Data and Metadata. 2025; 4:836
doi: 10.56294/dm2025836

ORIGINAL

Methodology for Vulnerability Assessment in WSNs Using CVSS and NIST SP 800-30

Metodología para Evaluación de Vulnerabilidades en WSNs Usando CVSS y NIST SP 800-30

Fabián Cuzme-Rodríguez[1], Kevin Oñate-Pozo[1], Henry Farinango-Endara[1], Luis Suárez-Zambrano[1], Edgar Jaramillo-Vinueza[1], Jorge Benalcázar-Gómez[1]

[1]Universidad Técnica del Norte, Carrera de Telecomunicaciones. Ibarra, Ecuador.

Cite as: Cuzme-Rodríguez F, Oñate-Pozo K, Farinango-Endara H, Suárez-Zambrano L, Jaramillo-Vinueza E, Benalcázar-Gómez J. Methodology for Vulnerability Assessment in WSNs Using CVSS and NIST SP 800-30. Data and Metadata. 2025; 4:836. https://doi.org/10.56294/dm2025836

Submitted: 13-07-2025 **Revised:** 10-09-2025 **Accepted:** 03-12-2025 **Published:** 04-12-2025

Editor: Dr. Adrián Alejandro Vitón Castillo

Corresponding Author: Fabián Cuzme-Rodríguez

ABSTRACT

Wireless Sensor Networks (WSNs) play a vital role in applications where protecting data is critical. This study presents a six-step methodology for performing intrusive security audits on IEEE 802.15.4-based WSNs, focusing on identifying and evaluating vulnerabilities that compromise confidentiality, integrity, and availability. The approach combines the Offensive Security framework, the NIST SP 800-30 risk assessment guidelines, and the CVSS scoring system to quantify vulnerabilities. Two experimental setups were used: one with temperature sensors, and another with both temperature and CO_2 sensors. Attacks including sniffing, spoofing, data tampering, and denial-of-service were executed using ZBOSS Sniffer, Wireshark, and a Zigbee CC emulator. Key vulnerabilities involved network tracking, unauthorized data interception, and manipulation of traffic flows. Results showed that sniffing was the most effective technique, achieving the highest CVSS scores, particularly in the dual-sensor scenario. The methodology proved effective in uncovering security weaknesses and highlights the need for tailored mitigation strategies (e.g., stronger commissioning, authenticated encryption, and anomaly detection) to improve WSN resilience.

Keywords: Wireless Sensor Networks; Vulnerability Assessment; Penetration Testing; Risk Assessment; Cybersecurity.

RESUMEN

Las redes de sensores inalámbricos (WSN) desempeñan un papel vital en aplicaciones donde la protección de los datos es crítica. Este estudio presenta una metodología de seis pasos para realizar auditorías de seguridad intrusivas en WSN basadas en IEEE 802.15.4, con énfasis en identificar y evaluar vulnerabilidades que comprometen la confidencialidad, integridad y disponibilidad. El enfoque combina el marco de Offensive Security, las directrices de evaluación de riesgos NIST SP 800-30 y el sistema de puntuación CVSS para cuantificar vulnerabilidades. Se evaluaron dos configuraciones experimentales: una con sensores de temperatura y otra con sensores de temperatura y CO_2. Se ejecutaron ataques de sniffing, suplantación, manipulación de datos y denegación de servicio utilizando herramientas como ZBOSS Sniffer, Wireshark y un emulador Zigbee CC. Las vulnerabilidades clave identificadas incluyeron el rastreo de red, la intercepción no autorizada de datos y la manipulación de flujos de tráfico. Los resultados mostraron que el sniffing fue la técnica más efectiva, alcanzando las puntuaciones CVSS más altas especialmente en el escenario con doble sensor. La metodología propuesta demostró ser eficaz para descubrir debilidades de seguridad y subraya la necesidad de estrategias de mitigación específicas (p. ej., commissioning reforzado, cifrado autenticado y detección de anomalías) para mejorar la resiliencia de las WSN.

Palabras clave: Redes de Sensores Inalámbricos; Evaluación de Vulnerabilidades; Pruebas de Penetración; Evaluación de Riesgos; Ciberseguridad.

INTRODUCTION

Wireless sensor networks (WSNs) are widely applied in various fields such as industrial automation, video surveillance, traffic monitoring, and smart homes. These sensors must incorporate robust mechanisms to detect and counteract attacks that could compromise their functionality and security. By identifying these attacks, effective strategies can be implemented to protect confidential information and prevent unauthorized access.

Before starting the first phase of the methodology, it is essential to carefully plan how it will be applied and consider the following critical aspects:

- Acquisition and Installation of Equipment: evaluate the technical specifications of sensors suited to the users' or clients' needs before purchase and installation.
- Sensor Protection: perform a detailed security analysis to identify possible attack vectors and establish appropriate defense mechanisms.
- Sensor Maintenance: develop a maintenance program that includes preventive and corrective actions to ensure the optimal performance of the sensors.
- Access Control to Sensors: periodically verify that the sensors are functioning properly and that there are no interferences or alterations in their operation.
- Sensor Relocation: replace or relocate equipment that is not functioning adequately after maintenance to ensure operational continuity.
- Network Access and Control: ensure the integrity and security of network access, including strict control over access to network servers.

Security in Wireless Sensor Networks

Security in WSNs is particularly challenging due to their distributed and often unattended nature. As multiple attack vectors can occur simultaneously, it is critical to protect the integrity of transmitted information and ensure system continuity.[1,2]

In this context, it is increasingly vital to consider information security as an essential objective and function in any system that handles data. A system is considered secure if it meets the following essential requirements:[3,4,5]

- Confidentiality: ensure that the data in the network is handled in a way that preserves its confidentiality, protecting it from unauthorized third-party access.
- Integrity: guarantee that the information remains complete and unaltered during processing.
- Data Updating: maintain the information constantly updated and relevant for the network users.
- Availability: ensure that the information is accessible at all times to users who need it.
- Self-management: implement protocols that allow the network to self-organize efficiently, minimizing energy consumption, which is critical in sensor networks.
- Synchronization: coordinate the nodes to establish synchronized energy-saving mechanisms, avoiding resource waste.
- Secure Location: it is essential to secure and monitor the location of the nodes to prevent and respond to failures.
- Authentication: verify the authenticity of the data to detect any manipulation.
- Non-repudiation: ensure the verification of identities during data transmission to prevent repudiation by the involved parties.
- Authorization: control system access through permissions that define which resources may be accessed by users.

As highlighted by Batista[4], traditional security techniques are often unsuitable for WSNs. Therefore, the selection of appropriate security mechanisms must consider the specific constraints and characteristics of each deployment. It is imperative that adequate security is incorporated from the network design phase. This holistic view of security at both the physical and logical levels has been emphasized in recent literature, particularly in the context of smart objects, which share vulnerabilities with WSNs.[6]

Security in IEEE 802.15.4 Networks

IEEE 802.15.4 is one of the most commonly used standards in WSNs, particularly due to its support for low-power and low-data-rate communication. However, its focus on energy efficiency introduces trade-offs in terms of security. Devices under this standard typically operate with limited processing capabilities, memory, and battery life, which complicates the implementation of advanced cryptographic protocols.

The security services specified in this standard include:[7,8]

- Data confidentiality: ensures that transmitted information is inaccessible to unauthorized third parties.
- Data authenticity: verifies the identity of senders and receivers to guarantee that the data originates from legitimate sources and is received by the correct recipients.
- Replay protection: prevents the duplication of transmitted information.

These mechanisms must be explicitly requested by higher layers in the protocol stack, which requires coordination and security awareness across the system architecture.

Vulnerabilities in IEEE 802.15.4-based WSNs have been widely documented; however, we identify an operational-methodological gap: the lack of reproducible auditing flows that integrate, step by step, offensive reconnaissance, tool-guided intrusive testing, and risk decision-making simultaneously aligned with NIST SP 800-30 and CVSS. Our contribution is a six-phase process, with decision points and configurable artifacts (traces, filters, CVSS templates) that can be replicated in academic laboratories, facilitating its transfer to field applications with minimal adjustments.

Unlike WSN audits focused on algorithmic/IDS classification, our focus is operational: a blueprint audit methodology with NIST/CVSS traceability and capture/attack guidelines for 802.15.4. Compared with updated control frameworks such as NIST SP 800-53 Rev.5 and recent mesh protocols as Thread or BLE Mesh, we outline how our pipeline can adapt without redesign: instruments and preconditions for evidence collection change, but the phases and evaluation logic remain intact.[9,10,11,12,13]

Structure of the Paper: Section 2 presents the proposed methodology; Section 3 covers the technical development and implementation phases; Section 4 discusses and interprets the results; and Section 5 offers conclusions.

METHOD

Security Auditing in Wireless Sensor Networks

Conducting security audits in Wireless Sensor Networks (WSNs) presents unique challenges, largely due to their heterogeneous architectures and operating constraints. These networks vary widely in terms of topology, hardware capabilities, energy budgets, and communication protocols. As such, evaluations must be tailored to the specific deployment context.

While audits in WSNs differ from those in conventional IT systems, the core principles remain aligned. The foundations of audit processes, such as defining scope, objectives, and procedures, are shared across domains. Nevertheless, auditing WSNs demands particular attention to physical vulnerabilities, communication layers, and energy-aware operation.[14,15]

In addition, a wide range of technical audit and risk analysis methodologies can be adapted to WSN environments. Among the most relevant are:

- Technical auditing frameworks: OSSTM, OWASP, ISSAF, and Offensive Security.
- Risk analysis models: OCTAVE, MEHARI, CRAMM, EBIOS, NIST SP 800-30, MAGERIT, and ISO/IEC 27005.

These methodologies provide well-defined structures for identifying vulnerabilities, evaluating threats, and prioritizing mitigation strategies in digital infrastructures.[16]

Threat Model & Assumptions

We consider a laboratory-grade IEEE 802.15.4 deployment with constrained motes (limited CPU, RAM, and battery), a single coordinator, and several end devices. The adversary is an external entity with proximity radio access and commodity tooling (e.g., ZBOSS Sniffer, Wireshark, XCTU). Capabilities include passive eavesdropping, traffic analysis, frame injection, and flooding; physical tampering and side-channel attacks are out of scope. We evaluate two security baselines: (i) minimal-security commissioning (unencrypted frames), and (ii) authenticated encryption enabled at MAC level (AES-CCM*) with replay protection. Success criteria are defined per attack vector (e.g., time-to-compromise, ability to infer PAN ID, data tampering visibility, DoS effectiveness). All experiments follow ethical and legal constraints, with isolated testbeds and no third-party traffic interception.

Applicability to Encrypted Networks

When authenticated encryption and replay protection are enabled, the attack surface changes. Passive sniffing no longer reveals payloads, shifting emphasis to: (i) metadata-centric analysis (traffic patterns, timing, link-layer headers); (ii) commissioning weaknesses and key management (e.g., insecure defaults, key reuse);

(iii) active desynchronization and jamming to induce re-joins; and (iv) endpoint compromise to extract keys. Our six-step procedure adapts accordingly: Phase 1 collects commissioning/configuration evidence; Phase 2 identifies crypto policy misconfigurations and key lifecycle risks; Phase 3 targets controlled tests on join/re-join; Phase 4 executes metadata-based correlation, controlled jamming/desync, and negative testing; Phase 5 quantifies impact with availability and delay/jitter metrics besides CVSS severity. Side-channel and physical attacks are acknowledged but left as future work due to ethical and laboratory constraints.

Proposed Methodology

This study proposes a security audit methodology specifically designed for WSNs, integrating offensive security principles with selected elements from OWASP and NIST SP 800-30, which follows a structured approach widely adopted in ethical hacking practices, particularly in web environments where adversarial modeling is essential.[17] The approach emphasizes hands-on, intrusive evaluation while maintaining alignment with recognized risk management frameworks. The process is conducted by a designated audit team, where roles and responsibilities are clearly defined for each phase.

The methodology is structured into six sequential phases:

1. Information gathering.
2. Vulnerability analysis.
3. Definition of secondary objectives.
4. Execution of attacks.
5. Analysis of results.
6. Final analysis and documentation.

This structured approach allows for a comprehensive, replicable, and technically grounded evaluation of WSN security posture. It addresses both the specific limitations of embedded devices and the broader organizational implications of network vulnerabilities.

Mapping of metrics to attack techniques

To clarify how each security test is quantitatively evaluated, table 1 links the main attack techniques with their security objectives, the primary and secondary metrics defined in the statistical plan, and the tools or artefacts used to collect the evidence. This mapping serves as a practical guide for replicating the audit and ensures that the proposed methodology can be reproduced in future deployments.

Table 1. Mapping between attack techniques, objectives, metrics, and tools

Attack	Objective (CIA)	Primary Metrics	Secondary Metrics	Tools / Artifacts
Sniffing (unencrypted)	Confidentiality (PAN ID, topology inference)	TTC (PAN-ID), #headers decoded	PDR impact (if passive), traffic periodicity	ZBOSS/Wireshark; .pcap, header logs
Sniffing (encrypted)	Metadata inference	Traffic periodicity, burstiness	Latency/Jitter under load	ZBOSS/Wireshark; timing traces
Identity Spoofing	Integrity (false data accepted)	TTC (first accepted fake), error rate at sink	PDR change, alarm triggers	XCTU, injector script; sink logs
Data Tampering	Integrity (payload alteration)	#altered samples detected	Latency to detection	Injector script; app logs
DoS / Flooding	Availability (service disruption)	PDR drop, outage duration	Latency inflation, energy proxy	XCTU, flood script; duty-cycle logs
Desync / Re-join	Availability/Integrity (state reset)	Re-join count, TTC to instability	PDR oscillation, jitter	Jammer/desync script; re-join logs

Measurement Variables and Statistical Plan

Although the original testbed is no longer available for quantitative validation, the following metrics are defined to guide future replications:

- Packet Delivery Ratio (PDR): $PDR=N_{rx}/N_{tx}$
- End-to-End Latency: $L\_{}_i=t_i^{rx}-t_i^{tx}$, reported as mean ±SD.
- Jitter: $J=1/(N^{rx}-1)\ \sum_{i=2}^{Nrx}|L_i-L_{i-1}|$
- Time-to-Compromise (TTC): elapsed time from attack start to first successful breach.
- Energy consumption: $E\approx V(I_{tx}\ T_{tx}+I_{rx}\ T_{rx}+I_{id}\ T_{id})$

Statistical validation for future experiments includes Shapiro–Wilk normality testing and ANOVA or Mann–Whitney tests (95 % confidence).

These definitions ensure that, even without current measurements, the proposed audit framework remains reproducible and ready for quantitative validation.

DEVELOPMENT

Phase 1: Information Gathering

To initiate the audit, it is crucial to compile a comprehensive understanding of the system under evaluation, facilitating an accurate diagnosis. The activities are detailed below:

Current Situation

The process flow of the coordinator node, the sensors, and the network topology is analyzed.

The scenarios are executed over unencrypted 802.15.4 frames to maximize reproducibility and observability of effects (tracking, interception, spoofing, DoS). This decision does not invalidate the process in encrypted environments; it simply requires instrumentation adjustments such as probes and key/provisioning phases and evidence collection criteria, while maintaining the same six phases.

This stage includes the planning of attacks aimed at compromising the system's confidentiality, integrity, and availability. Two real-world scenarios are established to identify vulnerabilities and define preventive measures:

Scenario 1: Wireless sensor network measuring temperature

The described process begins with configuring the network and ports, followed by data verification and acquisition to display temperature levels. Three types of attacks are considered to assess the network's security, which is primarily used in modern agriculture. According to MeteoSur SRL,[18] this technology is essential for monitoring variables such as weather, temperature, and soil moisture, allowing farmers to mitigate risks such as droughts, fungal infections, and heatwaves, thereby improving the profitability and quality of crops through informed decision-making.[19]

The network is configured to manage and visualize temperature data, and attacks are planned to evaluate the security of the collected information.

Scenario 2: Sensor network measuring temperature and CO_2

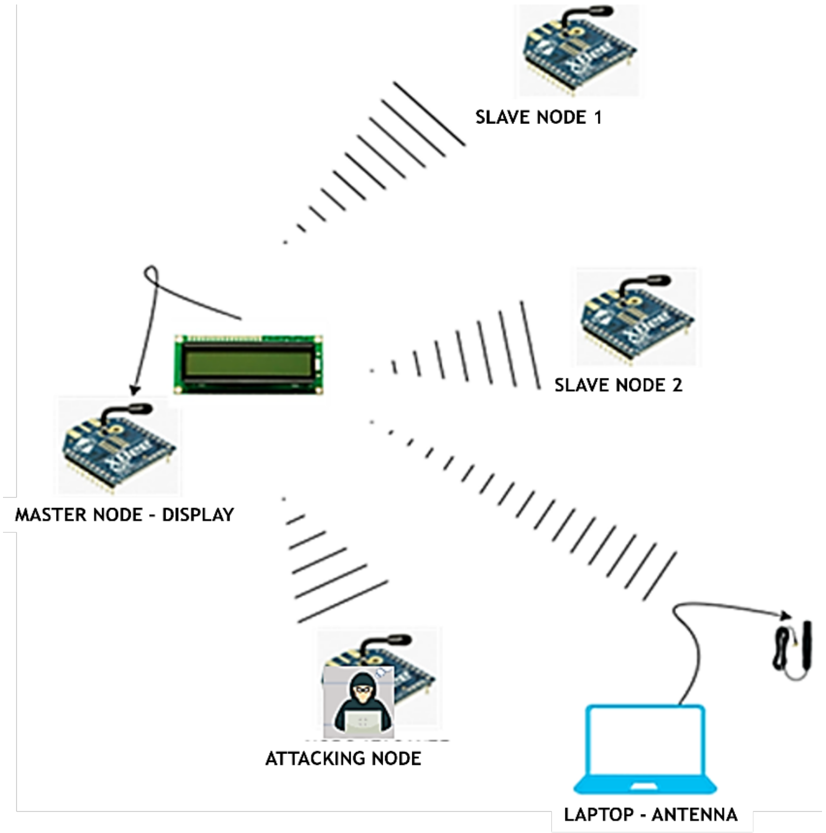


Figure 1. System Element Topology

In the second scenario, the network adds the functionality of CO_2 measurement, applicable in the transportation and automotive industries to monitor air quality and urban temperature. This design supports transportation authorities in making decisions to mitigate pollution.(20,21)

To provide a detailed view of the configuration and components of the wireless sensor network, a diagram of the topology and critical system elements is developed. Figure 1 presents the topology and system components.

The system topology includes:

- A master node with a display to show data received from the slave nodes.
- Two slave nodes that measure temperature and CO_2, transmitting the information to the master node.
- A laptop with an antenna to capture the frames sent by the slave nodes.
- An attacker node responsible for executing attacks on confidentiality, integrity, and availability.

Figure 2 below illustrates the operational flow of the coordinator node and the sensor nodes for both scenarios.

It is also important to emphasize the selection of the evaluator responsible for executing the attack. For coordination, it is necessary to determine the appropriate tools, such as ZBOSS Sniffer, Wireshark, the Zigbee CC emulator, debugger, and USB programmer. The considered attacks may target confidentiality, integrity, and availability. Additionally, the attack plan must outline the activities, durations, required resources, and assigned responsibilities.

Attack Planning

The scope and flow of the attacks, shown in figure 2, are adapted based on the nature of the sensors. The attacks begin with frame capture using ZBOSS and packet analysis with Wireshark, identifying the PAN ID of the coordinator node for the specific execution of attacks, including brute-force if necessary.

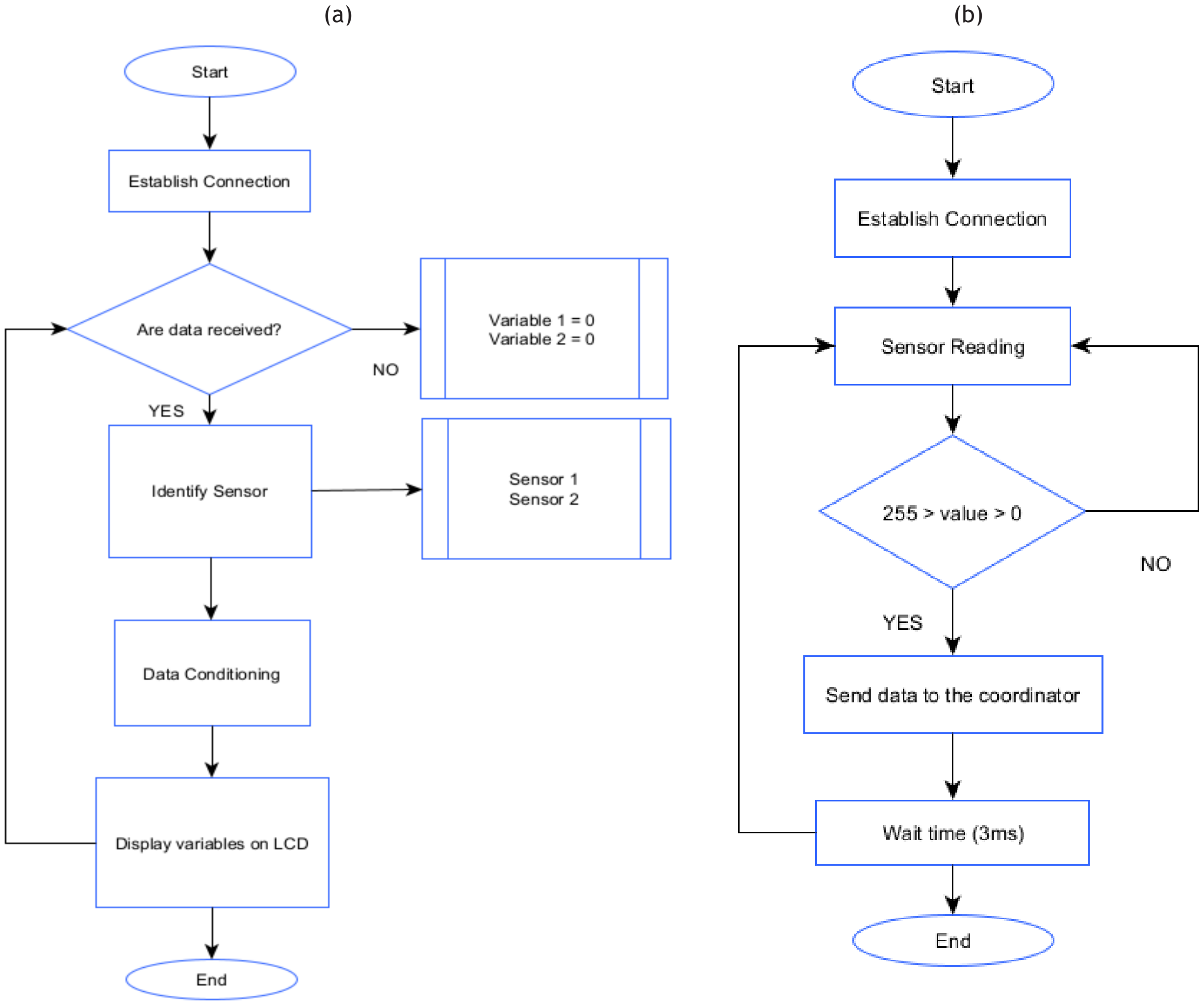


Figure 2. Flowchart Diagram: (a) Coordinator node. (b) Sensor nodes

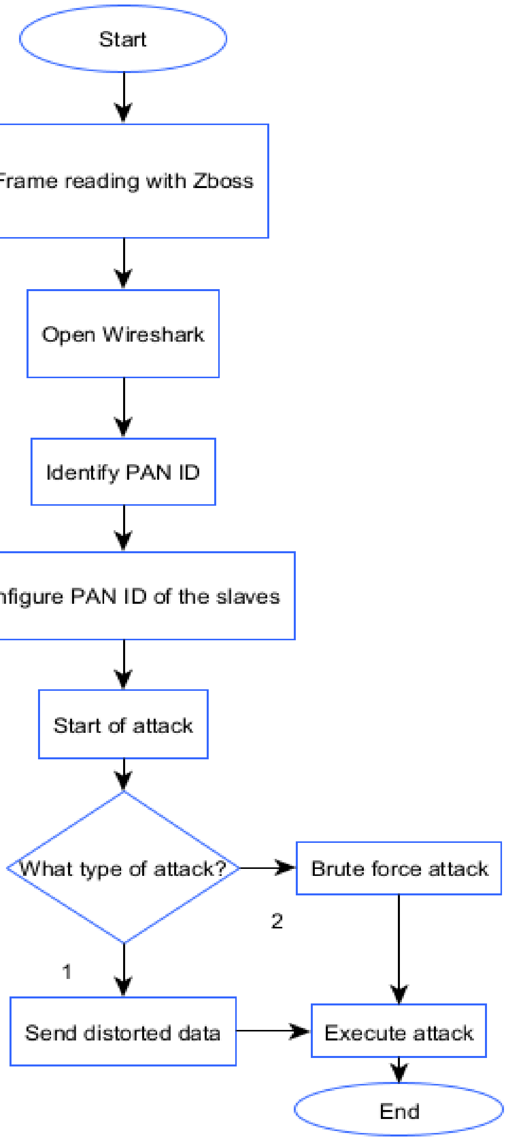


Figure 3. Attack Process Flowchart

The selection of the audit team and tools (ZBOSS Sniffer, Wireshark, Zigbee CC emulator, debugger, USB programmer) is crucial for the effective execution of the planned attacks, including a detailed description of the activities, timelines, required resources, and assigned responsibilities.

Phase 2: Vulnerability Analysis

To proceed with the vulnerability analysis, the criteria established by the NIST SP 800-30 methodology are applied.

Preparation for Risk Assessment

The risk levels associated with each planned attack are identified using the NIST SP 800-30 methodology for an accurate risk evaluation. A risk matrix is defined to assess the probability, impact, and necessary actions.

Conducting the Risk Assessment

Table 2 presents the risk assessment conducted on a wireless sensor network, identifying assets, attacks, vulnerabilities, and associated threat sources. For confidentiality, vulnerabilities such as network tracking, decryption of sensitive information, active traffic capture, and data reading are described, all attributed to hacking activities.

Integrity is compromised through the injection of manipulated data and random modification of displayed data, associated with data tampering. Availability is threatened by denial-of-service (DoS) attacks, also resulting from hacking efforts.

Table 2. Threat Source Matrix

Asset	Attack	Vulnerability	Threat Source
Wireless sensor network	Confidentiality	Network Tracking	Hacking
		Descifra información sensible	Hacking
		Active Traffic Capture	Hacking
		Packet Capture	Hacking
		Data reading	Hacking
	Integrity	Sending Manipulated Data	Data Alteration
		Random modification of displayed data	Data Alteration
	Availability	Denial of service	Hacking

Subsequently, the risk assessment matrix is developed. Table 3 provides a risk assessment matrix that assigns values to the threat probability, impact, and risk rating for each vul nerability, offering a quantitative view of the risk associated with each type of attack, which facilitates the prioritization of mitigation measures.

Table 3. Risk Evaluation Matrix

Asset	Attack	Vulnerability	Threat Probability	Impact	Risk Rating
Wireless Sensor Network	Confidentiality	Network Tracking	1,0	100	100
		Decryption of sensitive information	1,0	100	100
		Active Traffic Capture	1,0	100	100
		Packet Capture	0,5	100	50
		Data reading	0,5	50	25
	Integrity	Sending Manipulated Data	0,5	100	50
		Random modification of displayed data	0,1	50	5
	Availability	Denial of Service	1,0	50	50

Communicating and Sharing Risk Assessment Information

Based on the assessment conducted, it is identified that the threats affecting wireless sensors are related to hacking and data manipulation. The vulnerabilities are primarily associated with network tracking, decryption of sensitive information, data reading, among others. Regarding the risk evaluation, confidentiality attacks exhibit high levels of threat probability, impact, and risk rating, representing 38 % of the total identified vulnerabilities.

Maintaining the Risk Assessment

Once the vulnerabilities are identified, ongoing maintenance is established through appropriate control measures, taking into account the ISO/IEC 27002 (2022) standard. This means that for each mitigation measure defined, corresponding controls are established to ensure compliance.

These controls consider the following areas:

- Physical controls (wireless sensors)
- Information security properties (confidentiality, integrity, etc.)
- People (personnel)
- Technology (network infrastructure)

Table 4. Risk Control Matrix

Tipo de control	Information	Security	Operational Capability	Security Domain	Frequency
Preventive	Physical, information security, personnel and technology	Information review and planning protection measures	Identity management	Regulation and policies	Quarterly
Detective		Maintenance when the problema arises for protection	Access management		Semiannual
Corrective		Resource nauntenace (information			Annual

The controls are described in table 4.

Phase 3: Definition Of Secondary Objectives

Specific and secondary objectives are defined for the project, focusing on the identification of vulnerabilities and the development of attacks following the OWASP methodology. This includes selecting appropriate tools, assigning responsibilities, and planning activities to manage the development of the attacks.

Specific Objectives

- Determine the appropriate tool for carrying out the attack.
- Assign the person responsible for the implementation of the attack.
- Plan activities for managing the attack development process.

Secondary Objectives

The secondary objectives for identifying vulnerabilities in the sensor network are detailed as follows:

- Apply the attacks established during the planning phase.
- Perform a comparative analysis to select the most suitable intrusive technique for identifying vulnerabilities, based on the planned attacks and in accordance with the OWASP methodology.
- Develop the final report detailing the vulnerabilities found and the corresponding attacks, along with their proposed solutions.

This summary provides a detailed and structured description of the initial phases of the WSN security audit, setting the stage for a thorough vulnerability analysis and the implementation of protective measures.

Phase 4: Attacks

The network is initially designed, including its corresponding nodes, which are configured with a similar embedded hardware and software architecture. This setup is illustrated in figure 4, which shows the deployment of the wireless network and the distribution of its various nodes. Once the nodes complete their operations, they enter a sleep mode to minimize energy consumption and extend battery life. All simulated nodes are equipped with a microcontroller, memory, and a transceiver. Both the gateway and sensor nodes operate with a data acquisition frequency of every 30 seconds.

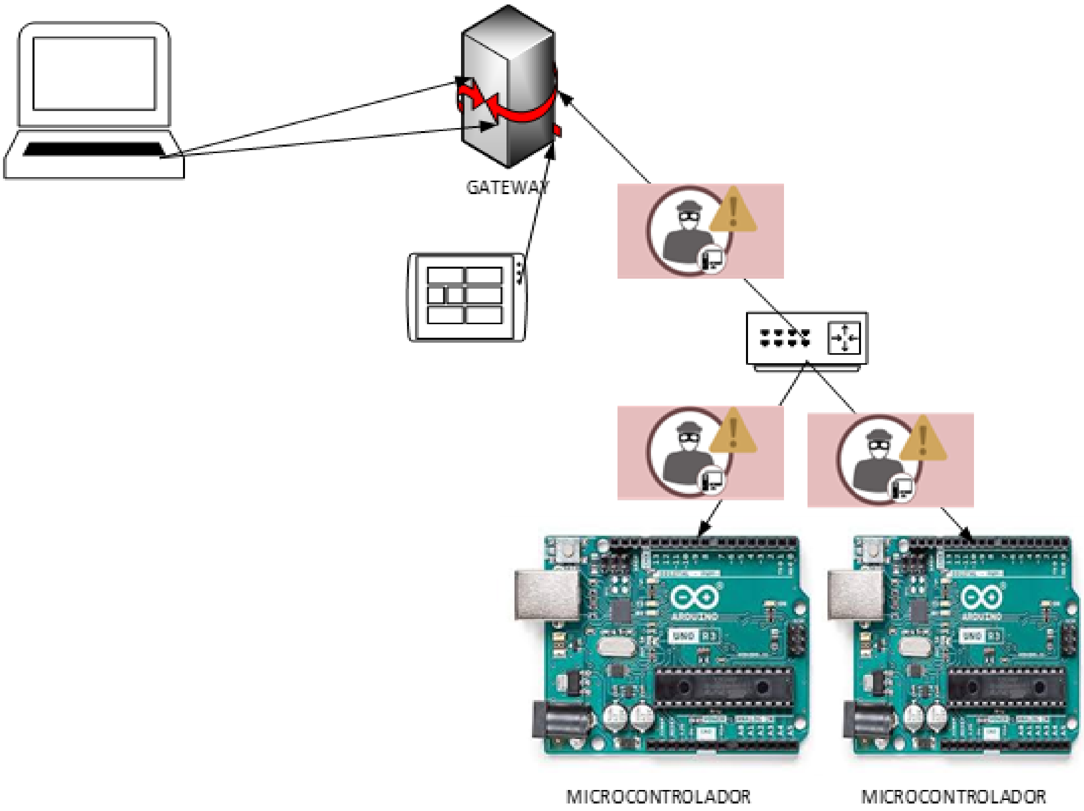


Figure 4. Network topology for evaluation

Once the network is fully configured, we proceed with executing the attacks defined in earlier phases, targeting core aspects of confidentiality, integrity, and availability.

Confidentiality Attack

The confidentiality attack process is illustrated in the following diagram (figure 5):

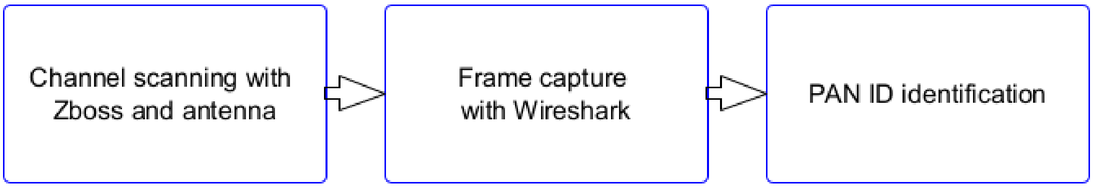
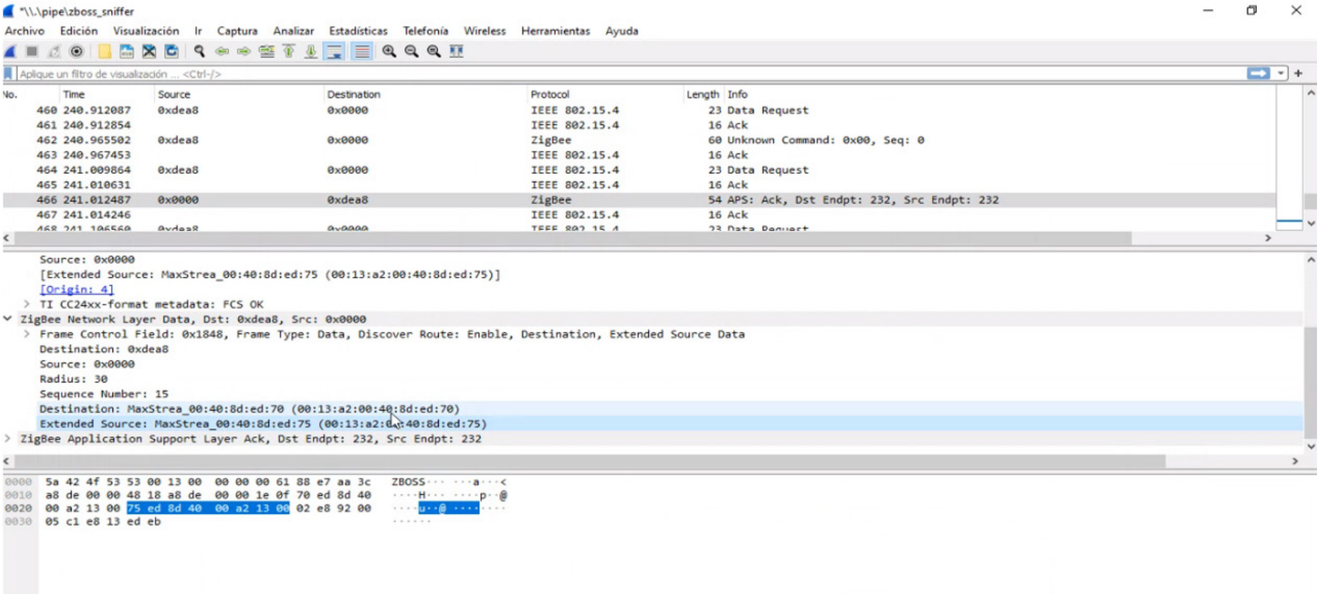

Channel scanning with Zboss and antenna
Frame capture with Wireshark
PAN ID identification

Figure 5. Sequence diagram for confidentiality attack

In other words, the confidentiality attack sequence began with scanning the network layer channels using the ZBOSS tool, which connects to the antenna to obtain the available channels. Once the channels were identified, the Wireshark tool was used to capture the frames. On the computer, Wireshark was launched to visualize the existing networks and interfaces, and the active network was identified. Double-clicking the selected network enabled the capture of inbound and outbound traffic. Finally, the PAN ID of the network was identified, which is essential for carrying out subsequent attacks.

Figure 6 shows the frames from both the coordinator and client nodes. These frames are analyzed for information extraction. If the Zigbee network configuration is not protected by encryption, the data within the frames can be viewed directly. The coordinator's address, transmitted data, PAN ID, and other information useful for further attacks can be identified.


*\\.\pipe\zboss_sniffer
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>

```
No.   Time        Source   Destination  Protocol       Length Info
  460 240.912087  0xdea8   0x0000       IEEE 802.15.4      23 Data Request
  461 240.912854                        IEEE 802.15.4      16 Ack
  462 240.965502  0xdea8   0x0000       ZigBee             60 Unknown Command: 0x00, Seq: 0
  463 240.967453                        IEEE 802.15.4      16 Ack
  464 241.009864  0xdea8   0x0000       IEEE 802.15.4      23 Data Request
  465 241.010631                        IEEE 802.15.4      16 Ack
  466 241.012487  0x0000   0xdea8       ZigBee             54 APS: Ack, Dst Endpt: 232, Src Endpt: 232
  467 241.014246                        IEEE 802.15.4      16 Ack
  468 241.106560  0xdea8   0x0000       IEEE 802.15.4      23 Data Request
```

```
    Source: 0x0000
    [Extended Source: MaxStrea_00:40:8d:ed:75 (00:13:a2:00:40:8d:ed:75)]
    [Origin: 4]
  > TI CC24xx-format metadata: FCS OK
v ZigBee Network Layer Data, Dst: 0xdea8, Src: 0x0000
  > Frame Control Field: 0x1848, Frame Type: Data, Discover Route: Enable, Destination, Extended Source Data
    Destination: 0xdea8
    Source: 0x0000
    Radius: 30
    Sequence Number: 15
    Destination: MaxStrea_00:40:8d:ed:70 (00:13:a2:00:40:8d:ed:70)
    Extended Source: MaxStrea_00:40:8d:ed:75 (00:13:a2:00:40:8d:ed:75)
> ZigBee Application Support Layer Ack, Dst Endpt: 232, Src Endpt: 232
```

```
0000  5a 42 4f 53 53 00 13 00  00 00 00 61 88 e7 aa 3c   ZBOSS··· ···a···<
0010  a8 de 00 00 48 18 a8 de  00 00 1e 0f 70 ed 8d 40   ····H··· ····p··@
0020  00 a2 13 00 75 ed 8d 40  00 a2 13 00 02 e8 92 00   ····u··@ ········
0030  05 c1 e8 13 ed eb                                  ······
```

Figure 6. Frame capture

Integrity Attack

To illustrate the process of an integrity attack on the wireless sensor network, a flow diagram has been developed detailing each step involved in the execution. The complete sequence of events is shown in figure 7.

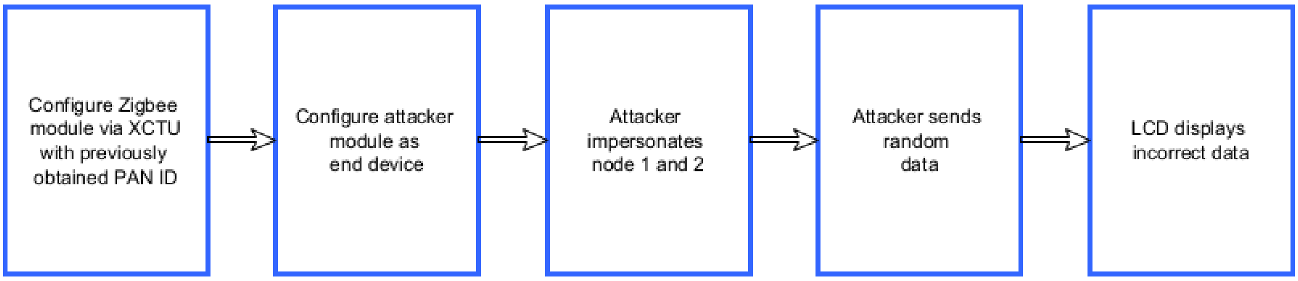

Configure Zigbee module via XCTU with previously obtained PAN ID
Configure attacker module as end device
Attacker impersonates node 1 and 2
Attacker sends random data
LCD displays incorrect data

Figure 7. Sequence diagram for integrity attack

The integrity attack begins with the configuration of the Zigbee module using the XCTU software, where the modules are displayed through a graphical interface. The attacking module is configured as an end device. The attacker then performs identity spoofing for nodes 1 and 2, modifying and randomly sending falsified data based on the PAN ID obtained during the confidentiality attack.

Next, the digital port is read, and the attacker's Arduino generates random data, which is transmitted to the network impersonating nodes 1 and 2 at random intervals. As a result, the LCD screen on the coordinator node displays incorrect information, such as randomly generated temperatures instead of those originating from the legitimate network sensors (figure 8).

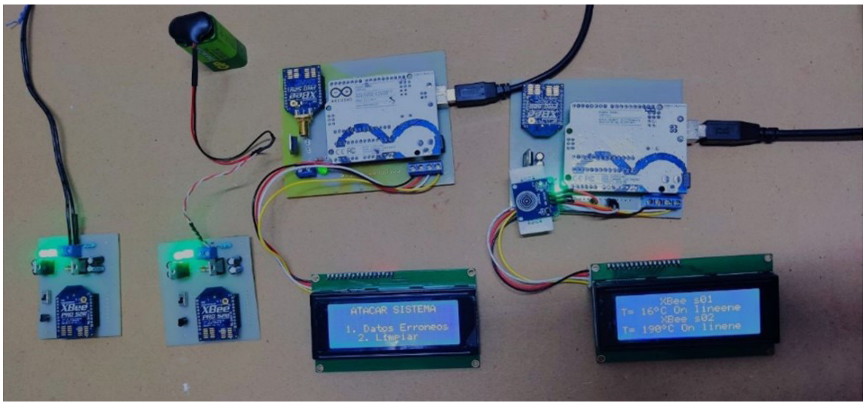


Figure 8. Integrity attack

Availability Attack

The availability attack process is illustrated in the sequence diagram shown in figure 9.

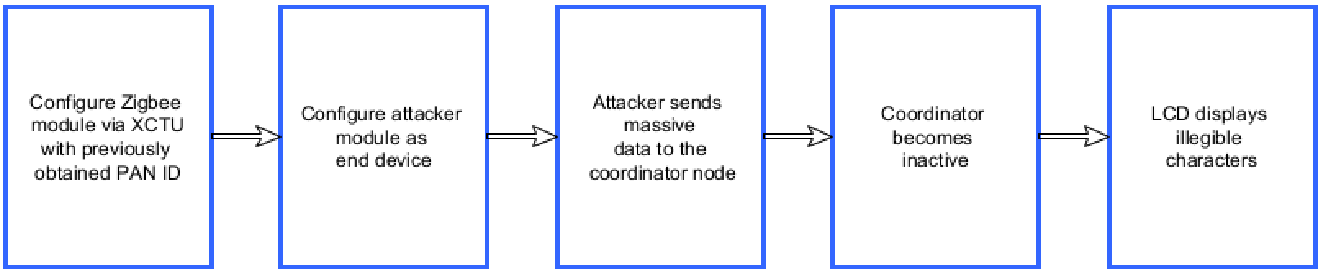

Configure Zigbee module via XCTU with previously obtained PAN ID
Configure attacker module as end device
Attacker sends massive data to the coordinator node
Coordinator becomes inactive
LCD displays illegible characters

Figure 9. Sequence diagram for availability attack

This stage simulates a Denial of Service (DoS) attack, where the network is deliberately saturated with traffic to test its resilience under stress. The Zigbee module is again configured as an end device using XCTU. The attacker floods the coordinator node with massive amounts of data, using the PAN ID obtained in the confidentiality attack. As a result, the coordinator becomes unresponsive. The Arduino attacker randomly sends data to the network, posing as nodes 1 and 2. Finally, the LCD on the coordinator displays illegible characters, strings generated with special characters not supported by the display (figure 10).

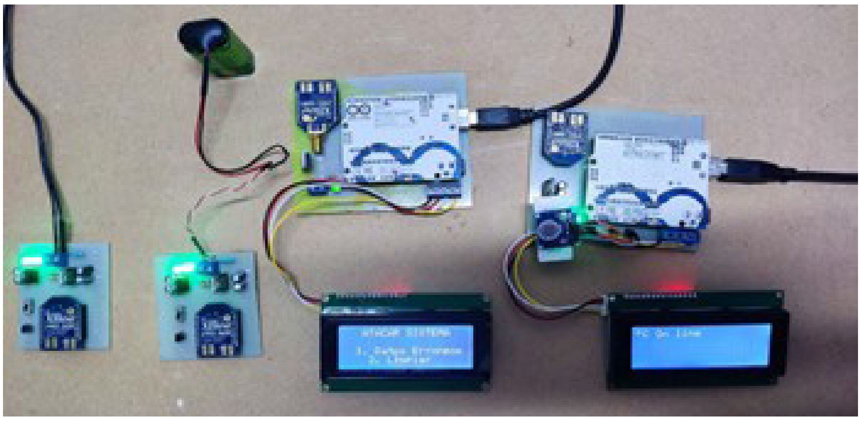


Figure 10. Availability attack: coordinator LCD corruption under DoS flooding

Phase 5: Results Analysis

In the fifth phase, the analysis of the results is presented, including the findings of the vulnerabilities identified in each scenario, the selection of the comparative method, the metrics used, and other relevant factors.

Presentation of Findings

The vulnerabilities identified in each scenario are listed below:

Table 5. Presentation of findings (vulnerability)

Scenario	Finding
Scenario 1: Wireless sensor network measuring temperature	Temperature data reading Transmission of manipulated data, resulting in erroneous temperature levels, this affects crop quality due to improper irrigation Denial of service, as no temperature data is displaye Traffic capture, which prevents identification of temperature load peaks at regular intervals Unusual packet capture in the network
Scenario 2: Sensor network measuring temperature and CO_2	Network tracking Decryption of sensitive temperature and CO_2 data intended only for authorized entities Active traffic capture Packet capture Unauthorized reading of temperature data in the traffic and CO_2 levels in internal combustion Manipulated transmission of CO_2 data Random modification of displayed temperature data Denial of service, temperature and CO_2 data become unavailable

From table 5, it is evident that a greater number of vulnerabilities were found in Scenario 2. The use of specialized technological tools made it possible to identify more than three distinct vulnerabilities, unlike in Scenario 1. As a result, targeted protection mechanisms can be implemented accordingly.

Determination of Comparative Method

The Common Vulnerability Scoring System (CVSS) was used as the comparative method to facilitate the evaluation of the intrusive testing results. This approach enabled the identification of key characteristics and the assignment of scores to the selected metrics. In the end, each intrusive test was scored based on these metrics, and the test with the highest rating was selected according to the predefined scale (table 6).

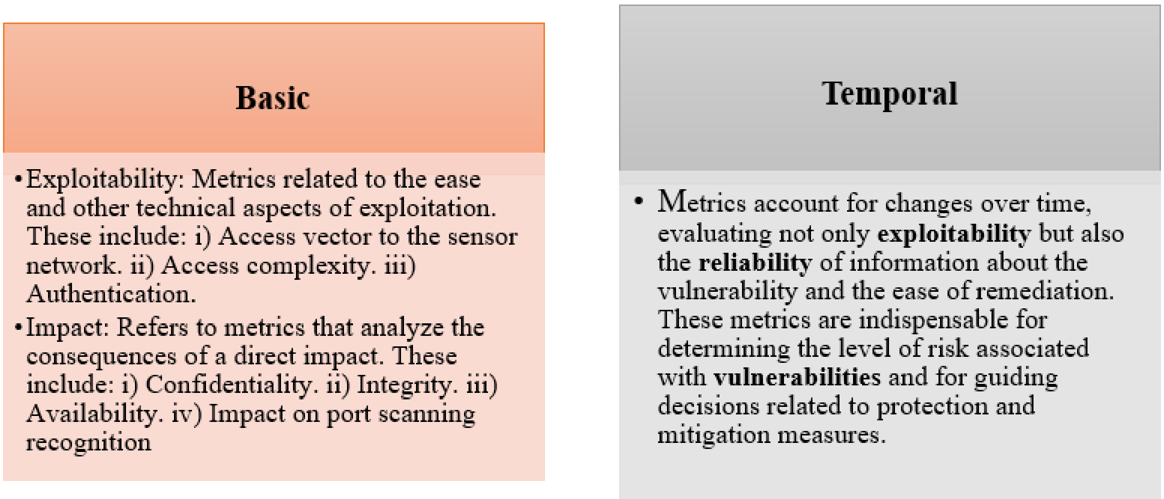
Table 6. CVSS rating scale

Rating	Scale
0	Null
1 – 3,9	Low
4 – 6,9	Medium
7 – 8,9	High
9 - 10	Very High

Metric Determination

Metrics can be classified as basic or temporal. Basic metrics refer to characteristics that remain constant within the user environment. Temporal metrics are variable and reflect vulnerabilities that evolve over time.

The chart in figure 11 outlines a fundamental classification of security metrics into two key categories: Basic and Temporal. These are essential for the comprehensive evaluation of vulnerabilities in information systems. Basic metrics assess the ease of exploiting a vulnerability and the potential impact of that exploitation on the system's confidentiality, integrity, and availability. Factors considered include the access vector, access complexity, and the need for authentication. On the other hand, temporal metrics account for changes over time, evaluating not only exploitability but also the reliability of information about the vulnerability and the ease of remediation. These metrics are indispensable for determining the level of risk associated with vulnerabilities and for guiding decisions related to protection and mitigation measures.



Basic

- Exploitability: Metrics related to the ease and other technical aspects of exploitation. These include: i) Access vector to the sensor network. ii) Access complexity. iii) Authentication.
- Impact: Refers to metrics that analyze the consequences of a direct impact. These include: i) Confidentiality. ii) Integrity. iii) Availability. iv) Impact on port scanning recognition

Temporal

- Metrics account for changes over time, evaluating not only **exploitability** but also the **reliability** of information about the vulnerability and the ease of remediation. These metrics are indispensable for determining the level of risk associated with **vulnerabilities** and for guiding decisions related to protection and mitigation measures.

Figure 11. Metric Determination

Intrusive Test Comparison

The cybersecurity tests described assess system vulnerabilities against various types of attacks. Sniffing captures traffic to analyze network weaknesses. Phishing deceives users to extract confidential data, highlighting the importance of security awareness. Data modification tests a system's ability to detect changes in information. Denial of Service (DoS) evaluates the robustness of the system under extreme request loads. These tests are essential for organizations to identify their weak points and enhance their security posture.

When link-layer encryption is enabled, sniffing focuses on metadata (headers, timing, channel utilization). Although payloads are concealed, traffic analysis still reveals periodicity, burst patterns, and re-join events relevant to attack planning and anomaly detection.

Table 7. Comparison of intrusive tests

Test	Advantages	Disadvantages
Sniffing	Ability to monitor traffic Does not require sophisticated knowledge to apply Enables verification of user behavior Helps identify weaknesses and strengths in analyzed equipment Allows security configuration changes Captures usernames and passwords Identifies most frequently used services Detects inappropriate resource usage	Requires prior knowledge
Identity Spoofing	Does not require sophisticated knowledge to apply Helps identify spam messages, emails, or confidential information Enables filtering of safe messages	Does not reveal technical vulnerabilities
Data Modification	Low cost for implementation Provides simple and practical information about vulnerabilities Enables detection of altered information and corrective measures	May create bottlenecks
Denial of Service (DoS)	Easy to implement technique Allows assessment of network traffic capacity Helps detect packet alterations Can send code with special characters	Requires prior technical knowledge

These results shown in table 7 underscore the importance of selecting the appropriate technique based on the specific context of the network and the capabilities of the security team, in order to maximize test effectiveness and minimize potential disadvantages.

Comparative Analysis

A comparative evaluation was also performed on the mechanisms used to conduct the attacks on the wireless sensor network. Four intrusive techniques were considered, and the base metrics from the CVSS (Common

Vulnerability Scoring System) model were adapted accordingly. Ultimately, the technique with the highest score was selected. The results are detailed in table 8 below:

Table 8. Attack comparison

Parameter	P	Spoofing		DoS		Sniffing		Data Modification	
		C	T	C	T	C	T	C	T
Access Vector to Sensor Network	0,10	4,0	0,40	6,9	0,69	10	1,00	6,0	0,60
Access Complexity to Sensor Network	0,10	6,9	0,69	7,0	0,70	9,0	0,90	3,9	0,39
Authentication	0,09	3,9	0,35	4,0	0,36	8,9	0,80	6,0	0,54
Confidentiality	0,09	6,0	0,54	4,0	0,36	10	0,90	6,0	0,54
Integrity	0,09	10	0,90	6,9	0,62	7,0	0,63	10	0,90
Availability	0,09	6,9	0,62	10	0,90	9,0	0,81	6,0	0,54
Exploitability	0,09	7,0	0,63	8,9	0,80	10	0,90	7,0	0,63
Reliability	0,09	3,9	0,35	3,9	0,35	7,0	0,63	6,0	0,54
Impact on Port Scanning Recognition	0,10	6,0	0,60	6,0	0,6	8,0	0,80	6,0	0,60
Ease of Remediation	0,08	6,0	0,48	6,0	0,48	7,0	0,56	7,0	0,56
Vulnerability Report Reliability	0,08	6,0	0,48	9,0	0,72	9,0	0,72	9,0	0,72
Total	1,00		6,04		6,58		8,65		6,56

The previous table shows the results, indicating that within the sensor network, the Sniffing technique achieved the highest score, with a rating of 8,65, followed by DoS with 6,58 points. Therefore, these techniques are considered the most suitable for identifying the most frequent vulnerabilities in the sensor network.

Phase 6: Final Analysis and Documentation

This final phase consolidates the findings and ensures the audit is traceable, repeatable, and actionable. It is organized into three subcomponents:

Documentation Artifacts

Comprehensive technical records were compiled, including:

- Captured packet logs from Wireshark and ZBOSS Sniffer.
- Network topology diagrams and flowcharts.
- Configuration files of Zigbee modules and XCTU logs.
- Attack scripts and observed anomalies.

These elements support the reproducibility of the experiment and provide forensic evidence for further audits or legal use (table 9).

Table 9. Summary of evidence

Scenario	Attack	Attack Technique	Tools Used	Vulnerability
Wireless sensor network measuring temperature	Confidentiality Integrity Availability	Sniffing Identity spoofing and data modification DoS	ZBOSS Sniffer WireShark XCTU Zigbee	Data Reading Manipulated data transmisión Denial of service Active traffic capture Packet capture
Sensor network measuring temperature and CO_2	Confidentiality Integrity Availability	Sniffing Identity spoofing and data modification DoS	ZBOSS Sniffer WireShark XCTU Zigbee	Network tracking Decryption of sensitive information Active traffic captu Packet capture Unauthorized data reading Manipulated CO_2 data transmission Random modification of temperature data Denial of service (no temperature or CO_2 data available)

Findings

A significant issue discovered in the wireless sensor network was the ease of data access, which could lead to misuse. The network was found to be particularly vulnerable due to inadequate encryption. One of the most revealing outcomes was observed during the first confidentiality attack: the system failed to detect any intrusion activity. This undetectability highlights a critical weakness in the network's monitoring capabilities. Without this attack, it would have been impossible to obtain the PAN ID, which is essential for performing subsequent attacks. Therefore, it was determined that access to the sensor network could be easily achieved in the absence of robust solutions or mechanisms. Consequently, it is imperative to implement protective measures to prevent or mitigate attacks on wireless sensor networks.

The findings from the attacks executed on the sensor network were categorized into positive and negative aspects, detailed in table 10 below:

Table 10. Positives and negatives

Aspects	Description
Negatives	Security weaknesses due to ease of tracking, decryption, and data capture. Eavesdropping attacks are stealthy and often go undetected. Limitations in network encryption.
Positives	Network stability, as there was minimal variability in the connection.

Once the vulnerabilities and attacks to which the wireless sensor network is exposed have been identified, it is recommended to review the cabling and wireless access to the network, implementing authentication mechanisms that allow only authorized users to gain access. If the wireless sensor network is to be used within an organization, security policies should be defined accordingly.

Technical Recommendations

Each identified vulnerability was mapped to mitigation strategies based on recognized standards (NIST SP 800-30, ISO/IEC 27002, OWASP Top 10 for IoT) (table 11):

- For confidentiality: encrypt frame payloads, use secure keys, enforce channel obfuscation.
- For integrity: enable packet authentication, deploy message integrity codes (MIC), enforce strict ID verification.
- For availability: rate-limit requests, detect anomalies, and implement resilience planning with fallback routing.

This approach aligns with previous studies addressing protocol-specific vulnerabilities, such as those affecting MQTT, where open-source IDS/IPS systems have demonstrated practical mitigation capabilities in IoT environments.(22)

Table 11. Attack Results Identified and Measured

Vulnerabilities	Attacks	Mitigation Measures
Network tracking Decryption of sensitive information Active traffic capture Packet capture Data reading	Confidentiality attacks	Apply encryption keys with neighboring nodes. Implement the SCADD protocol for detection and defense; encrypt the network. Monitor changes in network coverage. Use basic coverage inference protocols. Encrypt essential data.
Manipulated data transmission	Integrity attack	Use routing and authentication protocols. Enable authentication of incoming packets. Adopt recognized standards. Monitor the network continuously. Apply network segmentation. Implement physical access control.
Random modification of displayed data		Use advanced security technologies. Perform frequent data backups. Ensure strong authentication mechanisms.

		Adopt IEEE 802.1x and TKIP (Temporal Key Integrity Protocol). Implement intrusion detection and prevention systems (IDPS). Keep software up to date. Manage users and privileged accounts properly. Analyze packet content for application-layer protocol detection.
Denial of service	Availability attack	Apply a recovery plan (regular backups). Intercept incoming traffic. Monitor newly established network connections from or to untrusted hosts.

As observed, the proposed measures are aligned with the identified vulnerabilities and are based on the guidelines provided by MITRE, NIST, and OWASP standards.

Replicability and Scalability

The methodology is designed to be adaptable across other low-power and lossy networks (LLNs), including Thread and BLE mesh systems. A template was developed to guide audit teams through the six-phase process in similar deployments.

This structured documentation ensures the audit's findings can be reused, extended, or applied to continuous security assessment strategies.

The described scenarios are deterministic (same topology, seeds, and configurations), which ensures that CVSS scores remain consistent upon re-execution. As a complementary auxiliary descriptive metric, available in our logs, we report the percentage of captured packets during sniffing and the packet loss rate under DoS. These figures do not alter the risk ranking (tracking remains highest) but illustrate magnitude and consistency, particularly in the dual-sensor case.

DISCUSSION

The results obtained in this study reflect a clear and recurring challenge in the field of wireless sensor networks: the fragility of these systems when exposed to common cyberattacks. Although standards such as IEEE 802.15.4 provide a foundational framework for low-power communication, they are not inherently secure. As noted in prior literature[3] and further evidenced in our own experiments, many of the vulnerabilities stem from limited encryption practices and lack of authentication mechanisms.

From a practical perspective, the attack simulations confirmed that even with basic equipment and public tools such as Wireshark or ZBOSS Sniffer, it is possible to compromise the confidentiality, integrity, and availability of the network. Notably, sniffing attacks stood out not only for their simplicity but also for their stealth. In many cases, data could be intercepted without triggering any alerts on the system, a critical concern also raised by Alabdulatif[8] in his analysis of IEEE 802.15.4 vulnerabilities.

It is essential to note that the second scenario, which introduced CO_2 sensors, increased the attack surface and revealed a greater number of vulnerabilities. This aligns with Nithya et al.[15], who argue that heterogeneous nodes, while improving sensing capability, often bring complexity that weakens the overall security posture.

Our use of the CVSS model proved effective for quantifying and comparing the risk levels of different attack vectors. This scoring method enabled a prioritization of threats, providing actionable insight for mitigation. The combination of CVSS with NIST SP 800-30 reinforced the credibility and standardization of the evaluation.

Beyond numbers and tools, this research reinforces a key principle: WSNs must be designed with security as a core requirement, not as an afterthought. The audit methodology presented here provides a replicable and scalable approach for identifying critical weaknesses, particularly in environments where resilience and data integrity are essential.

Practical implications: In smart agriculture (Scenario 1), DoS and spoofing can distort irrigation or climate-control decisions if telemetry is delayed or falsified; enforcing authenticated encryption and anomaly detection at the gateway reduces this risk. In urban air-quality monitoring (Scenario 2), metadata leakage still supports traffic profiling under encryption; rate limiting and join throttling mitigate re-join bursts and service instability during desync attempts.

Applicability to Thread and BLE Mesh. In Thread (1.4), device commissioning uses authenticated sessions and certificates (TCAT), restricting passive inspection and shifting the discovery phase toward commissioning metadata and telemetry. Risk assessment remains aligned with NIST/CVSS. In BLE Mesh, provisioning and key distribution similarly limit access to the data plane; evaluation then emphasizes the control plane, resilience testing, and security configuration checks. In both cases, the pipeline is preserved, with only instrumentation varying.

Limitations and Future Work

Limitations. The study is limited to small-scale, unencrypted networks and basic attacks; it does not address side-channel threats, large-scale heterogeneity, or integration with 5G/LoRaWAN IoT ecosystems.

Future work. Extend the evaluation to encrypted meshes (Thread/BLE Mesh) and larger topologies; incorporate energy-consumption metrics and performance under load; validate with basic statistical analysis ($n \geq 5$, mean ± SD); and explore lightweight IDS/AI modules integrated into the pipeline. Future studies will leverage NIST SP 800-53 Rev.5 for prioritization and ENISA ETL 2023 for threat contextualization.

CONCLUSIONS

This study demonstrated the effectiveness of a structured security audit methodology tailored to wireless sensor networks. Organized into six sequential phases and rooted in the principles of Offensive Security and the IEEE 802.15.4 standard, the approach enabled the successful identification of critical vulnerabilities through hands-on experimentation with tools such as Wireshark, ZBOSS Sniffer, and XCTU.

The application of intrusive testing techniques, including sniffing, identity spoofing, denial of service (DoS), and data modification, revealed a consistent pattern of weaknesses, particularly in areas where encryption and authentication were lacking. Among these, sniffing emerged as the most effective and stealthy vector, as measured by the Common Vulnerability Scoring System (CVSS), which accounted for access complexity, exploitability, and potential impact.

Based on the detected vulnerabilities, specific mitigation strategies were proposed, aligning with international standards such as NIST SP 800-30, ISO/IEC 27002, and OWASP for IoT. These recommendations reinforce the scalability and adaptability of the proposed methodology to different network configurations and threat landscapes.

Ultimately, this work contributes a practical and standardized auditing framework that not only diagnoses security gaps but also supports continuous improvement in the cybersecurity posture of WSNs, especially in environments where data confidentiality, integrity, and availability are non-negotiable.

BIBLIOGRAPHIC REFERENCES

1. Valencia L, Guarda T, Patricio G, Arias L, Ninahualpa Quiña G. Seguridad de la Información en WSN aplicada a Redes de Medición Inteligentes basado en técnicas de criptografía. Revista Ibérica de Sistemas e Tecnologias de Informação. 2019;(E17):393–406. https://www.risti.xyz/issues/ristie17.pdf

2. Chinnow J, Bsufka K, Schmidt AD, Bye R, Camtepe A, Albayrak S. A simulation framework for smart meter security evaluation. In: SMFG 2011 - IEEE International Conference on Smart Measurements for Grids, Proceedings. doi: 10.1109/SMFG.2011.6125758; 2011. p. 1–9. doi: 10.1109/SMFG.2011.6125758.

3. Oreku GS, Pazynyuk T. Security in wireless sensor networks. Security in Wireless Sensor Networks. Springer Cham; 2015. 1–87 p. doi: 10.1007/978-3-319-21269-2.

4. Batista Guerra FK. Diseño e implementación de un modelo individual para la simulación de la propagación de malware en redes de sensores inalámbricas. Universidad de Salamanca; 2020. https://gredos.usal.es/handle/10366/145241

5. Calle-Tenesaca ME, Andrade-Amoroso RP. Ciberseguridad en contabilidad: protegiendo la integridad de los datos financieros en empresas comerciales. Revista Metropolitana de Ciencias Aplicadas. 2024;7(S2):87–98. https://remca.umet.edu.ec/index.php/REMCA/article/view/734

6. Cuzme-Rodríguez F, Zambrano-Romero W, Moreira-Zambrano C, Almeida-Zambrano E, Cuenca Álaba W. Security in smart objects, a general view at the physical and logical level. INNOVATION & DEVELOPMENT IN ENGINEERING AND APPLIED SCIENCES. 2019 Jun 6;1(1):33–46. https://revistasojs.utn.edu.ec/index.php/ideas/article/view/5

7. Vásquez A. Auditoría de seguridad e investigación de protocolos IoT (Thread y Zigbee). Universidad de Santiago de Compostela; 2021. https://nootropico.li/files/tfg/TFG_IoT_ZigbeeThread.pdf

8. Alabdulatif AA. Security Attacks in IEEE 802.15.4: A Review Disassociation Procedure. Advances in Intelligent Systems and Computing. 2020;1073:477–85. https://link.springer.com/chapter/10.1007/978-3-030-33582-3_45

9. Bluetooth SIG. Mesh Security Overview | Bluetooth® Technology Website. 2025. https://www.bluetooth.com/bluetooth-resources/mesh-security-overview/

10. Thread Group. Thread 1.4 Features White Paper. 2024. https://www.threadgroup.org/ThreadSpec.

11. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD; 2020 Dec. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

12. López Delgado JL, López Ramos JA. A Comprehensive Survey on Generative AI Solutions in IoT Security. Electronics 2024, Vol 13, Page 4965. 2024 Dec 17;13(24):4965. https://www.mdpi.com/2079-9292/13/24/4965

13. Pinto A, Herrera LC, Donoso Y, Gutierrez JA. Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. Sensors 2023, Vol 23, Page 2415. 2023 Feb 22; 23(5):2415. https://www.mdpi.com/1424-8220/23/5/2415

14. Tejedor Doria JA. Pentesting Iot Device Smart Doorlock. Universidad Complutense de Madrid; 2020. https://hdl.handle.net/20.500.14352/9080

15. Nithya N, Rajendran N. Secure Data Aggregation Technique using Audit based scheme for Wireless Sensor Network. Turkish Online Journal of Qualitative Inquiry. 2021;12(6):8643–54. https://tojqi.net/index.php/journal/article/view/3318

16. Tejena-Macías MA. Análisis de riesgos en seguridad de la información. Polo del Conocimiento. 2018;3(4):230–44. https://polodelconocimiento.com/ojs/index.php/es/article/view/809

17. Cuzme-Rodríguez F, León-Gudiño M, Suárez-Zambrano L, Domínguez-Limaico M. Offensive Security: Ethical Hacking Methodology on the Web. In: Botto-Tobar M, Barba-Maggi L, González-Huerta J, Villacrés-Cevallos P, S. Gómez O, Uvidia-Fassler M, editors. Information and Communication Technologies of Ecuador (TICEC) TICEC 2018 Advances in Intelligent Systems and Computing. Springer, Cham; 2019. p. 127–40. https://link.springer.com/chapter/10.1007/978-3-030-02828-2_10

18. MeteoSur. Nuevo sistema de sensores inalámbricos hace posible el monitoreo en tiempo real para la agricultura por ambientes. 2020. https://www.meteosur.com/node/18

19. Negi R, Gupta S, Hasan W, Kumar D. IoT Sensors and Networks for Crop Monitoring and Management. Agriculture 40. 2024;45–67. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003570219-3/iot-sensors-networks-crop-monitoring-management-radhika-negi-sheetanshu-gupta-wajid-hasan-dhirendra-kumar

20. Mordor Intelligence. Pronóstico del mercado de la red de sensores inalámbricos (2022 - 27) | Tamaño de la industria, tendencias. 2023. https://www.mordorintelligence.com/es/industry-reports/wireless-sensor-networks-market

21. Zhang D, Woo SS. Real Time Localized Air Quality Monitoring and Prediction through Mobile and Fixed IoT Sensing Network. IEEE Access. 2020;8:89584–94. https://ieeexplore.ieee.org/document/9090830

22. Heredia-Andrango A, Cuzme-Rodríguez F, Maya-Olalla E, Domínguez-Limaico HM, Jaramillo-Vinueza E. Mitigating MQTT Vulnerabilities in IoT with Open-Source IDS/IPS: A Practical Approach. 2025;13–22. https://link.springer.com/chapter/10.1007/978-3-031-92651-8_2

FINANCING

The author(s) received no financial support for the research.

CONFLICT OF INTEREST

The authors declare no conflicts of interest. The funders had no role in the study design, in the manuscript writing, or in the decision to publish the results.

AUTHORSHIP CONTRIBUTION

Conceptualization: Fabián Cuzme-Rodríguez, Kevin Oñate-Pozo.
Data curation: Kevin Oñate-Pozo, Fabián Cuzme-Rodríguez, Henry Farinango-Endara.
Formal analysis: Luis Suárez-Zambrano, Edgar Jaramillo-Vinueza.
Research: Kevin Oñate-Pozo, Fabián Cuzme-Rodríguez, Luis Suárez-Zambrano.
Methodology: Kevin Oñate-Pozo, Edgar Jaramillo-Vinueza.

Project management: Fabián Cuzme-Rodríguez, Jorge Benalcázar-Gómez.
Resources: Kevin Oñate-Pozo.
Software: Kevin Oñate-Pozo.
Supervision: Fabián Cuzme-Rodríguez, Luis Suárez-Zambrano, Jorge Benalcázar-Gómez.
Validation: Fabián Cuzme-Rodríguez, Luis Suárez-Zambrano.
Display: Kevin Oñate-Pozo.
Drafting - original draft: Kevin Oñate-Pozo, Henry Farinango-Endara.
Writing - proofreading and editing: Fabián Cuzme-Rodríguez, Henry Farinango-Endara.