الجمهوريـــة الجزائريـــة الديمقراطيـــة الشعبيـــة
People's Democratic Republic of Algeria

وزارة التعليـــم العالـــي والبحـــث العلمـــي
Ministry of Higher Education and Scientific Research

جامعـــة غـــردايـــــــة
University of Ghardaia

Registration No
/..../..../..../

كـــليـة العـلـــوم والتكنولـوجيـــا
Faculty of Science and Technology

قســـم الرياضيـــات والاعـــلام الآلـــي
Department of Mathematics and Computer Science

Master Thesis

Presented to obtain the academic Master diploma in Computer Science

Specialty : Intelligent Systems for Knowledge Extraction

THEME

Secure Clustering Approach based on Particle Swarm Optimization Algorithm in Wireless Sensor Networks

Publicly defended on 24/06/2024

by:

Akram CHERGUI & Ahmed Yacine BOUAMER

Jury members

Mr. Slimane BELLAOUAR	*MCA*	*Univ. Ghardaia*	*President*
Ms. Asma BOUCHEKOUF	*MAA*	*Univ. Ghardaia*	*Examiner*
Mr. Ahmed SAIDI	*MCB*	*Univ. Ghardaia*	*Supervisor*

University Year: 2023/2024

Acknowledgment

We thank first our great God for giving us courage and will during difficult times and who gave us strength and patience.

We would like to thank our supervisor, Mr. Ahmed Saidi, for his support, advice, and efforts to complete this work successfully.

In addition to all the engineers who helped us with some information and guidance for the success of our memorandum during our waiting period.

We also extend our sincere thanks to our parents and family who instilled in us the spirit of persistence and determination and helped us with their advice in completing our thesis.

Finally, we would also like to thank all the people and all our classmates who contributed directly or indirectly to the completion of this work.

I dedicate this humble work to my parents who support me a lot in my life and their sacrifices.

To my brothers and sisters and all my relatives who supported and encouraged me .

To every professor who taught me a letter and helped me reach where I am now , especially our dear colleague bouchra boukanoun .

ملخص

مؤخرًا، شهدت شبكات الاستشعار اللاسلكية (WSN's) استخدامًا متزايدًا في مجموعة متنوعة من التطبيقات، بما في ذلك أجهزة كشف الإنذار وأجهزة الاستشعار. لقد تم تطوير عدد من خوارزميات التجميع لتحسين كفاءة استخدام الطاقة في شبكة الاستشعار اللاسلكية (WSN) وزيادة عمر الشبكة. تم تصميم هذه الخوارزميات أساسًا لتحقيق توفير في استهلاك الطاقة دون أخذ الأمان بعين الاعتبار. في الهندسة التجميعية، يلعب رئيس المجموعة (CH) دورًا محوريًا في الشبكة. لذا، فإن اختيار عقدة رئيس المجموعة (CH) الأكثر موثوقية وجدارة بالثقة ضروري لزيادة عمر الشبكة. إدارة الثقة تعد تقنية أمنية هامة تسمح بكشف العقد الخبيثة بناءً على سلوكها في الشبكة. تقدم هذه الدراسة خوارزمية تجميع تعتمد على تقنية تحسين سرب الجسيمات (PSO)، والتي تدمج الأمان واستهلاك الطاقة في عملية اختيار (CH). تم إدخال تقنية الثقة أثناء اختيار (CH) لضمان عدم وجود عقدة خبيثة في هذا الدور. تساعد الخوارزمية المقترحة في تشكيل المجموعات واختيار (CH) بشكل فعال. تمت تجربتها بشكل واسع، وتمت مقارنة نتائجها مع الخوارزميات السابقة المقترحة. وخلصت الدراسة إلى أن خوارزمية التجميع التي تعتمد على (PSO) تختار العقدة الأكثر جدارة بالثقة كـ (CH) وتتجنب العقد الخبيثة بفعالية.

كلمات مفتاحية : شبكات الاستشعار اللاسلكية، إدارة الإئتمان، ،سوء السلوك، البرامج الضارة ، الهجمات

Abstract

Recently, Wireless Sensor Networks (WSNs) are increasingly utilized across various applications, serving as alarm detectors and sensors. Several clustering algorithms have been developed to enhance WSN energy efficiency and prolong network lifespan. These algorithms typically prioritize energy conservation without addressing security concerns. In clustering topologies, the cluster head (CH) holds a pivotal role, necessitating the selection of reliable and trustworthy CHs to extend network longevity. Trust management emerges as a critical security measure, identifying malicious nodes based on their behavior within the network. This study proposes a clustering algorithm leveraging Particle Swarm Optimization (PSO) to integrate both security and energy considerations during the CH selection process. The algorithm incorporates a trust mechanism to ensure that selected CHs are devoid of malicious intent. It facilitates cluster formation and CH selection, extensively evaluated through experiments comparing its performance with existing algorithms. The findings demonstrate that the PSO-based approach effectively selects trustworthy CHs while mitigating the influence of malicious nodes.

Keywords: Wireless sensor networks, Management trust, Misbehavior, Malicious, attacks

---

Résumé

Récemment, les réseaux de capteurs sans fil (WSN) ont été largement adoptés dans divers domaines, notamment comme détecteurs d'alarme et capteurs. Plusieurs algorithmes de regroupement ont été développés pour optimiser l'utilisation de l'énergie dans les WSN et prolonger la durée de vie du réseau. Ces algorithmes sont principalement conçus pour économiser l'énergie et ne prennent généralement pas en compte les aspects de sécurité. Dans une architecture hiérarchique, le rôle du chef de cluster (CH) est crucial pour le bon fonctionnement du réseau. Par conséquent, il est crucial de sélectionner un CH fiable et digne de confiance afin de maximiser la durée de vie du réseau. La gestion de la confiance est une technique de sécurité essentielle qui permet de détecter les nœuds malveillants en analysant leur comportement au sein du réseau. Cette étude propose un algorithme de regroupement basé sur la technique d'optimisation par essaim de particules (PSO) qui intègre à la fois des considérations de sécurité et d'énergie lors du processus de sélection du CH. Une méthode de confiance est appliquée lors de la sélection du CH pour s'assurer qu'il ne présente aucun comportement malveillant. L'algorithme proposé facilite la formation des clusters et la sélection des CHs. Il a été rigoureusement évalué à travers diverses expériences comparatives avec d'autres algorithmes existants. Les résultats obtenus indiquent que l'algorithme de clustering basé sur PSO permet de sélectionner efficacement le CH le plus digne de confiance tout en évitant les nœuds malveillants. Cette approche offre ainsi une solution prometteuse pour améliorer la sécurité et l'efficacité énergétique des réseaux de capteurs sans fil dans divers scénarios d'application.

Mots clés : Réseaux de capteurs sans fil, Gestion de la confiance, Mauvais comportement, Malicieux, attaques

---

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

WSN : Wireless Sensor Network

IoT :Internet of Things

PSO :Partical Swarm Optimization

BS :Base Station

CH :Cluster Head

GPU :Graphics Processing Unit

GENERAL INTRODUCTION

Wireless Sensor Networks (WSNs) have revolutionized the way we collect and transmit data in various fields, including healthcare, military, and disaster management. These networks consist of numerous small sensors deployed in a controlled environment, tasked with detecting desired objects and transmitting data to a base station.However, the limited power supply of these sensors poses a significant challenge, as their battery life is shortened during data collection, leading to a low power consumption problem. The need to prolong the lifespan of WSNs has become a pressing concern, particularly in scenarios where replacing or recharging batteries is not feasible. This has motivated researchers to develop protocols that can efficiently manage energy consumption and extend network lifetime.

Despite the existence of various protocols, they often fall short in meeting the requirements of WSNs, particularly in terms of energy efficiency and scalability. The limitations of these protocols have sparked interest in exploring alternative solutions that can effectively address the energy consumption problem. One approach to mitigating this issue is through the use of clustering-based routing protocols. These protocols have shown promise in reducing energy consumption by dividing the network into smaller sub-networks, each with a designated cluster head responsible for data collection and transmission. However, the selection of an optimal cluster head remains a challenge, and existing solutions often rely on simplistic methods that do not fully consider the energy and positional constraints of the nodes.

The most common problem with sensor networks is that they have limited resources such as energy, memory and processing power, making them vulnerable to many types of attacks. And when the subject is network security, we talk about the security of connected nodes against internal and external attacks, an

internal attack is carried out by a network node malicious that threatens other network nodes, an external attack carried out by nodes which are outside the network. They try to hack the network in several ways. THE The danger in these types of attacks is that they can hear communications traffic and modify the content of the information .

In this work, we propose a cluster-based routing protocol that leverages the Particle Swarm Optimization (PSO) algorithm to choose the most appropriate cluster head for each cluster. By taking into account the power and position characteristics of each node, our protocol aims to minimize power consumption and maximize the lifetime and reliability of the network, enabling it to operate efficiently in a variety of applications.

Chapter 1: Based on PSO and trust techniques in WSN, we present some general information on wireless sensor networks to provide an overview of their characteristics, their architecture and their areas of application.

Chapter 2: Presents the state of the art on clustering-based routing protocols algorithms in WSN and the clustering methods, we have detailed the k-means method, we have explained the clustering-based routing protocol using the PSO algorithm and the energy model used.

Chapter 3: We explained our proposed model, presented the results, and provided an analysis of them .

1 BACKGROUND AND OVERVIEW

1.1 Introduction

Recent innovations in communication technology and remarkable research achievements in recent years have led to the emergence of WSN. These networks consist of many small devices, called sensors, that are placed in a geographic area to monitor physical or environmental factors such as vibration, sound, temperature, light, or motion. Given the advantages of WSNs such as low cost, convenience, and deployment speed, this type of network is ideal for a variety of applications, including combat, environmental, medical, and surveillance applications. However, sensor cables are used in unsafe areas and have no signal strength. In addition, limited resources such as energy, memory and processing power prevent it from adapting to different types of attacks. There are two main topologies or architectures in the context of WSNs: distribution architecture, also called distribution architecture, and class architecture, also called cluster architecture. Project-based construction suitable for large networks. The larger it is, the more traffic goes to the base station, which affects weather conditions. Therefore, all sensors are connected to a network and each cluster is controlled by a single node to save energy and reduce overhead. Topic selection is a well-studied problem in the literature and is called the NP problem.

Recently, trust management techniques have been proposed as a security solution that can counter negative tendencies, selfishness, and instability. The concept of trust is used in various fields such as e-commerce, peer-to-peer networking, web services and virtual networks. So far, trust-based security solutions in WSNs have used trust-based technologies in various applications such as CH security mining, trusted paths, trusted locations, security aggregation, and malicious behavior detection.

Throughout this chapter various terms, metrics and obstacles related to WSNs are introduced to pave the way for exploration in sections. The aim is to establish an understanding of the aspects of WSNs preparing for detailed discussions on clustering algorithms, energy saving techniques, security measures and other crucial topics necessary, for effectively deploying and managing wireless sensor networks.

1.2 Overview

A wireless sensor network consists of numerous micro-sensors forming an ad-hoc network. These sensors autonomously gather and transmit environmental data (Sahraoui, 2013). The nodes are typically scattered randomly across a geographical region, known as the "catchment field," which corresponds to the area of interest for the observed phenomenon.

Figure (1.1) illustrates: The basic components of WSN

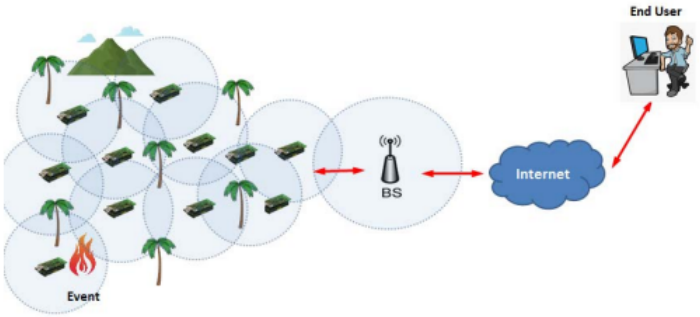

Figure 1.1: Example of WSN network (Saidi, 2021)

1.2.1 What is a sensor node?

A sensor node, often referred to as a mote, is a component within a wireless sensor network that possesses the capability to process data, collect sensory information, and communicate with other nodes within the network. However, while all motes are nodes within the network, not all nodes in the network are necessarily motes (Jawarkar et al., 2013).

Figure (1.2) illustrates the sensor node

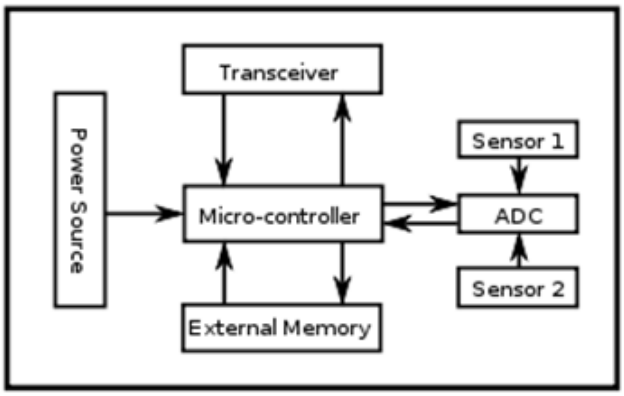

Figure 1.2: Architecture of sensor node (Jawarkar et al., 2013)

1.2.2 The components of a sensor node

- **The acquisition unit :**This unit is responsible for collecting data from built-in physical sensors, such as temperature, humidity, brightness, pressure and sound sensors (Djedouboum et al., 2018).
- **The communication unit:** It manages communication between the sensor nodes, thus facil- itating the transmission of the collected data(Djedouboum et al., 2018).
- **The processing unit:** This unit is responsible for processing and analyzing the collected data before transmitting it to a base node or to a node coordination (Djedouboum et al., 2018).
- **The energy unit:** Sensor nodes operate on battery power, which means they have a limited source of energy. Efficient energy management is essential to ensure the operational lifespan of the node(Djedouboum et al., 2018) .

Figure (1.3) illustrates the components of a sensor node composed of three unit such as:

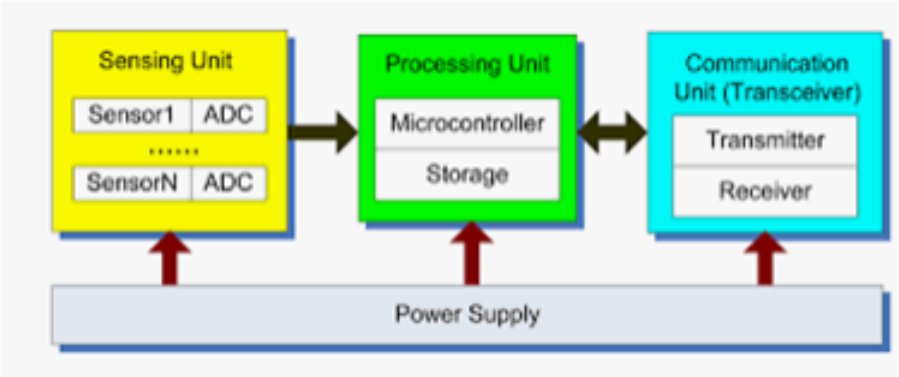

Figure 1.3: The components of a sensor node (Xia, 2009)

1.2.3 The WSNs protocol stack

The protocol that the sensor node uses to communicate with the base station, as shown in the figure (1.4) . As explained by (Akyildiz et al., 2002), the protocol stack of a wireless sensor network (WSN) is very similar to the traditional protocol stack and consists of various components: application, transport, network, communication, physical layer, power management layer, and management and workforce management level (Fahmy, 2020).

1. **The application layer**

   The application layer is responsible for providing application-specific information and facilitating the transfer of requested information from the application layer to lower levels in the protocol stack. The software is implemented in a system based on the sensor used (Nayyar, 2017).

2. **The Transport Layer**

   The transport unit is designed for data management, especially when data captured by sensor nodes must be presented via the Internet or external communication networks (Nayyar, 2017).

3. **The Network Layer**

   Networks take responsibility for routing data, including calculating the best path to send data from destination to destination. In wireless sensor networks (WSNs), network design also considers factors such as power consumption, data-based communication, and data collection (Nayyar, 2017).

4. **The Data Link Layer**

The data link is responsible for a variety of tasks, including routing information, defining data frames, controlling resiliency, and checking for errors (Nayyar, 2017).

5. **The Physical Layer**

The physical body is primarily responsible for important functions such as frequency selection, carrier frequency generation, signal recognition, processing and information processing(Nayyar, 2017).

Figure (1.4)illustrates WSN protocol stack

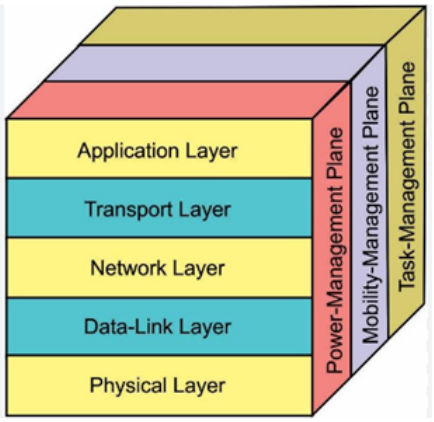

Figure 1.4: The WSNs protocol stack (Nabila and Kahina, 2017)

1.2.4 Wireless sensor network topology

WSN topology is a visual representation of the network structure. It has a significant impact on network performance, including reliability, energy consumption and scalability.

Sensor networks can be divided into two main structural categories: flat sensor networks and hierarchical networks (Boussag, 2017).

1. **flat topology**

A wireless sensor network is an integrated network where all nodes have the same characteristics in terms of battery capacity and functionality. The only exception is the repository, which acts as a gateway and is responsible for sending the collected data to the end user (Boussag, 2017).

The flat topology is shown in the figure (1.5).

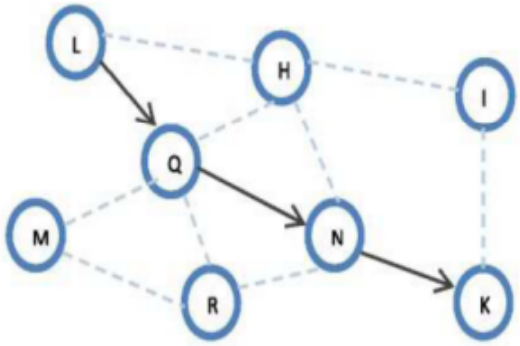

Figure 1.5: Flat topology (Bouguer, 2012)

- **Sink node:**The sink or base station is a specific node within the network and is tasked with collecting data from various nodes in the network. Consequently, it needs to be active and possess unlimited energy resources (Boussag, 2017).

2. **Hierarchical topology**

A hierarchical architecture has been proposed to reduce costs and simplify communication in wireless sensor networks (WSN) (Lasla, 2007). This involves incorporating expensive and complex layers, creating an infrastructure that removes many network functions from cheap, simple nodes. The hierarchical architecture consists of several layers, including the sensor layer, transmission layer, and access point, as shown in Figure (1.6). This program provides an example of sequential structures(Boussag, 2017).

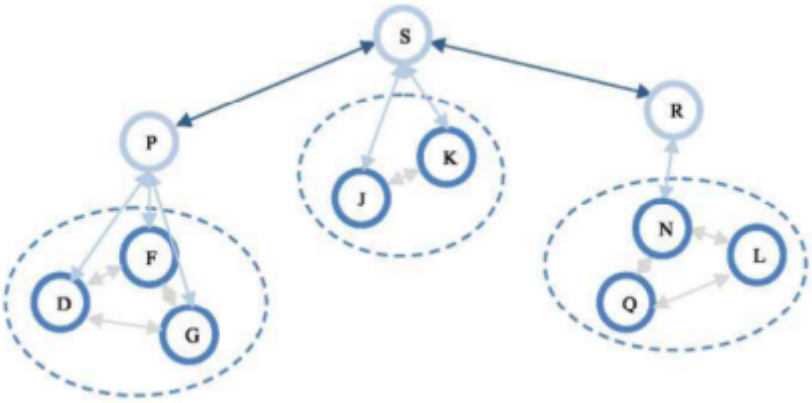

Figure 1.6: Hierarchical topology (Bouguer, 2012)

1.2.5 The characteristics of WSNs

Wireless sensor networks (WSNs) have a number of unique characteristics that distinguish them from other computer networks. They characterized by:

1. **Lack of Infrastructure**

   Sensor networks are characterized by the absence of pre-existing infrastructure and any kind of centralized administration (Sahraoui, 2013).

2. **Large size**

   A sensor network can contain thousands of nodes (Benouda and Benabderrahmane, 2023) .

3. **Interference**

   Two simultaneous transmissions can interfere on the same frequency, or use close frequencies (Benahmed, 2011).

4. **Dynamic Topology**

   Sensors can be attached to moving objects that move freely and arbitrarily. It changes frequently due to the continuous mobility of the nodes that form the network topology (Sahraoui, 2013).

5. **Self-Organization**

   Sensor nodes in the network must be self-organizing. This is very important because sensor nodes are operated in an unknown environment and are not monitored. To adapt to this complex environment, sensor nodes work together to change their configuration through distributed algorithms that facilitate the creation of an automatic network. This integration capability enables the sensor network to be efficient and perform the intended tasks without monitoring (Ahmed et al., 2012) .

6. **Limited Physical Security**

   Wireless sensor networks are more security sensitive than traditional networks. This is justified by practical limitations and restrictions, which mean that control over the transferred data must be reduced (Sahraoui, 2013).

7. **Limited Bandwidth**

   Sensors operate at low rates to minimize the energy consumed when transferring data between nodes (Ali, 2011).

8. **Energy, Storage, and Computing Constraint**

   It is a very important feature of WSNs because each sensor in the network has a small amount of energy (battery). To improve network service, it is necessary to reduce the energy consumption of each node. Therefore, the storage capacity and computing power of the sensor are limited (Benahmed, 2011).

1.3 Connectivity and Coverage in WSN

1.3.1 Connectivity

Connectivity is a crucial issue in both fixed and mobile sensor networks and is highly dependent on traffic availability. An additional issue is dynamic changes in the topology of the network caused by factors such as node movements, faults, and potential attacks. These changes lead to negative effects such as

loss of communication channels, isolation and network fragmentation. In wireless sensor networks (WSNs), connectivity has been shown to be an important performance indicator, especially for WSN applications. To improve the performance of this program, it is important to carefully study and evaluate the characteristics of the connection during the design of the network and its stage implementation, as shown in the description (Ngom, 2016) .

1.3.2 Coverage

Coverage in WSNs refers to the importance of monitoring a specific area using a sensor deployment. Essentially, this evaluates how well and how often sensors can track the body's position. Simply put, coverage indicates the extent to which each person is within the detection range of the network monitored by at least one sensor(Elhabyan et al., 2019) .

1.4 Data aggregation

This strategy include creating additional content based on key information gathered from the environment. This method uses aggregation of sensor nodes to combine data from multiple sensors and transform it into quality data. This not only significantly reduces the amount of data transferred, but also requires less power and therefore increases network service time. Moreover, it also solves the election explosion problem that reduces the speed of the network (Nabila and Kahina, 2017) .

The typical data aggregation process is depicted in Figure (1.7).

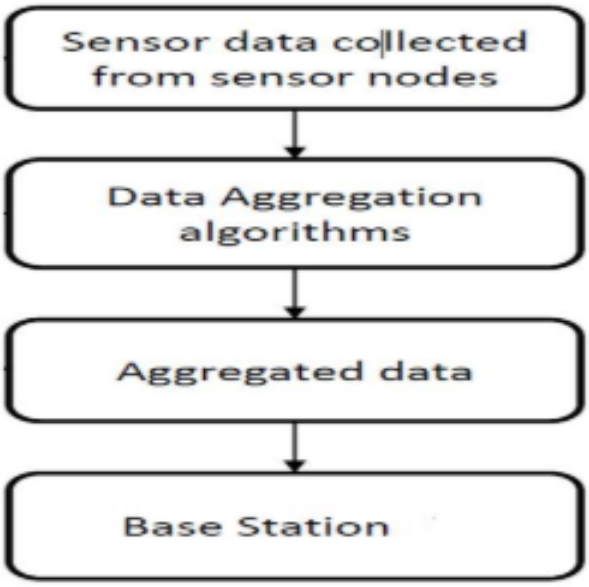

Figure 1.7: The structure of data aggregation (Saeedi and Al-Qurabat, 2021) .

Solutions for Data Aggregation Security

To address the security challenges, different solutions can be implemented:

- **Encryption :**It is the method used to ensure information security. This involves converting data into an unreadable form using encryption algorithms and secret keys. Unlocking encrypted data is only possible with the full key. This ensures that data remains safe and protected during storage, transmission and processing(Seboru, 2023) .
- **Digital signatures:** use public keys and provide strong data quality assurance and authentication. The hash value is encrypted with the sender's private key, and the receiver can decrypt it with the sender's public key. Verifying digital signatures using the public key assures recipients that the information has not been altered during transmission (Seboru, 2023).

1.5 Routing in WSNs

The routing task in wireless sensor networks (WSNs) is crucial and requires careful consideration. The signaling mechanism is important to facilitate communication between sensor nodes and base stations and to establish effective communication in the network (Nabila and Kahina, 2017).

Routing Protocols in WSNs

1. **Flat Routing Protocols:** All nodes have the same functionality. Besides the base station that controls the network and is responsible for collecting all the data from different sensors to reach the end user, the node's decision to send the packet to others also depends on its location (Makhmouk and Melouk,),(Priya and Brindha, 2016).
2. **Hierarchical Routing Protocols :** Hierarchical routing protocols are initiated by dividing nodes into multiple roles. One of the most commonly used methods is clustering, which divides the network into groups. A team consists of a team leader and team members (Priya and Brindha, 2016),(Chaudhary and Vatta, 2014).
3. **Location-based routing:**Location-based routing protocols use underlying information to guide the discovery, maintenance, and transfer of data. It also allows data transfer and prevents the entire network from being flooded with information needed to calculate the distance between two specific nodes, so energy consumption can be compared and reduced (Chaudhary and Vatta, 2014).

1.6 The problems of the WSN

Energy problem

Power charging is often a critical issue in WSNs. This process can be very expensive or even impossible in some cases. To determine the performance of the sensors, it is necessary to adjust their power(Sofiane and Bouabdallah, 2008).

1.7 Security in the WSN

Security poses a complex challenge for sensor networks, given their vulnerability to various attacks arising from inherent characteristics and applications (Bouhicha and Zohra, 2023) This section delves into the vulnerabilities, security challenges, classifications of attacks.

1.7.1 Terminologies

- **Threat:** A potential danger to a resource or to the functioning of the network (Sadiqui, 2019).
- **Vulnerability:** Weakness in the system, usually exploited by attackers(Sadiqui, 2019).

- **Risk :** Is the probability of an adverse event occurring or the possibility of potential loss or damage (Sadiqui, 2019).
- **Attack :** An action taken to harm a resource (Sadiqui, 2019).
- **Monitoring:** Monitoring is a passive informational mechanism that analyzes the status of the system and provides indicators (Sahraoui, 2016).
- **Supervision:** Monitoring a system and taking action if the system does not meet control objectives (Sahraoui, 2016).
- **Safety:** Safety is a set of measures used to prevent malicious human activities, to protect property and people from the effects of theft or aggression(Benahmed, 2011),(Bettahar and Challal, 2008).

1.7.2 Security problem

WSNs face serious security issues as they are vulnerable to malicious attacks. Sensors are often installed in remote and dangerous locations and are therefore difficult to protect against attacks. Attacks can take various forms, including phishing, identity theft, and network disruptions. These attacks can compromise the integrity, confidentiality, and availability of collected data, which can have a significant impact on network users. Strong security solutions are essential for maintaining WSNs (Lamine, 2008).

1.7.3 Security objectives of WSNs

Wireless networks require practical solutions in various applications to ensure widespread data security. Data transmitted in a WSN must meet a number of security requirements.(Laroussi, 2012);(Sen, 2012).

1. **Confidentiality** :Is the guarantee that the content exchanged between the sensor nodes can only be viewed and understood by those who are authorized to access it (Athmani, 2018).
2. **Availability** : Is the permanent ability to access all services that the network provides to each network member (Athmani, 2018).
3. **Integrity**: Ensure the accuracy, consistency and integrity of data throughout the network life- cycle and prevent unauthorized changes or modification (Athmani, 2018).

4. **Authentication** : It suggests that the sensor nodes engaged in communication are authentic and possess legitimate access to the network (Keerthika and Shanmugapriya, 2021).

1.7.4 Vulnerabilities of wireless sensor networks

WSNs face a number of vulnerabilities that can be exploited by attackers to compromise security of the network.

- **Wireless technology:** The weakness of the wireless network is that an attacker can gain unauthorized access to transmitted data or other information (Lamine, 2008).
- **resource limit:**Any security system requires additional resources, including data storage, computing resources, and the ability to run sensor nodes (Athmani, 2018).
- **Unattended operation:**Sensor nodes are often used in inaccessible locations such as the battlefield, for example at sea or on large machinery, and therefore must be able to operate independently in a single area (Lamine, 2008).
- **Routing mechanisms:**A route is a way to connect data to a specific location over a specific network. Many protocols are so fragile that they are vulnerable to attacks (Lamine, 2008); (Tlili, 2011).

1.7.5 Security challenges in the WSN

Security for sensor networks is a challenging issue due to several factors:

1. **Wireless communication challenges:**One of the risks of wireless communications is that an attack can disrupt and disrupt user traffic. As mentioned, to ensure complete security in this area, confidentiality, integrity and authentication must be guaranteed (Lamine, 2008).
2. **The computing and processing capacity challenges** It comes from limited computing and storage resources with significant power constraints in sensor networks. The key challenge in sensor technology is to design a protocol that effectively reduces energy consumption and ultimately extends the lifespan of the web (Aghiles, 2013).

3. **Challenges associated with the energy problem** : Around the important issue of energy saving in sensor networks. As emphasized, it is important to reduce energy consumption during many network security operations (Lamine, 2008).
4. **Challenges Related to the Deployment Environment:** Wireless sensor networks (WSNs) offer exciting opportunities for environmental monitoring and data collection. However, the unique characteristics of the distribution environment present many challenges that significantly impact network performance and longevity. Here are some important questions:
   - Heterogeneity and dynamics: Heterogeneity and dynamics are two important characteristics of wireless sensor networks (WSNs), which are networks of sensors deployed in a location to monitor physical or environmental conditions (Akyildiz et al., 2002).
     ✓ **Environmental factors:** Wind, rain, heat and humidity can alter signal transmission and affect the sensor (Akyildiz et al., 2002) .
   - Energy Constraints:
     ✓ **Uneven energy depletion:** Different locations face different communication and environmental stresses, leading to similar energy consumption and network degradation(Heinzelman, 2002).

1.7.6 Attacks in wireless sensor networks

Cyber attacks use a variety of methods to exploit network vulnerabilities and cause damage. These attacks can occur locally or remotely, raising security concerns and affecting everything from earshots to complete destruction of the traffic network, depending on the attacker's capabilities. To combat these attacks effectively, you need to understand the nature of the attacker and the different types and types of attacks so that you can implement the best solutions(Berrachedi and Diarbakirli, 2009).

1. **Attack Classification**

   ❶ **According to the degree**
   – **Low degree attacks:** These attacks do not cause much damage to the network. They can be used to collect data or disrupt network activities .

- **High degree attacks:** These attacks can cripple or destroy the network. They can be used to steal information, destroy networks, or cause physical damage.

❷ **According to the origin** Attacks in WSNs can be classified according to their origin into two categories:

- **External attacks:** a Performed by a node that does not belong to the network or does not have access rights (Rachida, 2011).
- **Internal attacks:** Used by internal nodes. Defensive measures are aimed at preventing attacks from outside. However, insider attacks pose a serious threat that can affect the performance of WSNs (Rachida, 2011).

❸ **According to the nature**

- **Passive attacks :** A trigger is when an unauthorized node gains access to a device without altering data or disrupting network operations. Once the attacker obtains sufficient information, he or she can launch an attack on the network, turning a passive attack into a serious attack (Rachida, 2011).
- **Active attacks:** Triggered when a node finds a way to do something by changing data or disrupting the normal operation of the network (Rachida, 2011).

2. **Description of some attacks**

1. **Wormholes attack**

To initiate a snake attack, at least two malicious heads must be placed on the sensor array. One node establishes a strong interconnection and allows other nodes at different distances to be used. The figure shows example of Wormhole attacks figure (1.8).

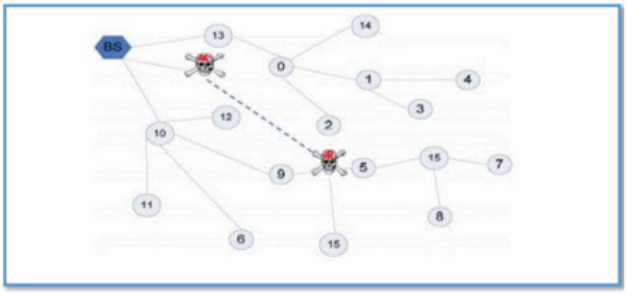

Figure 1.8: Wormhole attack (Boudhir, 2013).

2. **Jamming attack (Radio attack)**
   Jamming is a common form of attack that attackers can easily perform to obtain information about wireless communications networks used in wireless sensor networks (WSN). In this attack, the attacker uses lines similar to WSN to make the internet less disruptive to the communication network and prevent the communication network from functioning properly. An example of a jamming attack can be seen in Figure (1.9).

Figure 1.9: Jamming attack (Benahmed et al., 2018).

3. **Sybil attack**
   In this attack, hosts present multiple identities to aliases on the network, causing inconsistencies in the neighbor's router table. In algorithms where the trust process is implemented by creating redundant paths, an attacker can change the performance of the system by providing more than one identity, thus creating multiple paths that are effectively a single path on a malicious header (Challal, 2008).
   The figure shows an example of a Sybil attack (1.10).

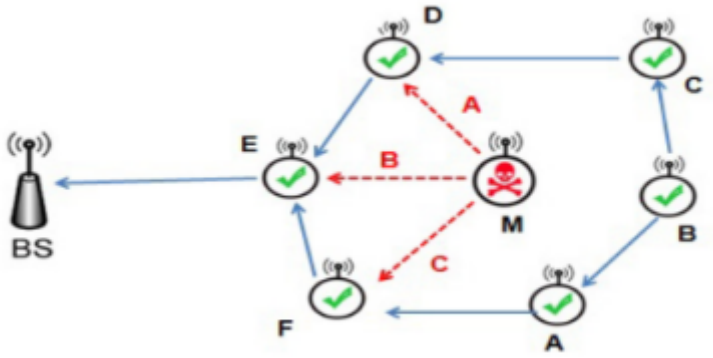

Figure 1.10: Sybil attack (Benahmed et al., 2018)

4. **Black hole attack**

A blackmail attack is initiated by injecting malicious elements into the network and forcing neighboring nodes to share their information online using various methods. Similar to a black hole in space, all data passing through this node is intercepted, making it inaccessible to other networks. (Lamine, 2008) ; (Karlof and Wagner, 2003) . The figure (1.11)shows an example of a black attack.

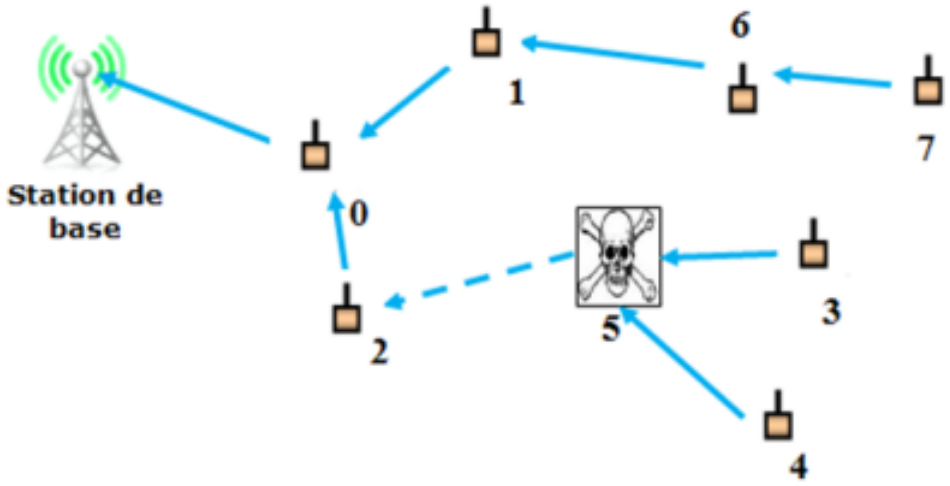

Figure 1.11: Black hole attack (Benahmed, 2011)

1.8 Clustering in WSN

1.8.1 Definition of clustering

Clustering is a technique used to analyze and retrieve data in unsupervised learning. The main purpose is to divide the data into groups or clusters to ensure that the data in one cluster is similar to the other (Hastie et al., 2009).

1.8.2 Types of clustering

1.Clustering based on the node degree

A simple and effective technique for connecting wireless networks. Each network node is assigned a unique identification (ID). The packer then distributes the ID to its neighbors as shown in Figure (1.12). Each node compares its identity with the identity of its neighbors and calls itself the cluster leader if it has the lowest identity. Non-cluster heads then join the cluster head groups with the most frequent points(Mehmeti et al., 2009).

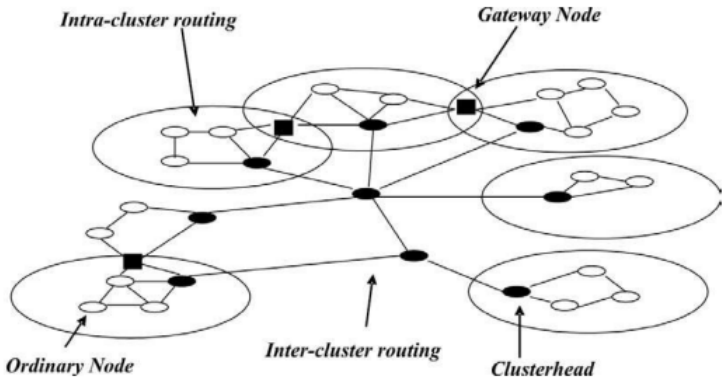

Figure 1.12: Lowest-ID heuristic (Mehmeti et al., 2009)

2.Highest-Degree heuristic

In the clustering technique, nodes with the highest degree are selected as cluster nodes. This technique does not require universal knowledge of network topology. However, this may lead to large cluster sizes and may be affected by migration (Mehmeti et al., 2009).

3.Energy-based clustering

Clustering techniques consider the energy levels of nodes when selecting cluster nodes. This is especially important for battery-powered cordless phones. Energy-based clustering can help increase network uptime while reducing cluster energy (Reddy, 2011).

4.Connectivity-based clustering

Network-based technology: Network technology that uses network communications to connect data to a group of components. This technique generally works by finding groups of topics that are closely related and related to areas in other groups. Connection-based networking techniques are resilient to shifts and changes in topology and can be used to improve the performance of various networking applications such as networking, data and power management (Reddy, 2011).

5.Hierarchical clustering

Hierarchical clustering : A type of unsupervised learning algorithm that links groups of data into hierarchical clusters. Algorithm development can be both additive and divisive. Agglomerative algorithms start with each data point as its own component and then combine combinations until the desired number is reached. Clustering algorithms start by collecting all the cluster data into a single cluster and then cluster the clusters until the desired number is reached (Murphy, 2012).

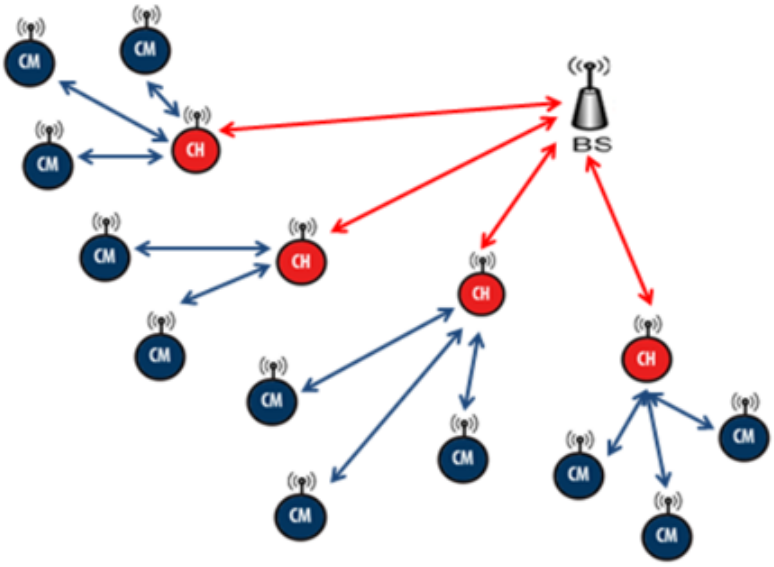

Figure 1.13: Hierarchical clustering (Murphy, 2012)

6.Density-based clustering

A type of aggregation that groups data by size in the data field. Density-based clustering algorithms typically represent clusters as high-density areas separated from other similar clusters by low-density areas (Han et al., 2011) .

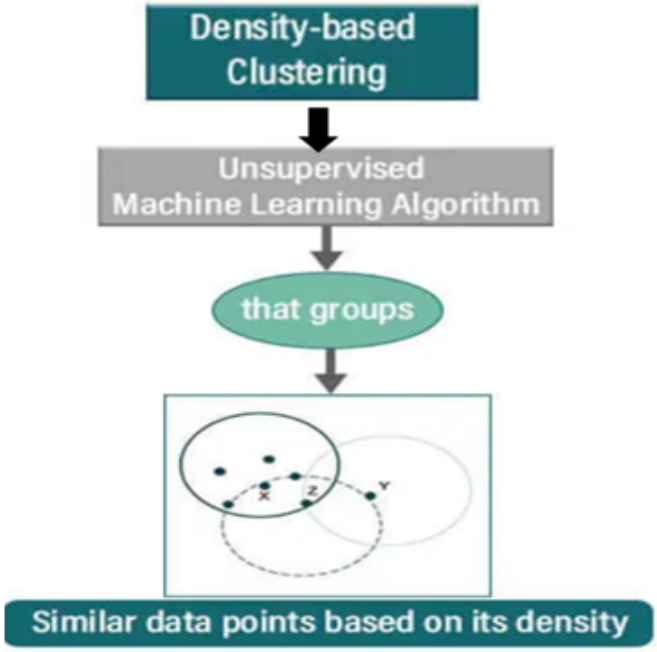

Figure 1.14: Density-based clustering (Han et al., 2011)

7.Grid-based clustering

This type of clustering algorithm divides the data space into a grid of cells and assigns data to clusters based on the number of cells they belong to. Network-based raster algorithms tend to be more efficient because they can be implemented using simple structural algorithms such as hash tables. However, they may be sensitive to network selection and may not affect the supply chain in different ways (Aggarwal and Reddy, 2014).

8.Partitioning-based clustering

This type of clustering algorithm divides the data into a fixed number of disjoint families so that each data point belongs to the same cluster. Segmentation algorithms are typically greedy and work by repeatedly assigning data points to the source based on an objective function such as minimizing the sum of squared distances between data points and cluster centers (Mitchell, 1997).

1.9 Metrics used for clustering

1.9.1 Lifespan

The lifetime of a WSN is the period during which it can operate effectively before its performance reserves are exhausted or its hardware components fail. This is a crucial factor to consider in WSN design and implementation, as many WSNs are deployed in remote or inaccessible locations, making maintenance and battery replacement difficult or expensive(Nabil Mekki, 2018).

1.9.2 Energy

WSNs are usually powered by batteries, which have limited capacity. Therefore, energy consumption in WSNs is a major concern. The proposed approach should be designed to minimize energy consumption by optimizing clustering, data transfer and forwarding(Nabil Mekki, 2018).

1.9.3 Load balancing

In a WSN, load balancing refers to the distribution of power consumption and data traf- fic among network nodes. This is important to ensure that no nodes are overloaded and the network can operate efficiently. The proposed approach should be designed to bal- ance the load on the network in order to extend the network's lifetime and improve its performance(Nabil Mekki, 2018).

1.9.4 Security

WSNs are vulnerable to a variety of security threats, such as Sybil attacks, black hole attacks, and wormhole attacks. These attacks can disrupt network operations, compromise data confidentiality and integrity, and even cause physical damage to sensor nodes. The proposed approach should include security mechanisms to protect the network from these threats(Nabil Mekki, 2018).

1.9.5 Distance

The distance between nodes in a WSN can affect energy consumption and network perfor- mance. In general, longer distances require more energy to transmit data and can also lead to higher packet loss rates. The proposed approach should consider the distance between nodes when selecting cluster heads and routing data(Nabil Mekki, 2018).

1.9.6 Connectivity

Connectivity is the ability of nodes in a WSN to communicate with each other. This is important for the network to function properly and collect data from the surrounding area. The proposed approach aims to ensure that all nodes in the network are connected and that the network can maintain connectivity even if nodes fail or move(Nabil Mekki, 2018).

1.9.7 Mobility

In some WSN applications, nodes can be mobile, that is, they can move around the environment. This can add complexity to network design and

make it more difficult to maintain connectivity and stability. The proposed approach should be designed to handle mobility and ensure that the network can function effectively even when nodes are moving(Nabil Mekki, 2018).

1.10 Overview of optimization methods

The PSO algorithm is used to find profits or reduce costs while meeting constraints in different categories. Commonly used optimization methods include linear programming (LP) for problems involving linear relationships, indirect programming (IP) for decisions about variables, and dynamic programming (DP) for linear and straight-line problems. Additionally, meta-heuristic algorithms such as Genetic Algorithms (GA) and Simulation Annealing (SA) provide an easy way to solve complex problems. Using this approach, organizations can make comprehensive decisions to improve performance, resource allocation, and overall performance(Cormen et al., 2022).

1.11 Classification of optimization methods

The main differences between continuous and discrete methods, where problems involve real or random changes. Another important factor is planning and development; the former is based on decision rules and the latter is participatory. While the world is moving towards the best solution in every field of research, the most important evolution of the solution is taking place in the environment. The skill-based approach uses data from to guide the search, unlike the freely derived approach which is suitable for non-mountainous scenarios. information. Optimal distributions combine convex functions, while sub optimal optimization solves complex problems. The black box makes the actual transaction transparent, while the white box exploits known issues. Finally, internet optimization comes into play (Cormen et al., 2022).

1.11.1 Heuristic optimization methods

Heuristic optimization methods provide versatile and scalable approaches for solving complex optimization problems. Drawing inspiration from natural phenomena or employing meta-heuristic algorithms, these techniques efficiently explore solution spaces to find near- optimal solutions. Nature-inspired algorithms like genetic algorithms, particle swarm optimization,

and ant colony optimization mimic biological processes to guide the search process. Meta-heuristic algorithms such as simulated annealing and tab search offer general purpose optimization frameworks adaptable to diverse problem domains. Population-based algorithms like differential evolution and evolutionary strategies maintain populations of candidate solutions, evolving them iterative to improve solution quality. Despite not guaranteeing optimally, heuristic optimization methods excel in tackling real-world challenges across engineering, operations research, and machine learning domains (Cormen et al., 2022).

1.11.2 PSO algorithm

Particle Swarm Optimization (PSO) is an emerging optimization-based technique that is dynamic in nature. Its simplicity and adaptability have made it popular in various fields of research. Since its founding in 1995, PSO has been continuously developed and improved by researchers around the world. These efforts led to the development of revisions and extensions of the original algorithm with preliminary study of behavioral parameters. This article provides an overview of PSO by explaining its basic concepts and parameters as PSO evolves through transformation, expansion, hybridization, and analysis(Jain et al., 2022).

1.11.3 Ant colony algorithm

Ant Antoni (ACO) emerged in the early 1990s as a powerful breeding technique inspired by the behavior of real colonial herbs. This standard has been used to solve many development problems such as insight and continuous improvement, as well as communication problems such as coordination and division of tasks. Initially, KKO algorithms were designed based on this biological approach for optimal performance. The concept was later expanded to cover a wide range of quality improvement issues and led to the development of various ACO structures. The article also demonstrates the application of ACO to the problem of continuous improvement and explains the method of blending with older engineering and research techniques, demonstrating the different methods and capabilities of different research activities(Blum, 2005).

1.12 Trust technique in WSN

Trust, according to (Wei et al., 2008) is a notion that embodies a faith, in someone's trustworthiness, integrity and capability. It entails being open to depending on and believing in the credibility of another person organization or system. Trust serves as the cornerstone of relationships among people within organizations and across societies shaping the dynamics of interactions and collaborations, between individuals.

1.12.1 Characteristic of trust

- **Directionality:** Trust flows in a certain direction. A may trust B, but B may not trust A to the same extent or in the same way (Han and Kamber, 2006).
- **Asymmetry:** The level of trust between two entities can be unequal (McEvily et al., 2016).
- **Transitivity:** Trust doesn't always transfer through a chain of relationships (Falcone and Castelfranchi, 2010).
- **Context-dependency:** Trust can vary depending on the specific situation or context (Chaurasia and Tomar, 2012).

1.12.2 Types of Trust systems

We divide the trust system ins two types :

1. **Certificate-based trust systems**

   A trust-based system is a powerful tool for building trust in distributed systems. They provide a way to transparently bind public keys to attributes. This can be used to authenticate companies and create secure communication networks(Millán et al., 2009).

2. **Behavior-based trust systems**

   Behavioral trust systems are a promising new approach to establishing trust in distributed networks. Behavior-based trust systems can overcome many of the limitations of traditional trust systems by using orga-

nizational behavior to evaluate their trustworthiness,such as their (Selvaraja and Anand, 2012).

1.13 Conclusion

As a result, security research in wireless sensor networks (WSNs) highlights the limitations and vulnerabilities of the system. The main theme of this research is the need for strong security measures to protect the integrity, confidentiality and availability of data in WSNs. A comprehensive analysis of vulnerabilities, threats, and attack types reveals many important findings. WSNs are an attractive technology with many advantages, including low cost, flexibility, and rapid deployment. However, WSNs pose many research challenges, including security, energy, location, and distribution vulnerabilities. Security is one of the biggest problems facing the company. Therefore, this section presents the basic concepts of WSNs. These key concepts are important for the reader to understand.

2

STATE OF THE ART

2.1 Introduction

In the context of the rapid development of wireless networks (WSNs), Iterative algorithms play an important role in improving data analysis, energy efficiency and network performance. After providing information about state-of-the-art algorithms for security integration when using wireless sensor networks (WSNs), the following paragraphs introduce trust and recognition-based integration algorithms, focusing on the problems and evaluation criteria of distributed networks.

2.2 Related works

2.2.1 Clustering based on consumed energy

1.Low Energy Adaptive Clustering Hierarchy (LEACH)

LEACH stands out as a widely adopted hierarchical routing algorithm for sensor networks. The concept involves grouping sensor nodes into clusters based on strong received signals in their vicinity. These clusters utilize local cluster-heads as intermediaries to transmit data towards the destination. This approach conserves energy by limiting transmissions to cluster-heads rather than requiring all sensor nodes to transmit directly (Abdesselam and Belouatek, 2013).

2.Firefly Low Energy Adaptive Clustering Hierarchy (Fire-LEACH)

(Fire-LEACH) is a protocol suite for wireless sensor networks (WSNs) based on the Firefly algorithm (FA). It was developed to solve energy consump-

tion, network reliability and distribution efficiency problems in WSNs. FA is a meta-heuristic algorithm that optimizes the aggregation process in WSNs by using the temporal behavior of random variables. By simulating how fireflies attract each other, FA accurately selects the cluster heads (CH) that are closest to station and have residual energy. This results in a reliable and robust protocol implementation (Palan et al., 2017).

3.Neural Networks-LEACH (NN-LEACH)

The NN-LEACH protocol, a variant of the LEACH protocol introduced by (Sanhaji et al., 2019), incorporates neural network principles to enhance the clustering process within LEACH, particularly focusing on the selection of cluster heads (CHs). Inspired by the functionality of natural neurons, the protocol aims to optimize CH selection based on the remaining energy levels of nodes, favoring those with higher energy reserves.

For instance, the model includes three layers: an input layer with nodes representing energy levels and bias, a hidden layer with four nodes utilizing sigmoid activation functions, and an output layer with a single node indicating whether a node is chosen as a CH (denoted by "1") or not (denoted by "0") [(Sanhaji et al., 2019),(Sanhaji et al., 2017)].

4.Hybrid Energy-Efficient Distributed Clustering (HEED)

HEED (Hybrid Energy Efficient Distribution Clustering) is a distributed network of sensor systems (WSNs) that aims to achieve energy efficiency and increase network uptime by harmonizing power consumption between networks. This is done by selecting cluster heads (CH) based on a combination of their remaining energy and the second part, such as a node close to its neighbors or a node's ranking. This method assumes that CHs are chosen to minimize the total energy consumption of the network while preserving the channel. consumption while maintaining network connectivity(Younis and Fahmy, 2004).

2.2.2 Clustering based on Trust of sent data

1.Particle Swarm Optimization protocol for Hierarchical Clustering (PSO-HC)

"SO-HC (Particle Swarm Optimization Protocol for Hierarchical Clustering) is an integrated Internet protocol for wireless sensor networks (WSNs) that uses the Particle Swarm Optimization (PSO) algorithm to reduce clustering. Groups. The goal is to achieve energy efficiency and extend network lifetime by reducing the number of active nodes (CHs) and increasing bandwidth" (Riham and Yagoub, 2014).

2.Secure clustering approach based on bio inspired technique (BTCWSN)

"BTCWSN is a secure network protocol for wireless sensor networks (WSNs) that uses biotechnology to create a secure and reliable network. The aim is to close the vulnerability of traditional protocols such as LEACH, which are vulnerable to various attacks such as Sybil attacks, blackmail attacks and worm attacks"(Sahoo et al., 2015).

3.Weighted Clustering Algorithm for Mobile Ad-Hoc Networks (WCA)

"WCA (Weighted Clustering Algorithm for Mobile Ad-Hoc Networks) is a proposed clustering algorithm for mobile ad-hoc networks (MANETs) that takes into account optimal range, transmission power, mobility and mobility. The goal is to reduce computing and communication costs while maintaining network stability and improving energy efficiency" (Chatterjee et al., 2002).

4.Distributed Weighted Clustering Algorithm for Mobile Ad-Hoc Networks (DWCAr)

" (DWCAr) is an adaptive clustering algorithm for mobile ad hoc networks (MANETs) that takes into account the mobility, residual energy and centrality of mobile nodes. The aim is to improve energy efficiency, network stability and packet delivery in MANET by dynamically adapting the pooling structure to network conditions" (Choi and Woo, 2006).

Clustering based on communication trust

1.Balanced and Safe Weighted Clustering Algorithm in Wireless Sensor Networks (BS-WCA)

BS-WCA (Secure and Balanced Weighted Clustering Algorithm in Wireless Sensor Net- works) is a clustering algorithm for wireless sensor networks (WSNs) that aims to achieve balanced power consumption, long network lifetime and improved security. It uses a combination of node residual energy, node degree, and node behavior metrics to select cluster heads (CHs) that are well connected, have sufficient energy, and are reliable. This ap- proach helps to optimize the cluster structure, ensure the reliability of data transmission and protect the network from malicious nodes (Dahane et al., 2015).

2.Spatially Distributed Collaborative Anomaly Detection (SD-CA)

SDCA is a distributed monitoring approach to detect misbehavior in wireless sensor networks (WSNs). The aim is to address the challenges of centralized mechanisms for detecting misconduct, such as: B. the high communication effort and the susceptibility to individual sources of error. SDCA uses a combination of local monitoring and collaborative filtering to detect misbehaving nodes in a distributed and robust manner (Benahmed et al., 2012).

3.Genetic algorithm and an adaptive fuzzy logic system (GA-ANFIS)

A hybrid approach that combines genetic algorithms and adaptive fuzzy logic systems to optimize clustering in wireless sensor networks, aiming to achieve efficient clustering formation and management while considering network dynamics and uncertainties(Hussain et al., 2007).

2.3 Summary and evaluation

Table 2.1: Synthesis and Evaluation of some Proposed Algorithms (Comparison against other clustering algorithms)

Approach	Clustering Technique	Trust			Security	Distance	Energy	Load Balancing	Connectivity	Mobility	Simulator
		Data Trust	Communication Trust	Energy Trust							
LEACH (Akkaria et al., 2015)	Probability	x	x	x	x	x	☑	x	☑	☑	MATLAB
FireLEACH (Palan et al., 2017)	Firefly Algorithm	x	x	x	x	☑	☑	x	☑	☑	MATLAB
NN-LEACH (Singh et al., 2017)	Neural Networks	x	x	x	x	☑	☑	x	x	x	OMNET++
HEED(Younis and Fahmy, 2004)	Particle Swarm Optimization	x	x	x	x	x	☑	☑	☑	x	Network Simulator
PSO-HC(Riham and Yagoub, 2014)	Particle Swarm Optimization	x	x	x	x	☑	☑	☑	☑	☑	OMNET ++
BTCWSN(Sahoo et al., 2015)	Honey Bees Mating	x	x	x	x	x	x	x	x	x	MATLAB
WCA(Chatterjee et al., 2002)	Weighting	x	x	x	x	☑	☑	x	☑	☑	OMNET++
DWCA(Choi and Woo, 2006)	Weighting	x	x	x	x	☑	☑	x	☑	x	OMNET++
BS-WCA(Dahane et al., 2015)	Weighting	x	☑	x	☑	☑	☑	☑	☑	☑	Self-based
SDCA(Benahmed et al., 2012)	Weighting	x	☑	x	☑	x	☑	x	☑	x	Self-based
GA-ANFIS (Hussain et al., 2007)	Genetic Algorithm	x	☑	x	☑	☑	x	x	x	x	MATLAB
Our Scheme	Particle Swarm Optimization	☑	☑	☑	☑	☑	☑	☑	☑	☑	MATLAB

Table (2.1) describes the evaluation of some proposed algorithms. The evaluation can be summarized in the following points:

- The algorithms that take into account one type of trust , data or energy trust. Focusing on a single type of trust does not make the node trustworthy because it can be trustworthy for one type but not for other types.
- All algorithms are designed for wireless sensor networks (WSNs) in particular LEACH, Fire-LEACH, NN-LEACH, and HEED are all based on the Low Energy Adaptive Clustering Hierarchy (LEACH) algorithm, but they each use different techniques to improve cluster head selection and energy efficiency .
- Most of the algorithms use a clustering approach to organize the nodes in the network into groups, with a cluster head responsible for collecting and transmitting data from its cluster members.
- The algorithms like WCA, DWCAr, and BS-WCA are designed for mobile ad-hoc networks and use a weighted metric to select cluster heads, taking

into account factors such as node energy, communication cost, and security. and may perform better in those scenarios.

- In terms of performance, LEACH, Fire-LEACH, NN-LEACH, and HEED have similar performance, while PSO-HC and BTCWSN have better performance due to the use of optimization techniques. WCA, DWCAr, and BS-WCA have slightly lower performance, while SDCA has the lowest performance due to the complexity of the anomaly detection algorithm.
- In terms of protection, LEACH, Fire-LEACH, NN-LEACH, HEED, WCA, DWCAr do not provide any specific security measures. However, BS-WCA have built-in security measures to prevent attacks and ensure data privacy. SDCA does not provide any specific security measures, but it can be used in conjunction with other security algorithms to provide protection.
- In terms of performance, LEACH, Fire-LEACH, NN-LEACH, and HEED have similar performance, while PSO-HC and BTCWSN have better performance due to the use of optimization techniques. WCA, DWCAr, and BS-WCA have slightly lower performance, while SDCA has the lowest performance due to the complexity of the anomaly detection algorithm.
- The majority of researchers either use MATLAB or develop their own simulator. There is a lack in the trust simulators that are designed specifically for trust evaluation in WSNs and they are easy for implementing new protocols and frameworks.
- The recommendations method of some algorithms focuses on one type of information, ex positive or negative recommendation. Tacking on one type of information into consideration is not enough.

2.4 Conclusion

Traditional security techniques such as encryption and authentication are insufficient to address the unique challenges of wireless sensor networks (WSNs) due to their limited capacity and distribution. Additionally, compromised nodes may have valid keys and identities, making these techniques ineffective against insider attacks. On the other hand, trust management is a promising solution for WSNs, enabling detection and isolation of malicious nodes based on their behavior. However, our analysis of modern trust management approaches reveals that they often focus only on communications-based trust, neglecting other fundamental aspects such as information and energy trust. Therefore, it is necessary to develop a more comprehensive approach to trust management that takes into account multiple forms of trust to ensure the reliability and security of WSNs.

3

SECURE CLUSTERING ALGORITHM IN THE WSN

3.1 Introduction

This chapter introduces the proposed model for detecting bad behavior in wireless sensor networks. It provides an in-depth discussion on the design and implementation of the detection mechanism, including the theoretical framework and practical considerations. The chapter also outlines the methodologies used for evaluating the model's performance. Furthermore, it presents and analyzes the results of experimental simulations conducted to test the model's effectiveness. Key findings and insights derived from the simulations are discussed, highlighting the model's strengths and potential areas for improvement.

3.2 The proposed network architecture

Our network is a hierarchic topology which contains three types of nodes: the cluster member, the cluster head and base station. Figure (3.1)shows a network design based on the following assumptions:

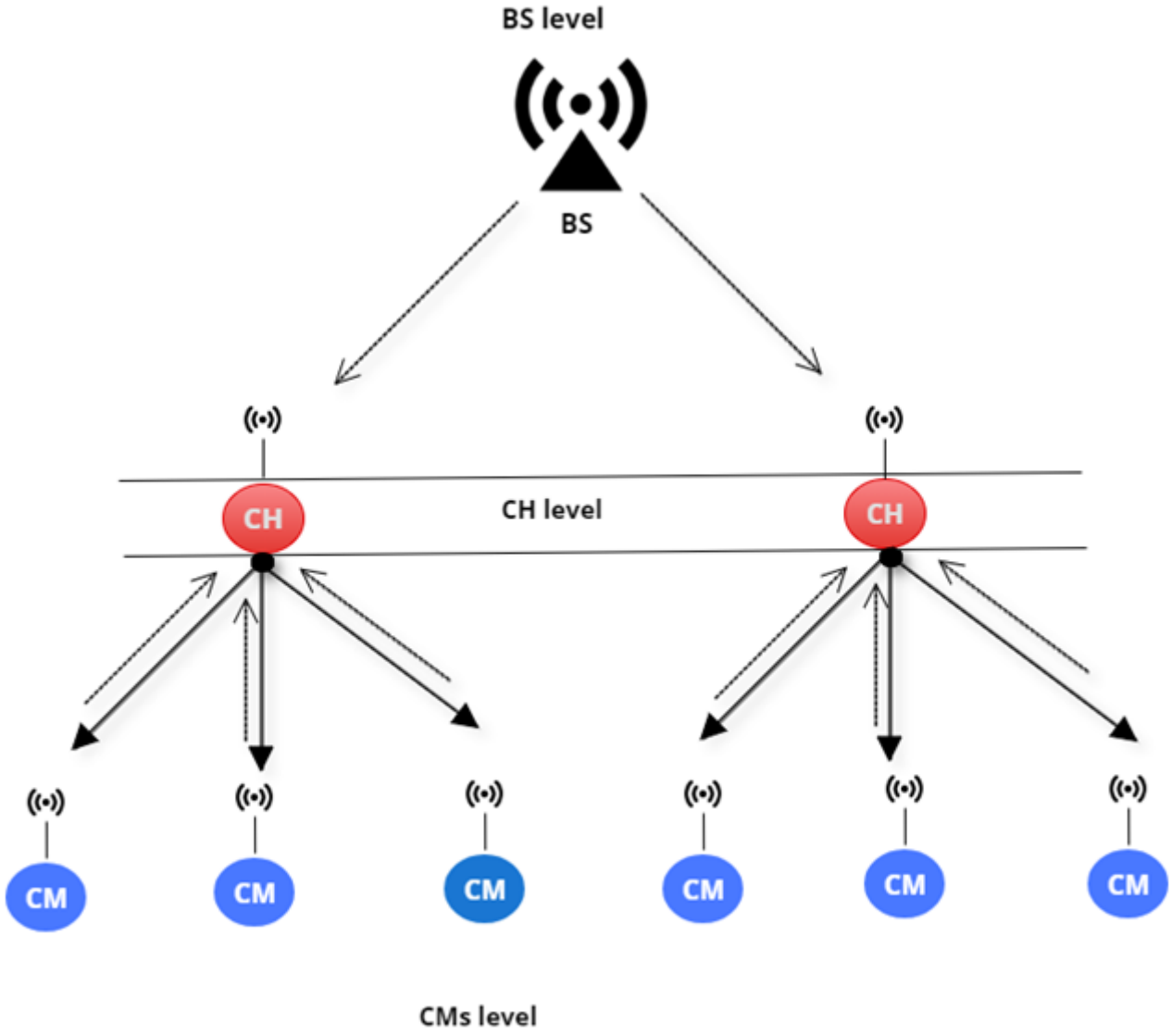

Figure 3.1: Network design of the proposed scheme (Saidi, 2021)

- **Base station node (BS)**: It is the most powerful node in the network.
- **Cluster head node (CH)**: It is the manager of the cluster. We select the most trustworthy node as cluster head because it supervises the behavior of its cluster.

- **Cluster member (CM)**: a regular sensor node that joins a cluster under the supervision of the CH.

3.3 Assumptions

- Nodes are trustworthy at the first stage of deployment.
- Nodes are able to localize themselves; the exact details of the localization technique are not discussed in this thesis.
- Each node has only one ID registered at the BS.
- For trust evaluation purpose, we assume that all nodes can hear and communicate with their neighbors located in their connectivity range.
- For trust information exchange, we assume a secure wireless channel.
- Each cluster is monitored by only one CH and it is awake during all the time of the round.

3.4 Presentation of the proposed model

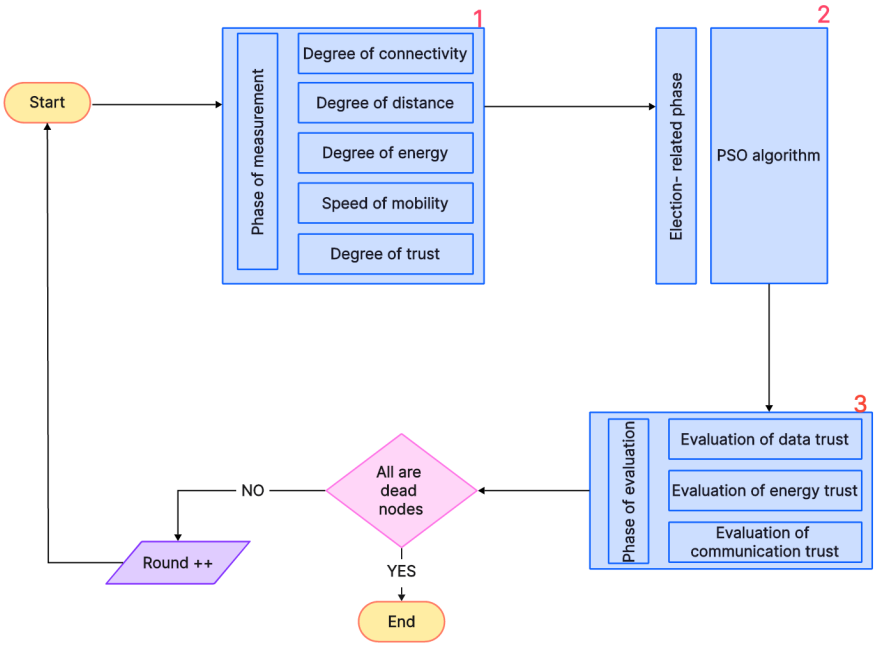

Figure 3.2: Our proposed model

3.4.1 Measurement phase

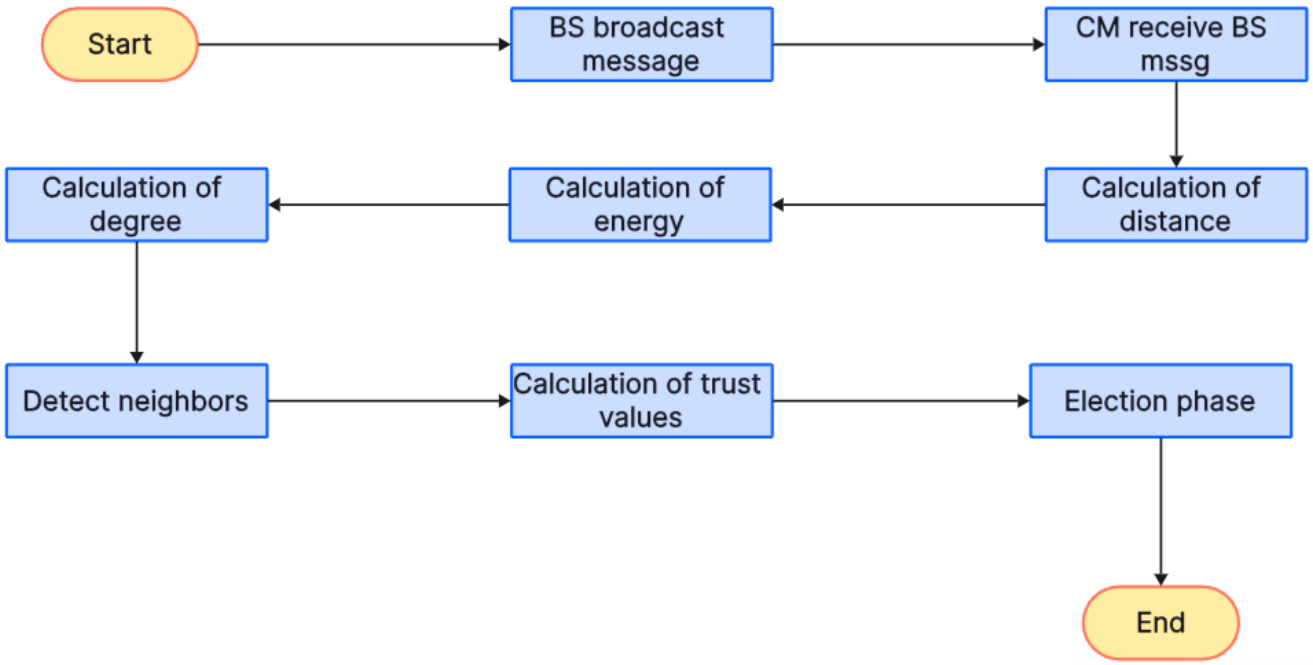

Figure 3.3: Cluster head measurement phase

Distance

The cluster heads must be very close to others clusters in order for communications between them to be very easy and not to consume a lot of energy. To do this, we chose distance euclidean to create the shortest paths between the clusters.

It calculates the distance euclidean as defined in the equation 3.1 (Guerti and Halilem, 2020) .

$$AB = \sqrt{(x_B - x_A)^2 + (y_B - y_A)^2} \tag{3.1}$$

Energy

Each node uses little energy for activities such as sensing, processing, storage and transmission. A node in the network must know how much energy will be used to perform a new task to which it is assigned. The energy consumed may vary depending on the type of functionality or activity it has to perform.

In our model, the energy consumption rate is represented by minimum and maximum thresholds as described in the two equations.

It calculates the energy as defined in the equation 3.10 ((Bouhicha and Zohra, 2023)) .

$$\text{ENGi}(t) = \frac{E_i(t-1)}{E_i(t)} \tag{3.2}$$

$$\text{ENGj}(t) = \frac{E_j(t-1)}{E_j(t)} \tag{3.3}$$

E_i means the energy spent by node i at time t0 and E_j means the energy spent by the target node at times t0,t respectively.

- **Degree**

  The degree of a node is determined by the number of neighboring nodes it has. In Equation (3.4), Txrange denotes the transmission radius. When a node falls within the communication range of another node, it is considered a neighbor of that node. N(i) represents the collection of neighbors of node i. Ci signifies the node's degree and is determined by the count of its neighbors. Dis(i, j) represents the distance between nodes i and j (Saidi, 2021).

$$C_i = \bigcup_{j \in N, j \neq i} \{j | d(i,j) < Txrange\} \tag{3.4}$$

Trust

There are several ways to evaluate the trust of the nodes proposed in the literature. In our approach, we chose two methods :

- **Rating Formulation :** The trust value calculated by (Bouhicha and Zohra, 2023) as follows:

$$\text{Trust} = \frac{S(t) - U(t)}{S(t) + U(t)} \tag{3.5}$$

The values of S and U represent the number of times the node performs malicious actions in the monitoring window T.

- **Bayesian formulation :**The trust value calculated by (Bouhicha and Zohra, 2023) as follows:

$$E(\text{trust}) = \frac{S(t) + 1}{S(t) + U(t) + 2} \tag{3.6}$$

The values of S and U represent the number of times the target node performs malicious actions in the monitoring window T. Details of the beta function are found in.

3.4.2 Election phase

Once the construction of the clusters is completed, the base station sends an announcement to each sensor node linked to a cluster, after the creation of CH begins at the level of each cluster according to the according to the process depicted in figure (3.4)

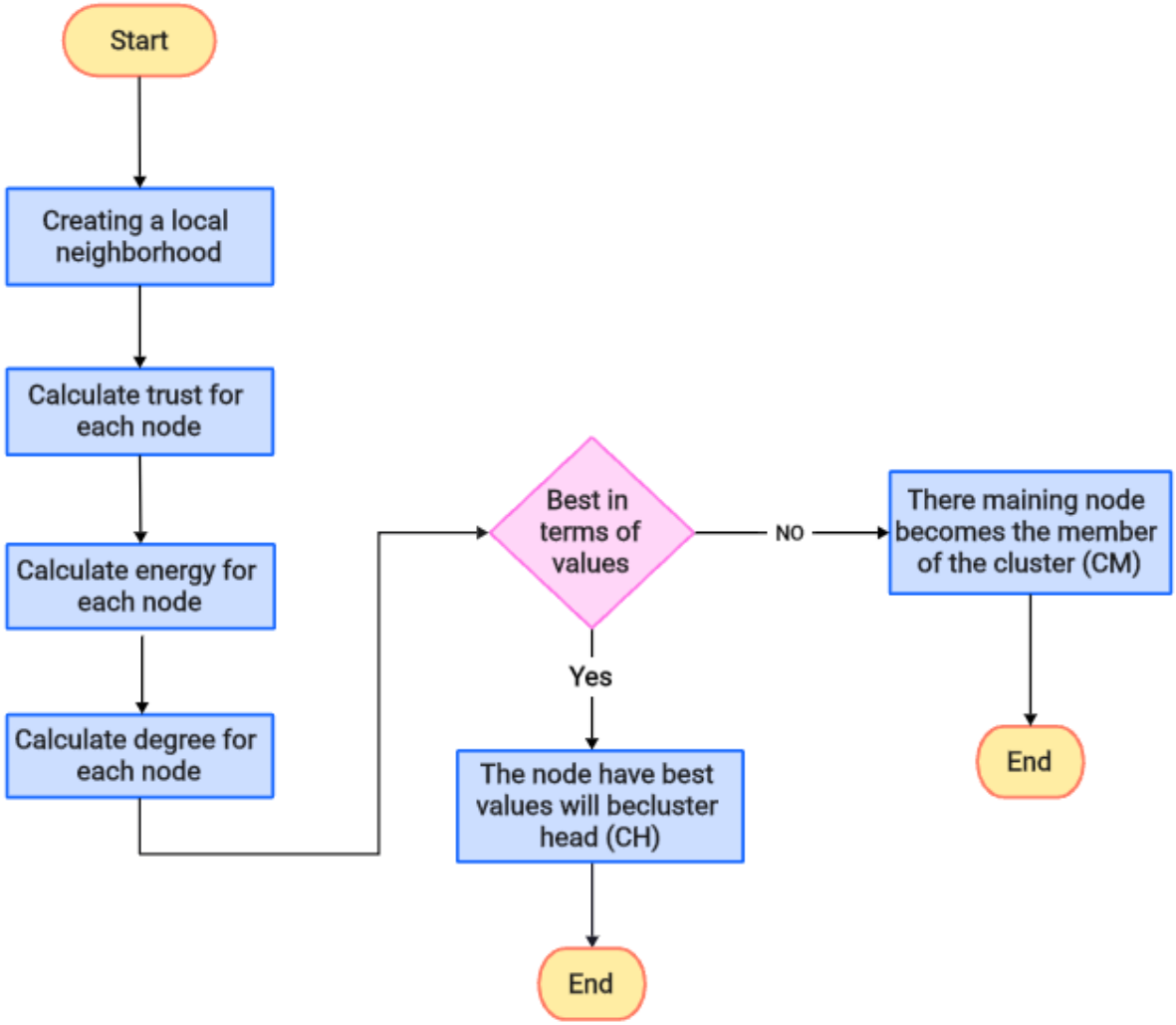

Figure 3.4: Cluster head election process

PSO algorithm

```
# PSO parameters
num_particles = 30
max_iterations = 100
c1 = 2.0
c2 = 2.0
w = 0.7
p1=0.5
p2=0.3
p3=0.1
p4=0.1
# Define the fitness function
def career_goal(sensor):
    return p2*sensor["power"] + p3*sensor["connection"] + p4*sensor["distance"] + p1*sensor["trust"]

# Initialize particles and velocities
particles = []
velocities = []
for i in range(num_particles):
    particle = random.sample(sensor_settings, 20)  # Randomly select 20 sensors as a particle
    particles.append(particle)
    velocities.append([random.uniform(-1, 1) for _ in range(20)])

# PSO main loop
gbest = None
gbest_fitness = float('-inf')

for iteration in range(max_iterations):
    for i, particle in enumerate(particles):
        particle_fitness = sum(career_goal(sensor) for sensor in particle)
        if particle_fitness > gbest_fitness:
            gbest = particle
            gbest_fitness = particle_fitness
```

```
# PSO main loop
gbest = None
gbest_fitness = float('-inf')

for iteration in range(max_iterations):
    for i, particle in enumerate(particles):
        particle_fitness = sum(career_goal(sensor) for sensor in particle)
        if particle_fitness > gbest_fitness:
            gbest = particle
            gbest_fitness = particle_fitness

        for j, sensor in enumerate(particle):
            # Update velocity
            velocities[i][j] = w * velocities[i][j] + c1 * random.random() * (gbest[j]["x"] - sensor["x"]) + c2 * random.random() * (sensor_settings[j]["x"] - sensor["x"])
            # Update position
            particle[j] = sensor_settings[j]  # Reset particle to initial position
            input_to_sigmoid = min(max(velocities[i][j], -10), 10)  # Clip input to sigmoid function
            if random.random() < 1 / (1 + math.exp(-input_to_sigmoid)):  # Sigmoid function for updating position
                particle[j] = sensor_settings[j]

# Select the top sensors as cluster heads and the remaining sensors as cluster members
cluster_head = sorted(gbest, key=career_goal, reverse=True)[:20]
cluster_member = [sensor_settings for sensor in gbest if sensor not in cluster_head]

# Print the settings of all the sensors selected by PSO
print("Cluster Heads:")
for sensor in cluster_head:
    print(sensor)
```

Figure 3.5: PSO algorithm

The type of this PSO algorithm is a Binary PSO (BPSO) algorithm. In BPSO, each particle's position is represented as a binary string, where each bit corresponds to the presence (1) or absence (0) of a particular feature or sensor. The velocity update equation is modified to accommodate the binary nature of the particles' positions. In this specific implementation, the sigmoid function is used to convert the velocity values to probabilities, which are then used to update the particles' positions. This is a common approach in BPSO algorithms. The main characteristics of this BPSO algorithm are: Binary representation of particles' positions Velocity update equation modified for binary positions Sigmoid function used to convert velocity values to probabilities Particles' positions updated based on probabilities BPSO algorithms are often used for feature selection, sensor selection, and other discrete optimization problems.

3.4.3 Evaluation phase

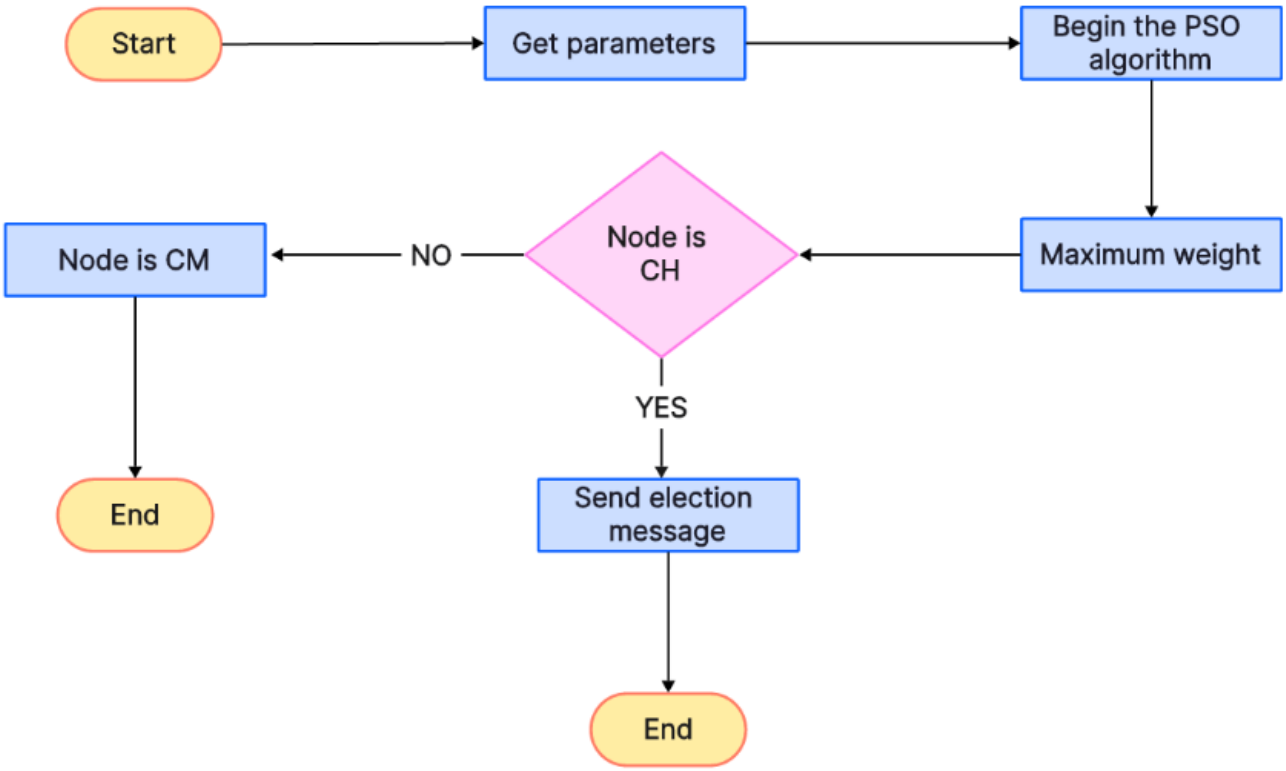

Figure 3.6: Cluster head evaluation phase

- **Data trust calculation :** Data trust is calculated by (Bouhicha and Zohra, 2023) with the following expression:

$$\mathrm{DT} = \frac{S(t) - U(t)}{S(t) + U(t)} \tag{3.7}$$

- The value S represents number of positive actions for data .

- The value U represents number of negative actions for data .

- **Communication trust calculation :** Communication trust is calculated by (Bouhicha and Zohra, 2023) with the following expression:

$$\mathrm{CT} = \frac{S(t) - U(t)}{S(t) + U(t)} \tag{3.8}$$

- The value S represents number of positive actions for routing .

- The value U represents number of negative actions for routing .

- **Energy trust calculation** Energy trust is calculated by (Bouhicha and Zohra, 2023) with the following expression:

$$\mathrm{ET} = \frac{S(t) - U(t)}{S(t) + U(t)} \tag{3.9}$$

- The number of times the energy sensor is close.

- The number of times the energy sensor is far apart .

- **Global trust calculation :** Global trust is calculated by (Saidi, 2021) with the following expression:

$$\mathrm{GT} = \frac{DT + CT + ET}{3} \tag{3.10}$$

3.5 Simulation and analysis

In this study, we simulate a wireless sensor network (WSN) deployed over a large area of 10000 × 10000 square meters. The network comprises 100 sensor nodes scattered across the area to monitor environmental conditions, collect data, and communicate this information back to a central base station located at the coordinates (5000, 5000) — the center of the network.

Each sensor node starts with an initial trust value ranging from 0.5 to 1, indicating its reliability. This trust value can influence the node's interactions and data transmission within the network. Additionally, every node is equipped with an initial energy reserve of 10 Joules, which will be consumed through various operations such as sensing, processing, and transmitting data.

3.5.1 Simulation environment

- ❶ **Processor:** Core(TM) i7-7200U CPU 2.20 GHz .
- ❷ **Ram :** 8,00 Go .
- ❸ **GPU :** 4.0Go.
- ❹ **Operating system** Windows 10 Professional.

Table 3.1: Simulation parameters

Setting	Value
The surface of the network	$10000 \times 10000\,\mathrm{m}^2$
The position of the base station	$X = 5000$, $y = 5000$
The number of nodes	100
Initial node trust	0.5–1
Initial node energy	10J

- ❺ **Python:** Is a cross-platform interpreted programming language, it supports both object and procedural programming and has a large standard library. Python is supported on most operating systems.
- ❻ **Scikit-Learn:** Is a free Python library intended for machine learning, it provides a collection of powerful tools for machine learning and statistical modeling.

3.5.2 Simulation result

1. **The beginning of the algorithm**

   First, we have the blue points representing a group of cluster members distributed over the surface of the network, and the red point is the base station and is located in the center of the surface of the network, as shown in figure (3.7).

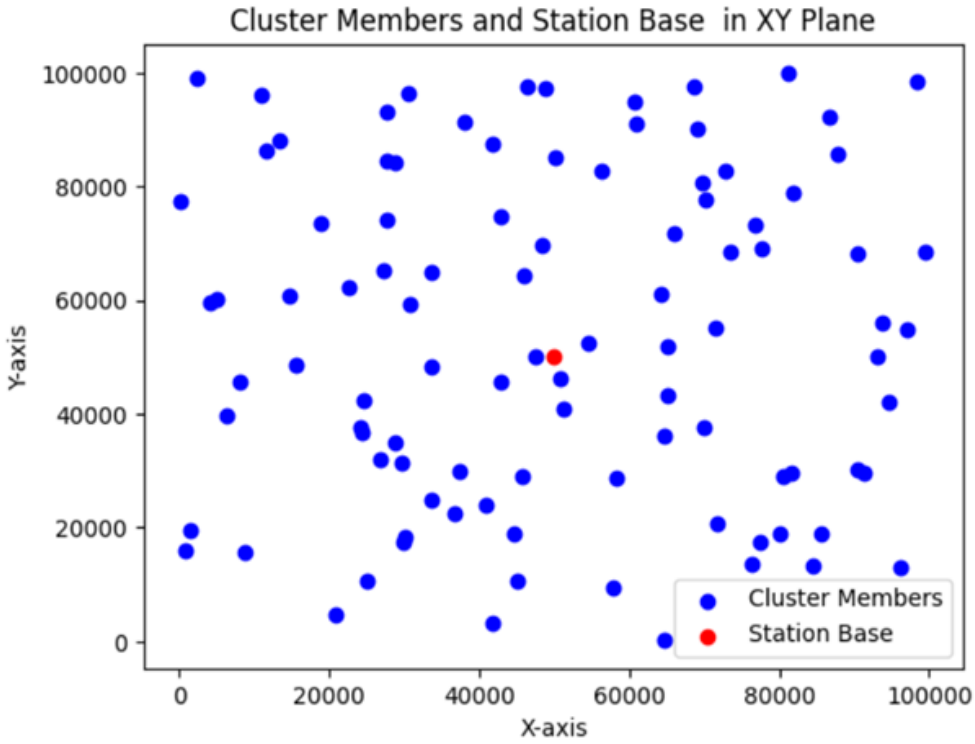

Figure 3.7: Initial clusters distribution

2. Identify the clusters head

After applying the PSO for cluster head selection due to its effectiveness in optimizing cluster formation based on various criteria such as energy efficiency, network coverage, and lifetime maximization algorithm, we identified a group of clusters head , The green dots in the figure (3.8) shows the group of clusters head that were chosen by the PSO algorithm, while the red dot represents the base station.

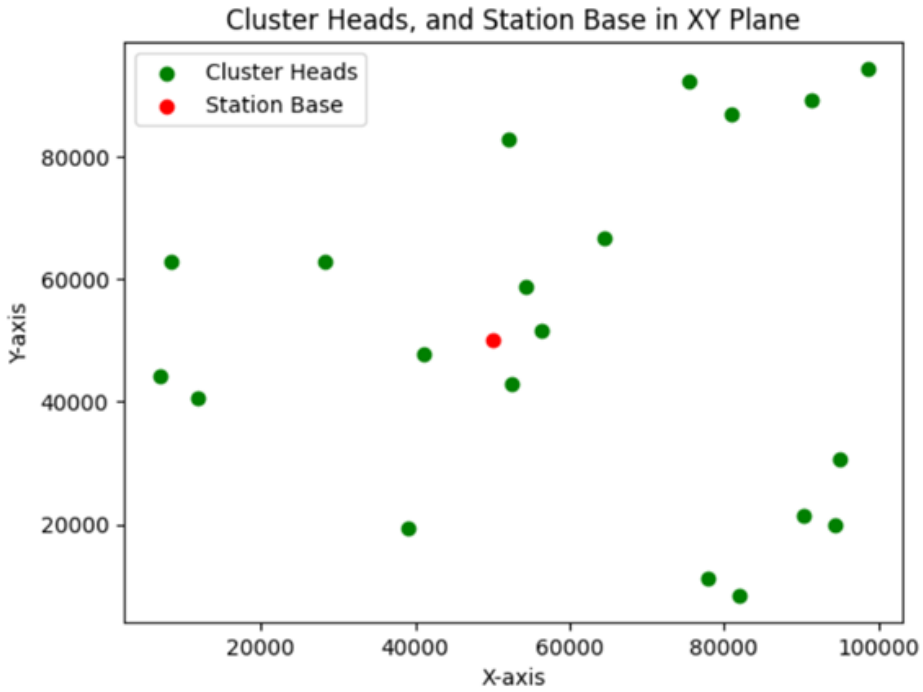

Figure 3.8: Clusters head chosen

3. Identify the clusters head with clusters members

The figure (3.9) shows the total distribution of clusters heads chosen by the PSO algorithm along with the distribution of clusters members, where the blue dots represent the distribution of clusters members and the green dots represent the distribution of clusters head while the red dot is the base station.

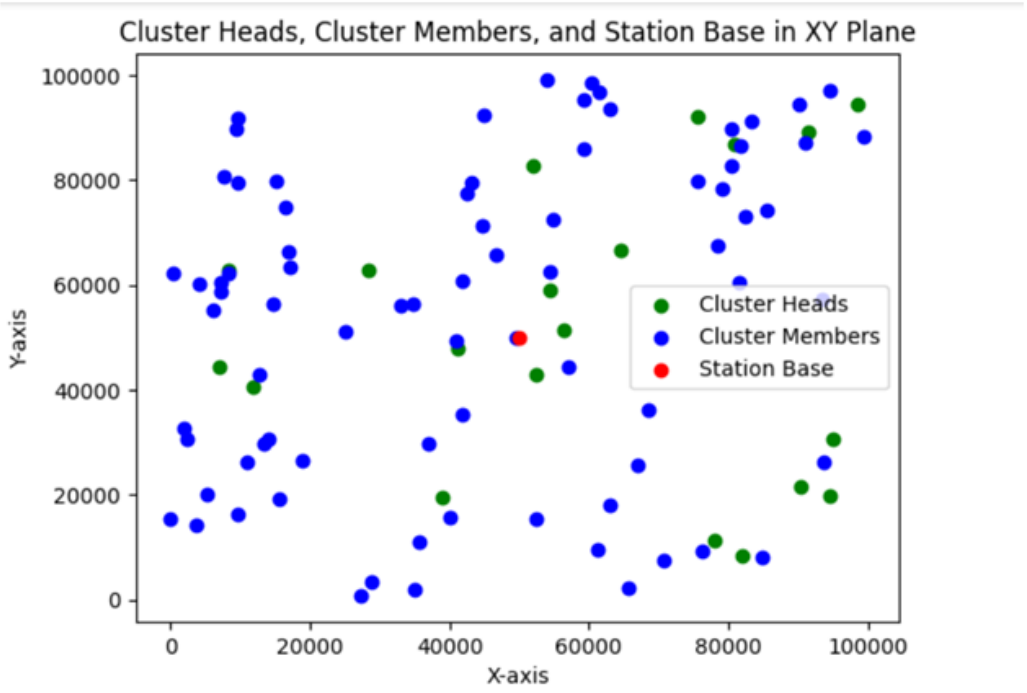

Figure 3.9: Distribution of clusters after PSO algorithm

4. Energy distribution curve

The curve in figure (3.10) represents the energy consumed by the Clusters in terms of numbers of iterations. We note that for the trusted sensors, the energy percentage was high and then gradually decreased as the numbers of iterations passed until it was non-existent, while the untrusted sensor energy was low and then decreased until it was non-existent.

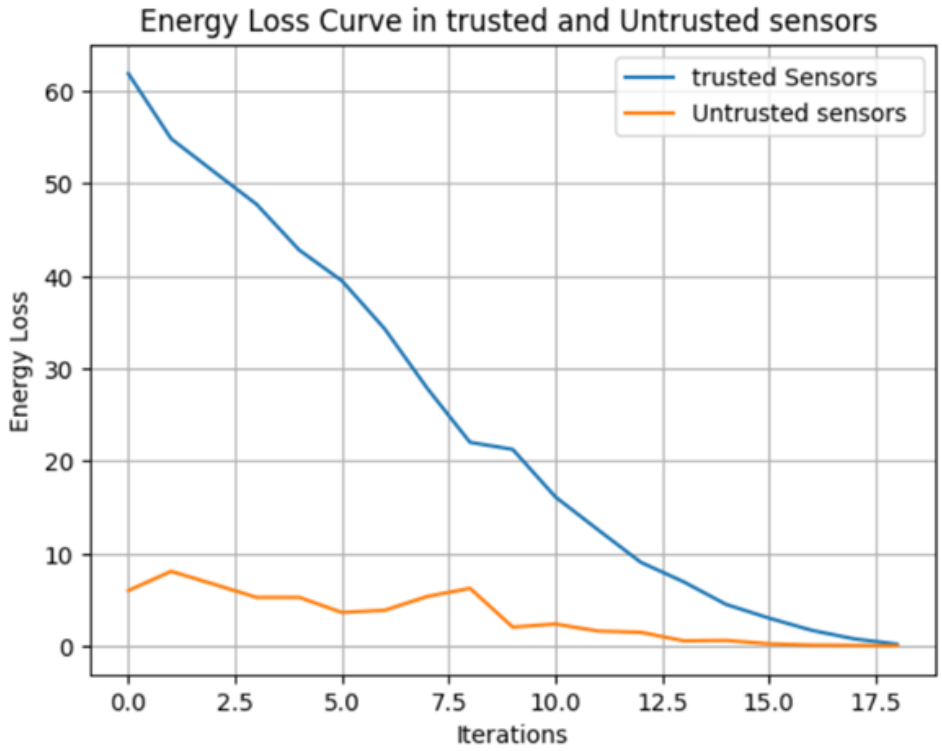

Figure 3.10: Energy distribution in trusted and untrusted sensor

5. Energy consumption at clusters head

The curve in figure (3.11) represents the energy consumed by the Clusters head in terms of numbers of iterations, we notice a rapid decrease in energy as the stages pass until it ceases to exist. This is due to the clusters head communicating with a large number of clusters numbers, as well as receiving a large number of information.

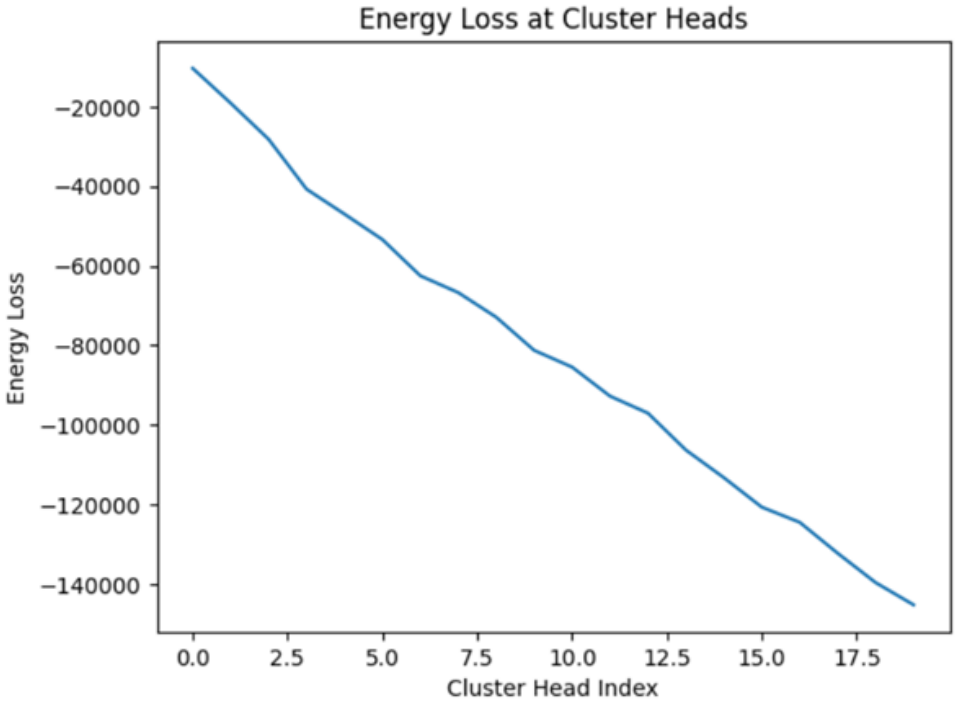

Figure 3.11: Energy loss at cluster head

6. Connection value for trusted and untrusted sensors

The figure (3.12) represents the number of connections between trusted and untrusted sensors. We note that trusted sensors have a higher connection than untrusted nodes.

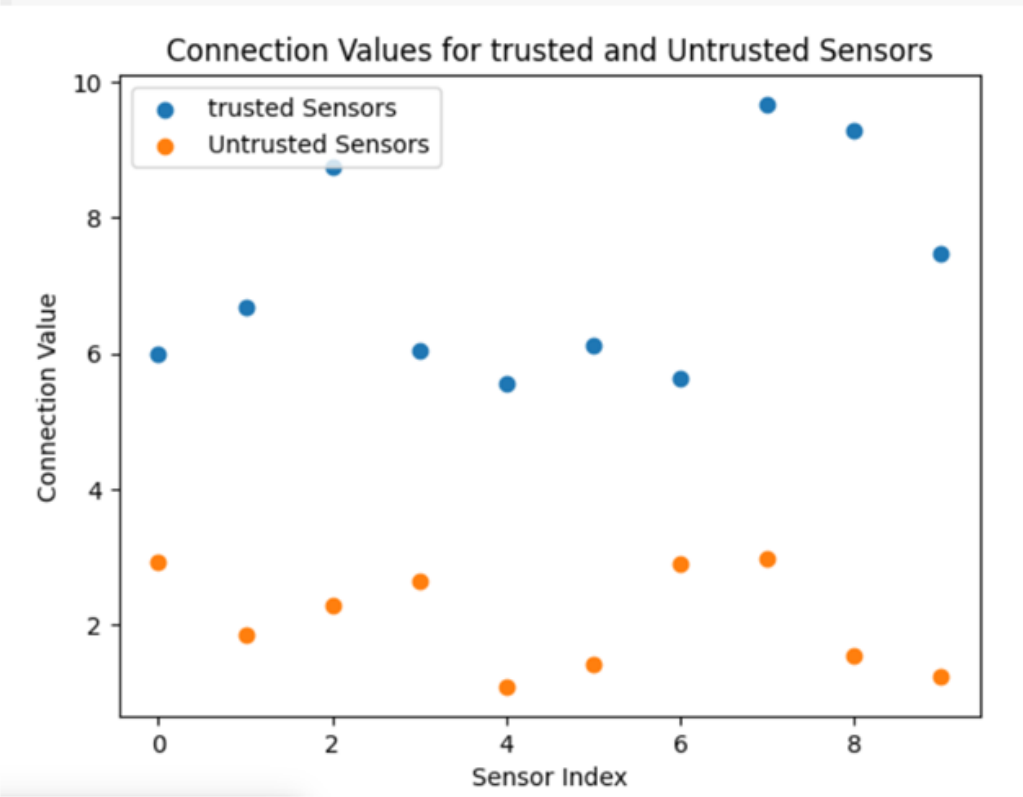

Figure 3.12: Connection value for trusted and untrusted sensors

7. **Trust value for trusted and untrusted sensors**

The figure (3.13) represents the trust between trusted and untrusted sensors. We note that trusted sensors have a higher trust than untrusted nodes.

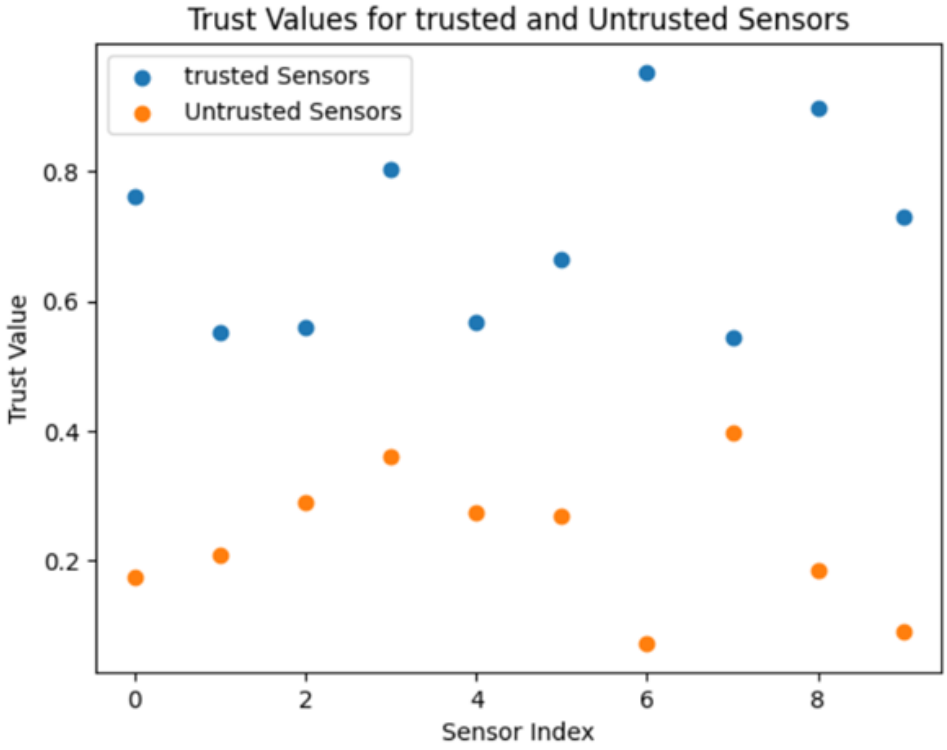

Figure 3.13: trust value for trusted and untrusted sensors

3.6 Conclusion

In this chapter, we defined the architecture of our proposed model for detecting bad behavior in wireless sensor networks. We thoroughly described the working environment and the conditions under which our model was tested. Based on the results obtained from our experimental simulations, our model demonstrates superior performance in identifying malicious nodes compared to existing approaches. The findings indicate that our model not only enhances detection accuracy but also improves overall network security and efficiency. These results underscore the potential of our model to be implemented in real-world wireless sensor network scenarios, providing a robust solution for mitigating security threats.

GENERAL CONCLUSION

We are in an era where sensor networks penetrate all areas, and the limited power of sensor nodes poses a major challenge, making it necessary to develop innovative solutions to conserve energy and extend sensors life. This thesis aims to address energy and transportation problems in sensor networks, focusing on detecting malicious nodes and optimizing energy consumption. To address this challenge, we proposed a model that evaluates the Connection between nodes and data and energy and distance. We used binary particle swarm optimization (BPSO) to select the most reliable cluster heads. Then classify nodes into normal and malicious categories.

Our results demonstrate the effectiveness of our proposed model in detecting malicious nodes and improving energy consumption. We successfully classified nodes into normal and malicious classes and selected trusted cluster heads, which demonstrated the differences in energy, connectivity, and reliability between trusted and untrusted clusters. However, an important limitation of our current architecture is scalability issues, especially in very large networks. Future research directions include developing more scalable architectures that can efficiently manage large networks. Improving the cluster head selection process using advanced algorithms can also contribute to improved scalability, ensuring that performance does not degrade as the network scales. The implications of our results are twofold, contributing to the development of more robust and resilient architectures for sensor networks and enabling more efficient energy management and extending network lifetime in real-world scenarios.

BIBLIOGRAPHY

Abdesselam, A. and Belouatek, M. (2012-2013). Conception d'un algorithme de routage basé sur l'heuristique du recuit simulé pour les réseaux de capteurs à grande échelle. Mémoire de fin d'études, Université Abou Bakr Belkaid– Tlemcen, Tlemcen. Pour l'obtention du diplôme de Master en Informatique.

Aggarwal, C. C. and Reddy, C. K. (2014). *Data Clustering: Algorithms and Applications*. Taylor & Francis Group, LLC.

Aghiles, N. A. (2013). *Sécurité par chiffrement dans les réseaux de capteurs sans-fil*. PhD thesis, Université Mouloud Mammeri.

Ahmed, M. R., Huang, X., Sharma, D., and Cui, H. (2012). Wireless sensor network: characteristics and architectures. *International Journal of Information and Communication Engineering*, 6(12):1398–1401.

Akkaria, W., Bouhdida, B., and Belghith, A. (2015). Leatch: Low energy adaptive tier clustering hierarchy. *Procedia Computer Science*, page 366.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer networks*, 38(4):393–422.

Ali, O. (2011). *Prise en charge d'un grand nombre de capteurs sans fil dans 6 LoWPAN*. PhD thesis, Université Mouloud Mammeri.

Athmani, S. (2018). *Protocoles pour la sécurité des réseaux de capteurs sans fil*. PhD thesis, Université de Batna 2.

Benahmed, K. (2011). *Surveillance distribuer pour la sécurité d'un réseau de capteurs sans fil*. PhD thesis, Thèse de Doctorateninformatique. Universitéd'Oran, Algérie.

Benahmed, K., Merabti, M., and Haffaf, H. (2012). Distributed monitoring for misbehaviour detection in wireless sensor networks. *SECURITY AND COMMUNICATION NETWORKS*, pages 392–394.

Benahmed, K., Saidi, A., and Seddiki, N. (2018). *Attacks and countermeasures in Wireless sensor networks.* Publisher.

Benouda, H. and Benabderrahmane, Y. (2022–2023). *Approche de sécurité adaptative pour la détection d'intrusion dans les réseaux capteur sans fil.* PhD thesis, Université de Ghardaia.

Berrachedi, A. and Diarbakirli, A. (2009). Sécurisation du protocole de routage hiérarchique leach dans les réseaux de capteurs sans fil.

Bettahar, H. and Challal, Y. (2008). Introduction à la sécurité informatique. Supports de cours, Systèmes Intelligents pour le Transport.

Blum, C. (2005). Ant colony optimization: Introduction and recent trends. *Physics of Life reviews*, 2(4):353–373.

Boudhir, A. (2013). Contributions to the energy optimization for security, localization and routing in wireless sensor networks.

Bouguer, S. (2012). *Étude et simulation comparative entre les réseaux de capteurs sans fils traditionnels et les réseaux de capteurs véhiculaires.* PhD thesis, Université Tlemcen.

Bouhicha, A. and Zohra, K. F. (2022/2023). *Une approche d'apprentissage automatique pour la détection des mauvais comportements dans les réseaux de capteurs sans fil.* PhD thesis, Université de Ghardaia.

Boussag, L. (2017). *Implementation and Simulation of Security Protocols for Wireless Sensor Networks (WSNs).* PhD thesis, FACULTY: mathematics and informatics DEPARTEMENT of computer science ….

Challal, Y. (2008). Réseaux de capteurs sans fils. *Cours, Systèmes Intelligents pour le Transport, Université de Technologie de Compiègne, France*, 17.

Chatterjee, M., Das, S. K., and Turgut, D. (2002). Wca: A weighted clustering algorithm for mobile ad hoc networks. *Kluwer Academic Publishers*, pages 195–197. Manufactured in The Netherlands.

Chaudhary, R. and Vatta, D. S. (2014). A tutorial of routing protocols in wireless sensor networks. *International Journal of Computer Science and Mobile Computing*, 3(6):971–979.

Chaurasia, B. K. and Tomar, R. S. (2012). Trust management model for wireless ad hoc networks. page 2. Springer. Proceedings of the International Conference on SocProS.

Choi, W. and Woo, M. (2006). A distributed weighted clustering algorithm for mobile ad-hoc networks. In *the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT/ICIW)*, pages 2–3.

Cormen, T. H., Leiserson, C. E., Rivest, R. L., and Stein, C. (2022). *Introduction to algorithms*. MIT press.

Dahane, A., Berrached, N.-E., and Loukil, A. (2015). Balanced and safe weighted clustering algorithm for mobile wireless sensor networks. In *International Conference on Computer Science and Its Applications (CIIA)*, pages 434–439.

Djedouboum, A. C., Abba Ari, A. A., Gueroui, A. M., Mohamadou, A., and Aliouat, Z. (2018). Big data collection in large-scale wireless sensor networks. *Sensors*, 18(12):4474.

Elhabyan, R., Shi, W., and St-Hilaire, M. (2019). Coverage protocols for wireless sensor networks: Review and future directions. *Journal of Communications and Networks*, 21(1):45–60.

Fahmy, H. M. A. (2020). *Wireless sensor networks*. Springer.

Falcone, R. and Castelfranchi, C. (2010). Transitivity in trust. page 2.

Guerti, M. and Halilem, A. (2020). *Améliorer les performances des RCSFs à l'aide de protocole de routage basé sur le clustering*. PhD thesis, .

Han, J. and Kamber, M. (2006). *Data Mining: Concepts and Techniques*. Morgan Kaufmann.

Han, J., Pei, J., and Kamber, M. (2011). *Data Mining: Concepts and Techniques*. Elsevier.

Hastie, T., Tibshirani, R., Friedman, J. H., and Friedman, J. H. (2009). *The elements of statistical learning: data mining, inference, and prediction*, volume 2. Springer.

Heinzelman, W. B. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS google schola*, 2.

Hussain, S., Matin, A. W., and Islam, O. (2007). Genetic algorithm for energy efficient clusters in wireless sensor networks. In *Fourth International Conference on Information Technology*, pages 2–4. IEEE.

Jain, M., Saihjpal, V., Singh, N., and Singh, S. B. (2022). An overview of variants and advancements of pso algorithm. *Applied Sciences*, 12(17):8392.

Jawarkar, U., Panchore, P., and Deshmukh, S. (2013). Overview of wireless sensor network and its applications. *International Journal of Electronics Communication and Computer Engineering*, 4(2):29–32.

Karlof, C. and Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, 1(2-3):293–315.

Keerthika, M. and Shanmugapriya, D. (2021). Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures. *Global Transitions Proceedings*, 2(2):362–367.

Lamine, M. M. (2008). Securite dans les reseaux de capteurs sans-fil. *Memoire de Magistere en Informatique Ecole Doctorale d'Informatique de bejaia*.

Laroussi, N. (2012). Secure routing in wireless sensors networks. Master thesis, National Engineer School of Sfax.

Lasla, N. (2007). La gestion de clés dans les réseaux de capteurs sans-fil. *Mémoire de Magister, Institut National de formation en Informatique (INI), Oued-Smar, Alger*.

Makhmouk, D. and Melouk, S. Approche de minimisation de la consommation d'énergie dans les réseaux de capteurs sans fil. Master's thesis.

McEvily, S., Perrone, V., Zaheer, A., and Marinova, S. (2016). Trust asymmetry and knowledge sharing in r&d alliances. *Strategic Management Journal*, page 742.

Mehmeti, A., Xhafa, K., and Gani, A. (2009). Clustering algorithms in mobile ad hoc networks. In *Conference on Computer Sciences and Convergence Information Technology*, page 1. IEEE.

Millán, L., Encinas, H., López, M., and Arribas, N. (2009). Inter-domain public key infrastructure trust management: Requirements, architecture, and performance. *Network and Computer Applications*, page 347.

Mitchell, T. M. (1997). *Machine Learning*. McGraw-Hill Science/Engineering/Math.

Murphy, K. P. (2012). *Machine Learning: A Probabilistic Perspective*.

Nabil Mekki, M. k. (2018). *Techniques de conservation d'énergie pour les réseaux de capteur sans fil*.

Nabila, M. and Kahina, M. (2017). *Approches du clustering dans les réseaux de capteurs sans fil*. PhD thesis, Université Mouloud Mammeri.

Nayyar, A. (2017). *Improvised Energy Efficient Routing Protocol based on Ant Colony Optimization (ACO) for Wireless Sensor Networks*. PhD thesis, Department of Computer Science, Desh Bhagat University Mandi Gobindgarh, India.

Ngom, D. (2016). *Optimisation de la durée de vie dans les réseaux de capteurs sans fil sous contraintes de couvertureet de connectivité réseau*. PhD thesis, Université de Haute Alsace-Mulhouse; Université Cheikh Anta Diop (Dakar).

Palan, N., Barbadekar, B., and Patil, S. (2017). Low energy adaptive clustering hierarchy (leach) protocol: A retrospective analysis. In *International Conference on Inventive Systems and Control ICISC*, page 2.

Priya, N. M. and Brindha, G. (2016). A survey on routing protocols in wireless sensor networks. In *International Conference on Computer Applications*, volume 38, page 45.

Rachida, A. (2011). *Sécurisation du protocole de routage direted diffusion dans les réseaux de capteurs sans fil*. PhD thesis, Université Mouloud Mammeri.

Reddy, T. A. (2011). *Applied Data Analysis and Modeling for Energy Engineers and Scientists*. The Design School and School of Sustainability, Arizona State University.

Riham, S. and Yagoub, M. C. (2014). Pso-hc: Particle swarm optimization protocol for hierarchical clustering in wireless sensor networks. In *International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pages 419–420.

Sadiqui, A. (2019). *Sécurité des réseaux informatiques*. ISTE Group.

Saeedi, I. D. I. and Al-Qurabat, A. K. M. (2021). A systematic review of data aggregation techniques in wireless sensor networks. In *Journal of Physics: Conference Series*, volume 1818, page 012194. IOP Publishing.

Sahoo, R. R., Sardar, A. R., Singh, M., Ray, S., and Sarkar, S. K. (2015). A bio-inspired and trust-based approach for clustering in wsn. *Springer Science+Business Media Dordrecht*, page 10.

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

Sahraoui, S. (2016). *Mécanismes de sécurité pour l'intégration des RCSFs à l'IoT (Internet of Things)*. PhD thesis, Université de Batna 2.

Saidi, A. (2021). *Models and mechanisms for surveillance of Wireless Sensor Networks*. PhD thesis, University-Bechar.

Sanhaji, F., Satori, H., and Satori, K. (2017). Clustering based on neural networks in wireless sensor networks. In *Proceedings of the International Conference on Computing and Wireless Communication Systems (ICCWCS'17)*, Larache, Morocco.

Sanhaji, F., Satori, H., and Satori, K. (2019). Cluster head selection based on neural networks in wireless sensor networks. *IEEE*.

Seboru, Y. (2023). What are the most secure methods for ensuring data integrity. `https://www.linkedin.com/pulse/what-most-secure-methods-ensuring-data-integrity-yusuf-seboru`.

Selvaraja, C. and Anand, S. (2012). Security issues of reputation management systems for peer-to-peer networks. *Elsevier*, pages 151–156.

Sen, J. (2012). Security in wireless sensor networks. page 2.

Singh, I., Pooja, and Varsha (2017). Neural network based leach clustering algorithm in wsn. *IJCSN International Journal of Computer Science and Network*, page 5.

Sofiane, M. and Bouabdallah, N. (2008). La consommation d'énergie dans les réseaux de capteurs sans fil. *Rapport de recherche, Institut De formation supérieure en informatique et communication IFSIC, Rennes*, 17.

Tlili, L. (2011). *Modèle de confiance pour sécuriser le routage dans les réseaux de capteurs sans fil*. Thèse de doctorat, Université Mouloud Mammeri.

Wei, D., Kaplan, S., and Chan, H. A. (2008). Energy efficient clustering algorithms for wireless sensor networks. pages 236–237.

Xia, F. (2009). Wireless sensor technologies and applications.

Younis, O. and Fahmy, S. (2004). Heed: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *TRANSACTIONS ON MOBILE COMPUTING*, page 3.

APPENDIX

République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de La Recherche Scientifique
كلية العلوم والتكنولوجيا
Faculté des Sciences et de la Technologie
قسم الرياضيات و الإعلام الآلي
Département des Mathématiques & de l'Informatique
جامعة غرداية
Université de Ghardaia

شهادة الترخيص بالإيداع

أنا الأستاذ : سليمان بالاعور

بصفتي رئيس لجنة المناقشة والمسؤول عن تصحيح مذكرة الماستر الموسومة بـ:

Secure Clustering Approach based on Particle Swarm Optimization Algorithm in Wireless Sensor Networks

من إنجاز الطالب: **بوعامر أحمد ياسين**

والطالب: **شرقي أكرم**

الكلية: العلوم والتكنولوجيا
القسم: الرياضيات والإعلام الآلي
الشعبة: إعلام آلي

التخصص: الأنظمة الذكية لاستخراج المعارف
تاريخ المناقشة: 2024/26/24

أشهد أن الطلبة قاموا بالتصحيحات المطلوبة من طرف لجنة المناقشة وأن المطابقة بين النسخة الورقية والالكترونية استوفيت جميع شروطها.

مصادقة رئيس القسم

إمضاء المسؤول عن التصحيح