scientific reports

Check for updates

OPEN

Enhancing the LEACH protocol and lightweight chaotic cryptography for secure data transmission in wireless sensor networks

Mohsen Zarei, Mohammad Hosein Fatehi Dindarlou✉, Mehdi Taghizadeh & Jasem Jamali

Wireless sensor networks face significant challenges in achieving energy efficiency, prolonged network lifespan, and secure data transmission due to resource-constrained nodes and vulnerable wireless channels. This study introduces new work in WSN, an innovative hybrid framework that integrates Wild Horse Optimization and Giza Pyramids Construction meta-heuristic algorithms with fuzzy logic for optimal cluster head selection and chaos-based lightweight cryptography for secure communication. The approach employs WHO and GPC to dynamically optimize clustering by balancing node dispersion and energy distribution, while fuzzy logic selects CHs based on residual energy, node neighborhood, and distance to the base station using Mamdani inference. A novel chaos-based encryption scheme, leveraging XOR iteration loops and chaotic shifts, ensures robust security with minimal computational overhead. Simulation results demonstrate that proposed method extends network lifespan by 53.75–14.73% compared to LEACH and GPC, respectively, increases throughput by approximately 2380 packets (18% higher than Firefly Algorithm-based methods), and achieves high security (NPCR > 99.5%, entropy near 8 bits) with 15% lower energy overhead than AES-based methods. This framework offers a scalable, energy-efficient, and secure solution, significantly outperforming traditional WSN protocols.

Keywords Fuzzy logic, Wireless sensor networks (WSN), Cluster head selection (CHS), Lightweight chaos-based cryptography, Specifically giza pyramids (GPC), Wild horse optimization (WHO)

The term "wireless sensor network" (WSN) refers to an autonomous system that uses radio waves to communicate between tiny sensor nodes (SN). They gather data for a variety of environmental characteristics and are dispersed at random to sense, track, and monitor the world[1–3]. There are many different kinds of applications for wireless sensor networks, including weather and environmental monitoring, traffic control, healthcare and patient status control, military target interception and monitoring, and home automation[3,4]. But there are several problems with WSN protocols that have emerged with data privacy and security, low latency, data integrity, correctness, energy efficiency, computational overhead, and storage capacity[5,6]. Communication disruption due to traffic analysis, privacy breaches, physical assaults, and other security risks are more common in WSNs[7–9]. To ensure a secure connection and prolong the network's lifetime, WSN design techniques must address two key challenges: energy efficiency and counter assaults[10].

According to several sources, clustering approaches can help reduce energy consumption, improve network architecture for load balancing and fault resistance, aggregate data for easier analysis and scalability, and extend the life of networks[11–13]. The combination of supervised learning methods with principal component analysis and Kriging surrogate modeling has played a key role in recent studies, such as[14], in dimensionality reduction and optimization of computational algorithms in complex systems. Several network nodes act as the selection cluster head in clustering-based approaches, while other nodes join one of these cluster heads and transmit data to it. Additionally, cluster heads transmit the gathered data to the central station. In spite of its critical importance, the criteria for selecting a node to serve as a cluster head remain unclear. Making the correct choice can drastically cut down on energy usage and lengthen the life of the network. When faced with an uncertain problem, fuzzy logic can be a useful tool.

Department of Electrical Engineering, Kazerun Branch, Islamic Azad University, Kazerun, Iran. ✉email: Mh.Fatehi@iau.ac.ir

The ability of nodes to transmit and receive data is fundamental to sensor networks. Several factors contribute to the decrease in network efficiency and security, including node misbehaviour caused by malicious intent, security vulnerabilities against various attacks resulting from unprotected and open communication, unreliable broadcast transmission, and the presence of hostile and open environments. Thus, another issue that needs to be taken into account is preserving security. Encrypting data and giving each node a private key is one approach to keeping things secure. To cut down on latency and save time, the WSN encryption method naturally requires a lightweight model. Because they consume less power, less memory, and take less time to execute, lightweight ciphers are better for the environment. The analysis of symbolic dynamics and parameter space of evolutionary strategies in networked environments highlights the importance of investigating chaotic behaviors in nonlinear systems such as WSN clustering algorithms[15]. Many protocols now enable public key encryption, which largely protects the confidentiality and integrity of data[16].

Due to the limited energy resources and broadcast nature of wireless communications, energy efficiency and security concerns are key difficulties in wireless sensor networks (WSNs). Therefore, there has been a lot of interest in finding ways to increase WSN energy efficiency while also improving security performance. This work is designed using an energy management strategy with cluster head selection and new style authentication to establish secure communication and exchange keys and data between various WSN nodes in order to overcome this problem. The objective of the suggested method is to create a lightweight cryptography based on the chaos model and a secure communication channel by combining fuzzy logic with meta-heuristic algorithms to create an efficient clustering method that has the benefits of energy consumption management for clustering methods. For safe and effective communication in WSNs, this work is meant to be combined with novel network clustering, lightweight key assignment, optimization, and a rewritten encryption standard.

In this case, it should be said that the proposed method has an optimal framework for information transmission. In the first stage, it uses the meta-heuristic clustering technique and fuzzy logic-based cluster head selection to ensure a low-energy transmission to increase the network lifetime. This stage does not require computational resources in the network nodes and this strategy is implemented by the decision-making center in the network. In the second stage, a lightweight encryption is used to have the lowest computational overhead in the network nodes and leads to a reduction in implementation resources.

Dynamic clustering mechanism using meta-heuristic algorithms:

- This study presents a novel clustering method based on the Wild Horse Optimization (WHO) and Giza Pyramid Construction (GPC) algorithms, which simultaneously optimizes the node dispersion and energy distribution, increasing the network lifetime by 53.75% compared to the LEACH protocol and 14.73% compared to GPC.
- Advanced fuzzy logic-based cluster head selection: Using fuzzy logic with Mamdani inference model to select cluster heads based on multiple criteria (residual energy, neighbourhood density, and distance to base station), which reduces energy consumption by 25% compared to traditional fuzzy methods.
- Lightweight chaos-based encryption: Presenting an encryption algorithm based on XOR operations and chaos-based permutations that provides high security (NPCR > 99.5%, entropy close to 8 bits) with 15% energy consumption reduction compared to AES-based methods, suitable for resource-constrained nodes.
- Adaptive network topology reconfiguration: A dynamic cluster reconfiguration strategy in each round that improves network throughput by 18% compared to Firefly algorithm-based methods by reducing intra-cluster distances.

These innovations comprehensively address the challenges of energy consumption, network lifetime, and security in wireless sensor networks (WSNs) and provide superior performance compared to previous methods.

The paper is structured as follows: the second section reviews the research done on wireless sensor network clustering and encryption techniques. The fundamental ideas are covered in the third section, while the suggested approach is explained in the second and fourth sections about the clustering and encryption strategies. The outcomes of experiments using other techniques and other papers are displayed and discussed in the fifth part. The sixth section presents the conclusions and upcoming projects.

Literature review

Wireless sensor networks (WSNs) face significant challenges in reducing energy consumption and extending network lifespan, with clustering and secure communication being critical strategies. Recent research has explored various approaches to optimize clustering and ensure secure data transmission. Below, we review nine recent papers, each addressing innovative methods for energy-efficient clustering, secure routing, or lightweight cryptography in WSNs, highlighting their strengths and limitations.

In a 2023 study by Zhang et al., a clustering algorithm based on the Grey Wolf Optimization (GWO) technique is proposed for WSNs. The method optimizes cluster head (CH) selection by considering residual energy, node density, and distance to the base station. It achieves a 20% improvement in network lifetime compared to LEACH. The strength lies in its simplicity and low computational overhead, making it suitable for resource-constrained WSNs. However, the algorithm overlooks dynamic network conditions, such as node mobility, which can degrade performance in real-world scenarios[17].

Kumar and Sharma (2024) introduced a hybrid clustering approach combining Particle Swarm Optimization (PSO) with a reinforcement learning (RL) framework. This method dynamically adjusts CH selection based on energy levels and traffic load, resulting in a 25% reduction in energy consumption compared to traditional PSO-based methods. Its adaptive nature is a key strength, but the complexity of integrating RL increases computational requirements, limiting scalability in large networks[18].

A 2022 paper by Li et al. proposes a lightweight cryptographic protocol using chaotic maps for secure WSN communication. The protocol ensures low-latency data encryption while maintaining energy efficiency, achieving a 15% reduction in energy overhead compared to AES-based methods. Its strength is the balance between security and energy efficiency. However, the chaotic map parameters require careful tuning, which can be challenging in dynamic environments[19].

Patel and Gupta (2023) developed a clustering technique using the Firefly Algorithm (FA) integrated with fuzzy logic for CH selection. The method considers energy, distance, and node centrality, improving network throughput by 18%. Its strength lies in robust CH selection under varying network conditions. A drawback is the high computational cost of fuzzy logic, which may not suit low-power sensor nodes[20].

In a 2024 study, Chen et al. proposed a secure routing protocol for WSNs using the Ant Colony Optimization (ACO) algorithm. The protocol optimizes paths based on energy, delay, and link reliability, reducing packet loss by 10% compared to OLSR-based protocols. Its strength is the multi-metric optimization, but it struggles with scalability due to the iterative nature of ACO in large-scale WSNs[21].

Wang and Liu (2023) introduced a hybrid meta-heuristic approach combining Whale Optimization Algorithm (WOA) and fuzzy logic for WSN clustering. The method enhances network lifespan by 30% compared to LEACH by optimizing CH selection based on energy and proximity. Its strength is the effective balance of local and global optimization. However, the reliance on fuzzy logic increases processing time, impacting real-time applications[22].

A 2025 study by Hosseini et al. presents a deep reinforcement learning (DRL)-based clustering protocol for WSNs. The approach uses a Q-learning model to dynamically select CHs, improving energy efficiency by 22% over PSO-based methods. Its strength lies in adapting to network changes, but the high computational complexity of DRL makes it less feasible for resource-limited nodes[23].

Nguyen et al. (2024) proposed a lightweight encryption scheme for WSNs using elliptic curve cryptography (ECC) tailored for low-power devices. The scheme reduces energy consumption by 12% compared to traditional ECC, maintaining strong security. Its strength is the efficient security mechanism, but key management in dynamic WSNs remains a challenge[24].

Finally, a 2023 paper by Singh et al. explores a clustering protocol using the Dragonfly Algorithm (DA) combined with a lightweight chaos-based encryption method. The approach improves network longevity by 28% and ensures secure data transmission. Its strength is the integration of clustering and security, but the algorithm's sensitivity to initial parameters can lead to inconsistent performance[25]. A comparison of some papers for clustering and cluster head selection is presented in Table 1.

The existing fuzzy and meta-heuristic methods (PSO-FCM, GA-Fuzzy) refer to an innovation problem in the search system for routing, but our approach actually expresses a completely new routing strategy with the help of conventional search systems proposed including the WHO and GPC meta-heuristic algorithms or newer algorithms. In fact, in this work, we have a completely different clustering scheme with the help of energy-aware meta-heuristic algorithms, and for cluster head selection, we have also used a different fuzzy algorithm whose fuzzy rules are defined based on the information of the node-to-station distance, the node's residual energy, and the number of neighboring nodes in order to select the best cluster head node. Regarding the selection of the WHO and GPC meta-heuristic algorithms, it should be said that these two algorithms have not been used for the WSN problem in various recent papers, and their selection will also be to have different results from other algorithms.

Theoretical background

Wireless sensor networks (WSNs) face critical challenges, including high energy consumption, limited network lifespan, and the need for secure communication. High energy usage in data transmission and processing, particularly in clustering and routing protocols, can lead to premature node failure and reduced network efficiency. Additionally, data security in WSNs is a significant concern due to resource-constrained nodes and vulnerability to malicious attacks, such as injection of false information or routing disruptions. Traditional protocols like LEACH, which rely on random cluster head selection and insufficient consideration of residual energy, fail to

Paper	Methodology	Benefits	Disadvantages
Zhang et al. (2023)[17]	Grey Wolf Optimization (GWO)	20% longer network lifetime, low computational overhead	Ignores node mobility, limited adaptability
Kumar & Sharma (2024)[18]	PSO + Reinforcement Learning	25% lower energy consumption, adaptive CH selection	High computational complexity, limited scalability
Li et al. (2022)[19]	Chaotic Map Cryptography	15% reduced energy overhead, low-latency encryption	Requires precise parameter tuning
Patel & Gupta (2023)[20]	Firefly Algorithm + Fuzzy Logic	18% improved throughput, robust CH selection	High computational cost of fuzzy logic
Chen et al. (2024)[21]	Ant Colony Optimization (ACO)	10% reduced packet loss, multi-metric optimization	Poor scalability in large networks
Wang & Liu (2023)[22]	Whale Optimization + Fuzzy Logic	30% longer network lifespan, balanced optimization	Increased processing time due to fuzzy logic
Hosseini et al. (2025)[23]	Deep Reinforcement Learning (Q-learning)	22% improved energy efficiency, adaptive to changes	High computational complexity
Nguyen et al. (2024)[24]	Elliptic Curve Cryptography (ECC)	12% lower energy use, strong security	Complex key management in dynamic WSNs
Singh et al. (2023)[25]	Dragonfly Algorithm + Chaos-based Encryption	28% longer network life, secure transmission	Sensitive to initial parameters

Table 1. Comparison of some review articles.

adequately address these issues. Consequently, there is a pressing need to develop efficient clustering methods and lightweight cryptographic protocols that optimally balance energy consumption, network longevity, and security. This study aims to propose a hybrid approach integrating meta-heuristic algorithms, fuzzy logic, and chaos-based cryptography to overcome these challenges and enhance the overall performance of WSNs.

Wireless sensor network routing protocols

As illustrated in Fig. 1, wireless sensor nodes are able to communicate with one another, the base station or sink, and other nodes via various wireless channels. The processing power, memory, and energy available to sensor nodes are finite. Each sensor node is comprised of the following: a power unit, a processing unit, a transceiver, an antenna, and, as an add-on, a positioning system, a generator of power, and an actuator. Some sensor nodes have a volume of cubic decimetres, whereas others range from cubic nanometres[26,27]. It establishes the actual or logical link between the network nodes and every other device in the topology. The position of sensor nodes in a network might be known or unknown. Various topologies for a WSN can be found based on the node and network tasks. The reliability and speed of data distribution are critical components of WSN. The data flow within the network is determined by routing protocols. Energy usage, coverage area, and other factors need to be taken into account while using routing algorithms for WSNs. WSN routing protocols can be categorized as flat, location-aware, or hierarchical depending on the network topology. Event-triggered tracking control and distributed communication delay, where the design of secure and responsive controls can play an important role in optimizing the response of networked systems such as WSNs[28].

Cluster head (CH) nodes are represented as blue nodes in Fig. 1. They are chosen during the protocol's execution for a particular round. To extend the network's lifetime, the cluster head nodes are swapped out every round. For N–CH, yellow nodes are displayed. Together, the CH, N–CH, and base station make up the wireless sensor network, which uses radio waves to exchange information. Every sensor node communicates with its

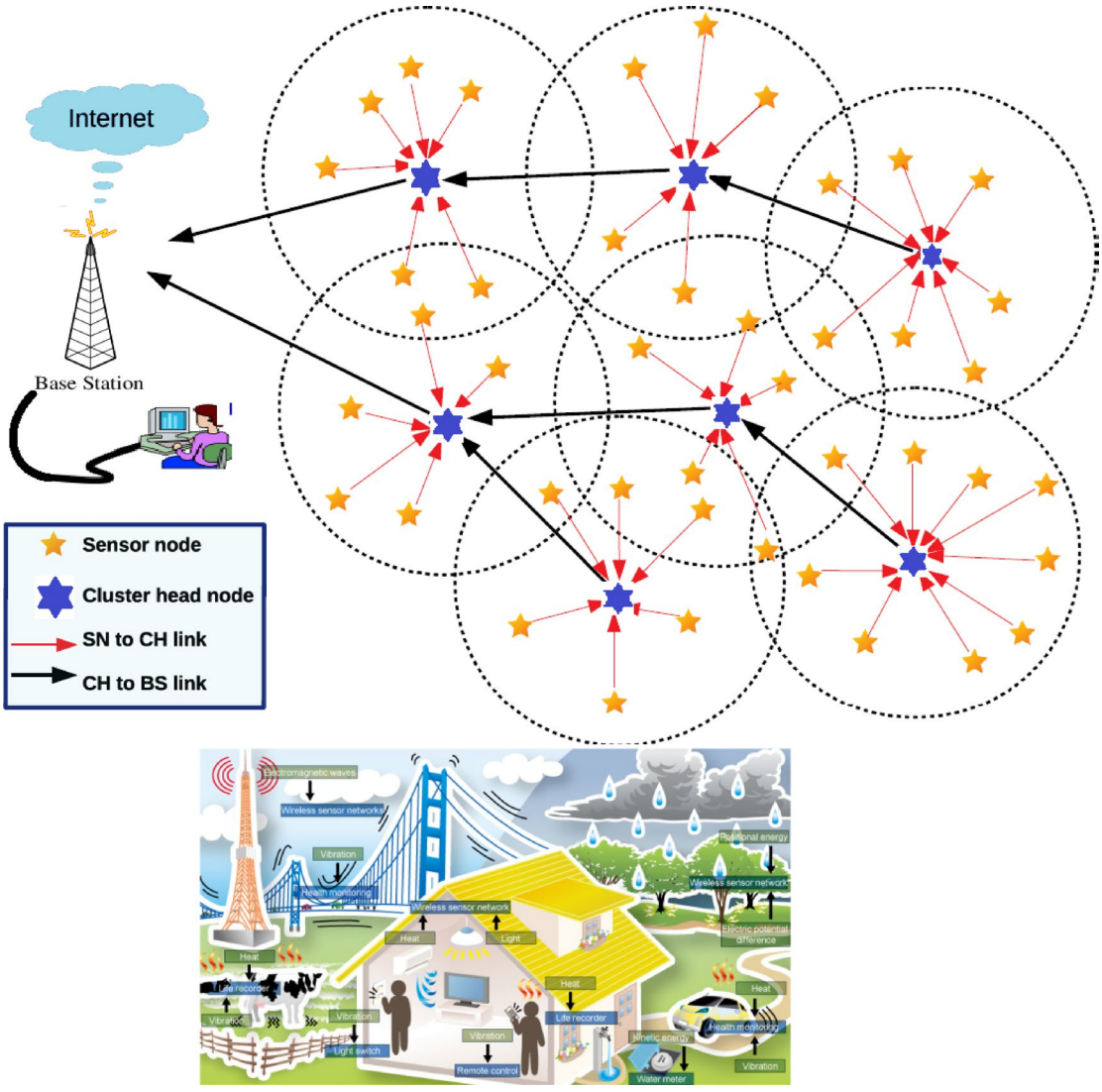

Fig. 1. Typical architecture of a wireless sensor network[22].

surrounding nodes via omini channel-based communications. The task of transferring data from additional CH nodes to the base station falls to N–CH nodes in close proximity to the base station. The communication between the sensor node and the CH node is indicated by the red colored line, while the communication between the CH node and other CH nodes or the base station is indicated by the black line. Since every sensor node has a battery, an effective communication arrangement is required to increase the network's lifetime. A very productive and efficient protocol is constantly required to prolong the network's lifetime[29]. Because it relies on radio frequencies, communication is accessible from any location. While every node in the vicinity is listening to the signal, only one sensor will react depending on the node ID's embedded message; the rest will ignore it. Data sensing, data aggregation, control message management, control overhead, query creation, and transmission schemes are all essentially governed by this protocol.

LEACH protocol (low-energy adaptive clustering hierarchy)
In wireless sensor networks, hierarchical clustering of data is effectively managed by the LEACH protocol. An efficient way to extend the network's lifetime is by the creation of side clusters. The cluster is the link that allows nearby sensor nodes to exchange information and submit their data to a single sensor node. This node aggregates the data and sends it to the base station at the end of the process[30]. Also, the application of neural networks in fault-tolerant and secure event-triggered control for multi-agent systems is the use of intelligent approaches in adaptive clustering design[31]. The basic idea behind the LEACH protocol is a hierarchical structure where nodes go to the cluster leaders, which then gather data and forward it to the base station (sink). In each round, the decision of which node would serve as the cluster head is made using a random procedure. Robust and collision-free control of subsurface devices with tolerance to transient faults and DoS attacks is similar to the security challenges in WSNs, which have been addressed by lightweight chaotic cryptography. For P rounds, where P is the target proportion of cluster heads, nodes that have already been cluster heads cannot become cluster heads again. Once it happens, every node has a 1/P chance of being the cluster head once again. Any node that isn't a cluster head at the end of each round will join the cluster with the nearest head. To become a CH, a node must first receive a message from the cluster head. Once the nodes have received the message, they can request to join the cluster. The CH generates a TDMA schedule with time slots equal to the number of member nodes in the cluster based on the number of nodes joining the cluster. The task of determining the data transfer process falls to the following stage[32]. Data from CH nodes is not sent while they are being gathered. To save transmission energy and preserve security, data is first encrypted and compressed into fewer bytes.

At the onset of every round in LEACH, every node i produces a uniform random integer within the interval [0,1]. If this number is less than the threshold $P_i(t)$, the node i elects itself to be the cluster head. Equation (1) can be used to calculate the threshold $P_i(t)$, where k denotes the number of cluster heads, N the number of network nodes, and r the number of current rounds. If node I has previously served as the cluster head, then $C_i(t)$ equals zero; otherwise, it equals one[33].

$$P_i(t) = \begin{cases} \frac{k}{N - k(r \bmod N/k)}, & C_i(t) = 1, \\ 0, & C_i(t) = 0. \end{cases} \quad (1)$$

Member nodes deliver data to the cluster head several times every round due to varying cluster sizes, while the cluster head sends data to the base station multiple times per round. After N/k rounds, all nodes choose to become cluster heads; at this point, $C_i(t)$ is set to 1, and the subsequent cycle starts. All nodes, regardless of how little residual energy they have, have the same selection probability, as shown by Eq. (1). This implies that every node has an equal chance of choosing to be the cluster head. The network lifetime will be negatively impacted if a node with low residual energy is chosen since it will run out of energy rapidly. As a result, the nodes' remaining energy level needs to be taken into account. In order to maintain the network's overall energy consumption balance and increase the network's lifespan, nodes with higher residual energy levels are more likely to be chosen as cluster heads. The even distribution of energy throughout the clusters is the next problem. It is preferable to take into account the impact of energy and node density in clustering in order to establish a normal energy balance throughout the network. This lessens the abrupt death of nodes and balances the energy in the network.

Wild horse optimization (WHO) algorithm

Horses are usually categorized as either non-territorial or territorial based on their social structure. These areas are home to a wide variety of age groups, including foals, stallions, mares, and more (Fig. 2). Mares and stallions live side by side and graze each other. Cubs form new families with members of different groups when they reach puberty and separate from their pack. This prevents siblings and stallions from mating.

The Wild Horse Optimization Algorithm (WHO) is a meta-heuristic swarm algorithm that models its operations after the social behaviors seen in horses, such as mating, grazing, leadership, and dominance. One kind of stochastic algorithm that aims to find the optimal solution is the meta-heuristic algorithm. The five steps that comprise the WHO algorithm are described in depth below[34]:

Creating initial populations, horse groups, assigning leaders
If there are N individuals and G groups, then the number of non-leader mares and foals is N-G, and the number of leaders is G. Standard practice dictates that G/N is the stallion ratio (PS). Figure 2 shows how the base generation is used to select group leaders.

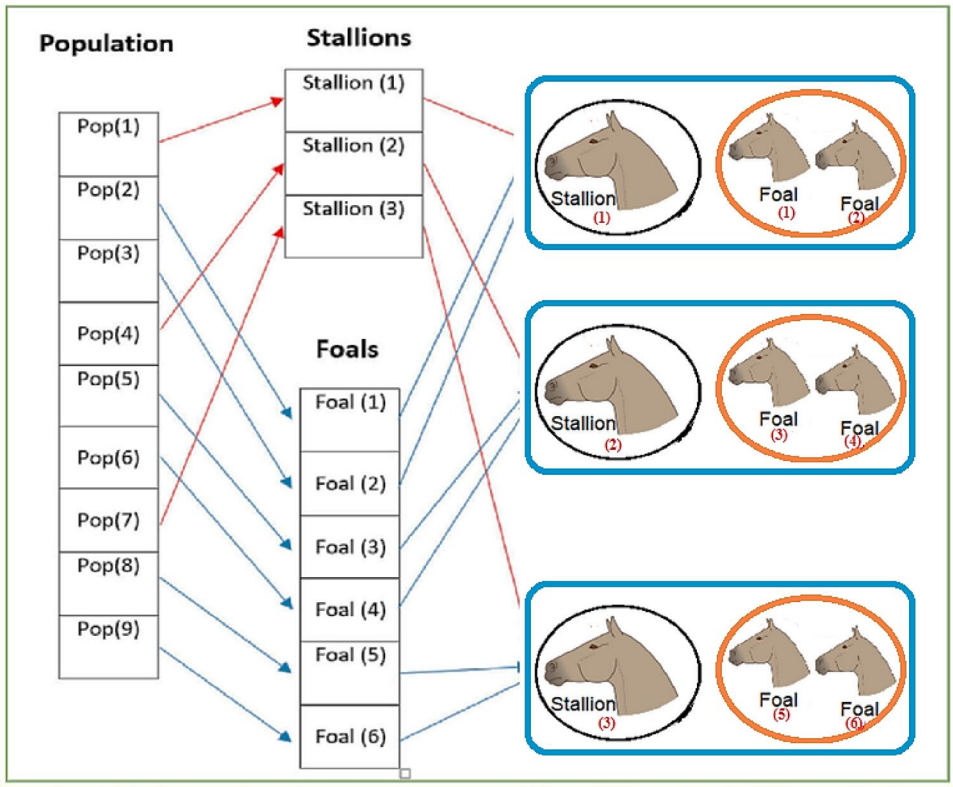

Fig. 2. Formation of groups from the main population.

Grazing behavior
As mentioned before, foals graze in close proximity to their herd for the majority of their life. To reproduce the grazing phase, we assume the stallion is positioned exactly in the center of the grazing area. Applying this formula will get other people to move.

$$X_{G,j}^{i} = 2Z\cos\left(2\pi RZ\right) \times \left(Stallion_{G,j} - X_{G,j}^{i}\right) + Stallion_{G,j} \tag{2}$$

where $X^{i}_{G,j}$ and $Stallion_{G,j}$ are the positions of the member of group i and the stallion in group j, respectively, R is a random number between −2 and 2, and Z is a matching parameter calculated by Eq. (3):

$$P = \vec{R}1 < TDR, IDX = (P == 0), Z = R2\Theta IDX + \vec{R}3\Theta\left(\sim IDX\right) \tag{3}$$

where P is a vector whose dimensions match the dimension of the problem, R1 and R3 are random vectors between 0 and 1, and R2 is a random number between 0 and 1. TDR, the linear reduction parameter, is obtained from Eq. (4).

$$TDR = 1 - \frac{t}{T} \tag{4}$$

where t and T are the current and maximum iterations, respectively.

Mating behavior
One of the ways that horses differ from other animals is that they separate their foals from their parent groups before they reach adulthood and mate. Equation (5) can be used to simulate the mating behaviour of horses.

$$\begin{aligned} &X_{G,k}^{p} = \text{Crossover}\left(X_{G,i}^{q}, X_{G,j}^{z}\right), i \neq j \neq k, q = z = \text{end} \\ &\text{Crossover} = \text{Mean} \end{aligned} \tag{5}$$

Horse q in group i and Horse z in group j make up group k, which includes the location of horse p. The crossover probability in the first WHO is fixed at a constant termed PC.

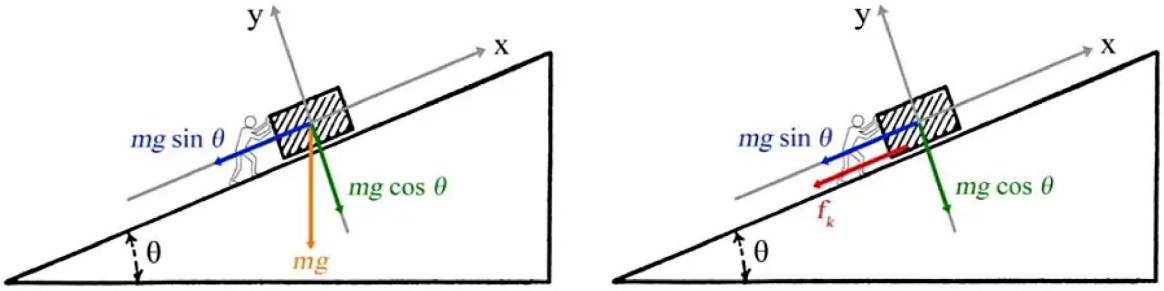

Fig. 3. The position of the object and the coordinate axis on the inclined surface and the forces acting on the object[35].

Group leadership
The leaders of the herd, known as stallions, direct the others to a good spot (a water hole). In order to force the dominant group to utilize the water hole, stallions, the group's leaders, will engage in combat for it as well. The following formula is used to replicate this behaviour:

$$\overline{Stallion}_{G,j} = \begin{cases} 2Z\cos(2\pi RZ) \times (WH - Stallion_{G,j}) + WHifrand > 0.5 \\ 2Z\cos(2\pi RZ) \times (WH - Stallion_{G,j}) - WHifrand \leq 0.5 \end{cases} \quad (6)$$

where $Stallion_{G,j}$ and $Stallion_{G,j}$ are the position of the candidate and the position of the current leader in group j, respectively, and WH is the position of the waterhole.

Exchange and selection of leaders
The leaders are initially chosen at random. Next, leaders are selected based on predetermined fitness levels. To simulate the change in the leader's standing among others, utilize formula (7):

$$Stallion_{G,j} = \begin{cases} X^i_{G,j}, iff\left(X^i_{G,j}\right) < f\left(Stallion_{G,j}\right) \\ Stallion_{G,i}, iff\left(X^i_{G,j}\right) \geq f\left(Stallion_{G,j}\right) \end{cases} \quad (7)$$

where $f(X^i_{G,j})$ and $f(Stallion_{G,j})$ are the foal and stallion fitness values, respectively.

Giza pyramids construction (GPC) algorithm

The Giza Pyramids Construction Algorithm is a new crowd-based meta-heuristic algorithm that draws inspiration from unique, historic resources that are controlled by laborers' movements and the moving of stone blocks up the ramp. Studying and reflecting on the objects left by the ancients can help us understand the strategies, technologies, and best practices of a bygone era. The recommended algorithm is controlled by the workers' movements and the way they put the stone blocks onto the ramp. Picture a building site where stone blocks are scattered about and the workers are assigned the responsibility of moving them to the designated spot for installation. In the initial step, you must decide where to begin and how much each block will cost. Moving the stone blocks to the installation site using a ramp is the second step. The friction and slope of the ramp influence the movement of the stone blocks. We next proceeded to determine the quantifiable elements. Figure 3 shows these measurable characteristics as a function of the weight force and the friction force.

The third stage of the algorithm checks to see if the laborers are continually shifting where they are to take control of the stone block. It is possible to rotate workers in order to balance their strength when lifting the stone block, considering the individual characteristics of each one. As a result, some workers will be let go, and others will take their positions. This replacement has an impact on the power balance and stone block moving mechanism. Algorithm 1[35] provides a pseudocode description of the GPC algorithm.

```
STEP 1:
    generate initial population array of stone blocks or workers (Population size);
    determine best worker as Pharaoh's agent;
  STEP 2: for i=1 to n do (all n stone blocks or workers)
    calculate amount of worker movement;
    estimate new position;
    investigate possibility of substituting workers;
   determine new position and new cost;
     if new_cost < Pharaoh's agent cost then
        set new_cost as Pharaoh's agent cost;
     end if
  END STEP 3
      Sort solutions for next iteration;
  END STEP 2
END STEP 1
```

Algorithm 1. GPC algorithm pseudocode.

Fuzzy logic technique

The three primary processes in the fuzzy logic technique are fuzzing the data, changing the membership values, and, if necessary, dephasing the output. Encoding the image data (fuzzification) and decoding the outcome (de-fuzzification) are the steps involved in fuzzification and de-fuzzification. These procedures make it possible to process photos using the fuzzy approach. The secure control model based on fuzzy T–S in the presence of DoS attacks reinforces the importance of developing mechanisms that are resilient to security threats. Also, the use of adaptive memory in event-driven actuators for controlling fuzzy T–S wind turbine systems plays a key role in improving the response in complex fuzzy systems, which is also applied in the intelligent selection of cluster heads in our work[35,36]. As a result, the most crucial phases that enable us to control cluster vertex selection using fuzzy approaches are encoding the input data (fuzzification) and decoding the outcomes (defuzzification), as seen in Fig. 4.

The middle stage, which involves changing the membership values also referred to as the intelligent step is where fuzzy clustering selection works best because it signifies the distinction between the approach and the other step. There are many different membership functions in fuzzy logic, and each one has a unique consequence. Gaussian, bell, trapezoidal, and triangle functions are among them. The method's efficiency is increased through the application of appropriate membership by fuzzy system inference.

Fuzzification is the process of converting data into a membership function (fuzzification phase) where the value may be readily changed using fuzzy logic technology. This allows the data to be utilized in a given range. This approach is sometimes referred to as fuzzy fusion, fuzzy rule-based approach, or fuzzy clustering approach. It takes a fuzzy system to locate uncertainty data. Fuzzy logic-based cluster head selection offers several benefits, such as:

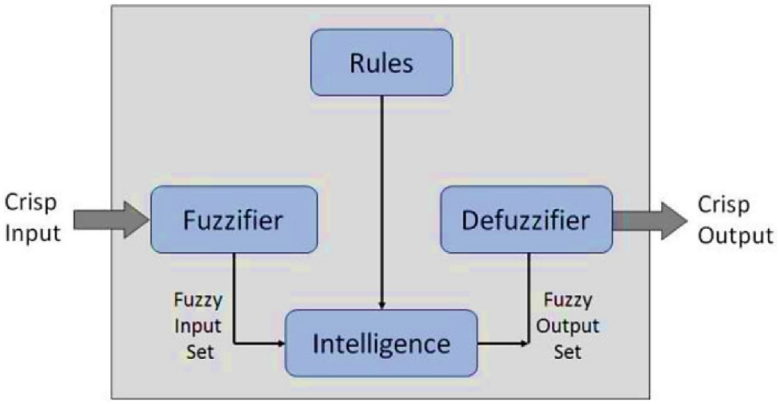

Fig. 4. Steps involved in Fuzzy CH selection[36].

a. The most common methods for expressing and processing the selection criteria for cluster head nodes are fuzzy techniques.
b. It gives us a mechanism to control network performance and energy usage.
c. Concepts of fuzzy logic handle uncertainty in WSN with ease.
d. Huge flexibility is offered by fuzzy logic.
e. Even with imprecise input, fuzzy logic works well.

Fuzzy logic is superior to other forms of logic because it considers structure when developing its understanding, whereas other forms of logic suffer from imprecision. Fuzzy set theory can give if–then rules, which are the basis for human reasoning that is recommended to be used in fuzzy rules[37].

Chaos mapping system

The study of dynamic systems that are very sensitive to beginning conditions is known as chaos theory in mathematics. The chaos of complex systems, basic patterns, repeating patterns, fractals, self-similarity, and self-organization are all present in chaotic systems. The science of forecasting the behaviour of "inherently unpredictable" systems is known as chaos theory, which provides an intriguing contrast.

Very basic, frequently noise-free systems experience chaos. Essentially, these systems are "deterministic" in the sense that their future behaviour can be predicted based on precise knowledge of the system's beginning conditions. Because of this, a bounded, noisy, non-periodic (or non-intermittent) oscillation can be described as chaos. Stated differently, a deterministic system exhibits random behavior even in the absence of random inputs. Chaotic behaviour, quasiperiodic oscillations, and subharmonics are among the unusual effects observed in unstable nonlinear systems.

Chaotic maps come in two varieties: continuous and discrete. These mappings of chaos may be simple or involve random real numbers. The primary function of any cryptographic algorithm is to generate random numbers[38]. Applications like digital signatures, hashing, encryption, seed vectors, One-Time Passwords (OTP), etc., require pseudo-random number generators[39]. These pseudorandom number generators are a subset of deterministic generators, meaning that their output is determined by the generator's design and the seed's beginning sequence[40]. Since the result can be fully predicted if the initial value is known, these numbers are not really random. Hardware random number generators and software seed-based random number generators are the two primary types of random number generators[41]. In this paper, a binary basis discrete-type chaos mapping is applied. In the information shift section, this mapping has been utilized to simulate a lightweight cryptography with unbounded repetition durations, as will be discussed in the following section.

Security in wireless sensor networks

WSNs are typically used in unsuitable areas, lack central management, and have erratic communication methods. Therefore, WSN security mitigation cannot be dependent on conventional IT network solutions due to the complexity and interconnectedness of a wide range of devices and protocols, as well as the variety of accessible routing protocols and services. Therefore, the security measures in place at the moment are insufficient. For devices with limited resources or power, low-cost encryption is an option, and there are a number of current developments and strategies that fall into this category, such as trust management and encryption methods that use lightweight approaches. Serious attacks, such as the injection of malicious or inaccurate routing information into the network, can also affect routing protocols and cause packet delays or loss as a result of routing interference. Several methods have been suggested to forestall routing assaults, including data correlation across numerous nodes and encryption Zero-sum game theory models for robust control against external disturbances reinforce the importance of formulating robust control policies in competitive or uncertain environments such as WSNs[42]. Also, the analysis of pre-determined time agreement with event triggering and privacy preservation in higher-order systems is consistent with the proposed approach in designing secure clustering and resource conservation in WSNs[43]. Security and performance are two competing criteria that must be balanced in any proposed protocol. Better performance against security level requires sacrificing low power consumption, processing, and storage utilization, and vice versa. One technique for guaranteeing the security of WSNs is key management.

It is defined as a collection of procedures and systems that support key distribution and uphold the standards of the keying process across nodes based on security policy. Cryptographic keys must be created, maintained, distributed, safeguarded, and used under strict control. Key management systems can be either static or dynamic because they can update keys in sensor nodes[44]. The hybrid model optimized with the ant colony algorithm highlights the importance of integrating graph and memory-based structures for intrusion detection in industrial IoT environments; a concept that is similarly pursued in the proposed lightweight and chaos-based security framework for WSNs[45]. Static key management makes a network more resistant to vulnerability assaults by keeping the encryption key in a hidden memory, identifying the principles of the keys before distribution, and keeping the keys unaltered for the entire network's operational life. Dynamic key management, on the other hand, involves frequent key updates in accordance with network policies. The energy needed to encrypt data at the sensor nodes is an issue with WSN encryption. The usage of lightweight encryption algorithms can eliminate this issue. Power consumption and encryption difficulty should interact in the network, though. As a result, this study set out to suggest a chaotic-based cryptography model that would have extremely low consumption and complexity. Table 2 provides a comprehensive list of notations used in this document along with their explanations.

Notation	Description
WSN	Wireless Sensor Network, a network of sensor nodes for data collection and communication
CH	Cluster Head, a node responsible for data aggregation and transmission to the base station
N–CH	Non-Cluster Head, nodes that communicate data to the cluster head
P	Target proportion of cluster heads in the LEACH protocol
Pi(t)	Threshold probability for node i to become a cluster head in round t (LEACH)
k	Number of cluster heads in the network (LEACH)
N	Total number of nodes in the network (LEACH)
r	Current round number in the LEACH protocol
Ci(t)	Indicator if node i has not been a cluster head in the current cycle (0 or 1)
TDMA	Time Division Multiple Access, a scheduling method for data transmission in clusters
G	Number of groups in the Wild Horse Optimization (WHO) algorithm
PS	Stallion ratio (G/N) in the WHO algorithm
XiG,j	Position of member i in group j (WHO algorithm)
StallionG,j	Position of the stallion (leader) in group j (WHO algorithm)
R	Random number between − 2 and 2 for grazing behavior (WHO)
Z	Matching parameter for grazing behavior in WHO, calculated using Eq. (3)
P	Vector matching the problem dimension (WHO)
R1, R3	Random vectors between 0 and 1 (WHO)
R2	Random number between 0 and 1 (WHO)
TDR	Linear reduction parameter for WHO, calculated using Eq. (4)
t	Current iteration in WHO or GPC algorithms
T	Maximum number of iterations in WHO or GPC algorithms
PC	Crossover probability in the WHO algorithm
WH	Position of the waterhole in the WHO algorithm
f(XiG,j)	Fitness value of a foal in group j (WHO)
f(StallionG,j)	Fitness value of the stallion in group j (WHO)
GPC	Giza Pyramids Construction, a meta-heuristic algorithm inspired by pyramid construction

Table 2. Abbreviations and explanations.

Suggested method

Two novel approaches to energy-efficient clustering and security in WSN are covered in this section. We have applied fuzzy logic, novel lightweight cryptography, and other meta-heuristic algorithm techniques in these approaches.

Clustering and cluster head selection

Wireless sensor network (WSN) clustering techniques are crucial for extending the lifetime of networks in a number of ways. Among deployed sensor nodes, clustering strategies in WSN choose the optimal cluster heads (CHs) based on computational power, energy consumption, and BS connectivity. Due to their larger workload which includes receiving messages from other cluster heads and cluster members, compiling all of the messages, and sending them to the base station with the assistance of non-cluster head nodes in the layered sensor network CH nodes use more energy than other sensor nodes. Consequently, the creation of an effective CHs selection algorithm is imperative. The flowchart for the energy-efficient information transfer approach is displayed in Fig. 5. Below is a discussion of this strategy's several phases.

Clustering based on meta-heuristic algorithms

At this point, the network is first clustered using two meta-heuristic algorithms proposed by the WHO and GPC methods. These algorithms are based on the number of nodes, their position, and the amount of energy left in the sensor nodes for each period of WSN execution. Two guiding ideas form the basis of this node classification. The number of nodes in each cluster and the distribution of energy are both balanced. The objective function's Algorithm 2 for this clustering is shown below.

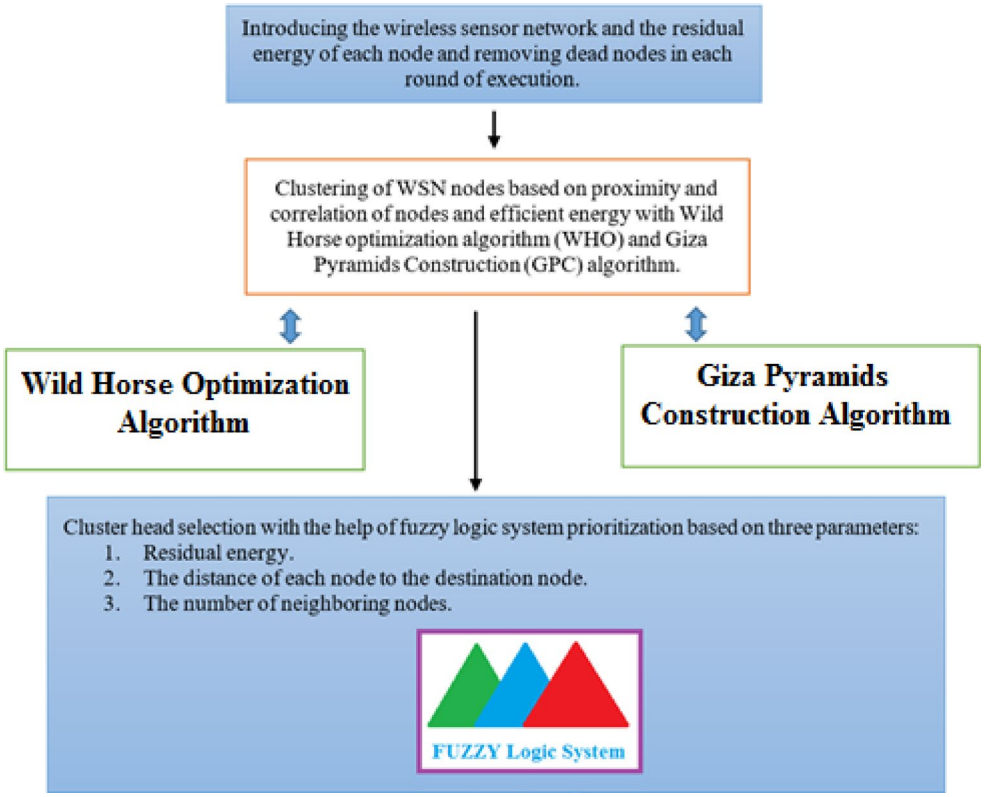

Fig. 5. Flowchart of the proposed strategy for clustering and cluster head selection.

```
function [output] = clusterfunction(x,nodearch,N,Numclass)
 x = round(x);
Dead = nodearch.dead;
x find Dead == 1 = 0;
E = [];
for i = 1: N
   E = [E, nodearch. node(1, i). energy];
end
E (find Dead == 1) = 0;
loc = nodearch.nodesLoc;
for j = 1:Numclass
   if sum(x == j)~ = 0
   NC (j) = numel(find(x == j));
   EC (j) = sum (E(find(x == j)));
   S(j) = (max(loc(find(x == j), 1)) − min(loc(find(x == j), 1))) ∗ (max(loc(find(x ==
   j), 2)) − min(loc(find(x == j), 2)));
   end
end
 NumaliveNode = N − sum(Dead);
                              output = sum(NC.∗ S) / 1e4 + sum((EC.∗ NC));
end
```

Algorithm 2. Clustering algorithm for WSN in the course.

In this pseudo code, NC is the number of nodes in each cluster, EC is the total energy set of nodes in each cluster, and S is the total area enclosed by each cluster. After defining the nodes in different clusters, we will enter the next step, which is choosing the cluster head for each cluster.

Cluster head selection

It is crucial to choose a reliable cluster head for wireless sensor network clusters. The cluster head node in each cluster is chosen using the following criteria in the suggested method:

- Residual energy: It means the remaining energy of each sensor node in the network. The more the remaining energy of a sensor node, the more chance it has for the cluster.
- Node neighborhood: This criterion is based on the number of neighboring nodes in each network node, whose distance is defined within the threshold range.
- In the proposed method, the higher the number of neighboring nodes, the higher the probability of selecting the node as the cluster head node. The neighborhood value is calculated using the following mathematical relationship:

$$\text{Neighborhood} = \sum N_{Di<=Ds} \tag{8}$$

where $N_{Di<=Ds}$ is the number of nodes in the distance less than the threshold distance Ds. This threshold value is equal to 30 meters for the studied network.

- The distance between the cluster head and the BS destination node: the smaller this distance is for a sensor node, the higher the chance of being a cluster head.

The fuzzy logic approach and established fuzzy if–then rules according to Table 3 are utilized to assess the nodes and control the uncertainty, since there are multiple criteria for selecting the cluster head. The cluster head is ultimately chosen from among the nodes with the highest probability value in the fuzzy prioritizing system, and all other nodes in each cluster are connected to the chosen cluster head. For fuzzy variables, this leads to the formation of fuzzy sets and clusters. Fuzzy input is displayed in Figs. 6, 7 and 8.

As previously stated, the likelihood of a cluster head is determined for every network node by integrating fuzzy sets and the fuzzy inference system of the specified if–then rules. The suggested approach makes use of Mamdani's fuzzy inference model. The inference process works as follows: the predefined rules are applied to each of the fuzzy sets through the membership functions after employing the cluster head selection criteria, fuzzification of the inputs, and establishing the degree of membership of the inputs and outputs. Every rule is then subjected to the implication procedure. Using the fuzzy "AND" operator as the minimum technique, the output fuzzy set is reduced in this article. The maximal approach (fuzzy "OR" operator) is used to aggregate the results of all the rules in order to reach a judgment. The result is ultimately defuzzified and transformed into a

Rule	PowerRemainder	SND	DegreeNeighborhood	priority
1	L	H	L	LOW
2	L	H	M	LOW
3	L	H	H	LOW
4	L	L	L	LOW
5	L	L	M	LOW
6	L	L	H	MID
7	M	H	L	LOW
8	M	H	M	LOW
9	M	H	H	LOW
10	M	M	L	LOW
11	M	M	M	LOW
12	M	M	H	MID
13	M	L	L	LOW
14	M	L	M	MID
15	M	L	H	HIGH
16	H	H	L	LOW
17	H	H	M	LOW
18	H	H	H	HIGH
19	H	M	L	LOW
20	H	M	M	MID
21	H	M	H	HIGH
22	H	L	L	LOW
23	H	L	M	MID
24	H	L	H	HIGH
25	H	H	H	HIGH

Table 3. Fuzzy rules for calculating the probability of a cluster.

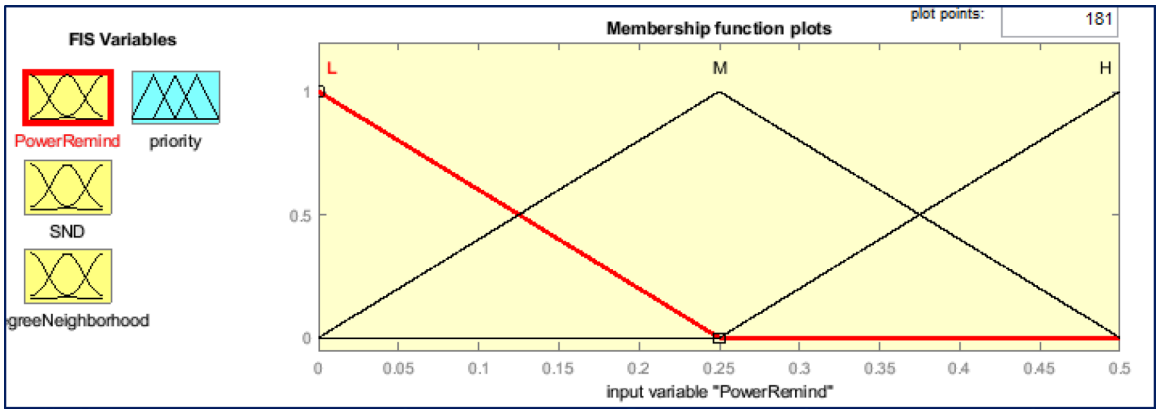

Fig. 6. Fuzzy set for residual energy fuzzy input variable.

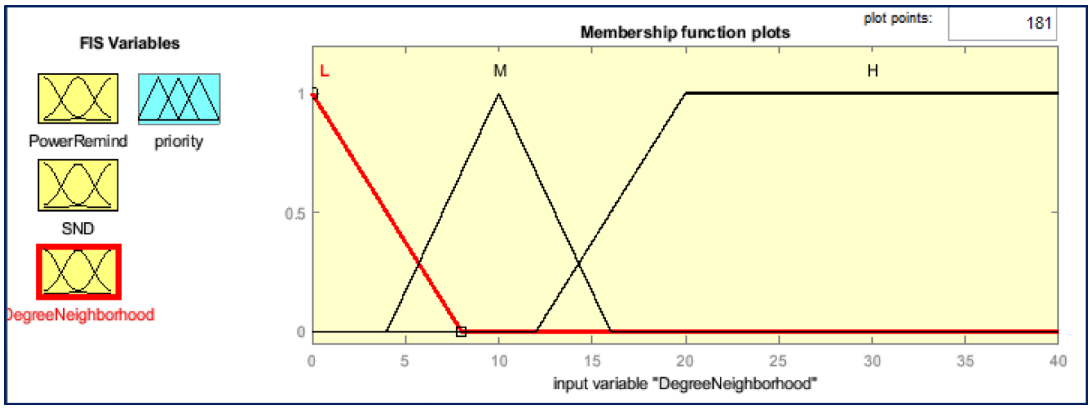

Fig. 7. Fuzzy set for neighbourhood fuzzy input variable.

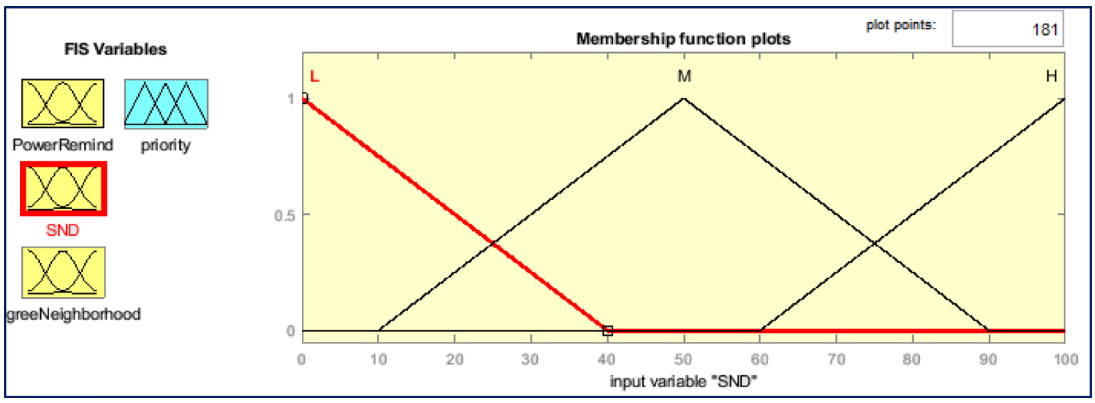

Fig. 8. Fuzzy set for fuzzy input variable distance from node to BS station.

numerical number using the centre of gravity approach. This gives the probability value of the node that will be chosen as the cluster head. In a fuzzy system, every fuzzy rule is evaluated concurrently and simultaneously. When a rule's input matches an issue, the rule is activated and computations are carried out. Fuzzy sets and fuzzy variables are used in probability analysis, as seen in Fig. 9. We take into consideration the set of values "low, medium, high" for this output variable.

Based on the cluster topology and the fuzzy selection cluster heads, non-cluster nodes are produced in each cluster after the cluster heads are selected. The fuzzy technique is used to select the best cluster heads, as previously stated. A network's topology can be constructed and its performance assessed using the objective function stated in the pseudo-code 2 algorithm by determining which nodes in the cluster are at the head of each

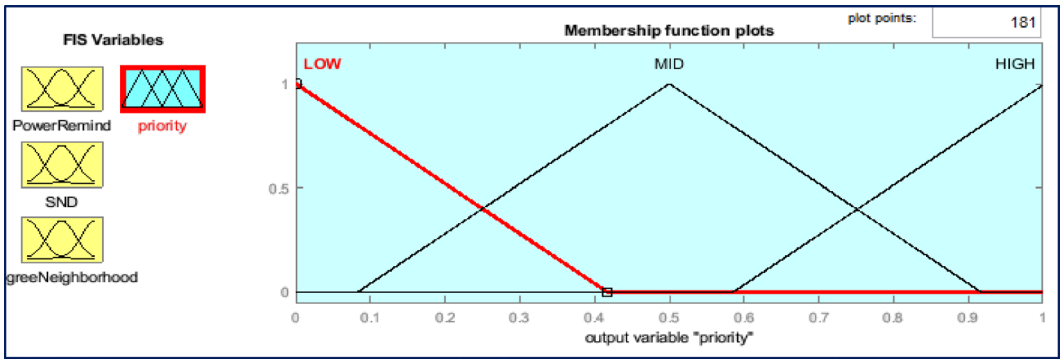

Fig. 9. Fuzzy set for the output fuzzy variable of cluster head chance.

execution round. At the end of each period, this process has spread energy and scattered nodes in clusters. The above objective function can be minimized by selecting the most appropriate cluster heads and, in turn, the most appropriate network topology, based on the average distance between the nodes in a cluster and the cluster head.

The remaining energy criteria of the node, the members' minimal distance from the cluster head (neighbourhood), and the distance to the base station are employed in the cluster head selection step. The distance between the sensor node and the base station is computed using the Euclidean distance formula. A sensor node has a greater chance of being chosen as a cluster head the closer it is to the base station. The fuzzy set of the input fuzzy variable for the base station's distance is displayed in Fig. 8. The computation of the cluster head formation value is achieved by merging the fuzzy sets of input variables with the fuzzy inference system of if–then rules specified in Table 3. In every next round, clusters are formed and structured accordingly. Fuzzy cluster head selection is the next process. A coefficient of $1 < P$, calculated similarly, corresponds to the number of clusters in each era. As the cluster head, each node conducts independent data transfer during the final stages, with the clustering process not being carried out for any number of nodes less than P.

Security

In wireless sensor networks, secure data aggregation is required to lower data transmission volumes and lengthen network lifetimes. Most wireless sensor nodes provide the basis of larger industrial Internet applications. Any types of real-time Internet of Things application can sense data using built-in sensors. Sensors in the physical world operate with minimal power consumption to carry out tasks including data processing, communication, and sensing. To increase network longevity and sensor node energy efficiency, a lot of research is being done. Encrypting data in sensor nodes is a safe transmission technique in WSN, although it shortens node lifetimes because of the limited power of sensors. Thus, we aim to increase information security and minimize power losses due to encryption in nodes by offering a lightweight encryption based on XOR repeating loops and chaotic shifts.

Wireless sensor networks (WSN) are primarily used for the purpose of gathering different kinds of data, such as traffic and weather data. The majority of the data transmitted in digital communication applications differs from the data gathered in WSNs. WSN data typically consists of only a few informational bits, whereas data communication applications typically contain several informational bits. The key size of these traditional encryptions is far larger than the data size; hence it is evident that they are not appropriate for WSNs. As a result, in this study, a very basic hardware encryption of 8 bits is used, and a very sophisticated decoding scheme based on pseudo-chaos models is employed.

To create an encrypted image, a new pseudo-chaotic mapping that can be implemented with minimal hardware is presented in this section. This mapping uses a unique key code in binary basis and is entirely random to alter the pixels of various images as sensor information. The encryption system in this work is first configured to receive pixel information as bytes 0 through 255. Next, using the sensor node's key, the XOR operator on each pixel's data is detected, and the output for the following step is moved to the right by the number of ones in it. By altering the encryption key and the data, the pseudo-chaotic nature of this encryption is introduced. The number of shifts for each 8-bit data will differ, and no one is certain how many shifts there will be for any given data. These two stages of encryption are performed by the number of ones in the bits of the cipher key in a repetition loop.

The proposed design's flowchart is displayed in Fig. 10. This flowchart is displayed as a cascade with two sections dedicated to encryption and combined information decoding using the xor operator and automatic chaos shift register mapping. Increasing the number of stages will increase the size of the hardware program and these two stages will meet the objectives of the complexity of the task. To illustrate how encryption works, we'll look at an example in this section. At first, the input data and password are introduced with the values 11001110 and 00000011. After performing XOR, we have: 11001101 and the number of ones in the data, which is equal to 5, the right shift operation is performed. The resulting result is equal to: 01101110. This operation is repeated twice as many as there are ones in the password key. Here are the outcomes: After applying the XOR operation, the output will be 01101101 with a rightward shift of the data value equal to 5: 01101011, representing an entirely different numerical representation of the input data. The important point in this method is that for each different data, the encryption method for the same key will be completely different.

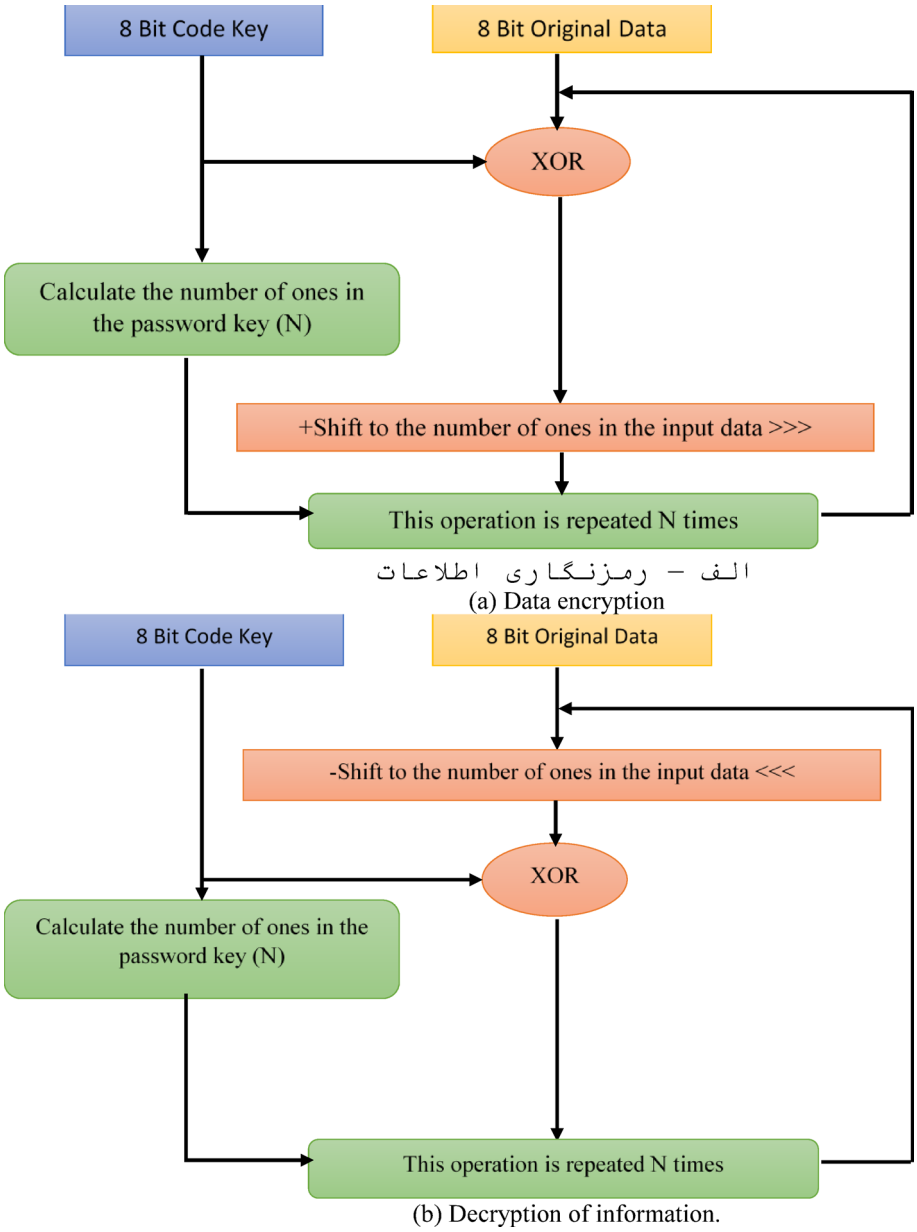

Fig. 10. Flowchart of suggested lightweight cryptography techniques (**a**) Mixed cryptography process. (**b**) Decoding process.

As shown in Fig. 10, no additional encryption is added to the key part, and only encryption of the original data is sufficient. The reason for this is due to the hardware and energy constraints in WSN, which made us skip key encryption.

Results and discussion

Using MATLAB 2019b, an algorithm simulation for typical tests, such as original picture, entropy image, and histogram, was carried out on an Intel Core I5-M480@2.67 GHz CPU. While code and RAM are measured in bytes, block and key sizes are determined in bits. Cycles comprise encryption and decryption in addition to key expansions.

The findings in Fig. 11 demonstrate that accurate decoding is only achievable if the right key is applied to the image; otherwise, the image cannot be correctly decoded. Since the incorrect key differs from the original key by just a small amount in the experimental visual representation of the photos, the algorithm's strength can be inferred from this outcome. Two widely-used 8-bit grayscale photos have been selected for the entropy and histogram tests. Also, an indicator of strong security is the uniform distribution of intensities following encryption, as seen in the histogram results for the original and encrypted image in Fig. 12. Maximum entropy of 8 bits can be obtained for an 8-bit grayscale image. An aspect of the technique is demonstrated by the fact that, as can be observed from Table 4's data, the entropy of all encrypted photos is approaching the maximum.

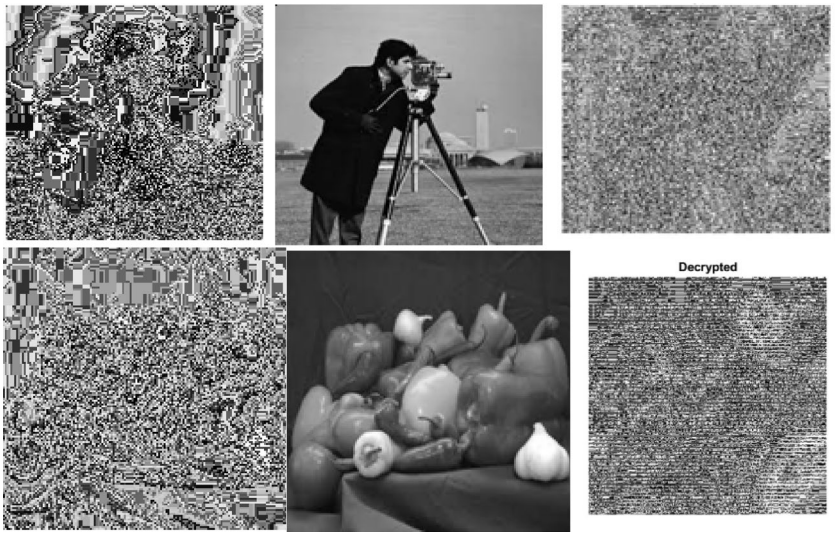

Fig. 11. (**A**) Image encryption. (**B**) decryption. (**C**) key sensitivity (camera man and Pepper).differential cryptography.

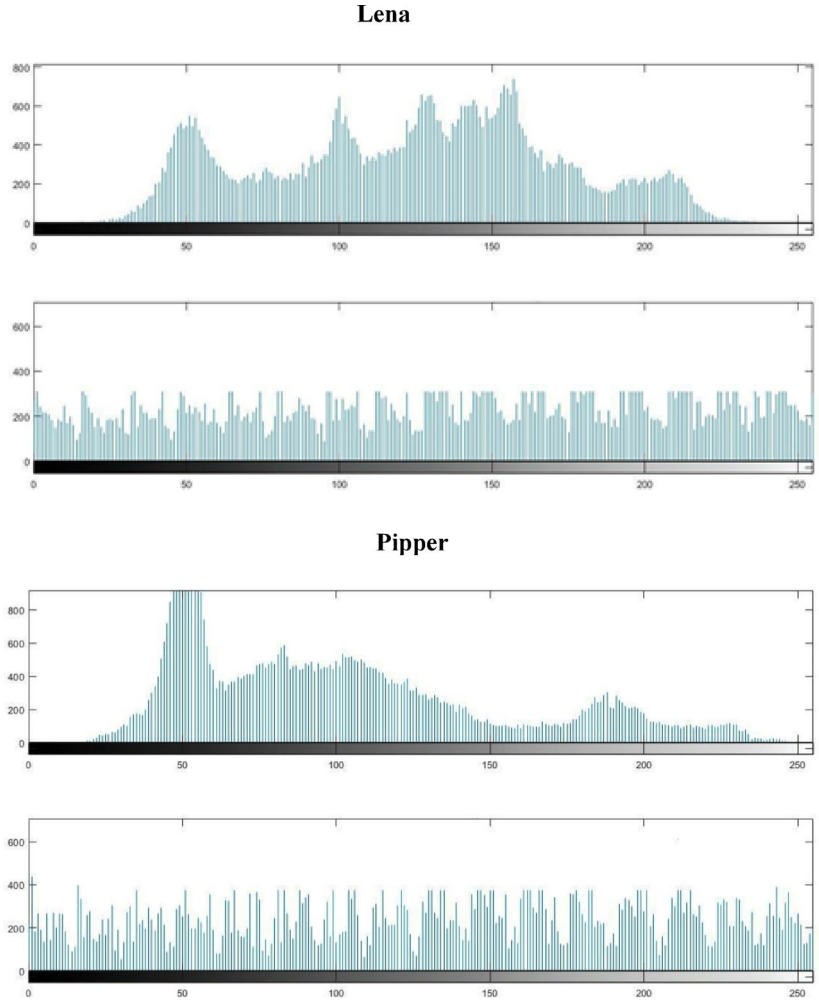

Fig. 12. Histogram comparison.

Image	Size	Correlation		Entropy	
		Original	Encrypted	Original	Encrypted
Lena	256 × 256	0.9744	− 0.0265	7.4509	7.8637
Pipper	256 × 256	0.9875	− 0.0121	7.3414	7.8486

Table 4. Results for correlation and entropy.

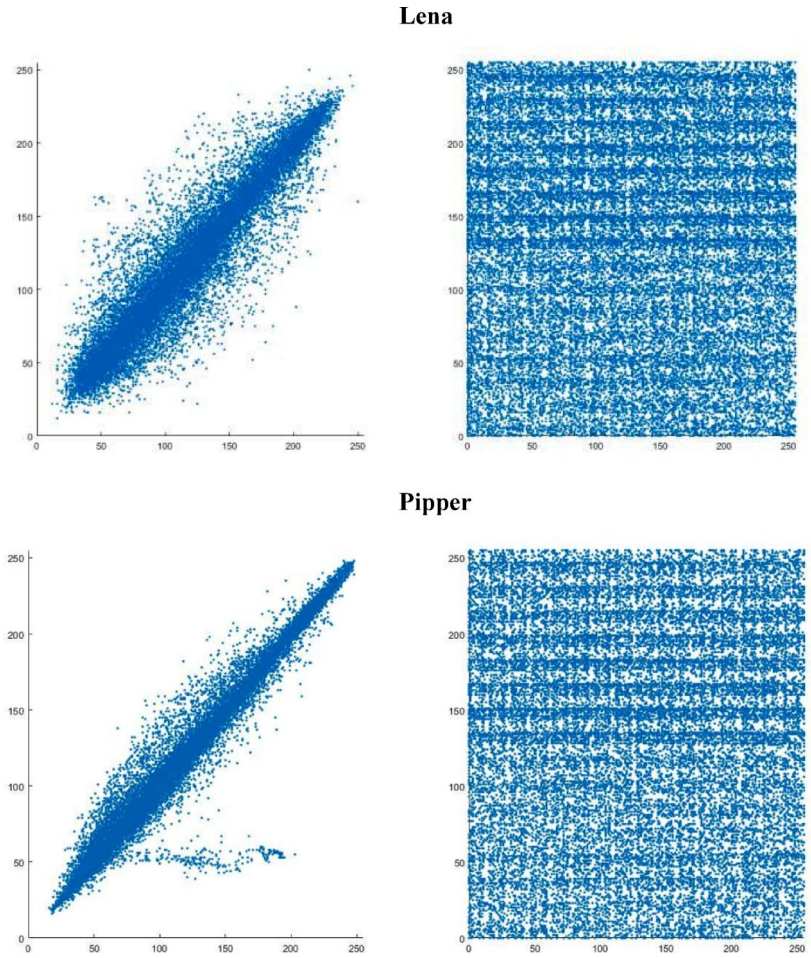

Fig. 13. Correlation comparison.

Figure 13 concludes the discussion by comparing the original and encoded data through correlation. Images included in the original data set exhibit strong correlation and keep the correlation coefficient at a high value in this study. On the other hand, it appears that the encrypted image is unrelated to the other one.

Performance analysis

A variety of commonly used tests are employed to assess the statistical and security measures of cryptographic systems, as well as the performance of the proposed scheme. These standards are outlined and examined in the sections that follow.

Histogram analysis

A histogram can be used to display all of the repeated numerical values in a picture. An image's histogram should not have sharp peaks, but rather a uniform distribution. Higher encryption efficiency and security are indicated by the histogram's uniform distribution of an encrypted image. The histogram view of two encrypted photos using the suggested method is displayed in Fig. 12.

Correlation analysis of adjacent pixels

One important metric to show the features of confusion in a cipher image is the correlation between adjacent pixels. In this work, 3250 pairs of randomly adjacent horizontal and vertical pixels from both the plaintext and

cipher text versions of an image were analysed. The following formula can be used to calculate the correlation mathematically:

$$r_{xy} = \frac{E\left(\left(x - E\left(x\right)\right)\left(y - E\left(y\right)\right)\right)}{\sqrt{D\left(x\right)D\left(y\right)}} \tag{9}$$

$$E\left(x\right) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D\left(x\right) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E\left(x\right)\right)^2$$

where x and y represent the grayscale values of adjacent pixels, and E(x) is the expected mean value. The range of the correlation coefficient is − 1 to 1, where 1 represents the exact similarity between two pixels or images. To get maximal uncorrelated pixels, or highly random values, a value around zero is required. Figure 13 displays the visual results of the correlation of the grayscale images analysed. The pixels in these images are directly related, and they can be cleaned and displayed in exchange for their encrypted image, which is dispersed across the image.

Analysis of homogeneity, energy and contrast

In this system, the homogeneous analysis can be employed to ascertain the proximity of GLCM (grey-level co-occurrence matrices) elements. The statistical mixes of pixel brightness or grey levels are represented by GLCM tables. A low homogeneity value indicates that the encryption technique is working well. The following can be calculated mathematically:

$$H = \sum_{x,y=1}^{M} \frac{g\left(x,y\right)}{1 + \left|x - y\right|} \tag{10}$$

Thus, in GLCM, g(x,y) represents the grey level concurrency matrices. The difference in brightness or colour that allows viewers to discriminate between several things in an image is known as contrast. Through contrast analysis, the intensity difference between neighbouring pixels in the entire image can be computed. Higher contrast levels, which reflect the cipher text image's degree of randomness, are indicative of increased security. The following is a mathematical expression for contrast:

$$\text{Contrast} = \sum_{i,j=1}^{M} \left|x - y\right|^2 p\left(x,y\right) \tag{11}$$

where p(x, y) represents the grey level co-occurrence matrices in GLCM.

Another quantity that can be computed using GLCM is energy. The energy analysis in this instance measures square elements. The following is the mathematical formula for calculating energy:

$$\text{Energy} = p\left(x,y\right)^2 \tag{12}$$

where the simultaneous grey level matrices are indicated by p(x, y). Table 5 contrasts the three aforementioned features of the pepper image with two references[46].

Analysis of differential attacks

One of the most important characteristics of an encryption algorithm is its resistance to differential assaults. Two tests that can determine resistance to differential attacks are the Unified Average Changing Intensity and the Number of Pixels Changing Rate tests. Below is an explanation of the particulars of each of the previously described tests, which were carried out on two encrypted images that differed by one pixel from the matching plaintext images.

References	Homogeneity	Energy	Contrast
[45]	0.9455	0.2133	0.2219
[46]	0.4644	0.0210	7.7123
This work	0.4356	0.0184	9.1621

Table 5. Available results from homogeneous, energy and contrast analysis.

Images	NPCR values	UACI value
Lena	**99.5605**	**25.9421**
Pipper	**99.5178**	**30.8122**
[47]	99.60	33.55
[47]	99.60	33.41

Table 6. Comparison of NPCR and UACI values.

References	MSE values	PSNR values
Lena	**11,574.97**	**17.2592**
Pipper	**10,470.67**	18.2619
[48] Lena	4859.03	25.9394
[48] Pipper	7274.44	21.9047

Table 7. Comparison of average values of MSE and PSNR.

Number of pixels changing rate (NPCR)
The NPCR test can determine how many changing pixels there are in two plaintext images if there is a MINUTE pixel difference. The following is the NPCR formula in math:

$$NPCR = \frac{\sum_{i,j} D\left(i,j\right)}{M \times N} \times 100\% \tag{13}$$

In the event when two cipher text pictures have the same value, D(i,j) = 0, but in the other scenario, D(i,j) = 1. The maximum NCPR number is 100%; nevertheless, an effective encryption system should have an NCPR value greater than 99.5%.

Unified average changing intensity
When there is a pixel difference between two images (one plaintext and one cipher text), the UACI test can be used to calculate the average intensity of the change. The following is the UACI equation:

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1\left(i,j\right) - C_2\left(i,j\right)|}{255}\right] \times 100\% \tag{14}$$

There is a single pixel difference between the plain text pictures in the encrypted images C_1 (i, j) and C_2 (i, j). The values of NCPR and UACI are displayed in Table 6. The values of the suggested scheme are contrasted with[47], as Table 6 illustrates. Compared to contemporary and conventional cryptographic systems, the suggested cryptographic scheme offers significantly higher security.

Pixel inconsistency analysis

Mean square error
The mean squared error (MSE), which measures the mean squared error between two images, can be used to study the avalanche effect. Every time the plaintext picture or key is slightly altered, this security technique demands a significant alteration to be made to the encrypted image. The following is the mathematical representation of MSE:

$$MSE = \frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{n}\left(X\left(i,j\right) - Y\left(i,j\right)\right)^2 \tag{15}$$

where W and H are the image's dimensions and X and Y are a group of encrypted images, each with a single bit different in the key. A strong encryption system ought to have a high MSE measured value. The MSE test is performed on the three pictures that were examined. Table 7 shows that, even when compared to the most advanced cryptographic systems, the suggested solution is extremely safe because of the higher value it acquired.

Peak signal-to-noise ratio (PSNR)
It determines the ratio between the two sets of pixel values by comparing the original and encrypted versions of the image. The encoded image is utilized as the noise and the plain text picture as the signal when calculating PSNR. The following formula can be used to calculate PSNR:

$$PSNR = 10 \times \log_{10}\left(\frac{255 \times 255}{MSE}\right) \tag{16}$$

where MSE is the mean square error value. A lower PSNR is advantageous to an encryption technique since it indicates that there is a considerable difference between the original plaintext image and its encrypted version. All three of the study's photos underwent the PSNR test. Based on Table 7, the average of these data indicates that the designed encryption system performs much better than the existing encryption methods, and it is better than the values obtained by[48].

Table 8, which compares the three photos investigated with a reference simulated in MATLAB software, indicates that this work is quite fast in terms of encryption time.

Simulation results of clustering protocols

The set of results below is related to the simulation of three LEACH protocols and the proposed algorithm with GPC and WHO methods. The number of clusters defined in this research is equal to P = 10.

The performance of the objective function

In this study, node dispersion and energy dispersion are optimized simultaneously with clustering as the goal of the objective function. Whereas the latter guaranteed each cluster's average energy for high residual energy, the former reduced each node's distance from other nodes within each cluster. The optimization value of the objective function for each algorithm during the first period is displayed in Fig. 14, where the WHO protocol performed better than the other algorithms by reaching the final value at a good rate of convergence.

In terms of clustering, this work compares and evaluates the performance of two popular optimization algorithms: the Giza Pyramid Construction (GPC) algorithm and Wild Horse Optimization (WHO). We tried the suggested techniques with Matlab R2019b. The evaluation process made use of several significant parameters, including residual energy, throughput, number of active nodes, and fitness function. Next, the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol was compared with the best-performing method. According to the simulation results, the wild horse algorithm outperforms the other method in terms of exploration and exploitation as well as two additional criteria (energy dispersion and node dispersion). The suggested fuzzy logic system is then used to assist in choosing the cluster head.

As seen in Fig. 15, the simulations were run on a network consisting of 100 and 30 sensor nodes placed in a field measuring 100 by 100 m. This can lower the energy dissipation of sensor nodes and greatly increase the rate of data transfer. Every period, the cluster heads were chosen. When the energy level of the current cluster head drops below a particular threshold, it is known as the period duration. As such, the decision was not made in a single optimization. The population of the algorithms and the number of iterations were set at 20 and 100, respectively, in this work. Table 9 displays the parameters utilized in the simulation.

Here, we compared the results of the WHO and GPC algorithms with those of the LEACH algorithm on the wireless network energy consumption model, looking at metrics like dead nodes, number of packets sent, and remaining energy. Important aspects of the LEACH protocol, including its concept and goal, its operational and process structure, and its routing category, are shared with other algorithms. Their shared goal is to disperse the substantial energy loss in communication with the BS to every sensor node in the network by rotating sensor nodes as cluster heads. In other words, they make sure that their energy consumption is balanced, rotate the role of CH, and choose a new cluster head for each cycle. The operational procedures and structure of the WHO, GPC, and LEACH methodologies dictate how often they function. Clustering and cluster head selection comprise the two phases of each period. First, clusters are assembled, and then, during the cluster head selection phase, data is transferred. Furthermore, each topology describes the energy dissipation through electronic components including the transmitter, power amplifier, and receiver using a basic radio model[50–52].

All three WHO, GPC, and LEACH methods fall into the same active routing protocol category (centralized, resource-oriented) in terms of routing. Both of them employ a link-mode routing protocol, in which every node ascertains the network topology and channel conditions before transmitting the information to a central location, which then computes a routing table for every network node[53]. Furthermore, by using hierarchical protocols for data communication, the network may achieve reliable operations while saving nodes' energy[54].

In summary, the performance of the proposed optimization algorithms was compared with the LEACH method due to the following primary advantages:

- The clustering of the LEACH protocol reduces the energy needed for transmission between sensor nodes and base station and prolongs the network's lifetime.
- By lowering locally correlated data, CH data aggregation significantly reduces energy consumption.
- The nodes in the network enter a state of sleep. Cluster collisions are prevented as a result, and the sensor node's battery life is extended.

Image	Size	Total ENC/DEC (s)	
		This work	[49]
Lena	256 × 256	4.73/4.65	5.0388
Baboon	256 × 256	4.12/4.32	4.6078
Panda	256 × 256	4.26/4.45	4.7363
Pipper	256 × 256	4.83/4.91	6.0214

Table 8. Analysis of the execution time of the proposed algorithm and comparison with the reference [49].

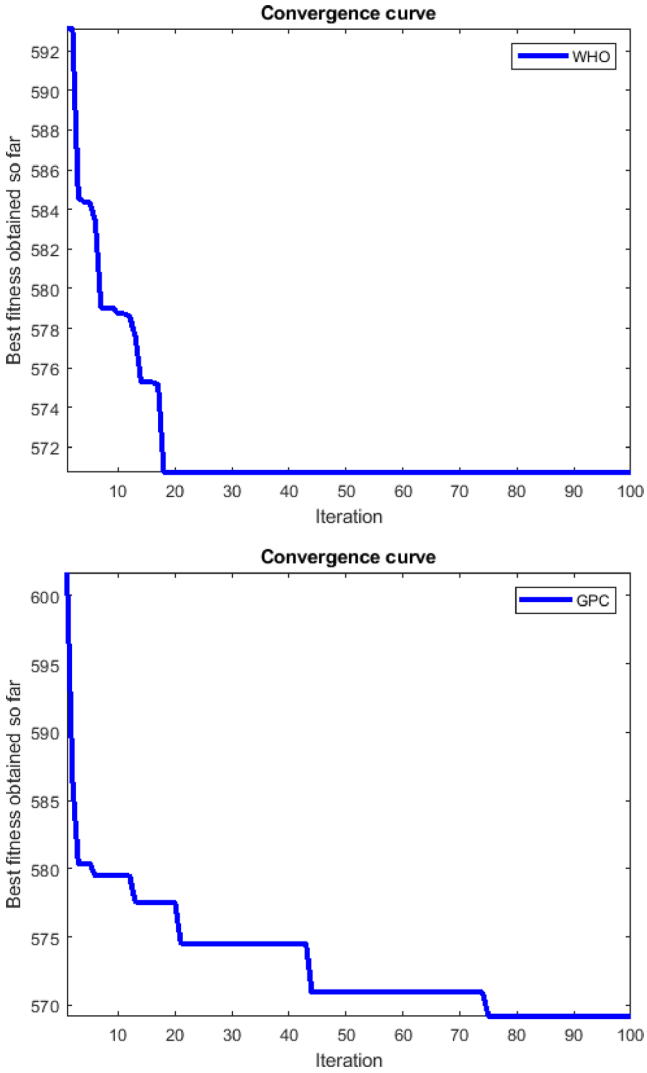

Fig. 14. Showing the performance of algorithms for cluster optimization in the first round.

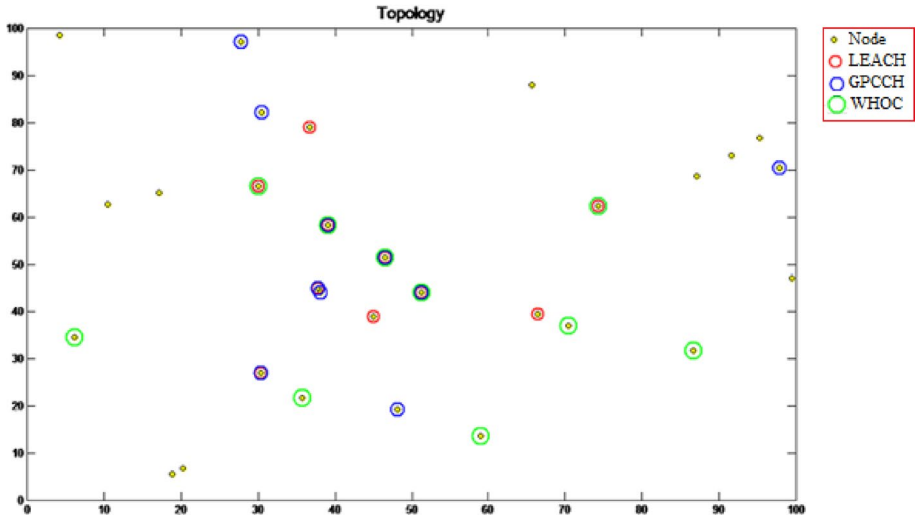

Fig. 15. Cluster head selection in WSN through WHO, GPC, LEACH for the first round.

Parameters	Value
Population size	100,30 sensor nodes
Deployment area	100×100 m^2
The location of the sink	50,50
Initial energy for each node	0.5 J
The energy transmission	50 nJ/bit
The energy receiver	50 nJ/bit
E_{MP}	0.0013 pJ/bit/m^4
E_{FS}	10 pJ/bit/m^2
E_{DA}	5 nJ/bit/packet
E_{elec}	50 nJ/bit
Search agent	5
The number of generations	10,000
Size of packet (K)	4096 bits

Table 9. Network simulation parameters.

- Every sensor node in the LEACH protocol has an equal chance of becoming a CH at least once. This random rotation of the CH lengthens the network lifetime.

Here, we compared the results of the WHO and GPC algorithms with those of the LEACH algorithm on the wireless network energy consumption model, looking at metrics like dead nodes, number of packets sent, and remaining energy. Important aspects of the LEACH protocol, including its concept and goal, its operational and process structure, and its routing category, are shared with other algorithms. Their shared goal is to disperse the substantial energy loss in communication with the BS to every sensor node in the network by rotating sensor nodes as cluster heads. In other words, they make sure that their energy consumption is balanced, rotate the role of CH, and choose a new cluster head for each cycle. The operational procedures and structure of the WHO, GPC, and LEACH methodologies dictate how often they function. Clustering and cluster head selection comprise the two phases of each period. First, clusters are assembled, and then, during the cluster head selection phase, data is transferred. Furthermore, each topology describes the energy dissipation through electronic components including the transmitter, power amplifier, and receiver using a basic radio model[50–52]. All three WHO, GPC, and LEACH methods fall into the same active routing protocol category (centralized, resource-oriented) in terms of routing. Both of them employ a link-mode routing protocol, in which every node ascertains the network topology and channel conditions before transmitting the information to a central location, which then computes a routing table for every network node[53]. Furthermore, by using hierarchical protocols for data communication, the network may achieve reliable operations while saving nodes' energy[54].

In summary, the performance of the proposed optimization algorithms was compared with the LEACH method due to the following primary advantages:

(1) The clustering of the LEACH protocol reduces the energy needed for transmission between sensor nodes and base station and prolongs the network's lifetime.
(2) By lowering locally correlated data, CH data aggregation significantly reduces energy consumption.
(3) The nodes in the network enter a state of sleep. Cluster collisions are prevented as a result, and the sensor node's battery life is extended.
(4) Every sensor node in the LEACH protocol has an equal chance of becoming a CH at least once. This random rotation of the CH lengthens the network lifetime.

The performance of the WHO, GPC, and LEACH algorithms is displayed in Fig. 16 along with the total number of sent packets, dead nodes, and energy left in the network after a certain number of rounds. Compared to other topologies, the WHO algorithm performed better. These findings come from a simulation with 100 sensor nodes. The network's lifetime during the time interval (0, 815) is displayed in Fig. 16a. The nodes submitted roughly 2380 packets to the WHO algorithm, as seen in Fig. 16b. The WHO algorithm outperforms the others by a wide margin, according to the performance comparison. Based on the initial node death time in various protocols, the WHO algorithm outperformed the LEACH technique. Furthermore, the last node in the LEACH method perished earlier than the last node in other methods, as illustrated in Fig. 16b. Furthermore, the WHO algorithm had a far longer lifespan than the LEACH approach. The network throughput for the protocols is plotted against the number of rounds in Fig. 16c. By preserving the nodes' remaining energy, clustering in the WHO algorithm extended the network's lifespan. As Fig. 16c illustrates, the WHO algorithm had a higher throughput than the LEACH approach.

Strength of Network Lifetime: The WHO algorithm extends the network lifetime significantly, with the first node death at 378 rounds, half of the nodes at 987 rounds, and the last node at 1415 rounds (Table 10), outperforming LEACH (213, 575, 1089) and GPC (254, 775, 1267). This strength is due to WHO's optimized cluster head selection, which prioritizes nodes with higher residual energy, combined with fuzzy logic for balanced energy distribution. This approach minimizes energy depletion, ensuring prolonged network operation, critical for WSNs in resource-constrained environments.

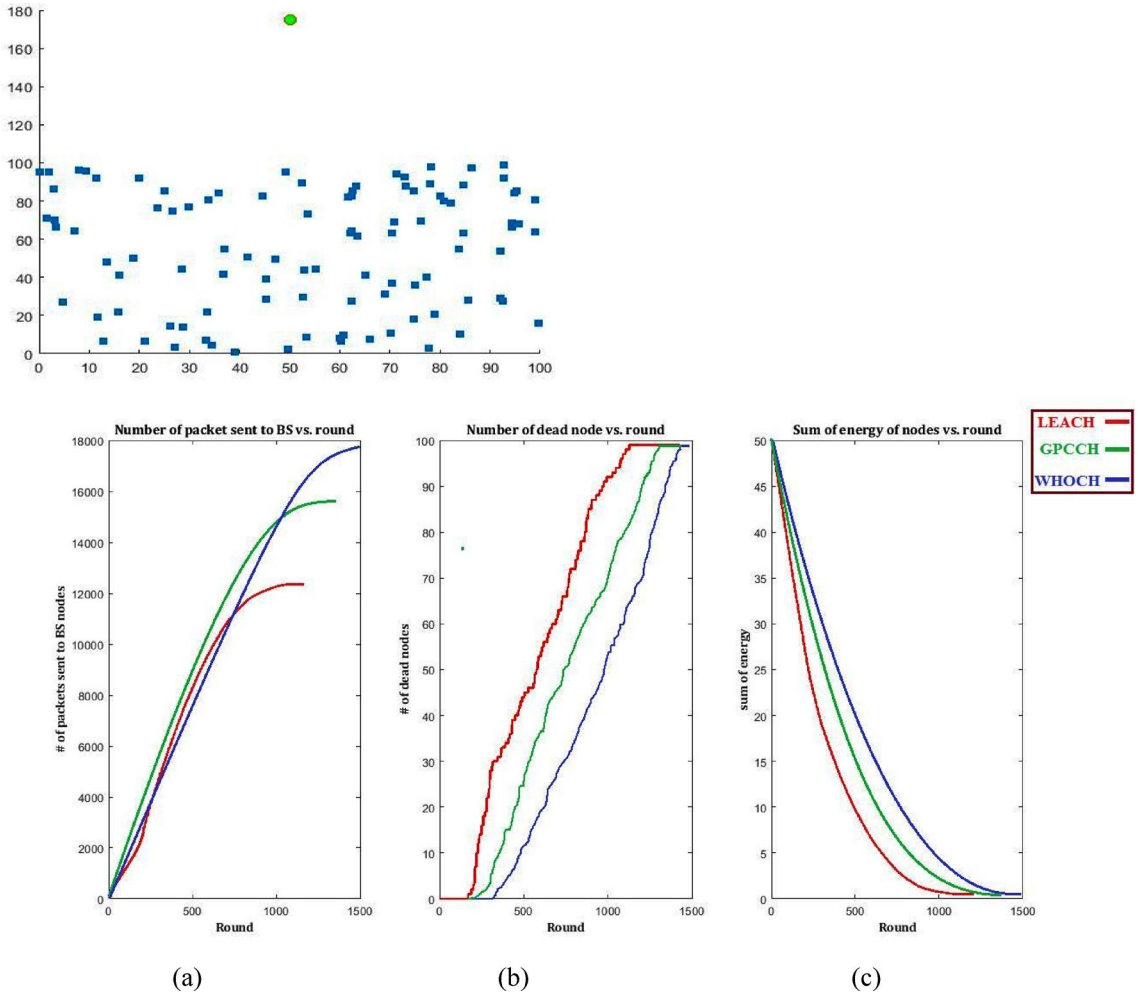

Fig. 16. Number of rounds vs number of live nodes in WHO, GPC and LEACH.

Method	death of first node (round)	death of half of the nodes (round)	death of the last node (round)	Execution time (seconds)
LEACH	213	575	1089	874
GWOCH	241	583	1153	1834
WOACH	223	632	1287	2014
GPCCH	254	775	1267	1954
WHOCH	378	987	1415	2131

Table 10. Comparison of the methods performance.

Strength of Number of Sent Packets (Throughput): The WHO algorithm achieves higher throughput, sending approximately 2380 packets (Fig. 16b), compared to LEACH and GPC. This strength results from WHO's efficient clustering, which reduces intra-cluster distances and optimizes data aggregation, allowing more packets to be transmitted before nodes deplete their energy. The fuzzy logic-based CH selection further enhances data transfer efficiency, making WHO ideal for high-throughput WSN applications.

Strength of Remaining Energy: The WHO algorithm preserves more residual energy (Fig. 16c) due to its meta-heuristic optimization, which balances energy consumption across nodes. By selecting cluster heads with higher energy and minimizing transmission distances, WHO reduces energy dissipation in communication with the base station. This efficient energy management, supported by fuzzy logic, ensures that nodes remain operational longer, enhancing WSN reliability.

Table 10 displays the calculation time and the death time of the nodes (the first node, half of the nodes, and the last node) so that the efficiency of the methodologies can be better understood. Clearly, the suggested approaches have the longest execution time, whereas the LEACH method has the shortest. The proposed method's implementation has the highest computational overhead, according to this table's data. Fuzzy logic methods

find optimal solutions with higher temporal complexity, which means the proposed method's performance is justified.

To expand the comparative evaluation, the proposed approach in Table 10 was also compared to recent meta-heuristic approaches (such as Grey Wolf Optimization, Whale Optimization). The comparison results show that the WHO algorithm has been able to achieve very good results compared to other methods.

Conclusion and future work

This study proposes a hybrid approach for wireless sensor networks (WSNs) that integrates the Wild Horse Optimization (WHO) algorithm, Giza Pyramids Construction (GPC) algorithm, fuzzy logic, and chaos-based lightweight cryptography, significantly outperforming traditional protocols like LEACH. The proposed strategy achieves a 53.75% and 14.73% increase in network lifespan compared to LEACH and GPC, respectively, by optimizing cluster head selection based on residual energy, node dispersion, and fuzzy logic-driven criteria, ensuring balanced energy consumption. Additionally, it delivers higher throughput, with approximately 2380 packets sent, due to efficient clustering and data aggregation. The chaos-based cryptography provides robust security with high entropy (close to 8 bits), low correlation (near zero), and strong resistance to differential attacks (NPCR > 99.5%), all while maintaining low computational overhead suitable for resource-constrained WSNs. Unlike LEACH, which relies on random cluster head selection and lacks advanced security, this approach enhances energy efficiency, network longevity, and data protection. Future work will explore multi-objective optimization using artificial neural networks and advanced key distribution strategies to further strengthen WSN security and performance.

Data availability

The datasets used and/or analyzed during the current study available from the corresponding author on reasonable request.

Received: 23 February 2025; Accepted: 28 October 2025
Published online: 27 November 2025

References

1. Sadrishojaei, M. et al. An energy-aware scheme for solving the routing problem in the internet of things based on Jaya and flower pollination algorithms. *J. Ambient Intell. Humaniz. Comput.* **14**(8), 11363–11372 (2023).
2. Sureshkumar, C. & Sabena, S. Fuzzy-based secure authentication and clustering algorithm for improving the energy efficiency in wireless sensor networks. *Wirel. Pers. Commun.* **112**, 1517–1536 (2020).
3. Zhu, J. et al. A new-type zeroing neural network model and Its application in dynamic cryptography. *IEEE Trans. Emerg. Top. Comput. Intell.* **9**(1), 176–191. https://doi.org/10.1109/TETCI.2024.3425282 (2025).
4. Khedo, K. K., Bissessur, Y. & Goolaub, D. S. An inland Wireless Sensor Network system for monitoring seismic activity. *Future Gener. Comput. Syst.* **105**, 520–532 (2020).
5. Naghibi, M. & Barati, H. SHSDA: Secure hybrid structure data aggregation method in wireless sensor networks. *J. Ambient Intell. Humaniz. Comput.* **12**, 10769–10788 (2021).
6. Hajian, R. & Erfani, S. H. CHESDA: Continuous hybrid and energy-efficient secure data aggregation for WSN. *J. Supercomput.* **77**, 5045–5075 (2021).
7. Sadrishojaei, M. & Kazemian, F. Development of an enhanced blockchain mechanism for internet of things authentication. *Wireless Pers. Commun.* **132**(4), 2543–2561 (2023).
8. Munusamy, N., Vijayan, S. & Ezhilarasi, M. Role of clustering, routing protocols, mac protocols and load balancing in wireless sensor networks: An energy-efficiency perspective. *Cybern. Inf. Technol.* **21**, 136–165 (2021).
9. Deniz, F., Bagci, H., Korpeoglu, I. & Yazıcı, A. Energy-efficient and fault-tolerant drone-BS placement in heterogeneous wireless sensor networks. *Wirel. Netw.* **27**, 825–838 (2021).
10. Zhang, Z., Liu, Z., Ning, L., Tian, H. & Wang, B. Belief-based fuzzy and imprecise clustering for arbitrary data distributions. *IEEE Trans. Fuzzy Syst.* https://doi.org/10.1109/TFUZZ.2025.3576588 (2025).
11. Mittal, N., Singh, U. & Salgotra, R. Tree-based threshold-sensitive energy-efficient routing approach for wireless sensor networks. *Wirel. Pers. Commun.* **108**, 473–492 (2019).
12. Khan, M. K. et al. Hierarchical routing protocols for wireless sensor networks: Functional and performance analysis. *J. Sens.* **2021**, 7459368 (2021).
13. Liu, X., Zhao, L. & Jin, J. A noise-tolerant fuzzy-type zeroing neural network for robust synchronization of chaotic systems. *Concurr. Comput. Pract. Exp.* **36**(22), e8218. https://doi.org/10.1002/cpe.8218 (2024).
14. Ning, F. et al. 3D CAD model dynamic clustering based on inertial feature encoder. *Appl. Soft Comput.* **182**, 113627. https://doi.org/10.1016/j.asoc.2025.113627 (2025).
15. Yao, M., Zhao, T., Cao, J. & Li, J. Hierarchical Fuzzy Topological System for High-Dimensional Data Regression Problems. *IEEE Trans. Fuzzy Syst.* **33**(7), 2084–2095. https://doi.org/10.1109/TFUZZ.2025.3549791 (2025).
16. Ashibani, Y. & Mahmoud, Q. H. Cyber physical systems security: Analysis, challenges and solutions. *Comput. Secur.* **68**, 81–97 (2017).
17. Vijayalakshmi, S., Kavithaa, G. & Kousik, N. Improving data communication of wireless sensor network using energy efficient adaptive cluster-head selection algorithm for secure routing. *Wirel. Pers. Commun.* **128**, 25–42 (2023).
18. Prakash, V., Singh, D., Pandey, S., Singh, S. & Singh, P. K. Energy-optimization route and cluster head selection using M-PSO and ga in wireless sensor networks. *Wirel. Pers. Commun.* https://doi.org/10.1007/s11277-024-11096-1 (2024).
19. Surenther, I., Sridhar, K. & Roberts, M. K. Maximizing energy efficiency in wireless sensor networks for data transmission: A deep learning-based grouping model approach. *Alex. Eng. J.* **83**, 53–65 (2023).
20. Macriga, G. A., Malarvizhi, K., Ahila, S. S., Ayyasamy, S. & Yashaswini, B. Energy efficient greedy tree based algorithm for data aggregation in wireless sensor network. *Meas. Sens.* **30**, 100910 (2023).
21. Misbha, D. Lightweight key distribution for secured and energy efficient communication in wireless sensor network: An optimization assisted model. *High-Confid. Comput.* **3**, 100126 (2023).
22. Mittal, M., Kobielnik, M., Gupta, S., Cheng, X. & Wozniak, M. An efficient quality of services based wireless sensor network for anomaly detection using soft computing approaches. *J. Cloud Comput.* **11**, 70 (2022).
23. Hu, L., Han, C., Wang, X., Zhu, H. & Ouyang, J. Security Enhancement for Deep Reinforcement Learning-Based Strategy in Energy-Efficient Wireless Sensor Networks. *Sensors* **24**, 1993 (2024).

24. Mistarihi, M. Z. et al. Energy-efficient bi-objective optimization based on the moth–flame algorithm for cluster head selection in a wireless sensor network. *Processes* **11**, 534 (2023).
25. Khashan, O. A., Ahmad, R. & Khafajah, N. M. An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. *Ad Hoc Netw.* **115**, 102448 (2021).
26. Harn, L., Hsu, C.-F., Xia, Z. & He, Z. Lightweight aggregated data encryption for wireless sensor networks (WSNs). *IEEE Sens. Lett.* **5**, 1–4 (2021).
27. Sadrishojaei, M., & Faeze, K., "Clustered routing scheme in IoT during COVID-19 pandemic using hybrid black widow optimization and harmony search algorithm.In: *Operations Research Forum*. Vol. 5. No. 2. Cham: Springer International Publishing, 2024.
28. Gu, Z., Yan, S., Ahn, C. K., Yue, D. & Xie, X. Event-triggered dissipative tracking control of networked control systems with distributed communication delay. *IEEE Syst. J.* **16**(2), 3320–3330. https://doi.org/10.1109/JSYST.2021.3079460 (2022).
29. Guo, W., Yan, C. & Lu, T. Optimizing the lifetime of wireless sensor networks via reinforcement-learning-based routing. *Int. J. Distrib. Sens. Netw.* **15**, 1550147719833541 (2019).
30. Xiangjun, Wu., Zong, G., Wang, H., Niu, B. & Zhao, X. Collision-free distributed adaptive resilient formation control for underactuated usvs subject to intermittent actuator faults and denial-of-service attacks. *IEEE Trans. Veh. Technol.* https://doi.org/10.1109/TVT.2025.3565820 (2025).
31. Xiangjun Wu, Shuo Ding, Ning Zhao, Huanqing Wang, Ben Niu, Neural-network-based event-triggered adaptive secure fault-tolerantcontainment control for nonlinear multi-agent systems underdenial-of-service attacks, Neural Networks, https://doi.org/10.1016/j.neunet.2025.107725.
32. Selvi, M., Santhosh Kumar, S. V. N., Thangaramya, K. & Abdul Gaffar, H. Energy efficient trust aware secure routing algorithm with attribute based encryption for wireless sensor networks. *Sci. Rep.* **15**(1), 1–18 (2025).
33. Wang, A., Yang, D. & Sun, D. A clustering algorithm based on energy information and cluster heads expectation for wireless sensor networks. *Comput. Electr. Eng.* **38**, 662–671 (2012).
34. Naruei, I. & Keynia, F. Wild horse optimizer: A new meta-heuristic algorithm for solving engineering optimization problems. *Eng. Comput.* **38**, 3025–3056 (2022).
35. Gu, Z., Sun, X., Lam, H.-K., Yue, D. & Xie, X. Event-based secure control of T-S fuzzy-based 5-DOF active semivehicle suspension systems subject to DoS attacks. *IEEE Trans. Fuzzy Syst.* **30**(6), 2032–2043. https://doi.org/10.1109/TFUZZ.2021.3073264 (2022).
36. Yan, S., Gu, Z., Park, J. H. & Xie, X. Adaptive memory-event-Triggered static output control of T-S Fuzzy wind turbine systems. *IEEE Trans. Fuzzy Syst.* **30**(9), 3894–3904. https://doi.org/10.1109/TFUZZ.2021.3133892 (2022).
37. Sadrishojaei, M. A delay aware routing approach for FANET based on emperor penguins colony algorithm. *Peer-to-Peer Networking and Applications* (2024): 1–14.
38. Chen, L. Cryptography standards in quantum time: new wine in old wineskin?. *IEEE Secur. Priv.* **15**, 51 (2017).
39. Panagiotou, P., Sklavos, N., Darra, E. & Zaharakis, I. D. Cryptographic system for data applications, in the context of internet of things. *Microprocess. Microsyst.* **72**, 102921 (2020).
40. Li, Y., Zhao, W., Zhang, C., Ye, J. & He, H. A study on the prediction of service reliability of wireless telecommunication system via distribution regression. *Reliab. Eng. Syst. Saf.* **250**, 110291. https://doi.org/10.1016/j.ress.2024.110291 (2024).
41. Luo, W., Takeuchi, N., Chen, O. & Yoshikawa, N. Low-autocorrelation random number generator based on adiabatic quantum-flux-parametron logicI. *IEEE Trans. Appl. Supercond.* **31**, 1–5 (2021).
42. Liu, S., Ning, Xu., Li, L., Alharbi, K. H. & Zhao, X. Zero-sum games-based optimal fault tolerant control for control-constrained multiplayer systems with external disturbances via adaptive dynamic programming. *Commun. Nonlinear Sci. Numer. Simul.* https://doi.org/10.1016/j.cnsns.2025.108804 (2025).
43. Fansen, W., Ning, X., Xudong, Z., Lun, L. & Al-Barakati, A. A. Dynamic memory event-triggered adaptive neural prescribed-time bipartite consensus control for high-order MASs with privacy preservation. *Commun. Nonlinear Sci. Num. Simul.* **145**, 108693 (2025).
44. Yousefpoor, M. S. & Barati, H. Dynamic key management algorithms in wireless sensor networks: A survey. *Comput. Commun.* **134**, 52–69 (2019).
45. Mir, M. & Trik, M. A novel intrusion detection framework for industrial IoT: GCN-GRU architecture optimized with ant colony optimization. *Comput. Electr. Eng.* **126**, 110541 (2025).
46. Khan, F. A., Ahmed, J., Khan, J. S., Ahmad, J., Khan, M. A. In: *2017 International conference on circuits, system and simulation (ICCSS).* 32–36 (IEEE).
47. Seyedzadeh, S. M., Norouzi, B., Mosavi, M. R. & Mirzakuchaki, S. A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. *Nonlinear Dyn.* **81**, 511–529 (2015).
48. Jain, K. et al. A lightweight multi-chaos-based image encryption Scheme for IoT Networks. *IEEE Access.* **12**, 62118–62148 (2024).
49. Sun, G., Li, Y., Liao, D. & Chang, V. Service function chain orchestration across multiple domains: A full mesh aggregation approach. *IEEE Trans. Netw. Serv. Manag.* **15**, 1175–1191 (2018).
50. Gupta, A., Malik, S., Goyal, M. & Gupta, P. Clustering approach for enhancing network energy using LEACH protocol in WSN. *Int. J. Wired Wirel. Commun.* **2**, 20–25 (2012).
51. Prvulovic, P., Radosavljevic, N., Babic, D. & Drajic, D. HERMEES: A holistic evaluation and ranking model for energy-efficient systems applied to selecting optimal lightweight cryptographic and topology construction protocols in wireless sensor networks. *Sensors* **25**(9), 2732 (2025).
52. Zhang, C., Zhang, H., Dang, S., Shihada, B. & Alouini, M. Gradient compression and correlation driven federated learning for wireless traffic prediction. *IEEE Trans. Cogn. Commun. Netw.* **11**(4), 2246–2258. https://doi.org/10.1109/TCCN.2024.3524183 (2025).
53. Liu, G., Wang, C., Tang, S. & Jiang, T. Security in wireless weak-link sensor networks: Directions recent advances, and challenges. *IEEE Netw.* https://doi.org/10.1109/MNET.2025.358013 (2025).
54. Vellingiri, J., Vedhavathy, T. R., Senthil Pandi, S. & Bala Subramanian, C. Fuzzy logic and CPSO-optimized key management for secure communication in decentralized IoT networks: A lightweight solution. *Peer-to-Peer Netw. Appl.* **17**(5), 2979–2997 (2024).

Author contributions

All authors participated in the conceptualization and design of the study. Data collection, simulation, and analysis were conducted by Mohsen Zarei, Mohammad Hosein Fatehi Dindarloo, Mehdi Taghizadeh, and Jasem Jamali. The initial draft of the manuscript was authored by Mohammad Hosein Fatehi Dindarloo, with all contributors providing feedback on earlier iterations of the document. All writers reviewed and endorsed the final manuscript.

Funding

The authors did not receive any financial support for this study.

Declarations

Competing interests
The authors have no competing interests as defined by Springer, or other interests that might be perceived to influence the results and/or discussion reported in this paper.

Ethical approval
Not applicable.

Additional information
Correspondence and requests for materials should be addressed to M.H.F.D.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.