TIDS: Trust Value-Based IDS Framework for Wireless Body Area Network

Thesis submitted in fulfillment of the requirements of the degree of
Master by Research
College of Engineering and Science
Victoria University

by

Mohammad Yaghoubi

March 2023

Supervisors: Yuan Miao, Khandakar Ahmed

Victoria University, Melbourne, Australia

Intelligent Technology Innovation Lab, Victoria University, Melbourne, Australia

VICTORIA UNIVERSITY
MELBOURNE AUSTRALIA

Declaration of Authenticity

"I, Mohamad Yaghoubi, declare that the Master by Research thesis entitled TIDS: Trust Value-Based IDS Framework for Wireless Body Area Network is no more than 60,000 words in length including quotes and exclusive of tables, figures, appendices, bibliography, references, and footnotes. This thesis contains no material that has been submitted previously, in whole or in part, for the award of any other academic degree or diploma. Except where otherwise indicated, this thesis is my own work".

Signature:  Date:16 August 2022

Acknowledgements

I want to take this opportunity to express my deepest gratitude and appreciation to all the staff members and panel members, especially Dr Elmira Jamei and the research office of Victoria University. They have cooperated closely and mutually with me since the beginning of this research study to help me successfully finish this thesis.

I am pleased to express my utmost gratitude and appreciation to my supervisors, Prof. Yuan Miao and Dr Khandakar Ahmed. They shared valuable knowledge and experience they had acquired over the years. They enabled me to choose an up-to-date research topic. Moreover, their continuous suggestions and helpful guidance made this difficult path easier for me. Without the support of these two prominent academics, it would have been impossible to follow this path. Dr Khandakar's unique personality and charisma have inspired me to pursue this research study professionally and full-time with more interest. Dr Khandakar has always devoted his time to my academic progress. He has always raised my spirit to study more, and after two years, I have concluded that research helps with my mental development, which is all due to Dr Khandakar. I would also like to thank Prof Yuan for suggesting a suitable and creative model that improves the research results.

Since the beginning of this research study, I have lost some relatives and friends, including my father, grandfather, aunt and uncle, all of whom are in my mind and heart forever. Unfortunately, I could not meet them even for the last time due to the restrictions of Covid19. Here is probably a good opportunity to mention them, and I hope that one day I will be able to meet my family. I am also very grateful to my mother, who always encourages me to expand my knowledge on novel matters and serve humanity.

Abstract

This study aims to develop an Intrusion Detection System (IDS) to identify and prevent Denial of Sleep attacks (DoSL) in Wireless Body Area Networks (WBAN). In a DoSL attack, the attacker sends malicious and false information packets, keeping the sensors implanted in the patient's body active for a long time, resulting in quick battery drainage and a reduction in network efficiency. To prevent this attack (DoSL), this study employs pre-distributed random keys, random passwords, the trust value of each node, node energy consumption, the IDS, and an IDS database. The IDS plays a critical role in detecting and preventing DoSL attacks by monitoring the network traffic received and sent between nodes and analyzing data from the IDS database. Moreover, the IDS database is responsible for recording and archiving the events of the WBAN, the number of packets sent and received between nodes, and reporting the recorded information to the IDS. Based on the data from the database and continuous monitoring of the network traffic received and sent between the nodes, the mentioned IDS can detect, prevent, and remove malicious DoSL packets and nodes from the WBAN.

WBANs are an advanced technology in medical and therapeutic care where the sensors distributed on the patient's body collect and send the patient's vital information in real-time. Since sending and receiving information packets and traversing the path within the network consumes the sensors' energy, recharging the WBAN sensors is almost impractical and uneconomical. Adopting an appropriate and optimal method to reduce energy consumption and selecting efficient routing is necessary. To tackle this issue, the metaheuristic Artificial Intelligence (AI) mechanism and modified Genetic Algorithm (GA) have been used for clustering and selecting the optimal Cluster Head (CH) based on maximum residual energy and minimum distance between nodes. Furthermore, the modified Ad-hoc On-demand Distance Vector (AODV) routing protocol, which relies on demand, has been used for intra-cluster routing.

To evaluate the effectiveness of the proposed IDS in detecting and preventing attacks, we conducted simulations both with and without the presence of IDS and compared various network parameters such as throughput, network lifetime, Packet Delivery Rate (PDR), and node residual energy. We also benchmarked the proposed method against a sample case, the "Secure and energy-efficient framework

using Internet of Medical Things (IoMT) for e-healthcare (SEF-IoMT)." Our simulation results showed that the proposed method, which integrated a combination of normalization, intelligent clustering, demand-based routing, and intelligent intrusion detection, enhanced network parameters such as PDR (12%), end-to-end delay (11%), throughput (11%), and energy consumption (11%). It is worth noting that all experiments were conducted using the NS2 simulator.

Table of Contents

List of Figures

List of Tables

Acronyms

The following is the list of acronyms that are used in this thesis :

IDS	Intrusion Detection System
DoSL	Denial of Sleep Attacks
WBAN	Wireless Body Sensor Network
AI	Artificial Intelligence
GA	Genetic Algorithm
CH	Cluster Head
AODV	Ad-hoc On-demand Distance Vector
PDR	Packet Delivery Rate
IoMT	Internet of Medical Things
SEF-IoMT	Secure and energy-efficient framework using the Internet of Medical Things for e-healthcare
QoS	Quality of Service
WHO	World Health Organization
BSN	Body Sensor Network
WSN	Wireless Sensor Network
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
TDMA	Time Division Multiple Access
ECG	Electrical Activity of the Heart
RTS	Request-to-Send
CTS	Clear-to-Send
DoS	Denial of Service
AMC	Absorbing Markov Chain
HWSNET	Heterogeneous Wireless Sensor Network
SEC-TMP	Security Topology Maintenance Protocol
TMP	Topology Maintenance Protocol
ITIDS	Isolation Table Intrusion Detection System
BS	Base Station
PCH	Primary Cluster Head

SCHS	Several Secondary Cluster Headers
CARL	The Adaptive Classification Rate Limit
MDP	Markov Decision Plan
TE2S	Two-Tire Energy-Efficient Security Scheme
HPOR	Hierarchical Power Optimization Routing Protocol
HEAT	Horizontal Moveable Energy-efficient Adaptive Threshold-Based
DEAR	Energy-Aware Routing Algorithm
AP	Access Point
EERS	Energy Efficient Routing Scheme
A-MAC A	Adaptive Environment Access Control
EH-RCB	Energy Harvested-Aware Routing protocol with Clustering Approach in Body Area Network
GPS	Global Positioning System
CBR	Constant Bit Rate
IoT	Internet of Things
NS2	Simulator Version 2
TPR	True Positive Rate
FPR	False Positive Rate
TNR	True Negative Rate
FNR	False Negative Rate
EMG	Electromyography
EEG	Electroencephalography
MANET	Mobile Ad Hoc Network

CHAPTER 1 Introduction

1.1 Introduction

As an integral part of cutting-edge medical science, WBAN is an inventive type of ultra-short-range wireless networking technology whereby tiny sensors are attached to, installed in, or placed around an ailing human body to improve quality of life. With a WBAN-based e-healthcare system, patients' medical records can be automatically collected through multiple sensor nodes and accessed and handled by the local or remote medical staff via a computer network or a fixed infrastructure. As a result, patients can be discharged early from the hospital as their condition can be controlled at home. Health staff can be informed and provide remote nursing aid if a patient's condition deteriorates. WBAN facilitates real-time and consistent surveillance in various fields, including telemedicine, entertainment, sports, and military training, especially benefits for chronic diseases early detection and treatment [1]. Despite the aforementioned benefits of WBAN networks, it is worth noting that the existing connections between WBAN nodes are wireless, as a result security challenges arise for sending and receiving data. In this regard, attacks have been discovered that can reduce security in WBANs which increases energy consumption and disrupts the routing of the entire network [2]. One of the most common and important attacks is called the DoSL attack that removes the confidentiality of the data transfer between nodes [3]. This malicious attack continuously tries to keep the network awake.

In the future, with the continual development of micro-sensor technologies and moderate-power wireless networking, biomedical sensors will inevitably become smaller. However, with nanoscale nodes, resource-constrained issues could become challenging. These challenges must be addressed to be adopted in practical usage. Furthermore, it is envisioned that people will be able to wear WBAN sensors embedded in clothing and purchase directly from retailers or manufactured utilizing 3D printing, thereby achieving greater flexibility and adaptability during the development of security protocols. However, many challenges exist to accomplishing a secure, confidential, and user-friendly WBAN framework deployment process [1,4].

WBAN technology faces numerous challenges within the deployment process. Firstly, connectivity capabilities, accessible memory, and computing efficiency are constrained in WBAN nodes, primarily those inserted within the body. Each node will have a significantly lower transmission power due to its small form factor.

These considerations are designed to avoid external interference and tackle health issues. Secondly, the mobility of nodes, energy efficiency, and environmental barriers enhance dynamism in WBANs, including continuous change in topology and networking components that increase the complexity of Quality of Service (QoS). In addition, the quality of links between nodes in WBANs fluctuates as a function of time due to various physical motions. Finally, vital information can be spoofed and replicated in the interaction between sensor nodes, which may cause considerable damage as sensitive data can be used for illegal purposes [4].

DoSL is a special attack that hinders battery-powered sensor nodes from accessing sleep mode, thus disturbing network performance [5]. In this attack, the intruder node can forward fake data packets to the authorized nodes, which results in unauthorized transmissions. On receipt of the data packets, if the recipient cannot identify the source, it will handle the data obtained from the intruder. This causes the receiver node to be awake until data transmission is completed, consequently depleting the nodes' battery power. The design and implementation of technologies that protect the WBAN system against DoSL involve challenges. First, such an attack could raise sensor nodes' energy consumption by degrading patients' sleeping patterns [6]. Second, a DoSL attack could have increased influence over legitimate nodes' erroneous information by creating fake identities [6,7]. However, by defending against DoSL attacks, a trusted key server can be implemented to authenticate nodes with each other and launch a shared session key for encrypted communications. This enables each node to share a secret key with the key server to improve authentication and identify malicious nodes.

This study aims to develop an IDS to identify and prevent DoSL in WBAN. To detect and prevent DoSL attacks, this study employed pre-distributed random keys, random passwords, the trust value of each node, node energy consumption, and a database for IDS. Since sending and receiving information packets within the network consumes the energy of the sensors, adopting an appropriate and optimal method to reduce energy consumption and select efficient routing is necessary. To tackle this issue, GA has been used for choosing the optimal CH. Moreover, the AODV routing protocol has been used for intra-cluster routing. In this research, an attack has been simulated to the WBAN once in the presence of IDS and once in its absence. Afterwards, to verify the efficiency and effectiveness of IDS in each simulation, various network parameters such as: throughput, network lifetime,

Packet PDR, and node's residual energy have been investigated and compared in both methods. The network parameters of the proposed method have once again been compared and benchmarked with a sample case "Secure and energy-efficient framework using Internet of Medical Things (IoMT) for e-healthcare (SEF-IoMT)". The simulation results and their comparison with the proposed benchmark method showed that it had significantly improved the network parameters. It should be noted that all tests and experiments were conducted by the NS2 simulator[8].

1.2 Background

World Health Organization (WHO) estimates cardiovascular disorders have been the number one cause of death worldwide, culminating in 17.9 million deaths annually [9]. In Australia, cerebrovascular disorder, lung cancer, and chronic obstructive pulmonary disease are the top five major underlying causes of death for men and women of all ages. This rise will likely overwhelm healthcare services, severely affecting the quality of life [10]. Studies have demonstrated that certain illnesses are preventable if diagnosed early. Hence, healthcare programs in the future should enhance effective well-being management and focus on detecting and avoiding diseases early on. One conventional approach for more affordable and preemptive healthcare services is through wearable illness-tracking systems efficient in the early diagnosis of abnormal symptoms leading to significant changes in the quality of life [11].

WBAN is a recent technological development providing remote medical data access through body-worn sensors. It is immensely acknowledged that a substantial degree of device protection and privacy is crucial in providing safety for the data utilized by healthcare practitioners and stored to assure that patients' medical information is secure from intruders. WBAN nodes are often susceptible to external attacks and intrusions, resulting in a patient's life loss [12].

Due to the vulnerabilities of sensors, WBAN nodes are open to a large variety of invasions. One significant attack menacing WBAN is the DoSL attack. DoSL attacks influence energy depletion patterns in WBAN sensors by keeping nodes active and preventing them from going into energy-saving mode. DoSL withholds the radio

from going into sleep mode to exhaust the battery fully. In normal circumstances, the energy of the sensors can hold for months, whereas the DoSL empties the battery in a few days by keeping the radio transmitter on [13].

This research study included several stages to identify and tackle DoSL attacks in WBAN. Firstly, network clustering was set up with the help of GA, and intra-clustering routing was implemented with the AODV routing protocol. Then, the IDS agent was designed to detect DoSL attacks by consistently monitoring the WBAN. Finally, the network is simulated in two scenarios: one with IDS and one without IDS. The obtained results were analyzed and compared based on the mentioned network parameters to prove the proposed method is effective.

In this research study, NS2 was used to test and compare the results of the proposed method. The results were demonstrated on a graph based on network parameters such as throughput, network lifetime, PDR, and the residual energy of each node.

1.3 Overall Aim and Motivation

As mentioned above, cardiovascular disorders have been the leading cause of death worldwide, especially in Australia. Australian Government is allocating one strong health care record of $132 billion in 2022-23, and this budget is predicted to be increased to $140 billion in 2025-26. These statistics and numbers threaten each society and country[9,10].

WBANs are a particular type of sensor network using wireless sensor nodes on a person's body to measure physiological parameters such as blood pressure, body temperature, heart rate, and blood sugar level, enabling a patient's health to be monitored remotely. WBANs can be either wearable or implantable. The primary purpose of WBANs is to ensure people's health by sending physiological information to medical servers using sensors on the body to enable physicians to understand the patient's health [1]. These systems can assist the medical board and individuals in emergencies by providing services such as monitoring and delivering pharmaceutical and medical information, improving patient processing data, controlling home appliances, and communicating data. WBANs can also significantly reduce patient treatment costs by monitoring the patient's vital sign-related data over a long period. However, These sensor nodes in the network have access to limited energy resources. In

physical sensor networks, sensors (like motion sensors) are installed on a patient's body to observe the patient's vital signs or detect motion. By monitoring a patient's vital signs, the body sensor network provides an instant response to the user through which the user can follow the progression of a patient's disease and take the necessary precautions. In this type of network, the energy utilization of the sensors is critical because if the energy source is exhausted, the life duration of the network will be shortened [1,2].

Denial of sleep (DoSL) is the malign attack against WBAN, which drains sensors' batteries by holding them in an active state for an extended period. The main aim of this study was to create an efficient and robust system to satisfy the security of WBAN. Specifically, in this study, we sought to develop a DoSL attack detection system to prevent sensor nodes from going into sleep mode, which per se had a detrimental effect on network performance and energy consumption. Therefore, by implementing and adopting this protection approach, it was expected that the applied security framework could respond well to DoSL attacks by isolating and eliminating DoSL attackers. To devise this security system in this research study, one IDS has been designed to monitor the behaviour of nodes and packets in WBAN constantly. These IDS overcame depleted battery issues due to the DoSL attack. Several components like pre-distribution key, random password (Event-ID), and path trust value were employed for escalating the security system. Moreover, in this research study, we aimed to utilise GA for intelligent clustering and AODV for routing inside the WBAN. Furthermore, network simulation was performed by NS2 simulator software.

1.4 Research Questions

This research study aimed to create one novel security system and implement a metaheuristic algorithm to develop a predictive security model to assess whether it would assist in identifying intense DoSL attacks and preventing inappropriate, malicious DoSL traffic. To this end, the research questions below are aimed to be answered :

1. How to design an IDS agent to identify DoSL attacks to optimize energy consumption and ensure network security?

2. To accelerate the routing operation, what parameters must be used to estimate the amount of path trust value?

3. How can the obtained heterogeneous parameters be compared to calculate the path trust value?

By addressing these questions, it was possible to explore whether the proposed security system could be a practical model to identify a DoSL attack and justify the plausible benefits and threats.

1.5 Contribution

This research includes a comprehensive and integrated system of four phases: normalization, intelligent clustering, routing and security to maximize the protection of the WBAN against DoSL attacks and improve the energy consumption pattern among the WBAN nodes. The contribution of this research study is summarized below:

• Identification of WBAN routes that have the highest trust value. Max/Min normalization technique is used to calculate the trust value of the path. In this method, the trial-and-error method was used to collect AODV PDR and RREP packets and place them as input values. Then the range of 0.98 to 1 has been used as the reliable path. In the following, these trusted routes are being utilized by the AODV routing protocol, so that routing can be done faster and more reliably. By identifying the alternative trust path routes, it has become possible, in addition to the best course with the most trust value, to always have secondary and alternative routes to keep routing, sending and receiving information with minimal loss of time and delay in case of intra-network routing problems. Paths outside the 0.98-1 range are selected as alternative trust paths in normalization and are manually and statically placed in the AODV routing table.

• To reduce energy consumption and increase fast decisions in routing, a lightweight routing protocol like AODV has been used. This protocol can quickly detect and recover the broken path, which improves the time of sending information and reduces the delay of sending and receiving body information. Furthermore, the integration of this protocol with the normalization method has helped improve and increase routing reliability.

• Intelligent clustering: Unlike traditional methods, a genetic artificial intelligence algorithm has been used to select the CH to reduce network energy consumption and increase security and optimal routing. Max residual energy and min distance parameters of nodes are used as input to find the optimal CH in the genetic algorithm.

• To detect and prevent DoSL attacks, this study used pre-distributed random keys, random passwords, the trust value of each node, node energy consumption and a database for IDS. This database is responsible for recording and archiving WBAN events, the number of packets sent and received between nodes, the mechanisms used on sensors distributed on the body, and finally, reporting the recorded information to the IDS. Based on the data from the database and continuous monitoring of the network traffic received and sent between the nodes, the mentioned IDS can identify, prevent and remove malicious DoSL packets and nodes from the WBAN. To increase quick decision-making capability and reduce possible decision-making errors, a unique table has been considered for each CH, BS, and IDS.

• To collect and analyze information through the NS2 simulator, five-time intervals of 100, 150, 200, 250, and 300 seconds were considered. The network's important and sensitive parameters were tested ten times in each execution, once with the IDS and once without the IDS. Finally, we witnessed progress in PDR, throughput, delay, and energy consumption parameters by comparing the benchmark with a sample model.

1.6 Statement of Significance

W.H.O reported that heart stroke, cerebrovascular disorder, lung cancer, and chronic obstructive pulmonary disease are the primary cause of death in Australia [9,10]. The cerebrovascular disorder is now the leading cause of death universally. It is predicted that healthcare expenditure will reach 20% of the U.S Gross Domestic Product (GDP) by 2022, threatening the U.S economy [14]. Moreover, Australia's growing world population and increasing life expectancy increase the healthcare cost [15].

WBAN networking is an emerging technology addressing critical medical research and technology issues that reduce healthcare costs. This network is an accumulation of large sensor nodes scattered and mounted in an environment such as the human body. The most important part of this network is the safe monitoring of patient's

medical conditions, such as vital signs (fever, heartbeat, etc.). Establishing security in this network is the primary concern, owing to the high importance of the body's vital signs.

One of the most significant challenges in such a network is setting up security. The most significant threat against this network is the potential breach of patient privacy and the increasing energy consumption of the monitoring sensors. DoSL is one of the most notorious attacks against this network, causing energy consumption to rise. This attack shortens the network's life and eliminates the patients from the monitoring tracking system.

In clinical hospitals, monitoring the patient's health and periodically reporting the patient's condition to the relevant doctors are of great importance. In developed medical societies (The US, Canada, Australia, etc.), this network's security and energy consumption have recently drawn the researchers' attention to monitoring an individual's body, enabling the medical associations to predict, diagnose and respond effectively to various conditions on time. In such cases, the higher the network's energy consumption, the shorter the network's lifespan will be [14].

By continuously sending direct or indirect unnecessary packets to the network's nodes, the DoSL attacker awakens the sensors, eventually leading to battery drain and a shorter lifespan. It can be concluded that DoSL attacks pose a severe threat to WBAN networks.

The security issues, health programs, and medical services for the patients were explored in this section. To deploy a security framework in this project, an IDS Agent needed to be designed to reduce energy consumption and increase the network lifespan. This system attempted to detect the DoSL infiltration using pre-distribution keys, random password generation, path trust value calculation, and specific CH, BS and IDS databases.

1.7 List of Publications

1. M. Yaghoubi, K. Ahmed, and Y. Miao, “Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges,” *Journal of Sensor and Actuator Networks*, vol. 11, no. 4, p. 67, Oct. 2022, DOI: 10.3390/jsan11040067.
2. M. Yaghoubi, K. Ahmed and Y. Miao, "TIDS: Trust Value-Based IDS Framework for Wireless Body Area Network," *2022 32nd International Telecommunication Networks and Applications Conference (ITNAC)*, Wellington, New Zealand, 2022, pp. 142-148, doi: 10.1109/ITNAC55475.2022.9998329.

1.8 Thesis Composition

The rest of this thesis includes the following chapters:

Chapter 2: This chapter reviews the literature and techniques necessary to implement a safe and efficient system to reduce energy consumption and increase human body sensor networks' security system. It presents the methods of estimating the trust level of a path along with optimal routing. Moreover, the literature on network clustering and partitioning methods, which are necessary for selecting the optimal CH , have been examined. In addition, different types of attacks, especially DoSL, and how to reduce the effects of such attacks on the human body using IDS are investigated. Finally, relevant studies and literature are mentioned for comparing and choosing the benchmark model. The literature review shows that, as far as we know, the simultaneous and integrated use between high-reliability route selection, lightweight and low-energy routing, optimal CH selection, and the use of IDS has not been found in the existing literature.

Chapter 3:This chapter seeks to answer the research study's first question: "How to design an IDS agent to identify DoSL attacks to optimize energy consumption and ensure network security?" In short, the WBAN technology has been introduced along with its essential features. Then, considering the IEEE 802.15 standard, the application requirements and structure of the WBAN are proposed. The ways this technology can help humans, patients and older people have been investigated from physical and psychological aspects. Furthermore, the components and belongings of the WBAN have been examined along with the challenges and limitations. Security

and amnesty restrictions have been given more attention and emphasis among all the limits and challenges. A table has been compiled for comparison, which contains the necessary information to compare the limitations and challenges between the WBAN and WSN. The architecture of information transfer between WBAN layers and different physical sensors has been explained and discussed. In the final part of this chapter, to complete and clarify topics such as the causes of energy wastage and consumption, factors that increase energy consumption among network sensors, categorization and classification of attacks, metaheuristic security techniques with the help of artificial intelligence algorithms for balance between maximizing security and reducing energy consumption have been mentioned. Finally, the design and implementation of IDS have been made possible with the information obtained from this chapter and considering the security specifications in WBAN.

Chapter 4: This chapter is based on methodology and benchmarks in detail. At first, the problems in the WBAN were introduced, and then, the flowchart related to GA and IDS was designed by taking into account the scientific approach model and conceptual design. In the IDS flowchart, the different phases of normalization, clustering, routing and security are shown along with the relationships between them. In addition, tables and databases related to ids, BS, along with detailed information are displayed in each column. The formulas used to calculate and estimate the important and sensitive parameters of the network have also been examined in this chapter. In the end, the methods related to data collection and information analysis for the NS2 simulator are explained.

Chapter 5: This chapter generally deals with the simulation of the presented methodology along with the calculation, collection and analysis of information with the help of the NS2 simulator. After introducing TCL and C++ programming language, the simulation parameters were recorded as input. In this method, in 5 rounds with time intervals of 50, 100, 150, 200, and 250 seconds, each round was simulated for 10 times. Next, after choosing a sample pattern for the simulator benchmark, simulation was done 10 times in 5 rounds in time intervals of 50, 100, 150, 200 and 250 seconds. In the end, by comparing the results obtained in the methodology and benchmarking, we were able to achieve a significant improvement in the network parameters.

Chapter 6: This chapter draws a conclusion based on the results obtained from the simulation and comparison of network parameters, including Delay, Throughput, PDR, Energy consumption and the analysis of the resulting graphs. The conclusion included the reduction of energy consumption and time delay along with increased throughput and PDR.

VICTORIA UNIVERSITY

THE NEW WAY TO DO UNI

OFFICE FOR RESEACH TRAINING ,QUALITY AND INTEGRITY

DECLARATION OF CO-AUTHORSHIP AND CO-CONTRIBUTION: PAPERS INCORPORATED IN THESIS

This declaration is to be completed for each conjointly authored publication and placed at the beginning of the thesis chapter in which the publication appears.

1. PUBLICATION DETAILS (to be completed by the candidate)

Title of Paper/Journal/Book:	Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges," Journal of Sensor and Actuator Networks, vol. 11, no. 4, p. 67, Oct. 2022, DOI: 10.3390/jsan11040067.
Surname:	Yaghoubi
First name:	Moha[redacted]
Institute:	Institute for Sustainable Industries and Liveab
Candidate's Contribution (%):	70%
Status:	
Accepted and in press:	☐
Date:	[redacted]
Published:	✔
Date :	Oct 2022

2. CANDIDATE DECLARATION

I declare that the publication above meets the requirements to be included in the thesis as outlined

In the HDR Policy and related Procedures – policy.vu.edu.au.

MOHAMMAD YAGHOUBI Digitally signed by MOHAMMAD YAGHOUBI	14 Nov 2022
Signature	**Date**

3. CO-AUTHOR(S) DECLARATION

In the case of the above publication, the following authors contributed to the work as follows:

The undersigned certify that:

1. They meet criteria for authorship in that they have participated in the conception, execution or interpretation of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;

3. There are no other authors of the publication according to these criteria;
4. Potential conflicts of interest have been disclosed to a) granting bodies, b) the editor or publisher of journals or other publications, and c) the head of the responsible academic unit; and
5. The original data will be held for at least five years from the date indicated below and is stored at the following **location**(**s**):

Name(s) of Co-Author(s)	Contribution (%)	Nature of Contribution	Signature	Date
Mohammad Yaghoubi	70%	Concept, Methodology, Experiment, Result Processing Draft	[redacted]	11/11/22
Khandakar Ahmed	20%	Concept, Validation, Review, Proof Read	[redacted]	15/11/2022
Yuan Miao	10%	Review, Proof Read	[redacted]	14/11/22

Chapter 2 Literature Review

2.1 Introduction

Wireless Body Area Network (WBAN) is a special wireless sensor network that measures the biological parameters of a person by using wireless sensor nodes in the body area, enabling remote monitoring of the patient's health. Energy management and energy efficiency in the body sensor networks are two of the main challenges. Wireless networks on the surface of the body have made it possible to continuously monitor the health of patients outside the hospital. Several sensors are placed in the body that can measure heart rate, determine blood sugar levels and check vital medical data. The collected data in these sensors are sent to the medical care center via mobile phones or other portable devices, and in case of a critical situation, the necessary decisions are made by the specialized physicians and the necessary measures are taken [1].

One of the challenges of the WBAN is the limited energy of the body sensor nodes, which is generated from very low-power batteries. Increasing the battery power leads to an increase in the weight and size of the sensor nodes, which contradicts the lightness and portability ease of the sensors considered in the physicality of wireless sensor networks. One of the methods to reduce energy consumption that has been proposed in wireless sensor networks is how to cover the sensor nodes and communicate with the sink node [2]. Therefore, we must look for methods that can increase the short life of the network due to the limited energy of the sensor nodes. Unlike wireless sensor networks, the body sensor networks use a star topology architecture. In this topology, an access point (sink hole) is located in the body to collect data from the nodes. The sensor nodes in the WBANs are limited in energy resources, and the energy consumption of the sensors is very important, and if the energy source of the sensors is exhausted, the life duration of the network will be shortened over time. Therefore, among the issues discussed is the reduction of energy consumption in wireless networks of the body, the major part is in receiving data through sensors and transmitter and receiver units. Therefore, according to the above-mentioned facts, one of the most important issues in the wireless body area networks is to increase the lifespan of these networks. Consequently, in order to achieve this goal, most research and articles in recent years have discussed reducing energy consumption. In some of these algorithms, the only goal is to reduce energy consumption. In addition to reducing energy consumption, some others have considered other criteria such as increasing or decreasing the

communications, package delivery rate, etc. which have proved to be good algorithms. However, there is still a need for algorithms that can provide a good response in an acceptable time, i.e., high throughput.

The leading cause of death in the world is cardiovascular disease, which accounts for about 30% of all global mortality. Millions of people die each year from heart attacks or strokes, according to the World Health Organization. These deaths can often be prevented with proper prevention through medical care and lifestyle changes. Millions of people around the world suffer from diabetes. Frequent monitoring can control the appropriate dose, reduce the risk of fainting, and loss of blood circulation, and other complications in these patients. The need for remote care in some outpatients demonstrates the importance of continuous and beneficial monitoring of disease. Examples of such are continuous or long-term monitoring of high blood pressure, asthma, Alzheimer's, Parkinson's, postoperative monitoring, stress monitoring, and so on [16].

Recent advances in wireless electronics and telecommunications have provided the ability to design and manufacture sensors with low-power consumption, small size, reasonable price, and versatility. These small sensors, which are capable to perform functions such as receiving, limiting processing, and transmitting information, have given rise to the idea of creating and expanding networks called wireless sensor networks. One of the interesting applications of these networks is in controlling and improving the health status of all people, especially the elderly, patients, and children. The Body Sensor Network (BSN) is a special-purpose wireless sensor network that uses wireless sensor nodes around a person's body to measure their biological parameters and enable their health to be monitored remotely. The main purpose of physical sensor networks is to transmit the user's health condition to the person, hospital, or specialist doctor immediately without causing any inconvenience to the person. Bandwidth, computing power, telecommunication power, power consumption, scalability, limited processing, and limited computing are among the challenges of physical sensor networks. This is one of the most important research topics in physical sensor networks, as most of these challenges are due to power constraints, and energy efficiency optimization determines the life of the network in question.

Since WBANs monitor the health of people and patients, the security of data transmission between WBAN nodes and patients is of extreme importance [17]. Therefore, if security is not established in this network, there will be technical and security problems such as security risks, lack of confidentiality, lack of integrity, and excessive increase in energy consumption. Hence, the mentioned network becomes insecure and unstable. This problem is regarded as one of the technical and security issues that must be resolved and accounted for in the design of WBAN [18] .In this section, several methods that have been proposed by researchers to solve security problems in WBAN-based networks have been analyzed.

2.2 Literature Review

This proposed research was a hybrid type of experiment that was conducted around the AI metaheuristic world. This research emphasized the practical security solution for the WBAN network with the aid of AI. However, the current research study reached beyond the most approaches that were traditionally carried out by investigating the possibility of detecting abnormalities and preventive actions. The advantage of this study fell upon increasing the network performance by optimizing energy consumption.

Below were the four latest relevant papers that we addressed in order to specify the gaps and to Justify the current research position:

Concerning paper 1: "An Intrusion Detection System for the Internet of Medical Things." This study proposed an innovative wireless IDS agent that protected the topology of interconnected biomedical devices. Specifically, the proposed scheme was hierarchical, autonomous, and used a regression algorithm that automatically detected system-level flaws as well as irregularities in wearable sensors. This simulation indicated a rising precision in detecting the invasions with a limited overhead by modeling a medical network framework and conducting thorough experiments on simulated areas of the internet of medical things [19].

In the detective agent phase, data collection occurred solely on each node; however, operational detection took place with CH elected by a traditional clustering algorithm. CH was responsible for close monitoring of sensor nodes throughout the sensor groups in each cluster. CH Agent performs anomaly detection at periodic intervals.

The consequence was that by selecting the appropriate CH, the network's energy consumption improved. Researchers evaluated a total of 72 separate simulation testes with approximate maximum and minimum case identification accuracy of 99.9% and 92.91%, respectively.

Even though the CH idea was promising, applying the traditional approaches and increasing the network devices could significantly affect reliability. The comparison between the current study and paper 1 showed that the resemblance was the soul of the CH approach. Nevertheless, applying an AI algorithm to glean data led to an optimized approach for selecting the most qualified node as CH and resulted in developing a structure-based database for the IDS agent.

The following is a summary of the similarities and limitations between "Paper 1" and our current research study.

Similarities :

• Utilized the IDS system.

• Implemented clustering and proper CH selection .

• Both studied were able to detect DoSL attacks.

• Involved the implantation of sensor agent.

• Provided a proposed algorithm for reducing energy consumption and enhancing security.

However, we have also identified the following limitations in "Paper 1":

• Involved high time complexity.

• Increased processing time .

• Increased end-to-end delay time.

• Increased overhead control .

Concerning Paper 2: “A Hybrid Trust-Based Intrusion Detection System for Wireless Sensor Networks". Identifying malignant nodes and isolating them in Wireless Sensor Networks (WSNs) was a crucial task to carry out. Because of limited resources of sensor nodes, traditional approaches of security such as authentication and encryption could not be useful for WSNs today. In this article, an IDS agent was proposed along with a clustering system. The main goal of the study was to have each sensor calculate their neighbor node’s trust value, and CHs send the trust value to the BS.

The article’s proposed method was similar to ours in several ways:

- Both methods attempted to calculate the trust value.
- Both methods attempted to segment the network with hierarchical technique.
- Both methods aimed to detect the intruder node by calculating the trust value and each CH.
- In both methods, the IDS agent operated based on the trust value.
- Both methods consider two simulation scenarios: one with IDS and another without IDS.

The method employed in the article came with some calculation complexity which affects the results. In such cases, using simpler methods can be crucial since it helps with better service quality and higher network efficiency. Our proposed method was simpler with less complicated calculation in comparison with the article’s method as there was no need to calculate the trust value for every CH. In our method, path and alternative path trust value were utilized. The article proposed a method requiring sending the trust value to the BS; however, in our proposed method, the identity information was sent to the BS only on special occasions [20].

Concerning paper 3: “Intrusion Detection System Based on Trust Value in Wireless Sensor Networks". In this study, by relying on security methods to preventing sinkhole, Sybil, jamming, wormhole, blackhole, etc. In the proposed method, the trust value was calculated dynamically by the monitoring node. If the value was less than the threshold, the node is considered an attacker.

As the article was explored, we realized that this article had some similarities in methodology. Moreover, this article was identical to ours regarding the results (presented metrics). Also, both articles used NS2 simulator software. The significant similarities were as the following [21]:

- Both attempted to identify attacker node,
- both studied identify trust value,
- trust value was calculated based on the number of successfully transmitted packets,
- in both, increasing packet delivery rate and throughput were the main metrics in service quality.

As the article was investigated, there were some gaps compared to our method, and filling these gaps could help improve the proposed method leading to better results. The gaps were as the following:

- selection of a monitoring node for calculating the trust value of neighbor nodes (introduction of monitoring node in the article),
- calculation of path trust value in cases of packet loss (considering path trust value calculation in cases of packet loss),
- selection of an alternative path when there was a path with a trust value lower than the threshold.

The mentioned factors could cause more energy consumption and less network lifetime due to high computational complexity compared to our methodology.

Concerning paper 4: In the paper titled "Trust-Based Data Communication in Wireless Body Area Network for Healthcare Applications," researchers [22] sought to improve the security of WBAN communications for healthcare applications. They proposed a secure communication protocol based on a multi-layered trust model to improve sensor node communication. Simulation tests demonstrated the effectiveness of the proposed protocol in ensuring secure and reliable communication in WBAN healthcare applications. Overall, the paper contributes to the development of safer and more efficient WBAN communication techniques in healthcare settings. Studying the paper, we could notice the similarities and limitations of this article to our proposed method as below:

Similarities :

• Considering network trust

• Calculation of node trust

• Using the clustering model

• Providing simulation results of important network metrics such as PDR, Delay, Throughput

Limitations:

• Traditional and elementary leach-based clustering

• Implementation of the complexity of calculation formulas

• High computational overhead

• Failure to address routing weaknesses

In conclusion, the aforementioned limitations had an impact on the overall network lifespan and performance of the entire WBAN network.

2.3 Security Attacks and Current Solutions

A number of studies on privacy attacks show that patients' private and sensitive medical information can be exposed to unauthorized persons through simple eavesdropping [23,24]. Kumar et al. Investigated attacks that threaten the integrity of patient's data by tracking physiological data and subsequently altering them to create errors in diagnostic inferences [25]. This type of security attack has serious consequences since misdiagnosis can lead to physical injury or death in severe cases. Researchers have also shown that routing attacks on WBANs, such as selective attacks, submergence, and sybils, can potentially compromise medical information on the way to the destination (gateway device, cloud, hospital server, etc.) [26,27] . Aggressive nodes can remove important information from being reached to the destination or absorb all the data for selfish reasons.

Several solutions have been proposed to address the above security concerns in smart medical networks [28,29]. The IEEE 802.15.6 standard for WBAN provides a pre-installed encryption security system with options for authentication and privacy. However, the inherent encryption protocol still has design flaws that reveal other vulnerabilities [30]. A number of other encryption security measures have been proposed for the efficient management of keys and encrypted communications in connected healthcare networks [31]. Other security solutions consider trust-based mechanisms to assess the trust of each node in the network [32,33]. Several physical layer security solutions such as artificial noise injection, anti-eavesdropping signal design and co-based secure transmission techniques have also been developed to secure wireless communications [34,35]. Unlike traditional encryption approaches, physical layer security solutions take advantage of the inherent features of wireless channels to achieve secure keyless transmission through signal design and signal processing. Soderi et al. Proposed a new transceiver architecture design to secure wireless communications using a jamming receiver with a wide-range signaling method [36]. The authors show that their solution challenges eavesdropping and achieves greater secrecy capacity. However, wide-range-based schemes suffer from distribution challenges and code management challenges. Cipriani et al. Proposed a solution using noise as a data carrier that provides a secure channel for wireless systems without any prior knowledge between source and destination [37]. Artificial Noise (AN) injection is an effective means of creating a channel quality advantage for legal transmission links. However, most of these designs rely on the deployment of multiple antennas in the transmitter, which is a challenge in low-cost and resource-limited WBAN devices.

Intrusion Detection Systems (IDS) are a common security control to monitor network / system traffic and detect suspicious anomalies and behaviors. While IDS solutions are well-developed for wireless body networks, these security measures are limited to parts of WBAN networks, and especially to IoT-connected healthcare systems. In [33, 37], researchers performed experiments on intrusion detection in previous WBAN implementations based on the IEEE 802.15.4 standard . The authors designed a system to evaluate node communication patterns and a blacklist of those that are malicious. In [28], an intrusion detection system was developed using genetic algorithms to detect deviations in device activities in the context of WBAN networks.

In [38], the authors proposed a relatively versatile protocol that includes a static factor per host that performs three different sub-factors to analyze access, privilege use, and network access respectively, while this is the system and the only breaking point at the management level is a significant drawback for this method. This protocol is also designed for traditional systems with user ratings and privileges that are different from sensors on the patient.

The paper [39] presents an intrusion detection system based on hybrid trust for wireless sensor networks for the detection of malignant nodes and their isolation in wireless sensor networks (WSN). Due to the limited resources of sensor nodes, traditional security approaches cannot be useful for WSNs compared to modern authentication and encryption. In this paper, an IDS agent is proposed along with a clustering system. The main purpose of the study is for each sensor to calculate the trust value of its neighbor node and the CHs to send the trust value to BS.

This paper [8] is about providing a secure and efficient IoMT framework for e-healthcare (SEF-IoMT) with the primary goal of reducing communication burden and energy consumption among biosensors during healthcare data transfer. On the other hand, medical data protects patients against invalid and malicious nodes in order to improve privacy and network integrity. One of the challenges this paper mentioned concerns the destructive nodes.

The main goal of the DoSL attack is to disrupt the WBAN network and reduce its remaining energy. In the papers [40-42], authors have divided DoSL-based attacks into two categories: those at the node level and those at the WBAN level. In DoSL attacks at the node level, the attacker targets individual devices and nodes in the network, keeping them permanently active. In contrast, in DoSL attacks at the network level, the attacker aims to disrupt communications between nodes and devices, effectively disrupting the entire network. The authors suggest the use of energy-efficient communication protocols and the implementation of security mechanisms to mitigate the impact of DoSL attacks.

2.4 Overview Of Benchmarking

The Wireless Sensor Network (WSN) also called sensor nodes consists of various sensor stations which are scattered in the observation area to sense the data [43-46]. All nodes are autonomous and operate independently and temporarily at nominal cost. Further data analysis is routed to the Base Station (BS) of sink node through a CH or local controller [47-49]. WSN is useful for many applications such as healthcare, military, agriculture, industry, smart vehicles, natural disasters, security, surveillance, energy, transmission and processing power etc. [50,51]. The WBAN is a subset of the WSN and can be used to determine the condition of the human body. Medical professionals obtained the required information from BS by using the Internet to monitor the patient's health status continuously. In healthcare programs, various biosensor nodes are attached to garment or even implanted inside the human body to sense the activity of different parts.

The concept of WBAN was first introduced by Van Dam.K [52] and other researchers showed interest later. Similar to WSN and WBAN, Mobile Ad Hoc Network (MANET) has limitations in terms of energy, processing, computing, heterogeneity, and storage . These biosensors are used to determine the condition of different parts of the patient's body such as temperature, Electrocardiography (ECG) , blood pressure, heart rate, movements, and Electroencephalography (EEG). The body sends the central coordinator of healthcare information to the BS through intermediate devices. Then, medical professionals obtain the required data from the BS by using the Internet for appropriate tests and studies. Accordingly, the physician can suggest appropriate medications to the patient or take immediate action whenever the sensor detects a problem. WBAN architecture can be divided into three layers: Intra WBAN, Inter WBAN and Beyond WBAN. In Intra WBAN, biosensors are placed inside the human body or on the surface to detect different parts of the body and transmit the received information to a local coordinator. The local coordinator is usually a personal server and is considered as a gateway that interacts with another level. In Inter WBANs, local coordinators or sink nodes process and collect the received data and send it to the BS through various access points (APs). Finally, in Beyond WBANs, data are transmitted to medical centers mostly from the BS to store the patient history on various database servers. In the third stage, the physician can receive the patient data remotely and perform the treatment on an emergency basis [53] .

WBAN domain is inherited from WSN technologies. So, implanted biosensor nodes require long-term battery power to function properly and process healthcare data like WSN. Low-power consumption, low latency, secure data aggregation, and QoS-aware transmissions are the main requirements of WBAN. The energy of biosensors is depleted during measurement, processing and transfer operations, and it is not possible to change or recharge the battery source during operation; So, improving energy consumption among biosensors without affecting the delivery ratio in healthcare applications is one of the cases. In addition, the patient's sensitive data is transmitted through the insecure Internet. An unauthorized user can manipulate healthcare measurements. Thus, data security and integrity are another major research interest for the WBAN [54] .

Therefore, the aim of this article is to provide a safe and efficient framework by using IoMT for digital healthcare applications to reduce the over-energy consumption of biosensor nodes and to obtain data quickly. The proposed data collection and routing strategy is based on artificial intelligence methods to bear the lowest costs of communication and transmission. The proposed framework for digital healthcare programs using IoMT is to provide secure, energy-aware conversation algorithms to identify patients' initial pre-care information. The proposed framework facilitates digital healthcare-related applications for intelligent analysis of patients' data. Hence, medical experts provide possible timely treatment. The proposed framework integrates artificial intelligence techniques with biosensors for automated analysis of patients' data and achieves results with minimal computational and communication costs. Given this, digital health-related applications have a broad capability to enhance medical achievements in terms of analysis and treatment recommendations. In addition, the proposed framework provides secure and authentic methods in order to prevent privacy breaches and information integrity for digital healthcare applications.

The proposed framework contributions using IoMT Primary Health Care are based on the three layers outlined below:

First, the IoMT parts are connected to each other in a complete diagram, so that there must be a unique edge, and numerical weights are assigned to each edge using a combination of factors.

Second, using the Kruskal algorithm, the subgraphs are extracted by evaluating the minimum cost and optimizing the routing decision from IoMT sensors to medical centers with the least network burden and energy consumption.

Finally, important and sensitive medical information of patients through the Internet is protected against malicious and potential threats based on light cryptographic methods. The proposed framework provides a reliable and credible mechanism for routing patient healthcare information and ensures its integrity for patients' data by avoiding dangerous damages.

WBAN routing protocols can be divided into temperature-aware, QoS-aware, cluster-based, and multilayer categories. In the QoS-aware routing protocol, various gauges are provided for data transmission. In cluster-based solutions, the network is divided into clusters with a CH inside each cluster, and the connection to the BS can be single-hop or multi-hop. The goal of temperature-aware routing protocols is to reduce the temperature rise of sensor nodes while achieving balanced energy consumption and efficient routing decision-making. In multi-layer routing solutions, protocols work on different layers to share network information, and the optimal path is selected based on different network parameters [55] .

In this article [56], the authors proposed a self-organizing protocol (ANY-BODY) for the WBAN, which aims to split the sensors into clusters. As a result, the data packets are transferred from the clusters to the sink node. The proposed protocol uses single-hop instead of multi-hop communication and sends data packets directly from the CHs to the sink node. The proposed solution improves network performance compared to the traditional LEACH protocol [57] and reduces energy consumption among sensors. In this article [58] it also shows that network reliability and energy efficiency are the main research needs in the WBAN for exact monitoring of patient's health. They highlight the problem of multi-hop during data collection from the patient's body, and uneven energy consumption occurs among WBAN sensors due to the traffic issue. They proposed the tree-based Energy Efficient Routing Scheme (EERS) to achieve multi-jump routing with low burden. In addition, the proposed solution

suggests an all-around routing approach in an energy-efficient manner with adaptive transmission power of WBAN sensors .

In this article [59] , the researchers suggested a proposed protocol in iM-SIMPLE, which aims to provide a reliable and efficient routing protocol. Experimental results show that the proposed solution increases network power and reduces energy consumption among sensor nodes [60]. The cost function is selected using the residual energy and the distance to the sink and the data are also selected using the minimum cost. In addition, energy consumption and network output are formulated by using an integer linear program.

The researchers in [61] proposed the Adaptive Environment Access Control (A-MAC) protocol for the WBAN based on linear programming, which aims to reduce power consumption and increase data flow. In the proposed protocol, the sensors continuously monitor different parts of the human body and provide up-to-date information. If the current value is within the normal range, the proposed solution indicates that no channel access is required. However, if the flow value exceeds the permitted range, the sensors turn on their transmitter and receiver and gain access to the channels. The simulated results show that the proposed protocol improves the lifespan and throughput of the network compared to the existing work .

The authors in [62] also proposed an Energy Efficient Routing Protocol (EERP) for WBAN, which aims to provide an efficient and reliable solution for power consumption and network stability. In the proposed solution, the cost-based function is used through the usage of two different parameters. It also reduces the communication distance for sending data using multi-hop data transfer. Simulation experiments show better results than other solutions. In one article, the authors proposed an efficient, cost-effective, low-consumed routing protocol for the WBAN that aims to increase energy efficiency and reliability. The proposed solution uses a GA and an optimal cost function based on residual energy, bond reliability, and path loss factors. Accordingly, the optimized path is used to transfer data from body coordinators to the sink node. In addition, the proposed solution uses multi-hop routing and reduces the communication distance between the sensor nodes. Simulation experiments have improved performance compared to the existing work .

In an article [63], the researchers proposed a robust and efficient Energy Harvested-aware Routing protocol with Clustering approach in Body area networks (EH-RCB) for the WBAN. The proposed solution stabilized the WBAN operation due to the selection of the best sender nodes. The forward node is selected using the cost function, which consists of the signal-to-noise ratio, transmission power, distance between nodes, and the sum of available energy factors. The simulated results show the improvement of network performance in terms of different performance indexes compared to existing studies .

2.4.1 The Proposed IoMT Method

Healthcare of this section provides a detailed discussion of the proposed framework designed and developed for medical applications. The proposed framework improves energy consumption among biosensors and increases the level of security of patients' data using a WBAN from a sink node to medical centers. This framework provides efficient, reliable, and trustworthy techniques for monitoring the physical health of the patients from a remote location in an emergency. Before discussing the details of the framework, we mention some network considerations for modeling and designing the framework. All sensor nodes are equipped with Global Positioning System (GPS) . As a result, they recognize their adjacent nodes. All sensor nodes are homogeneous in terms of energy, memory and transmission power. The sink node has no resource constraints and has more computing power than sensors. The sensor nodes take the data from the patient's body and move towards the sink node, which is also inside the patient's body. Healthcare data are received by medical professionals through intermediate devices from the sink node. Malicious nodes can attack network infrastructure to invade data privacy, authenticity, and integrity. They simply drop the data packets and distribute the invalid packets to the path requests and responses to show its realism [8].

2.4.2 Architecture of The Proposed Method

The proposed framework design consists of two main algorithms. In the first algorithm, the biosensors are connected to each other in the form of a complete graph G, and there is a rim E between the set of N nodes. Using a multi-parameter metric, a weight value is assigned to each rim, indicating its cost. Costs include weight residual energy, number of jumps to the sink, distance to neighborhoods, and queue delay factors. The cost function

represents the generation of the pervasive sub-chart Siin diagrams in terms of minimum cost with some conditions as follows. First, there are no cycles in the sub-diagram. Second, all vertices must be connected. And lastly, for n vertices, there must be n - 1 rims in the sub-diagram. This subgraph has been formed based on Kruskal's algorithm in a way that each node contains an optimal list of neighboring nodes to send healthcare information to the sink node and from the sink node to medical centers. Unlike many other solutions, the proposed framework uses combined parameters to calculate the cost function. In addition, these subgraphs are retrieved based on updated cost using optimal learning. Finally, healthcare data is securely transmitted to medical professionals based on a cryptography block chain algorithm. The details of the proposed algorithm are discussed in the following subsections. Research design of a safe and low-consumed framework based on artificial intelligence for medical systems using IoMT is presented [8].

In this algorithm, biosensors are connected to each other in a non-directional diagram using the cost function f (c). The cost function is based on the residual weight of the WRE energy, the number of jumps up to h (c), and the distance to the Ndand Qdfactors zones of the queue delay. All factors are summarized, and each section is crucial in calculating the cost function. All biosensors create a connected graph that encloses a tree, so that each biosensor must be connected to its neighbors. There must be a unique rim between two consecutive nodes that represent the value of the calculated cost using multiple parameters.

Initially, the sink node advertised its position by flooding the location package. Accordingly, the sensors determine the current position of the sink. Each time each sensor node receives the sink node location, it records the number of jumps in the routing table and increases the packet counter value by Each node routing table also contains its point-to-point identifier. In addition, the sensor nodes calculate their weighted residual energy ratio over the periodic time t and send the information to one-hop neighbors so that they can update the routing tables.

2.4.3 Simulation

This section provides simulation settings using the NS2 simulation tool. The sensor nodes are located in an area of 15 square meters. The number of sensor nodes is then set to be 10, which are set on the patient's body. The sink node is in the center of the patient's body and acts as a local coordinator. The sink node is more powerful than

the sensor nodes in terms of resources. The simulation interval is set to be 250 seconds. The data flow between the sensors and the sink node is based on a Constant Bit Rate (CBR).

Throughput

The simulation results show that SEF-IoMT significantly increases the network throughput ratio at variable time intervals compared to other solutions. This is because SEF-IoMT uses multi-mutant data transfer between the sensors and the sink node. In addition, existing solutions do not consider link measurement for data routing, and weak transmission channels are mostly adopted for data transmission. The proposed SEF-IoMT provides more reliable and efficient links for routing using AI-based techniques and improves network throughput. In addition, existing solutions ignore data security in routing, and false entities often generate route request packets, which leads to severe network density. Besides, existing solutions cannot prevent malicious node notifications that reduce throughput to an unacceptable level [8].

Package Loss Rate

Package loss rates shows the behavior of SEF-IoMT in comparison to existing solutions. The simulation results show that SEF-IoMT reduces the level of package loss rate compared to other solutions at different time intervals. SEF-IoMT performs better than other methods since the cost function designed for SEF-IoMT is based on several factors and leads to the shortest and most conscious routing decisions with efficient energy. Furthermore, integrating data security using block chain increases the security level of each data block and makes it very difficult for malicious nodes to change and drop data packets. Due to the lack of link measurement and data security in existing solutions, it allows malicious nodes to generate network traffic in the transmission media and thus disrupt the flow of data packets. SEF-IoMT provides more stable routing paths from biosensors to the sink node and from the sink node to remote medical centers, which reduces the likelihood of packets being dropped and increases the stability of delivered performance [8].

End-to-end Latency

The simulation results showed that SEF-IoMT reduces the end-to-end delay ratio at different time intervals compared to other solutions. This is because SEF-IoMT selects low-consuming, safer, and more stable routes for data transmission and minimizes the possibility of data latency by wireless retransmission. Unlike other solutions that choose the next mutation regardless of the wireless channel conditions and lead to rapid path rediscovery, such approaches face additional overall delays in receiving data. SEF-IoMT uses the next evaluation based on artificial intelligence and uses multi-parameter metrics. Such an approach increases path lifespan and reduces network latency. In addition, integrating the security aspect into SEF-IoMT prevents malicious node behavior for data routing over longer distances as well as reducing network disconnection, which reduces end-to-end latency [8].

Energy Consumption

The performance results of SEF-IoMT are compared with the existing task in terms of energy consumption. Numerical analysis shows that SEF-IoMT improves energy consumption at different time intervals compared to other tasks. Other solutions use additional communication costs and energy consumption to build reliable routing paths. Such solutions do not judge the status of transmission media while sending data packets. This case leads to a high reduction in the proportion of energy sources in paths reconstruction. The SEF-IoMT design focuses on energy-efficient, shortest, most consistent and reliable routing paths that balance energy consumption among these sensor nodes. Multi-parameter metrics reduce the additional costs at node levels by selecting the most secure links to send information, and reduce the nodes' energy consumption ratio in the production of unnecessary path request packets [8,64].

After analyzing the benchmark paper and reviewing its similarities to our current research study, we have concluded that this paper [8] is a suitable reference for comparison. Specifically, we have identified several similarities between our research and the benchmark paper, as below :

- Using a secure routing

• Network segmentation with clustering and clustering techniques

• Transferring data between network devices using a secure method

• Using the same energy model as the proposed method

• Using homogeneous sensors

• Having the same aim to reduce energy consumption and increase security

• Using the same NS2 emulator software

• Analysis of simulation results under End-To-End Delay, Throughput, PDR, Energy Consumption metrics

Therefore, we believe that this paper can serve as a proper sample to compare with our current research study.

2.5 Conclusion

The WBAN plays a vital role in medical systems by monitoring patients' health and sending information to remote medical centers for appropriate actions. However, due to the limitations of the sensors, there was a need for an energy-efficient and reliable data transfer solution. In addition, patients' sensitive data are more prone to potential threats and lead to data security. In this task, we propose a secure and efficient framework using IoMT for e-healthcare that aims to reduce energy consumption and increase the timely delivery of data to medical professionals. The next step is selected based on several parameters that use Kruskal algorithm to achieve optimal routing by minimum cost. Based on the Kruskal algorithm, the proposed subgraph framework intelligently extracts from the complete diagram and reduces the overall cost of communication. In addition, as far as patients' data is transmitted over the insecure Internet through various access points, such data transmission is detrimental to data privacy and negotiates data integrity. In this task, SEF-IoMT uses a cryptographic block chain to transmit information. The data is used in the form of a chain which increases the security level of e-healthcare data against malicious traffic. Furthermore, along with the encryption block chain algorithm, public key-based digital authentication is also included in the data transmission to ensure its validity and integrity. Simulation-based experiments have been performed and their statistical analysis shows that SEF-IOMT is energy-efficient and safer

with less network latency than other tasks. In the next task, our goal is to improve SEF-IoMT in mobility-based medical scenarios in which the position of the sensors changes mainly due to the movement of the human body. Also, the proposed SEF-IoMT framework needs to improve energy consumption and network security to convert data among WBANs.

In various fields, the Internet of Things (IoT) is gaining in popularity due to the performance of independent sensors at the lowest cost. In medical and healthcare applications, IoT devices create ecosystems to sense patients' medical conditions such as blood pressure, oxygen level, heart rate, temperature, etc., and to take appropriate action in an emergency. Through its usage, patients' healthcare data is transmitted to remote users and medical centers for post-analysis. Various solutions have been proposed using the WBAN to monitor the medical condition of patients based on low-power biosensor nodes, however, preventing increased energy consumption and communication costs is a challenging and interesting problem. The issue of unbalanced energy consumption among biosensor nodes reduces the timely delivery of patients' information to remote centers and has a negative impact on the medical system. In addition, patient sensitive data is transmitted over the insecure Internet and prone to vulnerable security threats. Thus, data privacy and integrity due to malicious traffic is another challenging research issue for medical applications. The aim of this research paper is to provide a safe and efficient framework using the Internet of Medical Things (IoMT) for e-healthcare (SEF-IoMT) with the primary goal of reducing communication overhead and energy consumption among biosensors while transmitting healthcare data. It protects patients' medical data in a convenient way against invalid and malicious nodes to improve privacy and network integrity. The simulated results showed that the proposed framework increases the performance of medical systems compared to other advanced solutions in network throughput metrics. On the other hand, it reduces packet loss rate as well as end-to-end latency and energy consumption.

DoSL attack is one of the energy-consuming attacks on WBANs. This attack affects the network from two dimensions. The first dimension is related to the level of the entire network (Network Level) and the second dimension is related to the level of network devices (Device Level). In such a case, the following methods are suggested to deal with this attack:

Network Level: At this level, the DoSL attack assaults the entire WBAN and circumvents the security of the network with sophisticated attacks that cause damage and destruction to the entire network. To deal with these conditions, security mechanisms that can protect different layers of the network are utilized. In this research study, to deal with DoSL attacks at the network level, we have used an IDS-based intrusion detection system along with intelligent clustering based on genetic algorithms, which is capable of detecting DoSL attackers at the level of the entire WBANs.

Device Level: At this level, DoSL attackers disrupt the WBANs by focusing on devices and network nodes. To deal with DoSL attacks at the device level, security solutions such as the design of secure hardware that is wearable have been provided. This solution is subject to weaknesses such as not being able to deal with security threats in the generalization mode with threats. It is recommended to use security hardware modules to boost the security of devices and network nodes. In this research study, the modified AODV model has been used to increase the routing speed between network nodes and increase the reliability between nodes. In addition, in this research paper, we have used pre-shared keys to increase the security of data transmission at the device and node levels.

OFFICE FOR RESEACH TRAINING ,QUALITY AND INTEGRITY

DECLARATION OF CO-AUTHORSHIP AND CO-CONTRIBUTION: PAPERS INCORPORATED IN THESIS

This declaration is to be completed for each conjointly authored publication and placed at the beginning of the thesis chapter in which the publication appears.

1. PUBLICATION DETAILS (to be completed by the candidate)

Title of Paper/Journal/Book:	Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges," Journal of Sensor and Actuator Networks, vol. 11, no. 4, p. 67, Oct. 2022, DOI: 10.3390/jsan11040067.
Surname:	Yaghoubi
First name:	Mohammad [redacted]
Institute:	Institute for Sustainable Industries and Liveab
Candidate's Contribution (%):	70%
Status:	
Accepted and in press:	☐
Date:	[redacted]
Published:	✔
Date :	Oct 2022

2. CANDIDATE DECLARATION

I declare that the publication above meets the requirements to be included in the thesis as outlined

In the HDR Policy and related Procedures – policy.vu.edu.au.

MOHAMMAD YAGHOUBI Digitally signed by MOHAMMAD YAGHOUBI	14 Nov 2022
Signature	**Date**

3. CO-AUTHOR(S) DECLARATION

In the case of the above publication, the following authors contributed to the work as follows:

The undersigned certify that:

1. They meet criteria for authorship in that they have participated in the conception, execution or interpretation of at least that part of the publication in their field of expertise;

2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;

3. There are no other authors of the publication according to these criteria;

4. Potential conflicts of interest have been disclosed to a) granting bodies, b) the editor or publisher of journals or other publications, and c) the head of the responsible academic unit; and

5. The original data will be held for at least five years from the date indicated below and is stored at the following **location**(**s**):

Name(s) of Co-Author(s)	Contribution (%)	Nature of Contribution	Signature	Date
Mohammad Yaghoubi	70%	Concept, Methodology, Experiment, Result Processing, Draft	[redacted]	22
Khandakar Ahmed	20%	Concept, Validation, Review, Proof Read		15/11/2022
Yuan Miao	10%	Review, Proof Read		14/11/22

PO Box 14428, Melbourne,
Vic 8001, Australia
+61 3 9919 6100

CHAPTER 3 Analysis of WBAN from The Perspective of Security and Energy Consumption

3.1 Introduction

Wireless body area networks are one of the new technologies used in recent years to enhance the quality of human life, monitor the condition of patients inside or outside the hospital, monitor the activities of athletes, military applications, and multimedia [22,65]. WBANs consist of smart energy-efficient small sensors and a core node commonly called coordinator or sinkholes, usually worn inside clothes, on the body, or embedded under the skin [66,67]. These sensors collect information about the disturbed parts of a person's body and send it to the coordinator node through which to detect and transmit the collected data to other networks or other devices such as Mobile phones. Special devices, called relay nodes, can also be used to collect information from the sensors and send them to the sinkholes in the wireless body area networks, thereby extending the life of the network and increasing its liability [68,69]. In fact, relay nodes play a very important role in reducing energy consumption in the wireless body area networks, the advantages of which are highlighted in the following:

1- Protecting body tissues against radiation and sensor heat

2- Reducing the sensors' energy consumption

The IEEE 802.15 standard communication protocol is for implementing low-power and low-frequency communications, which is used for the wireless body area networks to optimize inbound and outbound communications and connectivity. It is also possible with other devices [70]. It is important to note that the challenges facing the wireless body area networks are similar to those of wireless sensor networks, but with a few inherent differences For instance:

Most wireless sensor network protocols consider energy efficiency for homogeneous sensors, while in wireless body area networks the sensors are not of the same kind and each is different in terms of input traffic rate and transmitted data rate [71-74].

The movement and mobility of sensors in sensor networks is about one meter to 10 meters, while this is about 10 cm for wireless sensor networks of the body due to topological changes [75-76].

The most important difference between wireless sensor networks and the wireless body area networks is the characteristics of the wireless channel, and the reason is that the human body is also part of the network communication in a manner that the geophysical and kinetic properties of the human body affect the passage between the nodes and the loss of path.

Various performance metrics are set for modern wireless body area networks, including the rate of received packet latency, power consumption, and network life, depending on the network topology, and the design of communication protocols. It should be noted, however, that research has shown that the Star topology does not usually provide high reliability in these new networks [77,78] and that the multi-Hop topology is a viable alternative, allowing the sensors to send information to each of the other nodes to improve network communication [79]. Owing to the fact that the energy of the sensors is supplied by a battery with a limited capacity, the communication of the sensors is considered the most energy dissipating, and the energy limitations that exist for the sensors, careful energy management is required for wireless sensor networks of the body in order to prolong the life of these networks. In recent years, researchers have tried to establish various communications between sensors in the wireless body area networks to optimize energy consumption in such networks.

By affecting the WBANs, security attacks reduce safety and increase energy consumption at the level of the entire network and device [40,41], which allows attackers to gain unauthorized access. To deal with this challenge, methods have been proposed including encryption algorithms, authentication, as well as secure and reliable routing protocols [80]. In this section, an attempt has been made to examine and analyze the methods for dealing with security challenges and improving energy consumption.

3.2 Structure and Operation of The Body Sensor Network

Today, the use of wireless sensor networks plays an important role in improving the level of intelligence and coordination of industrial or environmental screens. One of the special applications of wireless sensor networks in human health protection systems is known as wireless sensor networks. This sensor network sends physiological signals received from patients or the elderly to medical care centers in the treatment environment and after discharge in their living environment [81] . Therefore, physicians and emergency centers will monitor the

condition of patients simultaneously or with a slight delay and will respond to their treatment needs with higher speed and accuracy [81].

3.3 Application of Body Sensor Networks

Increasing the elderly population, there is a need for cheaper and alternative ways of monitoring and medical care, the demand for information integration and the discovery of knowledge embedded in information through data mining techniques, coordinating medical care, and encouraging patients to participate in their treatment and relevant training programs has been one of the motivations for the development of these networks[82]. In many medical systems, inadequate personnel, medical errors, and the impossibility of prompt and timely transfer to hospitals in remote areas create many problems in providing medical care services [83]. The concept of ubiquitous physical, physiological and medical parameters in any environment and without activity restrictions has only recently been provided with the advancement of technology. Not only has more precise patient care been provided in environments that have not been possible before, but also physical sensor networks have enhanced the quality of medical services provided to date; since these networks allow long-term and real-time monitoring of patients, even at home or at work. Implementing these networks on a large scale, without disturbing users, can significantly reduce healthcare costs, especially for long-term use by the elderly and the disabled where the high cost of patient care in the hospital can be reduced and the quality of life can significantly improve. At the same time, using medical sensor networks reduces the possibility of medical errors. Physical sensor networks have made health monitoring all-encompassing and economical, and will soon revolutionize the way people manage their health. Not only does this shift to preventive health care improves the quality of life, but also dramatically reduces health care costs [84].

3.4 WBAN Components

in Sensor node: The sensors in the wireless body area network are used to measure and analyze the biological signals received from the human body. The number of sensor nodes and their function depends mainly on their application [85]. Each sensor node includes hardware components as follows: 1- sensor unit, 2- power supply unit, 3- microcontroller unit, 4- communication unit, 5- memory unit.

Transmitter: The success of a physical WBAN often depends on the performance of the transmitter. The transmitter must be small, energy-efficient, and strong. The function of the transmitter is 1- data collection and processing, 2- data buffering and compression, 3- data security, and 4- communication [86]. There is a platform the wireless body area network that is a sensor transmitter called Mote .

3.5 The Difference Between WBAN and WSN

The difference between a body wireless sensor network and a wireless sensor network is that the wireless body area network is a communication network in which several small sensor nodes are located on the body. Wireless sensor networking techniques and CASE networks are commonly used to communicate efficiently between nodes. Body sensor networks share many challenges and opportunities with wireless sensor networks. The basic conceptual differences between the wireless body area network and the wireless sensor network from different aspects are given in Table 1. The wireless body area network nodes are usually smaller than the wireless sensor network [87].

Table1 - The Difference Between WBAN and WSN [87]

Features	wireless sensor network	wireless body area network
Scale	Environmental monitoring	Human body
Node no.	Numerous nodes to cover a large area	A limited number of nodes
Node size	Preferably small but not so important	Small
Network topology	Fixed	Variable due to body movement
Data rate	Homogenous	Homogenous
Node replacement	Easy	Hard
Node life	Several years/months	Several years/months (less battery capacity)
Power supply	Accessible & replaceable	Inaccessible and difficult to replace
Security level	Low	High
Wireless technology	Zigbee, Bluetooth, WLAN, GPRS	IEEE 802.15

3.6 The Architecture of Body Sensor Networks

The architecture of the wireless body area networks is divided into the following three levels [16], as shown in Figure 1.

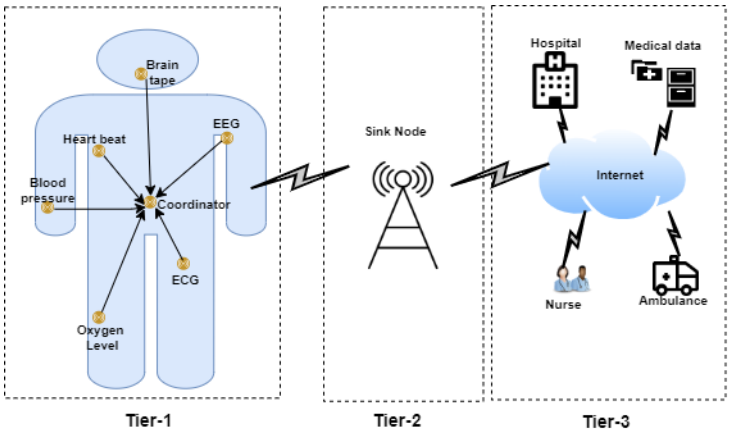


Figure 1 - The Architecture of Body Sensor Networks [88]

Level 1) Medical sensor nodes implanted on the human body or inside the body along with the sinkhole are located at this level [88].

Level 2) At this level, the sensor nodes send their data to the sinkhole and the sinkhole sends the data to the base station by aggregating and processing it [88].

Level 3) At this level, after receiving the data, it is sent to the base station through the Internet infrastructure to medical centers for remote monitoring and treatment. In general, in the architecture of this type of network, each sensor receives sensory information from the body's vital signs and then sends it to the base station in order to monitor the individual's health for medical control centers to provide medical care [88].

3.7 The Function of The Body Sensor Network

Sensor nodes are responsible for monitoring important parameters of the body, including the individual's disease status and vital signs. In a body sensor network, vital signs are mainly monitored such as body temperature, heart rate, blood pressure, respiration rate and blood oxygen level, and so on.

In addition to vital signs, other applications of medical sensors include ECG monitoring to monitor cardiac activity, brain signal (EEG), muscle signal Electromyography (EMG), glucose monitoring, and physical activity monitoring to determine an individual's health status [88].

When using sensor networks to obtain reasonable and appropriate results, different sensors should be placed in the network and different sensor information should be used to monitor the patient's condition to make appropriate decisions. Examples of different types of sensors used in various ways include dermal electrodes, wristbands, etc., as shown in Table 2.

Table 2 - Various Medical Sensors on The Human Body [89]

Sensor	Description
ECG	Electrical activity of the heart
Blood flow	Measurement of accelerating forces in three-dimensional space of the body
Blood pressure	The force exerted by the blood circulation on the walls of blood vessels
Body or skin temperature	Index of the body's ability to create and release heat
Respiration rate	Number of inhaling and exhaling movements per unit time
Oxygen level	Indicates the oxygen flowing in the patient's blood
Heartbeat	Frequency of the cardiac cycle
Blood sugar	Measure the amount of sugar (type, source, energy) in the blood
Muscle signal	Electrical activity of skeletal muscles (nervous, muscular system)
Brain tape	Spontaneous measurement of brain activity and other brain potentials

As it can be seen in Table 2, each of these sensors is placed on the human body according to its position and shows the patient's symptoms according to the type of sensor. For example, body temperature is one of the most important factors that should be measured to determine the patient's health status. A high body temperature is a sign of illness, and a low body temperature to a certain extent indicates an increased risk of illness. Blood pressure can be used to estimate high blood cholesterol, clogged arteries, or irregular heartbeat. The heart rate sensor can also be used to indicate the level and amount of stress. When blood pressure is measured under the influence of stress, it is not at the normal level, or a person's heart rate and body temperature are directly related to a person's level of activity [90].

3.8 Limitations of Body Sensor Networks

The rise of wireless equipment and recent advances in downsizing sensors have proven the feasibility of health monitoring systems. However, researchers of physical sensor networks face limitations in providing user satisfaction with ease of use, size, reliability, and network security. To pervasive this technology, a great deal of research has been done to troubleshoot and upgrade these networks to fit the seemingly existing capacities [91].

Networks that are implanted in the body must be compatible with the body, resistant to error and breakdown, and not in need of repair. Wearable nets should be light and portable so as not to disturb the patient's daily activities. Both types of networks must be scalable, highly secure, reliable, and energy-efficient. The general limitations of wireless sensor networks are also in terms of bandwidth, energy, computing power, telecommunication power, and memory. Also, medical sensors should be light in weight and small, and their energy consumption should be minimal. The short transmission range in body area networks provides local security in this part of the system. In fact, not only is the scalability of the human body smaller than other wireless sensor networks, but such an environment requires a different kind of frequency for monitoring. Basically, body sensor networks have different limitations than wireless sensor networks, and the fact that wireless sensor networks are designed and available are not ideally suited for body monitoring has led to the development of body sensor networks. However, the problems that the body sensor networks face are in many ways similar to wireless sensor networks [92].

3.9 Reduce Energy Consumption in The Body Sensor Networks

Considering the important role of the wireless body area networks in the quality and speed of treatment operations, attention is paid to the needs of these networks such as reducing energy consumption, quality of service, and security. In the last decade [93], many efforts have been made to optimize wireless sensor networks. But when we come across the specific application of this network for the human body, we must also consider its unique features of this network. In the table, a comparison has been made between the wireless sensor networks and their specific application for the wireless sensor network of the body. In Table 3, among the issues raised in the construction of body sensor nodes are their weight and dimensions, as well as energy consumption limitations. Due to the use of these nodes in the body or on the body, the issue of their size and weight is important for the

network design a huge part of which is related to the power supply or battery. On the other hand, these nodes are in direct contact with the user, so it is noteworthy in terms of the amount and number of times the battery is charged. Therefore, one of the ways to optimize these nodes is to reduce energy consumption, which leads to smaller batteries and less need for charging [93].

Table 3 - Comparison Between WBAN and WSN [94]

Compared item	Wireless sensor networks	Wireless body area network
Nodes number	a large number in a wide range	Less than 10 in the human body
Topology	Compound	Star
Type of nodes	Often homogenous	Heterogeneous
Physical properties of the node	No special restrictions	Implantable in the body
Energy supply source	Limited	Very limited
Energy efficiency	Requires high efficiency	Requires very high efficiency
Security	No special restrictions	Personal data of patients in need of high security
Connections	Less sensitive to service quality	Requires service quality
An example of a sensor node	MicaZ, IMote2	Sensium

3.11 Sources of Energy Loss in The Body Sensor Networks

The amount of energy that can be stored depends on the capability of the MAC sublayer protocols and the four primary energy loss sources associated with the network itself and the nodes, including collisions, overhead control packets, packet reception, and channel hearings that will be defined respectively as follows:

Collisions: The energy loss associated with collisions depends on the collision of packets sent over the wireless channel. If the sent packets are not sent with the appropriate signal strength on the receiver side, the packets will be received erroneously and distorted or a collision occurs in the channel, so the process must be repeated. Erroneous data can be recovered by error correction algorithms (ECCs). Although ECCs create a transmission overhead, they can be effective in reducing signal strength and battery power consumption [95].

Overhead Control Packets: Depending on the MAC protocols used in the network, different control packets are sent to all network nodes to configure the nodes. Improper protocols in a network with many nodes can result in wasting battery power. Battery life will be severely affected if network nodes are forced to wake up by improper

control packets. As an example of control packages, the following can be mentioned Which are used in IEEE802.11 protocols [96].

- request-to-send (RTS)
- clear-to-send (CTS)

Receiving packets: This waste source causes the nodes to emit radio waves to the environment while waiting to receive the packet. Many MAC protocols in WSN can reduce this waiting time. One way to avoid this waiting time is to exchange RTS / CTS control packets. Within these control packets, there is a network allocation vector (NAV) that has the time to send or receive all packets, both controls, and main [96].

Channel hearing: The radio waves of the nodes when monitoring, channel monitoring in updates, and notifications of collisions will consume energy [96].

3.10 Discussion of Energy Conservation in Body Sensor Networks

From a body sensor network perspective, the model shown in Figure 2 is mainly considered to consist of four components: (a) a sensing subsystem consisting of one or more sensors (with analog converters to the relevant digital) for data acquisition. (b) A processing subsystem including a microcontroller and memory for local data processing. (c) A radio subsystem for wireless data communications. And (d) the power supply unit. Depending on the specific application, sensor nodes can include additional components such as a locator to determine their positions, a relocation device or configuration, and so on. Nonetheless, we must consider the following statements in general:

Communication subsystems have much higher energy consumption than computing subsystems. It shows that transmitting a bit may consume as much energy as executing several thousand instructions [97,98].

Radiation energy consumption is often the same in reception, transmission, and idle modes, while power is cut off at least once in sleep mode. Therefore, the radio transceiver should go to sleep (or shut down) whenever possible. Depending on the specific application, the metering subsystem can be such a significant source of energy consumption that its power consumption should be reduced.

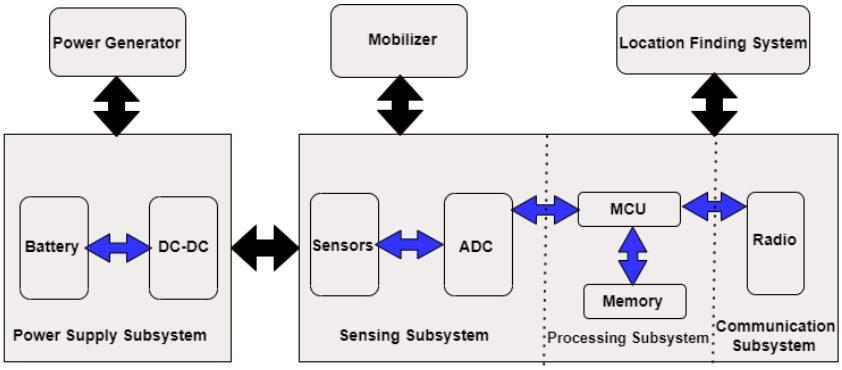


Figure 2 - Architecture of Wireless Sensor Network [99]

In general, energy conservation exists at five different levels [100-102] :

- Efficient programming of the sensor node states between sleep and active modes
- Efficient transmission power control to ensure a balance between optimal energy consumption and connectivity
- Efficient routing of energy, clustering, and data aggregation
- Data compression (source code) to reduce the amount of data transferred in vain
- Access to efficient channels and packet retransmission protocols in the data-link layer

Based on the above architecture and power decomposition, three main methods are provided: task cycle, data center, and mobility.

3.12 Factors Affecting Energy Consumption in The Sensor Network

Sensor nodes expire when their battery runs out of energy, and technically they die. The death of a node itself damages the network in two ways. The first is that the sensor that was part of the network's sensing functions is now dead and removed from the network. Most optimistically, this per se reduces the throughput of the network as much as the absence of a sensor. The second aspect is that usually the sensor nodes in wireless sensor networks are not only responsible for sensing, but in most cases play the role of permanent or temporary routers. This leads to a condition that if a node dies, some of the paths in the sensor network will either be completely lost or the quality of that path (if alternative paths are possible) will be inevitably affected. Consequently, this causes the

death of other nodes related to the area of the dead node to occur sooner. In other words, nodes can cause premature death of other nodes in the network with their wrong behaviors or with their death. The second effect is so important that some sources have defined network death as such; whenever a node in the sensor network dies, it is said that the whole network is dead. In other words, network life is the length of time that the network takes from the moment the network is established until the first node death. Of course, phenomena such as node death and network death usually need to be precisely defined based on the application of the sensor network. In the following, we attempted to formulate and generalize definitions for these concepts. These definitions are the starting point for our entry into the topic of energy consumption and the factors affecting it, then we propose solutions to save energy in each of these sectors [1].

3.12.1 Death of Sensor Node

A sensor node can be divided into two general parts. The power generation unit, which can be the same as the battery, and the energy-consuming units, which include the transmission and receiving units, the computing and control unit, and the sensing unit. All these units need the energy to perform their tasks properly. Sometimes not having enough energy can lead to incorrect or incomplete activity, which in many cases carries more serious costs than the sensor node not starting the activity in the first place. Therefore, part of the control unit should be responsible for examining whether the sensor node has enough energy to fully perform the activity it is currently planning to undertake. So, we find that the problem of energy in sensor networks has various dimensions that need to be considered. Each node that is produced has a series of nominal characteristics that the manufacturer of that node has identified those characteristics through various tests [103]. One of the most essential features of sensor nodes is their battery specifications. In the article [4], a statistical analysis has been performed on the discharge of battery charge in wireless sensor networks. This analysis is from the aspects of the internal components of the battery as well as the influential environmental conditions such as heat, humidity, and shocks due to incorrect installation and the level of transmission power, packet length, and so on. The test platform utilized in this paper is MICA2DOT Motes. In the model we present, we assume that a battery in a sensor node can be placed in three positions. The best situation, the average situation, and the worst situation. Usually, the number of computations

throughout the sensor network is not evenly distributed among the nodes, and routing algorithms try to make the distribution of computations throughout the network as level as possible. Thus, any algorithm better succeeding in so doing, the more satisfactory results it obtains in terms of increasing the life of the network. Among the reasons that the distribution of computations in sensor networks is not evenly distributed across all nodes can be such factors as the location of the nodes, the unpredictable behavior of environmental stimuli, and the coefficient importance of the areas noted by the BS. What is presented from the viewpoint of a sensor node is that as long as it has energy, it must respond to its predefined tasks as well as the queries it receives from other nodes. Sometimes nodes are located in areas of the network (especially in random deployment) that are less likely to be queried, which means that when the entire network dies, those nodes will still have energy. In this case, it is technically said that the node battery is in the best condition. Sometimes the node lasts about as long as the entire network. At this point, it is reported that the sensor node battery is in the middle position. In case the sensor node suffers from premature death caused by any factor (even damages due to incorrect placement are included in this clause), it is pinpointed that the node battery is in the worst condition. It is easy to conclude that in order to maximize the overall throughput of the entire sensor network, it is necessary to place the sensor batteries in the medium position or a position nearby.

3.12.2 Extending The Sensor Network Lifespan

If we want to make a list of all the effective factors during the life of the sensor network, we will notice the variety of these factors and sometimes the lack of direct connections between them. This shows that the lifespan of the sensor network is a function of various parameters that are proposed in different domains and layers. In general, a set of factors affecting the life of the sensor network can be divided into three general categories: intra-node factors, inter-node factors, and environmental factors. Environmental factors are usually random and somewhat unpredictable. Intra-network factors are also related to the internal layers and the connections between the layers and the protocols in these layers, the efficiency or inefficiency of these protocols as well as the node failures that can also be part of the sensor node. The inter-node factors that we focus more on in this study depend

more on routing protocols and how well the nodes communicate with each other. The following is a list of factors that cause energy loss in sensor networks and are rooted in the inter-node and routing protocols:

The number of transmitted messages includes the messages transmitted by each sensor node and the transmitted messages throughout the sensor network. Number of messages received by each sensor node and in the entire sensor network, sick or unwanted transmissions, erroneous or unwanted received data, size or volume of data sent by each node and in the whole sensor network. The volume of processing performed in the sensor nodes and the entire sensor network. The number of hardware resources used in the nodes, such as the number of memory references. The average duration of the waking period in each sensor node and the whole sensor network. Redundancy in data transmission and the effectiveness of the measures taken to deal with this case and the distance in packet transmission [104].

3.12.3 Utilizing Sensors to Control Health

Most patients see a doctor when they experience abnormal symptoms in their bodies. After visiting a doctor or going to the hospital, in fact, some time has passed since the person's illness commenced and the patient should be treated immediately. In fact, the time for the prevention of the disease has passed and the patient may have to spend a huge deal of money on his/her treatment. But by using a network of sensors, not only can physical health be detected quickly, but also it can even predict the disease and reduce the subsequent costs and risks during treatment. According to the latest news, new research by electrical engineers at Oregon State University has confirmed that an electronic technology called ultra-wideband, which can be used in a network of monitoring sensors, may be available in the future. This technology can be utilized as a part of a solution to achieve an ambitious goal in monitoring the health of the body or monitoring the physical health of individuals [105].

Sensor networks will be widely used in healthcare in the future. Some of these more rudimentary sensors are now used in some advanced hospitals to monitor patient physiology data, track courses of medication, and monitor physicians and patients in the hospital. One of the applications of sensor networks in this field is nursing the elderly. For this purpose, pressure cameras, a compass, and sensors are installed in sensor cameras to detect muscle activity, which creates a complex network. This network monitors the elderly person's falling, unconsciousness,

vital signs, diet, and exercise. Experts say that in the future, with the advancement of technology by utilizing very broadband technology, such networks can continuously and regularly help to determine the exact condition of the body's health. Real-time health diagnosis of this technology can compensate for delays in identifying degenerative diseases and save lives, thereby reducing health costs. Health can now be monitored remotely in some cases, but it still takes longer to complete remote monitoring systems. But the above-mentioned recent surveillance sensor, which works with very wideband technology, will most likely be very small and wearable and may receive the energy it needs from body heat. Despite its small size, this device will be able to transmit large amounts of information and will greatly improve the conditions of medical services and care, reduce the cost of treatment and help prevent diseases. "A band-sized device will be designed for this type of health assessment and monitoring," said Patrick Chiang, a specialist in wireless electronics and assistant professor at the Medical School of Electrical Engineering and Computer Science (at OSU). This sensor allows the transmission of data about some important things such as heart health, bone volume, blood pressure, or insulin status in the body. At its best, with this device, not only will people be able to monitor their health but they can also prevent disease before they catch it. For example, the diagnosis of arrhythmias and the prediction of heart attacks may be among the things that this device can be effective in preventing. This device should be cheap and accessible to everyone and should also be able to store and deliver large amounts of data [106].

3.13 Security in Wireless Sensor Networks of The Body

The wireless sensor networks of the body were created to collect information from an unreliable environment. Almost all security protocols for wireless sensor networks believe that the enemy or intruder can take full control of a sensor node through direct communication. Security is very important in accepting the use of wireless body area networks in various applications. In this section, we investigate the security of these networks and express their common attacks and security goals of them [107].

3.14 Sensor Safety Challenges

Wireless interface: The wireless interface is inherently less secure because the nature of its recording and playback makes eavesdropping easier. Any transmission can be easily changed or re-performed with an alternative agent. A wireless interface allows an attacker to easily receive and penetrate valuable packets [108].

Strong deployment: The network topology is always subject to changes due to node deficiency, addition, or movement. Although they may change position due to climate change, nothing is known in the pre-deployment topology as nodes may displace in the network. Therefore, the configuration itself is required to support it. Security diagrams must be able to function in this dynamic environment. Zoe and Haas stated that any safety solution with a static configuration is not enough. The changing nature of sensor networks to more robust designs for security techniques is essential to overcome such dynamics [108].

Aggressive environment: The third challenging factor is the attacking environment in which the sensor nodes operate. Particles are exposed to the possibility of being destroyed or abduction by attackers. Because nodes are in an attacking environment, attackers can easily access physical devices. Attackers can abduct a node, physically disable it, and extract valuable information from it [109].

Source scarcity: Infinite resource constraints on sensor devices pose significant challenges to resource-requiring security mechanisms. Security mechanisms must pay adequate attention to optimal energy consumption in order for the performance to be useful and effective [109].

Large-scale: Finally, the proposed scale of sensor networks has an important challenge for security mechanisms. Networking can easily cover hundreds of thousands of nodes, which is a significant task. Security proof in such networks is challenging to the same extent. The safety mechanisms must be scalable for a wide range of networks while maintaining high communication efficiency and computation [109].

3.15 Obstacles for Implementing Common Security Mechanisms for WBAN

Limited memory and storage space: Each sensor is a tiny gadget with a limited quantity of memory and storage for the code. The code size of security algorithms must be kept at a minimum in order to construct effective security measures [110].

Power limitation: Energy is the biggest limitation of the capabilities of WBAN networks. It is assumed that after setting up the sensor network, the network nodes cannot be easily inserted or charged. When an encryption function or protocol is to be implemented inside sensor network nodes, the effect of added security codes on energy must be taken into consideration.

In other words, when considering security in the WBAN network, we are interested in knowing its impact on the lifespan of the nodes. The extra energy consumed by the nodes for security is due to the required processing to perform the security functions, the transfer of security-related data, and finally the storage of parameters such as the encryption key in a secure method [110].

Unreliable transmission: generally, due to packet-based routing in the WBAN network, communications are unrelated, which signifies that data transmission is unreliable. Packets may be corrupted due to channel errors or deleted due to network congestion. This results in a package loss or miss. If protocols are deprived of proper error management, critical security packages may not reach their destination properly or be lost [111].

Encounter: Even if the channel is reliable, the connection itself may be unreliable. This is emerged due to the diffuse nature of WBAN networks. If the packets collide in the middle of their way, the transfer operation will fail. This can cause a serious problem in high-density networks and also lead to critical security packages not reaching their destination properly or being lost.

Delay: Multiple routing, network congestion, and node processing can lead to long delays, which may prevent synchronization in the WBAN networks. Synchronization cases are very important for the security of the sensor network where security mechanisms rely on reporting critical events or playing the encryption key.

Node's seizure Attacks: Sensors may be deployed in environments accessible to the enemy. Therefore, a node of a sensor is much more likely to be physically attacked than in a situation in which a server in a secure location is attacked by the network. Having taken the node, the attacker can read its important information which can include cryptographic keys [7].

3.16 Security Needs

The security needs to be considered in the WBAN networks can be summarized as follows [112]:

Data privacy: Data privacy is one of the most important issues in the security of the WBAN networks. In the sensor network, privacy depends on the following:

A sensor network should not disclose the data read by a sensor to its neighbors. Because nodes communicate sensitive data in many applications, establishing a secure communication channel in a wireless body area network is critical. In order to be safeguarded from traffic analysis attacks, sensor general information, such as sensor identification and public keys, must also be encrypted. To some degree, the sensor's generic information must also be encrypted to avoid traffic analysis assaults. The conventional method for keeping sensitive data private is to encrypt it using a secret key that is only known by the receiver; this is how confidentiality is achieved. One of the implemented solutions to provide confidentiality is to use the RC5 algorithm. Algorithms such as DES are not suitable for implementation due to high memory consumption as well as high computations. Another cryptographic algorithm is SKIPJACK.

Identity authentication: An attacker's attacks are not just summarized in changing information in packets; they can also modify the entire package by injecting additional packets. The receiver, therefore, needs to be ensured that the packets used in decision processing are genuine. On the other hand, when a sensor network is created, authentication is important for various management tasks.

In mutual communication, data authentication can be achieved through a highly symmetric mechanism: the sender and receiver share a secret key to calculate the authentication code message for all exchanged data.

Data novelty: Even if the confidentiality and comprehensiveness of the data are guaranteed, we must also ensure that each message is novel. Simply put, data novelty argues that the received data should not be outdated. They should be related to the recent times while ensuring that the old data is not sent. This requirement becomes important when we use the shared key strategy in the design. Although it takes time to spread the shared key across the network, shared keys need to be changed over time. Also, if the sensor is not aware of the new key change time, it is easy to disrupt the normal operation of the sensor. To solve this problem, a timer can be added to the packet to make sure the data is novel. An enemy not only can modify the datum packets but also can change this flow by adding the packet to the packet stream. Therefore, the recipient must make sure that the received data is received from the correct source. On the other hand, identity authentication is required to perform management tasks such as network programming and controlling the duty cycle of sensors.

Self-organizing: A wireless body area network is a mobile case network that requires each node to be independent and flexible enough in order to be self-organizing and self-repairing in different situations. There is no fixed infrastructure for sensor network management, and this inherent feature challenges network security. For example, due to network dynamics, it is not possible to place a common key between the base station u1607 and the entire sensors in advance. In addition to multi-step routing support, the self-organizing feature is also used to manage the key and create a reliable relationship between the sensors. If the sensor network lacks self-organizing, damages from an attack or even a high-risk environment can be devastating.

Time Sync: Most sensor network applications use some form of time synchronization. To maintain power, a sensor radio may be turned off for some time. In addition, the sensors may want to calculate the delay of sent packets between a pair of sensors (transmitter and receiver) that are moving. Interconnected WBAN networks may require group synchronization to track applications [113].

Secure positioning: The usefulness of a sensor network often depends on the ability to locate each sensor in the network accurately and automatically. A sensor network is designed to pinpoint the exact location of an error using location information that is sent correctly. Unfortunately, an attacker could easily manipulate the information

of insecure location by incorrectly reporting signal strength, retransmitting signals, etc. also using cursors in source number[106].

3.17 Classification of Attacks

Active or inactive: Attacks can be active or inactive. In inactive attacks, the attacker collects information that is available on the network without being detected. In this case, an attacker secretly eavesdrops and pretends to be a normal node, and at a certain time takes the collected information and leaves the network. This information may also contain security stuff [114].

Since the attacker leaves no evidence in these attacks, it is difficult to identify such attacks, but at the same time, the amount of damage that the attacker can inflict is limited.

In an active attack, the attacker tries to create a loophole in the security protocols through which to penetrate the network and carry out attacks such as packet modification, injection, and images to the network through these types of attacks are much arere severe than inactive attacks, yet it is easier to detect such attacks because the attacker is openly involved in the network [114].

Internal or External: All nodes in a network are considered collaborative entities to external attacks, an attacker can only carry out attacks outside the network, and usually such attacks have limited damage.

If an attacker can gain access to the network, this type of attack is called an internal attack. Having been considered a legal entity. In this case, an attacker can cause more serious damages than external attacks. Attackers usually launch active attacks by intervening through a node or implementing a malicious node that can bypass network access mechanisms.

By small or large tools: In attacks with small tools, the attacker uses the same network nodes or nodes similar to the ones in the network, and in this case, the attacking tool has the same function as other nodes. But in attacks with large tools, the attacker can use more powerful devices, including computers, which have more processing power and energy. The attacker has more opportunity and power to damage the network in a portable PDA or these attacks [115].

3.18 Attacks on The Physical Layer

Congestion: There is a well-known attack on wireless communications that easily interferes with the radio frequencies used by a transceiver of the device. This case displays the attack in the existing section. The only difference between congestion and normal radio broadcast is a delay in service status of the former. The degree of congestion is determined by physical characteristics such as high power, antenna design, obstacles, and a wide field. This type of attack is particularly effective against single fixed frequency networks when the nodes are in a small, single spectrum mode. Standard defense against congestion includes the use of a wide range of frequency techniques [116].

Frequency transmission is a type of broad-spectrum in which a sequence is used to change the transmission frequency. The receiver, also called a sequence, can re-transmit a signal to reconstruct the original message. Frequency transfer resists unexpected congestions, i.e., interferences. Broad-spectrum techniques resist noisy environments in which sensor networks are destroyed. Although this set of inverse criteria has been carefully studied, their inherent complexity includes broad-spectrum systems which cost a lot for sensor particles [116].

Frequency jump requires high power and high financial cost which are two important sources in the sensors network. Preventing service attacks is a difficult task because most sensor networks recently use single-frequency communications. Researchers in [117] have proposed a "Jam Dense Area Mapping" that emphasizes identification and compatibility in response to congestion.

They assume that only a part of the network is congested. It tries to map the area. Therefore, it can be avoided. Nodes in the affected area are synchronized with the low-power state. Information about congested areas is transferred to the network layer. So, packets can be easily rooted around ruined areas. If broad-spectrum techniques cannot be integrated into particles, detection algorithms such as Jam can be significant in the case of defending against congestion attacks.

Tapping: A secondary problematic issue in the physical layer is the relative ease and potential difficulty of tapping the device. This is raised by the large scale, robustness, and special nature of sensor networks. Access to

thousands of nodes over several kilometers cannot be completely controlled. Attackers can have more access to nodes than network operators. Nodes may be abducted, or trapped without emerging problems. Although node destruction is undesirable, node inclusion can be dangerous due to some cryptographic processes [118].

One type of defense involves regulating the physical temperature of the devices. Nodes must react to knocking by removing sensitive cryptographic information; nevertheless, tapping-resistance packing increases the cost of the device and reduces their economic utility.

The best solution is an algorithmic solution. Algorithms that reduce the impact of a single key factor on a perfect network have a security impression. For example, if each node has a key with its agents and neighbors, a smaller part of it is included than the time the network has a set of keys. Although this software achievement is less costly, it does not provide significant protection. In fact, tapping is one of the most important problems in sensor network security [119].

3.19 The Datalink Layer and Its Attacks

The datalink layer is responsible for data flow multiplexing, data frame detection, media access, and error control. Attacks in this layer include collisions, termination of resources, and unfair attacks.

Collision: A collision occurs [120] when two nodes simultaneously transmit a message on the same frequency. When packets collide with each other, a change occurs in a part of the data, which causes the packet to not match the receiver, and therefore the packets are also rejected. The attacker uses this technique to create a collision with some packets such as confirmation messages. Since the node of the packet sender does not receive the confirmation message from the recipient, it sends the packet through identifying and analyzing radio transmissions that are close to the demolished node, an attacker could modify some of the important elements of the package including the fields used in Checksum. By doing so, the attacker could cause the demolished node to send many packets resulting in wasting the energy of accessing the channel and transmitter. One of the obvious consequences of the collision is that the cost of backtracking increases in some protocols such as the Media Access Control Protocol.

Unfortunately, it is difficult to detect a collision in transmission in wireless networks. One way to deal with a collision attack is to use error correction codes. These codes are suitable for covering random errors that may occur in bits independent of a message. But on the other hand, these codes naturally have additional computational and transfer responsibility, which causes redundancy in the message. Most of these codes work properly with the lowest level of collisions and are also compatible with types of collisions such as environmental and possible collisions. But it should be noted that an attacker can always change the ability of the network to correct changes. Unless the malicious collisions are fully identified, a perfect defense strategy for this type of attack cannot be provided.

Fatigue (resource termination): Repeated collisions by an attacker can cause resource termination. Even if the network traffic rate is not high, if a node continuously performs the retransmission operation, it will cause a collision and this operation will eventually cause the power to run out. For example, if the connection layer is not implemented properly, the related node will permanently send outdated packets until this useless action is detected and prevented, or the power of the sender node and adjacent nodes runs out. In this method, the attacker only needs to change part of a long message or create noise in the confirmation message so that the whole package is sent again, and with resending, there is a possibility of collision as well as energy depletion. Random reversals are only used to reduce unintentional collisions and are therefore not a good solution, as the attacker can easily listen and wait for the next attempt. This cycle will continue as long as the attacker can react before the packet is fully transmitted.

One of the possible ways to counter this attack is to set the rate range in the MAC protocol acceptance control section. That is, specifying the maximum number of requests to be answered or sent on the network. This allows the network to reject the large and unusual number of requests without being transmitted over radio waves, thus preventing the nodes from running out of energy due to repeated transmissions. The rate range can be determined through the date of recent requests in the network and it should be noted that the rate range is such that it does not reduce the efficiency and bandwidth of the network. The second technique is to use a time division that assigns a time slot to each node, and the intended node can only do transmission operations at that specific period. But on

the other hand, as far as the nodes must wait for their sending time to arrive, network performance decreases. This method is also suitable for solving the problem of indefinite procrastination.

Unfair attack: This attack can be considered a weakened form of DOS or a partial DOS attack. The attacker leads to this attack by repeatedly using other attacks including collisions and fatigue or abusing the MAC protocol prioritization mechanisms. This attack reduces the usefulness and efficiency of service instead of preventing it completely. For example, it causes users who use the network in real-time mode to see their Deadline [121].

In fact, in this attack, a malicious node constantly sends an access request to the channel, thus causing an eagerness for other nodes in the network to access the channel, and will take over the channel according to the size of the message. One of the defense strategies for this attack is to use small frames; the nodes can only have the channel for a short time and therefore the attacker will not have enough time to seize the channel. But if the network transmits long messages, this method increases the responsibility of frames. On the other hand, an attacker can defeat this strategy by cheating in competing for channel access; Sending the channel access request repeatedly, while other nodes send this request with a time delay and randomly [122].

3.20 Network Layer and Its Attacks

In this section, the attacks against routing in the sensor network are introduced. Many of the WBAN networks routing protocols are very simple. Accordingly, they are often prone to attack. These types of attacks are divided into the following [114]:

- Denial of Service (DoS)
- Spoofed, Altered, or Replayed Routing Information
- Sybil Attacks
- Sinkhole Attacks
- Wormhole Attacks
- Hello flood Attacks

- Selective Forwarding

Denial of Service (DoS) attacks are not new. There are several standard techniques used in computing to withstand several common denial attacks. However, this is still a major problem in the network security community. The simplest type of denial-of-service attack is trying to unload existing resources in a weak node. By sending too many unnecessary packets, the enemy prevents legitimate network users from accessing the services or resources they deserve. DoS attacks do not only mean doe enemy is trying to sabotage, disrupt or dismantle the network, but also many incidents that impair memory capacity in providing a service.

The following can be done to counter denial of service attacks [123]. Denial of service (DoS) attacks are standard attacks on sensor wireless networks, causing parasites in a node or group of nodes. In noise transmission, the attacker transmits a radio signal that interferes with the radio frequencies used in sensor networks. In a network, a parasite penetrates in two ways: fixed parasite and scattered parasite. In fixed parasite, it shapes a complete parasite into the integrated network; as a result, no message can be sent or received. If the parasite is scattered, the nodes can exchange messages periodically not in a steady-state.

Routing Information that is Spoofed, Altered, or Replayed: The most frequent direct attack on a routing system is to target the routing information that is transferred among nodes. Unprotected routing in the WBAN networks causes such vulnerabilities in routing; because any node in the sensor network can act as a router and thus can directly affect the routing information. By eavesdropping, modifying, or repeating routing information, intruders can create routing loops, generate error messages, and network segmentation, increase end-to-end latency, and increase or decrease source paths.

We can use the code 1 authentication message attached to the main message in order to counteract eavesdropping and change routing information. By adding a code authentication message, the recipient can detect a fake or modified message. Counters and time stamps can also be used in the sent message to counter the repetition of routing information. In general, the solution to deal with such attacks is to validate nodes and encrypt data packets.

Sybil Attacks: In the simplest definition, a Sybil attack can be expressed as follows: A malicious node that foists itself instead of many other nodes through impersonation. This attack was first introduced by Mr. Doser 2 is analogous networks. He realized that this attack could prevent redundancies in distributed networks in a way that it impersonates others and does not allow real distribution. Mr. Karloff and Mr. Wagner then defined this type of attack in WBAN networks [110].

Assuming that the additional identities of the malicious device are cyber nodes, Sybil attacks can be divided into three dimensions :

1. Direct communication compared to indirect communication

2. A fake identity compared to an abducted identity

3. Simultaneity [124].

First dimension**:** direct communication compared to indirect communication

Direct communication: One way to carry out this attack on Sybil nodes is for them to communicate directly with legitimate nodes. When a legitimate node sends a message with radio waves, one of the malicious devices listens to the message. In addition, the message sent from a Sybil node is sent from a malicious device.

Indirect communication: In this case of attack, no legitimate node can communicate directly with Sybil. Instead, one or more malicious devices claim to have access to Sybil. The sent message is routed through one of these malicious nodes, which pretends to have transmitted the message to the Sybil node.

Second dimension: Fake identities compared to abducted identities

A Sybil node can abduct identity in two ways. This node can forge an identity or abduct it from a legitimate node.

Fake identity: In some cases, an attacker can create optional Sybil identities. For example, if each node is identified by a 32-bit integer, then the attacker can easily assign a 32-bit integer to each Sybil node.

Abducted identity: If a mechanism is implemented according to which the identity of legitimate nodes can be identified, the attacker can no longer forge a new identity. For example, suppose we intentionally restrict the namespace; as a result, the attacker can no longer enter a new identity. In this case, the attacker must assign other legal identities to the Sybil nodes. Identity abduction may not be detectable if the attacker destroys or temporarily disables nodes whose identities have been duplicated.

The problem here is that the same identity will be used repeatedly in different parts of the network. This problem is called duplication of identity 1. Although investigating this problem requires extensive research, we briefly point out two ways to deal with it as follows:

- Positioning any identity that can be done centrally or by DHT tables.
- Counting the number of identity connections; if the number of identity connections was more than usual, that identity should be deleted.

Third dimension: Simultaneity

Synchronous: The attacker may want to share all its identities in the network at the same time. Since each piece of hardware can only act as one identity at a time, the attacker will circulate among these identities to show that all their identities are on the network at the same time.

Asynchronous: In this case, the attacker shows many of his identities in the network intermittently and over a period, while a small number of its identities are permanently present in the network. An attacker does this by pretending that identity has left the network and that another identity has entered the network instead.

An attacker can remove and insert a certain number of network identities into the network, or it can use a new identity each time. In another case, the attacker could have multiple physical devices in the network; hence it could displace identities among them.

Defense strategies against Sybil attacks: To defend against Sybil attacks, we must make sure that each provided identity belongs to a physical node. This goal can be achieved in two ways:

- Direct confirmation: Node directly examines whether its contact node is authentic or not.
- Indirect confirmation: In this case, the approved node can confirm or reject another node [124].

Three solutions to counter a Sybil attack are considered as follows :

- radio source testing
- key authentication for pre-distributed keys
- node registration, and location verification [125].

Wormhole attack:

In this attack, the attacker connects two points of the network with a relatively fast communication platform which is called the wormhole. This communication platform can be Ethernet cable, high-range wireless communication, or even fiber optics. Once the wormhole path is implemented, the attacker seizes packets sent by nodes from one side of the network and spreads them through the wormhole path to the other side of the network. It should be noted that in this attack, the wormhole nodes act completely invisibly, i.e., they are not visible to the network. Accordingly, it does not need to have encryption keys or even a network ID [126].

Sinkhole attack:

A sinkhole attack is one of the most interesting and dangerous attacks in WBANs. One of the interesting features of this attack is that it can plan another attack in the middle of a specified attack. In this attack, the general goal is to mislead the neighboring and adjacent nodes by a node whose information and specifications are fake in order to pass their information to the malicious node. This is when the attacker can make any changes to the information, including changing message 2 or even rejecting packets 3 and other attacks.

Communication is step-by-step in wireless body area networks which means that the message is transmitted from one node to another until it reaches its destination. In this case, the nodes usually choose the shorter path, and the node in which the Hop Count is less than the others choose the so-called optimal path as its source. The attack starts when one sensor node decides to make itself attractive to other nodes. As far as there is a discussion

of optimal path selection in sensor networks, sensors in the network also try to choose the best path that has the least cost to convey their message. Cost criterion can also be the amount of processing, the consumed energy consumed etc. So, a malicious node in this type of attack shows itself to its neighbors in such a way that they think it has the lowest cost and the shortest path to the base station. This is when the attack enters its main phase, as the neighboring nodes select the malicious node as their source and send the information to it, unaware that the node is reporting fake information and the distance to the base station is completely unreal. At this time, a so-called penetration zone 4 is created in the network in which a huge amount of network traffic enters this node and a lot of information is being changed and forged. The malicious attack can be of the laptop class, in which case it has a lot of processing and battery power, and can continue its sabotage operation for a long time.

In sensor networks, there are two commonly used routing protocols called MultihopLQI and MintRoute [127].

Hello flood attack: A new attack on of WBAN network is the hello flood attack. In many protocols, nodes need to publicly broadcast Hello packets to declare their existence to other nodes, and a node that receives such a packet assumes that the transmitter node is in the radio range. This assumption can be misleading. That is, it publicly distributes routing information or other information with high transmission power, and a laptop – an intruder of a category can convince the neighboring nodes in the network. As an instance, an intruder may broadcast to all nodes in the network a high-quality link to the base station and can cause many nodes to use this path. But those nodes that are too far from the intruder send their packages from another route. An intruder does not necessarily need to be able to generate authorized traffic in order to use a hello flood attack. It can simply re-distribute packets publicly with high power so that they could be received by any node in the network.

The simplest defense against a hello flood attack is to examine a link on both sides before performing a meaningful action on a received message from a link; however, this countermeasure loses its efficiency when an intruder has a strong receiver like its strong transmitter. In this way an intruder can efficiently create a wormhole. Since the link between these nodes and the intruder is mutual, the above method is unlikely to be able to detect and resist a hello flood.

One possible solution to this problem would be for each node to authenticate its neighbors with an authentication protocol from a secure base station. If the protocol sends messages in both directions of the connection among the nodes, the hello flood can be repelled when the intruder has a strong transmitter since it examines the connection protocol in both directions.

Note: flood distribution is commonly used to spread a message that is to be received by all nodes in a multi-step topology, while in a hello flood attack, a one-step public broadcast is used to convey a message to many recipients.

A major challenge in securing g large network is their self-organizing and decentralized u1570 nature. When network size is limited or topology is well-constructed or controlled, general knowledge can be used as a security mechanism. Imagine a relatively small network of one hundred nodes or less. If we can assume that there are no unauthorized nodes in the development stage, then the initial topology is formed and each node can send information to its neighbors and send its geographical location to the base station. Using this information, the base station can plot the entire network topology. The reason for the topology change is due to radio interferences or node error. The nodes periodically update the appropriate information of a base station, causing the base station to map the network topology correctly.

Selective Forwarding Attack: Multi-step routing networks perform on the assumption that the intermediate nodes participating in the routing send the received messages completely and intact to the next node. In a selective forwarding attack, unauthorized nodes may not send specific messages to the next node and decide to delete them to ensure that these messages will not be propagated in any case. The unauthorized node operates as a black hole in one version of this attack and does not send any packet to the next node. Finally, it will be deleted.

If an intruder is threatened by its neighbor nodes and going to be removed from the path, it decides to look for another path. A very subtle form of this attack is when an intruder selectively sends packets. An intruder tends to delete or modify packets originating from a certain number of nodes and send the rest of the packets correctly; Thereby, reducing suspicion of unauthorized activity.

Selective forwarding attacks are usually very effective when the intruder is located exactly in one direction of the data stream. However, the intruder may eavesdrop on the passage of neighboring nodes and cause other nodes to simulate actions such as selective forwarding by creating parasites or crashes. Given that this attack takes place through authenticated nodes, we need to improve authentication mechanisms to deal with them. So far, several solutions have been proposed to deal with these types of attacks which are as follows [128]:

1. Attack identification through the concept of node authentication

2. The concept of multiple data streams

3. Detection with the help of the concept of heterogeneous networks.

3.21 Summary of Countermeasures Against Attacks

WBAN networks are highly vulnerable to attacks, and the ability to withstand attacks is one of the challenges of developing these networks nowadays. The main reasons for these problems are [121]:

- Shared data transmission radio channel
- Unsafe operating environment
- Insufficient central power
- Limited resources
- Being physically vulnerable
- Insufficient connection of middle nodes

The structure of these networks is based on the use of radio signals instead of wires and cables. Using these signals, and indeed without limiting the coverage of the network structure, inflators can break into the not-so-strong security barriers of these networks, and impersonate themselves as a member of them. If this is the case, there exists a possibility of accessing critical information, attacking the organization's service providers, corrupting

information, disrupting the communication of network nodes with each other, producing unrealistic and misleading data, abusing effective network bandwidth and other destructive activities.

To deal with parasite transmission in the physical layer [129], various broad-spectrum methods such as frequency jump 2 or code distribution 3 are used. Frequency jump in broad-spectrum 4 is a method of transmitting telecommunication signals in which the carrier frequency is switched rapidly among a certain number of channel frequencies and using a quasi-random function specified for the transmitter and receiver. The enemy will not be able to send parasites on a frequency used at the specified time without the ability to follow the selected frequency sequence. However, since the number of selected frequencies is limited, the enemy may achieve its goal by sending noise over a wide range of frequencies.

Code broadcasting is another method used to counteract attacks containing parasite transmission, and is a common method used in mobile networks. But this method has a high design complexity that leads to high energy consumption in the WBAN. In general, considering the needs of the sensor network for low power consumption and low-cost sensor nodes, the sensor nodes are limited to the use of a frequency, which makes the WBAN networks susceptible to attacks containing the parasites.

Like many wireless and wired networks, WBAN needs security to perform routing properly, advance data packets, and maintain and update routing information. In fact, security is a necessary condition for the proper functioning of network operations, without which, there is no guarantee that these operations will be performed properly, and attackers can easily disrupt the integrity of the network.

Data link layer encryption and authentication, multi-path routing, ID authentication, mutual link authentication, and public distribution authentication can protect routing protocols against aliens, fake routing information, Sybil and hello flood attacks, and eavesdropping. And it is possible to equip existing protocols to these mechanisms. And wormholes pose major challenges to the design of routing protocols, and it is unlikely that there exist any defense mechanisms against these attacks once the routing protocol design is completed. Designing a protocol to

boost these two work attacks is tough, but with protocols such as geo-routing, there is hope to overcome these attacks.

In the following section, the methods used to diagnose and prevent denial of sleep attack in the WBAN and the methods used in them will be reviewed and evaluated. The purpose of this section is to present the background of the topic of discussion, investigation of the strengths and weaknesses of each one, and finally determine the gaps in the research and the subject of the research for the future [130].

3.21.1 Absorbing Markov Chain Model (AMC)

A mathematical model based on the Absorbing Markov Chain (AMC) has been used to detect sleep denial attacks in sensor networks [131] and the possible nature of the sensor nodes has been detected using the AMC model. Considering the expected time of death in this method, the sleep denial attack is detected by sensor networks under a common scenario.

The method of investigating the behavior in high-risk sensor nodes is executed according to the Markov chain with an absorption mode. In the absorption method, the Markov chain is used to model each of the sensor nodes. That is, instead of focusing on the behavior of a sensor node, the network stream is monitored by an intrusion detection method. In this method, the absorption expectation time of the sensor network is examined, which indicates the life span of the network. If the state of the network is prone to rapid death, we compare the common death time of the sensor networks. After that, the network is attacked by sleep denial (affected by sleep denial attack). This method is much more accurate than the definitive model method.

A hierarchical framework based on distributed participatory approaches

A hierarchical framework based on distributed collaboration method [132] has been used to detect sleep denial attacks in WSN. This method uses a two-step anomaly detection to minimize the possibility of incorrect intrusion. As a result, a heterogeneous WSN with effective and reliable performance will be presented. These variables are compared with specific predefined parameters in a normal index to detect anomalies. The task of each node is to make dynamic changes to minimize the burden created by another node. In order to decrease the possibility of this

attack, the physical method prevents the malicious node from entering the network and rejects fake packets. In [133], a layer of efficient energy with a security mechanism is used to protect the network from sleep denial attacks. The simulation showed that in this approach, significant efficiency of sleep denial attacks is obtained by preventing network nodes from going to sleep mode. This layer-by-layer interaction concept was used to prevent sensor nodes from wasting energy attacks.

3.21.2 Light Hierarchical Model for HWSNET

Heterogeneous wireless sensor networks (HWSNETs) are much more suitable for real-life applications than their homogeneous counterparts. HWSNET [134] security along with the rapid development of HWSNET has been considered an important issue. A small hierarchical model has been used in HWSNET to detect insomnia of sensor nodes that are affected by sleep deprivation attacks this method, a cluster-based active energy (force) is used to create a five-layer hierarchical network to increase the scalability of the network and its lifespan. Here, sensor networks are subdivided into clusters which they elves are again subdivided into separate sections. Configuring the sensor field prevents redundant communication messages among the sensor nodes by maintaining communication bandwidth. In this method, energy efficiency is achieved by maintaining a minimum number of active sensors. The dynamic model is designed to overcome the sudden death of the IDS of sensor nodes due to the power decrease which is responsible for detecting tasks. The anomaly detection method has been used in approaches that have avoided detecting pseudo-intrusion [135].

3.21.3 Congestion-Based Defense Approach

Congestion-based [136] defense method is used for sleep denial attacks using anomaly detection model to determine the impact of traffic between nodes. Considering this issue, the frequency oscillation method was developed, and factors are used as congestion information to collect the oscillation time frequency and communication frequency. The defective channel is detected according to the oscillation time frequency, and when the node is split, these data are generated and the defective channels are removed. The simulation results show that this method is effective in detecting defective channel. Information relating to the least consumed energy is

diagnosed using ants. To prevent sleep denial attacks, a framework consists of four key components is formed including [137]:

• Strong link layer authentication

• Anti-duplication protection

• Accumulation Identification and reduction

• Defense of general broadcast attack [37].

Achieving a strong link layer is the most important and first part of sleep denial defense and should include any WSN that may be attacked.

3.21.4 Security-Topology Maintenance Protocol (SEC-TMP)

The topology maintenance protocol is scalable from flexible sleep denial attacks. SEC-TMP does not require basic routing and confidential double nodes. This provides very high scalability for newly established TMP (Topology Maintenance Protocol) already existed nodes in the network. Using one-hop communications, a new method for detecting sleep deprivation attacks based on wireless body area networks (WBAN) has been categorized. This recursive classification is obtained from the sensors that are required one by one. The classification algorithm (FFUCA) is used without flexible and fast observer[138]. The opposite node is selected as the leader in order to launch the sleep deprivation attack .

3.21.5 Random Advantage, Hash-Based Layout and Rotation Period

Three classification methods to reduce sleep deprivation, random advantage, Round Robin and Hash-based design have been investigated [139] .This method prevents the opposite node from becoming a leader and minimizes the sleep deprivation attack. The Round Robin design randomly selects the leader. It is used to overcome the lack of scalability in the Round Robin classification algorithm. In the Round Robin design, the categories were held for a long time. The Round Robin design consists of two stages: the start-up phase and the maintenance phase, the initial category was being formed in the start-up phase. During the maintenance phase, the exact members of each cluster are updated by adding new nodes, removing nodes from the network, and node

dynamics. The Round Robin design only needs a single upgrade to select the leader. But the list of nodes in a category indicates that each sensor node must be always maintained in the Round Robin design. In the Round Robin design, the extra load in the Round Robin model naturally overcomes the selective lead-cluster in the hash-based model. The dynamic cluster is executed by error and attack method, without bearing additional load. Many sleep denial attacks do not require a fixed signal. It is then difficult to identify traffic as a destructive issue in order to identify the attacker node by transmitting its emitted force [140]. The sleep denial attack focuses on the MAC protocol. Intelligent sleep denial preserves radio messages from sensor nodes so that batteries discharge spontaneously within a few days. The sleep denial attack is reduced by a framework including these features, link layer authentication, protection against general distribution attack, and resistance against interference.

3.21.6 Isolation Table Intrusion Detection System (ITIDS)

Isolation and routing tables are combined to diagnose abnormalities. The Isolation Table Intrusion Detection System (ITIDS) detects malicious nodes based on attack behavior. An abnormal node is detected by its unusual behavior. Sensor node behaviors are compared with attack behaviors to determine abnormal information. If the node becomes abnormal, it is disconnected and recorded in the isolation table. In ITIDS, different types of sensor nodes are responsible for monitoring and controlling each other to detect a sleep denial attack. The four features of ITIDS are [141]:

• Base Station (BS)

• Primary Cluster Head (PCH)

• Several Secondary Cluster Headers (SCHS)

• Remaining sensor node MNs (node is a member).

This method consists of four steps. First, it defines the IDS pre-system. The MNs are then monitored by SCH and after the PCH, by SCH and MN. Finally, IDS is supported and placed in the isolation table existed in the base station [142].

3.21.7 Ant-Based Routing Algorithm

Ant-based routing algorithm has been used to detect sleep deprivation attacks in WSN [143]. Denial sleep attacks have been identified through age, energy and reliability parameters. The effect of distributed denial attacks on WSN performance is evaluated by using OPNET modeler. Package authentication is used to prevent sleep denial attacks [144]. Continuous sleep timer resets and data link layer authentication are used in order to protect WSN against sleep denial attacks.

3.21.8 Safe Consciousness Plan

The Safe Consciousness Plan activates the sensor node by a safe conscious wave in case that messages are waiting from legitimate and approved nodes [145]. This method uses a small approved security plan in which a node can operate without the need for modification. The network can be protected from the sleep deprivation attack with approved movements from the application level to the physical level. Time coordination provides a plan with a single-time password for a validated secure consciousness [146].

This plan consumes less battery under the denial of self-discharge sleep deprivation. The main idea is to always keep the node in a state of being asleep and awake, especially when communication is essential. Therefore, a subsidiary receiver remains in standby mode with a small amount of energy consumed. The request for communication with this receiver is maintained, and parts of the node are also awakened in order to receive data. It approves and receives all incoming requests from the conscious receiver in order to prevent energy depletion. The request that wireless sensor nodes use to wake each other is known as a token. By calculating these tokens, unnecessary traffic is reduced and replaced with them. A counter that matches a password is also used to create this token.

3.21.9 Storm Control Mechanism

Storm control mechanism has been used to reduce flooding and sleep denial attacks [147]. The frequency of packets received by the system is tracked and alerted when the configuration exceeds a certain limit. The node sends an alarm to the base station and shuts down its wireless receiver for a predetermined period. The storm

control mechanism in Tiny OS is performed as a security layer registered in a communication package. TOSSIM is used for implementation testing.

3.21.10 Adaptive Classification Rate Limit (CARL)

The adaptive classification rate limit (CARL) method depends on conventional host-based intrusion detection methods to prevent sleep denial attacks [148]. This is a limited rate approach. In this method of adaptive rate, network traffic is limited when there is a possibility of the existence and attack of malicious packets. This method can be used in order to maintain better throughput and network life span even during sleep deprivation attacks. Fake program switches with RSSI measurement method can protect the network against sleep deprivation attack [149]. This plan is implemented in S-MAC protocol. The fastest process of intrusion detection plan is Markov Decision Plan (MDP) which keeps the minimum number of sensors activated [150]. This method ensures that transmission, computing, and energy consumption for the sensor is reduced. It also ensures that network life span is reduced. Secure intrusion detection systems were used to prevent sleep denial attack in WSN [151].

3.22 Methods Based on Pattern Authentication

In conventional wireless security mechanisms, data transmission is encrypted by symmetric or asymmetric encryption algorithms. Wireless networks prefer symmetric algorithms to avoid complex and energy-wasting calculations. But encrypted data wastes energy even worse than sleep denial attacks. An anti-node can send the "garbag" encrypted datum to the receiver. This attack forces the receiver to decrypt, and the receiver spends a lot of energy reopening the code before realizing that the datum is "garbag". This processing keeps the node conscious for a long time; hence, an easy and fast cross-authentication pattern in integration with the MAC protocol is needed in order to counter the sleep denial attack [152].

In any generalized security mechanism of WBAN networks, sensor nodes must be awakened before receiving data and controlling security features. A practical plan should have a simple process to counteract the loss of energy of sleep denial attacks. The design of the security pattern at the upper layers may be integrated with the data link layer mechanism. In [153], an interlayer design of the integrated security model of the MAC protocol, called the two-tire energy-efficient security scheme (TE2S) is referred as possessing the ability to protect WBAN

networks from the attacks based on the initial framework presented in [154,155]. This interlayer scheme involves connecting two layers at design time without creating a new user interface for sharing information at runtime [58]. The design principles and features of this safe design are as follows:

• Energy conservation

• Low complexity

• Bilateral certification

• Symmetric cryptography

• Dynamic subsidence key generated with challenge text

• Ability to deal with sleep denial attack

• MAC protocol integration

Utilizing the hash chain which is used to generate the dynamic subsidence key, the proposed secure two-layer design can be used for cross-authentication and symmetric encryption keys. The only dynamic subsidence key calculations are hash functions such as MD5 or SHA-1 which are very simple and fast. With MAC protocol integration, there are no additional packages compared to existing MAC schemes. The two-tire scheme can check and stop attacks at different counterpoints. Combining the security process with low complexity and the design of multiple counterpoints can defend against attacks and put the nodes to sleep mode as quickly as possible. Security analysis showed that this scheme could withstand a replay attack, and energy analysis showed that this scheme was energy-efficient. It has also been successful in distributing energy. The results show a balance between energy conservation and security plans [156].

3.23 Mac Correction Protocols In WSN

B-MAC is an LPL-based wireless sensor network MAC protocol [157], which separates the transmitter and receiver with a time synchronizer. The receiver wakes up periodically to sense the preamble message from the sender and then receive and process the data. When the sender needs to send data, it sends a long preamble message

to make sure that the node receiver wakes up from its sleep period and receives it. Figure 3 shows the timeline of the B-MAC protocol that does not have an Ack and the receiver listens to it and waits for it to be completed by the sender. This plan is the long preamble message of the LPL protocol on both sides of the transmitter and receiver. This LPL protocol is the main energy consumer on both sides.

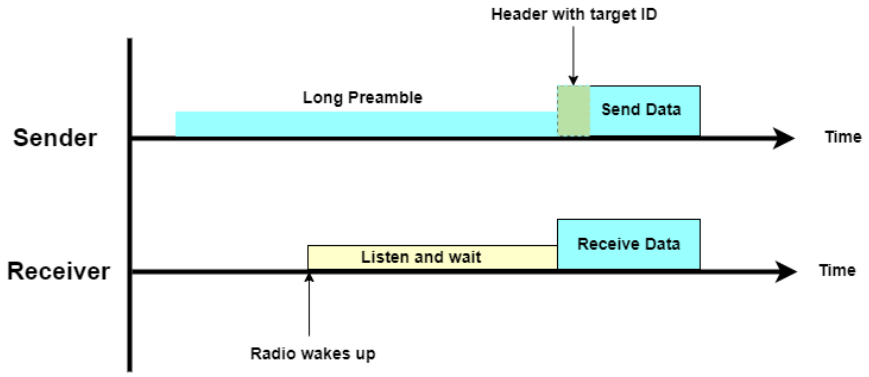


Figure 3 - B-MAC Protocol Timeline [158]

Through replacing the long short preamble in the B-MAC protocol [61], the X-MAC protocol has tried to make it more efficient. Figure 4 shows the X-MAC protocol timeline, in which the receiver sends an Ack message to the sender as soon as it receives the preamble message and does not wait so long for the sender to complete the preamble message. This scheme reduces energy consumption on both sides of the transmitter and receiver.

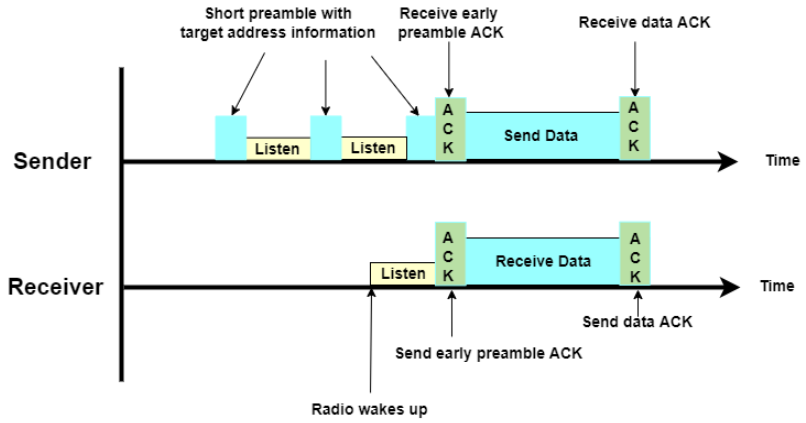


Figure 4 - X-MAC Protocol Timeline [158]

The RI-MAC protocol is a method proposed to minimize channel occupation time by a pair of transmitter and receiver [159]. Figure 5 shows the timeline of the RI-MAC protocol in which it allows the sender to send the Ack and related data to the sender as soon as the receiver realizes the sender's signals.

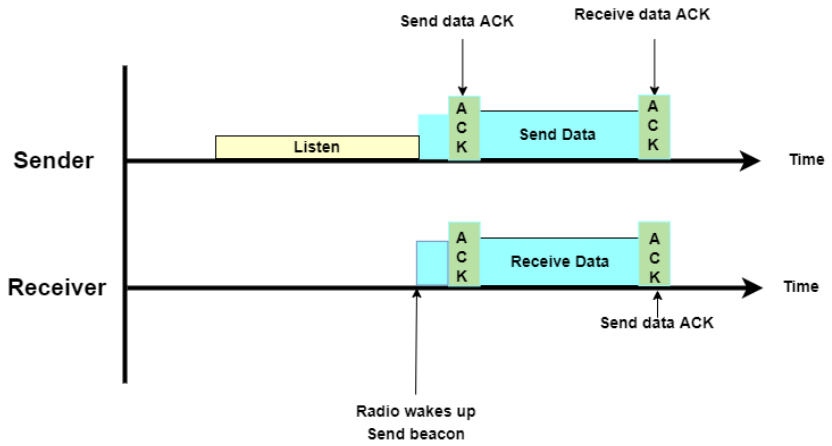


Figure 5 - RI-MAC Protocol Timeline [159]

3.24 Mechanisms For Optimizing and Reducing Energy Consumption in The WBAN Networks

There are various challenges and issues in the WBAN networks. First, sensors cannot fully monitor an entire area due to the limited sensory angle of them; second, the energy of the sensors is limited and their batteries are not easily rechargeable, especially in harsh environments. Therefore, energy conservation mechanisms that make optimal use of sensor energy have a great impact on extending the life span of the network [156,157]. In general, WBAN networks operate in such a way that most of the time they are in an idle mode and only occasionally send data. In addition, the amount of energy consumed to listen to the idle channel (unused) is equivalent to the amount of energy consumed when sending and receiving data. By using sleep / wake scheduling techniques and their effectiveness, energy loss can be reduced in idle (sleep) mode, which itself reduces the energy consumption of the sensors. The same is true of wireless body area networks. In sleep and wake scheduling, network sensors can have two states of being asleep or awake. When a node is in sleep mode, it is inactive and consumes very little energy, as opposed to a node that is awake and monitors the area it covers [157].

3.24.1 Sleep/Wake Timing Mechanism of Sensor Nodes

The sleep-wake timing mechanism of the sensor nodes has the advantage of reducing redundancy. This technique divides the sensors into several cover sets, each of which can monitor all points of interest. In addition, this technique determines the amount of time each cover set can be active. Cover sets are continuously active for a predetermined period. When a cover set is active, sensors belonging to other sensor groups become inactive. This increases the lifespan of the network to a great extent [158,159].

Benefits of using the sleep-wake schedule approach that extends network lifespan:

- Inactive sensors consume significantly less power than active sensors.
- The battery of a sensor will last longer if it is constantly switched between active and inactive mode.

3.24.2 Sleep / Wake Scheduling of Sensor Nodes Using Genetic Algorithms

John and his colleagues have proposed a method based on GA for scheduling sensor nodes in [160]. In the proposed method, individuals are defined in the GA. In fact, a binary two-dimensional array is used to define each person. Each element of this two-dimensional array can contain only two values of one or zero (0 or 1). The number 1 in each element indicates that the corresponding sensor node is active or awake, and the number 0 indicates that the corresponding sensor node is inactive or asleep. Each row of the 2D array represents a node in the WBAN network, and each column represents a period in which a specific cover set is active.

At the beginning of the algorithm, all individuals (chromosomes in the genetic algorithm) are created randomly. Two criteria are considered to evaluate each chromosome:

- Maximum environment coverage
- Optimization of energy consumption

Any chromosome that can achieve these goals to an acceptable extent will then be more suitable and have a better chance of being selected for the next generation. After evaluation, chromosomes should be selected for the next generation. In this article, the roulette cycle method is used to select chromosomes. The single-point

combination method has also been used for the combination operator. The proposed method based on GA has been able to provide acceptable results and perform better than similar previous methods [161].

3.24.3 Scheduling Sensor Nodes Using Learning Automata

presents a method based on learning automata for scheduling sensor nodes in WBAN networks. An automata learner is a machine with limited modes that can perform a limited number of operations. Each selected action is evaluated by a random environment and a response is given to the learner automaton. The learning automaton uses this response and selects its action for the next step. During this process, the automata learner learns how to choose the best action from its authorized actions [162].

In the method proposed by Meybodi and his colleagues, they have assumed that all sensor network nodes are the same and each network node can have two states: 1) active node 2) inactive node. The amount of energy consumption in the active state is much higher than in the inactive state. An automaton learner with a variable structure can be represented by quadrants {α, β, P, T} in which α = {α_1,… α_n} set of operations, β = {β_1,… β_n} set of inputs, P = {P_1,…, P_n} is the vector of the probability of selecting each of the operations and P (n + 1) = T [α (n), β (n), P (n)] is the automaton learning algorithm [163].

A: desirable response from the environment

$$P_i(n+1) = P_i \quad (n) + a[1 - P_i(n)]$$

$$P_j(n+1) = (1-a)P_i(n) \qquad \forall_j, j \neq i$$

B: undesirable response from the environment

$$P_i(n+1) = \frac{b}{(r-1)} + (1-b)P_i(n)$$

$$P_j(n+1) = P_j(n) \qquad \forall_j, j \neq i$$

In the proposed method, each node in the network is equipped with an automaton learner. The covering graph of the existing sensor network is then created according to the above definition. The number of the applications of each automaton is equal to the number of output edges of the covering graph related to the network. If n is the

number of output edges on the vertices of the graph, then the probability of each operation of this automaton is defined according to the following equation:

$$\forall_i \ P_i = 1/n$$

It is assumed that each node can communicate with all nodes within the communication range of that node. The range value for the edges between the vertices of the graph is also assumed to be as variable as the probability of link failure. This value is considered as a possibility during the simulation operation that the received response from the neighboring node is not correct or that the intrusion operation in the network is performed and the received packets by the malicious node in the network are sent to this node.

At this stage, the corresponding learner automaton starts with one of the nodes that can monitor at least one area, and this node selects one of its areas. Each node performs an exploratory search on the received packet when receiving the packet from its neighbors and follows the following rules [162,164]:

- Rewards the neighbors with the shortest distance from the hypothetical point according to the penalty (the neighbor who has the most coverage of the common areas with the node); and the other nodes (those who have the least coverage of the common areas or no common areas at all).
- If a node does not monitor any non-shared area, it will be penalized, while nodes that cover areas not shared with other nodes will be rewarded.

This stage continues until the number of learning repetitions stage reaches the maximum number of learning times. When the number of learning repetitions exceeds this value, the desired node selects the most likely edge from its output edges and uses it as the next node in the covering graph. Thus, with each implementation of the proposed method, a group of nodes is selected to cover all areas in WBAN networks. Selecting these nodes ensures the coverage of network areas.

3.24.4 Scheduling Sensor Nodes Using Phase Logic

Hakan Bugsy and his colleagues [159] have proposed a method for sleep/wake scheduling in phase logic-based WBAN networks. The method presented in this paper is centralized, i.e., all the collected data as well as the

calculations of how to cover the areas are performed in the central station. In this paper, two criteria or parameters have been used for phase construction, which is as follows:

• The average distance between live nodes and the main station

• Residual energy (in living nodes)

Three-phase states are considered for the remaining energy parameter. Each of these three modes is displayed as low energy residue, medium energy residue, and high energy residue. The next parameter is the distance between the live nodes and the main station. Three-phase modes are considered for this parameter including low distance, medium distance, and large distance (high).

After specifying the phase inputs, the phase output variables will be shown in Figures 6. In this figure 6, there are 9 phase output variables that are defined based on each of the parameters mentioned above. In fact, each of these nine variables indicates whether a sensor node is suitable or not for its manner of covering the environment. Accordingly, Table 4 shows the if-then phase rules. The if-then rules shown in the table below show how each node is scheduled.

Table4 - If-Then Phase Rules [165]

Distance to Base	**Residual Energy**	**Competition Radius**
Close	Low	Very small
Close	Medium	Small
Close	High	Rather small
Medium	Low	Medium small
Medium	Medium	Medium
Medium	High	Medium large
Far	Low	Rather large
Far	Medium	Large
Far	High	Very large

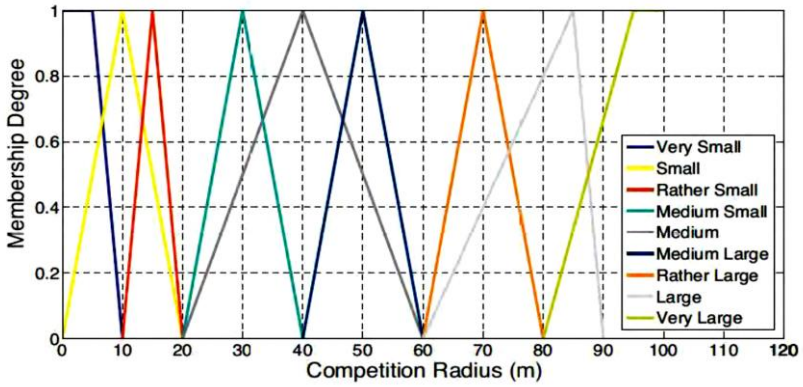


Figure 6 - Phase Output Variables Containing Nine Outputs [165]

3.24.5 Sensor Node Scheduling Using The Selection of Coordinator Node

Jay and his colleagues [56] have proposed a method based on sensor node scheduling to reduce energy consumption in physical WBAN networks. In this method, first, the coordinating node is selected based on the amount of workload in each node. The node with the lowest workload is selected as the coordinating node and announced to all other available nodes. The method of selecting a coordinator node is as follows [166]:

- Initially all nodes are considered coordinator nodes (labeled coordinator).
- If the nodes have more workload than (at least one node) of their neighboring nodes, then the coordinator node label is removed.
- For all nodes, the previous step is repeated and finally a coordinator node is selected.

The coordinator node announces itself as a coordinator node to all broadcast nodes of the network. Figure 7 shows the steps for selecting a coordinator.

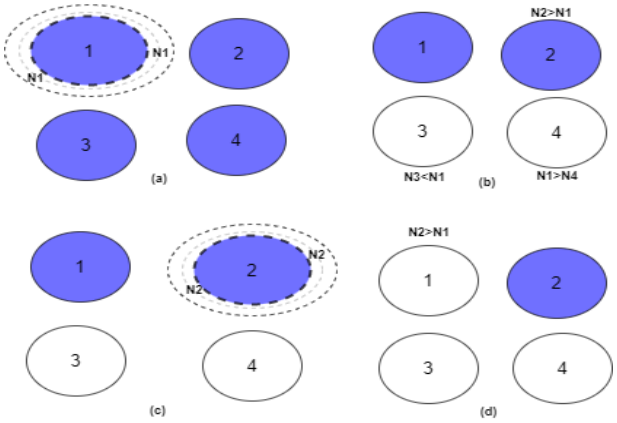


Figure 7 - Coordinator Selection Steps [166]

In this paper, a scheduling method is used to send data from nodes to the sink node. The coordinator node determines how other nodes are scheduled based on the following equation, and then the other nodes wake up according to this schedule and monitor their controlled area and send the data to the central station.

$$N_i = \frac{I_c}{I_i} \qquad I_c \% I_i = 0$$

$$N_i = \frac{I_c}{I_i} + 1 \qquad I_c \% I_i \neq 0$$

In the above equation, N_i shows the node i. I_c is the time allocated to the coordinate node and I_i is the time allocated to the i-node, at which time it can monitor the area and send data to the central station. The method of connecting network nodes and sink node is shown in Figure 8.

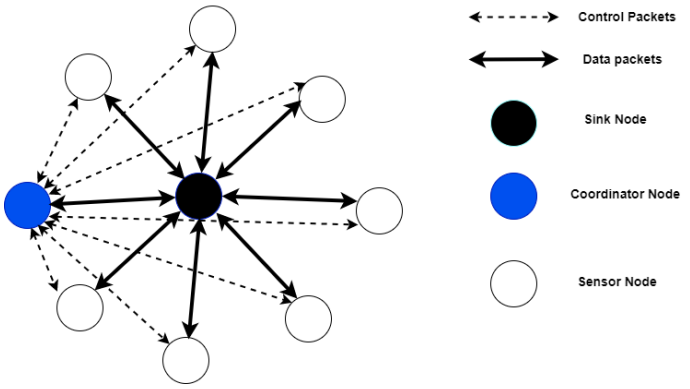


Figure 8 - The Connection of Network Nodes and Sink Node [166]

3.24.6 Heuristic Method For Nodes Scheduling in Physical WBAN Networks

The authors in [158] have proposed a covetous algorithm for sensor nodes scheduling in wireless sensor networks. As mentioned earlier, due to the limitations of sensor nodes, the algorithms proposed for conventional wireless sensor networks may not be applicable to physical wireless sensor networks. In the above article, first, the cost function is modified to be able to evaluate the distribution of the sensor path instead of the sensor. This is because each sensor can only monitor a part of a coverage area in a single time unit. Second, the algorithms have been modified in a way to avoid selecting more than one path and one sensory range of each sensor to build a cover set. Third, the function is added to the algorithms to improve their performance by eliminating redundant sensory areas (if any). In this algorithm, the network operation enters several stages (the number of stages depends on the sensor selection strategy) and the output of each stage is a cover set that can monitor all areas as well as presenting appropriate timing for the sensor nodes. Once a cover set has been established, an appropriate activation time is assigned to the cover set at the upper bound of the given data to maintain the possibility of a solution. The process of turning on and setting the cover sets continues until all areas of the cover set are completed. The following description describes the algorithm in detail.

In the above article, the heuristic scheduling algorithm is such that this algorithm organizes a maximum of one cover set at a time. A cover set refers to the nodes that are placed in a set to wake up at a specific time. Each cover set is created so that it can be used to schedule sensor nodes. Initially, the algorithm starts with an empty cover that monitors all areas. Then, it proceeds with the highest coverage distribution among all the candidates. Accordingly, the list of uncovered areas is provided by removing the areas which are updated by the sensory navigator. This process continues until all monitored areas have been completed. Once a cover set has been established, the maximum possible set time of the cover set is updated based on the remaining lifespan of the sensors in the cover set. Empty sensors are then removed from the list of sensors. The process of creating a new cover set continues until all the desired areas are covered.

3.24.7 Adjusting The Sensory Range of Sensor Nodes

Another technique to increase network lifespan is to adjust the range of sensor nodes. This technique helps the sensor save its energy when it needs to monitor the points around it. The smaller the sensory range of the sensor nodes, the less energy it will consume; In contrast, the larger the sensory range of the sensor nodes, the more energy it will consume [167].

The range-setting technique evaluation (such as sensors with different energy levels) has the potential to extend network lifespan. This is because this technique increases the number of possible cover sets that can cover the entire area.

3.24.8 Efficient, Cost Effective, and Optimal Energy Design of The WBAN Networks

In this article [168], a model for WBAN network is presented, which is based on relay nodes. By presenting this model, an attempt has been made to change the network topology by adding relay nodes and managing their method of placement in the network so that energy consumption and start-up costs are reduced. The authors of the article have named their model EAWD; the general objectives of which are as follows [168]:

- Determining the optimal number for relay nodes that are placed in the network.
- Optimal detection of relay nodes to several sensors
- Network routing optimization

The architecture introduced in this paper is such that the network consists of three new sensors, relays and sink nodes in such a way that sensors sense the information of the disrupted parts of the body and send the information to the sink nodes through the relay nodes.

3.24.9 An energy efficient method for reliable and Secure Data Transmission in The WBAN Networks

In this article [169], the authors have tried to provide a solution for transmitting messages safely and securely by considering the energy efficiency of the sensors to the medical server that can be seen by medical personnel. The goal is to securely transmit data packets and provide a routing protocol called RelAODV [170] to improve network reliability. This article seeks to ensure the security requirements, data confidentiality, data validation, data

integration, and data novelty protection. The article focuses on packet-driven and event-driven methods for the sake of reliability.

3.24.10 Improving The Energy Efficiency of Cooperative Communications Based on Incremental Relays in The WBAN Networks

In [171], the energy efficiency in a participatory communication scheme is investigated, which is based on placing relay nodes in the network in an incremental way. Three communication schemes are considered: direct communication, one-relay partnership and two-relay partnership. In the first scheme, only a direct communication between the origin and the destination is possible. In the second case, a two-phase participatory protocol is considered in which a relay node helps the data transfer from the origin to the destination. In the third case, a three-phase participatory protocol is considered. In this part, there are two relay nodes to help the origin. Closed error rate and energy efficiency of this method have been tested. The simulation and evaluation results show that the participatory communication scheme based on the addition of relay nodes has significantly improved energy efficiency and reliability compared to the direct communication between the origin and the destination.

3.24.11 M-ATTEMPT Routing Protocol

This protocol uses a multi-step routing scheme for heterogeneous networks in the body area [151]. This protocol uses direct communication to route and send data when emergency data or solicited data is requested while the connection is multi-step for delivery. One of the main challenges of this protocol is the heat generated by the sensors.

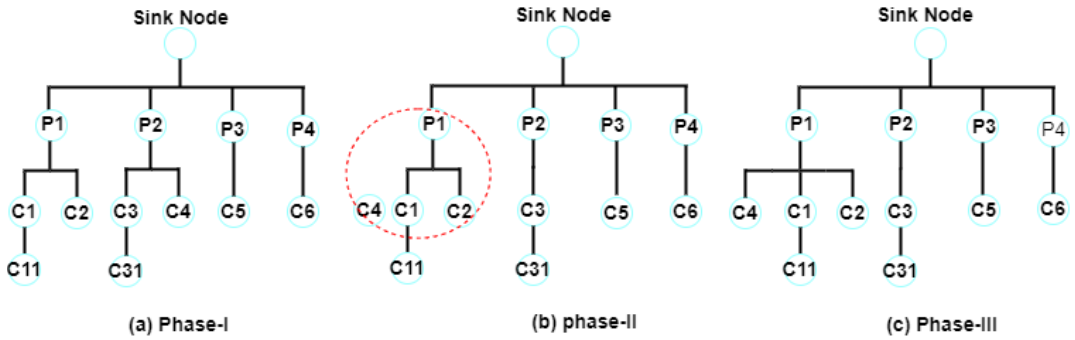


Figure 9 - Execution Steps of M-ATTEMPT Protocol [151]

According to figure 9, all nodes broadcast a greeting message in the initial phase of this protocol. This message contains neighbor information and the distance of the nodes to the sink node. In this way, all nodes know their neighbor and the location of the sink node. Also, accessible node-to-sink node routes are determined. The second phase of this protocol is implemented by calculating the paths with a smaller number of steps to the sink node. The path with less steps is selected as the data transmission path.

3.24.12 SIMPLE Routing Protocol

A reliable and efficient SIMPLE protocol has been proposed in order to increase the routing power of wireless networks in the body area. In this protocol, we want to minimize energy consumption and maximize network lifespan by using multi-step technology [153]. The protocol proposes to use a cost function to select the parent node or data carrier. The goal is to select the parent node whose cost function has the highest amount of energy and the shortest distance to the sink node. In this protocol, after placing the sensors on the human body and in order to identify the position of the sink node on the body, a message containing the spatial information of the sink node on the human body is disseminated to the public. Through receiving this information, each sensor becomes aware of the position of the sink node, and a package containing information about residual energy disseminates the distance to the sink node. By doing this, each sensor becomes aware of its neighbors. The sink node selects a node as the parent node (forwarder) based on the information that it receives from all the sensors and by calculating the cost function which is resulted from the following equation [153]:

$$C.F(i) = \frac{d\ (i)}{R.E\ (i)}$$

In this relation d (i) is the distance of node i to the sink node and R.E (i) is the energy of node i.

The sink node selects a node as a forwarder according to the calculation of the cost function of each node. The node with the most residual energy and the shortest distance to the sink node is selected as the forwarder node. After selecting the forwarder node, all nodes send their information to it and the forwarder node transfers them to the sink node at specified intervals.

3.25 Hierarchical Power Optimization Routing Protocol (HPOR)

The purpose of this protocol is to improve energy and high routing power for body area networks. In this protocol, we minimize energy consumption and maximize network lifespan by hierarchical routing [154]. In this protocol [172], one node collects data from the other nodes as a CH and then sends it to the base station. In this protocol, the basis of work is the use of energy in a clustering scheme based on the minimum control rate for data transfer. In this method, the sensors divide the network into clusters and each cluster receives one CH. The CH manages the connection of nodes with the base station. Therefore, the sensor nodes are no longer directly connected to the base station.

3.26 Horizontal Moveable Energy-Efficient Adaptive Threshold-Based (HEAT)

The approach of using the wireless network of the body area in a health care program is very limited which is currently in use. The purpose of the proposed protocol (adaptive power protocol to save energy by horizontal displacement) is to move the routing movement horizontally over the body, using direct communication for emergency data and multi-step communication for normal data [155]. This protocol increases the lifespan of the network and provides the best period of stability in which the human body is assumed to move horizontally while walking, and the sink node is placed on the abdomen. When the human body is in a fixed position, the nodes are arranged according to a table. The position of the nodes is shown in Table 5 in which each node is placed on the human body according to the distance.

Table5 - Position of Nodes on the Body [155]

Node No.	X Coordinate (CM)	Y Coordinate (CM)
1	40	90
2	60	90
3	50	60
4	50	60
5	50	30
6	50	30
7	50	08
8	50	08

All nodes are located in different parts of the body and they send their data to the sink node due to the displacement of the human body. For example, nodes 1 and 2 are on the chest and nodes 3 and 4 are on the arms. In this method, there are two types of data namely critical and normal. Direct data connection to the sink node is used in critical times and multi-step communication is used to send data in normal times.

3.27 Routing Protocol of Ant Genetic Algorithm

One of the most important issues that can be addressed in the sensor networks of the body is the energy consumption of the nodes. Since the nodes have battery limitations, it is not possible to replace and charge it or in other words, it has a difficult process. Therefore, in order to optimize energy consumption, proper routing and long life of nodes in the network are required. In this algorithm, it has been proposed the idea of using the genetic mechanism of ants so that the routing process in sensor networks of the body area will be possible [156]. The proposed algorithm consists of two phases. In the first stage, the energy-aware routing algorithm (DEAR) is proposed. The purpose of this stage is to interact the amount of total network energy in the sensor networks of the body area to maximize the lifespan of the network. In the second phase, the GACA algorithm [173] is proposed. The purpose of this algorithm is to select the optimal path through ant GA. Figure 10 shows the architecture of this proposed algorithm.

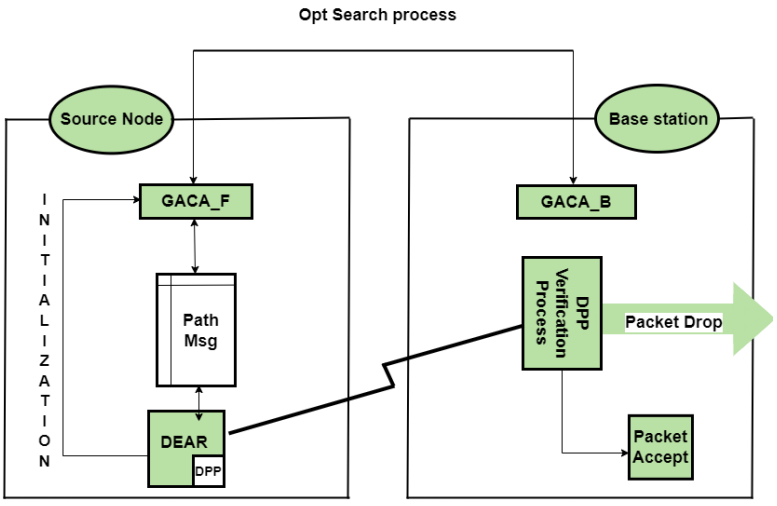


Figure 10 - The Proposed Algorithm Architecture in WBAN Networks [156]

Considering the shape of the ant GA, it is suggested to search for an optimal path from the origin to the base station. There are three types of packages in this scheme: data packages, ant packages, and neighbor packages. Data packages are those that are referred in the sensor network. This algorithm has nothing to do with the contents of this package, and only the ants move this package back (GACA-B) and forward (GACA-F). These packages are for updating the routing table. These packages consist of 4 sections: destination addresses, initiation time, destination arriving time, and a stack of nodes that passed through them. The information in this package is stored for control.

3.28 Conclusion

In this chapter, many methods and mechanisms are presented to deal with security challenges, such as preventing DoSL attacks, as well as the ways to deal with routing and energy consumption challenges. With a more detailed investigation, we came to the conclusion that to reduce energy consumption in WBANs, different methods such as energy-aware routing and efficient communication protocols are needed. Furthermore, to design a secure WBAN, the use of strong cryptographic algorithms is required so that the network can send and receive data in a safe and secure manner. According to the mentioned cases, to secure the WBAN and reduce energy consumption, we presented the methods that make the designed WBAN secure.

VICTORIA UNIVERSITY

THE NEW WAY TO DO UNI

OFFICE FOR RESEACH TRAINING ,QUALITY AND INTEGRITY

DECLARATION OF CO-AUTHORSHIP AND CO-CONTRIBUTION: PAPERS INCORPORATED IN THESIS

This declaration is to be completed for each conjointly authored publication and placed at the beginning of the thesis chapter in which the publication appears.

1. PUBLICATION DETAILS (to be completed by the candidate)

Title of Paper/Journal/Book:	M. Yaghoubi, K. Ahmed and Y. Miao, "TIDS: Trust Value-Based IDS Framework for Wireless Body Area Network," *2022 32nd International Telecommunication Networks and Applications Conference (ITNAC)*, Wellington, New Zealand, 2022, pp. 142-148, doi: 10.1109/ITNAC55475.2022.9998329.
Surname:	Yaghoubi
First name:	Mohammad
Institute:	Institute for Sustainable Industries and Liveab
Candidate's Contribution (%):	70%
Status:	
Accepted and in press:	
Date:	
Published:	✔
Date:	NOV 2022

[redacted]

2. CANDIDATE DECLARATION

I declare that the publication above meets the requirements to be included in the thesis as outlined in the HDR Policy and related Procedures – policy.vu.edu.au.

MOHAMMAD YAGHOUBI Digitally signed by MOHAMMAD YAGHOUBI	14 Nov 2022
Signature	Date

3. CO-AUTHOR(S) DECLARATION

In the case of the above publication, the following authors contributed to the work as follows:

The undersigned certify that:

1. They meet criteria for authorship in that they have participated in the conception, execution or interpretation of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;

3. There are no other authors of the publication according to these criteria;
4. Potential conflicts of interest have been disclosed to a) granting bodies, b) the editor or publisher of journals or other publications, and c) the head of the responsible academic unit; and
5. The original data will be held for at least five years from the date indicated below and is stored at the following **location**(**s**):

Name(s) of Co-Author(s)	Contribution (%)	Nature of Contribution	Signature	Date
Mohammad Yaghoubi	70%	Concept, Methodology, Experiment, Result Processing, Draft	[redacted]	16/11/22
Khandakar Ahmed	20%	Concept, Validation, Review, Proof Read		15/11/2022
Yuan Miao	10%	Review, Proof Read		15/11/2022

CHAPTER 4 Research Methodology Design

4.1 Introduction

Nowadays, life is unimaginable without wireless communication. Advances in CMOS technology and the creation of smaller and smaller circuits have made it possible to use wireless circuits in most of electronic devices. This development has also led to the development of micro-sensors. These micro-sensors can perform countless sensations in tasks such as sound detection in order to sense an earthquake. They also provide information gathering in remote areas and places that are not appropriate for human explorations. Cars can use wireless micro-sensors to control engine status, tires pressure, and oil level, etc. Assembly lines can use these sensors to control the production process. In strategic situations, micro-sensors can be released by aircraft on enemy lines and then used to track a target (such as a car or a human). In fact, the main difference between these networks is their relationship with the environment and physical phenomena. Traditional networks provide communication between humans and databases, while the sense / work network communicates directly with the physical world, using sensors to observe the physical environment, and make decisions based on their observations, and perform appropriate operations. Wireless sensor network name is a general name for different types that are designed for specific purposes [174].

Traditional networks provide communication between humans and databases, while the sensor network is directly connected to the physical world. Using sensors, they observe the physical environment, make decisions based on their observations, and perform appropriate operations. Wireless sensor networks are made up of small nodes with sensing, processing, and computing capabilities. Recent advances in the technology of creating integrated circuits in small sizes on the one hand and the development of wireless communication technology on the other hand have paved the way for the design of wireless sensor networks. Recent advances in electronics and wireless communications have caused the ability to design and generate sensors with low power consumption, small size, reasonable price and various applications. These small sensors, which can perform functions such as receiving, processing and transmitting various environmental information based on the type of sensor, have given rise to the idea of creating and expanding networks called Wireless Sensor Networks (WSN). A sensor network consists of many sensor nodes that are widely distributed in an environment and collect information from the

environment. The location of the sensor nodes is not necessarily pre-determined. Such a feature makes it possible to leave them in dangerous or inaccessible places.

On the other hand, this means that sensor network protocols and algorithms must have self-organizing capabilities. Another unique feature of sensor networks is the ability to cooperate and coordinate among sensor nodes. Each sensor node has a processor on its board, and firstly it performs a series of basic and simple processes on the information it has obtained instead of sending all the raw data to the center or to the node that is responsible for processing and concluding the information, Then, it sends the semi-processed data. Although each sensor itself has low capability, the combination of hundreds of small sensors offers new opportunities. In fact, the power of wireless sensor networks lies in their ability to use many small nodes that can be assembled and organized themselves, and can be used in a variety of applications such as simultaneous routing, environmental monitoring, or health monitoring of structures or system equipment. The wireless sensor networks range of use is very wide and ranges from agricultural, medical and industrial applications to military ones. One of the most common applications of this technology is to monitor a remote environment. For example, chemical leak in the environment of a large factory can be monitored by hundreds of sensors that automatically form a wireless network; and the center can be also notified immediately when a chemical leak occurs.

One of the main applications of these networks is related to environments in which humans cannot be present, such as the ocean floor or military sites due to the presence of the enemy or nuclear and chemically contaminated environments. The smallest example of a hardware implementation is the Smart Dust Sensor nodes [175], which is a cubic millimeter node. But efforts are still being made to make them so small that they can be suspended in the air and floated by airflow and send the sensed items for hours or days. Security is a critical issue in some military applications, for example, making network wireless communication becomes more difficult for security measures. One of the weaknesses of the sensor network is the lack of energy source, and the enemy causes the neighboring nodes to step out of sleep mode for no reason by settling an intruder node that regularly generates high-energy wake-up messages. Keeping of this process on wastes the energy of the nodes and shortens their lifespan. Due to the limitations, simple and efficient solutions should be sought based on the nature of the sensor

network. For example, high-density nodes can be distributed and each node has little information or the data is valid for a short period of time. These features can be used as a strong point in solving security problems. There are basically many challenges ahead of sensor network security, and research topics in this area are extensive and complicated.

According to the issues mentioned in this chapter, the IDS-Agent methodology has been presented to increase the security of DoSL attack penetration detection and a genetic algorithm-based clustering phase to reduce energy consumption.

4.2 Statement of The Problem

The security of the Wireless Body Area Network (WBAN) has become a significant issue due to the rising usage of it. As the usage of sensors grows in different domains, the various attacks that threaten them also increase day by day. An attack detection system is one of the main and effective defense methods against attacks in the wireless body sensor networks. Denial of Service (DoSL) attack is one of the attacks in this domain, which is a special type of service denial attacks. A DoSL attack is one of the major known attacks on WBAN networks. It is the most dangerous type of attack that targets the sensor nodes energy and leads to the death of the node. DoSL attacks can be divided into six categories according to the policy pursued by the attack [176]:

• Sleep deprivation attack

• Dam attack

• Synchronization attack

• Replay attack

• Collision attack

• Global broadcast attack

In the DoSL attack, the attacker's main goal is to increase the energy consumption of the sensor. Accordingly, the lifespan of the sensor node and consequently the lifespan of the whole network is reduced and its efficiency is

severely reduced. This attack does its job by creating preoccupations for the sensor node and preventing it from remaining dormant. Therefore, the energy of the sensor nodes is wasted and this leads to deprivation of services through sleep deprivation. Due to the impossibility of replacing the battery or supplying the sensor energy through other ways, sleep deprivation attack is a very destructive one in wireless sensor networks. A dam attack forces its victims to expend more energy by making legitimate demands. In both attacks, due to the influx of torrential requests, the sensor node does not have a chance to rest and its energy is severely dwindled. The purpose of the synchronization attack is to create a problem in the related time of synchronization in MAC layer. Synchronization attack detection is very difficult because it remains within the protocol. A replay attack is a security breach attack in which data is stored without authentication and then resent for deception in order to dwindle the receiver's sensor energy. In a global broadcast attack, in addition to the global broadcasting of unnecessary data, unauthorized traffic is imposed on the network, which causes energy loss and reduction of the sensor nodes lifespan and thus the network. This type of attack is difficult to detect because it does not affect the throughput of the network which is an indicator of an attack to the network. A collision attack can be triggered by an endangered node that does not follow environmental access control protocols. Collision with the transmission packet of the neighboring node is done by creating a short noise packet and sending it. Many methods have been proposed to solve this problem based on definite models. But in the wireless body area networks, changes are instantaneous and indefinable. Therefore, the use of indefinite and exploratory methods in detecting and counteracting the attack can be effective [176].

4.3 Challenges of Denial-of-Service Attack

In this section, we intend to examine the challenging points that can be an effective help for researchers in order to present new ideas in this field.

There are several ways to prevent denial of service attack. But the most fundamental way is authentication. In order to prevent denial of service attacks, the node needs to be authenticated and authenticated to change asleep or dormancy status so that the synchronization message received from the authenticated node is accepted. WSN node security can be compromised when authentication is performed using symmetric keys and hash functions.

Any malicious node that has access to the symmetric key can also access the information of the station. When main station data is available to malicious nodes, the entire WBAN will be compromised. This can be addressed using the challenge-response protocol. In challenge-based authentication, the claimant is forced to disclose its original identity to the identifier in order to prove itself. In such a situation, if the identifier is vulnerable, whatever information the receiver receives from the claimant node can also be accessed by the malicious node. When such information is available to the attacker, the attacker can prove to be a normal node to the identifier and have access to confidential information. In sensor networks, the central station is considered a sensitive and vital resource that must be protected. Any data that reaches the central station should not be disclosed to other nodes. This data can be used by a malware which acts as a central station and collect all the data from the cluster tab. In zero-knowledge-based authentication, the claimant's secrets are never shared directly. The claimant's secret key is used to calculate a value that can be used for the interaction between the claimant and the identifier for authentication process. Zero-knowledge protocol is a very powerful encryption technique that uses a challenge created by the identifier and is very difficult to be dismantled. Therefore, it can be used in many cryptographic applications and operations such as recognition, authentication, key exchange, etc [177].

The following section proposes an intrusion detection algorithm to identify intruder nodes (malicious nodes) in the wireless sensor network. Using this method, the problem of discharging the energy source of the sensor nodes can be solved. The proposed method is composed of three phases. The first phase is clustering and CH selection by using LEACH clustering algorithm. In this phase, that sensor which has more energy than the others is selected as the CH . The second phase is the path selection for sending and receiving data between nodes within the cluster and the CH sink nodes by the AODV routing protocol. And the third phase is to detect the DoSL node. In this phase, malicious nodes are detected based on IDS factor, pre-distributed random key, a random password, and a trust value.

4.4 Methodology and Conceptual Framework

In this section, the methodologies and conceptual framework covering the research design and approaches for collecting and analyzing the data were explained in more detail. This section also addressed the research problems, research approaches, and the feasibility of the research design.

4.4.1 Scientific Approaches

This study contained three methodologies integrated for improving the ultimate performance of the WBANs.

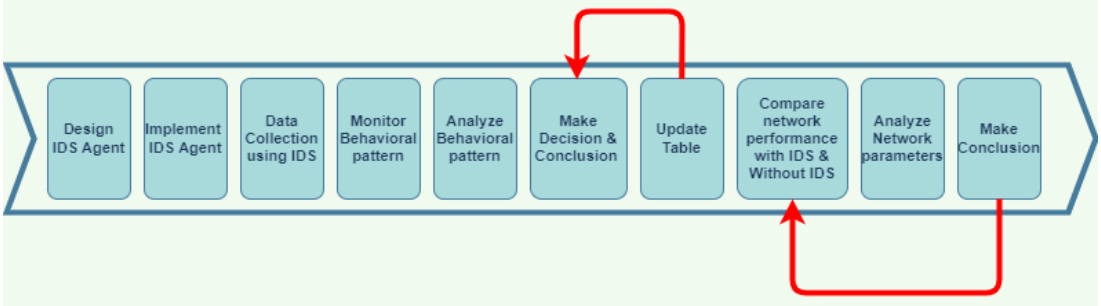


Figure 11 - Scientific Approach

4.4.2 IDS Implementation

This hybrid methodology was outlined as follow:

1). IDS Agent: in this section, an IDS agent was developed to recognize the network nodes intruded inside the WBAN network. This approach overcame the depleting battery issues due to DoSL. To identify the malicious nodes, various types of components engaged in the detection process were as the following:

- Sensor agent: it is an independent program operating continuously on a cross-sensor platform that observes data packets for detecting suspicious activities to empower this autonomous system (Sensor agent).
- The pre-distribution key for sensor nodes:

In this research, random secret keys were needed to be distributed among nodes to identify the legitimate nodes in order to build up a safe network. Firstly, a pool was needed to distribute the key. This pool contained all the keys needed to be distributed among the nodes. The pool was developed inside the IDS, and the keys inside were distributed among the nodes whenever needed. Each node possessed a ring capable of holding several keys. The

distributed keys were irreplaceable and irreversible, meaning that when a key was distributed, it did not return to the pool, and no new key was added to the pool to replace the distributed key. For each key added to the keyring, a time tag was attached to its structure when it was created. When sharing a key between two nodes, each node inspected the key generation time, and the one with the least time value (the newest key) was chosen as the shared key. If there were keys with the same time value, the key with the highest key ID was selected.

Note: When sharing a key between two nodes, the shared key was selected from among the keyring of the node that commences the communication.

- Password Generator

One random password needed to be generated to identify an event between nodes. Whenever each sensor node commenced the initiation phase, the random password generator provided a new password, which was a random value. The IDS table structure contained a node ID, random value, password generation time, and expiration time. In this table, by exploring the previous random password histories, the password generator supplied a new one-time password (OTP).

Once it was created, the generated password linked a communication channel between two nodes, lasting 60 seconds after generation.

If another connection was required, the node needed to generate a new password, even if the previous password had not been expired. Every random password is made up of 10 characters. The characters used in the password include uppercase, lowercase, and numbers.

- Trust value

The network was run approximately 20 times for finding the PDR and RREP packets. then Max and Min amount of these parameters were selected. After normalization, the range between 0.98 - 1 was selected as the trusted area. This trust value was inserted statically as the static route in AODV routing table which accelerated routing process.

- IDS Agent Data-Base

This DB included Node-ID, and Random Password, Keys, Node’s energy level.

- Intruder table

This table archived the attackers' identification nodes.

- Random password Generator table

Table6 - Random Password Table

Expiration Time	Generation Time	Random Password	Node ID
T1 + 60 seconds	T1	…….	A

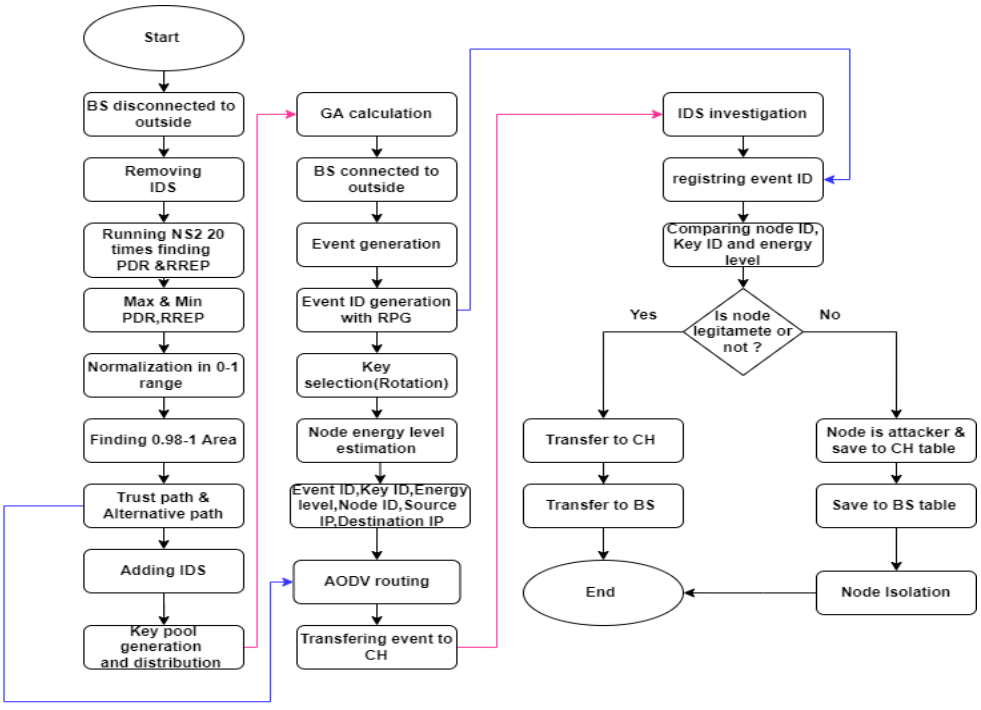


Figure 12 - IDS Agent Flowchart

- BS database

Base station developed this database after sending an inquiry to the IDS agent database to record attacker nodes.

Table7 - BS Database

CLUSTER HEAD IDENTFICATION	ATTACKER IDENTFICATION
CH3	N2
CH2	N9

2) Genetic-Based Algorithm

GA starts with a wide range of solutions named initial population. Each solution is called a chromosome. The fitness function computes the fitness score for each chromosome. Two-parent chromosomes are randomly selected for a crossover, followed by a mutation to achieve a better solution. This procedure repeats until the elite node is identified as the CH based on the minimum distance to the BS and maximum energy [178].

In this paper, the formula below was used to calculate the energy expected for transmitting and receiving packets [179]:

$E_{send} = E_{trans} * s + E_{amp} * d^2$

$E_{receive} = E_{recv} * s$

$Etrans$ represents the amount of used energy for sending data, S represents the message size (per packet), d indicates the message transfer distance, and $Eamp$ indicates the energy consumed in the signal amplifier, and $Erecv$ represents the energy required for receiving a bit of data.

Note: Important network parameters for running the simulator:

Number of Nodes, Network Area, Size of Population, Length of the chromosome, Crossover Rate, Mutation Rate, Initial Energy, Data packet Size.

3) Intra-Cluster Routing

As the present research dealt with dynamic topology and potential time-sensitivity issues, AODV was an efficient intra-cluster routing protocol.

The advantage of the AODV protocol was utilizing the least congested route rather than the shortest one [180]. It also allowed a path that consumes less energy selected by computational processing. This protocol also reacted to the topological changes impacting active paths. Based on the above-mentioned benefits of AODV, the study employed this routing protocol to route the data between WBAN nodes.

4.4.3 AODV Implementation Steps

1. Sending RREQ control package as broadcast by the source node to its One-Hop neighbors

2. Receiving the REEQ control package by neighbors

3. Receiving the RREQ package by the destination

4. Sending Unicast RREP by destination to the source of the route

5. Receiving the RREP package in the middle of the source

6. Creating a path between the source and destination nodes

7. Recording the new route in the source routing table [181]

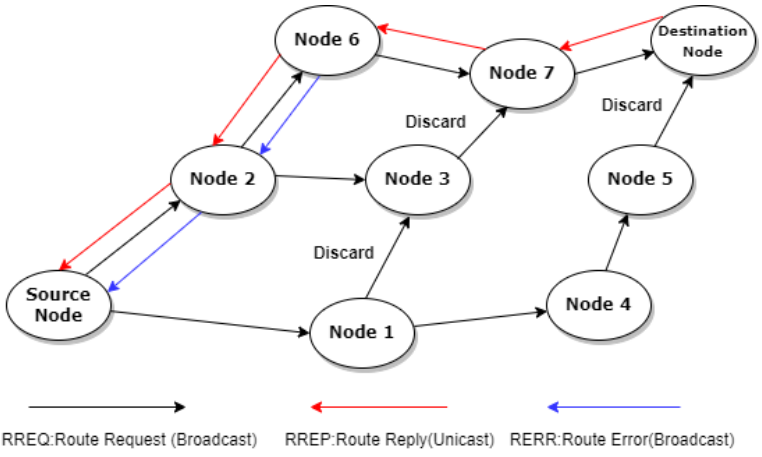


Figure 13 - AODV Routing [182]

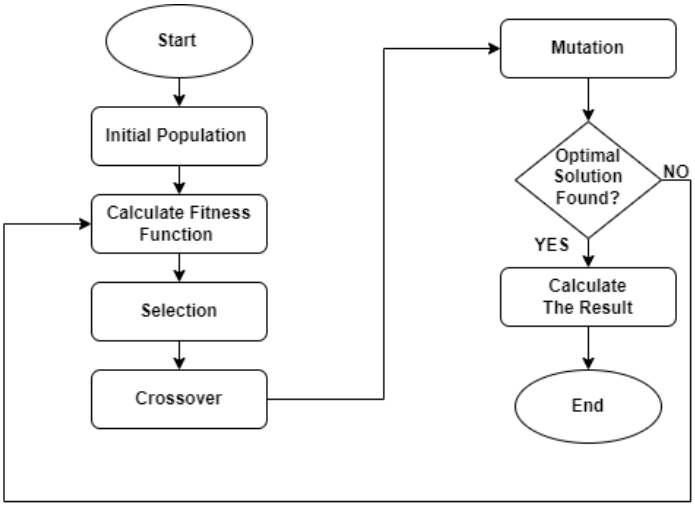


Figure 14 - Flowchart for GA-Clustering [183]

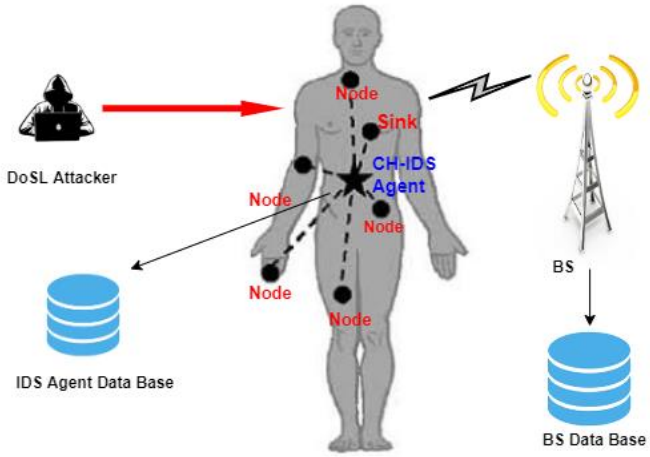


Figure 15 - Conceptual Design

4.5 Data Collection

The worldview in this research project was positivist. Because of this worldview paradigm, the project was intended to obtain factual knowledge through calculation, verification, and measurement. The approach in this research was deductive for developing and testing hypotheses.

Mono methods were used to carry out this study. The proposed IDS Agent collected data from respective network components upon implementation in the WBAN system. Following where and how the data were

processed in this research, multiple network components such as BS, CH, and IDS collected data. However, the security analysis process was conducted centrally by an IDS agent. Furthermore, it was preferred to hire direct monitoring to obtain data directly from the appropriate source before analyzing. Direct monitoring allowed the accuracy to reflect in the host, and every single incident report to occur in IDS agent coming up with minimum delay amongst sensor nodes along with ease of modification or implementation in any programming language. It should also be added that other public datasets were used for developing other parts of the research project.

4.6 Quantitative

In this research, all on-body sensor nodes were mounted with Radio Frequency (RF) and Transceiver to forward or relay patients' physical and physiological data. During the initial phase, BS collected the information about the distance and energy of distributed nodes. To improve the network's performance, the BS processes the suggested GA to allocate CH to all nodes. Later, AODV was considered the node's parameters to compute the shortest path between nodes.

It can be claimed that the IDS agent in this study collects data through direct observation of nodes instead of passive monitoring through recording audit logs.

4.7 Data Analysis

For analyzing and simulating network parameters in this research study, the Network Simulator version 2(NS2) was selected. It was an object-oriented network simulator, written in C++ and OTcl language. It simulated a variety of network parameters. Being open-source and allowing customization or modification of codes were the main reasons for selecting NS2 in this research. However, poor GUI support was the main drawback of this simulator. Other simulation tools for mimicking network traffic behavior like QuaNet and OPNET were rejected in this study due to being available only for commercial uses and not supporting open-source codes.

4.7.1 Network Simulator Parameters

The performance of the proposed research study was compared with an intruded network without IDS. Below is the list of network simulator parameters:

- Number of Nodes
- Crossover Rate
- Network Size
- Chromosome Size
- Mutation Rate
- Energy level
- Packet Size
- Type of Selection

This project was simulated with a hypothetical network with 10-15 nodes, the initial energy of 10 joules, simulation space of 180 cm by 40 cm, simulation run time of 50-300 seconds, assuming the installation of a node on a body. In executing this simulation, which is done as trial and error, the number of read-and-write processes is random in each execution, which directly affected the volume of the database. However, the utilizable volume of the database also changed owing to the expiration time of each event. A small portion of the database volume might be occupied during the simulation.

In this simulation, the used sensors were sensitive to temperature, heartbeat, respiration rate, etc., which were placed on the body.

It should be noted that to test the performance of the proposed method in this simulation, the proposed method was first compared to a method without the IDS, and the accuracy of the proposed method was measured. Then in the next step, the proposed method was benchmarked and compared with a similar method.

4.8 Analyzing The Simulation Results

After running the simulation phase, it was expected that the proposed method would have higher efficiency in comparison with a network without IDS based on the mentioned network parameters. At this stage, the effectiveness of this research was evaluated by considering the critical metrics as follow:

- PDR

Packet delivery rate could be estimated as PDR=DP received/DP sent (Total number of data packets received and total data packets sent successfully, respectively)

- Delay (D)

In this experimental research, the numerical end-to-end latency was calculated as follow:

Delay [i] = Receiving time [i] - Sending time [i].

- Normalization [184]

$Z = \frac{X - Xmin}{Xmax - Xmin}$

- Energy

The following model was used to measure energy consumption for the current research. The energy consumed by the nodes includes the energy used to send and the energy used to receive information. The energy required to send; is per Equation 1, and the energy required to receive data by the node is per Equation 2. The proposed energy formula was as follows [185]:

1. $E_{send} = E_{trans} * s + E_{amp} * d^2$

2. $E_{receive} = E_{recv} * s$

E_{trans}, is the amount of energy consumed to transmit data, S is the message size (per packet), d is the message transmission distance, and $Eamp$ is the energy consumed in the signal amplifier. E_{recv} is the energy required to receive a bit of data.

- Throughput

Throughput is the rate (In bps or packet per second) at which packets or bytes are successfully delivered over the network nodes in a specific period.

The reason for the throughput measurement in this research study was that network protocols often want to choose the maximum data rate in a communication link between nodes.

The following equation calculates how to estimate throughput in the wireless sensor network, which is usually based on kilobytes per second:

$X = C / T$

X: Represents the number of successful packets per second

T: Represents the total time that system has been monitoring the packet delivery (Second)

C: Total number of successful packets transmitted (number)

- Accuracy

The following function predictions were considered to foretell the accuracy of IDS Agent and to measure the precision of this research [186]:

Table 8 - Detection Rate Formulae [186]

$\mathrm{DR} = \frac{\mathrm{TPR}}{\mathrm{TPR} + \mathrm{FNR}} * 100$
$\mathrm{FPR} = (\frac{\mathrm{FPR}}{\mathrm{FPR} + \mathrm{TNR}}) * 100$
$\mathrm{FNR} = \frac{\mathrm{TPR} + \mathrm{TNR}}{\mathrm{ALL}} * 100 \ , \mathrm{All} = \mathrm{FPR} + \mathrm{FNR} + \mathrm{TPR} + \mathrm{TNR}$
$\mathrm{TPR} = \frac{\mathrm{TPR}}{\mathrm{TPR} + \mathrm{FNR}} * 100$
$\mathrm{TNR} = \frac{\mathrm{TNR}}{\mathrm{TNR} + \mathrm{FPR}} * 100$

Table 9 - Parameters Used for Detection Rate [186]

Parameters	Description
True Positive Rate (TPR)	The ratio of a normal packet that was correctly detected as a normal packet.
False Positive Rate (FPR)	The ratio of a normal packet to total normal packet that was mistakenly detected as a DoSL attack.
True Negative Rate (TNR)	Correctly rejected—the ratio of a malicious packet that was correctly detected as a malicious packet.
False Negative Rate (FNR)	The ratio of a malicious packet to a total normal packet was mistakenly detected as a normal packet.

At this phase, it was expected that more values in TPR and TNR would be achieved. However, low values in FNR and FPR were expected to be obtained in order to justify the accuracy of this experimental research.

4.9 The First Phase of Clustering The LEACH Algorithm

The LEACH algorithm emphasizes the selection of clusters randomly and with a fixed probability. (All nodes have the same probability of being CH.) Nodes are assumed to be homogeneous (nodes have the same initial energy). In this algorithm, the sensors are randomly distributed in one area and are also considered fixed. They are categorized into groups or clusters, and each group selects a head, through which each area communicates directly with the central station at the center of the network. This reduces both the number of transmissions and receptions on the network and omits the redundant data. These data are generated due to the proximity of the sensors in a cluster to each other. The protocol function consists of courses in which there are several rounds. The optimal probability of nodes being CH is equal to Popt and considered fixed. The optimal number of clusters is selected based on the appropriate distribution among all sensors and minimizing energy consumption. Each course consists of 1 / Popt round. If the node is being CH in the current round, it will not occur again until the end of the next round. The node selects a random number in the interval [0-1] and compares the random number with the threshold T (S). If the selected number is less than the threshold, the node will be CH in the current round. If the sensor is not being CH in this round, its probability of being in such a situation increases and continues to do so until the probability reaches 1 in the last round. It means that if the node is not being CH until the last round, this

will happen in the last round. Nodes that have not been CH in the current period belong to set G, and the probability of them being CH increases in each round.

$$T(n) = \begin{cases} \frac{p_{opt}}{1-p_{opt}\left(r \times mod \frac{1}{p_{opt}}\right)}, & if\ n \in G \\ 0, & otherwise \end{cases} \quad (1)$$

In (1), the parameters are as follows [187]:

- r = The current round and its initial value, which is zero.
- $T(n)$= threshold
- G= Nodes that have not become CH
- p_{opt}= The ratio of CH selection
- n = Node

Equation of CH selection

In this equation, r indicates the current round and its initial value which is zero. The reason of the selection of this equation in the LEACH protocol lies in the fact that those nodes that have not been recently CH will be in such position in the current round; Because it can be expected that these nodes have more energy than the nodes that have recently been tasked to be CH (which consumes a lot of energy). It also can be expected that each node to be CH on average once in each round of N / Kopt.

When a node becomes a CH, the probability of the sensor being CH is zero until the next course. And the probability of being CH increases for those nodes that are not in such a position in the current round.

The G set includes sensors that have not become CH so far and can be so at time t. The probability of them being CH is obtained through below Equation [188].

$$E[G] = N - K \times \left(r\ mod \frac{N}{K}\right) \quad (2)$$

In (2), N is the total number of nodes in the network, K is the total number of clusters in each round, and r is the current round.

LEACH has four operational stages: offer, group formation, scheduling, and data transfer. In the suggestion stage, CH introduces itself to other nodes with a message. The sensors select the nearest CH from these offers and

send a membership request to it. The CH node creates a schedule for members and sends it to registered sensors. The nodes send their data to the CH at the announced schedule, and it collects and sends the data to the central station. The energy consumption of CH nodes is higher than that of registered nodes due to the collection of information by registered groups, and the composition and transmission of combined data to a further central station. The energy consumption is well distributed among nodes by randomly selecting the CH and thus changing its role among the nodes [189].

The most important application of LEACH is that it is used to collect data, and since it does not require a wide routing table, it has low hardships and is one of the most successful protocols of its kind. The advantage of nodes' heterogeneity (more energy sensors existence) is the reduction in system development costs; Because the same operation can be done by increasing the number of homogeneous nodes at the beginning, but since the cost of adding a new node instead of placing an extra battery on some sensors is ten times higher, nodes' heterogeneity and their proper use can significantly reduce costs.

Each sensor in this algorithm generates a random number to decide whether it is CH or not. Due to the random selection of CHs , it is possible that in some cases there is no part of the CH network and in others the density of CH is high. In general, there are no logical rules that affect the selection of nodes as CHs based on topological changes and residual energy of the sensors. LEACH has only been able to select the CH in the network.

Classical protocols (also the LEACH protocol) assume that the energy of the nodes is the same, and therefore nodes do not represent their full advantages if they are heterogeneous in terms of energy. Node heterogeneity has many reasons, such as different initial configuration, network performance, or the addition of new nodes to previous sensors. If the nodes are heterogeneous, the protocol will not perform its desired operation properly, and network performance will be unstable especially since the death of the first node.

LEACH assumes that all nodes can be transmitted with sufficient power to reach the main station if required, and that each node has computing power to support different MAC protocols. Therefore, network expansion is not feasible in a wide scale. It also assumes that nodes have data to send and those nodes that are close to each other

have interdependent data. It is not clear how the number of preset leaders is evenly distributed across the network. Therefore, it is possible for the selected leaders to be concentrated in one part of the network. Some nodes may not have any leaders in their vicinity. In addition, the idea of dynamic clustering creates hardships to solve this problem [189].

4.10 Genetic Algorithm

The GA is an innovative and optimized probing method inspired by the theory of natural selection proposed by Charles Darwin. This algorithm represents the theory of natural selection which determines the most suitable people to continue generation and make babies.

The GA is far faster and more effective than traditional methods. This method provides a set of solutions instead of one. But, like any other method and algorithm, the GA also has a series of limitations including that the algorithm is not suitable for all problems, especially for simple issues and with limited parameters. The compatibility of each member of the population should be continuously measured and this measurement requires a large number of calculations. If this algorithm is not properly applied, it is possible that the answers will not be converged [190,191].

This algorithm can be used in probing issues; we consider several solutions for a problem and choose the best of them. Five phases and steps are considered for GA [190,191]:

• Initial population

• Fitness function

• Selection

• Crossover

• Mutation

4.10.1 Initial Population

This process begins with a set of people and solutions that we call them population. Each person in that population is a solution to a problem that we want to solve. There are a few things to keep in mind about population in the GA [191]:

- Population variability should be maintained and early convergence of responses to a single response should be avoided (this is done by mutation operators).
- The population density should not exceed a determined extent as this will slow down the performance of the GA. Also, the population density should not be so small that it becomes impossible to select two effective parents among this population. So, an optimal density for the population is needed to determine the extent by trial and error.
- Each person in this population is described and classified by a set of parameters, each of which we call a gene.
- These genes combine to form a string called chromosome that provides all the features of our solution.
- In the GA, the genes of each solution are represented by an alphabetic letter. These strings are usually expressed by integers or decimals, the most important of which is the binary representation.

4.10.2 Fitness Function

The fitness function determines how compatible each person in this community is with the environment (each person's ability to compete with other members of the community), thereby assigning privileges to each member of the community and the likelihood of a person from the society chosen to continue the generation depends on the privilege that is assigned to it based on fitness. The fitness function must have two important characteristics which are mentioned below:

• This function must be fast enough to perform calculations.

• It should also be able to quantify the fitness degree of the initial solutions as well as the solutions created by combining the two parents' solutions [191,192].

4.10.3 Selection

Selection is the process of selecting the right parents who can be combined with each other to create the next generation. At this stage, we select the best and most adaptable people in the community and allow them to pass on their genes to the next generation. Two pairs of this population are selected according to the maximum adaptability that we call them the parents. People with the highest adaptability have a better chance of being selected and continuing the generation [192].

4.10.4 Crossover

Crossover is the most important and fundamental phase of a GA. Each of these parent pairs combine to form a new offspring. The recombination point is randomly selected within the genes. An offspring is born with the transfer of parental genes and the transfer of one gene from the first parent to the second parent and vice versa. This transfer takes place from the beginning of the genes to the point of recombination correspondingly, and new offspring is added to the population [192].

4.10.5 Mutation

After the formation of offspring, some of their genes are mutated, which is unlikely to be accidental. The main purpose of the mutation is to maintain diversity and differentiation among the population and to prevent the early convergence of the population to species [192].

4.10.6 Termination of The Algorithm and Final Points

The algorithm terminates when the population converge to a specific instance and solution. That is, in fact, children are not significantly different from their parents. In this case, it can be said that the GA has provided a set of solutions to our problem.

- Each population has a specific extent, and when a new generation is formed, those with the least adaptability disappear and a new space is provided for new offspring.
- This sequence of steps and phases is repeated to create people who are better and more adaptable than their predecessors [192].

4.11 Method of Cluster-Head Selection Based on Genetic Algorithm

In our proposed idea, the lifespan of the wireless sensor network is mentioned and a combination of different algorithms is used to achieve our goals. So, the existing network is examined through phasic logic and chaotic-based GA from these aspects [179]:

- CH selection in each round

In this section, the proposed hypotheses, problem and algorithm are explained. Hypotheses are:

- The sensors are fixed in their own place.
- In each round, each sensor can both send and receive data
- Each node knows its position and residual energy and sends them to the cluster.
- The energy used to send a message with a length of k bits at distance d is calculated by below Equation :

$$E_{Tx}(k,d) = \begin{cases} k \times E_{elec} + k \times \epsilon f_s \times d^2, d < d_0 ; \\ k \times E_{elec} + k \times \epsilon mp \times d^4, d > d_0 . \end{cases} \quad (3)$$

The parameters of (3) are as follows [179]:

- E_{Tx}=Transmission energy consumption of a sensor node
- E_{elec}= Circuit energy consumption of transmitting data
- k=Length of data (bit)
- d= Distance between the transceiver and receiver
- d_0 = Square root of ϵf_s/ ϵm_P
- ϵf_s= Free space mode (factor)
- ϵmp=Multi-Path fading mode (factor)

4.12 Conclusion

Based on the information mentioned in previous sections, it is understandable that WBAN networks play an essential role in monitoring the patients' diseases and particular behaviors. This type of network poses significant challenges, including issues related to energy consumption and establishing security against intrusions. One of the attacks raising the network's energy consumption is the DoSL attack, which decreases the network's life and poses

a significant threat. In this project, an attempt was made to avoid DoSL attacks by using an IDS, clustering based on GA, and a demand-based intra-cluster routing.

The IDS system in this study included pre-distribution keys, a random password generator, and nodes' trust value calculation. By calling and recording the data in the predesigned tables in the IDS system and the BS, this system attempted to detect DoSL attacks. The tables involved a random password generator table in each node, an IDS agent table in the IDS database, and a CH table in the CH. Moreover, there was a table in the BS database. The attacker-node-related information was saved in the BS table.

The entire proposed method was simulated in NS2 simulator software. The obtained output was investigated based on metrics such as energy consumption, package delivery rate, end-to-end delay, correct detection rate.

The simulation and comparison of the proposed method were made in two separate scenarios: one under the DoSL attack involving the IDS and another without the IDS.

Delivering better performance, the proposed method could contribute to various benefits, including data confidentiality, integrity, and availability. By establishing these parameters, it would be possible to prevent intrusions to the WBAN system and increase the patient's monitoring system's security.

OFFICE FOR RESEACH TRAINING ,QUALITY AND INTEGRITY

DECLARATION OF CO-AUTHORSHIP AND CO-CONTRIBUTION: PAPERS INCORPORATED IN THESIS

This declaration is to be completed for each conjointly authored publication and placed at the beginning of the thesis chapter in which the publication appears.

1. PUBLICATION DETAILS (to be completed by the candidate)

Title of Paper/Journal/Book:	M. Yaghoubi, K. Ahmed and Y. Miao, "TIDS: Trust Value-Based IDS Framework for Wireless Body Area Network," *2022 32nd International Telecommunication Networks and Applications Conference (ITNAC)*, Wellington, New Zealand, 2022, pp. 142-148, doi: 10.1109/ITNAC55475.2022.9998329.

Surname: Yaghoubi First name: Mohammad

Institute: Institute for Sustainable Industries and Liveab Candidate's Contribution (%): 70%

Status:

Accepted and in press: ☐ Date:

Published: ✔ Date: NOV 2022

2. CANDIDATE DECLARATION

I declare that the publication above meets the requirements to be included in the thesis as outlined in the HDR Policy and related Procedures – policy.vu.edu.au.

MOHAMMAD YAGHOUBI	Digitally signed by MOHAMMAD YAGHOUBI	14 Nov 2022
Signature		**Date**

3. CO-AUTHOR(S) DECLARATION

In the case of the above publication, the following authors contributed to the work as follows:

The undersigned certify that:

1. They meet criteria for authorship in that they have participated in the conception, execution or interpretation of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;

3. There are no other authors of the publication according to these criteria;
4. Potential conflicts of interest have been disclosed to a) granting bodies, b) the editor or publisher of journals or other publications, and c) the head of the responsible academic unit; and
5. The original data will be held for at least five years from the date indicated below and is stored at the following **location**(**s**):

Name(s) of Co-Author(s)	Contribution (%)	Nature of Contribution	Signature	Date
Mohammad Yaghoubi	70%	Concept, Methodology, Experiment, Result Processing, Draft	[redacted]	16/11/22
Khandakar Ahmed	20%	Concept, Validation, Review, Proof Read		15/11/2022
Yuan Miao	10%	Review, Proof Read		15/11/2022

PO Box 14428, Melbourne,
Vic 8001, Australia
+61 3 9919 6100

CHAPTER 5 Simulation

5.1 Introduction

We have implemented the proposed method in NS2 software and compared the proposed method with the protocol (LEACH) method which is close to the proposed method. We have made these comparisons in the metrics of energy consumption and package delivery rate, end-to-end latency and network throughput, and we have measured the performance of the above methods in the mentioned sections.

NS2 is an object-oriented simulation that discretely simulates the network based on events. This software has been developed at Berkeley University in C ++ and Otcl languages. Basically, NS2 can be useful for the establishment of wide local networks. Although using NS2 will be easy for those who are familiar with the basics of emulators, it is quite difficult for novice users to use emulators because the number of suitable documentation and guides for novice users is very limited. However, there are many guidelines written by simulation professionals for the professional users [193]. The purpose of this article is to provide some ideas on how simulators work, how to create new network components, a guide to developing and continuing the path, familiarity with network components in emulator code and so on. Most of the material is presented with simple examples and brief explanations based on different experiences.

5.1.1 Overall Structure of NS2

NS2 is an event-oriented simulator developed at Berkeley University to simulate IP-based networks. In this simulator, network protocols such as TCP and UDP, the behavior of traffic sources such as Ftp, Telnet and Web, queue management mechanism in routers such as DropTail, RED and CBQ, routing algorithms such as Dijkestra etc. are applicable.

Also in NS, multicast transmission and some physical layer protocols can be implemented to simulate LANs. The NS project is currently part of the VINT project, which develops tools for displaying the results of simulation, analysis, and conversion of network topologies. VINT development through manufacturers that are well versed in NS. The current common NS is written and available in C ++ and Otcl (Otcl is an object-oriented scripting language developed at MIT). The structure of the

NS will be discussed briefly, but how to make the most of the NS will be explained in detail with examples [194].

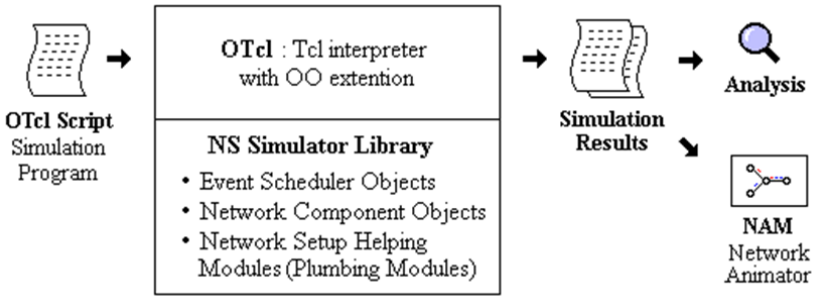


Figure 16 - Simplified for Better Understanding of Users [194]

As shown in Figure 16, NS2 is an object-oriented TCL script interpreter with a directory of simulation events and a library of network components' objects and network execution/regulation libraries from a simplified user perspective. In other words, we write in the Otcl script language to use NS. First, the user must write an Otcl script that creates an event directory (scheduler) to regulate and execute the network. The second stage deals with regulation of the network topologies of the network objects and functions in the libraries; and expressing the traffic sources at the start-up and stoppage time of the transmission of packets through the events scheduler is fulfilled lastly. The word vertical is used to set the network because setting the network vertically allows the data paths through the network objects by adjusting the pointer from one object to another. When users wish to construct a new network object, they may do it quickly by writing a new object or generating a composite object from the object library, then setting up the data flow between the objects. One of the important components of NS is the events scheduler besides network objects. Each event in NS is a unique ID with a regulated time for each packet that points to an Object that triggers the events. In NS, a scheduler event maintains the simulation and start-up time of all events [195]. Network components communicate with each other by sending packets, although this does not cause real-time simulation consumption. All network components spend part of their simulation time using packets. For example, a switch in the network that is simulated with an event delay of 20 microseconds for a packet is set to a 20-microsecond delay timetable for each event. The scheduler removes the event from the queue after 20 microseconds and sends it to the switch element, which itself then sends the packet to a specific output related element.

Another use of the event scheduler is as a timer. TCP, for example, requires a timer to keep packet transmissions on time. The only difference between timers and schedulers is that the timer measures the amount of time associated with a packet and assigns a specific action to that packet after the passage of a specified time.

NS2 is written not only in Otcl but also in C ++. NS2 distinguishes data paths from control paths because of its efficiency. The processing time of events (not simulation time), scheduler, and objects of the main network components in the data path are written and compiled in C ++ in order to reduce packets. These compiled objects are made available to the Otcl interpreter access through an Otcl connection. Each Otcl connection creates a pair of Otcl Objects for each C ++ Object through which control functions are established. The customizable variables specified by the C ++ Objects act as functions and member variables of the transmitted Otcl Objects. In this way, the control of C ++ objects is assigned to Otcl. It is also possible to add member functions and variables to a C ++ connection in the Otcl Object [195].

5.2 Simulation Scenario

According to table 10, we have adjusted the network parameters and presented the test results in the mentioned sections. In this experiment, the number of nodes is considered to be fixed and the simulation time is 100-300 seconds. The details of the simulation are given in full in the table below.

Due to the fact that the Leach algorithm is more common and used than the Heed, we utilized the Leach algorithm, and based on the conducted studies, the results obtained from the improvement of the Leach can also be better than the Heed.

Table 10 - Simulation Parameters

Parameter values	Parameters
180 * 40 cm	Environment
15	Nodes Numbers
250m	Transmission range
100-150-200-250-300	Simulation Times
CBR	Traffic Type
100 Packets	Buffer Size

10J	Initial Energy of network
Random	Location of Nodes
Attacker	DoSL
Communication technology	Zigbee

According to some studies, the nature of the Dosl attack is outside the network as this attack keeps all nodes active by not physically entering the network and but sending a signal into the network.

ZigBee is a low-cost, low-power wireless network standard that aims to develop the use of devices with long battery life in a variety of wireless control and monitoring applications. ZigBee devices have low latency, which reduces the average current consumption. ZigBee chips are mainly used with radios and microcontrollers with flash memory between 60-256 KB ZigBee is used in industrial, scientific and medical radio bands. 2.4 GHz is the most common frequency by global standards. This frequency is 784 MHz in China, 858 MHz in Europe and 915 MHz in the United States and Australia. The data transfer rate varies from 20 kbps (868 MHz band) to 250 kbps (2.4 GHz band). The ZigBee network layer potentially supports star and tree networks and public grid ones. Each network must have a coordinator whose purpose is to control the parameters of the network and its general maintenance. In star networks, the coordinator must be used as the central node. Both tree and net networks allow the use of ZigBee routers to increase network-level communication [196].

Owing to the nature of the network and the proposed method, the use of ZigBee is suitable because the designed network is a small one with a space of 180 x 40 cm in the dimensions of the human body with long battery life.

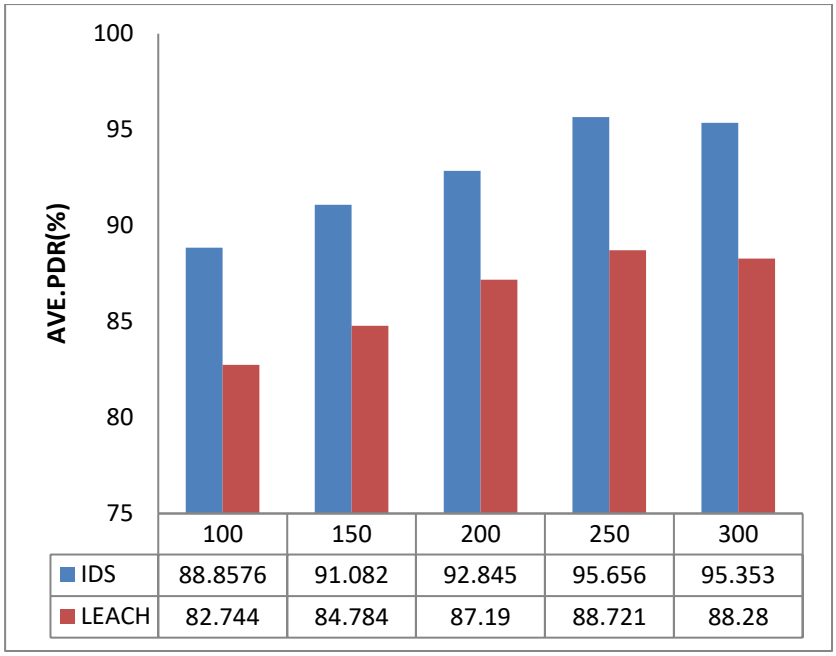


Figure 17 - Graph of Network Packet Delivery Rate in Proportion to Simulation Time Increase

The network packet delivery rate graph between the two methods is shown in Figure 17. The results show that the proposed method has the highest delivery rate in all the simulation times presented by the network. The detection of appropriate intrusion according to the proposed method mentioned in Chapter 3 has caused this increase. The results of this graph show that the proposed method has the highest delivery rate in the whole simulation.

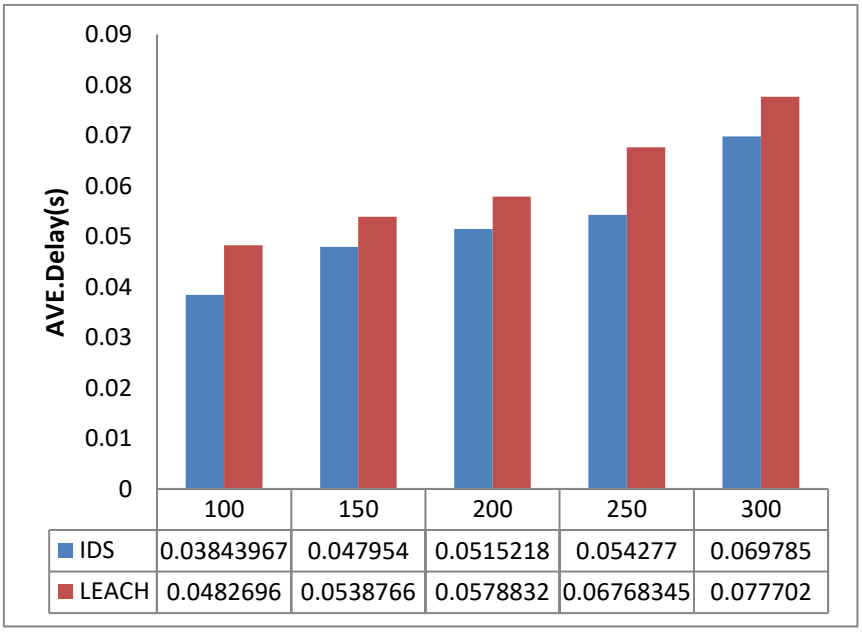
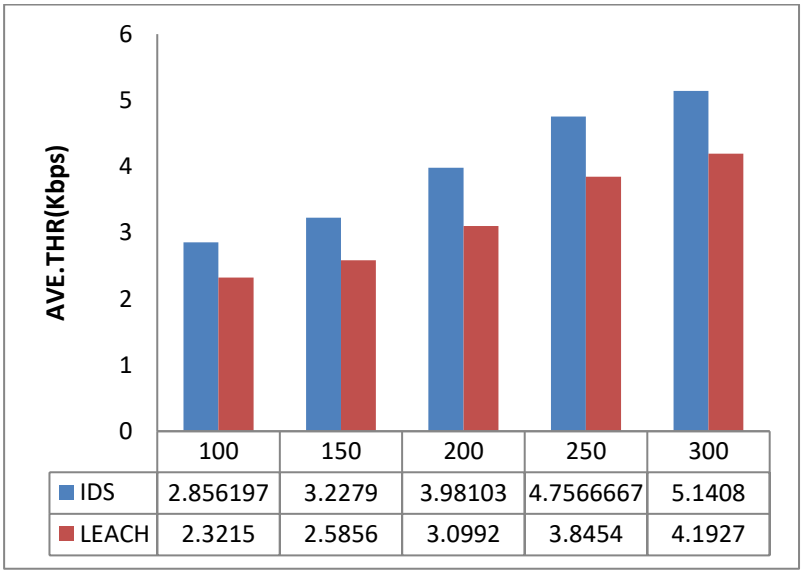


Figure 18 - End-to-End Network Delay in Proportion to Simulation Time Increase

Figure 18. The delay rate in both methods is shown in the graph above. The results show that the proposed method of total simulation has the lowest network latency with a significant distance compared to the other basic method. In this graph, the minimum recorded delay is related to 100 seconds from which it can be concluded that the higher the number of nodes, the longer the proposed method delay; but compared to the basic method, it has less delay.



	100	150	200	250	300
IDS	2.856197	3.2279	3.98103	4.7566667	5.1408
LEACH	2.3215	2.5856	3.0992	3.8454	4.1927

Figure 19 - Graph of Throughput in Proportion to Simulation Time Increase

Figure 19. Graph of throughput in both methods is shown in the graph above. The results show that the proposed method of total simulation has the highest network throughput with a significant distance compared to the other basic method. In this graph, the maximum recorded value is through 300 seconds from which it can be concluded that the longer the time, the greater the throughput of the proposed method.

5.2.1 Intrusion Detection Results of The Proposed Method

As defined in the sections above, the true and false detection rate of DoSL nodes is obtained from the parameters in Table 8. In other words, Table 8 is the detection rate of the probability of successful detection of all security threats. Therefore, the detection formula is shown in the equations of Table 8. Therefore, the results obtained in the first simulation scenario are as follows.

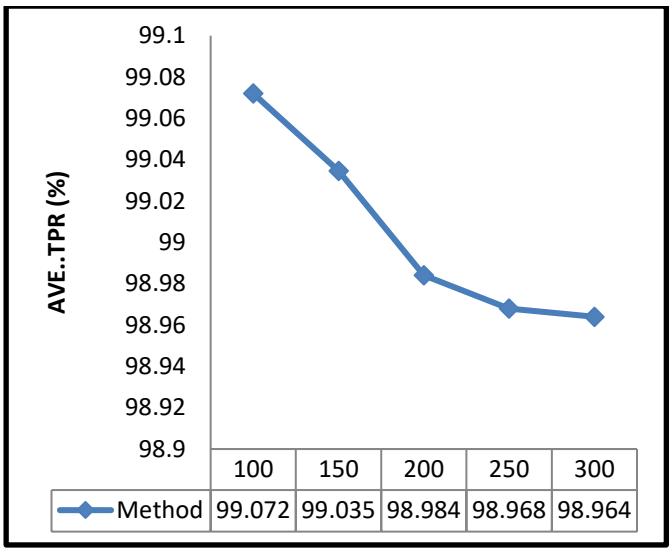


Figure 20 - Graph of True Positive Rate in Proportion to Simulation Time Increase

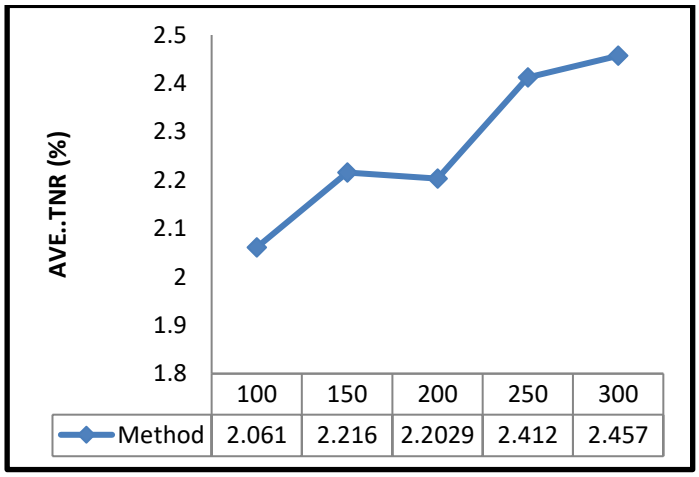


Figure 21 - Graph of True Negative Rate in Proportion to Simulation Time Increase

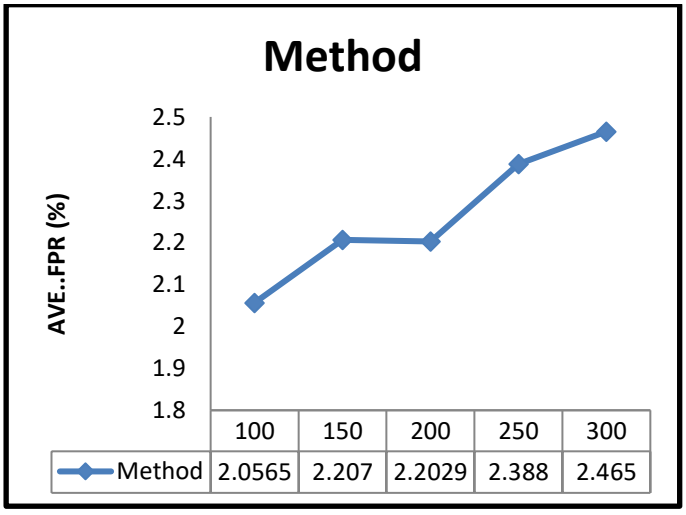


Figure 22 - Graph of False Positive Rate in Proportion to Simulation Time Increase

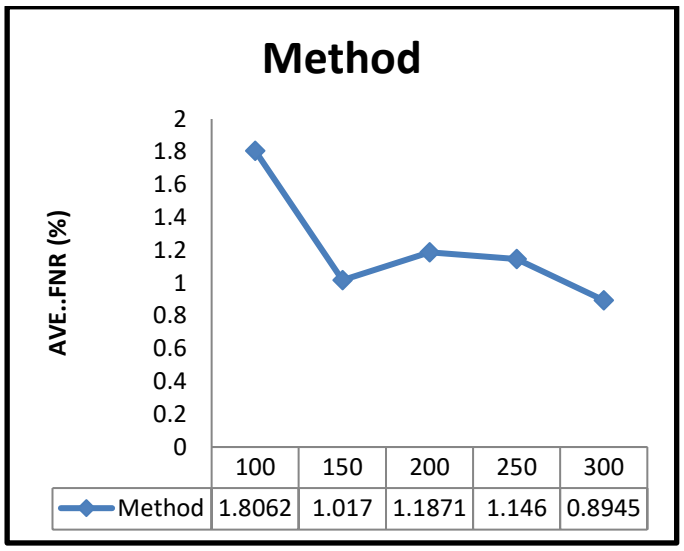


Figure 23 -Graph of Negative False Rate in Proportion to Simulation Time Increase

5.3 Simulation of The Second Scenario

In this simulator scenario, the simulation time of the variable is considered. Also, the number of fixed nodes and network space is 15 meters by 15 meters and the number of destructive nodes (sleep denial) is 5 . The selected benchmark article [8] has used 5 malicious evaluation and simulation nodes in NS2 software. These five malicious nodes in the benchmark article can play the role of the DoSL attacker, Sinkhole attacker, Black hole attacker, and so on. In the study we conducted, the malicious nodes play the role of a DoSL attacker, which tries to keep the nodes active and consume unnecessary energy by sending unnecessary packets. These five malicious nodes can potentially disrupt network communication and also disrupt the sleep and wakefulness of sensor nodes.

The complete specifications of the simulation network to execute the proposed method algorithm are as follows:

Table 11 - Simulation Scenario

Simulation Type	**NS2 2.35**
15 * 15	Environment
10	Number of Nodes
5	Number of Destructive Nodes
50-100-150-200-250s	Simulation Times

CBR	Traffic Type
500 Packets	Buffer Size
1 Joule	The initial energy of each sensor
Random	Location of nodes

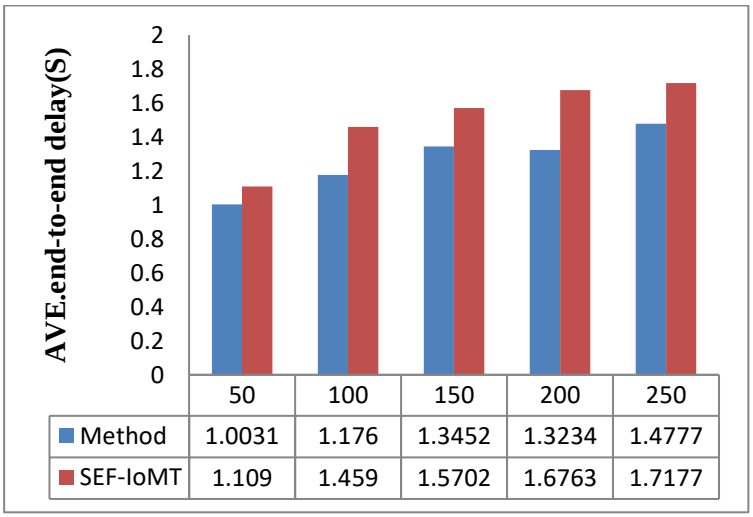


Figure 24 -End-to-End Delay in Proportion to Simulation Time Increase

Figure 24 calculates the end-to-end delay of the wireless areas of body which is equal to the initiation time of sending packet j to destination i apart from the arrival time of the same packet to destination i. As can be seen in the graph above, the proposed method has a better package delivery rate than another mode. And the reason of that is the selection of routes, the number of steps, short distances, and the detection of malicious nodes. So, the length of the route is reduced compared to another case and the package arrives at the destination earlier than another protocol which result in reduced latency.

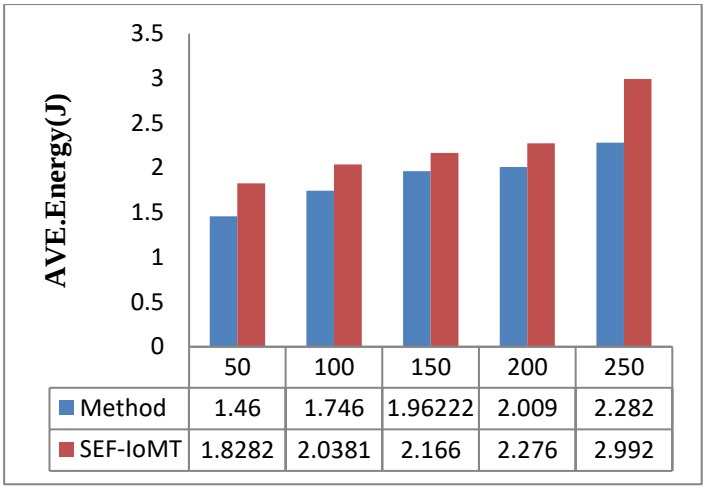


Figure 25 -The consumed Amount of Energy in Proportion to Simulation Time Increase

The two algorithms are compared with each other once more based on energy consumption versus simulation time in which case the number of nodes is fixed. As shown in Figure 25, through simulation time increase, the network energy consumption increases in both algorithms because when the simulation time in the whole network increases, it signifies that the number of transactions in a sample space was more or the network density has been increased. As a result, nodes consume more energy for routing. This process of reducing energy consumption in the proposed algorithm is due to the use of the proposed method. This confirms the scalability of the proposed algorithm. As shown in the figure 25, this energy reduction process in the proposed algorithm (method) is more intense than the SEF-IoMT algorithm.

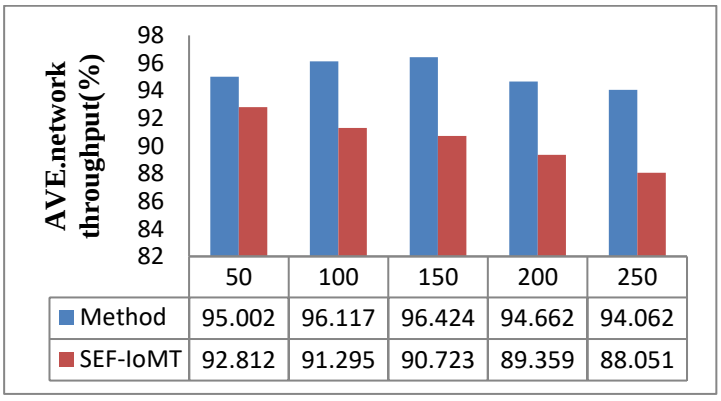


Figure 26 - The Amount of Throughput in Proportion to Simulation Time Increase

Figure 26 shows a comparison of the proposed method and the SEF-IoMT algorithm. Throughput is always an important and basic criterion in networks. Therefore, this criterion has been studied to evaluate the proposed method. Figure 26 shows that the proposed method has the highest average

throughput compared to the studied method. As mentioned in the previous section, the number of bytes that are correctly received by all nodes per unit time is called the throughput.

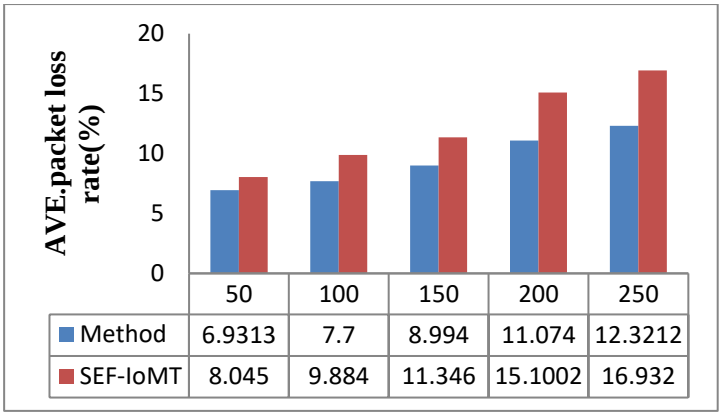


Figure 27 - The Number of Lost Packets in Proportion to Simulation Time Increase

Figure 27 shows the comparison of network state packet loss with the proposed method and SEF-IoMT algorithm. As can be seen in Figure 27, the proposed protocol (method) has less packet loss power than the other SEF-IoMT protocol; that is because of the use of the proposed mechanism to detect suspicious and malicious nodes.

5.3.1 Intrusion Detection Results of The Proposed Method

As defined in the sections above, the true and false detection rate of the number of DoSL nodes is obtained from the parameters of Table 8. In other words, Table 8 is the detection rate of the probability of successful detection of all security threats. The detection formula is shown in the equations of Table 8. Therefore, the results obtained in the first simulation scenario are as follows.

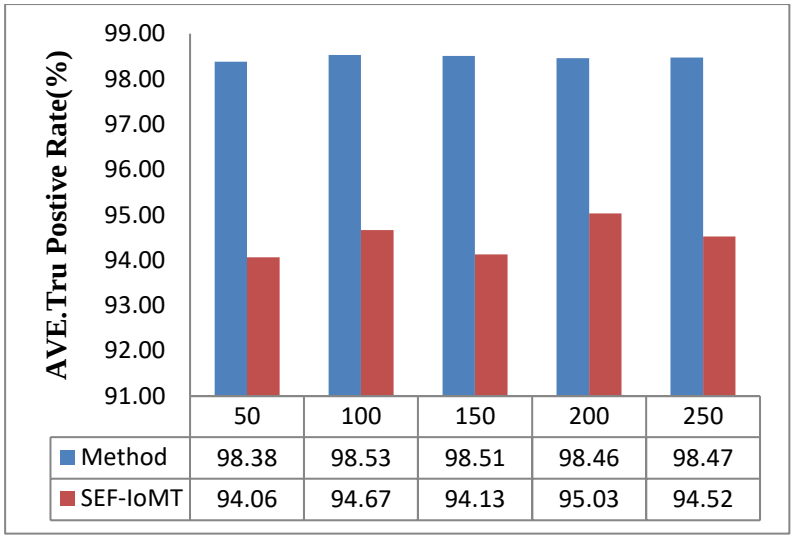


Figure 28 - True Positive Rate Ratio in Proportion to Simulation Time Increase

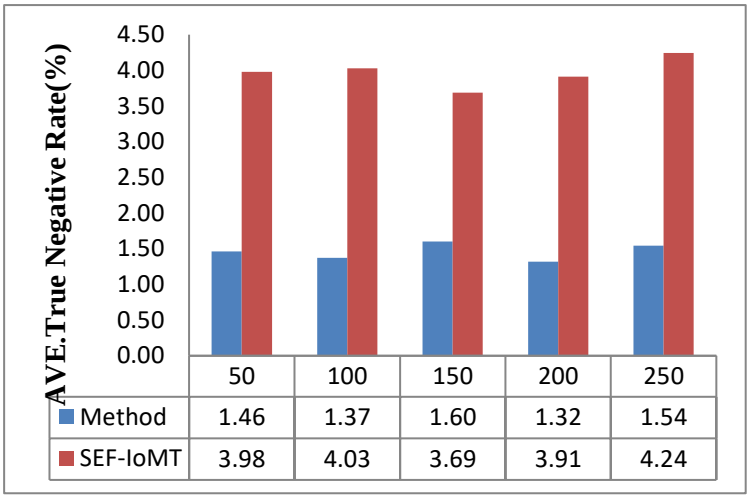


Figure 29 - True Negative Rate Ratio in Proportion to Simulation Time Increase

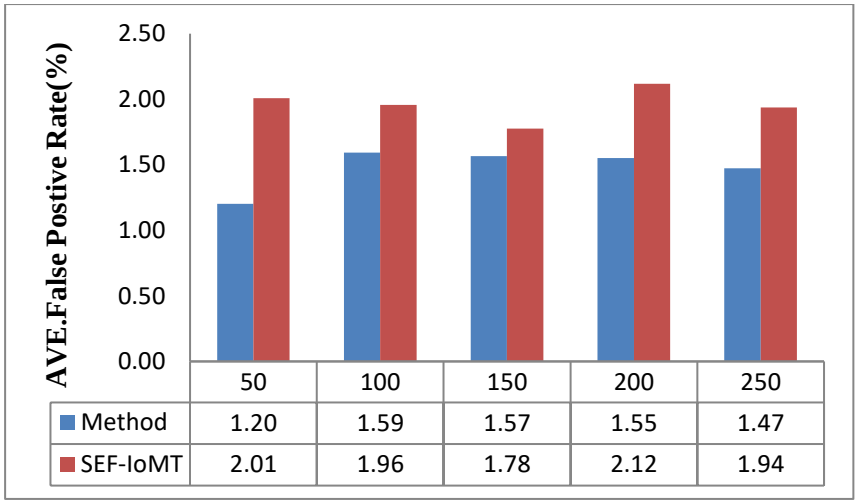


Figure 30 - False Positive Rate Ratio in Proportion to Simulation Time Increase

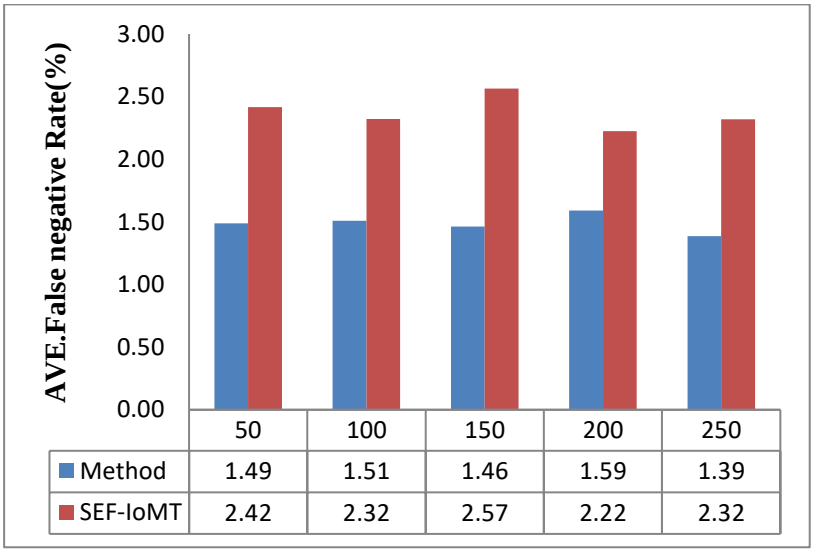


Figure 31 - False Negative Rate Ratio in Proportion to Simulation Time Increase

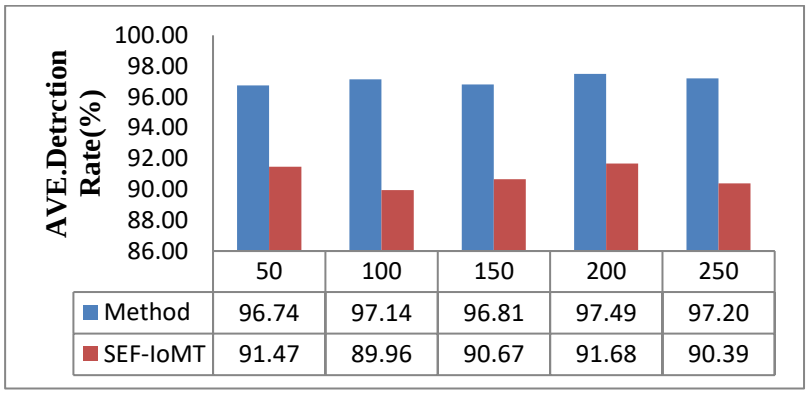


Figure 32 - Detection Rate Ratio in Proportion to Simulation Time Increase

Given that the identification rate is equal to dividing the number of incorrectly detected DoS nodes by the total number of actual misbehaved nodes, Figure 32 shows the detection rate against the simulation time in malicious nodes. What is meant by simulation time here is that packets in the network

are randomly transferred among nodes at arbitrary times; that is, each node sends at a different time. As shown in the results, using the SEF-IoMT method, the denial of sleep attack detection ratio is about 92% at 50 simulation time, which is reduced to about 90% at 250 simulation time. However, while estimating the simulation time, applying the proposed algorithm (method) in the network improves the network performance by almost 10% compared to the existing SEF-IoMT method [197].

According to the contents presented in the proposed method, the database operation is performed based on the registration of Node-ID, Event-ID, and Key-ID. By comparing the information in the database IDS, if the node is normal, the data will be transmitted first to the CH and then to the BS, otherwise the node will be recognized as an attacker and recorded in the BS table and the IDS database, and the node will be isolated.

The operations related to the IDS database and its interaction with the BS table are coded by NS2 software and are done behind the scenes, but the results of this interaction generally affect the network and under metrics such as End-to-End Delay (11%), Throughput (11%), PDR (12%), etc. are shown in the graph form.

Overall, with the investigations done on the limitations of papers 1-4 [19-22] in the literature review section, it can be concluded that all the literature review samples include high energy-consumption, high control overhead, high computational complexity, and high end-to-end delay. Therefore, it can be said that in the proposed method presented in this research study, using the IDS-Agent intrusion detection algorithm, modified genetic algorithm, and modified trust-based light AODV routing, it is possible to control overhead, energy consumption, end-to-end delay, and reduce the computational time and network energy consumption.

CHAPTER 6 Conclusion

6.1 Conclusion

The purpose of the simulation chapter was to evaluate the methods mentioned in the simulation software to introduce the optimal method. In the thesis, we briefly reviewed the security and navigation in the WBAN. Due to the weakness of such networks in terms of security and routing in the various network conditions, it is appropriate to examine these weaknesses in the networks more carefully so that they can be used with more confidence. As seen during this study, these networks were more vulnerable to attack than other networks. These attacks were categorized and investigated. Some of the most famous routing algorithms for routing and preventing the intrusion of attacks presented in this field were also introduced.

All these algorithms are basically quite acceptable in terms of network performance, but there are some problems. An extension is provided for each of these algorithms in order to solve these problems. These extensions have fixed the security problems of routing protocols but have made problems for them in terms of network performance. Therefore, it is necessary to provide a routing security method for the WBANs that has an acceptable level both in terms of security and network efficiency.

Operating power, average package delivery rate, end-to-end delay and packet loss, etc. were shown in a WBAN with a scenario of increasing simulation time in the presented graphs. As we can see, by time increase, the amount of throughput and the package delivery rate increases. The results showed that the proposed protocol in all graphs had a better performance in detecting DoSL intrusion than other protocols.

Finally, we evaluated the proposed protocol and compared it with the standard protocol under attack and the SEF-IoMT method in terms of packet delivery rate, throughput, average end-to-end delay, packet loss, etc. The graph results indicate a better method. So, this method is introduced as the optimal method.

According to the evaluation of the methodology presented in chapter 4 as well as the results obtained from the simulation of chapter 5 and improving the efficiency of the proposed method compared to the benchmark, the following can be mentioned:

• Reducing energy consumption by the clustering format presented in the proposed method: in this clustering format, a modified genetic algorithm is used to select the appropriate CH by considering the distance and energy criteria between network nodes.

• Use of IDS-Agent to increase WBAN security and detect DoSL attack penetration. In this phase, a Random Password Generator (RPG), as well as public pre-distributed keys, have been used to compare normal and attacker nodes.

• Use of modified AODV routing to increase optimal path selection between nodes by considering reliable paths: accelerating discovery of communication paths, reducing data transmission delay, and increasing trust between network nodes.

It can be concluded that the above-mentioned factors increase the efficiency of the proposed method in the WBANs under DoSL attacks.

6 .2 Limitations and Future Work

In this research study, an artificial intelligence algorithm was utilized for clustering, which was selected considering only two factors of energy and optimal CH distance. By modifying the linear gene and changing its structure from linear to matrix and adding other parameters such as sensor temperature, it would be possible to achieve better and more effective results in the future research methods. Moreover, in several similar studies, the use of the smart firefly algorithm proved to be faster than the genetic algorithm, which can be investigated. In addition, in the case of routing, the intelligent genetic algorithm can be used instead of AODV and show the comparison of the recovery time of the route. Additionally, in order to increase the security of this methodology, a smart firewall can be designed based on the performance of the unconventional behavior of the packets, which, by being integrated with the designed IDS, may provide the possibility to prevent malicious packets from entering the network if an attacker penetrates the network. In addition, in this research study, the ant colony method can be used to calculate the distance between nodes, which helps with the dynamics and flexibility of the WBAN, which is constantly moving. Moreover, in order to increase the security of the upcoming study, I intend to solve the problem of a single point of failure by decentralizing the network and using the security algorithm based on Blockchain. Therefore, if a node or a device from our network fails, the

rest of the parts can continue functioning without interruption and delay, and since the blockchain security system is heavy, I will use mechanisms based on probability such as Voting and Game theory, and I will try to equip this version of the blockchain with temporary short-term memories to present a new, up-to-date and lightweight version that can function on network sensor nodes while maintaining improved energy consumption. By considering these, the limitations of this study method can be overcome and used as the basis for new research in the future.

References

1. Muhamad, W. N. W., Naim, N. F., Hussin, N., Wahab, N., Abd Aziz, N., Sarnin, S. S., & Mohamad, R. (2009, December). Maximizing network lifetime with energy efficient routing protocol for wireless sensor networks. In 2009 Fifth International Conference on MEMS NANO, and Smart Systems (pp. 225-228). IEEE.
2. Razaque, A., Abdulghafour, M., & Khan, M. J. (2017, November). Detection of selfish attack over wireless body area networks. In *2017 IEEE Conference on Open Systems (ICOS)* (pp. 48-52). IEEE
3. Mohd, N., Singh, A., & Bhadauria, H. S. (2020). A novel SVM based IDS for distributed denial of sleep strike in wireless sensor networks. *Wireless Personal Communications*, *111*(3), 1999-2022.
4. Park, C., Lahiri, K., & Raghunathan, A. (2005, September). Battery discharge characteristics of wireless sensor nodes: An experimental analysis. In 2005 Second Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2005. IEEE SECON 2005. (pp. 430-440). IEEE.
5. Fotouhi, M., Bayat, M., Das, A. K., Far, H. A. N., Pournaghi, S. M., & Doostari, M. A. (2020). A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Computer Networks*, *177*, 107333.
6. Gunasekaran, M., & Periakaruppan, S. (2017). GA-DoSLD: genetic algorithm based denial-of-sleep attack detection in WSN. *Security and Communication Networks*, *2017*.
7. Ayed, S., Chaari, L., & Fares, A. (2020). A survey on trust management for WBAN: Investigations and future directions. Sensors, 20(21), 6041.
8. Saba, T., Haseeb, K., Ahmed, I., & Rehman, A. (2020). Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. *Journal of Infection and Public Health*, *13*(10), 1567-1575.
9. https://www.who.int/health-topics/cardiovascular-diseases#tab=tab_1
10. Australian Institute of Health and Welfare (AIHW) 2020, Deaths in Australia, viewed 4 March 2021, https://www.aihw.gov.au/reports/life-expectancy-death/deaths-in-australia
11. Dias, D., & Paulo Silva Cunha, J. (2018). Wearable health devices—vital sign monitoring, systems and technologies. Sensors, 18(8), 2414.
12. Hammood, D., & Alkhayyat, A. (2020, September). An overview of the survey/review studies in wireless body area network. In 2020 3rd International Conference on Engineering Technology and its Applications (IICETA) (pp. 18-23). IEEE.
13. Sawaneh, I. A., Sankoh, I., & Koroma, D. K. (2017, December). A survey on security issues and wearable sensors in wireless body area network for healthcare system. In 2017 14th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP) (pp. 304-308). IEEE.
14. Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., & Jamalipour, A. (2014). Wireless body area networks: A survey. *IEEE Communications surveys & tutorials*, *16*(3), 1658-1686.
15. https://www.health.gov.au/ministers/the-hon-greg-hunt-mp/media/record-investment-in-the-future-of-australias-health-system
16. https://www.who.int/en/news-room/fact-sheets/detail/cardiovascular-diseases-(cvds)
17. Pandey, I., Dutta, H. S., & Banerjee, J. S. (2019, March). WBAN: a smart approach to next generation e-healthcare system. In *2019 3rd International conference on computing methodologies and communication (ICCMC)* (pp. 344-349). IEEE
18. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal*, *18*(2), 113-122.
19. Thamilarasu G, Odesile A, Hoang A. An Intrusion Detection System for Internet of Medical Things. IEEE Access. 2020;8:181560-76.
20. Ozcelik MM, Irmak E, Ozdemir S, editors. A hybrid trust based intrusion detection system for wireless sensor networks. 2017 International Symposium on Networks, Computers and Communications (ISNCC); 2017: IEEE.
21. Patel MM, Patel PK, editors. Intrusion detection system based on trust value in wireless sensor networks. 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA); 2019: IEEE.
22. Ramaswamy, S., & Gandhi, U. D. (2022). Trust-Based Data Communication in Wireless Body Area Network for Healthcare Applications. *Big Data and Cognitive Computing*, *6*(4), 148.
23. Liu Q, Mkongwa KG, Zhang C. Performance issues in wireless body area networks for the healthcare application: a survey and future prospects. SN Applied Sciences. 2021;3(2):155.
24. Dimitriou, T., & Ioannis, K. (2008, October). Security issues in biomedical wireless sensor networks. In *2008 First International Symposium on Applied Sciences on Biomedical and Communication Technologies* (pp. 1-5). IEEE.
25. Kumar, P., & Lee, H. J. (2011). Security issues in healthcare applications using wireless medical sensor networks: A survey. *sensors*, *12*(1), 55-91.
26. Kambourakis, G., Klaoudatou, E., & Gritzalis, S. (2007, April). Securing medical sensor environments: the codeblue framework case. In *The Second International Conference on Availability, Reliability and Security (ARES'07)* (pp. 637-643). IEEE.
27. Nasser, N., & Chen, Y. (2007). SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks. *Computer communications*, *30*(11-12), 2401-2412.
28. Benaicha, S. E., Saoudi, L., Guermeche, S. E. B., & Lounis, O. (2014, August). Intrusion detection system using genetic algorithm. In 2014 Science and Information Conference (pp. 564-568). IEEE.
29. Rushanan, M., Rubin, A. D., Kune, D. F., & Swanson, C. M. (2014, May). Sok: Security and privacy in implantable medical devices and body area networks. In *2014 IEEE symposium on security and privacy* (pp. 524-539). IEEE.
30. Toorani, M. (2015, January). On vulnerabilities of the security association in the IEEE 802.15. 6 standard. In *International conference on financial cryptography and data security* (pp. 245-260). Springer, Berlin, Heidelberg.
31. Sangari, A. S., & Manickam, J. M. L. (2014, March). Public key cryptosystem based security in wireless body area network. In *2014 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014]* (pp. 1609-1612). IEEE.
32. Li, W., & Zhu, X. (2014, October). Recommendation-based trust management in body area networks for mobile healthcare. In *2014 IEEE 11th International conference on mobile ad hoc and sensor systems* (pp. 515-516). IEEE.
33. Anandkumar, K. M., Jayakumar, C., Kumar, A. P., Sushma, M., & Vikraman, R. (2012). Intrusion detection and prevention of node replication attacks in wireless body area sensor network. *International Journal of UbiComp*, *3*(3), 1.
34. Hu, L., Wen, H., Wu, B., Pan, F., Liao, R. F., Song, H., ... & Wang, X. (2017). Cooperative jamming for physical layer security enhancement in Internet of Things. *IEEE Internet of Things Journal*, *5*(1), 219-228.
35. Li, S., & Da Xu, L. (2017). *Securing the internet of things*. Syngress.
36. Soderi, S., Mucchi, L., Hämäläinen, M., Piva, A., & Iinatti, J. (2017). Physical layer security based on spread-spectrum watermarking and jamming receiver. *Transactions on Emerging Telecommunications Technologies*, *28*(7), e3142.

37. Mucchi, L., Ronga, L. S., & Cipriani, L. (2009). A new modulation for intrinsically secure radio channel in wireless systems. *Wireless personal communications*, *51*(1), 67-80.
38. Zhong, S. C., Song, Q. F., Cheng, X. C., & Zhang, Y. (2003, November). A safe mobile agent system for distributed intrusion detection. In *Proceedings of the 2003 International Conference on Machine Learning and Cybernetics (IEEE Cat. No. 03EX693)* (Vol. 4, pp. 2009-2014). IEEE.
39. A. Boukerche, X. Li, and K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor networks," Computer Communications., vol. 30, pp. 2413–2427, Sep. 2007.
40. Sinha, S. (2021, July). Impact of DoS attack in IoT system and identifying the attacker location for interference attacks. In *2021 6th International Conference on Communication and Electronics Systems (ICCES)* (pp. 657-662). IEEE.
41. Gallais, A., Hedli, T. H., Loscri, V., & Mitton, N. (2019, April). Denial-of-sleep attacks against IoT networks. In *2019 6th International Conference on Control, Decision and Information Technologies (CoDIT)* (pp. 1025-1030). IEEE
42. Fotohi, R., Firoozi Bari, S., & Yusefi, M. (2020). Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol. *International Journal of Communication Systems*, *33*(4), e4234.
43. Ali A, Ming Y, Chakraborty S, Iram S. A comprehensive survey on real-timeapplications of WSN. Future Internet 2017;9(4):77.
44. Ban–dur Đ, Jakˇsi´c B, Ban–dur M, Jovi´c S. An analysis of energy efficiency in WirelessSensor Networks (WSNs) applied in smart agriculture. Comput Electron Agric2019;156:500–7.
45. Hezaveh M, Shirmohammdi Z, Rohbani N, Miremadi SG. A fault-tolerant andenergy-aware mechanism for cluster-based routing algorithm of WSNs. In:Integrated network management (IM), 2015 IFIP/IEEE international sympo-sium. Ottawa: IEEE; 2015.
46. Mahajan S, Malhotra J, Sharma S. An energy balanced QoS based cluster headselection strategy for WSN. Egypt Inform J 2014;15(3):189–99
47. Ahmed G, Zou J, Zhao X, Sadiq Fareed MM. Markov chain model-based optimalcluster heads selection for wireless sensor networks. Sensors 2017;17(3):440
48. Thakkar A, Kotecha K. Cluster head election for energy and delay constraintapplications of wireless sensor network. IEEE Sens J 2014;14(8):2658–64
49. Wang A, Yang D, Sun D. A clustering algorithm based on energy informationand cluster heads expectation for wireless sensor networks. Comput Electr Eng2012;38(3):662–71
50. Dishongh TJ, McGrath M, Kuris B. Wireless sensor networks for healthcareapplications. 1 ed. Artech House; 2014.
51. Suciu G, Suciu V, Martian A, Craciunescu R, Vulpe A, Marcu I, et al. Big data,internet of things and cloud convergence – an architecture for secure E-Healthapplications. J Med Syst 2015;39(11):141.
52. Ha, I. (2015). Technologies and research trends in wireless body area networks for healthcare: a systematic literature review. International Journal of Distributed Sensor Networks, 11(6), 573538.
53. Bangash, J.I.; Abdullah, A.H.; Anisi, M.H.; Khan, A.W. A survey of routing protocols in wireless body sensor networks. Sensors 2014, 14, 1322–1357. https://doi.org/10.3390/s140101322
54. Rahangdale, H. A Review on WMSN (Wireless Medical Sensor Networks) for Health Monitoring Systems. ECS Trans. 2022, 107, 1973.
55. Qu, Y., Zheng, G., Ma, H., Wang, X., Ji, B., & Wu, H. (2019). A Survey of Routing Protocols in WBAN for Healthcare Applications. Sensors (Basel, Switzerland), 19(7), 1638. https://doi.org/10.3390/s19071638
56. Watteyne, T., Augé-Blum, I., Dohler, M., & Barthel, D. (2007, June). AnyBody: a self-organization protocol for body area networks. In BODYNETS (p. 6).
57. Al-Baz, A., & El-Sayed, A. (2018). A new algorithm for cluster head selection in LEACH protocol for wireless sensor networks. *International journal of communication systems*, *31*(1), e3407.
58. Liang, L., Ge, Y., Feng, G., Ni, W., & Wai, A. A. P. (2014). A low overhead tree-based energy-efficient routing scheme for multi-hop wireless body area networks. Computer Networks, 70, 45-58.
59. Javaid, N., Ahmad, A., Nadeem, Q., Imran, M., & Haider, N. (2015). iM-SIMPLE: iMproved stable increased-throughput multi-hop link efficient routing protocol for Wireless Body Area Networks. Computers in Human Behavior, 51, 1003-1011
60. Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000, January). Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the 33rd annual Hawaii international conference on system sciences* (pp. 10-pp). IEEE.
61. Javaid, N., Ahmad, A., Rahim, A., Khan, Z. A., Ishfaq, M., & Qasim, U. (2014). Adaptive medium access control protocol for wireless body area networks. International Journal of Distributed Sensor Networks, 10(3), 254397
62. Almalki, F. A., Ben Othman, S., A Almalki, F., & Sakli, H. (2021). EERP-DPM: energy efficient routing protocol using dual prediction model for healthcare using IoT. Journal of Healthcare Engineering, 2021.
63. Ullah, Z., Ahmed, I., Ali, T., Ahmad, N., Niaz, F., & Cao, Y. (2019). Robust and efficient energy harvested-aware routing protocol with clustering approach in body area networks. IEEE Access, 7, 33906-33921.
64. Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000, January). Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd annual Hawaii international conference on system sciences (pp. 10-pp). IEEE.
65. Bächlin, M., & Tröster, G. (2012). Swimming performance and technique evaluation with wearable acceleration sensors. Pervasive and mobile computing, 8(1), 68-81.
66. Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. (2011). Body area networks: A survey. Mobile networks and applications, 16(2), 171-193.
67. Alemdar, H., & Ersoy, C. (2010). Wireless sensor networks for healthcare: A survey. Computer networks, 54(15), 2688-2710.
68. Reusens, E., Joseph, W., Latré, B., Braem, B., Vermeeren, G., Tanghe, E., ... & Blondia, C. (2009). Characterization of on-body communication channel and energy efficient topology design for wireless body area networks. IEEE Transactions on Information Technology in Biomedicine, 13(6), 933-945.
69. Zhang, Q., Kortermand, K., Jacobsen, R. H., & Toftegaard, T. S. (2012, June). Reactive virtual coordinate routing protocol for body sensor networks. In 2012 IEEE International Conference on Communications (ICC) (pp. 3388-3393). IEEE.
70. Martelli, F., Buratti, C., & Verdone, R. (2011, April). On the performance of an IEEE 802.15. 6 wireless body area network. In 17th European Wireless 2011-Sustainable Wireless Technologies (pp. 1-6). VDE.
71. Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., ... & Kwak, K. S. (2012). A comprehensive survey of wireless body area networks. Journal of medical systems, 36(3), 1065-1094.
72. Ullah, S., Shen, B., Islam, S. R., Khan, P., Saleem, S., & Kwak, K. S. (2009). A study of MAC protocols for WBANs. Sensors, 10(1), 128-145.
73. Sthapit, P., & Pyun, J. Y. (2013). Medium reservation based sensor MAC protocol for low latency and high energy efficiency. Telecommunication Systems, 52(4), 2387-2395.
74. Garcia, M., Sendra, S., Lloret, J., & Canovas, A. (2013). Saving energy and improving communications using cooperative group-based wireless sensor networks. Telecommunication Systems, 52(4), 2489-2502.

75. Kim, B., & Cho, J. (2012, February). A novel priority-based channel access algorithm for contention-based MAC protocol in WBANs. In Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication (pp. 1-5).
76. Lewis, D. (2008); "802.15.6 Call for applications-response summary", IEEE 802.15-08-0407-05-0006.
77. Natarajan, A., De Silva, B., Yap, K. K., & Motani, M. (2009, June). To hop or not to hop: Network architecture for body sensor networks. In 2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (pp. 1-9). IEEE.
78. Ge, Y., Liang, L., Ni, W., Wai, A. A. P., & Feng, G. (2012, March). A measurement study and implication for architecture design in wireless body area networks. In 2012 IEEE International Conference on Pervasive Computing and Communications Workshops (pp. 799-804). IEEE.
79. Natarajan, A., De Silva, B., Yap, K. K., & Motani, M. (2009, September). Link layer behavior of body area networks at 2.4 GHz. In Proceedings of the 15th annual international conference on Mobile computing and networking (pp. 241-252).
80. Sawaneh, I. A., Sankoh, I., & Koroma, D. K. (2017, December). A survey on security issues and wearable sensors in wireless body area network for healthcare system. In *2017 14th international computer conference on wavelet active media technology and information processing (ICCWAMTIP)* (pp. 304-308). IEEE
81. Pramanik, P. K. D., Nayyar, A., & Pareek, G. (2019). WBAN: Driving e-healthcare beyond telemedicine to remote health monitoring: Architecture and protocols. In Telemedicine technologies (pp. 89-119). Academic Press.
82. Redfoot, D., Feinberg, F., & Houser, A. (2019). The aging of the baby boom and the growing care gap: a look at future declines in the availability of family caregivers. August 2013.
83. Hong, L., Luo, M., Wang, R., Lu, P., Lu, W., & Lu, L. (2018). Big data in health care: Applications and challenges. *Data and information management*, *2*(3), 175-197.
84. Baba, E., Jilbab, A., & Hammouch, A. (2018, April). A health remote monitoring application based on wireless body area networks. In 2018 International Conference on Intelligent Systems and Computer Vision (ISCV) (pp. 1-4). IEEE.
85. Wu, F., Wu, T., & Yuce, M. R. (2019, April). Design and implementation of a wearable sensor network system for IoT-connected safety and health applications. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)* (pp. 87-90). IEEE.
86. Bouguera, T., Diouris, J. F., Chaillout, J. J., Jaouadi, R., & Andrieux, G. (2018). Energy consumption model for sensor nodes based on LoRa and LoRaWAN. Sensors, 18(7), 2104.
87. Latré, B., Braem, B., Moerman, I., Blondia, C., & Demeester, P. (2011). A survey on wireless body area networks. Wireless networks, 17(1), 1-18
88. Gupta, M., Tanwar, S., Rana, A., & Walia, H. (2021, September). Smart Healthcare Monitoring System Using Wireless Body Area Network. In 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 1-5). IEEE.
89. Al-Saud, K. A., Mohamed, A., & Mahmuddin, M. (2011). Survey on Wireless Body Area Sensor Networks for healthcare applications: Signal Processing, data analysis and feedback. *In Proceedings of the 3rd International Conference on Computing and Informatics, ICOCI. 2011,8-9 June, 2011* Bandung, Indonesia. Paper No. 088
90. Maity, S., Das, D., & Sen, S. (2017, July). Wearable health monitoring using capacitive voltage-mode human body communication. In 2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC) (pp. 1-4). IEEE.
91. Tiwari, P., Saxena, V. P., Mishra, R. G., & Bhavsar, D. (2015). Wireless sensor networks: Introduction, advantages, applications and research challenges. HCTL Open International Journal of Technology Innovations and Research (IJTIR), 14, 1-11.
92. Engmann, F., Katsriku, F. A., Abdulai, J. D., Adu-Manu, K. S., & Banaseka, F. K. (2018). Prolonging the lifetime of wireless sensor networks: a review of current techniques. Wireless Communications and Mobile Computing, 2018.
93. Khan, R. A., & Pathan, A. S. K. (2018). The state-of-the-art wireless body area sensor networks: A survey. International Journal of Distributed Sensor Networks, 14(4), 1550147718768994.
94. Kurian, A.; Divya, R. A survey on energy efficient routing protocols in wireless body area networks (WBAN). In Proceedings of the International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Karpagam Coll Engn, Coimbatore, India, 17–18 May 2017
95. Kadel, R., Islam, N., Ahmed, K., & Halder, S. J. (2018). Opportunities and challenges for error correction scheme for wireless body area network—a survey. *Journal of Sensor and Actuator Networks*, *8*(1), 1.
96. Ullah, S., Hassan, M. M., Hossain, M. S., & Alelaiwi, A. (2020). Performance evaluation of rts/cts scheme in beacon-enabled ieee 802.15. 6 mac protocol for wireless body area networks. Sensors, 20(8), 2368.
97. Raghunathan, V., Schurgers, C., Park, S., & Srivastava, M. B. (2002). Energy-aware wireless microsensor networks. IEEE Signal processing magazine, 19(2), 40-50.
98. Pottie, G. J., & Kaiser, W. J. (2000). Wireless integrated network sensors. Communications of the ACM, 43(5), 51-58.
99. Khriji, S.; El Houssaini, D.; Kammoun, I.; Kanoun, O. Energy-efficient techniques in wireless sensor networks. In *Energy Harvesting for Wireless Sensor Networks: Technologies, Components and System Design*; De Gruyter Oldenbourg: Berlin, Germany, 2018.
100. Cardei, M., Thai, M. T., Li, Y., & Wu, W. (2005, March). Energy-efficient target coverage in wireless sensor networks. In Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies. (Vol. 3, pp. 1976-1984). IEEE.
101. Chong, C. Y., & Kumar, S. P. (2003). Sensor networks: evolution, opportunities, and challenges. Proceedings of the IEEE, 91(8), 1247-1256.
102. Chamam, A., & Pierre, S. (2007, October). Energy-efficient state scheduling for maximizing sensor network lifetime under coverage constraint. In Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007) (pp. 63-63). IEEE
103. Matin, M. A., & Islam, M. M. (2012). Overview of wireless sensor network. *Wireless sensor networks-technology and protocols*, *1*(3).
104. Pradha, S. E., Moshika, A., Balaji, N., Andal, K., Sambasivam, G., & Shanmugam, M. (2021). Scheduled Access Strategy for Improving Sensor Node Battery Life Time and Delay Analysis of Wireless Body Area Network. IEEE Access.
105. Tavera, C.A.; Ortiz, J.H.; Khalaf, O.I.; Saavedra, D.F.; Aldhyani, T.H. Wearable wireless body area networks for medical applications. Comput. Math. Methods Med. 2021, 2021, 5574376.
106. Mahmood, S. N., Ishak, A. J., Ismail, A., Soh, A. C., Zakaria, Z., & Alani, S. (2020). ON-OFF body ultra-wideband (UWB) antenna for wireless body area networks (WBAN): a review. IEEE Access, 8, 150844-150863.
107. Rath, M., Pati, B., & Pattanayak, B. K. (2018). An overview on social networking: design, issues, emerging trends, and security. Social Network Analytics: Computational Research Methods and Techniques, 21.
108. Naik, M. R. K., & Samundiswary, P. (2016, December). Wireless body area network security issues—Survey. In 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) (pp. 190-194). IEEE.
109. Al Barazanchi, I., Hashim, W., Alkahtani, A. A., Abbas, H. H., & Abdulshaheed, H. R. (2021, October). Overview of WBAN from Literature Survey to Application Implementation. In 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) (pp. 16-21). IEEE.

110. Ananthi, J. V., & Jose, P. (2021). A perspective review of security challenges in body area networks for healthcare applications. *International Journal of Wireless Information Networks*, *28*(4), 451-466
111. Bedi, R.K. An improved energy efficient TDMA based MAC protocol for WBAN. Int. J. Comput. Eng. 2018, 6, 34–39
112. Singla, R., Kaur, N., Koundal, D., & Bharadwaj, A. (2022). Challenges and developments in secure routing protocols for healthcare in WBAN: A comparative analysis. *Wireless Personal Communications*, *122*(2), 1767-1806.
113. Lasassmeh, S. M., & Conrad, J. M. (2010, March). Time synchronization in wireless sensor networks: A survey. In Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon) (pp. 242-245). IEEE.
114. Butun, I. Prevention and Detection of Intrusions in Wireless Sensor Networks. Ph.D. Thesis, University of South Florida, Tampa, FL, USA, 2013.
115. Wireless Body Area Networks for Health Monitoring: A Comprehensive Survey. Sensors, 22(9), 3539.
116. Shi, E.; Perrig, A. Designing secure sensor networks. IEEE Wirel. Commun. 2004, 11, 38–43.
117. Wood, A. D., Stankovic, J. A., & Zhou, G. (2007, June). DEEJAM: Defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks. In *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks* (pp. 60-69). IEEE.
118. Wood, A. D., Stankovic, J. A., & Zhou, G. (2007, June). DEEJAM: Defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks. In *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks* (pp. 60-69). IEEE.
119. JOUINI, O., & SETHOM, K. (2020, October). Physical Layer Security Proposal for Wireless Body Area Networks. In 2020 IEEE 5th Middle East and Africa Conference on Biomedical Engineering (MECBME) (pp. 1-5). IEEE.
120. Aborujilah, A., Nassr, R. M., Al-Hadhrami, T., Husen, M. N., Ali, N. A., Al-Othmani, A., ... & Ochiai, H. (2020). Security assessment model to analysis DOS attacks in WSN. In *Emerging Trends in Intelligent Computing and Informatics: Data Science, Intelligent Information Systems and Smart Computing 4* (pp. 789-800). Springer International Publishing.
121. Niksaz, P., & Branch, M. (2015). Wireless body area networks: attacks and countermeasures. Int. J. Sci. Eng. Res, 6(9), 556-568.
122. Karchowdhury, S., & Sen, M. (2019). Survey on attacks on wireless body area network. International Journal of Computational Intelligence & IoT, Forthcoming.
123. Khader, R., & Eleyan, D. (2021). Survey of dos/ddos attacks in iot. *Sustainable Engineering and Innovation*, *3*(1), 23-28.
124. Newsome, J., Shi, E., Song, D., & Perrig, A. (2004, April). The sybil attack in sensor networks: analysis & defenses. In Third international symposium on information processing in sensor networks, 2004. IPSN 2004 (pp. 259-268). IEEE.
125. Arshad, A., Hanapi, Z. M., Subramaniam, S., & Latip, R. (2021). A survey of Sybil attack countermeasures in IoT-based wireless sensor networks. PeerJ Computer Science, 7, e673.
126. Sasirekha, D., & Radha, N. (2017, October). Secure and attack aware routing in mobile ad hoc networks against wormhole and sinkhole attacks. In 2017 2nd international conference on communication and electronics systems (ICCES) (pp. 505-510). IEEE.
127. Asimakopoulos, V. (2019). *Datasets for intrusion detection for wireless body area networks* (Master's thesis, Πανεπιστήμιο Πειραιώς).
128. Kala, P. C., Agrawal, A. P., & Sharma, R. R. (2020, January). A novel approach for isolation of sinkhole attack in wireless sensor networks. In 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 163-166). IEEE.
129. Weidong Fang, Fengrong Li, Yanzan Sun, Lianhai Shan, Shanji Chen, Chao Chen, Meiju Li, "Information Security of PHY Layer in Wireless Networks", *Journal of Sensors*, vol. 2016, Article ID 1230387, 10 pages, 2016. https://doi.org/10.1155/2016/1230387
130. Selem, E.; Fatehy, M.; Abd El-Kader, S.M. mobthe (mobile temperature heterogeneity energy) aware routing protocol for wban iot health application. IEEE Access 2021, 9, 18692–18705
131. Bhattasali, T., & Chaki, R. (2012). AMC model for denial of sleep attack detection. arXiv preprint arXiv:1203.1777.
132. Bhattasali, T., Chaki, R., & Sanyal, S. (2012). Sleep deprivation attack detection in wireless sensor network. arXiv preprint arXiv:1203.0231.
133. Boubiche, D. E., Bilami, A., & Athmani, S. (2012, April). A Cross Layer Energy Efficient Security Mechanism for Denial of Sleep Attacks on Wireless Sensor Network. In International Conference on Networked Digital Technologies (pp. 151-164). Springer, Berlin, Heidelberg.
134. Wu, C. H., & Chung, Y. C. (2007, May). Heterogeneous wireless sensor network deployment and topology control based on irregular sensor model. In International Conference on Grid and Pervasive Computing (pp. 78-88). Springer, Berlin, Heidelberg.
135. Bhattasali, T., & Chaki, R. (2011). Lightweight hierarchical model for HWSNET. arXiv preprint arXiv:1111.1933.
136. Suma, S., & Harsoor, B. (2022). An approach to detect black hole attack for congestion control utilizing mobile nodes in wireless sensor network. *Materials Today: Proceedings*, *56*, 2256-2260.
137. Periyanayagi, S., & Sumathy, V. (2013). Swarm based defense technique for denial-of-sleep attacks in wireless sensor networks. Int. Rev. Comput. Softw.(IRECOS), 8(6), 1263-1270.
138. Gabrielli, A., Conti, M., Pietro, R. D., & Mancini, L. V. (2009, September). Sec-tmp: a secure topology maintenance protocol for event delivery enforcement in wsn. In International Conference on Security and Privacy in Communication Systems (pp. 265-284). Springer, Berlin, Heidelberg..
139. Pirretti, M., Zhu, S., Vijaykrishnan, N., McDaniel, P., Kandemir, M., & Brooks, R. (2006). The sleep deprivation attack in sensor networks: Analysis and methods of defense. International Journal of Distributed Sensor Networks, 2(3), 267-287.
140. Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. IEEE Pervasive Computing, 7(1), 74-81.
141. Chen, R. C., Hsieh, C. F., & Huang, Y. F. (2010). An isolation intrusion detection system for hierarchical wireless sensor networks. *J. Networks*, *5*(3), 335-342.
142. Chen, R. C., Hsieh, C. F., & Huang, Y. F. (2010). An isolation intrusion detection system for hierarchical wireless sensor networks. J. Networks, 5(3), 335-342.
143. Juneja, D., Arora, N., & Bansal, S. (2010). An ant-based routing algorithm for detecting attacks in wireless sensor networks. International Journal of Computational Intelligence Research, 6(2), 311-320.
144. Saha, S. (2013). ZigBee OPNET modeler: An efficient performance analyzer for wireless sensor networks. International Journal of Engineering Sciences & Research Technology, 2(8).
145. Falk, R., & Hof, H. J. (2009, June). Fighting insomnia: A secure wake-up scheme for wireless sensor networks. In 2009 Third International Conference on Emerging Security Information, Systems and Technologies (pp. 191-196). IEEE.
146. A. Kavoukis and S. Aljareh, "Efficient time synchronized one-time password scheme to provide secure wake-up authentication on wireless sensor networks," arXiv preprint arXiv:1302.1756, 2013.
147. R. Rughinis and L. Gheorghe, "Storm control mechanism in wireless sensor networks," in Roedunet International Conference (RoEduNet), 2010 9th, 2010, pp. 430-435.
148. D. R. Raymond and S. F. Midkiff, "Clustered adaptive rate limiting: Defeating denial-of-sleep attacks in wireless sensor networks," in Military Communications Conference, 2007. MILCOM 2007. IEEE, 2007, pp. 1-7.

149. C. Chen, L. Hui, Q. Pei, L. Ning, and P. Qingquan, "An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks," in Information Assurance and Security, 2009. IAS'09. Fifth International Conference on, 2009, pp. 446-449.
150. K. Premkumar and A. Kumar, "Optimal sleep-wake scheduling for quickest intrusion detection using sensor networks," in Proc. IEEE Infocom, 2008.
151. P. Sharma, N. Sharma, and R. Singh, "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network," International Journal of Computer Applications, vol. 41, pp. 16-21, 2012.
152. C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme for power exhausting attacks in wireless sensor networks," in Proc. 3rd Int. Conf. Ubiquitous Future Netw. (ICUFN), Dalian, China, Jun. 2011, pp. 258–263.
153. C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "Two-tier receiver-initiated secure scheme for hierarchical wireless sensor networks," in Proc. 12th Int. Conf. ITS Telecommun. (ITST), Taipei, Taiwan, 2012, pp. 254–258.
154. V. Srivastava and M. Motani, "Cross-layer design: A survey and the road ahead," IEEE Commun. Mag., vol. 43, no. 12, pp. 112–119, Dec. 2005.
155. Polastre, J., Hill, J., & Culler, D. (2004, November). Versatile low power media access for wireless sensor networks. In Proceedings of the 2nd international conference on Embedded networked sensor systems (pp. 95-107).
156. V. Srivastava, and M. Motani, "Cross-layer design: a survey and the road ahead," IEEE Communications Magazine, 2005, Vol. 43, No. 12, pp.112-119.
157. W. Ye, J. Heidemann, and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," in Proc. INFOCOM: Proceedings of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, Univ. of Southern California, CA, USA, 2002, pp. 1567- 1576.
158. M. Buettner, G. V. Yee, E. Anderson, and R. Han, "X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks," in Proc. ACM SenSys '06: Proceedings of the 4th International Conference on Embedded Networked Sensor Systems, Boulder, USA, 2006, pp.307-320.
159. Y. Sun, O. Gurewitz, and D. B. Johnson, "RI-MAC: a receiver-initiated asynchronous duty cycle MAC protocol for dynamic traffic loads in wireless sensor networks," In Proc. ACM SenSys'08: Proceedings of the 6th International Conference on Embedded Networked Sensor Systems, Raleigh, USA, 2008, pp. 1-14.
160. Joon-Min Gil and Youn-Hee Han. A Target Coverage Scheduling Scheme Based on Genetic Algorithms in Directional Sensor Networks. Sensors 2011, 11, 1888-1906; doi:10.3390/s110201888.
161. Bhatia, T., Kansal, S., Goel, S., & Verma, A. K. (2016). A genetic algorithm based distance-aware routing protocol for wireless sensor networks. Computers & Electrical Engineering, 56, 441-455.
162. M. Esnaashari, M.R. Meybodi. A learning automata based scheduling solution to the dynamic point coverage problem in wireless sensor networks. Computer Networks 54 (2010) 2410–2438.
163. Mostafaei, H., & Meybodi, M. R. (2013). Maximizing lifetime of target coverage in wireless sensor networks using learning automata. *Wireless Personal Communications*, *71*(2), 1461-1477.
164. Jung, B. (2005). Cooperative target tracking using mobile robots. University of Southern California.
165. Bagci, H.; Yazici, A. An energy aware fuzzy unequal clustering algorithm for wireless sensor networks. In Proceedings of the International Conference on Fuzzy Systems, Barcelona, Spain, 18–23 July 2010; pp. 1–8.
166. Zhi Li, Meng Chen, Guanglie Zhang. Variable-rate transmission method with coordinator election for wireless body area networks. Wireless Network (2015) 21:2169–2180.
167. Dimitrios Zorbas and Christos Douligeris. Power Efficient Target Coverage in Wireless Sensor Networks. Indian Journal of Science and Technology. Volume 7, Supplementary 4, April 2014.
168. Jocelyne Elias (2014); Optimal design of energy-efficient and cost-effective wireless body area networks, Elsevier, Ad Hoc Networks, 13, 560–574.
169. Kanaga Suba Raja, Usha Kiruthika (2015); "An Energy Efficient Method for Secure and Reliable Data Transmission in Wireless Body Area Networks Using RelAODV", Springer, Wireless Pers Commun
170. Vinodhini, R., & Gomathy, C. (2020). MOMHR: a dynamic multi-hop routing protocol for WSN using heuristic based multi-objective function. *Wireless Personal Communications*, *111*, 883-907.
171. Zhou, Z., Zhou, S., Cui, J. H., & Cui, S. (2008). Energy-efficient cooperative communication based on power control and selective single-relay in wireless sensor networks. IEEE transactions on wireless communications, 7(8), 3066-3078.
172. Guo, H., Wang, F., Zhang, L., & Luo, J. (2019). A hierarchical optimization strategy of the energy router-based energy internet. *IEEE Transactions on Power Systems*, *34*(6), 4177-4185.
173. Uthayakumar, J., Metawa, N., Shankar, K., & Lakshmanaprabu, S. K. (2020). Intelligent hybrid model for financial crisis prediction using machine learning techniques. *Information Systems and e-Business Management*, *18*, 617-645.
174. Radamson, H. H., Zhu, H., Wu, Z., He, X., Lin, H., Liu, J., ... & Wang, G. (2020). State of the art and future perspectives in advanced CMOS technology. Nanomaterials, 10(8), 1555.
175. Anderson, R., Chan, H., & Perrig, A. (2004, October). Key infection: Smart trust for smart dust. In Proceedings of the 12th IEEE International Conference on Network Protocols, 2004. ICNP 2004. (pp. 206-215). IEEE.
176. Udoh, E., & Getov, V. (2018, March). Performance analysis of denial-of-sleep attack-prone MAC protocols in wireless sensor networks. In *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim)* (pp. 151-156). IEEE.
177. Islam, M. N. U., Fahmin, A., Hossain, M., & Atiquzzaman, M. (2021). Denial-of-service attacks on wireless sensor network and defense techniques. *Wireless Personal Communications*, *116*(3), 1993-2021.
178. Mirjalili S, Dong JS, Sadiq AS, Faris H. Genetic algorithm: Theory, literature review, and application in image reconstruction. Nature-inspired optimizers. 2020:69-85.
179. Shi, Q., Qin, L., Ding, Y., Xie, B., Zheng, J., & Song, L. (2019). Information-aware secure routing in wireless sensor networks. Sensors, 20(1), 165.
180. Saini TK, Sharma SC. Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept. Ad Hoc Networks. 2020;103:102148.
181. Boulaiche M. Survey of Secure Routing Protocols for Wireless Ad Hoc Networks. Wireless Personal Communications. 2020;114(1):483-517.
182. Boulaiche M. Survey of Secure Routing Protocols for Wireless Ad Hoc Networks. Wireless Personal Communications. 2020;114(1):483-517.
183. Karthick, P. T., & Palanisamy, C. (2019). Optimized cluster head selection using krill herd algorithm for wireless sensor network. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *60*(3), 340-348.
184. Han, J., Pei, J., & Tong, H. (2022). Data mining: concepts and techniques. Morgan kaufmann.
185. Safara F, Souri A, Baker T, Al Ridhawi I, Aloqaily M. PriNergy: A priority-based energy-efficient routing method for IoT systems. The Journal of Supercomputing. 2020:1-18.

186. Otoum S, Kantarci B, Mouftah HT, editors. Mitigating False Negative intruder decisions in WSN-based Smart Grid monitoring. 2017 13th International wireless communications and mobile computing conference (IWCMC); 2017: IEEE.
187. Chen, H., Zhang, C., Zong, X., & Wang, C. (2013). LEACH-G: an Optimal Cluster-heads Selection Algorithm based on LEACH. *J. Softw.*, *8*(10), 2660-2667.
188. Yadav, L., & Sunitha, C. (2014). Low energy adaptive clustering hierarchy in wireless sensor network (LEACH). *International journal of computer science and information technologies*, *5*(3), 4661-4664.
189. Tandel, R. I. (2016). Leach protocol in wireless sensor network: a survey. International Journal of Computer Science and Information Technologies, 7(4), 1894-1896.
190. Mirjalili, S., Song Dong, J., Sadiq, A. S., & Faris, H. (2020). Genetic algorithm: Theory, literature review, and application in image reconstruction. Nature-inspired optimizers, 69-85.
191. Pal, V., Singh, G., & Yadav, R. P. (2015). Cluster head selection optimization based on genetic algorithm to prolong lifetime of wireless sensor networks. Procedia Computer Science, 57, 1417-1423.
192. Lambora, A., Gupta, K., & Chopra, K. (2019, February). Genetic algorithm-A literature review. In 2019 international conference on machine learning, big data, cloud and parallel computing (COMITCon) (pp. 380-384). IEEE.
193. Xian, X., Shi, W., & Huang, H. (2008, June). Comparison of OMNET++ and other simulator for WSN simulation. In *2008 3rd IEEE Conference on Industrial Electronics and Applications* (pp. 1439-1443). IEEE
194. Zhang, J., Li, W., Cui, D., Zhao, X., & Yin, Z. (2009, September). The NS2-based simulation and research on wireless sensor network route protocol. In 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing (pp. 1-4). IEEE.
195. Chung, J., & Claypool, M. (2002). NS by Example. Disponível na Internet via URL: http://nile. wpi. edu/NS. Arquivo capturado em, 20.
196. Zhong, L.; He, S.; Lin, J.; Wu, J.; Li, X.; Pang, Y.; Li, Z. Technological Requirements and Challenges in Wireless Body Area Networks for Health Monitoring: A Comprehensive Survey. *Sensors* 2022, *22*, 3539.
197. Yaghoubi, M., Ahmed, K., & Miao, Y. (2022, November). TIDS: Trust Value-Based IDS Framework for Wireless Body Area Network. In *2022 32nd International Telecommunication Networks and Applications Conference (ITNAC)* (pp. 142-148). IEEE