Advances in Engineering and Innovation

Advances in Engineering and Innovation
Vol. 11, No. 24, pp. 236-248
Enero - Junio 2026

www.progreso.tecnm.mx/revistaAEI
ISSN: 2448-685X

Análisis de mecanismos de tolerancia a fallas mediante agrupamiento en WSN dentro de aplicaciones IoT

Analysis of fault tolerance mechanisms by clustering in WSNs within IoT applications

Mauricio Emir Cabrera Baeza[1] y Víctor Sandoval Curmina[1*]

[1]*Tecnológico Nacional de México, Instituto Tecnológico de Mérida, Avenida Tecnológico Km. 4.5, Colonia Plan de Ayala, CP 97118, Mérida, Yucatán, México.*

**Corresponding author:*
victor.sc@merida.tecnm.mx

Resumen. Las redes de sensores inalámbricos se han consolidado como una de las tecnologías más relevantes dentro del IoT para aplicaciones como agricultura de precisión y la automatización en la industria 4.0, gracias a su capacidad para monitorear entornos físicos en tiempo real mediante nodos de sensores distribuidos espacialmente en dichos entornos. Sin embargo, su funcionamiento enfrenta limitaciones importantes debido a la escasez de energía, la inestabilidad de los enlaces y la posibilidad de fallas en los nodos, lo que afecta directamente la integridad y disponibilidad de los datos. En este contexto, los mecanismos de tolerancia a fallas permiten mantener la operación de la red incluso ante la presencia de errores o fallas parciales. Este trabajo presenta un análisis general sobre los fundamentos, tipos de fallas, estrategias preventivas y curativas, así como los principales protocolos de agrupamiento utilizados para garantizar la eficiencia energética y la resiliencia en WSN.

Palabras clave: redes de sensores inalámbricas / tolerancia a fallas / eficiencia energética / agrupamiento / IoT.

Abstract. Wireless sensor networks have established themselves as one of the most significant technologies within the IoT in applications such as precision agriculture and Industry 4.0, thanks to their ability to monitor physical environments in real time through spatially distributed sensor nodes. However, its operation faces significant limitations due to power shortages, link instability, and the possibility of node failures, which directly affect data integrity and availability. In this context, fault tolerance mechanisms allow network operation to be maintained even in the presence of errors or partial failures. This paper presents a general analysis of the fundamentals, types of failures, preventive and curative strategies, as well as the main clustering protocols used to ensure energy efficiency and resilience in WSN.

Keywords: wireless sensor networks / fault tolerance / energy efficiency / clustering / IoT.

I. INTRODUCCIÓN

Las redes de sensores inalámbricas (Wireless Sensor Networks, WSN) representan el corazón de un sistema basado en IoT, una de las arquitecturas más importantes dentro del panorama tecnológico actual debido a su aplicación en áreas tan diversas como la salud, el monitoreo ambiental, la agricultura inteligente, la automatización en la industria 4.0 y la gestión de infraestructuras críticas (Heinzelman et al., 2000; Adday et al., 2022). Una WSN está compuesta por un conjunto de nodos sensores distribuidos en un entorno determinado, los cuales pueden agruparse en clústeres y tienen la función de percibir, procesar y transmitir información hacia un nodo central o estación base (Base

Recibido: 15/Octubre/2025
Aceptado: 28/Noviembre/2025

Station, BS). Estos nodos suelen contar con capacidades limitadas de energía, procesamiento, almacenamiento y comunicación, lo que genera restricciones severas en su operación continua (Mohapatra & Rath, 2020).

La naturaleza de estas redes implica una alta vulnerabilidad de fallas, tanto en los nodos individuales como en los enlaces de comunicación, debido a factores como el agotamiento energético, interferencias electromagnéticas, condiciones ambientales extremas o defectos de hardware (Chouikhi et al., 2015). En consecuencia, garantizar la fiabilidad y disponibilidad de la información recolectada se convierte en un desafío central. Aquí es donde cobran relevancia los mecanismos de tolerancia a fallas (Fault Tolerance, FT), entendidos como la capacidad del sistema para mantener su funcionamiento correcto incluso en presencia de errores o fallas parciales (Karim et al., 2014).

Los mecanismos FT son esenciales en aplicaciones críticas donde la pérdida de datos o la desconexión de un nodo pueden comprometer toda la red. Por ejemplo, en el monitoreo estructural de puentes o en la supervisión ambiental de zonas de riesgo, la falla de un único nodo puede provocar brechas de cobertura o retrasos en la entrega de información, afectando la capacidad de respuesta del sistema (Behera et al., 2019). En términos generales, la FT en WSN no se limita únicamente a la detección y recuperación ante errores, sino que abarca también aspectos de prevención, redundancia, gestión de energía y reorganización dinámica de la red (Azharuddin et al., 2015). Esta diversidad de enfoques refleja la complejidad inherente de diseñar sistemas inalámbricos resilientes y energéticamente eficientes.

A lo largo de los últimos años, se han propuesto múltiples protocolos y estrategias FT orientados a prolongar la vida útil de la red y reducir la probabilidad de fallas energéticas debido a no tener la energía suficiente para establecer un enlace de comunicación. Entre ellos destacan los protocolos de agrupamiento (clustering), como LEACH (Low-Energy Adaptive Clustering Hierarchy), SEP (Stable Election Protocol), V-LEACH, FEHCA y NN_ILEACH, que buscan equilibrar el consumo energético entre nodos mediante el cambio de los nodos líderes de clúster (Cluster Heads, CH) con la finalidad garantizar la continuidad operativa ante fallas por no contar con la energía necesaria para establecer un enlace de comunicación con la BS (Smaragdakis et al., 2004; Choudhary et al., 2021; El-Sayed et al., 2024).

Ahora, si se piensa en una aplicación, la implementación de WSN en la agricultura de precisión presenta un desafío critico de conectividad: la distancia de la WSN con una BS. Frecuentemente, los cultivos se encuentran a kilómetros de la infraestructura de red principal, lo que hace inevitable el agotamiento energético acelerado en los nodos sensores si estos transmiten directamente a la BS que está dentro de la infraestructura de red. Esto impone el uso obligatorio de protocolos de agrupamiento jerárquico, como LEACH, que organizan los nodos en grupos y selecciona a un líder. Este líder agrega la información de sus miembros y la transmite directamente a la BS, lo que reduce las transmisiones individuales a larga distancia y optimiza el consumo energético. No obstante, esta dependencia de la jerarquía introduce un punto único de falla: CH. Si este nodo líder agota su energía prematuramente, todo su grupo queda aislado, perdiéndose información vital. Los mecanismos tradicionales de LEACH, basados en probabilidades aleatorias, no garantizan la disponibilidad ante estos eventos, y las soluciones existentes varían drásticamente en complejidad y eficiencia.

Por consiguiente, el objetivo de este trabajo es presentar un análisis de los mecanismos de FT basados en agrupamiento en WSN, evaluando su evolución y pertinencia dentro de aplicaciones IoT modernas como la agricultura de precisión, enfocándose en el uso de métricas de rendimiento específicamente orientadas a evaluar las fallas de los CHs o nodos sensores por agotamiento energético para discutir los retos y tendencias emergentes en su desarrollo.

II. FUNDAMENTOS TEÓRICOS DE LA WSN Y LA FT.

A. Contexto general de las WSN y FT.

Las WSN están conformadas por nodos sensores autónomos, pequeños dispositivos que integran sensores, microcontroladores, módulos de comunicación inalámbrica y, generalmente, una fuente de energía no renovable (como una batería de litio). Los nodos cooperan entre sí para recopilar información del entorno —como temperatura, humedad, vibraciones, presión o luz— y transmitirla hacia una BS, donde se realiza el procesamiento central (Akyildiz et al., 2002).

La FT se define como la capacidad de un sistema para continuar funcionando correctamente aun en presencia de fallas o errores parciales. En las WSN, este concepto cobra una importancia crítica debido a la vulnerabilidad inherente de los nodos, la comunicación inalámbrica y la dependencia energética. Según Karim et al. (2014), un sistema tolerante a fallas no evita necesariamente que los errores ocurran, sino que garantiza la continuidad del servicio mediante la detección, aislamiento y recuperación automática de los componentes defectuosos. En este contexto, los mecanismos FT pueden clasificarse en dos grandes categorías según el momento en que actúan: estrategias preventivas (orientadas a evitar o retrasar la aparición de fallas) y estrategias curativas (centradas en la recuperación del funcionamiento después de que se ha producido una falla) (Adday et al., 2022).

B. Arquitectura y componentes fundamentales

Una WSN se organiza normalmente en una topología jerárquica o plana, dependiendo de su aplicación y protocolo de comunicación. En la arquitectura plana, todos los nodos poseen las mismas funciones y responsabilidad de comunicación, mientras que, en la jerárquica de agrupamiento, los nodos se agrupan en clústeres, y un nodo especial, denominado CH, actúa como intermediario entre sus miembros y la BS (Heinzelman et al., 2000). Este modelo jerárquico es el más adoptado en aplicaciones de bajo consumo energético, dado que reduce la cantidad de transmisiones directas hacia la BS y permite agregar información antes de enviarla.

De acuerdo con Behera et al. (2019), una WSN típica está compuesta por cuatro subsistemas principales:

1. Subsistema de detección: formado por los sensores y actuadores responsables de percibir el entorno físico.
2. Subsistema de procesamiento: Integrado por un microcontrolador o microprocesador de bajo consumo que ejecute las tareas de procesamiento local.
3. Subsistema de comunicación: responsable del envío y recepción de datos, generalmente mediante radiofrecuencia bajo estándares como IEEE 802.15.4 o LoRa.
4. Subsistema de energía: Conformado por una batería o fuente de alimentación limitada que determina la vida útil del nodo.

Cada nodo sensor, a pesar de su simplicidad individual, adquiere un rol esencial dentro del sistema global, ya que la falla de uno o varios nodos puede afectar la cobertura espacial, la conectividad de red y la precisión de los datos recolectados (Chouikhi et al., 2015).

Dentro de la arquitectura de WSN modernas, la gestión de datos y la capacidad de cómputo se organiza en una jerarquía de tres capas donde es posible realizar el procesamiento de la información, conocidas como cómputo en la nube, en la niebla y en el borde (Bonomi et al., 2012).

El cómputo en la nube (cloud computing) es el modelo centralizado que permite el acceso a la red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (como redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser aprovisionados y liberados rápidamente con un esfuerzo de gestión o interacción con el proveedor (Mell & Grance, 2011). La nube opera de forma centralizada en vastos centros de datos remotos, lo que ofrece economía de escala y una capacidad de cómputo masiva y virtualmente ilimitada (Satyanarayanan, 2016). Sus casos de uso ideales son el análisis de Big Data, el almacenamiento a largo plazo de datos y el entrenamiento de modelos complejos de inteligencia artificial (Bonomi et al., 2012).

El cómputo en la niebla (fog computing) es una arquitectura de computación distribuida y altamente virtualizada que extiende el paradigma de cómputo en la nube al borde de la red (Bonomi et al., 2012; Naha et al., 2018). Utiliza la metáfora de que la niebla es una nube cerca del suelo para describir su posición arquitectónica (Bonomi et al., 2012). Proporciona servicios de cómputo, almacenamiento y redes entre los dispositivos finales de IoT y los centros de datos tradicionales de la nube (Bonomi et al., 2012; Naha et al., 2018; Stojmenovic & Wen, 2014; Kalyani & Collier, 2021). La función principal del cómputo en la niebla es actuar como una capa intermedia de orquestación e inteligencia contextual que gestiona un entorno local cohesivo (Stojmenovic & Wen, 2014). Los nodos en la niebla recopilan datos de múltiples dispositivos del borde, realizan un preprocesamiento y agregan los datos antes de enviarlos a la nube, reduciendo drásticamente el volumen de tráfico (Bonomi et al., 2012).

El cómputo en el borde (edge computing) es un paradigma que migra la computación o el almacenamiento de datos al borde de la red, cerca de los usuarios finales o en el mismo dispositivo que los genera (Yu et al., 2018; Kalyani & Collier, 2021). Su objetivo es llevar el cómputo a los datos, y no los datos al cómputo. Permite respuestas en el orden de milisegundos, crucial para la seguridad y el control de procesos de alta velocidad. Aunque a menudo se confunde este paradigma con el cómputo en la niebla, el cómputo en el borde se enfoca sobre el procesamiento en un nodo individual que tiene capacidades de cómputo y almacenamiento más limitadas que un nodo que realiza el cómputo en la niebla (Kalyani & Collier, 2021).

La Figura 1 presenta un modelo de arquitectura WSN que combina los paradigmas de cómputo en la niebla y en borde. La red está segmentada en clústeres, que representan la capa donde se realiza el cómputo en el borde. Dentro de cada clúster, varios nodos sensores (equipados con sensores, batería y capacidad de comunicación) recopilan datos y se los envían a otro nodo del clúster que tiene la función de CH. El CH actúa como un agregador local, procesando la información de su clúster para reducir la redundancia y el consumo de energía. La comunicación entre los clústeres y la infraestructura central se realiza a través de los CHs, que utilizan algún protocolo de red de área amplia y baja potencia (Low Power Wide Area Network, LPWAN) para enviar los datos consolidados a la BS. Esta estación se sitúa en la capa de cómputo en la niebla, actuando como intermediaria para un procesamiento de datos más complejo antes de que la información llegue, si es necesario, a la nube. Este diseño jerárquico optimiza el consumo de energía y la gestión del ancho de banda en la red.

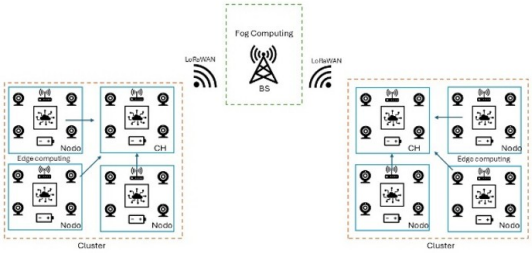

Figura 1. Estructura básica de una WSN con arquitectura de agrupamiento jerárquica. Fuente: Elaboración propia.

C. Limitaciones inherentes a las WSN

A diferencia de las redes tradicionales, las WSN enfrentan restricciones significativas en recursos físicos y computacionales; entre las limitaciones más críticas que competen al propósito de este trabajo se encuentran:

a) Energía: El consumo energético es el factor más determinante para el rendimiento de una WSN. La mayoría de los nodos funcionan con baterías no recargables, y su reemplazo puede ser inviable en entornos remotos o de difícil acceso (Adday et al., 2022). Según Heinzelman et al. (2002), el 70 % del gasto energético total de un nodo se destina a la transmisión de datos, lo que motiva el diseño de protocolos de comunicación eficientes y estrategias que reduzcan la cantidad de envíos innecesarios.
b) Comunicación inalámbrica: Las transmisiones inalámbricas están sujetas a interferencias, pérdidas de paquetes y fluctuaciones de señal. Además, los enlaces suelen ser asimétricos y altamente dependientes de la distancia entre nodos. Estas condiciones provocan fallas transitorias en la red y degradan el rendimiento si no se emplean mecanismos de recuperación adecuados (Choudhary et al., 2021).

D. Comunicación y jerarquía en las WSN

El modelo de comunicación más común en WSN jerárquicas es el modelo por rondas (round-based), donde el ciclo de operación se divide en dos fases: la fase de configuración (selección de CH y formación de clústeres) y la fase estable (transmisión de datos). En la primera, los nodos deciden si convertirse en CH con base en un umbral de probabilidad o en métricas como energía residual o distancia al BS. En la segunda, los nodos miembros envían sus datos al CH, que los agrega y transmite un único paquete al BS (Heinzelman et al., 2002). Este esquema reduce significativamente el número de transmisiones directas al BS, pero introduce una vulnerabilidad crítica: la falla del CH. Si un CH muere por agotamiento energético o daño físico, todos los nodos de su clúster quedan temporalmente aislados, perdiendo comunicación con el resto de la red (Choudhary et al., 2021). Por ello, la FT en estos sistemas debe contemplar mecanismos de respaldo o sustitución automática de los CH, así como estrategias de detección temprana de fallas.

E. Tipología de fallas en WSN

El correcto funcionamiento de una WSN depende de la cooperación continua entre múltiples nodos distribuidos espacialmente. Sin embargo, las limitaciones energéticas, las condiciones ambientales adversas y las fallas de hardware o software hacen que estas redes sean inherentemente propensas a fallas (Adday et al., 2022). En la Tabla 1 se muestran algunos de los tipos de fallas comunes.

Tabla 1. Clasificación y características de las fallas en WSN. Fuente: Elaboración propia con base en Adday et al. (2022), Chouikhi et al. (2015) y Choudhary et al. (2021).

Tipo de falla	Causa principal	Efecto sobre la red
Falla de nodo	*Agotamiento energético, daño de hardware o error de software*	*Pérdida de datos o nodo inactivo*
Falla de red	*Interferencias, colisiones, fallas de enlace o de enrutamiento*	*Retrasos, reenvíos múltiples, mayor consumo energético*
Falla de CH	*Sobrecarga energética o falla de comunicación*	*Aislamiento del clúster y pérdida de agregación de datos*

F. Estrategias preventivas

Las estrategias preventivas son aquellas que buscan minimizar la probabilidad de falla mediante una planificación eficiente del uso de recursos, una organización óptima de la red y la implementación de mecanismos de redundancia. Este enfoque tiene como objetivo principal prolongar la vida útil de la red y evitar fallas tempranas, especialmente los derivados del agotamiento energético (Heinzelman et al., 2000).

La redundancia es uno de los principios más antiguos y efectivos en el diseño de sistemas tolerantes a fallas. En el caso de las WSN, puede implementarse en distintos niveles:

1. Redundancia de nodos: Consiste en desplegar más nodos de los estrictamente necesarios para asegurar que la falla de uno no afecte la cobertura del área. Esta técnica es útil en aplicaciones críticas como monitoreo ambiental o industrial (Chouikhi et al., 2015).
2. Redundancia de rutas: Implica mantener múltiples rutas alternativas de comunicación entre nodos y la BS. Si un enlace falla, la red puede redirigir los datos automáticamente a través de otra ruta activa (Azharuddin et al., 2015).
3. Redundancia de datos: Los nodos pueden enviar lecturas repetidas o paquetes codificados para asegurar la recuperación de información aun si se pierde parte del mensaje (Mohapatra & Rath, 2020).

Dado que la energía es el recurso más limitado, una de las estrategias preventivas más estudiadas es la gestión energética adaptativa, cuyo propósito es describir equitativamente el consumo entre los nodos (Behera et al., 2019). Esta gestión se logra mediante mecanismos como:

- Rotación de roles: en los protocolos de agrupamiento, los nodos asumen de manera alternada la función de CH para evitar que unos pocos se agoten rápidamente (Heinzelman et al., 2000).
- Ajuste de potencia de transmisión: los nodos adaptan su nivel de potencia según la distancia a su receptor, minimizando el gasto energético (Adday et al., 2022).
- Programación de ciclos de sueño y actividad: permite que los nodos no involucrados en comunicación permanezcan inactivos temporalmente, reduciendo el consumo sin afectar la conectividad (Azharuddin et al., 2015).

El control de la topología busca mantener la red conectada incluso si algunos nodos fallan. Para ello, se aplican algoritmos que gestionan la posición lógica de los nodos activos y su grado de conectividad (Karim et al., 2014). Un enfoque común es el uso de k-conectividad, que garantiza que cada nodo tenga al menos k vecinos directos disponibles para comunicación (Pu et al., 2009). Los protocolos preventivos también utilizan modelos de autoorganización dinámica, donde los nodos ajustan su estado (activo o inactivo) en función de la densidad local, la energía residual y la demanda de comunicación.

Una estrategia preventiva menos discutida, pero crucial, es la planificación del despliegue. El diseño de la ubicación de los nodos determina la cobertura, conectividad y equilibrio energético de la red (Adday et al., 2022). Un despliegue uniforme con densidad suficiente permite compensar fallas individuales sin afectar la funcionalidad general. En cambio, un despliegue irregular puede generar “zonas muertas” donde la pérdida de un nodo deja el área sin monitoreo.

G. Estrategias curativas

A diferencia de las estrategias preventivas, las estrategias curativas actúan una vez que la falla ha ocurrido. Su propósito es detectar, aislar y recuperar el sistema afectado con el menor impacto posible sobre la red global (Mohapatra & Rath, 2020). Este tipo de mecanismos puede implicar reconfiguración topológica, reasignación de funciones o sustitución de nodos, dependiendo del tipo y gravedad de la falla.

El primer paso en toda estrategia curativa es la detección de fallas. Los nodos o la BS deben identificar cuando un componente deja de funcionar correctamente. Para ello se utilizan dos enfoques principales:

1. Detección proactiva: Los nodos envían periódicamente mensajes de confirmación o heartbeats para indicar su estado activo. Si un nodo o CH deja de enviar dichos mensajes, se asume que ha fallado (Lindsey & Raghavendra, 2002).
2. Detección reactiva: las fallas se identifican cuando se detectan anomalías en los datos recibidos, como valores atípicos, retardos excesivos o pérdidas de paquetes (Chouikhi et al., 2015).

Ejemplos representativos incluyen el protocolo FT-EEC (Fault-Tolerant Energy-Efficient Clustering), que combina la detección periódica de actividad con la evaluación de energía residual para determinar si un nodo o CH ha fallado (Karim et al., 2014).

Una vez identificado una falla, la red debe reorganizarse para mantener la conectividad. Este proceso de reconfiguración puede realizarse de manera centralizada, donde la BS toma decisiones globales, o distribuida, donde los nodos vecinos colaboran para sustituir al componente defectuoso (Adday et al., 2022).

Un ejemplo de estrategia distribuida es el algoritmo DFCR (Distributed Fault-tolerant Clustering and Routing), el cual permite que los nodos sin cobertura busquen de forma autónoma nuevos vecinos o CHs con alta energía para reenviar sus datos (Choudhary et al., 2021). En sistemas centralizados, como FEHCA, la BS designa un nuevo CH secundario para reemplazar al principal antes de que falle (Choudhary et al., 2021).
Los mecanismos de respaldo consisten en preparar nodos alternativos para asumir funciones críticas en caso de falla. Por ejemplo, el protocolo V-LEACH (Vice cluster head LEACH) designa en cada cluster un Vice Cluster Head (VCH) que asume el control inmediatamente si el CH principal deja de responder (Sasikala et al., 2015). De esta manera, se asegura la continuidad de la agregación y transmisión de datos sin necesidad de reconfigurar toda la red. Otros enfoques, como el FEHCA (Fault-Tolerant Energy-Efficient Hierarchical Clustering Algorithm), utilizan un modelo jerárquico donde cada CH tiene un secundario preparado para asumir su rol (Choudhary et al., 2021). Este método combina alta confiabilidad con eficiencia energética, aunque su implementación centralizada puede generar sobrecarga de procesamiento en la BS.

Otra técnica curativa consiste en la selección de nuevos CH o rutas alternativas considerando la energía residual (RE, Residual Energy) de los nodos activos. Este enfoque se observa en protocolos como DARE-SEP (Distance Aware Residual Energy-Efficient SEP), que selecciona líderes de clúster según la energía restante y la distancia al sumidero, reduciendo la probabilidad de falla prematuro (Naeem et al., 2021). Asimismo, el protocolo FR-LEACH (Fuzzy Rule LEACH) aplica lógica difusa para ajustar dinámicamente los umbrales de selección de CH con base en la energía, densidad de nodos y distancia promedio, mejorando la estabilidad general (Mohapatra & Rath, 2019).

El uso de IA y aprendizaje automático (Machine Learning, ML) se ha convertido en una herramienta poderosa para mejorar los mecanismos curativos. Por ejemplo, el NN_ILEACH (Neural Network Improved LEACH) utiliza redes neuronales para determinar el CH óptimo basándose en la energía residual y la historia de fallas, logrando una vida útil de red hasta 20 veces superior a LEACH (El-Sayed et al., 2024).

Estos métodos permiten predecir la probabilidad de falla antes de que ocurra, facilitando una reconfiguración preventiva o semicurativa. En la tabla 2 se muestra a grandes rasgos un resumen de las estrategias preventivas y curativas.

Tabla 2. Estrategias preventivas y curativas en mecanismos de FT. Fuente: Elaboración propia con base en Adday et al. (2022), Heinzelman et al. (2000), Choudhary et al. (2021) y El-Sayed et al. (2024).

Tipo de estrategia	Enfoque	Ejemplo	Ventajas	Limitaciones
Preventiva	*Redundancia*	*Rutas y nodos alternativos*	*Aumenta la robustez y cobertura.*	*Mayor consumo energético*
Preventiva	*Gestión energética*	*LEACH*	*Prolonga la vida útil de la red mediante rotación de roles.*	*No contempla fallas de CH.*
Preventiva	*Control de topología*	*k-conectividad*	*Mantiene conectividad ante fallas locales.*	*Sobrecarga en redes densas*
Curativa	*Reconfiguración*	*DFCR*	*Recuperación distribuida sin intervención del BS*	*Puede generar retrasos de sincronización.*
Curativa	*Mecanismo de respaldo*	*V-LEACH/ FEHCA*	*Sustitución inmediata del CH fallido*	*Aumento de complejidad y control centralizado*
Curativa	*IA y ML*	*NN_ILEACH*	*Predicción de fallas y selección óptima de CH*	*Requiere mayor procesamiento local.*

Estas estrategias —tanto preventivas como curativas— constituyen la base de los protocolos de agrupamiento tolerantes a fallas.

III. METODOLOGÍA

A. Importancia de la eficiencia energética

El consumo energético no solo limita la vida de un nodo individual, sino también la vida útil global de la red (Network Lifetime, NL). Dado que la sustitución o recarga de baterías suele ser complicada, se busca diseñar estrategias que distribuyan equitativamente el consumo entre todos los nodos. Este concepto es central en los protocolos de agrupamiento jerárquico, como LEACH y sus derivados, donde los roles de comunicación (por ejemplo, actuar como CH) se rotan para evitar que ciertos nodos se agoten prematuramente (Heinzelman et al., 2000).

Behera et al. (2019) señalan que la vida útil de una WSN se divide en tres fases: (1) período de estabilidad, donde todos los nodos están activos; (2) período de inestabilidad, cuando los primeros nodos comienzan a fallar; y (3) fase de colapso, en la que la red pierde conectividad.

B. Resiliencia y fiabilidad como objetivo de diseño

En las últimas dos décadas, la comunidad científica ha coincidido en que el diseño de WSN debe regirse por dos principios clave: eficiencia energética y resiliencia (Adday et al., 2022). La eficiencia energética busca minimizar el gasto de batería por transmisión, mientras que la resiliencia garantiza la capacidad del sistema de mantener un desempeño aceptable ante fallas internos o externos. Ambos factores están estrechamente relacionados: una red energéticamente eficiente tiende a ser más estable y, por ende, más tolerante a fallas. Sin embargo, lograr un equilibrio entre ambos aspectos es complejo. Las estrategias de redundancia y monitoreo continuo que aumentan la resiliencia suelen implicar un costo energético adicional, lo que obliga a buscar compromisos adaptativos entre consumo y fiabilidad (Azharuddin et al., 2015). Por ejemplo, protocolos como FEHCA y NN_ILEACH implementan mecanismos centralizados o inteligentes de selección de CH que consideran la energía residual, la distancia al BS y la estabilidad del enlace para maximizar la eficiencia global sin sacrificar robustez (Choudhary et al., 2021; El-Sayed et al., 2024).

C. Naturaleza y frecuencia de las fallas

Los estudios empíricos sobre despliegues reales de WSN muestran que las fallas de nodo (donde se encuentran las fallas por agotamiento energético, como se aprecia en la tabla 1) son responsables de aproximadamente el 60–70 % de las interrupciones de servicio (Behera et al., 2019), y si además la falla de un nodo sensor se presenta cuando está operando como CH, entonces se tiene un impacto desproporcionadamente alto en la pérdida de datos y en la conectividad de la red, por lo que la mayoría de los protocolos de agrupamiento modernos se centran en su prevención.

Otro aspecto importante para mencionar es que las fallas suelen seguir patrones temporales o espaciales como, por ejemplo, los nodos sensores que se encuentran más alejados de la BS van a sufrir de agotamiento energético más rápido que los que están más cerca cuando les toca operar como CH, lo que reduce el número de sensores vivos en la WSN.

El impacto de las fallas puede medirse mediante tres indicadores principales:

1. Reducción de la tasa de entrega de paquetes (Packet Delivery Ratio, PDR): las fallas por agotamiento energético de los nodos sensores que puedan funcionar como CH genera que menos nodos puedan transmitir sus paquetes y provoca una reducción en la cantidad de paquetes que se pueden transmitir.
2. Incremento del consumo energético: los nodos restantes de una WSN deben invertir más energía al transmitir a un CH que está más alejado de él cuando los nodos más cercanos a él ya no tienen energía para ser CH.
3. Disminución de la vida útil de la red: la energía se consume de forma desigual debido a las diferentes distancias entre los nodos con el CH o las distancias de un CH con la BS, lo que acelera la muerte de nodos y reduce la estabilidad general (Karim et al., 2014).

D. Métricas de rendimiento y evaluación

La evaluación del desempeño de los mecanismos de FT en WSN requiere la definición de métricas cuantitativas que reflejen su eficiencia, estabilidad y resiliencia ante fallas.

Dado que estas redes operan bajo severas limitaciones de energía y procesamiento, las métricas deben capturar el equilibrio entre consumo energético, confiabilidad de la comunicación y vida útil de la red (Behera et al., 2019).

El análisis de desempeño no solo permite comparar protocolos, sino también determinar el impacto real de las estrategias FT en la prolongación del servicio y la integridad de los datos. En la literatura, las métricas más utilizadas se agrupan en cuatro categorías principales: (1) energéticas, (2) de confiabilidad, (3) de desempeño temporal y (4) de estabilidad y cobertura (Choudhary et al., 2021).

Las métricas energéticas son fundamentales, ya que el consumo de energía determina directamente la durabilidad de la red. Las más utilizadas son:

a) Consumo energético promedio (E_avg): Indica la cantidad promedio de energía consumida por los nodos durante la operación de la red. Un valor bajo refleja un protocolo eficiente. Según Heinzelman et al. (2000), el consumo energético puede calcularse a partir de la energía total transmitida y recibida por nodo, sumando las pérdidas en agregación de datos.
b) Energía residual promedio (E_res): Corresponde al nivel medio de energía remanente en los nodos al finalizar una ronda o periodo de simulación. Esta métrica es clave para evaluar la distribución del consumo y la sostenibilidad del protocolo (Azharuddin et al., 2015).
c) Balance energético (E_balance): Evalúa la dispersión del consumo energético entre los nodos. Un protocolo equilibrado evita que ciertos nodos se agoten prematuramente, reduciendo el riesgo de “agujeros energéticos” (Adday et al., 2022).
d) Vida útil de la red (NL): Es la métrica energética más representativa y se define como el tiempo (o número

de rondas) hasta que un porcentaje determinado de nodos queda inactivo.

Las métricas de confiabilidad evalúan la capacidad de la red para mantener una comunicación estable y una entrega de datos correcta incluso en presencia de fallas. Las principales métricas de esta categoría son:

a) Tasa de detección de fallas (Fault Detection Rate, FDR): Mide la efectividad del mecanismo FT para identificar correctamente las fallas reales. Un FDR alto indica buena capacidad de monitoreo, pero debe complementarse con una baja tasa de falsos positivos (Adday et al., 2022).
b) Disponibilidad del sistema (System Availability, SA): Corresponde al porcentaje de tiempo en el que la red está plenamente operativa. Los sistemas con alta disponibilidad (superior al 95 %) son preferibles en aplicaciones industriales o de seguridad (Karim et al., 2014).

Las métricas de desempeño temporal se relacionan con la eficiencia de procesamiento y transmisión de información en la red. Estas métricas son especialmente relevantes en mecanismos curativos, donde las reconfiguraciones o reelecciones deben realizarse sin afectar significativamente el retardo global. Las principales métricas de desempeño temporales son:

a) Retardo extremo a extremo (End-to-End Delay, E2E): Es el tiempo total que tarda un paquete en ir desde el nodo sensor hasta la BS. Los mecanismos de FT pueden incrementar este valor si requieren pasos adicionales de verificación o recuperación (Chouikhi et al., 2015).
b) Tiempo de recuperación (Recovery Time, RT): Se define como el tiempo transcurrido entre la detección de una falla y la completa restauración de la funcionalidad del sistema. Protocolos como V-LEACH o FEHCA presentan tiempos de recuperación inferiores a 2 segundos debido a su mecanismo de respaldo inmediato (Choudhary et al., 2021).
c) Sobrecarga de comunicación (Communication Overhead, CO): Corresponde a la cantidad adicional de mensajes o paquetes de control necesarios para mantener la FT. Una sobrecarga excesiva puede degradar el desempeño energético y aumentar el riesgo de colisiones (Adday et al., 2022).

Las métricas de estabilidad y cobertura se utilizan para evaluar la sostenibilidad del protocolo a largo plazo, así como la capacidad de la red para mantener su cobertura espacial y operativa durante el tiempo. Las principales métricas de estabilidad y cobertura son:

a) Período de estabilidad (Stability Period, SP): Representa la duración del tiempo entre el inicio de la operación y la muerte del primer nodo. Un mayor SP refleja mejor eficiencia en el uso de energía y mayor FT tempranos (Smaragdakis et al., 2004).
b) Cobertura de red (Network Coverage, NC): Evalúa el porcentaje del área monitoreada activa respecto al total del área desplegada. Los protocolos con FT buscan mantener una cobertura superior al 90 % incluso después de varios eventos de falla (Behera et al., 2019).
c) Robustez estructural (Structural Robustness, SR): Mide la capacidad de la red para conservar la conectividad ante la pérdida de nodos o enlaces. La robustez se evalúa mediante indicadores topológicos como el grado medio de conectividad o el número de componentes activos en la red (Adday et al., 2022).

Para evaluar la eficacia y el desempeño de los mecanismos de FT, se usarán exclusivamente las métricas energéticas. Estas incluyen el cálculo de la vida útil de la red, definida como el tiempo hasta la muerte del último nodo, y el balance energético que evalúa la dispersión del consumo entre los nodos para prevenir el colapso de la red.

E. Enfoque experimental y simulación

La mayoría de los estudios sobre mecanismos FT utilizan simulaciones computacionales para evaluar estas métricas, debido a la dificultad de realizar pruebas en entornos físicos. Herramientas como MATLAB, NS-2/NS-3, OMNeT++ y Python (SimPy o LEACHSim) permiten recrear escenarios de despliegue de WSN y medir el impacto de distintas estrategias FT bajo condiciones controladas (Mohapatra & Rath, 2020). Un enfoque común consiste en comparar el rendimiento de protocolos clásicos frente a versiones mejoradas, midiendo variables como energía consumida, número de CH activos y tasa de entrega de paquetes. Los protocolos de agrupamiento clásicos son:

- LEACH: El primer y más influyente protocolo de agrupamiento jerárquico propuesto para WSN. Fue desarrollado por Heinzelman et al. (2000) con el objetivo de reducir el consumo energético mediante rotación probabilística de los CH.
- SEP: Introducido por Smaragdakis et al. (2004) como una mejora sobre LEACH, destinada a entornos

heterogéneos, es decir, redes donde los nodos poseen diferentes niveles iniciales de energía.

En el caso de protocolos con versiones mejoradas están:

- V-LEACH: Propuesto por Sasikala et al. (2015) como una extensión directa de LEACH, enfocada específicamente en la FT del CH. Cada clúster designa dos líderes: un CH principal, responsable de la agregación y transmisión de datos; y un VCH, que actúa como respaldo inmediato en caso de falla del CH principal.
- FEHCA: Combina un enfoque centralizado y jerárquico, donde la BS tiene un papel activo en la selección y gestión de los CH. De acuerdo con Choudhary et al. (2021), FEHCA utiliza información sobre la energía residual, la distancia al BS y la densidad local para seleccionar CH de manera óptima.
- NN_ILEACH: Propuesto por El-Sayed et al. (2024), este protocolo utiliza inteligencia artificial con un enfoque de aprendizaje supervisado dentro del aprendizaje de máquina mediante el empleo de una red neuronal artificial entrenada para predecir la probabilidad de falla de un nodo en función de su energía residual, distancia al BS y tasa de participación previa como CH, con el fin de evitar que los CH con bajo nivel de energía sean seleccionados en rondas posteriores.

IV. RESULTADOS

El análisis comparativo de los protocolos de agrupamiento jerárquicos enfocados en la FT por consumo energético en WSN se centra en la capacidad de los algoritmos para prolongar la vida útil de la red y gestionar de manera eficiente la energía residual de los nodos. Los resultados destacan las limitaciones del protocolo base LEACH y las mejoras sustanciales aportadas por protocolos conscientes de la energía y la heterogeneidad (SEP, NN_ILEACH, FEHCA) y aquellos que implementan mecanismos de redundancia (V-LEACH).

A continuación, se presenta el análisis comparativo de las estrategias de agrupamiento, evaluando sus mecanismos de recuperación ante la falla crítica del CH.

A. LEACH

Características y desventajas clave:

- Consumo y vida útil: LEACH logra una reducción de hasta 8 veces en la disipación de energía en comparación con los protocolos de enrutamiento convencionales, y en simulaciones, logró duplicar la vida útil del sistema.
- Gestión energética ineficaz: LEACH opera bajo el supuesto de que la red es homogénea, es decir, que todos los nodos poseen la misma energía inicial (Heinzelman, Chandrakasan, & Balakrishnan, 2000). Esta característica hace que su consumo de recursos energéticos no esté optimizado.
- Falla prematura y estabilidad: El protocolo LEACH es muy sensible a la heterogeneidad energética y pasa a un funcionamiento inestable rápidamente. No considera la energía residual de un nodo durante la selección de CH. Si un nodo con baja energía es elegido CH, mediante el proceso aleatorio basado en un umbral, se agotará anticipadamente, lo que afecta negativamente la vida útil de la red. La elección repetitiva de todos los nodos en el proceso de selección de CH consume una cantidad sustancial de energía.

B. SEP

Características y desventajas clave

- Mecanismo de selección: SEP es consciente de la heterogeneidad al asignar probabilidades de elección de CH ponderadas por la energía inicial relativa de los nodos. Es un protocolo de agrupamiento heterogéneo donde solo los “nodos avanzados” (aquellos con más energía inicial) son capaces de actuar como CH y realizar agregación de datos.
- Rendimiento: Las simulaciones indican que SEP siempre prolonga el periodo estable y su rendimiento promedio es superior a los protocolos que ignoran la heterogeneidad. En escenarios simulados, la región estable de SEP se extendió, por ejemplo, un 8% en comparación con LEACH. SEP es más resistente que LEACH en el consumo juicioso de la energía extra, logrando una región de estabilidad más larga para valores más altos de energía extra. Además, el rendimiento (throughput) de SEP es significativamente mayor que el de LEACH en la región estable y en la mayor parte de la región inestable.

C. V-LEACH

Características y desventajas clave

- Mecanismo de FT: V-LEACH utiliza un VCH, seleccionado en función de la energía residual de los nodos. El VCH reemplaza al CH principal cuando este último alcanza un nivel de energía bajo, evitando la muerte prematura de CH.

- Impacto en la red: El uso de un VCH garantiza que los datos se sigan enviando a la BS incluso si el CH muere en una ronda específica. Reemplazar un CH por un VCH evita la necesidad de una operación de reagrupamiento completa, lo que aumenta significativamente la vida útil de la red al ahorrar energía.
- Desventajas: La implementación de un CH extra introduce una sobrecarga adicional (overhead). Además, V-LEACH utiliza comunicación single-hop del CH a la BS, lo que no mitiga el problema de los costos de transmisión a larga distancia.

D. FEHCA

Características y desventajas clave

- Mecanismo de FT: FEHCA utiliza el algoritmo de clustering k-means para agrupar los nodos en un número óptimo de clústeres. Aborda las fluctuaciones en la disipación de energía causadas por el agrupamiento aleatorio de LEACH. Es capaz de manejar la pérdida de paquetes en caso de fallas permanentes en los CH.
- Rendimiento en longevidad: En simulaciones donde la BS estaba en el centro, FEHCA duró, en promedio, un 70% más que el algoritmo LEACH. Además, FEHCA prolongó la vida útil de la red en un 50% más de rondas que LEACH, manteniendo más del 90% de los nodos operativos durante la mayor parte del tiempo. También duplico las rondas de comunicación en comparación con LEACH cuando la BS estaba colocada lejos.

E. NN_ILEACH

Características y desventajas clave

- Técnicas clave: Utiliza una red neuronal para la selección dinámica y basada en datos de los CH, lo que asegura que los nodos más adecuados sean elegidos CH. Además, incorpora el mecanismo de eliminación de agujeros de energía (EHORM) para equilibrar el uso de energía y reducir las fallas prematuras de los nodos.

Rendimiento cuantificado:

- Vida útil y longevidad: NN_ILEACH extiende la vida útil de la red a 11,361 rondas, comparado con solo 505 rondas de LEACH en condiciones idénticas, lo que representa una mejora de más de 20 veces.
- Consumo energético: El protocolo reduce el consumo general de energía en un 40%. Numéricamente, NN_ILEACH alcanzó cero energías residuales en la ronda 11,362.
- Rendimiento de datos: NN_ILEACH demostró un aumento del 30% en el throughput y un 25% de mejora en el PDR en comparación con LEACH e ILEACH.

Como objetivo de analizar y comparar el rendimiento de los protocolos de agrupamiento, se utilizan comúnmente las métricas energéticas como la vida útil de la red y la energía residual promedio. En las figuras 2 y 3 ilustran los ejemplos de la gráfica del número de nodos vivos durante las rondas que está asociado con la métrica vida útil de la red y la gráfica de la energía en la red con la que quedan los nodos cuando ya no pueden transmitir a la BS (asociado con la energía residual promedio de los nodos). Este tipo de gráficas se espera replicar con la implementación simulada del sistema mediante el uso de Matlab o Python.

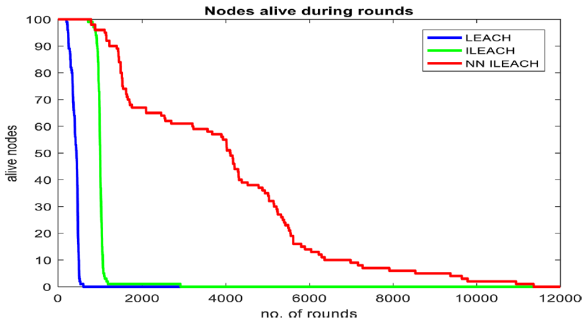

Figura 2. Grafica de nodos vivos por ronda con NN_ILEACH. Fuente: Tomado de El-Sayed et al. (2024).

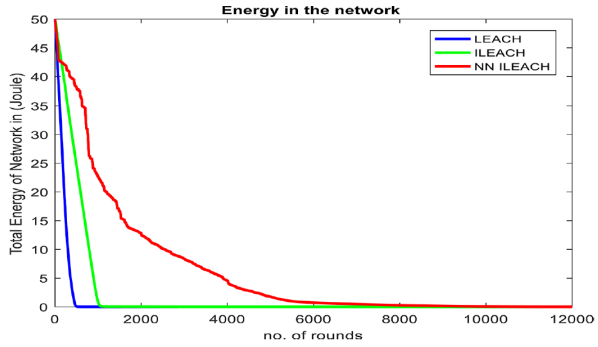

Figura 3 Grafica de energía de la red con NN_ILEACH. Fuente: Tomado de El-Sayed et al. (2024).

Según las referencias consultadas, los resultados típicos muestran que los protocolos con mecanismos FT integrados pueden aumentar la vida útil de la red entre un 25 % y un 60 %, dependiendo del escenario y la densidad de nodos (El-Sayed et al., 2024). Un aspecto clave en la evaluación es el compromiso entre resiliencia y eficiencia. Los mecanismos FT mejoran la confiabilidad, pero a

menudo incrementan el número de mensajes de control y el procesamiento local, lo cual puede elevar el consumo energético. Por tanto, el diseño óptimo debe buscar un punto de equilibrio dinámico, donde la red mantenga su estabilidad sin sacrificar la eficiencia global (Adday et al., 2022). Las tendencias actuales apuntan hacia sistemas inteligentes y adaptativos, capaces de modificar sus parámetros de operación según el contexto (energía restante, tasa de fallas, tráfico de red). El uso de modelos híbridos, que combinan algoritmos clásicos con predicción basada en IA, se perfila como la vía más prometedora para mantener este equilibrio en escenarios reales (El-Sayed et al., 2024).

V. DISCUSIÓN

El análisis comparativo evidencia una evolución progresiva en los protocolos de agrupamiento, desde esquemas probabilísticos y estáticos (como LEACH y SEP) hacia modelos predictivos e inteligentes (como NN_ILEACH).

Las primeras generaciones priorizaban la eficiencia energética, mientras que los desarrollos más recientes incorporan mecanismos explícitos de FT, basados en respaldo, redistribución y predicción.

Los resultados experimentales y simulaciones reportadas por diversos autores coinciden en que los algoritmos con capacidad de aprendizaje o selección adaptativa duplican la estabilidad de la red en comparación con versiones básicas (Adday et al., 2022; El-Sayed et al., 2024).

No obstante, esta mejora conlleva un costo en complejidad computacional y requerimientos de procesamiento local, lo cual sigue siendo un reto para dispositivos de baja capacidad. Por tanto, la investigación actual busca protocolos híbridos, donde la inteligencia se distribuye parcialmente entre la BS y los nodos. En la tabla 3 se muestra un resumen elaborado con la revisión de los resultados y aportaciones presentados por los cinco protocolos de agrupamiento que se analizaron.

VI. CONCLUSIONES

La FT es un pilar fundamental para el diseño y despliegue de WSN robustas y fiables. La vulnerabilidad inherente de los nodos, principalmente por el agotamiento energético, exige mecanismos que garanticen la continuidad operativa, especialmente en aplicaciones críticas.

La evolución de los protocolos de agrupamiento demuestra un avance significativo, pasando de estrategias probabilísticas enfocadas en la eficiencia energética mediante rotación de CH, como LEACH y SEP, a arquitecturas que integran mecanismos de respaldo explícitos, como V-LEACH y FEHCA. La tendencia más prometedora reside en la aplicación de inteligencia artificial, como se observa en NN_ILEACH, que permite una gestión predictiva de las fallas, seleccionando los nodos más estables como líderes y prolongando notablemente la vida de la red.

Tabla 3. Comparativa de protocolos de agrupamiento con mecanismos de FT. Fuente: Elaboración propia con base en Heinzelman et al. (2000), Smaragdakis et al. (2004), Sasikala et al. (2015), Choudhary et al. (2021) y El-Sayed et al. (2024).

Protocolo	Selección de CH	Ventajas	Limitaciones
LEACH	*Aleatoria y rotativa.*	*Simplicidad, bajo costo computacional.*	*Baja confiabilidad ante fallas de CH.*
SEP	*Probabilística basada en energía*	*Equilibrio energético, prolonga estabilidad*	*Sin respaldo o detección de fallas*
V-LEACH	*Aleatoria con rol secundario (VCH)*	*Alta fiabilidad, bajo retardo de recuperación.*	*Incremento de consumo energético*
FEHCA	*Selección basada en energía y distancia*	*Alta tolerancia, eficiencia global*	*Sobrecarga en BS, limitada escalabilidad.*
NN_ILEACH	*Basada en red neuronal.*	*Alta eficiencia y resiliencia*	*Complejidad computacional elevada*

A pesar de estos avances, el principal desafío sigue siendo el equilibrio entre la resiliencia y el consumo energético, junto con la complejidad computacional que los algoritmos más avanzados imponen sobre los nodos de bajos recursos. Las futuras líneas de investigación deberán enfocarse en el desarrollo de protocolos híbridos y adaptativos que puedan ajustar dinámicamente sus estrategias de FT en función de las condiciones de la red, logrando así sistemas más autónomos, eficientes y verdaderamente resilientes.

Para finalizar, con todo lo aprendido a través de la revisión del estado del arte sobre FT para WSN, ahora es necesario elegir una aplicación IoT donde el uso del concepto de FT para WSN resuelva una problemática

dada. En la figura 4 se muestra una arquitectura presentada para un sistema de agricultura de precisión basado en una WSN con un enfoque de computación distribuida en tres niveles.

En la base, la capa del borde (Edge Layer) está formada por múltiples nodos sensores autónomos desplegados directamente sobre el terreno agrícola y que serán los que se agrupen en clústeres. Estos nodos se encargan de la captura de datos primarios, como la intensidad lumínica, humedad, temperatura, etc. La información recolectada es transmitida mediante la tecnología de comunicación LoRaWAN, ideal para entornos rurales por su largo alcance, a la BS que es un nodo que se encuentra en la capa de la niebla (Fog Node). Esta capa consiste en una infraestructura local, como un servidor en la propia granja, que concentra los datos, los procesa previamente y puede tomar decisiones en tiempo real y es el punto de acceso al Internet. Finalmente, los datos agregados y preprocesados son enviados al servidor que se encuentra en la capa en la nube (Cloud Layer). En esta, un servidor de alta capacidad se encarga del almacenamiento masivo y del análisis complejo utilizando herramientas de Big Data y entrenamiento de modelos de inteligencia artificial. Esto permite identificar patrones a largo plazo, optimizar el uso de recursos y ofrecer al agricultor visualizaciones y alertas a través de un dashboard accesible desde cualquier lugar.

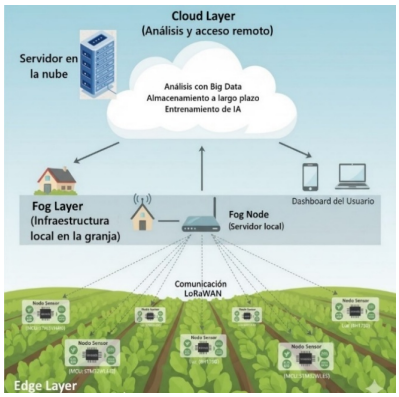

Figura 4. Modelo de arquitectura de una WSN para agricultura de precisión. Fuente: Elaboración propia.

REFERENCIAS

Adday, G. H., Subramaniam, S. K., Zukarnain, Z. A., & Samian, N. (2022). Fault Tolerance Structures in Wireless Sensor Networks (WSNs): Survey, Classification, and Future Directions. *Sensors, 22*(6041), 1-39.

Azharuddin, M., Kuila, P., & Jana, P. K. (2015). Energy efficient fault tolerant clustering and routing algorithms for wireless sensor networks. Computers & Electrical Engineering, 41, 177-190.

Behera, T. M., Mohapatra, S. K., Samal, U. C., Khan, M. S., Daneshmand, M., & Gandomi, A. H. (2019). Residual Energy-Based Cluster-Head Selection in WSNs for IoT Application. IEEE Internet of Things Journal, 6(3), 5132-5139.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the Internet of Things. *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, 13–16.

Choudhary, A., Kumar, S., Gupta, S., Gong, M., & Mahanti, A. (2021). FEHCA: A Fault-Tolerant Energy-Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks. Energies, 14(3935), 1-21.

Chouikhi, S., El Korbi, I., Ghamri-Doudane, Y., & Saidane, L. A. (2015). A survey on fault tolerance in small and large scale wireless sensor networks. Computer Communications, 69, 22-37.

El-Sayed, H. H., Abd-Elgaber, E. M., Zanaty, E. A., Alsubaei, F. S., Almazroi, A. A., & Bakheet, S. S. (2024). An efficient neural network LEACH protocol to extended lifetime of wireless sensor networks. Sensors, 24(6952), 1-17.

Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. En Proc. 33rd Hawaii Int. Conf. System Sciences (pp. 1-10). Maui, HI, USA.

Heinzelman, W. R., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications, 1(4), 660-670.

Karim, L., Nasser, N., & Sheltami, T. (2009). A Fault Tolerant Dynamic Clustering Protocol of Wireless Sensor Networks. Global Telecommunications Conference, IEEE, 1-6.

Karim, L., Nasser, N., & Sheltami, T. (2014). A fault-tolerant energy-efficient clustering protocol of a wireless sensor network. Wireless Communications and Mobile Computing, 14(1), 175-185.

Kalyani, Y., & Collier, R. (2021). A systematic survey on the role of cloud, fog, and edge computing combination in smart agriculture. *Sensors*, *21*(17), 5922.

Lindsey, S., & Raghavendra, C. S. (2002). PEGASIS: Power-Efficient Gathering in Sensor Information Systems. En Aerospace Conference Proceedings (pp. 3-1125-3-1130 vol.3).

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST Special Publication 800-145). National Institute of Standards and Technology.

Mohapatra, H., & Rath, A. K. (2019). Fault tolerance in WSN through PE-LEACH protocol. IET Wireless Sensor Systems, 9(6), 358-365.

Mohapatra, H., & Rath, A. K. (2020a). Fault-tolerant mechanism for wireless sensor network. IET Wireless Sensor Systems, 10(1), 23-30.

Mohapatra, H., & Rath, A. K. (2020b). Survey on fault tolerance-based clustering evolution in WSN. IET Networks, 9(4), 145-155.

Naeem, A., Javed, A. R., Rizwan, M., Abbas, S., Lin, J. C. W., & Gadekallu, T. R. (2021). DARE-SEP: A Hybrid Approach of Distance Aware Residual Energy-Efficient SEP for WSN. IEEE Transactions on Green Communications and Networking, 5(6), 611-621.

Naha, R. K., Garg, S., Georgakopoulos, D., Jayaraman, P. P., Gao, L., Xiang, Y., & Ranjan, R. (2018). Fog computing: Survey of trends, architectures, requirements, and research directions. *IEEE Access*, *6*, 47980–48009.

Pu, J., Xiong, Z., & Lu, X. (2009). Fault-tolerant deployment with k-connectivity and partial k-connectivity in sensor networks. Wireless Communications and Mobile Computing, 9, 909-919.

Sasikala, S. D., Sangameswaran, N., & Aravindh, P. (2015). Improving the energy efficiency of leach protocol using VCH in wireless sensor network. International Journal of Engineering Development and Research, 3, 918-924.

Satyanarayanan, M. (2016). The emergence of edge computing. *Computer*, *49*(10), 85–89.

Stojmenovic, I., & Wen, S. (2014). The Fog computing paradigm: Scenarios and security issues. *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems*, 1–8.

Smaragdakis, G., Matta, I., & Bestavros, A. (2004). SEP: A stable election protocol for clustered heterogeneous wireless sensor networks (Technical Report BUCS-TR-2004-022). Boston University, Boston, MA, USA.

Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2018). A survey on the edge computing for the Internet of Things. *IEEE Access*, *6*, 6900–6919.