Artigo Técnico

Identification of anomalies generated by sensors that use variants of the LEACH protocol

Haroldo da Silva Ferreira[a*], Anderson Aparecido Alves da Silva[f g h i j], Kaique Almeida Justino da Silva[b], Adilson Eduardo Guelfi[c], José Ewerton da Cruz de Souza[d], Victor Orlando Toso de Oliveira Silveira[e]

[a] Egresso do Mestrado Profissional em Engenharia da Computação, Instituto de Pesquisas Tecnológicas do Estado de São Paulo S.A., São Paulo-SP, Brasil.

[b] Egresso do Mestrado Profissional em Computação Aplicada, Instituto de Pesquisas Tecnológicas do Estado de São Paulo S.A., São Paulo-SP, Brasil.

[c] Departamento de Ciência da Computação, Unoeste, Presidente Prudente-SP, Brasil.

[d] Departamento de Ciência da Computação, UFRN, Natal-RN, Brasil.

[e] Departamento de Ciência da Computação, Unoeste, Presidente Prudente-SP, Brasil.

[f] Docente do Mestrado Profissional em Computação Aplicada, Instituto de Pesquisas Tecnológicas do Estado de São Paulo S.A., São Paulo-SP, Brasil.

[g] Departamento de Tecnologia da informação, UNIP, São Paulo-SP, Brasil.

[h] Departamento de Tecnologia da informação, SENAC, São Paulo-SP, Brasil.

[i] Departamento de Tecnologia da informação, FIAP, São Paulo-SP, Brasil

[j] Departamento de Engenharia de sistemas eletrônicos, USP, São Paulo-SP, Brasil

* e-mail: haroldo.ferreira@wilsonsons.com.br

Keywords: networks, sensors, energy, security, efficiency.

Abstract

A Wireless Sensor Network is composed of several sensor nodes that are usually energized by a battery. Many studies direct their efforts to the possibility of these devices consuming less energy. Protocols such as LEACH are used to optimize device energy consumption and minimize security features. The FTE-LEACH protocol is a variant of LEACH, which acts to mitigate failures. In this way, we propose a statistical model that uses standard deviation to identify anomalies in the collected data that could harm the behavior of the network. Through the analysis of data collected from a Wireless Sensor Network implemented with FTE-Leach protocol, we were able to detect anomalous behavior. In experiments, anomalous nodes increase the network lifetime, but create holes in the perimeter, which, depending on where the Sensor Network is applied, can become compromised or ineffective.

1 Introduction

Research on Wireless Sensor Networks (WSN) has a large range of applications. For example, there are technological applications that use the infrastructure of a WSN for the power grid, water grid, transportation, and smart homes (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2014; NARAYANAN; SARATH; VINEETH, 2016). The WSN is a concept linked to the Internet of Things (IoT). While IoT does not assume a specific communication technology, wireless communication technologies play a very important role in building optimized, scalable, secure, and efficient WSN environments (SILVA *et al.*, 2019; FERRAZ JUNIOR *et al.*, 2021). WSN allows the sensing and control of more critical environments, or inhospitable access to wired networks and support applications that require many devices, in the order of tens to hundreds of sensors (OLIVEIRA, 2015).

Even with the benefits brought using WSN, there are some issues that still deserve attention, such as problems associated with performance, security, and energy savings. Performance assurance is often a more discussed issue than power consumption in WSN (OLIVEIRA, 2015). However, since energy consumption is a security issue (FERRAZ JUNIOR *et al.*, 2021), many sensor networks currently use techniques to optimize the energy consumption of sensor nodes (SINGH; SORAM; KHAN, 2016). The data processing and transmission steps to the base station provide study opportunities to save energy and improve the efficiency of the use of network resources. Authors such as Razaque *et al.* (2016) and Handy, Haase and Timmermann (2002) state that the data transmission

step is responsible for most of the energy consumption of the sensor node batteries. According to Singh, Soram and Khan (2016), sensor nodes are able to collect data and then route it to the base station. Using this type of communication model implies high energy consumption, as some nodes are far from the base station, and, as a result, consumption is disproportionate among the sensor nodes of a WSN.

The Low-Energy Adaptive Clustering Hierarchy (LEACH) is a cluster-based protocol that uses random cluster head rotation to evenly distribute the energy load between sensor nodes (HEINZELMAN; CHANDRAKASAN; BALAKRISHNAN, 2000). For Razaque *et al.* (2016), a protocol for creating network clusters is essential in WSN that need to save energy. It is the task of the cluster head to collect the information sent by the nodes and transmit it in a grouped way to a base station, thus avoiding data transmission over very long paths, making energy consumption more equitable between the nodes.

Another energy issue occurs when a node (outlier) transmits anomaly data to the base station due to low energy (ABO-ZAHHAD *et al.*, 2015). In addition to erroneous data, sensors can transmit false data when targeted by intruders. It is difficult to provide security in WSN as sensor nodes have limited hardware resources. Therefore, it is sometimes not advantageous to use encryption mechanisms (EL-SAADAWY; SHAABAN, 2012). Thus, the recognition of anomalous nodes is a critical and challenging issue for the reliable and secure dissemination of data in WSN (ZHANG; MERATNIA; HAVINGA, 2010).

Some protocols derived from LEACH are event-driven, such as the Energy Efficient Clustering Algorithm (EECED) (BUYANJARGAL; KWON, 2009), Energy Efficient Heterogeneous Clustered (EEHC), and Fault-tolerant and Energy efficient LEACH (FTE-LEACH) for example. The FTE-LEACH protocol uses the Received Signal Strength Indicator (RSSI) to make its probabilistic choice of a new cluster head. Thus, the change of this information due to a faulty sensor node or intrusion target jeopardizes the entire performance of a WSN (OLIVEIRA, 2015). Assuming that a base station has abundant computing power and capacity, the collected data could be properly analyzed by the base station (ALI; DEY; BISWAS, 2008). This ensures the integrity of the submitted data and makes the environment more qualified for behavioral analysis. Behavior analysis is a technique that can be used to detect statistical limits, identify anomalous data, guarantee integrity, and also serve to improve the reliability of the data collected (SONGMA *et al.*, 2012).

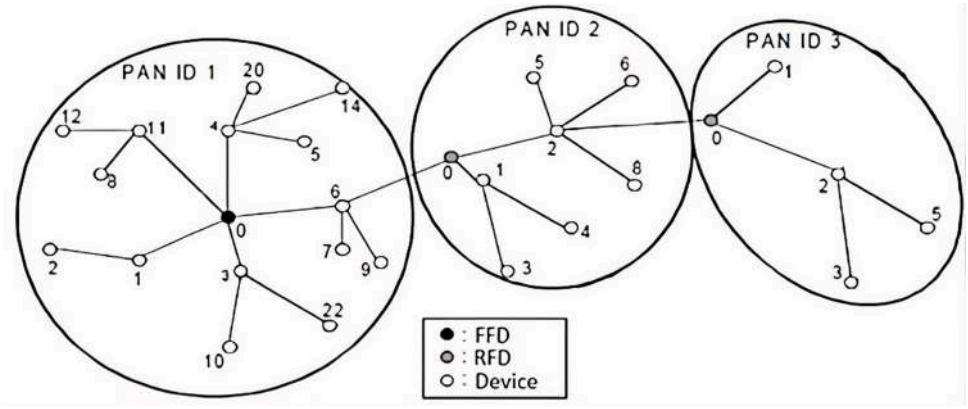
As can be seen in the referenced works, there is a need for research aimed at improving the security of the LEACH protocol variants, more specifically the analysis of energy consumption and the consequences that arise from this management, such as anomalous energy measurements. The creation of statistical models emerges as a viable alternative to alleviate these negative aspects.

This work intends to identify anomalies related to false information that is either maliciously inserted or sent unintentionally by devices with low power in variants of the LEACH protocol, working as an additional integrity layer to the information exchanged between the cluster head nodes and the base station. In addition to the Introduction, this work contains sections 2-Background and 3-Related Works, which deal respectively with the theory and the state of the art of research on LEACH. The proposal is described in section 4-Proposal, while the experiment and results are discussed in section 5-Experiments and Results and section 6-Results and general discussion. Finally, section 7-Conclusion brings conclusions about the paper.

2 Background

In a standard IEEE 802.15.4 network, two types of devices can be identified, Full Function Devices (FFD) and Reduced Function Devices (RFD). The FFD is a full-function device, as the name implies. These devices have greater processing and storage capacity on the network, in addition, the sensing function can have different activities, such as being a Cluster Head (SANTOS, 2017). For Santos (2017), the RFD, a reduced function device, is simpler, with less storage capacity, and is used at the ends of the networks, without a message resend function. These devices can only communicate with one FFD device and are not recommended for networks with many sensor nodes (IEEE 802.15.4, p. 4). **Figure 1** illustrates the IEEE 802.15.4 nodes and topology (SANTOS, 2017).

Figure 1 – IEEE 802.15.4 Topology



Source: Santos (2017)

As can be seen in **Figure 1**, the FFD node has hardware resources that meet the demand of its function, with continuous energy supply, characterizing itself as a base station – it is a Cluster Head. In turn, the RFD sensor node has sectored coordination and is generally used in clustered networks to communicate between the cluster sensor nodes and the FFD node.

The sensor node can be an FFD or RFD device, it has sensing functions and produces data to feed the WSN, and there can be several in each cluster. Since the IEEE 802.15.4 standard specifies only the physical layer and MAC, the network protocol responsible for delivering messages belongs to the network layer (OLIVEIRA, 2015). The biggest challenge is minimizing the energy consumption spent on routing tasks and maintaining aspects that preserve the quality of the network service (OLIVEIRA, 2015).

It is worth highlighting the definition of anomalous nodes in this paper. These are nodes that exhibit abnormal behaviors. These behaviors may be related to energy, processing, or even the dissemination of false messages. These nodes are called outliers precisely because they do not conform to normal patterns of behavior. Anomalous nodes pose a critical and challenging problem for WSN reliability, as they can be difficult to identify (ZHANG *et al.*, 2010).

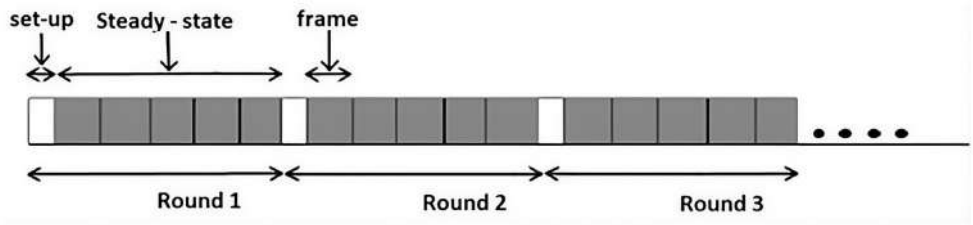
2.1 LEACH Protocol

The work of Heinzelman, Chandrakasan and Balakrishnan (2000) developed a cluster-based protocol that uses random Cluster Head rotation to evenly distribute the power load between sensor nodes. This type of protocol, called LEACH, uses coordination to allow scalability and robustness, in addition to incorporating data fusion into the routing protocol to reduce the amount of information that needs to be transmitted to the base station. Conventional direct broadcast, minimal power transmission, multi-hop routing, and static grouping protocols can be up to 80% less efficient when compared to LEACH (HEINZELMAN; CHANDRAKASAN; BALAKRISHNAN, 2000). The work of Handy, Haase and Timmermann (2002) describes the structure of the LEACH protocol, which works in two stages:

1) Set-up: corresponds to the configuration, comprising the stages of Cluster Head selection and the formation of clusters;

2) Steady-state: encompasses the aggregation and transmission of data to the base station, corresponding to the communication phase, as shown in **Figure 2**.

Figure 2 –LEACH Operation timeline



Source: Singh, Soram e Khan (2016).

As shown in **Figure 2**, the two phases (Set-up and Steady-state) take place during one round and each round has a fixed time duration. In the LEACH configuration phase, the algorithm selects the Cluster Heads, forming the cluster of nodes and assigning a Time Division Multiple Access (TDMA) slot to each member node. Each node participates in the Cluster Head election process, generating a priority value between 0 and 1.

When the generated value number for a node is less than the threshold value, then that node becomes a Cluster Head. This process is pertinent to avoid fixed Cluster Heads, which would accelerate energy consumption. The probability equation for a node to become a Cluster Head is presented below, as shown in **Equation 1**.

$$T(n) = \frac{P}{1-P\left(r \bmod \left(\frac{1}{p}\right)\right)}, \forall n \in G, T(n) = 0, \forall n \notin G \quad \textbf{(1)}$$

Where:

T(n) = probability threshold value for node n (dimensionless);

p = predefined probability of a node becoming a Cluster Head (dimensionless);

r = current round number (dimensionless);

mod = mathematical operator, which returns the remainder of a division;

n = unique identifier of the sensor node in the network (dimensionless);

G = mathematical set of sensor nodes that have not been elected as Cluster Heads in the last 1/p rounds (dimensionless);

∀= mathematical universal quantifier meaning "for all" or "for each";

∈ e ∉ = mathematical set operators meaning "belongs to" and "does not belong to", respectively".

Equation 1 shows the probability equation for electing a Cluster Head where r is the current round, T(n) is the probability of a node becoming Cluster Head in r, p is the desirable percentage of Cluster Heads, and $n \in G$ is the node which can be a candidate for Cluster Head in round r (HANDY; HAASE; TIMMERMANN, 2002).

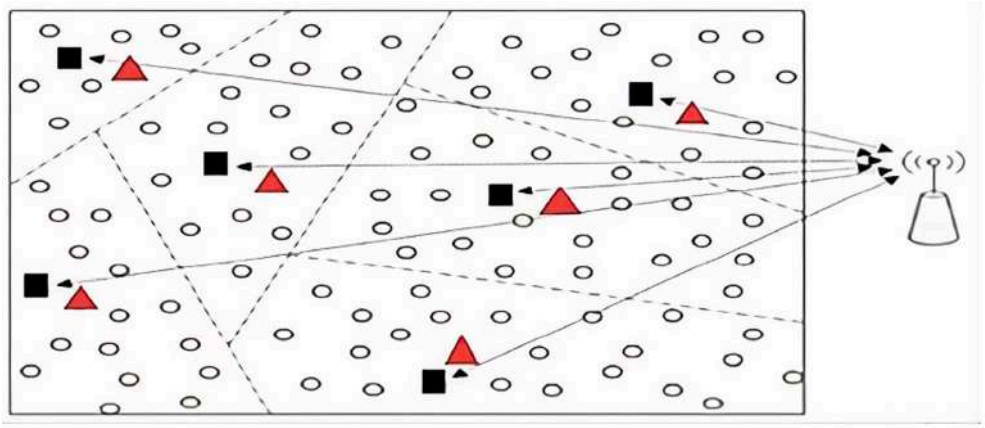
The LEACH protocol uses a probabilistic method for Cluster Head election, not based on the amount of energy that each node has, which can cause problems in the cluster formation process, giving priority to a node with low energy. If a node is used inefficiently, it is necessary to have more Cluster Heads **to form the clusters**, increasing energy consumption. In addition to the cluster creation step, the Cluster Head election determines the number of turns a network reaches (RAFIQ *et al.*, 2015). A turn is the cycle that begins with the choice of Cluster Head, followed by the formation of clusters, and ending when the last Cluster Head sends its data to the base station. A sensor is considered dead when it does not have enough power to communicate on the network and is no longer present for the next few turns. The number of turns is used to determine the lifetime of a WSN or can be used as a metric to determine the death (total power outage) of the first sensor node, the death of half of the network, and the end of the cycle of the entire network, when the last sensor dies. This metric is used by several authors, such as Abidi and Ezzedine (2017) and Abo-Zahhad *et al.* (2015), to determine the efficiency of an experiment.

To overcome this type of difficulty, Razaque *et al.* (2016) proposed an adaptation to the LEACH protocol, in its algorithm, considering the residual energy of each node to elect a Cluster Head. The algorithm, called Hybrid-Low Energy Adaptive Clustering Hierarchy (H-LEACH), is used to find the lifetime of each node and the WSN.

2.2 FTE-LEACH Protocol

The FTE-LEACH protocol, developed in the works of Oliveira (2015) and Souza (2017), is another variation of LEACH protocol, with **fault-tolerant and event-driven characteristics** and event driven. The purpose of FTE-LEACH is to be an energy efficient protocol while maintaining efficiency in communication and data dissemination on the network. This protocol was developed based on the IEEE 802.15.4 standard. FTE-LEACH is designed to operate on medium and large industrial WSN networks with limited energy resources. A feature that stands out in this protocol is the use of Vice Cluster-Head (VCH). This is a sensor node that will take the place of the Cluster Head in case of failure. **Figure 3** highlights each element of a network topology using FTE-LEACH.

Figure 3 – FTE-LEACH Network topology.



Source: Oliveira (2015)

In **Figure 3**, the nodes represented by circles indicate the nodes that are members of the network. The nodes represented by squares are the Cluster Heads of the round, while the nodes represented by triangles are the VCH. A differential used in FTE-LEACH to reduce interference is the use of the Four Color Theorem (HEAWOOD, 1949), distributing the clusters in a kind of map, where each cluster is represented by a color and allocated in channels. **Table 1** shows the distribution of the channels.

The channel distribution table in jumps considers the IEEE 802.15.4 standard, where there are 15 available channels on the 2.4 GHz frequency, starting at 2 and ending at 16, since channel 1 is considered the common channel of a WSN. The channels are distributed in jumps of 4, associating each color with a jump, the 4 colors represented are: Blue (B), Green (Gr), Pink (P), and Gray (G).

Table 1 – Distribution of the 15 available channels for the clusters, in steps of four, related to the Four Color Theorem.

Channels	2	6	10	14	3	7	11	15	4	8	12	16	5	9	13
Colors	B	Gr	P	G	P	Gr	P	G	B	Gr	P	G	B	G	P

Source: Oliveira (2015)

According to Oliveira (2015), the main contributions of FTE-LEACH are: reliability and availability of the network, sensing through the Cluster Head, scalability, event-driven data acquisition, prevention of intra-cluster interference, and active participation of the base station. In addition, it promises 20% more network lifetime compared to LEACH, although there is no simulation in the annexes of its work to evidence this claim.

3 Related Works

In this section, we seek to compare some relevant works that over time are related to the issues analyzed in this paper: studies on energy optimizations in WSN resulting from the application of the LEACH protocol and/or its variants; and the study of the influence of anomalies in these environments, as well as the identification of these malicious elements. **Table 2** contains a comparison between the studied references and the present paper.

Table 2 – Comparisons between related works.

Factors→ / References↓	Anomaly identification tool	Energy Saving method	Uses dataset	Simulation environment	LEACH Additional contributions	Uses LEACH	LEACH Variants
Rajasegarar *et al.* (2007)	Covariance, Mahalanobis distance	No	IBRL (INTEL BERKELEY RESEARCH LAB, 2004)	No	No	No	No
Sharma e Sharma (2012)	No	EEE-LEACH power analysis	No	MATLAB	Introduces Master Cluster Heads concept	Yes	EEE-LEACH
Tripathi *et al.* (2013)	No	Based on efficiency of protocol	No	NS-2	Yes	Yes	EELEACH-C
Abo-Zahhad *et al.* (2015)	No	Adaptative Immune Algorithm (AIA)	No	MATLAB	Introduces a mobile sink-based clustering protocol	Yes	MSIEEP
Xie, Hu e Guo (2015)	Covariance, Sperman correlation	No	IBRL (INTEL BERKELEY RESEARCH LAB, 2004)	No	No	No	No
Ferraz Junior *et al.* (2019)	Covariance, Mahalanobis, Euclidean distance	6LoWPAN Power Analysis	IBRL (INTEL BERKELEY RESEARCH LAB, 2004)	No	No	No	No
Almomani, Al-Kasasbeh e Al-Akhras (2016)	IDS, Neural Network	No	WSN-DS	NS-2	Develops a dataset	Yes	No
Ahmed *et al.* (2017)	No	Based on efficiency of protocol	No	NS-3	CH assigns a data transmission slot to each node	Yes	EESNR

Factors→ / References↓	Anomaly identification tool	Energy Saving method	Uses dataset	Simulation environment	LEACH Additional contributions	Uses LEACH	LEACH Variants
Almeida (2018)	Cluster, Mehalanobis distance	No	IBRL (INTEL BERKELEY RESEARCH LAB, 2004), LWSNDR (SUTHAHARAN *et al.*, 2010)	No	No	No	No
Mohapatra e Rath (2019)	Analyzes fault caused by power	Analyzes power depletion	No	MATLAB	Comparison with LEACH variants	Yes	PE-LEACH
Bhola, Soni e Cheema (2020)	No	Based on efficiency of protocol	No	MATLAB	Implements optimization with Genetic Algorithm	Yes	O-LEACH
Mittal *et al.* (2021)	IDS, SVM	Applies LMNN	NSLKDD	MATLAB	Comparison with EESR protocol	Yes	LEACH-LMNN
Bharany *et al.* (2021)	No	Based on efficiency of protocol	No	MATLAB	Comparison with LEACH variants, based on a flying ad-hoc network	Yes	No
Radhika e Sivakumar (2021)	No	Based on efficiency of protocol	No	MATLAB	Implements optimization with micro genetic algorithm	Yes	µGA-LEACH
Mittal *et al.* (2022)	SVM, KNN, LR	Based on efficiency of protocol and QoS	NSLKDD	MATLAB	Applies QoS	Yes	Sub-cluster LEACH
Nagarajan, Janakiraman e Balasubramanian (2022)	No	Based on efficiency of protocol	No	MATLAB	Implements optimization with Sail Fish Optimization and Jaya Algorithm	Yes	L-JSFO-LEACH
Ramya *et al.* (2022)	No	Based on efficiency of protocol	No	Yes	Analyses thermos-electrical efficiency	Yes	TN-LEACH
Ramesh *et al.* (2022)	No	Based on efficiency of protocol	No	Yes	Improvements with K-means	Yes	No
This Paper	Standard Deviation	Measurements in malicious and optimized scenarios	No	NS-3	Creates an attack environment	Yes	FTE-LEACH

Source: Elaborated by the author

The idea behind studying time frame references is simply to see if there are trends that come or go. However, as can be seen in Table 2, there is no predominance of trends over time. It is possible to see that a large part of the references, including this paper, use simulated environments to validate the results. The explanation is that since it is a driven--oriented protocol, LEACH is easily simulated, a fact that facilitates research. Although there are several variants of LEACH, the purpose of this paper is not to contribute or create a specific variant, so the choice of using FTE-LEACH happens simply because it is a protocol already used in a study focused on security (OLIVEIRA, 2015).

As it is essential in our proposal, we researched studies that carried out some type of analysis of energy consumption, including some that did not use LEACH. A point to be emphasized in this paper are the energy measurements performed in malicious (anomalous) situations and their comparison with the scenarios considered normal. Indeed, creating malicious scenarios and analyzing how anomalies can influence LEACH energy performance is one of the main contributions of this paper. There are few references that focus on security within the context studied. It is also important to point out that the anomaly identification method suggested here (standard deviation) is one of the simplest and fastest.

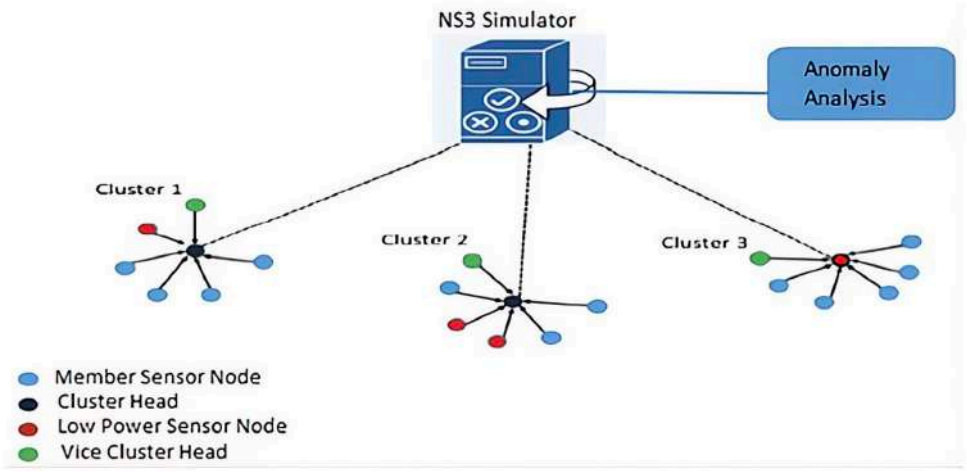
4 Proposal

It is considered that the occurrence of anomalous data (as stated in section 2) in WSN impairs the correct functioning of the environment, in addition to possibly increasing the energy consumption of the sensors and leading to the premature termination of the activities of a network (RASSAM; ZAINAL; MAAROF, 2013). The objective of the current work is to identify anomalies related to false information, maliciously inserted, or sent unintentionally by devices with power problems, in networks that use the LEACH protocol or its variants.

4.1 WSN topology using LEACH-based protocols

The topology applied to perform the simulation of a WSN that uses the LEACH protocol or its variants is shown in **Figure 4**. The base station is responsible for the analysis of anomalies, and the standard deviation model is used to identify them.

Figure 4 – WSN network topology using FTE-LEACH protocol.



Source: Elaborated by the author

The topology shown in **Figure 4**, elaborated in the NS-3 simulator, is the basis for the elaboration of the other scenarios used in this work. The scenario shows the low power nodes, which can unintentionally send false data, representing just one of the scenarios that are simulated and observed. An example of an anomalous scenario is sensor nodes that send opposite information about the current power state to other WSN nodes.

Each scenario studied uses twice as many Cluster Head sensor nodes elected in a round, when compared to normal scenarios. The works of Almomani, Al-Kasasbeh and Al-Akhras (2016), Oliveira (2015) and Souza (2017) provide the basis for using a scenario with LEACH and FTE-LEACH protocols, since the codes compiled for the simulation environments in the research are used with few alterations and serve to collect data from a standard environment. After executing the WSN lifecycle, a file with the network information is generated. Considering that energy resources are limited, anomaly identification must occur within the network itself and within the anomaly identification model executed in the base station.

4.2 Anomaly Identification Model

The purpose of anomaly detection is to identify data that does not conform to the patterns displayed by the majority of data in a set.

To perform this task, the current work presents the model for identifying anomalies. **Figure 5** shows its activity cycle, composed of 4 steps:

1) Preparation;
    a) Scenario compilation;
    b) Training and definition of statistical measures and limits;

2) Collection;
    a) Sending data from nodes;
    b) Receipt of data at the base station;
    c) Data formatting (period);
    d) Extraction of statistical characteristics;

3) Analysis;
    a) Statistical calculations of the standard deviation;

4) Comparison;
    a) General comparison of scenarios;
    b) Identification of anomalies.

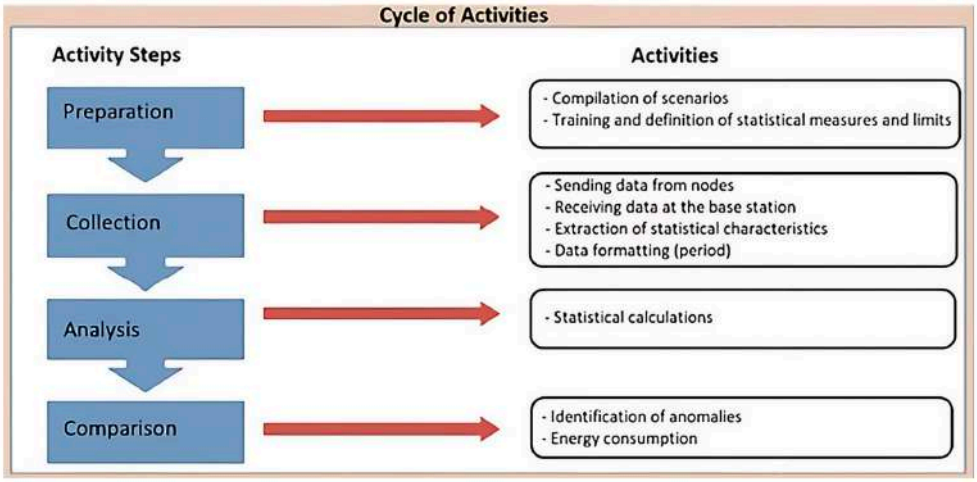
Preparation: Compile the proposed scenarios with the characteristics mentioned in Section 4.1. After the execution of the life cycle of a WSN in the simulation environment, which consists of sending the data made by the nodes, in the aggregation of the data made by the CH and sending it to the base station. A database is structured that aims to store the measurements collected.

Collection: The volume of measurements is considered and the time intervals necessary to obtain the measurements are defined. Time intervals assess temporal correlation, which combined with the number of measurements, allows standard deviation analysis.

Analysis: Next comes the definition of statistical measures, with the objective of providing the input of the analysis that will find the behavior of normal and anomalous measurements. The variability (standard deviation) of the measurements is observed.

Comparison: Compare the variability of energy measurements between normal nodes and poisoned nodes, using standard deviation.

Figure 5 – Activity cycle of the anomaly identification model.



Source: Elaborated by the author

5 Experiment and Results

To make the experiment feasible, the FTE-LEACH simulator is used (SOUZA, 2017). It is an adaptation with improvements for NS-3 on Linux Ubuntu made to the FTE-LEACH protocol (OLIVEIRA, 2015), emulated in MATLAB. The protocol is encapsulated within WHART and according to the author, this proves that in a simulation environment the protocol is more efficient and can be better analyzed.

Three identical virtual machines based on VMWare Workstation software are used, hosted on a desktop. A script (bash/Linux) is utilized to automate the simulation routines. Python's Random library is used to generate random numbers in some scenarios. The CC2500 transceiver (https://www.ti.com/product/CC2500) is used as a model of energy consumption for the sensors simulated in the experiments, working with different scales of its energy capacity measured in milliampere-hours (mAh). **Table 3** presents the equipment, software, and hardware used in the simulation environment.

For the choice of scenarios, different characteristics are important to simulate environments closer to the real situation and extract samples for later analysis, among these characteristics are: number of sensors (nodes), perimeter size, battery capacity (mAh), and the status of the sensors (anomalous or normal). All these properties are determined in the simulator source code before the simulation is compiled and run. **Table 4** details the 8 scenarios used.

Table 3 – Equipment, software and hardware used.

Hardware/Software	Function
Desktop Dell Core i7-8700, 2.4GHz, 16GB RAM, 120 HD SSD and Windows 10	Base equipment for the structure of experiments and virtual machine host.
VMWare Workstation 15.0 Player	Software for using virtual machines.
Linux Ubuntu 14.04 LTS	Base Operating System running on the virtual machine.
NS-3 3.26	Simulator Used.
Python and C++	NS-3 support and code compilation.

Source: Elaborated by the author.

Table 4 – Setup of scenarios

Simulation without anomalous sensors				
Scenario	Qty. Sensors	Perimeter	Same Initial Battery	Varying Initial Battery
1	20	100x100	S	S
2	20	200x200	S	S
3	100	100x100	S	S
4	100	200x200	S	S

Simulation with anomalous sensors				
Scenario	Qty. Sensors	Perimeter	Same Initial Battery	Varying Initial Battery
5	20	100x100	S	S
6	20	200x200	S	S
7	100	100x100	S	S
8	4	100	200x200	S

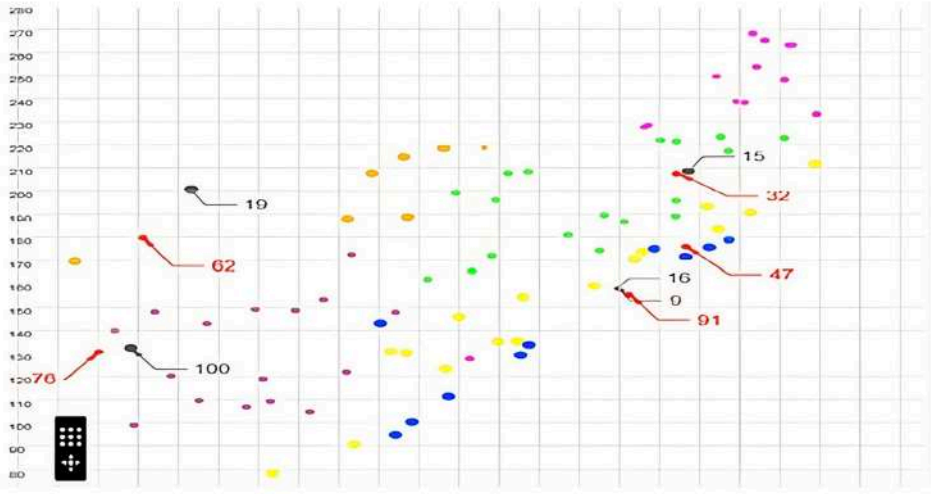
Source: Elaborated by the author.

In the experiments, 1800mAh batteries are used for scenarios with 20 sensor nodes and 3500mAh for scenarios with 100 sensor nodes. In scenarios with varying initial battery levels, the Python random library is used to generate random numbers and determine the initial percentage of battery level for sensor nodes. **Figure 6** shows how the nodes are distributed along the network perimeter, dividing their clusters by color, with the base station in the lower left corner.

The black sensor nodes 19, 100, 16, 9, and 15 are cluster heads. In red, the sensor nodes 76, 62, 91, 47, and 32 are the vice cluster head type. The clusters are divided by different colors. In the second round onwards in the scenarios with anomalous nodes, the sensor nodes further away from the base station always report having 5% more battery than the normal sensor node with the most battery in the round, thus forcing their election as cluster head while their real battery does not run out. The LEACH protocol chooses an ideal number of cluster heads; this number is determined by the number of sensor nodes in the network.

To simulate scenarios with anomalous nodes, double the number of anomalous nodes is adopted in relation to the ideal number of cluster heads. That is, when there are 5 cluster heads in the normal scenario, there are 10 poisoned nodes in the anomalous scenario. After all anomalous sensor nodes are depleted of energy, the network continues to function normally until the end of its life cycle. **Figure 6** shows setup with 100 nodes and 200x200 perimeter.

Figure 6 - Setup with 100 nodes and 200x200 perimeter.



Source: Elaborated by the author

5.1 Data collection

Each simulation starts after setting the scenario. The end is determined when all sensor nodes are out of power or when there are no nodes communicating with the base station. After the initialization phase, the simulation follows the steps determined by the LEACH protocol:

1) The protocol configuration phase, where the cluster heads and their clusters are elected;

2) The communication phase, when the cluster heads gather the information received and send it to the base station.

This process is repeated until the end of the network. After the end, the simulation environment extracts the output files, which contain information such as: number of turns, node consumption, node status, RSSI, number of packets sent, number of packets received, and residual energy per round.

Theoretically, the LEACH protocol tends to transform all nodes into CH or VCH over time, evenly dividing the energy consumption in each round. Therefore, to calculate the standard deviation of nodes, the number of rounds adopted is exactly the number of nodes in the network. In scenarios with 20 nodes, the standard deviation of each node is calculated every 20 runs. Likewise, in scenarios with 100 nodes, the calculation occurs every 100 rounds.

5.2 Comparison of the network characteristics

Some characteristics observed between the normal and anomalous scenarios are compared in **Table 5**. It maps some characteristics of the network, showing which data are collected and in what ways they are used in this research, in addition to describing the purpose of collecting each piece of data.

Table 5 - Characteristics of scenarios

Data collected	How it is used	Objective
Rounds	Check the number of the last round	Determine the size of the network lifetime
Consumption	Sum of node consumption per round	Check total network consumption per round and CH consumption per round.
Packets Sent	Sum of packets sent	Check the sum of all packets sent to the base station per round
Residual Energy	Mean Residual Energy of each sensor node	Check the average residual energy for each round
RSSI	Mean RSSI value of sensor nodes	Check the average RSSI value of each round
Sensor Node Status	Checks if the node is alive, dead, or has stopped communicating with the base station	Add up all dead nodes in each round.
Standard deviation	Checks for variability between anomalous and normal scenarios	Standard deviation of every n rounds (n = number of nodes)

Source: Elaborated by the author

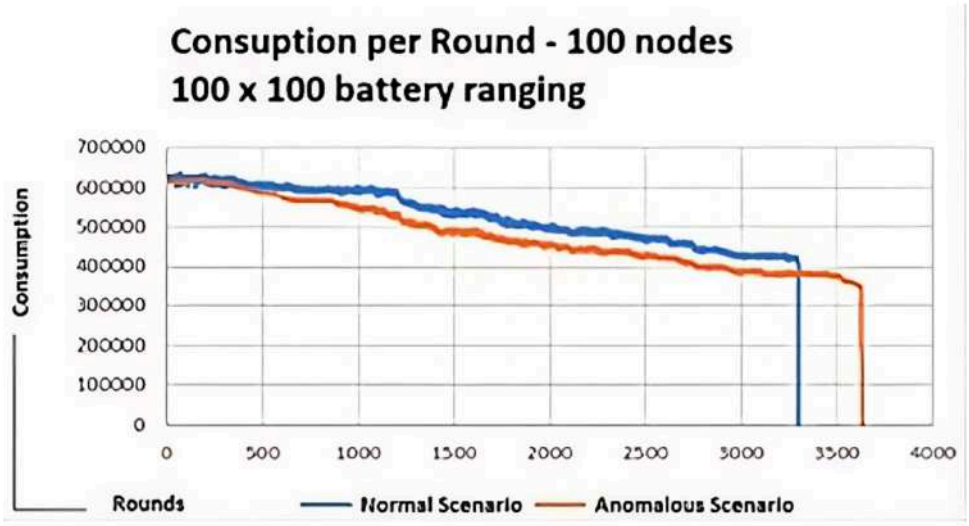
6 Results and general discussion

In total there are 8 scenarios created for the experiments. However, the comparisons involve only 3 normal scenarios with their respective anomalous versions, as these summarize the results found. **Figures 7, 8,** and **9** are a compilation of these 3 scenarios, called here A, B, and C.

It is worth noting that this choice is made precisely because A, B, and C represent all the results achieved in the other scenarios. Essentially, the results are repeated; therefore, to avoid unnecessary repetition, only these scenarios are discussed.

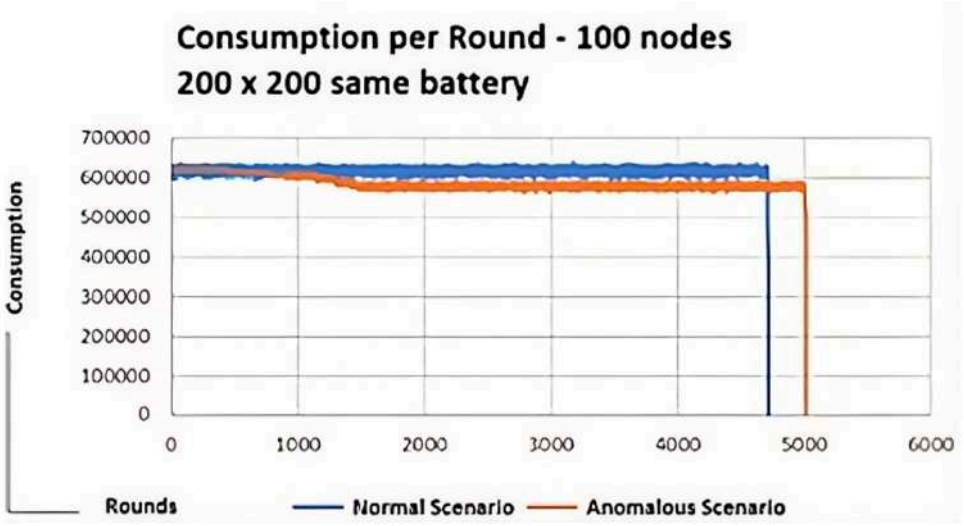
In **Figures 7, 8,** and **9,** the average consumption of nodes in anomalous scenarios is lower than in normal scenarios. The increase in the useful life of the network is around 10%, contrary to the initial expectations of this work. This occurs because the first sensor nodes to die are the nodes furthest from the base station, which were intentionally placed as anomalous nodes in the experiment, leaving the network more compact and generating cluster heads closer to the base station, which consume less energy because they are closer to the base station, which increases the life of the network.

Figure 7 – Consumption per round scenario A



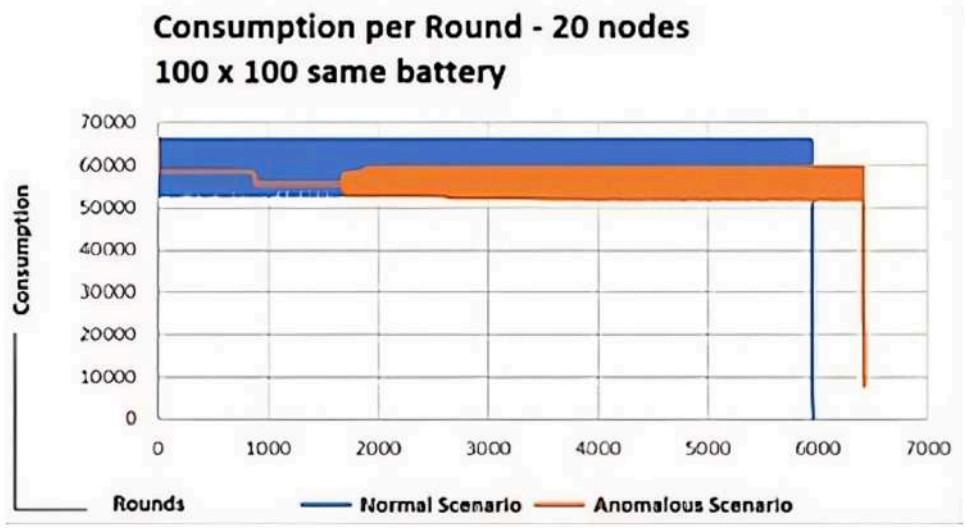
Source: Elaborated by the author

Figure 8 - Consumption per round scenario B



Source: Elaborated by the author

Figure 9 - Consumption per round scenario C

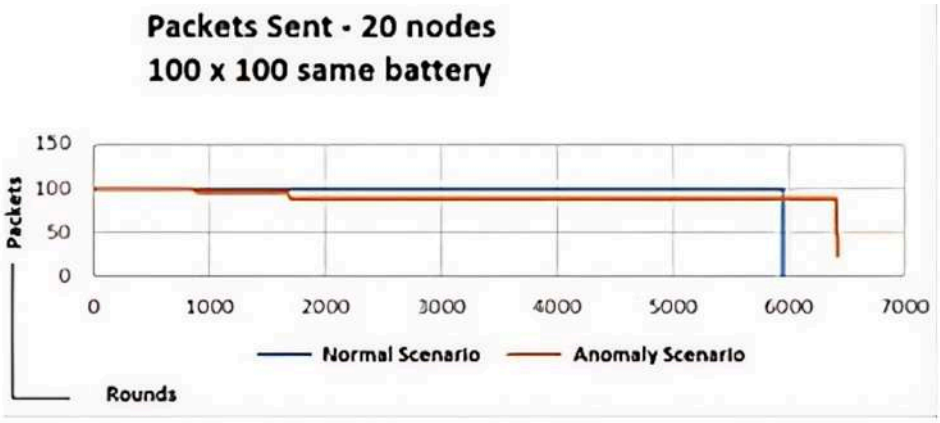


Source: Elaborated by the author

On the other hand, this causes holes in the network, leaving spaces around the perimeter without sensing. This result also contradicts the very reason for using variants of the LEACH protocol, which is to distribute the load between nodes – even if this decreases the network lifetime, holes in coverage tend not to occur. **Figures 10, 11,** and **12** show the compilation that deals with the number of packets sent by the sensor nodes.

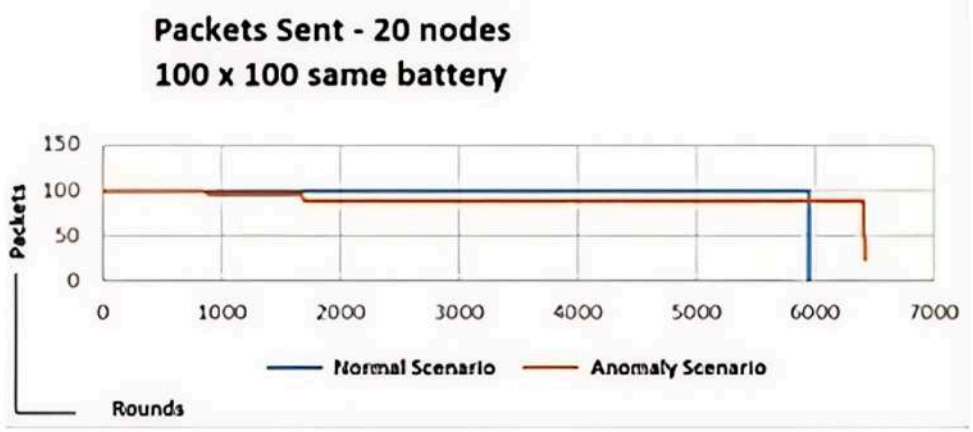
The number of packets sent refers to the packets transmitted by the sensor nodes to the cluster head and from the cluster head to the base station. As seen in **Figure 9**, all scenarios (normal and anomalous) start with the same number of packets sent. In anomalous scenarios, poisoned nodes run out of power before normal nodes. This ends up decreasing the number of active nodes in anomalous scenarios more quickly, as the anomalous sensor nodes die before half of the network's useful life, leaving areas without sensing.

Figure 10 – Packets sent scenario A.



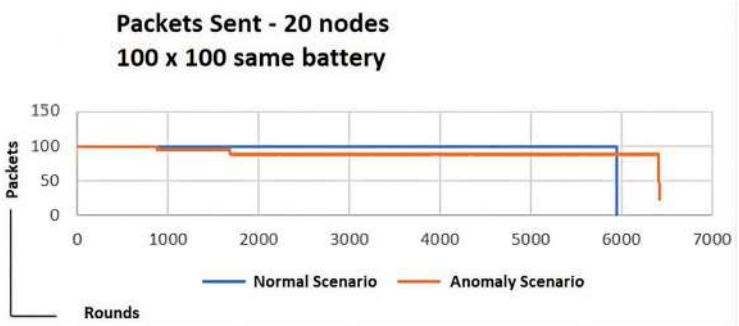
Source: Elaborated by the author

Figure 11 - Packets sent scenario B.



Source: Elaborated by the author

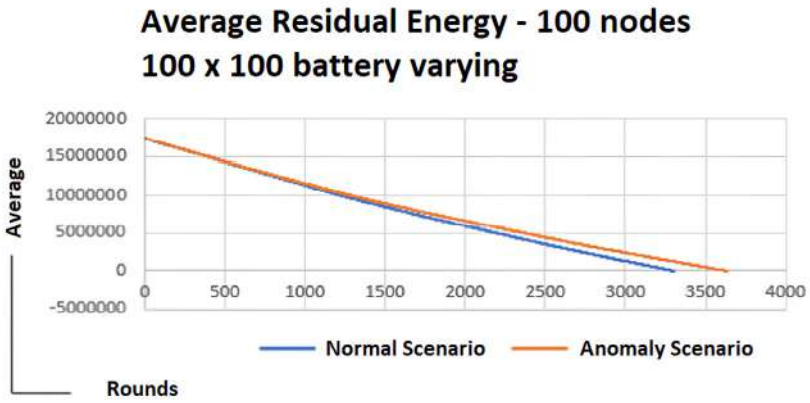
Figure 12 - Packets sent scenario C.



Source: Elaborated by the author

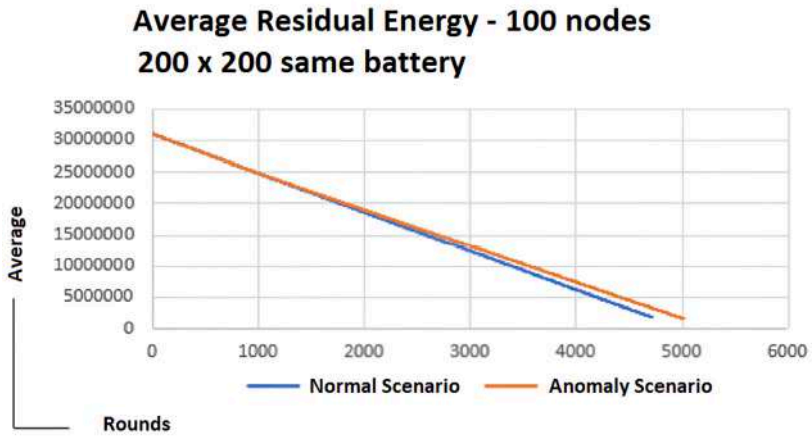
Figures 13, **14**, and **15** deal with the average residual energy of each sensor node per round.

Figure 13 – Mean residual energy scenario A.



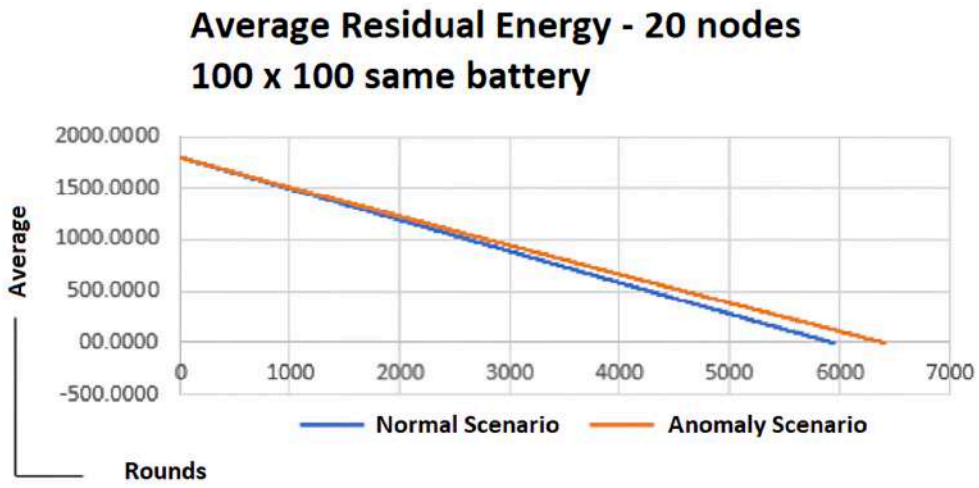
Source: Elaborated by the author

Figure 14 – Mean residual energy scenario B.



Source: Elaborated by the author

Figure 15 - Mean residual energy scenario C.

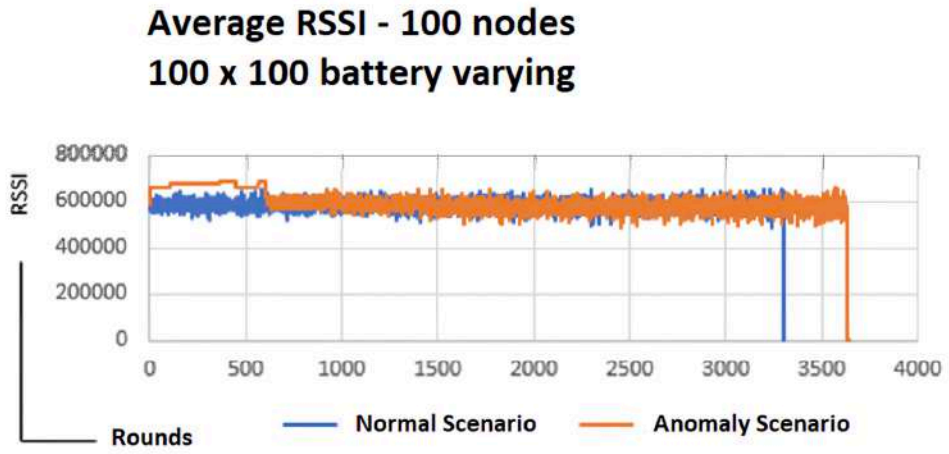


Source: Elaborated by the author

As seen in **Figures 13, 14** and **15**, in all scenarios the mean residual energy is linear. The actual consumption measured in this scenario uses the actual residual energy of each sensor node as given. Note that an anomalous sensor node sends a false energy value to the base station, however, **Figure 10** shows the real residual energy value of the nodes. As can be seen, the residual energy in both scenarios follows the same decreasing pattern, with the difference that in the anomalous scenario the useful life of the network is longer. **Figures 16, 17,** and **18** show the mean RSSI value of sensor nodes per round.

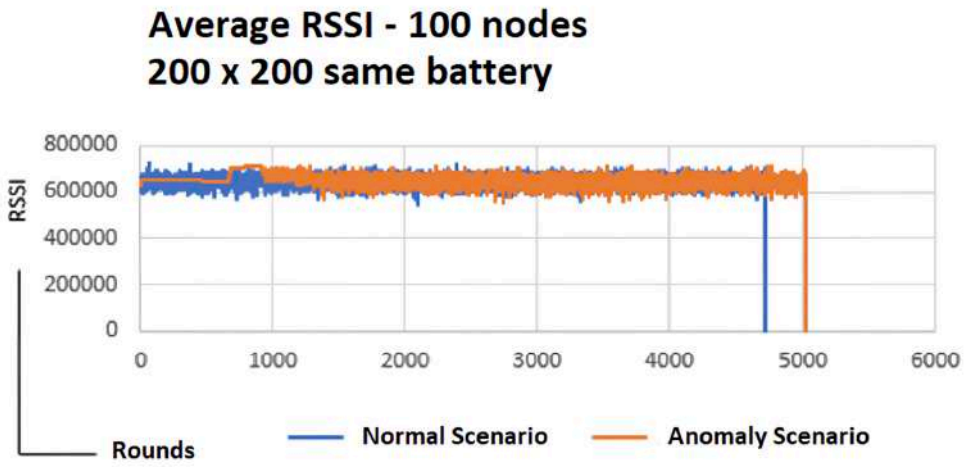
The mean RSSI is higher at the beginning of the anomalous scenarios, due to the fact that the cluster heads are the most distant sensor nodes from the base station in these scenarios. This fact is evident in the scenario with 100 sensor nodes and 100x100 perimeter, in the scenario with a 200x200 perimeter this accentuation is not so strong because sensor nodes with more than 224 meters do not communicate with the base station. When this occurs, the simulation algorithm chooses intermediate sensor nodes, that is, sensor nodes that are closer to the base station, to ensure that these anomalous sensor nodes communicate with the base station. As they are at distances close to normal sensor nodes, the RSSI average is very similar in both scenarios.

Figure 16 – Mean RSSI scenario A.



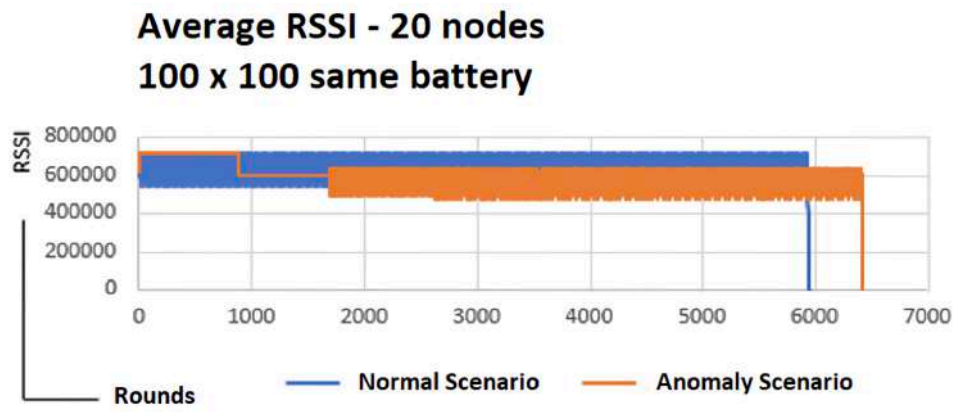
Source: Elaborated by the author

Figure 17 – Mean RSSI scenario B.



Source: Elaborated by the author

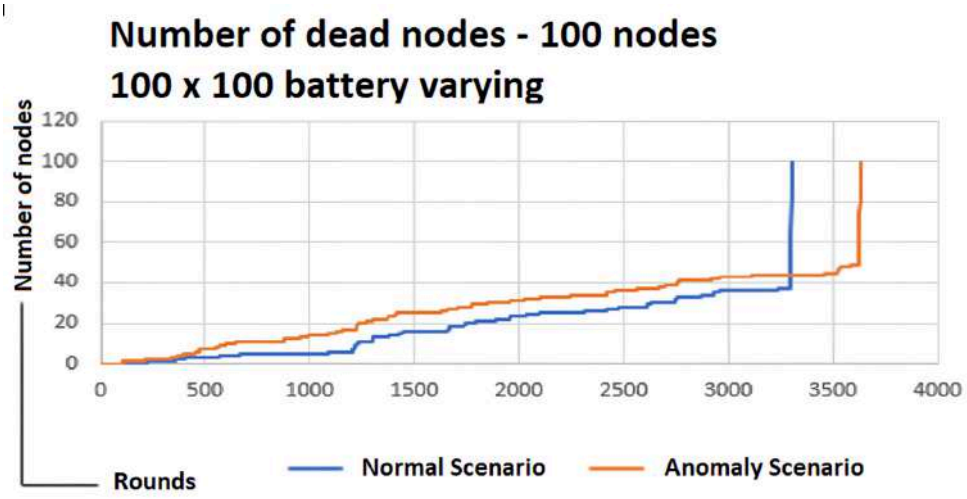
Figure 18 - Mean RSSI scenario C.



Source: Elaborated by the author

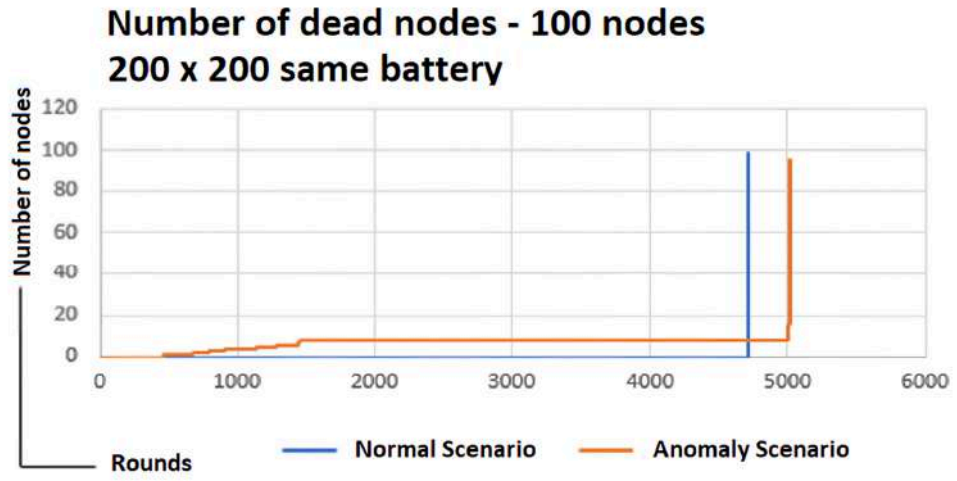
Next, in **Figures 19, 20,** and **21**, the beginning of sensor node deaths is shown.

Figure 19 – Death of sensor nodes scenario A.



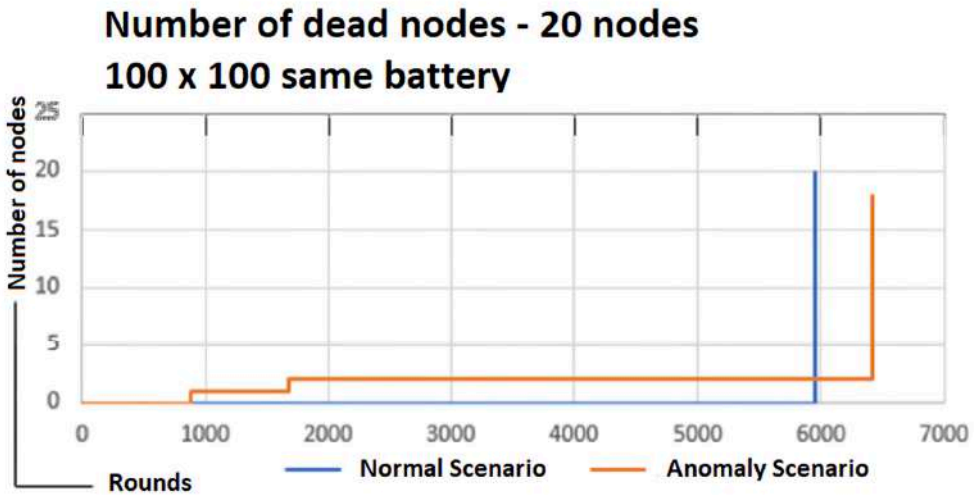
Source: Elaborated by the author

Figure 20 – Death of sensor nodes scenario B.



Source: Elaborated by the author

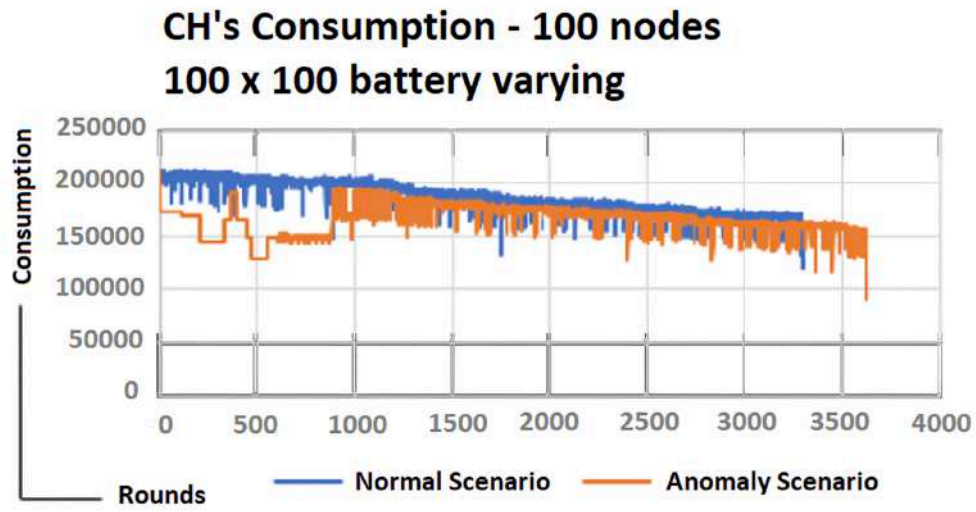
Figure 21 – Death of sensor nodes scenario C.



Source: Elaborated by the author

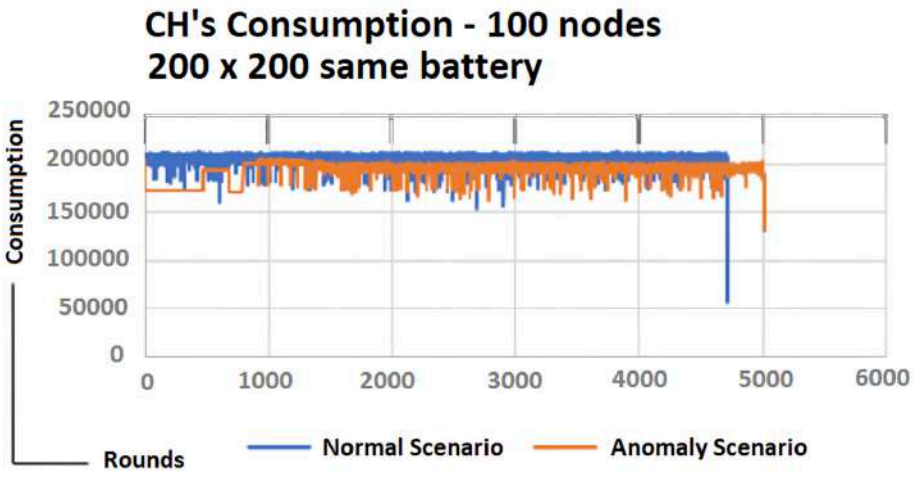
As seen in **Figures 19, 20,** and **21**, in anomalous scenarios, sensor nodes die well in advance of normal nodes, since they are the nodes that have cluster head status until the end of their life cycle. The final graphs, comparing the characteristics of the network (**Figure 22**, **23,** and **24**), deal with the cluster head consumption per round.

Figure 22 – Cluster head consumption scenario A.



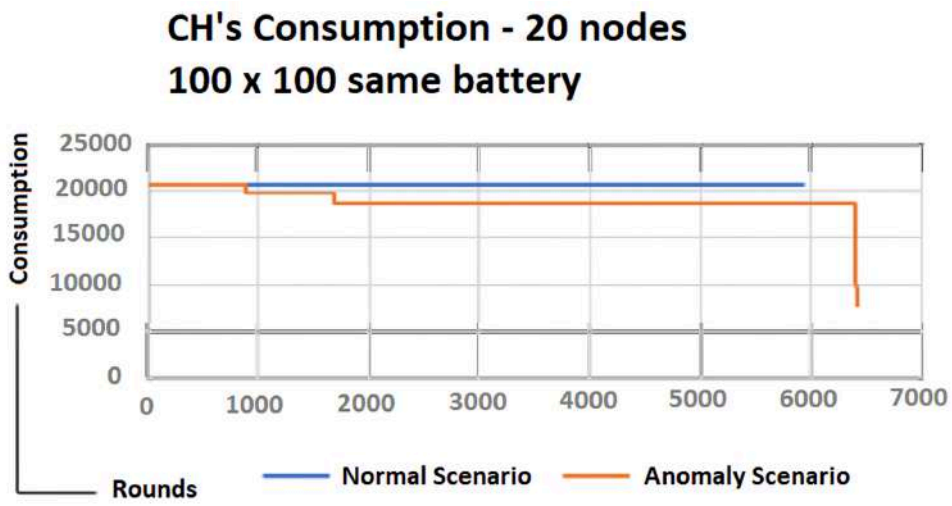
Source: Elaborated by the author

Figure 23 - Cluster head consumption scenario B.



Source: Elaborated by the author

Figure 24 - Cluster head consumption scenario C.



Source: Elaborated by the author

As seen in **Figures 22, 23,** and **24,** cluster head consumption in anomalous scenarios with 100 sensor nodes (**Figure 22** and **23**) is lower than in scenarios with 20 nodes (**Figure 24**). This is because when the most distant sensor nodes inform the false power status, the LEACH protocol elects them as cluster head. Thus, the protocol itself, based on the residual energy and distance from the sensor nodes, starts to use fewer clusters in the network, reducing the number from 5 to 4 cluster heads. In the scenario with 20 sensor nodes (**Figure 24**), initial consumption is the same, but after the death of the anomalous sensor nodes (which are the nodes furthest from base station) the live sensor nodes become the cluster head closer to the base station. The shorter the distance from the cluster head to the base station, the lower the consumption of this sensor node for transmitting the grouped data. Thus, a lower mean RSSI value is maintained in anomalous scenarios when compared to normal scenarios.

6.1 Identification of anomalies

As in the previous section, the comparison involves a reduced number of normal scenarios with their respective anomalous scenarios, as these summarize the results found in all scenarios. For each scenario, the graphs of 4 analyses performed are presented:

1) Standard deviation and a set of n rounds (n=number of nodes);

2) Mean of the standard deviation of the set of rounds;

3) Total standard deviation of the set of rounds;

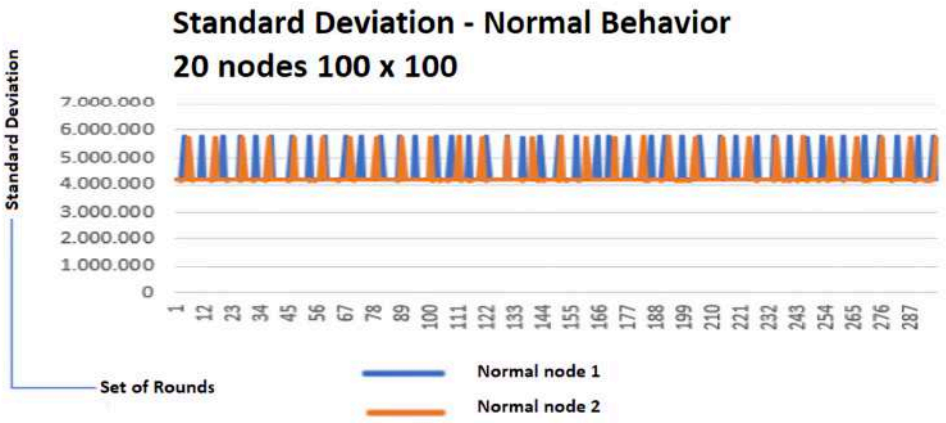
4) Number of times each sensor node is elected cluster head.

A set of rounds is used for scenarios with 20 sensor nodes, each set consists of 20 rounds. This section demonstrates more clearly how to identify anomalous behavior.

Figures 25 and **26** compare the standard deviation per round between 2 normal sensor nodes and 2 anomalous sensor nodes.

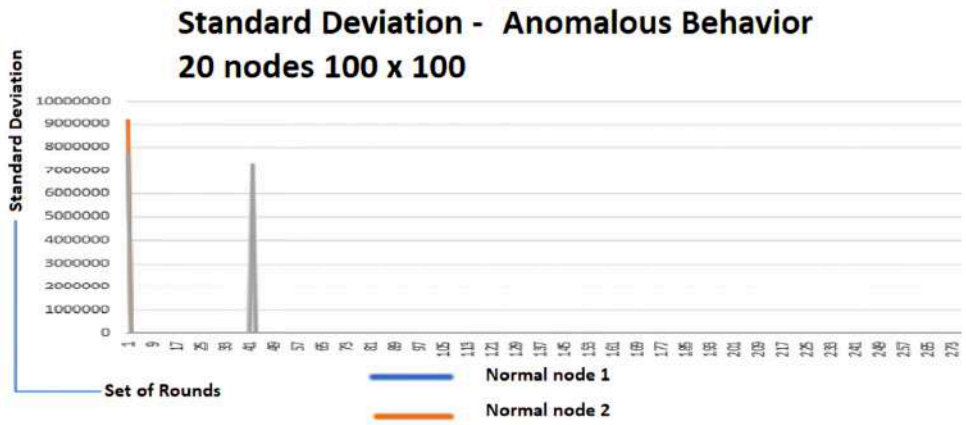
In the graph in **Figure 25**, a pattern of behavior is observed that occurs due to the alternation of the cluster head proposed by the FTE-LEACH protocol. The sensor node alternates its consumption, varying between high and low until the end of the network's useful life. In **Figure 26**, the graph with 2 sensor nodes with anomalous behavior, very little changes in the standard deviation over time, except for two gigantic peaks, one at the beginning and another between rounds 41 and 49.

Figure 25 - Standard deviation scenario A



Source: Elaborated by the author

Figure 26 - Standard deviation scenario B



Source: Elaborated by the author

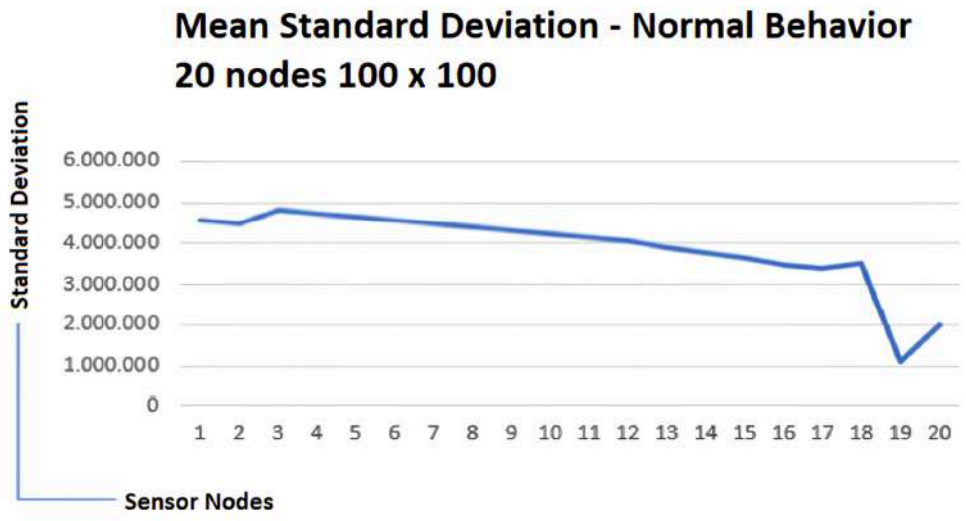
The explanation is that the two anomalous nodes assume the cluster head function precisely at these peaks. This radically alters the consumption pattern of these anomalous nodes. However, as these are constantly chosen as cluster head, due to the false energy value propagated in the network, the variability in the nodes decreases sharply in later rounds. This is repeated until the real power of the first anomalous node runs out and the second malicious node is chosen as cluster head, yielding the same results. It is important to note that the standard deviation of consumption of the other nodes in the network is also low, since they do not transform into cluster head during the periods of poisoning and almost always consume the same (little) energy during the rounds.

The graphs presented in **Figures 27** and **28** deal with the mean of the standard deviation of all sensor nodes in the network in the scenario with 20 nodes, with a perimeter of 100x100 and the same initial battery.

It is observed that the mean standard deviation found in the graph of **Figure 27** is linear and has a more accentuated decrease at the end, as nodes 19 and 20 are rarely used as cluster head due to the simple choice of protocol. Thus, these have a low mean standard deviation, while the others have a high mean standard deviation. In the graph of **Figure 28**, the highest point of the mean occurs in sensor nodes 11 and 12, which are anomalous sensor nodes, leaving the graph irregular, due to the mean standard deviation of these nodes being high.

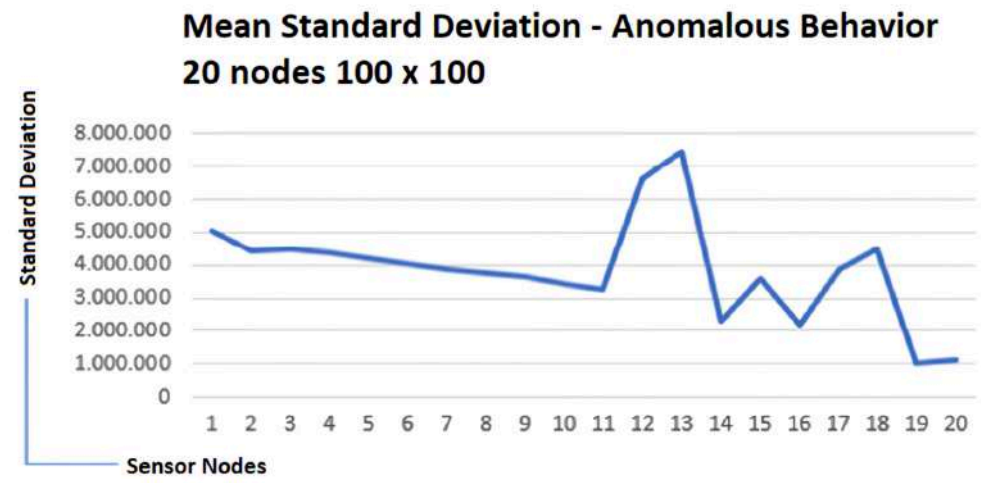
The increase in the mean standard deviation in the anomalous nodes occurs precisely because they were chosen as cluster head and alternating high and low consumption values, as previously observed in the peaks of **Figure 28.**

Figure 27 – Mean standard deviation scenario A



Source: Elaborated by the author

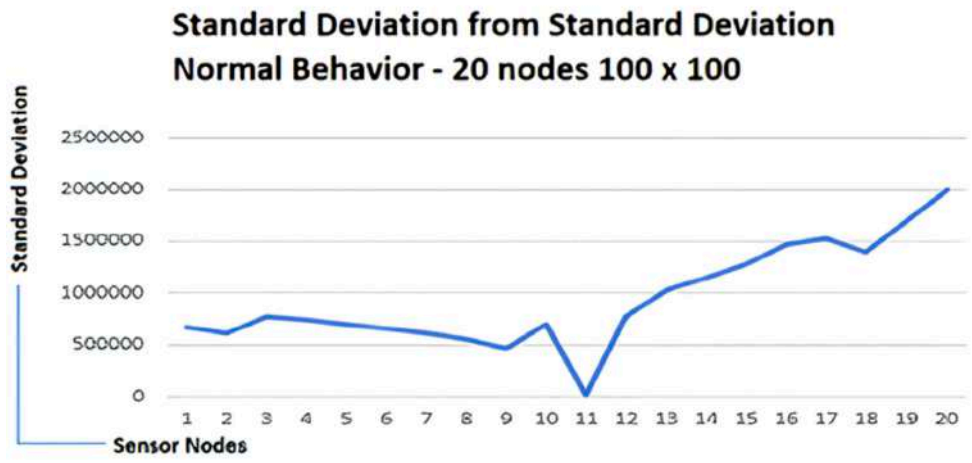
Figure 28 - Mean standard deviation scenario B



Source: Elaborated by the author

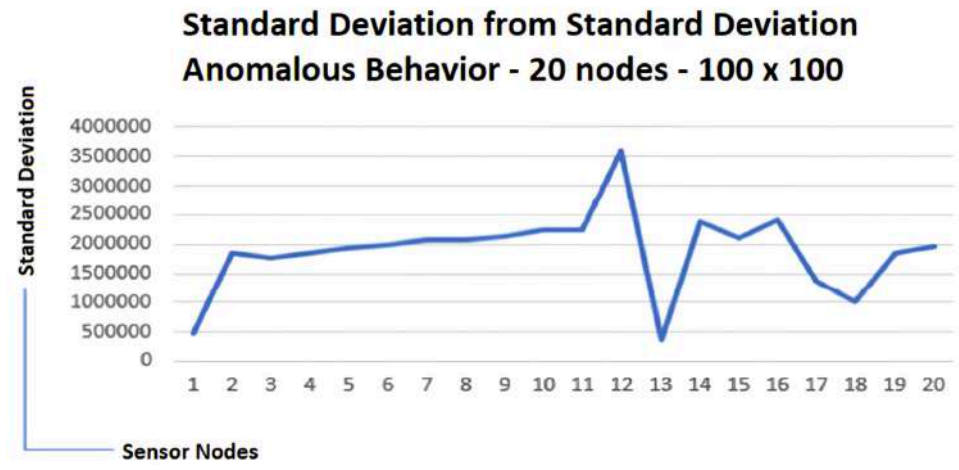
Seeking to generate graphs that can quantify and qualify all these analyses, **Figures 29** and **30** deal with the calculation of the total standard deviation for the set of standard deviations calculated per group of n rounds (n=number of nodes) for all sensor nodes in the network.

Figure 29 – Standard deviation of standard deviation scenario A



Source: Elaborated by the author

Figure 30 - Standard deviation of standard deviation scenario B

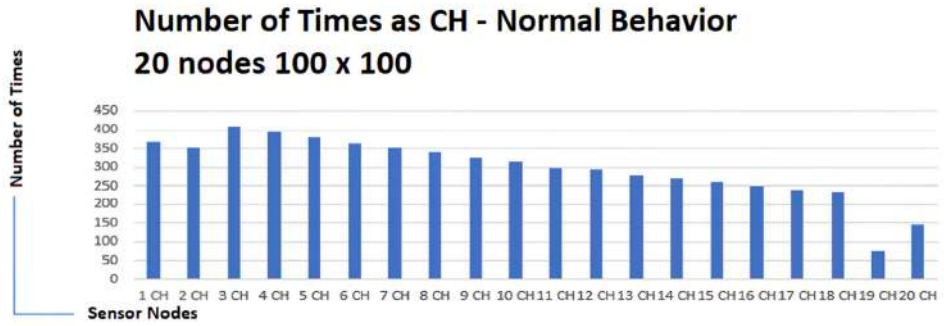


Source: Elaborated by the author

In the graph of **Figure 29**, sensor nodes 19 and 20, which were little chosen as cluster head, have a high standard deviation, while the others have a low total standard deviation. In the graph of **Figure 30**, the anomalous sensor nodes (11 and 12) have a higher total standard deviation, while the others have a lower value, but with an increasing trend.

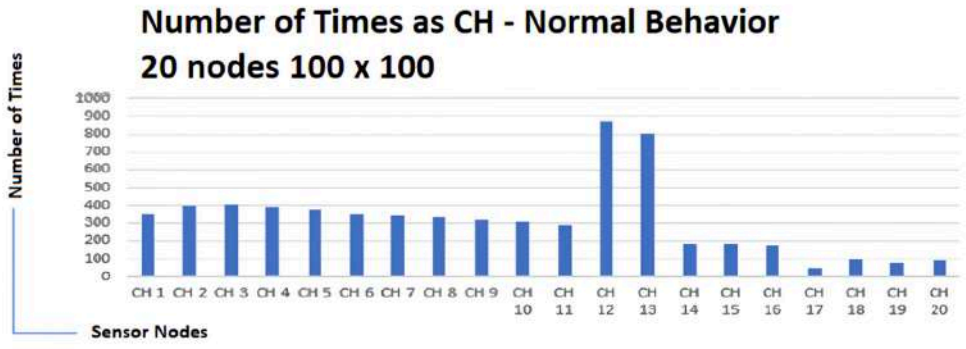
The next analysis presented is the quantification of times that each sensor node is elected cluster head during the lifetime of the network. It is advisable to perform this check to see if the protocol is working to ensure uniform consumption across the entire network. Visually, it is possible to verify that the behavior of the graphs presented in **Figures 31** and **32** is similar to the graphs already presented in **Figures 27** and **28**.

Figure 31 - Number of times as cluster head scenario A



Source: Elaborated by the author

Figure 32 - Number of times as cluster head scenario B



Source: Elaborated by the author

It can be clearly seen in the graph of **Figure 31** how nodes 19 and 20 were the least elected as cluster head, a fact that justifies the individual result of these nodes in **Figures 27** and **29**. In **Figure 32**, it can be seen how the anomalous nodes (11 and 12) were elected as cluster head more often than the other nodes. Thus, differences can be seen between the standard deviation patterns of consumption between normal and anomalous networks, as shown in **Table 6.**

Table 6 - Standard deviation of sensor nodes

Round	SD of Normal Node A	SD of Normal Node B	SD of Anomalous Node A	SD of Anomalous Node B
0	8.273	8.265	8.273	0.000
500	11.338	8.265	0.000	0.000
100	8.273	8.273	0.000	0.000
1000	8.273	8.265	0.000	0.000
1500	8.273	8.265	0.000	0.000
2000	8.273	8.265	0.000	0.000
3000	11.338	8.265	0.000	0.000
3500	8.273	8.265	0.000	0.000
4000	8.273	8.265	0.000	0.000
4500	8.273	8.265	0.000	0.000
5000	8.273	8.265	0.000	0.000

Source: Elaborated by the author

It can be seen in **Table 6** that the standard deviation of the sensor nodes in scenarios without the presence of anomalous nodes, presents a value above zero, with little change during the useful life of the network. In scenarios with anomalous sensor nodes, the default behavior also undergoes few alterations, however, in most rounds it is set to zero, with exceptions between cluster head changes. **Table 7** presents other details about the scenario presented with 20 sensor nodes.

Table 7 – Information about Cluster head x Rounds.

Scenario with 20 nodes 100x100 - Battery Equal					
Anomalous nodes			Normal nodes		
Node ID	12	13	Node ID	8	9
Number of times as CH	873	807	Number of times as CH	340	326
Start of round as CH	2	876	Start of round as CH	8	9
Last round as CH	875	1683	Last round as CH	5936	5940
Number of rounds in the network		6418	Number of rounds in the network		5952

Source: Elaborated by the author

Table 7 shows the number of times a sensor node is elected cluster head, the round in which it is elected the first and last time as cluster head, in addition to the total number of rounds in the network. In the anomalous scenario, the sensor node that is most often elected cluster head, remains as cluster head during almost 13% of the network rounds, while in the normal scenario, this is no more than 9%.

7 Conclusion

The objective of this work was to propose an anomaly identification model, generated by anomalous nodes that send false information about their residual energy to the base station, in addition to considering general characteristics of the network to verify the consumption and performance between experiments of a normal network and a network with anomalous nodes. Comparing the general characteristics between the scenarios proposed in the experiment, it was found that in all cases with anomalous nodes, the network lifetime became 10% longer, on average, when compared to experiments with a normal network. At the beginning of the experiments, a network with anomalous sensor nodes was expected to have a shortened lifespan, but the experiments proved otherwise. The reason is that the consumption concentrated in anomalous nodes contributes to the increase in the network useful life. However, this behavior generates holes in the network coverage, which, in some cases, can make the network more susceptible to packet loss.

As the poisoned nodes die prematurely, the network coverage becomes precarious. Note that analyzing holes in a WSN is an ineffective approach for identifying anomalies, as these holes are typically the result of the actions of anomalous nodes. For example, in industrial sensor networks that need a balance of consumption generated by the rotation of node functions. Furthermore, the concentration generated by the poisoning of nodes goes against the very definition of networks based on the LEACH protocol, which is the alternation of responsibilities between nodes.

In the identification of anomalies, the study of the variability (standard deviation) of the experiments carried out showed that it is possible to identify the standard behavior of the sensor nodes and detect possible anomalous behaviors. Basically, the analyses were based on:

1) The number of packets sent;

2) Energy consumption;

3) The RSSI signal of the nodes;

4) The number of times the nodes were elected as cluster head.

As a metric, we used:

1) The standard deviation of a set of n rounds (n=number of nodes);

2) The mean of the standard deviation calculated every n rounds;

3) The total standard deviation of the set of standard deviations calculated every n runs.

From these elements, it was possible to identify anomalies implemented in the experiments.

The current work contains limitations that can provide opportunities for further research. An example is that the calculations were performed after the experiments. There is a need to perform real-time verification of poisoning. In fact, improvements to the proposed method may allow this quick verification in the base station. It is also necessary to use other statistical models that allow comparisons and rapid diagnosis of node poisoning. The analyses could also be extended to other variants of the LEACH protocol, as well as to **parameters other than energy consumption.** Likewise, it is necessary to test other types of attacks against WSN. Finally, if the scenarios and parameters chosen in the experiments are altered, new analyses may indicate interesting paths for the use and security of the LEACH protocol and its variants.

8 References

ABIDI, W.; EZZEDINE, T. Fuzzy Cluster Head Election algorithm based on LEACH protocol for wireless sensor networks. In: INTERNATIONAL WIRELESS COMMUNICATIONS AND MOBILE COMPUTING CONFERENCE (IWCMC), 13th., 2017. Proceedings... IEEE, 2017. p. 993–997.

ABO-ZAHHAD, M. *et al.* Mobile Sink-Based Adaptive Immune Energy-Efficient Clustering Protocol for Improving the Lifetime and Stability Period of Wireless Sensor Networks. IEEE Sensors Journal, v. 15, n. 8, p. 4576–4586, 2015.

AHMED, A. *et al.* Energy Efficient Sensor Network Routing (EESNR) Protocol For Large Distributed Environmental Monitoring Applications. In: IEEE INTERNATIONAL CONFERENCE ON INTELLIGENT DATA ACQUISITION AND ADVANCED COMPUTING SYSTEMS: TECHNOLOGY AND APPLICATIONS (IDAACS), 9th., 2017, Bucharest. Electronic Proceedings... IEEE, 2017. p. 6.

AKYILDIZ, I. F. *et al.* Wireless sensor networks: A survey. Computer Networks, v. 38, n. 4, p. 393–422, 2002.

ALI, M. S.; DEY, T.; BISWAS, R. ALEACH: Advanced LEACH routing protocol for wireless microsensor networks. In: INTERNATIONAL CONFERENCE ON ELECTRICAL AND COMPUTER ENGINEERING (ICECE), 5th., 2008, Dhaka. Proceedings... IEEE, 2008. p. 909–914.

ALMEIDA, F. C. de. Análise Baseada em Limites Estatísticos para Identificação de Comportamento e Anomalia em Sensores IoT. 2017. Dissertação (Mestrado em Engenharia) - Instituto de Pesquisas Tecnológicas do Estado de São Paulo (IPT), São Paulo, 2018.

ALMOMANI, I.; Al-KASASBEH, B.; Al-AKHRAS, M. WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks. Journal of Sensors, v. 2016, p. 1–16, 2016.

BHARANY, S. *et al.* Energy-efficient clustering scheme for flying ad-hoc networks using an optimized LEACH protocol. Energies, v. 14, n. 19, p. 6016, 2021.

BHOLA, J.; SONI, S.; CHEEMA, G. K. Genetic algorithm based optimized leach protocol for energy efficient wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, v. 11, n. 3, p. 1281–1288, 2020.

BUYANJARGAL, O.; KWON, Y. An energy efficient clustering algorithm for Event-Driven Wireless Sensor Networks (EECED). In: INTERNATIONAL JOINT CONFERENCE ON INC, IMS, AND IDC (NCM), 5th., 2009. Proceedings... IEEE, 2009. p. 1758–1763.

EL-SAADAWY, M.; SHAABAN, E. Enhancing S-LEACH security for wireless sensor networks. In: IEEE INTERNATIONAL CONFERENCE ON ELECTRO INFORMATION TECHNOLOGY (EIT), 2012, Indianapolis. Proceedings... IEEE, 2012. p. 1–6.

FERRAZ JUNIOR, N. *et al.* IoT6Sec: reliability model for Internet of Things security focused on anomalous measurements identification with energy analysis. Wireless Networks, v. 25, n. 4, p. 1533–1556, 2019.

HANDY, M. J.; HAASE, M.; TIMMERMANN, D. Low energy adaptive clustering hierarchy with deterministic cluster-head selection. In: IEEE INTERNATIONAL WORKSHOP ON MOBILE AND WIRELESS COMMUNICATIONS NETWORK (MWCN), 4th., 2002. Proceedings... IEEE, 2002. p. 368–372.

HEAWOOD, P. J. Map-colour theorem. Proceedings of the London Mathematical Society, v. 51, n. 1, p. 161–175, 1949.

HEINZELMAN, W. R.; CHANDRAKASAN, A.; BALAKRISHNAN, H. Energy-efficient communication protocol for wireless sensor networks. Ad-Hoc and Sensor Wireless Networks, v. 30, n. 3-4, p. 301–322, 2000.

IBRL. Intel Berkeley ResearchLab Dataset, 2004. Disponível em: http://db.csail.mit.edu/labdata/labdata.html. Acesso em: 15 jan. 2012.

INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). Internet of Things: Wireless Sensor Networks Market Strategy Board, whitepaper, p. 78, 2014. Disponível em: http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf.

JUNIOR, N. F. *et al.* Lightweight and Secure Publish-Subscribe System for Cloud-Connected Ultra Low Power IoT Devices. Journal of Communication and Information Systems, v. 36, n. 1, p. 100–113, 2021.

MINGOTI, S. A. Análise de dados através de métodos de estatística multivariada: uma abordagem aplicada. 3. reimpr. Belo Horizonte: Editora UFMG, 2016.

MITTAL, M. *et al.* Machine learning techniques for energy efficiency and anomaly detection in hybrid wireless sensor networks. Energies, v. 14, n. 11, p. 3125, 2021.

MITTAL, M. *et al.* An efficient quality of services based wireless sensor network for anomaly detection using soft computing approaches. Journal of Cloud Computing, v. 11, n. 1, p. 1–21, 2022.

MOHAPATRA, H.; RATH, A. K. Fault tolerance in WSN through PE-LEACH protocol. IET Wireless Sensor Systems, v. 9, n. 6, p. 358–365, 2019.

MORETTIN, P. A.; BUSSAB, W. D. O. Estatística básica. São Paulo: Editora Saraiva, 2017.

NAGARAJAN, M. K.; JANAKIRAMAN, N.; BALASUBRAMANIAN, C. A new routing protocol for WSN using limit-based Jaya sail fish optimization-based multi-objective LEACH protocol: an energy-efficient clustering strategy. Wireless Networks, v. 28, n. 5, p. 2131–2153, 2022.

NARAYANAN, R. P.; SARATH, T. V.; VINEETH, V. V. Survey on nodes used in wireless sensor networks. International Journal of Pharmacy and Technology, v. 8, n. 4, p. 21272–21278, 2016.

OLIVEIRA, F. D. M. de. FTE-LEACH: um protocolo energeticamente eficiente e tolerante a falhas aplicado às redes industriais de sensores sem fio. 2015. Tese (Doutorado em Engenharia) - Universidade Federal do Rio Grande do Norte (UFRN), Natal, 2015.

RADHIKA, M.; SIVAKUMAR, P. Energy optimized micro genetic algorithm based LEACH protocol for WSN. Wireless Networks, v. 27, n. 1, p. 27–40, 2021.

RAFIQ, A. *et al.* A consistent approach towards clustering in low energy adaptive clustering hierarchy protocol. In: INTERNATIONAL CONFERENCE ON HIGH-CAPACITY OPTICAL NETWORKS AND ENABLING/EMERGING TECHNOLOGIES (HONET-ICT), 12th., 2015, Islamabad. Proceedings... IEEE, 2015. p. 1–5.

RAJASEGARAR, S. *et al.* Analysis of anomalies in IBRL data from a wireless sensor network deployment. In: INTERNATIONAL CONFERENCE ON SENSOR TECHNOLOGIES AND APPLICATIONS (SENSORCOMM), 2007, Valencia. Proceedings... IEEE, 2007. p. 158–163.

RAMESH, S. *et al.* Optimization of Leach Protocol in Wireless Sensor Network Using Machine Learning. Computational Intelligence and Neuroscience, v. 2022, p. 1–11, 2022.

RAMYA, R. *et al.* Energy efficient enhanced LEACH protocol for IoT based applications in wireless sensor networks. In: INTERNATIONAL CONFERENCE ON INVENTIVE COMPUTATION TECHNOLOGIES (ICICT), 2022, Lalitpur. Proceedings... IEEE, 2022. p. 953–961.

RASSAM, M. A.; ZAINAL, A.; MAAROF, M. A. Advancements of data anomaly detection research in Wireless Sensor Networks: A survey and open issues. Sensors, v. 13, n. 8, p. 10087–10122, 2013.

RAZAQUE, A. *et al.* H-LEACH: Hybrid-low energy adaptive clustering hierarchy for wireless sensor networks. In: IEEE LONG ISLAND SYSTEMS, APPLICATIONS AND TECHNOLOGY CONFERENCE (LISAT), 2016, Farmingdale. Proceedings... IEEE, 2016. p. 1–4.

SANTOS, C. I. L. dos. Dependabilidade Aplicada A Protocolo Hierárquico Baseado No Leach. 2017. Dissertação (Mestrado em Ciência da Computação) - UERN/UFERSA, Mossoró, 2017.

SARKAR, T. K.; PALMA, M. S.; ABDALLAH, M. N. The Physics and Mathematics of Electromagnetic Wave Propagation in Cellular Wireless Communication. Wiley-IEEE Press, 2018.

SHARMA, M.; SHARMA, K. An energy efficient extended LEACH (EEE LEACH). In: INTERNATIONAL CONFERENCE ON COMMUNICATION SYSTEMS AND NETWORK TECHNOLOGIES (CSNT), 2012, Rajkot. Proceedings... IEEE, 2012. p. 377–382.

SILVA, A. A. A. *et al.* Grouping detection and forecasting security controls using unrestricted cooperative bargains. Computer Communications, v. 146, p. 155–173, 2019.

SINGH, T. S.; SORAM, R.; KHAN, A. K. Distance Based Multi Single Hop Low Energy Adaptive Clustering Hierarchy (MS LEACH) Routing Protocol in Wireless Sensor Network. In: IEEE INTERNATIONAL ADVANCED COMPUTING CONFERENCE (IACC), 6th., 2016, Bhimavaram. Proceedings... IEEE, 2016. p. 613–617.

SONGMA, S. *et al.* Classification via k-means clustering and distance-based outlier detection. In: INTERNATIONAL CONFERENCE ON ICT AND KNOWLEDGE ENGINEERING, 2012, Bangkok. Proceedings... IEEE, 2012. p. 125–128.

SOUZA, J. E. D. C. de. Técnicas de Eficiência Energética aplicadas ao Protocolo FTE-LEACH em NS-3. 2017. Dissertação (Mestrado em Ciência da Computação) - UERN/UFERSA, Mossoró, 2017.

SUTHAHARAN, S. *et al.* Labelled data collection for anomaly detection in wireless sensor networks. In: INTERNATIONAL CONFERENCE ON INTELLIGENT SENSORS, SENSOR NETWORKS AND INFORMATION PROCESSING (ISSNIP), 6th., 2010, Brisbane. Proceedings... IEEE, 2010. p. 269–274.

TRIPATHI, M. *et al.* Energy efficient LEACH-C protocol for wireless sensor network. In: INTERNATIONAL CONFERENCE ON COMPUTATIONAL INTELLIGENCE AND INFORMATION TECHNOLOGY (CIIT), 3rd., 2013, Mumbai. Electronic Proceedings... v. 12, n. 13, p. 234–241, 2013.

WARNEKE, B. *et al.* Smart dust: communicating with a cubic-millimeter computer. Computer, v. 34, n. 1, p. 44–51, 2001.

XIE, M.; HU, J.; GUO, S. Segment-based anomaly detection with approximated sample covariance matrix in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, v. 26, n. 2, p. 574–583, 2015.

YICK, J.; MUKHERJEE, B.; GHOSAL, D. Wireless sensor network survey. Computer Networks, v. 52, n. 12, p. 2292–2330, 2008.

ZHANG, Y.; MERATNIA, N.; HAVINGA, P. Outlier detection techniques for wireless sensor networks: A survey. IEEE Communications Surveys and Tutorials, v. 12, n. 2, p. 159–170, 2010.

xxxxxxxxxxx