sur la même fréquence, ou utilisant des fréquences proches (Benahmed, 2011).
- **Topologie dynamique :** Les capteurs peuvent être attachés à des objets mobiles qui se déplacent d'une façon libre et arbitraire. Elle change d'une manière fréquente suite à la mobilité continue des noeuds qui forment la topologie du réseau (Sahraoui, 2013).
- **Sécurité physique limitée :** Les réseaux de capteurs sans fil sont plus affectées par le facteur de sécurité que les réseaux filaires classiques. Ceci est justifié par les contraintes et limitations physiques qui signifient que le contrôle des données transférées doit être minimisé (Sahraoui, 2013).
- **Bande passante limitée :** Les capteurs opèrent à bas débit pour minimiser l'énergie consommée lors de transfert de données entre les noeuds (Ali, 2011) .
- **Contrainte d'énergie, de stockage et de calcul :** C'est la caractéristique la plus importante dans RCSF car chaque capteur du réseau dispose de faibles ressources énergétiques (batterie). Pour prolonger la durée de vie du réseau, il doit minimiser la dépense énergétique à chaque noeud. Ainsi, la capacité de stockage et la puissance de calcul sont limitées dans un capteur (Benahmed, 2011).

1.2.6 Domaines d'application dans les RCSF

À cause de la disponibilité d'une grande variété de capteurs disponibles (thermique, optique, vibrations, etc.) et de la miniaturisation des micro-capteurs, et de l'utilisation de la technologie de communication sans fil. Permet d'appliquer les réseaux de capteurs dans certains domaines, parmi lesquels :

- **Domaine militaire :** Les caractéristiques de ce type des réseaux telles que le déploiement rapide, le coût réduit, l'auto-organisation font un outil précieux dans ce domaine. Actuellement, les RCSF peuvent être une partie intégrante dans le commandement, le contrôle, la surveillance, la reconnaissance, la détection des mouvements des ennemis, etc (Bader, 2009).
- **Domaine environnemental :** On peut utilisé les réseaux de capteurs pour détecter des catastrophes naturelles (feux de forêts, tremblements de terre, etc.), ou pour détecter des produits toxiques (gaz, produits chimiques, pétrole, etc.) dans les stations-service ou des zones industrielle (Bader, 2009).

- **Domaine commercial :** Dans ce domaine, les réseaux de capteurs ont également prouvé leur utilité, qui peuvent utilisé pour connaître la position, l'état et l'orientation d'un paquet ou d'une cargaison, dans la surveillance de l'état du matériel, de suivre les processus de production, le contrôle et l'automatisation des processus d'usinage, etc (Bader, 2009).
- **Domaine médicale :** L'utilisation du réseaux de capteurs devient importante dans le domaine médicale, car elle facilite le diagnostic des maladies en surveillant constamment les patients et en collectant de meilleures informations physiologiques (Bader, 2009).

1.2.7 Les problèmes existant dans les RCSF

Parmi les problèmes posés sur réseaux de capteurs :

- **La localisation :** La localisation consiste à sélectionner chaque noeud pour estimer sa position dans un repère le problème c'est que les réseaux de capteurs sont déployés aléatoirement dans des zones d'intérêt, et l'intervention humaine ne peut pas l'organiser (Boushaba, 2007).
- **Énergie :** Est une problématique nécessaire dans les RCSFs. L'énergie d'un capteur est limitée, et la recharge des sources d'énergie est très coûteuse et parfois impossible. Il faut donc que les capteurs économisent au maximum l'énergie car la durée de vie d'un capteur dépend grandement de la durée de vie de la batterie (KHALILI, BOUCHRA, KADDI et al., 2019).
- **Couverture :** Le problème de couverture est que la durée de vie du réseau insuffisante pour couvrir la zone d'intérêt pendant une période plus longue. Pour cela il faut augmenter la durée de vie du réseau (Kerkar et al., 2008).

1.3 La sécurité dans les réseaux de capteurs sans fil

La sécurité est un problème complexe dont souffrent les réseaux de capteurs, car ils sont vulnérables à diverses attaques en raison de leurs caractéristiques et de leurs applications. Dans cette section, on parle sur les vulnérabilités, les défis de sécurité, les classifications des attaques, les mécanismes et les approches de surveillance.

1.3.1 Terminologies

On commence par la description de quelques terminologies utilisées dans le domaine de la sécurité informatique avant de passer aux différentes techniques de sécurité avancées.

- **Menace :** La possibilité de voir une menace informatique plus ou moins grave se transformer en événement réel entraînant une perte (Aghiles, 2013).
- **Vulnérabilité :** C'est un point faible d'un système qui permet à un attaquant de porter atteinte à l'intégrité de ce système à son fonctionnement normal ou à la sécurité ou à l'intégrité des données qu'il contient (Lamine, 2008).
- **Risque :** Cause potentielle d'un incident, qui pourrait entraîner des dommages sur les systèmes informatiques, les réseaux...etc. Si cette menace se concrétisait (Louiza, 2012).
- **Attaque :** Est tout incident qui entraîne l'accès non autorisé à des applications, des données, des réseaux ou des appareils informatiques dans le but de causer des dommages (Cayirci et Rong, 2008).
- **Sûreté :** La sûreté est un ensemble de mesures utilisées pour prévenir les activités humaines malveillantes, pour protéger les biens et les personnes contre les effets du vol ou l'agression (Benahmed, 2011 ; Bettahar et Challal, 2008).

1.3.2 Les objectifs de sécurité

La sécurité doit générer les objectifs suivants :

- **La confidentialité :** Est la garantie que le contenu échangé entre les noeuds capteurs ne peut être consulté et compris que par ceux qui sont autorisés à y accéder (ATHMANI, 2018).

- **L'intégrité de données :** Il doit fournir des mécanismes permettant aux noeuds de communications de détecter qu'un paquet n'a pas été trafiqué, altéré ou modifié pendant la transmission (ATHMANI, 2018).
- **L'authentification :** L'authentification fiable doit effectuée la vérification d'identité pour assurer que le demandeur soit une entité légitime et autorisée à récupérer ce service ou information. Et les capteurs doivent s'assurer que les données reçues proviennent d'une source identifiée (ATHMANI, 2018).
- **La disponibilité :** Est la capacité permanente d'accéder à tous les services que le réseau fournit à chaque membre du réseau (ATHMANI, 2018).

1.3.3 Vulnérabilités des réseaux de capteurs sans fil

- **Technologie sans fil :** La vulnérabilité des réseaux sans fil qu'un pirate peut obtenir des données ou tout ce qui est transmit sans fil (Lamine, 2008).
- **Fonctionnement sans surveillance :** Les noeuds capteurs sont souvent déployés dans des endroits inaccessibles comme des champs de bataille, au fond de l'océan, à l'intérieur de grandes machines, ils doivent donc fonctionner sans surveillance dans n'importe quelle zones (Lamine, 2008).
- **Les mécanismes de routage :** Le routage est une méthode d'acheminement des informations vers la bonne destination via un réseau de connexion donné. La plupart des protocoles de routage sont assez simples et donc assez vulnérables aux attaques (Lamine, 2008 ; Lynda, 2011).

1.3.4 Les défis de sécurité dans RCSF

La sécurité pour les réseaux de capteurs est un problème difficile pour les raisons suivantes :

1. **Les défis liés à la communication sans fil :** Un risque de communication sans fil est qu'un attaquant a une capacité d'intercepter et déchiffrer le trafic des utilisateurs. Pour être considéré comme totalement sécurisé il doit assurer la confidentialité, l'intégrité et l'authentification (Lamine, 2008).

2. **Les défis liés à la capacité de calcul et de traitement :** Les ressources de calcul et de mémoire des noeuds sont faibles. La contrainte la plus forte aux capacités d'un noeud de capteur est l'énergie. Le plus grand défi dans le domaine des réseaux de capteurs reste la conception de protocoles, qui minimisent la puissance pour maximiser la durée de vie du réseau (Aghiles, 2013).

3. **Les défis liés au problème d'énergie :** L'énergie est un problème important dans les réseaux de capteurs, Donc on doit minimiser la consommation de l'énergie tout en maximisant les performances de sécurité (Lamine, 2008).

1.3.5 Les attaques dans les réseaux de capteurs sans fil

Connaître les classes et les types d'attaques est essentiel pour concevoir une défense solide contre elles.

1.3.5.1 Classification des attaques

1. **Selon l'origine :** Il y a deux catégories distinguées selon l'origine : attaque interne et externe.

   - **Attaque externe :** Effectué par des noeuds qui ne sont pas dans le réseau ou n'a pas la permission d'accès, pour diffuser des informations de routage erronées (Louiza, 2012).
   - **Attaque interne :** Effectué par un noeud interne malveillant. Sont la menace la plus sévères pour perturber la fonctionnalité du réseau (Louiza, 2012).

2. **Selon la nature :** Un attaquant pouvant opérer au niveau des données échangées entre les noeuds, on peuvent être classées ces attaques en deux catégories : actives et passives.

   - **Attaque passive :** Cette attaque est facile à réaliser et difficiles à détecter L'attaquant ne modifie pas les paquets échangés, il se limite à écouter la collecte des données et l'analyse du trafic échangé, cela permet à un attaquant d'intercepter le contrôle et d'observer les données entre les noeuds (ATHMANI, 2018).
   - **Attaque active :** Elle participe à tout le trafic quelques soient les paquets de contrôle ou de données, dans ce cas elle peut ajouter son propre trafic pour modifier, supprimer des messages et même falsifier les informations de routage (Cayirci et Rong, 2008).

1.3.5.2 Description de quelques attaques

Les réseaux de capteurs sans fil peuvent être vulnérables à plusieurs attaques. Parmi eux :

- **Attaque de brouillage (Jamming) :** C'est une attaque de type déni de Service (DoS), qui empêche d'autres noeuds d'utiliser le canal pour communiquer en utilisant un appareil puissant de brouillage (ZERADNA et CHORFI, 2022).

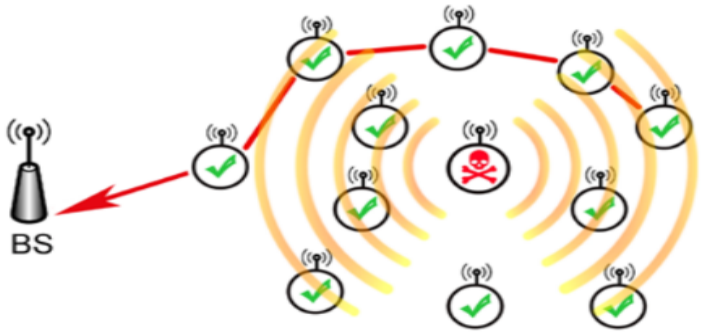

FIG. 1.7 : Attaque Jamming (KHELIFA BENAHMED et SEDDIKI, 2018)

- **Attaque de trou noir (Blackhole) :** Un noeud malicieux ne transmet pas et n'informe pas les autres noeuds des données qu'il reçoit (KHELIFA BENAHMED et SEDDIKI, 2018).
- **Attaque Sybil :** C'est l'une des attaques les plus dangereuses dans RCSF. Le noeud malicieux présente différentes identités de plusieurs noeuds du réseau pour dégrader l'intégrité des données (DOUMI, 2018).

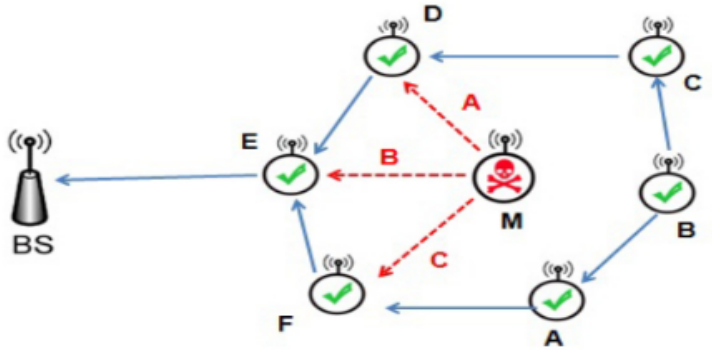

FIG. 1.8 : Attaque Sybil (KHELIFA BENAHMED et SEDDIKI, 2018)

- **Attaque de trou de puits (Sinkhole) :** Le noeud malicieux utilise une puissance de transmission élevée afin d'attirer tout le trafic vers lui permettant de contrôler la plus part des données circulant dans le réseau (Doumi, 2018).

1.3.6 Les mécanismes de prévention

1.3.6.1 La cryptographie

Elle se définit comme la science qui permet de transformer des informations "non chiffrées" en chiffrement (encodage). C'est-à-dire transformer les informations incompréhensibles et récupérer les informations originales à partir de ces informations cryptées (Athmani, 2010). D'abord il est utile de définir la notion de clé qui sera utilisés dans cette partie.

- Clé : Pour obtient un message crypté secret on se base sur une information secrète appelée la clé, qui est un paramètre que doit être utilisé avec les algorithmes pour produire le message crypté (Bettahar et Challal, 2008).

1.3.6.2 Les outils cryptographiques

1. **Le chiffrement :** Est un système cryptographique qui transforme un message clair en un message crypté à l'aide de clé. Selon cet usage, il existe deux types de chiffrement : symétrique ou asymétrique (Athmani, 2010 ; Bettahar et Challal, 2008).
    - **Le chiffrement symétrique :** Il partage la même clé entre l'émetteur et le récepteur. Il utilise Cette clé par l'émetteur pour chiffrer le message et par le récepteur pour le déchiffrer à l'aide d'un algorithme de chiffrement symétrique (Bettahar et Challal, 2008).
    - **Le chiffrement asymétrique :** Deux clés asymétriques sont générées : Une clé publique qui est distribuée à tout le monde et une clé privée qui est gardée secrète chez le récepteur. Chaque message chiffré avec la clé publique ne peut être déchiffré qu'avec la clé privée (Bettahar et Challal, 2008).
2. **Le code dauthentification de message MAC :** C'est une mécanisme de cryptage qui vérifie l'authenticité de l'origine et de l'intégrité des données comme toute autre fonction de hachage.

Pour assurer l'authenticité de l'origine, doit partager une clé symétrique entre l'émetteur et le récepteur, qui sera utilisé par l'émetteur pour calculer un MAC qui est la preuve d'authenticité. Le récepteur utilisera la même clé privée pour calculer un MAC. On compare entre les deux valeurs de MAC si elles sont égales alors le message et l'origine sont authentiques. Sinon, l'origine n'est pas authentique (Bettahar et Challal, 2008).

3. **Certificat électronique :** Appelé aussi certificat numérique, c'est une structure de donnée signée numériquement qui vérifie l'identité du propriétaire de la clé privée correspondant à la clé publique.

   Peut être considéré comme une carte d'identité numérique liée à une clé publique contenant certaines informations. À l'aide d'une clé publique qui connue de manière sécurisée elle peut être signée numériquement par une autorité de certification qui approuvée par les utilisateurs. Le récepteur peut déchiffrer les signatures après avoir vérifié la signature apposée sur le certificat à l'aide de la clé publique (Bettahar et Challal, 2008).

1.3.7 Les travaux de détection

1.3.7.1 Système de détection d'intrusion IDS

Ce système, généralement composé de logiciel et de matériel, a pour mission de détecter les tentatives d'intrusion. Il est destiné à analyser de certaines informations afin de détecter des activités malveillantes ou suspectes sur une cible analysée (un réseau ou un hôte). Peut avoir connaissance des tentatives d'intrusion réussies et échouées (Batouche, Saci et al., 2015 ; Embarka et Selyna, 2017).

1. **IDS basé sur la signature :** Il est basé sur une bibliothèque de descriptions d'attaques (signatures) qui utilisées dans les systèmes de détection d'intrusion, il analyse chaque événement dès qu'une alerte soit est émise immédiatement après la détection de la signature, il se révèle efficace uniquement si la base de signatures est régulièrement maintenue à jour (Batouche, Saci et al., 2015).

2. **IDS basé sur l'anomalie :** Pour illustrer les écarts de comportement possibles un modèle de référence a été créé montrant le comportement de l'entité surveillé en situation de fonctionnement normale. Ce modèle permet de comparer entre le comportement de l'entité surveillée et son modèle de référence. Un comportement qui ne fait pas partie du schéma normal est classé comme une anomalie indiquant une intrusion ou une tentative d'intrusion (Batouche, Saci et al., 2015).

1.3.7.2 IDS basé sur la confiance et réputation

1. **Définition de la confiance (Trust) :** Croyance spontanée ou acquise des valeurs morales, affectives, professionnelles... au début, la confiance en cette personne sera limitée, et augmentera ou diminuera au fur et à mesure que les relations de travail se développent. La même chose s'applique à RCSF, la relation entre les noeuds soit il augmente ou il diminue selon le comportement de chaque noeud avec les autres noeuds du réseau (Barbara Schaetti, 2017 ; Momani, 2008).

2. **Confiance direct/indirect :**

   - **Confiance directe :** Elle consiste en des transactions directes dans une période. La qualité des réponses(des fausses informations) entre les noeuds est le résultat de l'examen de la confiance dans la communication (Grandison et Sloman, 2000).
   - **Confiance indirect :** Elle est complètement éloigné des relations directes, elle ne se contente que du jugement à travers les opinions des autres. Nous ne pouvons pas être assez sûre de la qualité de la confiance (Barbara Schaetti, 2017).

3. **Caractéristique de la confiance :** La confiance a des caractéristiques qui sont :

   - **Subjective :** Le noeud basé sur les observations et les preuves fournies par les autres noeuds dans une situation donnée (Momani, 2008).
   - **Non transitive :** Si un noeud A fait confiance au noeud B et que B fait confiance au noeud C, alors le noeud A peut ou non faire confiance au noeud C (Momani, 2008).
   - **Asymétrique :** Le noeud A fait confiance au noeud C, mais cela ne signifie pas que le noeud C fait confiance au noeud A (Momani, 2008).
   - **Dynamique :** La confiance change de manière dynamique au fil du temps (Momani, 2008).
   - **Réflexive :** Le noeud se fait confiance (Momani, 2008).

4. **Système de confiance à base du certificat :** Les modèles de confiance basés sur la certification visent à d'établir des relations de confiance entre les noeuds en fonction du certificat pour indiquer qu'un noeud est déjà authentifié dans le système et peut être approuvé (Aivaloglou, Gritzalis et Skianis, 2008 ; Omar, Challal et Bouabdallah, 2012).

5. **Système de confiance à base du comportement :** Les modèles de confiance comportementaux évaluent le comportement des noeuds à travers la coopération

des noeuds voisins. L'objectif est d'isoler les noeuds qui se comportent de manière malveillante (Aivaloglou, Gritzalis et Skianis, 2008).

1.3.8 Les approches de surveillance utilisés dans RCSF

On peut citer quatre approches dans un système de détection d'intrus adapté pour les réseaux de capteurs sans fil :

1. **L'approche centralisée :** Le seul responsable dans cette approche c'est la station de base qui effectue tous les contrôles de sécurité et la détection des intrus et fourniture d'itinéraires sûrs (Athmani, 2010).
2. **L'approche autonome ou distribuée :** Dans cette approche les capteurs détectent le comportement malicieux et il fait toutes les contrôles de sécurité sans avoir besoin de coopérer avec ses voisins ou de la station de base (Athmani, 2010).
3. **L'approche coopératifs :** Dans cette approche, tous les noeuds participent à la détection des tentatives d'intrusions au niveau local et prennent des décisions d'intrusion (Boubiche, 2013).
4. **L'approche hiérarchique ou hybride :** Pour assurer la sécurité du réseau, les capteurs et la station de base travaillent ensembles. Tous les capteurs envoient des informations sur le réseau à la station de base, qui traite ces informations pour prendre des décisions sur la sécurité du réseau (Athmani, 2010).

1.4 Apprentissage automatique (ML)

Peut être défini l'apprentissage automatique comme étant une technologie d'intelligence artificielle qui permet aux machines d'apprendre sans être préalablement spécifiquement programmées à cet effet. En particulier, nécessite de grande quantité de données à analyser sur lesquelles s'entraîner pour apprendre et grandir (Azencott, 2022). L'apprentissage automatique est un champ assez vaste, en va parler sur deux type :

1. **Apprentissage supervisé :** Consiste à créer et entraîner un modèle à partir des données étiquetées. L'apprentissage supervisé peut être utilisé pour deux types de problèmes qui sont : La régression qui évalue les performances de précision concernant les erreurs minimales et la classification qui est classée en fonction de la logique (Amutha, S. Sharma et S. K. Sharma, 2021).

2. **Apprentissage non supervisé :** Consiste à entraîner un modèle à partir des données non étiquetées et regrouper les données similaires. Ce type permet de surmonter les problèmes des RCSFs tels que le routage, l'agrégation de données, les problèmes de connectivité et la détection d'anomalies. Il peut être utilisé pour deux approches : Le regroupement(clustering) et l'association (Amutha, S. Sharma et S. K. Sharma, 2021).

1.5 Conclusion

Dans ce chapitre, on a abordé les différents concepts de base liés aux réseaux de capteurs sans fil, les concepts liés aux mécanismes de sécurité et de surveillance des réseaux et enfin, une présentation des notions de base sur l'apprentissage automatique. Dans le chapitre suivant, on passe en revue quelques façons typiques de la surveillance du réseaux de capteurs sans fil.

Chapitre2

ETAT DE L'ART

2.1 Introduction

La recherche sur la sécurité des réseaux de capteurs et les systèmes de gestion de la confiance a récemment reçu beaucoup d'attention et comprend des recherches sur différentes opérations. Alors, on présente dans ce chapitre des travaux sur la surveillance des RCSF, qui peuvent être divisés en deux parties : des travaux classiques et des travaux basés sur l'apprentissage automatique (ML). Finalement, ce chapitre est terminé par une évaluation de ces travaux.

2.2 Le système de confiance utilisé dans la littérature

Le modèle de confiance comportementale est représenté comme un système composé de plusieurs unités, telles que des unités de surveillance, d'évaluation, de recommandation, de mise à jour et d'intégration. On définit la responsabilité de chaque unité :

1. **Unité de surveillance :** elle fournit des données aux unités d'évaluation. elle est connecté à l'interface réseau pour surveiller et recueillir des preuves sur les noeuds cibles (Saidi, 2022).
2. **Unité d'évaluation :** C'est l'unité centrale du système de confiance, elle calcule la confiance directe sur la base des preuves envoyées par l'unité de surveillance (Saidi, 2022).
3. **Unité de recommandation :** Si la valeur de confiance directe entre les noeuds sujet et cible est faible, le noeud sujet demande un recommandation des noeuds voisins. Ces recommandations représentent la réputation du noeud cible dans le réseau, servent à construire une valeur de confiance indirecte entre les noeuds sujet et cibles (Saidi, 2022).

4. **Unité d'intégration :** Elle combine la recommandation et la confiance directe pour générer la valeur de confiance totale, puis envoie le résultat à l'unité de mise à jour de confiance (Saidi, 2022).

5. **Mise à jour de confiance :** Met à jour la valeur de confiance globale en fonction des valeurs actuelles et précédentes. Une fois la confiance mise à jour, elle est comparée au seuil de confiance spécifié pour décider si le noeud cible est fiable ou non (Saidi, 2022).

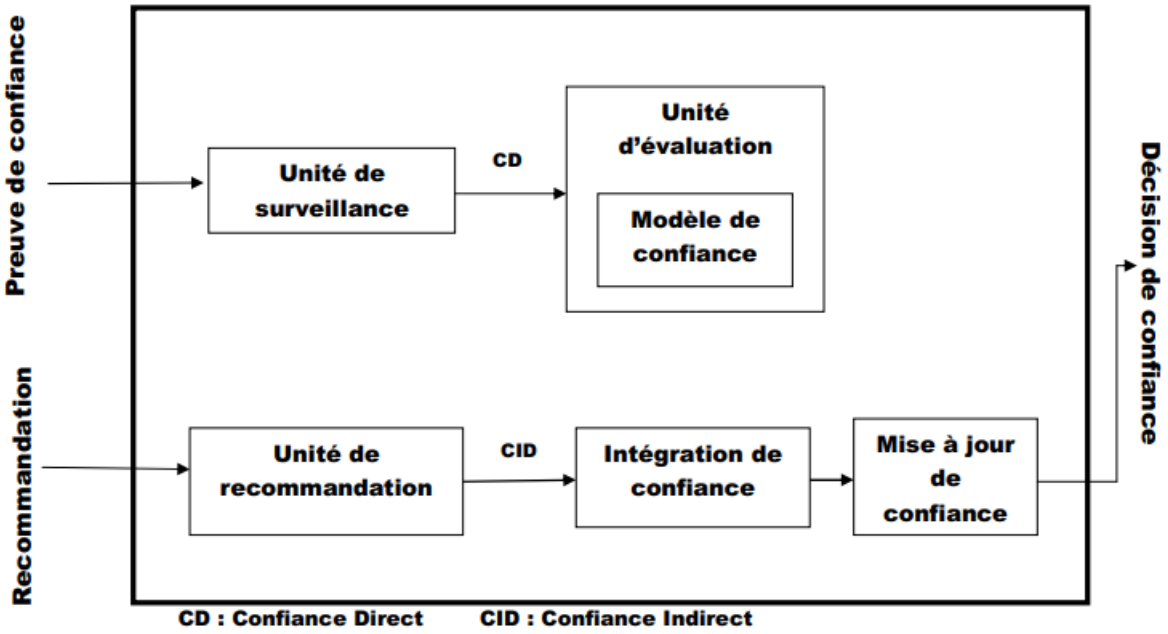

Fig. 2.1 : Système de confiance (Saidi, 2022)

2.3 Travaux connexes pour la surveillance des RCSF

Travaux classique

- **STMWSN (Sociopsychological Trust Model for Wireless Sensor Networks)**

  Heena Rathore, Venkataramana Badarla et George KJ ont présenté un modèle de confiance inspiré à partir de système de défense immunitaire (STMWSN) 2.2 . Le modèle proposé est divisé en deux composants : un composant socio-psychologique qui sert à renforcer la confiance d'un noeud, et un composant immunitaire, qui sert à supprimer un noeud frauduleux lorsque sa confiance diminue. Selon les auteurs, la confiance peut être évaluée sur trois facteurs : la compétence, la bienveillance et l'intégrité. Le modèle a été implémenté sur la plate-forme Lab-VIEW et les résultats justifient la fiabilité de ce modèle (Rathore, Badarla et George, 2016).

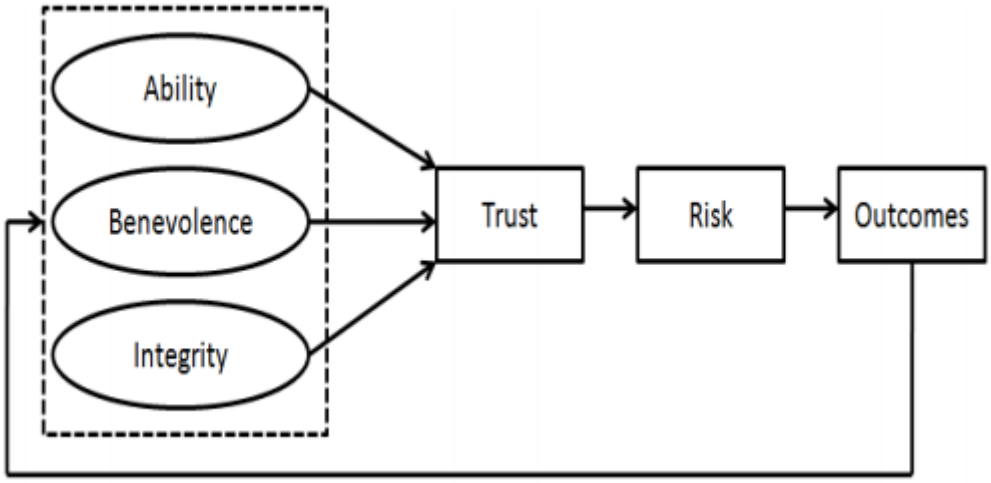

Fig. 2.2 : Modèle de confiance STMWSN (Rathore, Badarla et George, 2016)

- **NBBTE (A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory)**

  Renjian Feng, Xiaofeng Xu, Xiang Zhou et Jiangwen Wan ont proposé un algorithme NBBTE basé sur la théorie de Dempster-Shafer pour évaluer la confiance entre les noeuds dans les réseaux de capteurs sans fil (RCSF). Ils ont utilisé différents caractéristiques de communications et de données pour calculer la valeur de confiance directe et indirecte à l'aide des règles de combinaison révisées de Dempster pour obtenir la valeur de confiance finale d'un noeud. Les résultats de la simulation montrent que NBBTE peut détecter efficacement les noeuds malveillants (Feng, Xu et al., 2011).

- **BTMS (A Credible Bayesian-Based Trust Management Scheme for Wireless Sensor Networks)**

  Renjian Feng, Xiaona Han, Qiang Liu, et Ning Yu ont présenté un schéma de gestion de la confiance basé sur la théorie bayésienne (BTMS) pour les Réseaux de capteurs sans fil. La valeur de confiance totale est calculée selon les données de confiances directes et indirectes, qui sont calculées sur la base de la théorie bayésienne. La confiance indirecte est calculée uniquement lorsque la confiance directe est très incertaine et la théorie de l'entropie est utilisée pour estimer l'incertitude. La plate forme Matlab est adoptée pour la simulation et l'évaluation des performances de l'approche proposée. Les résultats montrent que le modèle BTMS a une forte capacité à évaluer la confiance et la résistance aux attaques (On-Off Attack, Bad Mouthing Attack et Ballot Stuffing Attack) (Feng, Han et al., 2015).

- **EDTM (An Efficient Distributed Trust Model for Wireless Sensor Networks)**

  Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu et Mohsen Guizani ont introduit une approche de sécurité basée sur un modèle de confiance distribuée pour le RCSF (EDTM) 2.3. Ce modèle calcule la confiance directe à partir de la confiance de communication, d'énergie et de donnée. Pour la confiance indirecte, ils ont estimé le nombre des paquets de recommandation reçus par les autres capteurs dans le réseau. L'expérimentation est réalisée sur Matlab et les résultats obtenus montrent que l'EDTM est un modèle de confiance efficace et résistant aux attaques (Jiang et al., 2014).

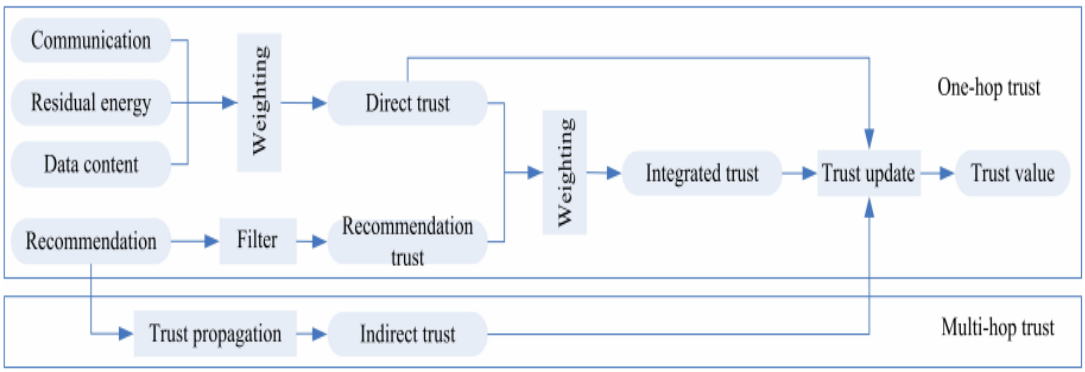

Fig. 2.3 : La structure EDTM (Jiang et al., 2014)

- **NTMS-DS (A novel trust management scheme based on DempsterShafer evidence theory for malicious nodes detection in wireless sensor networks)**

  Wei Zhang, Shiwei Zhu, Jian Tang et Naixue Xiong ont produit un schéma de gestion de la confiance basé sur la théorie de Dempster-Shafer (NTMS-DS) pour détecter les noeuds malicieux dans les RCSFs. La valeur de confiance d'un noeud dans ce schéma est calculée sur la base des informations collectées à partir des noeuds capteurs voisins. Un modèle de confiance est créé pour estimer la valeur de la confiance directe et indirecte, puis calculer la confiance totale. À l'aide de la plate-forme Matlab, ils ont construit une topologie hiérarchique de RCSF et simulé la phase de communication. Selon les résultats de la simulation, le taux de détection des noeuds malicieux est supérieure à 80% et le taux de données agrégées est 95% (W. Zhang et al., 2018).

- **TEM-CM (Trust evaluation method for clustered wireless sensor networks based on cloud model)**

  Tong Zhang, Lisha Yan et Yuan Yang ont proposé une méthode d'évaluation de la confiance basée sur un modèle mathématique appelé cloud model 2.4 pour les RCSFs. Le modèle proposé utilise l'espérance mathématique et l'entropie pour l'évaluation de la confiance des noeuds. Le modèle proposé prendre en considération le facteur de communication, le facteur de message et le facteur d'énergie qui peuvent affecter la valeur de confiance du noeud du capteur. L'expérimentation de la méthode est réalisée sur la plate-forme de simulation de réseau OMNET, et la simulation est basée sur la structure en cluster du protocole LEACH. Donc, comme résultats un taux de détection de 80% à 99% pour diverses attaques persistantes (T. Zhang, Yan et Yang, 2018).

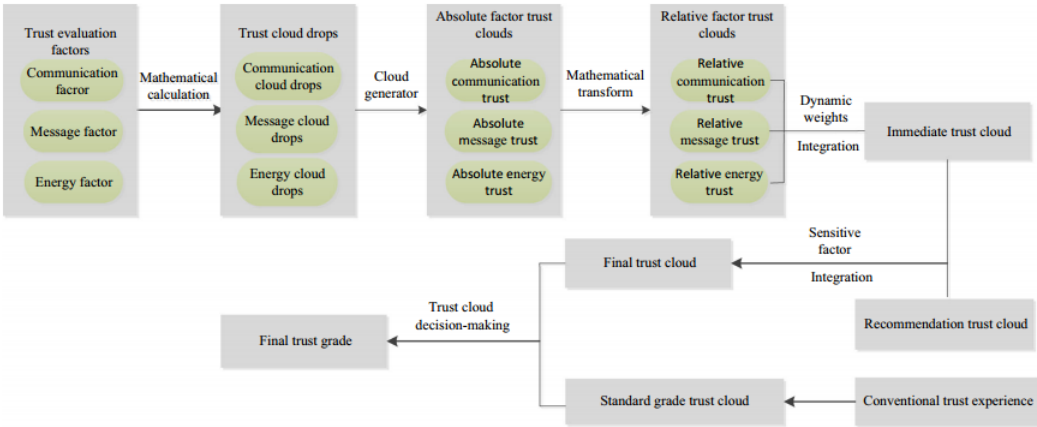

Fig. 2.4 : L'architecture de la méthode d'évaluation de la confiance (T. Zhang, Yan et Yang, 2018)

Travaux basés sur l'apprentissage automatique

- **TAAPML (Trust aggregation authentication protocol using machine learning for IoT wireless sensor networks)**

  Santhanakrishnan et Annapurani ont proposé un protocole d'authentification d'agrégation de confiance utilisant l'apprentissage automatique (TAAPML) 2.5 pour les réseaux de capteurs sans fil IoT(Internet of Things). L'objectif est de concevoir un protocole d'authentification léger pour une consommation d'énergie réduite, concevoir une technique de détection distribuée et réduire la charge de calcul. la valeur de confiance est évaluée par la valeur de confiance comportementale (BT), qui est calculée en fonction du taux de réussite des paquets RREQ (RQSR), du taux de réussite des paquets RREP (RPSR), du taux de transfert de données (DFR), du taux de livraison des paquets (PDR). et par la valeur de confiance de données (DT) qui est calculée avec la capacité résiduelle attendue de la batterie (EC) et la valeur différentielle absolue (AD). La valeur de seuil de confiance est déterminée de manière adaptative à l'aide de la technique d'apprentissage SVM à partir des données de trafic collectées. Le simulateur utilisé pour cette technique est NS2, et ses performances sont évaluées en fonction du taux de livraison des paquets, du délai, de l'énergie résiduelle et de la surcharge de calcul (Chinnaswamy et Annapurani, 2021).

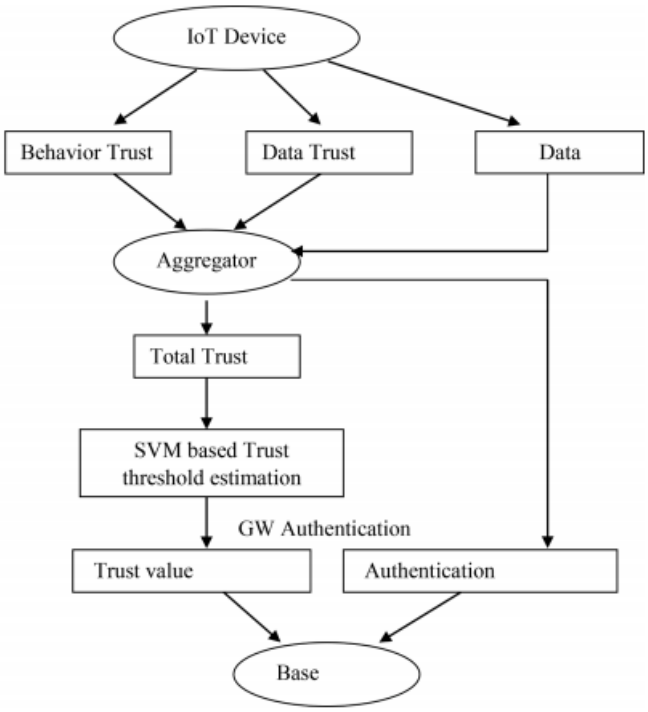

Fig. 2.5 : La structure de TAAPML (Chinnaswamy et Annapurani, 2021)

- **IDS-KNN (A new intrusion detection system based on KNN classification algorithm in WSN)**

  Wenchao Li, Ping Yi, Yue Wu, Li Pan et Jianhua Li ont proposé un système de détection d'intrusion basé sur l'algorithme de classification KNN dans un réseau de capteurs sans fil. Ce système détecte l'attaque par inondation et détecte les noeuds malveillants dans le RCSF. Ce système utilise des noeuds GAINZ Zigbee. Ils ont effectué plusieurs tests pour étudier l'effet d'une attaque par inondation (flodding). Selon les résultats de la simulation, le taux de détection moyen est de 90% et le taux moyen de fausses alarmes est de 1,5% (Li et al., 2014).

- **ML-TCM (Machine Learning Based Trust Computational Model for IoT Services)**

  Jayasinghe et des autres ont proposé un modèle de confiance basé sur l'apprentissage automatique pour les services IoT (Internet of Things). Les caractéristiques utilisées pour former le modèle sont : Relation de co-localisation (CLR), Relation de co-travail (CWR), Mutualité et Centralité (MC), Coopérativité-Fréquence-Durée (CFD) et Récompense. L'algorithme a été divisé en deux parties : la première partie est basée sur l'algorithme k-means pour regrouper les interactions selon les caractéristiques précédentes et la deuxième partie basée sur la technique SVM, qui permet d'identifier le meilleur niveau de seuil qui sépare les interactions de confiance . Les résultats de la simulation montrent la capacité et la précision de l'algorithme à identifier les interactions de confiance fiables (Jayasinghe et al., 2018).

- **EEML-DOS(An extended evaluation on machine learning techniques for Denial-of-Service detection in Wireless Sensor Networks)**

  Silvio E, Juliano F et Vagner E ont présenté une évaluation approfondie des techniques d'apprentissage automatique supervisées(Farthest First, Expected Maximization et KMeans) et non supervisées(Random Tree, REPTree et J48) pour détecter les attaques(Flooding, Grayhole, Blackhole) de déni de service (DOS) dans les réseaux de capteurs sans fil. L'évaluation est basée sur des échantillons normaux et d'attaque de l'ensemble de données WSN-DS décrit dans la figure 2.6. Cet ensemble est réduit par des algorithmes de sélection de caractéristiques (Information Gain (IG), Gain Ratio (GR) et OneR) 2.7. Les résultats indiquent que les techniques supervisées présentent de meilleures performances que les non supervisées (S. E. Quincozes, Kazienko et V. E. Quincozes, 2023).

Feature	Description
1. Node ID	Sensor node unique identification
2. Time	Simulation timestamp
3. Is_CH	*Cluster Head* (CH) flag
4. Who_CH	Who is CH in the current run
5. Distance_to_CH	Distance between the node and CH
6. ADV_CH_Sent	Count of advertising CH sent
7. ADV_CH_Received	Count of advertising CH messages received
8. Join_REQ_Sent	Count of join requests sent;
9. Join_REQ_Received	Count of join request received by CH;
10. ADV_SCH_Sent	Count of TDMA messages sent
11. ADV_SCH_Received	Count of TDMA messages received
12. Rank	Node rank in TDMA scheduling
13. Data_Sent	Count of packets sent from node to CH
14. Data_Received	Count of received packets from CH
15. Data_Sent_To_BS	Count of packets sent from CH to BS
16. Distance_CH_To_BS	Distance between CH and BS
17. Send_Code	Cluster send code
18. Energy_Consumption	Amount of energy consumed in last turn

FIG. 2.6 : Les caractéristiques globales du WSN-DS (S. E. QUINCOZES, KAZIENKO et V. E. QUINCOZES, 2023)

	IG	GR	OneR
Blackhole	3, 6, 12, 13, 18	3, 6, 9, 10, 13	3, 4, 6, 7, 18
Grayhole	3, 6, 12, 13, 18	3, 6, 8, 12, 13	3, 6, 7, 15, 18
Flooding	3, 6, 7, 13, 16	3, 6, 12, 13, 17	4, 6, 7, 8, 17

FIG. 2.7 : La sélection de caractéristiques basée sur IG, GR et OneR (S. E. QUINCOZES, KAZIENKO et V. E. QUINCOZES, 2023)

- **EES-WCA (energy efficient and secure weighted clustering for WSN using machine learning approach)**

  Gulganwa et Jain ont présenté un algorithme de clustering pondéré sécurisé et économe en énergie (EES-WCA) pour les réseaux de capteurs. EES-WCA est une combinaison d'EE-WCA et d'un système de détection d'intrusion centralisé (IDS) 2.8 basé sur l'apprentissage automatique . L'objectif est de créer un algorithme intelligent sur la station de base pour surveiller les différentes activités des noeuds capteurs. Cet algorithme crée des clusters de réseau pour optimiser la consommation d'énergie du réseau. Après cela, il analyse le trafic réseau au niveau de la station de base pour identifier les noeuds malveillants du réseau. Des échantillons de trafic sont utilisés avec deux algorithmes d'apprentissage automatique : Support Vector Machine (SVM) et Multi-Layer Perceptron (MLP) Pour détecter un réseau d'attaque. L'implémentation a été réalisée avec le simulateur NS2.35. L'analyse expérimentale montre que le système offre une sécurité suffisante contre différents types d'attaques de réseau et a une efficacité énergétique (GULGANWA et JAIN, 2022).

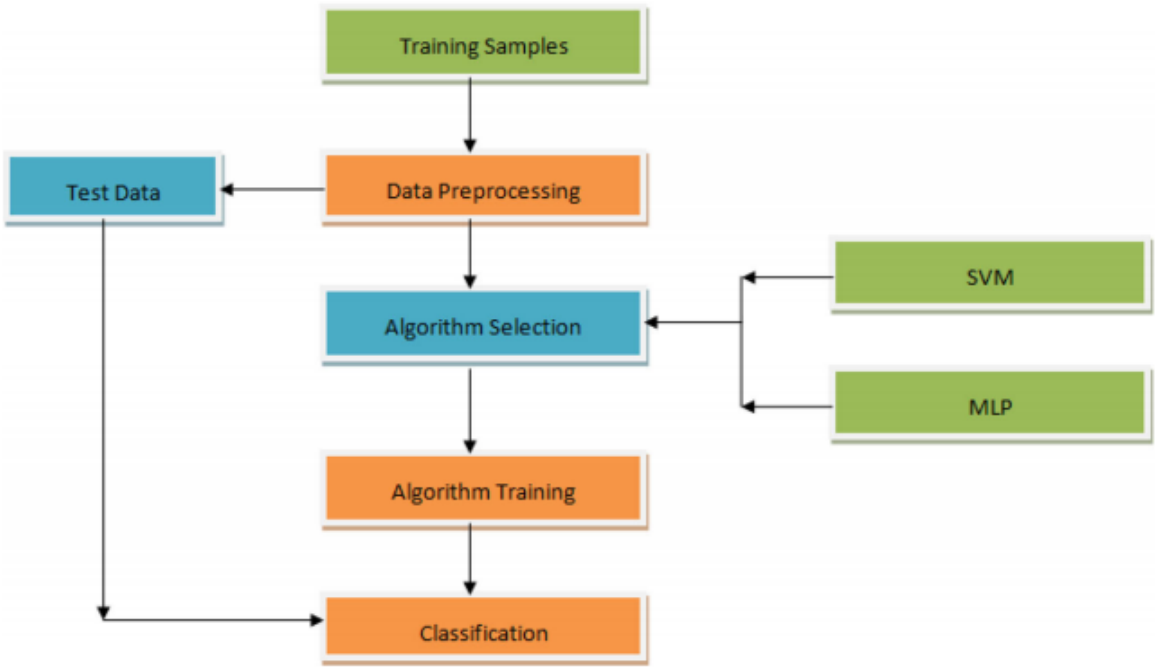

FIG. 2.8 : Le système IDS proposé (GULGANWA et JAIN, 2022)

- **IDS-BLR (An Intrusion Detection System for Constrained WSN and IoT Nodes Based on Binary Logistic Regression)**

  Christiana et Vasos ont présenté et évalué un système de détection d'intrusion léger mIDS basé sur un modèle de régression logistique binaire (BLR) pour détecter les attaques (Forward et Blackhole) dans chaque noeud contraint. Le système mIDS utilise des données bénignes et malveillantes de la couche réseau de routage de chaque noeud, et un outil de surveillance du temps d'exécution (RMT) est utilisé pour collecter ces données et surveiller l'activité des capteurs locaux. Le simulateur COOJA a été utilisé pour analyser le modèle BLR. Selon les résultats, les attaques avec la précision la plus faible sont les attaques Forward. Et en passant, si une attaque Blackhole est présente et attire du trafic vers un noeud malveillant, les noeuds malveillants sont plus faciles à détecter (IOANNOU et VASSILIOU, 2018).

2.4 Critères d'évaluation des approches proposées

On veut évaluer les approches précédentes selon les critères suivants :

1. **Type de confiance :** La relation de confiance dans les RCSFs est la combinaison de trois types de confiances :
   - **La confiance liée à la communication :** C'est la confiance liée aux facteurs de communication comme le nombre de paquets envoyés, le nombre de paquets reçus.
   - **La confiance liée aux données :** c'est la confiance liée à la précision des informations envoyés par les capteurs. Elle est généralement utilisé pour détecter les capteurs qu'ils envoyé des faux données.
   - **La confiance liée à l'énergie :** C'est la confiance liée à la consommation d'énergie. Elle est utilisé pour détecter les noeuds égoïstes qu'ils ne participent pas aux l'échange de données dans le réseau.
   - **La confiance liée à la mobilité :** La confiance de mobilité indique la façon dont le noeud du capteur modifie sa trajectoire et sa vitesse par rapport au reste des autres capteurs.
2. **Type de modèle utilisé :** Représente la méthodologie utilisé pour construire la relation de la confiance par exemple : machine learning, Cloud modèle, théorie bayésienne, théorie Dempster-Shafer.
3. **Objective de modèle :** C'est l'objectif et le but de modèle proposé.
4. **Architecture de réseau :** Type de réseau utilisé hiérarchique ou distribué.
5. **Simulateur :** L'environnement de simulation choisie.

Le tableau 2.1 présente l'évaluation des approches classiques et le tableau 2.2 présente l'évaluation des approches basées sur l'apprentissage automatique.

TAB. 2.1 : Critères d'évaluation d'approches classiques

L'approche proposée	**Méthodologie**	**Objective**	**Architecture**	**CC**	**CD**	**CE**	**CM**	**Simulateur**
STMWSN	Modèle de confiance sociopsychologique	Evaluation de confiance des nœuds capteurs	NM	✔	✔	**X**	**X**	Lab-View
NBBTE	Dempster-Shafer	Détection des nœuds malicieux	NM	✔	✔	✔	**X**	MATLAB
BTMS	Bayésienne Modéle	Evaluation de confiance	NM	✔	**X**	**X**	**X**	MATLAB
EDTM	Modèle de Confiance distribuée	Calculation de la valeur de confiance	Distribuée	✔	✔	✔	**X**	MATLAB
NTMS-DS	Dempster-Shafer	Détection des nœuds malicieux	Hiérarchique	✔	✔	**X**	**X**	MATLAB
TEM-CM	Cloud modèle	Evaluation de confiance	Hiérarchique	✔	✔	✔	**X**	OMNET

CC : Confiance de Communication CD : Confiance de Donnée CE : Confiance d'Energie

CM : Confiance de Mobilité NM : Non Mentionné

TAB. 2.2 : Critères d'évaluation d'approches ML

L'approche proposée	Méthodologie	Objective	Architecture	CC	CD	CE	CM	Simulateur
TAAPML	Technique SVM	Evaluation de confiance pour réduire la consommation d'énergie	NM	✔	✔	✔	**X**	NS2
IDS-KNN	Technique KNN	Détection d'attaque Flooding et des nœuds malicieux	NM	✔	✔	**X**	**X**	NM
ML-TCM	Techniques K-MEANS & SVM	Calculation de la valeur de confiance pour les services IOT	NM	✔	**X**	**X**	**X**	NM
EEML-DOS	Machine learning	Détection des attaques DOS	Hiérarchique	✔	✔	✔	**X**	NM
EES-WCA	Techniques SVM & MLP	Détection des attaques pour optimiser l'énergie	Hiérarchique	✔	**X**	✔	**X**	NS2.35
IDS-BLR	Technique BLR	Détection des attaques	Hiérarchique	✔	✔	**X**	**X**	COOJA
Notre approche	Machine learning	Détection des nœuds malicieux	Distribuée	✔	✔	✔	✔	Python

CC : Confiance de Communication CD : Confiance de Donnée CE : Confiance d'Energie

CM : Confiance de Mobilité NM : Non Mentionné

2.5 Synthèse

D'aprés tous ce que on a vue sur les approches précédentes, la plupart des modèles ont des taux de détection élevés et convergents, par exemple, le modèle STMWSN a un taux de 90%, le modèle KNN a aussi 90% et le modèle TEM-CM a un taux entre 80% et 99%. Mais chaque modèle utilise une méthodologie différente, comme l'approche NBBTE qui utilise la théorie Demphster-Shafer et l'approche BTMS qui utilise la théorie bayésienne.

Il existe des approches qui utilisent la structure hiérarchique, telles que NTMS-DS, TEM-CM, EEC-WCA et IDS-BLR, mais cette structure peut causer des problèmes lorsque le chef de groupe (CH) est attaqué ou compromis, de nombreuses informations de confiance seront perdues.Il existe aussi des approches qui pourraient détecter les attaques, telles que l'approche IDS-KNN qui détecte l'attaque flooding et l'approche IDS-BLR qui détecte les attaques forward et blackhole. Et pour la simulation, la plupart des chercheurs utilisent MATLAB ou développent leurs propres simulateurs.

Pour La confiance, elle est adoptée dans la plupart des travaux de sécurité des RCSF et plusieurs modèles ont été proposés pour modéliser la confiance à savoir des modèles formels ou des modèles basés sur l'apprentissage automatique(ML). Ces modèles n'ont pas pris en compte tous les types de confiance, par exemple : les approches BTMS et ML-TCM évaluent uniquement la confiance dans les métriques de communication. Dans ce cas, le noeud n'est fiable que pour la communication, mais pas pour la détection de données et d'énergie. Et toutes les approches étudiées ne prennent pas la métrique de mobilité comme valeur d'évaluation, ce qui peut poser des problèmes lors du changement d'emplacement d'un noeud. Par conséquent, il est préférable de considérer toutes les métriques d'évaluation. Et même la complexité du modèle doit être étudiée puisque le capteur est équipé avec une faible ressources (mémoire et processeur), surtout pour les modèles de ML.

La plupart des chercheurs se concentrent trop sur l'unité d'évaluation pour produire le système de confiance le plus précis, mais ils ne donnent pas l'importance pour les autres unités (surveillance et recommandation). Et la plupart des approches recommandent de combiner les informations directes avec les informations utilisées, mais nécessitent toujours une manière appropriée de les combiner.

la relation de confiance nécessité un certain degré des interactions et des échanges des messages entre les captures. Ce degré d'interactions doit être étudié puisque il peut affecté les ressources des capteurs (énergie, calcul,...etc).

2.6 Conclusion

Dans ce chapitre, on a discuté de certaines techniques utilisées par les chercheurs dans le domaine de surveillance des RSCF et on a évalué les travaux par des critères. Et pour le chapitre suivant, on propose un modèle de surveillance utilisant une approche d'apprentissage automatique (Machine Learning).

Chapitre3

CONCEPTION ET RÉALISATION

3.1 Introduction

Ce chapitre présente notre modèle proposé et les différents niveaux d'évaluation pour la détection des mauvais comportement dans les réseaux de capteurs sans fil, et discute des résultats de simulation expérimentale.

3.2 Présentation de modèle

On veut détecter les noeuds malicieux (mauvais comportement) dans un réseau de capteurs sans fil avec un modèle de confiance qui est basé sur un architecture distribuée dans la quelle tous les noeuds sont de même niveau.

La figure 3.1 illustre le modèle de confiance proposé composé de trois types des noeuds :

- Noeud sujet : représente le noeud qui initié l'évaluation des autres noeuds.
- Noeud cible : c'est le noeud évalué par le noeud sujet.
- Noeud de recommandation : c'est le noeud qui envoie des recommandations vers les autres.

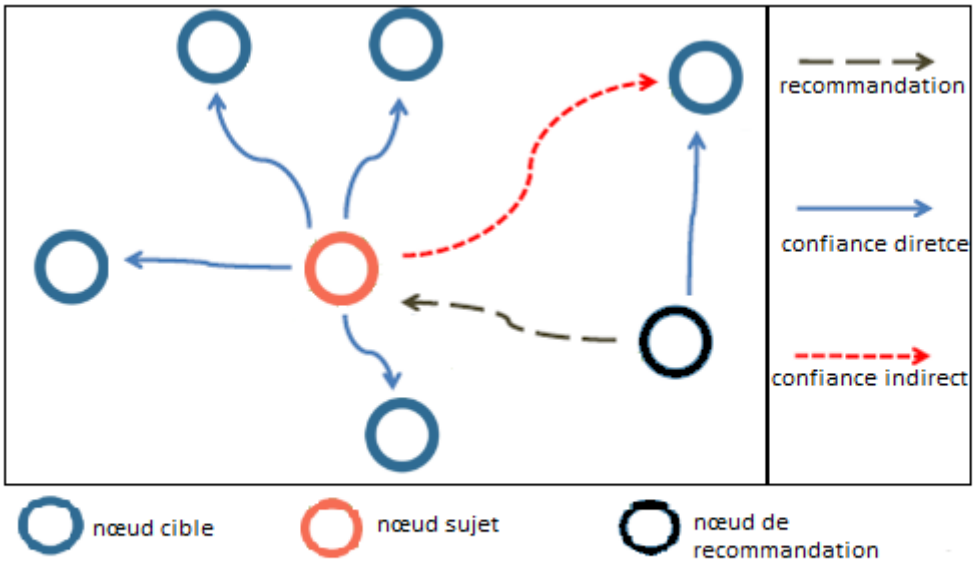

FIG. 3.1 : Conception de réseau

Notre modèle se base sur les hypothèses suivants :

1. Durant de la création de réseau, tous les noeuds sont considérés comme fiable.
2. Les noeuds sont tous homogène avec les mêmes caractéristiques.
3. Afin d'évaluer la confiance entre les noeuds, on suppose que tous les noeuds sont capables de communiquer entre eux via une canal de communication sécurisée.

L'approche est modélisée sous forme d'un graphe bipartite. Le graphe bipartite est un type de graphe composé de deux ensembles des sommets disjoints U et V tels que chaque arête a une extrémité dans U et l'autre dans V. Puisque ce type de graphe permet notamment de représenter des relations binaires, si pour cela on a modélisé les relations de chaque noeud avec ses caractéristiques sous forme de deux groupes des sommets. Un groupe représente les noeuds cibles (voisins) et l'autre groupe représente ces caractéristiques Figure 3.2.

Cette représentation permet de bien évaluer le comportement des noeuds à travers la classification des noeuds avec les mêmes comportements.

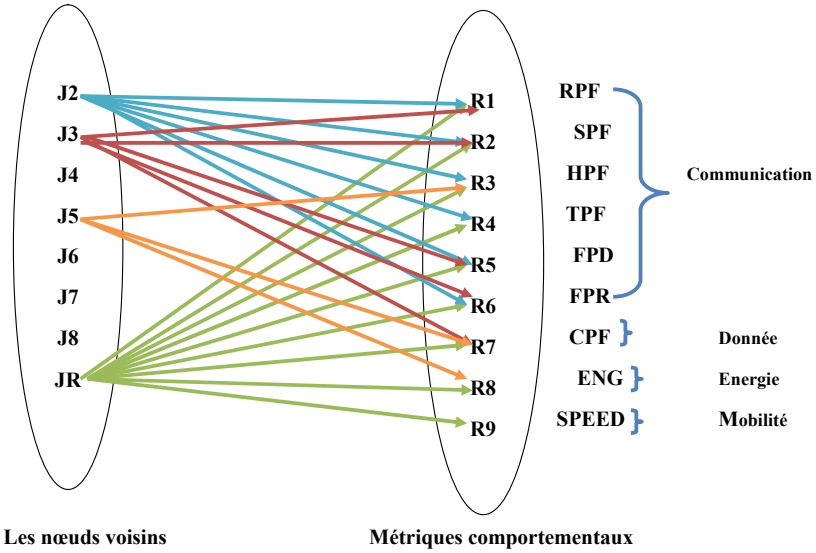

FIG. 3.2 : Evaluation de confiance directe

3.2.1 Architecture de notre modèle

On résume notre travail sur le schéma suivant :

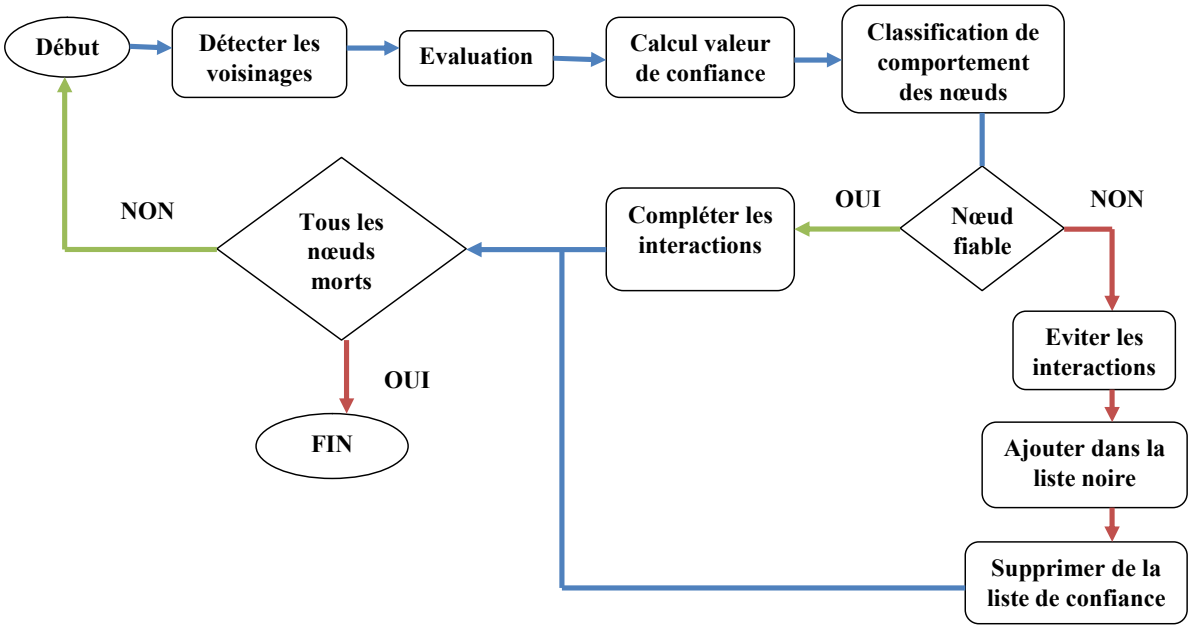

FIG. 3.3 : Achitecture de modèle

3.3 Les critères utilisés pour l'évaluation du comportement d'un noeud

Dans l'évaluation de confiance directe, chaque noeud surveille ses voisins pendant une durée appropriée pour assurer que le comportement du noeud ne dépasse pas les limites acceptables, cette limite est définie comme un intervalle avec des seuils supérieur et inférieur. Par exemple, lorsque un noeud évalue la confiance directe d'un noeud cible, il attribue 1 si le noeud respecte la règle ou 0 si le noeud ne respecte pas la règle (dépasse les limites acceptable). Ces règles reposent sur quatre critères : la communication, les données, l'énergie et la mobilité.

3.3.1 Les critères liés à la communication

Les modèles de communication sont calculés à l'aide des éléments suivants :

- **Le taux de paquets reçus(Factor of received packets rate) :** Le noeud évalue ces voisins et vérifie le nombre de paquets ACK envoyés par le noeud cible, s'il ne dépasse pas les limites du seuil supérieur et inférieur, cela signifie qu'il respecte la règle concernant le débit de paquets reçus. On calcule ce facteur à l'aide de l'équation 3.1.

$$RPFij(t) = \frac{RPij(t) - RPij(t-1)}{RPij(t) + RPij(t-1)} \tag{3.1}$$

  RPF : Signifie le facteur de taux de paquets reçus.

  RP : Signifie le nombre de paquets reçus.

  i etj représentent le noeud et ces noeuds voisins, t et t-1 représentent les paquets reçus à l'instant respectivement.

  ACK : Représente le nombre de paquets bien reçus.

- **Le taux d'envoi réussi des paquets(Factor of seccessful sending packets rate) :** Ce facteur reflète la capacité du noeud à transmettre avec succès des paquets sans les retransmettre. Par conséquent, vous pouvez voir combien de paquets ont été envoyés et combien ont été retransmis. Si les limites de seuil supérieure et inférieure n'ont pas été dépassées, alors ce noeud fonctionne correctement selon la règle de ce facteur. Comme décrit dans l'équation 3.2.

$$SPFij(t) = \frac{SPij(t)}{SPij(t) + SFij(t)} \tag{3.2}$$

SPF : Signifie le taux d'envoi réussi de paquets.

SP : Représente le nombre de paquets envoyés.

SF : Représente le nombre de paquets retransmis.

- **Le taux de disponibilité(Factor of avaibility) :** Afin de découvrir les voisins de chaque noeud, il envoie un message Hello, certains noeuds ne répondent pas aux paquets qu'ils ont reçus ou deviennent inaccessibles. En raison de problèmes de communication ou de conditions environnementales, ce facteur représente la disponibilité du noeud et il est calculé en fonction du nombre de paquets répondus comme décrit dans l'équation 3.3.

$$HPFij(t) = \frac{ACKij}{ACKij + NACKij} \tag{3.3}$$

HPF : Signifie le taux de disponibilité.

ACK : Représente le nombre de paquets bien reçu par j.

NACK : Représente le nombre de paquets qui n'ont pas été reçus par j.

- **Le taux de transmission des paquets(Factor of packets forwarding) :** Le coût de communication très élevé pour un noeud communique avec la station de base (BS), pour cela il envoie des paquets via d'autres noeud jusqu'à il reçu par la BS, afin de minimiser le coût de la communication directe avec la BS. On calcule ce facteur à l'aide de l'équation 3.4.

$$TPFij(t) = \frac{FPij(t) - FPij(t-1)}{FPij(t) + FPij(t-1)} \tag{3.4}$$

TPF : Signifie le taux de transmission des paquets.

FP : Représente le nombre de paquets transmis au temps t, t-1 respectivement.

- **Le nombre de paquets rejetés(Factor of packets dropped) :** Pour dégrader les performances du réseau, les noeuds malveillants se comportent mal en abandonnant les paquets reçus. Ce comportement est généralement le résultat d'une attaque. Ce facteur mesure le nombre de paquets abandonnés par rapport aux paquets reçus comme suit 3.5.

$$FPDij(t) = \frac{NPRij - NPDij}{Totalpackets} \tag{3.5}$$

NPRij : Indique le nombre de paquets reçus par le noeud. NPDij : Indique le nombre de paquets abandonnés par le noeud.

- **Le nombre de paquets envoyés(Factor of packets sent) :** Ce facteur signifie la capacité du noeud à envoyer avec succès les paquets à ses voisins.

$$FPRij(t) = \frac{NPRs}{NPRt} \tag{3.6}$$

NPRs : Représente le nombre des paquets reçus par le noeud sujet.

NPRt : Représente le nombre des paquets envoyés par le noeud cible.

3.3.2 La métrique liée aux données

On a une seule métrique pour évaluer les données.

- **Le facteur de cohérence (Consistency factor) :** Si le noeud reçoit un paquet de ces voisins, il utilise son propre modèle de données pour évaluer ce paquet. Si l'intervalle autorisé n'est pas dépassé, le nombre de paquets reçus de manière fiable augmente. Il calcule le paquet de données non fiable tel que défini dans l'équation 3.7.

$$CPFij(t) = \frac{EPij(t)}{EPij(t) + NEPij(t)} \tag{3.7}$$

EP : Signifie le nombre de paquets de données fiables.

NEP : Signifie le nombre de paquets de données non fiables.

3.3.3 La métrique liée consommation d'énergie

Il est nécessaire de consommer l'énergie efficacement, si un noeud de capteur fonctionne mal, il consommera une puissance anormale, plus les noeuds capteurs deviennent coopératifs plus leur taux de consommation devient similaire. Dans notre modèle, le taux de consommation d'énergie est représenté par des seuils minimum et maximum comme décrit dans les deux équations 3.8, 3.9.

$$ENGi(t) = \frac{Ei(t-1)}{Ei(t)} \tag{3.8}$$

$$ENGj(t) = \frac{Ej(t-1)}{Ej(t)} \tag{3.9}$$

Ei : Signifie l'énergie dépensée par le noeud i au temps t0.

Ej : Signifie l'énergie dépensée par le noeud cible aux instants t0,t respectivement.

3.3.4 La métrique liée à la mobilité

L'utilisation des capteurs mobiles est récemment devenue courante dans de nombreuses applications RCSF. Le modèle de mobilité spécifie comment un noeud modifie sa trajectoire et sa vitesse par rapport au reste des autres noeuds, si le noeud respecte le modèle et la limite de vitesse, donc ça fonctionne normale, si ce noeud se déplace trop lentement ou trop vite par rapport à la majorité des noeuds, alors il est considéré comme anormal car il ne respecte pas la règle de mobilité.

3.4 Algorithme proposée

Pour illustrer le processus d'évaluation de la confiance voici l'algorithme suivante :

Algorithme d'évaluation de la confiance

```
Pour chaque node(i) Faire
    Créer voisin_liste
    Sélection le noeud cible
    Si (le nœud cible ∈ voisin_liste )
        /* commencer l'évaluation de confiance */
        Pour(NB_interaction <= Max_interaction) Faire
            /* calculer les modèles de communications */
            Calcule RPF,SPF,HPF,FPD,FPR et TPF
            /* calculer les modèles des données */
            Calcule CPF,EP and NEPF
            /* calculer le modèle d'energie */
            Calcule ENG
            /* calculer le modèle de mobility */
            Calcule SPEED
            Calcule la canfiance direct
```

Et pour la classification, on a choisie le modèle SVM pour classifier les résultats en deux catégories des noeuds normaux et des noeuds malicieux.

- **SVM :** Est un algorithme d'apprentissage supervisé utilisé pour résoudre des problèmes de classification et de régression. Le but de SVM est de créer une limite de décision entre deux classes qui permet de prédire des éléments à partir d'un ou plusieurs vecteurs de caractéristiques (Huang et al., 2018) .

3.5 Simulation et analyse

Au cour de la simulation, on a utilisé le langage python et on a déployé un réseau de 250 à 2000 noeuds dans un surface de 250 x 250 avec une injection progressive jusqu'à 15% de noeuds malicieux. La configuration utilisée indiquée dans la table 3.1.

Tab. 3.1 : Configuration de la simulation

Configuration	Valeur
Connectivité	50 m
Nombres de capteurs	[250 , 2000]
Taille de la zone	250 x 250 m^2
Énergie initiale du nœud	0.5 J

- **L'environnement expérimental**
  - Processeur : Core(TM) i5-5200U CPU 2.20 GHz
  - Ram : 8,00 Go
  - GPU : 4.0Go
  - SE : Windows 10 Professionnel
  - IDE : Visual Studio Code avec Jupyter Notebook Extension.
  - Anaconda : Une plate-forme intégrée basés sur les langages Python et R qui comprend divers packages utilisés en science des données et en apprentissage automatique.
  - Python (version 3.7.9) : Est un langage de programmation interprété, multi-plateformes, il prend en charge à la fois la programmation objet et procédurale et dispose d'une grande bibliothèque standard. Python est pris en charge sur la plupart des systèmes d'exploitation.

– Scikit-Learn : Est une bibliothèque libre Python destinée à l'apprentissage automatique, elle fournit une collection d'outils puissants pour lapprentissage automatique et de modélisation statistique.

Dans le réseau de capteurs sans fil avec une architecture distribuée, chaque noeud a des voisins qui appartiennent au champ de captage de ce noeud ou sa surface de connectivité. Il va surveiller le comportement de ses voisins et les évaluer durant les interactions selon les critères de confiance qui reposent sur la communication entre les noeuds, le changement d'énergie, les données envoyées/reçues et la mobilité. Afin de classifier le comportement des noeuds, notre modèle est basé sur le dataset publié dans (Saidi, 2021). Ce dataset est présenté dans le tableau 3.2.

Tab. 3.2 : Les caractéristiques utilisées

Métriques comportementale	**Seuils normal**	**Seuils anormal**
Nombre de paquets reçus à l'instant T1(RP1)	[50,60]	[30,40]
Nombre de paquets reçus à l'instant T2 (RP2)	[50,60]	]50,60[
Facteur de taux de paquets reçus (RPF)	[-0.09,0.09]	]-0.09,0.09[
Nombre de paquets envoyés avec succès (SP)	[50,60]	]50,60[
Nombre de paquets retransmis (SF)	0	>= 0,25 % de SP
Taux d'envoi réussi de paquets (SPF)	[0.85,1]	]0.85,1[
ACK	[50,60]	]50,60[
NACK	[0,3]	>= 0,25 \% de NACK
Taux de disponibilité (HPF)	[0.83,1]	]0.83,1[
Nombre de paquets transmis à l'instant T1 (FP1)	[50,60]	[30,40]
Nombre de paquets transmis à l'instant T2 (FP2)	[50,60]	]50,60[
Facteur de taux de paquets transmis(TPF)	[-0.09,0.09]	]-0.09,0.09[

Nombre de paquets reçus(NPR)	[50,60]	]50,60[
Nombre de paquets rejetés(NPD)	0	>= 0,25 % de NPR
Facteur de paquets rejetés(FPD)	[0.66,1]	]0.66,1[
Facteur de paquets envoyés entre le sujet et le nœud cible(FPR)	[0.9,1]	]0.9,1[
Paquets de données cohérents(EP)	[50,60]	]50,60[
Paquets de données incohérents(NEP)	0	>= 0,25 % de EP
Facteur de cohérence(CPF)	[-0.09,0.09]	]-0.09,0.09[
Energie consommée à l'instant T1	[0.01,0.500]	]0.01,0.500[
Energie consommée à l'instant T2	[0.01,0.500]	]0.01,0.500[
Métrique d'énergie(ENG)	[-0.09,0.09]	]-0.09,0.09[
Vitesse maximale	20m/s	>= 20m/s
Vitesse minimale	10m/s	<= 10m/s

Ces critères sont définis comme des intervalles avec des seuils supérieur et inférieur, en donnant la valeur 1 pour les noeuds qui respectent l'intervalle donné et 0 pour les noeuds qui dépassent les limites d'intervalle.

On crée des noeuds de mauvais comportement en modifiant leurs critères, on observe les interactions entre les noeuds de capteurs, puis on extrait les comportements. On compare les valeurs des critères de chaque noeud par les intervalles acceptés et on définit le comportement des noeuds selon la comparaison des noeuds. Les noeuds qui respectent les seuils défini dans le dataset comportent de la même manière et deviennent similaire.

3.5.1 Évaluation de résultat

Pour évaluer les performances de notre modèle, voici quelques résultats :

- **Évaluation du nombre de voisins de chaque noeud**

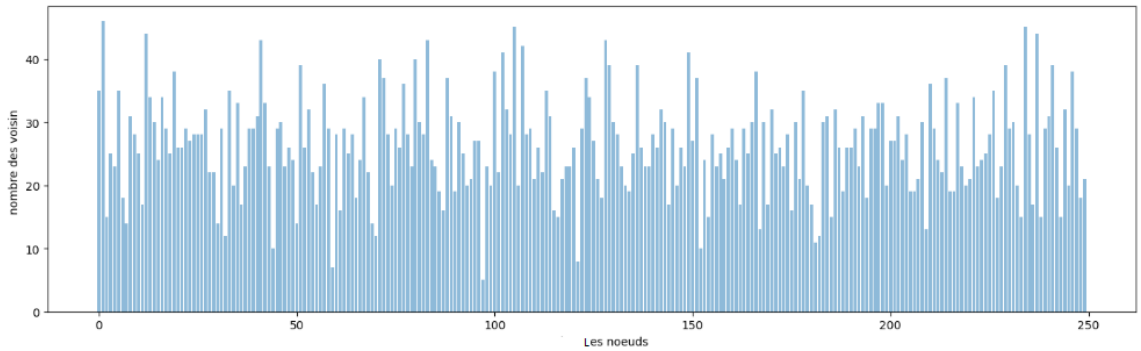

FIG. 3.4 : Nombre des voisins

- **Évaluation du paquets envoyés**

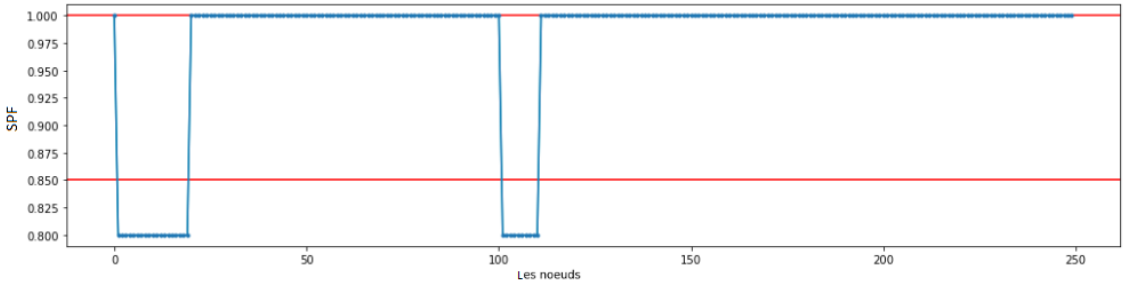

FIG. 3.5 : Les paquets envoyés

- **Évaluation du paquets reçus**

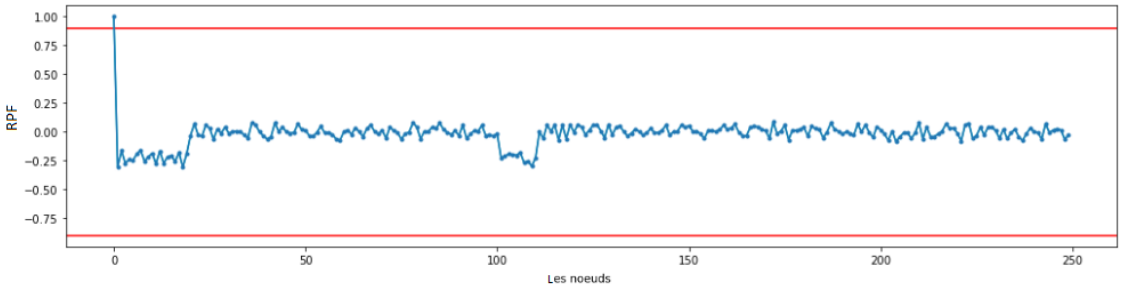

FIG. 3.6 : Les paquets reçus

- **Évaluation du données**

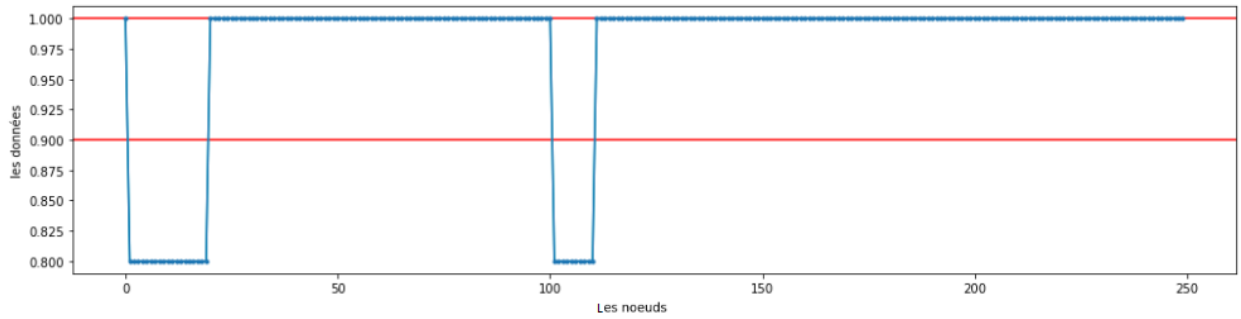

FIG. 3.7 : Le taux de données
en

- **Évaluation d'énergie**

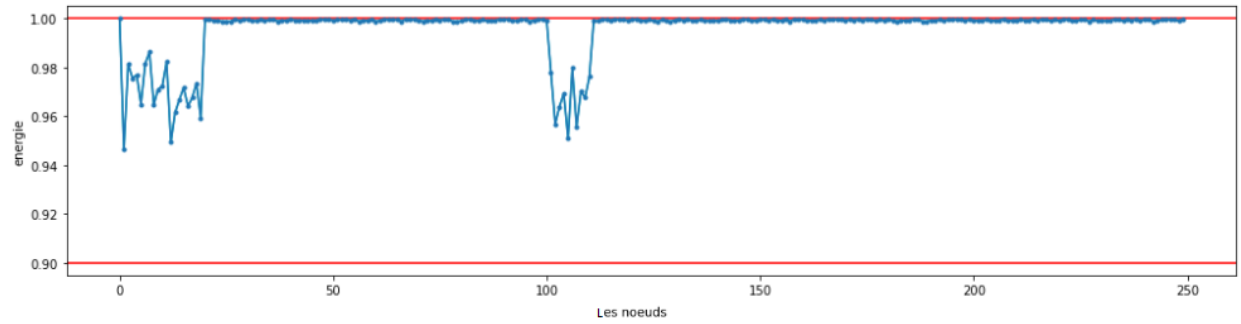

FIG. 3.8 : L'énergie

- **Évaluation du mobilité des noeuds**

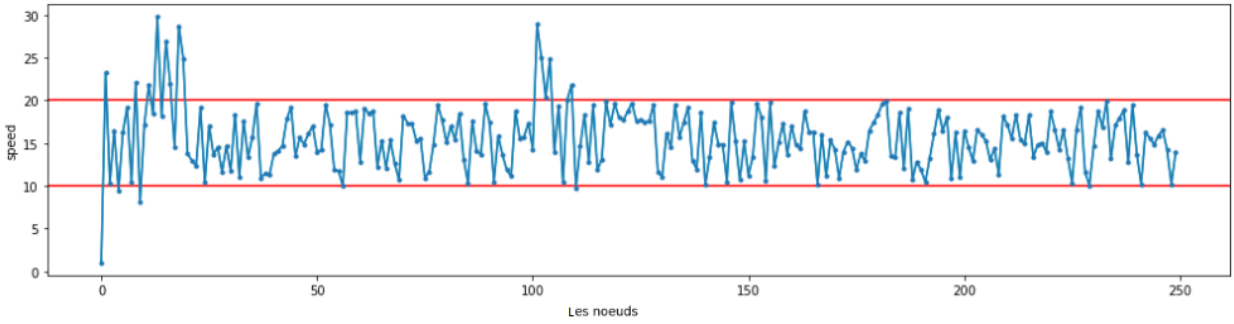

FIG. 3.9 : La vitesse

Les bornes qui sont en rouge dans les graphes précédents représentent les seuils supérieurs et inférieurs de chaque critères. Les noeuds qui dépassent ces seuils sont considérés comme des noeuds malveillants pour chaque critère. Et pour l'évaluation d'énergie, on remarque qu'il y a des noeuds avec une énergie réduite par rapport aux autres.

- **Évaluation du valeur de confiance**

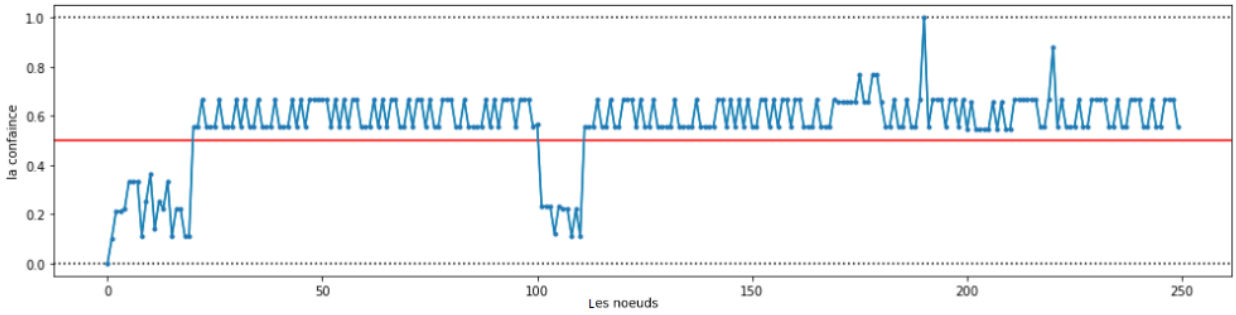

FIG. 3.10 : La valeur de confiance pour chaque noeud

la valeur de confiance varie de 0 à 1, les noeuds proches de 1 étant les plus fiables et les noeuds proches de 0 étant malicieux.

3.5.2 Classification SVM

On a classifié la valeur de confiance par rapport le risque de chaque noeud. La valeur de risque représente l'inverse de la confiance. Chaque fois que la valeur de confiance augmente, la valeur de risque diminue comme présenté dans la figure 3.11 .

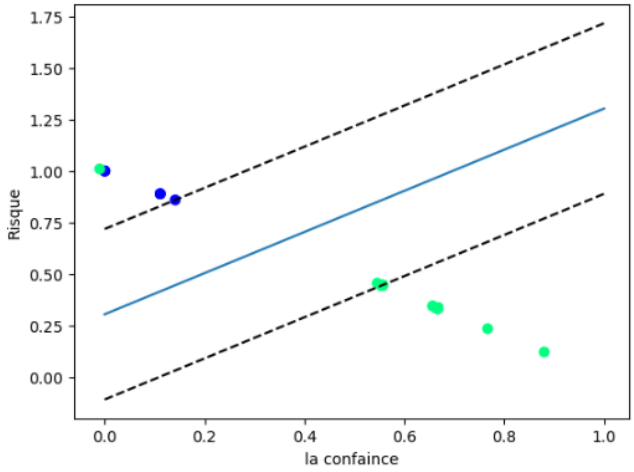

FIG. 3.11 : Classification SVM

On observe que les valeurs de confiance sont convergents, les noeuds verts ont des valeurs de confiance élevées, indiquant un comportement normal et le noeuds bleus ont des valeurs de confiance faibles, indiquant un comportement anormal.

3.6 Comparaison entre les algorithmes

Dans cette section, on a choisi deux approches différentes qui sont le modèle STMWSN classique (Rathore, Badarla et George, 2016) et le modèle d'apprentissage automatique ML-TCM (Jayasinghe et al., 2018) présenté dans le chapitre 2 pour faire la comparaison avec notre modèle selon les performances suivante :

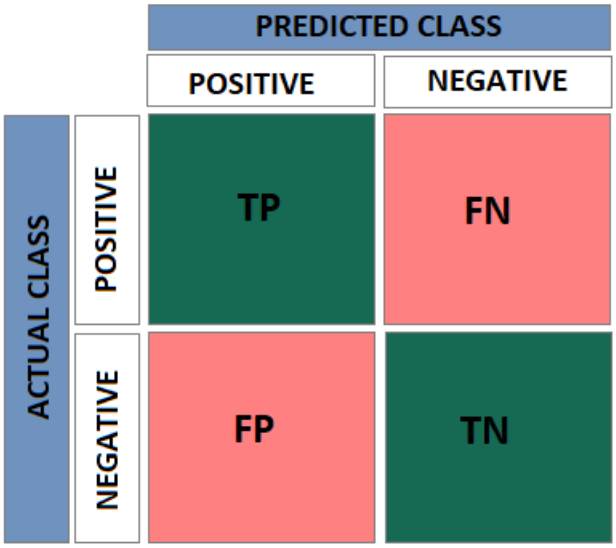

Fig. 3.12 : Matrice de confusion

- **Vrai positif (TP) :** Classe anormal est correctement classé comme anormal.
- **Faux positif (FP) :** Classe normal est classé comme anormal.
- **(Vrai négatif (TN) :** Classe normal est correctement classé comme normal.
- **Faux négatif (FN) :** Classe anormal est classé comme normal.

Ensuite, on va calculer les mesures de performance à partir des formules suivantes :

- **Accuracy :** C'est les échantillons qui ont classés correctement sur le nombre total d'échantillons.

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \times 100\% \tag{3.10}$$

- **La précision :** pour la valeur prédictions correctes des intrusions, la précision divisera ces vraies valeurs positives par les classes qui ont été prédits comme positifs.

$$Precision = \frac{TP}{TP + FP} \times 100\% \tag{3.11}$$

- **Recall :** Le rappel est calculé en divisant les vrais positifs par tout ce qui devraient être prédits comme positifs.

$$Recall = \frac{TP}{TP + FN} \times 100\% \tag{3.12}$$

- **F1-score :** C'est la moyenne équilibrée ou harmonique de la précision et du rappel si la valeur f1-score est égal à 1, cela signifie que toutes les classes sont correctement prédites.

$$F1 = \frac{2 \times P \times R}{P + R} \tag{3.13}$$

3.6.1 Résultats expérimentaux de notre modèle

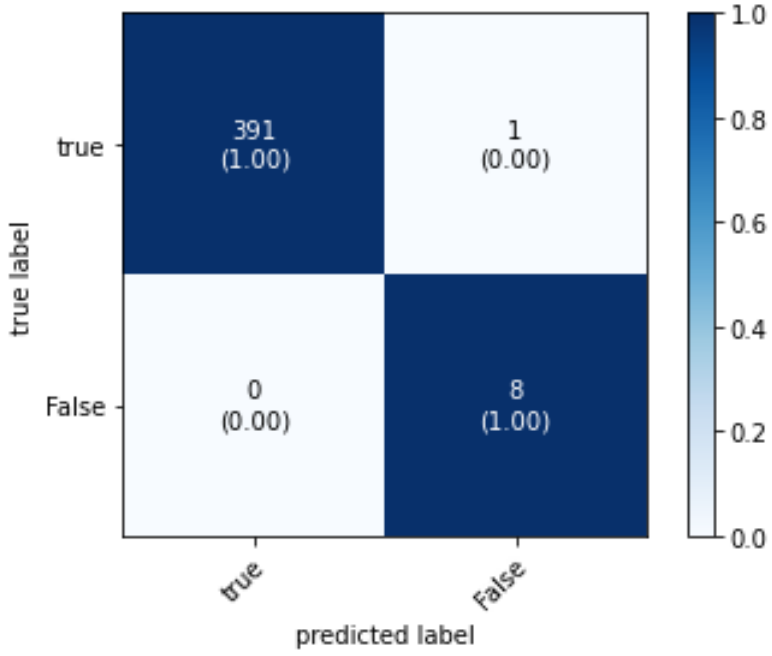

FIG. 3.13 : Matrice de confusion de classification

TAB. 3.3 : Résultats des performances

Accuracy (%)	Précision (%)	Recall (%)	F1-score (%)
99.75	100	99.74	99.87

3.6.2 Discussion

D'après les résultats obtenus de notre modèle, on constate que notre approche donne des valeurs mieux par rapport le modèle STMWSN qui donne un taux de faux négative entre]0.2,0.1] et pour le modèle ML-TCM qui a un taux faux négative 0.018, un taux vrai négative 0.99 et un taux de précision 0.98. Ceci est justifié par le fait que notre approche prendre on considération toutes les caractéristiques du capteur (Communication, données,énergie et mobilité) pour évaluer le comportement des noeuds. Les approches proposées évaluent juste une partie de comportement de noeud (données ou communication). C'est pour cela les noeuds malicieux avec une bonne participation dans le réseau peut être incorrectement classifiés comme fiables même s'ils envoient des fausses données.

3.7 Conclusion

Dans ce chapitre, on a défini l'architecture de notre modèle, présenté l'environnement de travail et mis les résultats du modèle et les comparer avec d'autres approches de référence de la littérature. Sur la base des résultats obtenus, le modèle donne de meilleurs résultats dans la détection des noeuds malicieux.

CONCLUSION GÉNÉRALE

La sécurité des réseaux de capteurs reste toujours un problème ouvert et non totalement couvert par les chercheurs travaillant dans ce type de réseau. Par conséquent, fournir des solutions de sécurité est devenu très urgent et important. Les solutions de sécurité basées sur la surveillance contribuent à certains facteurs pour résoudre ce problème.

Dans notre travail, on a proposé un modèle qui détecte les noeuds malicieux dans les réseaux de capteurs, et on est intéressée au modèle proposé qui est basé sur la relation de confiance entre les noeuds comme une solution de sécurité qui évaluer la communication entre les noeuds, les données, l'énergie de chaque noeud et la mobilité. On a utilisé l'apprentissage supervisé pour classer les noeuds en deux catégories : normaux et malicieux.

Les résultats expérimentaux montrent que le modèle proposé donne une bonne précision pour la classification avec l'utilisation de l'algorithme d'apprentissage supervisé SVM. Et comme perspective, on souhaite mesurer les performances de notre modèle avec d'autres travaux et calculé aussi sa complexité par rapport les autres approches.

BIBLIOGRAPHIE

Aghiles, Nait Ali (2013). «Sécurité par chiffrement dans les réseaux de capteurs sans-fil». Thèse de doct. Université Mouloud Mammeri.

Aivaloglou, Efthimia, Stefanos Gritzalis et Charalabos Skianis (2008). «Trust establishment in sensor networks : behaviour-based, certificate-based and a combinational approach». In : *International Journal of System of Systems Engineering* 1.1-2, p. 128-148.

Ali, Oubaziz (2011). «Prise en charge d'un grand nombre de capteurs sans fil dans 6 LoWPAN». Thèse de doct. Université Mouloud Mammeri.

Ammar, Ziani (2012). «Etude de la sécurité des données dans les réseaux de capteurs sans-fil (ZigBee).» Thèse de doct. Université Mouloud Mammeri.

Amutha, J, Sandeep Sharma et Sanjay Kumar Sharma (2021). «Strategies based on various aspects of clustering in wireless sensor networks using classical, optimization and machine learning techniques : Review, taxonomy, research findings, challenges and future directions». In : *Computer Science Review* 40, p. 100376.

ATHMANI, Samir (2018). «Protocoles pour la sécurité des réseaux de capteurs sans fil». Thèse de doct. Université de Batna 2.

Athmani, Samir (2010). «Protocole de sécurité Pour les Réseaux de capteurs Sans Fil». Thèse de doct. Université de Batna 2.

Azencott, Chloé-Agathe (2022). *Introduction au Machine Learning-2e éd.* Dunod.

Bader, Kaci (2009). «Détection dintrusions dans les réseaux de capteurs sans fil». In : *Master recherche* 2.

Barbara Schaetti, Phyllis Thompson et Françoise Gariazzo-Dessiex (2017). «Communication directe et indirecte». In : url : https://ubuntu-communication.ch/resources/pdf/2017-Comm_directe_indirecte_f_final.pdf.

Batouche, Sonia, Souhila Saci et al. (2015). «Etude et mise en place dun système de Détection dintrusion sous Linux». Thèse de doct. Université A/Mira de Bejaia.

Benahmed, K (2011). «Surveillance distribuer pour la sécurité dun réseau de capteurs sans fil». Thèse de doct. thèse de doctorat, spécialité informatique, option : sécurité informatique.

Bettahar, Hatem et Yacine Challal (2008). «Introduction à la sécurité informatique». In : *Supports de cours, Systèmes Intelligents pour le Transport, Université de Technologie de Compiègne, France* 15.

Boubiche, Djallel Eddine (2013). «Une approche Inter-Couches (cross-layer) pour la Sécurité dans les RCSF». Thèse de doct. Université de Batna 2.

Boushaba, Mustapha (2007). «Localisation des noeuds dans les réseaux de capteurs sans fil». In.

Cayirci, Erdal et Chunming Rong (2008). *Security in wireless ad hoc and sensor networks*. John Wiley & Sons.

Chinnaswamy, Santhanakrishnan et K Annapurani (2021). «Trust aggregation authentication protocol using machine learning for IoT wireless sensor networks». In : *Computers & Electrical Engineering* 91, p. 107130.

Doumi, Abdelmoumain (2018). «La Sécurité des Communications dans les Réseaux de Capteurs sans Fils». Thèse de doct. FACULTE DES MATHEMATIQUES ET DE LINFORMATIQUE DEPARTEMENT DINFORMATIQUE.

Embarka, Ben brahim et Amiche Selyna (2017). «Mise en place dune solution de détection dintrusion». Thèse de doct. Université Mouloud Mammeri.

Feng, Renjian, Xiaona Han et al. (2015). «A credible Bayesian-based trust management scheme for wireless sensor networks». In : *International Journal of Distributed Sensor Networks* 11.11, p. 678926.

Feng, Renjian, Xiaofeng Xu et al. (2011). «A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory». In : *Sensors* 11.2, p. 1345-1360.

Grandison, Tyrone et Morris Sloman (2000). «A survey of trust in internet applications». In : *IEEE Communications Surveys & Tutorials* 3.4, p. 2-16.

Gulganwa, Pooja et Saurabh Jain (2022). «EES-WCA : energy efficient and secure weighted clustering for WSN using machine learning approach». In : *International Journal of Information Technology* 14.1, p. 135-144.

Huang, Shujun et al. (2018). «Applications of support vector machine (SVM) learning in cancer genomics». In : *Cancer genomics & proteomics* 15.1, p. 41-51.

Ioannou, Christiana et Vasos Vassiliou (2018). «An intrusion detection system for constrained WSN and IoT nodes based on binary logistic regression». In : *Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, p. 259-263.

Jayasinghe, Upul et al. (2018). «Machine learning based trust computational model for IoT services». In : *IEEE Transactions on Sustainable Computing* 4.1, p. 39-52.

Jiang, Jinfang et al. (2014). «An efficient distributed trust model for wireless sensor networks». In : *IEEE transactions on parallel and distributed systems* 26.5, p. 1228-1237.

Kerkar, Moussa et al. (2008). «Le traitement du problème de la couverture dans les réseaux de capteurs sans fil». Thèse de doct. Université de Béjaia.

KHALILI, Zeyneb, Meryem BOUCHRA, Mohammed KADDI et al. (2019). «Une technique doptimisation de la consommation dénergie dans les réseaux de capteurs sans fil». Thèse de doct. Université Ahmed Draia-ADRAR.

Khelifa Benahmed, Ahmed Saidi et Nouredine Seddiki (2018). «Attacks and countermeasures in Wireless sensor networks». In.

Lamine, Messai Mohamed (2008). «Securite dans les Reseaux de Capteurs Sans-Fil». In : *Memoire de Magistere en Informatique Ecole Doctorale dInformatique de bejaia.*

Li, Wenchao et al. (2014). «A new intrusion detection system based on KNN classification algorithm in wireless sensor network». In : *Journal of Electrical and Computer Engineering* 2014.

Louiza, Idres (2012). «Système de détection dintrusion hybride et hiérarchique pour les réseaux de capteur sans fil». Thèse de doct. Université Mouloud Mammeri.

Lynda, Tlili (2011). «Modele de confiance pour securiser le routage dans les réseaux de capteurs sans fil». Thèse de doct. Université Mouloud Mammeri.

Maarouf, Samia et Souhila Ouadah (2014). «Implémentation et évaluation des schémas de routagesur une plateforme réelle de réseaux de capteurs sans fil.» Thèse de doct.

Momani, MM (2008). «Bayesian methods for modelling and management of trust in wireless sensor networks». Thèse de doct.

Monnet, Quentin (2015). «Modèles et mécanismes pour la protection contre les attaques par déni de service dans les réseaux de capteurs sans fil». Thèse de doct. Paris Est.

Nada, Zaidi (2021). «Optimisation réseaux de capteurs intelligent pour éclairage». In : *Université Badji Mokhtar-Annaba.* URL : https://biblio.univ-annaba.dz/ingeniorat/wp-content/uploads/2022/02/Zaidi-Nada.pdf.

Ngom, Diery (2016). «Optimisation de la durée de vie dans les réseaux de capteurs sans fil sous contraintes de couvertureet de connectivité réseau». Thèse de doct. Université de Haute Alsace-Mulhouse ; Université Cheikh Anta Diop (Dakar).

Omar, Mawloud, Yacine Challal et Abdelmadjid Bouabdallah (2012). «Certification-based trust models in mobile ad hoc networks : A survey and taxonomy». In : *Journal of Network and Computer Applications* 35.1, p. 268-286.

Quincozes, Silvio E, Juliano F Kazienko et Vagner E Quincozes (2023). «An extended evaluation on machine learning techniques for Denial-of-Service detection in Wireless Sensor Networks». In : *Internet of Things*, p. 100684.

Rathore, Heena, Venkataramana Badarla et KJ George (2016). «Sociopsychological trust model for wireless sensor networks». In : *Journal of Network and Computer Applications* 62, p. 75-87.

Sahraoui, B (2013). «Etude dun protocole de routage basé sur les colonies de fourmis dans les réseaux de capteurs sans fil». In : *Mémoire de Master, Université Tlemcen.*

Saidi, Ahmed (2021). «Trust evaluation method for Wireless Sensor Networks based on behavioral similarity and similarity coefficient». In : *2021 International Conference on Networking and Advanced Systems (ICNAS)*. IEEE, p. 1-6.

— (2022). «Security Solutions Based on Trust Management in Wireless Sensor Networks : A Review». In : *Artificial Intelligence and Heuristics for Smart Energy Efficiency in Smart Cities : Case Study : Tipasa, Algeria*, p. 395-408.

ZERADNA, Rim et Imen CHORFI (2022). «L'utilisation de l'apprentissage automatique pour la détection des attaques Déni de Service (DOS) dans les réseaux de capteurs sans fil». Thèse de doct. Université Ibn Khaldoun-Tiaret-.

Zhang, Tong, Lisha Yan et Yuan Yang (2018). «Trust evaluation method for clustered wireless sensor networks based on cloud model». In : *Wireless Networks* 24, p. 777-797.

Zhang, Wei et al. (2018). «A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks». In : *The Journal of Supercomputing* 74, p. 1779-1801.