Kurdistan Region Government/Iraq
Presidency of the Council of Ministers
Ministry of Higher Education & Scientific Research
Erbil Polytechnic University
Technical Engineering College
Information System Engineering Department

PCD and DCPN Detection Algorithms for Securing WSN

A Thesis

Submitted to the Council of the College of Technical Engineering at Erbil Polytechnic University, in Partial Fulfillment of the Requirements for the Degree of Master of Information System Engineering

By

Kurdistan Wns HamaAli

B.Sc. Information System Engineering

Supervised by

Assist. Prof. Dr. Reben Mohammad Saleem Kurda

Erbil- Kurdistan Region

February 2023

بسم الله الرحمن الرحيم

(نَرْفَعُ دَرَجاتٍ مَنْ نَشاءُ وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ)

سورة يوسف - أ ية 79

Declaration

I declare that the Master Thesis entitled: “PCD and DCPN Detection algorithms for Securing WSN” is my own original work, and hereby I certify that unless stated, all work contained within this thesis is my own independent research and has not been submitted for the award of any other degree at any institution, except where due acknowledgment is made in the text.

Signature:

Student Name: **Kurdistan Wns HamaAli**

Date: /2/2023

Linguistic Review

I can affair that I have carefully reviewed the thesis titled “PCD and DCPN Detection algorithms for Securing WSN” Also, from an English linguistic point of view, I can fully approve that this thesis is free of both grammatical and spelling mistakes.

Signature:

Name: **Assistant Lecturer Xalid AbdulJabar AbdulHamid**

Date: 10/10/2022

Supervisor Certificate

This thesis has been written under my supervision and has been submitted for the award of the degree of Master of Information System Engineering with my approval as supervisor. .

Signature:

Name: **Assist. Prof. Dr. Reben Kurda**

Date: /2/2023

I confirm that all requirements have been fulfilled.

Signature:
Name: **Dr. Roojwan Sc. Hawezi**

Head of the Department of Information System Engineering

Date: /2/2023

I confirm that all requirements have been fulfilled.

Postgraduate Office
Signature:

Name:

Date: /2/2023

Examining Committee Certification

We certify that we have read this thesis: “PCD and DCPN Detection algorithms for Securing WSN” and as an examining committee examined the student (**Kurdistan Wns HamaAli**) in its content and what related to it. We approve that it meets the standards of a thesis for the degree of Master in Information System Engineering.

Signature:
Name: **Assist. Prof. Dr. Kayhan Zrar**
Member
Date: /2/2023

Signature:
Name: **Assist. Prof. Dr. Shavan Askar**
Member
Date: /2/2023

Signature:
Name: **Assist. Prof. Dr. Reben Kurda**
Supervisor and Member
Date: /2/2023

Signature
Name: **Prof. Dr. Subhi Rafeeq**
Chairman
Date: /2/2023

Approved by:
Dean of the College of Erbil Technical Engineering
Signature:
Name: **Prof. Dr. Ayad Zaki Saber**
Date: /2/2023

Acknowledgements

In the name of Allah, the Merciful and the Compassionate. We are grateful to Almighty Allah for supporting us in order to complete this thesis. We are also grateful to those people who have contributed in the completion of this work.

I am grateful to Professor Dr. Reben Kurda for being the best guider and advisor for us during the completion of this research work requirement in all fields. His ideas and inspirations have helped me make this idea of mine into a fully-fledged project. Without, I may never had tried research works.

Again I am thankful to my batch-mates for supporting me at times of my implementation part. I am also grateful to all the professors in my department for always being a constant source of inspiration and motivation during the entire course of the project.

Lastly, I thank both of my parents, my brother, and especially my husband for all their encouragement, support and guidance which enabled me to reach this stage in my research project.

Dedication

This thesis is dedicated to Almighty Allah,

Asking for acceptance while also hoping that this will be a good work for all the fellow scholars and researchers.

For all people who never lost hope in me and always believed in me.

To my brother who supported me and helped me to complete this study.

To my mother who raised and guided me throughout my whole life while always supporting me in each and step.

To my husband who was always on my side no matter what.

Abstract

The integration of Five Generation networks and Wireless Sensor Networks is crucial for the new area of the Internet of Things, which is used for a wide range of applications. Such as: daily living, manufacturing, health care and transportation, etc. Wireless sensor networks consist of small sensor nodes with limited energy. Such nodes have the ability to monitor the physical conditions and communicate information among the nodes without the requirement of the transmission medium. Wireless Sensor Networks are autonomous and are distributed in space. Due to the absence of central authority and random deployment of nodes in the network, Wireless Sensor Network is prone to security threats.

Wireless Sensor Network are vulnerable to so many network layer attacks such as wormhole and replay attacks. Also, Energy conservation is critical in Wireless Sensor Network because the main source of power for sensor nodes is battery with a limited energy. It cannot be easily replaced or recharged. Therefore, power saving is essential to increase the lifetime of sensor nodes. Attackers compromise the internal sensor nodes from which they launch attacks. By sending malicious information, attackers may decrease the sensor nodes' lifetime from years to days and have a severe impact on the energy of the sensor network. Therefore, The larger amount of energy consumed by sensor nodes during the illegal packet transmission by the attackers. Our work proposed a Detect and Compare Packet Nonce (DCPN) algorithm and Packet Count Detection (PCD) algorithm for Wireless Sensor Networks. These algorithms efficiently identify and isolate attacks like wormhole and replay while avoiding possible service degradation like energy consumption in sensor nodes. The simulation results show that our mechanism can outperform existing techniques in terms of energy consumption and lifetime of sensor nodes. DCNP saves energy by (21.6%) per hour for a wormhole attacks, whereas PCN saves up energy by (12%) per hour for replay attacks, thus increases the lifetime of the sensor node by (19.2%) per hour when using DCPN and by (12%) per hour when using PCD. Finally, the study also shows the temperature monitoring of some mobile sensor nodes. By implementing these algorithms, the temperature of the sensors can be reduced by (1^{0}C- 2.5^{0}C) per (2.5) minutes.

Table of Contents

List of Figures

List of Tables

List of Algorithms

List of Abbreviations

Abbreviation	Acronyms
AdS	Adversary Sensor
AES	Advanced Encryption Standard
AOMDV	Ad-hoc on Demand Multipath Distance Vector
ARP	Address Resolution Protocol
AS	Anchor Sensor
BS	Base Station
dBm	Decibel milliwatts
DCPN	Detect and Compare Packet Nonce
DES	Discrete Event System
DNS	Domain Name System
DoS	Denial of Services
DP	Detection Packet
FP	Feedback Packet
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
M_Snode	Mobile Sensor node
MAC	Media Access Protocol
MAP	Message Authentication and Passing
MCRP	MAC Centralized Routing Protocol
MCRP	MAC Centralized Routing Protocol
MHz	Megahertz
OSI	Opens System Interconnect
PCD	Packet Count Detection
PDR	Packet Delivery Ratio
PRD	Packet Delivery Ratio
PSO	Particle Swarm Optimization
RAP	Receiver Authentication Protocol
RPC	Random Password Comparison
RSSI	Received Signal Strength Indicator
SIC	Synchronized Incremental Counter
SNs	Sensor Nodes
St_Snode	Static Sensor node
TBID	Trust Based Identity Detection
TDMA	Time Division Multiple Access
WRHT	Wormhole Resistant Hybrid Technique
WSN	Wireless Sensor Network

CHAPTER ONE: INTRODUCTION

1.1 Overview

The Internet of Things (IoT) is a new technology that requires the integration of Five Generation (5G) networks and Wireless Sensor Networks (WSNs). 5G communication technologies encourage the use of mobile networks to not only link people, but to also connect machines and other things and control them(Martínez et al., 2017). This integration is essential for a broad variety of different applications, including remote surgery, self-driving cars, virtual reality, health care, smart city, flying drones, security and surveillance, and many more. These applications contribute and support the day-to-day activities of the community. In this kind of communication environment, every device and user communicates with one another through the internet. One way to think about IoT is as a more advanced form of WSNs. WSN is a network of geographical diverse autonomous devices that are employing sensors to monitor physical/environmental factors such as temperature, sound, and motion/pollutants at various places (Galkin, 2018). However, 5G technology provide an IoT network architecture that is full coverage, fast, and energy efficient. But the amount of energy used by sensors in WSNs is a key problem. Sensor nodes in WSN are devices with limited energy, bandwidth, storage, and processing resources. There are characterized by sensor devices that are powered by batteries. That is need some kind of plan to extend the amount of time that sensor devices can run on their batteries(Dâmaso et al., 2017).

WSNs are used in critical monitoring and control applications. Therefore, Security is another issue that WSNs confront nowadays. In today's technological advanced world, every device a human uses is linked to the Internet. This raises the possibility of sensitive material leaking even more. A single error in this system may negatively impact its overall performance. This is the primary disadvantage of this kind of communication. If information is not managed appropriately, sensitive information may be disclosed to a third party. Therefore, robust authentication, access control, intrusion detection, and privacy preservation protocols are essential for IoT connection in order to prevent any sort of attacks that lead to data leaking (Ahmad et al., 2018). WSNs are vulnerable to a wide variety of attacks due to the fact that they are open networks that only include a limited number of nodes at each location. It's possible that some of them are susceptible to a variety of attacks(Hou et al., 2019) Therefore, it is possible for the confidential information to be disclosed due to illegal access and manipulation. Eavesdropping, compromised nodes, interruption, modification, or injection of malicious packets are the most common types of threats that may be posed to the security of a WSN (Abidin, 2018). Attackers compromise the internal sensor nodes from which they lunch attacks. By sending malicious information to the sensor nodes in WSN network and have severe impact on the energy of the sensor networks (Dutta et al., 2019, Rajaram et al., 2020b). Therefore, it is necessary to safeguard the communication of IoT devices at all times from any conceivable threat. The large amount energy consumed by sensors during the illegal packet transmission by malicious node. As a result, it reduces the lifetime of sensor nodes.

Network layer attacks present security risks to WSNs.. In order to conduct attacks that are difficult to detect, attackers hack the internal sensor nodes that are located across the network (Jaitly et al., 2017). The operation of adversary nodes in a network is similar to that of other normal nodes in the network. But, after catching the network, adversary nodes can perform the additional function of searching for and discarding critical malicious messages to disrupt the whole network by minimizing the energy of nodes. Therefore, detecting network layer attacks is essential. (Kaur and Sandhu, 2021).

The use of a WSN in the design phase is essential for identifying security vulnerabilities. Furthermore, understand the impact (especially the power consumption impact) of the most typical attacks on a node (or the entire network) help to prevent possible problematic vulnerabilities. Proposed a Detect and Compare Packet Nonce (DCPN) algorithm is used to detect wormhole attacks and Packet Count Detection (PCD) algorithm is used to detect replay attacks. There is also an adaptive control that reduces the energy consumption of the sensor nodes and increases their lifetime.

1.2 Problem Statement

WSN is faced with security issues today. Therefore, WSNs are vulnerable to a wide variety of attacks due to the fact that they are open networks with limited resources of nodes that only include a limited number of nodes at each location. As a result, any loss of security in these systems may have real and direct consequences on efficiency and safety on whole of WSN network. Eavesdropping, node compromising, interruptions, modifications, or injection of malicious packets to change the behavior of the packets, compromised privacy are the most common types of attacks that may be launched against the security of WSNs. The attacker can compromise the internal network by sending illegal information, which will decrease the lifetime of sensors from years to days and have a severe impact on the energy of the sensor network. Due to the fact that the sensors have limited resources such as storage space, processing power, and energy, devices are susceptible to being readily influenced by attackers.

In the WSN, energy conservation is a major concern. Because the main source of power for sensor nodes is a battery with limited energy, it cannot be easy to replace or recharge. Therefore, power saving is very important to increase the lifetime of sensors. Energy consumption refers to the entire amount of energy that is used by network in order to carry out transmission and communication between nodes. The large amount of energy consumed by sensors during the illegal information transmission by the malicious (adversary) node. As a result, it reduces the lifetime of sensor nodes. Also, due to high processing in the sensors for transmitting and receiving malicious data, this has a direct influence on the temperature of the sensors. The most logical strategy to minimize the amount of energy that is used is to decrease the number of illegal packets that are exchanged between sensor nodes.

1.3 The Aim of Research

Designing WSN at the early stage is very important for identifying security vulnerabilities, and it is also very important to understand the power consumption that will impact the lifetime of sensors in WSN. The aim of this research is to demonstrate two techniques for detecting network layer attacks on WSNs, such as wormhole and replay attacks. By implementing these algorithms, they protect the WSN environment against these attacks, and the sensor nodes' overall energy consumption is significantly reduced, which is done by decreasing or eliminating malicious data. That would be beneficial since it would considerably increase the network’s lifetime. Also, the temperature of the sensor nodes would be stable.

1.4 Research Objectives

The main objective of this research is to propose two algorithms that are used to detect two types of network layer attacks in WSN. This study concentrated on the following objectives:

- To protect WSN environment against any type of attack by monitoring the gathering, processing, and transmission of data from sensor networks.

- The proposed algorithms are used to detect network layer attacks such as (wormhole attacks and replay attacks).
- To save the energy consumption of the sensor nodes by eliminating the malicious data that are sent by illegal nodes.
- To increase the lifetime of the sensor nodes by reducing energy consumption.
- To monitor the temperature of the sensor nodes due to high processing in the sensors for transmitting and receiving malicious data that directly affects WSNs.
- This detection scheme doesn’t need any special hardware such as a directional antenna, sonar, or GPS.

1.5 Outline of Research

The outline of this thesis is also included with this chapter and the following chapters:

Chapter 2: Contains background and literature reviews of WSN security and describes network layer attacks such as (Wormhole attacks and Replay attacks).

Chapter 3: Proposes a Detect and Compare Packet Nonce (DCPN) algorithm is used to detect wormhole, Packet Count Detection (PCD) algorithm is used to detect replay attacks.

Chapter 4: Demonstrates the simulation and the results, accompanied with figures, in order to identify network layer attacks in WSNs and to provide a solution for the issue of sensor nodes' energy consumption.

Chapter 5: Presents the conclusions and future work about this thesis.

CHAPTER TWO: BACKGROUND and LITERATURE REVIEWS

2.1 Introduction

The integration of 5G networks and WSNs is crucial for the new area of the IoT, for a wide range of applications. The WSN is one of the IoT's most important components, and it's in charge of gathering and distributing physical phenomena and data from a variety of heterogeneous and resource-constrained sensors (Agiwal et al., 2016). Due to the general characteristics of WSNs, which include low costs, low power consumption, open media, and multifunctional nodes that communicate at short distances through wireless links and so on. WSNs have become an integral part of our everyday lives and have drawn the attention of a significant number of people who are working in this field. A typical WSN is shown in Fig. 2-1.

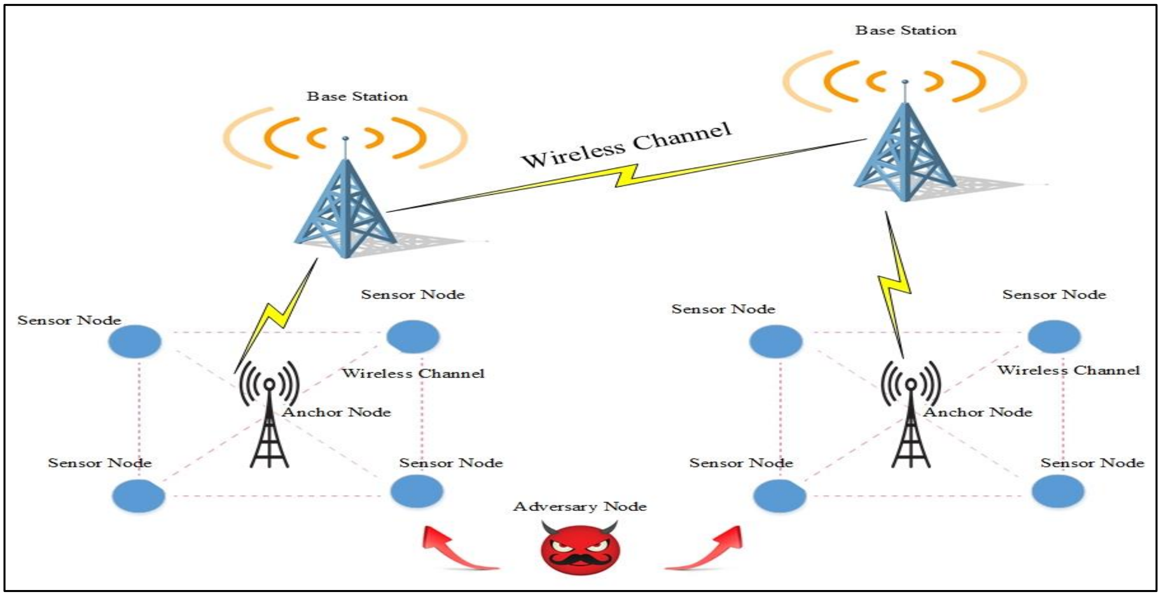


Fig. 2-1 Wireless Sensor Network

Security procedures are needed for all sorts of sensor networks in order to ensure the operation of a WSN, particularly in malevolent situations (BenSaleh et al., 2020). However, the security of a WSN is made considerably more difficult by resource constraints in the sensor nodes and multi-hop communications over an open wireless channel. More sensors and smart gadgets will surround us as a result of WSNs and 5G-integrated IoT, thus reaching much deeper into our private lives. This improves connection and gives us better convenient services, but it also increases the number of surface attacks. The nodes established in a network are relatively easy to compromise, which means that the nodes are not under the control of the system and an adversary may quickly get completely accessed to those nodes. Hence, in the targeted nodes, all the data may be altered and restored. Thus, developing some new security mechanisms is necessary for sake of the nodes since the traditional security mechanisms are no longer effective and an adversary can easily lunch attacks with a legitimate status of the network (Karakaya and Akleylek, 2018). When an attacker gains control of a node and pretends to be a valid node after a network deployment, it is referred to as a compromised node.

Although, the issue of general stability is very important to consider in any WSN. In order to work on the internal security, we need to realize its features and the different types of attacks. One of the focuses of this chapter is to give an overview about different network layer attacks on a WSN.

2.2 Fifth Generation 5G Technology

The world is rapidly changing, and the rate of technological innovation and implementation of new technologies is accelerating exponentially. Although the 4G system was deployed in 2011 and provided faster mobile broadband services than its predecessor 3G, the race to obtain more advanced mobile traffic is still growing rapidly. However, the need for more advanced broadband networks will force the existing system's standards beyond their limit in order to provide better communication speeds. Nowadays, the development of 5G technology, which is extensively deployed at the beginning of the 2020s, provides devices with much more reliability and connection speed. (Li et al., 2021). The 5G technology will facilitate an internet connection with a speed of multi Gigabit per second, which will bring a significant rise in the IoT technology as it is illustrated in Fig. 2-2.

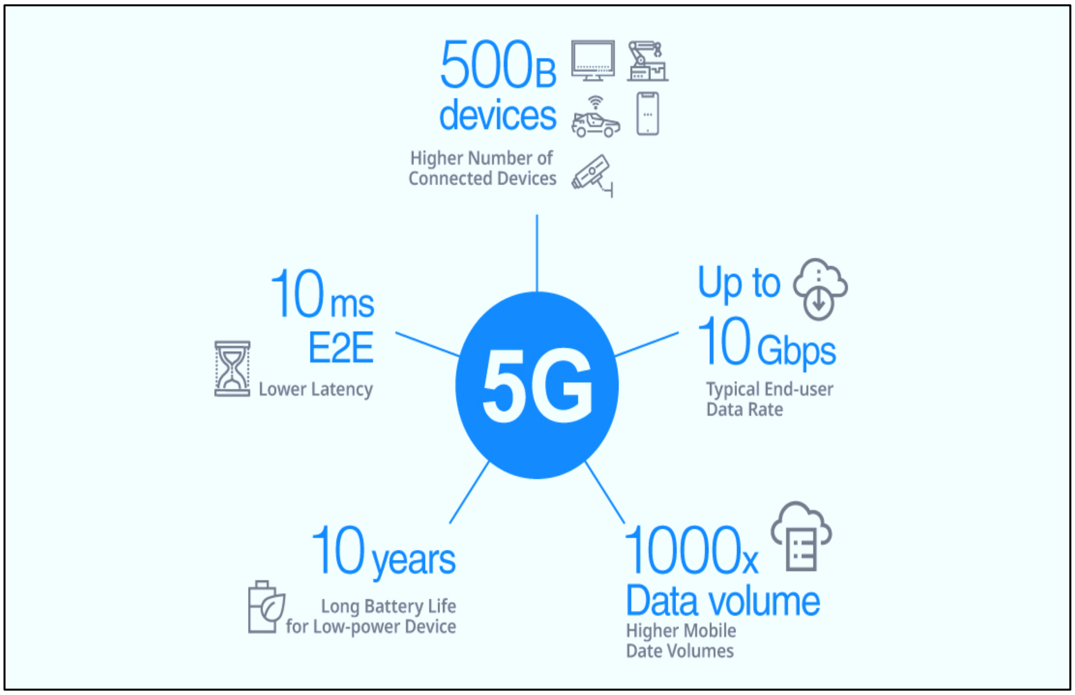

500B devices
Higher Number of Connected Devices
10ms E2E
Lower Latency
5G
Up to 10Gbps
Typical End-user Data Rate
10years
Long Battery Life for Low-power Device
1000x Data volume
Higher Mobile Date Volumes

Fig. 2-2 Fifth Generation

According to Cisco's 2019 report on corporate social responsibility, the expansion of 5G technology will increase the connectivity from approximately 29 billion in 2022 to 300 billion by 2030. Also, more than 3.5 billion individuals will use the internet for the first time in their lives. This remarkable progress gives a huge chance to address and solve fundamental global issues such as improving health, decreasing pollution, and creating smart cities (Kaur et al., 2020). 5G technology would be a huge convergent platform which facilitates a vast variety of uses.

Moreover, it will help the smart grid technology, which allows the power system to function more effectively and reliably.

2.3 Internet of Things

IoT is one of the most recent technologies in our time, paving the way for a variety of services and technological advancements. For instance, identification, sensing, communication, processing, services, and semantics are all integrated into the system (Burhan et al., 2018). There are many IoT applications that may be classified into categories such as healthcare, Smart Cities, Agriculture, smart meters, and so on. This enables smart items to be dispersed via a distributed infrastructure with wireless communication. Due to the rapid increase in the number of people moving to cities for work, there has been a drastic increase in the use of smart devices such as sensors, smartphones, and smart appliances, all of which contribute to the IoT goal which is connecting everyone and allowing them to exchange data via the internet (Gopika and Panjanathan, 2020). The perception layer, which comprises devices such as sensors, actuators, and smartphones, is part of the IoT architecture. An IoT system's endpoint is represented by these linked devices. The Network layer, also known as the connectivity or edge computing layer, allows devices to communicate with one another. Additionally, the acquired data is sent to a cloud platform for data processing, which includes mining, machine learning, and data reporting. Finally, the application layer interprets the data and displays it to end users in a graphical format, which benefits in business, decision-making, and cooperation by using data collected via IoT computing, there are several IoT applications that use WSN as their underlying architecture.

The amount of energy stored in each node is directly proportional to the amount of time the network is active. The primary purpose of the nodes is to gather information about a physical occurrence and transform that data into signals that can then be subjected to further processing and examination. There are many different tasks, such as communicating, sleeping, idle listening, controlling the overhead, and collision, that use a significant quantity of energy. The transmission and receiving of information data are the very same operations that utilize the greatest amount of available energy. The applications for the IoT which are built on WSN are many and varied, so they makes people's lives much simpler overall (Porkodi and Bhuvaneswari, 2014).

2.4 Wireless Sensor Network

WSN is composed of a central base station and a large number of sensor nodes that have been placed across the network. WSNs can be defined as a self-configured and infrastructure-less wireless network to observe physical or environmental conditions, like temperature, pressure, motion, sound, vibration, or pollutants, and to directly pass their data or information through the network to a base station which is also called the main location where the information is often observed and analyzed. The sensor nodes are some small devices that have a limited memory, processing capabilities. They also use a low amount of energy and have a low price tag. The sensory nodes can communicate with each other by using radio signals. The wireless sensor nodes are equipped with sensing and radio transceivers, computing devices, and power components. Also, the base station serves as a gateway between the sensor networks and the outside environment. Base stations not only provide a significant amount of data processing ability, but they also have a very large storage capacity which is quite helpful for the network as a whole (Sharma et al., 2016). The primary responsibility of the base station is to be responsible for the distribution of the significant amount of data that has been obtained from the sensor nodes. The batteries of the sensor nodes that power them are similarly small. As a result, the sensor's batteries do not degrade quickly and cannot be readily refilled since they are dispersed in broad regions. As a result, the network's lifetime decreases, which is a major concern.

Lifetime of wireless sensor node is correlated with the battery current usage profile. By being able to estimate the energy consumption of the sensor nodes, applications and routing protocols are able to make informed decisions that increase the lifetime of the sensor network. However, it is in general not possible to measure the energy consumption on sensor node platforms. Minimizing energy consumption and size are important in order to make WSN deployable. As most WSN nodes are battery powered, their lifetime is highly dependent on their energy consumption. Due to the low cost of an individual node, it is more cost effective to replace the entire node than to locate the node and replace or recharge its battery supply. Hardware components are characterized at a very detailed level to simulate power consumption of a node as close as possible. (Fu et al., 2018).

2.5 Applications of WSN

Generally, WSN could be defined as a small system of nodes which accommodatingly sense, monitor, capture, process and control situations such as data/signals around an application, supporting dealings between peoples/computer systems and the immediate surrounding. WSN may use sensors with low sampling frequencies for magnetic, seismic, optical, infrared, thermal, radar, and acoustic data. WSNs are mostly used for military, health, residential, environmental, and some other commercial purposes (Vladimirov et al., 2018), as shown in Fig. 2-3.

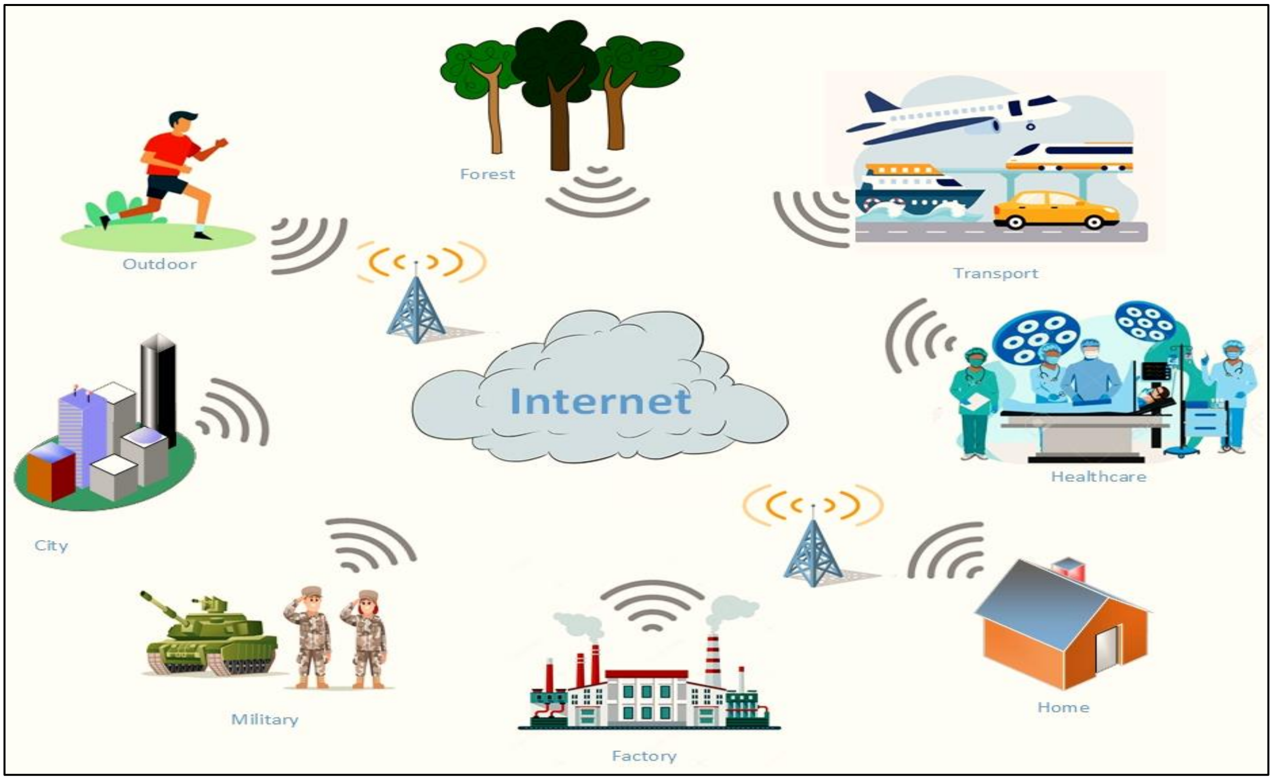


Fig. 2-3 Applications of WSN

2.5.1 Monitoring

Monitoring applications include indoor and outdoor real-time environmental monitoring for uncontrollable animals and farms, health, power, safety monitoring, inventory position monitoring, structural, geological, manufacturing unit monitoring, and automation process for monitoring. The popularity of environmental monitoring usage as a tool for management and security has increased in recent years. This has resulted in the creation of real-time systems that are both low-cost and energy-efficient. In addition to that, customers may use it to keep tabs on things like woods, interior living spaces, green homes, and climate change.

2.5.2 Tracking

Target tracking is one of the most intriguing advancements in WSNs since it involves detecting and tracking distant targets. This makes it one of the most exciting applications of WSNs. The location of moving targets may quickly get conveyed to the user of the application by sensor nodes once they have detected and communicated their position (Parvin and Vasanthanayaki, 2019). Target tracking has a broad variety of uses in the real world, some of which include identifying illegal border crossings, monitoring animals, monitoring battlefields, identifying how fires progress, monitoring gas leaks, and monitoring fire spread. Monitoring a target may be done by a single node or by several sensors working in conjunction with one another.

2.5.3 Military

Utilizing sensor networks to monitor and gather information on enemy activities, detonations, frontline monitoring, detection of biological, nuclear, and chemical danger, and inquiry is recommended. The sensor can distinguish, discriminate, and identify threads based on their amount, number, and category, whether they are armored vehicles or soldiers on foot, their kind, and quantity of weapons they carry, among other factors. Additionally, the technology facilitates army preparation and reduces response time. (Prabhu et al., 2017).

2.5.4 Environmental Applications

The quality of the air, traffic movements, and weather conditions are just some of the things that a WSN device can monitor and regulate. These devices can also gather and analysis an enormous amount of information. WSN has been used to aid people with their jobs, monitoring animals’ movements, identifying environmental conditions that impacts crops and livestock, and tracking animal migrations. The usage of WSN also include chemical and biological identification, precision agriculture, biological monitoring, tracking of forest fires and volcanoes, detection of floods and pollutants, meteorological or geophysical observation, and analysis.

2.5.5 Healthcare Applications

The physiological data of patients might be monitored via body sensor networks. It can recognize and monitor the behaviors of elderly individuals, such as when a patient has fallen, it allows patients to have more freedom of movement and support clinicians in detecting symptoms early. The small sensor can also identify and track hospital patients and physicians.

2.5.6 Home Applications

The extensive variety of WSN applications make life simpler and more cost-effective. With technological advancements, sensors are now possible to be integrated into appliances such as microwave ovens, vacuum cleaners, and refrigerators. They will connect via each other, the room server, and investigate the available resources such as copying, faxing, and scanning (Belghith and Obaidat, 2016). These sensor nodes and room servers, when paired with existing fixed equipment, may be used to construct self-regulating, adaptive networks that are also capable of self-organization, thus creating a dynamic ecosystem.

2.5.7 Traffic Control

WSN is capable of monitoring and controlling traffic conditions efficiently. It is possible to keep tabs on transient occurrences like road construction and accidents. It does this by collecting data on traffic and then using that information to manage the flow of traffic. The majority of traffic light installations use timer systems that has a predetermined length of cycle time and switches the lights on and off at certain intervals. Drivers would not waste time waiting for traffic signals to change, which may lead to collisions and traffic infractions in case drivers lost their patience. The whole principle behind intelligent traffic system is so that drivers would not waste time waiting for traffic signals to change (Al-Nasser and Mahmoud, 2012).

2.6 Challenges in WSN

During the implementation of WSNs, a number of technological challenges must be resolved. A number of these concerns are detailed below:

- Ad hoc deployment: A huge number of sensor nodes were placed in a variety of places lacking in infrastructure. The sensor nodes were dispersed around the areas using a variety of approaches. Due to the fact that these nodes configure their own connection and distribution, they are what to be known as self-configuring nodes (Gouvy et al., 2013).
- Unattended operation: After the nodes have been installed in the WSN, there is no need for any sort of human contact to take place anywhere inside the WSN. The nature of nodes is set in such way that they may self-configure, and they are also capable of adapting to whatever changes that may take place inside these networks (Kaur and Kumari, 2014).
- Untethered: In these networks, there is no link between the sensor nodes and any external energy source. There is just a limited energy available inside the sensor node, which is used during processing and communication between sensor nodes. The processing is entirely dominated by communication with the energy use. Efforts should be made to minimize energy usage to the greatest extent feasible in order to make optimal use of the network's energy capacity.
- Fault tolerance: Fault tolerance refers to the process of maintaining a network in such a way that the failure of a single node does not influence the performance of the whole network. Many different adaptive protocols have been used in these networks in order to guarantee this outcome.
- Security issues: Threats and attacks against WSNs are on the rise in an attempt to compromise WSN’s security. Furthermore, attacks may be

possible due to the wireless communication. Wireless networks, in comparison to other networks, are extremely vulnerable to many forms of security attacks due to the presence of an unguided transmission medium that is very sensitive to security attacks. Due to the broadcasting nature of the wireless communications that occurred here, the direct candidate may be exploited to eavesdrop. Most of security vulnerabilities and dangers have been found in wireless ad hoc networks, which will be addressed in several ways. (Wang and Guo, 2013).

- Synchronization and Localization: The data collected from each node may be used by various applications. Therefore, the synchronization of these nodes is crucial. Within the WSNs, synchronization of the clock is a crucial component. In the networks, nodes are more like clocks that allow for synchronization of time. With the guidance of a global clock built into the sensor architecture, the data is immediately organized and categorized. This facilitates the prediction of the future framework requirements of these networks. In addition to the transmission delays, the network has several additional difficulties. Due to the lack of a broadcasting clock inside the network, it is also impossible to synchronize nodes. Localization of sensor nodes using the relative locations of the sensors is a crucial test inside sensor networks. Consequently, several techniques have been suggested to solve all these problems. Within these networks, distributed algorithms play a crucial role in enhancing the accuracy of the networks.
- Short Range Transmission: Within WSNs, a node's limited broadcast range must be taken into account in order to reduce the likelihood of eavesdropping. This helps to reduce the likelihood of eavesdropping. Long-distance transmissions need a larger transmission power in order to allow point-to-point transmission between nodes. This is the main reason why there is an

increase likelihood of a network packet to be intercepted (Neamatollahi et al., 2011).

- Energy consumption: Within the WSNs, the use of energy is a serious problem that has to be addressed. Because of their tiny size, the sensor nodes contain only a restricted amount of energy. The network itself contains the batteries, which are rather small and difficult to replace relative to their location. As a result of that, multiple scholars have presented a variety of protocols and algorithms connected to power in an effort to find a solution for this problem.

2.7 Characteristics of WSN

Mobility, switching behavior, and battery life are a few of the factors that restrict the capacity of WSNs. Compared to the wireless networks, WSN offers a number of distinct properties. The followings are some of attributes of a WSN (Yong-Min et al., 2009):

- Computing capabilities: The program and memory capacity of the sensor is significantly constrained due to cost, size, and battery power consumption limits.
- Battery’s energy: As energy is expended, sensor nodes are often disregarded and rendered ineffective. Therefore, protocols and algorithms for battery energy saving should be regarded as trimming. Additionally, the energy spent by nodes that transmit data is larger than the energy consumed by nodes that do computation.
- Cost: The cost of the sensor network may be kept to minimum by lowering the cost of sensor networks as much as it is humanly feasible.
- Communication capabilities: The senor network's communication capacity is restricted and inconsistent, and the communications range is just a few tens to

several hundred meters. Since the natural environment, consisting of things like hills, homes, and winds, as well as precipitation and lighting, obstacles presented by the terrain, and weather, would have a significant impact on the senor: Both the hardware and the software of a WSN need to be dependable and tolerant of errors.

- Dynamic: Due to the needs of the activities, extra sensor nodes may be relocated or added to the network. Due to these advancements in network structure, the WSN topology must be capable of reconfiguration, dynamic adaptation, and self-adjustment. The sensor nodes are either randomly or evenly distributed.
- No Centre, self-organization: Before deploying wireless networks, it is not necessary to install any network infrastructure. After the nodes are activated, the sensor node will establish an autonomous network simply and effectively by cooperatively adjusting its output and distribution algorithm. The WSN is a peer-to-peer network.
- Application relevance: WSNs differ from traditional networks since they rely heavily on applications; their primary function is to collect environmental data. Due to the fact that diverse sensor network applications handle distinct physical signals, sensor network routing protocols cannot be efficiently extended to all of them. The focus of WSNs is on applications.

2.8 Security Requirements in WSN

The WSNs consist of hundreds or thousands of nodes spread over a geographic region. These nodes are easily capable of self-organization to conduct any data collecting tasks (Bhasin et al., 2020). This self-organization of nodes results in a dynamic network in which nodes relay for their neighbors. As a result of the network's dynamic and the inherent constraints of each node, the network is vulnerable to attacks. The ability of sensor nodes to defend themselves against external threats is a serious security problem. This vulnerability to attacks is even further increased by the broadcast nature of the communication medium. Additionally, these nodes are often placed in hostile or dangerous areas, and they are not tamper-resistant. The security protocols' designers find it rather challenging to strike a compromise between minimizing resource consumption and enhancing security. Meaning, large-scale scaling of security mechanisms is somehow challenging (Ramesh et al., 2012). The purpose of the security services included in a sensor network is to protect the aggregated data against intrusion and other forms of malicious activities. The following set of acceptable metrics for data integrity, self-organization, and temporal synchronization, protected localization, cost efficiency, and self-healing should be included in security protocols:

2.8.1 Availability

The data gathered by the sensor network must be fully accessible even in the event of attacks; a network-blocking attack. Attackers are undertaken to render an inaccessible portion of the network (Cayirci and Rong, 2008). While considering these assaults, it is essential for the accessibility of the network to be ensured. The inclusion of redundant nodes is one way to guarantee that a node and the information it contains will always be accessible. However, the very redundant nodes in a network results in the same sort of data being produced, which increases the amount of network traffic. The aggregation of data collected at different sensor nodes is one method that may be used in order to overcome this problem.

2.8.2 Authorization

A sensor node should be authorized for transmitting and receiving data in order to participate in data transmission over the network, which means that it should be possible for legitimate sensors to take part in the process. Authentication is necessary in order to have a secure communication inside the network, an attacker or a malicious node shouldn't be able to pose as a genuine node and pass themselves off as such. Since the masquerader is able to send huge numbers of unwanted messages into the network, this might shorten the node's battery lifetime and ultimately cause it to fail. As a result, the authentication of nodes is an essential component.

2.8.3 Confidentiality

It is important for the neighbors to maintain confidentiality while they are talking to one another. For example, when node A is transmitting information to node B, another node C should not overhear this communication, even if it is in a proximate place to both of them. When the communication channel is wireless, this takes on a much greater level of significance. Encryption of data gives a measure of privacy for the data.

2.8.4 Integrity

When a message is transferred from one node to another, this helps to guarantee that the message will not be corrupted by malicious nodes that are in between the two nodes. Also, in the event that the messages are changed while they are being sent, the receiver is responsible for ensuring that the altered messages are not acknowledged. Authentication and data integrity have a strong relationship with one another due to the fact that message authentication code is utilized to offer both of these qualities.

2.8.5 Support Various Communication Patterns

The security protocol must be compatible with the network's current communication patterns, such as connectionless (sending a message to a single node), local broadcast (sending a packet to all the nodes in the neighborhood), and global broadcast (communicating messages to all the nodes in the network) (Bhasin et al., 2020).

2.8.6 Energy Efficiency

Network’s energy efficiency is what determines if a sensor network will survive and functioning or not. The restricted battery power of a sensor node necessitates the minimization of costly cryptographic calculations and message transfers. Additionally, so security solutions must be scalable.

2.9 Natures and Types of Attacks

Due to the nature of the network's transmission channel, which is broadcast, wireless networks are more vulnerable to security breaches than conventional wired networks. Since nodes in WSN can be installed randomly in dangerous environments, an adversary has a greater opportunity to launch an attack on the WSN that is being targeted. Regarding the safety of a WSN, it is possible to investigate it from a range of perspectives. For example, WSN attacks can be divided into two main categories: passive and active attacks, or in other words they can be recognized as external or internal attacks based on the domain of attacks. Additionally, WSN attacks can be investigated from a variety of angles (Lupu et al., 2009). The following definitions are provided to explain all of the previously discussed terminologies:

A. Passive attack: Is an attack that is taking place outside of the network, it will not have any direct impact on the network. Eavesdropping or detecting the packets that are being sent and received inside a WSN is a kind of attack known as a passive attack.

B. Active Attacks: Is an attack in which the attacker sends data to either one of the nodes or both of them, or possibly send chunks of the data stream in either one or both ways over the communication channel. Active attackers have the potential to interrupt the regular operation of the whole network, which might result in the alteration of the information, the modification of the original data, or the collection of false data. It acts just as a valid node in the network would in terms of behavior.

A taxonomy of the numerous attacks that may be launched against wireless networks is shown in Fig. 2-4, which can be seen below.

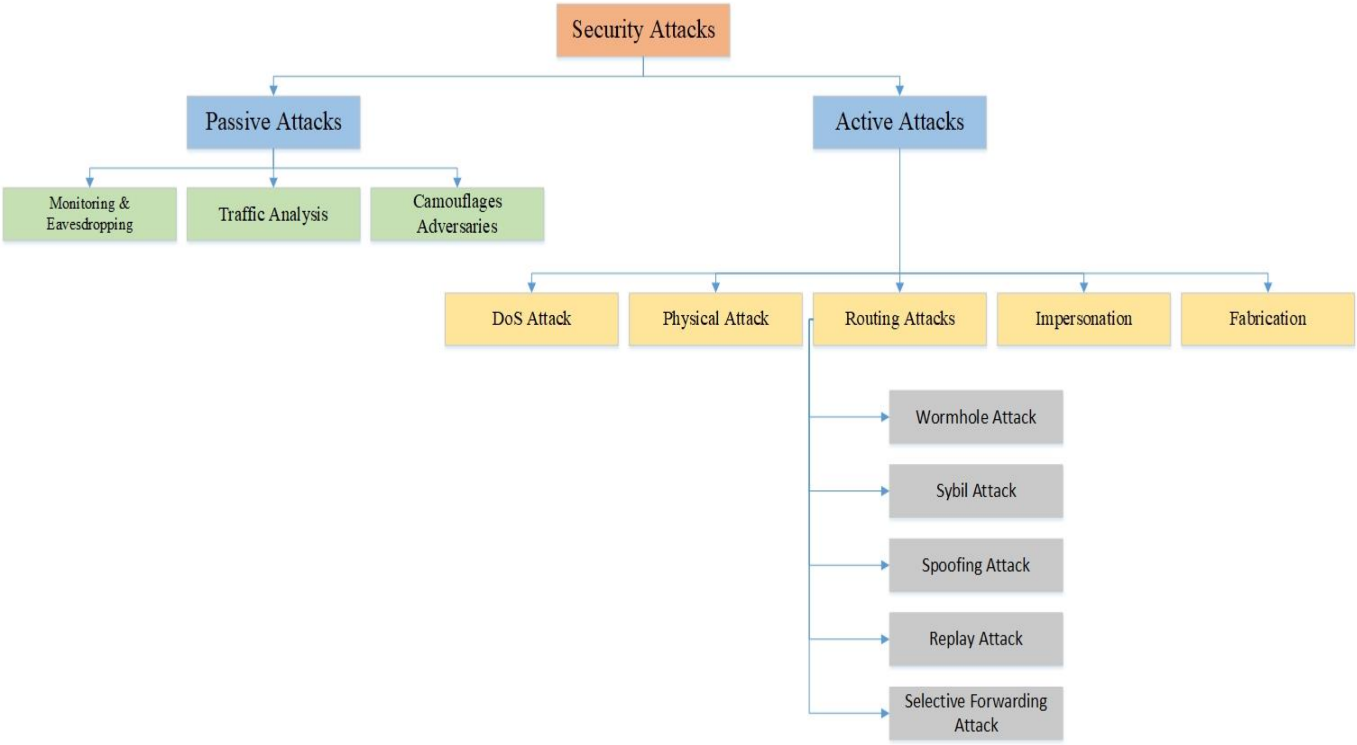


Fig. 2-4 Security attacks

The compromised node has the following characteristics (Hsieh and Huang, 2017):

➢ Typically, it will execute some malicious code that is distinct from the code that is running on a valid node and it will attempt to either obtain data from the sensor network or disrupt its regular operation.

- A node is able to interact with the other standard sensor nodes since it operates on the same radio frequency as those other nodes.
- The node has been verified as legitimate and now is a member of the sensor network. Because cryptographic keys are used to encrypt and authenticate secure communication in sensor networks, the compromised nodes that get the secret keys of a valid node are able to take part in the networks secret and verify communication.

It is evident that compromised nodes are more risky than uncompromised nodes because an adversary may quickly get accessed to information from the compromised nodes and then use that knowledge to launch further attacks using the confidence of other sensors. It is not easy to defend against or prevent this sort of attack. Because of this, protecting WSN against coming attacks from inside the network itself has become a difficult challenge. In a wide variety of applications, it is essential for the intelligence gathered from the sensing nodes to be both legitimate and retained in confidentially. In security issues, every node in the network, whether it is false or malicious, has the potential to intercept private information or broadcast false signals to other nodes in the network. Wormhole attacks, Sybil attacks, Spoofed attacks, Blackhole attacks and Replayed routing information attacks are the most significant types of cyberattacks. Based on the Opens System Interconnect (OSI) model the attack can be tabulated in table 2-1:

Table 2-1 Layer based security attacks

Layer	**Attacks**
Physical layer	Jamming, Tampering, Sybil Attack

Data Link Layer	Collision, Sybil Attack, Spoofing and Altering Routing Attack, Replay Attack
Network Layer	Sybil Attack, Blackhole Attack, Spoofing and Altering Routing Attack, Wormhole Attack, Selective Forwarding Attack, Hello Flood Attack.
Transport Layer	Flooding Attack, Desynchronization
Application	Spoofing and Altering Routing Attack, False Data Injection,

Network attacks are typically carried out by malicious nodes with the intention of modifying, destroying, or stealing sensitive data. Attackers on a network will usually try to get into the network's internal systems by getting past the network's perimeter. Wormhole attacks and replay attacks are two types of network layer attacks on WSN that are the primary focus of this study.

2.10 Wormhole Attack

An attacker carries out a Wormhole attack by first receiving packets at one point in the network, then "tunneling" those packets to another point in the network, and then re-entering those packets into the network from that point, as shown in Fig. 2-5. An attacker breaks into communications that were initiated by the sender, copies either a portion or the entire packet, and then speeds up the sending of the copied packet through a particular Wormhole tunnel in such a way that the copied packet arrives at the destination before the original packet, which travels through the conventional routes. Sending the copied packet through a wired network and then transmitting it over a wireless channel at the end of the tunnel is one way to create such tunnel. Other ways to do so include making use of a boosting long-distance antenna, sending the data through a route with a low latency, or utilizing any channel that is outside of the normal range of transmission. The Wormhole attack poses several dangers, particularly to routing protocols and other protocols that depend largely on geographic location and proximity. Also, many following attacks may be launched too once the Wormhole route has attracted a significant number of packets crossing it (Xie et al., 2018). If used combined with a Sybil attack, it is difficult to identify the attack.

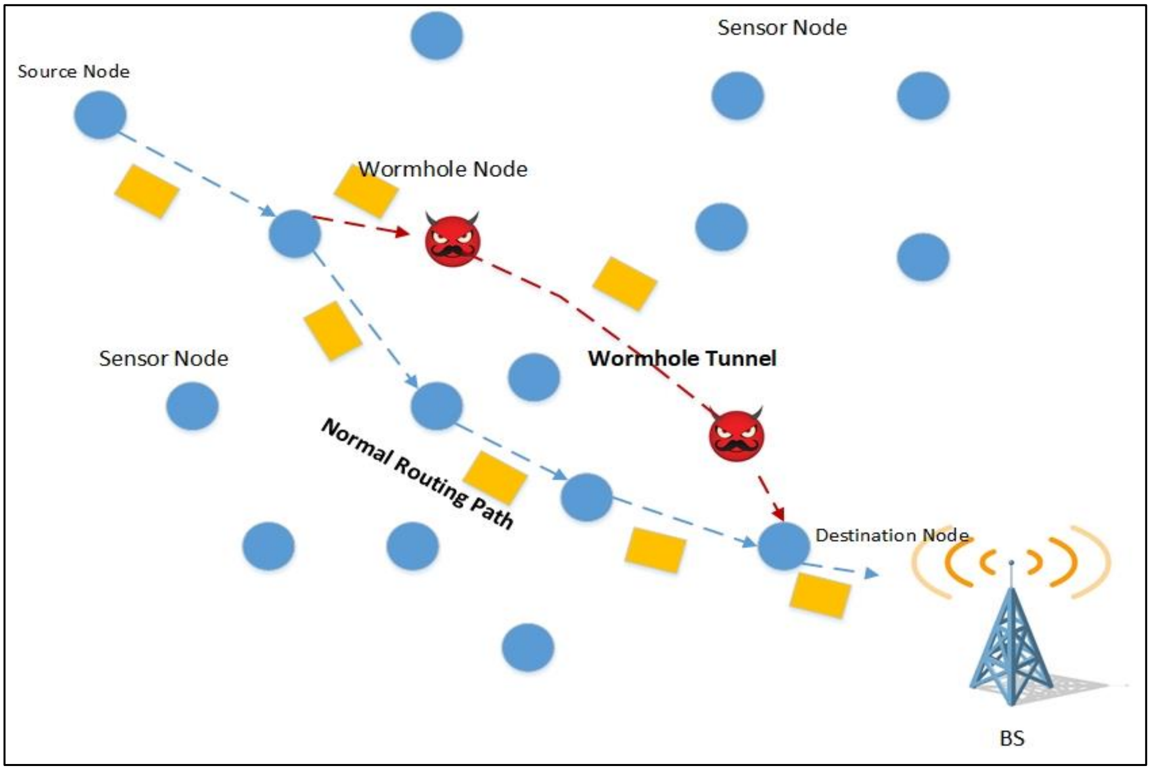


Fig. 2-5 Wormhole attack

2.10.1 Wormhole Attack Can be Classified under Three Main Categories

1. Open Wormhole: In this kind of scenario, the packets of data are first sent from the source to a Wormhole, which then tunnels them to another Wormhole which sends them to the destination. However, the other network nodes are rejected and not utilized for data transportation (Pruthi et al., 2019).
2. Half-open Wormhole: In this scenario, the data packets are transported from the source to a Wormhole, which then sends them on to the destination in an uninterruptible manner.
3. Closed Wormhole: In this scenario, the data packets are transported straight from the source to the destination in a single hop, making the source and the destination appear as fake neighbors.

2.10.2 Some Countermeasures against Wormhole Attacks

- **Watchdog Model**: According to the Watchdog model, if some information is transmitted from one node to another through a middle node, then the sender node will keep a check on the middle node. This ensures that the information is transmitted correctly. If the data packet is not sent within the given amount of time by the middle node, then it will be considered forgotten, and a new route will be devised to get to the destination node instead (Cho et al., 2012). Although this watchdog approach cannot always accurately identify Wormholes and may possibly get tricked by an attacker if a Wormhole attack is paired with a selective forwarding attack, still this approach is a viable solution. The likelihood of obtaining false positive results is likewise rather significant in this scenario.
- **Discovering Separate route Algorithm**: In this, an algorithm is discovered that can detect a Wormhole attack based on the various pathways that may be taken between two nodes. This method discovers all of the single hop and

double hop neighbors, as well as the majority of the routes that connect the nodes. Therefore, it is simple for it to determine whether or not the claim that a node makes about being on the route that is the shortest distance to the destination is accurate.

- **Packet Leashes**: Is proposed as a preventive method against Wormhole attacks. These leashes impede the transfer of packets over long distances. These packet lashes are also classified as:
    1. Geographical Leash: Ensures that data cannot be transported more than a specified distance in a single hop.
    2. Temporal Leash: Specifies the maximum distance a data packet can travel despite several hops.
- **Multi-Dimension Scaling-Visualization of Wormhole method**: In this technique, the base station determines the network's physical structure based on the strength and distance of the signal between nodes. The topology of WSNs under Wormhole attack differs from that of networks with typical nodes. If a node incorrectly claims to be a single-hop route, it will be shown on the layout.

2.11 Replay Attack

This is a type of network layer attack in which an attacker illegally delays or repeats data transportation after detecting it. The data transferred is delayed or repeated by the sender or the malicious party, which in turn intercepts the data and retransmits it. (Dhunna and Al-Anbagi, 2019). In a WSN, a malicious node will intercept packets that have been delivered, and then it will replay those packets again to a valid node in order to destroy that node's limited energy supply and take control of the communication channels as it is shown in Fig. 2-7.

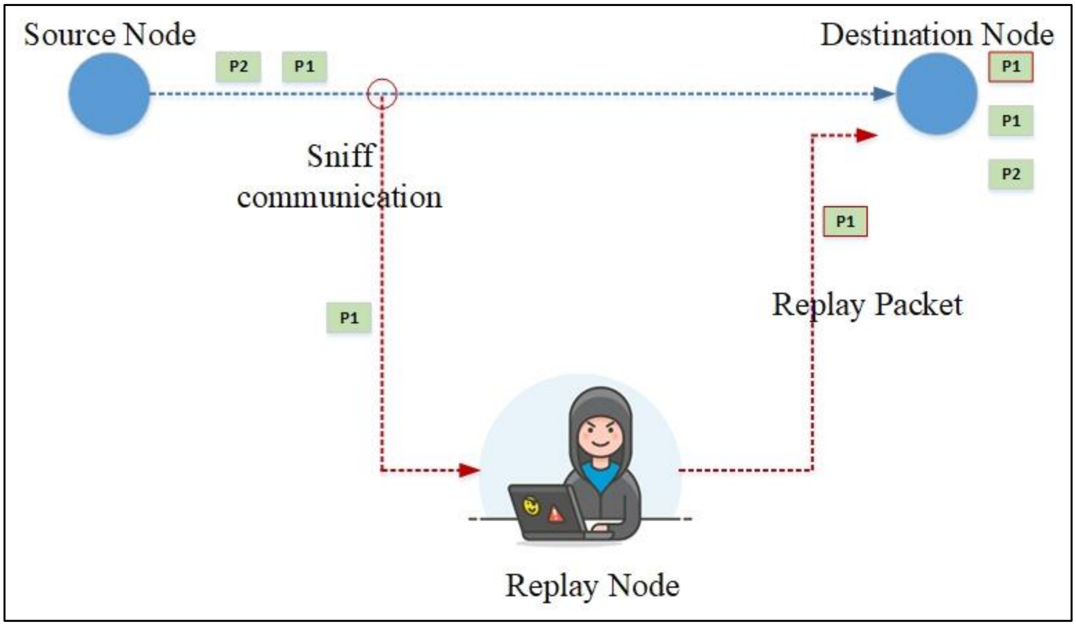


Fig. 2-6 Replay attack

Attackers typically complete and duplicate transaction, get access to a network, or obtain information that they otherwise would not have had easy access to with the use of Replay attacks.

2.11.1 Some Mitigation Techniques of Replay attack

The following strategies mentioned below are some of the ways used in order to identify and protect against Replay attacks:

- **Timestamps**: It is a process to ensure that the message will always be up to date. This is a very traditional way for determining whether or not the message received was original or a replay. A timestamp is attached to each and every message that is sent using this method (Gelenbe and Kadioglu, 2018). After receiving the message, the receiver will first determine whether or not the timestamp falls within the permissible range. If it does, the message will be accepted; otherwise, it will be ignored. By using Network Time Protocol, each and every machine will be able to accurately keep the time. The clocks of the two entities must be synchronized in order for this technique to be implemented correctly. The accuracy and precision of the timestamp can only be preserved via the process of synchronization, which is rather necessary. In this case, it will need to compile a list of historic timestamps, which will take up a lot of storage space, and the verification cost will be significant.

- **Sequence number**: Each transmitted message is allocated a sequence number that increases or decreases monotonically. If a message is replayed, the sequence number will be extremely little or very old, and it may be disregarded.
- **Receiver Authentication Protocol**: RAP could be used for both detection and prevention. The purpose of the detection strategy is to identify an attacker that is replaying signals without attempting to stop it from doing so. As for the prevention mode, the message exchanged consisting of a challenge and a response is carried out prior to the data transformation. Once the receiver has been shown to be legitimate, only then the sender is allowed to pass across the data. Energy efficiency is a primary necessity, thus under normal conditions, detection is carried out, and the system only shifts into the more costly prevention mode when it is absolutely necessary to do so.

2.12 Literature Reviews

With the increased availability of WSNs, it is crucial to use the specific methods for establishing a secure communication in these systems. The following subsections provide solutions (strategies and techniques) to defend (detect, prevent or mitigate) against wormhole and replay attacks towards the WSNs.

2.12.1 Wormhole Attack Reviews

(Singh et al., 2016) have presented a Wormhole Resistant Hybrid Technique (WRHT). WRHT is based on the watchdog and Delphi systems and guarantees that the Wormholes in the sensor network does not remain unchecked. In order to calculate the value the probability of Wormhole presence, WRHT uses a dual Wormhole detection technique that calculates the factor time delay probability and packet loss probability of the established link. The most unique feature of WRHT is its ability to fight against practically all types of Wormhole attacks without requiring any extra hardware, such as a global positioning system, timing information, or synchronized clocks, or typical cryptographic systems that need a lot of work. The findings have clearly shown that the suggested approach outperforms the existing strategies. The authors (Aliady and Al-Ahmadi, 2019) presented a network connectivity-based energy-saving security measure with the goal of detecting wormhole attacks. This measure is based on the connectedness of the network. The experiment is evaluated using Network Simulator 3, after which the suggested measure is implemented into the Ad-hoc On-Demand Distance Vector (AODV) routing protocol. According to the findings, the detection performance is 100% percent whenever the length of the wormhole tunnel is at least four hops long. In addition, the method is inexpensive because it is not dependent on any plugged hardware, such as synchronized clocks or a geographic positioning system. Also, (Aneja et al., 2019) identify and defend WSN from wormhole attacks, they suggested a cluster-based method. At some point, the entire network is partitioned into clusters, and each cluster is led by a Cluster Head (CH). The security of the network has been improved, and the wormhole attack within the network has been rendered useless due to Round Trip Time (RTT) and hop count. It has been found that the proposed strategy results in a significant improvement in both throughput and latency. (Tamilarasi and Santhi, 2020) proposed a technique for detecting wormhole attacks as well as an optimum or secure route selection. The Ad-hoc On-Demand Multipath Distance Vector (AOMDV) routing protocol generates many pathways between the source and destination. The source node then determines the attacked wormhole route by confirming the destination's Detection Packet (DP) and Feedback Packet (FP). The source node uses the Particle Swarm Optimization (PSO) method to choose the best route among the attacker free pathways after recognizing the attacked wormhole pathways. Based on the performance of the suggested approach, the results revealed the noticeable increase in both energy efficiency and network's lifetime. Also, (Ahutu and El-Ocla, 2020) For 802.15.4 WSN, the MAC Centralized Routing System (MCRP) was suggested as a centralized-based routing protocol. To compute and distribute routing pathways, manage the network topology, and execute other energy-intensive functions, MCRP employs a high-energy BS. Because WSN nodes are often powered by batteries, so they have limited processing capabilities since they are restricted in terms of resources and energy. Because of the less secure environment in WSN, malicious nodes may easily tunnel packets to another place at any given time, thus causing a network damage in terms of monitoring and packet loss. In comparison to its competitors, MCRP enhances network scalability in terms of energy consumption, end-to-end latency, throughput, and frame delivery ratio. Furthermore, (Bhawsar et al., 2020) mentioned the AODV protocol, which is based on trusted calculation, was developed as a technique to identify and avoid Wormhole attacks. The multiple route selection approach is utilized in this method to discover the optimum routing path. The route is checked for Wormhole attacks, and when a node is discovered, a data packet transmitted between the source and destination chooses the best path from the several options available, thus improving packet delivery overall. The suggested mechanism's Packet Delivery Ratio (PDR) is computed, and the results show that the PDR has improved, throughput has increased, and latency has reduced. (Farjamnia et al., 2020) enhanced the Distance Vector-Hop (DV-Hop) algorithm and increased the efficiency of wormhole attack detection in WSNs based on the localization approach. In order to reduce the amount of mistake that is produced by DV-Hop, a new duration that is formulated on the correction of Hop-size and gap measurement has been suggested. According to the findings of the simulation and evaluation, the suggested model performs much better than DV-Hop in a variety of topologies. Specifically, the proposed model has significantly higher localization accuracy in these topologies.

2.12.2 Replay Attack Reviews

(Medjadba et al., 2016) have proposed an effective intrusion detection method for preventing data replay attacks in WSN. The planned intrusion detection system is named as DR-IDS (Data Replay Intrusion Detection System). The findings later demonstrated that the suggested solution is adequately resilient. Also, The defense mechanism was devised by (Sharma and Hussain, 2017) to mitigate replay attacks in WSN. Each node in the proposed work maintains an assorted value of a received packet in a table, and the reply attack is detected or mitigated based on the assorted value of the previously received packets in that very node. It was later discovered that the suggested approach decreases the risk of a replay attacks, protects the network, and requires much less processing time. (Marigowda et al., 2018) have proposed Synchronized Incremental Counter (SIC) mechanism which focuses on security in WSN against Jamming and replay attacks. Attacks on the Modified Constrained Function based Authentication (MCFA) technique are mitigated by using an Advanced Encryption Standard (AES) with Open Channel Backbone (OCB) mode, which is symmetric key cryptography. Each one of the suggested collective approaches successfully offer security while not reducing network performance, resulting in reduced packet loss and communication time, thus improving the lifetime of the network much further. Furthermore, (Rath and Pattanayak, 2019) introduced an Intrusion Detection Mechanism Based Framework (IDMBF) for protected routing in a highly specific and complex mobile ad hoc network. Based on the results, the system that was suggested has a lower rate of packet loss and a lower end-to-end latency when sending data. Also, prevents replay attack. (Ye, 2019) suggested to use a trust security technique based on cloud modeling and node behavior analysis. The transmission rate component, the spatial correlation component, and the replay attack component are three types of trust characteristics that are designed and added to the trust security algorithm based on the characteristics of common attacks. According on these three trust characteristics, the cloud model is used to assess the nodes' security level. That the proposed method can successfully find impersonation attacks, identify malicious nodes, and find malicious nodes like replay attacks. (Dhunna and Al-Anbagi, 2019) introduced a low-power cyber-security mechanism that can be utilized in smart grid monitoring applications that are based on WSNs. That mechanism is capable of identifying and isolating a variety of attacks, including the denial of sleep attack, the forge attack, and the replay attack, in an efficient manner. The results of the simulation shown that their method could surpass other techniques in terms of power efficiency while preserving the same levels of latency and dependability. (Chung and Cho, 2020) improved an Energy-efficient Distributed Deterministic Key management (EDDK) based on Message Ahutentication Code (MAC). The sequence number of EDDK is used to prevent replay attacks and improve energy efficiency. it also represents a new attack target for attackers. If an attacker modulates the sequence number, a new type of replay attack is possible. This replay attack consumes energy of sensor nodes by sending the previous message. the proposed scheme performs sequence number verification by selecting an intermediate verification node to increase the energy efficiency. as a result, the proposed scheme detects replay attacks and improves the energy efficiency by about 7%. Also, (Rajaram et al., 2020a) improved method of deep learning for identifying and avoiding the replay attack. In order to demonstrate the effectiveness of the dataset, decision trees with the assistance of Support Vector

Machines (SVM) were applied to the data. The critical function of this attack is to disable the network's ability to function effectively. False packets span the full route from the sensor node to the base station in this attack. As a result, the receiver side generates a false signal intensity and simulated time of transmission based on the assumed distance and irrelevant location. The outcome of authentication combined with deep learning methodology can identify replay attacks.

Table 2-2 Summaries of literature reviews in both wormhole and relay attacks.

Type of attacks	**References**	**Years**	**Algorithms**	**Objectives**	**Results**
Wormhole attack	(Singh et al., 2016)	2016	WRHT	detection of wormhole attacks	greater wormhole detection accuracy than existing strategies
	(Aliady and Al-Ahmadi, 2019)	2019	AODV	Energy-saving security measure with the goal of detecting wormhole attacks	The detection performance is 100% percent whenever the length of the wormhole tunnel is at least four hops long.
	(Aneja et al., 2019)	2019	Cluster-based method	The wormhole attack detection based on Round Trip Time (RTT) and hop count.	A significant improvement in both throughput and latency

	(Tamilarasi and Santhi, 2020)	2020	AD- PSO	Detecting wormhole attacks as well as an optimum or secure route selection.	The results are enhanced in both energy efficiency and the network's lifetime.
	(Ahutu and El-Ocla, 2020)	2020	MCRP	detection of wormhole attacks	Enhanced network scalability in terms of energy consumption, lower latency, throughput, and frame delivery ratio
	(Bhawsar et al., 2020)	2020	AODV With PDR	Identify and avoid wormhole attacks	The results show that the packet delivery ratio has improved, throughput has increased, and latency has reduced.
	(Farjamnia et al., 2020)	2020	DV-Hop	Enhanced DV-Hop algorithm that is used for wormhole attack detection	The detection accuracy is better than DV-Hop. It has significantly higher localization accuracy.

Replay Attacks	(Sharma and Hussain, 2017)	2017	Assorted value of a received packet in a table	Mitigate replay attacks in WSN	The results show that they decrease the risk of replay attacks, protect the network, and require much less processing time.
	(Marigowda et al., 2018)	2018	SIC with MCFA	Focuses on security in WSN against Jamming and replay attacks.	The network's lifetime is extended by reducing packet loss and communication time.
	(Rath and Pattanayak, 2019)	2019	IDMBF	Protecting the routing packet in WSN	The rate of packet loss is reduced, as is the end-to-end latency.
	(Ye, 2019)	2019	Trust security technique	Trust security technique based on cloud modeling and node behavior analysis.	The results can successfully find impersonation attacks and identify malicious nodes.
	(Dhunna and Al-Anbagi, 2019)	2019	low-power cyber-security mechanism	Identifying and isolating a variety of attacks, including the denial of sleep attack, the forge	The Lo-ADI mechanism saves up to 43% more power when the network is under attack.

				attack, and the replay attack	
	(Chung and Cho, 2020)	2020	EDDK-MAC	Replay attack detection and preserve the energy consumption of the sensor nodes.	Replay attacks are detected, and the sensor nodes' energy improves by 7% per hour.
	(Rajaram et al., 2020a)	2020	SVM	Identifying and avoiding the replay attack	Based on the arrival time of the signal and the fake distance, the replay attacks are detected.

2.13 Summary

This chapter highlights the security issue of the WSN. Security is one of the biggest challenges in sensor network. Some applications such as military, healthcare, tracking need a secure communication. In order for secure communication network to happen, it must fulfil some security requirements. Finally, we have discussed various existing techniques and protocols for detection of network layer attacks such as wormhole attack and replay attack to handle them independently and comprehensively.

CHAPTER THREE: THESIS METHODOLOGY

3.1 Introduction

WSNs, which may be used to monitor surroundings, offer a wide variety of interesting applications that demand this ability. The applications that may utilize WSN could be of a sensitive nature, and as a result, the environment in which they run could need increased security. Due to the fact that sensors are used to monitor sensitive regions, it is crucial to take security and energy efficiency into consideration when building WSNs. Batteries are used to provide the sensor nodes with their necessary power. It is not possible to recharge the sensor nodes since they are placed in such an extreme environment. In order to lengthen the network's lifetime and make it more reliable, energy usage has to be optimized. The larger amount of energy consumed by sensor nodes during the illegal packet transmission by the malicious node. As a result, it reduces the lifetime of sensor nodes. Without security, adversaries have the ability to destroy the whole functioning of a sensor network by launching a variety of attacks such as message manipulation, message dropping either in part or in its entirety, and message flooding, amongst others. It is critical for the dependability of applications that use the sensor networks to identify the attackers and detect against these same attackers. Implementing security algorithms for processing sensor nodes increase the lifetime of the sensor nodes in WSNs.

This work proposed a Detect and Compare Packet Nonce (DCPN) algorithm that is used to detect Wormhole attacks, Packet Count Detection (PCD) algorithm is used to detect Replay attacks. The different forms mentioned earlier, works on detecting each and every malicious node. There is also an adaptive control that energy saving of the sensor nodes to solve the energy efficiency problem of WSN and increase the lifetime of sensor nodes.

3.2 System Model and Assumption

The proposed system model is deployed via the node initialization procedure, which includes deploying the Sensor, Anchor, and Base stations. We consider a set of Base Station BS_i (i=0,…,I) are geographically localized in a rural area, with a set of several kinds of sensor nodes $Snode_j$ (j=0,…,J) such as static sensor nodes St_Snode_l (l=0,…,L) , mobile sensor nodes M_Snode_m (m=0,…,M), anchor sensor AS_n (n=0,…,N) as well as a set of adversary sensor AdS_k (k=0,…,K). The transmission data of each sensor is in narrow band TDMA schemes, the radio spectrum is divided into time slots, and in each slot, only one Sensor is allowed to be either transmitted or received. We consider, the M_Snode as any client that can move and the instruction services from a specific BS. Furthermore, the St_Snode sends the information periodically about it as weather environment to their BS by sending alarms as a notifications in case of a slight change in temperature. While the BS uses centralized scheduling and routing to allocate bandwidth for each traffic between Sensor-BS and Sensor-Sensor, as shown in Fig. 3-1.

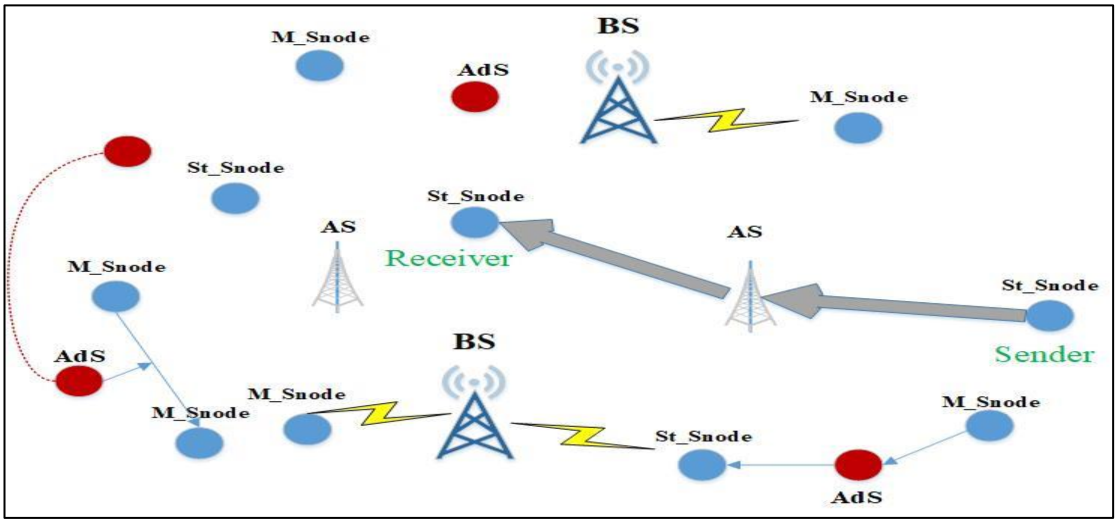


Fig. 3-1 Wireless Channel

When a sensor node is in idle mood, it start to search and discover all its neighboring nodes in order to find the possibility of connection through measuring the distance under some predefined condition such as the sensor displacement as the following Eq. (3.1) (Kurose and Ross, 2021):

$$D_{i,\,j} = \sqrt{(x_i - y_i)^2 + (x_j - y_j)^2} \tag{3.1}$$

Where D is the distance between nodes and (x, y) are coordinate position of node i and node j. Then, each sensor/node such as (St_Snode, M_Snode and BS) finds the nodal processing delay (d_{nodal}).The time it takes to process a packet in a network node along the communication path (Kurose and Ross, 2021) to all estimated nodes Eq. (3.2) consequently.

$$d_{nodal} = d_{proc} + d_{trans} + d_{prop} + d_{queue} \tag{3.2}$$

Where, d_{proc} is processing delay, it is the time it takes to process the packet header, transmission delay d_{trans} is the amount of time required to push all the packets bits into the medium (wireless). Propagation delay d_{prop} is the amount of time required for a signal to be received after it has been sent and d_{queue} is the time a job waits in a queue until it can be executed.

$$d_{trans} = \frac{L}{R} \tag{3.3}$$

In Eq. (3.3), L is the length bits in a packet and R denotes the transmission rate of the link from sender to receiver which measured by bps.

$$d_{prop} = \frac{D_{(x,y)}}{C} \tag{3.4}$$

And C is the speed of light in Eq. (3.4). The propagation delay is the time duration that it takes for one bit to travel from node to another. Then by using Eq. (3.3) and Eq. (3.4) it calculates the total transmission time ($Node'_{TX}$) needed to send a packet, see Eq. (3.5).

$$Node'_{TX} = \frac{L}{R} + \frac{D_{(x\,,\,y)}}{c} \tag{3.5}$$

3.2.1 Received Signal Strength Indicator (RSSI)

RSSI is an estimated measurement of how well a device can hear, detect and receive signals from any sensor nodes in the WSN. RSSI is a value for determining a good wireless connection.

In the next step, all sensors calculate P_{RX} Eq. (3.6) (Franek, 2017), after it's send/receive a packet/data $Node'_{TX}$ from all neighboring nodes. Moreover, the P_{RX} represent the (RSSI) used as a measurement report to determine the strength of connectivity between two communicating nodes as well as carrying out the decision if the nodes can detect and receive packets well or not, for that reason P_{RX} value is compared with the threshold value (Thr) , Thr is a minimum power needed for receiving signals.

$$P_{RX} = \frac{P_{TX} \times G_T \times G_R \times \lambda^2}{(4 \times \Pi \times D_{(x,y)})^2} \tag{3.6}$$

Where, P_{TX} is output power of transmitting antenna, G_T gain of the transmitting antenna, G_R gain of the receiving antenna, λ is wavelength.

The connection between nodes are applied when verify the following condition:

$$P_{RX} \geq \text{ Thr} \tag{3.7}$$

3.2.2 Energy Consumption in WSN

Energy is a limited resource in WSNs. As a matter of fact, the reduction of power consumption is essential to increase the lifetime of low power sensor networks. In general, energy consumption is one of biggest challenges when it comes to WNS (Sangaiah et al., 2019). Since the biggest amount of energy is used for communication, the most logical way to reduce the energy consumption is to reduce the number of packets transmitted between nodes. In order to estimate the energy consumption, attributing Snode is able to make informed decisions that increase the lifetime of the sensor networks. We assume each Snode has the energy to transmit and receive packets named $\text{NodeE}_{TX,}$ NodeE_{RX}. Furthermore, in the Eq. (3.8) a NodeE could be considering the general energy used by a Snode for many reasons including sensing, processing, transmitting and receiving sensory data.

$$\text{NodeE} = \text{P} \times \text{Node}'_{(TX,RX)} \tag{3.8}$$

Then the energy consumption that can be used to transmit data (packet) by each NodeE_{TX}, can be represented as follows in Eq. (3.9), also consumed as energy according to Node_{TX} and j is the set of sensor nodes.

$$\text{NodeE}^{j}_{TX} = \text{P}_{TX} \times \text{Node}^{j}_{TX} \tag{3.9}$$

$$\text{NodeE}^{j}_{\text{initial}} = \text{NodeE}^{j}_{\text{initial}} - \text{NodeE}^{j}_{TX} \tag{3.10}$$

Where, Eq. (3.10) $\mathrm{NodeE}^{j}_{\mathrm{initial}}$ is initial energy of the source node will decrease. The energy consumption of receiving a packet by each $\mathrm{NodeE}_{\mathrm{RX}}$ in the Eq. (3.11). And consumed energy is based on $\mathrm{Node}_{\mathrm{RX}}$ of the receiver node.

$$\mathrm{NodeE}^{j}_{\mathrm{Rx}} = \mathrm{P}_{\mathrm{RX}} \times \mathrm{Node}^{j}_{\mathrm{Rx}} \tag{3.11}$$

$$\mathrm{NodeE}^{j}_{\mathrm{initial}} = \mathrm{NodeE}^{j}_{\mathrm{initial}} - \mathrm{NodeE}^{j}_{\mathrm{RX}} \tag{3.12}$$

In the Eq. (3.12) $\mathrm{NodeE}^{j}_{\mathrm{initial}}$ is the initial energy of the destination node, it will decrease.

3.3 WSN Attack and Detection Algorithms

3.3.1 Attack Procedures

A vulnerability is an issue in a WSN that an attacker can use to launch a successful attack. When the sensor node is deployed in a communication environment unattended, the nodes are vulnerable to various attacks. These can be caused by weakness of the system or user error, and attackers will attempt to exploit any of them, to achieve their end goal.

3.3.1.1 Wormhole Attack Procedure

Wormhole attack is a severe type of attack for wireless networks. For introducing a wormhole attack, an adversary can establish a wormhole link by connecting two distant points in the network using a direct low latency communication link known as the wormhole link, such as an Ethernet cable, a long range wireless transmission, or an optical link, among other things, let assume $\mathrm{AdS}_{\mathrm{s\_wormhole}}$ is wormhole sender and $\mathrm{AdS}_{\mathrm{r\_wormhole}}$ is wormhole receiver between nodes. Just like the figure 3-2 shows the two attackers are located in a strong strategic position in the network.

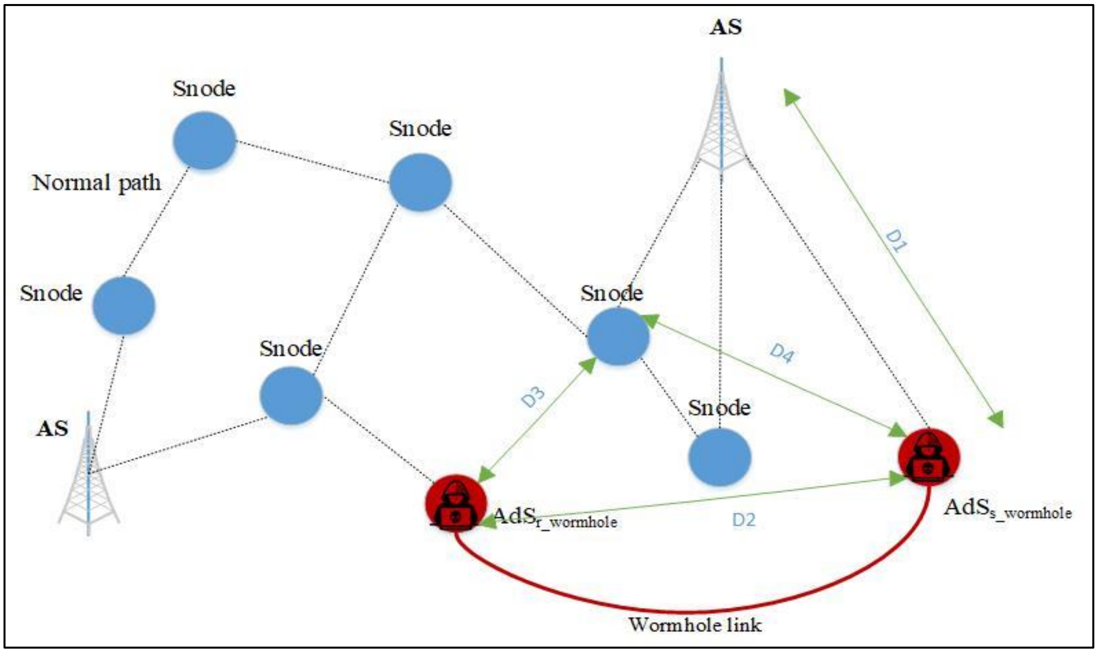


Fig. 3-2 Wormhole attack procedure

To establish the connection between $Snode_j$ (j=0,…,J), AS_n (n=0,…, N) and AdS_k (k=0,…,K) by using the following steps:

- Step 1: Compute the distance between Snode, AS and AdS by using Eq. (3.1). D1 is the distance between AS and $AdS_{s\_wormhole}$, D2 is the distance between $AdS_{s\_wormhole}$ and $AdS_{r\_wormhole}$, D3 is the distance between Snode and $AdS_{r\_wormhole}$ and D4 is the distance between Snode and $AdS_{s\_wormhole}$, as shown in Fig. 3-2.
- Step 2: After that, it is necessary to find P_{RX} for each one by using Eq. (3.6). $P_{RX}^{n.ks\_wormhole}$ is based on D1, $P_{RX}^{ks\_wormhole.ks\_wormhole}$ is based on D2, $P_{RX}^{j.kr\_wormhole}$ based is on D3 and $P_{RX}^{j.ks_{wormhole}}$ is based on D4.

- Step 3: The P_{RX} value for each one are compared with Thr value, so a wormhole attack is applied whenever the evaluated ($P_{RX}^{n.ks\_wormhole}$) and $AdS_{s\_wormhole}$ confirm the following conditions Eq. (3.13):

$$P_{RX}^{n.ks\_wormhole} \geq Thr \;\&\&\; P_{RX}^{ks_{wormhole},kr_{wormhole}} \geq Thr \;\&\&\; P_{RX}^{j.kr\_wormhole} \geq Thr \;\&\&\; P_{RX}^{j.ks_{wormhole}} < Thr \qquad (3.13)$$

Where, $P_{RX}^{n.ks\_wormhole}$ is the power received from a distance between Snode and $AdS_{s\_wormhole}$ is greater than Thr value. Then the energy consumption is calculated by Eq. (3.12). Finally, transmitting malicious data ($Pkt_{wormhole}$) to wireless channel (W-channel). The pseudo code of wormhole attack is shown in algorithm1.

Algorithm 1: Wormhole Attack

```
Let j be the set of Snode
Let n be the set of AS
Let $k_{s,r}$ be the set of AdS
Let s is wormhole sender
Let r is wormhole receiver
Let Range k=[20,40,60,80,100]
Set $Thr = \emptyset$, is the set of value
Let $P_{TX,RX}$ be the set of P
Set $E_{initial}$ =1000 joule                    //residual energy of node
Let $D_{j,n,k}$ be the set of distance
Initiate wormhole attack connection
for all j ∈ W-channel do                         //Connection between different nodes
```

```
if j. $E_{initial} > 0$ then                                   //Nodes are active
for s $\in$ k do
for r $\in$ k do
if s is equal to r then
Calculate $D_{n,k}$ , $D_{ks,kr}$ ,$D_{j,kr}$ ,$D_{j,ks}$             // calculate distance using Eq.(3.1)
Calculate $P_{RX}^{n.ks}$ , $P_{RX}^{kr.ks}$, $P_{RX}^{j.kr}$ , $P_{RX}^{j.ks}$       //calculate power reviving for each node using Eq. (3.5)
if $P_{RX}^{n.ks} \geq$ Thr then
Calculate $E_j \leftarrow P_{RX}^{j} * Tx_j$
    if j. $E_{initial} \geq E_j$ then
    Generate j. $E_{initial} \leftarrow$ j. $E_{initial} - E_j$           // Decrease energy
Generate Add $Pkt_{wormhole}$ to W-channel          //Add malicious data to a wireless channel
```

3.3.1.2 Replay Attack Procedure

A replay attack is carried out by continuously keeping track of the packets exchanged between Snode and replayed later to either bring down the target node, or to affect the performance of the target network. To create connection with the other Snode, we will be following these steps:

- ➢ Step 1: Find the distance between Snode, AS, AdS, by using Eq. (3.1)
- ➢ Step 2: After that find P_{rx} for each one by using Eq. (3.6). P_{RX}^{n,k_replay} is based on the distance between AS and AdS, and $P_{RX}^{j.n}$ is based on the distance between Snode and AS
- ➢ Step 3: The P_{rx} for each one are compared with Thr value, in the Eq. (3.14).

$$P_{rx}^{j.n} \geq \text{ Thr } \&\& \ P_{rx}^{n,k\_replay} \geq \text{ Thr} \qquad (3.14)$$

When $P_{RX}^{j.n}$is greater than P_{E}^{Three} value and also P_{RX}^{n,k_replay} is greater than P_{E}^{Three} value then the connection is established. After that compute, the energy consumption is calculated by Eq. (3.12). Next is sending malicious data (Pkt_{replay}) across the W-channel. The pseudo code of replay attack is shown in algorithm 2.

Algorithm 2: Replay Attack

```
Let j be the set of Snode
Let n be the set of AS
Let k be the set of AdS
Let Range k=[20,40,60,80,100]
Set  Thr =∅, is the set of value
Let $_{TX, RX}$ be the set of P
Set $E_{initial}$ =1000.0 joule
Let $D_{j,n,k}$ be the set of distance
Initiate replay attack connection
for all j ∈ W-channel do                              //Connection between different nodes
  if  j. $E_{initial} > 0$ then                       //Nodes are active
    Calculate $D_{j,n}$ ,$D_{n,k}$
    Calculate  $P_{RX}^{j,n}$ , $P_{RX}^{n,k}$
    if $P_{RX}^{j.n} \geq$  Thr && $P_{RX}^{n,k} \geq$ Thr  then
      Calculate $E_j \leftarrow P_{RX}^{j} * Tx_j$
      if j. $E_{initial} \geq E_j$ then
        Generate j. $E_{initial} \leftarrow$ j. $E_{initial} - E_j$        // Decrease energy
        Generate Add  $Pkt_{replay}$ to W-channel     //Add malicious data to a wireless channel
```

3.3.2 Detection Procedure

In a WSN environment, these algorithms are what monitor network traffic to detect illegal nodes which are designed to detect attacks such as wormhole attacks and replay attacks in WSNs in order to protect all networks from being vulnerable to packet loss, delay, and adversaries that can misdirect the multi-hop routing. The amount of energy that is used by each node in a network is the most important aspect of this new approach that has been offered. The energy module maintains track of the current energy status of each and every node that is involved in the packet transmission process between nodes.

3.3.2.1 Wormhole Detection Procedure

This work is based on the detection of wormhole attacks in a particular network. In this proposal, a detection mechanism is proposed in securing the communications between source and destination node. A technique to detect and further defend the sensor network from attacks is to use Detect and Compare Packet Nonce (DCPN) algorithm. A nonce is randomly generated by the party that introduces it into the conversation which is used only once per request. It's essential that the attacker should not be able to affect the Nonce’s choice, nor to be able to predict it. The nonce used in the encrypted parts of the data packet is sent in the same data packet. The header of data will contain the nonce. Also, the adversary nodes have a special packet nonce that are sent with the malicious data to the target. The packets are transmitted by the source sensor including packet nonce ($\mathrm{Pkt}_{\mathrm{nonce}}^{\mathrm{j}}$) and packet nonce id ($\mathrm{Pkt}_{\mathrm{nonceID}}^{\mathrm{j}}$). Also, adversary nodes have packet nonce ($\mathrm{Pkt}_{\mathrm{nonce}}^{\mathrm{k}}$) and packet id ($\mathrm{Pkt}_{\mathrm{nonceID}}^{\mathrm{k}}$) as shown in Eq. (3.15).

$$\text{If}\begin{cases}\text{Pkt}^{j}_{\text{nonceID}} \neq \text{Pkt}^{k}_{\text{nonceID}} & \text{Wormhole attacks are detected}\\ \\ \text{Pkt}^{j}_{\text{nonce}} \neq \text{Pkt}^{k}_{\text{nonce}} & \text{Wormhole attacks are detected}\end{cases} \qquad (3.15)$$

After the attacks detection, the packet will be dropped. If the packet does not contain malicious data, the packet will be decrypted by the receiving node and the message must be matched with the one distributed. The pseudo code for wormhole detection is shown in algorithm 3.

Algorithm 3: DCPN Algorithm

```
Let j be the set of Snode
Let n be the set of AS
Let k be the set of AdS
Let Range k=[20,40,60,80,100]
Initial  Wormhole detection
If $k_{\text{wormhole\_Pkt}} \neq 0$ then
for all $j \in$ Snode do
 for all $n \in$ AS do
 for each $\text{Pkt}_{\text{nonce}} \in \text{Pkt}^{n}_{\text{nonce}}$ do
 Generate ID$\leftarrow \text{Pkt}_{\text{nonceID}}$
  Generate nonce$\leftarrow \text{Pkt}_{\text{nonce}}$
  if  ID== $\text{Pkt}^{j}_{\text{nonceID}}$&& nonce== $\text{Pkt}^{j}_{\text{nonce}}$then
 Generate Add data to destination$_j$        // add the secure packet in to the receiving side
```

3.3.2.2 Replay Detection Procedure

In this work, a mechanism has been designed to detect replay attacks by proposing Packet Count Detection (PCD). PCD is designed to be monotonically either increasing or decreasing for each transmitted packet. If a packet is replayed, it will have a very small or very old sequence number that be will be discarded. Each packet has its own ID; whenever a packet is received by the receiver, the packet will be counted (Pkt_{count}). In the Eq. (3.16) if the received packet from adversary is less than the sensor received packet, the replay attack will be detected and the last received packet will be discarded as a result of that.

$$\text{-If} \qquad Pkt_{count} > Pkt_j \text{ -1} \qquad \text{Replay attack is detected} \tag{3.16}$$

Then the data is added into receiving side. Otherwise, the data is replayed once and discarded by the Snode destination. The pseudo code of replay detection is shown in algorithm 4.

Algorithm 4: PCD Algorithm

```
Let j be the set of Snode
Let k be the set of AdS
Let Range k=[20,40,60,80,100]
**Initial** Replay detection
**for** each j ∈ Snode **do**
    **for** each Pkt ∈ $j_{Pkt}$ **do**
        **if** $k_{replay}$ is not equal to 0 **then**
            **Generate** $Pkt_{count} \leftarrow 0$                //used to reject duplicate packet
            **if** $Pkt_{count} > Pkt_j$ -1  &&  $k_{replay\_Pkt} \neq 0$ **then**
                **Generate** Reject the last received packet
```

3.4 Summary

This chapter proposes a Detect and Compare Packet Nonce (DCPN) algorithm is used to detect wormhole attacks and Packet Count Detection (PCD) algorithm is used to detect replay attacks. In order to overcome the WSN's energy efficiency issue, there is also improves the sensor nodes' energy efficiency and enhances the lifetime of sensor node.

CHAPTER FOUR: EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Introduction

In a previous contribution (Chapter three), The (DCPN) algorithm is proposed for detecting wormhole attacks, and the (PCD) algorithm is proposed for detecting replay attacks. The algorithms increased the sensor nodes' lifetime by minimizing their energy consumption. Energy conservation is critical in WSN, as sensor nodes carry a limited, non-rechargeable power source, and it is not easy to replace the nodes, which makes power saving important to increase the lifetime of nodes. Since The larger amount of energy consumed by sensor nodes during the illegal packet transmission by the malicious node Thus, the most rational strategy is to decrease the amount of energy, which means decreasing and eliminating the number of malicious packets that are exchanged between sensor nodes.

This chapter shows the results of DCPN and PCD algorithms and the temperature monitoring of some mobile sensor nodes in WSN channel.

4.2 Experimental Results and Analysis

The proposed system architecture is simulated to evaluate its effectiveness and confirm theoretical background. The simulated findings of each algorithm are shown and discussed separately.

4.2.1 Simulation Environment

To investigate the performance of the proposed power consumption of each node and reduction mechanisms by implementing the aforementioned algorithms based on WSN Localization simulator (Naguib and Computers Engineering Department, 2011). The network topology consists of five BSs, they are located at (20, 20), (520, 20), (270, 270), (20, 520), and (520, 520). Several Snodes are randomly distributed in a 540 x 540 M^2 area with other nodes acting as the AdS to generate several types of packets such as Wormhole attacks and Replay attacks. The results indicate the efficiency of our protocol even despite the number of adversary nodes increasing. The simulation parameters are detailed in table 4-1.

Table 4-1 Simulation parameters

Parameters	**Values**	**Parameter**	**Values**
M_Snode	200	Size of Ack Packet	40 byte
AS	20	Average Temp.	25 ^{o}c
AdS	0,20,40,60,80,100	Maximum Temp.	50 ^{o}c
Sensor model Mica2	914 MHz	Thr	≥ 0.1
Initial Energy	1000 Joule	Packet Error Rate	0.01 byte
TX Power	16.23 dBm	Mobility Speed	0-10 m/sec
RX Power	14.62 dBm	AdS Radius	150 m
Data rate	38000 bps	Wormhole Link	300 m
Packet size	512 byte	AS Antenna Type	Omni-directional
Size of Neg packet	210 byte	Simulation Time	150 sec

4.2.2 Performance Evaluation

The simulation results are analyzed for parameters such as energy consumption and the increased lifetime and temperature monitoring of sensors in the case of wormhole and replay attacks. Most of the energy consumption mechanisms lie in data transmission.

4.2.2.1 Energy Consumption

The effectiveness of wormhole and replay attacks are shown in Fig. 4-1 and Fig. 4-2. A number of adversaries are extremely impacting on the energy efficiency of WSNs. As the number of adversaries increase, the energies are severely consumed due to the large numbers of the aggregation processes for illegal or malicious information performed by these nodes. Fig. 4-1 shows the energy efficiency of each node in every round compared with wormhole attacks and DCPN algorithm. While applying wormhole attacks on the particular node, the residual energy is reduced dramatically, so the DCPN algorithm is used to detect the impact of wormhole attacks and save the energy of the sensor node. However, the nodes consume energy to secure data transmission. The blue line shows a wormhole attack scenario. While the number of adversaries is (80), the total energy consumption is (3%) with wormhole attacks. The red dash line shows that preventing wormhole attacks improve the lifetime of the sensor network significantly. By implementing DCPN, energy consumption is reduced to (1.7%) which means the energy consumption is reduced by (1.3%). When comparing the power consumption to packet delivery with and without Wormhole attacks, it becomes clear that when wormhole attacks are avoided, performance improves.

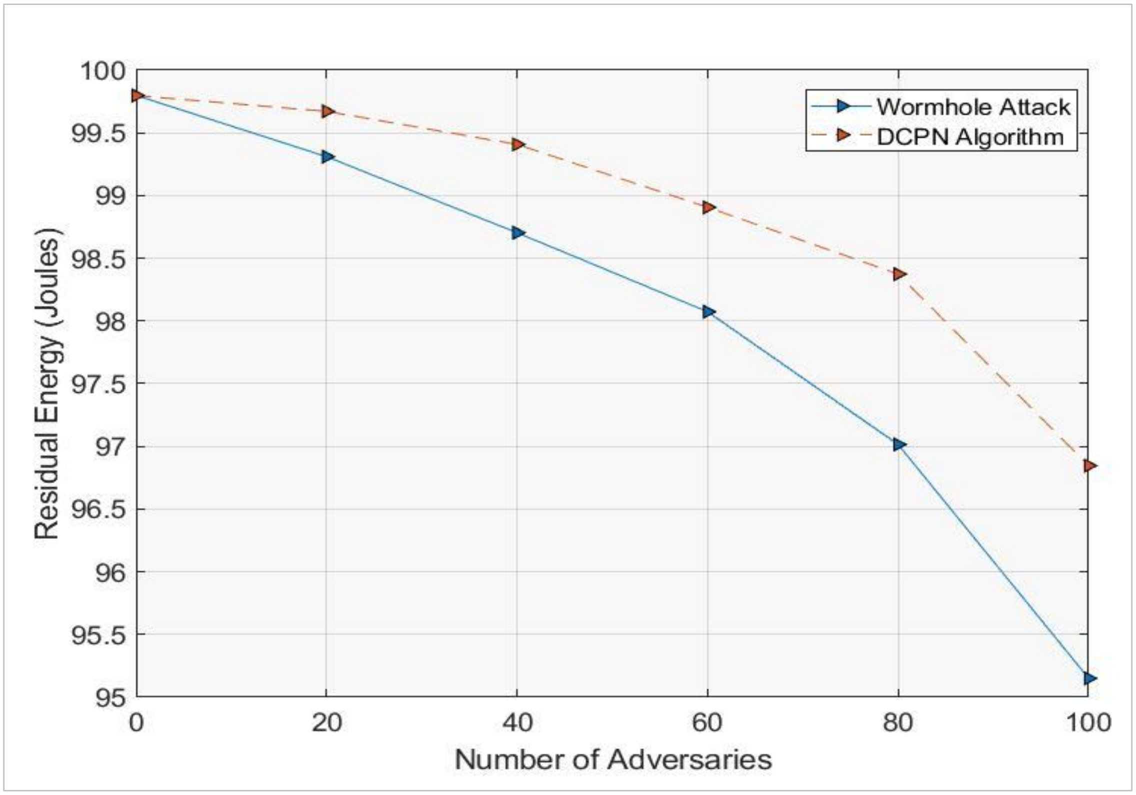


Fig. 4-1 Residual energy of nodes during wormhole attack and DCPN algorithm

In comparison to the replay attacks and the PCD algorithm, Fig. 4-2 shows the energy efficiency of each node in each round. When the number of adversaries' reaches 80, the overall energy consumption with Replay attack is (1.6%). because, it can directly send malicious packet to the destination node. since the PCD is used to eliminate the replay attack packets. When the PCD is applied, the energy consumption drops to (1.1%), thus reducing the energy consumption by (0.5%) at this point and optimizing the lifetime of the nodes.

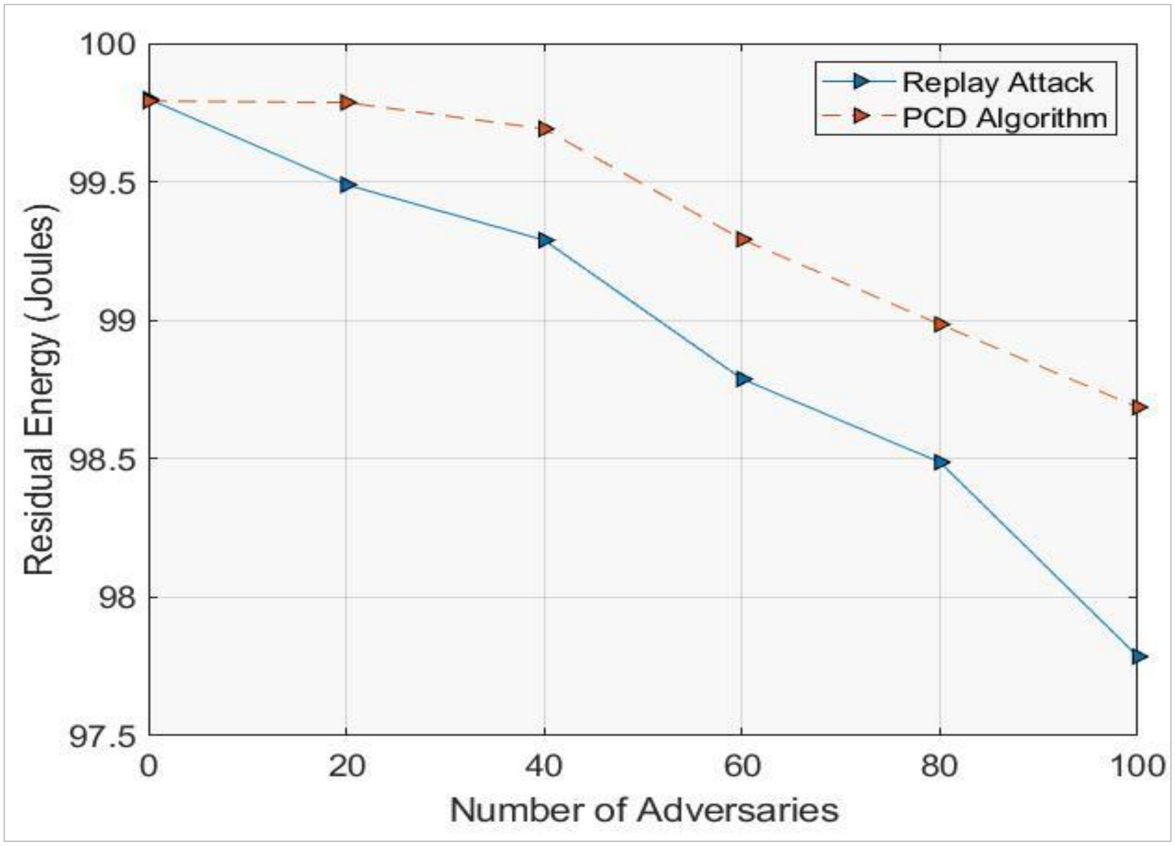


Fig. 4-2 Residual energy of nodes during replay attack and PCD algorithm

4.2.2.2 Lifetime of the Sensor Nodes

A WSN's lifetime is the period of time during which it would be fully functional. Two interrelated key components of WSN are the lifetime and energy requirements of the sensor node. It is possible to lengthen the sensor network's lifetime and improve its dependability by minimizing or eliminating illegal information and data transmissions as well as duplicate data transmissions. In Fig. 4-3, as showed the lifetime of all sensors in each round. While using the DCPN, the lifetime of sensors is increased by (19.2%) per hour. The lifetime of the sensor nodes is also improved. When the PCD algorithm is used, the lifetime is increased to (12%) per hour. Table 4-2 showed a set of sensor lifetime information, including DCPN and PCD for each round.

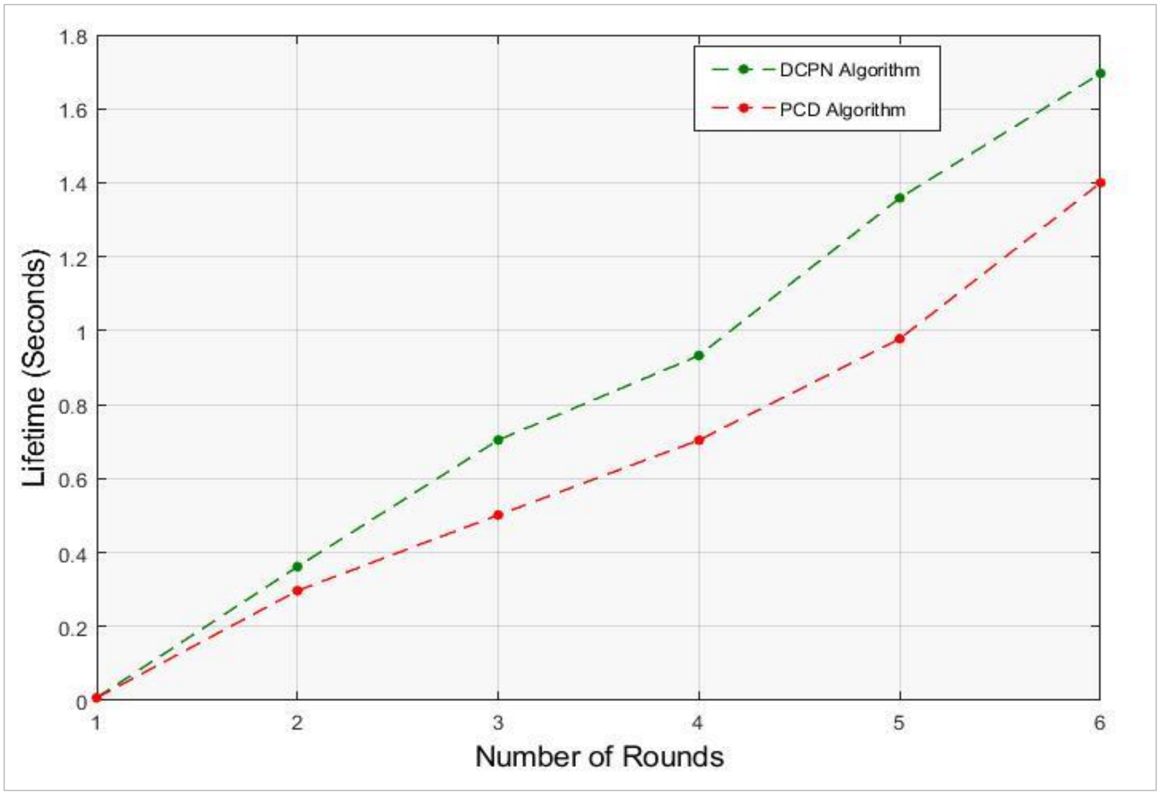


Fig. 4-3 Lifetime of sensor nodes

Table 4-2 Lifetime of Sensor Nodes

No. of Rounds	DCPN Algorithm(S)	PCD Algorithm(S)
1	0.007495	0.007228
2	0.361773	0.296864
3	0.704285	0.501668
4	0.932769	0.704074
5	1.35886	0.978364
6	1.695851	1.399883

4.2.2.3 Temperature of Mobile Sensor Nodes

Temperature has a direct influence on WSNs through sensor batteries, as showed from Fig. 4-4 and Fig. 4-5. Due to high processing in the sensors for transmitting and receiving data, the sensor temperature will be high. Applying wormhole attacks and replay attacks on the sensors by sending malicious data, the computation will further increase which lead to more power consumption. DCPN, PDC implementation on sensors will stabilize the temperature of the sensors and prohibits further increase in temperature. By implementing these algorithms, the temperature of the sensors can be reduced by (1^0C- 2.5^0C) per (2.5) minutes.

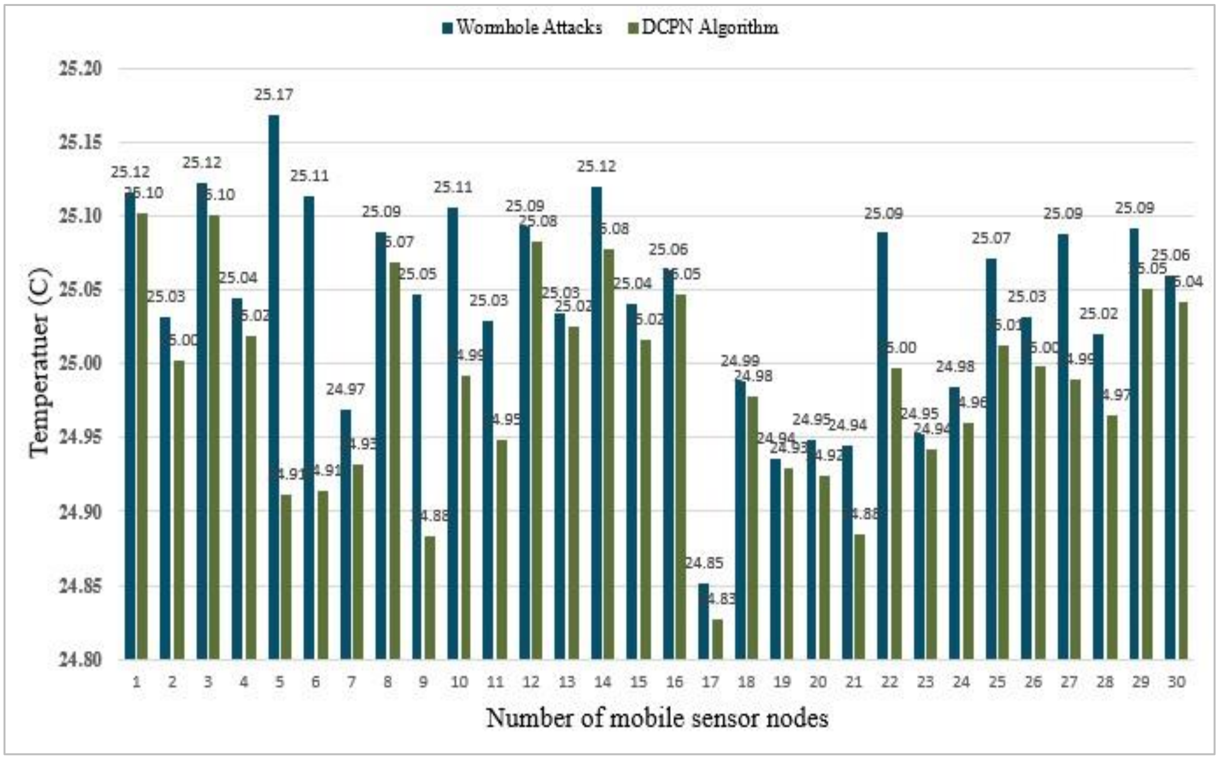


Fig. 4-4 Temperature of sensor nodes with wormhole attack and DCPN algorithm

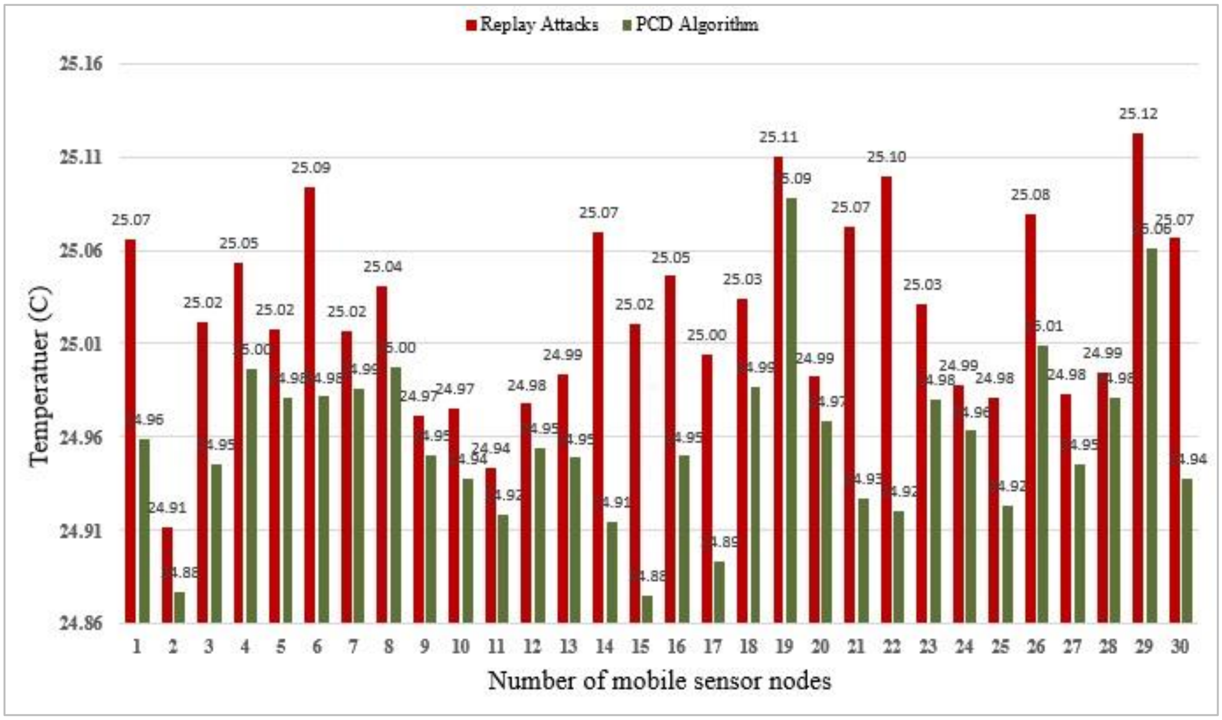


Fig. 4-5 Temperature of sensor nodes with replay attack and PCD algorithm

Implementation of these algorithms will increase lifetime of nodes since they make sensors to dissipate less power and stabilize the node temperature into a safe level.

4.3 Discussion

The proposed algorithms improve the efficiency of the sensor nodes by lowering their energy consumption and increasing the lifetime of the sensors. The simulation results show that proposed algorithms can outperform existing techniques in terms of energy consumption and the lifetime of sensor nodes. The comparison is shown in table 4-3 and table 4-4.

Table 4-3 Comparing the results of DCPN with other existing algorithms

Wormhole attacks	**MCRP** (Ahutu and El-Ocla, 2020)	**AD-PSO** (Tamilarasi and Santhi, 2020)	**DCPN**	**Description**
Number of nodes	100	500	200	The results showed that the performance of the proposed DCPN outperformed that of the existing MCRP and AD-PSO in terms of energy consumption and network lifetime.
Simulation time	300s	100s	150s	
Thr value	3.5J	1J	≥ 0.1J	
Conserves energy	19.2% per hours	10% per hour	21.6% per hour	
Lifetime of sensor	Medium	low	High	
Detection performance	100%	90%	100%	

In terms of energy consumption and network lifetime. The results indicated that the DCPN algorithm performed better than the MCRP and AD-PSO algorithms, as shown in Fig. 4-6. In other words, the DCPN algorithm was found to consume less energy and extend the lifetime of the network more effectively than the other two algorithms. These findings could have important implications for the development and implementation of future network protocols, particularly those aimed at optimizing energy usage and prolonging the life of the network.

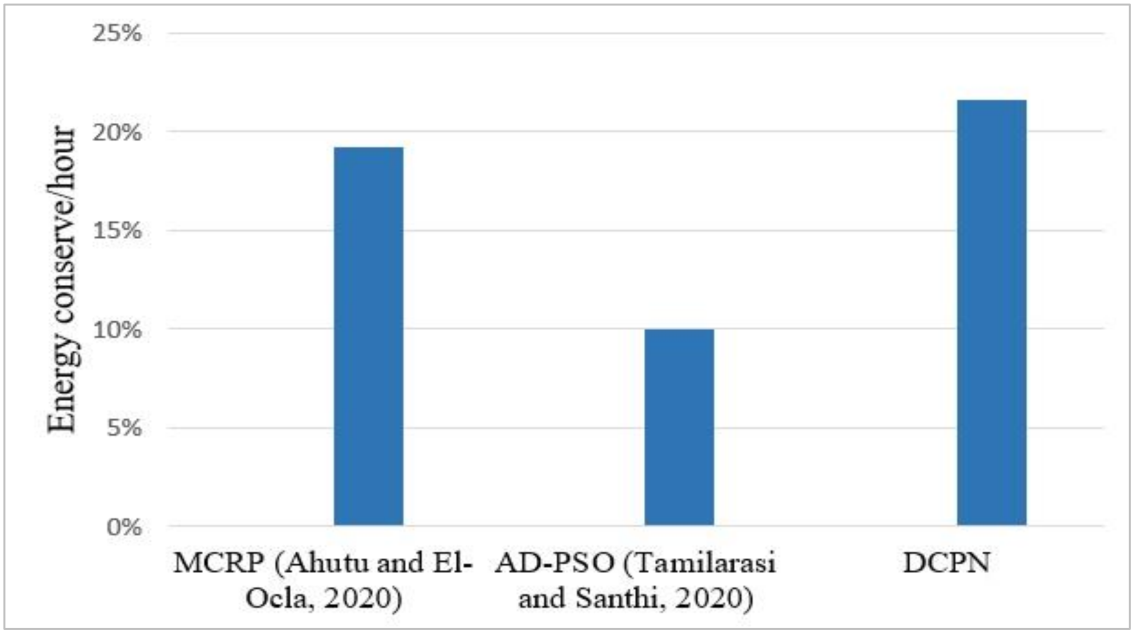


Fig. 4-6 Conserve energy comparison with DCPN

Table 4-4 Comparing the results of PCD with other existing algorithms

Replay attacks	**SIC-MCFA** (Marigowda et al., 2018)	**EDDK-MAC** (Chung and Cho, 2020)	**PCD**	**Description**
Number of nodes	50-100	300	200	The results showed that the performance
Simulation time	150s	180s	150s	

Thr value	≥ 1J	1J	≥ 0.1J	of the proposed PCD outperformed that of the existing SIC-MCFA and EDDK-MAC in terms of energy consumption and network lifetime.
Conserves energy	10% per hours	7% per hour	12% per hour	
Lifetime of sensor	Medium	Medium	High	
Detection performance	95%	100%	100%	

Also, The results that the proposed PCD algorithm had a better performance than the other two algorithms in energy consumption and network lifetime. In other words, the PCD algorithm was found to consume less energy and extend the lifetime of the network more effectively than the SIC-MCFA and EDDK-MAC algorithms. As showed in Fig. 4-7.

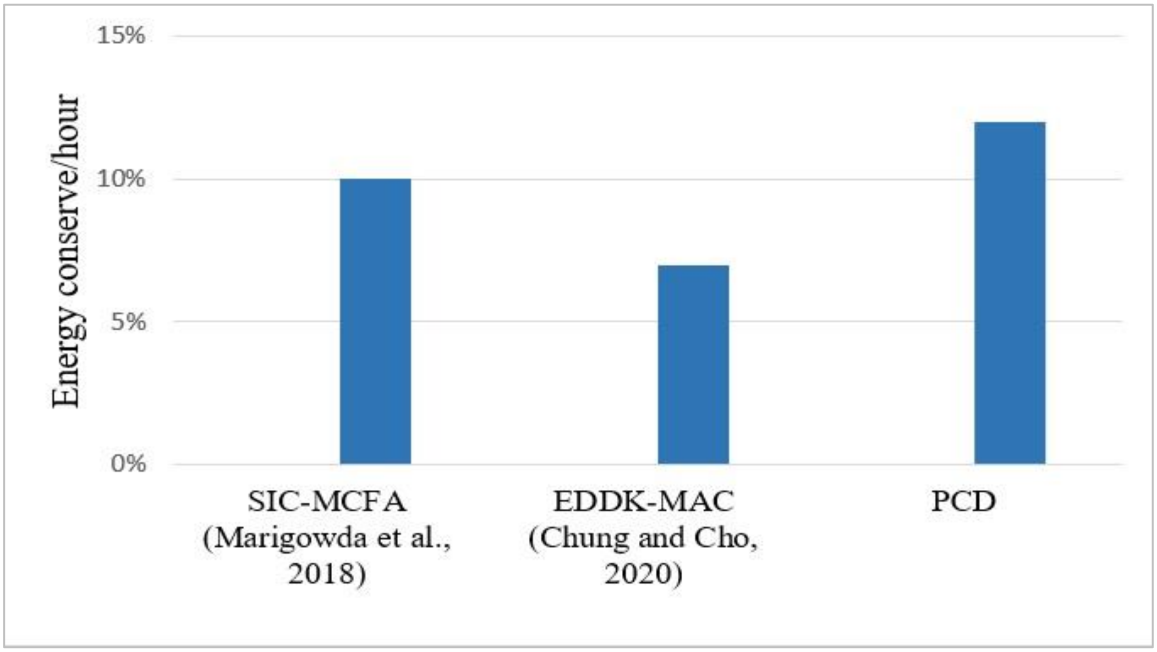


Fig. 4-7 Conserve energy comparison with PCD

4.4 Summary

This chapter shows the results of our algorithms. DCPN and PCD are capable of handling security requirements for mitigating different attacks on WSNs. Thus, the algorithms improve the efficiency of the sensor nodes by lowering their energy consumption. In each algorithm we achieved efficient energy. For instance, DCNP saves up energy by (21.6%) per hour for wormhole attacks, while PCD saves up energy up to (12%) per hour replay attacks, thus extending the network's lifetime much further, enhances the lifetime of the sensor node by (19.2%) per hour with DCPN and (12%) per hour with PCD. Also this chapter shows the monitoring temperature of some mobile sensor nodes. By implementing these algorithms, the temperature of the sensors can be reduced by (1^0C- 2.5^0C) per (2.5) minutes.

CHAPTER FIVE: CONCLUSION AND FUTURE WORKS

5.1 Introduction

This chapter ends the thesis and summarizes the most significant contributions and discoveries. The first section is the summary of the thesis, while the later section discusses the constraints of the study and presents a list of potential possibilities for further research.

5.2 Conclusion

WSNs provide new options for economical, efficient, and quality data collection due to their compelling advantages over manual data collection. They have the potential to allow new applications for environmental monitoring, give high-resolution analysis of scientific phenomena, save costs in logistical tracking, and provide early warning for military and border control applications, among other uses. In the WSN, energy conservation is a major concern. Because the main source of power for sensor nodes is a battery with limited energy, it cannot be easy to replace or recharge. The large amount of energy consumed by sensors during the illegal information transmission by the malicious node. As a result, it reduces the lifetime of sensor nodes. Also, due to high processing in the sensors for transmitting and receiving malicious data. Therefore, thorough assessment of the security risks and prospective attacks are essential in order to guarantee that the systems will not fail in unexpected ways. To detect malicious attacks and outside subversion from impeding public acceptance of WSN deployments, it is crucial to consider the impact of common security threats on their data relaying methodologies and to develop in depth defense in which routing technologies recommend preventing threats within the network.

In Chapter 2, we analyzed the security of WSNs from the perspective of an attacker since we consider such perspectives as something that cannot be ignored when assessing security challenges. The greatest challenge of the sensor network is security. Some applications such as military, healthcare, tracking and so on, need a secure communication. In order to achieve a secure communication, the network must fulfill some security requirements.

In chapter 3, we identified that the primary aim of WSN is either security or energy efficiency. Therefore, the proposed system named as DCPN and PCD that can jointly mitigate energy issues for a large scale WSN. DCPN and PCD are capable of handling security requirements for mitigating different network layer attacks on WSNs. particularly focusing on Wormhole and Replay attacks. Thus, the proposed system improves the efficiency of the sensor nodes by lowering their energy consumption and increasing the lifetime of sensor nodes.

Chapter 4 was inspired and resulted by Chapter 3. In each algorithm we achieved efficient energy, DCNP saves energy by (21.6%) per hour for a Wormhole attacks, whereas PCN saves up energy by (12%) per hour for Replay attacks, thus increases the lifetime of the sensor node by (19.2%) per hour when using DCPN and by (12%) per hour when using PCD. Also, it enables both optimum node maintenance and safe data aggregation. The simulation's results showed a significant improvements in terms of energy consumption and overall performance of WSN. This chapter also discusses how to monitor the temperature of various mobile sensor nodes. By implementing these algorithms, the temperature of the sensors can be reduced by (1^0C- 2.5^0C) per (2.5) minutes.

5.3 Future Works

There were a number of unresolved concerns that need further investigation in the future. Only the most promising ones are highlighted from our perspective. We foresee a possible design area for some innovative and intrusion detection algorithms that might operate effectively despite privacy protections. Modification of the utilized attacker models would be an interesting research direction, particularly in terms of privacy protections for WSNs. We believe that the existing models of attackers do not accurately depict real-world adversaries. Therefore, by using machine learning, the WSN network can analyze patterns and learn from them to help detect and prevent different types of attacks and respond to changing behavior. It can help security teams be more proactive in preventing threats and responding to active attacks in real time.

Security research about WSNs in its original form is slowly becoming obsolete. Even the abstract model of a sensor network as partly presented in this thesis should be replaced by a real world sensor network with a particular application scenario. We have tried to move in this direction by designing a practical adaptive security architecture based on a security and privacy requirement analysis of a concrete application scenario. However, we expect future studies to go even further by using artificial intelligence and machine learning based security algorithms in WSNs. Because machine learning models can analyze large amounts of data, expose network vulnerabilities, and anticipate when and how future attacks will occur

We anticipate that the proposed algorithms and schemes presented in this thesis study will be possible when applied (with some modifications, such as using artificial intelligence) to the new emerging technologies such as pervasive computing, cloud computing, and ubiquitous computing in order to provide efficient energy clustering and the prevention and detection of various attacks. This is truly something that we are very excited about.

REFERENCES

ABIDIN, S. Enhancing security in WSN by artificial intelligence. 2018. International Conference on Intelligent Data Communication Technologies and Internet of Things, Springer, 814-821.

AGIWAL, M., ROY, A. & SAXENA, N. 2016. Next generation 5G wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials,* 18**,** 1617-1655.

AHMAD, I., KUMAR, T., LIYANAGE, M., OKWUIBE, J., YLIANTTILA, M. & GURTOV, A. 2018. Overview of 5G security challenges and solutions. *IEEE Communications Standards Magazine,* 2**,** 36-43.

AHUTU, O. R. & EL-OCLA, H. J. I. A. 2020. Centralized routing protocol for detecting wormhole attacks in wireless sensor networks. 8**,** 63270-63282.

AL-NASSER, F. A. & MAHMOUD, M. S. 2012. Wireless sensors network application: a decentralized approach for traffic control and management. *Wireless Sensor Networks: Technology and Applications***,** 347-374.

ALIADY, W. A. & AL-AHMADI, S. A. 2019. Energy preserving secure measure against wormhole attack in wireless sensor networks. *IEEE Access,* 7**,** 84132-84141.

ANEJA, D., KUMAR, L. & SHARMA, V. 2019. A cluster based approach for detection and protection of wormhole attack in wireless sensor network. *Sensor Letters,* 17**,** 955-964.

BELGHITH, A. & OBAIDAT, M. 2016. Wireless sensor networks applications to smart homes and cities. *Smart cities and homes.* Elsevier.

BENSALEH, M. S., SAIDA, R., KACEM, Y. H. & ABID, M. 2020. Wireless sensor network design methodologies: A survey. *Journal of Sensors*.

BHASIN, V., KUMAR, S., SAXENA, P. & KATTI, C. 2020. Security architectures in wireless sensor network. *International Journal of Information Technology,* 12**,** 261-272.

BHAWSAR, A., PANDEY, Y. & SINGH, U. 2020 Detection and prevention of wormhole attack using the trust-based routing system. 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), IEEE, 809-814.

BURHAN, M., REHMAN, R. A., KHAN, B. & KIM, B.-S. 2018. IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors,* 18**,** 2796.

CAYIRCI, E. & RONG, C. 2008. *Security in wireless ad hoc and sensor networks*, John Wiley & Sons.

CHO, Y., QU, G. & WU, Y. 2012 Insider threats against trust mechanism with watchdog and defending approaches in wireless sensor networks. IEEE symposium on security and privacy workshops, 2012. IEEE, 134-141.

CHUNG, W. & CHO, T. 2020. Detection of Replay Attack through Sequence Number Encryption in EDDK based WSNs. *International Journal of Innovative Technology and Exploring Engineering,* 9**,** 593-599.

DÂMASO, A., ROSA, N. & MACIEL, P. J. S. 2017. Integrated evaluation of reliability and power consumption of wireless sensor networks. 17**,** 2547.

DHUNNA, G. S. & AL-ANBAGI, I. 2019. A low power WSNs attack detection and isolation mechanism for critical smart grid applications. *IEEE Sensors Journal,* 19**,** 5315-5324.

DUTTA, N., SINGH, M. M. J. A. C. & TECHNOLOGIES, C. 2019. Wormhole attack in wireless sensor networks: a critical review. 147-161.

FARJAMNIA, G., GASIMOV, Y. & KAZIMOV, C. 2020. An Improved DV-Hop for Detecting Wormhole Attacks in Wireless Sensor Networks. *Journal of Communication Engineering,* 9**,** 29-52.

FRANEK, O. 2017. Phasor alternatives to Friis' transmission equation. *IEEE Antennas and Wireless Propagation Letters,* 17**,** 90-93.

FU, S., ZHAO, L., SU, Z. & JIAN, X. 2018. UAV based relay for wireless sensor networks in 5G systems. *Sensors,* 18**,** 2413.

GALKIN, P. 2018. Model of reducing the power consumption for node of wireless sensor network in embedded control systems. 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), IEEE, 252-256.

GELENBE, E. & KADIOGLU, Y. M. 2018 Energy life-time of wireless nodes with network attacks and mitigation. IEEE International Conference on Communications Workshops (ICC Workshops), 2018. IEEE, 1-6.

GOPIKA, D. & PANJANATHAN, R. 2020. Energy efficient routing protocols for WSN based IoT applications: A review. *Materials Today: Proceedings*.

GOUVY, N., HAMOUDA, E., MITTON, N. & ZORBAS, D. 2013. Energy efficient multi-flow routing in mobile Sensor Networks. 2013 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, 1968-1973.

HOU, J., QU, L. & SHI, W. 2019. A survey on internet of things security from data perspectives. *Computer Networks,* 148**,** 295-306.

HSIEH, M.-Y. & HUANG, Y.-M. 2017. Adaptive security modules in incrementally deployed sensor networks. *International Journal on Smart Sensing and Intelligent Systems,* 1.

JAITLY, S., MALHOTRA, H. & BHUSHAN, B. 2017 Security vulnerabilities and countermeasures against jamming attacks in Wireless Sensor Networks: A survey. International Conference on Computer, Communications and Electronics (Comptelix), 2017. IEEE, 559-564.

KARAKAYA, A. & AKLEYLEK, S. 2018 A survey on security threats and authentication approaches in wireless sensor networks. 6th international symposium on digital forensic and security (ISDFS), 2018. IEEE, 1-4.

KAUR, K., KUMAR, S. & BALIYAN, A. 2020. 5G: a new era of wireless communication. *International Journal of Information Technology,* 12**,** 619-624.

KAUR, K. & KUMARI, N. 2014. Evaluation and analysis of active RFID protocol in wireless sensor networks. *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* 4**,** 11-19.

KAUR, R. & SANDHU, J. K. 2021. A study on security attacks in wireless sensor network. 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), IEEE, 850-855.

KUROSE, J. F. & ROSS, K. W. 2021. Computer Networking: A Top-Down Approach. Edition. *Addision Wesley*.

LI, R., DECOCQ, B., BARROS, A., FANG, Y. & ZENG, Z. 2021. Complexity in 5G Network Applications and use cases. 31st European Safety and Reliability Conference, Research Publishing Services, 3054-3061.

LUPU, T.-G., RUDAS, I., DEMIRALP, M. & MASTORAKIS, N. 2009. Main types of attacks in wireless sensor networks. WSEAS international conference. proceedings. recent advances in computer engineering, WSEAS.

MARIGOWDA, C., THRIVENI, J., GOWRISHANKAR, S. & VENUGOPAL, K. 2018. An Efficient Secure Algorithms to Mitigate DoS, Replay and Jamming Attacks in Wireless Sensor Network. Proceedings of the World Congress on Engineering and Computer Science.

MARTÍNEZ, S. H., SALCEDO, P. O. J. & DAZA, B. S. R. 2017. IoT application of WSN on 5G infrastructure. 2017 International Symposium on Networks, Computers and Communications (ISNCC), IEEE, 1-6.

MEDJADBA, Y., SAHRAOUI, S. J. I. J. O. C. N. & SECURITY, I. 2016. Intrusion Detection System to Overcome a Novel Form of Replay Attack (Data Replay) in Wireless Sensor Networks. 8.

NAGUIB, A. J. S. & COMPUTERS ENGINEERING DEPARTMENT, A.-A. U., CAIRO, EGYPT 2011. Wireless sensor network localization simulator v1. 1.

NEAMATOLLAHI, P., TAHERI, H., NAGHIBZADEH, M. & YAGHMAEE, M.-H. 2011. A hybrid clustering approach for prolonging lifetime in wireless sensor networks. International Symposium on Computer Networks and Distributed Systems (CNDS), 2011. IEEE, 170-174.

PARVIN, J. R. & VASANTHANAYAKI, C. 2019. Particle swarm optimization-based energy efficient target tracking in wireless sensor network. *Measurement,* 147**,** 106882.

PORKODI, R. & BHUVANESWARI, V. 2014 The internet of things (IOT) applications and communication enabling technology standards: An overview. International conference on intelligent computing applications, 2014. IEEE, 324-329.

PRABHU, S. B., BALAKUMAR, N. & ANTONY, A. J. 2017. Evolving constraints in military applications using wireless sensor networks. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN***,** 2347-5552.

PRUTHI, V., MITTAL, K., SHARMA, N. & KAUSHIK, I. 2019 Network layers threats & its countermeasures in WSNs. International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2019. IEEE, 156-163.

RAJARAM, P., SATHISHKUMAR, A. & KHADIRKUMAR, N. 2020a. An Enhanced Deep Learning Approach for Preventing Replay Attacks in Wireless Sensor Network. *Solid State Technology,* 63**,** 8010-8023.

RAJARAM, P., SATHISHKUMAR, A. & KHADIRKUMAR, N. J. S. S. T. 2020b. An Enhanced Deep Learning Approach for Preventing Replay Attacks in Wireless Sensor Network. 63**,** 8010-8023.

RAMESH, P., PRIYA, F. E. M. & SANTHI, B. 2012. Review on security protocols in wireless sensor networks. *Journal of Theoretical and Applied Information Technology,* 38**,** 1-4.

RATH, M. & PATTANAYAK, B. K. 2019. Prevention of replay attack using intrusion detection system framework. *Progress in Advanced Computing and Intelligent Engineering.* Springer.

SANGAIAH, A. K., SADEGHILALIMI, M., HOSSEINABADI, A. A. R. & ZHANG, W. 2019. Energy consumption in point-coverage wireless sensor networks via bat algorithm. *IEEE Access,* 7**,** 180258-180269.

SHARMA, S., BANSAL, R. K. & BANSAL, S. 2016. Energy-efficient data collection techniques in wireless sensor networks. *Emerging Communication Technologies Based on Wireless Sensor Networks: Current Research and Future Applications, CRC Press, Taylor & Francis, USA***,** 275-296.

SHARMA, V. & HUSSAIN, M. 2017. Mitigating replay attack in wireless sensor network through assortment of packets. Proceedings of the First International Conference on Computational Intelligence and Informatics, Springer, 221-230.

SINGH, R., SINGH, J. & SINGH, R. J. M. I. S. 2016. WRHT: a hybrid technique for detection of wormhole attack in wireless sensor networks. 2016.

TAMILARASI, N. & SANTHI, S. J. W. P. C. 2020. Detection of wormhole attack and secure path selection in wireless sensor network. 114**,** 329-345.

VLADIMIROV, I. K., TACHEVA, D. & DOBRINOV, V. 2018. The Present and Future of Embryo Cryopreservation. *Embryology-Theory and Practice.* IntechOpen.

WANG, Y. & GUO, S. 2013. Optimized energy-latency cooperative transmission in duty-cycled wireless sensor networks. 2013 IEEE International Conference on Mechatronics and Automation, IEEE, 185-190.

XIE, H., YAN, Z., YAO, Z. & ATIQUZZAMAN, M. 2018. Data collection for security measurement in wireless sensor networks: A survey. *IEEE Internet of Things Journal,* 6**,** 2205-2224.

YE, D. 2019. Analysis of Wireless Sensor Networks Behavior for Trustworthiness Evaluation. Trusted Computing and Information Security: 12th Chinese Conference, CTCIS 2018, Wuhan, China, October 18, 2018, Revised Selected Papers, Springer, 301.

YONG-MIN, L., SHU-CI, W. & XIAO-HONG, N. 2009. The architecture and characteristics of wireless sensor network. 2009 International Conference on Computer Technology and Development, IEEE, 561-565.

Title of Paper:

Impact of Attacks on Performance and Energy Consumption in Wireless Sensor Network

Published in:

2022 8th International Engineering Conference on Sustainable Technology and Development (IEC)

Date of Conference: 23-24 February 2022

Date Added to IEEE Xplore: 30 June 2022

Electronic ISBN: 978-1-6654-7829-8

Print on Demand (PoD) ISBN: 978-1-6654-7830-4

INSPEC Accession Number: 21846199

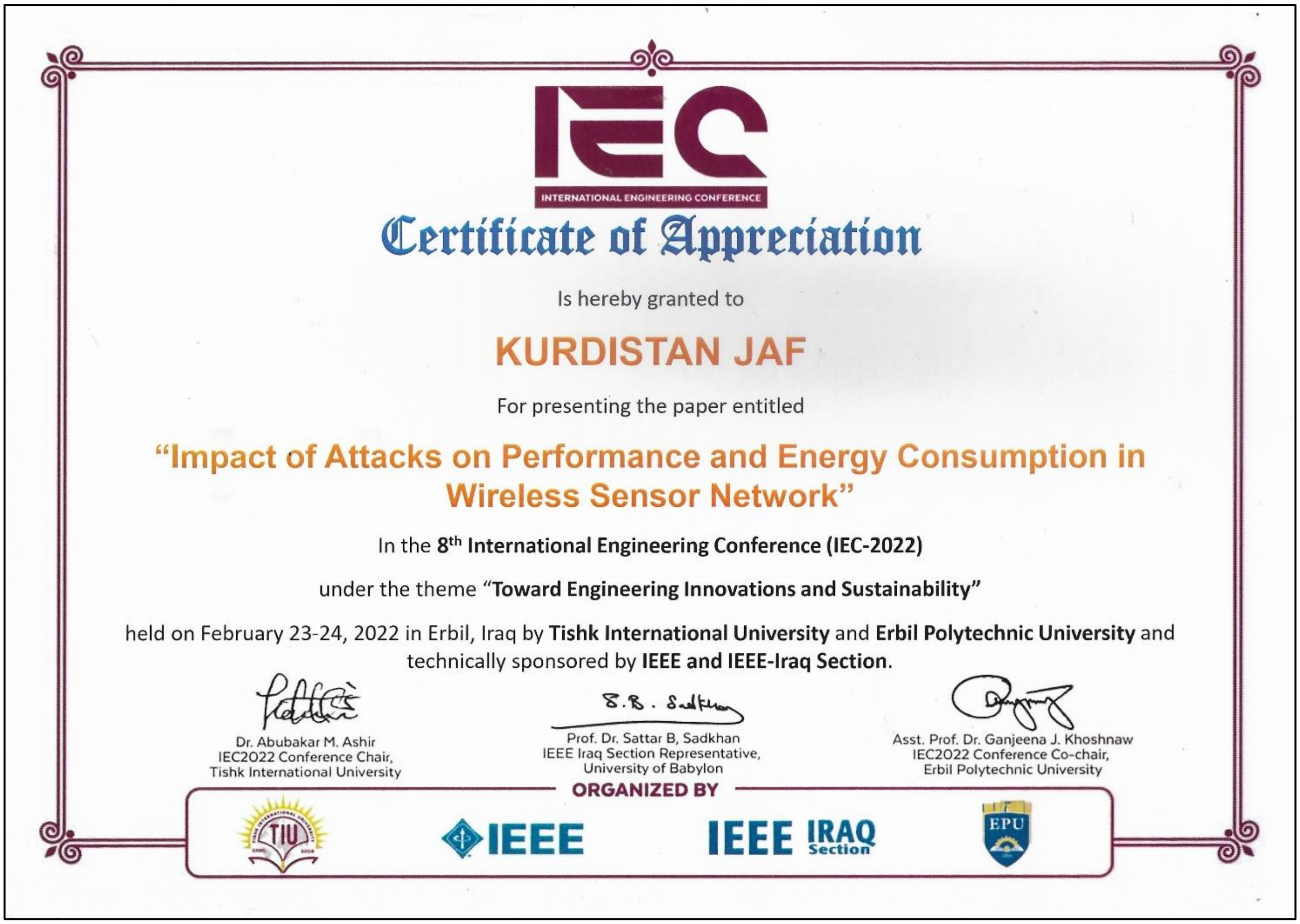
DOI: 10.1109/IEC54822.2022.9807506

Publisher: IEEE

Conference Location: Erbil, Iraq

IEEE Paper Link: https://ieeexplore.ieee.org/document/9807506

Impact Factor: 3.557



IEC

INTERNATIONAL ENGINEERING CONFERENCE

Certificate of Appreciation

Is hereby granted to

KURDISTAN JAF

For presenting the paper entitled

“Impact of Attacks on Performance and Energy Consumption in Wireless Sensor Network”

In the 8th **International Engineering Conference (IEC-2022)**

under the theme “**Toward Engineering Innovations and Sustainability”**

held on February 23-24, 2022 in Erbil, Iraq by **Tishk International University** and **Erbil Polytechnic University** and technically sponsored by **IEEE and IEEE-Iraq Section**.

Dr. Abubakar M. Ashir
IEC2022 Conference Chair,
Tishk International University

S.B. Sadkhan
Prof. Dr. Sattar B, Sadkhan
IEEE Iraq Section Representative,
University of Babylon

Asst. Prof. Dr. Ganjeena J. Khoshnaw
IEC2022 Conference Co-chair,
Erbil Polytechnic University

ORGANIZED BY

TIU IEEE IEEE IRAQ Section EPU

8th International Engineering Conference on advances in Computer and Civil Engineering Towards Engineering Innovations and Sustainability, (IEC-2022), Erbil-Iraq

2022 8th International Engineering Conference on Sustainable Technology and Development (IEC) | 978-1-6654-7829-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/IEC54822.2022.9807506

Impact of Attacks on Performance and Energy Consumption in Wireless Sensor Network

Kurdistan Jaf
Erbil Polytechnic University
Erbil , Iraq
Kurdistan.hamaali@epu.edu.iq

Reben Kurda
Erbil Polytechnic University
Erbil , Iraq
reben.kurda@epu.edu.iq

***Abstract*—In the new technology of the Internet of Things (IoT), the integration of 5G networks and wireless sensor networks (WSNs) are crucial for a wide range of applications. Thousands of sensors are often used in wireless sensor network platforms, which are powered by limited energy resources. The energy consumption of sensor nodes is the most critical issue in a wireless sensor network since it has a direct influence on the network's lifetime. Since wireless sensor network is primarily used to gather information from the environment, it is essential to keep sensitive data safe from unauthorized users. Due to the broadcast nature of radio transmission, sensor nodes are subject to different security attacks. This form of attack may decrease the sensor lifetime from years to days, and have a severe impact on a sensor network. This paper proposes a Detect and Compare Packet Nonce (DCPN) algorithm and Packet Count Detection (PCD) algorithm for wireless sensor networks. These algorithms efficiently identify and isolate attacks like wormhole and replay attacks while avoiding possible service degradation like energy consumption in sensor nodes. The simulation results show that our mechanism can outperform existing techniques in terms of energy consumption. By applying these algorithms, we achieved a maximum energy saving of 33% per hour. Finally, the study also shows the temperature monitoring of some mobile sensor nodes.**

Keywords*— *5G, Internet of Things (IoT), Wireless Sensor networks (WSN), Wormhole attack, Replay attack, energy consumption

I. INTRODUCTION

Internet of Things (IoT) can be considered as an evolved version of WSNs. The concept of IoT has been widely adopted in many fields, such as daily living, manufacturing, health care and transportation, etc. 5G can provide an energy efficient, fast and full coverage network infrastructure for IoT systems [1]. However, the energy consumption and efficiency of WSNs are major concerns in the IoT. WSNs typically characterized by battery powered sensor devices. We need some scheme to enhance the battery life of sensor devices [2]. WSN is a network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical/environmental conditions such as temperature, sound, motion/pollutants at different locations [3]. In WSNs, the energy required to provide smart monitoring, detection and in network activities remains a problem particularly for indoor operations, in which the data-centric temperature increases that eventually leads to more energy requirement. Another challenges that WSN face today is security. WSNs are susceptible to many types of attacks because they serve as an open network with the limited resources of nodes. The most conventional threats to the security of WSN include eavesdropping, node compromised, interrupt, modify or inject malicious packets [4]. The deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks. The communication between sensor nodes in WSNs is accomplished wirelessly by radio. Wormhole and Replay attacks are threats to the security of WSNs [5, 6]. Attackers compromise the internal sensor nodes from which they launch attacks, which are difficult to detect [7]. Adversary nodes work in the same manner as other nodes in the network field, but these adversary nodes try to find the important messages and drop them before sending the whole packets to the next nodes [8]. Based on existing researchers' results, limited power and low memory are obstacles that make conventional security measures inappropriate for WSNs.

In WSNs, Localization of nodes was a key technology for application of WSN. For this purpose, Kalman Filter Localization [9] is extensively used in WSN to identify the optimal location of the sensor nodes. The Kalman Filter estimates the actual output as compared to an input measurement from reality by using previous sensor data.

The use of a WSN in the design phase is essential for identifying security vulnerabilities. Furthermore, understand the impact (especially the power consumption impact) of the most typical attacks on a node (or the entire network) helps to prevent possible problematic vulnerabilities. The main target of this paper is proposes a Detect and Compare Packet Nonce (DCPN) algorithm uses to detect wormhole attack and a Packet Count Detection (PCD) algorithm uses to detect replay attack. There is also an adaptive control that enhances the energy efficiency of the sensor nodes to solve the energy efficiency problem of WSN.

The rest of this paper is structured as follows: Section II describes related work. The system model and the problem definition are illustrated in Section III. Section IV presents the proposed detect and isolate attack algorithms. The results along with implementation features are discussed in Section V. Finally, section VI concludes the paper.

II. RELATED WORK

WSN is a relatively new technology with a larger coverage scope. Wormhole attack and Replay are the various attacks performed in WSN. There are a variety of approaches for detecting and preventing attacks. The following is a concise description of some of these approaches:

پوخته

یەکخستنی تۆڕەکانی 5G و تۆڕەکانی هەستەوەری بێ تەل (WSN) بۆ بوارە نوێیەکەی ئینتەرنێتی شتەکان (IoT) زۆر گرنگە، کە بۆ کۆمەڵێک بەرنامەی بەرفراوان بەکاردەهێنرێت. وەک: ژیانی ڕۆژانە، بەرهەمهێنان، چاودێری تەندروستی و گواستنەوە و هتد.. تۆڕی هەستەوەری بێ تەل لە گرێی هەستەوەری بچووک پێکدێت کە وزەی سنووردارە. ئەم جۆرە گرێیانە توانای چاودێریکردنی بارودۆخی فیزیکی و گەیاندنی زانیارییان هەیە لە نێوان گرێکاندا بەبێ ئەوەی پێویستی بە میدیای گواستنەوە هەبێت. تۆڕەکانی هەستەوەری بێ تەل سەربەخۆن و لە بۆشایی ئاسمان دابەش دەکرێن. بەهۆی نەبوونی دەسەڵاتی ناوەندی و جێگیرکردنی هەڕەمەکی گرێکان لە تۆڕەکەدا، تۆڕی هەستەوەری بێ تەل تووشی هەڕەشەی ئەمنی دەبێت.

تۆڕی هەستەوەری بێ وایەر بەرەوڕووی زۆرێک لە هێرشەکانی چینەکانی تۆڕ دەبنەوە وەکو هێرشی وۆرمهۆل و ریپلەی. هەروەها پاراستنی وزە لە تۆڕی هەستەوەری بێ تەلدا زۆر گرنگە چونکە سەرچاوەی سەرەکی هێز بۆ گرێ هەستەوەرەکان پاترییە کە وزەیەکی سنووردارە. ناتوانرێت بە ئاسانی بگۆڕدرێت یان بارگاوی بکرێتەوە. بۆیە پاشەکەوتکردنی کارەبا زۆر گرنگە بۆ زیادکردنی تەمەنی گرێ هەستەوەرەکان. هێرشبەران سازش لەسەر ئەو گرێ هەستەوەرە ناوخۆییانە دەکەن کە هێرشەکانیان لێیەوە ئەنجام دەدەن. بە ناردنی زانیاری زیانبەخش، هێرشبەران لەوانەیە تەمەنی گرێ هەستەوەرەکان لە ساڵێکەوە بۆ ڕۆژێکی تر کەم بکەنەوە و کاریگەرییەکی توندیان لەسەر وزەی تۆڕی هەستەوەرەکان هەبێت. بۆیە، بڕی زیاتری وزە کە لەلایەن گرێ هەستەوەرەکانەوە بەکاردەهێنرێت لە کاتی گواستنەوەی پاکێتی نایاسایی لەلایەن هێرشبەرانەوە. تێزەکەمان پێشنیار چەندین لۆگاریتم دەکات وەک لۆگاریتمی Detect and Compare packet Nonce (DCPN) و لۆگاریتمی Packet Count Detection (PCD) لەبۆ تۆری ئامێرە وایرلێسەکان. ئەم جۆرە لۆگاریتمانە بەشێوازێکی کارامە ئەو هێرشانە دیار دەکات و جیادەکاتەوە وەک نموونەی هێرشی وۆرمهۆل و ریپلەی لە هەمان کاتدا خۆیان لە ئەگەری تێکچوونی خزمەتگوزاری وەک بەکارهێنانی وزە لە گرێ هەستەوەرەکاندا بەدوور دەگرن. ئەنجامی هاوشێوەکردنەکان(Simulation) دەریدەخەن کە میکانیزمەکەمان دەتوانێت لە تەکنیکەکانی ئێستا باشتر بێت لە ڕووی بەکارهێنانی وزە و تەمەنی گرێ هەستەوەرەکانەوە. DCNP وزە بە ڕێژەی (21.6%) لە کاتژمێرێکدا پاشەکەوت دەکات بۆ هێرشەکانی کونە کرمێک، لە کاتێکدا PCN وزە بە ڕێژەی (12%) لە

کاتژمێرێکدا پاشەکەوت دەکات بۆ هێرشەکانی دووبارەکردنەوەی، بەم شێوەیە تەمەنی گرێی هەستەوەرەکە بە ڕێژەی (19.2%) لە کاتژمێرێکدا زیاد دەکات لەکاتی بەکارهێنانی DCPN و... بە ڕێژەی (12%) لە کاتژمێرێکدا لە کاتی بەکارهێنانی PCD. لە کۆتاییدا، توێژینەوەکە هەروەها چاودێریکردنی پلەی گەرمی هەندێک لە ئامێرە هەستیارەکانی جولاو(mobile) پیشان دەدات. بە جێبەجێکردنی ئەم ئەلگۆریتمانە دەتوانرێت پلەی گەرمی هەستەوەرەکان بە ڕێژەی (1^0C- 2.5^0C) لە هەر (2.5) خولەکدا کەم بکرێتەوە.

حکومەتی هەرێمی کوردستان – عێراق
سەرۆکایەتی ئەنجومەنی وەزیران
وەزارەتی خوێندنی باڵا و توێژینەوەی زانستی
زانکۆی پۆلیتەکنیکی هەولێر
کۆلێژی تەکنیکی ئەندازیاری
بەشی ئەندازیاری سیستەمی زانیاری

ئەلگۆریتمەکانی دیاریکردنی PCD و DCPN بۆ پاراستنی WSN

تێزێکە

پێشکەشی ئەنجومەنی کۆلێژی تەکنیکی ئەندازیاری کراوە لە زانکۆی پۆلیتەکنیکی هەولێر وەکو بەشێك لە پێداویستیەکانی بەدەست هێنانی پلەی ماستەرلە ئەندازیاری سیستەمی زانیاری

لەلایەن

کوردستان ونس حەمەعلی

بەکالۆریۆس لە ئەندازیاری سیستەمی زانیاری

بەسەرپەرشتیاری

پرۆفیسۆری یاریدەدەر دکتۆر رێبین محمد سلیم کوردە

هەولێر- کوردستان

رێبەندان ٢٠٢٣